J.P. Morgan Access®
Credential Services
User Guide

April 2020

Last modified: April 13, 2020

This guide is confidential and proprietary to J.P. Morgan and is provided for your general information only. It is subject to change without notice and is not intended to be legally binding. All services described in this guide are subject to applicable laws and regulations and service terms. Not all products and services are available in all locations. Eligibility for particular products and services will be determined by JPMorgan Chase Bank, N.A. or its affiliates. J.P. Morgan makes no representation as to the legal, regulatory or tax implications of the matters referred to in this guide.

J.P. Morgan is a marketing name for the Wholesale Payments businesses of JPMorgan Chase Bank, N.A. and its affiliates worldwide. JPMorgan Chase Bank, N.A., organized under the laws of U.S.A. with limited liability.

Table of Contents

Introduction to Credential Services

As a Security Administrator (SA), you are entrusted by your company to handle security-related information for employees who use J.P. Morgan Access® applications. In that role, you will be managing many of your activities through Credential Services, which is the area within Access Administration that lets you manage User IDs, passwords and digital signing credentials for your company's employees. Credential Services enables you to handle many of your employee requests without contacting J.P. Morgan.

Through Credential Services you can:

- Manage user authentication methods
- Manage machine registration
- Manage self-service client security preferences
- Order and track security tokens

Authentication

Access supports two types of authentication:

- Password-based authentication allows a user to log on with a user ID and password.
- Token-based authentication requires both a password and a second level of security: a security token provided by J.P. Morgan, which will be assigned by you as the SA.

Security Tokens

A security token is a hand-held or software device that displays a new security code every 60 seconds. Users are prompted to enter the numeric code (known as a "token code") appearing on the device, along with a personal password, in order to gain access to protected information and transaction capabilities within Access.

Security tokens are assigned to users for a number of reasons: in order to provide multifactor authentication, meet regulatory mandates, act as a Security Administrator, perform sensitive activities such as wire payment approval and release, or to meet their own corporate requirements.

There are two types of security tokens used by Access. A user can only be assigned one type of token at a time.

An **RSA SecurID®** token is the default token type and is available in two options: a hardware version or a software version.

Users and SAs who are issued an RSA token cannot use it to access China accounts. If access to China accounts is required, the user or SA must use the second type of token, a Feitian token.

A **Feitian** token is for any user who is entitled to China accounts or who resides in China. Security Administrators who oversee users with China accounts will also use a Feitian token. Users and SAs who use a Feitian token can use the same token to access both China and non-China accounts.

Credential Services enables you to assign security tokens to users and to manage and maintain the use of those tokens.

Approving Security Activities

Security Administrators can use Credential Services to initiate or approve security-related activities. Some critical tasks may require two SAs. For example, one SA may initiate a user setup action (e.g., retrieving a user password), but another SA must approve the action.

The following actions do not require dual-SA approval:

- Inactivate an active user
- Retrieve password for new user
  (The user is auto-activated when the Add User Request is approved. The system will email the user their User ID and password.)
- Unlock password
- Get activation code
- Activate/deactivate Single Machine Registration
- Unlink a machine from a User ID
- Unassign a token
- Revoke temporary token codes for existing user
  (Temporary token codes MUST be revoked to enable the user to resume use of a physical token again.)

Getting Started

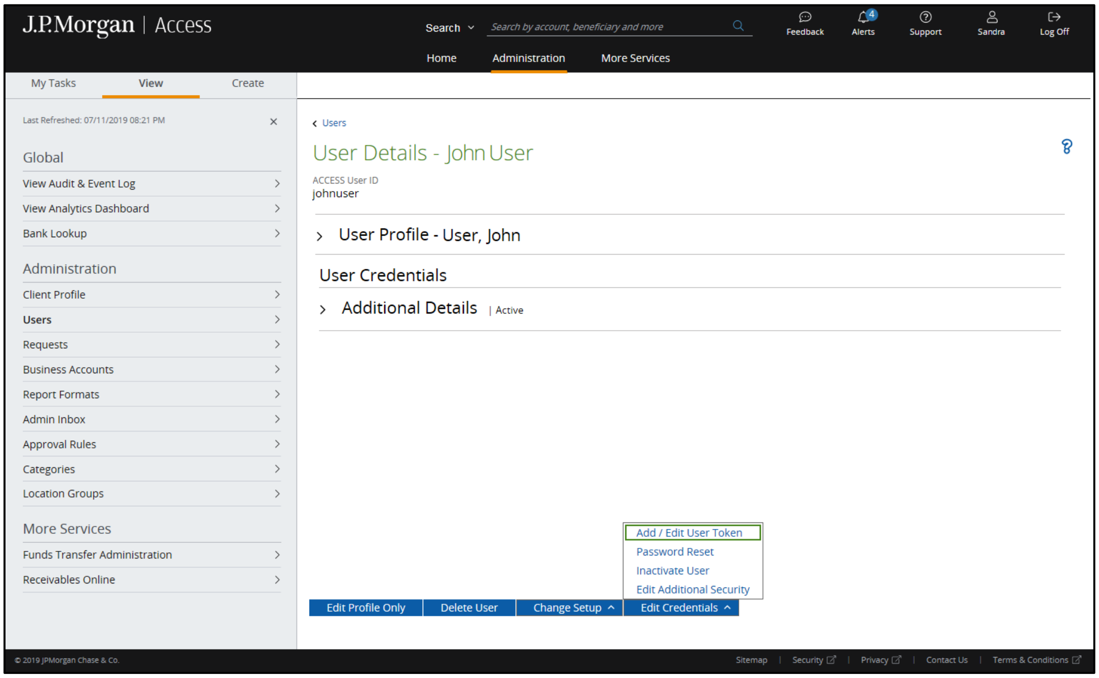
Accessing Credential Services

You can access Credential Services in Access Administration from either the User Details screen or the Edit Users screen. Depending on your entitlements, Credential Services options may include:

- Reactivate User
- Inactivate User
- Unlock User
- Reset Password
- Edit Additional Security
- Add/Edit User Token

To access Credential Services from the User Details screen:

1. From the View tab on the Activity Bar, click **Users**.
2. Select a user from the Users list.
3. Click **Edit Credentials** and select a Credential Services option.



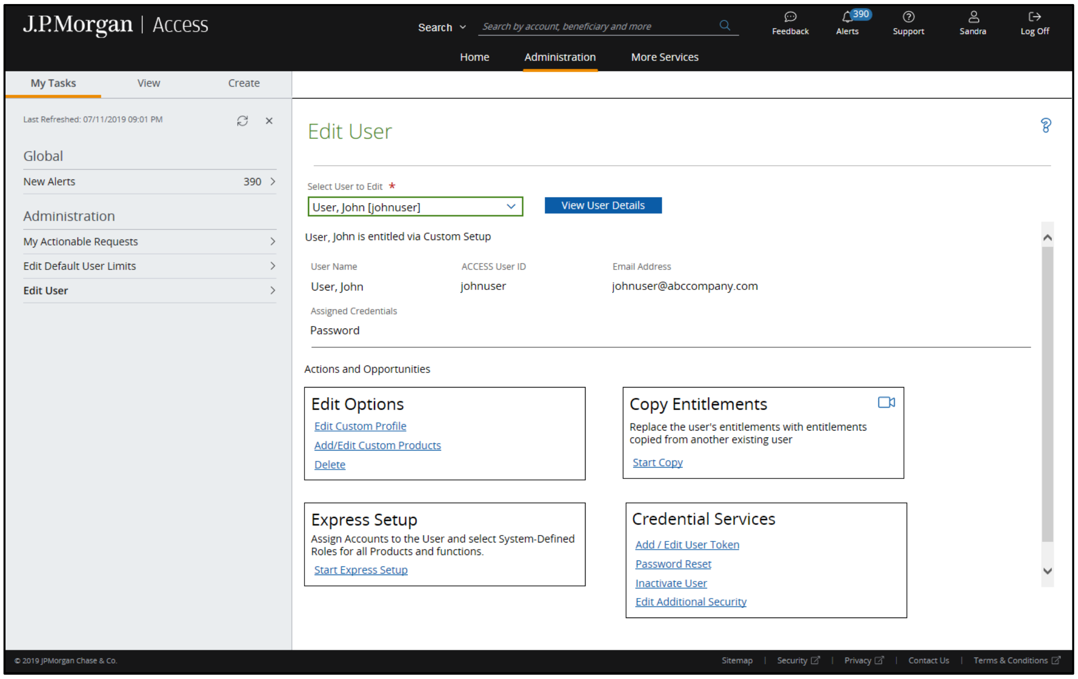
User Details - John User

ACCESS User ID
johnuser

Last Refreshed: 07/11/2019 08:21 PM

To access Credential Services from the Edit User screen:

1. From the My Tasks tab on the Activity Bar, click **Edit User**.
2. Type a user name or select one from the dropdown.
3. Select an option from the Credential Services box.



Last Refreshed: 07/11/2019 09:01 PM

Global

New Alerts 390

Administration

My Actionable Requests

Edit Default User Limits

Edit User

Edit User

Select User to Edit *

User, John [johnuser]

User, John is entitled via Custom Setup

User Name	ACCESS User ID	Email Address
User, John	johnuser	johnuser@abccompany.com

Assigned Credentials

Password

Actions and Opportunities

Edit Options

- Edit Custom Profile
- Add/Edit Custom Products
- Delete

Copy Entitlements

Replace the user's entitlements with entitlements copied from another existing user

- Start Copy

Express Setup

Assign Accounts to the User and select System-Defined Roles for all Products and functions.

