



Rural Development
U.S. DEPARTMENT OF AGRICULTURE

SINGLE FAMILY HOUSING GUARANTEED LOAN PROGRAM

LTE System Access and Security Guide

Final Version 1.0

8/24



Contents

1	USDA LENDER INTERACTIVE NETWORK CONNECTION (LINC) TEST ENVIROMENT	3
1.1	Introduction	3
1.2	Accessing LINC LTE	3
2	EAUTHENTICATION/LOGIN.GOV	3
2.1	Creating an “unverified” Login.gov id	4
3	Link Login.gov id	9
3.1	Link to existing eAuth account	9
3.2	Link new login.gov id without an existing eAuth account	10
4	MANAGING YOUR LOGIN.GOV ACCOUNT (FORGOTTEN PASSWORD, UPDATE CONTACT INFO, ETC.)	12
4.1	Forgotten Password	12
4.2	Update Login.gov account information	13
5	APPLICATION AUTHORIZATION SECURITY MANAGEMENT (AASM) SYSTEM – Security Administrators ONLY .	14
5.1	Creating User Roles	16
5.2	Viewing a User List	18
5.3	Role Maintenance	18
5.4	Removing Roles or Users	20
5.5	Validation Errors	21
5.6	Adding or Removing Security Administrators	23
6	Contact US	23

1 USDA LENDER INTERACTIVE NETWORK CONNECTION (LINC) TEST ENVIRONMENT

1.1 Introduction

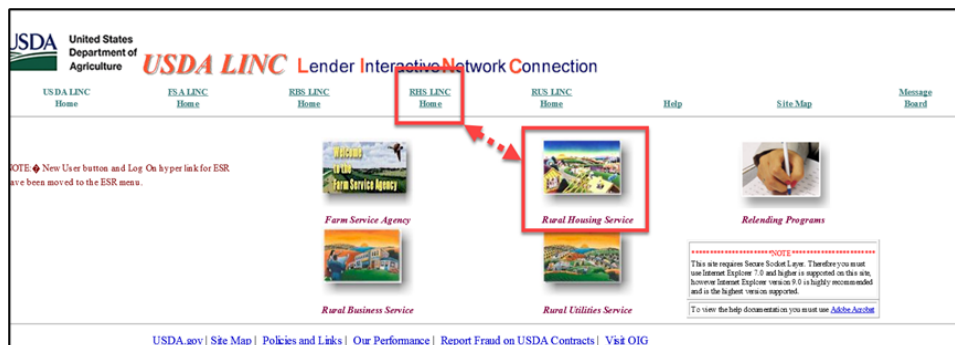
The USDA Lender Interactive Network Connection (LINC) Lender Test environment (LTE) is a web based interactive system that provides approved Rural Housing Service (RHS) lenders access to Single Family Housing Guaranteed (SFHG) systems and resources. RHS takes security very seriously due to the sensitivity 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 a Login.gov account (see section II).
2. Security Administrators must establish appropriate security roles for their associates in the Application Authorization System Management (AASM).

1.2 Accessing LINC LTE

To access LINC LTE, please go to: <https://usdalinc-le.cert.sc.egov.usda.gov/> and select **RHS LINC Home** or the Rural Housing Service icon:



Select Guarantee Underwriting System (GUS LTE). Visit the [Training and Resource Library](#) extensive SFHG training materials and resources:

2 EAUTHENTICATION/LOGIN.GOV

eAuthentication was 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 are encouraged to create a Login.gov ID and link their existing eAuth ID to the Login.gov ID. Requirement of Login.gov IDs to be transitioned is by September 30, 2024.
- **Login.gov ID** - New users will be required to create a Login.gov account to gain access to USDA systems.

2.1 Creating an “unverified” Login.gov id

To create an unverified Login.gov test account visit the RHS LINC page and select GUS LTE (screenshots below):

1. Select RHS Linc page <https://usdalinc-le.cert.sc.egov.usda.gov/>



2. Select USDA System.

Single Family Guaranteed Rural Housing
[Electronic Status Reporting \(ESR\)](#)
[Electronic Status Reporting Corrections](#)
[Guaranteed Annual Fee](#)
[Mortgage Recovery Advance Receivable Payments](#)
[Mortgage Recovery Advance Receivable History](#)
[Loss Claim Administration](#)
[Guaranteed Underwriting System \(GUS\)](#)
[Lender Loan Closing/Administration](#)
[ID Cross Reference](#)
[Application Authorization](#)
[Lender PAD Account Maintenance](#)
[Training and Resource Library](#)

3. Select **Customer** as the type of user and **Continue**.

Account Registration ?

What type of user are you?

- ☒ Customer
- ☐ USDA Employee / Contractor
- ☐ Other Federal Employee / Contractor

Continue

4. 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.

Continue to Login.gov

Cancel

5. Select **Create an Account**, enter your email address, select email language preference, acknowledge and accept login.gov Rules of Use, and select **Submit**.



