Financial Industry Regulatory Authority

FINRA Entitlement Program Frequently Asked Questions (as of 02/26/15)

Q1: What is FINRA Entitlement?

A: FINRA Entitlement is the process by which a user is granted secure access to a participating FINRA Web Application(s) by a Super Account Administrator (SAA) or an Account Administrator who maintains that account. Entitlement includes creating and deleting accounts and granting and denying specific privileges within an application(s) for a given user so that a user may access the specific functionality that the privilege supports.

Super Account Administrator (SAA) Information

Q2: What are the responsibilities of an SAA?

A: Each organization with access to FINRA's Entitlement Program must designate an SAA. An SAA is entitled as an administrator for all applications participating in the FINRA Entitlement Program that are available to that organization. An SAA is able to create, edit and delete accounts for both Account Administrators and users at an organization. The SAA also monitors and reviews accounts to ensure proper access and ensures that users adhere to FINRA's security procedures and related terms and conditions. An SAA is required to complete the FINRA Entitlement User Accounts Certification Process when prompted by FINRA.

Q3: What are the designating criteria of an SAA?

A: An organization is responsible for selecting an SAA and ensuring that all related FINRA Entitlement procedures and policies are followed. The SAA is a powerful role with administrator rights to all applications and entitlements that are available for your organization and careful consideration should be made when designating an SAA. Consider the following when designating your 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's account, 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.

Q4: How many SAAs can an organization have?

A: For security reasons, an organization may designate only one (1) SAA to serve in this role. The FINRA Entitlement Program automatically checks that only one SAA is designated for an organization. An organization is defined as an entity with a unique Org ID # (whether an entity or an affiliate of an entity).

Q5: How do I designate an SAA for my new organization?

A: Complete the New Organization SAA Form when your new organization is first requesting access to the FINRA Entitlement Program and needs to designate its SAA. Follow the specific instructions on the form, noting the requirements for an Authorized Signatory.

Q6: How do I replace an SAA or update the current SAA's information?

A: The Update/Replace SAA Form is used 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.

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.

Note: If your firm is an investment-adviser that already has access to the FINRA Entitlement Program and has not yet filed your initial ADV, you must complete the New Organization SAA Form to update/replace your SAA.

.

Q7: Who does FINRA define as an Authorized Signatory?

A: FINRA defines an Authorized Signatory for a firm as follows:

- Broker-Dealer firms: Chief Compliance Officer (CCO) or authorized officer (or other authorized person) listed on Schedule A of the Organization's Initial/Current Form BD
- Investment Adviser firms: Chief Compliance Officer (CCO) or Additional Regulatory Contact (ARC) who will be listed on the initial Form ADV or is listed on the current Form ADV.
- Service Provider: Officer authorized to act on behalf of the organization.

Q8: What are the other signatory requirements of SAA Form?

A: In addition to an Authorized Signatory signing the SAA Form, FINRA's other requirements include:
The signer and the designated SAA may **not** be the same individual, unless:

- Broker-Dealer firms: The SAA is a) the sole proprietor of the organization or b) the SAA is the only person listed on Schedule A of the Organization's Initial/Current Form BD who is authorized to execute agreements for the organization
- Investment Adviser firms: The SAA is a) the sole proprietor of the organization or b) the SAA is the only person listed as a CCO or Additional Regulatory Contact on the Organization's Form ADV **and** the only person who is authorized to execute agreements for the organization.

The Special Circumstances section of an SAA form must be completed if your firm meets one of the conditions that warrant this section to be completed. Conditions include, but are not limited to, self-signed forms (when the SAA designated is also the Authorized Signatory) and when an individual is authorized to execute the Agreement on behalf of the organization, but does not meet the Authorized Signatory requirements as stated on the form. FINRA validates information provided in this section and will not process the request for information that cannot be validated.

Q9: Can the same individual be designated as an SAA for multiple firms (affiliated or non-affiliated)?

A: Yes, as long as the individual is formally delegated appropriate authority to act on behalf of the organization.

