# FCC New Hire Login User Guide

This document will take you through the steps to log in to your FCC Okta account to set your network password and multifactor authentication (MFA) method. This will then allow you to access Office 365, OneDrive, and SharePoint to complete your work duties until your FCC Government-Furnished (GFE) Laptop is provisioned and assigned to you. Please note that you will need to have an FCC network account (created by FCC IT during your Onboarding process) in order to log in to Okta, Office 365, and your GFE laptop. Additionally, please follow and complete the steps in the RSA Secure Token iOS/Android tip sheets (for multifactor authentication) that accompany this packet prior to attempting your first login. The Okta Verify mobile app setup (optional, for multifactor authentication) will take place during the first login attempt, instructions for which are integrated below.

## Set Network Password and MFA using Okta

### Setting Your Network Password

1. On your computer, open a web browser and navigate to fcc.okta.com.

2. An FCC login prompt should appear with fields for your FCC username and network password. In the username field, enter your FCC username (firstname.lastname). Do not enter your full FCC email address with the @fcc.gov domain.

3. In the network password field, enter default network password listed below.

   Default network password: ***Password01!!***

4. You will be prompted to set and confirm a new network password of your choosing. The password strength and complexity requirements are listed in the table below.

| **PASSWORD REQUIREMENTS:** | |
|---|---|
| **Complexity** | Passwords must contain **three** of the four following criteria: |
| **Minimum Password Length** | 12 Characters<br>At least one uppercase letter (A-Z)<br>At least one lowercase letter (a-z)<br>At least one number and a special character<br>Do not use the word "**password"** or any part of your name. |
| **Expiration Date** | 60 days |
| **Password Reuse** | Users may not use their previous 24 passwords. With normal password expirations this is equal to 5 years. |

| | |
|---|---|
| **Inactive Accounts Disabling** | Inactive accounts will be disabled 45 days following password expiration. After 90 days, the account will be deleted. |

5. Enter your desired network password into the New Password field, then re-enter the same password in the Confirm New Password field. When finished, press **Enter** on your keyboard to continue.

   *Note: In the future, the FCC will require use of your FCC PIV card when logging in to the laptop. The PIV card uses a 6-8 digit PIN of your choosing that is set when the PIV card is received from the FCC Security Office. However, there will still be some FCC sites or systems that will require the use of your network password, so it is important to remember or make a note of your password for use in those instances.*

## Setting Your RSA Multifactor Authentication

*Note that this section requires you to have previously set up the RSA SecurID Authenticator app on your mobile device. The RSA instructions for Android and iOS device types have been included in your onboarding packet.*

1. After setting your network password, you should now see a screen prompting you to configure your RSA SecurID token. Click the blue **Configure Factor** button.

2. A new login box should appear, with fields for your FCC username and RSA passcode. In the username field, enter your FCC username.

3. In the RSA passcode field, enter the 8 digits that display in the RSA token app on your mobile device, then click **Verify**.

4. The login should return and prompt you to set and confirm your RSA PIN. In the **New PIN** text box, enter your new 4 to 8 digit PIN.

   *Note: It is strongly recommended that you use at least a 6 digit PIN.*

5. After the PIN is accepted, you will be prompted to enter your RSA passcode information once more. **From this point forward, each time you are prompted for your RSA passcode during a login attempt, your RSA passcode will be your PIN first, followed by the digits from your token, all entered within the same field.**

   *Example: I set my RSA PIN to 9999. My RSA token is displaying the code 12345678. My RSA passcode for login would therefore be 999912345678 (i.e. PIN plus token code).*

6. You will now be taken to a screen that confirms that your RSA SecurID token is connected to your account. Ensure that you see RSA SecurID listed under the Enrolled Factors section on this page. You will also see the option to set up Okta Verify multifactor authentication, instructions for which are included in the next section of this document.

*Note: At this time, Okta Verify is not required to log in. However, it is strongly encouraged that you set up this factor as well, as the RSA token will eventually be phased out of use.*

*Note: You will also have the option to set up SMS text authentication for multi-factor authentication. You may set this up if desired; however, the use of SMS authentication is not recommended at this time.*

### Setting Your Okta Verify Multifactor Authentication

1. After setting up your RSA SecurID multifactor authentication, you will be taken to a screen that lists Okta Verify as an additional multifactor authentication option. Click the **Setup** button.

2. When prompted, select your device type (iOS device or Android). After selecting your device type, you should see a QR code displayed on the screen. ***Do not leave this screen.*** You will be using this QR code momentarily.

3. On your cell phone or other mobile device, access the app store and download the Okta Verify app.

4. Once the app has installed on your device, open the app and click the **Add an Account** button, then select **Organization**.

5. If prompted, select the option to allow Okta Verify to access your device's camera. Hold the device in front of your computer screen, such that the camera aligns with the QR code that is displayed on your screen. The Okta Verify app will detect the QR code and automatically finish the account setup.

6. You may be prompted to send a push notification to your device. If so, click the **Send Push** button. A push notification should appear on your mobile device, asking you to confirm your login attempt.

## Accessing Office 365

1. Open a web browser and navigate to office.com. Once the page loads, select **Sign In**.

2. On the login screen, enter your full FCC email address (firstname.lastname@fcc.gov). You will be redirected to an FCC login page.

3. When prompted, enter your FCC network password that you set in the section above.

4. You will then be prompted for your RSA passcode. Recall from the section above that your RSA passcode consists of the RSA PIN that you set previously, plus the 8 digit token code that appears in the RSA SecurID app on your mobile device.

5. Once you complete the login process, you will be taken to the Office 365 landing page. From here, you may access Office 365 webmail, OneDrive, and other Office 365 web applications.

## IT Service Center Contact Information

If at any point during the login process you experience an issue, please contact the FCC IT Service Center at 202-418-1200 or Service-Center@fcc.gov. Our technicians are available 7:00 a.m. – 9:00 p.m. Monday through Friday and 9:00 a.m. – 5:00 p.m. on weekends.