MyGinnieMae Portal
Access Management Console (AMC)
User Manual
for Organization Administrators

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

Ginnie Mae, Office of Securities Operations

V 2.6
### Application Details

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

### Document History

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

1 INTRODUCTION ........................................................................................................................................... 10
   1.1 Application Overview ................................................................................................................................. 10
      1.1.1 Access Management Console ............................................................................................................. 10
   1.2 Security Protocols ...................................................................................................................................... 11
   1.3 Authorized Use/Permission .......................................................................................................................... 11

2 SYSTEM PREREQUISITES ............................................................................................................................ 11

3 GETTING STARTED ......................................................................................................................................... 11
   3.1 Logging into MyGinnieMae ........................................................................................................................... 11
LIST OF FIGURES

Figure 3.1 Tools Drop-Down Menu .................................................................................. 12
Figure 3.2 Portal Warning ................................................................................................. 12
Figure 3.3 AMC Landing Page – Organization Administrator ........................................... 12
Figure 3.4 Return to MyGinnieMae Portal ........................................................................ 13
Figure 3.5 Exit Access Management Console .................................................................. 14
Figure 3.6 Outlook Rule for Organization Administrator Group Notifications ................ 16
Figure 3.7 Outlook Rule for Individual Account Notifications .......................................... 15
Figure 3.8 AMC Dropdown Menu ...................................................................................... 16
Figure 3.9 AMC Change Password Screen (Filled-In) ....................................................... 16
Figure 3.10 Password Change Successful Message .......................................................... 17
Figure 3.11 Password Failed Validation Error Message ..................................................... 17
Figure 4.1 MyGinnieMae Onboarding Workflow ................................................................. 18
Figure 4.2 Access Management Console Landing Page .................................................. 18
Figure 4.3 New User Registration Interface ...................................................................... 19
Figure 4.4 User Request Invitation Form .......................................................................... 20
Figure 4.5 New User Registration Interface ...................................................................... 20
Figure 4.6 User Registration Approval Request Notification Email .................................... 21
Figure 4.7 Access Management Console Landing Page .................................................. 21
Figure 4.8 Pending Approvals – User Registration Approval ............................................. 22
Figure 4.9 Request Title Hyperlink .................................................................................... 22
Figure 4.10 User Approval Details ..................................................................................... 23
Figure 4.11 Confirm Registration Approval Dialog Box .................................................... 23
Figure 4.12 User Registration Approval Notification Ribbon .............................................. 24
Figure 4.13 User Rejection Details .................................................................................... 25
Figure 4.14 Rejection Justification Reason Drop Down ...................................................... 26
Figure 4.15 New User Registration Rejection ..................................................................... 26
Figure 4.16 User Registration Rejection Notification ....................................................... 26
Figure 4.17 Access Management Console Landing Page ................................................ 27
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.18</td>
<td>Request Access for Others Search</td>
<td>28</td>
</tr>
<tr>
<td>4.19</td>
<td>Select Organization Key(s)</td>
<td>28</td>
</tr>
<tr>
<td>4.20</td>
<td>Request Functional Roles Selection Page</td>
<td>29</td>
</tr>
<tr>
<td>4.21</td>
<td>Functional Role Entities Overlay</td>
<td>29</td>
</tr>
<tr>
<td>4.22</td>
<td>Functional Role Entities Overlay With Status</td>
<td>30</td>
</tr>
<tr>
<td>4.23</td>
<td>Request Functional Role Review</td>
<td>30</td>
</tr>
<tr>
<td>4.24</td>
<td>Confirm Access Request</td>
<td>31</td>
</tr>
<tr>
<td>4.25</td>
<td>Role Access Request</td>
<td>31</td>
</tr>
<tr>
<td>4.26</td>
<td>Access Management Console Landing Page</td>
<td>32</td>
</tr>
<tr>
<td>4.27</td>
<td>Select User</td>
<td>32</td>
</tr>
<tr>
<td>4.28</td>
<td>Request Access Button</td>
<td>33</td>
</tr>
<tr>
<td>4.29</td>
<td>Access Request Approval Notification</td>
<td>34</td>
</tr>
<tr>
<td>4.30</td>
<td>AMC Homepage—Pending Approvals Tile</td>
<td>34</td>
</tr>
<tr>
<td>4.31</td>
<td>List of Pending Access Requests</td>
<td>34</td>
</tr>
<tr>
<td>4.32</td>
<td>Review Page for Functional Role Approval</td>
<td>35</td>
</tr>
<tr>
<td>4.33</td>
<td>Confirm Functional Role Approval</td>
<td>35</td>
</tr>
<tr>
<td>4.34</td>
<td>Request Approval Successful</td>
<td>35</td>
</tr>
<tr>
<td>4.35</td>
<td>End User Notification</td>
<td>36</td>
</tr>
<tr>
<td>4.36</td>
<td>Review Page for Functional Role Rejection</td>
<td>36</td>
</tr>
<tr>
<td>4.37</td>
<td>Reject Role Request Justification Reason</td>
<td>37</td>
</tr>
<tr>
<td>4.38</td>
<td>Access Request Rejection</td>
<td>37</td>
</tr>
<tr>
<td>4.39</td>
<td>Functional Role Rejection Notification</td>
<td>38</td>
</tr>
<tr>
<td>4.40</td>
<td>Access Request Rejection Email Notification</td>
<td>38</td>
</tr>
<tr>
<td>4.41</td>
<td>Select User</td>
<td>39</td>
</tr>
<tr>
<td>4.42</td>
<td>User Management – Disable Account</td>
<td>40</td>
</tr>
<tr>
<td>4.43</td>
<td>Confirm Disable Account</td>
<td>40</td>
</tr>
<tr>
<td>4.44</td>
<td>Disable Account Notification</td>
<td>41</td>
</tr>
<tr>
<td>4.45</td>
<td>Select Disabled User Functional Roles</td>
<td>41</td>
</tr>
<tr>
<td>4.46</td>
<td>Functional Role Missing Status</td>
<td>42</td>
</tr>
<tr>
<td>4.47</td>
<td>User Management Disabled User</td>
<td>43</td>
</tr>
</tbody>
</table>
Figure 4.48 User Management Enable Account

