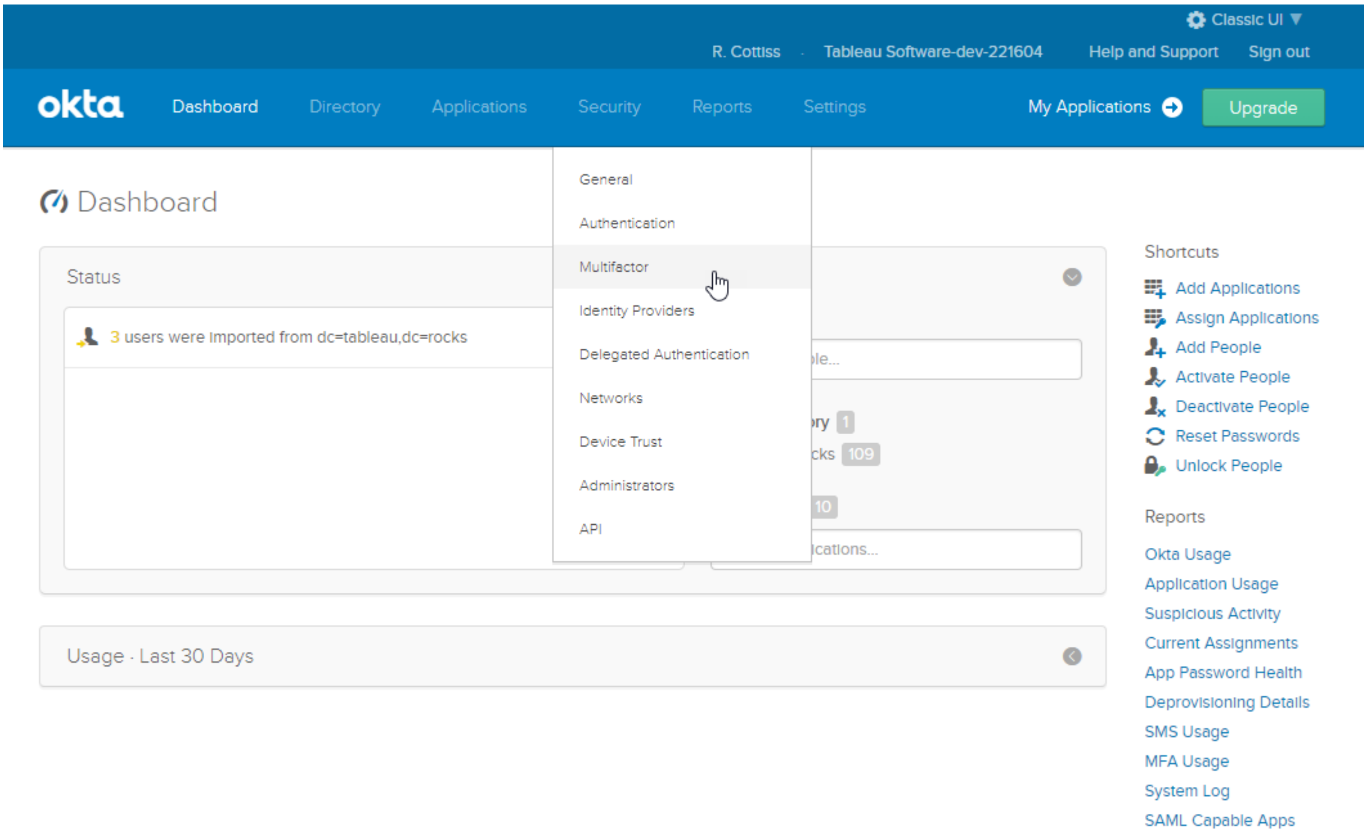
SAML Lab Part 2 - Enable Okta for MFA

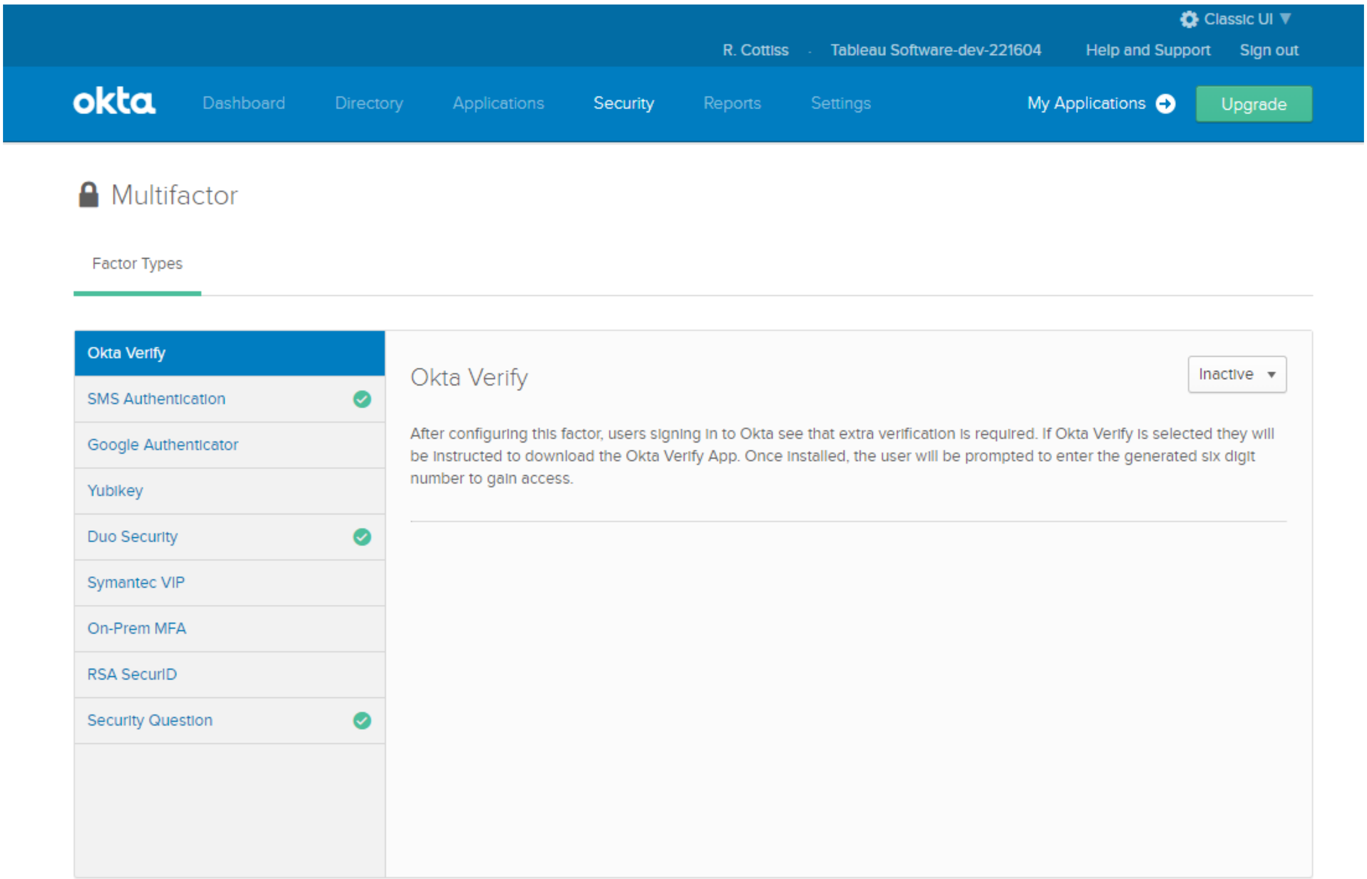
Okta and most other IdPs support Second Factor Authentication (2FA) or Multi-Factor Authentication (MFA). MFA is becoming more and more common in our customers because it is more secure than a Single Factor. In this part of the lab you will enable MFA for your SAML users. The configuration is all in Okta - Tableau does not really know that MFA is enabled. All Tableau needs to do is present any web pages that the MFA flow renders in web pages.

