**Contents**

1. **USDA LENDER INTERACTIVE NETWORK CONNECTION (LINC)**
   - 1.1 Introduction
   - 1.2 Accessing LINC
   - 1.3 Systems

2. **EAUTHENTICATION/LOGIN.GOV**
   - 2.1 eAuthentication System Requirement
   - 2.2 Creating an “unverified” Login.gov id

3. **Link Login.gov id**
   - 3.1 Link to existing eAuth account
   - 3.2 Link new login.gov id without eAuth account

4. **VERIFIED IDENTITY FOR LOGIN.GOV**
   - 4.1 Verify Identity at Login.gov
   - 4.2 Verify Identity by visiting a USDA Service Center

5. **MANAGING YOUR LOGIN.GOV ACCOUNT (FORGOTTEN PASSWORD, UPDATE CONTACT INFO, ETC.)**
   - 5.1 Forgotten Password
   - 5.2 Update Login.gov account information

6. **APPLICATION AUTHORIZATION SECURITY MANAGEMENT (AASM) SYSTEM – Security Administrators ONLY**
   - 6.1 Creating User Roles
   - 6.2 Adding a User Role (more than 1 role)
   - 6.3 Viewing a User List
   - 6.4 Role Maintenance
   - 6.5 Removing Roles or Users
   - 6.6 Validation Errors

7. **Contact US**

8. **APPENDIX**
   - Trading Partner Agreement
   - Addendum E to Trading Partner Agreement
   - Lender User Agreement for SFH Guaranteed Annual Fees (GAF)
   - Service Bureau Addendum for SFH Guaranteed Annual Fees (GAF)
   - GUS User Agreement & Training Certificate
   - Lender Agent Request Form
   - Lender Request for Branch Addition/Modification to the Rural Development Database
   - Request for Adding or Removing a Security Administrator
   - Form RD 3555-16, Agreement for Participation in Single Family Housing Guaranteed / Insured Loan Programs
1 USDA LENDER INTERACTIVE NETWORK CONNECTION (LINC)

1.1 Introduction

The USDA Lender Interactive Network Connection (LINC) is a web based interactive system that provides approved Rural Housing Service (RHS) lenders access to Single Family Housing Guaranteed (SFHG) systems and resources. RHS takes security very seriously due to the sensitivity of the data electronically shared and the threat of compromised web sites. RHS uses multiple mechanisms, each building on the other to create a very secure environment. First, the web browser on the PC being used to access the USDA LINC web site must support 128-bit encryption using Secure Socket Layer. Encryption scrambles the data sent so that no one except the intended recipient can read the confidential data. Secondly, each financial organization must complete the applicable User Agreement(s) for each system(s) requested (see the Appendix to this Guide for a list of Agreements). In the Agreement(s), one or more Security Administrators from your organization are identified and must be set up by USDA.

There are important actions which users and Security Administrators must complete first to gain access to the SFHG systems available on the LINC website (these are explained in detail later in this Guide):

1. All users must obtain an eAuthentication (eAuth)/Login.gov account (see section II).
2. Security Administrators must establish appropriate security roles for their associates in Application Authorization System Management (AASM).

1.2 Accessing LINC

To access LINC, please go to: https://usdalinc.sc.egov.usda.gov/USDALINChome.do and select RHS LINC Home or the Rural Housing Service icon:

Select the applicable SFHG system or select the Message Board for system messages such as updates or expected downtimes. Visit the Training and Resource Library to review extensive SFHG training materials and resources:
1.3 Systems

The chart below provides a general description of each of the SFHG systems users can access through LINC, once the appropriate eAuth account and AASM security role has been established for each user.

