**Enabling Screen Lock Confirmation for Okta Verify App**

**Table of Contents**

1. [Introduction and Purpose](#introduction-and-purpose)
2. [When will this change take place](#Change_date)
3. [Screen Lock Data and Privacy](#screen-lock-data-and-privacy)
4. [Summary of Key Steps](#summary-of-key-steps)
5. [For Existing Users with Screen Lock Enabled](#for-existing-users-with-screen-lock-ena)
6. [For Existing Users Without Screen Lock Enabled](#for-existing-users-without-screen-lock-)
7. [Detailed End-User Instructions](#detailed-end-user-instructions)
   * [For iOS Users](#for-ios-users)
   * [For Android Users](#for-android-users)
8. [End-User Experience with Screen Lock Confirmation](#end-user-experience-with-screen-lock-co)
9. [Troubleshooting](#troubleshooting)
10. [Support](#support)
11. [Additional Resources](#additional-resources)

**Introduction and Purpose**

Enabling screen lock confirmation for the Okta Verify app is a critical security enhancement designed to ensure that only authorized users can approve authentication requests. This feature protects against unauthorized access in scenarios where a device is lost or stolen, adding an extra layer of security by requiring screen lock verification (such as Face ID, Touch ID, or a device password, PIN or pattern for android). By implementing screen lock confirmation, organizations can significantly reduce the risk of unauthorized access.

**When will this change take place**

This feature will be enabled (go-live) on November 15th, 2024 at 9:00 AM ET

**Screen Lock Data and Privacy**

Your screen lock data (e.g., fingerprints, facial recognition, passcodes) is never transmitted to Okta or your organization. Instead, it is securely stored locally on your device within the device's trusted hardware, such as the Secure Enclave on iPhones. Okta only receives a verification response from your device indicating whether the authentication was successful or not. This ensures that neither Okta nor your organization has access to your screen lock data, maintaining your privacy and security.

**Summary of Key Steps**

1. Back up your device data (recommended).
2. Remove existing Okta Verify account.
3. Reinstall Okta Verify app (if needed).
4. Set up a new Okta Verify account.
5. Enable screen lock confirmation.
6. Test the new setup.

Estimated time to complete: 5-10 minutes

**For Existing Users with Screen Lock Enabled currently in Okta verify app**

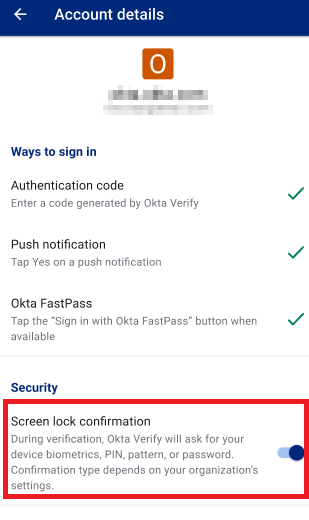
If you already have screen lock confirmation enabled in the Okta Verify app, no further action is required. Your current setup continues to function seamlessly with the enhanced security policies. This ensures that your authentication process remains secure without any additional steps.

**For Existing Users Without Screen Lock Enabled in Okta verify app**

If you have not yet enabled screen lock confirmation, you will need to remove and re-add your Okta Verify account to apply the new security settings. Follow the detailed steps below for both Android and iOS users.

**Check if the screen lock confirmation is enabled on not currently on your device:**

Open OKTA verify App on your mobile device.  
Click on the your account shown in the okta verify app.   
  
Under Security section:  
If the radio button for “Screen Lock confirmation” is “Checked”, you are good to go! (image below)



**Detailed End-User Instructions for Enabling Screen Lock Confirmation in Okta Verify**

**For iOS Users**

**Step 1: Remove the Existing Okta Verify Account**

1. Open the Okta Verify app on your iPhone.
2. Tap on your account, typically identified by your organization's name or your email address.
3. Scroll to the bottom of the screen and tap **Remove Account**.
4. Confirm the removal when prompted.

**Step 2: Reinstall Okta Verify (\*Optional)**

* If you have uninstalled Okta Verify, download it again from the App Store.

**Step 3: Begin New Okta Verify Setup**

1. Open the Okta Verify app.
2. Tap **Add Account** to initiate the setup process.
3. When prompted, enter your organization’s sign-in URL (e.g., example.okta.com).
4. Authenticate with your userid and password.

**Step 4: Enable Face ID or Passcode Confirmation**

1. Okta Verify will prompt you to enable Face ID (for iPhone X and later) or Touch ID (for iPhone models with a fingerprint sensor).
2. Tap **Enable** and follow the on-screen instructions to allow Okta Verify to use Face ID/Touch ID or a device passcode.
3. If you haven’t set up screen lock, Okta Verify will guide you to the iOS Settings app to configure either Face ID or a passcode.

**Step 5: Test Authentication**

1. Log in to a protected app using Okta Verify.
2. Approve the push notification using Face ID, Touch ID, or your device passcode.

**For Android Users**

**Step 1: Remove the Existing Okta Verify Account**

1. Open Okta Verify on your Android device.
2. Tap on your account.
3. Tap **Remove Account** and confirm.

**Step 2: Download and Install Okta Verify**

* Download Okta Verify from the Google Play Store.
* Install and open the app.

**Step 3: Begin New Okta Verify Setup**

1. Tap **Add Account**.
2. Tap **No, sign in instead**.
3. Enter your organization’s sign-in URL (e.g., example.okta.com).
4. Authenticate with your userid and password.

