



MyGinnieMae Organization Administrator Guide

MyGinnieMae (Ginnie Mae Enterprise Portal 2.0)

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

October 2018

Solution Information

	Information
Solution Name	MyGinnieMae
Solution Acronym	MyGinnieMae
Project Cost Accounting System (PCAS) Identifier	N/A
Document Owner	BNYM
Primary Segment Sponsor	Office of Securities Operations (OSO)
Version/Release Number	1.7

Document History

Version	Date	Author	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



Table of Contents

1	Solution Summary.....	1
1.1	Features.....	2
1.2	Organization Administrators Functionality	2
1.2.1	Prerequisites	2
1.2.2	Access Management Console	3
1.2.3	Onboarding Workflow	4
1.2.4	Functional Roles	5
2	Logging On and Off	10
2.1	Logging on to MyGinnieMae	10
2.2	Navigating to the Access Management Console	13
2.3	One-Time Password	14
2.4	Exiting the Solution	15
2.4.1	Exiting MyGinnieMae	16
2.4.2	Exiting the Access Management Console and Exiting MyGinnieMae	16
2.4.3	Exiting the Access Management Console and Returning to MyGinnieMae	17
3	Onboarding and Managing End User Accounts.....	17
3.1	Send an Invitation to Register	18
3.2	Approve a New User Registration.....	22
3.3	Request Functional Role.....	26
3.4	Approve an Access Request.....	31
3.5	Remove Functional Roles from a User	34
3.6	Disable a User Account.....	38
3.7	Enable a User's Account	42
3.8	Lock a User's Account	45
3.9	Unlock a User's Account.....	48
3.10	Update a User's Profile Attributes	50
3.11	Reset a User's Password.....	52
3.12	Reject a New User Registration	54
3.13	Reject a Functional Role	57
3.14	Review the Status of an Access Request	59
3.15	Verify an Assigned Functional Role.....	60



Organization Administrator Manual

4	Troubleshooting and System Errors.....	63
4.1	AMC Error Page.....	63
4.2	AMC Module Error Notification Ribbons.....	64
4.3	User Registration Invitation Errors	65
4.3.1	Email is Already Registered.....	66
4.3.2	Three Invitations Sent Alert	67
4.3.3	Five Time Invitation Flag.....	68
4.4	New Password Mismatch Error	69
4.5	Invalid Username or Password	70
4.6	Incorrect OTP.....	70
4.7	OTP Not Received	71
4.8	Disable Pop-Up Blocker	71
5	Reporting	73
5.1	Report Capabilities	73
5.2	Report Procedures	73
6	Getting Help.....	77
6.1	Getting More Help	77
6.2	Help Desk.....	77
	Appendix A: Key Features	79
	Appendix B: Reference Documents.....	80
	Appendix C: Glossary and Key Terms	81



1 Solution Summary

The purpose of this document is to familiarize Organization Administrators with MyGinnieMae functionality relevant to their role. Organization Administrators are persons who would have previously performed the Security Officer role in GMEP 1.0 or the Enrollment Administrator role in GinnieNET. Since an Organization Administrator is also a user of MyGinnieMae, refer to the MyGinnieMae End User Handbook for functionality common to all users of the application.

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.

Ginnie Mae is in the midst of 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 GMEP 1.0 and serve as a primary platform for extending information technology (IT) capabilities to the Ginnie Mae community. MyGinnieMae delivers security features which Ginnie Mae established to specifically address business constraints, security concerns, and compliance issues that hinder GMEP 1.0 today. Currently MyGinnieMae allows a secure entrance for users into many Ginnie Mae business applications.

MyGinnieMae was created to provide 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.

MyGinnieMae 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 GinnieNET.

The platform enables secure access to integrated applications and provides a framework to address the challenges listed above. Among the benefits provided to Ginnie Mae stakeholders are:

- Improve cyber security operations by reducing the 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.
- Reduce IT operational expenses by fully automating new user registration process and enabling user self-service capabilities like password reset, application access requests, and delegated account administration.



- Improve IT governance and compliance capabilities such as automated role management, Segregation of Duties (SoD) monitoring, and centralized audit reports.

1.1 Features

MyGinnieMae provides the following security and business features:

- **MyGinnieMae Access Management Console (AMC):** Provides a user friendly interface for administrators to initiate access requests, manage end users within their organization(s), and perform additional administrative functions when following the workflow(s) provided in the guide.
- **Application Access Controls:** Utilizes Functional Roles to enforce Portal access security for all users and systems. MyGinnieMae provides a means to associate authenticated system users with applicable rights and privileges within the Portal and associated application programs.
- **Web Based Self-Service Interface:** Provides self-service password management capabilities through a standard web-based interface.
- **Audit Support:** Provides relevant reports and email notifications for Ginnie Mae business users to enable transparency across the organization. For Organization Administrators, MyGinnieMae provides reports reflecting user access, workflow request/approval details, and account status.
- **Invitation Model:** Automates the user registration process through an invitation model. Registration must be completed before being granted access to the system.
- **Portal Capabilities:** Central access point to all Ginnie Mae business applications including Single Sign-On (SSO) to GMEP1.0 and GinnieNET. Includes communications via the Marquee, Event Calendar, and messaging from Ginnie Mae Account Executives, instructional materials, and notes and tasks/lists feature for capturing action items and/or reminders for Ginnie Mae business activities.
- **Multifactor Authentication via One-Time Password (OTP):** Provides an additional level security for access to Ginnie Mae business applications through a single use password received via email.

Please refer to [Appendix A – Key Features](#) for more detailed feature descriptions.

1.2 Organization Administrators Functionality

1.2.1 Prerequisites

The Organization Administrator must be an authorized signer listed on the relevant Form HUD-11702 on the [MBS Guide: Forms website](#). In order to set up an Organization Administrator account in MyGinnieMae, the Operations Administrator team must initiate the registration process and assign the proper roles to the new Organization Administrator. Each unique Organization must have at least two Organization Administrators.



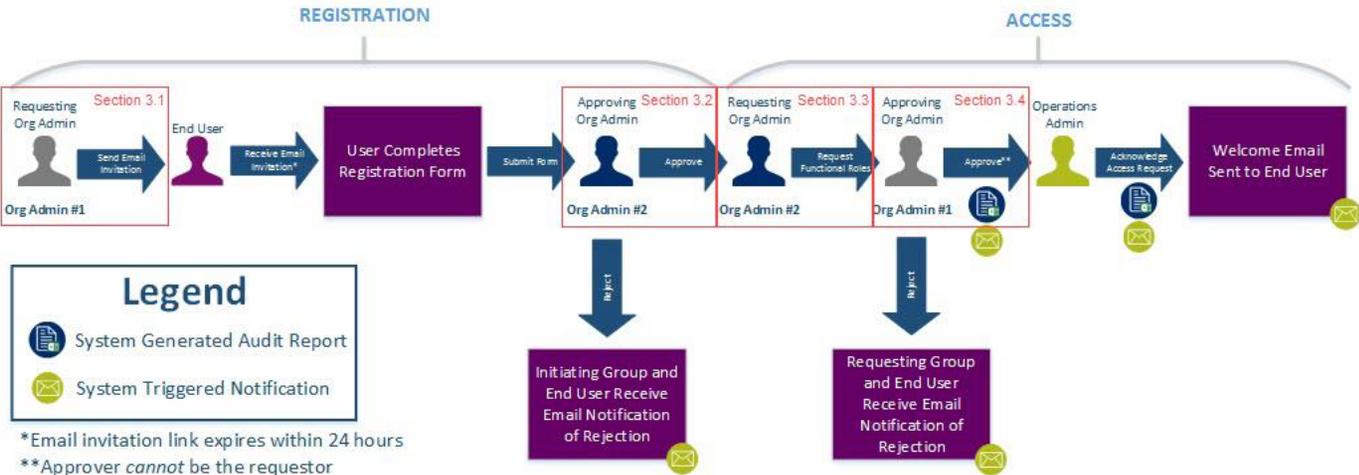
1.2.2 Access Management Console

The MyGinnieMae Access Management Console (AMC) provides the ability to register new MyGinnieMae users, grant access to modernized business applications (e.g. Multifamily Pool Delivery Module (MFPDM)), grant access to legacy business applications (GMEP 1.0 and GinnieNET), and 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 approve user registration, initiate access requests, and manage user information within the permitted organization, as well as perform additional responsibilities as identified by Ginnie Mae. As an added level of security, to complete registration and access approvals, two Organization Administrators are required since there is a separation of duties between an administrator that submits a request and administrators that can approve a request.



1.2.3 Onboarding Workflow



NOTE: Org Admins are expected to know the access and end user needs.

Figure 1 – MyGinnieMae Access Workflow



The following table lists the various administrative user types and the responsibility/description for each user type within MyGinnieMae. Each organization must maintain at least two Organization Administrators.

Table 1 - MyGinnieMae Responsibilities

User Type	Responsibility / Description
Operations Administrator (Ops Admin)	Operations Administrators have general oversight of the Portal. They can only provide final acknowledgement of access requests and cannot make any changes to end user accounts. Refer to Section 6.2: Help Desk for Operations Administrators.
Organization Administrator (Org Admin)	Organization Administrators have the privilege to invite end users to register for a Portal account, approve user registration, initiate access request via Functional Role assignments to users, and approve the access request within a single organization. Note: Separation of duties within the registration and access request workflows does not allow the Organization Administrator to initiate a registration and approve that same registration, or request access via Functional Role assignment and approve that same access request. A minimum of two Organization Administrators are required. It is recommended to have more than the minimum from an operational perspective.
End User	End Users are the various types of Ginnie Mae employees, business partners, and contractors who require access to the business applications and information within the Portal, including various self-service functions.

1.2.4 Functional Roles

In MyGinnieMae, users are provided access based on their business activities which are organized into meaningful access profiles called Functional Roles. Use of Functional Roles ensures users have appropriate level of access in relation to their job functions/responsibilities, enforces the least privilege principle, and makes the account provisioning/de-provisioning actions easier for Organization Administrators. These roles are grouped and vary by type (Single Family, Multi-Family, HECM, etc.) as summarized in the Functional Roles tables below. For more detail, please refer to [Appendix B: Reference Documents](#).



Table 2 – Single Family Functional Roles

Functional Role Name	Functional Role Description
SF-Post-Closing User	Access to review collateral, obtain loan insurance, forward initial and trailing documents to a Document Custodian.
SF-Loan Delivery and Pooling Basic User	Upload/enter pool and loan information for delivery; verify availability of commitment authority; clear document deficiencies and pooling exceptions; access to prepare but not execute PIIT/TAI transactions.
SF-Loan Delivery and Pooling Authorized Signer	Only for HUD 11702 signatories. All rights of a Loan Delivery and Pooling Basic User, plus authority to submit pools for issuance and request additional commitment authority and execute PIIT/TAI transactions.
SF -Investor Reporting Basic User	Submit monthly pool and loan level accounting data; submit quarterly custodial account verification data; review monthly remittance information; review monthly reporting exception feedback and errors.
ISF-Investor Reporting Authorized Signer	Only for HUD 11702 signatories. All rights of an Investor Reporting Basic User, plus authority to certify the monthly pool and loan accounting report and submit edits needed to clear exception feedback and monthly reporting errors.
SF-Compliance and Oversight User	Review portfolio servicing and investor reporting metrics and reports; oversee subservicer performance when applicable.
SF-Bulk Transfers Authorized Signer	Initiate, manage, and accept bulk transfer transactions; initiate and coordinate transfers of collateral files with transferee and transferor Issuers or Document Custodians.
SF-Collateral Management Authorized Signer	Process releases of collateral from the Document Custodian in accordance with servicing obligations (HUD-11708 Releases).
SF-Agency Relationship User	Access reports containing portfolio performance and liquidity metrics; receive targeted Ginnie Mae communications for individual responsible for managing agency relationships.
SF-Processing Master Agreements Authorized Signer	Only for HUD 11702 signatories. Edit, submit, and certify Master Agreement documents and data required by Ginnie Mae.
SF-Financial Statements User	Submit annual audited financial statements for review by Ginnie Mae's IPA.
SF-Special Loans User	Upload and process SCRA reimbursement requests.



Table 3 – Multi-Family Functional Roles

Functional Role Name	Functional Role Description
MF-Loan Delivery and Pooling Basic User	Upload/enter pool and loan information for delivery; verify availability of commitment authority; clear document deficiencies and pooling exceptions; access to prepare but not execute PIIT/TAI transactions.
MF-Loan Delivery and Pooling Authorized Signer	Only for HUD 11702 signatories. All rights of a Loan Delivery and Pooling Basic User, plus authority to submit pools for issuance and request additional commitment authority and execute PIIT/TAI transactions
MF-Investor Reporting Basic User	Submit monthly pool and loan level accounting data; submit quarterly custodial account verification data; review monthly remittance information, review monthly reporting exception feedback and errors.
MF-Investor Reporting Authorized Signer	Only for HUD 11702 signatories. All rights of an Investor Reporting Basic User, plus authority to certify the monthly pool and loan accounting report and submit edits needed to clear exception feedback and monthly reporting errors.
MF-Compliance and Oversight User	Review portfolio servicing and investor reporting metrics and reports; oversee subservicer performance when applicable.
MF-Master Agreements Authorized Signer	Only for HUD 11702 signatories. Edit, submit, and certify Master Agreement documents and data required by Ginnie Mae
MF-Financial Statements User	Submit annual audited financial statements for review by Ginnie Mae's IPA.
MF-Transfers Authorized Signer	Initiate, manage and accept bulk transfer transactions; Initiate and coordinate transfers of collateral files with transferee and transferor Issuers or Document Custodians.

Table 4 – HECM Functional Roles

Functional Role Name	Functional Role Description
HECM-Post-Closing User	Access to review collateral, obtain loan insurance, forward initial and trailing documents to a Document Custodian.
HECM-Loan Delivery and Pooling Basic User	Upload/enter pool, loan and participation data into GinnieNET; verify available commitment authority and clear document and/or GinnieNET pooling exceptions. Basic user cannot finalize transactions or submissions.



