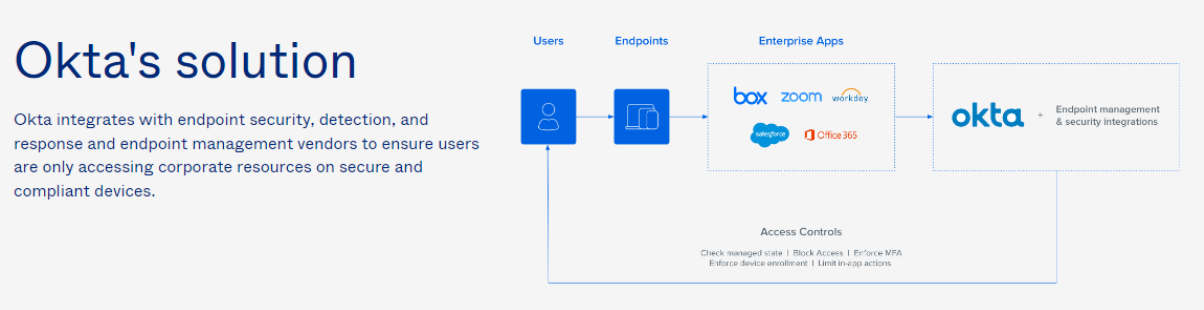
DEVICE TRUST USING ADAPTATIVE MFA

Manu Venugopalan

Contents

Device Trust and Adaptative 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.

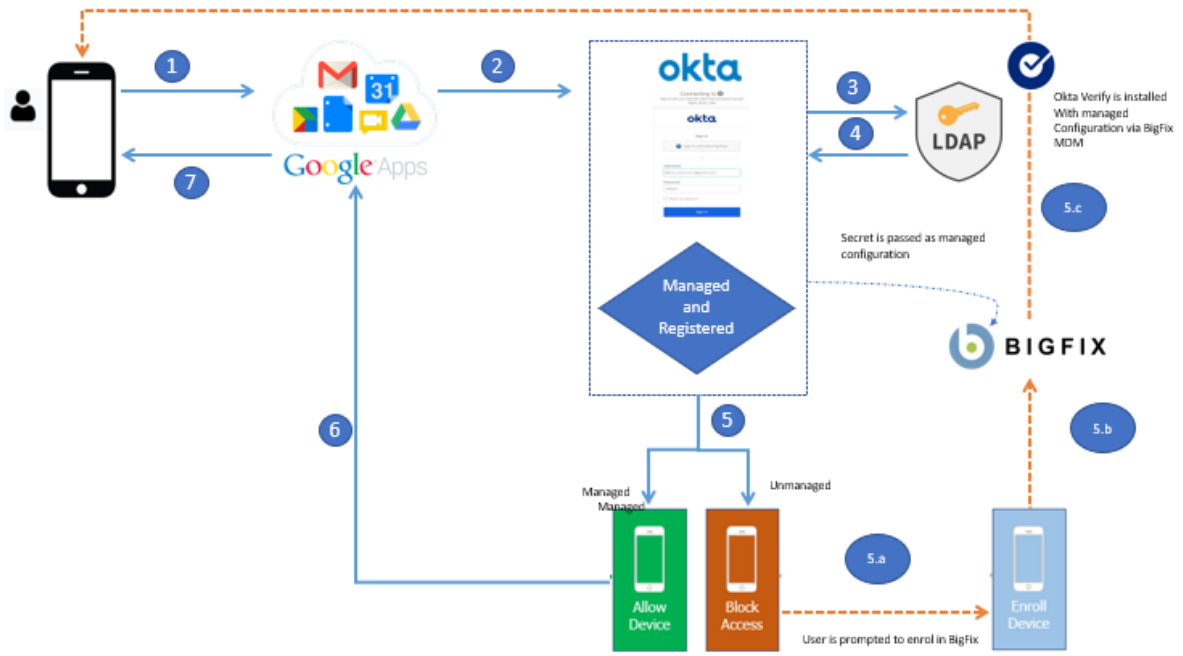
With Adaptive MFA, you can set up policies that use different factors depending on the level of trust for a device. For example, you can set up a policy that requires a user to enter a passcode if they are logging in from a new device, but only uses push notifications for verification on a device that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

