cornerstone

CSX - Multi-Factor Authentication (MFA)

Implementation Guide

July 2024

Cornerstone CSX

Version history

	Date	Description
1.0	Dec 2023	Open Beta (v1, Stage only)
2.0	March 2024	Early Adopter version (v2) • Skip on subsequent logins • Corporate Styling • Feature Activation • Copy Down • Multi-Language support
3.0	July 2024	Generally Available (v3) • MFA support for Partner accounts

Table of contents

Overview

Introduction

Multi-Factor Authentication (MFA) is a security mechanism that adds an extra layer of protection to online accounts and services.

It is designed to enhance the security of user accounts by requiring the user to provide two different forms of authentication before they can access their account.

The goal of MFA is to prevent unauthorized access even if an attacker obtains the user's password. Even if a malicious actor obtains your password, they will still need the second authentication factor to gain access.

Categories

Multi-factor authentication typically falls into these categories:

1. **Something You Know**
   This is usually a password or PIN that the user knows. It is the traditional form of authentication with which most people are familiar.

2. **Something You Have**
   This involves a physical device or object that only the legitimate user possesses. For example, this could be a smartphone.

3. **Something You Are**
   This refers to biometric authentication methods, such as fingerprint scans or facial recognition.

Cornerstone MFA

Cornerstone MFA provides a standard, built-in, smart, and secure two-factor authentication solution to build stronger authentication into the Cornerstone CSX standard login process.

Use Cases

Today, if a client is not integrated with Single Sign-On (SSO) providers already supporting MFA or has users not a part of the SSO organization, these users do not have a way to authenticate into the Cornerstone system using multi-factor authentication.

Examples:

- External users like vendors/partners
- Part-time employees
- Users in a special Location
- Users in a special Division
- New employees via acquisition

Key Features

The Cornerstone MFA solution is characterized by the following features:

- Standard, built-in solution
- No dependency on any third-party provider
- Using open and secure industry standards
- Using something you have (company phone, BYOD)
- Enable MFA for all users or only for a subset of users
  (by Location/Division OU, individual users)
- Easy to enable, implement, and rollout
- No impact on any existing SSO integrations; can run in parallel

Prerequisites

Users who are required to log in with MFA need to use a mobile device (e.g., smartphone) with a virtual authenticator app (TOTP app) that supports the time-based one-time password (TOTP) algorithm (RFC 6238). Examples: Google Authenticator, Microsoft Authenticator, Okta Verify, and many others available in app stores.

Considerations

Out of Scope

The following features are not supported by the Cornerstone MFA solution:

- Email or SMS/text-message authentication
- Recruiting: External Candidates login
- Mobile app (comes with its own device registration process)
- Extended Enterprise (EXE): Self-registration process where a new account will be created and logged in to the portal immediately. Note: The MFA process will initiate on subsequent logins.
- E-Signature, e.g., for training completion, where the user is required to re-enter their username and password to apply the electronic signature

Time-based One-time Password

Cornerstone has implemented multi-factor authentication support using **time-based one-time passwords** (TOTP).

Introduction

- The most widely adopted two-step verification method is a time-based one-time passcode (TOTP) generated by a software token.
- TOTP is an Internet Engineering Task Force (IETF) standard, RFC 6238.
- It is the most convenient and easiest to implement because it uses hardware the user already owns.

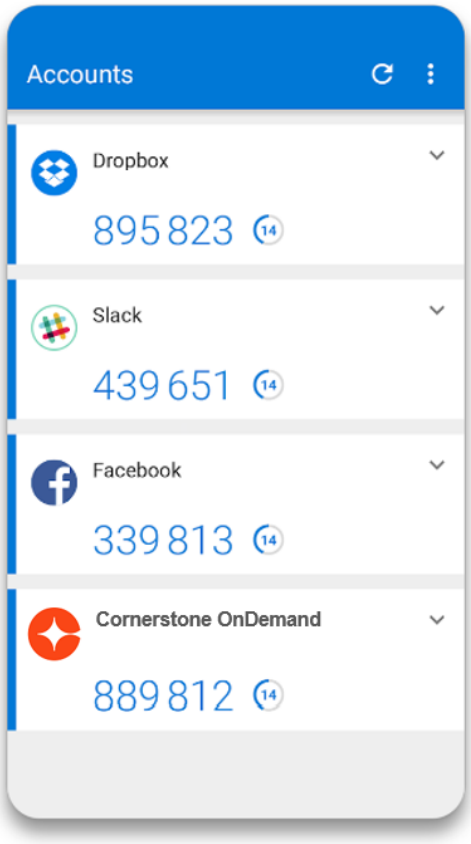
Authentication Device

Virtual Authenticator App (TOTP App)

Virtual authenticator apps implement the time-based one-time password (TOTP) algorithm and support multiple tokens (applications) on a single mobile device.

The virtual authenticator app needs to be installed on the users' authentication mobile device.

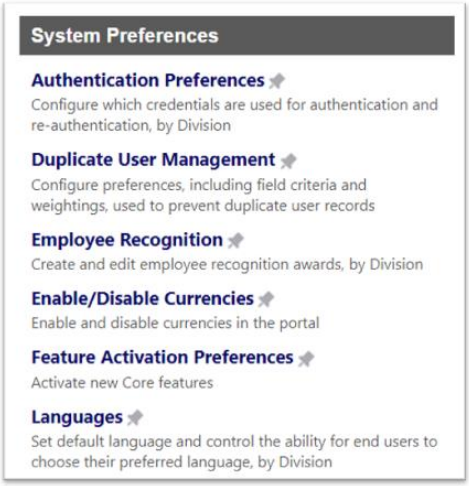
Some popular authenticator apps include Google Authenticator, Microsoft Authenticator, and many others available (free of charge) in app stores.



Administrator

Enable Multi-Factor Authentication

Multi-Factor Authentication (MFA) is disabled by default and needs to be enabled per portal by a **client-administrator** via **Feature Activation Preferences** (Admin > Tools > Core Functions > Feature Activation Preferences).



Note: Enabling MFA for a portal does not mean that the end users must log in with multi-factor authentication immediately.

It means that the general functionalities are made available for a **client-administrator** to configure the MFA settings, for example, to identify the users required to log in with MFA.

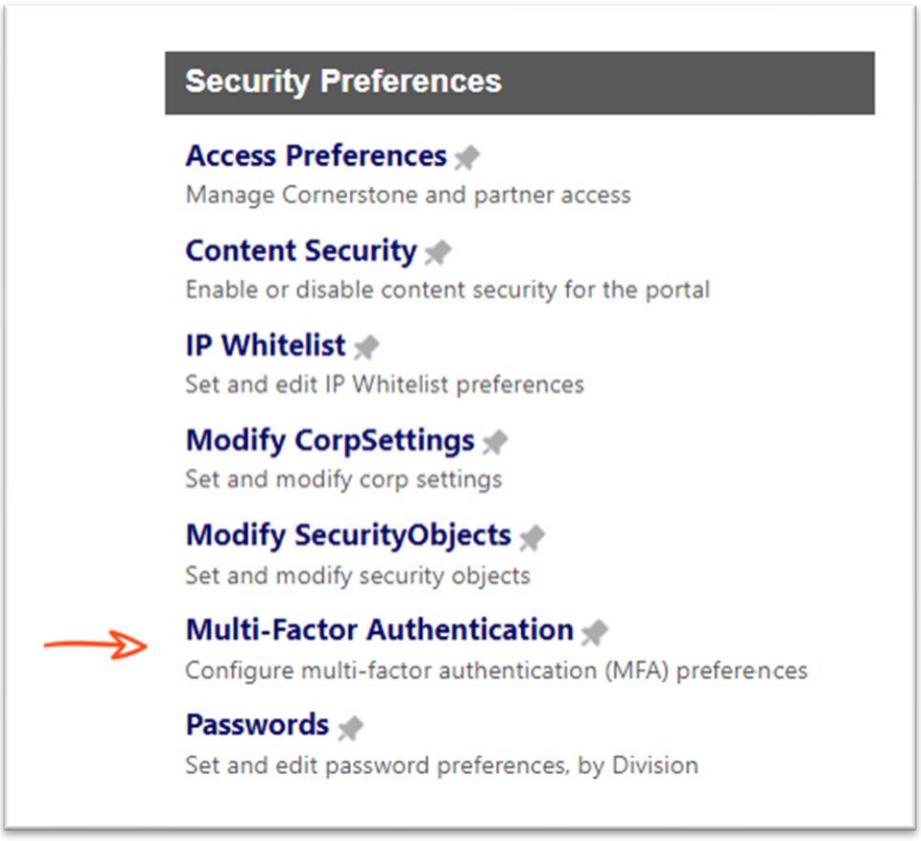
It is recommended to test multi-factor authentication in either your Pilot or Stage environment before setting it up in Production.

