

# MyGinnieMae Portal – Getting Started Manual

U.S. Department of Housing and Urban  
Development (HUD)

Ginnie Mae, Office of Securities Operations (OSO)

Version 2.4



## Application Details

Application Information	Description
Application Name	MyGinnieMae
Application Acronym	MGM
Ginnie Mae SVP, Sponsor	John Daugherty, SVP OSO
Ginnie Mae Application Owner	
Version/Application Release Number	2.4

## Document History

Version	Date of the Document	Author (Last Name, First Name)	Entity (Company or Department Author Represents)	Revision Description
2.0	09/23/2019	Matheny, Micah - PM	Falcon Capital Advisors	Reconstructed from pre-full release document
2.1	11/21/2019		BNYM	Updated content with early adopter feedback
2.2	12/19/2019	Dana Manor-Zahavi, Jeff Janovsky	BNYM	Update for Ops Feedback and Mobile Authenticator, Removal of OAAM CRs
2.2	12/30/2019	Dana Manor-Zahavi	BNYM	Updates based on completed testing of OAAM removal and OMA + Ginnie Mae virtual review updates
2.2	1/15/2019	Dana Manor-Zahavi	BNYM	Updated QRCs
2.2	11/16/2022	Renee Just-Buddy Dave Cannon	Ginnie Mae Ampcus	Revised to reflect formatting changes to Ginnie Mae's User Manual Framework, provided by the Customer Experience Group.
2.2	10/12/2023	Burleson, Sarah	Deloitte	Updated QRCs, updated to reflect Self-Service RSA SecurID Soft Token Replacement

Version	Date of the Document	Author (Last Name, First Name)	Entity (Company or Department Author Represents)	Revision Description
2.3	08/14/2024	Nebelsick, Sarah	Deloitte	Updated for password policy, user registration, name updates, and OTP security enhancements
2.4	07/28/2025	Zia, Laraib	Deloitte	Updated for Password Expiry Warning email and Password Expired email changes

# TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION .....</b>	<b>7</b>
1.1	Application Overview .....	7
1.2	Business Workflow .....	8
<b>2</b>	<b>USING THE MYGINNIEMAE PORTAL .....</b>	<b>8</b>
2.1	System Prerequisites.....	8
2.1.1	Compatibility Settings.....	9
(1)	Support TLS 1.2 .....	10
(2)	Accessing Video Files .....	10
2.1.2	Prerequisites to Accessing MyGinnieMae Portal .....	11
2.1.3	Functional Roles.....	11
2.1.4	Contingencies and Alternate Modes of Operation .....	12
2.2	Creating a User Account .....	12
2.3	Registration Email Invitation .....	13
2.3.1	Required User Information.....	13
2.3.2	Expiration of Email Invitation .....	16
2.3.3	Invitation Limits .....	17
2.4	Requesting Functional Roles for My User Account .....	17
2.5	Accessing the One-Time PIN (OTP) via Smart Device .....	17
2.5.1	Register with the Oracle Mobile Authenticator .....	18
2.5.2	De-register with the Oracle Mobile Authenticator.....	21
2.6	Managing Your MyGinnieMae Account .....	24
2.6.1	Profile Management.....	24
2.6.2	Issuer ID .....	24
2.6.3	Edit Profile.....	24
2.6.4	Associated Accounts.....	25
2.7	Resetting Passwords .....	26
2.7.1	Change Password .....	26

2.7.2	Forgotten Password .....	29
2.7.3	Expired Password .....	33
2.7.4	Logging In After an Admin Reset a User's Password.....	36
2.8	Logging into MyGinnieMae .....	38
2.8.1	Entering a Username and Password .....	38
2.8.2	Choosing and Entering a One-Time PIN (OTP) .....	39
2.8.3	Logging In After an Admin has Enabled User's Account.....	41
2.9	Exiting .....	41
2.9.1	Manually Exiting MyGinnieMae.....	42
2.9.2	Automatic Logout.....	42
2.10	Navigating the Portal .....	43
2.10.1	Accessing Business Applications .....	43
2.10.2	Marquee .....	44
2.10.3	My Dashboard .....	44
2.10.4	Bookmarks .....	45
2.10.5	Industry News.....	45
2.10.6	Messages.....	46
2.11	Dashboard Components/Widgets .....	46
2.11.1	Commitment Authority Dashboard Chart .....	47
2.11.2	Pool Numbers Dashboard Chart.....	47
2.11.3	Issuer Operational Performance Profile (IOPP) Scorecard .....	48
2.12	Communities.....	49
2.12.1	Leadership Blog.....	49
2.12.2	Discussion Forums.....	49
2.13	Knowledge Center .....	50
2.14	Portal Search.....	50
2.15	Requesting an RSA SecurID Soft Token for The First Time .....	51
2.16	Self-Service RSA SecurID Soft Token Replacement .....	51

<b>3</b>	<b>TROUBLESHOOTING AND SYSTEM ERRORS.....</b>	<b>56</b>
3.1	Basic Error Handling.....	56
3.2	New Password Mismatch Error .....	56
3.3	Invalid Username or Password .....	57
3.4	Incorrect OTP .....	57
3.5	OTP Not Received .....	58
3.6	Disable Pop-Up Blocker .....	58
3.7	Account Locked .....	59
3.8	MyGinnieMae Portal Profile Accounts tab: GMEP 1.0 or GinnieNET IDS are Unavailable .....	59
3.9	Registration Invitation Form Errors .....	60
<b>4</b>	<b>RESOURCES.....</b>	<b>61</b>
4.1	Organization Administrators .....	61
4.2	Training Resources.....	61
4.3	QRCS .....	61
4.4	Help Desk Contact Information .....	62
4.5	MyGinnieMae Portal Dictionary .....	62
4.6	MyGinnieMae Self Help Tools .....	62
<b>5</b>	<b>APPENDIX .....</b>	<b>62</b>
5.1	MyGinnieMae Business Features .....	62
5.2	QRCS .....	63
5.3	Figures .....	66
5.4	Tables .....	70



## 1 INTRODUCTION

---

This manual is written to provide instructions on how to use the MyGinnieMae Portal. End Users utilize the MyGinnieMae Portal to access Ginnie Mae's systems, applications, and resources.

Below are links that address common topics that pertain to the MyGinnieMae Portal.

- [Logging In to MyGinnieMae](#)
- [System Prerequisites](#)
- [Creating a User Account](#)
- [Entering a One Time PIN \(OTP\)](#)
- [Managing Your MyGinnieMae Account](#)
- [Resetting Passwords](#)
- [MGM Portal Dictionary](#)
- [Troubleshooting and System Errors](#)

[Back to Table of Contents](#)

### 1.1 Application Overview

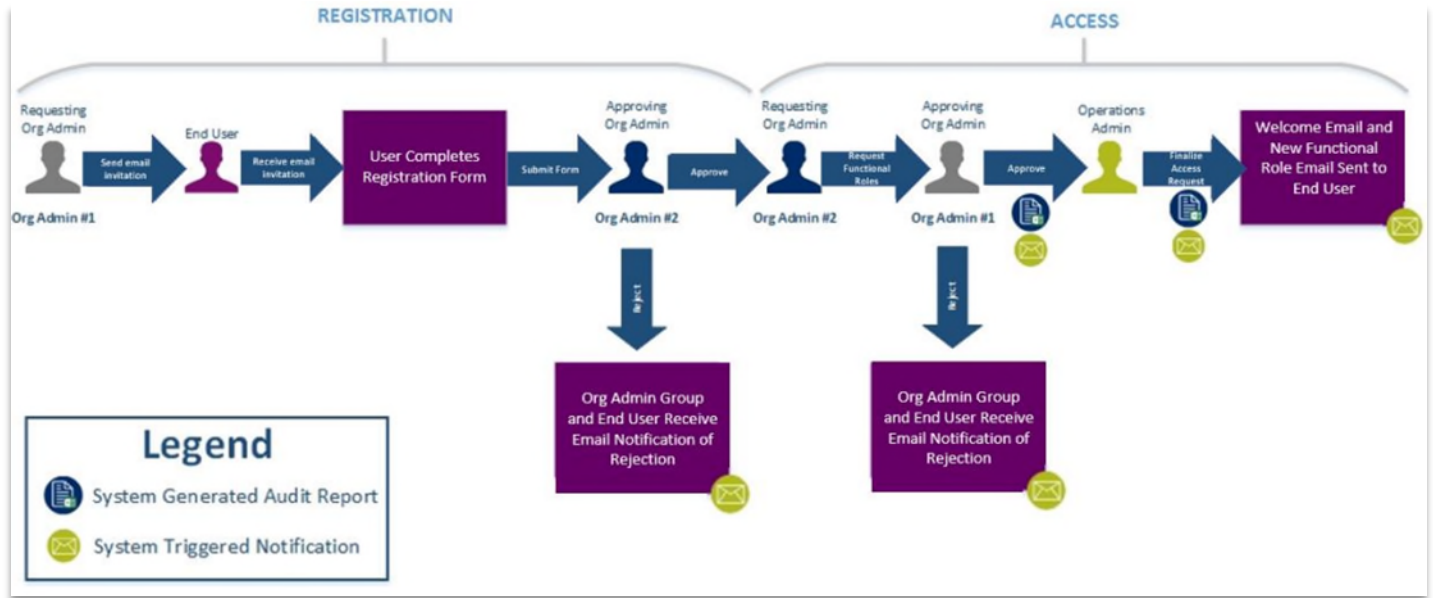
Ginnie Mae successfully developed a single gateway to Ginnie Mae's systems, applications, and resources through the MyGinnieMae (MGM) Portal. MGM replaced the Ginnie Mae Enterprise Portal, commonly known as GMEP 1.0, and now serves as the primary platform for extending information technology capabilities to the Ginnie Mae community.

The MyGinnieMae Portal includes multi-factor authentication to improve security and reduce identity administration costs. It also connects to applications as defined in the application prioritization briefing to include enabling federated Single Sign-On to GMEP 1.0 and GinnieNET.

## 1.2 Business Workflow

The high-level Workflow for onboarding users into the MyGinnieMae Portal is shown in the figure below:

Figure 1.2-1 MyGinnieMae Onboarding Workflow



## 2 USING THE MYGINNIEMAE PORTAL

This section provides a general walkthrough of the process for requesting a user account and functional roles to access business applications, as well as step-by-step instructions on how to log into the MyGinnieMae Portal, navigate its security features and manage your account.

### 2.1 System Prerequisites

The Organization Administrator must be an authorized signer listed on the relevant Form HUD-11702 (Resolution of Board of Directors and Certificate of Authorized Signatures) found on the [MBS Guide: Forms website](#). To set up an Organization Administrator account in MyGinnieMae, the Operations Administrator team must initiate the registration process and assign the proper roles to the new Organization Administrator. As an added level of security, each unique organization must have at least two Organization Administrators. To complete registration



and access approvals, one Organization Administrator will submit requests and the other Organization Administrator will approve requests.

[Back to Table of Contents](#)

### 2.1.1 Compatibility Settings

MyGinnieMae can be accessed using one of the following supported web browsers—Google Chrome 42+, Internet Explorer 11.x, and Mozilla Firefox 31+. Google Chrome has resulted in fewer errors for Portal users. However, some functions in the legacy systems, GMEP 1.0 and GinnieNET, may still require the use of Internet Explorer. If using IE, ensure browser is up to-date; validate with your System Admin before selecting one of the download links 32-bit system / 64-bit system.

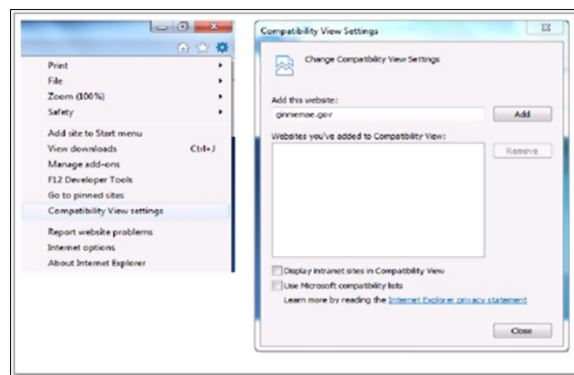
**NOTE:** You must disable the browser’s pop-up blocker prior to accessing MyGinnieMae.

**NOTE:** Screens with a resolution greater than 1920X1080 (23") may render differently than images shown in this manual.

To access MyGinnieMae via Internet Explorer, the user may need to disable the browser compatibility settings as follows:

1. Open Internet Explorer.
2. Select the “Tools” icon.
3. Select “Compatibility View Setting.”
4. Make sure the “Display intranet sites in Compatibility View” option is not checked.
5. Select “Close” to continue.

Figure 2.1-1 Compatibility View Settings



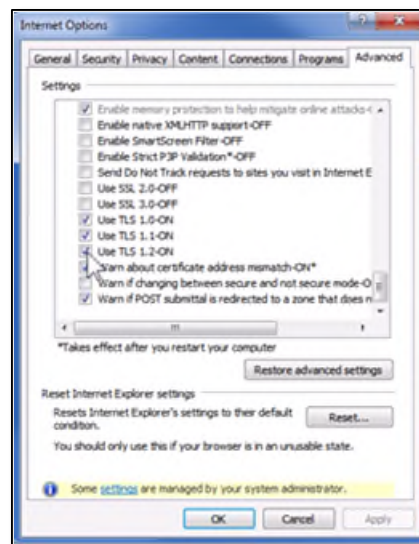
[Back to Table of Contents](#)

## (1) Support TLS 1.2

If using Internet Explorer, the user must set up the browser to support TLS 1.2. (This supersedes SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1.). The user may need to adjust the user interface as follows:

1. Select **"Tools"** from the menu bar.
2. Select **"Internet Options."**
3. Select the **"Advanced"** tab.
4. From the **"Settings"** menu, scroll down to the "Security" leaf and select the checkbox to enable "Use TLS 1.2."
5. Select **"Apply"** to save the update.
6. Select **"OK"** to close the window.

Figure 2.1-2 Use TLS 1.2



**NOTE:** Chrome and Firefox provide support for TLS 1.2 by default within their current releases. The setting is not user adjustable through the standard user interface.

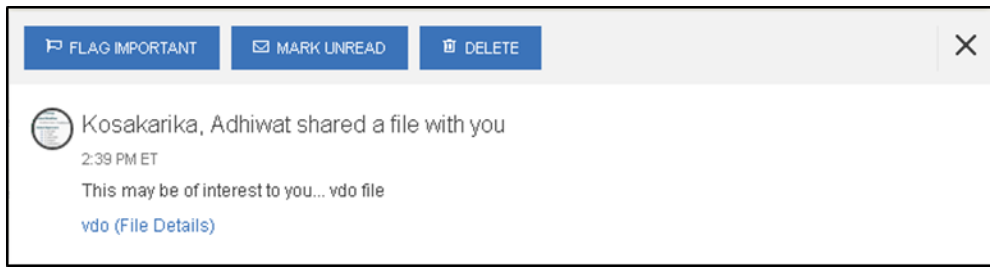
[Back to Table of Contents](#)

## (2) Accessing Video Files

When attempting to access a video file stored in MyGinnieMae, the user must download the file before opening it to play within Windows Media Player. Follow these steps if Internet Explorer is the default web browser.

1. To download a file shared via a link within a message or email, right-click the file link.

Figure 2.1-3 Download File



2. Select **“Save target as...”** to initiate the download.
3. Specify a file location and select **“Save.”**
4. Select **“Open”** from the action prompt to view the file’s content.

If the user is not currently logged into MyGinnieMae, the user will be prompted for their credentials in order to initiate the download.

**NOTE:** Chrome and Firefox automatically prompt users to download before playing video files.

### 2.1.2 Prerequisites to Accessing MyGinnieMae Portal

Before being granted access to the MyGinnieMae Portal, the user must complete the registration process. Privileged users called Organization Administrators, formerly known as Security Officers and Enrollment Administrators, facilitate the registration and access provisioning process within each organization. The Organization Administrator will register the account and, once registered, will arrange access for the account. See the [Creating a User Account](#) section for more information on the user registration process.

[Back to Table of Contents](#)

### 2.1.3 Functional Roles

In MyGinnieMae, users are provided access based on their business activities which are organized into meaningful access profiles called Functional Roles. Use of Functional Roles ensures users have appropriate level of access in relation to their job functions/responsibilities, enforces the “least privilege principle,” and makes the account provisioning/deprovisioning actions easier for Organization Administrators. These roles are grouped and vary by type (Single-Family, Multifamily, HECM, etc.) as summarized in the [Functional Roles Matrix](#). For more detail, refer to the [Requesting Functional Roles](#) section.

Functional Roles are based upon general responsibilities for a specific position which a user may share with other users. If a user sees a link that may not be applicable to their specific role, the user should contact their Organization Administrator for assistance. If a user is an Organization Administrator who also performs business functions, Functional Roles must be added to that user profile in addition to the Organization Administrator access. The following portal users can have customized Functional Roles:

- Issuers (such as Single-Family, Multifamily, HECM)
- Subservicers
- Document Custodians
- Depositors
- Agents
- Operations
- Ginnie Mae

#### 2.1.4 Contingencies and Alternate Modes of Operation

The MyGinnieMae Information System (IS) Contingency Plan exists to ensure resumption of time-sensitive operations and services in the event of an emergency and/or disaster (fire, power or communications blackout, tornado, hurricane, flood, earthquake, civil disturbance, etc.). The MyGinnieMae Contingency Plan applies to the functions, operations, and resources necessary to restore and resume operations applicable to MyGinnieMae.

Full Plan activation occurs in the event of a major system failure. At that time, the system fails over to the alternate processing site. Users of the system are notified in accordance with standard IT Operations notification – first that full plan activation is in progress, and again when activation is complete. In addition, [Ginnie Mae Customer Support](#) is provided with regular system status updates.

If there is a minor system failure or a planned outage, related outage information including start time, end time, and estimated duration is posted to the MyGinnieMae Portal [Public Landing Page](#). Ginnie Mae is notified, and a message is provided to [Ginnie Mae Customer Support](#) for assisting users when they call. This notification is provided a week in advance for planned outages such as a Disaster Recovery exercise.

If users observe any security related abnormal behavior in MyGinnieMae, they must report the observation to the Pool Processing Agent (PPA) by contacting [Ginnie Mae Customer Support](#).

