MyGinnieMae Portal
Organizational Administrator Training

Pilot V1.1

TRAINING **AGENDA**

- **Objectives**
- **Overview**
- **Organization Administrator Role**
- **Getting Started**
  - Registering for an account
  - Logging On and Off
- **Preparing for Onboarding End Users**
- **Registration and Access Provisioning for End User Accounts**
  - Functional Roles
  - Rejecting Access
  - Review Status of Access Request
- **User Management Tasks**
  - Enable/Disable a User Account
  - Unlock/Lock a User Account
  - Update a User's Profile Attributes
  - Reset a User's Password
- **Reports**
- **Troubleshooting and System Errors**
- **Getting Help**

TRAINING **OBJECTIVES**

- **Provide a high-level overview of general portal features**
- **Provide instructions on how to register for your own portal account**
- **Provide guidance on how to prepare for onboarding your End Users**
- **Provide instructions on onboarding End Users**
- **Provide information on troubleshooting and getting help**

OVERVIEW **KEY FEATURES**

MyGinnieMae is an integral component to the Ginnie Mae modernization effort. It provides usability and features that are familiar to present day online application usage experiences. **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 password.

- **Secure Image and Phrase** – adds security by showing users their designated secure image and phrase in conjunction with the login screen.

- **One-Time Password (OTP)** – this code is sent to the user's email when accessing a secured application.

GinnieMae
Our Guaranty Matters

OVERVIEW **OTHER KEY FEATURES**

- **MyGinnieMae Access Management Console (AMC):** User friendly interface for administrators to initiate access requests, manage end users within their organization(s), and perform other administrative functions.

- **Functional Roles:** Application Access Controls presented as Functional Roles enforce security of portal access for all users and systems with a means to associate authenticated system users with applicable rights and privileges within the Portal and associated application programs.

- **Self-Service Interface:** Self-service password management through a standard web-based interface.

- **Audit Support:** 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:** Method to initiate the user registration process through an invitation that automates parts of the Registration Workflow.

ORG ADMIN ROLE **RESPONSIBILITIES**

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.

User Type	Responsibility / Description
Operations Administrator	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.
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 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 Org Admins 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.

ORG ADMIN ROLE **PRIVILEGES**

- Initiate registration invitations to End Users

- Approve or reject registration requests from End Users

- Initiate access request/functional role for an End User account

- Approve or reject functional role for an End User account

- Remove a functional role from an End User account

- Enable/Disable and Lock/Unlock End User accounts

GETTING STARTED **ACCOUNT REGISTRATION**

Each new user to the portal is sent an email invitation to register for an account in MyGinnieMae. The invitation is valid for 24 hours and has a link that directs the user to a registration form. Instructions for completing this form are contained in *QRC IS/DC-03*. https://www.ginniemae.gov/issuers/issuer_training/Documents/register_newuser_myginniema e_qrc.pdf. Once registration has approved the user will receive a system generated *Welcome Email*. The user will also receive a *New Functional Role Assignment* email for each functional role that is assigned. Shortly thereafter the user may log into the portal and begin work.

GETTING STARTED **LOGGING ON AND OFF**

Below are tips for opening, maintaining, and closing portal sessions in MyGinnieMae and Access Management Console (AMC). See Section 2: Logging On and Off in the Organization Administrator User Guide for more information.

> Do not bookmark the Login Page. The correct page to bookmark is the Public Landing Page at https://my.ginniemae.gov.

> The Access Management Console (AMC) is the user interface used by Org Admins to manage Portal user accounts. It is accessible via the Tools > Applications menu.

> The Portal does *not* recognize activity in the AMC as Portal activity. If the Org Admin is active within AMC for longer than 20 minutes the system will prompt to re-enter credentials when navigating back to the Portal.

> Signing out of AMC terminates the user's Portal session.

> The One-Time Password (OTP) is an eight-digit code which is valid for 10 minutes and is sent to the user's email address. It is required to access Business Applications within the Portal and is valid for 120 minutes.

