



Configuration of IDCS MFA

Inge Os

Inge.os@oracle.com

The flow of configuring MFA

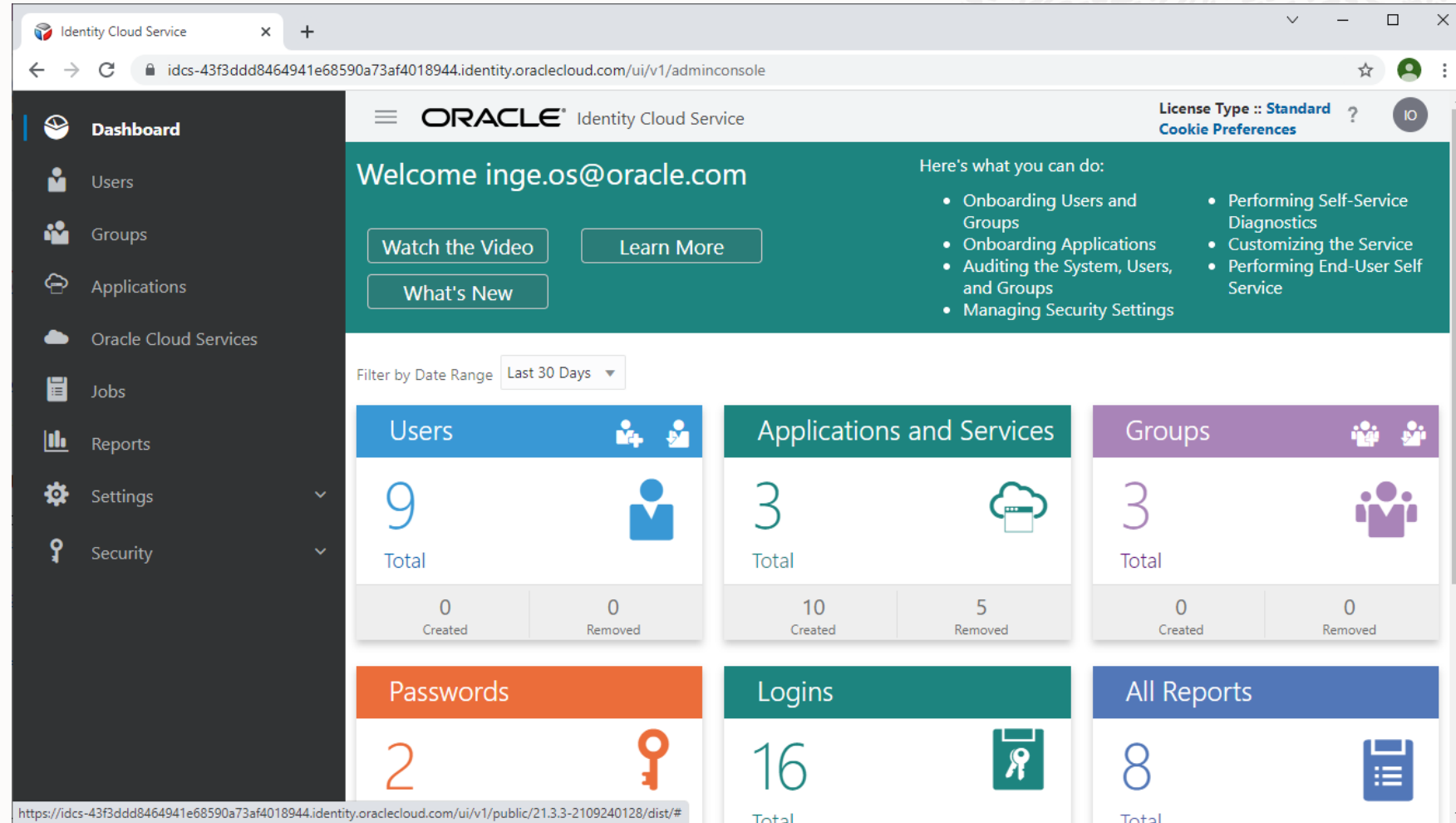
MFA is a Standard feature of IDCS, and the IDCS stripe is required to be on any of the non-foundation subscription type

When MFA is enabled, users are requested to register themselves for MFA, ie. Add phone number 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



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...

Edit Default Sign-On Rule

* Rule Name Enter 256 or fewer characters.

Conditions

If the user is authenticated by

And is a member of these groups

And is an administrator ☐

And is not one of these users

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

Actions

Access is

☐ 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

License Type :: Standard
Cookie Preferences

Multi-Factor Authentication (MFA) Settings

Cancel Save

Select the factors that you want to enable: ⓘ

- ☐ Security Questions [Configure](#)
- ☐ Mobile App Passcode [Configure](#)
- ☐ Mobile App Notification [Configure](#)
- ☐ Phone Number [Configure](#)
- ☐ Text Message (SMS)
- ☐ Phone Call
- ☐ Email [Configure](#)
- ☐ Bypass Code [Configure](#)
- ☐ 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

Identity Cloud Service

idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/adminconsole?root=security&security=factors-settings

ORACLE Identity Cloud Service

License Type :: Standard
Cookie Preferences

Factors

Mobile App Phone Number Security Questions Email Duo Security FIDO Authenticator

Mobile App Settings

Configure the mobile app settings for MFA.

Passcode Policy ⓘ

* Passcode Length 6

* New Passcode Generation 30 seconds

Hashing Algorithm SHA1

Secret Key Refreshed 60 days

Notification Policy

☒ Enable pull notifications

App Protection Policy

App Protection None ⓘ

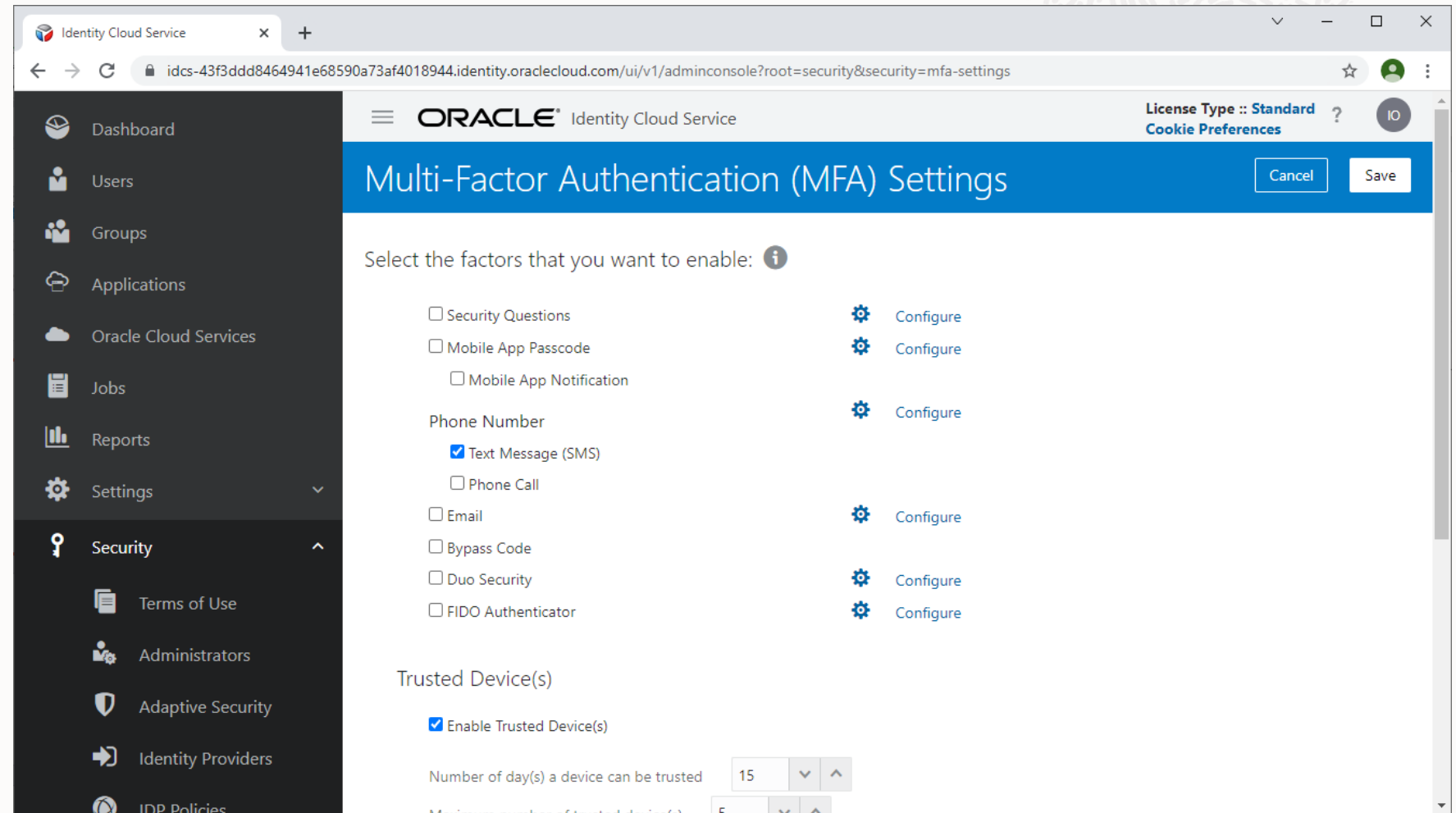
☐ Unlock app on startup

☐ App Lock Duration 300 seconds

Cancel Save

Enable the preferred factor as a enabled factor

SMS example



Identity Cloud Service

idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/adminconsole?root=security&security=mfa-settings