<table>
<thead>
<tr>
<th>SFHG SYSTEM</th>
<th>GENERAL DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Status Reporting (ESR)</td>
<td>This system is for SFHG loan servicers to submit their monthly investor/default status reports and make corrections (ESR Status Reporting Corrections link). Electronic reporting is required.</td>
</tr>
<tr>
<td>Guaranteed Annual Fee</td>
<td>This system is for SFHG loan servicers to access and pay the monthly bills for annual fees due on their portfolio.</td>
</tr>
<tr>
<td>Guaranteed Underwriting System (GUS)</td>
<td>This system is for SFHG originating lenders to enter guaranteed loan applications and submit them to the Agency’s underwriting system, which will provide an underwriting recommendation on the loan and determine eligibility of the applicant, loan, and property. Loans are submitted to the Agency electronically via GUS and eliminates manual file submissions.</td>
</tr>
<tr>
<td>Lender Loan Closing / Administration</td>
<td>This system is for SFHG originating lenders to submit loan closing transactions, the upfront guarantee fee and technology fee electronically. All required documents are uploaded to the system and the Loan Note Guarantee generated is by the system once approved by the Agency.</td>
</tr>
<tr>
<td>Application Authorization System Maintenance (AASM)</td>
<td>This system is for Security Administrators to establish new lender users, define security roles for lender users, modify user roles and access levels, add lender agent, and delete lender users from the SFHG systems. The security role assigned in AASM controls the system functionality the user can access within a specific SFHG system.</td>
</tr>
<tr>
<td>Lender Pre-Authorized Debit (PAD) Account Maintenance</td>
<td>This system is for SFHG lenders to set up Pre-Authorized Debit (PAD) accounts that they will use to electronically send the payment of the upfront guarantee fees and technology fees. SFHG loan servicers will use this system to set up the PAD account they will use to electronically pay all annual fees that are owed.</td>
</tr>
<tr>
<td>Loss Claim Administration</td>
<td>This system is for SFHG loan servicers to enter and submit their loss claims to the Agency electronically to collect on the guarantee and upload all required documentation.</td>
</tr>
<tr>
<td>Loss Mitigation System</td>
<td>This system is for SFHG loan servicers to submit loan servicing plans electronically to the Agency and upload all required supporting documentation. Servicers input and approve their own servicing plans. This system is accessed through Loss Claim Administration</td>
</tr>
<tr>
<td>Mortgage Recovery Advance Receivable (MRARCV)</td>
<td>This System will allow servicers to consent to pre-authorized debit (PAD) receivable payments &amp; review receivable payment history for SFHG loans with MRA’s.</td>
</tr>
</tbody>
</table>
2 EAUTHENTICATION/LOGIN.GOV

eAuthentication will be updated Monday, September 11, 2023, to introduce a new login user interface for USDA systems. eAuthentication has partnered with Login.gov to provide public customers a multi-factor authentication login option for secure and convenient access to USDA sites.

To conduct official business transactions online (remitting fees, forms, completing applications, etc.) users must create a Login.gov account or have an existing eAuthentication (eAuth) account. An eAuth/Login.gov account provides secure, convenient access to multiple USDA applications, websites, and programs.

- **eAuthentication (eAuth) ID** – Existing users of the system currently have an eAuth ID. These users can continue to use their current eAuth ID and are not required to create a Login.gov ID at this time. However, existing users are encouraged to create a Login.gov ID and link their existing eAuth ID to the Login.gov ID. An implementation date for the requirement of Login.gov IDs has not been determined and will be communicated later.

- **Login.gov ID** - New users will be required to create a Login.gov account to gain access to USDA systems.

2.1 eAuthentication System Requirement

Following is a chart of account requirements for each of the SFHG Systems which can be accessed on the USDA LINC website at [https://usdalinc.sc.egov.usda.gov/](https://usdalinc.sc.egov.usda.gov/).

Once registered you may use the same Eauth credential/Login.gov credential for all SFHG systems. It is recommended to bookmark the USDA LINC page and always access systems from this menu.

Note: A GUS user cannot act as both an approved lender and a lender agent in GUS with the same credential. One credential must be established for the approved lender and a separate credential for the lender agent. Reference the below chart to determine Verified or Non-verified system requirements. As a reminder, once a user has established an eAuthentication/login.gov account, additional authorization is required in the Application Authorization Security Management System (AASM) by their organization’s respective system Security Administrator. See Section 6.
## SUMMARY OF eAUTH/LOGIN.GOV ACCOUNT REQUIREMENTS FOR SFHG SYSTEMS

<table>
<thead>
<tr>
<th>System</th>
<th>UNVERIFIED identity eAuth/Login.gov account required (f/k/a Level 1)</th>
<th>VERIFIED identity eAuth/Login.gov account required (f/k/a Level 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Authorization (AASM)</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Electronic Status Reporting Corrections</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Electronic Status Reporting</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Guarantee Annual Fee</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Guaranteed Underwriting System (GUS)</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Lender Loan Closing/Administration (LLC)</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Lender PAD Account Maintenance</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Loss Claim Administration</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Mortgage Recovery Advance (MRA)</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

### 2.2 Creating an “unverified” Login.gov id

To create an unverified Login.gov account visit the RHS LINC page and select the link for the system needed (screenshots below):

1. Select RHS Linc page [https://usdalinc.sc.egov.usda.gov/RHShome.do](https://usdalinc.sc.egov.usda.gov/RHShome.do)
2. Select USDA System.

