

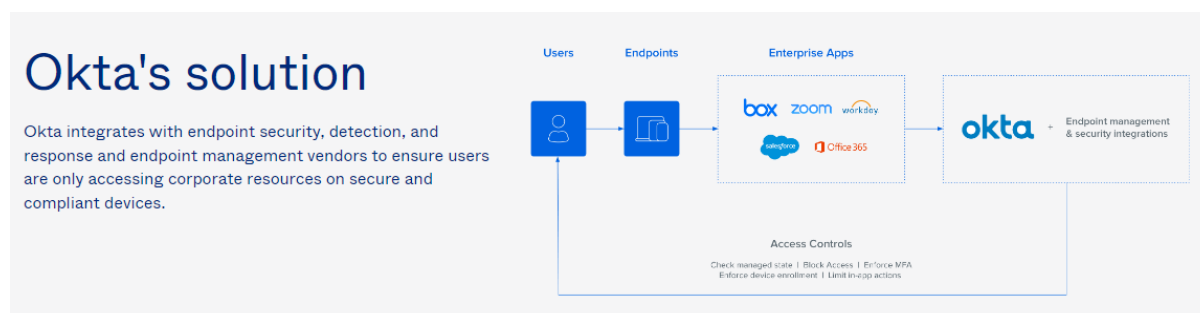
# DEVICE TRUST USING ADAPTATIVE MFA

Manu Venugopalan

## Contents

Device Trust and Adaptive MFA .....	2
What is Device Trust in Okta ? .....	2
What is adaptive MFA in Okta ? .....	2
Okta Classic and Okta Identity Engine .....	2
Current support for protecting app in Android using adaptive MFA.....	2
High Level Flow .....	3
Configuration in Okta for enabling access from trusted devices only(Android) .....	3
Google Workspace .....	3
Configuration in Okta.....	3
Start this procedure .....	6
Integrating Okta with BigFix.....	7
Managed app configurations for Android devices.....	8
Payload for app installation with managed configuration for Bigfix .....	9
Try Access business account from unmanaged Device .....	10
Access google workspace from Managed Device.....	10
Recording of all configuration and Testing .....	11

## Device Trust and Adaptive MFA



### What is Device Trust in Okta ?

Device Trust is a feature in Okta that allows administrators to enforce device-level security policies for accessing sensitive applications. This feature uses device attributes, such as operating system, security software, and network information, to assess the trustworthiness of a device before allowing access to protected resources. The aim of Device Trust is to provide an extra layer of security to an organization's application access and protect against potential threats from compromised devices.

### What is adaptive MFA in Okta ?

Adaptive Multi-Factor Authentication (MFA) is a feature in Okta that enables organizations to balance security and user experience by using various authentication methods based on risk assessment. The risk assessment is based on various factors, such as the location of the user, the device they are using, and the type of login being performed. Based on this assessment, Adaptive MFA can require a user to provide multiple forms of authentication, such as a password, a one-time code sent to their phone, or biometric verification, to access protected resources. The aim of Adaptive MFA is to provide flexible and secure access to sensitive resources while minimizing the inconvenience to the user.

### Okta Classic and Okta Identity Engine

Okta Classic and Okta Identity Engine are two different products offered by Okta, a leading provider of identity and access management solutions.

Okta Classic is the original product offered by Okta, which provides a cloud-based platform for managing and securing user access to applications and resources. It includes features such as single sign-on (SSO), multi-factor authentication (MFA), user provisioning, and access management.

Okta Identity Engine is a more recent product that builds on the functionality of Okta Classic, but also includes additional capabilities such as identity governance, risk-based access, and adaptive multifactor authentication.

### Current support for protecting app in Andorid using adaptive MFA

Device Trust feature is not available in the latest Okta versions. Device trust functionality was replaced by Adaptive Multi-Factor Authentication (MFA) which allows to set up MFA based on device trust. So you can set up a policy that requires MFA only when the device is not trusted, or when the user is accessing from a new device.

