How To: Setting Up Multi-factor Authentication (MFA)

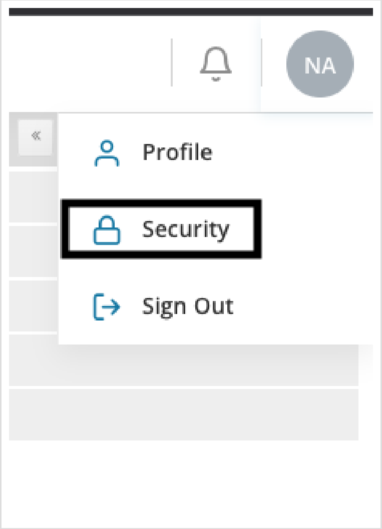
Last Modified on 03/26/2025 11:37 am EDT

Multi-Factor Authentication (MFA) adds an additional layer of security to your account beyond just a username and password for login. For Updox accounts with MFA enabled, this guide will provide the how-to steps for individual user MFA setup as well as account management settings for account holders.

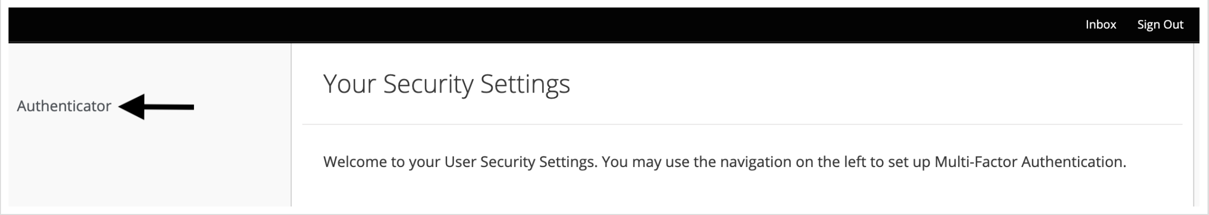
General User Setup

If it is enabled for your account, individual users can set up MFA even if the account does not require it.