Step 1 - Configure MFA

Sign back into Okta using the Okta Administrator account. From the **Security** menu select **Multifactor**


3 users were imported from dc=tableau,dc=rocks

Okta supports several factor types and you can activate multiple types at the same time. SMS Authentication is one of the simpler to set up if you have a phone that can receive SMS messages. Enable SMS Authentication if you think you can receive SMS messages during the Lab session or you want to test this later

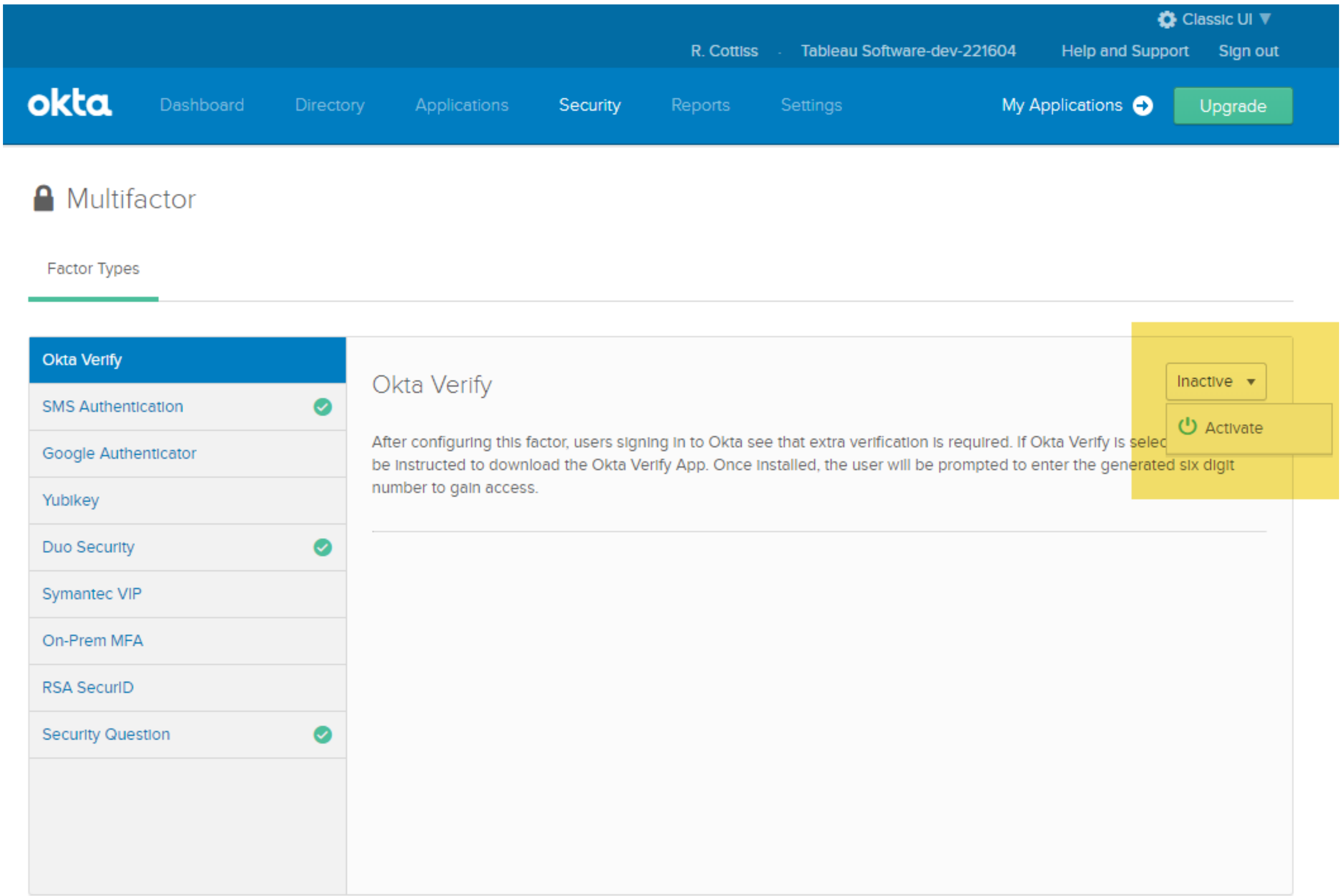


Okta Verify

After configuring this factor, users signing in to Okta see that extra verification is required. If Okta Verify is selected they will be instructed to download the Okta Verify App. Once installed, the user will be prompted to enter the generated six digit number to gain access.

You can also create a security question. Enable this factor in addition to SMS. You will configure Okta to allow you to choose which factor to use on login.