License Type :: Standard
Cookie Preferences

Multi-Factor Authentication (MFA) Settings

Cancel Save

Select the factors that you want to enable: ⓘ

- ☐ Security Questions [Configure](#)
- ☐ Mobile App Passcode [Configure](#)
- ☐ Mobile App Notification [Configure](#)
- Phone Number [Configure](#)
 - ☒ Text Message (SMS)
 - ☐ Phone Call
- ☐ Email [Configure](#)
- ☐ Bypass Code [Configure](#)
- ☐ Duo Security [Configure](#)
- ☐ FIDO Authenticator [Configure](#)

Trusted Device(s)

- ☒ Enable Trusted Device(s)

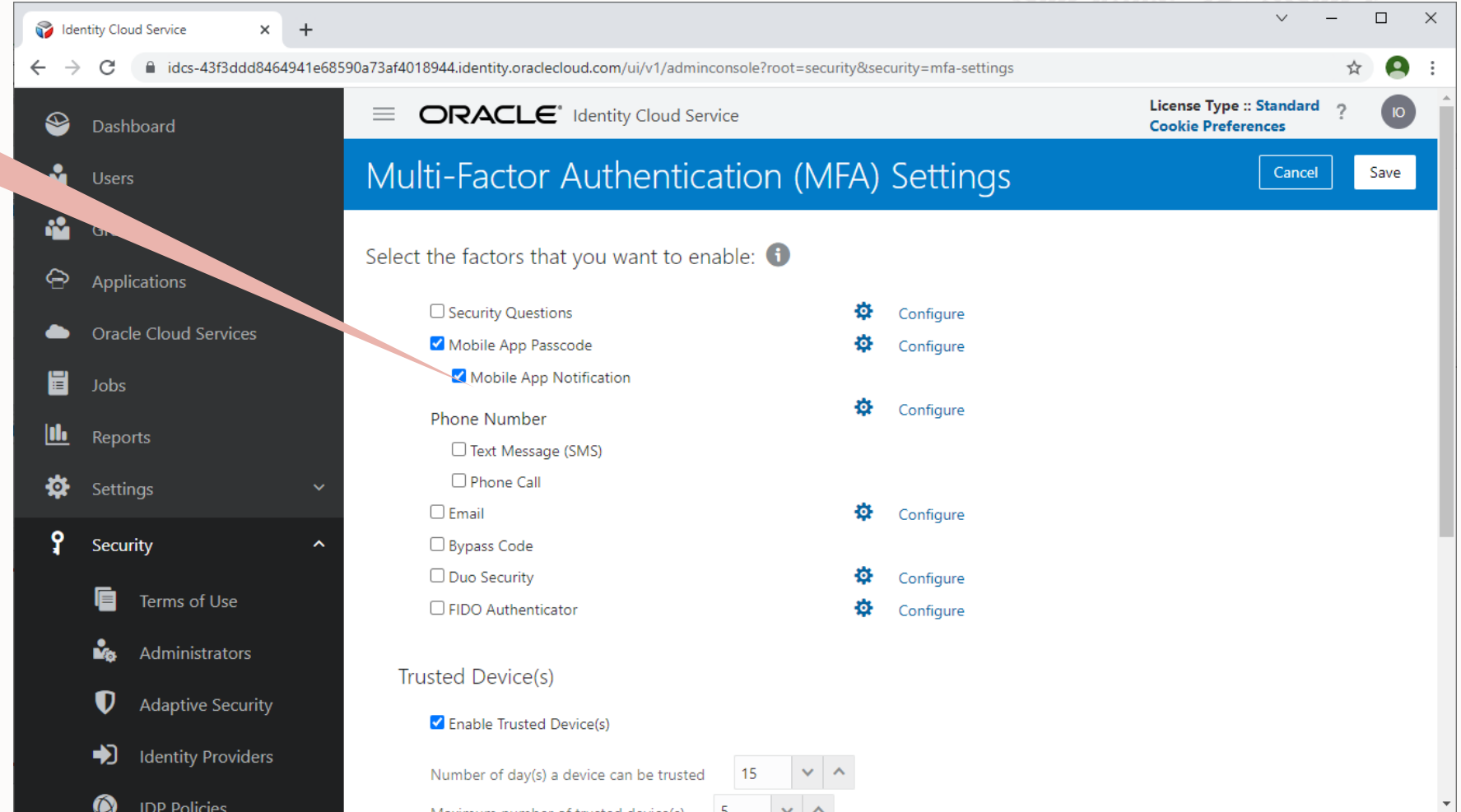
Number of day(s) a device can be trusted: 15

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



Identity Cloud Service

idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/adminconsole?root=security&security=mfa-settings

ORACLE Identity Cloud Service

License Type :: Standard ?
Cookie Preferences

Multi-Factor Authentication (MFA) Settings

Cancel Save

Select the factors that you want to enable: ⓘ

- ☐ Security Questions [Configure](#)
- ☒ Mobile App Passcode [Configure](#)
- ☒ Mobile App Notification [Configure](#)

Phone Number [Configure](#)

- ☐ Text Message (SMS)
- ☐ Phone Call

Email [Configure](#)

- ☐ Bypass Code [Configure](#)
- ☐ Duo Security [Configure](#)
- ☐ FIDO Authenticator [Configure](#)

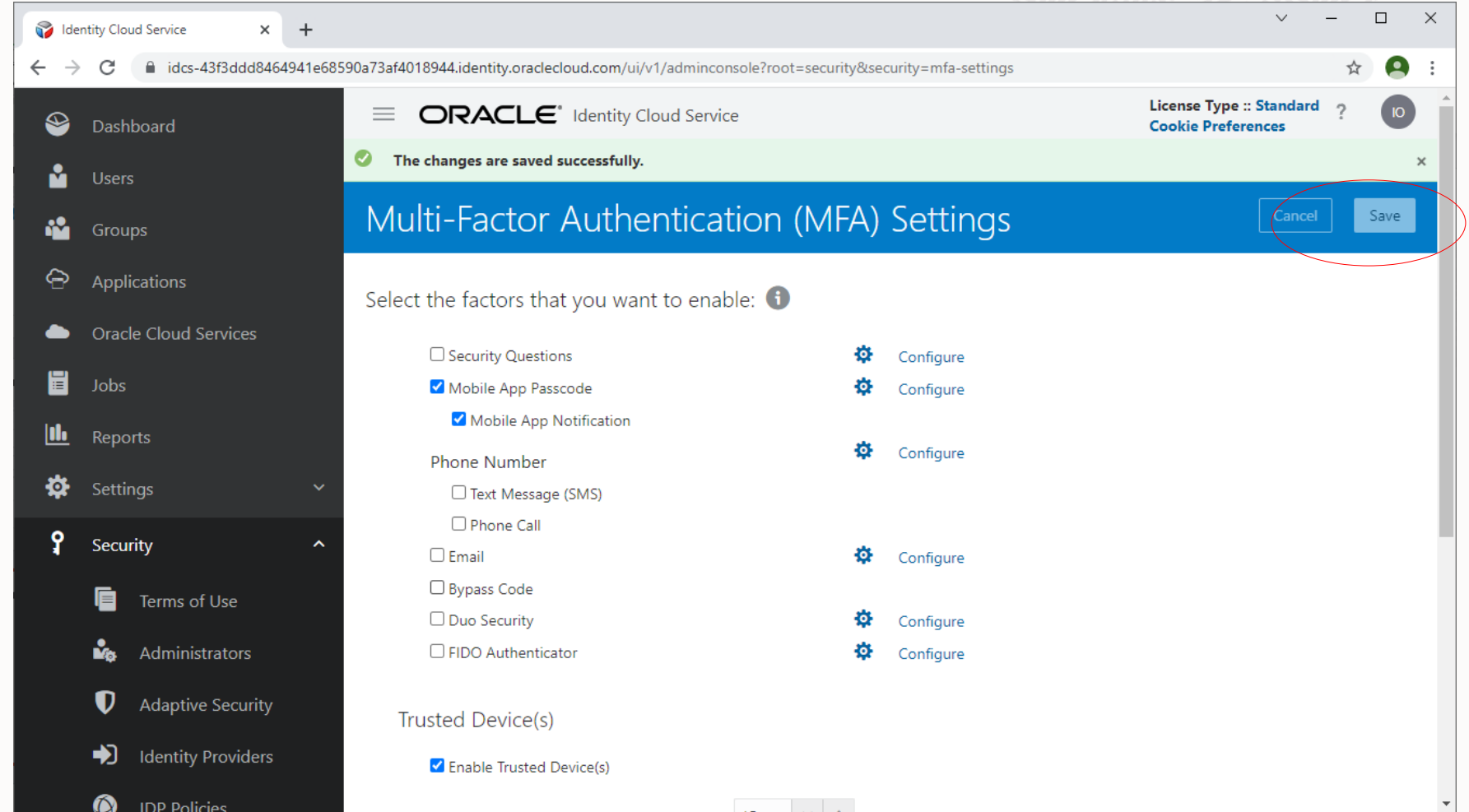
Trusted Device(s)

