J.P.Morgan

Access & Security Manager Go-To Guide

Last updated April 2026

Overview

Summary

Access & Security Manager allows users to easily manage company entitlements. The feature can be accessed through the “Access & Security” tab and is available to all System administrators. Within Access & Security Manager, Primary admins can:

- Add additional users
- Manage user info, company-level and account-level rights as well as daily transaction limits for users
- Add up to three proxy admin(s) to assist with account management tasks
- View recent user and transaction activity
- Initiate and edit IP Security
- Activate Dual Control for administrative actions and transactions for added security

Proxy admins have access to Access & Security Manager but do not have the full rights of a Primary admin. Please refer to the Proxy Administrator Go-To Guide for more information.

New Connect users will need to review and activate applicable Pay & Transfer, Collect & Deposit and Security features before building user profiles.

Table of Contents

Adding Authorized Users

Note: Before adding additional users, ensure there are email addresses and phone numbers for individuals

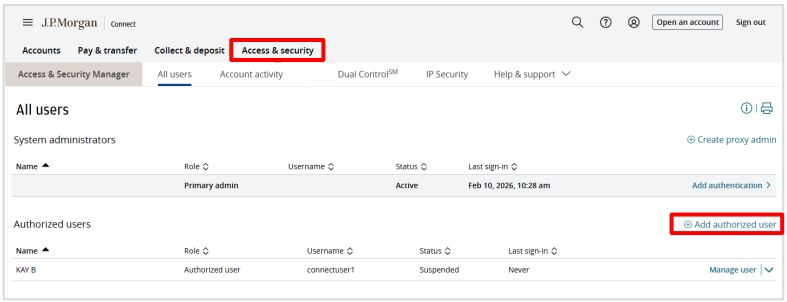
1. Select **Access & Security Manager** from the **Access & Security** menu
    a. On the **All users** page, select **Add authorized user**
2. Enter details about authorized user
    a. Enter First Name, Last Name, Primary email, and Primary phone
    b. Set a Username

    Note: Usernames must be at least eight characters and contain at least one letter, one number and no special characters

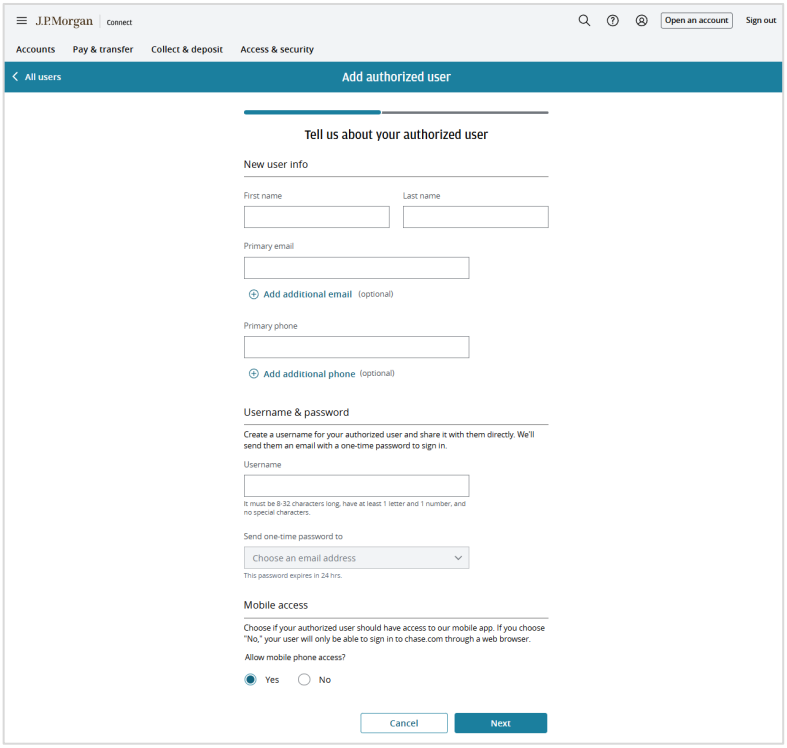
    a. Determine if Mobile access is needed

    Note: The system defaults to allow Mobile Access
3. The new user will receive an email detailing how to sign in for the first time, including authenticator instructions and a temporary password

