TitleWorkPlace MFA

FAQs and Troubleshooting Guide

June 10, 2022

Table of Contents

Introduction

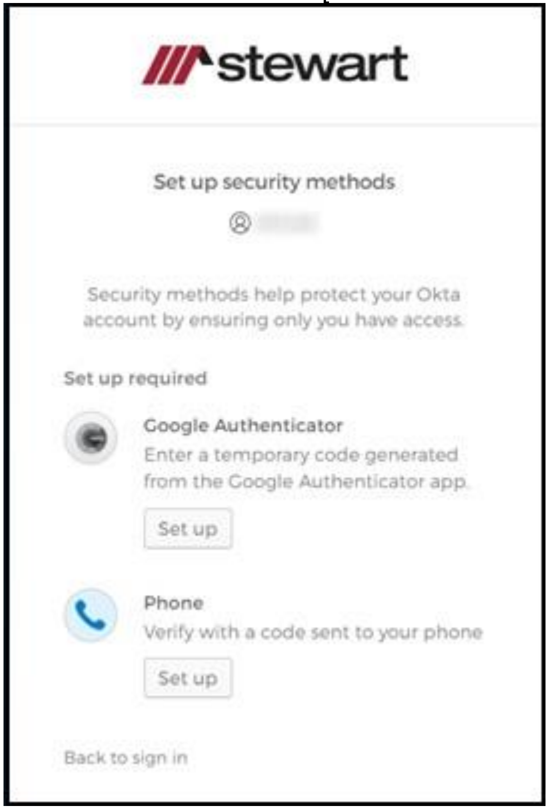
Stewart Title has partnered with **Okta** (https://www.okta.com) – a leading Identity and Access Management company, to enable **Multi-Factor Authentication (MFA)** for **TitleWorkPlace** end-users.

The purpose of this document is to provide enrollment steps, provide self-service options, and list frequently asked questions (FAQs) and common issues related to using **Okta MFA**.

Enroll / Configure MFA

1. Browse to: mfa.titleworkplace.biz
2. Enter your existing **TitleWorkPlace** username | **Next**
3. Enter your TitleWorkPlace password | **Verify**
4. If TWP account is set to force user set a new password, then you will see a password expiration screen and list of requirements for the new password.

   Enter new password | Click **Change Password**
5. Select one or more factors [We recommend choosing at least two]

   Set up security methods

   Security methods help protect your Okta account by ensuring only you have access.

   Set up required

   Google Authenticator
   Enter a temporary code generated from the Google Authenticator app.

   Set up

   Phone
   Verify with a code sent to your phone

   Set up

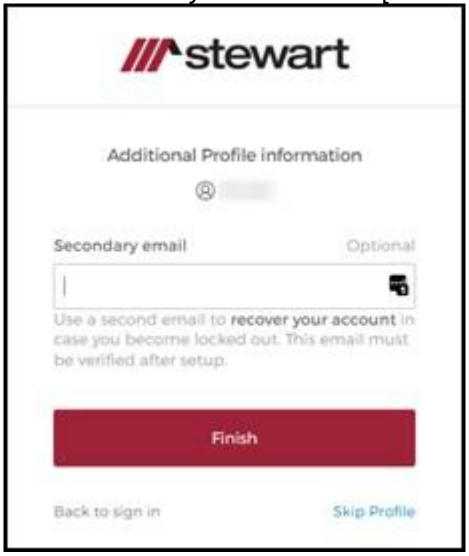
   Back to sign in
6. Available Factors:

   Google Authenticator – Mobile app which provides a time-based one-time-password as a second factor of authentication. Download the app first, and then launch it to scan the QR code on your screen.

Phone Voice Call - The Voice Call Authentication factor allows users to authenticate themselves using a one-time passcode (OTP) that is delivered in a voice call to the user's phone. Users can provide a phone number for a landline or mobile phone. Extension numbers for landlines are also supported.

Phone SMS - The SMS Authentication factor allows users to authenticate themselves using a one-time passcode (OTP) that is delivered to your phone in an SMS message.