- Start Express Setup

Credential Services

- Add / Edit User Token
- Password Reset
- Inactivate User
- Edit Additional Security

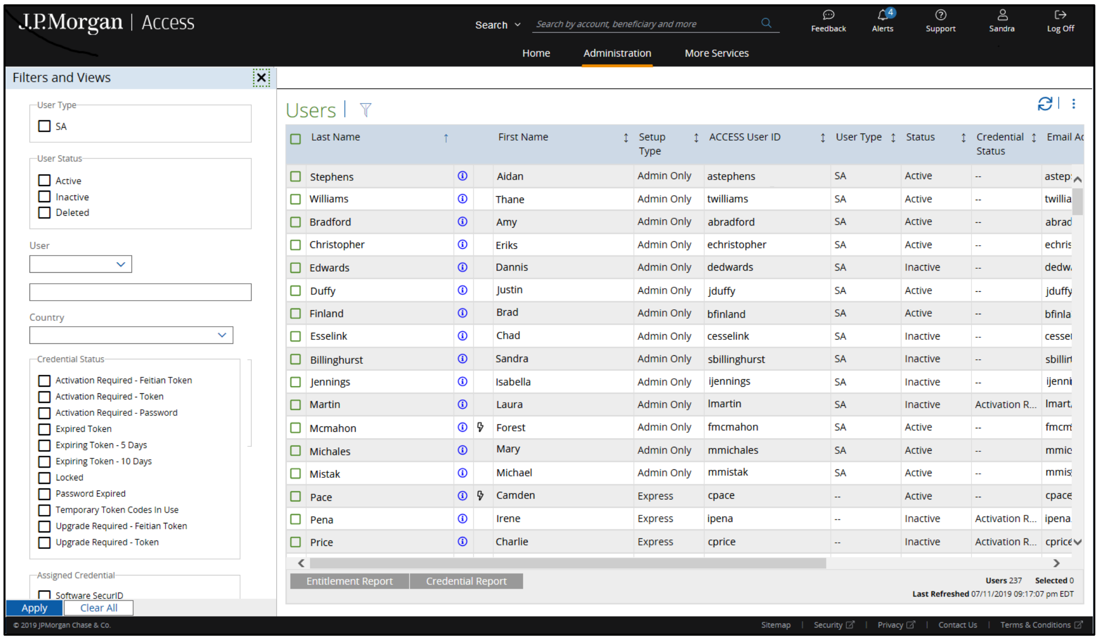
© 2019 JPMorgan Chase & Co.
Sitemap | Security | Privacy | Contact Us | Terms & Conditions

Viewing Credential Status of Users

You can view credential status as well as search for users by credential status on the Users list.

1. From the View tab on the Activity Bar, click **Users**.
2. The Credential Status column displays credential activity by user.
3. Click the filter icon at the top of the list and select filters from the Credential Status box, including statuses such as Activation Expired, Activation Pending, Activation Required, Token Expired, Temporary Tokens in Use, Token Upgrade Required and more.
4. Click **Apply** to display the filtered list of users.

Note: You can also generate a Credential Report that provides user credential status and token expiry details by clicking the **Credential Report** button at the bottom of the Users list.



Filters and Views

User Type
☐ SA

User Status
☐ Active
☐ Inactive
☐ Deleted

User

Country

Credential Status
☐ Activation Required - Feitian Token
☐ Activation Required - Token
☐ Activation Required - Password
☐ Expired Token
☐ Expiring Token - 5 Days
☐ Expiring Token - 10 Days
☐ Locked
☐ Password Expired
☐ Temporary Token Codes In Use
☐ Upgrade Required - Feitian Token
☐ Upgrade Required - Token

Assigned Credential
☐ Software SecurID

Users

Last Name	First Name	Setup Type	ACCESS User ID	User Type	Status	Credential Status	Email Ac
Stephens	Aidan	Admin Only	astephens	SA	Active	--	astep
Williams	Thane	Admin Only	twilliams	SA	Active	--	twillia
Bradford	Amy	Admin Only	abradford	SA	Active	--	abrad
Christopher	Eriks	Admin Only	echristopher	SA	Active	--	echris
Edwards	Dannis	Admin Only	dedwards	SA	Inactive	--	dedw.
Duffy	Justin	Admin Only	jduffy	SA	Active	--	jduffy
Finland	Brad	Admin Only	bfinland	SA	Active	--	bfinla
Esselink	Chad	Admin Only	cesselink	SA	Inactive	--	cessel
Billinghurst	Sandra	Admin Only	sbillinghurst	SA	Inactive	--	sbillin
Jennings	Isabella	Admin Only	ijennings	SA	Inactive	--	ijenni
Martin	Laura	Admin Only	lmartin	SA	Inactive	Activation R...	lmart.
Mcmahon	Forest	Admin Only	fmcmahon	SA	Active	--	fmcm
Michales	Mary	Admin Only	mmichales	SA	Active	--	mmic
Mistak	Michael	Admin Only	mmistak	SA	Active	--	mmis
Pace	Camden	Express	cpace	--	Active	--	cpace
Pena	Irene	Express	ipena	--	Inactive	Activation R...	ipena
Price	Charlie	Express	cprice	--	Inactive	Activation R...	cprice

Users 237 **Selected** 0
Last Refreshed 07/11/2019 09:17:07 pm EDT

© 2019 JPMorgan Chase & Co.

Sitemap | Security | Privacy | Contact Us | Terms & Conditions

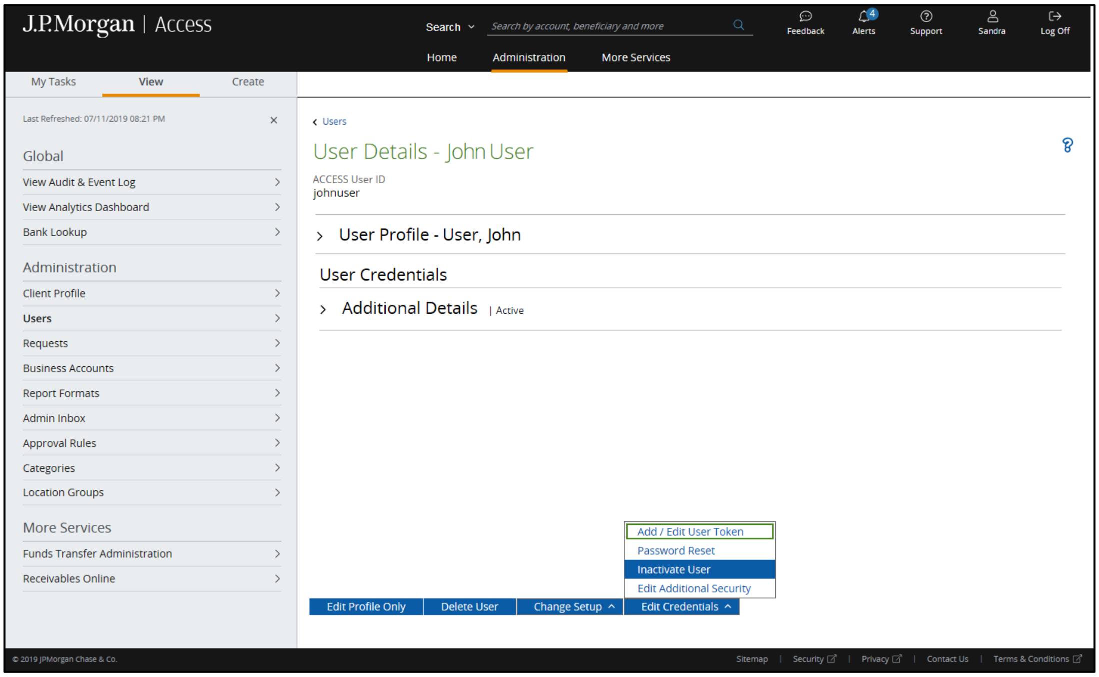
Inactivating/Reactivating Users

Inactivating Users

Security Administrators must inactivate active users if they wish to prevent them from using Access. One Security Administrator may inactivate an active user; an approving SA is not required.

To inactivate an active user:

1. From the User Details page, click **Edit Credentials** and select **Inactivate User**.
2. Click **Continue**, and then click **Ok** to close the confirmation window. The status is now changed to Inactive and the user will not be able to log on.



User Details - John User

ACCESS User ID
johnuser

Reactivating Users

A user becomes inactive if the user has not logged on for an extended period or if an SA has inactivated the user.

To reactivate an inactive user:

1. From the User Details page, click **Edit Credentials** and select **Reactivate User**.
2. Click **Submit for Approval**, and then click **Ok** to close the confirmation window. The user is activated pending another SA's approval.

Approving Reactivated Users

1. From the View tab on the Activity Bar, click **Requests.**
2. Click the Reactivate User request you want to approve.
3. Click **Approve** at the bottom of the Request Details page.
4. Click **Continue**, and then click **Ok** to close the confirmation window. The user is now activated.

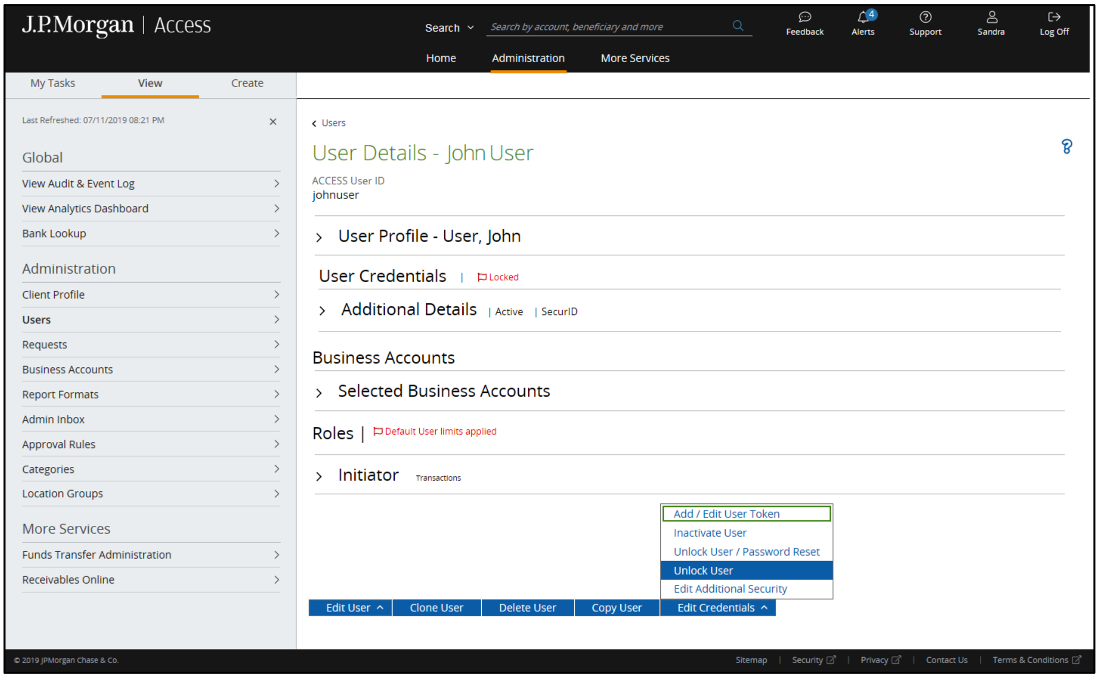
Managing Passwords

Unlocking Users

After excessive unsuccessful logon attempts, users are locked out and may not log on until their User IDs are unlocked. One Security Administrator can unlock a user; a second SA's approval is not required.