Q10: Can a firm designate its own SAA as well as its affiliates even if the affiliates are assigned to a different group?

A: Yes.

Q11: If I am a new FINRA Entitlement user and designated as an SAA, how will I receive my User ID and Password?

A: For security reasons, the SAA will receive two (2) separate emails; one with the user ID and one with a temporary password. You must change the temporary password with the first log on.

Q12: What can I expect as an SAA when I first log in with the User ID and temporary password provided to me by the FINRA Entitlement Group?

A: To ensure that only you have access to your password, when you first log into any participating FINRA Entitlement application to which you have been entitled, you will be directed to create your own password. You will first need to enter the temporary password provided to you by the FINRA Entitlement Group and then create and enter your own password for future use. You will also be directed to select three Security Questions and Responses. The Security Information will be used if you forget your password or become locked out of your account. When you call the Gateway Call Center, you will be asked to confirm your identity as an Account Administrator by providing your response to the Security Information you selected.

Q13: If I already have a FINRA Entitlement account and later am designated as the SAA, will I receive a new user ID and password?

A: No, an existing FINRA Entitlement account that is upgraded to an SAA can use his/her existing user ID and password. Any entitlements previously granted prior to the SAA designation will also remain.

Q14: What does my organization do if our SAA will be out of the office for an extended period of time?

A: First consider if your firm's Account Administrators are able to perform the entitlement activity needed (e.g., creating, updating, or deleting user accounts, resetting user passwords). If there are no Account Administrators, and an SAA will be unavailable for an extended period of time, your organization should request a temporary replacement SAA. An Authorized Signatory must contact the Gateway Call Center to request an Update/Replace SAA Form. FINRA will only process the request from an Authorized Signatory and when the form meets all requirements. If the former SAA returns to that role; he/she will need to be re-designated as the SAA through the submission of an Update/Replace SAA Form.

Q15: When a new SAA is designated by an organization, what happens to the existing SAA?

A: The previous SAA's account is deleted.

Q16: How will an organization be notified when an SAA is designated?

A: Both the Authorized Signatory who signed the SAA Form and the SAA will receive an email when the SAA account has been processed by FINRA (including when replacement SAAs are processed).

Q17: How does an SAA update his/her name, email address, or contact information?

A: SAAs are able to update their phone and fax numbers on-line using the Account Management application. Name and email address changes can only be updated by submitting an Update/Replace SAA Form. An Authorized Signatory must contact the Gateway Call Center to request an Update/Replace SAA Form. FINRA will only process the request from an Authorized Signatory.

Note: If your firm is an investment-adviser that already has access to the FINRA Entitlement Program and has not yet filed their initial ADV, you must complete the New Organization SAA Form to update/replace your SAA or when you need to change the SAA's name or email address.

Q18: What should an SAA do if his/her account has to be reset?

A: The SAA should contact the Gateway Call Center to have his/her password reset or account unlocked.

Q19: How do I find out who my organization's SAA is?

A: Users can click on the "Applications & Administrator" link under "My Account" to see who their SAA is. Account Administrators can also see the SAA designation in the Account Management Search Results Screen.

Q20: Are there any FINRA Entitlement Program applications that are excluded from the SAA process?

A: Yes, the file transfer protocol (FTP) and internet file transfer (IFT) accounts are excluded from the SAA process. Due to the unique environment of these applications, FINRA maintains account administration rights to create these types of accounts. For access, an Authorized Signatory will need to request the FTP/IFT Entitlement Form by contacting the Gateway Call Center. The FINRA Entitlement Group confirms the identity of the requester and pre-populates the form with a unique identifier specific to the request. The pre-populated information on the form must match the unique identifier that FINRA provided. FINRA sends the form only to an Authorized Signatory at the firm, using the individual's contact information on file.

Q21: I'm a new SAA to the FINRA Entitlement Program and cannot access Web CRD, FOCUS, or any other application I need. Why?