1. Go to your profile in the upper right-hand corner of your account and select **Security.**



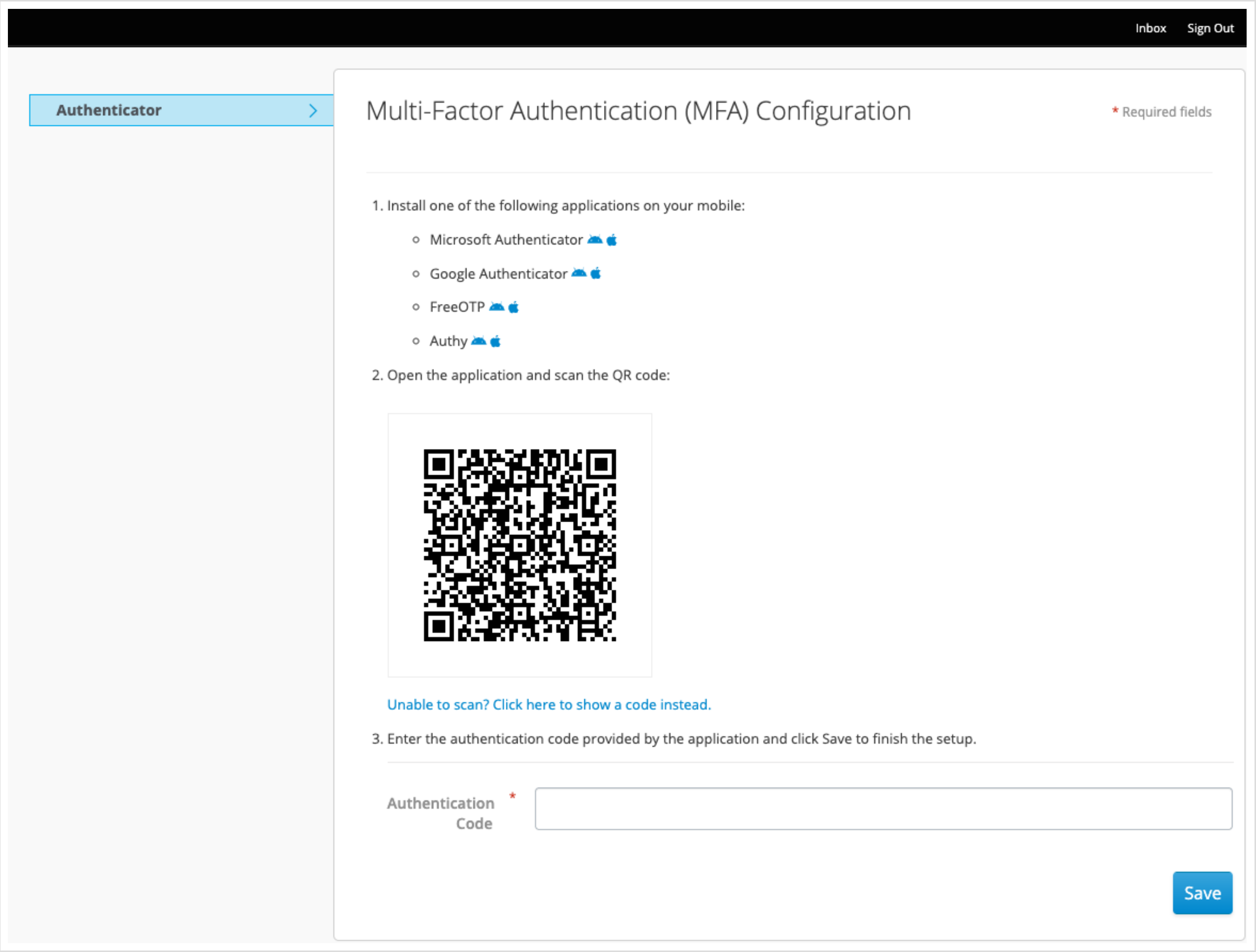
2. A new tab will open in your browser. Click on the **Authenticator** link.



Your Security Settings

Welcome to your User Security Settings. You may use the navigation on the left to set up Multi-Factor Authentication.

3. On the MFA Configuration page, you will be prompted to select an authenticator. Once you have one installed on your device, scan the QR code to proceed. You will need to enter the authentication code generated by the authenticator app you installed. Click **Save** when finished.



Inbox Sign Out

Authenticator

Multi-Factor Authentication (MFA) Configuration

* Required fields

1. Install one of the following applications on your mobile:
   - Microsoft Authenticator
   - Google Authenticator
   - FreeOTP
   - Authy
2. Open the application and scan the QR code:

Unable to scan? Click here to show a code instead.

3. Enter the authentication code provided by the application and click Save to finish the setup.

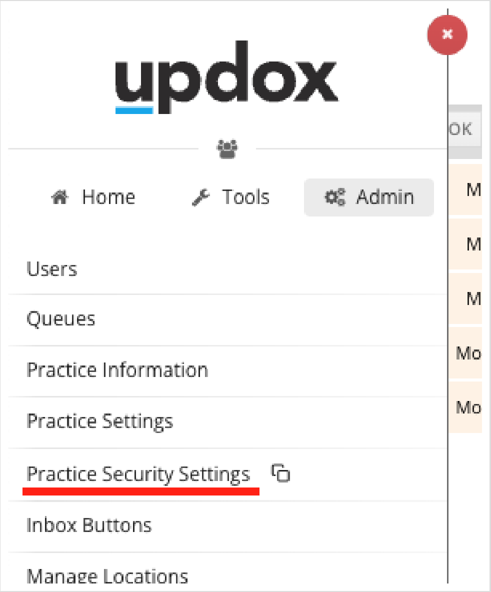
Authentication Code *

Save

Note: If you have your MFA reset, but your account doesn't require MFA, you will be able to log in directly without being prompted to set up a new one. If you want to set up MFA again, you will have to go through the above steps.

