Multi-Factor Authentication (MFA) Tools

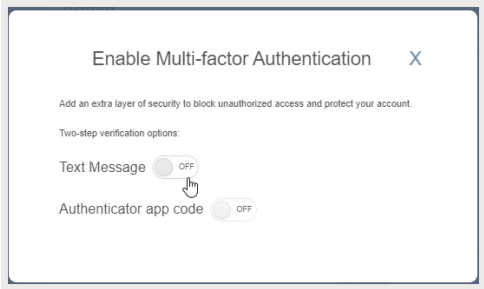
The Cloud Services portal has added multi-factor authentication (MFA) security protocols to ensure that your communications-related data is always protected. This means that the sign in process for individual portal access accounts (users and admins) has been enhanced to require successful setup and entry of a randomized verification code prior to Portal entry. The set up and management process is simple, with easy to follow instructions provided to assist with all the steps required to get MFA successfully activated.
Note: *Each account holder must set up their own Multi-factor authentication method for themselves.*

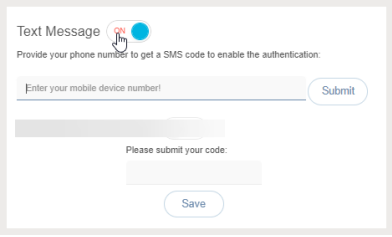
The login process when Multi-Factor Authentication (MFA) security protocols are in effect is:

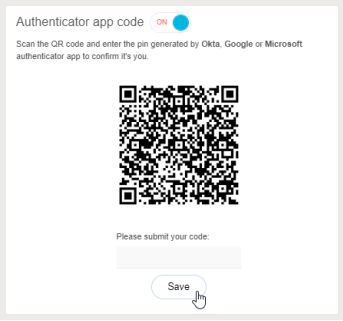
1. Navigate to the Cloud Services Portal sign in page in your web browser.

2. Enter your Cloud Services Portal account **Username|Password** credentials as usual and click Submit.
   If those credentials are correct, the system will prompt the user for MFA next steps:

   A. If you have not yet activated MFA, and its use is *mandatory*, the system will display your MFA options for selection and activation. Follow the instructions in the dialog to set up an MFA verification code receipt method (via SMS Text or use of an App (Okta Verify, Microsoft Authenticator, **or** Google Authenticator) if offered. Upon completion of the activation steps, the MFA method you activate and Save here will be saved to your Portal Profile for review and self-management within the Portal. **Please note**: *No one else can set up your MFA protocol for you*.

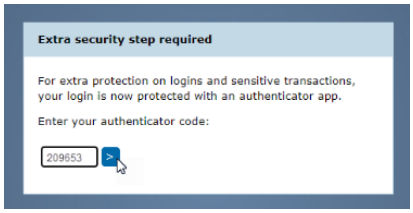






   B. If an active MFA method (SMS Text or App) is already defined in your Portal Profile, the system will simply prompt for entry of the 6-digit code generated for you via your chosen MFA method.

3. Enter the 6-digit code you receive via your activated MFA method in the field provided and click the send > button to Save/Submit.



