MyGinnieMae Portal
Organization Administrator Training
Onboarding End Users

V 1.1
TRAINING AGENDA

• Objectives
• Overview
  – What is MyGinnieMae?
  – Why the Change?
  – How is it changing?
  – Roles & Responsibilities
• Getting Started
  – Registering for your individual account
  – Access Management Console
• Live Demo
  – Registration Requests & Approvals
  – Access Requests and Approvals
• Troubleshooting
• Preparing for Onboarding End Users
  – Requirements
  – Tips
  – What’s Next
• Q&A
The objective of this training is to provide Organization Administrators with the following:

- High-level overview of general portal features
- Instructions on how to register for your individual portal account
- Guidance on how to prepare for onboarding your End Users
- Instructions on onboarding End Users
- Information on troubleshooting and getting help
The MyGinnieMae portal provides **enhanced security** and a **single entry-point** to all approved applications for individual users. This means, **one account with one** single username and password will provide users access to all systems, applications and Organization IDs/Issuer IDs.
OVERVIEW-MYGINNIEMAE WHY THE CHANGE?

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. This includes:

- **Single Sign-On:**
  - Provides seamless access to business applications using a single ID and One-Time Pin (OTP)

- **Multi-Factor Authenticator:**
  - A One-Time Pin (OTP) sent to the user’s email or via Oracle Mobile Authenticator when accessing a secured application

- **Functional Roles:**
  - A set of entitlements grouped by business function, with the intention of providing least privilege access

- **Invitation Model:**
  - Credentials set securely by the End User. Then, the onboarding workflow continues with access requests and approvals controlled by Organization Administrator’s access and segregation of duties
# Overview

## How is it changing?

### Legacy Environment

<table>
<thead>
<tr>
<th>GMEP 1.0 and GinnieNET</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LEGACY ENVIRONMENT</strong></td>
</tr>
<tr>
<td>Ginnie Mae Admins provide access to users</td>
</tr>
<tr>
<td>Issuers provided system access to their subservicer’s users</td>
</tr>
<tr>
<td>Go directly to access legacy systems to login</td>
</tr>
<tr>
<td>Username and password required</td>
</tr>
<tr>
<td>Access identified by applications and system</td>
</tr>
<tr>
<td>Separate username and password for each system</td>
</tr>
<tr>
<td>Password and user profile management performed by Ginnie Mae Admins</td>
</tr>
</tbody>
</table>

### Modernized Environment

<table>
<thead>
<tr>
<th><strong>MODERNIZED ENVIRONMENT</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Administrator at each organization provide access to users</td>
</tr>
<tr>
<td>Subservicers have their own Org Admins and manage their employee users</td>
</tr>
<tr>
<td>Login through MyGinnieMae to access legacy systems and modernized applications</td>
</tr>
<tr>
<td>Also requires a One-Time PIN (OTP)</td>
</tr>
<tr>
<td>Role privileges determined by a business function</td>
</tr>
<tr>
<td>One username and one password; same for RSA</td>
</tr>
<tr>
<td>Self service features to reset password, manage password, register, and update the user profile</td>
</tr>
</tbody>
</table>
**Organization Administrators** are privileged users who control system access, assign functional roles, and perform other user management activities. These individuals are responsible for ensuring that End Users at their respective organizations are provided the appropriate level of access for their business role with Ginnie Mae. They were formerly known as Security Officers and Enrollment Administrators.

<table>
<thead>
<tr>
<th>User Type</th>
<th>Responsibility / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations Administrator</td>
<td>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. This function is provided by BNYM Operations on behalf of Ginnie Mae, with Ginnie Mae Information Security serving as the Super Administrator over the entire system.</td>
</tr>
</tbody>
</table>
| Organization Administrator | Organization Administrators have the privilege to invite end users to register for a Portal account, approve user registration, initiate access request via functional role assignment to user and approve the access request within a single organization. Formerly known as Security Officers and Enrollment Administrators.  
Note: Separation of duties within the registration and access request workflows does not allow the Organization Administrator to initiate a registration and approve that same registration nor request access via functional role assignment and approve that same access request. A minimum of two Organization Administrators are required and it is recommended to have more than the minimum from an operational perspective. |
| End User             | End Users are the various types of Ginnie Mae employees, business partners, and contractors who require access to the business applications and information within the Portal, including various self-service functions. |
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, Multi-Family, HECM, etc.).

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Role Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SF-Loan Delivery and Pooling Basic User</td>
<td>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.</td>
</tr>
<tr>
<td>SF-Loan Delivery and Pooling Authorized Signer</td>
<td>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.</td>
</tr>
<tr>
<td>MF-Investor Reporting Basic User</td>
<td>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.</td>
</tr>
<tr>
<td>MF-Investor Reporting Authorized Signer</td>
<td>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.</td>
</tr>
<tr>
<td>HECM-Compliance and Oversight User</td>
<td>Review portfolio servicing and investor reporting metrics and reports; oversee subservicer performance when applicable.</td>
</tr>
<tr>
<td>SS-Investor Reporting Basic User</td>
<td>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.</td>
</tr>
</tbody>
</table>
## ORG ADMIN ROLE PRIVILEGES

MyGinnieMae introduces self service functions and additional controls for administrators at each organization. This chart highlights some of those functions.

