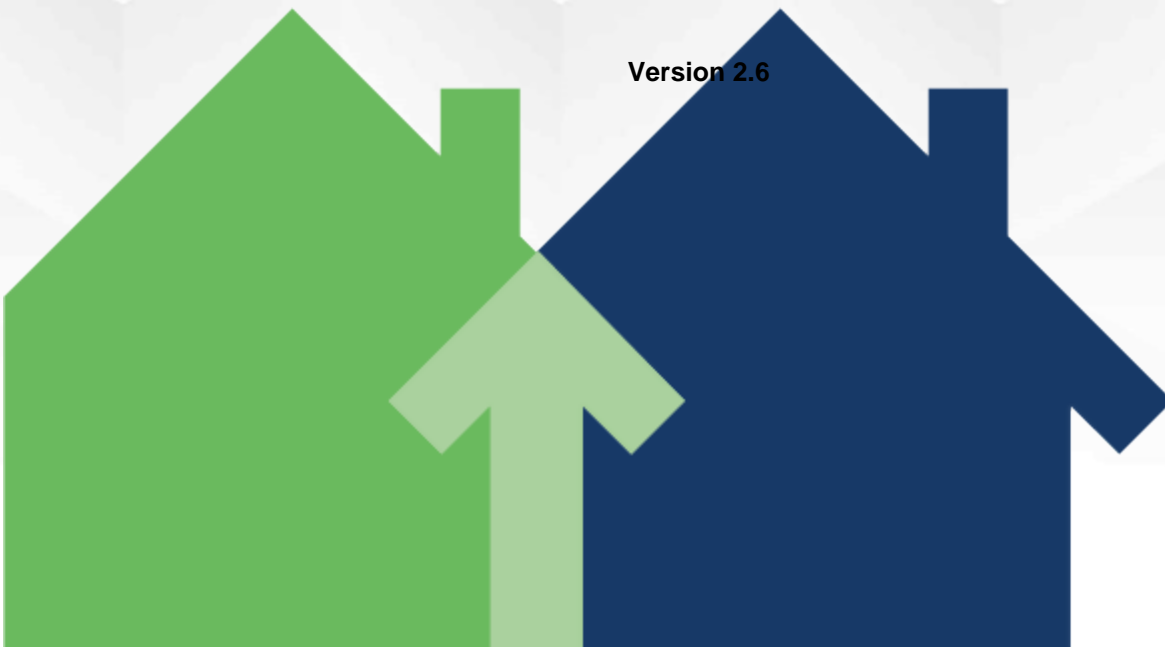# MyGinnieMae Portal Access Management Console (AMC) User Manual

for Organization Administrators

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

Ginnie Mae, Office of Securities Operations

Version 2.6

Application Details

Application Information	Description
Application Name	Access Management Console
Application Acronym	AMC
Ginnie Mae SVP, Sponsor	John Daugherty SVP OSO
Ginnie Mae Application Owner	
Version/Application Release Number	2.6

Document History

Version	Date of the Document	Author (Last Name, First Name)	Entity (Company or Department Author Represents)	Revision Description
1.8	10/17/2018		BNYM	Incorporated final feedback from CAG and Ginnie Mae
1.9	6/21/19		BNYM	1.9 6/21/19 BNYM Updated document based on the latest feedback
2.0	09/30/19	Matheny, Micah – PM	Falcon Capital Advisors	Updated document framework
2.1	11/20/19		BNYM	Add Additional Content into version of template provided by CAG
2.2	12/05/19		BNYM	Collected feedback as part of BNYM review and addressed it
2.3	12/12/19		BNYM	Ops feedback
2.4	12/18/19		BNYM	Additional comments Ops feedback and CRs
2.5	1/2/19		BNYM	Applied updates for Ops feedback and CRs
2.6	12/1/2020	Laticia Jefferson Dave Cannon	Ginnie Mae Ampcus	Added content on reports and adding RSA tokens. Formatting updates, including the separation of QRCs

Version	Date of the Document	Author (Last Name, First Name)	Entity (Company or Department Author Represents)	Revision Description
2.6	11/29/2022	Renee Just-Buddy Dave Cannon	Ginnie Mae Ampcus	Revised to reflect formatting changes to Ginnie Mae's User Manual Framework, provided by the Customer Experience Division.

TABLE OF CONTENTS

1   INTRODUCTION

This manual is written to provide instructions on how to use the Access management Console (AMC) in the MyGinnieMae portal. Privileged users of the MyGinnieMae portal, called Organization Administrators (Org Admin) are responsible for managing End User access and accounts within their organizations. Organization Administrators are also responsible for ensuring End Users are provided the appropriate level of access for their business role with Ginnie Mae. To be eligible to request the Organization Administrator privileged role, you must be listed on the Form HUD-11702 (Resolution of Board of Directors and Certificate of Authorized Signatures).

Below are links that address common topics that pertain to the Access Management Console (AMC) application in the MyGinnieMae portal.

- How to get access to MyGinnieMae
- Refer to the MyGinnieMae Getting Started Manual for System Prerequisites
- How to Request a New User Registration
- How to Approve a New User Registration
- How to Request a Functional Role
- How to Reject a Functional Role
- My Ginnie Mae Portal Dictionary

[Back to Table of Contents]

1.1   Application Overview

The MyGinnieMae Access Management System (AMC) is an application in MyGinnieMae used by Organization Administrators to register new MyGinnieMae users, to grant access to modernized business applications such as MyGinnieMae Portal, Access Management Console Manual, the Multifamily Pool Delivery Module (MFPDM), and legacy business applications such as GMEP 1.0 and GinnieNET.

Organization Administrators will send a registration invitation, approve user registration, initiate and approve access requests, manage user information within the permitted organization and perform additional responsibilities as identified by Ginnie Mae.

The following sections detail common actions you take as an Organization Administrator, in the Access Management System (AMC) application to onboard new users, request functional roles and manage existing user accounts. The complete Onboarding Workflow automates the user account registration and access request process and provides an audit history of user access.

1.2   Business Workflow

The high-level workflow for onboarding end users into MyGinnieMae user accounts is shown in the figure below:
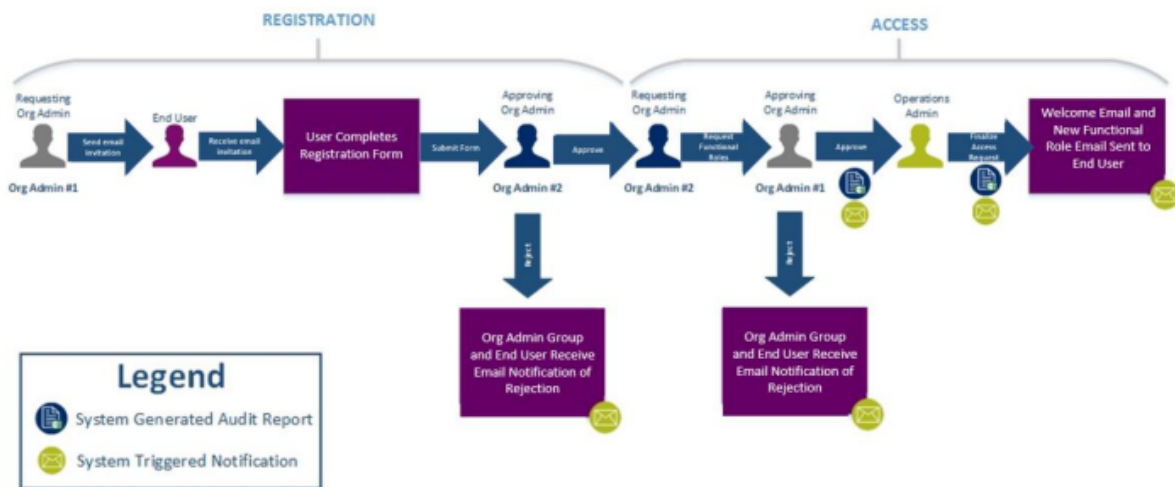
The following Onboarding Workflow reflects the different operational activities for how an Org Admin requests and approves a new user registration and assigns access via functional role assignments.

- The Requesting Org Admin will follow the instructions for Logging into MyGinnieMae to initiate the onboarding workflow, by Sending an Email Invitation to the End User
- After submission, the User Invitation Form closes automatically. An email with a unique URL is automatically sent to the End User to complete their registration within 24 hours.
- The End User will complete and submit their registration form for approval.
- An approving Org Admin with either Approve the New User Registration
- Decision – Rejecting a New User Registration
  - o In the event there is a problem or error with a registration request, the Approving Org Admin should Reject the End User Registration Request with the Access Management Console
- Once the End User's registration is approved, the Requesting Org Admin will proceed with Requesting a Functional Role for the End User
- Once an Access Request has been submitted, an Org Admin Group, except for the Org Admin who submitted the access request, will receive an email notification that a request is available for approval and will either Approve or Reject the Functional Role Request.
  - o Once the Approving Org Admin Approves the Functional Role Access Request, the system will display a green confirmation ribbon at the top of the screen indicating the Functional Role request was approved successfully.

o   Once the Approving Org Admin [Rejects the Functional Role Access Request](#), the system will display a green confirmation ribbon at the top of the screen indicating the Functional Role request was rejected successfully.
- Operations Admin grants access to the functional role.
- End User can access the application. (Refer to the [MyGinnieMae Getting Started Manual](#) or the [Logging into MyGinnieMae & Accessing Business Applications QRC](#))

[Back to Table of Contents]

2   GETTING STARTED

2.1   Logging into MyGinnieMae

Refer to the [Logging into MyGinnieMae & Accessing Business Applications QRC](#) for step-by-step instructions on how to log into the portal or the Section on Logging into MyGinnieMae in the [MyGinnieMae Portal Getting Started Manual](#).

2.2   Navigating to the Access Management Console

The Access Management Console (AMC) is the user interface used to manage user accounts and retrieve system audit reports for your organization. To navigate to the AMC:
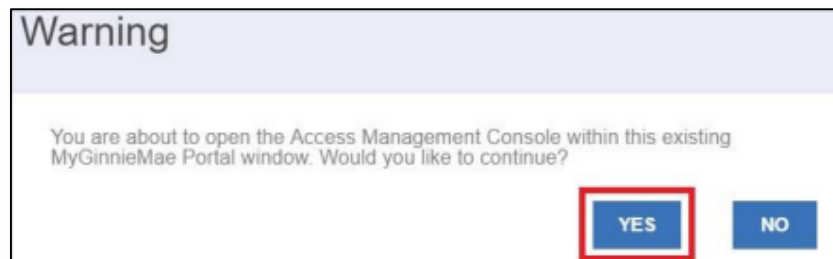1.   From the Global Header of any page,
       a.   Select **Tools**
       b.   Select **Access Management Console**
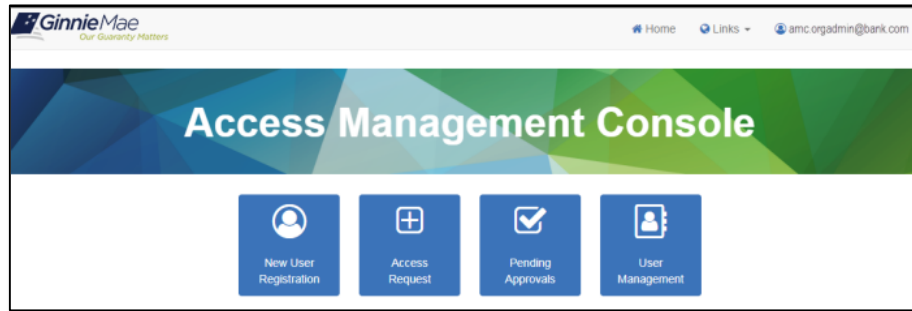
Figure 2.2-1 Tools Drop-Down Menu
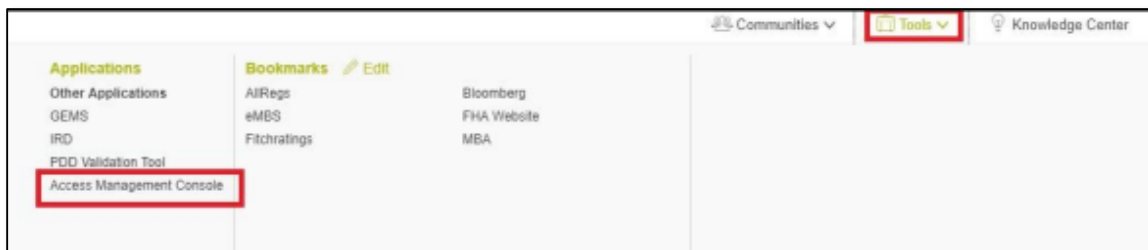
2.   Select **Yes** when prompted to open the AMC within this existing MyGinnieMae Portal window.

Figure 2.2-2 Portal Warning

3.   The system will open the AMC in a new browser window.

Figure 2.2-3 AMC Landing Page - Organization Administrator
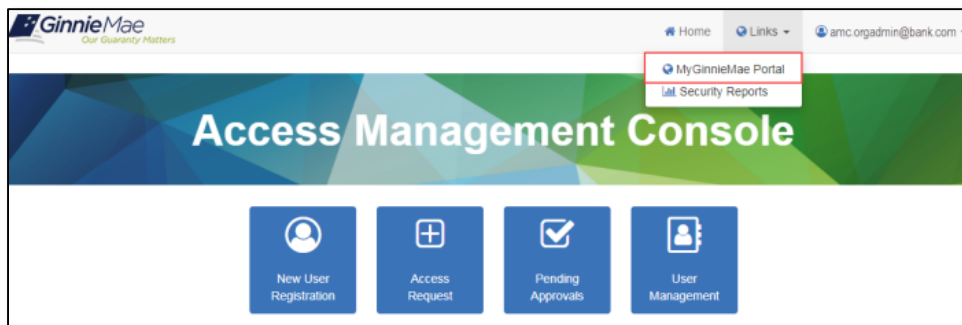

[Back to Table of Contents]

2.3 Exiting the Access Management Console

When exiting the Access Management Console (AMC) you may choose to return to My Dashboard in the MyGinnieMae portal to continue working in Ginnie Mae business applications or to leave the portal completely. Below are instructions and implications for each method of leaving the AMC.

2.3.1 Exiting AMC and Returning to MyGinnieMae

1. Select the down arrow beside **Links** on the toolbar at the top of the page.
2. Select **MyGinnieMae Portal**.

Figure 2.3-1 Return to MyGinnieMae Portal

[Back to Table of Contents]

2.3.2   Exiting AMC and MyGinnieMae

You may simultaneously exit the AMC and the MyGinnieMae portal by following the instructions below:

NOTE: If you have any legacy system sessions open in other windows those sessions must be exited separately to securely end all pool activity.
1. Select The down arrow beside the username on the toolbar at the top of the page.
2. Select **Sign out**.

Figure 2.3-2 Exit Access Management Console
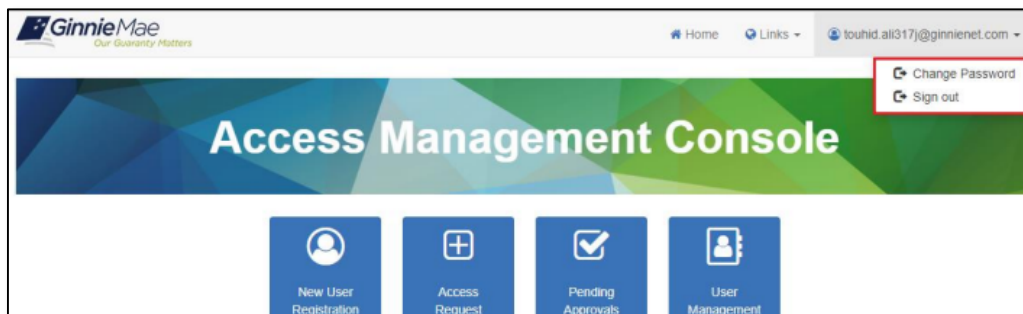
NOTE: Upon signing out of the AMC, the portal session is terminated. To return, you will need to follow the steps in the Logging into MyGinnieMae and Accessing Business Applications QRC.

[Back to Table of Contents]

2.4   Outlook Rules for Email Notifications

During the onboarding of End Users, you will receive several email notifications for each user. The steps below provide guidance on how to setup the Microsoft Outlook rule for segregation of notifications generated to the Org Admin Group versus messages regarding you will receive about your own individual MyGinnieMae account. It is recommended to do this before you begin onboarding End Users to ensure registration and access notifications for those actions are easily managed and important notifications about your own user account access are not missed.

2.4.1   Outlook Rules for Organization Administrator Group Notifications

Each Organization Administrator will receive several notifications relating to registration and access workflow items for each End User in your organization. If you would like to automatically move those notifications from your Microsoft Outlook Inbox to a designated folder, the following criteria will assist. For detailed instructions on creating a Rule in Microsoft Outlook visit Microsoft Office Support and search "Manage email messages by using rules".

Criteria:

From: donotreply_access@ginniemae.gov

Subject contains

"Action Required: User Registration Request for Approval"

"Action Required: Access Request for Approval"

"New Functional Role Assignment"

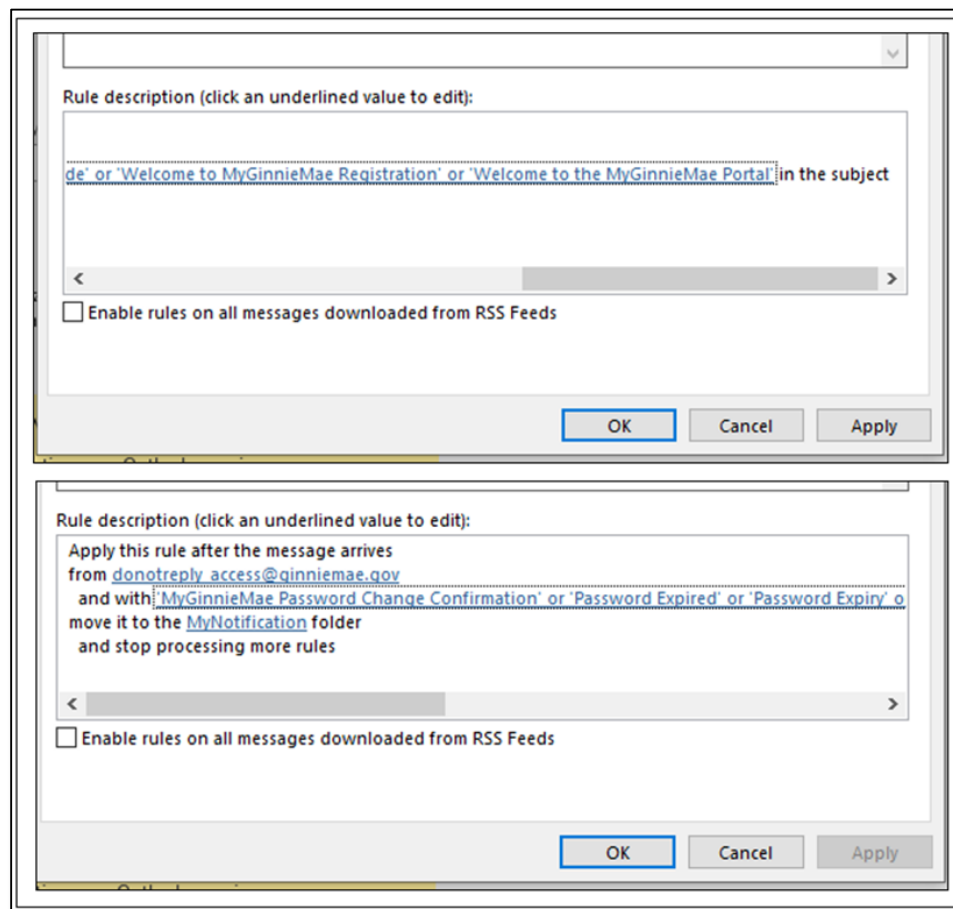"Action Required: RSA Token Role Assignment"

Target folder: Any user defined outlook folder. In the screenshot provided below, OrgAdminNotification is the user defined folder.

