Each organization must designate one (1) Super Account Administrator (SAA) per Organization. The SAA is the main point of contact for Account Administrator entitlement at the organization. SAAs have "Administrator" access to all applicable FINRA applications and privileges. SAAs need to set their own entitlement (self-entitle) in order to access the applications and privileges needed to perform their job responsibilities for their organization. SAAs create Account Administrators (AA) who manage entitlement for other users within the organization. Both SAAs and AAs can create, delete and maintain user accounts. SAAs are responsible for verifying all user accounts for their organization and must comply with the annual FINRA Entitlement User Account Certification Process.

NOTE:
This job aid covers information specific to SAAs. Go to the FINRA Entitlement Program -- Entitlement Help & Training -- FINRA Entitlement Reference Guide for general help for Account Administrators (AAs) & Super Account Administrators (SAAs).

Content:
- Considerations for Designating an SAA (pg. 2)
- SAA Concept (pg. 2)
- Authorized Signatory Instructions and Requirements (pg. 2)
- Steps for Designating an Individual to be an SAA (pg. 3)
- Steps for Updating or Replacing an Existing SAA (pg. 4)
- How to Self-Entitle “User” Privileges as an SAA (pg. 4)
- How to Access Account Management to Self Entitle “User” Privileges as an SAA using FINRA Firm Gateway (pg. 5)
- How to Create an Account Administrator (pg. 11)
- How to Set Unique IDs for TRACE MPIDs, Equity MPIDs and/or MSRB Numbers (pg. 16)
  - Setting Unique IDs for an Account Administrator (pg. 16)
  - Setting Unique IDs for a User (pg. 18)
- How to directly access the Account Management URL Address (pg. 19)
- How to Identify an SAA in Account Management (pg. 21)
- How to Change Your Security Questions and Answers (pg. 22)
- How to Log Out (pg. 24)
Considerations for Designating an SAA:

- Each firm must designate one (1) SAA.
- For firms with affiliates, the same SAA or a different SAA may be designated; however, each affiliate (with its Organization ID#) must provide a signed SAA Entitlement Form.
- SAA must be formally delegated the authority by the organization_agency and as authorized in the New Organization SAA Form (or Update/Replace SAA Form) to perform the SAA responsibilities on its behalf. In order for FINRA to create an SAA account for a new organization, the designation must be executed on the current version of FINRA’s New Organization SAA Form (or Update/Replace SAA Form), as instructed, and be executed by an Authorized Signatory, as defined by FINRA.
  - An SAA may serve in this role for multiple organizations (affiliated or non-affiliated). NOTE: a separate user name and password is required for each organization.
  - The individual does not need to have an existing FINRA Entitlement Account.

SAA Concept:

- The FINRA Entitlement Program has two Super Account Administrator Forms. The New Organization SAA Form is used to designate an SAA when your organization is new and needs access to the FINRA Entitlement Program. The Update/Replace SAA Form is used when your firm needs to replace the SAA or update the name and/or email of your current SAA.
- FINRA creates one SAA for each Organization ID#.
- An SAA creates, updates and deletes AAs who in turn manage user accounts. An SAA is also able to create, modify and delete users accounts.
- An SAA certifies that their users are properly entitled to the applications in the FINRA Entitlement Program and the sensitive data these applications may contain.

Authorized Signatory Instructions and Requirements:

The New Organization SAA Form is used to designate an SAA when your organization is new and requires access to the FINRA Entitlement Program. This form has specific instructions and signature requirements noted in the form which must be met for processing.

This form can be submitted electronically via DocuSign or a downloadable PDF submitted via email, fax or mail.

Only person(s) authorized to execute this Agreement on behalf of the Organization must sign this form. The SAA and the Authorized Signatory may be the same person only if there is no one at the Organization authorized to act as the Authorized Signatory (e.g., a sole proprietor). You must provide an explanation if you are authorized to execute this agreement on behalf of the Organization but do not meet the Authorized Signatory requirements below.