Select Activate on the drop down after clicking on the factor you want to enable:



Multifactor

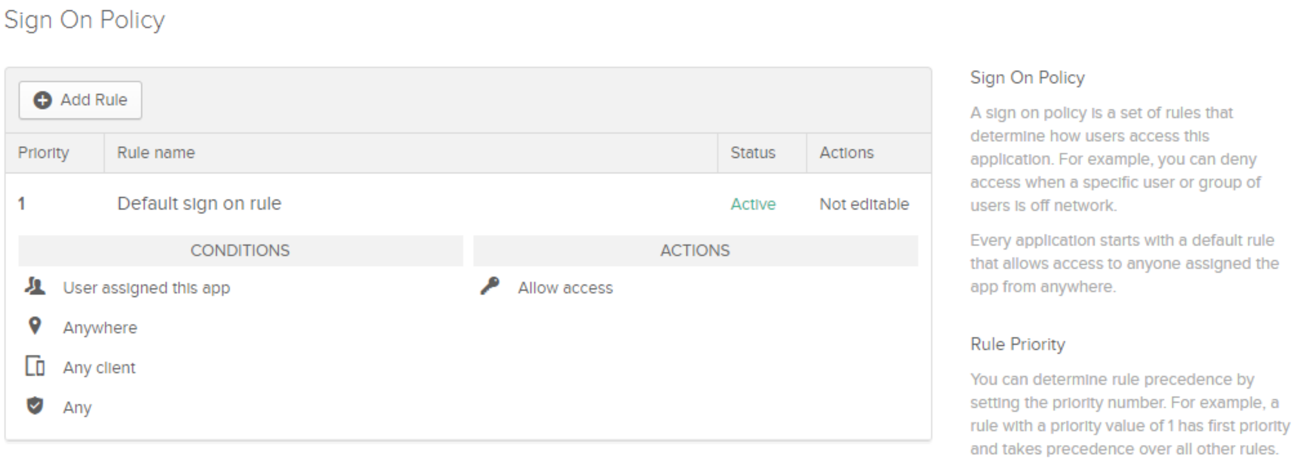
Factor Types	
Okta Verify	
SMS Authentication	✓
Google Authenticator	
Yubikey	
Duo Security	✓
Symantec VIP	
On-Prem MFA	
RSA SecurID	
Security Question	✓

Okta Verify

After configuring this factor, users signing in to Okta see that extra verification is required. If Okta Verify is selec be instructed to download the Okta Verify App. Once installed, the user will be prompted to enter the generated six digit number to gain access.

Okta is very flexible in how you enable MFA for groups or users. Some IdPs allow the user to self register for MFA. In this Lab we will force all users of Tableau Online to use one of the activated Multi Factor Types when authenticating.

In the Tableau Online Application scroll to the bottom where the Sign On Policy is located:



Sign On Policy

Priority	Rule name	Status	Actions
1	Default sign on rule	Active	Not editable

CONDITIONS	ACTIONS
User assigned this app	Allow access
Anywhere	
Any client	
Any	

Sign On Policy

A sign on policy is a set of rules that determine how users access this application. For example, you can deny access when a specific user or group of users is off network.

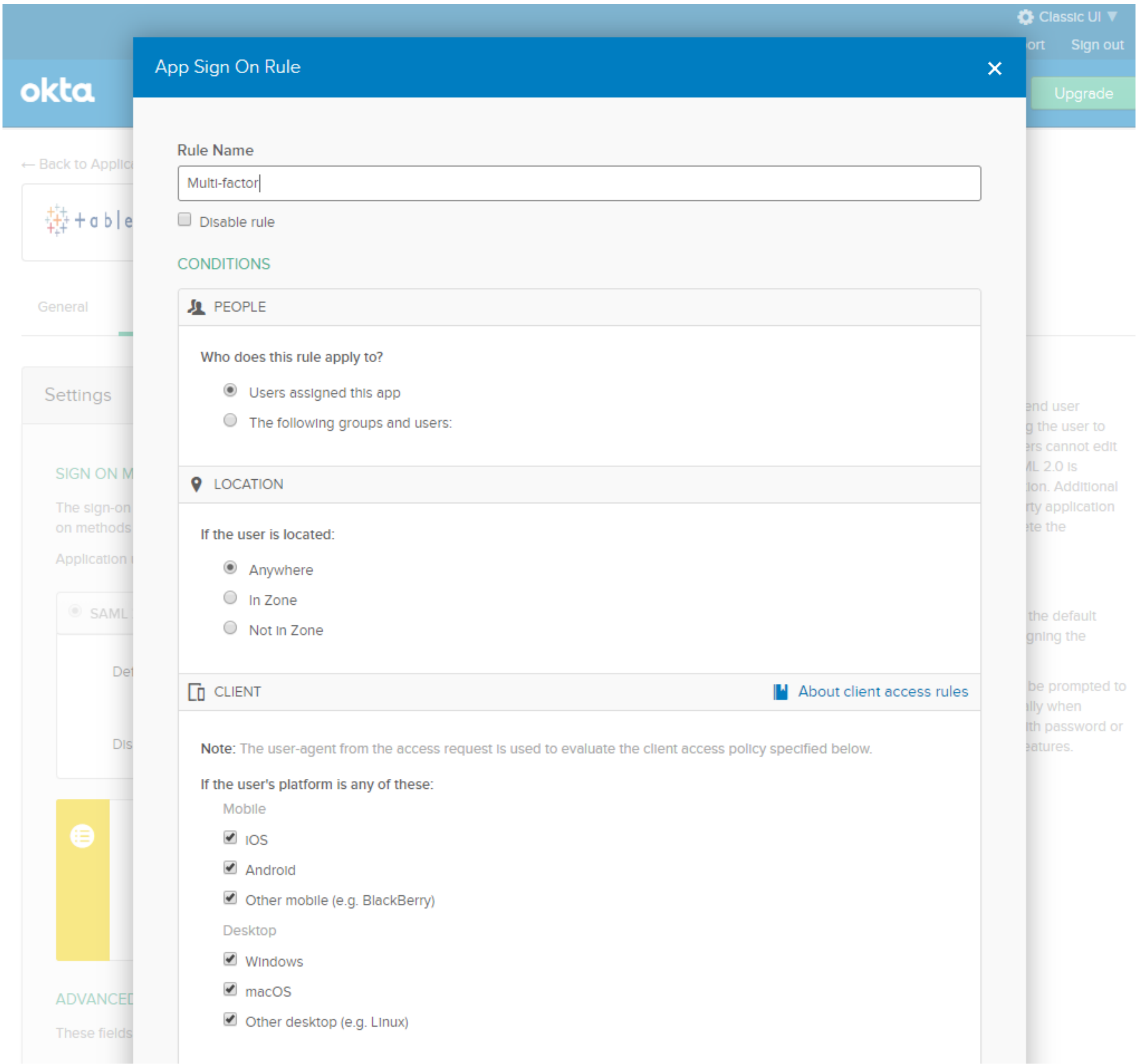
Every application starts with a default rule that allows access to anyone assigned the app from anywhere.

Rule Priority

You can determine rule precedence by setting the priority number. For example, a rule with a priority value of 1 has first priority and takes precedence over all other rules.