7. Enter Secondary email address [used for account recovery] | **Finish**



stewart

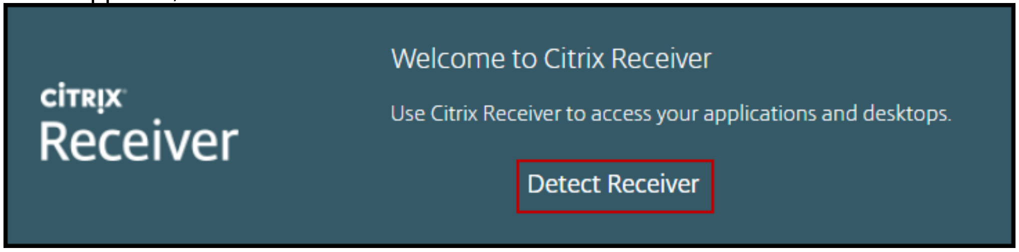
Additional Profile information

[redacted]

Secondary email — Optional

Use a second email to **recover your account** in case you become locked out. This email must be verified after setup.

8. **Note**: Check secondary email inbox to confirm the account.
9. If this appears, then click **Detect Receiver**



Welcome to Citrix Receiver

Use Citrix Receiver to access your applications and desktops.

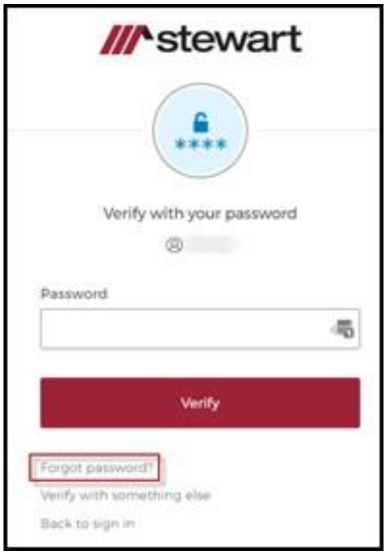
10. You will then see list of available Desktops/Apps on the TitleWorkPlace page.
11. Use mfa.titleworkplace.biz every day to access your applications in TitleWorkPlace.

Self-Service Features

Once you've confirmed the secondary email address in step #8 above, then you will be able to use the following self-service features.

Reset Password

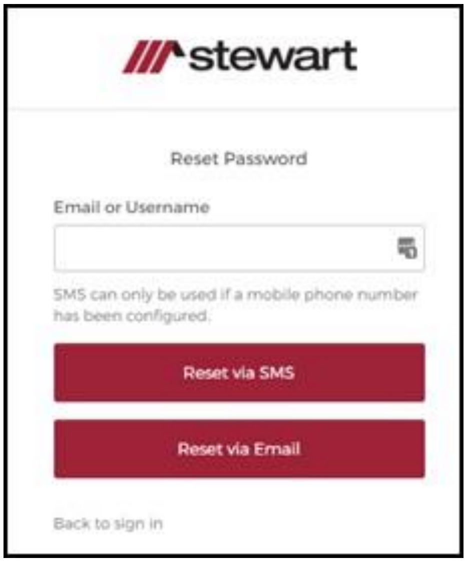
1. From the login screen mfa.titleworkplace.biz | click **Forgot Password.**



Verify with your password

Password

2. Enter TitleWorkPlace username | Select method to reset your TitleWorkPlace password



Reset Password

Email or Username

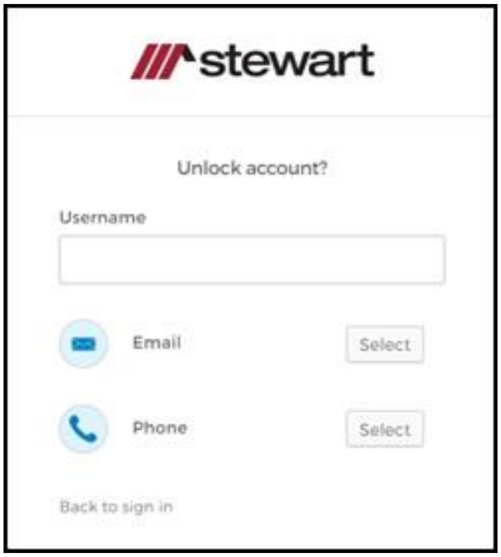
SMS can only be used if a mobile phone number has been configured.