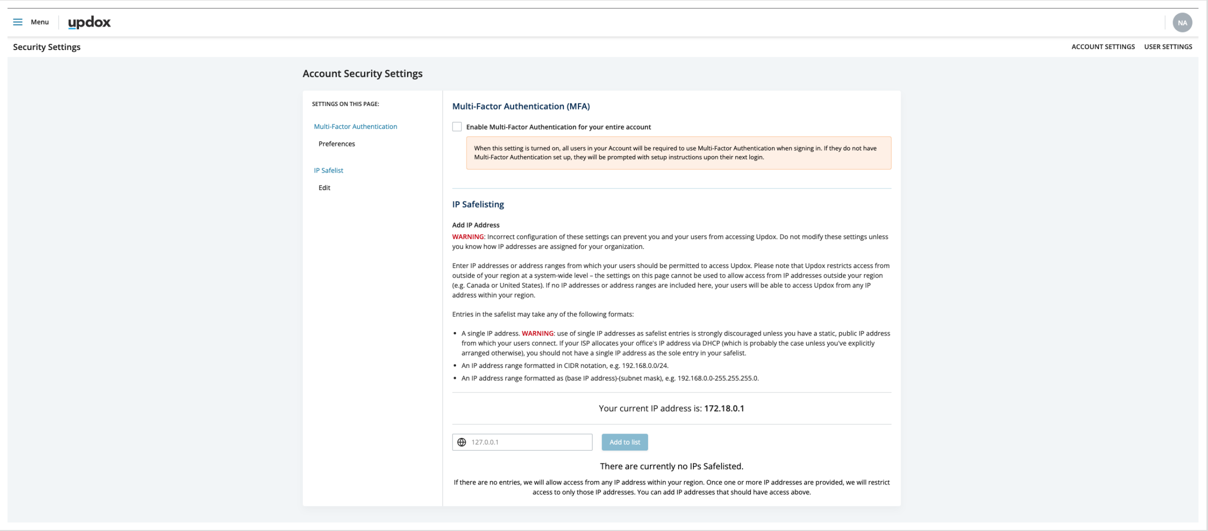
Enforcing MFA for All Users

1. Sign in to your Updox account. Under **Menu**, select **Admin** and click **Practice Security Settings**.



2. You will be taken to the Security Settings page for your account. Here you can manage multi-factor

authentication and the IP Safelist.



Security Settings

Account Security Settings

Multi-Factor Authentication (MFA)

□ Enable Multi-Factor Authentication for your entire account

When this setting is turned on, all users in your Account will be required to use Multi-Factor Authentication when signing in. If they do not have Multi-Factor Authentication set up, they will be prompted with setup instructions upon their next login.

IP Safelisting

Add IP Address

WARNING: Incorrect configuration of these settings can prevent you and your users from accessing Updox. Do not modify these settings unless you know how IP addresses are assigned for your organization.

Enter IP addresses or address ranges from which your users should be permitted to access Updox. Please note that Updox restricts access from outside of your region at a system-wide level – the settings on this page cannot be used to allow access from IP addresses outside your region (e.g. Canada or United States). If no IP addresses or address ranges are included here, your users will be able to access Updox from any IP address within your region.

Entries in the safelist may take any of the following formats:

- A single IP address. WARNING: use of single IP addresses as safelist entries is strongly discouraged unless you have a static, public IP address from which your users connect. If your ISP allocates your office's IP address via DHCP (which is probably the case unless you've explicitly arranged otherwise), you should not have a single IP address as the sole entry in your safelist.
- An IP address range formatted in CIDR notation, e.g. 192.168.0.0/24.
- An IP address range formatted as (base IP address)-(subnet mask), e.g. 192.168.0.0-255.255.255.0.

