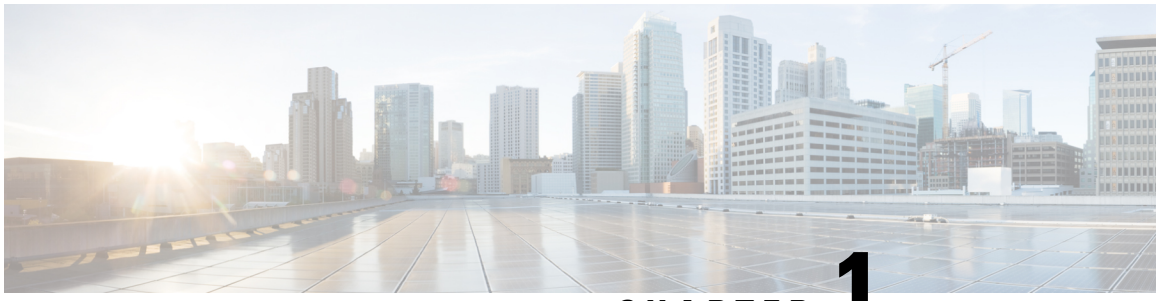
Cisco Security Cloud Sign On

First Published: 2019-10-01

Last Modified: 2023-08-23

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2019-2023 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

Overview

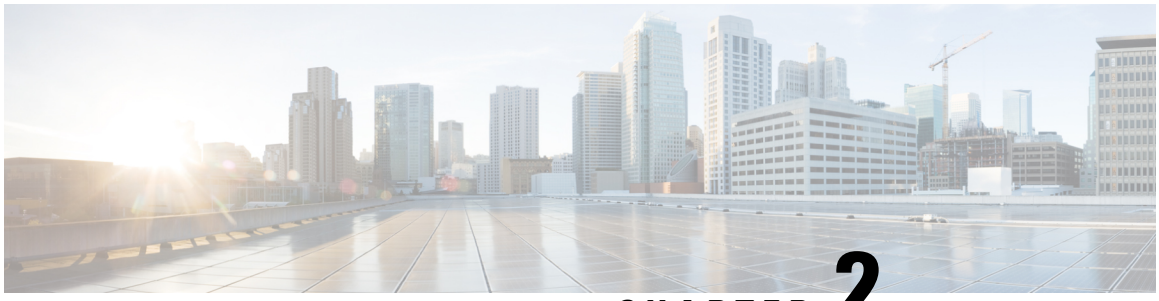
- Overview, on page 1

Overview

With Cisco Security Cloud Sign On, you can easily access many Cisco Security products with one set of credentials from any device. Once you sign in with your username and password, all your Cisco Security products are displayed as apps in your customizable dashboard.

- Click an app and you're automatically signed-in, for seamless workflows across your Cisco Security products. You no longer have to remember and juggle multiple passwords.
- Integration with Duo's Multi-Factor Authentication (MFA) means adaptive, layered, and simplified authentication. One push notification, one tap, instant access.
- Optionally, use Security Cloud Control to integrate your own identity provider (IdP) with Security Cloud Sign On.

Overview



CHAPTER 2

What's New

- New Portal, on page 3
- Cisco SecureX, on page 3
- Microsoft Azure, on page 3
- Cisco.com, on page 4
- URL Change, on page 5

New Portal

The look, feel, and usability of Cisco SecureX sign-on has been improved in its new portal. Choose your region of the world and launch into SecureX or any of your other Cisco Security products from the enhanced portal.

Cisco SecureX

Sign In to Cisco SecureX Using Cisco Security Cloud Sign On

Now you're able to sign in to Cisco SecureX using your Cisco Security Cloud Sign On account.

Microsoft Azure

Sign In to Cisco Secure Sign-On Using Your Microsoft Azure Account

Now you're able to sign in to Cisco Secure Sign-On using your Microsoft Azure account.

- Who can use this method?

  Customers who use Microsoft Azure as their organization's identity provider (IdP).

- What do I do to enable this method?

  Depending on the customer’s Microsoft Azure configuration, it works transparently for the organization. Otherwise, once the first user attempts access, an administrator needs to approve it in the Azure portal. For configuration details, go to the Microsoft Docs website and see their Azure documentation on these topics:

  - assign a user or group to an enterprise app
  - grant tenant-wide admin consent to an app
  - configure the admin consent workflow

- Does this pull user identity attributes from the customer's Microsoft Azure Active Directory (AD) profile?

