Quick Start Guide

Portal Multi-Factor Authentication (MFA) 101

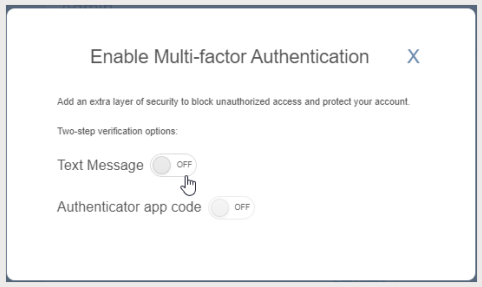
The My Cloud Services portal has added multi-factor authentication (MFA) security protocols to ensure that your communications-related data is always protected. This means that the sign in process for individual portal access accounts (users and admins) has been enhanced to require successful setup and 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.*

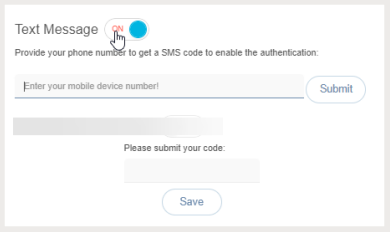
The login process when Multi-Factor Authentication (MFA) security protocols are in effect is:

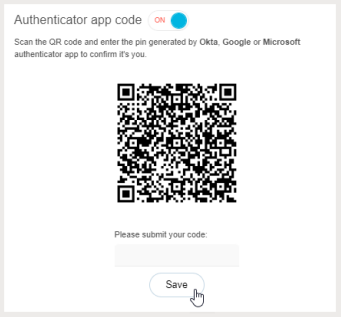
1. Navigate to the Cloud Services Portal sign in page in your web browser.

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*.

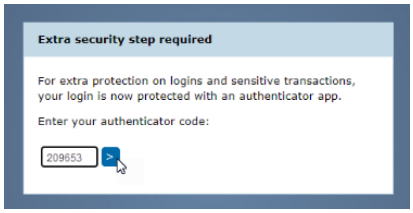






   B. If an active MFA method (SMS Text or App) is already defined in your Portal Profile, the system will simply prompt for entry of the 6-digit code generated for you via your chosen MFA method.

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.



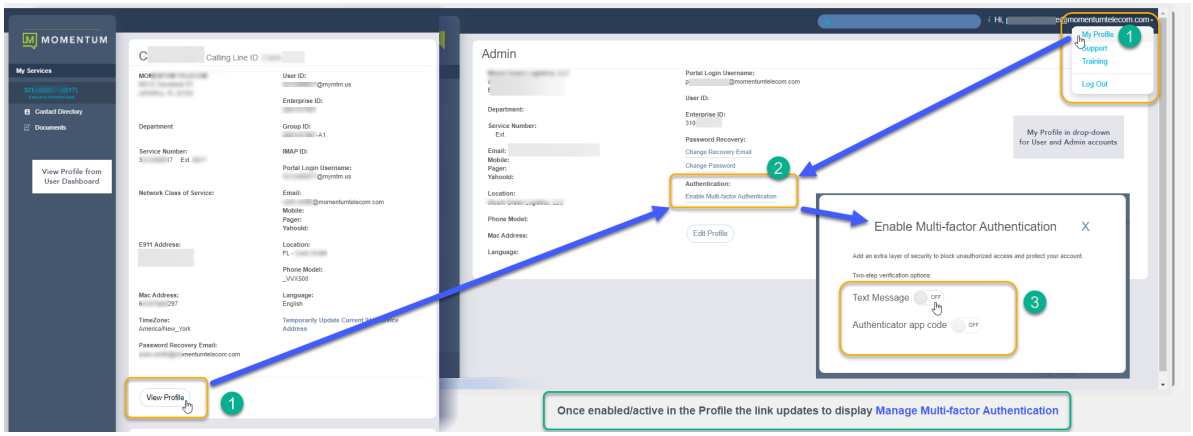
Upon successful submission of the correct (currently active) 6-digit MFA verification code, the Portal opens and the User/Admin may proceed to work in the Portal.

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.

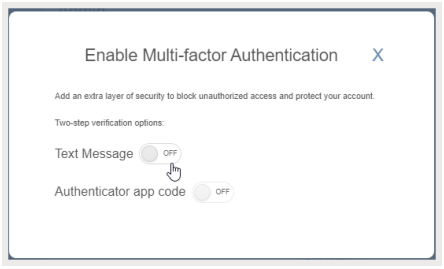
Enable/Manage Multi-factor Authentication (MFA)

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.

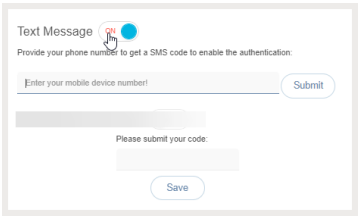


1. Click on the Enable/Manage Multi-factor Authentication link in your *View Profile* dialog.

2. Choose one of the MFA Verification options:

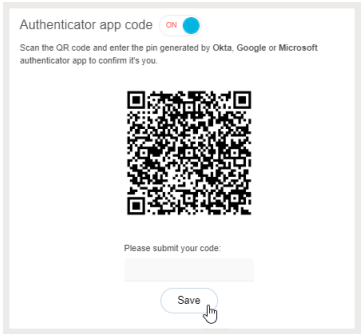


Text Message
- Click to toggle this option ON
- Enter your SMS-enabled 10-digit phone number in the field provided and click the Submit button.



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