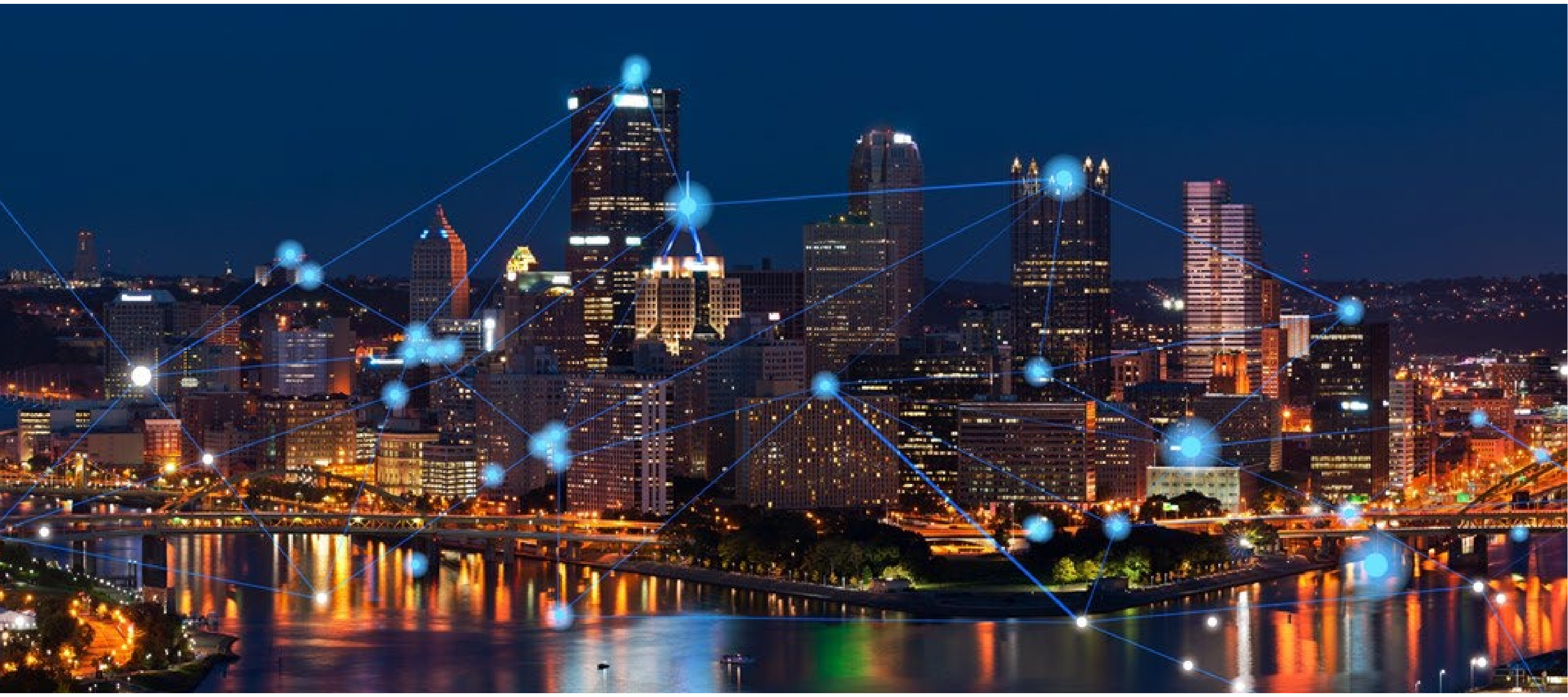


Cybersecurity and Infrastructure Security Agency (CISA) Repository for Software Attestations and Artifacts (RSAA) User Guide

Publication: March 2024
Cybersecurity and Infrastructure Security Agency

Table of Contents

PURPOSE

OMB issued memorandum M-22-18 on 14 September 2022. Due to the importance and scope of the Federal Government's information and communications technology (ICT) products and services, Memorandum 22-18 was drafted to ensure software integrity. Software integrity is key to protecting Federal systems from nation state and criminal actors seeking to disrupt our nation's critical functions. The goal is to reduce overall risk from cyber-attacks. One way to achieve this is by Federal agencies only using software from software producers who can attest to complying with the Government-specified secure software development practices, as described in the NIST Guidance.

Following the issuance of M-22-18, on 09 June 2023, OMB issued memorandum M-23-16. OMB Memorandum M-23-16 reinforces the requirements established in M-22-18, reaffirms the importance of secure software development practices, and extends the timelines for agencies to collect attestations from software producers. Additionally, this memorandum provides supplemental guidance on the scope of M-22-18's requirements and on agencies' use of Plan of Actions and Milestones (POA&Ms) when a software producer cannot provide the required attestation but plans to do so. To the extent any provision of this memorandum may be read to conflict with any provision of M-22-18, this memorandum is controlling.

The Repository for Software Attestation and Artifacts (RSAA) serves to satisfy the requirements set forth in M-22-18 and M-23-16.

INTRODUCTION

The RSAA User Guide provides users with instructions to create an RSAA account, the required CISA Okta Partner Platform account with multifactor authentication (MFA) and use the RSAA application effectively. The RSAA application serves as a repository for all software producers' Attestations.

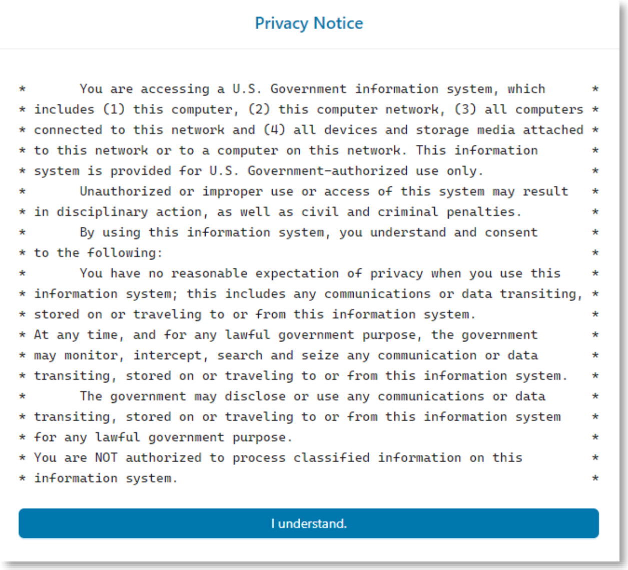
The Secure Software Development Attestation Form may be found at Secure Software Development Attestation Form | CISA. This site provides a link to download the Self Attestation Common Form that must be completed and uploaded in pdf form. This Self-Attestation form identifies the minimum secure software development requirements a software producer must meet, and attest to meeting, before software subject to the requirements of M-22-18 and M-23-16 may be used by Federal agencies. This form is used by software producers to attest that the software is developed in conformity with specified secure software development practices.

CREATE A USER ACCOUNT

Step 1. Navigate to https://softwaresecurity.cisa.gov.

Please Note: The CISA RSAA Application performs best using Edge or Chrome browsers.

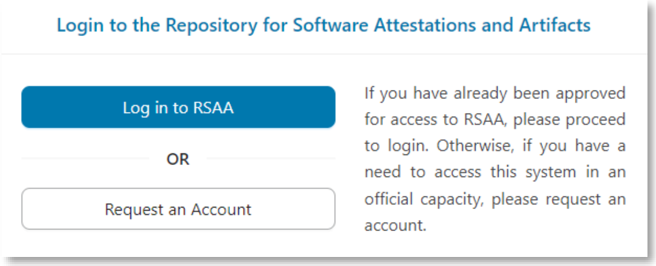
Step 2. Read the Access Warning and Authorization Disclaimer. Click “I Understand” to proceed.



Privacy Notice

```
*       You are accessing a U.S. Government information system, which      *
* includes (1) this computer, (2) this computer network, (3) all computers *
* connected to this network and (4) all devices and storage media attached *
* to this network or to a computer on this network. This information       *
* system is provided for U.S. Government-authorized use only.              *
*       Unauthorized or improper use or access of this system may result   *
* in disciplinary action, as well as civil and criminal penalties.         *
*       By using this information system, you understand and consent       *
* to the following:                                                        *
*       You have no reasonable expectation of privacy when you use this    *
* information system; this includes any communications or data transiting, *
* stored on or traveling to or from this information system.               *
* At any time, and for any lawful government purpose, the government       *
* may monitor, intercept, search and seize any communication or data       *
* transiting, stored on or traveling to or from this information system.   *
*       The government may disclose or use any communications or data      *
* transiting, stored on or traveling to or from this information system    *
* for any lawful government purpose.                                       *
* You are NOT authorized to process classified information on this         *
* information system.                                                      *
```

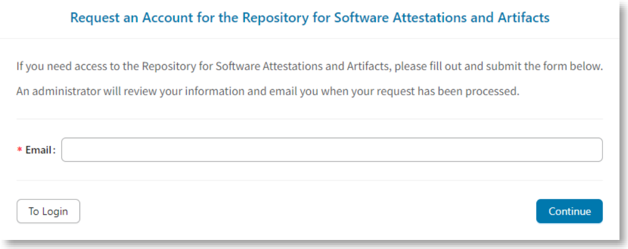
Step 3. The RSAA login prompt will appear. Click on “Request an Account.”



Login to the Repository for Software Attestations and Artifacts

If you have already been approved for access to RSAA, please proceed to login. Otherwise, if you have a need to access this system in an official capacity, please request an account.

Step 4. Enter the requestor email address and click “Continue.”

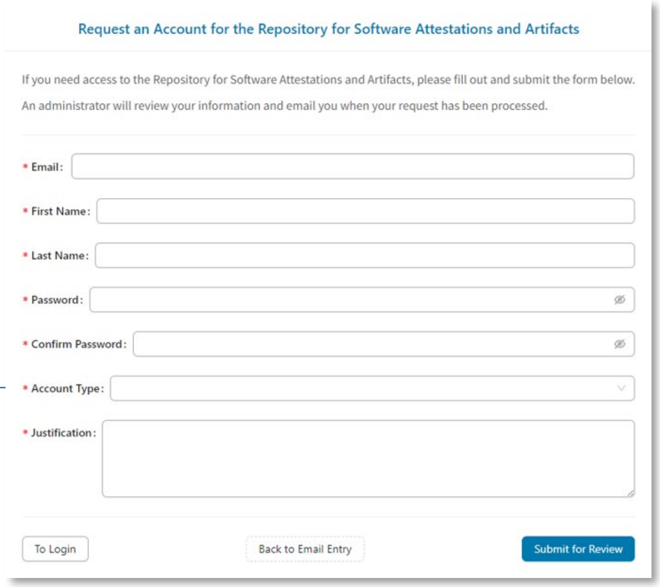


Request an Account for the Repository for Software Attestations and Artifacts

If you need access to the Repository for Software Attestations and Artifacts, please fill out and submit the form below. An administrator will review your information and email you when your request has been processed.

* Email:

Step 5. Complete the Request for Account. Populate the required personal information: Enter First Name, Last Name, and mandatory fields.



Request an Account for the Repository for Software Attestations and Artifacts

If you need access to the Repository for Software Attestations and Artifacts, please fill out and submit the form below. An administrator will review your information and email you when your request has been processed.

* Email:

* First Name:

* Last Name:

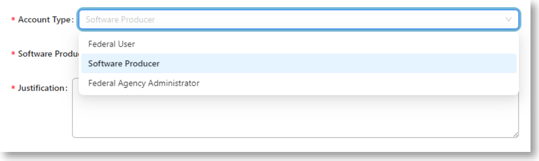
* Password:

* Confirm Password:

* Account Type:

* Justification:

Select the account type from the “Account Type” drop-down menu. Reference Table 1 CISA RSAA User Role Guidance for guidance on which role to select.



* Account Type: Software Producer

* Software Produ

* Justification:

Account Type Guidance:

Account Type	Description	General Permission
Federal User	Federal users for a specific agency	Can add or modify content for their own agency and can view content from any agency.
Software Producer	Software Producers	Allows for a software producer to submit records, attestations, and artifacts.
Federal Agency Administrator	Federal agency administrative user for a specific agency	Can create, manage, and assign agency users to agency records, attestations, and artifacts. Can add or modify content for all agency records and artifacts.

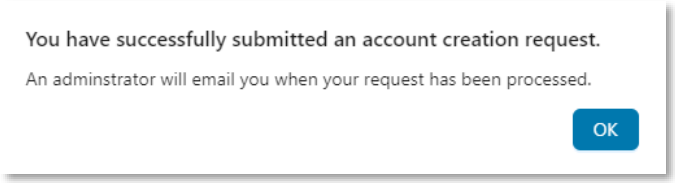
Table 1 CISA RSAA User Role Guidance

Step 6. Once the account type is selected, a new drop-down menu will appear to select from. This selection associates the requestor with the agency or organization being represented. If the appropriate agency or organization is not listed, please skip to Step 9.

a. If **Federal User** is selected, select the applicable federal agency from the drop-down.
b. If **Software Producer** is selected, select the applicable software producer organization from the drop-down.
c. If **Federal Agency Administrator** is selected, select the applicable federal agency.

Step 7. Enter the justification for requestor access. If a federal user, the justification may be to manage the agency's records and view all Attestations. If a software producer, it may be to register and upload software Attestations and/or artifacts. If a Federal Agency Administrator, the justification may be to manage Attestation records for the agency.

Step 8. Click "Submit for Review." A notification will appear confirming the account creation request has been successfully submitted. Click "OK" to complete the process. Account requests are reviewed and processed within approximately 2 business days. Upon processing, an email is sent to the requestor to notify that the account has been created.



You have successfully submitted an account creation request.

An adminstrator will email you when your request has been processed.

IMPORTANT - Upon RSAA account approval, an email notification will be sent to the requestor from the CISA Okta Partner Platform. For instructions on setting up the required Okta account and multifactor authentication (MFA), please refer to **Appendix A**.