[Back to Table of Contents](#)

## 2.2 Creating a User Account

The MyGinnieMae Account Management Console (AMC) is a self-service user registration process which collects, verifies, and creates a new user account. It provides a single identity, enabling users to access the portal and the business applications that reside within the portal. This process automates user account creation and access request provisioning and provides an audit history of user access.

The following conditions must be met for user registration and access provisioning to be completed successfully:

1. The invitation has been sent to an end user's organization business email address five or fewer times.
2. The individual must be employed by an organization which has been on-boarded and authorized to do business with Ginnie Mae.
3. The participant organization approves of their employee being granted access to Ginnie Mae's systems.
4. The participant organization approves the level of access requested for the user.

5. Operations agrees with the level of access requested.

An email with a link to register for MyGinnieMae is sent only after the Organization Administrator submits an invitation to register.

**NOTE:** Platinum Application users have a different registration process. For more information, refer to the [Platinum Pool Processing](#) section.

[Back to Table of Contents](#)

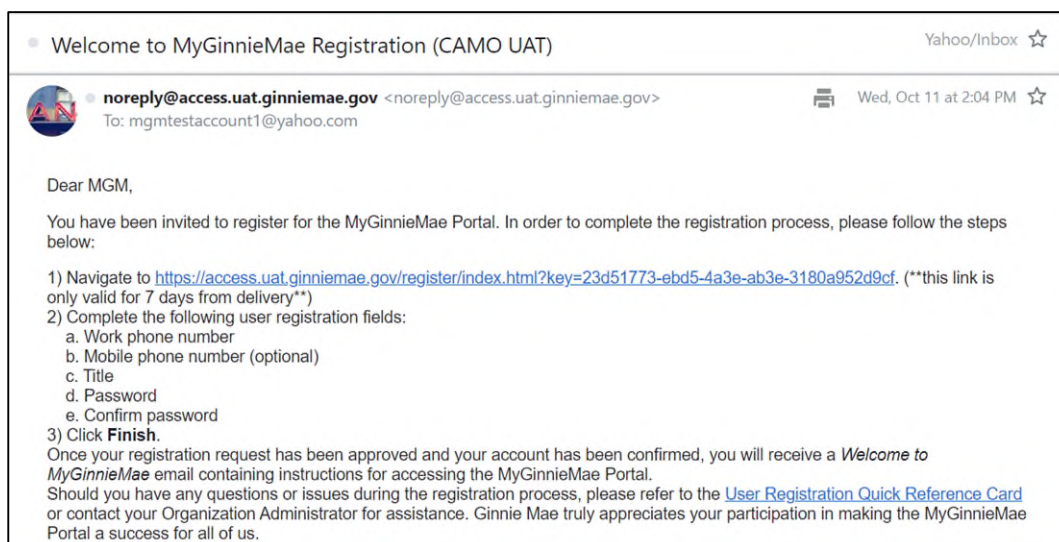
## 2.3 Registration Email Invitation

### 2.3.1 Required User Information

1. Navigate to the unique registration link in the MyGinnieMae registration email.

**NOTE:** The link is only active for 24 hours.

Figure 2.3-1 MyGinnieMae Registration Email



2. Fill out the following fields on the **New User Registration Form**:
  - Work Phone Number (be in the (555) 555-5555 format and cannot begin with a 1 or a 0.)
  - Mobile Phone Number (optional)
  - Title
  - Password
  - Confirm Password
  - RSA Token Serial Number (if applicable)

Figure 2.3-2 New User Registration

The screenshot shows the 'New User Registration Form' for GinnieMae. The header includes the GinnieMae logo and the tagline 'Our Guaranty Matters'. Below the header, a sub-header reads 'New User Registration Form' followed by the text 'This wizard will guide you through Ginnie Mae's registration process.' A blue button labeled '1. Additional Information' is positioned above the form fields. The form itself is titled 'Additional Information' and contains several input fields: 'MGM' (with a person icon), 'Middle Name' (with a person icon), 'Test' (with a person icon), 'Email' (containing 'mgmttestaccount1@yahoo.com'), a dropdown menu (showing 'Ms'), 'Work Phone' (with a phone icon), 'Mobile Phone' (with a phone icon), 'Password' (with a lock icon and a question mark icon), and 'Verify Password' (with a lock icon). Below the fields are two checkboxes: 'I agree with the Terms and Conditions.' and 'I accept the privacy policy.' A blue 'Finish' button is located at the bottom right of the form.

**NOTE:** Select the question mark icon to reveal the Password Policy. Make sure the password meets the following password policy requirements:

- Must not match or contain the user's first name or last name
- Must be 8-20 characters long
- Must contain at least 2 alphabetic character(s), and at least 1 uppercase and lowercase letter(s)
- Must contain at least 1 numeric character(s).
- Must contain at least 1 special character(s).

3. Select the "I agree with the Terms and Conditions" link or checkbox.
  - a. When the message box displays, review the text, scroll to the bottom, and Yes **(Agree)**.
  - b. The "I agree with the Terms and Conditions" checkbox is now checked.

Figure 2.3-3 Rules of Behavior

The screenshot shows a message box with the text: 'I acknowledge that I have read the attached Rules of Behavior for Use of Information Resources. I understand, accept, and agree to comply with all terms and conditions of these Rules of Behavior.' At the bottom right of the message box are two buttons: 'Cancel' and 'Yes (Agree)'. The 'Yes (Agree)' button is highlighted with a red border.

4. Select the "I accept the privacy policy" link or checkbox.
  - a. Select the "Ginnie Mae Privacy Policy" link when the message box displays.

- b. Review the text and select **Yes**.

Figure 2.3-4 Privacy Policy



Please review the Ginnie Mae Privacy Policy.

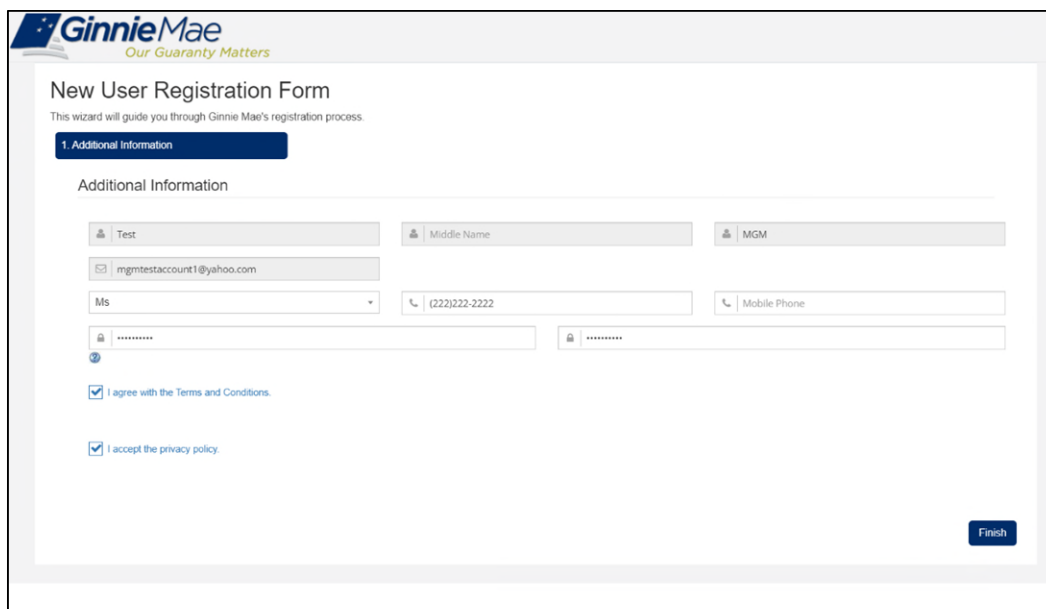
By selecting **Yes** I agree to the Ginnie Mae privacy policy.

This link will open a new tab in your browser. You must navigate to the new tab, read the policy and then return to this page to continue.

[Ginnie Mae Privacy Policy](#)

5. Select **Finish** once the Privacy Policy and Terms and Conditions have been accepted.

Figure 2.3-5 New User Registration Form - Completed



**GinnieMae**  
Our Guaranty Matters

### New User Registration Form

This wizard will guide you through Ginnie Mae's registration process.

**1. Additional Information**

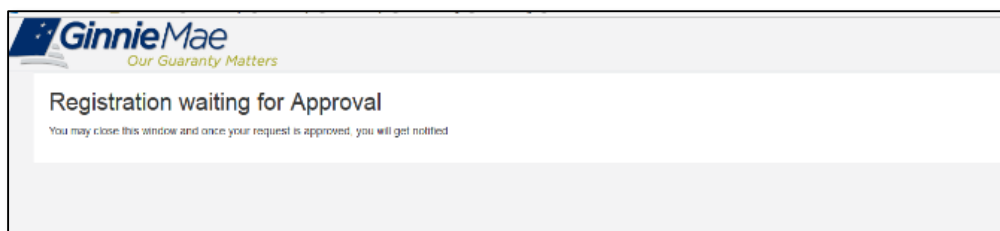
Additional Information

☒ I agree with the Terms and Conditions.

☒ I accept the privacy policy.

6. A message will display confirming the form was submitted successfully and is awaiting approval by the Organization Administrator.

Figure 2.3-6 Registration Request Complete



**GinnieMae**  
Our Guaranty Matters

### Registration waiting for Approval

You may close this window and once your request is approved, you will get notified

7. Once the request is approved and access is granted, both a Welcome Email and a New Functional Role Assignment Email will be sent to the user's email address and the portal can be accessed using the enterprise ID (email address) and password.

**NOTE:** In the event users login to the portal before functional roles are assigned, they will not yet be able to view My Dashboard or access business applications.

Figure 2.3-7 Welcome Email

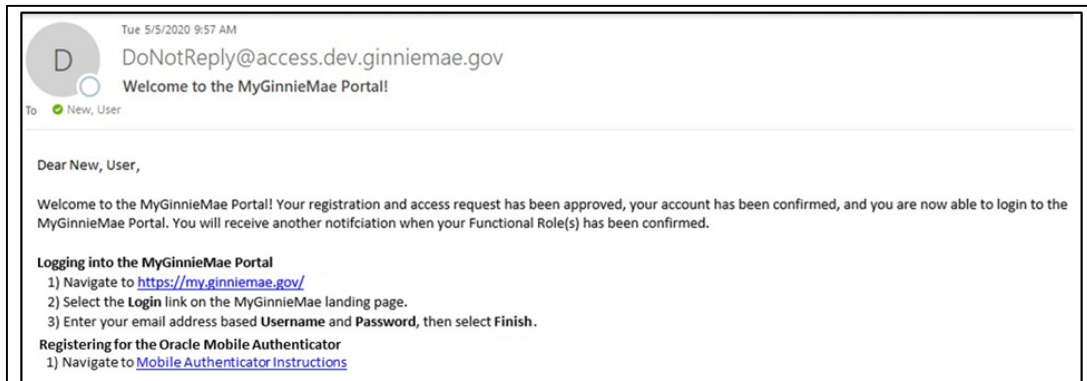
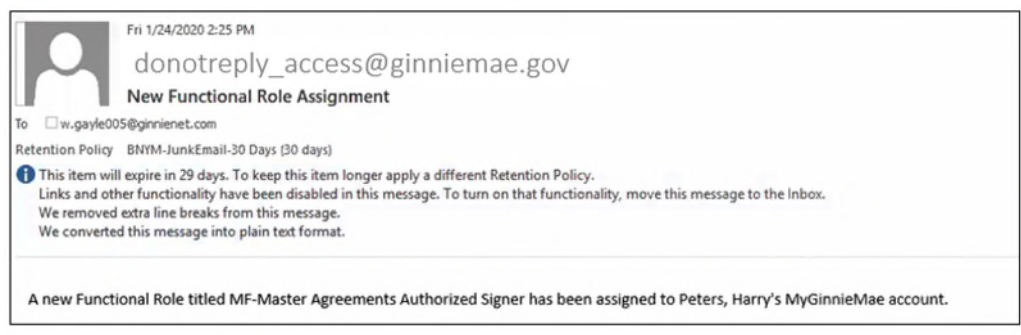


Figure 2.3-8 New Functional Role Assignment Email



[Back to Table of Contents](#)

## 2.3.2 Expiration of Email Invitation

A registration link is active for only 7 days. Contact the Organization Administrator should there be any questions or issues with the access and registration process. If the Organization Administrator has questions, contact [Ginnie Mae Customer Support](#).

[Back to Table of Contents](#)



### 2.3.3 Invitation Limits

If an invitation has already been sent to the email address a total of five times, the email address will be flagged, and the Organization Administrator will not be able to send another request. In order to send another invitation, contact [Ginnie Mae Customer Support](#).

[Back to Table of Contents](#)

## 2.4 Requesting Functional Roles for My User Account

Functional Roles have been introduced to combine existing Ginnie Mae business systems/applications access roles from GMEP 1.0 and GinnieNET into meaningful access profiles. Use of Functional Roles ensures users have the appropriate level of access in relation to their job functions/responsibilities, enforces the “least privilege principle,” and makes the account provisioning/de-provisioning actions easier for Organization Administrators. These roles are grouped and vary by type (Single Family, Multi-Family, HECM, etc.). For details on functional roles, refer to the [Functional Role Matrix](#). Contact the Organization Administrator to ensure access to the appropriate Functional Roles for the user’s MyGinnieMae account.

[Back to Table of Contents](#)

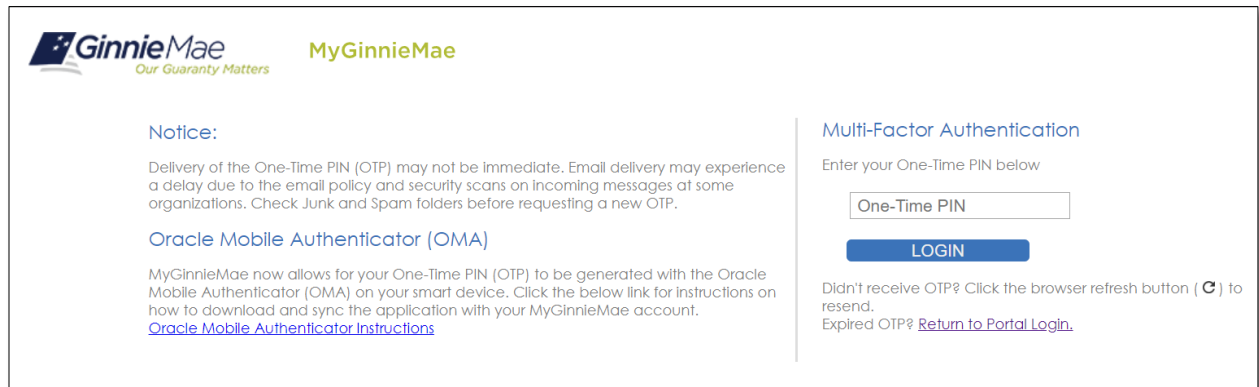
## 2.5 Accessing the One-Time PIN (OTP) via Smart Device

In addition to email delivery, portal users will have the option to receive their OTP via Oracle Mobile Authenticator (OMA) which offers ease of delivery and enables users to securely verify their identity by using their smart device as an authentication factor. The mobile authenticator OTP is a six-digit code and will be valid for 30 seconds.

For the instructions on how to download and sync the OMA App with your MyGinnieMae account, follow these steps:

1. From a computer, log in to MyGinnieMae via <https://my.ginniemae.gov>.
  - a. Enter **Username**
  - b. Enter **Password**
  - c. Select **LOGIN**
2. The system will direct to the Multi-Factor Authentication Page.
  - a. Select the link for **Oracle Mobile Authenticator Instructions** on the left side of the page
  - b. This will open the **OMA Instructions with QR Code** so you can register with OMA

Figure 2.5-1 Multi-Factor Authentication Page



**GinnieMae**  
Our Guaranty Matters

**MyGinnieMae**

**Notice:**

Delivery of the One-Time PIN (OTP) may not be immediate. Email delivery may experience a delay due to the email policy and security scans on incoming messages at some organizations. Check Junk and Spam folders before requesting a new OTP.

**Oracle Mobile Authenticator (OMA)**

MyGinnieMae now allows for your One-Time PIN (OTP) to be generated with the Oracle Mobile Authenticator (OMA) on your smart device. Click the below link for instructions on how to download and sync the application with your MyGinnieMae account.  
[Oracle Mobile Authenticator Instructions](#)

**Multi-Factor Authentication**

Enter your One-Time PIN below

One-Time PIN

**LOGIN**

Didn't receive OTP? Click the browser refresh button ( ⌂ ) to resend.  
Expired OTP? [Return to Portal Login.](#)

**NOTE:** Alternatively, you can access the Oracle Mobile Authenticator Instructions using your smart device. This page is accessible either via a link in the Welcome Email received upon registration approval, via a link on the Multi-Factor Authentication page with the OTP prompt, or by directly accessing <https://my.ginniemae.gov/gnma/oma.html>.