PREPARING ONBOARDING END USERS

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

REQUIREMENTS

- Minimum of **2 Org Admins** is required per Org ID (per MBS Guide)

- User must be listed on **Form HUD 11702** to be provided Org Admin privileges

- Org Admins are not allowed to manage their own account registration or access

- The browser's pop-up blocker must disabled prior to accessing MyGinnieMae

TIPS

Org Admins should become familiar with Functional Roles. A table of Functional Roles and their descriptions is available in the Appendix of the MyGinnieMae User Manual for Organization Administrators.

Org Admins will need to know the following information in order to send a registration invitation to an End User:

- ❑ Display Name (First Last)
- ❑ Job Title
- ❑ Email Address
- ❑ Telephone Number
- ❑ Token Holder – Y/N?
- ❑ Issuer Name(s)
- ❑ Issuer ID(s)

PREPARING **FUNCTIONAL ROLES**

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.). See Section 1.2.4: Functional Roles in the Organization Administrator Guide.

Role Name	Role Description
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.
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
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; submit edits needed to clear exception feedback and monthly reporting errors.
HECM-Compliance and Oversight User	Review portfolio servicing and investor reporting metrics and reports; oversee subservicer performance when applicable.
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

REGISTRATION **EMAIL INVITATION**

- **Registration Workflow** – creates a portal account
- **Access Workflow** – assigns functional role(s)

REGISTRATION **EMAIL INVITATION**

- **Registration Workflow** – creates a portal account
- **Access Workflow** – assigns functional role(s)

REGISTRATION

ACCESS

Legend
- System Generated Audit Report
- System Triggered Notification

*Email invitation link expires within 24 hours
**Approver *cannot* be the requestor
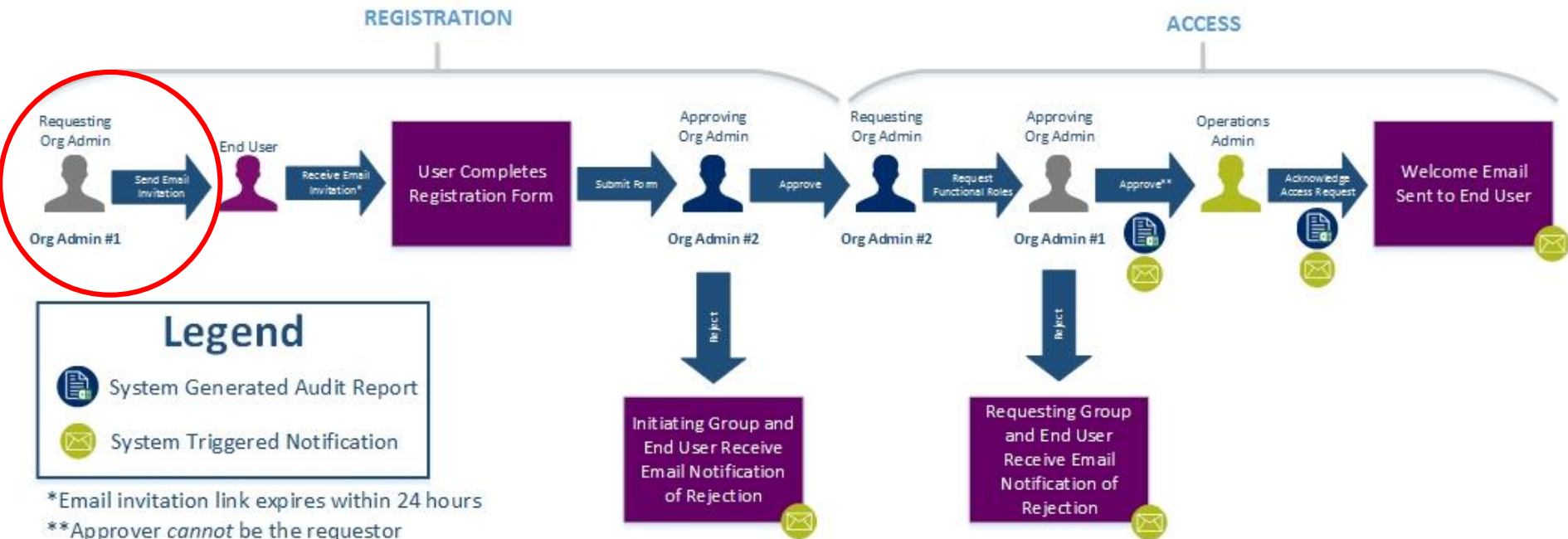
NOTE: Org Admins are expected to know the access and end user needs.