3. Select Create Account Option on the eAuth login page.

4. Select Customer as the type of user and Continue.

5. Select Continue to Login.gov

Customers - Use Login.gov

eAuth is now using Login.gov for our Public Citizens who want to conduct business online with USDA. Please click the Continue to Login.gov button to create your account.
6. Select Create an Account, enter your email address, select email language preference, acknowledge and accept login.gov Rules of Use, and select Submit.

7. Check your email account.

Check your email

We sent an email to ca___________@com with a link to confirm your email address. Follow the link to continue creating your account.

Didn't receive an email? Resend

Or, use a different email address

You can close this window if you're done.

8. Confirm your email address from your email account.
9. Create a strong password and select Continue.

Create a strong password
Your password must be 12 characters or longer. Don’t use common phrases or repeated characters, like abc or 111.

Password

Confirm password

Show password

Password strength: Good

Continue

10. Select two authentication methods (most common chosen are text/voice and backup codes). Select Continue.

Authentication method setup
Add another layer of security by selecting a multi-factor authentication method. We recommend you select at least two different options in case you lose one of your methods.

- Authentication application
  Download or use an authentication app of your choice to generate secure codes.

- Text or voice message
  Receive a secure code by (SMS) text or phone call.

- Backup codes
  A list of 10 codes you can print or save to your device. When you use the last code, we will generate a new list. Keep in mind backup codes are easy to lose.

- Security key
  A physical device, often shaped like a USB drive, that you plug in to your device.

- Government employee ID
  PIV/DAC cards for government and military employees. Desktop only.

Continue
11. Example if Text is chosen. Enter Phone number SMS or Phone call and select **Send code**. Note: you can choose another authentication method by selecting the link at the bottom of the screen.

12. Enter your one-time code received.

13. Phone was added to your account. Example is for choice of backup codes. If you want to use back up code, select **Continue**. Otherwise choose the link at the bottom for another authentication method.
14. Save backup codes by downloading, printing, or copying. Check you have saved codes and select **Continue**.

15. Select **Agree and Continue** to share your information with USDA eAuth. Your login.gov account has been created. You will be taken to USDA eAuth page where you will choose to link your newly created id with or without an existing eAuth id.

For more assistance visit the contact us page at the bottom of the login.gov screen
https://www.login.gov/contact/
3 Link Login.gov id

Existing users should choose “Use an existing eAuth account to link to my Login.gov account”. New users should choose “Continue without linking to an existing eAuth account”. You will receive this page from step 13 above or the first time you log in to Login.gov after initial setup.

3.1 Link to existing eAuth account

1. Select “Use an existing eAuth account to link my Login.gov account” and select Continue.

2. Select Customer.
3. Enter your existing eAuth User ID and Password. Select Log In.

![Customer Login]

User ID
Forgot User ID
AshleyTest

Password
Forgot Password

Log In

4. Select Yes to continue to Link your eAuth ID with Login.gov.

![Continue Link with Login.gov]

Note: After linking, your Login.gov account must be used for all future access to USDA websites and Application. Users should also keep a record of the eAuthentication credential the new Login.gov credential is linked with.

5. User will receive an email notification eAuth account was successfully linked.

If you have current roles assigned in USDA systems, you can continue to use those systems with your Login.gov credential. Select the application link from [https://usdalinc.sc.egov.usda.gov/RHShome.do](https://usdalinc.sc.egov.usda.gov/RHShome.do). Select Customer, Login.gov, Sign in, Enter email address and password.
3.2  **Link new login.gov id without eAuth account**

1. Select “**Continue without linking to an existing eAuth account**” and select **Continue**.

2. Enter users **First name** and **Last name**. Select **Submit**
   
   **User Information Required**

   ![User Information Form](image)

   - First name: Ashley
   - Last name: Carlson

3. The account information screen will display with the user’s information and Login.gov as linked.

4. To gain access to systems that allow “unverified” eAuth ID access (i.e., GUS), the user must provide the Lender’s Security Administrator with their Login.gov email address to be added as a user and assigned a security role. Continue to Section 4 for steps to complete Verified Identity.
4 VERIFIED IDENTITY FOR LOGIN.GOV

Most SFHG systems require a Login.gov account with verified identity or an existing eAuth credential linked with a Login.gov account with verified identity. If a user has an unverified Login.gov account or an existing unverified eAuth linked account and attempts to access a system which requires identity verification, user will receive a message and will be prompted to Verify Identity (online is strongly recommended).