Figure 4.49 Confirm Enable Account

Figure 4.50 Enable Account Notification

Figure 4.51 GMEP2 User Role Enablement

Figure 4.52 Disabled Organization User Profile

Figure 4.53 Access Management Console Landing Page

Figure 4.54 Search Users Results

Figure 4.55 User Management – Lock Account

Figure 4.56 Confirm Account Lock

Figure 4.57 Lock Account Notification

Figure 4.58 Locked User Search

Figure 4.59 User Management Unlock Account

Figure 4.60 Confirm Unlock Account

Figure 4.61 Unlock Account Notification

Figure 4.62 User Management Update User Profile

Figure 4.63 Telephone Incorrect Format

Figure 4.64 Confirm User Profile Update

Figure 4.65 Update User Profile Notification

Figure 4.66 User Management Update User Profile Screen

Figure 4.67 Reset Password Button

Figure 4.68 Reset Password Form

Figure 4.69 Reset Password Notification

Figure 4.70 Access Management Console Landing Page

Figure 4.71 Select User

Figure 4.72 User Profile

Figure 4.73 Remove Functional Roles

Figure 4.74 Confirm Functional Role Removal

Figure 4.75 Functional Role Removal Notification

Figure 4.76 Functional Role Removal Notification

Figure 4.77 Functional Role Status
Figure 4.78  Functional Role Entity Status Overlay .......................................................... 63
Figure 4.79  User Management – Verify Functional Roles ............................................. 64
Figure 4.80  Verified Functional Role Status ............................................................... 65
Figure 4.81  Re-Request Functional Role ..................................................................... 66
Figure 4.82  Re-request Functional Role Status Update ............................................... 66
Figure 4.83  Re-Request Role Error .............................................................................. 66
Figure 4.84  Access Management Console Landing Page ............................................ 67
Figure 4.85  Search Users Results ............................................................................... 67
Figure 4.86  De-register OMA Button on the User Profile Page .................................. 67
Figure 4.87  Confirm De-registration of OMA as Org Admin ...................................... 68
Figure 4.88  Message of Successful De-registration ..................................................... 68
Figure 4.89  Back-End Service is Unavailable Error ..................................................... 69
Figure 4.90  Return to AMC Landing Page ................................................................. 69
Figure 4.91  Failed Access Request Submission .......................................................... 70
Figure 4.92  Failed User Registration Approval .......................................................... 70
Figure 4.93  Email is Already Registered Error ............................................................ 71
Figure 4.94  Three Invitations Sent Alert ................................................................... 71
Figure 4.95  Five Time Invitation Flag ......................................................................... 72
Figure 4.96  Registration Email Form Error ............................................................... 72
Figure 4.97  Registration Email Form Error ............................................................... 73
Figure 4.98  New Password Does Not Match Error .................................................... 73
Figure 4.99  Security Reports Link .............................................................................. 76
Figure 4.100  Report Catalog Folders ........................................................................ 76
Figure 4.101  Oracle Identity Manager Reports ......................................................... 76
Figure 4.102  Open User Profile History Report ....................................................... 77
Figure 4.103  Search Profile History ......................................................................... 77
1 INTRODUCTION

This manual is written for Organization Administrators (Org Admins) in the MyGinnieMae portal. You should use this manual for instructions on how to use the Access Management Console (AMC) in MyGinnieMae. Organization Administrators, formerly known as Security Officers and Enrollment Administrators, are privileged users who control system access, assign Functional Roles, and perform other user management activities. As a privileged user, Organization Administrators are responsible for ensuring that End Users in your organization are provided the appropriate level of access for their business role with Ginnie Mae.

The purpose of this document is to familiarize you with the Access Management Console (AMC) which hosts the functionality relevant to your role. Organization Administrators would have previously performed the Security Officer role in GMEP 1.0 or the Enrollment Administrator role in GinnieNET. For information common to all users of the portal, not specific to the Access Management Console (AMC), refer to the MyGinnieMae Getting Started User Manual.

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

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

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

Among the benefits provided by the portal to Ginnie Mae stakeholders are:

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

1.1 Application Overview

1.1.1 Access Management Console

The MyGinnieMae Access Management Console (AMC) is an application in MyGinnieMae used by Organization Administrators to register new MyGinnieMae users, to grant access to modernized business applications (for example,
the Multifamily Pool Delivery Module (MFPDM)) as well as legacy business applications (that is, GMEP 1.0 and GinnieNET), and to manage existing Portal user accounts. Security Officers and Enrollment Administrators in legacy systems, become privileged users known as Organization Administrators and utilize the AMC to manage the users within their organization.

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

### 1.2 Security Protocols

Refer to Section 1.2: Security Protocols of the MyGinnieMae Portal Getting Started Manual for descriptions of several security features in MyGinnieMae including Multifactor Authentication, Single Sign-On, SecurID Token, Automatic Logout and more.

### 1.3 Authorized Use/Permission

Refer to Section 1.3: Authorized Use/Permission of the MyGinnieMae Portal Getting Started Manual for descriptions of MyGinnieMae User Types, including Operations Administrator, Organization Administrator, and End User.

