

MyGinnieMae Portal - Getting Started Manual

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

Ginnie Mae, Office of Securities Operations (OSO)

V2.2



Application Details

Application Information	Description
Application Name	MyGinnieMae
Application Acronym	MGM
Application Developer	BNYM
Application Approver	(TBD)
Submission Date	
Ginnie Mae SVP, Owner	John Daugherty, SVP OSO
Ginnie Mae Director, Approver	Stewart Spettel, Director Operations
Approval Date	
Version/Release Number	2.2

Document History

Version	Date	Author	Entity	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

TABLE OF CONTENTS

1	INTRODUCTION TO MYGINNIEMAE	10
1.1	Portal Overview	10
1.2	Security Protocols	11
1.2.1	Multi-Factor Authentication	11
1.2.2	New Enterprise ID and Single Sign-On	11
1.2.3	Using SecurID Token within Applications	12
1.2.4	Automatic Logout	12
1.2.5	Overview of Self-Service Functionalities	12
1.2.6	Authorized Use / Permission	12
2	SYSTEM PREREQUISITES	14
2.1	Compatibility Settings	14
2.1.1	Support TLS 1.2	15
2.1.2	Accessing Video Files	15
2.2	Prerequisites to Accessing MyGinnieMae Portal	16
2.3	Functional Roles	16
2.4	Contingencies and Alternate Modes of Operation	20
3	GETTING STARTED	21
3.1	Creating a User Account	21
3.2	Registration Email Invitation	22
3.2.1	Required User Information	22
3.2.2	Expiration of Email Invitation	25
3.2.3	Invitation Limits	25
3.3	Requesting Functional Roles for My User Account	25
3.4	Accessing the One-Time PIN (OTP) via Smart Device	26
3.4.1	Register with the Oracle Mobile Authenticator	26
3.4.2	De-register with the Oracle Mobile Authenticator	29
3.5	Managing Your MyGinnieMae Account	31
3.5.1	Profile Management	31

3.5.2	Issuer ID	31
3.5.3	Edit Profile.....	32
3.5.4	Associated Accounts.....	32
3.6	Resetting Passwords	33
3.6.1	Change Password	33
3.6.2	Forgotten Password	35
3.6.3	Expired Password.....	38
3.6.4	Logging In After an Admin Reset a User’s Password.....	40
3.7	Logging into MyGinnieMae	42
3.7.1	Entering a Username and Password	42
3.7.2	Choosing and Entering a One-Time PIN (OTP)	43
3.7.3	Logging In After an Admin has Enabled User’s Account.....	45
3.8	Exiting	46
3.8.1	Manually Exiting MyGinnieMae.....	46
3.8.2	Automatic Logout.....	46
3.9	Navigating the Portal	47
3.9.1	Accessing Business Applications	47
3.9.2	Marquee	48
3.9.3	My Dashboard	48
3.9.4	Bookmarks	49
3.9.5	Industry News.....	49
3.9.6	Messages.....	49
3.10	Dashboard Components/Widgets.....	50
3.10.1	Commitment Authority Dashboard Chart	50
3.10.2	Pool Numbers Dashboard Chart.....	51
3.10.3	Issuer Operational Performance Profile (IOPP) Scorecard	51
3.11	Communities.....	52
3.11.1	Leadership Blog.....	52
3.11.2	Discussion Forums.....	52
3.12	Knowledge Center	53

3.13	Portal Search.....	53
3.14	Troubleshooting and System Errors	54
3.14.1	Basic Error Handling	54
3.14.2	New Password Mismatch Error.....	55
3.14.3	Invalid Username or Password	55
3.14.4	Incorrect OTP.....	55
3.14.5	OTP Not Received.....	56
3.14.6	Disable Pop-Up Blocker.....	56
3.14.7	Account Locked.....	57
3.14.8	MyGinnieMae Portal Profile Accounts tab: GMEP 1.0 or GinnieNET Account IDs are Unavailable	57
3.14.9	Registration Invitation Form Errors	57
4	APPLICATIONS.....	59
4.1	Access Management Console (AMC)	59
4.2	Platinum Pool Processing.....	59
4.3	Multifamily Pool Delivery Module (MFPDM)	59
4.4	GinnieNET.....	59
4.5	RFS - Reporting and Feedback System	59
5	GETTING HELP	60
5.1	Self-Help Tools	60
5.2	Organization Administrators	60
5.3	Ginnie Mae Customer Support	61
5.3.1	Customer Support Help with System Access	61
5.3.2	Customer Support Help with Portal Applications.....	61
6	APPENDIX.....	62
6.1	Key Features	62
6.2	Functional Roles	63
6.2.1	Single-Family Issuer Functional Roles	63
6.2.2	Multifamily Issuer Functional Roles	65
6.2.3	HECM Issuer Functional Roles.....	67

6.2.4	Subservicer Functional Roles	70
6.2.5	Document Custodian Functional Roles	72
6.2.6	Depositor Functional Roles	73
6.3	MyGinnieMae Portal Dictionary	73
7	QUICK REFERENCE CARDS	74
7.1	Registering for an Account in MyGinnieMae QRC	74
7.2	Logging into MyGinnieMae QRC	76
7.3	Changing a Password in MyGinnieMae QRC	78
7.4	Forgot Password in MyGinnieMae QRC	79

LIST OF FIGURES

Figure 1	Portal Session Timeout Timer	12
Figure 2	Compatibility View Settings	14
Figure 3	Use TLS 1.2	15
Figure 4	Download File	15
Figure 5	MyGinnieMae Onboarding Workflow	21
Figure 6	MyGinnieMae Registration Email	22
Figure 7	New User Registration	22
Figure 8	Rules of Behavior	23
Figure 9	Privacy Policy	23
Figure 10	New User Registration Form – Completed	24
Figure 11	Registration Request Complete	24
Figure 12	Welcome Email	25
Figure 13	New Functional Role Assignment Email	25
Figure 14	Multi-Factor Authentication Page	26
Figure 15	The Oracle Mobile Authenticator Icon	26
Figure 16	(Left) Oracle Mobile Authenticator (OMA) no prior accounts (Center) OMA List View (Right) OMA Grid View	27
Figure 17	OMA Instructions with QR Code	27
Figure 18	Oracle Mobile Authenticator Login	28
Figure 19	Oracle Mobile Authenticator Error for Already Registered Accounts	28

Figure 20 Multi-Factor Authentication Page - Choose Preferred OTP Method	28
Figure 21 Disabled User / Invalid Credentials Error.....	29
Figure 22 Edit My Profile	29
Figure 23 User's Profile Account Tab.....	30
Figure 24 Change Password Page	30
Figure 25 De-registration Confirmation Window	30
Figure 26 Successful De-registration Message	31
Figure 27 Toggle View.....	31
Figure 28 Manage Profile.....	32
Figure 29 Associated Accounts	32
Figure 30 Edit User's Profile.....	33
Figure 31 Change Security Settings	34
Figure 32 Change Password Page	34
Figure 33 Successful Password Change Message	34
Figure 34 Change Password Confirmation Email.....	35
Figure 35 Login Page.....	35
Figure 36 Forgot Password Username Prompt.....	36
Figure 37 Forgot Password Username Prompt – Error.....	36
Figure 38 Disabled User Username Prompt – Error	36
Figure 39 Reset Password Page	37
Figure 40 Successful Password Change Message	37
Figure 41 Redirect to Login Page	37
Figure 42 Password Change Confirmation Email.....	38
Figure 43 Login Page	38
Figure 44 Enter New Password Page	39
Figure 45 Successful Password Change Message	39
Figure 46 Redirect to Login Page	39
Figure 47 Password Change Confirmation Email.....	40
Figure 48 Temporary Password Email	40
Figure 49 Login Page.....	40
Figure 50 Enter New Password Page	41

Figure 51 Successful Password Change Message	41
Figure 52 Password Change Confirmation Email.....	42
Figure 53 Public Landing Page	42
Figure 54 Login Page.....	43
Figure 55 Incorrect Username/Password Error.....	43
Figure 56 Multi-Factor Authentication Page	44
Figure 57 (Above) One-Time PIN (OTP) through Email / (Right) OTP from Oracle Mobile Authenticator (OMA)	44
Figure 58 System Error Message	45
Figure 59 My Dashboard.....	45
Figure 60 Logout Lock Icon	46
Figure 61 Portal Logout	46
Figure 62 Portal Session Timeout Timer	47
Figure 63 Accessing a Business Application.....	47
Figure 64 Marquee	48
Figure 65 My Dashboard.....	48
Figure 66 Bookmarks	49
Figure 67 Industry News	49
Figure 68 Messages	50
Figure 69 Commitment Authority Details.....	50
Figure 70 Pool Number Details.....	51
Figure 71 IOPP Scorecard.....	52
Figure 72 Leadership Blog.....	52
Figure 73 Knowledge Center.....	53
Figure 74 Portal Search.....	53
Figure 75 Search Results.....	54
Figure 76 System Error Message	54
Figure 77 New Password Does Not Match Error	55
Figure 78 Invalid Password Error	55
Figure 79 Incorrect OTP Error	56
Figure 80 Disable Pop-up Blocker	57
Figure 81 Account Locked.....	57

Figure 82 Registration Email Form Error	58
Figure 83 Email Submit Error	58
Figure 84 Registration Email Form Error	58

LIST OF TABLES

Table 1 MyGinnieMae Responsibilities.....	13
Table 2 Single-Family Functional Roles Summary	17
Table 3 Multifamily Functional Roles Summary	18
Table 4 HECM Functional Roles Summary.....	19
Table 5 Subservicer Functional Roles Summary	20
Table 6 Document Custodian Functional Roles Summary.....	20
Table 9 Multifamily Issuer Roles Access	66
Table 10 HECM Roles Access	69
Table 12 Document Custodian Roles Access	72
Table 13 Depositor Roles Access	73

1 INTRODUCTION TO MYGINNIEMAE

Ginnie Mae is modernizing its Securitization Platform technology, processes, and related policies in response to the growing need for increased transparency and improved service delivery to its Issuers and Investors. Ginnie Mae has already successfully developed a single gateway to Ginnie Mae's systems, applications, and resources through a Portal called MyGinnieMae. MyGinnieMae will eventually replace the Ginnie Mae Enterprise Portal—more commonly known as GMEP 1.0—and will serve as a primary platform for extending information technology capabilities to the Ginnie Mae community. MyGinnieMae delivers features that specifically address the business constraints, security concerns, and compliance issues that hinder GMEP 1.0 today.

MyGinnieMae provides security controls that adhere to the Federal Information Security Management Act of 2002 (FISMA) and Federal Identity, Credential, and Access Management (FICAM) implementation guidance. It serves as the centralized security control for Ginnie Mae portals and applications, as well as providing identity management for its users. It also provides users with an industry-standard secure method for access to client portals and integrated applications.

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

Among the benefits provided to Ginnie Mae stakeholders are:

- Improved cyber security operations by reduced reliance on basic username and password, thus aligning more closely to Federal Identity, Credentials, and Access Management (FICAM) and The National Institute of Standards and Technology (NIST) compliant Single Sign-On and multi-factor authentication schemes.
- Reduced technology operational expenses by a fully automated new user registration process and user self-service capabilities like password reset, application access requests, and delegated account administration.
- Improved technology governance and compliance capabilities such as automated role management, Segregation of Duties (SoD) monitoring, and centralized audit reports.

1.1 Portal Overview

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.

1.2 Security Protocols

1.2.1 Multi-Factor Authentication

MyGinnieMae requires a strong authentication system to meet FFIEC (Federal Financial Institutions Examination Council) and FISMA requirements. MyGinnieMae ensures that the appropriate security controls and context are established prior to conducting business. This approach allows Ginnie Mae to maintain an access management system that complies with Federal guidelines and security controls that align with leading industry security capabilities to reduce fraud, replay attacks, and phishing. MyGinnieMae is designed and configured to enable strong authentication through its Multi-Factor Authentication (MFA) service.

When accessing secured applications and information in the Portal, a single use password called a One-Time PIN (OTP) provides an added level of security. This can be an eight-digit code, valid for 10 minutes that is sent to the user's email address or it six-digit code, valid for 30 seconds that is received on the user's smart device via the Oracle Mobile Authenticator (OMA) app. Users are required to enter the OTP each time they login.

1.2.2 New Enterprise ID and Single Sign-On

MyGinnieMae is accessed via a single enterprise ID or username. This new enterprise ID is the user's corporate email address, which must be unique, and serves as the login for personalized credentials set up during registration. Once the account has been granted access to various applications, Single Sign-On (SSO) provides secure and seamless navigation to those applications without the need to maintain and re-enter credentials for multiple GMEP 1.0 accounts or GinnieNET.


1.2.3 Using SecurID Token within Applications

There is no change to the usage of SecurID authentication practices for transaction submissions. After a user's account has been created in MyGinnieMae and access is provisioned, their new MyGinnieMae enterprise ID (corporate email account) and associated GMEP 1.0 accounts are associated to their existing SecurID Token.

1.2.4 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 on 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.

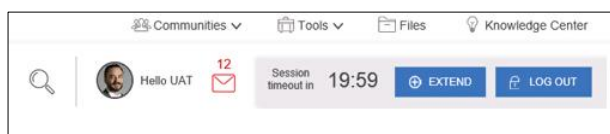


Figure 1 Portal Session Timeout Timer

NOTE: For security reasons, always log out after finishing a session and before closing the browser. Select the “Log Out” button to log out of the session.

1.2.5 Overview of Self-Service Functionalities

The following self-service functionalities are included for accurate and efficient management of user account information and security:

- Managing user profile information;
- Changing passwords; and
- Resetting expired or forgotten passwords.

1.2.6 Authorized Use / Permission

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 [Section: Creating a User Account](#) for more information on the user registration process.

The following table lists the various administrative user types and the responsibility/description for each user type within MyGinnieMae. As noted above, each organization must maintain at least two Organization Administrators.

User Type	Responsibility / Description
Operations Administrator (Ops Admin)	Operations Administrators have general oversight of the Portal. They can only provide final acknowledgement of access requests and cannot make any changes to end user accounts. Refer to Section: Getting Help for more information on the role of Operations Administrators.
Organization Administrator (Org Admin)	<p>Organization Administrators have the privilege to invite end users to register for a Portal account, approve user registration, initiate access request via Functional Role assignments to users, and approve the access request within a single organization.</p> <p>NOTE: Separation of duties within the registration and access request workflows do not allow the Organization Administrator to initiate a registration and approve that same registration or request access via Functional Role assignment and approve that same access request. A minimum of two Organization Administrators is therefore required. From an operational perspective, it is recommended that an organization have more than the minimum of two Organization Administrators.</p>
End User	End Users are Ginnie Mae employees, business partners, and contractors who require access to the business applications and information within the Portal, including various self-service functions.

Table 1 MyGinnieMae Responsibilities

2 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](#). In order 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.

2.1 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, GMPE 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.

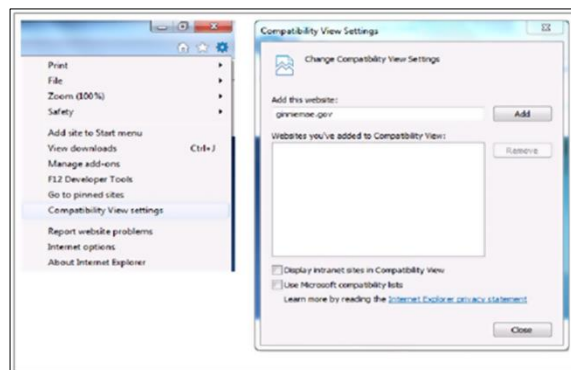


Figure 2 Compatibility View Settings

2.1.1 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.

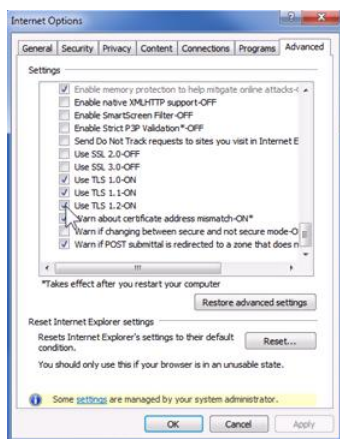


Figure 3 Use TLS 1.2

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.

2.1.2 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.

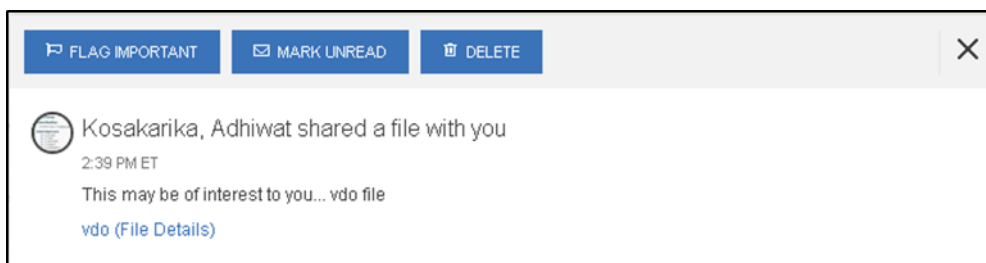


Figure 4 Download File

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.

2.2 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 [Section: Creating a User Account](#) for more information on the user registration process.

2.3 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/de-provisioning actions easier for Organization Administrators. These roles are grouped and vary by type (Single-Family, Multifamily, HECM, etc.) as summarized in the Functional Roles tables below. For more detail, refer to [Section: Functional Roles](#).

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

Functional Role Name	Functional Role Description
SF-Post-Closing User	Access to review collateral, obtain loan insurance, forward initial and trailing documents to a Document Custodian.
SF-Loan Delivery and Pooling Basic User	Upload/enter pool and loan information for delivery; verify availability of Commitment Authority; clear document deficiencies and pooling exceptions; access to prepare but not execute PIIT/TAI transactions.

Functional Role Name	Functional Role Description
SF-Loan Delivery and Pooling Authorized Signer	Only for HUD 11702 signatories. All rights of a Loan Delivery and Pooling Basic User, plus authority to submit pools for issuance and request additional Commitment Authority and execute PIIT/TAI transactions.
SF-Investor Reporting Basic User	Submit monthly pool and loan level accounting data; submit quarterly custodial account verification data; review monthly remittance information; review monthly reporting exception feedback and errors.
SF-Investor Reporting Authorized Signer	Only for HUD 11702 signatories. All rights of an Investor Reporting Basic User, plus authority to certify the monthly pool and loan accounting report and submit edits needed to clear exception feedback and monthly reporting errors.
SF-Compliance and Oversight User	Review portfolio servicing and investor reporting metrics and reports; oversee subservicer performance when applicable.
SF-Bulk Transfers Authorized Signer	Initiate, manage, and accept bulk transfer transactions; initiate and coordinate transfers of collateral files with transferee and transferor Issuers or Document Custodians.
SF-Collateral Management Authorized Signer	Process releases of collateral from the Document Custodian in accordance with servicing obligations (HUD-11708 Releases).
SF-Agency Relationship User	Access reports containing portfolio performance and liquidity metrics; receive targeted Ginnie Mae communications for individuals responsible for managing agency relationships.
SF-Processing Master Agreements Authorized Signer	Only for HUD 11702 signatories. Edit, submit, and certify Master Agreement documents and data required by Ginnie Mae.
SF-Financial Statements User	Submit annual audited financial statements for review by Ginnie Mae's IPA.
SF-Special Loans User	Upload and process SCRA reimbursement requests.

