How to Disable Duo Inline Enrollment for Unenrolled Users

This document describes how to disable the ability for inline enrollment for unenrolled users.

By default, the Duo Global Policy's 'New User Policy' is configured to prompt unenrolled users to enroll whenever possible. This means a user that successfully logs in with correct credentials that has never used or enrolled in Duo can automatically enroll their first 2FA device.

This feature of allowing unenrolled users to enroll on first access is standard practice for multifactor authentication including from other providers. It provides flexible enrollment for newly onboarded users or accounts. It comes with the risk that a compromised unenrolled account can complete MFA enrollment and gain unauthorized access.

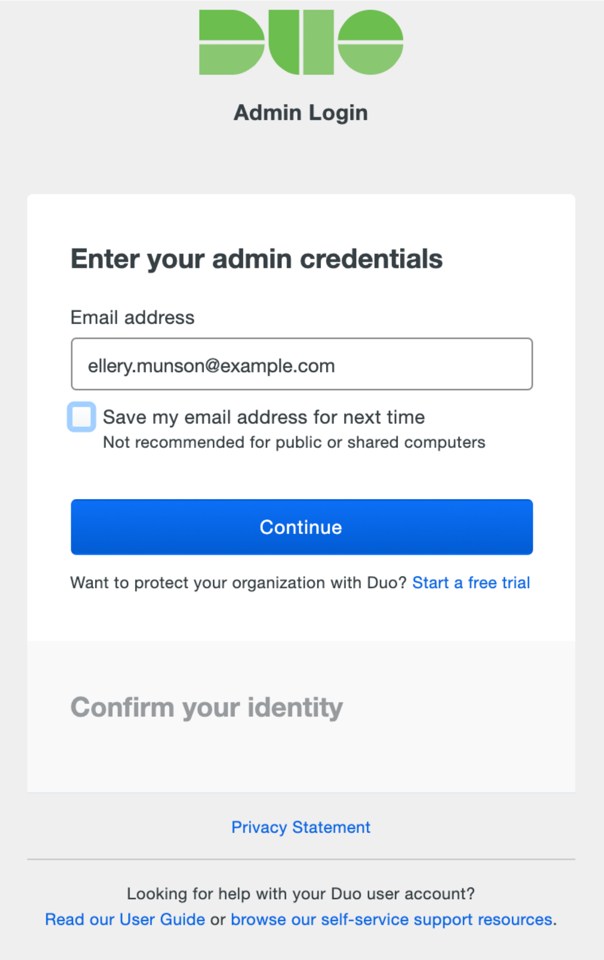
Before disabling inline enrollment for unenrolled users consider how you plan to enroll these users. Some alternate Duo enrollment methods are:

a. Populate phone number information for users in Active Directory, OpenLDAP, or Azure, and use directory sync to import those users into Duo with phones attached.
b. Send first-time enrollment emails directly to users with bulk self-enrollment.
c. Use CSV import to create new Duo users with attached phones or bulk import phone information for existing users without devices.
d. Utilize help desk or other similar resources to manually enroll users' first devices during onboarding.
e. Create an enrollment portal behind other security technologies. For example, only allow unenrolled users to enroll a device after they've connected to a VPN service with specific PKI or other security requirements.

When new Duo users have phones attached by directory sync or CSV import ensure that you've enabled either SMS passcodes or phone callback in your Authentication Methods, or send the users Duo Mobile activation links so they can authenticate with Duo Push.

Change the new user enrollment setting default for all applications without a superseding policy attached by editing the Global Policy:

1. Login to the Duo Admin Panel as an administrator with the Owner or Administrator role at https://admin.duosecurity.com.



Admin Login

Enter your admin credentials

Email address

ellery.munson@example.com

□ Save my email address for next time
Not recommended for public or shared computers

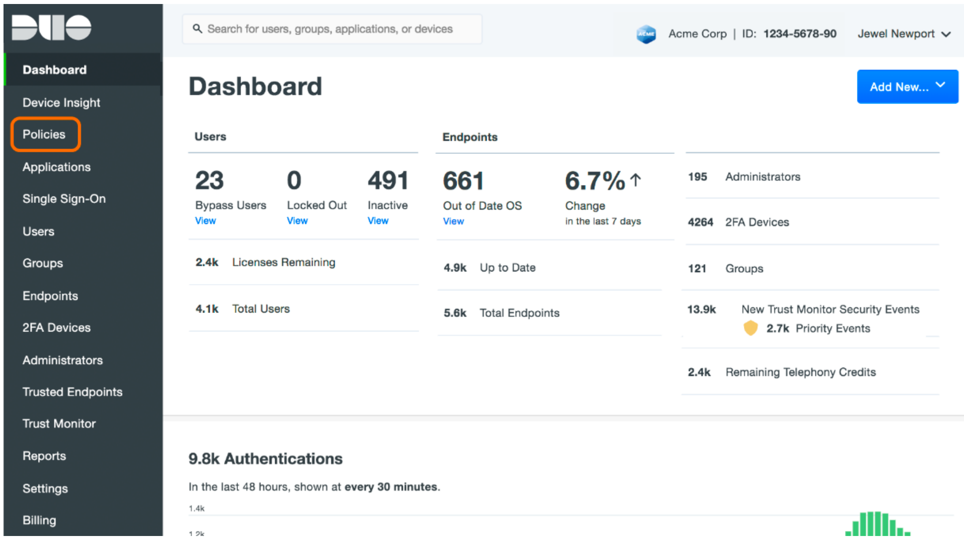
Want to protect your organization with Duo? Start a free trial

