Duo Cloud-based User Directory

Administrator Preview Testing Guide

Version 1.8 - Updated 03/30/2025

Overview

Duo continues to expand our access management offering. As part of this new preview, we are making available core functionality that will enable you to use Duo as a true identity provider (IdP), including:

- A cloud-based user directory with the ability create your own schema with custom attributes
- Password storage and management (enrollment and self-service resets)
- Expanded external directory integrations, now including Google and Okta

- Flexible passwordless integrations
- Automated provisioning into external applications

This program is the first preview of Duo's transition from an access management solution to a full-stack identity management solution, with the goal of achieving lower total cost of ownership, simpler management, and most importantly better security for our customers.

We have designed the features included in this preview for maximum deployment flexibility, allowing you to both use Duo as your primary identity provider or as value on top of your existing Identity and Access Management (IAM) stack.

We at Cisco Duo thank you in advance for your participation in this program and look forward to hearing from you about any feedback!

What Features are Available in this Preview

The following features are introduced through this preview. Click on the links to view vidcast overviews of each feature and the use cases they support.

- Duo Directory with custom attributes and password storage
- Enforcement of password change
- Passwordless new user enrollment
- Disable fallback to password and enforce passwordless-only
- Flexible temporary access in complete passwordless flow
- Dynamic routing rules for different authentication sources
- Sync users and groups from Okta with Inbound SCIM
- Sync users and groups from Google with directory sync
- Sync admins and automatically assign them Duo administrator roles with Google Admin Sync
- Granular enrollment policies for setting of authenticators and the password requirement
- Automated provisioning of users and groups into Microsoft 365, Google Cloud/Workspace, and SCIM supported applications

Use Cases

We have organized this document to support a few of the most common use cases we expect our customers to benefit from. Here are some brief descriptions of these use cases:

Duo Directory as your primary IdP

This use case supports customers that either do not have an existing IdP or are looking to migrate from their existing IdP to a more secure, easier to use solution: Duo Directory. The steps outline the process of creating your own custom user schema in Duo Directory, syncing users and groups from your existing identity infrastructure, configuring SSO applications, setting up password/passwordless and application policy, enrolling users, and ultimately confirming access for your users. Use these instructions if you plan on using Duo as your primary IdP.

Passwordless authentication with existing IdP and Complete Passwordless

Passwordless authentication reduces friction and improves security, and Duo Directory makes it easier than ever to deploy passwordless for your users and applications! We have previously limited our passwordless offering only to customers who have Microsoft Active Directory on premises. Now, you can use Duo's passwordless solution regardless who your existing IdP is, and of course, without any external IdP at all.

We are also introducing our 'Complete Passwordless' flow, which allows your users to enroll into Duo without ever creating a password!

Automate Provisioning of users and groups with supported applications

User lifecycle changes can make access management a daunting and potentially insecure task. Automated Provisioning aims to simplify this for our customers, allowing customers to use Duo to automatically provision, maintain and deprovision users and groups into supported downstream applications. Once groups are assigned to an application, Duo will automatically:

- Provision all members of that group to the application
- Create groups in the application, as well as propagate group name changes (if supported)
- Continue to provision new users to the application as they are added to provisioned groups, or deprovision users from the application if they are removed from a provisioned group
- Update user attributes for members of provisioned groups when any provisioned attribute is changed within Duo
- Deprovision all members of the group from the application if the group is ever removed from provisioning

This feature depends on the support enabled by your target applications, so some results may vary. This feature can be used whether you are using Duo as your primary IdP, or as value layered on top of your existing IAM stack.

View this vidcast to learn more about this feature.

Duo SSO and/or Passwordless for Microsoft 365 and Google

Microsoft 365 and Google Cloud/Workspace are hugely popular applications. Historically, Duo has required a customer to have a local Microsoft Active Directory in order to use either Duo SSO or Passwordless with either application. With Duo Directory, these limitations are no longer, and all customers can now utilize Duo SSO and Passwordless with either application!

For Google, the only requirement is to have a valid e-mail address (on a configured domain for Google) on each user record. For Microsoft 365, the automated provisioning feature must be used to create users on the federated domain.

View this vidcast to learn more about

Directory for Non-traditional/External Users

Many companies have non-traditional users that they wish to have access management capabilities for. Some examples include contractors, vendors, guest users, etc. These users may need access to many of the same applications that a traditional employee uses. This desire can be difficult to achieve with many existing identity solutions which may require all users to exist within the same limited set of domains.

With Duo Directory and our new Routing Rules functionality, it becomes easier than ever to provide access management for both your core and non-traditional users.

View this vidcast to learn more about this use case.

Use Case Instructions

The following sections illustrate recommended paths to achieve each of the aforementioned use cases. Follow the testing steps for your respective use case:

Use Case: Duo as the Primary Identity Provider

1. In-product guidance
2. Import/make users to Duo (link to Duo Documentation). Skip if already done
    a. Create Duo directory custom attributes
    b. Sync users and groups from Google with directory sync (optional)
    c. Sync users and groups from Okta with Inbound SCIM (optional)
    d. Sync admins and automatically assign them roles from Google with Admin Sync
3. Configure an SSO application
    a. Set up routing rules for multiple authentication sources
4. Review or edit policy (link to Duo Documentation)
5. Configure and apply an enrollment policy
6. Enforce a password change
7. Enroll a new user
    a. Enroll via a prior identity provider
    b. Enroll via enrollment codes
    c. Enroll via enrollment emails
8. Complete a password and 2FA or passwordless authentication

9. Check admin logs and authentication logs

Use Case: Passwordless Authentication with Existing Identity Provider and Complete Passwordless

1. Import/make users to Duo (link to Duo Documentation). Skip if already done
    a. Create Duo directory custom attributes
    b. Sync users and groups from Okta with Inbound SCIM (optional)
2. Configure an SSO application
    a. Set up routing rules for multiple authentication sources
3. Review or edit authentication method policy (link to Duo Documentation)
4. Configure an enrollment policy without a password requirement
5. Enroll a new user
    a. Enroll via a prior identity provider
    b. Enroll via enrollment codes
    c. Enroll via enrollment emails
6. Disable password fallback and enforce passwordless-only
7. Enable bypass code to unblock user access in a passwordless auth
    a. New configuration options for bypass code
    b. New user and admin notification for bypass code
8. Complete a passwordless authentication
9. Check admin logs and authentication logs

Notes: Refer to FAQs for more information about the setup with individual identity providers.

Use Case: Automate Provisioning of Users and Groups with supported applications

View this vidcast to learn more about this feature.

1. Import/make users to Duo (link to Duo Documentation). Skip if already done
    a. Create Duo directory custom attributes
    b. Sync users and groups from Google with directory sync (optional)
    c. Sync users and groups from Okta with Inbound SCIM (optional)
2. Create an SSO supported application
3. Set up provisioning into SCIM supported applications (optional)
4. Set up provisioning for Microsoft 365 (optional)
5. Set up provisioning for Google (optional)
6. View provisioning logs

Use Case: Use Duo SSO and/or Passwordless with Microsoft 365

If you would like to use Duo SSO and/or Passwordless with Microsoft 365 without an on-premises Active Directory, you must set up automated provisioning for Microsoft 365 for all users. This flow captures a specific attribute required to enable this authentication flow.

Certain attributes must exist on the user prior to setting up provisioning. These can be added within Duo, but we recommend syncing them in from Entra for any existing users. The attributes are: mail, mailNickname, userPrincipalName, and displayName

1. Import/make users to Duo (link to Duo Documentation). Skip if already done
   a. Create Duo directory custom attributes
   b. Sync users and groups from Google with directory sync (optional)
   c. Sync users and groups from Okta with Inbound SCIM (optional)
2. Sync any existing Microsoft 365 users from the domain you plan on federating into Duo
3. Create M365 SSO supported application
   a. Note: Ensure that the routing rule for is set to use Duo Directory for this application
4. Federate M365 domain to Duo in Entra
5. Disable Entra Directory Sync in Duo for the federated domain (if previously set up)
6. Set up provisioning for Microsoft 365
7. View provisioning logs (optional)
8. Configure policy to enable passwordless (if desired)

Use Case: Directory for Non-traditional/External Users

View this vidcast to learn more about this use case.

1. Import/make users to Duo (link to Duo Documentation). Skip if already done
   a. Create Duo directory custom attributes
   b. Sync users and groups from Google with directory sync (optional)
   c. Sync users and groups from Okta with Inbound SCIM (optional)
2. Configure an SSO application
   a. Set up routing rules for multiple authentication sources
   b. Note: Ensure that any application which you would like to make available for non-traditional users is routed to Duo. If you would like to share an application
3. Enroll a new user
   a. Enroll via a prior identity provider
   b. Enroll via enrollment codes
   c. Enroll via enrollment emails

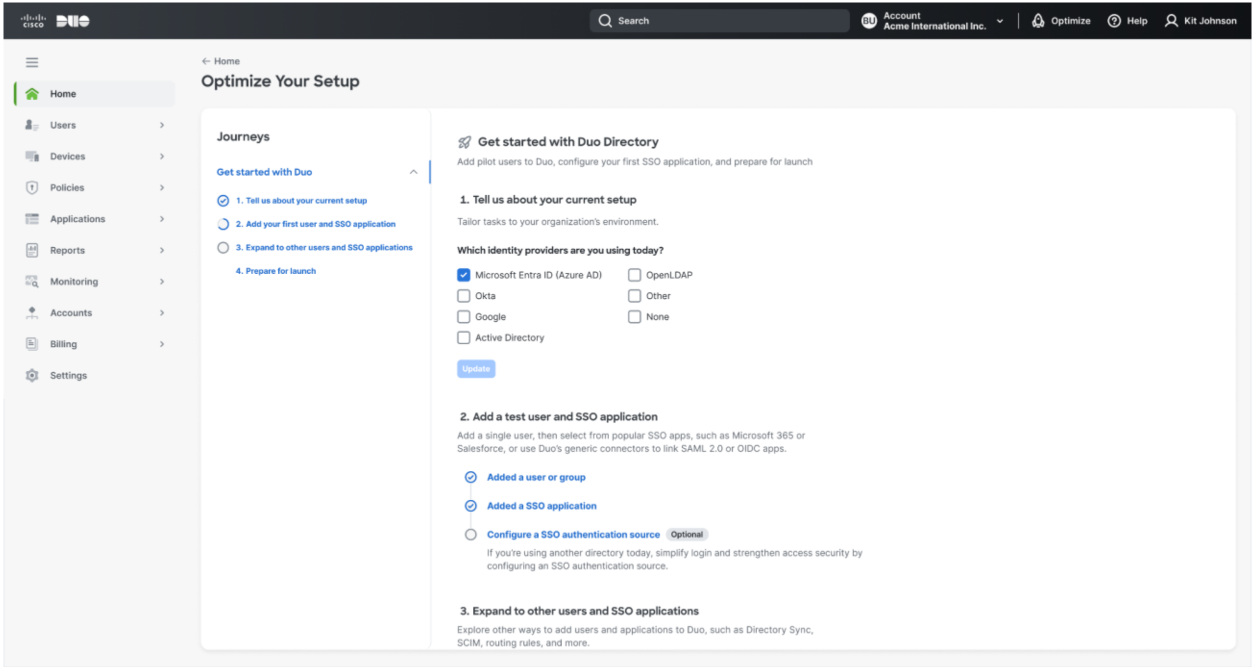
Feature Instructions

The following sections deliver instructions to test each feature available in the preview. These instructions can be used in support of the Use Case Instructions as outlined in the previous instructions, but also apply to general use of the feature.

In-product guidance

At any time, administrators can review steps in the product to enable Duo as their IdP. Steps will be marked complete once the action is done.

1. Log in to the Duo Admin Panel
2. Click **Optimize** in the header menu



Optimize Your Setup

Journeys

Get started with Duo

1. Tell us about your current setup
2. Add your first user and SSO application
3. Expand to other users and SSO applications
4. Prepare for launch

Get started with Duo Directory

Add pilot users to Duo, configure your first SSO application, and prepare for launch

1. Tell us about your current setup

Tailor tasks to your organization's environment.

Which identity providers are you using today?

☑ Microsoft Entra ID (Azure AD) ☐ OpenLDAP
☐ Okta ☐ Other
☐ Google ☐ None
☐ Active Directory

Update

2. Add a test user and SSO application

Add a single user, then select from popular SSO apps, such as Microsoft 365 or Salesforce, or use Duo's generic connectors to link SAML 2.0 or OIDC apps.

✓ Added a user or group
✓ Added a SSO application
○ Configure a SSO authentication source Optional
If you're using another directory today, simplify login and strengthen access security by configuring an SSO authentication source.

3. Expand to other users and SSO applications

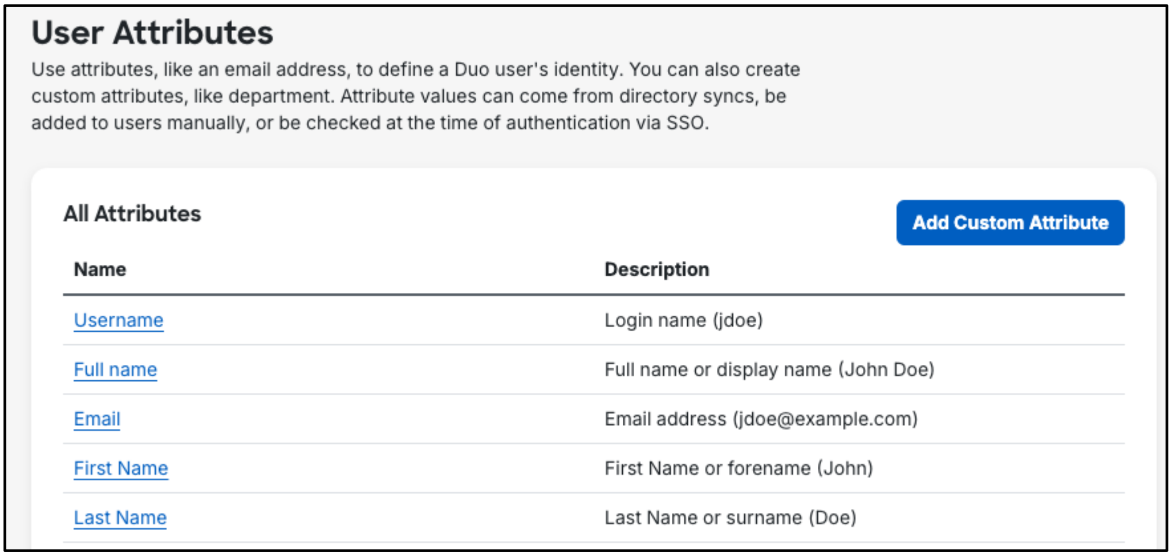
Explore other ways to add users and applications to Duo, such as Directory Sync, SCIM, routing rules, and more.

3. Complete required steps and review optional steps.

Create Duo Directory Custom Attributes

1. Locate **Users** in the left side bar and then click **User Attributes** on the submenu.

2. Click **Add Custom Attribute**



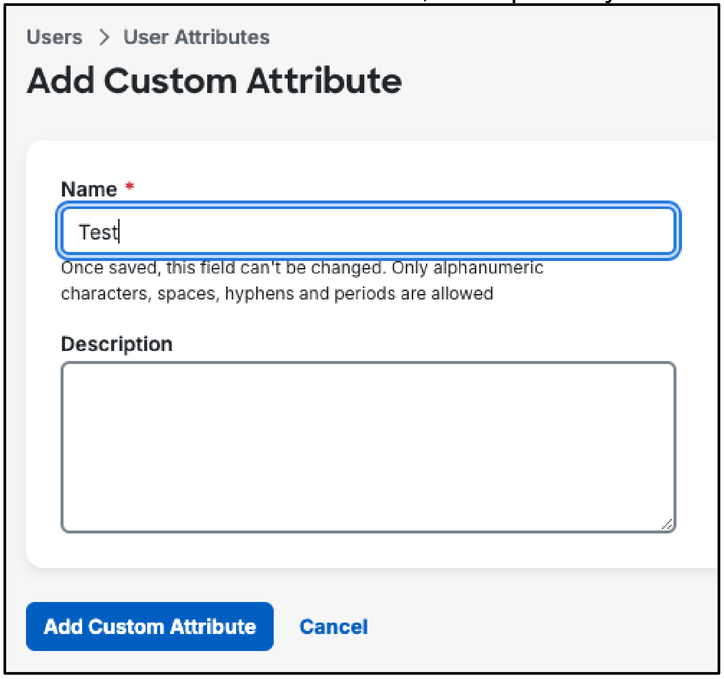
User Attributes

Use attributes, like an email address, to define a Duo user's identity. You can also create custom attributes, like department. Attribute values can come from directory syncs, be added to users manually, or be checked at the time of authentication via SSO.

All Attributes

Name	Description
Username	Login name (jdoe)
Full name	Full name or display name (John Doe)
Email	Email address (jdoe@example.com)
First Name	First Name or forename (John)
Last Name	Last Name or surname (Doe)

3. Enter a name in the ‘Name’ field, and optionally enter a description.



Users > User Attributes

Add Custom Attribute

Name *

Test

Once saved, this field can't be changed. Only alphanumeric characters, spaces, hyphens and periods are allowed

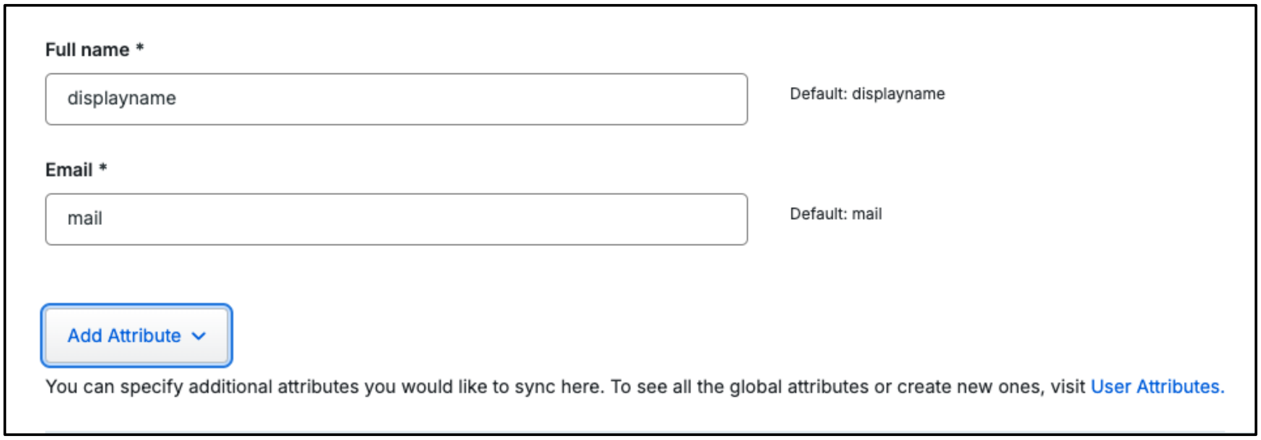
Description

4. Click **Add Custom Attribute** to complete

After you have created all of your attributes, you can use them throughout the Duo Admin Panel.

Use Custom Attributes in Directory Sync

1. In either a new or existing sync, scroll down until you see the **Add Attribute** button



Full name *

displayname

Default: displayname

Email *

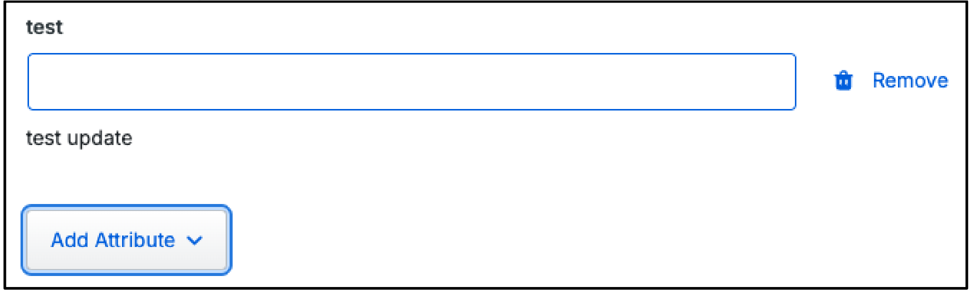
mail

Default: mail

Add Attribute ⌄

You can specify additional attributes you would like to sync here. To see all the global attributes or create new ones, visit User Attributes.

2. Click on the button and select the attribute you would like to add to the directory sync. In this example, we have chosen an attribute named ‘test’
3. The selected attribute will now appear above the button. Enter the source attribute name in the open text field.



test

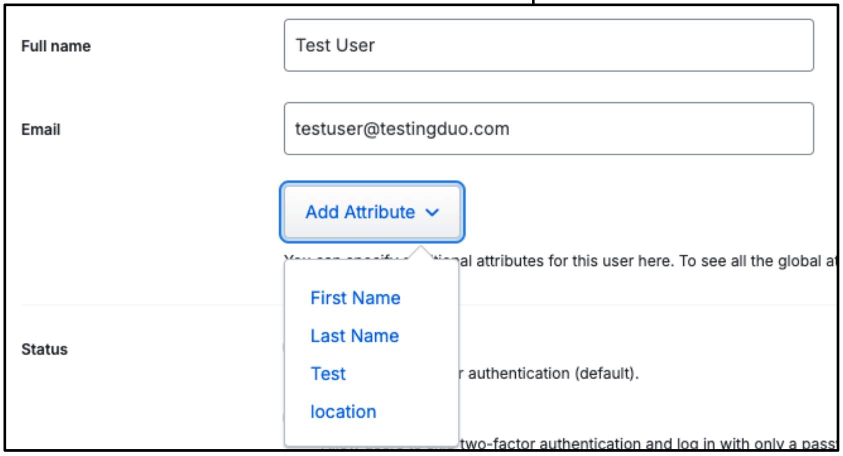
Remove

test update

Add Attribute ⌄

Add Custom Attributes to a Specific User

1. Navigate to the details page of a user by first clicking **Users** in the left navigation of the admin panel and then clicking on a specific user.
2. Scroll down until you see the **Add Attribute** button. Click this button.
3. Select an available attribute from the dropdown list.



Full name: Test User

Email: testuser@testingduo.com

Add Attribute ⌄

al attributes for this user here. To see all the global a

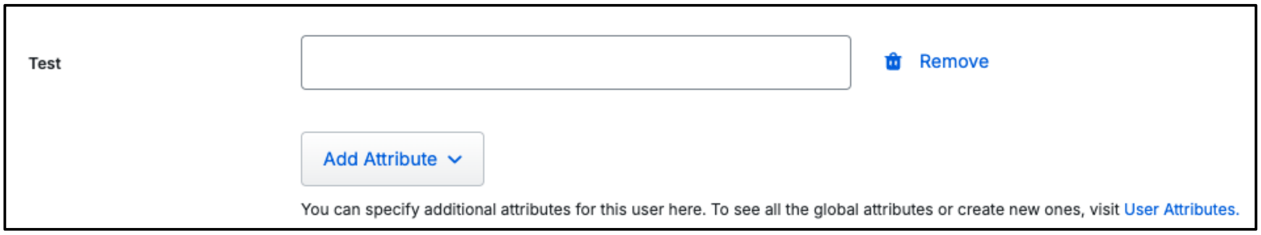
First Name
Last Name
Test
location

Status

r authentication (default).

two-factor authentication and log in with only a pass

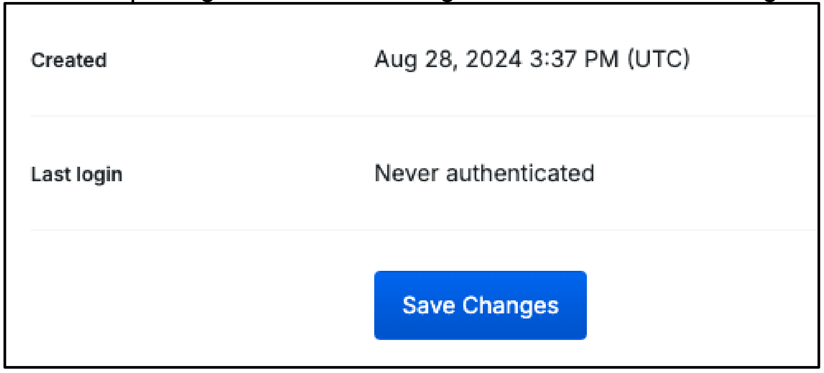
4. The selected attribute will then appear above the button, with an editable text box to manually enter a value.



Test

You can specify additional attributes for this user here. To see all the global attributes or create new ones, visit User Attributes.

5. After completing all attribute changes, click the Save Changes button



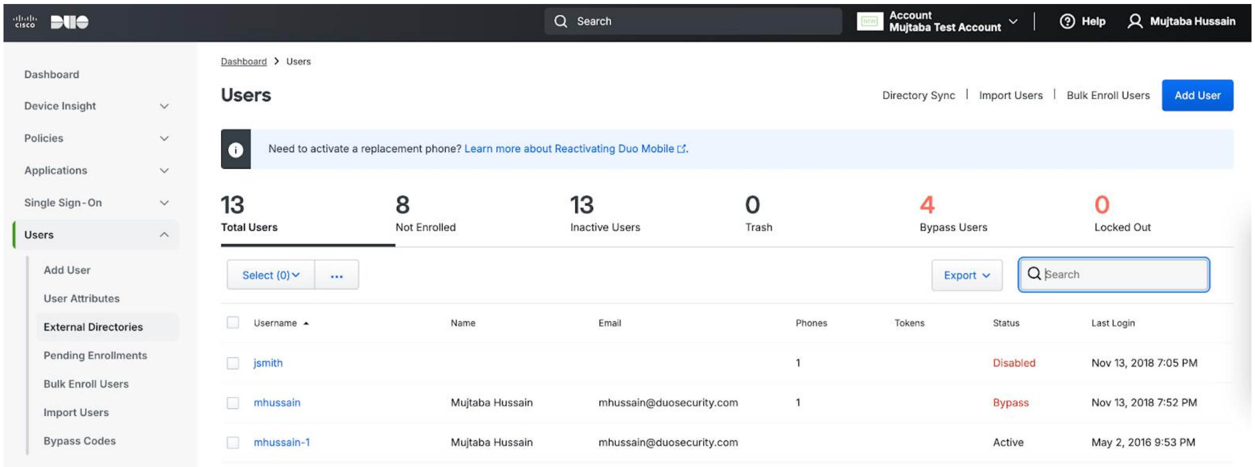
Created: Aug 28, 2024 3:37 PM (UTC)

Last login: Never authenticated

This process can also be followed for new users created in Duo.

Sync users and groups from Google with Directory Sync

1. Log in to the Duo Admin Panel.
2. Locate **Users** in the left side bar and then click **External Directories** on the submenu

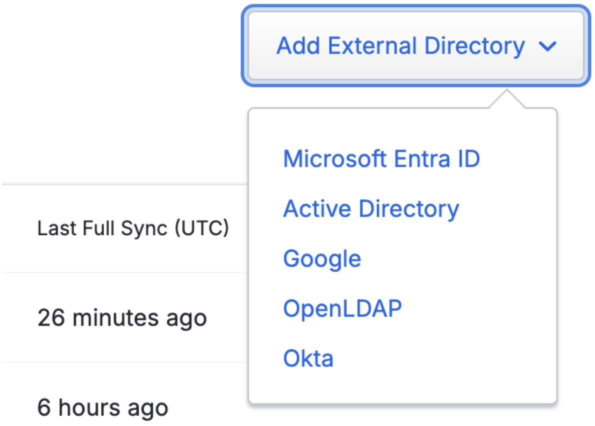


Need to activate a replacement phone? Learn more about Reactivating Duo Mobile.

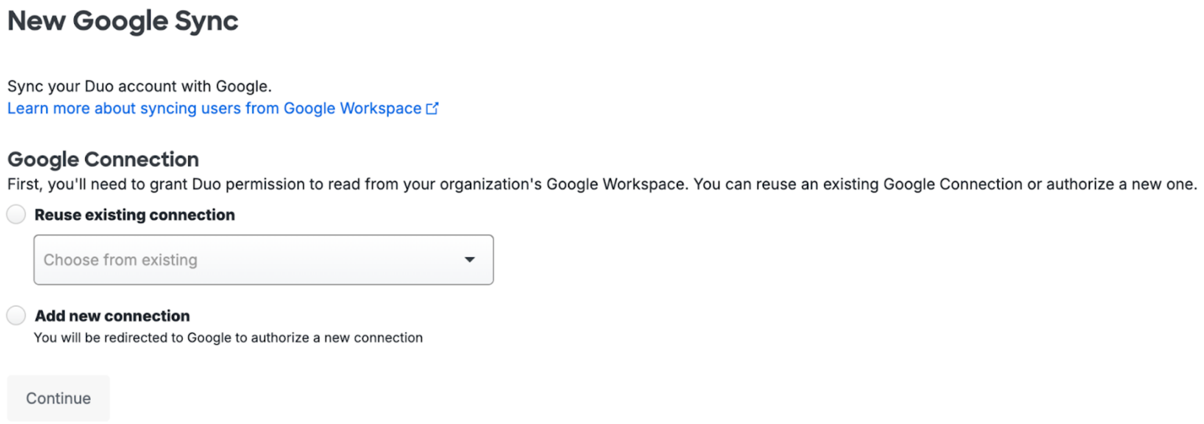
13	8	13	0	4	0
Total Users	Not Enrolled	Inactive Users	Trash	Bypass Users	Locked Out

Username	Name	Email	Phones	Tokens	Status	Last Login
jsmith			1		Disabled	Nov 13, 2018 7:05 PM
mhussain	Mujtaba Hussain	mhussain@duosecurity.com	1		Bypass	Nov 13, 2018 7:52 PM
mhussain-1	Mujtaba Hussain	mhussain@duosecurity.com			Active	May 2, 2016 9:53 PM

3. Click “Add External Directory” and select Google from the drop down menu



4. Select ‘Add new connection’ if you have not connected to Google from Duo before. If you have an existing connection, select ‘Reuse existing connection’ and select the desired connection name from the dropdown. The instructions in this guide will assume this is your first time connecting to Google. Click ‘Continue’ after you have made your selection.



New Google Sync

Sync your Duo account with Google.
Learn more about syncing users from Google Workspace

Google Connection

First, you'll need to grant Duo permission to read from your organization's Google Workspace. You can reuse an existing Google Connection or authorize a new one.

