Create a SecureX Business with Cisco Secure Sign-On

Contents

Introduction

This document describes the steps to create a new SecureX business using Cisco Secure Sign-On.

Contributed by Uriel Torres, Brenda Marquez, and Edited by Yeraldin Sanchez, Cisco TAC Engineers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic navigation in Cisco Security Service Exchange (**SSE**)
- A Cisco Smart/Virtual Account or one of the following devices: Security Management Appliance (**SMA**) Email/WebFirepowerEmail Security Appliance (**ESA**)Web Security Appliance (**WSA**)Stealthwatch Enterprise

Components Used

The information in this document is based on these software and hardware versions:

- Cisco SSE
- SecureX version 1.52
- Cisco Duo Mobile Android version 3.34.0
- ESA with Async OS version 13.0.0

- Firefox Mac Version 78.0.1

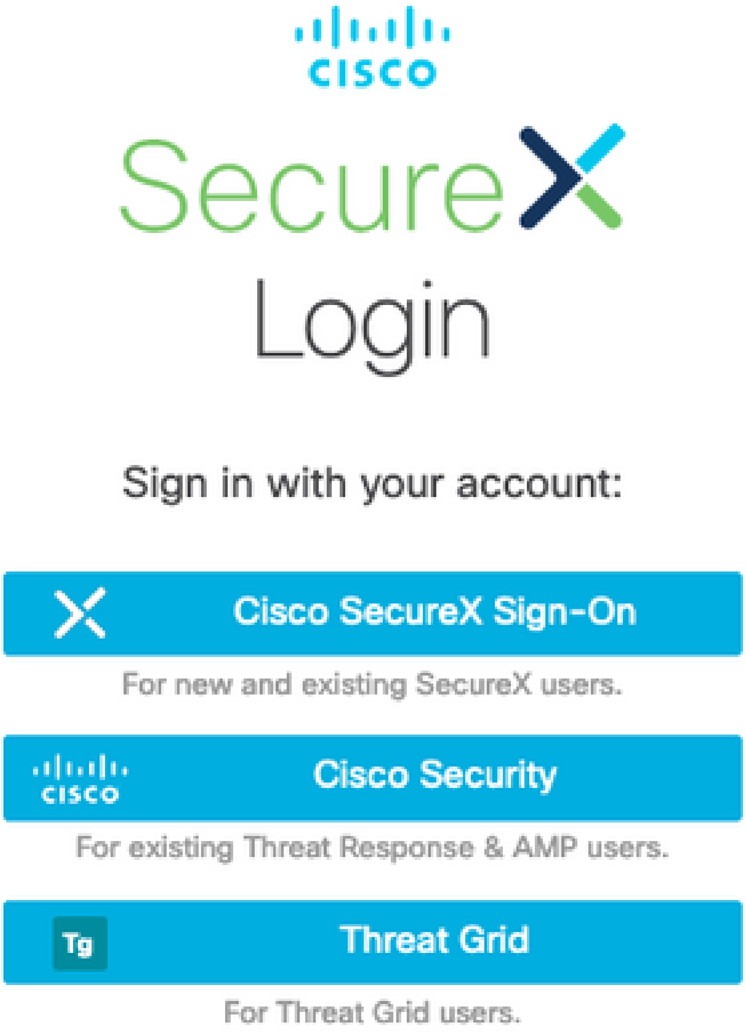
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The Cisco SecureX platform connects the breadth of Cisco's integrated security portfolio and the customer's infrastructure for a consistent experience that unifies visibility, enables automation, and strengthens your security across network, endpoint, cloud, and applications. By connecting technology in an integrated platform, SecureX delivers measurable insights, desirable outcomes, and unparalleled cross-team collaboration.

Cisco SecureX has 3 different ways to login:

- Cisco Secure Sign-On
- Cisco Security Account (CSA)
- Threat Grid Account


cisco
SecureX
Login
Sign in with your account:
Cisco SecureX Sign-On
For new and existing SecureX users.
Cisco Security
For existing Threat Response & AMP users.
Tg
Threat Grid
For Threat Grid users.

In this article, a new SecureX business is created with Cisco Secure Sign-On.

Troubleshoot

This section provides the information you can use to troubleshoot your configuration.

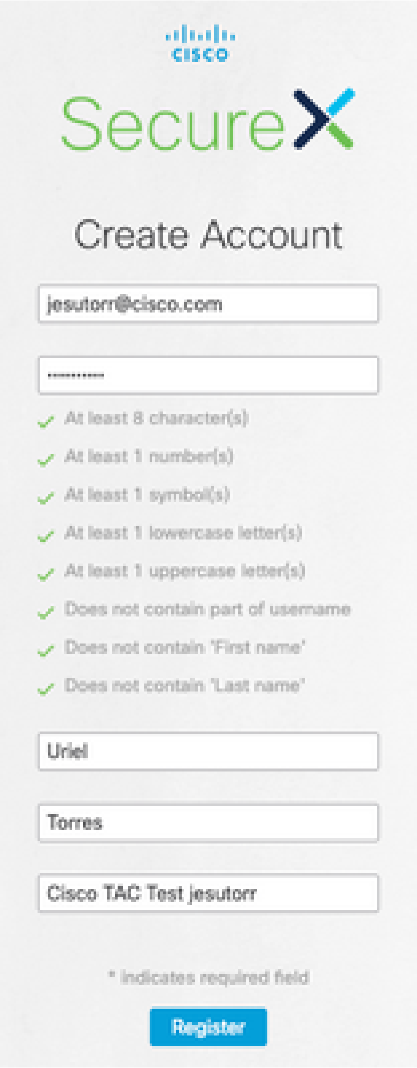
Create the Cisco Secure Sign-On account

> **Tip**: Use a private window in order to avoid any possible cache issues from the web browser.

> **Tip:** An email without a relationship with a Cisco Security Account is suggested in order to avoid accounts duplicated.

In order to create the Cisco Secure Sign-On account:

- In the web browser, navigate to https://sign-on.security.cisco.com/signin/register.
- Fill the information and click on **Register**, as shown in the image.



Create Account

jesutorr@cisco.com

••••••••••••

✓ At least 8 character(s)
✓ At least 1 number(s)
✓ At least 1 symbol(s)
✓ At least 1 lowercase letter(s)
✓ At least 1 uppercase letter(s)
✓ Does not contain part of username
✓ Does not contain 'First name'
✓ Does not contain 'Last name'