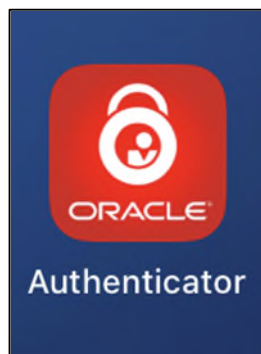
[Back to Table of Contents](#)

### 2.5.1 Register with the Oracle Mobile Authenticator

To register with the Oracle Mobile Authenticator App, follow these steps:

1. If you do not already have OMA installed on your smart device,
  - a. Go to Google Play Store (Android) or Apple App Store (iPhone)
  - b. Download the **Oracle Mobile Authenticator**

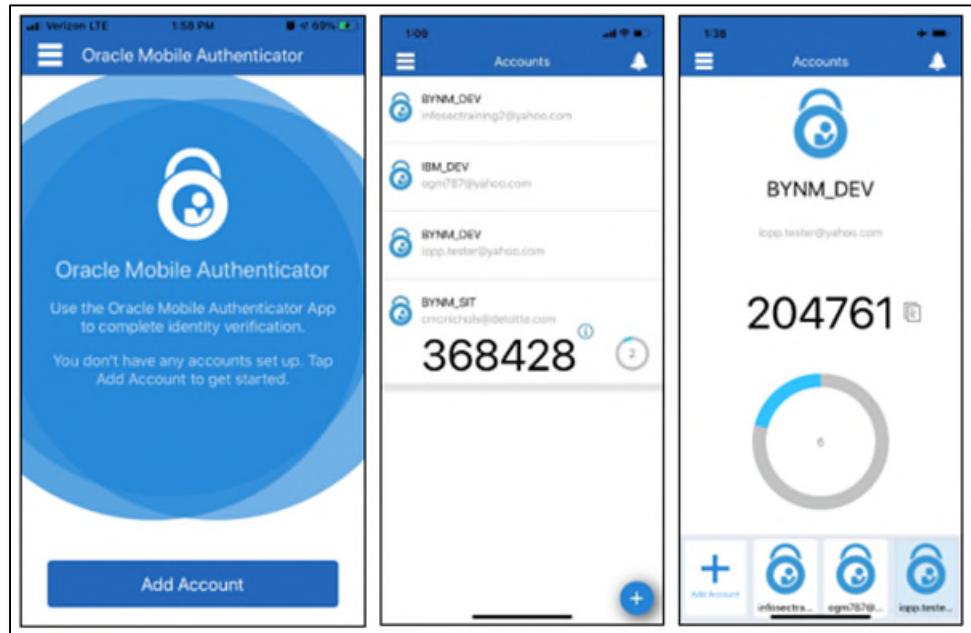
Figure 2.5-2 The Oracle Mobile Authenticator Icon



2. Once downloaded,
  - a. Open the **Oracle Mobile Authenticator** App

- b. Select the **+** button on the bottom of the display or the **Add Account** button if you are a first-time user. This will launch the camera on your smart device.

Figure 2.5-3 (Left) Oracle Mobile Authenticator (OMA) no prior accounts (Center) OMA List View (Right) OMA Grid View



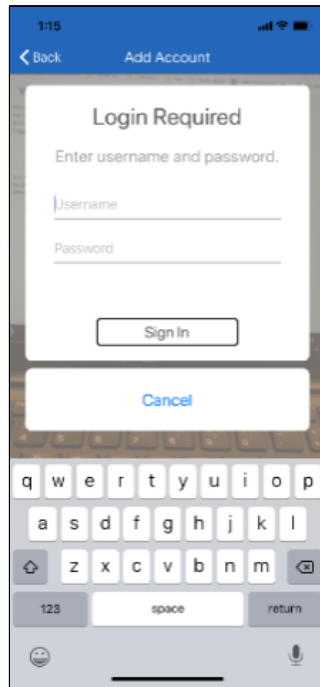
3. Use your smart device to Scan the **QR Code** found in the **OMA Instructions with QR Code** on your computer.

Figure 2.5-4 OMA Instructions with QR Code



- a. Use your MyGinnieMae credentials to, Enter your Username
- b. Enter your Password
- c. Select Sign In

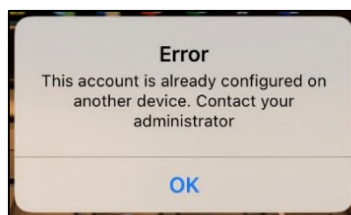
Figure 2.5-5 Oracle Mobile Authenticator Login



**NOTE:** If you attempt to re-register the OMA with your MyGinnieMae account on the same device after having de-registered the account, you will be prompted to either “Create a New Account”, “Overwrite”, or “Cancel”. The user should select “**Overwrite**.” If you select “Cancel”, you will have to de-register your device and re-register again in order to use the Oracle Mobile Authenticator. If you select “Create New Account”, the account must be saved with a unique name, different from your previous registration.

**NOTE:** The MyGinnieMae account may only be connected to one smart device. If you attempt to register OMA with a MyGinnieMae account that is already registered, either on the same device or a different device, you will be prompted with the following error message after entering credentials.

Figure 2.5-6 Oracle Mobile Authenticator Error for Already Registered Accounts



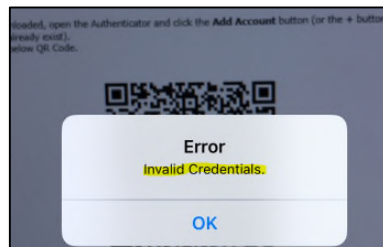
4. On your next login to MyGinnieMae, you will be given the option to receive either One Time Pin through Email or One Time Pin from Oracle Mobile Authenticator as shown below:

Figure 2.5-7 Multi-Factor Authentication Page - Choose Preferred OTP Method

The screenshot shows the 'Multi-Factor Authentication' page. On the left, under 'Notice:', it states: 'Please select the method of retrieving your One-Time PIN (OTP). The Oracle Mobile Authenticator, on your smart device, will generate your OTP, or you can have your OTP delivered to you via the registered email address.' On the right, under 'Multi-Factor Authentication', it says 'Please choose your preferred method' and lists two options: 'One Time Pin through Email' and 'One Time Pin from Oracle Mobile Authenticator'. Both options are currently unselected. Below the list is a blue 'OK' button.

**NOTE:** If you attempt to register with the Oracle Mobile Authenticator and your MyGinnieMae account is disabled, or you enter your credentials incorrectly, the following error message is displayed.

Figure 2.5-8 Disabled User / Invalid Credentials Error



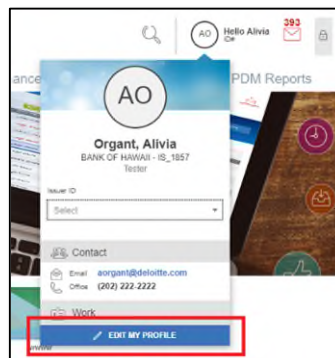
[Back to Table of Contents](#)

## 2.5.2 De-register with the Oracle Mobile Authenticator

A user may need to de-register their smart device if they replace their current device with a new one, if they delete and re-download the Oracle Mobile Authenticator, or if they no longer wish to see OTP generated by the Oracle Mobile Authenticator as an option. To de-register a smart device, follow these steps:

1. Follow the instructions for [Logging into MyGinnieMae](#).
2. From My Dashboard, select the user avatar or initials from the Global Header at the top of the page.

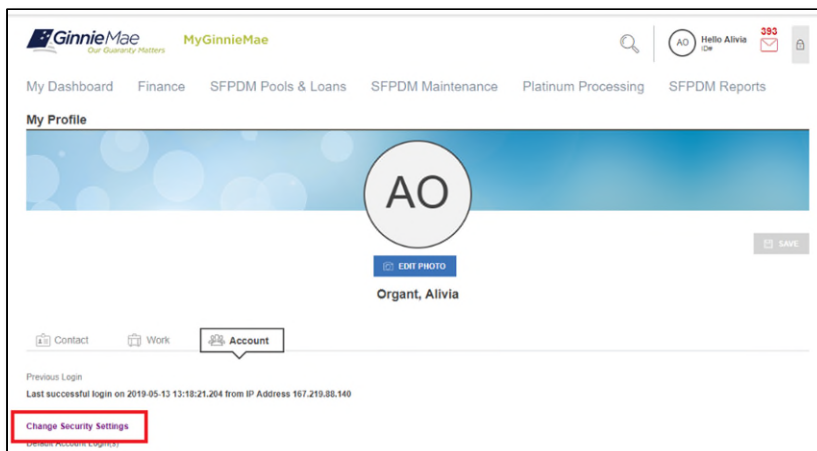
Figure 2.5-9 Edit My Profile



3. Select **Edit My Profile**.
4. Select the **Account** tab.

5. Select **Change Security Settings**.

Figure 2.5-10 User's Profile Account Tab



6. The system will redirect to the Password Change Authentication screen. Enter the username and current password.

Figure 2.5-11 User's Profile Account Tab

A screenshot of the Password Change Authentication screen. The page features the GinnieMae logo and the text 'MyGinnieMae'. On the left, a 'Password Change Notice' states: 'You are being required to re-authenticate to change your password. This ensures that the registered email address is still valid.' On the right, the 'Password Change Authentication' section prompts the user to 'Please provide your username and password.' It includes input fields for 'Username' and 'Password', an 'ENTER' button, and a 'Forgot Password?' link.

**NOTE:** This page may open in a new tab, however the Portal session in the original tab will continue. It is recommended that, once the user has changed their password, the user close one of these tabs.

7. The system will prompt the Multi-Factor Authentication through Delivery of the OTP via Email delivery.

Figure 2.5-12 User's Profile Account Tab

The screenshot shows the 'MyGinnieMae' portal. On the left, a blue sidebar contains the 'GinnieMae' logo and 'Our Guaranty Matters'. The main content area is divided into two sections. The left section, titled 'Notice:', contains text about One-Time PIN (OTP) delivery delays and instructions to check Junk and Spam folders. The right section, titled 'Multi-Factor Authentication', prompts the user to 'Enter your One-Time PIN below'. It features a text input field labeled 'One-Time PIN', a blue 'ENTER' button, and a note: 'Didn't receive OTP? Click the browser refresh button (⌂) to resend. Expired OTP? [Return to Portal Login.](#)'

**NOTE:** Oracle Mobile Authenticator cannot be used to complete the OTP for Password Change Authentications. The user can only proceed with the OTP via Email delivery.

8. Once re-directed to the Change Password screen, select **De-register** on the Change Password Page.

Figure 2.5-13 Change Password Page

The screenshot shows the 'Change Password' page. At the top, there's a navigation bar with 'Home', 'Links', and a user email 'cmonichols@deloitte.com'. The main heading is 'Change Password'. Below it, a 'Password Policy' section lists requirements: password must not match or contain first or last name; must be 8-20 characters long; must contain at least 2 alphabetic characters and at least 1 uppercase and lowercase letter(s); must contain at least 1 numeric character(s); must contain at least 1 special character(s); and must not contain the username or match the last 24 previous passwords. To the right, there are three input fields: 'Current Password:', 'New Password:', and 'Confirm New Password:'. A blue 'Submit' button is below the 'Confirm New Password' field. Below the input fields, there's a section titled 'De-register Oracle Mobile Authenticator' with the text 'To de-register the Oracle Mobile Authenticator from your account, click the De-register button below.' and a blue 'De-register' button. At the bottom left of this section is a 'Return to Portal' link.

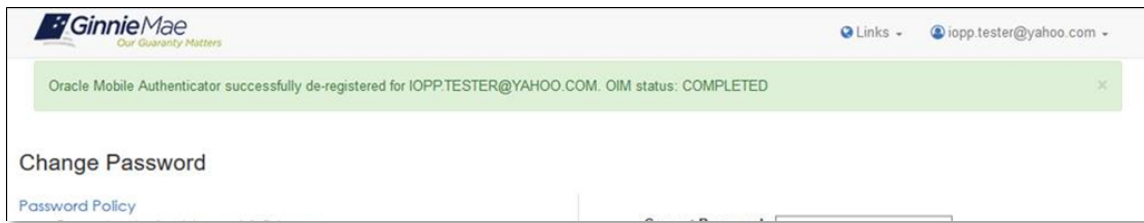
9. Select **Confirm** in the Confirmation window.

Figure 2.5-14 De-registration Confirmation Window

The screenshot shows a confirmation dialog box titled 'Confirm De-registration of Oracle Mobile Authenticator'. The main text inside the dialog asks, 'Are you sure you want to de-register your Oracle Mobile Authenticator?'. At the bottom right of the dialog, there are two buttons: a 'Cancel' button and a blue 'Confirm' button. The dialog is overlaid on a blurred background of the 'Change Password' page.

10. A message that the de-registration was successful will display. To return to the portal, select **Return to Portal**.

Figure 2.5-15 Successful De-registration Message



**NOTE:** If you need to re-register a smart device with the Oracle Mobile Authenticator follow the instructions in the [Register with Oracle Mobile Authenticator](#) section.

[Back to Table of Contents](#)

## 2.6 Managing Your MyGinnieMae Account

### 2.6.1 Profile Management

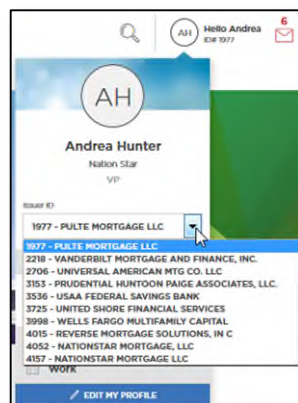
To manage a user profile, select the user avatar. A drop-down menu will appear with the Issuer profile.

### 2.6.2 Issuer ID

Issuers associated with multiple Issuer IDs can toggle their view to display data specific to each individual business entity. This data is shown within the Commitment Authority Chart and Pool Numbers Chart.

**NOTE:** Subservicers will **not** be able to see Commitment Authority or to Request Pool Numbers.

Figure 2.6-1 Toggle View



[Back to Table of Contents](#)

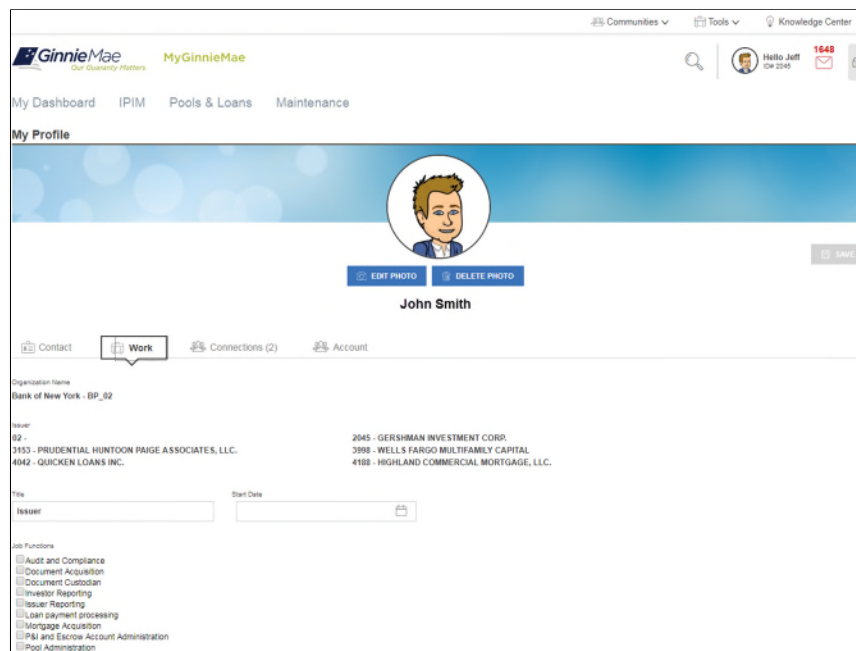
### 2.6.3 Edit Profile

Select “Edit My Profile” to:



- View the user's profile picture as well as change and delete the current photo. Select "Edit Photo" to select a new profile photo. Select "Delete Photo" to remove the current profile photo.
- Toggle between editing contact and work information.
- View "Connections" to display assigned Ginnie Mae Account Executive with their contact information.
- Edit public work profile information such as:
  - Start Date – duration of organizational experience
  - Title – current job title
  - Job Functions – details about the user's responsibilities
  - Professional Background Summary – brief biographical sketch of a user's professional experience

Figure 2.6-2 Manage Profile

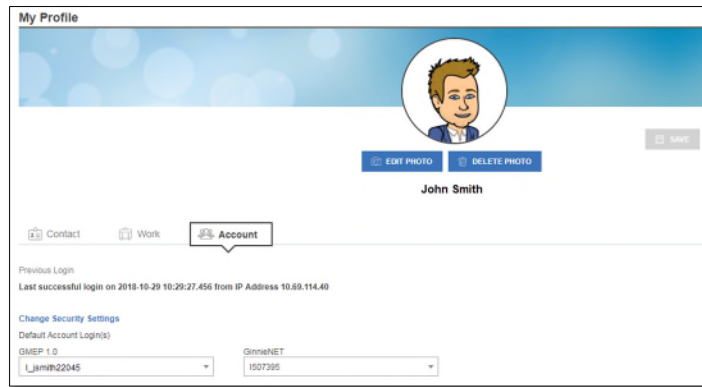


[Back to Table of Contents](#)

## 2.6.4 Associated Accounts

Select the "Account" tab to view and update the profile setting for Single Sign-On identity association with other applications such as GMEP 1.0 or GinnieNET. Use the drop-down menu to select a default ID for each application.

Figure 2.6-3 Associated Accounts



[Back to Table of Contents](#)

## 2.7 Resetting Passwords

There are several reasons for why a user may want or need to reset their password. In most cases this can be done without the assistance of a system administrator. This section of the guide identifies the various circumstances for resetting a password and provides detailed instructions on what to steps to take in each instance.

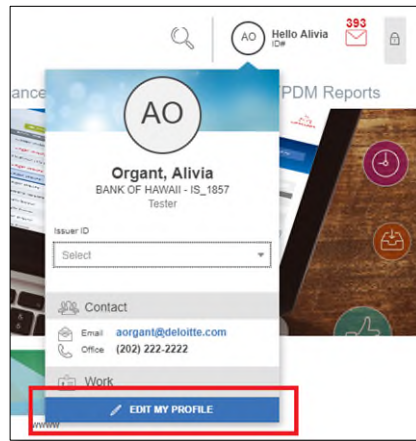
### 2.7.1 Change Password

As a security requirement, portal passwords are set to expire every 90 days. If a user has received an email notification that their password is about to expire or would like to change their password for any other reason, the user can do so by following these steps:

**NOTE:** If you are changing your password after receiving the Password Expiry Warning email link, you will skip steps 1-5, and begin at step 6.

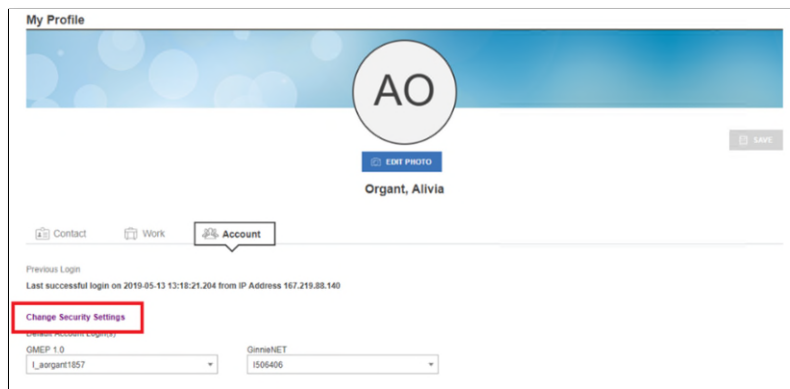
1. Follow the instructions for [Logging into MyGinnieMae](#).
2. Select the user avatar or initials from the Global Header at the top of the page on My Dashboard.
3. Select **Edit My Profile**.