## 2 SYSTEM PREREQUISITES

Before being granted access to the MyGinnieMae Portal, the user must complete the registration process. Organization Administrators facilitate the registration and access provisioning process within each organization.

Refer to Section 2: System Prerequisites of the MyGinnieMae Portal Getting Started Manual for information on web browser compatibility and descriptions of each MyGinnieMae Functional Role.

## 3 GETTING STARTED

The following sections detail common actions taken to access and exit the Management Console (AMC). This information will be helpful to set up your email account to help segregate important messages about your individual account from Org Admin Group notifications.

### 3.1 Logging into MyGinnieMae

Refer to the Logging into MyGinnieMae & Accessing Business Applications QRC for step-by-step instructions on how to log into the portal or the Section on Logging into MyGinnieMae in the MyGinnieMae Portal Getting Started Manual.
3.2 Navigating to the Access Management Console

The Access Management Console (AMC) is the user interface to manage user accounts and retrieve system audit reports for your organization. To navigate to the AMC:

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

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

3. The system will open the AMC in a new browser window.
3.3 Exiting the Access Management Console

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

3.3.1 Exiting AMC and Returning to MyGinnieMae

1. To exit the Access Management Console and navigate back to My Dashboard in the portal.
   a. Select down arrow beside Links on the toolbar at the top of the page.
   b. Select MyGinnieMae Portal

![Return to MyGinnieMae Portal](image)

3.3.2 Exiting AMC and MyGinnieMae

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

**NOTE**: If you have any legacy system sessions open in other windows those sessions must be exited separately to securely end all portal activity.
1. To exit the Access Management Console, simultaneously closing the Portal session,
   a. Select the down arrow beside the username on the toolbar at the top of the page
   b. Select **Sign out**

![Access Management Console](image)

Figure 3.5 Exit Access Management Console

**NOTE**: Upon signing out of the AMC, the portal session is terminated. To return, you will need to follow the login steps in the [Logging into MyGinnieMae & Accessing Business Applications QRC](#).

### 3.4 Outlook Rules for Email Notifications

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

#### 3.4.1 Outlook Rule for Organization Administrator Group Notifications

Each Organization Administrator will receive several notifications relating to registration and access workflow items for each End User in your organization. If you would like to automatically move those notifications from your Microsoft Outlook Inbox to a designated folder, the following criteria will assist. For detailed instructions on creating a Rule in Microsoft Outlook visit Microsoft Office Support at [https://support.microsoft.com/en-us](https://support.microsoft.com/en-us) and search “Manage email messages by using rules”.

**Criteria:**

- **From**: donotreply_access@ginniemae.gov
- **Subject contains**: "Action Required: User Registration Request for Approval"
"Action Required: Access Request for Approval"
"New Functional Role Assignment"
"Action Required: RSA Token Role Assignment"

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

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

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

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

![Outlook Rule for Individual Account Notifications](image-url)

**Figure 3.6 Outlook Rule for Individual Account Notifications**
3.4.2 Change Password via the AMC

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

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

![AMC Dropdown Menu](image)

Figure 3.7 AMC Dropdown Menu

2. Select **Change Password**.

3. The system redirects to the Change Password screen.
   a. Enter the **Current Password**
   b. Enter the **New Password** (Must comply with the Password Policy)
   c. **Confirm New Password**
   d. Select **Submit**.

![AMC Change Password Screen](image)

Figure 3.8 AMC Change Password Screen (Filled-In)

4. A message will display confirming the password change was successful. You can then select “Return to Portal” to proceed.
NOTE: If you enter the incorrect current password, you will receive an “At least one of the provided passwords failed validation” error message.

**Figure 3.10** Password Failed Validation Error Message

### 4 USING THE APPLICATION

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

#### 4.1 Onboarding End Users - Registration & Access Workflow

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

**NOTE:** Separation of duties within the Registration and Access Workflows do not allow you to initiate a registration and approve that same registration or request a Functional Role access assignment and approve that same access request. A minimum of two Organization Administrators is therefore required. From an operational perspective, it is recommended that an organization have at least three Organization Administrators.
4.1.1 New User Registration

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

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

   ![Access Management Console Landing Page](image)

4. The system opens the New User Registration interface in a new window.
   a. Select **Applications** from the menu on the left
   b. Select **User Registration** to open the User Invitation form in a new window.
Figure 4.3 New User Registration Interface

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

5. Complete the following fields in the User Request Form:
   - Title
   - First Name (alphabetic, hyphen, or underscore only)
   - Middle Name (optional, alphabetic, hyphen, or underscore only)
   - Last Name (alphabetic, hyphen, or underscore only)
   - Job Title (do not enter a job title greater than 30 characters)
   - Org ID dropdown (Org Admins will only see Org IDs for which they have been assigned the privileged role to perform user access and management functions)
   - Email (use only lower-case characters to register; not mixed or upper case). The email domain is validated against a whitelist of valid domains based on organizations with which Ginnie Mae works. If domain changes are needed for an organization, contact [Ginnie Mae Customer Support](#).

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

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

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

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

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

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

Figure 4.6 User Registration Approval Request Notification Email

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

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

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

4. Review the table under the “User Registration Approval” accordion which displays the list of available registration requests awaiting approval.
5. Select Request Title hyperlink for the desired End User to begin the approval of the registration request.

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

6. Review the user approval details for accuracy. If the details are correct, select Approve Registration.
**NOTE:** Some User Registration fields are not editable for the approving Organization Administrator. If there are any errors or incorrect information in the request, follow the steps to reject the request in [Reject a New User Registration](#). Then work with the requesting Organization Administrator and the affected End User to submit a new registration beginning with the steps in [New User Registration](#).