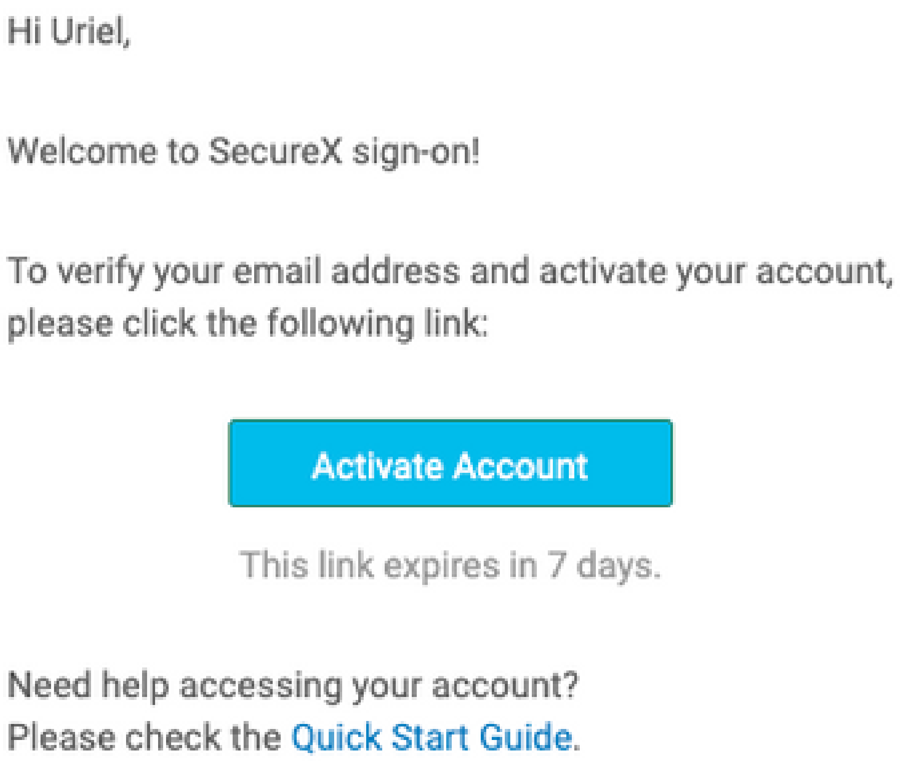
Uriel

Torres

Cisco TAC Test jesutorr

* indicates required field

- An email is sent to the email that was used to register, as shown in the image.



Hi Uriel,

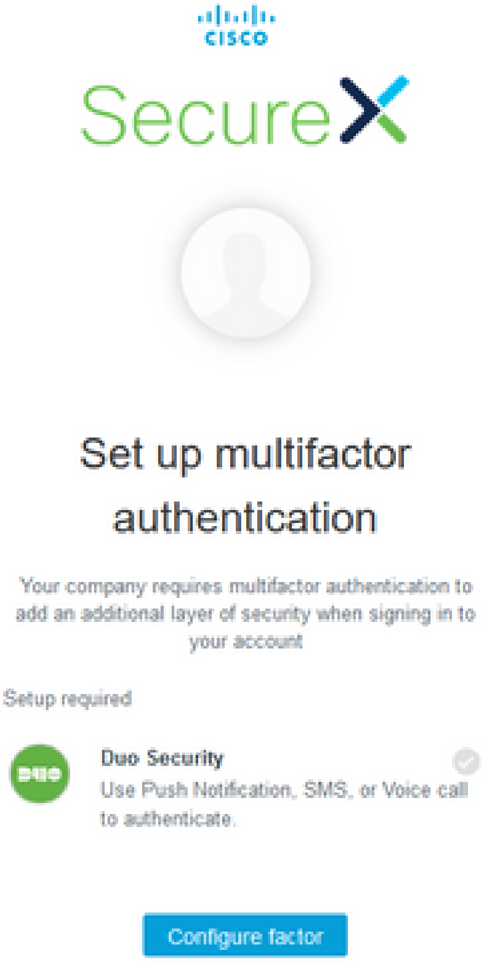
Welcome to SecureX sign-on!

To verify your email address and activate your account, please click the following link:

This link expires in 7 days.

Need help accessing your account?
Please check the Quick Start Guide.

- The Activate Account link has the URL format https://sign-on.security.cisco.com/tokens/[RegistryToken]/verify
- Complete the registration process with DUO.
- Click on the **Configure factor** button.



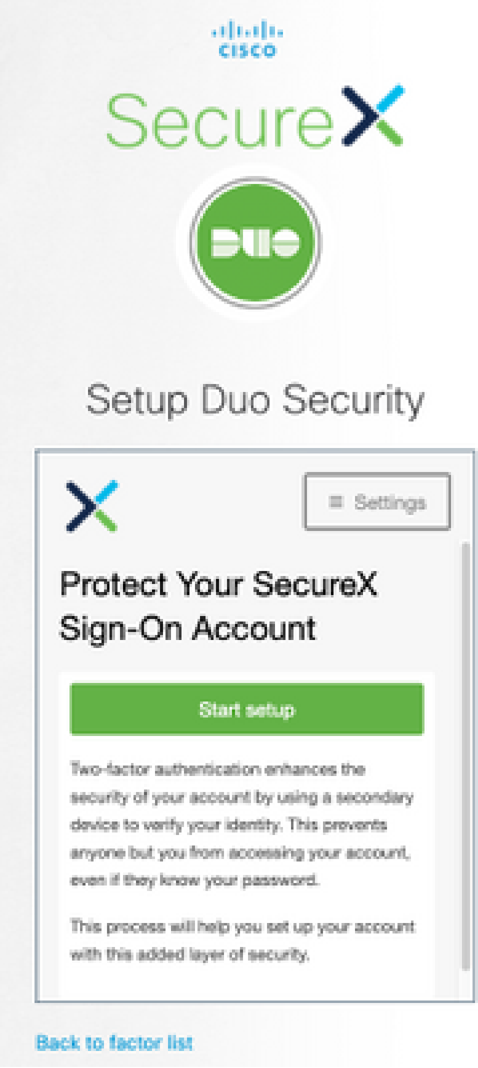
Set up multifactor authentication

Your company requires multifactor authentication to add an additional layer of security when signing in to your account

Setup required

Duo Security
Use Push Notification, SMS, or Voice call to authenticate.

- Click on the **Start Setup** button, as shown in the image.



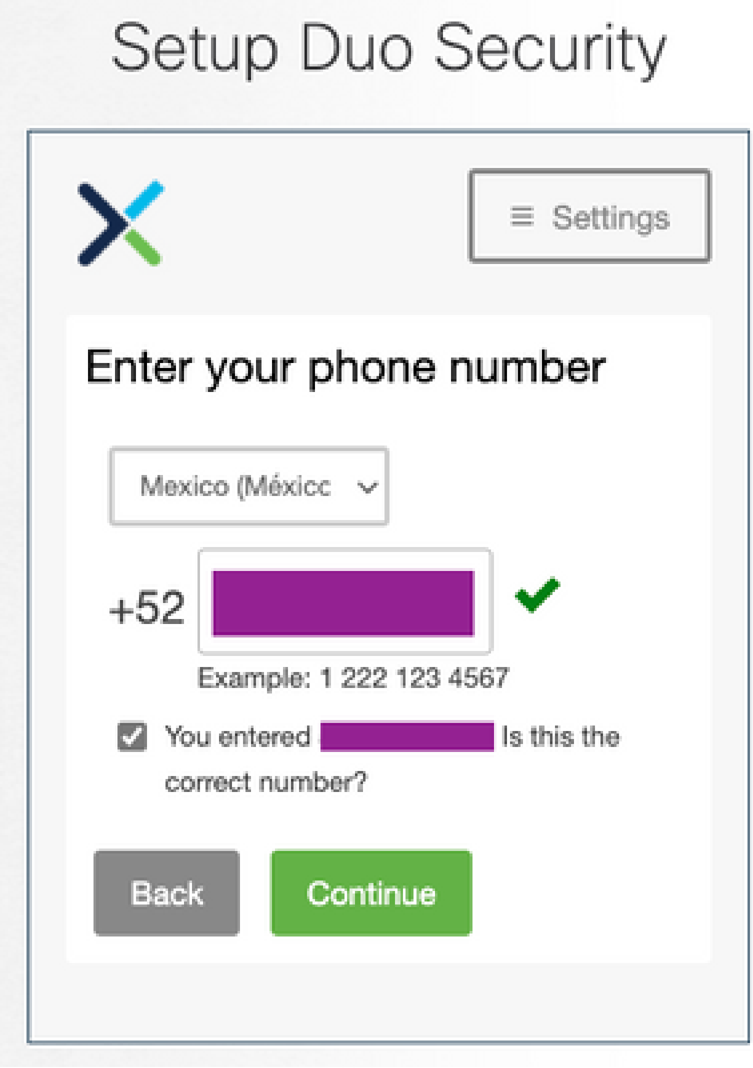
Setup Duo Security

Protect Your SecureX Sign-On Account

Two-factor authentication enhances the security of your account by using a secondary device to verify your identity. This prevents anyone but you from accessing your account, even if they know your password.

