ORACLE

Configuration of IDCS MFA

Inge Os

Inge.os@oracle.om

The flow o configuring MFA

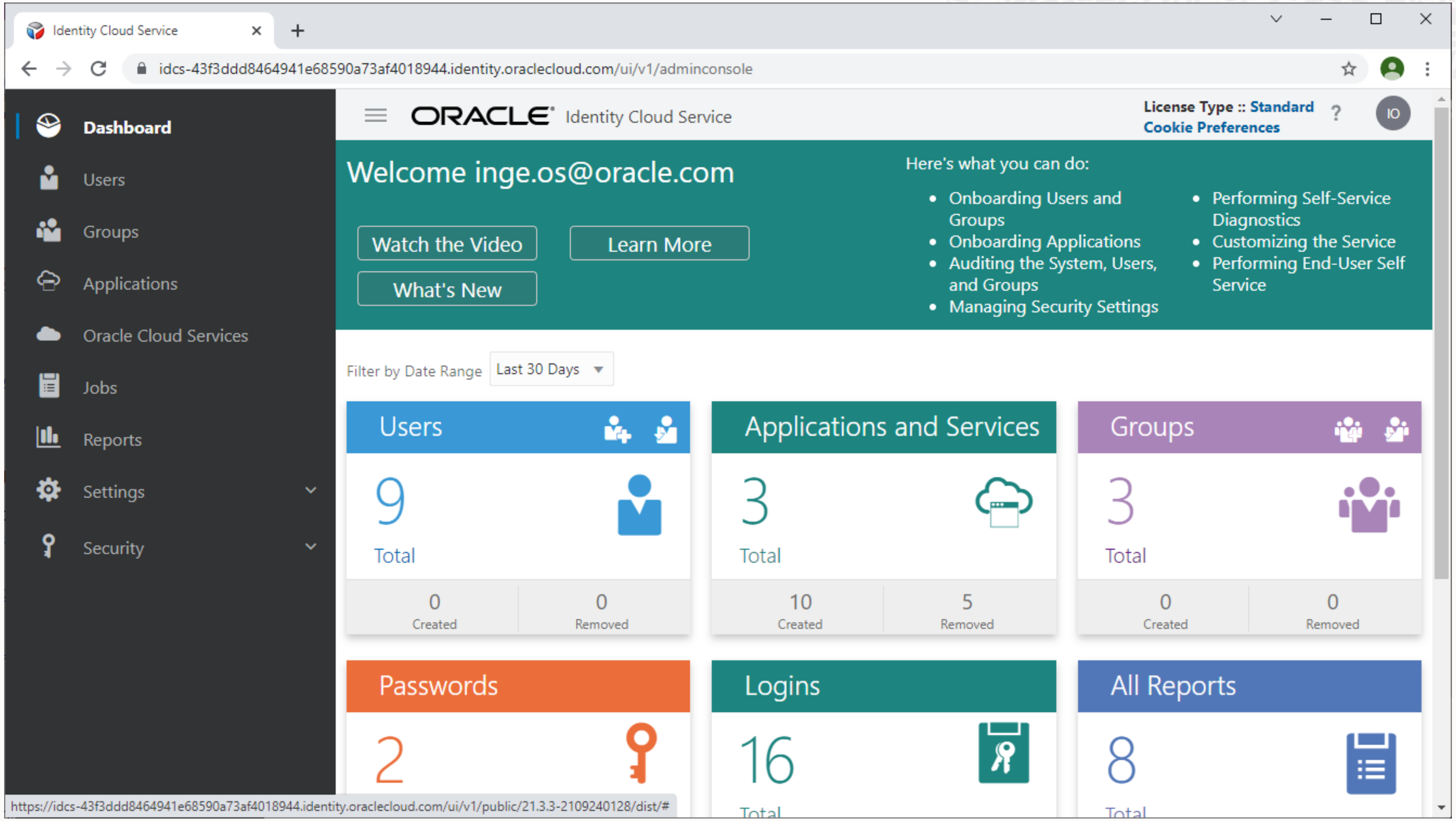
MFA is a Standard feature of IDCS, and the IDCS stripe is required to be on any of the non-foundation subscription type

When MFA is enabled, users are requested to register them selves for MFA, ie. Add phonenmuber for SMS, first time of logon after MFA is enabled

The steps are

- Configure the properties of the selected MFA Factor
- Configure which MFA Factor to enable
- Modify the default SSO Login policy to reflect the added Factor

Default configuration without MFA



Welcome inge.os@oracle.com

Here's what you can do:

- Onboarding Users and Groups
- Onboarding Applications
- Auditing the System, Users, and Groups
- Managing Security Settings
- Performing Self-Service Diagnostics
- Customizing the Service
- Performing End-User Self Service

License Type :: Standard

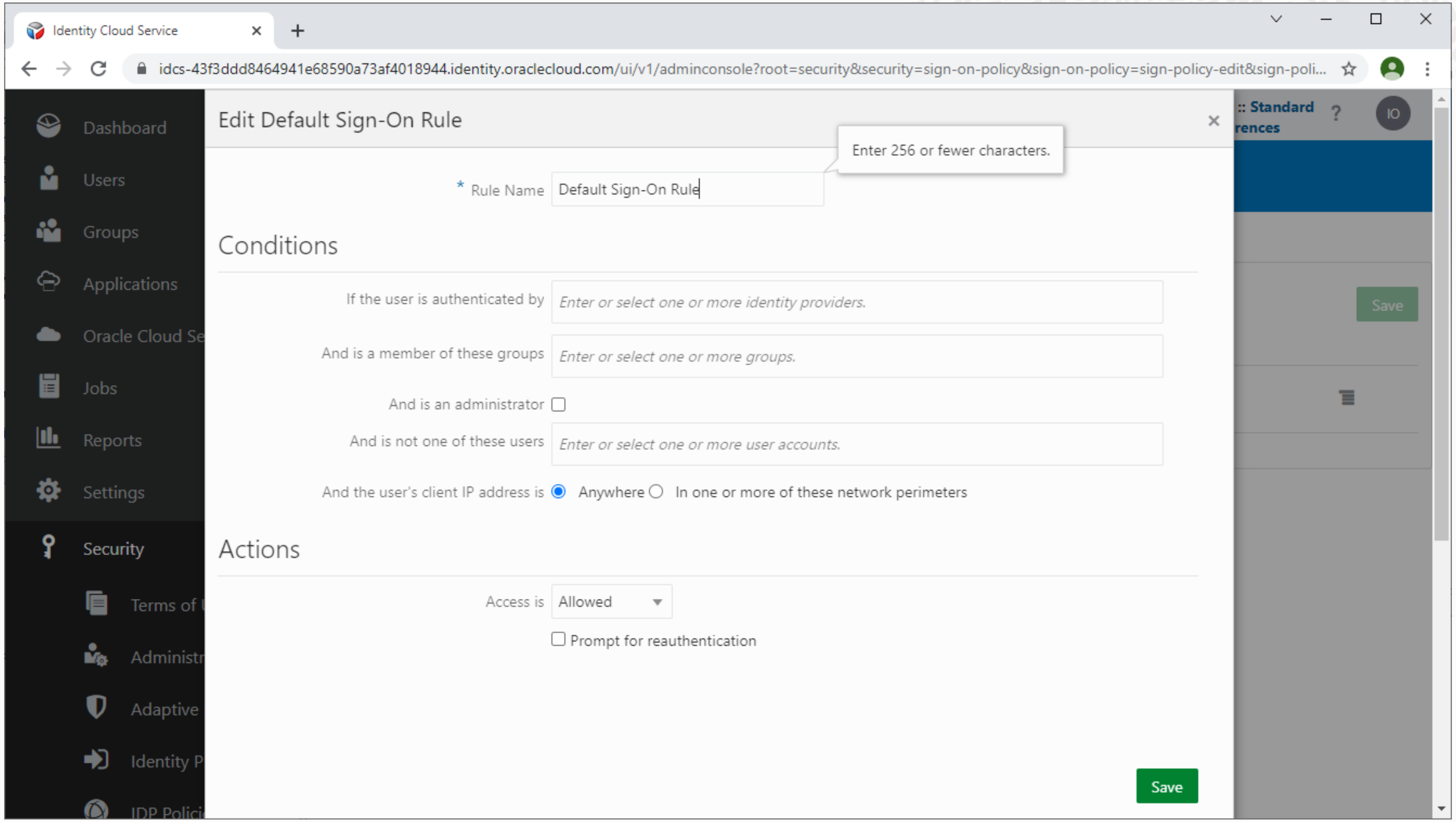
Filter by Date Range: Last 30 Days

Tile	Total	Created	Removed
Users	9	0	0
Applications and Services	3	10	5
Groups	3	0	0
Passwords	2		
Logins	16		
All Reports	8		

idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/adminconsole

https://idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/public/21.3.3-2109240128/dist/#

Default configuration without MFA, Default SSO rule



Identity Cloud Service
idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/adminconsole?root=security&security=sign-on-policy&sign-on-policy=sign-policy-edit&sign-poli...
Dashboard
Users
Groups
Applications
Oracle Cloud Se
Jobs
Reports
Settings
Security
Terms of
Administr
Adaptive
Identity P
IDP Polici
:: Standard
rences
IO
Save

Edit Default Sign-On Rule

Enter 256 or fewer characters.

* Rule Name: Default Sign-On Rule

Conditions

If the user is authenticated by: Enter or select one or more identity providers.

And is a member of these groups: Enter or select one or more groups.

And is an administrator □

And is not one of these users: Enter or select one or more user accounts.

