Touchstone FAQ

Touchstone FAQ

On this page:

General

- **What is MIT Touchstone?**
  MIT Touchstone is a web authentication service for the MIT community and beyond. It provides a federated authentication approach, based on Internet2's Shibboleth System. The service enables MIT users to authenticate to enabled systems both on campus and off.

- **Is MIT Touchstone a single sign-on solution?**
  MIT Touchstone provides a single sign-on solution for applications that have been coded and configured to use the system. Within the context of Touchstone-enabled applications, users will be able to seamlessly transition between systems without being prompted for additional authentication information.

- **Why did IS&T introduce Touchstone?**
  MIT Touchstone introduced some new functionality into the MIT environment. Touchstone-enabled applications typically allow MIT users (i.e. users with MIT Kerberos accounts) to choose one of several available authentication mechanisms (currently supported mechanisms include MIT X.509 certificates, username and password over TLS, and Kerberos tickets). It also enables MIT users to access some web applications at other sites without establishing new accounts, and, similarly, allows MIT web applications to support users from federated institutions.

- **How does MIT Touchstone improve the user experience?**
  MIT users can use one of several mechanisms to authenticate to Touchstone-enabled web applications, rather than being restricted to using only MIT X.509 certificates. This is quite useful, for example, when using a computer on which it is not feasible to install a certificate; users can then authenticate with username and password. Users can also set a preference so that they always authenticate using their certificate (or Kerberos tickets), so that they will generally not land at the login page. Also, Touchstone is a single sign-on system, so that users can access multiple Touchstone-enabled applications once they have logged in.

- **Why should a department, lab, or center, integrate their web application into Touchstone?**
  By adopting one technology, the web server essentially outsources the authentication task, and enables its users to choose among several authentication mechanisms, including username/password, X.509 certificates, and Kerberos. At the same time, the web server avoids the typical risks and concerns associated with consuming passwords, and does not have to have any code to deal with certificates, Kerberos, etc.
  Another benefit is that the web application will no longer have to maintain its own local accounts database to support non-MIT users. Instead the management of that community can be outsourced to Touchstone's Collaboration Accounts Management System, a self-service account registration system. Users with an account at an InCommon Federation participant can also be supported easily. This means that web applications will have the same interfaces and code paths to deal with authenticated users.

IS&T is no longer offering Touchstone Collaboration accounts. Until a new collaboration account system is launched, please contact the IS&T Service Desk if you need access to any products or services.

- **What is an identity provider?**
  An 'Identity Provider' (sometimes abbreviated 'IdP') is a service hosted by an organization which publishes electronic identity information for users that have an account, or some relationship, with the organization.
  An 'Identity Provider' acts as a trusted third party when a user attempts to access an application. The application can communicate with the IdP to determine if the user is authenticated and potentially obtain further information about the user.
  As part of MIT Touchstone, MIT operates two IdPs. One of the IdPs serves all of the people that have an MIT Kerberos username. The other IdP serves people that have a Collaboration Account, hosted by TouchstoneNetwork.net.

- **What is a WAYF?**
  WAYF stands for "Where Are You From". When an application is willing to support users from multiple identity providers, or a federation of identity providers, it needs to determine which IdP should be used for a specific user. The WAYF provides this ability, typically by

asking the user to indicate which organization has his or her account information.
MIT Touchstone operates one WAYF. Using that WAYF people may select the MIT IdP, the TouchstoneNetwork IdP, or they may select a third choice which will bring them to the WAYF operated by the InCommon Federation.

- **What is federated identity and federated authentication?**
  Identity Federation provides users access to applications across the Internet without the need for multiple login credentials or accounts. Federated authentication allows organizations to share credentials and attributes for authentication and authorization, reducing the need to maintain user profiles in multiple systems.