This process will help you set up your account with this added layer of security.

- Continue the setup and use your phone number to create the two-factor authentication.



Setup Duo Security

Enter your phone number

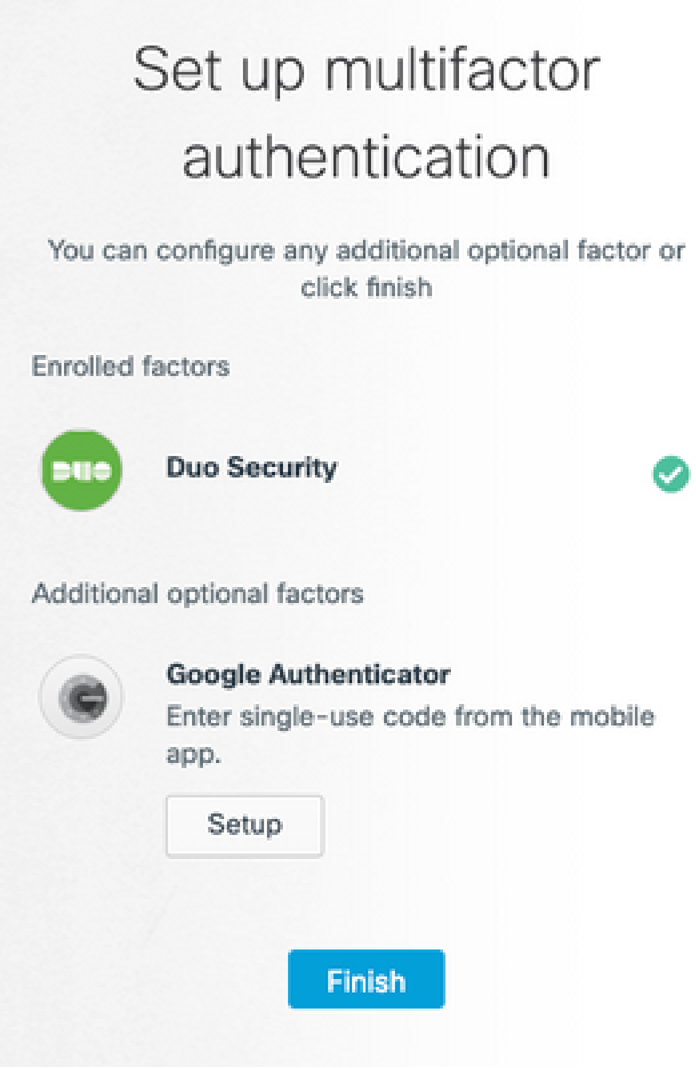
Mexico (Méxicc

+52 [redacted] ✓

Example: 1 222 123 4567

☑ You entered [redacted] Is this the correct number?

- Click on the **Finish** button to complete the enrollment process.



Set up multifactor authentication

You can configure any additional optional factor or click finish

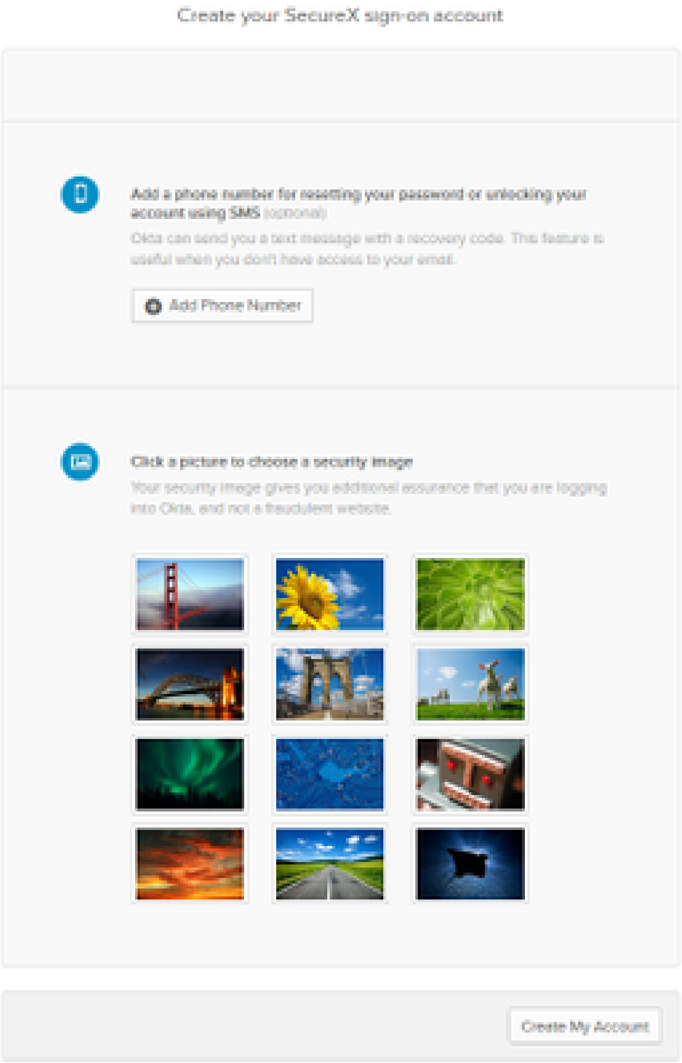
Enrolled factors

Duo Security ✓

Additional optional factors

Google Authenticator
Enter single-use code from the mobile app.

- Click on **Create My Account**, as follows.



Create your SecureX sign-on account

Add a phone number for resetting your password or unlocking your account using SMS (optional)

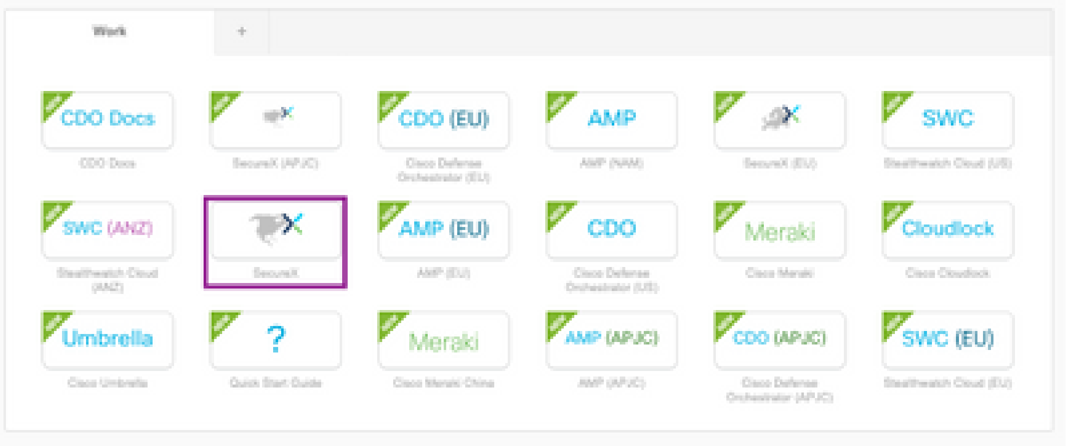
Okta can send you a text message with a recovery code. This feature is useful when you don't have access to your email.