ACCESS **FUNCTIONAL ROLE REQUEST**

- **Registration Workflow** – creates a portal account
- **Access Workflow** – assigns functional role(s)

ACCESS **FUNCTIONAL ROLE APPROVAL**

- **Registration Workflow** – creates a portal account
- **Access Workflow** – assigns functional role(s)

ACCESS **FINALIZATION**

Finalization is completing by the Operation's Administrator (BNYM). The Ops Admin is notified when an End User account requires finalization. During the Early Adopter Pilot please allow 2-3 business days for this step to be complete.

LIVE DEMO
Registration Request and Approval
& Access Request and Approval
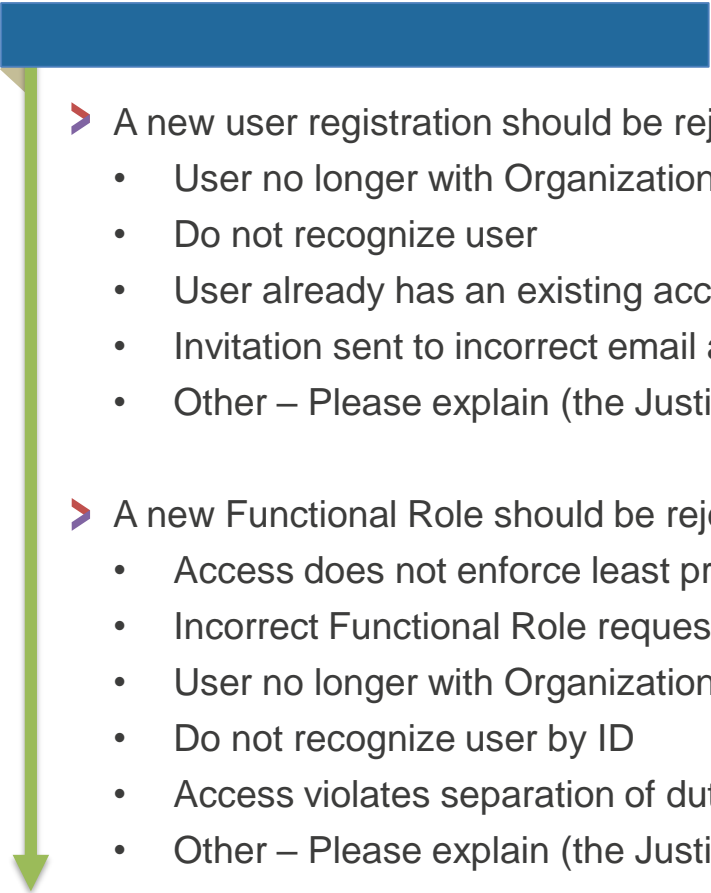
REGISTRATION **ONBOARDING TIPS**

The following notes and tips regarding sending an invitation to register for the Portal through approval of a registration request. See Sections 3.0-3.4 in the Organization Administrator User Guide for more information.

> User registration uses a self-service registration form to collection information from potential end users that is verified and used to create a new user account.

> Once the User Invitation Form is completed, an email is sent to the email address entered in the form with a unique URL that is valid for 24 hours for the End User to complete their registration.

> All Org Admins, except the one that sent the Registration Invitation, will be notified via email to approve the User Registration request once it has been completed.

> If there are multiple registration requests for the same user email, the system will only allow to approve one request record. The remaining request(s) should be rejected.

> Within the AMC Approvals screens, User Registration fields are *not* editable. If there are any errors or incorrect information the request must be rejected, and a new registration must be submitted.

GinnieMae
Our Guaranty Matters

ACCESS **REJECTING REQUESTS**

The following notes and tips regard rejecting a new user registration or functional role request. See Sections 3.12-3.13 in the Organization tor User Guide for more information.

> A new user registration should be rejected if:
>
> - User no longer with Organization
> - Do not recognize user
> - User already has an existing account
> - Invitation sent to incorrect email address
> - Other – Please explain (the Justification Description will be required)

> A new Functional Role should be rejected if:
>
> - Access does not enforce least privilege
> - Incorrect Functional Role requested
> - User no longer with Organization
> - Do not recognize user by ID
> - Access violates separation of duties
> - Other – Please explain (the Justification Description will be required)

> 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 Sections 3.14 in the Organization Administrator User Guide for more information.

