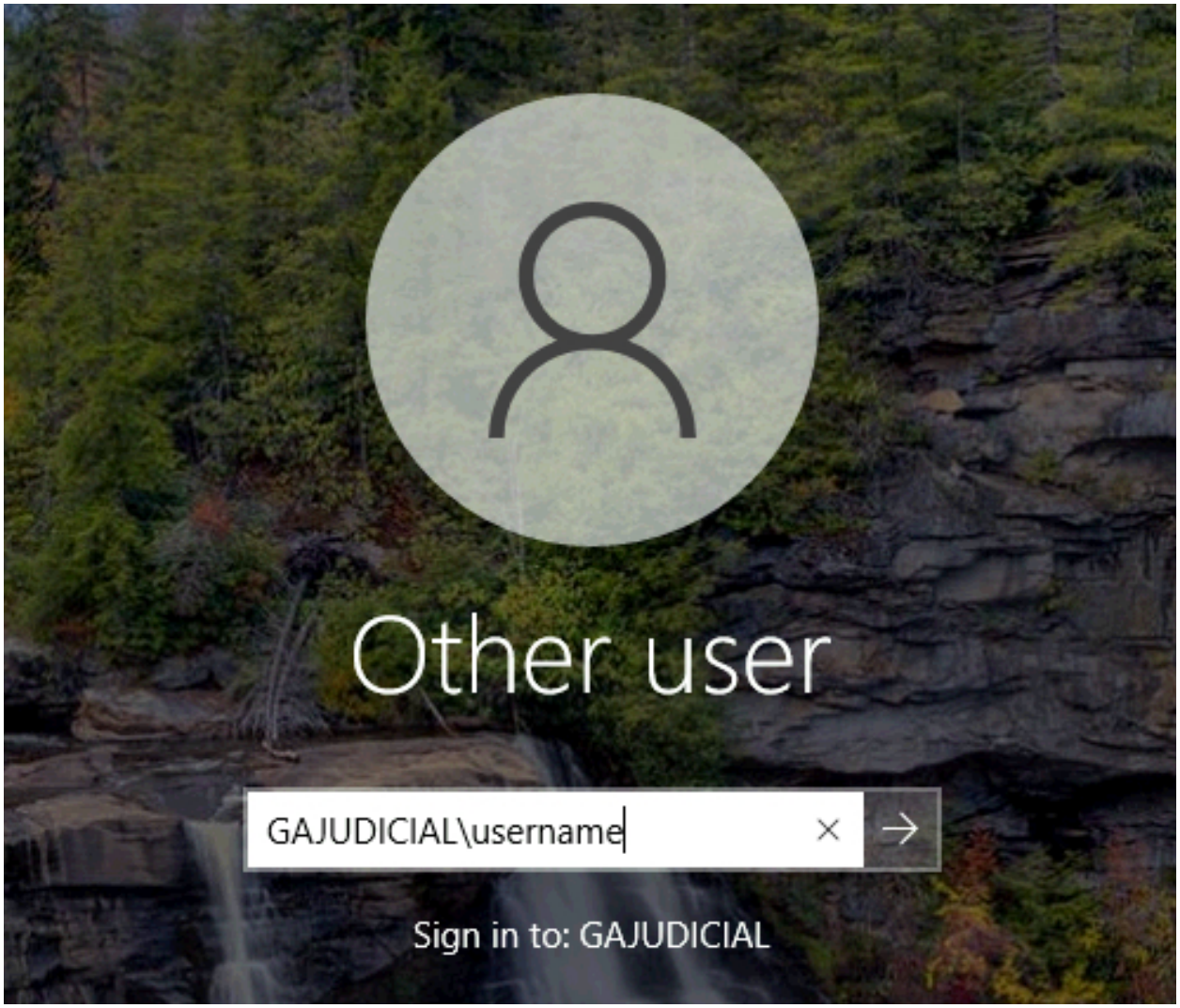
Workstation MFA Instructions

Multi-factor authentication (MFA) will soon be required for workstation access. Similar to the recent rollout for web-based resources users will be allowed to choose one of three second factor methods when logging in and are explained in detail in this document:

- MFA-Smartphone
- MFA-SMS Message
- MFA-OneTimePasscode

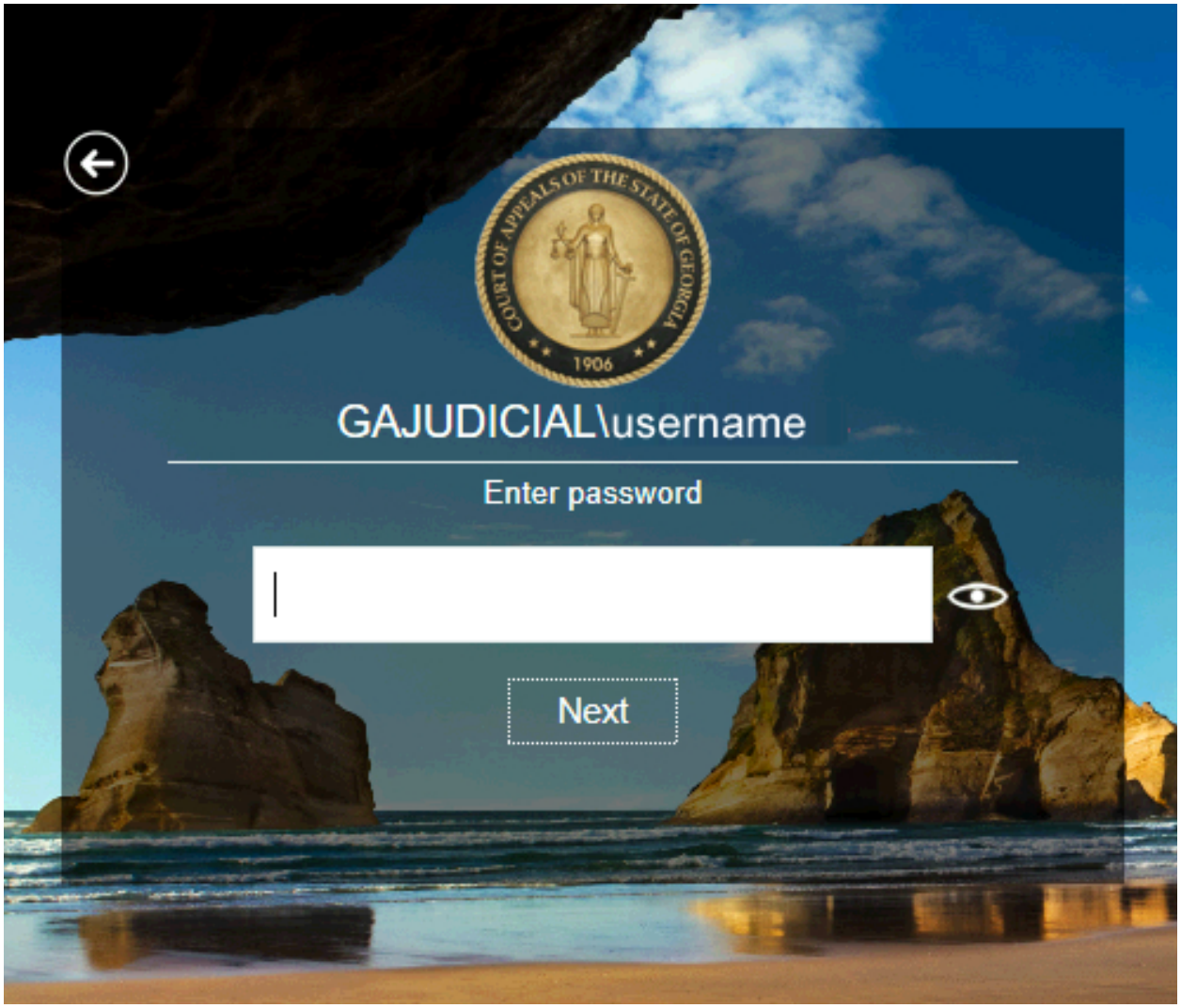
The instructions below provide an overview of how to go through the workstation MFA sign-on process.