**Step 4: Enable Screen Lock Confirmation**

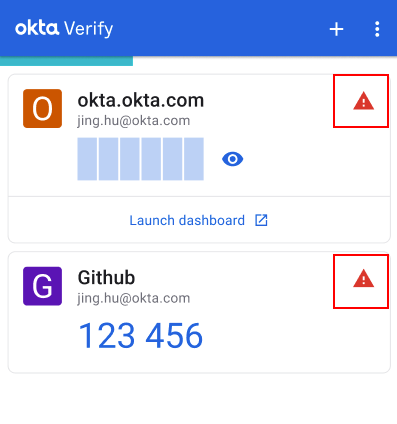
1. Okta Verify will prompt you to enable biometric (fingerprint, face unlock) or device screen lock (PIN, pattern, password).
2. Follow on-screen instructions to set up fingerprint, face unlock, or screen lock.
3. If your device does not support biometrics, you must set up a PIN, pattern or passcode.

**Step 5: Test Authentication**

1. Log in to a protected app using Okta Verify.
2. Approve the push notification using biometrics or your screen lock method.

**What will happen if I don’t enable screen lock confirmation before the go-live date.**

You will NOT be able to use PUSH or the 6 digit code from the OKTA verify app to log in to VPN or other applications. You will only be able to use TEXT / SMS as the second factor option.  
  
You will see a red warning sign next to your account in the OKTA verify app next to your account.   
(image below)

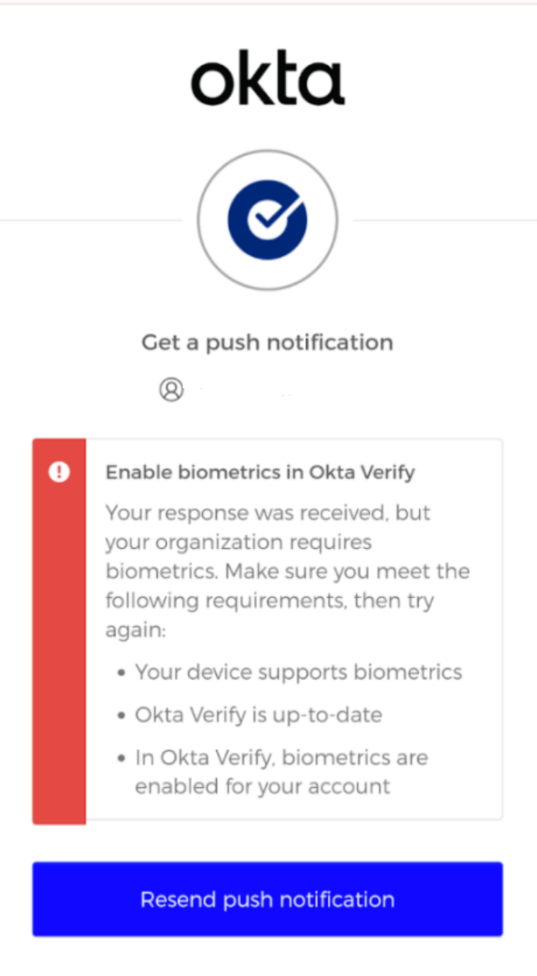


When you login into any website and try to send a PUSH notification you will see an error on the web page stating:

**Enable biometrics in Okta Verify**  
Your response was received, but your organization requires biometrics. Make sure you meet the following requirements, then try again:

* Your device supports biometrics
* Okta Verify is up-to-date
* In Okta Verify, biometrics are enabled for your account

(image below)



**Supported Versions and Devices**

* **Android:**
  + **Supported android Versions:** Android 6.0 (Marshmallow) and above.
  + **Supported android Devices:** Most Android smartphones and tablets that support Android 6.0 or later. Note that devices with work profiles may have limitations with biometric setups.
* **iOS:**
  + **Supported ios Versions:** iOS 13.0 and later.
  + **Supported iphone Devices:**
    - **Face ID:** iPhone X and newer models.
    - **Touch ID:** iPhone 5s and later models with a fingerprint sensor.

**Troubleshooting**

If you encounter issues during the setup process, try the following:

1. **App not responding**: Force close the app and restart it.
2. **Unable to add account**: Check your internet connection and try again.
3. **Biometrics not working**: Ensure your device's biometric settings are properly configured in the system settings.
4. **Push notifications not received**: Check your device's notification settings for Okta Verify.
5. **Authentication fails**: Double-check your login credentials and try again.

If problems persist, contact your IT support team or Okta support.

**Support**

For additional assistance or questions, please contact your organization's IT support team or Okta support at [support email/phone number].

Remember to keep your Okta Verify app updated to ensure you have the latest security features and improvements.

**Additional Resources**

For the most up-to-date and detailed information about Okta Verify, please refer to the official Okta documentation. You can typically find this information by:

1. Visiting the official Okta website
2. Navigating to the Help or Documentation section
3. Searching for "Okta Verify" within the documentation

Key topics you may want to explore in the official documentation include:

* Okta Verify Overview
* Setting Up Okta Verify
* Using Okta Verify
* Frequently Asked Questions about Okta Verify
* Okta Verify Security Features

Always ensure you're referencing the most recent documentation, as features and processes may be updated over time.

If you need specific guidance, contact your organization's IT support team or Okta administrator. They can provide you with the most relevant and current resources for your organization's Okta implementation.