Click a picture to choose a security image

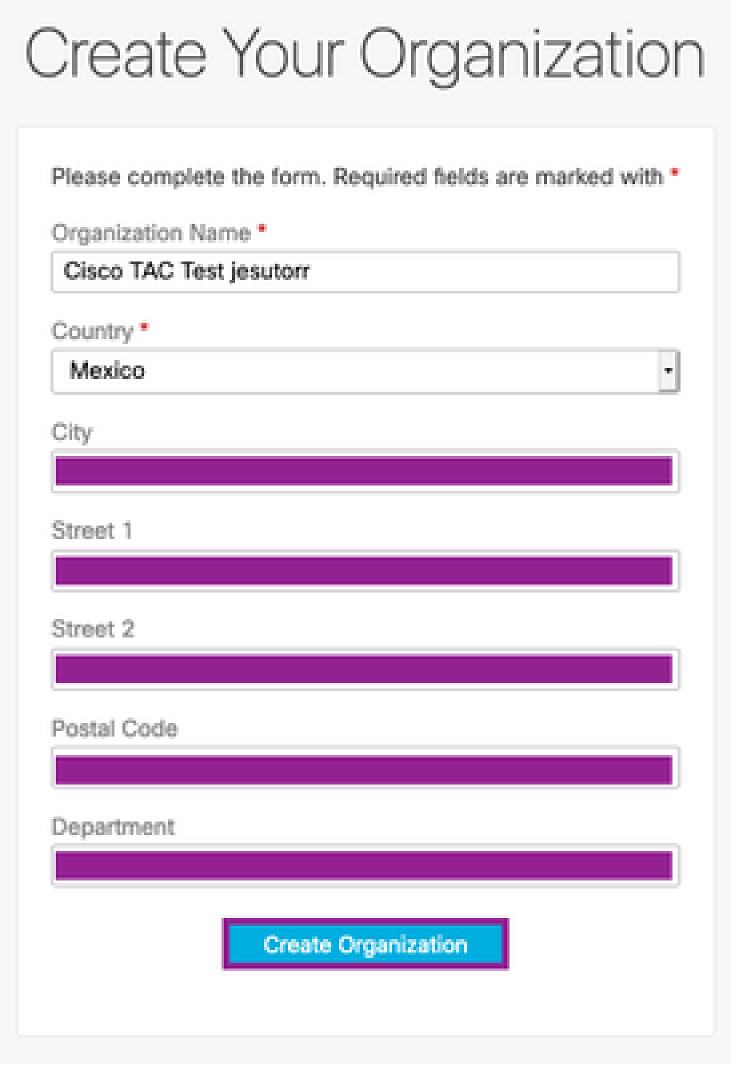
Your security image gives you additional assurance that you are logging into Okta, and not a fraudulent website.

Create the Cisco SSE account

- The Secure Sign-on page is displayed.



- Click on SecureX (For this guide North America region is used).
- Log on SecureX with DUO and the Cisco Secure Sign-On.
- Create your New SecureX Organization.



Create Your Organization

Please complete the form. Required fields are marked with *

Organization Name *

Cisco TAC Test jesutorr

Country *

Mexico

City

[redacted]

Street 1

[redacted]

Street 2

[redacted]

Postal Code

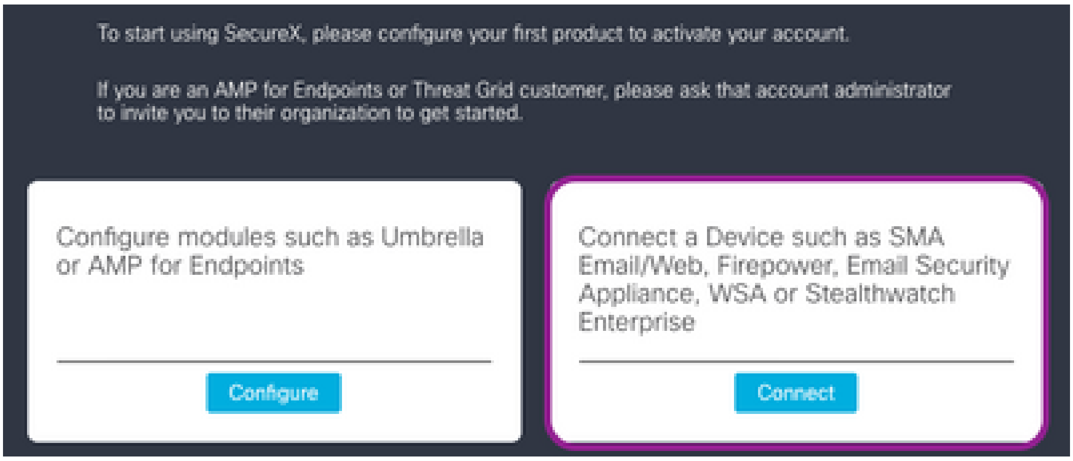
[redacted]

Department

[redacted]

- Once the organization is created, the account requires activation.

Activate the SecureX account via SSE



To start using SecureX, please configure your first product to activate your account.

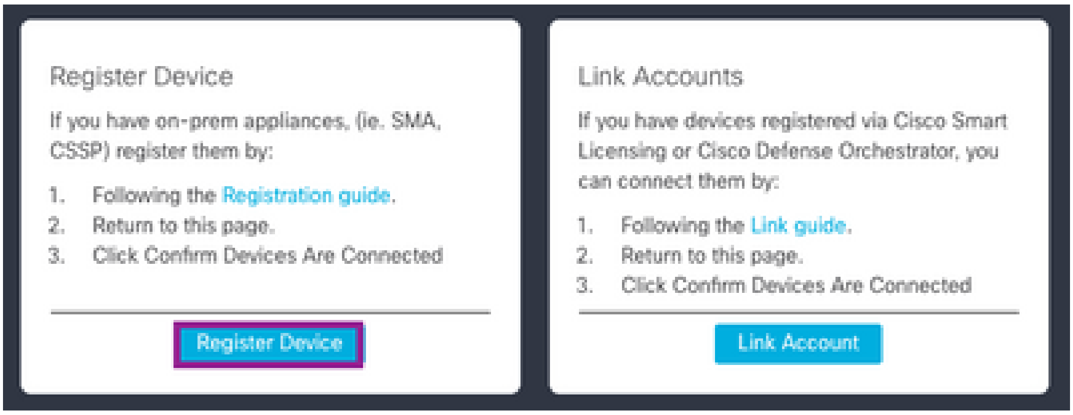
If you are an AMP for Endpoints or Threat Grid customer, please ask that account administrator to invite you to their organization to get started.