Functional Role Name	Functional Role Description
HECM-Loan Delivery and Authorized Signer	Upload/enter pool, loan and participation data into GinnieNET; verify available commitment authority and clear document and/or GinnieNET pooling exceptions. Authority to finalize or execute business transactions with Ginnie Mae (HUD-11702 Signers), including the authority submit requests for additional commitment authority as needed and to submit pools for issuance.
HECM-Investor Reporting Basic User	Submit the monthly pool, loan and participation data; submit the custodial account verification data; review monthly remittance information and reporting exception feedback and errors. Ability to track loans approaching 98% of MCA (Maximum Claim Amount) to identify if loans need to be bought out and coordinate participation agent for assurance that all participations in other pools are bought out accordingly.
HECM-Investor Reporting Authorized Signer	Submit the monthly pool, loan and participation data; submit the custodial account verification data; review monthly remittance information and reporting exception feedback and errors. Ability to track loans approaching 98% of MCA (Maximum Claim Amount) to identify if loans need to be bought out and coordinate participation agent for assurance that all participations in other pools are bought out accordingly. Including the authority submit requests for additional commitment authority as needed and to submit pools for issuance.
HECM-Compliance and Oversight User	Review portfolio servicing and investor reporting metrics and reports; oversee subservicer performance when applicable.
HECM-Bulk Transfers Authorized Signer	Initiate, manage and accept bulk transfer transactions; initiate and coordinate transfers of collateral files with transferee and transferor Issuers or Document Custodians.
HECM-Collateral Management Authorized Signer	Process releases of collateral from the Document Custodian in accordance with servicing obligations (HUD-11708 Releases).
HECM-Agency Relationship User	Access reports containing portfolio performance and liquidity metrics; receive targeted Ginnie Mae communications for individual responsible for managing agency relationships.
HECM-Processing Master Agreements Authorized Signer	Only for HUD 11702 signatories. Edit, submit, and certify Master Agreement documents and data required by Ginnie Mae.
HECM-Financial Statements User	Submit annual audited financial statements for review by Ginnie Mae's IPA.
HECM-Special Loans User	Upload and process SCRA reimbursement requests.



Functional Role Name	Functional Role Description
HECM-Participation Agent	Third Party participation agent and who perform all monitoring and accounting activities related to pooled Participations on behalf of a HECM Issuer.

Table 5 – Subservicer Functional Roles

Functional Role Name	Functional Role Description
SS-Investor Reporting Basic User	Submit monthly pool and loan level accounting data; submit quarterly custodial account verification data; review monthly remittance information, review monthly reporting exception feedback and errors
SS-Investor Reporting Authorized Signer	Only for HUD 11702 signatories. All rights of an Investor Reporting Basic User, plus authority to certify the monthly pool and loan accounting report and submit edits needed to clear exception feedback and monthly reporting errors.
SS-Compliance and Oversight User	Review portfolio servicing and investor reporting metrics and reports; oversee subservicer performance when applicable.
SS-Special Loans User	Upload and process SCRA reimbursement requests.

Table 6 – Document Custodian Functional Roles

Functional Role Name	Functional Role Description
DC-Pool Certification Basic User	View Schedule of Pooled Mortgages submitted; review pool and loan files for compliance with Ginnie Mae pool certification standards. Cannot certify pools or loan packages.
DC-Pool Certification and Collateral Release Management Authorized Signer	Only for HUD 11702 Signatories. All the rights of a Pool Certification Basic User, plus authority to submit initial certification, final certification and recertification; authority to process releases of pool and/or loan files electronically via Ginnie Mae systems.
DC-Management and Oversight	Oversee document review and pool certification procedures; access and submit the Master Agreement documents and data as required by Ginnie Mae; serve as an Organization Administrator for My Ginnie Mae.
DC-Transfer Specialist	Monitor and manage pool transfer activities to ensure successful relocation of collateral files.



2 Logging On and Off

The following sections detail common actions taken by Organization Administrators to access MyGinnieMae, including AMC and One-Time Password. **Note:** It is important that the browser's pop-up blocker is disabled prior to accessing MyGinnieMae. See [Section 4.8 - Disable Pop-Up Blocker](#) for the steps to do this.

2.1 Logging on to MyGinnieMae

1. Navigate to the Public Landing Page at <https://my.ginniemae.gov> and select "Login". **Note:** It is recommended to bookmark this page.

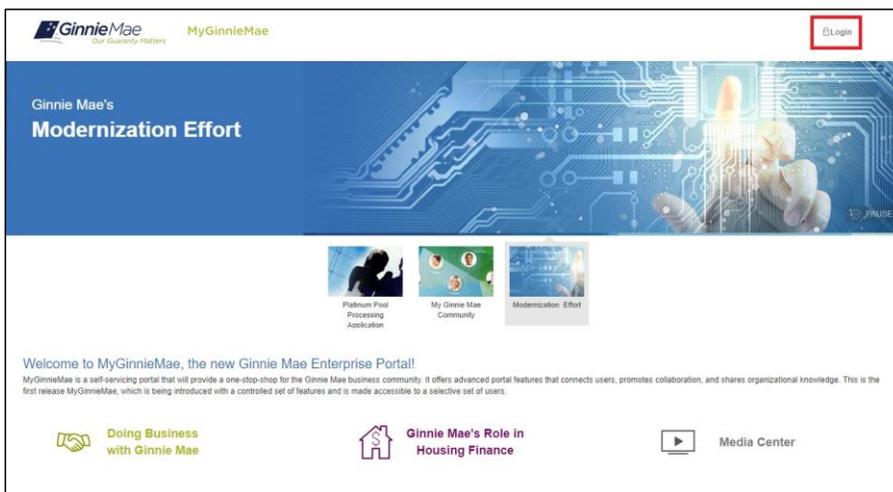


Figure 2 - Public Landing Page



2. On the Login Page, enter a valid user name and password and select "Login". **Note:** Do not bookmark the Login Page. The correct page to bookmark is the Public Landing Page at <https://my.ginniemae.gov>. Bookmarking any other page will cause navigation issues.

Government Security Disclosure

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following:

1. You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search and seize any communication or data transiting or stored on this information system.
2. Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.
3. Your consent is final and irrevocable. You may not rely on any statements or informal policies purporting to provide you with any expectation of privacy regarding communications on this system, whether oral or written, by your supervisor or any other official, except HUD or Ginnie Mae's Chief Information Officer.

[Forgot Password?](#)

Figure 3 - Login Page



3. Based on the assigned Functional Role, the system will redirect to a MyGinnieMae Landing Page.

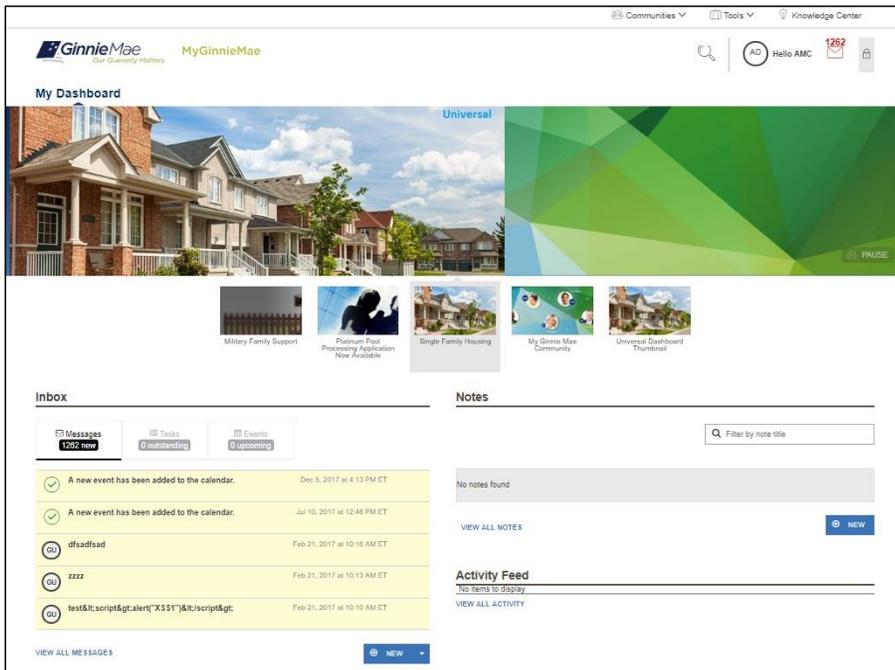


Figure 4 - MyGinnieMae Landing Page (My Dashboard – Issuer View)



2.2 Navigating to the Access Management Console

The Access Management Console (AMC) is the user interface used by Organization Administrators to manage Portal user accounts for their organization. Refer to [Section 2.1: Logging on to MyGinnieMae](#) to access the Access Management Console and then follow these steps:

1. From any Portal page, select the “Tools” drop-down at the top and select “Access Management Console”.

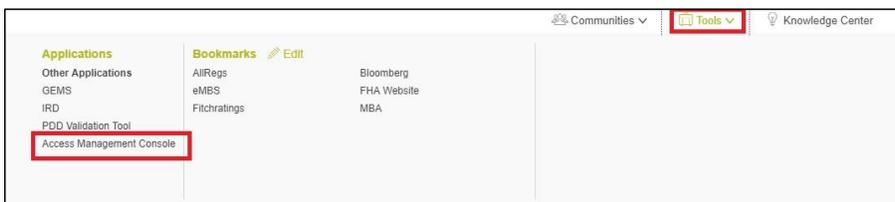


Figure 5 – Tools Drop-Down Menu

2. Select “Yes” when prompted to open the AMC within the current Portal window.

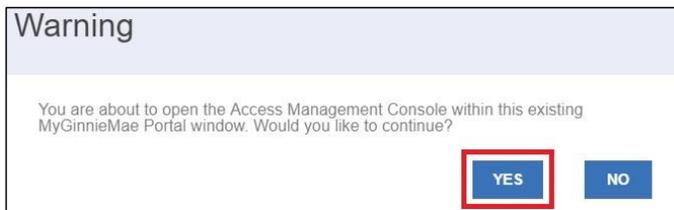


Figure 6 – Portal Warning



3. Complete the steps for the One-Time Password (OTP) in [Section 2.3: One-Time Password](#). The system will open the AMC in a new window.



Figure 7 – AMC Landing Page – Organization Administrator

Note: The Portal does not recognize activity in the AMC as Portal activity. If the Organization Administrator is active within the AMC for longer than 20 minutes, the system will prompt the user to re-enter their credentials when navigating back to the Portal (See [Section 2.4.3: Exiting the Access Management Console and Returning to MyGinnieMae](#)).

2.3 One-Time Password

When accessing secured applications and information in the Portal, a One-Time Password (OTP) provides an added level of security to protect the information. This is an eight-digit code which is valid for 10 minutes and sent to the user’s email address. The OTP is only required if the user has not entered an OTP in the previous 120 minutes.



Figure 8 – Sending OTP Message

1. After selecting a secured application in the portal, navigate to the user’s corporate email inbox to retrieve the OTP. In some cases the email may be redirected to Junk or other filtered folders.
2. Return to the page displaying the Secure Image and Phrase to enter the OTP in the “Password” field then select “Enter”.



Note: If the user does not receive an OTP, select “Did not Receive OTP?” at the bottom of the page to initiate a resend. If OTP is still not received, confirm that pop-ups have been disabled using the instructions in [Section 4.8: Disable Pop-Up Blocker](#).



Figure 9 – One-Time Password Email and Secure Image & Phrase

2.4 Exiting the Solution

The following sections provide instructions to log out and end a session in MyGinnieMae or Access Management Console. Users may exit the solution in a variety of ways:

- End the Portal session without affecting the AMC session
- Simultaneously end both the AMC and Portal session
- End the AMC session and return to the Portal



2.4.1 Exiting MyGinnieMae

1. To exit MyGinnieMae at any point, select the “Lock” icon at the top right of the page.



Figure 10 - Logout Lock Icon

2. Select “Log Out”.



Figure 11 - Portal Logout

2.4.2 Exiting the Access Management Console and Exiting MyGinnieMae

1. To exit the Access Management Console and thereby close the Portal session and any open windows and applications, select the drop-down arrow beside the username in the top right corner of the page.



2. Select “Sign out”.



Figure 12 - 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 2.1: Logging on to MyGinnieMae](#).

2.4.3 Exiting the Access Management Console and Returning to MyGinnieMae

1. To exit the Access Management Console and navigate back to the Portal, select the “MyGinnieMae Portal” link on the toolbar at the top of the screen.



Figure 13 - Return to MyGinnieMae Portal

3 Onboarding and Managing End User Accounts

The following sections detail common actions taken by Organization Administrators to onboard new users, request access, and manage existing user accounts. The complete Onboarding Workflow ([Figure 1 – MyGinnieMae Access Workflow](#)) automates the user account registration and access request provisioning processes and provides an audit history of user access.



MyGinnieMae User Registration uses a self-service registration form to collect information from potential end users. This verified and used to create a new user account in MyGinnieMae. User registration provides a single identity, enabling users to access MyGinnieMae and the business applications that reside within the Portal using a corporate email address.

MyGinnieMae Access Provisioning employs a model that assigns system access based on the user's business function within their organization. Access Provisioning is completed using an automated workflow that guides Organization Administrators through assigning each user the proper Functional Role(s) for the corresponding organization(s).

Security controls have been built into the Portal. As explained in [Onboarding Workflow](#), a minimum of two Organization Administrators are required to participate in the onboarding of an end user. The administrator that provides an approval cannot be the same administrator that initiated the request. Additionally, an Organization Administrator may not participate in initiating a request or providing an approval for their own account. Other controls affecting user registration include that each invitation email is valid for 24 hours and will expire if the end user does not submit the registration information. The system will limit the total number of invitations sent to an end user to five. If an additional invitation must be sent after five unsuccessful invitations, refer to [Section 6.2: Help Desk](#).

The following conditions must be met for user onboarding to be completed successfully:

- A minimum of two Organization Administrators with active Portal accounts are required before sending an end user a registration invitation
- An Organization Administrator cannot participate in their own registration and access request nor can they manage their own user account
- The end user must submit the completed User Access Form within 24 hours of the invitation being sent
- The invitation cannot be sent to the end user more than five times
- The end user must be employed by an organization which has been onboarded and authorized to do business with Ginnie Mae
- The Home Organization approves of the employee being granted access to Ginnie Mae systems
- The Home Organization approves the level of access requested for the user

Commented [CRH1]:

Commented [CRH2]:

Commented [CRH3]: Is this supposed to be end user must complete the registration invitation within 24 hours. User Access Form is what the Org Admin sees/completes to initiate the invitation.