And the user's client IP address is ● Anywhere ○ In one or more of these network perimeters

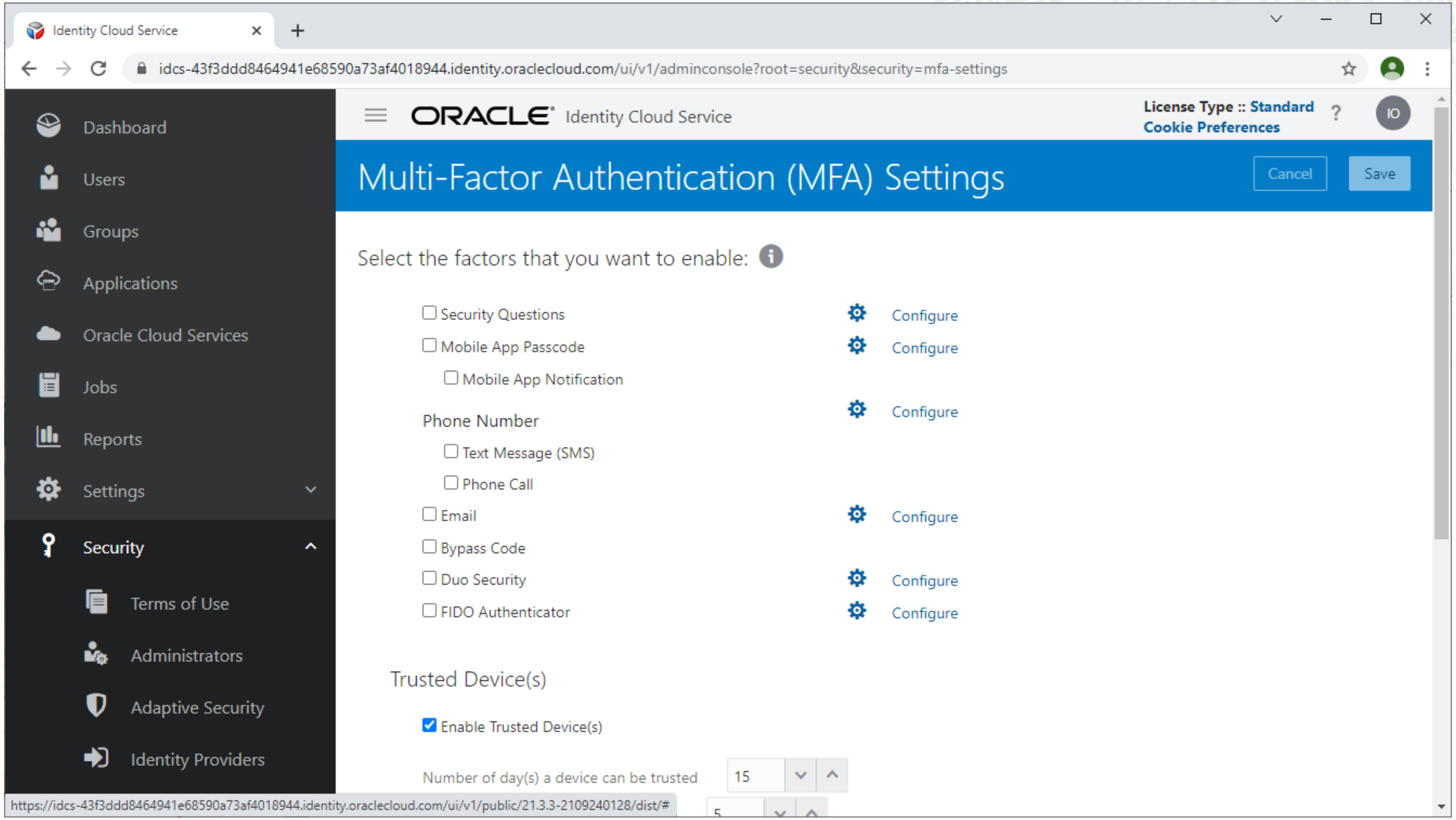
Actions

Access is: Allowed

□ Prompt for reauthentication

Save

Default configuration without MFA, no factors enabled


Identity Cloud Service
idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/adminconsole?root=security&security=mfa-settings
Dashboard
Users
Groups
Applications
Oracle Cloud Services
Jobs
Reports
Settings
Security
Terms of Use
Administrators
Adaptive Security
Identity Providers
ORACLE Identity Cloud Service
License Type :: Standard
Cookie Preferences
IO
Cancel
Save
https://idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/public/21.3.3-2109240128/dist/#

Multi-Factor Authentication (MFA) Settings

Select the factors that you want to enable:

- □ Security Questions — Configure
- □ Mobile App Passcode — Configure
  - □ Mobile App Notification
- Phone Number — Configure
  - □ Text Message (SMS)
  - □ Phone Call
- □ Email — Configure
- □ Bypass Code
- □ Duo Security — Configure
- □ FIDO Authenticator — Configure

Trusted Device(s)

☑ Enable Trusted Device(s)

Number of day(s) a device can be trusted: 15

Configuring MFA

Define setting of each Factor

Enable the preferred factor as a enabled factor

Enable MFA in the Single Signon Policy

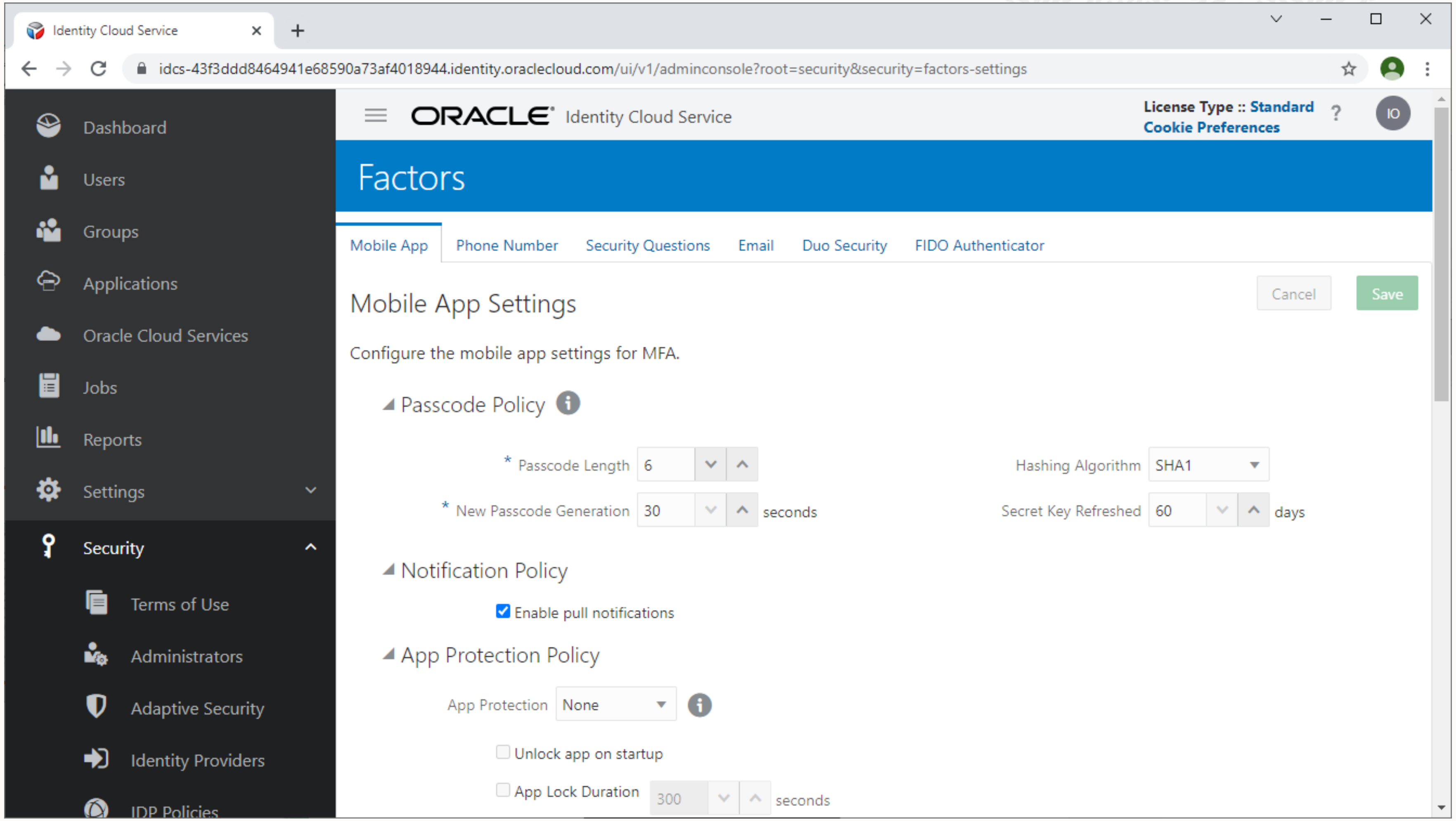
Note on Oracle Authenticator

- Download from Appstore
- Two types of MFA with authenticator, Pin or approval. Approval is valid for x number of days since last application of pin code

Define setting of each Factor

One tab for each factor type

This tab show the options For Oracle Authenticator



Factors

Mobile App | Phone Number | Security Questions | Email | Duo Security | FIDO Authenticator

Mobile App Settings

Cancel Save

Configure the mobile app settings for MFA.

Passcode Policy

* Passcode Length: 6

Hashing Algorithm: SHA1

* New Passcode Generation: 30 seconds

Secret Key Refreshed: 60 days

Notification Policy

☑ Enable pull notifications

App Protection Policy

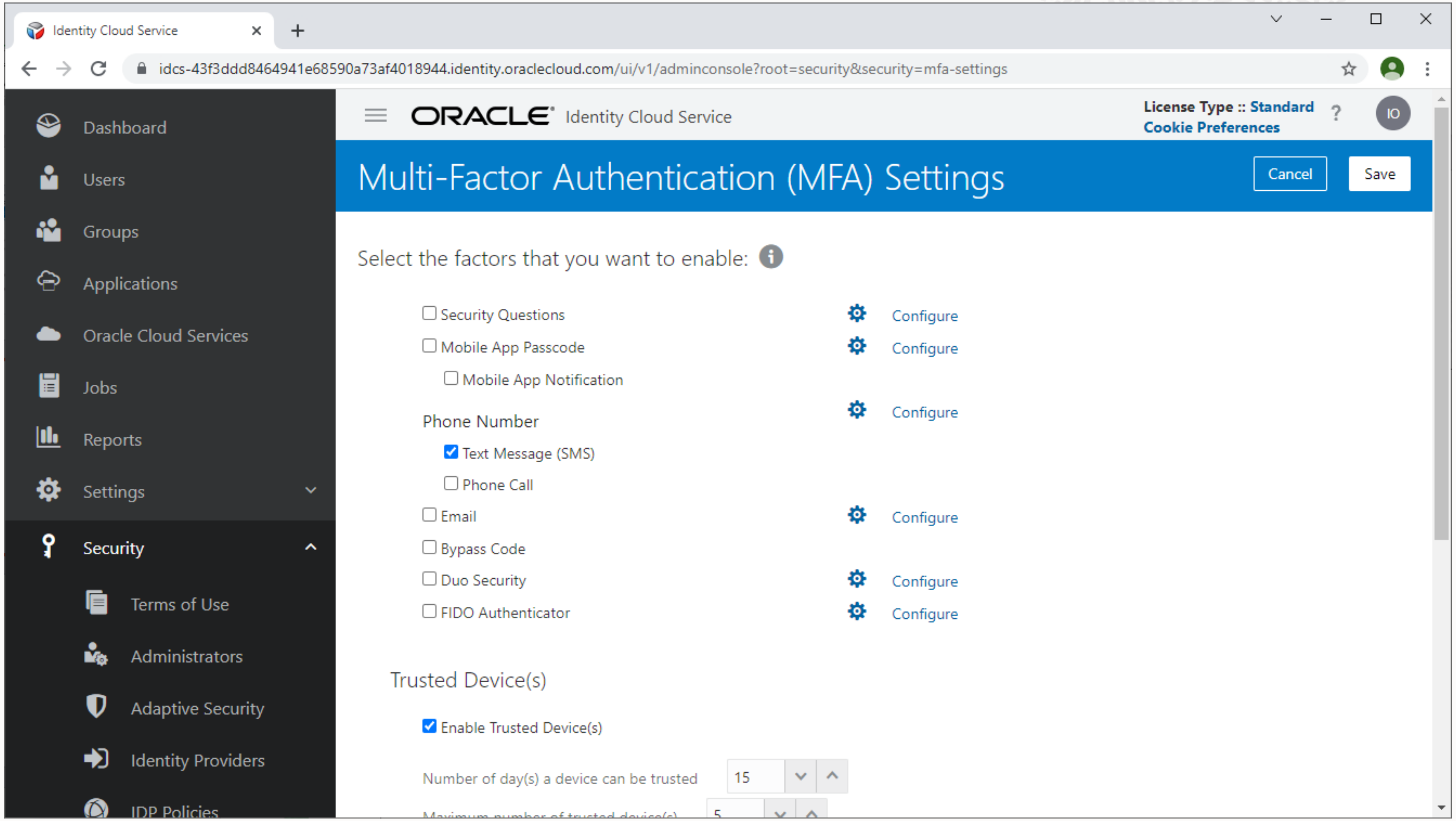
App Protection: None

□ Unlock app on startup

□ App Lock Duration 300 seconds

Enable the preferred factor as a enabled factor

SMS example



Multi-Factor Authentication (MFA) Settings

Select the factors that you want to enable:

- □ Security Questions — Configure
- □ Mobile App Passcode — Configure
  - □ Mobile App Notification
- Phone Number — Configure
  - ☑ Text Message (SMS)
  - □ Phone Call
- □ Email — Configure
- □ Bypass Code
- □ Duo Security — Configure
- □ FIDO Authenticator — Configure

Trusted Device(s)

☑ Enable Trusted Device(s)

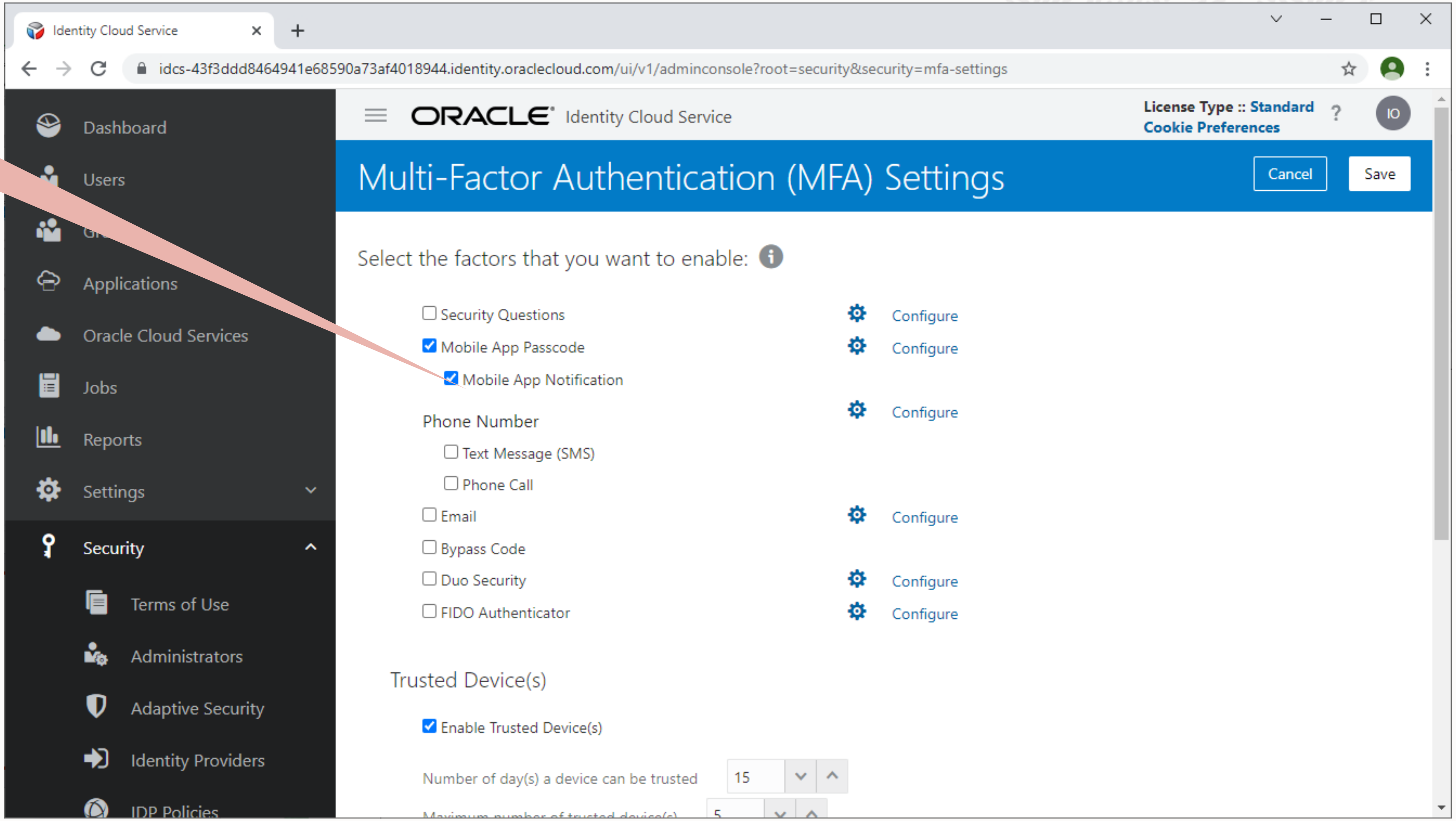
Number of day(s) a device can be trusted: 15

Maximum number of trusted device(s): 5

Enable the preferred factor as a enabled factor

Authenticator example

Enable this is approval in the app is sufficient



Multi-Factor Authentication (MFA) Settings

Select the factors that you want to enable:

- □ Security Questions — Configure
- ☑ Mobile App Passcode — Configure
  - ☑ Mobile App Notification
- Phone Number — Configure
  - □ Text Message (SMS)
  - □ Phone Call
- □ Email — Configure
- □ Bypass Code
- □ Duo Security — Configure
- □ FIDO Authenticator — Configure

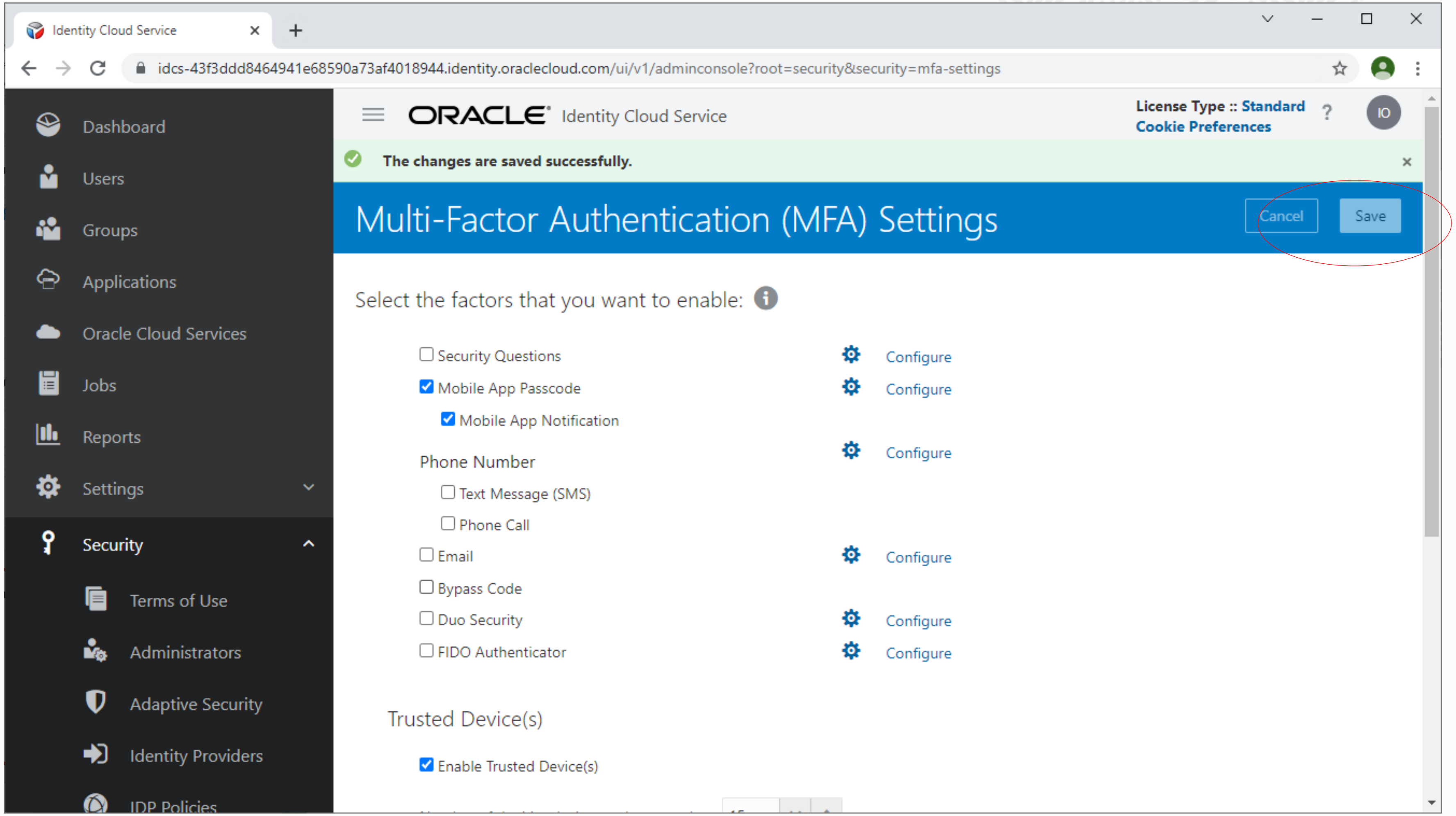
Trusted Device(s)

☑ Enable Trusted Device(s)

Number of day(s) a device can be trusted: 15

Maximum number of trusted device(s): 5

Remember to save



The changes are saved successfully.