> From the Access Management Console, select the "User Management" tile and select a user.

> Select the arrow next to the "Manage User Permissions" heading 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 and the underlying roles are in the process of being assigned to the user.

> Clicking on the Functional 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.
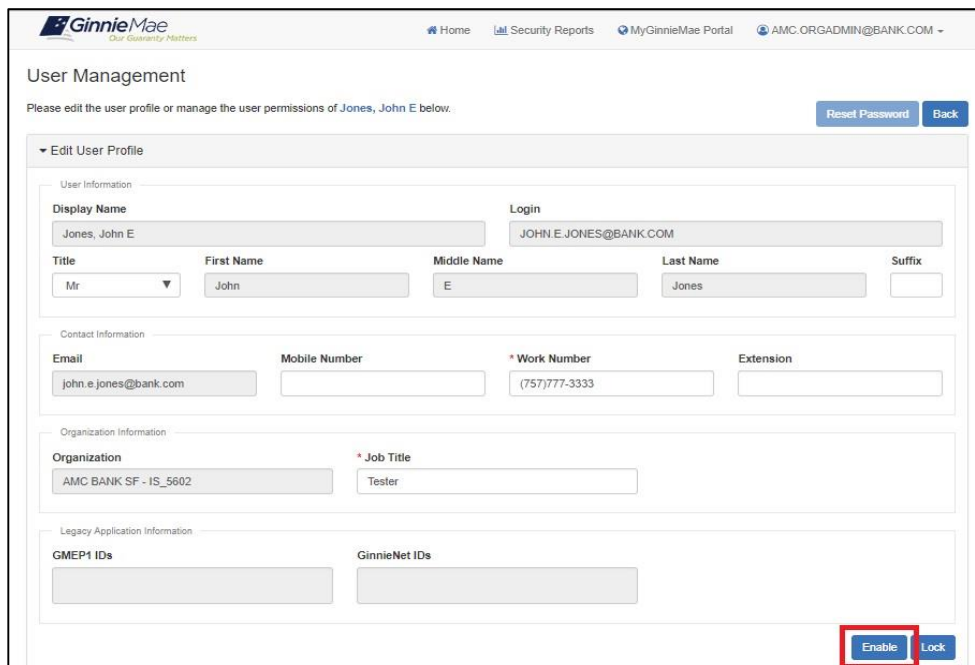
MANAGEMENT **RESTRICTING USER ACCOUNTS**

The following notes and tips regarding removing Functional Roles, disabling a user account, and locking a user account. See Sections 3.5, 3.6, or 3.8 in the Organization Administrator User Guide for more information.

> Org Admins are responsible for removing Functional Roles from users that no longer require that particular role/access.

> Org Admins are responsible for disabling a user's account from AMC if the user has left the organization or for other organization specific reasons (such as a change in role).

> Locking a user's account is a temporary action and can be reverted.

A user's account may be disabled due to 90 days of inactivity or disabled manually (due to change of job, etc.) and needs to be enabled. Advise the user to login to MyGinnieMae within 24 hours once their account has been enabled, or the account will automatically be disabled again.

> Always check to ensure the green success banner is displayed at the top of the screen once an action has been performed.

