NIGC TRIBAL MANAGEMENT SERVICES (TMS) PORTAL GUIDE V.1.0

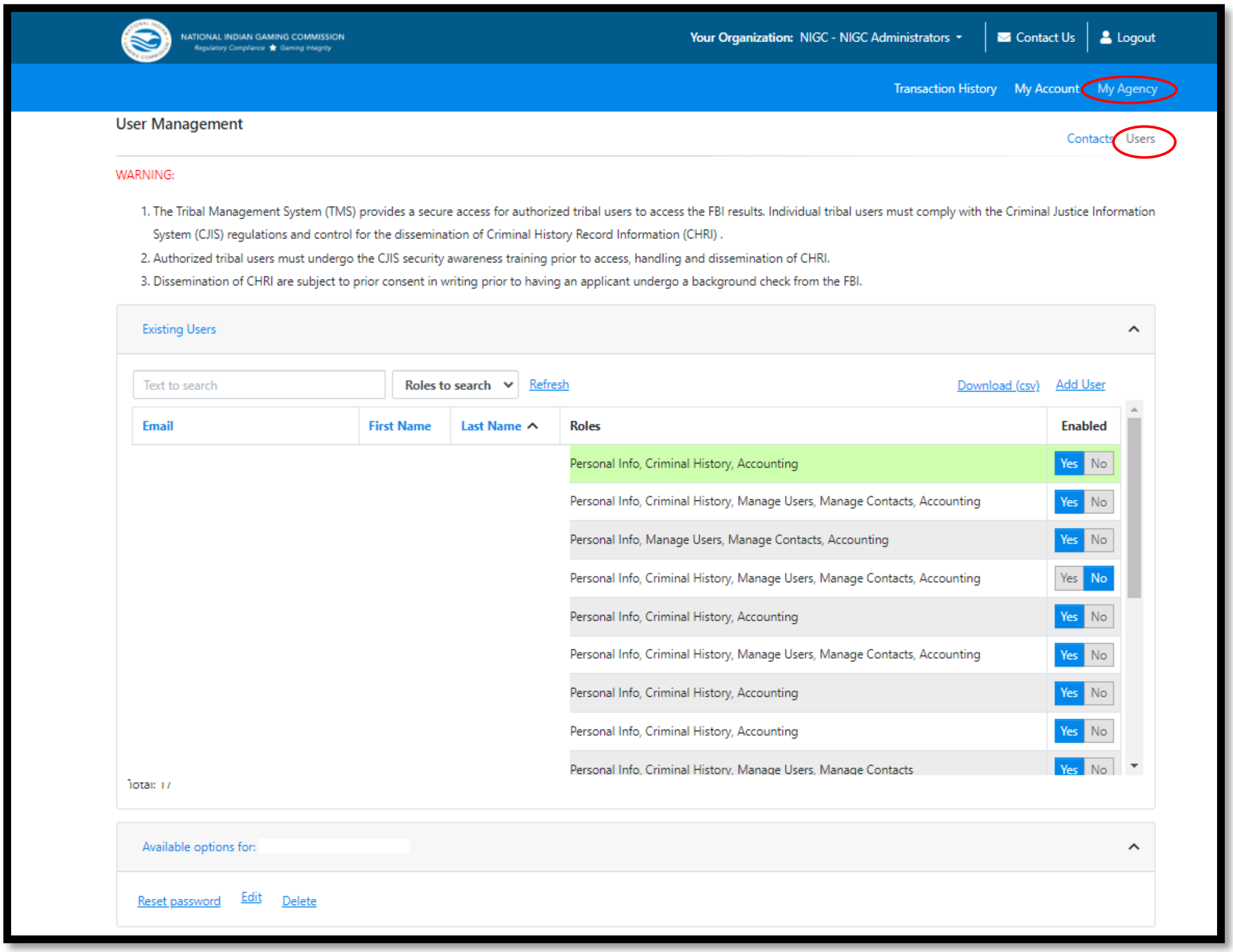
CJIS Audit Unit

Table of Contents

How to manage users in the TMS Portal (FP.NIGC.GOV)

Users with these roles can add, edit, and remove users associated with the agency as well as reset other users' passwords. All users can reset their own passwords, however users that can manage other users can reset other users' passwords when needed. In addition, all users can be configured to require a second form of authentication, called Two-Factor Authentication or Multi-Factor Authentication. The second form of authentication may be configured using SMS Text, DigiPass or Key Fob, or Authenticator App.

To access the User Management page, navigate to the "My Agency Tab" then to "Users" as seen below.


NATIONAL INDIAN GAMING COMMISSION
Regulatory Compliance ★ Gaming Integrity
Your Organization: NIGC - NIGC Administrators
Contact Us
Logout
Transaction History
My Account
My Agency
Contacts
Users

User Management

WARNING:

1. The Tribal Management System (TMS) provides a secure access for authorized tribal users to access the FBI results. Individual tribal users must comply with the Criminal Justice Information System (CJIS) regulations and control for the dissemination of Criminal History Record Information (CHRI) .
2. Authorized tribal users must undergo the CJIS security awareness training prior to access, handling and dissemination of CHRI.
3. Dissemination of CHRI are subject to prior consent in writing prior to having an applicant undergo a background check from the FBI.

Existing Users

Text to search | Roles to search | Refresh | Download (csv) | Add User

Email	First Name	Last Name ^	Roles	Enabled
			Personal Info, Criminal History, Accounting	[✓ Yes] No
			Personal Info, Criminal History, Manage Users, Manage Contacts, Accounting	[✓ Yes] No
			Personal Info, Manage Users, Manage Contacts, Accounting	[✓ Yes] No
			Personal Info, Criminal History, Manage Users, Manage Contacts, Accounting	Yes [✓ No]
			Personal Info, Criminal History, Accounting	[✓ Yes] No
			Personal Info, Criminal History, Manage Users, Manage Contacts, Accounting	[✓ Yes] No
			Personal Info, Criminal History, Accounting	[✓ Yes] No
			Personal Info, Criminal History, Accounting	[✓ Yes] No
			Personal Info, Criminal History, Manage Users, Manage Contacts	[✓ Yes] No

Total: 17

Available options for:

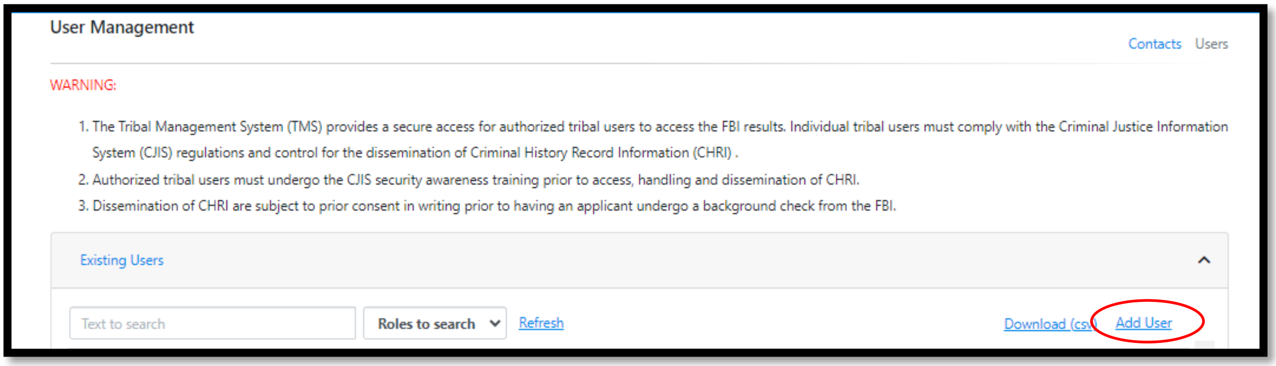
Reset password Edit Delete

Add an Agency User:

For Admins:

Adding a user to an agency will create a user account for the user if it does not already exist to another agency. Once the user has been configured and added, the activation process needs to be completed by the newly added user. They will receive an email with an expiring single-use link to complete the activation process.

To Add a User, expand the "Existing Users" Tab under User Management and click on "Add User" as seen below.

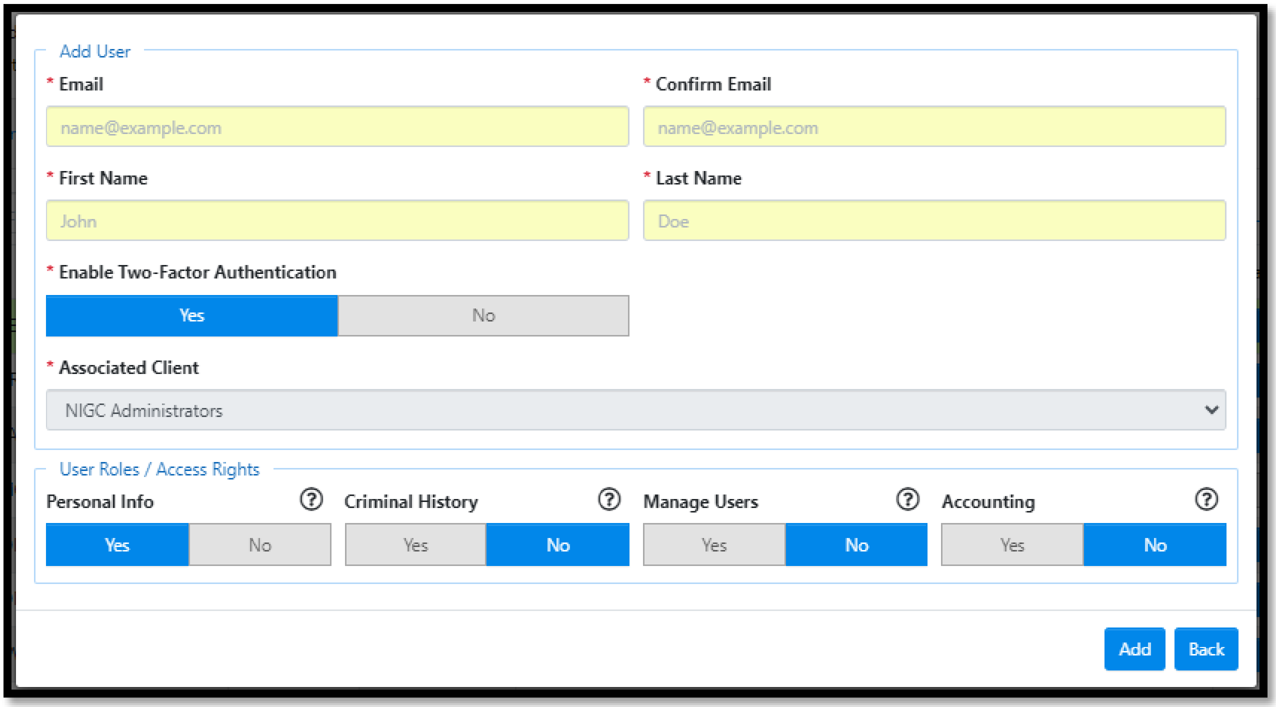


User Management

WARNING:

1. The Tribal Management System (TMS) provides a secure access for authorized tribal users to access the FBI results. Individual tribal users must comply with the Criminal Justice Information System (CJIS) regulations and control for the dissemination of Criminal History Record Information (CHRI) .
2. Authorized tribal users must undergo the CJIS security awareness training prior to access, handling and dissemination of CHRI.
3. Dissemination of CHRI are subject to prior consent in writing prior to having an applicant undergo a background check from the FBI.