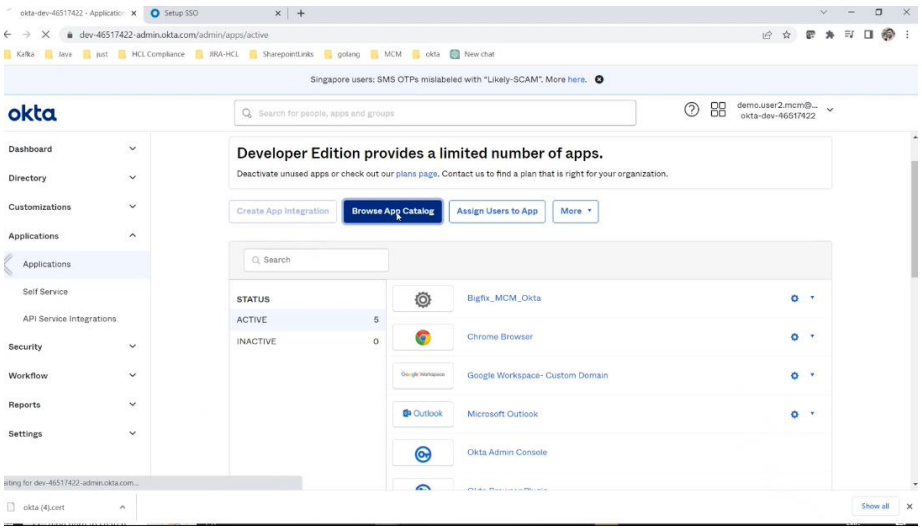
   b. Choose a **Use Case** and optionally select one or more functionalities to filter the results. When you see the desired app integration in the main panel, click it to open the details page for more information about the integration.

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:

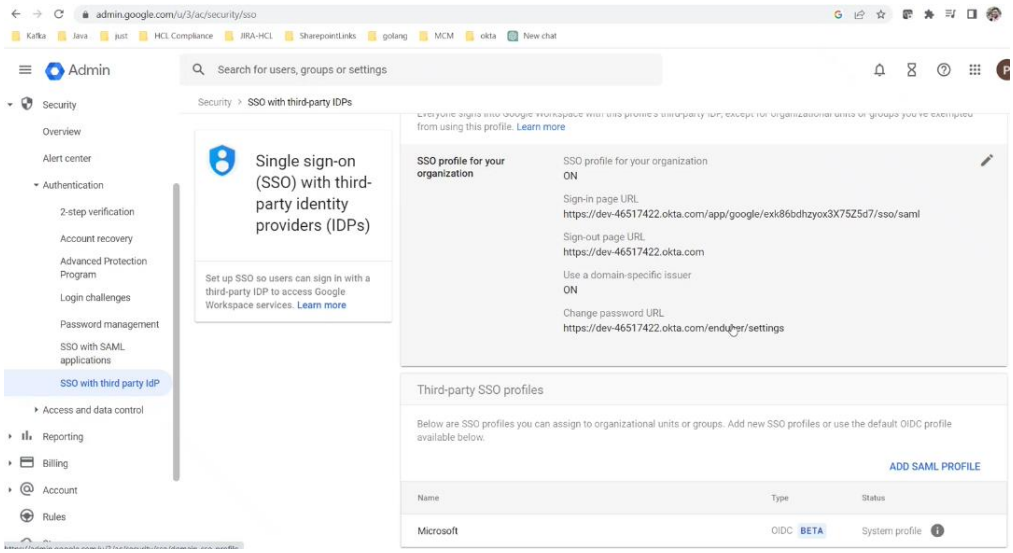
   a. **Okta Verified**: This integration was created by Okta or by Okta community users, then tested and verified by Okta.

   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.