- **How do I know if I have an** MIT Kerberos account (username and password)?
  Many MIT computer-based systems and services share the same username/password authentication service, Kerberos. This means a user has to keep track of only one username and password -- the user's MIT Kerberos username and password -- for many systems. If you have an email account at MIT with the form <username>@mit.edu, then you have an MIT Kerberos username, and most likely know its password.
  If you are a registered student, or a full time employee, you have an MIT Kerberos account. Many other people also have an MIT account. One prerequisite for having an MIT Kerberos account is to have an MIT ID number.
  An MIT Kerberos account comes with some default entitlements. It means that you also have an MIT email address. It means that you can obtain an MIT X.509 certificate. It means that you have some file system quota assigned to you.

- **How do I obtain an MIT Kerberos account?**
  If you are a registered student or a full time employee, you have an MIT Kerberos account or are eligible to register for one if you have not already done so.

- **What is a Collaboration Account?**
  A Collaboration Account is not a traditional MIT Kerberos account. MIT Touchstone created a new accounts management system in order to support people that are not part of the traditional MIT user community, and do not have an account with a member of the InCommon Federation. We call these accounts Collaboration Accounts.
  If you are a registered student, or a full time employee, you have an MIT Kerberos account. Many other people also have an MIT account. One prerequisite for having an MIT Kerberos account is to have an MIT ID number.
  An MIT Kerberos account comes with some default entitlements. It means that you also have an MIT email address. It means that you can obtain an MIT X.509 certificate. It means that you have some file system quota assigned to you.

- **What is CAMS?**
  CAMS stands for Collaboration Accounts Management System. It is one of the services that makes up MIT Touchstone.
  If an MIT web application needs to support users that do not have an MIT Kerberos account, then the application should be configured to enable users with Collaboration Accounts to authenticate to it.

- **How do I obtain a Collaboration Account?**

  > IS&T is no longer offering Touchstone Collaboration accounts. Until a new collaboration account system is launched, please contact the IS&T Service Desk if you need access to any products or services.

- **How do I edit my Collaboration Account profile and manage my account?**
  Edit your Collaboration Account profile, change your name, manage your account or delete your account.
  Note: An MIT email address cannot be used to register for a Collaboration Account.

- **What is InCommon or the InCommon Federation?**
  InCommon's goal is to eliminate the need for researchers, students, and educators to maintain multiple passwords and usernames. Online service providers no longer need to maintain user accounts. Identity providers manage the levels of their users' privacy and information exchange. InCommon uses SAML-based authentication and authorization systems (such as Shibboleth®) to enable scalable, trusted collaborations among its community of participants.
  The mission of the InCommon Federation is to create and support a common framework for trustworthy shared management of access to on-line resources in support of education and research in the United States. To achieve its mission, InCommon will facilitate development of a community-based common trust fabric sufficient to enable participants to make appropriate decisions about access control information provided to them by other participants. InCommon is intended to enable production-level end-user access to a wide variety of protected resources. InCommon uses standards-based, SAML-compliant Shibboleth® as its federating system.

- **I have an account with an InCommon participant, can I still register for a Collaboration Account?**
  Yes. However, the registration process may warn you that you do not need a Collaboration Account and that your account from another InCommon Federation participant may meet your needs just as well.

Developer Support

- **As a developer, do I need MIT Touchstone?**
  MIT Touchstone is of interest if you're supporting a web application on an Apache or Microsoft IIS web server that needs to authenticate its users, especially if the population may be drawn from not only the faculty, staff, or students of MIT, but also other institutions in the InCommon federation, or other users that do not already have an MIT Kerberos account. For MIT users, it allows the user to select among multiple authentication mechanisms; it also provides the ability for your application to support non-MIT users without having to manage its own accounts management system. Some additional information about users can also be provided to your application via attributes for personalization or, in some limited cases, authorization.

- **If I am a developer interested in enabling an application, do I need to know about all of the MIT Touchstone technologies? Or do I just need to know about Shibboleth?**
  Most of the technologies and systems that are implemented and used by MIT Touchstone are abstracted away from the individual web application developer or system administrator. However, Shibboleth must be used by individual web applications. Developers, system integrators, and system administrators responsible for web applications should become familiar with Shibboleth.

