My GinnieMae Portal - Access Management Console (AMC)

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

Ginnie Mae, Office of Securities Operations

V 2.5

Application Details

Application Information	Description
Application Name	Access Management Console
Application Acronym	AMC
Application Developer	MBSOA/PPA
Application Approver	Ginnie Mae
Submission Date	10/2/2018
Ginnie Mae SVP, Owner	John Daugherty, SVP OSO
Ginnie Mae Director, Approver	Stewart Spettel, Director of Operations
Approval Date	10/17/2018
Version/Release Number	4

Document History

Version	Date of the Document	Author	Entity (Company or Department Author Represents)	Revision Description
1.0	6/13/2017		BNYM	Original issue
1.1	7/18/2017		BNYM	Updated with feedback from BNYM reviewers
1.2	4/25/2018		BNYM	Updated with new screens and functions
1.3	5/21/2018		BNYM	Updated with high level feedback
1.4	6/26/2018		BNYM	Reconciliation of further Ginnie Mae feedback
1.5	8/1/2018		BNYM	Updated with new screens and functions
1.6	9/25/1028		BNYM	Updated per CAG feedback
1.7	10/2/2018		BNYM	Updated as per the last round of CAG feedback and finalized for approval

1.8	10/17/2018		BNYM	Incorporated final feedback from CAG and Ginnie Mae
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

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

In MyGinnieMae, 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.

The purpose of this document is to familiarize Organization Administrators with MyGinnieMae functionality relevant to their role. Organization Administrators would have previously performed the Security Officer role in GMEP 1.0 or the Enrollment Administrator role in Ginnie*NET*. Since an Organization Administrator is also a user of MyGinnieMae, refer to the MyGinnieMae End User Guide for functionality common to all users of the portal.

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

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

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

Among the benefits provided to Ginnie Mae stakeholders are:

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

1.1 Application Overview

1.1.1 Access Management Console

The MyGinnieMae Access Management Console (AMC) is used to register new MyGinnieMae users, to grant access to modernized business applications (for example, the Multifamily Pool Delivery Module (MFPDM)) as well as legacy business applications (that is, GMEP 1.0 and Ginnie*NET*), and to manage existing Portal user accounts. Current

Security Officers and Enrollment Administrators will become privileged users known as Organization Administrators and utilize AMC to manage the users within their organization.

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.

1.2 Security Protocols

Refer to Section: Security Protocols in the MyGinnieMae Portal Getting Started Manual.

1.3 Authorized Use/Permission

Refer to Section: Authorized Use/Permission in the MyGinnieMae Portal Getting Started Manual

2 SYSTEM PREREQUISITES

Before being granted access to the MyGinnieMae Portal, the user must complete the registration process. Privileged users called Organization Administrators, formerly known as Security Officers and Enrollment Administrators, facilitate the registration and access provisioning process within each organization.

Refer to Section: System Prerequisites in the MyGinnieMae Portal Getting Started Manual.

3 GETTING STARTED

The following sections detail common actions taken by Organization Administrators to access MyGinnieMae Access Management Console (AMC).

3.1 Logging on to MyGinnieMae

Refer to the Section: Logging into MyGinnieMae in the MyGinnieMae Portal Getting Started Manual.

3.2 Navigating to the Access Management Console

The Access Management Console (AMC) is the user interface used by Organization Administrators to manage user accounts and retrieve system audit reports for their organization.

1. From the Global Header of any page,
    a. Select **Tools**
    b. Select **Access Management Console**

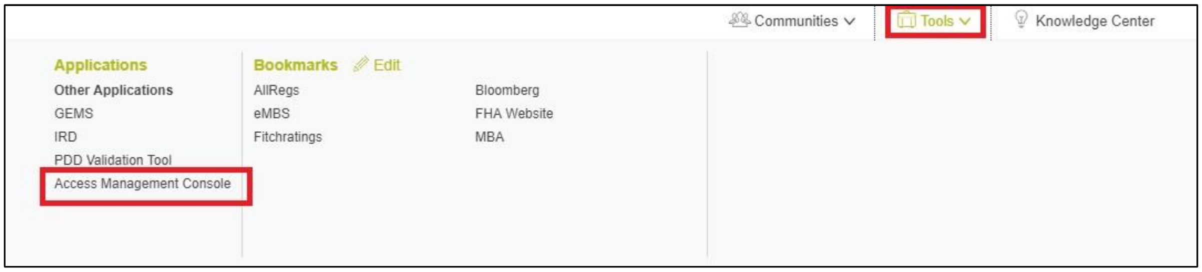


Figure 1 – Tools Drop-Down Menu

2. Select **Yes** when prompted to open the AMC within this existing MyGinnieMae Portal window.

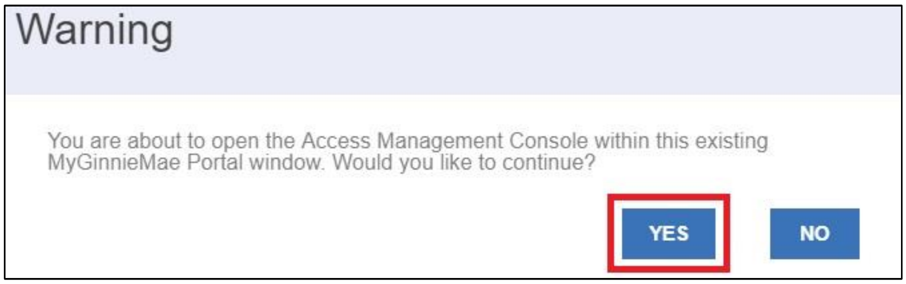


Figure 2 – Portal Warning

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

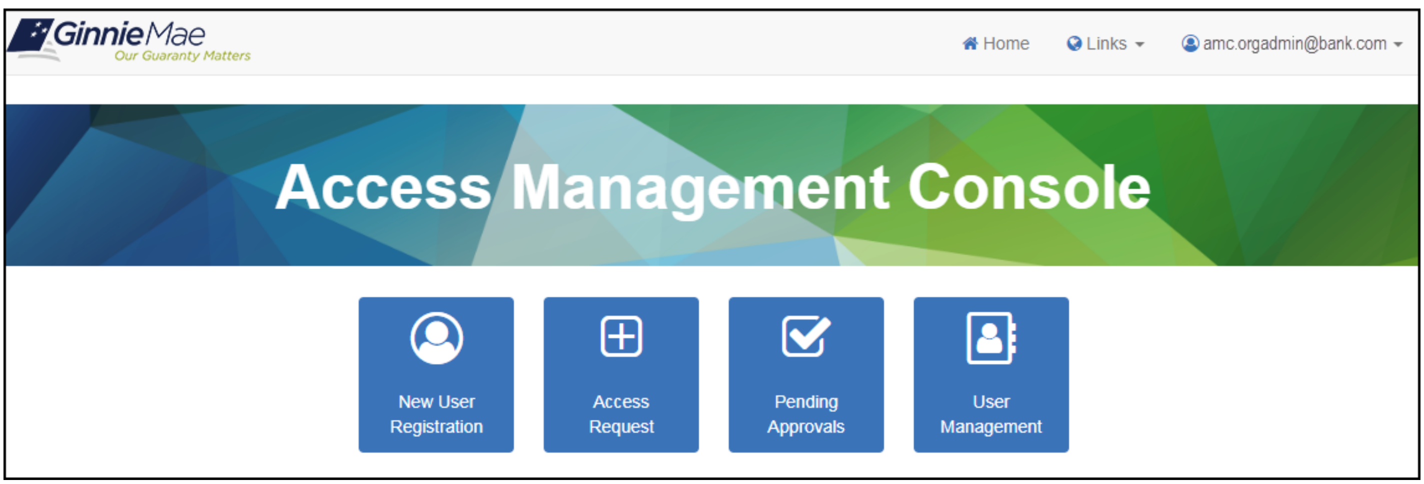


Figure 3 – AMC Landing Page – Organization Administrator

3.3 Exiting

When exiting the Access Management Console (AMC) Organization Administrators 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.

3.3.1 Exiting the Access Management Console and Returning to MyGinnieMae

1. To exit the Access Management Console and navigate back to My Dashboard in the portal.

   a. Select down arrow beside **Links** on the toolbar at the top of the page.

b. Select **MyGinnieMae Portal**

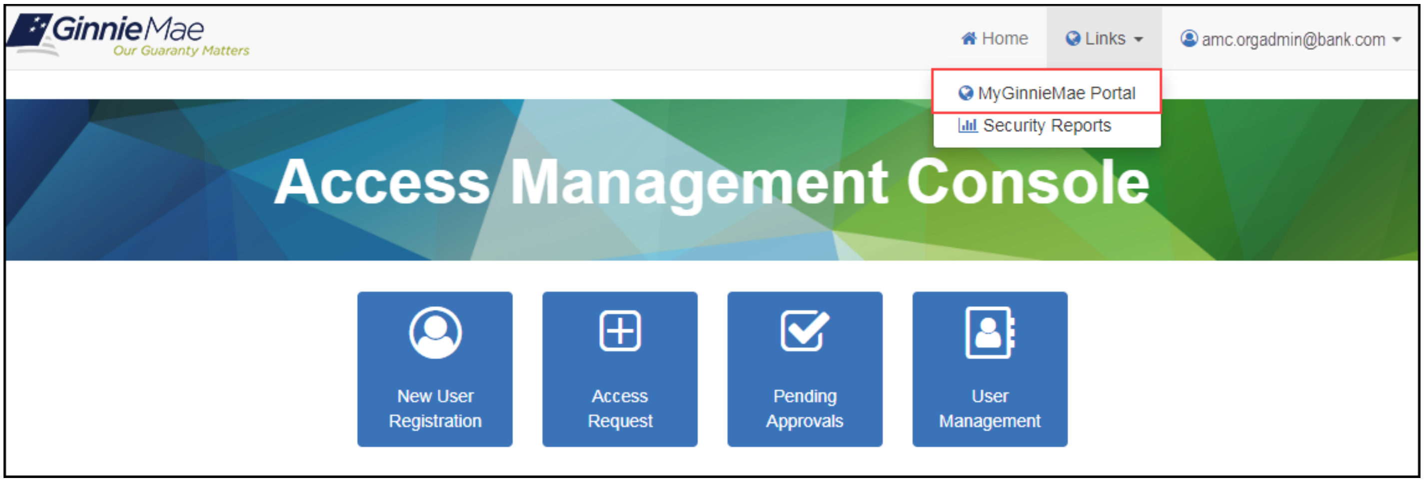


Figure 4 - Return to MyGinnieMae Portal

3.3.2 Exiting the Access Management Console and MyGinnieMae

Organization Administrators may simultaneously exit the AMC and MyGinnieMae portal by following the instructions the following instructions:

NOTE: If the user has any legacy system sessions open in other windows those sessions must be exited separately to securely end all portal activity.

1. To exit the Access Management Console, simultaneously closing the Portal session,

   a. Select the down arrow ▾ beside the username on the toolbar at the top of the page
   b. Select **Sign out**

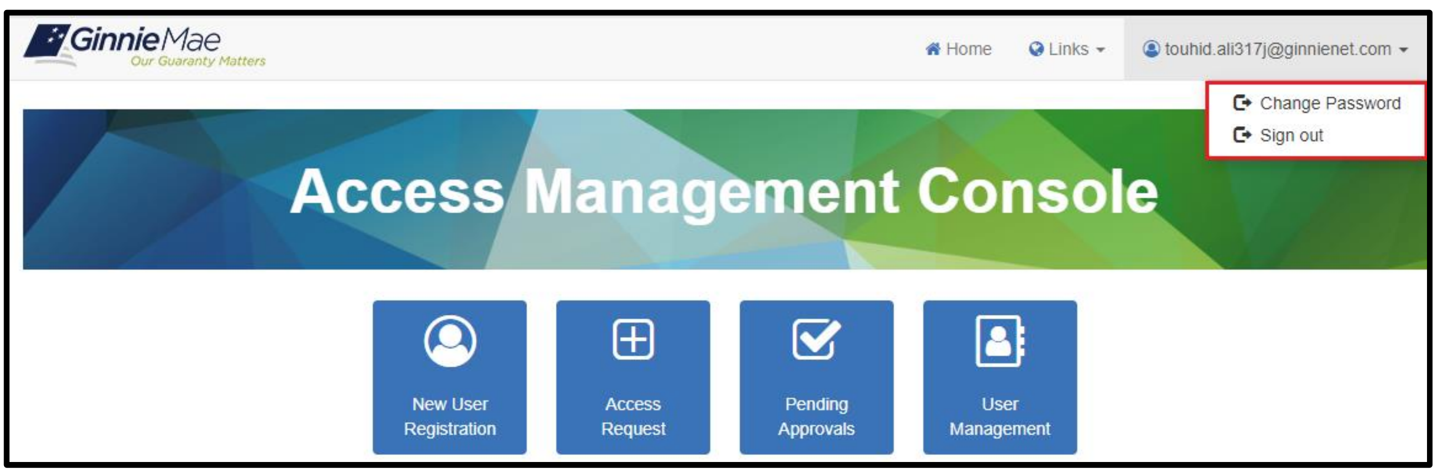


Figure 5 - Exit Access Management Console

NOTE: Upon signing out of the AMC, the user's portal session is terminated. To return, the user will need to follow the login steps in Section: Logging into MyGinnieMae.

4 USING THE APPLICATION

The following sections detail common actions taken by Organization Administrators 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.

4.1 Outlook Rules for Email Notifications

During the onboarding of End Users Organization Administrators will receive several email notifications for each user. The steps below provide guidance on how to setup the Outlook rule for segregation of notifications generated to the Org Admin Group versus messages regarding your 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.

4.1.1 Outlook Rule for Organization Administrator Group Notifications

Each Organization Administrator will receive several notifications relating to registration and access workflow items for each End User in their organization. If the Org Admin would like to automatically move those notifications from the Inbox to a designated folder, the following criteria will assist. For detailed instructions on creating a Rule in Microsoft Outlook visit Microsoft Office Support at https://support.microsoft.com/en-us 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 outlook rule description can be seen in the figure below:

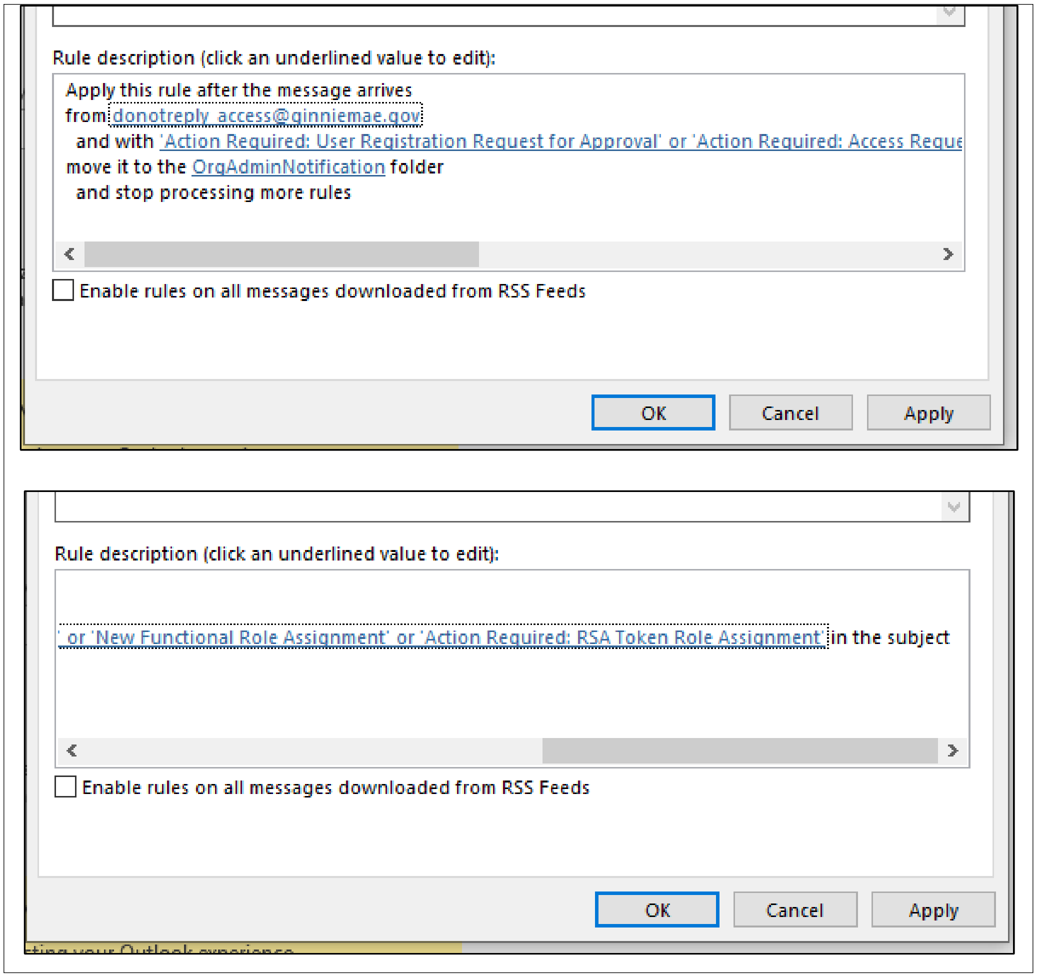


Figure 6 - Outlook Rule for Organization Administrator Group Notifications

4.1.2 Outlook Rule for Individual Account Notifications

Organization Administrators will receive key notifications to their Inbox relating to their own individual portal account. If the Org Admin would like to automatically move those notifications from the Inbox to a designated folder, the following criteria will assist. For detailed instructions on creating a Rule in Microsoft Outlook visit Microsoft Office Support at https://support.microsoft.com/en-us and search “Manage email messages by using rules”.

Criteria:

From: donotreply_access@ginniemae.gov
Subject contains
"MyGinnieMae Password Change Confirmation"
"Final Password Expiration Notice"
"Password Expiration Warning"
"Ginnie Mae OTP Code"
"Welcome to MyGinnieMae Registration"
"Welcome to the MyGinnieMae Portal"
Target folder: Any user defined outlook folder. In the screenshot provided below, “MyNotification" is the user defined folder.

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

- One-Time PIN (OTP) generation
- Password about to expire
- Password expired
- Password changed confirmation
- MGM Portal registration invitation
- MGM Portal successful registration

The Outlook Rule Description can be seen in the figure below:

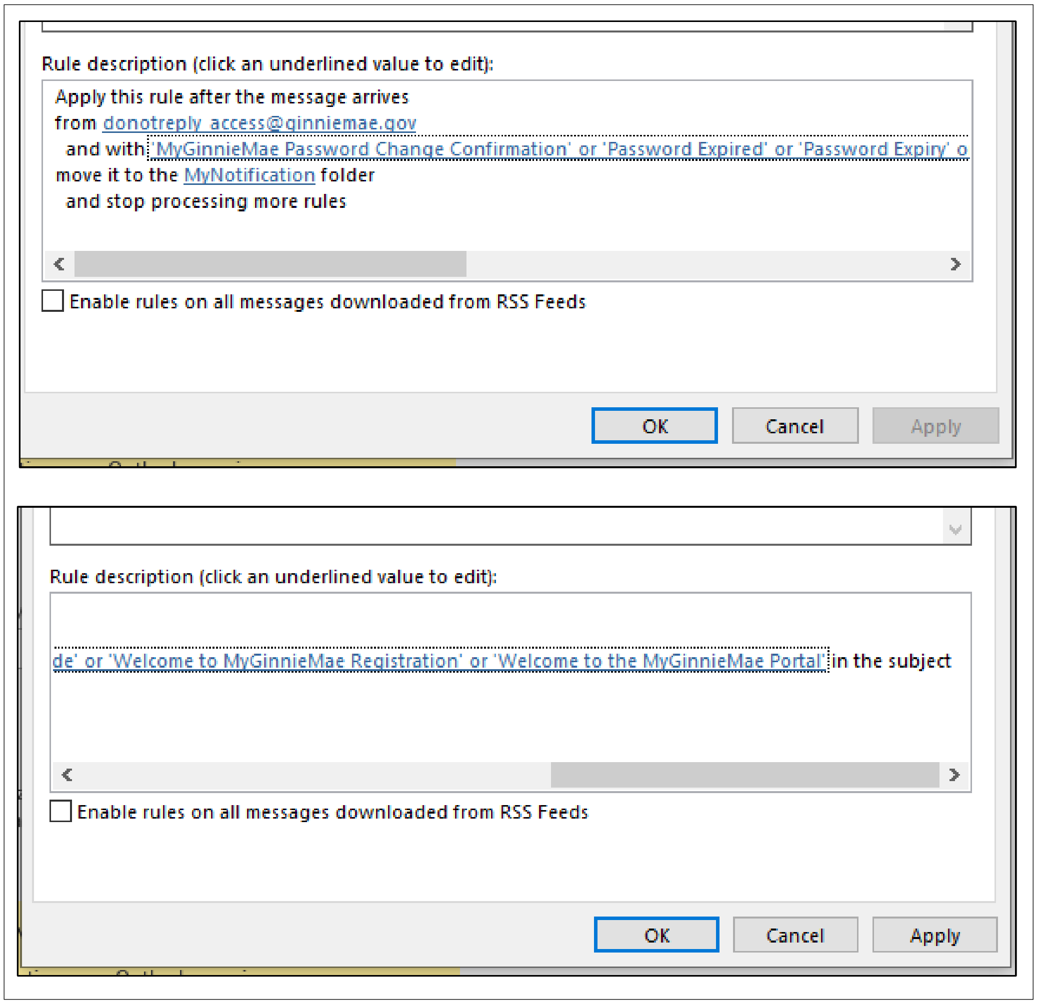


Figure 7 - Outlook Rule for Individual Account Notifications

4.1.3 Change Password via the AMC

If an administrator using the Access Management Console (AMC) would like to change their login password, the Org Admin can do this from the AMC Landing Page, rather than navigating back to the Portal. To change the login password from the AMC Landing Page, the Org Admin should follow these steps:

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

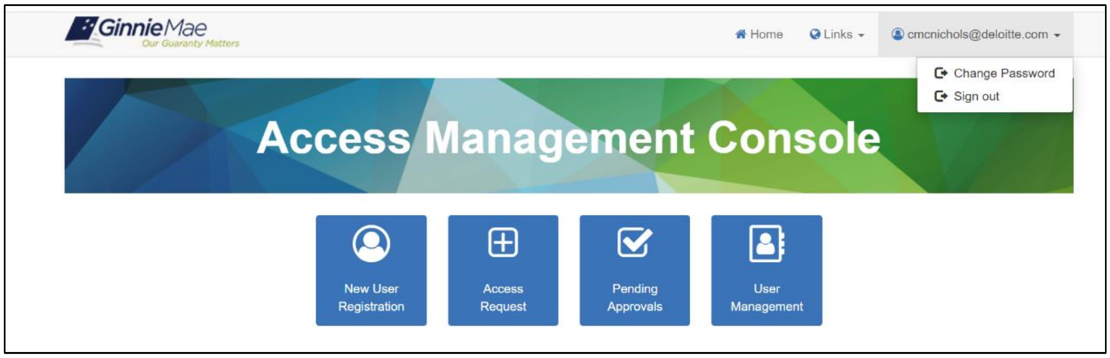


Figure 6 – AMC Dropdown Menu

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 7 – AMC Change Password Screen (Filled-In)

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

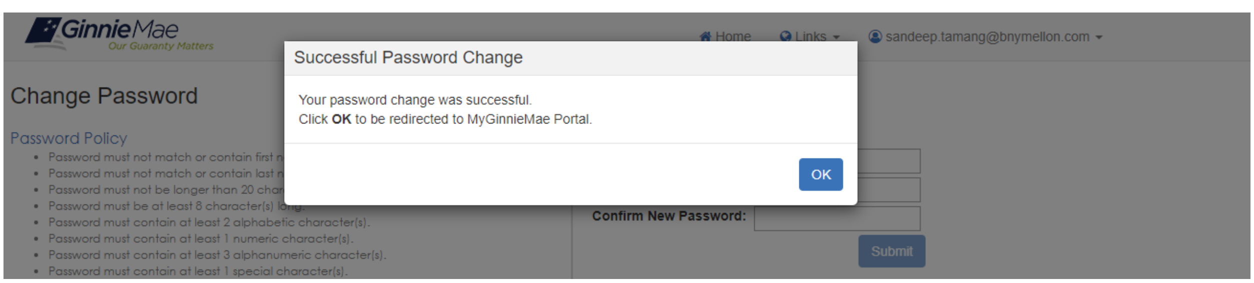


Figure 8 – Password Change Successful Message

NOTE: If the user enters the incorrect current password, they will receive an "At least one of the provided passwords failed validation" error message

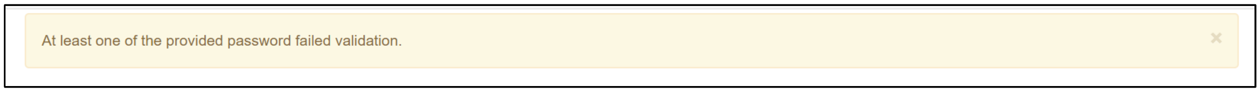


Figure 9 – Password Failed Validation Error Message

4.2 Onboarding End Users - Registration & Access Workflow

Organization Administrators are responsible for providing access to Ginnie Mae business systems via MyGinnieMae for End Users within their organization. This is done through an automated Onboarding Workflow in the Access Management Console (AMC). This section contains instructions for Org Admins 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 request workflows do not allow the Organization Administrator to initiate a registration and approve that same registration or request access via Functional Role assignment and approve that same access request. A minimum of two Organization Administrators is therefore required. From an operational perspective, it is recommended that an organization have more than the minimum of two Organization Administrators.

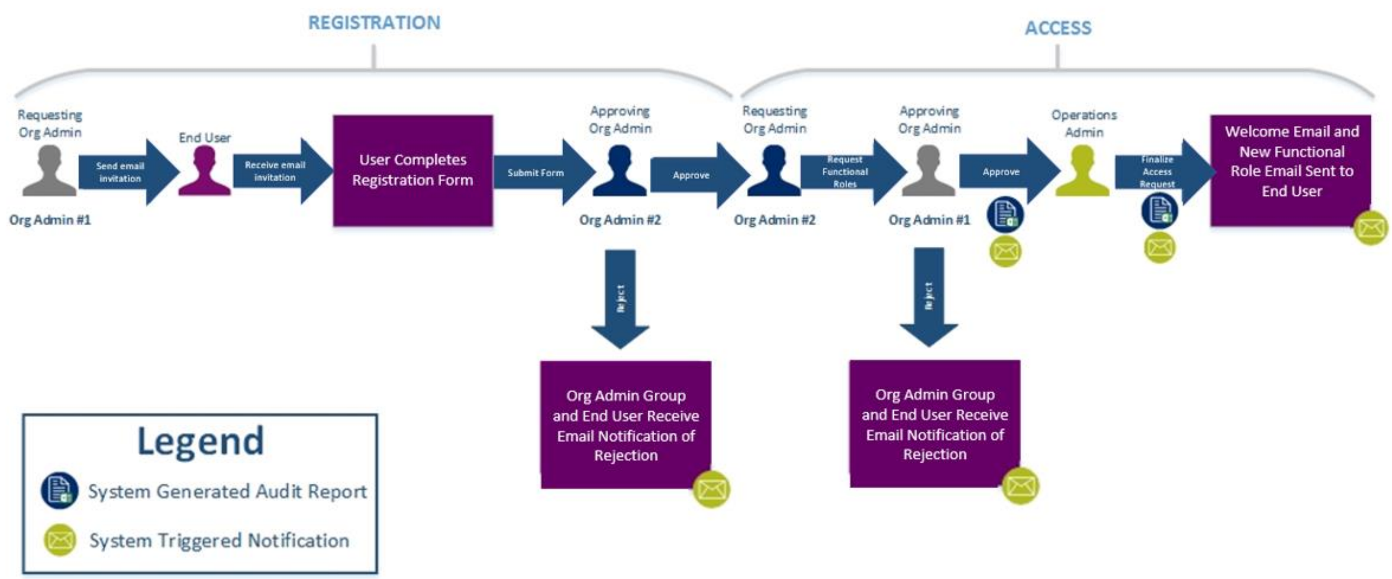


Figure 10 - MyGinnieMae Onboarding Workflow

4.2.1 New User Registration

To create a new user account in MyGinnieMae, an Organization Administrator initiates the workflow via an email invitation sent to the End User within their organization as follows:

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

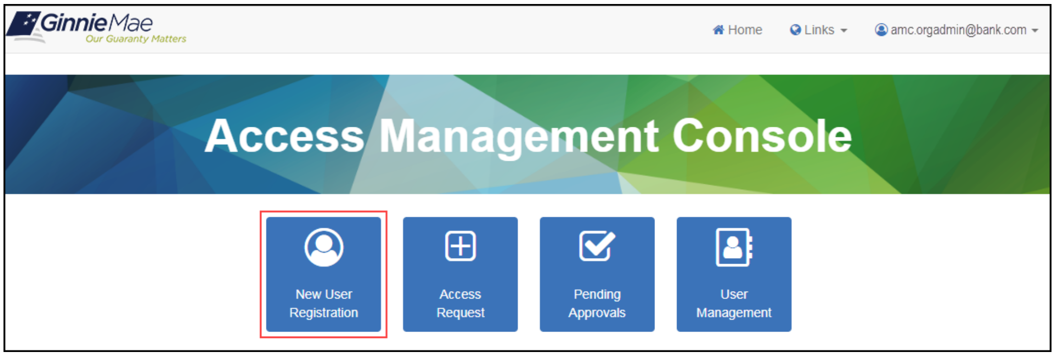


Figure 11 - Access Management Console Landing Page

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.