3. An email will be sent to your backup/secondary email address. The link and code to reset the password expires 30 minutes after it was sent.

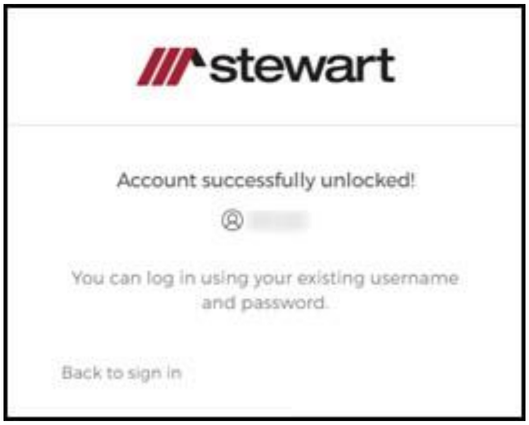
Unlock Account

TitleWorkPlace accounts are locked out after repeated failed login attempts. If you suspect your TitleWorkPlace account is locked out, then proceed with these steps to unlock it.

1. From the login screen mfa.titleworkplace.biz | click **Unlock Account**
2. Enter your TitleWorkPlace username | Select verification method.



3. If verification was successful, then you will receive the following confirmation:



Account successfully unlocked!

You can log in using your existing username and password.

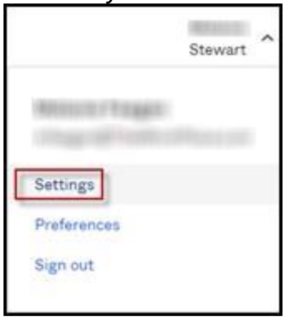
Dashboard

A dashboard is available to view your Okta account and make changes, such as adding or removing Security Methods: titleworkplace.okta.com

Logon with your TitleWorkPlace credentials to access this site.

Settings

Click on your name at the top-right then click on **Settings:**

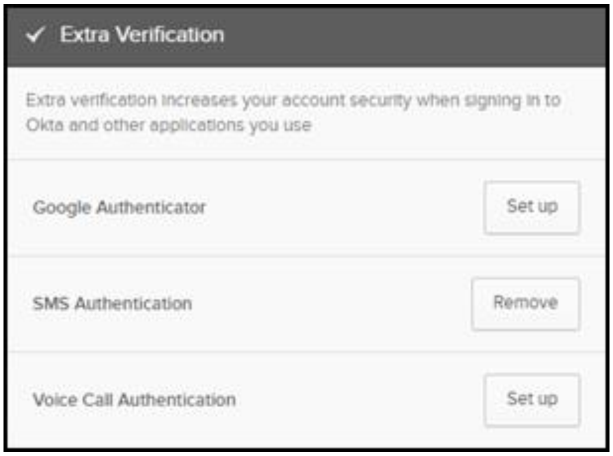


Personal Information

Click **Edit** to make changes to any section on this page: personal information, language, change TWP account password, and security methods.

Personal Information: You can edit secondary email and mobile phone ONLY. Cannot change other personal information, this is pulled from the system.

Security Methods: Remove or configure additional factors for your account.



✓ Extra Verification

Extra verification increases your account security when signing in to Okta and other applications you use

Google Authenticator

SMS Authentication

Voice Call Authentication

Okta How-To/Troubleshooting FAQs

How do I register a new device for MFA?

To register a new device, login to the Okta dashboard using existing TitleWorkPlace credentials: titleworkplace.okta.com

At the top-right, click the drop-down icon next to your name, go to **Settings**.

Scroll down to **Security Methods** to make changes to existing enabled factor methods or Set Up new.

What if I am unable to use a previously configured factor method?

If you previously configured an additional factor, such as SMS Text, and you are unable to use that device, then contact the **Agency Support Center** at **(844) 835-1200** and request to have MFA reset on your account. Once complete, then proceed to the login page (mfa.titleworkplace.biz), sign-in, and you will be prompted to re-enroll.

I am stuck on the "Enrolling Your Device" screen

If you get stuck in a loop when attempting to register via SMS/Email/QR code, or you are not getting any code to enter or any push notification, it means your device may not have enrolled correctly. In this case, you need to contact the **Agency Support Center** to have MFA reset on your account. Once complete, then proceed to the login page (mfa.titleworkplace.biz), sign-in, and you will be prompted to re-enroll.