Figure 2.7-1 Edit User's Profile



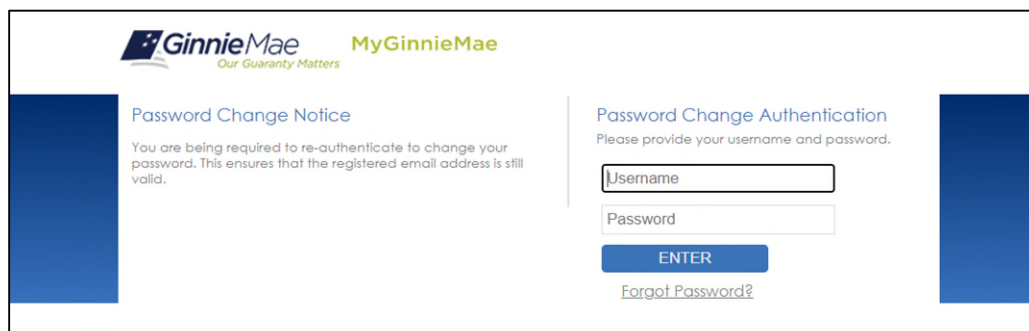
4. Select the **Account** tab.
5. Select **Change Security Settings**.

Figure 2.7-2 Change Security Settings



6. The Password Change Authentication Screen will be displayed. Enter your **Username** and **Current Password**. Select **Enter**.

Figure 2.7-3 Password Change Notice



**NOTE:** This page will open in a new tab, however, the Portal Session in the original tab will continue. Once you have changed your password, close one of these tabs to avoid an Automatic Logout.

7. The system will prompt the Multi-Factor Authentication. You will receive your One-Time Pin (OTP) via email.

**NOTE:** Oracle Mobile Authenticator cannot be used to complete the OTP for password change authentications. You may only complete authentication with the OTP received via email delivery.

8. Enter the **OTP** received via email in the One-Time PIN field and select Enter.

Figure 2.7-4 Password Change Notice

**NOTE:** If a user account is disabled, the user will see the following error message. This error message will also show up if an invalid username and password are submitted:

Figure 2.7-5 Disabled User Username Prompt - Error

9. On the Change Password page,
  - a. Enter the **Current Password**
  - b. Enter a **New Password**
  - c. **Confirm New Password**
  - d. Select **Submit**

Figure 2.7-6 Change Password Page

**Change Password**

**Password Policy**

- Password must not match or contain first or last name.
- Password must be 8-20 characters long.
- Password must contain at least 2 alphabetic characters, and at least 1 uppercase and lowercase letter(s).
- Password must contain at least 1 numeric character(s).
- Password must contain at least 1 special character(s).
- Password must not contain the username or match the last 24 previous passwords.

**Current Password:**

**New Password:**

**Confirm New Password:**

**Submit**

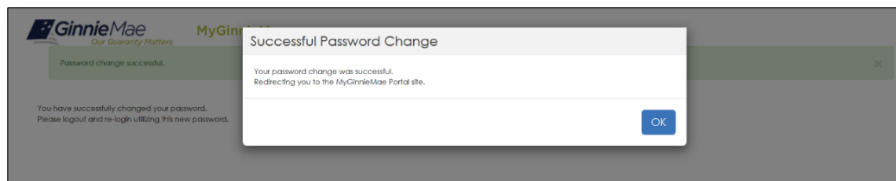
**Display RSA Token QR Code**  
To display RSA Token QR Codes for importing into mobile devices, click the RSA QR Code button below.

**RSA QR Code**

[Return to Portal](#)

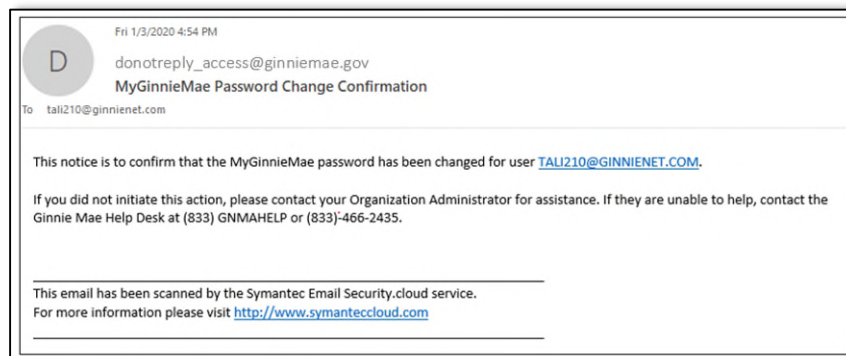
7. A successful password change message will display,
  - a. Select **OK**

Figure 2.7-7 Successful Password Change Message



8. The user will receive a confirmation email that their password has been changed.

Figure 2.7-8 Change Password Confirmation Email



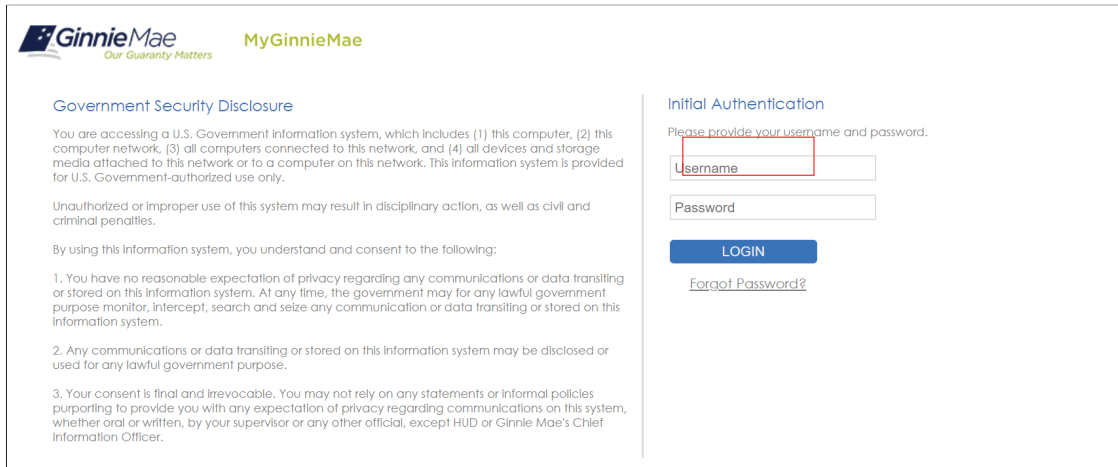
[Back to Table of Contents](#)

## 2.7.2 Forgotten Password

If a user has forgotten their password, they may change it on their own by following the instructions below.

1. Navigate to the Public Landing Page at <https://my.ginnie Mae.gov/>.
2. Select **Login**.
3. Select **Forgot Password?**

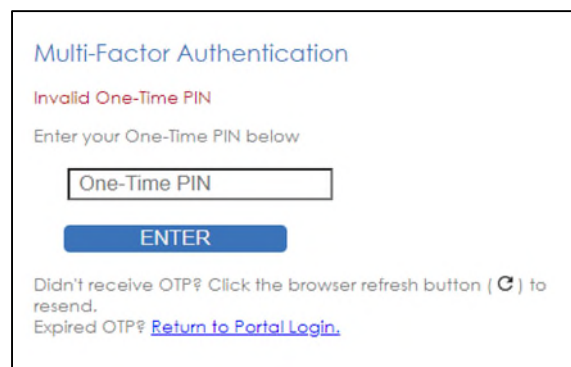
Figure 2.7-9 Login Page



The screenshot shows the MyGinnieMae login interface. On the left, there is a 'Government Security Disclosure' section with text about U.S. Government Information system access and a list of three consent points. On the right, the 'Initial Authentication' section prompts the user to provide a username and password. It includes input fields for 'Username' and 'Password', a blue 'LOGIN' button, and a link for 'Forgot Password?'. The 'Username' field is highlighted with a red rectangle.

**NOTE:** If the user enters the incorrect username or does not have a registered MGM account, they will see the following error message:

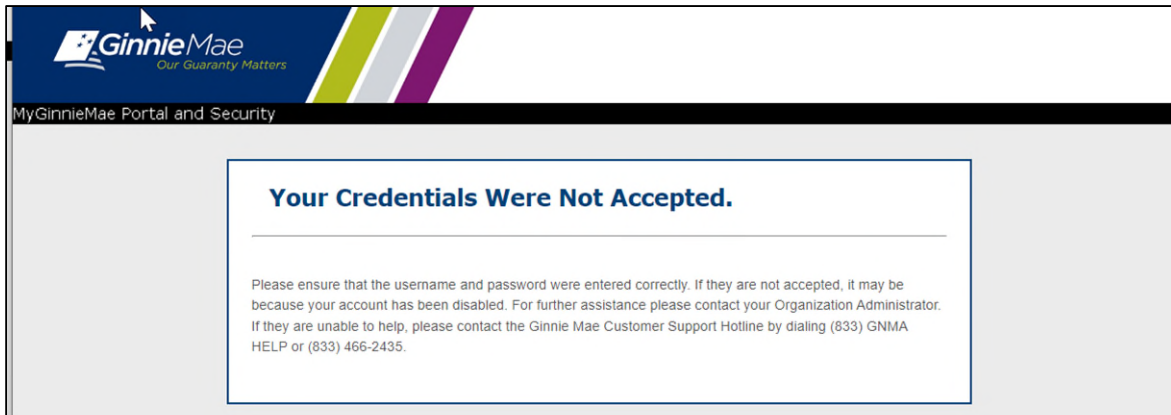
Figure 2.7-10 Forgot Password Username Prompt - Error



The screenshot displays a 'Multi-Factor Authentication' error screen. It features a red heading 'Invalid One-Time PIN' and a prompt to 'Enter your One-Time PIN below'. Below this is an input field labeled 'One-Time PIN' and a blue 'ENTER' button. At the bottom, there are instructions: 'Didn't receive OTP? Click the browser refresh button (⌂) to resend.' and 'Expired OTP? [Return to Portal Login.](#)'.

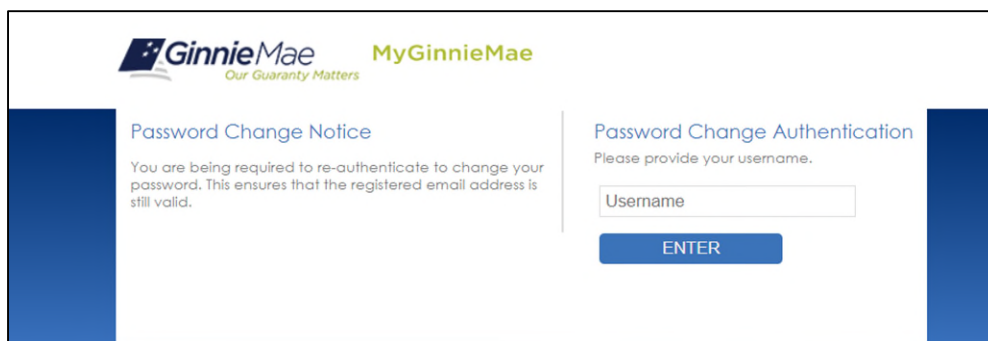
**NOTE:** If a user account is disabled, the user will see the following error message. This error message will also show up if an invalid username and password are submitted:

Figure 2.7-11 Disabled User Username Prompt - Error



4. The system will redirect to the Password Change Authentication screen. **Enter your username**, then select “Login.”

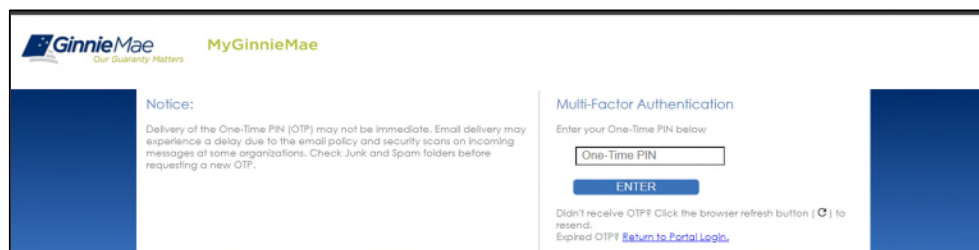
Figure 2.7-12 Forgot Password Username Prompt



5. After successfully entering their username, **Enter the OTP received via email in the One-Time PIN field and select Enter.**

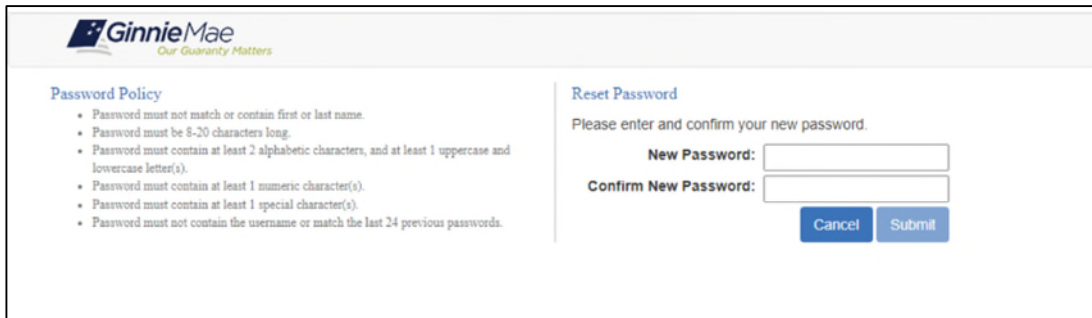
**NOTE:** Oracle Mobile Authenticator cannot be used to complete the OTP for Password Change Authentications. The user can only proceed with the OTP via Email delivery.

Figure 2.7-13 OTP via Email Delivery



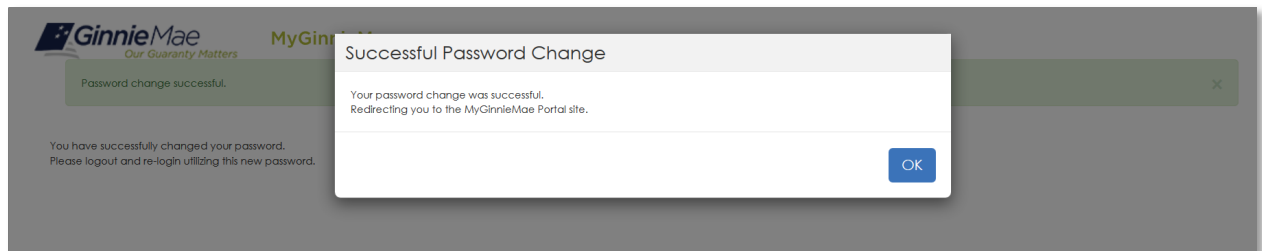
6. After successfully entering the OTP, the user will be directed to the Reset Password page to,
  - a. Enter a **New Password**
  - b. Confirm **New Password**
  - c. Select **Submit**

Figure 2.7-14 Reset Password Page



7. A successful password change message will display,
  - a. Select **OK**

Figure 2.7-15 Successful Password Change Message



8. The user will be redirected to the Login Page, where they can login using their new password.



Figure 2.7-16 Redirect to Login Page

The screenshot shows the MyGinnieMae login interface. On the left, under the GinnieMae logo, is a "Government Security Disclosure" section. It contains text about accessing a U.S. Government information system and lists three points of consent. On the right, under the "MyGinnieMae" logo, is the "Initial Authentication" section. It prompts the user to provide a username and password, with input fields for both. Below these fields is a blue "LOGIN" button and a link for "Forgot Password?".

**GinnieMae** Our Guaranty Matters **MyGinnieMae**

**Government Security Disclosure**

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following:

1. You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search and seize any communication or data transiting or stored on this information system.
2. Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.
3. Your consent is final and irrevocable. You may not rely on any statements or informal policies purporting to provide you with any expectation of privacy regarding communications on this system, whether oral or written, by your supervisor or any other official, except HUD or Ginnie Mae's Chief Information Officer.

**Initial Authentication**

Please provide your username and password.

Username

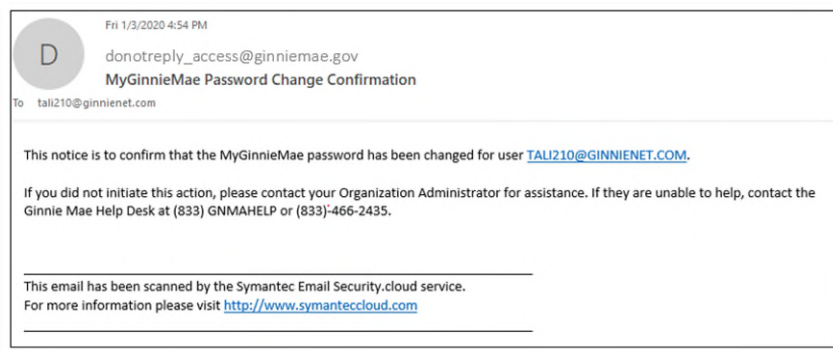
Password

**LOGIN**

[Forgot Password?](#)

9. The user will receive a confirmation email that their password has been changed.

Figure 2.7-17 Password Change Confirmation Email



[Back to Table of Contents](#)

### 2.7.3 Expired Password

As a security requirement, portal passwords are set to expire every 90 days. Once a password has expired, a notification email is sent, and the user will have to follow the instructions to change passwords upon next login. If the user has forgotten the expired password, contact the Organization Administrator to have the password reset. After three unsuccessful attempts to enter a password, the account will be locked, and the user must contact the Organization Administrator to have the account unlocked. See the [Organization Administrators](#) section.

**NOTE:** Users will receive a daily email notification of impending password expiration starting the 81<sup>st</sup> day until the 90<sup>th</sup> day or until the password has been reset. A password expiration email is sent after the 90<sup>th</sup> day.

**NOTE:** If you are changing your password after receiving the Password Expired email link, you will skip step 1 and begin at step 2.

1. Navigate to the Public Landing Page at <https://my.ginnie Mae.gov/> and select **Login**.
2. Login using the Username and **Expired Password**. See the [Entering a Username and Password](#) section.