Step 9. If the organization or agency being represented does not appear in the drop-down lists or options presented, please contact the CISA Technology Operations Center (TOC) to request the missing organization or agency be added to the CISA RSAA system:

CISA Technology Operations Center
(202) 771-CISA (2472)
TOC@mail.cisa.dhs.gov

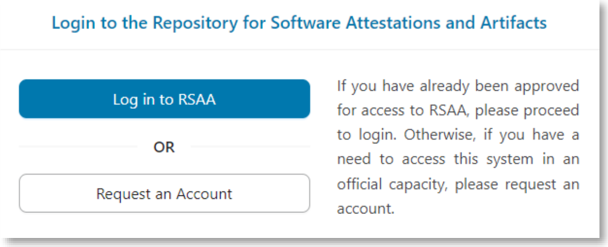
CREATE A SOFTWARE RECORD

With an RSAA account created AND activation of the CISA Okta Partner Portal account with MFA, registered users may create software record(s) for the agency or organization. Each record is specific to the software product and version(s). Registered users may also search existing software records, subject to the user privileges.

Step 1. Navigate to [https://softwaresecurity.cisa.gov.](https://softwaresecurity.cisa.gov)

Please note – the approval of the RSAA account alone will not allow a user to login to the RSAA application. Before attempting, please be sure to have the CISA Okta Partner Platform account and MFA configured.

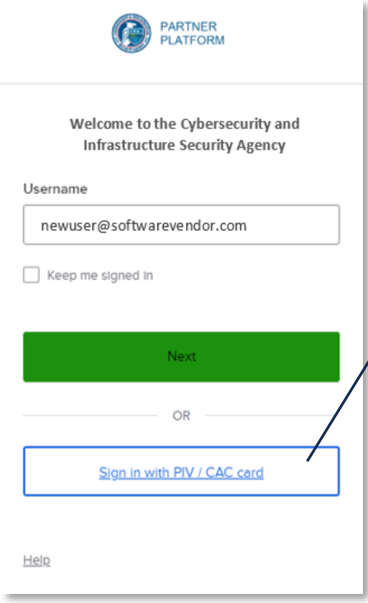
Step 2. Click on “Log in to RSAA.”



Login to the Repository for Software Attestations and Artifacts

If you have already been approved for access to RSAA, please proceed to login. Otherwise, if you have a need to access this system in an official capacity, please request an account.

Step 3. Login with the registered email as the Username and click “Next.” This will launch the Login.gov screen used by the CISA Okta Partner Platform. The PIV/CAC option is for *.cisa.dhs.gov accounts only.



Welcome to the Cybersecurity and Infrastructure Security Agency

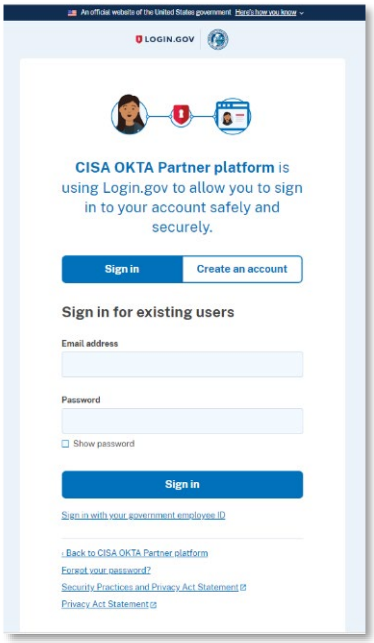
Username: newuser@softwarevendor.com

□ Keep me signed in

Important

Non *.cisa.dhs.gov accounts will not be able to sign in with PIV and will need to use email, Google Authenticator, Microsoft Authenticator, or Okta Verify for MFA.

Step 4. Login to the CISA Okta Partner Platform with the registered email address and password set up when configuring the Okta account (Appendix A).



An official website of the United States government Here's how you know
LOGIN.GOV

CISA OKTA Partner platform is using Login.gov to allow you to sign in to your account safely and securely.

Sign in
Create an account

Sign in for existing users

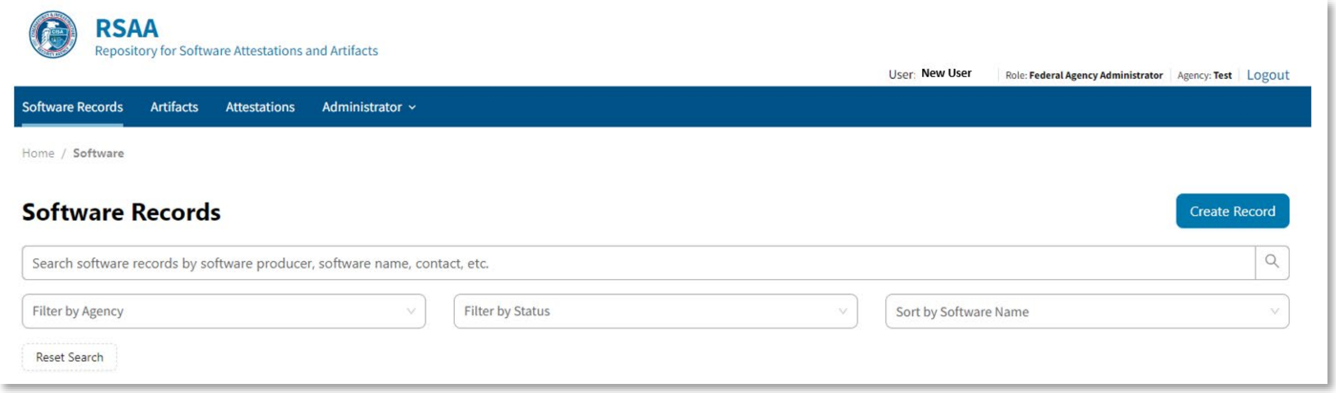
Email address

Password

□ Show password

Sign in
Sign in with your government employee ID
‹ Back to CISA OKTA Partner platform
Forgot your password?
Security Practices and Privacy Act Statement
Privacy Act Statement

Step 5. Upon login, the RSAA landing page is launched. To create a new software record, click the “Create Record" button. Software records may also be searched here, filterable by Agency, status, or software name.

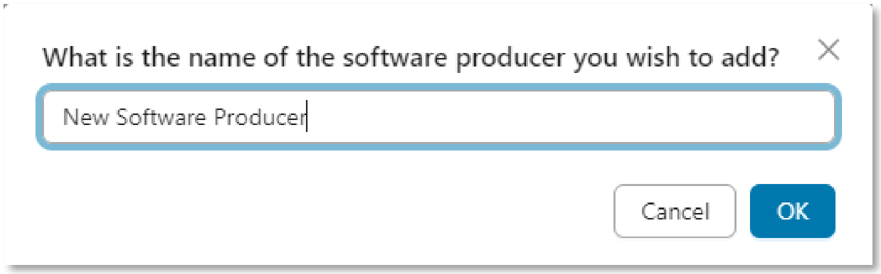


User: New User | Role: Federal Agency Administrator | Agency: Test | Logout

Software Records

Step 6. If creating a new software record, complete the required fields in the Create Software Record form which displays and identifies required data for the submission:

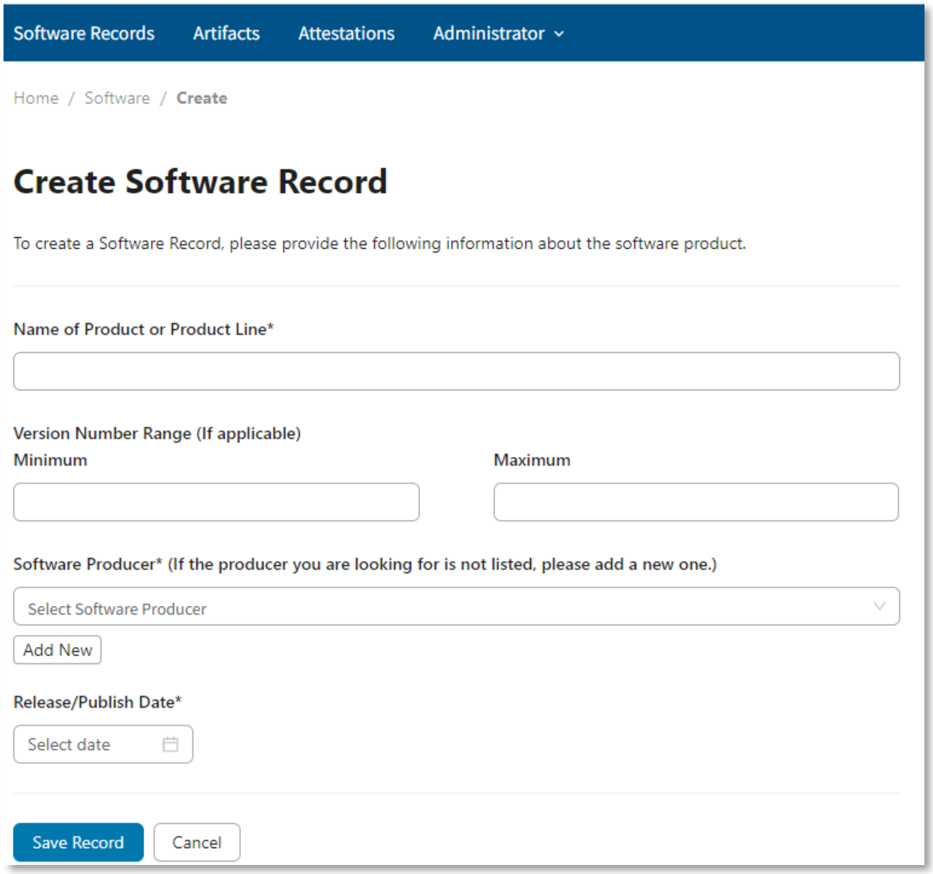
a. Populate the Name of Product or Product Line field.
b. Enter the Version Number Range (if applicable).
c. Enter the software producer entity. If the software producer is not registered in the system, Click the "Add New" option, and when prompted, enter the software producer entity, and click "OK." The entity will now be available to enter in the software producer field of the Create Software Record form.



What is the name of the software producer you wish to add?

New Software Producer

d. Enter the Release/Publish Date.
e. Click "Save Record."



Create Software Record

To create a Software Record, please provide the following information about the software product.

Name of Product or Product Line*

Version Number Range (If applicable)

Minimum

Maximum

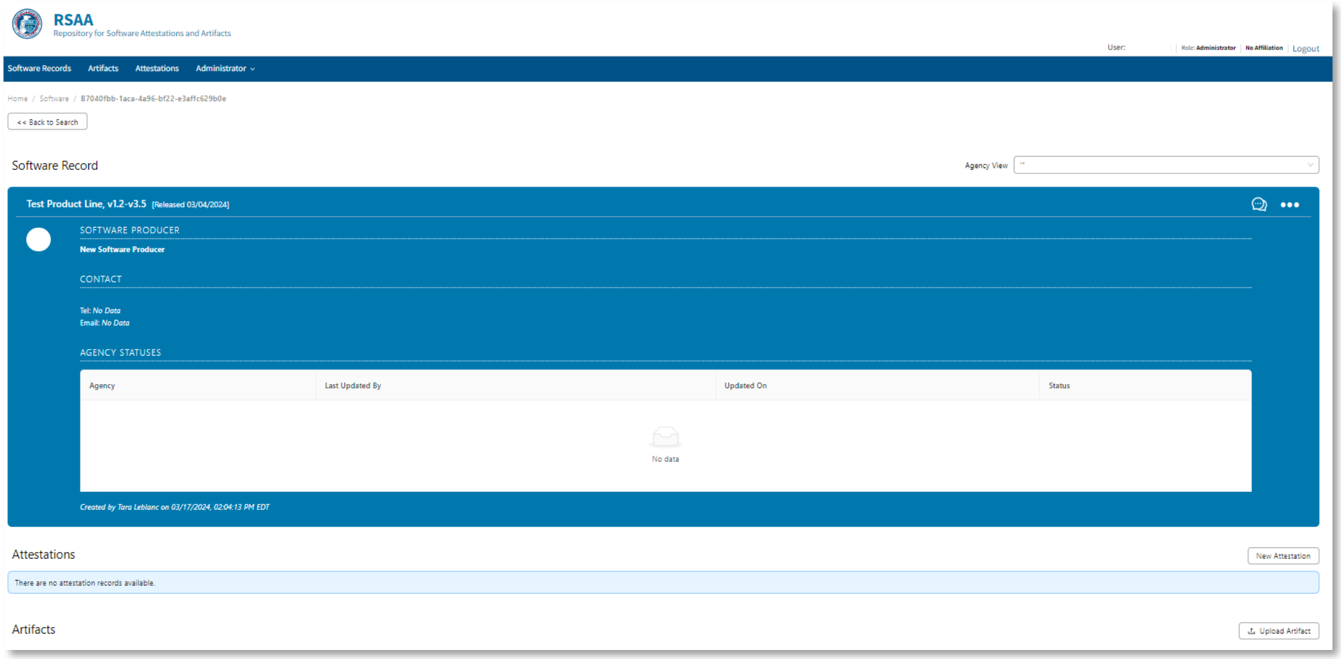
Software Producer* (If the producer you are looking for is not listed, please add a new one.)

Select Software Producer

Release/Publish Date*

Select date

Step 7. The Software Record appears with the information provided. From this form, the software record may be associated with an agency, attached to an existing attestation, or edit the record or record contact information. A new attestation may be initiated by clicking on "New Attestation" and artifacts may be uploaded using the "Upload Artifact" feature.



