



Applied Cloud MFA

User Guide

Last updated: December 16, 2022

Copyright © 2022 by Applied Systems, Inc., 200 Applied Parkway, University Park, IL 60484. All rights reserved. Reproduction or transmission is expressly prohibited unless authorized by Applied in writing. Specific product information regarding Applied Epic® and related products and services, including any related documentation are the exclusive property of Applied and Applied retains all right, title, and interest therein. No endorsement or ownership of third-party products or services should be implied by their mention and use. All trademarks, product names, and logos appearing herein are the property of their respective owners. All workflows are suggested and common workflows. Users of this material agree that Applied Systems cannot be held liable for any omissions or errors within the guide.



Contents

About This Document.....	3
Adding an Email Address for MFA	4
Adding an email as an administrator	4
Setting Up Multi-Factor Authentication	4
Okta Verify	4
Google Authenticator	10
SMS	11
Voice Call	11
Email	12
Logging in with MFA.....	13
Okta Verify	13
Google Authenticator	15
SMS	15
Voice Call	15
Email	15
Unlocking an Okta Account	16
Changing Your Authentication Method	16
Setting Up a New Device with MFA	17
Adding New Employees to MFA	18

About This Document

To enhance system security, we have enabled multi-factor authentication (MFA) for Applied Cloud products using Okta for identity and access management.

To use MFA, you must complete the following steps:

1. Provide an email address that is accessible outside of your Applied Cloud remote desktop session.
2. Select a preferred method of authentication.
3. Complete your MFA setup.

This document includes instructions for you to set up your Okta account to use MFA to verify your identity when using Applied Cloud products.

Adding an Email Address for MFA

Multi-factor authentication requires a unique email address for each user to directly communicate with that user. A business email address is preferred for MFA and must be accessible outside of your Applied Cloud remote desktop session.

All users must have an email address associated with their accounts.

Adding an email as an administrator

1. Open Applied Cloud Management (ACM).
2. Select the user and enter a **Business Email** in the *ACM – Account Properties* window.
3. Click **Save**.

Setting Up Multi-Factor Authentication

As part of your MFA setup, you must choose a method of authentication. This is the second factor the system uses to verify your identity when you sign in to your account. Applied Systems recommends using the Okta Verify app as your MFA option.

Note: If you are on private cloud, the AppAdmin account also requires MFA.

Choose one of the following methods to use for multi-factor authentication on your account.

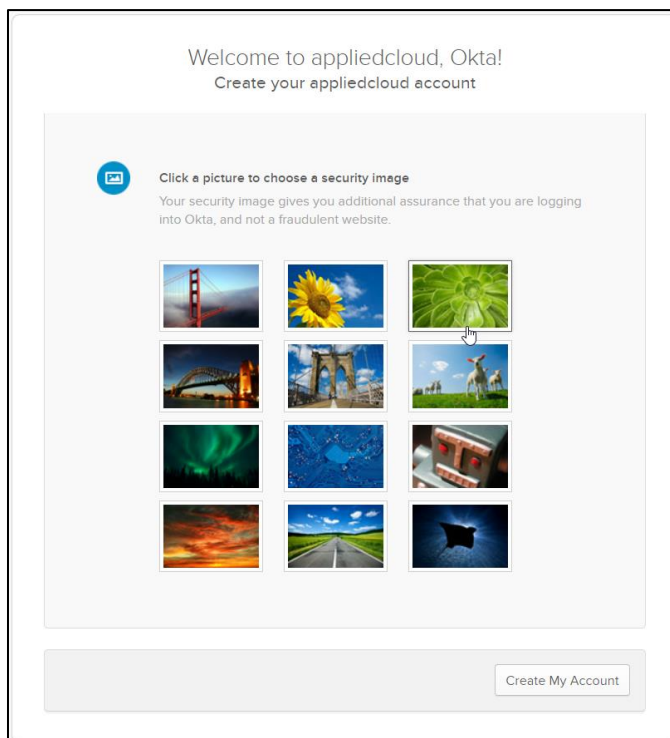
- **Okta Verify:** Requires you to install the Okta Verify app on your smart device.
- **Google Authenticator:** Requires you to install the Google Authenticator app on your smart device.
- **SMS:** Requires you to have an SMS enabled device that can receive text messages.
- **Voice Call:** Requires you to have a device that can receive phone calls.
- **Email:** Requires access to a business email address outside the RDP (Cloud) environment – such as accessing email locally using a desktop or smart device.

