ENTERPRISE
TECHNOLOGY

1616 Guadalupe St, Austin, TX 78701 - UTA Building | tech.utexas.edu

IAM Cloud Integration

July 2020

Guidelines Policies

Introduction

When planning the implementation of an externally hosted or cloud-based service university colleges, schools, and units need to understand and consider implications related to identity, authentication, authorization, and access management.

These guidelines help inform campus constituencies of the available tools, techniques, and best practices to inform the planning and execution of their cloud service implementations.

Terms to Know

Attributes

The data associated with an identity. For example, the UT EID, name, email address, major, department, etc.

eduPersonPrincipalName (ePPN)

Format: <UT EID>@utexas.edu
A scoped username used to distinguish UT Austin accounts from accounts at other institutions. The ePPN is not the same as an email address.

Enterprise Authentication

The university's centralized Identity Provider and authentication solution. Enterprise Authentication leverages Shibboleth software using the SAML2 standard to support the integration of internally and externally hosted services with UT EID authentication.

Identity Provider (IdP)

A Service Provider can offload authentication and identity attribute responsibilities to an Identity Provider. This has the practical effect of facilitating Single Sign-On (SSO) and limiting Service Provider exposure to data unneeded, sensitive data.

The University of Texas at Austin's centralized Identity Provider is run by the IAM Team. This Identity Provider allows Service Providers to use UT EID authentication and receive approved identity attributes for the authenticated user.

Institutional Identifier (IID)

Format: <UT EID>@eid.utexas.edu
Many cloud services operate off identifiers that take the form of an email address. These identifiers are typically immutable and do not account for changes in the user's email address. To mitigate anticipated problems, the university created the Institutional Identifier (IID), also known as the utexasCloudID, to be a constant even if EID holders change their official email addresses on record.

To preserve cloud functionality, emails sent to the IID are automatically routed to the user's email address on file. IIDs can be made available to SPs for Member- and Affiliate-class UT EIDs, as well as Guest EIDs with a special entitlement code.

Provisioning and Deprovisioning

Provisioning is the process of creating user accounts and providing the accounts with the appropriate authorizations.

Deprovisioning is the process of deleting, archiving, or making inactive a user account when it is no longer needed by the Service Provider.

Security Assertion Markup Language (SAML)

SAML is an XML-based open standard data format for exchanging authentication and attribute data between parties. In particular, the university's Identity Provider and a Service Provider will communicate using SAML. The university uses the SAML2 standard to support the integration of externally hosted services with UT EID authentication.

SAML Metadata

The IdP and SP have their own, complimentary metadata which facilitates secure communication. This metadata contains certificate and endpoint information about each party.

Service Provider (SP)

The service which a college, school, or unit is looking to provide to their users is offered by the Service Provider.

The Service Provider can offload authentication and identity attribute responsibilities to the Identity Provider. This has the practical effect of facilitating Single Sign-On (SSO) and limiting Service Provider exposure to data unneeded, sensitive data.

Sponsor

The department or organization within the university which is sponsoring or purchasing the application/service provided by the Service Provider.

Shibboleth

A federated identity solution widely deployed and used in educational institutions. The university's central Identity Provider is powered by Shibboleth.

UT EID

The University of Texas at Austin Electronic Identifier. The primary identifier for faculty, staff, students, and alumni at the university.

Resourcing

1. All Service Providers (SPs) must have a Sponsor. Sponsors must be a university college, school, unit, department, center, division, etc.
2. All Sponsors must provide contact information. It is strongly recommended that this contact information be in the form a group email address.
3. All Sponsors are required to sign an Acceptable Use Policy (AUP) and must delegate the signer role to an appropriate AUP Signer in their area.
4. Roles and responsibilities of both the Sponsor and the Service Provider (SP) should be clearly understood and documented prior to the implementation and the ongoing sustainment of the service.
5. The Sponsor should consult the IAM Team early in their vendor selection process to help assess the Service Provider's ability to successfully integrate with the university's central Identity Provider (IdP).
6. The Sponsor should develop an implementation plan that includes regular checkpoints with the IAM Team.
7. The Sponsor should request that the Service Provider (SP) identify and provide a dedicated technical contact that is familiar with SAML2 integration.
8. The Sponsor should determine who should provide ongoing user support for the service (the Service Provider, the Sponsor, or some other group).