![User Approval Details](image)

**Figure 4.10** User Approval Details

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

![Confirm Registration Approval Dialog Box](image)

**Figure 4.11** Confirm Registration Approval Dialog Box
The system submits the approval task and reopens the “Pending Approvals” screen, displaying the “User registration request #XXXXXX approved successfully” green notification ribbon.

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

![Figure 4.12 User Registration Approval Notification Ribbon](image)

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

### 4.1.3 Reject a New User Registration

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

1. Follow the instructions for [Logging into MyGinnieMae](#).
2. [Navigate to the Access Management Console](#).
3. Select **Pending Approvals** tile.
4. Review the table under the “User Registration Approval” accordion which displays the list of available registration requests awaiting approval.
5. Select **Request Title** hyperlink for the desired End User.
6. Select **Reject Registration**.
7. The system displays a Confirmation Registration Reject dialog box for the rejection justification reason. This required field has the following options:
   - User No Longer with Organization
   - Do Not Recognize User
   - User already has an existing account
   - Invitation sent to incorrect email address
   - Other – Please Explain (the Justification Description will be required)
8. Choose the Justification Reason
   a. If required, enter a Justification Description.
   b. Select **Confirm** to send the rejection to the system.

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

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

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

1. **Request Function Role from Access Management Tile**

To request access through the Access Management tile:

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

![Access Management Console Landing Page](image)

4. The system displays a table which contains the list of all registered users within the organization(s) the Org Admin manages. From the table,
   
   a. Select the hyperlink for the Display Name of the End User needing a Functional Role.
NOTE: Users are listed in alphabetical order by Last Name. The table can be sorted or searched across any of the fields—Display Name, Email, or Home Organization.

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

6. The system displays a list of Functional Roles available for the selected Home Organization.
   a. Select the checkbox next to each Functional Role(s) to be requested for the user.
   b. Select Assign Roles to confirm the selections.

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

If the Functional Role has already been requested for the user, it will not be displayed in the table to select. Already assigned or requested Functional Roles are listed under the table at the bottom of the request screen.
NOTE: Selecting on the Functional Role title within the Functional Role Table will open the Functional Role Entities overlay. The overlay contains information about which entities (systems, applications, and functions) are included in the role.
NOTE: Selecting the Functional Role title within the Currently Assigned Roles section will open the Functional Role Entities Status overlay. The overlay contains information about the status of functional roles currently pending, approved, or finalized for the user.

![Functional Role Entities Overlay](image)

**Figure 4.22 Functional Role Entities Overlay With Status**

7. The system displays a review page with the requested Functional Role(s) and the underlying entities that make up that Functional Role(s).
   a. Select **Submit**.

![Request Functional Role Review](image)

**Figure 4.23 Request Functional Role Review**

8. The system displays an access request confirmation dialog box.
   a. Select **Confirm** to submit the roles for approval.
**NOTE:** After confirmation, the access request is submitted. The system displays a loading bar at the top of the page to indicate the submission is processing. **DO NOT RESUBMIT.** Navigational buttons can be used to move to another screen but a resubmit should not be performed.

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

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

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

(2) Request Functional Role from the User Management Tile

To request access through the User Management tile:
1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.

![Access Management Console](image)

**Figure 4.26 Access Management Console Landing Page**

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

![User Management](image)

**Figure 4.27 Select User**

5. Once the "User Profile" screen opens,
   a. Select down arrow next to Edit User Profile down arrow.
   b. Select Request Access.

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

**NOTE:** The “Request Access” button will be disabled if the user's profile attributes are incomplete or incorrectly formatted.
6. The system directs the user to the Organization screen of the Access Request workflow where you can follow steps 5 - 9 of Request Functional Role from Access Management Tile to request functional role access.

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

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

1. Follow the instructions for [Logging into MyGinnieMae](#).
2. Navigate to the Access Management Console.
3. Select Pending Approvals tile.

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

4. Review the table under the “Access Request Approval” accordion (collapsible section) which displays the list of available access requests pending approval.
   a. Select the Request ID for the Functional Role request that corresponds to the desire End User.
5. The details of the requested Functional Role display in the Review Page.
   a. Review the request details.
   b. Select Approve to activate the confirmation message.

![Review Page for Functional Role Approval](image)

**Figure 4.32** Review Page for Functional Role Approval

6. Select Confirm to submit the approval.

![Confirm Functional Role Approval](image)

**Figure 4.33** Confirm Functional Role Approval

7. The system displays a green confirmation ribbon at the top of the screen when the request has been approved successfully.

![Request Approval Successful](image)

**Figure 4.34** Request Approval Successful
NOTE: If the request has not been approved successfully, review the error message, and attempt to re-approve if possible. If the error persists, contact the Ginnie Mae Customer Support. If an error occurs upon approval, the current selection(s) and/or page within the module are retained.

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

![New Functional Role Assignment](image)

Figure 4.35 End User Notification

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

4.1.6 Reject a Functional Role Access Request

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

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

![Access Request Approval](image)

Figure 4.36 Review Page for Functional Role Rejection
6. The system displays a Confirmation Rejection of Role Request dialog box for the rejection justification reason. This required field has the following options:
   - Access Does Not Enforce Least Privilege
   - Incorrect Functional Role Requests
   - User No Longer with Organization
   - Do Not Recognize User
   - Access Violates Separation of Duties
   - Other – Please Explain (the Justification Description will be required)

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

![Figure 4.37 Reject Role Request Justification Reason](image)

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

![Figure 4.38 Access Request Rejection](image)
9. The system will display a green notification ribbon to indicate the Functional Role rejection was successful.