Software Record

Test Product Line, v1.2-v3.5 [Released 03/04/2024]

SOFTWARE PRODUCER

New Software Producer

CONTACT

Tel: *No Data*
Email: *No Data*

AGENCY STATUSES

Agency	Last Updated By	Updated On	Status

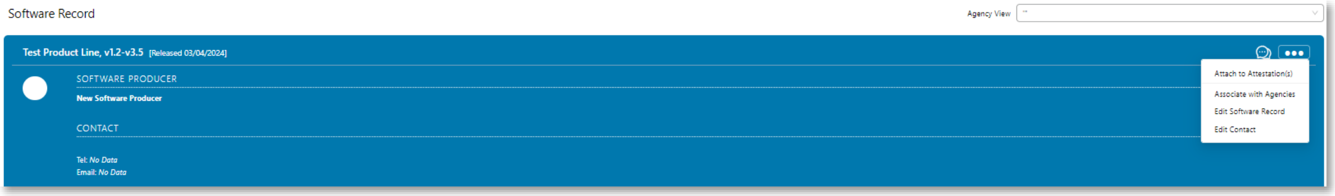
Created by Tara Leblanc on 03/17/2024, 02:04:13 PM EDT

Attestations

There are no attestation records available.

Artifacts

Within the software record, click on the three dots to present the drop down to attach the record to Attestation(s), Associate the record with Agencies, edit the software record, or edit the contact information.



Software Record

Test Product Line, v1.2-v3.5 [Released 03/04/2024]

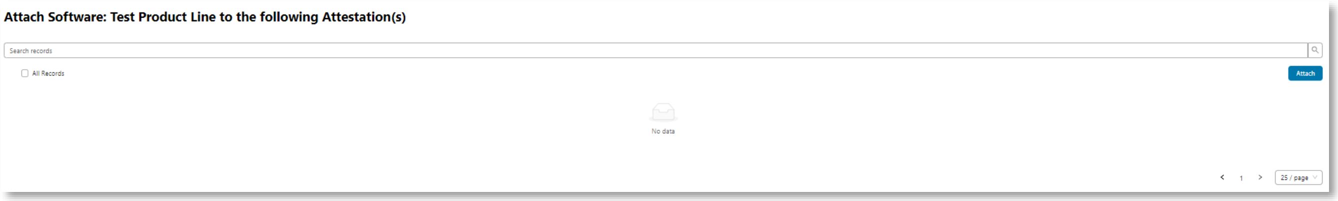
SOFTWARE PRODUCER

New Software Producer

CONTACT

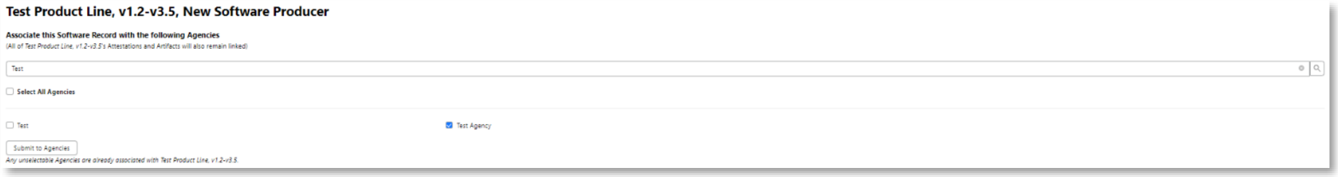
Tel: *No Data*
Email: *No Data*

If the appropriate Attestation has already been uploaded, select "Attach to Attestion(s) from the drop-down menu." Search for the Attestation(s), click on the appropriate record(s) and click on "Attach."



Attach Software: Test Product Line to the following Attestation(s)

To associate the software record with an Agency, select "Associate with Agencies" from the drop-down menu, search for or select the appropriate Agency, and click on "Submit to Agencies." The record will update.



Test Product Line, v1.2-v3.5, New Software Producer

Associate this Software Record with the following Agencies
(All of *Test Product Line, v1.2-v3.5*'s Attestations and Artifacts will also remain linked)

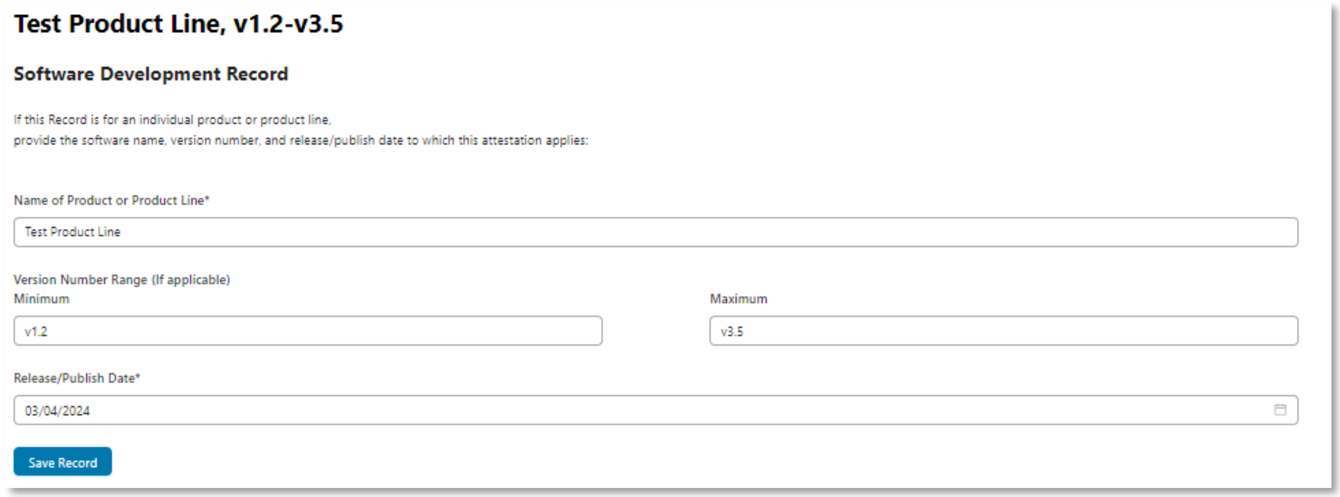
Test

□ Select All Agencies

□ Test ☑ Test Agency

Any unselectable Agencies are already associated with Test Product Line, v1.2-v3.5.

To edit the software record, select "Edit Software Record" from the drop-down menu, edit the record, and click on "Save Record."



Test Product Line, v1.2-v3.5

Software Development Record

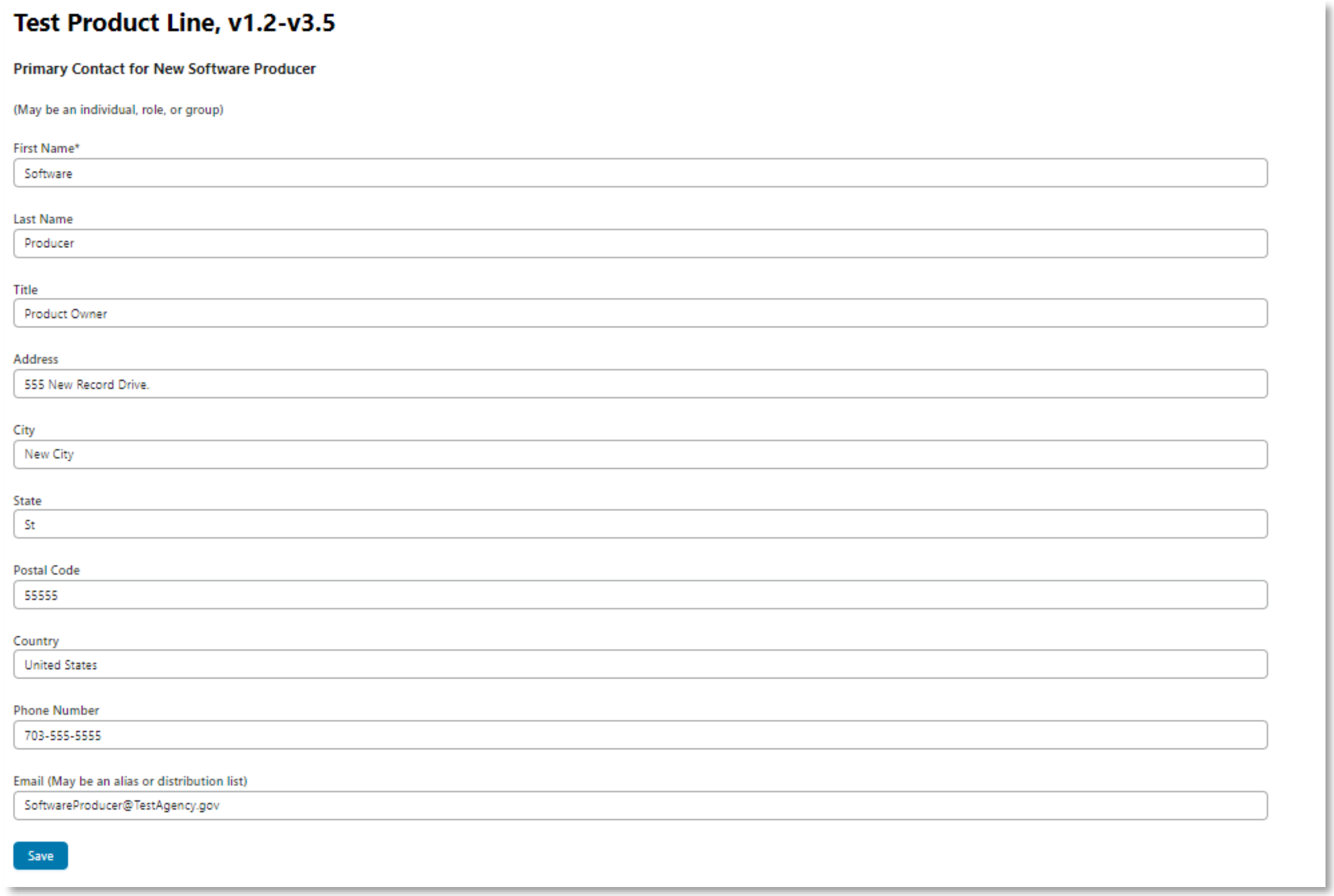
If this Record is for an individual product or product line,
provide the software name, version number, and release/publish date to which this attestation applies:

Name of Product or Product Line*: Test Product Line

Version Number Range (If applicable)
Minimum: v1.2
Maximum: v3.5

Release/Publish Date*: 03/04/2024

To edit the contact information for the software record, select "Edit Contact" from the drop-down menu, populate or edit the contact information, and click "Save."



Test Product Line, v1.2-v3.5

Primary Contact for New Software Producer

(May be an individual, role, or group)

First Name*: Software

Last Name: Producer

Title: Product Owner

Address: 555 New Record Drive.

City: New City

State: St

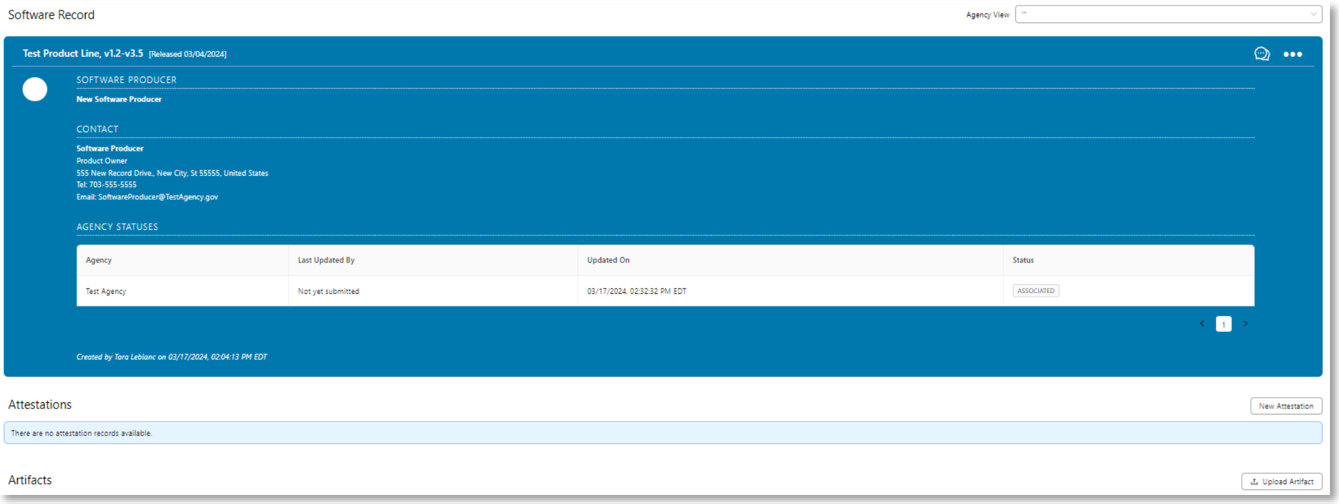
Postal Code: 55555

Country: United States

Phone Number: 703-555-5555

Email (May be an alias or distribution list): SoftwareProducer@TestAgency.gov

The software record should then reflect all associations and edits:



Test Product Line, v1.2-v3.5 [Released 03/04/2024]

SOFTWARE PRODUCER

New Software Producer

CONTACT

Software Producer
Product Owner
555 New Record Drive., New City, St 55555, United States
Tel: 703-555-5555
Email: SoftwareProducer@TestAgency.gov

AGENCY STATUSES

Agency	Last Updated By	Updated On	Status
Test Agency	Not yet submitted	03/17/2024, 02:32:32 PM EDT	ASSOCIATED

Created by Tara Leblanc on 03/17/2024, 02:04:13 PM EDT

Attestations

There are no attestation records available.

