

ILPartner Account Setup Instructions



Index

Updated 6/25/24

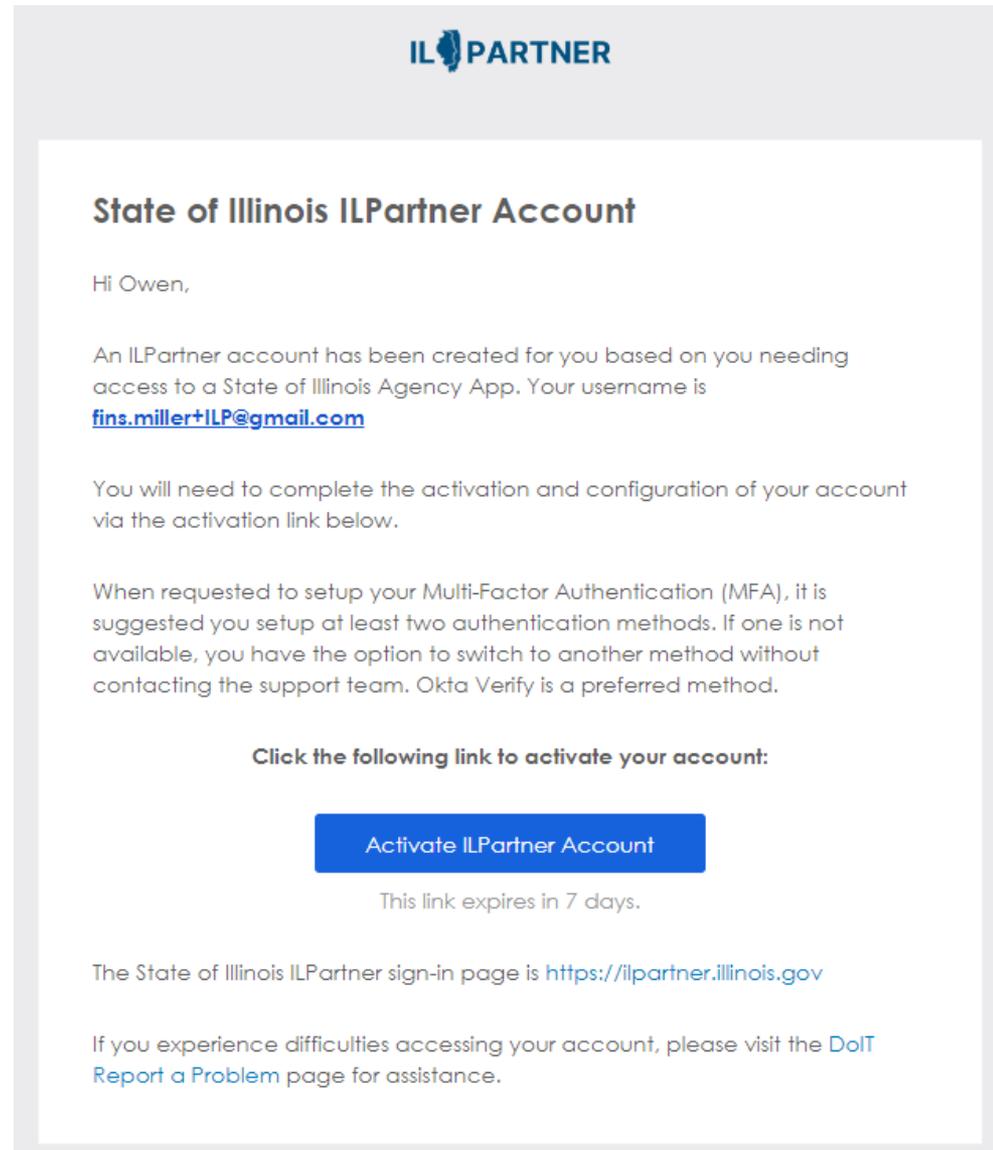
1. Receive ILPartner Activation email	2
2. Start the Activation process	3
3. SELECT At Least ONE of the below MFA options	4
I. Option 1: Okta Verify	5
II. Option 2: Google Authenticator	7
III. Option 3: SMS Authentication	9
IV. Option 4: Voice Call Authentication	11
V. Option 5: Security Key or Biometric Authenticator	13
4. Logout of ILPartner	14
5. Additions, Changes and Adjustments after initial setup	15

1. How to Activate your new State of Illinois ILPartner Account

Once you receive the ILPartner activation email from SOI.No-Reply@illinois.gov, click on the Blue “Activate Okta Account” button.

Note: this link expires after 7 days, so important to activate your account ASAP. After 7 days you will have to contact your appropriate service desk source to have an activation email resent. Your email may have different content depending on the Agency app requested.

Reminder: your email address will be your Okta Username.