![Functional Role Rejection Notification](image)

**Figure 4.39 Functional Role Rejection Notification**

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

![Access Request Rejection Email Notification](image)

**Figure 4.40 Access Request Rejection Email Notification**

### 4.2 Managing and Maintaining User Accounts

#### 4.2.1 Disable a User Account

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

To disable an account, follow the steps below.

1. Follow the instructions for [Logging into MyGinnieMae](#).
2. [Navigate to the Access Management Console](#).
3. Select [User Management tile](#).
4. The system displays a list of available users. Search for a user by typing one of the following user properties into the search field to locate the desired End User:
   - Display Name
   - Email
   - Home Organization

5. Select the Display Name for the desired user.

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

8. The system displays a “User [User Name] successfully disabled” green notification ribbon and updates the Account Status to “Disabled.” No additional approval is required when disabling a user account. When a user is disabled, the system removes all Functional Roles provisioned to the user.
9. Reselect the “Manage User Permissions” down arrow to confirm the Functional Roles have been removed from the user; the Status will display as Revoked.
4.2.2 Enable a User’s Account

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

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

**NOTE:** If the user was disabled due to 90 days of inactivity, the system will display the user’s Functional Roles as “Missing.” See screenshot below. To re-request a Function Role for a user who was disabled due to 90 days of inactivity, see [Re-Request a Functional Role](#).

![Figure 4.46 Functional Role Missing Status](image)

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

1. Follow the instructions for [Logging into MyGinnieMae](#).
2. Navigate to the Access Management Console.
3. Select **User Management** tile.
4. Verify the user is disabled by confirming that there is a disabled icon (-disabled) to the left of their Display Name.
   a. Select the Display Name of the user to enable.
5. Once the "User Profile" page opens, select the “Enable” button in the bottom right of the “Edit User Profile” accordion.

6. The system displays an overlay to confirm the enabling of the selected user’s account.
   a. Select Confirm to submit the request.
7. The system displays a “User [User Name] successfully enabled” message and updates the Account Status as “Enabled.” Follow the steps in Section: Request Functional Role to begin the workflow for assigning roles.

**NOTE:** If the user previously had two or more Functional Roles that included the GMEP2_User role, the GMEP2_User role status may only be updated in one. Upon verification (see Verify an Assigned Functional Role), the status will update accurately.
Functional Role Entity Status

<table>
<thead>
<tr>
<th>DISPLAY NAME</th>
<th>Request Date</th>
<th>Requester</th>
<th>Approval Date</th>
<th>Approver</th>
<th>Finalized Date</th>
<th>Finalizer</th>
<th>Status</th>
</tr>
</thead>
</table>

Table 4.51 GMEP2 User Role Enablement

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

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

![User Management Profile](image)

Figure 4.52 Disabled Organization User Profile
4.2.3 Lock a User’s Account

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

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

![Access Management Console Landing Page](image)

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

![Search Users Results](image)

5. Select the “Edit User Profile” down arrow
   a. Select Lock.
6. The system opens a dialog box to confirm the account lock.
   a. Review the user details.
   b. Select Confirm.

![Confirm User Lock](image)

Figure 4.56 Confirm Account Lock

7. The system displays a “User [UserName] successfully locked” green notification ribbon message and updates the Account Status to “Locked.”
4.2.4 Unlock a User’s Account

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

- Locked out by the Organization Administrator
- Three failed attempts to enter correct username and password

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

1. Follow the instructions for [Logging into MyGinnieMae](#).
2. Navigate to the [Access Management Console](#).
4. Find and select the Display Name of the user account.
5. Select the “Edit User Profile” down arrow
   a. Select Unlock.

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

b. Select **Confirm**.

![Confirm User Unlock](image)

**Figure 4.60 Confirm Unlock Account**

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

![Unlock Account Notification](image)

**Figure 4.61 Unlock Account Notification**
4.2.5 Update a User’s Profile Attributes

End Users have limited ability to update their own Profile Attributes which include, mobile number, fax, job title, start date, job functions, and professional background summary. All other account attributes must be updated by the Organization Administrator. Follow the steps below to update any of the following user’s account attribute information.

- Title (Mr., Mrs., etc.) [required attribute]
- Suffix
- Mobile Number
- Work Number [required attribute]
- Extension
- Job Title [required attribute]
- Does this user have an RSA token? (Y/N)
- RSA Token Serial Number (See Update a User’s RSA Token.)

**NOTE:** If the user’s email address has changed, a new End User account must be created. Contact [Ginnie Mae Customer Support](#) for assistance.

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

   a. Edit the fields for desired user attributes
   b. Select Save.

**NOTE:** The “Save” button is not displayed unless an attribute has been edited.

The “Save” button is not displayed unless an attribute has been edited.
Figure 4.62 User Management Update User Profile

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

Telephone numbers must be in the (555) 555-5555 format, and the number and area code cannot begin with a 1 or a 0.
The system displays a dialog box to confirm the updated attributes.

a. Select **Confirm**

![Confirm User Update](image)

A “User [User Name] successfully updated” green notification ribbon displays.
4.2.6 Update a User’s RSA Token Information in MyGinnieMae

(1) Update an Existing Token Holder

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

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

2. Refer to Update User’s Profile Attribute above.
3. Update the following fields in the User Management Update User Profile screen.

Figure 4.66 User Management Update User Profile Screen

(2) Update a New Token Holder

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

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

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

4.2.7 Reset a User's Password

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

1. Follow the instructions for Logging into MyGinnieMae.
2. **Navigate to the Access Management Console.**
3. Select **User Management** tile.
4. Find and select the Display Name of the user account.
5. Select **Reset Password.** **NOTE:** This button is inactive if the user is disabled.
6. The system opens a dialog box to confirmation that an auto-generated temporary password will be sent to the user.
   a. Select **Confirm**.