Due to various caching mechanisms, it can take up to **60 minutes** before MFA has been enabled on your portal.

Multi-Factor Authentication Preferences

After multi-factor authentication has been enabled for a portal, an administrator can navigate to the MFA Preferences to configure the multi-factor authentication settings.

Admin > Tools > Core Functions > Core Preferences > Security Preferences > Multi-Factor Authentication



General Settings

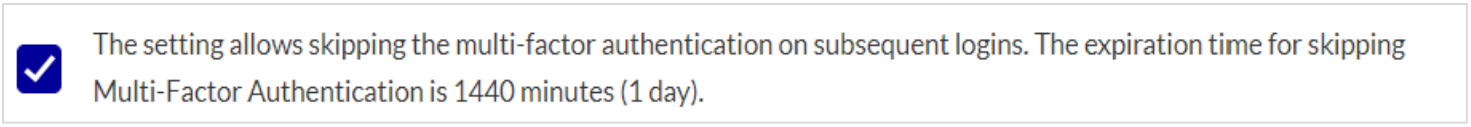
Help Link

Customers can configure a custom online help page with more specific, company-related help and instructions. Keeping this field empty will open the default Cornerstone online help.

Skip on subsequent logins

The setting allows users to skip the multi-factor authentication on subsequent logins.
The expiration time for Skip Multi-Factor Authentication is **24 hours** by default.

If this setting is set to true, then users will see the Multi-Factor Authentication screen only for the first login attempt. After successfully logging in, the Multi-Factor Authentication screen will be bypassed for one day.



Organizational Units and Users

Two sections control how OUs and users are configured to be required to log in with MFA: "**Include**" and "**Exclude**." It is important to note that the second section (Exclude) takes precedence over the first section (Include).

Check out the **User Identification Process** workflow to understand how users are identified as required to log in with MFA.

Include Organizational Units and Users

This section controls the OUs or users who are required to log in with MFA.

All Users

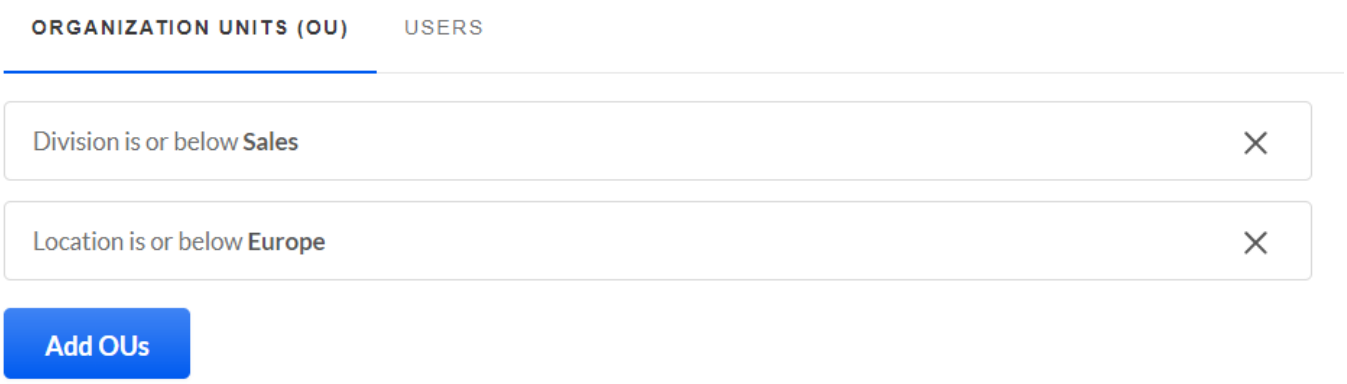
Select this option to enable MFA for all users.

If the **All users** option is selected, is it not possible to add or remove individual OUs and Users; the “Add OUs” and “Add Users” buttons will not be visible anymore.

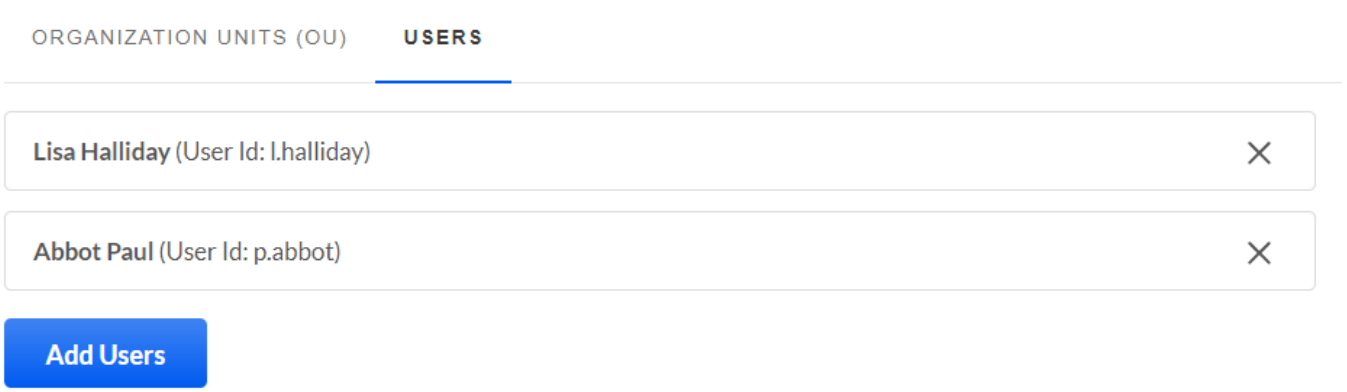
Individual OUs and Users

Select OUs or users who are required to log in with MFA. Note that a selected OU always includes all child OUs (“is or below”). A user must belong to one of the selected OUs to be considered.

Example: **Organizational Units**



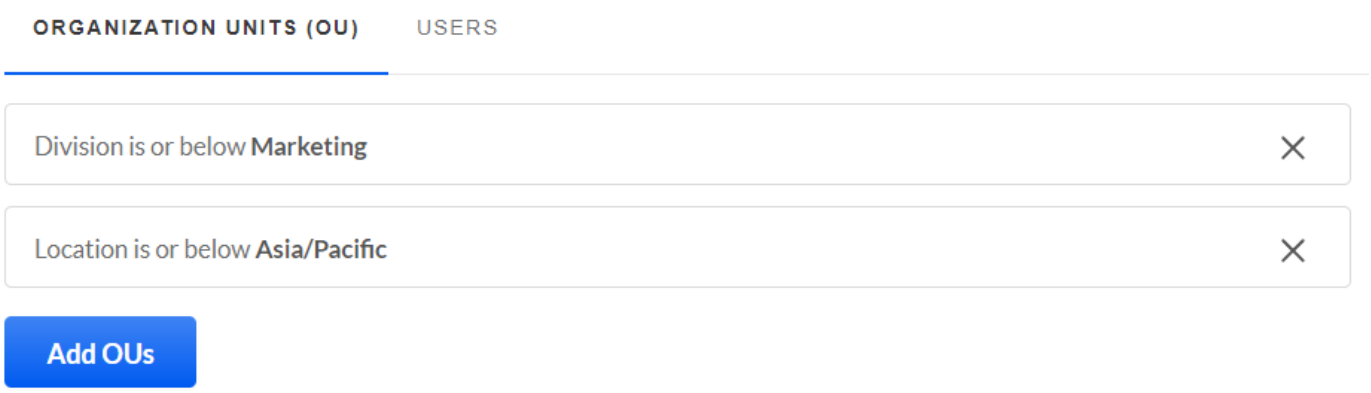
Example: **Individual Users**



Exclude Organizational Units and Users

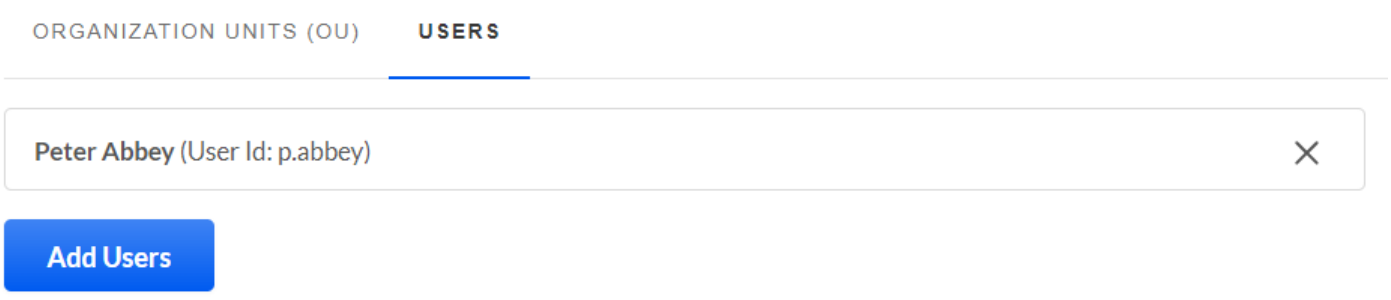
Select OUs or users who should be excluded from being required to log in with MFA. The OUs and users listed here have precedence over the first (Include) section, where OUs and users can be added. Note that a selected OU always includes all child OUs ("is or below"). A user must belong to one of the selected OUs to be considered.