Okta Verify

The Okta Verify app is the recommended method for MFA. This option pushes a notification to the Okta Verify app on your device when you sign in to your account. Once you verify that it's you in the app, you are signed in to Applied Cloud.

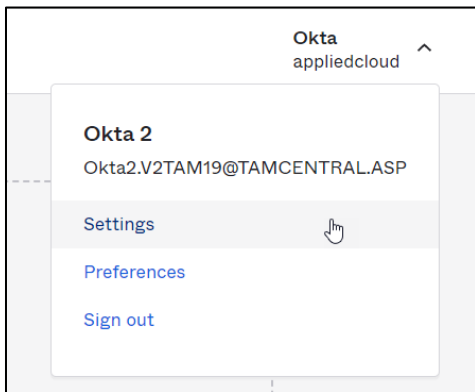
To set up Okta Verify as your MFA method:

1. Download and install the Okta Verify application from the Apple App Store or Google Play on your smart device.
2. Go to <https://appliedcloud.okta.com> from a web browser on your computer.
3. Enter your Applied Cloud **Username** and **Password** and click **Sign In**. Do not include your domain name (for example, \TAMCENTRAL) when entering your username.
4. Enter a secondary email address, if you have one.
5. Choose a security question and type the response. You can also select **Create your own security question** from the dropdown to add your own question.
6. Select a *security image*. This image displays each time you log in to your account.