Once "Add User" is clicked, a window should appear as seen below.



Add User

* Email: name@example.com

* Confirm Email: name@example.com

* First Name: John

* Last Name: Doe

* Enable Two-Factor Authentication: [✓ Yes] No

* Associated Client: NIGC Administrators

User Roles / Access Rights

Personal Info: [✓ Yes] No

Criminal History: Yes [✓ No]

Manage Users: Yes [✓ No]

Accounting: Yes [✓ No]

Email

The email address of the user to be added.

1. The email address could be for an existing user if they are not already associated with an agency.
2. This is the address the Activation email will be sent to.

First and Last Names

The respective names of the user

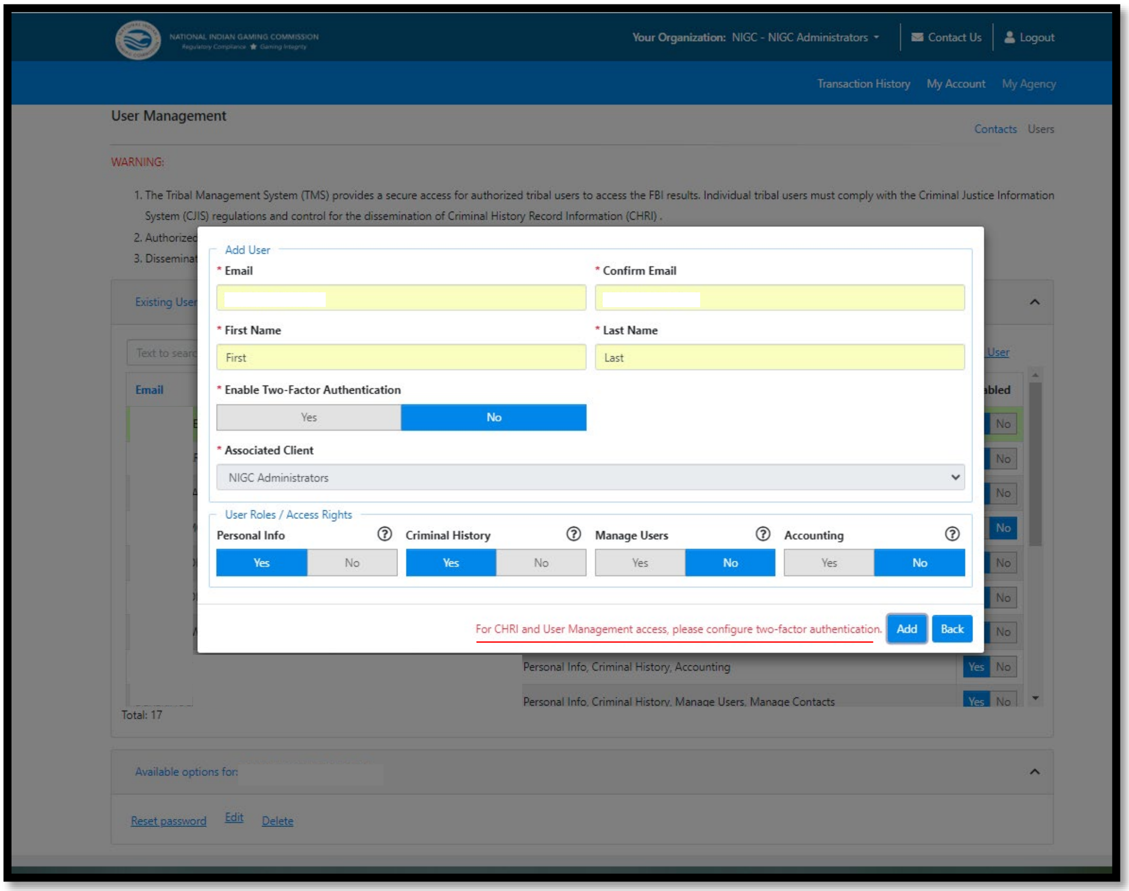
1. If the user account already exists, their existing names are used when addressing the user in the Activation email.

Enable Two-Factor Authentication

Whether the user is required to use a second method of authentication during login

1. This option is initially enabled by default if your agency requires Two-Factor Authentication for all record types.
2. The toggle will automatically be set to **Yes** if the **Criminal History** or **Manage Users** roles are enabled.

NOTE: If the **Criminal History** or **Manage Users** roles are enabled, AND the **Enable Two-Factor Authentication** toggle is set to **No,**
YOU WILL NOT BE ABLE TO FINISH ADDING A USER



User Management

WARNING:

1. The Tribal Management System (TMS) provides a secure access for authorized tribal users to access the FBI results. Individual tribal users must comply with the Criminal Justice Information System (CJIS) regulations and control for the dissemination of Criminal History Record Information (CHRI) .
2. Authorized
3. Disseminat

Add User

* Email

* Confirm Email

* First Name: First

* Last Name: Last

* Enable Two-Factor Authentication: Yes [✓ No]

* Associated Client: NIGC Administrators

User Roles / Access Rights

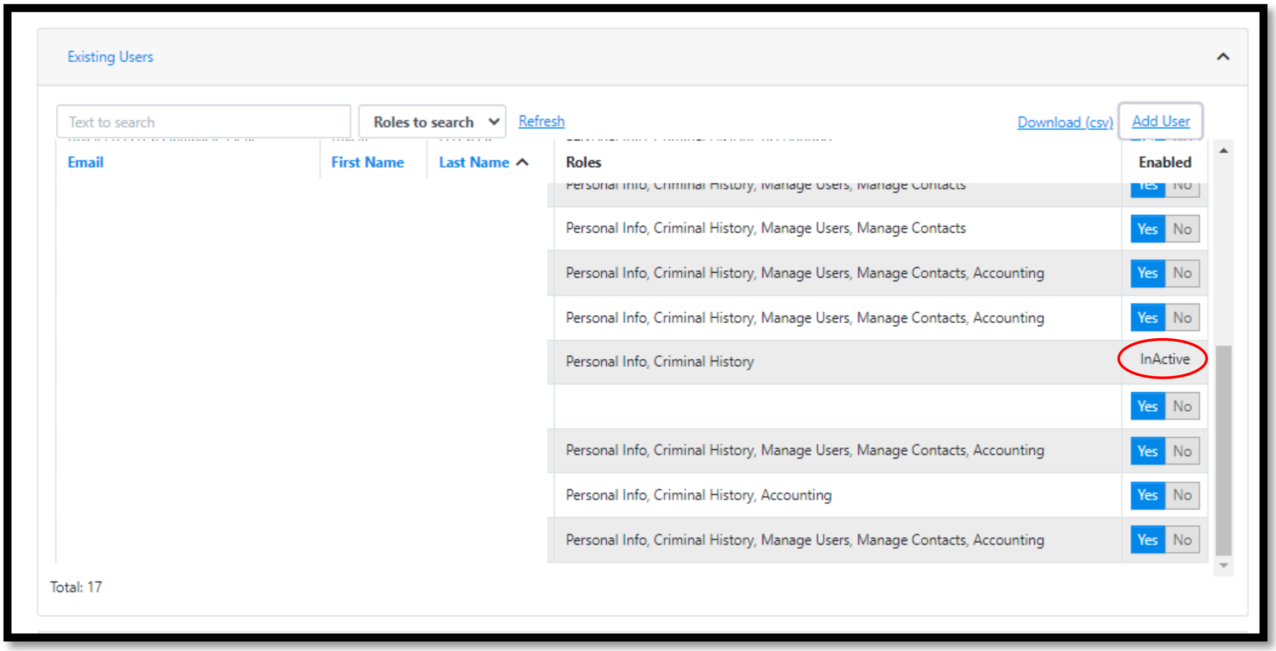
Personal Info	Criminal History	Manage Users	Accounting
[✓ Yes] No	[✓ Yes] No	Yes [✓ No]	Yes [✓ No]

For CHRI and User Management access, please configure two-factor authentication.

Add Back

Personal Info, Criminal History, Accounting	Yes	No
Personal Info, Criminal History, Manage Users, Manage Contacts	Yes	No

Once the configuration is valid there will be a confirmation window to confirm before adding the user. Once Confirmed the user will be successfully added. Exit out of the window by clicking "Back". The page will reload, and the new user can be seen as **InActive**.



Email	First Name	Last Name	Roles	Enabled
			Personal Info, Criminal History, Manage Users, Manage Contacts	Yes No
			Personal Info, Criminal History, Manage Users, Manage Contacts	Yes No
			Personal Info, Criminal History, Manage Users, Manage Contacts, Accounting	Yes No
			Personal Info, Criminal History, Manage Users, Manage Contacts, Accounting	Yes No
			Personal Info, Criminal History	InActive
				Yes No
			Personal Info, Criminal History, Manage Users, Manage Contacts, Accounting	Yes No
			Personal Info, Criminal History, Accounting	Yes No
			Personal Info, Criminal History, Manage Users, Manage Contacts, Accounting	Yes No

Total: 17

The **InActive** status on the right indicates that the user has not yet completed the activation process.

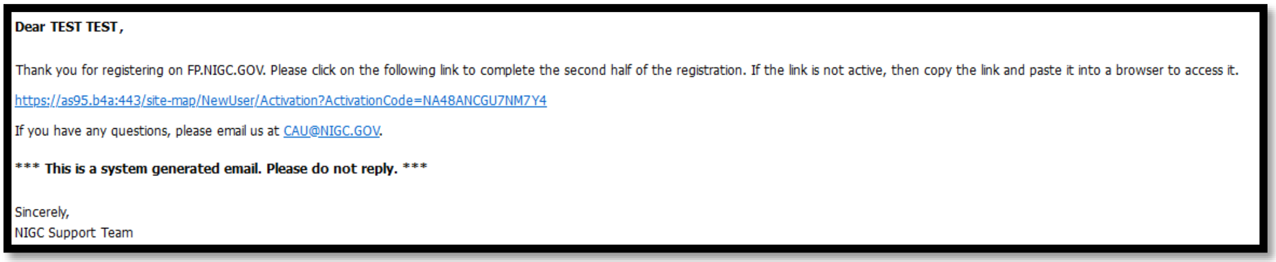
1. If the user's status is **InActive**, an option to **Resend Activation Link** to the user can be found in the **Available Options** menu.
2. When a user's activation link is resent, a new link is generated, and the previous link is invalidated.

For Users:

Activation Link

1. This link will expire 30 minutes after the user was added.
2. Users must **access** the link before it expires, however they can submit the activation form even after the link has expired.
3. Refreshing the page will check if the link has expired, so we recommend not refreshing the page once the user has accessed the link.
4. If the link expires before the user accesses the form, they will be redirected to the login page with a message that their link has expired.
5. If the user attempts to use an activation link after they have already completed activation, they will be redirected to the login page with a message that their account is already active.