This rule will mark all the notifications for the following actions:

- New user registration approval
- Access request approval
- New functional role assignment notification
- RSA token role assignment notification

The MS Outlook rule description can be seen in the figure below:

Figure 2.4-1 Outlook Rule for Individual Account Notifications

2.4.2 Change Password via the AMC

If you would like to change your login password using the Access Management Console (AMC), you can do this from the AMC Landing Page, rather than navigating back to the MyGinnieMae landing page. To change the login password from the AMC Landing Page, you should follow these steps:

1. Select the down arrow ▼ next to your username in the corner of the screen to display the menu.

Figure 2.4-2 AMC Dropdown Menu
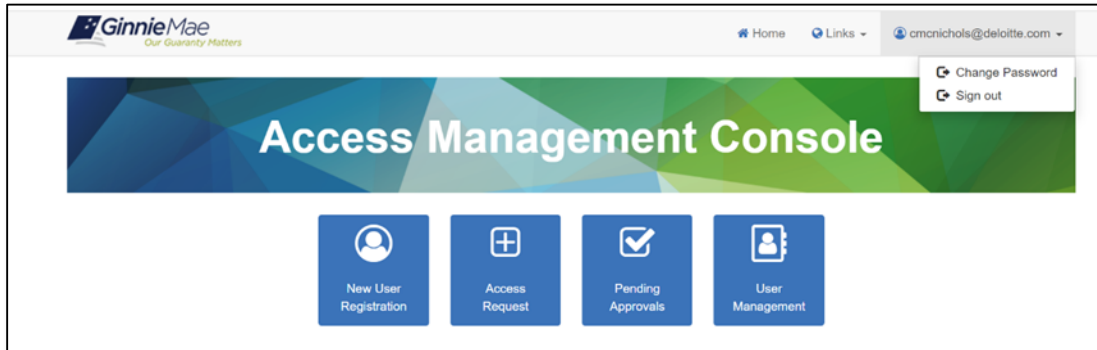
2. Select **Change Password**.
3. The system redirects to the Change Password screen.
   a. Enter the **Current Password**
   b. Enter the **New Password** (Must comply with the Password Policy)
   c. Confirm **New Password**
   d. Select **Submit**

Figure 2.4-3 AMC Change Password Screen (Filled-In)

4. A message will display confirming the password change was successful. You can then select "Return to Portal" to proceed.

Figure 2.4-4 Password Change Successful Message
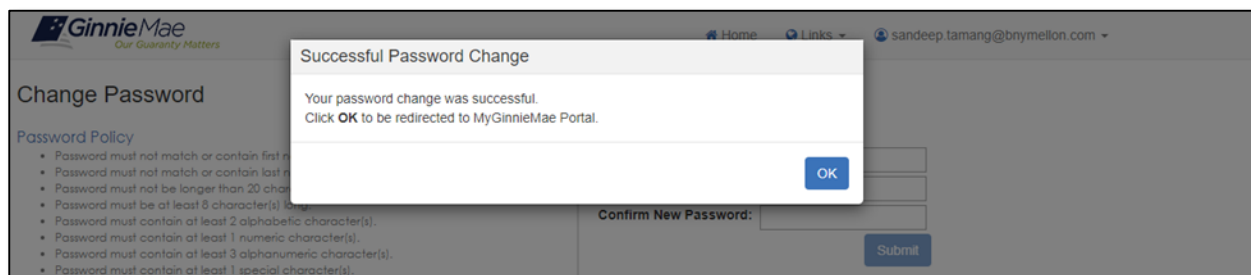
NOTE: If you enter the incorrect current password, you will receive an "At least one of the provided passwords failed validation" error message.

At least one of the provided password failed validation.   ✕

3   USING THE APPLICATION

The following sections detail common actions you take, as an Organization Administrator, in the Access Management Console (AMC) application to onboard new users, request functional roles, and manage existing user accounts. The complete Onboarding Workflow automates the user account registration and access request provisioning processes and provides an audit history of user access.

3.1   Onboarding End Users – Registration & Access Workflow

As an Organization Administrator, you are responsible for providing access to Ginnie Mae business systems via MyGinnieMae for End Users within your organization. This is done through an automated Onboarding Workflow in the Access Management Console (AMC). This section contains instructions on how to request and approve new user registration and assign access via functional role assignments.

NOTE: Separation of duties within the Registration and Access Workflows do not allow you to initiate a registration and approve that same registration or request a Functional Role access 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 at least three Organization Administrators.

3.1.1   New User Registration

To create a new MyGinnieMae user account, initiate the Registration Workflow by sending an email invitation to the End User using the following steps:

1. Follow the instructions for Logging into MyGinnieMae in the MyGinnieMae Portal Getting Started Manual.
2. Navigate to the Access Management Console.
3. Select the **New User Registration** tile.

Figure 3.1-1 Access Management Console Landing Page
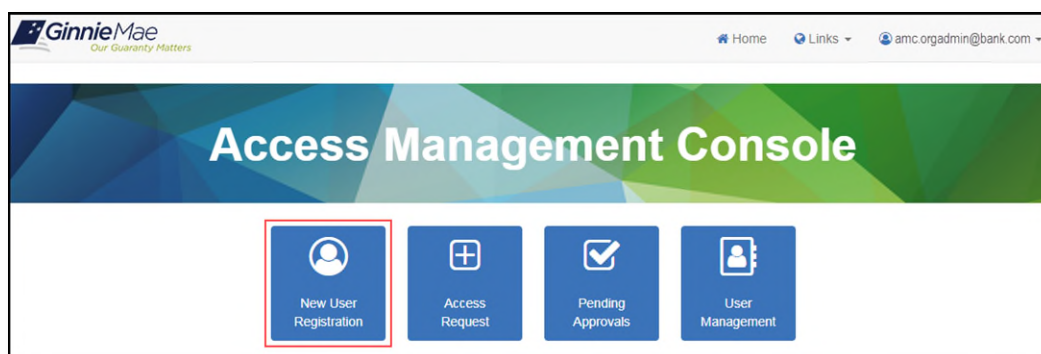
4. The system opens the New User Registration interface in a new window.
   a. Select **Applications** from the menu on the left

b. Select **User Registration** to open the User Invitation form in a new window

Figure 3.1-2 New User Registration Interface
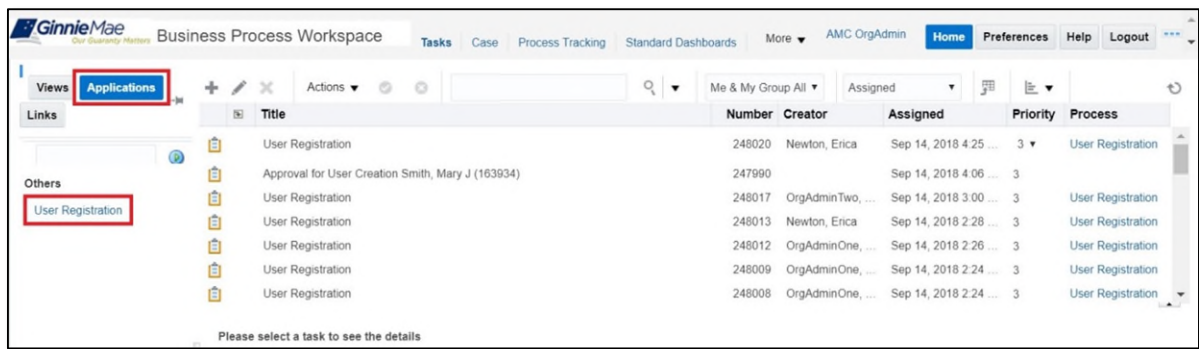
- Ginnie Mae Customer Support information can is located in the MyGinnieMae Portal Getting Started Manual.

NOTE: Web browser pop-up blockers must be disabled in order for the User Request form to open.

5. Complete the following fields in the User Request Form:
    - Title

    - First Name (alphabetic, hyphen, or underscore only)

    - Middle Name (optional, alphabetic, hyphen, or underscore only)

    - Last Name (alphabetic, hyphen, or underscore only)

    - Job Title (do not enter a job title greater than 30 characters)

    - Org ID dropdown (Org Admins will only see Org IDs for which they have been assigned the privileged role to perform user access and management functions)

      Email (use only lower-case characters to register; not mixed or upper case). The email domain is validated against a whitelist of valid domains based on organizations with which Ginnie Mae works. If domain changes are needed for an organization, contact Ginnie Mae Customer Support.

NOTE: The Org ID selected should be the Home Org which employs that user. Users may be provided access to conduct business under additional Org IDs through the steps in Request for Functional Role.

6. Select **Submit**.

Figure 3.1-3 User Request Invitation Form

NOTE: It is not necessary to attach any files to this form. Attached files are not communicated in any way to the End User or other Organization Administrators.

7. After submission, the User Invitation Form closes automatically. An email is automatically sent with a unique URL to the End User to complete their registration within 24 hours.

Figure 3.1-4 New User Registration Interface

8. If sending additional invitations, repeat steps 4 through 6. If not, close the New Registration interface.

NOTE: After the End User completes registration, a second Organization Administrator reviews and approves the request (See Approve a New User Registration).

[Back to Table of Contents]

3.1.2 Approve a New User Registration

Once an End User has completed and submitted the User Registration Form, all the Organization Administrator for the End User's Org ID, except the one who sent the Registration Invitation to that End User, will be notified via email to approve the User Registration request. The following steps describe how to approve those requests.

Figure 3.1-5 User Registration Approval Request Notification Email

NOTE: Selecting the hyperlink in the email notification will navigate directly to the MyGinnieMae Login Page.

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
3. Select the **Pending Approvals** tile.

NOTE: When the Pending Approvals module is loading, the system displays a loading bar at the top of the page to indicate the progress. Once the Pending Approvals have loaded, the system automatically expands any sections with a Pending Approval.

Figure 3.1-6 Access Management Console Landing Page
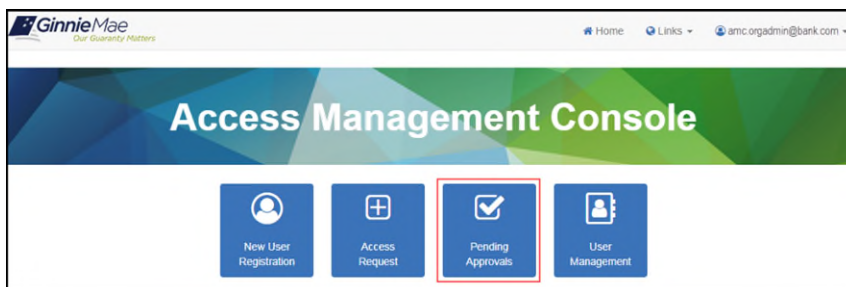
4. Review the table under the "User Registration Approval" accordion which displays the list of available registration requests awaiting approval.

Figure 3.1-7 Pending Approvals - User Registration Approval
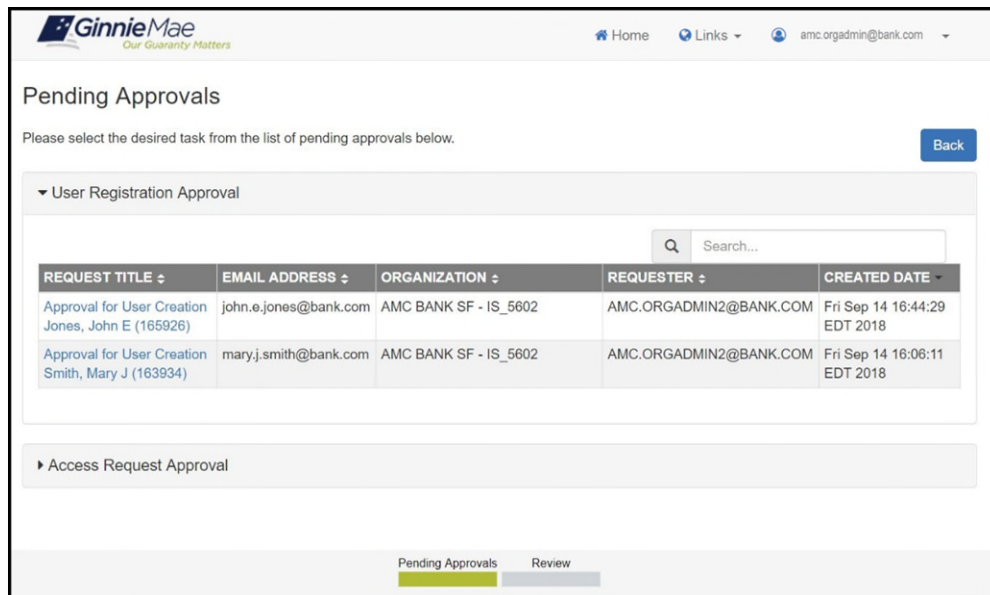
5. Select **Request Title** hyperlink for the desired End User to begin the approval of the registration request.

Figure 3.1-8 Request Title Hyperlink
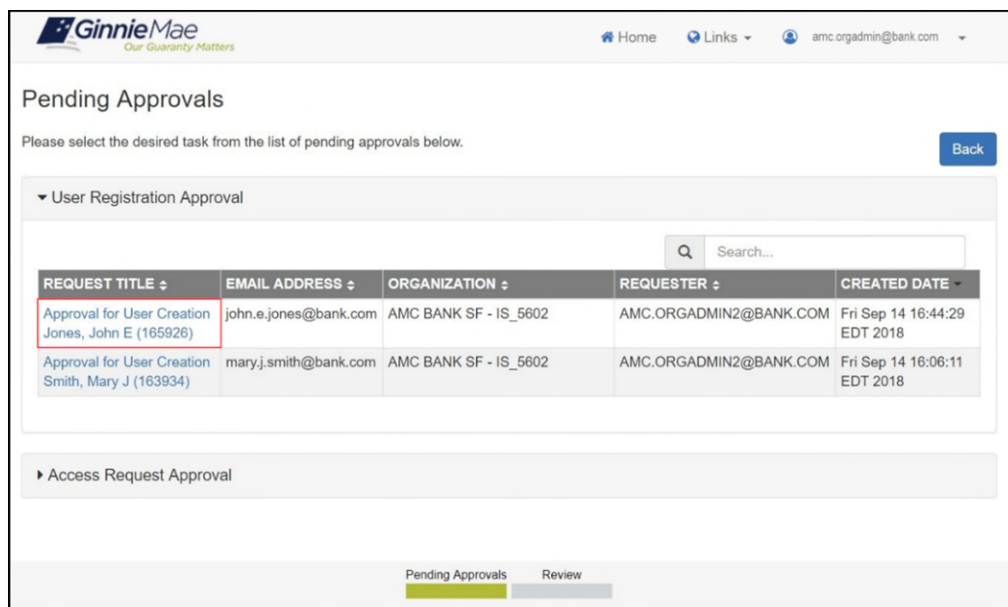
NOTE: If there are multiple registration requests for the same user email, only one of these requests should be approved. The remaining should be rejected. Follow the steps in Reject a New User Registration.

6. Review the user approval details for accuracy. If the details are correct, select **Approve Registration**.

NOTE: Some User Registration fields are not editable for the approving Organization Administrator. If there are any errors or incorrect information in the request, follow the steps to reject the request in Reject a New User Registration. Then work with the requesting Organization Administrator and the affected End User to submit a new registration beginning with the steps in New User Registration.

Figure 3.1-9 User Approval Details

7. The system displays the Confirm Registration Approval dialog box. Select **Confirm** to approve the request.

Figure 3.1-10 Confirm Registration Approval Dialog Box

The system submits the approval task and reopens the "Pending Approvals" screen, displaying the "User registration request #XXXXXX approved successfully" green notification ribbon.

NOTE: If the request has not been processed successfully, attempt to approve the access again. If the error persists, see Help Desk.

Figure 3.1-11 User Registration Approval Notification Ribbon
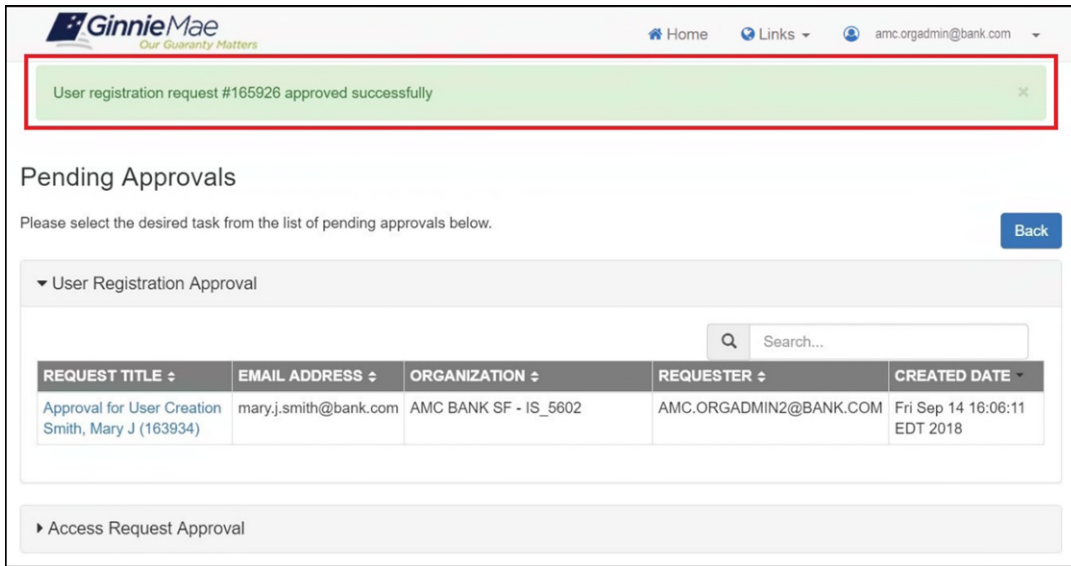
8. It is strongly recommended that the approving Organization Administrator immediately proceed to the access request as detailed in Section: Request Functional Role.

[Back to Table of Contents]

3.1.3   Reject a New User Registration

In the event that there is a problem or error with a registration request, you should reject the user registration request within the Access Management Console using the follow steps.

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
3. Select the **Pending Approvals** tile.
4. Review the table under the "User Registration Approval" accordion ▼ which displays the list of available registration requests awaiting approval.
5. Select the **Request Title** hyperlink for the desired End User.
6. Select **Reject Registration**.

Figure 3.1-12 User Rejection Details

7. The system displays a Confirmation Registration Reject dialog box for the rejection justification reason. This required field has the following options:

    - 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)

Figure 3.1-13 Rejection Justification Reason Drop Down

8. Choose the Justification Reason.
   a. If required, enter a Justification Description.
   b. Select **Confirm** to send the rejection to the system.

Figure 3.1-14 New User Registration Rejection

9. After rejection is complete, the system notifies the Org Admin Group with the following email message.

Figure 3.1-15 User Registration Rejection Notification

3.1.4   Request Functional Role

An Organization Administrator can submit a functional role access request for an End User using one of two tiles in the AMC, 1) Access Management Tile or 2) User Management Tile. The following instructions will guide you on using either method. These instructions may be followed for both new users and to add additional Functional Roles to an active existing user account.

NOTE: An Organization Administrator may not participate in an access request for their own account. If you require Functional Role(s) to complete business processes, this access request must be completed by other members of the Organization Administrator group.

NOTE: Organization Administrators share in the responsibility of system security and are expected to provide only the access that a user requires to complete their Ginnie Mae business responsibilities, no more and no less. Org Admins should work closely with End Users and their supervisors to determine the appropriate set of Functional Roles that need to be provisioned for each user.

3.1.5   Request Functional Role from the Access Management Tile

To request through the Access Management tile:

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
3. Select **Access Request** tile.

Figure 3.1-16 Access Management Console Landing Page
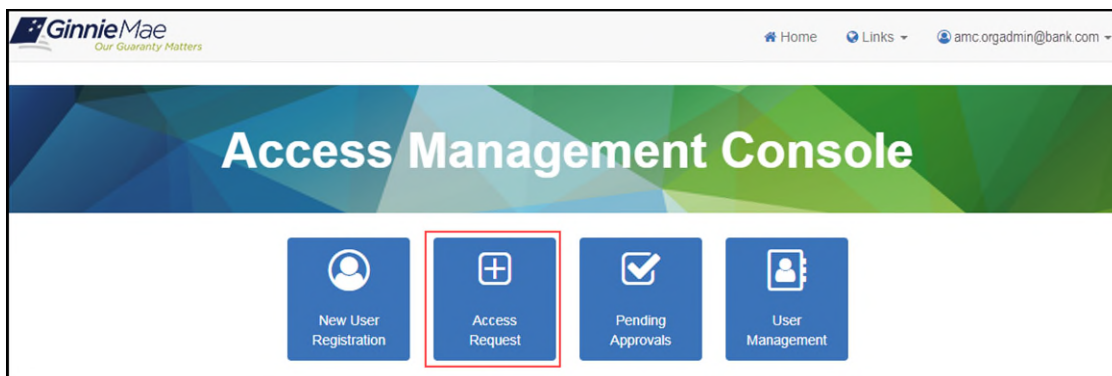
4. The system displays a table which contains the list of all registered users within the organization(s) the Org Admin manages. From the table,
     a. Select the hyperlink for the Display Name of the End User needing a Functional Role.

