



NCUA
National Credit Union Administration

NCUA Connect & Admin Portal User Guide

September 2024



NCUA

National Credit Union Administration

[This page intentionally left blank]





Version Updates

Version #	Date	Changes Made
2.0	7/27/2020	July 2020 release
2.1	8/28/2020	Chapter 1: NCUA Connect <ul style="list-style-type: none">• Clarified assistance available if a user cannot login Chapter 2: Admin Portal <ul style="list-style-type: none">• Clarified how administrators can obtain access to MERIT (and related applications) and username functionality• Added User Status information
2.2	6/20/21	Updated all chapters and Appendix A to clarify functionality and incorporate changes to the Admin Portal.
2.3	11/21	Minor functional clarifications; Updated system images
2.4	4/2023	Add CUOnline and CCUOnline
2.5	4/2024	Add SSA Access to Partner Gateway, Secure File Transfer Portal, and SSA Email Lists
2.6	07/2024	Add SSA Access to the LAMP
2.7	09/2024	Updates to support User Report access



Table of Contents

Chapter 1: NCUA Connect	1
Overview.....	1
Obtaining Access to NCUA Connect	1
NCUA Users – Accessing NCUA Connect	2
External Users – Accessing NCUA Connect.....	2
Initial Multifactor Authentication (MFA) Set Up.....	3
Signing into NCUA Connect	8
Using Multifactor Authentication (MFA).....	10
NCUA Connect Assistance and Resetting Passwords	13
Adding Apps to NCUA Connect	13
Chapter 2: Admin Portal.....	15
Overview.....	15
Introduction to Admin Portal	15
Accessing the Admin Portal.....	16
NCUA Connect User Roles	17
Opening the Admin Portal Application	23
Adding Users	23
Updating and Removing Users	25
Access User Reports	27
Appendices.....	30
Appendix A – Admin Portal Email Notifications.....	30

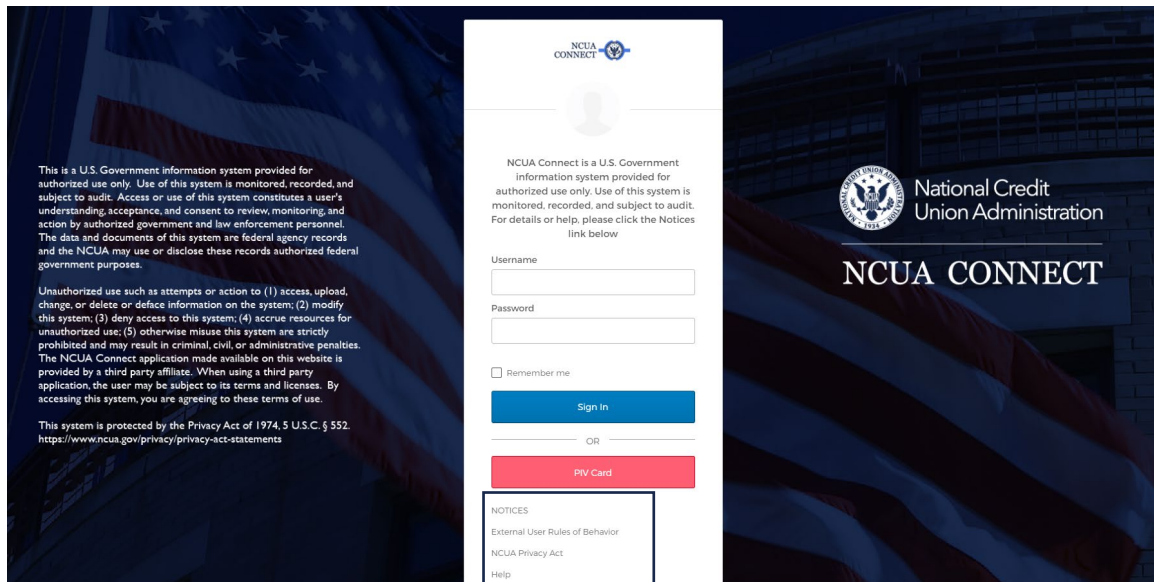


Chapter 1: NCUA Connect

Overview

NCUA Connect is a secure portal to access NCUA applications implemented as part of the Enterprise Solution Modernization initiative. NCUA Connect enables users to securely interact and share information with the NCUA and embraces important security practices such as multifactor authentication, least privilege role-based access, and data encryption at transit and rest. All users of NCUA systems must comply with the NCUA Rules of Behavior. The External User Rules of Behavior are available on the NCUA's website at www.ncua.gov.

From the login page, users can click the **NOTICES** option beneath the **PIV Card** button for links to the External User Rules of Behavior and the NCUA's Privacy Act information.



Obtaining Access to NCUA Connect

Users must be granted access to NCUA Connect. NCUA staff will automatically be provisioned access based on your employee attributes. External users, including credit

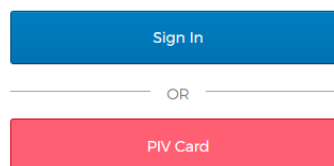


unions and state supervisory authorities (SSA), must have an account created by an administrator through the [Admin Portal](#).