To unlock a user:

1. From the User Details page, click **Edit Credentials** and select **Unlock User**.
2. Click **Continue** to unlock the user, and then click **Ok** to close the confirmation window.
3. Inform the user that his/her User ID has been unlocked.



You can also unlock a user and reset their password:

1. From the User Details page, click **Edit Credentials** and select **Unlock User/Password Reset**.
2. Click **Submit for Approval**, and then click **Ok** to close the confirmation window. The password is reset pending another SA's approval.

Resetting Passwords

If a user forgets a password, a Security Administrator can reset it. To reset a user's password, the user must have a status of Active.

To reset a password:

1. From the User Details page, click **Edit Credentials** and select **Password Reset**.
2. Click **Submit for Approval**, and then click **Ok** to close the confirmation window.
3. If the user is a password-only user, provide the temporary password to the user in a secure manner.
4. All password resets (for both password-only and security token users) require approval by a second SA.

Notes:

- For security token users, the temporary password is not displayed. After the second SA approves the password reset, token users will receive an email.
  - Non-Hong Kong ALU (HKALU) users will receive an email message containing a temporary password from J.P. Morgan.
  - HKALU users will receive an email with instructions on how to retrieve their password via the Forgot or Retrieve Password/User ID link on the logon page.
- Access provides a way for users to reset their own passwords online, when a new user is initially set up or at any time thereafter.
  - Non-HKALU users can register for Express Password Reset. Instruct users to select **Profile** or **Preferences** from the Access dashboard and click **Password Setup**. After registering for Express Password Reset, users can click **Forgot or Retrieve Password/User ID** on the logon page any time they forget their password.
  - HKALU users can click the Forgot or Retrieve Password/User ID link and select their preferred delivery method for the temporary password message (SMS text or voice callback).

Approving Password Resets

To approve a password reset:

1. Before approving, confirm that the user has requested the password reset. If the user is a password-only user, confirm that he/she has received the new temporary password from the initiating SA.
2. From the View tab on the Activity Bar, click **Requests**.
3. Click the Password Reset request you want to approve.
4. Click **Approve** at the bottom of the Request Details page.
5. Click **Continue**, and then click **Ok** to close the confirmation window. An email message is sent to the user containing either a temporary password associated with the token or instructions on how to obtain it through SMS text or voice callback.

Note: Temporary passwords are only valid for five days; SAs should notify users to log on to Access and change the temporary password as soon as possible.

Machine Registration and User Activation

Edit Additional Security

You can change machine registration settings through Credential Services.

Multiple Machine Registration

Multiple Machine Registration (MMR) allows users to log on to Access from multiple computers.

To enable registration for multiple machines and get activation codes for them:

1. From the User Details page, click **Edit Credentials** and select **Edit Additional Security**.
2. Under Machine Registration Preference, select **Multiple**.
3. From the Select Action dropdown, select **Get Activation Codes**.
4. Click **Submit**, and then click **Continue.** A confirmation window will display with the user's Activation Codes.
5. Record the Activation Codes and distribute it to the user in a secure manner.
6. Click **Ok** to close the confirmation window.

Single Machine Registration

Single Machine Registration (SMR) is designed to prevent unauthorized logons to Access. When SMR is activated, the user will be able to log on from only one computer. If the user attempts to log on to Access from a different computer, access is denied.

To change the computer that is registered:

1. From the User Details page, click **Edit Credentials** and select **Edit Additional Security**.
2. Under Machine Registration Preference, select **Single**, and then click **Submit**.
3. Click **Continue**, and then click **Ok** to close the confirmation window. The computer is now unregistered.
4. Log off and then log on from the computer to be registered.
5. Request and enter an Activation Code and complete the logon. The new machine is now registered.

Unlink Machines

Each time a user logs on to Access, the computer they use must be registered and is thereby linked to their User ID. You may unlink machines if a user loses a computer or is suspected of fraudulent activity.

To unlink machines from a User ID:

1. From the User Details page, click **Edit Credentials** and select **Edit Additional Security**.
2. Under Machine Registration Preference, select **Multiple**.

3. From the Select Action dropdown, select **Unlink Machines**, and then click **Submit**.
4. Click **Continue**, and then click **Ok** to close the confirmation window. All computers associated with the User ID are now unregistered. If the user has several computers linked to his/her User ID, you cannot unlink a single machine.

Note: Unlinking unregisters all the user’s associated computers. When the user attempts to log on to Access from any computer, he/she will be required to request and enter an activation code to register the machine.

Password User Auto Activated

When a user is created with password-only credentials, they are automatically activated and will receive email approval of user creation indicating that they have auto activated and can log on.

Managing Security Token Users

New Security Token Users

New users, or password-only users being upgraded to security tokens, can be administered through the Credential Services. Token users must have a specific token associated with their User ID.

There are two types of tokens available:

- **RSA SecurID** tokens (hardware or software)

  Note: Users can only use either a hardware token or a software token; they cannot use both.

- **Feitian** tokens are to be assigned to China users. China users are defined as:
  - Users and Security Administrators who reside in China
  - Users who have access to China accounts
  - Security Administrators who support clients with users who have access to China accounts.

  Note: Users who have access to both China and non-China accounts will use a Feitian token to access both types of accounts.

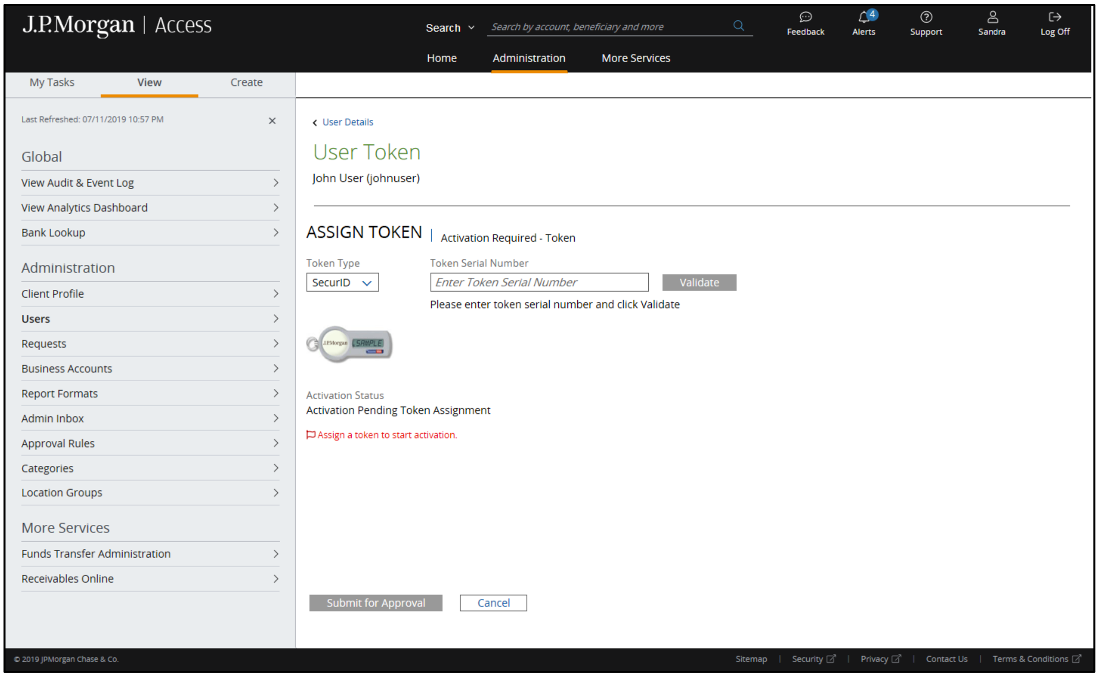
Security Administrators have the responsibility of assigning tokens and distributing hardware tokens to users who require them. All SAs in your organization will receive an email message when there is a user who requires a new token.

Add/Edit User Token

Assigning Hardware Tokens

To assign a token to a new or existing user:

1. From the User Details page, click **Edit Credentials** and select **Add/Edit User Token**.
2. On the User Token page, select a Token Type from the dropdown.
3. Obtain an unassigned token from your inventory. Make sure the token type matches the token type you've selected (and the token image displayed on the screen).
4. Locate the serial number on the back of the token, enter it in the Token Serial Number field and click **Validate**.
5. After you receive a Validation Successful message, click **Submit for Approval**.
6. Click **Submit for Approval**, and then click **Ok** to close the confirmation window.
7. Distribute the token to the user in a secure manner.
8. Notify another Security Administrator within your organization that the token requires approval. The second SA completes the token assignment process.



Last Refreshed: 07/11/2019 10:57 PM

User Token

John User (johnuser)

ASSIGN TOKEN | Activation Required - Token

Token Type: SecurID

Token Serial Number: Enter Token Serial Number

Please enter token serial number and click Validate

Activation Status

Activation Pending Token Assignment

Assign a token to start activation.