1. Select a SFHG System (verified identity required) link from https://usdalinc.sc.egov.usda.gov/RHShome.do.

2. Select Verify Identity choice of Verify my identity at Login.gov (Recommended) or Visit a USDA Service Center.

4.1 Verify Identity at Login.gov

1. Select Verify my identity at Login.gov (Recommended) and Continue

   ![Verify Identity](image)

2. Select Continue to Login.gov

   ![Verify Identity at Login.gov](image)

3. Sign in with your login information at Login.gov and follow the prompts to verify identity. For additional instructions refer to https://login.gov/help/. You will receive an email once your identity has been verified online.
4. **For Security Administrators and initial system access:** additional steps are required via AASM. See Section 6.
   **For Lender Employees:** Contact your System Administrator for your company to gain access to the appropriate SFHG system.

4.2 **Verify Identity by visiting a USDA Service Center**

1. **Select Visit a USDA Service Center and Continue**

   **Verify Identity**
   You have reached this page because you were unable to complete the identity verification process at Login.gov. You can either try again at Login.gov, or visit a USDA Service Center for in-person identity verification.

   - [ ] Verify my identity at Login.gov
   - [ ] USDA Service Center for in-person identity verification

   **Continue**

2. **Enter Date of birth and select Continue.**

   **Verify Identity**
   You have selected the option to visit a USDA Service Center in person.

   To start the process, please provide your date of birth. This information must match your government issued photo ID (e.g., State Driver’s License). Upon submitting this form, you are certifying you provided your correct and true information.

   **Date of birth**
   For example: 04 28 1986
   Month  Day  Year

   **Continue**

3. **Enter Additional Data Required and select Continue.**

   **Verify Identity In-Person**
   To approve online, visit a USDA Service Center. We need to collect some additional information. Please complete the form below and submit it in person. This information must match your government issued photo ID (e.g., Driver’s License).

   **First name:**
   
   **Middle name (optional):**
   
   **Last name:**
   
   **Suffix (optional):**
   
   **Home country:**
   
   **Home address:**
   
   **Home city:**
   
   **Home state:**
   
   **Home zip code:**
   
   **Home phone:**
   
   **Date of birth:**
   
   **Continue**
4. Select Find Service Center.

5. Select State and County and select GO. Closest local offices will be displayed.

6. User will receive an email that Final Step Needed

7. For Security Administrators and initial system access: additional steps are required via AASM. See Section VI.
   For Lender Employees: Contact your System Administrator for your company to gain access to the appropriate SFHG system.

5. MANAGING YOUR LOGIN.GOV ACCOUNT (FORGOTTEN PASSWORD, UPDATE CONTACT INFO, ETC.)

Users can manage their account from Login.gov or eAuthentication screen which will take the user to Login.gov

5.1 Forgotten Password

1. Select Sign in with LOGIN.GOV
2. Select **Forgot your password**.

3. Enter **Email address** and select **Continue**.

4. User will receive a link to reset password. Once acceptable password has been reset, user will receive an email stating password was reset.

5.2 **Update Login.gov account information**

1. Visit [https://www.login.gov/](https://www.login.gov/)

2. Select **Sign in with LOGIN.GOV**
3. Enter Login.gov Sign in information and select Sign in.

4. Update account information as needed.

Note: If you add a new email address, once confirmed, log back in to Login.gov and delete the old email address. The new email address will become your sign in email address.
6 APPLICATION AUTHORIZATION SECURITY MANAGEMENT (AASM) SYSTEM – Security Administrators ONLY

In addition to eAuth/Login.gov account requirements, each person using a SFHG system is assigned a Security Role in the AASM system. To access AASM, financial organizations must first designate Security Administrators. AASM provides a means for these designated Security Administrators to:

- Establish new lender users
- Define security roles for lender users
- Modify user roles and access levels
- Add lender agents
- Delete lender users from the system

The security role, as assigned by the Security Administrator, controls the system functionality the user can access within each specific SFHG system.