Commented [CRH4]:

Commented [CRH5]:

3.1 Send an Invitation to Register

The User Registration workflow is a self-service process used to create a new user account in MyGinnieMae. An Organization Administrator initiates the workflow via an invitation sent to the end user within their organization as follows:

1. Log into the Portal and navigate to the Access Management Console.



2. Select the “New User Registration” tile.



Figure 14 - Access Management Console Landing Page

3. The system opens the New User Registration interface in a new window.

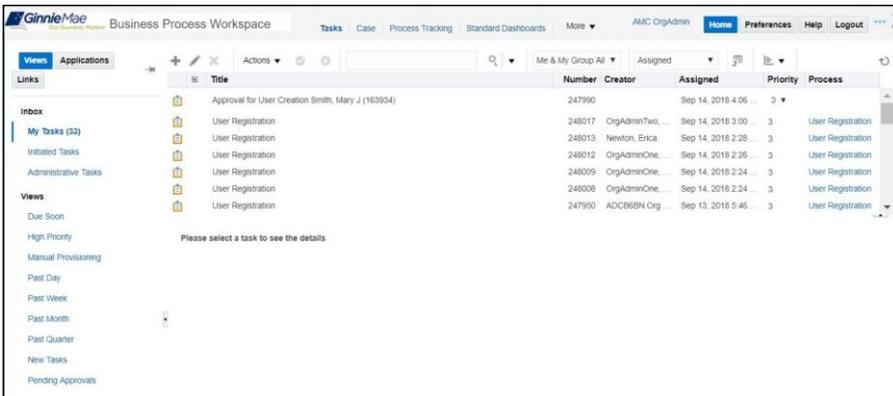


Figure 15 – New User Registration Interface



4. Select “Applications” from the left and select “User Registration” to open the User Invitation form in a new window.

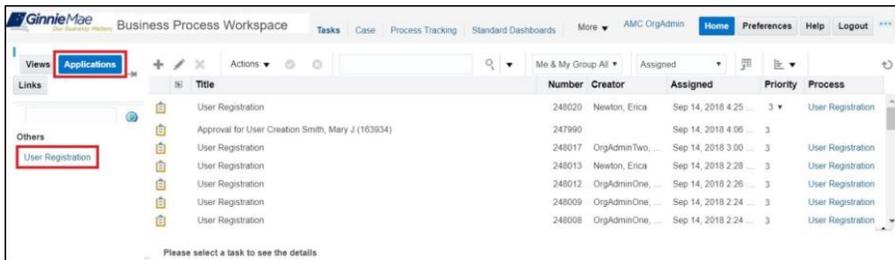


Figure 16 – New User Registration Interface – Open User Invitation Form

Note: Organization Administrators need to disable the pop-up blockers for this site in order to open the User Request form. See [Section 4.8: Disable Pop-Up Blocker](#).

5. Complete the following fields in the user request form and select “Submit”.
 - 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 (limited to the organizations that the Admin has the Organization Administrator role)
 - Email (only register using lower case characters; not mixed or upper case). The email domain is validated against a whitelist of valid domains based on organizations Ginnie Mae works with. If domain changes are needed for an organization see [Section 6.2: Help Desk](#).

Commented [CRH6]: Suggest language revision for more clarity. Option could be - Limited to the organization (s) which the Organization Administrator User has been assigned the privileged role to perform user access and management functions



User Request Submit Actions

Details

Contents

* Title: Mr
* Job Title: Tester
* First Name: John
* Org Id: AMC BANK SF - IS_5602
Middle Name: E
* Email: john.e.jones@bank.com
* Last Name: Jones

History

Comments
No data to display

Attachments
No data to display

Figure 17 - User 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.

- After submission, the User Invitation Form closes automatically. An email is sent to the email address entered in the form with a unique URL that is valid for 24 hours for the End User to complete their registration.

Title	Number	Creator	Assigned	Priority	Process
Approval for User Creation Smith, Mary J (163934)	247990		Sep 14, 2018 4:05	3	
User Registration	248017	OrgAdminTwo, ...	Sep 14, 2018 3:00	3	User Registration
User Registration	248013	Newton, Erica	Sep 14, 2018 2:28	3	User Registration
User Registration	248012	OrgAdminOne, ...	Sep 14, 2018 2:26	3	User Registration
User Registration	248009	OrgAdminOne, ...	Sep 14, 2018 2:24	3	User Registration
User Registration	248008	OrgAdminOne, ...	Sep 14, 2018 2:24	3	User Registration
User Registration	247960	ADCB6BN Org, ...	Sep 13, 2018 5:46	3	User Registration

Figure 18 – New User Registration Interface

- If additional invitations need to be sent, repeat steps 4-6. If not, close the New User Registration interface. After the end user completes registration, a second Organization Administrator reviews and approves the request (see [Section 3.2: Approve a New User Registration](#)).



3.2 Approve a New User Registration

Once an end user has completed and submitted the User Registration Form, all Organization Administrators, except the one that 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 19 - User Registration Approval Request Notification Email

Note: Selecting the hyperlink in the email notification will navigate directly to the AMC Login Page.

1. Log into the Portal and navigate to the Access Management Console and select the “Pending Approvals” tile.



2. 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 20 - Access Management Console Landing Page

3. Review the table under “User Registration Approval” accordion (collapsible section) which displays the list of available registration requests to approve.

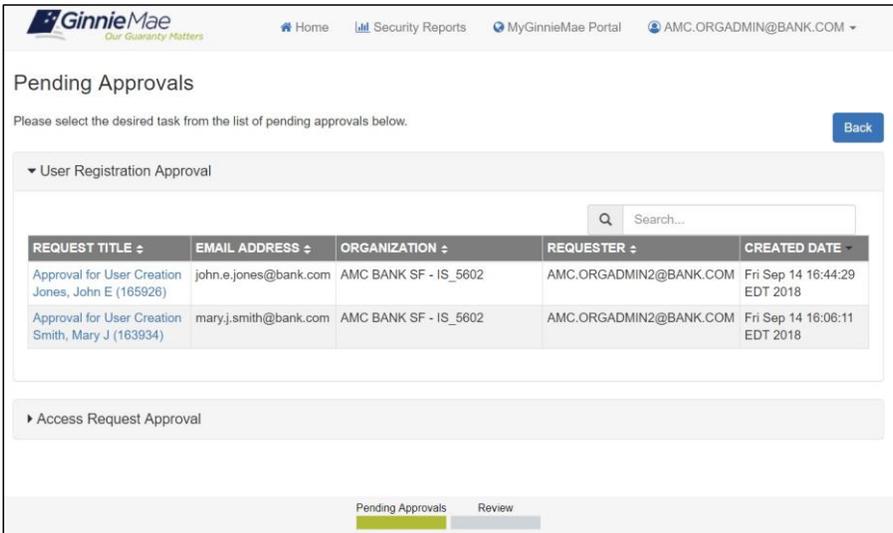


Figure 21 – Pending Approvals – User Registration Approval



4. Select the “Request Title” hyperlink of the desired End User to begin the approval of their registration request.

The screenshot shows the GinnieMae 'Pending Approvals' page. At the top, there are navigation links for Home, Security Reports, MyGinnieMae Portal, and AMC.ORGADMIN@BANK.COM. Below the navigation is a 'Pending Approvals' section with a 'Back' button. A dropdown menu is set to 'User Registration Approval'. A search bar is present above a table of pending approvals. The table has columns for REQUEST TITLE, EMAIL ADDRESS, ORGANIZATION, REQUESTER, and CREATED DATE. The first row is highlighted with a red box, showing 'Approval for User Creation Jones, John E (165926)'. Below the table is an 'Access Request Approval' section. At the bottom, there are two tabs: 'Pending Approvals' (active) and 'Review'.

REQUEST TITLE	EMAIL ADDRESS	ORGANIZATION	REQUESTER	CREATED DATE
Approval for User Creation Jones, John E (165926)	john.e.jones@bank.com	AMC BANK SF - IS_5602	AMC.ORGADMIN2@BANK.COM	Fri Sep 14 16:44:29 EDT 2018
Approval for User Creation Smith, Mary J (163934)	mary.j.smith@bank.com	AMC BANK SF - IS_5602	AMC.ORGADMIN2@BANK.COM	Fri Sep 14 16:06:11 EDT 2018

Figure 22 - 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 [Section 3.12: Reject a New User Registration](#).

5. Review the user approval details and select the “Approve Registration” button from the bottom right of the page.

Note: User Registration fields are not editable. If there are any errors or incorrect information in the request, follow the steps to reject the request in [Section 3.12: Reject a New User Registration](#). Afterward, work with the Organization Administrator Group and the affected End User to submit a new registration beginning with the steps in [Section 3.1: Send an Invitation to Register](#).



New Registration Approval

Please review the user details and confirm the request being submitted: Back

Registration Request Details

Display Name: Jones, John E	First Name: John
Middle Name: E	Last Name: Jones
Email Address: john.e.jones@bank.com	Organization: AMC BANK SF - IS_5602
Department Name (Ginnie Mae):	User Login: john.e.jones@bank.com
Job Title: Tester	Telephone Number: (757)777-3333
Telephone Extension:	Mobile Phone:

Reject Registration Approve Registration

Figure 23 - User Approval Details

- The system displays the Confirm Registration Approval dialog box. Select the "Confirm" button in the bottom right to approve the user registration request.

Confirm Registration Approval

Are you sure you want to approve user registration for: **Jones, John E**?

Cancel Confirm

Figure 24 - Confirm Registration Approval Dialog Box



- The system submits the approval task and reopens the “Pending Approvals” displaying the “User registration request approved successfully” notification ribbon in green. **Note:** If the request has not been processed successfully attempt to approve the access again. If the error persists, please see [Section 6.2: Help Desk](#).

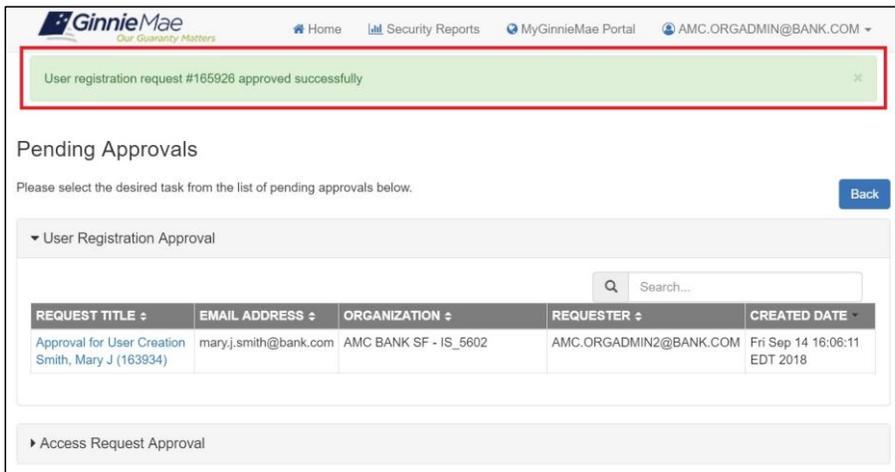


Figure 25 - User Registration Approval Notification Ribbon

- It is recommended to immediately proceed to the access request; [Section 3.3: Request Functional Role](#).

3.3 Request Functional Role

Once a User Registration request has been approved, a portal account has been established for that user in MyGinnieMae, and the Organization Administrator should proceed with requesting Functional Roles for that End User. This same process may be followed 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 additional Functional Roles, this process must be completed by other members of the Organization Administrator Group.

- Log into the Portal and navigate to the Access Management Console.

Commented [CRH7]: remove additional. Org Admin role is not a functional role. Suggest "If an Organization Administrator requires functional role (s) to complete business processes, this access request must be completed by other members of the Organizatin Administrator group.



2. Select the "Access Request" tile.



Figure 26 - Access Management Console Landing Page

3. The system displays a table which contains the list of all registered users within the organization(s) the Organization Administrator manages. From the table, select the hyperlink for the Display Name of the End User in need of a Functional Role.

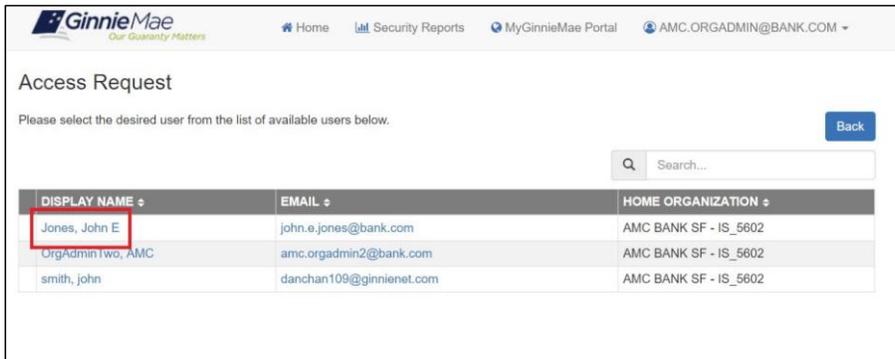


Figure 27 - Request Access for Others Search

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.



- If the Organization Administrator has multiple Org Keys, a list of organizations associated with the Organization Administrator will be displayed. Select the box next to each organization that the Functional Role(s) selected on the following page will apply and select the “Assign Roles” button on the right side of the page. **Note:** If the Organization Administrator only has one Org Key, the Organization Administrator will be sent directly to the Functional Role list (Step 5).

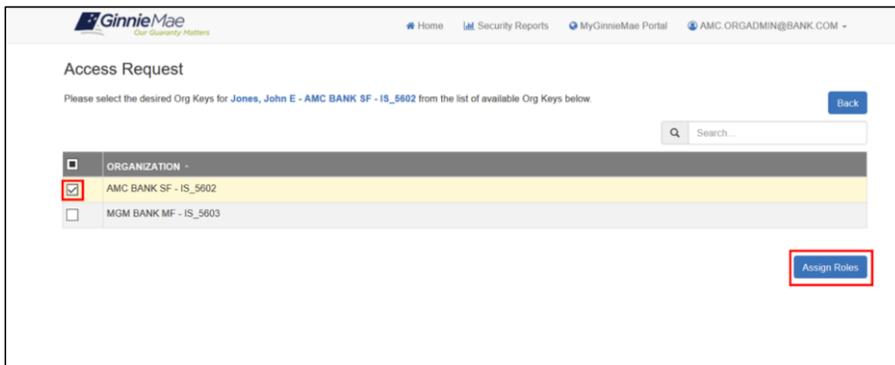


Figure 28 - Select Organization Key(s)

- The system displays a list of Functional Roles available for the selected Home Organization. Select the Functional Role(s) to be requested for the user and select the “Assign Roles” button in the bottom right to confirm the selections.

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



Access Request

Please select the desired Functional Roles for Jones, John E - AMC BANK SF - IS_5602 from the list of available Functional Roles. Back

AMC BANK SF - IS_5602

<input type="checkbox"/>	FUNCTIONAL ROLE	DESCRIPTION
<input type="checkbox"/>	SF-Bulk Transfers Authorized Signer	Initiate, manage and accept bulk transfer transactions; initiate and coordinate transfers of collateral files with transferee and transferor issuers or Document Custodians.
<input type="checkbox"/>	SF-Collateral Management Authorized Signer	Process releases of collateral from the Document Custodian in accordance with servicing obligations (HUD-11706 Releases).
<input type="checkbox"/>	SF-Compliance and Oversight User	Review portfolio servicing and investor reporting metrics and reports; oversee subservicer performance when applicable.
<input type="checkbox"/>	SF-Investor Reporting Authorized Signer	Only for HUD 11702 signatories. All rights of an Investor Reporting Basic User, plus; authority to certify the monthly pool and loan accounting report; submit edits needed to clear exception feedback and monthly reporting errors.
<input type="checkbox"/>	SF-Loan Delivery and Pooling Authorized Signer	Only for HUD 11702 signatories. All rights of a Loan Delivery and Pooling Basic User, plus; authority to submit pools for issuance, request additional commitment authority and execute PIT/TAI transactions.
<input type="checkbox"/>	SF-Loan Delivery and Pooling Basic User	Upload/enter pool and loan information for delivery; verify availability of commitment authority; clear document deficiencies and pooling exceptions; access to prepare but not execute PIT/TAI transactions.
<input checked="" type="checkbox"/>	SF-Post-Closing User	Access to review collateral, obtain loan insurance, forward initial and trailing documents to a Document Custodian.
<input checked="" type="checkbox"/>	SF-Processing Master Agreements Authorized Signer	Only for HUD 11702 signatories. Edit, submit and certify Master Agreement documents and data required by Ginnie Mae.
<input type="checkbox"/>	SF-Special Loans User	Upload and process SCRA reimbursement requests.
<input type="checkbox"/>	SF-Test Inv Rep Auth Signer Description	Access to prepare monthly pool submission and loan level accounting report and validate custodial account data. Ability to review monthly remittance information and monthly reporting exception feedback and errors. Finalize/execute business transactions with authority to certify monthly pool and loan accounting report and submit edits to clear exception feedback and monthly reporting errors (HUD-11702 Signer).