Assigning Software Tokens

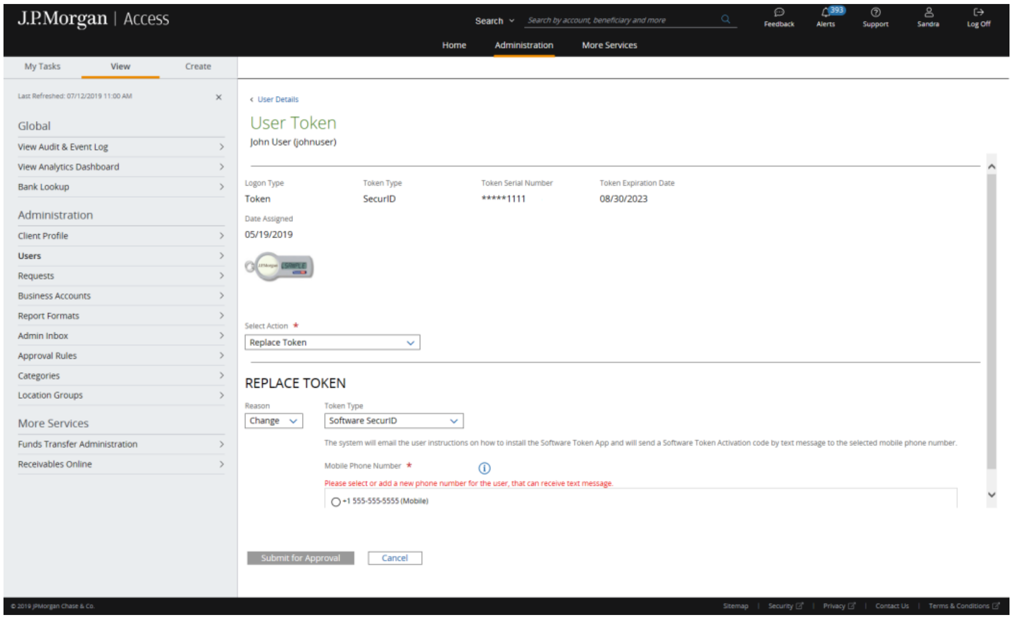
To assign a token to a new or existing user:

1. From the My Tasks tab on the Activity Bar, click **Edit Users** and select a user to be edited from the dropdown.
2. Select **Add/Edit User Token** under Credential Options.
3. On the User Token page, select **Replace Token** from the Select Action dropdown, select **Change** from the Reason dropdown, and select **Software SecurID** from the Token Type dropdown.
4. Select a mobile phone number that can receive text messages.

   Note: User must have a mobile number in their Access profile before a software token is assigned in order to receive an activation code to register the token.

5. Click **Submit for Approval**, and then click **Ok** to close the confirmation window.
6. Notify another Security Administrator within your organization to approve the request.
7. Once the request is approved, the user will receive a text message with the software token activation code as well as email with logon credentials and instructions on how to download the RSA SecurID Software Token App onto their mobile device and authenticate it.

Note: Users should ensure that they are able to access the Apple® App Store^{SM} or Google Play^{TM} for Android^{TM} online store, which typically require a personal authentication on their mobile device before allowing the download.



User Token

John User (johnuser)

Logon Type	Token Type	Token Serial Number	Token Expiration Date
Token	SecurID	*****1111	08/30/2023

Date Assigned
05/19/2019

Select Action *
Replace Token

REPLACE TOKEN

Reason: Change
Token Type: Software SecurID

The system will email the user instructions on how to install the Software Token App and will send a Software Token Activation code by text message to the selected mobile phone number.

Mobile Phone Number *

Please select or add a new phone number for the user, that can receive text message.

○ +1 555-555-5555 (Mobile)

Software Token Instructions for New Users

New Access users that are set up with a software token will receive two emails:

- One email will contain the User ID and two documents attached: the J.P. Morgan Access New User Quick Start Guide and RSA Soft Token Registration instructions in PDF format.
- The other email will contain a temporary password and instructions to set up a new password.

Any user that is provisioned with a software token will be automatically converted to an Alternate Logon User-Hardware Security Model (ALU-HSM) status which has additional password rules.

Software Token Instructions for Current Users

Current Access users that are set up with a software token will receive one notification email, which will have the RSA Soft Token Registration instructions in PDF format attached.

If the user is not already an ALU-HSM status (e.g., they are currently Password Only or SecurID only users), when they are assigned a software token, they will be automatically converted to an ALU-HSM status and will receive a second email with a temporary password and instructions to set up a new password.

Note: You can retain your hardware token until you are comfortable with using the software token only. If you no longer require the hardware token, please mail or courier the token to:

Attention: J.P. Morgan Access Expired Tokens
10410 Highland Manor Drive - Floor 03
Tampa, FL, 33610-9128, United States

J.P. Morgan Access® Mobile^{sm} Application Users

If a user is also entitled to the J.P. Morgan Access® Mobile^{sm} application, they will need to log on to Access via a desktop or laptop with the software token first. After the first logon, they will be able to use software token with Mobile.

Software Token Restricted Countries

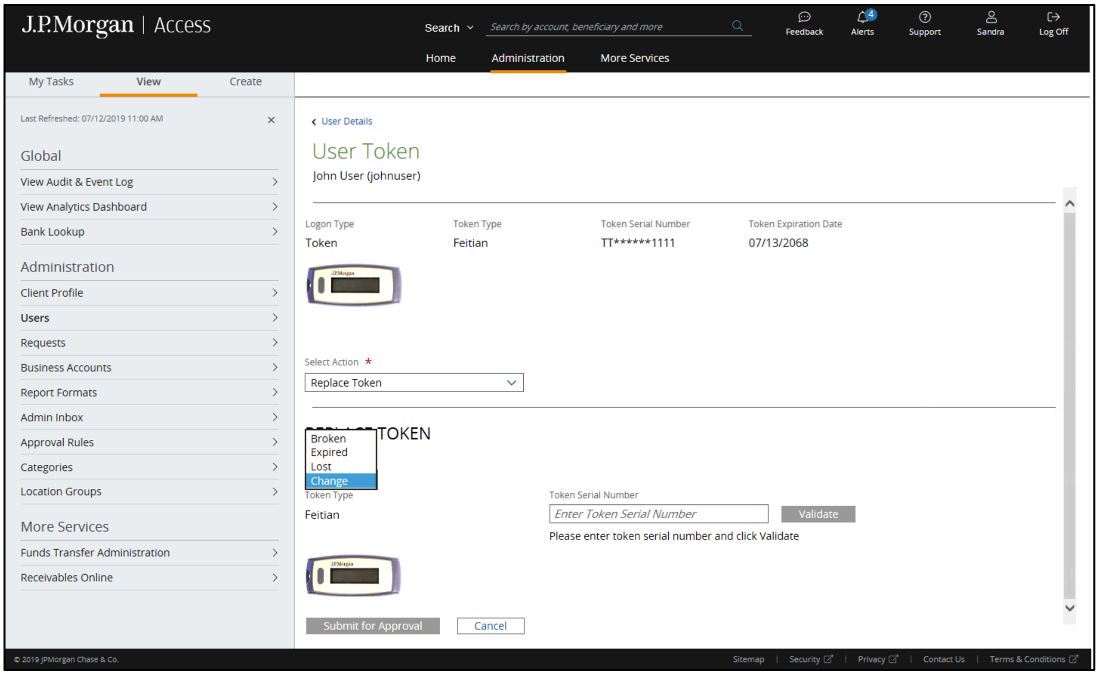
If your Client profile is entitled to a country whose accounts are restricted from using software tokens, you will not be able to provision a software token to any users who have access to those. Such users will be assigned (or continue to use) hardware tokens. At this time there are no countries that are restricting software tokens. If at any point this changes, we will notify clients of their options to adhere to that country's regulatory restrictions.

Replacing Tokens

In the event that a token is broken, expired or lost, a user will need a replacement.

To replace the security token:

1. From the User Details page, click **Edit Credentials** and select **Add/Edit User Token**.
2. On the User Token page, select **Replace Token** from the Select Action dropdown.
3. In the Replace Token panel, select a Reason (Broken, Expired, Lost or Change).
4. Obtain a new and unassigned security token from your inventory. Make sure the token type is accurate.
5. Locate the serial number on the back of the token, enter it in the Token Serial Number field and click **Validate**.
6. After you receive a Validation Successful message, click **Submit for Approval**.
7. Click **Submit for Approval**, and then click **Ok** to close the confirmation window.
8. In a secure manner, provide the security token to the user.
9. Notify another Security Administrator to approve your request. The new security token can be used only if it is approved.



User Token

John User (johnuser)

Logon Type	Token Type	Token Serial Number	Token Expiration Date
Token	Feitian	TT******1111	07/13/2068

Select Action * Replace Token

REPLACE TOKEN

Token Type: Feitian

Token Serial Number: Enter Token Serial Number

Please enter token serial number and click Validate

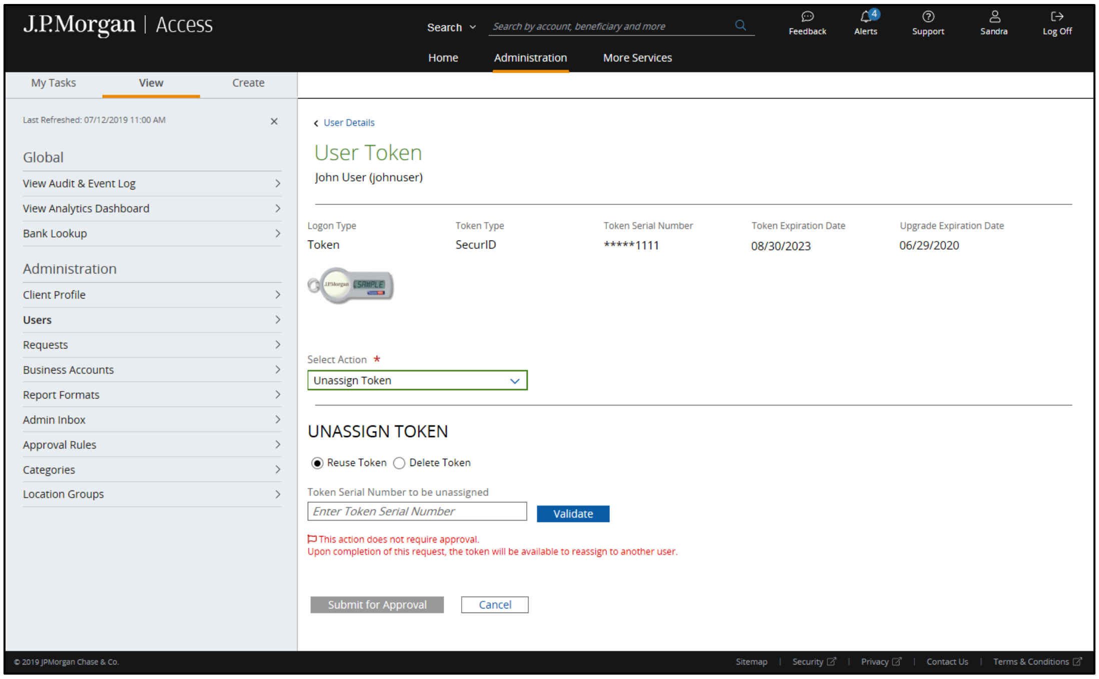
Unassigning Tokens

If a user leaves the company or no longer needs to use Access, their security token can be unassigned and then reassigned to another user.