Multi-Factor Authentication (MFA) Settings

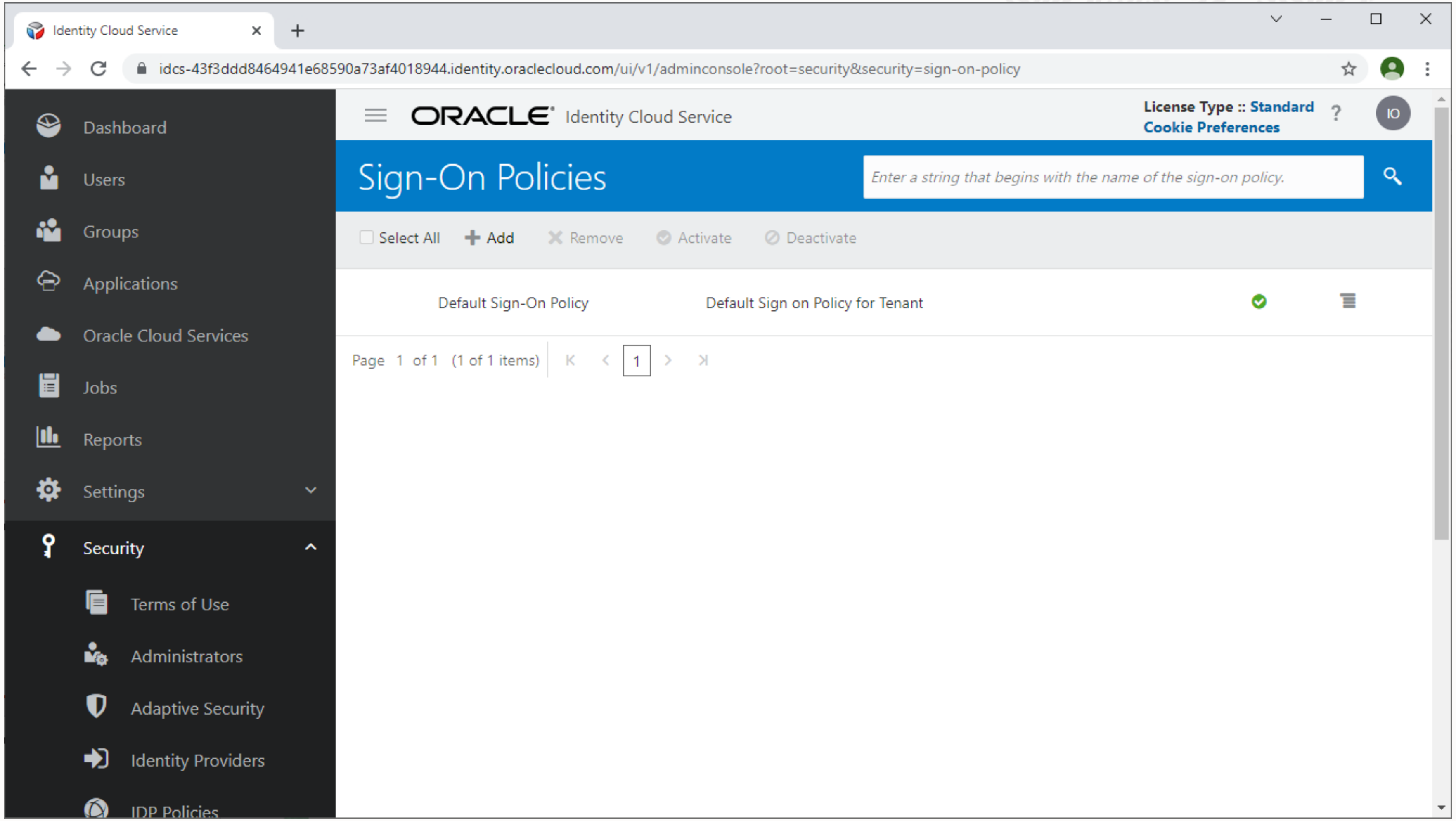
Select the factors that you want to enable:

- ☐ Security Questions
- ☑ Mobile App Passcode
  - ☑ Mobile App Notification
- Phone Number
  - ☐ Text Message (SMS)
  - ☐ Phone Call
- ☐ Email
- ☐ Bypass Code
- ☐ Duo Security
- ☐ FIDO Authenticator

Trusted Device(s)

- ☑ Enable Trusted Device(s)

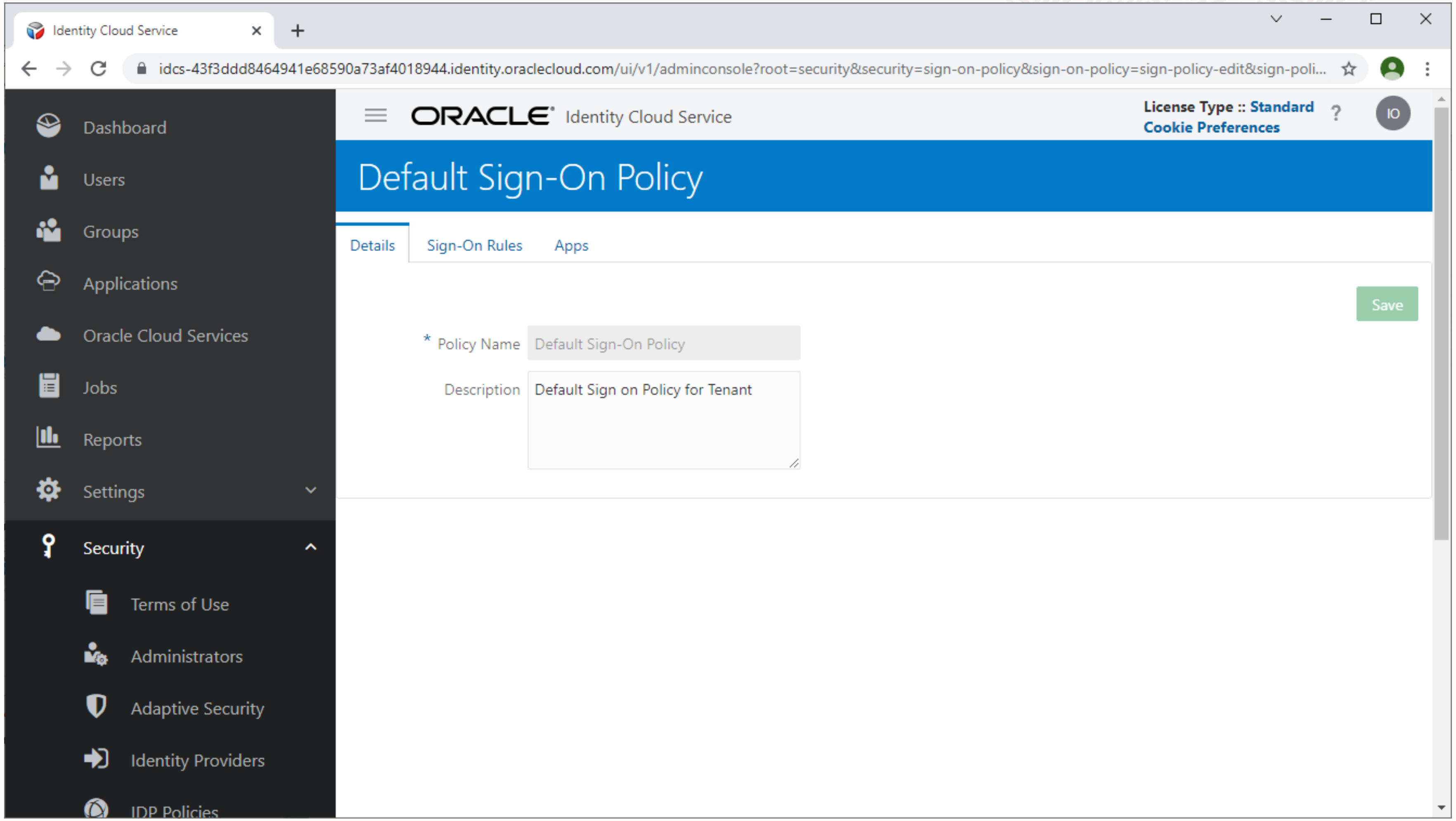
Enable MFA in the Single Signon Policy



Default Sign-On Policy | Default Sign on Policy for Tenant | ✓

Page 1 of 1 (1 of 1 items) 1

Enable MFA in the Single Signon Policy



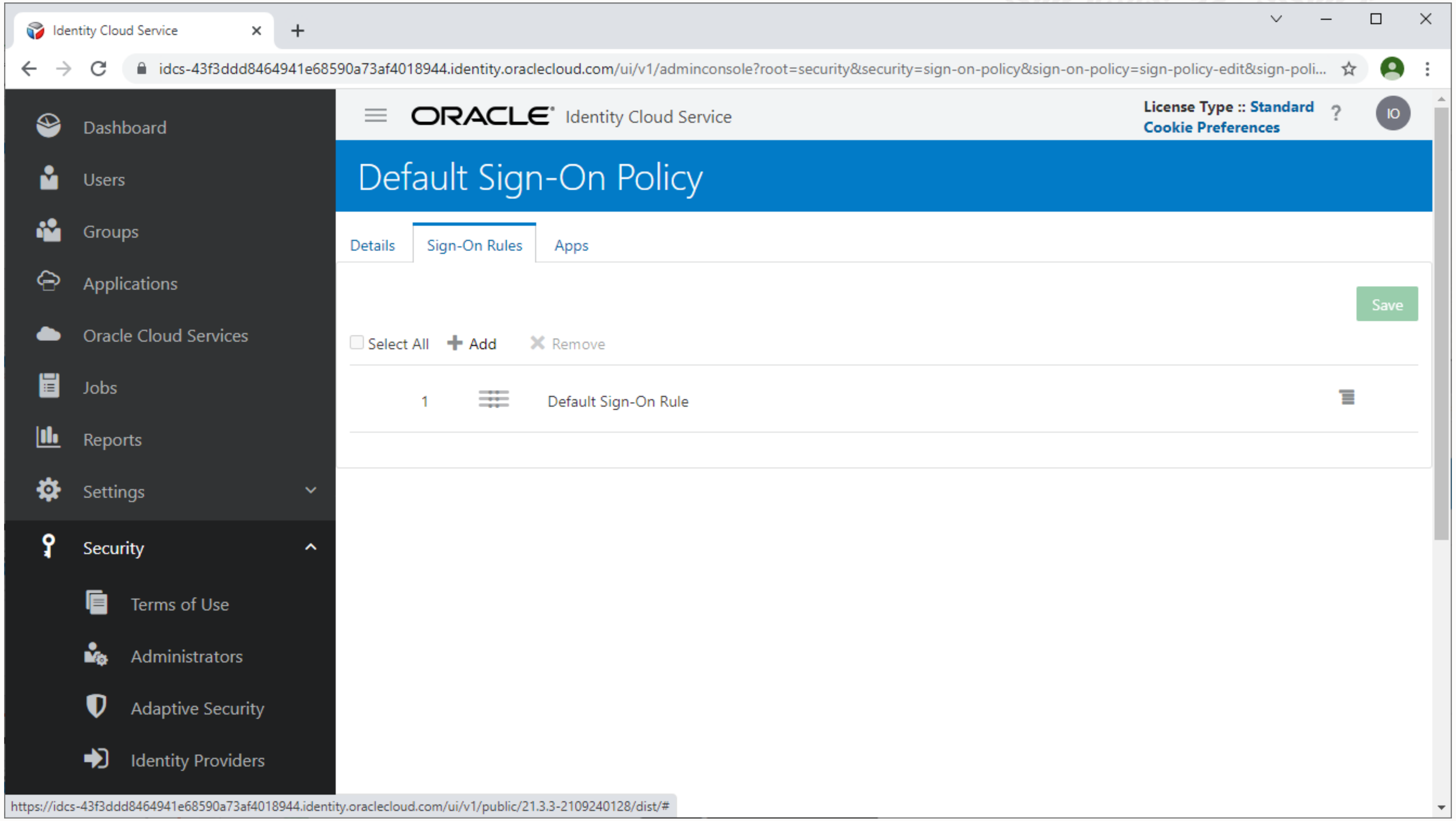
idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/adminconsole?root=security&security=sign-on-policy&sign-on-policy=sign-policy-edit&sign-poli...

