Authentication Tools at MIT

This article explains the various options community developers have for authenticating members of the MIT community to their application or web service.

OpenID Connect

Use case(s): Web applications that authenticate members of MIT community; desktop or mobile applications
Pros: dynamic self-registration, anyone can self-sign-up, does not require special software on web server; can also be used for desktop or mobile applications
Cons: can only authenticate MIT community members
How to get started: visit this page
Product owner: some combination of Integration and Identity & Access Management

Recommended!

Touchstone

Touchstone is our branding of Shibboleth, which is used in many other educational institutions for Single Sign On.

Use case(s): Web applications that authenticate members of the MIT community AND non-MIT collaborators who create a "Collaboration Account"
Pros: lets web application developers restrict access to both MIT and non-MIT users
Cons: needs server-side help to get set up, requires special software, requires configuration changes on web server; only available for web applications
How to get started: visit this page
Product owner: Bob Basch

LDAP authentication

Use case(s): software that only knows how to use LDAP as its authentication mechanism
Pros: Often the lowest-common-denominator for commercial products that support central authentication
Cons: Can be overly complex, group and user synchronizations are limited to 100 records unless special arrangements are made.

⚠️ If someone really needs this, point them to Escalations team, or Implementation team.

Certificate authentication

In general, Touchstone or Open ID Connect should be preferred. Certificate authentication has a number of quirks based on browser behavior, and may behave poorly in an environment where certificates are optional.

If you must use it, you will need mitCAclient.pem from the apache-ssl locker, and will need to configure your web server to require personal certificates and validate them against that chain. Directions for doing so will vary based on web server software, and are outside the scope of this document.