- Broker-Dealer (BD) and CAB Firms: An Authorized Signatory is the Chief Compliance Officer (CCO) or authorized officer (or other authorized person) listed on Schedule A of the Organization’s Initial Form BD and the signer and the designated SAA are not the same person.
- Investment Adviser Firms: An Authorized Signatory is either the Chief Compliance Officer (CCO) or Additional Regulatory Contact (ARC) who will be listed on the Organization’s Initial Form ADV and the signer and the designated SAA are not the same person.
- Regulators: An Authorized Signatory is the Securities Commissioner, Chief Regulatory Officer or other Authorized Signatory and the signer and the designated SAA are not the same person.
Steps for Designating an Individual to be an SAA:

1. Complete the New Organization SAA Form following the directions on the form and send to FINRA. The form can be found at www.finra.org/entitlement
2. FINRA Entitlement will set the SAA designation and give “Administrator” access for all applications and privileges. No “User” privileges will be set.
3. Once approved, the SAA will receive two (2) emails. One email will contain the user name and the other email will contain the temporary user password. NOTE: The Authorized Signatory who signed the form will also receive an email indicating that the SAA has been designated.
4. Upon receipt of the emails, the SAA should log into the application using the user name and temporary password provided by the FINRA Entitlement Group.
5. System/Application Information link is located at www.finra.org/entitlement.
6. Firms can access the FINRA Firm Gateway at: https://firms.finra.org
7. Select a new password, select three Security Questions, and enter three Security Responses.
8. Log into the application again, using the user ID and new password.
9. An SAA can self-entitle by marking “User” for any required application/privilege that he/she needs to perform their job.
10. An SAA can create, update and/or delete accounts for Account Administrators and users.

Steps for Updating or Replacing an Existing SAA:

Complete the Update/Replace SAA Form to replace an SAA or update the name or email address of the current SAA. This form must be requested by an Authorized Signatory of your organization. An Authorized Signatory contacts the Gateway Call Center to request the Update/Replace SAA Form. The FINRA Entitlement Group confirms the identity of the requester and pre-populates the form with a unique identifier specific to the request. FINRA sends the form only to an authorized signatory at the firm, using the individual’s contact information on file.

- For Broker-Dealers, the Authorized Signatory is the Chief Compliance Officer (CCO) or authorized officer (or other authorized person) listed on Schedule A of the firm’s initial or current Form BD.
- For Investment Advisers, the Authorized Signatory is the Chief Compliance Officer (CCO) or Additional Regulatory Contact (ARC) listed on the firm’s initial or current Form ADV.
  - Note that IA firms that have access to the FINRA Entitlement Program and need to replace their SAA but have not yet filed their initial Form ADV must use the New Organization SAA Form to replace or update their SAA.
- For Funding Portals: An Authorized signatory is the Chief Compliance Officer (CCO), Chief Executive Officer (CEO), Chief Financial Officer (CFO), Chief Legal Officer (CLO), Chief Operations Officer (COO) or a Director or any other individuals with similar status or functions and the signer and the designated SAA are not the same person.

When the completed form is returned to FINRA, the pre-populated information on the form must match the unique identifier that FINRA provided. FINRA assigns a unique identifier to each update/replace request and therefore, a firm must request another Update/Replace SAA Form for a subsequent request.

Requests are made by contacting the Gateway Call Center:

- Broker-Dealers: (301) 869-6699
- Investment Adviser: (240) 386-4848
- Funding Portals: (301) 590-6500
How to Self-Entitle “User” Privileges as an SAA:

As a new SAA, you will need to entitle yourself to any “User” privileges you need to perform your job.

The Account Management functionality can be accessed several ways:

- Firms can access Account Management via the FINRA Firm Gateway at:  https://firms.finra.org
  or directly at:  https://accountmgmt.finra.org/ewsadmin2/index.jsp

- SAAs and AAs can also access Account Management via the Account Administration link located within certain applications (i.e. Web CRD, IARD and FPRD).

**NOTE:** This guide will provide the steps for you to access Account Management via Firm Gateway and Account Management directly.
How to Access Account Management to Self-Entitle “User” Access as an SAA using FINRA Firm Gateway:

**Step 1:** Firms can access the FINRA Firm Gateway at: [https://firms.finra.org](https://firms.finra.org)

**Step 2:** Enter your **User ID**, read the **Terms and Conditions** and click **Accept**.

**NOTES:**
- If you do not know your user ID or password, click the **Forgot User ID or Password** hyperlink. Select the appropriate User ID or Password radio button, enter the required information and click **Submit**. An email with your User ID or a temporary password will be sent to you.
- Clicking **Decline** prevents you from accessing the application.
- To improve application security, FINRA has shortened the time before users are automatically logged off due to inactivity to 30 minutes. Please make sure to save your work frequently to avoid lost work due to a system timeout.
Result: The Password screen appears.

Step 3: Enter your Password and click Log in.

NOTES:

- If you do not know your Password, click the Forgot User ID Password hyperlink. Enter your User ID, email address and click Submit. An email with a temporary password will be sent to you.
- Periodically you will be presented with a security question that you have preselected and provided responses. When your security question is presented, enter the appropriate answer to the question, and click Continue.