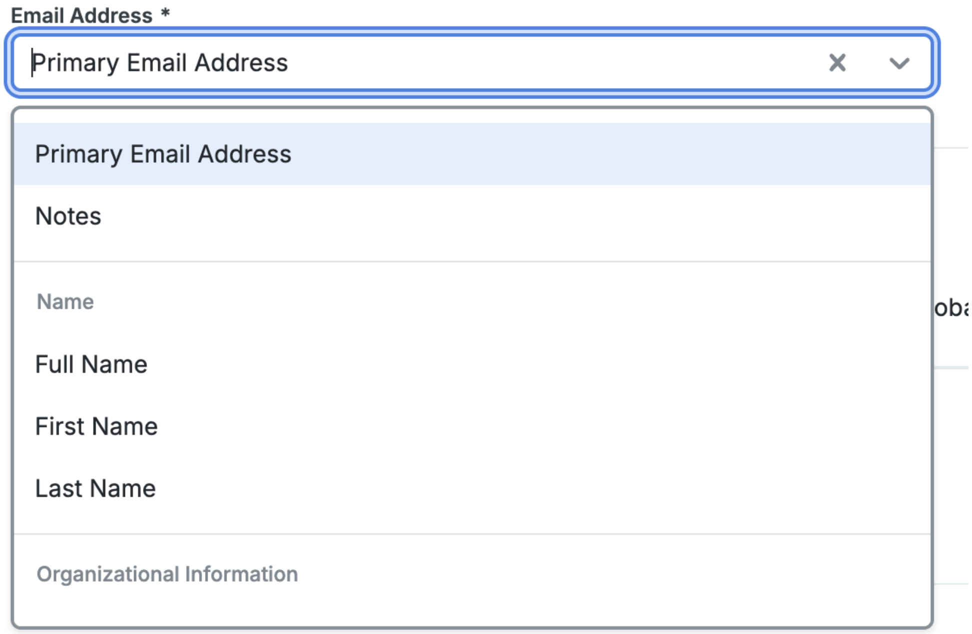
○ **Reuse existing connection**

Choose from existing ▾

○ **Add new connection**
You will be redirected to Google to authorize a new connection

Continue

5. Sign-in to your Google Workspace administrator account, and authorize the requested permissions
6. The name of your directory sync will automatically update from ‘New Google Sync’ to your Google account’s organization name. If you want to change the name of your sync, click ‘Rename’ and enter the new value.
7. Assign either individual users or groups of users from your Google organization for syncing. You can assign up to 50 individual users (separated by commas), and unlimited groups for syncing. For groups, click the drop down arrow to see your available groups, and select the desired group – repeat until you have captured all of your desired groups.
8. Specify which attributes you want to retrieve from Google. You must make a selection for username, e-mail address and display name. Optionally, you can add additional Duo attributes by clicking the ‘Add Attributes’ button and choosing from your Duo user schema. For each attribute, select the dropdown and you will be presented with a list of all attributes that Duo was able to retrieve from your Google account.



Email Address *

Primary Email Address ✕ ⌄

Primary Email Address

Notes

Name

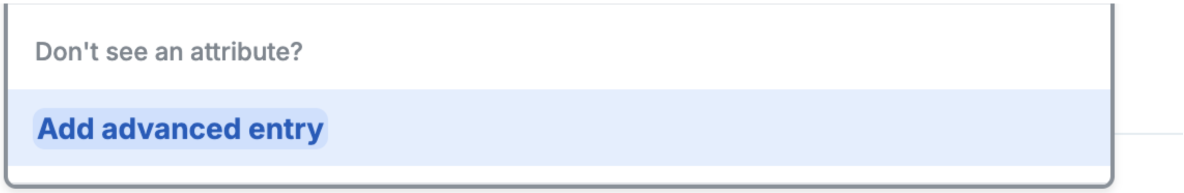
Full Name

First Name

Last Name

Organizational Information

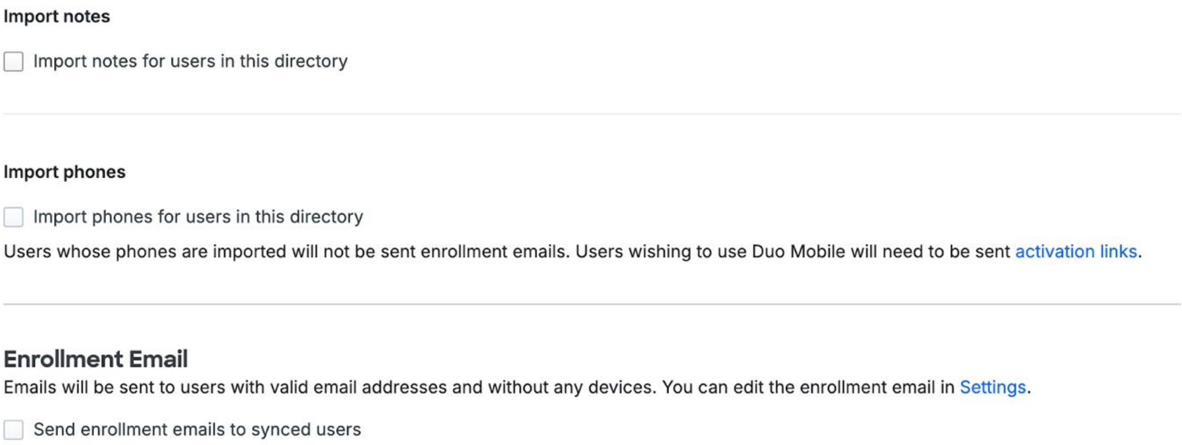
If an attribute you wish to desire is not in the list, scroll to the bottom of the dropdown and select ‘Add advanced entry.’ Follow the steps to add the missing attribute.



Don't see an attribute?

Add advanced entry

9. Optionally, you can choose to import notes, import phones and/or send enrollment e-mails to synced users. If you choose to import phones, all phone numbers stored in Google will be retrieved.



Import notes

□ Import notes for users in this directory

Import phones

□ Import phones for users in this directory

Users whose phones are imported will not be sent enrollment emails. Users wishing to use Duo Mobile will need to be sent activation links.

Enrollment Email

Emails will be sent to users with valid email addresses and without any devices. You can edit the enrollment email in Settings.

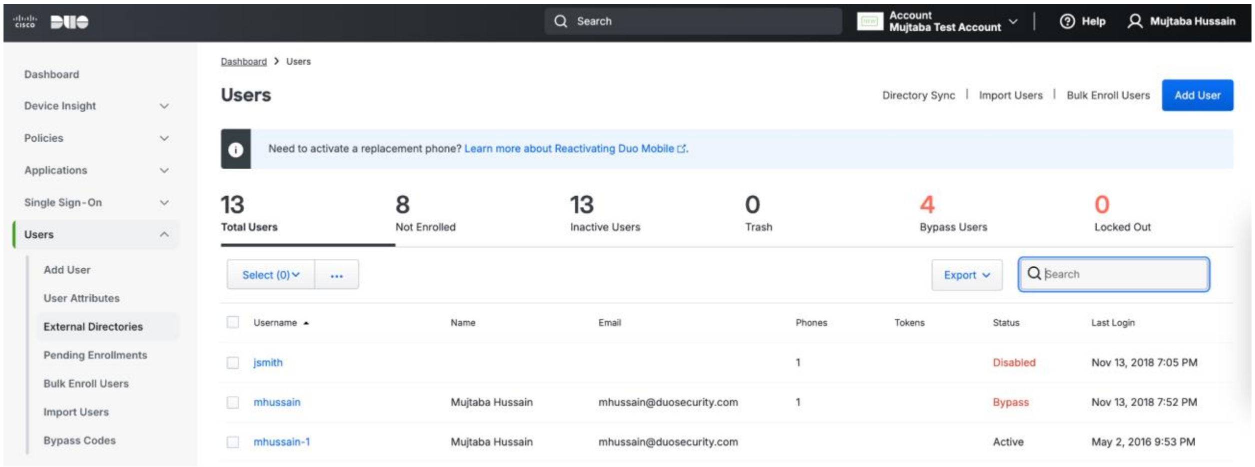
□ Send enrollment emails to synced users

Sync users and groups from Okta with Inbound SCIM

Enable SCIM in Duo

To start setting up SCIM:

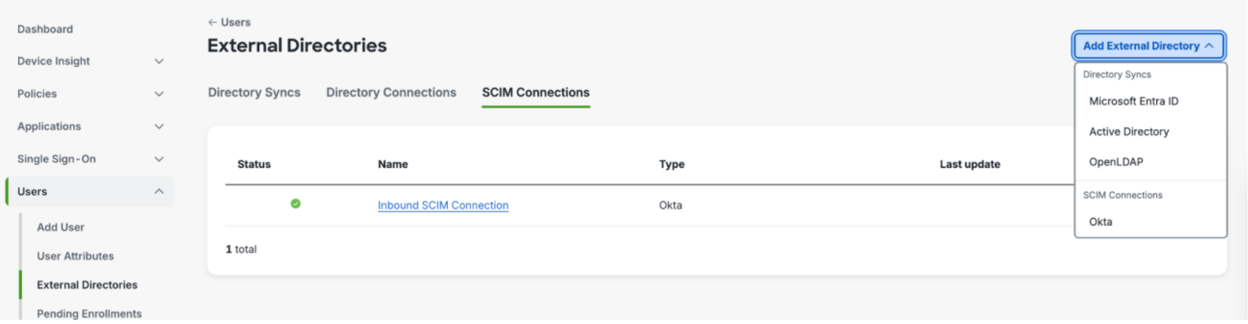
1. Log in to the Duo Admin Panel.
2. Locate **Users** in the left side bar and then click **External Directories** on the submenu



Need to activate a replacement phone? Learn more about Reactivating Duo Mobile.

□	Username ▲	Name	Email	Phones	Tokens	Status	Last Login
□	jsmith			1		Disabled	Nov 13, 2018 7:05 PM
□	mhussain	Mujtaba Hussain	mhussain@duosecurity.com	1		Bypass	Nov 13, 2018 7:52 PM
□	mhussain-1	Mujtaba Hussain	mhussain@duosecurity.com			Active	May 2, 2016 9:53 PM

3. Click “Add External Directory” and select Okta from the drop down menu

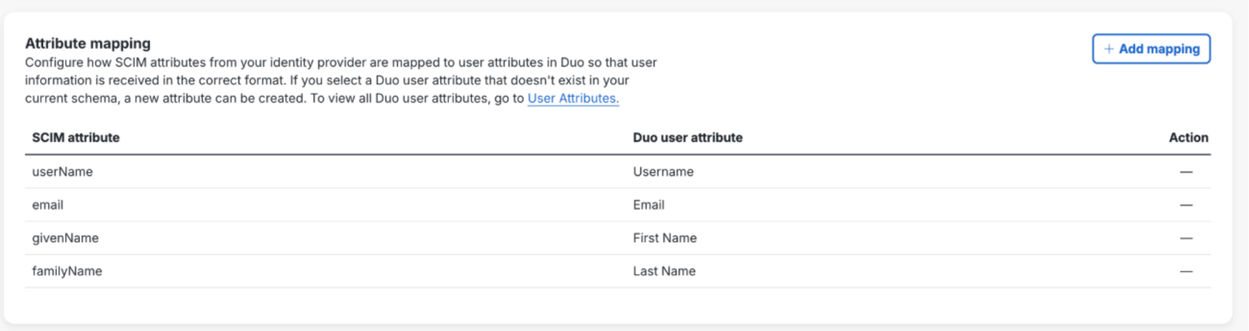


Status	Name	Type	Last update
●	Inbound SCIM Connection	Okta	

1 total

4. Review the Attribute Mapping section to make sure all of the attributes you want to bring in from Okta are included. Username, email address, first name and last name are

required attributes.

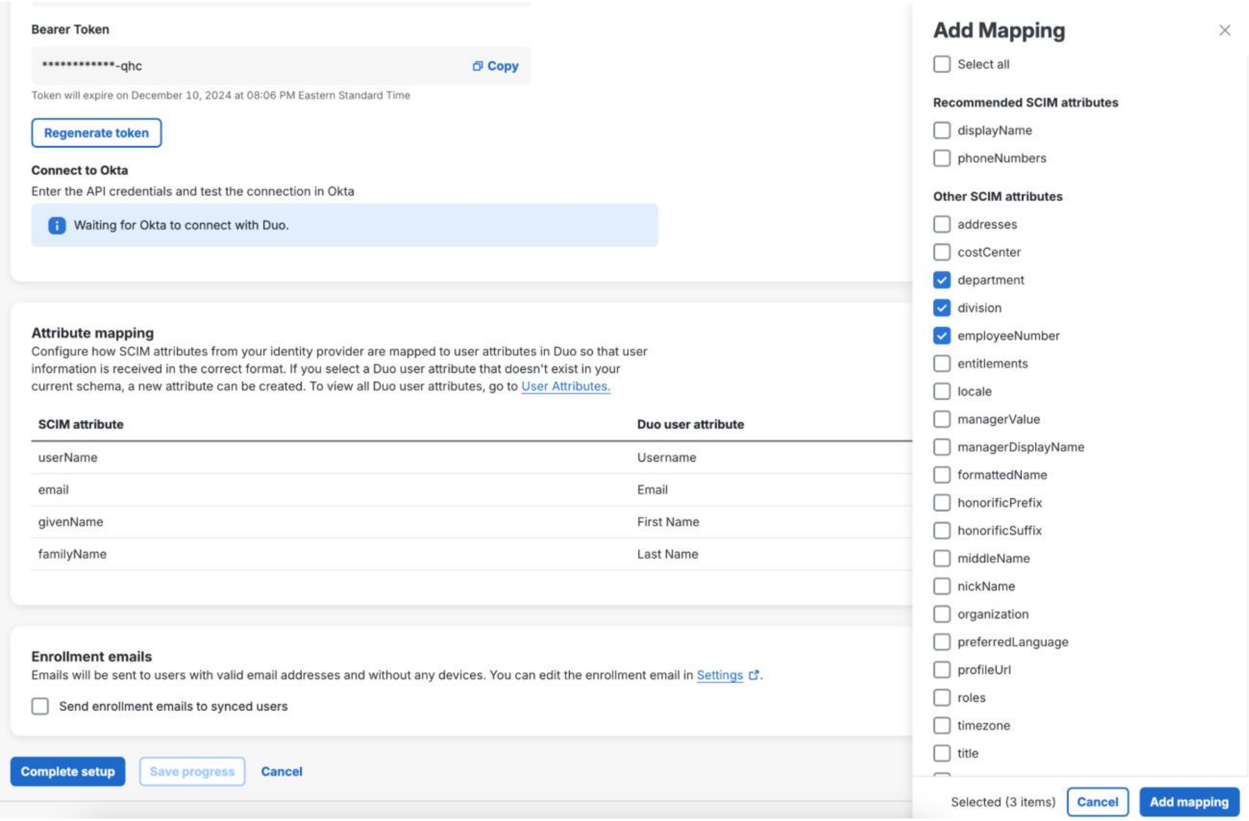


Attribute mapping

Configure how SCIM attributes from your identity provider are mapped to user attributes in Duo so that user information is received in the correct format. If you select a Duo user attribute that doesn't exist in your current schema, a new attribute can be created. To view all Duo user attributes, go to User Attributes.

SCIM attribute	Duo user attribute	Action
userName	Username	—
email	Email	—
givenName	First Name	—
familyName	Last Name	—

5. If you want to bring in additional attributes, click the '+ Add Mapping' button and click the check boxes next to the attributes you want to add. Click the blue 'Add Mapping' button to complete.



Bearer Token

*************-qhc

Token will expire on December 10, 2024 at 08:06 PM Eastern Standard Time

Connect to Okta

Enter the API credentials and test the connection in Okta

Waiting for Okta to connect with Duo.

Attribute mapping

Configure how SCIM attributes from your identity provider are mapped to user attributes in Duo so that user information is received in the correct format. If you select a Duo user attribute that doesn't exist in your current schema, a new attribute can be created. To view all Duo user attributes, go to User Attributes.

SCIM attribute	Duo user attribute
userName	Username
email	Email
givenName	First Name
familyName	Last Name

Enrollment emails

Emails will be sent to users with valid email addresses and without any devices. You can edit the enrollment email in Settings.

☐ Send enrollment emails to synced users

Add Mapping

☐ Select all

Recommended SCIM attributes

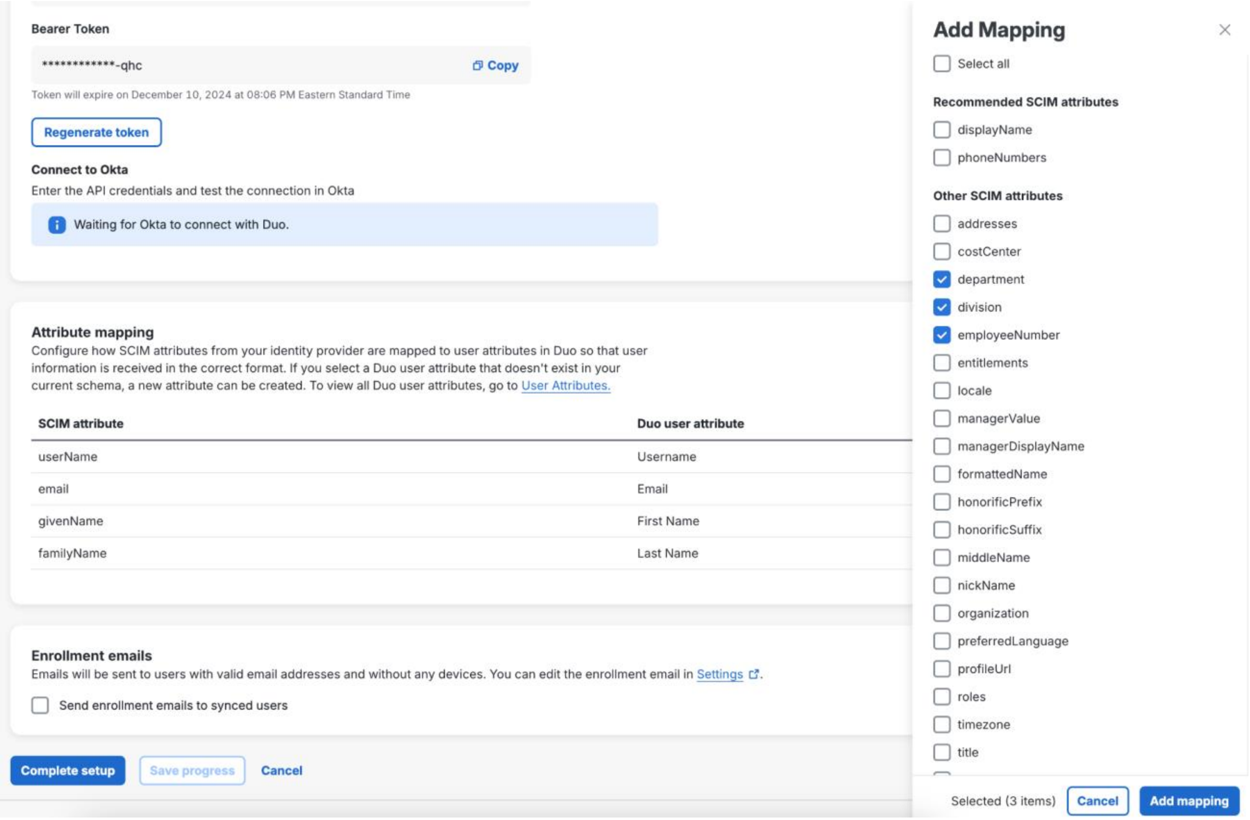
☐ displayName
☐ phoneNumbers

Other SCIM attributes

☐ addresses
☐ costCenter
☑ department
☑ division
☑ employeeNumber
☐ entitlements
☐ locale
☐ managerValue
☐ managerDisplayName
☐ formattedName
☐ honorificPrefix
☐ honorificSuffix
☐ middleName
☐ nickName
☐ organization
☐ preferredLanguage
☐ profileUrl
☐ roles
☐ timezone
☐ title

Selected (3 items)

6. For each added attribute, select which Duo User Attribute you want to store the synced attribute into. You can select among existing attributes by clicking the dropdown arrow, or you can create a new user attribute on the fly by typing in the desired attribute name.



Bearer Token

*************-qhc Copy

Token will expire on December 10, 2024 at 08:06 PM Eastern Standard Time

Regenerate token

Connect to Okta

Enter the API credentials and test the connection in Okta

Waiting for Okta to connect with Duo.

Attribute mapping

Configure how SCIM attributes from your identity provider are mapped to user attributes in Duo so that user information is received in the correct format. If you select a Duo user attribute that doesn't exist in your current schema, a new attribute can be created. To view all Duo user attributes, go to User Attributes.

SCIM attribute	Duo user attribute
userName	Username
email	Email
givenName	First Name
familyName	Last Name

Enrollment emails

Emails will be sent to users with valid email addresses and without any devices. You can edit the enrollment email in Settings.

□ Send enrollment emails to synced users

Complete setup | Save progress | Cancel

Add Mapping

□ Select all

Recommended SCIM attributes

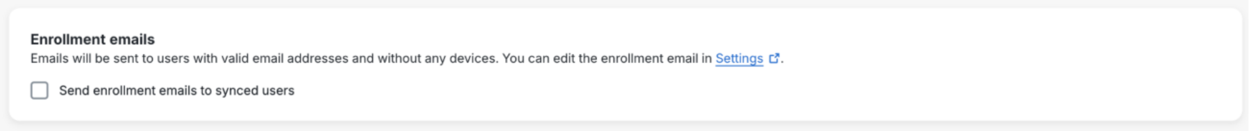
□ displayName
□ phoneNumbers

Other SCIM attributes

□ addresses
□ costCenter
☑ department
☑ division
☑ employeeNumber
□ entitlements
□ locale
□ managerValue
□ managerDisplayName
□ formattedName
□ honorificPrefix
□ honorificSuffix
□ middleName
□ nickName
□ organization
□ preferredLanguage
□ profileUrl
□ roles
□ timezone
□ title

Selected (3 items) Cancel Add mapping

7. Optionally, you can choose to send enrollment emails by clicking the checkbox.



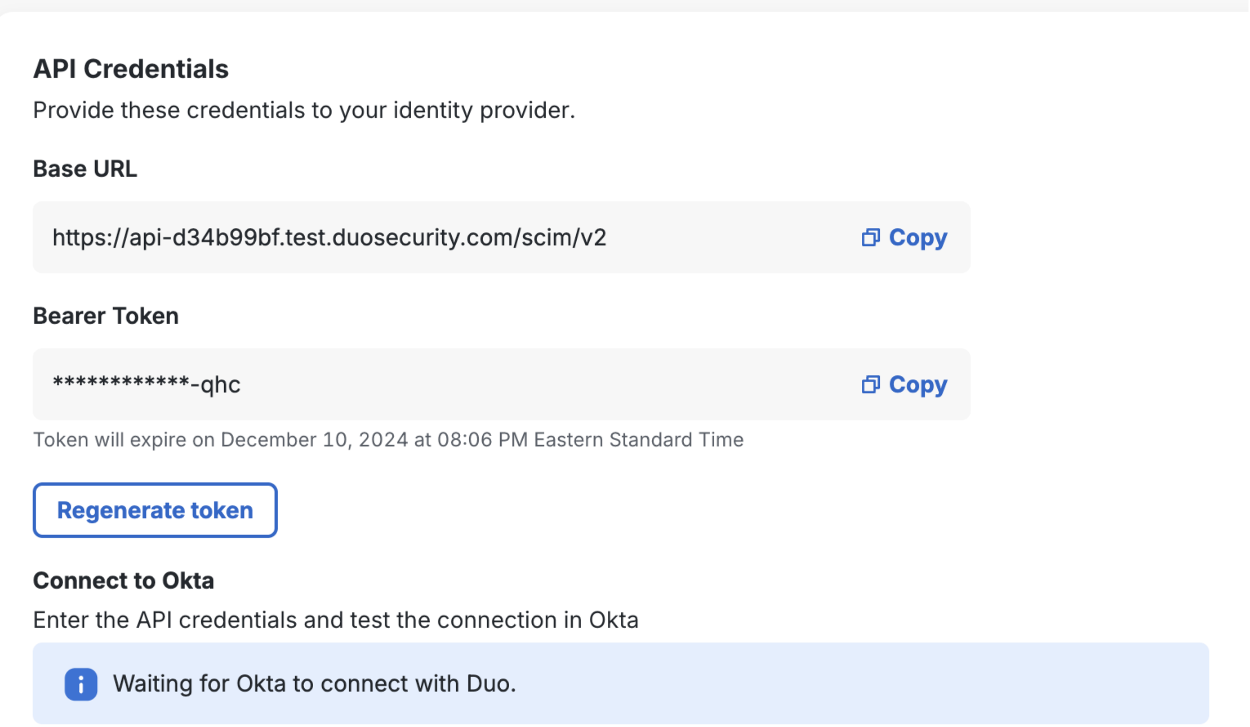
Enrollment emails

Emails will be sent to users with valid email addresses and without any devices. You can edit the enrollment email in Settings.

□ Send enrollment emails to synced users

8. Click the ‘Complete Setup’ button and proceed to configuring SCIM in Okta.

   Note: you will need to copy the API Credentials from the Duo Admin Panel and paste in Okta as part of the Okta configuration.



API Credentials

Provide these credentials to your identity provider.

Base URL

https://api-d34b99bf.test.duosecurity.com/scim/v2

Bearer Token

************-qhc

Token will expire on December 10, 2024 at 08:06 PM Eastern Standard Time

Connect to Okta

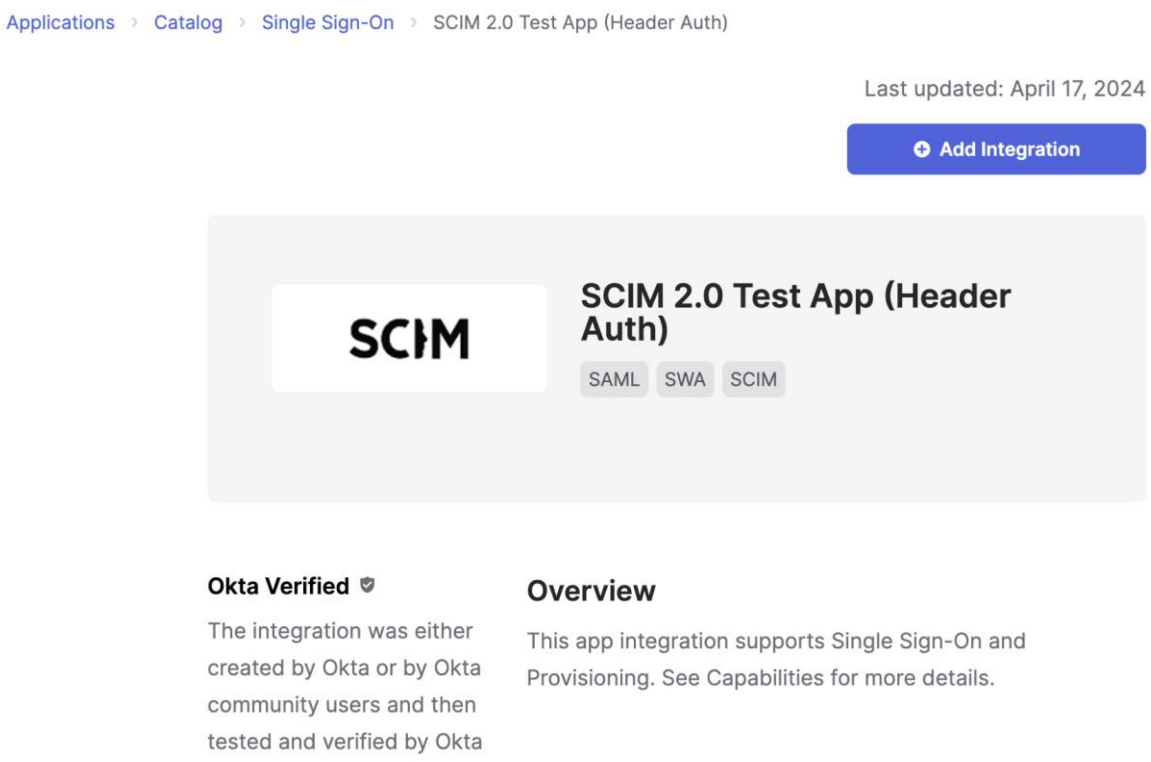
Enter the API credentials and test the connection in Okta

Waiting for Okta to connect with Duo.

Configure SCIM in Okta

1. Log in to the Okta's Admin Console and click **Applications** in the navigation bar on the left, then click Applications again in the submenu.

2. Select **Browse Application Catalog** and search for 'SCIM 2.0 test app (header auth)'. Select **Add Integration.**



Applications › Catalog › Single Sign-On › SCIM 2.0 Test App (Header Auth)

Last updated: April 17, 2024

SCIM 2.0 Test App (Header Auth)

SAML SWA SCIM

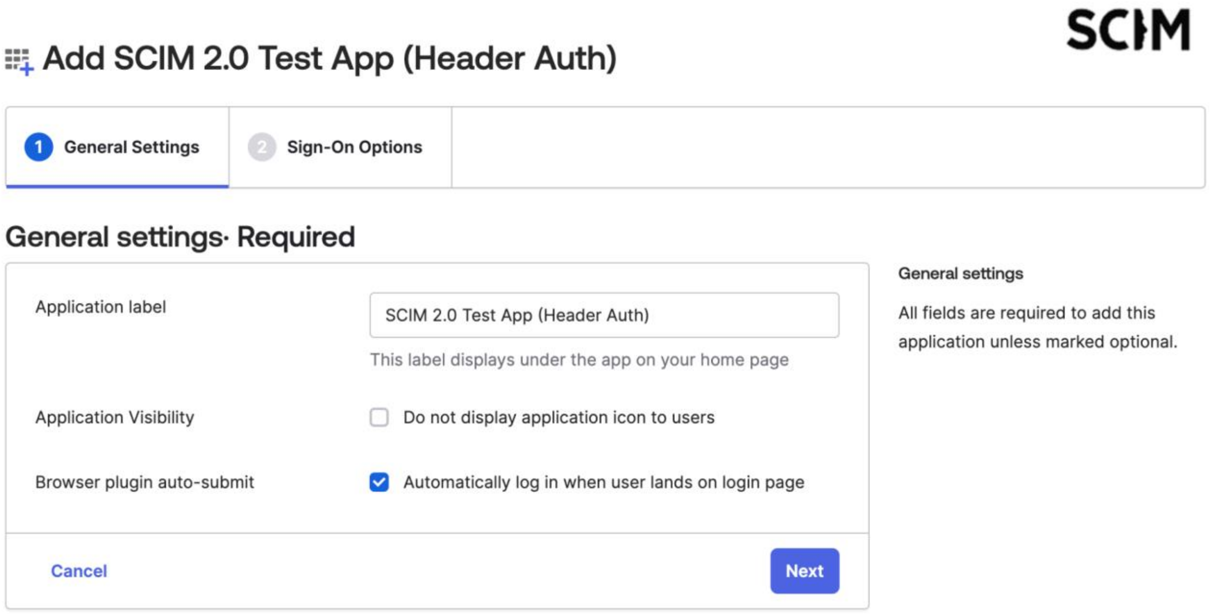
Okta Verified

The integration was either created by Okta or by Okta community users and then tested and verified by Okta

Overview

This app integration supports Single Sign-On and Provisioning. See Capabilities for more details.