  Yes, it pulls first name, last name, display name, title, mobile phone, and organization.

- Does this pull Azure group information and allow it to be recognized and used by applications secured by Cisco Secure Sign-On?

  No, group assignment and role permissions are handled by each Cisco application individually.

- Does this change the way I access applications that use Cisco Secure Sign-On?

  No, as long as you use the same username, you remain mapped into the applications just as before; it only changes the way you authenticate.

- Will I be able to keep and use both accounts?

  Yes and yes.

- How does this affect Cisco employees with an @cisco.com username?

  Cisco has not enabled Microsoft sign-in for @cisco.com accounts, so if you try to sign in using this method, you'll receive a failure message.

- What happens if I use the **Sign in with Microsoft** option, but I don't have a Cisco Secure Sign-On account?

  This will work transparently for you and allow you to sign in directly, without having to create a separate account.

Cisco.com

Sign In to Cisco Secure Sign-On Using Your Cisco.com Account

Now you're able to sign in to Cisco Secure Sign-On using your cisco.com account.

- How is this different than my Cisco Secure Sign-On account?

  This is your standard cisco.com account (formerly known as CCO), the same account used to access support, download software, and so on.

- Does this change the way I access applications that use Cisco Secure Sign-On?

  No, as long as you use the same username, you remain mapped into the applications just as before; it only changes the way you authenticate.

- Will I be able to keep and use both accounts?

  Yes and yes.

- How does this affect Cisco employees with an @cisco.com username?

Cisco employees are encouraged to use the **Sign in with Cisco.com** option, so that we can recognize them as an employee in our metrics and ensure that they receive only one MFA prompt.

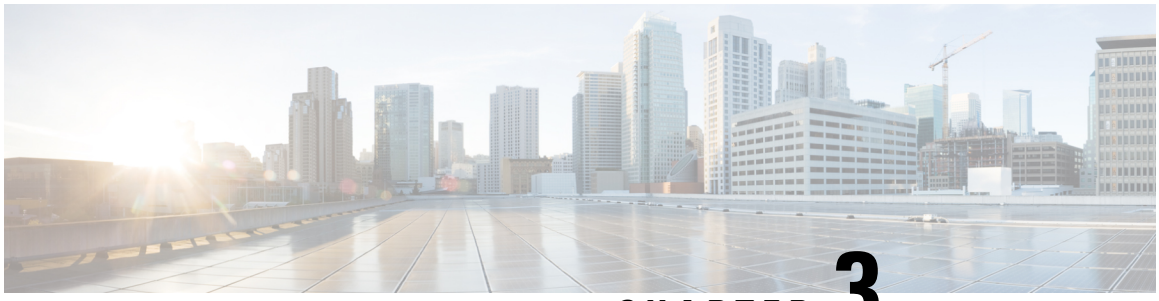
- What happens if I use the **Sign in with Cisco.com** option, but I don't have a Cisco Secure Sign-On account?

  This will work transparently for you and allow you to sign in directly, without having to create a separate account.

URL Change

URL Change

On March 24, 2020, the Cisco Secure Sign-On domain moved from security.cisco.com to sign-on.security.cisco.com to accommodate Cisco SecureX. Update your bookmark and password manager (such as LastPass, 1Password, or DashLane) to reference the new URL.



CHAPTER 3

Getting Started

- Signing in with Security Cloud Sign On, on page 7
- Creating a Security Cloud Sign On account, on page 7

Signing in with Security Cloud Sign On

Before you begin

You need to have a Security Cloud Sign On account to complete this procedure. See Creating a Security Cloud Sign On account, on page 7 for help creating an account.

Step 1 Open https://sign-on.security.cisco.com.

Step 2 If you have a Security Cloud Sign On account:

a) Enter your username, and click **Next**.

b) Enter your password, and click **Log in**.

c) Authenticate with Duo MFA or Google Authentication (if configured).

Or, to sign in with **Cisco** or **Microsoft** identity services, click **Other login options** and click the identity provider you want to authenticate with.

Creating a Security Cloud Sign On account

To create a Security Cloud Sign On account, you need to provide an email address where the account activation email will be sent. Every Security Cloud Sign On user account is required to use multifactor authentication (MFA). Duo MFA is included with Security Cloud Sign On account at no charge, or you can use a time-based one-time password from the Google Authenticator app.

