

# UW Web Identity Provider (IdP) support

The focus of this analysis document is which web-based Identity Provider(s) (IdP) UW-IT should support and recommend at a baseline level. For the purposes of clarity, we will refrain from using the term “UW IdP” to refer to a specific identity provider because it implies a preferred identity provider, whose future state this paper discusses.

The reference document for this topic is the [Web Authentication Brick](#). Unfortunately, that reference document<sup>1</sup> does not differentiate what each lifecycle designation means in terms of support provided to UW customers or to what degree UW-IT might recommend a given technology. In practice, UW Shibboleth is the preferred provider for web-based application integrations and UW-IT provides application integration consulting to the UW community at no cost. This support and benefit are among the undocumented expectations customers might have for an identity provider in baseline lifecycle status.

## [Executive Summary](#)

### [Protocol support](#)

### [Application fulfillment and delegated support](#)

## [Background](#)

## [Assumptions](#)

## [Discussion](#)

### [Request fulfillment](#)

### [Capabilities](#)

#### [Basic capabilities \(protocol support\)](#)

#### [Reliability](#)

#### [Application fulfillment and delegated support](#)

#### [External identity support](#)

#### [Security protections \(CARTA & OFD\)](#)

### [Costs](#)

### [Ability to customize](#)

## [Conclusions](#)

### [Exit Strategy](#)

### [Transition scenarios](#)

#### [What do we do with UW Shibboleth?](#)

##### [Scenario 1](#)

---

<sup>1</sup> In contrast, the Microsoft Infrastructure service [supports the UW Azure AD at a baseline level, with an explanation of what each lifecycle designation means](#) in terms of expected customer support.

[Scenario 2](#)

[Scenario 3](#)

[How to switch from Duo to Azure MFA](#)

[Existing UW Shibboleth applications](#)

[Other implications](#)

[Recommendation](#)

[Landing place for thoughts which don't yet have a good place](#)

## Executive Summary

Over the past several decades, the UW has used several implementations of web authentication identity providers:

- UW Pubcookie: 1998-2019
- UW Shibboleth: 2005-today
- UW ADFS: 2013-2022
- UW Azure AD: 2013-today

Currently, the UW predominantly uses Shibboleth and Azure AD.

Azure AD is provided by Microsoft, with a very large engineering and support organization, and is tightly integrated into their identity security capabilities. The University currently uses Azure AD to provide a number of services.

Shibboleth is an open-source solution provided by the Shibboleth Foundation. The University implementation of Shibboleth is customized and maintained by UW-IT. It is utilized solely for identity management and authentication at the UW.

Table 1 - Summary of Traits of IdPs















	UW Shibboleth	UW Azure AD
Protocol support		
Reliability		
Application fulfillment and delegated support		
External identity support		
Secure		
Cost-Effective		
Ability to customize		

Table 1 represents a high-level summary of traits of UW Shibboleth and UW Azure AD as covered in much more detail in the discussion sections of this analysis paper. Brief explanations of the ratings of each of these traits are provided here.

## Protocol support

Today the major web authentication protocols are SAML, OAuth 2.0, OIDC, and SCIM. Every commercial identity provider supports all of these protocols. Azure AD supports all 4 of these protocols; UW Shibboleth supports only SAML and OIDC. Each gets the same number of thumbs as major protocols supported. Additionally, there are less widely adopted protocols supported by each. Microsoft is recognized as the leader for Authentication by IDC Marketscape.

## Reliability

The reliability of authentication infrastructure is of critical importance, with a direct impact on the UW community. Over the past 3 year period, both UW Shibboleth and UW Azure AD have had a roughly equal small number of P1 or P2 incidents, which earns them one thumb each. During 2021, Microsoft has made significant improvements in Azure AD reliability and continues to invest heavily in this area, which earns it another thumb.

## Application fulfillment and delegated support

Both UW Shibboleth and UW Azure AD allow for self-service fulfillment of basic application integration, earning both one thumb. More advanced application configurations require UW-IT involvement to enable, with slightly more UW-IT involvement required for UW Shibboleth advanced features. UW Azure AD gets 2 additional thumbs for its large template library with detailed instructions on how to integrate over a thousand applications, delegated access to application sign in logs, and additional delegated capabilities for more advanced configurations.

