CISCO SECURE | DUO

The bridge to possible

New Duo Feature Guide: Strengthening Your MFA

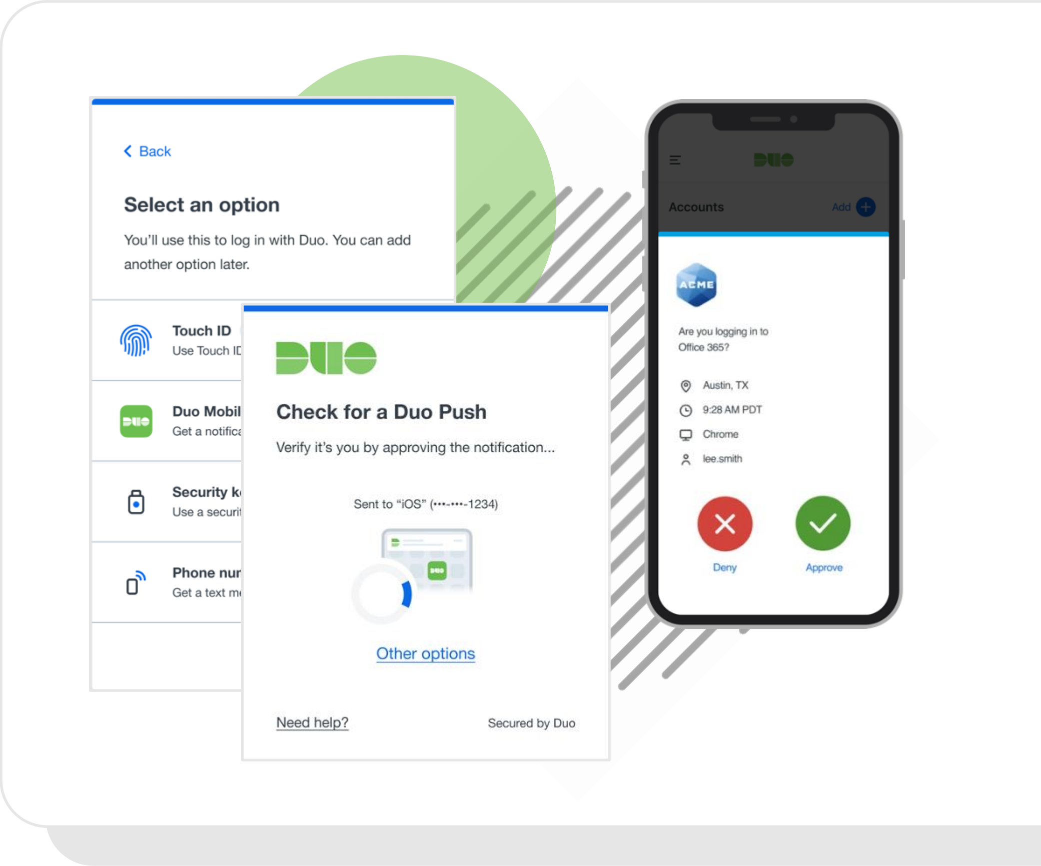
Introduction: Threat Landscape

Challenges Facing Organizations Today

Cybersecurity attacks seem to never fade from front page news. From data breaches to expensive ransomware payments, ranging from small to large businesses and across industries, attackers continue to find new ways to gain access to internal systems.

One type of attack that has gained attention recently is the exploitation of multi-factor authentication (MFA) meant to protect user login credentials. While MFA solutions have been available for some time now, over the past few years they have become a popular account safeguard.

However, simply adding MFA to a user login flow might not be enough to prevent the new and more sophisticated types of attacks that are making headlines. Instead, it is important organizations see MFA as one tool in their security toolbox that can be deployed along with other security measures to help protect their users and data.



< Back

Select an option

You'll use this to log in with Duo. You can add another option later.

Touch ID
Use Touch ID

Duo Mobil
Get a notifica

Security k
Use a securit

Phone nur
Get a text m

Check for a Duo Push

Verify it's you by approving the notification...

Sent to "iOS" (•••-•••-1234)

Other options

Need help?

Secured by Duo

Accounts

Add

Are you logging in to Office 365?

Austin, TX

9:28 AM PDT

Chrome

lee.smith

Deny

Approve

Overview: MFA Attacks

What exactly do MFA attacks look like and how are attackers able to gain access? Because MFA is such a common solution to protect logins, attackers must get creative to find ways around it. MITRE ATT&CK, a global knowledge base of cyber-attack tactics, provides communities with knowledge to protect themselves and improve their security posture.