The functional roles listed below have been requested for this user and are either pending, approved or finalized.

- SF-Investor Reporting Basic User - Submit monthly pool and loan level accounting data; submit quarterly custodial account verification data; review monthly remittance information, review monthly reporting exception feedback and errors.
- SF-Agency Relationship User - Access reports containing portfolio performance and liquidity metrics; receive targeted Ginnie Mae communications for individuals responsible for managing agency relationships.
- SF-Financial Statements User - Submit annual audited financial statements for review by Ginnie Mae's IPA.

Assign Roles

Figure 29 – Select Functional Role(s) for End User

Note: 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.



- The system displays a review page with the requested Functional Role(s) and the underlying roles that makeup that Functional Role(s). Select the “Submit” button in the bottom right.

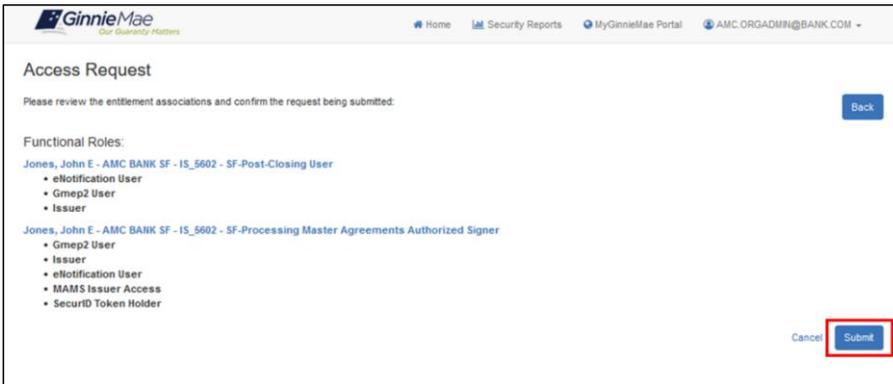


Figure 30 - Request Functional Role Review

- The system displays an access request confirmation dialog box. Select “Confirm” to submit the roles to the system.



Figure 31 – Confirm Access Request

- 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 but a resubmit should not be performed.



9. After successful submission, the system displays a confirmation ribbon at the top of the screen.

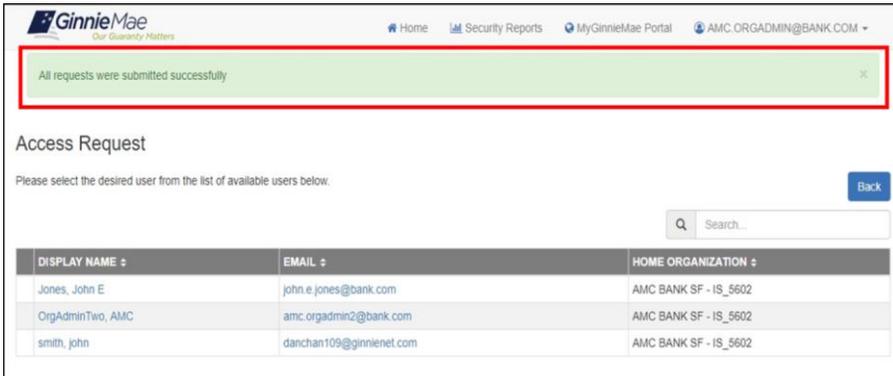


Figure 32 - Role Access Request

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. If the error persists, please see [Section 6.2: Help Desk](#).

3.4 Approve an Access Request

Once an Access Request has been submitted, another Organization Administrator (other than the one who submitted the access request) within the organization must approve the access request. All Organization Administrators within the organization will receive an email notification that a request is available for approval.



Figure 33 - Access Request Approval Notification

1. Within the Access Management Console, navigate to 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 34—AMC Homepage—Pending Approvals Tile

2. Review the table under “Access Request Approval” accordion (collapsible section) which displays the list of available Functional Role requests pending approval. Select the Request ID for the Functional Role.

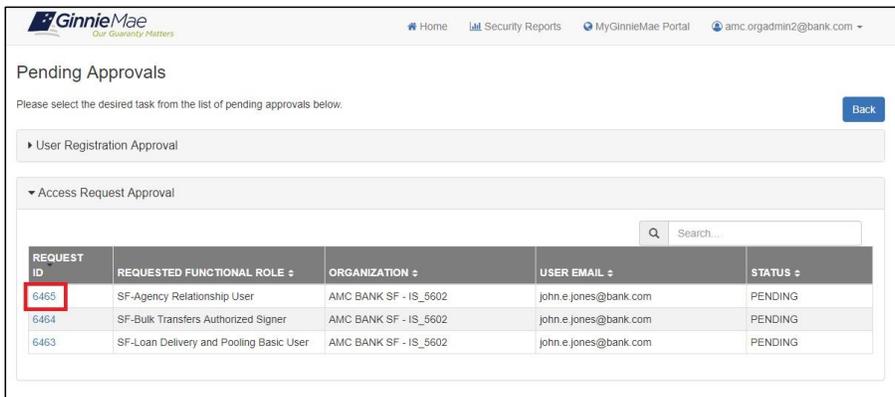


Figure 35 - List of Pending Access Requests



- The details of the requested Functional Role display in the review page. Review the request details and select “Approve” to activate the confirmation message.

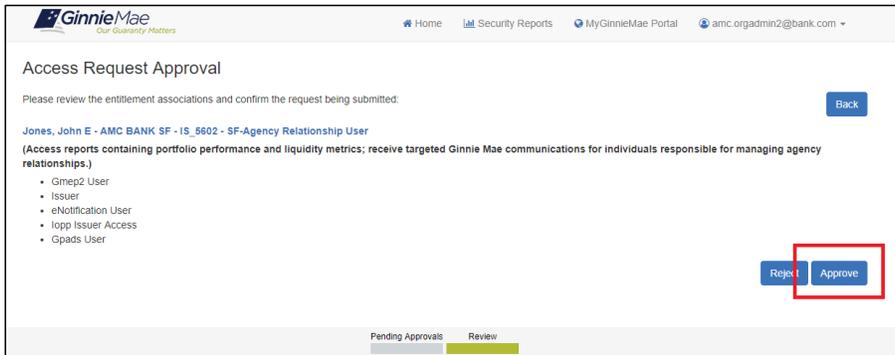


Figure 36 - Review Page for Functional Role Approval

- Select the “Confirm” button and submit the approval to the system.

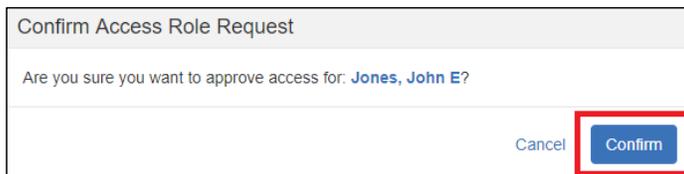


Figure 37 – Confirm Functional Role Approval



- 5. The system displays a successful notification at the top of the screen when the approval has been submitted successfully.

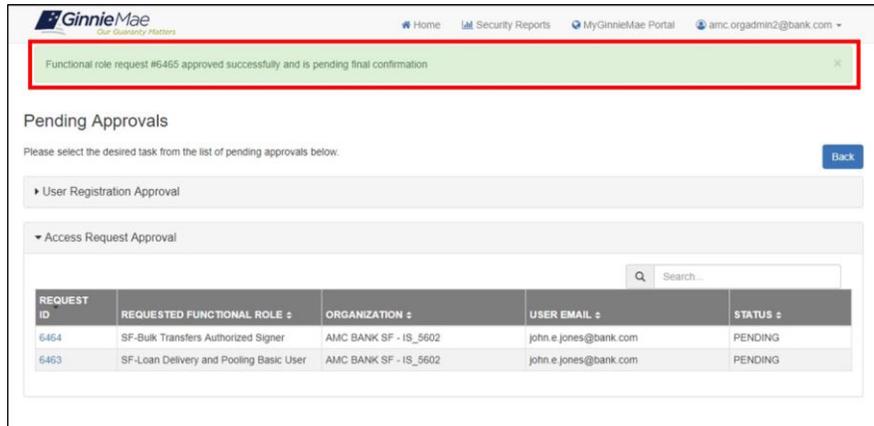


Figure 38 – Request Approval Successful

Note: If the request has not been processed successfully, review the error message and attempt to re-request if possible. If the error persists, please see [Section 6.2: Help Desk](#). If an error occurs upon submission, the current selection(s) and/or page within the module are retained.

- 6. The system routes the request to, and notifies, the Operations Administrator group to perform required action to complete the approval 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.

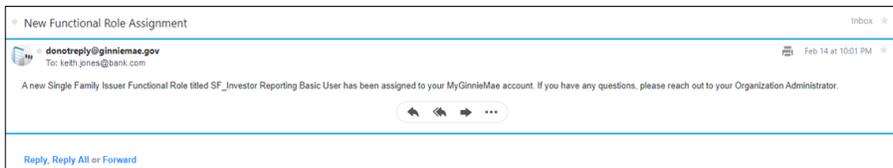


Figure 38 - End User Notification

3.5 Remove Functional Roles from a User

If a user no longer requires access to a specific Functional Role, Organization Administrators are responsible for removing that role from the user’s account. To remove a role from an account, follow the steps provided below.



1. Access the Access Management Console.
2. On the Access Management Console Landing Page, select the “User Management” tile.

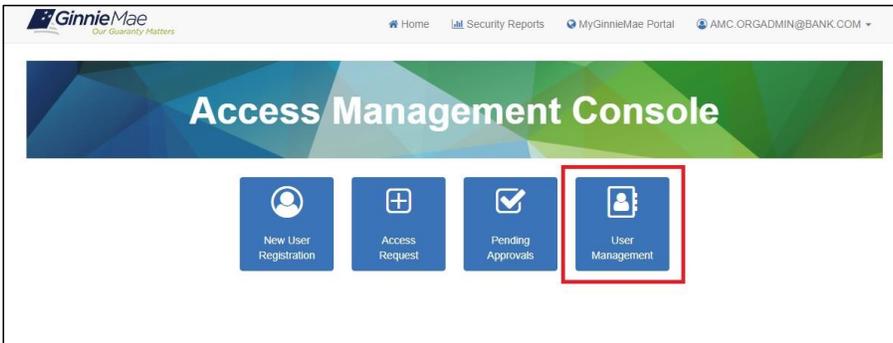


Figure 39 - Access Management Console Landing Page

3. The system displays a list of the users within the Organization Administrator’s organization(s). Search for a user by typing the Display Name of the user in the search field and select the Display Name. The following user properties can also be searched for within the search field:
 - Email
 - Home Organization



Figure 40 - Select User



- The system displays the User Profile page. Select the arrow next to the "Manage User Permissions" heading to open up the accordion and the system displays the roles assigned to the user.

GinnieMae
The Standard Matters

Home | Security Reports | MyGinnieMae Portal | AMC.ORGADMIN@BANK.COM

User Management

Please edit the user profile or manage the user permissions of Jones, John E below. [Reset Password](#) [Back](#)

Edit User Profile

User Information

Display Name: Jones, John E. Login: JOHN.E.JONES@BANK.COM

Title: Mr. First Name: John. Middle Name: E. Last Name: Jones. Suffix:

Contact Information

Email: john.e.jones@bank.com. Mobile Number: . Work Number: (757)777-3333. Extension:

Organization Information

Organization: AMC BANK SF - IS_5602. Job Title: Tester

Legacy Application Information

GMEPI IDs: l_jones5602. GinnieNet IDs:

[Disable](#) [Lock](#)

Manage User Permissions

Figure 41 – User Profile



- Review the listed roles for the user and select the Functional Role and then select the "Remove" button to remove the role from the user.

User Management

Please edit the user profile or manage the user permissions of Jones, John E below: Reset Password Back

▶ Edit User Profile

▼ Manage User Permissions

Functional Role

ROLE NAME	ROLE DESCRIPTION	ORG KEY	STATUS	SELECT
SF-Bulk Transfers Authorized Signer	Initiate, manage and accept bulk transfer transactions; initiate and coordinate transfers of collateral files with transferee and transferor issuers or Document Custodians.	IS_5602	CONFIRMED	<input checked="" type="checkbox"/>
SF-Loan Delivery and Pooling Basic User	Upload/enter pool and loan information for delivery; verify availability of commitment authority; clear document deficiencies and pooling exceptions; access to prepare but not execute PIIT/TAI transactions.	IS_5602	CONFIRMED	<input type="checkbox"/>

Verify Re-Request Remove

System Role

ROLE NAME	ROLE DISPLAY NAME	REQUESTABLE	SELECT
ALL USERS	ALL USERS	false	<input type="checkbox"/>

Figure 42 - Remove Functional Roles

- The system displays a confirmation message. Select the "Confirm" button in the bottom right to confirm the removal of the selected Functional Role.

Confirm Remove Functional Role

Are you sure you want to remove the selected Functional Roles from user: **Jones, John E**?

Cancel Confirm

Figure 43 - Confirm Functional Role Removal



7. The system displays a success/error notification ribbon at the top of the page.

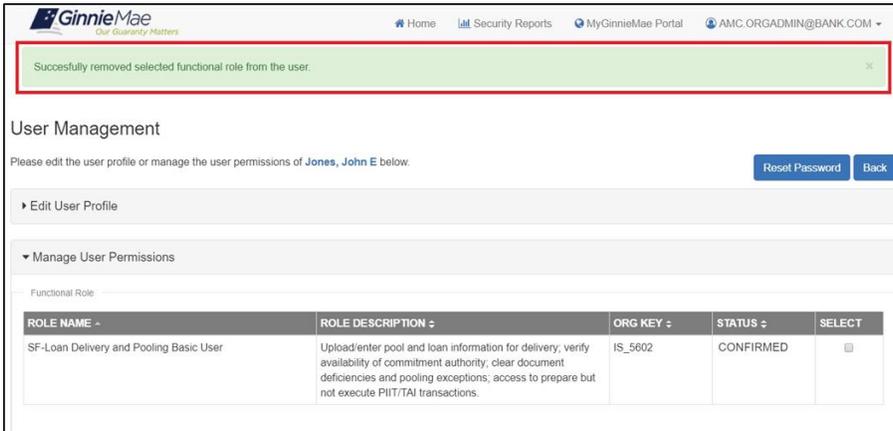


Figure 44 - Functional Role Removal Notification

8. No additional approvals are required after the removal is confirmed.

Note: If a Functional Role is removed inadvertently, it can be requested again by following the steps in [Section 3.3: Request Functional Role](#).