3. Leave **General Settings** and **Sign-On Options** as the defaults, optionally giving a custom 'Application label'



Add SCIM 2.0 Test App (Header Auth)

General settings· Required

Application label: SCIM 2.0 Test App (Header Auth)

This label displays under the app on your home page

Application Visibility: □ Do not display application icon to users

Browser plugin auto-submit: ☑ Automatically log in when user lands on login page

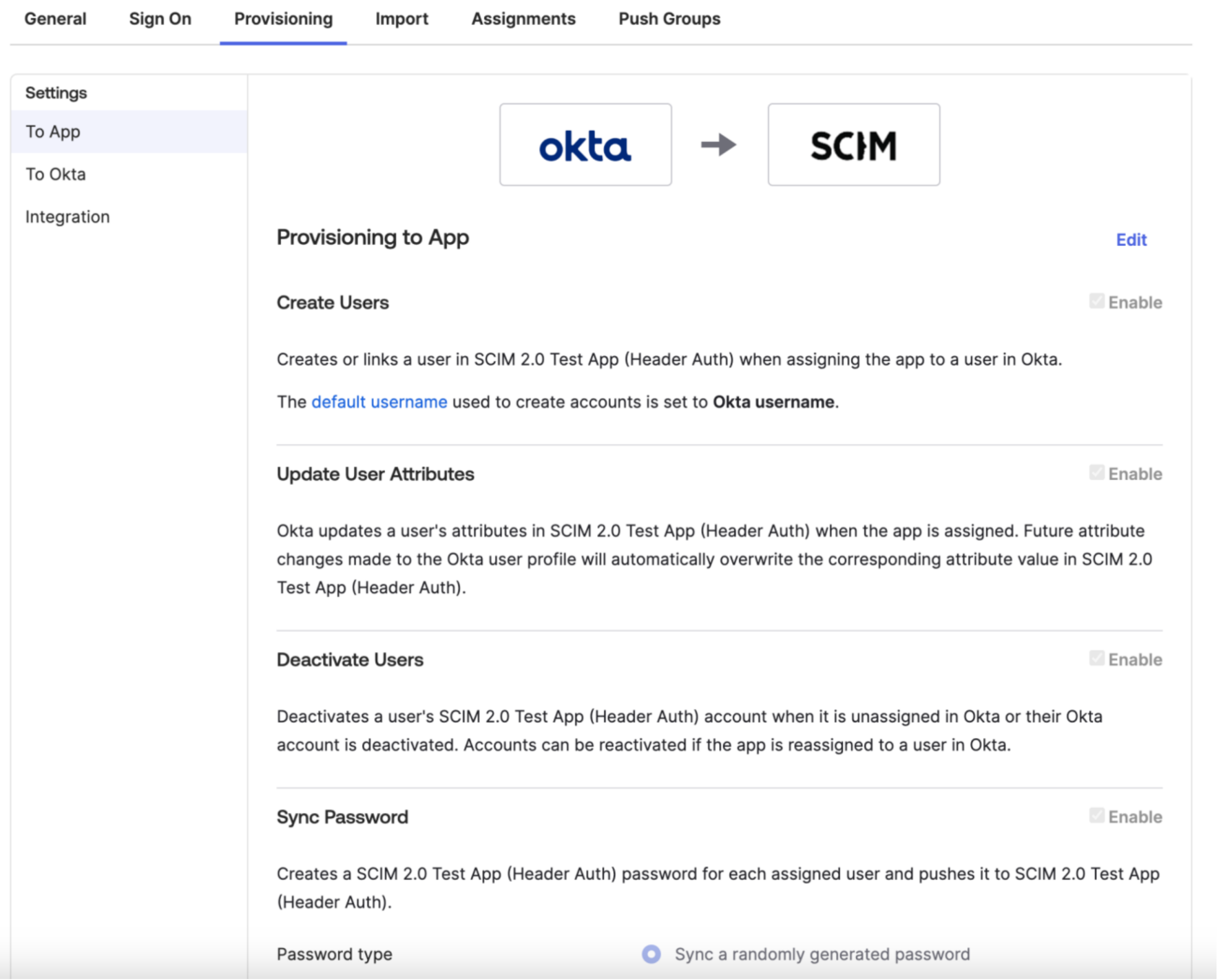
General settings

All fields are required to add this application unless marked optional.

4. Go to **Provisioning** tab
   c. Click **Configure API Integration**
   d. Click **Enable API integration**
   e. Add the **API hostname** from your Duo admin panel as the **Base URL**

f. Add the **API Token** from your Duo admin panel as the **Bearer Token**
g. Click **Save**

5. You should automatically return to the **Provisioning** tab. In the ‘To App’ section, click Edit, and enable the options of your choosing. We recommend enabling all, though Duo will not do anything with the passwords.



Provisioning to App

Create Users ☑ Enable

Creates or links a user in SCIM 2.0 Test App (Header Auth) when assigning the app to a user in Okta.

The default username used to create accounts is set to **Okta username**.

Update User Attributes ☑ Enable

Okta updates a user's attributes in SCIM 2.0 Test App (Header Auth) when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in SCIM 2.0 Test App (Header Auth).

Deactivate Users ☑ Enable

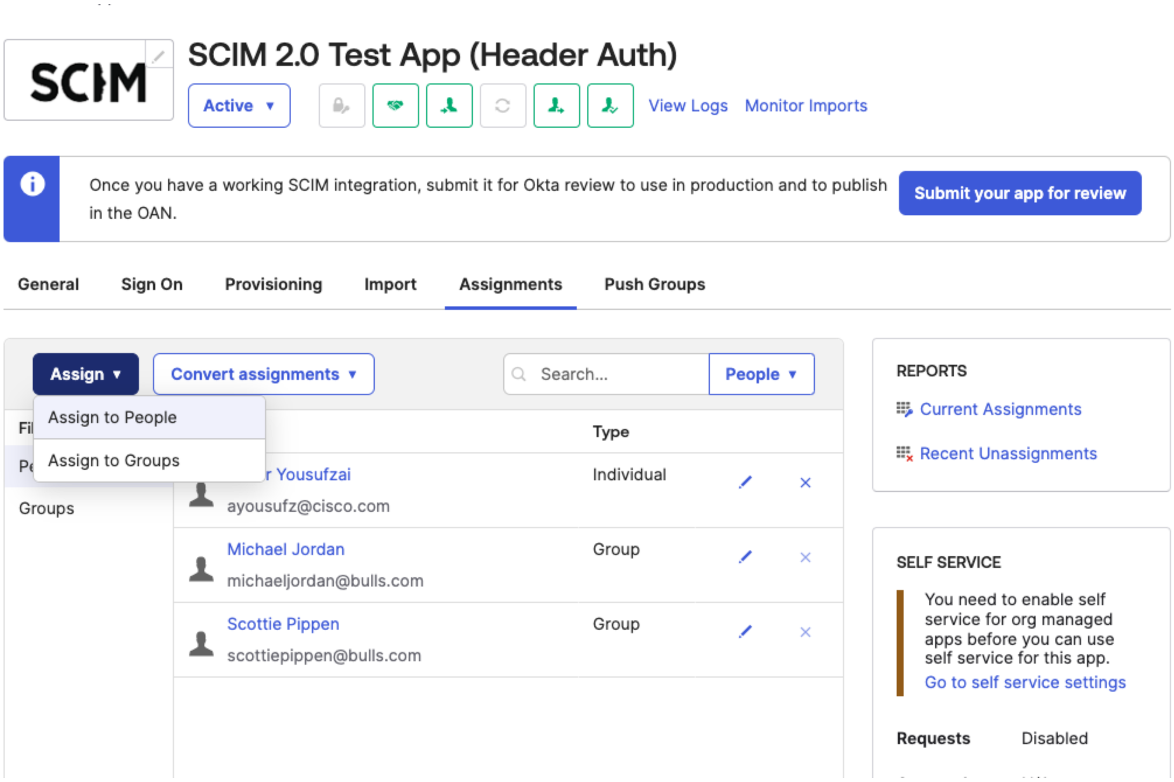
Deactivates a user's SCIM 2.0 Test App (Header Auth) account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

Sync Password ☑ Enable

Creates a SCIM 2.0 Test App (Header Auth) password for each assigned user and pushes it to SCIM 2.0 Test App (Header Auth).

Password type ● Sync a randomly generated password

6. To assign users, go to Assignments > Assign > Assign to People



SCIM 2.0 Test App (Header Auth)

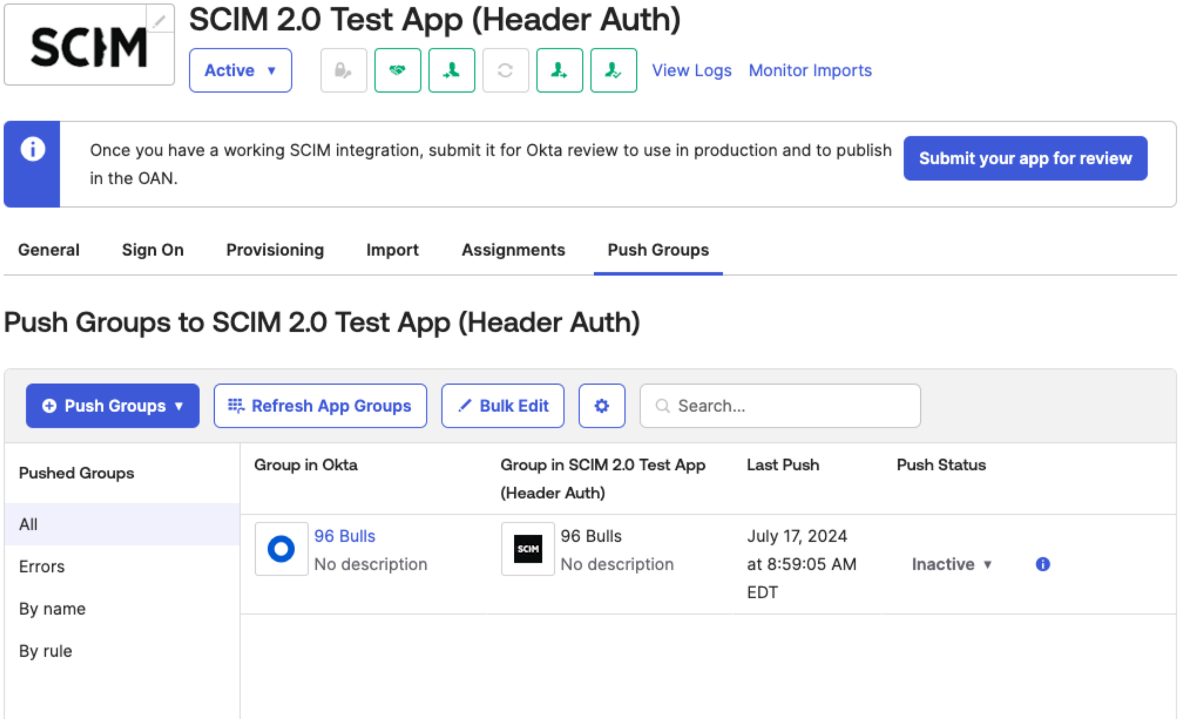
Once you have a working SCIM integration, submit it for Okta review to use in production and to publish in the OAN.

	Type
r Yousufzai ayousufz@cisco.com	Individual
Michael Jordan michaeljordan@bulls.com	Group
Scottie Pippen scottiepippen@bulls.com	Group

You need to enable self service for org managed apps before you can use self service for this app.

Requests Disabled

7. To assign a group, go to Assignments > Assign > Assign to Group. After assigning the group, go to Push Groups > + Push Groups > Find Groups by Name and add your Okta group



SCIM 2.0 Test App (Header Auth)

Once you have a working SCIM integration, submit it for Okta review to use in production and to publish in the OAN.

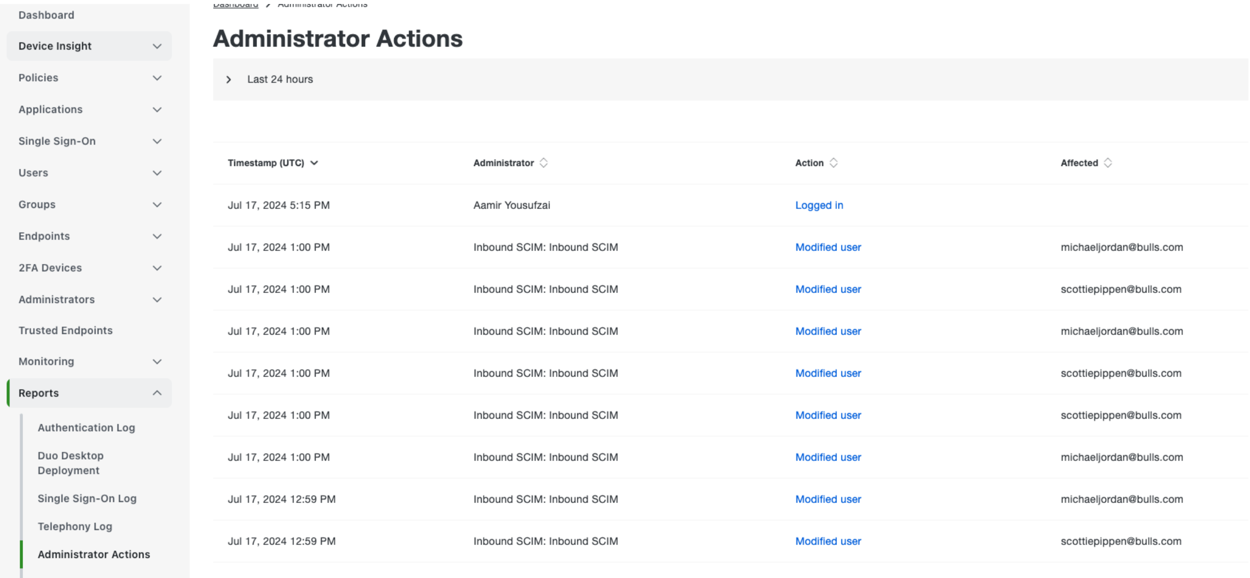
Push Groups to SCIM 2.0 Test App (Header Auth)

Group in Okta	Group in SCIM 2.0 Test App (Header Auth)	Last Push	Push Status
96 Bulls No description	96 Bulls No description	July 17, 2024 at 8:59:05 AM EDT	Inactive ▾

That’s it! At this point, your users and/or groups should start to appear in Duo. Please visit the Duo Admin Panel and review the Users and Groups tabs to see the results of your SCIM integration.

Additional Notes

Actions related to Inbound SCIM are logged in the Administrator Actions Report.



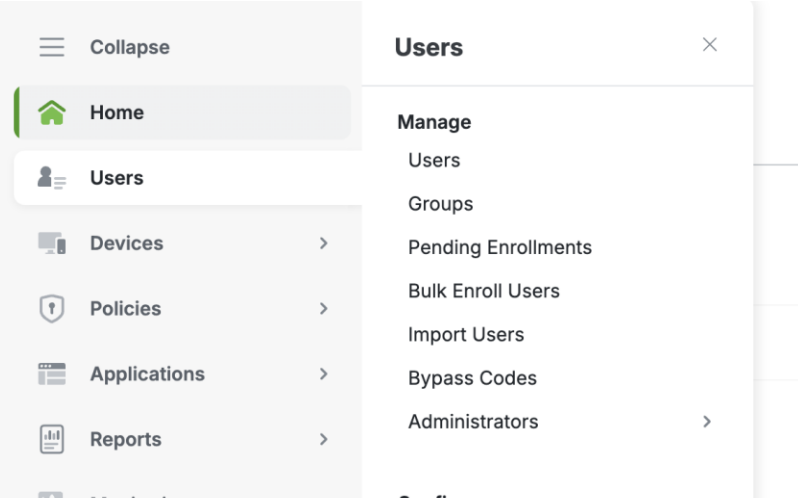
Administrator Actions

Last 24 hours

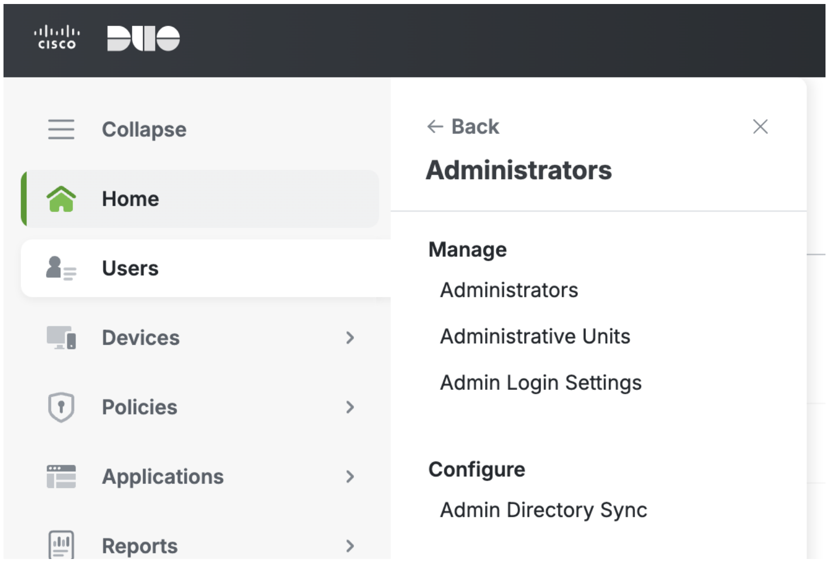
Timestamp (UTC)	Administrator	Action	Affected
Jul 17, 2024 5:15 PM	Aamir Yousufzai	Logged in	
Jul 17, 2024 1:00 PM	Inbound SCIM: Inbound SCIM	Modified user	michaeljordan@bulls.com
Jul 17, 2024 1:00 PM	Inbound SCIM: Inbound SCIM	Modified user	scottiepippen@bulls.com
Jul 17, 2024 1:00 PM	Inbound SCIM: Inbound SCIM	Modified user	michaeljordan@bulls.com
Jul 17, 2024 1:00 PM	Inbound SCIM: Inbound SCIM	Modified user	scottiepippen@bulls.com
Jul 17, 2024 1:00 PM	Inbound SCIM: Inbound SCIM	Modified user	scottiepippen@bulls.com
Jul 17, 2024 1:00 PM	Inbound SCIM: Inbound SCIM	Modified user	michaeljordan@bulls.com
Jul 17, 2024 12:59 PM	Inbound SCIM: Inbound SCIM	Modified user	michaeljordan@bulls.com
Jul 17, 2024 12:59 PM	Inbound SCIM: Inbound SCIM	Modified user	scottiepippen@bulls.com

Sync admins from Google and automatically assign them Duo admin roles with Admin Sync

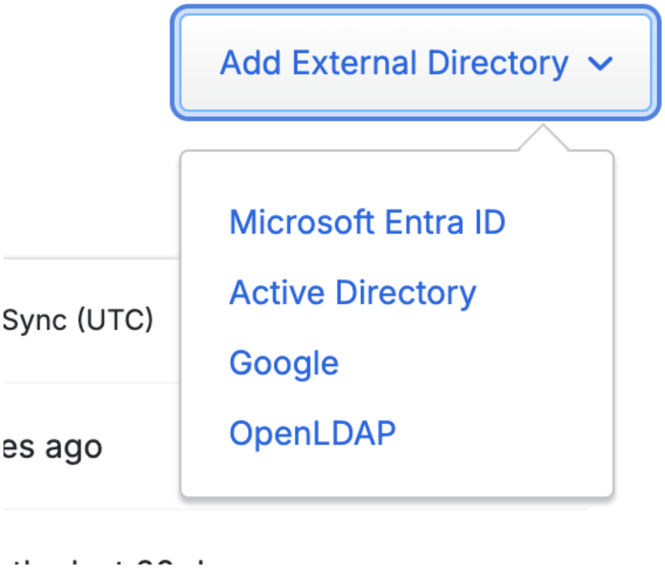
1. Log in to the Duo Admin Panel.
2. Locate **Users** in the left side bar and then click **Administrators** on the submenu



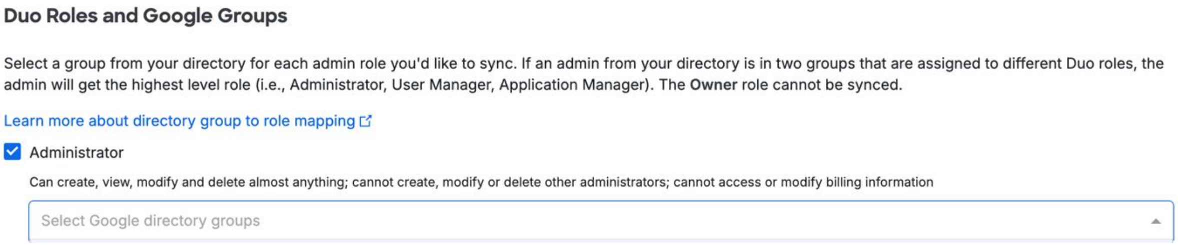
3. Select *Admin Directory Sync* under the *Configure* submenu



4. Click *Add External Directory* and then select *Google* from the dropdown



5. If you already have an existing Google Directory Sync from users, you can choose to reuse your existing connection. If not or if undesired, select **Add new connection** and follow the steps to login and authorize the admin sync connection.
6. The Duo Admin Roles are listed under the *Duo Roles and Google Groups* section. Select the checkbox next to the Duo Admin Role that you want to automatically assign users to. Then, click the box and select which Google directory groups you wish to automatically sync and assign to that Duo Admin Role.



Duo Roles and Google Groups

Select a group from your directory for each admin role you'd like to sync. If an admin from your directory is in two groups that are assigned to different Duo roles, the admin will get the highest level role (i.e., Administrator, User Manager, Application Manager). The **Owner** role cannot be synced.

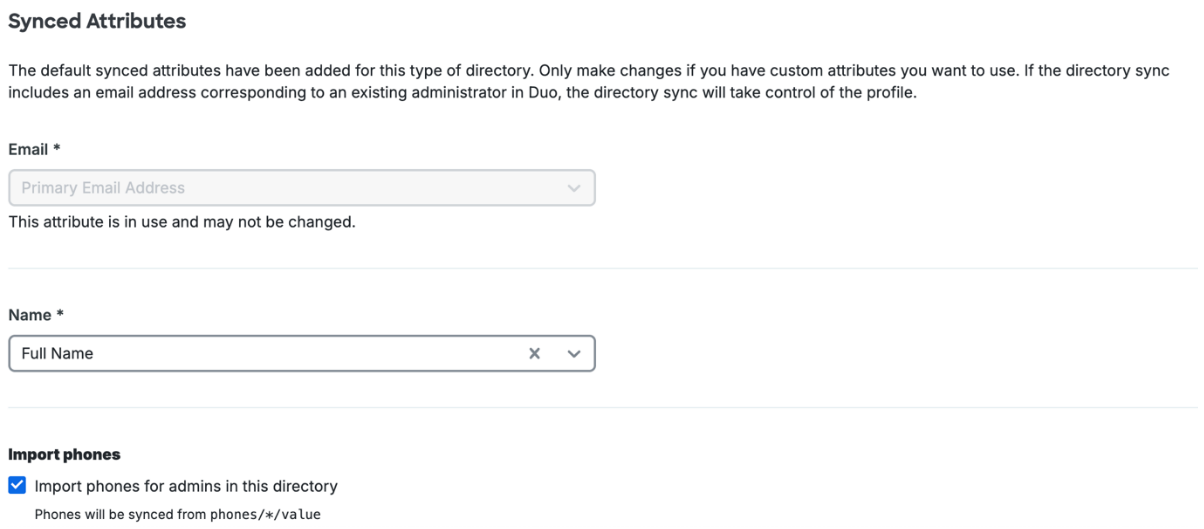
Learn more about directory group to role mapping

☑ Administrator

Can create, view, modify and delete almost anything; cannot create, modify or delete other administrators; cannot access or modify billing information

Select Google directory groups

7. Specify which Google attributes you wish to source values from during the admin sync process. Both attributes are defaulted to the most commonly used attributes. Control whether or not you wish to sync phone numbers using the checkbox.



Synced Attributes

The default synced attributes have been added for this type of directory. Only make changes if you have custom attributes you want to use. If the directory sync includes an email address corresponding to an existing administrator in Duo, the directory sync will take control of the profile.

Email *

Primary Email Address

This attribute is in use and may not be changed.

Name *

Full Name

Import phones

☑ Import phones for admins in this directory

Phones will be synced from phones/*/value

8. Wrap up the setup by setting your communication preferences. Click **Save** to finish the setup.

Configure an SSO Application

To configure a Duo SSO application, follow these instructions in our public documentation. Please be aware that you will may need to swap some of the attributes used in the integrations or configure your generic configurations

Use Case: Set up Routing Rules for Multiple Authentication Sources

Technical Description

Duo SSO's new Routing Rules feature enhances login flexibility and precision, enabling smart policy creation that funnels users to the correct Active Directory or SAML source or for preview customers, the Duo Directory. This resolves the complexities of evolving business structures, such as mergers and contractor usage, by providing a streamlined, user-specific sign-in process. With Routing Rules, the system no longer indiscriminately searches all directories, which previously led to errors with users in multiple ADs. Instead, it directs users to the appropriate environment, easing the load on authentication systems and offering tailored accuracy.

Routing Rules parameters can be set based on specific applications, domain names, and IP address ranges, with a default limit of 30 rules per customer. Upon activation, users will always encounter the Duo SSO login page for email input, allowing domain-based routing. Additionally, for ease of transition, existing authentication sources will be automatically integrated into Routing Rules, setting a default based on current configurations, whether that's a single SAML source, one AD, or multiple ADs.

Prerequisites

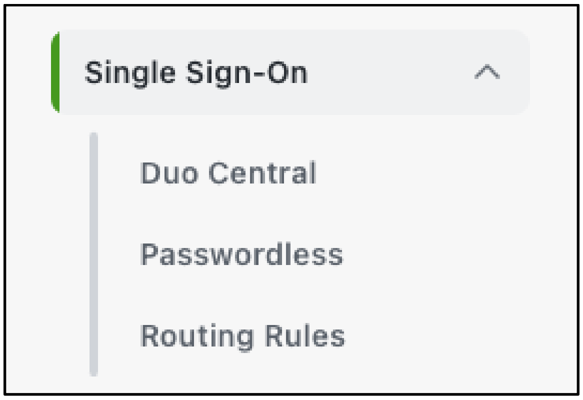
For the early preview, our engineering team will manually backfill your account, so it continues behaving and authenticating in the same way it does today.

As part of this backfill, the Default Rules (that takes effect when no other rules are met) will be set to the following based on your current configuration:

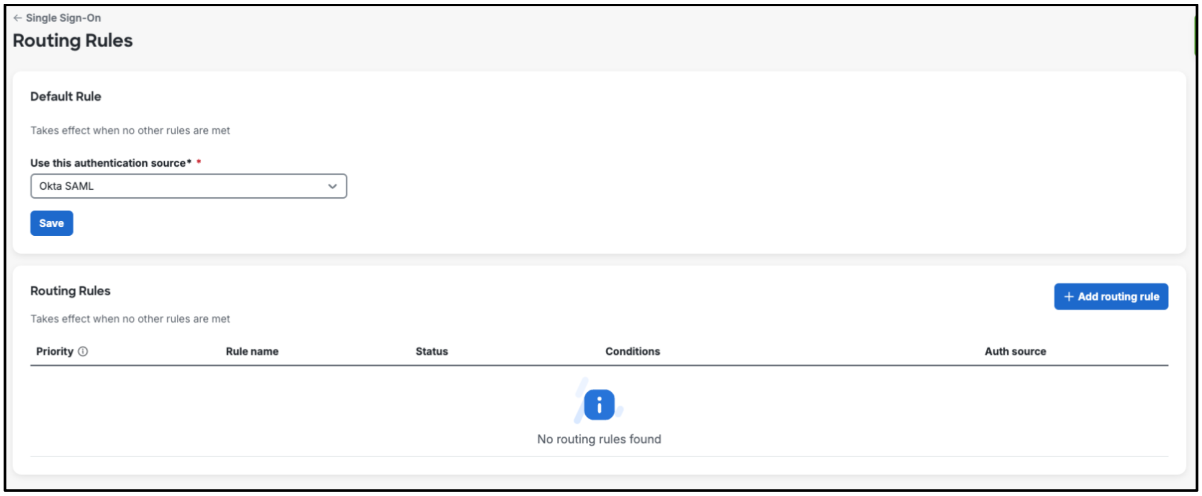
- If using a SAML authentication source à the Default Rule will be set to that SAML Authentication Source
- If using a single Active Directory authentication source à the Default Rule will be set to that Active Directory Authentication source
- If using more than 1 Active Directory authentication source à the Default Rule will be set to All Active Directories

Configuration

1. In the Duo Admin Panel, click on the arrow next to Single Sign-On, and then click on **Routing Rules**



2. From here you should see the Routing Rules configuration page, including your Default Rule as defined by the prerequisites above.



← Single Sign-On

Routing Rules

Default Rule

Takes effect when no other rules are met

Use this authentication source* *: Okta SAML

Routing Rules

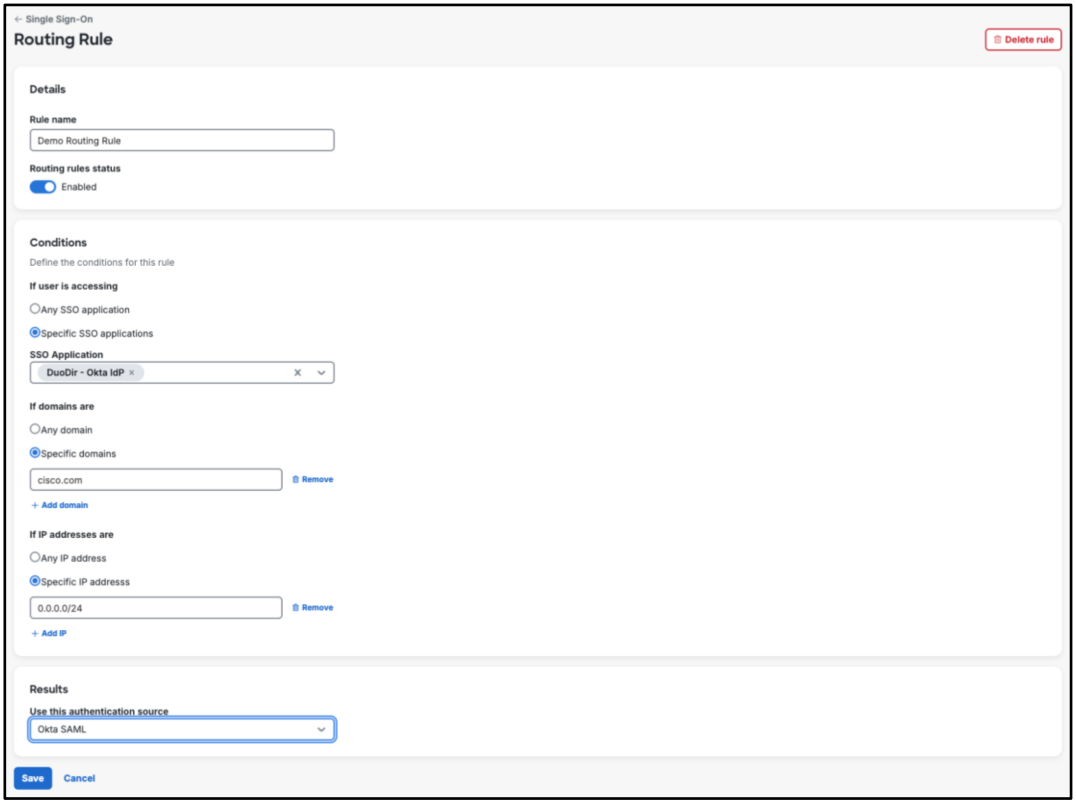
Takes effect when no other rules are met

Priority ⓘ	Rule name	Status	Conditions	Auth source

No routing rules found

3. Click **+ Add Routing Rule**

4. Give your Routing Rule a name
5. Choose the conditions for your Routing Rule
    a. You can choose based on Applications, Domain Names, and/or IP addresses/blocks
    b. For domain, just use domain.com, not @domain.com
6. Finally, select which authentication source to use when these conditions are met.