Default Sign-On Policy

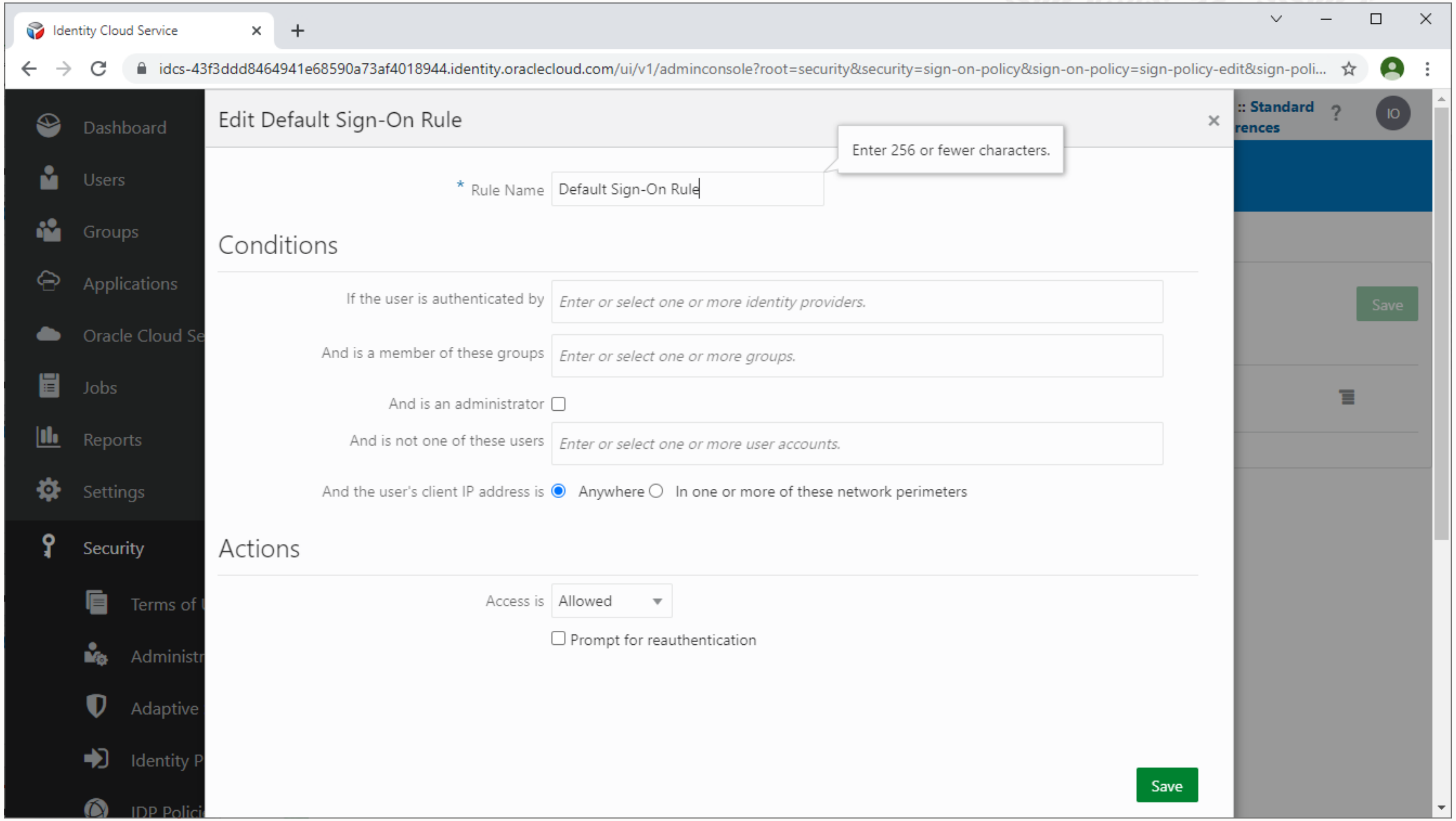
* Policy Name: Default Sign-On Policy

Description: Default Sign on Policy for Tenant

Enable MFA in the Single Signon Policy


Identity Cloud Service
idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/adminconsole?root=security&security=sign-on-policy&sign-on-policy=sign-policy-edit&sign-poli...
Dashboard
Users
Groups
Applications
Oracle Cloud Services
Jobs
Reports
Settings
Security
Terms of Use
Administrators
Adaptive Security
Identity Providers
ORACLE Identity Cloud Service
License Type :: Standard
Cookie Preferences
IO
Default Sign-On Policy
Details
Sign-On Rules
Apps
Save
Select All
Add
Remove
1
Default Sign-On Rule
https://idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/public/21.3.3-2109240128/dist/#

Enable MFA in the Single Signon Policy



Identity Cloud Service
idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/adminconsole?root=security&security=sign-on-policy&sign-on-policy=sign-policy-edit&sign-poli...
Dashboard
Users
Groups
Applications
Oracle Cloud Se
Jobs
Reports
Settings
Security
Terms of
Administr
Adaptive
Identity P
IDP Polici
:: Standard
rences
IO
Save

Edit Default Sign-On Rule

Enter 256 or fewer characters.

* Rule Name: Default Sign-On Rule

Conditions

If the user is authenticated by: Enter or select one or more identity providers.

And is a member of these groups: Enter or select one or more groups.

And is an administrator □

And is not one of these users: Enter or select one or more user accounts.

And the user's client IP address is ● Anywhere ○ In one or more of these network perimeters

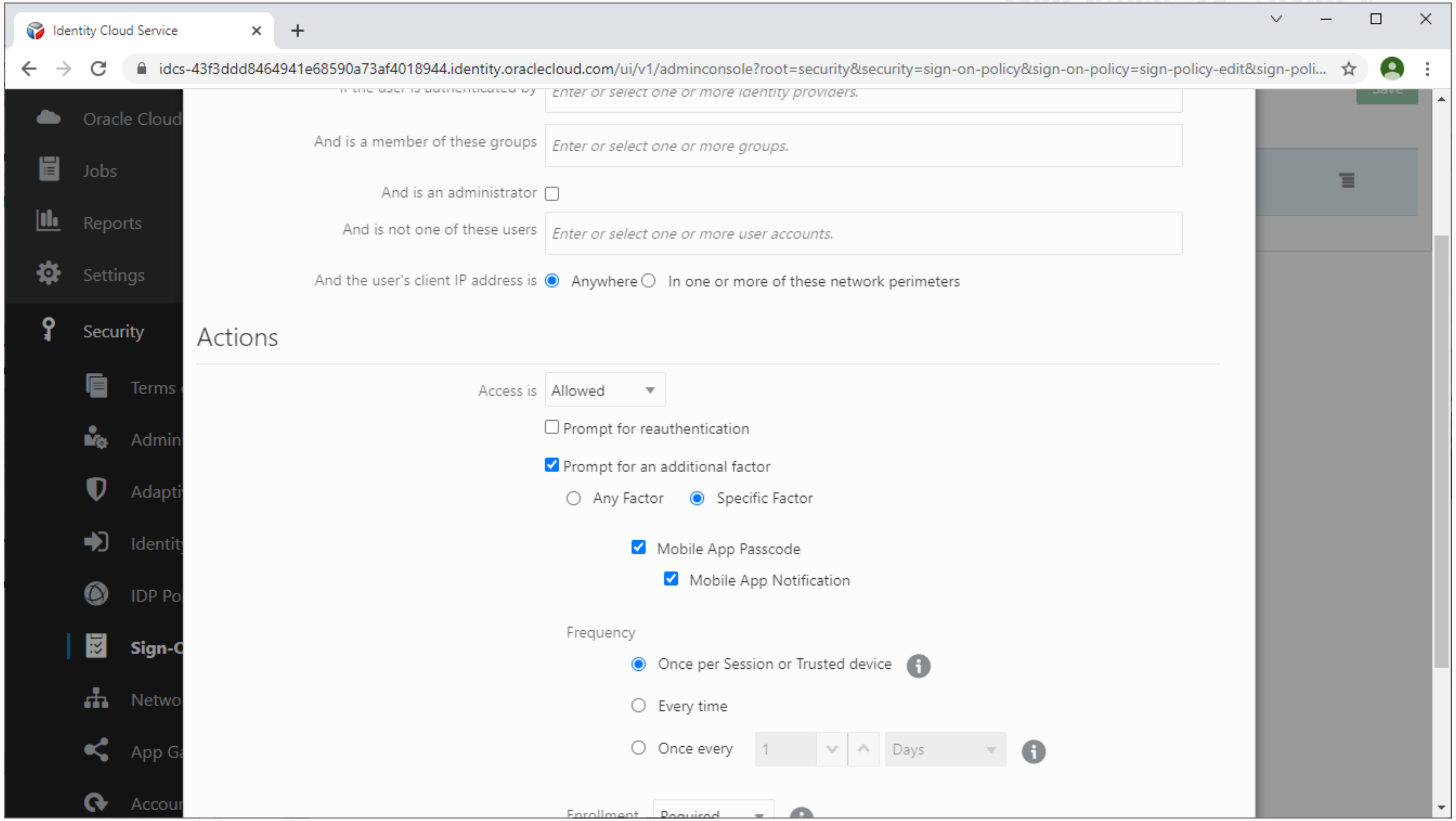
Actions

Access is: Allowed

□ Prompt for reauthentication

Save

Enable MFA in the Single Signon Policy


Identity Cloud Service
idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/adminconsole?root=security&security=sign-on-policy&sign-on-policy=sign-policy-edit&sign-poli...
Oracle Cloud
Jobs
Reports
Settings
Security
Terms
Admin
Adapti
Identit
IDP Po
Sign-O
Netwo
App Ga
Accour
Save

If the user is authenticated by: Enter or select one or more identity providers.

And is a member of these groups: Enter or select one or more groups.

And is an administrator ☐

And is not one of these users: Enter or select one or more user accounts.