3.6 Disable a User Account

If a user is leaving an organization or for other reasons requires their account to be disabled, the Organization Administrator is responsible for disabling the user's account from the Access Management Console. Disabling a user removes all assigned Functional Roles. If a user access needs to be temporarily blocked for a short amount of time, consider locking the user account as described in [Section 3.8: Lock a User's Account](#).



To disable an account, follow the steps below.

1. Access the Access Management Console and select the "User Management" tile. Within User Management Tile, select a user.

The screenshot shows the GinnieMae User Management interface. At the top, there is a navigation bar with links for Home, Security Reports, MyGinnieMae Portal, and the user email AMC.ORGADMIN@BANK.COM. Below the navigation bar, the page title is "User Management" and a message says "Please select the desired user from the list of available users below." There is a search bar and a "Back" button. A table lists three users:

DISPLAY NAME	EMAIL	HOME ORGANIZATION
Jones, John E	john.e.jones@bank.com	AMC BANK SF - IS_5602
OrgAdminTwo, AMC	amc.orgadmin2@bank.com	AMC BANK SF - IS_5602
smith, john	danchan109@ginnienet.com	AMC BANK SF - IS_5602

At the bottom of the table, there are buttons for "User" (highlighted in green) and "View / Edit".

Figure 45 - Select User



2. Select the “Disable” button in the bottom right of the “Edit User Profile” accordion.

Figure 46 - User Management – Disable Account

3. Select the “Confirm” button to submit the action. When a user is disabled, the system removes any existing Functional Roles provisioned to the user.

Figure 47 - Confirm Disable Account



- 4. The system displays a "User [User Name] successfully disabled" message and updates the Account Status as "Disabled."

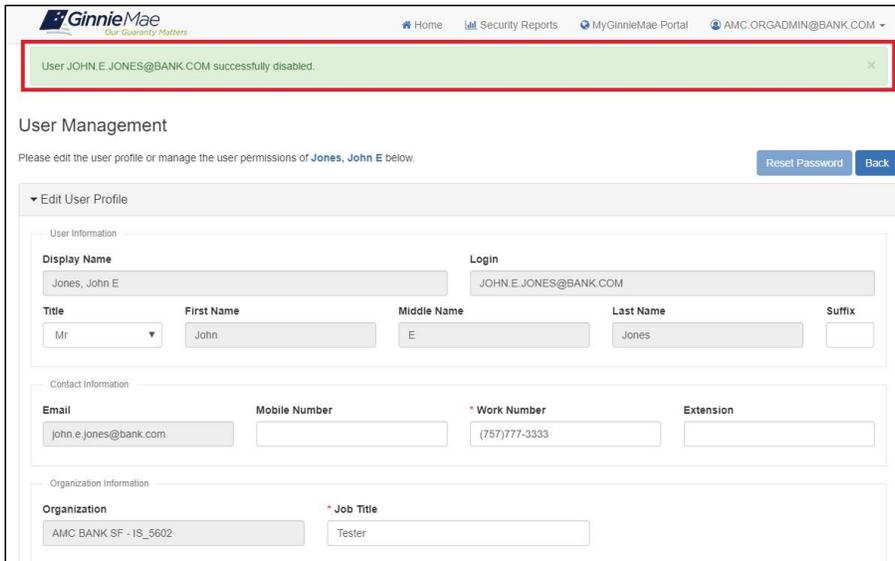


Figure 48 - Disable Account Notification

- 5. Scroll down and open the "Manage User Permissions" accordion to confirm the Functional Roles have been removed from the user.

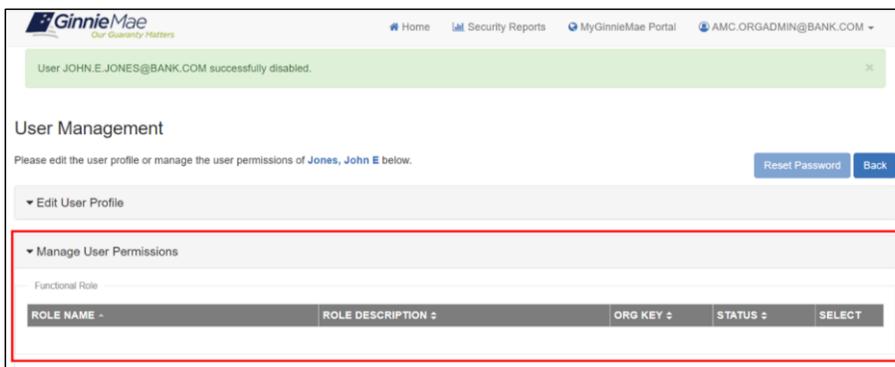


Figure 49 - Select Disabled User Functional Roles



3.7 Enable a User's Account

If a user's account has been disabled due to 90 days of inactivity or disabled manually, and needs to be re-enabled, complete the following steps in the Access Management Console.

Note: If a user was disabled due to 90 days of inactivity, instruct the user to login to MyGinnieMae after their account is enabled; otherwise the user will be disabled again the following day due to inactivity. The user should to be contacted via phone to confirm they login after their account is enabled.

1. Access the Access Management Console and select the "User Management" tile.
2. Select the Display Name of the user to enable. Verify the user is disabled by confirming that there is a disabled icon (⊘) to the left of their Display Name.

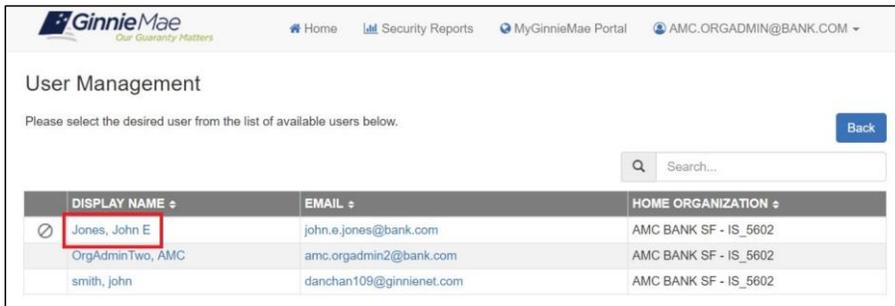


Figure 50 - User Management Disabled User



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

Figure 51 - User Management – Enable Account

- The system displays a dialog box to confirm the enabling of the selected user's account. Select the "Confirm" button to submit the enable request to the system.

Figure 52 - Confirm Enable Account



- The system displays a "User [User Name] successfully enabled" message and updates the Account Status as "Enabled". Follow the steps in [Section 3.3: Request Functional Role](#) to request roles for a user.

The screenshot shows the GinnieMae user management interface. At the top, a green notification banner reads "User JOHN.E.JONES@BANK.COM successfully enabled." Below this, the "User Management" section is displayed for the user "Jones, John E.". The interface includes a "Reset Password" and "Back" button. The user profile is divided into three sections: "User Information", "Contact Information", and "Organization Information".

User Information				
Display Name	Login			
Jones, John E	JOHN.E.JONES@BANK.COM			
Title	First Name	Middle Name	Last Name	Suffix
Mr	John	E	Jones	

Contact Information			
Email	Mobile Number	* Work Number	Extension
john.e.jones@bank.com		(757)777-3333	

Organization Information	
Organization	* Job Title
AMC BANK SF - IS_5602	Tester

Figure 53 - Enable Account Notification



- 6. 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.

The screenshot shows the 'User Management' interface for a user named John E. Jones. The user's profile is displayed with various fields for editing. The 'Organization' field is highlighted with a red box and contains the text 'AMC BANK SF - IS_5602'. Above this field, a red error message reads '(Organization Disabled)'. Other fields include 'Display Name' (Jones, John E), 'Login' (JOHN.E.JONES@BANK.COM), 'Title' (Mr), 'First Name' (John), 'Middle Name' (E), 'Last Name' (Jones), 'Suffix' (Jr), 'Email' (john.e.jones@bank.com), 'Mobile Number', 'Work Number' ((757)601-2121), 'Extension', 'Job Title' (Tester), 'GMEPI IDs', and 'GinnieNet IDs'. Buttons for 'Reset Password', 'Back', and 'Lock' are visible.

Figure 54 - Disabled Organization User Profile

3.8 Lock a User's Account

This process is used to lock a user's account, which will prevent the user from logging in with their MyGinnieMae account while retaining access. Locking is a more temporary action and is different from disabling a user account as described in [Section 3.6: Disable a User Account](#), which removes the user's access.



1. Access the Access Management Console and select the "User Management" tile.

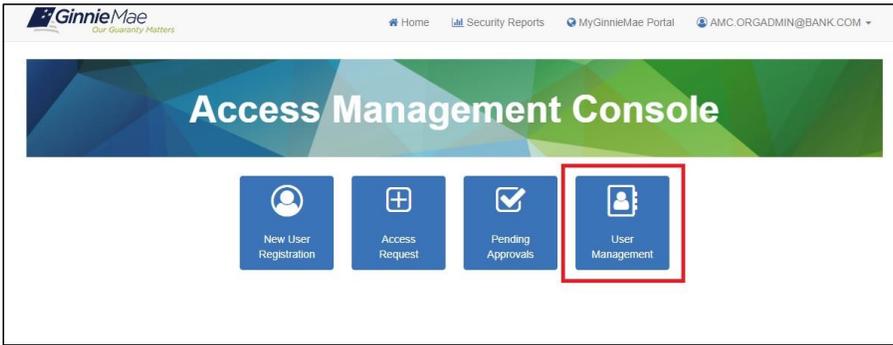


Figure 55 - Access Management Console Landing Page

2. Select the Display Name of the user to lock. Verify if the user is not already locked by identifying if there is no locked icon () to the left of their Display Name.



Figure 56 - Search Users Results



3. Within the open "Edit User Profile" accordion, select the "Lock" button at the bottom right.

The screenshot shows the 'User Management' page in the GinnieMae system. The user profile for 'Jones, John E.' is displayed. The 'Edit User Profile' accordion is open, showing fields for User Information, Contact Information, Organization Information, and Legacy Application Information. At the bottom right of the form, there are two buttons: 'Disable' and 'Lock'. The 'Lock' button is highlighted with a red rectangular box.

Figure 57 - User Management – Lock Account

4. The system opens a dialog box to confirm the account lock. Review the user details and select "Confirm."

The screenshot shows a dialog box titled 'Confirm User Lock'. The text inside the dialog box reads: 'Are you sure you want to lock access for: Jones, John E?'. At the bottom right of the dialog box, there are two buttons: 'Cancel' and 'Confirm'. The 'Confirm' button is highlighted with a red rectangular box.

Figure 58 - Confirm Account Lock



5. The system displays a “User [User Name] successfully locked” message and updates the Account Status as “Locked.”

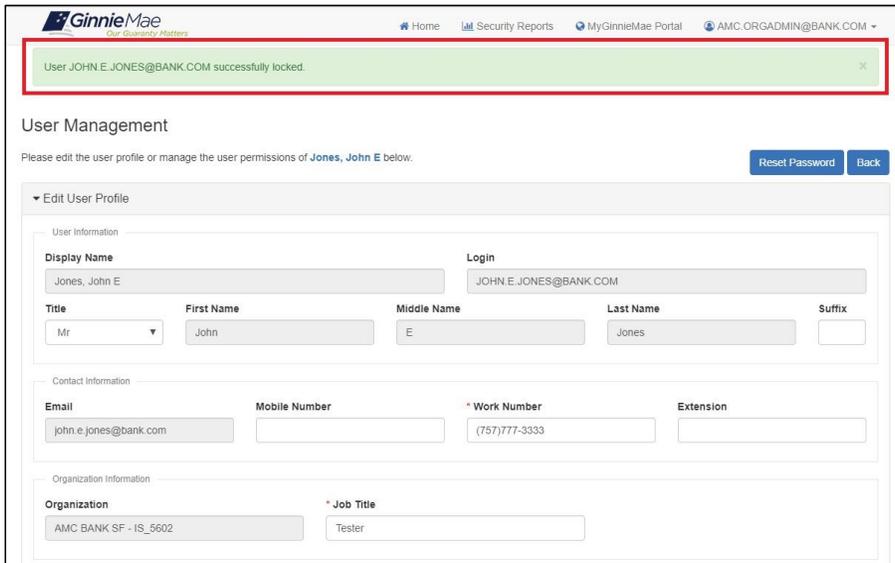


Figure 59 - Lock Account Notification

3.9 Unlock a User’s Account

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

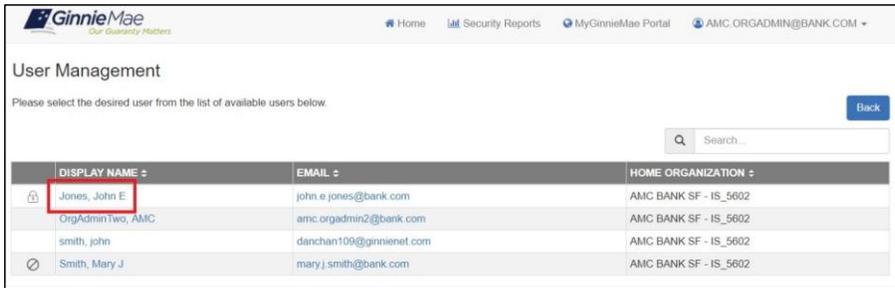
- Organization Administrator locked account; Organization Administrator can unlock
- Three failed attempts to enter correct user name and password; Organization Administrator can unlock
- Three failed attempts to enter correct OTP; Operations Administrator group can unlock. If a user is locked out due to an incorrect OTP, see [Section 6.2: Help Desk](#).

Note: The AMC/User Management page will not indicate to the Organization Administrator that the account has an OTP lock.