MANAGEMENT **UNLOCK/LOCK AN ACCOUNT**
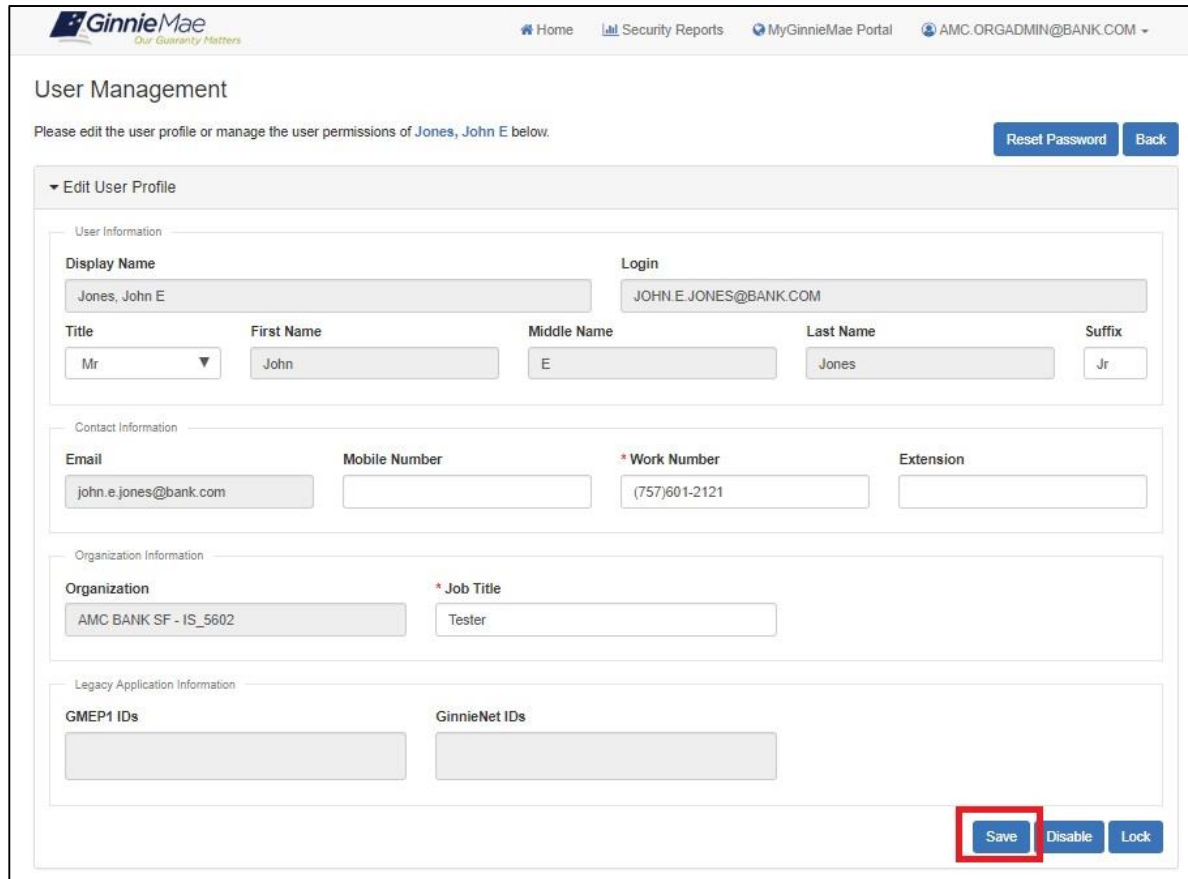
A user can become locked out of their account due to an Organization Administrator locking or three failed attempts at entering their username/password.