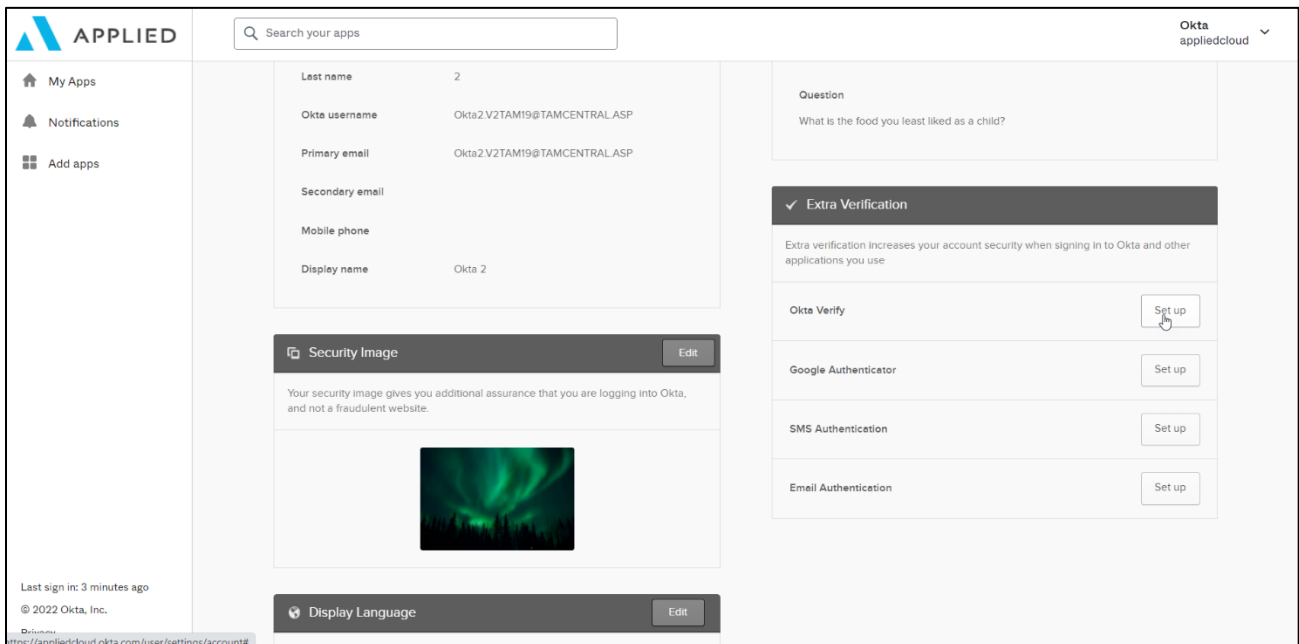


7. Click **Create My Account**.
8. Click the **Profile icon** for your name on the *Okta Dashboard*.

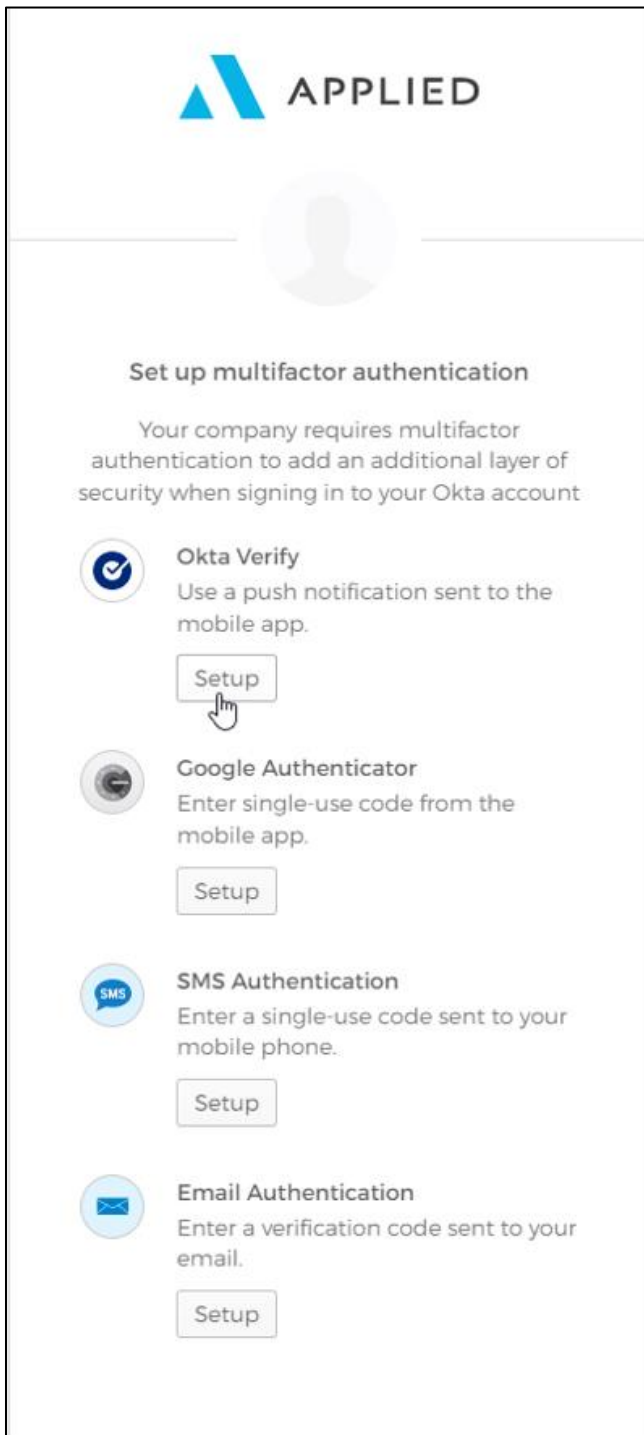
9. Select **Settings**. The *Account Settings* page displays.