## External Identity support

UW Shibboleth and UW Azure AD have useful but different approaches to providing support for external identities. There are benefits and downsides to their different approaches. Shibboleth via EduGain has access to more than 5K IdPs. Azure AD has access to more than 200K IdPs. UW Azure AD can support social IdPs natively, whereas UW Shibboleth requires a 3rd party gateway service. Azure AD provides broader support natively which results in the slight advantage in thumbs.

## Secure

UW Shibboleth provides the basic *mechanisms* so an application does not need to handle a user's credentials and has rudimentary adaptive controls. Azure AD is a noted leader of the relevant Gartner Magic Quadrant, not only delivering a full set of security features but demonstrating a compelling vision for the future. UW Shibboleth earns one thumb for the basic

security features it possesses. Azure AD earns one thumb for the same, one for its broad set of security features, and one for having a compelling roadmap.

## Cost-effective

For the broad web application authentication value it provides, UW Shibboleth costs very little. On an annual basis, there are minimal hosting costs, and reasonable engineering costs to maintain the hardware and software. Costs to assist customers with application integration are about the same as engineering costs. In contrast, UW Azure AD has no hosting costs and no engineering costs to maintain hardware or software. Costs to assist customers with application integration to UW Azure AD are less than UW Shibboleth.

UW Shibboleth in combination with Duo are the existing pillars of UW web authentication. Duo is very expensive. Azure AD works with Duo, but prefers Azure MFA, and costs for the UW to use Azure MFA for web authentication are extremely low in comparison to Duo.

So with the overall web authentication background included, UW Azure AD is much less costly than UW Shibboleth.

## Ability to customize

UW Shibboleth allows full customization of the user interface, authentication flows via experimental plug-ins, and the user experience. The limits to customization are only constrained by imagination and technology.

UW Azure AD allows customization of high value elements including user interface branding, session management length, custom terms of use per application, and other needs which customers have identified. The limits to customization are constrained by what Microsoft deems critical to satisfy customers. Beyond UW Azure AD, customers with greater customization needs can deploy Azure AD B2C for extreme levels of customization, including support for external data sources for claims.

The approach to customization for each product generally reflects the basic difference between open-source and vendor software. Over time, open-source software requires greater amounts of effort via customization, while vendor software trends toward becoming a commodity focused on common business needs. We are aware of no unique UW business needs for customization, so while there is an upper limit on what Microsoft can provide immediately, we ultimately score these equal with two thumbs.

## Background

Modern web-based authentication involves an identity provider, a specialized service which authenticates a user and provides a verifiable token which can be given to web applications to establish the user identity with that web application. When web-based authentication does not

involve the web application collecting user credentials, it simplifies support and minimizes the points of risk. This modern web-based authentication pattern is sometimes referred to as [Identity 2.0](#).

An identity provider (IdP) primarily provides authentication services to relying applications, also called relying parties or service providers, which are applications that rely on the identity asserted by the IdP. Applications, primarily web applications, outsource the user authentication step to a trusted IdP. The IdP issues a token that is proof of authentication which is then used to gain access to the application.

IdPs also provide identity information, often called claims, which can be used for access control decisions. Modern expectations for an IdP can be found in recent Gartner papers, such as [IAM Leaders Guide to User Authentication](#) (Dec 2020) and [Market Guide for User Authentication](#) (Jun 2020). These expectations include security features, such as online fraud detection (OFD) and continuous adaptive risk and trust assessment (CARTA) capabilities.