NCUA Users – Accessing NCUA Connect

Below are the steps for a NCUA user to obtain access to NCUA Connect:

1. When a user’s access is granted, retrieve an email from NoReply@Okta.com with the subject “Welcome to NCUA Connect.” If you are granted access to a training environment as well as the main system, you will receive multiple email notifications.
2. Click the link to the sign-in page in the email to access the secure webpage.
3. Click **PIV Card** (or enter your temporary network username and password, if applicable, and click **Sign In**).



4. Set up at least one of three multifactor authentication methods: Okta Verify app, SMS text messaging, and/or voice call authorization. See the section below on [Setting Up Multifactor Authentication \(MFA\)](#) for more information.
5. When done, click **Finish**.

Note: If the user does not download the Okta Verify app to their phone, the only MFA options available to the user are SMS text messaging or a voice call. The Okta Verify app provides the user with a MFA code even when cellular service is unavailable.

External Users – Accessing NCUA Connect

Outlined below are steps for external users, such as credit unions and SSAs, to obtain access to NCUA Connect:

1. When a user’s access is granted, retrieve an email from NoReply@Okta.com with the subject “Welcome to NCUA Connect.” If you are granted access to a training



environment as well as the main system, you will receive multiple email notifications.

2. Click the **Activate Okta Account** link in the email.

To activate your account and initiate access to NCUA applications, please click the following button and follow the registration process.

Activate Okta Account

3. Follow the on-screen prompts and complete the registration process (e.g., create password, establish a challenge question, and choose a security image). Click **Create Account**.
4. Set up at least one of three multifactor authentication methods: Okta Verify app, SMS text messaging, and/or voice call authorization. See the section below on [Setting Up Multifactor Authentication \(MFA\)](#) for more information.
5. When done, click **Finish**.

Note: If the user does not download the Okta Verify app to their phone, the only MFA options available to the user are SMS text messaging or a voice call. The Okta Verify app provides the user with a MFA code even when cellular service is unavailable.

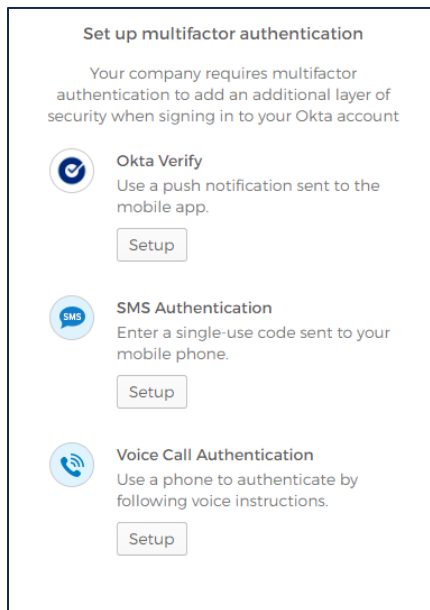
Initial Multifactor Authentication (MFA) Set Up

To provide the highest level of security, once logged in with a PIV card or through username credentials, users are required to undergo a MFA process. There are three options for MFA: the Okta Verify app, SMS text messaging, and voice call authentication.



Okta Verify App	SMS Text Messaging	Voice Call Authentication
<p>Using a smartphone, users approve a verification request. Alternatively, users enter a code (from the app) on the NCUA Connect verification page. The app can be used without cellular phone reception and still obtain a MFA code.</p>	<p>Okta sends a text message containing a code. Entering this code on the NCUA Connect verification page will grant the user access to NCUA Connect.</p>	<p>Announces code via phone call. Entering this code on the NCUA Connect verification page will grant the user access to NCUA Connect.</p>

Users are encouraged to set up all three methods and may use different phone numbers for each option. When using the MFA function, users can select the option they want to use by clicking the arrow next to the authentication type.




For additional information about the Okta Verify app not covered in this user guide, click this [link](#).



First-time NCUA Connect users will be prompted to set up at least one MFA method. If a user would like to set up an additional MFA method at a later time, they can do so from their profile, after signing into NCUA Connect. See the section below on [Updating Multifactor Authentication Options](#).

MFA Setup: Okta Verify app

1. Using a mobile device, download the **Okta Verify** app from the Android Play Store or the Apple App Store.
2. Sign into NCUA Connect for the first time and click **Setup** beneath the **Okta Verify** option.
3. Choose the mobile device type and click the **Next** button.
4. On the smartphone, launch the Okta Verify app.
5. Click **Get Started**.
6. Click **Next** on the screen describing *How it works*.
7. Click **Add Account**. (Note: returning users may see a circle with a plus sign in the bottom right corner ).
8. Select **Organization** for the Account Type.
9. Click **Scan a QR Code**. You may need to allow Okta Verify to access your camera for the next step.
10. Using the smartphone camera, scan the QR code on the computer screen to enroll the smartphone device.



11. Click **Allow** to approve or deny requests without opening the Okta Verify app.
12. Click **Done**.
13. Upon successful completion, the user should receive a confirmation email.

Note: If a user obtains a new phone, they must setup their Okta Verify account again on the new device.



MFA Setup: SMS Text Message Authentication

1. After signing into NCUA Connect for the first time, click **Setup** beneath **SMS Authentication** option.
2. Enter the mobile device’s phone number then click **Send Code**.
3. The mobile device will receive a code via SMS text message.
4. Enter the code and click **Verify**.
5. The user will receive a message indicating the phone number has successfully been verified.