Via Email



Dear TEST TEST ,

Thank you for registering on FP.NIGC.GOV. Please click on the following link to complete the second half of the registration. If the link is not active, then copy the link and paste it into a browser to access it.

https://as95.b4a:443/site-map/NewUser/Activation?ActivationCode=NA48ANCGU7NM7Y4

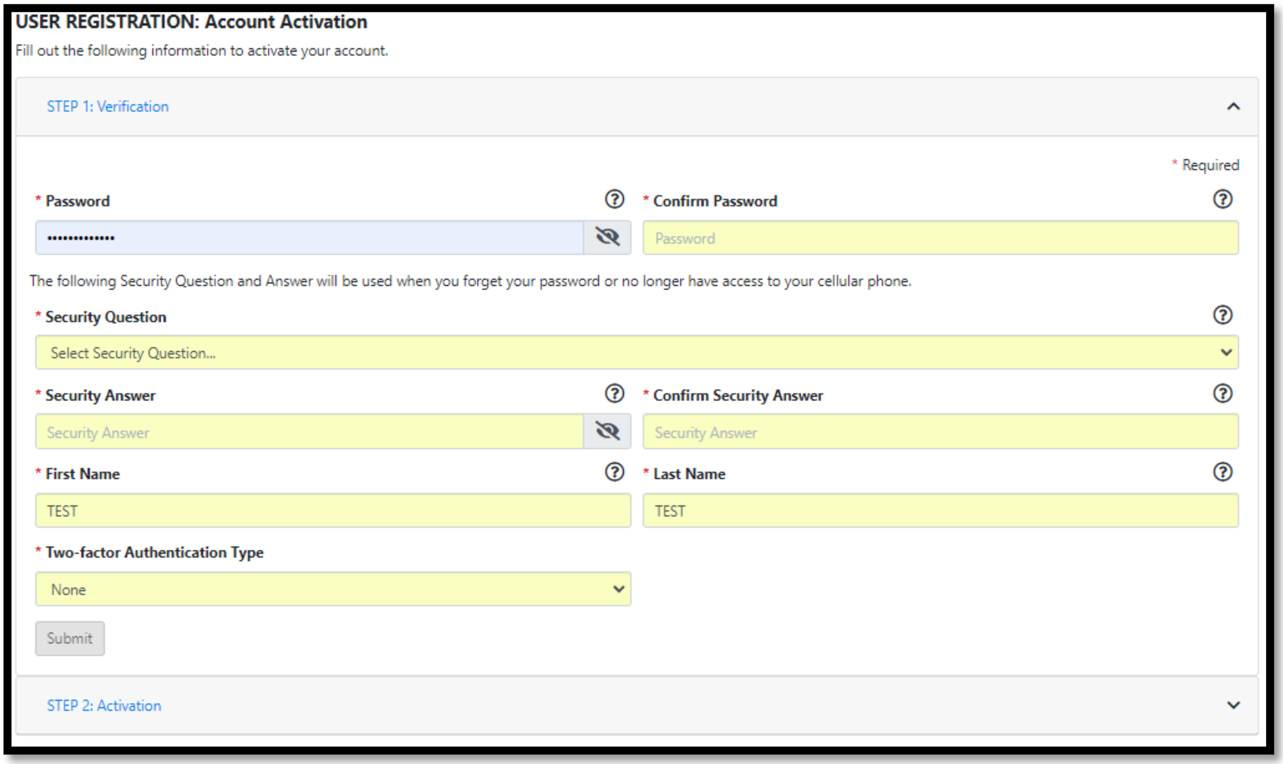
If you have any questions, please email us at CAU@NIGC.GOV.

***** This is a system generated email. Please do not reply. *****

Sincerely,
NIGC Support Team

Account Activation

Once the link is accessed, the image below will appear.



USER REGISTRATION: Account Activation

Fill out the following information to activate your account.

STEP 1: Verification

* Required

* **Password**: ••••••••••••••

* **Confirm Password**: Password

The following Security Question and Answer will be used when you forget your password or no longer have access to your cellular phone.

* **Security Question**: Select Security Question...

* **Security Answer**: Security Answer

* **Confirm Security Answer**: Security Answer

* **First Name**: TEST

* **Last Name**: TEST

* **Two-factor Authentication Type**: None

STEP 2: Activation

Password & Confirm Password

1. Must be at least 8 characters long.
2. Must contain at least 1 alphanumeric character (a letter or number)
3. Must contain at least 1 special character.
4. Cannot contain whitespace.
5. Cannot be the user's email address.

Security Question, Security Answer & Confirm Security Answer

These fields will be used if the user needs to reset their own password. They will need to verify **both** their Security Question **and** Answer in order to reset their password.

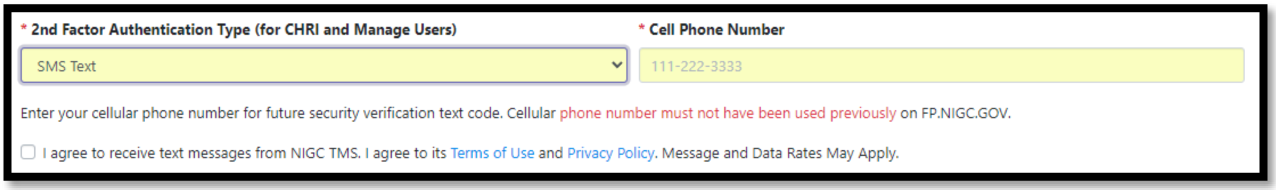
First & Last Names

1. Will be auto filled from the user's data.
2. This is an opportunity to correct any mistakes in their names.

Two-Factor Authentication Type

1. This will only appear if Two-Factor Authentication was enabled during the "Add User" step.
2. This is the method they will use to receive an access code during login.
3. There are 3 options available: SMS Text, Key FOB, and Authenticator App.
4. Each option requires a step to register the authentication method.

Two-Factor Authentication Type - SMS Text



* 2nd Factor Authentication Type (for CHRI and Manage Users)

SMS Text

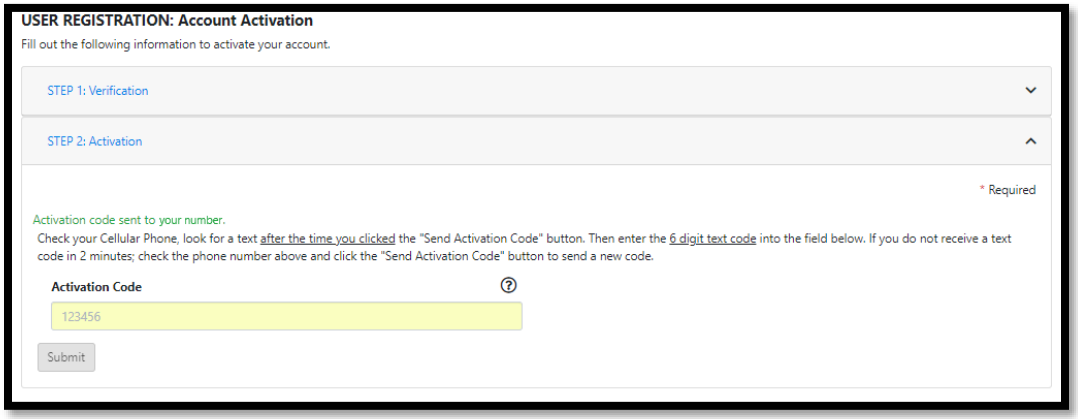
* Cell Phone Number

111-222-3333

Enter your cellular phone number for future security verification text code. Cellular phone number must not have been used previously on FP.NIGC.GOV.

□ I agree to receive text messages from NIGC TMS. I agree to its Terms of Use and Privacy Policy. Message and Data Rates May Apply.

If **Step 1: Verification** was submitted successfully, **Step 2: Activation** will expand, where the user can enter the access code, they receive via SMS Text. The code will be given as a 6-digit code that will expire after 5 minutes. Enter that code under Activation Code.



USER REGISTRATION: Account Activation

Fill out the following information to activate your account.

STEP 1: Verification

STEP 2: Activation

* Required

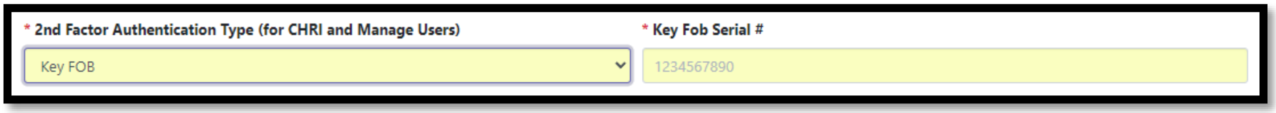
Activation code sent to your number.

Check your Cellular Phone, look for a text after the time you clicked the "Send Activation Code" button. Then enter the 6 digit text code into the field below. If you do not receive a text code in 2 minutes; check the phone number above and click the "Send Activation Code" button to send a new code.

Activation Code

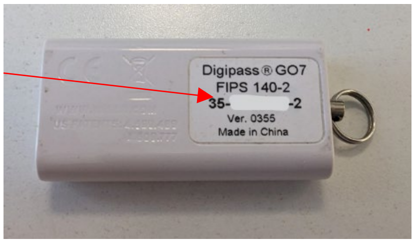
123456

Two-Factor Authentication Type – Key Fob



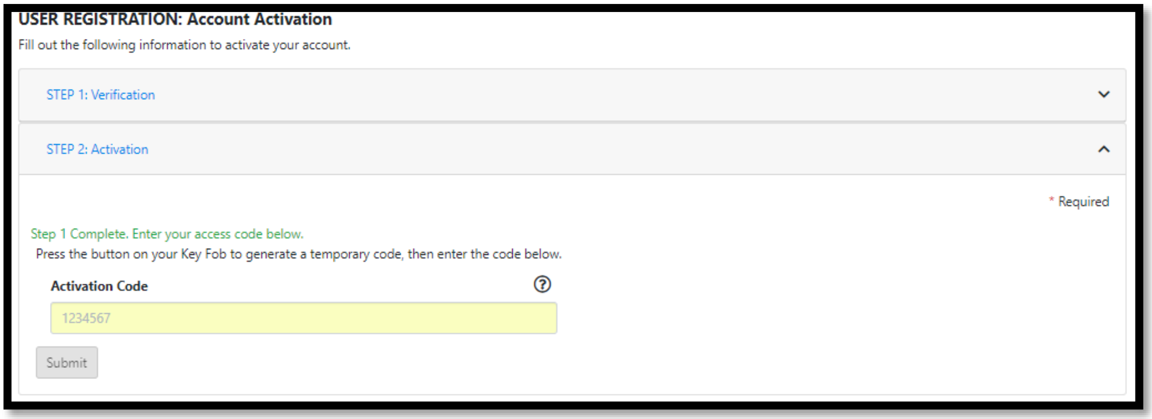
* 2nd Factor Authentication Type (for CHRI and Manage Users): Key FOB

* Key Fob Serial #: 1234567890



The Key Fob Serial# can be found on the back of the device in the row indicated by the red arrow. Enter the entire 10-digit number and exclude the dashes. Once finished filling out all required information, click Add to save the user.

