Duo Authentication Landing Page

Duo Authentication Landing Page

Touchstone and Duo updated March 22
Touchstone and Duo authentication has been updated with some visual changes and an improved two-factor authentication experience as Information Systems and Technology (IS&T) implemented updates to the Institute's single sign-on web authentication service on Friday, March 22.

- IS&T News: Touchstone and Duo updates coming March 22
- Duo Universal Prompt Guide

For more information on securing your data, see Information Protection @ MIT.

On this page:

Overview
How to Obtain
Registering Devices
How to Use
Who is required to use Duo?
What devices can I use with Duo?
What services use Duo authentication?
Authenticating
Traveling with Duo
Lost/Stolen Device or Changed Phone Number
Troubleshooting
FAQ's
Get Help

Overview

Duo is a two-factor authentication system that requires both a credential (certificate, username/password) *and* a registered thing you have (smart phone, tablet, yubikey) to "Approve" system access to applications that require Touchstone Authentication.

By default, every time a website prompts you to login via Touchstone, you will get a Duo prompt to approve the login. This is usually once per day, or whenever you restart your web browser. If you prefer to be prompted less frequently, the Duo login page has a "Remember this device" checkbox. If this option is selected, you will not be prompted again for 30 days. For more information, see: Duo Remember My Device for 30 Days FAQ.

How to Obtain

Registering Devices

In order to leverage Duo's two-factor authentication system, you must first register your device(s) with MIT Duo at https://duo.mit.edu.

IS&T recommends registering at least *two (2)* devices. In case your device is lost or stolen, the second device will allow you to login to Duo, deactivate the lost device, and configure the replacement.

- How to Register a Smart Phone for Duo two-factor authentication
- How to Register a non-smart Phone for Duo two-factor authentication
- How do I register my YubiKey for use with Duo 2FA?
- How do I register an iPad, Android tablet, or other device for Duo?
- How do I register a D100 Token for Duo two-factor authentication?
- Using an Apple Watch with Duo

How to Use

Who is required to use Duo?

Duo is required for the entire MIT community including students, faculty, staff and affiliates.

What devices can I use with Duo?

There are several ways you can authenticate via Duo. No smartphone or data plan is required. IS&T recommends setting up at least two in case your registered device is lost or stolen.

- A push notification sent to your smart phone or tablet with the free, IS&T Recommended Duo Security Mobile app (available for iOS and Android).
- An SMS message sent to your cell phone (not supported with some international numbers)
- A phone call made to your cell phone
- A phone call made to a landline
- By entering a one-time code generated by a YubiKey.
  Good for traveling or when cell coverage is poor.

What services use Duo authentication?

Services that use Touchstone. These include:

- VPN
- Atlas
- CertAid
- The Duo management pages
- See more...

Authenticating

Using Two Factor Authentication

- How do I login to MIT services that leverage Duo two-factor authentication?
- How do I authenticate with a YubiKey?

Traveling with Duo

Before you travel, it's important to think about how you'll use Duo on the road. If your smartphone won't work where you're going, you may want to request a yubikey or install the IS&T Recommended Duo Security Mobile app (available for iOS and Android) so you can use push authentication with the app.

- How do I prepare for traveling with Duo?

Lost/Stolen Device or Changed Phone Number

What should I do if my Duo registered device is lost, stolen or I change my phone number?

You should immediately deactivate the device. If you have another registered device, use that to login to https://duo.mit.edu, deactivate the lost/stolen/changed device, and register the replacement.

- What do I do if my duo enabled device is lost, stolen or I changed my phone number?

If your only Duo-registered device is lost/stolen or you have changed phone numbers, you will need to contact IS&T to verify your identity and get your account reset. See: Get Help.

Troubleshooting

- Touchstone Duo Error - Remember device for 30 days - cookie error
- Why can't I select Remember for 30 Days when using DUO?
- My account has been locked out due to excessive authentication failures.
- I get a blank grey box instead of my push options when trying to authenticate with duo. What do I do?
- How do I resolve Duo Prompt display issues related to iOS or macOS content restrictions?

- Common Duo Issues on iOS

FAQ's

- Duo Two-factor Authentication FAQ
- Why is Duo required?
- How do I request a Yubikey?
- What do I do if my duo enabled device is lost, stolen or I changed my phone number?
- Duo - What should I do if I get a new phone? How to switch registered devices.
- How can staff that share the office VoIP phone and don't have a Smartphone enable Duo?
- I am having trouble with my International phone number. What do I do?
- Configuring MacPorts Kerberos for Duo Authentication
- Do I need a smartphone with a data plan?

Get Help

For additional assistance with Duo, troubleshooting, lost/stolen devices, or any other Duo issues, contact the Service Desk.

Account resets for lost/stolen devices or changed phone numbers require identity verification. You will need to bring or provide proof via a valid photo ID (MIT ID, government issued ID card, driver's license, passport, etc).

- IS&T Service Desk

Additional escalation information for Help Staff can be found here: [hd:Duo Authentication Recon].