USDA eAuth - Cert is using
Login.gov to allow you to sign in to
your account safely and securely.

Sign in

Create an account

Create an account for new users

Enter your email address

Select your email language preference

Login.gov allows you to receive your email communication in English, Spanish or French.

☒ English (default)

☐ Español

☐ Français

☐ I read and accept the Login.gov [Rules of Use](#)

Submit

6. Check your email account.

Check your email

We sent an email to **ca [REDACTED] com** with a link to confirm your email address. Follow the link to continue creating your account.

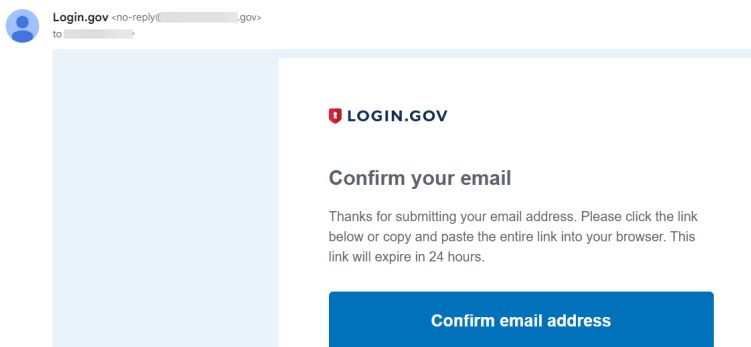


Didn't receive an email? [Resend](#)


Or, [use a different email address](#)

You can close this window if you're done.

7. Confirm your email address from your email account.



8. Create a strong password and select **Continue**.

 You have confirmed your email address

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


9. Select two authentication methods (most common chosen are text/voice and backup codes however only 1 choice is required). 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/CAC cards for government and military employees. Desktop only.

Continue

10. 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.

Get your one-time code

We'll send you a one-time code each time you sign in.

Phone number

How you'll get your code

☒ Text message (SMS)

☐ Phone call

You can change this anytime. If you use a landline number, select "Phone call."

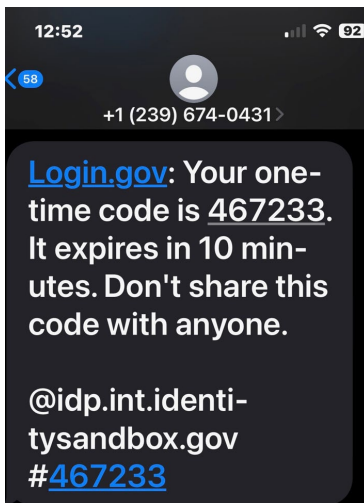
Send code

Message and data rates may apply. Do not use web-based (VOIP) phone services or premium rate (toll) phone numbers.

[Mobile terms of service](#)

[Choose another authentication method](#)

11. Enter your one-time code received.



Enter your one-time code

We sent a text (SMS) with a one-time code to +1 704-4. This code will expire in 10 minutes.

One-time code
Example: 123456

☒ Remember this browser

Submit

[Send another code](#)

12. 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 or choose **skip for now** and go to step 14.

✓ A phone was added to your account.

Are you sure you want to use backup codes?

Backup codes are the least preferred authentication method because the codes can easily be lost. Try a safer option, like an authentication application or a security key.

We'll give you 10 codes that you can download, print, copy or write down. You'll enter one code every time you sign in.

Continue

[Choose another authentication method](#)

13. Save backup codes by downloading, printing, or copying. Check you have saved codes and select **Continue**.

Save these backup codes

If you lose your device, you'll need these codes to sign into Login.gov. Save or print them and put them somewhere safe.

B26S-MVHE-CQVK	443T-0FJ6-0YK3
RPS6-ZYMQ-P1RZ	XHKN-E13M-55KV
WZPJ-8RGN-TS6H	89E7-XNFQ-0J14
R5XD-TJFZ-1QYM	AK8S-T8V4-DD2S
JZ3S-K8M8-TDK8	CMVK-2RPX-C8WS

⚠ Each code can only be used once. We'll give you new codes after you use all ten.

[Download](#) [Print](#) [Copy](#)

☒ I've put my backup codes in a safe place.

Continue

14. 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.

✓ Backup codes were added to your account.

Continue to USDA eAuth - Cert

We'll share your information with **USDA eAuth - Cert** to connect your account.

✓ Email address
ca[redacted].com

Agree and continue

[Cancel](#)

Customer Login

[Need an account?](#)
Not a Customer? [Change user type](#)

Select an option to continue

Login.gov
Enter Login.gov User ID and Password

eAuth User ID
Enter User ID and Password

Please wait...