1. Enter GAJUDICIAL\your username, then click the arrow or press Enter.

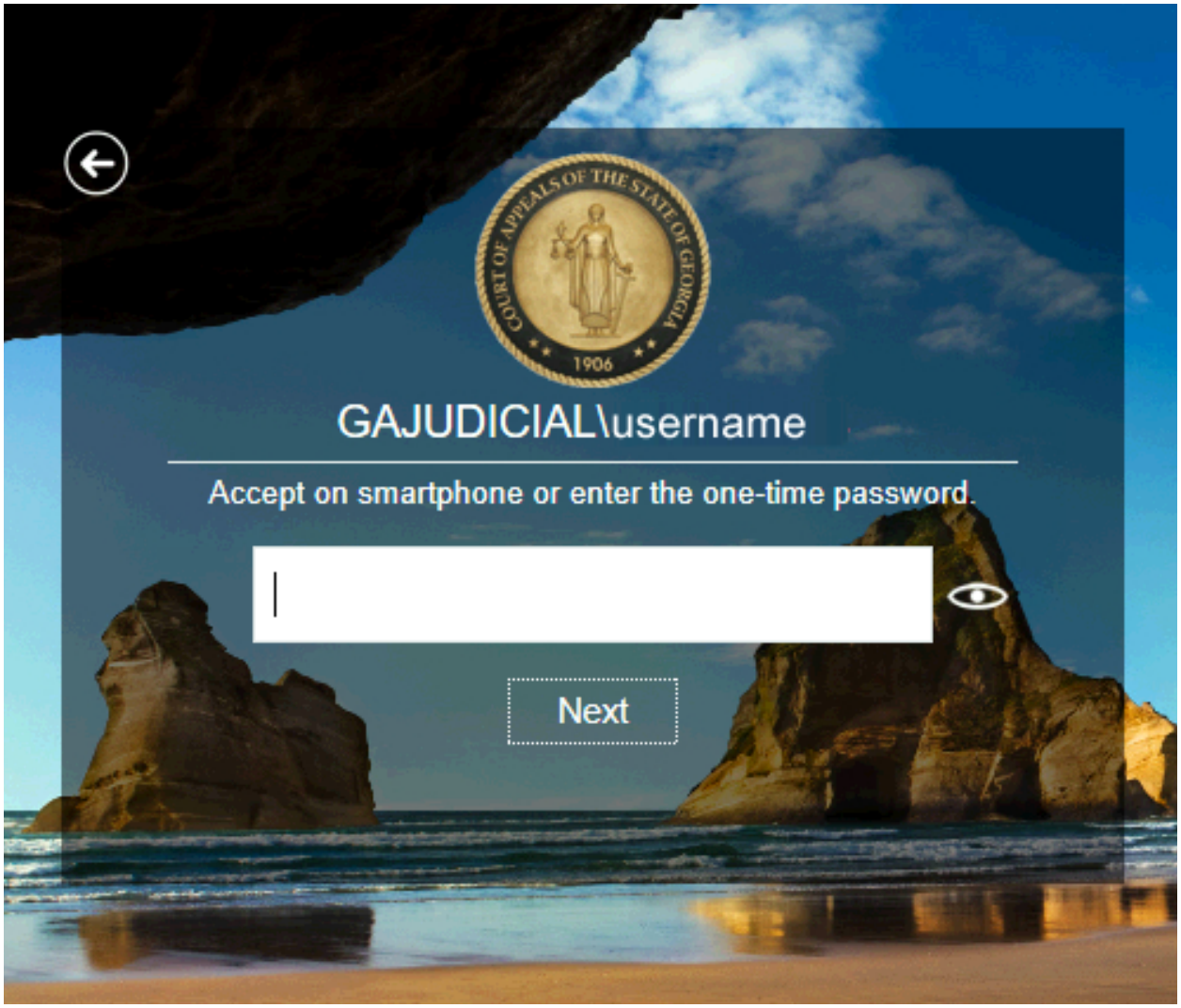


2. Choose one of the listed MFA methods. You will only see options here for methods you've previously enrolled.

3. After choosing a method you will be prompted to enter your network password. Click "Next" to continue.



4. Once your password has been validated you will be instructed on how to proceed in order to provide a second factor. For example, if you had chosen MFA-Smartphone you would be prompted to take one of two actions as seen below.