10. Under the *Extra Verification* section, click **Setup** next to Okta Verify.



11. When you are prompted to setup Okta Verify, click **Setup**.



 APPLIED

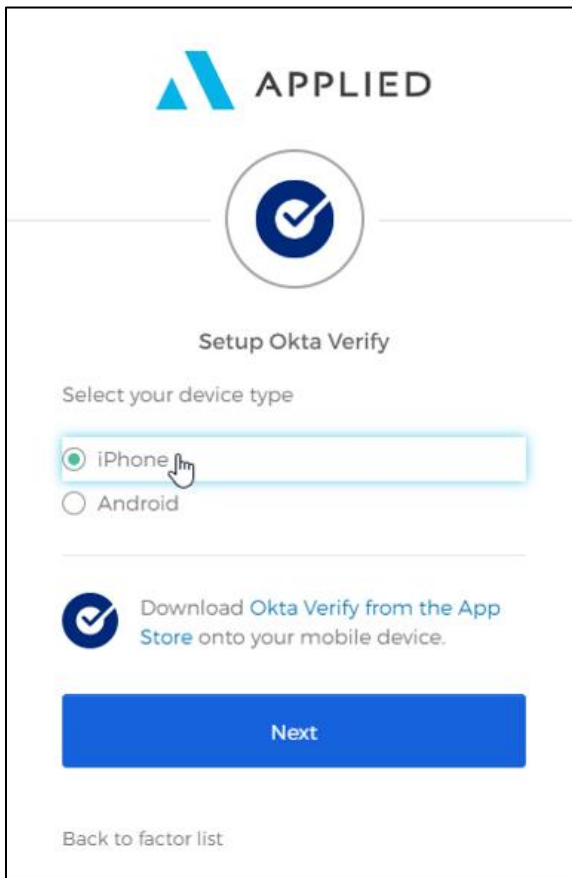


Set up multifactor authentication

Your company requires multifactor authentication to add an additional layer of security when signing in to your Okta account.

-  **Okta Verify**
Use a push notification sent to the mobile app.
-  **Google Authenticator**
Enter single-use code from the mobile app.
-  **SMS Authentication**
Enter a single-use code sent to your mobile phone.
-  **Email Authentication**
Enter a verification code sent to your email.

12. Select either **iPhone** or **Android** as the smart device you are using.



APPLIED

Setup Okta Verify

Select your device type

☒ iPhone

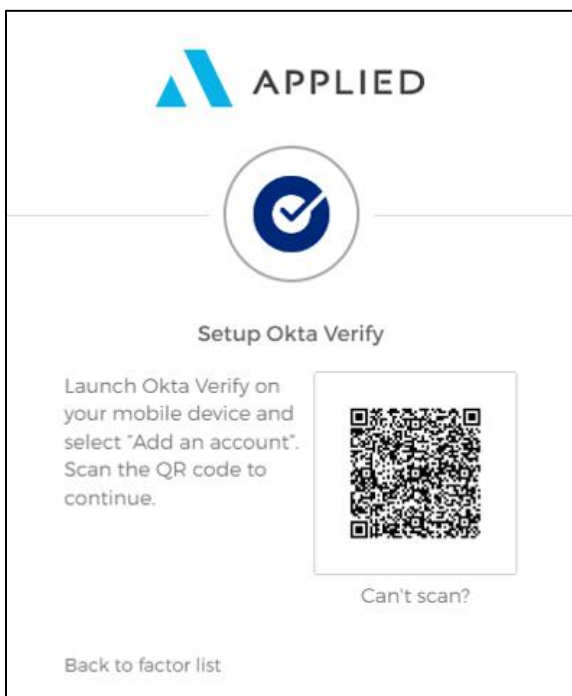
☐ Android

Download Okta Verify from the App Store onto your mobile device.

Next

Back to factor list

13. Click **Next**. A QR code displays.



APPLIED

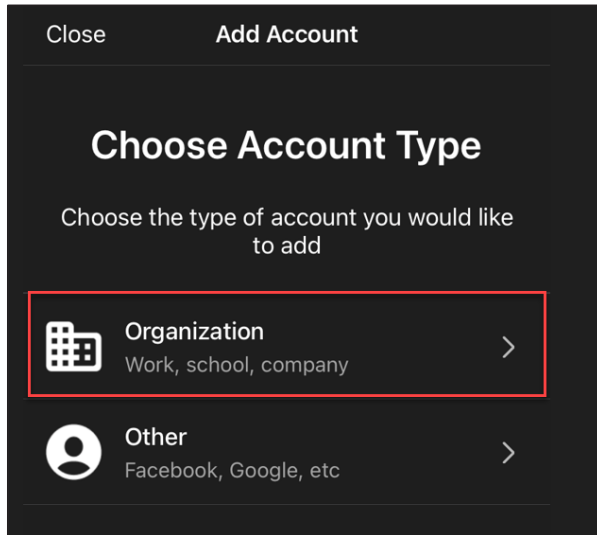
Setup Okta Verify

Launch Okta Verify on your mobile device and select "Add an account". Scan the QR code to continue.

