Financial Industry Regulatory Authority

FINRA Entitlement Program: Super Account Administrators

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: AA Quick Reference Guide for help regarding **Account Management for Account Administrators (AAs) & Super Account Administrators (SAAs).**

Content:

Questions on EWS®? Call the FINRA Gateway Call Center at **301-869-6699**
8 AM through 8 PM, ET, Monday-Friday.

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.

Signature Requirements of SAA Forms:

The New Organization SAA Form and the Update/Replace SAA Form have specific instructions and signature requirements which must be met for processing. The forms must be signed by an Authorized Signatory as defined on the forms and all required fields must be completed.

For Broker-Dealer firms, 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 Adviser firms, the Authorized Signatory is the Chief Compliance Officer (CCO) or Additional Regulatory Contact (ARC) listed on the firm's initial or current Form ADV.

Other Signatory Requirements/Special Circumstances:

In addition to an Authorized Signatory signing the SAA Form, FINRA's other requirements include that 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.

FINRA confirms Authorized Signatory information on the SAA form matches the information on the Form BD or Form ADV. In addition, the email address provided by the firm's Authorized Signatory must match the email address that will be or is currently filed in CRD, IARD, or on the FINRA Contact System. FINRA will suspend all accounts if information does not match or is not verifiable.

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. FINRA-registered 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-Dealer firms, 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 Adviser firms, the Authorized Signatory is the Chief Compliance Officer (CCO) or Additional Regulatory Contact (ARC) listed on the firm's initial or current Form ADV.
- For Service Providers, the Authorized Signatory is an officer authorized to act on behalf of the organization

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 Platform and has not yet filed their initial Form ADV, you must complete the New Organization SAA Form to update/replace your SAA.

Requests are made by contacting the Gateway Call Center :

- Broker-Dealer firms: (301) 869-6699
- Investment Adviser firms: (240) 386-4848

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:

- FINRA-registered firms can access Account Management via the FINRA Firm Gateway at: https://firms.finra.org
- Users can access Account Management directly at https://accountmgmt.finra.org/ewsadmin2/index.jsp
- Users can access Account Management via the Account Administration link located within certain applications (i.e. Web CRD and IARD).

NOTE: This guide will provide the steps for you access Account Management via Firm Gateway and Account Management directly.

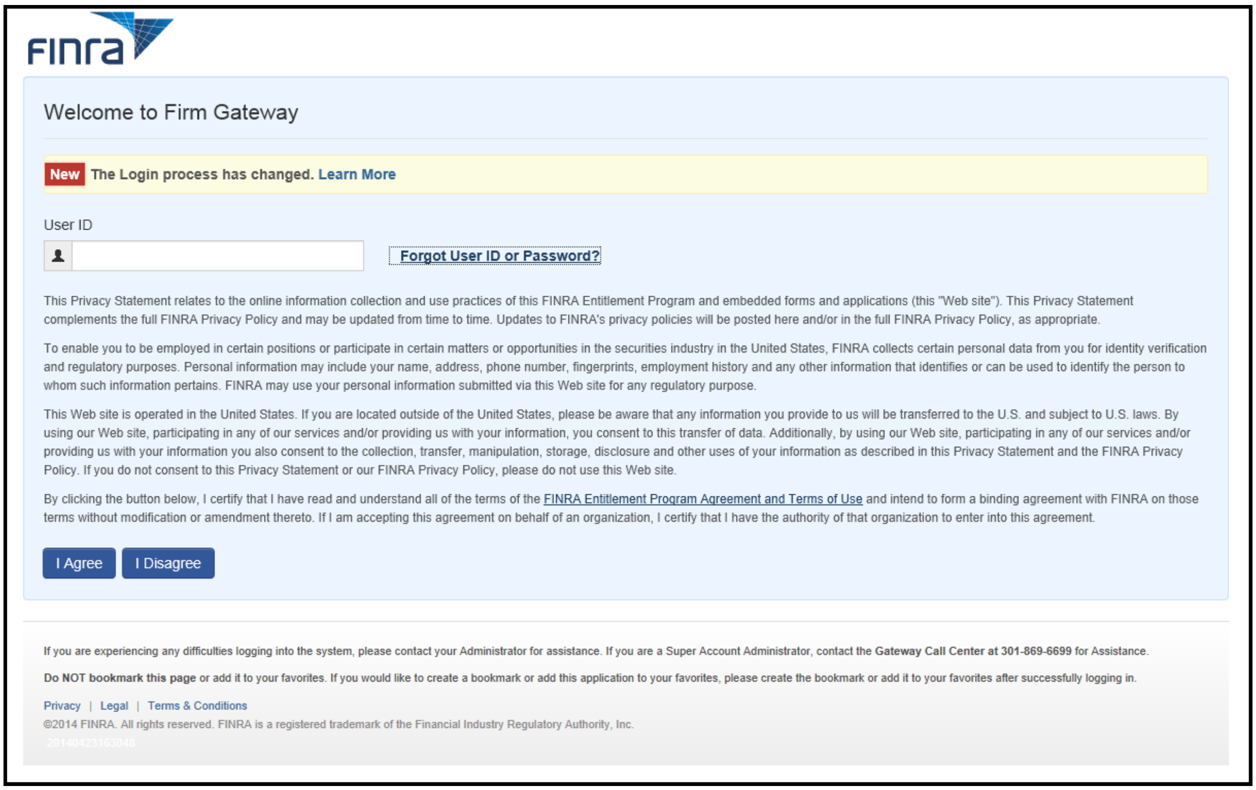
How to Access Account Management to Self Entitle "User" Privileges as an SAA using FINRA Firm Gateway:

Step 1: FINRA-registered firms can access the FINRA Firm Gateway at https://firms.finra.org

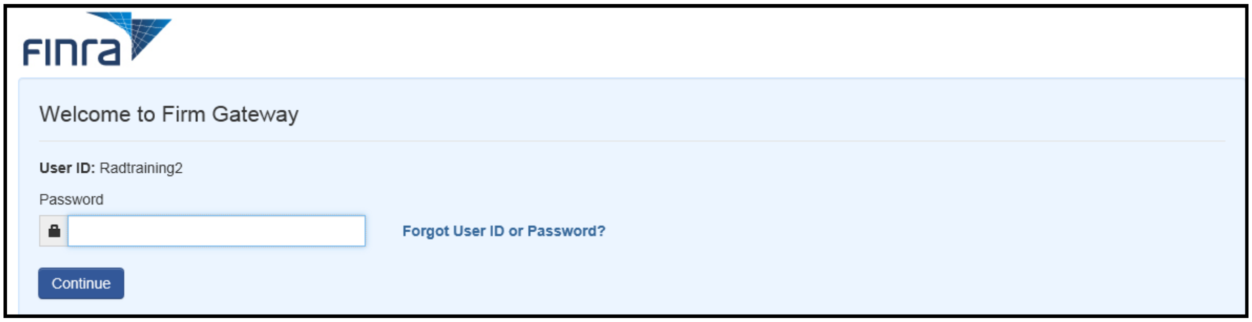
Step 2: Enter your **User ID**, read the **Terms and Conditions** and click **I Agree**.

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.
- Clicking **I Disagree** prevents you from accessing the application.



Result: The *Password* screen appears.

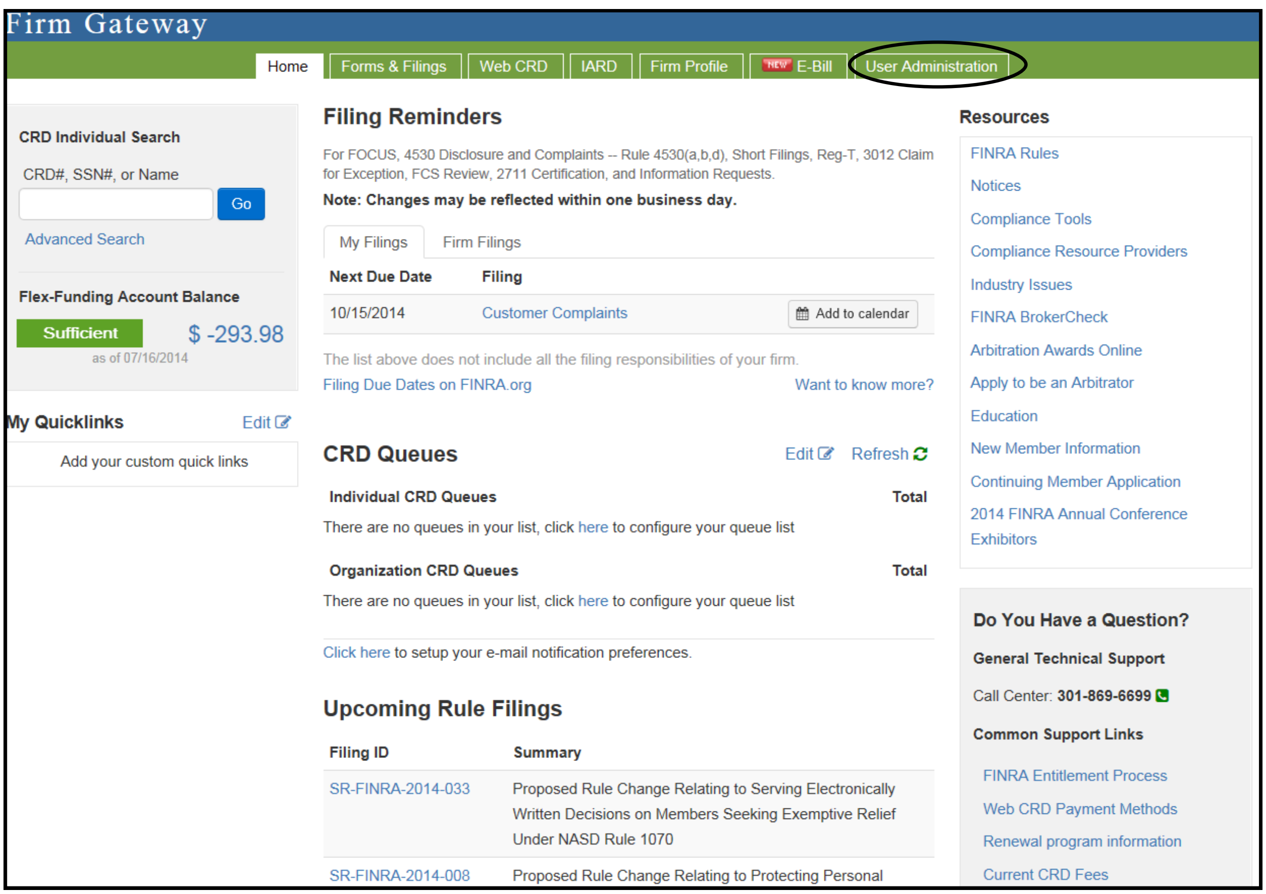


Step 3: Enter your **Password** and click **Continue.**

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**.