Receive a code via SMS to authenticate

United States

Phone number

+1 7035482411 Sent

Enter Code

Verify

MFA Setup: Voice Call Authentication

1. After signing into NCUA Connect for the first time, click **Setup** beneath the **Voice Call Authorization** option.
2. Enter the phone number. An extension may be added, but is not required.
3. Click **Call**. The user will receive a phone call that will announce the verification code twice.
4. Enter the code and click **Verify**.
5. The user will receive a message indicating that the phone number has successfully been verified.

Follow phone call instructions to authenticate

United States

Phone number Extension

+1 7033950194

Calling

Enter Code

Verify

Note: NCUA users should not click the [Do Not Challenge Me](#) checkbox while setting up their MFA options. If selected, the user will not be prompted to setup additional MFA options. Refer to the [Updating MFA Options](#) section to setup additional options.

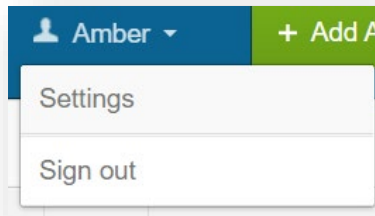
Adding and Updating Multifactor Authentication Options

Follow these steps to set up additional MFA options after initial setup or to change an existing MFA option.

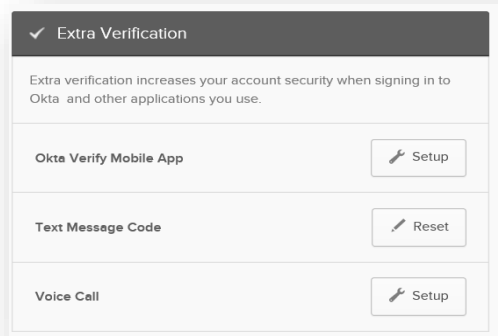
1. Sign into NCUA Connect to load the **MFA** landing page.
2. Click **Send Push**, **Enter Code**, or **Send Code** (depending on the MFA option selected).



3. Enter the code in the **Enter Code** box adjacent to **Send Code** then click **Verify**, if applicable.
4. Once successfully verified, the NCUA Connect home page appears.
5. Click the username in the upper right corner and select **Settings**.



6. Scroll to the **Extra Verification** section.
7. Click **Reset** or **Setup** next to the MFA method you wish to add or update.



Note: An external user can also contact their Admin Portal administrator or the NCUA’s technical assistance service at OneStop@NCUA.gov and request assistance to reset an MFA option.



Signing into NCUA Connect

Signing in using a PIV Card – NCUA Users Only

To log into NCUA Connect using a PIV card:

1. Navigate to the NCUA Connect sign in page.
2. Ensure the PIV card is securely inserted into the computer's designated slot.
3. Click the **PIV Card** button.
4. Enter your Pin number, if prompted.
5. Complete the selected MFA option. See the [Using Multifactor Authentication](#) section for additional details.

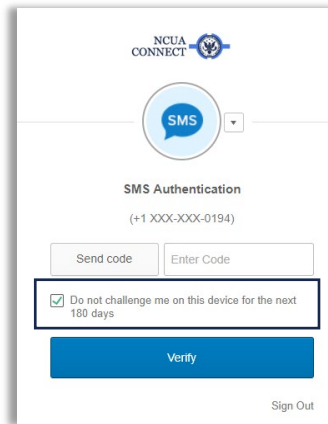
Note: For NCUA users who do not have a PIV card, they can use the temporary network username and password provided by the OneStop Help Desk to login.

Do Not Challenge Me Functionality - NCUA Users Only

By selecting the check box next to **Do not challenge me on this device for the next 180 days**, NCUA users will not be prompted for MFA after entering their PIV PIN for 180 days. To use this option, users must be connected to the NCUA secured network or through the VPN.

Note: The Do Not Challenge Me functionality is not available to contractors or external users such as credit unions and SSAs.

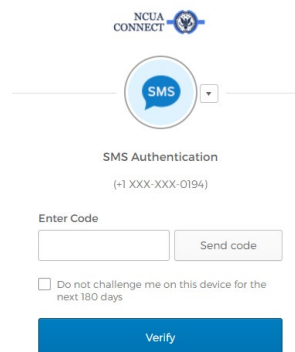
1. Click the **PIV Card** button.
2. Select the appropriate certificate to log in.
3. Input PIN, if prompted.
4. Enter the MFA code.
5. Select the **Do not challenge me...** check box.
6. Click **Verify**.



Signing in Using a Username and Password

To log into NCUA Connect with a username and password:

1. Navigate to the NCUA Connect sign in page.
2. Enter username and password credentials.
3. Click the blue **Sign In** button.
4. Complete the selected MFA option. See the [Using Multifactor Authentication](#) section for additional details.
5. Click **Verify**.

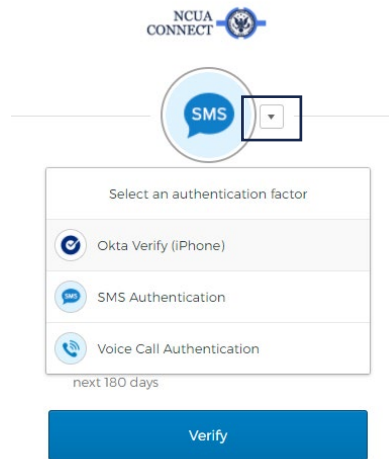


Note: Users can change their MFA preference by selecting the dropdown arrow near the top of the screen and choosing another MFA option.