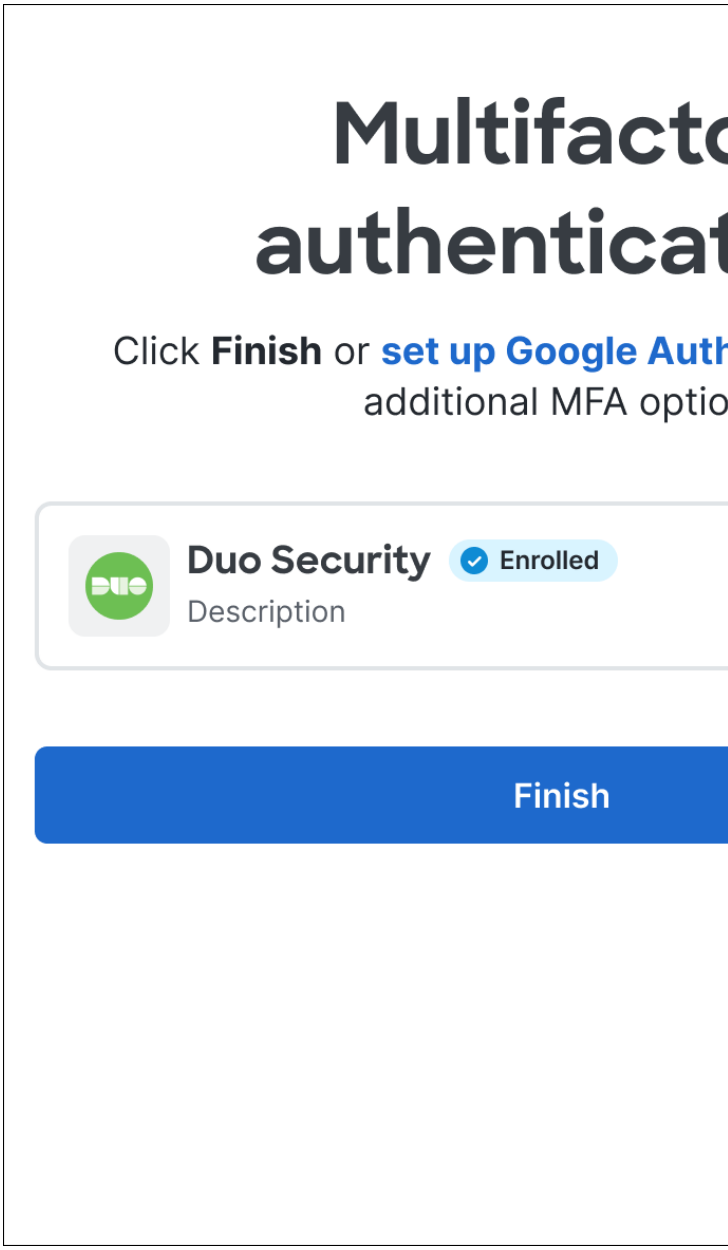
SUMMARY STEPS

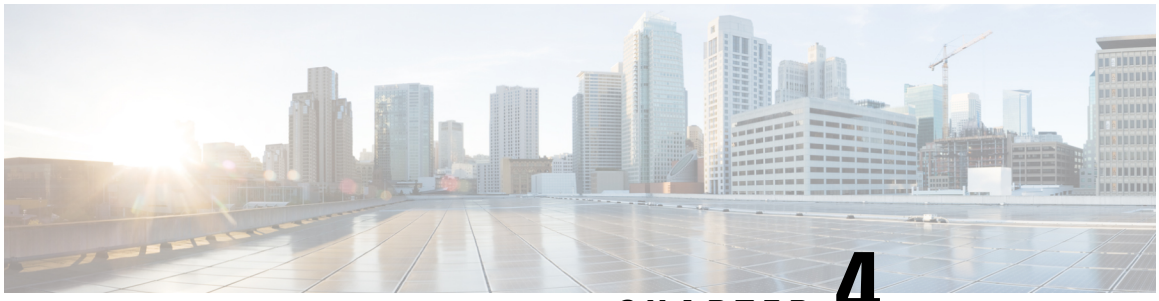
1. Open the Account Sign Up page.
2. Enter the requested information, agree to the end-user license agreement, and click **Sign up**.
3. Locate the "Activate Account" email from Cisco and click **Activate Account**.