Configure modules such as Umbrella or AMP for Endpoints

Connect a Device such as SMA Email/Web, Firepower, Email Security Appliance, WSA or Stealthwatch Enterprise

- For this guide, an ESA device is used in order to activate SecureX.
- Click on the **Connect** button.
- In the **Connect Device** window, a device or a Cisco Smart/Virtual account can be used to activate it.
- For this guide click on the **Register Device** button.

Tip: In order to register other devices than ESA, in the **Connect Device** window you can find the registration guide and the link guide.



Register Device

If you have on-prem appliances, (ie. SMA, CSSP) register them by:

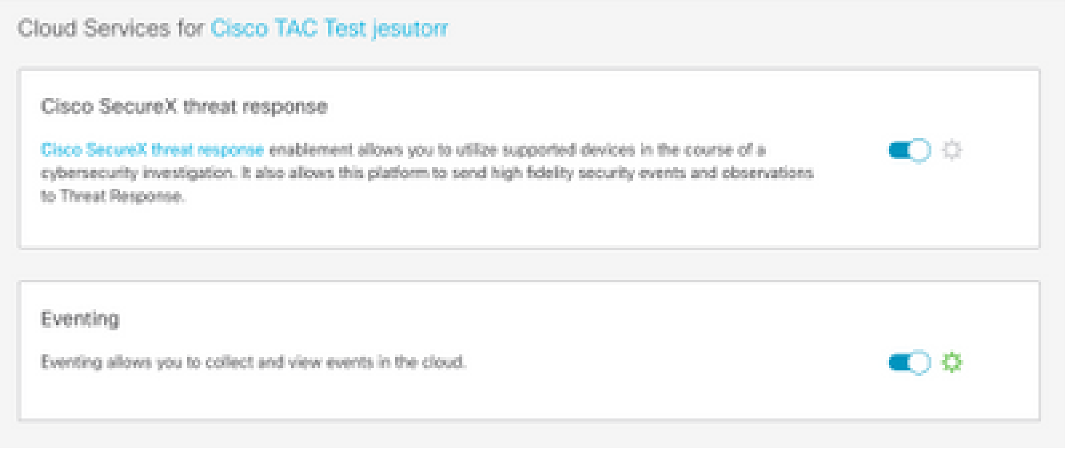
1. Following the Registration guide.
2. Return to this page.
3. Click Confirm Devices Are Connected

Link Accounts

If you have devices registered via Cisco Smart Licensing or Cisco Defense Orchestrator, you can connect them by:

1. Following the Link guide.
2. Return to this page.
3. Click Confirm Devices Are Connected

- You are redirected to the Cisco Security Service Exchange (SSE) portal.
- On SSE navigate to **Cloud Services** and enable **Cisco SecureX threat Response** and **Eventing**.



Cloud Services for Cisco TAC Test jesutorr

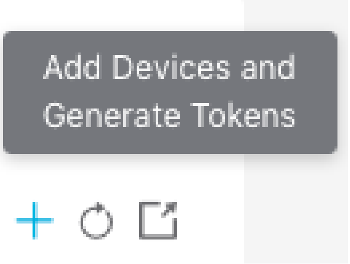
Cisco SecureX threat response

Cisco SecureX threat response enablement allows you to utilize supported devices in the course of a cybersecurity investigation. It also allows this platform to send high fidelity security events and observations to Threat Response.

Eventing

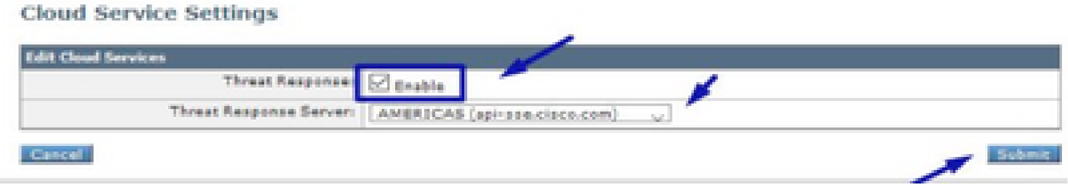
Eventing allows you to collect and view events in the cloud.

- On SSE navigate to **Devices** section.
- Click on the **Add Devices and Generate Tokens** option.



Tip: You can find more information about how to register a device with the token: **Here.**

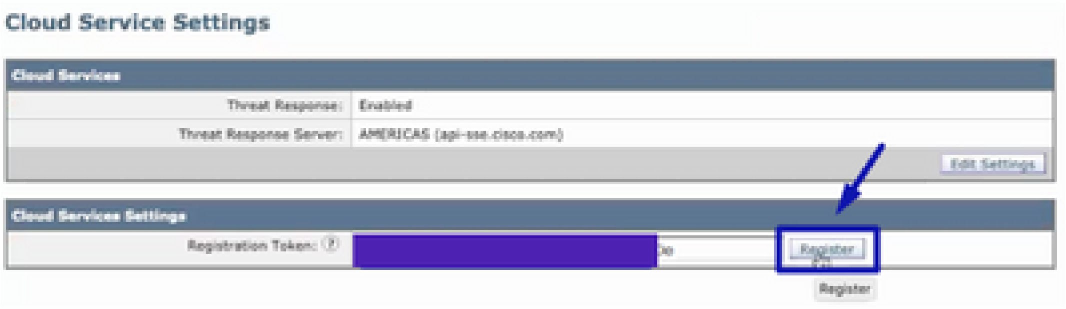
- Copy the registration token.
- Access to the ESA user interface.
- On the ESA navigate to **Network > Cloud Services Settings**.
- On Cloud Services Settings window click on the **Edit Settings** button.
- Enable **Threat Response,** the cloud server (AMERICAS in this guide).



Cloud Service Settings

Edit Cloud Services	
Threat Response:	☑ Enable
Threat Response Server:	AMERICAS (api-sse.cisco.com)

- Commit the changes.
- Paste the registration token and click on the **Register** button, as shown in the image.

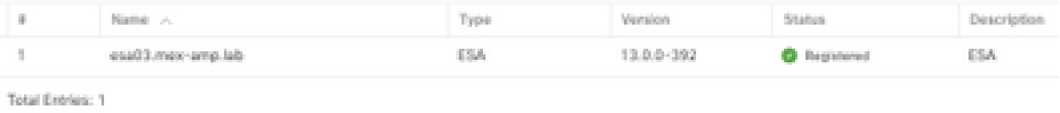


Cloud Service Settings

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)

Cloud Services Settings	
Registration Token: ?	[redacted]

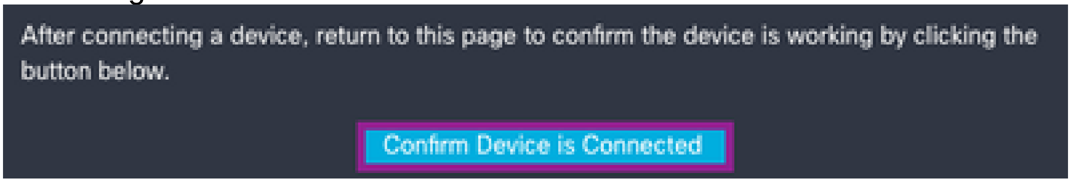
- Reload the SSE page, navigate to **Devices** and the ESA device is displayed.