Example: **Organizational Units**



Example: **Individual Users**

Adding a user to the "Exclude" list will overwrite all other settings, and the user will no longer be required to log in with MFA. Review the **User Identification Process** to understand the entire workflow.



Additional Information

To avoid latency while logging in to the system, the maximum number of configurable OUs and Users is limited.

Setting	Value
Maximum number of Organizational Units (OUs) to **Include**	40
Maximum number of Organizational Units (OUs) to **Exclude**	10
Maximum number of individual users to **Include**	100
Maximum number of individual users to **Exclude**	100

Corporate Styling

The following style elements are inherited from the Custom Login Page (as configured with the Custom Login Page tool). If a style or color is not inherited, defaults will be used.

Element	Style: Background	Style: Classic	Style: Colorblock
Company Logo	✓	✓	✓
Background Image	✓	-	-
Page Title	✓	✓	✓
Login Box - Background Color	✓	-	✓
Button - Background Color	✓	✓ (from banner background color)	✓
Button - Text Color	✓ (from background color of the login box)	-	✓ (from background color of the login box)

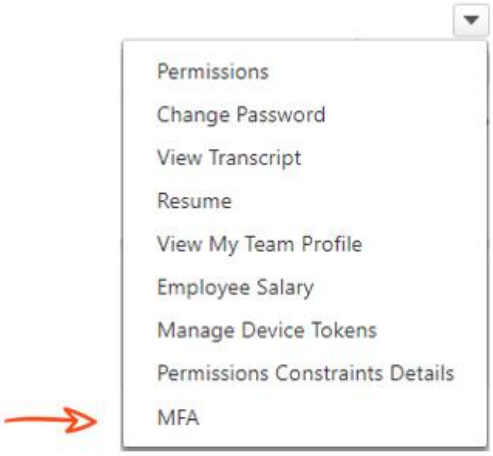
Remove Device from a User Account

Administrators with appropriate permissions can remove an existing mobile device from a User record.

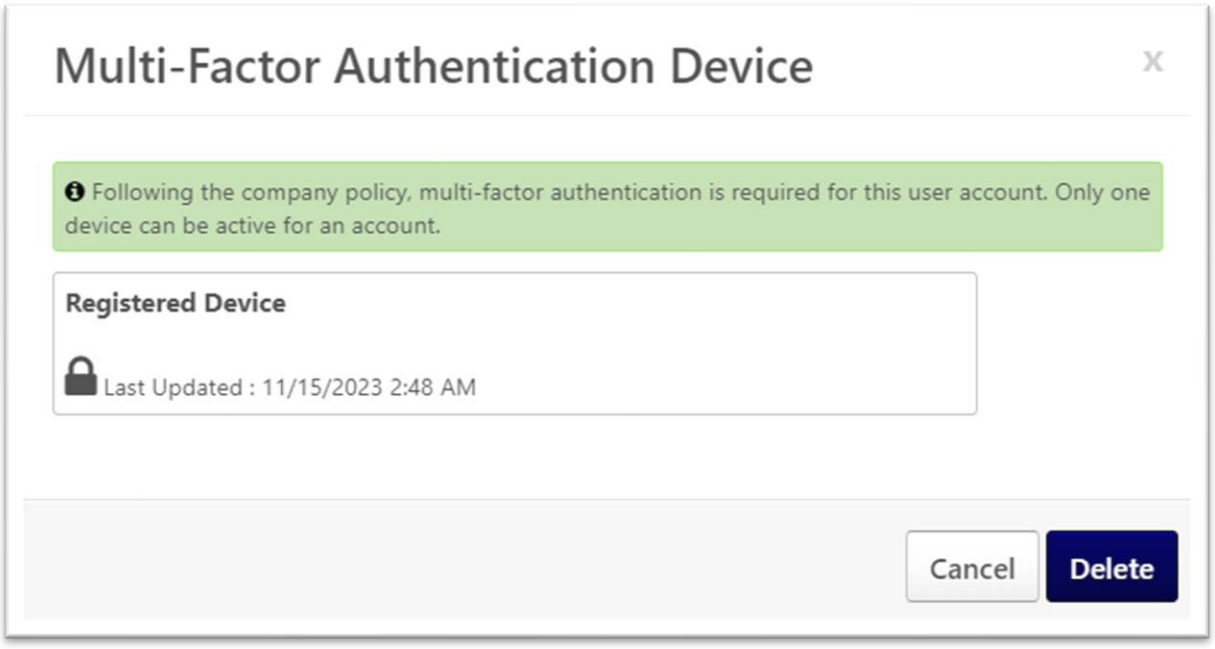
This may be necessary if a user cannot log in anymore because the existing registered mobile device is broken or unavailable. After the administrator removes the mobile device, the user can register a new mobile device as part of the (initial) login process.

User Record

Search for the **User record** and click the drop-down in the **Options** column, then select **MFA**.

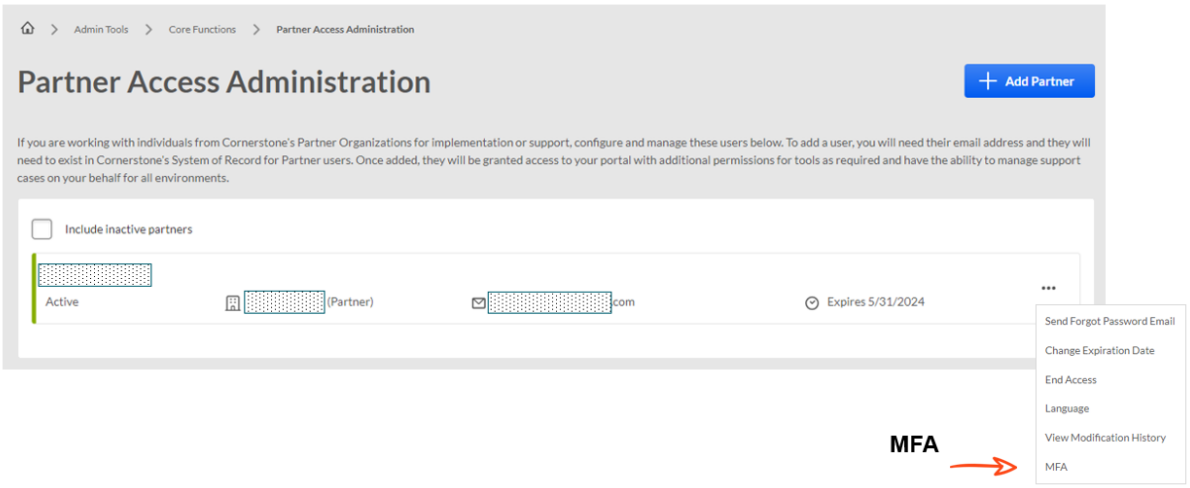


Example:



Partner Account

MFA devices for partner accounts can be managed via the Partner Access Administration tool.