Using Multifactor Authentication (MFA)

When logging into NCUA Connect, the system will default to the last MFA method used by that person. To select a different MFA option, click the arrow near the top of the screen to display the other options.



Note: If the user only set up one MFA option, the arrow to select other alternatives will not be available. See the section on [Adding and Updating MFA Options](#).

The steps below outline how users will authenticate their identity with each MFA method.

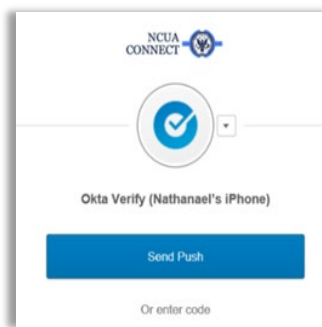
Using Okta Verify Authentication

1. Navigate to the NCUA Connect sign in page.
2. Sign into NCUA Connect.
3. Click **Send Push**.
4. The mobile device app will receive a notification asking to approve or deny the sign in request.
5. Select **Approve**. Users may be prompted to use **Touch ID for Okta Verify** to use a fingerprint to access their account.



6. Alternatively, the user can select the **Or Enter Code** hyperlink below the **Send Push** button:
 - a. Once selected, an **Enter Code** box will appear.
 - b. Open the **Okta Verify** app on the phone.
 - c. Enter the code appearing on the **Okta Verify** app landing page.
 - d. Click **Verify**.

Signing in successfully using either method will bring the user to the NCUA Connect landing page.

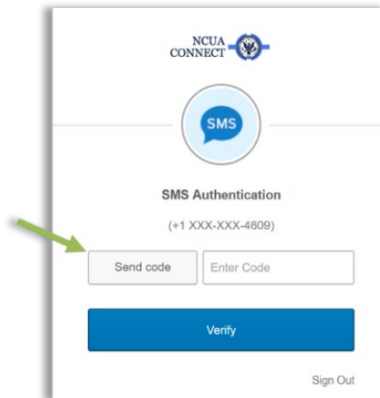


Using SMS Text Message Authentication

After logging in through NCUA Connect, the user will be asked to provide a code delivered through SMS text message. The SMS text message will be sent to the mobile phone number provided when initially setting up this form of MFA.

1. Navigate to the NCUA Connect sign in page.
2. Log into NCUA Connect.
3. Click **Send Code** to receive the SMS message containing the MFA code.
4. Enter the code in the **Enter Code** box.
5. Click **Verify**.

Once successfully verified, the user will be taken to the NCUA Connect home page.

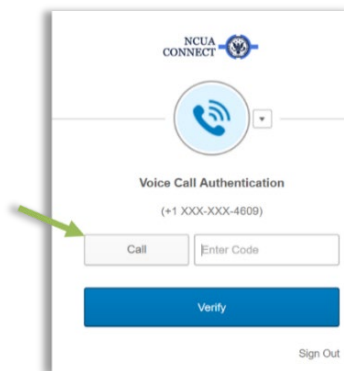


Using Voice Call Authentication

After signing in through the NCUA Connect page, the user will be asked to provide a code delivered through a voice call. The voice call will be made to the phone number provided when initially setting up this form of MFA.

1. Navigate to the NCUA Connect sign-in page.
2. Log into NCUA Connect.
3. Click **Call** to receive a phone call containing the code.
4. Enter the code in the **Enter Code** box adjacent to **Call**.
5. Click **Verify**.

Once successfully verified, the user will be taken to the NCUA Connect home page.





NCUA Connect Assistance and Resetting Passwords

Credit unions and SSAs are delegated the authority to add and update user accounts for their organization through the Admin Portal application. Designated administrators can assist their users with most access issues. If a SSA or credit union user needs assistance with their NCUA Connect account, it is recommended they contact their administrator first. NCUA’s Technical Support is also available by emailing OneStop@ncua.gov.

The table below outlines the resources available to assist SSA and credit union users with accessing NCUA Connect.

Assistance Requested	Resource
Cannot login	Contact your Admin Portal Administrator. They can unsuspend user accounts locked due to inactivity ¹ . If the account is locked because the user exceeded the maximum number of login attempts, the administrator can click the reset password option to unlock the account or contact NCUA’s Technical Support OneStop@NCUA.gov to unlock the account.
Password or MFA Reset	Contact your Admin Portal Administrator to reset your password or MFA.
Challenge Question Assistance	Contact NCUA’s Technical Support at OneStop@NCUA.gov . A temporary password will be emailed to the user and their challenge questions will be reset.

NCUA users should contact NCUA’s Technical Support at OneStop@ncua.gov for assistance with accessing NCUA Connect.

Adding Apps to NCUA Connect

For NCUA users, all approved applications will be populated on the user’s NCUA Connect *My Applications* landing page. If a user is missing an application, contact your supervisor to request access through OneStop.