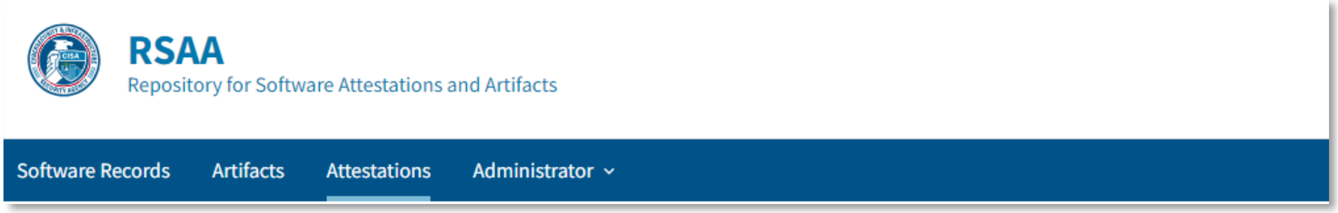
Artifacts

A new Attestation and any artifacts may be uploaded from within this form or follow the instructions in the Create and Upload an Attestation section.

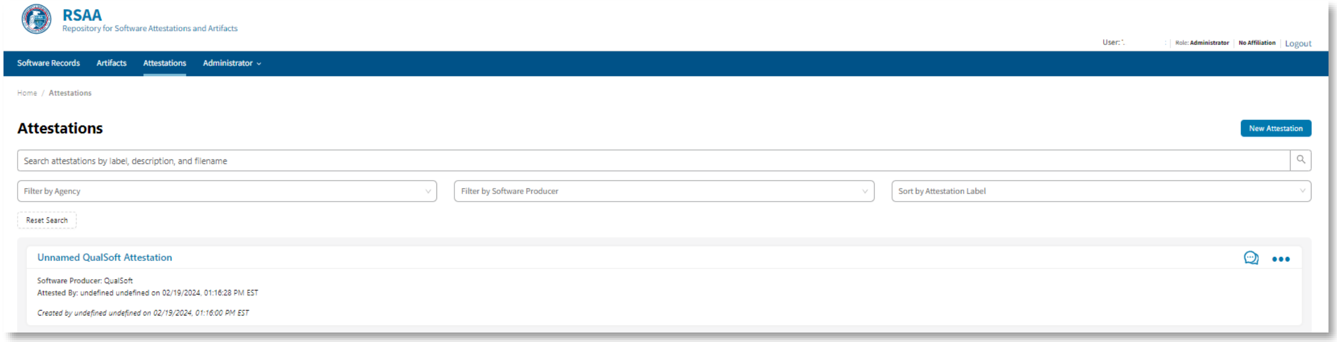
CREATE AND UPLOAD AN ATTESTATION

A completed Self Attestation Common Form must be uploaded and associated with software record(s). The Self Attestation Common Form includes instructions on how to complete the form. The instructions for uploading a new Attestation applicable to an individual software record, or all software records by a given organization follow.

Step 1. From the RSAA landing page, select "Attestations."



All existing Attestations viewable by the registered user will be listed. Attestations are also searchable using the search and filter features as the top of the form. If search results do not return any records, click on "Reset Search" to try other search criteria. Search instructions may also be found in the Find an Attestation section.



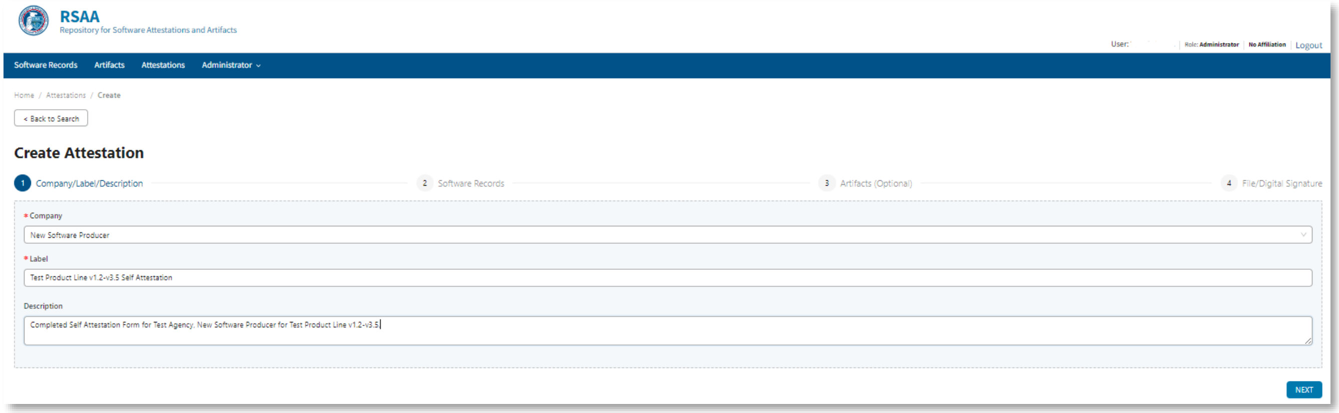
Attestations

Unnamed QualSoft Attestation

Software Producer: QualSoft
Attested By: undefined undefined on 02/19/2024, 01:16:28 PM EST

Created by undefined undefined on 02/19/2024, 01:16:00 PM EST

Step 2: Click on "New Attestation" to launch the Create Attestation form.



Create Attestation

* Company: New Software Producer

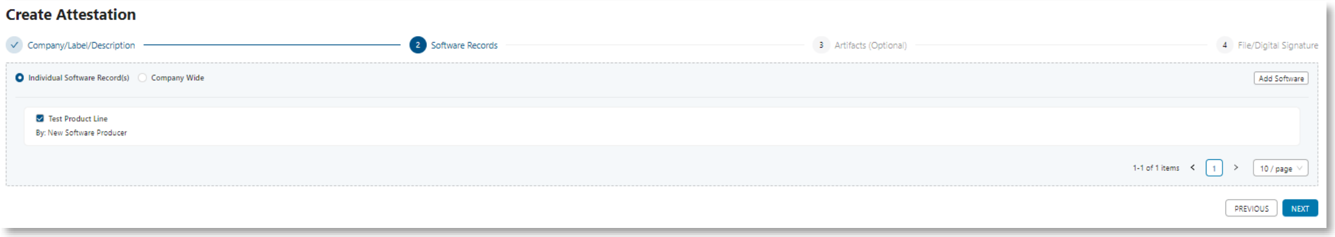
* Label: Test Product Line v1.2-v3.5 Self Attestation

Description: Completed Self Attestation Form for Test Agency, New Software Producer for Test Product Line v1.2-v3.5

Step 3. Complete the required fields in the Create Attestation form:

a. Select the Company from the drop-down menu.
b. Enter the Attestation title in the "Label" field.
c. Enter a document Description.
d. Click "Next."

Step 4. Choose and click either "Individual Software Record" or "Company Wide." If creating an Attestation for an individual software record, select "Individual Software Record" and click on the record from the list. Click on "Next."

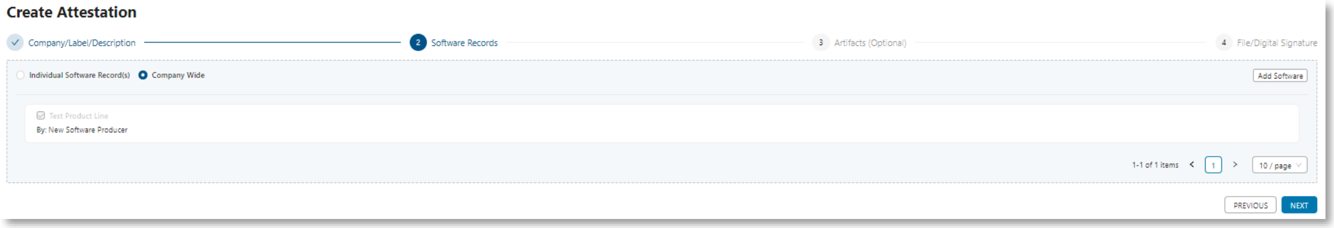


Create Attestation

● Individual Software Record(s) ○ Company Wide

☑ Test Product Line
By: New Software Producer

If creating an Attestion for all records for a Company (Agency or Organization), select "Company Wide." Click "Next."

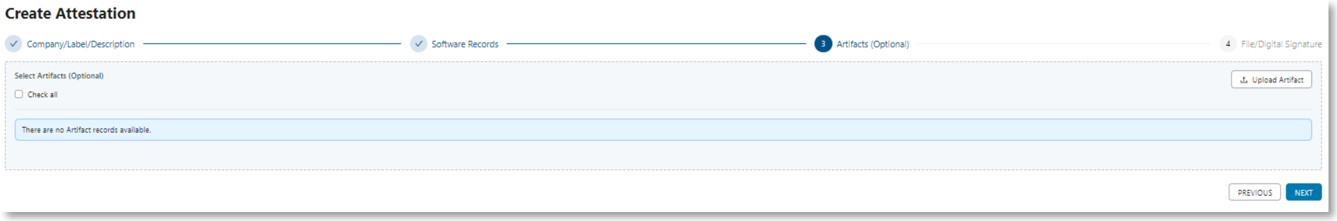


Create Attestation

○ Individual Software Record(s) ● Company Wide

☑ Test Product Line
By: New Software Producer

Step 5: The next screen supports the option to select any previously uploaded or upload any new Artifacts. Artifacts may include documentation supporting the Attestation or affiliation of the registered user with the Agency or Organization. This step is optional. **Please note - this is NOT where the Self Attestation Form is uploaded.** Click "Next."



Create Attestation

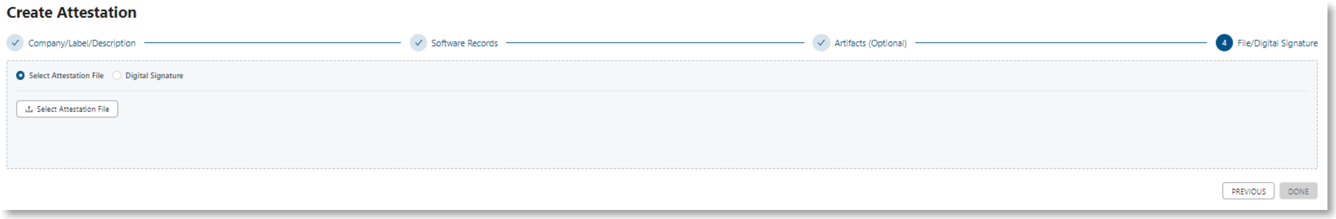
Select Artifacts (Optional)

□ Check all

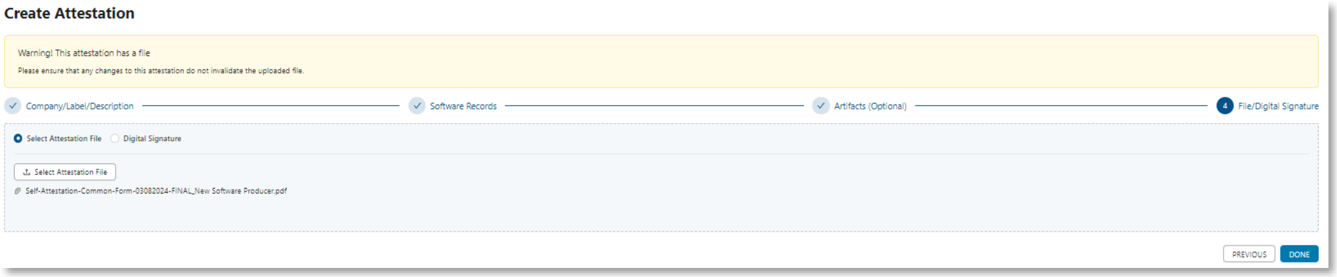
There are no Artifact records available.

Step 6: The Create Attestation form will appear. Upload an attestation file by clicking on "Select Attestation File."

The Secure Software Development Attestation Form may be found at [Secure Software Development Attestation Form | CISA](). This site provides a link to download the Self Attestation Common Form that must be completed and uploaded in pdf form.



Once the file is uploaded, a warning message appears to ensure any changes to the Attestation do not invalidate the completed and uploaded Self Attestation Common Form. The uploaded file will appear under the “select Attestation File” option. Click “Done.”



Warning! This attestation has a file

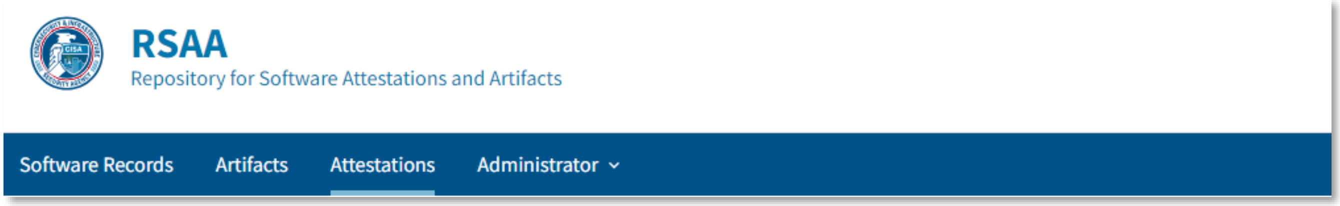
Please ensure that any changes to this attestation do not invalidate the uploaded file.

Self-Attestation-Common-Form-03082024-FINAL_New Software Producer.pdf

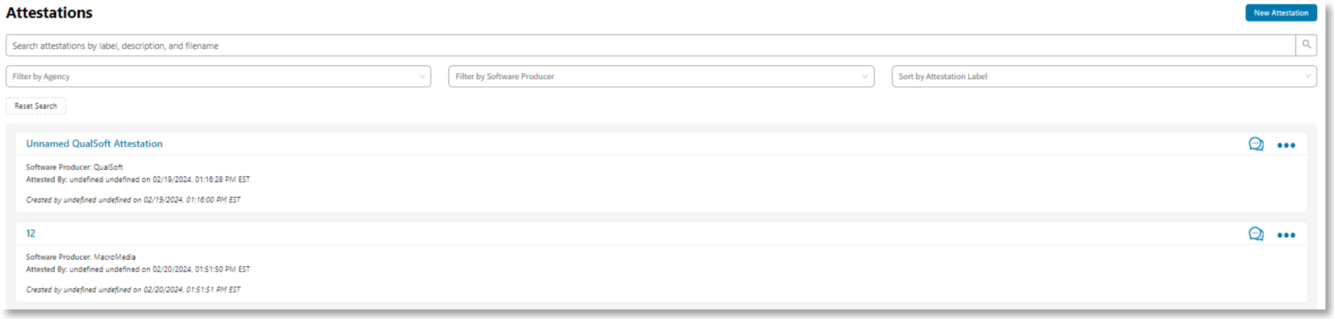
FIND AN ATTESTATION

The RSAA application includes a feature to search or find an Attestation by Label, description, or filename. Alternatively, results may be filtered by software producer or sorted by Attestation Label.