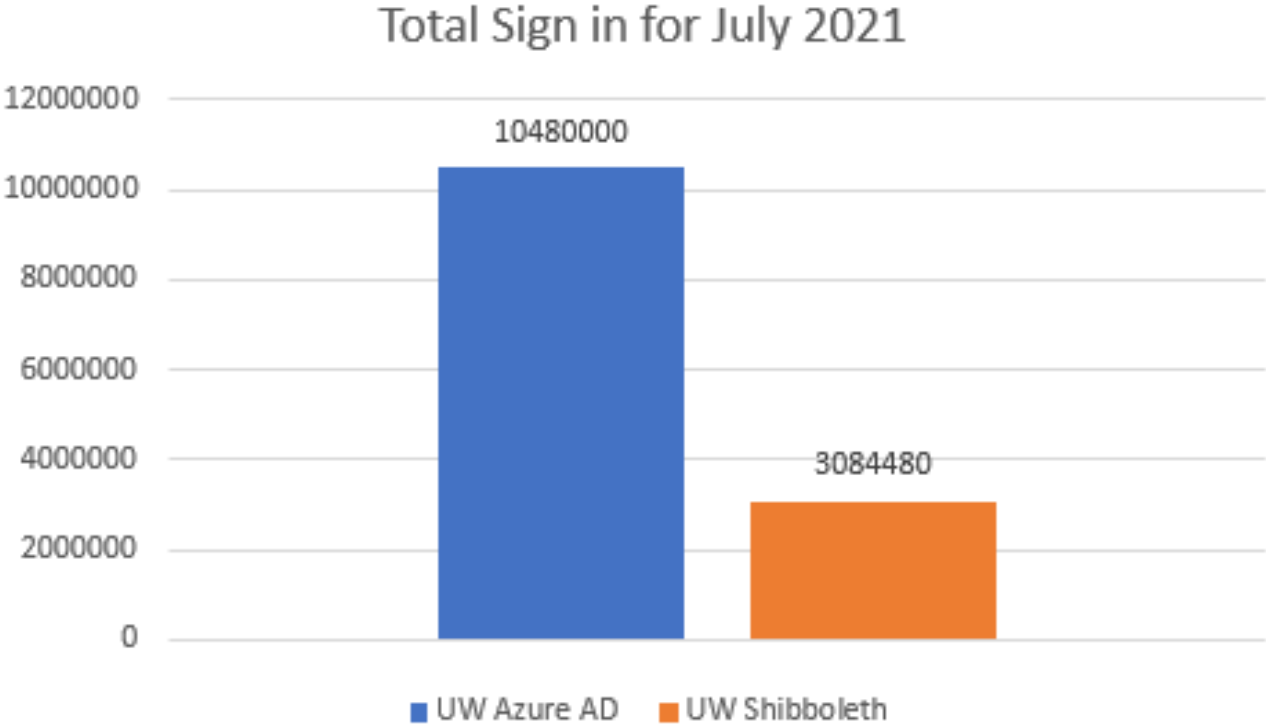
OFD capabilities include correlation of prior user behavior, current and past location, detection of known abuse patterns, publicly known compromised account credentials still in use, multiple authentications from geographically impossible locations, multiple failed authentications from the same locations, and other security signals. OFD is no longer an emerging technology, with Garner noting “[we now see forward-looking vendors broadening the range of capabilities that they offer](#)” and “There is strategic recognition by a growing number of vendors that, if they continue to offer a single capability in the field of OFD, they are likely to become increasingly marginalized in the market.”

CARTA capabilities include contextual data such as the location, known security-related characteristics of the client device, type of authentication factors presented, authentication from previously unused locations or applications, or even specific application activity being attempted.