1



2



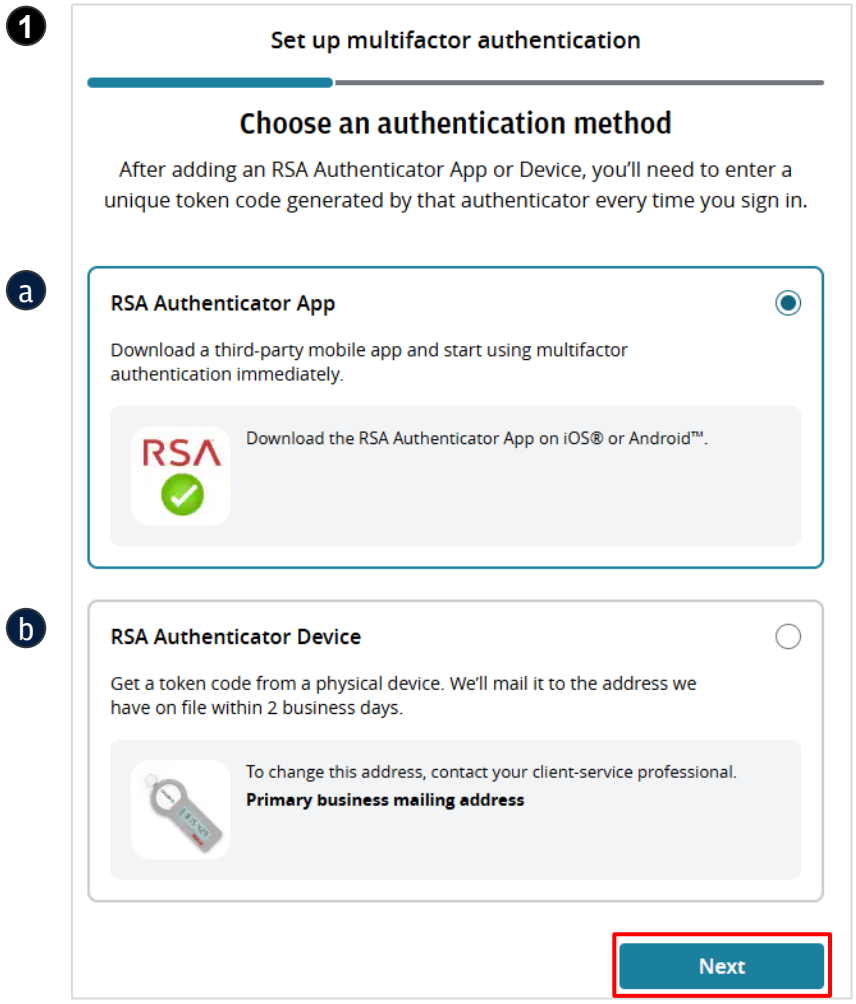
Choosing a Secure Authenticator

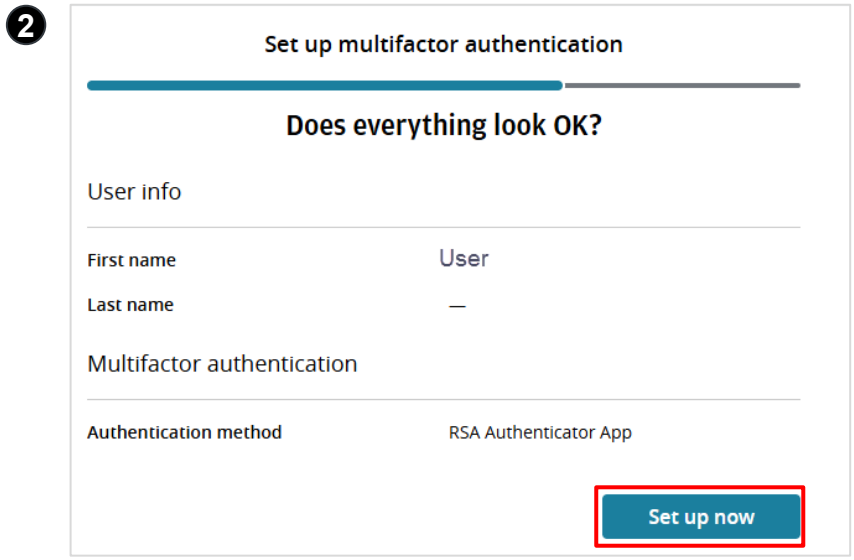
1. Enhance online account security by choosing one of the following authenticator options:

   a. **RSA Authenticator App (recommended):** Download the app, available on iOS or Android. Enjoy the convenience of accessing authenticator directly from smartphone

   b. **RSA Authenticator Device:** Receive a physical device, which will be mailed to the address provided