1. Access the Access Management Console and select the “User Management” tile.



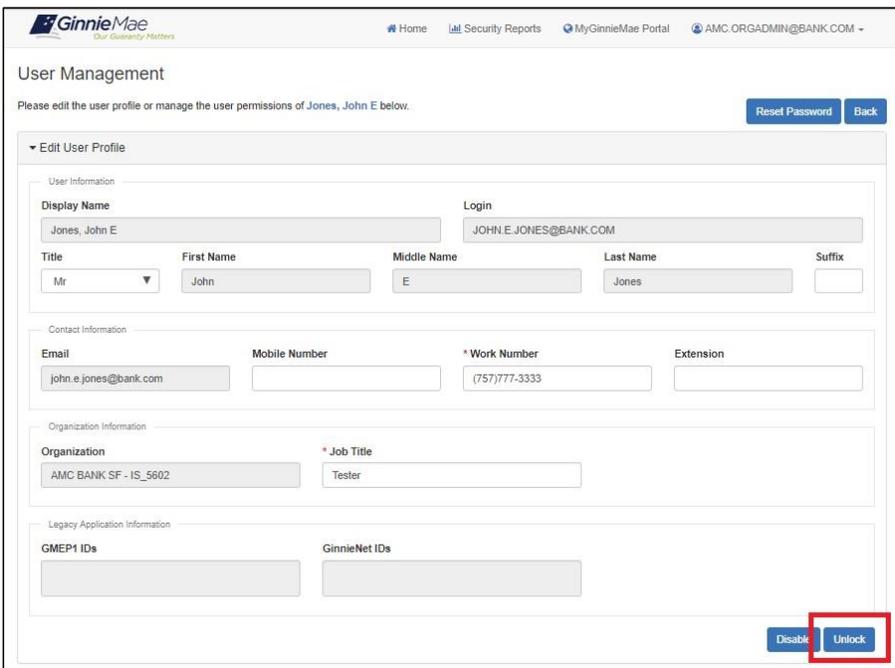
2. Select the Display Name of the user to unlock. Verify the user is locked by identifying there is a locked icon () to the left of their Display Name.



	DISPLAY NAME	EMAIL	HOME ORGANIZATION
	Jones, John E.	john.e.jones@bank.com	AMC BANK SF - IS_5602
	OrgAdminTwo, AMC	amc.orgadmin2@bank.com	AMC BANK SF - IS_5602
	smith, john	danchan109@ginnienet.com	AMC BANK SF - IS_5602
	Smith, Mary J	mary.j.smith@bank.com	AMC BANK SF - IS_5602

Figure 60 - Locked User Search

3. At the bottom right of the “Edit User Profile” accordion, select the “Unlock” button.



User Management

Please edit the user profile or manage the user permissions of Jones, John E below.

Reset Password Back

▼ Edit User Profile

User Information

Display Name: Jones, John E. Login: JOHN.E.JONES@BANK.COM

Title: Mr. First Name: John. Middle Name: E. Last Name: Jones. Suffix:

Contact Information

Email: john.e.jones@bank.com. Mobile Number: . Work Number: (757)777-3333. Extension:

Organization Information

Organization: AMC BANK SF - IS_5602. Job Title: Tester

Legacy Application Information

GMEP1 IDs: . GinnieNet IDs: .

Disable Unlock

Figure 61 - User Management – Unlock Account



- The system opens a dialog box to confirm the account unlock. Review the user details and select “Confirm.”



Figure 62 - Confirm Unlock Account

- The system displays a notification that “User [User Name] successfully unlocked.” The page updates the Account Status as “Unlocked.”

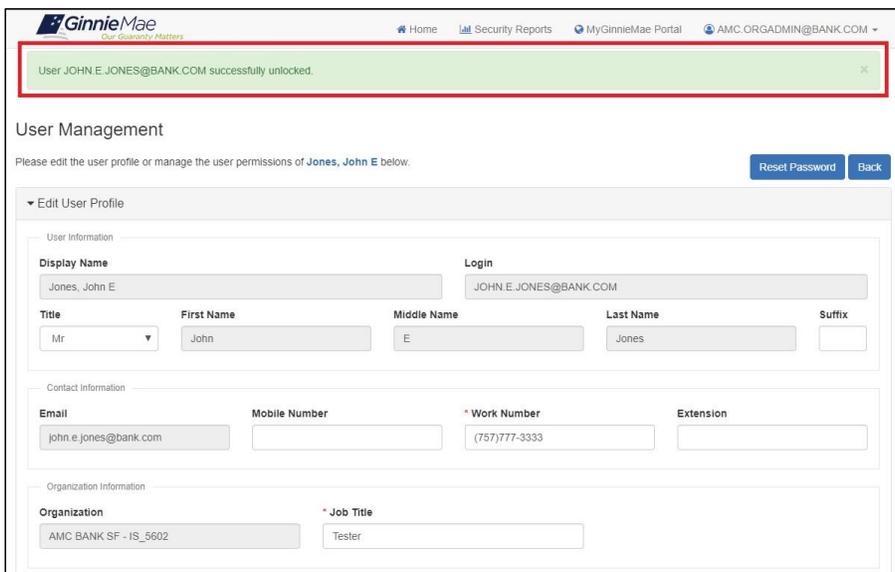


Figure 63 - Unlock Account Notification

3.10 Update a User’s Profile Attributes

Follow the steps below to update a user’s account attribute information.

- Access the Access Management Console and select the “User Management” tile. Within User Management Tile, select a user.



2. Within the “Edit User Profile,” edit the desired user attributes (listed below) and then select the “Save” button in the bottom right of the accordion. Note: The “Save” button is not displayed unless an attribute is edited.

- Title (Mr., Mrs., etc.) [required attribute]
- Suffix
- Mobile Number
- Work Number [required attribute]
- Extension
- Job Title [required attribute]

The screenshot shows the GinnieMae User Management interface. At the top, there is a navigation bar with links for Home, Security Reports, MyGinnieMae Portal, and the user's email address (AMC.ORGADMIN@BANK.COM). Below the navigation bar, the page title is "User Management" and a sub-header reads "Please edit the user profile or manage the user permissions of Jones, John E below." There are "Reset Password" and "Back" buttons in the top right. The main content area is an accordion titled "Edit User Profile". It contains four sections: "User Information" with fields for Display Name (Jones, John E), Login (JOHN.E.JONES@BANK.COM), Title (Mr.), First Name (John), Middle Name (E), Last Name (Jones), and Suffix (Jr.); "Contact Information" with fields for Email (john.e.jones@bank.com), Mobile Number, Work Number (757/601-2121), and Extension; "Organization Information" with fields for Organization (AMC BANK SF - IS_5602) and Job Title (Tester); and "Legacy Application Information" with fields for GMEP1 IDs and GinnieNet IDs. At the bottom right of the form, there are three buttons: "Save" (highlighted with a red box), "Disable", and "Lock".

Figure 64 - User Management – Update User Profile



- The system displays a dialog box to confirm the updated attributes. Select the “Confirm” button to send the updates to the system.



Figure 65 - Confirm User Profile Update

- A “User [User Name] successfully updated” notification displays.

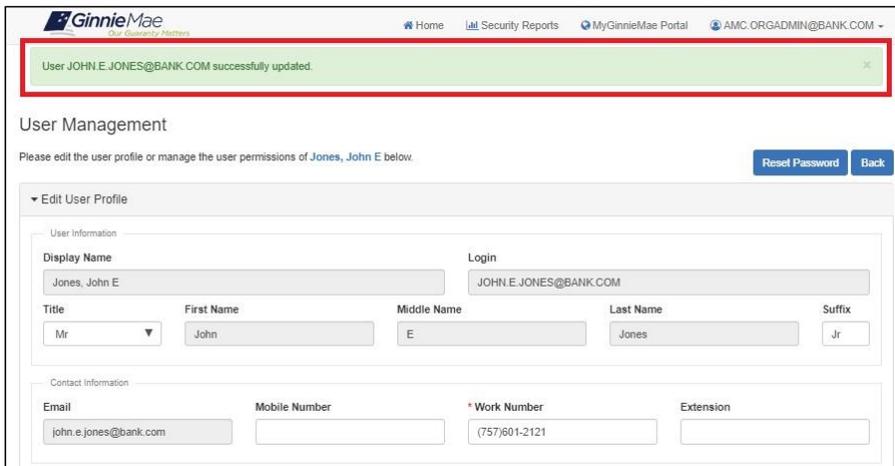


Figure 66 - Update User Profile Notification

3.11 Reset a User’s Password

This service is used in an event that the user has forgotten their password and is unable to reset it using self-service capabilities or they suspect their account has been compromised.

A user should be instructed to attempt to create a new password using the Forgot Password functionality first. If the user’s password cannot be reset using the Forgot Password functionality, follow the steps below:

- Access Management Console and select the “User Management” tile. Within User Management Tile, select a user.



- At the top right of the page, select the “Reset Password” button. **Note:** This button is inactive if the user is disabled.

The screenshot shows the GinnieMae User Management interface. At the top right, there are navigation links: Home, Security Reports, MyGinnieMae Portal, and AMC.ORGADMIN@BANK.COM. Below the navigation is the 'User Management' section with the instruction: 'Please edit the user profile or manage the user permissions of Jones, John E below.' A 'Reset Password' button and a 'Back' button are visible in the top right corner of the user management area. Below this is the 'Edit User Profile' section, which is divided into three tabs: 'User Information', 'Contact Information', and 'Organization Information'. The 'User Information' tab is active and shows fields for Display Name (Jones, John E), Login (JOHN.E.JONES@BANK.COM), Title (Mr), First Name (John), Middle Name (E), Last Name (Jones), and Suffix (Jr). The 'Contact Information' tab shows fields for Email (john.e.jones@bank.com), Mobile Number, Work Number ((757)601-2121), and Extension. The 'Organization Information' tab shows fields for Organization (AMC BANK SF - IS_5602) and Job Title (Tester).

Figure 67 – Reset Password Button

- The system opens a dialog box to verify that an auto-generated password will be emailed to the user.

The screenshot shows a dialog box titled 'Confirm Password Reset'. The text inside the dialog box reads: 'Are you sure you want to reset the password for: Jones, John E? A new, randomly generated, password will be created and emailed to: john.e.jones@bank.com'. At the bottom right of the dialog box, there are two buttons: 'Cancel' and 'Confirm'. The 'Confirm' button is highlighted with a red box.

Figure 68 - Reset Password Form



4. Select “Confirm” and the system displays a notification ribbon at the top of the page. The end user is required to change their password once they have logged in with the system generated password.

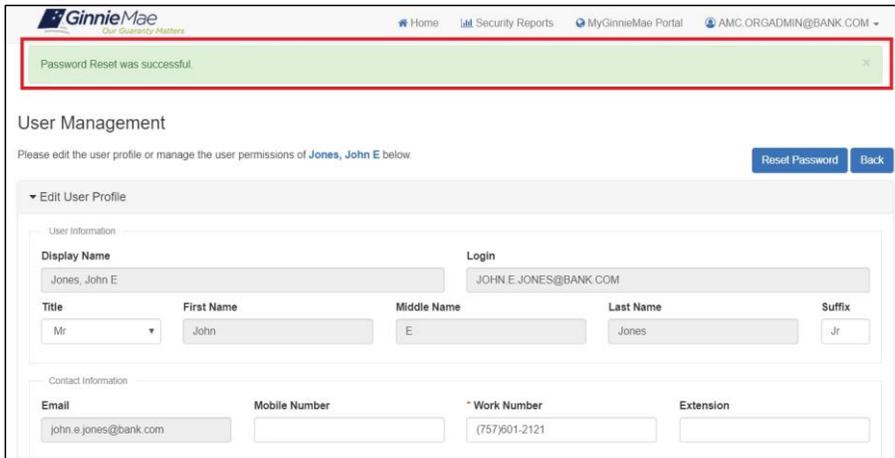


Figure 69 - Reset Password Notification

3.12 Reject a New User Registration

The following process will review the rejection of a user registration request within the Access Management Console.

1. Follow the first four steps for approving a New User Registration to navigate to the review screen (see [Section 3.2: Approve a New User Registration](#)).



2. Select the button to “Reject Registration” from the bottom right of the review page.

GinnieMae
Our Guaranty Matters

Home Security Reports MyGinnieMae Portal amc.orgadmin2@bank.com

New Registration Approval

Please review the user details and confirm the request being submitted. [Back](#)

Registration Request Details

Display Name: Erickson, Katherine A	First Name: Katherine
Middle Name: A	Last Name: Erickson
Email Address: katherine.a.erickson@bank.com	Organization: AMC BANK SF - IS_5602
Department Name (Ginnie Mae):	User Login: katherine.a.erickson@bank.com
Job Title: Tester	Telephone Number: (567)890-0987
Telephone Extension:	Mobile Phone: (234)567-8865

[Reject Registration](#) [Approve Registration](#)

Pending Approvals Review

Figure 70 - User Rejection Details

3. The system displays a dialog box for the rejection justification reason. This is a required field and 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)



Confirm Registration Reject

Are you sure you want to reject the registration for: **Erickson, Katherine A?**

Required: Select a justification reason ▼

Required: Select a justification reason

User No Longer with Organization

Do Not Recognize User

User already has an existing account

Invitation sent to incorrect email address

Other - Please Explain

Cancel

Figure 71 – Rejection Justification Reason Drop Down

4. Supply the Justification Reason and, if required, the Justification Description. Select the “Confirm” button to send the rejection to the system.

Confirm Registration Reject

Are you sure you want to reject the registration for: **Erickson, Katherine A?**

User No Longer with Organization ▼

Enter rejection justification description here...

Cancel Confirm

Figure 72 - New User Registration Rejection



- After rejection, the system notifies the Organization Administrator group with the following email template.



Figure 73 - User Registration Rejection Notification

3.13 Reject a Functional Role

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.

- Follow the first three steps for approving an Access Request to navigate to the review page, then select the “Reject” button.

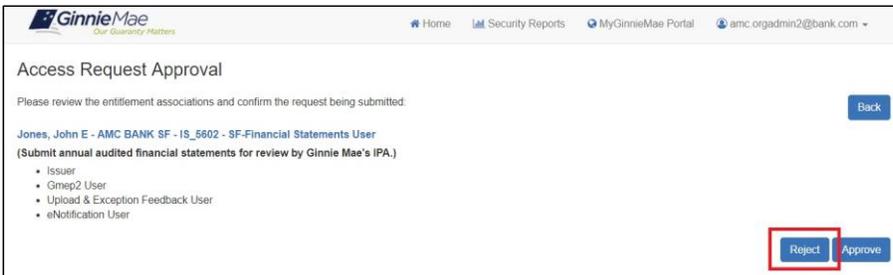


Figure 74 - Review Page for Functional Role Rejection

- The system displays a dialog box to provide a Justification Reason and optional Justification Description. The following justification reasons can be selected:
 - Access Does Not Enforce Least Privilege
 - Incorrect Functional Role Requested
 - User No Longer with Organization
 - Do Not Recognize User by ID
 - Access Violates Separation of Duties



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

Confirm Rejection of Role Request

Are you sure you want to reject access for: **Jones, John E?**

Required: Select a justification reason

Required: Select a justification reason

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

Cancel Reject

Figure 75 – Reject Role Request Justification Reason

3. After supplying the Justification Reason and, if required, the Justification Description, select the “Confirm” button to send the rejection to the system.

Confirm Rejection of Role Request

Are you sure you want to reject access for: **Jones, John E?**

User No Longer with Organization

Enter rejection justification description here...