- ☒ Enable Trusted Device(s)

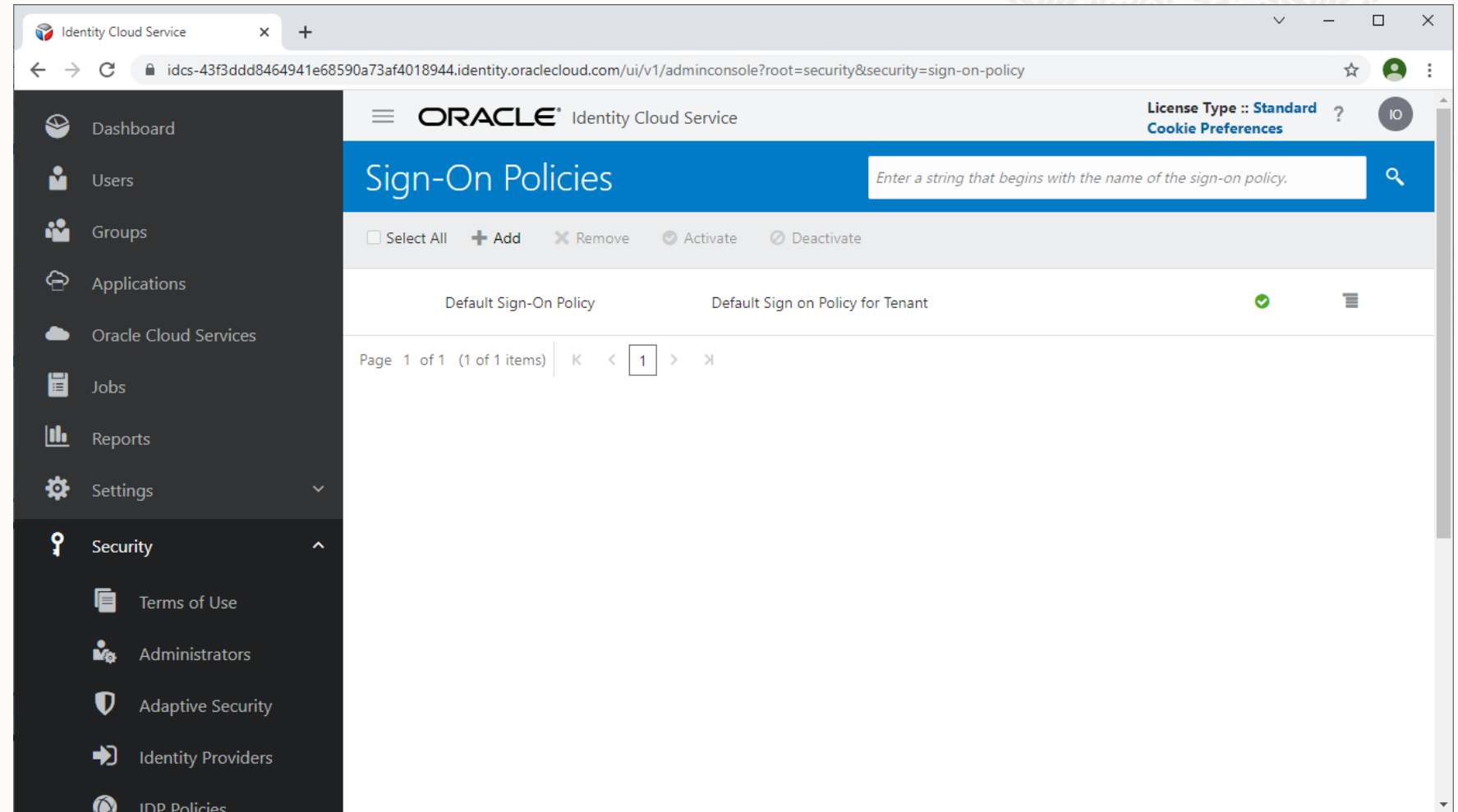
Number of day(s) a device can be trusted 15

Maximum number of trusted device(s) 5

Remember to save



Enable MFA in the Single Signon Policy



The screenshot displays the Oracle Identity Cloud Service Admin Console. The left sidebar contains a navigation menu with the following items: Dashboard, Users, Groups, Applications, Oracle Cloud Services, Jobs, Reports, Settings, and Security. The Security section is expanded, showing sub-items: Terms of Use, Administrators, Adaptive Security, Identity Providers, and IDP Policies. The main content area is titled "Sign-On Policies" and includes a search bar with the placeholder text "Enter a string that begins with the name of the sign-on policy." Below the search bar, there are action buttons: Select All, Add, Remove, Activate, and Deactivate. A table lists the policies, with the first row being "Default Sign-On Policy" and "Default Sign on Policy for Tenant", which is marked as active with a green checkmark. The table pagination shows "Page 1 of 1 (1 of 1 items)".

Identity Cloud Service

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

ORACLE Identity Cloud Service

License Type :: Standard
Cookie Preferences

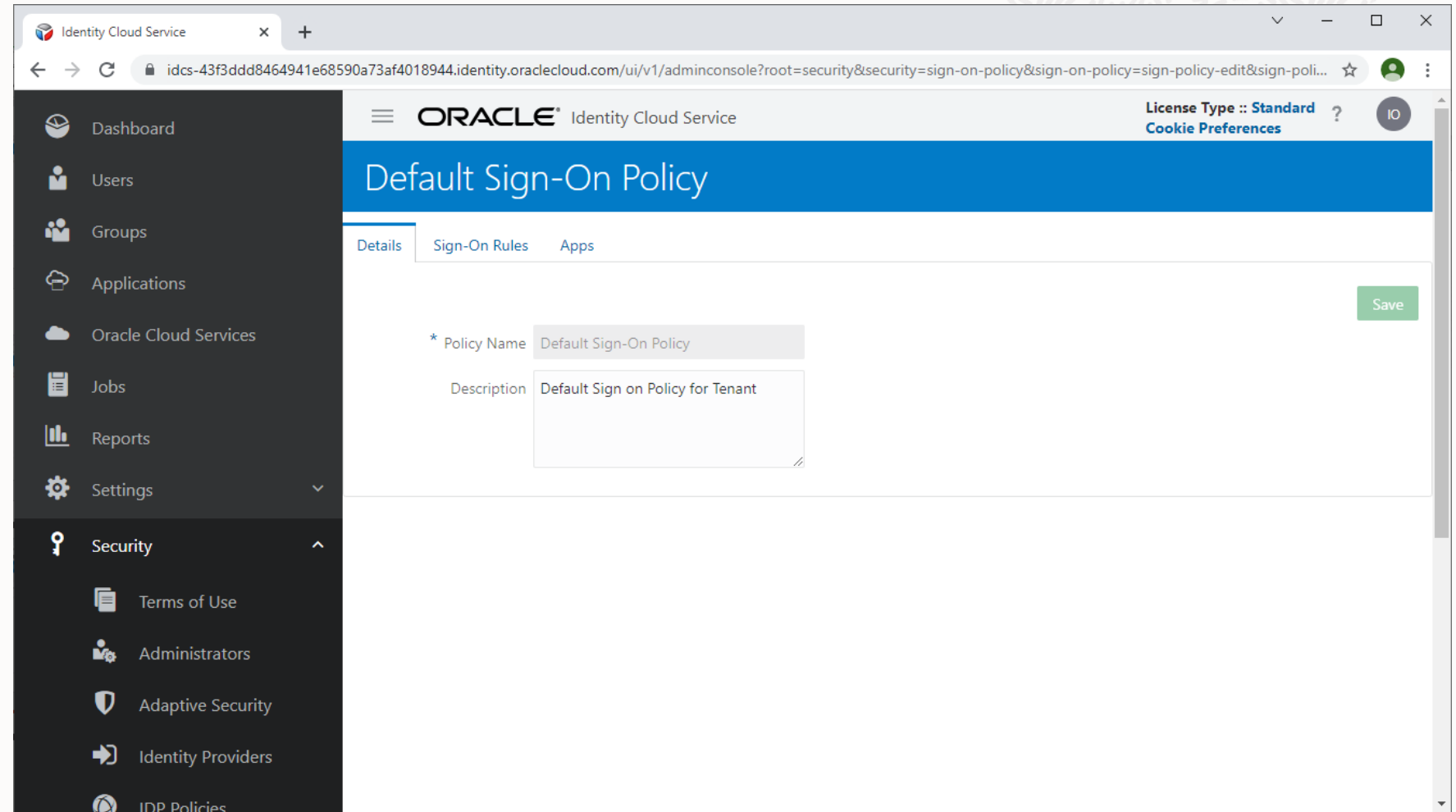
Sign-On Policies

Enter a string that begins with the name of the sign-on policy.