Why do I keep seeing MFA prompts?

If you continue to see MFA prompts after selecting "Do not challenge me on this device again," it could be for a few different reasons:

1. Cookie management: The "Do not challenge me again" choice is captured in a browser cookie. If you've recently cleared your cookies, or are using a new browser (like Chrome, Internet Explorer, Mozilla Firefox), it won't remember the choice.
2. Policy configuration: Your Okta administrator sets how often they want MFA challenge prompts to appear. You will receive MFA prompt per device with session expiring after 2 hours.
3. Exempted action: Certain actions, like editing your account profile, will always trigger an MFA prompt as an additional layer of security.

General MFA FAQs

What is Multi-Factor Authentication (MFA)?

Multi-Factor Authentication is a security practice that requires more than one method of authentication, using independent categories of credentials to verify a user's identity. For example, you may log in to a system using your password ("what you know") and then verifying a separate six-digit number that is sent to your phone ("what you have"). By combining "what you know" and "what you have" verification, the hackers will have harder time breaking into our systems as they may not have both your password and your phone.

What is a security "factor"?

The "factor" in MFA refers to a method of verifying your identity. The most basic type of factor is your password, which is often the primary, or initial authentication factor you'll be prompted for. Stewart Title has selected multiple additional "factor" options for TitleWorkPlace:

Google Authenticator- An app you download onto your phone. It generates a code you use to sign into TitleWorkPlace.

Phone Options

SMS - Okta sends a text message to your phone with a code that you then type into the website.

Voice - Voice authentication replaces SMS when a phone number can't receive text messages. Instead, the code comes through as a robotic voice on the other end of the line.

What is Google Authenticator?

Google Authenticator is a mobile application from Google that can be used to verify a user for MFA purposes. You receive a push notification on your mobile to confirm the second factor after the factor is set up.

Why is MFA required?

MFA is an effective way to provide enhanced security. Traditional usernames and passwords can be stolen, and they've become increasingly more vulnerable to malicious activity, and cyber-attacks like phishing or brute force attacks. MFA creates multiple layers of security to help increase the confidence that the user requesting access is who they claim to be.

Reports show that applications and identities are the initial targets in 86% of breaches. It has become a necessity to protect our applications and identities through a second layer of security.

Why isn't primary authentication enough, what's wrong with passwords?

One set of login credentials (such as username and password) is not solving important access challenges.

Passwords, in addition to being difficult to manage, are vulnerable to a variety of attacks like phishing, social engineering, etc.

By boiling all applications down to one username and password, security strength is only as strong as that one set of credentials. If it's a bad password, your security situation hasn't improved.

If hackers get a hold of a user’s login credentials, they can access all the user’s resources. This is especially a threat if that user has access to privileged information or mission-critical data.

What are the benefits of MFA?

Lower the chances of end-user identities (and, subsequently, their IT resources) becoming compromised.

Even if hackers have a user’s password, we can stop them by adding a personal, time-sensitive factor to the authentication process.

Peace of mind for enterprise, knowing that users’ sensitive data is made safer by an additional security layer.

MFA also adds a sense of mindfulness to authentication. By taking the time to add their second factor, users are reminded of the importance of tight identity security.

How does Okta keep MFA factors secure?

Okta encrypts your user credentials using two different software locks called keys. It stores user data and the keys used to unlock that data in separate databases. For extra security, it then encrypts the keys in three different ways for even stronger protection. No one person at Okta can access the encrypted master key, and Okta maintains an audit trail to show how it manages the keys.

Which MFA factors does Okta support?

Okta supports several factors. The factors available for TitleWorkPlace are: Login codes sent via mobile app (Google Authenticator), SMS text, or voice call.

Do I need to set up MFA again if I registered previously?

No. Once done or configured, you need not set up a factor again.

Can I turn off MFA?

If your administrator has enabled MFA, you can’t choose to opt out. That would leave a huge hole in the organization’s security and leave everyone’s data vulnerable to an attack.

How do I access Okta-integrated applications?

Users can go to mfa.titleworkplace.biz, sign in, and then choose the application or desktop they want to access.