

Creazione di un'azienda SecureX con Cisco Secure Sign-On

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Risoluzione dei problemi](#)

[Creare l'account Cisco Secure Sign-On](#)

[Crea l'account SSE di Cisco](#)

[Attiva l'account SecureX tramite SSE](#)

[Gestione utenti in SecureX \(invito, abilitazione, disabilitazione\)](#)

[Invita utente](#)

Introduzione

In questo documento viene descritto come creare una nuova attività SecureX utilizzando Cisco Secure Sign-On.

Contributo di Uriel Torres, Brenda Marquez e a cura di Yeraldin Sanchez, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Navigazione di base in Cisco Security Service Exchange (**SSE**)
- Uno Smart Account/account virtuale Cisco o uno dei seguenti dispositivi: E-mail/Web di Security Management Appliance (**SMA**) Firepower Email Security Appliance (**ESA**) Web Security Appliance (**WSA**) Stealthwatch Enterprise

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco SSE
- SecureX versione 1.52
- Cisco Duo Mobile Android versione 3.34.0
- ESA con Async OS versione 13.0.0

- Firefox Mac versione 78.0.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La piattaforma Cisco SecureX collega l'ampia gamma di prodotti per la sicurezza integrata di Cisco e l'infrastruttura del cliente per offrire un'esperienza coerente che unifica la visibilità, consente l'automazione e rafforza la sicurezza su rete, endpoint, cloud e applicazioni. Collegando la tecnologia in una piattaforma integrata, SecureX offre informazioni dettagliate misurabili, risultati desiderati e una collaborazione tra team senza precedenti.

Cisco SecureX può accedere in tre modi:

- Cisco Secure Sign-On
- Account di sicurezza Cisco (CSA)
- Account griglia minaccia



Sign in with your account:



In questo articolo viene creata una nuova attività SecureX con Cisco Secure Sign-On.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

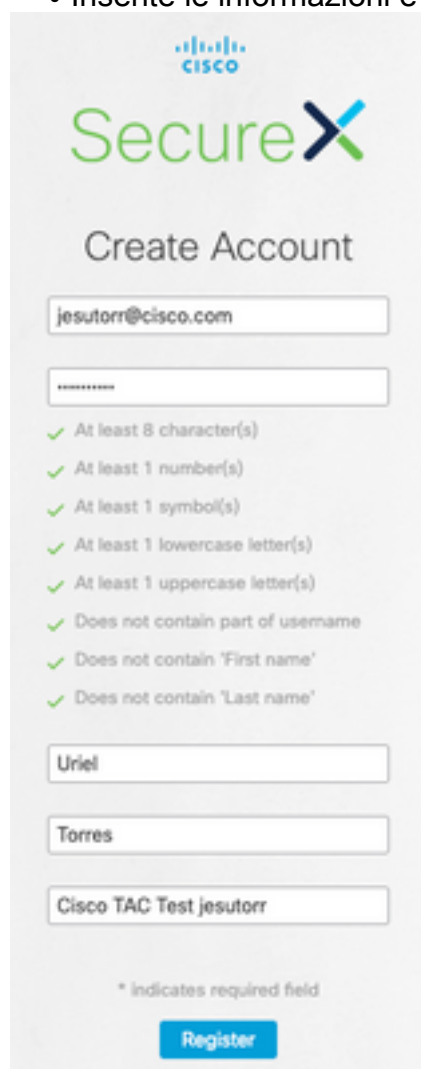
Creare l'account Cisco Secure Sign-On

Suggerimento: Utilizzare una finestra privata per evitare possibili problemi di cache dal browser Web.

Suggerimento: per evitare che gli account siano duplicati, si consiglia di inviare un'e-mail senza avere una relazione con un account di sicurezza Cisco.

Per creare l'account Cisco Secure Sign-On:

- Nel browser Web passare a <https://sign-on.security.cisco.com/signin/register>.
- Inserite le informazioni e fate clic su **Register**, come mostrato nell'immagine.



The image shows a screenshot of the Cisco Secure Sign-On registration page. At the top, there is the Cisco logo and the 'Secure X' logo. Below that, the text 'Create Account' is displayed. The form contains several input fields: an email address field with 'jesutorr@cisco.com', a password field with masked characters, a first name field with 'Uriel', a last name field with 'Torres', and a company name field with 'Cisco TAC Test jesutorr'. Below the password field, there is a list of validation rules, each preceded by a green checkmark: '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'', and 'Does not contain 'Last name''. At the bottom of the form, there is a blue 'Register' button and a note: '* Indicates required field'.