To unassign a security token:

1. From the User Details page, click **Edit Credentials** and select **Add/Edit User Token**.
2. On the User Token page, select **Unassign Token** from the Select Action dropdown.
3. In the Unassign token panel select **Reuse Token** to unassign the token and make it available to reassign to another user or select **Delete Token**, to unassign the token and permanently delete the token from inventory so it cannot be reused.
4. If you have selected Reuse Token, enter the Token Serial Number that you would like to unassign and click **Validate**.
5. Click **Submit for Approval**.
6. Click **Continue**, and then click **Ok** to close the confirmation window.
7. If you have selected Reuse Token, you may now assign the token to another user using the standard token assignment process.

Note: You should use the Unassign token button only if a user no longer requires the security token. If you unassign a token in error, please contact the Help Desk immediately.



User Token

John User (johnuser)

Logon Type	Token Type	Token Serial Number	Token Expiration Date	Upgrade Expiration Date
Token	SecurID	*****1111	08/30/2023	06/29/2020

Select Action *: Unassign Token

UNASSIGN TOKEN

● Reuse Token ○ Delete Token

Token Serial Number to be unassigned: Enter Token Serial Number

This action does not require approval.
Upon completion of this request, the token will be available to reassign to another user.

Upgrading Token Type

Users are required to change from a RSA SecurID token to a Feitian token if they have new entitlements to China accounts or changed their location to China. Security Administrators are required to change from an RSA SecurID token to a Feitian token if the client he/she supports has users who have new or upgraded entitlements to China accounts.

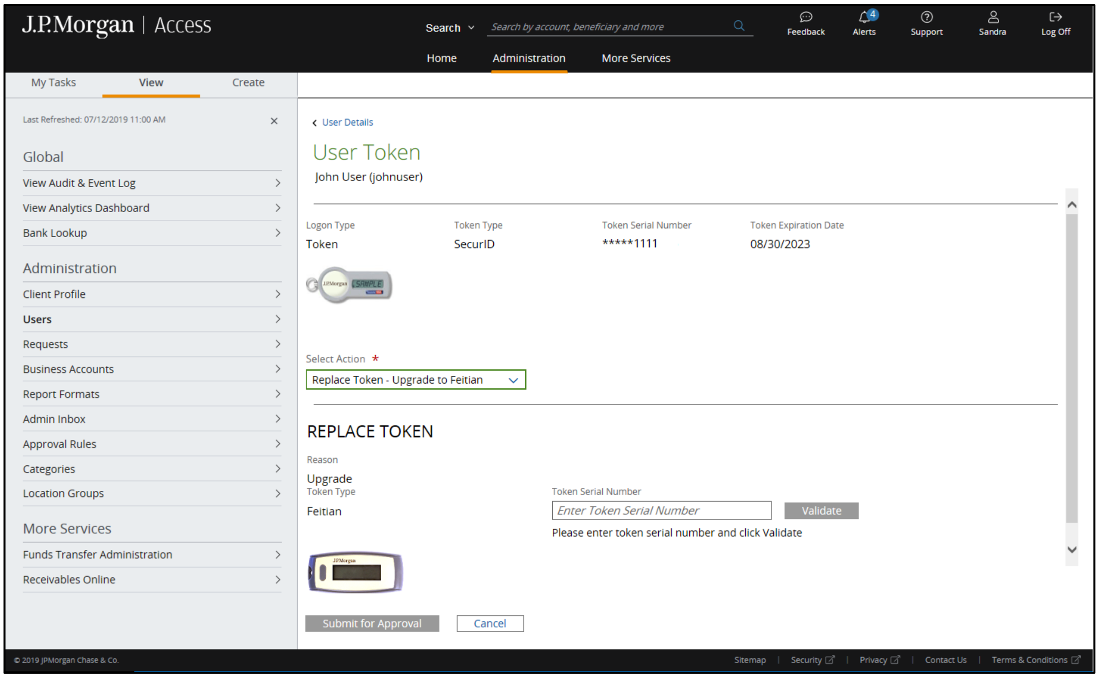
Note: Users and Security Administrators may use a Feitian token to access both China and non-China accounts.

When users qualify for Feitian tokens, the system will automatically detect the new token type requirement and will trigger the token type migration process. Emails will be generated to Security Administrators to assign Feitian tokens to the users.

To change a user's token assignment:

1. From the User Details page, click **Edit Credentials** and select **Add/Edit User Token**.
2. On the User Token page, select **Replace Token - Upgrade to Feitian** from the Select Action dropdown.
3. Obtain a new and unassigned Feitian token from your inventory.
4. Locate the serial number on the back of the token, enter it in the Token Serial Number field and click **Validate**.
5. After you receive a Validation Successful message, click **Submit for Approval**.
6. Click **Submit for Approval**, and then click **Ok** to close the confirmation window.
7. In a secure manner, provide the new token to the user.

8. Notify another Security Administrator to approve your request. The new token can be used only if it is approved.



User Token

John User (johnuser)

Logon Type	Token Type	Token Serial Number	Token Expiration Date
Token	SecurID	*****1111	08/30/2023

Select Action *

Replace Token - Upgrade to Feitian

REPLACE TOKEN

Reason

Upgrade

Token Type

Feitian

Token Serial Number

Enter Token Serial Number

Please enter token serial number and click Validate

Assigning and Revoking Temporary Token Codes

In the event a user's security token is damaged, stolen, lost or left at home, an SA can request temporary token codes. The SA enters the number of token codes that the user requires and a second SA must approve the action. Upon approval by the second SA, the user will receive an email message with a link that enables that user to retrieve the temporary token codes so they may perform their routine functions in Access even without a security token in their possession.

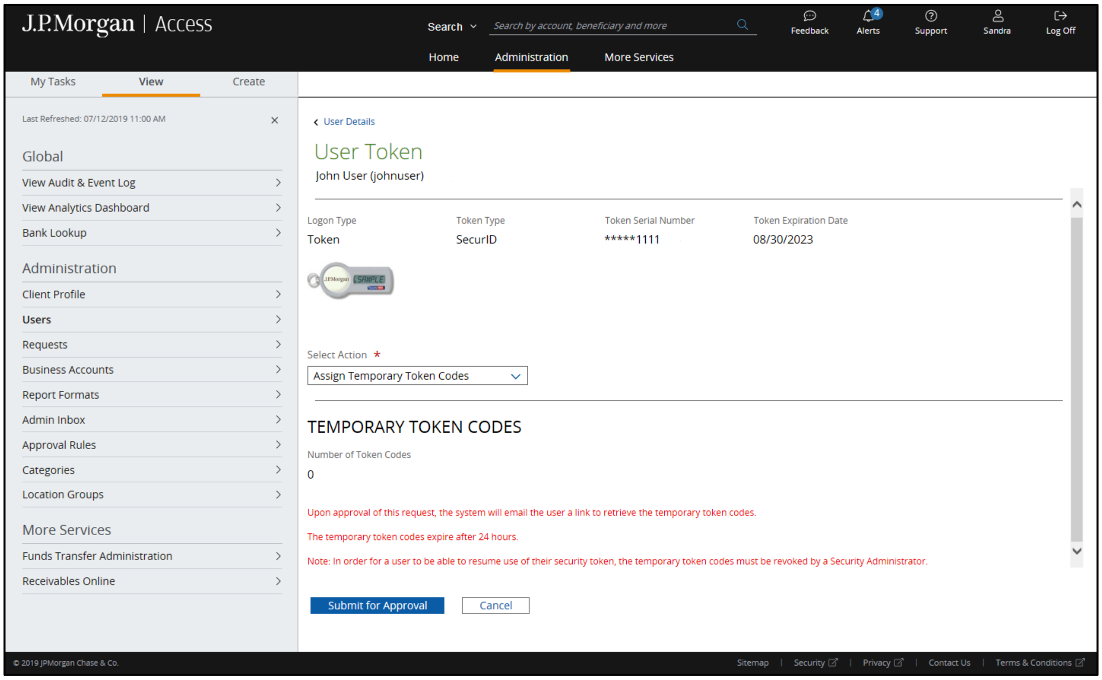
Note: These temporary codes can be viewed and used only by the intended user.

Temporary token codes:

- Can be assigned only to active users
- Can be used for one action only (e.g., one temporary token code to log on, another code to digitally sign); the user is requested to use a new temporary token code with each action
- Expire 24 hours after issuance
- Must be revoked by the Security Administrator so that the user can resume use of his/her physical security token

To assign temporary token codes:

1. From the User Details page, click **Edit Credentials** and select **Add/Edit User Token**.
2. On the User Token page, select **Assign Temporary Token Codes** from the Select Action dropdown.
3. In the Temporary Token Codes panel, click **Submit for Approval**.
4. Click **Submit for Approval**, and then click **Ok** to close the confirmation window.