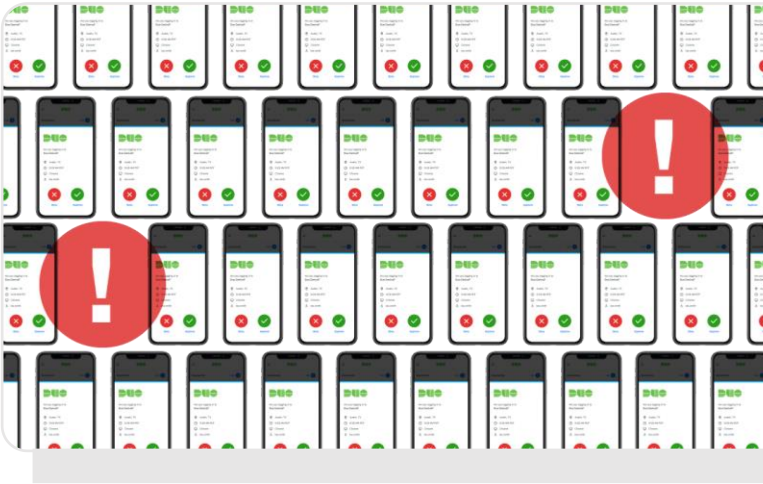
Below are some of the most common MFA attacks that MITRE ATT&CK has been following:

MFA Interception (MITRE ID T1111): An attacker can steal a one-time code that is sent through an "out-of-band" communication (meaning outside of the primary communication channel), such as a SMS text message or email. If the device or service is compromised, an attacker can steal that code and proceed to login with the user's credentials and MFA code.

Fraudulent Enrollment (MITRE ID T1098.005): If a user's credentials (username & password) are stolen, an adversary can register a new device to that controlled account. That new, fraudulent device can then enroll in the MFA system and gain persistent access to an internal system.

Adversary-in-the-Middle, AiTM (MITRE ID T1539): After a user has successfully logged in, that user is granted a session cookie that enables them to continue to access the resource for a set amount of time. One attack technique used to gain access is to steal that session's cookie to gain access as an already authenticated user, bypassing the need to MFA at all.

Push Phishing (MITRE ID T1621): When an adversary has a valid username and password, but an organization has MFA set up, each time that adversary attempts to login, the owner of those credentials gets an MFA request ("is this you trying to sign-in?"). Most users will ignore or deny an MFA request if they are not trying to sign-in. However, in push phishing (also known as push bombing or push harassment), the attacker sends the MFA requests repeatedly until the authentic user caves and accepts to stop the harassment. This is typically due to "MFA fatigue," or can result from social engineering where someone posing as an IT employee reaches out and instructs a user to accept the request.