← Single Sign-On

Routing Rule

Delete rule

Details

Rule name: Demo Routing Rule

Routing rules status: Enabled

Conditions

Define the conditions for this rule

If user is accessing

○ Any SSO application
● Specific SSO applications

SSO Application: DuoDir - Okta IdP

If domains are

○ Any domain
● Specific domains

cisco.com — Remove

+ Add domain

If IP addresses are

○ Any IP address
● Specific IP addresss

0.0.0.0/24 — Remove

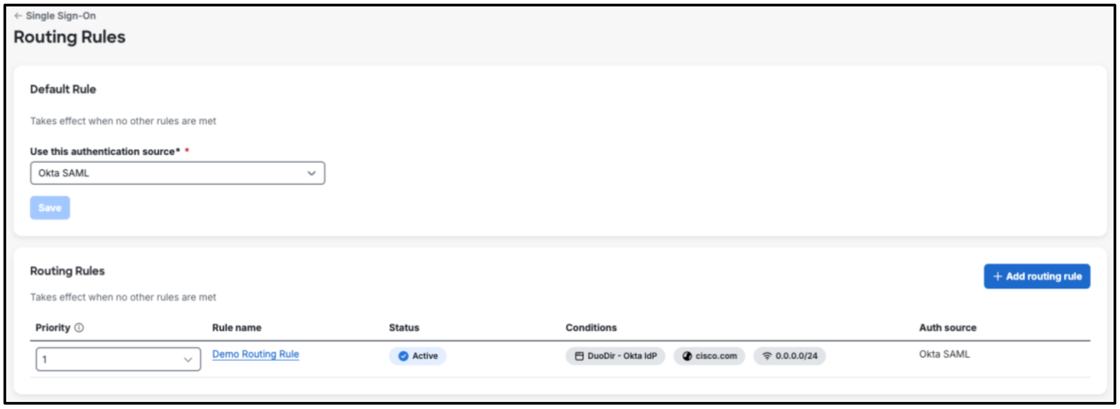
+ Add IP

Results

Use this authentication source: Okta SAML

Save Cancel

7. Click Save.
    a. Your Routing Rule is enabled by default, you can also toggle it off from this configuration page.
8. From here you should be back on the Routing Rules main configuration page with your new rule added.



← Single Sign-On

Routing Rules

Default Rule

Takes effect when no other rules are met

Use this authentication source* *: Okta SAML

Save

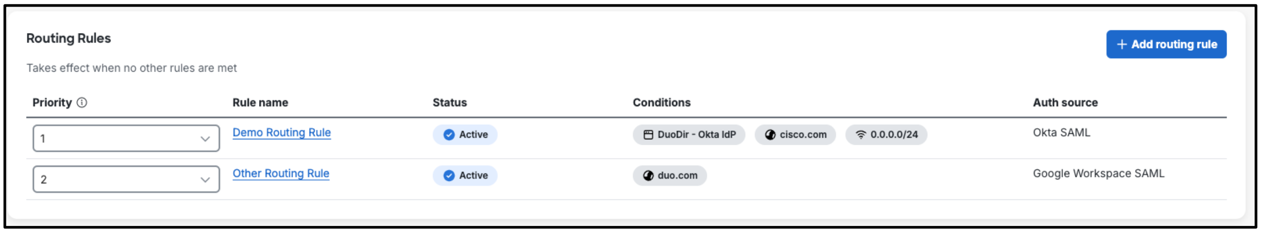
Routing Rules

Takes effect when no other rules are met

+ Add routing rule

Priority	Rule name	Status	Conditions	Auth source
1	Demo Routing Rule	Active	DuoDir - Okta IdP cisco.com 0.0.0.0/24	Okta SAML

Routing Rule Priority



Routing Rules

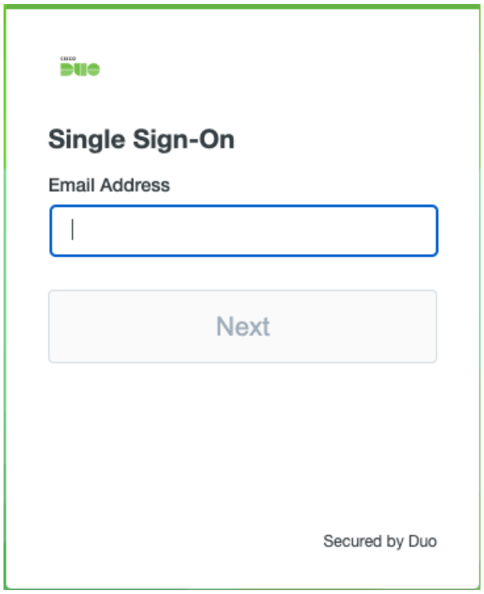
Takes effect when no other rules are met

Priority	Rule name	Status	Conditions	Auth source
1	Demo Routing Rule	Active	DuoDir - Okta IdP cisco.com 0.0.0.0/24	Okta SAML
2	Other Routing Rule	Active	duo.com	Google Workspace SAML

When adding multiple Routing Rules, we will start with #1, the highest priority and continue down the list until a rule is matched for a given user. If a user matches multiple rules, the highest priority will take effect. If no rules are matched, the Default Rule will be used.

UI Changes

When Routing Rules are enabled, users using a SAML authentication source will see a UI change when logging in. All users will now see the Duo SSO login page. This will allow us to perform user domain-based routing between a combination of Active Directory and SAML Authentication Sources.



Set up a Password Group Policy

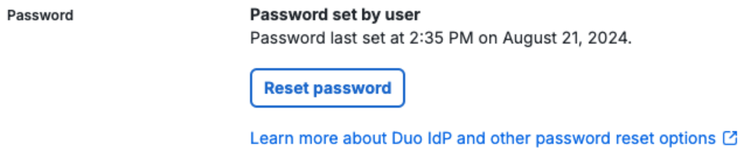
For users to be prompted to set a password with Duo, they will need to have an effective enrollment policy requiring one. Please see the enrollment policy section for details.

Note: The previous group password setting will soon be removed as enrollment policies fully replace this.

Enforce a Password Change

Admin: Enforce a Password Change

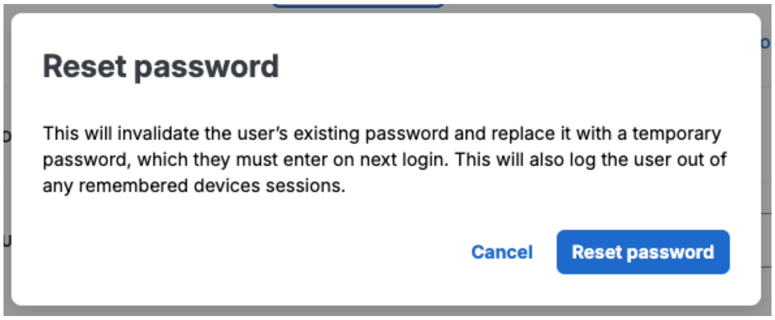
1. Navigate to the target user’s page
2. In the **Password** section, click **Reset password**



Password

Password set by user
Password last set at 2:35 PM on August 21, 2024.

3. Review and confirm again by clicking **Reset password**

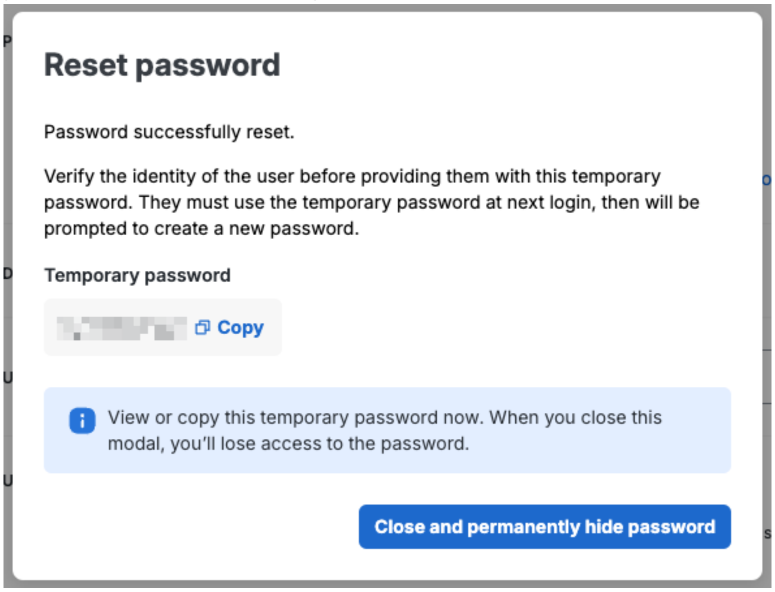


Reset password

This will invalidate the user’s existing password and replace it with a temporary password, which they must enter on next login. This will also log the user out of any remembered devices sessions.

Note: As this dialog indicates, the end-user’s current Duo password will be immediately invalidated, so you’ll want to ensure prompt delivery of the temporary password to ensure the end-user can continue to access protected applications.

4. The temporary password is displayed once. Once you’ve recorded/copied the password, you can close this dialog



Reset password

Password successfully reset.

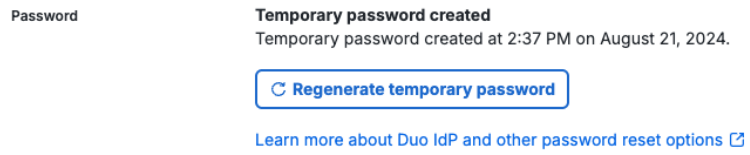
Verify the identity of the user before providing them with this temporary password. They must use the temporary password at next login, then will be prompted to create a new password.

Temporary password

[redacted]

View or copy this temporary password now. When you close this modal, you’ll lose access to the password.

5. The user page will indicate a temporary password has been generated:



Password

Temporary password created

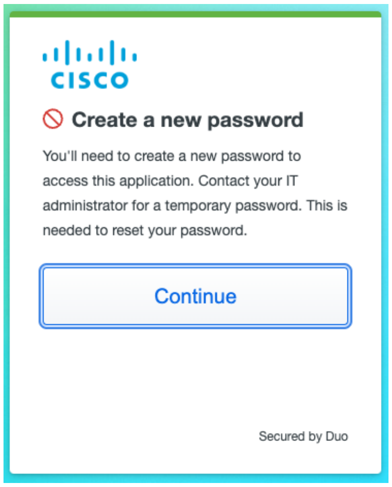
Temporary password created at 2:37 PM on August 21, 2024.

Regenerate temporary password
Learn more about Duo IdP and other password reset options

6. Once the user has set a new password, the user page will update again as initially seen in step 2.

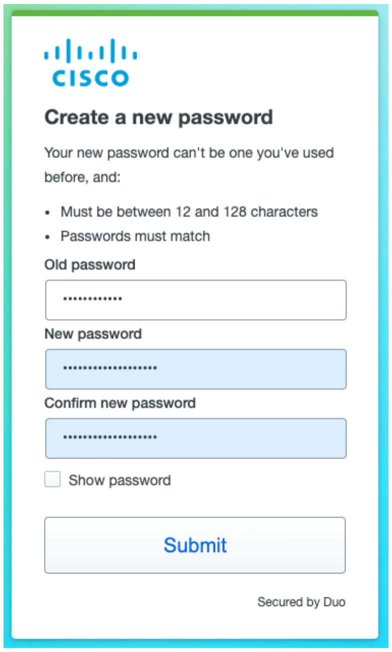
User Experience: Using the Temporary Password to Set a New One

1. The next time the user performs an MFA or Passwordless authentication to any SSO app, they will be prompted to set a new password after successful authentication.
    a. If using MFA authentication, the user will use the temporary password during login and again when changing their password
    b. If using passwordless authentication, the user will enter the temporary password only during the setting of the new password



Create a new password

You'll need to create a new password to access this application. Contact your IT administrator for a temporary password. This is needed to reset your password.



Create a new password

Your new password can't be one you've used before, and:

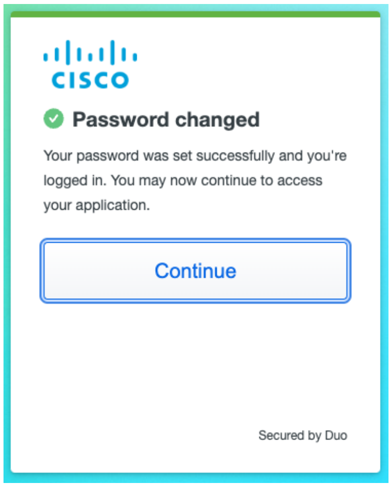
- Must be between 12 and 128 characters
- Passwords must match

Old password: ••••••••••••

New password: ••••••••••••••••••••

Confirm new password: ••••••••••••••••••••

□ Show password



Password changed

Your password was set successfully and you're logged in. You may now continue to access your application.

When temporary passwords are invalidated

Temporary passwords are invalidated when the user successfully commits a new password. Reuse of the temporary password is allowed to account for scenarios where a user might not be able to authenticate and they need to try again on a different device or browser so they can complete the operation. A user is always required to successfully authenticate with their enrolled device before they are able to set a new password.

Enroll a New User

Summary:
User Self-Enrollment can be implemented in a few different ways:

No	Enrollment Method	Access Location	Description
1	Prior IDP Enrollment	Hosted Enroll Portal	Users can sign in using their existing credentials from an external auth source configured with DuoSSO to enroll their device(s) and create their password (if required) with Duo.
2	Enrollment Codes	Hosted Enroll Portal	A short-lived code that users enter on the enroll portal. This code must be securely provided to the end-user via an out-of-band mechanism. If your organization decides to use enrollment codes, you will want to establish a process to ensure this is securely facilitated.
3	Enrollment Links	Link delivered to user via email or custom API implementation	This is existing Duo functionality that has been augmented to support user password creation. This sends a unique enrollment link to users via email (or generation of the link via API for custom applications/implementations, not covered in this document). This is a good option for scenarios where users already have email access.

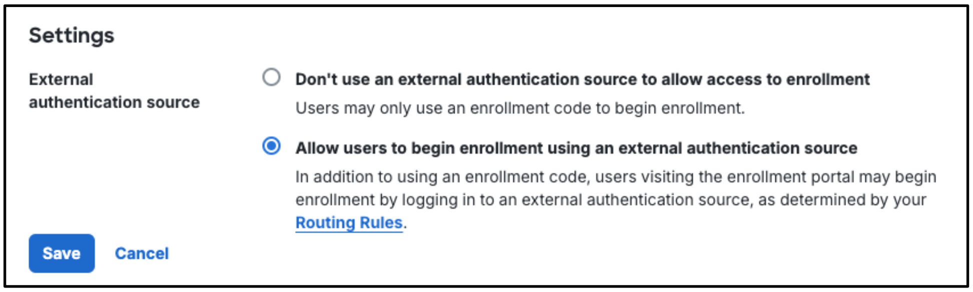
The Hosted Enroll Portal:
Duo provides a hosted enroll portal that is unique to each customer tenant. The hosted enroll portal is configured by default for enrollments using enrollment codes only and can be optionally configured for user enrollment via your prior IDP as well.

Method 1: Enroll via a Prior Identity Provider

Admin: Enabling Prior IDP Enrollment

1. If you have not already done so, configure any external IDP for use as an authentication source for DuoSSO
2. Ensure that the routing rules are configured to use the desired external auth source for the **Enroll Portal** application. See the routing rules section for instructions on this.
3. Navigate to **Policies → Enrollment**

4. Select the **Allow users to begin enrollment using an external authentication source** radio button and click **Save**.



Settings

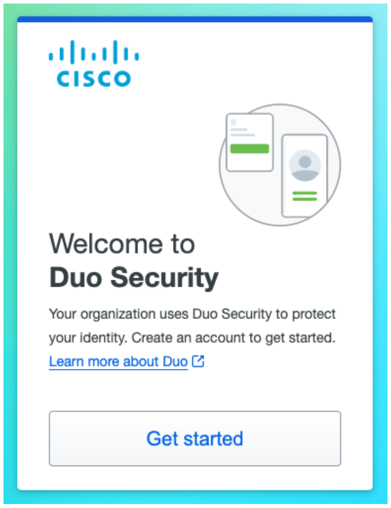
External authentication source

○ **Don't use an external authentication source to allow access to enrollment**
Users may only use an enrollment code to begin enrollment.

● **Allow users to begin enrollment using an external authentication source**
In addition to using an enrollment code, users visiting the enrollment portal may begin enrollment by logging in to an external authentication source, as determined by your Routing Rules.

User Experience: Prior IDP Enrollment

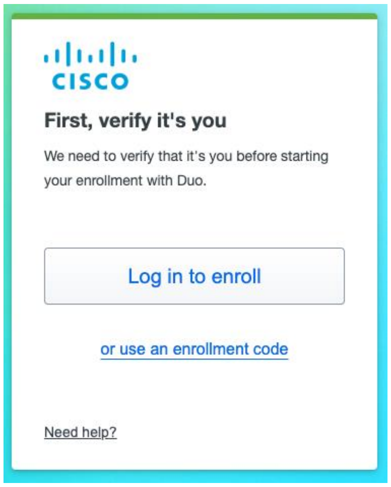
1. User visits the enroll portal URL



Welcome to **Duo Security**

Your organization uses Duo Security to protect your identity. Create an account to get started.

2. User selects **Log in to enroll**

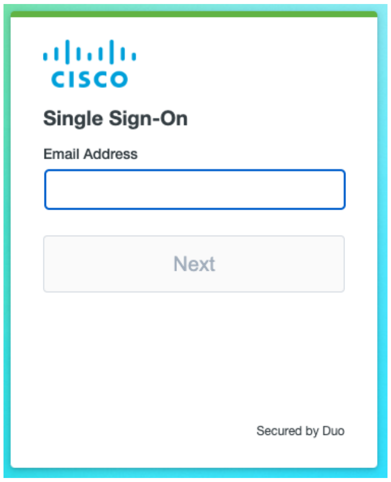


First, verify it's you

We need to verify that it's you before starting your enrollment with Duo.

3. Depending on the external authentication source being used, the experience will differ slightly here:

   a. Active Directory (AD) - User will encounter a Duo-hosted page to collect the user’s AD credentials:



CISCO

Single Sign-On

Email Address

Next

Secured by Duo

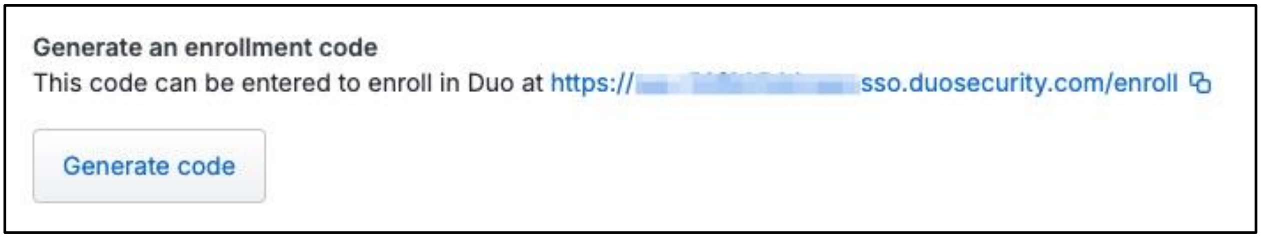
   b. SAML - User will be redirected to the SAML IDP to enter their credentials there

4. Upon successful authentication, the enrollment process starts

Method 2: Enroll via Enrollment Codes

Admin: Generating Enrollment Codes

1. After you have followed your organization’s identity verification process of the end-user who need to enroll, navigate to the specific user’s page in the admin panel
2. In the **Device enrollment → Generate an enrollment code** section, click **Generate code**

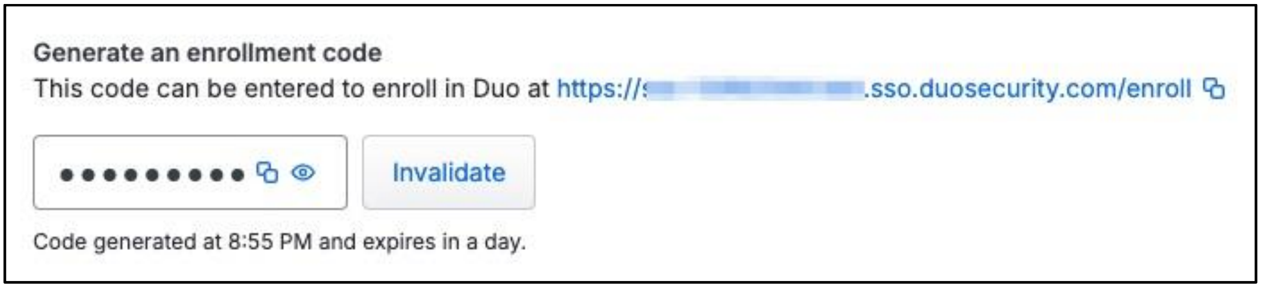


Generate an enrollment code

This code can be entered to enroll in Duo at https://[redacted]sso.duosecurity.com/enroll

Generate code

3. You can copy the code to your clipboard or reveal it from within the tooltips next to the obscured code.



Generate an enrollment code

This code can be entered to enroll in Duo at https://[redacted].sso.duosecurity.com/enroll

●●●●●●●●●

Invalidate

Code generated at 8:55 PM and expires in a day.

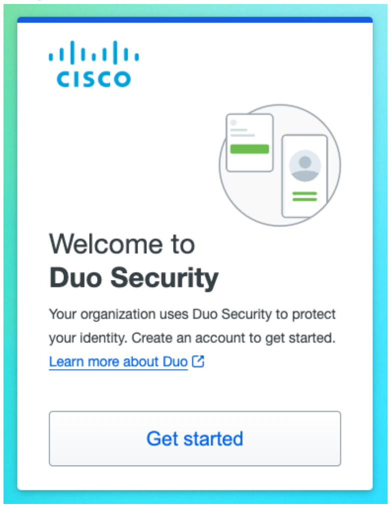
Notes:

- Your organization’s unique enroll portal URL is linked here for convenience

- On this page, enrollment codes can be invalidated before they expire, as well as regenerated.
- Treat enrollment codes with care as they can be used for enrollment of both password and authentication devices.
    - Ensure you are in a private space if you revealing the enrollment code in the admin panel
    - Ensure you have a secure means of sharing the enrollment code with the intended user

User Experience: Enroll Using an Enrollment Code

1. User navigates to your organization's unique enroll portal URL (example: https://acmeinc.sso.duosecurity.com/enroll)

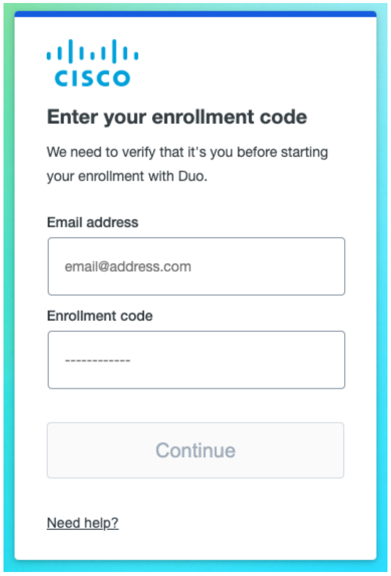


Welcome to
Duo Security

Your organization uses Duo Security to protect your identity. Create an account to get started.

Learn more about Duo

2. Depending on the prior IDP enrollment setting, the experience will differ slightly:
    a. If prior IDP enrollment is disabled, the only option will be enrollment code



Enter your enrollment code

We need to verify that it's you before starting your enrollment with Duo.

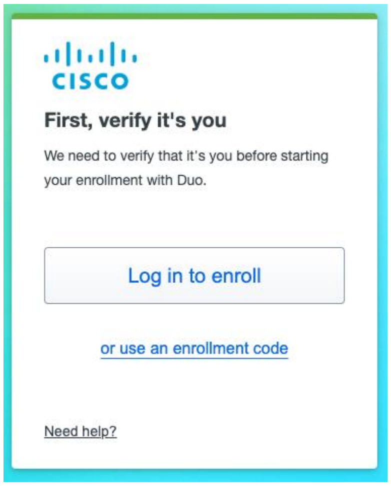
Email address

email@address.com

Enrollment code

----

    b. If prior IDP enrollment is enabled, the user will see the option to **Log in to enroll** and **or use an enrollment code**. The user will need to select the enrollment code option.



First, verify it's you

We need to verify that it's you before starting your enrollment with Duo.

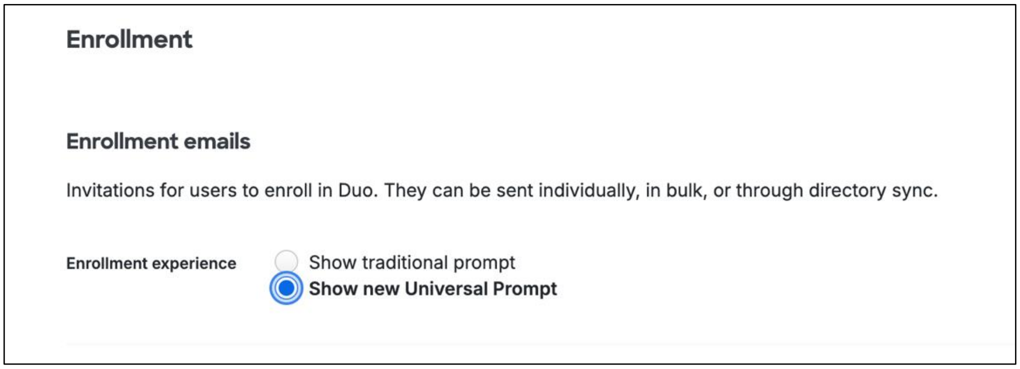
3. After entering their email address and their assigned, valid, and unexpired enrollment code is correctly entered, enrollment will start.

When enrollment codes are invalidated

Enrollment codes are invalidated immediately after a user has enrolled their first device or if the code reaches its expiration without being used. Reuse of an unexpired enrollment code is allowed to account for scenarios where a user might not be able to enroll their desired device and they need to try again on a different device or browser so they can complete the operation.

Setting a Password During Enrollment - User Experience:

Please note for your users to be prompted to set a password during enrollment, you must have the Enrollment experience found the Settings menu configured to Show new Universal Prompt as shown below:



Enrollment

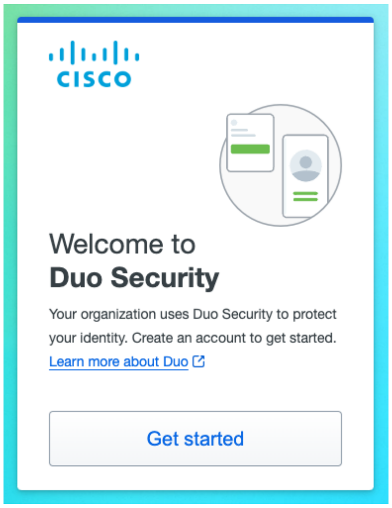
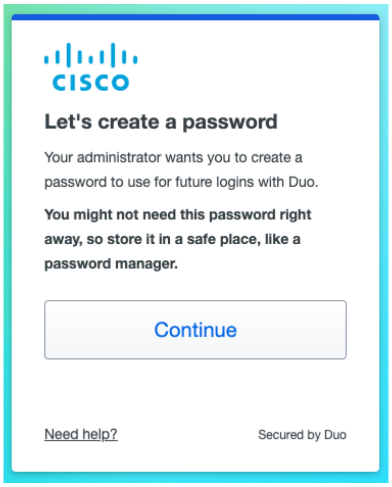
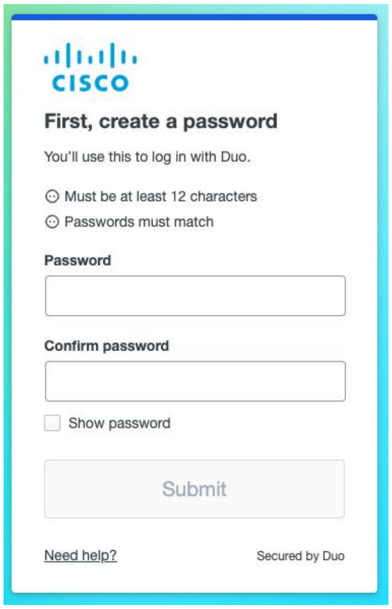
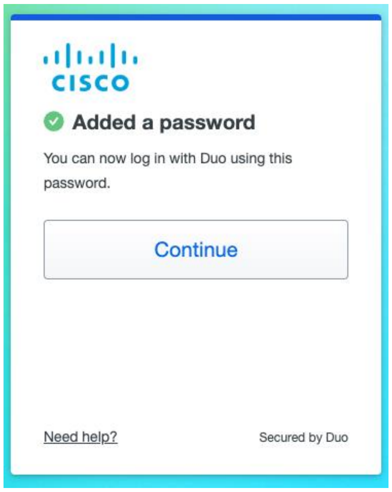
Enrollment emails

Invitations for users to enroll in Duo. They can be sent individually, in bulk, or through directory sync.

Enrollment experience: ○ Show traditional prompt / ● Show new Universal Prompt

When a user with a password requirement enters enrollment, they will experience the following steps:

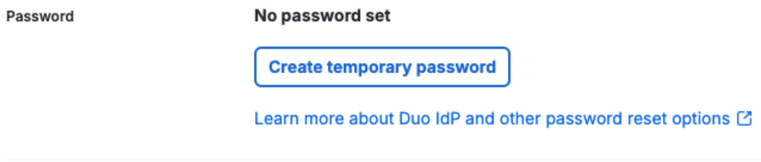
1. Welcome Screen:	2. Preparing the user to set a password:

 Welcome to **Duo Security** Your organization uses Duo Security to protect your identity. Create an account to get started. Learn more about Duo 	 **Let's create a password** Your administrator wants you to create a password to use for future logins with Duo. **You might not need this password right away, so store it in a safe place, like a password manager.**
3. Setting the password:  **First, create a password** You'll use this to log in with Duo. Must be at least 12 characters Passwords must match **Password** **Confirm password** □ Show password 	4. Confirmation  **Added a password** You can now log in with Duo using this password. Normal Universal Prompt continues from here (the remaining steps are the same as is documented in the user guide)

Setting a Password for Already Enrolled Users:
If a user already has device(s) enrolled and is later added to a group that requires setting a password, the user can set a password in two ways:

- **Enroll Portal Prior IdP flow -** When a device-enrolled user authenticates using the prior IdP flow

- **Setting a temporary password in the admin panel -** this is the least preferable option, but is available if you have a secure way to provide the user with a temporary password



Password

No password set

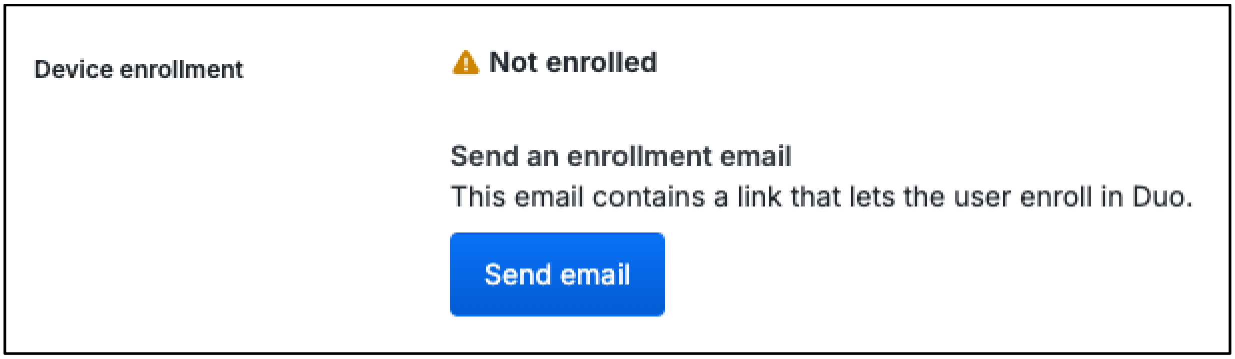
Create temporary password
Learn more about Duo IdP and other password reset options

Method 3: Enroll via Enrollment Emails

Admin: Sending Enrollment Emails

To send an enrollment email, you have 3 options:

1. Directory Sync: You can configure your synced external directory to automatically send an enrollment email to users as they are imported into Duo.
    a. For Inbound SCIM, see that section of this document
    b. For Active Directory, Entra ID, or OpenLDAP sync, see this documentation.
2. Generating an enrollment link via API (not covered in this document)
3. Manually (Easiest option for testing)
    a. Navigate to the desired user's page in the admin panel
    b. In the **Device enrollment**, click **Send email**



Device enrollment

⚠ Not enrolled

Send an enrollment email

This email contains a link that lets the user enroll in Duo.

