TRAINING AGENDA

• Objectives
• Overview
• User Management
  – Review Status of Access Request
  – Add/Remove Functional Role
  – Update a User’s Profile Attributes
  – Unlock/Lock a User Account
  – Enable/Disable a User Account
  – Reset a User’s Password
• Troubleshooting
• Reports
• Resources
• Q&A
The objective of this training is to provide Organization Administrators with the following:

- Guidance on how to review the status of an account access request
- Information about End User account management functions
- Information on troubleshooting and getting help
- Overview of reports available via the Access Management Console (AMC)
Onboarding an End User is a multi-step process that may take several days to complete and requires participation from the End User, Organization Administrators, and an Operations Administrator.

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

**OVERVIEW ONBOARDING WORKFLOW**

**REGISTRATION**

- Requesting Org Admin
- End User
- User Completes Registration Form
- Submit Form
- Approving Org Admin
- Org Admin #1

**ACCESS**

- Requesting Org Admin
- Approving Org Admin
- Org Admin #1
- Org Admin #2

Legend

- System Generated Audit Report
- System Triggered Notification

*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.
**OVERVIEW ORG ADMIN CONTROLS**

MyGinnieMae introduces self-service functions for End Users and provides account management controls for Organization Administrators at each organization. This chart highlights some of those functions and responsibilities.

<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>
The User Management Tile in the Access Management Console (AMC) is where Organization Administrators go to manage existing End User accounts for their organization.
Once an access request is submitted, the system adds the Functional Role to the user’s profile with a status of “Pending.” The role is not provisioned to the user until necessary approvals are completed. To review the status of a Functional Role request for a user, follow the steps below. See the AMC User Manual for more information.

- After selecting the desired user, find the arrow next to “Manage User Permissions” to open the accordion.

- The system displays the assigned Functional Role(s) with the status of the request:

  - **PENDING** – The Functional Role request is submitted and awaiting Organization Administrator approval.
  
  - **APPROVED** – The Functional Role is approved and awaiting Operations Administrator action.
  
  - **FINALIZED** – The Functional Role request has been Finalized by the Operations Administrator.
  
  - **CONFIRMED** – the underlying roles have been fully assigned to the user.

- Clicking on the Role Name reveals the Role Status overlay. The overlay contains information about the user’s Functional Roles, including Request Date, Requester, Approval Date, Approver, Finalized Date, Finalizer and Status.
If an End User requires a new functional role, this may be done from the User Management Tile in AMC within the Edit User Profile Section. This request would subsequently have to be approved by another Org Admin and finalized by the Operations Admin.

![User Management Interface](image)
If an End User no longer requires access to a specific Functional Role, possibly because their business responsibilities have changed, Organization Administrators are responsible for removing that role from the user’s account. This may be done within the Manage User Permissions section.
The following fields may be updated/changed for a user's account: **Title, Suffix, Mobile Number, Work Number, Extension, Job Title and RSA Token**. If not completed during New User Registration, Org Admins are responsible for adding the RSA Token to the token holder’s profile attributes and following up with an email to the Operations Administrator.
A user can become automatically locked out of their account due to 3 failed password attempts or if an Organization Administrator has manually locked the account via the AMC. Locking a user’s account is a temporary action and can be reverted.
USER MANAGEMENT  **ENABLE/DISABLE ACCOUNT**

A user’s account may become automatically disabled due to 90 days of inactivity. Enable the account and advise the user to login to MyGinnieMae within 24 hours once their account has been enabled, or the account will automatically be disabled again.

Org Admins should manually disable a user’s account if the user has left the organization or for other organization specific reasons (such as a change in role).

The Org Admin should wait for the successful action ribbon to display to ensure that actions have been completed.

User JOHN E.JONES@BANK.COM successfully enabled.
This service is used in an event that a user has forgotten their password and is unable to reset it using self-service capabilities, or they suspect their account has been compromised.

The **Reset Password** button is inactive if the user’s account is disabled. The account would need to be enabled prior to resetting the password.
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.
**TROUBLESHOOTING REGISTRATION INVITATION**

- **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.
The AMC provides Organization Administrators an audit trail and additional insight into the user accounts for their organization in Ginnie Mae business systems. These reports capture logs and event data for various identity and access management events.

The following reports are available to Org Admins via the AMC:

<table>
<thead>
<tr>
<th>Service</th>
<th>Reports</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Registration</td>
<td>Home Organization User List Org Admin View</td>
<td>Custom</td>
</tr>
<tr>
<td></td>
<td>User Profile History</td>
<td>Standard</td>
</tr>
<tr>
<td></td>
<td>User Registration Request History</td>
<td>Custom</td>
</tr>
<tr>
<td>Access Requests</td>
<td>AMC Functional Role Request History</td>
<td>Custom</td>
</tr>
<tr>
<td>Multifactor Authentication (MFA)</td>
<td>Accounts Locked Out Report</td>
<td>Standard</td>
</tr>
<tr>
<td></td>
<td>Authentication Statistics Report</td>
<td>Standard</td>
</tr>
<tr>
<td>Self-Service Change Password</td>
<td>Password Expiration Summary</td>
<td>Standard</td>
</tr>
</tbody>
</table>
From the AMC Security Reports tab the system will open ORACLE BI Publisher Enterprise in a new window.

1. Select Catalog Folders
2. Select Shared Folders
3. Select Administrative Reports
4. Select Open under the desired report
The AMC Functional Role Request History report contains the request history for functional roles for each user. The report displays the Request ID, User Login, Function Role Name, Functional Role Type, Organization Key, Functional Role Status, Requester, Request Date, Approver, Approval Date, Finalizer, Finalized Date, Revoker and Revoked Date fields.

The report can be filtered and sorted by selecting the drop-down arrow in the column heading.
**REPORTS TIPS**

**How to download, and save reports**

Once the report is opened from ORACLE BI Publisher Enterprise it will appear in the same window.

1. Select the **View** icon.
2. Select the **Excel** option (or other file type if needed).
3. Your browser will download the file and allow you to open and save it.

**How to create a list of active user accounts**

From the ORACLE BI Publisher Enterprise Administrative Reports folder:

4. Select **Open** to view the **Home Organization User List** report.
5. Once the report is opened, select the **Status** column dropdown and check **Active** box.
6. The result will display only the active user accounts.
GETTING HELP RESOURCES

• Modernization Page on GinnieMae.gov
  https://www.ginniemae.gov/issuers/issuer_training/Pages/modernization.aspx
  ✓ User Manuals (including: Access Management Console (AMC) User Manual)
  ✓ Quick Reference Cards
  ✓ Training Overviews
  ✓ Release and Training Schedule
  ✓ Training materials and recordings

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

• For technical questions about accessing the portal and using its applications contact Ginnie Mae Customer Support at 1-833-GNMA HELP / 1-833-466-2435 or ginniemae1@bnymellon.com

• For questions about, training, user materials and general MyGinnieMae inquires contact the Ginnie Mae Customer Experience Group at cxg@hud.gov