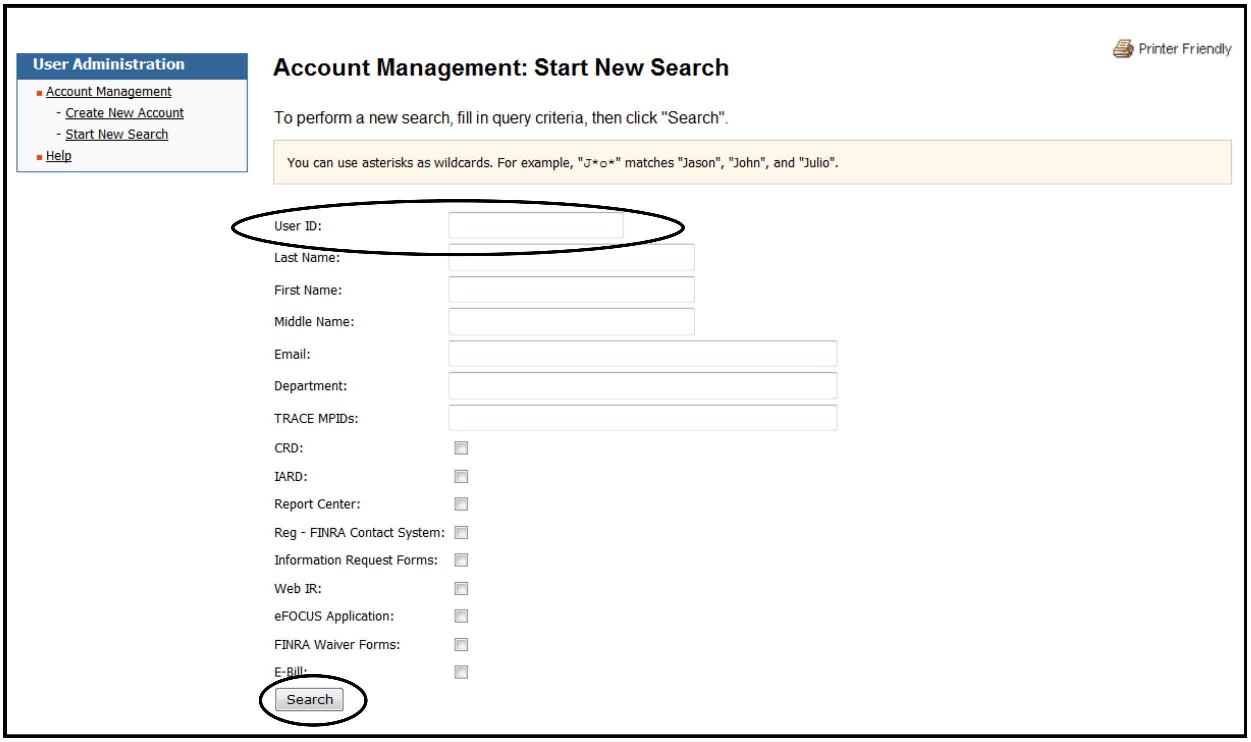
Result: The Firm Gateway: *Home* screen appears.



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

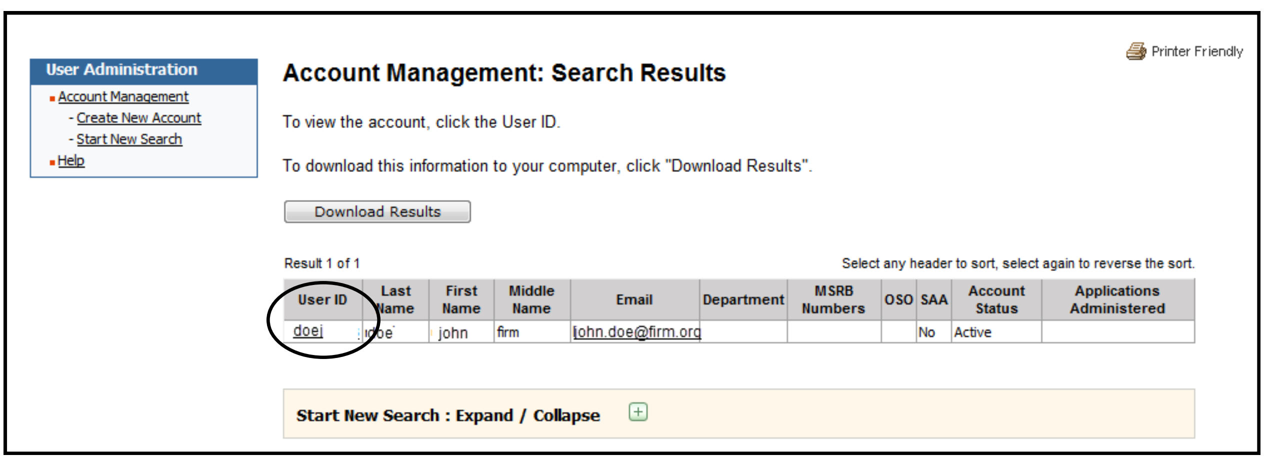
cont.

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



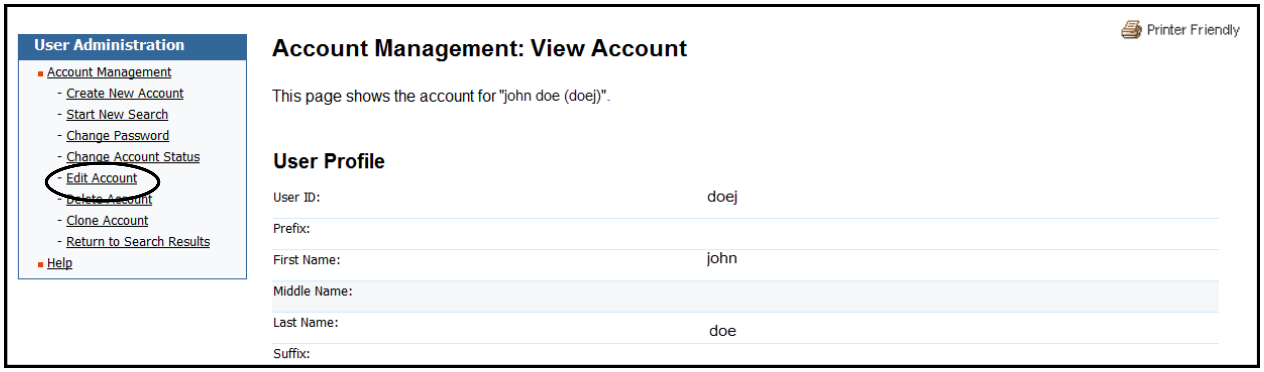
Step 5: Enter your User ID or Name information in the appropriate fields and click on *Search* located at the bottom of the screen.

Result: The *Search Results* screen displays.



Step 6: Click on your **User ID** hyperlink.

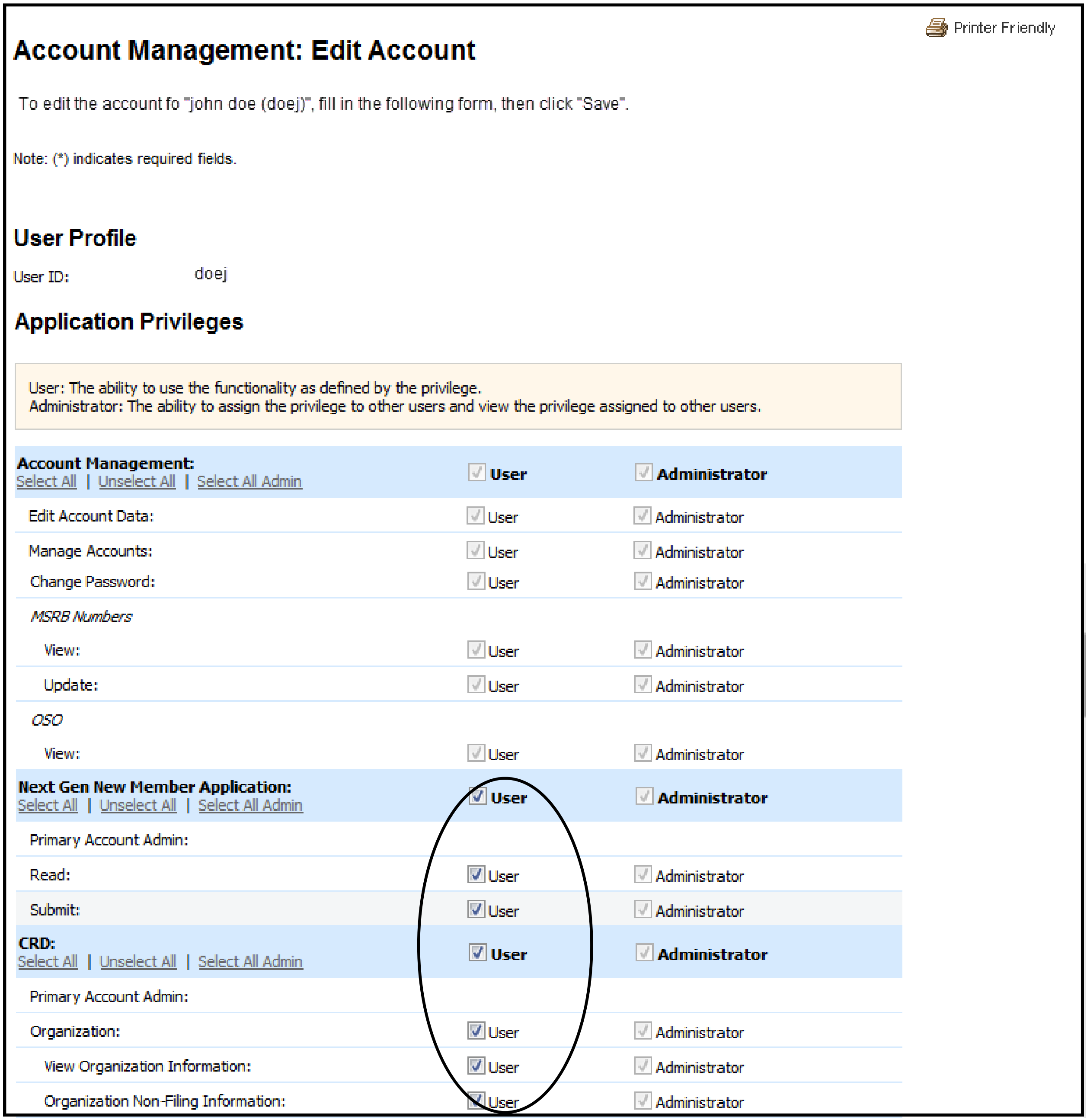
cont.
Result: The *View Account* screen displays.