Figure 3.1-17 Request Access for Others Search
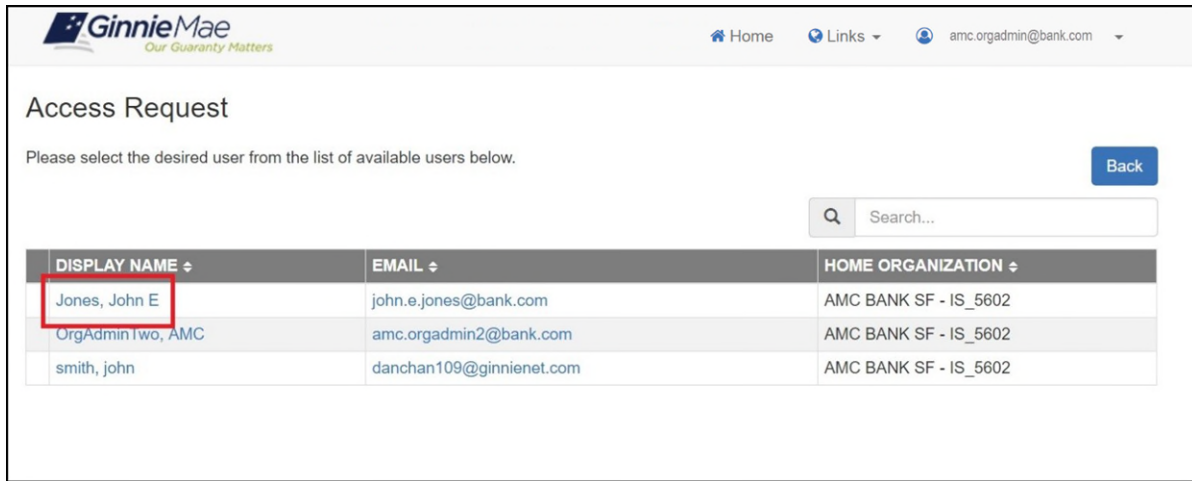
NOTE: Users are listed in alphabetical order by Last Name. The table can be sorted or searched across any of the fields—Display Name, Email, or Home Organization.

5. If you only have one Org Key, you will be sent directly to the list of Functional Roles (Step 6). you have multiple Org Keys, follow these steps:
   a. Select the box next to each organization for which the Functional Role(s), to be selected, will apply.
   b. Select **Assign Roles**.

Figure 3.1-18 Select Organization Key(s)
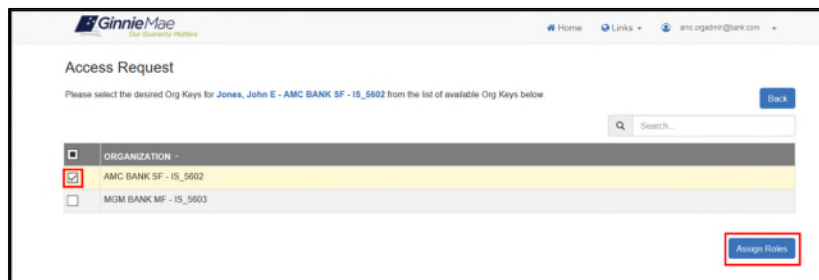
6. The system displays a list of Functional Roles available for the selected Home Organization.
   a. Select the checkbox next to each Functional Role(s) to be requested for the user.
   b. Select **Assign Roles** to conform selections.

NOTE: The system maps the available Functional Roles to the Organization Type (Issuer, Document Custodian, Depositor, etc.) and Program Eligibility (for example, if the Organization is an Issuer and eligible for Single-Family, the system displays Single-Family Issuer Functional Roles).

If the Functional Role has already been requested for the user, it will not be displayed in the table to select. Already assigned or requested Functional Roles are listed under the table at the bottom of the request screen.

Figure 3.1-19 Request Functional Roles Selection Page
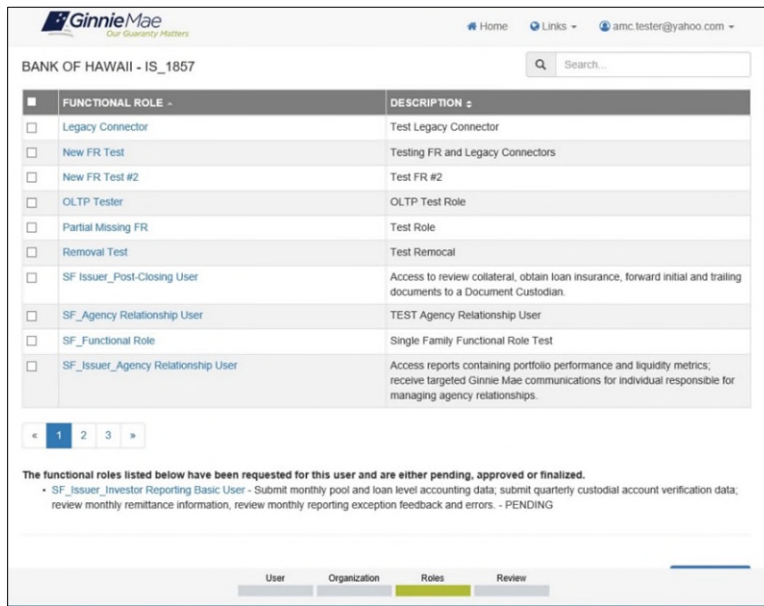
NOTE: Selecting the Functional Role title within the Functional Role Table will open the Functional Role Entities overlay. The overlay contains information about which entities (systems, applications, and functions) are included in the role.

Figure 3.1-20 Functional Role Entities Overlay
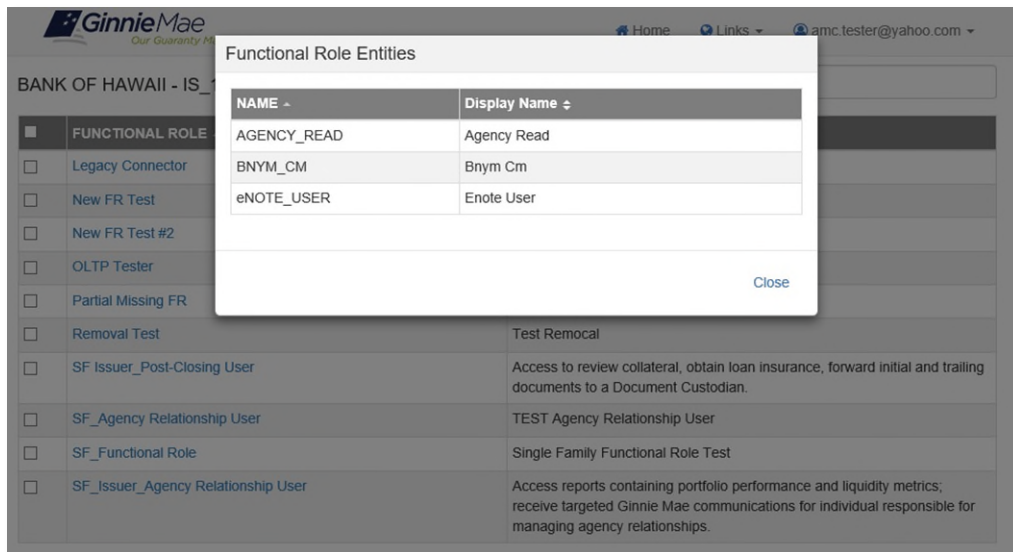
NOTE: Selecting the Functional Role title within the Currently Assigned Roles section will open the Functional Role Entities Status overlay. The overlay contains information about the status of functional roles currently pending, approved, or finalized for the user.

Figure 3.1-21 Functional Role Entities Overlay With Status
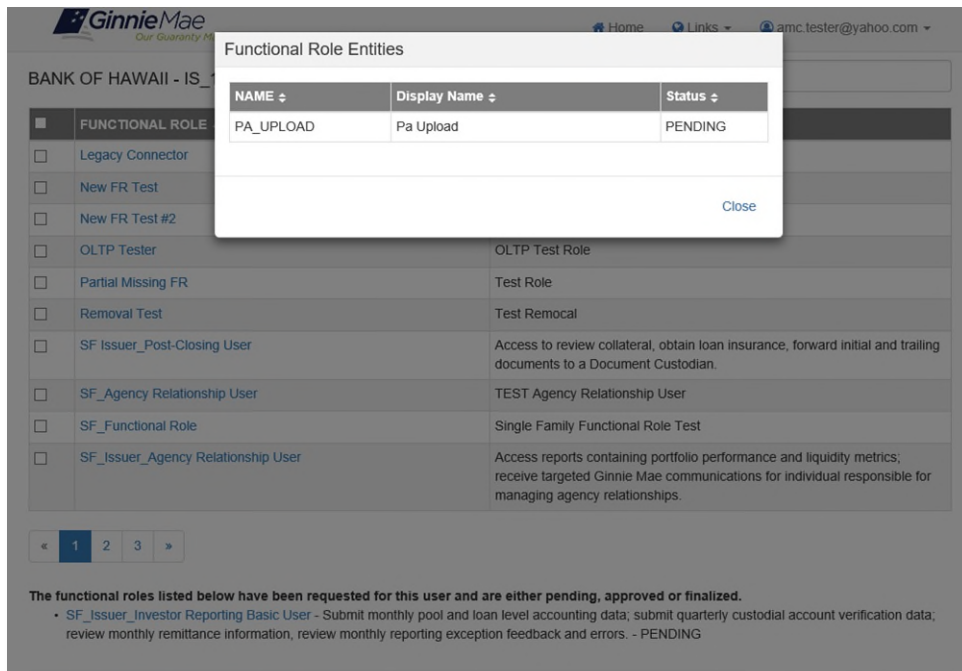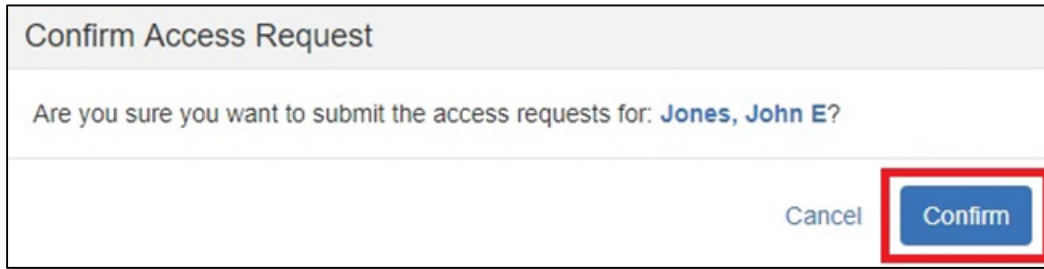
7. The system displays a review page with the requested Functional Role(s) and the underlying entities that make up that Functional Role(s).
   a. Select **Submit**.

Figure 3.1-22 Request Functional Role Review
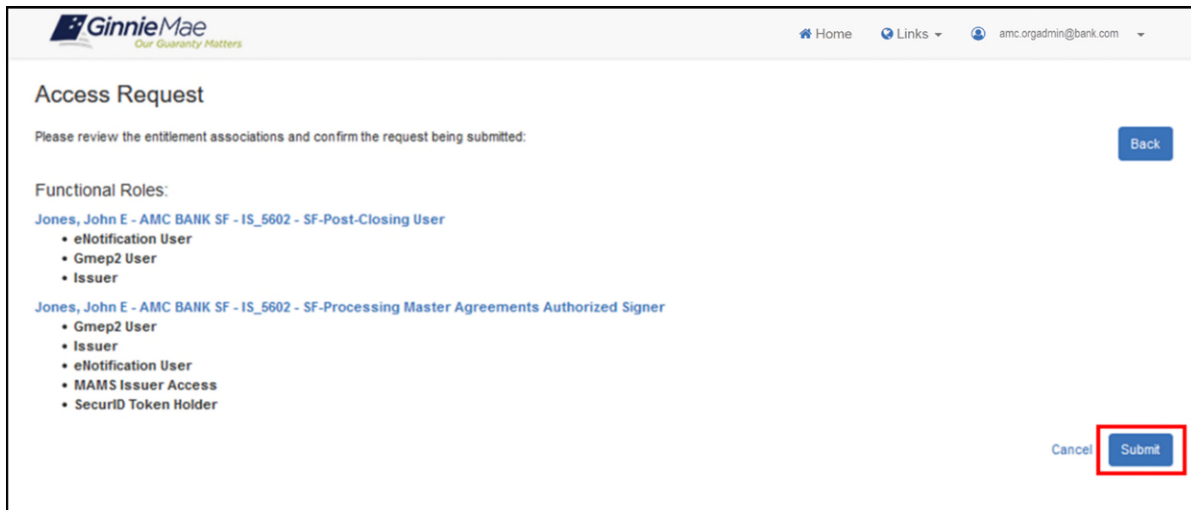
8. The system displays an access request confirmation box.
   a. Select **Confirm** to submit the roles for approval.

Figure 3.1-23 Confirm Access Request
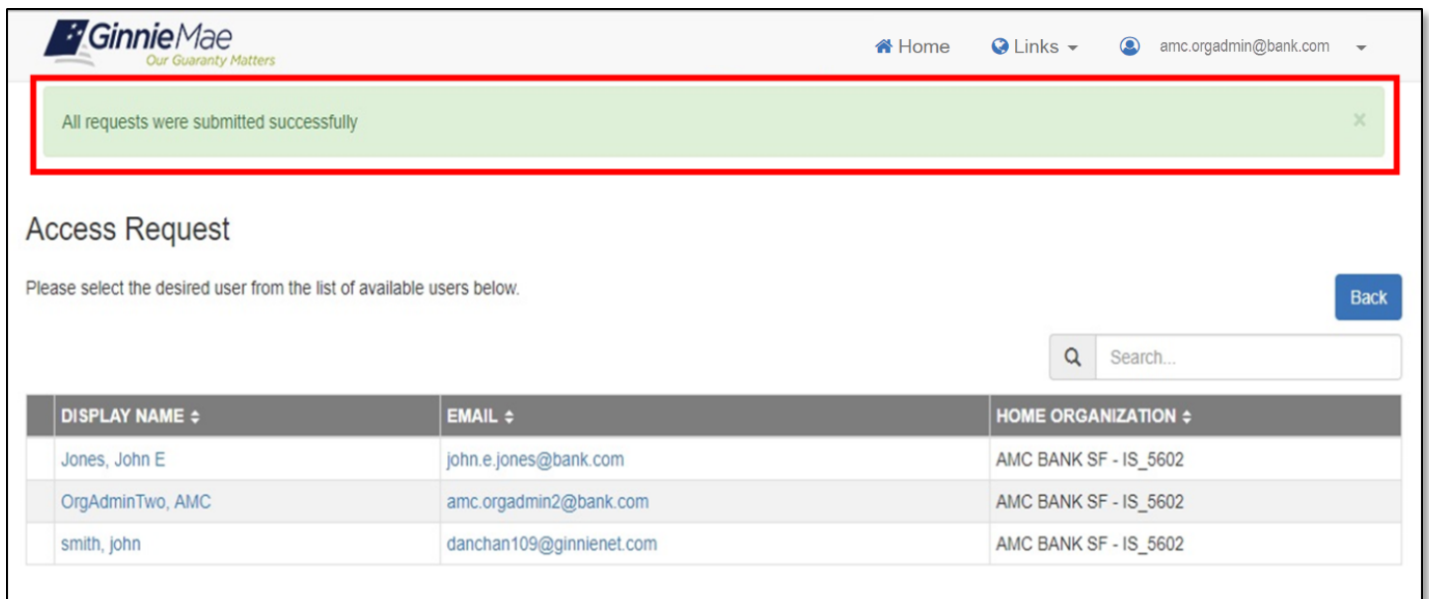
NOTE: After confirmation, the access request is submitted. The system displays a loading bar at the top of the page to indicate the submission is processing. **DO NOT RESUBMIT**. Navigational buttons can be used to move to another screen but a resubmit should not be performed.

9. After successful submission, the system displays a green confirmation ribbon at the top of the screen. A second Organization Administrator may review and approve the request (See Approve Access Request and Functional Roles).

Figure 3.1-24 Role Access Request

NOTE: If an error occurs upon submission, the current selection(s) and/or page within the module are retained and you may attempt to resubmit the request. For more information on errors please refer to Troubleshooting and System Errors. If the error persists, contact the Ginnie Mae Customer Support.

NOTE: Once the role has been finalized by an Operations Administrator and successfully in confirmed status, the Organization Administrator Group will receive a notification that a new Functional Role has been assigned to the End User's account.

3.1.6   Request Functional Role from the User Management Tile

To request access through the User management tile:

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
3. Select the **User Management** tile.

Figure 3.1-25 Access Management Console Landing Page
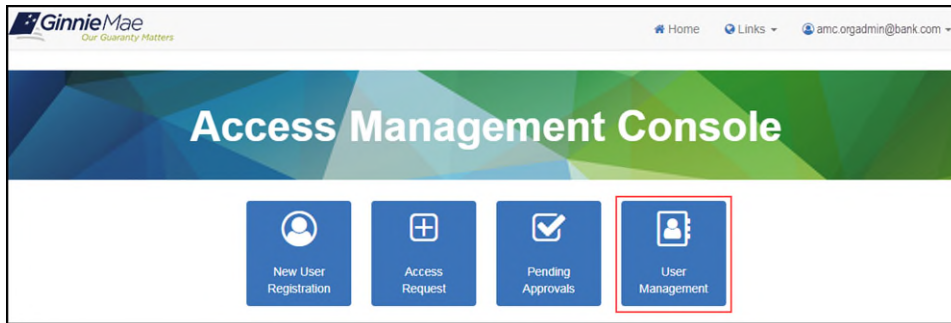
4. The system displays a list of available users. Search for a user by typing one of the following user properties into the search field to locate the desired End User:

    - Display Name
    - Email
    - Home Organization

Figure 3.1-26 Select User
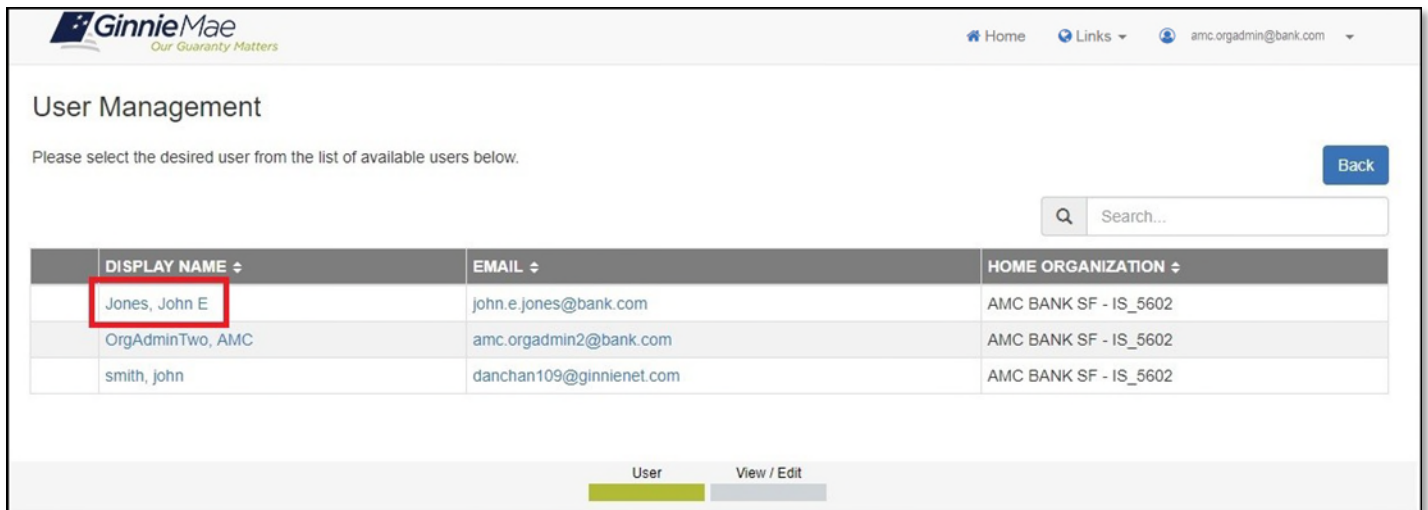
5. Once the "User Profile" screen opens,

    a. Select the down arrow ▼ next to **Edit User Profile** down arrow.
    b. Select **Request Access**.

NOTE: The "Request Access" button will not be visible if the user's status is "Locked" or "Disabled." To use the "Request Access" link on the User Management page, you must first unlock or enable the user.

NOTE: The "Request Access" button will be disabled if the user's profile attributes are incomplete or incorrectly formatted.

Figure 3.1-27 Request Access Button

6. The system directs the user to the Organization screen of the Access Request workflow where you can follow steps 5 - 9 of Request Functional Role from Access Management Tile to request functional role access.

NOTE: If a user receives an RSA Token after they have been registered for MyGinnieMae or did not enter their RSA Token correctly during registration, the Organization Administrator can add or update the RSA Token to a user's profile in the User Management screen. For more information, please see Update a User's Profile Attributes.

3.1.7   Approve Functional Role Access Request

Once an Access Request has been submitted, the Org Admin Group, except for the one who submitted the access request, will receive an email notification that a request is available for approval.

Figure 3.1-28 Access Request Approval Notification

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
3. Select the **Pending Approvals** tile.