User ID [Forgot User ID](#)

Password [Forgot Password](#)

☐ Show Password

Log In

For more assistance visit the contact us page at the bottom of the login.gov screen
<https://www.login.gov/contact/>

For agencies

[Become a partner](#)

[Developer guide](#)

Learn

[About us](#)

[Accessibility statement](#)

[Join us](#)

[Privacy & security](#)

Support

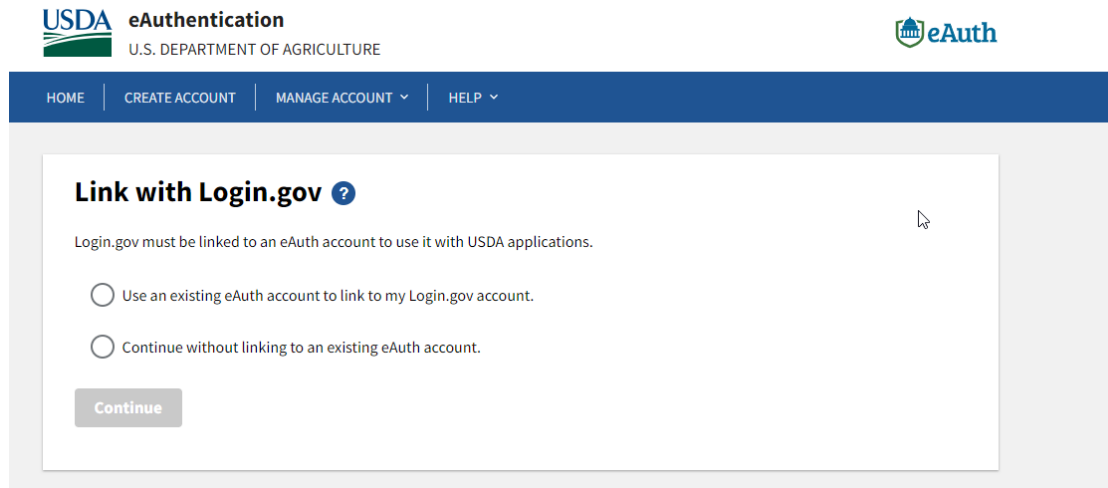
[Contact us](#)

[Help center](#)

[Login.gov system status](#)

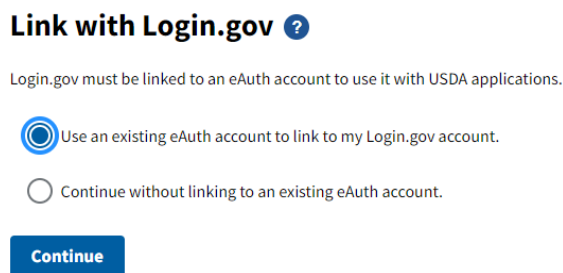
3 Link Login.gov id

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 14 above or the first time you log in to Login.gov after initial setup.

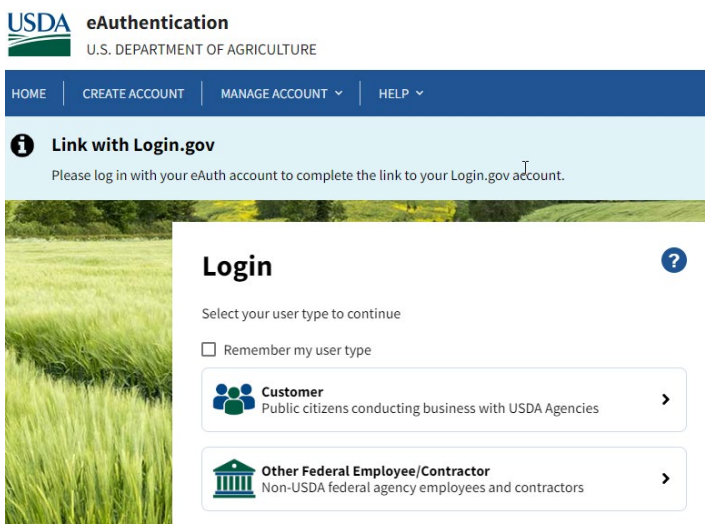


3.1 Link to existing eAuth account

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 ?

[Need an account?](#)
Not a Customer? [Change user type](#)

Select an option to continue

eAuth User ID
Enter User ID and Password

User ID [Forgot User ID](#)
Ashleytest

Password [Forgot Password](#)
Lo: [password field]

☒ Show Password

Log In

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

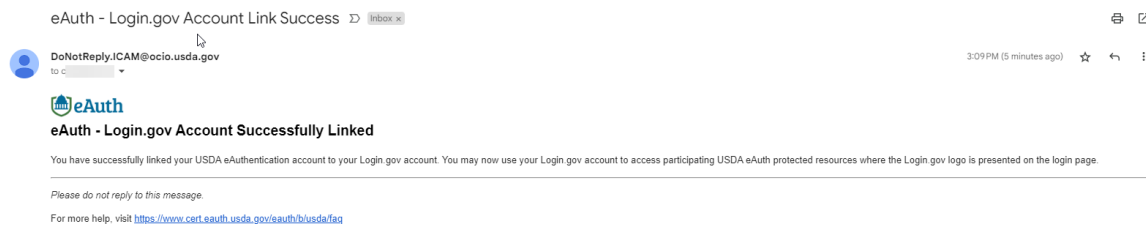
Continue Link with Login.gov?