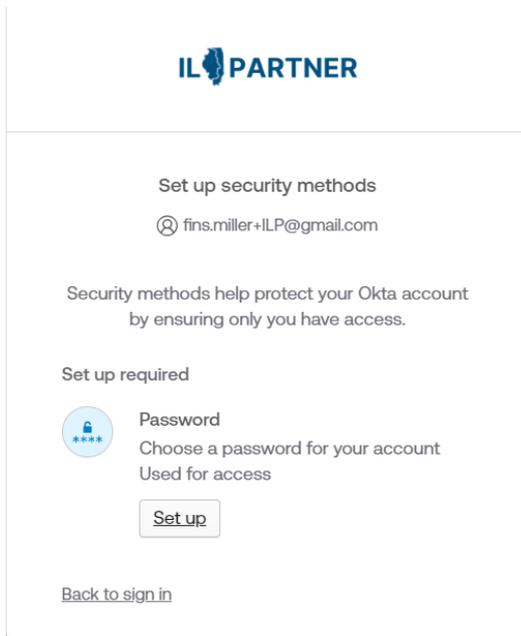


2. Start the account setup process

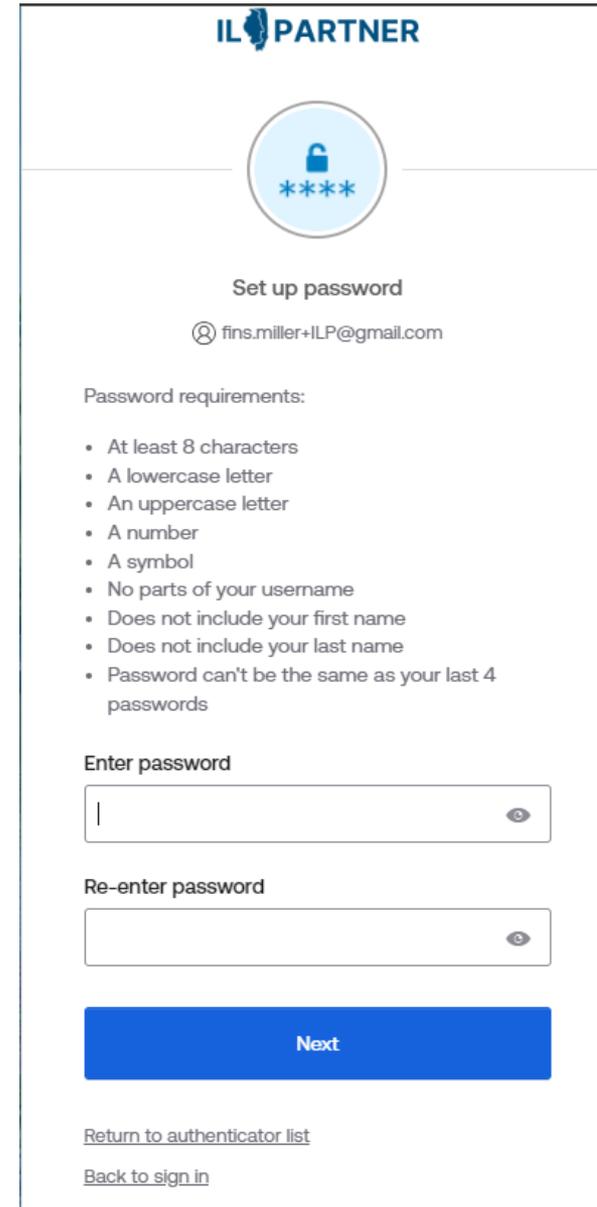
The link will open <https://ilpartner.illinois.gov/> using a special token for your account. All sections need to be completed before you will be able to access your account and applicaitons.

Note: the Google Chrome browser is the most stable for Okta.

1. Click on Set up and then provide a secure password and re-enter before clicking Next.



The screenshot shows the 'Set up security methods' page for the IL PARTNER account. At the top is the IL PARTNER logo. Below it, the text 'Set up security methods' is displayed, followed by the email address 'fins.miller+ILP@gmail.com'. A message states: 'Security methods help protect your Okta account by ensuring only you have access.' Under the heading 'Set up required', there is a 'Password' section with a lock icon and four asterisks. The text reads: 'Choose a password for your account Used for access'. A 'Set up' button is located below this section. At the bottom left, there is a link that says 'Back to sign in'.



The screenshot shows the 'Set up password' page for the IL PARTNER account. At the top is the IL PARTNER logo. Below it is a circular icon with a lock and four asterisks. The text 'Set up password' is displayed, followed by the email address 'fins.miller+ILP@gmail.com'. Under the heading 'Password requirements:', there is a list of requirements: 'At least 8 characters', 'A lowercase letter', 'An uppercase letter', 'A number', 'A symbol', 'No parts of your username', 'Does not include your first name', 'Does not include your last name', and 'Password can't be the same as your last 4 passwords'. Below the list are two input fields: 'Enter password' and 'Re-enter password', each with a toggle eye icon. A large blue 'Next' button is positioned below the input fields. At the bottom, there are two links: 'Return to authenticator list' and 'Back to sign in'.

3. Setup at least one of the below MFA options

(would be best to setup more than one in case one is not working, you can change to another setup method)

Choose one or more of the below options for registering Multi-Factor Authentication (MFA)

- I. Okta Verify (go to page 5 for detailed steps)
- II. Google Authenticator (go to page 7 for detailed steps)
- III. Phone - SMS Authentication (go to page 9 for detailed steps)
- IV. Phone - Voice Call Authentication (go to page 11 for detailed steps)
- V. Security Key or Biometric Authenticator (go to page 13 for detailed steps)

Note: Proceed to the next page as per the MFA option selected.

Set up security methods

📧 fins.miller+ILP@gmail.com

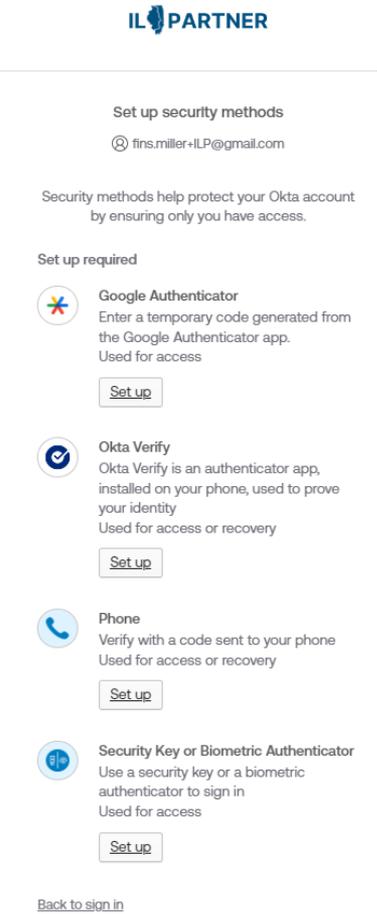
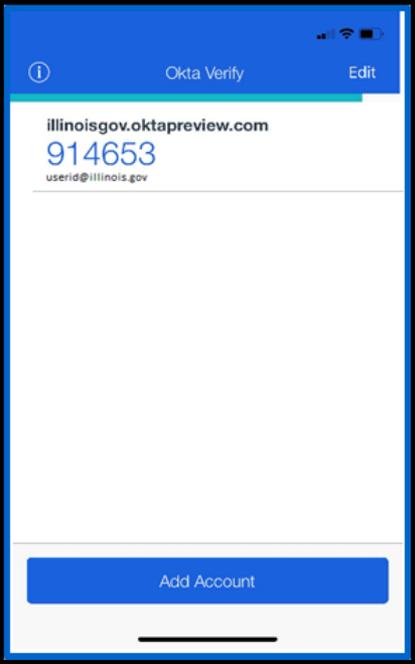
Security methods help protect your Okta account by ensuring only you have access.