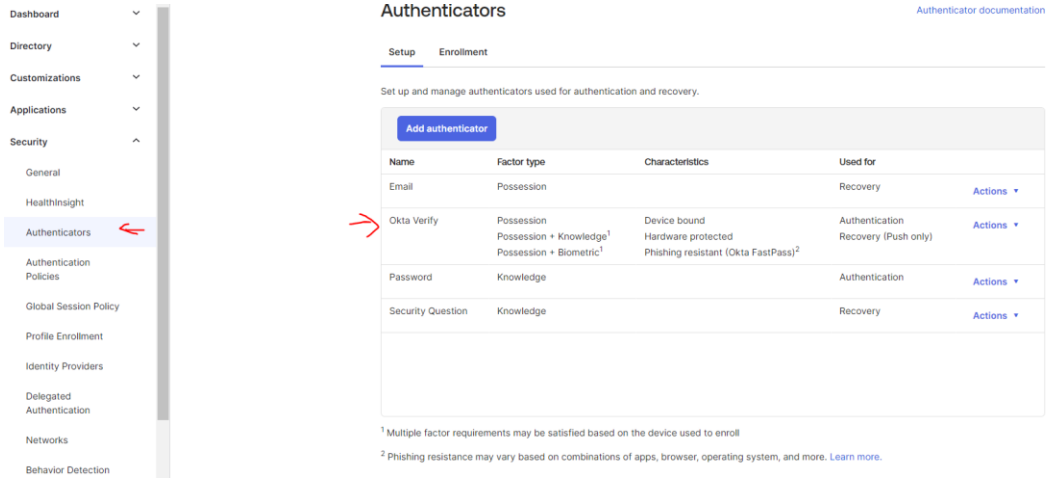
e) Click the **Capabilities** tab on the details page to see the supported **Access** and **Provisioning** features of the app integration.

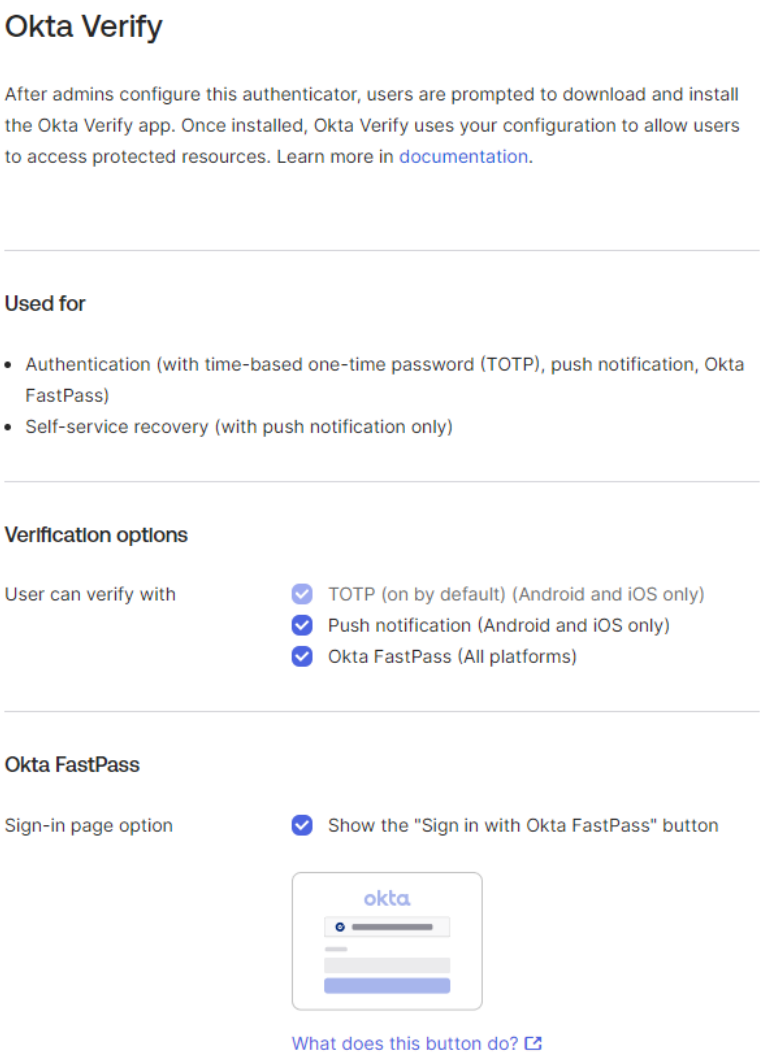


2. Configure the sign-on url and details in google workspace account after logging in as admin user



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





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	Managed_Rule_Custom	ENABLED	Actions