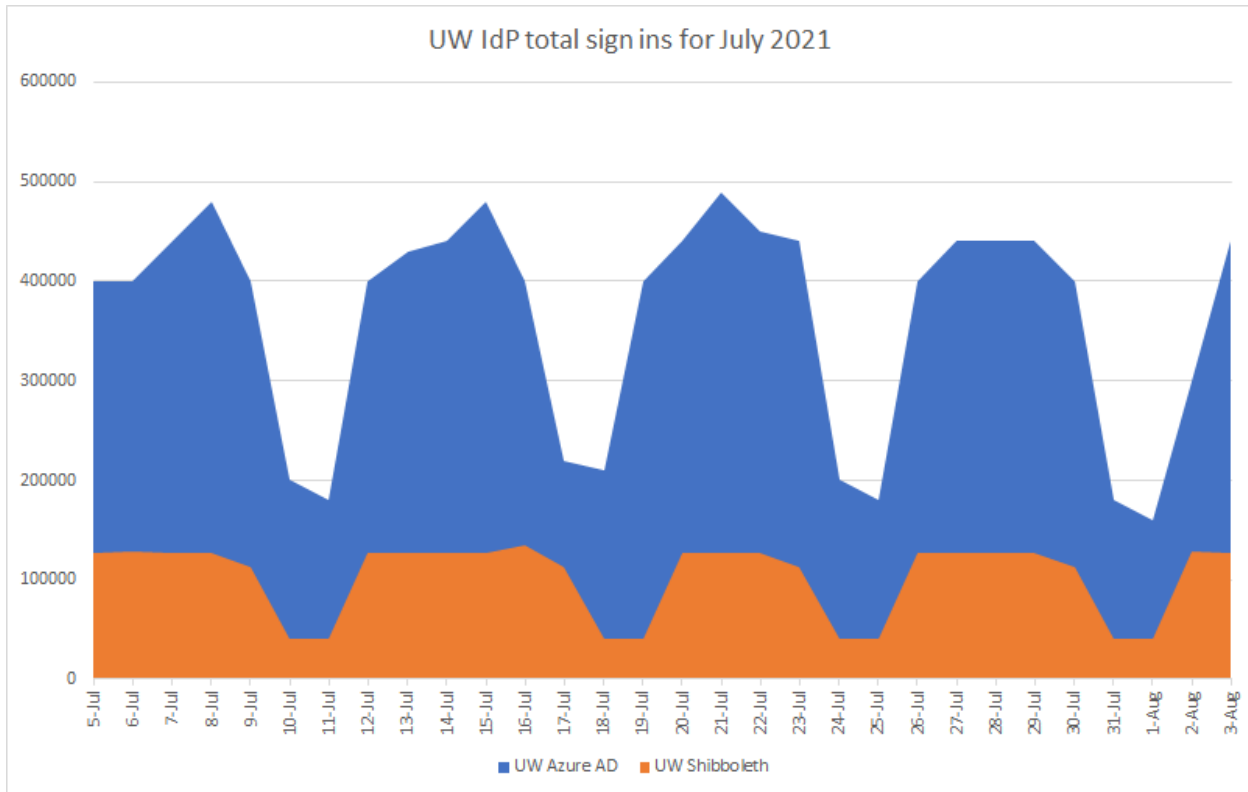
The primary reason OFD and CARTA are highly desirable is because they reduce risk and increase the trustworthiness of the authentication process. Having trustworthy authentication is the primary goal for an identity provider. Done correctly, both OFD and CARTA require an IdP to have adequate data sources, signal volume, processing power, and analytical capabilities to ensure authentications are promptly allowed or denied. Having sufficient trustworthy data and the ability to dynamically adjust your organization’s risk posture on a per-user basis to these risk signals is an important feature of these capabilities.

As noted in the [Web Authentication Brick](#), the UW has many identity providers and technologies in use. Among those, UW Shibboleth and UW Azure AD are the 2 used primarily by the UW community. By default, UW Shibboleth is recommended for application integrations and provides the expected experience for web-based user sign in at the UW. Today, UW Azure AD provides application integration for applications that need to integrate with Microsoft products, applications which require the OpenID Connect (OIDC) or OAuth 2.0 protocols, which require

the SCIM provisioning protocol, or which have some other need which UW Shibboleth cannot meet. Despite being the default identity provider for application integration, UW Shibboleth has about one-third the volume of sign in traffic<sup>2</sup> that UW Azure AD does.



<sup>2</sup>UW Shibboleth total sign ins are not tracked, so estimation using averages from [Grafana](#) data were used. The UW Azure AD total sign ins are sourced from Azure Portal.



Shibboleth is the reference Security Assertion Markup Language (SAML) protocol implementation, open-source, and widely used in the Education sector. Outside the Education sector, its use is extremely limited. UW Shibboleth has had a baseline support level since 2014. The UW Shibboleth IdP today has several code customizations to support a variety of capabilities important to the UW--see the 'Ability to customize' section for more information.