NOTE: When the Pending Approvals module is loading, the system displays a loading bar at the top of the page to indicate the progress. Once the Pending Approvals have loaded, the system automatically expands any sections with a Pending Approval.

Figure 3.1-29 AMC Homepage-Pending Approvals Tile
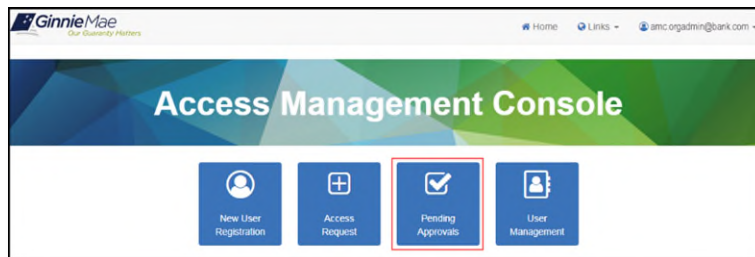
4. Review the table under the "Access Request Approval" accordion (collapsible section) which displays the list of available access requests pending approval.
   a. Select the Request ID for the Functional Role request that corresponds to the desire End User.

Figure 3.1-30 List of Pending Access Requests
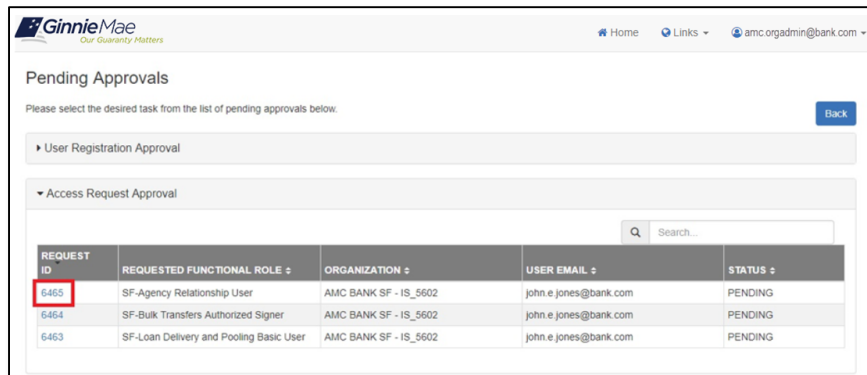
5. The details of the requested Functional Role display in the Review Page.
   a. Review the request details.
   b. Select **Approve** to activate the confirmation message.

Figure 3.1-31 Review Page for Functional Role Approval
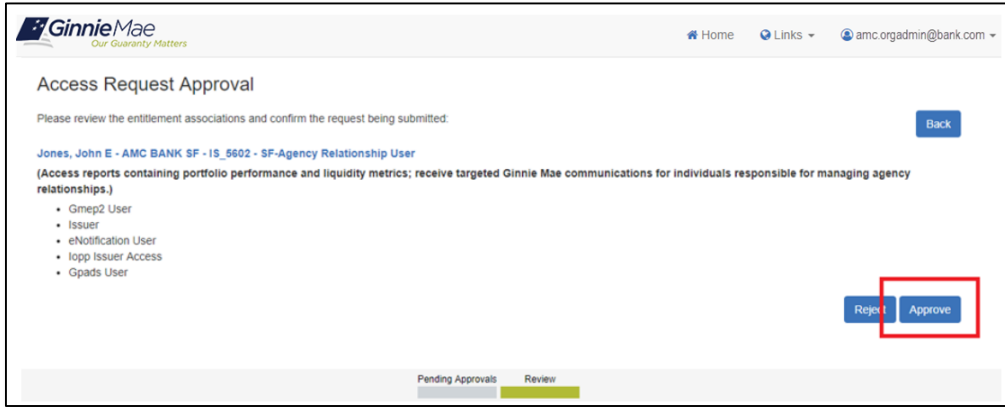
6. Select **Confirm** to submit the approval.

Figure 3.1-32 Confirm Functional Role Approval
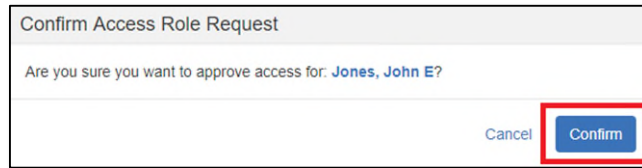
7. The system displays a green confirmation ribbon at the top of the screen when the request has been approved successfully.

Figure 3.1-33 Request Approval Successful
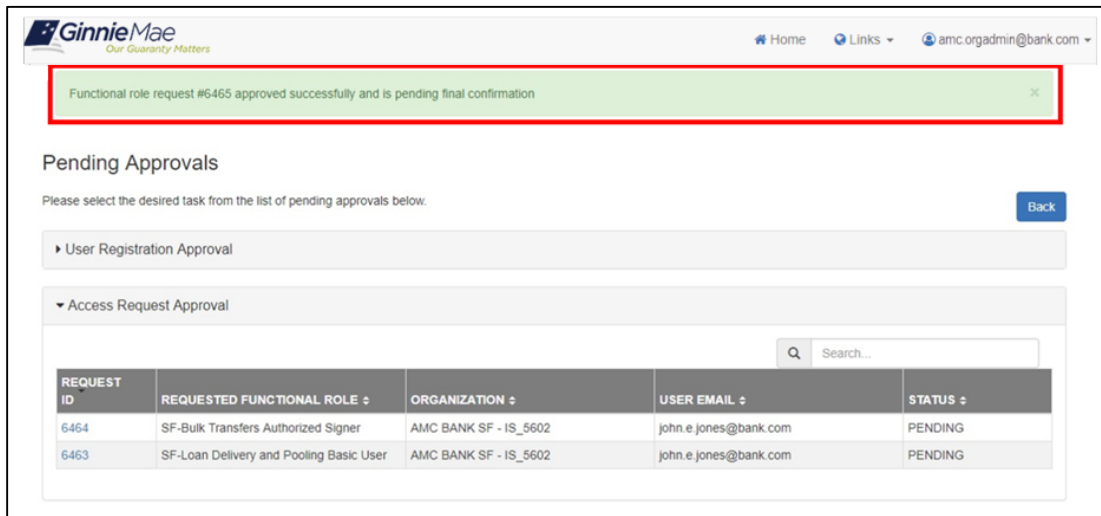
NOTE: If the request has not been approved successfully, review the error message, and attempt to re-approve if possible. If the error persists, contact the Ginnie Mae Customer Support. If an error occurs upon approval, the current selection(s) and/or page within the module are retained.

8. The system routes the request to, and notifies, the Operations Administrator group to perform the required action to complete the workflow. Once the workflow is complete and the Functional Role is assigned, the system sends a notification to the user that a new Functional Role has been assigned to their account.

Figure 3.1-34 End User Notification

New Functional Role Assignment   Yahoo/Inbox ☆

donotreply@accessdev.ginniemae.gov   🖨 May 1 at 4:00 PM ☆
To: notificationsthree@yahoo.com

A new Single Family Issuer Functional Role titled SF_Issuer_Bulk Transfers Authorized Signer has been assigned to your MyGinnieMae account. If you have any questions, please contact your Organization Administrator for assistance.

NOTE: If the functional role was assigned to a new user, the End User will also receive a Welcome Email notify the user that a MyGinnieMae account has been created.

[Back to Table of Contents]

3.1.8   Reject a Functional Role Access Request

An Organization Administrator has the option to reject a Functional Role Access Request for various reasons, such as the incorrect access being requested. The system provides a dropdown to select various justifications for the rejection.

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
3. Select **Access Request** tile.
4. Review the table under the "Access Request Approval" accordion (collapsible section) which displays the list of available access requests pending approval.
    a. Select the Request ID for the Functional Role request that corresponds to the desire End User.
5. The details of the requested Functional Role display in the Review Page.
    a. Review the request details.
    b. Select **Reject**.

Figure 3.1-35 Review Page for Functional Role Rejection
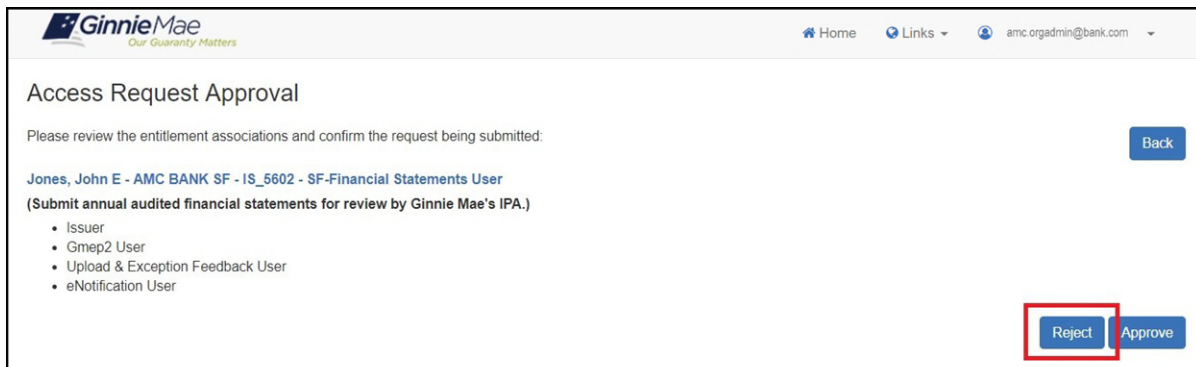
6. The system displays a Confirmation Rejection of Role Request dialog box for the rejection justification reason. This required field has the following options:

    •   Access Does Not Enforce Least Privilege

    •   Incorrect Functional Role Requests

    •   User No Longer with Organization

    •   Do Not Recognize User

- Access Violates Separation of Duties

- Other – Please Explain (the Justification Description will be required)

7. Choose the Justification Description.
   - If required, enter a Justification Description.

Figure 3.1-36 Reject Role Request Justification Reason

8. Select **Reject** to send the rejection to the system.

Figure 3.1-37 Access Request Rejection

9. The system will display a green notification ribbon to indicate the Functional Role rejection was successful.

Figure 3.1-38 Functional Role Rejection Notification
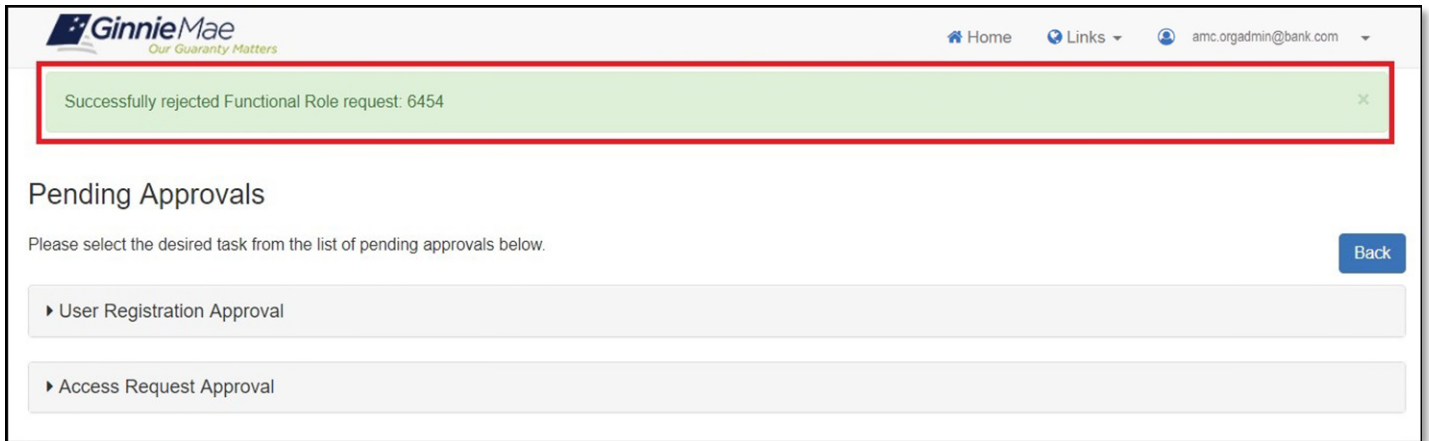
10. After rejection is complete, the system notifies the Org Admin Group with the following email message.

Figure 3.1-39 Access Request Rejection Email Notification

3.2 Managing and Maintaining User Accounts

3.2.1 Disable a User's Account

If the account of a user must be removed for any reason (for example, if the user is leaving the Home Organization), the Organization Administrator is responsible for disabling the End User account via the Access Management Console. Disabling a user removes all assigned Functional Roles, therefore, if user access needs to be temporarily blocked for a short period of time, consider locking the user account as described in Lock a User's Account.

To disable an account, follow the steps below.

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
3. Select the **User Management** tile.

Figure 3.2-1 Select User

4. The system displays a list of available users. Search for a user by typing one of the following user properties into the search field to locate the desired End User:

    - Display Name

    - Email

    - Home Organization

5. Select the Display Name for the desired user.
6. Select **Disable**.

Figure 3.2-2 User Management - Disable Account

7. Select **Confirm** to submit the action.

Figure 3.2-3 Confirm Disable Account

8. The system displays a "User [User Name] successfully disabled" green notification ribbon and updates the Account Status to "Disabled." No additional approval is required when disabling a user account. When a user is disabled, the system removes all Functional Roles provisioned to the user.

Figure 3.2-4 Disable Account Notification
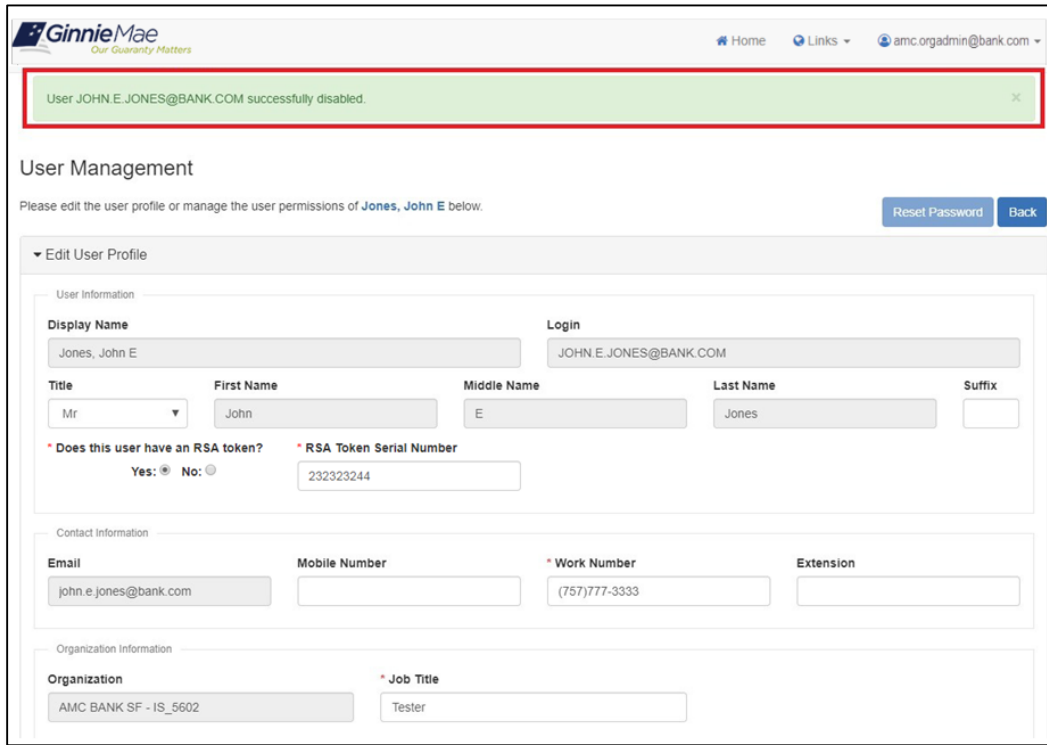
9. Reselect the "Manage User Permissions" down arrow [▼] to confirm the Functional Roles have been removed from the user; the Status will display as Revoked.

Figure 3.2-5 Select Disabled User Functional Roles
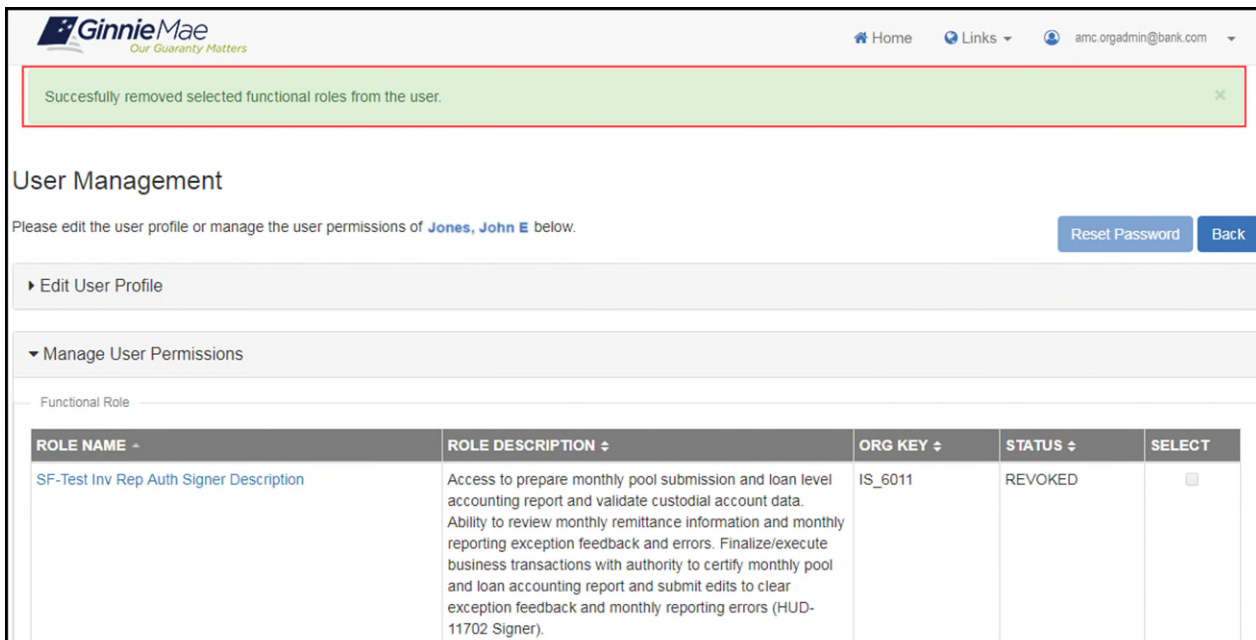
[Back to Table of Contents]

3.2.2 Enable a User's Account

Organization Administrators are advised to remind End Users to login to the portal at least every 90 days to avoid their accounts being disabled. Once an account is disabled, it must be enabled, and functional roles must be requested approved by two Organization Administrators and then finalized by the Operations Administrator to re-establish the user's access in Ginnie Mae systems.

NOTE: If a user was disabled due to 90 days of inactivity, instruct the user to log into MyGinnieMae the same day once their account is enabled; otherwise, the user will be disabled again the following day due to inactivity. The user should be contacted via phone to confirm that they do login after their account is enabled. In fact, it is recommended that the user logs into MyGinnieMae while on the phone or in contact with their Organization Administrator. The user will be able to log into MyGinnieMae right after account is re-enabled, even before the Functional Role access is provisioned.

NOTE: If the user was disabled due to 90 days of inactivity, the system will display the user's Functional Roles as "Missing." See screenshot below. To re-request a Function Role for a user who was disabled due to 90 days of inactivity, see Re-Request a Functional Role**.**

Figure 3.2-6 Functional Role Missing Status
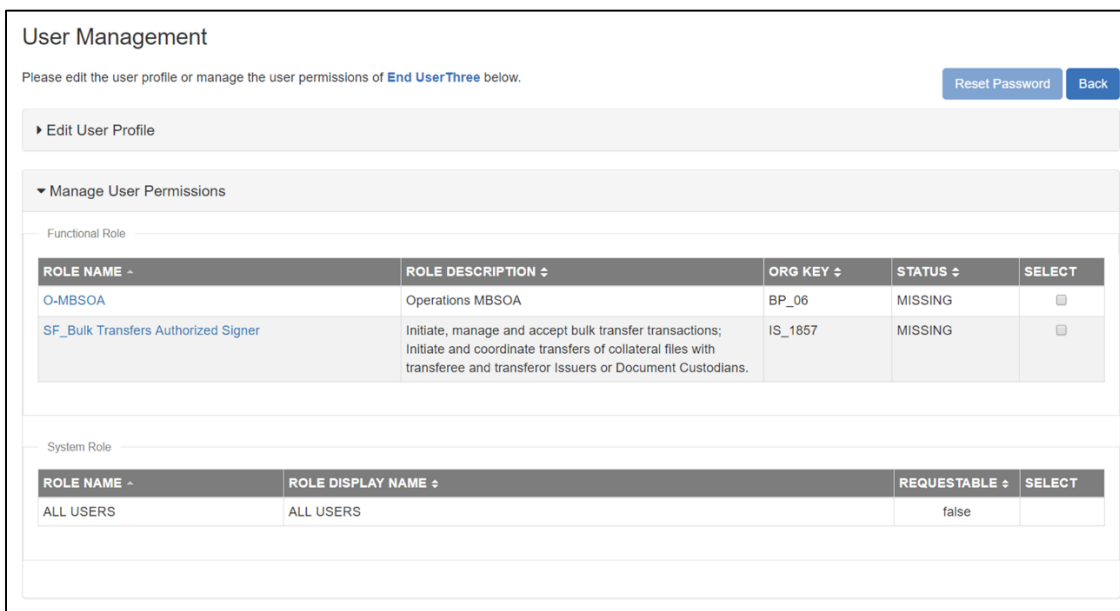
If a user's account has been disabled due to 90 days of inactivity or was disabled manually and must be re-enabled, complete the following steps in the Access Management Console.