Table 2 Single-Family Functional Roles Summary

Functional Role Name	Functional Role Description
MF-Loan Delivery and Pooling Basic User	Upload/enter pool and loan information for delivery; verify availability of Commitment Authority; clear document deficiencies and pooling exceptions; access to prepare but not execute PIIT/TAI transactions.
MF-Loan Delivery and Pooling Authorized Signer	Only for HUD 11702 signatories. All rights of a Loan Delivery and Pooling Basic User, plus authority to submit pools for issuance and request additional Commitment Authority and execute PIIT/TAI transactions.

Functional Role Name	Functional Role Description
MF-Investor Reporting Basic User	Submit monthly pool and loan level accounting data; submit quarterly custodial account verification data; review monthly remittance information, review monthly reporting exception feedback and errors.
MF-Investor Reporting Authorized Signer	Only for HUD 11702 signatories. All rights of an Investor Reporting Basic User, plus authority to certify the monthly pool and loan accounting report and submit edits needed to clear exception feedback and monthly reporting errors.
MF-Compliance and Oversight User	Review portfolio servicing and investor reporting metrics and reports; oversee subservicer performance when applicable.
MF-Master Agreements Authorized Signer	Only for HUD 11702 signatories. Edit, submit, and certify Master Agreement documents and data required by Ginnie Mae.
MF-Financial Statements User	Submit annual audited financial statements for review by Ginnie Mae's IPA.
MF-Transfers Authorized Signer	Initiate, manage and accept bulk transfer transactions; Initiate and coordinate transfers of collateral files with transferee and transferor Issuers or Document Custodians.

Table 3 Multifamily Functional Roles Summary

Functional Role Name	Functional Role Description
HECM-Post-Closing User	Access to review collateral, obtain loan insurance, forward initial and trailing documents to a Document Custodian.
HECM-Loan Delivery and Pooling Basic User	Upload/enter pool, loan, and participation data into GinnieNET; verify available Commitment Authority and clear document and/or GinnieNET pooling exceptions. Basic user cannot finalize transactions or submissions.
HECM-Loan Delivery and Authorized Signer	Upload/enter pool, loan, and participation data into GinnieNET; verify available Commitment Authority and clear document and/or GinnieNET pooling exceptions. Authority to finalize or execute business transactions with Ginnie Mae (HUD-11702 Signers), including the authority submit requests for additional commitment authority as needed and to submit pools for issuance.
HECM-Investor Reporting Basic User	Submit the monthly pool, loan, and participation data; submit the custodial account verification data; review monthly remittance information and reporting exception feedback and errors. Ability to track loans approaching 98% of MCA (Maximum Claim Amount) to identify if loans need to be bought out, and coordinate participation agent for assurance that all participations in other pools are bought out accordingly.

Functional Role Name	Functional Role Description
HECM-Investor Reporting Authorized Signer	Submit the monthly pool, loan, and participation data; submit the custodial account verification data; review monthly remittance information and reporting exception feedback and errors. Ability to track loans approaching 98% of MCA (Maximum Claim Amount) to identify if loans need to be bought out, and coordinate participation agent for assurance that all participations in other pools are bought out accordingly. Including the authority to submit requests for additional commitment authority as needed and to submit pools for issuance.
HECM-Compliance and Oversight User	Review portfolio servicing and investor reporting metrics and reports; oversee subservicer performance when applicable.
HECM-Bulk Transfers Authorized Signer	Initiate, manage and accept bulk transfer transactions; initiate and coordinate transfers of collateral files with transferee and transferor Issuers or Document Custodians.
HECM-Collateral Management Authorized Signer	Process releases of collateral from the Document Custodian in accordance with servicing obligations (HUD-11708 Releases).
HECM-Agency Relationship User	Access reports containing portfolio performance and liquidity metrics; receive targeted Ginnie Mae communications for individual responsible for managing agency relationships.
HECM-Processing Master Agreements Authorized Signer	Only for HUD 11702 signatories. Edit, submit, and certify Master Agreement documents and data required by Ginnie Mae.
HECM-Financial Statements User	Submit annual audited financial statements for review by Ginnie Mae's IPA.
HECM-Special Loans User	Upload and process SCRA reimbursement requests.
HECM-Participation Agent	Third Party participation agent who performs all monitoring and accounting activities related to pooled Participations on behalf of a HECM Issuer.

Table 4 HECM Functional Roles Summary

Functional Role Name	Functional Role Description
SS-Investor Reporting Basic User	Submit monthly pool and loan level accounting data; submit quarterly custodial account verification data; review monthly remittance information, review monthly reporting exception feedback and errors.
SS-Investor Reporting Authorized Signer	Only for HUD 11702 signatories. All rights of an Investor Reporting Basic User, plus authority to certify the monthly pool and loan accounting report and submit edits needed to clear exception feedback and monthly reporting errors.

Functional Role Name	Functional Role Description
SS-Compliance and Oversight User	Review portfolio servicing and investor reporting metrics and reports; oversee subservicer performance when applicable.
SS-Special Loans User	Upload and process SCRA reimbursement requests.

Table 5 Subservicer Functional Roles Summary

Functional Role Name	Functional Role Description
DC-Pool Certification Basic User	View Schedule of Pooled Mortgages submitted; review pool and loan files for compliance with Ginnie Mae pool certification standards. Cannot certify pools or loan packages.
DC-Pool Certification and Collateral Release Management Authorized Signer	Only for HUD 11702 Signatories. All the rights of a Pool Certification Basic User, plus authority to submit initial certification, final certification, and recertification; authority to process releases of pool and/or loan files electronically via Ginnie Mae systems.
DC-Management and Oversight	Oversee document review and pool certification procedures; access and submit the Master Agreement documents and data as required by Ginnie Mae; serve as an Organization Administrator for My Ginnie Mae.
DC-Transfer Specialist	Monitor and manage pool transfer activities to ensure successful relocation of collateral files.

Table 6 Document Custodian Functional Roles Summary

2.4 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](#).

3 GETTING STARTED

The following sections include detailed information on the process for requesting a MyGinnieMae user account and functional roles to access business applications, as well as step-by-step instructions on how to log into the portal, navigate its security features, like One-Time PIN and manage your account, including changing and resetting your password.

3.1 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:

- The invitation has been sent to an end user’s organization business email address five or fewer times.
- The individual must be employed by an organization which has been on-boarded and authorized to do business with Ginnie Mae.
- The participant organization approves of their employee being granted access to Ginnie Mae’s systems.
- The participant organization approves the level of access requested for the user.
- 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 [Section: Platinum Pool Processing](#).

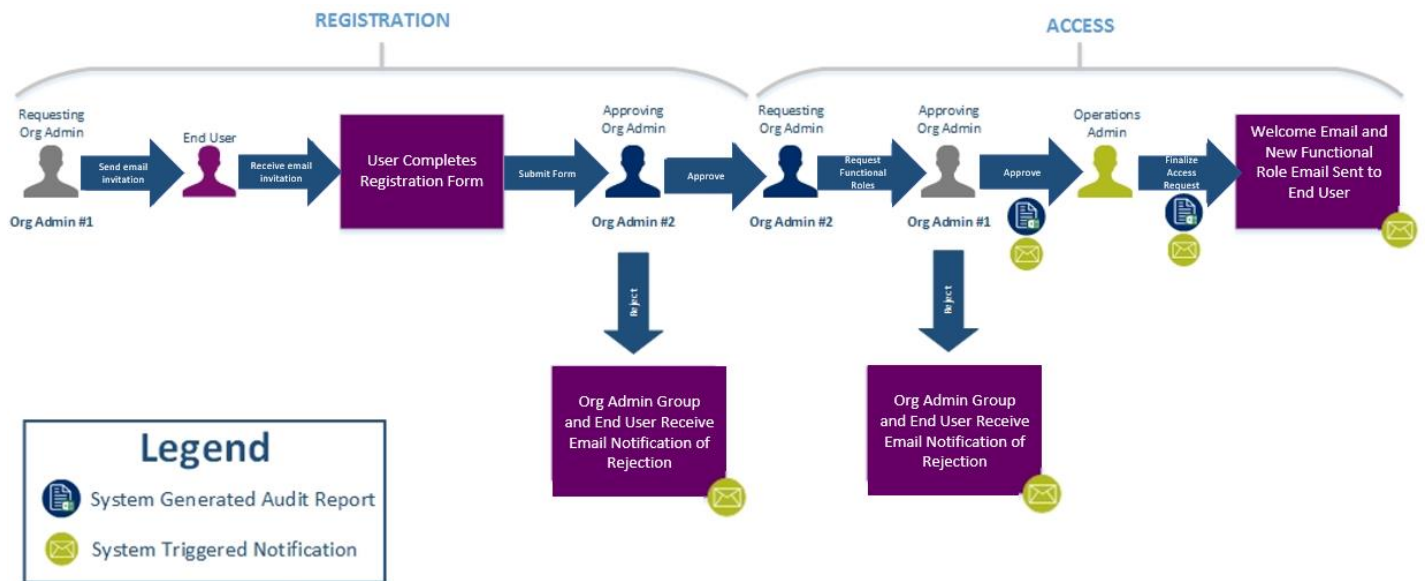


Figure 5 MyGinnieMae Onboarding Workflow

3.2 Registration Email Invitation

3.2.1 Required User Information

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

NOTE: The link is only active for 24 hours.

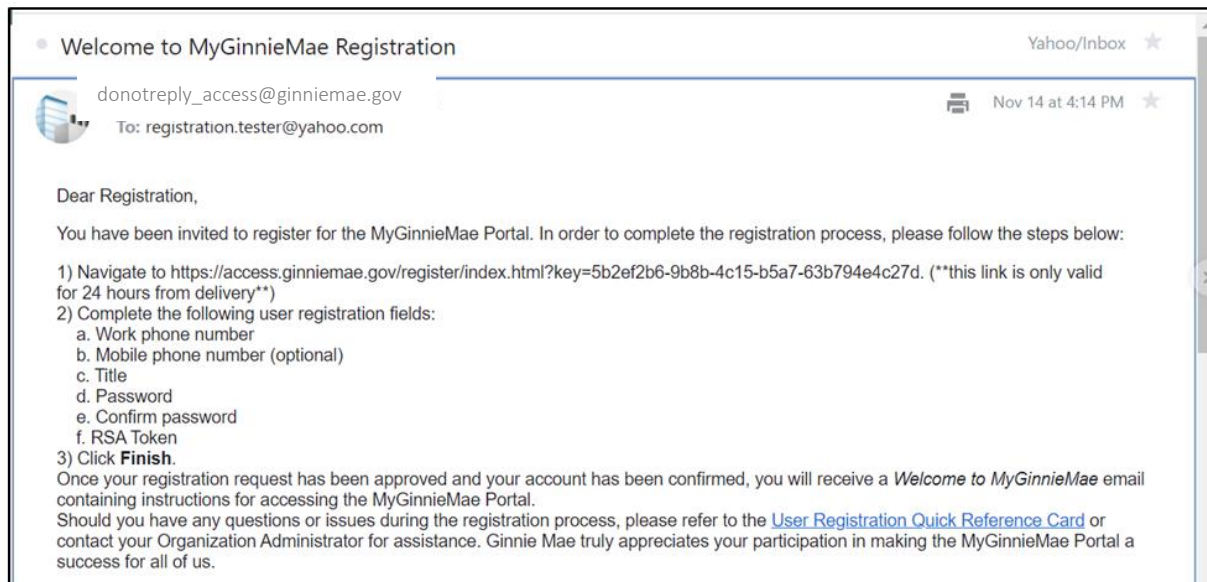


Figure 6 MyGinnieMae Registration Email

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)

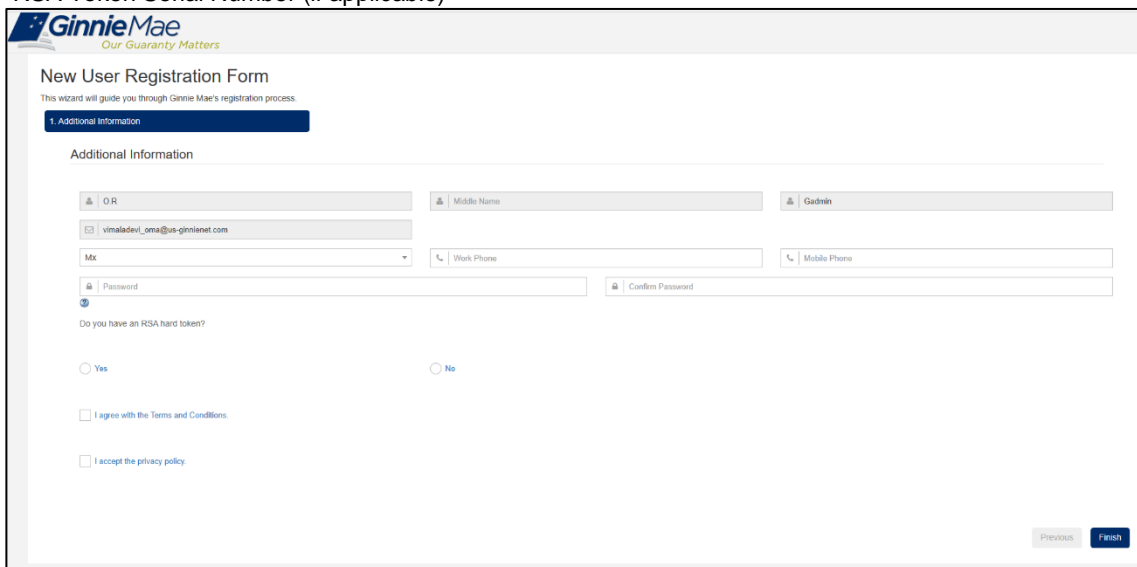
A screenshot of the "New User Registration Form" on the GinnieMae website. The form is titled "New User Registration Form" and includes a sub-header "1. Additional Information". The form fields include: "OR" (with a dropdown menu), "Middle Name", "Gadnin", "Email" (with the value vimaladevi_oma@us-ginnienet.com), "Mx" (with a dropdown menu), "Work Phone", "Mobile Phone", "Password", and "Confirm Password". There are also radio buttons for "Do you have an RSA hard token?" with options "Yes" and "No", and checkboxes for "I agree with the Terms and Conditions" and "I accept the privacy policy". At the bottom right, there are "Previous" and "Finish" buttons.

Figure 7 New User Registration

NOTE: Make sure the password meets the following password policy requirements:

- Must not match or contain the user's first name
- Must not match or contain the user's last name
- Must not be longer than 20 characters
- Must be at least 8 characters long
- Must contain at least 2 alphabetic character(s)
- Must contain at least 1 numeric character
- Must contain at least 3 alphanumeric character(s)
- Must contain at least 1 special character
- Must contain at least 1 uppercase letter
- Must contain at least 1 lowercase letter
- Must not match or contain user ID
- Must not be one of 24 previous passwords
- Any particular character in the password must not be repeated more than 2 time(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.

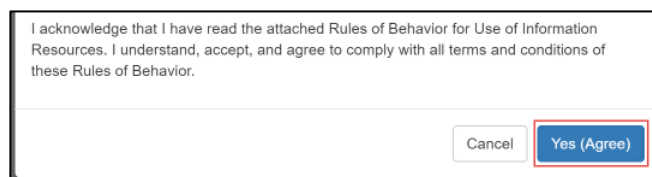


Figure 8 Rules of Behavior

4. Select the "I accept the privacy policy" link or checkbox.

- a. When the message box displays, select the "Ginnie Mae Privacy Policy" link
- b. Review the text and select **Yes**.



Figure 9 Privacy Policy

5. Once the Privacy Policy and Terms and Conditions have been accepted, select **Finish**.

Figure 10 New User Registration Form – Completed

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

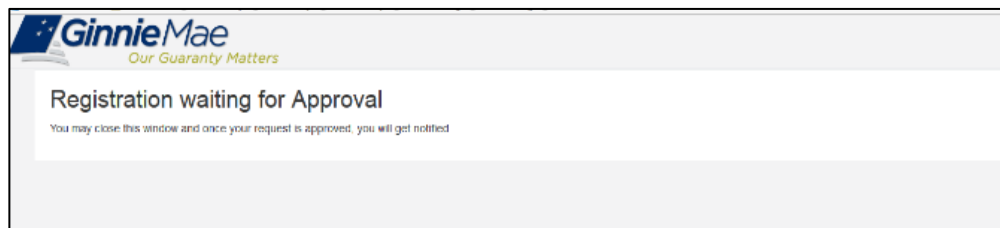


Figure 11 Registration Request Complete

- Once the request is approved and access is granted, both a Welcome Email and New Functional Role Assignment Email will be sent to the email address sent 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

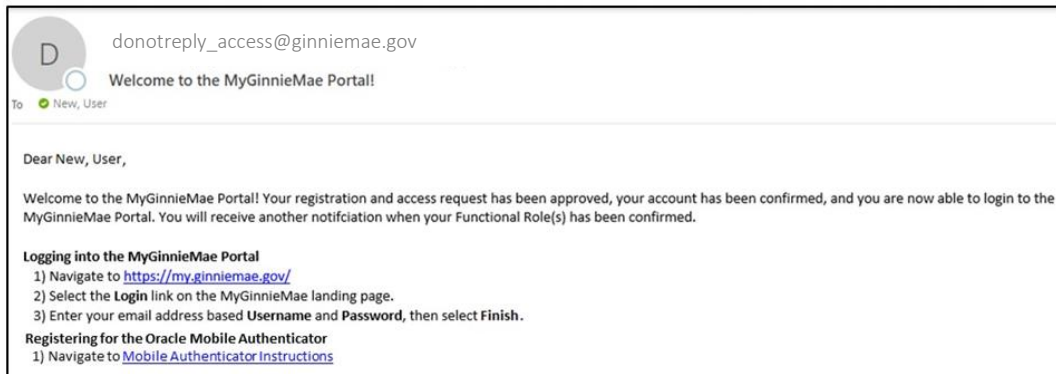


Figure 12 Welcome Email



Figure 13 New Functional Role Assignment Email

3.2.2 Expiration of Email Invitation

A registration link is active for only 24 hours. 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](#).

3.2.3 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](#).

3.3 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 [Appendix: Functional Roles](#). Contact the Organization Administrator to ensure access to the appropriate Functional Roles for the user's MyGinnieMae account.

3.4 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

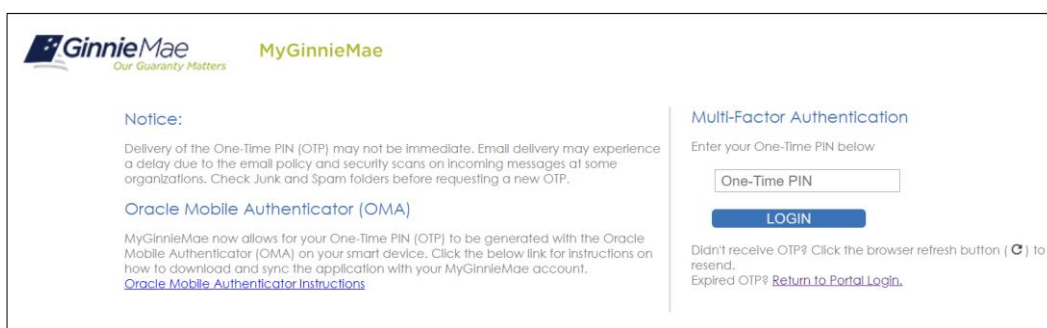


Figure 14 Multi-Factor Authentication Page

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>.

