# I forgot my password, can I have it reset?

## I forgot my password, can I have it reset?

1 I forgot my password, can I have it reset?
1.1 Self-Service Password Reset
1.1.1 <u>Reset via a Valid Certificate</u>
1.2 <u>Reset via Push-Enabled Duo 2FA Device</u>
1.2 Request Password Reset from Service Desk
1.3 Lincoln Lab Employees
1.4 Are password managers a good idea?
2 Related links
3 Troubleshooting



If you are using a computer joined to the WIN.MIT.EDU domain, and use your Kerberos credentials to log into your computer, you may find this page helpful: Remote Domain Computers and Password Changes.

### Self-Service Password Reset

Ensure the password you need reset is your **Kerberos** password. If you're attempting to access Google Workspace, or departmental email (e.g. sloan.mit.edu, csail.mit.edu, math.mit.edu, plant.mit.edu), then you may need to reset a *different password*, as those services do not use Kerberos or Touchstone for authentication.

To reset your password yourself, there are two options.

#### Reset via a Valid Certificate

If you have a valid MIT personal certificate installed you can reset your password online by visiting Change Your Kerberos Password (see second option on the page.)

😏 Be sure you have cookies enabled or you'll get unknown user error messages.

#### Reset via Push-Enabled Duo 2FA Device

If you have a push-enabled Duo device, you can reset your password online by visiting Change Your Kerberos Password using Duo Push

For requirements and recommendations when setting a new password, please see the Strong Passwords article.

## **Request Password Reset from Service Desk**

If you do not have a push-enabled Duo device, nor a valid MIT certificate, then you will need to contact the Service Desk.

Email accounts@mit.edu with the following information:

- 1. Statement that this is a password reset for your MIT/Kerberos account
- 2. Your MIT.EDU email address or Kerberos username
- 3. A photo of yourself, holding a valid photo ID this should be your MITID card (digital or physical)
- 4. An alternate email address where you can be reached

Please be sure the name and photo on the MIT ID are clear and please do not cover any part of your face with the ID.

It is very important that we can read the ID from this photo, so please make sure the ID is in focus and **can be read** from the image before sending it to us as an attachment.

Lo not send us pictures of just your ID, you must be present in the image and holding the ID for it to be a valid form of identification verification.

🕄 Tip: Getting closer to the camera and having someone assist you with taking this photo can make this method of password reset easier.

If you do not have an MIT ID, you can email servicedesk@mit.edu and request ID verification through a Zoom meeting. You can also visit the Atlas Service Center on the bottom floor of E17 for in-person assistance.

For requirements and recommendations when setting a new password, please see the Strong Passwords article.

#### Lincoln Lab Employees

Lincoln Lab employees should utilize the self-service password reset tools (MIT certificate or Duo Push). If those are unavailable, the recommended and most secure method is to request a Zoom meeting with the IS&T Service Desk for ID verification and a password reset: servicedesk@mit.edu or 617-253-1101.

If LL employees cannot use Zoom, they can request a password reset from the Service Desk by sending a photograph of themselves holding their MIT ID card to servicedesk@mit.edu. If you don't have one, this article will walk you through obtaining a digital or physical card.

#### Are password managers a good idea?

Yes, as long as you have a strong password protecting all your passwords in your password manager. Most password managers use encryption. If you use a browser-based password manager such as LastPass, you don't have to remember each individual password for your online accounts, but you do need to remember your master password. Be sure to change that master password regularly. Other options for password managers are 1Password, Dashlane, KeePass and RoboForm, among others. The basic versions of these are free. It is very important to enable Two-factor Authentication in your password manager so that a breach of the master password itself cannot provide an adversary access to your password list.

## **Related links**

- Certificates Landing Page
- Remote Domain Computers and Password Changes
- Strong Passwords

## Troubleshooting

• What to do if a browser or App is prompting for a password after updating my certificate?