Figure 2.7-18 Login Page

3. You will receive a One Time PIN (OTP) via your registered email. Enter your **OTP** and select **Enter**.

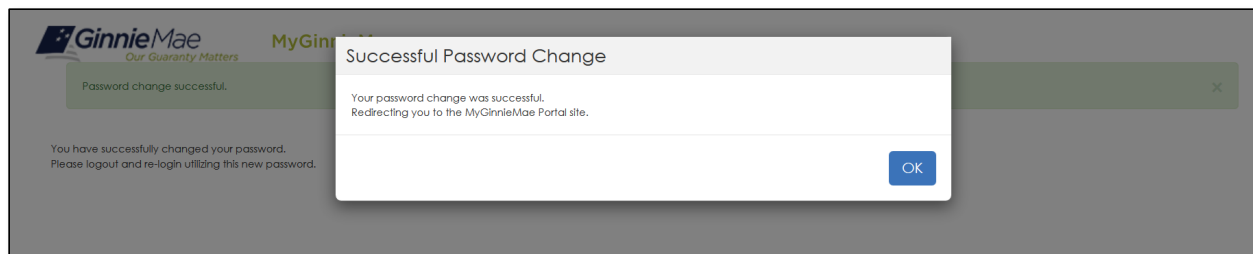
Figure 2.7-19 OTP Page

4. After successfully entering the OTP, the user will be directed to the Reset Password page to,
  - a. Enter a **New Password**
  - b. Confirm **New Password**
  - c. Select **Submit**

Figure 2.7-20 Enter New Password Page

5. A successful password change message will display.

Figure 2.7-21 Successful Password Change Message

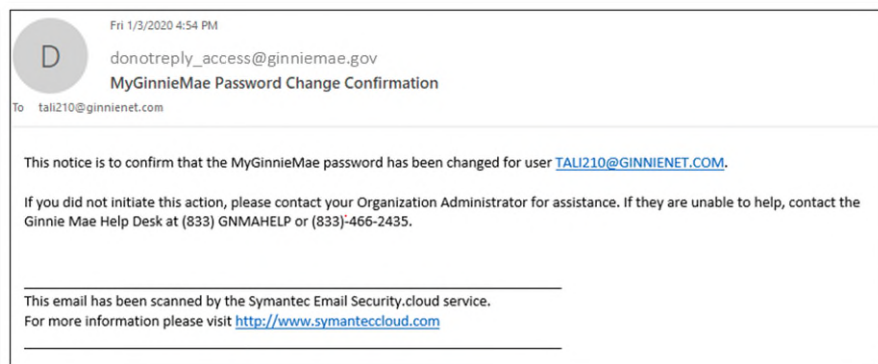


6. The user will be redirected to the Login Page, where they can login using their new password.

Figure 2.7-22 Redirect to Login Page

7. The user will receive a confirmation email that their password has been changed.

Figure 2.7-23 Password Change Confirmation Email

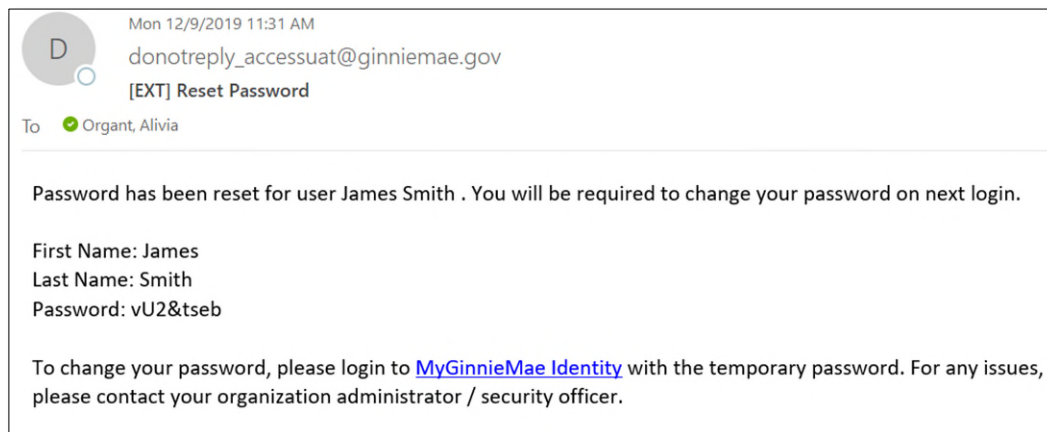


[Back to Table of Contents](#)

## 2.7.4 Logging In After an Admin Reset a User's Password

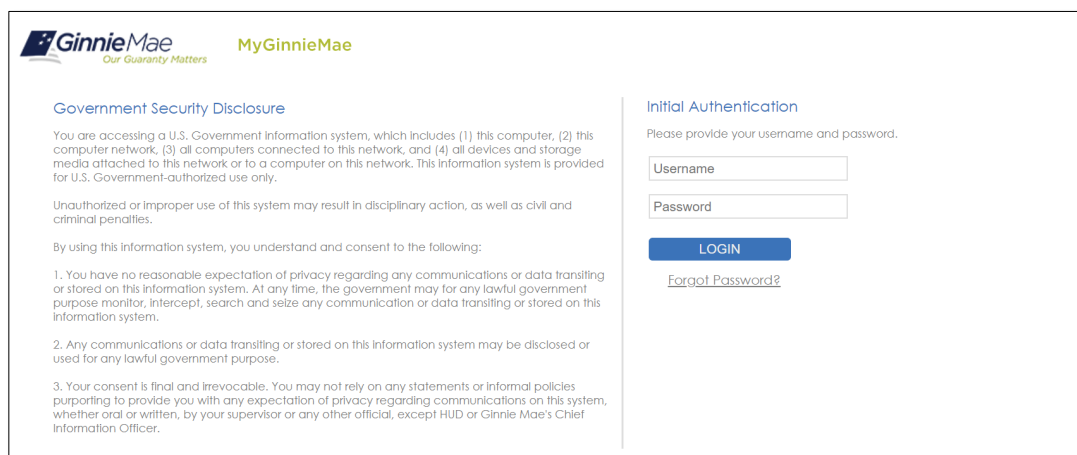
If an Organization or Operations Admin has reset a user's password using the Access Management Console, the user will receive an email containing a temporary password. The user will no longer be able to sign into the Portal with their old password and will be prompted to change their password upon first time login with the new, temporary password.

Figure 2.7-24 Temporary Password Email



1. Navigate to the Public Landing Page at <https://my.ginniema.gov/> and select **Login**.
2. Login using the Username and **Temporary Password**. See the [Entering a Username and Password](#) section.

Figure 2.7-25 Login Page



3. Select your **Preferred Method** of receiving a One-Time PIN (OTP) and select **OK**.

Figure 2.7-26 OTP Page

**GinnieMae** Our Guaranty Matters **MyGinnieMae**

**Notice:**  
Please select the method of retrieving your One-Time PIN (OTP). The Oracle Mobile Authenticator, on your smart device, will generate your OTP, or you can have your OTP delivered to you via the registered email address.

**Multi-Factor Authentication**  
Please choose your preferred method

☐ One Time Pin through Email  
☐ One Time Pin from Oracle Mobile Authenticator

**OK**

4. Enter your **OTP** and select **Login**.

Figure 2.7-27 OTP Page

**GinnieMae** Our Guaranty Matters **MyGinnieMae**

**Notice:**  
Delivery of the One-Time PIN (OTP) may not be immediate. Email delivery may experience a delay due to the email policy and security scans on incoming messages at some organizations. Check Junk and Spam folders before requesting a new OTP.

**Oracle Mobile Authenticator (OMA)**  
MyGinnieMae now allows for your One-Time PIN (OTP) to be generated with the Oracle Mobile Authenticator (OMA) on your smart device. Click the below link for instructions on how to download and sync the application with your MyGinnieMae account.  
[Oracle Mobile Authenticator Instructions](#)

**Multi-Factor Authentication**  
Enter your One-Time PIN below

One-Time PIN

**LOGIN**

Didn't receive OTP? Click the browser refresh button (↻) to resend.  
Expired OTP? [Return to Portal Login](#).

5. After successfully entering the OTP, the user will be directed to the Reset Password page to,
  - a. Enter a **New Password**
  - b. Confirm **New Password**
  - c. Select **Submit**

Figure 2.7-28 Enter New Password Page

**GinnieMae** Our Guaranty Matters

**Password Policy**

- Password must not match or contain first or last name
- Password must be 8-20 characters long.
- Password must contain at least 2 alphabetic characters, and at least 1 uppercase and lowercase letter(s).
- Password must contain at least 1 numeric character(s).
- Password must contain at least 1 special character(s).
- Password must not contain the username or match the last 24 previous passwords.

**Reset Password**  
Please enter and confirm your new password.

**New Password:**

**Confirm New Password:**

**Cancel** **Submit**

6. A successful password change message will display.
  - a. Select **OK**

Figure 2.7-29 Successful Password Change Message

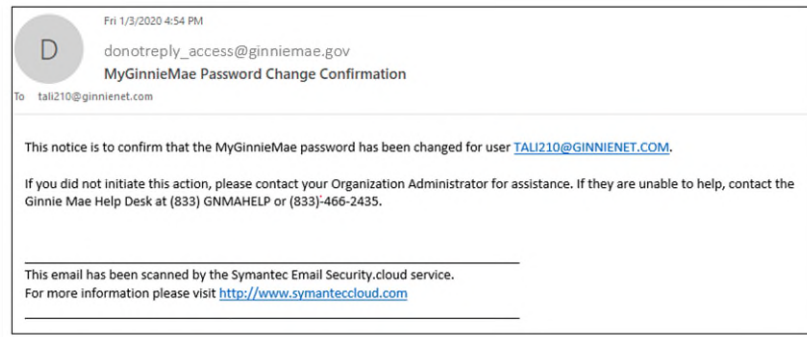
**Successful Password Change**

Your password change was successful.  
Click **OK** to be redirected to MyGinnieMae Portal.

**OK**

7. The user will be redirected to the Login Page, where they can login using their new password.
8. The user will receive a confirmation email that their password has been changed.

Figure 2.7-30 Password Change Confirmation Email



[Back to Table of Contents](#)

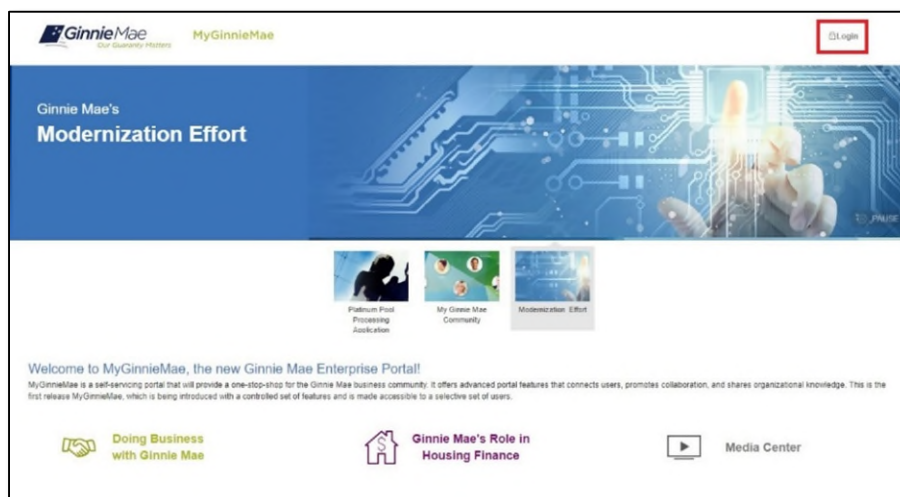
## 2.8 Logging into MyGinnieMae

To successfully log into the portal, users must correctly enter their username, which is the corporate email address used to register for the MyGinnieMae account, the current password, and One-Time PIN (OTP) sent to the corporate email address or through the Oracle Mobile Authenticator (OMA). Once entered users can navigate freely within the portal and its business applications.

### 2.8.1 Entering a Username and Password

1. Navigate to the Public Landing Page at <https://my.ginniemae.gov/> and select **Login**.

Figure 2.8-1 Public Landing Page



**NOTE:** It is recommended that users bookmark the Public Landing Page at <https://my.ginniemae.gov/>. Bookmarking any other page will cause navigation issues.

2. On the Login Page,
  - a. Enter **Username**
  - b. Enter **Password**
  - c. Select **Login**

Figure 2.8-2 Login Page

**GinnieMae** **MyGinnieMae**  
Our Guaranty Matters

**Government Security Disclosure**

You are accessing a U.S. Government Information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following:

1. You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search and seize any communication or data transiting or stored on this information system.
2. Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.
3. Your consent is final and irrevocable. You may not rely on any statements or informal policies purporting to provide you with any expectation of privacy regarding communications on this system, whether oral or written, by your supervisor or any other official, except HUD or Ginnie Mae's Chief Information Officer.

**Initial Authentication**

Please provide your username and password.

Username

Password

**LOGIN**

[Forgot Password?](#)

**NOTE:** If a user enters an incorrect username or password, or their account is disabled or locked, they will see the following error message. The user must retry and enter the correct username and password.

Figure 2.8-3 Incorrect Username/Password Error

**Initial Authentication**

Please provide your username and password.

**Username or password entered incorrectly.  
Please select the Forgot Password link if you  
require a password reset.**

Username

Password

**LOGIN**

[Forgot Password?](#)

[Back to Table of Contents](#)

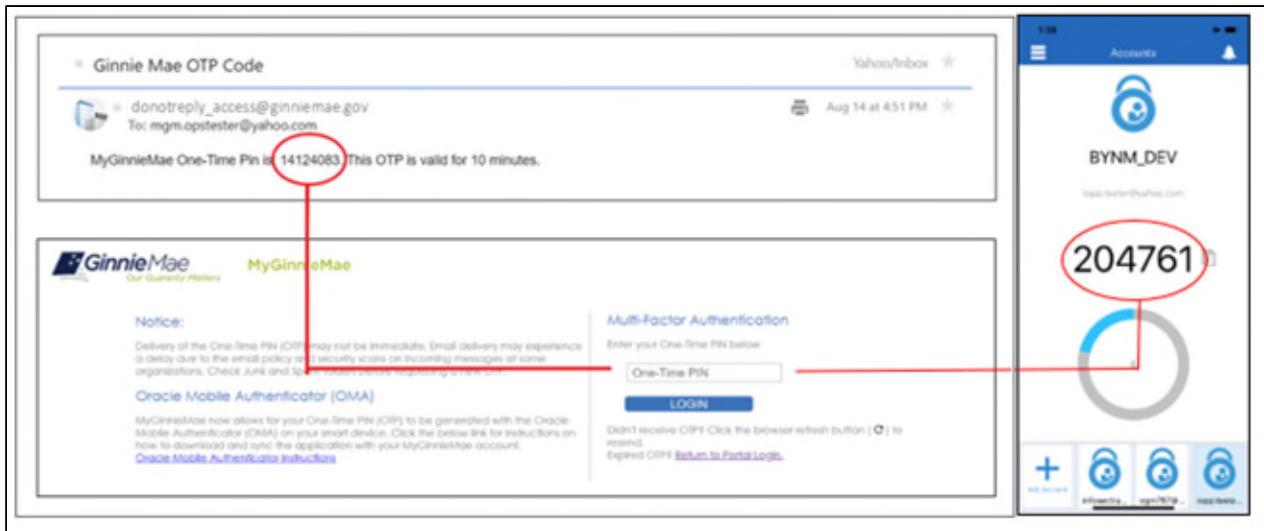
## 2.8.2 Choosing and Entering a One-Time PIN (OTP)

After successfully entering a username and password, the Multi-Factor Authentication Page will display.

1. If the user has enrolled with the Oracle Mobile Authenticator (OMA), the user will be prompted to select:
2. If the user has not enrolled with OMA, the system will automatically send the OTP through email.
3. A One-Time PIN field will appear,
  - a. Enter the OTP received
  - b. Select **LOGIN**



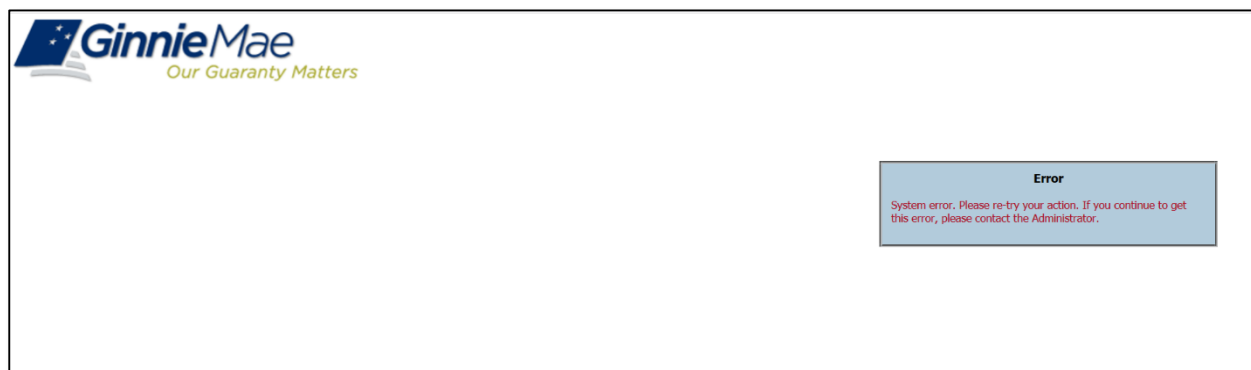
Figure 2.8-4 (Above) One-Time PIN (OTP) through email / (RIGHT) OTP from Oracle Mobile Authenticator (OMA)



**NOTE:** The OTP from OMA will regenerate every 30 seconds and the user must enter the OTP currently displaying. The OTP through email is valid for 10 minutes; once 10 minutes has elapsed, a new OTP must be generated. If the OTP has expired or a System Error displays, close the browser and return to the Public Landing Page to log in again. If you requested an OTP through email and did not receive it, select the browser refresh button to generate a new OTP.

The Multi-Factor Authentication Page will timeout after 15 minutes if the user does not make a selection or enter an OTP and a System Error will be generated. The user must close the browser and return to the Public Landing Page to log in again.