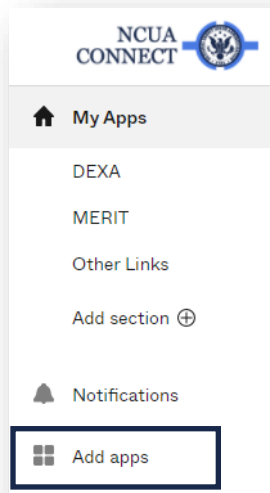
¹ NCUA Connect accounts become suspended due to inactivity if the user has not accessed NCUA Connect in the last 120 days.



For SSA and credit union users, application access is controlled by your Admin Portal Administrator. Once access is requested by the administrator and approved by the NCUA, the application will be available on NCUA Connect.

Note: The first time a user is approved for application access, they will receive a *Welcome to NCUA Connect* email. Each subsequent approved application will trigger a *Notification of Application Approval* email to the user.

The **Add Apps** functionality in NCUA Connect is not being used at this time.





Chapter 2: Admin Portal

Overview

Introduction to Admin Portal

The Admin Portal application provides designated credit union and SSA users the ability to manage user access to NCUA Connect and its associated applications for users within their organization. The Admin Portal is not used to grant access to NCUA Connect for NCUA users. It also, allows SSA and NCUA staff the ability to run NCUA application user reports to support application access monitoring and credit union access customer service.

The following application access can be granted through the Admin Portal. Please note, not all applications are available to all users.

- Modern Examination and Risk Identification Tool (MERIT) – The NCUA’s web-based examination tool. When access is granted to MERIT, users also obtain access to the Data Exchange Application (DEXA). DEXA is the NCUA’s web-based data ingest tool used to import credit union member loan and share data provided in compliance with [Share and Loan Record Specifications](#).
- Consumer Access Process and Reporting Information System (CAPRIS) – The NCUA’s upgrade to the Field of Membership Internet Application (FOMIA). CAPRIS is used only by multiple common bond federal credit unions to submit field of membership (FOM) application forms for the purpose of adding occupational or associational common bond groups to its FOM. All other credit unions should refrain from requesting access to CAPRIS.
- CUOnline – The NCUA’s web-based application used by credit unions and state supervisory agencies to submit and certify operational and quarterly financial information to the NCUA for natural person credit unions. CUOnline contains two sections: the Profile and Call Report.
- Corporate CUOnline (CCUOnline)– The NCUA’s web-based application used by credit unions and state supervisory agencies to submit and certify operational and quarterly financial information to the NCUA for corporate credit unions.



- Partner Gateway (SSA users only) – The NCUA’s enclave for sharing examination and supervision related information including access to reports and other applications.
- Secure File Transfer Portal (NCUA and SSA users only) – The NCUA’s application for initiating and managing secure file sharing.
- Email Distribution Groups (SSA users only) – Utility for adding or updating SSA staff member contact information in the NCUA’s SSA Email distribution lists (e.g., Examiners and Officials).
- Learning and Managing Performance (LAMP) (SSA users only) – The NCUA’s web-based application for managing and tracking training courses. The Admin Portal includes email notifications to inform the NCUA, Admin Portal administrators, and NCUA Connect users throughout the workflow processes. See Appendix A for a listing and description of the email notifications.

Accessing the Admin Portal

The Admin Portal is an application on NCUA Connect. The NCUA must authorize and provide access to identified credit union and SSA administrators. Once provisioned, credit union and SSA administrators are responsible for authorizing, provisioning, and deactivating users within their organization. The following indicates the steps to request creation of an Admin Portal administrator account for a credit union or SSA:

1. A verified and authorized credit union (e.g., official contact in CU Profile and/or existing NCUA Connect Administrator) or SSA official submits a request to create an administrator account to NCUA’s Technical Support at OneStop@ncua.gov indicating your organization, name, email address, and any applications you may need to access in addition to the Admin Portal (e.g., MERIT, CAPRIS, etc.).
2. NCUA will coordinate with the respective NCUA regional office or SSA, if applicable, to verify any requests.
3. Once the administrator account is approved, the NCUA Connect account will be created. The designated administrator will retrieve the email sent from NoReply@Okta.com. This email includes a link to the NCUA Connect site.
4. Follow the instructions and complete the process to access [NCUA Connect](#).



Note: NCUA and SSA supervisor/examiners with MERIT access will automatically be provisioned with the Admin Portal application’s report module but no administrative functions. An NCUA Connect Administrator role is required for admin functionality. Also, approved Admin Portal administrators are automatically granted access to the Admin Portal application. If the administrator has access to another NCUA application, they can request additional application access for their own account using the access change function located in the action button. Administrators who require additional application access can also request a peer Admin Portal administrator make an access change to their account. Finally, the NCUA technical team at OneStop@NCUA.gov is able to assist if needed.

If an administrator’s NCUA Connect account is locked or needs to be reset, the administrator should first contact a peer Admin Portal administrator and request a reset. If the locked-out user doesn’t remember the answers to their security challenge questions, then contact the NCUA’s Technical Support team at OneStop@NCUA.gov. For this reason, organizations are encouraged to assign two Admin Portal administrators to ensure user account management is not interrupted if one administrator is obtaining technical assistance.

NCUA Connect User Roles

All NCUA Connect users must be assigned at least one user role. This role determines the applications the user can access and their permissions within various systems. A role must be assigned when the user account is established and can be modified by the Admin Portal administrator for the organization, if needed. Upon account creation, the administrator triggers a workflow to the NCUA Application owner’s delegates who are then responsible for approving application access.