And the user's client IP address is ● Anywhere ○ In one or more of these network perimeters

Actions

Access is: Allowed

☐ Prompt for reauthentication

☑ Prompt for an additional factor

○ Any Factor ● Specific Factor

☑ Mobile App Passcode

☑ Mobile App Notification

Frequency

● Once per Session or Trusted device

○ Every time

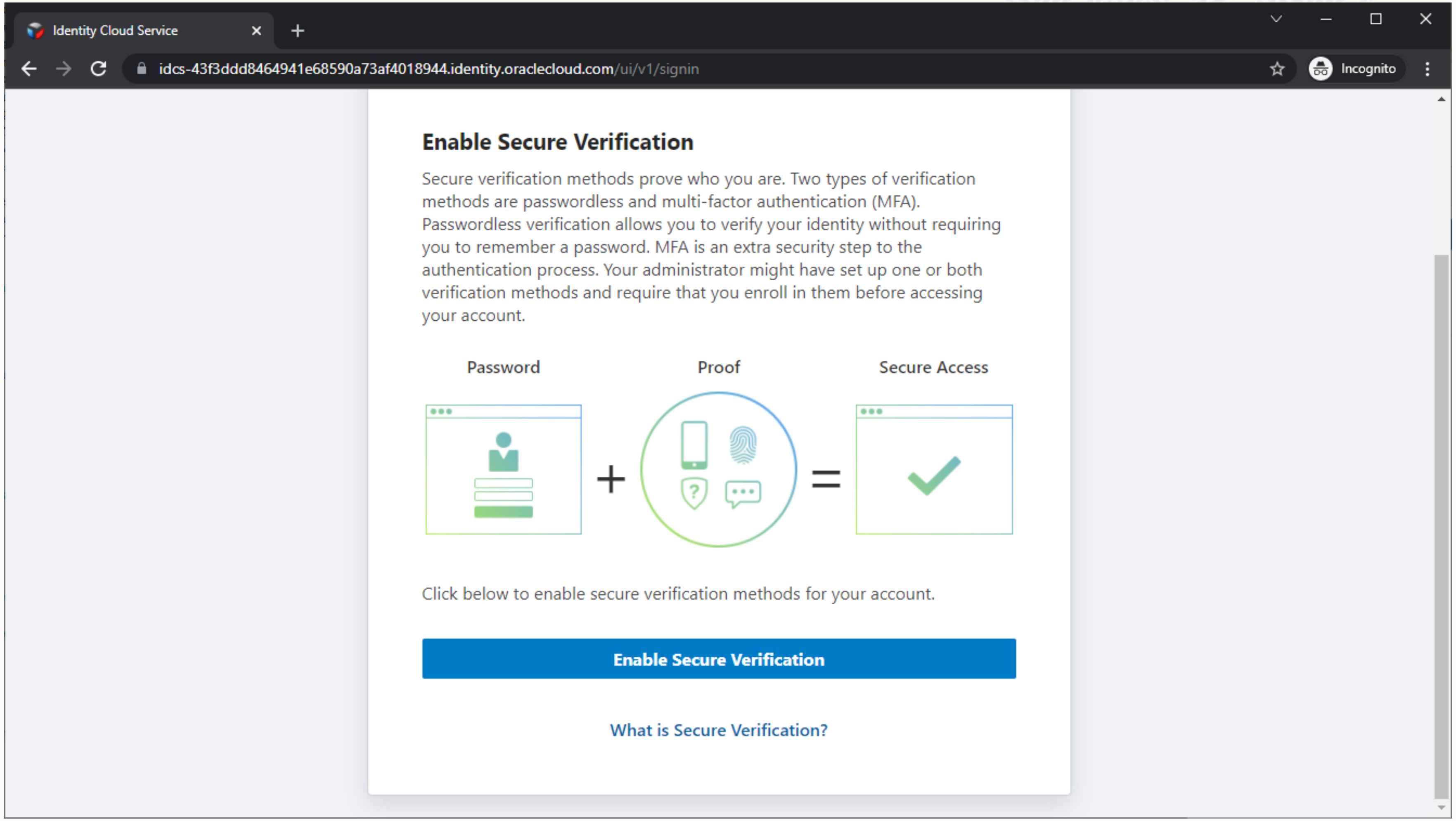
○ Once every 1 Days

Enrollment: Required

User enrolment

The users are asked to enrol their MFA first time they log on after the MFA is enabled

Mobile app enrolment



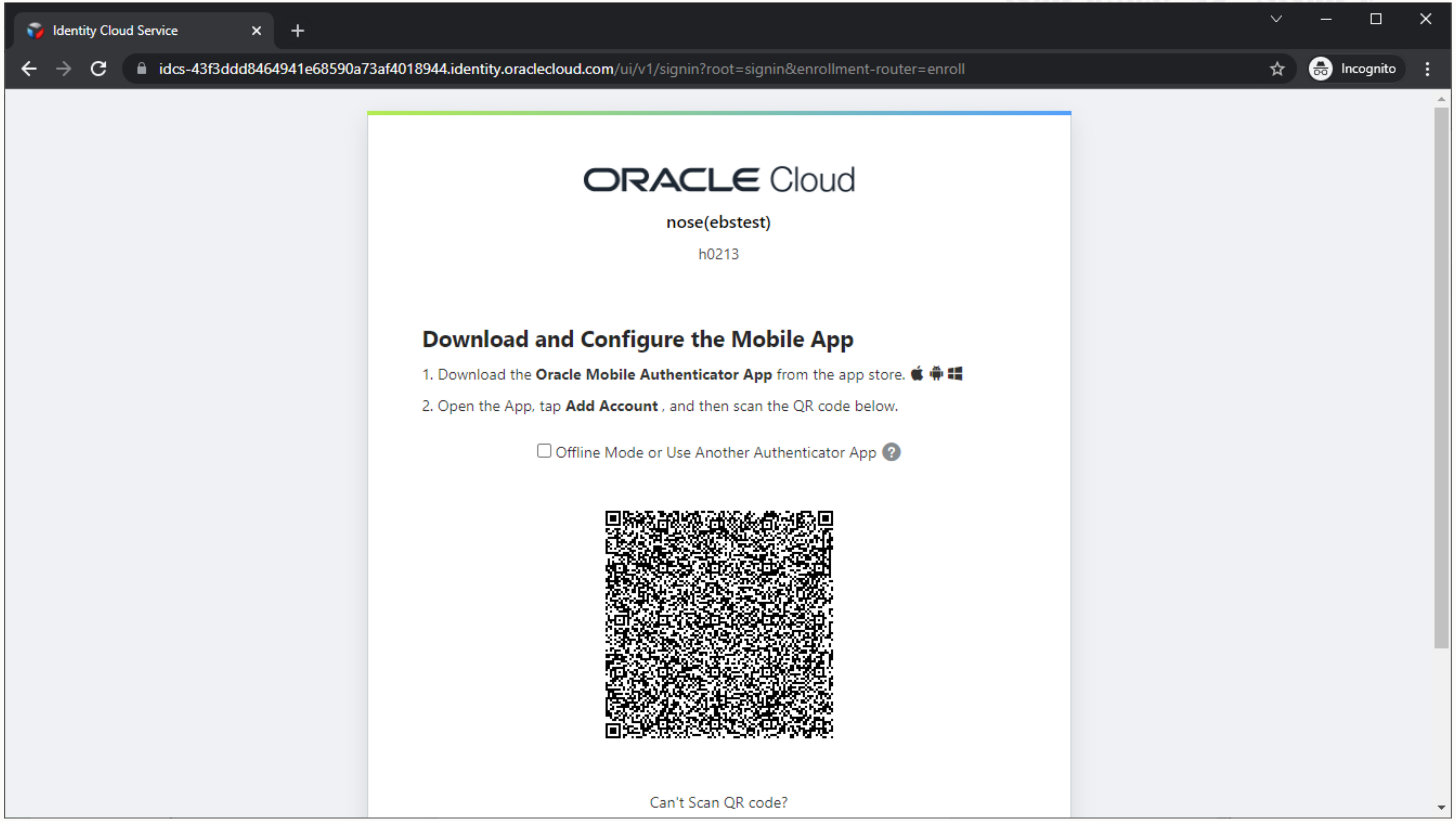
Identity Cloud Service
idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/signin
Incognito

Enable Secure Verification

Secure verification methods prove who you are. Two types of verification methods are passwordless and multi-factor authentication (MFA). Passwordless verification allows you to verify your identity without requiring you to remember a password. MFA is an extra security step to the authentication process. Your administrator might have set up one or both verification methods and require that you enroll in them before accessing your account.

Click below to enable secure verification methods for your account.

Mobile app enrolment



Identity Cloud Service
idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/signin?root=signin&enrollment-router=enroll
Incognito
ORACLE Cloud

nose(ebstest)

h0213

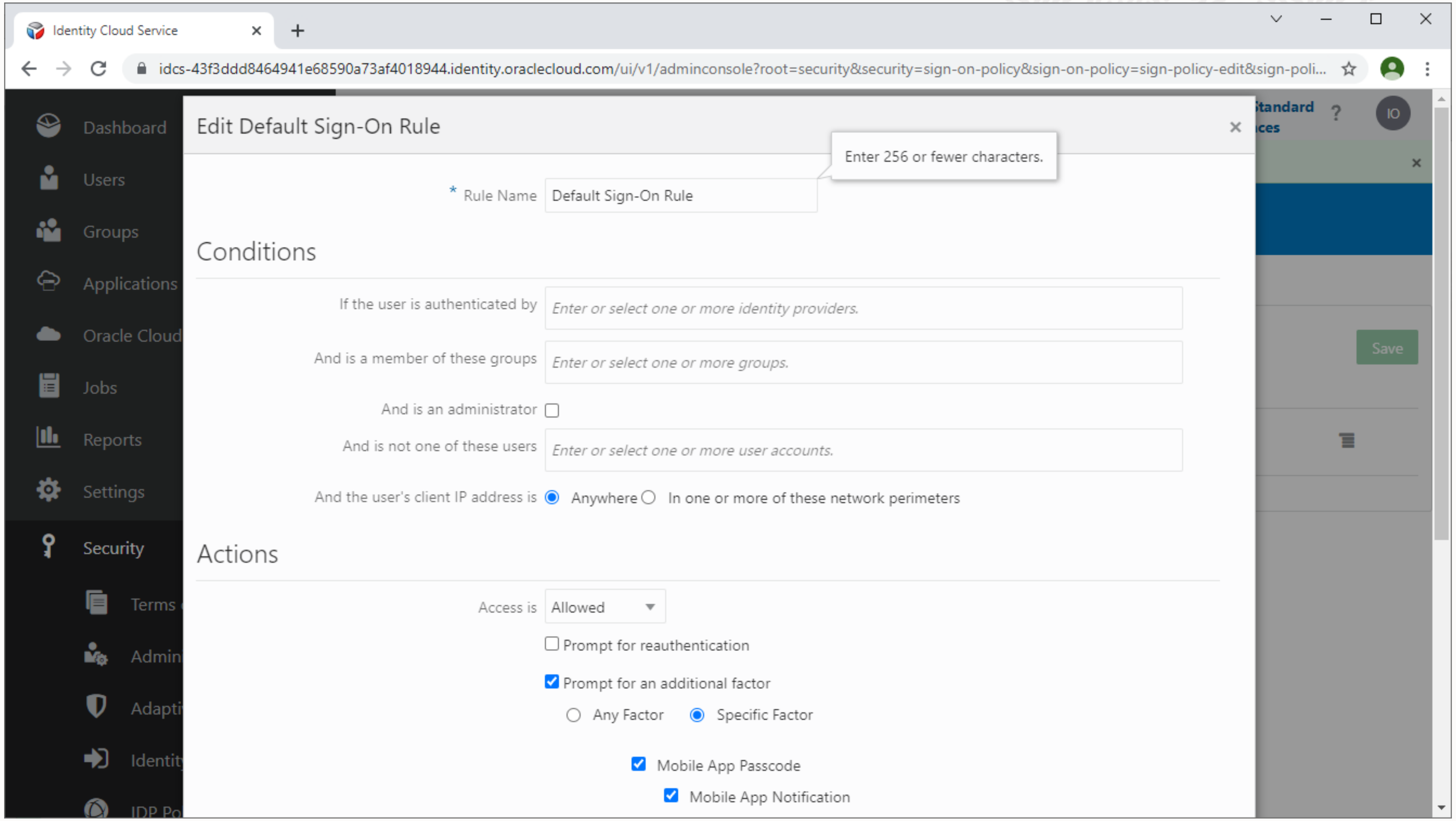
Download and Configure the Mobile App

1. Download the **Oracle Mobile Authenticator App** from the app store.
2. Open the App, tap **Add Account** , and then scan the QR code below.