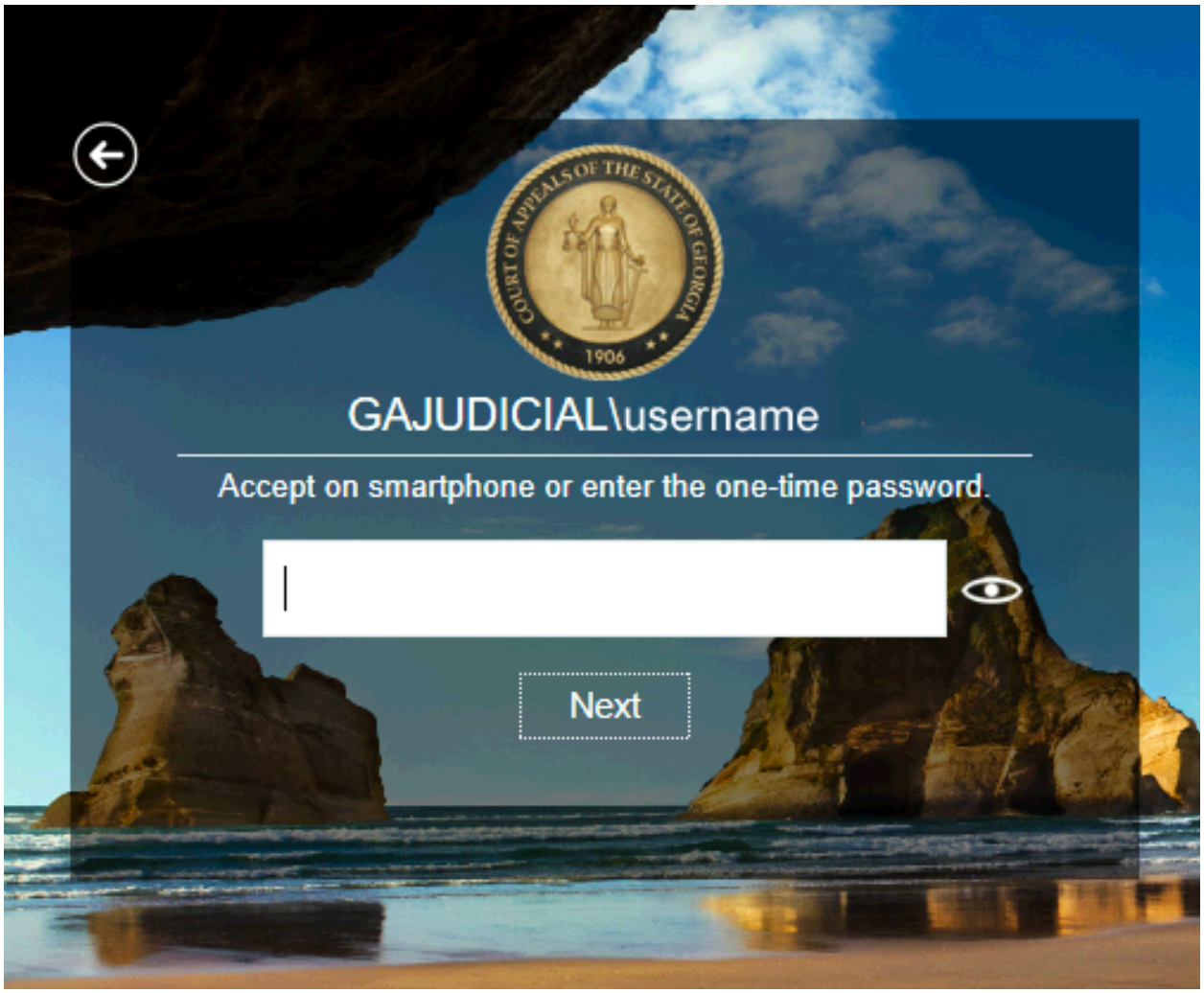


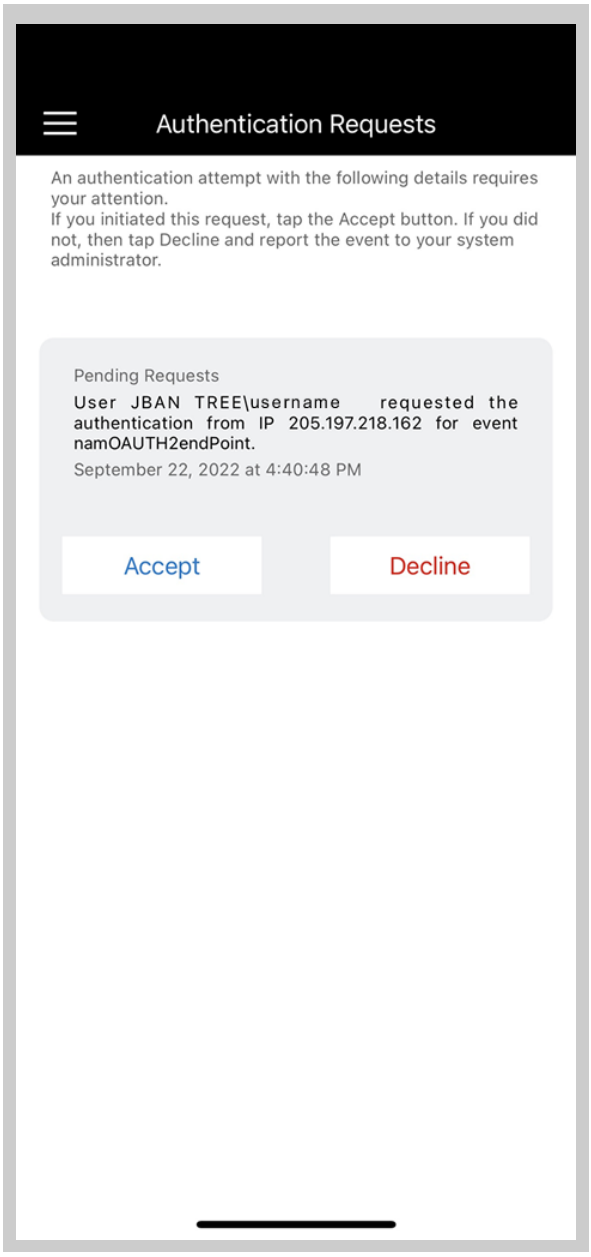
Second Factor Methods Explained

This section outlines the details of the second factor methods and what their individual log in flows will look like.

Smartphone

This method uses the NetIQ Advanced Authentication App. When the device on which this app has been installed is connected to the