*A financial organization must have at least one associate (two is highly recommended) assigned a Security Administrator role by the Agency. Security Administrator roles are requested using the appropriate User Agreement(s), which are included in the Appendix of this guide. Security Administrators will receive an email when their ID has been activated by the Agency.

*The financial organization’s Security Administrator(s) are responsible for assigning the proper security type roles to their associates. This is done to give the financial organization control over which of their associates can access / use the system, and their level of access.

*Users MAY NOT share access identification in any system. Each user must have an accurately assigned role, as roles define how much functionality is allowed.

*While Security Administrators are responsible for assigning/modifying/deleting security roles for their associates, requests for adding, removing, or inactivating a Security Administrator user must be completed by USDA. The financial organization must submit the form Request for Adding or Removing a Security Administrator to the Agency. This form is in the Appendix.
PLEASE REVIEW THE GENERAL DESCRIPTIONS OF EACH AASM SECURITY ROLE, AS WELL AS A SUMMARY OF AASM SECURITY ROLES BY SYSTEM, ON THE NEXT TWO PAGES.

<table>
<thead>
<tr>
<th>AASM Security Role</th>
<th>General Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*Branch Administrator</td>
<td>Allows the user to grant branch roles for only the lender branch for which the user is associated. Also allows the user full update and submit authority for only the lender branch for which the user is associated.</td>
</tr>
<tr>
<td>*Branch Rep</td>
<td>Allows the user full update (but no submit authority) for only the lender branch for which the user is associated; allowed to perform loan closing transactions for only their associated branch, etc. Branch Reps can complete preliminary submittals in GUS.</td>
</tr>
<tr>
<td>*Branch Rep w/Final Submit Authority</td>
<td>Allows the user full update and submit authority for only the lender branch for which the user is associated.</td>
</tr>
<tr>
<td>*Branch Viewer</td>
<td>Allows the user view only capabilities of all applications for the branch for which the user is associated.</td>
</tr>
<tr>
<td>Lender Administrator</td>
<td>Allows the user to grant lender or branch roles to other users assigned to any of the lender’s branches. Also allows the user full update and submit authority for all the lender's branches.</td>
</tr>
<tr>
<td>Lender Agent</td>
<td>Allows the user to enter GUS applications on behalf of a Lender and perform preliminary submissions. When the Lender Agent has completed their portion of the application process, they will release the application to the Lender for underwriting processing. Lender Agent users can only be associated with one lender agent organization; however, they can be associated with multiple approved lenders. Note: The approved lender’s GUS Security Administrator must enter the Lender Agent ID (i.e. nine-digit Federal Tax ID Number of the Agent’s organization) when establishing this role in the system. If the Lender Agent ID does not exist in USDA’s system, the Security Administrator will receive an error prompting them to contact the RD Help Desk to establish the Lender Agent ID in the system. See Appendix for the Lender Agent Request Form.</td>
</tr>
<tr>
<td>Lender Rep</td>
<td>Allows the user full update, but no submit authority for all the lender’s branches; allowed to perform loan closing transactions, etc.</td>
</tr>
<tr>
<td>Lender Rep w/Final Submit Authority</td>
<td>Allows the user full update and submit authority for all the lender’s branches.</td>
</tr>
<tr>
<td>Lender Viewer</td>
<td>Allows the user view only capabilities associated with the lender Tax ID for all branches.</td>
</tr>
<tr>
<td>Service Bureau Administrator</td>
<td>Allows the user to grant Service Bureau roles to other users assigned to any of the Service Bureau’s branches. Also allows the user full update and submit authority for all the Lender Branches associated to the Service Bureau.</td>
</tr>
<tr>
<td>Service Bureau Rep</td>
<td>Allows the user full update, but no submit authority for all the Lender Branches associated to the Service Bureau.</td>
</tr>
<tr>
<td>Service Bureau Rep w/Final Submit Authority</td>
<td>Allows the user full update and submit authority for all the Lender Branches associated to the Service Bureau.</td>
</tr>
<tr>
<td>Service Bureau Viewer</td>
<td>Allows the user view only capabilities for all the Lender Branches associated to the Service Bureau.</td>
</tr>
</tbody>
</table>

*Each lender doing business with Rural Development (RD) is assigned a branch number within the RD database. Branches are created with information provided by the lender. To request an addition or modification of branches, a person within your organization authorized to report and make changes may submit the form USDA Branch Addition/Modification Request form found in the appendix.
### AASM ROLES BY SYSTEM