Step 1: From the RSAA landing page, select “Attestations’ from the banner.



Step 2: Scroll down and select the desired Attestation or utilize the search function to search for the desired attestation by label, description, and/or filename. Press “enter” or click on the magnifying glass icon to initiate the search. The “Filter by Software Producer” or “Sort by Attestation Label” selection boxes are optional.


Attestations
New Attestation
Search attestations by label, description, and filename
Filter by Agency
Filter by Software Producer
Sort by Attestation Label
Reset Search

Unnamed QualSoft Attestation

Software Producer: QualSoft
Attested By: undefined undefined on 02/19/2024, 01:16:28 PM EST

Created by undefined undefined on 02/19/2024, 01:16:00 PM EST

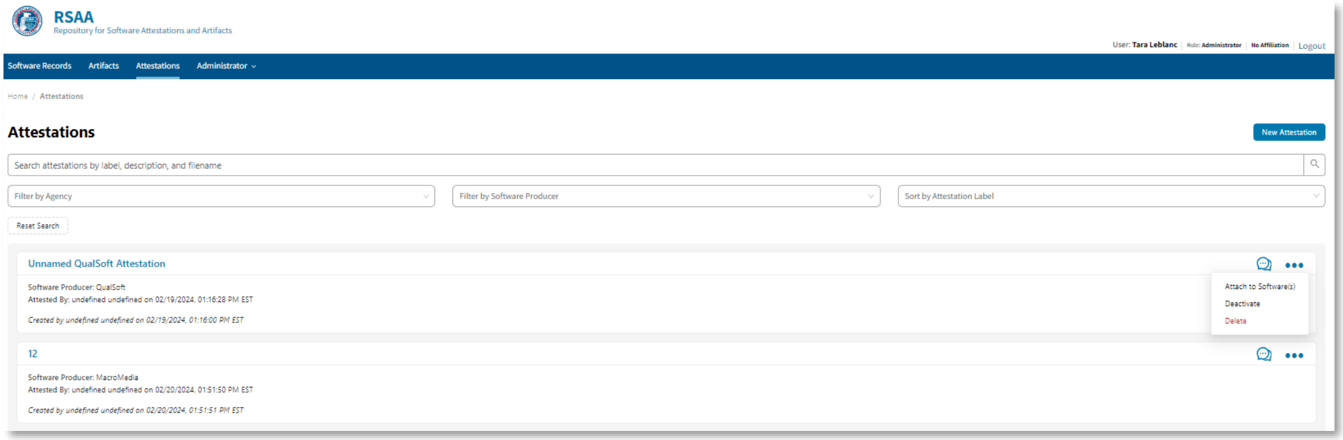
12

Software Producer: MacroMedia
Attested By: undefined undefined on 02/20/2024, 01:51:50 PM EST

Created by undefined undefined on 02/20/2024, 01:51:51 PM EST

ASSOCIATE AN ATTESTATION WITH SOFTWARE

Step 1: Highlight the desired Attestation and press the three dots in the upper right corner. From the resulting drop-down menu, select “Attach to Software(s).”



Attestations

Unnamed QualSoft Attestation

Software Producer: QualSoft
Attested By: undefined undefined on 02/19/2024, 01:16:28 PM EST

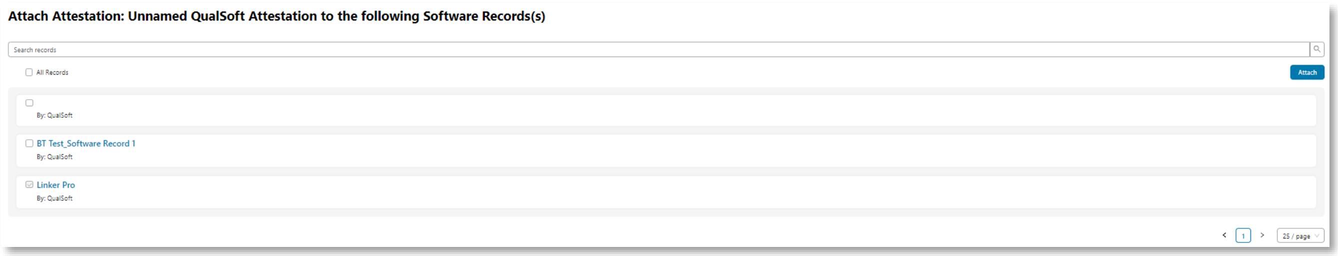
Created by undefined undefined on 02/19/2024, 01:16:00 PM EST

12

Software Producer: MacroMedia
Attested By: undefined undefined on 02/20/2024, 01:51:50 PM EST

Created by undefined undefined on 02/20/2024, 01:51:51 PM EST

Step 2: Select the “All Records” check box or select specific software(s) individually. Click on “Attach” to complete the task.



Attach Attestation: Unnamed QualSoft Attestation to the following Software Records(s)

☐ All Records

☐
By: QualSoft

☐ BT Test_Software Record 1
By: QualSoft

☑ Linker Pro
By: QualSoft

If any issues are encountered while using the RSAA application, please contact the CISA Technology Operations Center for support:

CISA Technology Operations Center
(202) 771-CISA (2472)
TOC@mail.cisa.dhs.gov

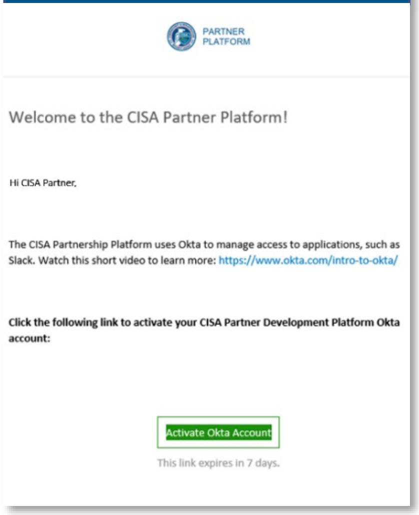
APPENDIX A: CISA OKTA PARTNER PLATFORM LOGIN INSTRUCTIONS

All accounts use email address for authenticating via the CISA Partner Authentication Service. Registered external Accounts received an activation email to initiate authentication and setup of Microsoft or Google Authenticate, or the Okta Verify Mobile App for multi-factor authentication (MFA).

STEP 1

CISA Partner Authentication - Activation Email: Users will receive an Okta activation email from Okta noreply@okta.com with the subject line "Welcome to the CISA Partner Platform." This includes guidance to set up your password and Multi-factor Authentication.

Users have **7 days** to activate the CISA Partner Authentication account. Begin by clicking on "Activate Okta Account."



Welcome to the CISA Partner Platform!

Hi CISA Partner,

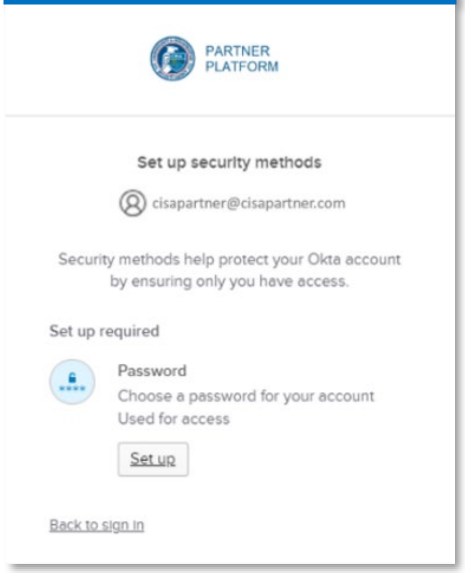
The CISA Partnership Platform uses Okta to manage access to applications, such as Slack. Watch this short video to learn more: https://www.okta.com/intro-to-okta/

Click the following link to activate your CISA Partner Development Platform Okta account:

This link expires in 7 days.

STEP 2

CISA Partner Platform User Setup: Upon activation of the Okta account, users will be prompted to set up a password. To begin, click "Set up."



Set up security methods

cisapartner@cisapartner.com

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

Set up required

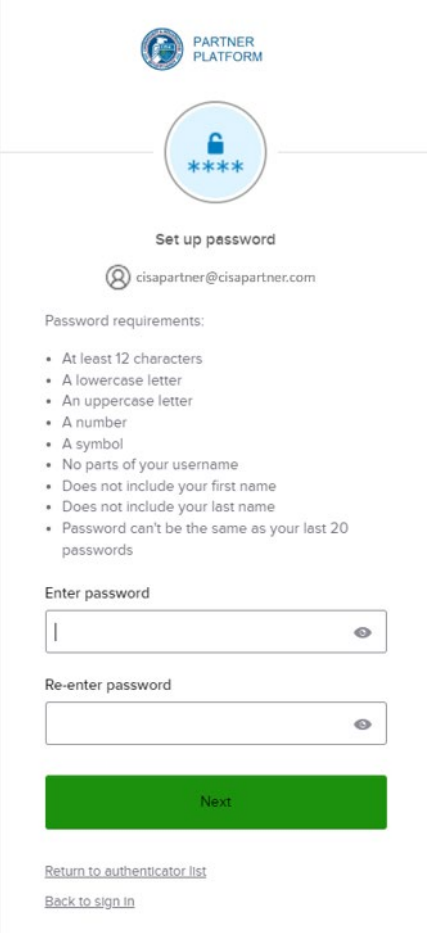
Password

Choose a password for your account

Used for access

STEP 3

Set up a password: Create a password adhering to the password criteria and click "Next."



Set up password

cisapartner@cisapartner.com

Password requirements:

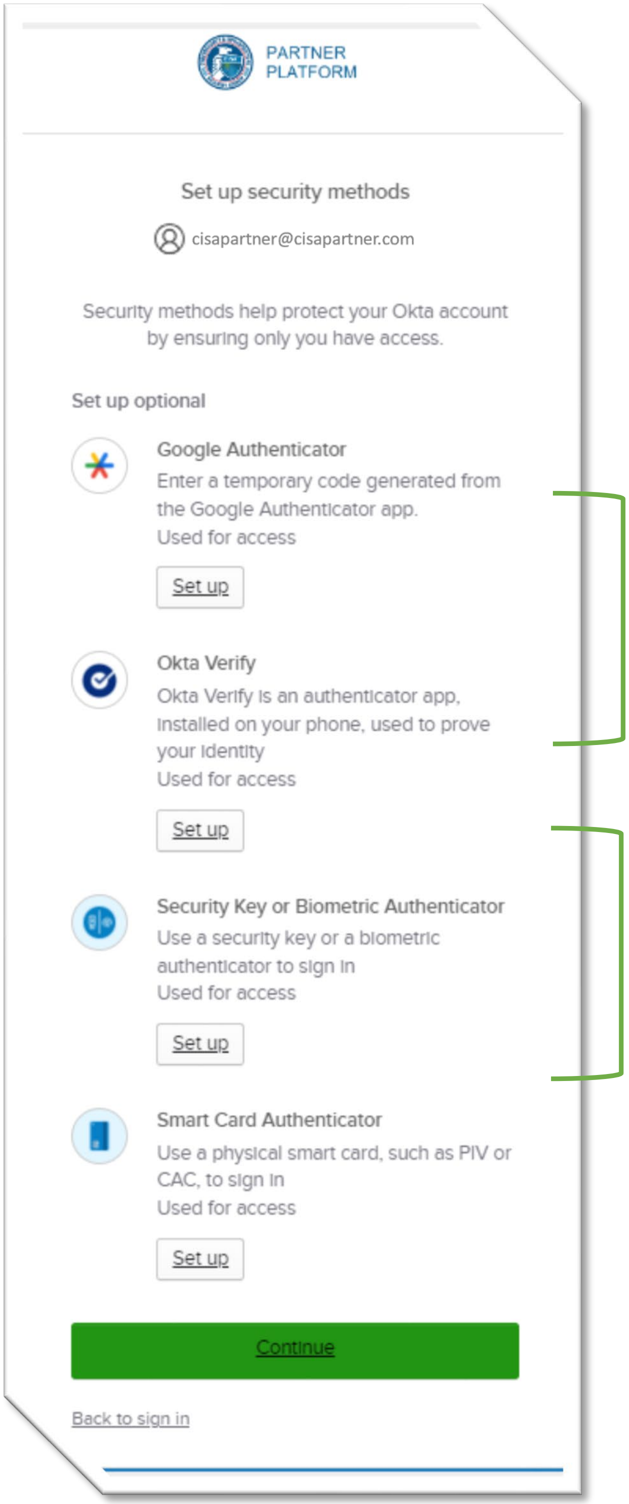
- At least 12 characters
- A lowercase letter
- An uppercase letter
- A number
- A symbol
- No parts of your username
- Does not include your first name
- Does not include your last name
- Password can't be the same as your last 20 passwords

Enter password

Re-enter password

Set up Multi-factor Authentication:

STEP 4



PARTNER PLATFORM

Set up security methods

cisapartner@cisapartner.com

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

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

Security Key or Biometric Authenticator
Use a security key or a biometric authenticator to sign in
Used for access

Smart Card Authenticator
Use a physical smart card, such as PIV or CAC, to sign in
Used for access

If you experience any problems with the CISA Okta Account Activation process, please contact the TOC at TOC@mail.cisa.dhs.gov, or call 202-771-2472

Multi-factor Authentication Method: While there are multiple methods available, CISA recommends using Google Authenticator (select this same option to setup Microsoft Authenticator if using Microsoft) or Okta Verify, in that order of preference.