internet, a push notification with Accept or Reject buttons is displayed and a tap is all that is required to confirm your second factor, as shown below.



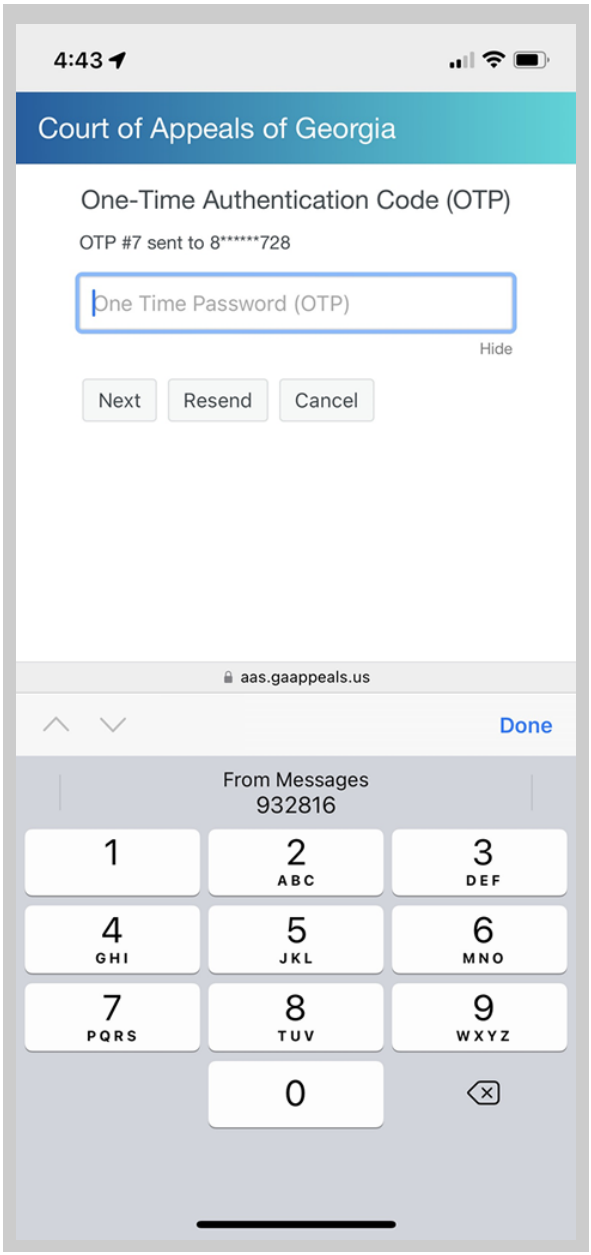


The Smartphone method can still be used to provide a second factor even when offline by entering code displayed in the Smartphone authenticator (for Offline) as the “one-time password.”