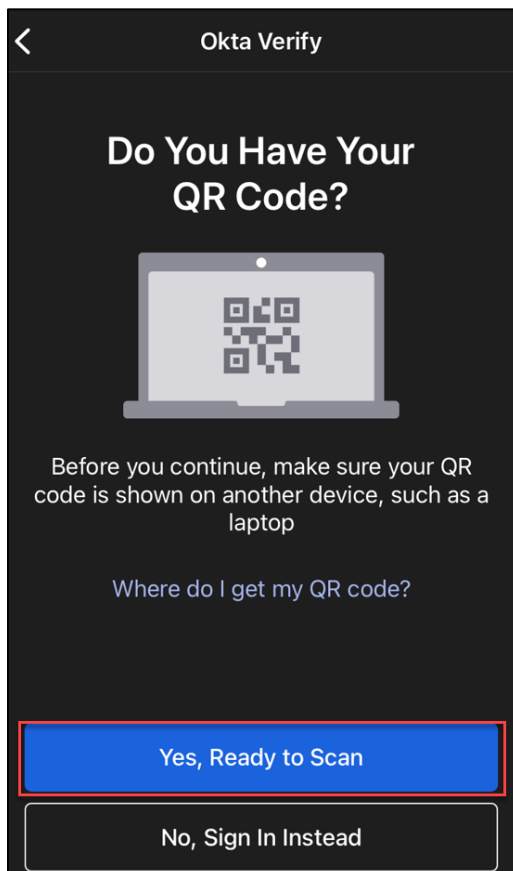
Can't scan?

Back to factor list

14. Open the Okta Verify application on your smart device.
15. Tap **[+]** at the top of the application to add a new account.
16. On the *Choose Account Type* screen, select **Organisation**.



17. Tap **Yes, Ready to Scan** when prompted. Scan the QR code displayed on the website.



18. Click **Done** once you receive the *Account Added* message. The account is added to your Okta Verify app.

You may want to bookmark <https://appliedcloud.okta.com> in your browser. If you lose or replace the device you enabled with Okta Verify, you will need to navigate to this page to update your settings.

Google Authenticator

When you select Google Authenticator as your MFA method, you receive a push notification to the Google Authenticator app on your device when you sign in to your account. Once you verify that it's you in the app, you are signed in to Applied Cloud.

To set up Google Authenticator as your MFA method:

1. Go to <https://appliedcloud.okta.com> from a web browser on your computer.
2. Enter your Applied Cloud **Username** and **Password** and click **Sign In**. Do not include your domain name (For example, \TAMCENTRAL) when entering your username.
3. Enter a secondary email address, if you have one.
4. Choose a security question and type the response. You can also select **Create your own security question** from the dropdown to add your own question.
5. Select a *security image* and click **Create My Account**.
6. Select **Settings**. The *Account Settings* page displays.
7. Under the *Extra Verification* area, click **Setup** next to *SMS Google Authenticator*.
8. Click **Setup** under *Google Authenticator* in the *Setup multifactor authentication* page.
9. Select either **iPhone** or **Android** as the smart device you are using and click **Next**. A QR code displays.
10. Open the Google Authenticator application on your smart device.
11. Tap **[+]** at the top of the application to add a new account.
12. Select **Scan a QR Code** and scan the QR code displayed on the website. Your account is added to Google Authenticator.
13. Click **Next** in the Okta webpage.
14. Enter the six-digit **code** displayed in Google Authenticator and click **Verify**.

You may want to bookmark <https://appliedcloud.okta.com> in your browser. If you lose or replace the device you enabled with Google Verify, you will need to navigate to this page to update your settings.

SMS

When you select SMS (or text messaging) as your MFA method, you receive a text to the number you have linked to your account when you sign in to your account. Once you enter the code received via text, you are signed in to Applied Cloud.

To set up SMS as your MFA method:

1. Go to <https://appliedcloud.okta.com> from a web browser on your computer.
2. Enter your Applied Cloud **Username** and **Password** and click **Sign In**. Do not include your domain name (For example, \TAMCENTRAL) when entering your username.
3. Enter a secondary email address, if you have one.
4. Choose a security question and type the response. You can also select **Create your own security question** from the dropdown to add your own question.
5. Select a *security image* and click **Create My Account**.
6. Select **Settings**. The *Account Settings* page displays.
7. Under the *Extra Verification* area, click **Setup** next to *SMS Authentication*.
8. Click **Setup** under *SMS Authentication* in the *Setup multifactor authentication* page.
9. Select the appropriate country code and enter your 10 digit phone number, starting with the area code.
10. Click **Send Code**. SMS messaging and data rates may apply.
11. Enter the code sent to you via SMS and click **Verify**.

