Passwords and Identities Landing Page

Passwords and Identities Landing Page

On this page:

Overview

Passwords and identities and the keys to your accounts and systems. Make it a priority to take care with them; they're protecting your data and access. Use strong passwords, and change them at least annually. If there's any hint one of your passwords might be compromised, change it immediately anywhere it may be in use. Also change any vendor supplied passwords as those are likely known by a large number of people, and not all good actors. It's also a good idea to remove any default accounts as those are similarly easy to compromise. Finally, protect your passwords by making sure to only store and transmit encrypted passwords.

- For more information on how to classify and secure your data, see Information Protection @ MIT.

How to

Change Your Password Immediately if You Suspect a Compromise

- How to change your MIT Kerberos password:
  - IS&T's Change Your Kerberos Password
  - Change Your Kerberos Password Online
  - How do I change my Kerberos password in Windows?
  - How do I change my Kerberos password in Mac OS X?
  - How can I change my MIT Kerberos account password on Athena?
  - How can I change my root or extra password?
  - What page allows me to change my Kerberos password using my current password or MIT personal certificate?
  - IS&T Policies: MIT Kerberos Accounts Password Policy
- Change Your Data Warehouse Password
- How do I reset my password for a TSM backup node name account?
- [Reset Touchstone Collaboration Account password]
- CertAid manages the entire certificate and identity preference setup procedure, giving users a more reliable installation experience.
  - Obtain Certaid
  - CertAid Landing Page

Create a Strong Password

- Strong Passwords

Never reuse passwords for multiple systems or services.

- If one password is compromised, attackers often attempt to use it across your other accounts knowing many people reuse passwords. You can protect yourself from this risk by using unique passwords for each system or service that requires one.
- Do not use your Kerberos password for non-Kerberos enabled systems.

A Password Manager

IS&T licenses LastPass for MIT community use.

- LastPass Landing Page
- How do I sign up for MIT's LastPass Service?
- What do I need to know about using LastPass at MIT?
- LastPass Frequently Asked Questions - FAQ

Change Default Vendor Passwords/Accounts

Many devices come with default passwords and/or accounts set up on them. Unfortunately, hackers are very aware of this. If you connect these devices to the internet, they can (and likely will) be compromised quickly. As part of the initial setup process, it is recommend to replace any default accounts and passwords.

Vendor setup documentation usually has instructions on how to replace default accounts and passwords. Some things that may come with default accounts and passwords or no passwords at all are:

- Raspberry Pi
- Routers
- Databases
- Virtual Machines
- IS&T Field Support Default Machines
- Webcams

Store and Transmit only Encrypted Passwords

- If you need to share a password, LastPass can help share passwords securely.

Have Questions or Still Need Help?

- Contact the IS&T Service Desk