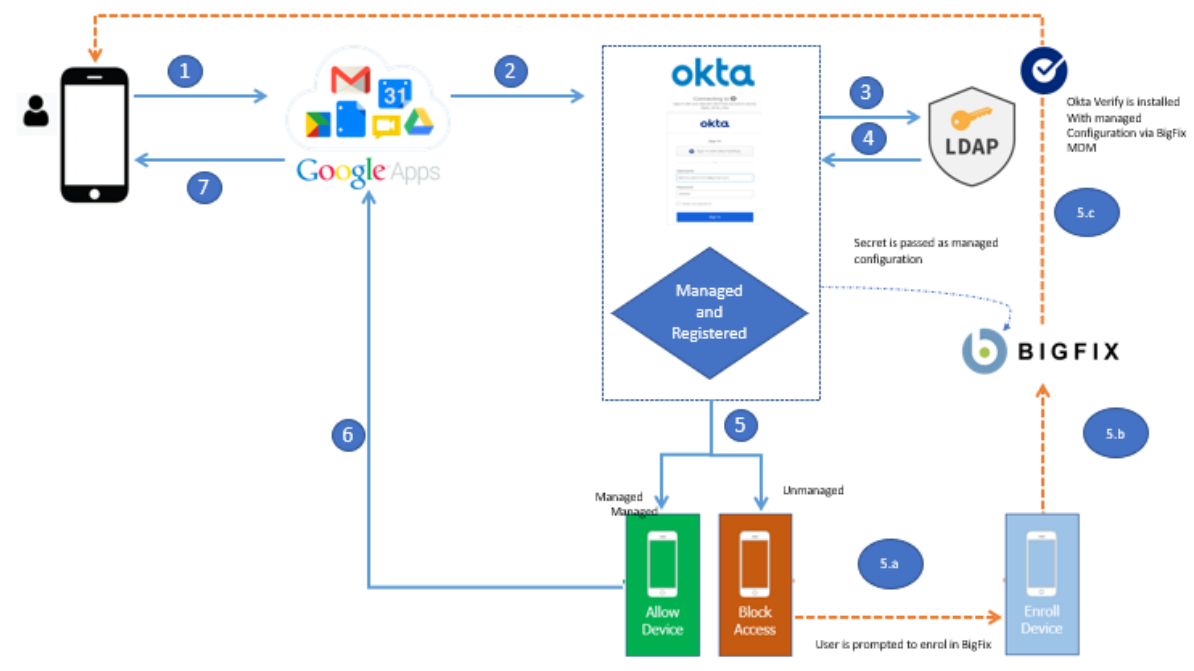
With Adaptive MFA, you can set up policies that use different factors depending on the level of trust for a device. For example, you can set up a policy that requires a user to enter a passcode if they are logging in from a new device, but only uses push notifications for verification on a device that has been previously used and is trusted.

**Device Trust (Identity Engine) is currently only available to customers who had Device Trust (Classic Engine) and upgraded to Identity Engine.**

Link to okta documentation : Device Trust (Identity Engine) is currently only available to customers who had Device Trust (Classic Engine) and upgraded to Identity Engine.

<https://help.okta.com/oie/en-us/Content/Topics/identity-engine/devices/dt-main.htm>

## High Level Flow



## Configuration in Okta for enabling access from trusted devices only(Android)

The document goes through the configuration and changes needed to ensure that organizational user can access **google workspace** apps only from managed devices. If the user is trying to login from an unmanaged device, the user will be prompted to enroll the device using BigFix.

### Google Workspace

Create a new domain and google workspace account for a user if not available.