4. Select a Duo multifactor authentication option (Touch, Duo Mobile, Security Key, or Phone Number) and complete the verification process. See Duo Guide to MFA and Device Enrollment for help.
5. Optionally, add additional authentication factors, or click **Skip for now**.
6. Click **Log in with Duo** and sign in using with your preferred authentication option.
7. Click **Finish** to finish sign in, or optionally click the link to add Google Authenticator as an additional MFA option.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Open the Account Sign Up page.	
Step 2	Enter the requested information, agree to the end-user license agreement, and click **Sign up**.	An activation email is sent to the address you provided.
Step 3	Locate the "Activate Account" email from Cisco and click **Activate Account**.	**Note** The activation link expires in 7 days.
Step 4	Select a Duo multifactor authentication option (Touch, Duo Mobile, Security Key, or Phone Number) and complete the verification process. See Duo Guide to MFA and Device Enrollment for help.	
Step 5	Optionally, add additional authentication factors, or click **Skip for now**.	
Step 6	Click **Log in with Duo** and sign in using with your preferred authentication option.	

	Command or Action	Purpose
Step 7	Click **Finish** to finish sign in, or optionally click the link to add Google Authenticator as an additional MFA option.	



CHAPTER 4

Supported Products

- Supported products, on page 11
- Supported products in emerging technology and incubation, on page 12

Supported products

This guide lists Cisco security products that support Security Cloud Sign On. Some products support Security Cloud Sign On by default and require no configuration changes. Other Cisco security products require you to opt-in to Security Cloud Sign On or migrate your users.

For each product listed below it's indicated if Security Cloud Sign On is enabled by default or requires you to opt-in or migrate your users. For products that require opt-in or user migration, links are provided to the relevant documentation.

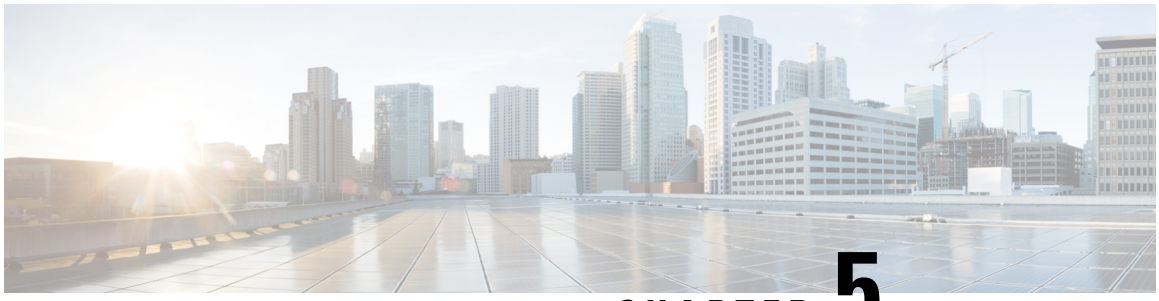
Product	Opt-in required?	Documentation
Cisco Cloudlock	**Yes**	Opt-in guide
Cisco Defense Orchestrator	**Yes**	Opt-in guide
Cisco Meraki	**Yes**	Opt-in guide
Cisco Secure Access	**No**	Secure Access Single Sign-On Authentication
Cisco Secure Cloud Analytics (formerly Stealthwatch Cloud)	**Yes**	Migration guide
Cisco Secure Email Threat Defense (formerly Cloud Mailbox)	**No**	N/A
Cisco Secure Endpoint (formerly Advanced Malware Protection for Endpoints)	**Yes**	Opt-in guide
Cisco Secure Malware Analytics (formerly Threat Grid)	**Yes**	Opt-in guide (requires sign in)
Cisco SecureX	**No**	N/A

Product	Opt-in required?	Documentation
Cisco Umbrella	**Yes**	Opt-in guide
Cisco XDR	**No**	N/A

Supported products in emerging technology and incubation

The following lists products in emerging technology and incubation that support Security Cloud Sign On.

Product	Opt-in required?	Documentation
Cisco Panoptica	**No**	N/A



CHAPTER 5

Frequently Asked Questions

• Frequently Asked Questions, on page 13

Frequently Asked Questions

Currently, I'm using OneLogin. What do I need to do to migrate to Security Cloud Sign On?

Go to the Security Cloud Sign On page, and click **Sign up now** to start the self-enrollment process.

How long is the account activation email valid?

Your account activation email is valid for 7 days from when it was sent.

How do I change my account password?

Note If you sign in to Security Cloud Sign On with your organization's SSO provider you can't change your password as described below. You need to change your password with your SSO provider.