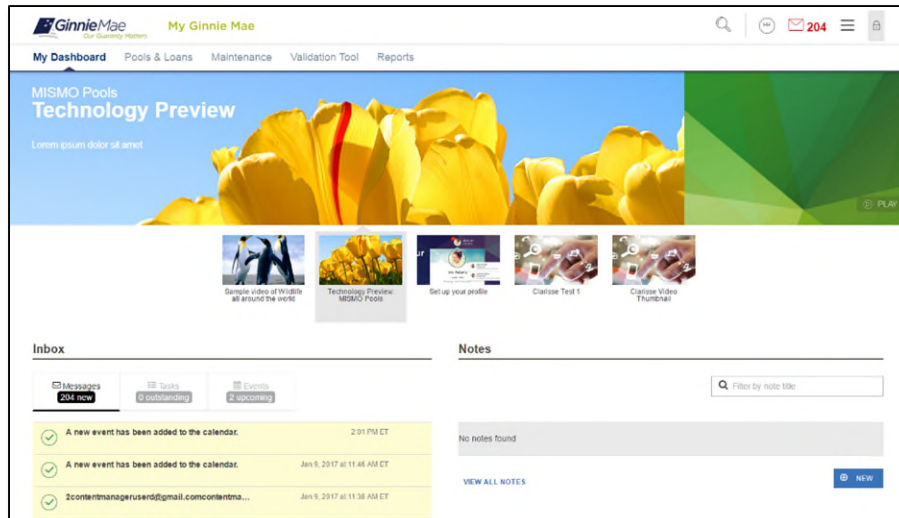
Figure 2.8-5 System Error Message



4. Once all credentials are successfully entered, the system will direct to the My Dashboard landing page.



Figure 2.8-6 My Dashboard



**NOTE:** If the user does not have functional roles assigned, the system will not direct the user to My Dashboard and the user will see an error. The user should contact their Organization Administrator to request a role(s).

[Back to Table of Contents](#)

### 2.8.3 Logging In After an Admin has Enabled User's Account

If the user's account has been disabled due to 90 days of inactivity or for any other reason, the account must be re-enabled, and Functional Roles must be access must again be provisioned by the Organization Administrators. See the [Organization Administrators](#) section. Once the account is re-enabled, a user must log into the account the same day; if the user does not log in to MyGinnieMae on the same day the account is re-enabled, the system will disable the account again the following day. It is suggested that the user log into MyGinnieMae while on the phone or in contact with their Organization Administrator.

**NOTE:** The recommendation is for users to log in to MyGinnieMae at least once each 90-day period to avoid the account becoming inactive and to ensure that access is readily available whenever urgently needed at short notice.

[Back to Table of Contents](#)

## 2.9 Exiting

Users may exit the portal in one of two ways manually and automatically. Whichever way the user chooses to exit the portal it is important to know that closing a portal session does not close any application sessions that have opened in new browser windows. For security reasons, a user should make sure to properly exit all open sessions when finished working.

## 2.9.1 Manually Exiting MyGinnieMae


1. To exit MyGinnieMae at any point, select the  lock icon at the top right of the page.

Figure 2.9-1 Logout Lock Icon



2. Select **LOG OUT**.

Figure 2.9-2 Portal Logout



**NOTE:** For security reasons, always select “LOG OUT” after finishing a session and before closing the browser.

[Back to Table of Contents](#)

## 2.9.2 Automatic Logout

The Portal Session Timeout timer is a security feature that automatically logs the user out after 20 minutes of inactivity while also indicating how much time is left before the session times out. The session timer will automatically extend when the user:

- Manually refreshes the page,
- Selects the Extend button to extend the session, or
- Navigates from page to page within the Portal


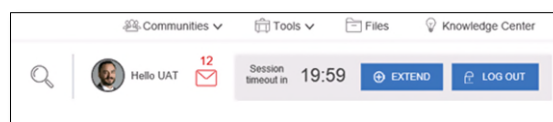
To reveal the Portal Session Timeout timer, select the  lock icon in the top right corner of the page.

Figure 2.9-3 Portal Session Timeout Timer



The timeout period for business applications on the Portal is the federal security standard 20 minutes of inactivity. If the session times out, close the browser and open a new browser session before attempting to log back into MyGinnieMae.

[Back to Table of Contents](#)

## 2.10 Navigating the Portal

### 2.10.1 Accessing Business Applications

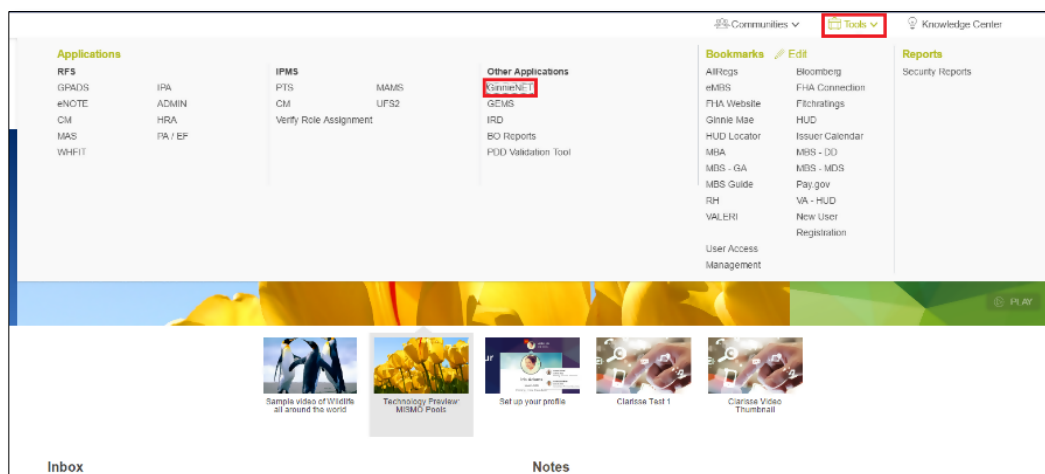
MyGinnieMae Portal is protected with Multi-Factor Authentication (MFA) via a One-Time PIN (OTP) sent to the corporate email address or through the Oracle Mobile Authenticator. Once entered users can navigate freely within the portal and its business applications.

If the user has access to multiple organizations, that user must select the preferred organization ID before navigating to business applications to avoid navigation errors. See the [Issuer ID](#) section for more information on selecting the proper organization ID on the user's profile.

1. Once logged into the portal, select the “Tools” drop-down from the Global Header top of the page.
2. Select the business application (i.e. GinnieNET) to be accessed.

**NOTE:** If the application does not open immediately, wait 10 to 20 seconds before selecting the link again.

Figure 2.10-1 Accessing a Business Application



**NOTE:** The first time a new portal user selects a GMEP 1.0 or GinnieNET application from the Tools drop-down, a one-time dialog box will be displayed. Choose “Select” to pick the Default User ID. Users with multiple GMEP 1.0 accounts (for example, organizations sub-servicing for other Issuers) must keep track of the access/orgs provided to them for each account when selecting those accounts in My Profile.

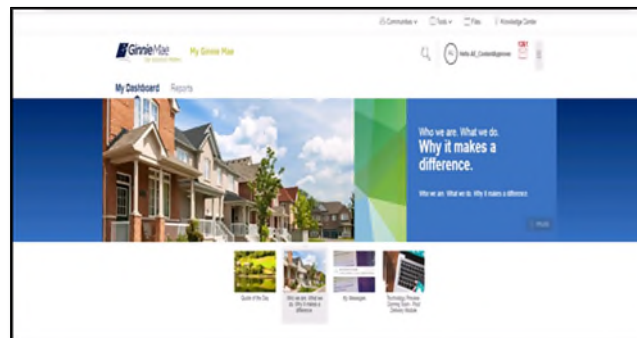
- When switching between business applications, if the user has access to multiple organizations and wants to view data for one organization in particular, the user must first select the preferred organization ID before navigating to another business application. See the [Issuer ID](#) section for more information on selecting the proper organization ID on the user's profile.

[Back to Table of Contents](#)

## 2.10.2 Marquee

On both the MyGinnieMae Public Landing Page and My Dashboard, the user can navigate through the marquee content and pause the carousel rotation. Use the left or right navigation arrows to cycle through content and select the Pause button to stop the carousel's rotation. Users may select on the marquee to open the full article detail which can display text, images, and video content.

Figure 2.10-2 Marquee

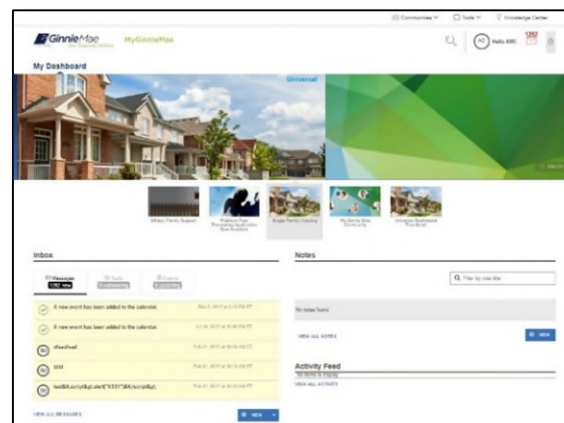


[Back to Table of Contents](#)

## 2.10.3 My Dashboard

Upon authentication, the user will be directed to their tailored landing page.

Figure 2.10-3 My Dashboard



On the My Dashboard page, the user is able to preview all the MyGinnieMae news, updates, and activities in the Portal. For instance, the user can:

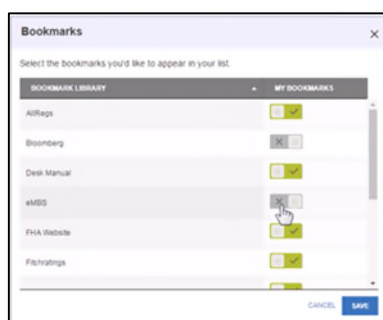
- Access Communities, Tools, Files, and the Knowledge Center using the Global Header. Select Communities or Tools to view a drop-down menu of predefined links.
- View recent messages. Select on an individual list item to view the entire message. Additionally, the user can view all their messages by selecting the VIEW ALL MESSAGES link.
- Access the Activity Feed for summarized updates from shared components such as community forums and files. Feed items include navigation links allowing the user to view or download a file or view a forum post or comment.

[Back to Table of Contents](#)

## 2.10.4 Bookmarks

In the “Tools” drop down, each user has a section titled “Bookmarks.” Users can manage visibility preferences for the items available in this section. Select the “Edit” link to access the personalization control panel. Select to hide or show bookmarks. When done, select “Save” to display the personalized view of bookmarks within Tools.

Figure 2.10-4 Bookmarks

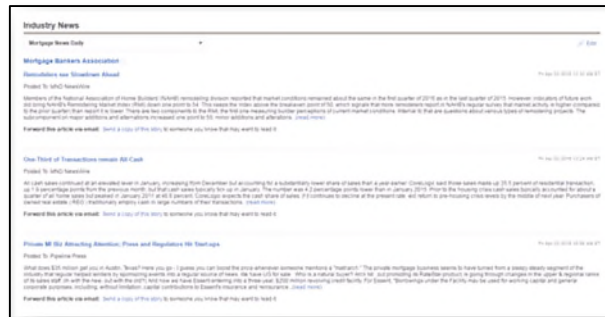


[Back to Table of Contents](#)

## 2.10.5 Industry News

Select a news feed from the drop-down menu to see currently available news content from a particular publisher. Select the two-line summary to view the full article summary. Select the headline to view the complete article in a separate tab that will redirect to the publisher's site.

Figure 2.10-5 Industry News

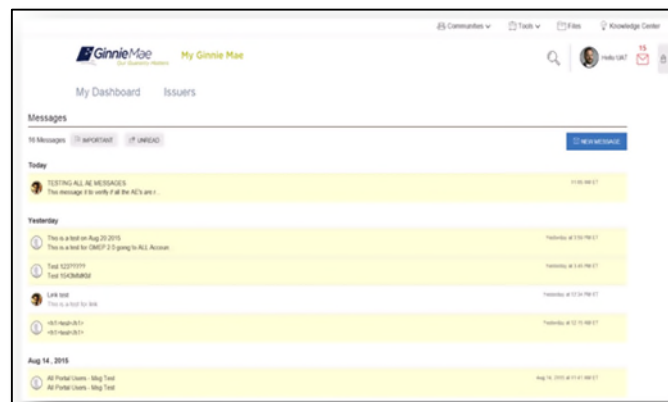


[Back to Table of Contents](#)

## 2.10.6 Messages

Users can send, view, and filter messages in their inbox. Select the “IMPORTANT” and/or “UNREAD” buttons to filter messages being displayed. Users can view individual messages with the ability to Flag, Mark as Read/Unread, and Delete. Ginnie Mae Account Executives also have a “New Message” option to send a message.

Figure 2.10-6 Messages



[Back to Table of Contents](#)

## 2.11 Dashboard Components/Widgets

Dashboard components/widgets provide business information based on “persona type” such as Issuer, Document Custodian, and Ginnie Mae Staff. A user’s persona type determines which components/widgets will show on their dashboard.

### 2.11.1 Commitment Authority Dashboard Chart

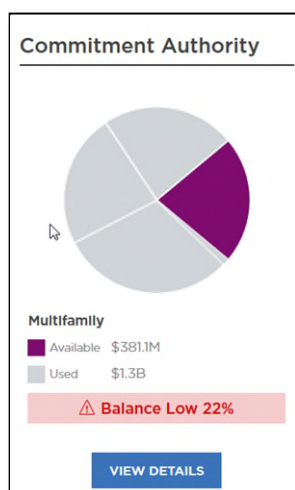
Users with the assigned Functional Role that includes access to the Commitment Management (CM) application may view the organization's available and used Commitment Authority. The user will only be able to access their organization's information. Select the associated Issuer ID list to view data specific to each business entity for which the user is responsible.

When the user hovers over the pie-chart widget, a rounded dollar value will display along with the assigned expiration date for those funds, including available and used.

A low balance alert will display when available funds fall below the predefined 25% threshold.

Select the "View Details" button to access the appropriate module to retrieve details or request additional Commitment Authority.

Figure 2.11-1 Commitment Authority Details



[Back to Table of Contents](#)

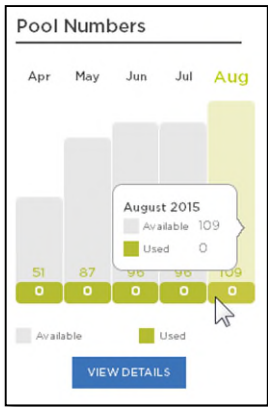
### 2.11.2 Pool Numbers Dashboard Chart

Users with the assigned Functional Role that includes access to the Request Pool Number (RPN) application may view their organization's utilization of pool numbers over time. The user will only be able to access their organization's information.

When users hover over any bar-chart segment, the number of pool numbers used and available in the selected month is displayed.

Select the "View Details" button to access the appropriate module within the GMEP 1.0 Portal.

Figure 2.11-2 Pool Number Details



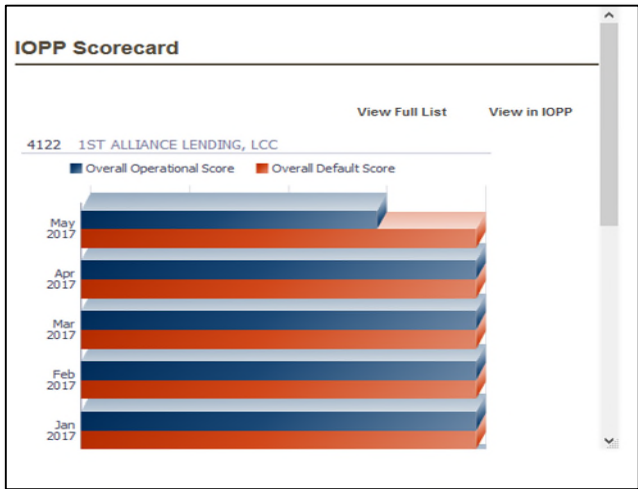
[Back to Table of Contents](#)

2.11.3 Issuer Operational Performance Profile (IOPP) Scorecard

Ginnie Mae Issuers have a high-level view of their respective Issuer Operational Performance Profile (IOPP) information. The user can access more detailed issuer performance information by navigating to IOPP via the “View in IOPP” link from the Dashboard component/widget, including:

- Issuer details for the currently selected issuer,
- Overall Operational score,
- Overall Default score (Single-Family Issuers only), and
- Full Issuer report in IOPP (GMEP 1.0).
- The “View in IOPP” hyperlink will redirect to the IOPP application.

Figure 2.11-3 IOPP Scorecard



[Back to Table of Contents](#)



## 2.12 Communities

Provides access to blog posts and discussion forums to share information on a variety of business topics. Not all “personas” are granted discussion forum access. Currently, Ginnie Mae Account Executives may initiate and respond to discussions, while some users are able to comment on existing discussions, and others do not have access to this feature at all.

### 2.12.1 Leadership Blog

Ginnie Mae leadership may use blog posts to communicate industry events and information and Ginnie Mae announcements with the MyGinnieMae user community. Select “Communities” in the header and select “Leadership Blog” from the drop-down. A list of blog posts will display. The user will see only blog posts targeted to them. Select “Read More” to display the full-page view of the blog post.

Figure 2.12-1 Leadership Blog



Select “Comments” to display all comments made to the blog post. To add a comment, enter the text in the “Leave a Comment” field and select “Post Comment.”

[Back to Table of Contents](#)

### 2.12.2 Discussion Forums

Discussion forums provide a central location where a user can create and discuss relevant Ginnie Mae topics with other users. The user can view discussions details including:

- Topics
- Author
- Thread Started
- Replies
- Last Post

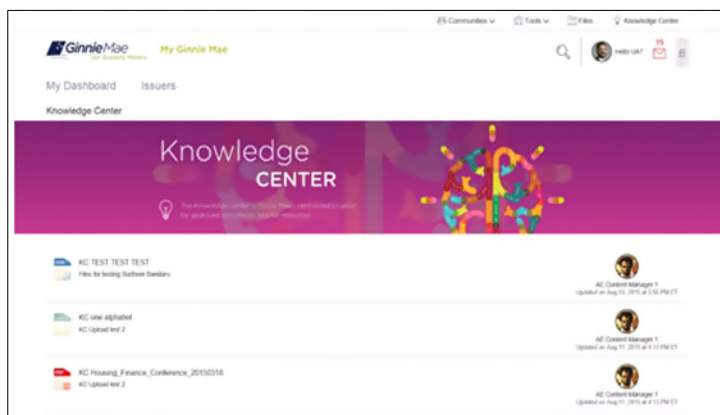
Select the “New Discussion” link to create a new discussion topic. A window will appear in which the user may start a discussion. Current forums include an Account Executive to Issuer Forum and an Account Executive to Account Executive Forum. Additional forums may be added based on input and feedback from Portal users.