IF **Device:** Registered, Managed THEN **Access:** Allowed with password

Your org's authenticators that satisfy this requirement:

Password

Re-authentication frequency is: Every sign-in attempt

Priority	Rule	Status	Actions
2	Non_Managed	ENABLED	Actions

IF **Device:** Registered, Not managed

Platform: Android

THEN **Access:** Denied

Priority	Rule	Status	Actions
3	Catch-all Rule	ENABLED	Actions

IF Any request THEN **Access:** Denied

Edit Rule

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

Rule name: Managed_Rule_Custom

IF

IF User's user type is: Any user type

AND User's group membership includes: Any group

AND User is: Any user

AND Device state is:
- ○ Any
- ◉ Registered

Setup Okta Verify as Authenticator

AND Device management is:
- ○ Not managed
- ◉ Managed

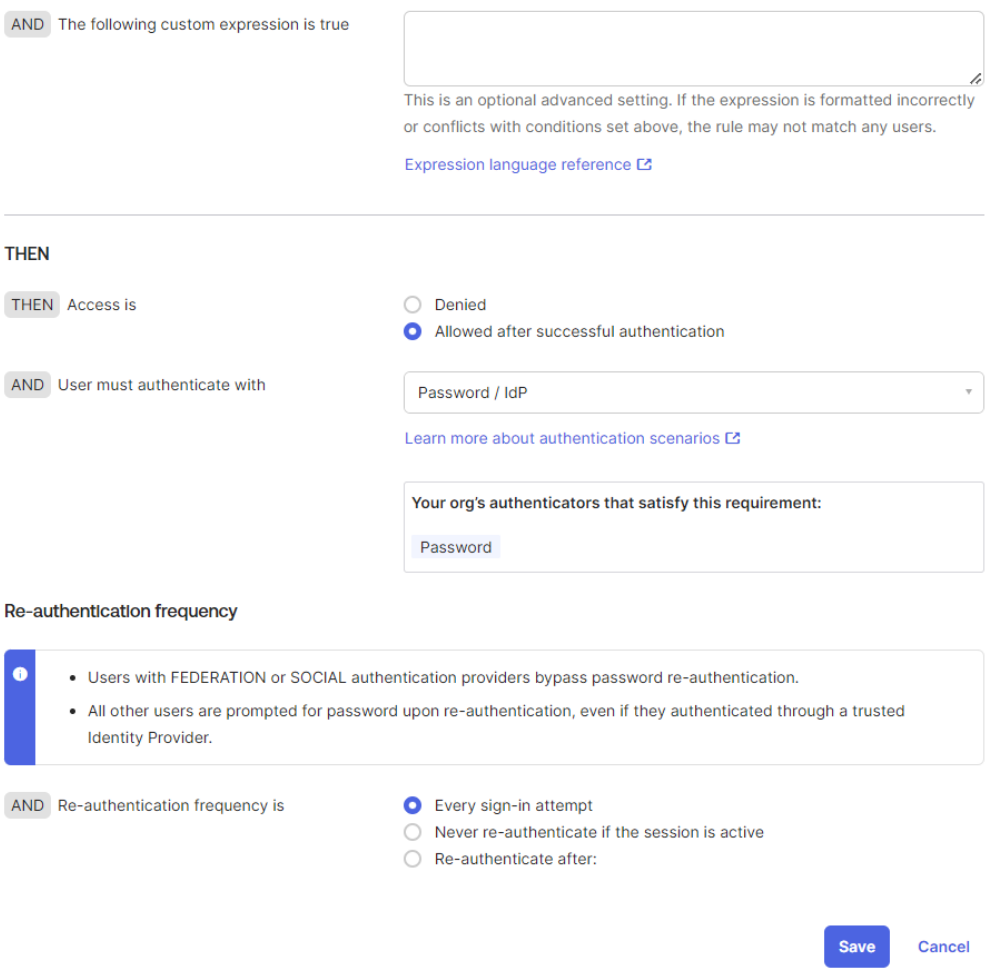
Go to Device Management

AND Device assurance policy is: No policy

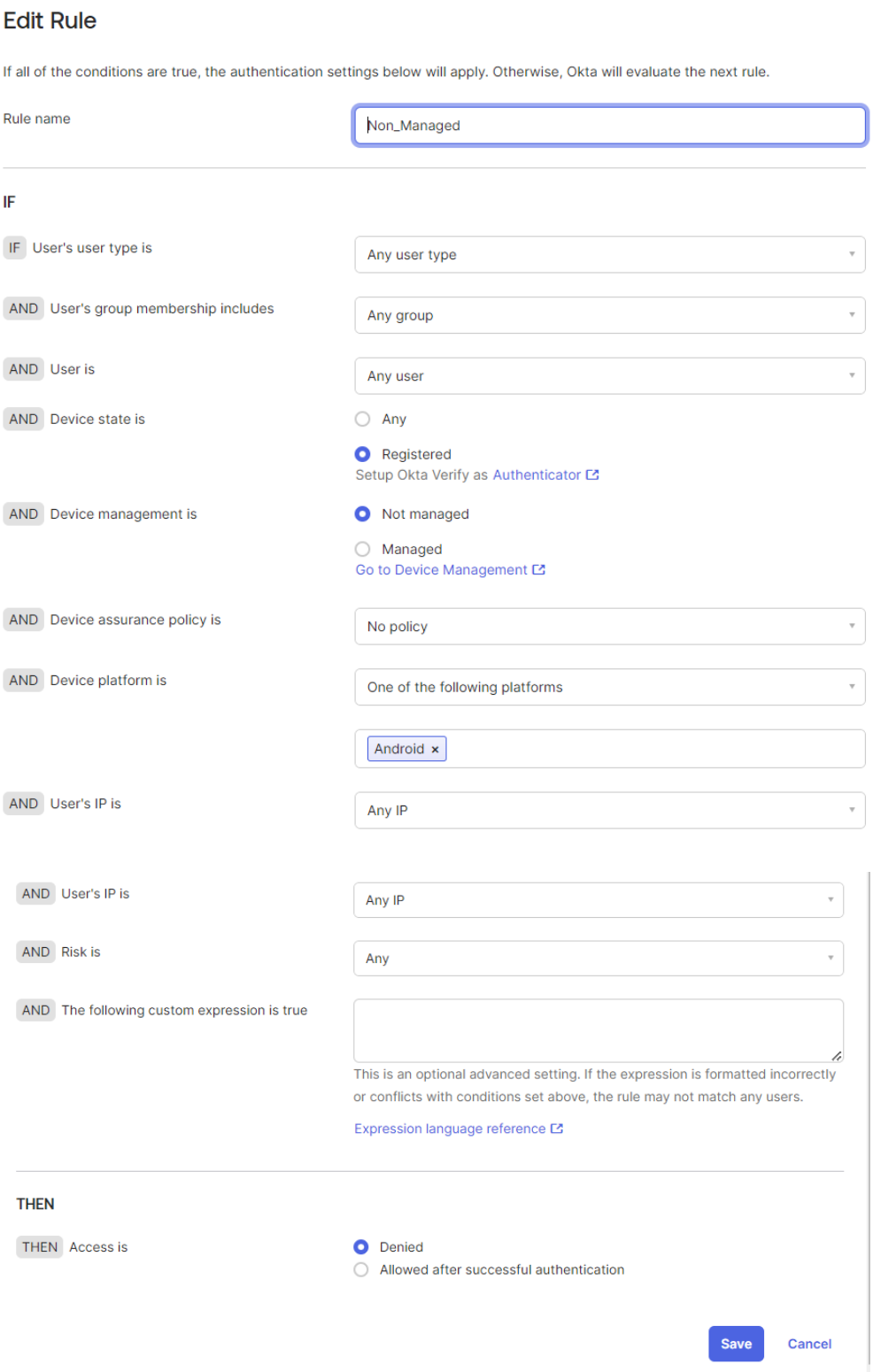
AND Device platform is: Any platform

AND User's IP is: Any IP

AND Risk is: Any



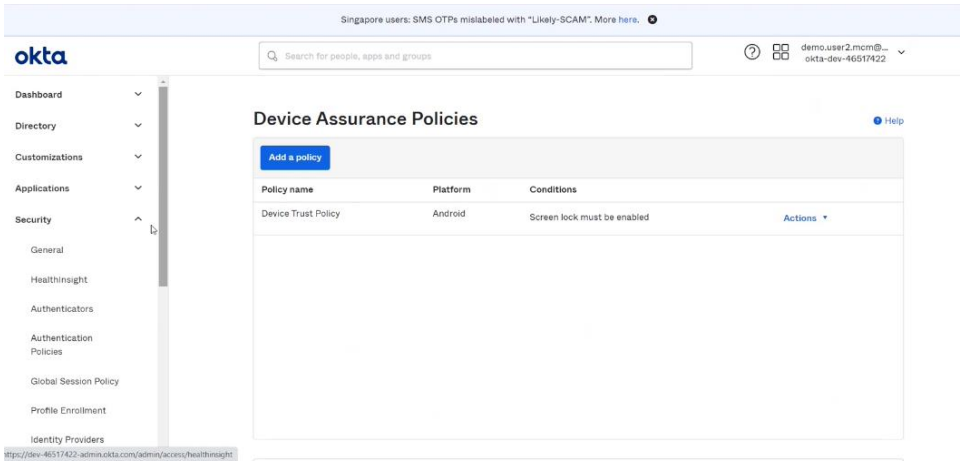
Screen shots for blocking access for non-managed devices