- **How can I get some help getting started?**
  Contact touchstone-support. This will create an MIT Request Tracker case with the group that supports MIT Touchstone.

- **What platforms and environments are supported?**
  Refer to the Shibboleth Consortium's list of supported platforms (listed in the lower left column).

- **Do I need to register or sign up with IS&T to have my application use Shibboleth or MIT Touchstone?**
  Yes; currently our IdPs will display an error page to a user who is directed there by an unregistered application.
  This protects user privacy by ensuring that only services that are known and authorized to receive personal information can do so. To receive additional information, applications must be registered with IS&T so that the IdP will know what information to release to the application.
  If you are interested in registering your services, you will be asked to describe your application(s) and how you intend to handle and protect the personal information you receive.

System Integrator Questions about Shibboleth

- **How long do user sessions last and is there an inactivity timeout?**
  The Shibboleth SP software allows you to control the time elapsed before its session expires. A separate configurable timeout based on inactivity (i.e. without accessing Shibboleth-protected content) is also enforced. However, these are distinct from the lifetime of the IdP session that enables single sign-on; in many cases, using a local timeout that is shorter than the single sign-on session time is not useful (an exception may be when the application does its own session management, so there is no point in maintaining the Shibboleth session). Currently, the single sign-on session lifetime enforced by the MIT identity provider is eight (8) hours. Other identity providers will likely have different policies.

- **Does Shibboleth support logout?**
  Not at this time. Instead users should exit the browser in order to logout. (This is the same as we currently recommend for users of personal X.509 certificates). The Shibboleth SP provides a local logout mechanism, which is useful primarily for any session cleanup you may wish to perform; remember that, with single sign-on, a user typically can still access protected content on your server without having to login again.

- **Can Shibboleth be set up without a WAYF?**
  Yes. This is reasonable if your application will only support one user community, or one identity provider. However, we recommend that you strongly consider supporting a wider user community if it makes any sense for your application or business function.
  It is also possible to set up your application without using a WAYF even if you are supporting the use of more than one identity provider. Sometimes an application wants to tightly control its own look and feel. In such cases the application can function as if it were its own WAYF. Although this is possible we generally recommend that systems use the WAYF. We feel that consistency in appearance, across multiple applications, for this aspect of authentication is desirable.

Attribute Release Policies and Privacy

- **What is an attribute release policy?**
  An attribute release policy defines the information that will be released by the Identity Provider to a particular Service Provider (i.e. application web server) for an authenticated user. The information is released as a set of named attributes with one or more values for the user.

- **Can a user restrict what information about them gets released?**
  No, not at this time.

- **What attributes do you release to MIT service providers?**
  Generally we release the following attributes to MIT Service Providers, for both MIT Kerberos and Collaboration accounts:

- eppn (eduPersonPrincipalName)
  This is the authenticated user name, "scoped" to a particular domain, e.g. jdoe@mit.edu. This value is typically mapped to REMOTE_USER by the Service Provider software.
- displayName, e.g. John Doe
- mail
  (For MIT users, currently this is always username@mit.edu.)

For MIT users, we also release these affiliation attributes:

- affiliation
  This is a "scoped" value, e.g. staff@mit.edu
- unscoped_affiliation, e.g. staff
- primary_affiliation, e.g. staff

The set of affiliation values is:

- student
- staff
- affiliate

We release the following additional attributes for Collaboration accounts:

- givenName, e.g. John
- sn (surname), e.g. Doe

- **What attributes do you release to non-MIT service providers?**
  This varies, but generally our policy is to release only those attributes that are required in order for the provider's application to function properly. Usually, but not always, this includes the user name (eppn), but some providers now accept an opaque persistent ID instead of the user name; the Identity Provider for MIT users can generate and release such an opaque ID to these providers.

See Also

- MIT Touchstone Authentication Landing Page