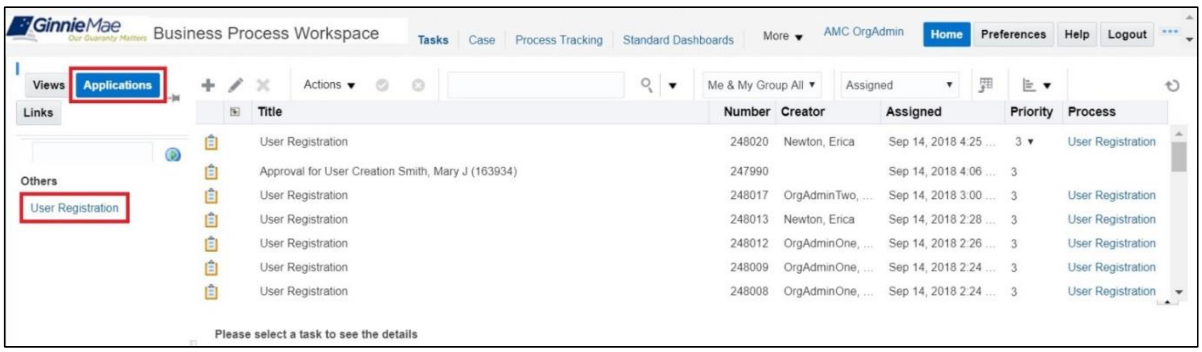


Figure 12 – New User Registration Interface

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

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've 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 the Ginnie Mae Customer Support Hotline.

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 Section: Request for Functional Role.

6. Select **Submit**.

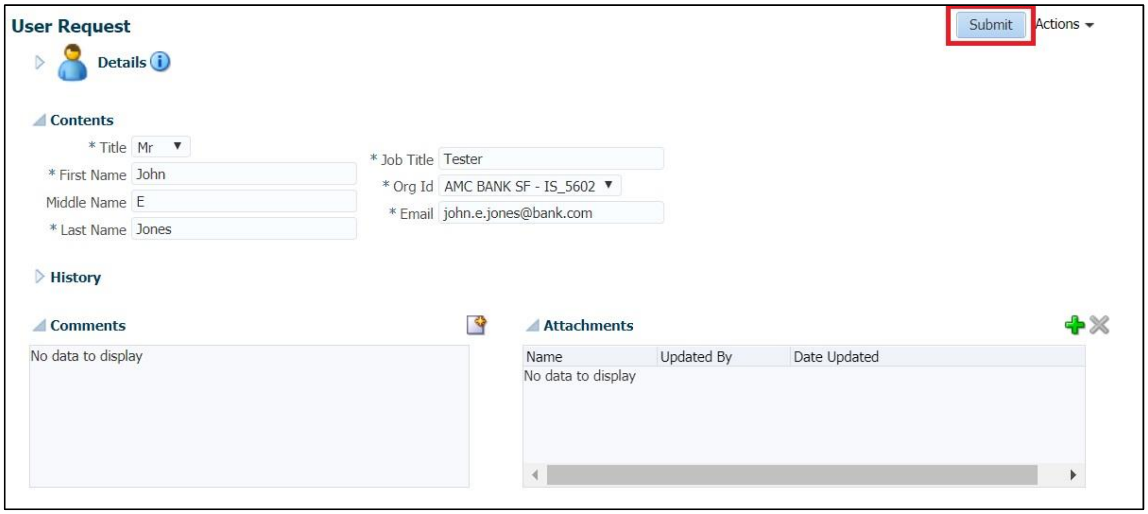


Figure 13- User Request Invitation Form

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.

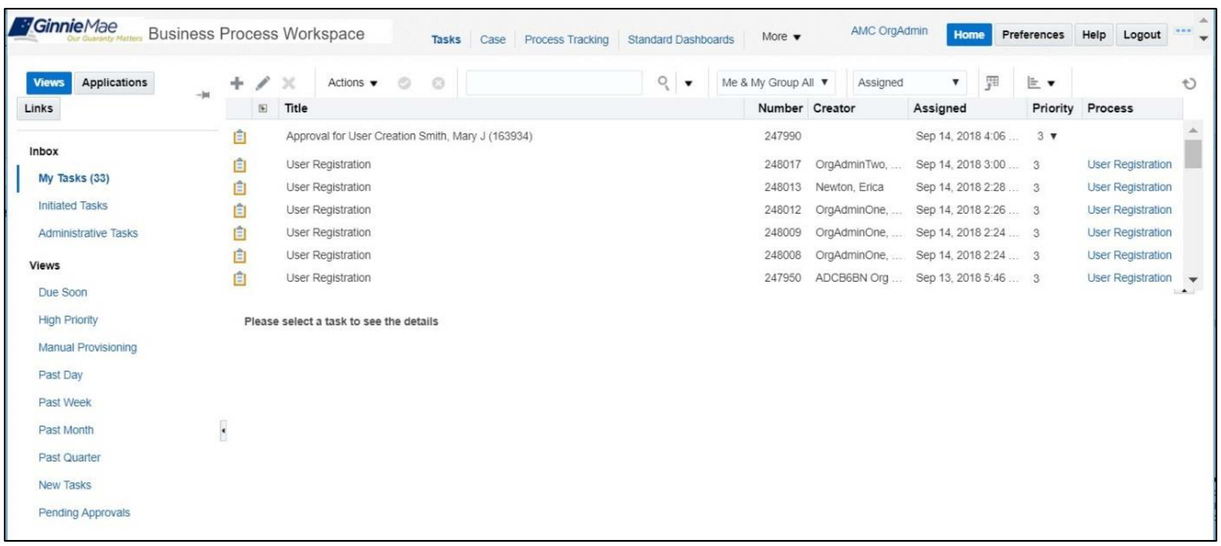


Figure 14– New User Registration Interface

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

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

4.2.2 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 15- 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 **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.

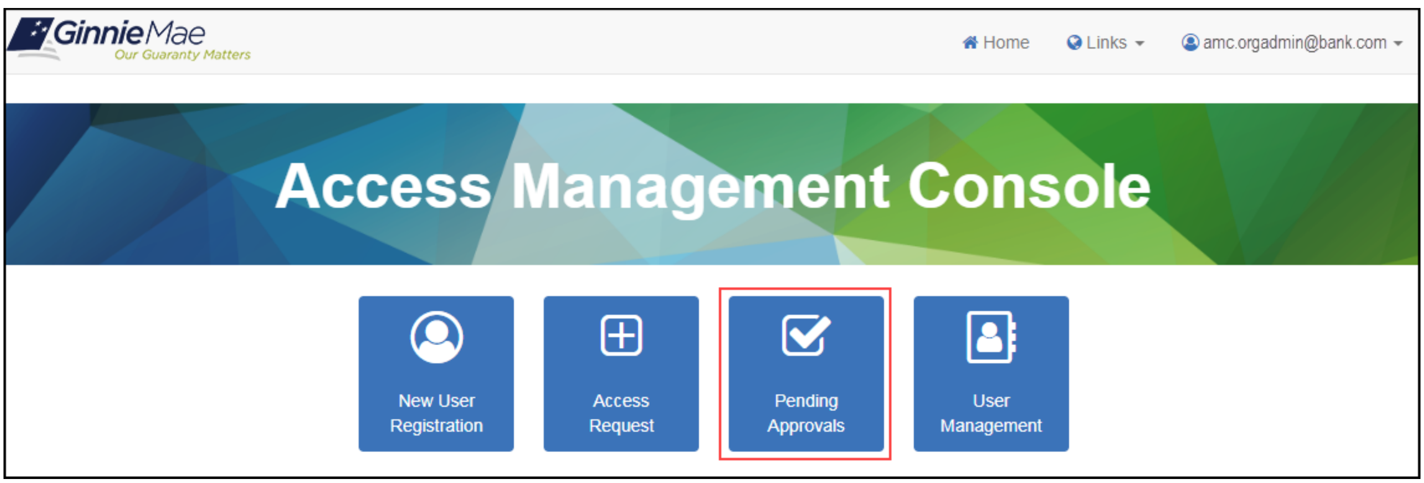


Figure 16- Access Management Console Landing Page

4. Review the table under the “User Registration Approval” accordion which displays the list of available registration requests awaiting approval.

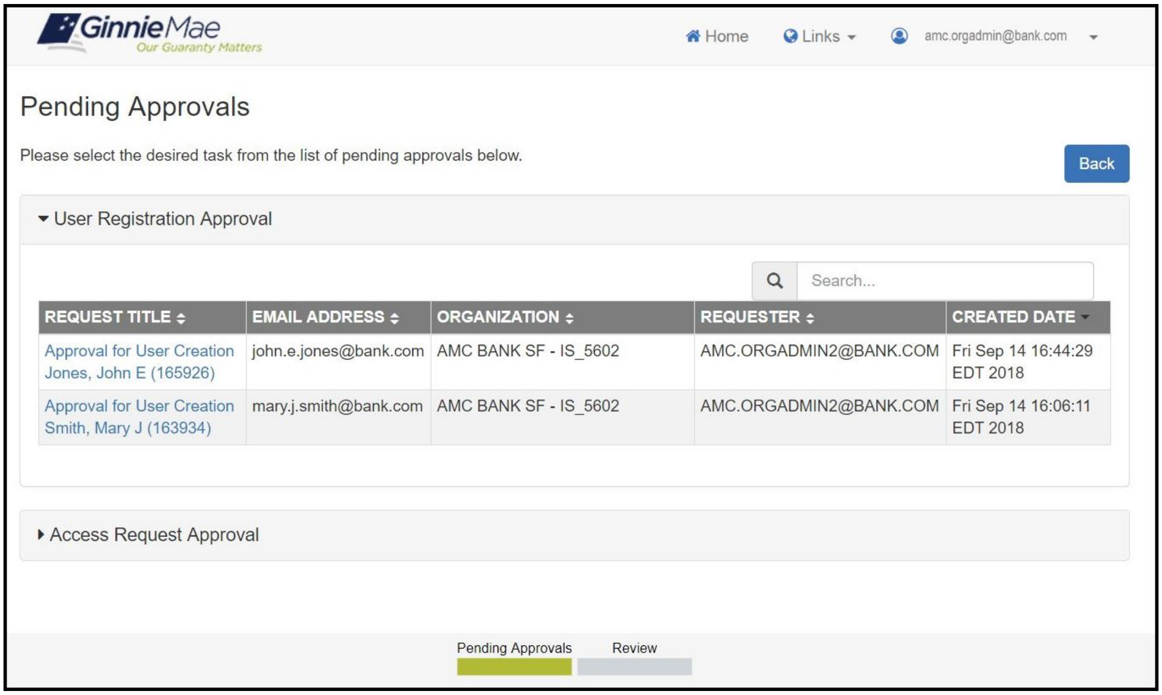


Figure 17– Pending Approvals – User Registration Approval

5. Select **Request Title** hyperlink for the desired End User to begin the approval of the registration request.

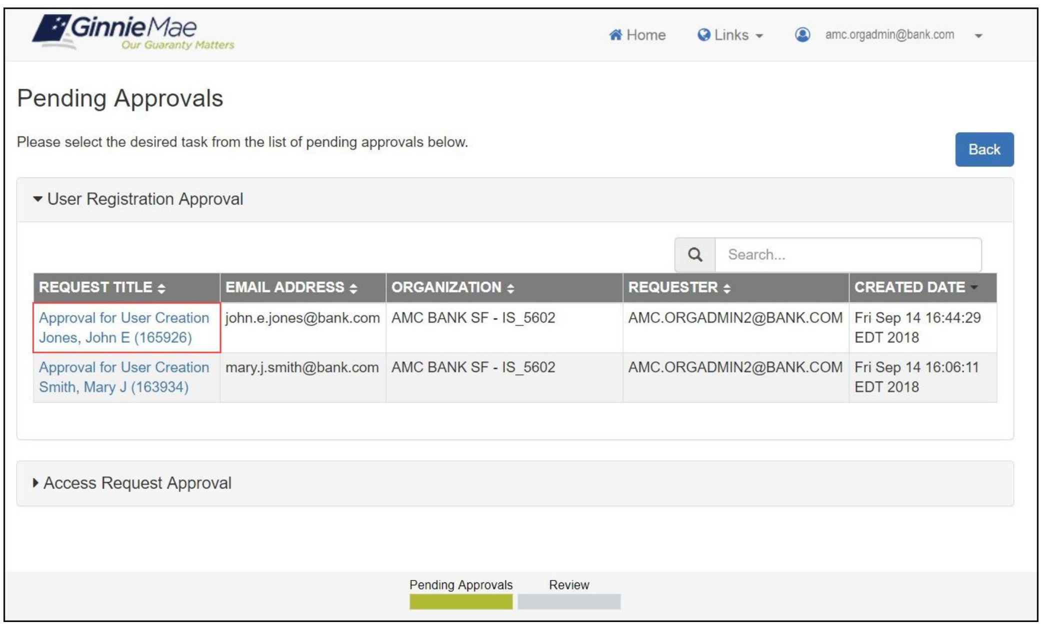


Figure 18- Request Title Hyperlink

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 Section: New User Registration.

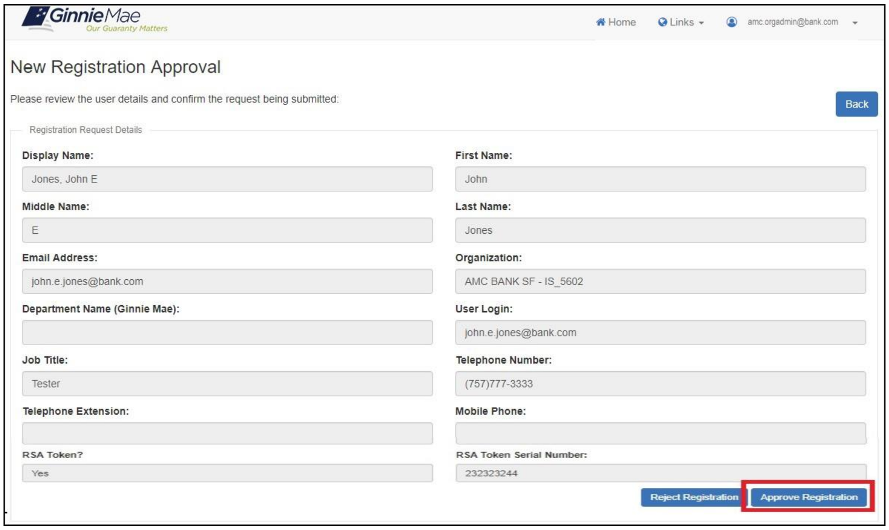


Figure 19- User Approval Details

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

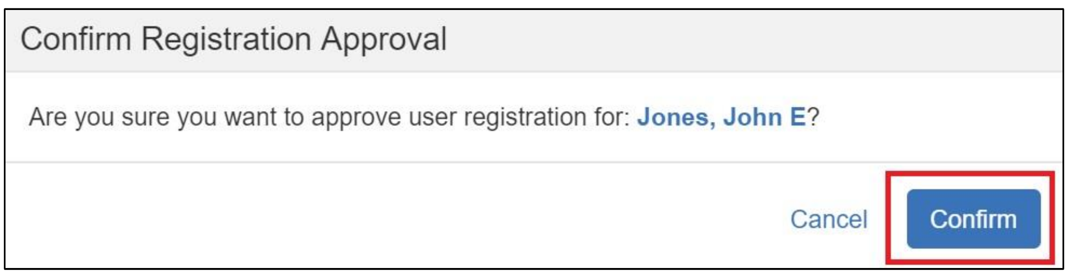


Figure 20 - Confirm Registration Approval Dialog Box

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.

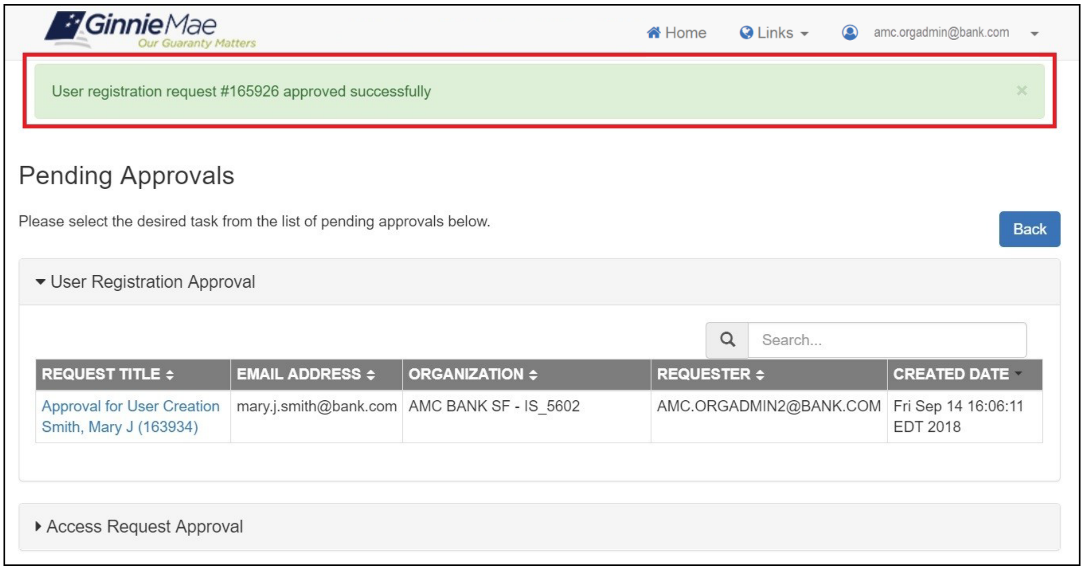


Figure 21- User Registration Approval Notification Ribbon

8. It is strongly recommended that the approving Organization Administrator immediately proceed to the access request as detailed in Section: Request Functional Role.

4.2.3 Reject a New User Registration

In the event that there is a problem or error with a registration request, an Organization Administrator 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 **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 **Request Title** hyperlink for the desired End User.
6. Select **Reject Registration.**

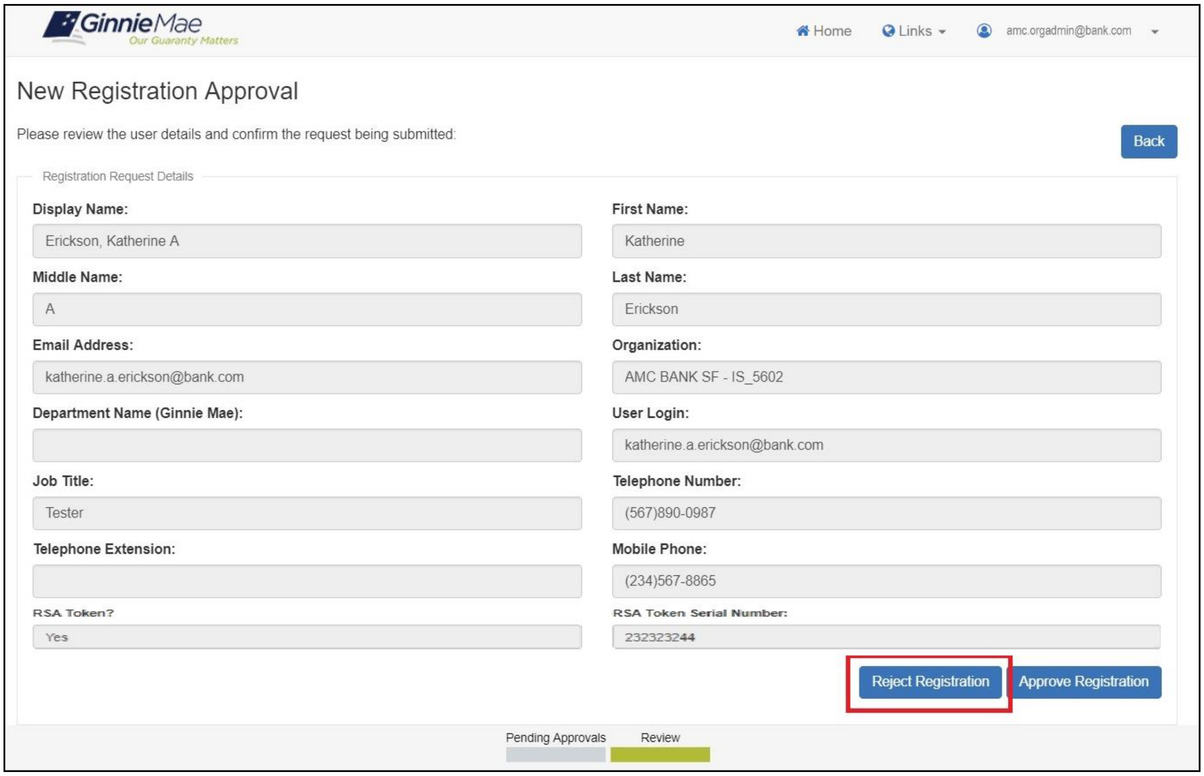


Figure 22 - User Rejection Details

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)

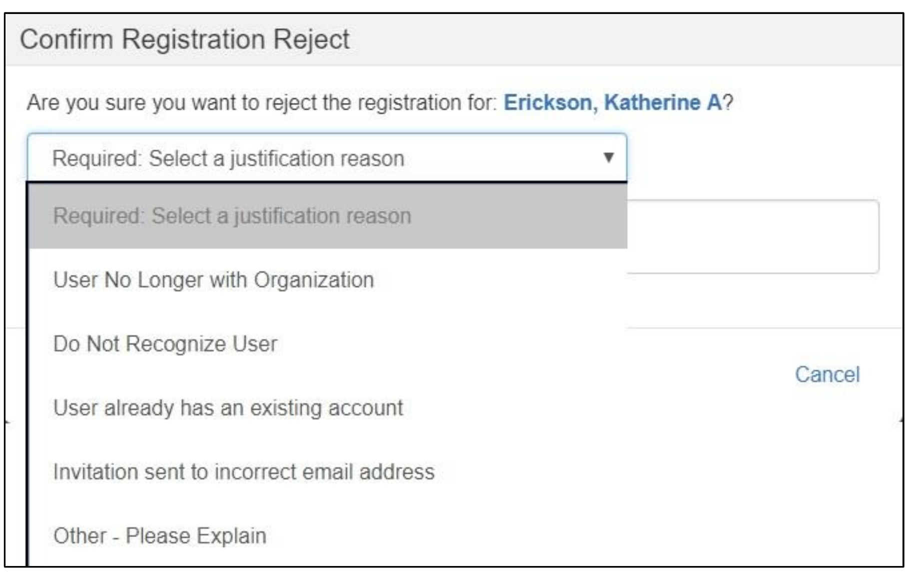


Figure 23 – Rejection Justification Reason Drop Down

8. Choose the Justification Reason

  a. If required, enter a Justification Description.

  b. Select **Confirm** to send the rejection to the system.

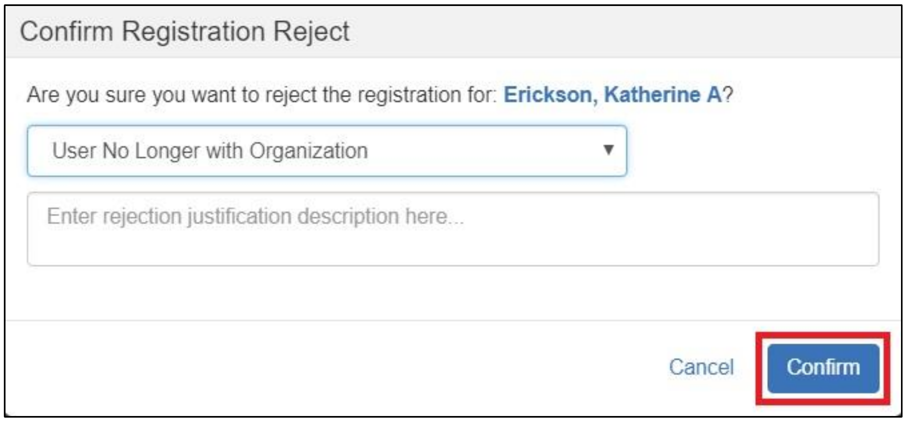


Figure 24 - New User Registration Rejection

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

Figure 25 - User Registration Rejection Notification

4.2.4 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 an Organization Administrator requires 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.

(1) Request Function Role from Access Management Tile

To request access 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.

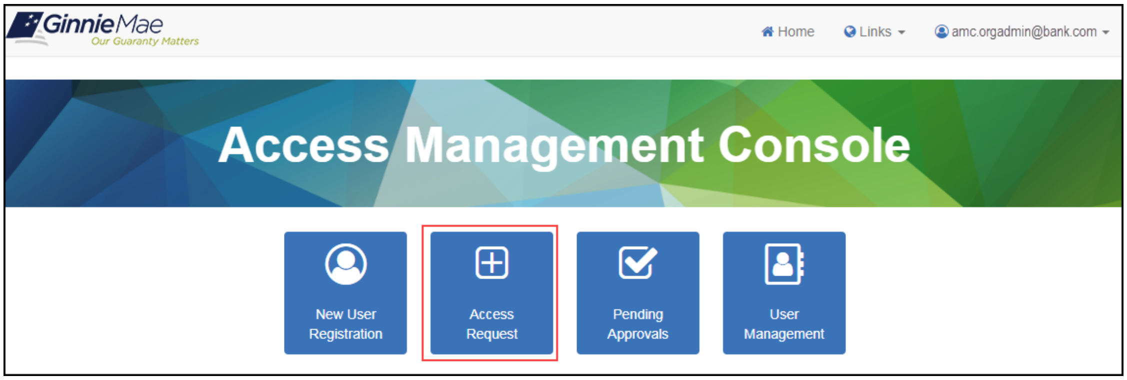


Figure 26 - Access Management Console Landing Page

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.