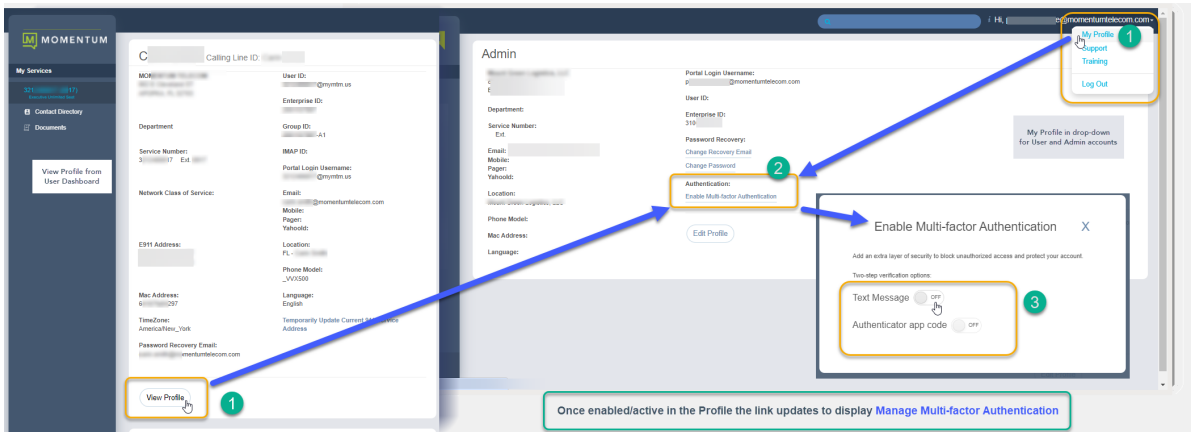
Upon successful submission of the correct (currently active) 6-digit MFA verification code, the Portal opens and the User/Admin may proceed to work in the Portal.

Once an MFA method has been activated, the system will require the MFA code entry step during each sign in attempt for Portal access.

The next sections in this quick start guide cover the MFA self-management tools and the Administrator-level tool for assisting users with MFA-related login issues.

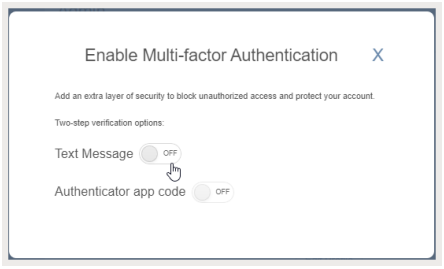
Enable/Manage Multi-factor Authentication (MFA)

The Enable / Manage Multi-factor Authentication link in the View Profile or My Profile dialog allows the account holder to define and manage the preferred security authentication method via SMS Text or supported code generator.

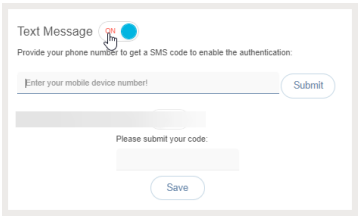


1. Click on the Enable/Manage Multi-factor Authentication link in your *View Profile* dialog.

2. Choose one of the MFA Verification options:

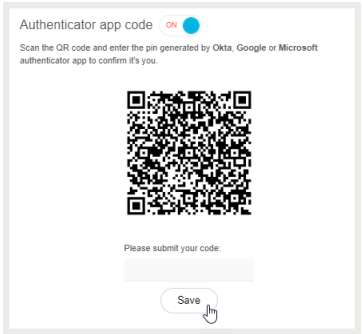


Text Message
- Click to toggle this option ON
- Enter your SMS-enabled 10-digit phone number in the field provided and click the Submit button.



OR

Authenticator App Code
- Click to toggle this option to ON
- Scan the single-use QR code that is created to connect your Okta Verify, Google Authenticator, or Microsoft Authenticator app and follow the App's instructions for setup.



3. Enter the six (6) digit code you receive via the method you just setup in the Please submit your code field below.

4. Click on the Save button.

   Once completed, *entry of the 6-digit code received via your selected MFA verification method will be required on all subsequent portal sign in attempts.*

Repeat the steps above to modify/change the MFA verification method selection from this dialog.

NOTE: *When changes are made to these settings, the system deactivates the old MFA method. Users/Admins must complete the steps above in full again for the preferred MFA option to set up a new method.*