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

No **Yes**

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 GUS LTE, you can continue to use GUS LTE with your Login.gov credential. Select GUS link from <https://usdalinc-le.cert.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 an existing eAuth account

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

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

2. Enter users **First name** and **Last name**. Select **Submit**

User Information Required ?

In order to complete setting up your Login.gov account with USDA eAuth, please provide the following information:

First name

Ashley

Last name

Carlan

Submit

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

USDA eAuthentication
U.S. DEPARTMENT OF AGRICULTURE

HOME | CREATE ACCOUNT | MANAGE ACCOUNT | HELP

Account Information ? [Logout](#)

Login Information

Email address: carlan@usda.gov

Login.gov ? Linked
To update your Login.gov account, please visit [Login.gov](#).

Personal Information [Edit](#)

Name: Ashley Carlan

Multi-Factor Authentication (MFA) Options

PIV/CAC ? [Enable](#)
Use your non-USDA Federal PIV/CAC to login to your eAuth account.

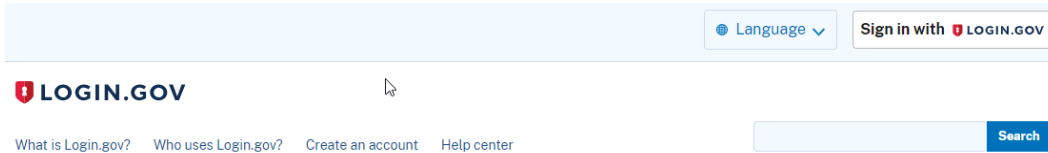
4. To gain access to GUS LTE, the user must provide the Lender's LTE Security Administrator with their Login.gov email address to be added as a user and assigned a security role in the testing environment.
- *If you are signing up initially for GUS LTE, you will put your information on the Addendum to the GUS USER AGREEMENT for the GUS LTE Environment (Verified Identity is not required for GUS LTE).

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

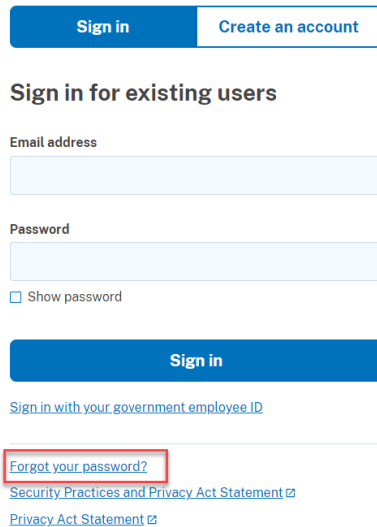
4.1 *Forgotten Password*

1. Select **Sign in with LOGIN.GOV**



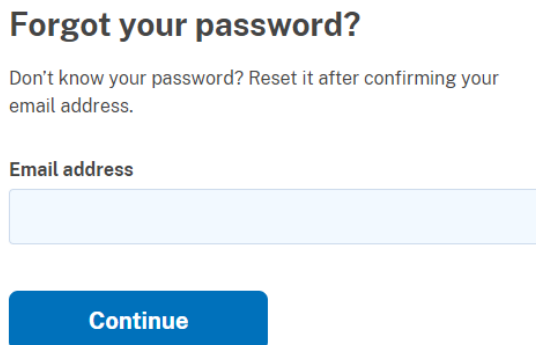
The screenshot shows the top navigation bar of the Login.gov website. On the right, there is a 'Language' dropdown menu and a 'Sign in with LOGIN.GOV' button. Below the navigation bar, the 'LOGIN.GOV' logo is displayed on the left, and a 'Search' button is on the right. In the center, there are links for 'What is Login.gov?', 'Who uses Login.gov?', 'Create an account', and 'Help center'.

2. Select **Forgot your password.**



The screenshot shows the 'Sign in for existing users' section of the Login.gov page. It includes input fields for 'Email address' and 'Password', a 'Show password' checkbox, and a 'Sign in' button. Below the 'Sign in' button, there is a link for 'Sign in with your government employee ID'. At the bottom, the 'Forgot your password?' link is highlighted with a red box. Other links include 'Security Practices and Privacy Act Statement' and 'Privacy Act Statement'.

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



The screenshot shows the 'Forgot your password?' page. It features the heading 'Forgot your password?' and a subheading 'Don't know your password? Reset it after confirming your email address.' Below this is an input field for 'Email address' and a 'Continue' button.

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/>
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. For more information go to [Manage My Account](#).