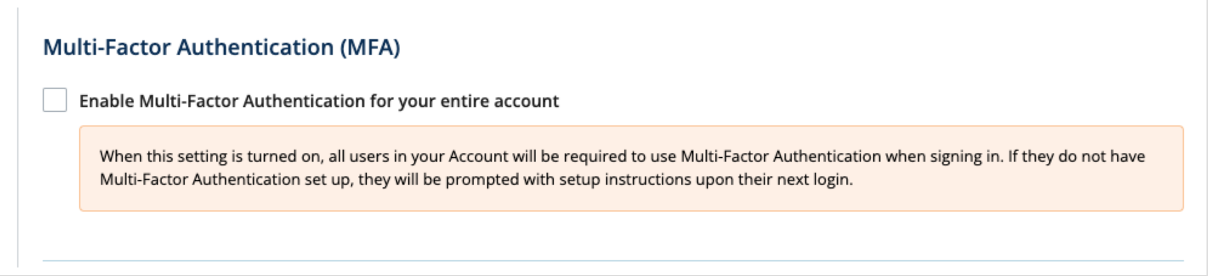
Your current IP address is: **172.18.0.1**

127.0.0.1

There are currently no IPs Safelisted.

If there are no entries, we will allow access from any IP address within your region. Once one or more IP addresses are provided, we will restrict access to only those IP addresses. You can add IP addresses that should have access above.

3. Check the box to enforce multi-factor authentication for **ALL** users of your account. Once MFA is enabled, **ALL** users will be required to set up and use MFA when accessing Updox. Otherwise, they will not be able to sign in.

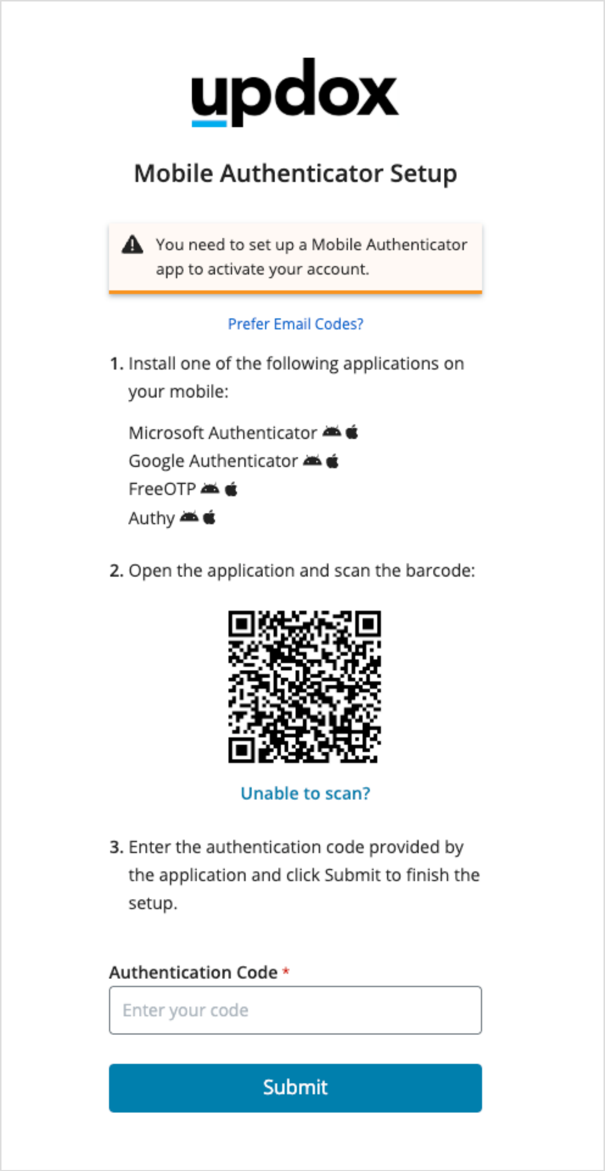


Multi-Factor Authentication (MFA)

□ Enable Multi-Factor Authentication for your entire account

When this setting is turned on, all users in your Account will be required to use Multi-Factor Authentication when signing in. If they do not have Multi-Factor Authentication set up, they will be prompted with setup instructions upon their next login.