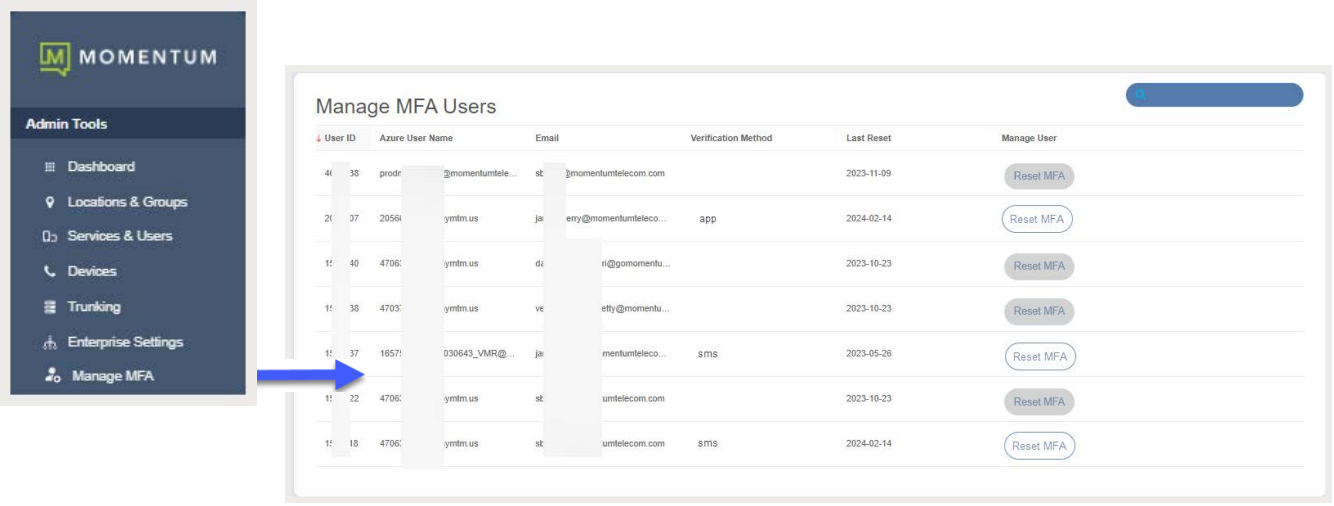
Contact your organization's Administrator if you need help to Reset MFA in order to access the Portal.

*Administrator Only - Reset MFA

This Admin Tools section displays a list of the portal accounts the Admin has been granted permission to view.

Click on the **Manage MFA** option in the left navigation menu to open the Manage MFA Users section.
This view displays a ↑ sortable ↓ and searchable list of the User and Admin portal access accounts that are currently set up on the organization's system. This area makes it very easy to view the MFA usage of the organization's portal users and quickly assist users who need help with MFA protocols to gain access to the portal.

The SuperAdmin can see information for all accounts for their organization.
Group Level Admins can see the information for the accounts in the groups/locations they are authorized to view.



Reset MFA

The Reset MFA button provides Admins with information about each account's MFA activation status and a simple way to immediately disable/disconnect the current setup and prompt the user to set up a new MFA protocol during the login process (if MFA use is Mandatory) or sign in and set up a new MFA method in their Profile (if MFA use is Optional).

- Grayed button = MFA is inactive/not currently set up for the account - a reset cannot be performed.
- White button = MFA is active/in use for the account - a reset can be performed.

Simply click on the Reset MFA button adjacent to the desired account if it is active to immediately deactivate the account's current MFA method (SMS Text or App). Once clicked, the button will turn gray and will not become available to click again until the user has set up an active MFA protocol for portal access.

This action will allow the selected portal account holder to:

Sign into the Portal using only their username/password credential if MFA use is still optional, **or -**
Be prompted by the system to select and set up a new MFA verification code receipt method (SMS Text or one of the authentication apps) during portal login if MFA use is Mandatory.

Note: If a user/Admin is currently logged into their own portal account, an MFA Reset is not necessary. Each Account holder may modify their own MFA method setup by going to My Profile | View Profile > Enable/Manage Multi-factor Authentication and following the relevant setup/activation steps (see page 2).

Important Note: To ensure security for each portal account, Admins *cannot* set up MFA for others and should not attempt to do so. **Each individual account holder must set up their own Multi-Factor Authentication protocol for their own portal account(s)** either during the sign in process or via the Enable/Manage MFA tool within their Portal account profile settings. There can be only one (1) active MFA protocol linked to each individual account's sign in credentials (username/password). *Portal Accounts cannot be shared.*