Cancel Reject

Figure 76 - Access Request Rejection



4. The system will display a notification to indicate the Functional Role rejection was successful.



Figure 77 – Functional Role Rejection Notification

5. After rejection, the system notifies the Organization Admin group with the following email template.
Note: if no Justification Description is submitted then the response within the email is “undefined”.

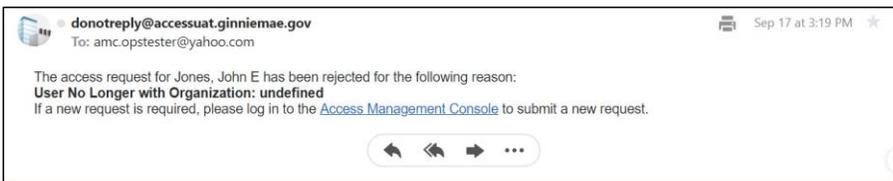


Figure 78 - Access Request Rejection Email Notification

3.14 Review the Status of an 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 user until necessary approvals are completed. To review the status of a Functional Role request for a user, follow the steps below.

1. From the Access Management Console, select the “User Management” tile and select a user.
2. Select the arrow next to the “Manage User Permissions” heading to open the accordion. 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.

The screenshot shows the 'User Management' page for user 'Jones, John E'. It features a 'Manage User Permissions' section with a table of functional roles. The 'STATUS' column is highlighted with a red box, showing 'APPROVED' and 'PENDING' statuses. Below the functional role table is a 'System Role' table with one entry: 'ALL USERS' with a 'REQUESTABLE' status of 'false'.

ROLE NAME	ROLE DESCRIPTION	ORG KEY	STATUS	SELECT
SF-Agency Relationship User	Access reports containing portfolio performance and liquidity metrics; receive targeted Ginnie Mae communications for individuals responsible for managing agency relationships.	IS_5602	APPROVED	<input type="checkbox"/>
SF-Financial Statements User	Submit annual audited financial statements for review by Ginnie Mae's IPA.	IS_5602	PENDING	<input type="checkbox"/>

ROLE NAME	ROLE DISPLAY NAME	REQUESTABLE	SELECT
ALL USERS	ALL USERS	false	<input type="checkbox"/>

Figure 79 - Functional Role Status

3.15 Verify an Assigned Functional Role

Once an Operations Administrator has finalized a functional role request, there is the potential that not all of the underlying roles were successfully assigned to the user. If there is a system error, the Organization Administrator group receives a notification (see Section 6.2: Help Desk). If an admin believes there was an issue related to provisioning and has not received confirmation, or has received an error notification then they can manual verify the status.

1. From the Access Management Console, select the “User Management” tile and select a user.



2. Navigate to the Manage User Permission accordion and select the Functional Role(s) from the list and then select “Verify.”

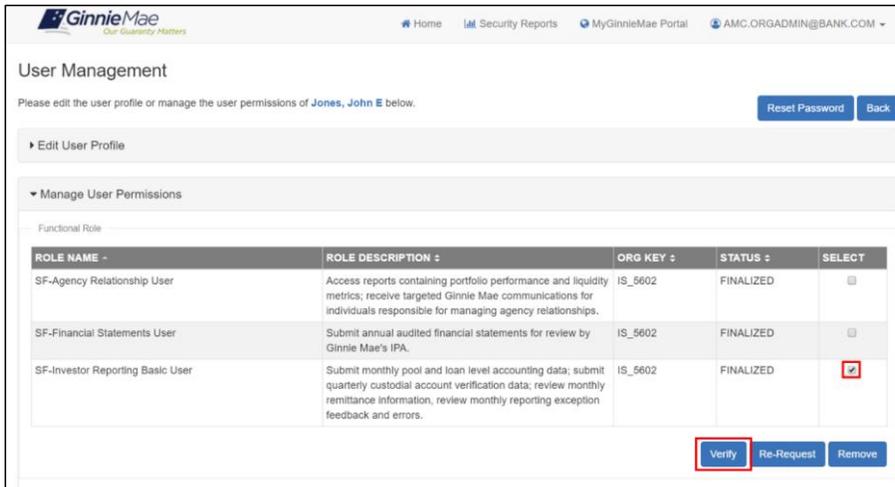


Figure 80 - User Management – Verify Functional Roles

3. The system checks the user’s access to underlying roles against the Functional Role profile and displays the updated “Status” of the Functional Role. Below are the possible statuses that may be returned.
 - CONFIRMED – all underlying roles of the Functional Role are provisioned successfully. Note: The status updates to “CONFIRMED” automatically upon successful provisioning of all underlying roles.
 - The entire set of underlying roles within a Functional Role is either successfully provisioned as described above or an error has occurred resulting in the other statuses below. In this case, check for an email regarding error notification, attempt to re-request and if the issue persists see [Section 6.2: Help Desk](#).
 - PARTIAL – MISSING
 - MISSING
 - PARTIAL – NO ACCOUNT
 - FAILED



Verify Functional Role completed.

User Management

Please edit the user profile or manage the user permissions of Jones, John E below. [Reset Password](#) [Back](#)

▶ Edit User Profile

▼ Manage User Permissions

Functional Role

ROLE NAME	ROLE DESCRIPTION	ORG KEY	STATUS	SELECT
SF-Agency Relationship User	Access reports containing portfolio performance and liquidity metrics; receive targeted Ginnie Mae communications for individuals responsible for managing agency relationships.	IS_5602	FINALIZED	<input type="checkbox"/>
SF-Financial Statements User	Submit annual audited financial statements for review by Ginnie Mae's IPA.	IS_5602	FINALIZED	<input type="checkbox"/>
SF-Investor Reporting Basic User	Submit monthly pool and loan level accounting data; submit quarterly custodial account verification data; review monthly remittance information, review monthly reporting exception feedback and errors.	IS_5602	PARTIAL-NOACCOUNT	<input type="checkbox"/>

Figure 81 - Verified Functional Role Status

4. If the "Status" is not "CONFIRMED," the role can be re-requested.

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.

The Functional Role Assignment status is PENDING and may not be re-requested.

Figure 82 – Re-Request Role Error



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 attempts to resolve issues using the suggested tips are unsuccessful or errors persist, refer to [Section 6.2: Help Desk](#).

4.1 AMC Error Page

Issue: The system displays an error message to the end user due to a service being temporarily unavailable.

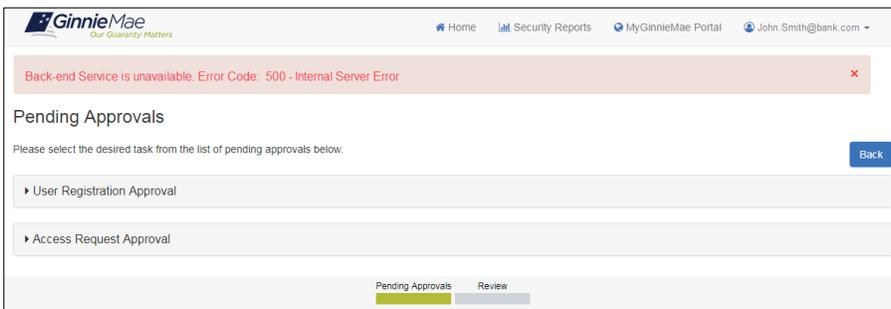


Figure 83 – Back-end Service is Unavailable Error

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 84 – Return to AMC Landing Page



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 (e.g. submit an access request or update 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 failed action.

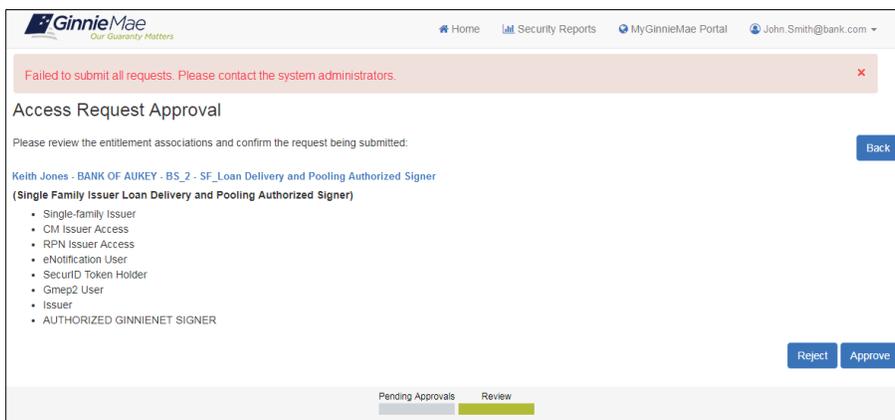


Figure 85 - Failed Access Request Submission



Failed to approve user registration request #65122

New Registration Approval

Please review the user details and confirm the request being submitted. [Back](#)

Registration Request Details

Display Name: Jones, Keith	First Name: Keith
Middle Name: (empty)	Last Name: Jones
Email Address: keith.jones@bank.com	Organization: Bank of Aukey - BP_02
Department Name (Ginnie Mae): (empty)	User Login: keith.jones@bank.com
Job Title: BA	Telephone Number: (123)123-1234
Telephone Extension: (empty)	Mobile Phone: (123)123-1234

[Reject Registration](#) [Approve Registration](#)

Figure 86 - Failed User Registration Approval

Resolution: Reattempt the action. If failures continue, see [Section 6.2: Help Desk](#).

4.3 User Registration Invitation Errors

When sending an invitation to an end user, three different errors/alerts may appear when entering the end user's email address:

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



4.3.1 Email is Already Registered

Issue: If an email address is already registered, an invitation will be unable to be sent to that user.

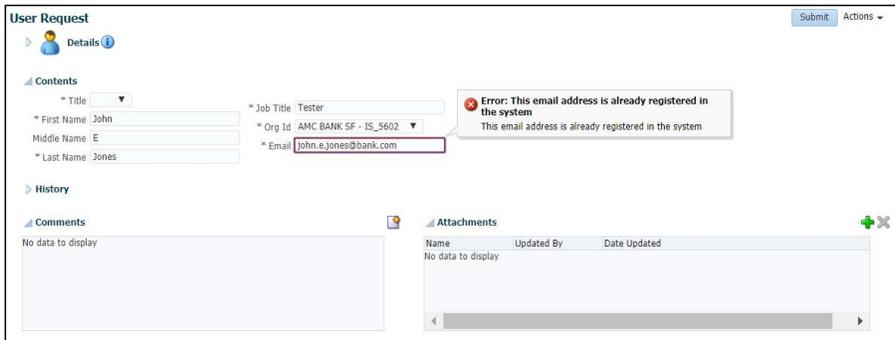


Figure 87 - Email is Already Registered Error

Resolution: Since the system is configured to prevent invitations to email addresses already registered, the Organization Administrator needs to consider the circumstances of one unique enterprise ID (email address) per person and decide whether a new email address will need to be used.



4.3.2 Three Invitations Sent Alert

Issue: If an invitation has already been sent to the user's email address a total of three times, an alert will be displayed as a warning. An invitation can only be sent a total of five times.

The screenshot shows a 'User Request' form with a blue 'Submit' button and an 'Actions' dropdown menu. The form is divided into several sections: 'Details' (with a user icon and 'Details' link), 'Contents' (with a dropdown for Title set to 'Mr', and input fields for First Name 'Keith', Middle Name, and Last Name 'Jones'), 'History', 'Comments' (with a 'No data to display' message), and 'Attachments' (with a table header: Name, Updated By, Date Updated, and a 'No data to display' message). An 'Information' alert box is overlaid on the form, containing the text: 'A User Registration Request has already been sent to this user 3 times' and an 'OK' button.

Figure 88 - Three Invitations Sent Alert

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



4.3.3 Five Time Invitation Flag

Issue: 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.

The screenshot shows a 'User Request' form with a red error message box at the top. The error message reads: 'Error: User Registration Request has been sent to this user more than 5 times. Please reach out to your administrator'. Below the error message, there is a text area with the message: 'User Registration has been sent to this user more than 5 times. Please reach out to your administrator.' The form includes several input fields: 'Last Name' with the value 'Jones', 'Email' with the value 'keith.jones@bank.com', and a dropdown menu for 'Bank of Aukey - BP_02'. There are also sections for 'Comments' and 'Attachments', both of which currently show 'No data to display'.

Figure 89 - 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 6.2: Help Desk](#).



4.4 New Password Mismatch Error

Issue: In the process of a password reset or forgot password when a user incorrectly enters their password, they will receive the system generated error, “New Password does not match”.

GinnieMae
Our Guaranty Matters

Change Your Password

A valid password must meet all of the following conditions:

- Password must not match or contain first name.
- Password must not match or contain last name.
- Password must not be longer than 20 character(s).
- Any particular character in the password must not be repeated more than 2 time(s).
- Password must contain at least 3 alphanumeric character(s).
- Password must contain at least 2 alphabetic character(s).
- Password must be at least 8 character(s) long.
- Password must contain at least 1 lowercase letter(s).
- Password must contain at least 1 numeric character(s).
- Password must contain at least 1 special character(s).
- Password must contain at least 1 uppercase letter(s).
- Password must not be one of 24 previous passwords.
- Password must not match or contain user ID.

Old Password **Completed**

New Password **New passwords entered do not match.**

Confirm New Password **New passwords entered do not match.**

To cancel changing your password, click >>

Figure 90 - New Password Does Not Match Error

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



4.5 Invalid Username or Password

Issue: When a user incorrectly enters either their username or password, they will receive the following error (the Portal validates both username and password simultaneously, rather than separately, for security purposes).

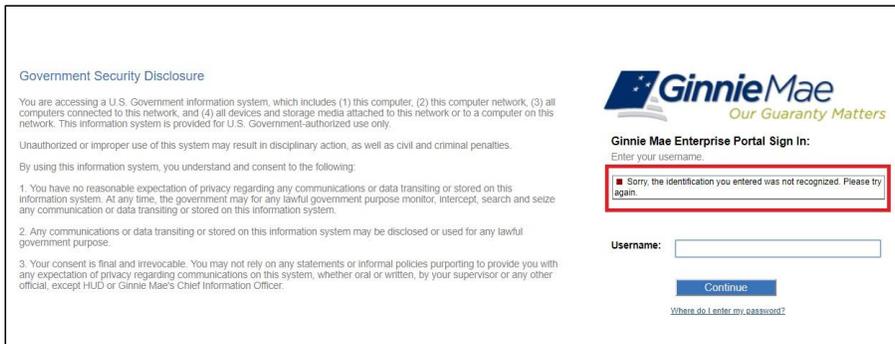


Figure 91 - Invalid Password Error

Resolution: The user must retry and enter the correct name and password.

4.6 Incorrect OTP

Issue: When a user enters an incorrect OTP, they will receive the system generated error, "Incorrect OTP. Please try again."