Result: The Firm Gateway home screen appears.
**Result:** The Funding Portal Gateway home screen appears.

![Funding Portal Gateway](image)

**Step 4:** Click the **User Administration** tab to search for your account.

**Result:** The Account Management: Start New Search screen appears.

![Account Management: Start New Search](image)
Step 5: Enter your User ID or Name information in the appropriate fields and click on Search located at the bottom of the screen.

Result: The Search Results screen displays.

Step 6: Click on your User ID hyperlink.

Result: The View Account screen displays.

Step 7: Click on Edit Account located on the navigation bar to the left side of the screen.
Result: The *Edit Account* screen displays.

### Account Management: Edit Account

To edit the account for "John Doe (Doe)", fill in the following form, then click "Save".

Note: (*) indicates required fields.

#### User Profile

User ID: Doe

#### Application Privileges

<table>
<thead>
<tr>
<th>User Role</th>
<th>Account Management</th>
<th>Edit Account Data</th>
<th>Manage Accounts</th>
<th>Change Password</th>
<th>MSRB Numbers</th>
<th>OCSA</th>
<th>NextGen New Member Application</th>
<th>Primary Account Admin</th>
<th>CRD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select All</td>
<td>Unselect All</td>
<td>Select All Admin</td>
<td>User</td>
<td>Administrator</td>
<td>User</td>
<td>Administrator</td>
<td>View</td>
<td>Update</td>
</tr>
</tbody>
</table>

*User: The ability to use the functionality as defined by the privilege.*

*Administrator: The ability to assign the privilege to other users and view the privilege assigned to other users.*
Step 8:
Select the appropriate privileges that you need for each application, mark “User” and click the Save button that is located at the bottom of the screen.

Important Note: As an SAA you must retain “Administrator” privileges to applications in order to create or manage AA and user accounts for your firm.

Options:
Select All - Use this option if “User” access is needed for all privileges for the application.
Unselect All - Use this option if access is no longer needed.

Roles:
User - The ability to use the application or function.
Administrator - The ability to see and assign a privilege to other users.
Privilege Viewer - Used only by FINRA Account Administrators.

Result: The Account Changed screen displays showing the changes that have been made.

Account Management: Account Changed

The account has been changed for "John Doe (doe)":

User Profile

<table>
<thead>
<tr>
<th>User ID:</th>
<th>doej</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix:</td>
<td></td>
</tr>
<tr>
<td>First Name:</td>
<td>John</td>
</tr>
<tr>
<td>Middle Name:</td>
<td></td>
</tr>
<tr>
<td>Last Name:</td>
<td>Doe</td>
</tr>
<tr>
<td>Suffix:</td>
<td></td>
</tr>
<tr>
<td>Title:</td>
<td></td>
</tr>
<tr>
<td>Department:</td>
<td></td>
</tr>
<tr>
<td>Primary Email:</td>
<td><a href="mailto:john.doe@firm.org">john.doe@firm.org</a></td>
</tr>
<tr>
<td>Secondary Email:</td>
<td></td>
</tr>
<tr>
<td>Primary Phone:</td>
<td>555-555-5555</td>
</tr>
<tr>
<td>Secondary Phone:</td>
<td></td>
</tr>
<tr>
<td>FAX:</td>
<td></td>
</tr>
</tbody>
</table>
How to Create an Account Administrator:

As a Super Account Administrator, you have the ability to create and edit accounts for Account Administrators.

**Step 1:** Log into Account Management.

**Result:** The **Firm Gateway** home screen appears.

![Firm Gateway Home Screen]

**OR**

**Result:** The **Funding Portal Gateway** home screen appears.

![Funding Portal Gateway Home Screen]

**Step 2:** Click the **User Administration** tab to search for your account.
cont.

Result: The Start New Search screen appears. It is recommended you search the system first to verify that the individual does not already have an account with your organization.

Step 3: Enter the AAs Last Name and First Name then click on Search located at the bottom of the screen.

Result: The Search Results screen displays.

If the AA has a user record, the name will appear in the results.

Step 4: Click Create New Account from the navigation panel..
cont.

Result: The Create New Account screen displays.

![Account Management: Create New Account](image)

**NOTES:**

- All fields marked with an asterisk (*) are required to create a new user account. To systematically generate a User ID, enter the user’s first and last names into the appropriate fields and click the Generate a new User ID hyperlink. To systematically generate a password, click the Generate a password hyperlink.