User Experience: Enroll Using an Enrollment Email

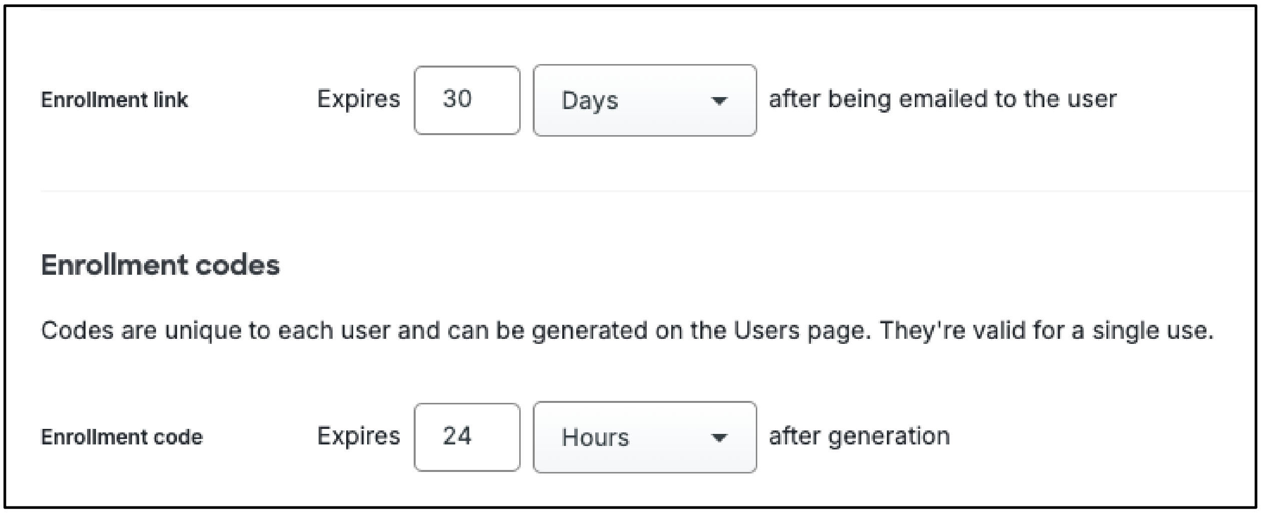
- Users will receive an email from no-reply@duosecurity.com containing the unique enrollment link.
- With the exception of setting a password (if required, see the "Setting a password during enrollment" section) at the beginning. The rest of the enrollment experience is documented in the public user guide here.
- If using directory sync, the user will receive reminder emails on a set schedule

Admin: Changing Enrollment Link / Enrollment Code Expiry

The default expiration values are:

- Email enrollment link - 30 days
- Enrollment codes - 24 hours

Careful consideration should be taken to adjust these values. The security of the delivery mechanism as well as your organization’s security tolerance should be determining factors in changing these values. To change the expiry, navigate to **Settings → Enrollment**:



Enrollment link Expires 30 Days after being emailed to the user

Enrollment codes

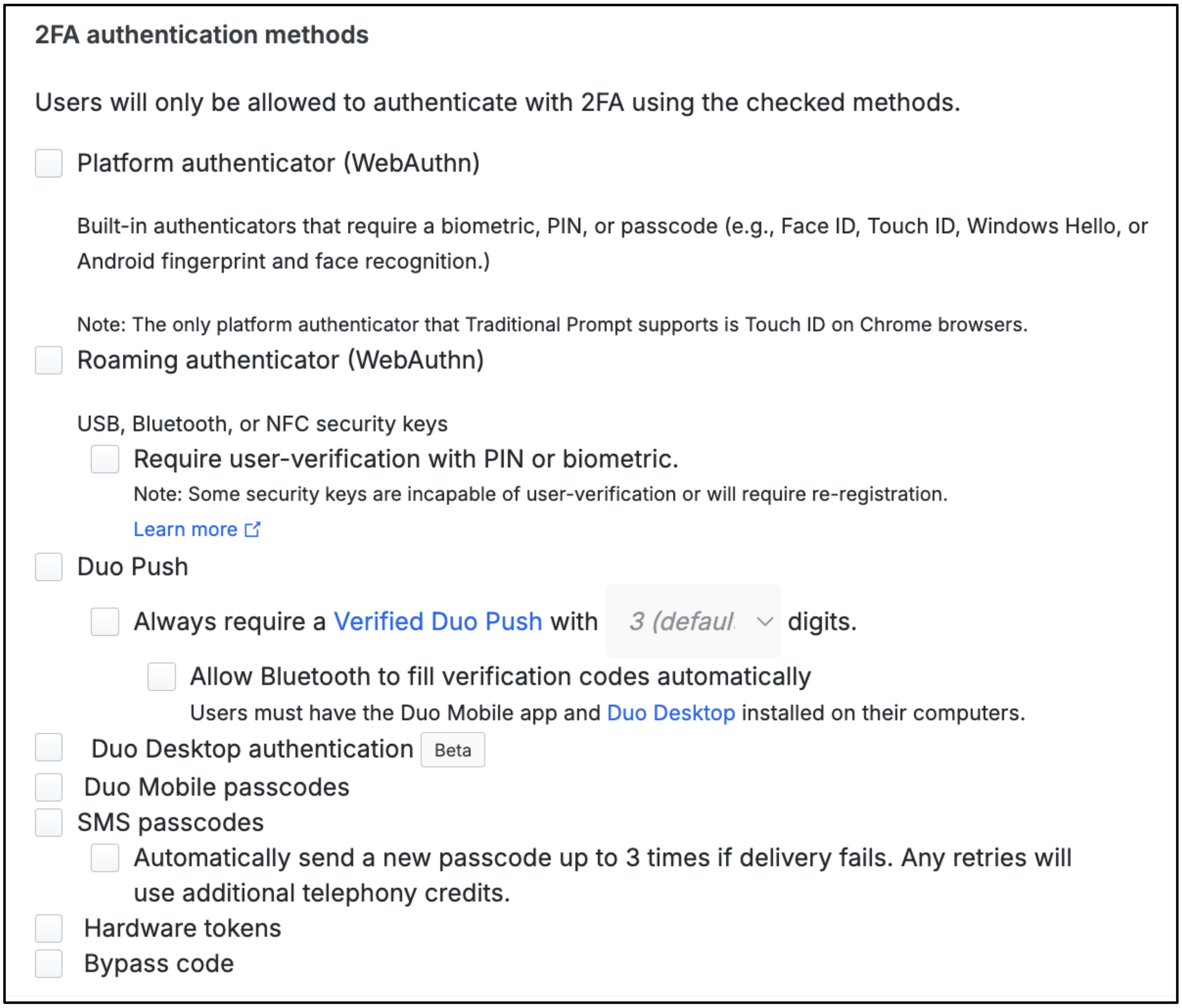
Codes are unique to each user and can be generated on the Users page. They're valid for a single use.

Enrollment code Expires 24 Hours after generation

Disable Password Fallback and Enforce Complete Passwordless

Admin: Set up Policy to Require Passwordless Auth Methods Only

1. **Edit Policy** and go to **Authentication methods** policy
   a. Recommended: create a group policy for your testing group
2. Disable all 2FA authentication methods to disallow the use of password + 2FA auth method
   a. Note: **bypass code** is a new option that is available for 2FA authentication methods policy configuration. When bypass code is not checked, end users will not be able to get temporary access through a bypass code.
3. If you’ve already enabled passwordless authentication methods, there is no change expected for the passwordless authentication methods.



2FA authentication methods

Users will only be allowed to authenticate with 2FA using the checked methods.

□ Platform authenticator (WebAuthn)

Built-in authenticators that require a biometric, PIN, or passcode (e.g., Face ID, Touch ID, Windows Hello, or Android fingerprint and face recognition.)

Note: The only platform authenticator that Traditional Prompt supports is Touch ID on Chrome browsers.

□ Roaming authenticator (WebAuthn)

USB, Bluetooth, or NFC security keys

- □ Require user-verification with PIN or biometric.
  Note: Some security keys are incapable of user-verification or will require re-registration.
  Learn more

□ Duo Push

- □ Always require a Verified Duo Push with 3 (defaul digits.
  - □ Allow Bluetooth to fill verification codes automatically
    Users must have the Duo Mobile app and Duo Desktop installed on their computers.

□ Duo Desktop authentication Beta

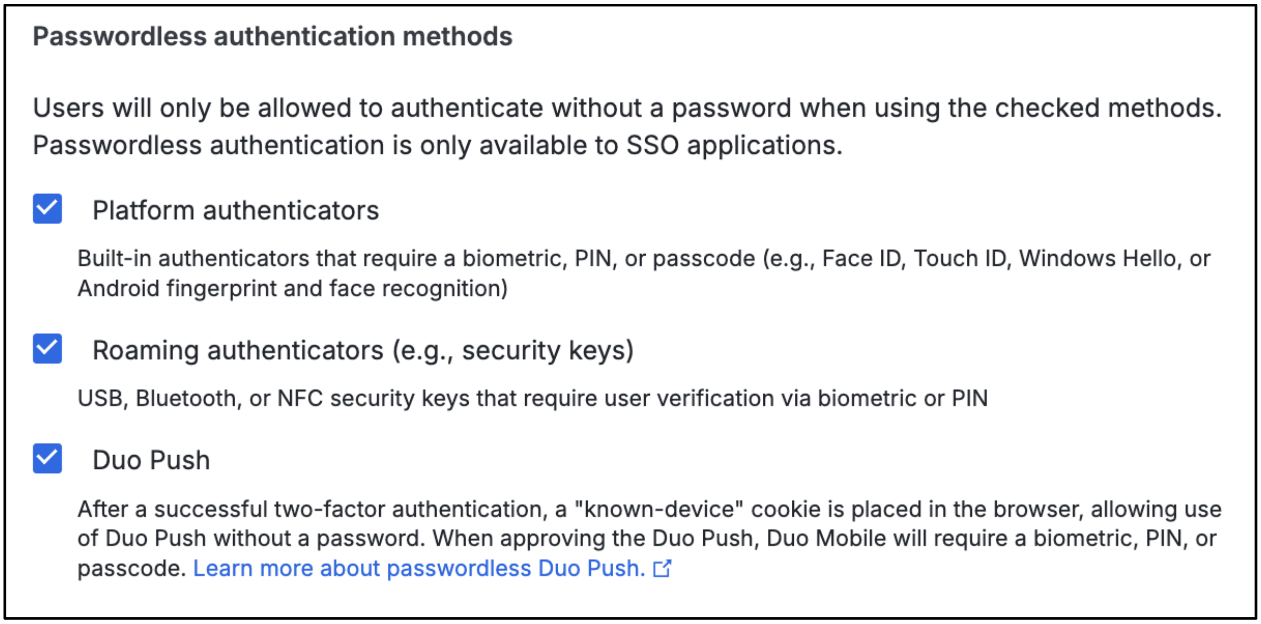
□ Duo Mobile passcodes

□ SMS passcodes

- □ Automatically send a new passcode up to 3 times if delivery fails. Any retries will use additional telephony credits.

□ Hardware tokens

□ Bypass code



Passwordless authentication methods

Users will only be allowed to authenticate without a password when using the checked methods. Passwordless authentication is only available to SSO applications.

☑ Platform authenticators

Built-in authenticators that require a biometric, PIN, or passcode (e.g., Face ID, Touch ID, Windows Hello, or Android fingerprint and face recognition)

☑ Roaming authenticators (e.g., security keys)

USB, Bluetooth, or NFC security keys that require user verification via biometric or PIN

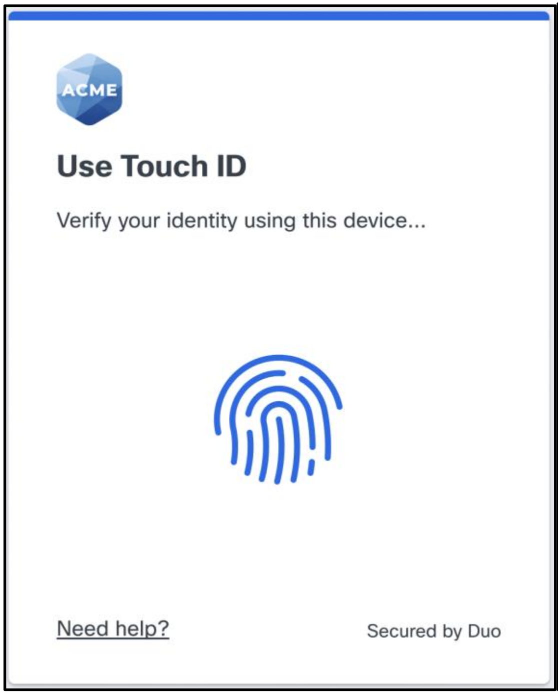
☑ Duo Push

After a successful two-factor authentication, a "known-device" cookie is placed in the browser, allowing use of Duo Push without a password. When approving the Duo Push, Duo Mobile will require a biometric, PIN, or passcode. Learn more about passwordless Duo Push.

User Experience: Passwordless Authentication when Fallback is Disabled

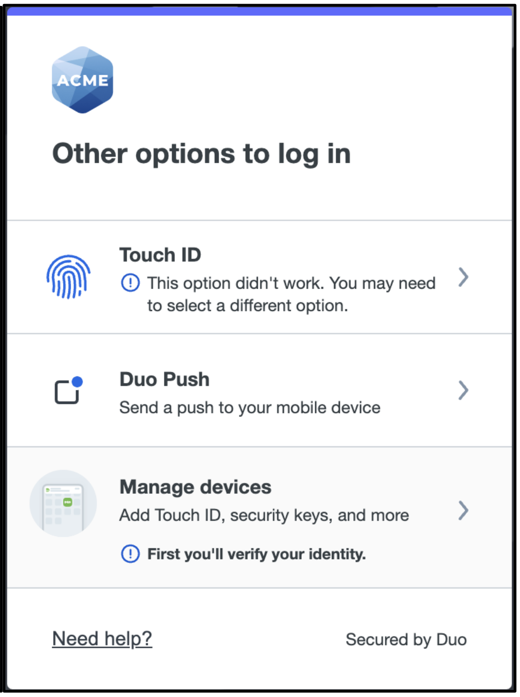
After an admin disables fallback to password + 2FA authentication methods:

1. For users who are using passwordless authenticators today, there will be no change to their day-to-day authentication experience. Users will be prompted to use their preferred passwordless authentication method automatically. If a user cancels an authentication, the user can select other passwordless authentication methods (if available) and the user will not have the option to fallback to a password and MFA authentication.



Use Touch ID

Verify your identity using this device...



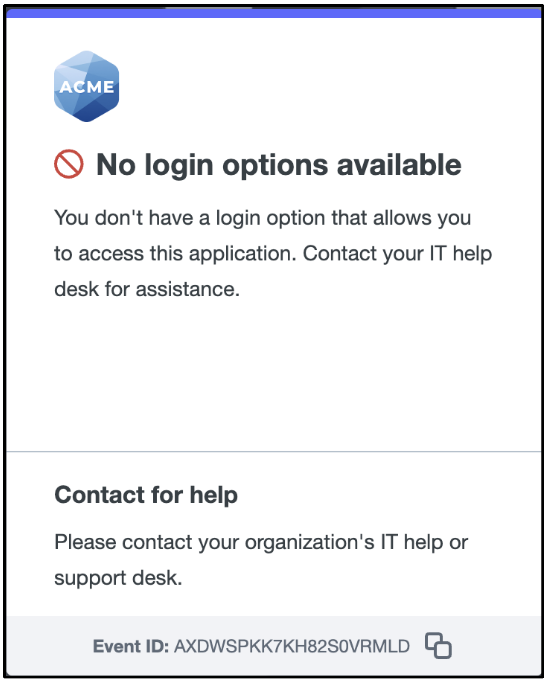
Other options to log in

Touch ID
ⓘ This option didn't work. You may need to select a different option.

Duo Push
Send a push to your mobile device

Manage devices
Add Touch ID, security keys, and more
ⓘ **First you'll verify your identity.**

2. If a user has not enrolled with a passwordless authenticator, a user will be blocked for access. The user needs to reach out to the help desk to enroll a passwordless authenticator following your company's device enrollment process.



No login options available

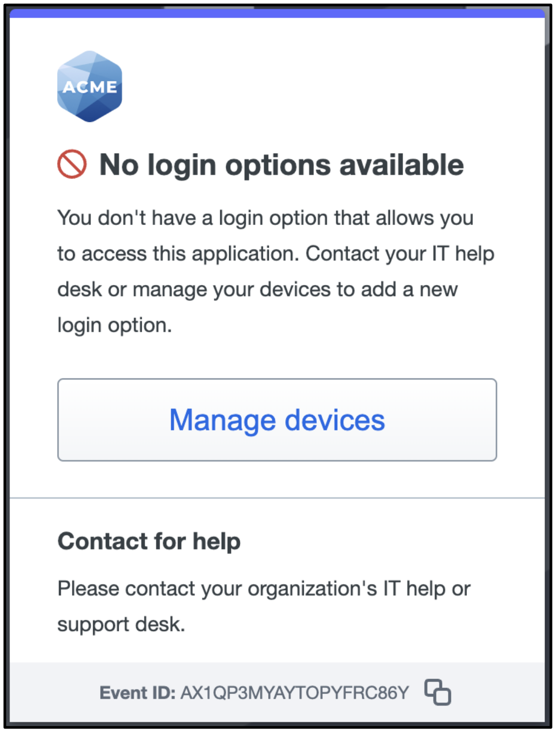
You don't have a login option that allows you to access this application. Contact your IT help desk for assistance.

Contact for help

Please contact your organization's IT help or support desk.

Event ID: AXDWSPKK7KH82S0VRMLD

3. If your organization allows self-service device registration, you've set up a Self-Service Portal policy with which the user has an authenticator permitted by the self-service portal policy, the user will have the option to access the self-service portal to enroll a passwordless authenticator and login again to access this application.



No login options available

You don't have a login option that allows you to access this application. Contact your IT help desk or manage your devices to add a new login option.

Contact for help

Please contact your organization's IT help or support desk.

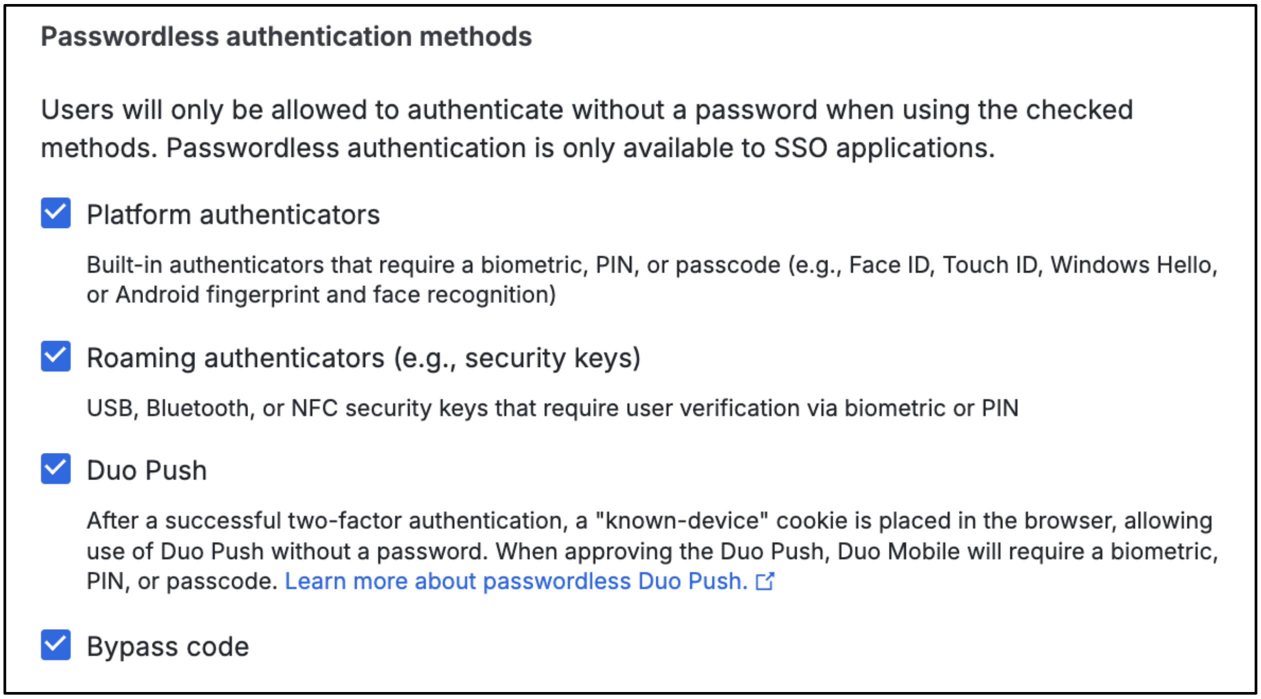
Event ID: AX1QP3MYAYTOPYFRC86Y

Enable bypass code to unblock user access in a passwordless auth

Admin: New option to enable or disable the use of bypass code in a passwordless auth

If you want to enable the use of bypass code in a passwordless authentication:

1. **Edit Policy** and go to **Authentication methods** policy
2. Check **Bypass code** under **Passwordless authentication methods.**
    a. When bypass code is checked, end users will be able to get temporary access by using a bypass code issued from the IT help desk.
    b. This option is not checked by default.
    c. Notes on restrictions to use bypass code in passwordless authentication:
        i. The use of bypass code in a passwordless authentication is restricted to users who can pass the mandatory endpoint verification, which means the identity of the endpoint can be verified by Duo Desktop or a browser cookie from an authentication within the last 30 days.
        ii. Note that when the identity of the endpoint cannot be verified, the bypass code option may show as available in the factors menu *even if it is disabled in policy*. This is because in a pre-auth context, we try to avoid leaking any information to bad actors about system configuration.
        iii. Bypass code is limited to one time use in a passwordless authentication regardless of the code reuse setting.



Passwordless authentication methods

Users will only be allowed to authenticate without a password when using the checked methods. Passwordless authentication is only available to SSO applications.

☑ Platform authenticators

Built-in authenticators that require a biometric, PIN, or passcode (e.g., Face ID, Touch ID, Windows Hello, or Android fingerprint and face recognition)

☑ Roaming authenticators (e.g., security keys)

USB, Bluetooth, or NFC security keys that require user verification via biometric or PIN

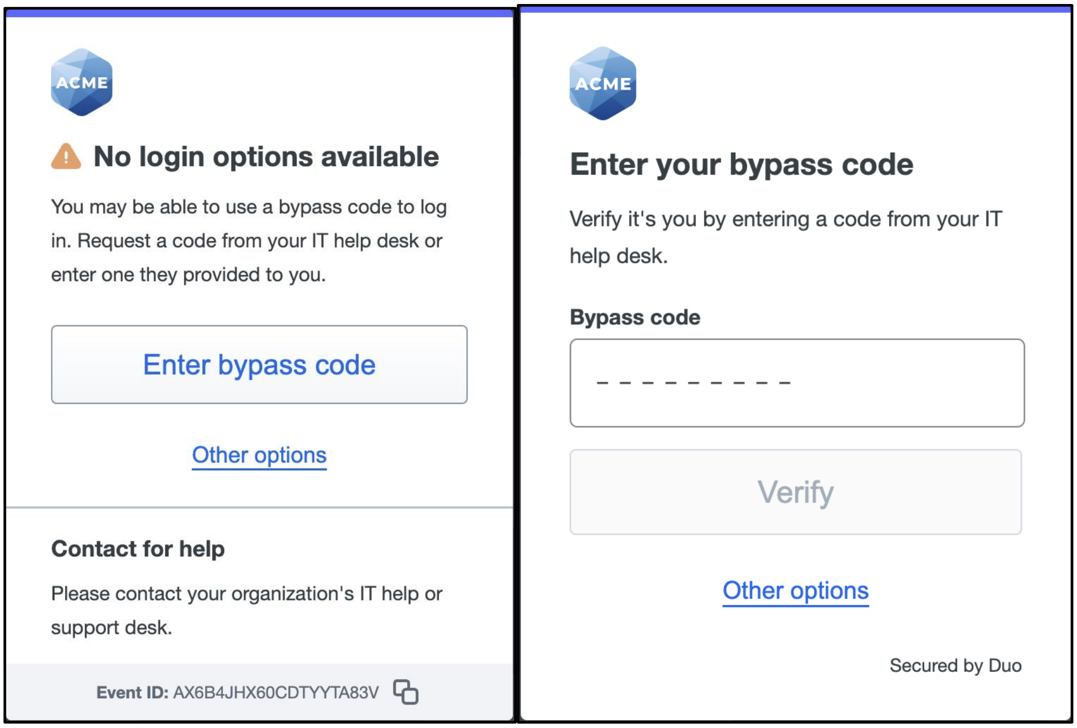
☑ Duo Push

After a successful two-factor authentication, a "known-device" cookie is placed in the browser, allowing use of Duo Push without a password. When approving the Duo Push, Duo Mobile will require a biometric, PIN, or passcode. Learn more about passwordless Duo Push.

☑ Bypass code

End User: Authentication experience

1. If a user does not have a passwordless authenticator that is permitted by policy, a user will be blocked for access. The user will be presented with the option to use bypass code that is issued from their IT help desk.


No login options available

You may be able to use a bypass code to log in. Request a code from your IT help desk or enter one they provided to you.

Enter bypass code

Other options

Contact for help

Please contact your organization's IT help or support desk.

Event ID: AX6B4JHX60CDTYYTA83V

Enter your bypass code

Verify it's you by entering a code from your IT help desk.

Bypass code

_ _ _ _ _ _ _ _ _

Verify

Other options

Secured by Duo

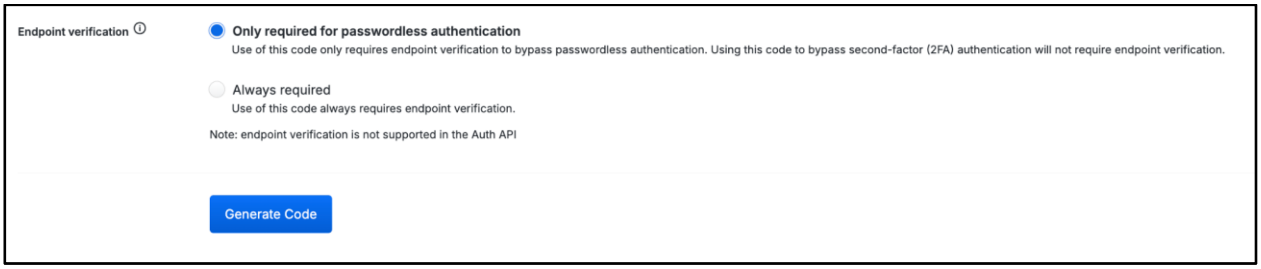
2. Users won’t be able to use the bypass code for passwordless authentication if their endpoint does not pass the endpoint verification. In the authentication log (Duo Admin Panel → **Reports** → **Authentication Log**), administrators will be able to view the details that users can’t use the bypass code because the endpoint verification fails.

New configuration options for bypass code

Admin: Require endpoint verification with the use of bypass code

Before creating a bypass code (Select a user → **Add Bypass Code**), administrators now have new options to require endpoint verification for the use of bypass code. Endpoint verification restricts the use of bypass code to endpoints whose identity can be verified by Duo Desktop or a browser cookie from an authentication within the last 30 days.

- Endpoint verification is mandatory for bypass code use in passwordless authentication.
- Administrators have the option to require endpoint verification for bypass code in both passwordless and 2FA authentications.
- Note that endpoint verification is not supported in the Auth API.


Endpoint verification ⓘ

● Only required for passwordless authentication
Use of this code only requires endpoint verification to bypass passwordless authentication. Using this code to bypass second-factor (2FA) authentication will not require endpoint verification.

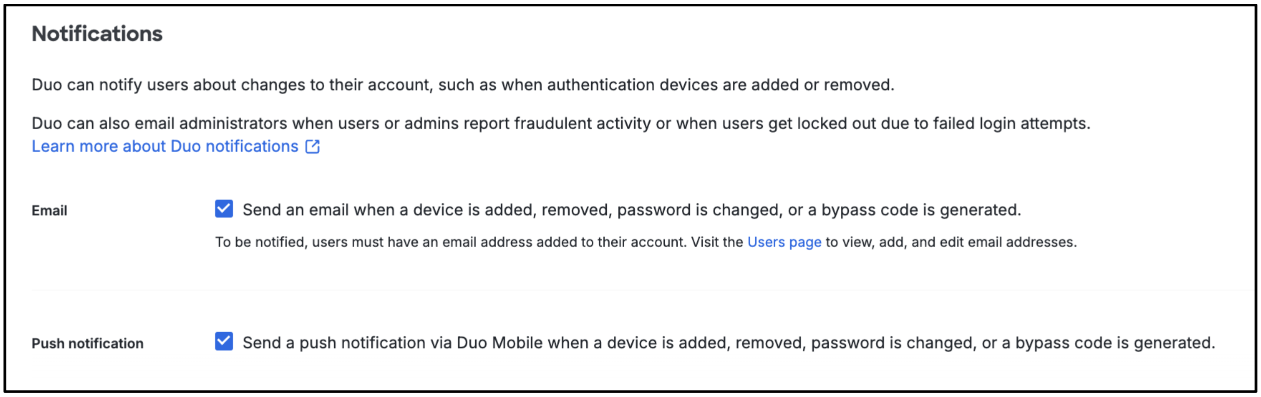
○ Always required
Use of this code always requires endpoint verification.

Note: endpoint verification is not supported in the Auth API

Generate Code

New user and admin notification for bypass code

If you turn on the user notifications in **Settings → Notifications,** users will also be notified by Email / Push notification if a bypass code is generated for their user account.



Notifications

Duo can notify users about changes to their account, such as when authentication devices are added or removed.

Duo can also email administrators when users or admins report fraudulent activity or when users get locked out due to failed login attempts.
Learn more about Duo notifications

Email ☑ Send an email when a device is added, removed, password is changed, or a bypass code is generated.
To be notified, users must have an email address added to their account. Visit the Users page to view, add, and edit email addresses.

Push notification ☑ Send a push notification via Duo Mobile when a device is added, removed, password is changed, or a bypass code is generated.

Users have the option to report "No, it wasn't me" through the email or push notification if the bypass code is not requested by them and the bypass code will be deleted immediately. All administrators will be notified of the fraud reported by the user via email.

Note: Push notification will be available after the Duo Mobile rollout between Nov-4 and Nov-10.

Admin Logs and Authentication Logs

Admin Logging

Any action taken by an administrator is logged in **Reports → Administrator Actions**

User Logging

- Device enrollment is logged in **Reports → Authentication Log**
- More specific user actions are logged to Activity Logs (API only). UI for Activity Logs will come in a future Duo release.

Enrollment Policies

In the past, all aspects of Duo's enrollment and self-service experiences have been controlled by the same set of policies that are also used for access/authentication. This has presented confusion and challenges for customers who may want to define these experiences separately. We are excited to introduce enrollment policies: an entirely new place to manage certain aspects of the end-user's enrollment and self-service portal experiences!

Some examples of where this may be beneficial are:

- You have a campaign to move users off telephony-based authentication methods. To prevent this problem from worsening, you can set an enrollment policy to no longer allow users to further enroll in telephony-only methods while still allowing existing users and devices to use telephony to allow for a smooth period of transition.

- You have certain users with privileged access that you only want to enroll in phishing-resistant authentication methods, but you're unable to hold all users to this high standard. You can use enrollment policy to accomplish this.

- You want to pilot Duo Passwordless and want to ensure this pilot group can only enroll in methods that are passwordless-capable. You can use enrollment policy to accomplish this.