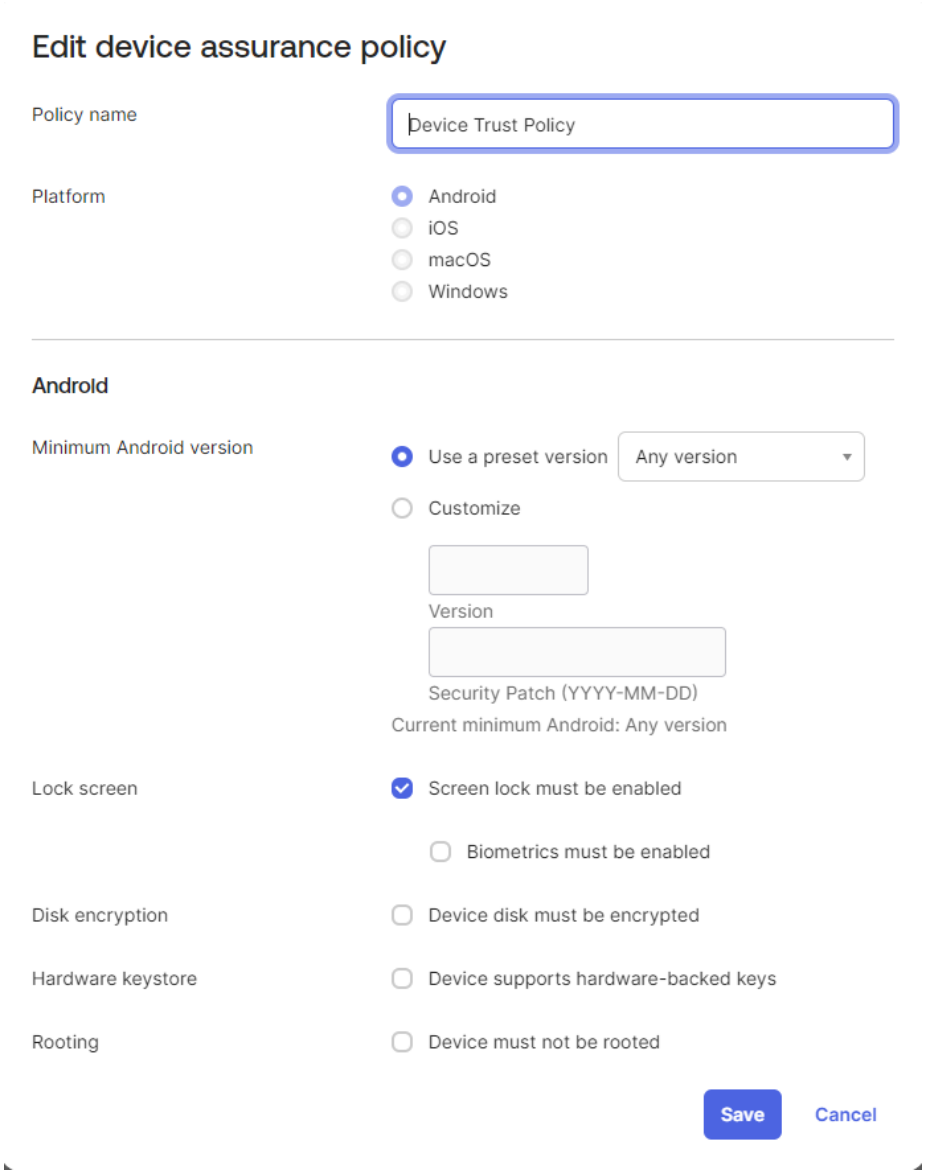


Note:- Reference Okta link :- https://help.okta.com/oie/en-us/Content/Topics/identity-engine/devices/add-app-signon-policy-mobile.htm

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.





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.

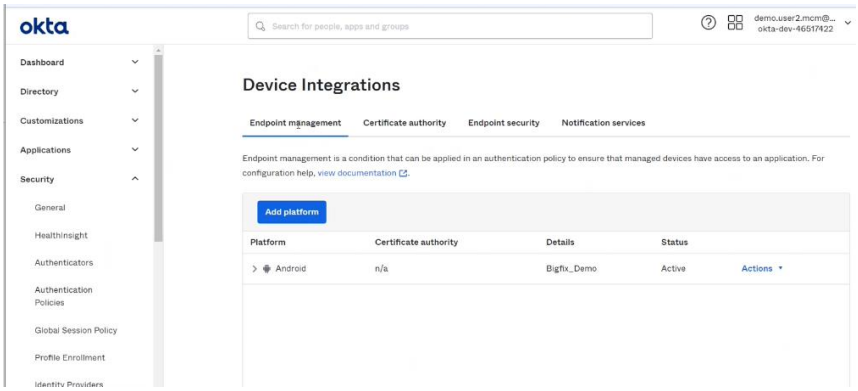
6. In Configure management attestation:
    a. Copy the provided Secret key to your clipboard by clicking the