A: New SAA accounts will automatically be set up with "Administrator" capabilities which will enable you to create account administrator or user accounts for your firm. However, in order to access or use any of the requested applications and privileges for yourself, you will need to set your own "User" privileges to your SAA account. You are responsible for determining and setting access to the applications and privileges which you need to use to perform your job functions. See the next Q&A on how to self-entitle "User" privileges for yourself.

Q22: How does an SAA self-entitle "User" privileges to applications in the Account Management Tool?

A: As a new SAA, you will need to entitle yourself to any "User" privileges for applications you need to use to perform your job functions. Keep in mind that you will not be able to access any application unless you have marked "User" for that application for your SAA account. To self-entitle "User," follow these steps:

1. Log into the Account Management Tool (see the URLs in the SAA Confirmation Packet for the link to the Account Management Tool).
2. Search for and open your user account.
3. Click Edit Account and select "User" for those privileges that you need to use to perform your job responsibilities.
4. Click the Save button. Close your Web Browser and reopen it again to access your newly self- entitled application privileges.

Q23: How does an SAA select Unique IDs and Report Center privileges for an Account Administrator?

A: This is a three step process. All steps must be followed to set Unique IDs.
1. In the FINRA Information Section of Account Management, the SAA must select the Unique ID(s) that the AA will need to perform his/her job function.

2. In the Application Entitlements Section for Account Management, the SAA needs to mark both the "View" **and "**Update" privileges for TRACE, Equity, and/or MSRB so that the Account Administrator will have the ability to assign a Unique ID(s) to a user.

3. In Account Management, under the Report Center section, the SAA must mark the associated privilege for that Unique ID. For example- If a TRACE MPID is selected, you must also have the associated privilege "Report Center – View TRACE Quality of Markets Report Card" marked with 'User and Administrator'. An error message will appear on the system if a Unique ID(s) is selected, but the associated privilege(s) is not.

Q24: How do I get 'Administrator' access to new Entitlement Applications/Privileges added on the FINRA Entitlement Program?

A: FINRA will systematically entitle the SAAs that are to be granted with the new entitlement. The SAAs that are granted the entitlement receive an email.

Q25: As an active SAA, why are there times when I can't edit/create a user's account?

A: On occasion, Entitlement functionality is temporarily suspended to allow the FINRA Entitlement Group to process transactions (e.g., set a new privilege) for a specific account. Once processing is complete, Entitlement functionality is re-established.

General Entitlement Information

Q26: What does it mean to "clone" an account?

A: Cloning an account is the process of creating a new account by duplicating (copying) an existing user account that is entitled to the same participating FINRA applications and privileges as the new user needs. If you have several users at your organization that use the same applications and privileges, cloning will minimize the time you spend setting up those accounts. You can access a user at your organization and clone that user's account (i.e., copy that user's entitlements) for each individual who requires the same applications and privileges.

Q27: Can I use the clone function to update an existing user's privileges?

A: No. Cloning may be used only when creating a new user account. If you need to update an existing user's privileges, you need to edit that user's account and modify the privileges as necessary.

Q28: How can a user change his/her Security Questions and/or Responses?

A: A user has the option to update his/her security questions and responses when he/she logs onto a FINRA Entitlement application/system. Look for the “Update Security Information” option on the Password screen. Note: Users must update their security questions and responses if they experience an account lockout due to multiple incorrect responses to their security questions or if they believe the responses to their security questions have been compromised.

Q29: What should a user at my organization do if he/she has forgotten the Password or locked his/her account?

A: A user who forgets his/her password and/or is locked out from attempting to enter a password more than five times can click on the Forgot Password? To use this functionality, the user must know his/her Security Response.

Q30: I am attempting to select a password for my account and the system keeps rejecting the passwords I choose. Why might this be happening?

A: The FINRA Entitlement system password must not contain your first, middle, or last name. If your middle name is abbreviated as a single initial, that letter may not be used in your password. Choose a password that does not contain that letter. Passwords cannot be reused.