<table>
<thead>
<tr>
<th>Role</th>
<th>Annual Fees</th>
<th>Electronic Status Reporting (ESR)</th>
<th>GUS</th>
<th>Lender Loan Closing (LLC)</th>
<th>Loss Claim</th>
<th>Loss Mitig.</th>
<th>PreAuth Debit (PAD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch Administrator</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Branch Rep</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Branch Rep w/Final Submit Auth.</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Branch Viewer</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Lender Administrator</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Lender Agent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lender Rep</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Lender Rep w/Final Submit Auth.</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lender Viewer</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Service Bureau Administrator</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Service Bureau Rep</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Service Bureau Rep w/Final Submit Auth.</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Bureau Viewer</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>
6.1 Creating User Roles

Once the intended user provides the Security Administrator with their eAuth/Login.gov ID, the Security Administrator will access the LINC website to update users and provide access to the applicable system(s) for their organization. Users will be unable to utilize the systems until the Security Administrator adds them as a user and assigns a user role. The website is: https://usdalinc.sc.egov.usda.gov/.

1. Go to LINC. Select RHS LINC from the menu:

![LINC website screenshot]

2. Select Application Authorization.

![Application Authorization menu]

3. Sign in using eAuth/Login.gov ID and password, Only Security Administrators are permitted access to this website.

4. The Application Authorization Security Management screen will appear:
5. To add a new user, select the applicable System ID, then select Add User.

*Note- Only the systems you have access to will show up in the system list

6. Enter the new users eAuth/login.gov User ID and tab out of the field. A message will appear at the top of your screen ‘Retrieving Data, Please Wait...’. Data the user submitted while creating the eAuth account will populate in the Name, Phone/Ext, and Email Address fields if available. All fields with an (*) must be completed. Select Save.

Note: If user has already been created in the system you will receive a popup message “Cannot add-User already exists. Would you like to continue in Change mode?” Select Ok, Select Add Role and move to step 8.
7. Pop-up box appears once the user is successfully created. However, a security role still needs to be established – select OK.

8. Select the **Authorized System** and **Security Role**, based upon responsibilities of the user. The Security Role dropdown will populate based on the Authorized System selected, as not all Security Roles are applicable to all Authorized Systems. A description of the available roles will display at the bottom of the screen. Also, you may refer to the **AASM Roles by System** chart in this Guide for a summary description of all security roles.

   Note: GUS access is referenced for illustration purposes.

9. Once SA selects the **Security Role**, the **Lender ID**, and **USDA Assigned Branch Nbr** fields will dynamically display. The Loan Program checkbox may appear. Complete the required fields and select **Save**:

   Add Successful pop-up message will appear. The added user will receive an auto-generated email which confirms their access.
6.2 Adding a User Role (more than 1 role)
A Security Administrator can add additional roles to existing users.

1. Access the User List page, select Add Role from the Action drop down, and press the link for the eAuth User ID.

2. Select the appropriate Authorized System:

3. Select applicable Security Role: Complete the Lender ID & USDA Assigned Branch Nbr fields, place a check in RH then select Save:

Note: In GUS you cannot have a role with an approved lender and a lender agent at the same time. However, lender agents may be tied to several approved lenders.
6.3 Viewing a User List
A Security Administrator can view a list of all activated users associated with their Tax ID.

1. Security Administrator will access the LINC. Select RHS Linc Home, then Application Authorization.
2. Type an asterisk (*) in the eAuth User ID field, or leave the eAuth User ID field blank, and select Submit. (You may opt to refine the search by selecting a specific system in the System ID dropdown.)

6.4 Role Maintenance
To modify an established user’s role, the Security Administrator will need to perform the below steps:

1. The Security Administrator will access LINC. Select RHS Linc Home, then Application Authorization to navigate to the User List.

2. Enter the eAuth/Login.gov User ID of a specific user and select Submit.

3. Select Maintain Role from the Action dropdown and select the Role hyperlink of the user you wish to modify.
4. The current assigned **Security Role** can be seen in the dropdown. Select the **new security role** from the dropdown, then select **Save**:

Note: If the user has multiple system roles you will choose the **Select radio button** to populate the **Lender ID and USDA Assigned Branch Nbr fields**.

5. The user will receive an email confirmation of the change.

6.5 **Removing Roles or Users**

When a user needs to be removed from the system (e.g., user leaves place of employment, changes area of concentration with same employer, etc.), Security Administrators are tasked with making changes in the system to ensure that only eligible users continue to have access.