Set up required

-  **Google Authenticator**
Enter a temporary code generated from the Google Authenticator app.
Used for access
[Set up](#)
-  **Okta Verify**
Okta Verify is an authenticator app, installed on your phone, used to prove your identity
Used for access or recovery
[Set up](#)
-  **Phone**
Verify with a code sent to your phone
Used for access or recovery
[Set up](#)
-  **Security Key or Biometric Authenticator**
Use a security key or a biometric authenticator to sign in
Used for access
[Set up](#)

[Back to sign in](#)

Option I: Okta Verify

Step 1	Step 2	Step 3
<p><u>User Action:</u> Select Okta Verify <i>Setup</i> button</p>	<p><u>User Action:</u> Download the 'Okta Verify' App to your smartphone.. Folow instructions provided</p>	<p><u>User Action:</u> Sample Screenshot from phone depicting a registered account.</p>
		

Option I: Okta Verify

Step 4

User Action:

When successful user can click Set up later or preferably setup additional methods.



Set up security methods

 okta.ford@illinois.gov

Security methods help protect your Okta account by ensuring only you have access.

Set up optional



Google Authenticator

Enter a temporary code generated from the Google Authenticator app. Used for access

[Set up](#)



Okta Verify

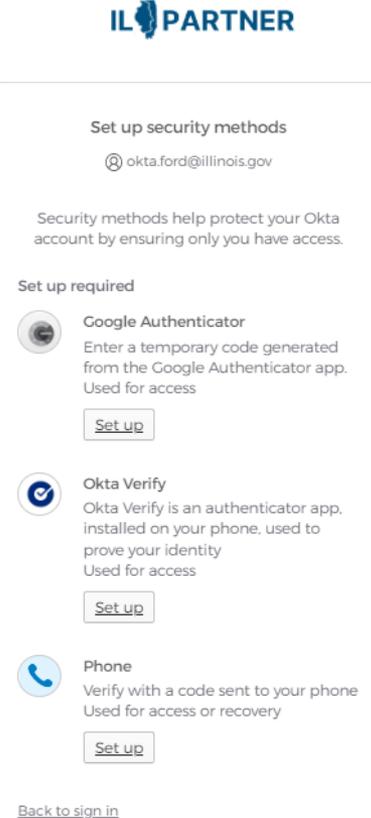
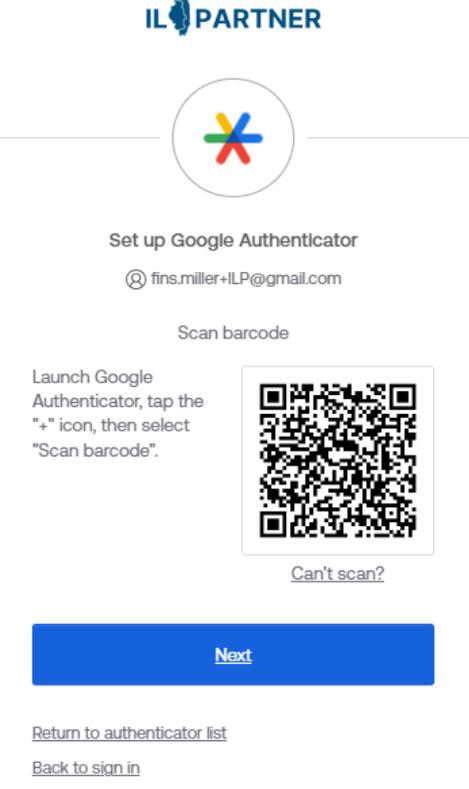
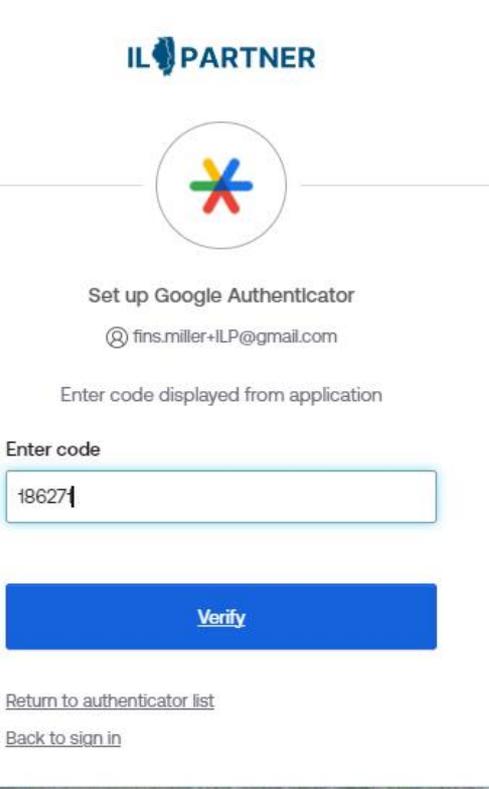
Okta Verify is an authenticator app, installed on your phone, used to prove your identity. Used for access

[Set up](#)