If **Step 1: Verification** was submitted successfully, **Step 2: Activation** will expand, where the user can enter the access code, they receive via DigiPass. To access code, flip the device to the front and press the button to generate the code. Enter that code under Activation Code.



USER REGISTRATION: Account Activation

Fill out the following information to activate your account.

STEP 1: Verification

STEP 2: Activation

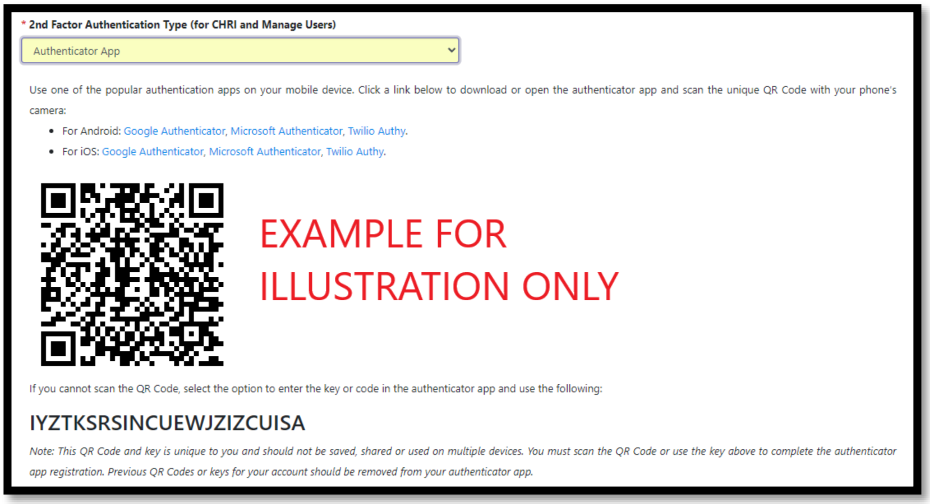
* Required

Step 1 Complete. Enter your access code below.

Press the button on your Key Fob to generate a temporary code, then enter the code below.

Activation Code: 1234567

Two-Factor Authentication Type – Authenticator App



* 2nd Factor Authentication Type (for CHRI and Manage Users): Authenticator App

Use one of the popular authentication apps on your mobile device. Click a link below to download or open the authenticator app and scan the unique QR Code with your phone's camera:

- For Android: Google Authenticator, Microsoft Authenticator, Twilio Authy.
- For iOS: Google Authenticator, Microsoft Authenticator, Twilio Authy.

EXAMPLE FOR ILLUSTRATION ONLY

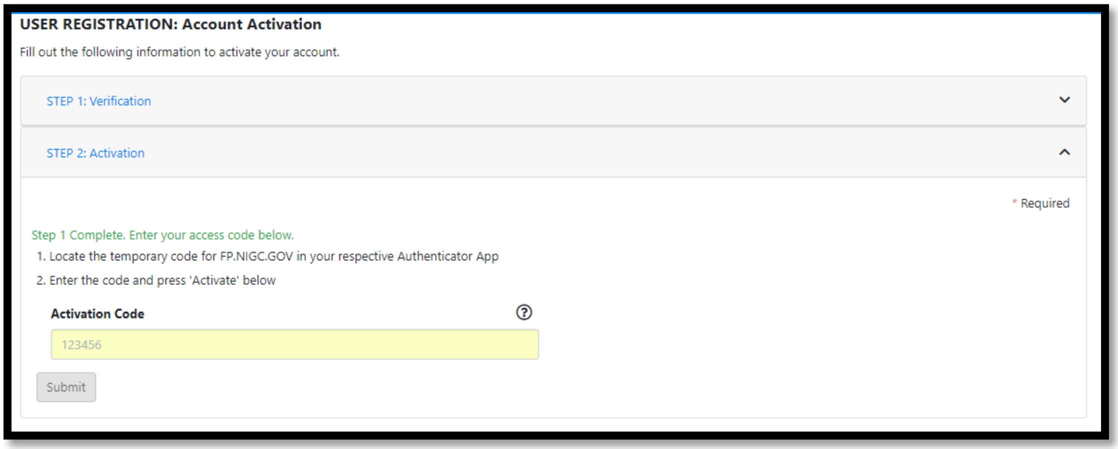
If you cannot scan the QR Code, select the option to enter the key or code in the authenticator app and use the following:

IYZTKSRSINCUEWJZIZCUISA

Note: This QR Code and key is unique to you and should not be saved, shared or used on multiple devices. You must scan the QR Code or use the key above to complete the authenticator app registration. Previous QR Codes or keys for your account should be removed from your authenticator app.

Note: If the user accidentally refreshes the page a new QR code will be generated, so they will have to remove any previous accounts from their Authenticator App and rescan the new QR code.

If **Step 1: Verification** was submitted successfully, **Step 2: Activation** will expand, where the user can enter the access code, they receive via Authenticator App.



USER REGISTRATION: Account Activation

Fill out the following information to activate your account.

STEP 1: Verification

STEP 2: Activation

* Required

Step 1 Complete. Enter your access code below.

1. Locate the temporary code for FP.NIGC.GOV in your respective Authenticator App
2. Enter the code and press 'Activate' below

Activation Code

123456

Edit Users:

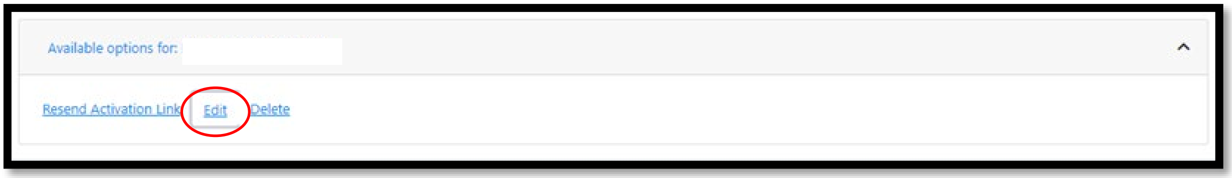
For Admins:

Editing a user in an agency only allows Agency Admin user to edit.

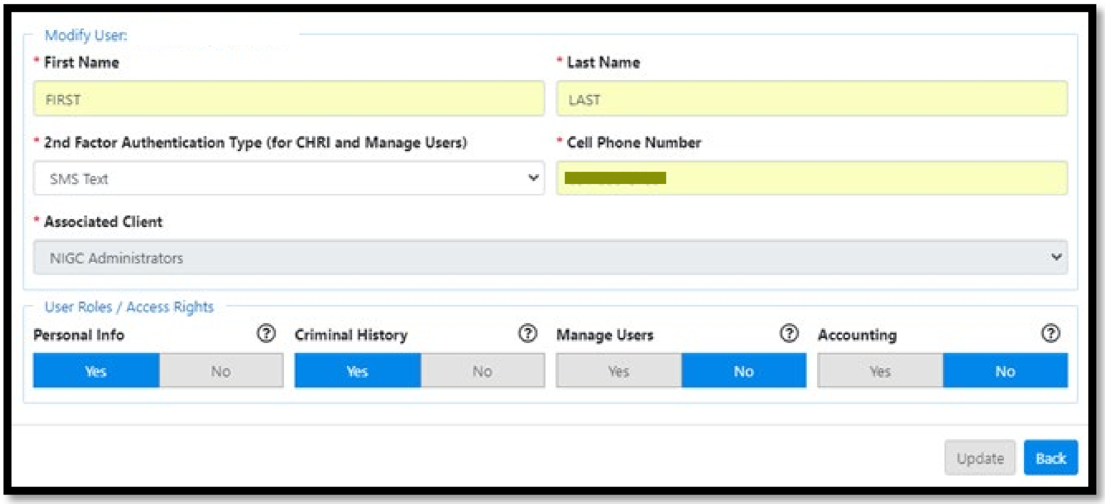
1. First and Last Name
2. 2 Factor Authentication
3. User Roles / Access Rights

There are two examples where you can edit a user.

Edit Pop up During Activation (User account has not been activated)



Available options for:



Modify User:

* First Name	* Last Name
FIRST	LAST
* 2nd Factor Authentication Type (for CHRI and Manage Users)	* Cell Phone Number
SMS Text	[redacted]
* Associated Client	
NIGC Administrators	

User Roles / Access Rights

Personal Info	Criminal History	Manage Users	Accounting
[✓ Yes] No	[✓ Yes] No	Yes [✓ No]	Yes [✓ No]

First and Last Names

The respective names of the user

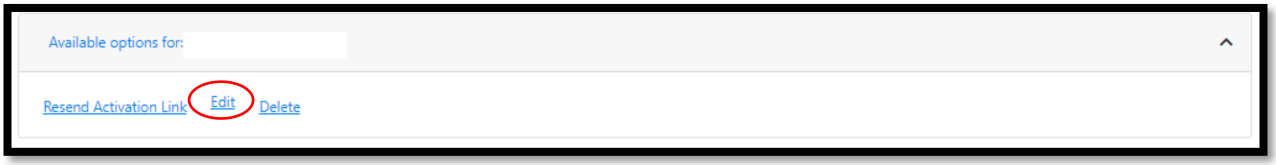
1. If the user account already exists, their existing names are used when addressing the user in the Activation email.

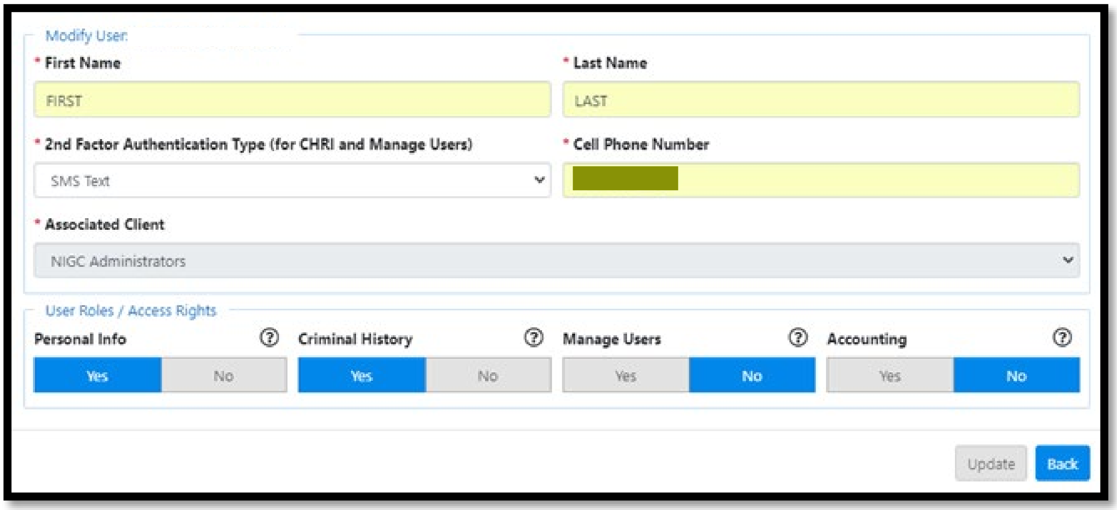
Enable Two-Factor Authentication

Whether the user is required to use a second method of authentication during login

1. This option is initially enabled by default if your agency requires Two-Factor Authentication for all record types.
2. The toggle will automatically be set to **Yes** if the **Criminal History** or **Manage Users** roles are enabled.