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

cont.

Result: The *Edit Account* screen displays.



Printer Friendly

Account Management: Edit Account

To edit the account fo "john doe (doej)", fill in the following form, then click "Save".

Note: (*) indicates required fields.

User Profile

User ID: doej

Application Privileges

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.

Account Management: Select All | Unselect All | Select All Admin	**User**	**Administrator**
Edit Account Data:	User	Administrator
Manage Accounts:	User	Administrator
Change Password:	User	Administrator
MSRB Numbers		
View:	User	Administrator
Update:	User	Administrator
OSO		
View:	User	Administrator
Next Gen New Member Application: Select All | Unselect All | Select All Admin	**User**	**Administrator**
Primary Account Admin:		
Read:	User	Administrator
Submit:	User	Administrator
CRD: Select All | Unselect All | Select All Admin	**User**	**Administrator**
Primary Account Admin:		
Organization:	User	Administrator
View Organization Information:	User	Administrator
Organization Non-Filing Information:	User	Administrator

cont.

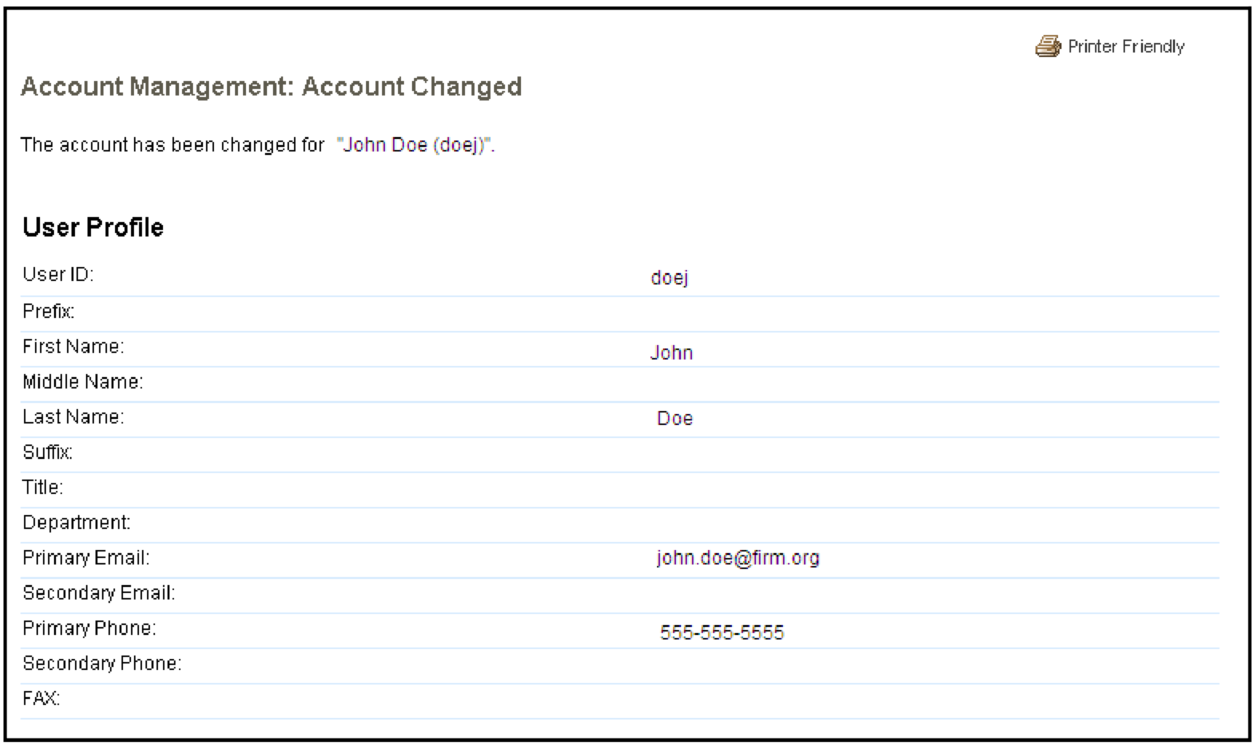
Step 8:
Select the appropriate privileges that you need for each application, mark "User" and click the **Save** button that is located at the bottom of the screen.

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 - Shortcut if all "User" privileges are needed for the application.
Unselect All - Shortcut if no privileges are needed for the application.

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.


Printer Friendly

Account Management: Account Changed

The account has been changed for "John Doe (doej)".

User Profile

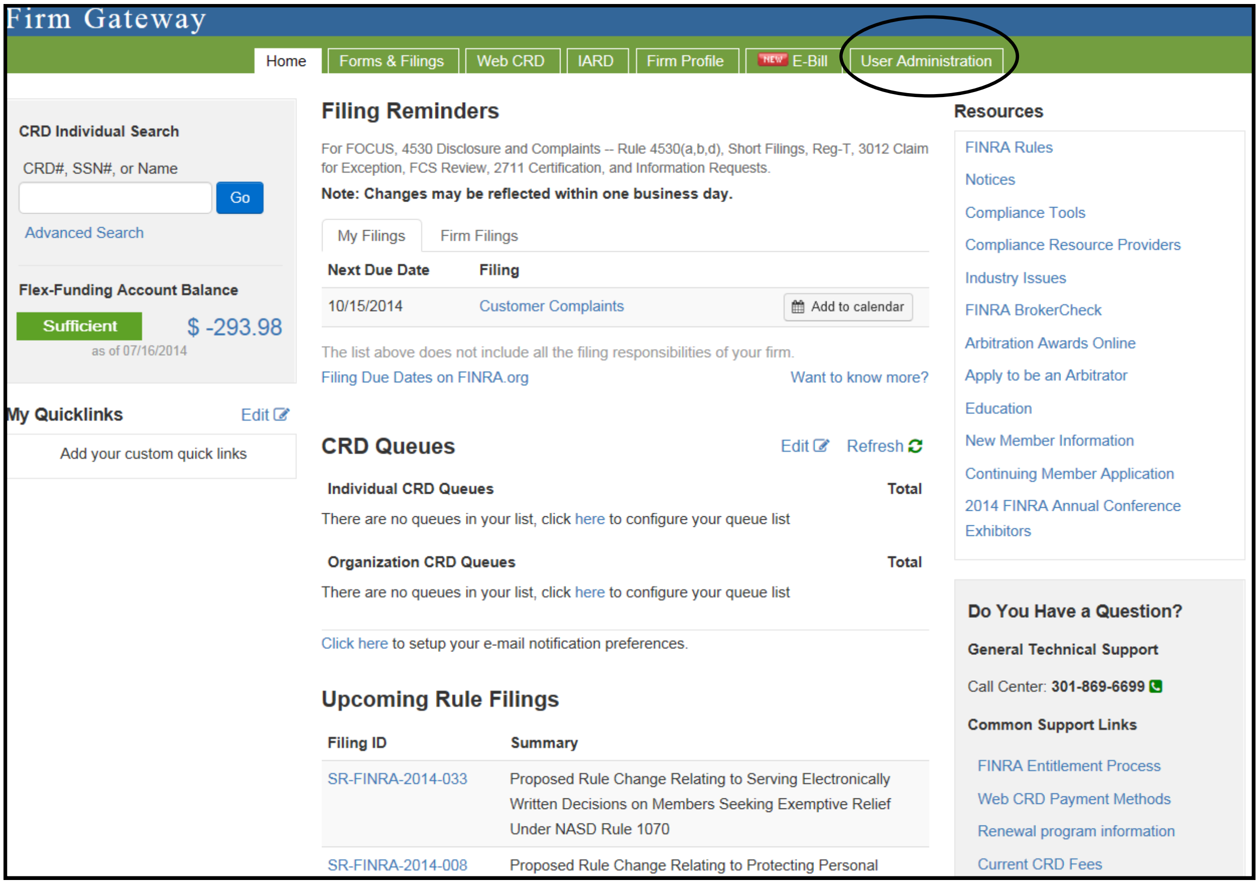
User ID:	doej
Prefix:	
First Name:	John
Middle Name:	
Last Name:	Doe
Suffix:	
Title:	
Department:	
Primary Email:	john.doe@firm.org
Secondary Email:	
Primary Phone:	555-555-5555
Secondary Phone:	
FAX:	

How to Create an Account Administrator:

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

Step 1: Log into Account Management.