- Viene inviato un messaggio e-mail all'indirizzo utilizzato per la registrazione, come mostrato nell'immagine.

Hi Uriel,

Welcome to SecureX sign-on!

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

[Activate Account](#)

This link expires in 7 days.

Need help accessing your account?
Please check the [Quick Start Guide](#).

- Il collegamento Attiva account ha il formato URL [https://sign-on.security.cisco.com/tokens/\[RegistryToken\]/verify](https://sign-on.security.cisco.com/tokens/[RegistryToken]/verify)
- Completare il processo di registrazione con DUO.
- Fare clic sul pulsante **Configura fattore**.



Set up multifactor authentication

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

Setup required



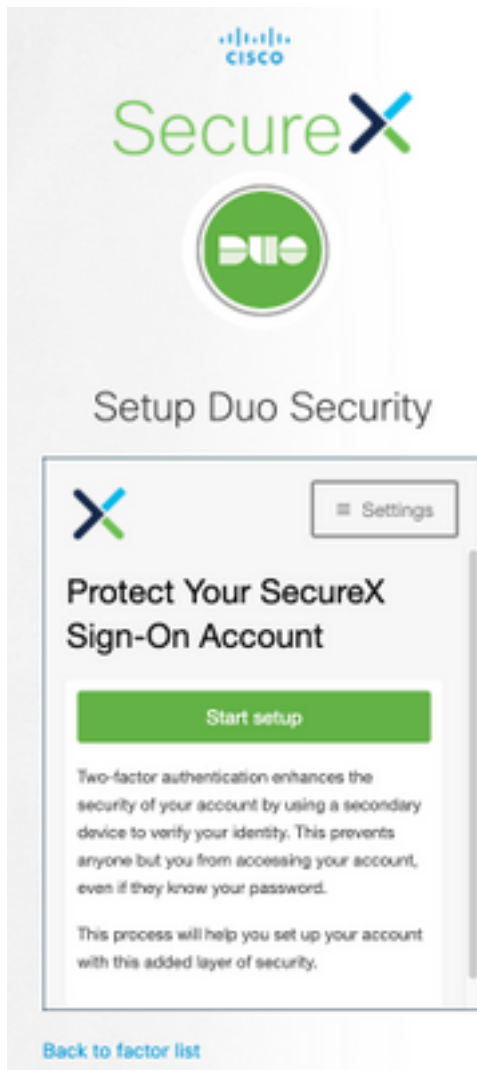
Duo Security

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



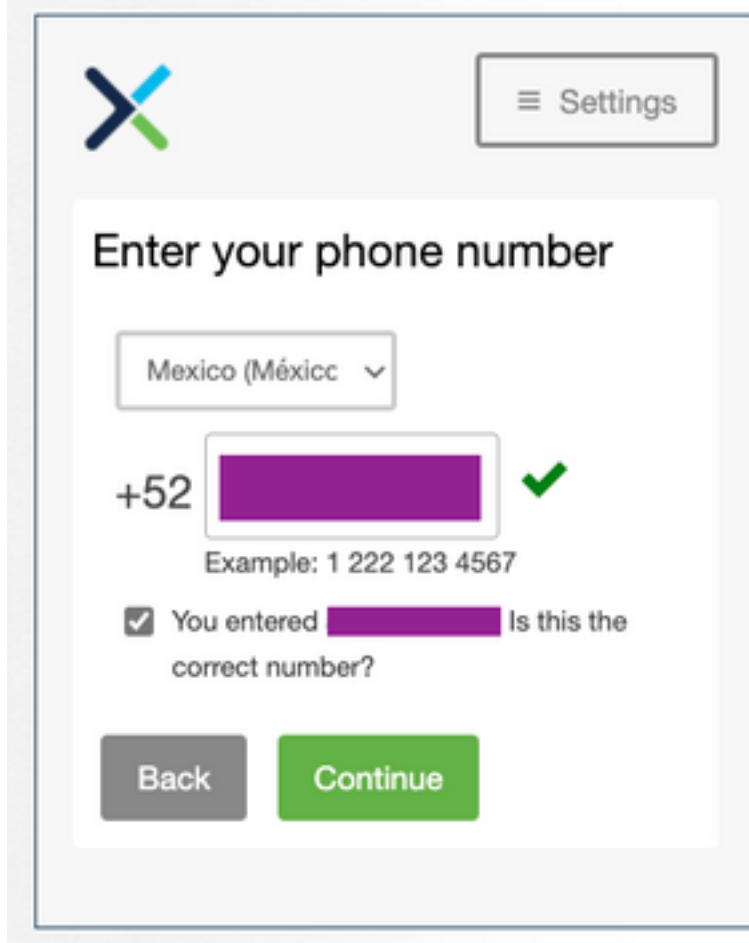
Configure factor

- Fare clic sul pulsante **Start Setup** (Avvia installazione), come mostrato nell'immagine.