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

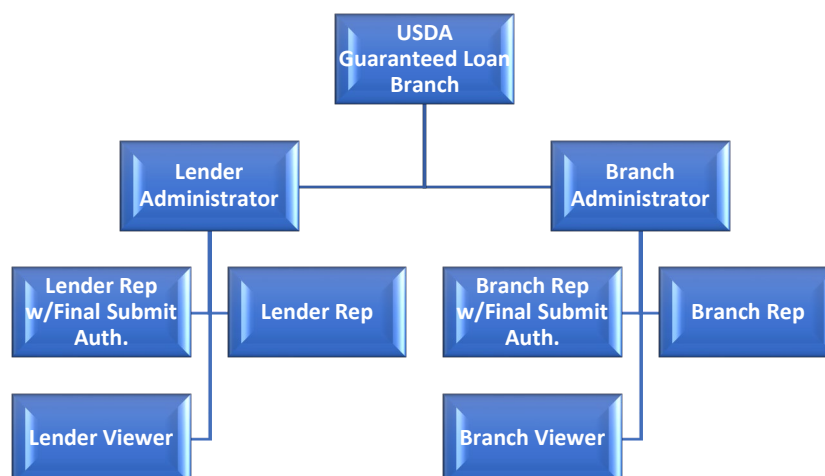
The security role, as assigned by the Security Administrator, controls the system functionality the user can access within each specific SFHG system.

*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.

AASM Security Role	General Description
*Branch Administrator	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.
*Branch Rep	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.
*Branch Rep w/Final Submit Authority	Allows the user full update and submit authority for only the lender branch for which the user is associated.
*Branch Viewer	Allows the user view only capabilities of all applications for the branch for which the user is associated.
Lender Administrator	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.
Lender Agent	<p>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.</p> <p><u>Note:</u> 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.</p>
Lender Rep	Allows the user full update, but no submit authority for all the lender's branches; allowed to perform loan closing transactions, etc.
Lender Rep w/Final Submit Authority	Allows the user full update and submit authority for all the lender's branches.
Lender Viewer	Allows the user view only capabilities associated with the lender Tax ID for all branches.

*Each lender doing business with Rural Development (RD) is assigned a branch number within the RD data base. 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.

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](https://usdalinc-le.cert.sc.egov.usda.gov/RHShome.do) 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-le.cert.sc.egov.usda.gov/RHShome.do>

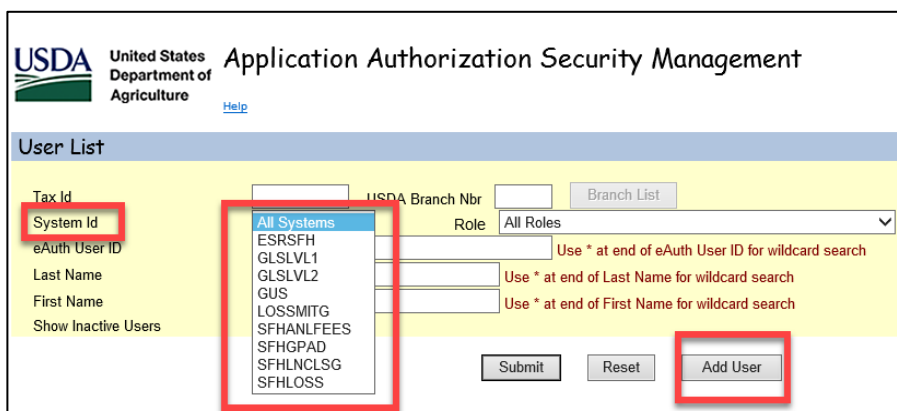
1. Go to [LINC](https://usdalinc-le.cert.sc.egov.usda.gov/RHShome.do).
2. Select **Application Authorization**.



3. Sign in using **Login.gov ID** and **password**, Only Security Administrators are permitted access to this website.
4. The *Application Authorization Security Management* screen will appear:

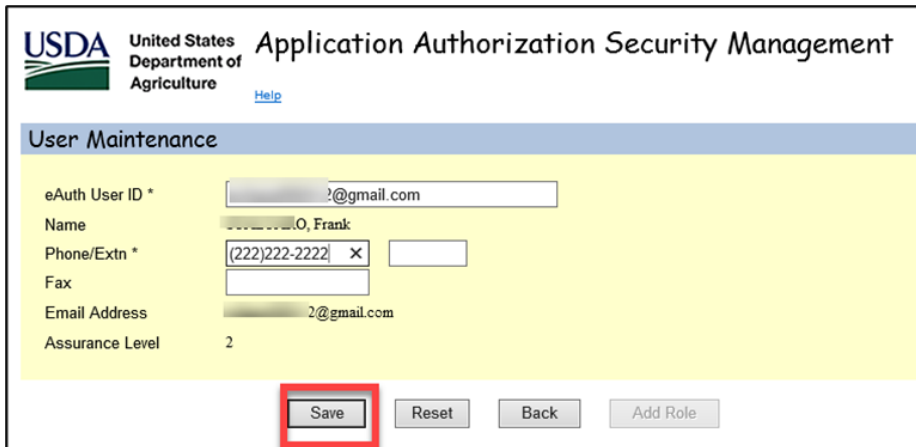


5. To add a new user, select **Guaranteed Underwriting System GUS**, then select **Add User**.



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/Logging.gov account will populate in the Name, Phone/Ext, and Email Address fields if available. You may have to enter the phone number. 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.