□ Offline Mode or Use Another Authenticator App

Can't Scan QR code?

Enabeling the preferred factors in the SSO Policy



Identity Cloud Service
idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/adminconsole?root=security&security=sign-on-policy&sign-on-policy=sign-policy-edit&sign-poli...
Dashboard
Users
Groups
Applications
Oracle Cloud
Jobs
Reports
Settings
Security
Terms
Admin
Adapti
Identit
IDP Po
Save

Edit Default Sign-On Rule

Enter 256 or fewer characters.

* Rule Name: Default Sign-On Rule

Conditions

If the user is authenticated by: *Enter or select one or more identity providers.*

And is a member of these groups: *Enter or select one or more groups.*

And is an administrator ☐

And is not one of these users: *Enter or select one or more user accounts.*

And the user's client IP address is ● Anywhere ○ In one or more of these network perimeters

Actions

Access is: Allowed

☐ Prompt for reauthentication

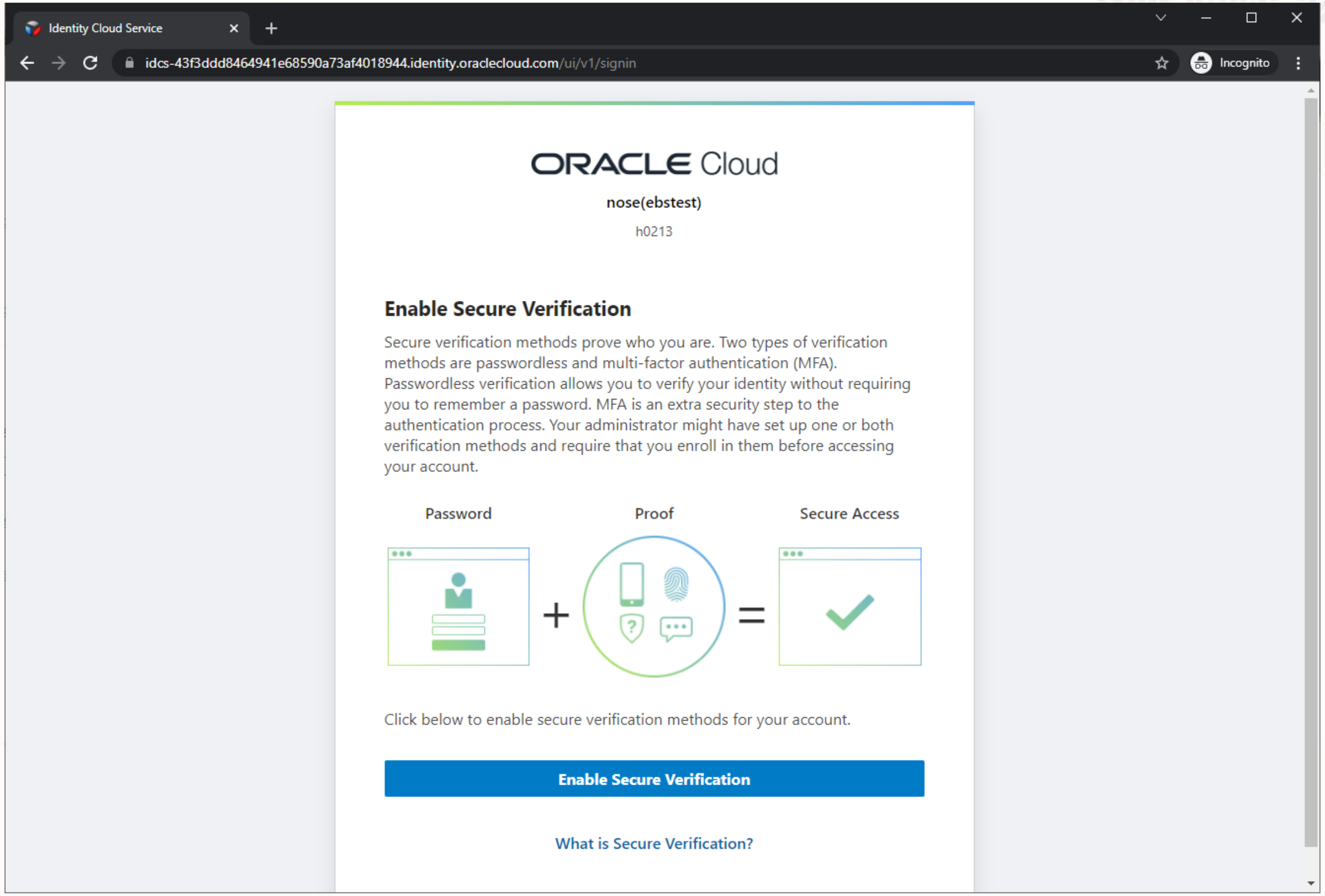
☑ Prompt for an additional factor

○ Any Factor ● Specific Factor

☑ Mobile App Passcode

☑ Mobile App Notification

SMS enrolment



Identity Cloud Service
idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/signin
Incognito

ORACLE Cloud

nose(ebstest)

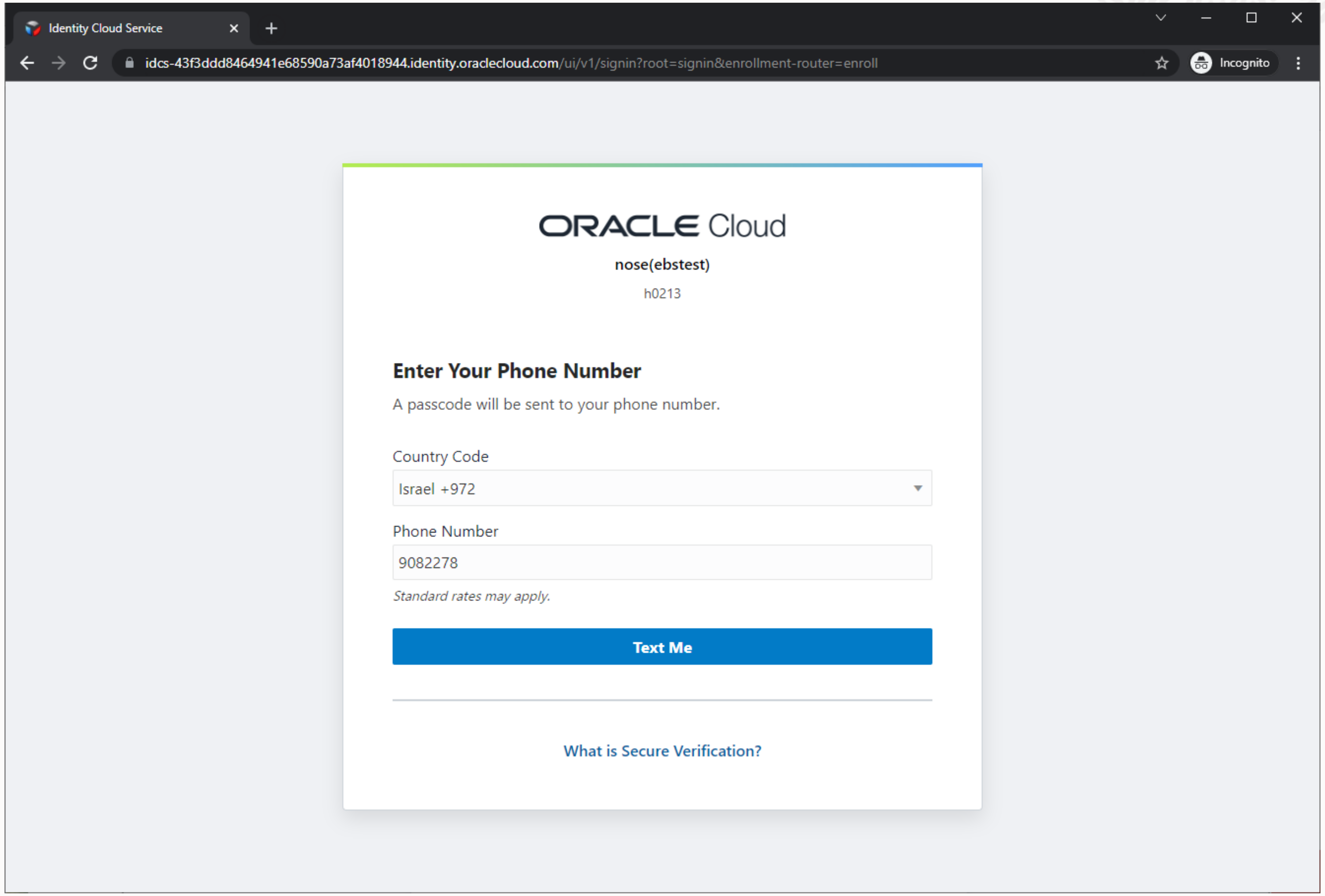
h0213

Enable Secure Verification

Secure verification methods prove who you are. Two types of verification methods are passwordless and multi-factor authentication (MFA). Passwordless verification allows you to verify your identity without requiring you to remember a password. MFA is an extra security step to the authentication process. Your administrator might have set up one or both verification methods and require that you enroll in them before accessing your account.

Click below to enable secure verification methods for your account.

SMS enrolment


Identity Cloud Service
idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/signin?root=signin&enrollment-router=enroll
Incognito

ORACLE Cloud

nose(ebstest)

h0213

Enter Your Phone Number

A passcode will be sent to your phone number.