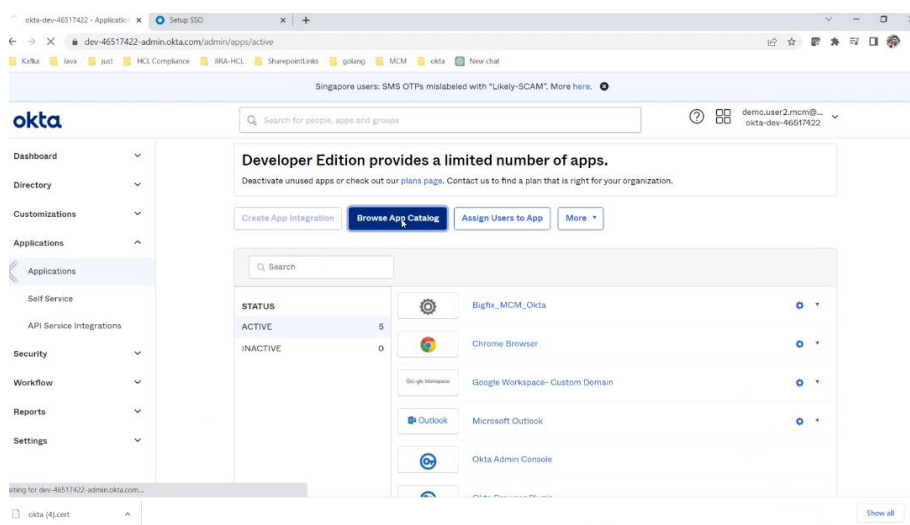
Note:- We cannot use account created using gmail.com domain for this testing.

## Configuration in Okta

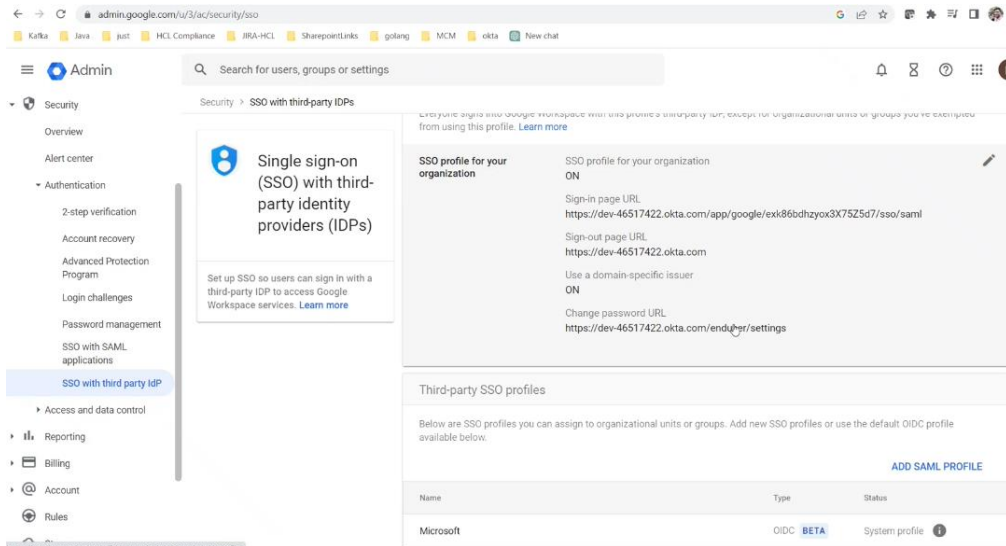
### 1. Configure application in okta

To add an existing app integration to your org:

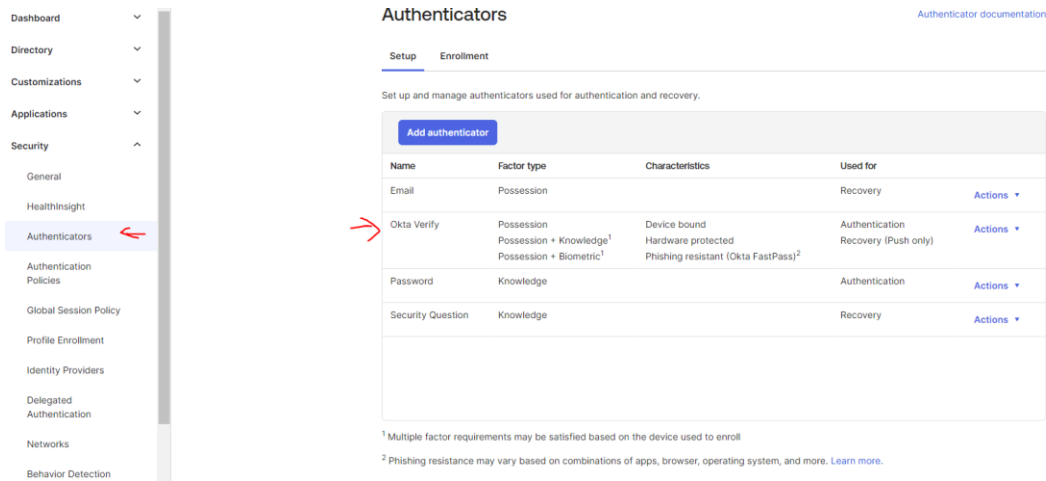
- a) In the Admin Console, go to **Applications > Applications**.
- b) Click **Browse App Catalog**.
- c) To search for the app integration, perform one of these two options:
  - a. Type the name of the specific app integration into the **Search...** bar. You can click the name in the dropdown list or click **See All Results** to have everything displayed as tiles in the main panel. Click the tile to open the details page for the app integration.
  - b. Choose a **Use Case** and optionally select one or more functionalities to filter the results. When you see the desired app integration in the main panel, click it to open the details page for more information about the integration.
- d) Determine if this is the correct app integration for your needs. The **Overview** tab on the details page shows a detailed description of the app integration and, if available, the Okta verification status:
  - a. **Okta Verified:** This integration was created by Okta or by Okta community users, then tested and verified by Okta.
  - b. **Community Created or Unverified:** This integration was created by the community and has shown some evidence of quality, such as active usage or multiple community members using it. However, Okta hasn't tested this app integration, and it isn't officially supported.
- e) Click the **Capabilities** tab on the details page to see the supported **Access** and **Provisioning** features of the app integration.