Confirm your identity

Privacy Statement

Looking for help with your Duo user account?
Read our User Guide or browse our self-service support resources.

2. Click **Policies** in the left-side navigation menu.



Dashboard

Users

23 Bypass Users View
0 Locked Out View
491 Inactive View

2.4k Licenses Remaining

4.1k Total Users

Endpoints

661 Out of Date OS View
6.7% ↑ Change in the last 7 days

4.9k Up to Date

5.6k Total Endpoints

195 Administrators

4264 2FA Devices

121 Groups

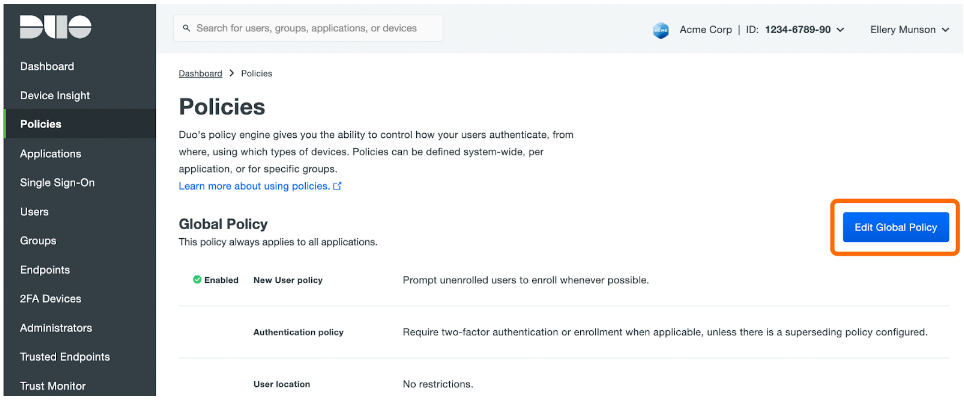
13.9k New Trust Monitor Security Events
2.7k Priority Events

2.4k Remaining Telephony Credits

9.8k Authentications

In the last 48 hours, shown at **every 30 minutes**.

3. On the “Policies” page in the Duo Admin Panel, click **Edit Global Policy** in the upper right of the Global Policy summary.



Search for users, groups, applications, or devices

Acme Corp | ID: 1234-6789-90

Ellery Munson

Dashboard
Device Insight
Policies
Applications
Single Sign-On
Users
Groups
Endpoints
2FA Devices
Administrators
Trusted Endpoints
Trust Monitor

Dashboard > Policies

Policies

Duo's policy engine gives you the ability to control how your users authenticate, from where, using which types of devices. Policies can be defined system-wide, per application, or for specific groups.

Learn more about using policies.

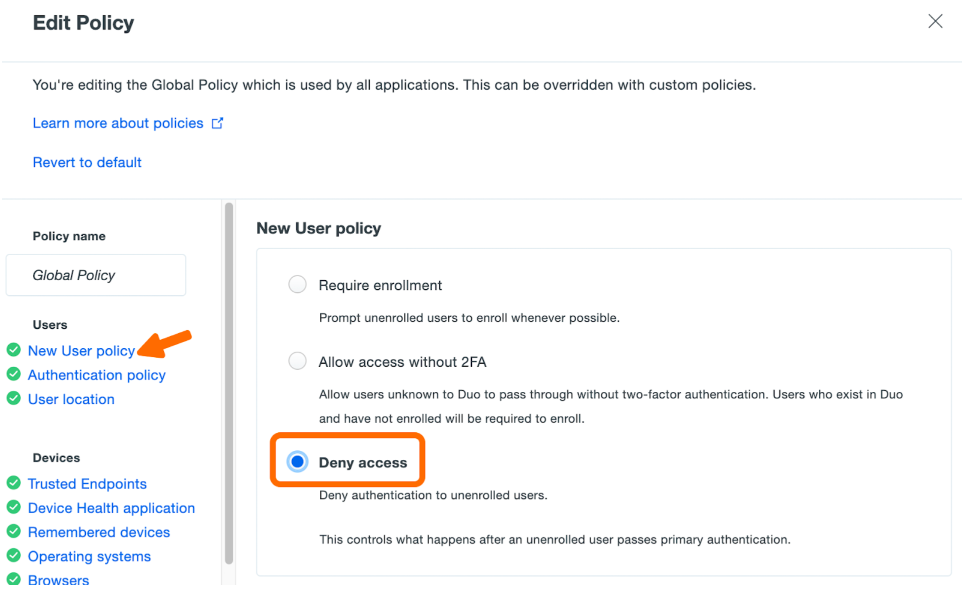
Global Policy

This policy always applies to all applications.