Country Code

Israel +972

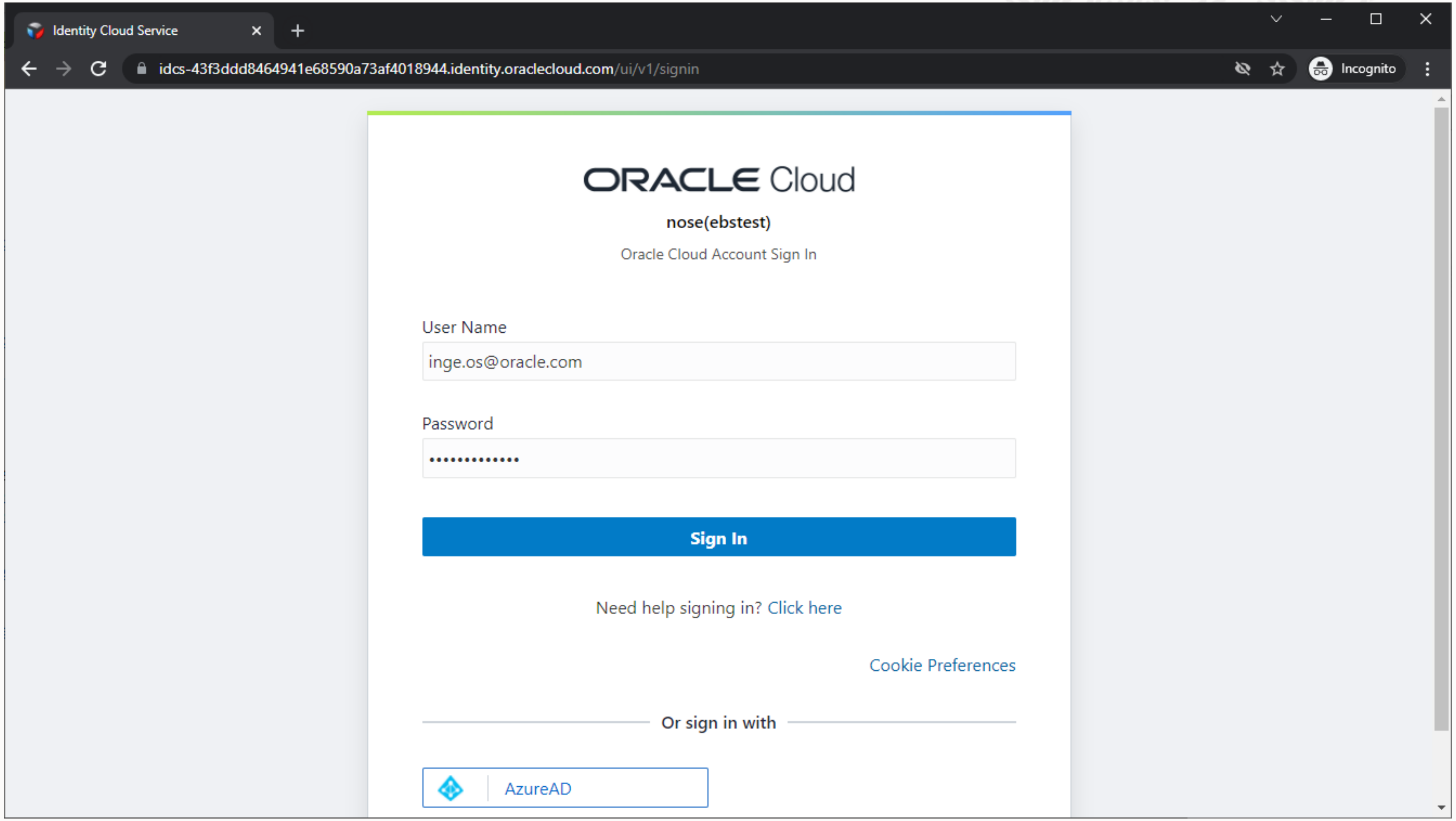
Phone Number

9082278

Standard rates may apply.

Text Me
What is Secure Verification?

First time logon



Identity Cloud Service
idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/signin
Incognito

ORACLE Cloud

nose(ebstest)

Oracle Cloud Account Sign In

User Name: inge.os@oracle.com

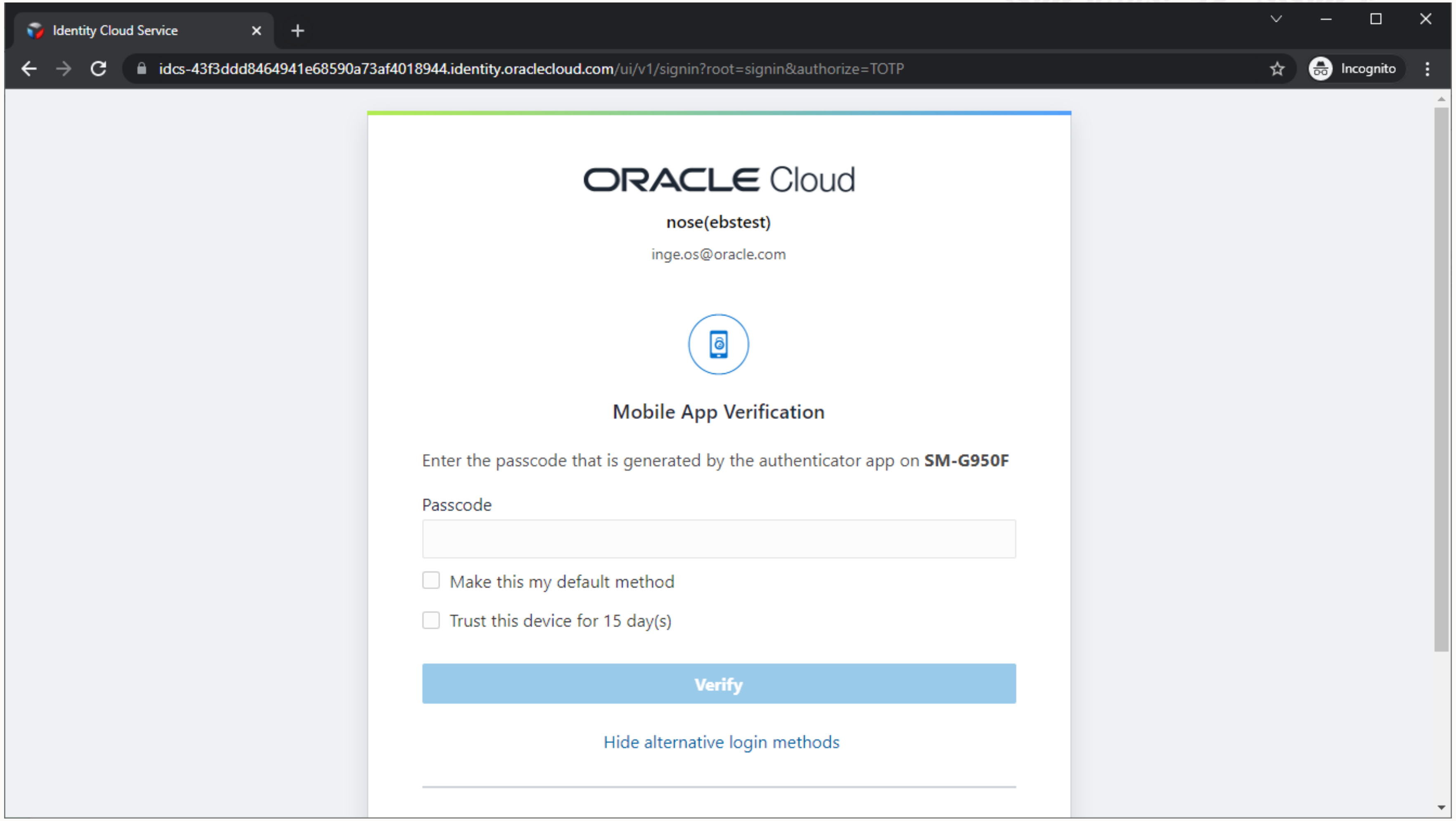
Password: •••••••••••••

Need help signing in? Click here

Cookie Preferences

Or sign in with

Mobile app MFA logon



Identity Cloud Service
idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/signin?root=signin&authorize=TOTP
Incognito

ORACLE Cloud

nose(ebstest)

inge.os@oracle.com

Mobile App Verification

Enter the passcode that is generated by the authenticator app on **SM-G950F**

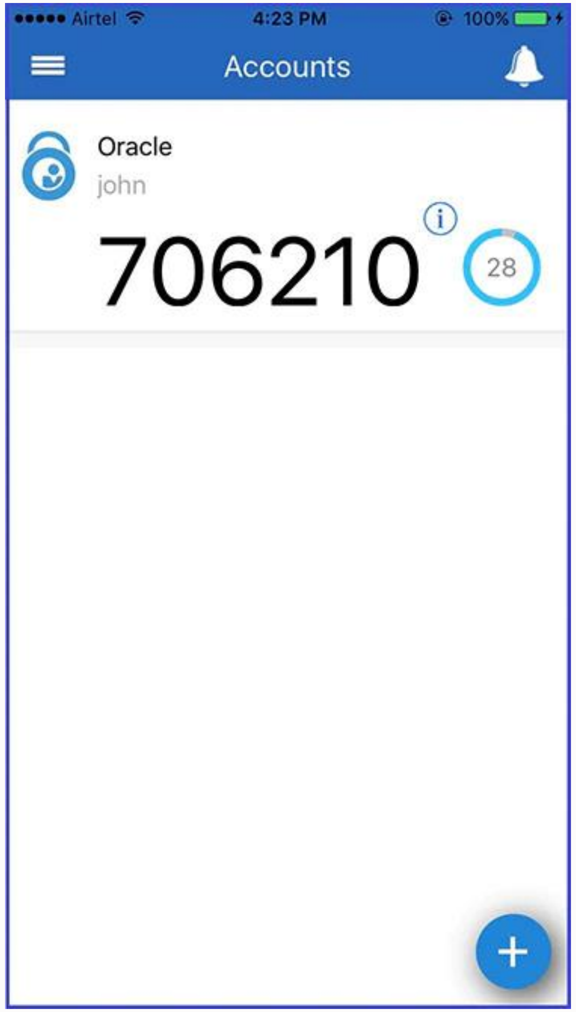
Passcode

□ Make this my default method

□ Trust this device for 15 day(s)

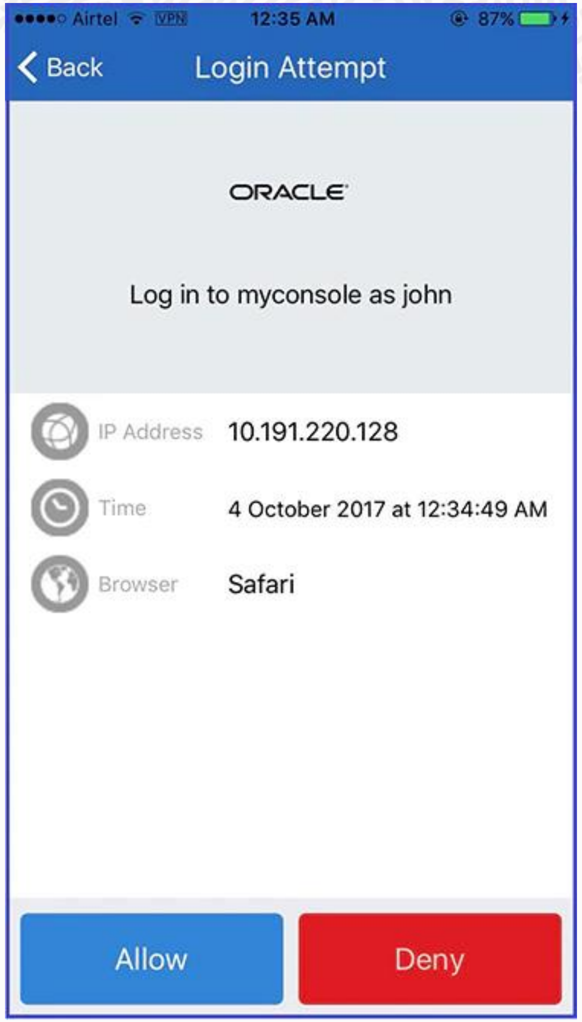
Verify
Hide alternative login methods

Mobile Authenticator



Oracle
john
706210
28

Pincode verification



Log in to myconsole as john

IP Address 10.191.220.128
Time 4 October 2017 at 12:34:49 AM
Browser Safari

Push verification

References

https://docs.oracle.com/en/cloud/paas/identity-cloud/uaids/manage-oracle-identity-cloud-service-multi-factor-authentication-settings1.html

https://www.oracle.com/webfolder/technetwork/tutorials/infographics/idcs_enabling_and_configuring_mfa/index.html

https://blogs.oracle.com/cloudsecurity/post/multi-factor-authentication-with-oracle-identity-cloud-service