- A new account automatically defaults to an Initial Account Status of Active, meaning the user can access an application as soon as they are provided with the User ID and Password. If the status is changed to Disable, the user cannot access the application until you activate it.
**Step 5:** Enter the appropriate information into the fields in the **User Profile, Account Profile, FINRA Information, and Application Privileges** sections of the **Create New Account** screen and click the **Save** button located at the bottom of the screen.
Step 6: Take note of the User ID and temporary Password that you will need to provide to the user. If providing by email, it is recommended that the User ID and temporary password be sent in separate emails for information security purposes. He/she can now access the application(s).

NOTES:
- Use the Paste Special command after copying the User ID and password so that the information will be visible. When the new user logs into the application for the first time with the User ID and password you have provided, they will immediately be directed to change his/her password and select three Security Questions and enter the Security Responses.
- The date and time the account was created displays in the Account Created on field, and the user ID of the person who created the account displays in the Account Created by field. If the account was created by an FINRA Administrator, it will display “FINRA”.

![Account Management: Account Saved](image)
How to Set Unique IDs for Trace MPIDs, Equity MPIDs and/or MSRB Numbers

Setting Unique IDs for an Account Administrator:

**Step 1:** In the FINRA Information Section of Account Management, select the Unique ID(s) that an Account Administrator will need to assign to other users. Select the Unique ID by clicking on the MPID(s) and/or MSRB(s). The selected ID will highlight.

**Step 2:** In the Application Privileges Section of Account Management, select “User” for both the ‘View’ and ‘Update’ privileges for TRACE, Equity, and/or MSRB so that an Account Administrator has the ability to assign that Unique ID(s) to other users.

**Roles:**

View - Provides the capability to view the list of accounts MPID(s) or MSRB(s).

Update - Provides the capability to add or delete from the list of accounts MPID(s) or MSRB(s).

**Step 3:** In Account Management, under the Report Center Section, select the associated privilege for the selected Unique ID.

For example- If a TRACE MPID is selected, you must also select the associated privilege which is ‘Report Center – View TRACE Quality of Markets Report Card’ with “User & Administrator”. An error message will appear on the system if a Unique ID(s) is selected, but the associated privilege(s) is not.
Options:
Select All - Use this option if “User” access is needed for all privileges or the application.
Unselect All - Use this option if access is no longer needed.
Select All Admin - Use this option if “Administrator” access is needed for all privileges for the application.

**Report Center Roles**
- **View Usage Log:**
  - User
  - Administrator
- **View Equity Report Card:**
  - User
  - Administrator
- **View TRACE Quality of Markets Report Card:**
  - User
  - Administrator
- **View TRACE Entitlement and Contact Report:**
  - User
  - Administrator
- **View MSRB Report Cards:**
  - User
  - Administrator
- **View Disclosure Reports:**
  - User
  - Administrator
- **View Online Learning Reports:**
  - User
  - Administrator
- **View Risk Monitoring Reports:**
  - User
  - Administrator

**Step 4:** Click the **Save** button that is located at the bottom of the screen.

**Scenarios for Setting Up an Account Administrator**

<table>
<thead>
<tr>
<th>FINRA Information Section</th>
<th>Report Center Application associated Privileges (The privilege below must be marked)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Equity MPID(s) by clicking on the Equity MPID(s) to highlight</td>
<td>Equity MPID View Update</td>
</tr>
<tr>
<td>Select TRACE MPID(s) by clicking on the TRACE MPID(s) to highlight</td>
<td>TRACE MPID View Update</td>
</tr>
<tr>
<td>Select TRACE MPID(s) by clicking on the TRACE MPID(s) to highlight</td>
<td>TRACE MPID View Update</td>
</tr>
<tr>
<td>Select TRACE MPID(s) by clicking on the TRACE MPID(s) to highlight</td>
<td>TRACE MPID View Update</td>
</tr>
<tr>
<td>Select TRACE MPID(s) by clicking on the TRACE MPID(s) to highlight</td>
<td>TRACE MPID View Update</td>
</tr>
<tr>
<td>Select TRACE MPID(s) by clicking on the TRACE MPID(s) to highlight</td>
<td>TRACE MPID View Update</td>
</tr>
<tr>
<td>Select MSRB Number(s) by clicking on the number(s) to highlight</td>
<td>MSRB Number View Update</td>
</tr>
</tbody>
</table>
Step 1: In the FINRA Information Section of Account Management, select the Unique ID(s) that an Account Administrator will need to assign to other users. Select the Unique ID by clicking on the MPID(s) and/or MSRB(s). The selected ID will highlight.

![FINRA Information](image)

**Step 2:** In Account Management, under the Report Center Section, select the associated privilege for the selected Unique ID.

