All About MFA Factors in Okta

David Raco - 2024-04-30 - Comments (0) - Okta

Default

Definitions

- **Okta**: Okta is a directory and single sign on (SSO) platform designed to make it both easy and secure to access all the online apps available to you through Southern Oregon University.
- **MFA**: MFA stands for “multi-factor authentication.” MFA describes the concept of using more than one “factor” to prove your identity to a system. Factors can be something you know (e.g. password), something you have (e.g. possession of a phone configured with Okta Verify), or something you are (e.g. biometrics). You achieve MFA whenever you use a combination of two or more of these factor types together to provide strong assurance of your identity when you access SOU’s systems through Okta.

MFA Setup in Okta

To keep your SOU account secure, you should configure one or more MFA factors in Okta for securing your account. (You may be required by SOU’s security policies to do this.) This article will provide you with more information about each factor available to you and how to use them with your Okta account.

Enrolling a MFA Factor

When you sign in to Okta (https://okta.sou.edu), you will first be prompted for your password. That is your first factor: something that only you should know. After you provide the correct password for your account, Okta will then ask you to present at least one other factor type before letting you in--unless your account is configured to skip this step.

If you are missing a suitable factor on your account for this second step, Okta will prompt you to enroll a factor that satisfies the requirement. (More on enrolling for these factors later.)

If you already have a suitable factor on your account for the second step, Okta will have you prove your possession of that factor, then it will let you into your account.

Note

Okta maintains a guide for first-time setup here. We do not support all the factors they mention, but the guide covers everything that we do support.

Enrolling or Removing a MFA Factor from Your Dashboard

Even when you have enough factors to satisfy Okta’s security requirements for your account, you always have the option of enrolling additional factors from your Okta Dashboard. Here are the steps:

1. Log in to Okta at https://okta.sou.edu
2. Navigate to your account settings by clicking on your name in the top-right corner of the screen, then select Settings from the menu. (See the screenshot below.)
3. On the Settings page, scroll down and look for the Security Methods section. That section of the Settings screen will show you all your enrolled MFA factors and will also present you with buttons you can use to either enroll additional factors or remove factors from your Okta account.
    1. Please avoid removing MFA factors from your account unless you no longer have possession of the factor. For example, if you bought a new phone and no longer have the old one, then go ahead and remove the old phone from your account and enroll the new phone.
    2. It is normal to be prompted for your password again when enrolling a new factor through your account settings. That is a security feature!
4. Follow the on-screen instructions to finish registering whichever factor you selected to enroll.

Available MFA Factors in Okta

See below for a description of each factor and how to set it up.

- **Something You Know**
    - Password
- **Something You Have**
    - Okta Verify (phone app)
    - Phone
    - One-time code hardware token
- **Something You Are**
    - Okta Verify (phone app): Okta Verify *optionally* supports the use of available biometric factors on smartphones that support fingerprint reading or facial recognition.

Password

Question

See our companion article at How to Change Your SOU Account Password in Okta for detailed instructions on how to change your password.

You can reset your password from your Okta dashboard settings (the same place you manage your MFA factors). The Change Password section is just above the Security Methods section. Provide your current password, then create a new password that conforms to the password policies displayed in the Change Password section. If you need help, contact our IT Helpdesk at 541-552-6900.

Okta Verify

Okta Verify is a versatile, free app that runs on your iOS or Android phone or tablet. Okta Verify is our recommended MFA factor for all users because of how powerful and convenient it is. Okta Verify supports push notifications sent to your device (tap to approve), time-based one-time codes, and biometric verification if your device supports doing that.

iOS Instructions	**Android Instructions**
Download Okta Verify for iOS	Download Okta Verify for Android
Learn all about using Okta Verify for iOS	Learn all about using Okta Verify for Android
Configuring biometric authentication for iOS	Configuring biometric authentication for Android

The push notification and biometric authentication methods in Okta Verify require an active data connection to function (Wi-Fi, 3G, 4G, 5G, etc).

The time-based one-time code authentication method in Okta Verify *does not require an activate data connection*. It can be used even when you have no Internet connectivity.

Phone

You can register any active phone number in your possession in Okta to receive one-time codes by text message (suitable for mobile phones) or by voice call (suitable for land lines and mobile phones). Charges may apply through your carrier.

One-time code hardware token

We have a limited supply of FEITIAN c200 TOTP tokens available for users who need them. These tokens must be registered in Okta by one of our Okta administrators on your behalf, and you may be asked to provide justification before we issue one to you due to supplies being limited.

The c200 tokens generate 6-digit one-time codes on a small screen that last for up to 30 seconds. The tokens are small enough to be attached to a keyring for portability. The c200 tokens do not rely on data signals of any kind. Instead, they rely on an internal clock being in sync with the Okta server in order to generate codes they can both agree on. The clocks in the c200 tokens naturally drift over time, and we expect they will stop working 2.5 years after being issued. At that time, you will need to contact infosec@sou.edu to receive a new token.

Still Need Help?

If you have questions after reading this article, please contact our IT Helpdesk at 541-552-6900 or at helpdesk@sou.edu.