3.4.1 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 15 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.

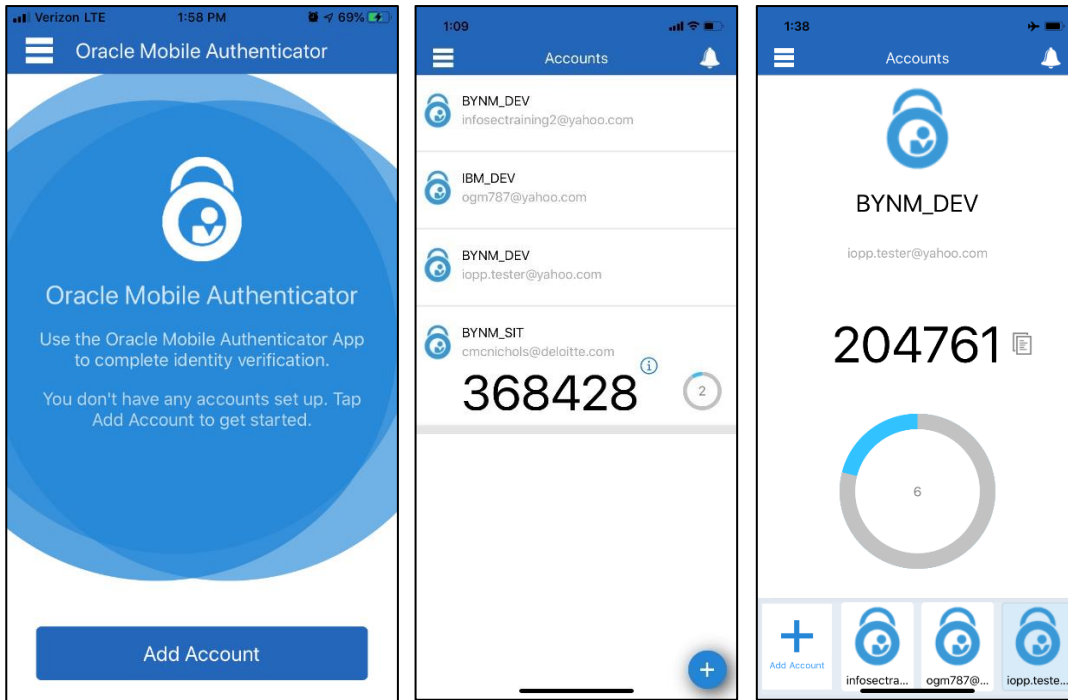


Figure 16 (Left) Oracle Mobile Authenticator (OMA) no prior accounts (Center) OMA List View (Right) OMA Grid View

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

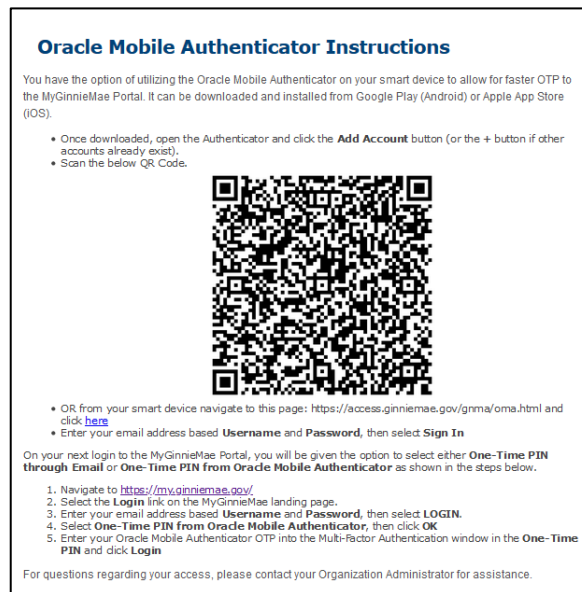


Figure 17 OMA Instructions with QR Code

- a. Use your MyGinnieMae credentials to, Enter your **Username**
- b. Enter **Password**

c. Select **Sign In**



Figure 18 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.

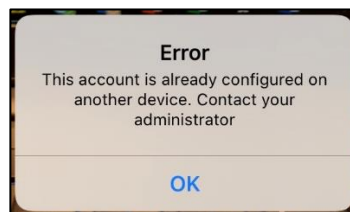


Figure 19 Oracle Mobile Authenticator Error for Already Registered Accounts

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:

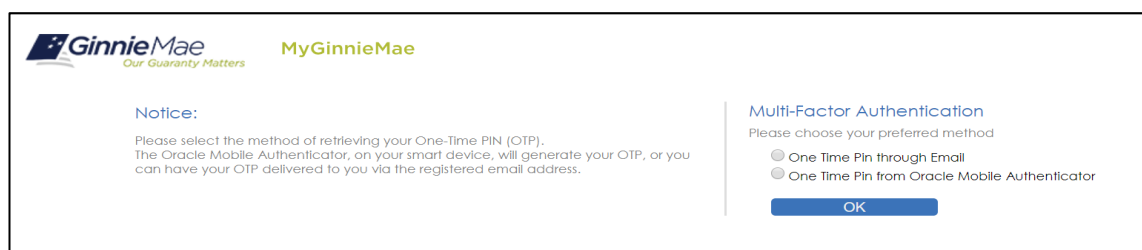


Figure 20 Multi-Factor Authentication Page - Choose Preferred OTP Method

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.

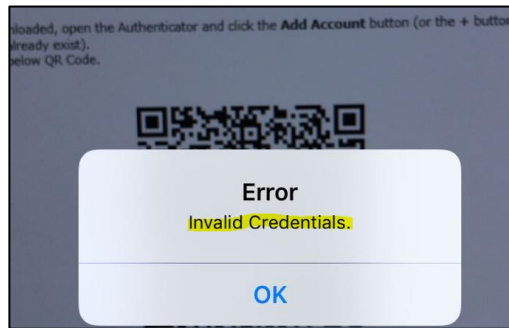


Figure 21 Disabled User / Invalid Credentials Error

3.4.2 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:

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

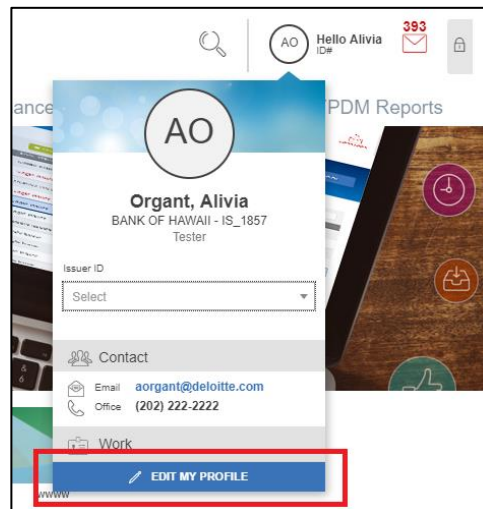


Figure 22 Edit My Profile

7. Select **Edit My Profile**
8. Select the **Account** tab
9. Select **Change Security Settings**

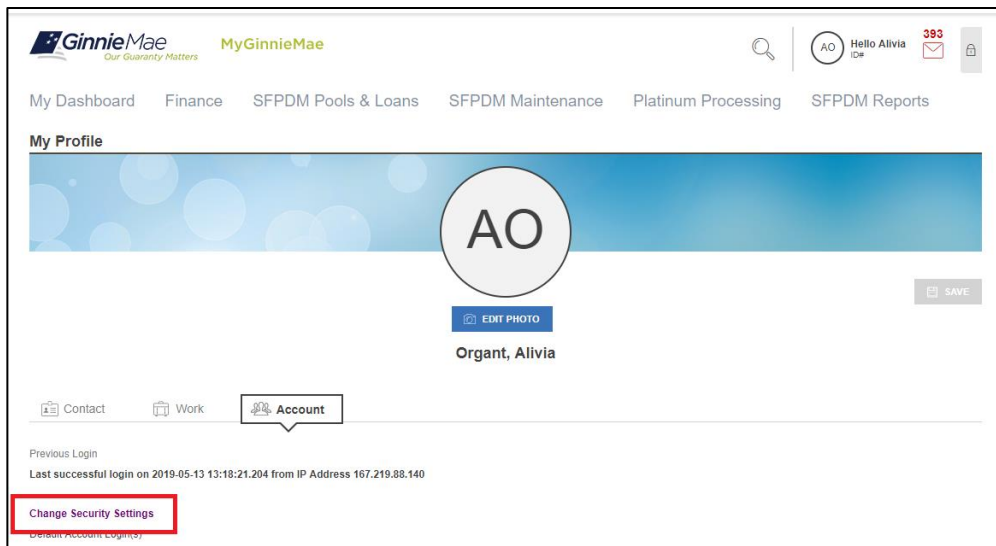


Figure 23 User's Profile Account Tab

10. On the Change Password Page, select **De-register**

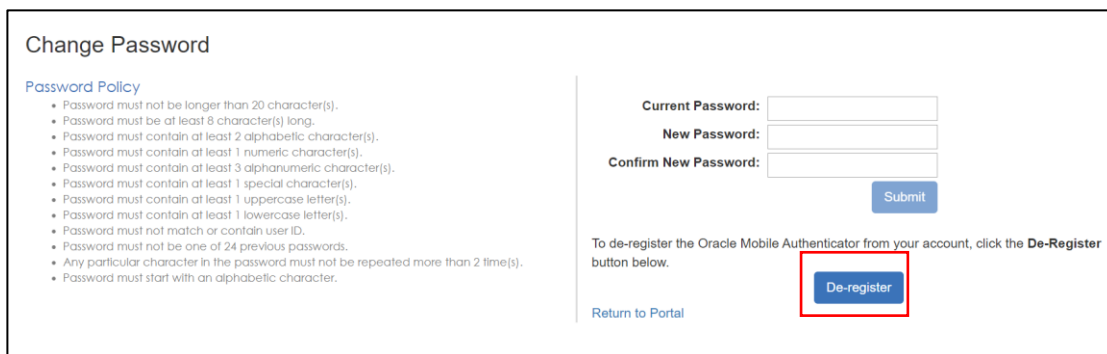


Figure 24 Change Password Page

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

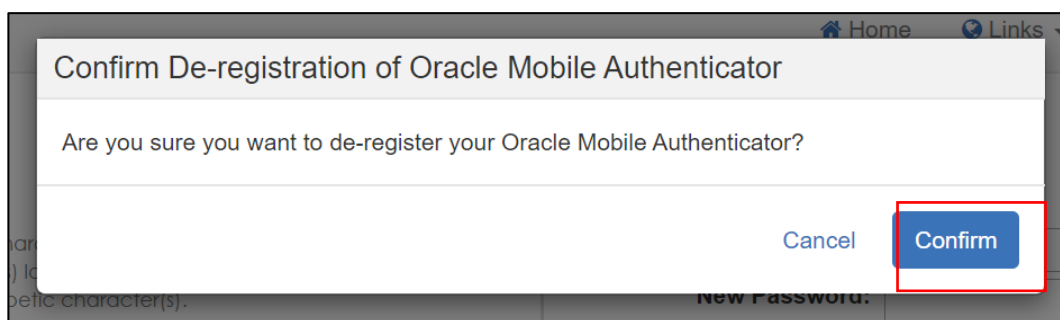


Figure 25 De-registration Confirmation Window

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

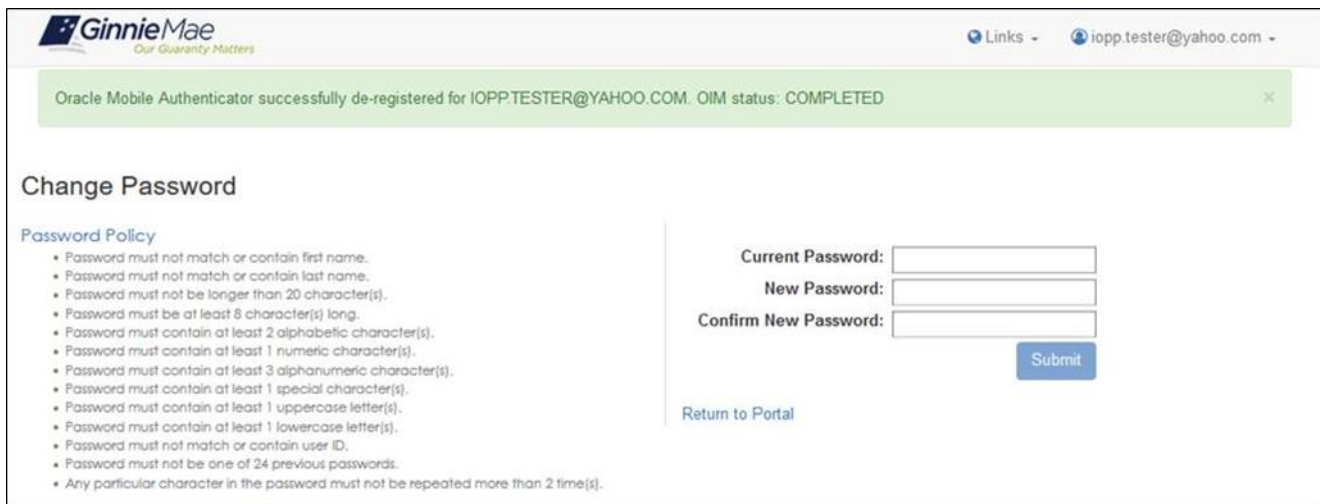


Figure 26 Successful De-registration Message

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

3.5 Managing Your MyGinnieMae Account

3.5.1 Profile Management

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

3.5.2 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.

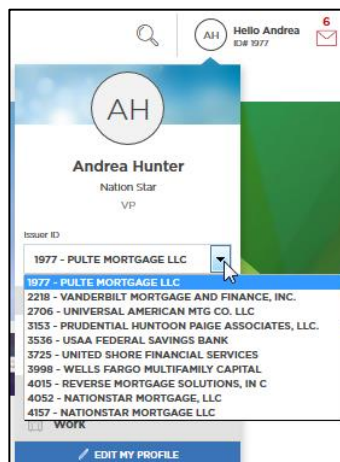


Figure 27 Toggle View

3.5.3 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

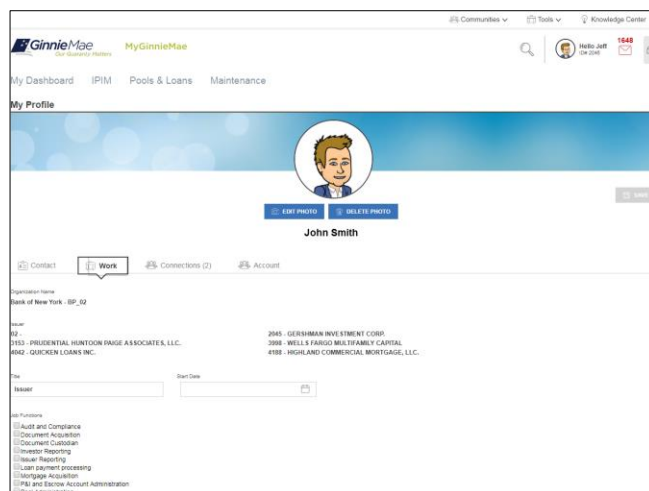


Figure 28 Manage Profile

3.5.4 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.

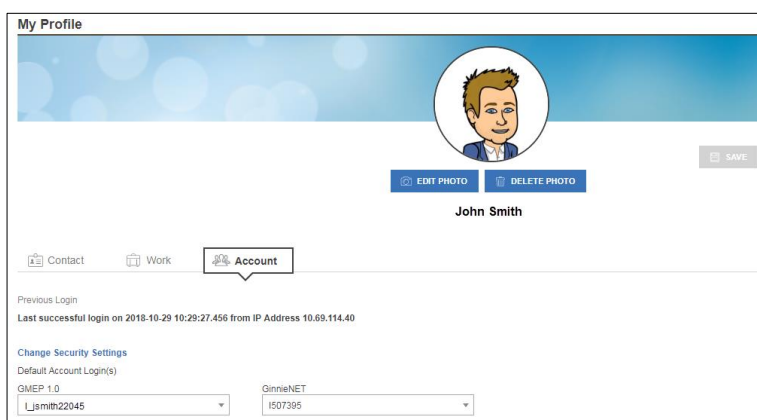


Figure 29 Associated Accounts

3.6 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 steps to take in each instance.

3.6.1 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:

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
3. Select **Edit My Profile**

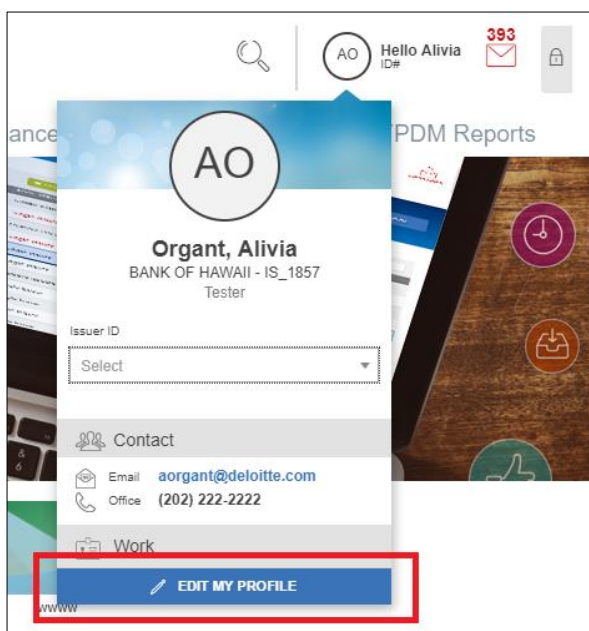


Figure 30 Edit User's Profile

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

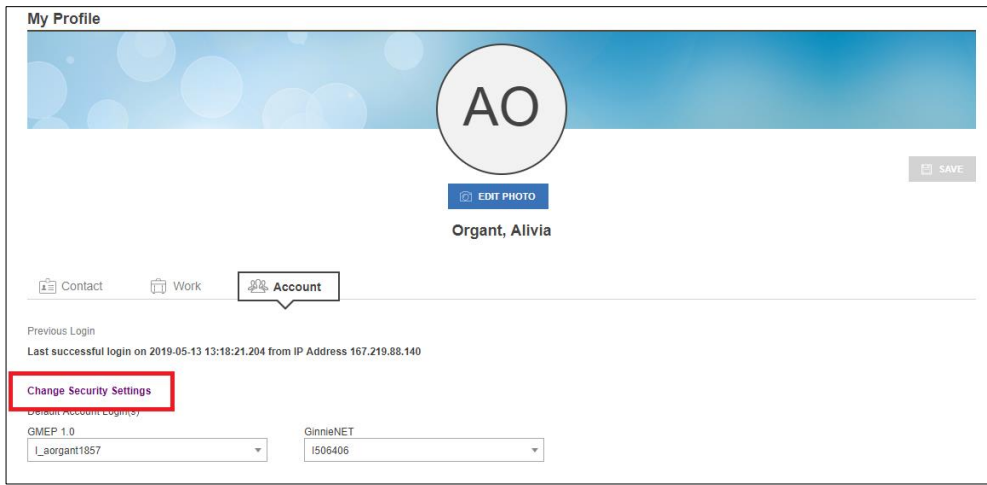


Figure 31 Change Security Settings

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

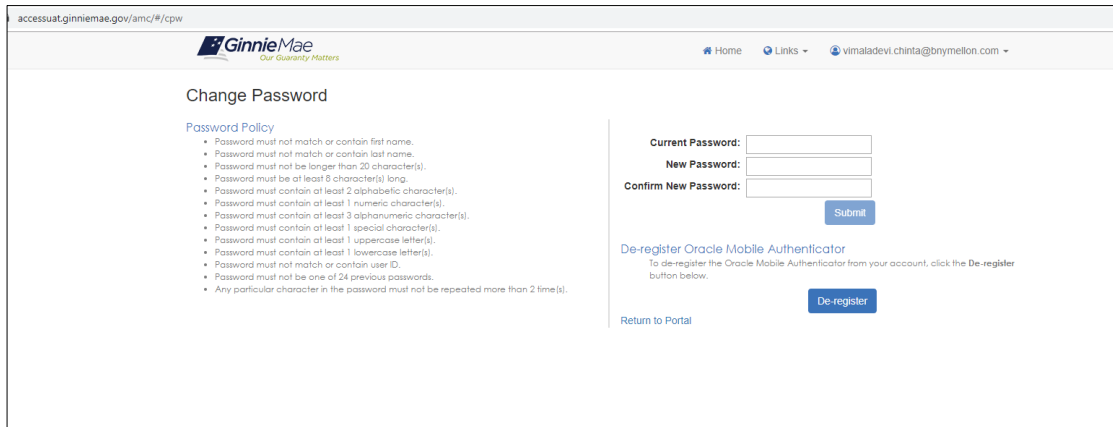


Figure 32 Change Password Page

NOTE: This page will 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 to avoid an Automatic Logout.