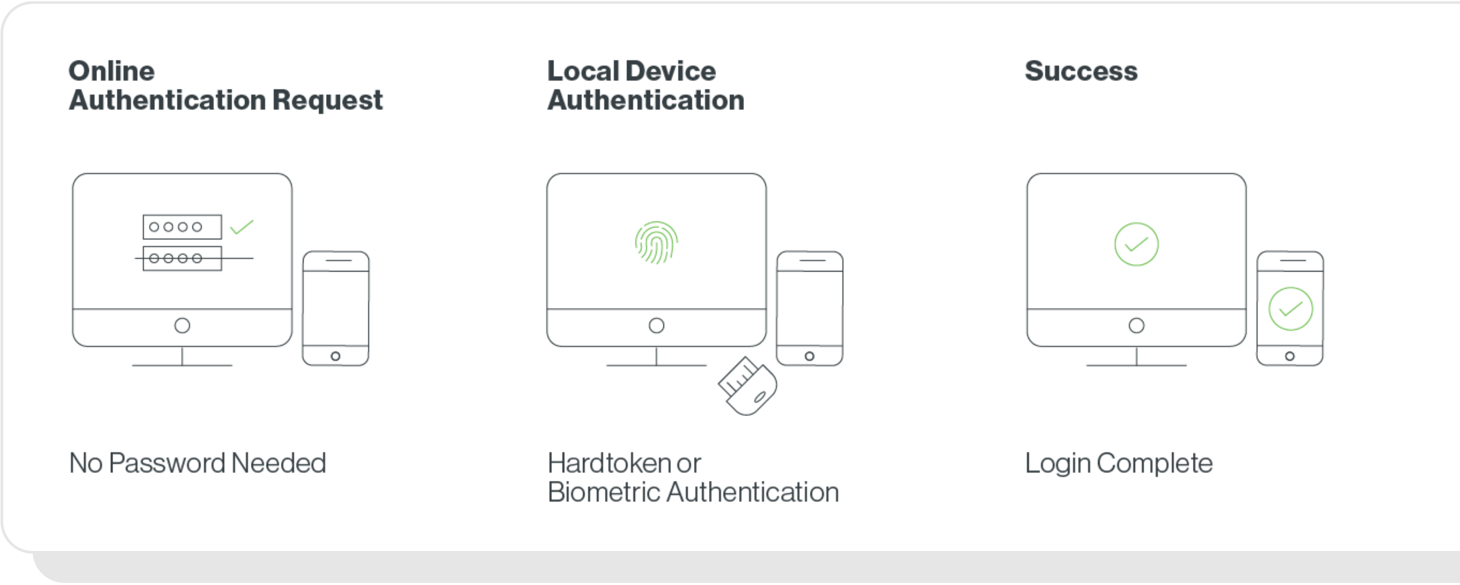


What Organizations Can Do

Secure Authentication

As adversaries get more sophisticated and the threat landscape continues to evolve, it can be overwhelming for organizations to continuously adapt to prevent these attacks. If an organization has not already moved authentication from RADIUS or LDAP to SAML or OIDC, that would be a good first step. The most effective methods of securing your environment increasingly rely on the telemetry and authentication methods that modern authentication protocols support.

Next, organizations need to consider what type of authentication works best for their environment. One solution for organizations is to adopt FIDO2 compliant authentication that is resistant to these new types of MFA attacks. A common way to achieve this is through passwordless authentication or security keys that use WebAuthn, which prevents typical MFA attacks because FIDO2 credentials can't be phished or used remotely by an attacker.



While FIDO2 offers the gold standard for authentication, not all organizations are able to implement this today. Shipping security keys to all users can be expensive and organizations might not have access to biometric authentication on users' devices.

Therefore, Duo has taken steps to put organizations in the best possible position to prevent these common attacks to meet them where they are, today.

How Duo Can Help

Getting Started

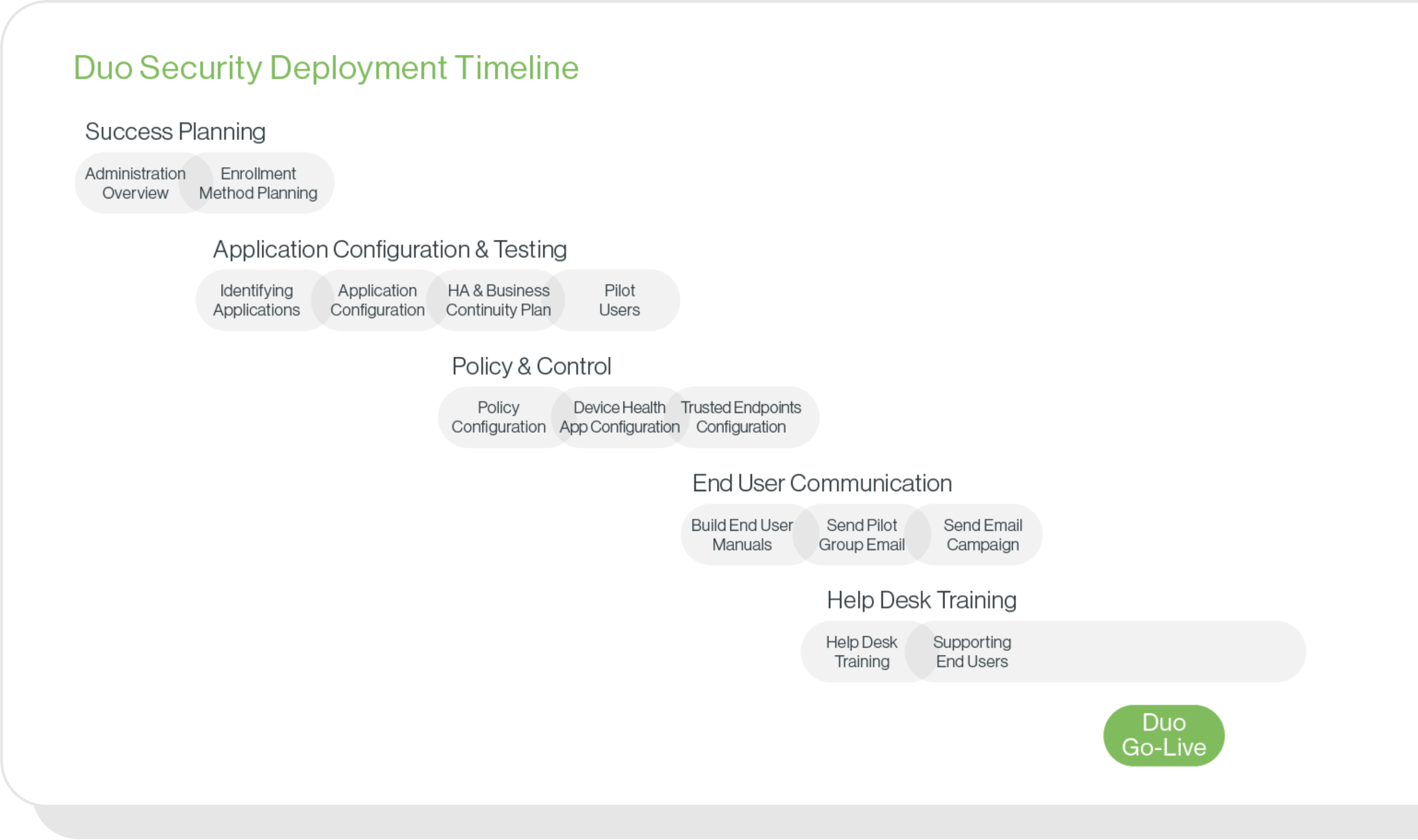
Duo announced the availability of the Universal Prompt in 2021 to simplify authentication and improve security for users. Since its release, customers have made the transition to the new prompt for a variety of reasons based on their organization's security goals. This might include gaining access to new authentication methods, like Verified Duo Push or Passwordless, or to respond to risk-signals at login through Risk-Based Authentication.