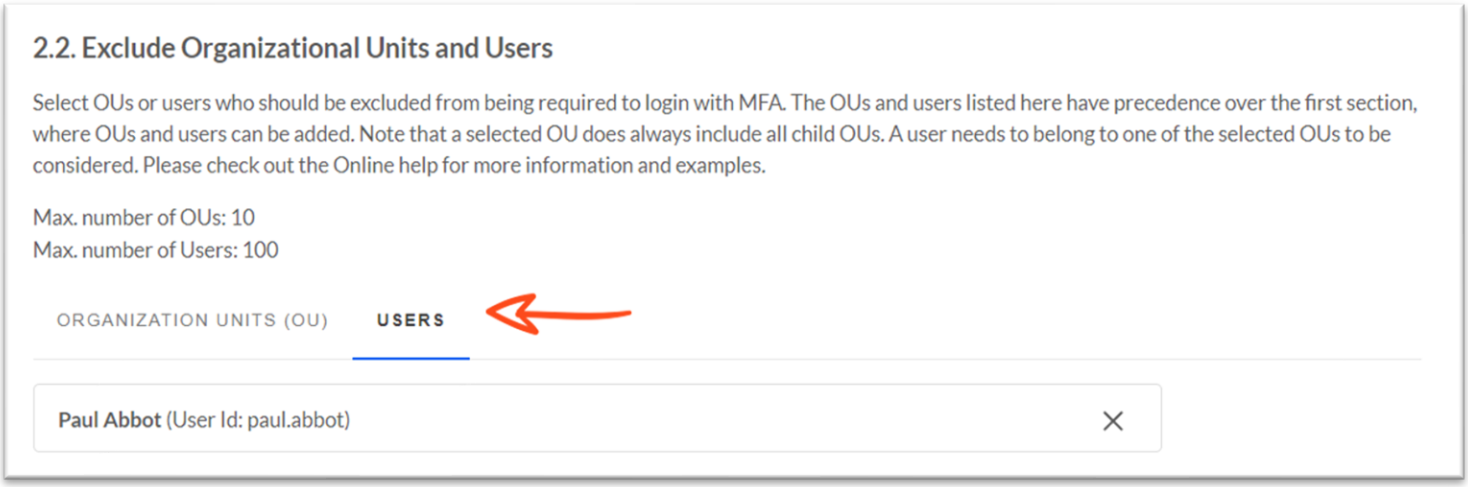


Disable MFA for a User Account

Administrators with appropriate permissions can disable MFA for a specific User record. This can be helpful, for example, to allow a user to log in for a short time without MFA and re-register their device.

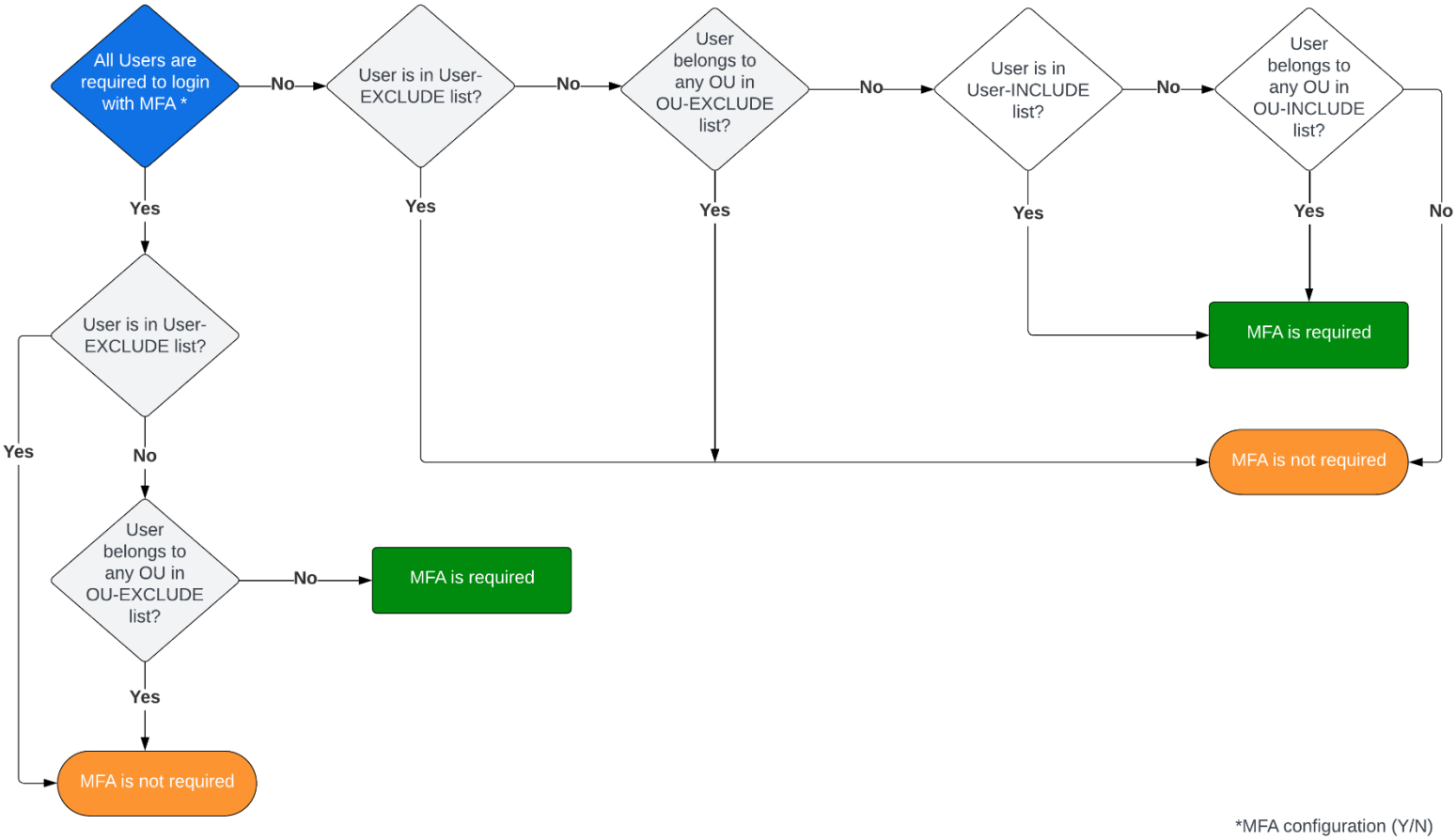
To disable MFA for a specific user, an MFA administrator can open the **MFA Preferences**, go to the section **Exclude Organizational Units and Users**, and add the user to the list of **Users**.

To add a user to the “Exclude” Users list, the user cannot be in the “Include” list at the same time.



User Identification Process

The Cornerstone MFA solution uses the following process to identify which users need to log in with MFA:

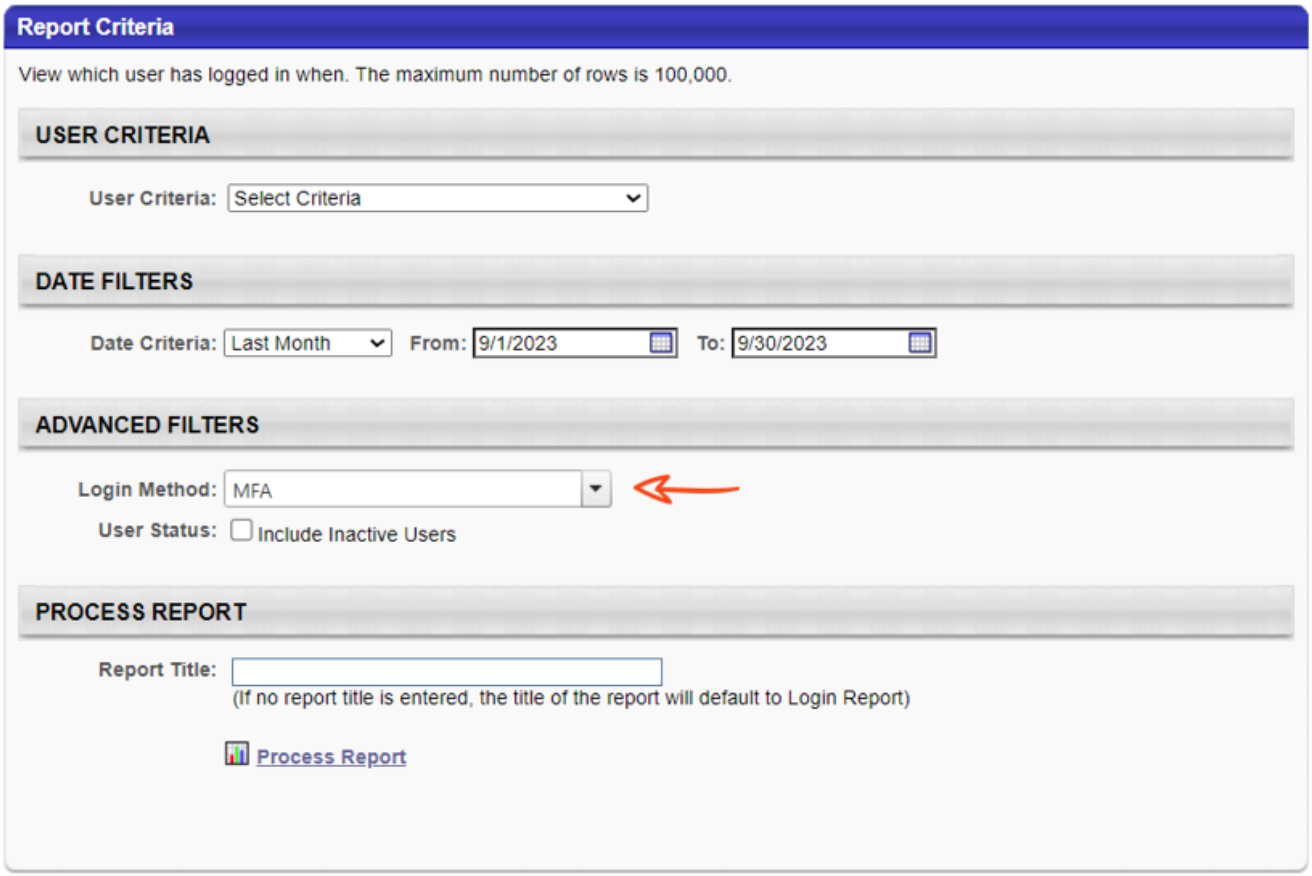


*MFA configuration (Y/N)

Login Report

The Login Report enables organizations to report on which users have logged in to the portal using multi-factor authentication (MFA) and when. Organizations may need to provide this information to auditors.