1. Follow the instructions for Logging into MyGinnieMae.

2. Navigate to the Access Management Console.

3. Select the **User Management** tile.

4. Verify the user is disabled by confirming that there is a disabled icon (⊘) to the left of their Display Name.

    a. Select the Display Name of the user to enable.

Figure 3.2-7 User Management Disabled User
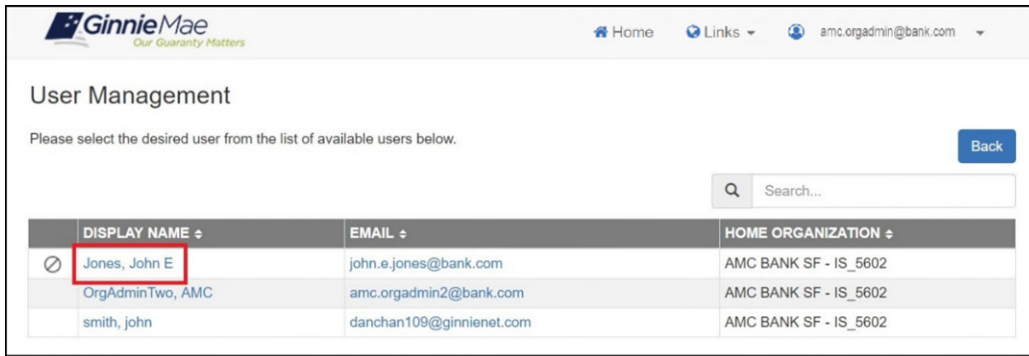
5. Once the "User Profile" page opens, select the "Enable" button in the bottom right of the "Edit User Profile" accordion.

Figure 3.2-8 User Management Enable Account
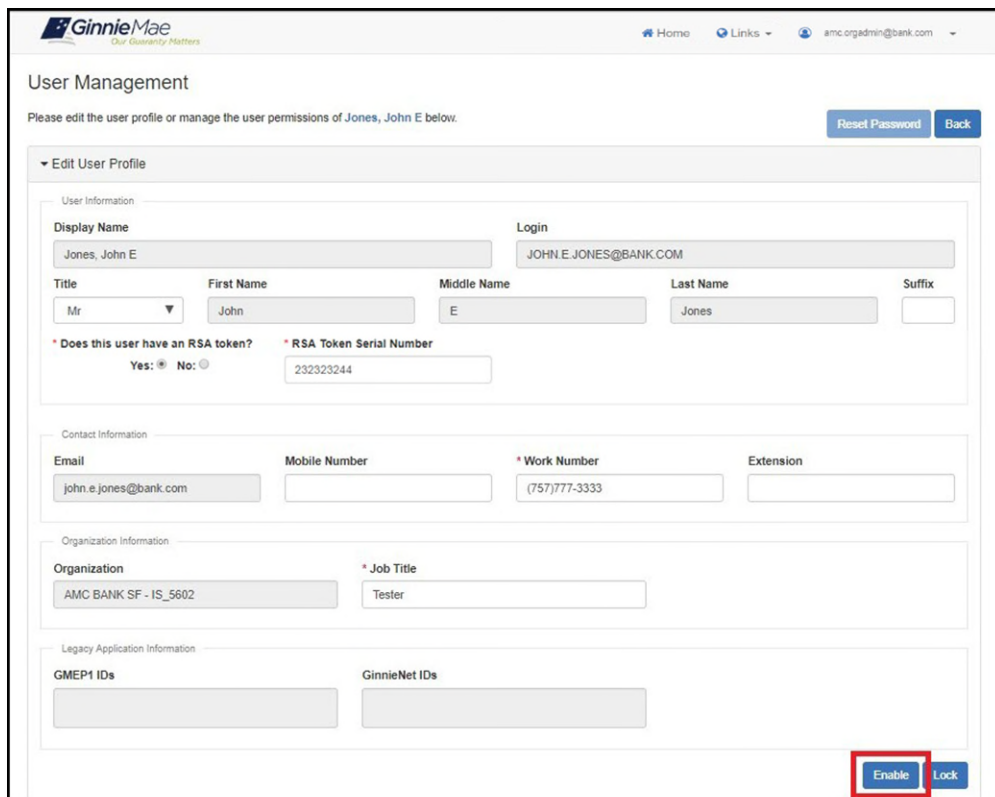
6. The system displays an overlay to confirm the enabling of the selected user's account.

   a. Select **Confirm** to submit the request.

Figure 3.2-9 Confirm Enable Account
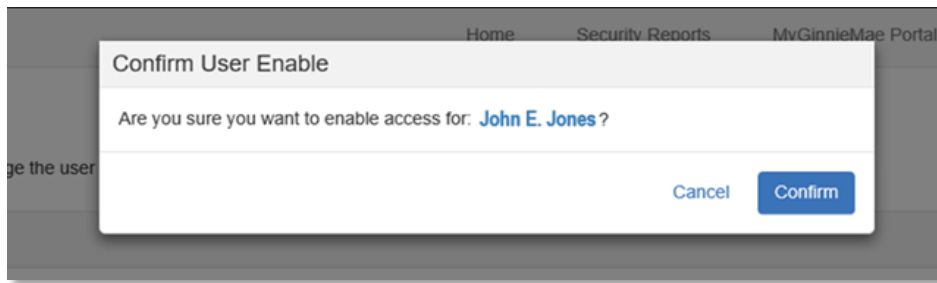
7. The system displays a "User [User Name] successfully enabled" message and updates the Account Status as "Enabled." Follow the steps in Section: Request Functional Role to begin the workflow for assigning roles.

Figure 3.2-10 Enable Account Notification
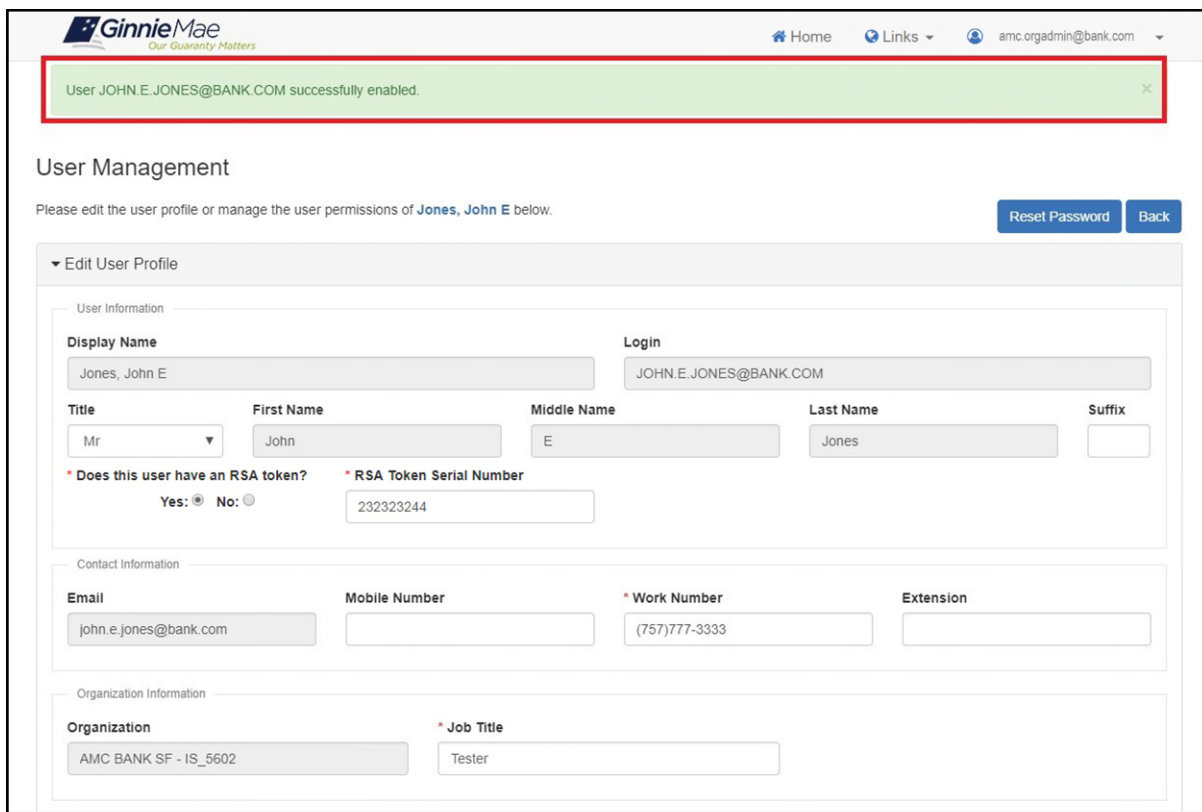
NOTE: If the user previously had two or more Functional Roles that included the GMEP2_User role, the GMEP2_User role status may only be updated in one. Upon verification (see Verify an Assigned Functional Role), the status will update accurately.

Figure 3.2-11 User Role Enablement

NOTE: If the user account was manually disabled, the GMEP2_User role will not be automatically provisioned, and the Functional Role must be requested upon enablement.

If a user is disabled because their organization has been disabled by an Operations Administrator, the user cannot be enabled, and a message will be displayed above the Organization field. The figure below displays the profile of a user in a disabled organization.

Figure 3.2-12 Disabled Organization User Profile

[Back to Table of Contents]

3.2.3 Lock a User's Account

This process is used to lock a user's account, which will prevent the user from logging in to their MyGinnieMae account while still retaining functional roles. Locking is a temporary action, different from permanently disabling a user account as described in Disable a User Account, which removes the functional roles from the user's account.

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
3. Select the **User Management** tile.

Figure 3.2-13 Access Management Console Landing Page
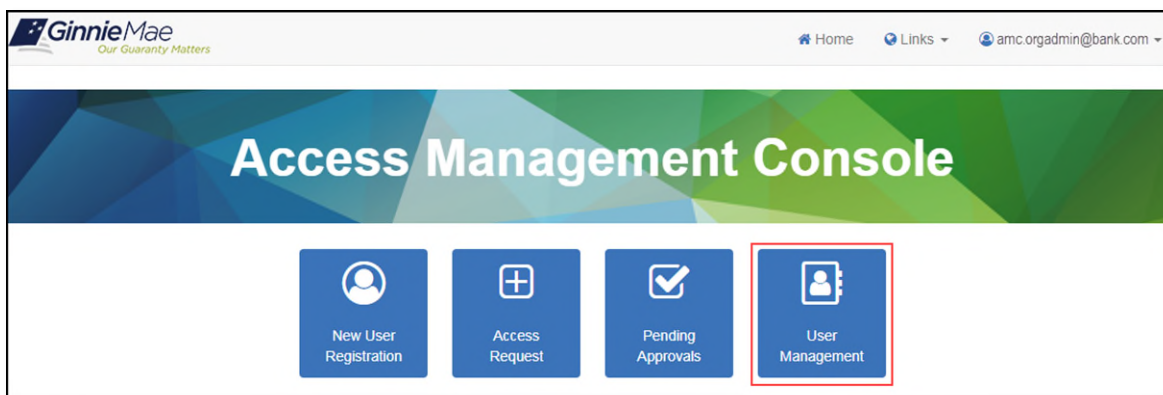
4. Find and select the Display Name of the user account to lock.

    a. Verify that the user is not already locked by confirming that there is no locked icon (🔒) to the left of their Display Name.

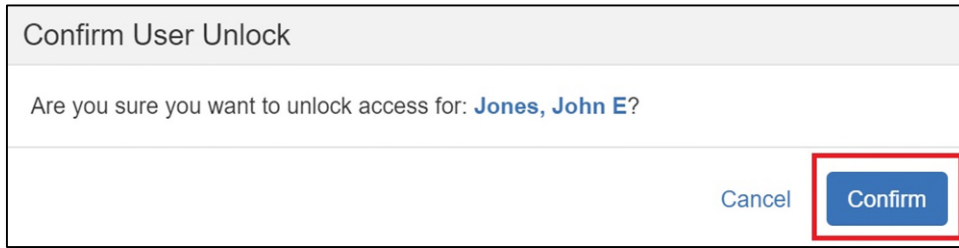**Figure 3.2-14 Search Users Results**
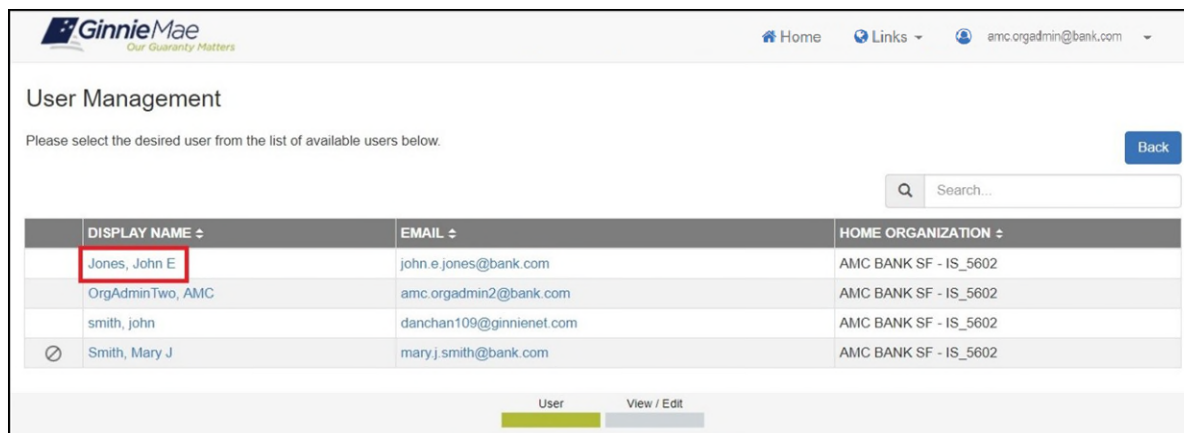
5. Select the "Edit User Profile" down arrow ▼.
    a. Select **Lock**.

Figure 3.2-15 User Management - Lock Account

6. The system opens a dialog box to confirm the account lock.
   a. Review the user details.
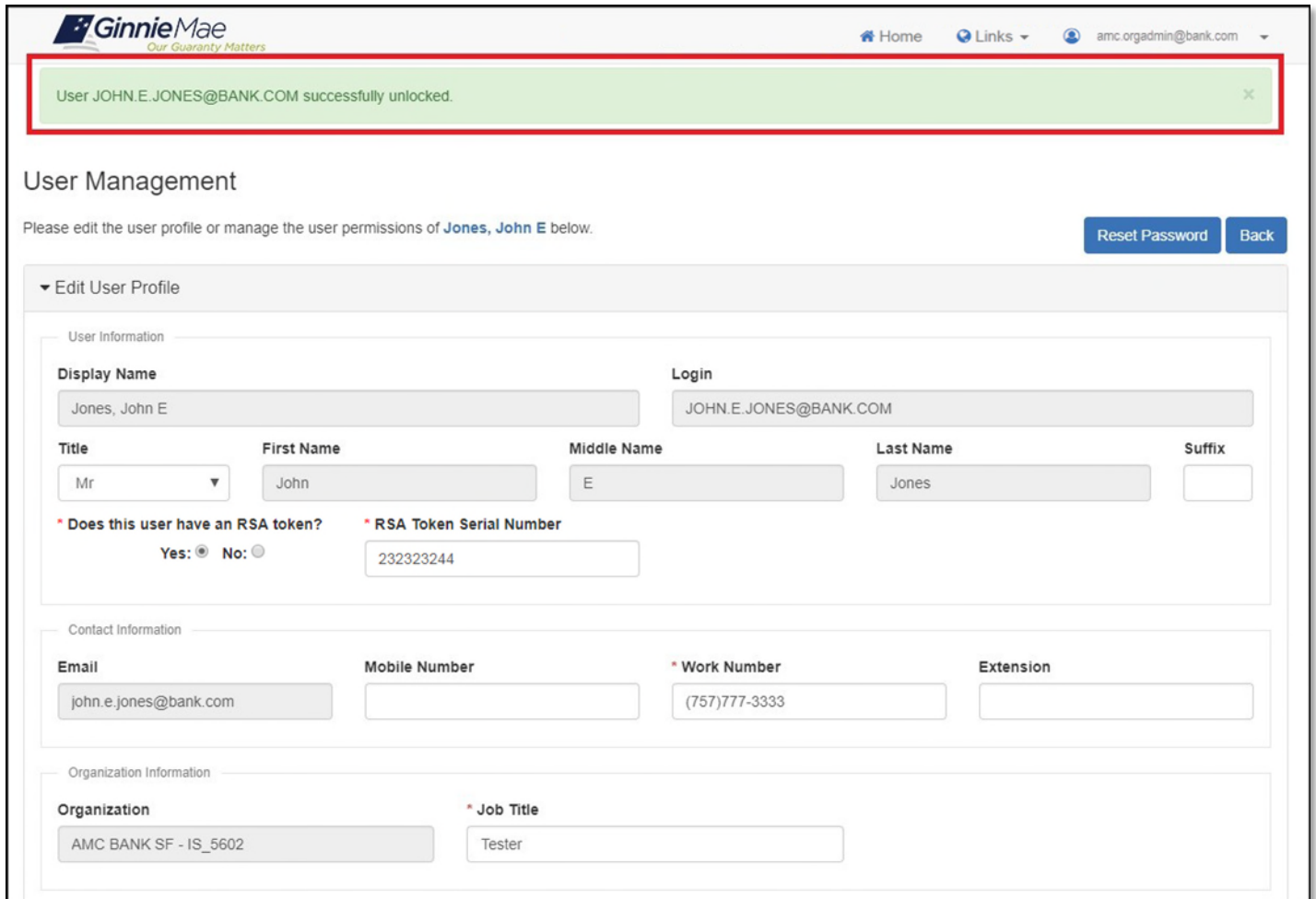   b. Select **Confirm**.

Figure 3.2-16 Confirm Account Lock

7. The system displays a a "User [User Name] successfully locked" green notification ribbon message and updates the Account Status to "Locked".

Figure 3.2-17 Lock Account Notification

[Back to Table of Contents]

3.2.4 Unlock a User's Account

A user can become locked out of their account for a variety of reasons including:

- Locked out by the Organization Administrator

- Three failed attempts to enter correct username and password

You can unlock the user's account by completing the following steps:

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
3. Select the **User Management** tile.
4. Find and select the Display Name of the user account.

Figure 3.2-18 Locked User Search
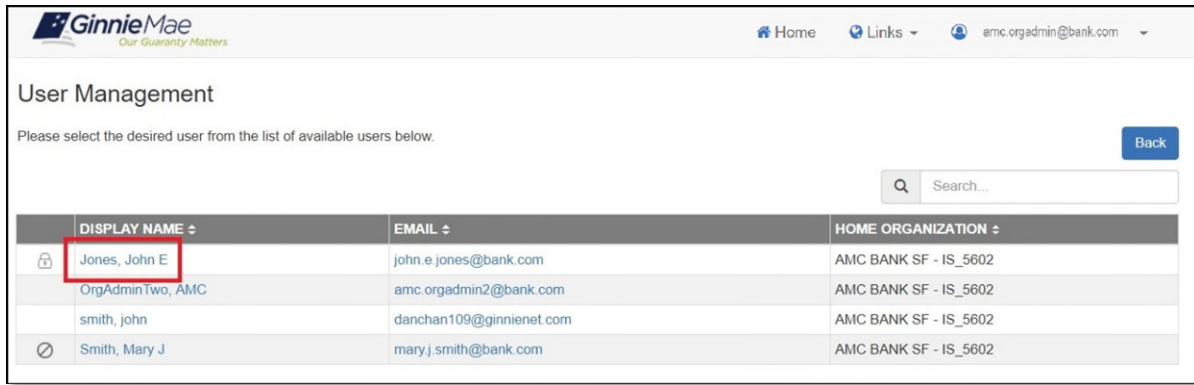
5. Select the "Edit User Profile" down arrow ▼ .
   a. Select **Unlock**.