   ![Confirm Password Reset]
   
   **Figure 4.68 Reset Password Form**

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

If an End User no longer requires access to a specific Functional Role, possibly because their business responsibilities have changed, Organization Administrators are responsible for removing that role from the user’s account. To remove a role from an End User account, follow the steps provided below.

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
4. The system displays a list of available users. Search for a user by typing one of the following user properties into the search field to locate the desired End User:
   - Display Name
   - Email
   - Home Organization

![User Management](image)

Figure 4.71  Select User

5. The system displays the User Profile page.
   a. Select the down arrow next to “Manage User Permissions” to display the roles assigned to the user.
6. Review the listed roles for the user,
   a. Select the check box for the Functional Role to be removed.
   b. Select **Remove**.
7. The system displays a confirmation message.
   a. Select **Confirm** to proceed with the removal of the selected Functional Role.

![Confirm Remove Functional Role](image)

**Figure 4.74 Confirm Functional Role Removal**

8. The system displays a success green notification ribbon at the top of the page.
9. When the role has been successfully removed, the status of the role changes to “REVOKED.” No additional approvals are required after the removal is confirmed.

NOTE: If a Functional Role is removed inadvertently, it can be requested again by following the steps in Request Functional Role.
4.2.9 Review the Status of a Functional Role Access Request

Once an access request is submitted, the system adds the Functional Role to the user’s profile with a status of “Pending.” The role is not provisioned to the End User until all necessary approvals are completed. To review the status of a Functional Role request for a user, follow the steps below.

1. Follow the instructions for Logging into MyGinnieMae.
2. Navigate to the Access Management Console.
4. Find and select the Display Name of the user account.
5. Select the down arrow next to “Manage User Permissions”. The system displays the Functional Role(s) assigned with various statuses indicating the state of the request in the Access Request Workflow:
   - PENDING – The Functional Role request is submitted and awaiting Organization Administrator approval.
   - APPROVED – The Functional Role is approved and awaiting Operations Administrator action.
   - FINALIZED – The Functional Role request has been finalized by the Operations Administrator and the underlying roles are in the process of being assigned to the user.

![Functional Role Status](image)

Figure 4.77 Functional Role Status
6. Select the “Role Name” to reveal the Functional Role Entity Status overlay. The overlay contains details about the user’s Functional Role(s):

- Request Date
- Requester
- Approval Date
- Approver
- Finalized Date
- Finalizer
- Status

![Functional Role Entity Status Overlay](image)

**Figure 4.78 Functional Role Entity Status Overlay**

### 4.2.10 Verify an Assigned Functional Role

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

1. Follow the instructions for [Logging into MyGinnieMae](#).
2. Navigate to the Access Management Console
4. Find and select the Display Name of the user account.
5. Select the down arrow next to “Manage User Permissions” to display the roles assigned to the user.

   - Select the checkbox for the corresponding Functional Role(s) from the list.
   - Select **Verify**.
6. The system checks the user’s access to underlying roles against the Functional Role profile and displays the updated “Status” of the Functional Role.

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

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

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

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

- PARTIAL – NO ACCOUNT—The legacy system (GMEP or GinnieNET) has not returned a legacy ID for a requested legacy role. (NOTE: If Legacy provisioning has not been fully completed before the user verifies, this status will be displayed. Provisioning should complete within 25 minutes after an Operations Administrator completes finalization. If the status is still “PARTIAL – NO ACCOUNT” after 25 minutes, the Organization Administrator should reach out to the Operations Administrator for troubleshooting and investigation).

- FAILED—The request did not complete successfully.

- REVOKED—The Functional Role was previously provisioned for the End User and has been removed or the requested role was rejected by the second Organization Administrator. A revoked role can be requested again through the Workflow.
If the “Status” is not “CONFIRMED,” the role can be re-requested following the steps in **Re-Request a Functional Role**.

### 4.2.11 Re-Request a Functional Role

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

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

**NOTE:** The “Re-Request” button will not be visible for a role whose status is listed as Revoked. To re-request a revoked role for a user, follow the Request Access Workflow in **Request Functional Role**.
7. The system submits a request for any missing Functional Role entities, displays a notification ribbon at the top of the screen, and updates the status of the role.

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.

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

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

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

![Access Management Console Landing Page](image1)

Figure 4.84 Access Management Console Landing Page

5) Select De-register OMA.

![Search Users Results](image2)

Figure 4.85 Search Users Results

![De-register OMA Button on the User Profile Page](image3)

Figure 4.86 De-register OMA Button on the User Profile Page
6) The system opens a dialog box to confirmation the de-registration of the OMA.
   a) Select **Confirm**.

   ![Figure 4.87 Confirm De-registration of OMA as Org Admin](image)

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

   ![Figure 4.88 Message of Successful De-registration](image)

### 4.3 Troubleshooting and System Errors

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

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

![Back-End Service is Unavailable Error](image)

**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.

![Return to AMC Landing Page](image)

4.3.2 AMC Module Error Notification Ribbons

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

**Issue:** If the backend system does not receive the confirmed action, an error message is displayed with notification of the failed action.
**Resolution:** Re-attempt the action. If failures continue contact [Ginnie Mae Customer Support](https://www.ginnie Mae.gov/custsupport).
4.3.3 Email is Already Registered

**Issue:** When sending a New User Registration invitation to an End User, if an email address is already registered, an invitation cannot be sent to that user.