Edit Global Policy

✓ Enabled	New User policy	Prompt unenrolled users to enroll whenever possible.
	Authentication policy	Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.
	User location	No restrictions.

4. Locate the **New User policy** and change the policy setting to **Deny access**. Click **Save Policy** at the bottom of the policy editor when done.



Edit Policy

You're editing the Global Policy which is used by all applications. This can be overridden with custom policies.

Learn more about policies

Revert to default

Policy name

Global Policy

Users

✓ New User policy
✓ Authentication policy
✓ User location

Devices

✓ Trusted Endpoints
✓ Device Health application
✓ Remembered devices
✓ Operating systems
✓ Browsers

New User policy

○ Require enrollment

Prompt unenrolled users to enroll whenever possible.

○ Allow access without 2FA

Allow users unknown to Duo to pass through without two-factor authentication. Users who exist in Duo and have not enrolled will be required to enroll.

● Deny access

Deny authentication to unenrolled users.

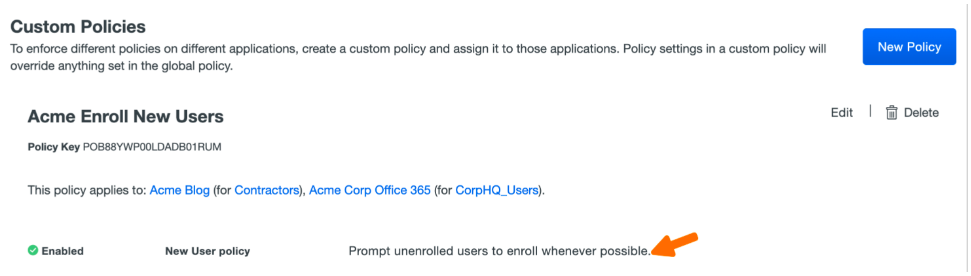
This controls what happens after an unenrolled user passes primary authentication.

If you applied custom group or application policies to individual applications with the New User policy setting configured, these custom policies continue to override the setting in the Global Policy. You will need to edit these custom policies as well to change the New User Policy from **Require enrollment** to **Deny Access**.

To update custom policy settings:

1. Scroll down to the **Custom Policies** section of the **Policies** page in the Duo Admin Panel.

2. Look for any of your custom policies that have the New User policy set to "Prompt unenrolled users to enroll whenever possible" or "Allow unenrolled users to pass through without two-factor authentication".



Custom Policies

To enforce different policies on different applications, create a custom policy and assign it to those applications. Policy settings in a custom policy will override anything set in the global policy.

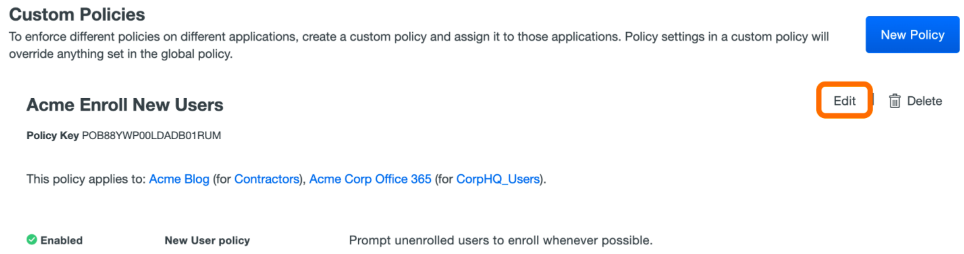
Acme Enroll New Users

Policy Key POB88YWP00LDADB01RUM

This policy applies to: Acme Blog (for Contractors), Acme Corp Office 365 (for CorpHQ_Users).

✓ **Enabled** | **New User policy** | Prompt unenrolled users to enroll whenever possible.

3. For each of these policies you want to change, click the **Edit** link shown to the right of the custom policy name.



Custom Policies

To enforce different policies on different applications, create a custom policy and assign it to those applications. Policy settings in a custom policy will override anything set in the global policy.

Acme Enroll New Users

Policy Key POB88YWP00LDADB01RUM

This policy applies to: Acme Blog (for Contractors), Acme Corp Office 365 (for CorpHQ_Users).

✓ **Enabled** | **New User policy** | Prompt unenrolled users to enroll whenever possible.

4. Change the **New User policy** in the policy editor for this custom policy to **Deny Access**, and then click **Save Policy**.

5. Repeat this for all the custom policies where you want to prevent enrollment of new users or access for unenrolled users.