Figure 3.2-19 User Management Unlock Account
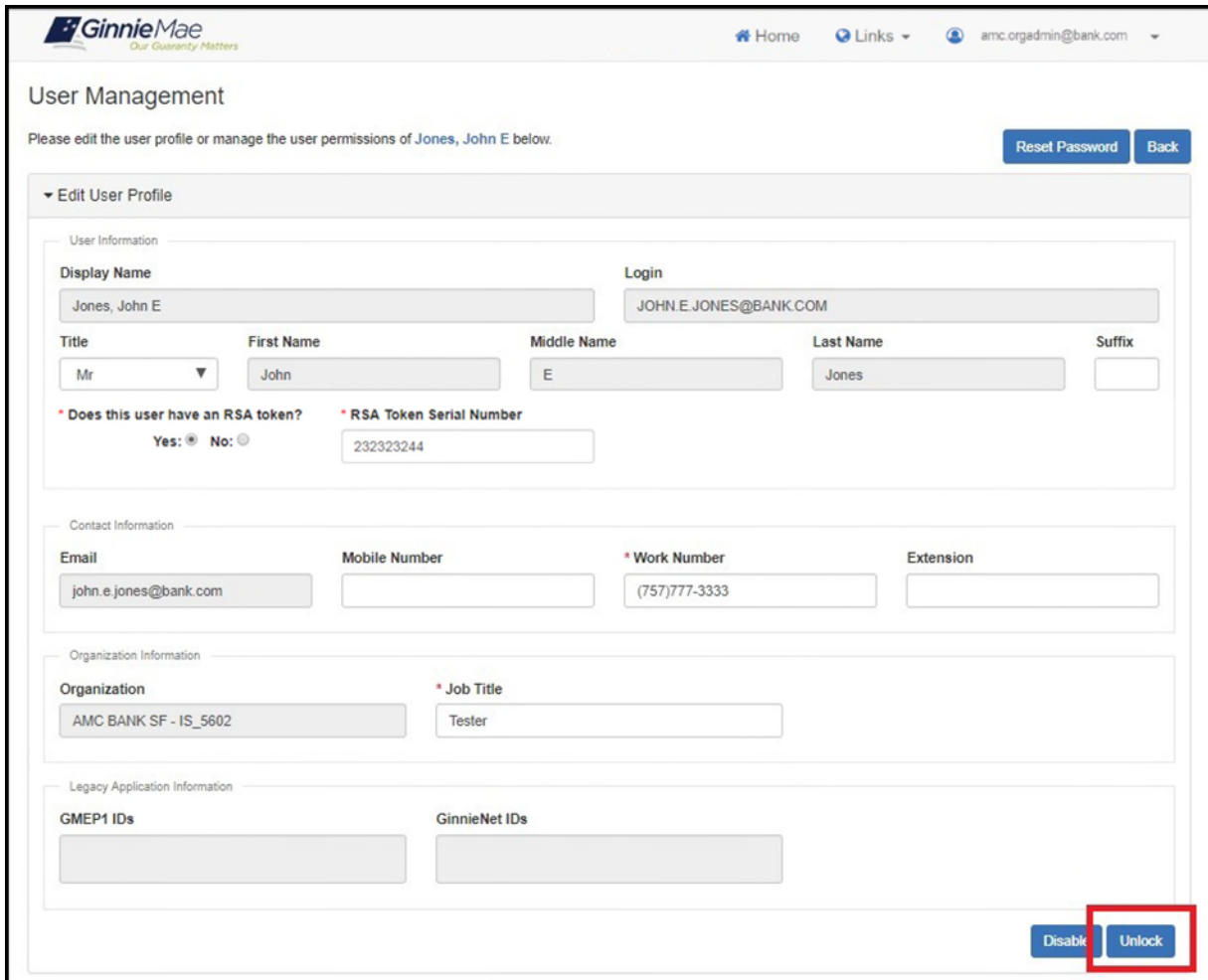
6. The system opens a dialog box to confirm the account lock.
   a. Review the user details.
   b. Select **Confirm**.

Figure 3.2-20 Confirm Unlock Account

7. The system displays a green notification ribbon that "User [User Name] successfully unlocked." The page updates the Account Status to "Unlocked".

Figure 3.2-21 Unlock Account Notification

[Back to Table of Contents]

3.2.5 Update a User's Profile Attributes

End Users have limited ability to update their own Profile Attributes which include, mobile number, fax, job title, start date, job functions, and professional background summary. All other account attributes must be updated by

the Organization Administrator. Follow the steps below to update any of the following user's account attribute information.

- Title (Mr., Mrs., etc.) [required attribute]

- Suffix

- Mobile Number

- Work Number [required attribute]

- Extension

- Job Title [required attribute]

- Does this user have an RSA token? (Y/N)

- RSA Token Serial Number (See Update a User's RSA Token.)

NOTE: If the user's email address has changed, a new End User account must be created. Contact Ginnie Mae Customer Support for assistance.

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
3. Select **User Management** tile.
4. Find and select the Display Name of the user account.
5. Select the "Edit User Profile" down arrow ▼ .
    a. Edit the fields for desired attributes.
    b. Select **Save**.

NOTE: The "Save" button is not displayed unless an attribute has been edited.

The "Save" button is not displayed unless an attribute has been edited.

Figure 3.2-22 User Management Update User Pofile

NOTE: Error notifications may be displayed on the User Profile screen in the AMC if attributes are in the incorrect format. The "Save" option will not be displayed until the format is corrected.

Telephone numbers must be in the (555) 555-5555 format, and the number and area code cannot begin with a 1 or a 0.

Figure 3.2-23 Telephone Incorrect Format

6. The system displays a dialog box to confirm the updated attributes.
    a. Select **Confirm**.

Figure 3.2-24 Confirm User Profile Update

7. A "User [User Name] successfully updated" green notification ribbon displays.

Figure 3.2-25 Update User Profile Notification

[Back to Table of Contents]

3.2.6 Update a User's RSA Token Information in MyGinnieMae

(1) Update an Existing Token Holder

If the user already has an active SecurID Token issued by BNYM on behalf of Ginnie Mae, retrieve the Token serial number and follow the steps below to ensure the Token will be associated with the account:

1. Send an email to GinnieMae1@bnymellon.com with the following information:
   a. Subject: MGM Account to be added to RSA Token for (user's name)
   b. Email Body:
      i. Title (Mr., Mrs., Ms.)
      ii. Token Holder Name
      iii. MGM Username
      iv. Job Title
      v. Phone Number
      vi. Issuer/Custodian ID
      vii. GMEO 1.0 ID
      viii. RSA Token Serial Number
2. Refer to Update User's Profile Attribute above.
3. Update the following fields in the User Management Update User Profile screen.

Figure 3.2-26 User management Update User Profile Screen

(2) Update a New Token Holder

If the user does not have an active SecurID Token, follow the steps below:

1. Fill out the SecurID Token Order form.
2. Send the completed SecurUD Order form to GinnieMae1@bnymellon.com to be processed.

The request will be processed, and you will receive confirmation within 72 hours. Incomplete requests will not be processed. **The user must be listed on the HUD 11702**.

[Back to Table of Contents]

3.2.7 Reset a User's Password

This service is used in the event the End User has forgotten their password and is unable to reset it using self-service capabilities or if the End User suspects their account has been compromised. The End User should first attempt to create a new password using the Forgot Password functionality. If their attempt is unsuccessful, follow the steps below:

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
3. Select the **User Management** tile.
4. Find and select the Display Name of the user account.
5. Select **Reset Password**.

NOTE: This button is inactive if the user is disabled.

Figure 3.2-27 Reset Password Button

6. The system opens a dialog box to confirmation that an auto-generated temporary password will be sent to the user.
   a. Select **Confirm**.

Figure 3.2-28 Reset password Form

7. The system displays a green notification ribbon at the top of the page that the password reset was successful. The End User may go to their email to retrieve the temporary password and will be required to change their password once upon next login.

Figure 3.2-29 Reset Password Notification

3.2.8 Remove Functional Roles from a User

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. To remove a role from an End User account, follow the steps provided below.

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
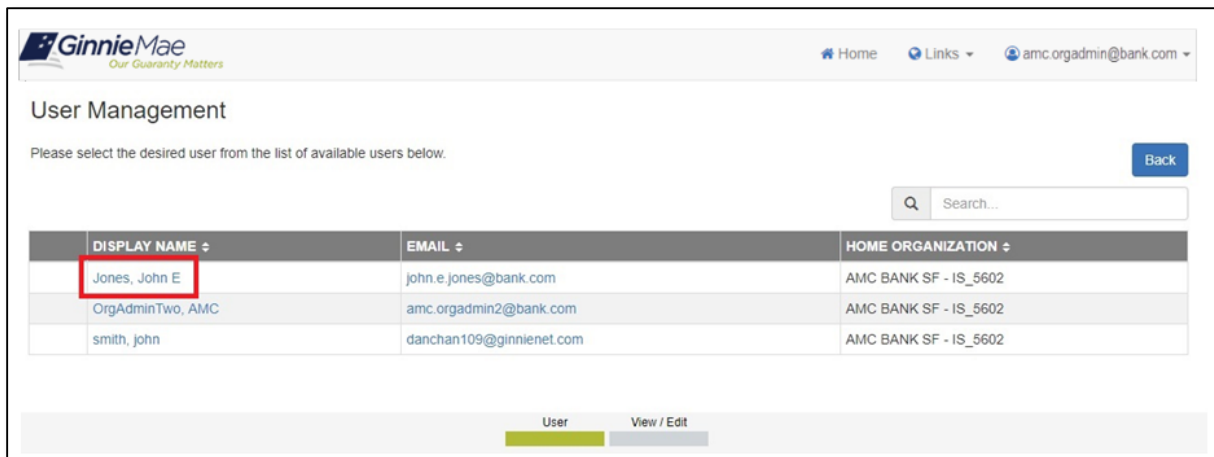3. Select the **User Management** tile.

Figure 3.2-30 Access Management Console Landing Page
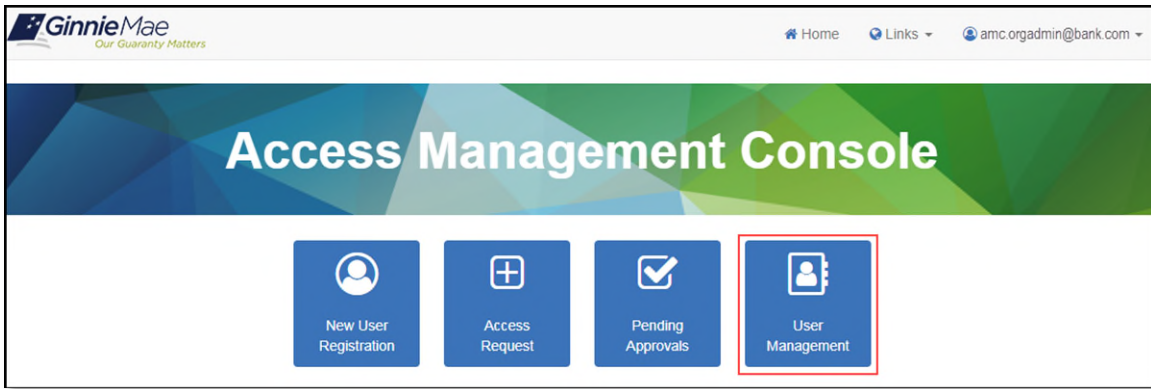
4. The system displays a list of available users. Search for a user by typing one of the following user properties into the search field to locate the desired End User:

- Display Name
- Email
- Home Organization

Figure 3.2-31 Select User

5. The system displays the User Profile page.

   a. Select the down arrow ▼ next to "Manage User Permissions" to display the roles assigned to the user.

Figure 3.2-32 User Profile

6. Review the listed roles for the user,
   a. Select the check box for the Functional Role to be removed.
   b. Select **Remove**.

Figure 3.2-33 Remove Functional Roles

7. The system displays a confirmation message.

    a. Select **Confirm** to proceed with the removal of the selected Functional Role.

Figure 3.2-34 Confirm Functional Role Removal

8. The system displays a success green notification ribbon at the top of the page.

Figure 3.2-35 Functional Role Removal Notification
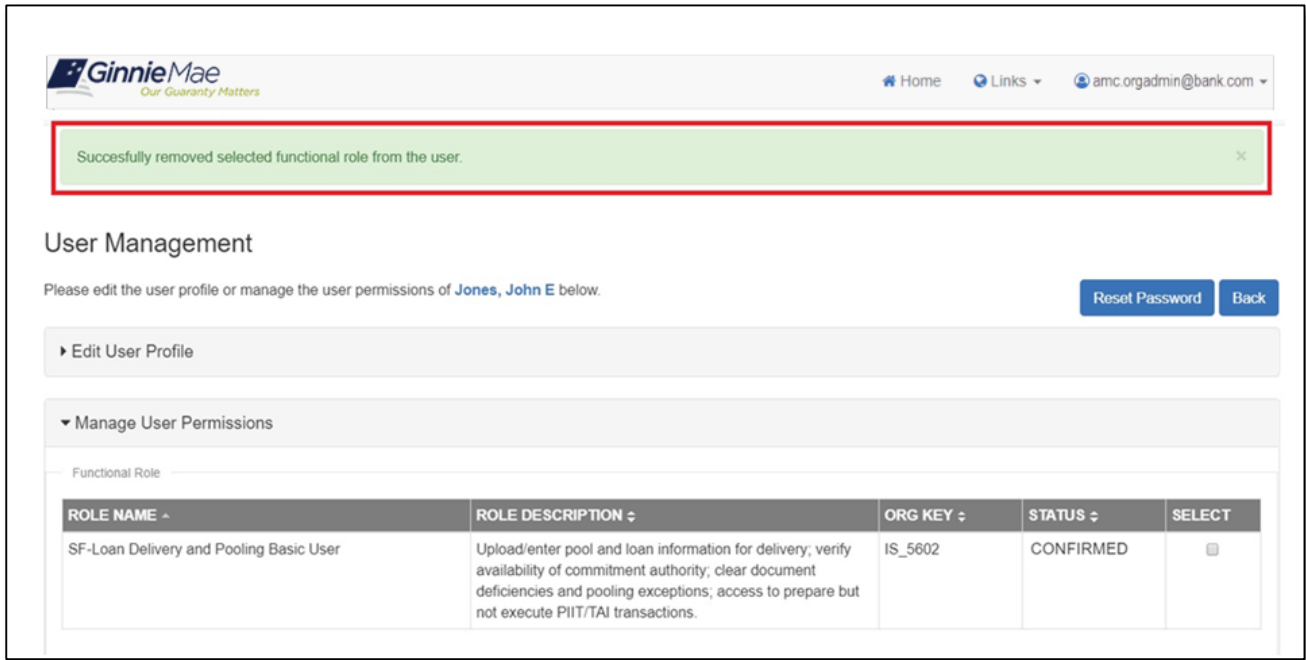
9. When the role has been successfully removed, the status of the role changes to "REVOKED." No additional approvals are required after the removal is confirmed.

Figure 3.2-36 Functional Role Removal Notification
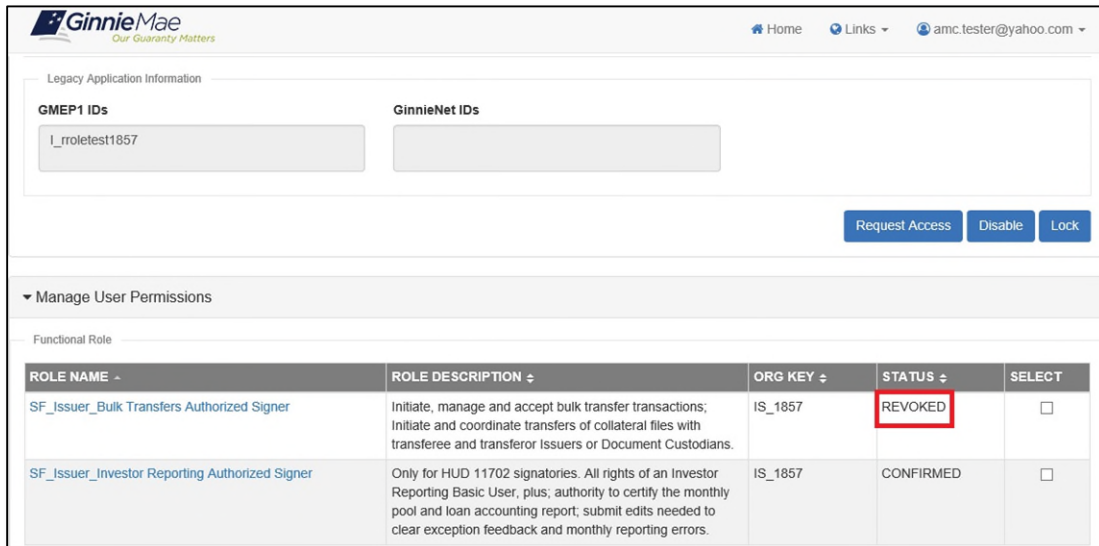
NOTE: If a Functional Role is removed inadvertently, it can be requested again by following the steps in Request Functional Role.

[Back to Table of Contents]

3.2.9 Review the Status of a Functional Role Access Request

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 End User until all necessary approvals are completed. To review the status of a Functional Role request for a user, follow the steps below.

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
3. Select the **User Management** tile.
4. Find and select the Display Name of the user account.
5. Select the down arrow ▼ next to "Manage User Permissions". The system displays the Functional Role(s) assigned with various statuses indicating the state of the request in the Access Request Workflow:
    - 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.

Figure 3.2-37 Functional Role Status

6. Select the "Role Name" to reveal the Functional Role Entity Status overlay. The overlay contains details about the user's Functional Role(s):
    - Request Date
    - Requester
    - Approval Date
    - Approver
    - Finalized Date

- Finalizer
- Status

Figure 3.2-38 Functional Role Entity Status Overlay

[Back to Table of Contents]

3.2.10 Verify an Assigned Functional Role

After the Operations Administrator has finalized a Functional Role request, it is advisable that the Org Admin verify that all the underlying roles were successfully assigned to the user account. If there is a system error, the Organization Administrator group will receive an email notification and will need to contact Ginnie Mae Customer Support. To manually verify the status of a Functional Role request, follow these steps:

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
3. Select User Management tile.
4. Find and select the Display Name of the user account.
5. Select the down arrow ▼ next to "Manage User Permissions" to display the roles assigned to the user.
   - Select the checkbox for the corresponding Functional Role(s) from the list.
   - Select **Verify**.

Figure 3.2-39 User Management - Verify Functional Roles
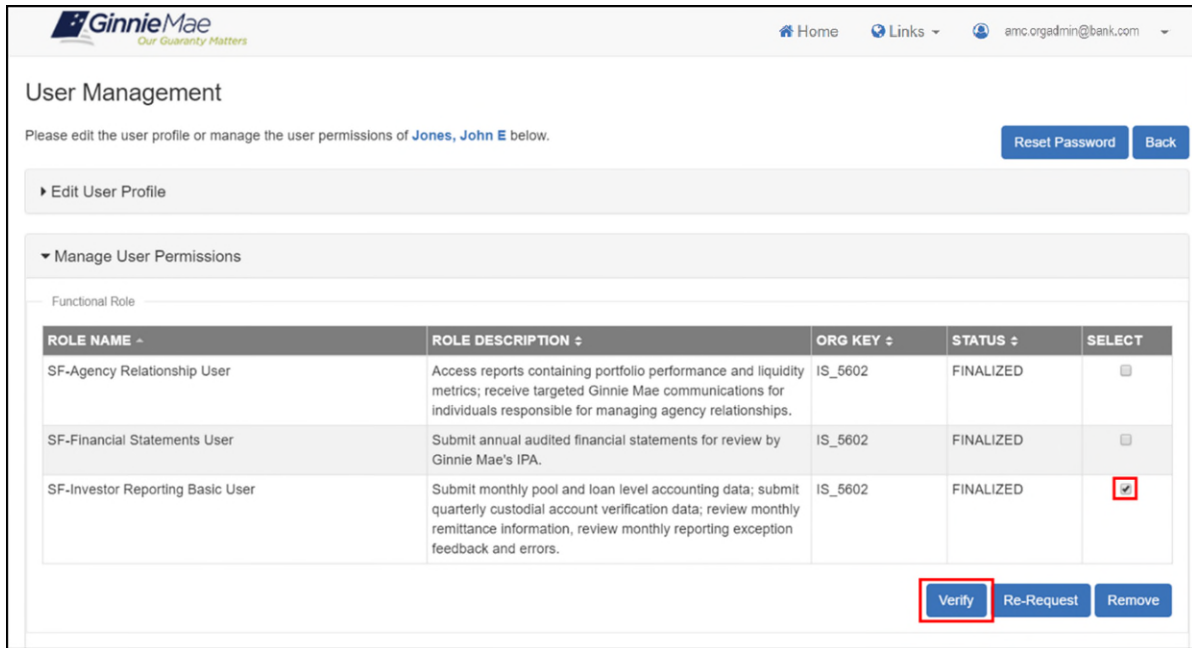
6. The system checks the user's access to underlying roles against the Functional Role profile and displays the updated "Status" of the Functional Role.