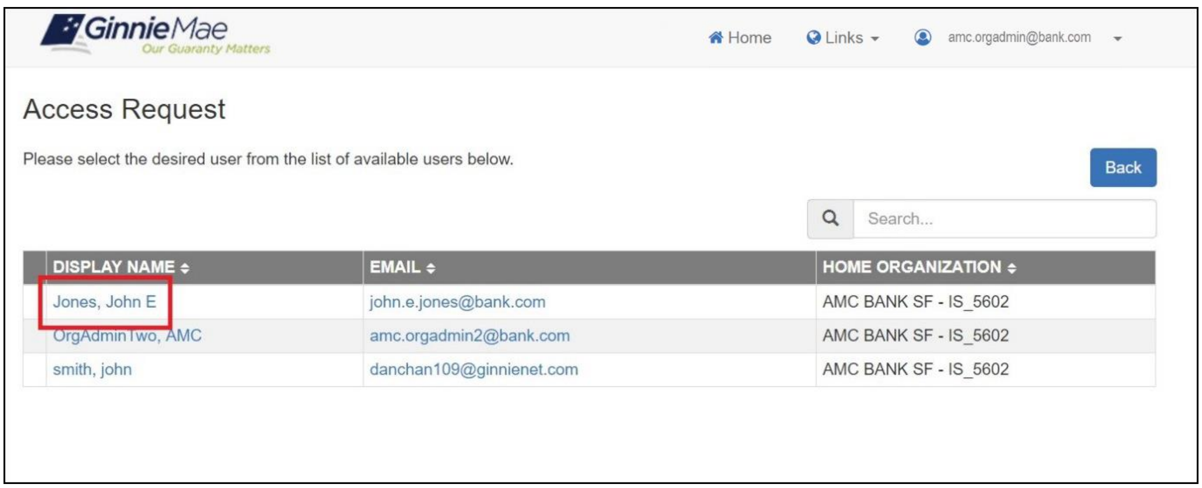


Figure 27 - Request Access for Others Search

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 the Organization Administrator only has one Org Key, the Organization Administrator will be sent directly to the list of Functional Roles (Step 6). If the Organization Administrator has 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**.

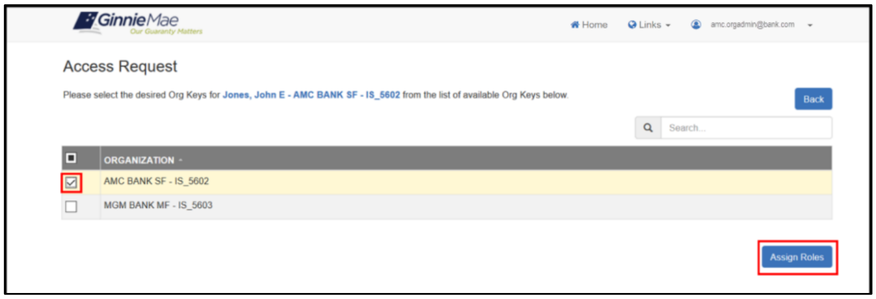


Figure 28 - Select Organization Key(s)

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 confirm the 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.

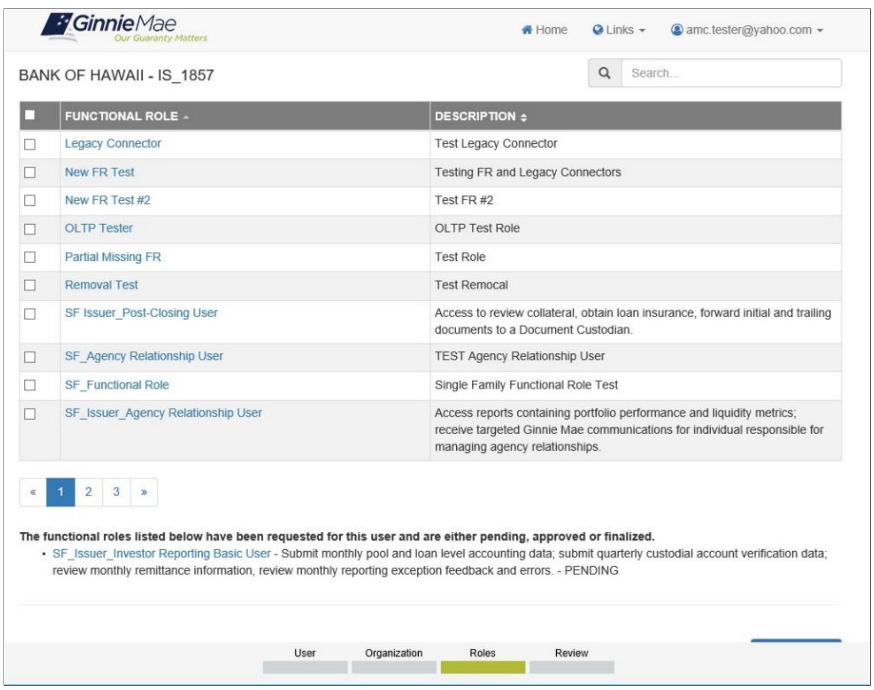


Figure 29 - Request Functional Roles Selection Page

NOTE: Selecting on 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.

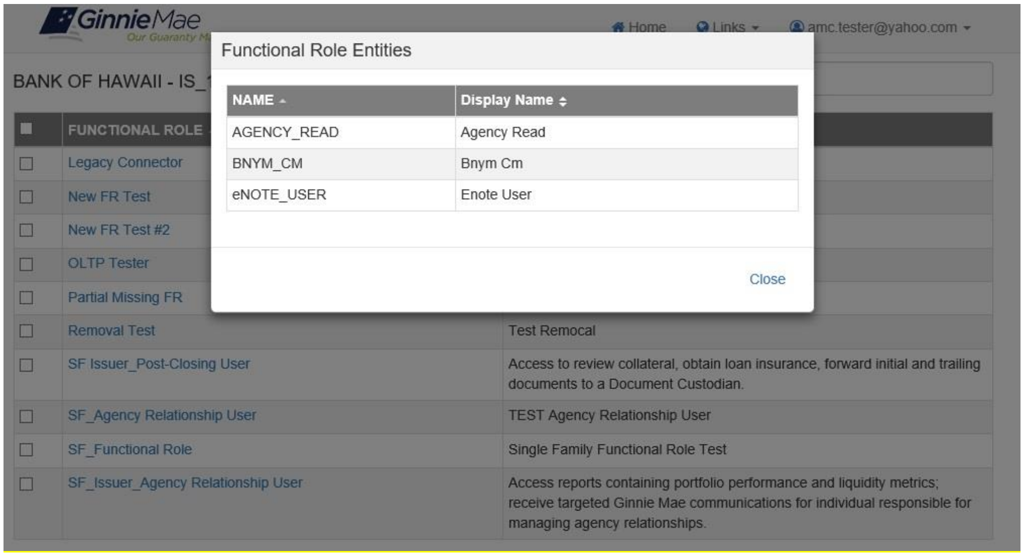


Figure 30 - Functional Role Entities Overlay

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.

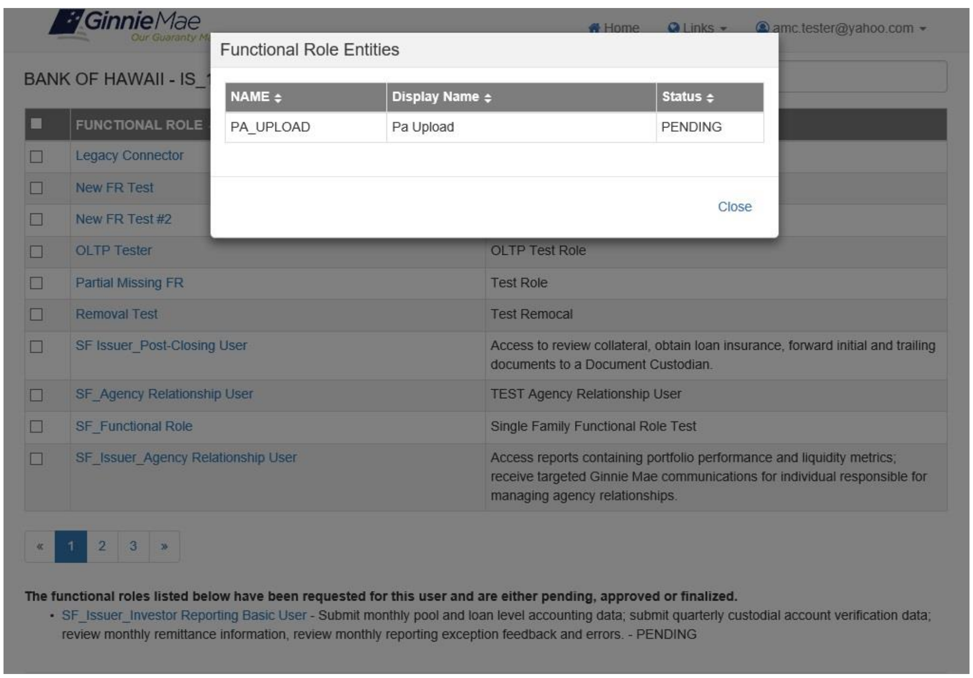


Figure 31 – Functional Role Entities Overlay With Status

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**.

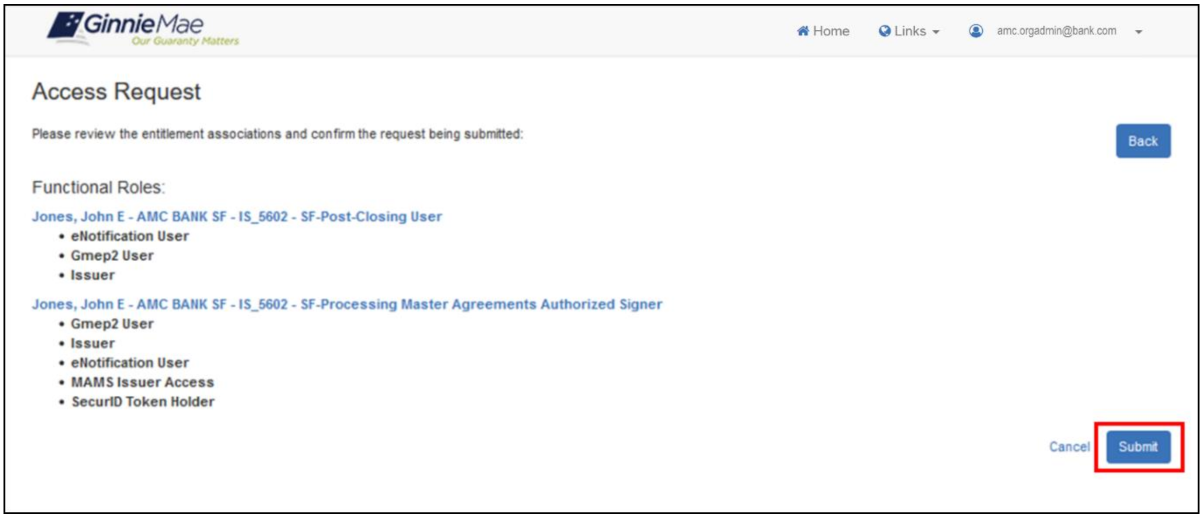


Figure 32 - Request Functional Role Review

8. The system displays an access request confirmation dialog box.
    a. Select **Confirm** to submit the roles for approval.

Figure 33 – 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 Section: Approve Access Request and Functional Roles).

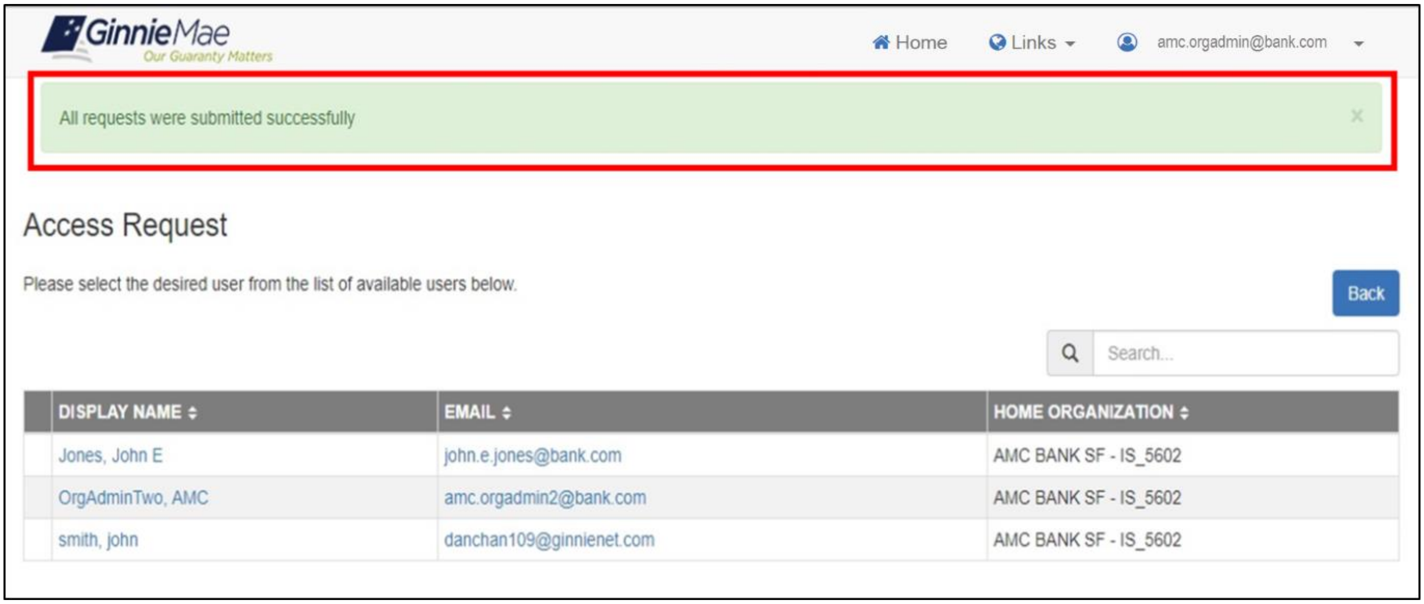


Figure 34 - Role Access Request

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

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

(2) 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 **User Management** tile.

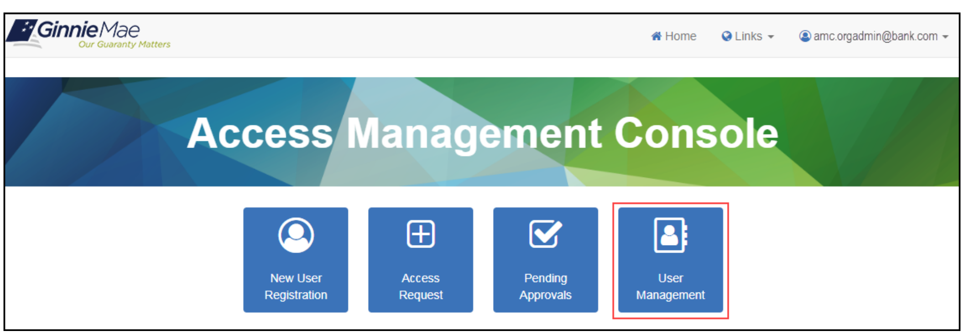


Figure 35 - Access Management Console Landing Page

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

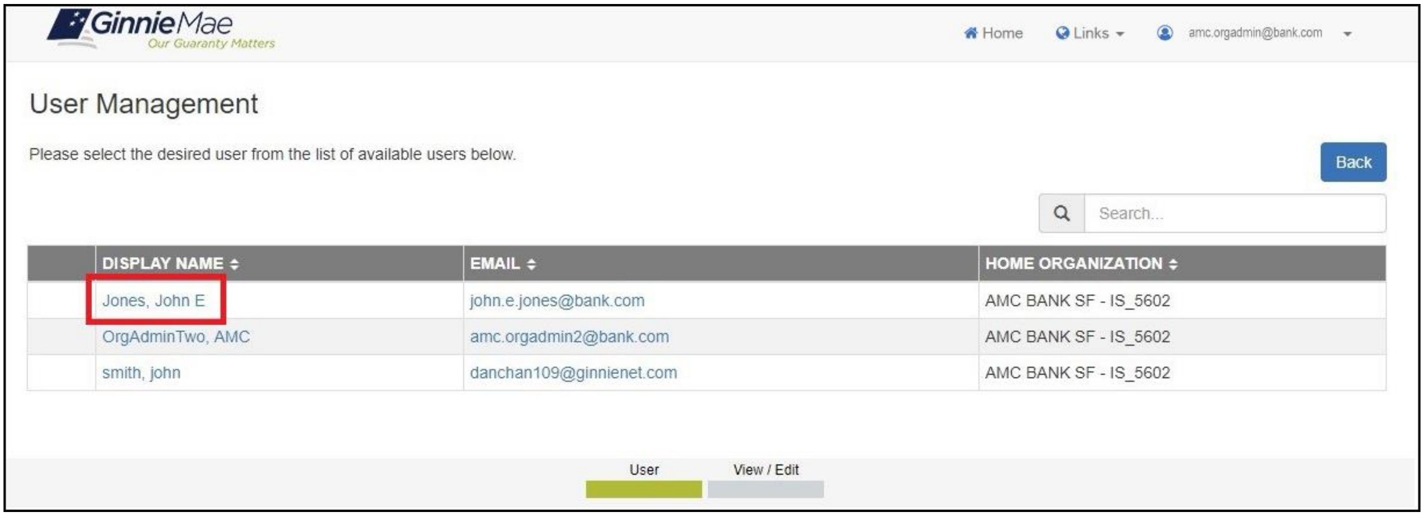


Figure 36 - Select User

5. Once the "User Profile" screen opens,

a. Select 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, the Organization Administrator 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.

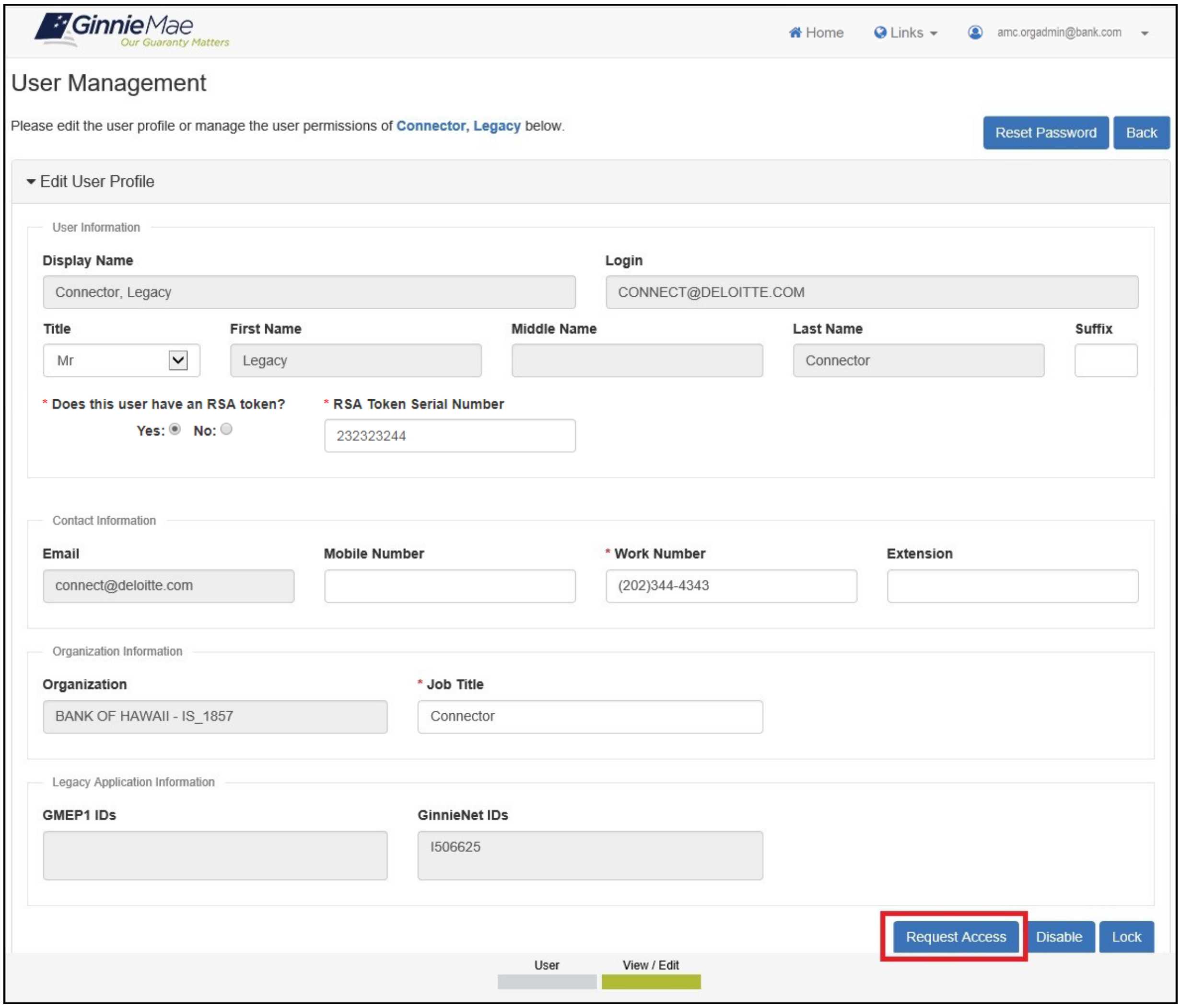


Figure 37 - Request Access Button

6. The system directs the user to the Organization screen of the Access Request workflow where the Org Admin can follow steps 5 - 9 of Section: 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 Section: Update a User's Profile Attributes.

4.2.5 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.

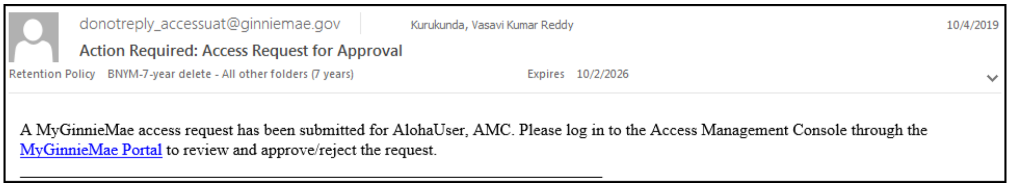


Figure 38 - Access Request Approval Notification

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

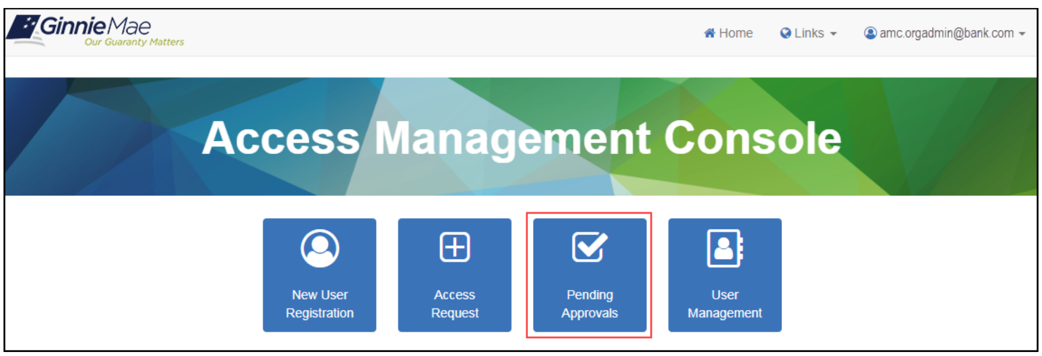


Figure 39 - AMC Homepage—Pending Approvals Tile

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

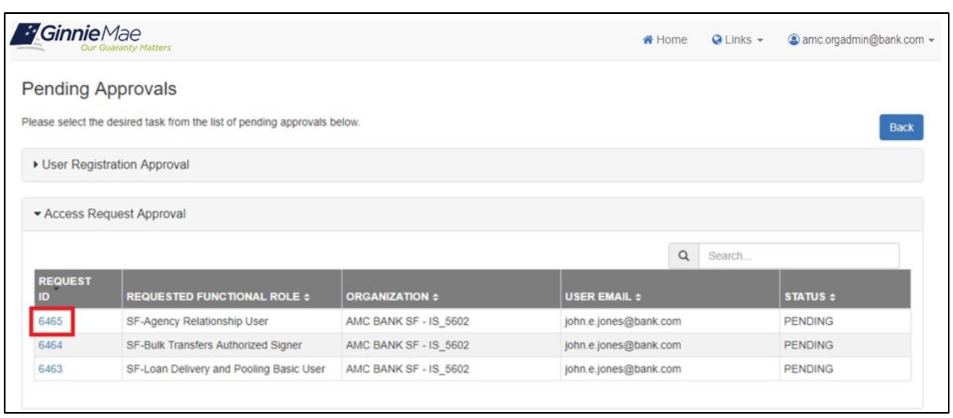


Figure 40 - List of Pending Access Requests

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.

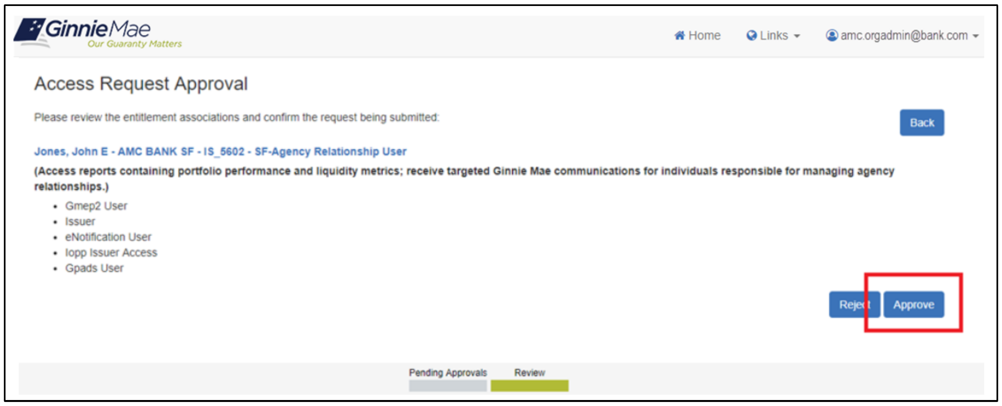


Figure 41 - Review Page for Functional Role Approval

6. Select Confirm to submit the approval.

Figure 42 – 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.

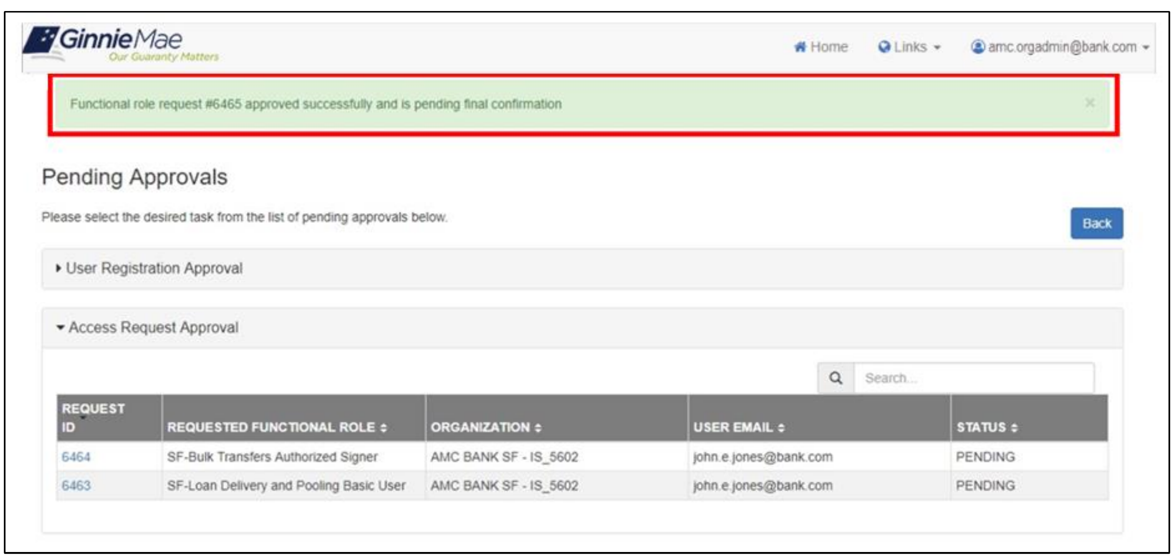


Figure 43 – Request Approval Successful

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 Hotline. 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.

