Contents

1 USDA LENDER INTERACTIVE NETWORK CONNECTION (LINC) ................................................................. 3
   1.1 Introduction ........................................................................................................................................... 3
   1.2 Accessing LINC ................................................................................................................................. 3
   1.3 Systems ............................................................................................................................................... 4

2 EAUTHENTICATION/LOGIN.GOV ........................................................................................................... 5
   2.1 eAuthentication System Requirement ............................................................................................... 5

2.1 Creating a Login.gov Id and Linking eAuth .......................................................................................... 6
   2.1.1 Link Login.gov id when email does not match existing eAuth email ........................................... 9
       2.1.1 Use an existing eAuth account to link to my Login.gov account ........................................... 9
       2.1.2 Continue without linking to an existing eAuth account ......................................................... 9
   2.2 Multiple eAuth Accounts found with same email as Login.gov account ......................................... 10

3 VERIFIED IDENTITY FOR LOGIN.GOV ............................................................................................... 10
   3.1 Verify Identity at Login.gov ............................................................................................................... 10
   3.2 Verify Identity by visiting a USDA Service Center .......................................................................... 11

4 MANAGING YOUR LOGIN.GOV ACCOUNT (FORGOTTEN PASSWORD, UPDATE CONTACT INFO, ETC.) .... 11
   4.1 Forgotten Password ............................................................................................................................ 11
   4.2 Update Login.gov account information ............................................................................................ 12

5 APPLICATION AUTHORIZATION SECURITY MANAGEMENT (AASM) SYSTEM – Security Administrators ONLY . 14
   5.1 Creating User Roles ........................................................................................................................... 17
   5.2 Adding a User Role (more than 1 role) ............................................................................................... 20
   5.3 Viewing a User List ............................................................................................................................. 21
   5.4 Role Maintenance ............................................................................................................................... 21
   5.5 Removing Roles or Users .................................................................................................................... 22
   5.6 Validation Errors ................................................................................................................................ 24

6 Contact US ............................................................................................................................................... 26

7 APPENDIX ............................................................................................................................................... 27
   • Trading Partner Agreement .................................................................................................................... 27
   • Addendum E to Trading Partner Agreement .......................................................................................... 27
   • Lender User Agreement for SFH Guaranteed Annual Fees (GAF) ....................................................... 27
   • Service Bureau Addendum for SFH Guaranteed Annual Fees (GAF) .................................................. 27
   • GUS User Agreement & Training Certificate ...................................................................................... 27
   • Lender Agent Request Form .................................................................................................................. 27
   • Lender Request for Branch Addition/Modification to the Rural Development Database .................. 27
   • Request for Adding or Removing a Security Administrator ................................................................. 27
   • Form RD 3555-16, Agreement for Participation in Single Family Housing Guaranteed / Insured Loan Programs ......................................................................................................................... 27
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 in order 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 each of their users in the Application Authorization Security Management (AASM) system.

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><strong>Electronic Status Reporting (ESR)</strong></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><strong>Guaranteed Annual Fee</strong></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><strong>Guaranteed Underwriting System (GUS)</strong></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><strong>Lender Loan Closing / Administration</strong></td>
<td>This system is for SFHG originating lenders to submit loan closing transactions, the upfront guarantee fee and technology fee (if applicable). All required documents are uploaded to the system and the Loan Note Guarantee is auto-generated once approved by the Agency.</td>
</tr>
<tr>
<td><strong>Application Authorization Security Maintenance (AASM)</strong></td>
<td>This system is for Security Administrators to establish new lender users, define security roles for lender users, modify existing user roles and access levels, add lender agent users, and delete lender users from SFHG systems. The security role assigned in AASM dictates what a user can access within a specific SFHG system.</td>
</tr>
<tr>
<td><strong>Lender PreAuthorized Debit (PAD) Account Maintenance</strong></td>
<td>This system is for SFHG lenders to set up PreAuthorized Debit (PAD) accounts that they will use to electronically send payment of the upfront guarantee fee and technology fee (if applicable) associated with loan closing transactions. 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><strong>Loss Claim Administration</strong></td>
<td>This system is for SFHG loan servicers to enter and submit loss claim requests to the Agency to collect on the loan guarantee and upload required documentation.</td>
</tr>
<tr>
<td><strong>Loss Mitigation System</strong></td>
<td>This system is for SFHG loan servicers to submit loan servicing plans to the Agency and upload required supporting documentation. Servicers input and approve their own servicing plans. This system is accessed through Loss Claim Administration</td>
</tr>
<tr>
<td><strong>Mortgage Recovery Advance Receivable (MRARCV)</strong></td>
<td>This System will allow servicers to consent to preAuthorized 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/.