You may want to bookmark <https://appliedcloud.okta.com> in your browser. If you change your phone number, you will need to navigate to this page to update your settings.

Voice Call

When you select voice call as your MFA method, you receive a voice call to the number you have linked to your account when you sign in to your account. Once you enter the code received via phone call, you are signed in to Applied Cloud.

1. Go to <https://appliedcloud.okta.com> from a web browser on your computer.

2. Enter your Applied Cloud **Username** and **Password** and click **Sign In**. Do not include your domain name (For example, \TAMCENTRAL) when entering your username.
3. Enter a secondary email address, if you have one.
4. Choose a security question and type the response. You can also select **Create your own security question** from the dropdown to add your own question.
5. Select a *security image* and click **Create My Account**.
6. Click the **Profile icon** that has your name displayed.
7. Select **Settings**. The *Account Settings* page displays.
8. Under the *Extra Verification* area, click **Setup** next to *Voice Call Authentication*.
9. Click **Setup** under *Voice Call Authentication* in the *Setup multifactor authentication* page.
10. Select your **Country** and enter your **Phone number** and **Extension**, if applicable.
11. Click **Call**.
12. Enter the code sent to your phone via automated message and click **Verify**.

Email

When you select email as your MFA method, you receive an email to the email address associated with your account every time you log in to the Applied Cloud. See [Adding an Email Address for MFA](#) for information on how to add an email to your account. You must have access to this email address outside of your RDP (Cloud) environment – either locally on your desktop or via your smart device. Once you enter the code received via email, you are signed in to Applied Cloud.

To set up email as your MFA method:

1. Go to <https://appliedcloud.okta.com> from a web browser on your computer.
2. Enter your Applied Cloud **Username** and **Password** and click **Sign In**. Do not include your domain name (For example, \TAMCENTRAL) when entering your username.
3. Enter a secondary email address, if you have one.
4. Choose a security question and type the response. You can also select **Create your own security question** from the dropdown to add your own question.
5. Select a *security image* and click **Create My Account**.

6. Click the **Profile icon** that has your name displayed.
7. Select **Settings**. The *Account Settings* page displays.
8. Under the *Extra Verification* area, click **Setup** next to *Email Authentication*.
9. Click **Setup** under *Email Authentication* in the *Setup multifactor authentication* page.
10. Click **Send me the code**.
11. Enter the code sent to you via email and click **Verify**. The code is sent to the email you previously entered for Applied Cloud.

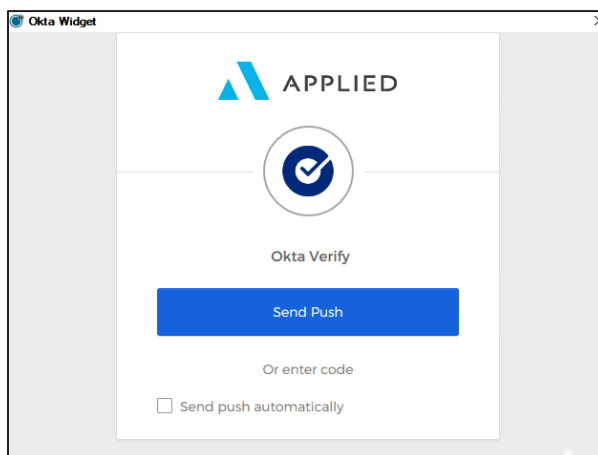
You may want to bookmark <https://appliedcloud.okta.com> in your browser. If you change your email address, you will need to navigate to this page to update your settings.