☐ Select All **+** Add **x** Remove **✓** Activate **⌂** Deactivate

Default Sign-On Policy	Default Sign on Policy for Tenant	
Page 1 of 1 (1 of 1 items)		K < 1 > >

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 Identity Cloud Service

License Type :: Standard ?
Cookie Preferences

Default Sign-On Policy

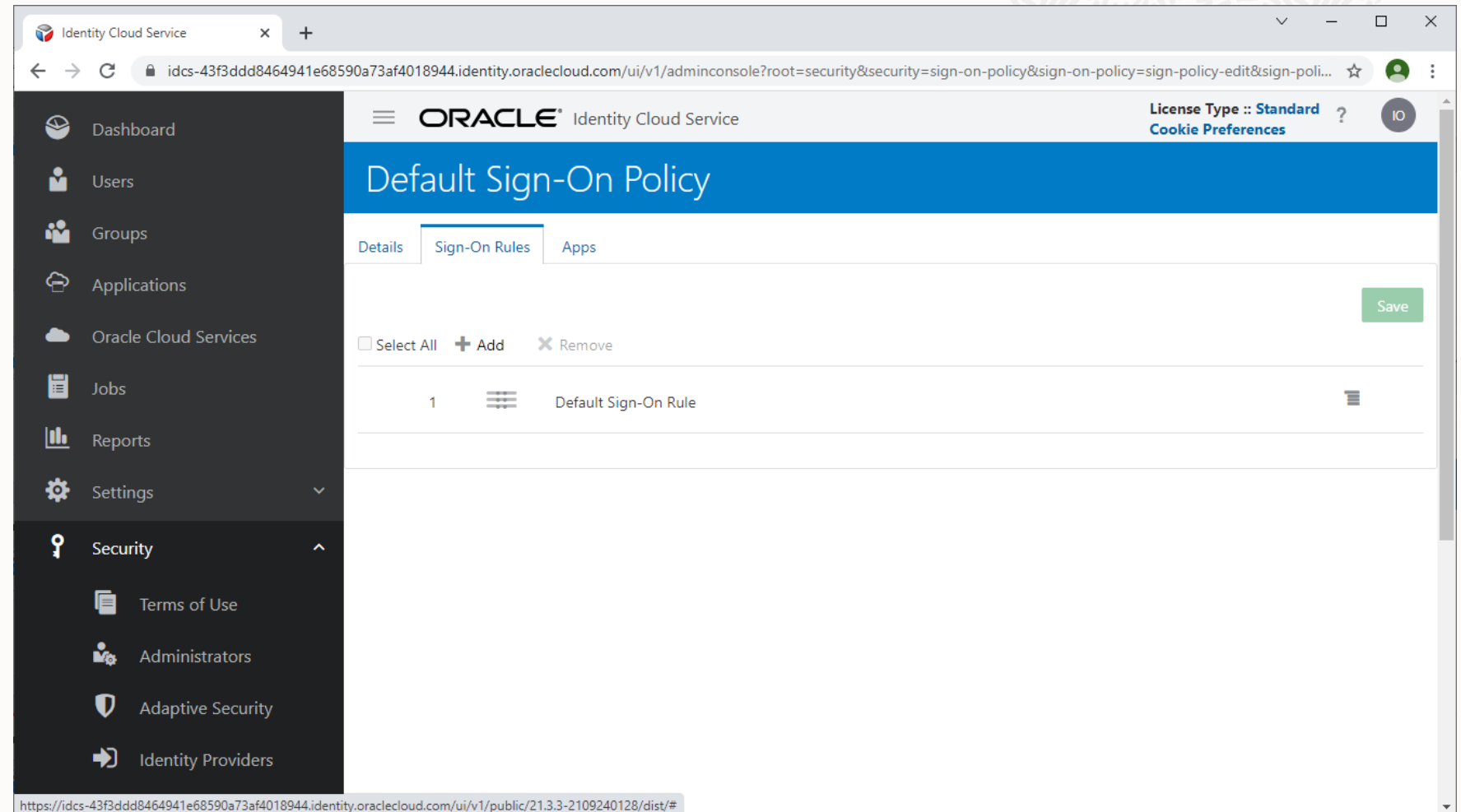
Details Sign-On Rules Apps

* Policy Name Default Sign-On Policy

Description Default Sign on Policy for Tenant

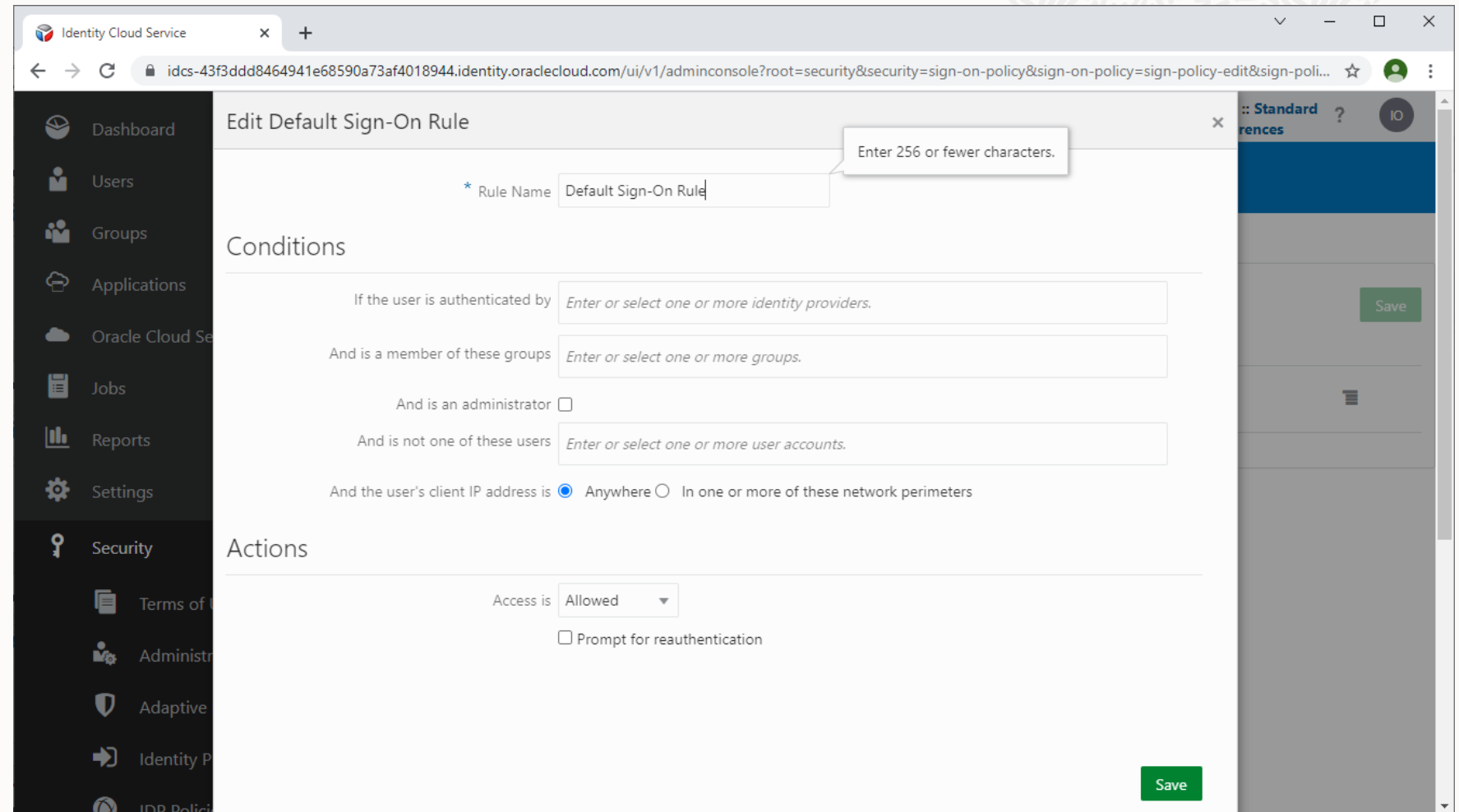
Save

Enable MFA in the Single Signon Policy



The screenshot displays the Oracle Identity Cloud Service (IDCS) admin console. The left sidebar contains navigation links: Dashboard, Users, Groups, Applications, Oracle Cloud Services, Jobs, Reports, Settings, and Security. The Security section is expanded, showing sub-links for Terms of Use, Administrators, Adaptive Security, and Identity Providers. The main content area is titled "Default Sign-On Policy" and has three tabs: Details, Sign-On Rules, and Apps. The "Sign-On Rules" tab is active, showing a table with one rule: "Default Sign-On Rule". Above the table are controls for "Select All", "Add", and "Remove". A "Save" button is located in the top right corner of the table area. The browser's address bar shows the URL: <https://idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/adminconsole?root=security&security=sign-on-policy&sign-on-policy=sign-policy-edit&sign-poli...>

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...