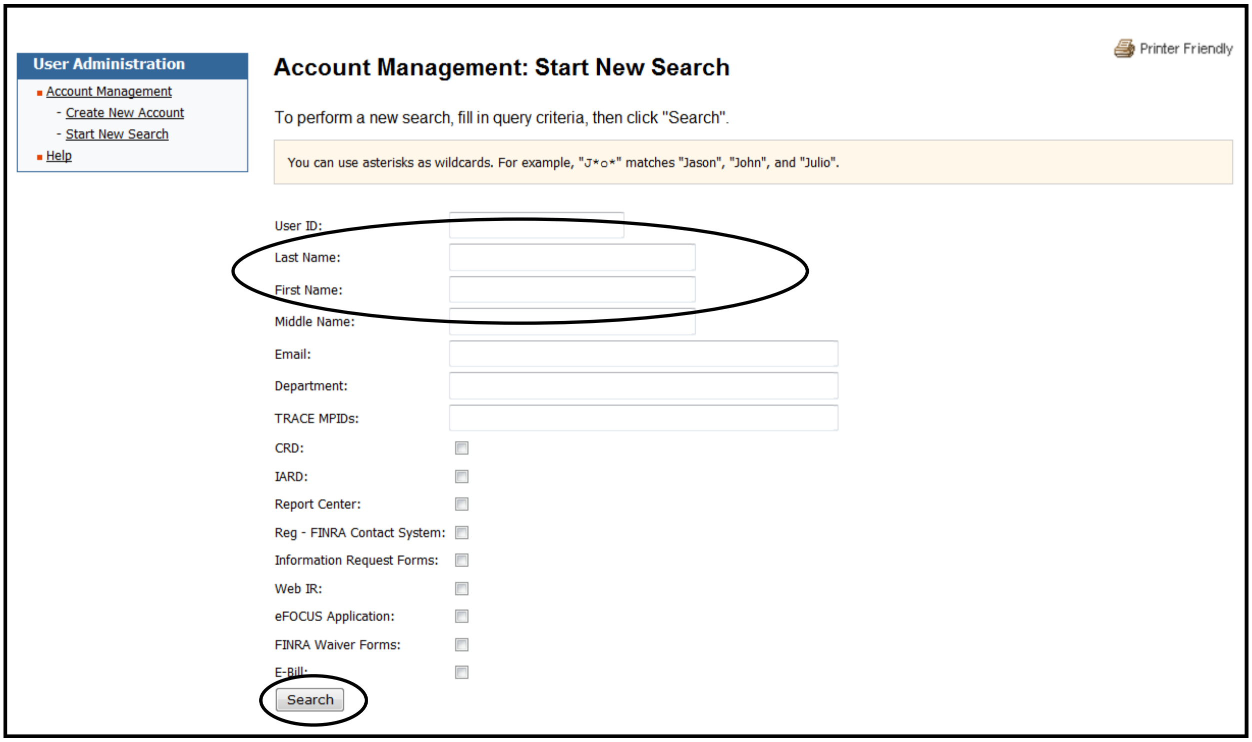
Result: The Firm Gateway: *Home* screen appears.



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

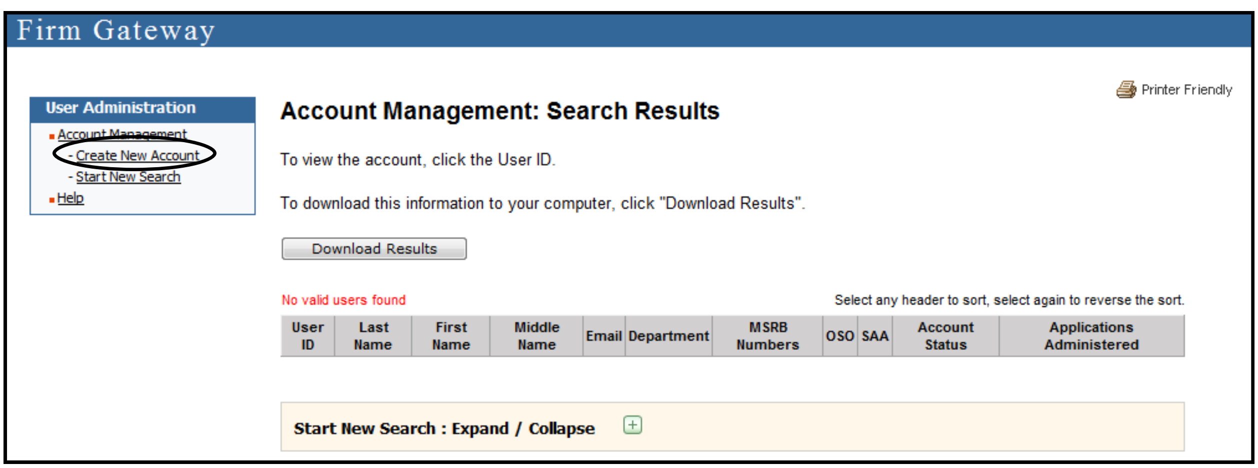
cont.
Result: The **Start New Search** screen appears. It is recommended you search the system first to verify that the individual does not already have an account with your organization.

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.

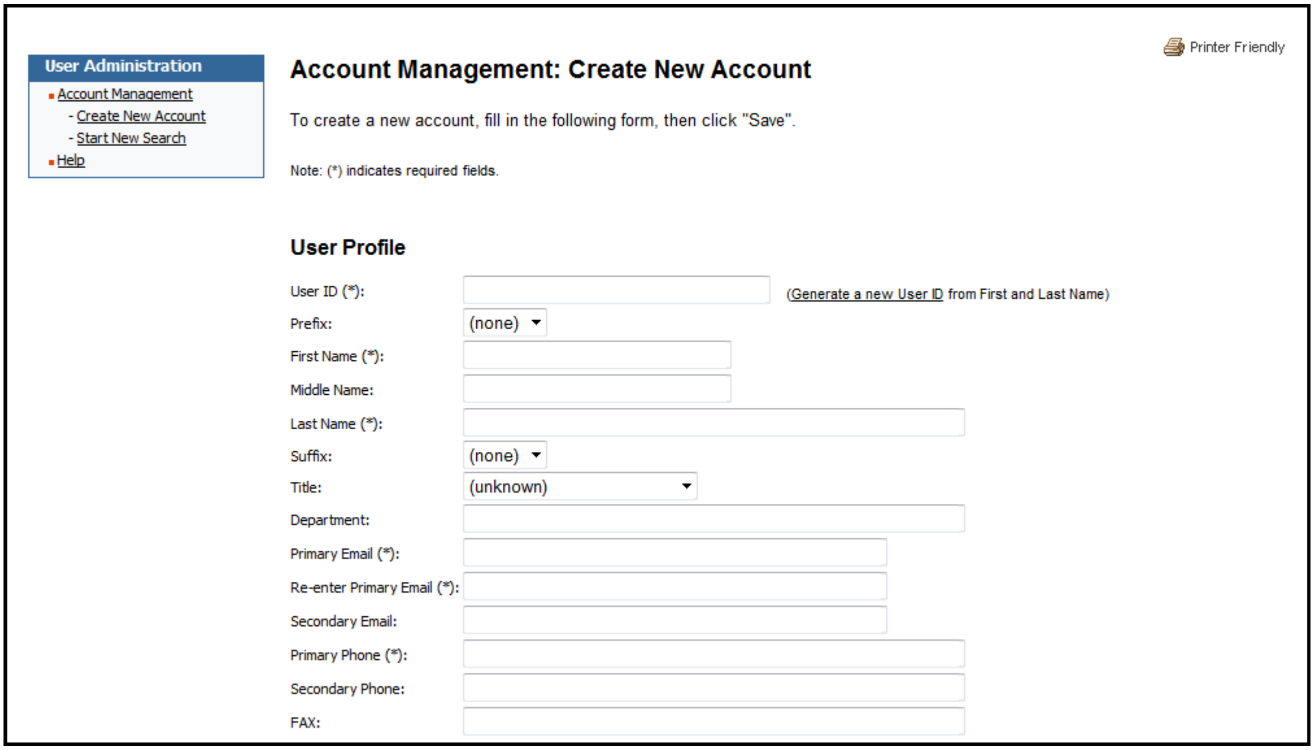
If the AA has a user record, the name will appear in the results.



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

cont.

Result: The **Create New Account** screen displays.



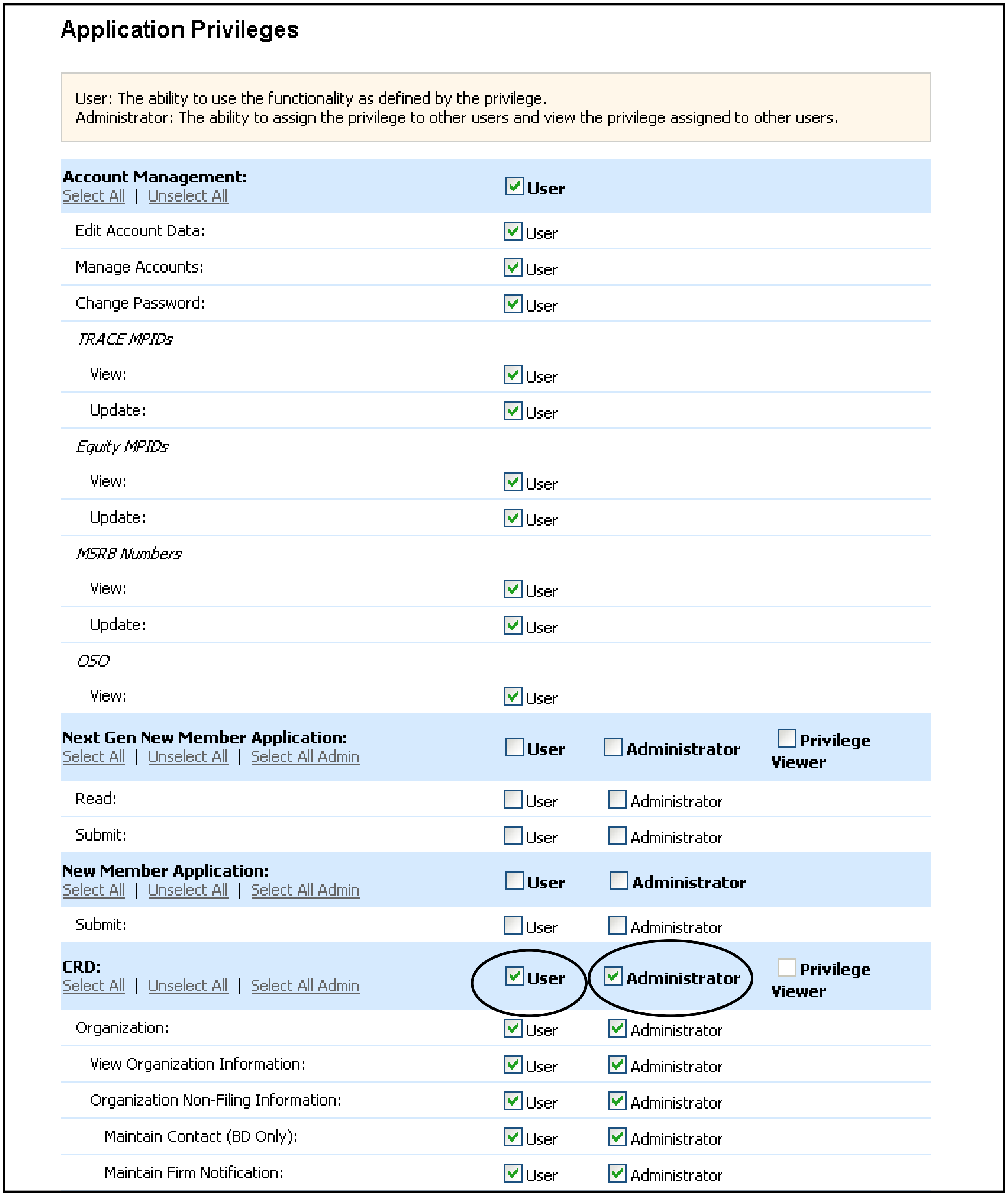
NOTES:

- 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.