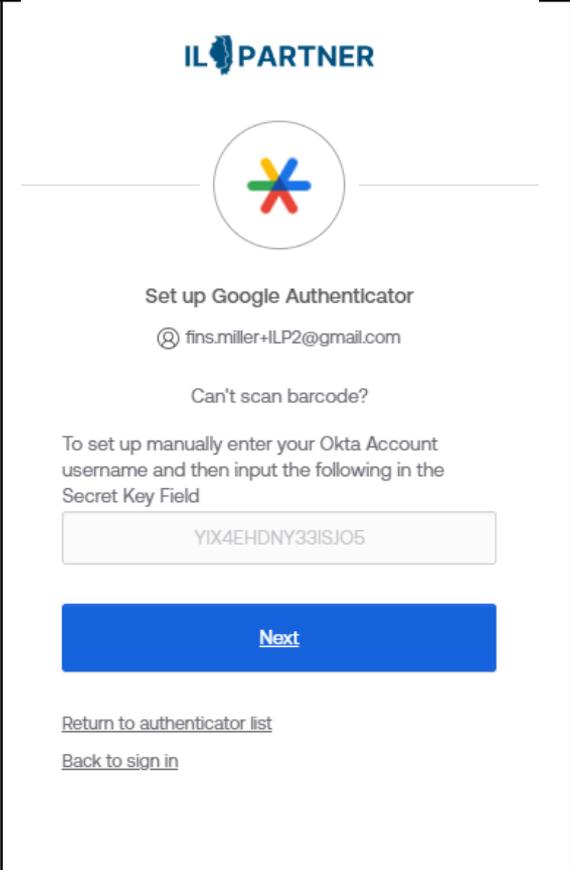
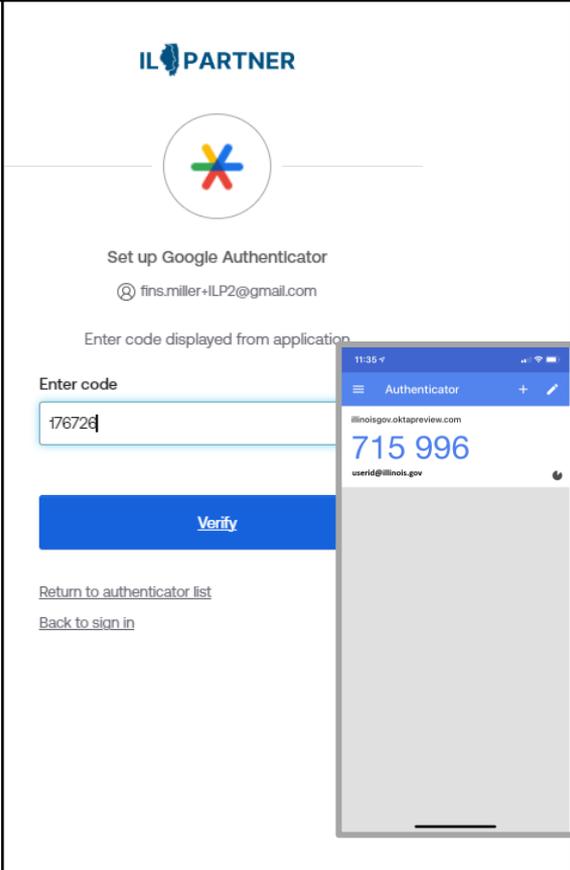
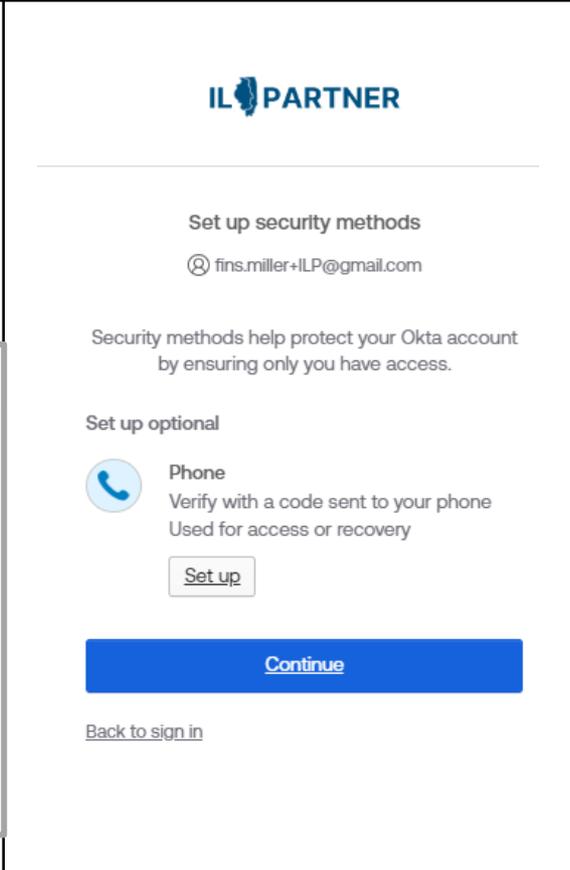
[Set up later](#)

[Back to sign in](#)