Microsoft is a leading software company which has a several decade history of providing market leadership in the Identity market space. Over 200K customer organizations use Azure AD, with 425 million monthly active users, and 30 billion authentications a day<sup>3</sup>. UW Azure AD is a Microsoft cloud-based identity provider which the UW implemented in June 2013 to support business needs provided by Microsoft technologies. Widely used across all business sectors, Azure AD supports SAML, OIDC, and OAuth 2.0. Microsoft provides many additional capabilities and a level of engineering support and investment which vastly exceeds the UW's ability to match. Notable among these additional capabilities are the ability to provision users via System for Cross-domain Identity Management (SCIM), a rich set of conditional access controls, and automated signals-based security detections that can be used to protect identities and access to resources. UW Azure AD had an emerging support designation from 2013 through July 2021, when it was adjusted to reflect the reality that it is at least in a tactical support designation.

<sup>3</sup> <https://www.microsoft.com/en-us/security/business/identity-access-management/azure-active-directory>

# Assumptions

The increasing prevalence and reliance on commercial Identity and Access Management systems are a rising trend across the IAM industry<sup>4</sup>. Shibboleth was the initial identity provider product, but the identity provider capabilities and customer business needs have moved beyond pioneer stage to commoditization.

## Capability Comparison of Shibboleth to commercial IdPs

	Shibboleth	Azure AD	Okta	Google	OneLogin	Auth0	PingFederate	Sailpoint IdentityIQ
SAML	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OIDC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OAuth 2.0	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SCIM	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2FA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Automated risk-based protections (CARTA)	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Online Fraud Detection (OFD)	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Pre-integrated application templates	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Supports multilateral federation	Yes	No	No	No	No	No	No	No

<sup>4</sup> Gartner: [Technology Insight for Customer Identity and Access Management](#) (May 2020), [Predicts 2021: Identity and Access Management and Fraud Detection](#) (Dec 2020), [Hype Cycle for Identity and Access Management Technologies, 2021](#) (see "IAM Managed Services") (Jul 2021)



Shibboleth is still very prevalent in the Education sector<sup>5</sup> among UW peers. Certainly, no other business sector is using Shibboleth to the extent the Education sector does. However, anecdotal evidence<sup>6</sup> suggests universities are increasingly shifting to commercial products.

## Commercial IdP use in Higher Education

	Azure AD	Okta	Cirrus Identity Bridge
Large R1 universities or equivalent <sup>7</sup>	<a href="#">Penn State</a> , <a href="#">Oxford</a> , <a href="#">John Hopkins</a> , <a href="#">U of Birmingham</a> , <a href="#">UC-San Diego</a>	<a href="#">Iowa State</a> , <a href="#">WSU</a>	Iowa State, Yale, UC-Berkeley, Michigan, MIT, CMU, Indiana, Arizona, Oregon
Other universities	<a href="#">DePaul</a> , <a href="#">UNCG</a> , <a href="#">Univ of Dundee</a> , <a href="#">U of Rhode Island</a> , <a href="#">U of Glasgow</a> , <a href="#">UNCP</a> , <a href="#">State Univ of NY New Paltz</a> , U of South Florida, Millersville University, <a href="#">Mansfield University</a> , <a href="#">SUNY Geneseo</a>  In progress <sup>8</sup> : Cedarville University, Campbell University, U of Louisville	<a href="#">U of Puget Sound</a> , <a href="#">Notre Dame</a> , <a href="#">CalState-Monterey Bay</a> , <a href="#">Union College</a> , <a href="#">U of Tampa</a>	<a href="#">CalState-Monterey Bay</a> , <a href="#">Union College</a> , Pomona College, Carleton, Millersville University, UNLV, Oregon Institution of Technology, American University at Sharjah, <a href="#">U of Tampa</a> , Icahn School of Medicine at Mount Sinai, <a href="#">U of Rhode Island</a> , Chapman University, Lock Haven University, <a href="#">Mansfield University</a> , <a href="#">U of Puget Sound</a>
Other Higher Ed entities	Educause <sup>9</sup>		Educause, NIH, Internet2

## Discussion

### Request fulfillment

Today, the majority of application integrations are directed to UW Shibboleth as the “preferred” option, with other options chosen only when an application requires a protocol or capability that UW Shibboleth does not provide. Since a standardized application integration practice emerged in September 2016 through early August 2021, there were 131 customer requests fulfilled by the UW IAM business service. Most web application integration requests have used this fulfillment pattern, so this provides a representative sample for analysis.