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

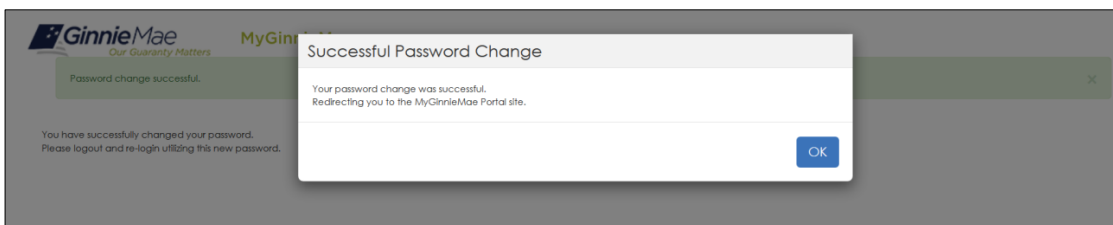


Figure 33 Successful Password Change Message

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

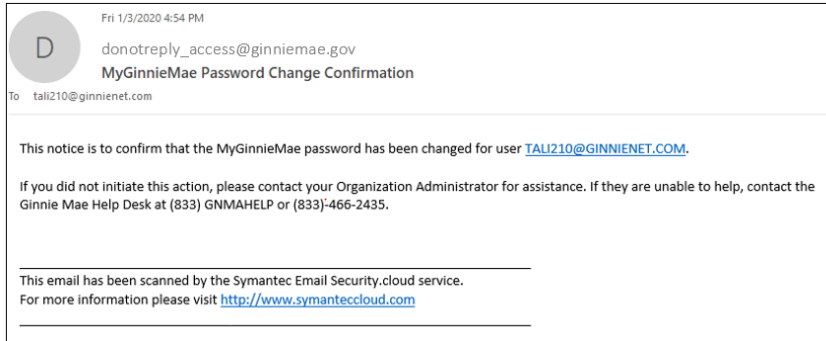


Figure 34 Change Password Confirmation Email

3.6.2 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.ginniemae.gov/> and select **Login**.
2. Select **Forgot Password?**

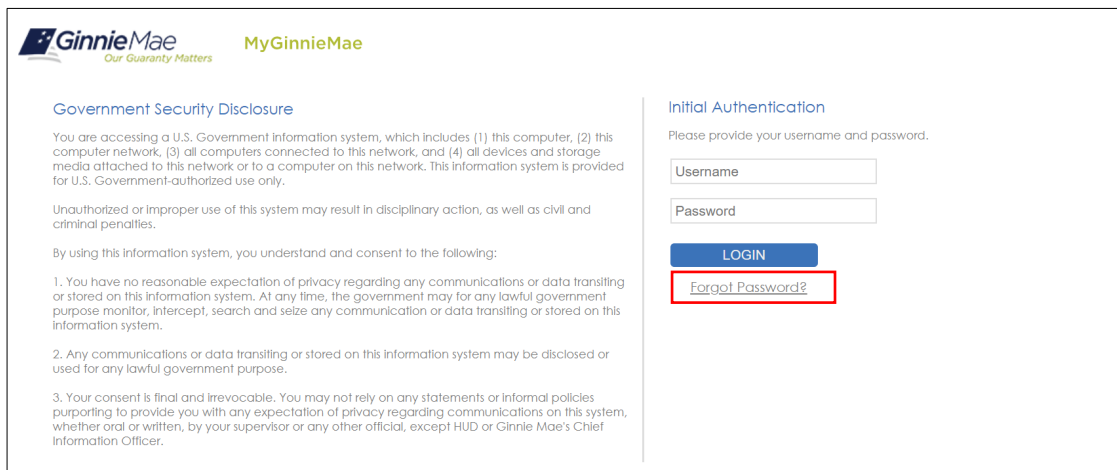
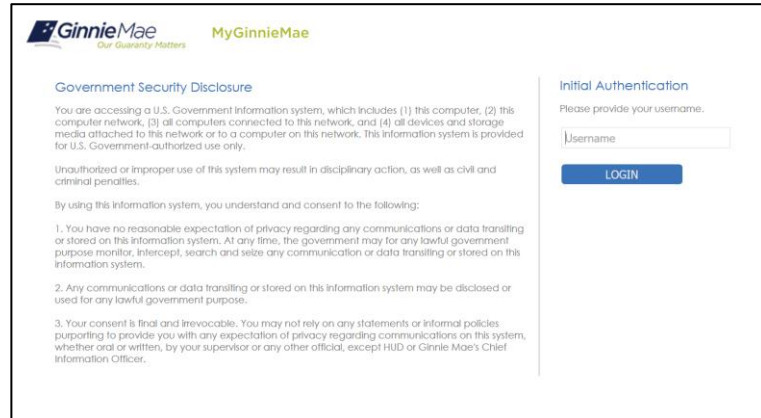


Figure 35 Login Page

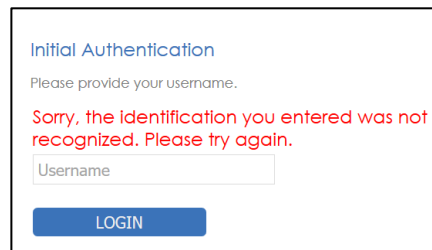
3. Enter the **Username**
4. Select **LOGIN**



The screenshot shows the MyGinnieMae login interface. On the left, there is a "Government Security Disclosure" section with text regarding U.S. Government Information system access and consent. On the right, the "Initial Authentication" section prompts the user to provide their username. It includes a text input field labeled "Username" and a blue "LOGIN" button.

Figure 36 Forgot Password Username Prompt

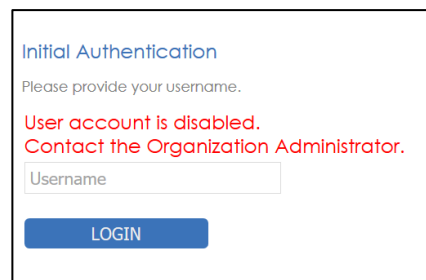
NOTE: If the user enters the incorrect username or does not have a registered MGM account, they will see the following error message:



The screenshot shows the "Initial Authentication" form with an error message in red text: "Sorry, the identification you entered was not recognized. Please try again." Below the error message is the "Username" input field and the "LOGIN" button.

Figure 37 Forgot Password Username Prompt – Error

NOTE: If a user account is disabled, the user will see the following error message:



The screenshot shows the "Initial Authentication" form with an error message in red text: "User account is disabled. Contact the Organization Administrator." Below the error message is the "Username" input field and the "LOGIN" button.

Figure 38 Disabled User Username Prompt – Error

5. After successfully entering their username, the user will be prompted to choose and enter a One-Time PIN (OTP). See [Section: Choosing and Entering a One-Time PIN \(OTP\)](#).
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**

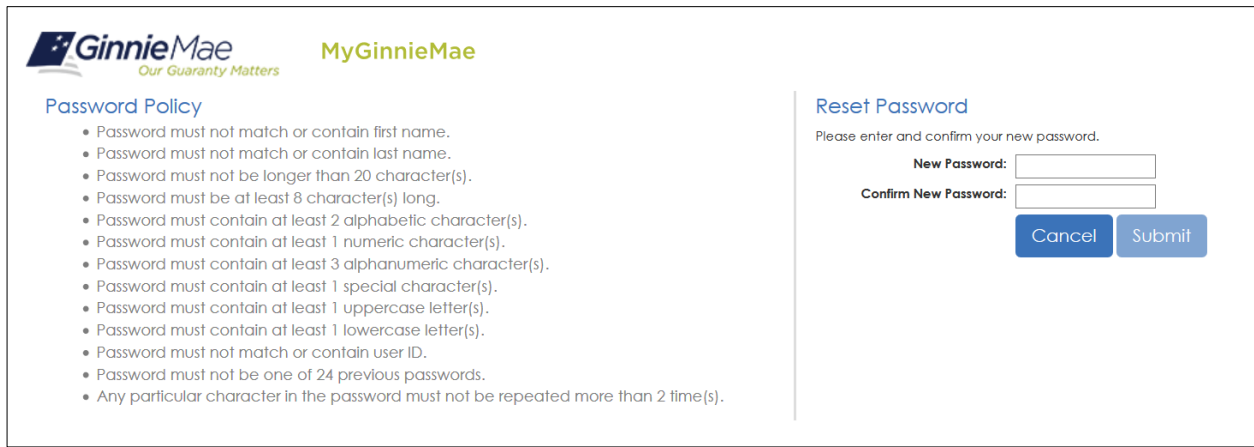


Figure 39 Reset Password Page

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

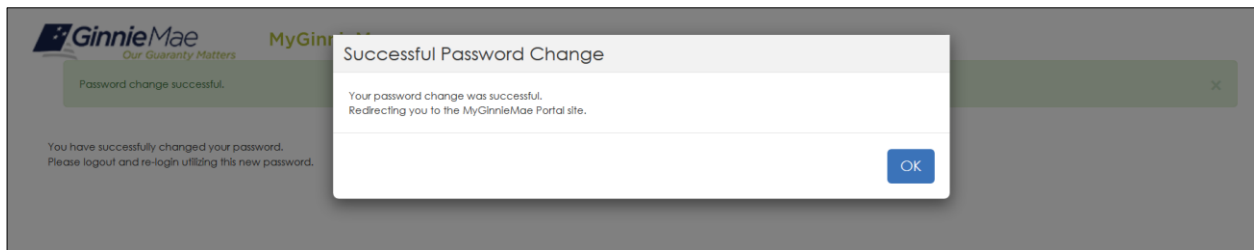


Figure 40 Successful Password Change Message

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

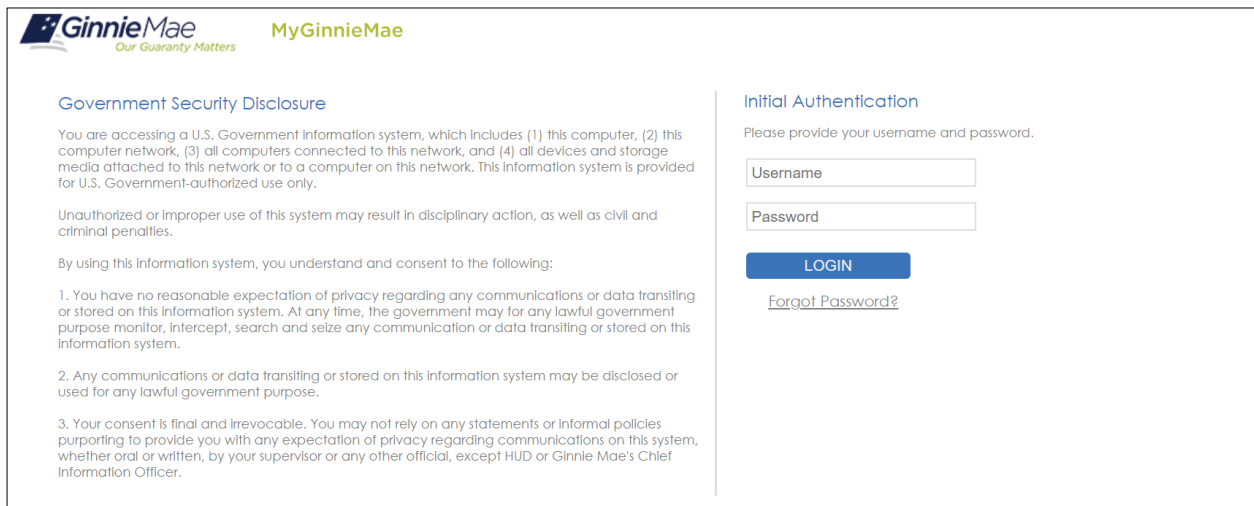


Figure 41 Redirect to Login Page

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

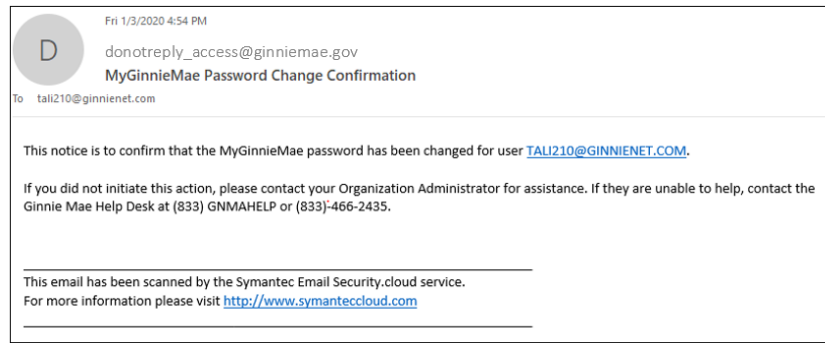


Figure 42 Password Change Confirmation Email

3.6.3 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 [Section: Organization Administrators](#).

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

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

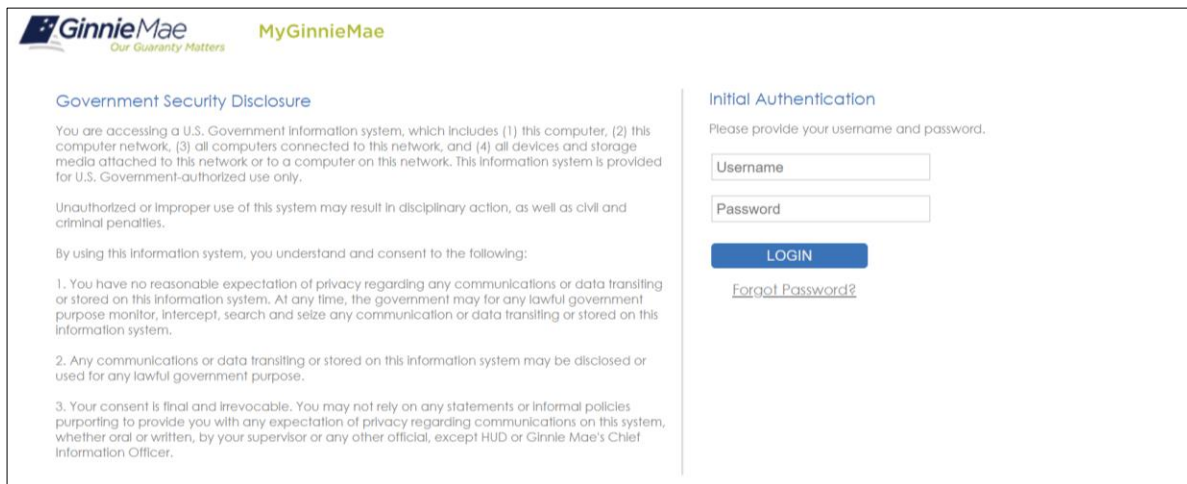


Figure 43 Login Page

3. Complete the steps to OTP. See [Section: Choosing and Entering a One-Time PIN \(OTP\)](#)
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**

