Duo Two-factor Authentication FAQ

Overview

IS&T has been working for a few years to strengthen its IT environment through the use of two-factor authentication. Duo Security’s system, called Duo, was selected as part of a U.S.-government-sponsored initiative with MIT and Internet2 to explore the use of two-factor technology in higher education environments. As part of these efforts, Duo has been integrated into several IT services, including Touchstone, Kerberos, and VPN. IS&T can now make these services more broadly available to the community.

With increased vulnerabilities within the Internet’s underlying encryption systems, such as the Secure Socket Layer (SSL), depending solely on passwords alone has demonstrated high risk in compromising systems, services and accounts.

For more information, see the Duo Authentication Landing Page

What services require Duo for login?

A number of MIT services including Touchstone, Kerberos, and VPN are enabled for Duo two-factor authentication. When you enable two-factor authentication with Duo for Touchstone, you will need to have your Duo activated device available in order to login to any service or web application that requires Touchstone for authentication. Touchstone and two-factor authentication enabled services include:

- Stellar
- VPN
- Atlas
- iMIT
- Request Tracker
- Webmoira
- Dropbox
- Athena Dialups
- CCURE
- The Duo management pages

Supported Browsers include Chrome, Firefox, Safari and Internet Explorer.

Services such as MIT Email, Knowledge Base, and SAP Services do not currently use Touchstone and do not require Duo authentication. The Athena Dialup service does not use Touchstone, but does require two-factor authentication through Duo.

Do I need a smartphone with a data plan?

It is not necessary to have a smartphone to use Duo. You can use a tablet, landline phone or YubiKey for your second factor instead. A data plan is not required for your device. If you have the Duo app on your phone, you can click key icon next to account to get a one-time passcode to log in, which doesn’t require any data usage.

Setting up Duo:

How do I register a Smart phone for Duo two-factor authentication?

How to Register a Smart Phone for Duo two-factor authentication
How do I prepare for traveling?

- Bring a registered smartphone with the IS&T Recommended Duo Security Mobile app (available for iOS, Android, BlackBerry and Windows Phone) - No connectivity or data plan is required if you use a one time passcode.
- Or bring a mobile phone that you have signed up as a "landline" for Duo Two-Factor authentication;
- Or bring a YubiKey with you.
- You can come E17-106 to pick up a YubiKey or submit a request for one

Due to the evolving Covid-19 situation, the Atlas Service Center ceased in-person services as of Tuesday, March 17 at 6:00pm.

IS&T Service Desk walk-in IT help and repair services will not be offered in the Atlas Service Center until further notice. If you have questions or need assistance, contact the IS&T Service Desk at any time 24/7 at 617-253-1101 or servicedesk@mit.edu.

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
- Email: servicedesk@mit.edu
- Phone: (617) 253-1101
- Walk-ins: Bldg E17-106, 40 Ames Street
  M-F, 9AM - 5PM