For example- If a TRACE MPID is selected, you must also select the associated privilege which is ‘Report Center – View TRACE Quality of Markets Report Card’ with “User”. An error message will appear on the system if a Unique ID(s) is selected, but the associated privilege(s) is not.

**Role:**

User - The ability to use the application or function.

<table>
<thead>
<tr>
<th>Report Center:</th>
<th>User</th>
<th>Administrator</th>
<th>Privilege Viewer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select All</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unselect All</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Select All Admin</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Report Center Roles**

- View Usage Log: User
- View Equity Report Card: User
- View TRACE Quality of Markets Report Card: User
- View TRACE Entitlement and Contact Report: User
- View MSRB Report Cards: User
- View Disclosure Reports: User
- View Online Learning Reports: User
- View Risk Monitoring Reports: User

**Scenarios for Setting Up a User**

<table>
<thead>
<tr>
<th>FINRA Information Section</th>
<th>Report Center Application associated Privileges (The privilege below must be marked)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Equity MPID(s) by clicking on the MPID(s) to highlight</td>
<td>View Equity Report Card</td>
</tr>
<tr>
<td>Select TRACE MPID(s) by clicking on the MPID(s) to highlight</td>
<td>View TRACE Quality of Markets Report Card</td>
</tr>
<tr>
<td>Select TRACE MPID(s) by clicking on the MPID(s) to highlight</td>
<td>View TRACE Entitlement and Contact Report</td>
</tr>
<tr>
<td>Select MSRB Number(s) by clicking on the number (s) to highlight</td>
<td>View MSRB Report Card</td>
</tr>
</tbody>
</table>
How to directly access the Account Management URL Address:

**Step 1:** Access the Account Management at [https://accountmgmt.finra.org/ewsadmin2/index.jsp](https://accountmgmt.finra.org/ewsadmin2/index.jsp)

**Step 2:** Enter your User ID and click Accept.

![Welcome to User Account Management](image)

**Result:** The Welcome to User Account Management screen opens.

**Step 3** Enter your Password and click Log in.

**NOTES:**
- If you do not know your User ID or Password, click the Forgot User ID or Password hyperlink. Select the appropriate User ID or Password radio button, enter the required information and click Submit. An email with a your User ID or a temporary password will be sent to you.
- Periodically you will be presented with a security question that you have preselected and provided responses. When your security question is presented, enter the appropriate answer to the question, and click Continue.
Result: The Account Management: Home screen appears.

Account Management: Home

Welcome to Account Management.

Please make a selection from the menu at the left. The available selections for Account Management are:

Home: Introduces the Account Management system, displays system announcements, and provides links to applications.

Account Management: Allows you to manage the list of accounts that can be used to log into any of the applications under the Account Management umbrella. You can view, add, and edit accounts from the list. This tool also enables you to designate the appropriate applications, roles, and privileges for each account.

Help: Provides help in using the Account Management system.
How to Identify an SAA in Account Management:

All users can view a list of their firm’s Super Account Administrator, Account Administrators and the list of all FINRA applications available to your organization.

**Step 1:** Access the Account Management site *(see pg. 5 or 19).*

**Step 2:** Select *My Account* from the header section of the screen.

**Result:** The *Applications & Administrators* screen appears.

**Result:** The *My Account: Account Information* screen appears.

**Step 3:** Click *Applications & Administrators* located on the navigation bar located on the left side of the screen.

**Result:** The *Applications & Administrators* screen appears.
How to Change Your Security Questions and Answers

The Security Questions and Answers can be changed by clicking the Edit Security Questions checkbox that is located on the Password screen.

OR

Step 1: Access the Account Management site (see pg. 5 or 19).

Step 2: Select My Account from the header section of the screen.

Result: The Applications & Administrators screen appears.

Step 3: Select Change Security Questions from the navigation bar.


Step 4: Change your **Security Questions and Answers** as desired and click **Save**.
How to Log Out
Select Log Out from the top right portion of the screen.

The **Logout Successful** screen will display. To log back in, select the **Click to Login** button. Follow the

**ADDITIONAL NOTES:**
- When you log out, your browser could contain a memory of the account information viewed during your session. For added security we recommend that you close your browser window.
- If you are inactive for 27 minutes you will get several prompts to **Continue Session**. If you don’t select **Continue Session**, at the end of 30 minutes, you will be logged off. If you select **Continue Session**, the clock will be reset for another 30 minute session.

**Example of the 27 minute timeout prompt.**

- This job aid covers information specific to SAAs. Go to the **FINRA Entitlement Program: Entitlement Reference Guide** to see steps for functions that are available to SAAs and AAs.