4. After enabling MFA, account users will be prompted with a screen asking them to enable MFA the next time they login. The user will need to download one of the suggested apps, scan the QR code on their screen and follow the instructions to set up MFA on their device. Once the application setup is complete, enter the Authentication Code that it has generated on the setup page in Updox and click Submit.



Mobile Authenticator Setup

You need to set up a Mobile Authenticator app to activate your account.

Prefer Email Codes?

1. Install one of the following applications on your mobile:

   Microsoft Authenticator
   Google Authenticator
   FreeOTP
   Authy

2. Open the application and scan the barcode:

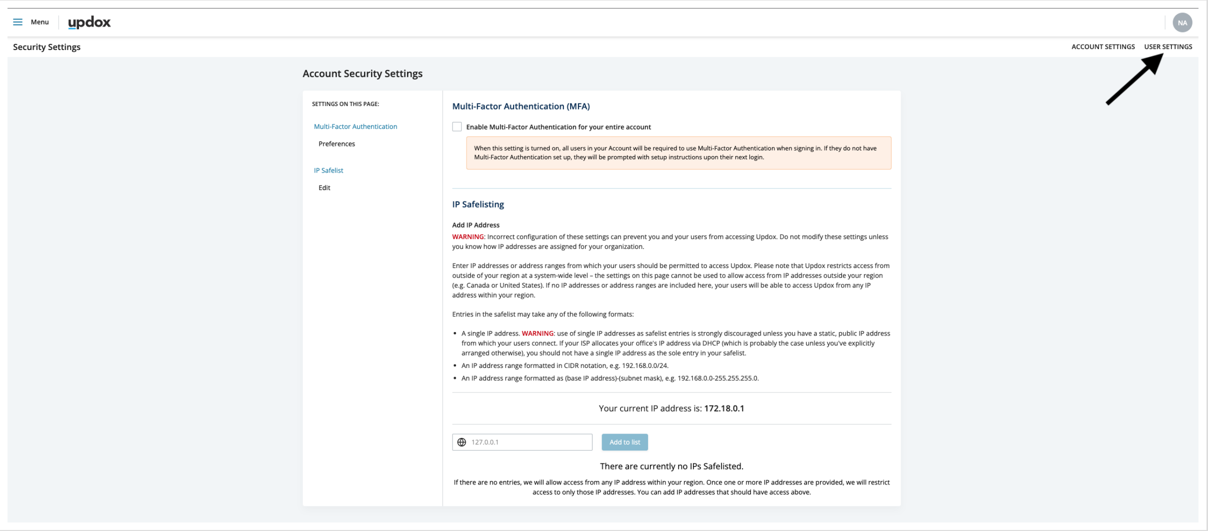
   Unable to scan?

3. Enter the authentication code provided by the application and click Submit to finish the setup.

Note: If you decide to disable MFA for your account, it **will NOT** turn off MFA for all of your users. The users will need to delete the instance from the authenticator app or an account holder will need to reset the MFA status for each individual user (see below steps).

MFA User Management

1. Account Holders have the ability to view the MFA status of any user. To manage MFA for your users click on the **User Settings** from the main Security Settings page.



Security Settings

Account Security Settings

Multi-Factor Authentication (MFA)

□ Enable Multi-Factor Authentication for your entire account

When this setting is turned on, all users in your Account will be required to use Multi-Factor Authentication when signing in. If they do not have Multi-Factor Authentication set up, they will be prompted with setup instructions upon their next login.

IP Safelisting

Add IP Address

WARNING: Incorrect configuration of these settings can prevent you and your users from accessing Updox. Do not modify these settings unless you know how IP addresses are assigned for your organization.