Options:
Select All - Shortcut if all “User” privileges are needed for the application.
Unselect All - Shortcut if no privileges are needed for the application.
Select All Admin - Shortcut if all “Administrator” privileges are needed for the application.

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.



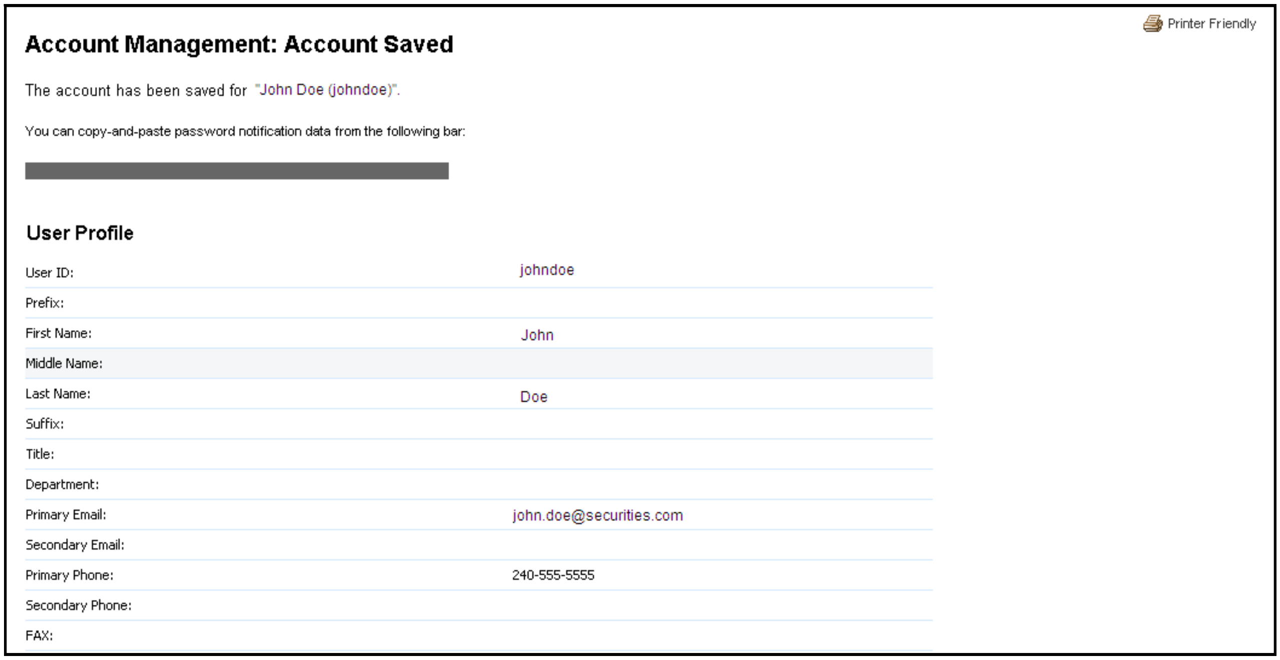
Application Privileges

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.

Account Management: Select All | Unselect All	**User**		
Edit Account Data:	User		
Manage Accounts:	User		
Change Password:	User		
TRACE MPIDs			
View:	User		
Update:	User		
Equity MPIDs			
View:	User		
Update:	User		
MSRB Numbers			
View:	User		
Update:	User		
OSO			
View:	User		
Next Gen New Member Application: Select All | Unselect All | Select All Admin	**User**	**Administrator**	**Privilege Viewer**
Read:	User	Administrator	
Submit:	User	Administrator	
New Member Application: Select All | Unselect All | Select All Admin	**User**	**Administrator**	
Submit:	User	Administrator	
CRD: Select All | Unselect All | Select All Admin	**User**	**Administrator**	**Privilege Viewer**
Organization:	User	Administrator	
View Organization Information:	User	Administrator	
Organization Non-Filing Information:	User	Administrator	
Maintain Contact (BD Only):	User	Administrator	
Maintain Firm Notification:	User	Administrator	

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.

cont.
Result: The **Create New Account** screen displays.

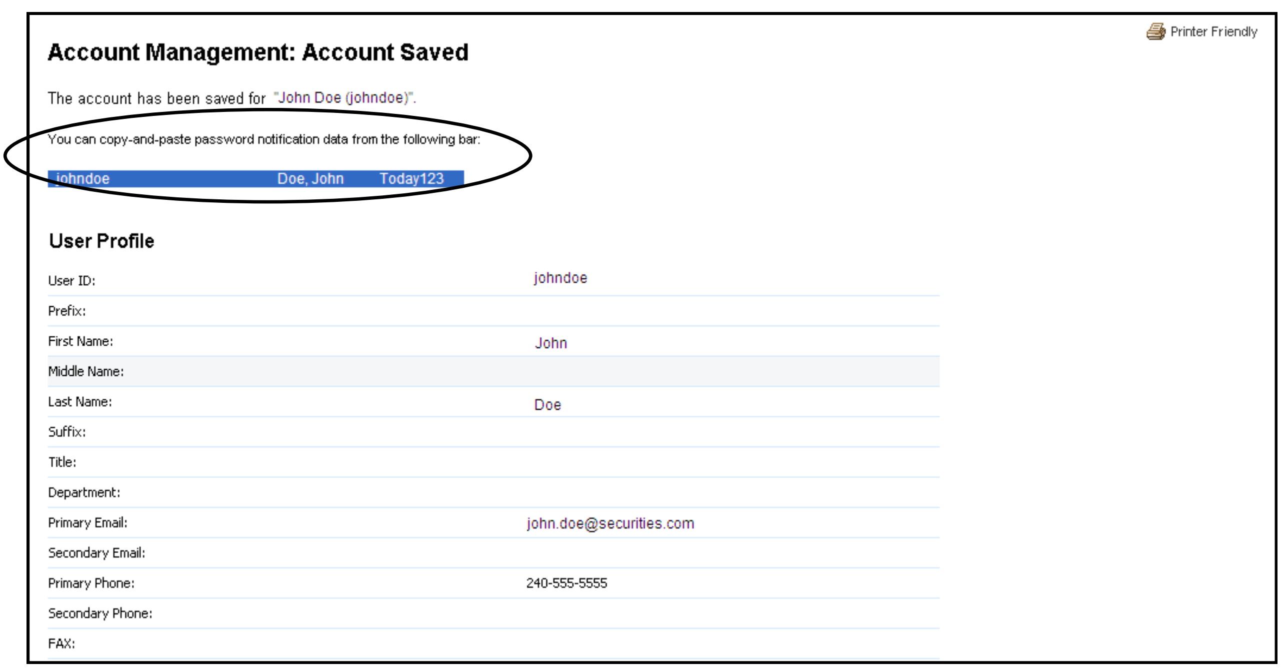


Step 6: Take note of the new User ID and Password, or highlight the bar to copy the User ID and Password, paste it into a document, and provide that information to the user. He/she can now access the application(s).

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**.

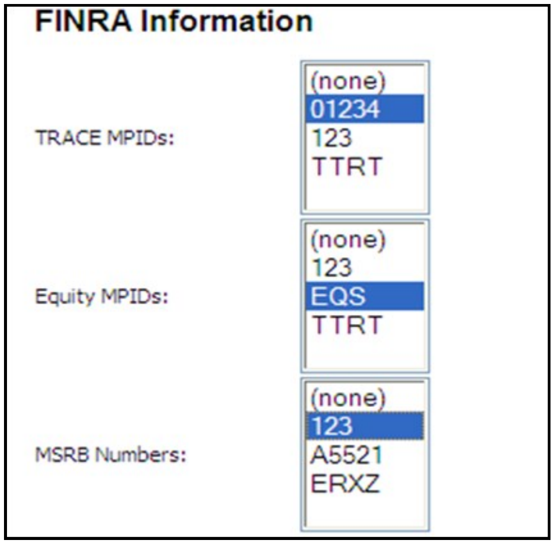
- The date and time the account was created displays in the **Account Created on** field, and the user ID of the person who created the account displays in the **Account Created by** field. If the account was created by an FINRA Administrator, it will display "FINRA".



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.

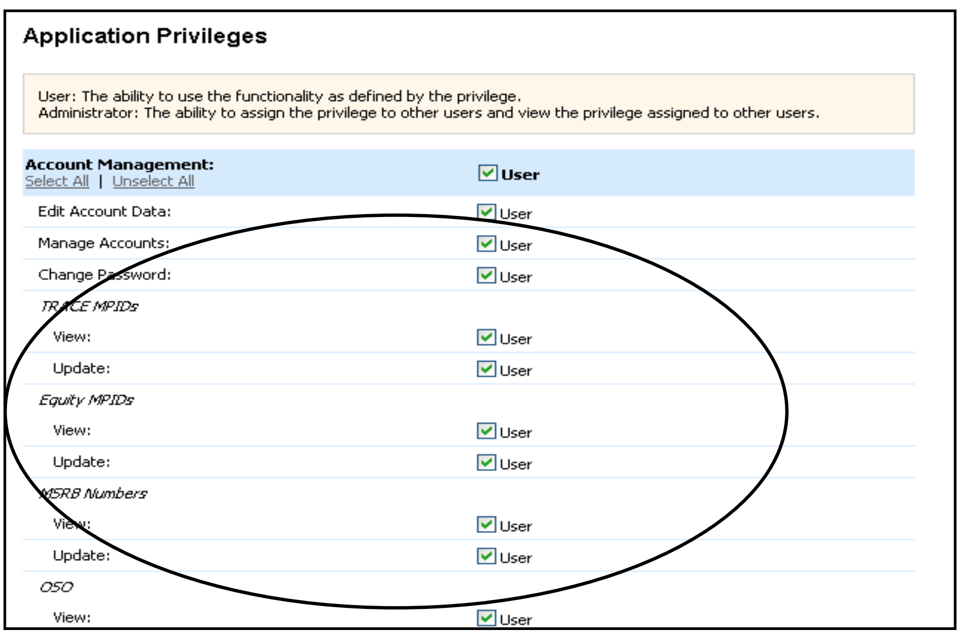


Step 2: In the Application Privileges Section of Account Management, select "User" for both the 'View' and 'Update' privileges for TRACE, Equity, and/or MSRB so that an Account Administrator has the ability to assign that Unique ID(s) to other users.