User Token

John User (johnuser)

Logon Type	Token Type	Token Serial Number	Token Expiration Date
Token	SecurID	*****1111	08/30/2023

Select Action *

Assign Temporary Token Codes

TEMPORARY TOKEN CODES

Number of Token Codes

0

Upon approval of this request, the system will email the user a link to retrieve the temporary token codes.

The temporary token codes expire after 24 hours.

Note: In order for a user to be able to resume use of their security token, the temporary token codes must be revoked by a Security Administrator.

Submit for Approval | Cancel

To revoke temporary token codes:

1. From the User Details page, click **Edit Credentials** and select **Add/Edit User Token**.
2. On the User Token page, select **Revoke Temporary Token Codes** from the Select Action dropdown.
3. In the Temporary Token Codes panel, click **Submit for Approval.**
4. Click **Continue**, and then click **Ok** to close the confirmation window. The temporary token codes will be revoked, the user's assigned token will be enabled and the user can log on.

Disabling and Enabling Tokens

If a user wants to stop using a token, but retain the ability to use the same token at a later time, their security token can be disabled temporarily and then enabled when necessary.

To disable a token:

1. From the User Details page, click **Edit Credentials** and select **Disable Token**.
2. Click **Continue**, and then click **Ok** in to close the confirmation window. The security token is now disabled.

To enable a token:

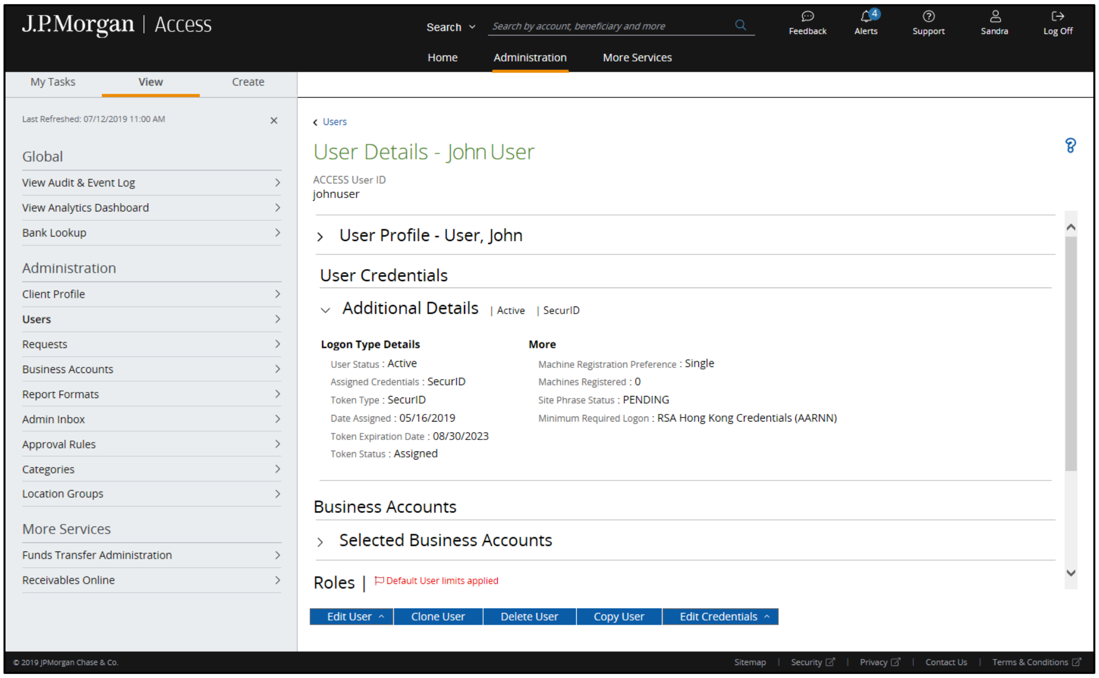
1. From the User Details page, click **Edit Credentials** and select **Enable Token**.
2. Click **Continue**, and then click **Ok** in to close the confirmation window. The security token is now enabled.

Viewing Token Details

You can view the details of a user's credentials from the Additional Details panel on the User Details screen, including Logon Type Details (e.g., User Status, Logon Type, Token Type, Minimum Required Logon, Token Expiration Date and Token Status), Logon Date Details and other details such as Locked Status, Machine Registration Preference and Site Phrase Status.

To view token details:

1. From the View tab on the Activity Bar, click **Users**.
2. Select a user from the Users list.
3. Click the down arrow to expand the Additional Details panel.



User Details - John User

ACCESS User ID
johnuser

User Profile - User, John

User Credentials

Additional Details | Active | SecurID

Logon Type Details

User Status : Active
Assigned Credentials : SecurID
Token Type : SecurID
Date Assigned : 05/16/2019
Token Expiration Date : 08/30/2023
Token Status : Assigned

More

Machine Registration Preference : Single
Machines Registered : 0
Site Phrase Status : PENDING
Minimum Required Logon : RSA Hong Kong Credentials (AARNN)

Business Accounts

Selected Business Accounts

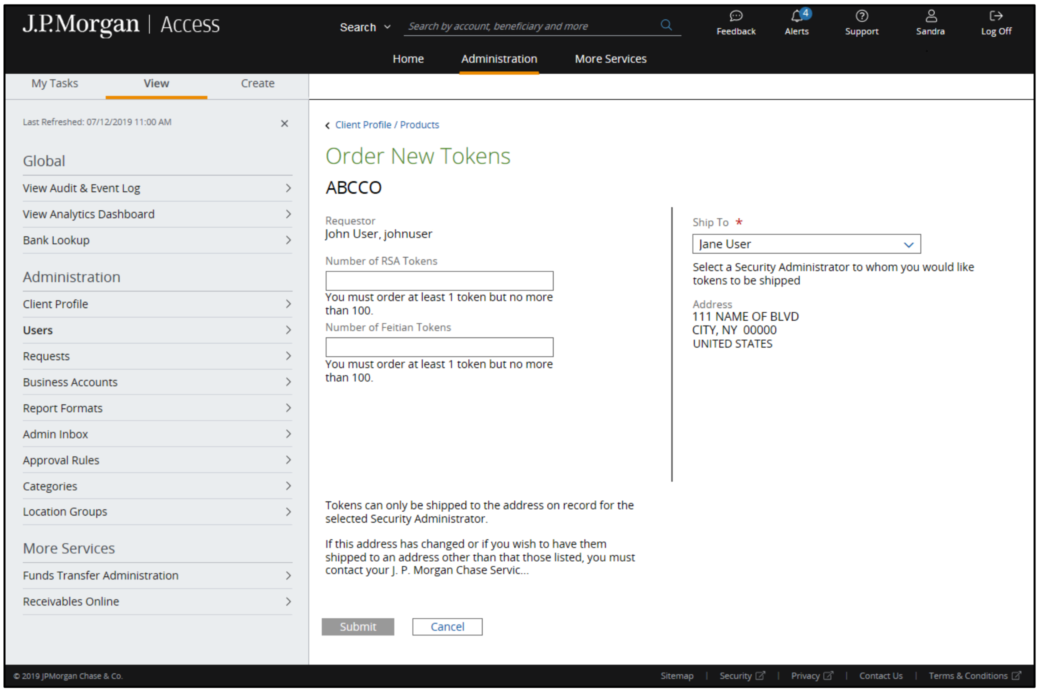
Roles | Default User limits applied

Ordering New Tokens

1. From the View tab on the Activity Bar, click **Client Profile**.
2. **Click Order New Tokens**.
3. Enter the number of tokens of each type to be ordered (at least one, but no more than 100), and select the appropriate Security Administrator to ship them to.

   Notes:

   - Tokens can only be shipped to the address on record for the selected Security Administrator. If this address has changed or if you wish to have them shipped to an address other than those listed, you must contact your J.P. Morgan Chase Service Representative.
   - Token requests received before 3 p.m. ET will be sent through an express shipping carrier for next business day delivery in the continental United States.
   - Requests received after 3 p.m. ET will be processed the next day.
   - Requests with international addresses will also be sent through an express shipping carrier, but may require additional business days for delivery due to custom processing, local conditions or other restrictions. Requests with international addresses will also be sent through an express shipping carrier, but may require additional business days for delivery due to custom processing, local conditions or other restrictions.
4. Click **Submit**, and then click **Continue**. The new Token Request ID is created and will be displayed in the New Token Requests panel on the Client Profile page, where you can track the request status.



Order New Tokens

ABCCO

Requestor
John User, johnuser

Number of RSA Tokens

You must order at least 1 token but no more than 100.

Number of Feitian Tokens

You must order at least 1 token but no more than 100.

Ship To *
Jane User

Select a Security Administrator to whom you would like tokens to be shipped

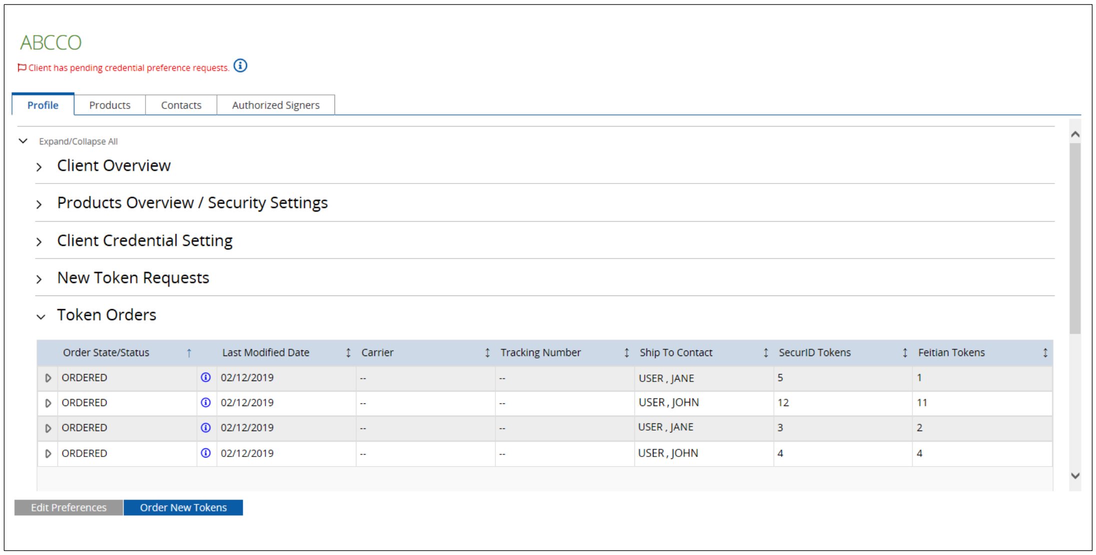
Address
111 NAME OF BLVD
CITY, NY 00000
UNITED STATES

Tokens can only be shipped to the address on record for the selected Security Administrator.