The initial functionality of enrollment policy is limited, but we expect to add additional enhancements and controls in time.

Prerequisites and limitations

- Enrollment Policy is available only for Duo's web-based Universal Prompt enrollment and self-service portals including:
    - Email enrollment
    - Enroll Portal Enrollment (both enrollment code and enrollment via external IDP)
    - Standalone Device Management Portal (DMP) enrollment
    - Self-Service Portal (SSP)
    - Duo Central Device Management (via the Duo Central launcher or the dedicated URL)
- The traditional prompt (which is end-of-support), admin panel, and custom api-driven enrollment is unaffected by enrollment policy.

The Role of enrollment policy

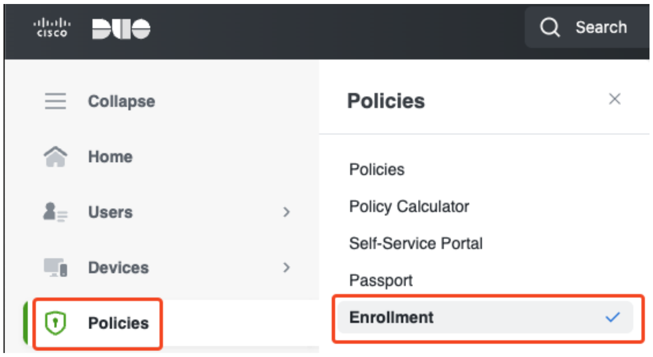
- Enrollment policy defines behavior for users once they have entered Duo’s **enrollment** or **self-service** portals:
  - **Unenrolled Users**
    - Enrollment policy defines certain aspects of unenrolled users’ enrollment experience
    - Enrollment policy **does not** define the decision for a user to enter enrollment or not. This continues to be handled by the effective authentication policy for that method of enrollment.
      - For email link enrollment, users will always be prompted to enroll
      - For inline enrollment, this decision is controlled by the effective authentication policy for the users accessing that inline application
      - For standalone Device Management Portal (DMP) enrollment, this decision is controlled by the effective authentication policy of the user for the DMP application in use.
  - **Enrolled Users**
    - Enrollment policy defines certain aspects of enrolled users’ self-service portal (SSP) experience once they have gained access to the SSP.
    - Enrollment policy **does not** define the requirements for access into the SSP. The effective policy for access into the SSP is determined by:

      When using SSP in line with an app or via Duo Central
      - If SSP Policy is enabled, the effective SSP policy for that user.
      - If SSP Policy is not enabled, the effective policy for the inline application being accessed.

      When using SSP with a DMP application
      - If using a DMP, the effective policy for the user accessing that DMP application.

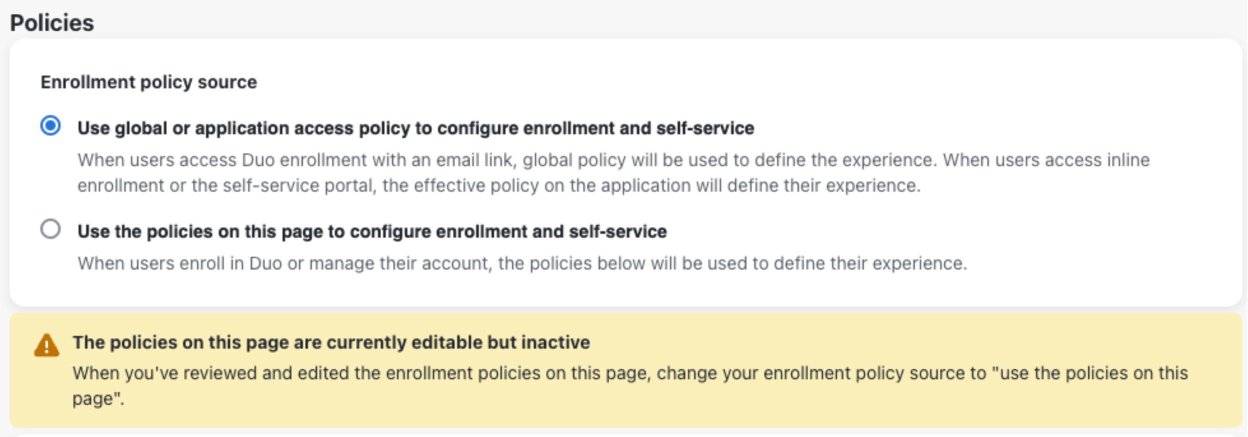
Navigation:

Enrollment Policy is in the Admin Panel under **Policies → Enrollment**



Enrollment Policy Source:

This setting defines, for overlapping controls, whether **Global or Application Polices** or **Enrollment policies** defined on this page will take effect for enrollment and self-service portals. A banner will display below this setting when this page's policies are not in effect. This is the current default.



Policies

Enrollment policy source

● **Use global or application access policy to configure enrollment and self-service**
When users access Duo enrollment with an email link, global policy will be used to define the experience. When users access inline enrollment or the self-service portal, the effective policy on the application will define their experience.

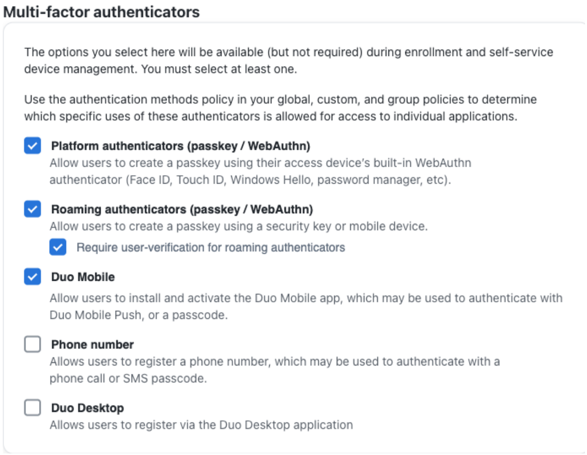
○ **Use the policies on this page to configure enrollment and self-service**
When users enroll in Duo or manage their account, the policies below will be used to define their experience.

⚠ **The policies on this page are currently editable but inactive**
When you've reviewed and edited the enrollment policies on this page, change your enrollment policy source to "use the policies on this page".

Note: Before enabling this setting, take care to ensure enrollment policies are configured as desired as this change takes place immediately.

Available Controls:

- **Multi-Factor Authenticators –** This control determines what options users will have when adding devices during enrollment and within the SSP. This is our recommended configuration for enabled authenticators:

  Multi-factor authenticators

  The options you select here will be available (but not required) during enrollment and self-service device management. You must select at least one.

  Use the authentication methods policy in your global, custom, and group policies to determine which specific uses of these authenticators is allowed for access to individual applications.

  ☑ **Platform authenticators (passkey / WebAuthn)**
  Allow users to create a passkey using their access device's built-in WebAuthn authenticator (Face ID, Touch ID, Windows Hello, password manager, etc).

  ☑ **Roaming authenticators (passkey / WebAuthn)**
  Allow users to create a passkey using a security key or mobile device.
  ☑ Require user-verification for roaming authenticators

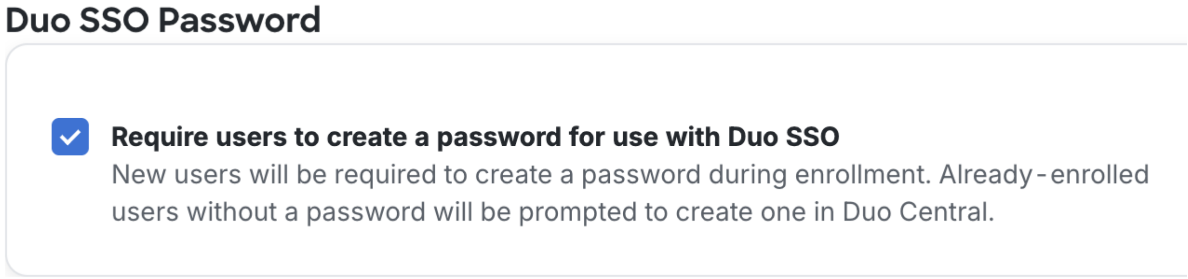
  ☑ **Duo Mobile**
  Allow users to install and activate the Duo Mobile app, which may be used to authenticate with Duo Mobile Push, or a passcode.

  □ **Phone number**
  Allows users to register a phone number, which may be used to authenticate with a phone call or SMS passcode.

  □ **Duo Desktop**
  Allows users to register via the Duo Desktop application

  Note: This control will be renamed since it contains both multi-factor and Passwordless authenticators.

- Duo SSO Password – This setting determines whether a user will be required to set a password during enrollment. If an already enrolled user without a password later becomes part of an enrollment policy requiring a password, they will be prompted to set it upon next successful authentication to any Duo SSO application.



Duo SSO Password

☑ **Require users to create a password for use with Duo SSO**
New users will be required to create a password during enrollment. Already-enrolled users without a password will be prompted to create one in Duo Central.

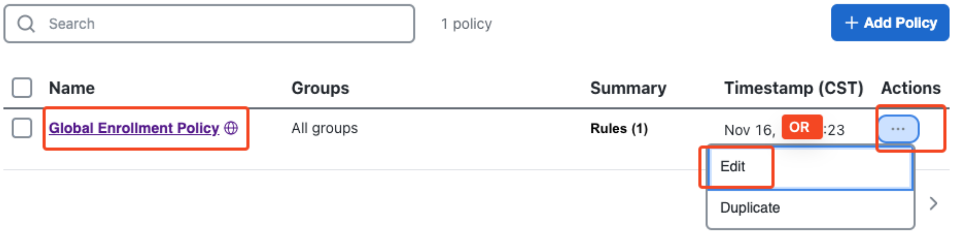
Configuring Policies:

Since the enrollment and self-service portals can be invoked from a variety of applications, enrollment policies apply across all applications and are set at the **Group** and **Global** scopes. The hierarchy works like this:

- **Group –** Items specified in this policy apply to all users who are members of any group(s) this policy is applied to. This applies across all applications. If users are members of multiple group policies, the effective policy will be determined by the order in which the global group policies are applied. Users cannot have more than one global group policy apply at one time.
- **Global –** This is the organization's default policy and is applied when no superseding policy applies.
    - If there are multiple configurable sections in the policy, it is possible that the user's effective enrollment policy will be a blend of an item specified at the Global Group and Global scopes. **Note:** There is currently only one configurable section, but this will be true as additional functionality is added in the future.
    - If a user is not subject to any Global Group policies, then they are subject only to the Global enrollment policy.

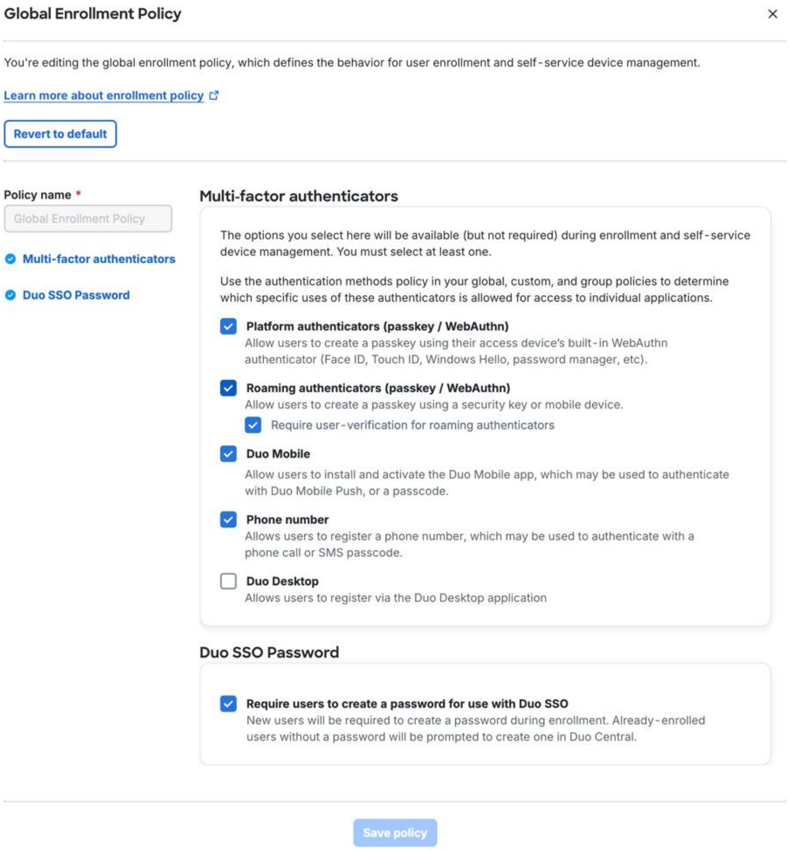
Configure the Global Enrollment Policy:

1. To configure the global enrollment policy, you can click on the policy name or click on the corresponding ellipses in the **Actions** column.



☐	Name	Groups	Summary	Timestamp (CST)	Actions
☐	Global Enrollment Policy	All groups	Rules (1)	Nov 16, :23	···

2. Ensure your organization's desired default settings for the available controls are set properly and click **Save Policy** if any changes have been made.



Global Enrollment Policy ×

You're editing the global enrollment policy, which defines the behavior for user enrollment and self-service device management.

Learn more about enrollment policy

Revert to default

Policy name *
Global Enrollment Policy

Multi-factor authenticators
Duo SSO Password

Multi-factor authenticators

The options you select here will be available (but not required) during enrollment and self-service device management. You must select at least one.

Use the authentication methods policy in your global, custom, and group policies to determine which specific uses of these authenticators is allowed for access to individual applications.

☑ **Platform authenticators (passkey / WebAuthn)**
Allow users to create a passkey using their access device's built-in WebAuthn authenticator (Face ID, Touch ID, Windows Hello, password manager, etc).

☑ **Roaming authenticators (passkey / WebAuthn)**
Allow users to create a passkey using a security key or mobile device.
☑ Require user-verification for roaming authenticators

☑ **Duo Mobile**
Allow users to install and activate the Duo Mobile app, which may be used to authenticate with Duo Mobile Push, or a passcode.

☑ **Phone number**
Allows users to register a phone number, which may be used to authenticate with a phone call or SMS passcode.

☐ **Duo Desktop**
Allows users to register via the Duo Desktop application

Duo SSO Password

☑ **Require users to create a password for use with Duo SSO**
New users will be required to create a password during enrollment. Already-enrolled users without a password will be prompted to create one in Duo Central.

Save policy

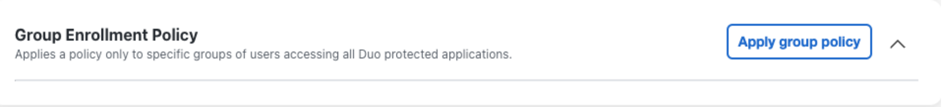
Note: The Global Enrollment Policy cannot be assigned, unassigned, or deleted.

Create a Group Enrollment Policy:

1. Select **Add Policy**
2. Enter a name for the policy
3. Click on and configure any sections you want to apply that differ from the global enrollment policy
4. Click **Create policy**

Apply a Group Enrollment Policy:

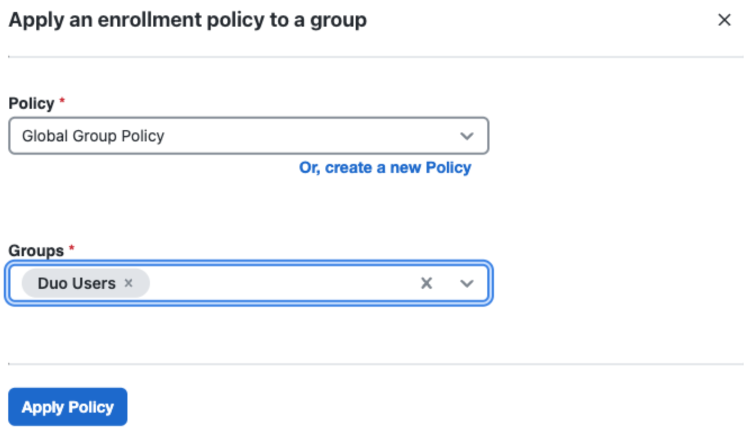
1. Under the **Group Enrollment Policy** section, click **Apply group policy**



Group Enrollment Policy

Applies a policy only to specific groups of users accessing all Duo protected applications.

2. Under **Policy**, select the Group Enrollment Policy you want to apply
3. Under **Groups**, select the group(s) you want to apply this policy to.
4. Click **Apply Policy**



Apply an enrollment policy to a group

Policy *

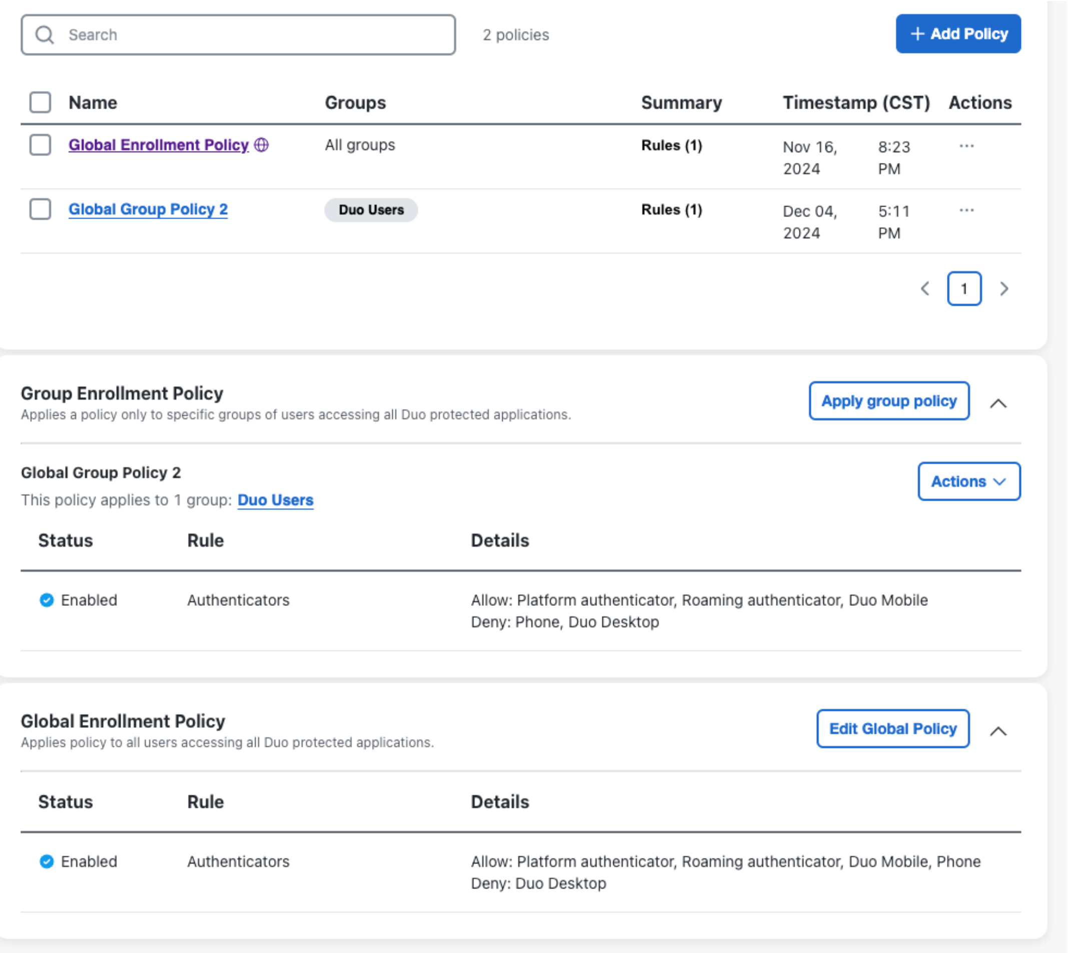
Global Group Policy

Groups *

Duo Users

5. You should now see the table of enrollment policies reflecting the changes you made. Additionally, you will see more detailed information and a visual hierarchy of the policies

below this summary table.



□	Name	Groups	Summary	Timestamp (CST)		Actions
□	Global Enrollment Policy	All groups	Rules (1)	Nov 16, 2024	8:23 PM	···
□	Global Group Policy 2	Duo Users	Rules (1)	Dec 04, 2024	5:11 PM	···

Group Enrollment Policy

Applies a policy only to specific groups of users accessing all Duo protected applications.

Global Group Policy 2

This policy applies to 1 group: Duo Users

Status	Rule	Details
Enabled	Authenticators	Allow: Platform authenticator, Roaming authenticator, Duo Mobile Deny: Phone, Duo Desktop

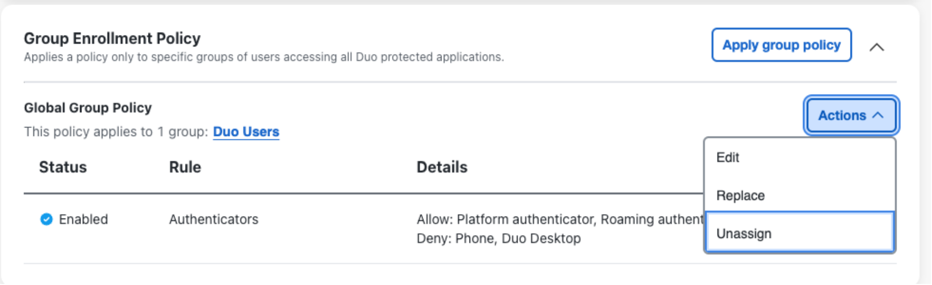
Global Enrollment Policy

Applies policy to all users accessing all Duo protected applications.

Status	Rule	Details
Enabled	Authenticators	Allow: Platform authenticator, Roaming authenticator, Duo Mobile, Phone Deny: Duo Desktop

Unassigning Group Enrollment Policies

1. Under the **Group Enrollment Policy** section, locate the policy you want to unassign
2. Select **Actions → Unassign**



Group Enrollment Policy

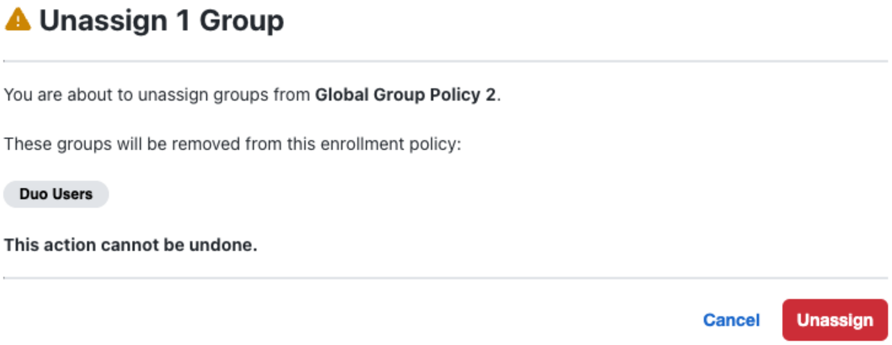
Applies a policy only to specific groups of users accessing all Duo protected applications.

Global Group Policy

This policy applies to 1 group: Duo Users

Status	Rule	Details
Enabled	Authenticators	Allow: Platform authenticator, Roaming authent Deny: Phone, Duo Desktop

3. A dialog will appear confirming your action. Select **Unassign** to continue



Unassign 1 Group

You are about to unassign groups from **Global Group Policy 2**.

These groups will be removed from this enrollment policy:

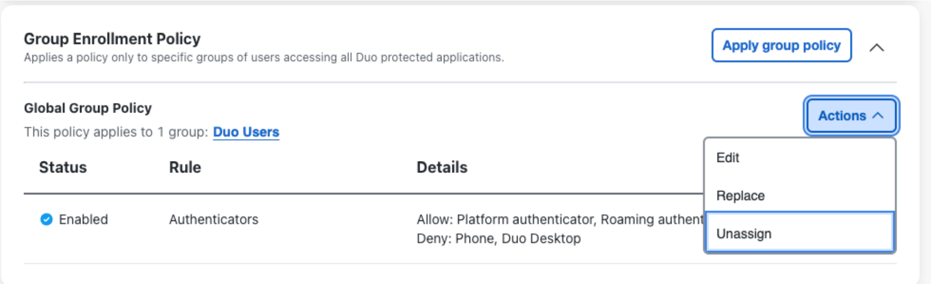
Duo Users

This action cannot be undone.

Replacing Group Enrollment Policies

As opposed to unassigning and then reassigning group enrollment policies, you can also simply replace them:

1. Under the **Group Enrollment Policy** section, locate the policy you want to replace
2. Select **Actions → Replace**



Group Enrollment Policy

Applies a policy only to specific groups of users accessing all Duo protected applications.

Global Group Policy

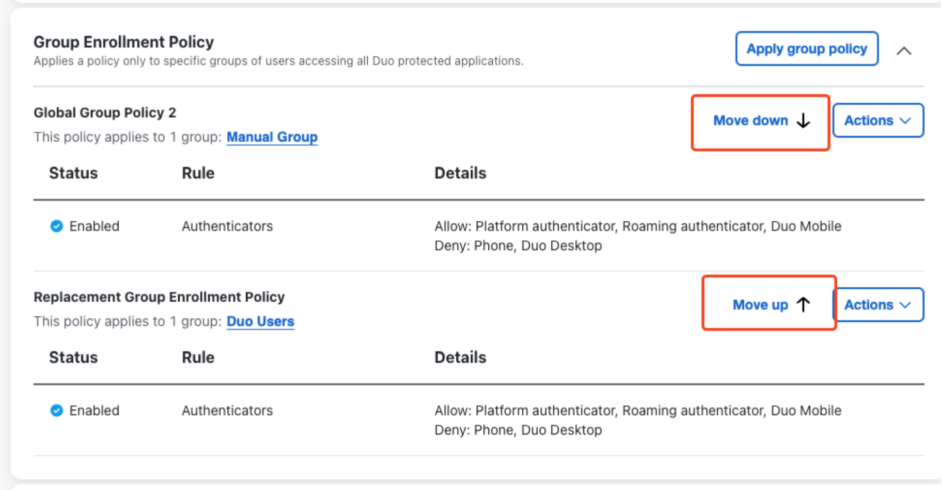
This policy applies to 1 group: Duo Users

Status	Rule	Details
✓ Enabled	Authenticators	Allow: Platform authenticator, Roaming authent Deny: Phone, Duo Desktop

3. Under **Policies**, select the policy you want to apply these groups too instead
4. Under **Groups,** review add or remove any groups to this reflects the desired application of this policy
5. Click **Apply Policy**

Reordering Group Enrollment Policies

If you have multiple group enrollment policies, you will see **Move Up** and **Move Down** options for each applied policy in the **Group Enrollment Policies** section



Group Enrollment Policy
Applies a policy only to specific groups of users accessing all Duo protected applications.

Global Group Policy 2
This policy applies to 1 group: Manual Group

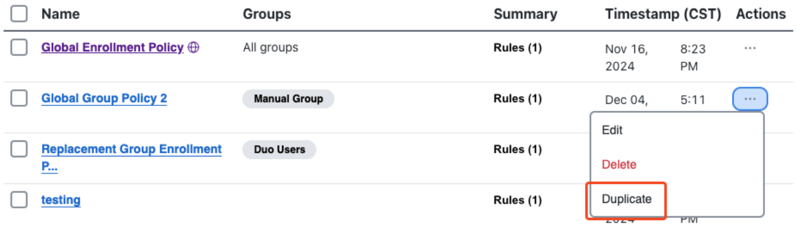
Status	Rule	Details
Enabled	Authenticators	Allow: Platform authenticator, Roaming authenticator, Duo Mobile Deny: Phone, Duo Desktop

Replacement Group Enrollment Policy
This policy applies to 1 group: Duo Users

Status	Rule	Details
Enabled	Authenticators	Allow: Platform authenticator, Roaming authenticator, Duo Mobile Deny: Phone, Duo Desktop

Duplicating Enrollment Policies

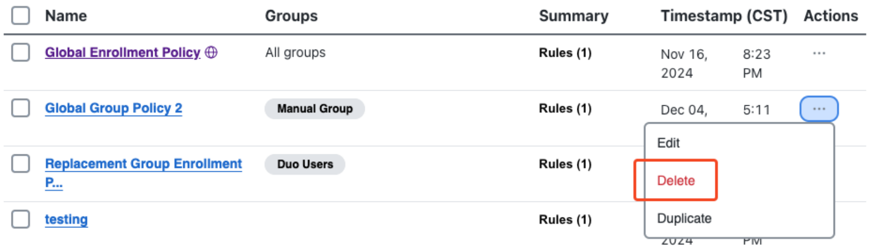
1. From the full enrollment policy list, locate the policy you want to duplicate and select the actions ellipses → **Duplicate**
2. A new policy will automatically be created under the same name, but with “copy” appended to the end
3. When duplicated, this new policy will not be assigned to any groups



□	Name	Groups	Summary	Timestamp (CST)	Actions
□	Global Enrollment Policy	All groups	Rules (1)	Nov 16, 2024 8:23 PM	···
□	Global Group Policy 2	Manual Group	Rules (1)	Dec 04, 5:11	···
□	Replacement Group Enrollment P...	Duo Users	Rules (1)		
□	testing		Rules (1)	2024 PM	

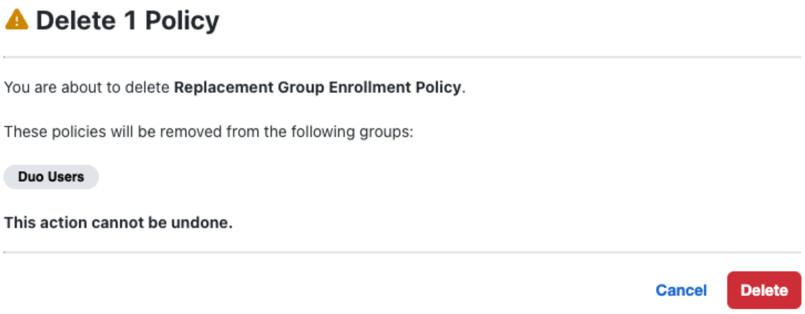
Deleting Group Enrollment Policies

1. From the full enrollment policy list, locate the policy you want to delete and select the actions ellipses → **Delete**



□	Name	Groups	Summary	Timestamp (CST)	Actions
□	Global Enrollment Policy	All groups	Rules (1)	Nov 16, 2024 8:23 PM	···
□	Global Group Policy 2	Manual Group	Rules (1)	Dec 04, 5:11	···
□	Replacement Group Enrollment P...	Duo Users	Rules (1)		
□	testing		Rules (1)	2024 PM	

2. Carefully review and then confirm by selecting **Delete**



⚠ Delete 1 Policy

You are about to delete **Replacement Group Enrollment Policy**.

These policies will be removed from the following groups:

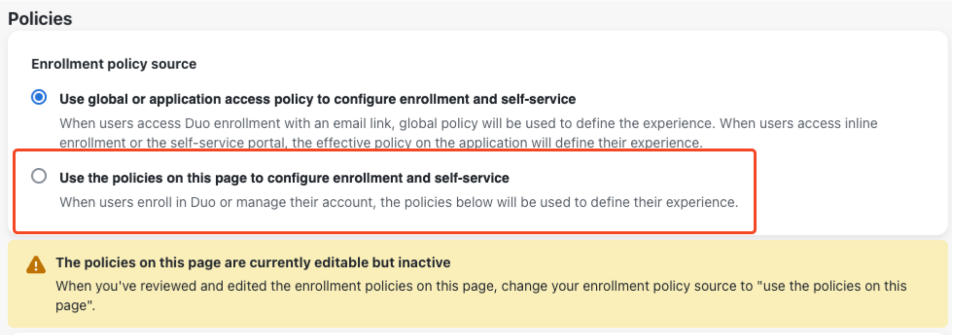
Duo Users

This action cannot be undone.