[Back to Table of Contents](#)

## 2.13 Knowledge Center

The Knowledge Center provides a central location to view and download approved resources. A Ginnie Mae Content Manager manages the Knowledge Center.

Figure 2.13-1 Knowledge Center



[Back to Table of Contents](#)

## 2.14 Portal Search

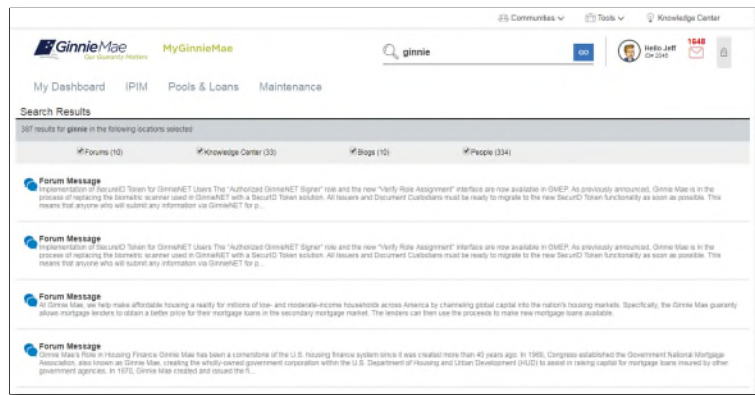
The search function allows a user to quickly find items such as files, forums, and people within MyGinnieMae. It is represented by a magnifying glass icon and located above the Marquee.

Figure 2.14-1 Portal Search



When the user selects the magnifying glass icon, a search bar will expand in which the user enters search keyword(s). Select the “Go” button to initiate the search. The system will display the search results page, which shows relevant items within MyGinnieMae based on the search criteria and permissions. Users can filter search results by Files, Forums, Knowledge Center, and People. The total match count is displayed on the top right of the filter bar and subset result counts are shown next to each filter.

Figure 2.14-2 Search Results



Contact information for people results includes basic contact information such as Title, Email, and Phone Number.

## 2.15 Requesting an RSA SecurID Soft Token for The First Time

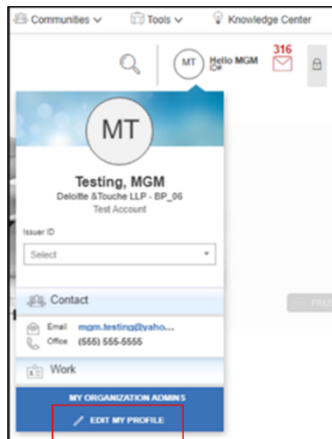
To request an RSA SecurID Soft Token, a user must reach out to their Organization Administrator. The Organization Administrator will verify the user is an authorized signer in the HUD-11702 and request an Authorized Signer Functional Role for the user. If the role provisioning is completed, the new RSA SecurID Soft Token will automatically be assigned and distributed to the user.

## 2.16 Self-Service RSA SecurID Soft Token Replacement

A user may need to replace their RSA SecurID Soft Token if they no longer have the device their soft token was installed on or want to switch the device their soft token is installed on. The self-service process below only applies to replacement soft tokens.

1. Follow the instructions for [Logging into MyGinnieMae.](#)
2. From My Dashboard, select the user avatar or initials from the Global Header at the top of the page.

Figure 2.16-1 Edit My Profile



3. Select **Edit My Profile**.
4. Select the **Account** tab.
5. Select **Change Security Settings**

Figure 2.16-2 User's Profile Account Tab



6. The Password Change Authentication Screen will be displayed. Enter your **Username** and **Current Password**. Select **Enter**.

Figure 2.16-3 Password Change Notice

The screenshot shows the 'GinnieMae' logo with the tagline 'Our Guaranty Matters' and 'MyGinnieMae'. The page is titled 'Password Change Notice' and contains the text: 'You are being required to re-authenticate to change your password. This ensures that the registered email address is still valid.' To the right, under 'Password Change Authentication', it says 'Please provide your username and password.' There are input fields for 'Username' and 'Password', an 'ENTER' button, and a link for 'Forgot Password?'.

7. The system will prompt the Multi-Factor Authentication. You will receive your One-Time Pin (OTP) via email.

**NOTE:** Oracle Mobile Authenticator cannot be used to complete the OTP for password change authentications. You may only complete authentication with the OTP received via email delivery.

8. Enter the **OTP** received via email in the One-Time PIN field and select Enter.

Figure 2.16-4 Password Change Notice

The screenshot shows the 'GinnieMae' logo and 'MyGinnieMae'. Under 'Notice:', it states: 'Delivery of the One-Time PIN (OTP) may not be immediate. Email delivery may experience a delay due to the email policy and security scans on incoming messages at some organizations. Check Junk and Spam folders before requesting a new OTP.' To the right, under 'Multi-Factor Authentication', it says 'Enter your One-Time PIN below'. There is an input field for 'One-Time PIN', an 'ENTER' button, and a note: 'Didn't receive OTP? Click the browser refresh button (🔄) to resend. Expired OTP? [Return to Portal Login.](#)'

**NOTE:** If a user account is disabled, the user will see the following error message. This error message will also show up if an invalid username and password are submitted:

Figure 2.16-5 Disabled User Username Prompt - Error

The screenshot shows the 'GinnieMae' logo and 'MyGinnieMae Portal and Security'. A central box contains the title 'Your Credentials Were Not Accepted.' followed by the text: 'Please ensure that the username and password were entered correctly. If they are not accepted, it may be because your account has been disabled. For further assistance please contact your Organization Administrator. If they are unable to help, please contact the Ginnie Mae Customer Support Hotline by dialing (833) GNMA HELP or (833) 466-2435.'

6. Select **RSA QR Code** on the Change Password Page.

Figure 2.16-6 Change Password Page

The screenshot shows the 'Change Password' page. On the left, under 'Password Policy', there are five bullet points: 'Password must not match or contain first or last name.', 'Password must be 8-20 characters long.', 'Password must contain at least 2 alphabetic characters, and at least 1 uppercase and lowercase letter(s).', 'Password must contain at least 1 numeric character(s).', and 'Password must contain at least 1 special character(s).'. Below these is a note: 'Password must not contain the username or match the last 24 previous passwords.' On the right, there are three input fields labeled 'Current Password:', 'New Password:', and 'Confirm New Password:'. A red rectangle highlights the 'Confirm New Password' field and the 'Submit' button. Below the input fields, there is a section titled 'Display RSA Token QR Code' with the text 'To display RSA Token QR Codes for importing into mobile devices, click the RSA QR Code button below:'. A blue button labeled 'RSA QR Code' is visible. At the bottom left, there is a link 'Return to Portal'.

7(A). **Mobile Use Only** – Select the mobile device type in which you will be installing the soft token.

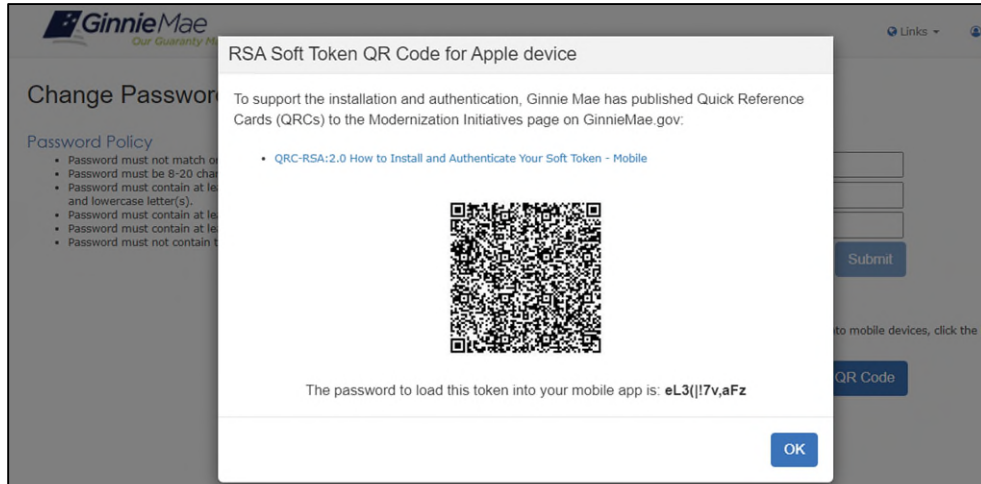
Figure 2.157 Select Device

Figure 2.16-7 Select Device

The screenshot shows the 'Change Password' page with a modal dialog titled 'Select Mobile Device' open in the center. The dialog contains the text 'Please select the mobile device for your RSA SecurID Authenticator.' and four buttons: 'Apple Device', 'Android Device', 'Windows Phone', and 'File Delivery'. A 'Cancel' button is also present. The background page is dimmed, showing the same 'Change Password' form as in Figure 2.16-6, including the password policy, input fields, and the 'RSA QR Code' button.

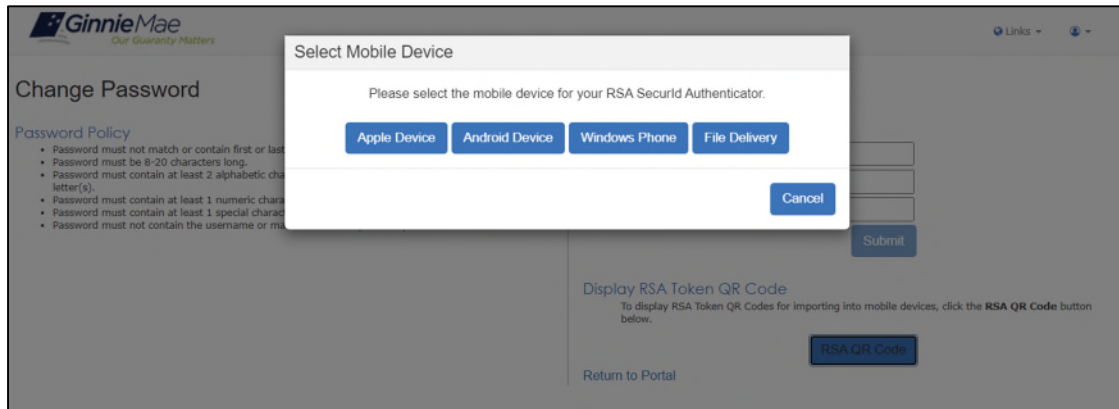
8(A). **Mobile Use Only** – Stay on this page as you will need the QR code. Open the [“How to Install and Authenticate Soft Tokens – Mobile”](#) QRC and follow the steps to Install and Authenticate your RSA SecurID Soft Token.

Figure 2.16-8 RSA Soft Token QR Code



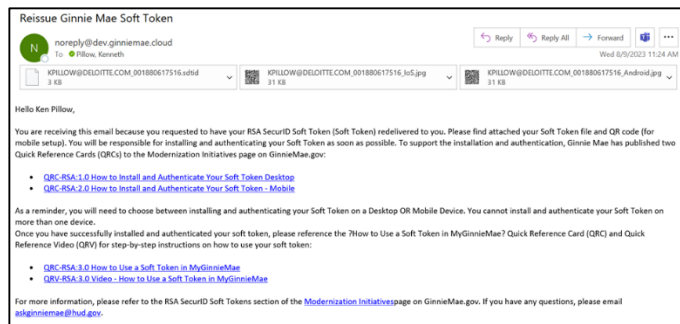
7(B). Desktop Use Only – Select File Delivery

Figure 2.16-9 Select Device



8(B). You will receive an email from [noreply@access.ginniemae.gov](mailto:noreply@access.ginniemae.gov) with the subject **Reissue Ginnie Mae Soft Token** containing your soft token file. Follow the instructions in the email to Install and Authenticate your RSA SecurID Soft Token.

Figure 2.16-10 Reissue Ginnie Mae Soft Token Email



## 3 TROUBLESHOOTING AND SYSTEM ERRORS

This section is designed to help identify common errors a user may encounter and other troubleshooting issues.

### 3.1 Basic Error Handling

**Issue:** An error message appears on the page that indicates the user should contact a System Administrator.

Figure 3.1-1 System Error Message



**Resolution:** Follow the steps below to troubleshoot the issue:

1. Determine which application the error message relates to – whether it is MyGinnieMae or a specific application within the portal.
  - a. Look to see if a specific application is mentioned in the error message text.
  - b. On the page on which the error message is displayed, check if there is a system name.
2. Review the documentation in the [Applications](#) section related to the appropriate application to ensure proper system usage.
3. Contact the Organization Administrator to ensure proper system access.
4. Contact [Ginnie Mae Customer Support](#).

[Back to Table of Contents](#)

### 3.2 New Password Mismatch Error

**Issue:** In the process of resetting a password, if a user incorrectly enters two new passwords that do not match, the system generates the error, “New passwords entered do not match.”

Figure 3.2-1 New Password Does Not Match Error



**Resolution:** The user must retry and enter a matching password.

[Back to Table of Contents](#)

### 3.3 Invalid Username or Password

**Issue:** When a user incorrectly enters either their username or password, they will receive the following error (the Portal validates both username and password simultaneously, rather than separately, for security purposes).

**Figure 3.3-1 Invalid Password Error**

**Resolution:** The user must retry and enter the correct username and password.

[Back to Table of Contents](#)

### 3.4 Incorrect OTP

**Issue:** When a user enters an invalid OTP during login, they will receive the system generated error, “Invalid One-Time PIN.” If you opted for email delivery and did not receive a One Time Pin, refresh the page (select “F5” on the keyboard or the refresh icon on the browser) to generate a new one.

Figure 3.4-1 Incorrect OTP Error

The screenshot shows the MyGinnieMae login interface. On the left, there is a 'Notice' section with text about OTP delivery delays and a link to 'Oracle Mobile Authenticator (OMA) Instructions'. The main area is titled 'Multi-Factor Authentication' and displays an 'Invalid One-Time PIN' error in red. Below the error, it prompts the user to 'Enter your One-Time PIN below' with a text input field labeled 'One-Time PIN' and a blue 'LOGIN' button. At the bottom, there are instructions for resending the OTP and a link to 'Return to Portal Login'.

**Resolution:** Check the OTP email and verify the correct OTP has been entered.

[Back to Table of Contents](#)

### 3.5 OTP Not Received

**Issue:** A user enters their username and password and is prompted to enter their OTP but has not received the email with the OTP.

**Resolution:** Allow for a reasonable amount of time (a few minutes) for messaging and email clients to deliver the OTP notification. The user should also check “Junk” and other filtered folders to determine if the email was misdirected. If the user has still not received an email with the OTP after several minutes, select the Refresh icon to prompt re-sending of the OTP email. If this second request still produces no results, contact the Operations Administrator via [Ginnie Mae Customer Support](#) to reset the OTP email.

Users are advised to [Register with the Oracle Mobile Authenticator](#) for reliable delivery of the OTP.

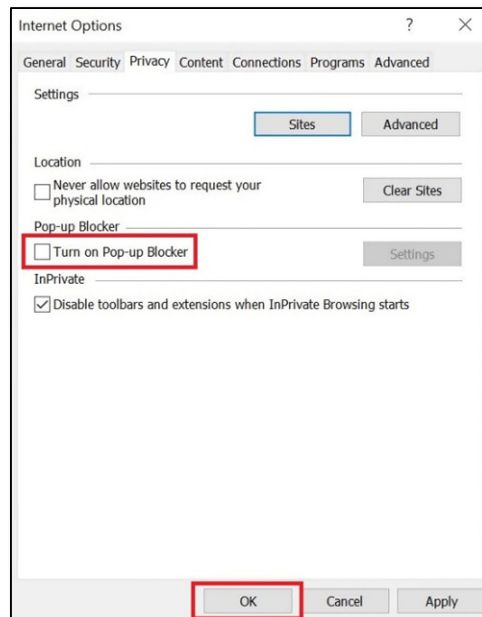
[Back to Table of Contents](#)

### 3.6 Disable Pop-Up Blocker

**Issue:** A user enters their username and password and is prompted to enter their OTP but has not received it. Allow for a reasonable amount of time (a few minutes) for messaging and email clients to deliver the OTP notification.

**Resolution:** Disable the pop-up blocker of the internet browser being utilized. For Internet Explorer, select the “Tools” button and then select Internet options. On the Privacy tab, uncheck the “Turn on Pop-up Blocker” checkbox and select “OK.” If the OTP has still not been received after a few minutes, contact an Operations Administrator via [Ginnie Mae Customer Support](#) to reset the OTP email.

Figure 3.6-1 Disable Pop-Up Blocker

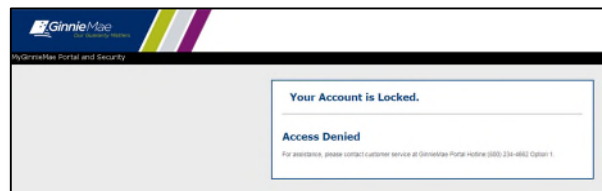


[Back to Table of Contents](#)

### 3.7 Account Locked

**Issue:** A user enters their username and password and receives an error message, “Your Account is Locked.”

Figure 3.7-1 Account Locked



**Resolution:** User should contact their Organization Administrator to request their account be unlocked.

[Back to Table of Contents](#)

### 3.8 MyGinnieMae Portal Profile Accounts tab: GMEP 1.0 or GinnieNET IDS are Unavailable

**Issue:** “Sorry, currently not available. Please try again later.” Error is displayed in MyGinnieMae Portal Profile Accounts tab under ‘GMEP 1.0’ and ‘GinnieNET’ ID section. The service for retrieving the GMEP 1.0 and GinnieNET accounts is temporarily unreachable, probably due to a network issue.

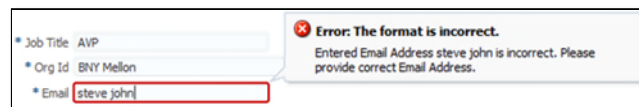
**Resolution:** There are automated alerts for the potential network issue, and it is likely that the issue is already being investigated. Contact an Operations Administrator via [Ginnie Mae Customer Support](#).