If this address has changed or if you wish to have them shipped to an address other than that those listed, you must contact your J. P. Morgan Chase Servic...

View Token Order Status

1. From the View tab on the Activity Bar, click **Client Profile**.
2. Click the down arrow to expand the Token Orders panel.
3. From the Token Orders panel, you can view the order status as well as shipping information such as carrier, tracking number and ship-to contact. This enables the SA to track the status of the token order without having to contact their service team.



ABCCO

Client has pending credential preference requests.

Order State/Status	Last Modified Date	Carrier	Tracking Number	Ship To Contact	SecurID Tokens	Feitian Tokens
ORDERED	02/12/2019	--	--	USER , JANE	5	1
ORDERED	02/12/2019	--	--	USER , JOHN	12	11
ORDERED	02/12/2019	--	--	USER , JANE	3	2
ORDERED	02/12/2019	--	--	USER , JOHN	4	4

Alternate Logon Users (ALU)

Certain countries have special banking regulations that require specific treatment of passwords for online banking users with access to reporting and initiation applications.

To comply with these regulatory requirements, all Access users with access to accounts based in these countries and established on the Access reporting and/or initiation services are subject to this requirement.

For example, most countries in Asia require ALU. The following countries are impacted:

- China
- Hong Kong
- Korea
- Singapore
- Taiwan
- Vietnam
- Mexico
- Argentina

These users are referred to as Alternate Logon Users (ALU). Their passwords are protected by a special type of security. They will:

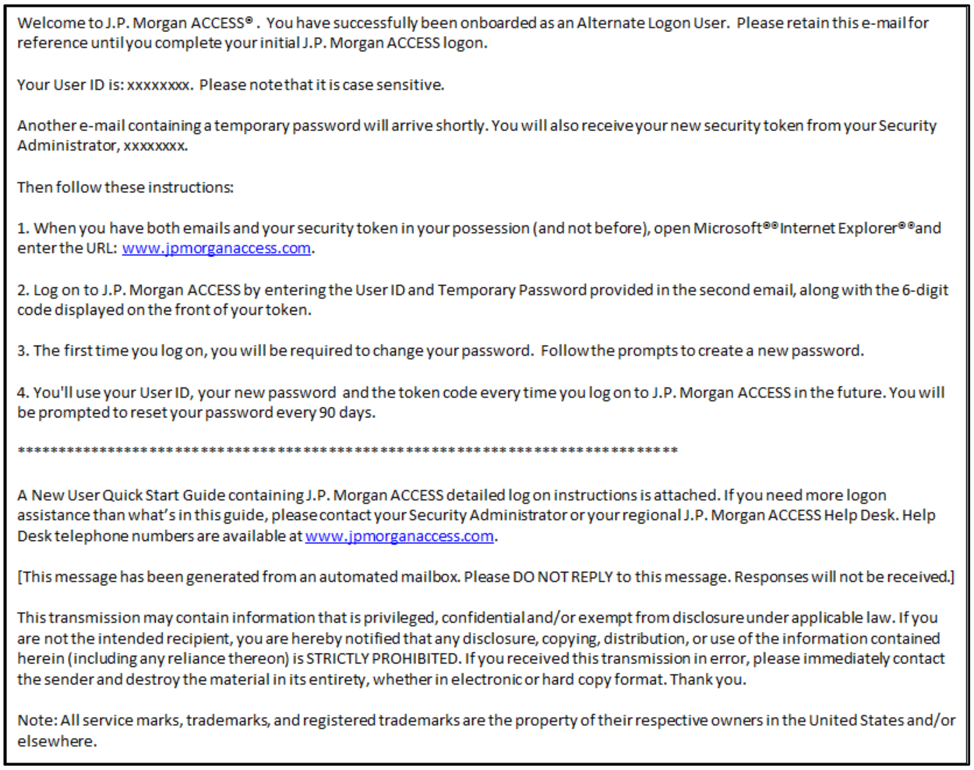
- Use a security token to logon to Access.
- Transition to ALU status.
- Change their password every 90 days.

Adding a New Account

The Security Administrator may entitle new users or existing users to J.P. Morgan accounts via Administration. If the accounts are based in any of the countries listed above, the user will auto-convert to an ALU status upon successful completion of the account add to the user's entitlements.

The user will receive two emails, one with the User ID and the other with the temporary password required for the initial logon. Once the initial logon is complete, the user will be prompted to change the password to a permanent one.

Note: End users that have been assigned a software token will also receive two emails: one with the User ID along with instructions for registering a hardware or software token on their mobile device, and the other with the temporary password required for the initial logon. Once the initial logon is complete, the user will be prompted to change the password to a permanent one.



Welcome to J.P. Morgan ACCESS® . You have successfully been onboarded as an Alternate Logon User. Please retain this e-mail for reference until you complete your initial J.P. Morgan ACCESS logon.

Your User ID is: xxxxxxxx. Please note that it is case sensitive.

Another e-mail containing a temporary password will arrive shortly. You will also receive your new security token from your Security Administrator, xxxxxxxx.

Then follow these instructions:

1. When you have both emails and your security token in your possession (and not before), open Microsoft®® Internet Explorer®® and enter the URL: www.jpmorganaccess.com.

2. Log on to J.P. Morgan ACCESS by entering the User ID and Temporary Password provided in the second email, along with the 6-digit code displayed on the front of your token.

3. The first time you log on, you will be required to change your password. Follow the prompts to create a new password.

4. You'll use your User ID, your new password and the token code every time you log on to J.P. Morgan ACCESS in the future. You will be prompted to reset your password every 90 days.

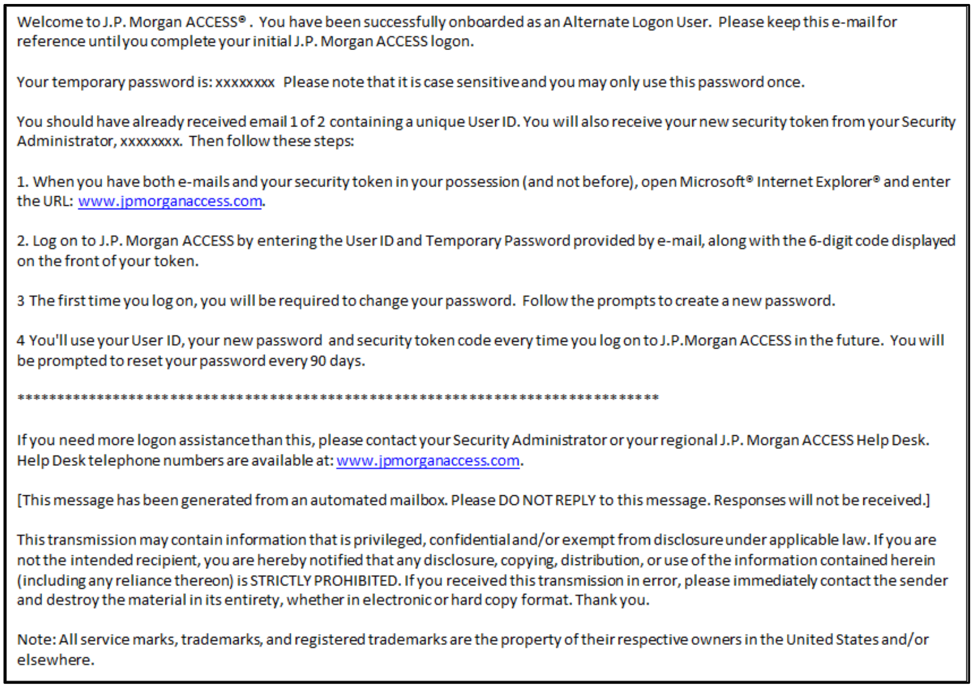
****

A New User Quick Start Guide containing J.P. Morgan ACCESS detailed log on instructions is attached. If you need more logon assistance than what's in this guide, please contact your Security Administrator or your regional J.P. Morgan ACCESS Help Desk. Help Desk telephone numbers are available at www.jpmorganaccess.com.

[This message has been generated from an automated mailbox. Please DO NOT REPLY to this message. Responses will not be received.]

This transmission may contain information that is privileged, confidential and/or exempt from disclosure under applicable law. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or use of the information contained herein (including any reliance thereon) is STRICTLY PROHIBITED. If you received this transmission in error, please immediately contact the sender and destroy the material in its entirety, whether in electronic or hard copy format. Thank you.

Note: All service marks, trademarks, and registered trademarks are the property of their respective owners in the United States and/or elsewhere.



Welcome to J.P. Morgan ACCESS® . You have been successfully onboarded as an Alternate Logon User. Please keep this e-mail for reference until you complete your initial J.P. Morgan ACCESS logon.

Your temporary password is: xxxxxxxx Please note that it is case sensitive and you may only use this password once.

You should have already received email 1 of 2 containing a unique User ID. You will also receive your new security token from your Security Administrator, xxxxxxxx. Then follow these steps:

1. When you have both e-mails and your security token in your possession (and not before), open Microsoft® Internet Explorer® and enter the URL: www.jpmorganaccess.com.

2. Log on to J.P. Morgan ACCESS by entering the User ID and Temporary Password provided by e-mail, along with the 6-digit code displayed on the front of your token.

3 The first time you log on, you will be required to change your password. Follow the prompts to create a new password.

4 You'll use your User ID, your new password and security token code every time you log on to J.P.Morgan ACCESS in the future. You will be prompted to reset your password every 90 days.