- Continuare l'installazione e utilizzare il numero di telefono per creare l'autenticazione a due fattori.

Setup Duo Security



The screenshot shows a mobile application interface for setting up Duo Security. At the top left is a logo consisting of two crossed lines, one blue and one green. At the top right is a button with a hamburger menu icon and the text "Settings". The main content area is titled "Enter your phone number". Below the title is a dropdown menu showing "Mexico (Méxicc" with a downward arrow. To the left of the phone number input field is the country code "+52". The input field itself is a purple rectangle. To the right of the input field is a green checkmark. Below the input field is the text "Example: 1 222 123 4567". Below the example is a checkbox that is checked, followed by the text "You entered" and another purple rectangle representing the entered number, and then the question "Is this the correct number?". At the bottom left is a grey button labeled "Back", and at the bottom right is a green button labeled "Continue".

- Fare clic sul pulsante **Finish** (Fine) per completare il processo di iscrizione.

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.

Setup

Finish


- Fare clic su **Create My Account** (Crea account personale), come indicato di seguito.

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.

[Add Phone Number](#)

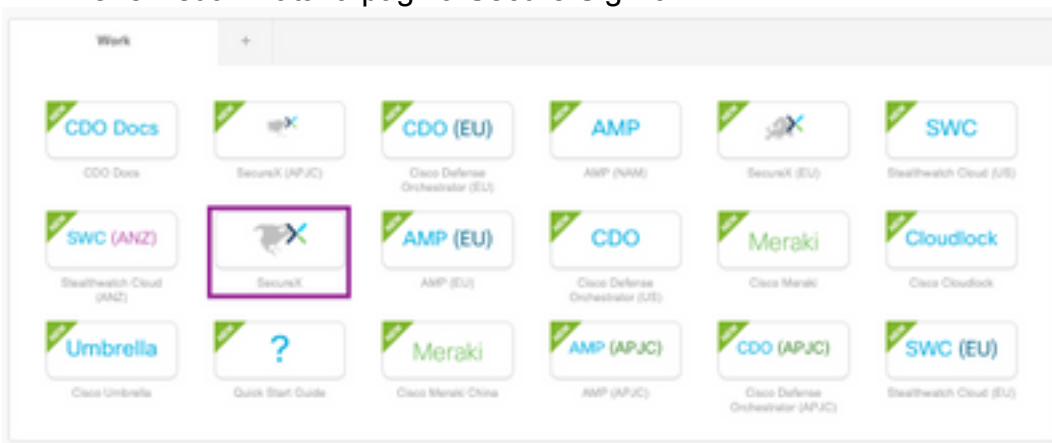
Click a picture to choose a security image
Your security image gives you additional assurance that you are logging into Okta, and not a fraudulent website.



[Create My Account](#)

Crea l'account SSE di Cisco

- Viene visualizzata la pagina Secure Sign-on.



- Fare clic su SecureX (per questa guida viene utilizzato il Nord America).
- Accedere a SecureX con DUO e Cisco Secure Sign-On.
- Creare la nuova organizzazione SecureX.

Create Your Organization

Please complete the form. Required fields are marked with *

Organization Name *

Cisco TAC Test jesutorr

Country *

Mexico

City

Street 1

Street 2

Postal Code

Department

Create Organization

- Una volta creata l'organizzazione, l'account deve essere attivato.