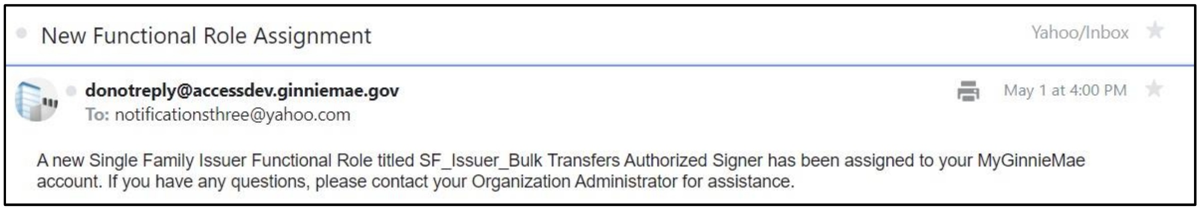


Figure 44 - End User Notification

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.

4.2.6 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**.

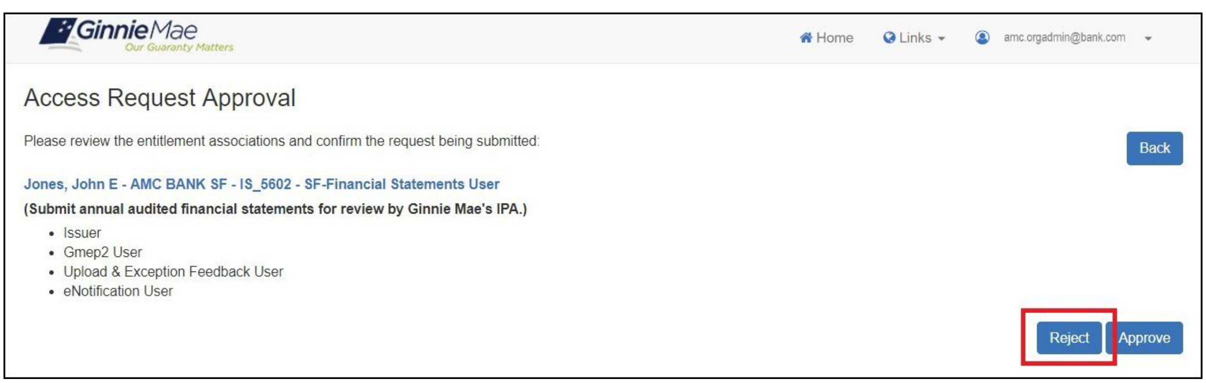


Figure 45 - Review Page for Functional Role Rejection

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 Reason
    - If required, enter a Justification Description.

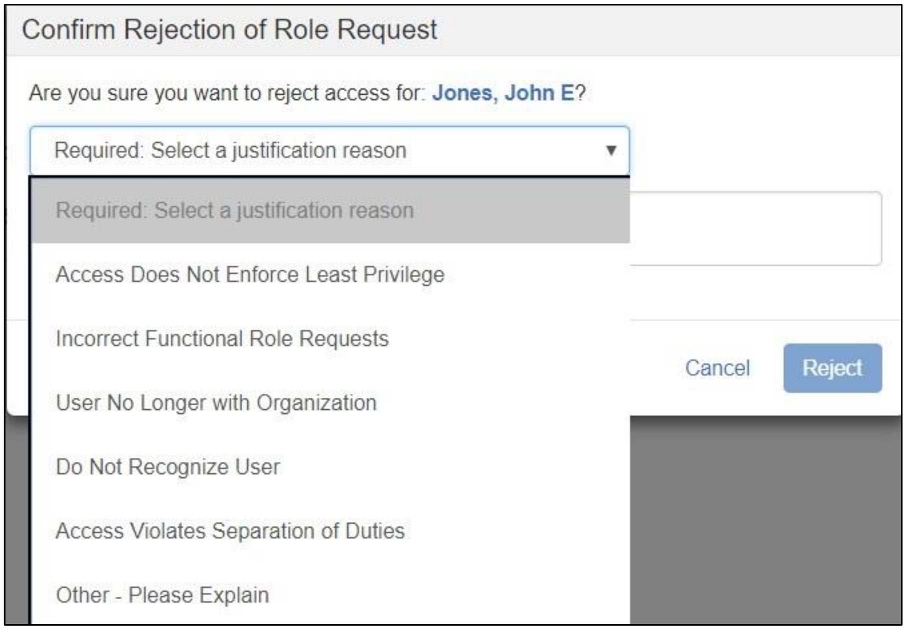


Figure 46 – Reject Role Request Justification Reason

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

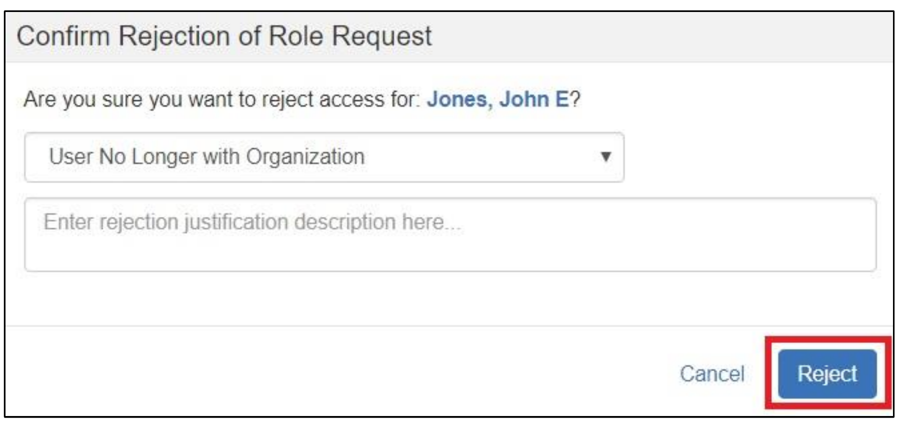


Figure 47 - Access Request Rejection

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

Figure 48 – Functional Role Rejection Notification

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

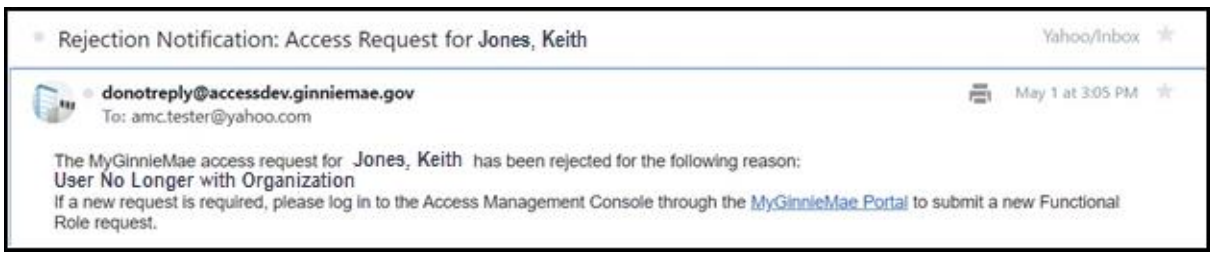


Figure 49 - Access Request Rejection Email Notification

4.3 Managing and Maintaining User Accounts

4.3.1 Disable a User 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 Section: 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 **User Management** tile.

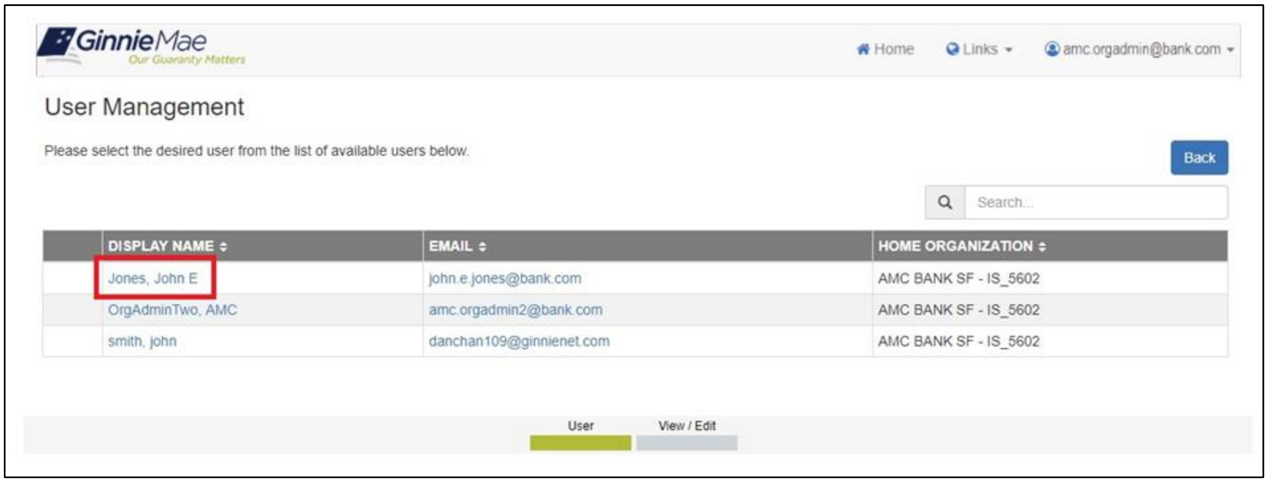


Figure 50 - Select User

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**.

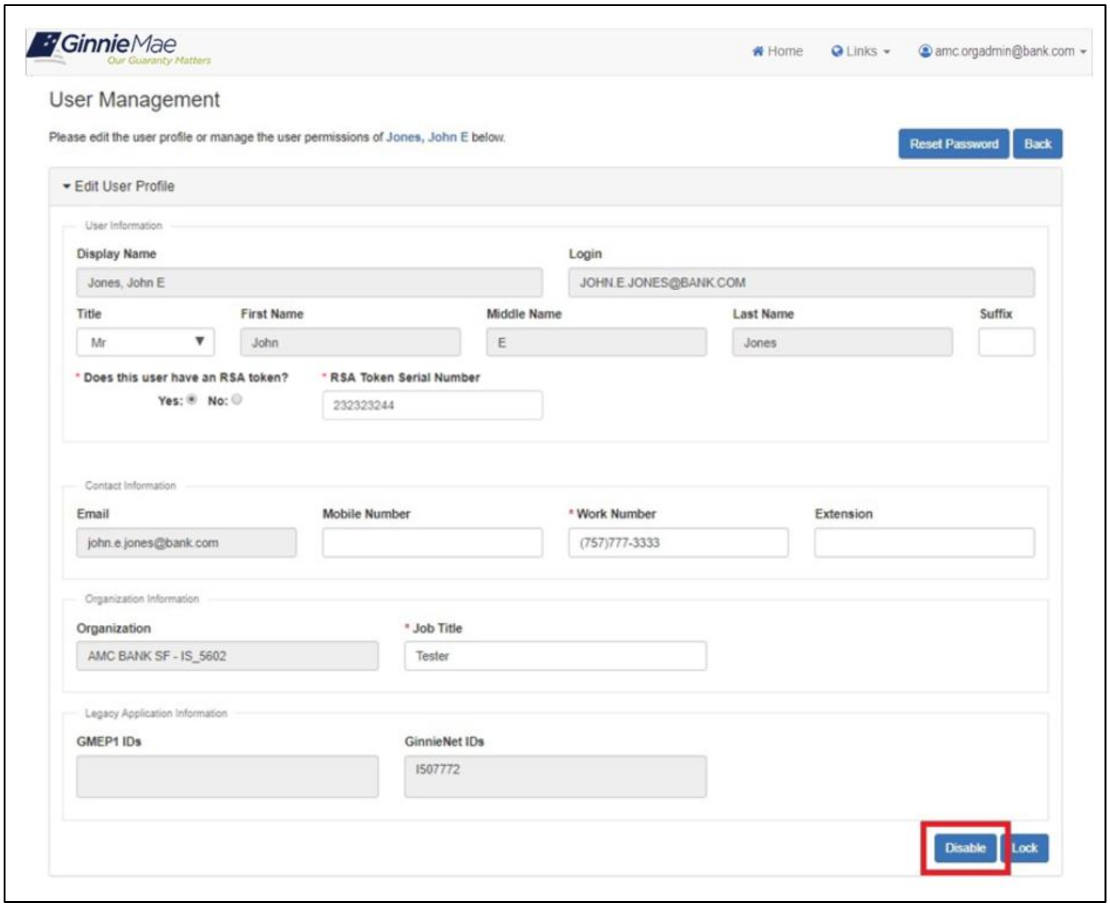


Figure 51 - User Management – Disable Account

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

Figure 52 - 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.

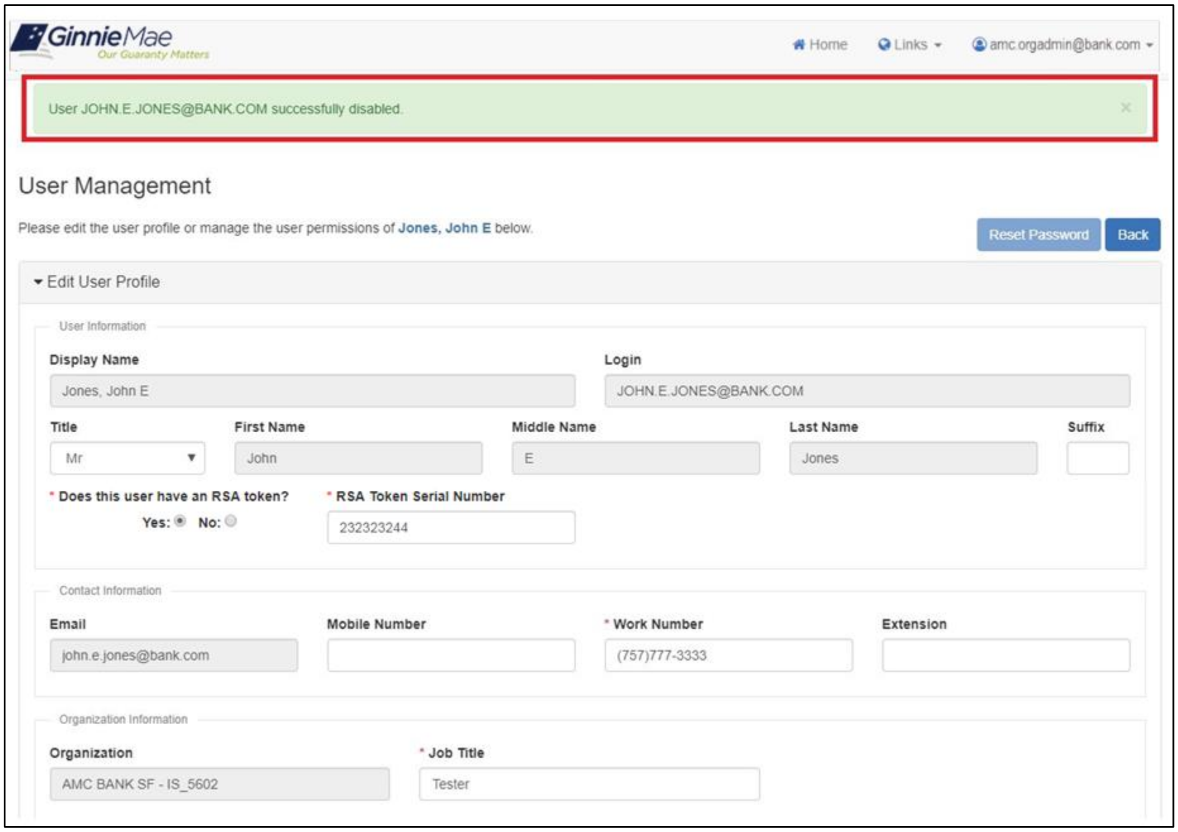


Figure 53 - Disable Account Notification

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.

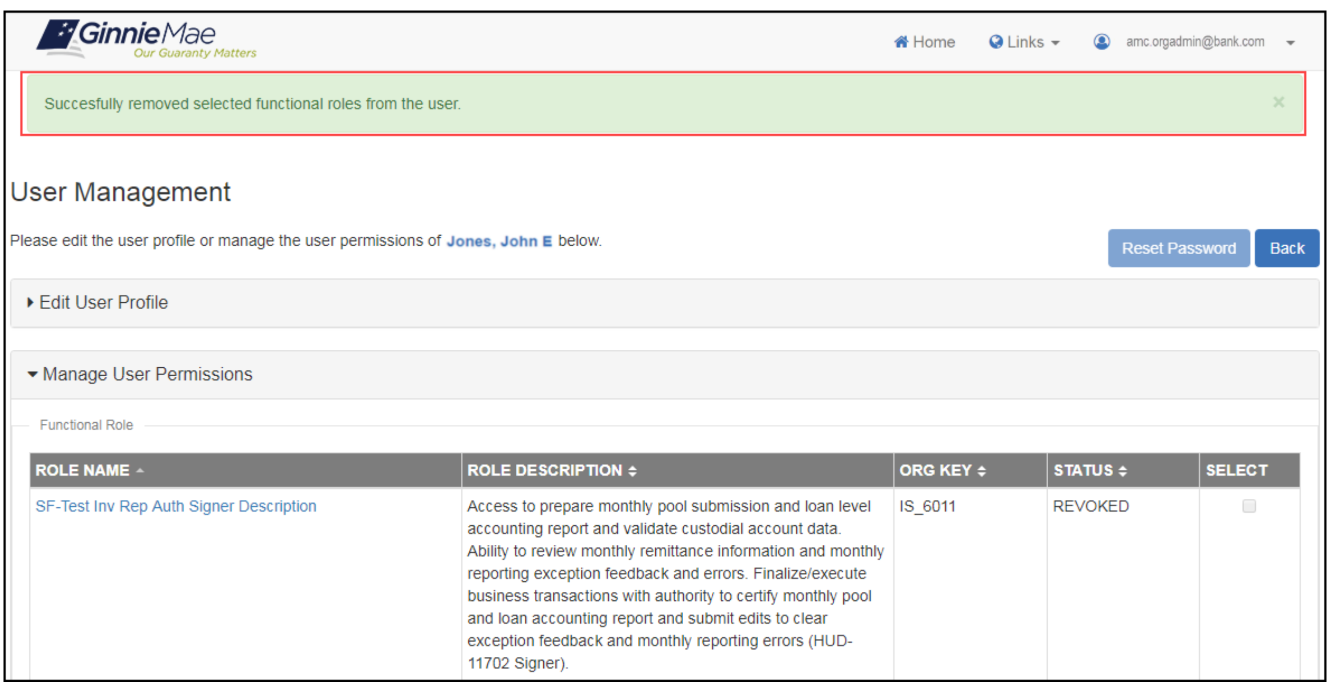


Figure 54 - Select Disabled User Functional Roles

4.3.2 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 and approved 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 Section: Re-Request a Functional Role**.**

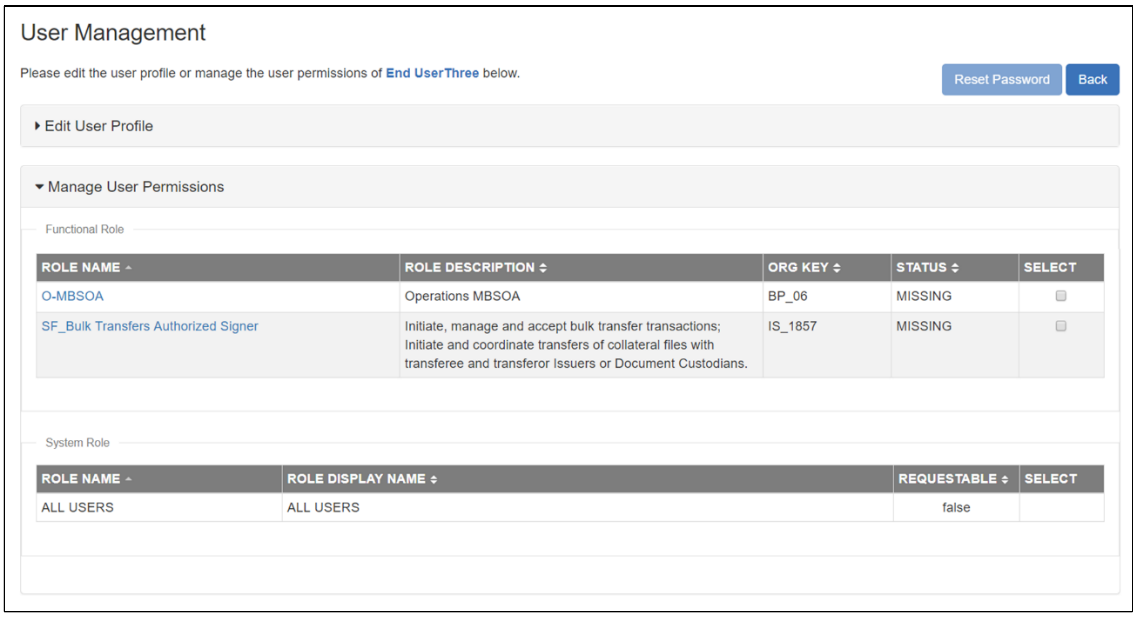


Figure 55 - Functional Role Missing Status

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 **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.

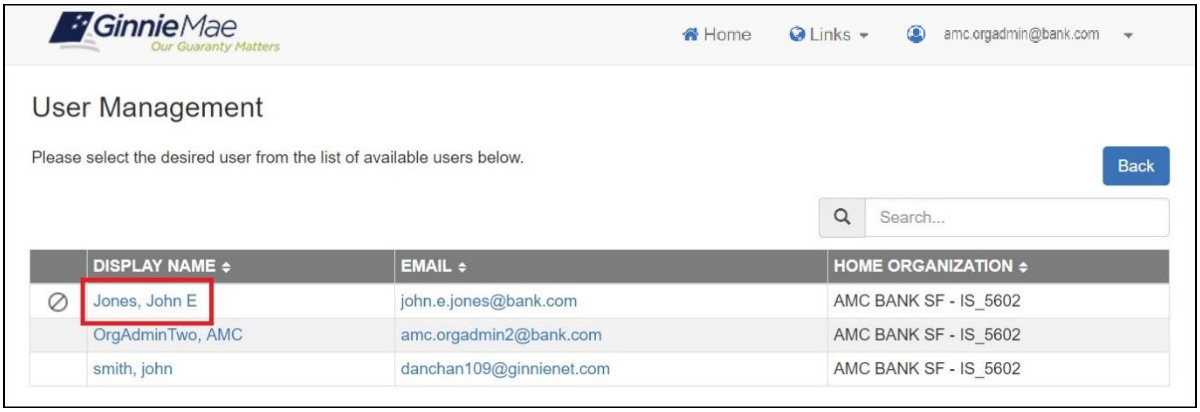


Figure 56 – User Management Disabled User

5. Once the "User Profile" page opens, select the "Enable" button in the bottom right of the "Edit User Profile" accordion.

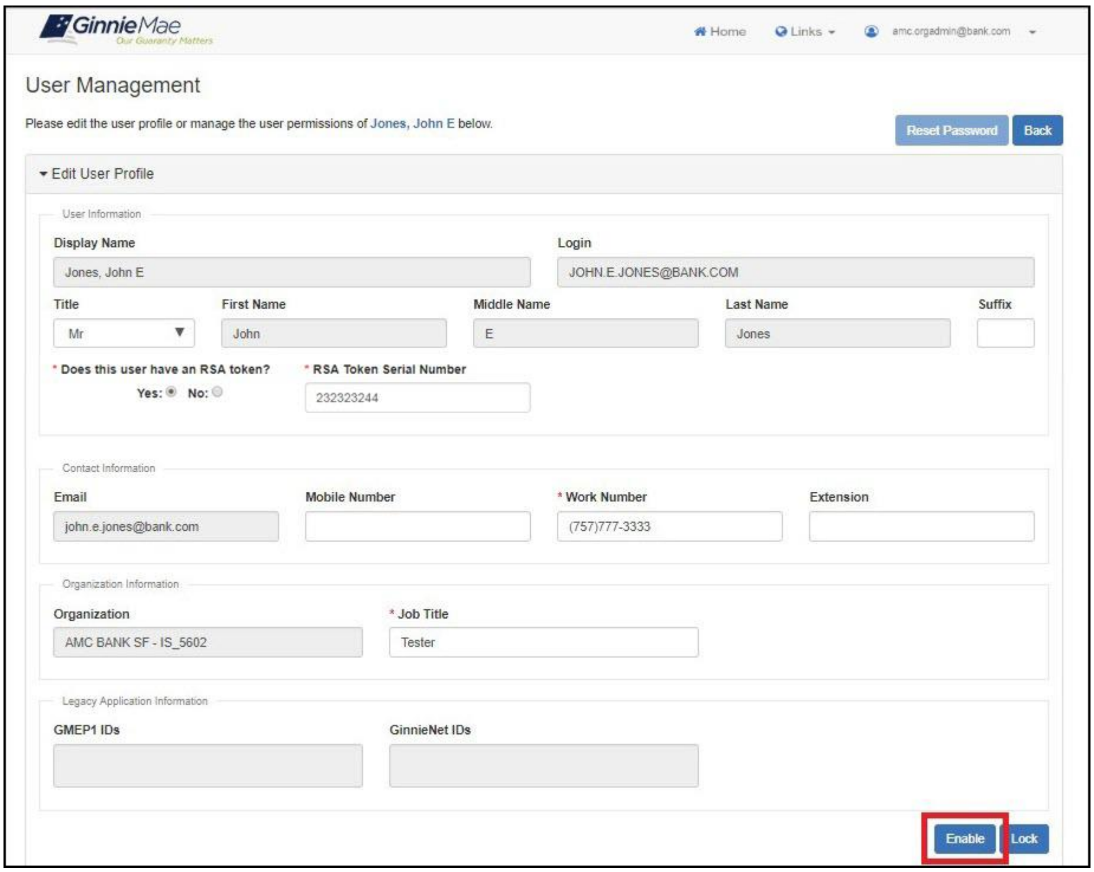


Figure 57 - User Management – Enable Account

6. The system displays an overlay to confirm the enabling of the selected user's account.
   a. Select **Confirm** to submit the request.

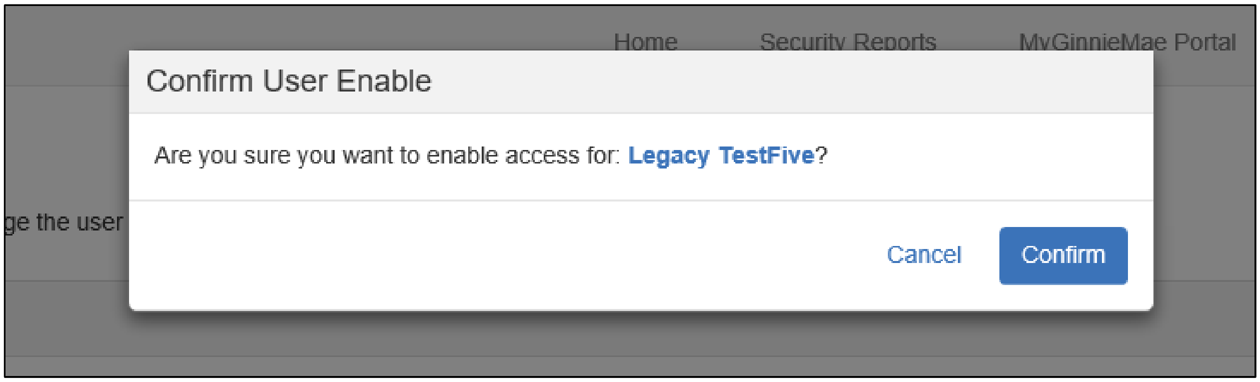


Figure 58 - Confirm Enable Account

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.