2. Review the user details and authenticator request, then confirm by selecting **Set up now**



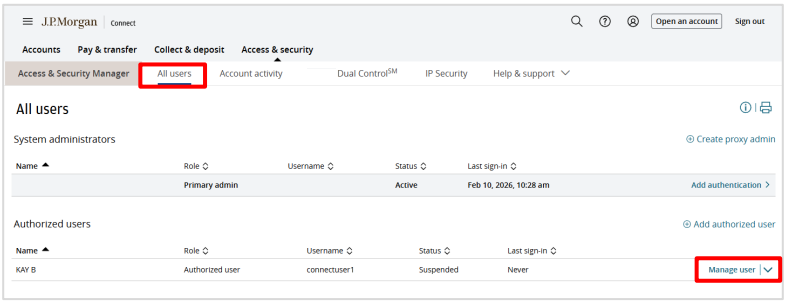


Managing Entitlements for Authorized Users

System administrators can assign user rights at the account level for enabled services. Every company and account in the profile will be listed, and access can be assigned for each one. If there are existing users, their settings can be copied by selecting **Copy access level from another user**. Time can also be saved by granting the user **Full access** or by selecting **Choose all** for an entire company or account

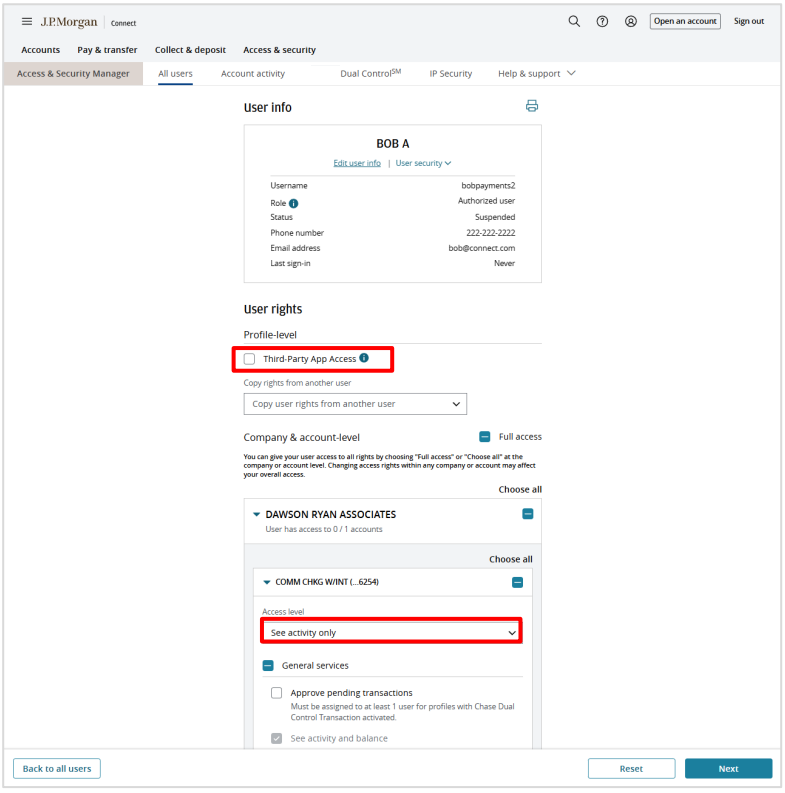
1. Select **Manage user** on the **All users** page
2. Select the **Third-party app access** checkbox for user access to connect and upload Connect account information into authorized third-party applications
3. For each account, select the **Access level**:
    - **See activity only:** User can see balances and account history, but can't initiate or approve transactions
    - **Transact only:** User can submit transactions for approval, but can't see balances or account history
    - **See activity and transact:** User can both see balances and account history as well as submit transactions for approval