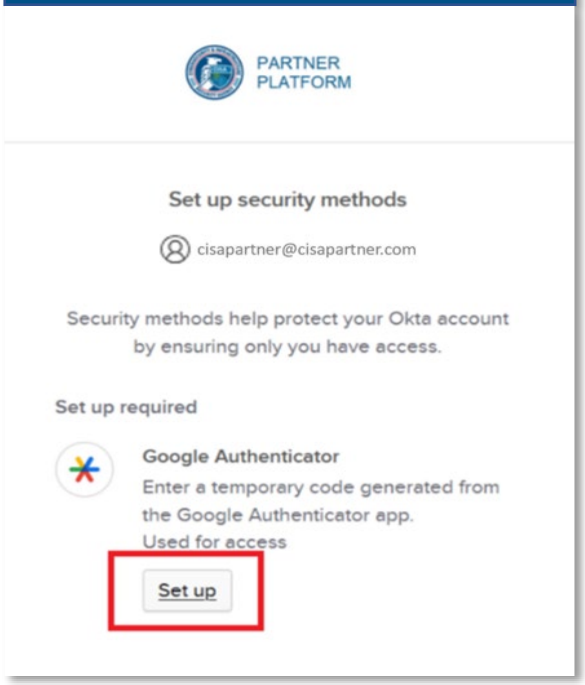
These methods are not yet supported within the CISA Partner Platform.

Steps 5-14 walk through configuring **Google or Microsoft Authenticator** and **Steps 15-X** guide the user on setting up **Okta Verify**, depending on user preference.

Adding Google or Microsoft Authenticator:

STEP 5

From the Okta login screen, under Google Authenticator, select “Set Up.”


PARTNER PLATFORM

Set up security methods

cisapartner@cisapartner.com

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

Set up required

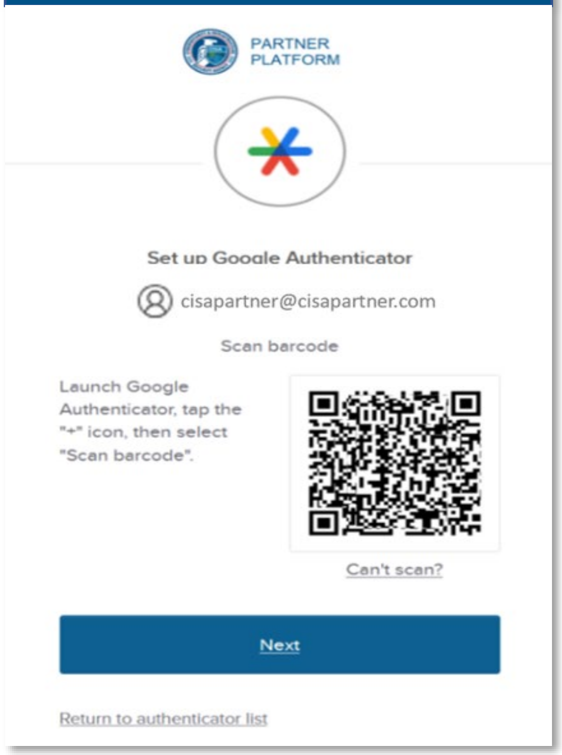
Google Authenticator

Enter a temporary code generated from the Google Authenticator app.

Used for access

STEP 6

Setup Google Authenticator.


PARTNER PLATFORM

Set up Google Authenticator

cisapartner@cisapartner.com

Scan barcode

Launch Google Authenticator, tap the "+" icon, then select "Scan barcode".

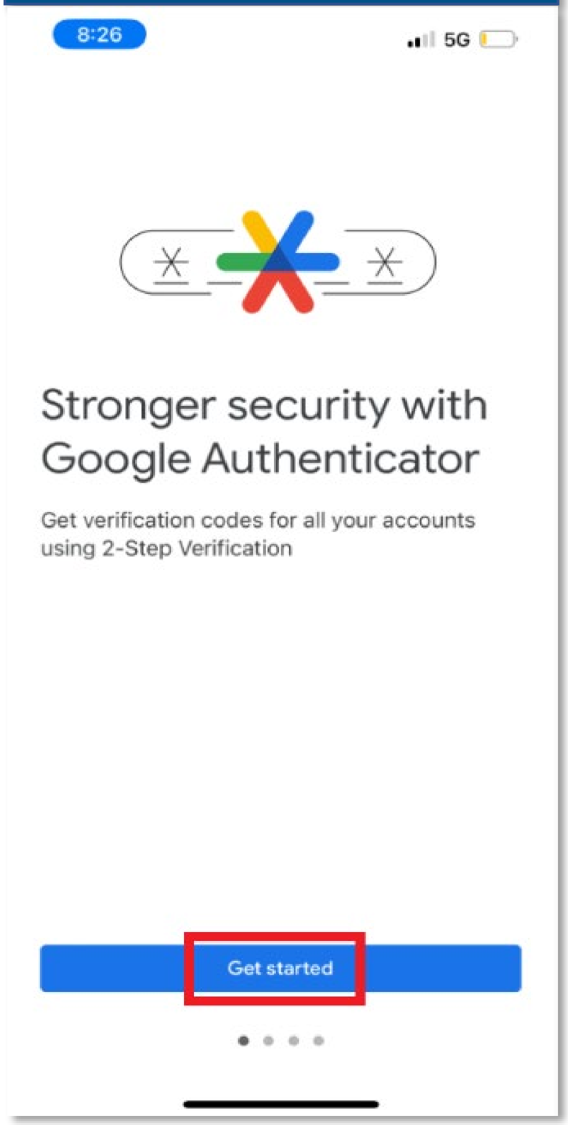
STEP 7

Install Google Authenticator on Mobile Device

- **iOS** App Installation
  - Go to the **App Store on iOS device** and follow instructions to install Google Authenticator. [Google Authenticator on the App Store (Apple.com)] or
  - [Microsoft Authenticator on the App Store (Apple.com)]
- **Android** App Installation
  - Go to **Google Play on Android device** and follow instructions to install Google Authenticator. [Google Authenticator - Apps on Google Play] or
  - [Microsoft Authenticator – Apps on Google Play]

STEP 8

After installing Google Authenticator, select "Get Started."

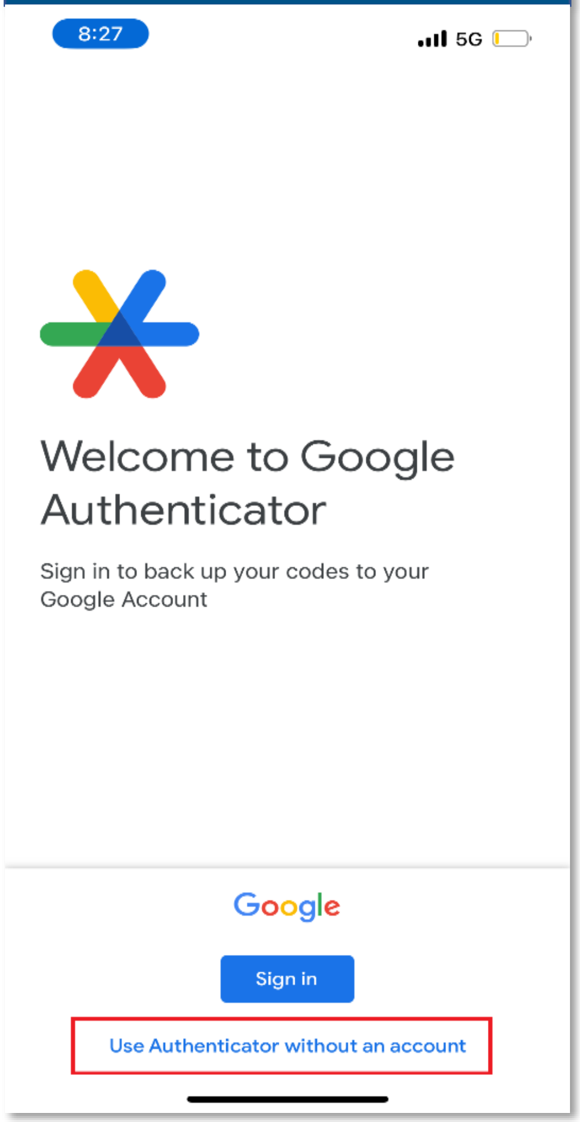


Stronger security with Google Authenticator

Get verification codes for all your accounts using 2-Step Verification

STEP 9

Select "Use Authenticator without an Account" if presented with the option below:

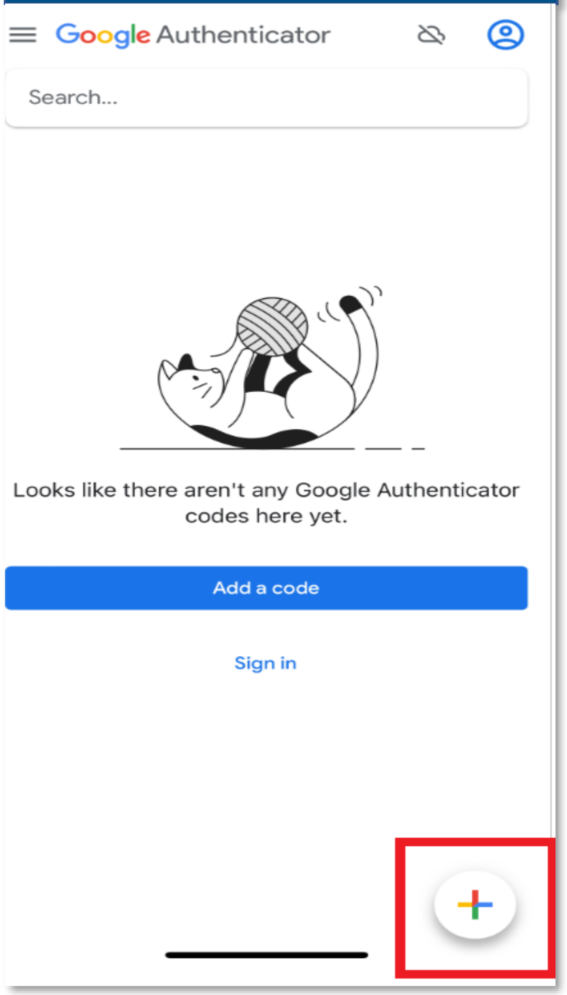


Welcome to Google Authenticator

Sign in to back up your codes to your Google Account

STEP 10

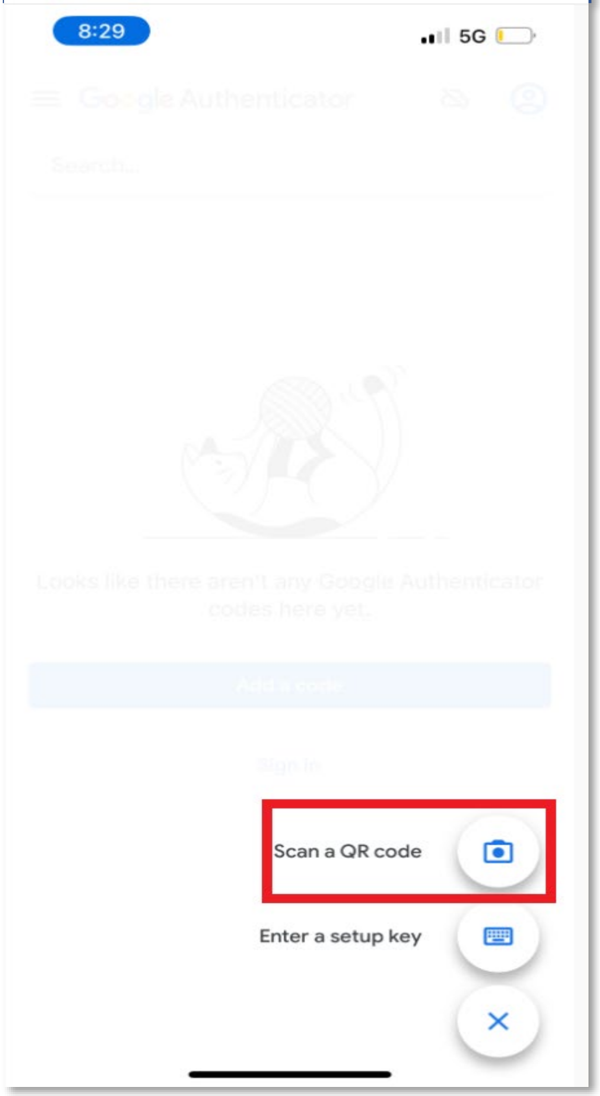
Select the “+” button to add an Account.



Looks like there aren't any Google Authenticator codes here yet.

STEP 11

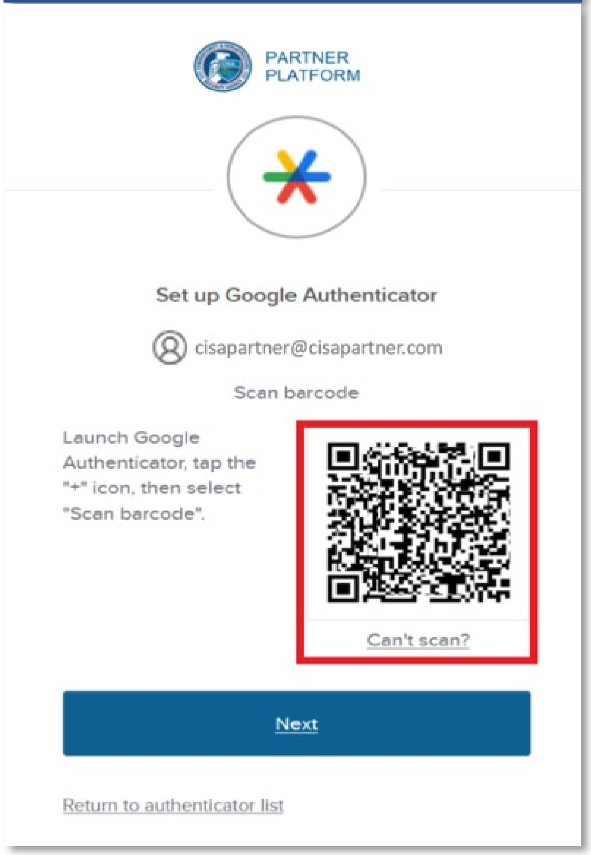
Select icon of the camera named “Scan a QR Code.”