To change your Security Cloud Sign On account password, click your profile icon SecureX App Dashboard in the top menu and select **User Identity Settings**. In the **Security** section, click **Change Password**. Enter your current password, your new password, click **Change Password**, and click **Save**.

Currently, I'm using Google Authenticator for multi-factor authentication. Will my ID get migrated?

No, your Google Authenticator MFA will not get migrated. All Security Cloud Sign On accounts are required to use Duo's MFA, as it allows calls and texts to hardware and software solutions. If you want to keep using Google Authenticator, you'll be able to add it as a backup factor for your account. During account activation, set up MFA with Duo (primary). Then, set up your additional MFA with Google Authenticator (backup).

Note Organizations that integrate their own identity provider with Security Cloud Sign On can opt-out of Duo MFA in favor of their own MFA solution.

Can I use my organization's Duo policies and settings for my Duo MFA?

Yes, if you integrate your own identity provider Security Cloud Sign On you can choose to opt-out of Duo MFA provided by Cisco in favor of your organization's Duo policies and settings.

What do I do if I've forgotten my password?

On the Security Cloud Sign On page, click **Need help signing in?** and **Forgot Password?**. You have three options to reset your password, in order of preference:

- Click **Reset via Duo**, authenticate to verify your identity, and enter your new password.
- Enter the mobile phone number you added to your account settings, and click **Reset via SMS**. Look for the SMS message, and follow the prompts.
- Enter your email or username, and click **Reset via Email**. Look for the email, and follow the prompts.

If these options are not available to you, please contact your Supported products team.

Is my password secure?

Yes, we provide rigorous security measures and controls to protect your information. These controls are audited and attested to in our SOC2 report.

Where and how is my username and password stored?

Just as we use strong encryption to secure your data, we use strong (256-bit AES) encryption for your username and password credentials as well.

What do I do if I have lost a phone that I was using to verify my identify with Duo?

If you have lost your phone, and can still sign in with your username and password, click **Settings** on the Duo verification page. Select **Add a new device** and follow the prompts to register your new replacement phone. For more information, see Duo Guide to Adding a New Device.

Why do I have to input my password for some apps and not others?

With Security Cloud Sign On, you can access your apps through a single, unified dashboard. Access to these apps is delivered through single sign-on (SSO) technology using Security Assertion Markup Language (SAML). With SAML, Security Cloud Sign On automatically passes access on through a token, so you don't need to manually make a change when the app requires an update.

How do I change my username and password for an existing app?

To change your existing password, hover your mouse pointer over the app's tile. On the upper-right corner of the tile, there's a gear icon. Click the gear icon to open the settings, and provide your current username and password to verify your identity. Once verified, you'll be able to enter a new password.

Can my administrator see my sign-in information?

Your administrator can see your username, but they do not have access to your password.

What do I do if I'm locked out of my account?

If your account is locked, click **Need help signing in?** and **Unlock Account** on the Security Cloud Sign On page. If these options are not available to you, please contact your Supported products team.

Why don't I see the security image sometimes?

The security image is a cookie that's set when you sign in. If the cookies in your browser have been cleared, you may not see the security image until the next time you sign in.

Why does my session expire but some of the apps are still open?

Although you may be logged out of your Security Cloud Sign On session, Security Cloud Sign On does not log you out of your apps.

How long does it take for the SecureX session token to expire?

The SecureX session token (JWT) expires after 24 hours.

What happens if Security Cloud Sign On goes down?

Security Cloud Sign On is built on an “Always-On” architecture. If the service was to go down, you would not be able to sign in and access your apps using single sign-on. However, you may still be able to access some apps through their direct link. If you cannot access Security Cloud Sign On and want to find out whether it's because of a service outage, please contact your Supported products team.

How do I delete an existing Cisco SecureX sign-on account?

Although product administrators can delete accounts to remove access to their individual product apps, you must contact Cisco TAC through your Supported products to have the Cisco SecureX sign-on engineering team delete the account for you.

My organization is already using an IdP for single sign-on. How do I integrate it with SecureX sign-on?

You may be able to "bring your own IdP" and integrate it with SecureX sign-on, so that you can access Cisco Security applications without having to manually recreate all your user accounts. For details, see the Cisco SecureX Sign-On Third-Party IdP Integration Guide.

Additional resources?