Enter IP addresses or address ranges from which your users should be permitted to access Updox. Please note that Updox restricts access from outside of your region at a system-wide level – the settings on this page cannot be used to allow access from IP addresses outside your region (e.g. Canada or United States). If no IP addresses or address ranges are included here, your users will be able to access Updox from any IP address within your region.

Entries in the safelist may take any of the following formats:

- A single IP address. WARNING: use of single IP addresses as safelist entries is strongly discouraged unless you have a static, public IP address from which your users connect. If your ISP allocates your office's IP address via DHCP (which is probably the case unless you've explicitly arranged otherwise), you should not have a single IP address as the sole entry in your safelist.
- An IP address range formatted in CIDR notation, e.g. 192.168.0.0/24.
- An IP address range formatted as (base IP address)-(subnet mask), e.g. 192.168.0.0-255.255.255.0.

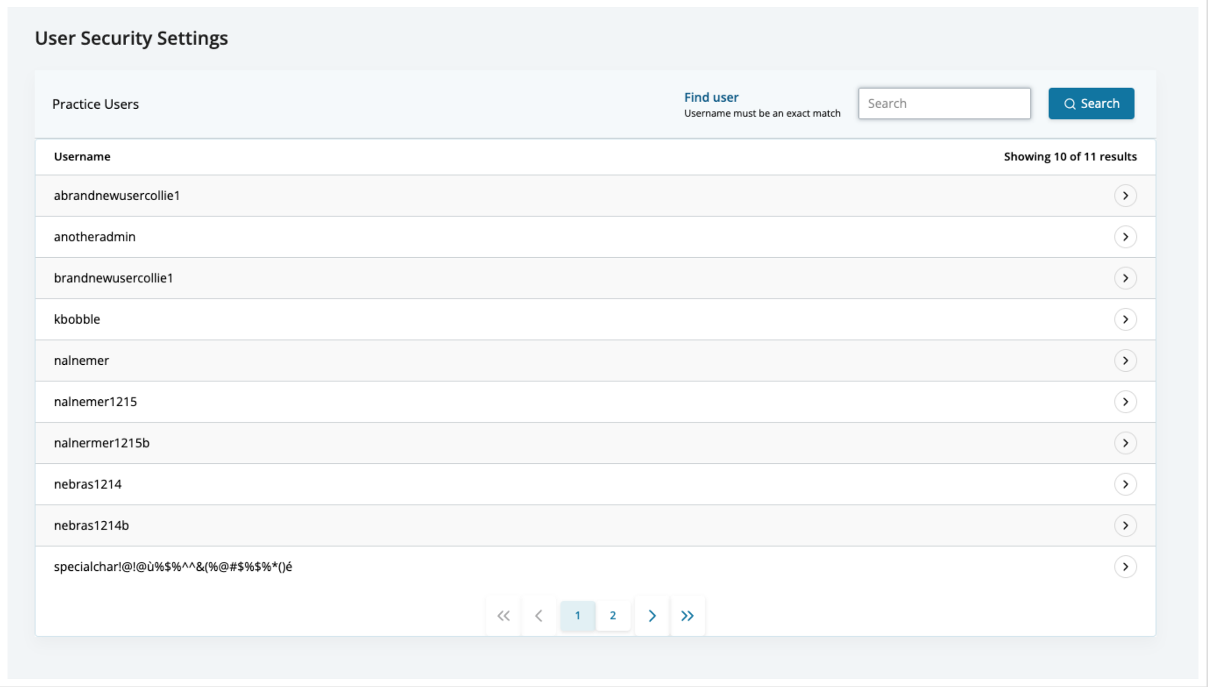
Your current IP address is: **172.18.0.1**

127.0.0.1

There are currently no IPs Safelisted.

If there are no entries, we will allow access from any IP address within your region. Once one or more IP addresses are provided, we will restrict access to only those IP addresses. You can add IP addresses that should have access above.