Edit Pop up for Existing User (user account has been activated)





Modify User

* First Name: FIRST

* Last Name: LAST

* 2nd Factor Authentication Type (for CHRI and Manage Users): SMS Text

* Cell Phone Number: [redacted]

* Associated Client: NIGC Administrators

User Roles / Access Rights

Personal Info	Criminal History	Manage Users	Accounting
[✓ Yes] No	[✓ Yes] No	Yes [✓ No]	Yes [✓ No]

First & Last Names

1. Will be auto filled from the user's data.
2. This is an opportunity to correct any mistakes in their names.

Two-Factor Authentication Type

1. This will only appear if Two-Factor Authentication was enabled during the "Add User" step.
2. This is the method they will use to receive an access code during login.
3. There are 4 options available: None, SMS Text, Key FOB, and Authenticator App
    a. NOTE: Selecting 'None' will disable Two Factor Authentication. To have a successful edit, Criminal History and Manage Users Roles need to be removed. NIGC does not recommend doing this.
4. Each option requires a step to register the authentication method.

<u>Changing the user's Authentication Type</u>

Our system supports three types of Two-Factor Authentication: SMS Text, Key FOB, and Authenticator App. When changing a user's authentication type, you can only switch a user to SMS Text or Key FOB. This is because both of these methods allow the admin user to enter the associated configuration. SMS Text requires a phone number and Key FOB requires the serial number of the FOB. Because the Authenticator App requires a user to install an app and configure the app themselves, this authentication method **cannot be configured by the Agency Admin user**.

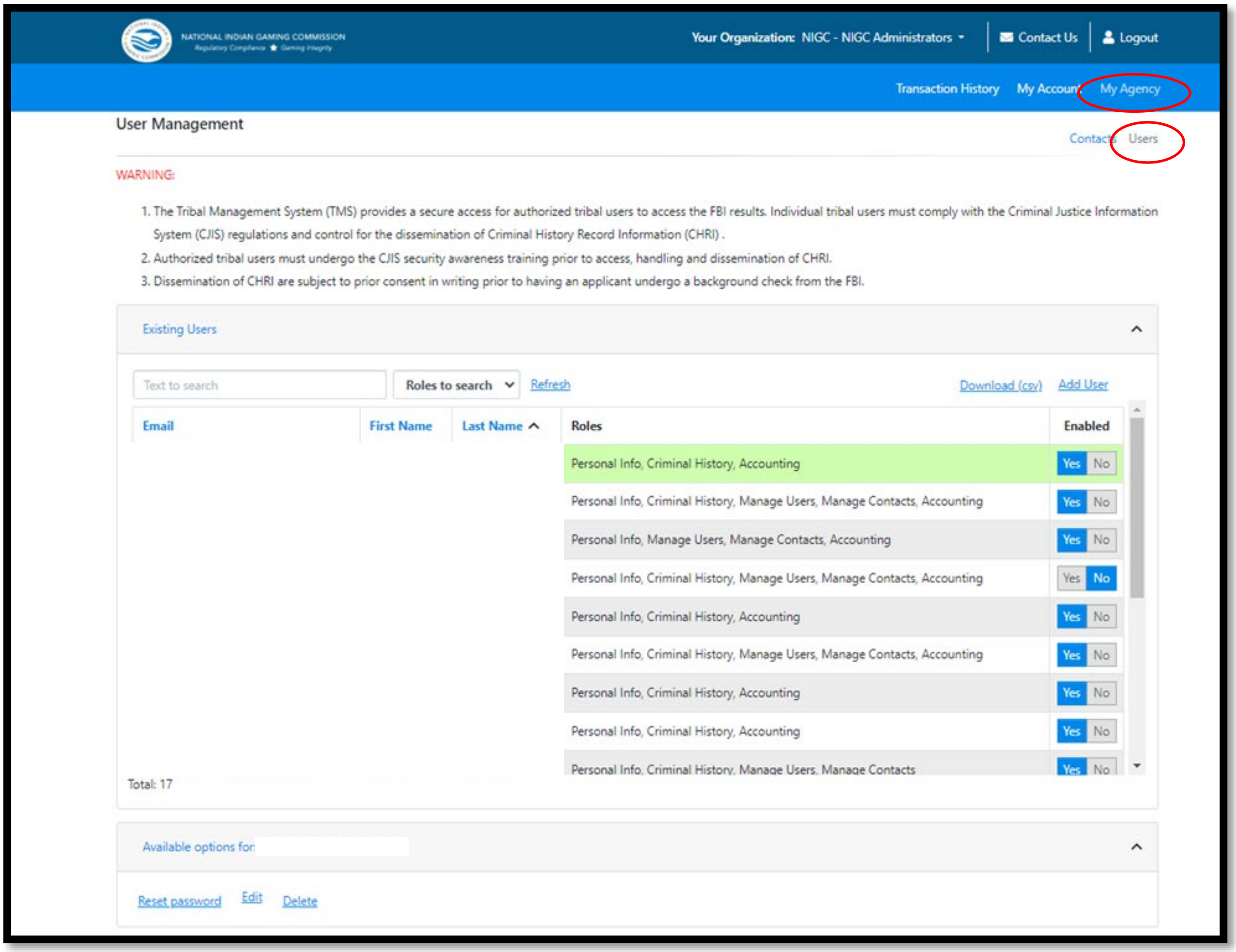
Reset Password:

There are two steps to reset a user's password. First, a password reset must be triggered. This will send the user an email with an expiring single-use link. The link expires 10 minutes from when the password reset is triggered. Second, the user clicks on the link and fills out the web form to complete the password reset.

For Admins:

This action can be accessed through the Admin Portal by a user with appropriate privileges.

To access the User Management page, navigate to the "My Agency Tab" then to "Users" as seen below.



User Management

WARNING:

1. The Tribal Management System (TMS) provides a secure access for authorized tribal users to access the FBI results. Individual tribal users must comply with the Criminal Justice Information System (CJIS) regulations and control for the dissemination of Criminal History Record Information (CHRI) .
2. Authorized tribal users must undergo the CJIS security awareness training prior to access, handling and dissemination of CHRI.
3. Dissemination of CHRI are subject to prior consent in writing prior to having an applicant undergo a background check from the FBI.

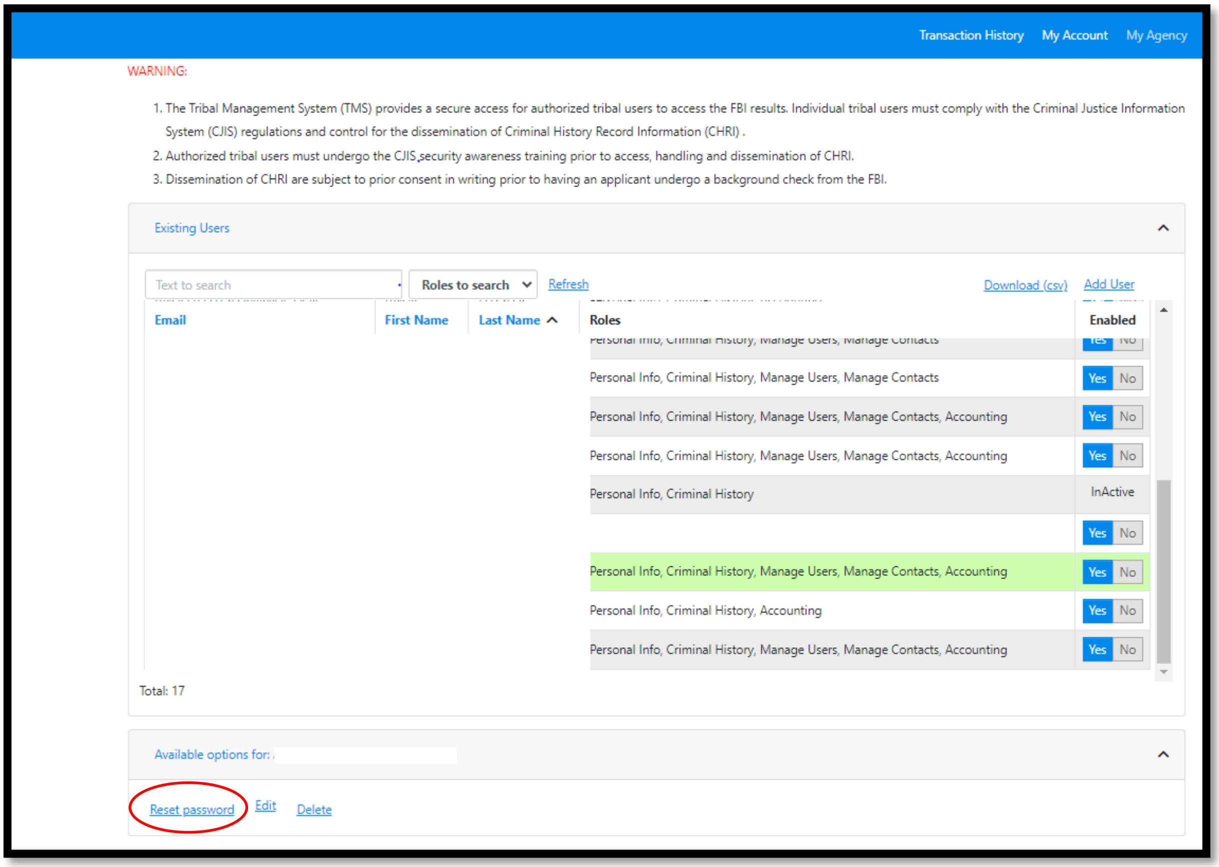
Existing Users

Email	First Name	Last Name	Roles	Enabled
			Personal Info, Criminal History, Accounting	[✓ Yes] No
			Personal Info, Criminal History, Manage Users, Manage Contacts, Accounting	[✓ Yes] No
			Personal Info, Manage Users, Manage Contacts, Accounting	[✓ Yes] No
			Personal Info, Criminal History, Manage Users, Manage Contacts, Accounting	Yes [✓ No]
			Personal Info, Criminal History, Accounting	[✓ Yes] No
			Personal Info, Criminal History, Manage Users, Manage Contacts, Accounting	[✓ Yes] No
			Personal Info, Criminal History, Accounting	[✓ Yes] No
			Personal Info, Criminal History, Accounting	[✓ Yes] No
			Personal Info, Criminal History, Manage Users, Manage Contacts	[✓ Yes] No

Total: 17

Available options for:

Select desired user, once selected available options for that user will appear at the bottom of the page as seen below. Click “Reset Password” to reset desired user’s password.