2. Configure the sign-on url and details in google workspace account after logging in as admin user



### 3. Ensure Okta verify is added in Authenticators section under Security



## Okta Verify

After admins configure this authenticator, users are prompted to download and install the Okta Verify app. Once installed, Okta Verify uses your configuration to allow users to access protected resources. Learn more in [documentation](#).

---

### Used for

- Authentication (with time-based one-time password (TOTP), push notification, Okta FastPass)
- Self-service recovery (with push notification only)

---

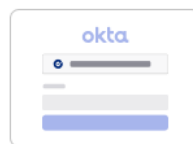
### Verification options

- User can verify with
- TOTP (on by default) (Android and iOS only)
  - Push notification (Android and iOS only)
  - Okta FastPass (All platforms)

---

### Okta FastPass

- Sign-in page option
- Show the "Sign in with Okta FastPass" button



[What does this button do? ↗](#)

## 4. Configure authentication policies in security in Okta

Authentication policies define and enforce access requirements for apps. Every app in your org already has a default authentication policy. You can customize the policy by creating rules that regulate, among other things, who can access an app, from what locations, on what types of devices, and using what authentication methods.

Rules are numbered. Okta evaluates rules in the same order in which they appear on the authentication policy page. You can reorder added rules by clicking and dragging the vertical dotted "handle" that appears under a rule's number.

The authentication policy is evaluated whenever a user accesses an app.

Priority	Rule	Status	Actions
1	<b>Managed_Rule_Custom</b> IF Device: Registered, Managed THEN Access: Allowed with password <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;">             Your org's authenticators that satisfy this requirement:              Password           </div> Re-authentication frequency is: Every sign-in attempt	ENABLED	Actions ▾
2	<b>Non_Managed</b> IF Device: Registered, Not managed AND Platform: Android THEN Access: Denied	ENABLED	Actions ▾
3	<b>Catch-all Rule</b> IF Any request THEN Access: Denied	ENABLED	Actions ▾

### Edit Rule

If all of the conditions are true, the authentication settings below will apply. Otherwise, Okta will evaluate the next rule.

Rule name

#### IF

- IF User's user type is
- AND User's group membership includes
- AND User is
- AND Device state is
  - Any
  - Registered  
Setup Okta Verify as [Authenticator](#)
  - Not managed
  - Managed  
[Go to Device Management](#)
- AND Device assurance policy is
- AND Device platform is
- AND User's IP is
- AND Risk is

**AND** The following custom expression is true

This is an optional advanced setting. If the expression is formatted incorrectly or conflicts with conditions set above, the rule may not match any users.