1



2

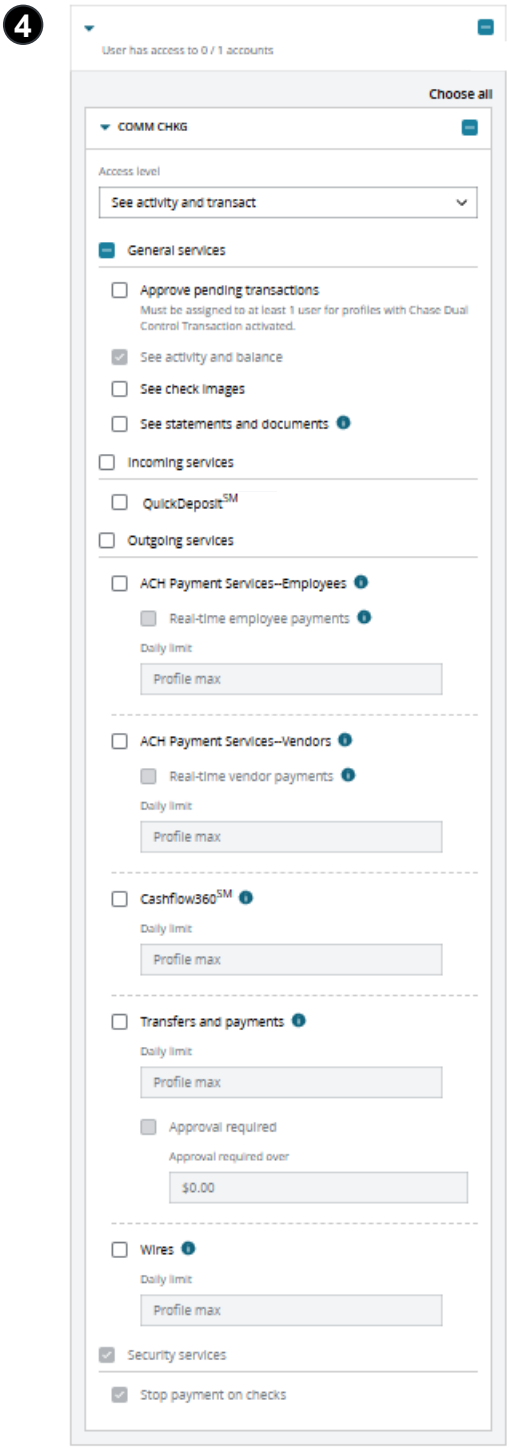
3



Managing Entitlements for Authorized Users (Continued)

4. Next, assign user rights, including daily limits and whether their transactions need approval. Options will vary based on services activated, account types and Access level

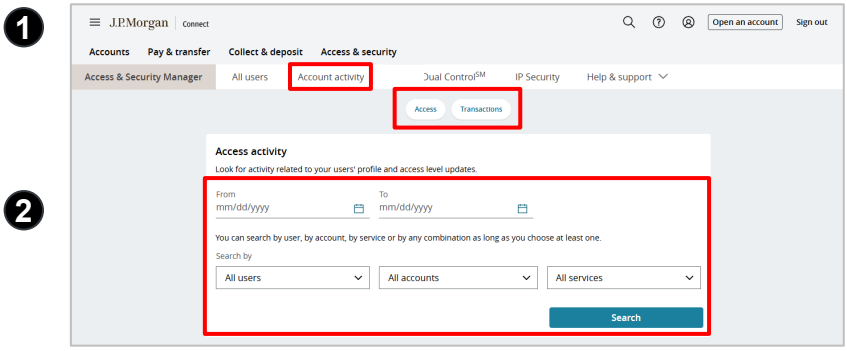
   - **General services:** Includes transaction approval, see activity and balances, see check images, see statements and documents
   - **Incoming services:** Includes entitlements for ACH Collections and QuickDeposit℠
   - **Outgoing services:** Includes entitlements for ACH Payments (Employee & Vendor), Wires, Account Transfers, etc.
   - **Security services:** Includes issuing a stop payment on checks, ACH Debit Block and Fraud Protection Services



View Account Activity

Primary admins can view up to one year of user activity and 90 days of transaction reports from within Access & Security Manager

1. Select **Account Activity** then select **Activity type**
    a. **Transactions:** Results will include who made what transactions against the accounts
    b. **Access:** Results will include history of changes to user rights and access to accounts
2. Select the date range and **Search by** parameters
    a. Select **Search**