WARNING:

1. The Tribal Management System (TMS) provides a secure access for authorized tribal users to access the FBI results. Individual tribal users must comply with the Criminal Justice Information System (CJIS) regulations and control for the dissemination of Criminal History Record Information (CHRI) .
2. Authorized tribal users must undergo the CJIS security awareness training prior to access, handling and dissemination of CHRI.
3. Dissemination of CHRI are subject to prior consent in writing prior to having an applicant undergo a background check from the FBI.

Existing Users

Email	First Name	Last Name	Roles	Enabled
			Personal Info, Criminal History, Manage Users, Manage Contacts	Yes No
			Personal Info, Criminal History, Manage Users, Manage Contacts	Yes No
			Personal Info, Criminal History, Manage Users, Manage Contacts, Accounting	Yes No
			Personal Info, Criminal History, Manage Users, Manage Contacts, Accounting	Yes No
			Personal Info, Criminal History	InActive
				Yes No
			Personal Info, Criminal History, Manage Users, Manage Contacts, Accounting	Yes No
			Personal Info, Criminal History, Accounting	Yes No
			Personal Info, Criminal History, Manage Users, Manage Contacts, Accounting	Yes No

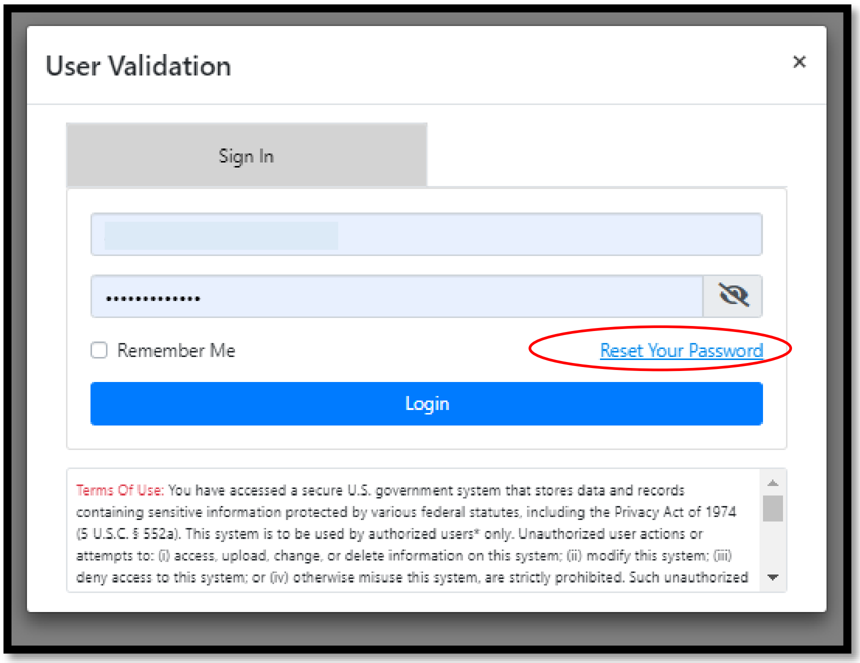
Total: 17

Available options for:

Once triggered, the user will receive an email with a link to reset their password.

For Users:

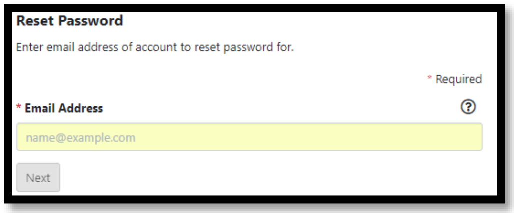
Via Login Dialogue Users can trigger a password reset by clicking the link on the login dialogue. Navigate to the login page and click on "Reset Your Password" as seen below.



User Validation

Terms Of Use: You have accessed a secure U.S. government system that stores data and records containing sensitive information protected by various federal statutes, including the Privacy Act of 1974 (5 U.S.C. § 552a). This system is to be used by authorized users* only. Unauthorized user actions or attempts to: (i) access, upload, change, or delete information on this system; (ii) modify this system; (iii) deny access to this system; or (iv) otherwise misuse this system, are strictly prohibited. Such unauthorized

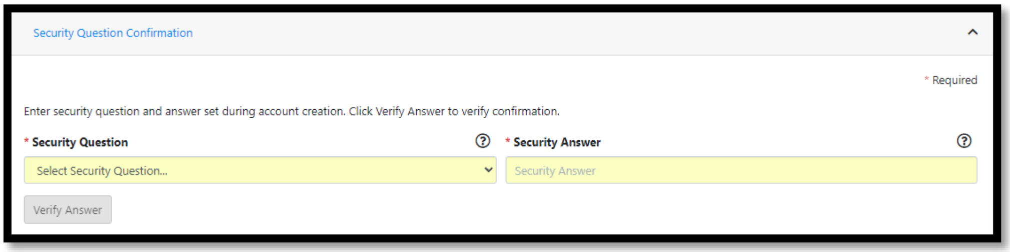
Once clicked this page will be shown, enter in the email address that is associated to the desired user to have their password reset.



Reset Password

Enter email address of account to reset password for.

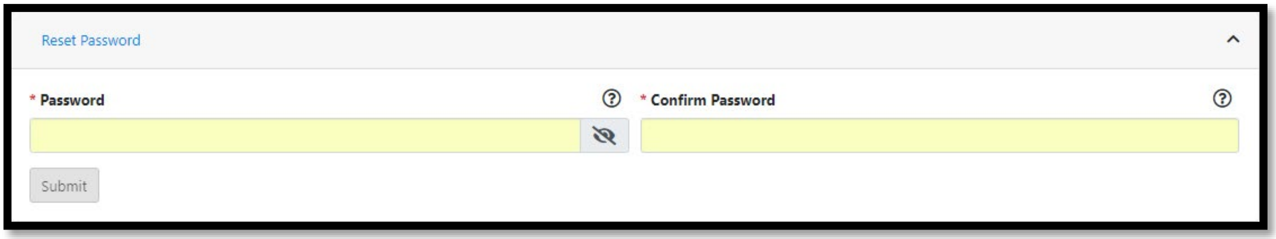
Once email is entered, please select the security question that is associated to the desired user and enter in the Security Answer. **Both** security question **and** answer must be correct to trigger the password reset email. If the question selected or the answer entered for the correct question are incorrect, no email will be sent.



Security Question Confirmation

Enter security question and answer set during account creation. Click Verify Answer to verify confirmation.

Once the link is accessed, reset your password.



a. This link will expire 10 minutes after the password reset was triggered.
b. Users must **access** the link before it expires, however they can submit the password reset form even after the link has expired.
c. Refreshing the page will check if the link has expired, so we recommend not refreshing the page once the user has accessed the link.

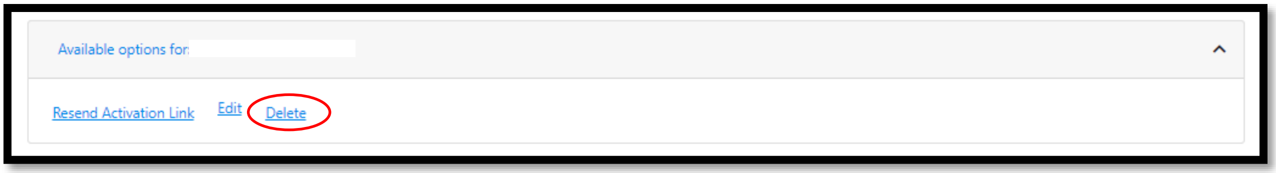
If the link expires before the user accesses the form or they have already completed the password reset, they will be redirected to the login page with a message that their link is invalid.

Delete Users:

For Admins:

There are two ways to remove the desired user.

1. Via Agency Admin User



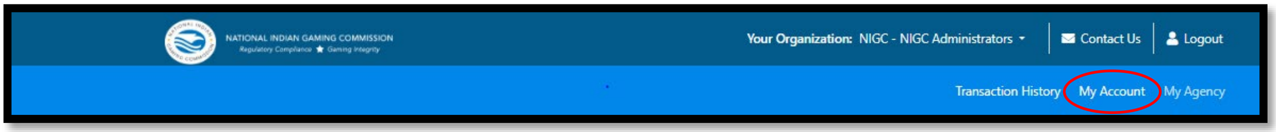
When clicking on "Delete" or "Delete User" after selecting a desired user, a confirmation window will ask you to confirm if you wish to remove the user. If so, confirm the deletion, or else cancel.

NOTE: There is no way of reverting back after deleting a user, please proceed with caution when deleting

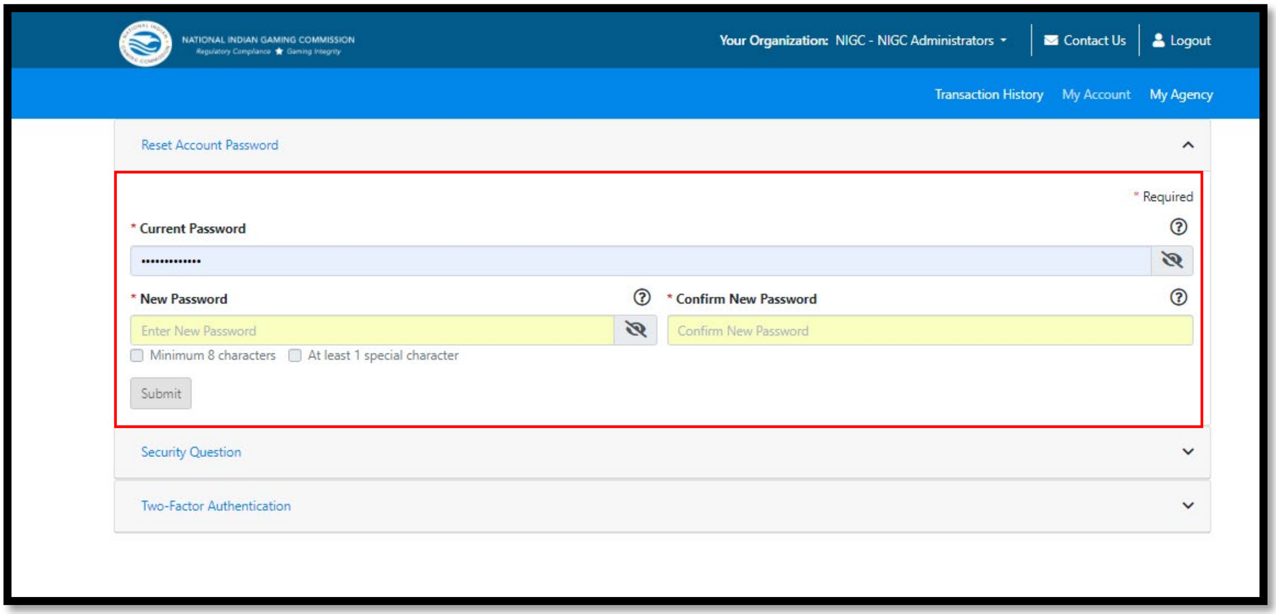
For Users:

My Account

The My Account Tab allows users to update their own password, security question, and their authentication type when logged in. To access your Account Information, navigate to the "My Account" as seen below.