Logging in with MFA

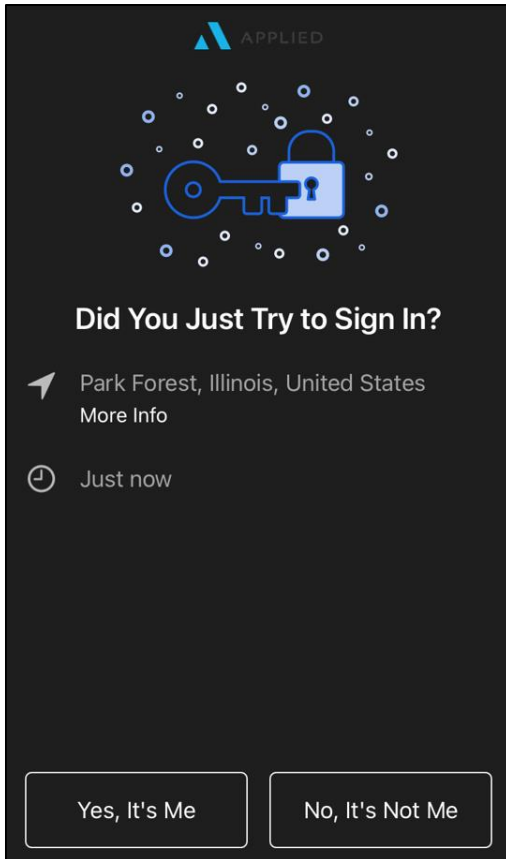
After you have set up a method of MFA, you can log in with MFA. The following section describes how to log in to Applied Cloud using each MFA method.

Okta Verify

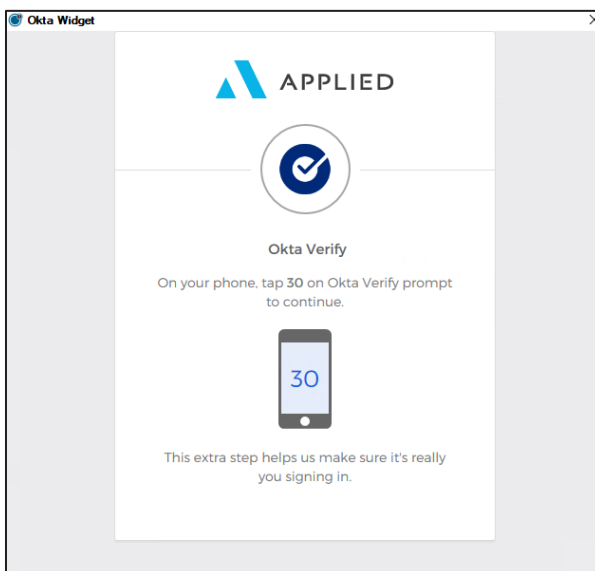
1. Log in to Applied Cloud with your **Username** and **Password**.
2. Click **Send Push** on the *Okta MFA* screen. A push notification is sent to your phone. The **Send push automatically** checkbox is not functional at this time.



3. Click **Yes, it's me**.



4. The first time you log in from a new location, the Okta Verify app displays three numbers on your phone. Select the **number** that matches the one shown on the *Okta MFA* screen on your Applied Cloud session. When you choose the correct number, you are logged in.



Google Authenticator

1. Log in to Applied Cloud with your ***Username*** and ***Password***.
2. In the *Applied Okta MFA* screen, enter the six-digit ***code*** displayed in Google Authenticator. When you enter the correct six-digit code, you are logged in.

SMS

1. Log in to Applied Cloud with your ***Username*** and ***Password***.
2. In the *Applied Okta MFA* screen, click ***Send code***.
3. Enter the ***code*** sent via SMS and click ***Verify***. When you enter the correct six-digit code, you are logged in.

Voice Call

1. Log in to Applied Cloud with your ***Username*** and ***Password***.
2. In the *Applied Okta MFA* screen, click ***Call***.
3. Enter the ***code*** sent via phone call and click ***Verify***. When you enter the correct five-digit code, you are logged in.

Email

1. Log in to Applied Cloud with your ***Username*** and ***Password***.
2. In the *Applied Okta MFA* screen, click ***Send me the code***.
3. Enter the ***code*** sent via email and click ***Verify***. When you enter the correct six-digit code, you are logged in.