Implementation

1. If the service has been implemented by multiple departments on campus, the Sponsor should strong consider implementing a single campus-wide service instance to reduce ongoing maintenance costs.
2. The Sponsor should confirm that the Service Provider (SP) has a robust and fully implemented SAML 2.0 capability.
3. The Sponsor should understand the limitations of what data the university Identity Providers (IdP) are able to provide to the Service Provider (SP).
4. The Sponsor should understand what data is transmitted from the university's Identity Provider (IdP), when it is transmitted, and how that impacts their business case. Attribute data is only provided during each successful authentication by the user. The Sponsor may have to devise a separate process to provide data to the Service Provider (SP) if account data needs to be loaded before users can authenticate to the new service, or if the user account data needs to be updated outside of user authentication.
5. The Service Provider (SP) should use UT EID or the eduPersonPrincipalName (EPPN), not an email address, as the user identifier. If the service provider requires the use of an email address as the user identifier, the IID can be used instead.
6. The Sponsor should determine if the Service Provider (SP) will need to authenticate non-person identities.
7. The Sponsor should discuss contract obligations with the Service Provider (SP) that specifically protect UT Austin identity information to the level mandated by the applicable laws/regulations including FERPA, HIPAA, etc.
8. The Sponsor should understand how the UT System Two Factor Authentication Mandate applies to the data being shared with the Service Provider (SP) and determine if Multi-Factor Authentication (MFA) is required beyond the existing baseline.
9. The Sponsor should understand and document how users will be provisioned and deprovisioned (i.e. on-demand, back-channel provisioning, etc.)
10. The Sponsor should confirm that the Service Provider (SP) is able to perform automatic, dynamic SAML metadata refreshes.

11. The Sponsor should confirm that user attributes are automatically consumed and updated by the Service Provider (SP) on every assertion. This will help ensure that all user attribute data stored in the service is up-to-date and eliminate the need for staff to keep these updated. Due to potential security concerns, users should not be allowed to manually update these attributes.
12. The Sponsor should verify that the Service Provider (SP) can handle authorization checks that take into consideration the complex conditions of UT Austin. For example, if the Service Provider (SP) needs to restrict access to a specific school or department, the service provider will need to be able to check multiple user attributes passed from the Identity Provider (IdP) to make the authorization decision.
13. The Sponsor should develop a detailed test plan that includes testing authentication and authorization functions of the system. For example, if there will be multiple types of users in the system (e.g., students and administrators) the tests should include verifying that the system operates properly for each of these user types.
14. The Sponsor should review the Enterprise Authentication documentation prior to the integration with a Service Provider (SP) to understand the features and limitations of the university's SAML IdP services. For example, Single Log Out (SLO) is not a feature of the SAML IdP.

- User sessions are not replicated between the authentication services on campus. The university is consolidating to Enterprise Authentication for authentication, so it is the recommended SAML IdP for a better Single Sign On (SSO) experience.

User Experience

1. The Sponsor should create an informational page that informs users of where and how to get support for the service.
2. The Service Provider (SP) should have a landing page that is *not* protected by authentication for users to bookmark. This landing page should have a link or button to take the user to the protected resource. Without a landing page, users may bookmark the IdP authentication page and will receive an error the next time they attempt to use the bookmarked page since the IdP will not know which service provider site to forward the user to. This landing page can be hosted anywhere (i.e., by the Service Provider (SP) or at the university by the Sponsor).

External References

Authentication Acceptable Use Policy
https://iamservices.utexas.edu/resources/policies/authentication-acceptable-use-policy/

IAM Integrations
https://iamservices.utexas.edu/integration/

Institutional Identifier (IID)
https://ut.service-now.com/sp?id=kb_article&number=KB0011278

TED Directory Attributes
https://pages.github.austin.utexas.edu/eis1-iam/ted-schema/