Best Practices for Administrators

This document provides recommended best practices for Corporate Administrators ("CAs") and User Administrators ("UAs") (collectively, "Administrators") who manage users' access to Fannie Mae ("FM") technology on behalf of the organizations they represent. The document includes an overview of Technology Manager ("TM") and covers the following: registering and modifying roles, creating and managing user profiles, tips for reviewing Administrator access, protecting user credentials, password expiration and other topics.

What is Technology Manager?

TM allows you to create and manage user-level access to selected FM technology applications. To access TM, Administrators will use their TM user ID and password. Please refer to Technology Manager: What is Technology Manager? for further information.

How to Register or Modify a User Administrator

Authorized representatives from your organization may register a new UA role, as well as update an existing one. In either instance, the representative must agree to be responsible for any actions taken by an Administrator using TM and to periodically review and confirm the status of each Administrator. Please see Technology Manager: Administration Management User Administrators for further information.

User Administrator Profile Maintenance

TM's Edit My Profile feature allows you to edit your profile, including contact, security and password information. See the Edit Your Profile job aid for further instructions on how to update this data.

Creating and Managing User Profiles

As an Administrator, you can use TM to create and manage user profiles and authorize user access to specific FM applications. You will create a profile for each user, authorize users' access to FM applications and assign roles and data folders. You can also grant Administrator privileges. Please see the Manage Users job aid for CAs at Technology Manager: Administration Management Corporate Administrators or for UAs at Technology Manager: Administration Management for User Administrators Non Lenders job aids for guidance on how to perform these actions.

Creating and Managing System IDs

System IDs are intended to facilitate system-to-system transactions and are not intended to be used to access browser-based UI applications. System ID passwords expire every 365 days and a System ID will be locked if the associated password is not reset prior to its scheduled expiration date. You can create and manage System IDs from within TM by selecting the 'Manage System IDs' function from the dashboard. After doing so, you may perform the following actions:

- Create a new System ID in a user group;
- Grant or remove access to a FM application that is associated with a System ID;
- Change the password associated with a System ID; and

- Deactivate and reactivate a System ID.

Please see Technology Manager: Managing System IDs with the Corporate Administrator Role for step-by-step instructions.

Policy for User IDs and Systems IDs

Please refer to Technology Manager: Policy for User IDs and System IDs for details and best practices regarding use of User IDs and System IDs.

Managing IP Address Restrictions

Administrators may be responsible for managing their organization's IP address restrictions, which is an optional feature that organizations can use to validate user and system access. When a User ID or System ID is used to access a FM application, the origination IP address associated with the access request is validated against the list of allowable IP addresses provided by the organization before the requested access can be granted. Please see IP Address Restrictions FAQs for further details.

User Reports in TM

Three user reports are available to help you manage your users' access and password issues more efficiently:

- **User Access Report:** Provides information about users' access to FM applications. This report can be customized, based on user group, active/deactivated status, and application name.
- **Locked User Report:** Lists all users that are currently unable to access FM applications.
- **Projected Inactivity and Password Expiration Report:** Lists those users who FM anticipates will be prevented from accessing its applications due to inactivity. This report can be customized, showing only those users whose access is expected to be locked within a specified number of days.

For more detailed information regarding TM user reports, please see Technology Manager: Generate a Project Inactivity and Password Expiration Report (CA).

User Access Review Tips for Administrators

FM recommends that organizations review each employee's access to FM applications on a regular basis to ensure that such access remains secure and is consistent with the employee's current job responsibilities.

Why is it important to review user access?

Regulatory compliance requirements and information security policies increasingly demand that organizations maintain effective controls over who has access to sensitive corporate and customer data. Complying with these requirements can be challenging, as users often have unique and changing business responsibilities, and, over time, may retain access to applications that they no longer need. Reviewing user access on a regular basis helps an organization to comply with its compliance and information security policies and requirements by validating existing user access and flagging questionable entitlements for possible change or removal.

What information in the user's profile should be reviewed regularly?