Credit Union User Roles

Credit union users are restricted to entering and viewing information for their organization within all applications.



	SYSTEMS			
	DEXA	MERIT	CAPRIS	CCU/CUOnline
MERIT CU View All	Upload loan and share files. View upload history.	View, respond to, and request due date changes on examination findings. Respond to surveys and document requests. Download completed exam reports.	N/A	N/A
MERIT CU Limited Access	Upload loan and share files. View upload history.	Respond to surveys and document requests.	N/A	N/A
Capris CU User	N/A	N/A	Submit occupational or associational group FOM expansion requests. Upload supporting documentation. View history. View housekeeping amendments.	N/A
CCU/ CUOnline CU Admin	N/A	N/A	N/A	Add, modify, remove Call Report Data, Submit Call Report. Add, modify, remove Profile data. Save, certify, and submit Profile. Delete previously submitted call reports.



ROLE	SYSTEMS			
	DEXA	MERIT	CAPRIS	CCU/CUOnline
CCU/ CUOnline CU User	N/A	N/A	N/A	Add, modify, remove Call Report Data, Submit Call Report. Add, modify, remove Profile data. Save, certify, and submit Profile.
CCUOnline CU Basic	N/A	N/A	N/A	View only (CCUOnline only).

State Supervisory Authority User Roles

SSA users are restricted to entering and viewing information for federally-insured state chartered credit unions in their state.

	SYSTEMS			
	DEXA	MERIT	Admin Portal	CCU/CUOnline
SSA MERIT Field Staff and SSA Field Supervisor	Upload loan and share files. View upload history.	Create Exams. View credit union information and analytics. View exam information.	Reports Tab (only)	N/A
SSA MERIT Office View All	Upload loan and share files. View upload history.	View credit union information and analytics. View exam information.	N/A	N/A



	SYSTEMS			
	DEXA	MERIT	Admin Portal	CCU/CUOnline
CUOnline SSA Admin	N/A	N/A	N/A	<p>For credit unions in their state:</p> <ul style="list-style-type: none"> Add and edit SSA information. Assign permissions for their specific credit unions to users with the SSA Examiner role. Add, modify, and remove Call Report data. Submit and validate Call Reports. Add, modify, and remove Profile data. Save, certify, and submit Profile. Delete previously submitted call reports. Use the My Credit Unions module to monitor and track Call Report submissions for all FISCUs/NFICUs.



	SYSTEMS			
	DEXA	MERIT	Admin Portal	CCU/CUOnline
CUOnline SSA Examiner	N/A	N/A	N/A	<p>For assigned credit unions in their state:</p> <p>Delete and update their assignments.</p> <p>Add, modify, and remove Call Report data.</p> <p>Submit and validate Call Reports.</p> <p>Add, modify, and remove Profile data, Save, Certify, and Submit Profile data.</p> <p>Use the My Credit Unions module to monitor and track Call Report submissions for all FISCUs/NFICUs.</p>
CUOnline SSA User	N/A	N/A	N/A	<p>For assigned credit unions in their state:</p> <p>View Call Report and Profile data.</p>
CCUOnline SSA Admin	N/A	N/A	N/A	<p>For assigned credit unions in their state:</p> <p>View Call Report and Profile data.</p>
CCUOnline SSA Examiner			N/A	<p>Use the My Credit Unions module to monitor and track Call Report submissions for all FISCUs/NFICUs.</p>
CCUOnline SSA User			N/A	<p>Use the My Credit Unions module to monitor and track Call Report submissions for all FISCUs/NFICUs.</p>



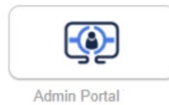
ADMINISTRATIVE SUPPORT SYSTEMS	
ROLE	USER ROLE DESCRIPTIONS
SSA User for Partner Gateway	<p>The Partner Gateway Tile provides multi-factor authentication to the applications hosted on the Partner Gateway including reports, utilities, and other applications.</p> <p>[<i>Note:</i> Users will receive separate communications from the NCUA regarding username and passwords when accounts are first created. Single sign on into the applications from the NCUA Connect is not implemented at this time.]</p>
SSA Secure File Transfer Portal	Provides access to the NCUA’s Secure File Transfer Portal and allows the user to initiate and manage file transfer and sharing.
SSA Examiner Email Distribution List	Adds SSA users to the NCUA email list for all SSA examination staff who routinely engage with the NCUA and use our systems/services.
SSA Officials Email Distribution Group	Adds SSA users to the NCUA’s email list for all SSA Office and Support staff who routinely engage with the NCUA and use our systems/services.
LAMP	Adds or removes SSA user access to the NCUA’s LAMP system.



Opening the Admin Portal Application

To access the Admin Portal application:

1. Log into NCUA Connect.



2. Click the Admin Portal tile.

Note: The Admin Portal works best using Google Chrome or Microsoft Edge browsers. The NCUA discourages using Internet Explorer.

Adding Users

The landing page for the Admin Portal includes options to search for users or add a new user. To add a user for your organization:

1. Click the **New User** button

2. Enter the user's First Name and Last Name. An optional Middle Name can be added.
3. Enter a valid Email Address. In most cases, this will be the user's Username for accessing NCUA Connect.