Please refer to these resources for additional information:

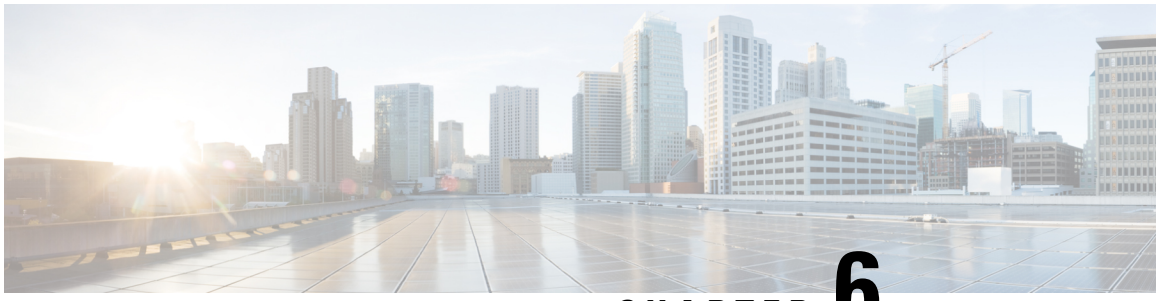
- Cisco SecureX sign-on product page
- Cisco SecureX sign-on privacy data sheet
- Cisco SecureX sign-on status page

Frequently Asked Questions

PART I

Appendix

- Export Applications, on page 19



CHAPTER 6

Export Applications

- Overview, on page 19
- Export Applications to Duo Access Gateway, on page 19
- Export Applications to Microsoft Azure, on page 20

Overview

The Export Applications page (accessed from your user profile menu on the SecureX App Dashboard) lists the Cisco Security product applications that you are able to access from Security Cloud Sign On. Next to each application are links to do the following:

- Copy the name of the application to your clipboard
- Copy the URL of the application to your clipboard
- Download the logo of the application to your computer

You can export Cisco Security product applications from here to your single sign-on (SSO) application portal: a landing page that presents a set of applications you can access with a single, common sign-on. Common SSO applications include Duo Access Gateway, Microsoft Azure, and Okta SSO, which allow you to sign in once and then access your applications with the same user identity and credentials. Use the links on the Export Applications page and the information in them to add and configure the application in your SSO application. This chapter describes the general process in two examples.

Export Applications to Duo Access Gateway

Follow these steps to add a bookmark in the Duo Access Gateway launcher to the Cisco Security product application.

Before you begin

- You must have access to the application in Cisco SecureX sign-on.
- You must have admin privileges in Duo Access Gateway.
- Set up and enable the Duo Access Gateway launcher: https://guide.duo.com/dag-launcher

Step 1 In the Duo Access Gateway admin console, click **Launcher**.

Step 2 Click **Bookmarks**.

Step 3 Click **Add a Bookmark**.

Step 4 Enter a **Name** for the app (**Copy Name** from the app on the Export Applications page).

Step 5 Enter a **URL** your users will use to access the app (**Copy URL** from the app on the Export Applications page).

Step 6 (Optional) Upload a **Logo** image for the app (**Download Logo** from the app on the Export Applications page).

Step 7 New bookmarks display to all users by default. You can use Duo groups to control which users see a bookmark. Check the **Only allow access from users in certain groups** or **Show this bookmark to only certain groups of users** box, and start typing in the group selection field to retrieve a list of Duo groups. Click each group that contains the users you want to see the new bookmark in the launcher.

Step 8 Click **Add** or **Save**.

Export Applications to Microsoft Azure

Follow these steps to add a Cisco Security product application to the Microsoft Azure portal.

Before you begin

- You must have access to the application in Cisco SecureX sign-on.
- You must have super admin privileges in Microsoft Azure.

Step 1 With super admin privileges, sign in to https://portal.azure.com.

Step 2 Click **Azure Active Directory**.

Step 3 On the left menu, choose **Enterprise applications**.

Step 4 Click **New application → Non-gallery application**.

Step 5 Enter a **Name** for the app (**Copy Name** from the app on the Export Applications page).

Step 6 (Optional) Upload a logo image for the app (**Download Logo** from the app on the Export Applications page).

Step 7 Click **Set up single sign on**.

Step 8 Choose **Linked**.

Step 9 Set **Sign on URL** to the URL you'll use to access the app (**Copy URL** from the app on the Export Applications page), and click **Save**.

Step 10 On the left menu for the app, click **Users and groups**.

Step 11 Assign users or groups to the app. Only assigned users will see the app when they access https://myapplications.microsoft.com.