SMS Message

This method generates a password that is sent via text message to the phone number you enrolled. Once you receive the text message with the code, enter the code into the box asking for One Time Password, as shown below:

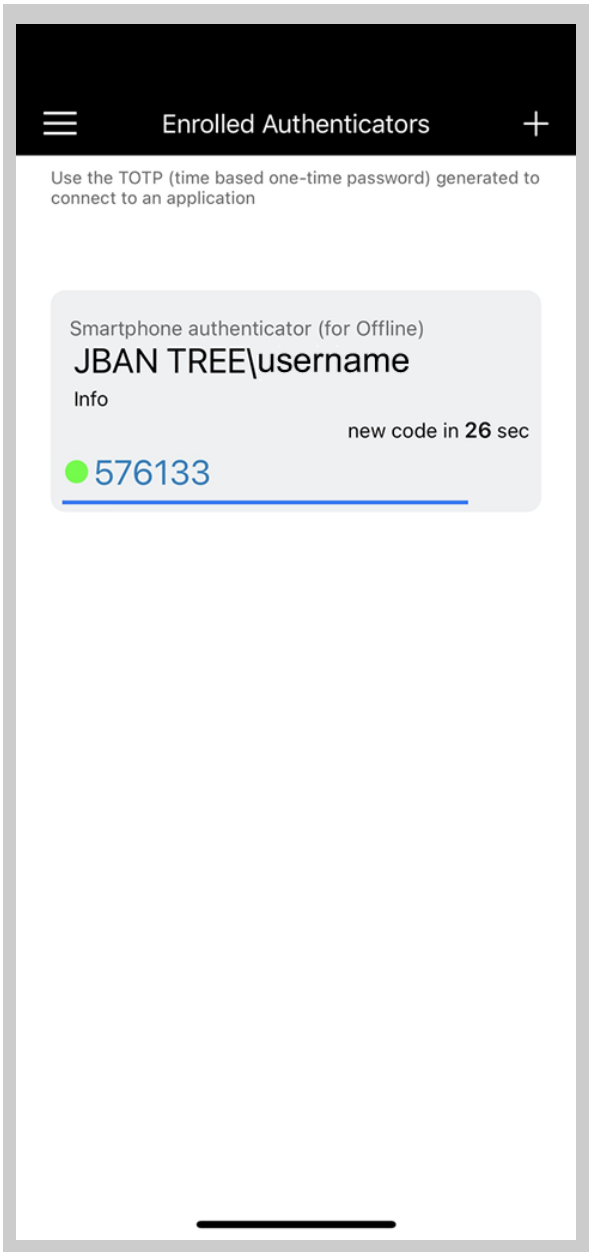

COURT OF APPEALS OF THE STATE OF GEORGIA
1906
GAJUDICIAL\username
OTP #1 sent to 8******728
Next