****

If you need more logon assistance than this, please contact your Security Administrator or your regional J.P. Morgan ACCESS Help Desk. Help Desk telephone numbers are available at: www.jpmorganaccess.com.

[This message has been generated from an automated mailbox. Please DO NOT REPLY to this message. Responses will not be received.]

This transmission may contain information that is privileged, confidential and/or exempt from disclosure under applicable law. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or use of the information contained herein (including any reliance thereon) is STRICTLY PROHIBITED. If you received this transmission in error, please immediately contact the sender and destroy the material in its entirety, whether in electronic or hard copy format. Thank you.

Note: All service marks, trademarks, and registered trademarks are the property of their respective owners in the United States and/or elsewhere.

IP Filtering and Location Groups

IP (Internet Protocol) filtering is an Internet security method that provides IP-address-based control of user access to J.P. Morgan Access. Access Administration offers the enhanced security benefit of IP filtering, allowing SAs to restrict logon access, at the user level, to an individual IP address or a group of IP addresses based on the user's physical work location. This prevents user from logging on remotely from other computers.

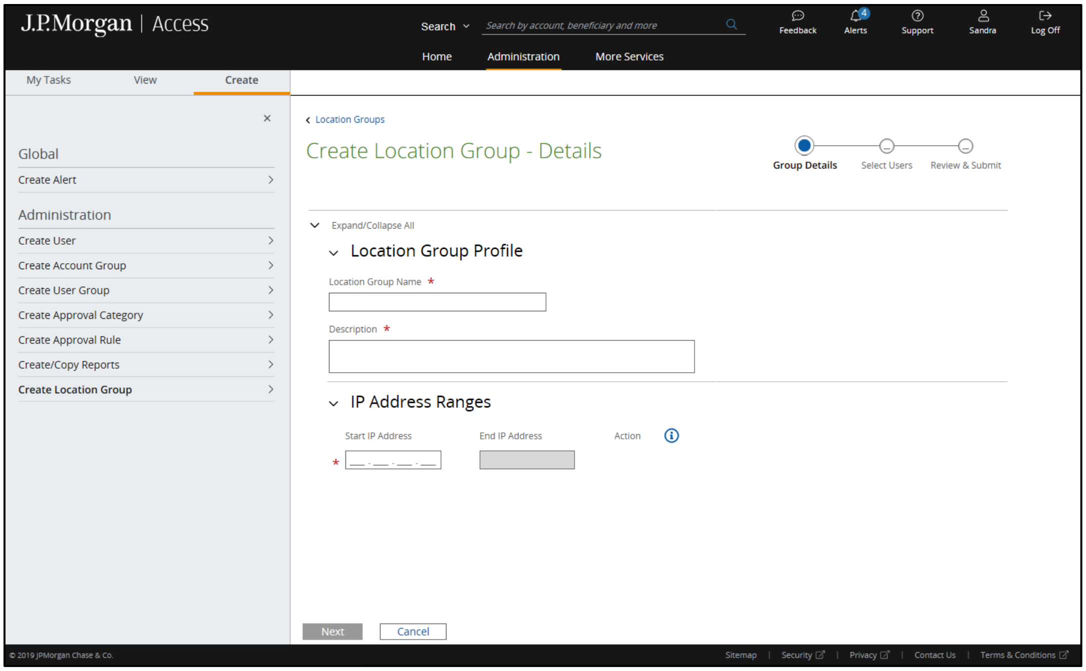
Creating Location Groups

By creating IP address Location Groups, you are able to create a custom-named grouping of IP addresses that you then assign to users. Users will be restricted to this group of IP addresses (or a single IP address) when they log on to Access.

To create a location group:

1. From Create tab on the Activity Bar, click **Create Location Group**.
2. Enter a Location Group Name and Description.
3. Enter the IP address(es), which can be defined in multiple ways:
   - Explicit IP Address (e.g., Start 100.112.92.68 and End 100.112.92.68)
   - IP Address Range (e.g., Start 100.112.92.72 and End 100.112.92.110)
   - Single Wildcard IP Address (e.g., Start 100.112.92.* and the End will default to 100.112.92.255)
   - Double Wildcard IP Address (e.g., Start 100.112.*.* and the End will default to 100.112.255.255)

   Note: You may use an asterisk (*) as a wildcard in the third and fourth octets or in the fourth octet only.



4. Click **Next** and select the users from the list of Available Users.
5. Click the >> right arrow button to move the users you selected to the Selected Users list.
6. Click **Next** to display the Create Location Group Review screen, and then click **Submit for Approval.**
7. Click **Submit for Approval**, and then click **Ok** to close the confirmation window.
   Note: You can remove a particular IP address range using the Remove link in the Action column.

Deleting Location Groups

To delete a location group:

1. From View tab on the Activity Bar, click **Location Groups**.
2. Select the location group(s) you want to delete and click **Delete Group**.
3. Click **Submit for Approval**, and then click **Ok** to close the confirmation window.

Note: You can also delete a location group from the Location Group Details screen.

Editing Location Groups

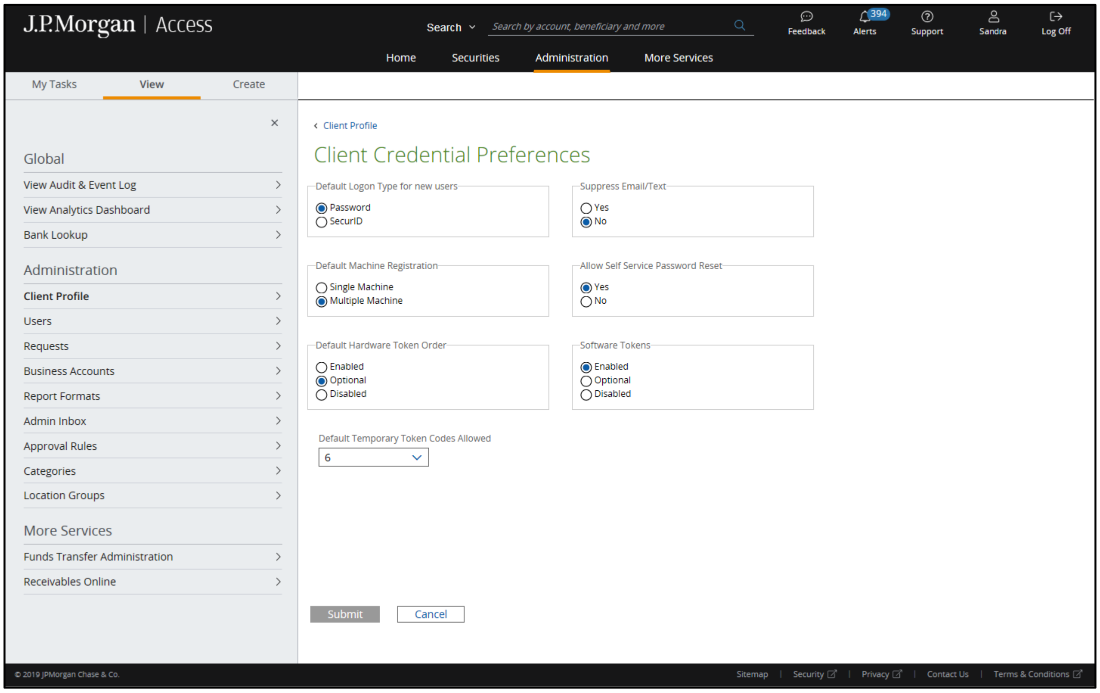
To edit a location group:

1. From View tab on the Activity Bar, click **Location Groups**.
2. Click the location group you want to edit to view the Location Group Details page.
3. Click **Edit Group** and select one of the following options:
   - Click **Edit Details** to edit the group name, description, IP address ranges, and/or assigned users
   - Click **Edit Assigned Users** to edit assigned users without modifying Location Group Profile information or IP address ranges
   - Click **Set as Default Group** to change the default location group
     Note: If you are editing the default location group, you can click **Remove As the Default Group** to remove the location group as the default
4. Once you have edited the location group as desired, click **Submit for Approval**, or **Continue**, and then click **Ok** to close the confirmation window.

Editing Client Credential Preferences

You can change the credential preferences of a client from the Client Profile page.

1. From the View tab on the Activity Bar, click **Client Profile**.
2. Click **Edit Preferences** to open the Client Credential Preferences screen.
3. Select options for any of the following preferences:
   - **Default Logon Type for new users** is used when you create a new user to populate the user's Logon Type.
   - **Suppress Email/Text** is used to determine if SAs or end users would like to receive emails/text messages from credential actions.
   - **Default Machine Registration** is used when you create a new user to populate the user's machine registration preference.
   - **Allow Self Service Password Reset** is used to determine if users are allowed to use Forgot Your Password to reset their own password at logon.
   - **Default Hardware Token Order** offers the following options:
     - **Enabled -** Automatically submits the request for auto-replenishment of tokens when you create a new Express Setup user.
     - **Optional -** Allows you to make the decision on token auto-replenishment when you create a new Express Setup user.
     - **Disabled -** Disables auto-replenishment and requires you to order tokens through the Order New Token button for both Express and Custom Setup users.
   - **Software Tokens** allows you to enable or disable assignment of an RSA SecurID® software token when creating a new user. The Optional selection enables the user to optionally select a software token in Express Setup.
   - **Default Temporary Token Codes Allowed** is used to determine the number of codes that is selected by default when assigning temporary token codes.
4. After you are done changing credential preferences, click **Submit for Approval**.
5. Click **Continue**, and then click **Ok** to close the confirmation window.



Client Credential Preferences

Default Logon Type for new users
● Password
○ SecurID

Suppress Email/Text
○ Yes
● No

Default Machine Registration
○ Single Machine
● Multiple Machine

Allow Self Service Password Reset
● Yes
○ No

Default Hardware Token Order
○ Enabled
● Optional
○ Disabled

Software Tokens
● Enabled
○ Optional
○ Disabled

Default Temporary Token Codes Allowed
6