Unlocking an Okta Account

If you use Okta Verify as your MFA method, you can unlock your account if it has been locked. An account may become locked after multiple failed attempts to verify. You must have a security question set up to unlock your account. You are prompted to set a secondary email address and security question when you log into your Okta account. If you have not set up a security question or forgot your answer, contact Applied Support to unlock your account.

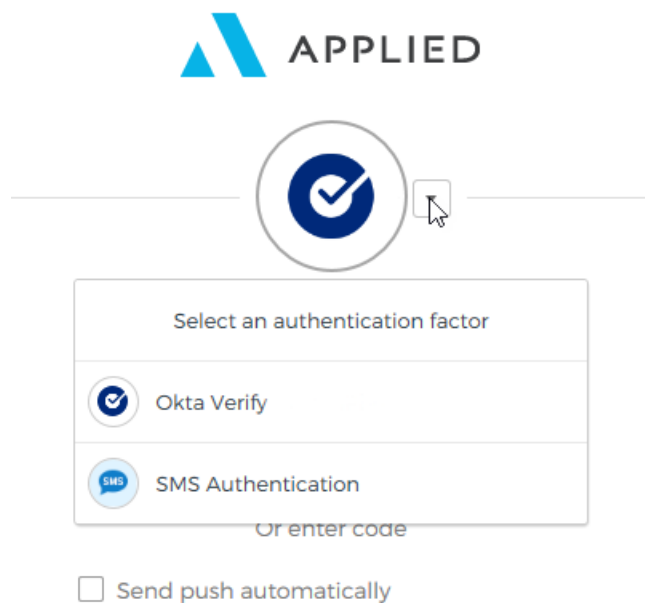
1. Go to <https://appliedcloud.okta.com> from a web browser on your computer.
2. Click **Need Help Signing in?** below the *Sign In* button.
3. Click **Unlock Account?**
4. Enter your Okta username, or your primary or secondary email address and click **Send Email**. An email is sent to the associated email address.
5. Navigate to the email and click the **Unlock Account** button.
6. Enter the answer to your security question and click **Unlock Account**.
7. Click **Back to Sign In** to try logging in again.

Changing Your Authentication Method

If needed, you can switch your authentication method or enable additional methods by completing the following steps:

1. Go to <https://appliedcloud.okta.com> from a web browser on your computer.
2. Enter your Applied Cloud **Username** and **Password** and click **Sign In**. Do not include your domain name (for example, \TAMCENTRAL) when entering your username.
3. Click the **Profile icon** for your name on the *Okta Dashboard*.
4. Select **Settings**. The *Account Settings* page displays.
5. Click **Edit Profile**. You may be prompted to verify your password.
6. Under the *Extra Verification* section, click **Set up** next to the authentication method you want to enable.
7. Follow the on-screen prompts to verify your authentication method. Enter the verification code sent to you.

You can enable multiple methods of authentication. When you go to authenticate, click the dropdown arrow to select which authentication method to use.



Setting Up a New Device with MFA

If you need to set up MFA on a new device, such as a new phone, complete the following steps while you still have your old device that is set up with MFA.

If you do not have access to your previous device that is set up with MFA, contact Applied Support.

Okta Verify can only be enabled on one device at a time.

1. Go to <https://appliedcloud.okta.com> from a web browser on your computer.
2. Enter your Applied Cloud **Username** and **Password** and click **Sign In**. Do not include your domain name (for example, \TAMCENTRAL) when entering your username.
3. Click the **Profile icon** for your name on the Okta Dashboard.
4. Select **Settings**. The Account Settings page displays.
5. Click **Edit Profile**. You may be prompted to verify your password.
6. Under the *Extra Verification* section, click **Remove** next to any enabled authentication methods. This removes your current device from your MFA account. You will not be able to log in to Applied Cloud when your authentication methods have been removed. If you need access to Applied Cloud during this time, you can use another device, such as a tablet, to set up MFA.
7. If you are using Okta Verify or Google Authenticator, go to the app and choose the account entry set up with the old device. Select **Delete Account**.

8. Once you have your new device, follow the steps for [setting up MFA](#).

Adding New Employees to MFA

To set up new employees to use MFA, complete the following steps:

1. An office administrator must enter the new user's email when creating their account. Wait 60 minutes before proceeding to the next step.
2. Select a preferred method of authentication. For more information, see [Setting Up Multi-Factor Authentication](#).