Click **Add Rule** and give it a name. Read the settings and understand the options. You can leave most options as defaults to enable MFA for all users assigned to the app.

> You can limit the rule to a subset of user or groups and to certain network zones. You can also limit the rule to certain platforms.



App Sign On Rule ✕

Rule Name

Multi-factor

□ Disable rule

CONDITIONS

PEOPLE

Who does this rule apply to?

● Users assigned this app
○ The following groups and users:

LOCATION

If the user is located:

● Anywhere
○ In Zone
○ Not in Zone

CLIENT — About client access rules

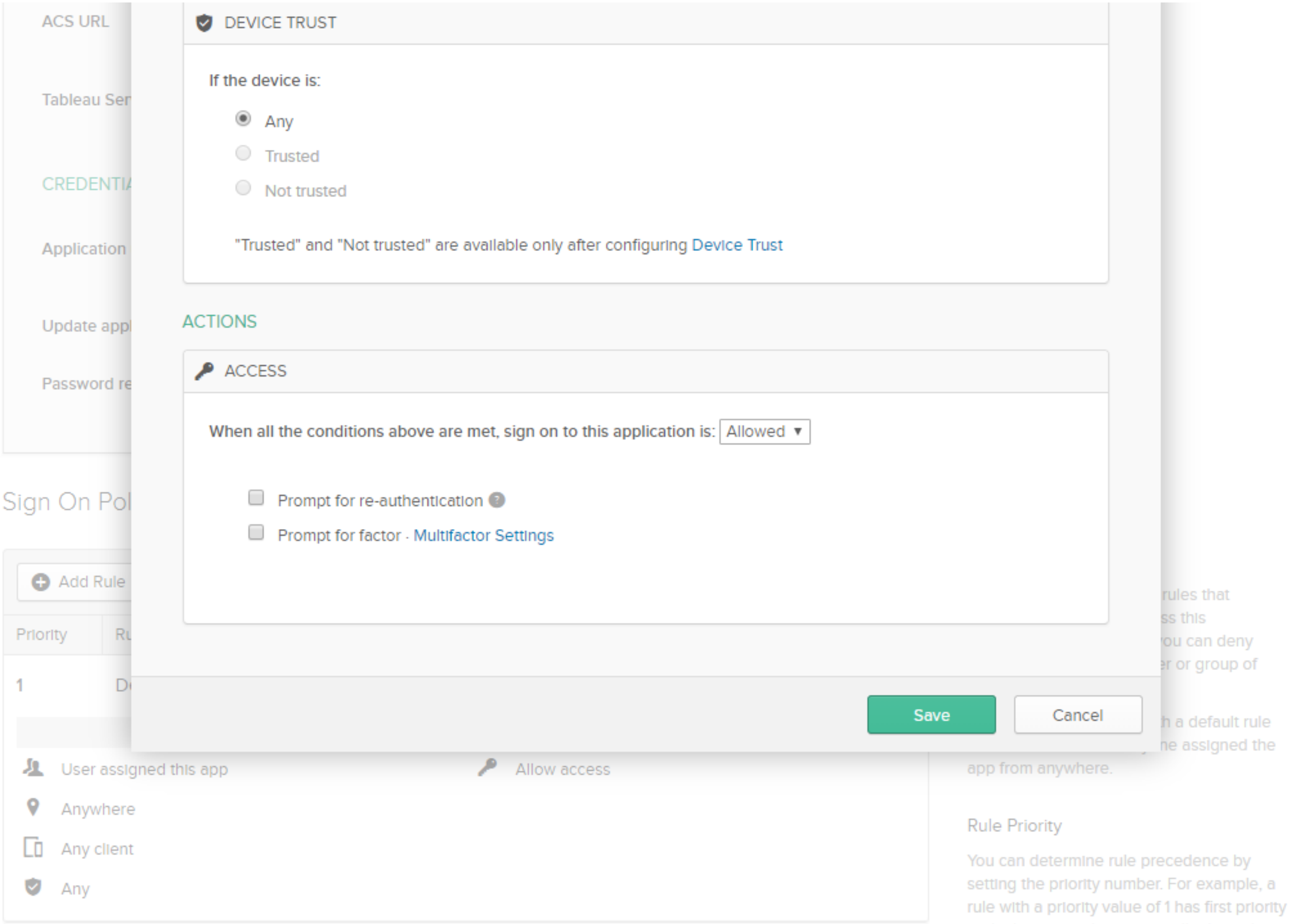
Note: The user-agent from the access request is used to evaluate the client access policy specified below.

If the user's platform is any of these:

Mobile
☑ iOS
☑ Android
☑ Other mobile (e.g. BlackBerry)

Desktop
☑ Windows
☑ macOS
☑ Other desktop (e.g. Linux)

The rules pop up has more sections. Scroll down to see the Device Trust and Actions Sections:



DEVICE TRUST

If the device is:

● Any

○ Trusted

○ Not trusted

"Trusted" and "Not trusted" are available only after configuring Device Trust

ACTIONS

ACCESS

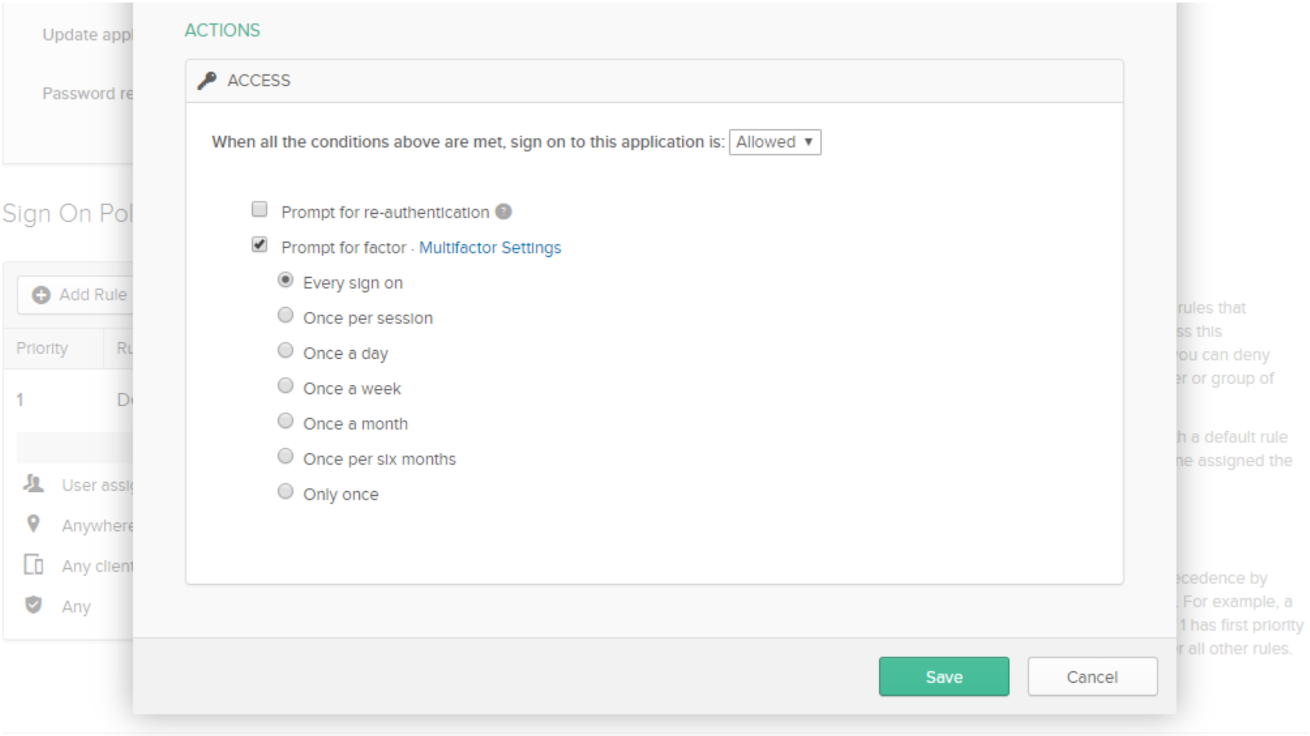
When all the conditions above are met, sign on to this application is: Allowed ▾

□ Prompt for re-authentication

□ Prompt for factor · Multifactor Settings

We did not configure device trust so Any is the only option.

For **Actions** select the *Prompt for Factor* checkbox. We already activated some Factor Types so all we need to do is to configure how often we want to prompt. Select *Every sign on* then Save



ACTIONS

ACCESS

When all the conditions above are met, sign on to this application is: Allowed ▾

□ Prompt for re-authentication

☑ Prompt for factor · Multifactor Settings

● Every sign on

○ Once per session

○ Once a day

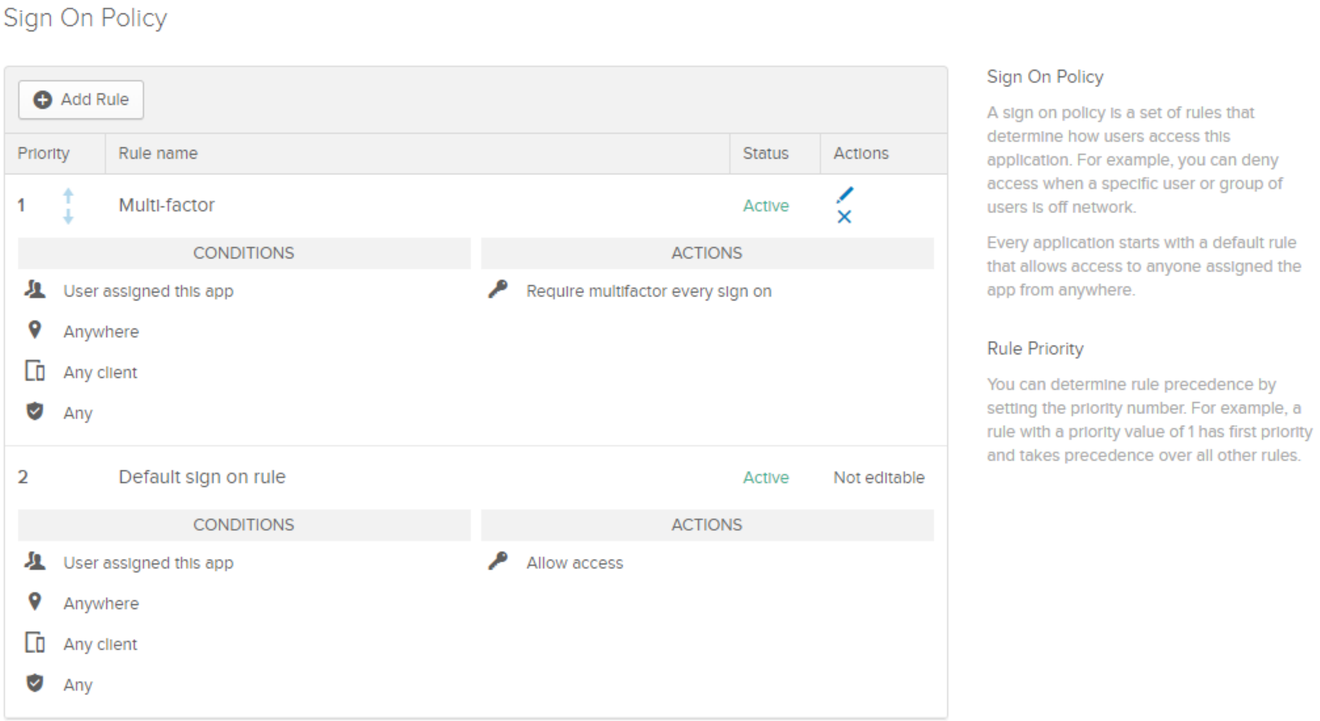
○ Once a week

○ Once a month

○ Once per six months

○ Only once

The Sign On Policy should look like this:



Sign On Policy

⊕ Add Rule

Priority	Rule name	Status	Actions
1	Multi-factor	Active	✎ ✕
2	Default sign on rule	Active	Not editable

Rule 1 – Multi-factor

CONDITIONS	ACTIONS
User assigned this app	Require multifactor every sign on
Anywhere	
Any client	
Any	

Rule 2 – Default sign on rule

CONDITIONS	ACTIONS
User assigned this app	Allow access
Anywhere	
Any client	
Any	

Sign On Policy

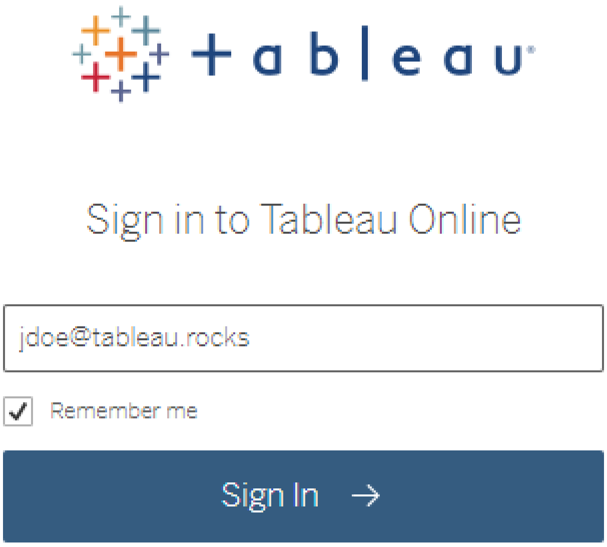
A sign on policy is a set of rules that determine how users access this application. For example, you can deny access when a specific user or group of users is off network.