[Expression language reference](#)

#### THEN

**THEN** Access is

- Denied  
 Allowed after successful authentication

**AND** User must authenticate with

[Learn more about authentication scenarios](#)

Your org's authenticators that satisfy this requirement:

Password

#### Re-authentication frequency

**i**

- Users with FEDERATION or SOCIAL authentication providers bypass password re-authentication.
- All other users are prompted for password upon re-authentication, even if they authenticated through a trusted Identity Provider.

**AND** Re-authentication frequency is

- Every sign-in attempt  
 Never re-authenticate if the session is active  
 Re-authenticate after:

Save

Cancel

Screen shots for blocking access for non-managed devices

## Edit Rule

If all of the conditions are true, the authentication settings below will apply. Otherwise, Okta will evaluate the next rule.

Rule name

Non\_Managed

### IF

<input type="checkbox"/> IF	User's user type is	<input type="text" value="Any user type"/>
<input type="checkbox"/> AND	User's group membership includes	<input type="text" value="Any group"/>
<input type="checkbox"/> AND	User is	<input type="text" value="Any user"/>
<input type="checkbox"/> AND	Device state is	<input type="radio"/> Any <input checked="" type="radio"/> Registered Setup Okta Verify as <a href="#">Authenticator</a>
<input type="checkbox"/> AND	Device management is	<input checked="" type="radio"/> Not managed <input type="radio"/> Managed <a href="#">Go to Device Management</a>
<input type="checkbox"/> AND	Device assurance policy is	<input type="text" value="No policy"/>
<input type="checkbox"/> AND	Device platform is	<input type="text" value="One of the following platforms"/> <input type="text" value="Android"/>
<input type="checkbox"/> AND	User's IP is	<input type="text" value="Any IP"/>
<input type="checkbox"/> AND	User's IP is	<input type="text" value="Any IP"/>
<input type="checkbox"/> AND	Risk is	<input type="text" value="Any"/>
<input type="checkbox"/> AND	The following custom expression is true	<input type="text"/>

This is an optional advanced setting. If the expression is formatted incorrectly or conflicts with conditions set above, the rule may not match any users.

[Expression language reference](#)

### THEN

<input type="checkbox"/> THEN	Access is	<input checked="" type="radio"/> Denied <input type="radio"/> Allowed after successful authentication
-------------------------------	-----------	--

Save

Cancel

Note:- Reference Okta link :- <https://help.okta.com/oie/en-us/Content/Topics/identity-engine/devices/add-app-signon-policy-mobile.htm>

## 5. Configure Device Assurance Policies

1. In the Admin Console, go to Security > Authentication Policies.
2. Click Add a policy.
3. Enter a policy Name and Description.
4. Click Save.

The screenshot displays the Okta Admin Console interface. At the top, a notification bar indicates "Singapore users: SMS OTPs mislabeled with 'Likely-SCAM'. More here." The Okta logo is on the left, and a search bar is in the center. The user profile "demo.user2.mcm@... okta-dev-46517422" is on the right. A left-hand navigation menu includes: Dashboard, Directory, Customizations, Applications, Security (expanded), General, Healthinsight, Authenticators, Authentication Policies, Global Session Policy, Profile Enrollment, and Identity Providers. The main content area is titled "Device Assurance Policies" and features a blue "Add a policy" button. Below the button is a table with the following data:

Policy name	Platform	Conditions	
Device Trust Policy	Android	Screen lock must be enabled	Actions ▾

At the bottom left of the page, the URL "https://dev-46517422-admin.okta.com/admin/oceres/healthinsight" is visible.

## Edit device assurance policy

Policy name

Platform  Android  
 iOS  
 macOS  
 Windows

---

**Android**

Minimum Android version  Use a preset version   
 Customize  
  
Version  
  
Security Patch (YYYY-MM-DD)  
Current minimum Android: Any version

Lock screen  Screen lock must be enabled  
 Biometrics must be enabled

Disk encryption  Device disk must be encrypted

Hardware keystore  Device supports hardware-backed keys

Rooting  Device must not be rooted

### 6. Configure Device Integration

When evaluating an authentication policy that requires devices to be managed, Okta determines the management status of your targeted Android and iOS devices by verifying whether there's a key installed on the device which matches a key you generated through the Okta Admin Console and entered in your MDM software's managed app configuration.