Roles:

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

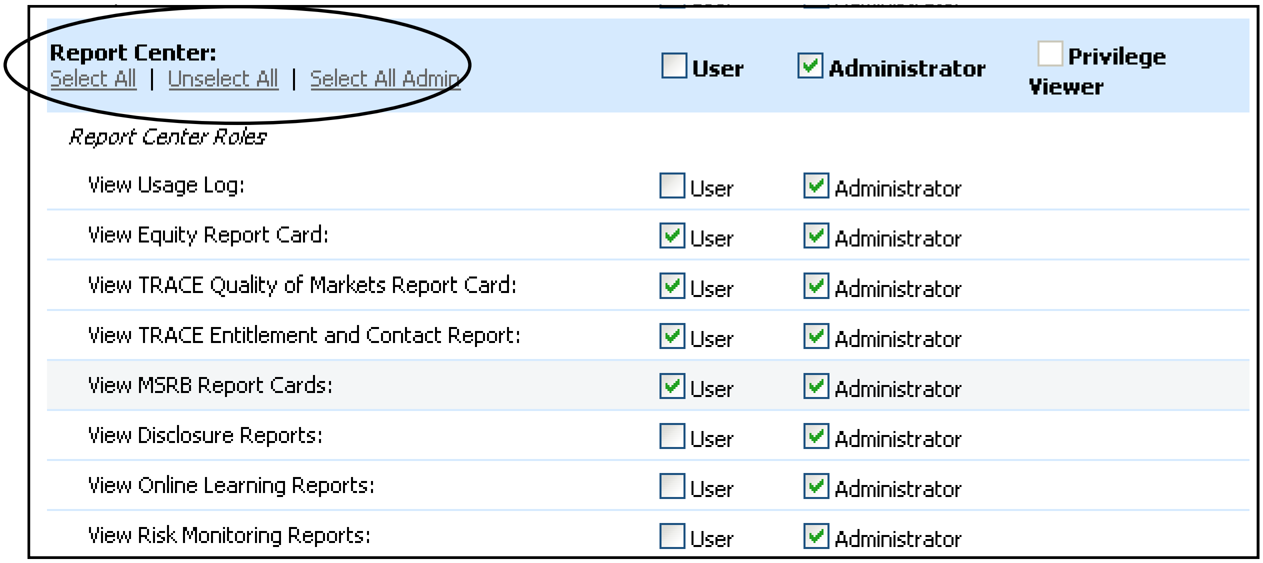
Update - Provides the capability to add or delete from the list of accounts MPID(s) or MSRB(s).



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.

cont.

Options:
Select All - Shortcut if all “User” privileges are needed for the application.
Unselect All - Shortcut if no privileges are needed for the application.
Select All Admin - Shortcut if all “Administrator” privileges are needed for the application.



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

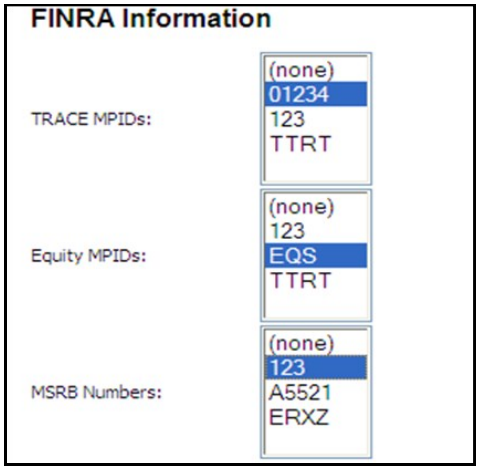
Scenarios for Setting Up an Account Administrator

FINRA Information Section	Account Management Application Privilege Section	Report Center Application associated Privileges (The privilege below must be marked)
Select Equity MPID(s) by clicking on the Equity MPID(s) to highlight	Equity MPID View Update	View Equity Report Card
Select TRACE MPID(s) by clicking on the TRACE MPID(s) to highlight	TRACE MPID View Update	View TRACE Quality of Markets Report Card
Select TRACE MPID(s) by clicking on the TRACE MPID(s) to highlight	TRACE MPID View Update	View TRACE Entitlement and Contact Report
Select TRACE MPID(s) by clicking on the TRACE MPID(s) to highlight	TRACE MPID View Update	TRACE Order Form Submit/Read All
Select TRACE MPID(s) by clicking on the TRACE MPID(s) to highlight	TRACE MPID View Update	TRACE New Issue Form Submit/Read All
Select TRACE MPID(s) by clicking on the TRACE MPID(s) to highlight	TRACE MPID View Update	FINRA Data Delivery TRACE Trade Journal
Select MSRB Number(s) by clicking on the number(s) to highlight	MSRB Number View Update	View MSRB Report Card

cont.

Setting Unique IDs for a User:

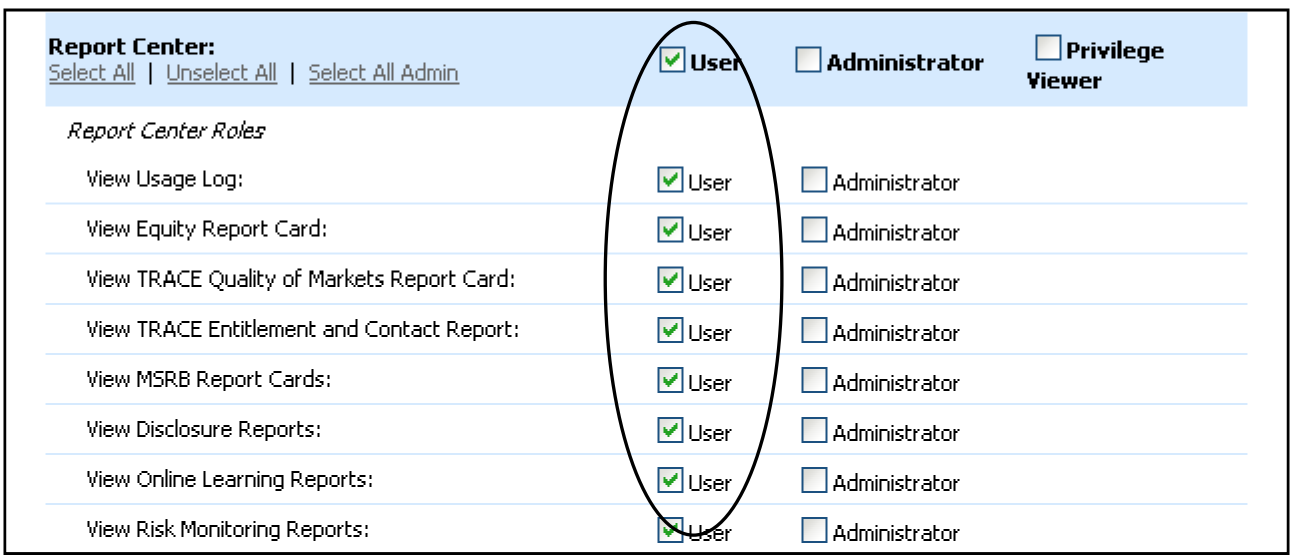
Step 1: In the FINRA Information Section of Account Management, select the Unique ID(s) that an Account Administrator will need to assign to other users. Select the Unique ID by clicking on the MPID(s) and/or MSRB(s). The selected ID will highlight.



Step 2: In 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.