Select **MFA** as a **Login Method** (filter) to process the report.



Copy-Down

The copy down process (from Production to Pilot/Stage) will copy the MFA configuration, but not the individual mobile device registrations. End users who are required to log in with MFA are required to register a new mobile device while they log in to the Stage/Pilot portal for the first time.

End User Experience

General

If a user is required to log in with MFA, they need to have a mobile device (e.g., smartphone) with a TOTP-compatible virtual authenticator app installed to log in.

Register New Device

Users can register a new mobile device in two different ways, in **My Account** or during the (first-time) **Login Process** (after MFA has been enabled for a user account).

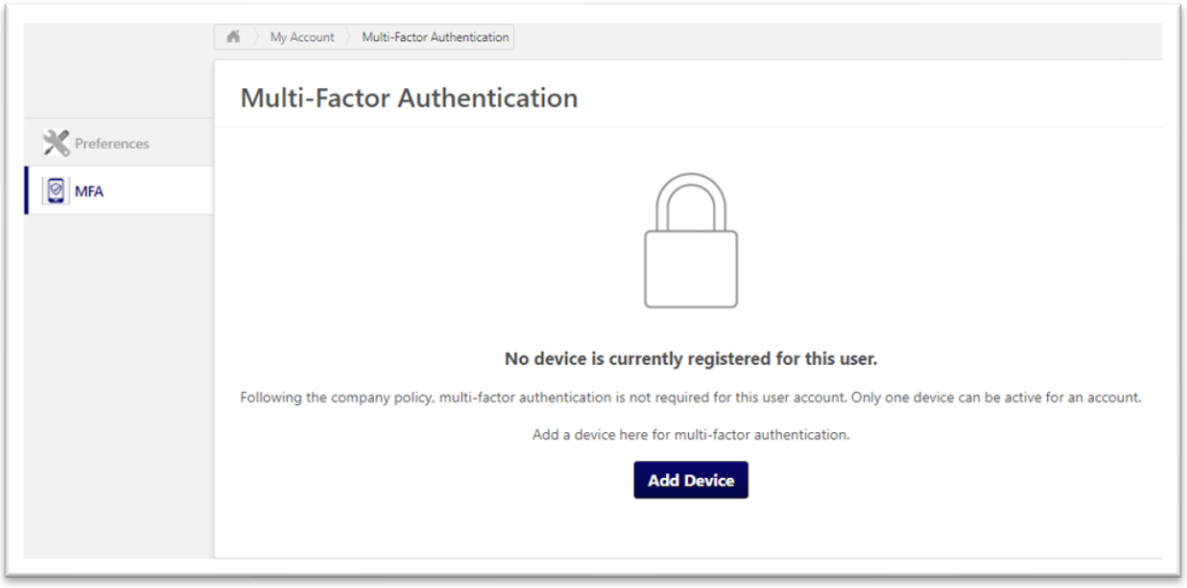
1. **My Account**
   This option is available to all users logged in to an MFA-enabled portal.
2. **Login Process**
   This option is available and mandatory to all users who are required to log in with MFA but have not yet registered a device.

My Account

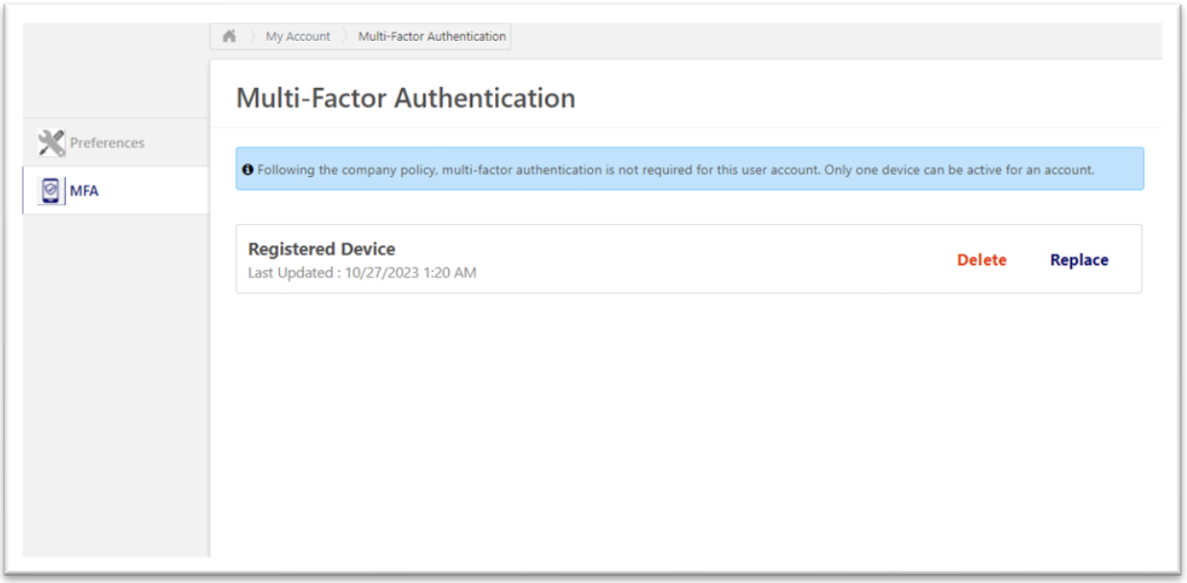
In **My Account**, users can register a new device or replace or delete an existing device.

In an MFA-enabled portal, **any user** can manage an MFA device, even if the user is not yet required to log in with MFA.

Screenshot: No device registered yet, with an option to add a new device.



Screenshot: Registered Device, with the option to delete or replace the device.



Login Process

The option to register a new MFA device as part of the login process is available and mandatory for all users who are required to log in with MFA but who have not yet registered a device.

If the following conditions are met, an MFA device must be registered as part of the (first-time) login process:

1. MFA has been activated for a user by the CSX administrator; for example, the user belongs to a given Location or Division OU or was added manually.
2. The user has no MFA device registered yet.

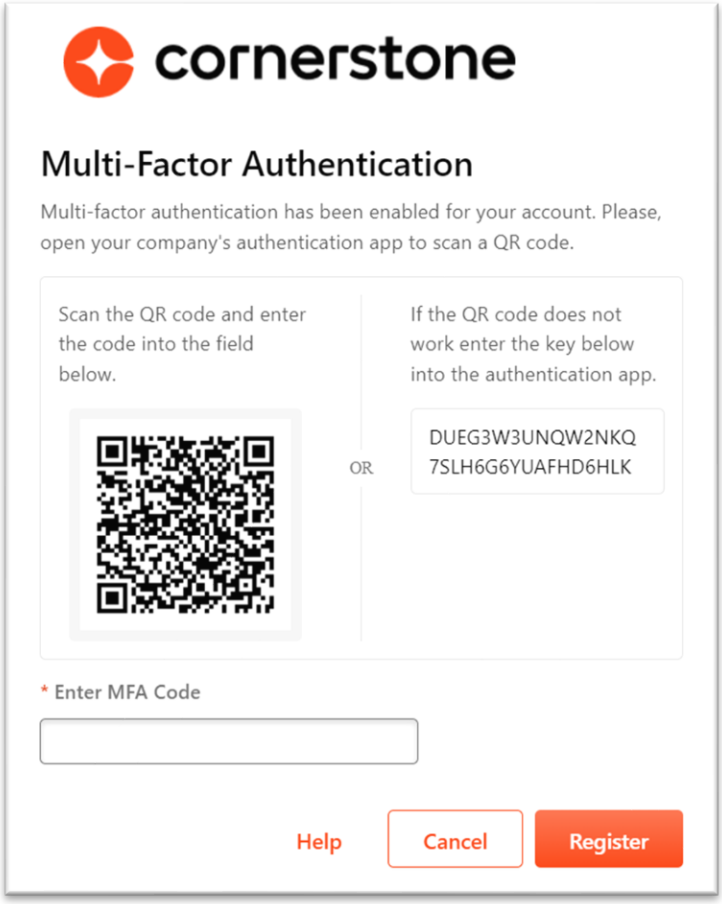
Check out the **Login Process Overview** to understand the entire workflow for an end user.