USDA United States Department of Agriculture Application Authorization Security Management

Help

User Maintenance

eAuth User ID * [?]@gmail.com

Name [?] O, Frank

Phone/Ext * (222)222-2222 X []

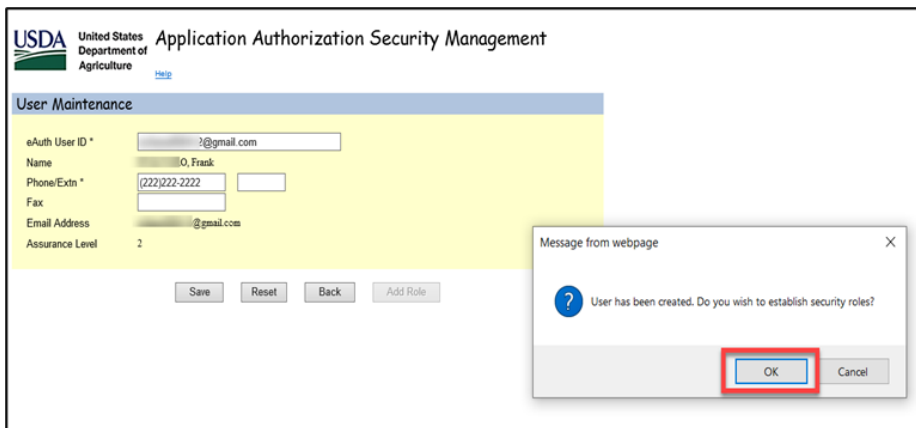
Fax []

Email Address [?]@gmail.com

Assurance Level 2

Save Reset Back Add Role

7. Pop-up box appears once the user is successfully created. However, a security role still needs to be established – select **OK**.



USDA United States Department of Agriculture Application Authorization Security Management

Help

User Maintenance

eAuth User ID * [?]@gmail.com

Name [?] O, Frank

Phone/Ext * (222)222-2222 X []

Fax []

Email Address [?]@gmail.com

Assurance Level 2

Save Reset Back Add Role

Message from webpage

User has been created. Do you wish to establish security roles?

OK Cancel

8. Select **GUS** 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.

User Role Maintenance

eAuth User ID: QU 73
 Last Name: P
 First Name: J
 Phone/Extn: ()
 Fax: ()
 Email Address: J. [redacted]@ov
 Assurance Level: 2
 Status: Active

Authorized System *: Guaranteed Underwriting System
 Security Role *: **Select**

Security Roles Ordered in Descending Order:

- Lender Representative with Final Submit Authority
- Lender Representative
- Lender Viewer
- Branch Representative with Final Submit Authority
- Branch Representative
- Branch Viewer
- Lender Agent

- 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 Viewing a User List

A Security Administrator can view a list of all activated users associated with their Tax ID.

- Security Administrator will access the [LINC](#) . Select **Application Authorization**.
- 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.)

USDA United States Department of Agriculture Application Authorization Security Management

User List

Tax Id: [] USDA Branch Nbr: [] Branch List: []
 System Id: All Systems Role: All Roles
 eAuth User ID: * Use * at end of eAuth User ID for wildcard search
 Last Name: [] Use * at end of Last Name for wildcard search
 First Name: [] Use * at end of First Name for wildcard search
 Show Inactive Users: ☐

Submit Reset Add User

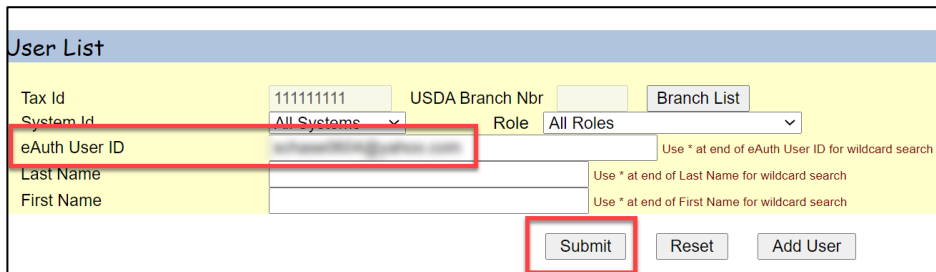
Action: Maintain Role

eAuth User ID	Name	Status	System	Role	Tax Id	Branch	Program	Lender Name
[redacted]	[redacted]	Active	GLSLV12	Branch Administrator	[redacted]	001	FSA	[redacted]
[redacted]	[redacted]	Active	GLSLV12	Lender Administrator	[redacted]	002	RH	[redacted]
[redacted]	[redacted]	Active	GLSLV12	Lender Administrator	[redacted]	001	BP, FSA	[redacted]
[redacted]	[redacted]	Active	GLSLV12	Branch Administrator	[redacted]	005	FSA	[redacted]

5.3 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 **Application Authorization** to navigate to the **User List**
2. Enter the **eAuth/Login.gov User ID** of a specific user and select **Submit**.