Looks like there aren't any Google Authenticator codes here yet.

STEP 12

Capture the QR Code displayed on Okta screen with the mobile device camera.



PARTNER PLATFORM

Set up Google Authenticator

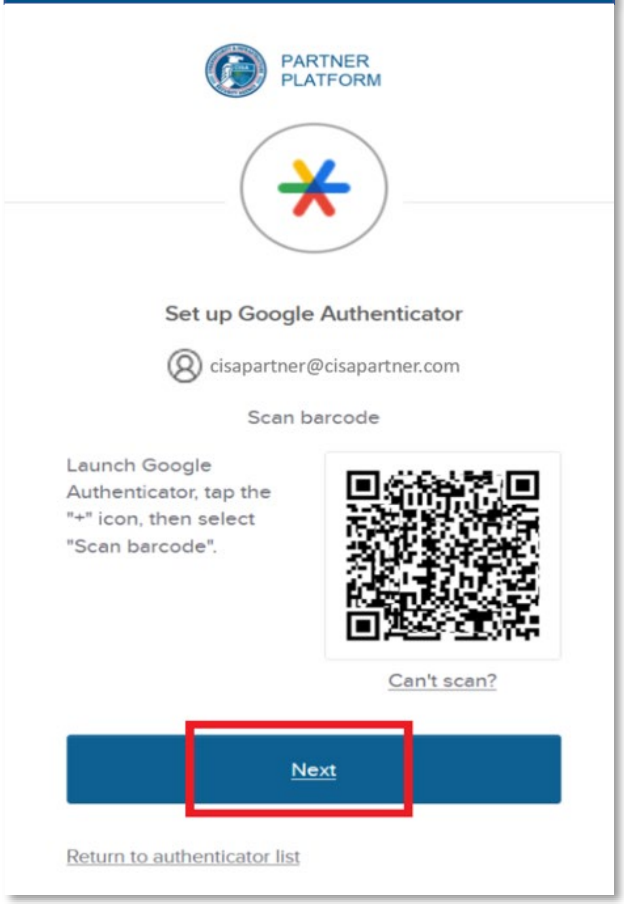
cisapartner@cisapartner.com

Scan barcode

Launch Google Authenticator, tap the "+" icon, then select "Scan barcode".

STEP 13

Select “Next” when presented with the Okta Screen after capturing the QR code presented.



PARTNER PLATFORM

Set up Google Authenticator

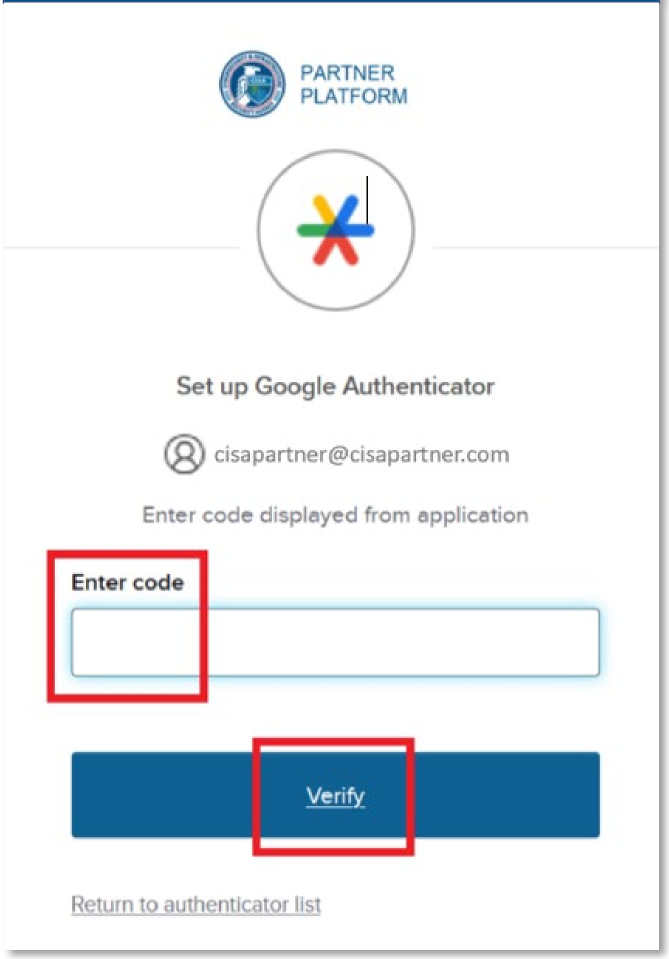
cisapartner@cisapartner.com

Scan barcode

Launch Google Authenticator, tap the "+" icon, then select "Scan barcode".

STEP 14

Enter a 6-digit Code presented from the App and select “Verify.” After this is done, Google Authenticator will be completely Successful and Verified.



PARTNER PLATFORM

Set up Google Authenticator

cisapartner@cisapartner.com

Enter code displayed from application

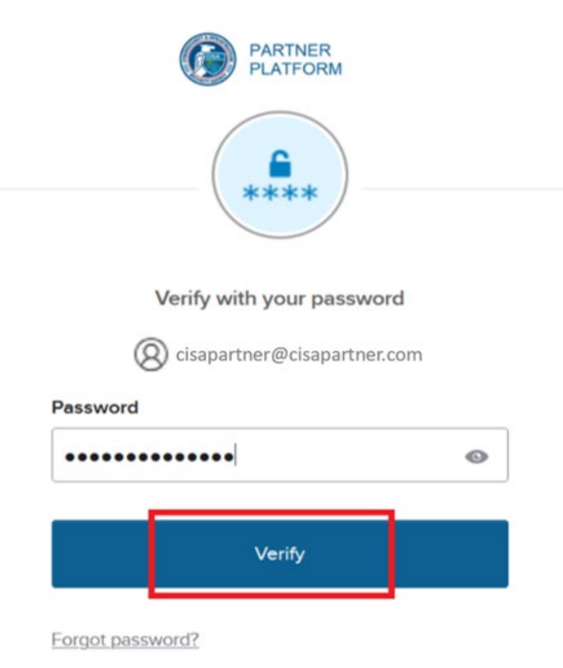
Enter code

This concludes the Google Authenticator setup. If preferred, the Okta Verify option for multi-factor authentication set up is described in steps 15-26.

Adding Okta Verify:

STEP 15

Select the Okta Verify "Set Up" button:



PARTNER PLATFORM

Verify with your password

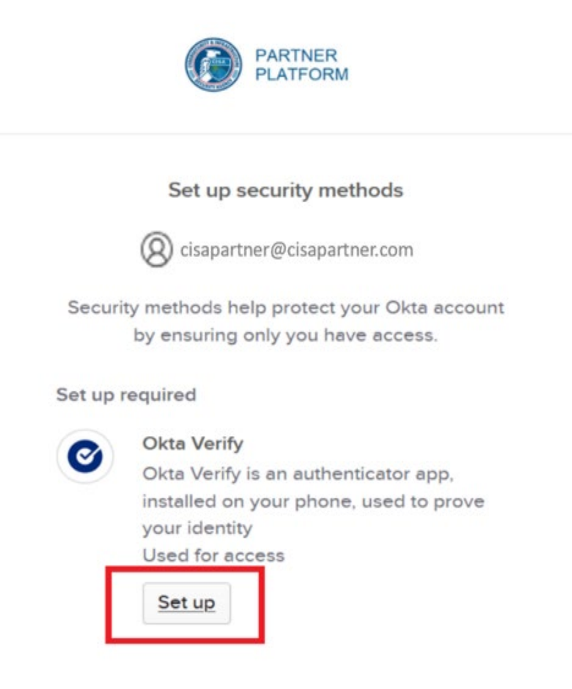
cisapartner@cisapartner.com

Password

••••••••••••••

STEP 16

Verify Identity before adding an authenticator. Provide an acceptable combination of credentials. Then Select "Set Up" in Okta Verify.



PARTNER PLATFORM

Set up security methods

cisapartner@cisapartner.com

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

Set up required

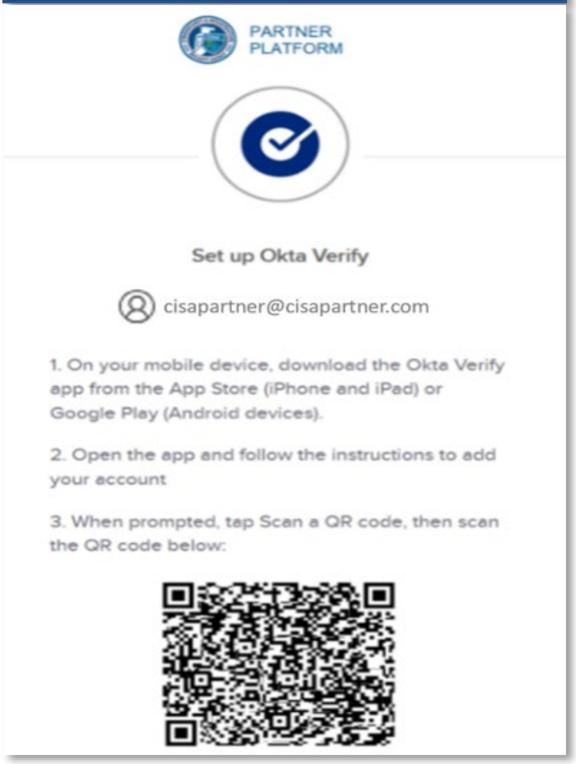
Okta Verify

Okta Verify is an authenticator app, installed on your phone, used to prove your identity

Used for access

STEP 17

The below prompt will display to initiate the install.



PARTNER PLATFORM

Set up Okta Verify

cisapartner@cisapartner.com

1. On your mobile device, download the Okta Verify app from the App Store (iPhone and iPad) or Google Play (Android devices).

2. Open the app and follow the instructions to add your account

3. When prompted, tap Scan a QR code, then scan the QR code below:

STEP 18

Install Okta Verify on Mobile Device

iOS App Installation

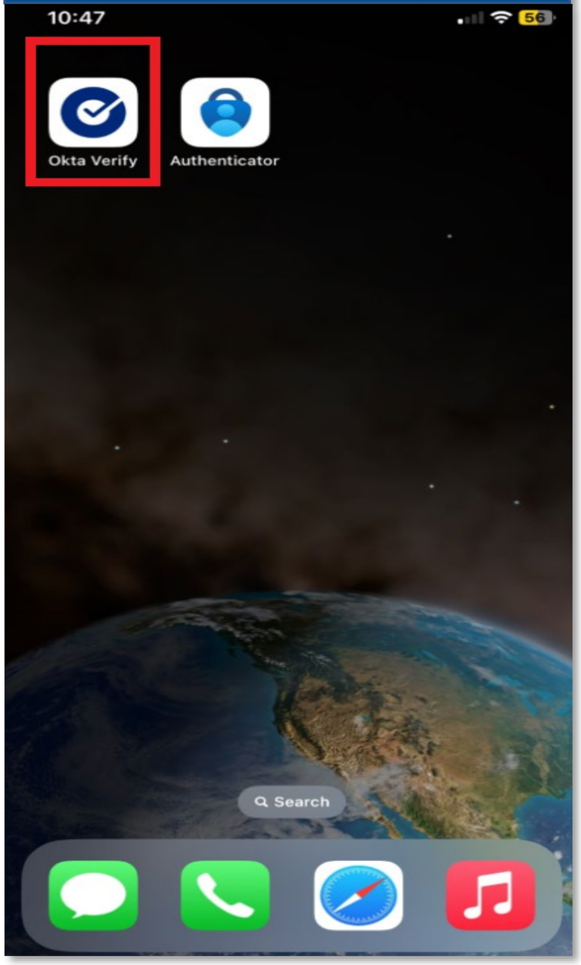
- Go to the **App Store on iOS device** and follow instructions to install Okta Verify. Okta Verify on the App Store (apple.com)

Android App Installation

- Go to **Google Play on Android device** and follow instructions to install Okta Verify. Okta Verify - Apps on Google Play

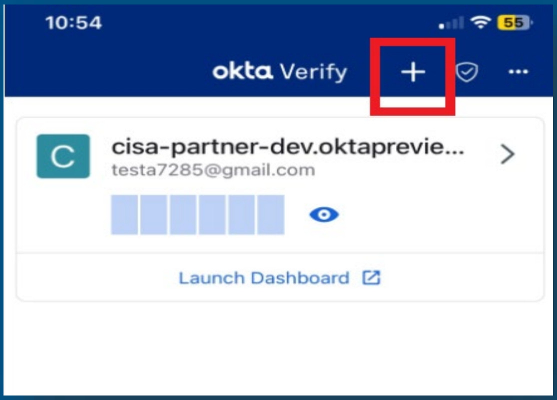
STEP 19

Open Okta Verify on the mobile device, e.g., iOS Mobile:



STEP 20

Add Account to Okta Verity. One of the two screens below will be presented.