copy icon adjacent to the field. You'll enter the Secret key later in your MDM software's app configuration as described in Integrate Okta with your MDM software.

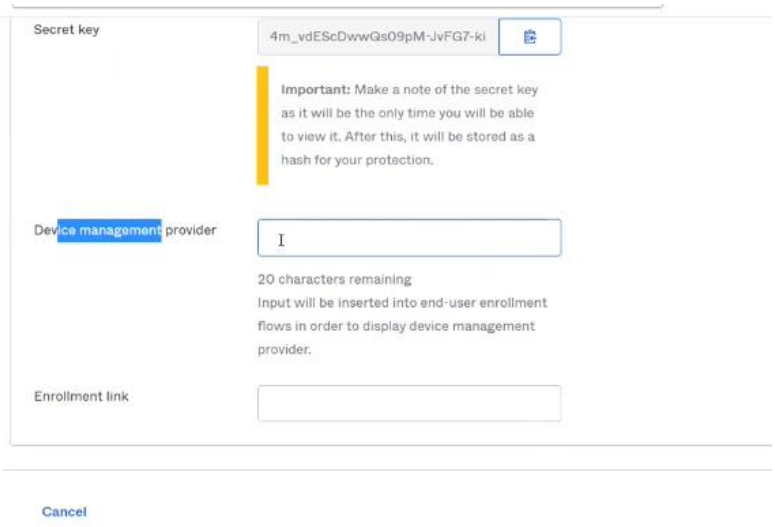
        Make a note of the provided Secret key value as this is the only time it will appear in Okta. If you generate a new Secret key by clicking Reset secret key, make sure to also update your MDM software configuration with the new key.