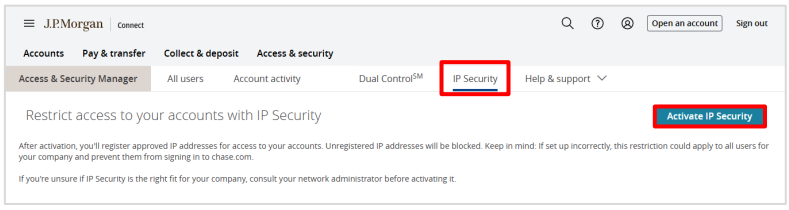


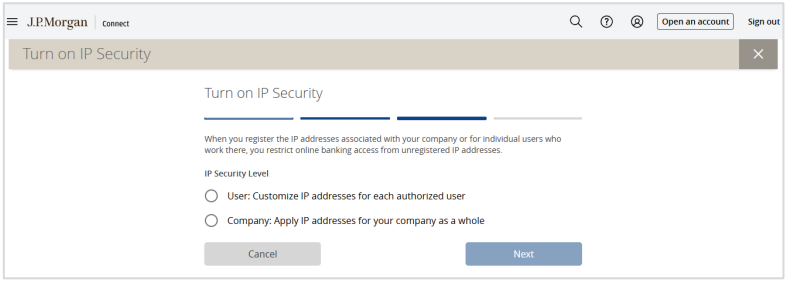
IP Security

Ensure Primary Admin activates IP Security, utilizing the RSA Authenticator and choosing either a company or user level. Non-authenticator clients need to call in for an activation code from service

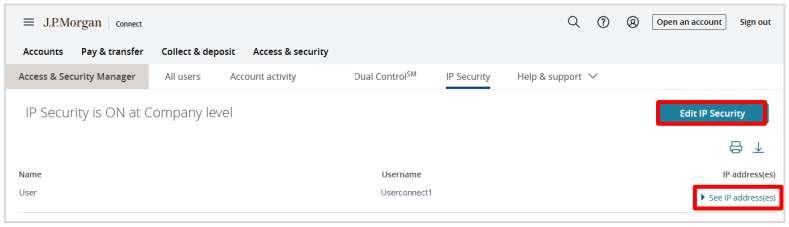
1. Select **IP Security** in the Access & Security Manager tab
    a. To Turn on IP Security, select **Activate IP Security** and the security level
2. Select **See IP address(es)** to see all addresses. For edits, select **Edit IP Security**
    a. Can switch between user and company level IP Security
    b. Option to turn off service
    c. Change/add addresses