Enabling Enrollment Policies:

Once you have fully configured your policies, return to the **Enrollment Policy Source** section:

1. Select **Use the policies on this page to configure enrollment and self-service**



Policies

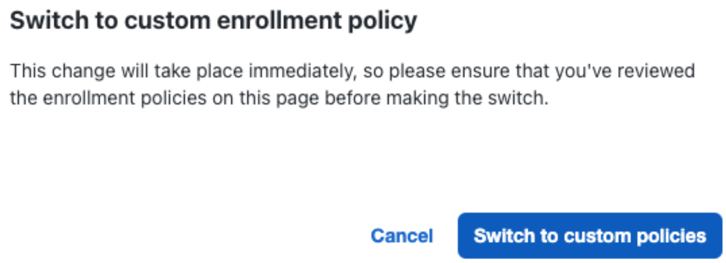
Enrollment policy source

● **Use global or application access policy to configure enrollment and self-service**
When users access Duo enrollment with an email link, global policy will be used to define the experience. When users access inline enrollment or the self-service portal, the effective policy on the application will define their experience.

○ **Use the policies on this page to configure enrollment and self-service**
When users enroll in Duo or manage their account, the policies below will be used to define their experience.

⚠ **The policies on this page are currently editable but inactive**
When you've reviewed and edited the enrollment policies on this page, change your enrollment policy source to "use the policies on this page".

2. Confirm the change by selecting **Switch to custom policies**



Switch to custom enrollment policy

This change will take place immediately, so please ensure that you've reviewed the enrollment policies on this page before making the switch.

You are now ready to test enrollment policies!

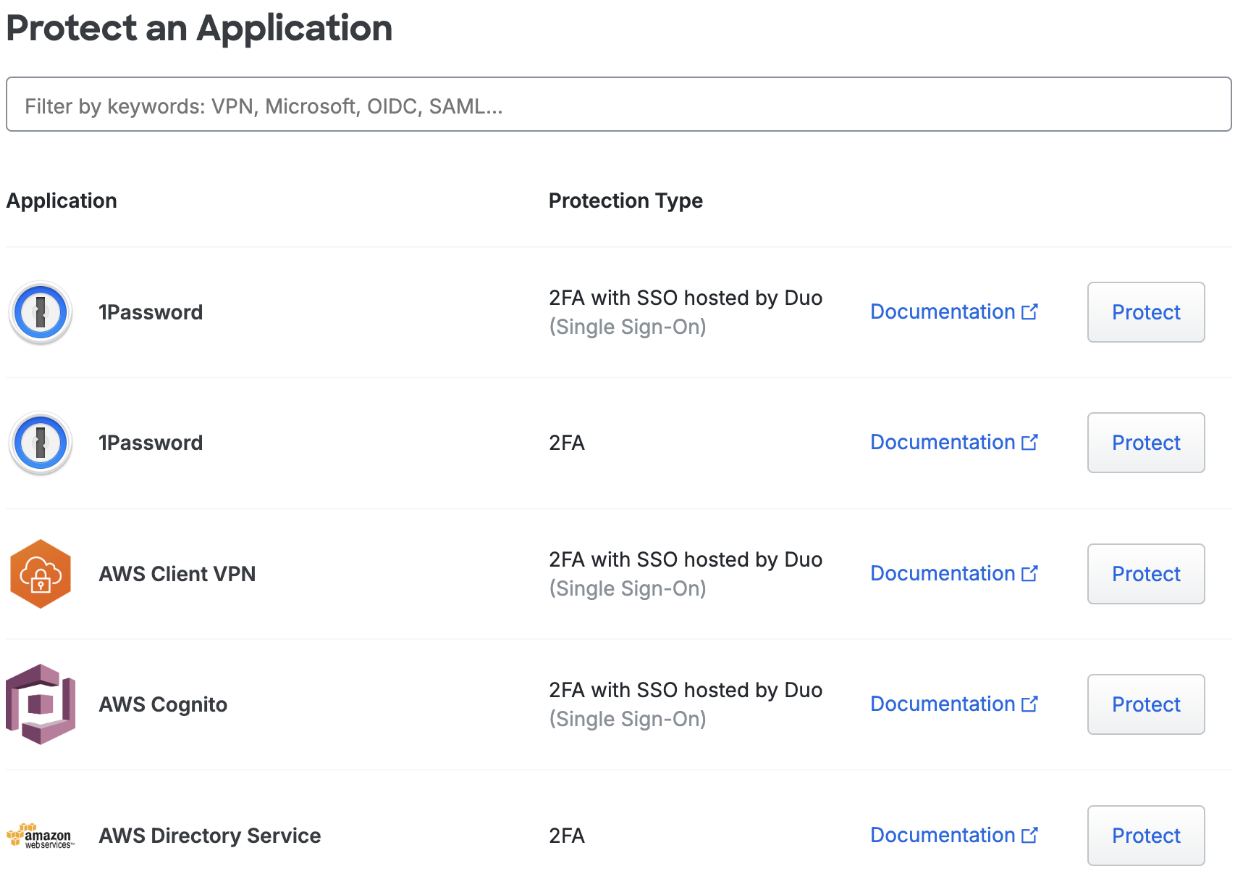
Enrollment Policy Limitations:

- When assigning or replacing an existing enrollment policy to a group the “Or, create a new Policy” button will send you to the modal to create an enrollment policy but will not drop you back into the assign/replace modal after. While we work on a fix, you will have to go back to the modal to manually select your newly added enrollment policy instead.

Create an SSO Supported Application

Role required: Owner, Administrator, or Application Manager.

1. Log into the Duo Admin Panel. To add a new application, navigate to **Applications** → **Protect an Application**. Alternatively, you can click the **Add New...** button in the top right of the Home page and then click **Application**.
2. The "Protect an Application" page lists the different types of services you can protect with Duo. The **Protection Type** column indicates how Duo protects that specific application.



Protect an Application

Filter by keywords: VPN, Microsoft, OIDC, SAML...

Application	Protection Type		
1Password	2FA with SSO hosted by Duo (Single Sign-On)	Documentation	Protect
1Password	2FA	Documentation	Protect
AWS Client VPN	2FA with SSO hosted by Duo (Single Sign-On)	Documentation	Protect
AWS Cognito	2FA with SSO hosted by Duo (Single Sign-On)	Documentation	Protect
AWS Directory Service	2FA	Documentation	Protect

You can scroll down the page to browse all available applications, or start typing the name of your product in the space provided to filter the applications list. Look for applications tagged with '2FA with SSO hosted by Duo (Single Sign-On)'

Set Up Provisioning Into SCIM Supported Applications

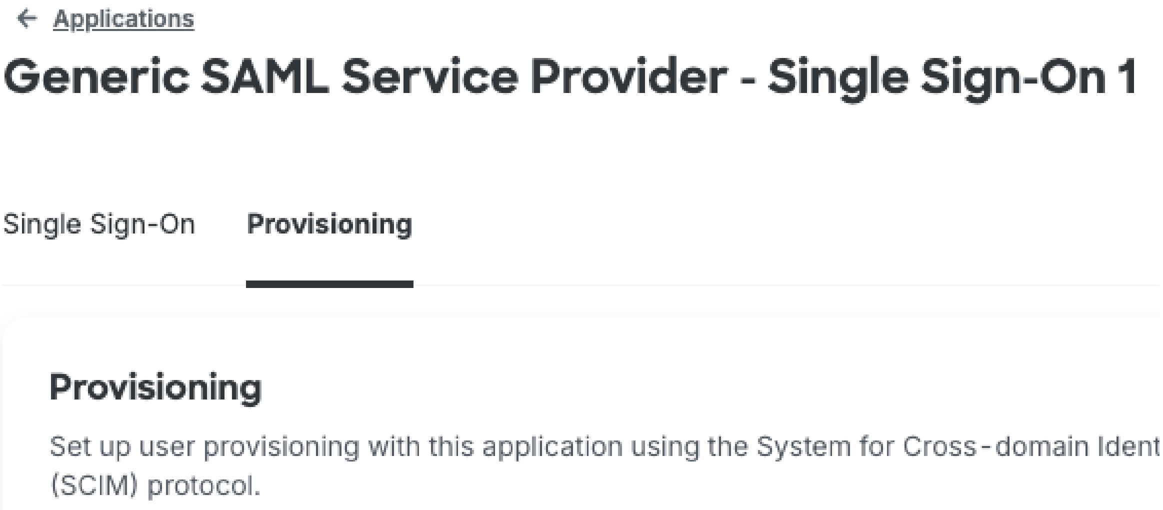
To use this feature successfully, make sure your target application supports SCIM provisioning, and review their documentation to identify:

- What attributes they support and require for a user
- What authentication mechanisms they support. Bearer token and client credential authentication mechanisms are available on all provisioning supported applications. A 'Cloud Connection' (OAuth Auth Code grant) flow for limited applications.

View this vidcast to learn more about this feature.

Steps:

1. Select your desired SSO application from your list of applications, and click the **Provisioning** tab



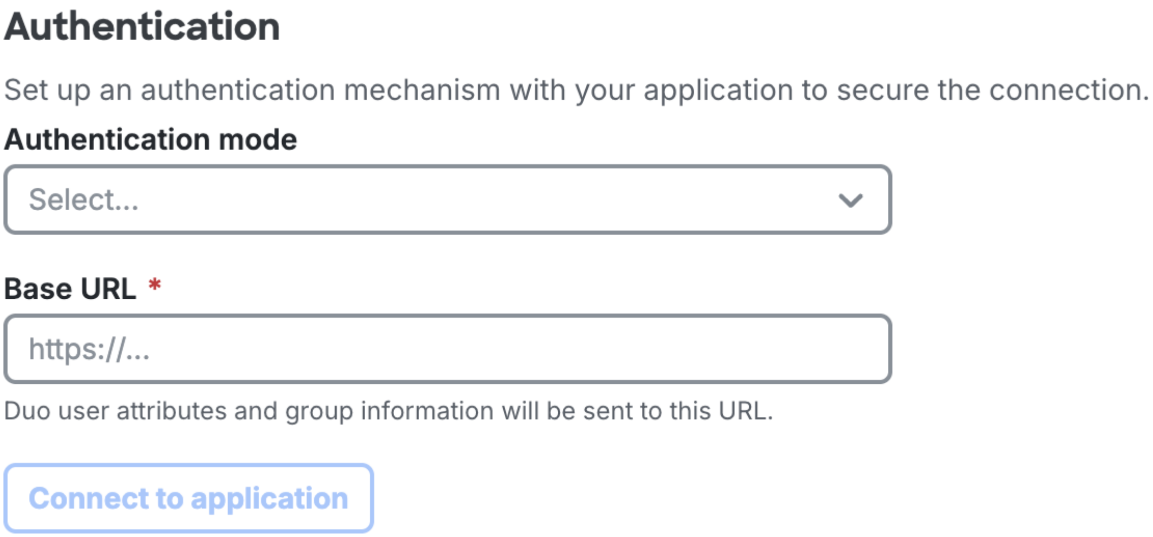
← Applications

Generic SAML Service Provider - Single Sign-On 1

Provisioning

Set up user provisioning with this application using the System for Cross-domain Ident
(SCIM) protocol.

2. Select which **Authentication mode** you would like use to connect to your target application. Please consult your target application's documentation to understand what authentication methods they support, and where to gather the credentials needed to authenticate.



Authentication

Set up an authentication mechanism with your application to secure the connection.

Authentication mode

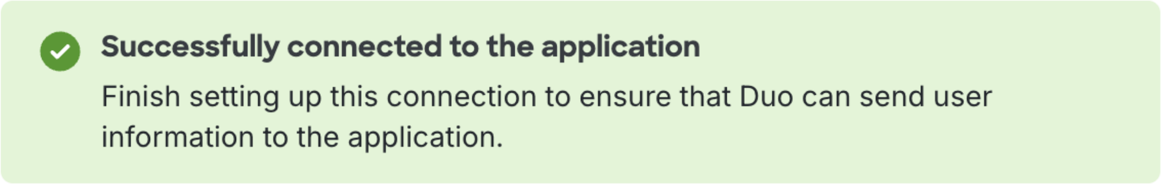
Select...

Base URL *

https://...

Duo user attributes and group information will be sent to this URL.

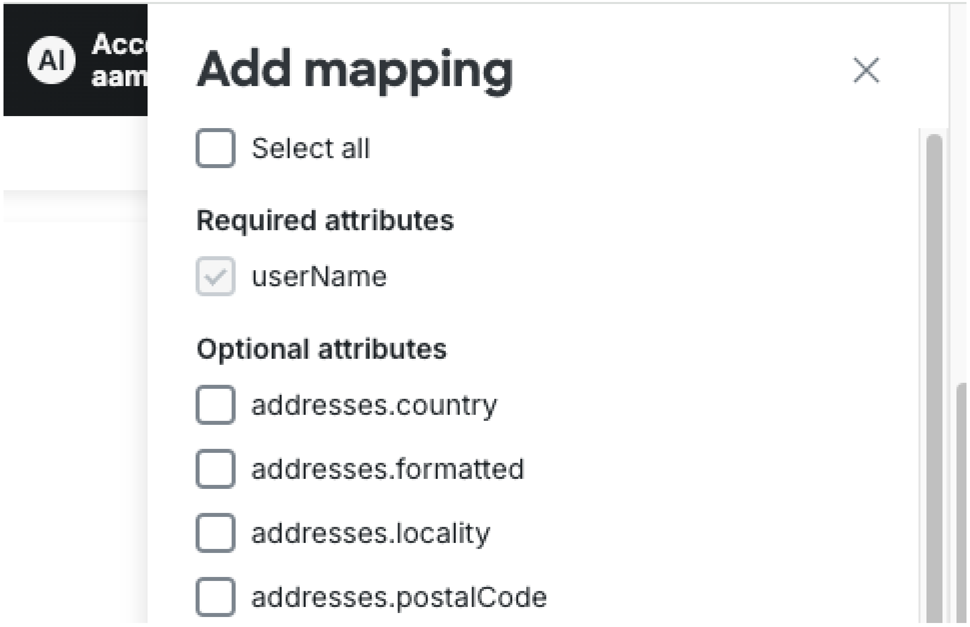
3. Copy and paste the Base SCIM URL into Duo and provide the rest of the required details from the application. Select ‘**Connect to Application**’ when you are finished. A confirmation message should appear if done successfully.



Successfully connected to the application

Finish setting up this connection to ensure that Duo can send user information to the application.

4. Select which attributes you would like to send to the application. Confirm what attributes are required with your target application by reviewing their documentation. To add additional attributes, click **+ Edit mappings** and select from the available SCIM attributes.



Add mapping

□ Select all

Required attributes

☑ userName

Optional attributes

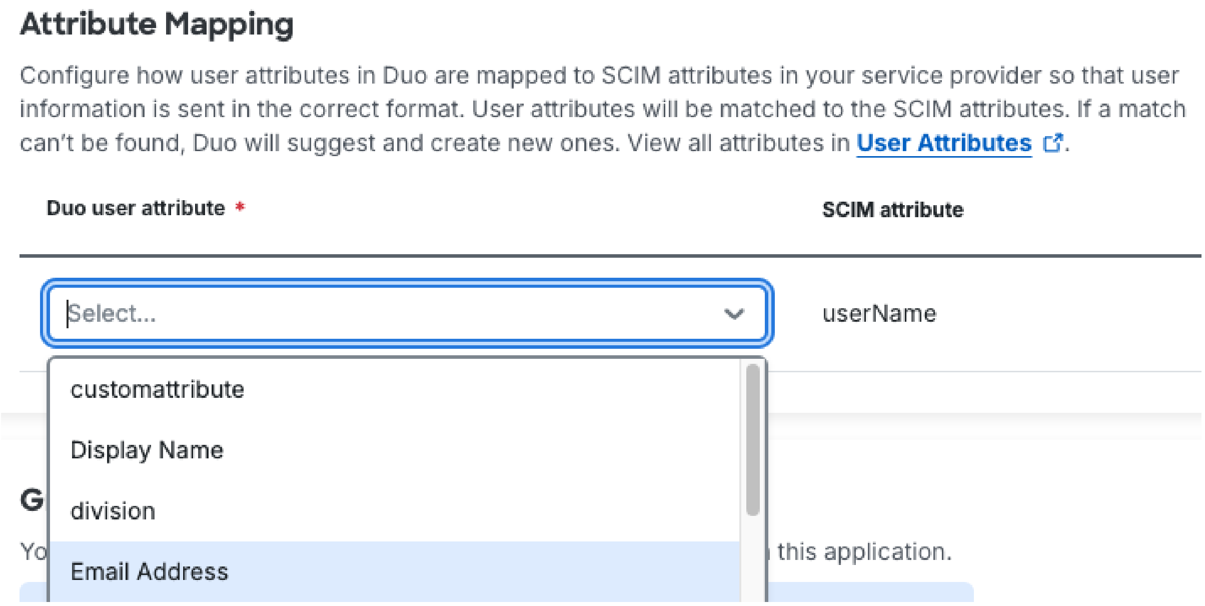
□ addresses.country

□ addresses.formatted

□ addresses.locality

□ addresses.postalCode

In the mapping table, select which Duo User Attributes you would like to send for each selected SCIM attribute.

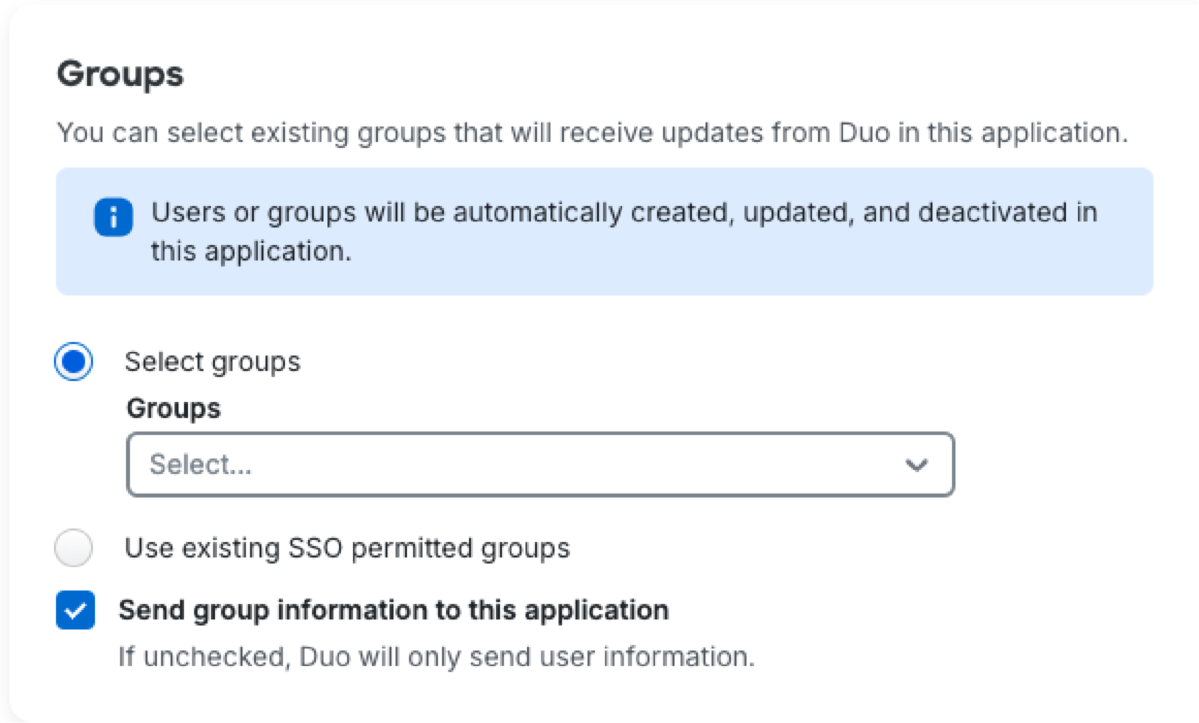


Attribute Mapping

Configure how user attributes in Duo are mapped to SCIM attributes in your service provider so that user information is sent in the correct format. User attributes will be matched to the SCIM attributes. If a match can't be found, Duo will suggest and create new ones. View all attributes in **User Attributes**.

Duo user attribute *	SCIM attribute
Select...	userName

5. Select which Groups you would like to provision into your target application. If you have already set up SSO with this application, you can quickly mirror your configuration by selecting the '**Use existing SSO permitted groups**' option. Alternatively, you can select groups individually from the drop down.



Groups

You can select existing groups that will receive updates from Duo in this application.

Users or groups will be automatically created, updated, and deactivated in this application.

● Select groups

Groups

Select...

○ Use existing SSO permitted groups

☑ **Send group information to this application**

If unchecked, Duo will only send user information.

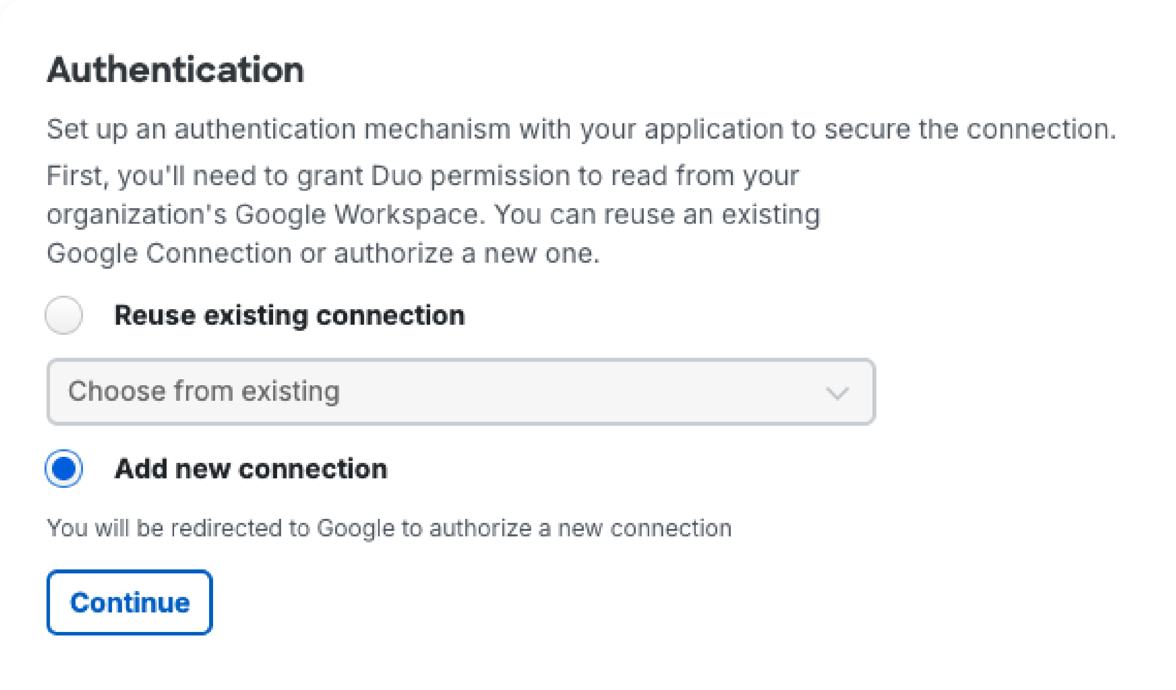
If you would like to create and manage these groups in your target application, leave the checkbox checked. If you would prefer to only provision users and not provision groups, uncheck this box.

6. Click **Save** and your provisioning should now be live. Confirm that it is working by looking at your connected application for the users and/or groups that you selected in the provisioning setup. You can also see reports of attempted actions within Duo by selecting **Reports** and then **Administrator Actions**.

Set Up Provisioning for Google

1. Open an existing “Google Workspace - Single Sign-On” application configuration page or create a new application by clicking *+ Protect an Application* and searching for Google Workspace.
2. Click on **Provisioning** tab.

3. Configure authentication to Google Workspace. Select either 'Add new connection' and click continue.



Authentication

Set up an authentication mechanism with your application to secure the connection.

First, you'll need to grant Duo permission to read from your organization's Google Workspace. You can reuse an existing Google Connection or authorize a new one.

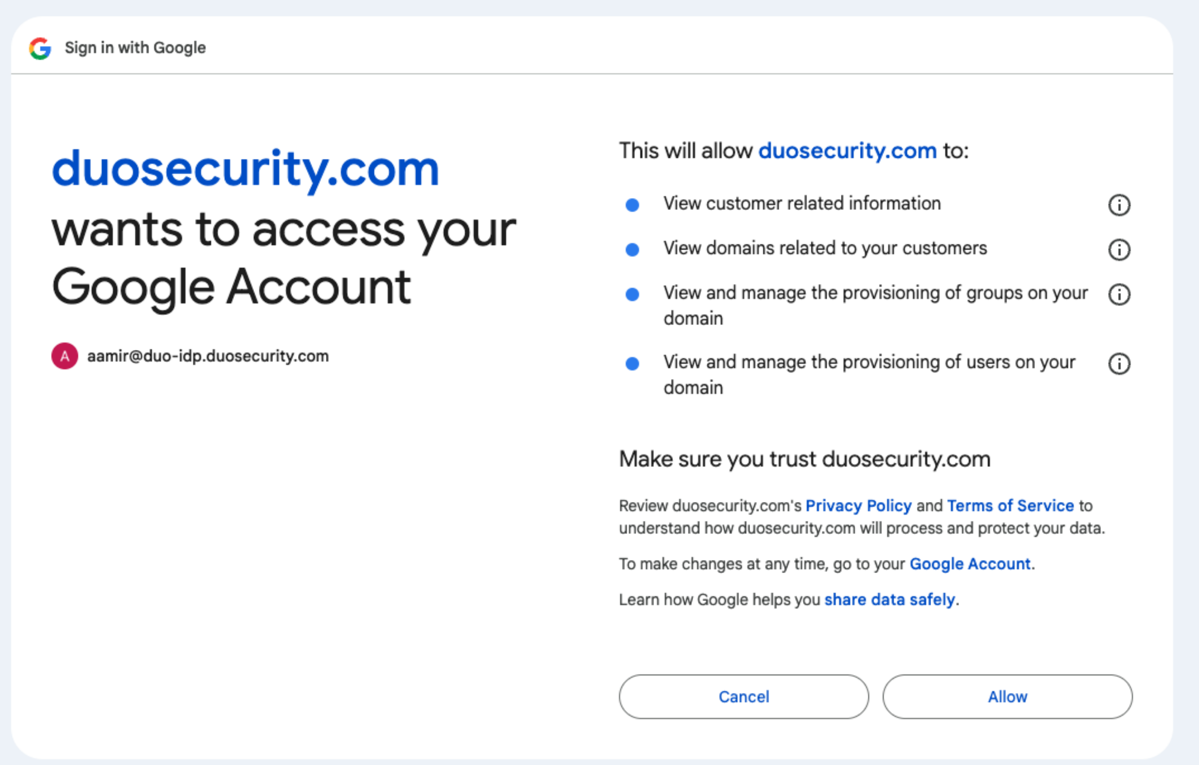
○ **Reuse existing connection**

Choose from existing

● **Add new connection**

You will be redirected to Google to authorize a new connection

4. Select 'Continue' and then choose your Google cloud identity login. You will be presented with a list of requested permissions. Click 'Allow'.



Sign in with Google

duosecurity.com wants to access your Google Account

aamir@duo-idp.duosecurity.com

This will allow **duosecurity.com** to:

- View customer related information
- View domains related to your customers
- View and manage the provisioning of groups on your domain
- View and manage the provisioning of users on your domain

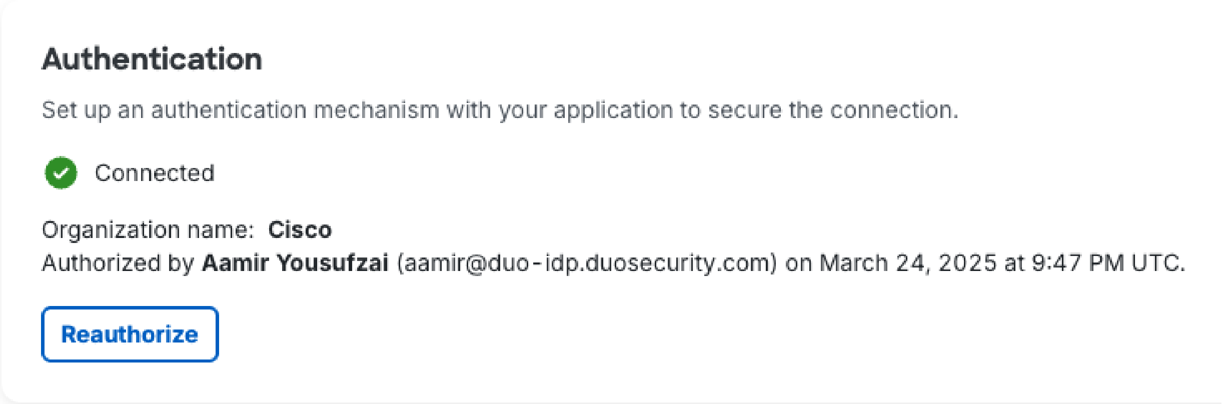
Make sure you trust duosecurity.com

Review duosecurity.com's **Privacy Policy** and **Terms of Service** to understand how duosecurity.com will process and protect your data.

To make changes at any time, go to your **Google Account**.

Learn how Google helps you **share data safely**.

5. You should be redirected back to your Google application in the Duo Admin Panel. Click the 'Provisioning' tab and confirm that you were connected successfully.



Authentication

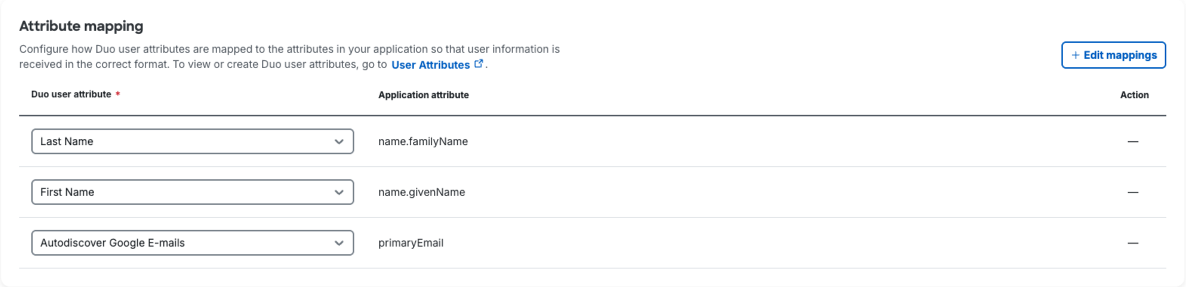
Set up an authentication mechanism with your application to secure the connection.

✓ Connected

Organization name: **Cisco**
Authorized by **Aamir Yousufzai** (aamir@duo-idp.duosecurity.com) on March 24, 2025 at 9:47 PM UTC.

6. In **Attribute mapping** section, the default required attributes should automatically appear. Suggested mappings are set, but you may choose which Duo User Attribute you wish to send for each required attribute by clicking the dropdown if you would like to send something else.

   Important Note: Google requires email values to belong to a domain you have configured in Google. The ‘Autodiscover Google E-mails' option will scan through the username, email and all alias values set for your users and automatically grab the value with the right domain. Alternatively, you can map to a specific Duo attribute if desired.