MANAGEMENT UPDATE PROFILE ATTRIBUTES

The following fields may be updated/changed for a user's account: Title, Suffix, Mobile Number, Work Number, Extension, Job Title.
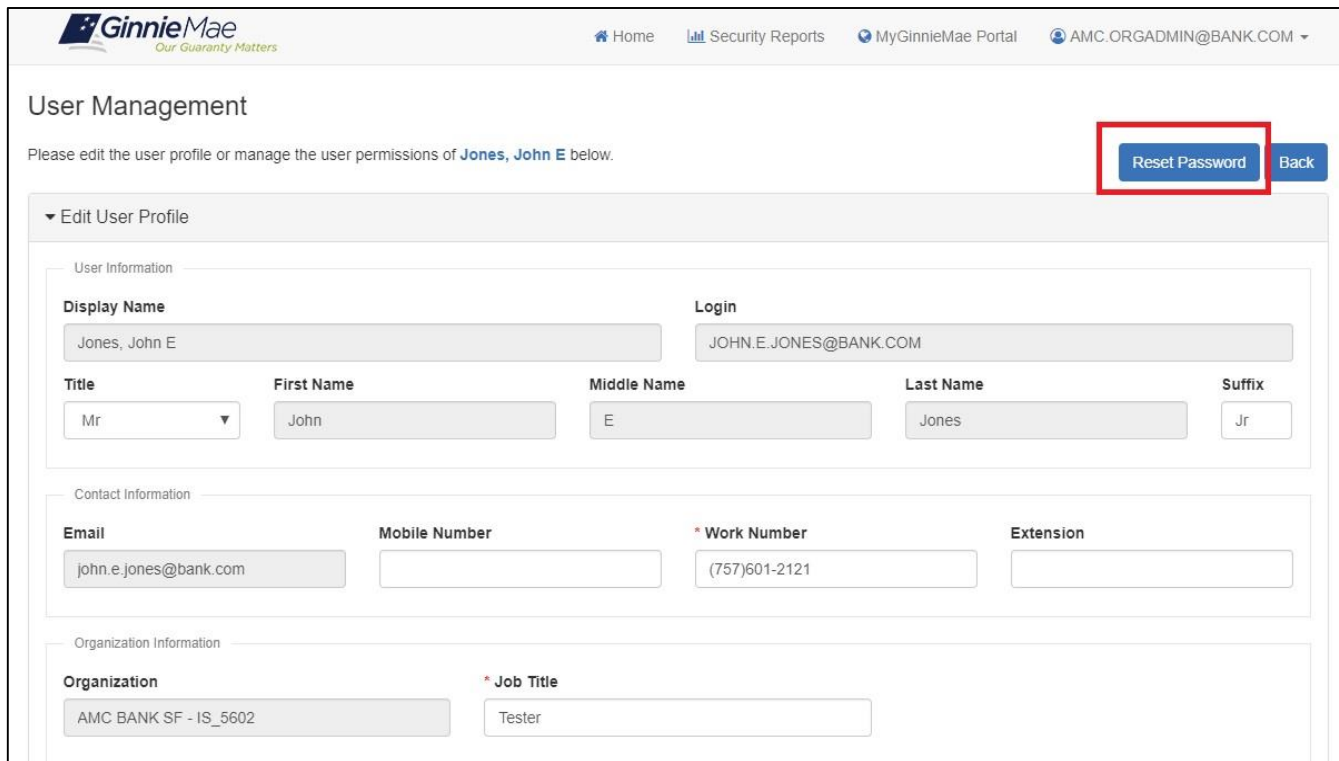
MANAGEMENT RESET A PASSWORD

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.

TROUBLESHOOTING **SYSTEM ERRORS**

The following notes and tips regard troubleshooting potential end user or system errors. See Section 4: Troubleshooting and System Errors in the Organization Administrator User Guide for more information.

> A notification ribbon appears at the top of AMC to indicate either a successful action (green text) or an error condition (red text).
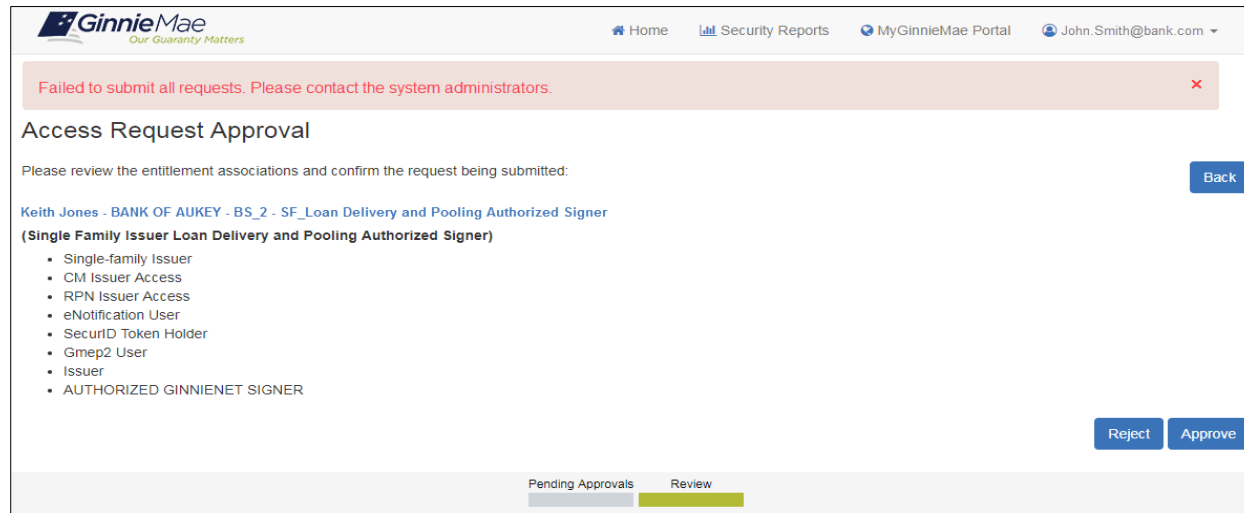
TROUBLESHOOTING **REGISTRATION INVITATION**