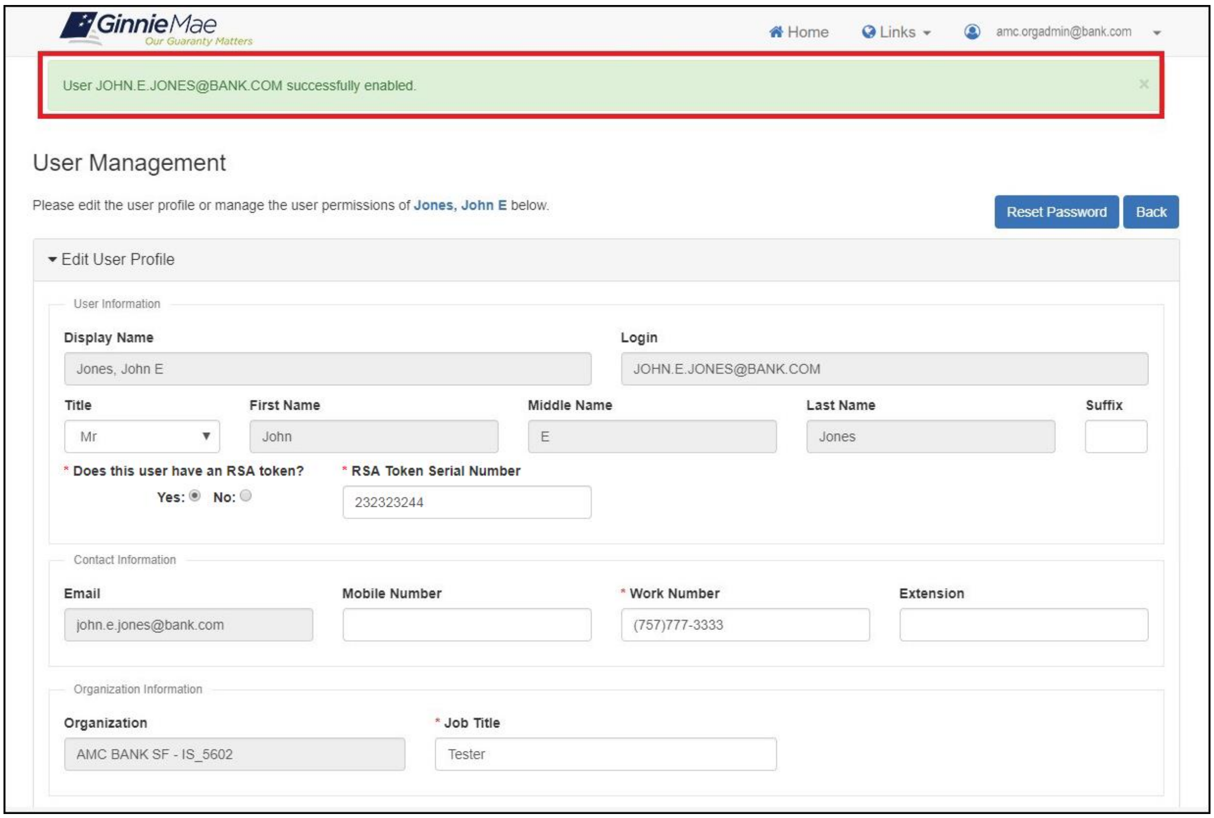
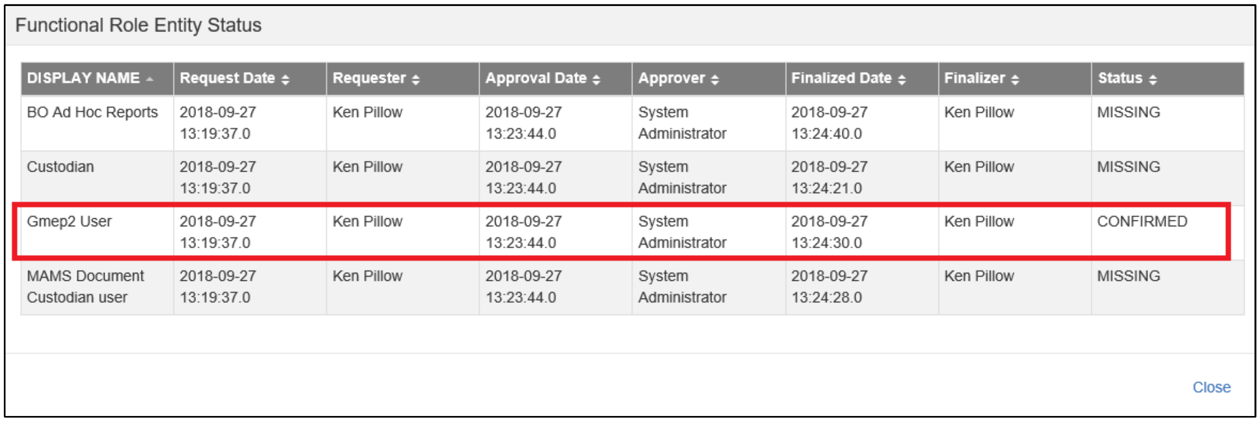


Figure 59 - Enable Account Notification

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 [Section: Verify an Assigned Functional Role),](#) the status will update accurately.



Functional Role Entity Status

DISPLAY NAME	Request Date	Requester	Approval Date	Approver	Finalized Date	Finalizer	Status
BO Ad Hoc Reports	2018-09-27 13:19:37.0	Ken Pillow	2018-09-27 13:23:44.0	System Administrator	2018-09-27 13:24:40.0	Ken Pillow	MISSING
Custodian	2018-09-27 13:19:37.0	Ken Pillow	2018-09-27 13:23:44.0	System Administrator	2018-09-27 13:24:21.0	Ken Pillow	MISSING
Gmep2 User	2018-09-27 13:19:37.0	Ken Pillow	2018-09-27 13:23:44.0	System Administrator	2018-09-27 13:24:30.0	Ken Pillow	CONFIRMED
MAMS Document Custodian user	2018-09-27 13:19:37.0	Ken Pillow	2018-09-27 13:23:44.0	System Administrator	2018-09-27 13:24:28.0	Ken Pillow	MISSING

Close

Figure 60 - GMEP2_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.

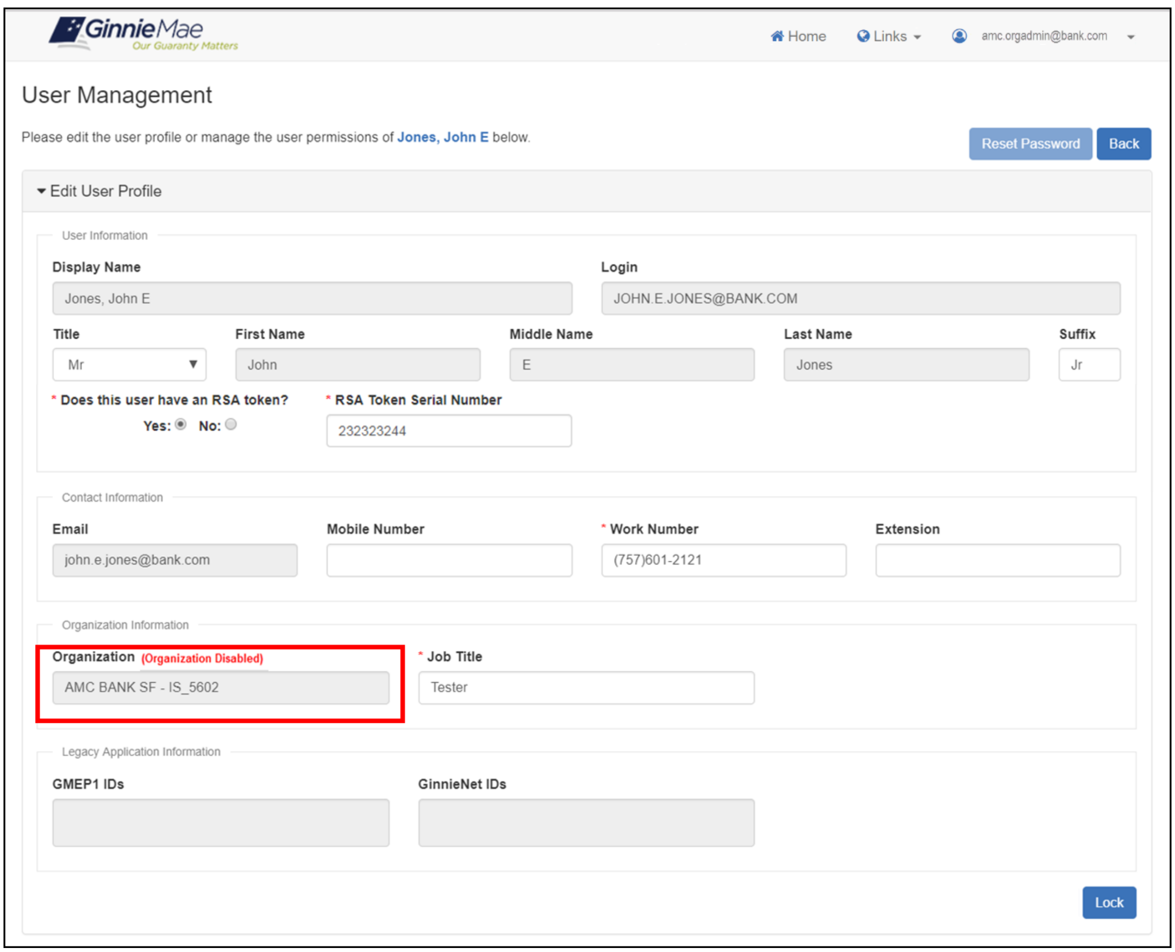


Figure 61 - Disabled Organization User Profile

4.3.3 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 Section: 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 **User Management** tile.

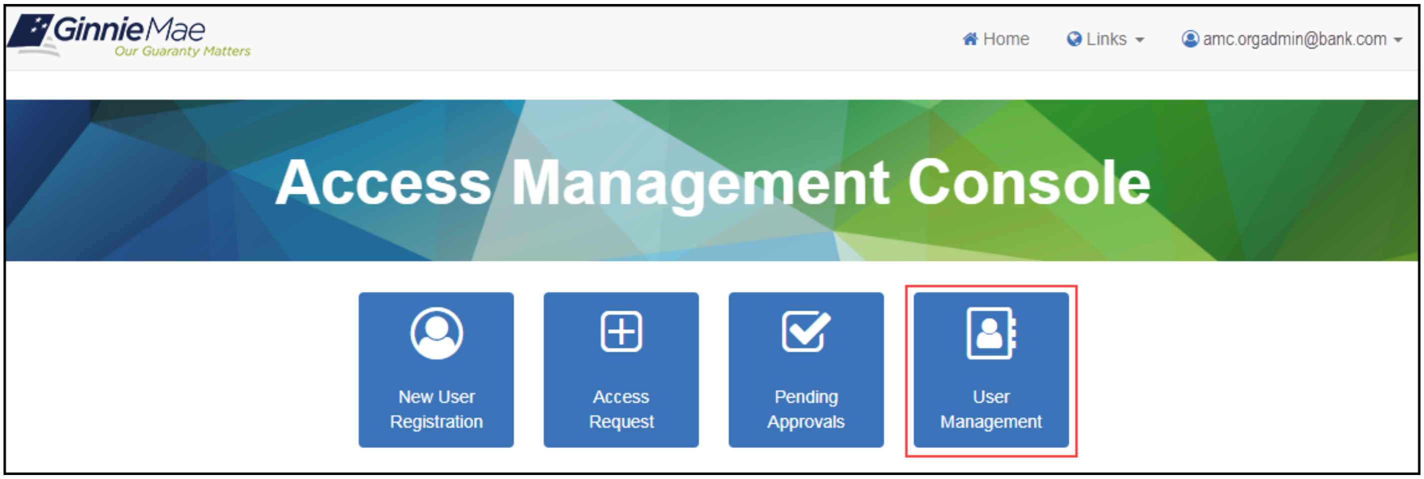


Figure 62 - Access Management Console Landing Page

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.

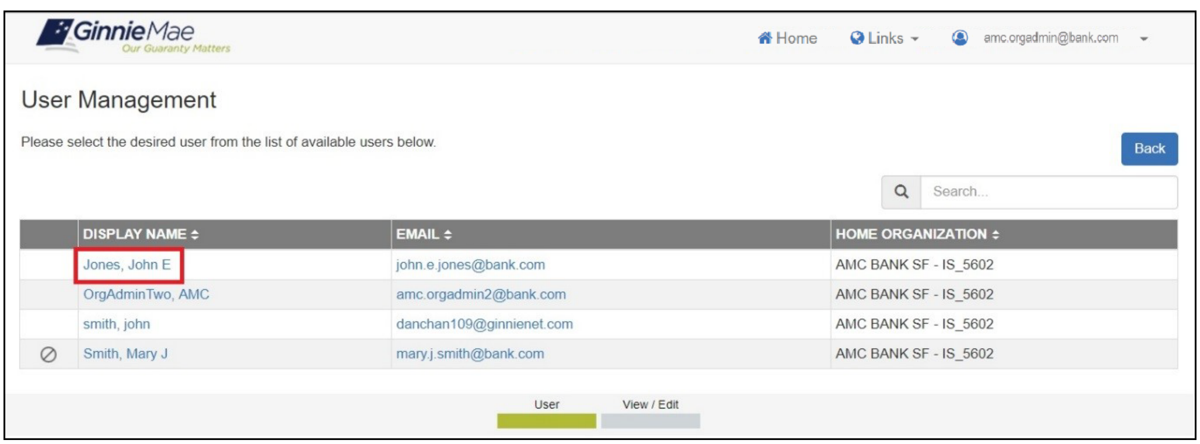


Figure 63 - Search Users Results

5. Select the "Edit User Profile" down arrow
   a. Select **Lock.**

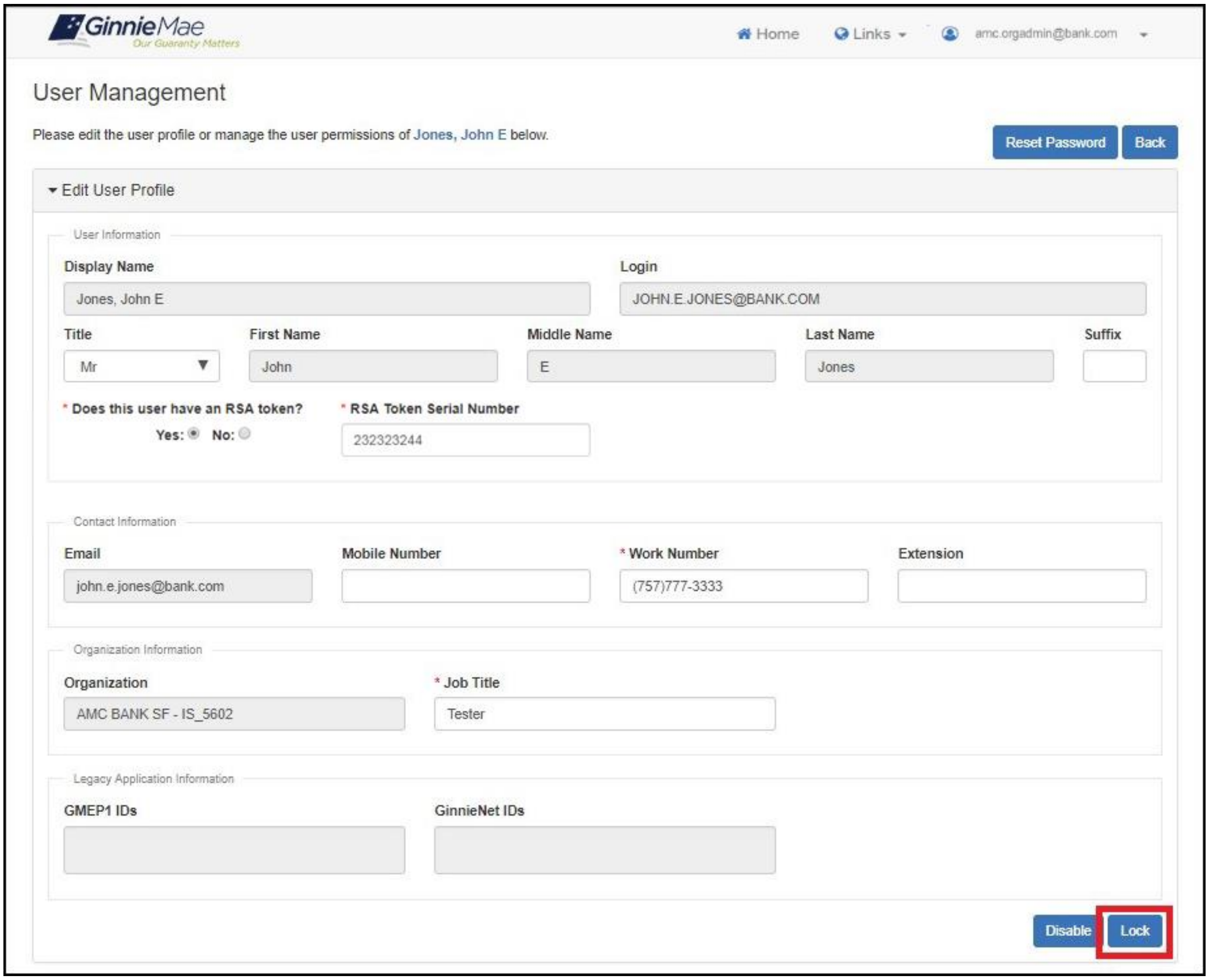


Figure 64 - User Management – Lock Account

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

Figure 65 - Confirm Account Lock

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

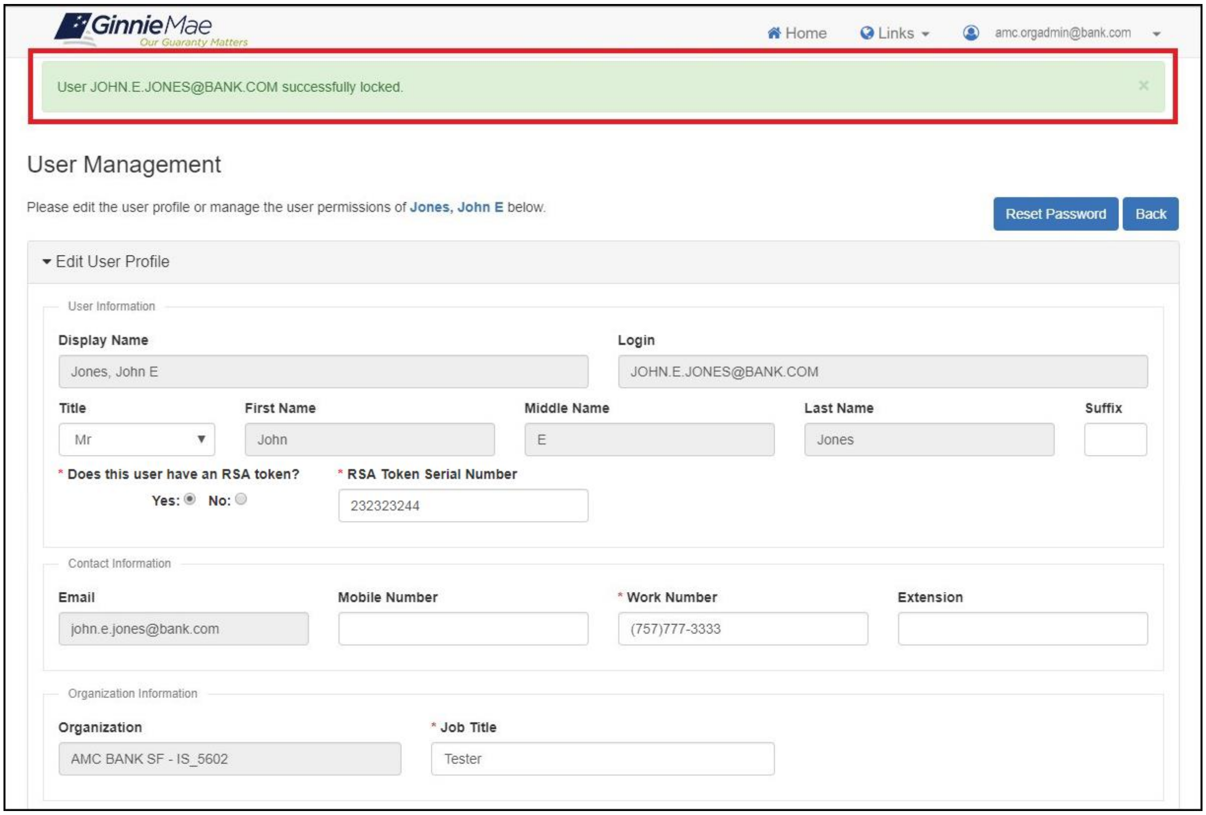


Figure 66 - Lock Account Notification

4.3.4 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

The Organization Administration 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 **User Management** tile.
4. Find and select the Display Name of the user account.

Figure 67 - Locked User Search

5. Select the "Edit User Profile" down arrow
   a. Select **Unlock.**

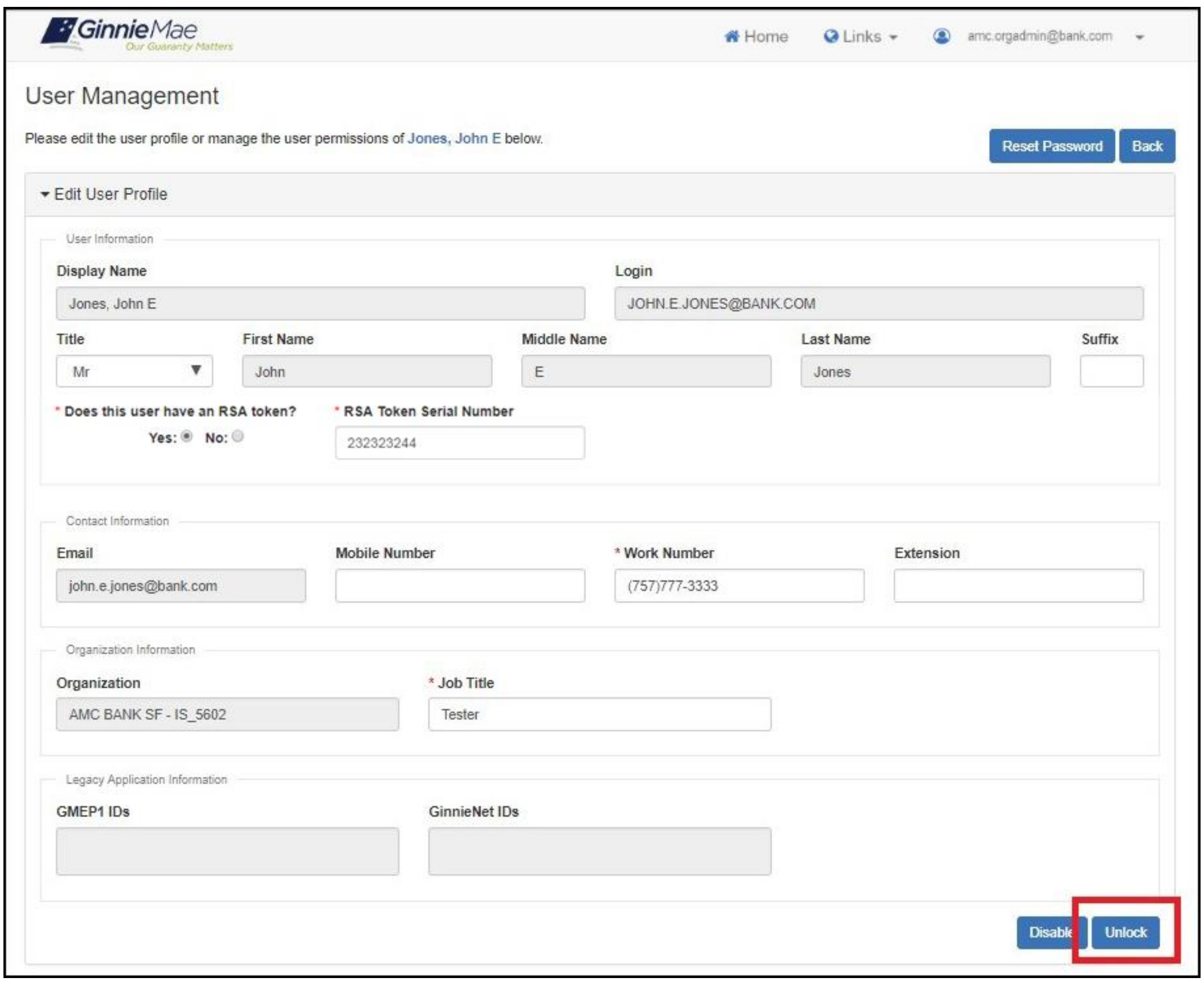


Figure 68 - User Management – Unlock Account

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

Figure 69 - 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."

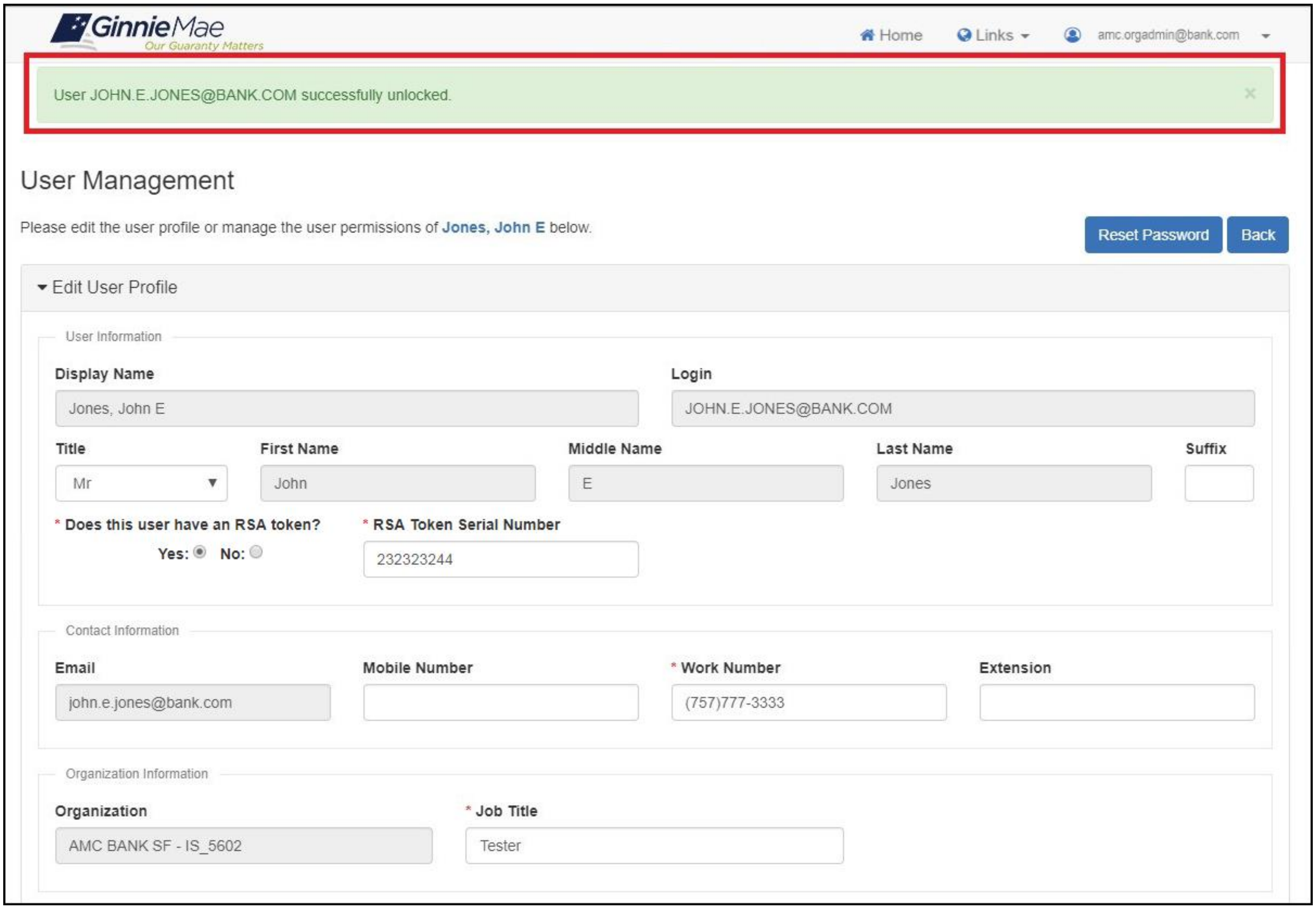


Figure 70 - Unlock Account Notification

4.3.5 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

NOTE: If the user's email address has changed, a new End User account must be created. Contact the Ginnie Mae Customer Support Hotline 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 user attributes
    b. Select **Save**.