At a minimum, the following information should be reviewed in each user's profile:

- First and Last Name: the name of the user registered in FM's system of record.
- User ID: the unique ID associated with an individual user that is used to log in to all FM applications to which the user has been granted access.
- Phone Number: the phone number at which the user can be reached.
- E-mail address: the e-mail address to which system communications, such as security notifications, are sent.
- Application: FM application(s) to which the user has been granted access.
- Role: the specific authorization role(s) assigned to the user for the associated application.

What are some best practice guidelines when conducting access reviews?

As access is reviewed, the following should be considered:

- Is the user still employed by your company?
- Has the user's job responsibilities changed?
- Should the user still have access to the specified FM technology?
- Should the user still have the assigned roles for the application?

Protecting User Credentials

FM strongly encourages user credentials be reviewed on a regular, pre-determined basis. Scheduled reviews will help you ensure FM applications and the data generated by and stored within them is secure and protected. Specifically, you should:

- Ensure each employee utilizes a unique user ID and password that is solely assigned to them; communicate that user IDs and passwords are not to be shared with others;
- Deactivate a user ID immediately if an employee transitions to a new position or leaves the company for any reason; and
- Update application and/or user access if an employee's role changes.

We recommend you review your company's designated CAs and UAs on a regular basis (or at least quarterly) to ensure those roles are staffed appropriately with trained TM users and that your staff know who to contact for access updates and password resets. CAs have the ability to enter into technology agreements on their company's behalf and individuals in this role should be reviewed regularly to ensure the current delegations remain appropriate.

Extraterritorial Use of Fannie Mae Technology

The General Terms and Conditions in FM's Software Subscription Agreement ("SSA") prohibit the access and use of FM applications and related data from any location outside of the U.S. and its territories unless expressly permitted in an SSA Schedule. Currently, the only SSA Schedules that permit extraterritorial use are the Document Certification Schedule and the Single-Family ("SF")Servicing Applications Schedule, and this permission only applies to access and use in India and the Philippines.

The SSA, which includes the General Terms and Conditions as well as all currently published Schedules, can be found in the Consolidated Technology Guide, which is available at Consolidated Technology Guide | Fannie Mae.

Third-Party Access to Fannie Mae Technology

Certain third-party providers who provide mortgage fulfillment services or other mortgage related services to single family SF lenders, FM-approved SF servicers, or FM-approved multifamily lenders (collectively, “Licensees”) may meet the definition of “Related Party,” as that term is defined in the SSA’s General Terms and Conditions. In such instance, the Licensee may issue an active Authentication Credential to the Related Party so that it may access one or more FM applications as Licensee’s “Authorized User” (as defined in the General Terms and Conditions), provided that the applicable Schedule(s) governing use of the application(s) permits the Licensee to do so. Licensees are responsible for all actions and inactions of Authorized Users with respect to a Licensed Application and must guarantee the full performance by its Authorized Users of all obligations under the SSA, regardless of whether the Authorized User is a Related Party or employee of Licensee.

Any Licensee that is not a SF Lender, FM-approved SF servicer or FM-approved multifamily lender is only permitted to issue Authentication Credentials to its own employees and not any of its Related Parties. Contact your Technology Account Manager if a mortgage service provider requires access to FM technology.

Data Access Authorization

Lenders are reminded that a Data Access Authorization Agreement must be executed in order for a mortgage service provider to be granted access to the lender’s data that is generated by and/or stored in a FM application. Additionally, mortgage service providers that wish to access a lender’s data from a FM application must have their own Software Subscription Agreement, allowing them to access and use such application, and, except in some limited circumstances, must obtain User IDs and passwords through their own TM account. Consult your Technology Account Manager for assistance. Please access Selling & Servicing Guide Forms at Selling & Servicing Guide Forms | Fannie Mae.

Questions?

For further assistance, call the Technology Support Center for FM customers seeking information or assistance with FM technology applications at 800-2FANNIE (800-232-6643).