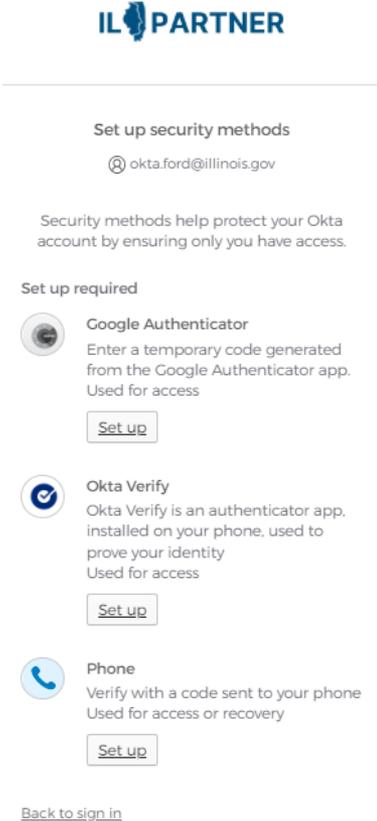
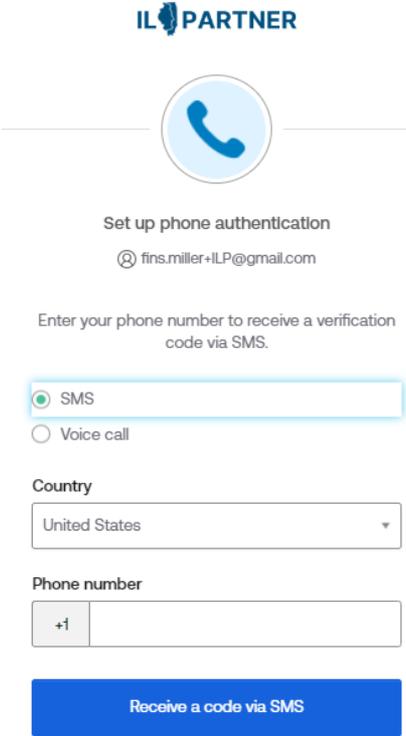
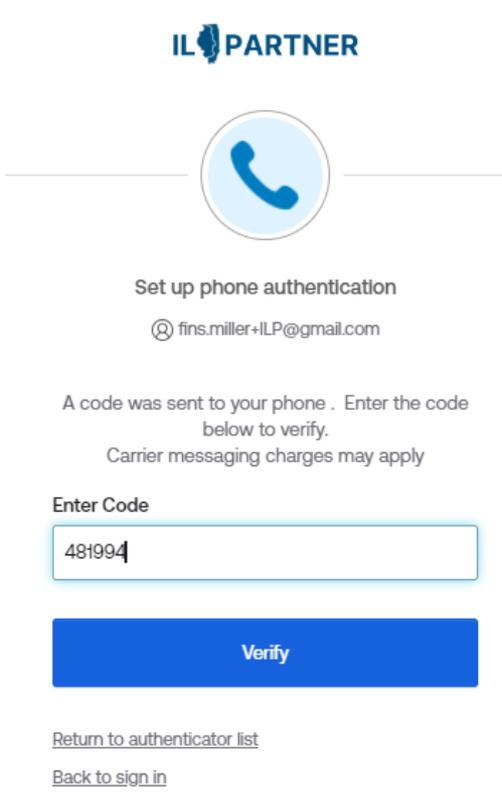
Option II: Google Authenticator

Step 1	Step 2	Step 3
<p><u>User Action:</u> Select <i>Google Authenticator Setup</i> button</p>	<p><u>User Action:</u> download and open the 'Google Authenticator' App to your smartphone.</p>	<p><u>User Action:</u> Scan code from <i>Google Authenticator</i> App in your mobile (or) proceed to Step 4 to enter manually</p>
 <p>IL PARTNER</p> <p>Set up security methods @ okta.ford@illinois.gov</p> <p>Security methods help protect your Okta account by ensuring only you have access.</p> <p>Set up required</p> <ul style="list-style-type: none"> Google Authenticator Enter a temporary code generated from the Google Authenticator app. Used for access Set up Okta Verify Okta Verify is an authenticator app, installed on your phone, used to prove your identity. Used for access Set up Phone Verify with a code sent to your phone. Used for access or recovery Set up <p>Back to sign in</p>	 <p>IL PARTNER</p> <p>Set up Google Authenticator @ fins.miller+ILP@gmail.com</p> <p>Scan barcode</p> <p>Launch Google Authenticator, tap the "+" icon, then select "Scan barcode".</p>  <p>Can't scan?</p> <p>Next</p> <p>Return to authenticator list</p> <p>Back to sign in</p>	 <p>IL PARTNER</p> <p>Set up Google Authenticator @ fins.miller+ILP@gmail.com</p> <p>Enter code displayed from application</p> <p>Enter code</p> <input type="text" value="186271"/> <p>Verify</p> <p>Return to authenticator list</p> <p>Back to sign in</p>

Option II: Google Authenticator

Step 4	Step 5	Step 6
<p>User Action: Enter Account ID manually and enter the Secret Key to activate Google Authenticator. Click Next</p>	<p>Enter the 6-digit Code on your Google App and click Verify. Sample Screenshot from phone depicting a registered account.</p>	<p>User Action: When successful user can click Set up later or preferably setup additional methods.</p>
 <p>IL PARTNER</p> <p>Set up Google Authenticator</p> <p>fms.miller+ILP2@gmail.com</p> <p>Can't scan barcode?</p> <p>To set up manually enter your Okta Account username and then input the following in the Secret Key Field</p> <p>YIX4EHDNY33ISJO5</p> <p>Next</p> <p>Return to authenticator list</p> <p>Back to sign in</p>	 <p>IL PARTNER</p> <p>Set up Google Authenticator</p> <p>fms.miller+ILP2@gmail.com</p> <p>Enter code displayed from application</p> <p>Enter code</p> <p>176726</p> <p>Verify</p> <p>Return to authenticator list</p> <p>Back to sign in</p> 	 <p>IL PARTNER</p> <p>Set up security methods</p> <p>fms.miller+ILP2@gmail.com</p> <p>Security methods help protect your Okta account by ensuring only you have access.</p> <p>Set up optional</p> <p>Phone</p> <p>Verify with a code sent to your phone Used for access or recovery</p> <p>Set up</p> <p>Continue</p> <p>Back to sign in</p>

Option III: SMS Authentication

Step 1	Step 2	Step 3
<p>User Action: Select Phone Setup button</p>	<p>User Action: Enter a Mobile phone number and click on “Receive a code via SMS”.</p>	<p>User Action: Enter the code received on the mobile phone and click ‘Verify’.</p>
 <p>IL PARTNER</p> <p>Set up security methods @ okta.ford@illinois.gov</p> <p>Security methods help protect your Okta account by ensuring only you have access.</p> <p>Set up required</p> <ul style="list-style-type: none">Google Authenticator Enter a temporary code generated from the Google Authenticator app. Used for access Set upOkta Verify Okta Verify is an authenticator app, installed on your phone, used to prove your identity. Used for access Set upPhone Verify with a code sent to your phone. Used for access or recovery Set up <p>Back to sign in</p>	 <p>IL PARTNER</p> <p>Set up phone authentication @ fins.miller+ILP@gmail.com</p> <p>Enter your phone number to receive a verification code via SMS.</p> <p><input checked="" type="radio"/> SMS <input type="radio"/> Voice call</p> <p>Country United States</p> <p>Phone number +1</p> <p>Receive a code via SMS</p> <p>Return to authenticator list Back to sign in</p>	 <p>IL PARTNER</p> <p>Set up phone authentication @ fins.miller+ILP@gmail.com</p> <p>A code was sent to your phone . Enter the code below to verify. Carrier messaging charges may apply</p> <p>Enter Code 481994</p> <p>Verify</p> <p>Return to authenticator list Back to sign in</p>