#	Name	Type	Version	Status	Description
1	esa03.mex-amp.lab	ESA	13.0.0-392	● Registered	ESA

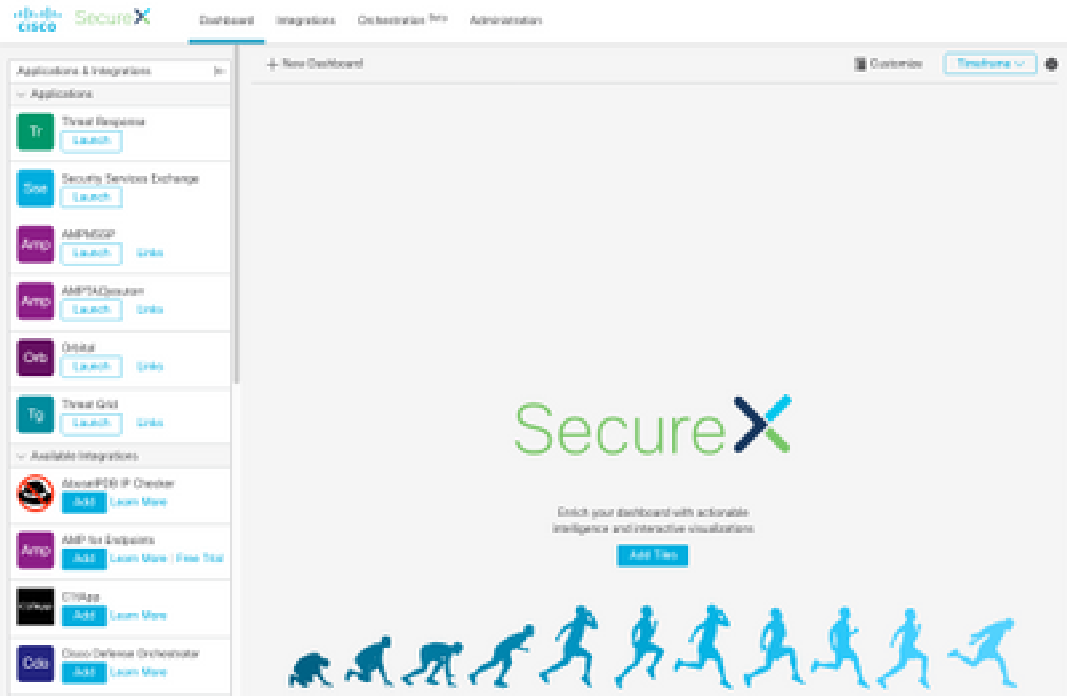
Total Entries: 1

- Navigate to SecureX and click on the **Confirm Device is Connected** button.



After connecting a device, return to this page to confirm the device is working by clicking the button below.

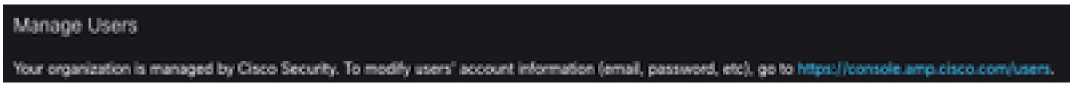
- After the confirmation, you are redirected to the SecureX portal, as shown in the image.



cisco SecureX
Dashboard
Integrations
Orchestration Beta
Administration
Applications & Integrations
Applications
Tr Threat Response Launch
Sse Security Services Exchange Launch
Amp AMPMSSP Launch Links
Amp AMPTAQesuiten Launch Links
Orb Orbital Launch Links
Tg Threat Grid Launch Links
Available Integrations
AbuseIPDB IP Checker Add Learn More
Amp AMP for Endpoints Add Learn More | Free Trial
CTIApp Add Learn More
Cdo Cisco Defense Orchestrator Add Learn More
+ New Dashboard
Customize
Timeframe
SecureX
Enrich your dashboard with actionable intelligence and interactive visualizations
Add Tiles

Manage Users in SecureX (Invite, Enable, Disable)

In case the SecureX account was activated with Advanced Malware Protection (**AMP**) for endpoints the users are managed directly on the AMP Console.



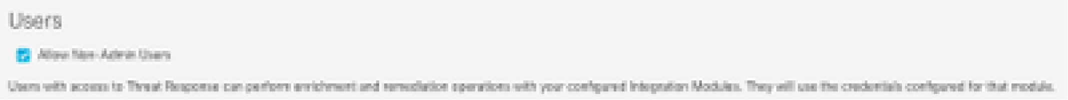
Manage Users

Your organization is managed by Cisco Security. To modify users' account information (email, password, etc), go to https://console.amp.cisco.com/users.

If the account was activated without AMP, the users are managed directly on the SecureX console, on SecureX you can have 2 types of roles:

- Admin
- User

In order to allow the **User** role, on SecureX navigate to **Your Account > Users**, check **Allow Non-Admin Users**, as shown in the image.