The entire set of underlying roles within a Functional Role is either successfully provisioned or an error occurred resulting in the other statuses below. In the latter case, check for an email regarding error notification, attempt to re-request, and, if the issue persists, contact the Ginnie Mae Customer Support.

- CONFIRMED—All underlying Functional Role entities are provisioned. The system updates the Functional Role to "CONFIRMED" automatically upon successful provisioning and receipt of legacy IDs. If that is not the case, the "CONFIRMED" status will not appear.

- PARTIAL – MISSING—Some Functional Role entities are not provisioned.

- MISSING—No Functional Role entities are provisioned. If the End User was disabled due to 90 days of inactivity, the Functional Role status will display as "MISSING."

- PARTIAL – NO ACCOUNT—The legacy system (GMEP or Ginnie*NET*) has not returned a legacy ID for a requested legacy role.

NOTE: If Legacy provisioning has not been fully completed before the user verifies, this status will be displayed. Provisioning should complete within 25 minutes after an Operations Administrator completes finalization. If the status is still "PARTIAL – NO ACCOUNT" after 25 minutes, the Organization Administrator should reach out to the Operations Administrator for troubleshooting and investigation).

- FAILED—The request did not complete successfully.

- REVOKED—The Functional Role was previously provisioned for the End User and has been removed or the requested role was rejected by the second Organization Administrator. A revoked role can be requested again through the Workflow.

Figure 3.2-40 Verified Functional Role Status

7. If the "Status" is not "CONFIRMED," the role can be re-requested following the steps in Re-Request a Functional Role.

[Back to Table of Contents]

3.2.11 Re-Request a Functional Role

After you have taken steps to Verify an Assigned Functional Role if you find roles that are not in "CONFIRMED" status, you can re-request the Functional Role to complete the provisioning of the role. Below are the steps to re-request a Functional Role. If the End User was disabled due to 90 days of inactivity, the you must Enable a User's Account before re-requesting Functional Roles.

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
3. Select **User Management** tile.
4. Find and select the Display Name of the user account.
5. Select the down arrow ▼ next to "Manage User Permissions" to display the roles assigned to the user.
6. Select the checkbox for the corresponding Functional Role that is in "Missing" status.
    a. Select **Re-Request**.

NOTE: The "Re-Request" button will not be visible for a role whose status is listed as Revoked. To re-request a revoked role for a user, follow the Request Access Workflow in Request Functional Role.

Figure 3.2-41 Re-Request Functional Role
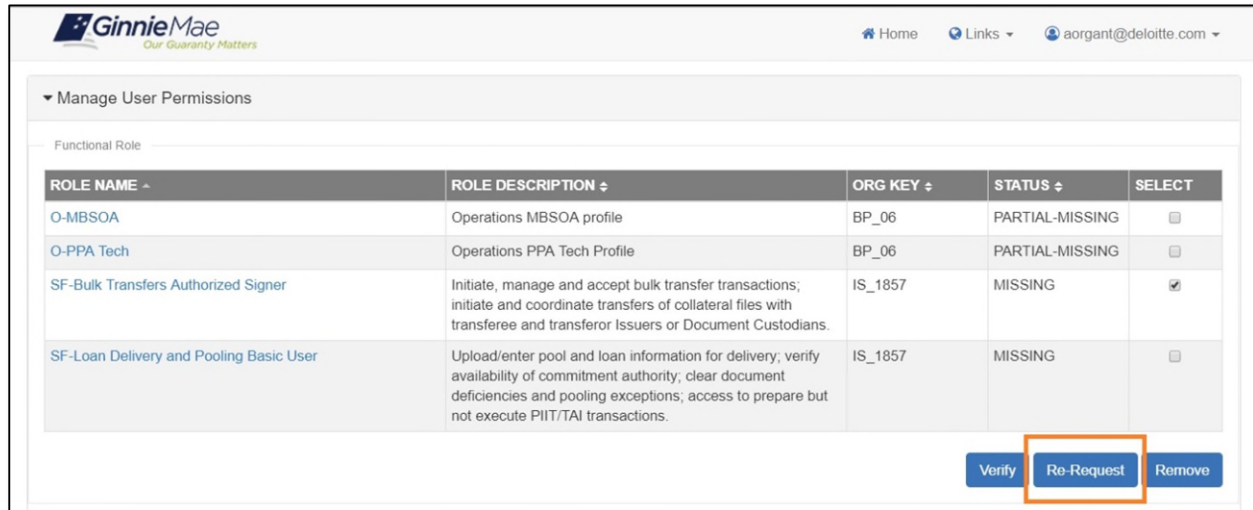
7. The system submits a request for any missing Functional Role entities, displays a notification ribbon at the top of the screen, and updates the status of the role.

Figure 3.2-42 Re-Request Functional Role Status Update

NOTE: If an attempt is made to re-request a "PENDING" or "APPROVED" role, the system displays a message that the role cannot be re-requested.

Figure 3.2-43 Re-Request Functional Role Error

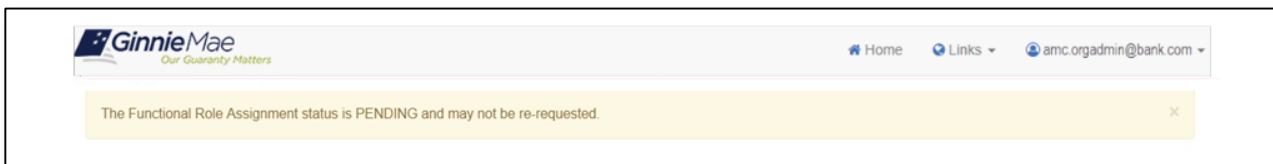[Back to Table of Contents]

3.2.12 How to De-register a User with the Oracle Mobile Authenticator

If a user has registered with the Oracle Mobile Authenticator (OMA) application to have the OTP delivered to a smart device, they will need to de-register if they replace their smart device, have deleted and re-downloaded the OMA, or no longer wish to have the option of accessing OTP generated by the OMA. This is a function that End Users are able to complete on their own following instructions on the Deregistering with the Oracle Mobile Authenticator QRC. To complete this process on behalf of and End User you may follow these steps:

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
3. Select **User Management** tile.

Figure 3.2-44 Access Management Console Landing Page
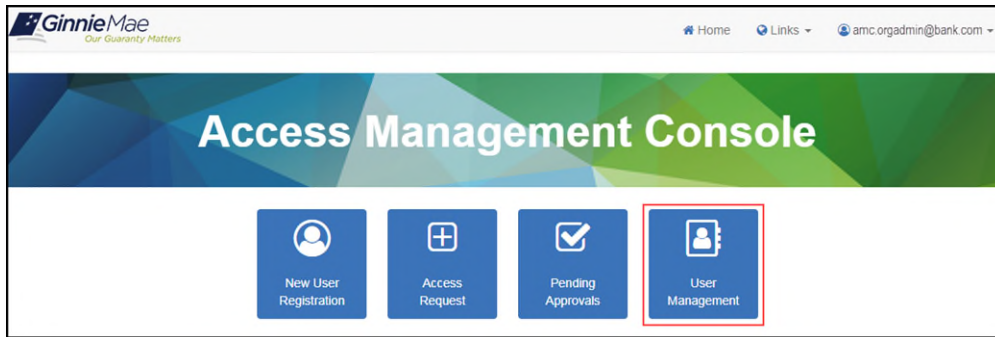
4. Find and select the Display Name of the user account.

Figure 3.2-45 Search Users Results

5. Select **De-register OMA**.

Figure 3.2-46 De-register OMA Button on the User Profile Page

6. The System opens a dialog box to confirmation the de-registration of the OMA.
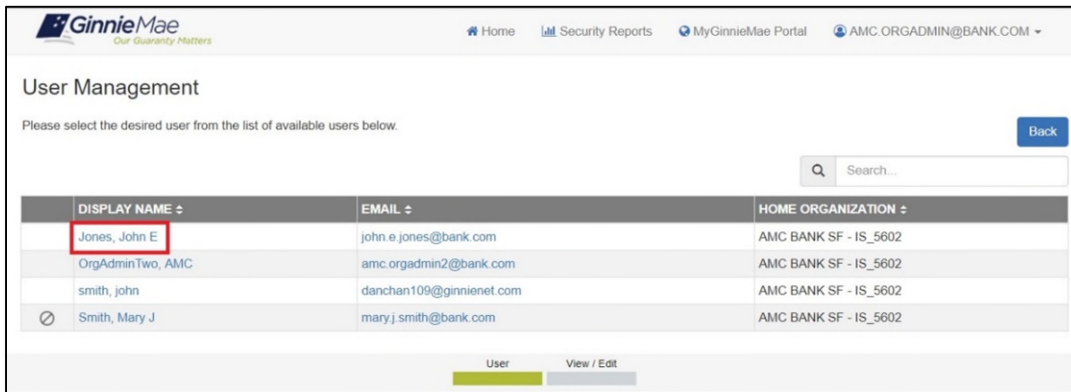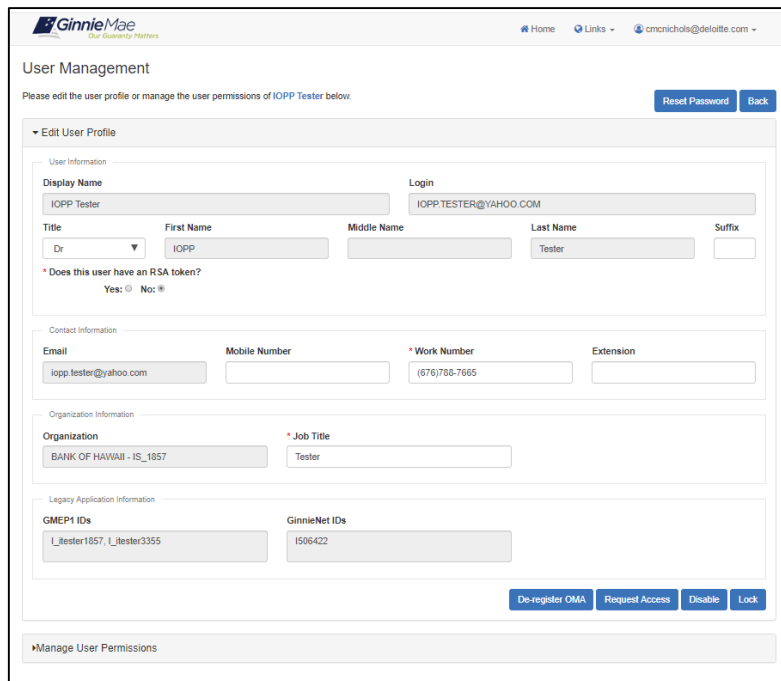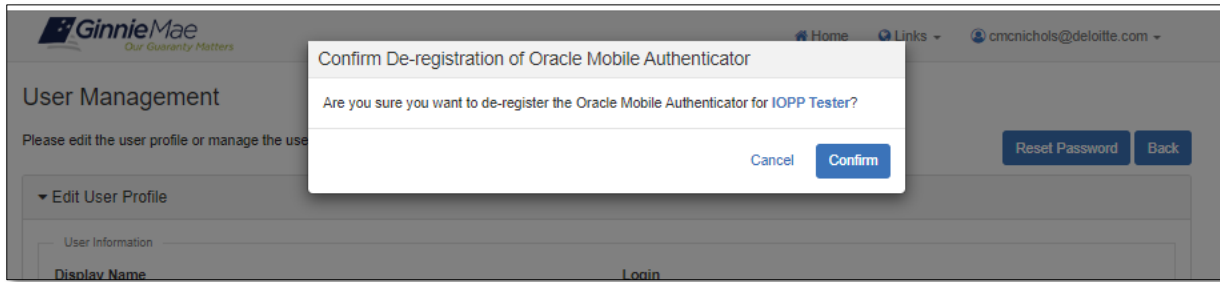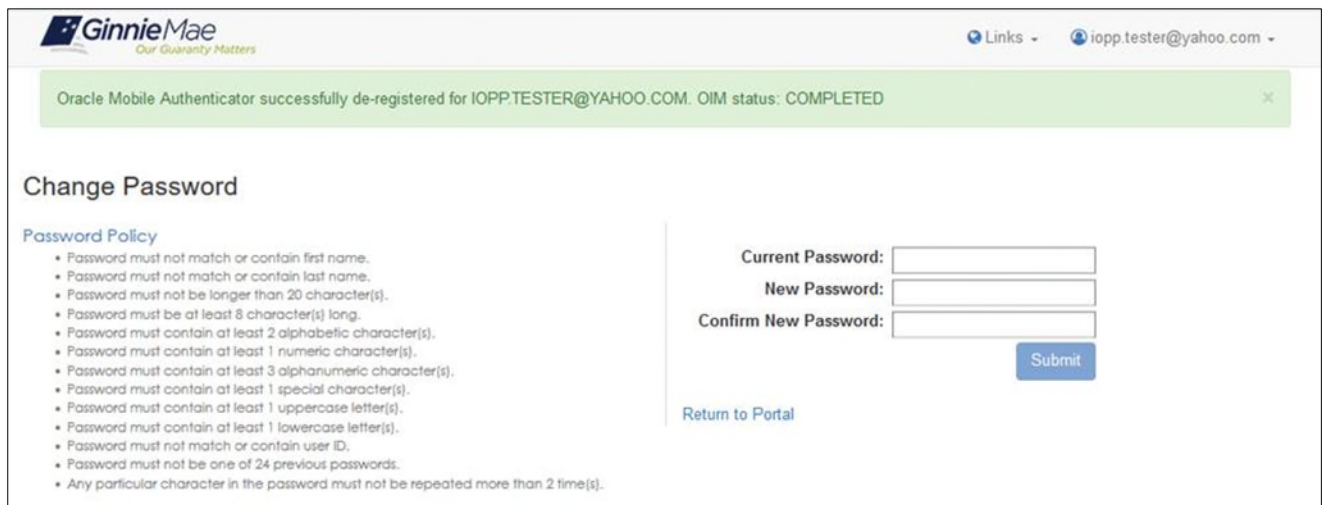   a. Select **Confirm**.

Figure 3.2-47 Confirm De-registration of OMA as Org Admin

7. The system displays a green notification ribbon that the user's device has been successfully de-registered.

Figure 3.2-48 Message of Successful De-registration

[Back to Table of Contents]

4   REPORTS

4.1   Administrative Reports

4.1.1   Report Types

The following reports are available to Organization Administrators via the AMC:

Table 4.1-1 Reporting for Organization Administrators

Service	Reports	Type	Description
User Registration	Home Organization User List Org Admin View User Profile History User Registration Request History	Custom Standard Custom	**Home Organization User List Org Admin View** – Provides a list of all users in your organization including phone number, job title, date the user's account was created, current status (active or disabled), the last date the user logged in and if the account is currently locked. You can also see if

Service	Reports	Type	Description
			the user has an RSA token. If the user has and token, you can see the RSA serial number. **User Profile History Org Admin View** – Provides users login audit information in your organization including last login date, Created By Login, Updated By Login, user id status etc. including Date Effective From, Time Effective From. **User Registration Request History Org Admin View** – Provides a list of user registration information for both completed registrations and registrations that have not been completed. Information that is provided for completed registrations include the request ID, user login, the Org Admin who sent the registration invitation to the user, the date the invitation was sent, the date the registration request was submitted by the user, the Org Admin who approved the registration request, the date the request was approved and the approval status. For registrations that have not been completed the task number, user login, the Org Admin who sent the registration invitation, the date the invitation was sent and the status of the invitation.
Access Requests	AMC Functional Role Request History	Custom	**AMC Functional Role Request History** – Provides the functional role request history for your organization. The information provided includes the request ID, user login, functional role type, Org key, Status, the Org Admin who submitted the request and the date the request was submitted, the Org Admin who approved the request and the date the request was approved, the Operations Admin who finalized the request and the date the request was finalized or the Operations admin who revoked the request and the date the request was revoked.
Multifactor Authentication (MFA)	Accounts Locked Out Report Authentication Statistics Report	Standard Standard	**Accounts Locked Out Report** – Provides a list of all locked users in your organization including user id, time stamp when the account was locked. **Authentication Statistics Report** – Provides the number of times and the dates the authentication process was attempted by the users in your organization. You have the ability to sort by date range or time range. You can also sort by authentication success, failure or all.

| Service	Reports	Type	Description
Self-Service Change Password	Password Expiration Summary	Standard	**Password Expiration Summary** – Provides a list of the users in your organization whose passwords have expired. You have the ability to sort by first name, last name, user ID. You can also sort by date range.

[Back to Table of Contents]

4.1.2 Accessing Administrative Reports

To access the list of available reports, follow the steps below:

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
3. Select the down arrow ▼ next to Links in the header.
   a. Select Security Reports.

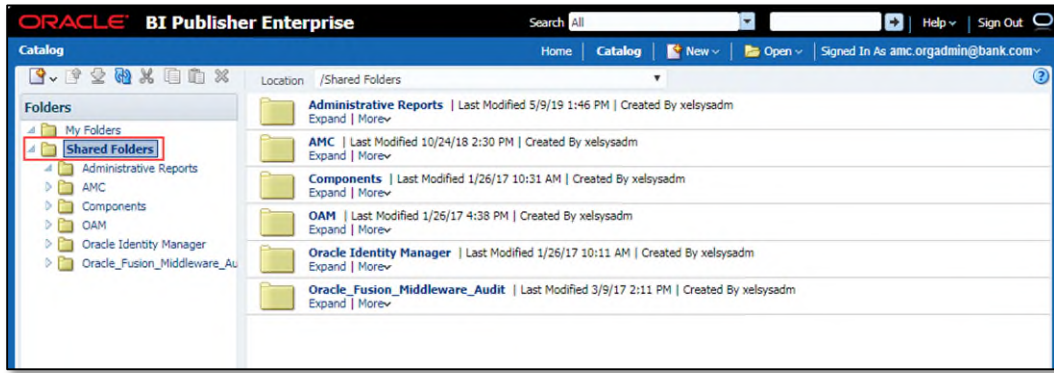**Figure 4.1-1 Security Reports Link**
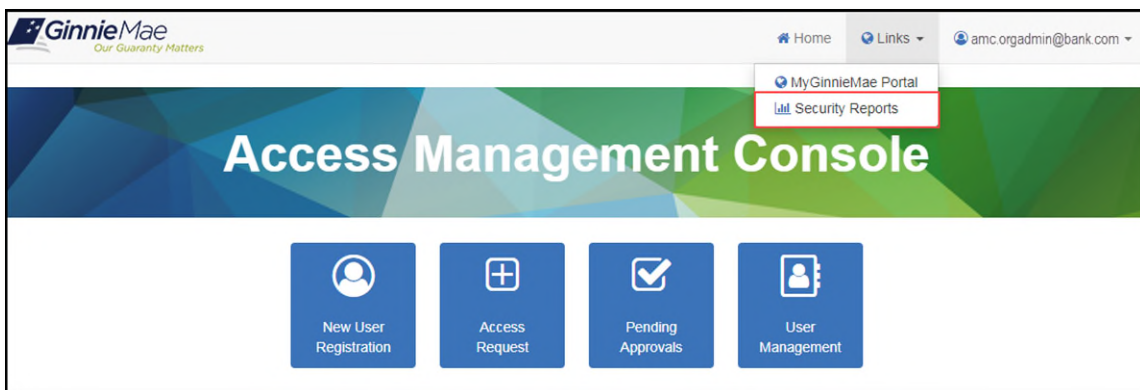
4. The system will open the BI Publisher Enterprise page in a new window.
   a. Select Catalog Folders on the left side of the page.