Edit Default Sign-On Rule

* Rule Name Enter 256 or fewer characters.

Conditions

If the user is authenticated by

And is a member of these groups

And is an administrator ☐

And is not one of these users

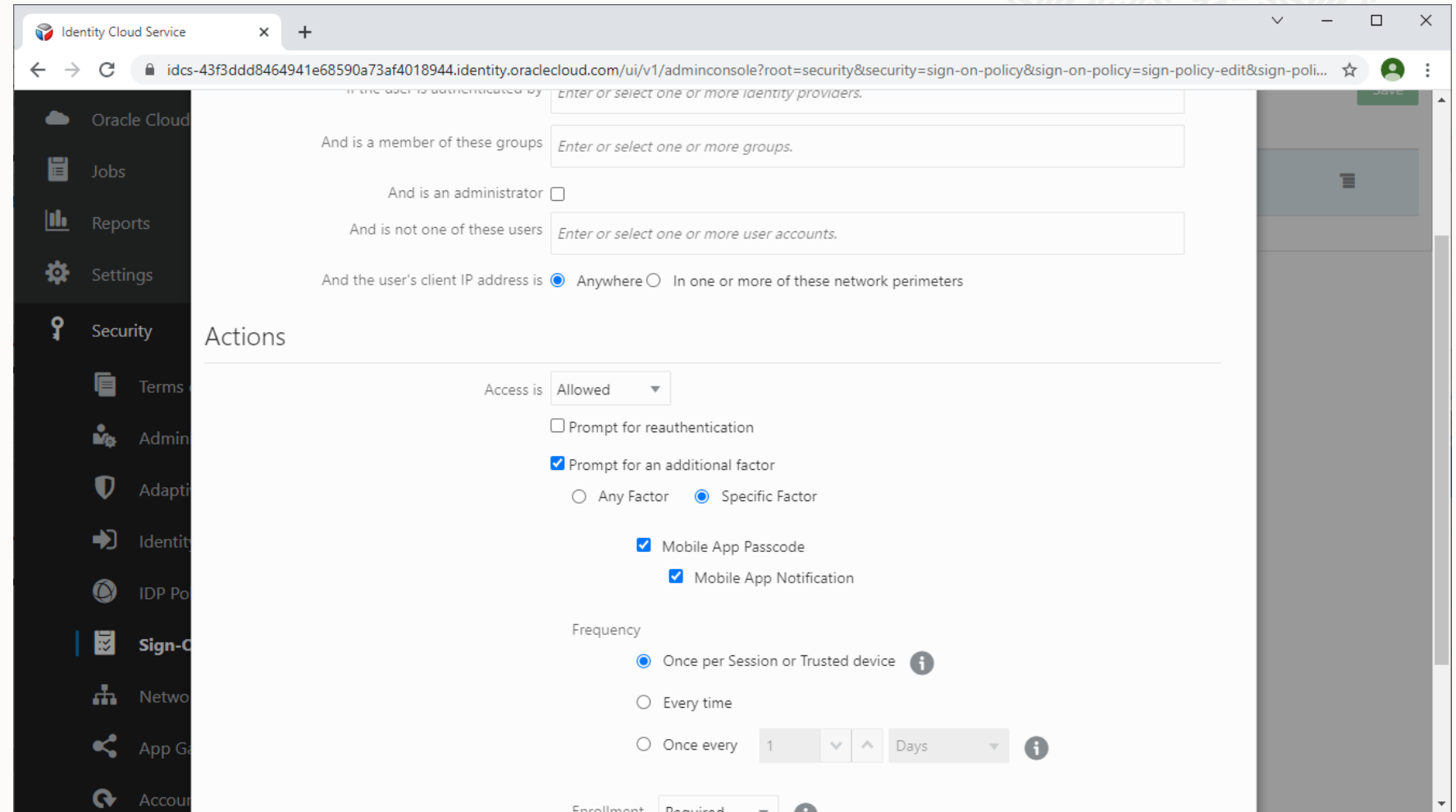
And the user's client IP address is ☒ Anywhere ☐ In one or more of these network perimeters

Actions

Access is

☐ Prompt for reauthentication

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-On

Netwo

App G

Account

And the user is authenticated by

And is a member of these groups

And is an administrator ☐

And is not one of these users

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

Actions

Access is

☐ 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

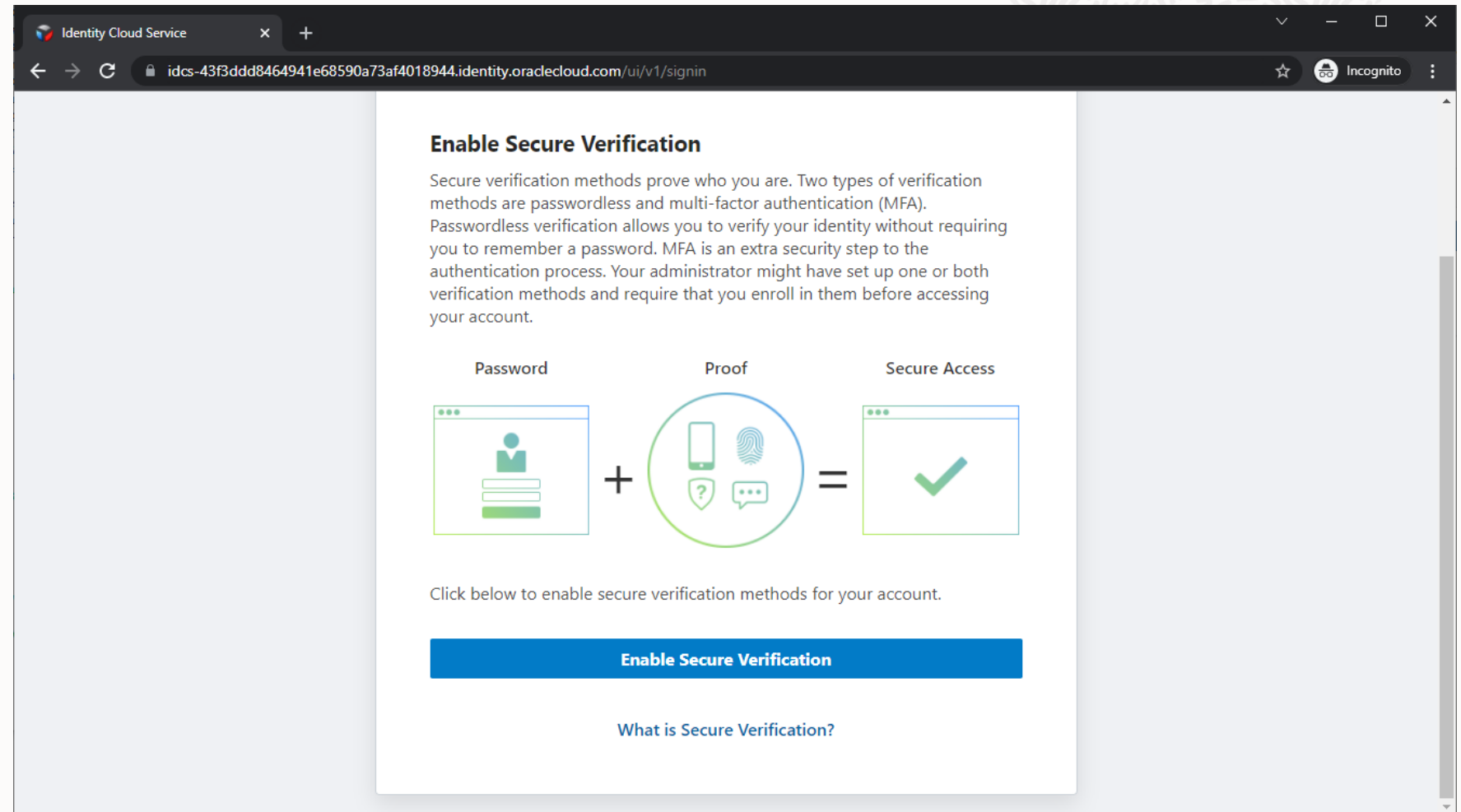
☐ Once every ⓘ

Enrollment

User enrolment

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

Mobile app enrolment



The screenshot shows a web browser window with the title 'Identity Cloud Service'. The address bar displays the URL 'idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/signin'. The page content is titled 'Enable Secure Verification' and includes a paragraph explaining secure verification methods. Below the text is a diagram showing 'Password' (represented by a user icon and a list) plus 'Proof' (represented by a circle containing a smartphone, a fingerprint, and a question mark) equals 'Secure Access' (represented by a checkmark). At the bottom of the page, there is a blue button labeled 'Enable Secure Verification' and a link labeled 'What is Secure Verification?'.