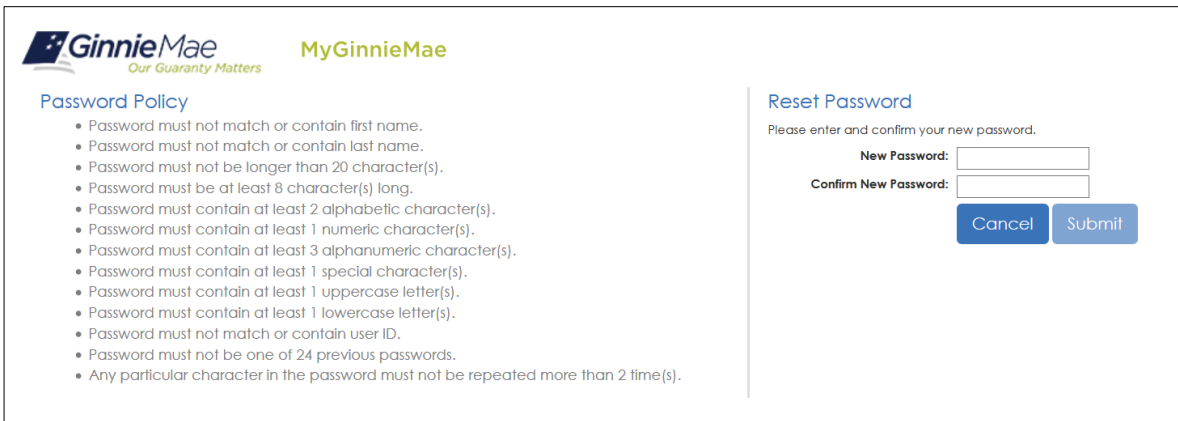


Figure 44 Enter New Password Page

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

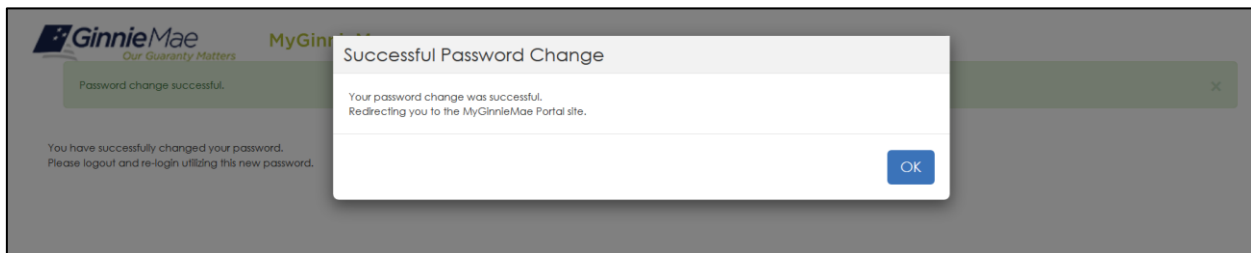


Figure 45 Successful Password Change Message

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

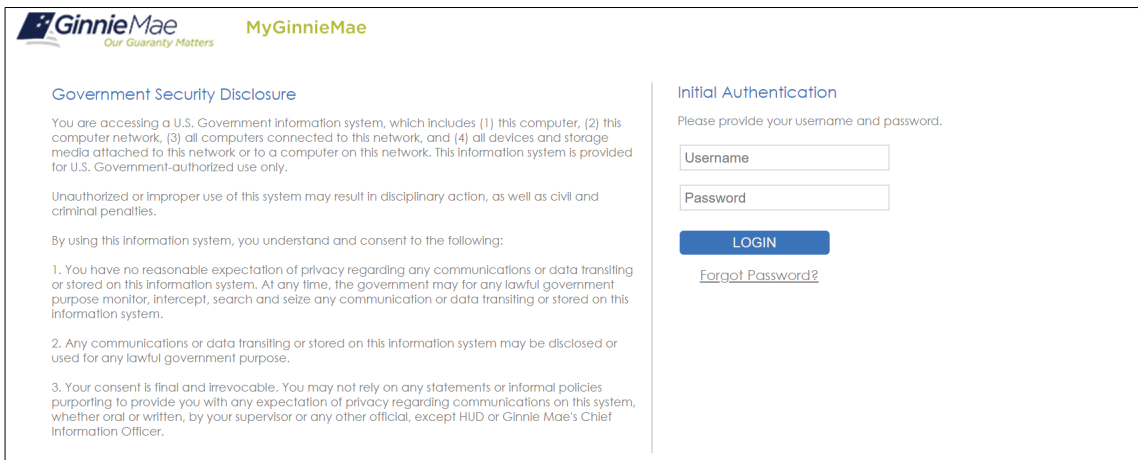


Figure 46 Redirect to Login Page

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

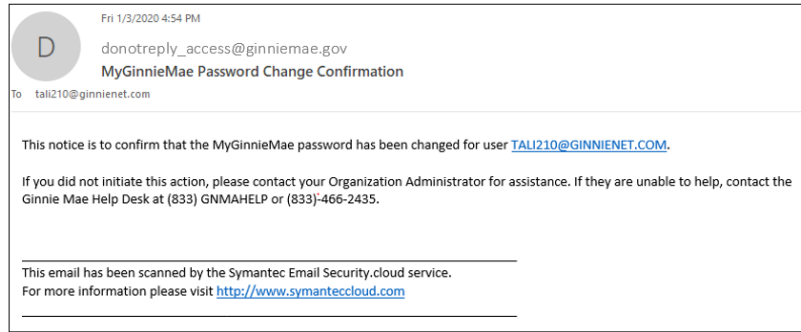


Figure 47 Password Change Confirmation Email

3.6.4 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.

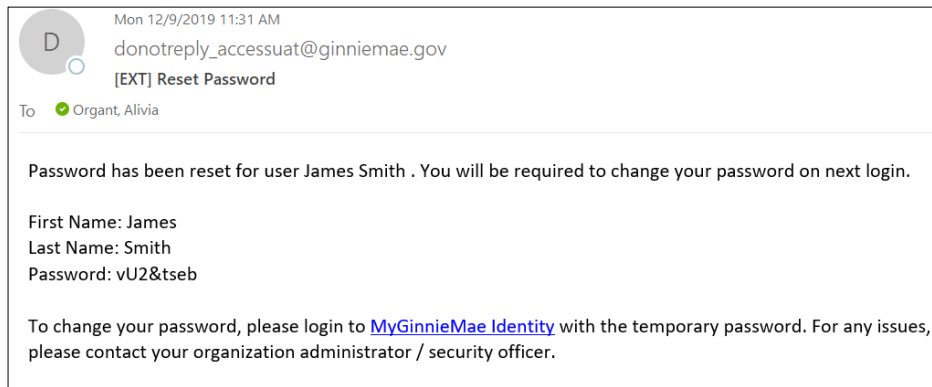


Figure 48 Temporary Password Email

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

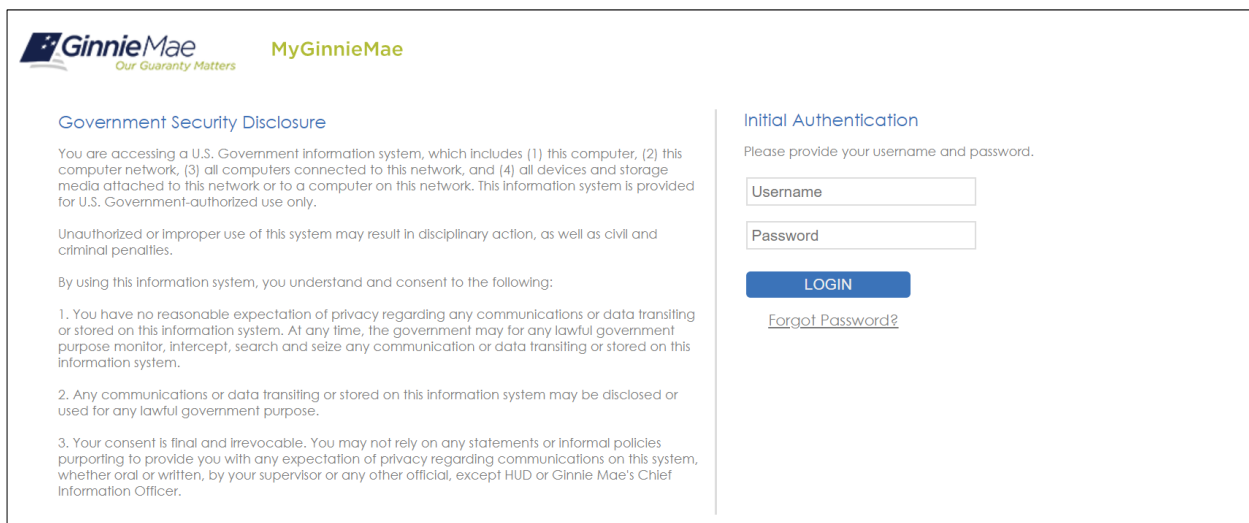


Figure 49 Login Page

3. Complete the steps to OTP. See [Section: Choosing and Entering a One-Time PIN \(OTP\)](#)
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**

GinnieMae
Our Guaranty Matters

MyGinnieMae

Password Policy

- Password must not match or contain first name.
- Password must not match or contain last name.
- Password must not be longer than 20 character(s).
- Password must be at least 8 character(s) long.
- Password must contain at least 2 alphabetic character(s).
- Password must contain at least 1 numeric character(s).
- Password must contain at least 3 alphanumeric character(s).
- Password must contain at least 1 special character(s).
- Password must contain at least 1 uppercase letter(s).
- Password must contain at least 1 lowercase letter(s).
- Password must not match or contain user ID.
- Password must not be one of 24 previous passwords.
- Any particular character in the password must not be repeated more than 2 time(s).

Reset Password

Please enter and confirm your new password.

New Password:

Confirm New Password:

Figure 50 Enter New Password Page

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

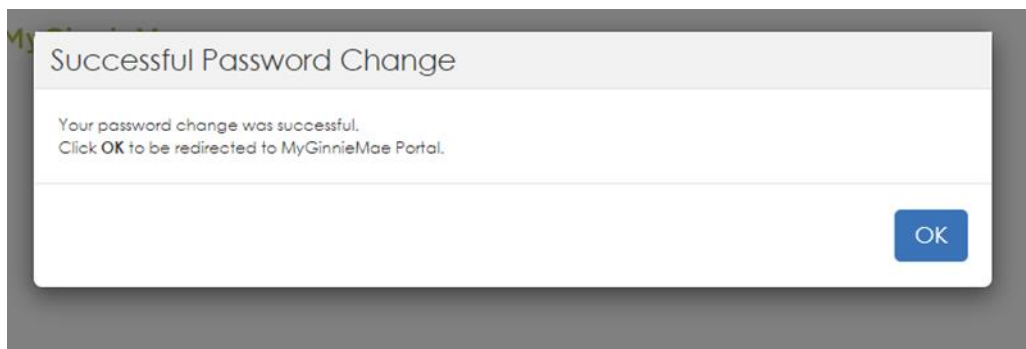


Figure 51 Successful Password Change Message

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

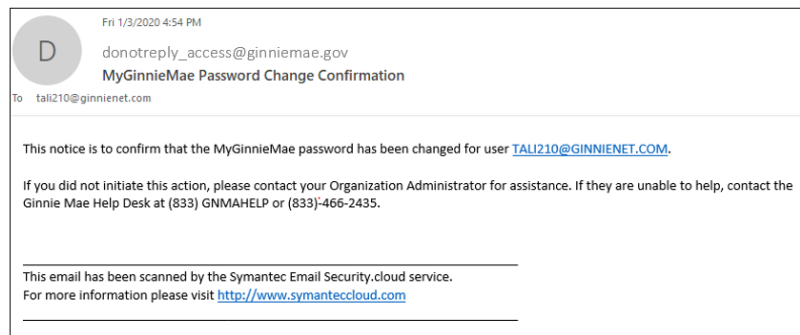


Figure 52 Password Change Confirmation Email

3.7 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.

3.7.1 Entering a Username and Password

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

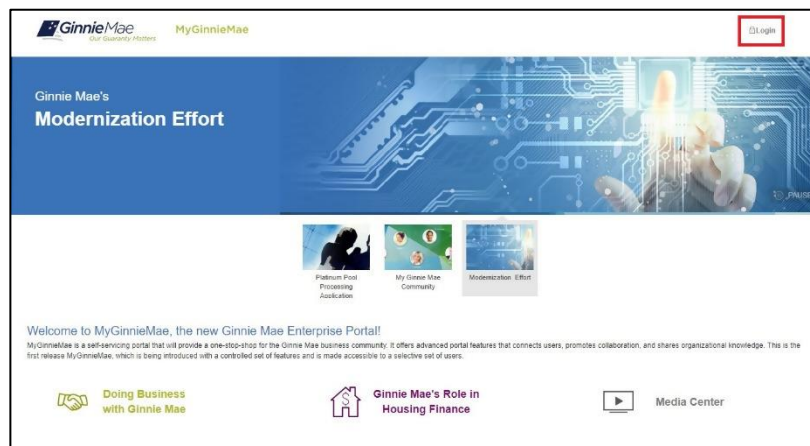


Figure 53 Public Landing Page

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**.

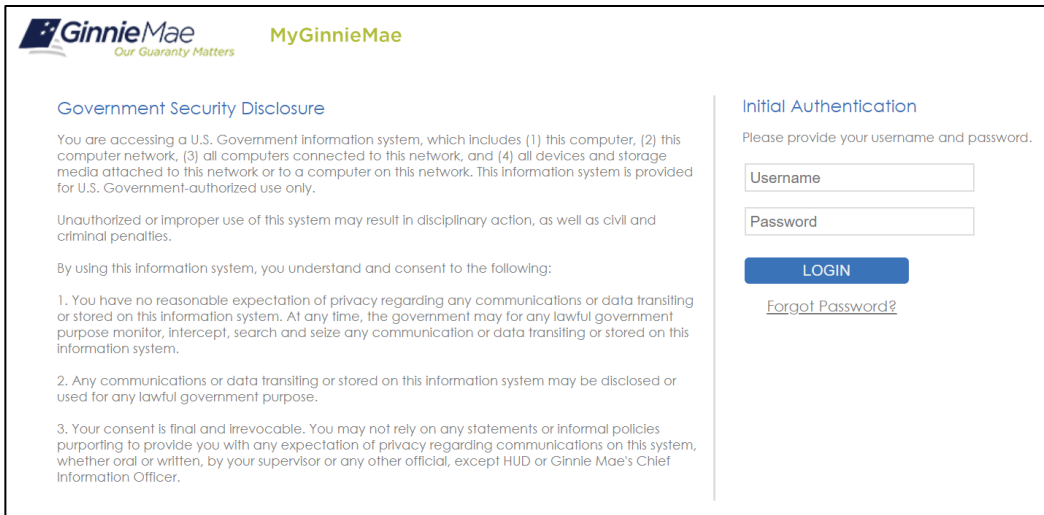


Figure 54 Login Page

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.

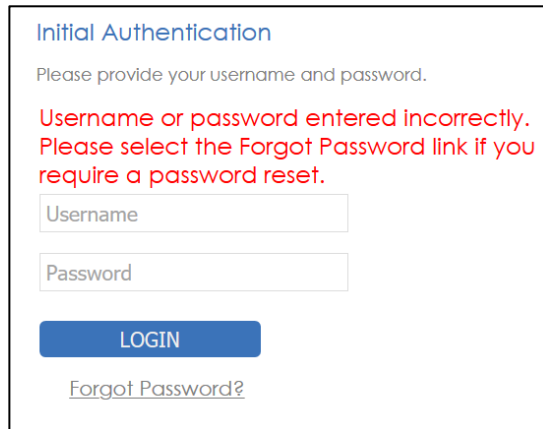


Figure 55 Incorrect Username/Password Error

3.7.2 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:
 - a. To receive an eight-digit OTP through the user's email, or

- b. To input a six-digit OTP generated from the OMA App

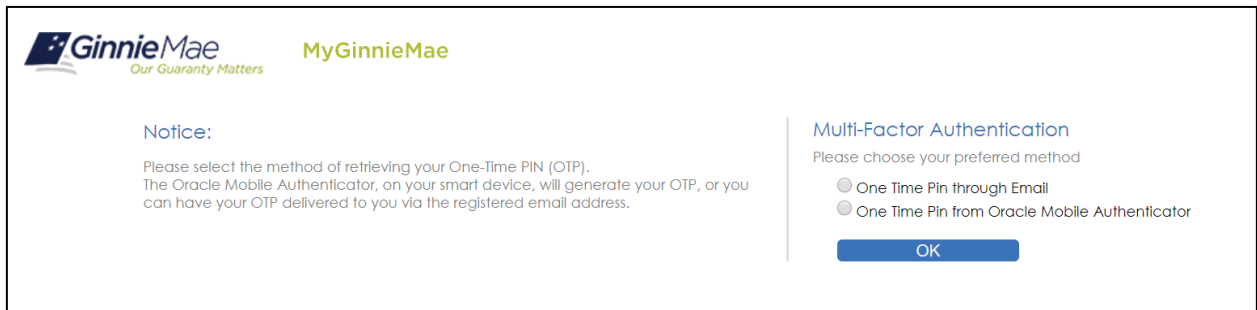


Figure 56 Multi-Factor Authentication Page

- 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**

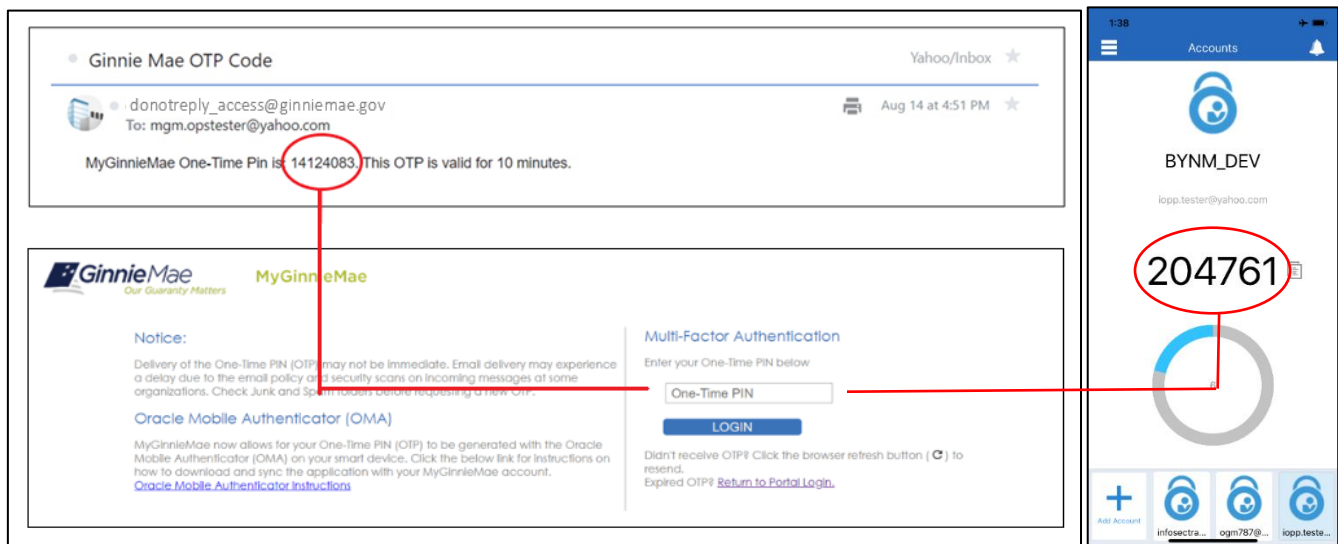


Figure 57 (Above) One-Time PIN (OTP) through Email / (Right) OTP from Oracle Mobile Authenticator (OMA)

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

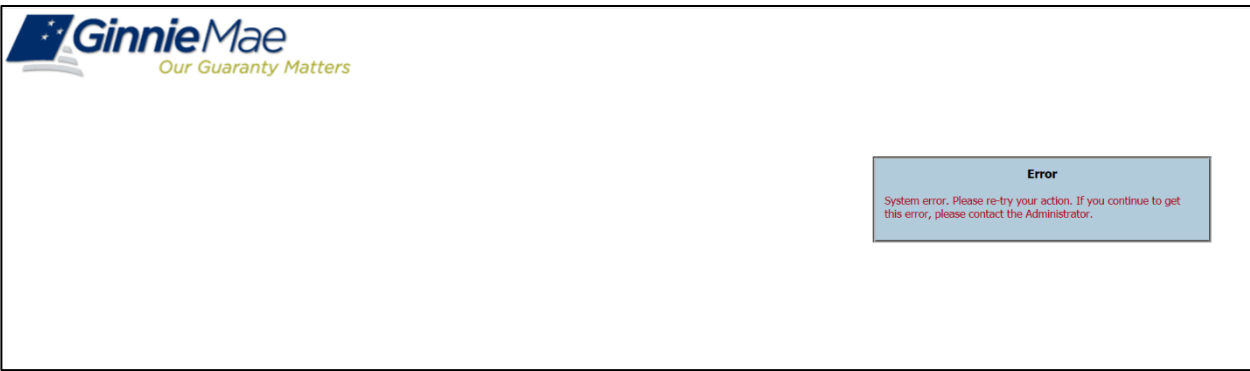


Figure 58 System Error Message

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

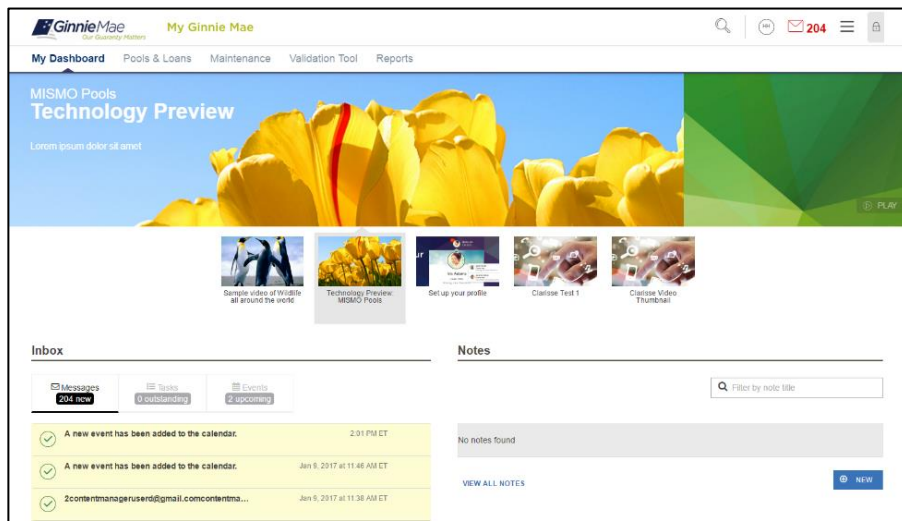


Figure 59 My Dashboard

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).