> Three different errors may appear when sending an invitation to an end user:

- Email is already registered
- Three invitations sent alert
- Five time invitation flag

TROUBLESHOOTING **END USER ERRORS**

> End user errors related to logging into the system may be one of the following:

- Invalid username or password
- Incorrect OTP
- OTP not received (this instance is not an error on login screens)

REPORTS **SECURITY REPORTS**

Several customized reports have been created for use by the Organization Administrators that will be placed into production prior to full onboarding. In the meantime, Organization Administrators are encouraged to use the AMC Functional Role Request History.
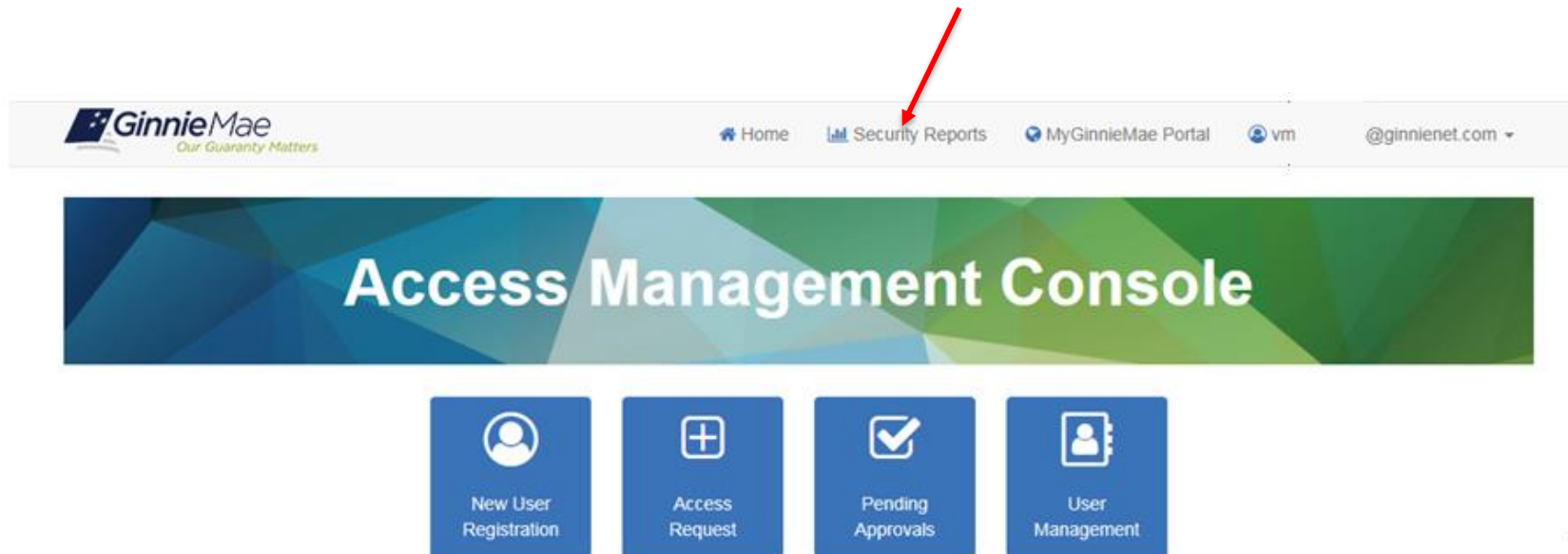
REPORTS **AMC FUNCTIONAL ROLE REQUEST HISTORY**
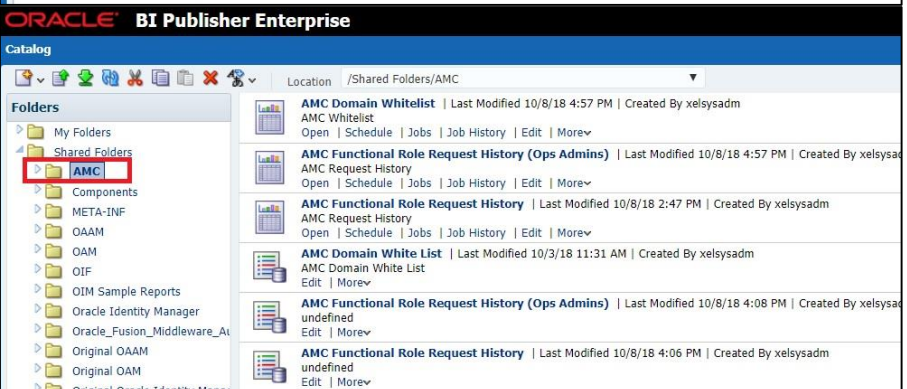
From the AMC Security Reports tab the system will open ORACLE BI Publisher Enterprise in a new window.