FINRA Password Policy
Passwords must meet the following criteria:

- Must contain at least eight characters
- Cannot contain your user ID
- Cannot contain your first, middle or last name or your middle initial
- Cannot contain the character "*", "&", "%", or “ “ (asterisk, ampersand, percent, or space)
- Must contain characters from at least three of the following four categories:
  - English uppercase characters (A-Z)
  - English lowercase characters (a-z)
  - Numeric characters (0…9)
  - Special characters ! $ # @ / ? | < > ~ = { } ; : ' ( ) + [ ] \ - _ ` . ^ ,

Q31: How long will it take to process my entitlement form?

A: Please allow

-approximately two business days from receipt of a non-deficient SAA Entitlement Form -for FTP users, approximately four business days from receipt of a non-deficient FTP entitlement form.

Dormant User Account Process

Q32: Does a user account ever get automatically deleted?

A: Per FINRA's Corporate Security Policy, a user account that has not accessed an application at least once during a consecutive 13-month period from the last password reset will be considered a "dormant" account and will be automatically deleted. If this should occur, an SAA or Account Administrator at the firm will need to recreate the account if the user again needs access to any of these applications. If the account that was deleted is for an SAA, a firm's Authorized Signatory will need to request an Update/Replace SAA Form by contacting the Gateway Call Center and submit the completed form to designate an SAA.

Certification Process

Q33: What is the FINRA Entitlement User Accounts Certification Process?

A: FINRA established the FINRA Entitlement User Accounts Certification Process as part of its ongoing efforts to protect the integrity and confidentiality of regulatory, proprietary and personal information maintained by FINRA. Additionally the certification requirement supports each organization's compliance with the management of authorized users on FINRA systems. The process provides a formal review of all user accounts in the FINRA Entitlement Program administered by an SAA.

Q34: How frequently will the FINRA Entitlement User Accounts Certification Process be conducted?

A: Certification is generally conducted annually.

Q35: Can an organization's Administrators review users' access at any time during the year or are user access reviews limited to only during the annual Certification Period?

A: FINRA strongly recommends Administrators review user accounts on a regular basis to ensure that accounts remain valid, have proper entitlement, have been deleted if access is no longer needed, and email addresses are correct. The frequency of access reviews may depend on the size of the organization, staff turn-over, the number of organizational changes, an organization's security guidelines, or other factors that an organization considers in its risk profile.

Q36: Which organizations are exempt from the FINRA Entitlement User Accounts Certification Process?

A: An organization is considered to be exempt when there is only one user at the organization on the start date of the Certification Period.

Q37: If during the Certification Period the number of users at my organization decreases to only one user, will my organization still need to certify?

A: If your organization had more than one user on the start date of the Certification Period, your organization still needs to certify regardless of the changes made to the user population during the Certification Period.

Q38: How long is the FINRA Entitlement User Accounts Certification Period?

A: The Certification Period is 30 calendar days.

Q39: Who at my organization is responsible for completing the Certification Process?

A: The SAA is responsible for ensuring that the Certification Process is completed by the due date.

Q40: What if my SAA is unavailable during the annual Certification Period?

A: FINRA requires your organization to replace your current SAA with a replacement SAA to complete the Certification Process.

Q41: How will an organization be alerted to begin the FINRA Annual Entitlement User Accounts Certification Process?

A: Your SAA will see the Certification message on the Account Management Home page and will receive an email that includes the start and due date of the Certification period.

Both your SAA and Chief Compliance Officer (or, for IA-firms, the Additional Regulatory Contact) will receive the following emails:

- Reminder email - If certification is not completed 10 days prior to due date.
- Past Due email - If certification is not completed by the 30th day.

Q42: When will an SAA be able to begin the Certification Process?

A: FINRA's Entitlement User Accounts Certification Process is typically an annual process. An SAA may begin the certification process as soon as he/she receives the Certification message on the Account Management Home Page and/or email notification.

Q43: How does the SAA begin the FINRA Entitlement User Accounts Certification Process?