3.7.3 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 [Section: Organization Administrators](#). 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.

3.8 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.

3.8.1 Manually Exiting MyGinnieMae


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



Figure 60 Logout Lock Icon

2. Select **LOG OUT**




Figure 61 Protal Logout

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

3.8.2 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.

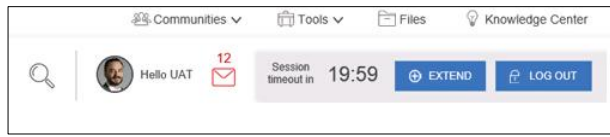


Figure 62 Portal Session Timeout Timer

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.

3.9 Navigating the Portal

3.9.1 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 it's 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 [Section: Issuer ID](#) 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 63 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.

3. 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 [Issuer ID](#) for more information on selecting the proper organization ID on the user's profile.

3.9.2 Marquee

On both the 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 64 Marquee

3.9.3 My Dashboard

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

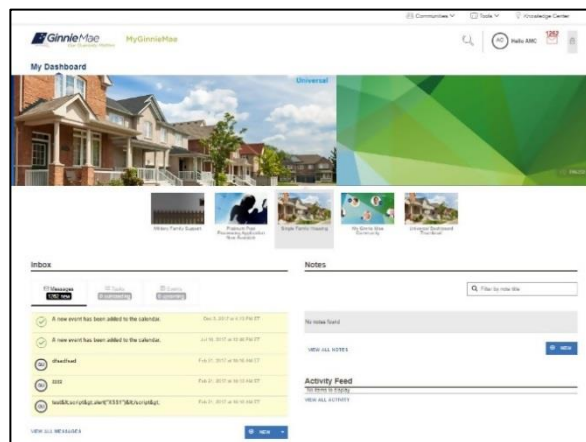


Figure 65 My Dashboard

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.

3.9.4 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.

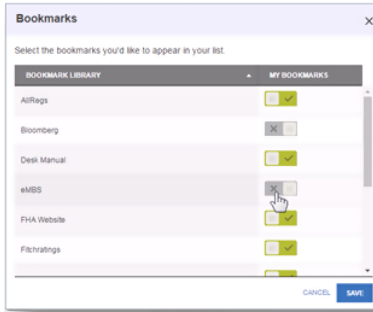


Figure 66 Bookmarks

3.9.5 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.

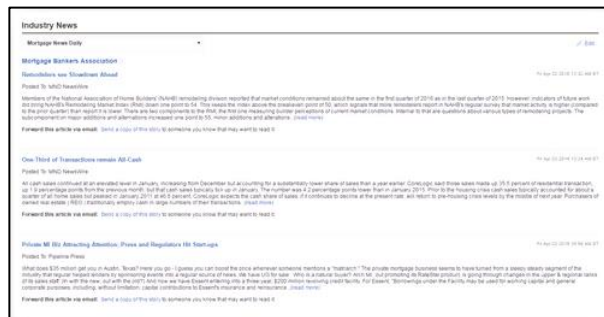


Figure 67 Industry News

3.9.6 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.

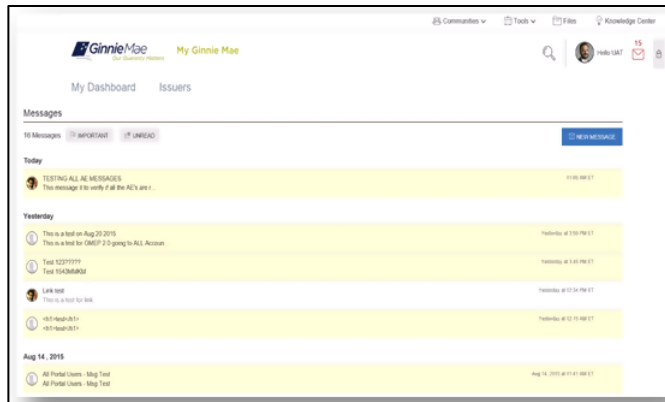


Figure 68 Messages

3.10 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.

3.10.1 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.

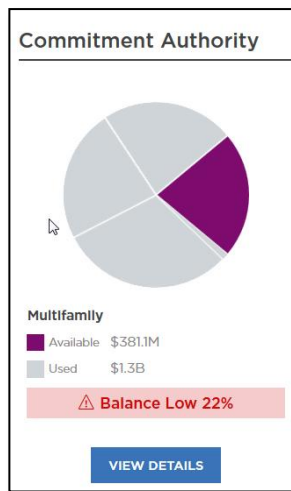


Figure 69 Commitment Authority Details

3.10.2 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.

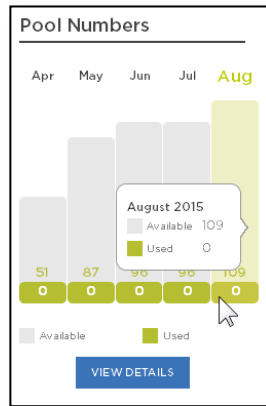


Figure 70 Pool Number Details

3.10.3 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.

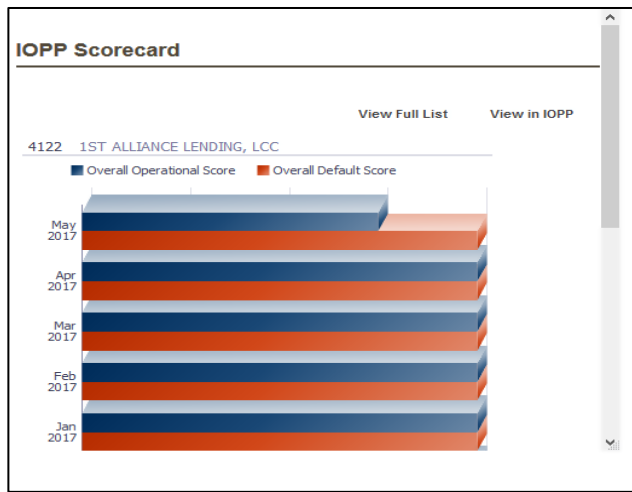


Figure 71 IOPP Scorecard

3.11 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.

3.11.1 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 72 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.”

3.11.2 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.

3.12 Knowledge Center

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

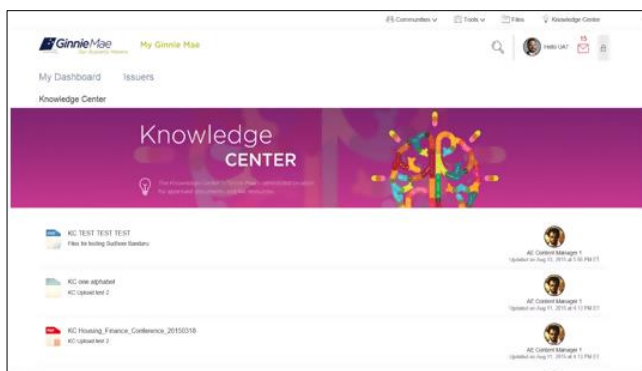


Figure 73 Knowledge Center

3.13 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.

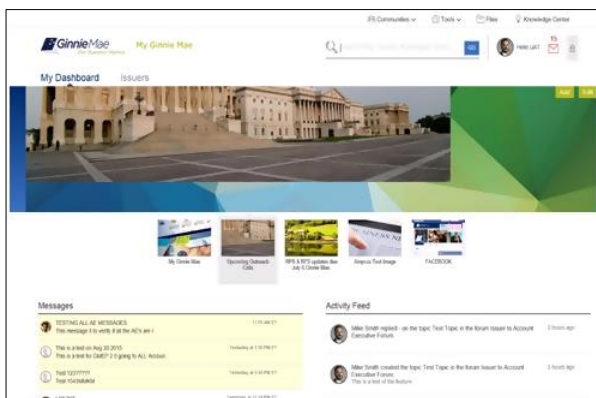


Figure 74 Portal Search

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.

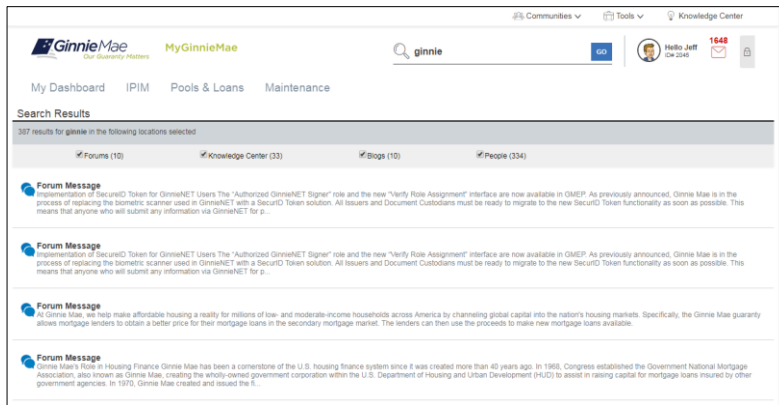


Figure 75 Search Results

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

3.14 Troubleshooting and System Errors

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

3.14.1 Basic Error Handling

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



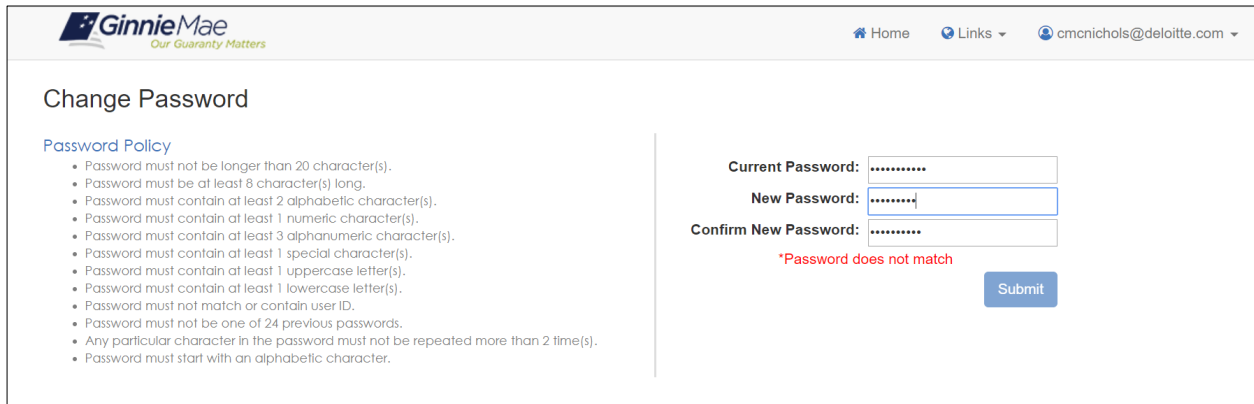
Figure 76 System Error Message

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 [Section: Applications](#) 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](#).

3.14.2 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.”



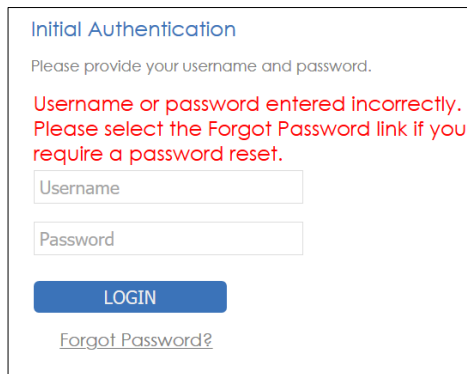
The screenshot shows the GinnieMae 'Change Password' page. On the left, there is a 'Password Policy' section with a list of requirements: password length (20 characters), minimum length (8 characters), character types (2 alphabetic, 1 numeric, 3 alphanumeric, 1 special, 1 uppercase, 1 lowercase), and other rules like no user ID, no previous passwords, and no repeated characters. On the right, there are three input fields: 'Current Password', 'New Password', and 'Confirm New Password'. The 'New Password' and 'Confirm New Password' fields contain asterisks. Below these fields, a red error message reads '*Password does not match'. A blue 'Submit' button is located at the bottom right of the form area.

Figure 77 New Password Does Not Match Error

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

3.14.3 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).



The screenshot shows the 'Initial Authentication' page. It prompts the user to provide their username and password. A red error message states: 'Username or password entered incorrectly. Please select the Forgot Password link if you require a password reset.' Below the error message are two input fields for 'Username' and 'Password'. At the bottom, there is a blue 'LOGIN' button and a link for 'Forgot Password?'.

Figure 78 Invalid Password Error

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

3.14.4 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.

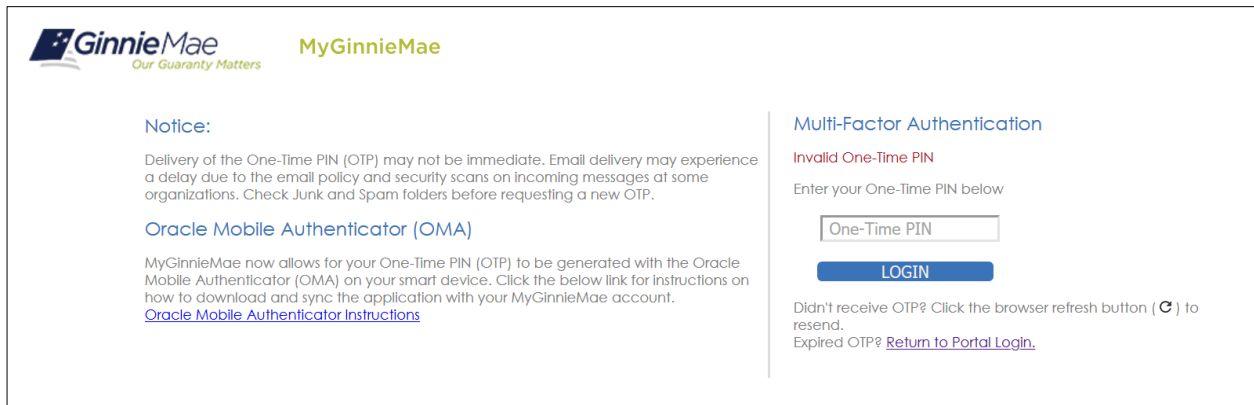


Figure 79 Incorrect OTP Error

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

3.14.5 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.

3.14.6 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.

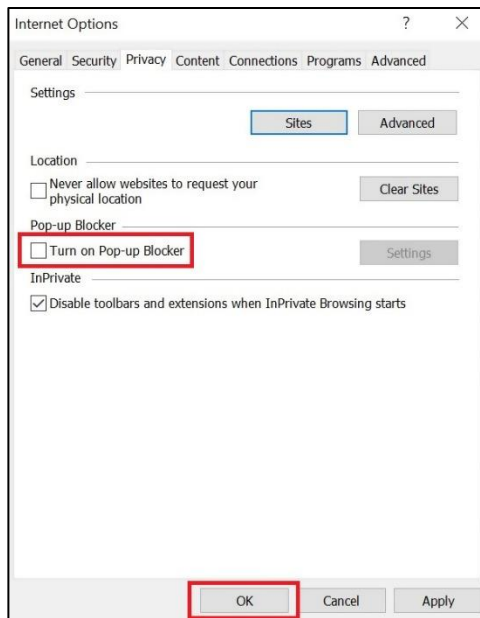


Figure 80 Disable Pop-up Blocker

3.14.7 Account Locked

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

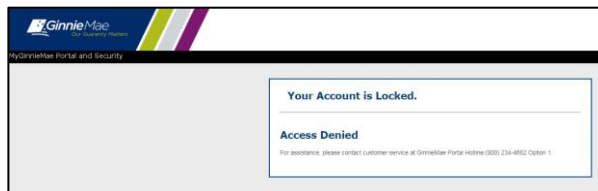


Figure 81 Account Locked

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

3.14.8 MyGinnieMae Portal Profile Accounts tab: GMEP 1.0 or GinnieNET Account 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](#).

3.14.9 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

A registration form with three input fields: * Job Title (AVP), * Org Id (BNY Mellon), and * Email (steve.john). A red box highlights the email field. An error message box is open, displaying: "Error: The format is incorrect. Entered Email Address steve.john is incorrect. Please provide correct Email Address."

Figure 82 Registration Email Form Error

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

A dialog box with the following text: "donotreply_access@ginnie.mae.gov", "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", and an "OK" button.

Figure 83 Email Submit Error

The registration page then displays the Error 500 shown below.

An error message box with the following text: "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."

Figure 84 Registration Email Form Error

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

4 APPLICATIONS

This section provides linked access to procedures for each application supported by the MyGinnieMae portal.

(The below placeholders will be updated with a hyperlink to the procedures stored on Ginnie Mae's website.)

4.1 Access Management Console (AMC)

4.2 Platinum Pool Processing

4.3 Multifamily Pool Delivery Module (MFPDM)

4.4 [GinnieNET](#)

4.5 RFS - Reporting and Feedback System

5 GETTING HELP

This section provides the user with information on where to search for information and resources to assist with their account, navigating the portal and its applications, and troubleshooting issues.

5.1 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 - [Section: Change Password](#) or [Changing a Password QRC](#)
- Resetting a forgotten password - [Section: Forgotten Password](#) or [Forgot Password QRC](#)
- Updating profile information - [Section: Edit Profile](#)
- Registering for mobile delivery of the OTP - [Section: Register with the Oracle Mobile Authenticator](#)
- Troubleshooting and System Errors - [Section: Troubleshooting and System Errors](#)

Easy reference tools like Quick Reference Cards (QRCs) in [Section: Quick Reference Cards](#) and the Portal Help Page at the bottom of each portal page, can be used to help answer common questions. 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.ginniemae.gov/issuers/issuer_training/pages/modernization.aspx.

5.2 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 such as a RSA Token
- 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.