Ultimately, the Universal Prompt is the first step organizations must take to unlock many of Duo's security focused new features. In the Guide to Duo Universal Prompt, your organization can find all the tools necessary to begin the journey towards adoption.

New Duo Capabilities

The Duo Lift Off Guide is a helpful tool that organizations can use to successfully launch and manage Duo in their environment. This guide breaks down Duo best practices to walk administrators through what features they should consider as they make their way through the deployment process.

In addition to these best practices, Duo has also introduced new features in response to the new attacks that have emerged in recent years. This can help strengthen an organization's defenses and stop bad actors using these common techniques that lead to high-profile breaches.



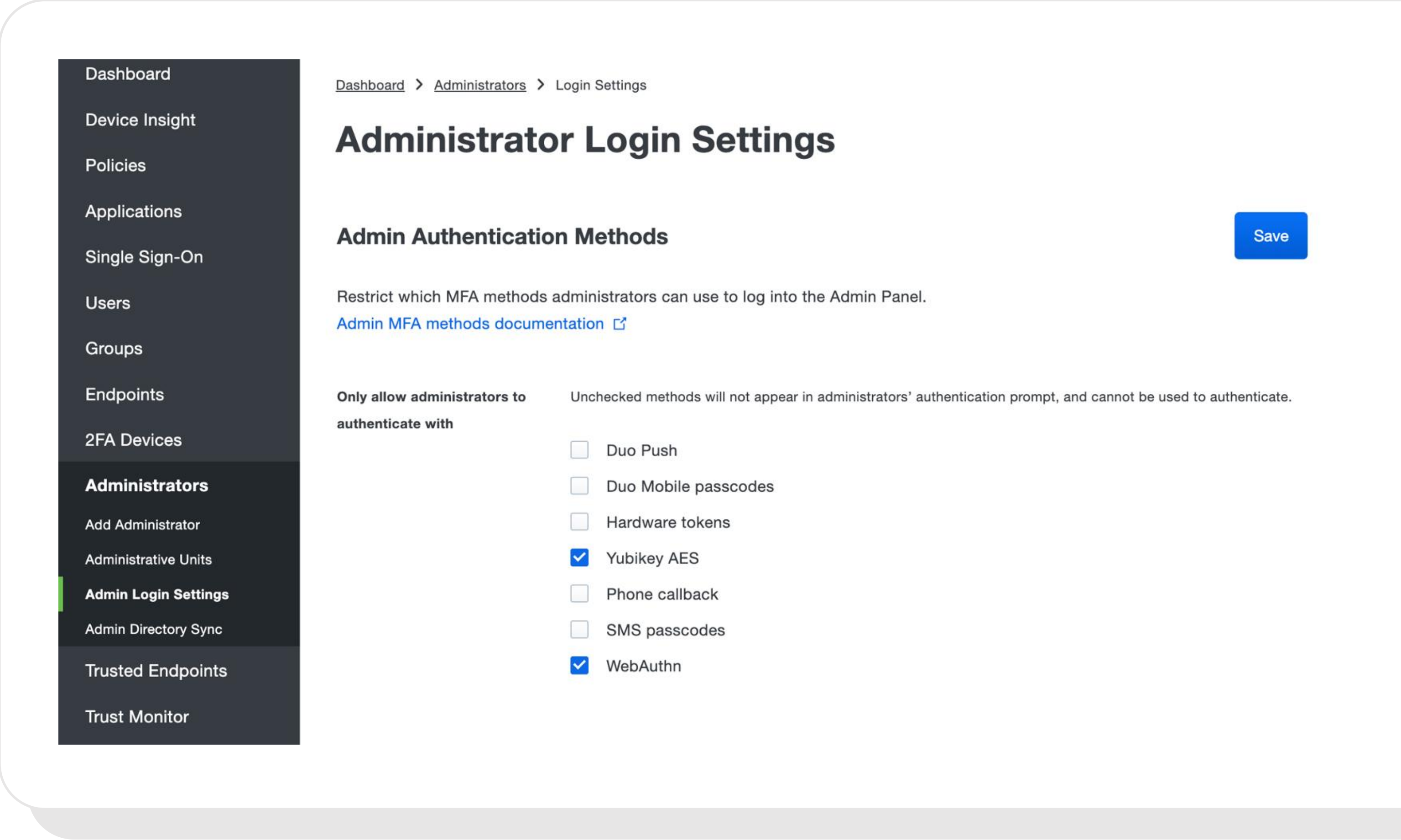
Success Planning

Protect Duo Administrators

One important aspect of setting up Duo is developing the privileges for Duo administrators. This role is important because the user has access to all user login, which makes it a high-value and high-stakes account to protect.