Register new Device with QR Code

Using the QR code is the most convenient way to set up a new device and use multi-factor authentication.

Steps to set up a device with a QR Code:

1. On your smartphone, open the TOTP app you have installed.
2. In the TOTP app, look for an option to add an account or scan the QR code. The QR code contains the information needed to set up your TOTP app.
3. Use your smartphone's camera to scan the QR code displayed on your computer screen. The app will automatically recognize the code and add the account.
4. After adding the account to your TOTP app, the app will generate a one-time code. Enter this code into the Cornerstone MFA page to verify the setup. This step confirms that the TOTP setup is working correctly.
5. Once verified, your MFA device is active. Now, each time you log in to your account, you must open your TOTP app to generate the current temporary code to complete the login process.

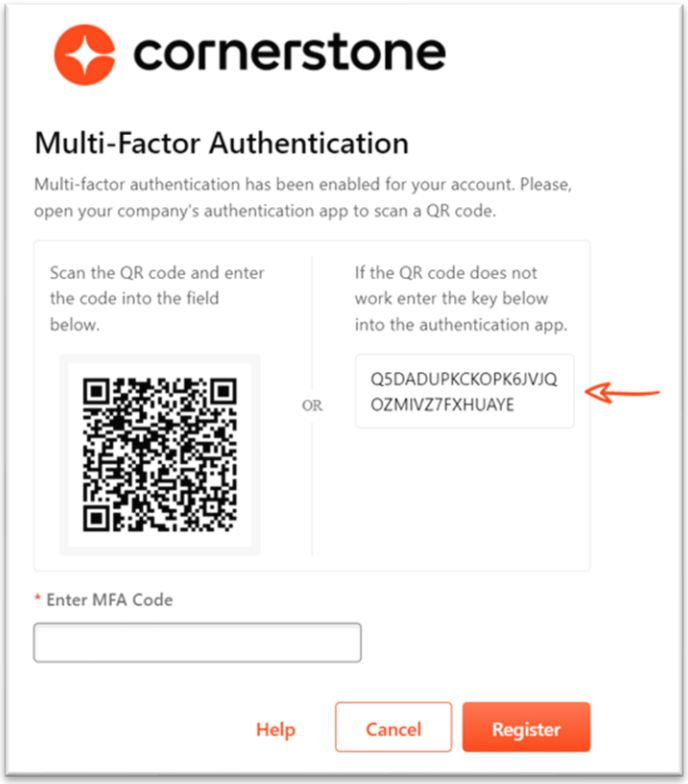


Register new Device with Secret Unique Key

Using a secret unique key is an optional way to set up and use multi-factor authentication.

Steps to Register a TOTP Device with a Secret Unique Key:

1. On your smartphone, open the TOTP app you have installed.
2. In the TOTP app, look for an option to "Add Account" or "Manual Entry."
3. Enter a name or label for the account.
4. Enter the secret key from the Cornerstone MFA page, for example: Q5DADUPKCKOPK6JVJQOZMIVZ7FXHUAYE
5. The app will recognize the secret code and add the account.
6. After adding the account to your TOTP app, the app will generate a one-time code. Enter this code into the Cornerstone MFA page to verify the setup. This step confirms that the TOTP setup is working correctly.

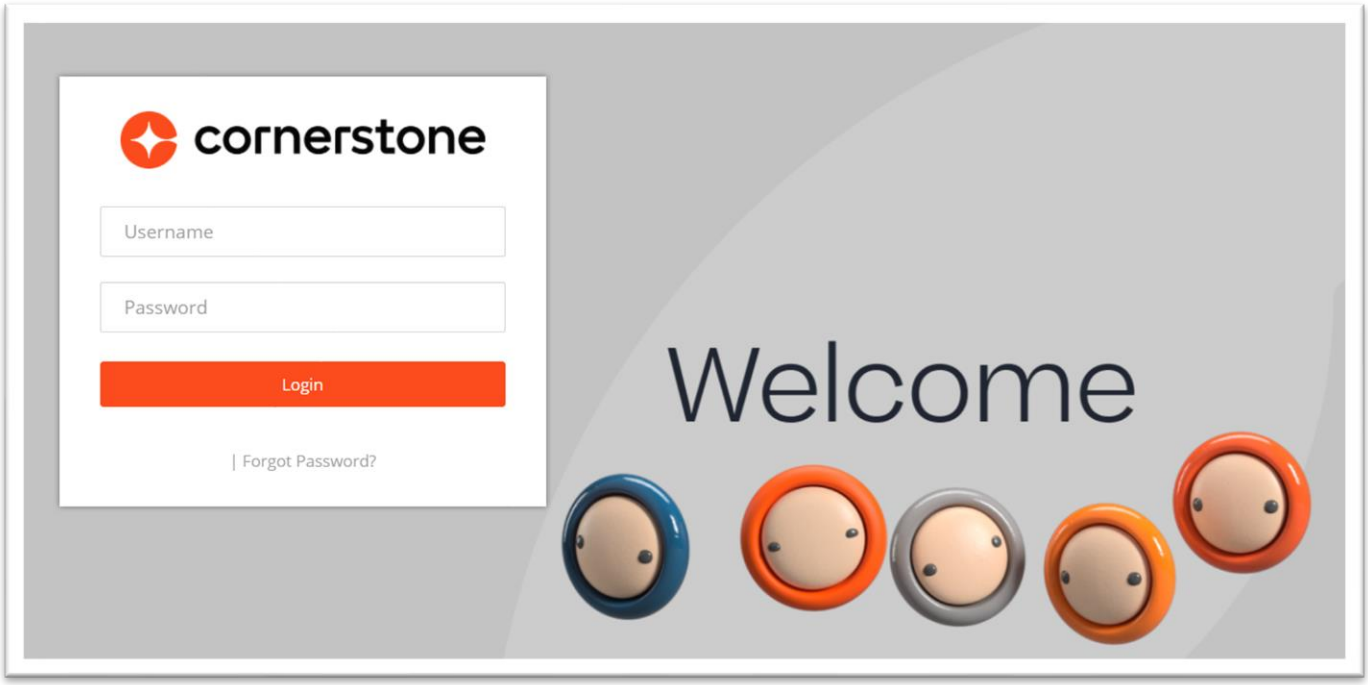


7. Once verified, your MFA device is active.
   Now, each time you log in to your account, you must open your TOTP app to generate the current temporary code to complete the login process.

Log in with MFA

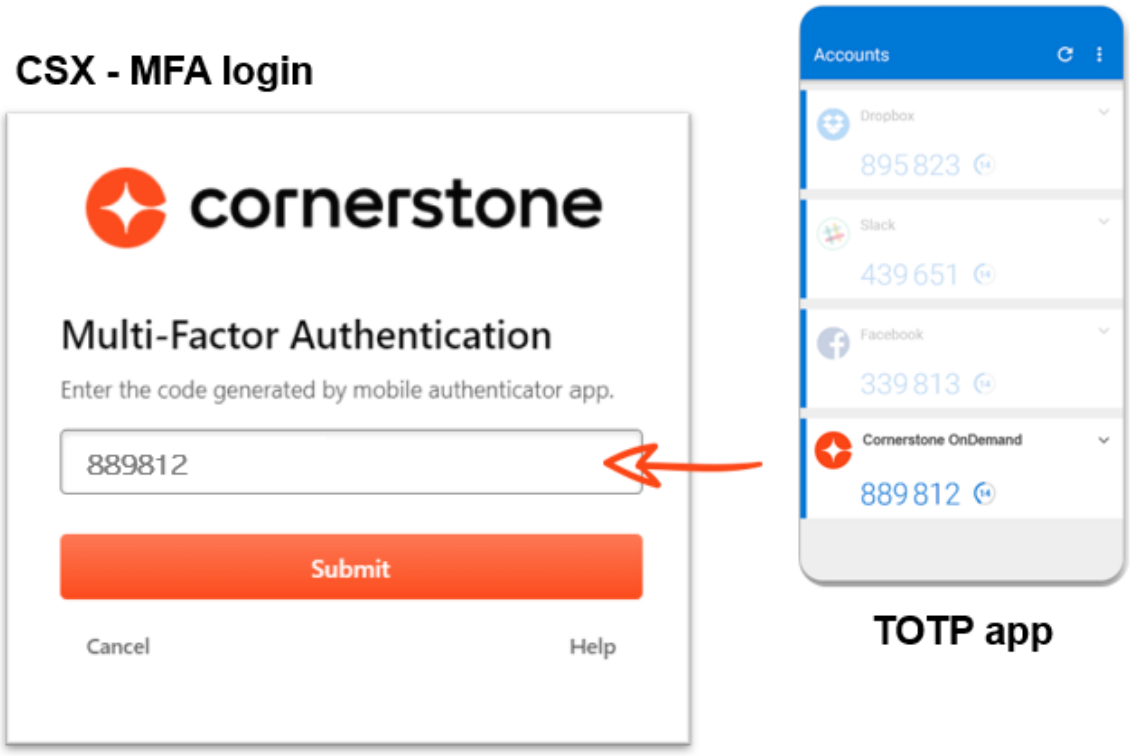
Users who must log in with MFA must enter a temporary generated code from their registered mobile device to complete the login process.