Attiva l'account SecureX tramite 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

Configure

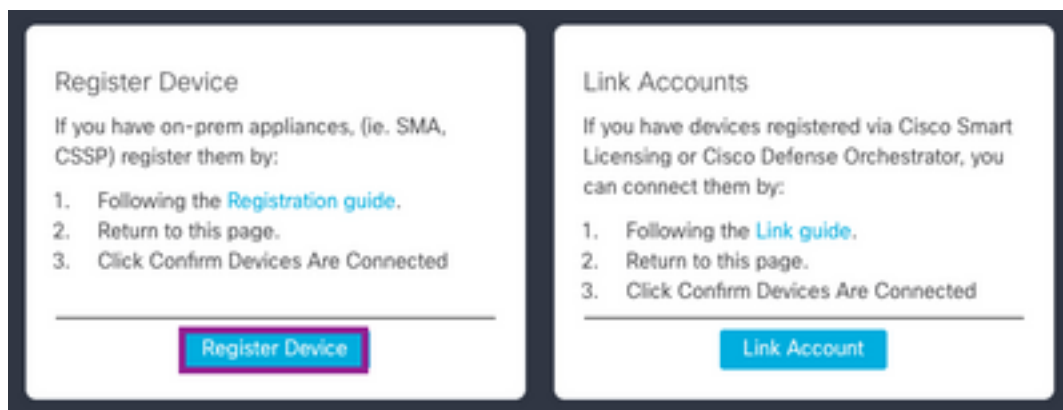
Connect a Device such as SMA Email/Web, Firepower, Email Security Appliance, WSA or Stealthwatch Enterprise

Connect

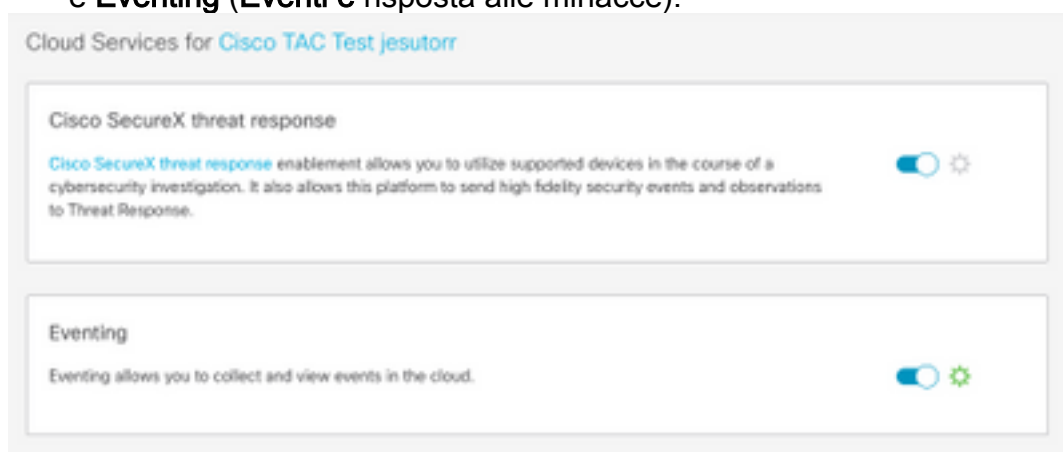
- In questa guida, viene usato un dispositivo ESA per attivare SecureX.
- Fare clic sul pulsante **Connect** (Connetti).
- Nella finestra **Connect Device**, è possibile usare un dispositivo o un account Cisco Smart/Virtual per attivarlo.
- Per questa guida fare clic sul pulsante **Register Device** (Registra dispositivo).

Suggerimento: Per registrare dispositivi diversi dall'ESA, nella finestra **Connect Device**

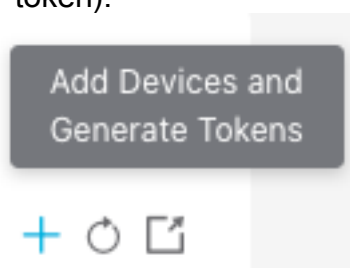
(Connetti dispositivo) si trovano la [guida alla registrazione](#) e la [guida ai collegamenti](#).



- L'utente viene reindirizzato al portale Cisco Security Service Exchange (SSE).
- Su SSE passare a **Cloud Services** (Servizi cloud) e abilitare **Cisco SecureX threat Response e Eventing** (Eventi e risposta alle minacce).



- In SSE passare alla sezione **Dispositivi**.
- Fare clic sull'opzione **Add Devices and Generate Tokens** (Aggiungi dispositivi e genera token).



Suggerimento: Per ulteriori informazioni su come registrare un dispositivo con il token, consultare: [Qui](#).