4. If a different email address is preferred for the Username, uncheck the box **Use as Username**, and a new field will appear where a different login Username can be entered. The Username must be in an email format for the system to accept the



entry but it does not have to be a valid email address. Each user must have a unique Username to access NCUA Connect. If the Username already exists, the user will receive an error message.

* Email Address

Use as User Name

* User Name

Limit the naming convention to the following characters: 0-9, a-z, A-Z, ! - _ . & ()

5. Select a [role](#) for the user.
6. Enter any optional **Comments**.
7. Click **Submit**.

Note: Okta Admin Portal Usernames do not accept special characters. If the user's email address has special characters, such as an apostrophe, please create a unique Username excluding any special characters.

Upon submission, an email notification is sent to the NCUA. A staff member will review the request for application access per NCUA security requirements and approve or deny the new user request. The requestor will receive an email notification once the request has been acted upon. NCUA staff may contact the administrator if they have any questions about the new user request. New accounts will not appear in the user list until reviewed, and approved or denied.

When a new account is approved, the new user will receive an email notification from NCUA Connect (noreply@okta.com) prompting them to set up their account similar to the message below. If an account is not approved, the original requestor will receive an email providing either a rationale or additional guidance for account request re-submission.



Hi Mike,

Welcome to NCUA Connect (via the Okta service), the National Credit Union Administration's secure, central access point for web applications.

Your username is
The sign-in page is

Your system administrator has created an Okta user account for you.

To activate your account and initiate access to NCUA applications, please click the following button and follow the registration process.

[Activate Okta Account](#)

This link expires in 7 days.

Watch this short [video](#) to learn more about NCUA Connect. By clicking the link above and activating your account you are agreeing to follow NCUA's system [rules of behavior](#). NCUA's system rules of behavior, user guides, and additional information are available for reference on [NCUA's web site](#).

If you experience difficulties accessing your account, send a request to your administrator or contact NCUA OneStop at OneStop@NCUA.gov or (703)518-6450 or (800)827-3255.

Note: Once a new user is submitted to the NCUA for approval, the user will not show on the organization's list of users in the Admin Portal until approved by the NCUA. If an administrator tries to add the same user twice, you will receive an error message.

Updating and Removing Users

Admin Portal Administrators can update and remove users for their organization. The following actions can be taken:

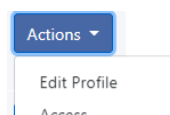
- **Edit Profile** – provides a form to update the user's First Name, Middle Name, Last Name, Username, and Email Address. [*Note:* If an SSA staff member that is only part of an email distribution group (no NCUA Connect Account) requires an update to their user profile (*e.g.*, name or email address) please contact onestop@ncua.gov.]



- **Access** – provides a form to update the user’s NCUA Connect and application role(s). In some cases, if a role is removed and added back, the NCUA approval process may be triggered (e.g., CAPRIS User role). If an application has more than one role available, such as MERIT, and a user already has one MERIT role, adding another MERIT role will not trigger the NCUA approval workflow.
- **Reset Password** – sends a password reset email notification to the user. The user must click a link in the email notification to reset their password. If a user locks their account due to a number of unsuccessful attempts logging in, this action will also unlock a user’s account.
- **Reset MFA** – sends a multifactor authentication email notification to the user.
- **Suspend** – disables the user’s account; however, allows the SSA or credit union administrator the ability to re-instate the account without NCUA intervention. Suspend should be used in situations where temporary access removal is necessary.
- **Unsuspend** – re-instates the suspended user’s account.
- **Deactivate** – removes the user account. Deactivation should be used in situations where the user has been off-boarded from your organization or will no longer require NCUA Connect access in the future.
- **Request Reactivation** – submits a reactivation request to the NCUA application approvers.

To update a user’s account:

1. Locate the user account to be updated.
2. Click **Actions**.
3. Select the action. A message will appear on screen indicating successful completion of the requested Action. To remove access to NCUA Connect for the user, select the **Suspend** or **Deactivate** option. To add applications or change roles, select **Access** and then select the appropriate user roles for each application. Addition of applications or role changes may trigger a review and approval step, and the new or updated role assignments will not display immediately.





Access User Reports

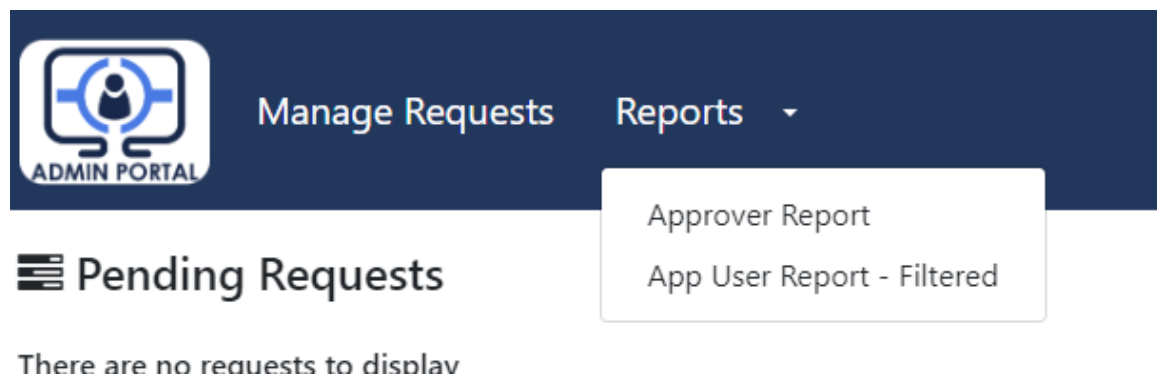
There are two user reports available in the Admin Portal:

- **Approver Report:** Available to NCUA Application approvers. This report includes two tabs with full insight into all NCUA Connect users including key attributes and system access.
- **App User Report – Filtered:** Available to CU/SSA NCUA Connect Administrators and SSA/NCUA Supervisor and Field staff with MERIT access. This report provides a single tab filtered view of NCUA Connect users for users under their purview.