5.3 Ginnie Mae Customer Support

Ginnie Mae Customer Support may be reached at:

1-833-GNMA HELP / 1-833-466-2435

ginniemae1@bnymellon.com

5.3.1 Customer Support Help with System Access

The Operations Administrators for the MyGinnieMae portal may be reached via [Ginnie Mae Customer Support](#). The Operations Administrators are responsible for creating and managing Organization Administrator accounts. The Operations Administrator is not authorized to create or otherwise manage End User accounts for Ginnie Mae business partners but may support Organization Administrators in their role to manage End User accounts on behalf of their organization.

5.3.2 Customer Support Help with Portal Applications

End Users are encouraged to utilize the application user manuals found in [Section: Applications](#) and invited to utilize [Ginnie Mae Customer Support](#) for additional guidance and support.

6 APPENDIX

6.1 Key Features

Services	Description
User Registration	MyGinnieMae user registration is a self-service user registration process used to collect, verify, and create a new user's identity information in MyGinnieMae, enabling the user to access MyGinnieMae and protected ecosystem. User registration provides a single identity for users accessing MyGinnieMae and protected applications. It automates the user account creation process and reduces costs.
Application Access Request Workflow	Access request workflow provides a single automated self-service interface for users to submit and approve requests for application access.
Federated Single Sign-On	Federated Single Sign-On is an extension of web Single Sign-On that reuses existing Ginnie Mae credentials to access external federated or cloud-based service providers.
Self-Service Password Management	The self-service password management feature provides the ability for an end user to change their password if known, as well as to be challenged if they have forgotten their password or entered an incorrect password.
Automated Workflow	Automated workflows are logical, repeatable processes during which documents, information, or tasks are passed from one participant to another for action, according to a set of procedural rules. A participant may be a person, or a machine, or both. Examples of automated workflows include role-based access request processes.
Invitation Model	A service that allows Organization Administrators to prefill details about users such as name and email address. Additionally, it will allow the Organization Administrators to send out an automated invitation to the end user to expedite the registration process.

Table 7 Key Features

6.2 Functional Roles

6.2.1 Single-Family Issuer Functional Roles

Functional Role	Description	RFS/GMEP 1.0	GinnieNET	MyGinnieMae
SF-Post-Closing User	Access to review collateral, obtain loan insurance, forward initial and trailing documents to a Document Custodian.	<ul style="list-style-type: none"> eNotification User 		<ul style="list-style-type: none"> GMEP2 User Issuer
SF-Loan Delivery and Pooling Basic User	Upload/enter pool and loan information for delivery; verify availability of commitment authority; clear document deficiencies and pooling exceptions; access to prepare but not execute PIIT/TAI transactions.	<ul style="list-style-type: none"> eNotification User 	Single-family Issuer	<ul style="list-style-type: none"> GMEP2 User Issuer PDM_SF_VIEW PDM_DATAENTRY
SF-Loan Delivery and Pooling Authorized Signer	Only for HUD 11702 signatories. All rights of a Loan Delivery and Pooling Basic User, plus; authority to submit pools for issuance, request additional commitment authority and execute PIIT/TAI transactions.	<ul style="list-style-type: none"> eNotification User RPN Issuer Access Authorized GinnieNET Signer CM Issuer Access SecurID Token Holder 	Single-family Issuer	<ul style="list-style-type: none"> GMEP2 User Issuer PDM_SF_VIEW PDM_DATAENTRY PDM_AUTHORIZEDSIGNER
SF-Investor Reporting Basic User	Submit monthly pool and loan level accounting data; submit quarterly custodial account verification data; review monthly remittance information, review monthly reporting exception feedback and errors.	<ul style="list-style-type: none"> Upload & Exception Feedback User eNotification User Pool Accounting User 	<ul style="list-style-type: none"> Investor Reporting Certification 	<ul style="list-style-type: none"> GMEP2 User Issuer PDM_SF_VIEW
SF-Investor Reporting Authorized Signer	Only for HUD 11702 signatories. All rights of an Investor Reporting Basic User, plus; authority to certify the monthly pool and loan accounting report; submit edits needed to clear exception feedback and monthly reporting errors.	<ul style="list-style-type: none"> Authorized GinnieNET Signer Upload & Exception Feedback User Pool Accounting User eNotification User SecurID Token Holder 	<ul style="list-style-type: none"> Investor Reporting Certification 	<ul style="list-style-type: none"> GMEP2 User Issuer PDM_SF_VIEW

Functional Role	Description	RFS/GMEP 1.0	GinnieNET	MyGinnieMae
SF-Compliance and Oversight User	Review portfolio servicing and investor reporting metrics and reports; oversee subservicer performance when applicable.	<ul style="list-style-type: none"> GPADS User eNotification User Pool Accounting User IOPP Issuer Access 	<ul style="list-style-type: none"> Investor Reporting Certification 	<ul style="list-style-type: none"> GMEP2 User Issuer
SF-Bulk Transfers Authorized Signer	Initiate, manage and accept bulk transfer transactions; initiate and coordinate transfers of collateral files with transferee and transferor Issuers or Document Custodians.	<ul style="list-style-type: none"> PTS Issuer Access eNotification User PTS Issuer Access 9000-series SecurID Token Holder Authorized GinnieNET Signer 		<ul style="list-style-type: none"> GMEP2 User Issuer
SF-Collateral Management Authorized Signer	Process releases of collateral from the Document Custodian in accordance with servicing obligations (HUD-11708 Releases).	<ul style="list-style-type: none"> eNotification User Authorized GinnieNET Signer 	Single-family Issuer	<ul style="list-style-type: none"> GMEP2 User Issuer PDM_SF_VIEW
SF-Agency Relationship User	Access reports containing portfolio performance and liquidity metrics; receive targeted Ginnie Mae communications for individuals responsible for managing agency relationships.	<ul style="list-style-type: none"> eNotification User IOPP Issuer Access GPADS User 		<ul style="list-style-type: none"> GMEP2 User Issuer
SF-Processing Master Agreements Authorized Signer	Only for HUD 11702 signatories. Edit, submit, and certify Master Agreement documents and data required by Ginnie Mae.	<ul style="list-style-type: none"> eNotification User SecurID Token Holder MAMS Issuer Access 		<ul style="list-style-type: none"> GMEP2 User Issuer
SF-Financial Statements User	Submit annual audited financial statements for review by Ginnie Mae's IPA.	<ul style="list-style-type: none"> eNotification User Upload & Exception Feedback User 		<ul style="list-style-type: none"> GMEP2 User Issuer
SF-Special Loans User	Upload and process SCRA reimbursement requests.	<ul style="list-style-type: none"> eNotification User SCRA User 		<ul style="list-style-type: none"> GMEP2 User Issuer

Table 8 Single-Family Issuer Roles Access

6.2.2 Multifamily Issuer Functional Roles

Functional Role	Description	RFS/GMEP 1.0	GinnieNET	MyGinnieMae
MF-Loan Delivery and Pooling Basic User	Upload/enter pool and loan information for delivery; verify availability of commitment authority; clear document deficiencies and pooling exceptions; access to prepare but not execute PIIT/TAI transactions.	<ul style="list-style-type: none"> eNotification User RPN Issuer Access CM Issuer Access 	Multifamily Issuer	<ul style="list-style-type: none"> GMEP2 User Issuer PDM_MF_VIEW PDM_DATAENTRY
MF-Loan Delivery and Pooling Authorized Signer	Only for HUD 11702 signatories. All rights of a Loan Delivery and Pooling Basic User, plus; authority to submit pools for issuance, request additional commitment authority and execute PIIT/TAI transactions.	<ul style="list-style-type: none"> Authorized GinnieNET Signer SecurID Token Holder RPN Issuer Access eNotification User CM Issuer Access 	Multifamily Issuer	<ul style="list-style-type: none"> GMEP2 User Issuer PDM_MF_VIEW PDM_DATAENTRY PDM_AUTHORIZEDSIGNER
MF-Investor Reporting Basic User	Submit monthly pool and loan level accounting data; submit quarterly custodial account verification data; review monthly remittance information, review monthly reporting exception feedback and errors.	<ul style="list-style-type: none"> eNotification User Upload & Exception Feedback User Pool Accounting User 	<ul style="list-style-type: none"> Investor Reporting Certification 	<ul style="list-style-type: none"> GMEP2 User Issuer PDM_MF_VIEW
MF-Investor Reporting Authorized Signer	Only for HUD 11702 signatories. All rights of an Investor Reporting Basic User, plus; authority to certify the monthly pool and loan accounting report; submit edits needed to clear exception feedback and monthly reporting errors.	<ul style="list-style-type: none"> Upload & Exception Feedback User Pool Accounting User eNotification User SecurID Token Holder Authorized GinnieNET Signer 	<ul style="list-style-type: none"> Investor Reporting Certification 	<ul style="list-style-type: none"> GMEP2 User Issuer PDM_MF_VIEW
MF-Compliance and Oversight User	Review portfolio servicing and investor reporting metrics and reports; oversee subservicer performance when applicable.	<ul style="list-style-type: none"> IOPP Issuer Access GPADS User eNotification User Pool Accounting User Upload & Exception Feedback User 		<ul style="list-style-type: none"> GMEP2 User Issuer PDM_MF_VIEW

Functional Role	Description	RFS/GMEP 1.0	GinnieNET	MyGinnieMae
MF-Master Agreements Authorized Signer	Only for HUD 11702 signatories. Edit, submit, and certify Master Agreement documents and data required by Ginnie Mae.	<ul style="list-style-type: none"> eNotification User SecurID Token Holder MAMS Issuer Access 		<ul style="list-style-type: none"> GMEP2 User Issuer PDM_MF_VIEW
MF-Financial Statements User	Submit annual audited financial statements for review by Ginnie Mae's IPA.	<ul style="list-style-type: none"> eNotification User Upload & Exception Feedback User 		<ul style="list-style-type: none"> GMEP2 User Issuer PDM_MF_VIEW
MF-Transfers Authorized Signer	Initiate, manage and accept bulk transfer transactions; Initiate and coordinate transfers of collateral files with transferee and transferor Issuers or Document Custodians.	<ul style="list-style-type: none"> PTS Issuer Access eNotification User PTS Issuer Access 9000-series SecurID Token Holder Authorized GinnieNET Signer 		<ul style="list-style-type: none"> GMEP2 User Issuer PDM_MF_VIEW

Table 7 Multifamily Issuer Roles Access

6.2.3 HECM Issuer Functional Roles

Functional Role	Description	RFS/GMEP 1.0	GinnieNET	MyGinnieMae
HECM-Post Closing User	Access to review collateral; obtain loan insurance, forward initial and trailing documents to a Document Custodian.	<ul style="list-style-type: none"> eNotification User 		<ul style="list-style-type: none"> GMEP2 User Issuer
HECM-Loan Delivery and Pooling Basic User	Upload/enter pool, loan, and participation data into GinnieNET. Verify available commitment authority and clear document and/or GinnieNET pooling exceptions. Basic user cannot finalize transactions or submissions.	<ul style="list-style-type: none"> eNotification User 	HECM Issuer	<ul style="list-style-type: none"> GMEP2 User Issuer
HECM-Loan Delivery and Pooling Authorized Signer	Upload/enter pool, loan, and participation data into GinnieNET. Verify available commitment authority and clear document and/or GinnieNET pooling exceptions. Possess the authority to finalize or execute business transactions with Ginnie Mae (HUD-11702 Signers), including the authority to submit requests for additional commitment authority as needed and to submit pools for issuance.	<ul style="list-style-type: none"> Authorized GinnieNET Signer SecurID Token Holder RPN Issuer Access eNotification User CM Issuer Access 	HECM Issuer	<ul style="list-style-type: none"> GMEP2 User Issuer
HECM-Investor Reporting Basic User	Submit the monthly pool, loan, and participation data. Submit the custodial account verification data. Review monthly remittance information and reporting exception feedback and errors. Ability to track loans approaching 98% of MCA (Maximum Claim Amount) to identify if loans need to be bought out and coordinate with Participation Agent	<ul style="list-style-type: none"> eNotification User Upload & Exception Feedback User Pool Accounting User HMBS User 	<ul style="list-style-type: none"> Investor Reporting Certification 	<ul style="list-style-type: none"> GMEP2 User Issuer

Functional Role	Description	RFS/GMEP 1.0	GinnieNET	MyGinnieMae
	for assurance that all participations in other pools are bought out accordingly.			
HECM-Investor Reporting Authorized Signer	Submit the monthly pool, loan, and participation data. Submit the custodial account verification data. Review monthly remittance information and reporting exception feedback and errors. Ability to track loans approaching 98% of MCA (Maximum Claim Amount) to identify if loans need to be bought out and coordinate with Participation Agent for assurance that all participations in other pools are bought out accordingly. Including the authority to submit requests for additional commitment authority as needed and to submit pools for issuance.	<ul style="list-style-type: none"> Authorized GinnieNET Signer Upload & Exception Feedback User Pool Accounting User eNotification User SecurID Token Holder HMBS Issuer 	<ul style="list-style-type: none"> Investor Reporting Certification 	<ul style="list-style-type: none"> GMEP2 User Issuer
HECM-Compliance and Oversight User	Review portfolio servicing and investor reporting metrics and reports; oversee subservicer performance when applicable.	<ul style="list-style-type: none"> IOPP Issuer Access GPADS User eNotification User Pool Accounting User HMBS Issuer 		<ul style="list-style-type: none"> GMEP2 User Issuer
HECM-Bulk Transfers Authorized Signer	Initiate, manage and accept bulk transfer transactions; Initiate and coordinate transfers of collateral files with transferee and transferor Issuers or Document Custodians.	<ul style="list-style-type: none"> Authorized GinnieNET Signer PTS Issuer Access eNotification User PTS Issuer Access 9000-series SecurID Token Holder 		<ul style="list-style-type: none"> GMEP2 User Issuer
HECM-Collateral Management Authorized Signer	Process releases of collateral from the Document Custodian in accordance with servicing obligations (HUD-11708 Releases).	<ul style="list-style-type: none"> eNotification User Authorized GinnieNET Signer SecurID Token Holder 	HECM Issuer	<ul style="list-style-type: none"> GMEP2 User Issuer

Functional Role	Description	RFS/GMEP 1.0	GinnieNET	MyGinnieMae
HECM-Agency Relationship User	Access reports containing portfolio performance and liquidity metrics; receive targeted Ginnie Mae communications for individual responsible for managing agency relationships.	<ul style="list-style-type: none"> eNotification User IOPP Issuer Access GPADS User 		<ul style="list-style-type: none"> GMEP2 User Issuer
HECM-Processing Master Agreements Authorized Signer	Only for HUD 11702 signatories. Edit, submit, and certify Master Agreement documents and data required by Ginnie Mae	<ul style="list-style-type: none"> Authorized GinnieNET Signer eNotification User SecurID Token Holder MAMS Issuer Access 		<ul style="list-style-type: none"> GMEP2 User Issuer
HECM-Financial Statements User	Submit annual audited financial statements for review by Ginnie Mae's IPA.	<ul style="list-style-type: none"> eNotification User Upload & Exception Feedback User 		<ul style="list-style-type: none"> GMEP2 User Issuer
HECM-Special Loans User	Upload and process SCRA reimbursement requests.	<ul style="list-style-type: none"> eNotification User SCRA User 		<ul style="list-style-type: none"> GMEP2 User Issuer
HECM-Participation Agent	Third Party Participation Agent; performs all monitoring and accounting activities related to pooled participations on behalf of a HECM Issuer.	<ul style="list-style-type: none"> Upload & Exception Feedback User eNotification User HMBS User MAMS Participation Agent Access 	HECM Issuer	<ul style="list-style-type: none"> GMEP2 User Issuer

Table 8 HECM Roles Access

6.2.4 Subservicer Functional Roles

Functional Role	Description	RFS/GMEP 1.0	GinnieNET	MyGinnieMae
SS-Compliance and Oversight User	Review portfolio servicing and investor reporting metrics and reports; oversee subservicer performance when applicable.	<ul style="list-style-type: none"> IOPP Issuer Access GPADS User eNotification User Pool Accounting User 		<ul style="list-style-type: none"> GMEP2 User ISSUER
SS-Special Loans User	Upload and process SCRA reimbursement requests.	<ul style="list-style-type: none"> eNotification User SCRA User 		<ul style="list-style-type: none"> GMEP2 User ISSUER
SS-SF Processing Master Agreements Authorized Signer	Only for HUD 11702 signatories. Edit, submit, and certify Master Agreement documents and data required by Ginnie Mae for the employed by Organization. To approve, reject or view any HUD 11707 - servicing agreement between the Issuer and a Subcontract servicer shall be subject to and subordinate to the Guaranty Agreement between the Issuer and Ginnie Mae. This functional Role supports Single Family Issuer (SF).	<ul style="list-style-type: none"> eNotification User SecurID Token Holder MAMS Subservicer Access Authorized GinnieNET Signer MAMS Issuer Access 		<ul style="list-style-type: none"> GMEP2 User ISSUER
SS-MF Processing Master Agreements Authorized Signer	Only for HUD 11702 signatories. Edit, submit, and certify Master Agreement documents and data required by Ginnie Mae for the employed by Organization. To approve, reject or view any HUD 11707 - servicing agreement between the Issuer and a Subcontract servicer shall be subject to and subordinate to the Guaranty Agreement between the Issuer and Ginnie Mae. This functional Role supports Multifamily Issuer (MF).	<ul style="list-style-type: none"> eNotification User SecurID Token Holder MAMS Subservicer Access Authorized GinnieNET Signer MAMS Issuer Access 		<ul style="list-style-type: none"> GMEP2 User ISSUER

Functional Role	Description	RFS/GMEP 1.0	GinnieNET	MyGinnieMae
SS-HECM Processing Master Agreements Authorized Signer	Only for HUD 11702 signatories. Edit, submit, and certify Master Agreement documents and data required by Ginnie Mae for the employed by Organization. To approve, reject or view any HUD 11707 - servicing agreement between the Issuer and a Subcontract servicer shall be subject to and subordinate to the Guaranty Agreement between the Issuer and Ginnie Mae. This functional Role supports HECM Issuer (HECM).	<ul style="list-style-type: none"> eNotification User SecurID Token Holder MAMS Subservicer Access Authorized <i>GinnieNET</i> Signer MAMS Issuer Access 		<ul style="list-style-type: none"> GMEP2 User ISSUER

Table 11 Subservicer Roles Access

6.2.5 Document Custodian Functional Roles

Functional Role	Description	RFS/GMEP 1.0	GinnieNET	MyGinnieMae
DC-Pool Certification Basic User	View Schedule of Pooled Mortgages submitted; review pool and loan files for compliance with Ginnie Mae pool certification standards; cannot certify pools or loan packages.	eNotification User	Custodian	<ul style="list-style-type: none"> • GMEP2 User • Document Custodian
DC-Pool Certification and Collateral Release Management Authorized Signer	Only for HUD 11702 Signatories. All the rights of a Pool Certification Basic User, plus; authority to submit initial certification, final certification, and recertification; authority to process releases of pool and/or loan files electronically via Ginnie Mae systems.	<ul style="list-style-type: none"> • eNotification User • SecurID Token Holder • Authorized GinnieNET Signer 	Custodian	<ul style="list-style-type: none"> • GMEP2 User • Document Custodian
DC-Management and Oversight	Oversee document review and pool certification procedures; Access, submit the Master Agreement documents and data as required by Ginnie Mae; serve as an Organization Administrator for My Ginnie Mae.	<ul style="list-style-type: none"> • eNotification User • MAMS Document Custodian user • SecurID Token Holder 		<ul style="list-style-type: none"> • GMEP2 User • Document Custodian
DC-Transfer Specialists	Monitor and manage pool transfer activities to ensure successful relocation of collateral files.	<ul style="list-style-type: none"> • eNotification User • PTS Document Custodian Report Access 		<ul style="list-style-type: none"> • GMEP2 User • Document Custodian

Table 9 Document Custodian Roles Access

6.2.6 Depositor Functional Roles

Functional Role	Description	RFS/GMEP 1.0	GinnieNET	MyGinnieMae
Depositor	A primary dealer (Dealer Investor) who allocates seasoned or new pools (MBS or older Platinum's) into a larger pool. The Depositor trades the Platinum on the Secondary Market.			<ul style="list-style-type: none">• GMEP2_User• Depositor• Platinum_Submit

Table 10 Depositor Roles Access

6.3 MyGinnieMae Portal Dictionary

The MyGinnieMae Portal Dictionary is a reference resource for End Users, Organization Administrators and Operations Administrators. 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](#).