![Figure 4.93 Email is Already Registered Error](image)

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

4.3.4 Three Invitations Sent Alert

**Issue:** When sending a New User Registration invitation to an End User, if an invitation has already been sent to the user’s email address three times, an alert will be displayed as a warning. An invitation can only be sent a total of five times.

![Figure 4.94 Three Invitations Sent Alert](image)

**Resolution:** This is a warning message. No action is required as an invitation can be sent up to five times.
4.3.5 Five-Time Invitation Flag

**Issue:** When sending a New User Registration invitation to an End User, if an invitation has already been sent to the user’s email address a total of five times, the email address will be flagged, and additional requests cannot be sent.

![Five Time Invitation Flag](image)

**Resolution:** In order to send another invitation to the user’s email address, action is required from the Operations Administrator group. Contact [Ginnie Mae Customer Support](#).

4.3.6 Incorrect Email Format

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

![Registration Email Form Error](image)

After the steps above, if a correct email format is entered and the” Submit” button is clicked, the following error is displayed: “ADF_FACES…”. The registration page then displays the 500-error shown below.
Resolution: When an incorrect email format is entered and the “Error: This format is incorrect” appears, close the User Registration Form, and follow the steps to start a new registration invite. Do not proceed to populate the same registration invitation form after seeing this error.

4.3.7 New Password Mismatch Error

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

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

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

#### 4.4.1 Report Types

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

<table>
<thead>
<tr>
<th>Service</th>
<th>Reports</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| User Registration | Home Organization User List Org Admin View  
User Profile History  
User Registration Request History | Custom      | Home Organization User List Org Admin View – Provides a list of all users in your organization including phone number, job title, date the user’s account was created, current status (active or disabled), the last date the user logged in and if the account is currently locked. You can also see if the user has an RSA token. If the user has an token, you can see the RSA serial number.  
User Profile History Org Admin View – Provides users login audit information in your organization including last login date, Created By Login, Updated By Login, user id status etc. including Date Effective From, Time Effective From.  
User Registration Request History Org Admin View – Provides a list of user registration information for both completed registrations and registrations that have not been completed. Information that is provided for completed registrations include the request ID, user login, the Org Admin who sent the registration invitation to the user, the date the invitation was sent, the date the registration request was submitted by the user, the Org Admin who approved the registration request, the date the request was approved and the approval status. For registrations that have not been completed the task number, user login, the Org Admin who sent the registration invitation, the date the invitation was sent and the status of the invitation. |
<p>| Access Requests | AMC Functional Role Request History | Custom      | AMC Functional Role Request History – Provides the functional role request history for your organization. The information provided includes the request ID, user login, functional role type, Org key, Status, the Org Admin who submitted |</p>
<table>
<thead>
<tr>
<th>Service</th>
<th>Reports</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multifactor Authentication (MFA)</td>
<td>Accounts Locked Out Report</td>
<td>Standard</td>
<td>Provides a list of all locked users in your organization including user id, time stamp when the account was locked.</td>
</tr>
<tr>
<td></td>
<td>Authentication Statistics Report</td>
<td>Standard</td>
<td>Provides the number of times and the dates the authentication process was attempted by the users in your organization. You have the ability to sort by date range or time range. You can also sort by authentication success, failure or all.</td>
</tr>
<tr>
<td>Self-Service Change Password</td>
<td>Password Expiration Summary</td>
<td>Standard</td>
<td>Provides a list of the users in your organization whose passwords have expired. You have the ability to sort by first name, last name, user ID. You can also sort by date range.</td>
</tr>
</tbody>
</table>

Table 4.1 Reporting for Organization Administrators

4.4.2 Accessing Administrative Reports

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

1) Follow the instructions for Logging into MyGinnieMae.
2) Navigate to the Access Management Console
3) Select the down arrow next to Links in the header.
   a) Select Security Reports
4) The system will open the BI Publisher Enterprise page in a new window.
   a) Select Catalog Folders on the left side of the page.

5) Select Shared Folders to expand the folder.
6) Select Administrative Reports folder.

![Image of Oracle BI Publisher Enterprise]

**Figure 4.102 Open User Profile History Report**

7) The reports will be displayed.
   a) Select Open under the desired report.

8) For Custom Reports,
   a) The report can be filtered and sorted by selecting the down arrow in the column header.

9) For Standard Reports,
   a) Search for specific users using the User Profile History.
   b) Filter to generate reports by users, roles, date range, etc.

![Image of Oracle BI Publisher Enterprise]

**Figure 4.103 Search Profile History**

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

---

5 Getting Help

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

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

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

Easy reference tools like Quick Reference Cards (QRCs) and the Portal Help link at the bottom of each portal page, can be used to help answer common questions. To get more help, users may access the training sessions and materials on the Issuer Training Page of the Ginnie Mae website at https://www.ginniemae.gov/issuers/issuer_training/pages/modernization.aspx.

5.2 Organization Administrators
Organization Administrators, formerly known as Security Officers and Enrollment Administrators, are privileged users inside each Ginnie Mae business partner organization that are responsible for creating and managing End User accounts in Ginnie Mae systems on behalf of their organization. Organization Administrators are responsible for the following functions:

- Create an End User Account
- Update Account Attributes such as an RSA Token
- Reset Password
- Add/Remove Functional Roles for an End User Account
- Disable/Enable An End User Account
- Lock/Unlock An End User Account

End Users that need their One-Time PIN (OTP) reset or have questions about how to use portal applications should seek assistance from Ginnie Mae Customer Support.