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

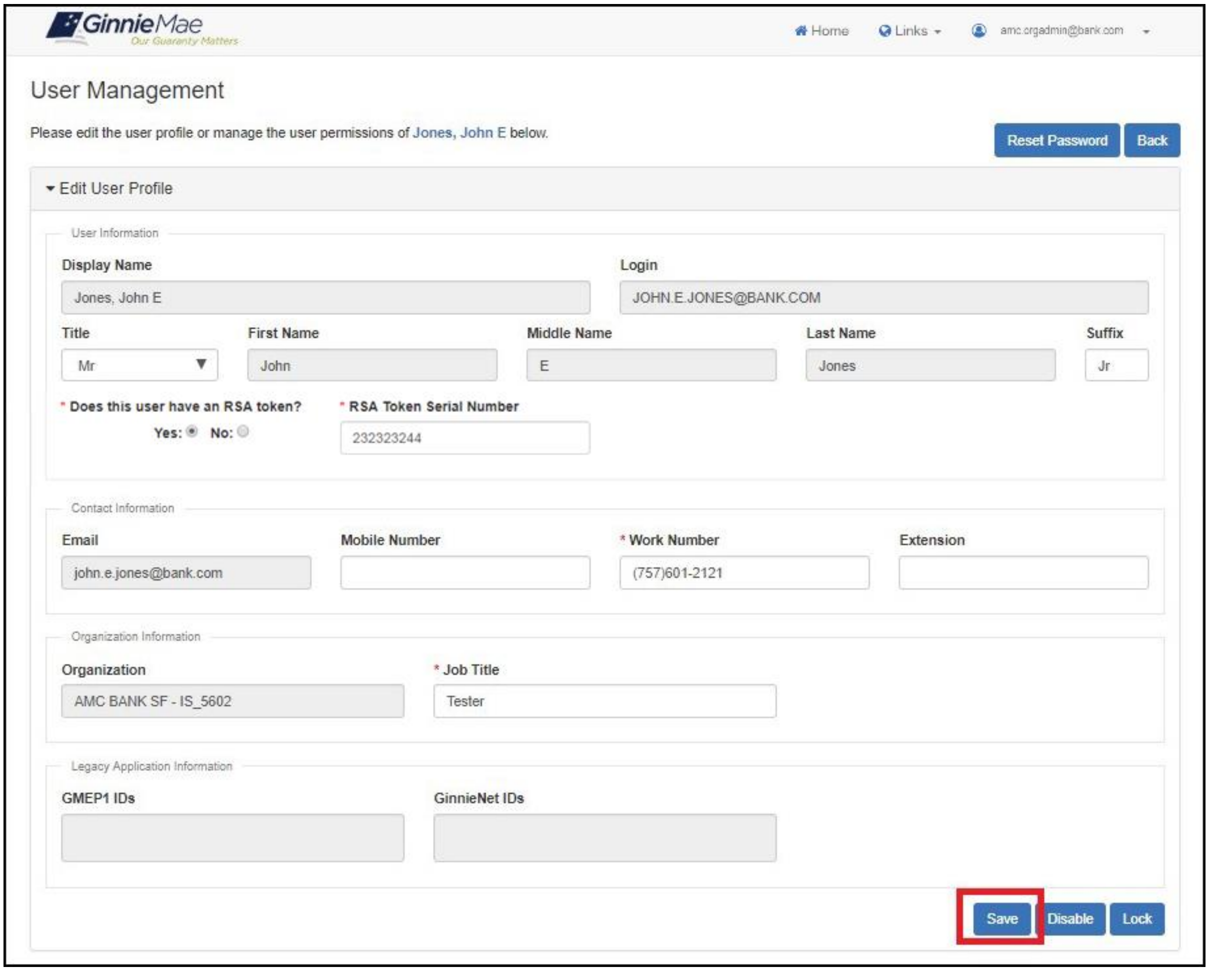


Figure 71 - User Management – Update User Profile

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.

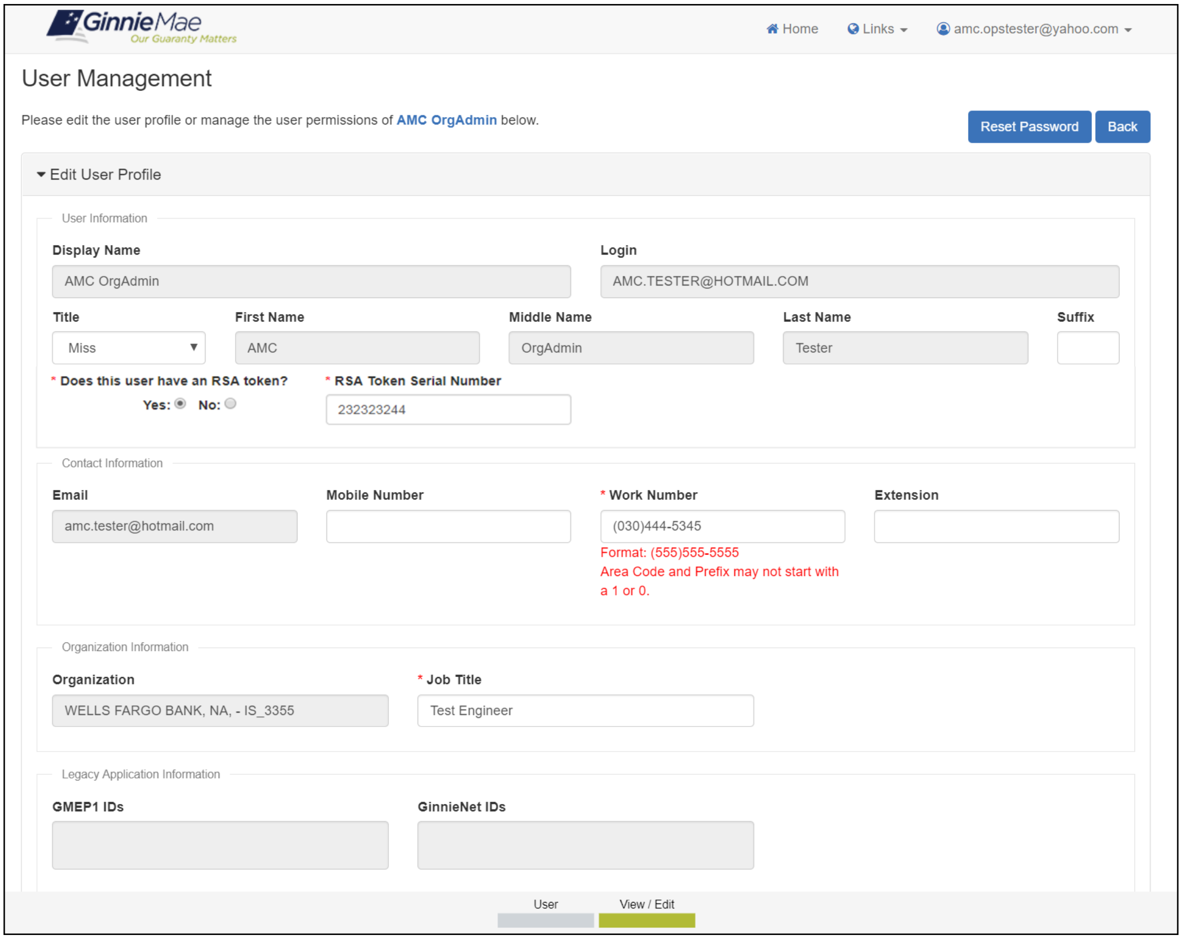


Figure 72 - Telephone Incorrect Format

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

Figure 73 - Confirm User Profile Update

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

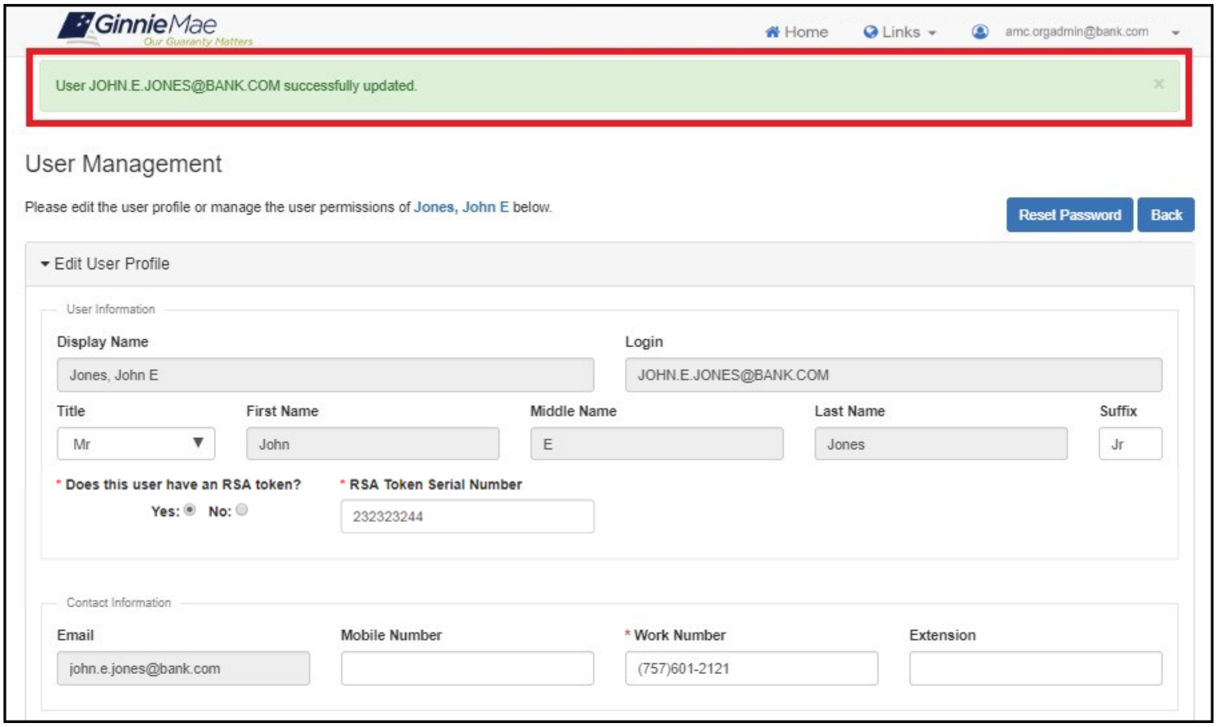


Figure 74 - Update User Profile Notification

4.3.6 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 **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

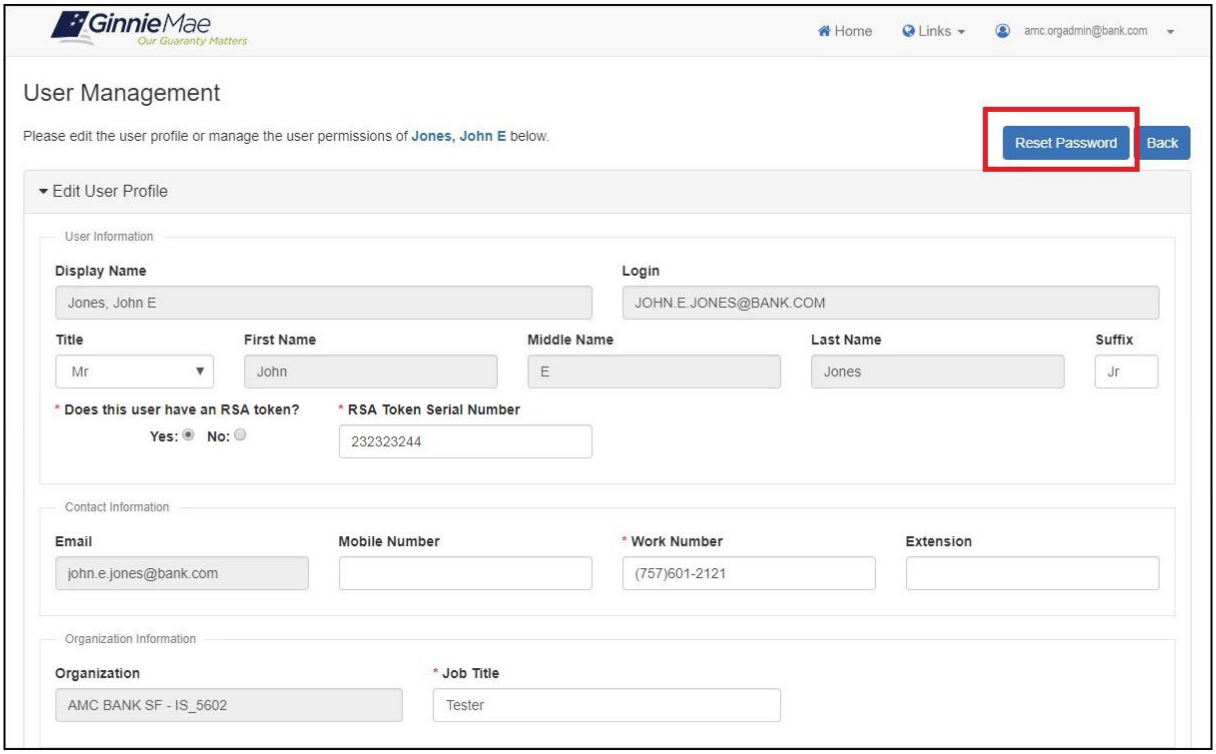


Figure 75 – Reset Password Button

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 76 - 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.

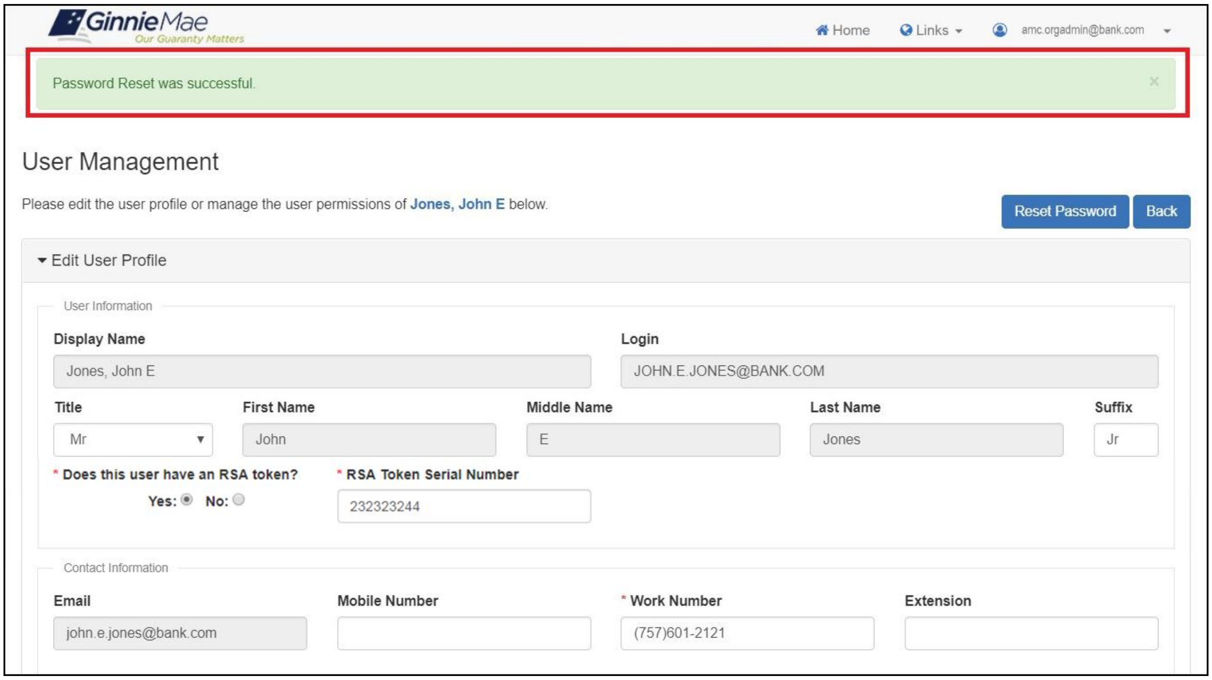


Figure 77 - Reset Password Notification

4.3.7 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 **User Management** tile.

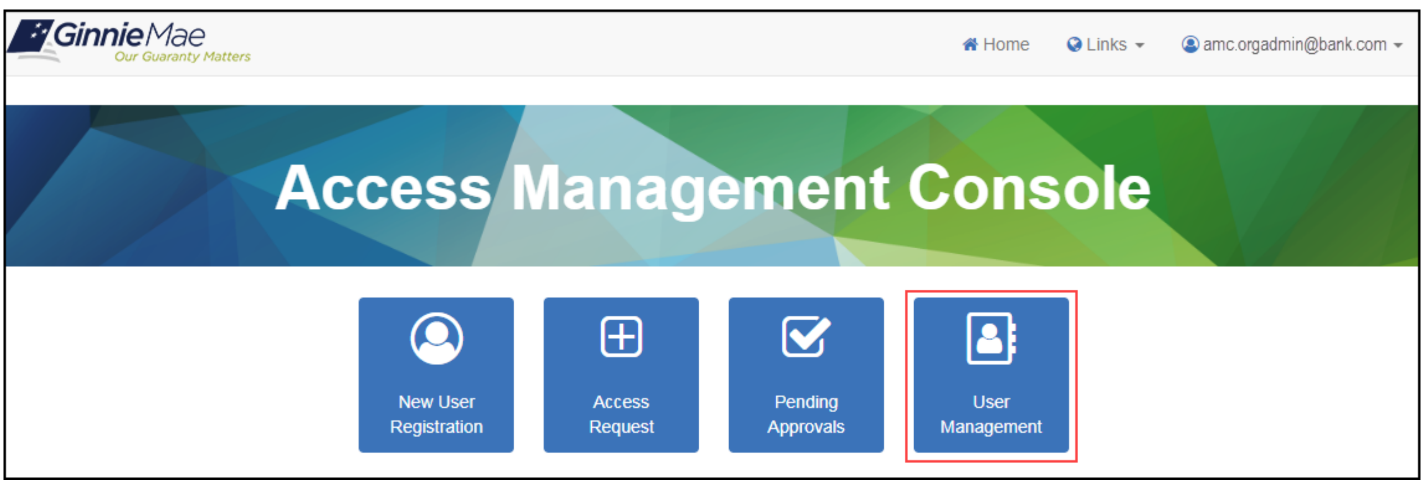


Figure 78 - Access Management Console Landing Page

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

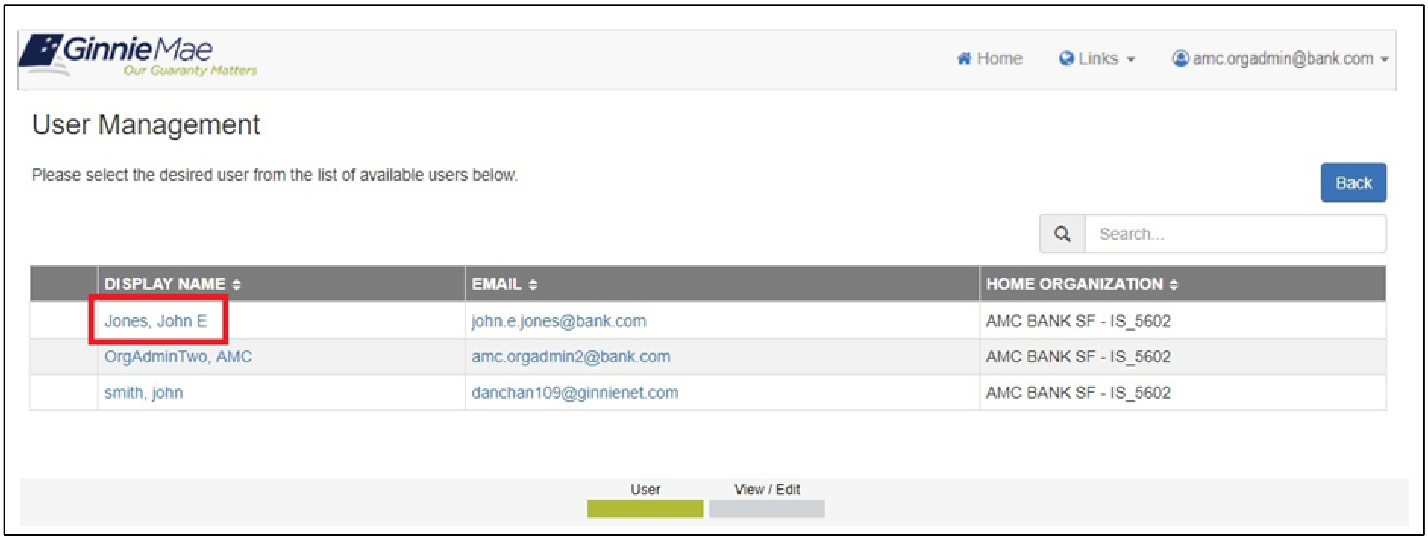


Figure 79 - Select User

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.

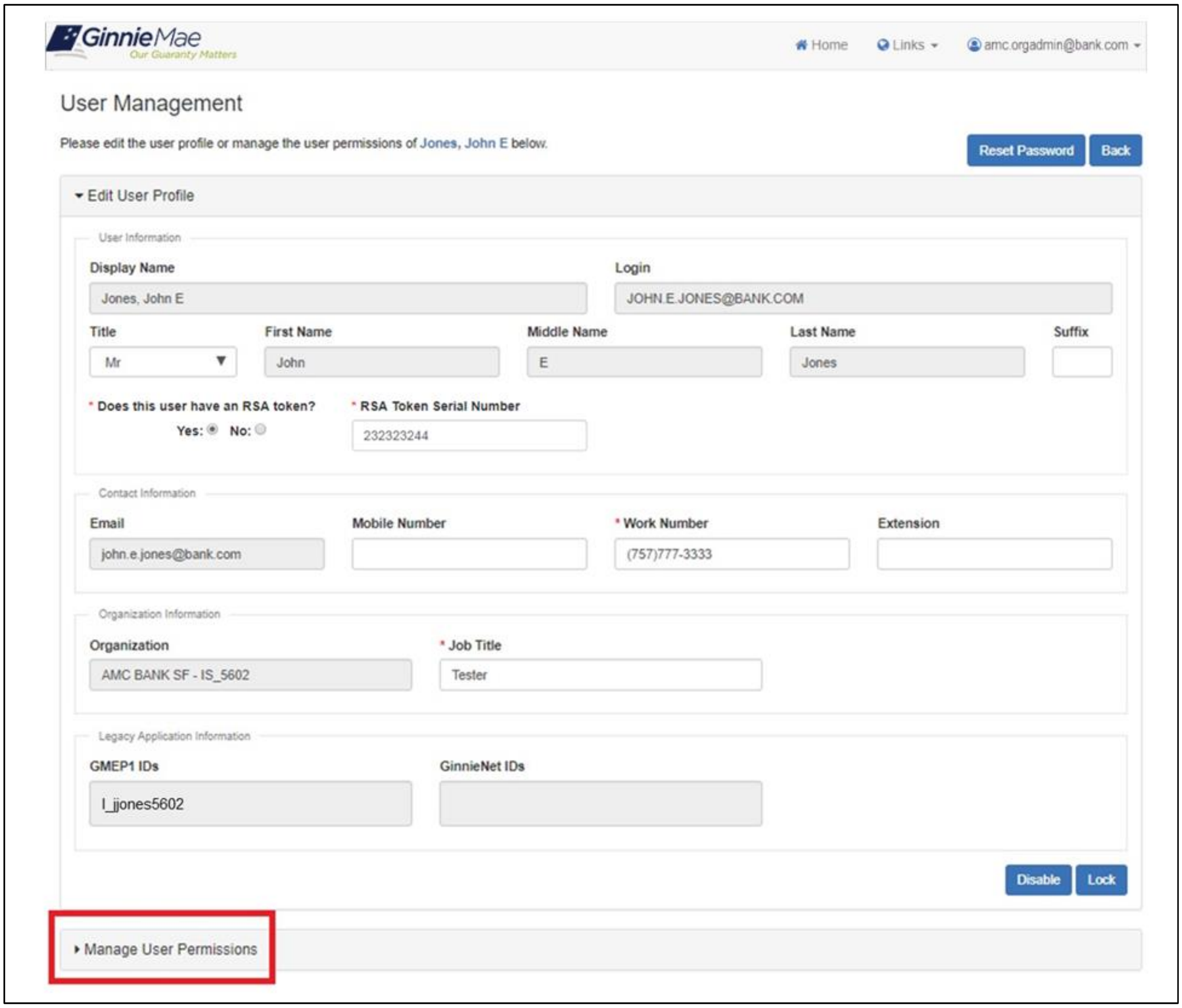


Figure 80 – User Profile

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

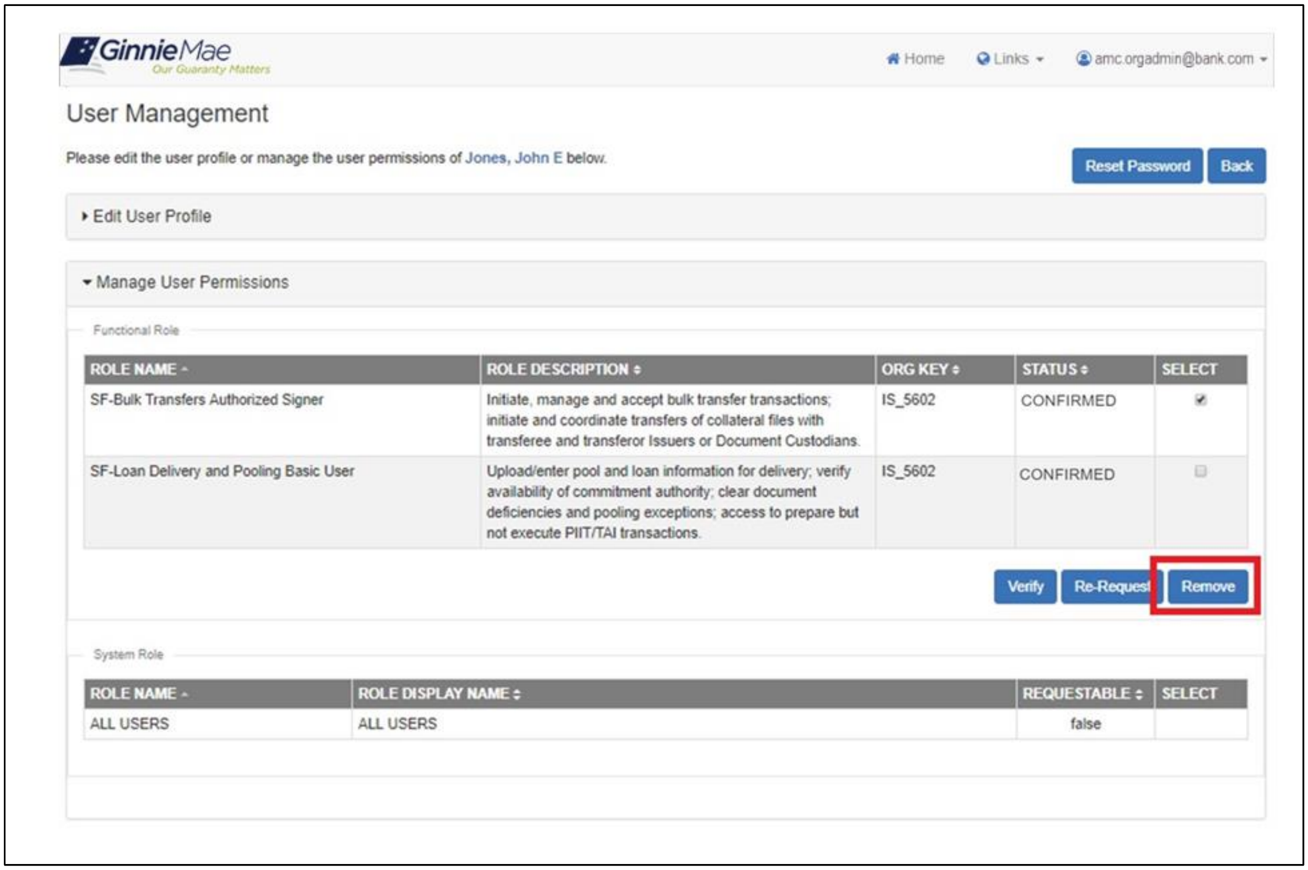


Figure 81 - Remove Functional Roles

7. The system displays a confirmation message.
   a. Select **Confirm** to proceed with the removal of the selected Functional Role.