Every application starts with a default rule that allows access to anyone assigned the app from anywhere.

Rule Priority

You can determine rule precedence by setting the priority number. For example, a rule with a priority value of 1 has first priority and takes precedence over all other rules.

Sign out of Okta and Tableau Online and Sign onto Online again using the Online user we set up for SAML.

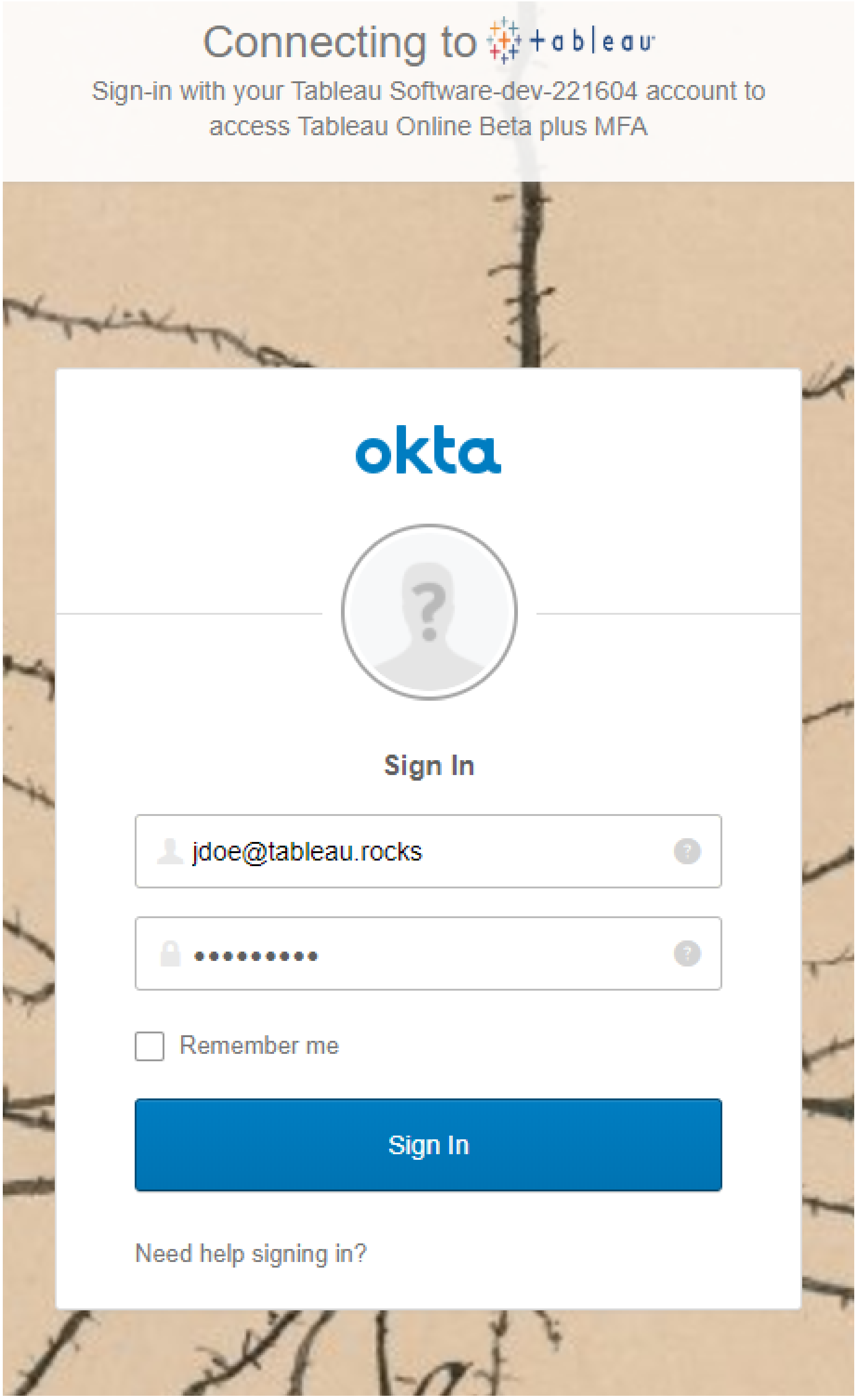


Sign in to Tableau Online

jdoe@tableau.rocks

☑ Remember me

You will be redirected to Okta:



Connecting to tableau

Sign-in with your Tableau Software-dev-221604 account to access Tableau Online Beta plus MFA