Users

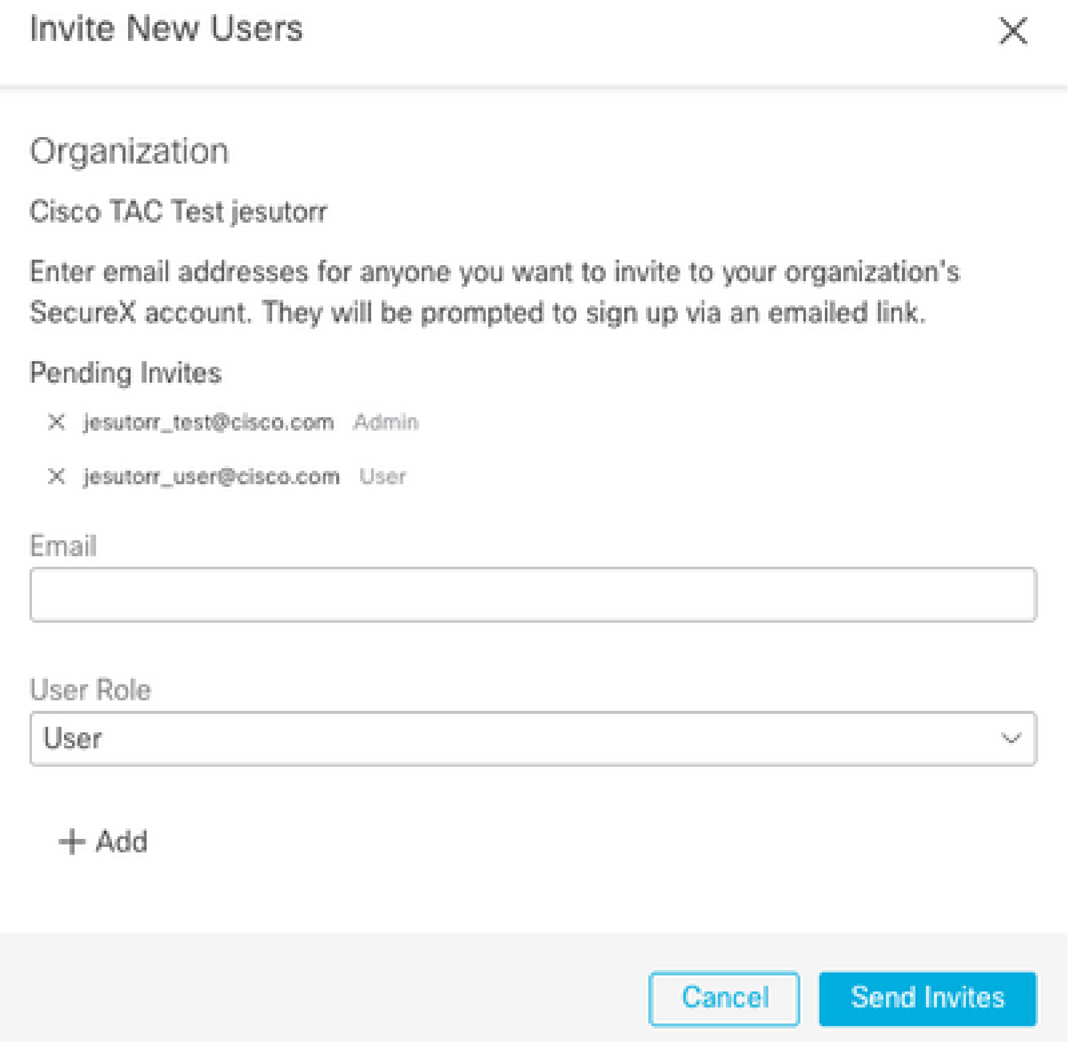
☑ Allow Non-Admin Users

Users with access to Threat Response can perform enrichment and remediation operations with your configured Integration Modules. They will use the credentials configured for that module.

Invite User

You can add new users to the SecureX organization.

- In order to add a new user role (Admin or User) on SecureX.
- Navigate to **Administration > Invite User** section.
- Use the email and role of the new user.
- Click on the **Add** button.
- If you want to add more users, fill the information of the new user and click on the **Add** button.
- Repeat this process until you have all your users added.
- Click on the **Send Invites** button.



Invite New Users

Organization

Cisco TAC Test jesutorr

Enter email addresses for anyone you want to invite to your organization's SecureX account. They will be prompted to sign up via an emailed link.

Pending Invites

× jesutorr_test@cisco.com Admin

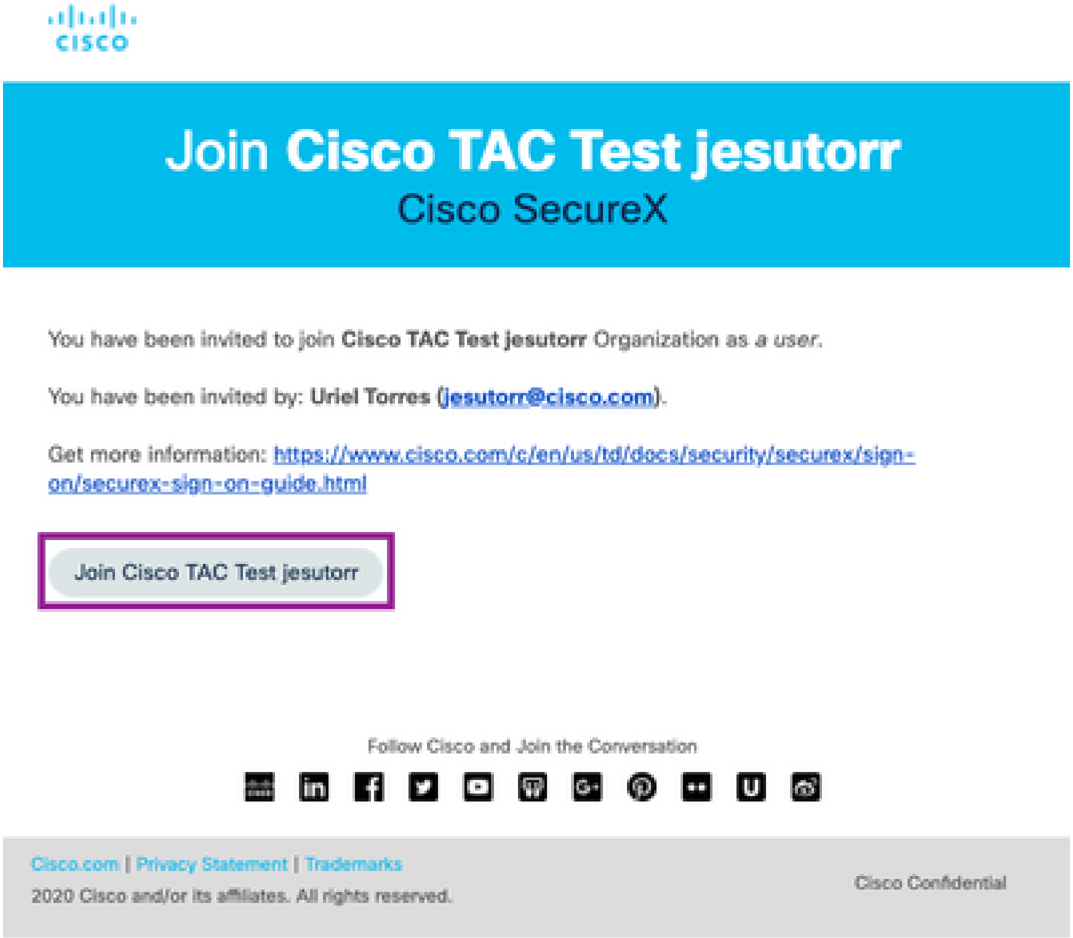
× jesutorr_user@cisco.com User

Email

User Role

User

- The new user receives an email with the information to access to the Secure X account.
- Click on the **Join...<Business Name>** button.



Join Cisco TAC Test jesutorr

Cisco SecureX

You have been invited to join **Cisco TAC Test jesutorr** Organization as *a user*.

You have been invited by: **Uriel Torres** (jesutorr@cisco.com).

Get more information: https://www.cisco.com/c/en/us/td/docs/security/securex/sign-on/securex-sign-on-guide.html

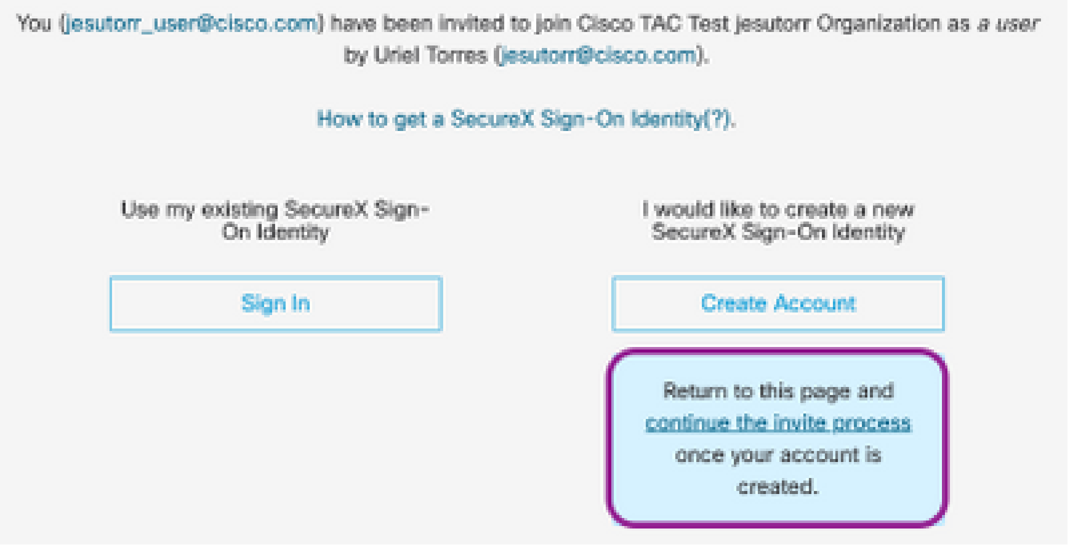
Follow Cisco and Join the Conversation

Cisco.com | Privacy Statement | Trademarks

2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

- The email redirects to the Secure X invitation login page.
- Click on **Continue the invite process**.