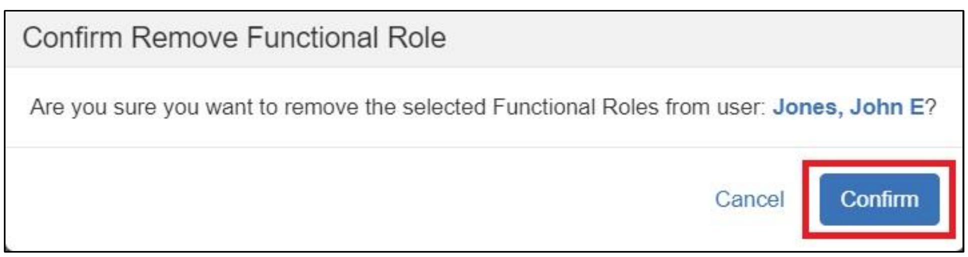


Figure 82 - Confirm Functional Role Removal

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

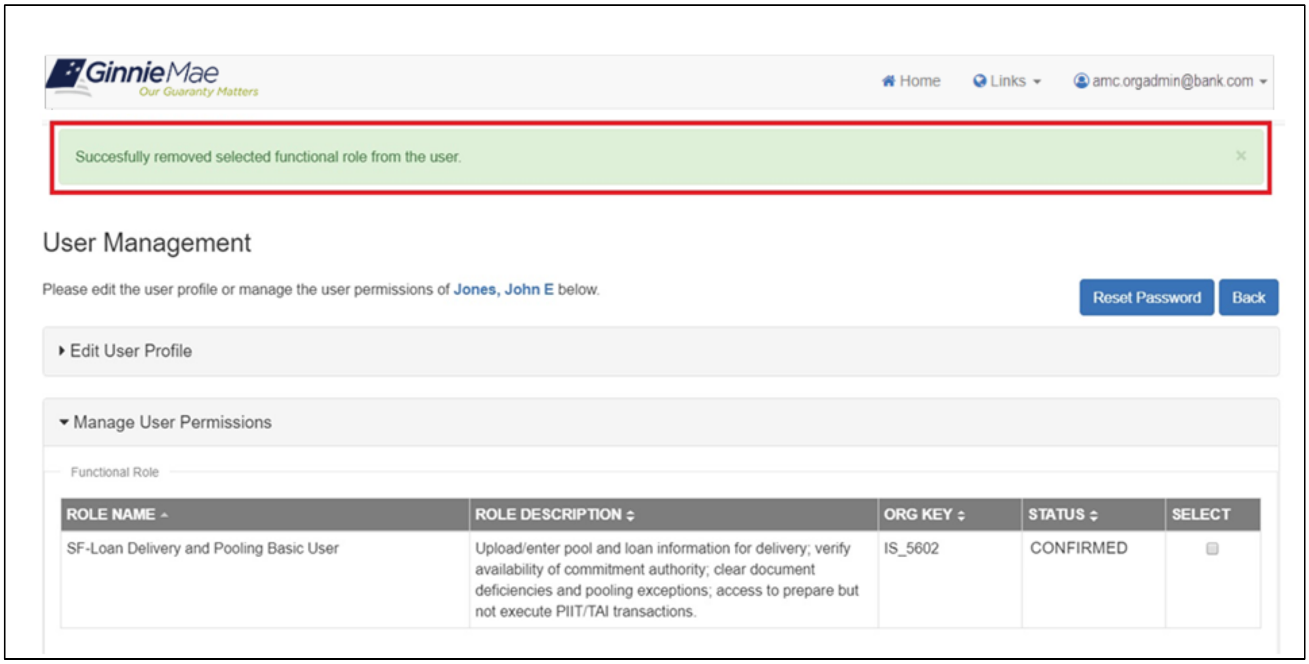


Figure 83 - Functional Role Removal Notification

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.

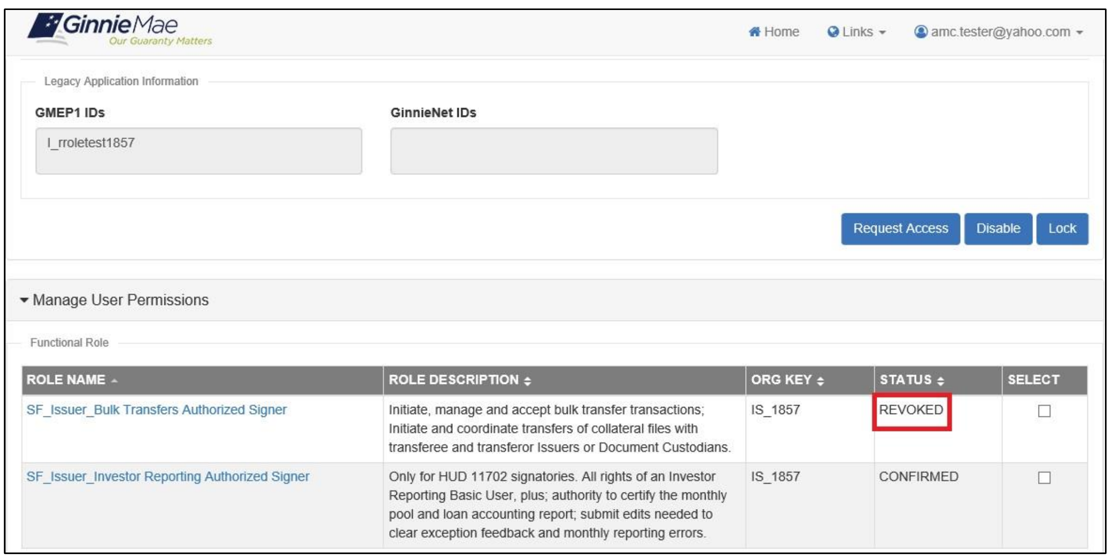


Figure 84 - Functional Role Removal Notification

NOTE: If a Functional Role is removed inadvertently, it can be requested again by following the steps in [Section: Request Functional Role].

4.3.8 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 **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.

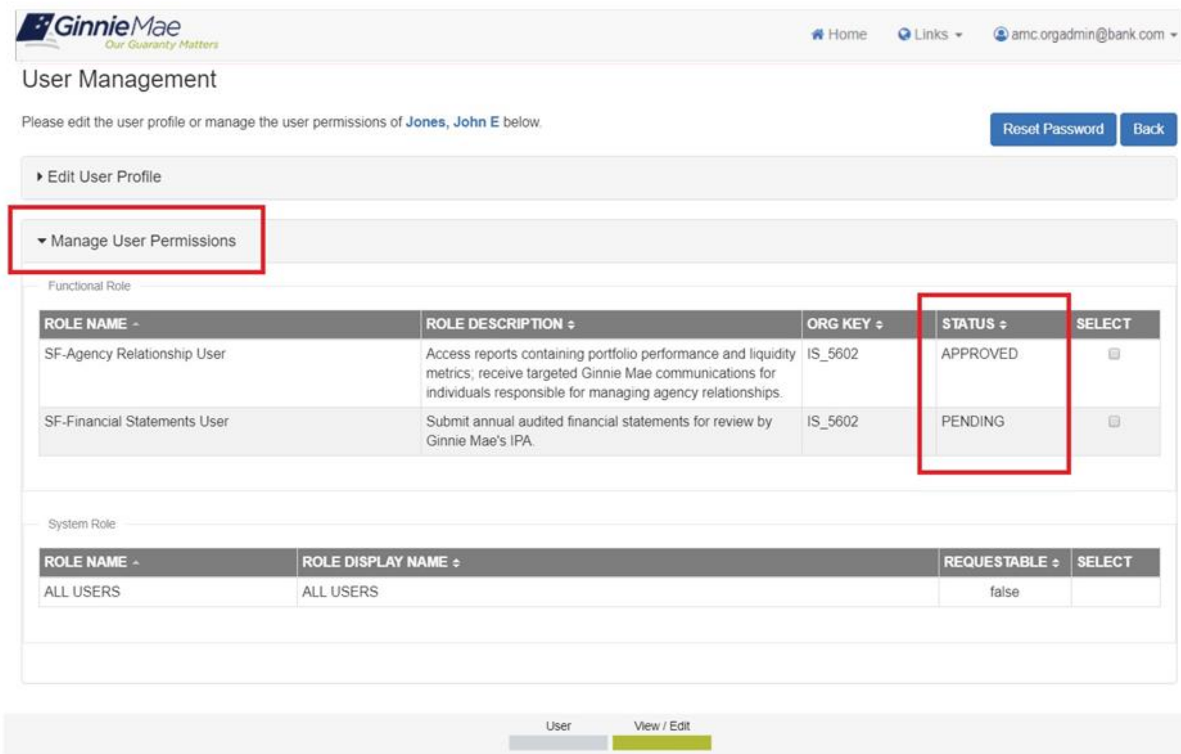


Figure 85 - Functional Role Status

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

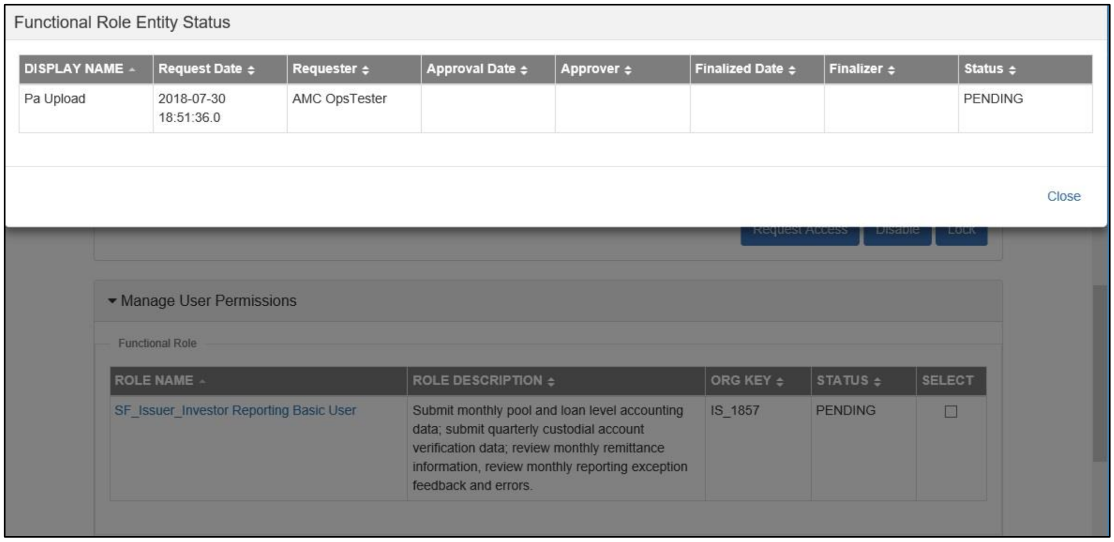


Figure 86 – Functional Role Entity Status Overlay

4.3.9 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 the Ginnie Mae Customer Support Hotline. 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**.

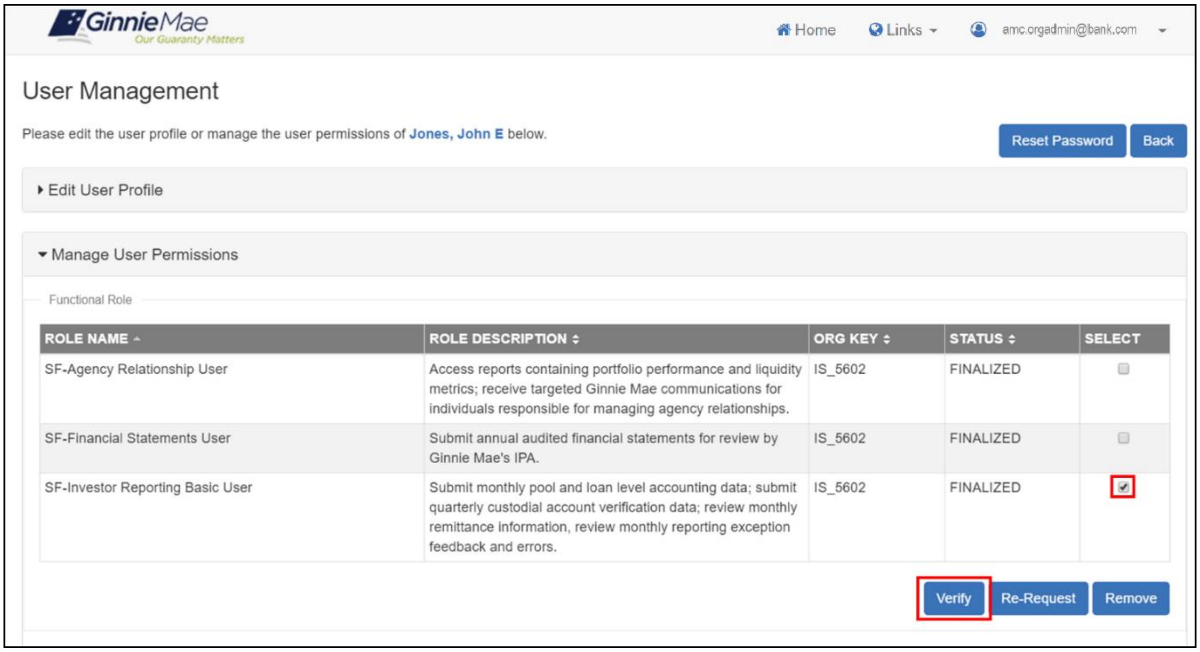


Figure 87 - User Management – Verify Functional Roles

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 Hotline .

- 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.

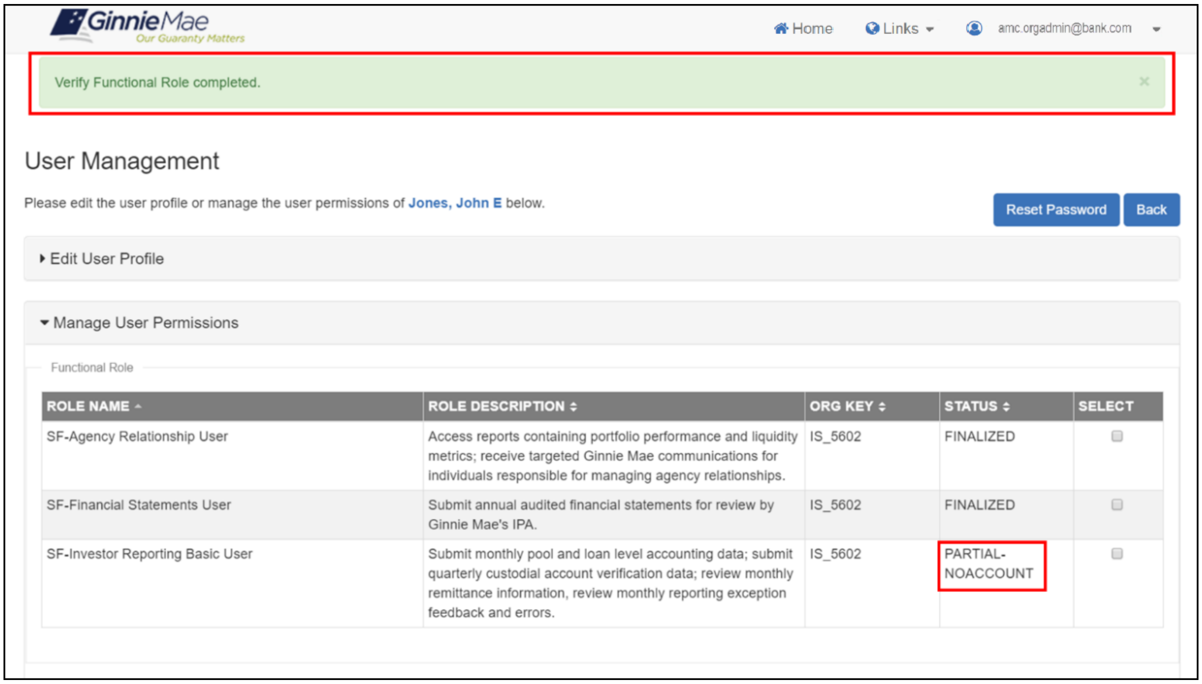


Figure 88 - Verified Functional Role Status

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

4.3.10 Re-Request a Functional Role

After the Org Admin has taken steps to Verify an Assigned Functional Role has entities that are not in “CONFIRMED” status, an Organization Administrator 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 Org Admin 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 Section: Request Functional Role.

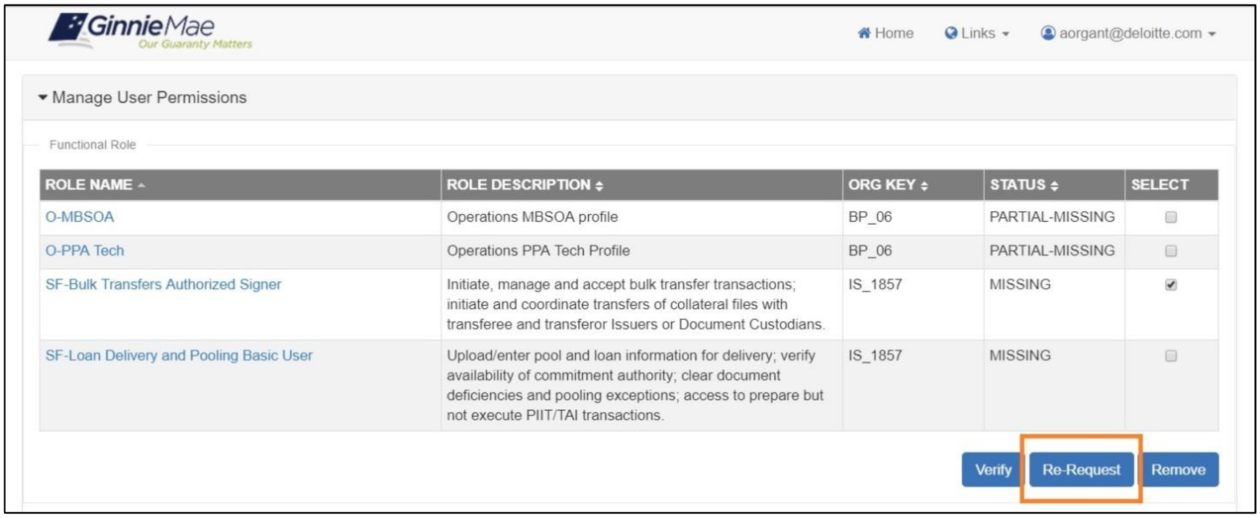


Figure 89 - Re-Request Functional Role

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 90 - 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 91 – Re-Request Role Error

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

If a user has registered with the Oracle Mobile Authenticator (OMA), they will need to de-register if they replaced 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 De-register with Oracle Mobile Authenticator. To complete this process on behalf of and End User the Org Admin may follow these steps:

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

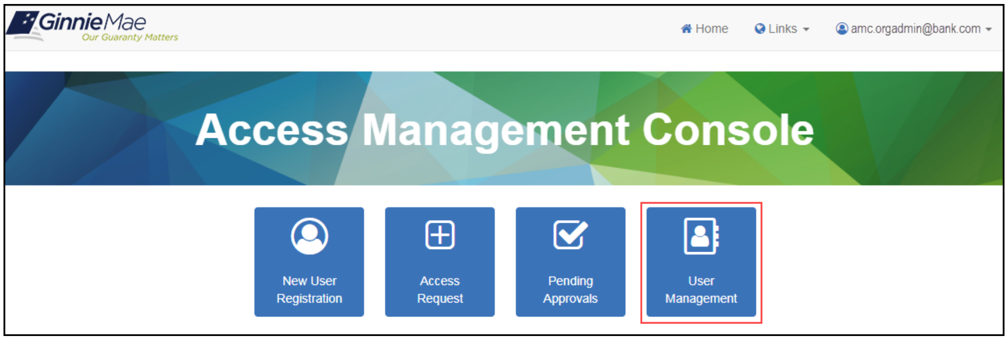


Figure 92 - Access Management Console Landing Page

4) Find and select the Display Name of the user account.

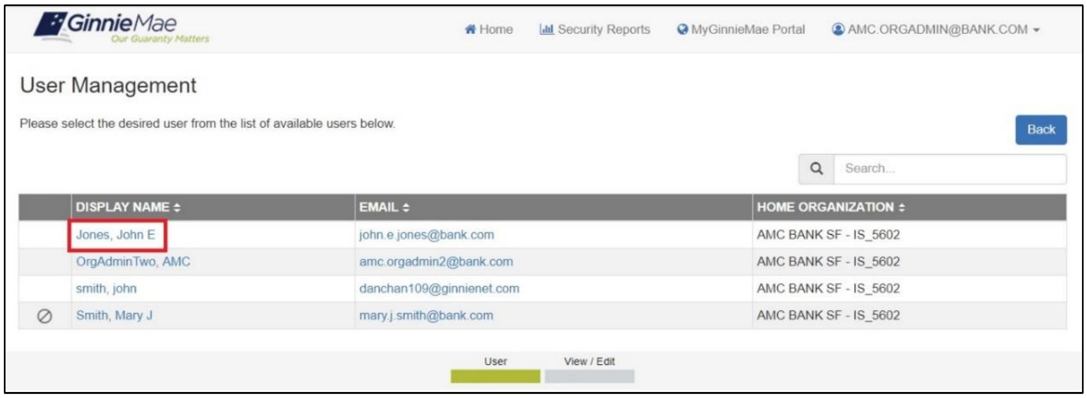


Figure 93 - Search Users Results

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

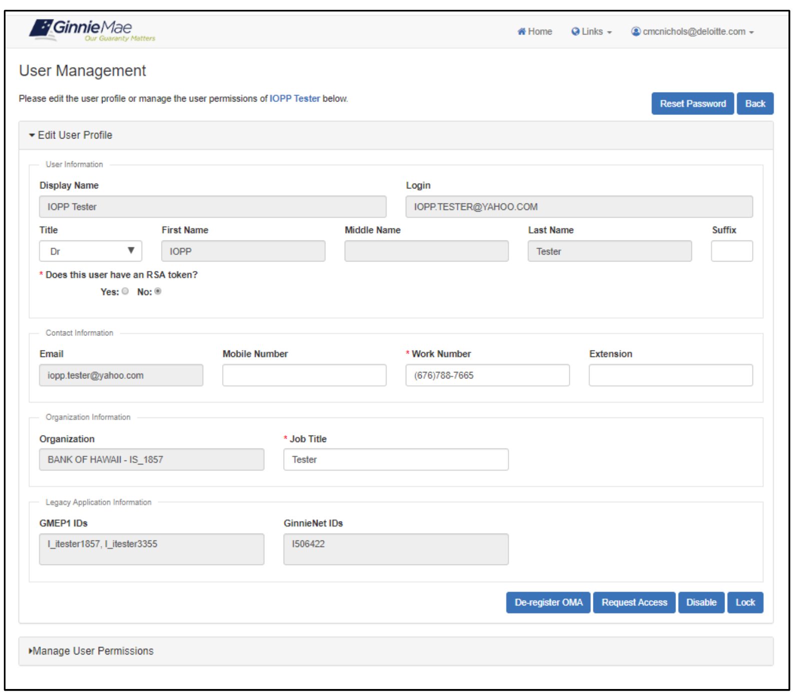


Figure 94 - De-register OMA Button on the User Profile Page

6) The system opens a dialog box to confirmation the de-registration of the OMA.

a) Select **Confirm**.