NATIONAL INDIAN GAMING COMMISSION
Regulatory Compliance ★ Gaming Integrity
Your Organization: NIGC - NIGC Administrators
Contact Us
Logout
Transaction History
My Account
My Agency

Reset Account Password


NATIONAL INDIAN GAMING COMMISSION
Regulatory Compliance ★ Gaming Integrity
Your Organization: NIGC - NIGC Administrators
Contact Us
Logout
Transaction History
My Account
My Agency
Reset Account Password
Submit
Security Question
Two-Factor Authentication

* Required

* Current Password: ••••••••••••

* New Password: Enter New Password

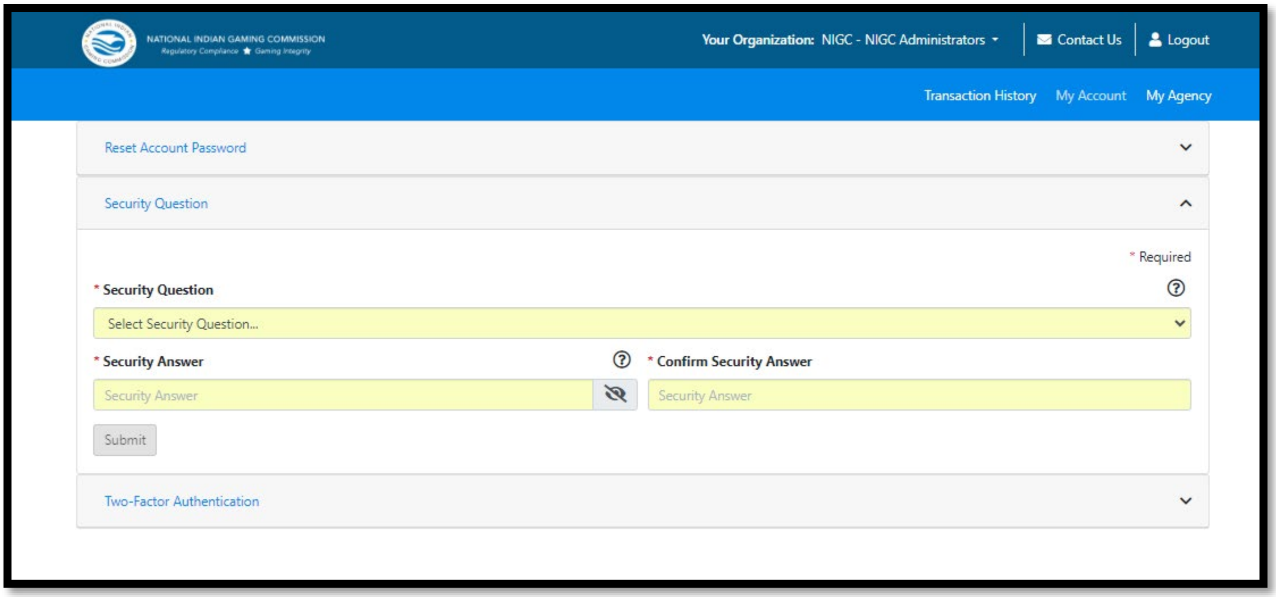
* Confirm New Password: Confirm New Password

□ Minimum 8 characters □ At least 1 special character

The first section of the "My Account" Tab is "Reset Account Password" To expand the tab click on the drop-down arrow on the left side of "Reset Account Password" as seen above. The user can update their password for their account. The user must enter the current password then the new password.

NOTE: The system will retain 10 of the most recent passwords when changed. These passwords are retained from a password expiring, a password reset, or a password update.

Security Question

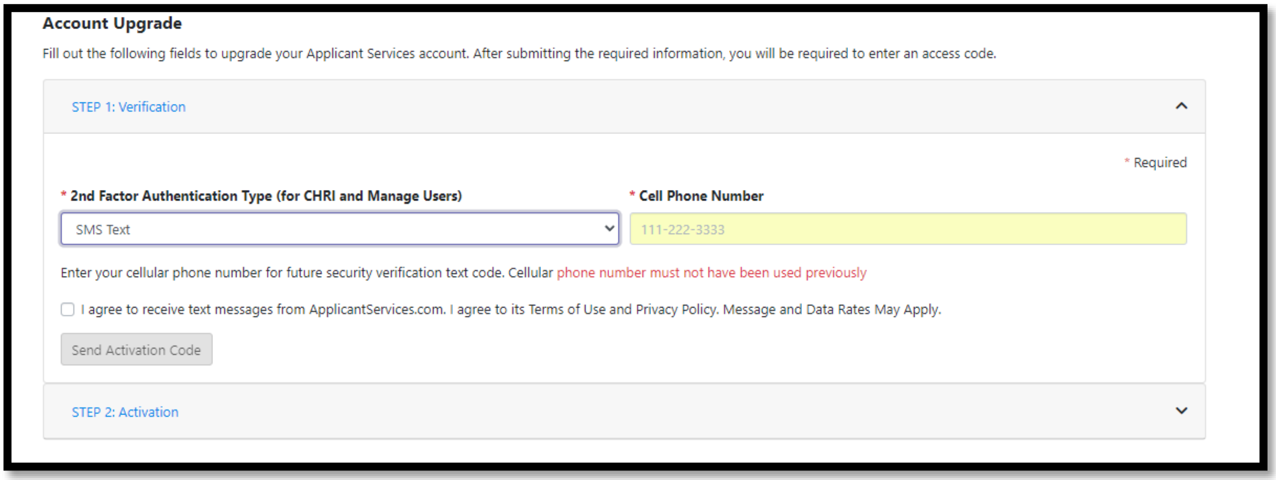

NATIONAL INDIAN GAMING COMMISSION
Regulatory Compliance ★ Gaming Integrity
Your Organization: NIGC - NIGC Administrators
Contact Us
Logout
Transaction History
My Account
My Agency
Reset Account Password
Security Question
* Required
* Security Question
Select Security Question...
* Security Answer
* Confirm Security Answer
Security Answer
Security Answer
Submit
Two-Factor Authentication

The second section of the "My Account" Tab is the "Security Question". To expand the tab, click on the drop-down arrow on the left side of "Security Question" as seen above. The user can update their own Security Question and Answer. These fields will be used if the user needs to reset their own password.

Account Upgrade

This section will appear if the account does not have Two-Factor Authentication. After reading through Privacy & Security Statements, Cookies and Session IDs, Links, and Data Security click 'Agree' to go to the page below. Continue to configure the Two-Factor Authentication for the user's account.

NOTE: When upgrading the user account to Two-Factor Authentication will not change the roles of the user to have Criminal History or Manage Users. If the user wants these roles, the user will need to contact an Agency Admin User of the user's associated Agency to edit those roles to be enabled.



Account Upgrade

Fill out the following fields to upgrade your Applicant Services account. After submitting the required information, you will be required to enter an access code.

STEP 1: Verification

* Required

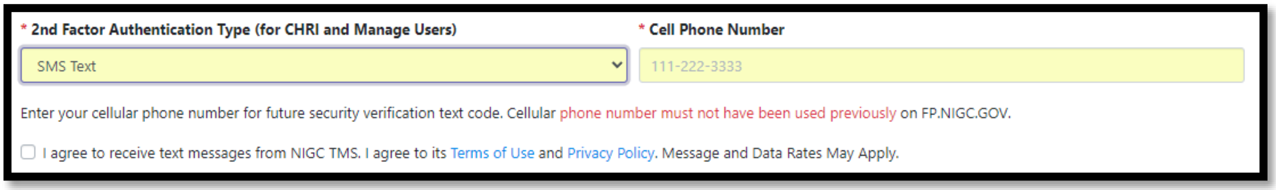
* 2nd Factor Authentication Type (for CHRI and Manage Users): SMS Text

* Cell Phone Number: 111-222-3333

Enter your cellular phone number for future security verification text code. Cellular phone number must not have been used previously

□ I agree to receive text messages from ApplicantServices.com. I agree to its Terms of Use and Privacy Policy. Message and Data Rates May Apply.

Two-Factor Authentication Type - SMS Text



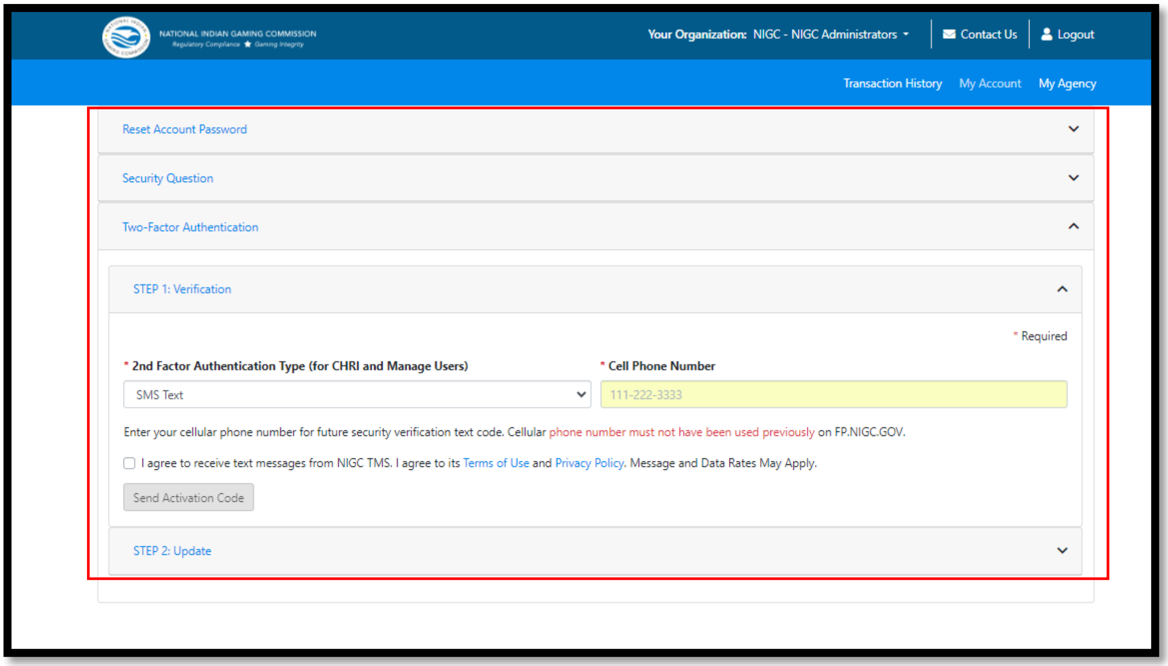
* 2nd Factor Authentication Type (for CHRI and Manage Users): SMS Text

* Cell Phone Number: 111-222-3333

Enter your cellular phone number for future security verification text code. Cellular phone number must not have been used previously on FP.NIGC.GOV.

□ I agree to receive text messages from NIGC TMS. I agree to its Terms of Use and Privacy Policy. Message and Data Rates May Apply.