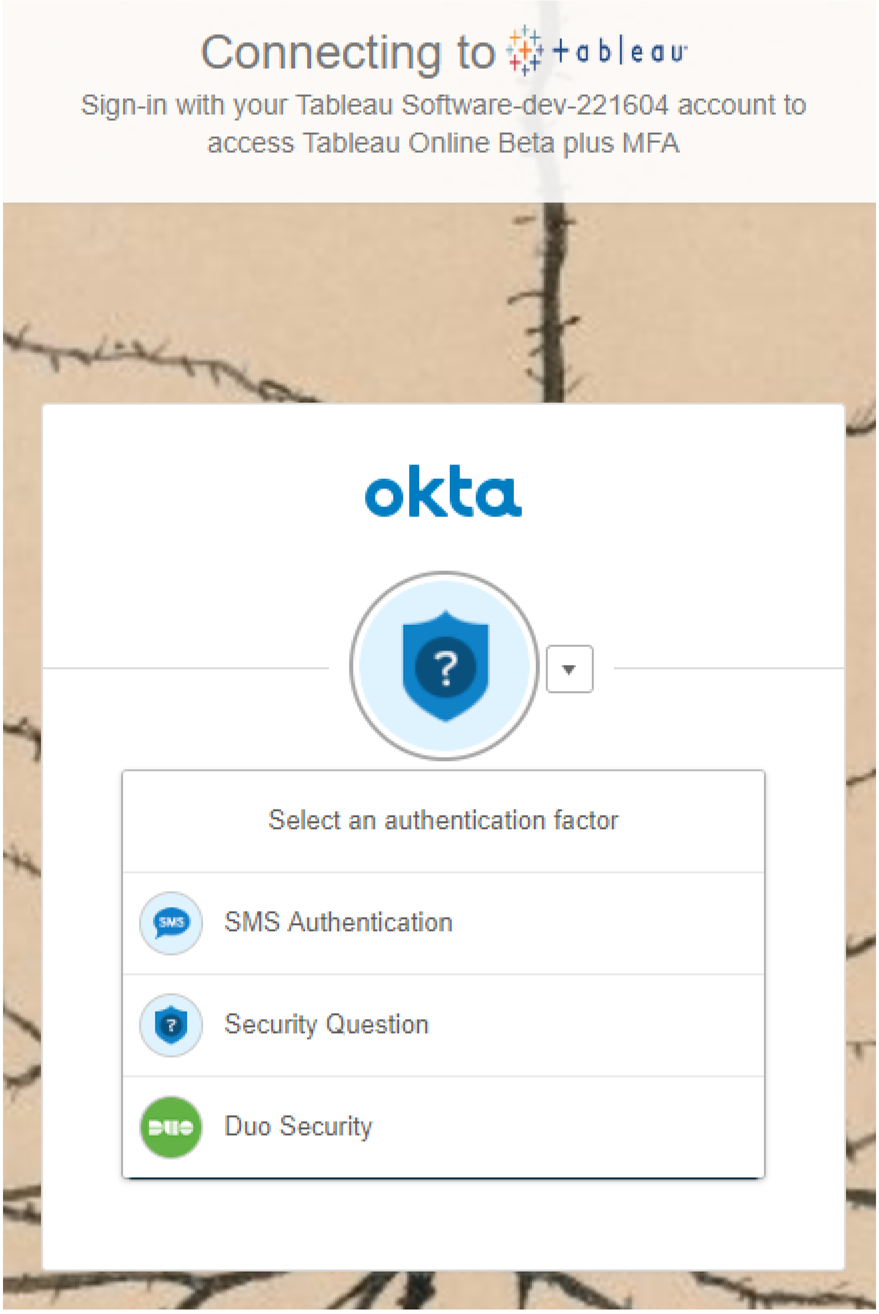
Sign In

jdoe@tableau.rocks

••••••••••

□ Remember me

After entering the usual username and password you should get a second factor prompt. You can choose which factor to use by clicking on the down arrow next to the shield:



Connecting to tableau

Sign-in with your Tableau Software-dev-221604 account to access Tableau Online Beta plus MFA

okta

Select an authentication factor

SMS Authentication

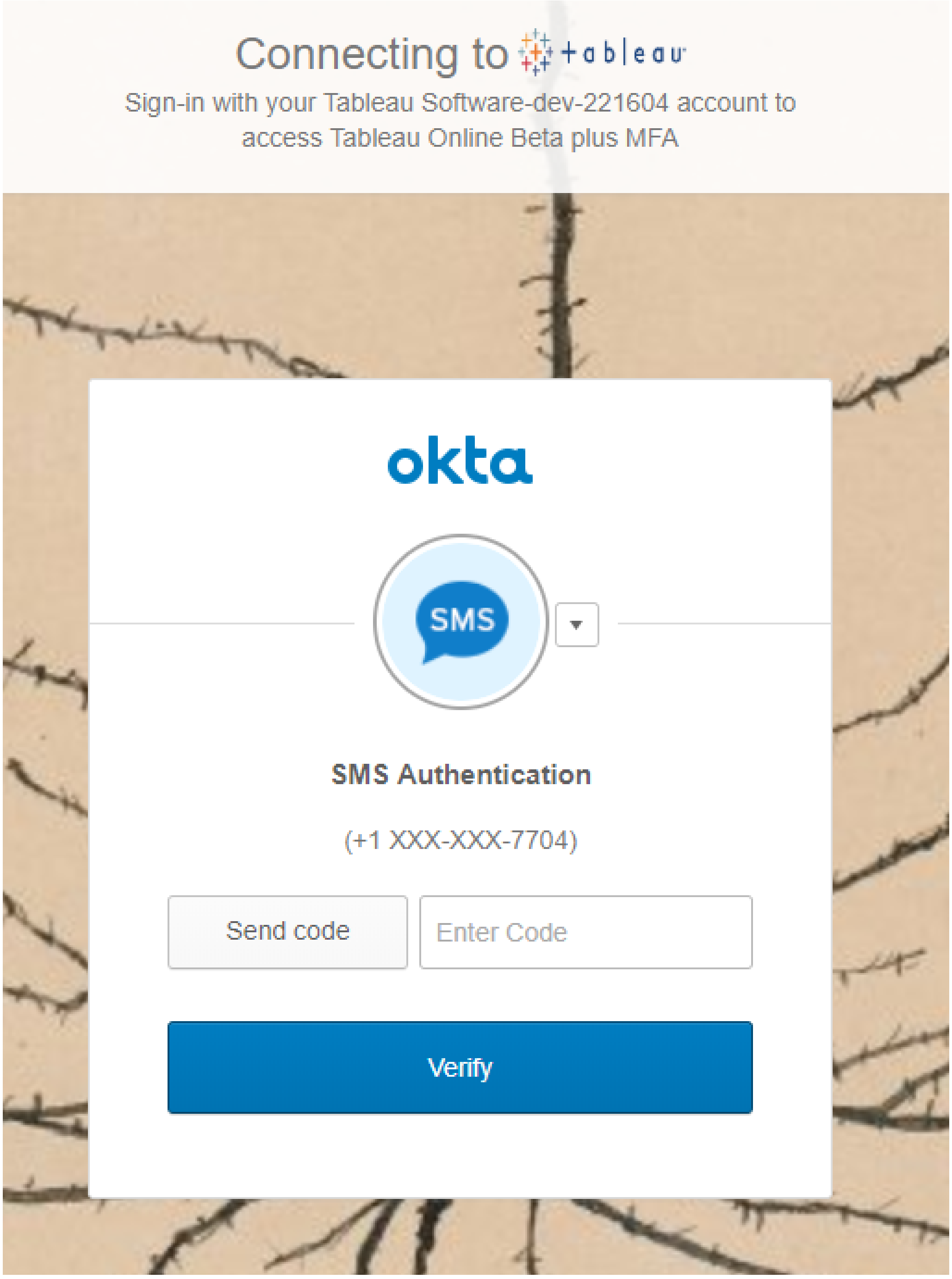
Security Question

Duo Security

Pick *SMS authentication* if you can receive Text Messages, or *Security Question* if you do not have your phone

> If this is the first time for SMS you may be prompted to enter phone information:

Here is how SMS Authentication looks:



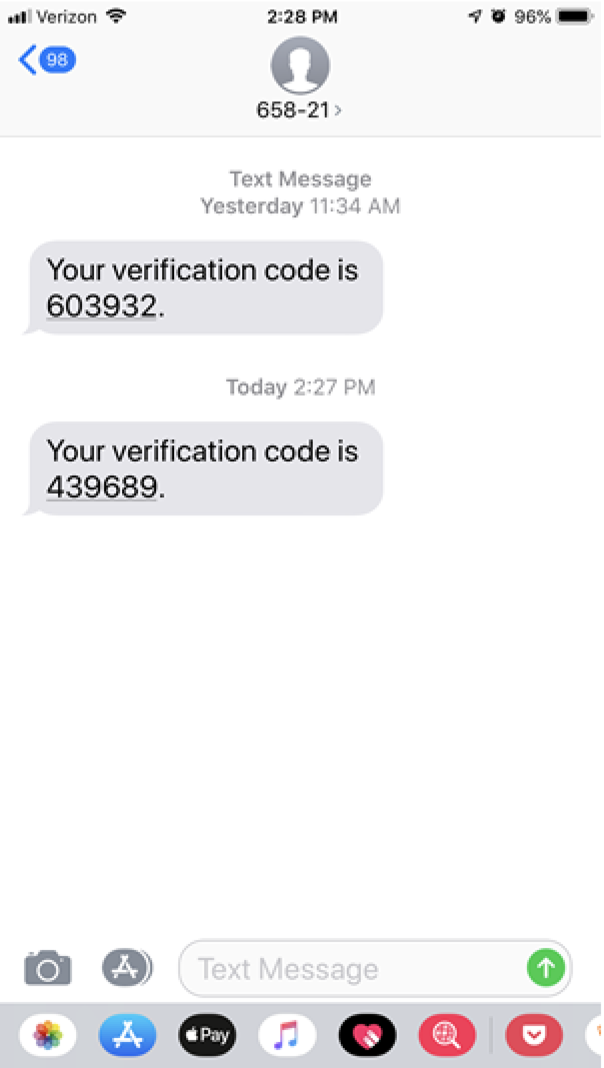
Connecting to tableau

Sign-in with your Tableau Software-dev-221604 account to access Tableau Online Beta plus MFA

SMS Authentication

(+1 XXX-XXX-7704)

In the Apple Messages app:



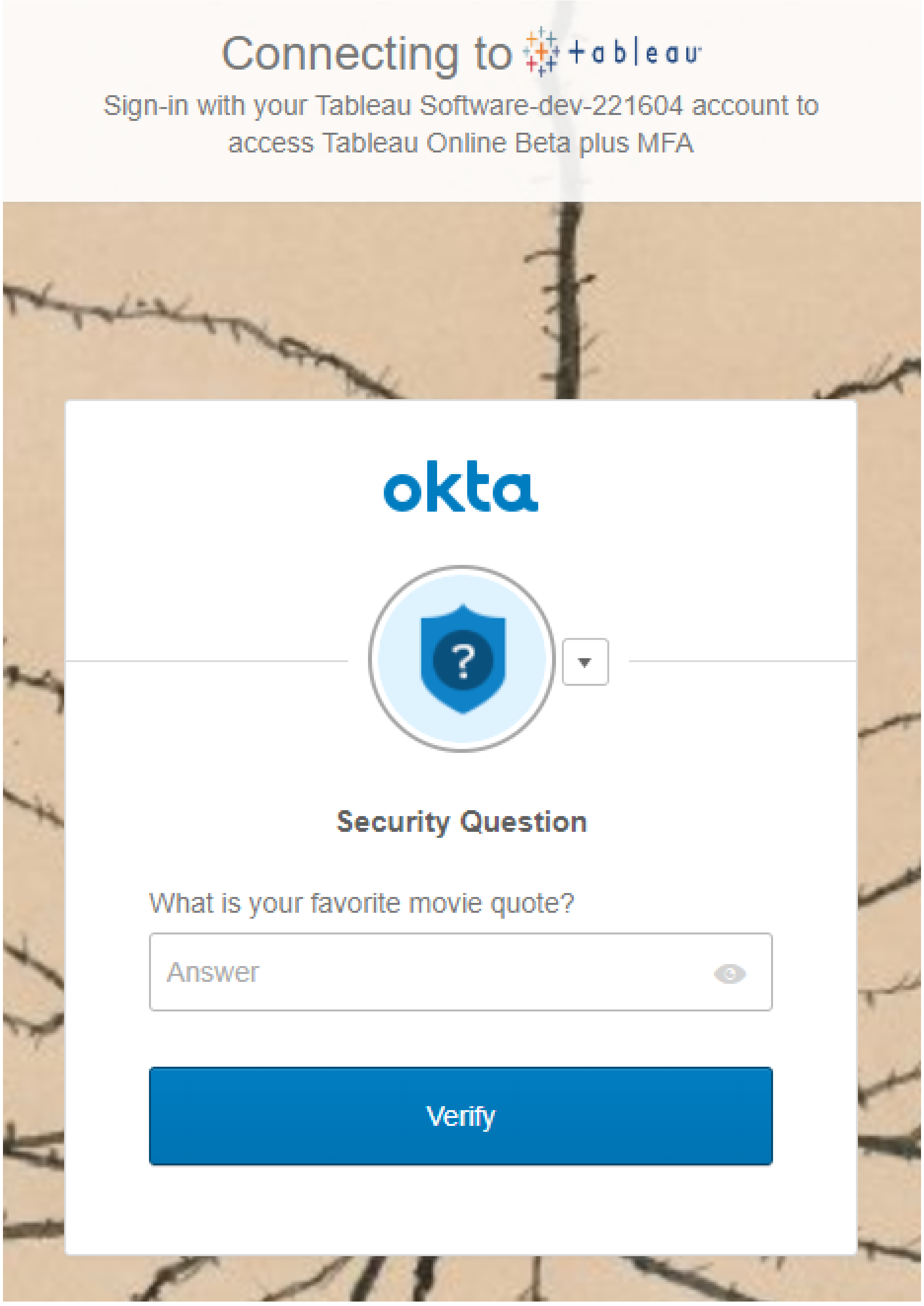
Text Message
Yesterday 11:34 AM

Your verification code is 603932.

Today 2:27 PM

Your verification code is 439689.

If you select Security Question you should be prompted to answer your question:



Connecting to tableau

Sign-in with your Tableau Software-dev-221604 account to access Tableau Online Beta plus MFA

What is your favorite movie quote?

Enter your answer anc click **Verify**