7 QUICK REFERENCE CARDS

7.1 Registering for an Account in MyGinnieMae QRC

This QRC demonstrates how to log into MyGinnieMae using a security feature called One-Time PIN (OTP).

COMPLETING THE REGISTRATION FORM

Users will receive an email inviting them to register in MyGinnieMae with the subject line “Welcome to MyGinnieMae Registration”.

1. Select the link in the email to access the form

NOTE: REGISTRATION LINK IS ONLY ACTIVE FOR 24 HOURS.

2. Fill out the **Additional Information** on the New User Registration Form:

- Work Phone Number
- Mobile Phone Number (optional)
- Title
- Password
- Confirm Password
- RSA Token Serial Number (if applicable)

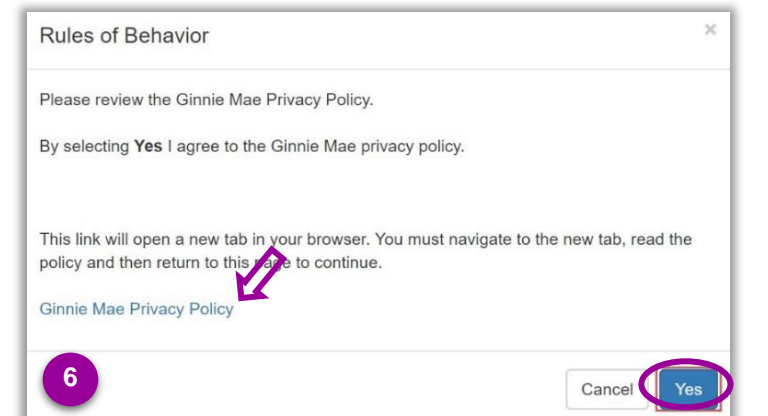
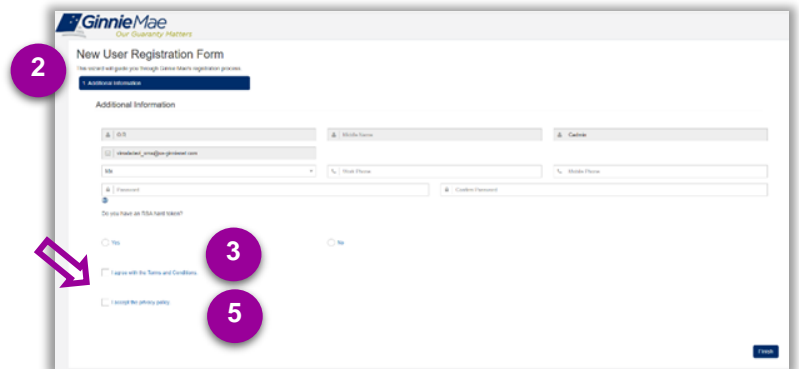
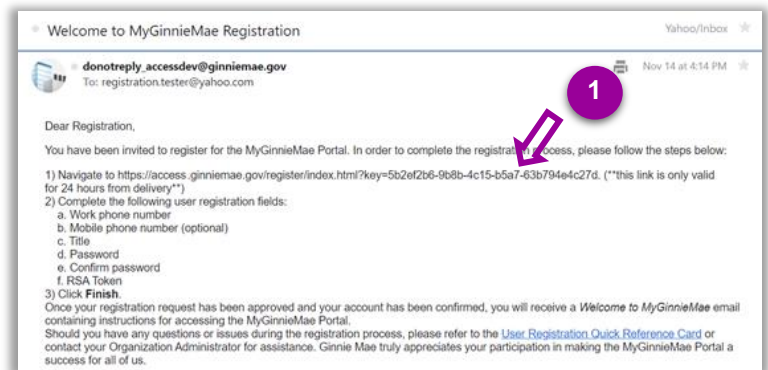
3. Select either the hyperlink that says “**I agree with the Terms and Conditions**” or check the box next to it.

4. A pop-up box will appear and display **Ginnie Mae’s Rules of Behavior**. Review the text, scroll to the bottom, and select **Yes (Agree)** to accept the Rules of Behavior.

The “I agree with the Terms and Conditions” checkbox is now checked on the New User Registration Form.

5. Select either the hyperlink that says, “**I accept the privacy policy**” or the check box next to it (See QRC Step 3 image).

6. A pop-up box will appear and display a link to the Ginnie Mae Privacy Policy. Select the link,



review the text and select **Yes** to accept the privacy policy.

The “I accept the privacy policy” checkbox is now checked on the New User Registration Form.

7. Select **Finish**.

The registration request is complete and awaiting approval.

Once the request has been approved, a **Welcome Email** will be sent to the email address provided and MyGinnieMae can be accessed using the Username (email address) and Password.

7.2 Logging into MyGinnieMae QRC

This Quick Reference Card (QRC) has been created to help users log into MyGinnieMae, One-Time PIN (OTP) entry and navigation to the business applications.

1. Navigate to <https://my.ginniemae.gov> to access MyGinnieMae.
2. Select **Login**.



3. On the **MyGinnieMae Login** page complete the following:
 - o Enter **Username** (email address).
 - o Enter **Password**.



4. Select **Login**.

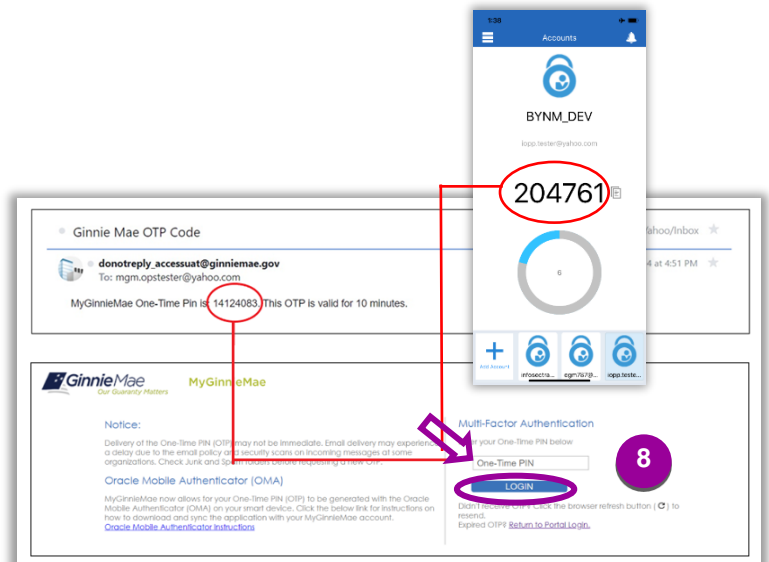
NOTE: IF YOU ARE NOT ABLE TO LOG IN OR HAVE FORGOTTEN YOUR PASSWORD, SELECT **FORGOT PASSWORD** AND FOLLOW INSTRUCTIONS

5. The Multi-Factor Authentication Page will display. Users enrolled with the Oracle Mobile Authenticator (OMA) will be prompted to select to receive a PIN to their email or via OMA.
6. Select **OK**.



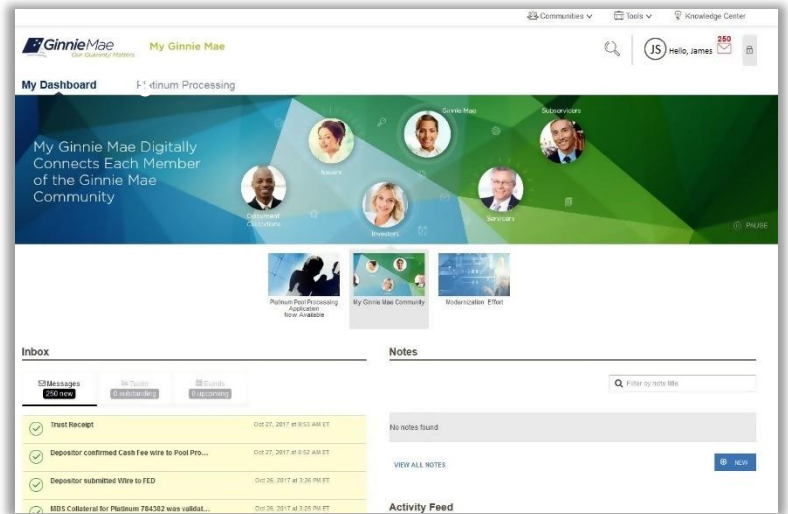
NOTE: FOR EMAIL, THE OTP WILL BE VALID FOR 10 MINUTES. ONCE 10 MINUTES HAS ELAPSED, A NEW OTP WILL BE REQUIRED. FOR OMA, OTP WILL REGENERATE EVERY 30 SECONDS. THE USER MUST ENTER THE OTP CURRENTLY DISPLAYING.

7. Enter the OTP received through email or generated by the OMA
8. Select **Login**.



NOTE: IF YOU REQUESTED OTP VIA EMAIL AND DID NOT RECEIVE OTP, SELECT THE BROWSER REFRESH BUTTON TO GENERATE A NEW PIN. IF THE OTP HAS EXPIRED OR A SYSTEM ERROR DISPLAYS, CLOSE THE BROWSER AND LOG IN AGAIN TO GET A NEW OTP.

9. The MyGinnieMae **My Dashboard** landing page will display. My Dashboard has been tailored for different user types to provide easier access to key information and applications.



BUSINESS APPLICATION LOGIN

Complete the following steps to access business applications on MyGinnieMae.

1. From **My Dashboard**, user can select the desired application from the tabs following My Dashboard (above the marquee).
2. For all other system applications select the **Tools** drop-down from the top of the page to display a list of the business applications that your account can access based on your roles.



3. Select the **Business Application** that you would like to access.



4. The first time a user selects a GMEP 1.0/GinnieNET application, a one-time dialog window will be displayed. Choose **Select** and then pick the default user ID. Users will not be prompted on future times accessing the application.



NOTE: IF MORE THAN ONE USER ID DISPLAYS, CONTACT YOUR ORGANIZATION ADMINISTRATOR FOR ASSISTANCE.

7.3 Changing a Password in MyGinnieMae QRC

MyGinnieMae requires that each user's portal password be reset every 90 days. Users will receive a daily automated reminder beginning 10 days before the current password expires. Users should follow the instructions in this Quick Reference Card to change their password prior to expiration. Once the password expires, the user will be required to change their password on their next logon.

CHANGING A PASSWORD

Log in to MyGinnieMae via <https://my.ginniemae.gov>

1. Select the Display Name in the Global Navigation Header in the top-right of the page.
2. Select **Edit My Profile** at the bottom of the Profile Box.
3. Go to the **Account** tab.
4. Select **Change Security Settings**.
5. The system will direct to the Change Password page.

NOTE: THIS PAGE WILL 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.

6. Enter your current password, new password and confirm new password and select "Submit."

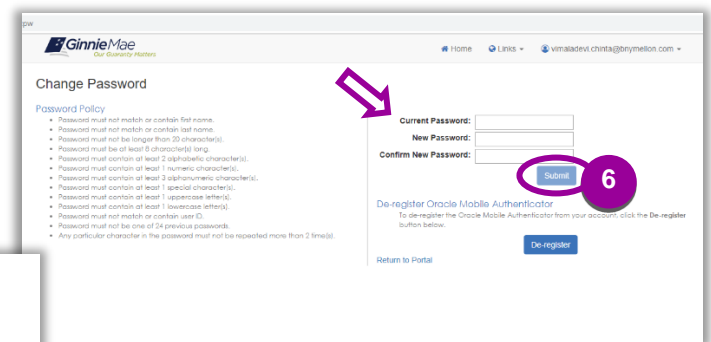
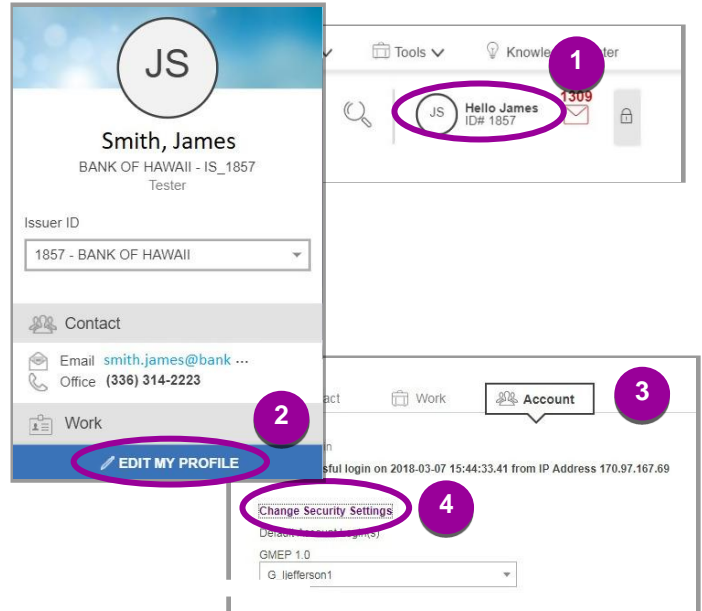
NOTE: A valid password must meet the following requirements.



Password Policy

- Password must not match or contain first name.
- Password must not match or contain last name.
- Password must not be longer than 20 character(s).
- Password must be at least 8 character(s) long.
- Password must contain at least 2 alphabetic character(s).
- Password must contain at least 1 numeric character(s).
- Password must contain at least 3 alphanumeric character(s).
- Password must contain at least 1 special character(s).
- Password must contain at least 1 uppercase letter(s).
- Password must contain at least 1 lowercase letter(s).
- Password must not match or contain user ID.
- Password must not be one of 24 previous passwords.
- Any particular character in the password must not be repeated more than 2 time(s).

7. You will receive a confirmation email that your password has been changed.



7.4 Forgot Password in MyGinnieMae QRC

This Quick Reference Card (QRC) guides MyGinnieMae users on how to use the Forgot Password link on the Login page, to create a new portal password in the event this user is unable to recall their portal password.

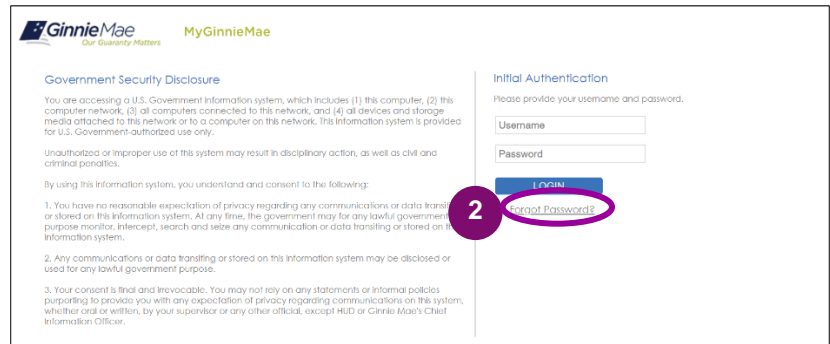
FORGOT PASSWORD

Log in to MyGinnieMae via <https://my.ginniemae.gov>

1. Select the **Login** button.



2. The system will direct to the MyGinnieMae Login page. Select **Forgot Password?**



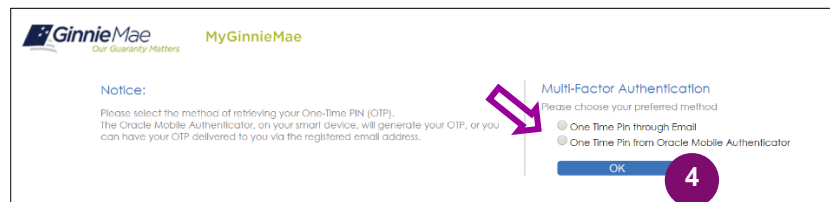
3. The system will prompt the user for their Username.

- Enter the **Username**
- Select **LOGIN**.



4. The Multi-Factor Authentication page will display. Users enrolled with the Oracle Mobile Authenticator (OMA) will be prompted to select to receive a PIN to their email or via OMA.

- Choose the preferred method.
- Select **OK**



NOTE: IF THE USER HAS NOT ENROLLED WITH THE ORACLE MOBILE AUTHENTICATOR (OMA), THEN THEY WILL AUTOMATICALLY BE DIRECTED TO THE PAGE WHERE THEY ARE PROMPTED TO ENTER THE OTP THAT HAS BEEN EMAILED TO THEM.

5. Enter the **One-Time PIN**, delivered via email or generated by the OMA, and select **LOGIN**.

GinnieMae MyGinnieMae
Our Guaranty Matters

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.

Multi-Factor Authentication
Enter your One-Time PIN below

One-Time PIN

LOGIN 5

Didn't receive OTP? Click the **Forgot OTP?** button (🔍) to resend.
Expired OTP? [Return to Portal Login.](#)

6. The Reset Password page will appear.
- Enter a **New Password**
 - Then **Confirm New Password**.
 - Select **Submit**.

GinnieMae MyGinnieMae
Our Guaranty Matters

Password Policy

- Password must not match or contain first name.
- Password must not match or contain last name.
- Password must not be longer than 20 character(s).
- Password must be at least 8 character(s) long.
- Password must contain at least 2 alphabetic character(s).
- Password must contain at least 1 numeric character(s).
- Password must contain at least 3 alphanumeric character(s).
- Password must contain at least 1 special character(s).
- Password must contain at least 1 uppercase letter(s).
- Password must contain at least 1 lowercase letter(s).
- Password must not match or contain user ID.
- Password must not be one of 24 previous passwords.
- Any particular character in the password must not be repeated more than 2 time(s).

Reset Password
Please enter and confirm your new password.

New Password:

Confirm New Password:

Submit 7

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

GinnieMae MyGinnieMae
Our Guaranty Matters

Successful Password Change

Your password change was successful.
Redirecting you to the MyGinnieMae Portal site.

OK 8

8. The Login Page will display, the user may login using the new password.
- Enter **Username**
 - Enter **Password**
 - Select **LOGIN**.

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 9

[Forgot Password?](#)