[Back to Table of Contents](#)

### 3.9 Registration Invitation Form Errors

**Issue:** If an incorrect email format has been entered in the Email field, the following validation message appears. The system is validating for the typical email format: sample@sample.sam.

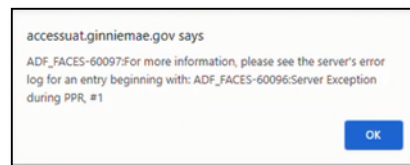
Figure 3.9-1 Registration Email Form Error



The screenshot shows a registration form with three fields: Job Title (AVP), Org Id (BNY Mellon), and Email (steve john). The Email field is highlighted with a red border. To the right of the form, a red error message box states: "Error: The format is incorrect. Entered Email Address steve john is incorrect. Please provide correct Email Address."

If a correct email format is then entered and the 'Submit' button is selected, the following error is displayed: "ADF\_FACES..."

Figure 3.9-2 Email Submit Error



The screenshot shows an error message box with the text: "accessuat.ginniemae.gov says ADF\_FACES-60097:For more information, please see the server's error log for an entry beginning with: ADF\_FACES-60096:Server Exception during PPR, #1". There is an "OK" button in the bottom right corner.

The registration page then displays the Error 500 shown below.

Figure 3.9-3 Registration Email Form Error



The screenshot shows an HTTP 500 Internal Server Error message. The text reads: "Error 500--Internal Server Error", "From RFC 2068 Hypertext Transfer Protocol -- HTTP/1.1:", "10.5.1 500 Internal Server Error", and "The server encountered an unexpected condition which prevented it from fulfilling the request."

**Resolution:** When an incorrect email format is entered and the "Error: The format is incorrect" appears, close the user registration form, and follow the steps to start a new registration invite. Do not proceed to populate the same registration.

[Back to Table of Contents](#)

## 4 RESOURCES

---

The Resources section provides information and resources to help navigate the MyGinnieMae portal application.

### 4.1 Organization Administrators

Organization Administrators, formerly known as Security Officers and Enrollment Administrators, are privileged users inside each Ginnie Mae business partner organization that are responsible for creating and managing End User accounts in Ginnie Mae systems on behalf of their organization. Organization Administrators are responsible for the following functions:

- Create an End User Account
- Update Account Attributes, including First/Middle/Last Name
- Reset Password
- Add/Remove Functional Roles for an End User Account
- Disable/Enable an End User Account
- Lock/Unlock an End User Account

End Users that need their One-Time PIN (OTP) reset or have questions about how to use portal applications should seek assistance from Ginnie Mae Customer Support.

[Back to Table of Contents](#)

### 4.2 Training Resources

For additional help, training sessions and materials can be found on the [Issuer Training Page](#) of the Ginnie Mae website at [https://www.ginniemae.gov/issuers/issuer\\_training/pages/modernization.aspx](https://www.ginniemae.gov/issuers/issuer_training/pages/modernization.aspx).

[Back to Table of Contents](#)

### 4.3 QRCs

A Quick Reference Card or QRC is an abbreviated one to two-page reference document with step-by-step instructions on how to complete a specific action. A list of QRCs for the content provided in this User Manual is available in the [Appendix](#). QRCs are posted to the Ginnie Mae website at [https://www.ginniemae.gov/issuers/issuer\\_training/pages/qrcs.aspx](https://www.ginniemae.gov/issuers/issuer_training/pages/qrcs.aspx).

[Back to Table of Contents](#)

## 4.4 Help Desk Contact Information

To contact Ginnie Mae Customer Support call 1-833-GNMA HELP (1-833-466-2435) or email at [ginniema1@bnymellon.com](mailto:ginniema1@bnymellon.com).

[Back to Table of Contents](#)

## 4.5 MyGinnieMae Portal Dictionary

The MyGinnieMae Portal Dictionary is a reference resource for all portal users. The dictionary contains definitions for terms that provide clarification around portal pages, applications, processes, and general functionality pertaining to the MyGinnieMae portal. Refer to the [MyGinnieMae Portal Dictionary](#).

[Back to Table of Contents](#)

## 4.6 MyGinnieMae Self Help Tools

Users should first reference the appropriate section of the MyGinnieMae Getting Started User Manual for information on creating a user account, requesting functional roles, and managing a user account. Some functions a user may complete without the assistance of a system administrator such as:

- Changing a password every 90 days – [Changing a Password in MyGinnieMae QRC](#)
- Resetting a forgotten password – [Forgot Password in MyGinnieMae QRC](#)
- Updating profile information – [Managing My Profile in MyGinnieMae QRC](#)
- Registering for mobile delivery of the OTP – [Registering with the Oracle Mobile Authenticator QRC](#)
- Troubleshooting Errors in MyGinnieMae – [Troubleshooting and Common Errors in MyGinnieMae QRC](#)

To get more help, users may access the training sessions and materials on the Issuer Training Page of the Ginnie Mae website at [https://www.ginniema.gov/issuers/issuer\\_training/pages/modernization.aspx](https://www.ginniema.gov/issuers/issuer_training/pages/modernization.aspx).

[Back to Table of Contents](#)

# 5 APPENDIX

## 5.1 MyGinnieMae Business Features

MyGinnieMae provides the following security and business features:

- Tailored, functional role-based landing pages called **My Dashboard**.
- One central access point to all Ginnie Mae business applications including **Single Sign-On (SSO)** to GMEP 1.0 and GinnieNET.

- **Marquee and Event Calendar** to communicate important announcements and events happening at Ginnie Mae.
- Enterprise **social** capabilities that promote collaboration and networking, including Discussion Forums, Messaging, RSS Feeds, Activity Feeds, and the collection of user feedback.
- **Search** Capabilities for MyGinnieMae content such as documents, people profiles, and discussion forums.
- **Productivity Widgets:**
  - *Notepad:* Create and manage personal notes. Notes are user specific.
  - *Task List:* Create and manage task lists and list items. Set reminders on the list items.
  - *Ginnie Mae Calendar of Events:* View and receive notifications on upcoming Ginnie Mae events.
- **Application Access Controls:** Utilizes Functional Roles to enforce Portal access security for all users and systems. MyGinnieMae provides a means to associate authenticated system users with applicable rights and privileges within the Portal and associated application programs.
- **Web-Based Self-Service Interface:** Provides self-service password management capabilities through a standard web-based interface.
- **Audit Support:** Provides relevant reports and email notifications for Ginnie Mae business users to enable transparency across the organization. For Organization Administrators, MyGinnieMae provides reports reflecting user access, workflow request/approval details, and account status.
- **Invitation Model:** Automates the user registration process through an invitation model. Registration must be completed before being granted access to the system.
- **Portal Capabilities:** Provides a central access point to all Ginnie Mae business applications including Single Sign-On (SSO) to GMEP 1.0 and GinnieNET. Includes communications via the Marquee, Event Calendar, and messaging from Ginnie Mae Account Executives, instructional materials, and notes and tasks/lists feature for capturing action items and/or reminders for Ginnie Mae business activities.
- **Multi-Factor Authentication via One-Time PIN (OTP):** Provides an additional level of security for access to Ginnie Mae business applications through a single use password received via email. Users also have the option to receive the OTP via Oracle Mobile Authenticator (OMA) app.

[Back to Table of Contents](#)

## 5.2 QRCs

Table 5-1 MGM Getting Started QRCs

User Manual	QRC#	QRC Name	Description
MyGinnieMae Getting Started	QRC-GS:3.1.1	Registering for an Account in MyGinnieMae	QRC with the steps to complete the MyGinnieMae portal registration form when a user receives the email invitation to register for an account.

User Manual	QRC#	QRC Name	Description
MyGinnieMae Getting Started	QRC-GS:3.2.2	Forgot Password in MyGinnieMae	QRC with the steps for using the Forgot Password link on the Login page of MyGinnieMae to create a new portal password when the user is unable to remember their password.
MyGinnieMae Getting Started	QRC-GS:3.2.3	Expired Password in MyGinnieMae	QRC with the steps to change the MyGinnieMae portal password when it has expired.
MyGinnieMae Getting Started	QRC-GS:3.2.4	Logging into MyGinnieMae After an Admin Resets a User's Password	QRC with the steps for logging into the MyGinnieMae portal using the temporary password that is sent via email when an Org Admin has reset a user's password.
MyGinnieMae Getting Started	QRC-GS:3.3.3	Registering with the Oracle Mobile Authenticator	QRC with the steps for users to register for Oracle Mobile Authenticator (OMA) so they can get the One-Time PIN (OTP) on their smart device.
MyGinnieMae Getting Started	QRC-GS:3.3.4	Deregistering with the Oracle Mobile Authenticator	QRC with the steps for deregistering a smart device with the Oracle Mobile Authenticator (OMA) so they can register a different smart device.
MyGinnieMae Getting Started	QRC-GS:3.4	Logging into MyGinnieMae & Accessing Business Applications	QRC with the steps for logging into the MyGinnieMae portal and for accessing business application using the tabs in My Dashboard or the Tools drop-down.
MyGinnieMae Getting Started	QRC-GS:3.4.2	Entering a One Time Pin (OTP) in MyGinnieMae	QRC with the steps for requesting a One-Time PIN (OTP) and entering the OTP on the Multi-Factor Authentication page when logging in to the MyGinnieMae portal.



User Manual	QRC#	QRC Name	Description
MyGinnieMae Getting Started	QRC-GS:3.5	Navigating the Dashboard in MyGinnieMae	QRC with the steps to access news, updates and activities on the Dashboard in MyGinnieMae.
MyGinnieMae Getting Started	QRC-GS:3.6.1	Changing a Password in MyGinnieMae	QRC with the steps to change a password in the MyGinnieMae portal.
MyGinnieMae Getting Started	QRC-GS:4.2.1	Selecting Organization IDs in MyGinnieMae	QRC that explains how Issuers and Subservicers with multiple Organization IDs can toggle between IDs to display data specific to each individual business entity.
MyGinnieMae Getting Started	QRC-GS:4.2.2	Confirming the Organization ID via GMEP 1.0	QRC with the steps to verify which Organization ID is being used once a user has chosen the Issuer or Custodian ID in the profile.
MyGinnieMae Getting Started	QRC-GS:4.2.3	Selecting Issuer or Subservicer ORG IDs via GinnieNET	QRC with the steps for Issuers and Subservicers with multiple Organization IDs to choose the appropriate Organization ID when accessing GinnieNET via the MyGinnieMae portal.
MyGinnieMae Getting Started	QRC-GS:4.2.4	Confirming Document Custodian ORG IDs via GinnieNET	QRC with the steps for Document Custodians to confirm they have chosen the appropriate Organization ID in GinnieNET.
MyGinnieMae Getting Started	QRC-GS:4.3	Managing My Profile in MyGinnieMae	QRC with the steps a user would follow to manage their profile in MyGinnieMae such as updating contact details, profile photo and other information.
MyGinnieMae Getting Started	QRC-GS:4.4	Troubleshooting and Common Errors in MyGinnieMae	QRC that explains common error messages a MyGinnieMae user may encounter and the steps to troubleshoot and resolve the issues.

User Manual	QRC#	QRC Name	Description
MyGinnieMae Getting Started	QRC-GS:4.6	Exiting MyGinnieMae	QRC that explains the two ways to exit the MyGinnieMae portal and the proper way to exit all open sessions.
MyGinnieMae Getting Started	QRC-RSA:1.0	How to Install and Authenticate Soft Token - Desktop	QRC with the steps to install an RSA SecurID Soft Token on a desktop computer.
MyGinnieMae Getting Started	QRC-RSA:2.0	How to Install and Authenticate Soft Token - Mobile	QRC with the steps to install an RSA SecurID Soft Token on a mobile device.
MyGinnieMae Getting Started	QRC-RSA:3.0	How to use a Soft Token in MyGinnieMae	QRC with the steps to use an RSA SecurID Soft Token when prompted for RSA validation.
MyGinnieMae Getting Started	QRC-RSA:3.0	Video - How to use a Soft Token in MyGinnieMae	Video that demonstrates the steps for using an RSA SecurID Soft Token when prompted for RSA validation.
MyGinnieMae Getting Started	QRC-RSA:4.0	Requesting a Replacement Token Via Self-Service	QRC with the steps to generate a new soft token via self-service if the token holder is transferring the device installed or has a new device

[Back to Table of Contents](#)

## 5.3 Figures

Figure 1.2-1 MyGinnieMae Onboarding Workflow .....	8
Figure 2.1-1 Compatibility View Settings.....	9
Figure 2.1-2 Use TLS 1.2.....	10
Figure 2.1-3 Download File .....	11
Figure 2.3-1 MyGinnieMae Registration Email.....	13
Figure 2.3-2 New User Registration.....	14
Figure 2.3-3 Rules of Behavior .....	14

Figure 2.3-4 Privacy Policy .....	15
Figure 2.3-5 New User Registration Form - Completed.....	15
Figure 2.3-6 Registration Request Complete.....	15
Figure 2.3-7 Welcome Email .....	16
Figure 2.3-8 New Functional Role Assignment Email .....	16
Figure 2.5-1 Multi-Factor Authentication Page .....	18
Figure 2.5-2 The Oracle Mobile Authenticator Icon .....	18
Figure 2.5-3 (Left) Oracle Mobile Authenticator (OMA) no prior accounts (Center) OMA List View (Right) OMA Grid View .....	19
Figure 2.5-4 OMA Instructions with QR Code.....	19
Figure 2.5-5 Oracle Mobile Authenticator Login .....	20
Figure 2.5-6 Oracle Mobile Authenticator Error for Already Registered Accounts.....	20
Figure 2.5-7 Multi-Factor Authentication Page - Choose Preferred OTP Method .....	21
Figure 2.5-8 Disabled User / Invalid Credentials Error .....	21
Figure 2.5-9 Edit My Profile .....	21
Figure 2.5-10 User's Profile Account Tab.....	22
Figure 2.6-1 Toggle View .....	24
Figure 2.6-2 Manage Profile .....	25
Figure 2.6-3 Associated Accounts.....	26
Figure 2.7-1 Edit User's Profile .....	27
Figure 2.7-2 Change Security Settings .....	27
Figure 2.7-3 Password Change Notice .....	27
Figure 2.7-4 Password Change Notice .....	28
Figure 2.7-5 Disabled User Username Prompt - Error .....	28
Figure 2.7-6 Change Password Page.....	29
Figure 2.7-7 Successful Password Change Message.....	29
Figure 2.7-8 Change Password Confirmation Email .....	29
Figure 2.7-9 Login Page.....	30
Figure 2.7-10 Forgot Password Username Prompt - Error .....	30
Figure 2.7-11 Disabled User Username Prompt - Error .....	31

Figure 2.7-12 Forgot Password Username Prompt .....	31
Figure 2.7-13 OTP via Email Delivery .....	31
Figure 2.7-14 Reset Password Page .....	32
Figure 2.7-15 Successful Password Change Message .....	32
Figure 2.7-16 Redirect to Login Page .....	33
Figure 2.7-17 Password Change Confirmation Email .....	33
Figure 2.7-18 Login Page .....	34
Figure 2.7-19 OTP Page .....	34
Figure 2.7-20 Enter New Password Page .....	34
Figure 2.7-21 Successful Password Change Message .....	35
Figure 2.7-22 Redirect to Login Page .....	35
Figure 2.7-23 Password Change Confirmation Email .....	35
Figure 2.7-24 Temporary Password Email .....	36
Figure 2.7-25 Login Page .....	36
Figure 2.7-26 OTP Page .....	36
Figure 2.7-27 OTP Page .....	37
Figure 2.7-28 Enter New Password Page .....	37
Figure 2.7-29 Successful Password Change Message .....	37
Figure 2.7-30 Password Change Confirmation Email .....	38
Figure 2.8-1 Public Landing Page .....	38
Figure 2.8-2 Login Page .....	39
Figure 2.8-3 Incorrect Username/Password Error .....	39
Figure 2.8-4 (Above) One-Time PIN (OTP) through email / (RIGHT) OTP from Oracle Mobile Authenticator (OMA) .....	40
Figure 2.8-5 System Error Message .....	40
Figure 2.8-6 My Dashboard .....	41
Figure 2.9-1 Logout Lock Icon .....	42
Figure 2.9-2 Portal Logout .....	42
Figure 2.9-3 Portal Session Timeout Timer .....	42
Figure 2.10-1 Accessing a Business Application .....	43
Figure 2.10-2 Marquee .....	44

Figure 2.10-3 My Dashboard .....	44
Figure 2.10-4 Bookmarks .....	45
Figure 2.10-5 Industry News .....	46
Figure 2.10-6 Messages .....	46
Figure 2.11-1 Commitment Authority Details .....	47
Figure 2.11-2 Pool Number Details.....	48
Figure 2.11-3 IOPP Scorecard .....	48
Figure 2.12-1 Leadership Blog .....	49
Figure 2.13-1 Knowledge Center .....	50
Figure 2.14-1 Portal Search.....	50
Figure 2.14-2 Search Results.....	51
Figure 2.16-1 Edit My Profile .....	52
Figure 2.16-2 User's Profile Account Tab.....	52
Figure 2.16-3 Password Change Notice .....	53
Figure 2.16-4 Password Change Notice .....	53
Figure 2.16-5 Disabled User Username Prompt - Error .....	53
Figure 2.16-6 Change Password Page.....	54
Figure 2.16-7 Select Device.....	54
Figure 2.16-8 RSA Soft Token QR Code.....	55
Figure 2.16-9 Select Device.....	55
Figure 2.16-10 Reissue Ginnie Mae Soft Token Email .....	55
Figure 3.1-1 System Error Message .....	56
Figure 3.2-1 New Password Does Not Match Error .....	56
Figure 3.3-1 Invalid Password Error .....	57
Figure 3.4-1 Incorrect OTP Error.....	58
Figure 3.6-1 Disable Pop-Up Blocker .....	59
Figure 3.7-1 Account Locked .....	59
Figure 3.9-1 Registration Email Form Error .....	60
Figure 3.9-2 Email Submit Error.....	60
Figure 3.9-3 Registration Email Form Error .....	60

**5.4 Tables**

Table 6-1 MGM Getting Started QRCs..... 63