One Time Passcode

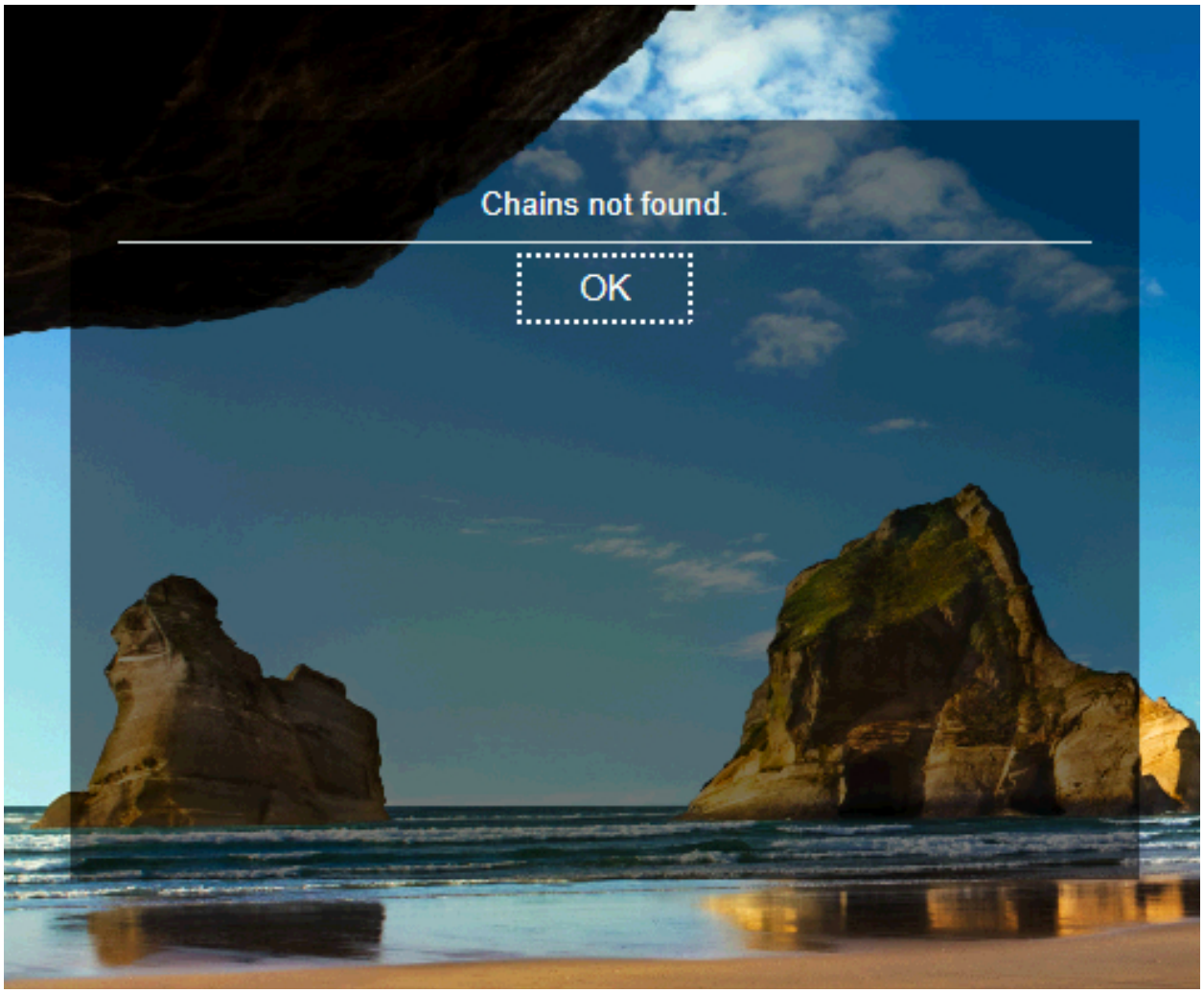
This method enables you to authenticate using a time-based-one-time password (TOTP). The TOTP is generated on the NetIQ Advanced Authentication app. Take the code generated in the app and enter into the box asking for the One Time Password.

The code is valid for a short time before changing, and the time remaining before the code changes is shown in the app, as shown in the screenshot below:

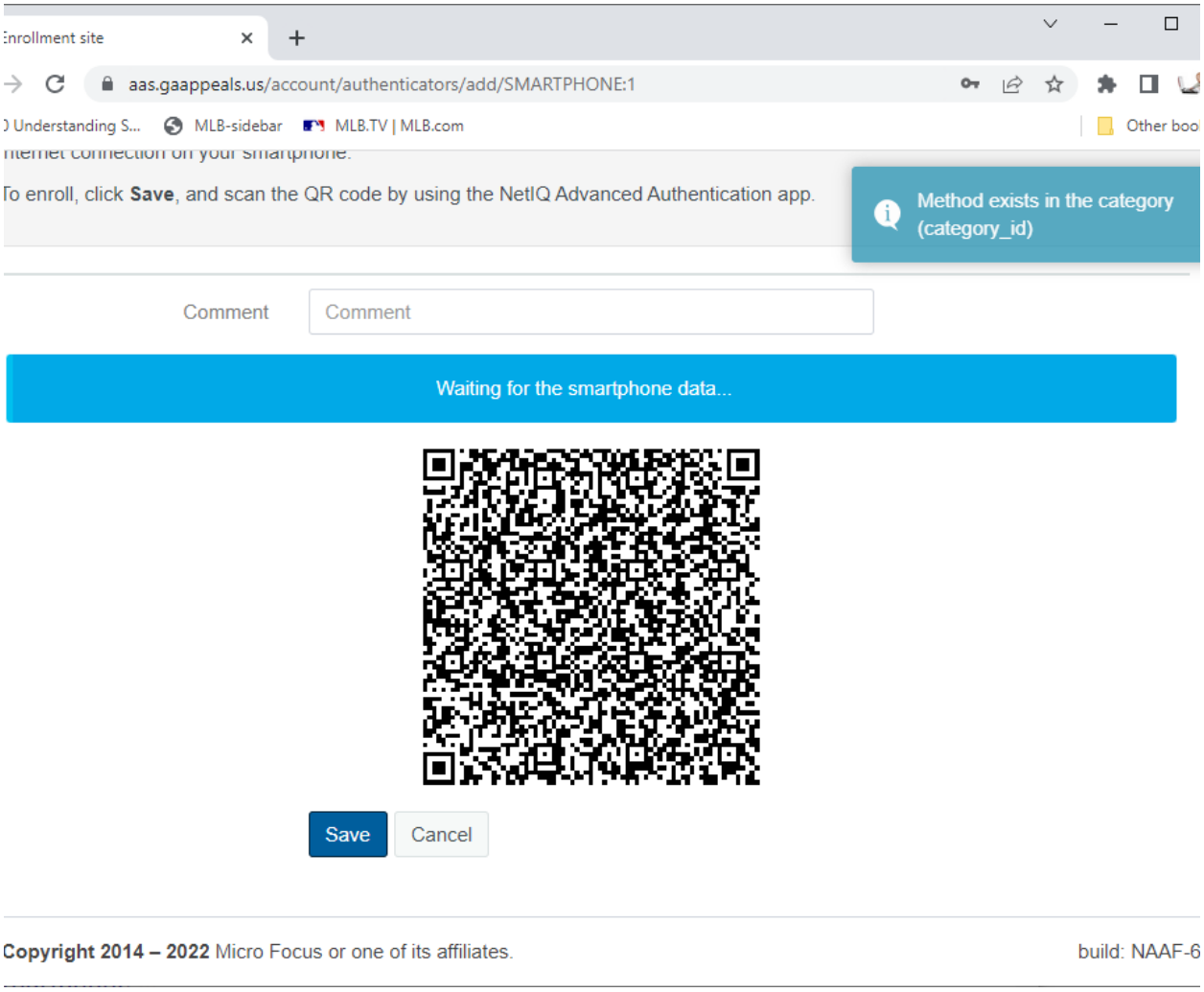

Enrolled Authenticators
Use the TOTP (time based one-time password) generated to connect to an application
Smartphone authenticator (for Offline)
JBAN TREE\username
Info
new code in 26 sec
576133

FAQ

- What happens if I have not yet configured a second factor?
    - You will not see a list of second factors to choose from when you attempt to login. Instead, the following message is displayed. It is not possible to continue until you complete your enrollment from another device.
      Enrollment site: (https://aas.gaappeals.us/account)



- Why am I unable to enroll my Smartphone?
    - If you have already enrolled for TOTP prior to enrolling your Smartphone the enrollment will fail due to certain settings having been enabled. Should you see the following error, delete your TOTP enrollment from the enrollment site as well the TOTP and Smartphone enrollments from your device. Once this has been done enroll your Smartphone and TOTP will be automatically enrolled as well.
      Enrollment site: (https://aas.gaappeals.us/account)


Enrollment site
aas.gaappeals.us/account/authenticators/add/SMARTPHONE:1
Understanding S...
MLB-sidebar
MLB.TV | MLB.com
Other boo
To enroll, click Save, and scan the QR code by using the NetIQ Advanced Authentication app.
Method exists in the category (category_id)
Comment
Comment
Waiting for the smartphone data...
Save
Cancel
Copyright 2014 – 2022 Micro Focus or one of its affiliates.
build: NAAF-6