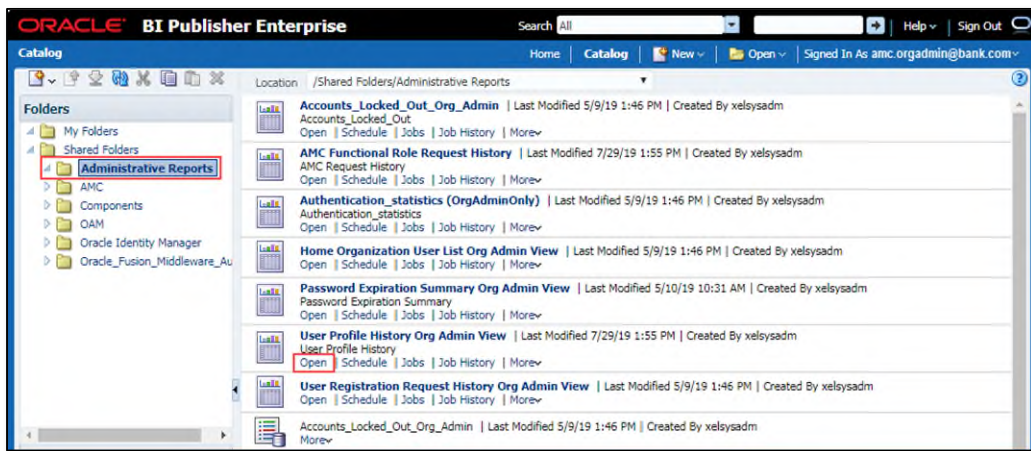**Figure 4.1-2 Report Catalog Folders**
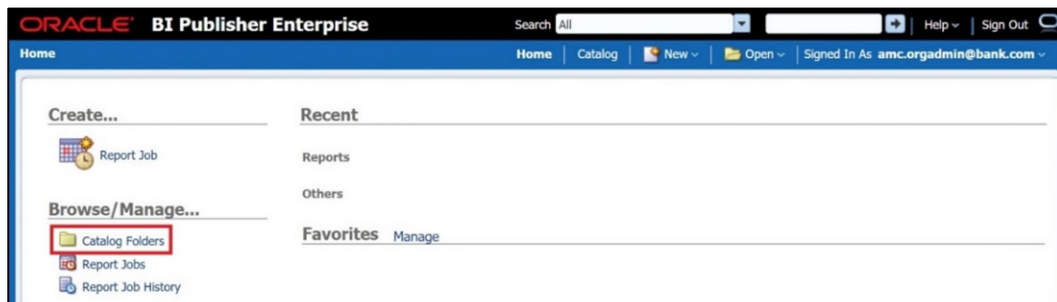
5. Select Shared Folders to expand the folder.

Figure 4.1-3 Oracle Identity Manager Reports

6. Select Administrative Reports folder.

Figure 4.1-4 Open User Profile History Report

7. The reports will be displayed.
    a. Select Open under the desired report.
8. For Custom Reports
    a. The report can be filtered and sorted by selecting the down arrow in the column header.
9. For Standard Reports,
    a. Search for specific users using the User Profile History.
    b. Filter to generate reports by users, roles, date range, etc.

Figure 4.1-5 Search Profile History
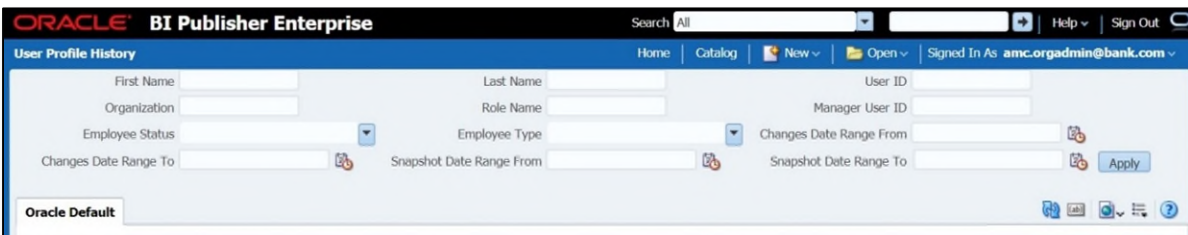
NOTE: Data will not be displayed if the date range filter is not used in conjunction with other filters.
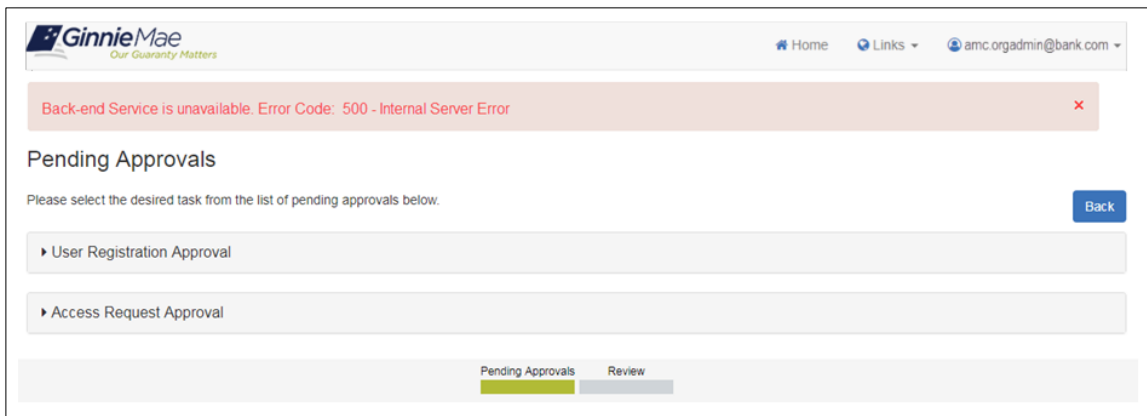
[Back to Table of Contents]

5 TROUBLESHOOTING AND SYSTEM ERRORS

This section is designed to help identify common errors you may encounter as an Organization Administrator and provide tips for troubleshooting issues. If the suggested tips are unsuccessful or errors persist, refer to Ginnie Mae Customer Support.

5.1 AMC Error Page

Issue: The system displays an error message to the End User because a service is temporarily unavailable.

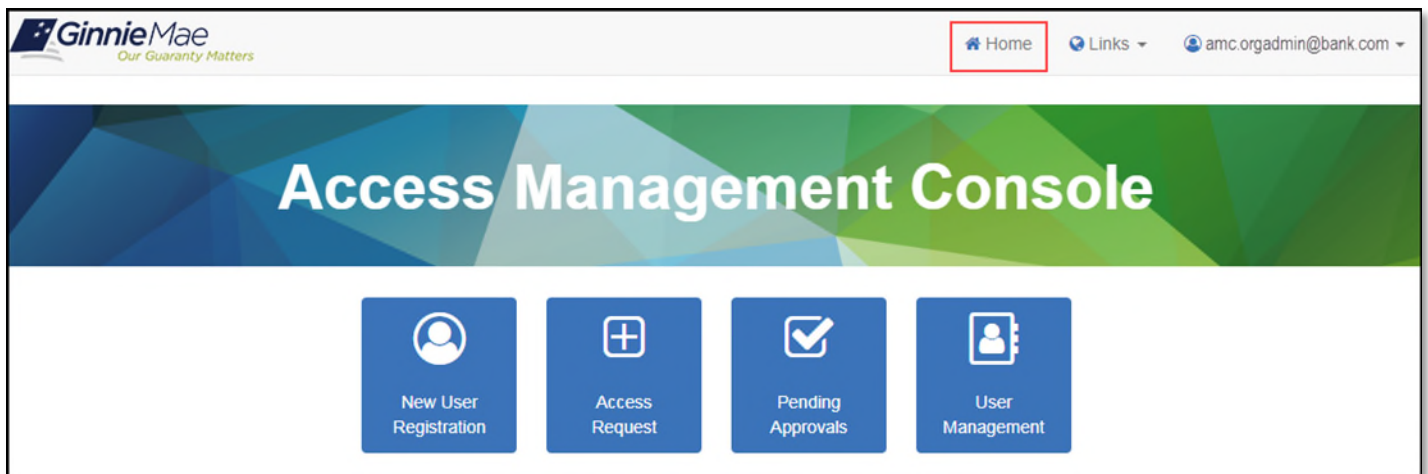**Figure 5.1-1 Back-End Service Unavailable Error**

Resolution: User should attempt to refresh ⟳ the page in the web browser or return to the AMC landing page by clicking the Home icon at the top of the screen.

Figure 5.1-2 Return to AMC Landing Page

[Back to Table of Contents]

5.2   AMC Module Error Notification Ribbons

Within each AMC module, the AMC displays a notification ribbon on the page each time a confirmed action is taken by the user (for example, after submitting an access request or updating a user attribute). Successful message notifications display in a green ribbon. Errors are displayed in a beige or red ribbon.

Issue: If the backend system does not receive the confirmed action, an error message is displayed with notification of the failed action.
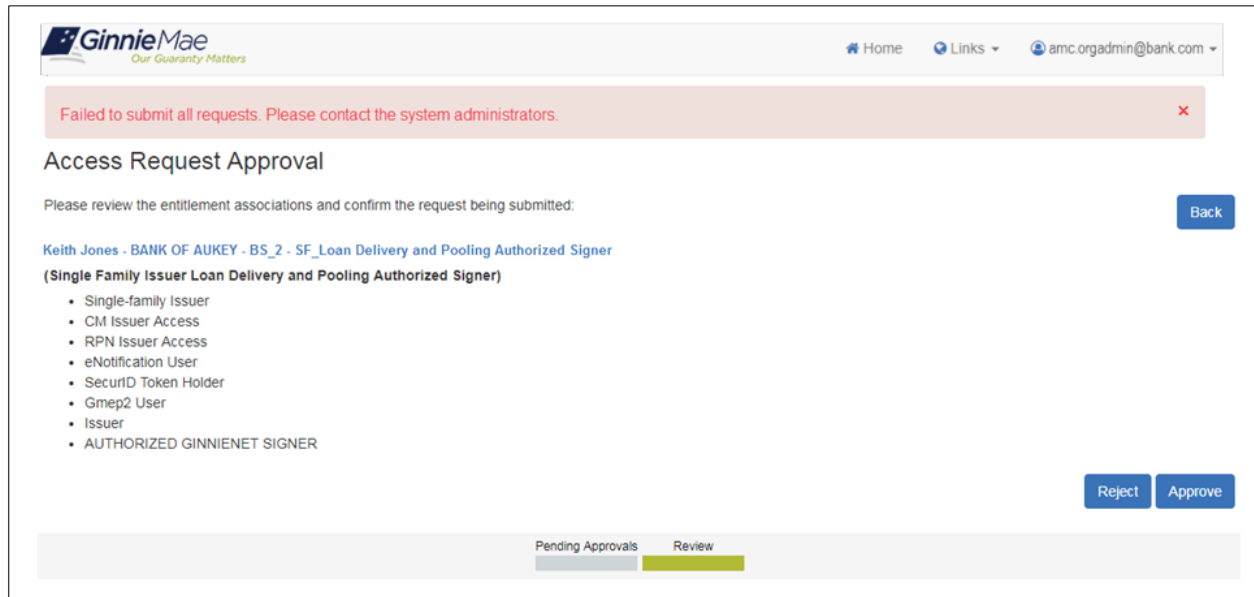
Figure 5.2-1 Failed Access Request Submission

Figure 5.2-2 Failed User Registration Approval

Resolution: Re-attempt the action. If failures continue contact Ginnie Mae Customer Support.

[Back to Table of Contents]

5.3   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**.**

Figure 5.3-1 Email is Already Registered Error

Resolution: Since the system is configured to prevent invitations to email addresses already registered. If attempting to add a functional role, please refer to Request Functional Role**.**

5.4   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.

Figure 5.4-1 Three Invitations Sent Alert

Resolution: This is a warning message. No action is required as an invitation can be sent up to five times.

5.5   Five-Time Invitation 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.

Figure 5.5-1 Five Time Invitation Flag

Resolution: In order to send another invitation to the user's email address, action is required from the Operations Administrator group. Contact Ginnie Mae Customer Support.

[Back to Table of Contents]

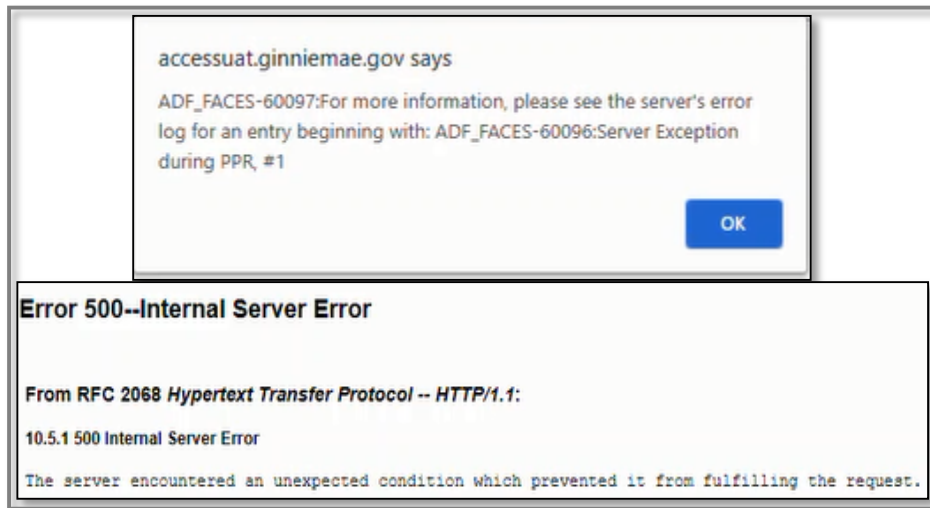## 5.6   Incorrect Email Format

Issue: When sending a New User Registration invitation to an End User, if an incorrect email format has been entered in the email field, the following validation message appears. The system is validating for the typical email format—sample@sample.sam.

Figure 5.6-1 Registration Email Form Error

After the steps above, if a correct email format is entered and the" Submit" button is clicked, the following error is displayed: "ADF_FACES…". The registration page then displays the 500-error shown below.

Resolution: When an incorrect email format is entered and the "Error: This 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 invitation form after seeing this error.

5.7   New Password Mismatch Error

Issue: In the process of a password reset or if a user incorrectly enters a matching password, they will receive the system generated error, "Password does not match."

Figure 5.7-1 New Password Does Not Match Error
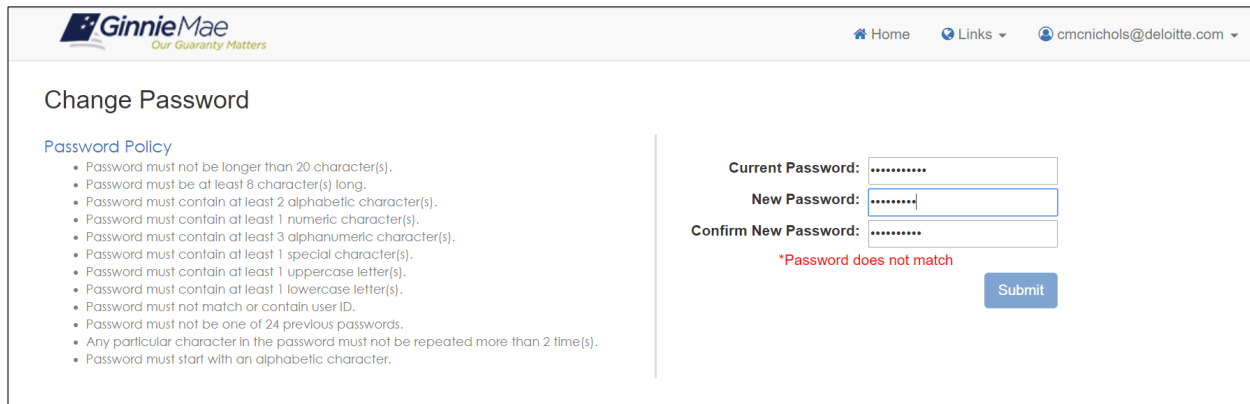
Resolution: The user must retry and enter a matching password.

MyGinnieMae provides Organization Administrators an audit trail and additional insight into the user accounts for your organization in Ginnie Mae business systems. These reports capture logs and event data for various identity and access management events. This section describes the reporting capabilities and provides instructions on how to access reports.

6   RESOURCES

The Resources 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.

Refer to MyGinnieMae Portal Getting Started Manual.

6.1   Training Resources

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

6.2   QRCs

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

6.3   Help Desk Contact Information

To contact Ginnie Mae Customer Support call (1-833-466-2435) or email askginniemae@hud.gov .

6.3.1   Help with System Access

The Operations Administrators for the MyGinnieMae portal may 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.

End Users are encouraged to utilize their Organization Administrators, the information found in the Getting Started Manual and other Tools and Resources found on the Ginnie Mae website. End User are invited to utilize Ginnie Mae Customer Support for additional guidance and support.

6.4   MyGinnieMae Portal Dictionary

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

6.5   MyGinnieMae Self-Help Tools

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

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

Easy reference tools like Quick Reference Cards (QRCs) and the Portal Help link 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.

6.6   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 RSA Token
- Reset Password
- Add/Remove Functional Roles for 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.

7   APPENDIX

7.1   Quick Reference Cards

Table 7.1-1 AMC QRCs

User Manual	QRC#	QRC Name	Description
Access Management Console	QRC-AMC:3.2	Navigating to the Access Management Console	QRC for Organization Administrators on how to navigate to the Access Management Console from MyGinnieMae.
Access Management Console	QRC-AMC:3.3	Exiting the Access Management Console	QRC for Organization Administrators on how to exit the Access Management Console and return to MyGinnieMae. The QRC also explains how to exit both the Access Management Console and MyGinnieMae.
Access Management Console	QRC-AMC:3.4.3	Change Password Via Access Management Console	QRC for Organization Administrators to change their password within the Access Management Console rather than navigating back to the MyGinnieMae landing page.

User Manual	QRC#	QRC Name	Description
Access Management Console	QRC-AMC:4.1.1	Send a Registration Invitation	QRC for Organization Administrators on how to send a Registration Invitation email to someone so they can register to become a MyGinnieMae end user.
Access Management Console	QRC-AMC:4.1.2	Approve a New User Registration	QRC for Organization Administrators on how to Approve a New User Registration.
Access Management Console	QRC-AMC:4.1.3	Reject a New User Registration	QRC for Organization Administrators on how to reject a New User Registration.
Access Management Console	QRC-AMC:4.1.4.1	Request a Functional Role From the Access Management Tile	QRC for Organization Administrators on how to submit a Functional Role request for someone through the Access Management tile in the Access Management Console.
Access Management Console	QRC-AMC:4.1.4.2	Request a Functional Role From the User Management Tile	QRC for Organization Administrators on how to submit a Functional Role request for someone through the User Management tile in the Access Management Console.
Access Management Console	QRC-AMC:4.1.5	Approve a Functional Role Request	QRC for Organization Administrators on how to approve a Functional Role request.
Access Management Console	QRC-AMC:4.1.6	Reject a Functional Role	QRC for Organization Administrators on how to reject a Functional Role request.
Access Management Console	QRC-AMC:4.2.1	Disable a User's Account	QRC for Organization Administrators on how to remove a user's MyGinnieMae account. This will remove all of the user's assigned functional roles.
Access Management Console	QRC-AMC:4.2.2	Enable a User's Account	QRC for Organization Administrators on how to enable a user's account so they can access MyGinnieMae.
Access Management Console	QRC-AMC:4.2.3	Lock a User's Account	QRC for Organization Administrators on how to prevent a user from logging in to their MyGinnieMae account, but still retain their functional roles.
Access Management Console	QRC-AMC:4.2.4	Unlock a User's Account	QRC for Organization Administrators on how to unlock a user's account so they can login to their MyGinnieMae account.
Access Management Console	QRC-AMC:4.2.5	Update a User's Profile	QRC for Organization Administrators on how to update a user's profile information such as title, work number, extension etc.

User Manual	QRC#	QRC Name	Description
Access Management Console	QRC-AMC:4.2.6	Update a User's RSA Token	QRC for Organization Administrators with the steps to follow when you receive a notification that a Functional Role requires an RSA association.
Access Management Console	QRC-AMC:4.2.7	Reset a User's Password	QRC for Organization Administrators on how to reset a password for a user when they have forgotten their password or cannot reset it themselves.
Access Management Console	QRC-AMC:4.2.8	Remove Functional Roles	QRC for Organization Administrators on how to remove a Functional Role when a user no longer requires the access.
Access Management Console	QRC-AMC:4.2.9	Review Functional Role Request Status	QRC for Org Admin to check the status of a Functional Role that has been requested for a user in your organization.
Access Management Console	QRC-AMC:4.2.10	Verify an Assigned Functional Role	QRC for Organization Administrators on how to verify that all the necessary underlying roles have been assigned to the user's account once the request has been finalized.
Access Management Console	QRC-AMC:4.2.11	Re-Request a Functional Role	QRC for Organization Administrators that need to re-request Functional Roles.
Access Management Console	QRC-AMC:4.2.12	De-Register a User with the Oracle Mobile Authenticator	QRC for Organization Administrators on how to de-register a user's smart device with the Oracle Mobile Authenticator so they can register a new smart device.
Access Management Console	QRC-AMC:4.3	AMC Troubleshooting-System Errors	QRC for Organization Administrators on how to resolve common system errors with the Access Management Console.
Access Management Console	QRC-AMC:4.4	Accessing Administrative Reports	QRC for Organization Administrators on how to access Administrative Reports in the Access Management Console.

7.2   Functional Role Matrix

Functional Roles are a system access profile based on business activities used to ensure End Users have the appropriate level of access to be able to perform their job functions and responsibilities. Functional roles are grouped and vary by type (refer to the Functional Role Matrix).

7.3   Figures

[Back to Table of Contents]

7.4   Tables

[Back to Table of Contents]