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.

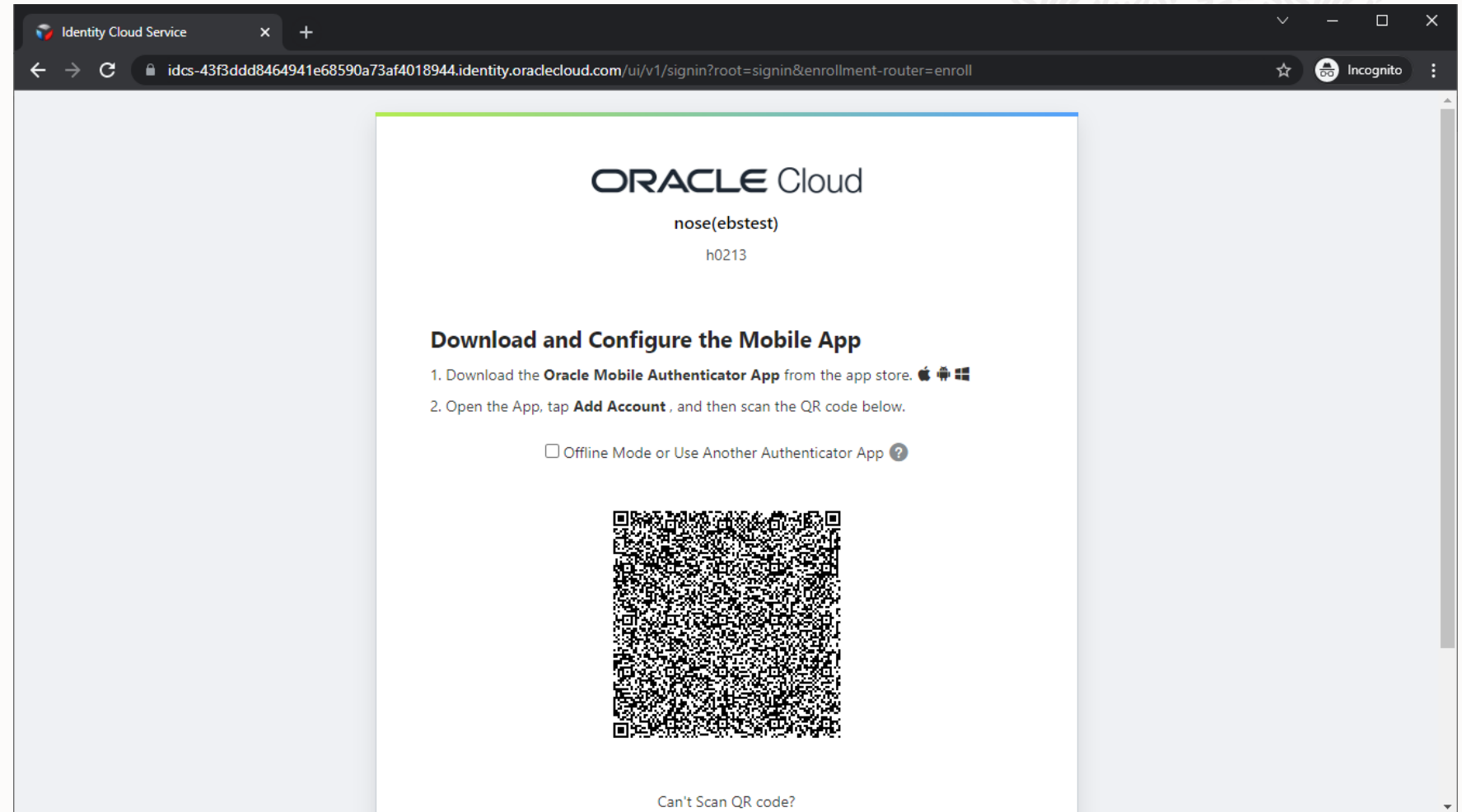
Password + Proof = Secure Access

Click below to enable secure verification methods for your account.

[Enable Secure Verification](#)

[What is Secure Verification?](#)

Mobile app enrolment



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...

Edit Default Sign-On Rule

* Rule Name Enter 256 or fewer characters.