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 5.
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>x</td>
<td></td>
</tr>
<tr>
<td>Electronic Status Reporting</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Guarantee Annual Fee</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Guaranteed Underwriting System (GUS)</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Lender Loan Closing/Administration (LLC)</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Lender PAD Account Maintenance</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Loss Claim Administration</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Mortgage Recovery Advance (MRA)</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

2. Creating a Login.gov Id and Linking eAuth

2. Select "USDA System" choice under Single Family Guaranteed Rural Housing header (i.e – Guaranteed Underwriting System (GUS), Electronic Status Reporting (ESR) or any other system listed you will be requesting access).

*Note: It is important, if you have an existing eAuth account that your email address on your existing eAuth account matches your email address you will be entering on your Login.gov account you will be creating. If it does not, update your eAuth profile on the eAuth login screen under "Manage Account" before beginning the process in Login.gov for a smoother transition.*

3. Select Customer as the type of user and Continue.
4. Select Login.gov
5. Select **Create an Account, Enter Info**, select **Submit**.
6. Check your email account.
7. Confirm your email address from your email account.
8. Create a strong password and select **Continue**.
9. Select at least one authentication method (most common methods chosen are text/voice and backup codes). Select **Continue**
   Examples:
   - Enter your one-time code received.
   - 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.
   - Save backup codes by downloading, printing, or copying. Check you have saved codes and select **Continue**.
10. **Add another method** or **Skip for now**
11. Select **Agree and Continue** to continue to USDA eAuth - Cert. Your Login.gov account has been created.
12. 1 of 3 messages will appear based on user specific scenario to connect your Login.gov to eAuth:

1. If the email address used on the Login.gov account is the same email address associated with an existing eAuth account, the accounts will link automatically. A message is presented, and the user is informed their Login.gov account must be used for all future logins with USDA. User will be prompted to continue with Login.gov by selecting Yes. User will be taken to the application.
   a. If user has an existing system security role, then no further action is needed, and the user can continue to use system(s) as normal. User will receive an email notification that their eAuth account was successfully linked.
   b. If user does not have an existing security role in the requested system, then the user will receive a message they do not have access. User can notify their Security Administrator (SA) to request a system role. SA will use the users Login.gov email address as the eAuth ID in AASM and add a security role. (See Section 5.1)

   Continue Link with Login.gov?

   After linking, your Login.gov account must be used for all future access to USDA websites and applications.

   [No] [Yes]

   Or;

2. If the user doesn’t have an existing eAuth account in the system, with the same email address as the Login.gov account they just created, eAuth will ask the user if they want to use an existing eAuth account to link with Login.gov or continue without linking to an existing eAuth account? (See 2.1 for further directions)

   Link with Login.gov

   Login.gov must be linked to an eAuth account to use it with USDA applications.

   [ ] Use an existing eAuth account to link to my Login.gov account.
   [ ] Continue without linking to an existing eAuth account.

   Continue

   Or;

3. If the user has multiple eAuth accounts in the system, with an email address that matches the Login.gov email address just created, the user will be notified that multiple existing eAuth accounts were found. (See Section 2.2 for further directions)
2.1 **Link Login.gov id when email does not match existing eAuth email**

Users with an existing eAuth account should choose “Use an existing eAuth account to link to my Login.gov account”. *(See 2.1.1)*

New users with only a Login.gov id or existing eAuth users that are unable to log in to their existing eAuth account (e.g., unable to reset password) would choose “Continue without linking to an existing eAuth account”. *(See 2.1.2)*

### 2.1.1 Use an existing eAuth account to link to my Login.gov account

1. Select “Use an existing eAuth account to link my Login.gov account” and select **Continue**.
   
   *Note: Sharing ID’s is not allowed. Do not link to an existing eAuth account if your personal information is not associated with the existing eAuth account profile.*

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

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

4. User will be taken to the application. If user has an existing security role no further action is needed, user can continue to use system(s) as normal. If user does not have an existing security role in a system, user will receive a message they do not have access. User can notify their Security Administrator (SA) to give them a security role. *(See Section 5.1)*

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

### 2.1.2 Continue without linking to an existing 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**

3. 1 of 2 messages will be received depending on the system the user clicked on to start the Login.gov process:
   - New GUS users will receive a message: GUS Login Failure – Your Account is missing a security role (proceed to step 4)
   - Other new system users (i.e., ESR, LLC, Loss Claim, etc.) – User should be prompted for “**Verified Identity**”. Continue to Section 4 for steps to complete **Verified Identity** for all other systems.