In order to better protect administrators, they can now add a WebAuthn authenticator as a second factor device and use it at the time of authentication. Administrators can easily turn on select WebAuthn authentication methods under “Administrator Login Settings.” Once this feature is enabled, the option to use a WebAuthn authenticator will appear on the login screen, even if you have not registered an authenticator.

To learn more, check out the Duo Administrator Documentation.



Administrator Login Settings

Admin Authentication Methods

Restrict which MFA methods administrators can use to log into the Admin Panel.
Admin MFA methods documentation

Only allow administrators to authenticate with

Unchecked methods will not appear in administrators’ authentication prompt, and cannot be used to authenticate.

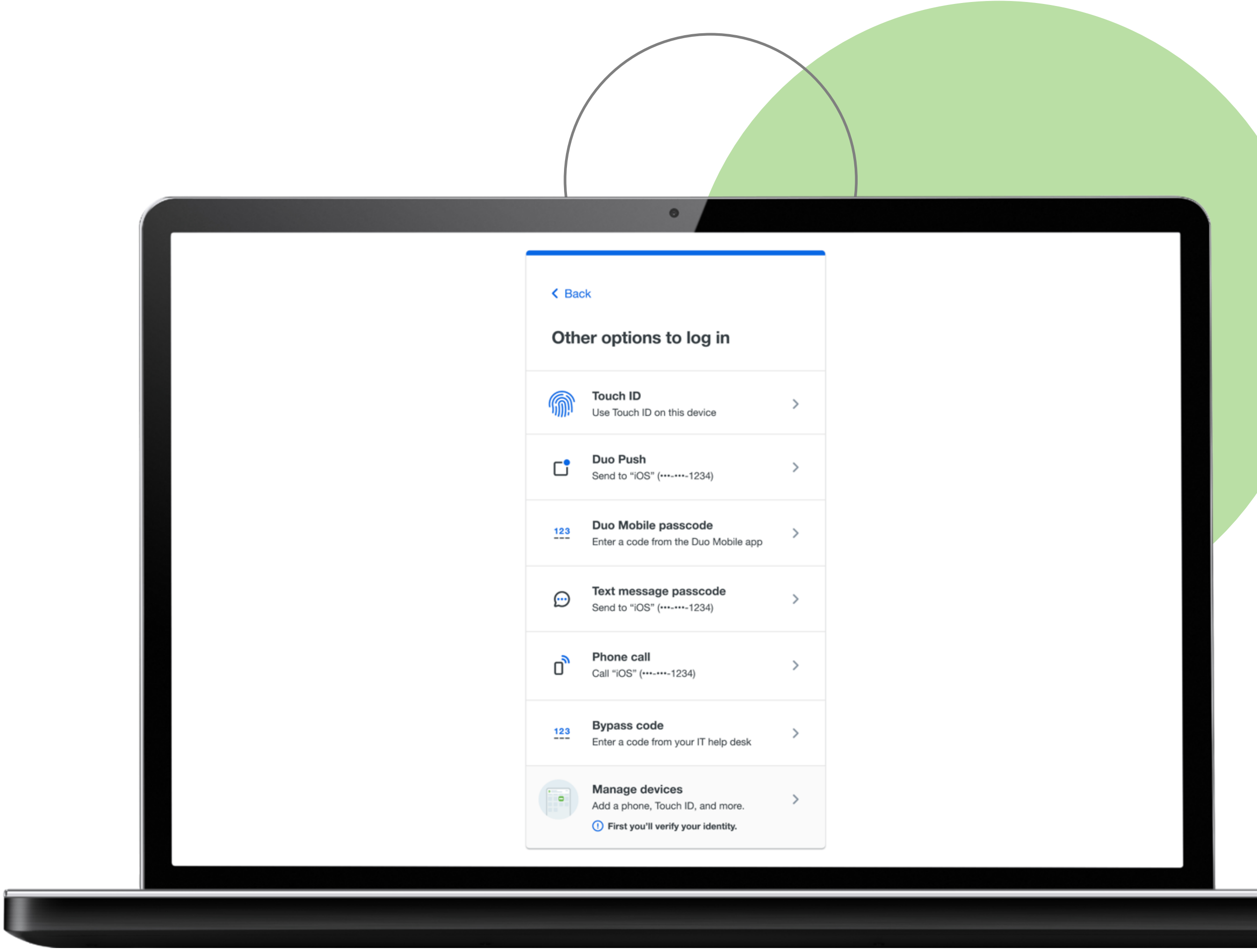
□ Duo Push
□ Duo Mobile passcodes
□ Hardware tokens
☑ Yubikey AES
□ Phone callback
□ SMS passcodes
☑ WebAuthn