Option III: SMS Authentication

Step 4

User Action:

When successful user is returned to setup additional Security Methods. Since user setup phone using SMS it is also automatically available for voice call. User can click Set up later or preferably setup additional methods.



Set up security methods

 okta.ford@illinois.gov

Security methods help protect your Okta account by ensuring only you have access.

Set up optional



Google Authenticator

Enter a temporary code generated from the Google Authenticator app. Used for access

[Set up](#)



Okta Verify

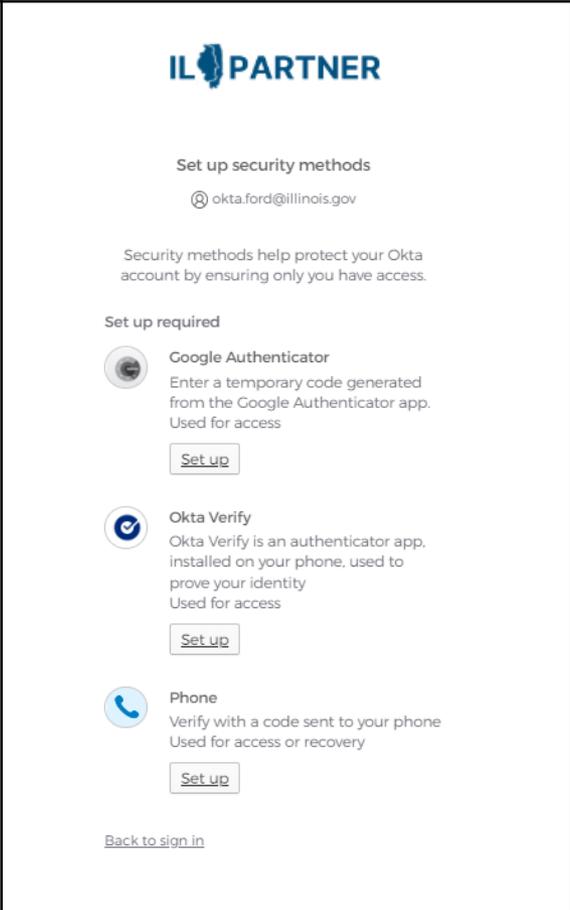
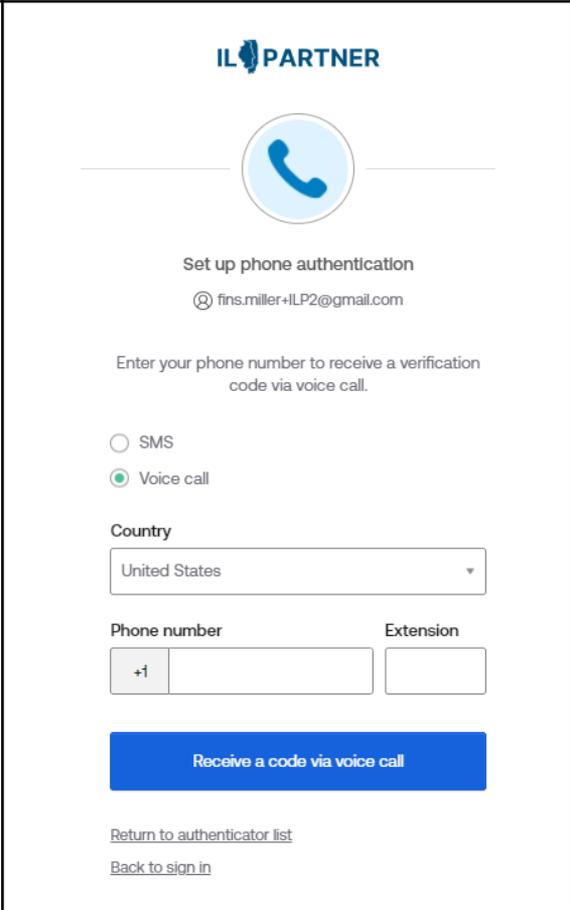
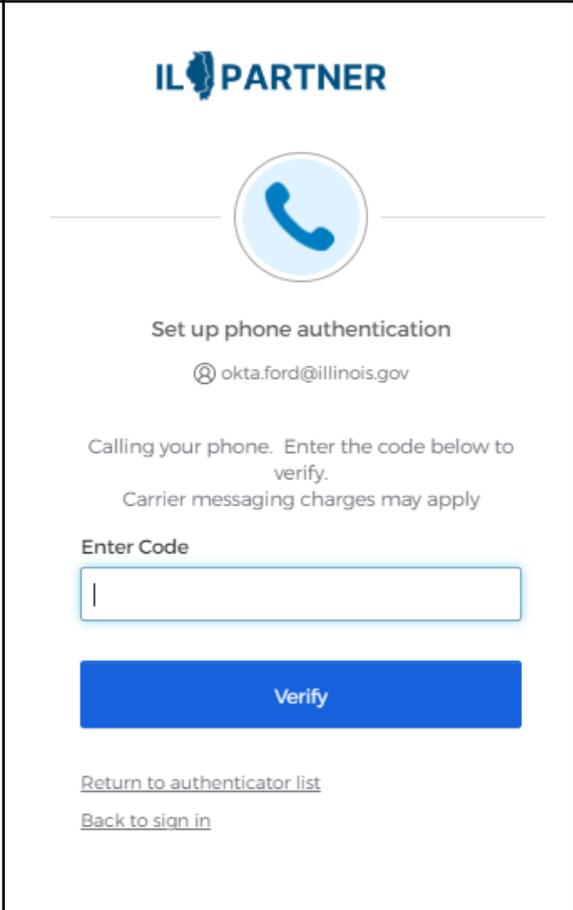
Okta Verify is an authenticator app, installed on your phone, used to prove your identity. Used for access