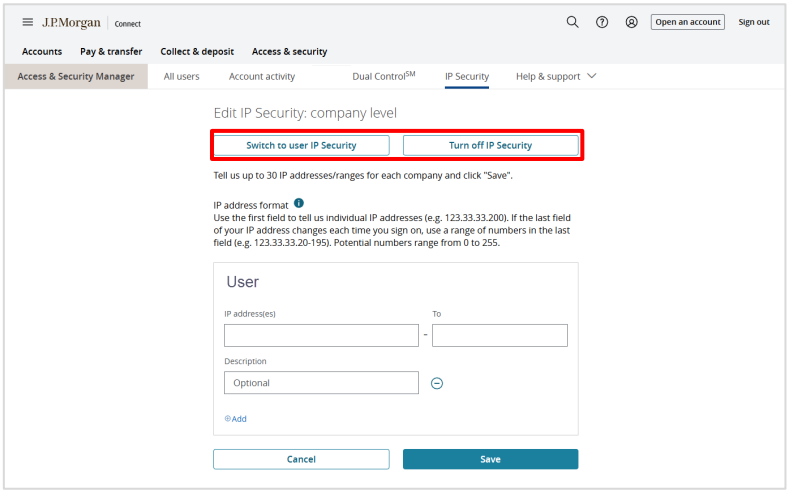
1





2



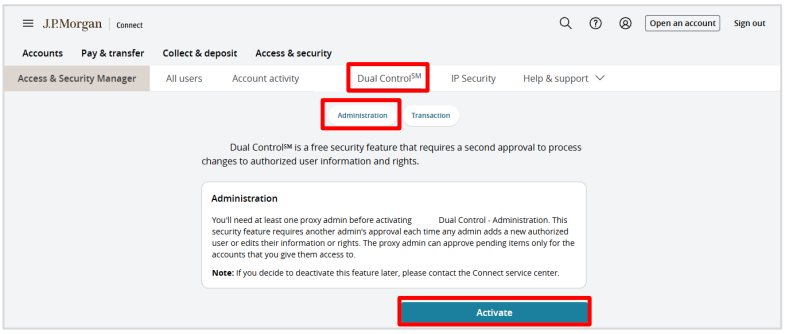


Activating Dual Control – Administration – Activation

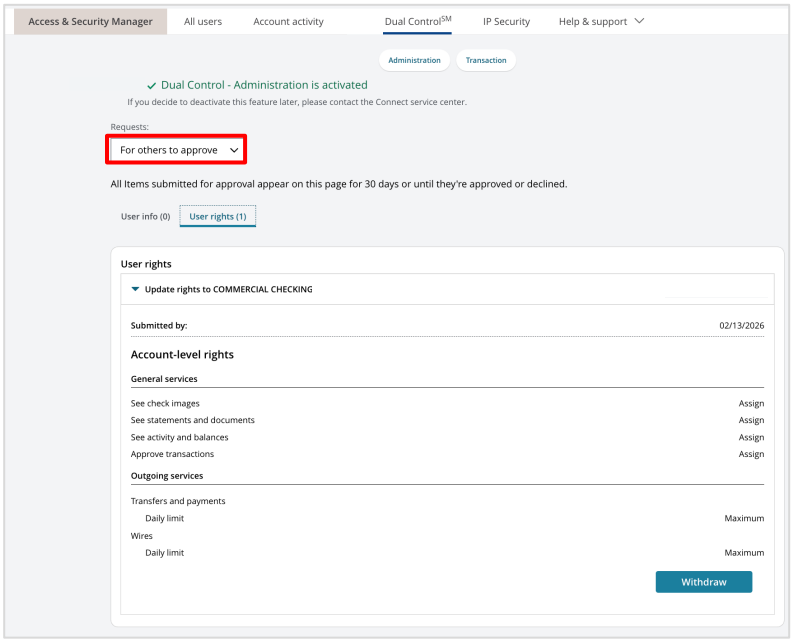
When Dual Control-Administration is activated, all administrative actions (e.g., updating user info, account-level rights, company-level rights) require approval by another System Administrator. Only primary admins can activate this feature, but proxy admins can review administrative tasks pending approval if they have account rights. Before activating, ensure there is at least one proxy admin created

1. Select **Dual Control** from Access & Security Manager
    a. Select **Administration** and read the information presented on the screen
    b. Select **Activate**
2. Once activated, actions that require approval can be found within Access & Security Manager on the **Dual Control**-Administration page. View actions that require approval or those that are assigned to others using the **Requests** dropdown. Transactions must be approved within three days

1



2

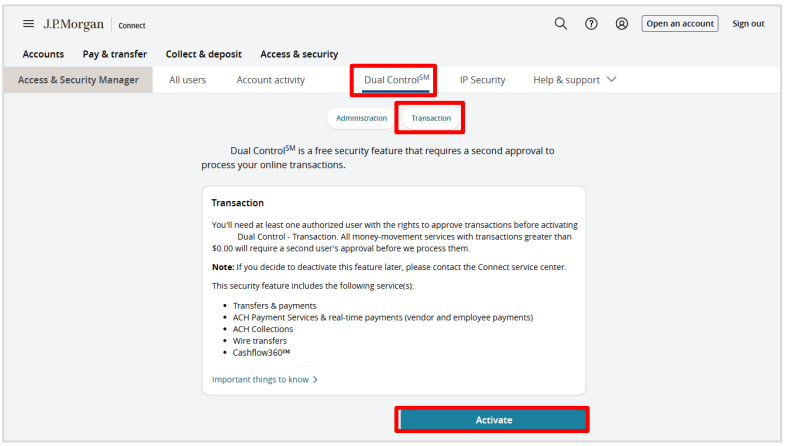


Activating Dual Control – Transaction

When Dual Control-Transaction is activated, all transactions will automatically require approval by another user except for transfers between J.P. Morgan accounts, loan advances and loan payments.
Only Primary admins can activate this feature. Before activating, ensure that at least one authorized user has rights to approve transactions by choosing **Approve pending transactions** within an account for that user

1. Select **Dual Control** from Access & Security Manager
    a. Select **Transaction** and read the information presented on the screen
    b. Select **Activate**
2. Once activated, pending transactions will appear in **Pending approvals** through **Pay & transfer** until another user approves them

1



2