Enrollment Protections

In order to address the challenges around fraudulent enrollment, Duo has added a variety of features to protect the enrollment process.

Self-Service Portal

The Duo Self-Service Portal is a more sensitive application relative to others since it allows users to enroll devices. When attackers target applications, that means the security measures protecting that application should step up and be secured by the strongest authentication factors. Now administrators have the power to set up the authentication method for the self-service portal separately from regular authentication methods, as well as add Verified Duo Push as a more secure factor.



< Back

Other options to log in

Touch ID
Use Touch ID on this device

Duo Push
Send to "iOS" (•••-•••-1234)

Duo Mobile passcode
Enter a code from the Duo Mobile app

Text message passcode
Send to "iOS" (•••-•••-1234)

Phone call
Call "iOS" (•••-•••-1234)

Bypass code
Enter a code from your IT help desk

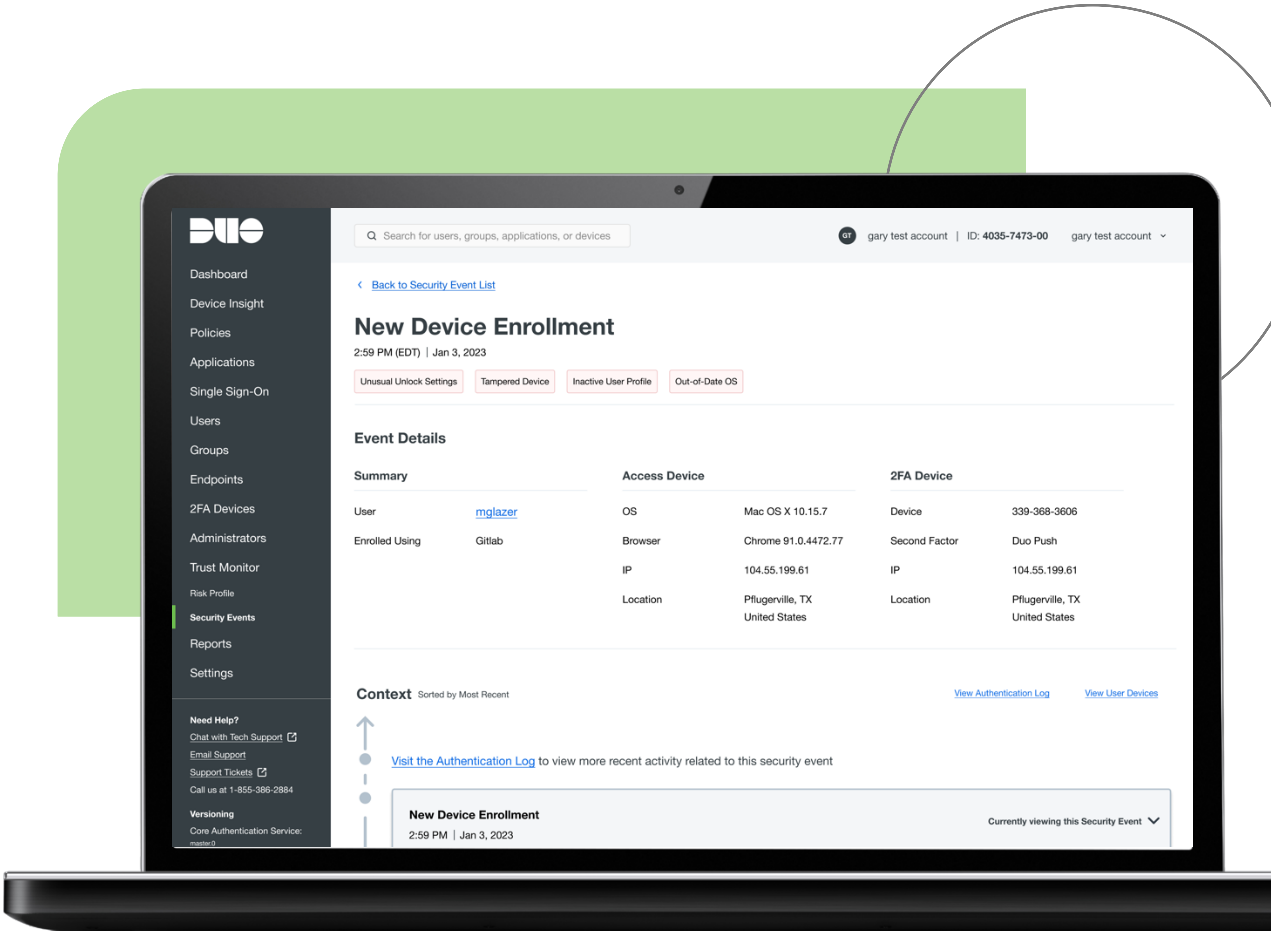
Manage devices
Add a phone, Touch ID, and more.
First you'll verify your identity.