5.3 Ginnie Mae Customer Support
Ginnie Mae Customer Support may be reached at:

1-833-GNMA HELP / 1-833-466-2435
ginniemae1@bnymellon.com
5.3.1 Help with System Access

The Operations Administrators for the MyGinnieMae portal may be reached via Ginnie Mae Customer Support. The Operations Administrators are responsible for creating and managing Organization Administrator accounts. The Operations Administrator is not authorized to create or otherwise manage End User accounts for Ginnie Mae business partners but may support Organization Administrators in their role to manage End User accounts on behalf of their organization.

5.3.2 Help with Portal Applications

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

5.4 MyGinnieMae Portal Dictionary

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

6 APPENDIX

6.1 Functional Role Matrix

Functional Roles are a system access profile based on business activities used to ensure End Users have the appropriate level of access to be able to perform their job functions and responsibilities. Functional roles are grouped and vary by type (refer to the Functional Role Matrix at https://www.ginniemae.gov/issuers/issuer_training/Documents/functional_role_matrix.pdf).

7 QUICK REFERENCE CARDS

A Quick Reference Card or QRC is an abbreviated one to two-page reference document with step-by-step instructions on how to complete a specific action. Below is a list of QRCs for the content provided in this User Manual. QRCs are posted to the Ginnie Mae website at https://www.ginniemae.gov/issuers/issuer_training/pages/qrcs.aspx.
<table>
<thead>
<tr>
<th>User Manual</th>
<th>QRC#</th>
<th>QRC Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:3.2</td>
<td>Navigating to the Access Management Console</td>
<td>QRC for Organization Administrators on how to navigate to the Access Management Console from MyGinnieMae.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:3.3</td>
<td>Exiting the Access Management Console</td>
<td>QRC for Organization Administrators on how to exit the Access Management Console and return to MyGinnieMae. The QRC also explains how to exit both the Access Management Console and MyGinnieMae.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:3.4.3</td>
<td>Change Password Via Access Management Console</td>
<td>QRC for Organization Administrators to change their password within the Access Management Console rather than navigating back to the MyGinnieMae landing page.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.1.1</td>
<td>Send a Registration Invitation</td>
<td>QRC for Organization Administrators on how to send a Registration Invitation email to someone so they can register to become a MyGinnieMae end user.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.1.2</td>
<td>Approve a New User Registration</td>
<td>QRC for Organization Administrators on how to Approve a New User Registration.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.1.3</td>
<td>Reject a New User Registration</td>
<td>QRC for Organization Administrators on how to reject a New User Registration.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.1.4.1</td>
<td>Request a Functional Role from the Access Management Tile</td>
<td>QRC for Organization Administrators on how to submit a Functional Role request for someone through the Access Management tile in the Access Management Console.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.1.4.2</td>
<td>Request a Functional Role from the User Management Tile</td>
<td>QRC for Organization Administrators on how to submit a Functional Role request for someone through the User Management tile in the Access Management Console.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.1.5</td>
<td>Approve a Functional Role Request</td>
<td>QRC for Organization Administrators on how to approve a Functional Role request.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.1.6</td>
<td>Reject a Functional Role</td>
<td>QRC for Organization Administrators on how to reject a Functional Role request.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access Management Console</th>
<th>QRC-AMC:4.2.1</th>
<th>Disable a User’s Account</th>
<th>QRC for Organization Administrators on how to remove a user’s MyGinnieMae account. This will remove all the user’s assigned functional roles.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.2.2</td>
<td>Enable a User’s Account</td>
<td>QRC for Organization Administrators on how to enable a user’s account so they can access MyGinnieMae.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.2.3</td>
<td>Lock a User’s Account</td>
<td>QRC for Organization Administrators on how to prevent a user from logging in to their MyGinnieMae account, but still retain their functional roles.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.2.4</td>
<td>Unlock a User’s Account</td>
<td>QRC for Organization Administrators on how to unlock a user’s account so they can login to their MyGinnieMae account.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.2.5</td>
<td>Update a User’s Profile</td>
<td>QRC for Organization Administrators on how to update a user’s profile information such as title, work number, extension etc.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.2.6</td>
<td>Update a User’s RSA Token</td>
<td>QRC for Organization Administrators with the steps to follow when you receive a notification that a Functional Role requires an RSA association.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.2.7</td>
<td>Reset a User’s Password</td>
<td>QRC for Organization Administrators on how to reset a password for a user when they have forgotten their password or cannot reset it themselves.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.2.8</td>
<td>Remove Functional Roles</td>
<td>QRC for Organization Administrators on how to remove a Functional Role when a user no longer requires the access.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.2.9</td>
<td>Review Functional Role Request Status</td>
<td>QRC for Org Admin to check the status of a Functional Role that has been requested for a user in your organization.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.2.10</td>
<td>Verify an Assigned Functional Role</td>
<td>QRC for Organization Administrators on how to verify that all the necessary underlying roles</td>
</tr>
</tbody>
</table>
have been assigned to the user’s account once the request has been finalized.

<table>
<thead>
<tr>
<th>Access Management Console</th>
<th>QRC-AMC:4.2.11</th>
<th>Re-Request a Functional Role</th>
<th>QRC for Organization Administrators that need to re-request Functional Roles.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.2.12</td>
<td>De-Register a User with the Oracle Mobile Authenticator</td>
<td>QRC for Organization Administrators on how to de-register a user’s smart device with the Oracle Mobile Authenticator so they can register a new smart device.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.3</td>
<td>AMC Troubleshooting-System Errors</td>
<td>QRC for Organization Administrators on how to resolve common system errors with the Access Management Console.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>QRC-AMC:4.4</td>
<td>Accessing Administrative Reports</td>
<td>QRC for Organization Administrators on how to access Administrative Reports in the Access Management Console.</td>
</tr>
</tbody>
</table>

Table 7.1 Organization Administrator QRCs