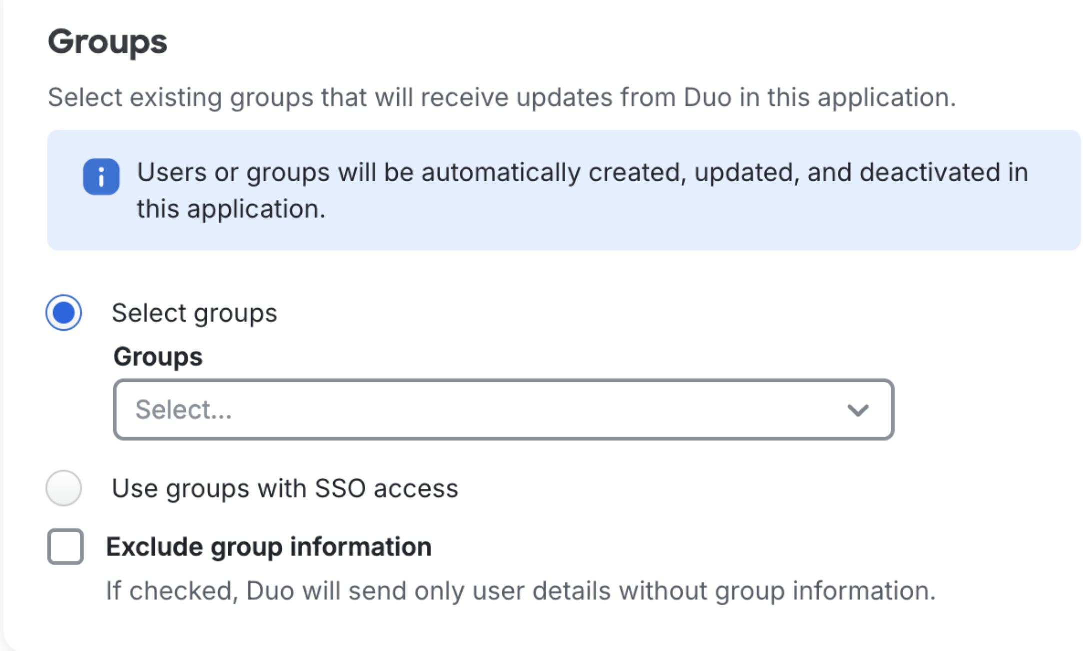


Attribute mapping

Configure how Duo user attributes are mapped to the attributes in your application so that user information is received in the correct format. To view or create Duo user attributes, go to **User Attributes**.

Duo user attribute *	Application attribute	Action
Last Name	name.familyName	—
First Name	name.givenName	—
Autodiscover Google E-mails	primaryEmail	—

7. Specify the desired **Groups** settings.



Groups

Select existing groups that will receive updates from Duo in this application.

Users or groups will be automatically created, updated, and deactivated in this application.

● Select groups

Groups

Select...

○ Use groups with SSO access

□ **Exclude group information**

If checked, Duo will send only user details without group information.

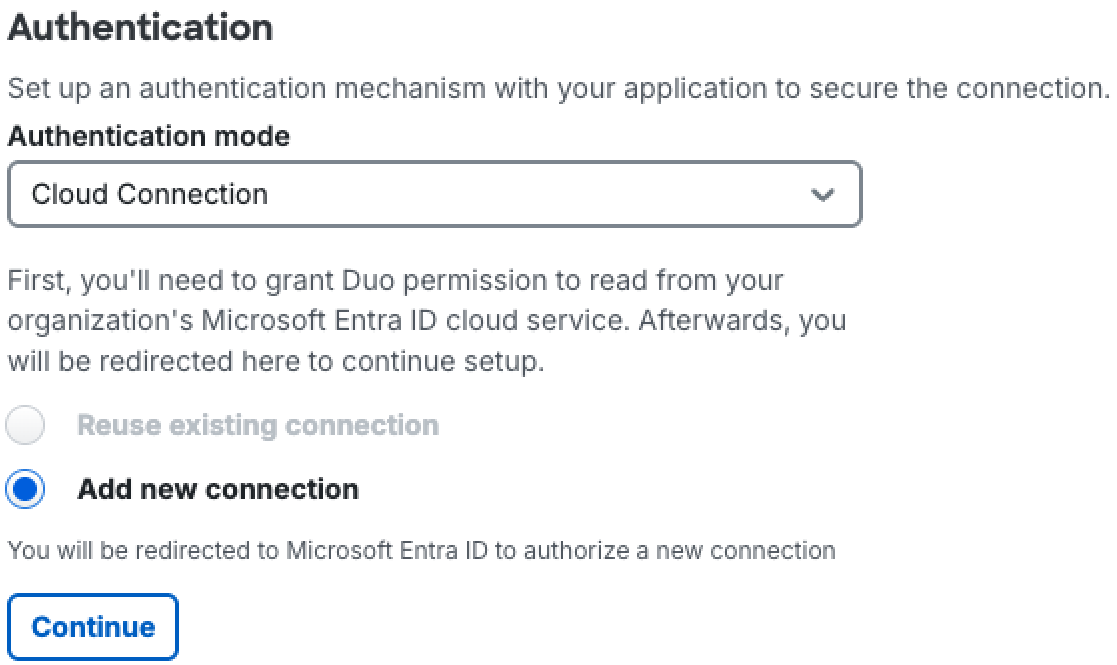
8. Click **Save**.

Set Up Provisioning for Microsoft 365

Configure Provisioning in the Microsoft 365 Application

1. Open an existing “Microsoft 365 - Single Sign-On” application configuration page or create a new application by clicking *+ Protect an Application* and searching for Microsoft 365.
2. Click on **Provisioning** tab.
3. Configure authentication to Microsoft 365. Select either ‘Cloud Connection’ or ‘Client Credential’ for authentication mode. These instructions assume you chose ‘Cloud

Connection.’ Instructions for the ‘Client Credential’ flow are found here.



Authentication

Set up an authentication mechanism with your application to secure the connection.

Authentication mode

Cloud Connection

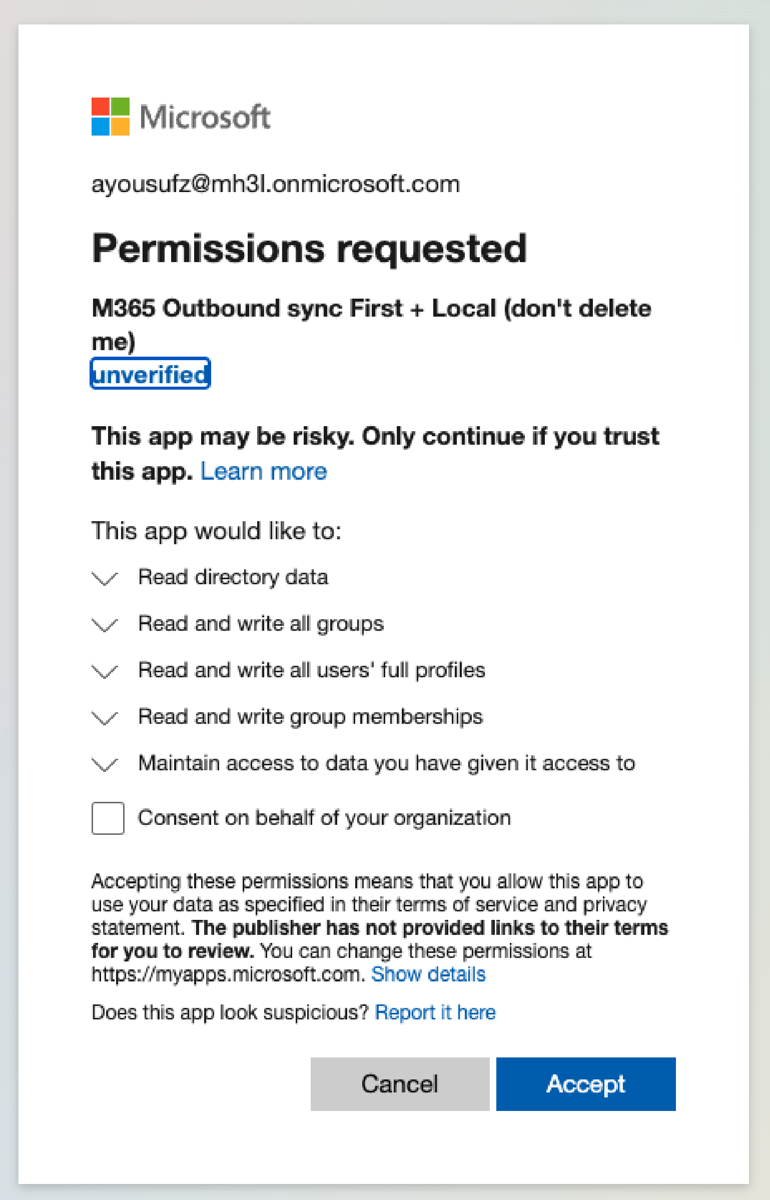
First, you'll need to grant Duo permission to read from your organization's Microsoft Entra ID cloud service. Afterwards, you will be redirected here to continue setup.

○ Reuse existing connection

● Add new connection

You will be redirected to Microsoft Entra ID to authorize a new connection

4. Select 'Continue' and then choose your Microsoft 365 login. You will be presented with a list of requested permissions. Click accept.



ayousufz@mh3l.onmicrosoft.com

Permissions requested

M365 Outbound sync First + Local (don't delete me)
unverified

This app may be risky. Only continue if you trust this app. Learn more

This app would like to:

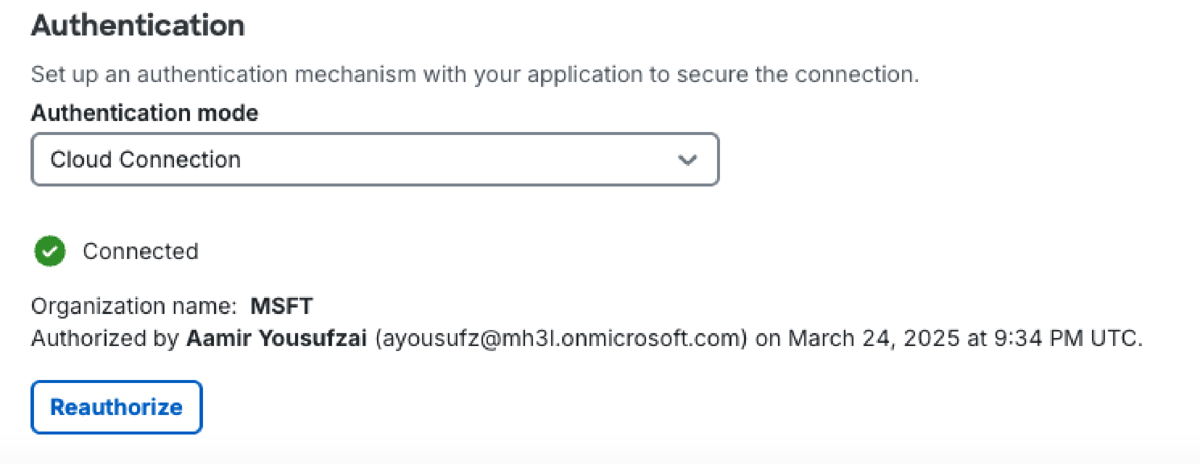
- Read directory data
- Read and write all groups
- Read and write all users' full profiles
- Read and write group memberships
- Maintain access to data you have given it access to

□ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

5. You should be redirected by to your Microsoft 365 application in the Duo Admin Panel. Click the 'Provisioning' tab and confirm that you were connected successfully.



Authentication

Set up an authentication mechanism with your application to secure the connection.

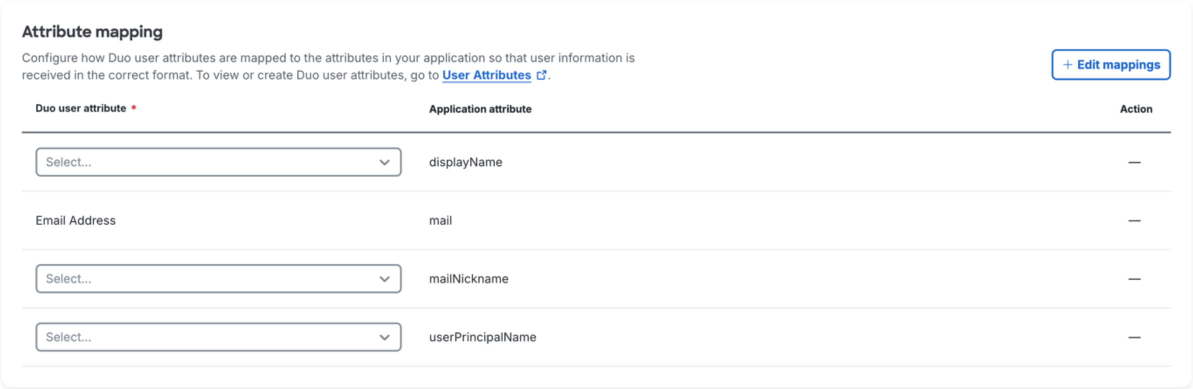
Authentication mode

Cloud Connection ⌄

✓ Connected

Organization name: **MSFT**
Authorized by **Aamir Yousufzai** (ayousufz@mh3l.onmicrosoft.com) on March 24, 2025 at 9:34 PM UTC.

6. In **Attribute mapping** section, the default required attributes should automatically appear. Choose which Duo User Attribute you wish to send for each required attribute by clicking the dropdown.



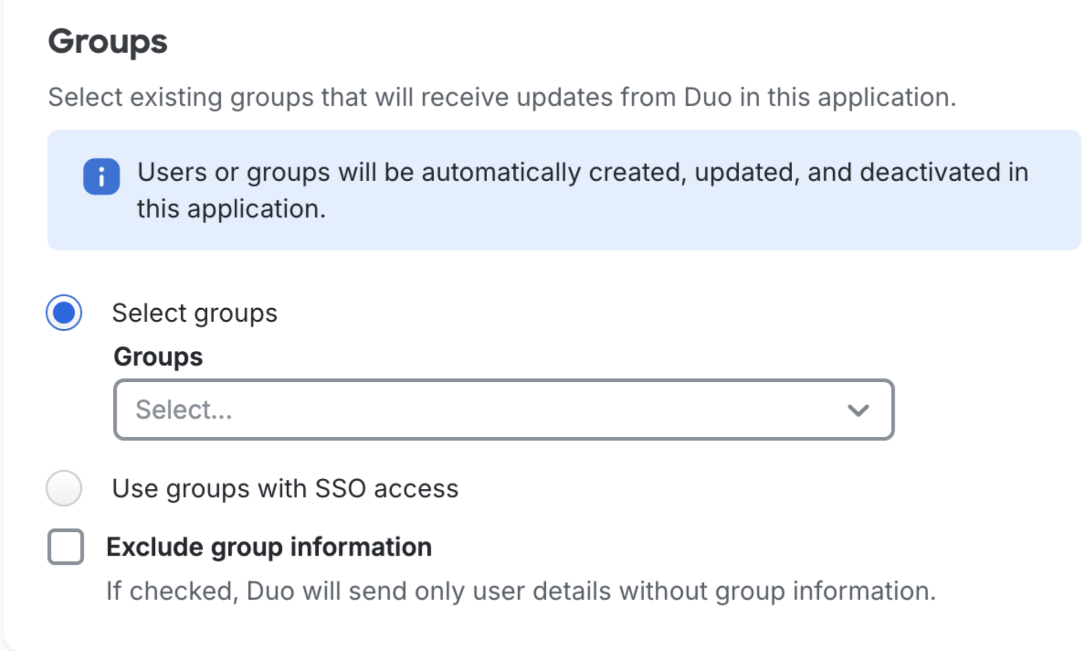
Attribute mapping

Configure how Duo user attributes are mapped to the attributes in your application so that user information is received in the correct format. To view or create Duo user attributes, go to User Attributes.

Duo user attribute *	Application attribute	Action
Select... ⌄	displayName	—
Email Address	mail	—
Select... ⌄	mailNickname	—
Select... ⌄	userPrincipalName	—

If you desire, you can add additional optional attributes by clicking the '+ Edit mappings' button and selecting from the drawer.

7. Specify the desired **Groups** settings.



Groups

Select existing groups that will receive updates from Duo in this application.

Users or groups will be automatically created, updated, and deactivated in this application.

● Select groups

Groups

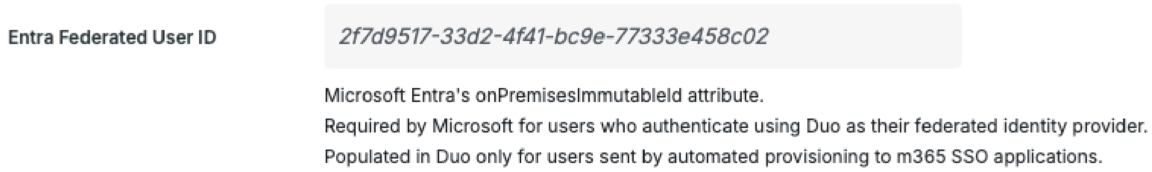
Select...

○ Use groups with SSO access

□ **Exclude group information**

If checked, Duo will send only user details without group information.

8. Click **Save**.
9. After you have provisioned users successfully, review at least one of the provisioned users in the Duo Admin Panel and confirm that they have a value populated for 'Entra Federated User ID'. This value is populated only by provisioning the user from Duo and is not editable. Users not assigned to provisioning for M365 should not have a value populated.



Entra Federated User ID: *2f7d9517-33d2-4f41-bc9e-77333e458c02*

Microsoft Entra's onPremisesImmutableId attribute.
Required by Microsoft for users who authenticate using Duo as their federated identity provider.
Populated in Duo only for users sent by automated provisioning to m365 SSO applications.

'Client Credential' Authentication for Microsoft 365

If you prefer to use the Client Credential flow instead of Cloud Connection, please follow these instructions:

Create Application

1. Sign in to the Microsoft Entra admin center with at least a Cloud Application Administrator privileges.
2. Go to **Identity** > **Applications** > **App registrations**.
3. Click on **+ New registration**.

4. Enter the name of the application.
5. Select the supported account types (e.g., Single tenant or Multi-tenant; Single tenant was used in this guide).
6. Click **Register**.
7. On the resulting page, copy **Application (client) ID** for later use as the Client ID in the Duo Admin Panel configuration page.
8. Copy the **Directory (tenant) ID** for later use as the Tenant ID in the Duo Admin Panel configuration page.

Create Client Secret

1. Go to **Certificates & secrets** > **New client secret**.
2. Enter a description and select an expiration period.
3. Click Add and copy the client secret **Value**. You'll need this in the Duo admin panel configuration page. Note that this value will only be shown once.

Grant Necessary Permissions for the application

1. In the registered application page, navigate to **API permissions**.
2. Click on **+ Add a permission**.
3. Select **Microsoft Graph**.
4. Select **Application permissions**.

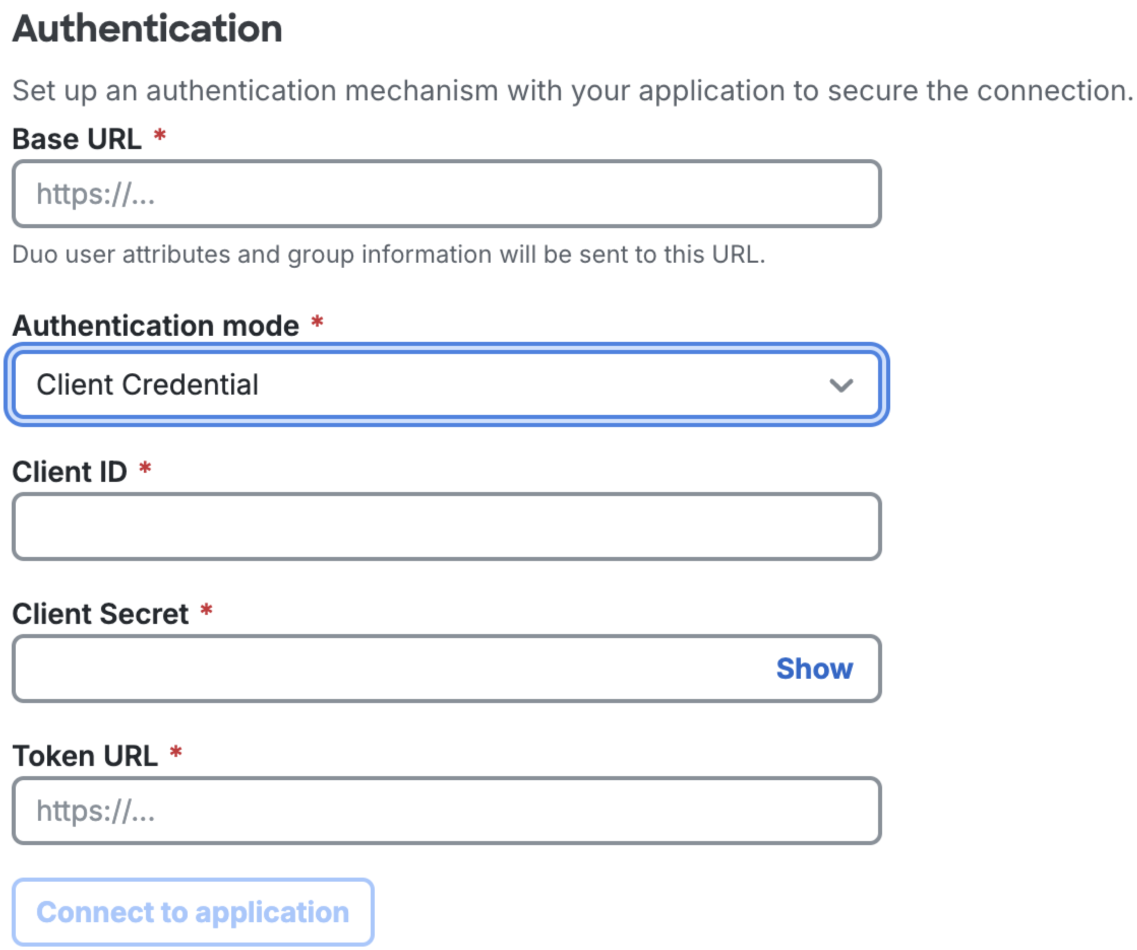
   Choose User.ReadWrite.All, Group.ReadWrite.All, GroupMember.ReadWrite.All, Directory.ReadWrite.All

5. Click **Add Permissions**.
6. Click **Grant admin consent for <your organization>** and then **Yes**.

Configure Provisioning in the Microsoft 365 Application

1. Open an existing "Microsoft 365 - Single Sign-On" application configuration page or create a new application by clicking *+ Protect an Application* and searching for Microsoft 365.

2. Click on **Provisioning** tab.



Authentication

Set up an authentication mechanism with your application to secure the connection.

Base URL *

https://...

Duo user attributes and group information will be sent to this URL.

Authentication mode *

Client Credential

Client ID *

Client Secret *

Token URL *

https://...

3. Configure authentication to Microsoft 365. At this time, select client credential flow is support.
   a. Set **Base URL** to https://graph.microsoft.com/v1.0/.
   b. Set **Authentication mode** to **Client Credential**.
   c. Enter the **Client ID**, and **Client Secret** that you copied in previous steps.
   d. Specify **Token URL** to https://login.microsoftonline.com/{TENANT_ID}/oauth2/v2.0/token replacing {TENANT_ID} with your actual Tenant ID.
4. Click **Connect to application** to verify the connection.

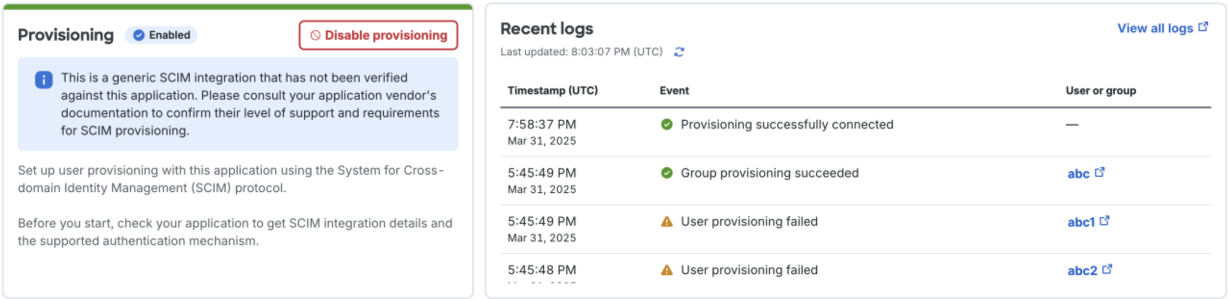
View Provisioning Logs

After you have configured an application for provisioning, Duo will begin to log any event related it generates for your review. These logs include:

- Configuration events, i.e. authenticating with your application

- User provisioning events (success/failure of individual user changes)
- Group provisioning events (success/failure of group changes)

These logs are viewable in two places. Immediately upon successful setup of an application, the **Recent logs** view will appear near the top right of the page. This view captures logs specific to the application you are currently viewing in the Duo admin panel, and updates in near real time with newly generated events.



Provisioning

This is a generic SCIM integration that has not been verified against this application. Please consult your application vendor's documentation to confirm their level of support and requirements for SCIM provisioning.

Set up user provisioning with this application using the System for Cross-domain Identity Management (SCIM) protocol.

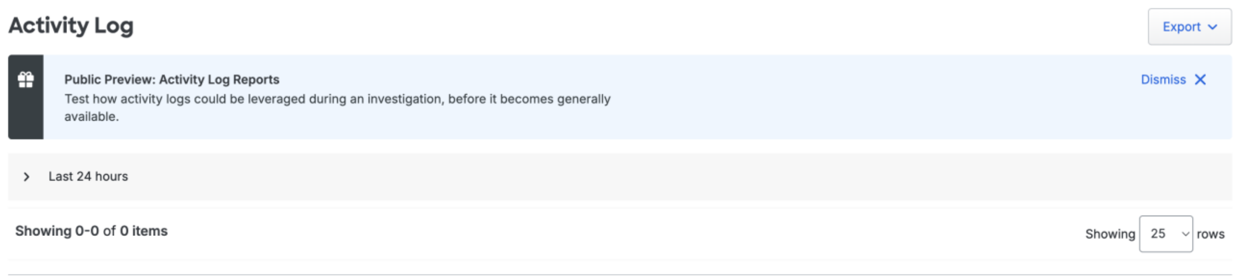
Before you start, check your application to get SCIM integration details and the supported authentication mechanism.

Recent logs

Last updated: 8:03:07 PM (UTC)

Timestamp (UTC)	Event	User or group
7:58:37 PM Mar 31, 2025	✓ Provisioning successfully connected	—
5:45:49 PM Mar 31, 2025	✓ Group provisioning succeeded	abc
5:45:49 PM Mar 31, 2025	⚠ User provisioning failed	abc1
5:45:48 PM	⚠ User provisioning failed	abc2

At the top right of the **Recent logs** view, you can click **View all logs** which will take you to our new **Activity Log**. Alternatively, this log can be reached from any place within the Duo admin panel by clicking *Reports* in the left navigation column, and then selecting *Activity Log*.



Activity Log

Export

Public Preview: Activity Log Reports

Test how activity logs could be leveraged during an investigation, before it becomes generally available.

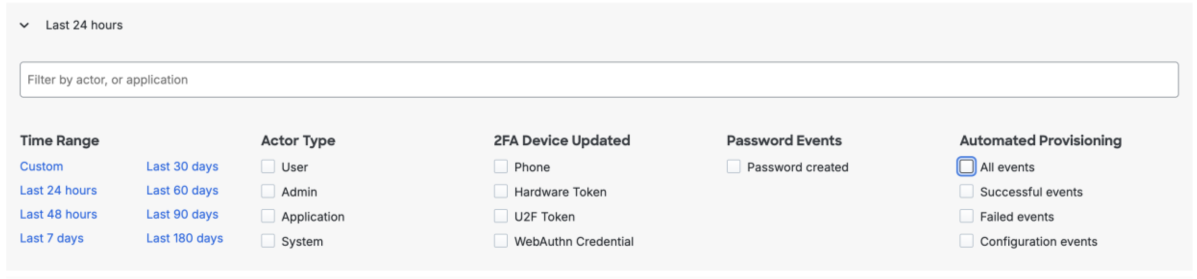
Dismiss ✕

› Last 24 hours

Showing 0-0 of 0 items

Showing 25 rows

The activity log is a new, single point of reporting for major events across Duo. It contains filters which allow you to narrow down the report to desired information. Click the > *Last 24 hours* row to view available filters. By default, no filter is selected.

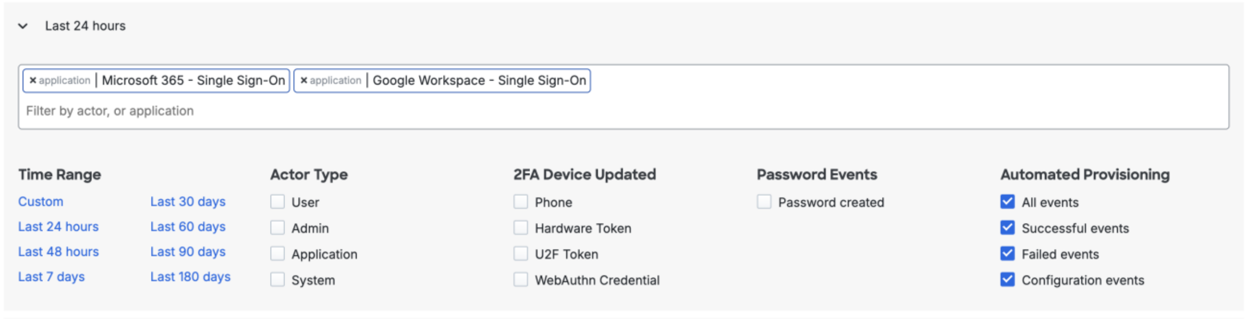


⌄ Last 24 hours

Filter by actor, or application

Time Range		Actor Type	2FA Device Updated	Password Events	Automated Provisioning
Custom	Last 30 days	□ User	□ Phone	□ Password created	□ All events
Last 24 hours	Last 60 days	□ Admin	□ Hardware Token		□ Successful events
Last 48 hours	Last 90 days	□ Application	□ U2F Token		□ Failed events
Last 7 days	Last 180 days	□ System	□ WebAuthn Credential		□ Configuration events

Click any of the Automated Provisioning filters to limit the report to just provisioning related activity. The results will include logged events from all of your applications set up with provisioning in one location. You can also use the top search bar to filter these results to specific applications. Please note – the filter by application search is case sensitive.



⌄ Last 24 hours

× application | Microsoft 365 - Single Sign-On × application | Google Workspace - Single Sign-On

Filter by actor, or application

Time Range		Actor Type	2FA Device Updated	Password Events	Automated Provisioning
Custom	Last 30 days	□ User	□ Phone	□ Password created	☑ All events
Last 24 hours	Last 60 days	□ Admin	□ Hardware Token		☑ Successful events
Last 48 hours	Last 90 days	□ Application	□ U2F Token		☑ Failed events
Last 7 days	Last 180 days	□ System	□ WebAuthn Credential		☑ Configuration events

FAQs

Question: How to set up passwordless authentication with Okta (or other IdP) as the external identity provider?
Answer: Follow the steps below:

- Import users to Duo via Okta inbound SCIM

    - Note: Email address used for authentication needs to be listed as a username alias
- Create the Okta application in Duo
    - You do not need to recreate the integrations per app in Duo in order to do passwordless authentication. However, creating individual integration in Duo gives you the benefit to leverage granular policy definition in Duo.
- [In Okta] Create the rule to route authentication from Okta to Duo
    - With Okta’s rule (“User is accessing”), you can define which applications to route from Okta for Duo.
- Setup or review policies in Duo
- Enroll a new user and complete a passwordless authentication

Feedback

If you have feedback or feature-related questions please send an Email with as much detail as possible to duo-idp-preview@cisco.com. This will allow the Duo team to track and we will get back to you as quickly as possible.

Thanks in advance for your participation!