API for User Activity Logs

Duo administrators can request user device enrollment threats through the API endpoint and ingest these events into a Security Information and Event Management (SIEM) tool. This allows increased visibility into enrollment actions, fraud and threats, such as registering a new phone, hardware token or creation of a WebAuthn credential. Learn more about Duo's API functionality in the documentation.

Enrollment Threat Detection

By doing the legwork of parsing through enrollment events and surfacing only those that appear fraudulent, enrollment threat detection makes it possible for administrators to review enrollment of new devices in a manageable workload. Duo's Trust Monitor evaluates data from real-world attacks to alert administrators to these potential risks.



New Device Enrollment

2:59 PM (EDT) | Jan 3, 2023

Unusual Unlock Settings | Tampered Device | Inactive User Profile | Out-of-Date OS

Event Details

Summary		Access Device		2FA Device	
User	mglazer	OS	Mac OS X 10.15.7	Device	339-368-3606
Enrolled Using	Gitlab	Browser	Chrome 91.0.4472.77	Second Factor	Duo Push
		IP	104.55.199.61	IP	104.55.199.61
		Location	Pflugerville, TX United States	Location	Pflugerville, TX United States

Context Sorted by Most Recent

Visit the Authentication Log to view more recent activity related to this security event

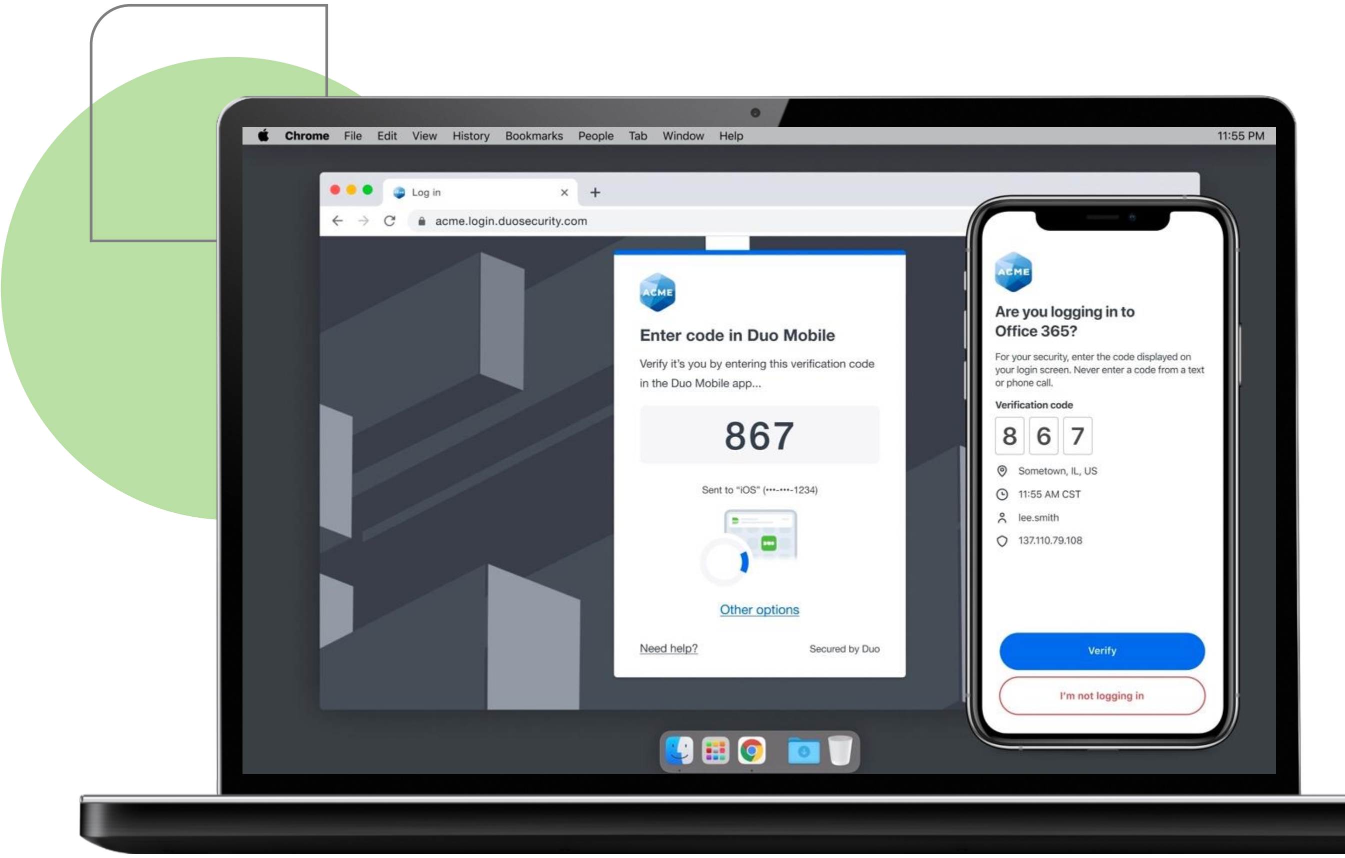
New Device Enrollment
2:59 PM | Jan 3, 2023
Currently viewing this Security Event