        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.





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
Pre-populate the org URL Enables admins to pre-populate the **First, enter your sign-in URL** screen with a sign-in URL, so end users do not need to enter it. This is available for Android Okta Verify v6.2.0 and later.	`domainName`	`<org_sign-in_URL>`	String	`example.okta.com`

Managed app configuration	Key	Value	Value type	Example
				
Provide a management hint Enables admins to specify a secret key, which indicates that a device is managed.	`managementHint`	`<secret_key>`	String	`3zr7Q~vw4C16FS2bH8UfS1gJ5cL6sj~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_-d9OGm0YArZ--9ebpmgUsDY2bddQ7o7Je8pYk"
          }
      },
   {
    "packageName": "com.android.chrome",
    "installType": "FORCE_INSTALLED",
    "defaultPermissionPolicy": "GRANT"
  },
```

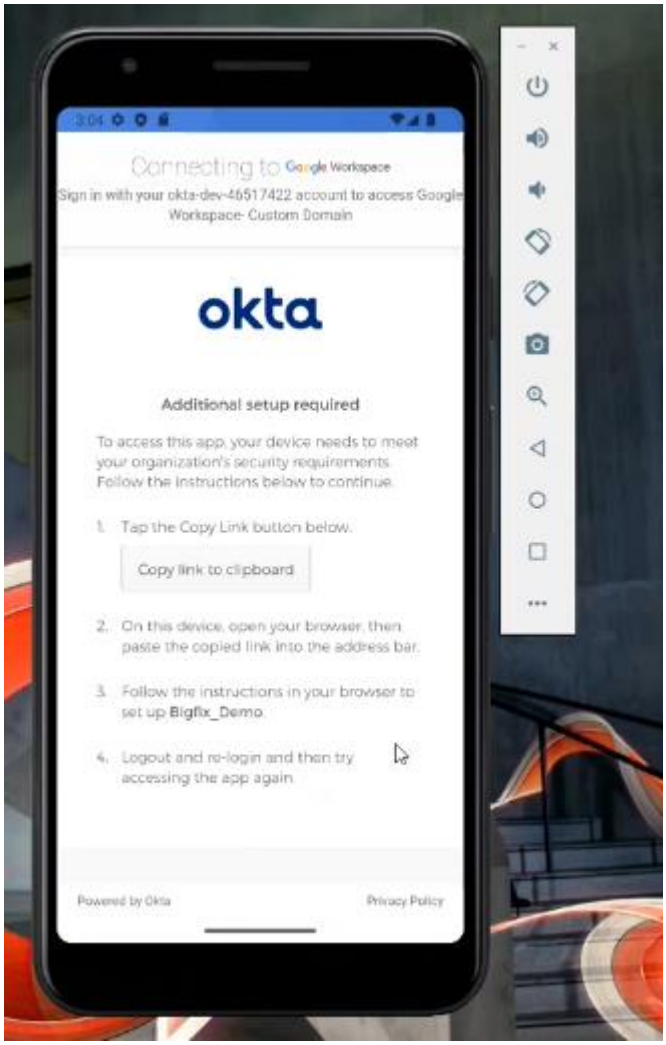
```
    {
    "packageName": "com.google.android.apps.docs.editors.docs",
    "installType": "FORCE_INSTALLED",
    "defaultPermissionPolicy": "GRANT"
  },
   {
    "packageName": "com.google.android.gm",
    "installType": "FORCE_INSTALLED",
    "defaultPermissionPolicy": "GRANT”
  }
]
```

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