- Copiare il token di registrazione.
- Accesso all'interfaccia utente ESA.
- Nell'ESA selezionare **Rete > Impostazioni servizi cloud**.
- Nella finestra Impostazioni servizi cloud fare clic sul pulsante **Modifica impostazioni**.
- Abilitare **Threat Response**, il server cloud (AMERICHE in questa guida).



- Eseguire il commit delle modifiche.
- Incollare il token di registrazione e fare clic sul pulsante **Register**, come mostrato nell'immagine.

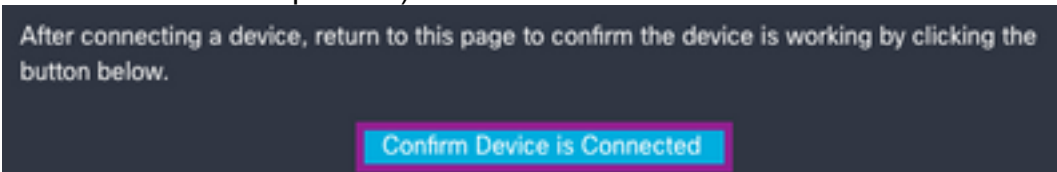


- Ricaricare la pagina SSE, selezionare **Devices** (Dispositivi) per visualizzare la periferica ESA.

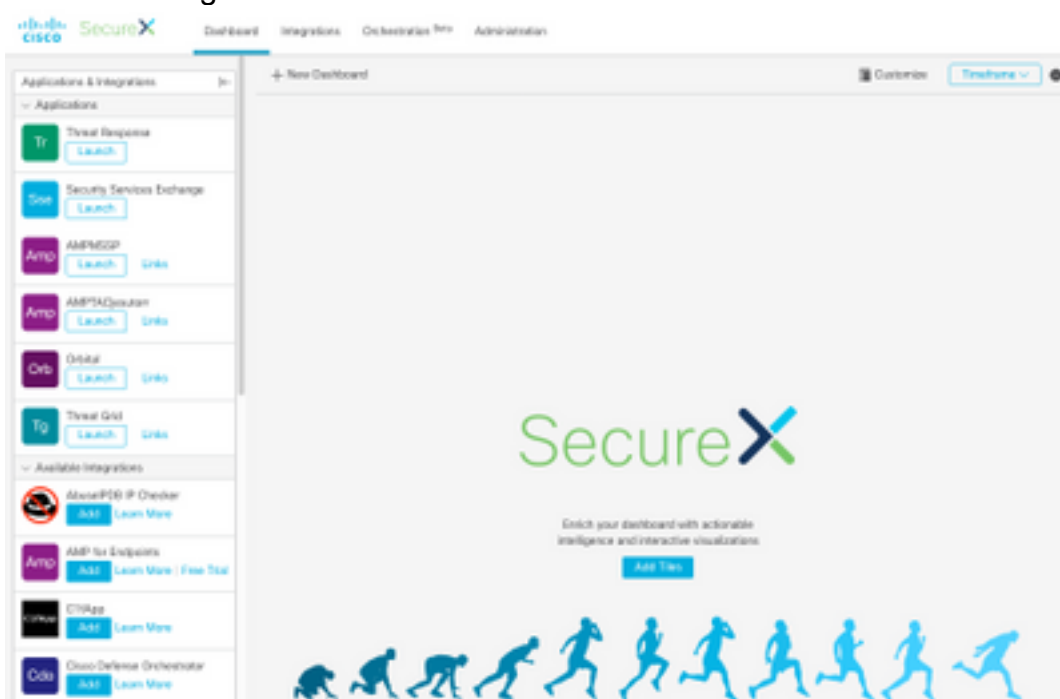
#	Name	Type	Version	Status	Description
1	esu03-mex-amp-lab	ESA	13.0.0-392	Registered	ESA

Total Entries: 1

- Passare a SecureX e fare clic sul pulsante **Confirm Device is Connected** (Conferma connessione dispositivo).



- Dopo la conferma, l'utente viene reindirizzato al portale SecureX, come mostrato nell'immagine.



Gestione utenti in SecureX (invito, abilitazione, disabilitazione)

Se l'account SecureX è stato attivato con Advanced Malware Protection (AMP) per gli endpoint, gli utenti vengono gestiti direttamente sulla console AMP.



Se l'account è stato attivato senza AMP, gli utenti vengono gestiti direttamente sulla console SecureX, su SecureX è possibile disporre di due tipi di ruoli:

- Admin
- Utente

Per consentire il ruolo **Utente**, in SecureX passare a **Account > Utenti**, selezionare **Consenti utenti non amministratori**, come mostrato nell'immagine.