Application Configuration & Testing

Protect Applications with Verified Duo Push

Similarly with the Duo Administrator login, some applications and data are particularly sensitive and important to maintaining an organization's security. Therefore, those applications should require additional steps in order to gain access. One way to protect these applications is by using Duo's application specific policy to set up more secure authentication methods.

A new method, Verified Duo Push, requires users to enter a unique code from the login device into the Duo mobile app, rather than simply select the green checkmark to login. This prevents bad actors from gaining access and also prevents trusted users from accidentally accepting a fraudulent MFA request due to MFA fatigue.



Enter code in Duo Mobile

Verify it's you by entering this verification code in the Duo Mobile app...

867

Sent to "iOS" (•••-•••-1234)

Other options

Need help?

Secured by Duo

Are you logging in to Office 365?

For your security, enter the code displayed on your login screen. Never enter a code from a text or phone call.

Verification code

8 6 7

Sometown, IL, US

11:55 AM CST

lee.smith

137.110.79.108

Policy Control

Policy & Configuration:

Duo policies allow Duo administrators to set guidelines and restrictions for user access based on each organizations risk appetite. There are some policies that are not only more secure, but also do not unnecessary friction to the end user experience. In order to help our customers utilize Duo policies, the following new defaults have been established:

- **Authentication Methods:** Organizations can still select the authentication methods that work best for their users, but Duo encourages using the most secure factors. This new policy will turn off phone call back and SMS passcodes as an authentication method and require the more secure, Verified Duo Push.

- **Update Duo Mobile:** In order to ensure Duo Mobile is up to date and has the latest security patches, this default requires users to update the application in order to authenticate and gain access to their account.

- **Flash & Java:** Duo will automatically block all versions of Flash Player, as it is a source of known vulnerabilities and has not been supported since 2020. Java also has several zero-day vulnerabilities and exploits, so Duo can warn users when their Java plugin is out of date.

- **Screen Lock:** Users that do not have a screen lock on the device will not be allowed to authenticate until screen lock is enabled.

- **Tampered Devices:** Devices that have been tampered, such as jailbroken devices, will no longer be automatically allowed to authenticate.

Try Duo for free using our 30-day trial https://signup.duo.com/

At Duo, we combine security expertise with a user-centered philosophy to provide multi-factor authentication, endpoint remediation and secure single sign-on tools for the modern era. It's so simple and effective, you get the freedom to focus on your mission and leave protecting it to us. Duo is built on the promise of doing the right thing for our customers and each other. This promise is as central to our business as the product itself. Our four guiding principles are the heart of the sensibility: Easy, Effective, Trustworthy, Enduring.

Duo Security makes security painless, so you can focus on what's important. Duo's scalable, cloud-based trusted access platform addresses security threats before they become a problem, by verifying the identity of your users and the health of their devices before they connect to the applications you want them to access. Experience advanced multi-factor authentication, endpoint visibility, custom user policies and more with your free 30-day trial. You'll see how easy it is to secure your workforce, from anywhere on any device with Duo MFA..