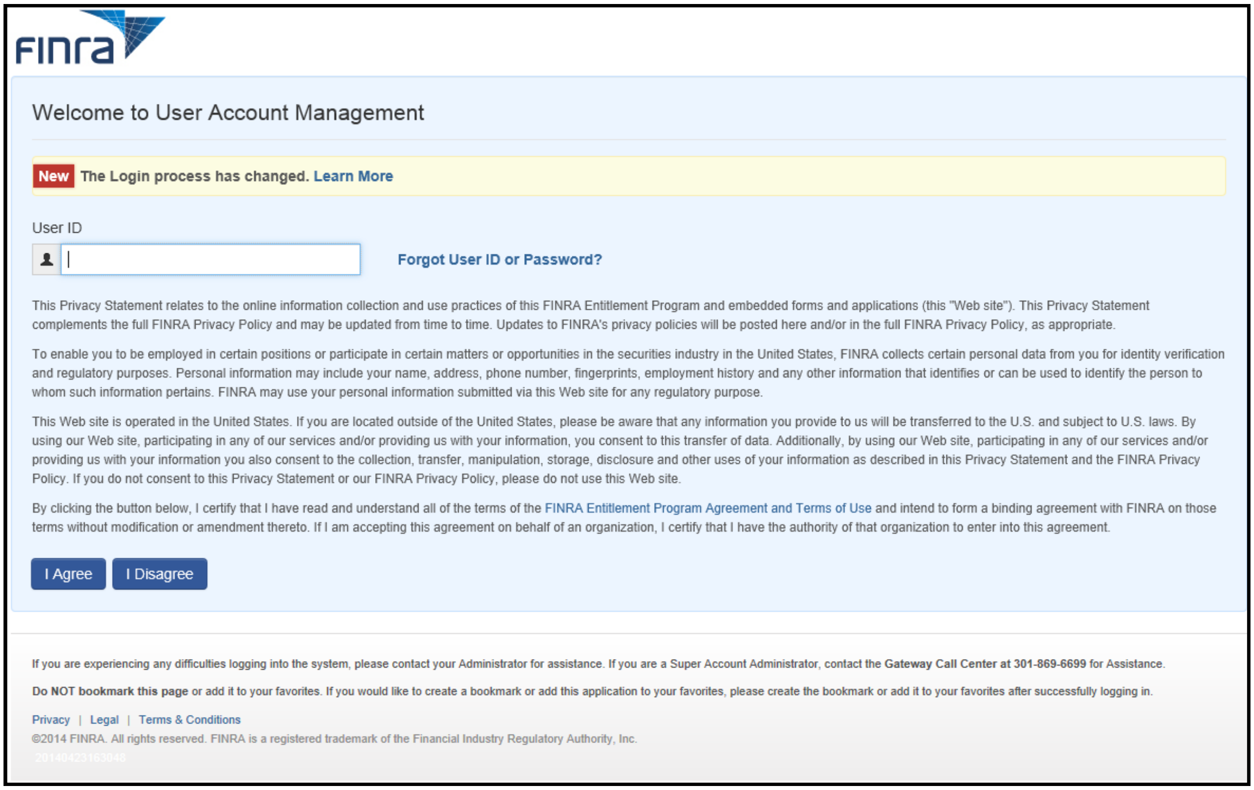
Scenarios for Setting Up a User

FINRA Information Section	Report Center Application associated Privileges (The privilege below must be marked)
Select Equity MPID(s) by clicking on the MPID(s) to highlight	View Equity Report Card
Select TRACE MPID(s) by clicking on the MPID(s) to highlight	View TRACE Quality of Markets Report Card
Select TRACE MPID(s) by clicking on the MPID(s) to highlight	View TRACE Entitlement and Contact Report
Select MSRB Number(s) by clicking on the number (s) to highlight	View MSRB Report Card

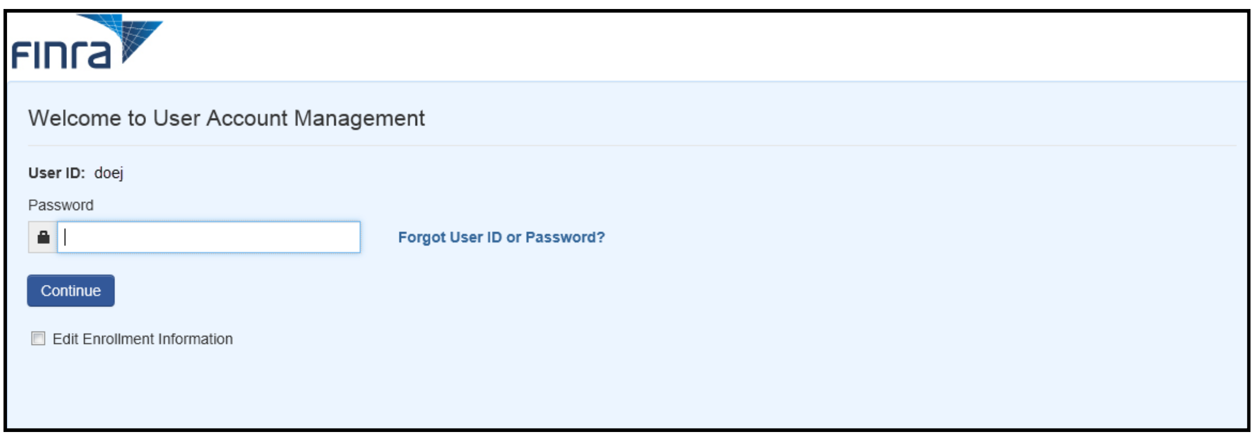
How to directly access the Account Management URL Address:

Step 1: Access the Account Management at
https://accountmgmt.finra.org/ewsadmin2/index.jsp

Step 2: Enter your **User ID**.



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

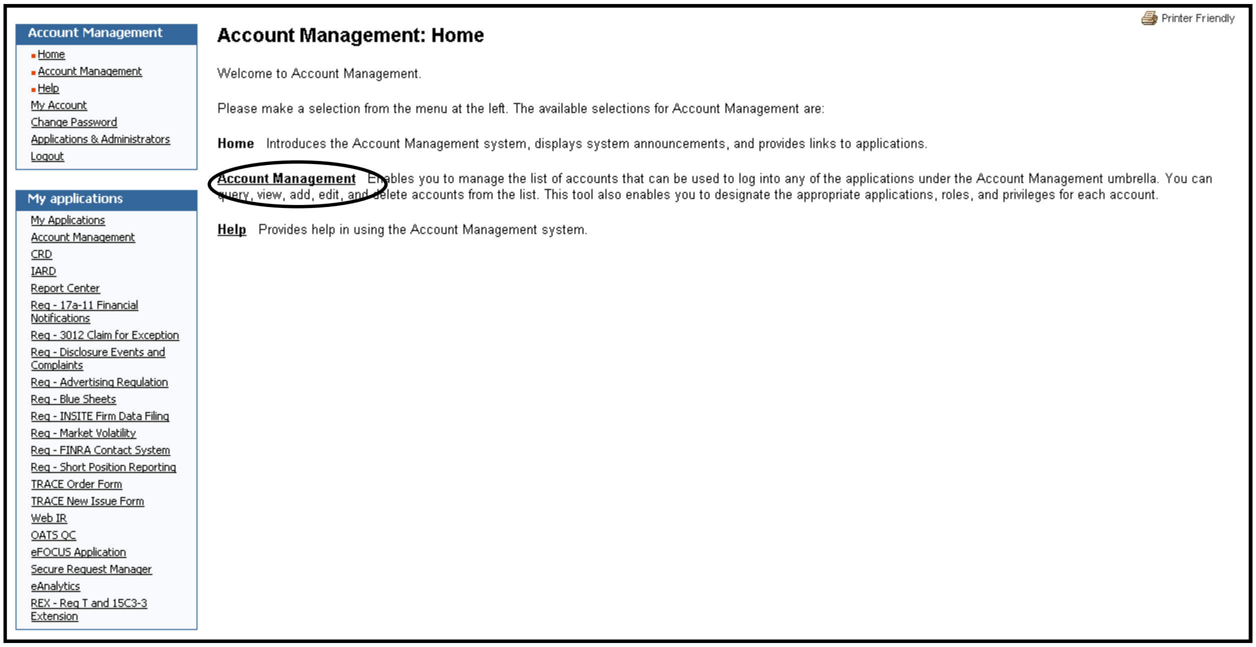


Step 3 Enter your **Password** and click **Continue**.

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.



How to Identify an SAA in Account Management:

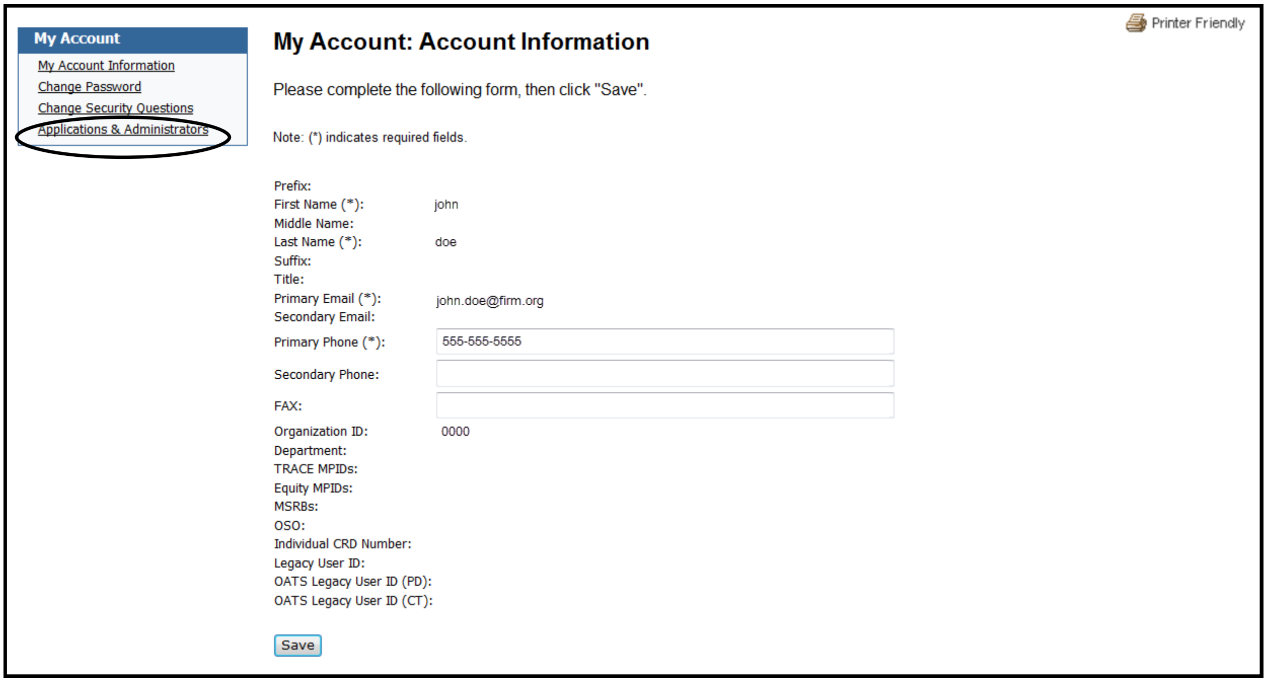
All users can view a list of their firm's Super Account Administrator, Account Administrators and the list of **all** FINRA applications available to your organization.