You (jesutorr_user@cisco.com) have been invited to join Cisco TAC Test jesutorr Organization as *a user* by Uriel Torres (jesutorr@cisco.com).

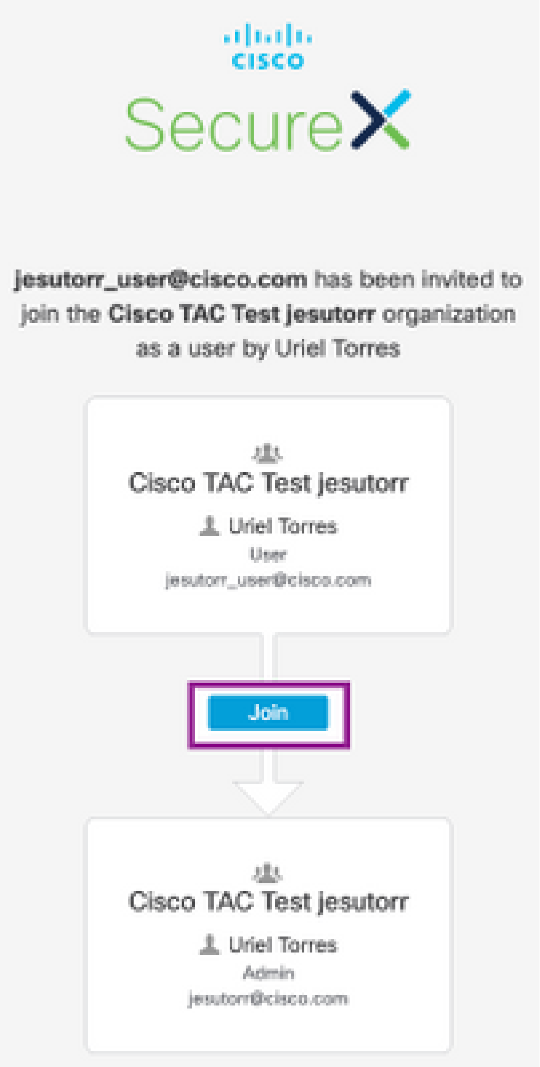
How to get a SecureX Sign-On Identity(?).

Use my existing SecureX Sign-On Identity

I would like to create a new SecureX Sign-On Identity

Return to this page and continue the invite process once your account is created.

- Complete the registration form.
- Once the registration was completed click on the **Join button**, as shown in the image.



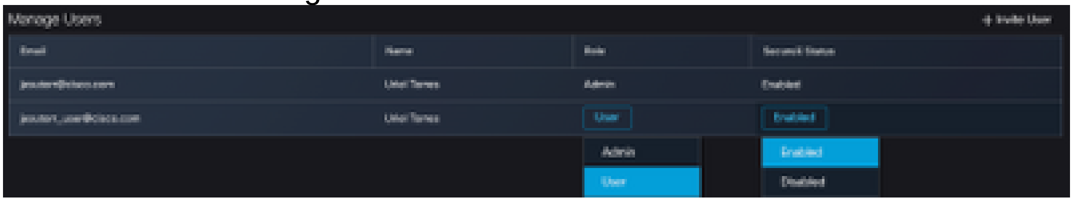
SecureX

jesutorr_user@cisco.com has been invited to join the **Cisco TAC Test jesutorr** organization as a user by Uriel Torres

Cisco TAC Test jesutorr
Uriel Torres
User
jesutorr_user@cisco.com

Cisco TAC Test jesutorr
Uriel Torres
Admin
jesutorr@cisco.com

- Once the user clicks on **join,** a new user is available in the **Administrator** window.
- In order to manage the users with an **Admin** account in SecureX navigate to the **Administration** section.
- On the **Administration** window, the users can be enabled/disabled or promoted/demoted, as shown in the image.

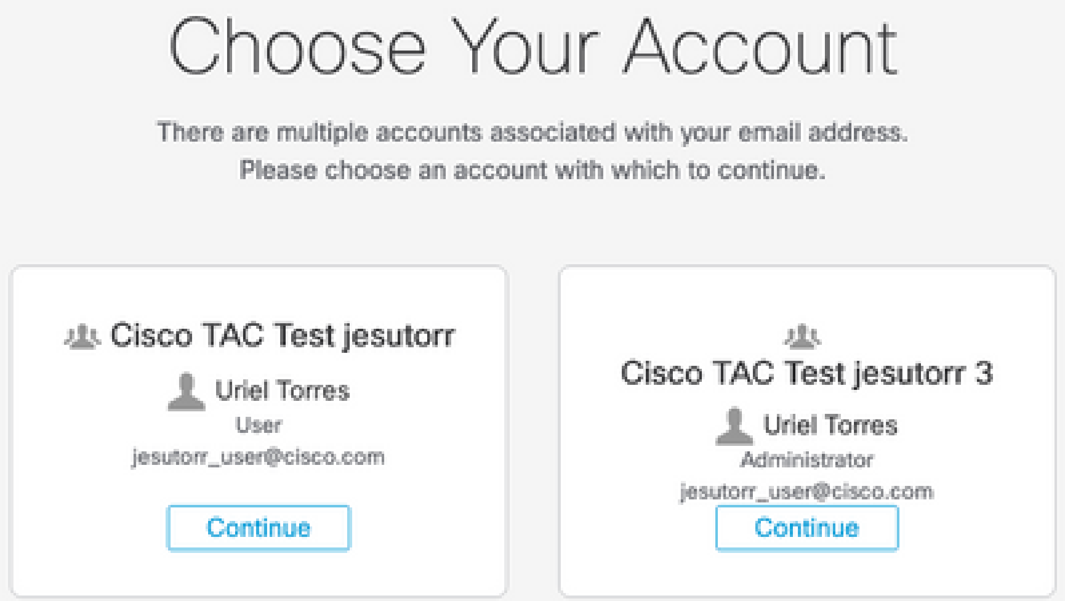


Manage Users

Email	Name	Role	SecureX Status
jesutorr@cisco.com	Uriel Torres	Admin	Enabled
jesutorr_user@cisco.com	Uriel Torres	User	Enabled

Note: At this moment the users can't be deleted from SecureX, if a user isn't necessary can be disabled.

Note: You can have different SecureX business with the same Secure Sign-on account, at the moment you use the Secure Sign-On option, the account can be selected.



Choose Your Account

There are multiple accounts associated with your email address.
Please choose an account with which to continue.

Cisco TAC Test jesutorr
Uriel Torres
User
jesutorr_user@cisco.com

Cisco TAC Test jesutorr 3
Uriel Torres
Administrator
jesutorr_user@cisco.com