Enhanced Authentication User Guide

Welcome to Nuvision Credit Union's Enhanced Authentication User Guide

At Nuvision Credit Union, safeguarding our members' information is our top priority. This guide provides simple, step-by-step instructions to help manage and protect your digital banking accounts. It ensures a safe and smooth experience while keeping your information secure. Enhanced Authentication provides an additional level of security to safeguard against phishing scams, credential theft, and online account takeovers (OATs). It simplifies the login process by providing easy options like biometric authentication, which makes it quicker and more convenient to verify your identity. Members are encouraged to follow these instructions for self-help. Thank you for choosing Nuvision Credit Union as your trusted financial partner.

First Time Enrollment

Follow these steps to enroll in Enhanced Authentication:

1. At initial login, use the Secure Access Code (SAC) to authenticate your login
2. Select the method to receive your Secure Access Code (SAC)
3. Enter the Secure Access Code (SAC)
4. A notification will be presented for "Experience heightened security"
    a. Select "Yes, I want to proceed", to navigate to the Advanced Authentication page, where you will be guided on how to add a trusted device
    b. If "Maybe Later" is selected, the option for "Experience heightened security" will be ignored, and it will reappear the next time you log in.
5. Once a trusted device is added you will be set up for enhanced authentication

Advanced Authentication

Manage trusted devices, browsers, and passkeys for secure authentication:

To Register a Trusted Mobile App

1. Once a mobile device is considered "trusted" you will only be prompted when certain transactions reach an amount determined to be high-risk
2. Visit the Google Play or Apple Store from your new mobile device
3. Download the Nuvision CU mobile app
4. Log in to the Nuvision CU mobile app
5. A push notification will be sent to the primary trusted device to add the new device
6. Select "Yes" to confirm the login from the new device
7. The device has been successfully linked; it will appear in the "Mobile Banking App" tab

To Register a Trusted Browser

A trusted browser is a specific browser authenticated and linked within the digital banking profile.

1. Log in to digital banking from the new browser
2. A push notification will be sent to the primary trusted device to authenticate the request
3. A prompt will display asking if they want to trust this new browser
4. Select "Trust this browser" to approve the trusted browser
5. The browser has been successfully linked; it will appear in the "Trusted Browsers" tab

To Register a Trusted Pass Key

A passkey is a private key assigned to a physical device used to allow unique authentication not accessible outside the device it is stored on.

1. Log in to digital banking
2. Choose "Settings" from the navigation menu
3. Select "Advanced Authentication" from the dropdown menu
4. Select "Create Passkey On This Device" or "Mobile phone via QR Code" button
5. Enter the device friendly name, e.g. "Jane's iPhone 13".
6. Selecting "Create Passkey On This Device"
    a. You will be prompted to store the passkey using either biometric authentication or by creating a unique password for the passkey.
7. Selecting "Mobile phone via QR Code"
    a. Scan the QR code using your mobile device and the passkey will be established on the mobile device
8. The Passkey has been successfully linked; it will appear in the "Passkeys" tab

Biometrics Authentication

Biometric authentication utilizes the distinct biological features of individuals to confirm their identity. It compares physical attributes with saved authentication data for verification.

1. Log in to digital banking
2. Choose "Settings" from the navigation menu
3. Select "Advanced Authentication" from the dropdown menu
4. Click on the toggle option in the "Biometrics" section
5. Select "Accept" to activate biometrics on your device
6. A message will be displayed confirming that biometrics have been enabled for your device
    a. For future logins or transaction approvals, you'll be prompted to authenticate using your biometrics instead of entering a password.

b. If biometric data changes (e.g., new fingerprint added), you'll receive a notification and may need to re-enable biometrics

Removing Trusted Devices

Changing the status of a trusted device is a sensitive security matter. Once a device is marked as trusted, it can be used to confirm any transaction. To remove a trusted device, you must first verify your identity using another trusted device. You can remove any trusted device from a browser, but you can only add passkeys as trusted devices through a browser.

1. Log in to digital banking from your primary trusted device on the mobile app
2. Choose "Settings" from the navigation menu
3. Select "Advanced Authentication" from the dropdown menu
1. Under "Trusted Devices", find the device you want to remove
2. Select the "Remove Device" option next to the device name
3. A push notification will be sent to the primary trusted device
4. Select "Yes" to confirm your request
5. Once confirmed, the device will no longer be able to authenticate login or transactions

Removing a Primary Trusted Device

Multiple trusted mobile devices can be assigned. However, one primary device will be assigned to authenticate the request. When removing your primary device, a warning is displayed as follows. After confirming, the current device will be made the new primary device.

1. Log in to digital banking from your primary trusted device on the mobile app
2. Choose "Settings" from the navigation menu
3. Select "Advanced Authentication" from the dropdown menu
4. Under "Trusted Devices", find the device marked as "Primary"
5. Select the "Remove Device" option next to the primary device
6. A push notification will be sent to the secondary trusted device
7. Select "Yes" to remove the device from the Advanced Authentication page
8. Once confirmed, the primary device is removed, and another trusted device will be promoted as primary

NOTE: If no other device exists, you'll need to set up a new primary device before continuing.