User List

Tax Id: 111111111 USDA Branch Nbr: Branch List:

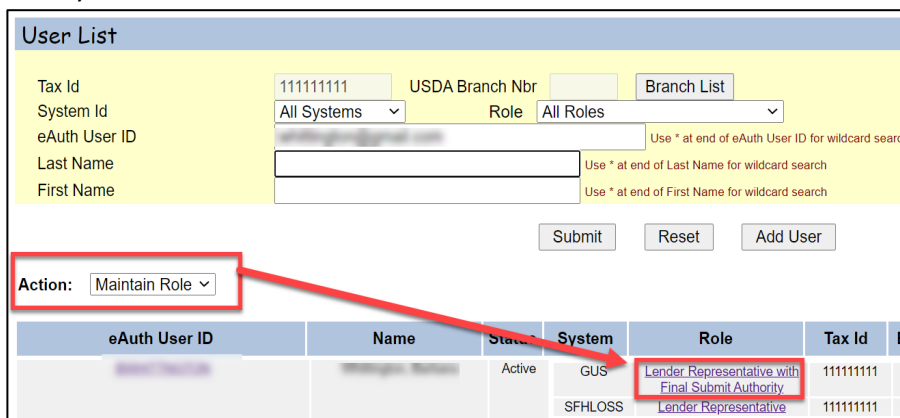
System Id: All Systems Role: All Roles

eAuth User ID Use * at end of eAuth User ID for wildcard search

Last Name Use * at end of Last Name for wildcard search

First Name Use * at end of First Name for wildcard search

3. Select **Maintain Role** from the Action dropdown and select the **Role hyperlink** of the user you wish to modify.



User List

Tax Id: 111111111 USDA Branch Nbr: Branch List:

System Id: All Systems Role: All Roles

eAuth User ID Use * at end of eAuth User ID for wildcard search

Last Name Use * at end of Last Name for wildcard search

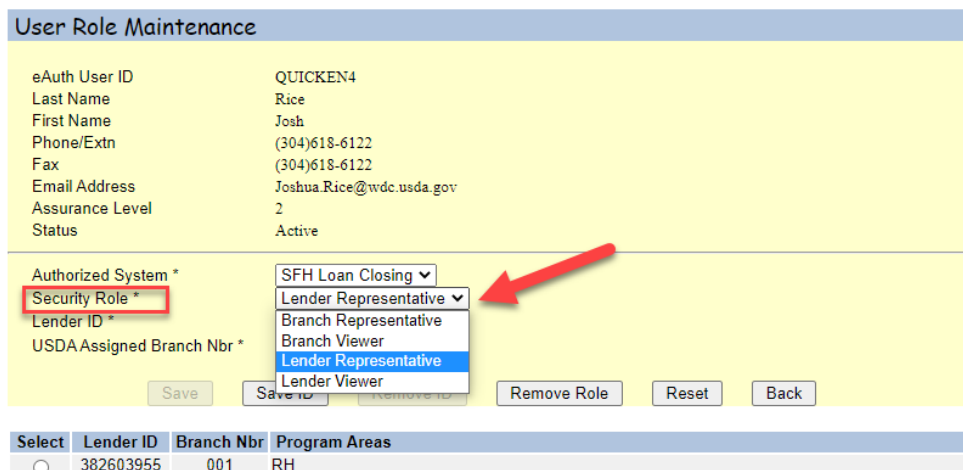
First Name Use * at end of First Name for wildcard search

Action:

eAuth User ID	Name	Status	System	Role	Tax Id	B
[Redacted]	[Redacted]	Active	GUS	Lender Representative with Final Submit Authority	111111111	
			SFHLOSS	Lender Representative	111111111	

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.



User Role Maintenance

eAuth User ID: QUICKEN4

Last Name: Rice

First Name: Josh

Phone/Extn: (304)618-6122

Fax: (304)618-6122

Email Address: Joshua.Rice@wdc.usda.gov

Assurance Level: 2

Status: Active

Authorized System *: SFH Loan Closing

Security Role * Lender Representative

Lender ID *:

USDA Assigned Branch Nbr *:

Select	Lender ID	Branch Nbr	Program Areas
<input type="radio"/>	382603955	001	RH

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

5.4 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 **Application Authorization** to navigate to the User List screen.
2. Enter the **eAuth/Login.gov User ID** of a specific user and select **Submit**.