Invita utente

È possibile aggiungere nuovi utenti all'organizzazione SecureX.

- Per aggiungere un nuovo ruolo utente (Admin o User) in SecureX.
- Passare alla sezione **Amministrazione > Invita utente**.
- Utilizzare l'indirizzo di posta elettronica e il ruolo del nuovo utente.
- Fare clic sul pulsante **Add**.
- Se si desidera aggiungere altri utenti, immettere le informazioni sul nuovo utente e fare clic sul pulsante **Aggiungi**.
- Ripetere questa procedura fino ad aggiungere tutti gli utenti.
- Fare clic sul pulsante **Invia inviti**.

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

+ Add

Cancel

Send Invites

- Il nuovo utente riceve un messaggio di posta elettronica contenente le informazioni necessarie per accedere all'account Secure X.
- Fare clic su **Join...**Pulsante **<Nome azienda>**.

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>

Join Cisco TAC Test jesutorr

Follow Cisco and Join the Conversation



[Cisco.com](#) | [Privacy Statement](#) | [Trademarks](#)

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

Cisco Confidential

- L'e-mail viene reindirizzata alla pagina di accesso dell'invito Secure X.
- Fare clic su **Continua il processo di invito**.

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

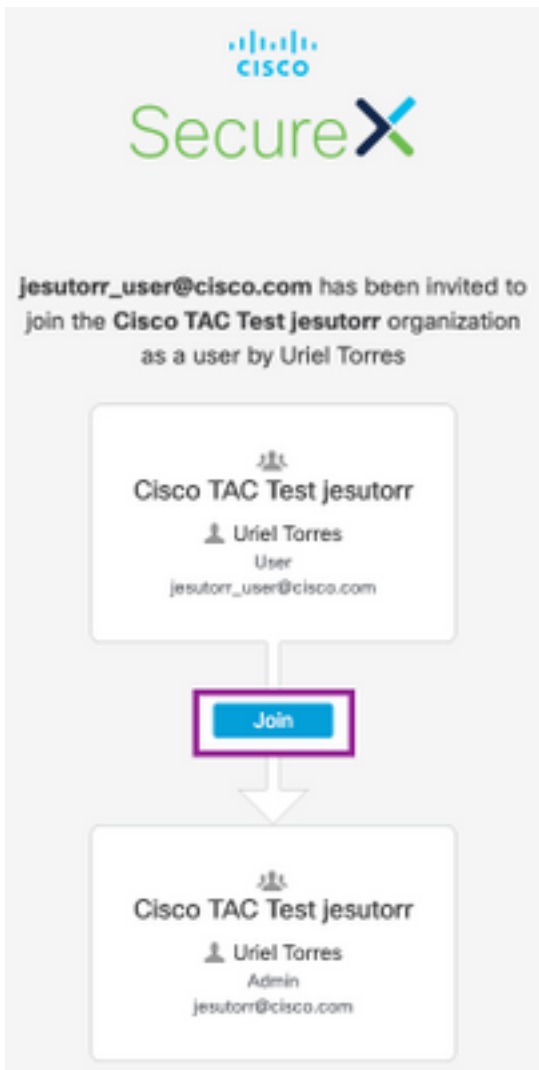
Sign In

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

Create Account

Return to this page and [continue the invite process](#) once your account is created.

- Compilate il modulo di registrazione.
- Una volta completata la registrazione, fare clic sul **pulsante Partecipa**, come mostrato nell'immagine.



- Quando l'utente fa clic su **join**, nella finestra **Administrator** è disponibile un nuovo utente.
- Per gestire gli utenti con un account **Admin** in SecureX, passare alla sezione **Amministrazione**.
- Nella finestra **Amministrazione**, gli utenti possono essere attivati/disattivati o alzati di livello/abbassati di livello, come mostrato nell'immagine.

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

Nota: Al momento non è possibile eliminare gli utenti da SecureX, se un utente non è necessario può essere disabilitato.

Nota: è possibile avere diverse transazioni SecureX con lo stesso account Secure Sign-On. Quando si utilizza l'opzione Secure Sign-On, è possibile selezionare l'account.

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

[Continue](#)



Cisco TAC Test jesutorr 3



Uriel Torres

Administrator

jesutorr_user@cisco.com

[Continue](#)