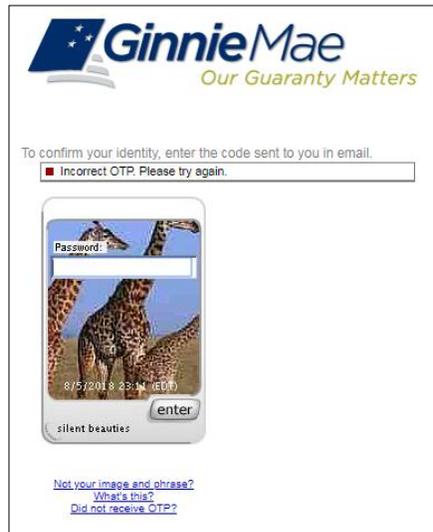


Figure 92 - Incorrect OTP Error

Resolution: Check the OTP email and verify the correct OTP has been entered. A user has three attempts to enter their OTP correctly. If the user fails three times within in ten minutes, they will require an OTP unlock performed by an Operations Administrator. Please see [Section 6.2: Help Desk](#).

4.7 OTP Not Received

Issue: A user enters their username and password and is prompted to enter their OTP, but has not received it. Please allow for a reasonable amount of time (a few minutes) for messaging and email clients to deliver the OTP notification.

Resolution: If the user has not received an email with the OTP, select the “Did not receive OTP?” link to re-send the OTP email again. If not received after a few minutes, contact an Operations Administrator to reset OTP email. Please see [Section 6.2: Help Desk](#).

4.8 Disable Pop-Up Blocker

Issue: A user enters their username and password and is prompted to enter their OTP, but has not received it. Please allow for a reasonable amount of time (a few minutes) for messaging and email clients to deliver the OTP notification.



Resolution: Disable the pop-up blocker of the internet browser being utilized. For Internet Explorer, select the Tools button and then select Internet options. On the Privacy tab, uncheck the Turn on Pop-up Blocker checkbox and select “OK”. If the OTP has still not been received after a few minutes, contact an Operations Administrator to reset OTP email. Please see [Section 6.2: Help Desk](#).

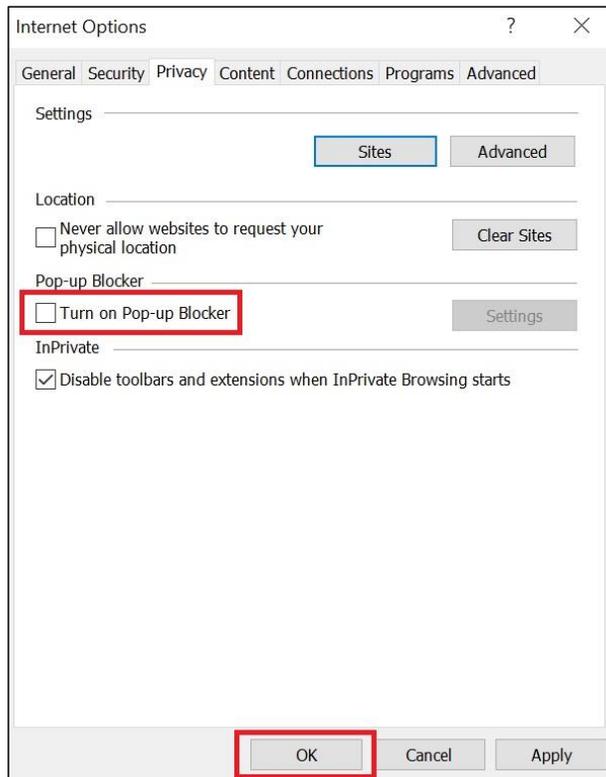


Figure 93 – Disable Pop-up Blocker



5 Reporting

MyGinnieMae provides reporting capabilities to specific administrator roles. These reports capture logs and event data for various identity and access management events.

5.1 Report Capabilities

The following reports are available to Organization Administrators.

Table 7 - Reporting for Organization Administrators

Service	Reports
User Registration	Approval Activity Request Details Request Summary User Profile History User Summary
Access Requests	Approval Activity Request Details Request Summary
Multifactor Authentication (MFA)	Accounts_Locked_Out Report Authentication Statistics Report
Self Service Change Password	Password Expiration Summary Password Reset Summary Resource Password Expiration
Application Resource Provisioning	Role Membership History Role Membership Profile Role Membership User Membership History

5.2 Report Procedures

To access the list of available reports for a user and run a report, follow the steps below.

1. Access the Access Management Console.



2. Select the “Security Reports” link in the header of the landing page.



Figure 94 - Security Reports Link

3. The system will open the BI Publisher page in a new window.
4. Select the “Catalog Folders” link on the left hand side of the page

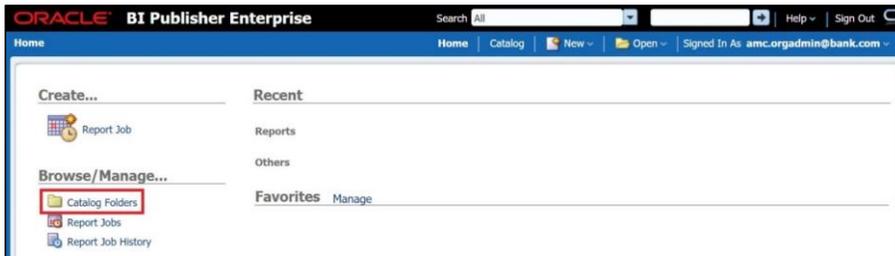


Figure 95 - Report Catalog Folders



5. Select “Oracle Identity Manager” from the list of folders on the left hand side of the page to expand the folder

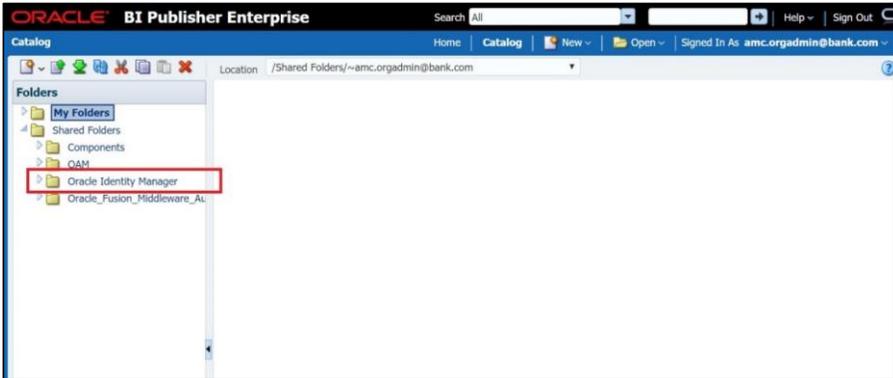


Figure 96 - Oracle Identity Manager Reports

6. Select the “User Reports” folder and then select “Open” on the desired report to run.

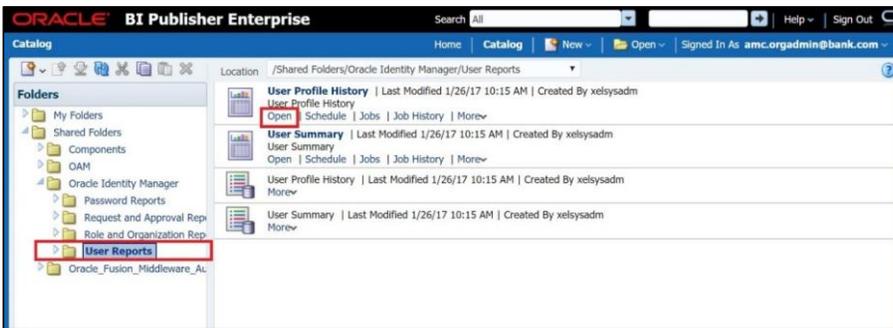


Figure 97 - Open User Profile History Report



7. The report will open and allow searching for specific users.

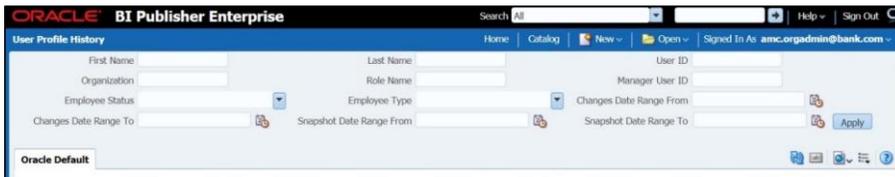


Figure 98 - Search Profile History

8. Use the available filters to generate reports for specific uses, roles, date range, etc.

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



6 Getting Help

Users should first reference the *Portal Help* link located at the bottom of MyGinnieMae Public Landing Page to troubleshoot their issue(s). If a solution is not found, the user should then seek assistance from the Ginnie Mae Help Desk according to the information provided below.

6.1 Getting More Help

The MyGinnieMae team is currently in the process of creating quick reference guides and quick reference models that can be used to help answer additional questions. To get more help, users may attend the training sessions and access the training materials on the Portal Help page as described in the training sessions.

6.2 Help Desk

The Ginnie Mae Help Desk team performs the following functions for specific user types.

Table 8 - Help Desk Functions

Help Desk Function	User Type
Sending an Invitation to Register	<ul style="list-style-type: none">Organization Admins Note: Organization Admins will be responsible for performing this task for users in their organization
Disable An Account	<ul style="list-style-type: none">Organization Admins Note: Organization Admins will be responsible for performing this task for users in their organization
Finalization of Access Requests	<ul style="list-style-type: none">All users
Lock A User Account	<ul style="list-style-type: none">Organization Admins Note: Organization Admins will be responsible for performing this task for users in their organization
Unlock A User Account	<ul style="list-style-type: none">Organization Admins Note: Organization Admins will be responsible for performing this task for users in their organization
Enable A User Account	<ul style="list-style-type: none">Organization Admins Note: Organization Admins will be responsible for performing this task for users in their organization
Update Account Attributes	<ul style="list-style-type: none">Organization Admins Note: Organization Admins will be responsible for performing this task for users in their organization



Help Desk Function	User Type
Password Reset	<ul style="list-style-type: none">Organization Admins Note: Organization Admins will be responsible for performing this task for users in their organization
Submit Access Requests	<ul style="list-style-type: none">Organization Admins Note: Organization Admins will be responsible for performing this task for users in their organization
Unlock a User's OTP	<ul style="list-style-type: none">Operations Administrators
Reset a User's OTP Email	<ul style="list-style-type: none">Operations Administrators

Help Desk team members can access the MyGinnieMae system to troubleshoot user problems and concerns. Users should contact the Ginnie Mae Help Desk at 1-800-234-GNMA (4662).



Appendix A: Key Features

Table 9 – Key Features

Services	Description
User Registration	MyGinnieMae user registration is a self-service user registration process used to collect, verify, and create a new user's identity information in MyGinnieMae, enabling the user to access MyGinnieMae and protected ecosystem. User registration provides a single identity for users accessing MyGinnieMae and protected applications. It automates the user account creation process and reduces costs.
Application Access Request Workflow	Access request workflow provides a single automated self-service interface for users to submit and approve requests for application access.
Federated Single Sign-On	Federated single sign-on is an extension of web single sign-on that reuses existing Ginnie Mae credentials to access external federated or cloud-based service providers.
Self-Service Password Management	The self-service password management feature provides the ability for an end user to change their password if known, as well as to be challenged if they have forgotten their password.
Automated Workflow	Automated workflows are logical, repeatable processes during which documents, information, or tasks are passed from one participant to another for action, according to a set of procedural rules. A participant may be a person, machine, or both. Examples of automated workflows include role-based access request processes.
Invitation Model	A service that allows Organization admins to prefill details about users such as name, and email address. Additionally, it will allow the organization admins to send out an automated invitation to the end user to expedite the registration process.



Appendix B: Reference Documents

The following table provides the names and documents relevant to the content presented within this document.

Table 10 – Reference Documents

Name	Document
MyGinnieMae Detailed Functional Role Matrix	 MyGinnieMae Detailed Functional R



Appendix C: Glossary and Key Terms

The following table provides definitions and explanations for terms and acronyms relevant to the content presented within this document.

Table 11 - Key Terms

Term	Definition
Accordion (Panel)	An Access Management Console feature that allows a section of content to be shown or hidden.
Access Management Console (AMC)	Provides a user friendly interface for administrators to initiate access requests, manage end users within their organization(s), and perform additional administrative functions.
Bank of New York Mellon (BNYM)	An American multi-national banking and financial services corporation.
Challenge Questions and Answers	A set of unique values chosen by a user upon registration. These values can be used by the system as an additional layer of security before resetting a user's password.
End User	Various types of Ginnie Mae employees, business partners, and contractors who require access to the business applications and information within the Portal, including various self-service functions.
Enterprise ID	One unique email address per end user.
Federal Identity, Credential, and Access Management (FICAM)	The Federal tools, policies, and systems that allow an organization to manage, monitor, and secure access to protected resources.
Federal Information Security Management Act (FISMA)	United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats.
Functional Role	In MyGinnieMae, users are provided access based on their business activities which are organized into meaningful access profiles called Functional Roles. Use of Functional Roles ensures users have appropriate level of access in relation to their job functions/responsibilities, enforces the least privilege principle, and makes the account provisioning/de-provisioning actions easier for Organization Administrators. These roles are grouped and vary by type (Single Family, Multi-Family, HECM, etc.).
Ginnie Mae Enterprise Portal (GMEP)	GMEP is the Ginnie Mae Enterprise Portal and the entry point for issuers, and subservicers, and document custodians to access our systems, for monthly reporting, pool transfers, managing master agreements, etc.
GinnieNET	GinnieNET is a Ginnie Mae system for issuance of mortgage-backed securities and pool certifications.



Organization Administrator Manual

Term	Definition
Home Organization	The organization that a user is employed by. In AMC, the Home Organization is set on the User Request Form Org ID field when a user is invited to register to MyGinnieMae.
U.S. Department of Housing and Urban Development (HUD)	A cabinet department in the executive branch of the United States federal government.
Multi-Factor Authentication (MFA)	A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.
MyGinnieMae	A web-based Portal that will allow users to conduct daily business activities through a single user interface.
Organization Administrator	Designates a Security Officer or Enrollment Administrator in MyGinnieMae
Organization Administrator Group	All Organization Administrators for a specific organization.
Organization Key	A unique identifier for each organization that consists of the Organization name, type, and ID.
Office of Securities Operations (OSO)	The HUD office responsible for three major business functions: Ginnie Mae Mortgage Backed Securities Operations; Ginnie Mae's Transformation and Modernization effort; and Ginnie Mae's Program Administration/Customer Outreach.
One-Time Password (OTP)	Provides an additional level security for access to Ginnie Mae business applications by receipt of a single use Password received via email.
Registration Invitation	An emailed request sent to an end user of MyGinnieMae inviting them to register to use the Portal.
Secure Image and Phrase	A security measure to ensure that users are providing credentials to a valid MyGinnieMae website.
Single Sign-On (SSO)	The ability for a user to enter the same ID and password to log onto multiple applications from MyGinnieMae such as GMEP 1.0 and GinnieNET.
Underlying Roles	Application/system roles and entitlements that comprise a Functional Role.