If **Step 1: Verification** was submitted successfully, **Step 2: Activation** will expand, where the user can enter the access code, they receive via SMSText. The code will be given as a 6-digit code that will expire after 5 minutes. Enter that code under Activation Code.



Your Organization: NIGC - NIGC Administrators

* Required

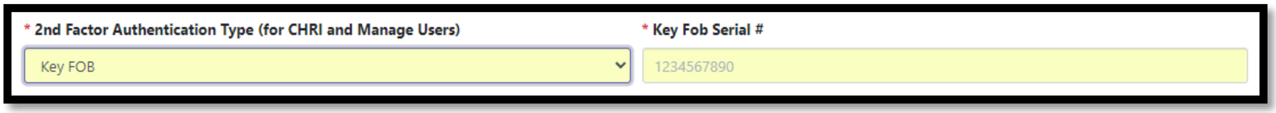
* 2nd Factor Authentication Type (for CHRI and Manage Users): SMS Text

* Cell Phone Number: 111-222-3333

Enter your cellular phone number for future security verification text code. Cellular phone number must not have been used previously on FP.NIGC.GOV.

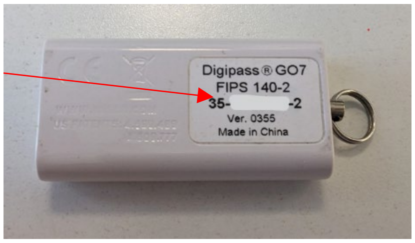
□ I agree to receive text messages from NIGC TMS. I agree to its Terms of Use and Privacy Policy. Message and Data Rates May Apply.

Two-Factor Authentication Type – Key Fob



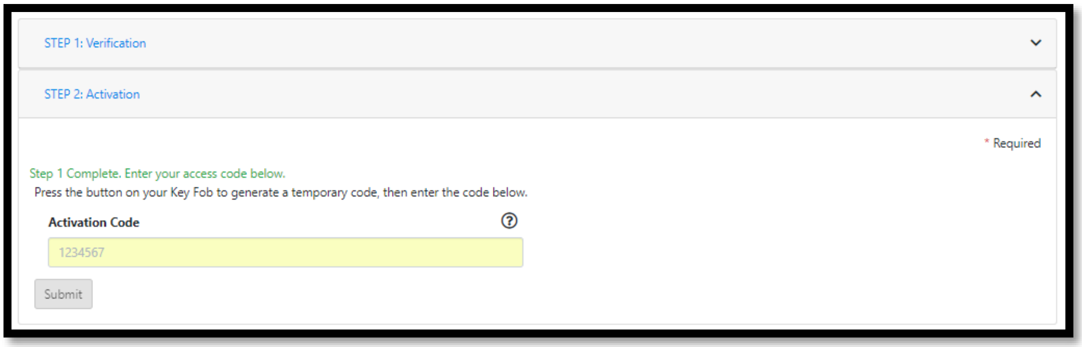
* 2nd Factor Authentication Type (for CHRI and Manage Users): Key FOB

* Key Fob Serial #: 1234567890



The Key Fob Serial# can be found on the back of the device in the row indicated by the red arrow. Enter the entire 10 digit number and exclude the dashes. Once finished filling out all required information, click Add to save the user.

If **Step 1: Verification** was submitted successfully, **Step 2: Activation** will expand, where the user can enter the access code, they receive via DigiPass. To access code, flip the device to the front and press the button to generate the code. Enter that code under Activation Code.



STEP 1: Verification

STEP 2: Activation

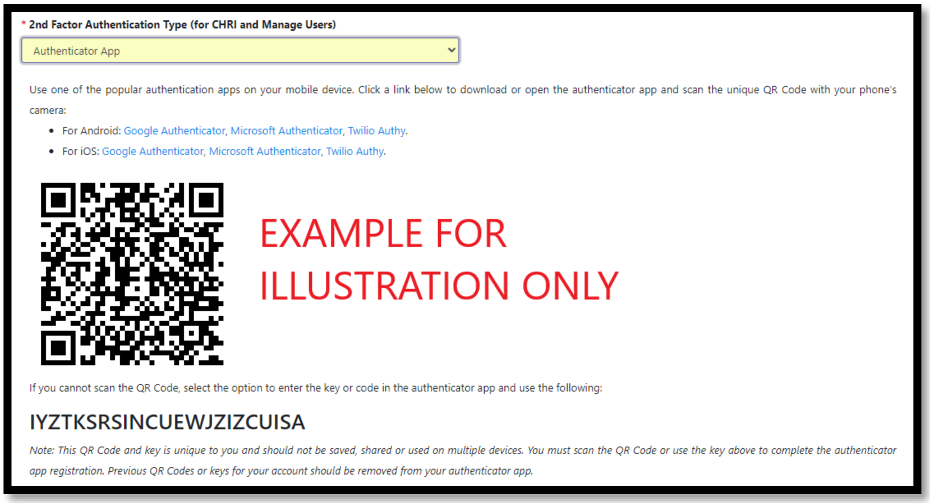
* Required

Step 1 Complete. Enter your access code below.

Press the button on your Key Fob to generate a temporary code, then enter the code below.

Activation Code: 1234567

Two-Factor Authentication Type – Authenticator App



* 2nd Factor Authentication Type (for CHRI and Manage Users): Authenticator App

Use one of the popular authentication apps on your mobile device. Click a link below to download or open the authenticator app and scan the unique QR Code with your phone's camera:

- For Android: Google Authenticator, Microsoft Authenticator, Twilio Authy.
- For iOS: Google Authenticator, Microsoft Authenticator, Twilio Authy.

EXAMPLE FOR ILLUSTRATION ONLY

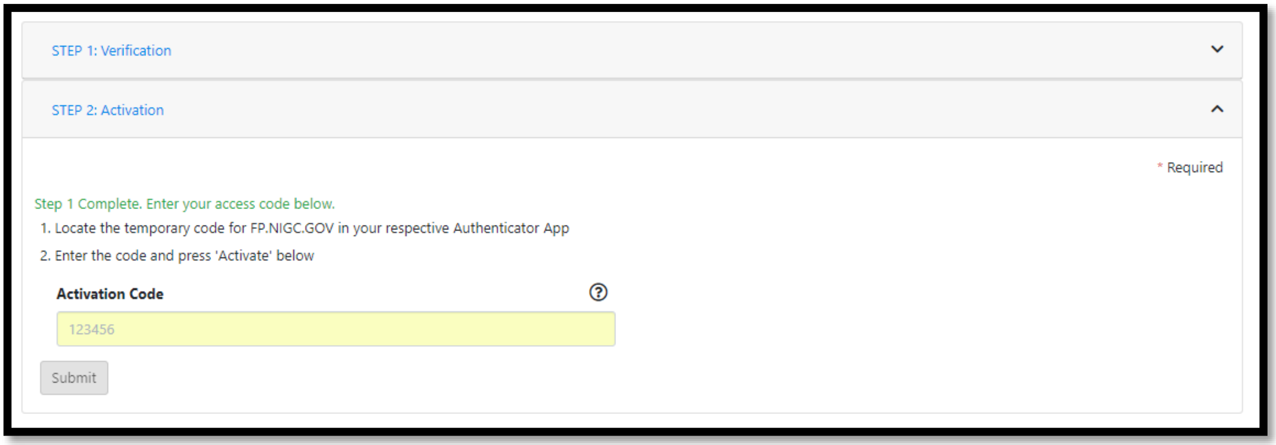
If you cannot scan the QR Code, select the option to enter the key or code in the authenticator app and use the following:

IYZTKSRSINCUEWJZIZCUISA

Note: This QR Code and key is unique to you and should not be saved, shared or used on multiple devices. You must scan the QR Code or use the key above to complete the authenticator app registration. Previous QR Codes or keys for your account should be removed from your authenticator app.

Note: If the user accidentally refreshes the page a new QR code will be generated, so they will have to remove any previous accounts from their Authenticator App and rescan the new QR code.

If **Step 1: Verification** was submitted successfully, **Step 2: Activation** will expand, where the user can enter the access code, they receive via Authenticator App.



Step 1 Complete. Enter your access code below.

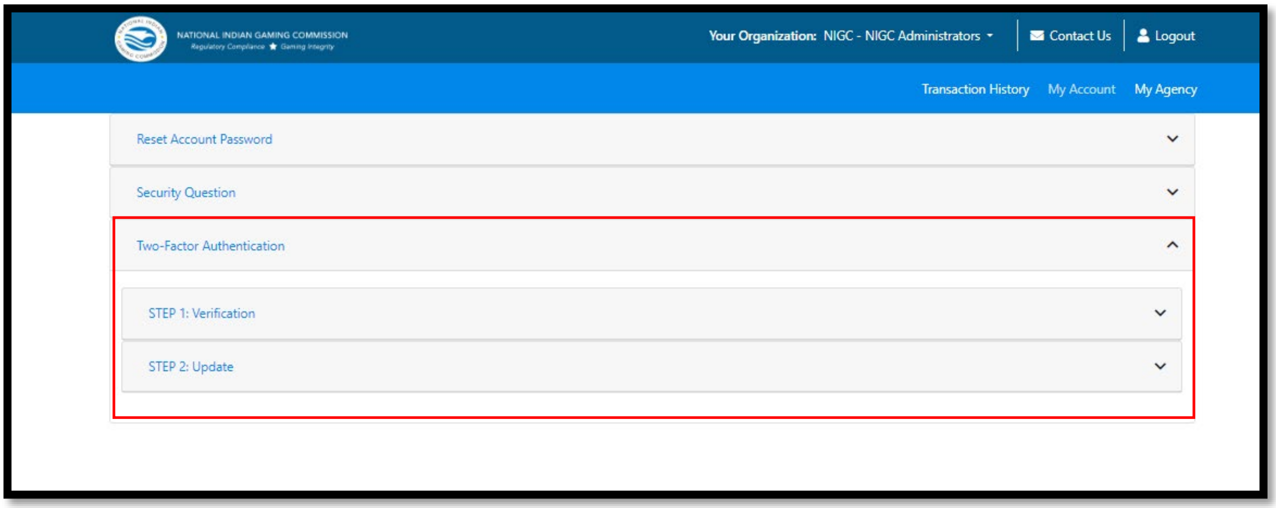
1. Locate the temporary code for FP.NIGC.GOV in your respective Authenticator App
2. Enter the code and press 'Activate' below

Activation Code

123456

Two-Factor Authentication

This section will appear if the account does have Two-Factor Authentication.


NATIONAL INDIAN GAMING COMMISSION
Regulatory Compliance ★ Gaming Integrity
Your Organization: NIGC - NIGC Administrators
Contact Us
Logout
Transaction History
My Account
My Agency
Reset Account Password
Security Question
Two-Factor Authentication
STEP 1: Verification
STEP 2: Update

To expand the tab, click on the drop-down arrow on the left side of “Two-Factor Authentication” as seen above. The user can update their own Two-Factor Authentication. The user can either switch the Authentication Type or update information on their current Authentication. Continue to update the Two-Factor Authentication for the user’s account.