1. Enter Username and Password

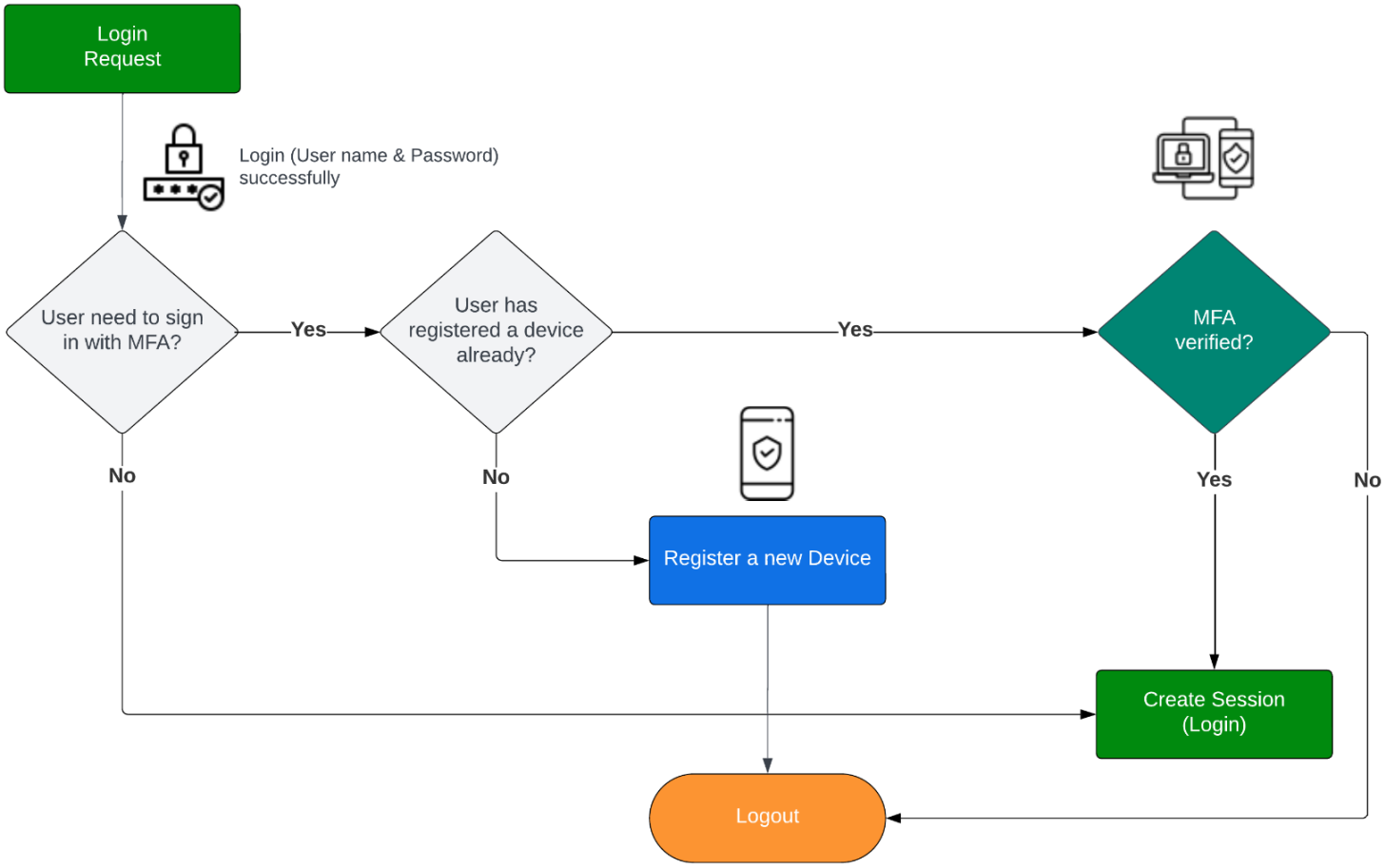


2. Enter MFA code

After the username and password have been successfully verified, the user needs to enter the random and temporary 6-digit number from the registered device (TOTP app) to log in to the Cornerstone portal.



Login Process



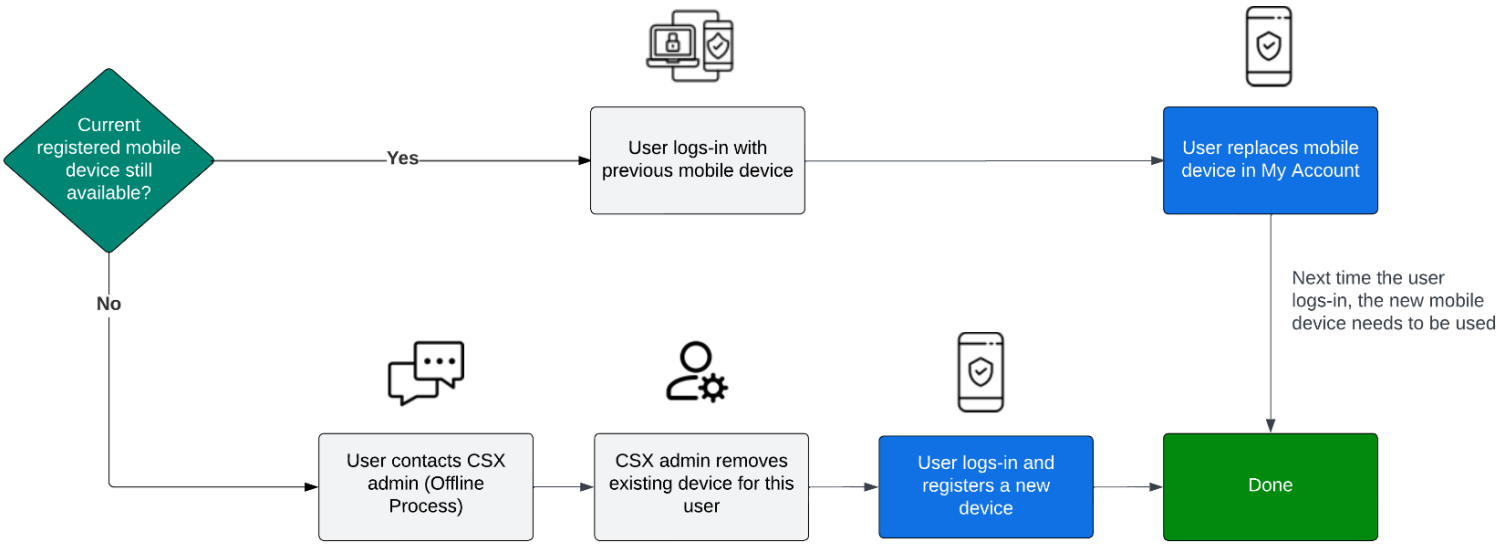
Replace Mobile Device

General

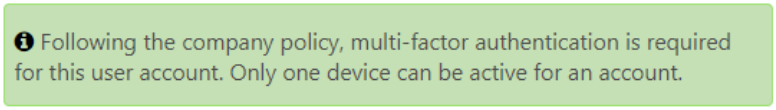
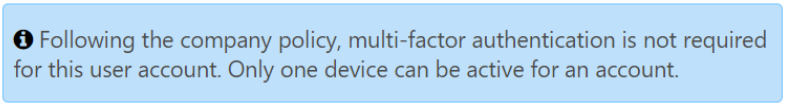
A mobile device can be replaced in two ways, depending on whether the previous mobile device is still available and working:

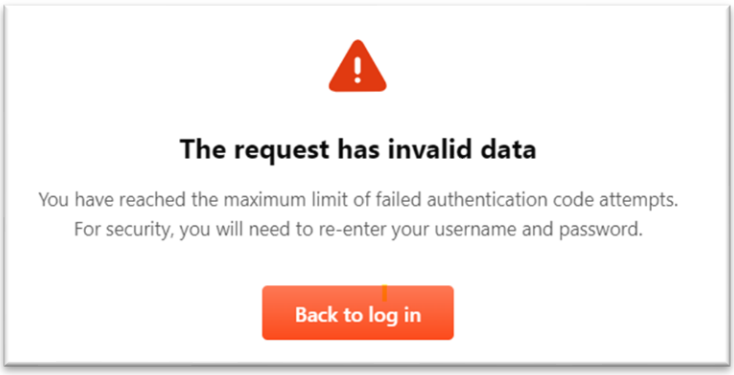
1. **Mobile device still available and working:**
   The user logs in with MFA and replaces the device in *My Account*.
2. **Mobile device not available/working anymore:**
   The user contacts the CSX administrator (offline process, e.g., via email or internal ticket system) to remove the existing mobile device from the user account. After the administrator has removed the device, the user can register a new mobile device as part of the login process.