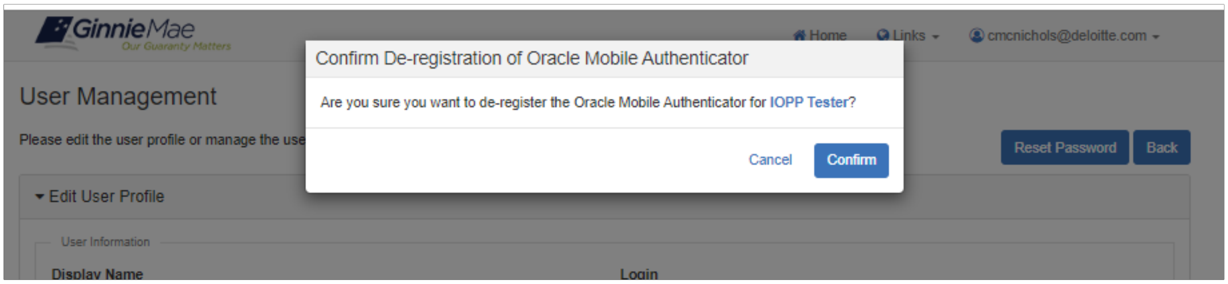


Figure 95 - Confirm De-registration of OMA as Org Admin

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

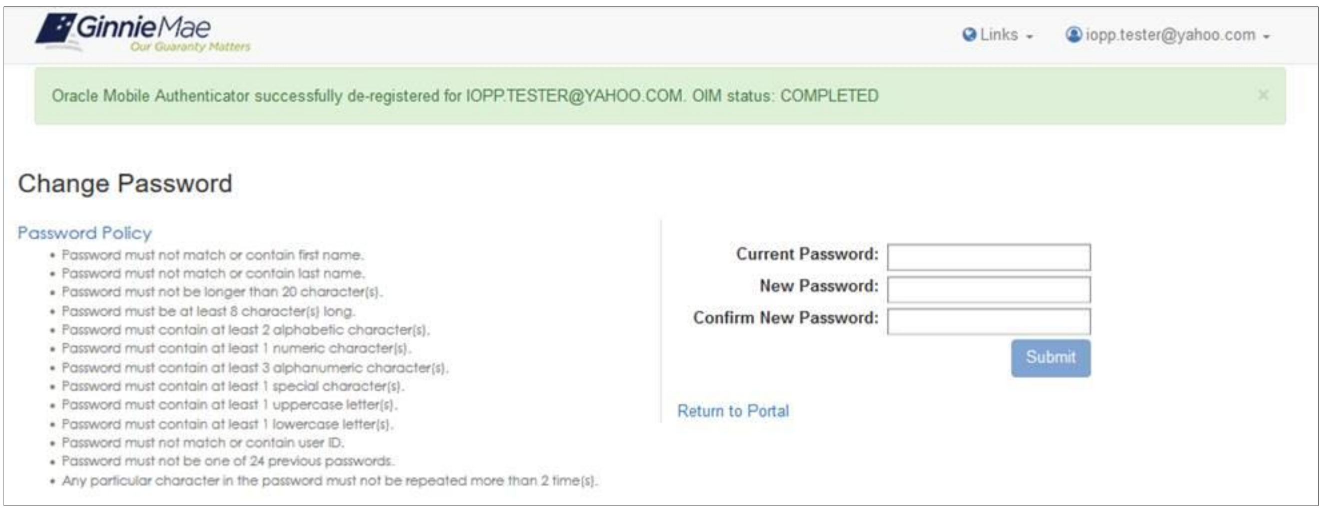


Figure 96 - Message of Successful De-registration

4.4 Troubleshooting and System Errors

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

4.4.1 AMC Error Page

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

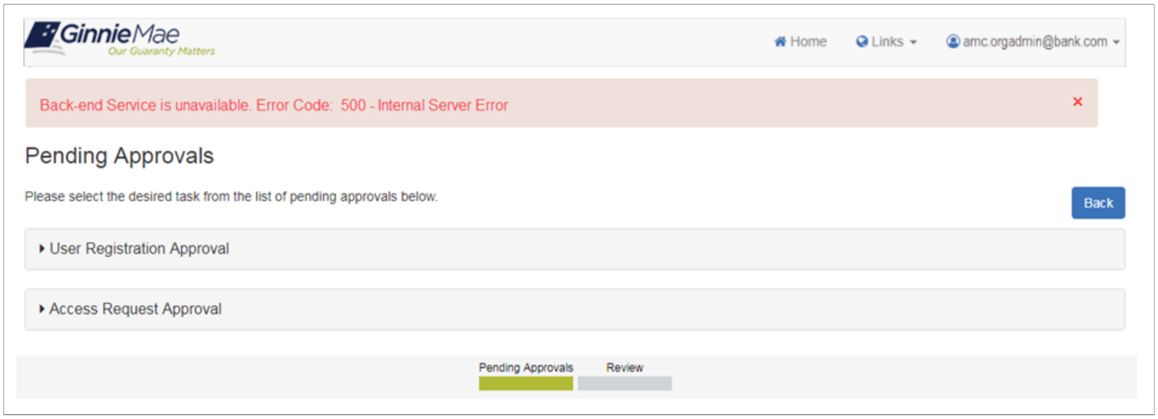


Figure 97 – Back-End Service is Unavailable Error

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.

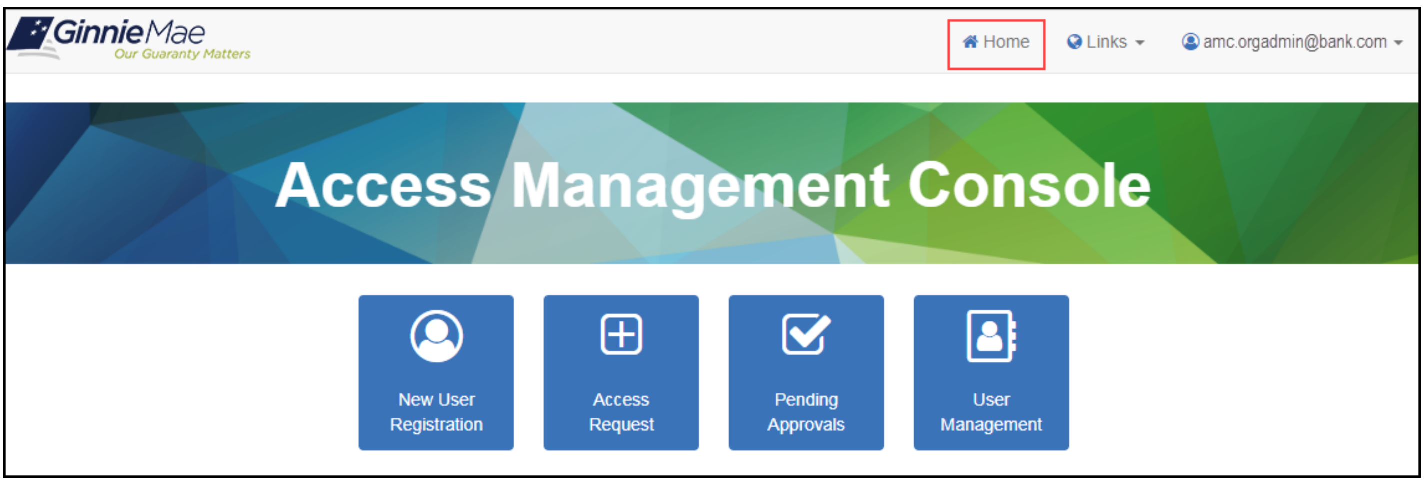


Figure 98 – Return to AMC Landing Page

4.4.2 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.

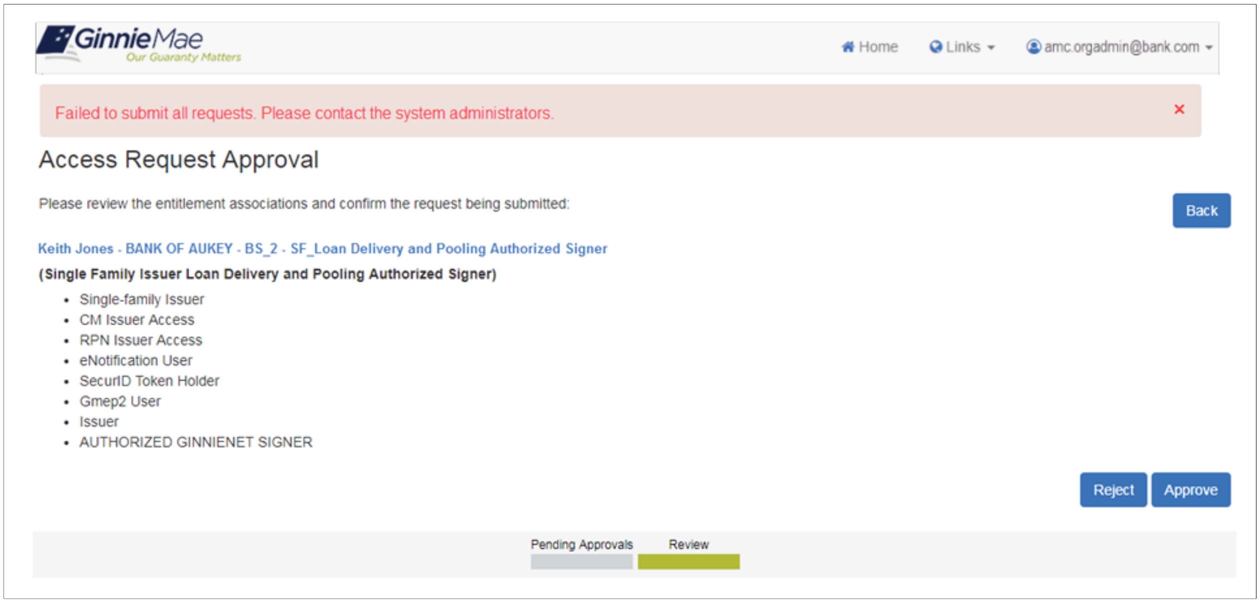


Figure 99 - Failed Access Request Submission

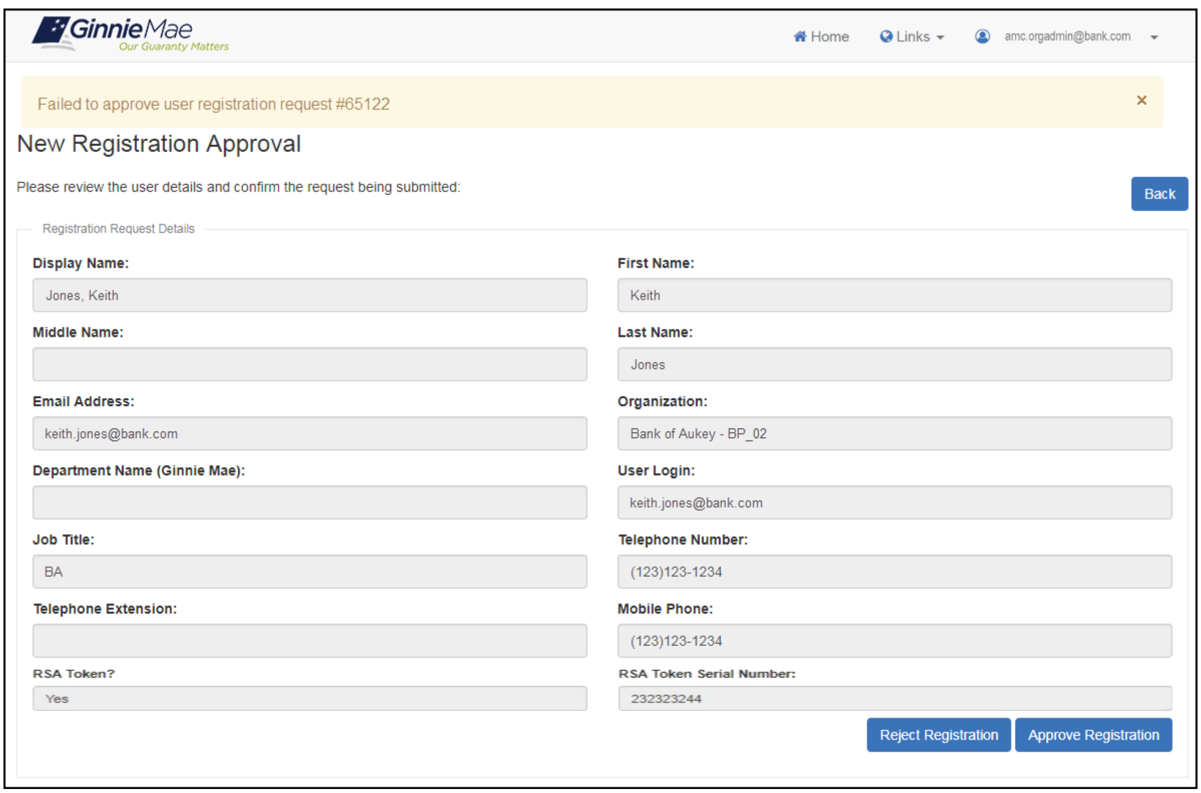


Figure 100 - Failed User Registration Approval

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

4.4.3 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.

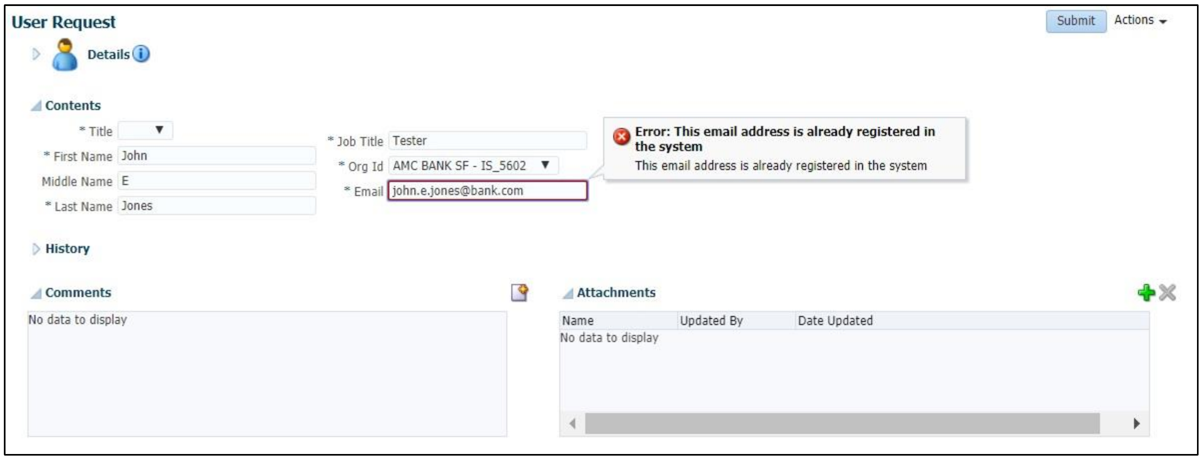


Figure 101 - Email is Already Registered Error

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

4.4.4 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.

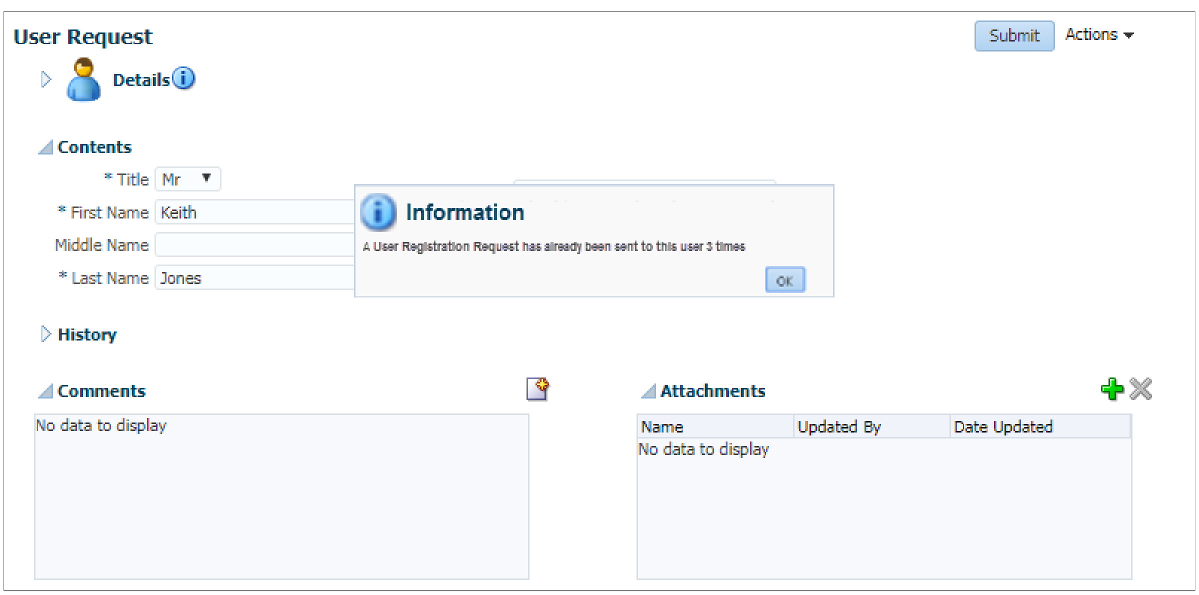


Figure 102 - Three Invitations Sent Alert

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

4.4.5 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.

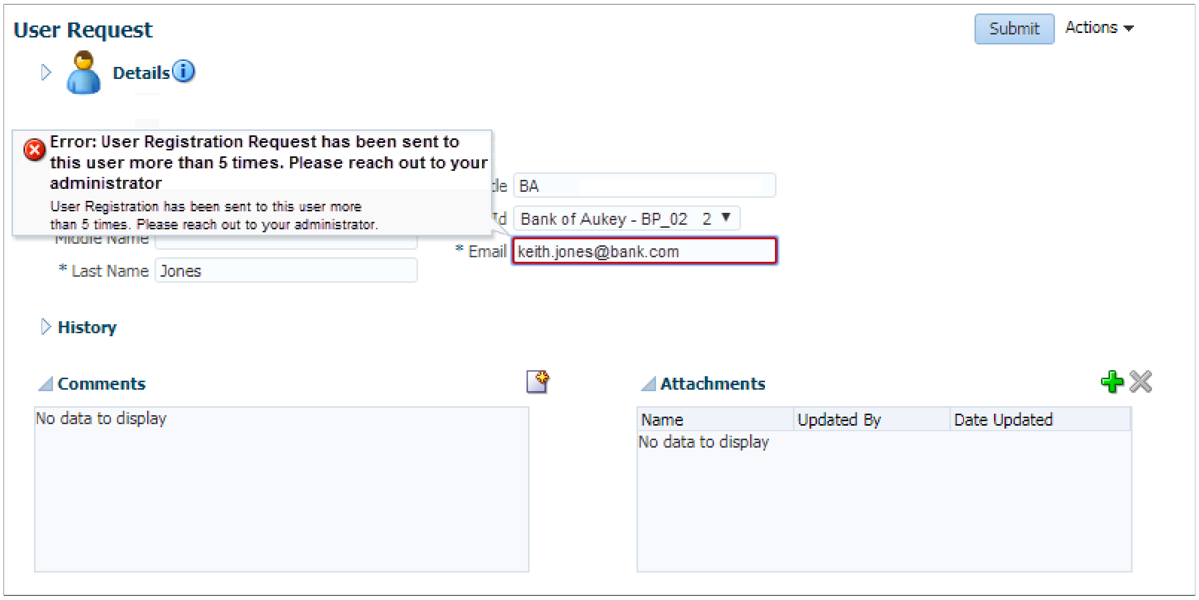


Figure 103 - Five Time Invitation Flag

Resolution: In order to send another invitation to the user's email address, action is required from the Operations Administrator group. See Section **Error! Reference source not found.**: Help Desk.

4.4.6 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.

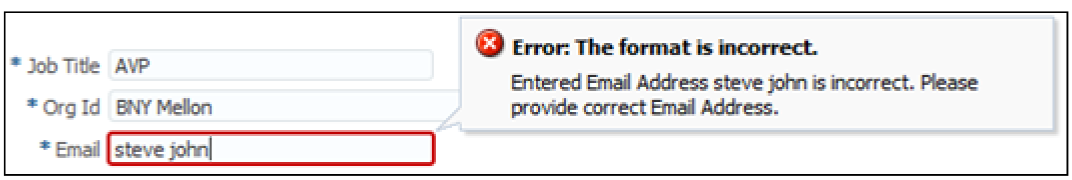


Figure 104 – Registration Email Form Error

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.

Figure 105 – Registration Email Form Error

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.

4.4.7 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, "New passwords entered do not match."

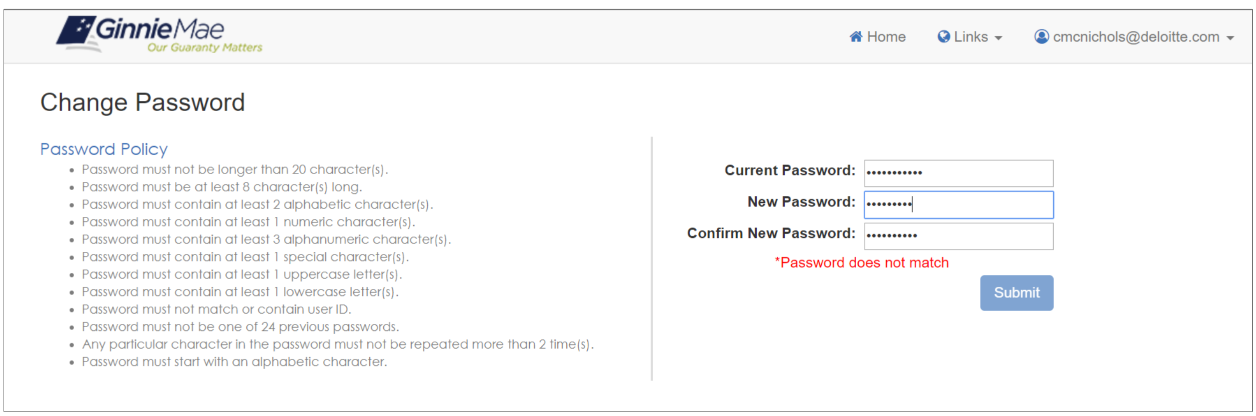


Figure 106 - New Password Does Not Match Error

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

5 REPORTING

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

5.1 Accessing Administrative Reports

5.1.1 Report Types

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

Service	Reports	Type
User Registration	Home Organization User List Org Admin View User Profile History User Registration Request History	Custom Standard Custom
Access Requests	AMC Functional Role Request History	Custom
Multifactor Authentication (MFA)	Accounts Locked Out Report Authentication Statistics Report	Standard Standard
Self-Service Change Password	Password Expiration Summary	Standard

Table 1 - Reporting for Organization Administrators

5.1.2 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**

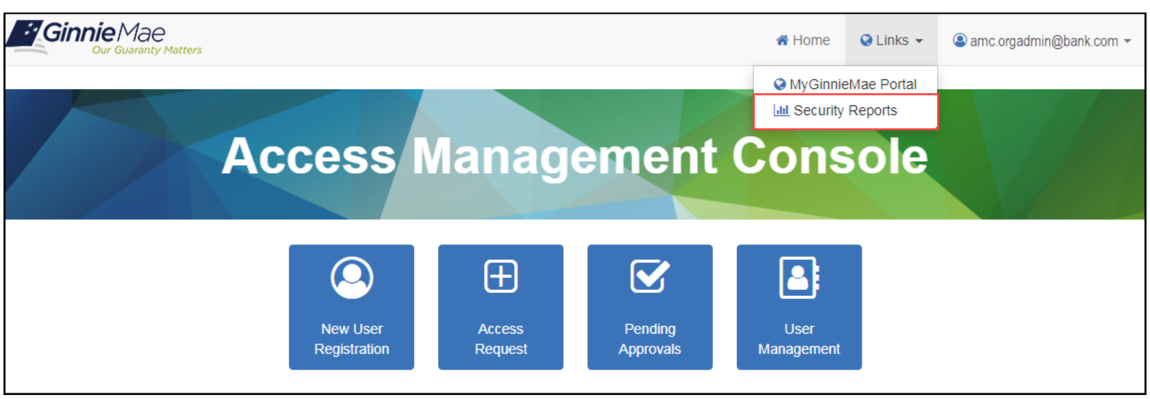


Figure 107 - Security Reports Link

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.

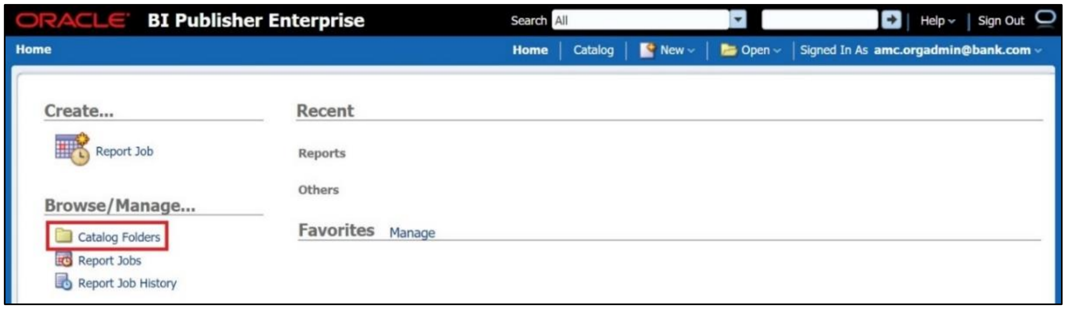


Figure 108 - Report Catalog Folders

5) Select **Shared Folders** to expand the folder.

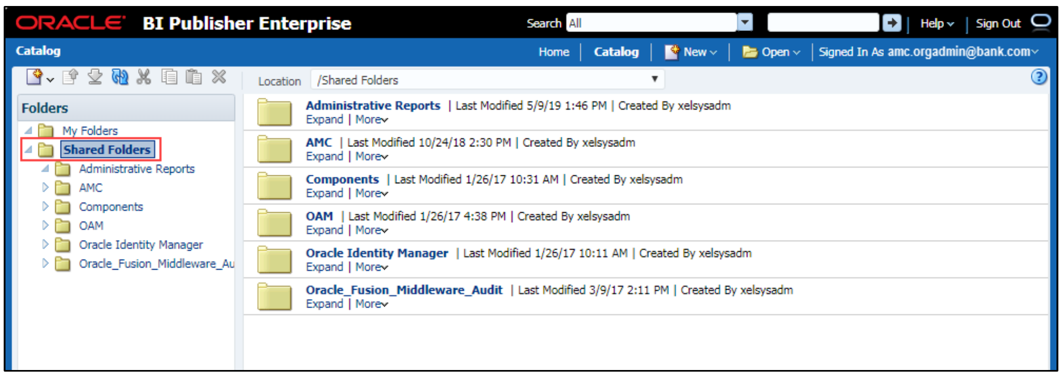


Figure 109 - Oracle Identity Manager Reports

6) Select **Administrative Reports** folder.

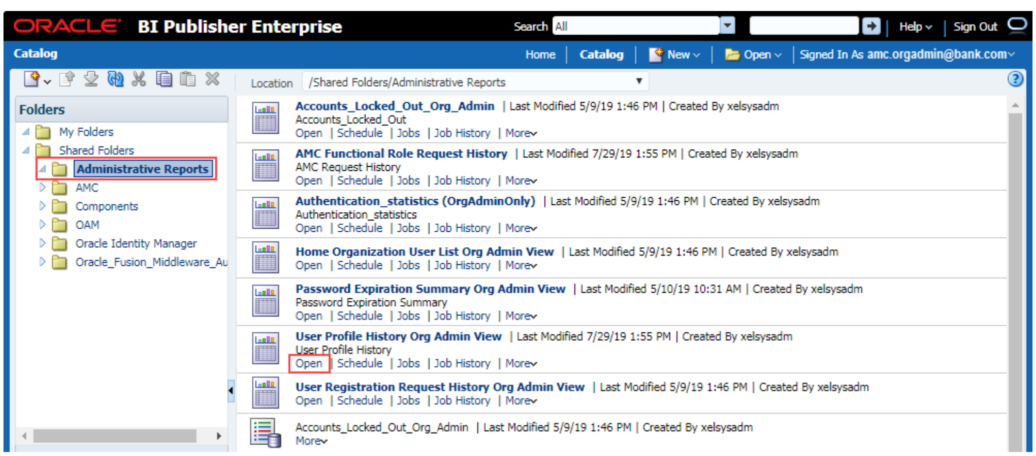


Figure 110 - Open User Profile History Report

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.

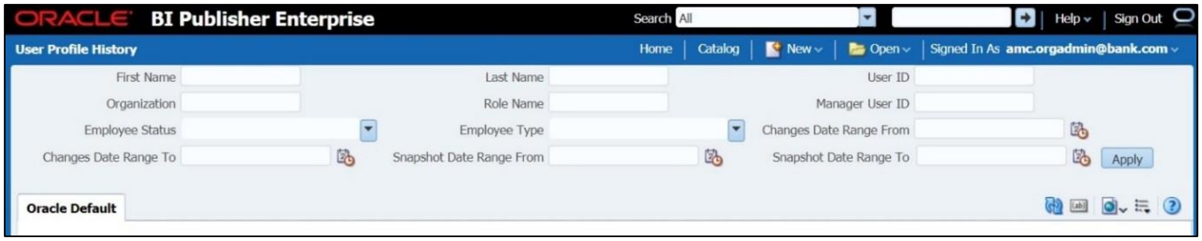


Figure 111 - Search Profile History

NOTE: Data will not be displayed if the date range filter is not used in conjunction with other filters.

6 GETTING HELP

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

Refer to MyGinnieMae Portal Getting Started Manual

6.1 MyGinnieMae Portal Dictionary

The MyGinnieMae Portal Dictionary is a reference resource for End Users, Organization Administrators and Operations Administrators. The dictionary contains definitions for terms that provide clarification around portal pages, applications, processes and general functionality pertaining to the MyGinnieMae portal.

Refer to MyGinnieMae Portal Dictionary **(This reference will be updated with a hyperlink to the Portal Dictionary stored on Ginnie Mae's website.)**

7 Quick Reference Cards

Section being held for AMC QRCs