[Set up](#)

[Set up later](#)

[Back to sign in](#)

Option IV: Voice Call Authentication

Step 1	Step 2	Step 3
<p><u>User Action:</u> Select Phone Setup button</p>	<p><u>User Action:</u> Click Voice Call and Enter a Mobile phone number and click 'Receive a code via SMS'.</p>	<p><u>User Action:</u> Enter the code given during the phone call and click 'Verify'.</p>
 <p>The screenshot shows the 'Set up security methods' page for an Okta Partner. The user is logged in as 'okta.ford@illinois.gov'. The page lists three security methods: Google Authenticator, Okta Verify, and Phone. The 'Phone' method is selected and highlighted. A 'Set up' button is visible for the Phone method. A 'Back to sign in' link is at the bottom.</p>	 <p>The screenshot shows the 'Set up phone authentication' page for the user 'fins.miller+ILP2@gmail.com'. The 'Voice call' option is selected. The user is prompted to enter their phone number to receive a verification code via voice call. The 'Country' is set to 'United States'. There are input fields for 'Phone number' (with a '+1' prefix) and 'Extension'. A blue button labeled 'Receive a code via voice call' is prominent. There are also links for 'Return to authenticator list' and 'Back to sign in'.</p>	 <p>The screenshot shows the 'Set up phone authentication' page for the user 'okta.ford@illinois.gov'. The user is prompted to enter the verification code received during the phone call. A text input field is provided for the code, and a blue 'Verify' button is below it. There are also links for 'Return to authenticator list' and 'Back to sign in'.</p>

Option IV: Voice Call Authentication

Step 4

User Action:

When successful user is returned to setup additional Security Methods. Since user setup phone using SMS it is also automatically available for voice call. User can click Set up later or preferably setup additional methods.



Set up security methods

 okta.ford@illinois.gov

Security methods help protect your Okta account by ensuring only you have access.

Set up optional



Google Authenticator

Enter a temporary code generated from the Google Authenticator app. Used for access

[Set up](#)



Okta Verify

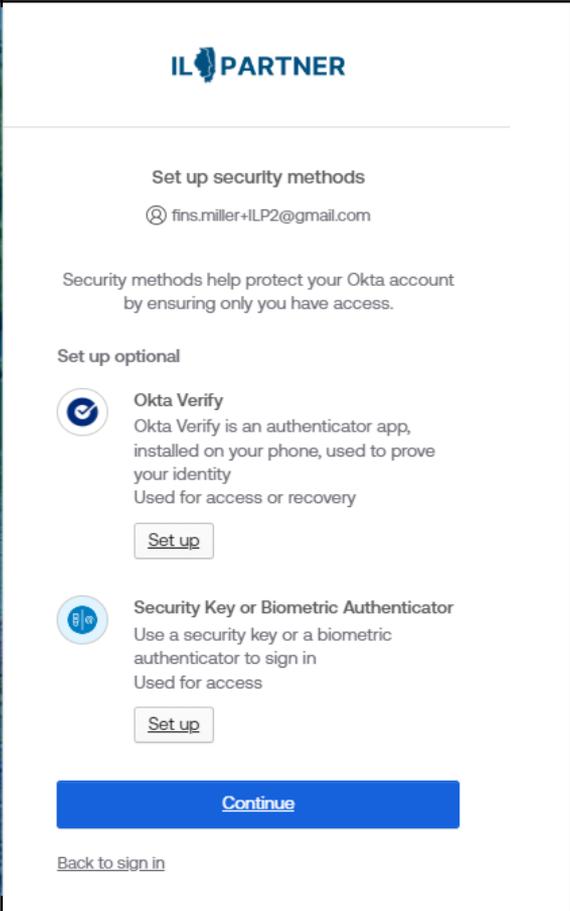
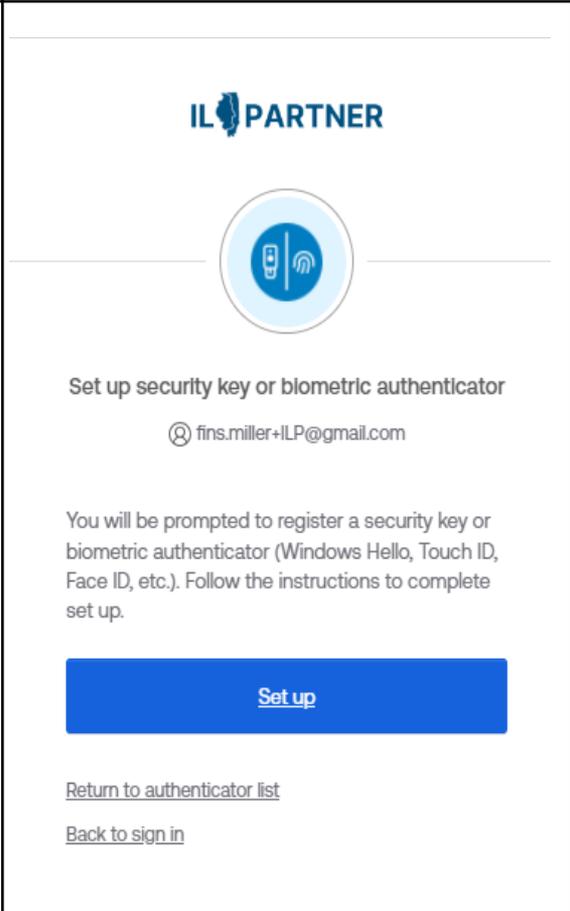
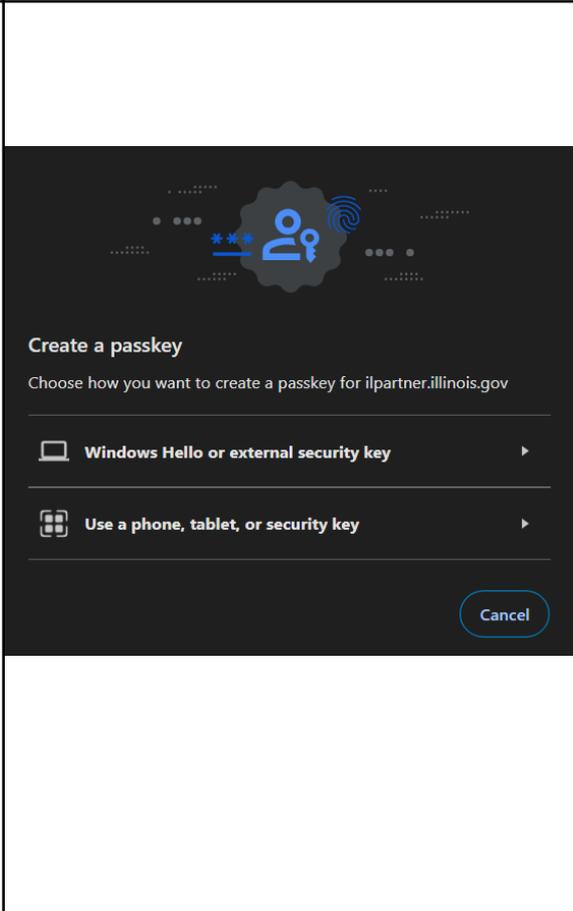
Okta Verify is an authenticator app, installed on your phone, used to prove your identity. Used for access