<table>
<thead>
<tr>
<th>Function</th>
<th>Self Service</th>
<th>Organization Administrator</th>
<th>Operation Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiate registration invitations to End Users</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approve or reject registration requests from End Users</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initiate access request/functional role for an End User account</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approve or reject functional role for an End User account</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove a functional role from an End User account</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable/Disable and Lock/Unlock End User accounts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forgot Password</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reset Password</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deregister Oracle Mobile Authenticator access</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update Account Attributes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Final acknowledgement of access requests</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
NEW USER REGISTRATION

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

1. Select the link to register. Note registration link is only active for 24 hours.

For questions or issuers with the registration link or process, please contact your Organization Administrator.

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 (Yes/No)

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

4. A pop-up box will appear and display Ginnie Mae’s “Rules of Behavior”. Review the text, then 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. When the message box displays, click on “Ginnie Mae Privacy Policy” link to review the text and click Yes.

6. Once the Privacy Policy and Terms and Conditions have been accepted, select Finish.
   - User registration request is complete. Once the request is approved and access is granted, a Welcome Email will be sent to the email address provided and the MyGinnieMae Portal can be accessed using the enterprise ID (email address) and password.
The Access Management Console (AMC) is the user interface module for Organization Administrators to create new End User accounts, grant End Users access to Ginnie Mae business applications via functional role assignment and manage existing End User accounts for the Organization ID(s) they manage.

The following steps outline how to enter the Access Management Console (AMC)

1. Select the “Tools” drop-down menu at the top of the screen and select “Access Management Console”.

2. Select “Yes”, when prompted to and open AMC within this existing MyGinnieMae Portal window

3. The system will then open the AMC in a new window.
Onboarding is a multi-step process that may take several days to complete and requires participation from the End User, Organization Administrators, and Ginnie Mae.

- **Registration Workflow** – creates a portal account and gives users access to the portal.
- **Access Workflow** – assigns functional role(s) and gives users access to business applications.

---

**Legend**

- ![System Generated Audit Report](image)
- ![System Triggered Notification](image)

*Email invitation link expires within 24 hours
**Approver cannot be the requestor

**NOTE:** Org Admins are expected to know the access and end user needs.
LIVE DEMO
Registration Request and Approval
&
Access Request and Approval
TROUBLESHOOTING REGISTRATION INVITATION

Three different errors may appear in the AMC when sending an invitation to an End User:

- **Email is Already Registered Issue**: When sending a New User Registration invitation to an End User, if an email address is already registered, an invitation cannot be sent to that user.

- **Resolution**: Since the system is configured to prevent invitations to email addresses already registered. If attempting to add a functional role, please refer to Section: Request Functional Role.
• **Three Invitations Sent Alert Issue**: When sending a New User Registration invitation to an End User, if an invitation has already been sent to the user’s email address three times, an alert will be displayed as a warning. An invitation can only be sent a total of five times.

• **Resolution**: This is a warning message. No action is required as an invitation can be sent up to five times.
• **Five invitations Sent Flag Issue**: When sending a New User Registration invitation to an End User, if an invitation has already been sent to the user’s email address a total of five times, the email address will be flagged, and additional requests cannot be sent.

• **Resolution**: In order to send another invitation to the user’s email address, action is required from the Operations Administrator group.
PREPARING ONBOARDING END USERS

The following information will help the organization and its Users prepare for the onboarding process.

ORG ADMIN REQUIREMENTS

- Minimum of **2 Org Admins** is required per Org ID (per MBS Guide). 3+ suggested.
- User must be listed on **Form HUD 11702** to be provided Org Admin privileges.
- Org Admins are not permitted to manage their own account registration or access.

SYSTEM REQUIREMENTS

- MyGinnieMae can be accessed using one of the following supported web browsers—Google Chrome 42+, Internet Explorer 11.x, and Mozilla Firefox 31+.
- Web browser pop-up blockers must be **disabled**.
ONBOARDING END USERS

The following information will help the organization and its Users prepare for the onboarding process.

USER INFORMATION REQUIRED

Org Admins should become familiar with **Functional Roles**. A table of Functional Roles and their descriptions is available in the Appendix of the MyGinnieMae Getting Started Manual.

Org Admins will need the following information to send a Registration Invitation to New End Users:

- Display Name (Should match the HUD 11702 for Authorized Signers)
- Email Address
- Issuer Name(s)
- Issuer ID(s)
- Job Title
- Telephone Number (optional)
- RSA Token (optional)

If “Yes”, the RSA Token Number must be added to the User’s new MyGinnieMae account.

OTHER TIPS

- Do not send registration invitations to users that are out of the office.
- Do not bookmark the Login Page, instead bookmark is the Public Landing Page at [https://my.ginniemae.gov](https://my.ginniemae.gov)
- Refer to the manuals on GinnieMae.gov
PREPARING WHAT’S NEXT?

Org Admins will receive an email invitation to register for a MyGinnieMae account
RESPOND WITHIN 24 HOURS
If unable to respond, contact Ginnie Mae Customer Support

Onboard the End Users at your organization by the Target Date
See Release & Training Schedule

Encourage End Users to attend MyGinnieMae Training
See Release & Training Schedule

Join Thursday Weekly Listening Sessions to ask questions and learn best practices

Check the Modernization Page often on GinnieMae.gov

Contact Ginnie Mae Customer Support if you require assistance
1-833-GNMA HELP / 1-833-466-2435
ginniema1@bnymellon.com