Conditions

If the user is authenticated by

And is a member of these groups

And is an administrator ☐

And is not one of these users

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

Actions

Access is

☐ Prompt for reauthentication

☒ Prompt for an additional factor

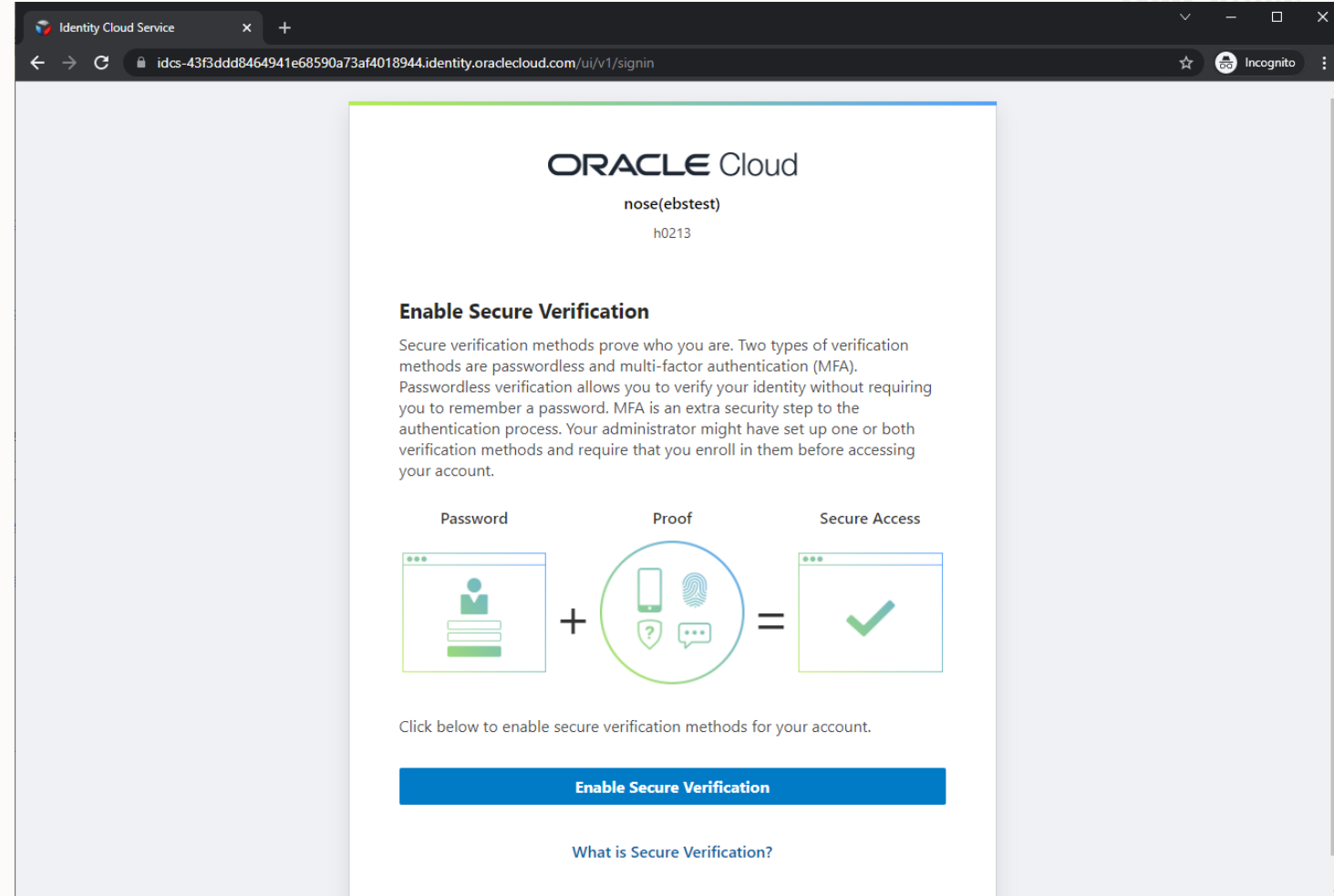
☐ Any Factor ☒ Specific Factor

☒ Mobile App Passcode

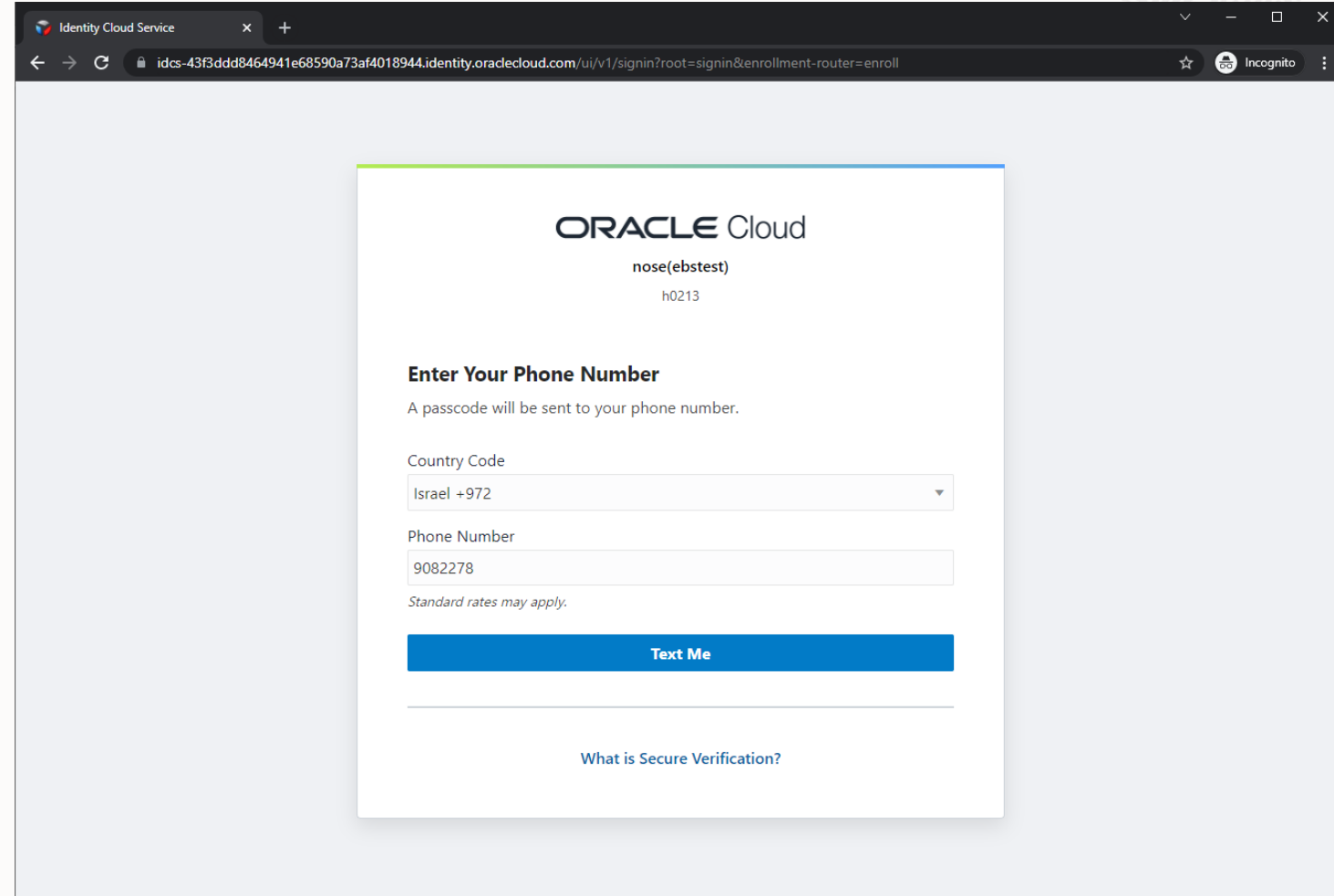
☒ Mobile App Notification

Save

SMS enrolment



SMS enrolment



The screenshot shows a web browser window with the title "Identity Cloud Service". The address bar displays the URL: `idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/signin?root=signin&enrollment-router=enroll`. The browser is in Incognito mode. The main content area features the Oracle Cloud logo and the text "nose(ebtest)" and "h0213". Below this, the heading "Enter Your Phone Number" is followed by the instruction "A passcode will be sent to your phone number." There are two input fields: "Country Code" with a dropdown menu showing "Israel +972" and "Phone Number" with the value "9082278". A note states "Standard rates may apply." A blue "Text Me" button is positioned below the inputs. At the bottom, there is a link that says "What is Secure Verification?".

Identity Cloud Service

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

Incognito

ORACLE Cloud

nose(ebtest)

h0213

Enter Your Phone Number

A passcode will be sent to your phone number.

Country Code

Israel +972

Phone Number

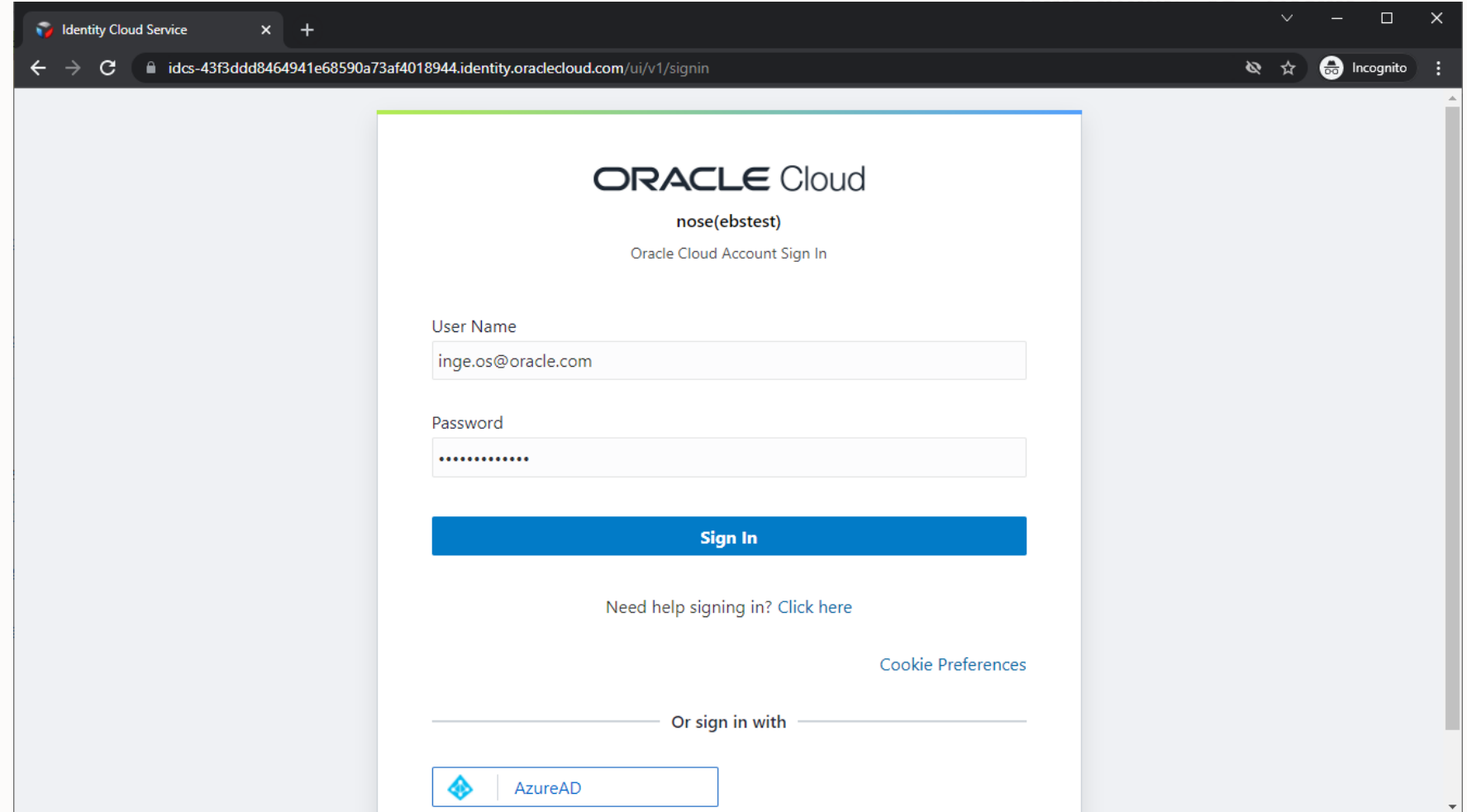
9082278

Standard rates may apply.

Text Me

[What is Secure Verification?](#)

First time logon



The screenshot shows a web browser window with the title "Identity Cloud Service". The address bar displays the URL "idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/signin". The page content includes the Oracle Cloud logo, the text "nose(ebtest)", and "Oracle Cloud Account Sign In". There are input fields for "User Name" (containing "inge.os@oracle.com") and "Password" (masked with dots). A blue "Sign In" button is positioned below the password field. Below the button, there is a link "Need help signing in? Click here" and a link "Cookie Preferences". At the bottom, there is a section "Or sign in with" followed by a button for "AzureAD".