Start this procedure


1. In the Admin Console, go to Security > Device integrations.
2. Click the Endpoint management tab.
3. Click Add platform.

If you add more than one configuration for the same type of platform, see [Devices known issues](#).

4. Select Android or iOS as applicable.
5. Click Next.

6. In Configure management attestation:

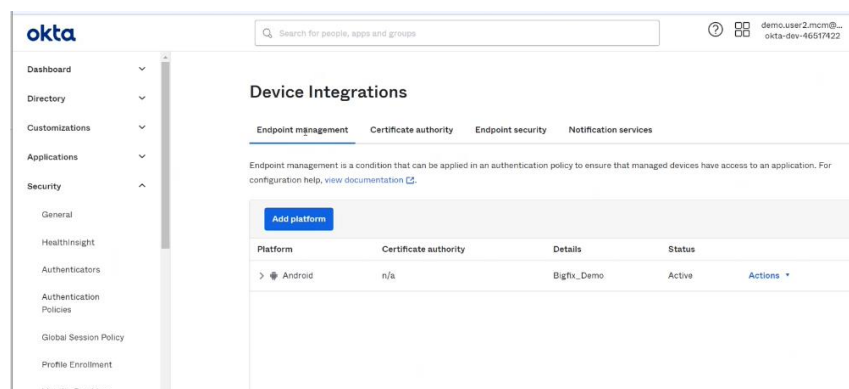
- a. Copy the provided Secret key to your clipboard by clicking the copy

icon  adjacent to the field. You'll enter the Secret key later in your MDM software's app configuration as described in Integrate Okta with your MDM software.

Make a note of the provided Secret key value as this is the only time it will appear in Okta. If you generate a new Secret key by clicking Reset secret key, make sure to also update your MDM software configuration with the new key.

The Device management provider field is pre-populated with the name of your MDM software but you can change it. The contents of this field are displayed to end users later when they enroll their device.

- b. In the Enrollment link field, enter a web address for redirecting end users with unenrolled devices. For example, you may want to redirect these users to a page with enrollment instructions or the enrollment page of your selected MDM software (assuming the MDM software supports web-based enrollment).
- c. Click Save.



The screenshot shows a configuration form with the following fields:

- Secret key:** A text input field containing the value '4m\_vdEScDwwGs09pM-JvFG7-ki' with a copy icon to its right.
- Important:** A yellow callout box with the text: 'Important: Make a note of the secret key as it will be the only time you will be able to view it. After this, it will be stored as a hash for your protection.'
- Device management provider:** A text input field containing the letter 'I'. Below the field, it says '20 characters remaining' and 'Input will be inserted into end-user enrollment flows in order to display device management provider.'
- Enrollment link:** An empty text input field.

Cancel

## Integrating Okta with BigFix

This procedure provides high-level integration instructions for **BigFix**.


1. Configure BigFix software to manage Okta Verify and to install Okta Verify on end-user devices that don't have it installed.
2. Configure the key-value pair, by using your MDM software's managed app configuration as described in their documentation:
  - Domain: Enter the URL of your Okta org
  - Key: `managementHint`
  - Value: Enter the Secret Key value that you saved during the [Configure Device Management for mobile devices](#) procedure.

### Managed app configurations for Android devices

You can use your device management solution to deploy managed app configurations. The managed app configurations allow you to enable functionality that is built into Android Okta Verify.

Use the examples in this table to help you configure your managed app configurations:

Managed app configuration	Key	Value	Value type	Example
<p>Pre-populate the org URL</p> <p>Enables admins to pre-populate the <b>First, enter your sign-in URL</b> screen with a sign-in URL, so end users do not need to enter it.</p> <p>This is available for Android Okta Verify v6.2.0 and later.</p>	<code>domainName</code>	<code>&lt;org_sign-in_URL&gt;</code>	String	<code>example.okta.com</code>

Managed app configuration	Key	Value	Value type	Example
				
<p>Provide a management hint</p> <p>Enables admins to specify a secret key, which indicates that a device is managed.</p>	managementHint	<secret_key>	String	3zr7Q~vw4C16FS2bH8UfS 1gJ5cL6sj~x_U9PQ