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

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

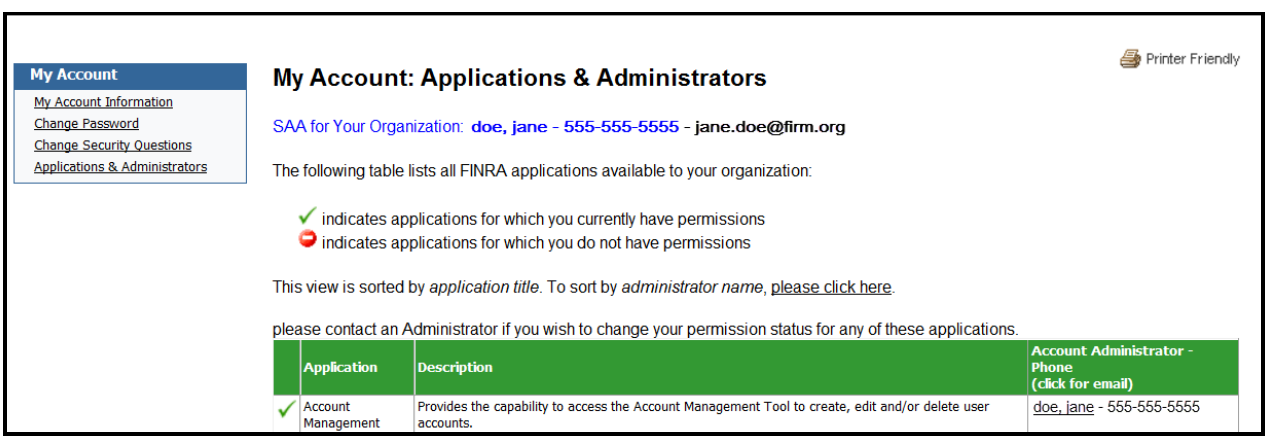
Result: The *Applications & Administrators* screen appears.

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 change by clicking the **Edit Security Questions** checkbox that is located on the **Password screen.**

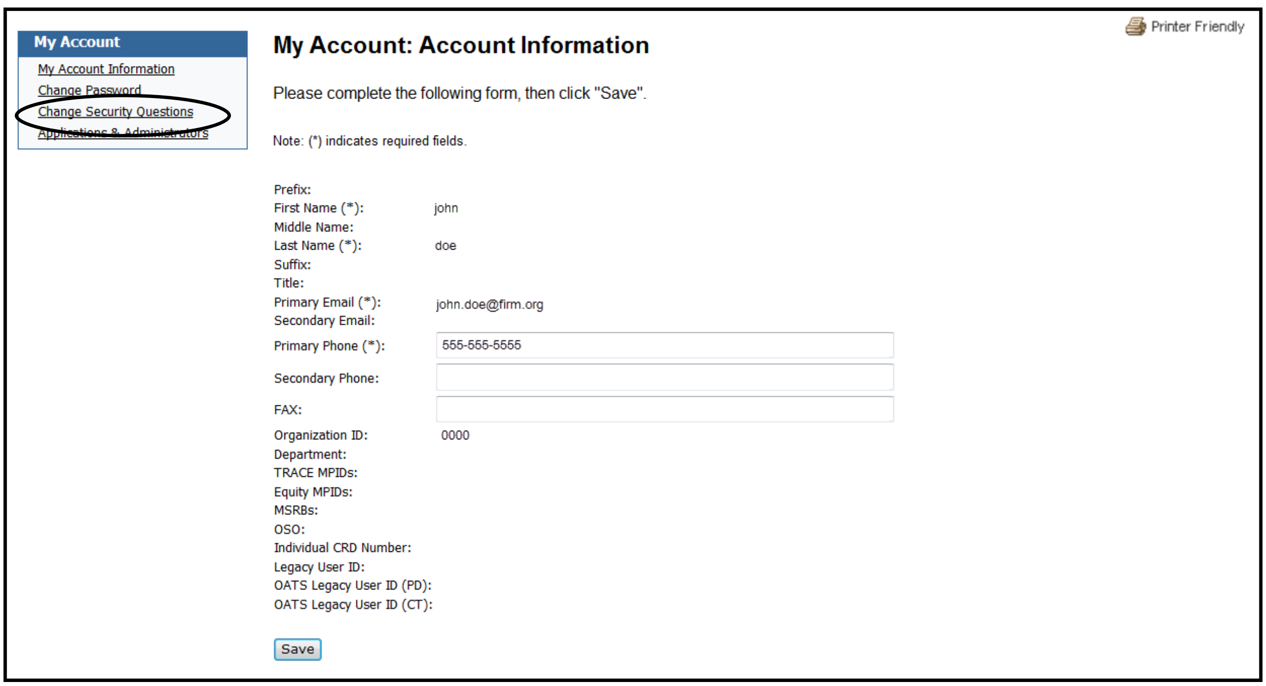
OR

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

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

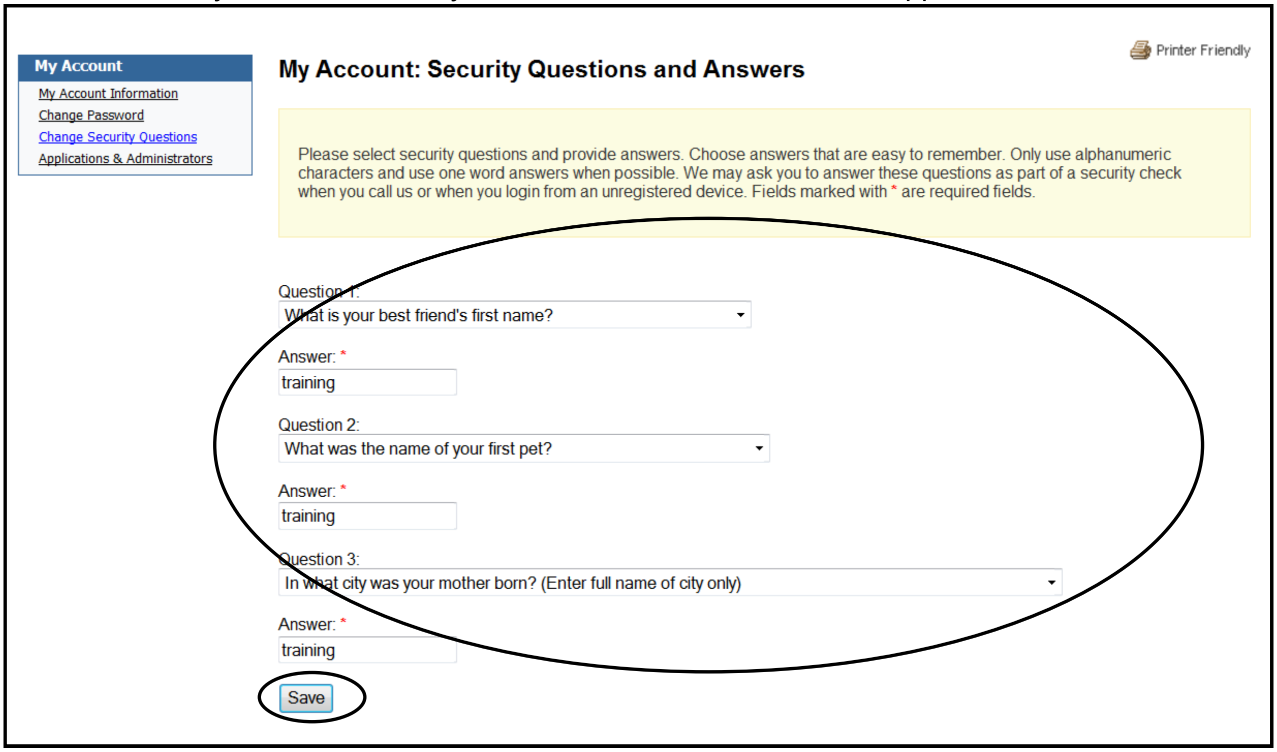
Result: The *Applications & Administrators* screen appears.

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



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

Result: The *My Account: Security Questions and Answers* screen appears.



Step 4: Change your **Security Questions and Answers** as desired and click **Save**.

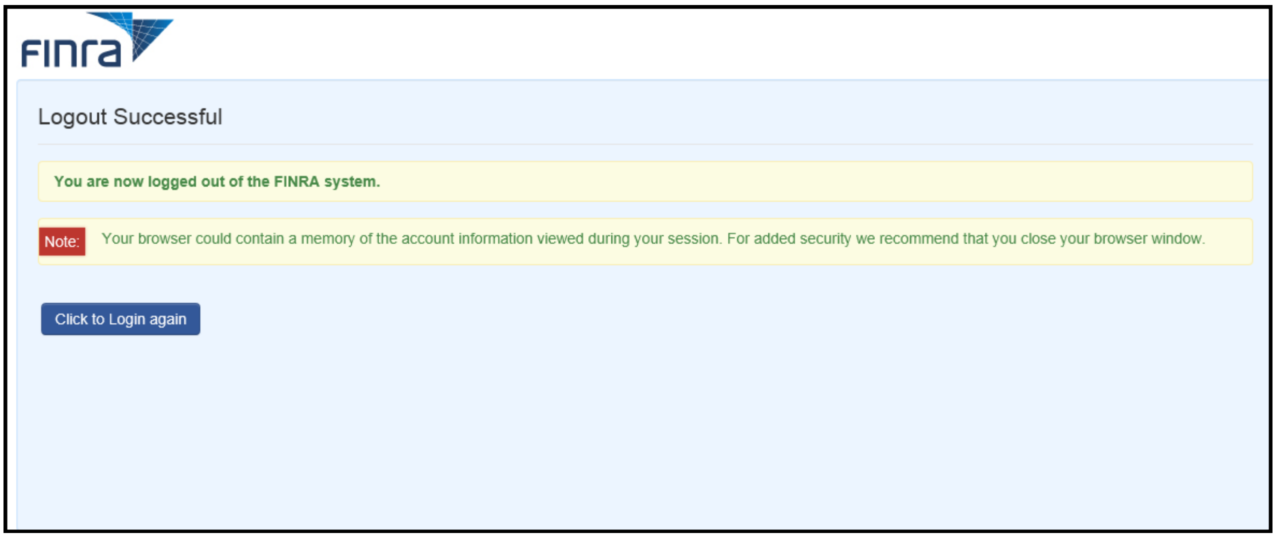
ADDITIONAL NOTES:

- 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.
- This job aid covers information specific to SAAs. Go to the **FINRA Entitlement Program: Account Management for Account Administrators (AAs) & Super Account Administrators (SAAs)** job aid to see steps for functions that are available to SAAs and AAs.

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 again** button. Follow the prompts to log back in.



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.
- This job aid covers information specific to SAAs. Go to the **FINRA Entitlement Program: Account Management for Account Administrators (AAs) & Super Account Administrators (SAAs)** job aid to see steps for functions that are available to SAAs and AAs.