A: Detailed instructions on how to begin the Certification Process are included in the FINRA Entitlement User Accounts Certification email messages and on the Account Management Home page during the certification period.

Q44: How will FINRA communicate to the SAAs during the Certification Period?

A: SAAs will receive a series of messages while in the Account Management Tool, that alerts them to the status of the Certification Process:

- Initial Message - The FINRA Entitlement User Accounts Certification Period is underway with start date and due date defined.
- Reminder Message - If certification is not completed 10 days prior to due date.
- Past Due Message - If certification is not completed by the 30th day.
- Successfully Completed Message – Alerts the organization that the SAA has successfully completed the Certification Process.

Q45: Once the SAA begins the Certification Process will he/she be able to exit the Account Management Tool and complete the Certification Process at a different time?

A: Yes, an SAA may complete the Certification Process at a different time; however, FINRA recommends that an SAA certify users on the same day the download of user account information is requested to prevent having to perform a subsequent review of users as the entitlement data may have been updated since the download was requested.

Q46: When would the SAA's Account Management Certification messages not appear?

A: The certification messages will not display in the Account Management Tool if your organization is exempt or has completed the Certification Process and the 30-day Certification Period has ended.

Q47: Which accounts are included in the FINRA Entitlement Certification Process?

A: All accounts that have access to an application in the FINRA Entitlement Program at a non-exempt organization are included in the certification process. An SAA is able to search online for a list of their user accounts.

Q48: How does an SAA get a list of user accounts to review?

A: After clicking the certification link, the Account Management Search Results page will display a list of your users. Click on each user to review the applications and functions that each account can access. For your convenience, you can download your user account information into a report to send to other individuals within your organization to confirm individuals' appropriate entitlements, including access to applications, privileges and sensitive data.

Q49: In the Download Report that lists user account information, there are some criteria that are offered for selection. Which criteria should be selected for the download report in order to conduct the review of user accounts?

A: The Download Report will automatically include the required criteria of user ID and permissions for each user account. Depending on the size of an organization, an SAA may find it helpful to include the first and last names of individuals, especially if the report will be sent to others in the organization to facilitate the review. FINRA recommends that email be selected as an option for review as email addresses may change. If individuals are assigned OSO numbers, then an SAA should select the OSO option to confirm this information. Other criteria may be selected based on an organization's decision to validate this information.

Q50: Is an SAA considered a user?

A: Yes, an SAA is considered a user of the FINRA Entitlement Program, with access to account management functionality, and possibly other applications.

Q51: What criteria should my organization use when reviewing our users?

A: You will need to review your organization's user accounts to determine that:

- each user has a continuing need to access FINRA application(s) on the organization's behalf;
- each user is entitled only to the applications and privileges needed to perform current job
- responsibilities; and
- only users who require access to sensitive data (*e.g.*, Criminal History Record Information, Social Security or tax identification numbers, dates of birth) are entitled to access this type of data

Q52: What are the consequences if my organization does not complete the Certification Process by the due date?

A: The capability to create, edit and clone accounts will be disabled and will remain disabled for **all** Administrators (SAAs & Account Administrators) until your organization's SAA completes the Certification Process. Other consequences may result including notification to the appropriate FINRA district office for FINRA member firms or notifications to other regulators for non-FINRA organizations. In addition, all user accounts for an organization may be suspended.

Q53: Can my firm still certify after the 30-day Certification Period?

A: Yes, however, if all accounts have been disabled by FINRA, the SAA will need to contact the Gateway Call Center to arrange for access to complete the certification.

Q54: Can an Administrator delete or disable user accounts or reset passwords if the organization has not certified within the 30-day period?

A: Yes, for security purposes, Administrators may continue to delete or disable user accounts and reset passwords.

Q55: If my organization has questions, who should we contact?

A: Broker/Dealers should contact the Gateway Call Center at (301) 869-6699.
Investment Advisers should contact the IARD Call Center at (240) 386-4848.