Note :- Reference Okta link :- <https://help.okta.com/oie/en-us/Content/Topics/identity-engine/devices/managed-app-configs-android.htm>

Payload for app installation with managed configuration for Bigfix

```
"applications": [
  {
    "packageName": "com.okta.android.auth",
    "installType": "FORCE_INSTALLED",
    "disabled": false,
    "managedConfiguration": {
      "domainName": "dev-46517422.okta.com",
      "managementHint": "D09Cv_-d90Gm0YArZ--9ebpmgUsDY2bddQ7o7Je8pYk"
    }
  },
  {
    "packageName": "com.android.chrome",
    "installType": "FORCE_INSTALLED",
    "defaultPermissionPolicy": "GRANT"
  },
]
```

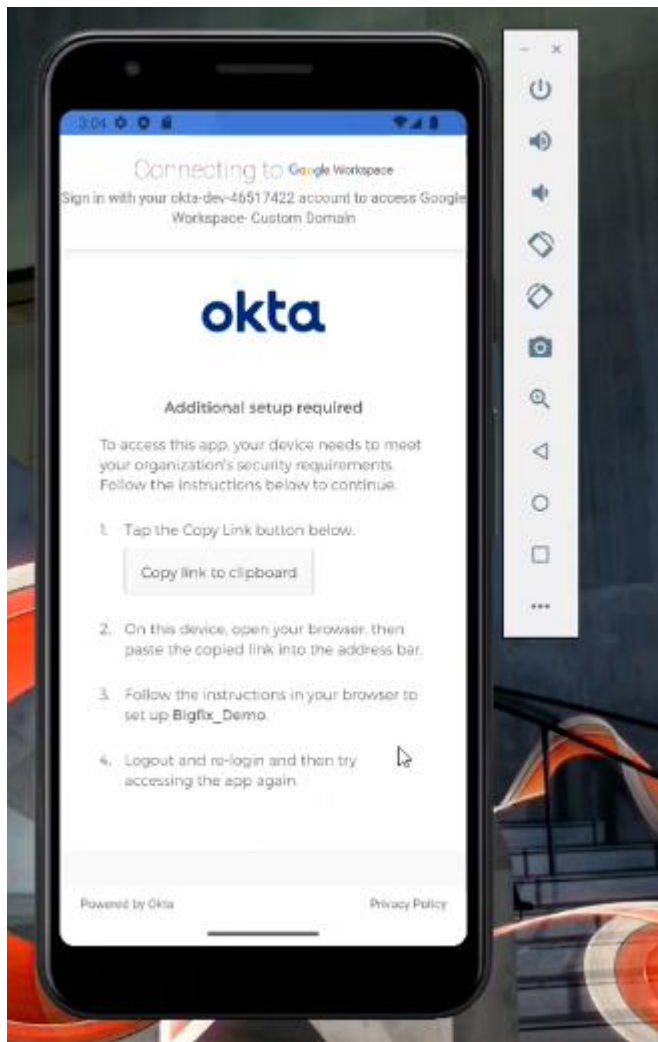
```
{
  "packageName": "com.google.android.apps.docs.editors.docs",
  "installType": "FORCE_INSTALLED",
  "defaultPermissionPolicy": "GRANT"
},
{
  "packageName": "com.google.android.gm",
  "installType": "FORCE_INSTALLED",
  "defaultPermissionPolicy": "GRANT"
}
]
```

ManagedConfiguration have to be added only for Okta Verify App. Example below :

```
"managedConfiguration": {
  "domainName": "dev-46517422.okta.com",
  "managementHint": "D09Cv_-d9OGm0YArZ--9ebpmgUsDY2bddQ7o7Je8pYk"
}
```

Try Access business account from unmanaged Device

User will be prompted to enroll from android device to bigfix. User can copy the link and enroll to access google workspace account after that.



## Access google workspace from Managed Device

Enroll the device via MCM Bigfix. Once enrolled, we should install Okta verify and other google workspace app using managed configurations as shown in the payload earlier.

Once Okta verify is installed and configured via MCM, open any google workspace app and try accessing the account. User will be prompted to enter user credentials on Okta login page and then successfully able to access the app.

## Recording of all configuration and Testing

Available in → [Device Trust](#)