USDA United States Department of Agriculture Application Authorization Security Management

LINC Home | Logoff | Help

User List

Tax Id: 111111111 USDA Branch Nbr: Branch List

System Id: All Systems Role: All Roles

eAuth User ID: [Redacted] Use * at end of eAuth User ID for wildcard search

Last Name: [Redacted] Use * at end of Last Name for wildcard search

First Name: [Redacted] Use * at end of First Name for wildcard search

Submit Reset Add User

3. Select **Maintain Role** from the **Action** dropdown and select the **Role hyperlink** of the user you wish to modify.

USDA United States Department of Agriculture Application Authorization Security Management

LINC Home | Logoff | Help

User List

Tax Id: 111111111 USDA Branch Nbr: Branch List

System Id: All Systems Role: All Roles

eAuth User ID: [Redacted] Use * at end of eAuth User ID for wildcard search

Last Name: [Redacted] Use * at end of Last Name for wildcard search

First Name: [Redacted] Use * at end of First Name for wildcard search

Submit Reset Add User

Action: Maintain Role

eAuth User ID	Name	Status	System	Role	Tax Id	B
[Redacted]	[Redacted]	Active	GUS	Lender Representative with Final Submit Authority	111111111	
[Redacted]	[Redacted]		SFHLOSS	Lender Representative	111111111	

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.

User Role Maintenance

eAuth User ID: [blurred]
 Last Name: [blurred]
 First Name: [blurred]
 Phone/Extn: [blurred]
 Fax: [blurred]
 Email Address: [blurred]
 Assurance Level: 1
 Status: Active

Authorized System *: SFH Annual Fees ▾
 Security Role *: Lender Representative with Final Submit Authority ▾
 Lender/Service Bureau ID *: Select ▾
 USDA Assigned Branch Nbr *: [] BranchList

Save Save ID Remove ID Remove Role Reset Back

Leave Blank

Select	Lender/Service Bureau ID	Branch Nbr	Program Areas
<input type="radio"/>	111111111	001	RH

- 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

eAuth User ID: [blurred]
 Last Name: [blurred]
 First Name: [blurred]
 Phone/Extn: [blurred]
 Fax: [blurred]
 Email Address: [blurred]
 Assurance Level: 1
 Status: Active

Authorized System *: SFH Annual Fees ▾
 Security Role *: Lender Representative with Final Submit Authority ▾
 Lender/Service Bureau ID *: 111111111 ▾ USDA RURAL DEVELOPMENT
 USDA Assigned Branch Nbr: 001 BranchList
 Loan Program *: (☒ RH)

Save Save ID Remove ID Remove Role Reset Back

Select	Lender/Service Bureau ID	Branch Nbr	Program Areas
<input checked="" type="radio"/>	111111111	001	RH

5.5 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:

- 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.

Validation Errors

This eAuth User ID cannot be added/modified in AASM. This is likely due to an email address change or an old user ID. There are 2 options to resolve this issue:

1. If the previous user ID role is assigned by current lender organization, click the back button and search for the previous user ID on the User List. If previous User ID is found, choose the Action "Maintain Role". Click Role hyperlink and click Remove Role. Click Ok. Once the previous eAuth User ID role has been removed, Lender's Security Administrator will be able to add the current eAuth User ID successfully.

Note: If the user has multiple roles with the previous eAuth User ID, all roles must be removed in order to add the new User ID.

2. If the previous user ID role was assigned by another lender organization and cannot be found on the User List, then the Lender's Security Administrator must contact the applicable program below and request the previous user ID role be removed.

For SFH Guaranteed loans contact the Help Desk at rd.hd@usda.gov or 800-457-3642 ext. 2, ext. 2.

For FSA and all other RD loan programs, contact the Guaranteed Commercial Branch: 314-457-6402 or SM.RD.SO.FCSB@usda.gov

User Maintenance

eAuth User ID *
 Name
 Phone/Extn *
 Fax
 Email Address
 Assurance Level 1

5.6 Adding or Removing Security Administrators

To remove or add a Security Administrator (SA) complete the **"Request for adding/removing Security Administrators"** at [GUS Lender Test Environment](#) page

6 Contact US

Technical Issues: GUS/GLS	RD.HD@usda.gov or 800-457-3642 Option 2, Option 2
Technical Issues: Login.gov ID	https://www.login.gov/help/
Technical Issues: eAuthentication Public FAQ's	https://www.eauth.usda.gov/eauth/b/usda/faq
Training & Guides	USDA LINC Training & Resource Library
USDA Single Family Housing Guaranteed Loan Contacts	https://www.rd.usda.gov/page/sfh-guaranteed-lender