1. The Security Administrator will access the **LINC**. Select **RHS Linc Home**, then **Application Authorization** to navigate to the User List screen.

2. Enter the **eAuth/Login.gov User ID** of a specific user and select **Submit**.
3. Select **Maintain Role** from the **Action** dropdown and select the **Role hyperlink** of the user you wish to modify.

4. On the User Role Maintenance screen, the **Remove Role** button removes the user's specified Security Role for all Authorized Systems. To remove individual roles, skip to step 5.
5. Alternatively, if the Security Administrator clicks on the **Select** radio button and populates the **Lender or Lender/Service Bureau ID** and **USDA Assigned Branch Nbr**, the Remove Role button becomes disabled and the **Remove ID** button becomes enabled. The Remove ID button removes the user’s specified Security Role for the Authorized System for ONLY the specified Lender ID or Lender/Service Bureau ID that user is associated with.

![User Role Maintenance](image)

6. **Validation Errors**

The Security Administrator may encounter validation errors when attempting to add users. See below examples

Occurs when a user updates their email address in their eAuth profile. In most situations, there are 2 options to correct the error which will display on the AASM screen. See screen print examples below for validation errors for each scenario:

1. Example: In this scenario, lender is attempting to add a previous eAuth user ID tied to an old email address and the address and eAuth user ID has been updated. See options in screen print.

![Validation Errors](image)
2. Example: In this scenario, lender is attempting to add a user id that exists in GUS with an existing role. See options in screen print.

3. Example: In this scenario, lender is adding an updated eAuth user id however an existing role exists with an old eAuth user ID (same eAuth profile but email address has changed/updated). See options in screen print.
## 7 Contact US

<table>
<thead>
<tr>
<th>Technical Issues: GUS/GLS</th>
<th><a href="mailto:RD.HD@usda.gov">RD.HD@usda.gov</a> or 800-457-3642 Option 2, Option 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training &amp; Guides</td>
<td>USDA LINC Training &amp; Resource Library</td>
</tr>
</tbody>
</table>
All listed forms can be found in the LINC Training and Resource Library under the SFHG System referenced below:


<table>
<thead>
<tr>
<th>SFHG SYSTEM</th>
<th>FORMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Status Reporting (ESR)</td>
<td>• Trading Partner Agreement</td>
</tr>
<tr>
<td></td>
<td>• Addendum E to Trading Partner Agreement</td>
</tr>
<tr>
<td>Guaranteed Annual Fee / Lender Pre-Authorized Debit (PAD) Account Maintenance</td>
<td>• Lender User Agreement for SFH Guaranteed Annual Fees (GAF)</td>
</tr>
<tr>
<td></td>
<td>• Service Bureau Addendum for SFH Guaranteed Annual Fees (GAF))</td>
</tr>
<tr>
<td></td>
<td>• Service Bureau User Agreement for SFH Guaranteed Annual Fees (GAF)</td>
</tr>
<tr>
<td>Loss Claim Administration</td>
<td>• Addendum E to Trading Partner Agreement</td>
</tr>
<tr>
<td>Guaranteed Underwriting System (GUS)</td>
<td>• GUS User Agreement &amp; Training Certificate</td>
</tr>
<tr>
<td></td>
<td>• Lender Agent Request Form</td>
</tr>
<tr>
<td></td>
<td>• Lender Request for Branch Addition/Modification to the Rural</td>
</tr>
<tr>
<td></td>
<td>Development Database</td>
</tr>
<tr>
<td>Lender Loan Closing / Administration</td>
<td>• User Agreement for Single Family Housing Guarantee Lender Loan</td>
</tr>
<tr>
<td></td>
<td>Closing (LLC)</td>
</tr>
<tr>
<td>Loss Mitigation System</td>
<td>• Loss Mitigation User Agreement</td>
</tr>
<tr>
<td>Mortgage Recovery Advance Receivable (MRARCV)</td>
<td>• SFH Mortgage Recovery Advance Receivable Lender User Agreement</td>
</tr>
<tr>
<td>Security</td>
<td>• Request for Adding or Removing a Security Administrator</td>
</tr>
<tr>
<td>SFH Guaranteed Loan Basic Training and Resources</td>
<td>• Form RD 3555-16, Agreement for Participation in Single Family</td>
</tr>
<tr>
<td></td>
<td>Housing Guaranteed / Insured Loan Programs</td>
</tr>
</tbody>
</table>