4. To gain access to systems that allow “unverified” eAuth ID access (i.e., GUS), the user must provide their Security Administrator (SA) with their Login.gov email address to be added as a user and assigned a security role. SA will use the users Login.gov email address as the eAuth ID in AASM and add a security role. *(See Section 5.1)*
2.2 **Multiple eAuth Accounts found with same email as Login.gov account**

1. Select the existing eAuth User ID from the list presented to link with Login.gov id just created and select **Continue**.
2. Enter your existing **eAuth User ID** and **Password**. Select **Log In**.
3. Select **Yes** to continue to Link your eAuth ID with Login.gov.
4. User will be taken to the specified application. If user has an existing security role, then no further action is needed, and the user can continue to use system(s) as normal. If user does not have an existing security role in a system, then the user will receive a message they do not have access. User can notify their Security Administrator (SA) to request a security role in the specified system. SA will use the user’s Login.gov email address as the eAuth ID in AASM and add a security role. (See Section 5.1)
5. User will receive an email notification eAuth account was successfully linked.

Once an existing eAuth account is linked with Login.gov, the Login.gov account must be used for all future access to USDA websites. If you attempt to log in with the eAuth account after it is linked, you will be informed you must use Login.gov for access.


3 **VERIFIED IDENTITY FOR LOGIN.GOV**

All SFHG systems, aside from GUS and AASM, 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 be prompted to **Verify Identity** (online is strongly recommended).

1. Select a system link under Single Family Guaranteed Rural Housing menu that requires verified identity (all systems, aside for GUS and AASM, will prompt for identity verification) from [https://usdalinc.sc.egov.usda.gov/RHShome.do](https://usdalinc.sc.egov.usda.gov/RHShome.do).
2. Select **Verify my identity at Login.gov** (Recommended) or **Visit a USDA Service Center**.

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

   **Verify Identity**

   The application you are accessing requires identity verification. Your account does not currently meet these requirements. Please select the method to verify your identity below.

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

   ![Continue](image)

3.1 **Verify Identity at Login.gov**

1. Select **Verify my identity at Login.gov** and **Continue**

2. Select **Continue to Login.gov**

3. Sign in with your login information at Login.gov and follow the prompts to verify Identity.

   Note: If your state issued id cannot be recognized via uploaded photo, then Login.gov offers an option to verify identity at a local post office. For additional instructions refer to [https://Login.gov/help/verify-your-identity/how-to-verify-your-identity/](https://Login.gov/help/verify-your-identity/how-to-verify-your-identity/). You will receive an email once your identity has been verified online or at a post office.
4. Once verified:
   - **For Security Administrators and initial system access**: additional steps are required via AASM. See Section 5.
   - **For Lender Employees**: Contact your System Administrator (SA) for your company to gain access to the appropriate SFHG system.

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

1. Select **Visit a USDA Service Center** and **Continue**
2. Enter **Date of birth** and select **Continue**.
3. Enter **Additional Data Required** and select **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 for final steps needed. Call the local office and make appointment to ensure Local Registration Authority (LRA) is available to assist you for in-person identity verification.
7. Once Verified:
   - **For Security Administrators and initial system access**: additional steps are required via AASM. See Section 5.
   - **For Lender Employees**: Contact your System Administrator (SA) for your company to gain access to the appropriate SFHG system.

4 **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

4.1 **Forgotten Password**

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

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

   **Forgot your password?**
   
   Don’t know your password? Reset it after confirming your email address.

   Email address

   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.

4.2 **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.
5 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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>See chart on the next page for description of each 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>x</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>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Lender Agent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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></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>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Bureau Rep</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Bureau Rep w/Final Submit Auth.</td>
<td></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></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.1 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 Screen]

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:

![Application Authorization Security Management Screen]

User List:
- Tax Id
- System Id
- eAuth User ID
- Last Name
- First Name

Submit, Reset, Add User
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 contine 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.
5.2 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.
5.3 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.)

5.4 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.

5.5 **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.

5.6 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.
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.
## 6 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>
7 APPENDIX

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