2. Here you can select or search for a user. You must use the user's full and exact username when searching.



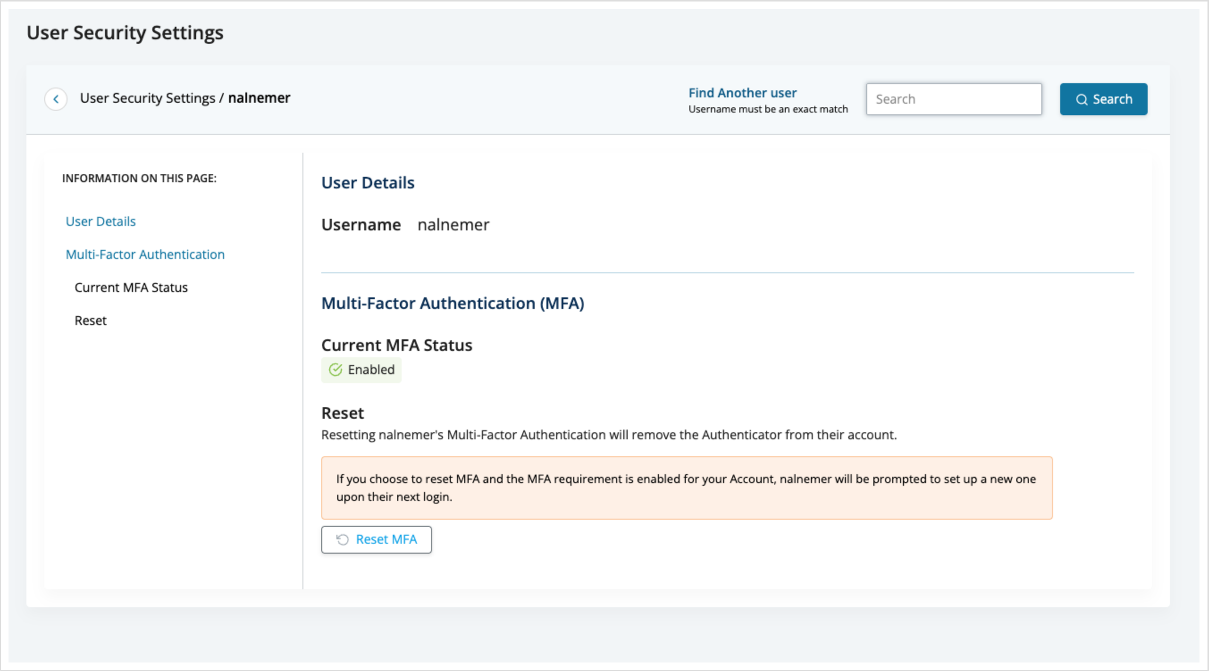
User Security Settings

Practice Users

Find user
Username must be an exact match

Username	Showing 10 of 11 results
abrandnewusercollie1	
anotheradmin	
brandnewusercollie1	
kbobble	
nalnemer	
nalnemer1215	
nalnermer1215b	
nebras1214	
nebras1214b	
specialchar!@!@ù%$%^^&(%@#$%$%*()é	

3. After selecting the user, you can reset their MFA by clicking the **Reset MFA** button.



User Security Settings

User Security Settings / **nalnemer**

Find Another user
Username must be an exact match

INFORMATION ON THIS PAGE:

- User Details
- Multi-Factor Authentication
  - Current MFA Status
  - Reset

User Details

Username nalnemer

Multi-Factor Authentication (MFA)

Current MFA Status
✓ Enabled

Reset
Resetting nalnemer's Multi-Factor Authentication will remove the Authenticator from their account.

If you choose to reset MFA and the MFA requirement is enabled for your Account, nalnemer will be prompted to set up a new one upon their next login.

If a user is having trouble with their MFA or if the user is locked out due to a lost MFA device, they should first contact the Account Holder. Account Holders have the option to reset MFA for that particular user. Keep in mind, if the account still requires MFA, that user will still be required to set up a new device upon their next login.

If an Account Holder loses an MFA device, they will need to contact Updox Support to reset their MFA.