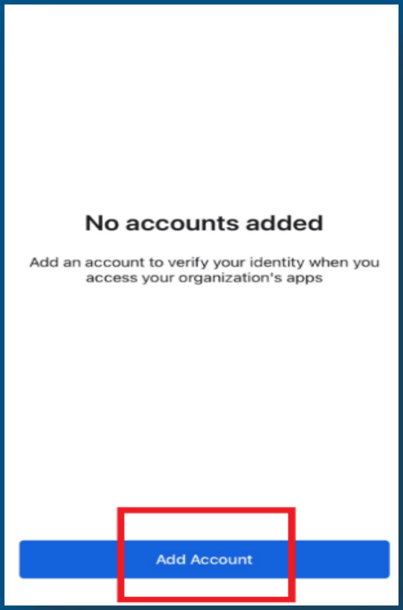


10:54

okta Verify

cisa-partner-dev.oktaprevie...
testa7285@gmail.com

Select the "+" sign or "Add Account."

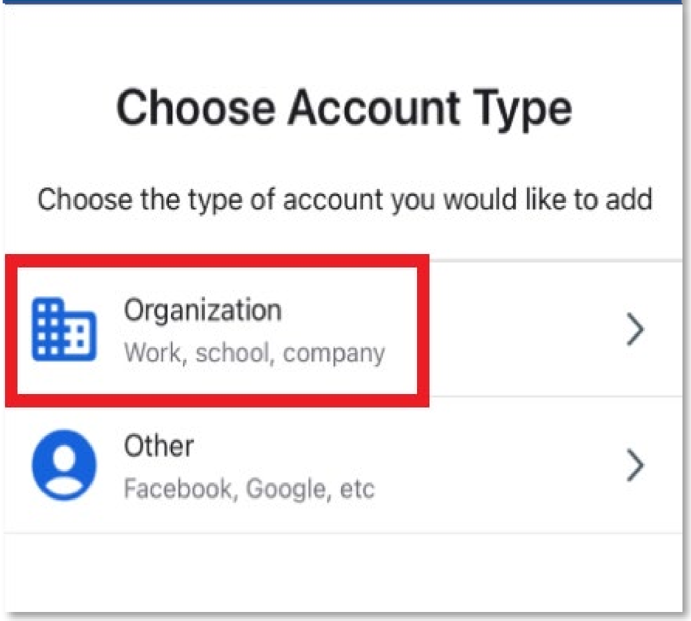


No accounts added

Add an account to verify your identity when you access your organization's apps

STEP 21

Select Account type as "Organization."

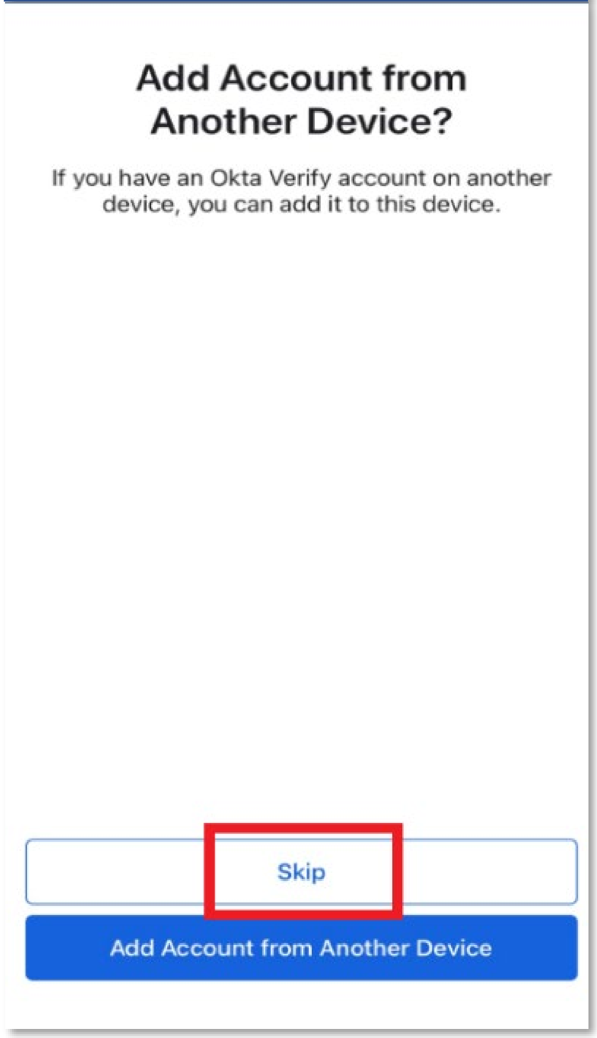


Choose Account Type

Choose the type of account you would like to add

STEP 22

Select “Skip” when asked if Adding Account from another device.

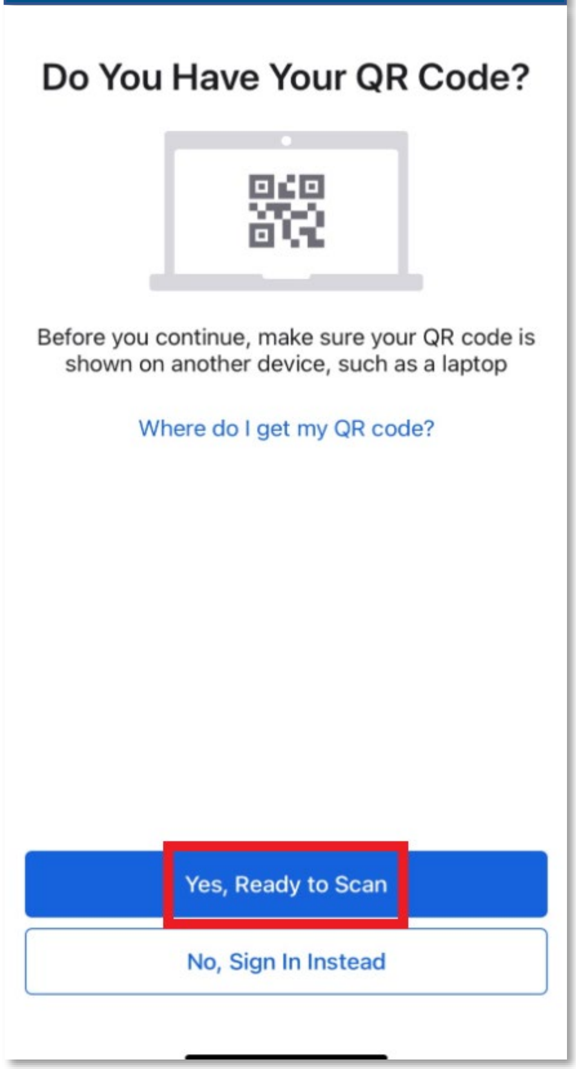


Add Account from Another Device?

If you have an Okta Verify account on another device, you can add it to this device.

STEP 23

Select “Yes, Ready to Scan” when prompted by the question “Do You Have Your QR Code?”

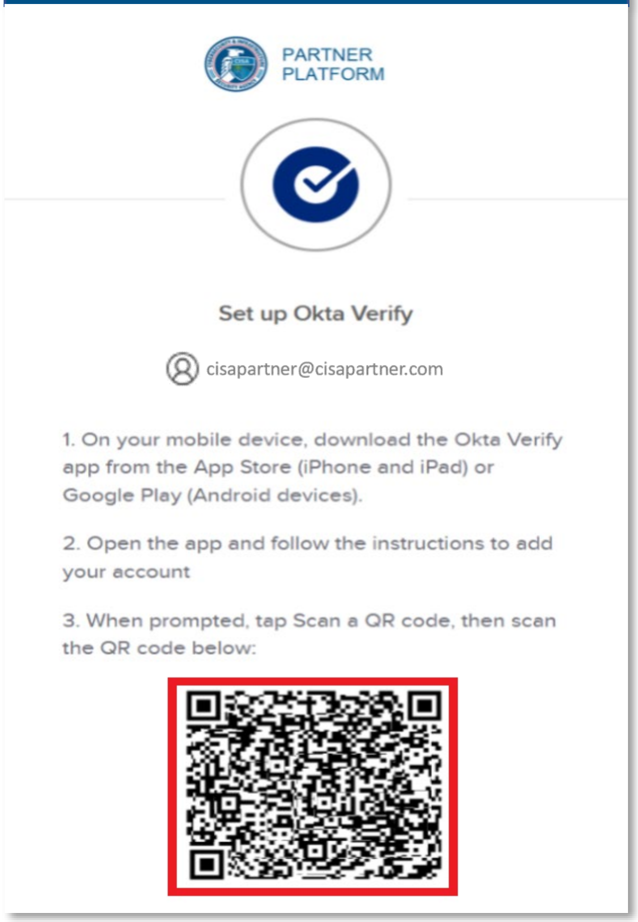


Do You Have Your QR Code?

Before you continue, make sure your QR code is shown on another device, such as a laptop

STEP 24

Capture the QR Code displayed on the Okta Verify Screen. (Note that the camera may scan the QR code before you can center it. While surprising, it still works.)



PARTNER PLATFORM

Set up Okta Verify

cisapartner@cisapartner.com

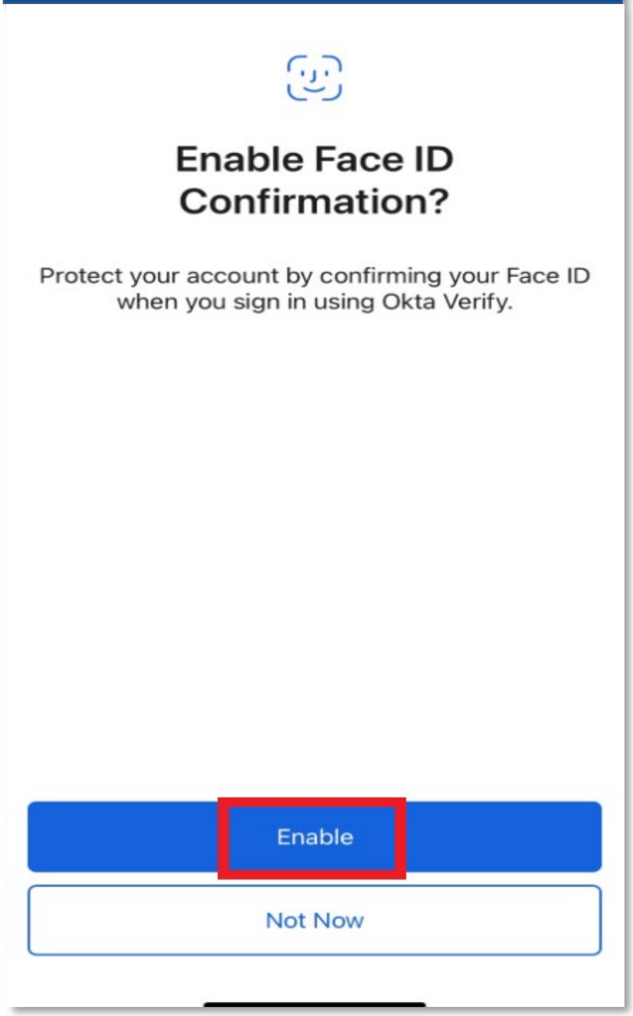
1. On your mobile device, download the Okta Verify app from the App Store (iPhone and iPad) or Google Play (Android devices).

2. Open the app and follow the instructions to add your account

3. When prompted, tap Scan a QR code, then scan the QR code below:

STEP 25

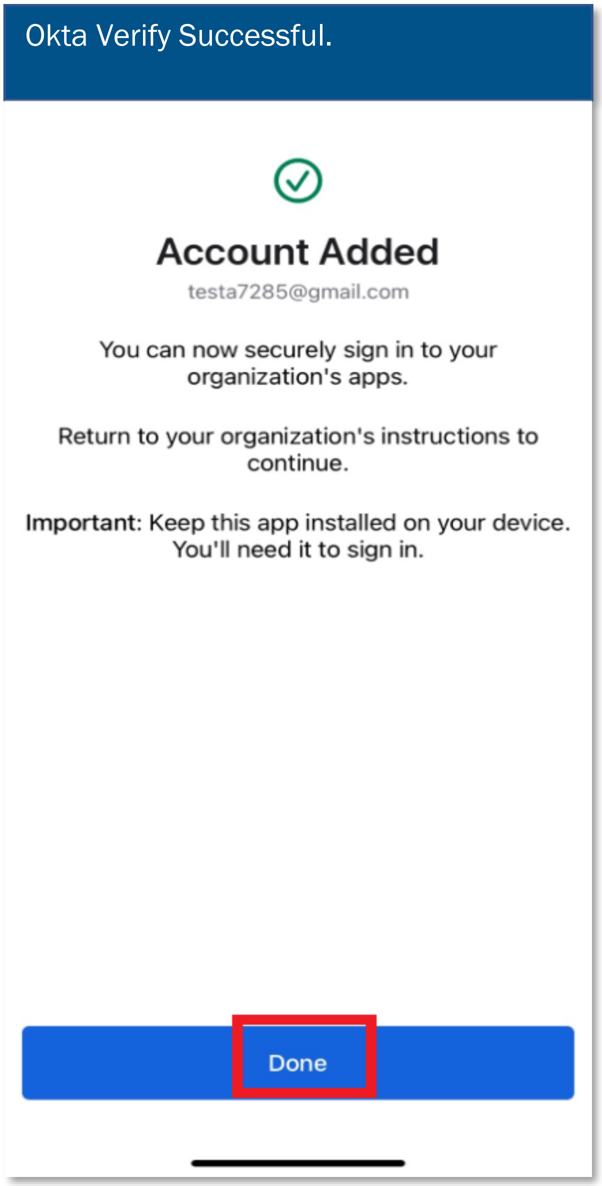
Enable Face ID Confirmation when asked on Okta Authenticator.



Enable Face ID Confirmation?

Protect your account by confirming your Face ID when you sign in using Okta Verify.

STEP 26



Okta Verify Successful.

Account Added

testa7285@gmail.com

You can now securely sign in to your organization's apps.

Return to your organization's instructions to continue.

Important: Keep this app installed on your device. You'll need it to sign in.

This concludes the Okta Verify setup. If preferred, the Google Authenticator option for multi-factor authentication set up is described in steps 5-14 above.