Identity Cloud Service

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

Incognito

ORACLE Cloud

nose(ebtest)

Oracle Cloud Account Sign In

User Name

inge.os@oracle.com

Password


.....

Sign In

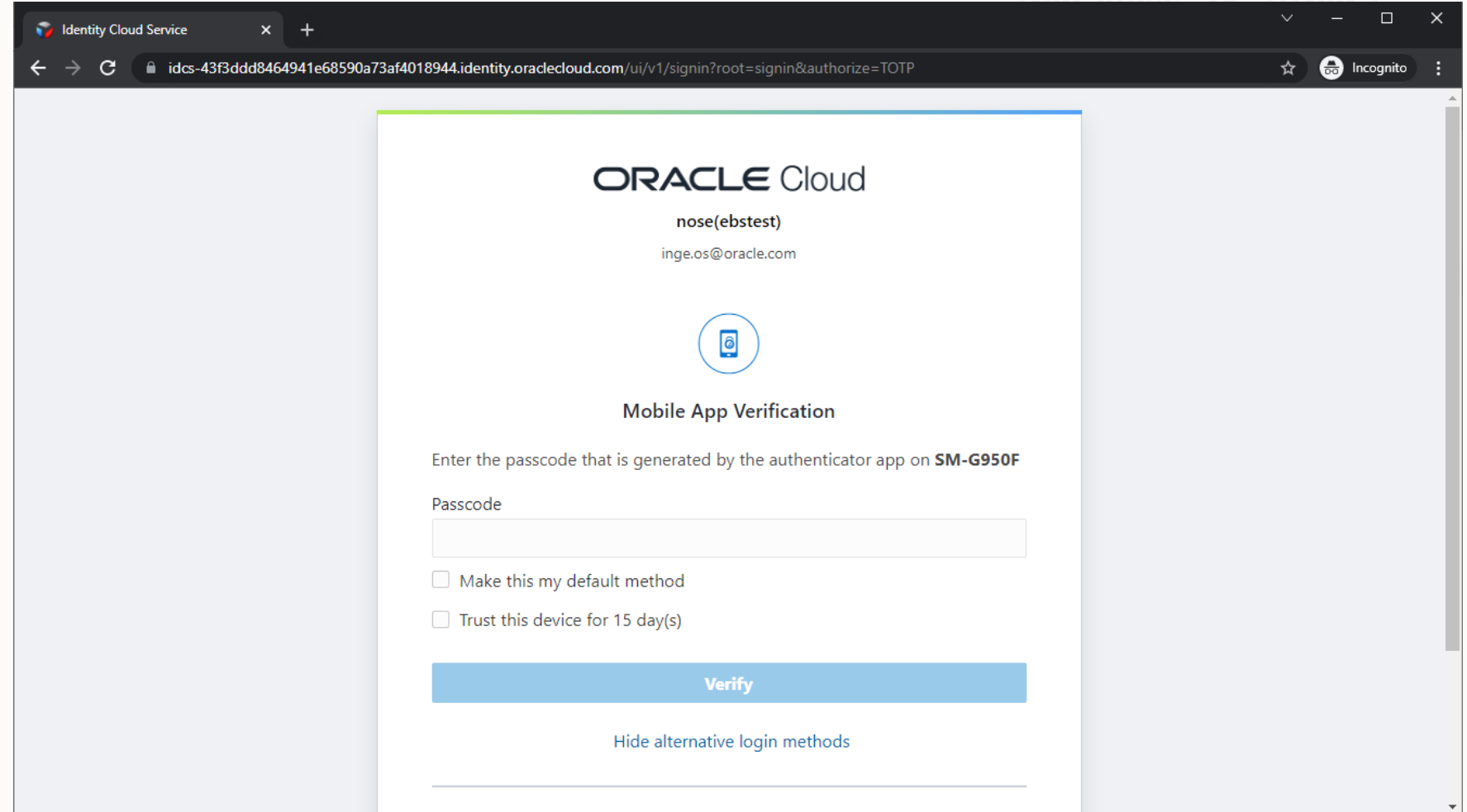

Need help signing in? [Click here](#)

[Cookie Preferences](#)

Or sign in with

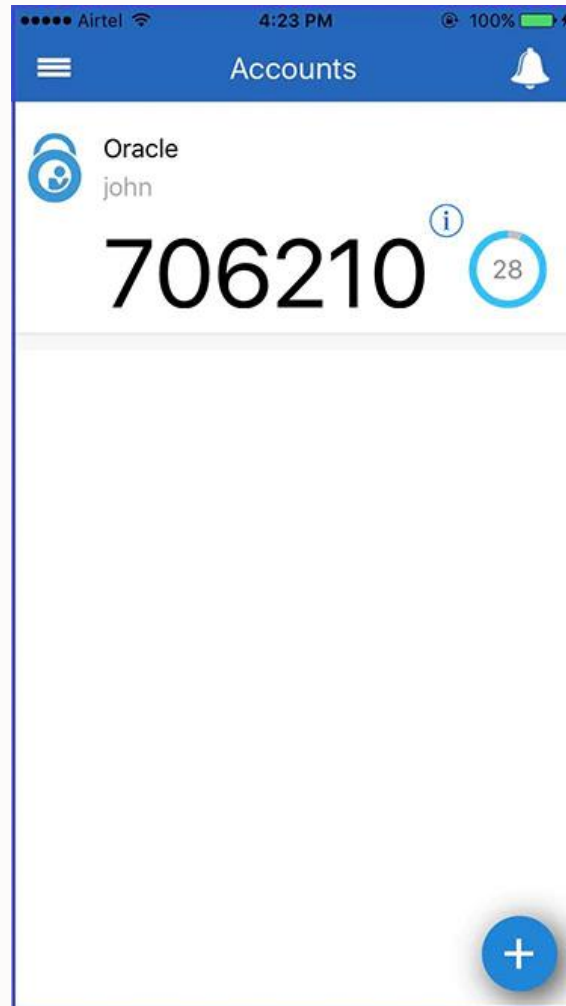
 AzureAD

Mobile app MFA logon



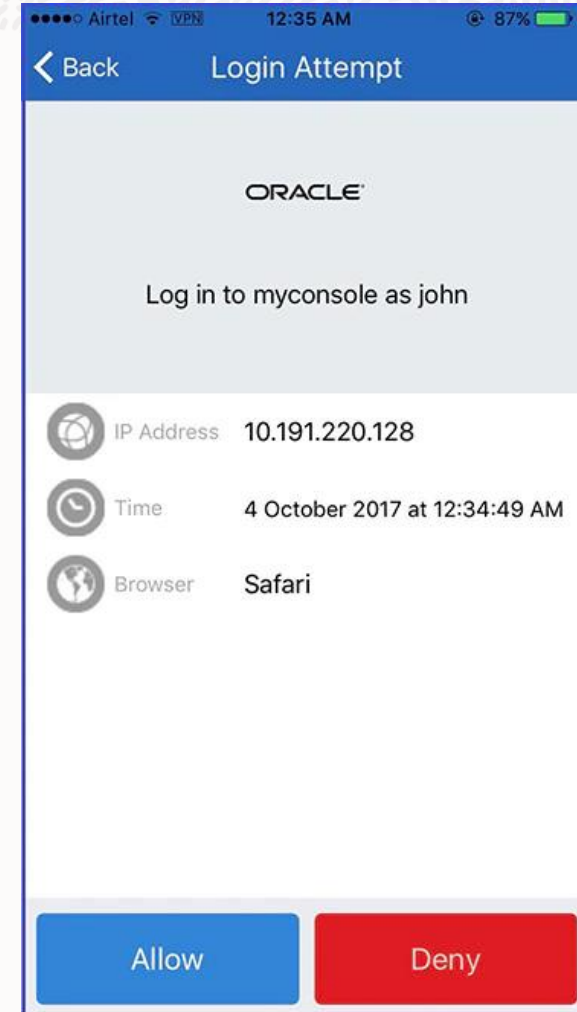
The screenshot shows a web browser window with the title "Identity Cloud Service". The address bar contains the URL: `idcs-43f3ddd8464941e68590a73af4018944.identity.oraclecloud.com/ui/v1/signin?root=signin&authorize=TOTP`. The browser is in Incognito mode. The main content area displays the "ORACLE Cloud" logo, the username "nose(ebtest)", and the email "inge.os@oracle.com". Below this is a circular icon representing a mobile app. The section is titled "Mobile App Verification". It instructs the user to "Enter the passcode that is generated by the authenticator app on **SM-G950F**". There is a text input field for the "Passcode". Below the input field are two checkboxes: "Make this my default method" and "Trust this device for 15 day(s)". A blue "Verify" button is at the bottom of the form. Below the button is a link that says "Hide alternative login methods".

Mobile Authenticator



Pincode verification

Copyright © 2022, Oracle and/or its affiliates. All rights reserved.



Push verification



References



<https://docs.oracle.com/en/cloud/paas/identity-cloud/uaid/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://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>