Process



FAQ

Question	Answer
Is it possible for administrators to register a device on behalf of a user?	No, this is not possible for security reasons, not even when proxying into the system as another user (“proxy-as-a-user”).
How do I identify if a user is required to log in with MFA?	Users can navigate to My Account > MFA, and administrators can select a User record > MFA to display the current (user-specific) MFA setting. Green: MFA is required for the user.  Blue: MFA is not required for the user. 
Does the user require an email address to log in with MFA?	No, an email address is not required.

How many devices can be registered by each user?	Cornerstone MFA supports only one secret key, which will be created and associated with the user while registering a new device. Usually, this means one mobile device per user. However, while registering a new device, it is possible to register more mobile devices by simply re-using the same QR code or secret key. Example: When a user registers a mobile device using the QR code, the user can register (scan) two mobile devices using the same QR code.
What is the maximum number of MFA code attempts, and will the user account be locked after multiple failed MFA code attempts?	The account will not be locked, but after three failed attempts, the user needs to log in with a username and password again for authentication. 
MFA configuration: How long does it take before the changes made by an administrator take effect?	There could be a delay of up to 15 minutes due to various caching mechanisms before the new MFA configuration takes effect.

What should a user do if they must log in with MFA, but the MFA code does not work for some reason, or the mobile device is no longer available?	The user must contact the CSX administrator (offline process, e.g., email or ticket system). The CSX administrator has two options: • Remove the device from the user, so the user must register a new device as part of the first-time login process. • Add the user to the individual exception list for a certain period, so the user does not need to log in with MFA anymore but can replace the device in "My Account."
Is it possible to restore a device using the Secret Unique Key?	Yes, regardless of whether a user has registered the MFA device using a QR code or manually using the secret unique key, the user can (optionally) store the unique key securely. If a user loses access to the TOTP app, they can use the secret key to register a new device and regain access to their account.
If MFA is enabled for 'all users', is there any impact to service accounts used for integrations (APIs)?	No, there's no impact. MFA only has an impact on the standard login process, but it does not have an impact on any existing integration via APIs.
Is it possible to authorize a single authentication application? For example: Authorize users to use only Okta Verify but block Google Authenticator and Microsoft Authenticator.	The CSX-MFA solution supports the "TOTP algorithm," which is supported by many applications. There is no way to authorize or block specific TOTP applications. However, customers can create and point to a custom MFA online help page with clear instructions to end users on which single authentication applications should be used following your corporate policies.
The "skip on subsequent logins feature" has a default of 24 hours. Is this configurable?	No, the default is always 24 hours; this is not configurable.

Appendix

A. Implementation / Rollout Strategy

The Cornerstone MFA solution is easy to activate and can be rolled out within hours. However, your end users may not be familiar with the MFA registration or login process or may need additional support initially. In this case, you may want to consider a soft launch in introducing MFA to your users.

Various options are available for a CSX administrator to enable and roll out MFA.

Option	Description
Enable MFA for all users.	This option allows you to easily enable MFA for all users, meaning all users must log in with MFA. However, before enabling MFA for all users, you should consider announcing the go-live via appropriate communication procedures first. You should also consider providing sufficient training and enablement in advance.
Soft launch by Location or Division.	If you expect a certain level of end-user support while launching MFA, you can consider rolling out MFA by Location or Division to keep the support level manageable for your help desk. For example, you can enable MFA for the “United States” first before enabling MFA for “Europe,” or you can enable MFA for “Sales” first before enabling it for “Marketing.”
Create a custom corporate online help page.	The MFA online help link can be customized to point to a corporate online help page. In the custom online help page, you can provide additional instructions to help your users register a device and log in with MFA. For example, you can provide clear instructions on which TOTP app should be downloaded and used to log in with MFA.

B. Cornerstone Security Permissions

Permission Name	Permission Description	Category
MFA - Administration - View	Grants the ability to view the Multifactor Authentication (MFA) configuration. This permission cannot be constrained. This is an administrator permission.	Core
MFA - Administration - Manage	Grants the ability to configure Multi-Factor Authentication (MFA) preferences. This permission cannot be constrained. This is an administrator permission.	Core
MFA – Admin - User Device – View	Grants the ability to view the user device information in the system. Administrators can view the page for user records within their constraints. This permission can be constrained by OU, User's OU, User's Self, User Self and Subordinates, and User. This is an administrator permission.	Core
MFA – Admin - User Device – Manage	Grants the ability to manage the user device information in the system. Administrators can manage (delete) devices for user records within their constraints. This permission can be constrained by OU, User's OU, User's Self, User Self and Subordinates, and User. This is an administrator permission.	Core
Core Features Activation	Grants access to Core Feature Activation Preferences page.	Core

C. Data Privacy and Security Statements

Time-based one-time passwords (TOTP)

Cornerstone has implemented multi-factor authentication support in using time-based one-time passwords (TOTP). TOTP is a computer algorithm that generates a one-time password in using the current time and a shared secret key (seed, 32 bytes string, unique by user) as a source of uniqueness. This algorithm is an evolution of HMAC-based One-Time Password (HOTP) algorithm (RFC 4226) and has been adopted as Internet Engineering Task Force (IETF) standard (RFC 6238).

Personally Identifiable Information / GDPR

The MFA solution does not exchange or hold any additional Personally Identifiable Information (PII) data or Sensitive Personally Identifiable Information (SPII) data. Pseudonymization procedures are in place so that the data cannot be directly or independently linked to an individual .

Data in Transit

Data in transit will be encrypted with TLS 1.2+. Please check out the latest Cornerstone CSX Technology Overview for more information.

Preferences / Audit Logs

The MFA preferences & audit logs are stored on AWS S3. Data at rest in S3 will be encrypted using KMS Custom Managed Key (CMK). S3 buckets are hosted in the customer's AWS region.

Device Registration and Secret

The user's device registration and secret are stored on the AWS DynamoDB in the respective customer's AWS region.

Cookie

If the "skip multi-factor authentication for frequent login attempts" feature is enabled by an administrator, the application creates a Cookie ("sf_ma") with a Cornerstone-signed JSON Web Token (JWT) after the user successfully logs in. The cookie automatically expires after 24 hours. Within this period, the user (who created the cookie) is not required to log in with MFA.

FAQ

Question	Answer
What does a generated TOTP token (MFA code) look like, and how long is the token valid?	The token is a numeric value with six digits, valid for up to 30 seconds. This is not configurable.
What is “Data at Rest”?	Data at rest refers to data that is stored in a non-volatile location, such as a hard drive, solid-state drive, or other storage device.
What is “AWS S3”?	Amazon Simple Storage Service (Amazon S3) is a scalable and highly durable object storage service provided by Amazon Web Services (AWS). https://aws.amazon.com/s3
What is “AWS DynamoDB”?	AWS DynamoDB is a highly scalable, fully managed NoSQL database service. https://aws.amazon.com/dynamodb/
What is “Pseudonymization”?	Pseudonymization is a data protection technique that involves replacing or encrypting personally identifiable information (PII) with a pseudonym, or a placeholder, so that the data cannot be directly linked to an individual without additional information. This helps enhance privacy and security while still allowing for data analysis and processing. For example, the User ID: “123-456” becomes “XWSERSAFSDA”.
Does the Cornerstone MFA solution use any third-party providers?	No, the MFA solution does not use any third-party solution or is exchanging data with any third-party solution.