[Set up](#)

[Set up later](#)

[Back to sign in](#)

Option V: Security Key or Biometric Authenticator

Step 1	Step 2	Step 3
<p>User Action: Select Security Key or Biometric authenticator Setup button</p>	<p>User Action: Click Setup; Then depending on the type key or authenticator you have</p>	<p>User Action: Select the proper option and follow instructions for your passkey.</p>
 <p>IL PARTNER</p> <p>Set up security methods</p> <p>fins.miller+ILP2@gmail.com</p> <p>Security methods help protect your Okta account by ensuring only you have access.</p> <p>Set up optional</p> <ul style="list-style-type: none"> Okta Verify Okta Verify is an authenticator app, installed on your phone, used to prove your identity Used for access or recovery Set up Security Key or Biometric Authenticator Use a security key or a biometric authenticator to sign in Used for access Set up <p>Continue</p> <p>Back to sign in</p>	 <p>IL PARTNER</p> <p>Set up security key or biometric authenticator</p> <p>fins.miller+ILP2@gmail.com</p> <p>You will be prompted to register a security key or biometric authenticator (Windows Hello, Touch ID, Face ID, etc.). Follow the instructions to complete set up.</p> <p>Set up</p> <p>Return to authenticator list</p> <p>Back to sign in</p>	 <p>Create a passkey</p> <p>Choose how you want to create a passkey for ilpartner.illinois.gov</p> <ul style="list-style-type: none"> Windows Hello or external security key Use a phone, tablet, or security key <p>Cancel</p>

4. Logout of ILPartner

Your list of available applications will be visible in the form of icons aka chiclets within the ILPartner user dashboard. Sample below.

Your account is now setup, and you can access an available app, logout from ILPartner (or) you can just close the *Google Chrome* browser window. Or the current browser you are using.

Note: you may be taken directly into the State Agency app you were provided access to and not the ILPartner User dashboard.

The screenshot displays the ILPartner user dashboard. At the top left is the ILPARTNER logo. A search bar labeled "Search your apps" is positioned at the top center. On the top right, there is an "Admin" button and the user's name "Rona illinoi". The left sidebar contains navigation options: "My Apps" (selected), "Work", "Add section", "Notifications" (with a 1 notification icon), and "Add apps". The main content area features a "Trust this account in the Okta browser plugin" notification with a close button and a link to "Need help?". Below this is the "My Apps" section, which includes a "Work" filter and a "Sort" dropdown. Five application icons are shown: "Agency Application Admin Portal", "Okta Workflows", "HFS Clinical Request Platform ...", "DoIT Customer Billing Portal (CBP)", and "DPH - LLCS Training". Each icon has a three-dot menu icon in the top right corner. At the bottom of the main content area is an "Add section" button.

5. ILPartner account Settings:

You can make additions, changes or adjustments to your ILPartner Account after initial setup from your User Dashboard. <https://ilpartner.illinois.gov/>

Click your name in the upper right corner and then click on **Settings**.

The screenshot shows the ILPartner user dashboard. On the left is a navigation sidebar with 'My Apps', 'Notifications', and 'Add apps'. The main content area is divided into three sections: 'Personal Information', 'Display Language', and 'Security Methods'. The 'Personal Information' section shows fields for First name (Owen), Last name (Miller), Okta username (fms.miller+LP2@gmail.com), Primary email (fms.miller+LP2@gmail.com), Secondary email, and Mobile phone. The 'Display Language' section shows the current language is English, with a note that the default language is set by the browser. The 'Security Methods' section lists various authentication methods: Password (with a Reset button), Okta Verify (with a Set up button), Security Key or Biometric Authenticator (with Set up another and Remove buttons), Google Authenticator (with a Remove button), and Phone (+1 XXX-XXX-6043, with Set up another and Remove buttons). At the bottom, there is an 'End All Sessions' section with a Sign out button. The top of the dashboard includes the ILPARTNER logo and a search bar for apps. The bottom left corner indicates 'Last sign in: a few seconds ago'.

You can make changes to or add (Optional):

- Change or Add MFA Verifications
- Reset Password
- Add Secondary Email
- Change your Language