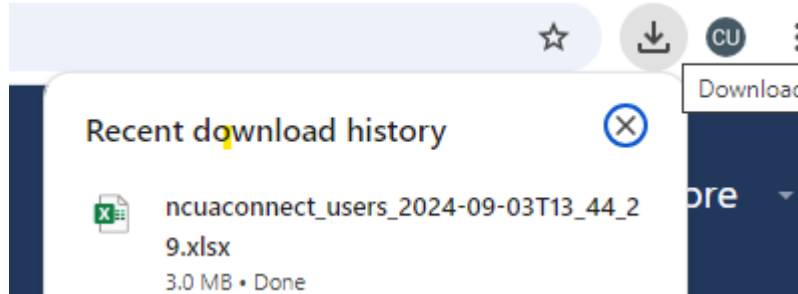
The reports should be used to complete routine monitoring of application users to ensure system access is up to date. Departed user’s accounts must be deactivated, and other user’s access should be limited (least privileged) based on the user’s role within their organization. The report can also be used to identify the NCUA Connect Administrators within an organization to help coordinate new/updated access, as needed.

To download a user report:

1. Sign into the Admin Portal.
2. Click Reports and select the report from the drop down.



3. Access the downloaded Microsoft Excel based report from the Downloads folder on your computer.



4. Open the report and filter on the on the most relevant field.

Note: Administrators will only be able to see information associated with users that fall within their administration and supervision authority as defined in MERIT’s least privilege role based security model. This report must be protected in accordance with NCUA’s rules of behavior and your organization’s information security policies.

Status Fields

The user list in the Admin Portal includes various account status fields including the following:

Status	Description
Active	User can login to NCUA Connect.
Deactivated	The user’s account is no longer active. All application assignments are removed. The account must be reactivated and approved by the NCUA for the user to access NCUA Connect.
Deleted	Refers to accounts that are in the Okta Admin Portal applications database, but no longer in NCUA Connect. These users do not have access to NCUA Connect.
Locked Out	The user’s account is locked. This is common if the user has multiple failed attempts at logging in. The administrator must Reset Password or



Status	Description
	Deactivate and Reactivate the account to unlock it. Deactivating the user's account will trigger a workflow for NCUA approval and require the user to set up their login options again. NCUA's Technical Support at OneStop@NCUA.gov can also unlock accounts..
Password Expired	The user's password has expired and needs to be reset by the administrator. Once reset, the user will receive an email notification with a password reset link.
Password Reset	The account requires a password to be: <ul style="list-style-type: none">• Established for the first time; or• The administrator needs to reset the password on their behalf. <p><i>Note:</i> If a user has forgotten the answer to their security questions, then the administrator will need to contact the NCUA Technical Support (OneStop@ncua.gov) and request a temporary password be sent to the end user.</p>
Provisioned (Pending User Action)	The user needs to take an action such as providing a new password or setting up their NCUA Connect multifactor authentication methods.
Recovery	The user's account has been reactivated, but the user has not completed the steps to set up their NCUA Connect account.
Staged	Accounts have been created, but the activation flow has not been initiated, or if there is a pending admin action.
Suspended	User account is inactive and must be unsuspended to login. This is common if the user has not logged into MERIT recently.



Appendices

Appendix A – Admin Portal Email Notifications

Notification	Recipients	Purpose
New Account Pending Approval	NCUA	Informs the NCUA a credit union or SSA Admin Portal administrator submitted a request to add or reactivate a user.
New Account Request Approved	Credit Union or SSA Admin Portal Administrator	Informs the requestor a new account request was approved by the NCUA. A separate email is sent to the new user prompting them to setup their NCUA Connect account. [Note: Application specific approval emails will be sent separately.]
New Account Request Denied	Credit Union or SSA Admin Portal Administrator	Inform the requestor a new user account request was denied and provides an explanation for the denial.
Access Change Request Pending Approval	NCUA	Informs the NCUA a credit union or SSA Admin Portal administrator submitted a request to add a role to user.
Application Approval	NCUA Connect User	Inform a user of new applications available on NCUA Connect
Application Change Request Approved	Credit Union or SSA Admin Portal Administrator	Inform the requestor a new application was approved by the NCUA.
User Reactivation Request Approved	Credit Union or SSA Admin Portal Administrator	Informs the requestor the account reactivation request was approved by the NCUA. A separate email is sent to the reactivated user prompting them to setup their NCUA Connect account.
User Reactivation Request Denied	Credit Union or SSA Admin Portal Administrator	Informs the requestor the user reactivation request was denied and provides an explanation for the denial.