1. Select the **Catalog Folders** folder
2. Select the **AMC** folder
3. Select **Open** under the AMC Functional Role Request History

REPORTS AMC FUNCTIONAL ROLE REQUEST HISTORY

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.

GETTING HELP **RESOURCES**

The MyGinnieMae Organization Administrator User Manual will provide answers to most questions. It is currently located on the Modernization Page for Pilot Users. You may also reference the Portal Help link located at the bottom of the MyGinnieMae Public Landing Page for general questions. If a solution cannot be found, seek assistance from the Ginnie Mae Help Desk at 1-800-234-GNMA (4662).
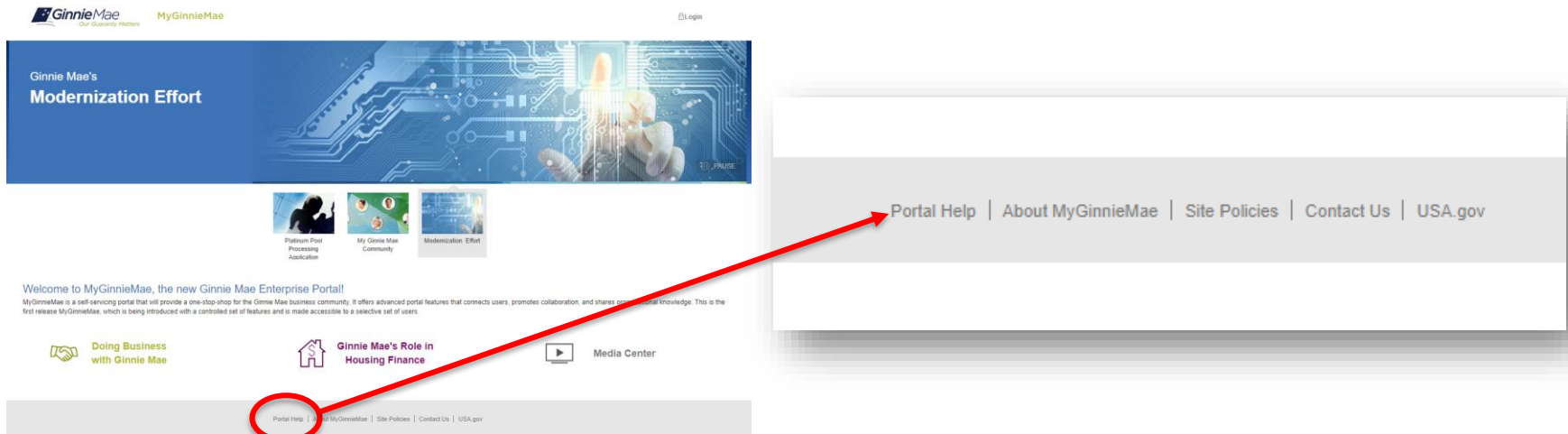
Org Admins can complete most functions on behalf of the organization. The Ginnie Mae Help Desk team must perform the following functions:

- Unlock any User's OTP
- Reset any User's OTP Email
- All Org Admin account registration and management activities