<sup>5</sup> Shibboleth Consortium: <https://www.shibboleth.net/>

<sup>6</sup> Azure AD: [Penn State](#), [DePaul](#), [UNCG](#), [Univ of Dundee](#), [U of Rhode Island](#), [U of Glasgow](#), [U of Birmingham](#), [Oxford](#), [John Hopkins](#), [UNCP](#), [State Univ of NY New Paltz](#)

Okta: [Notre Dame](#), [Iowa State](#), [U of Puget Sound](#), [WSU](#)

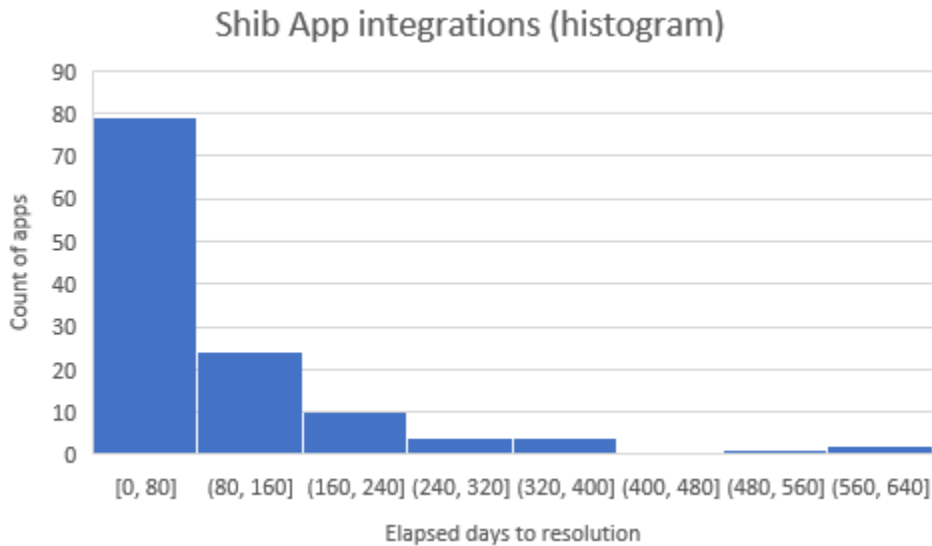
<sup>7</sup> The R1 designation is limited to US universities. Equivalence uses the other factors without regard to nationality. See [https://en.wikipedia.org/wiki/Research\\_1\\_university](https://en.wikipedia.org/wiki/Research_1_university)

<sup>8</sup> Source: [i@m@educause.edu](mailto:i@m@educause.edu) mailing list

<sup>9</sup> Go to <https://www.educause.edu/Login.ashx?returnUrl=/> (Cirrus Identity Bridge) and choose Educause as your source institution (and get AAD sign in)

Table 2 - Customer Application Integration Request Fulfillment<sup>10</sup>

	UW Shibboleth	UW Azure AD
Total requests	122	9
Average (elapsed) number of days to fulfill	97.7	52.5



The length of time to complete an integration request is dependent on a number of factors, including time spent waiting for the caller or vendor, and presumably has some correlation to the choice of IdP technology and the vendor's familiarity with it.

It's worth noting that all of the requests fulfilled using Azure AD had an additional routing delay due to first going to the Authentication/Identity and Access Management assignment group(s). It is also worth noting that there is no internal fulfillment documentation for Microsoft Infrastructure to fulfill these requests, so those times could be expected to lower significantly if the lifecycle support for Azure AD changed and that investment was made.

Overall, the data suggests that Azure AD based application integrations result in customer fulfillment more quickly, however, the sample size for AAD integrations is smaller, so there is some reduced confidence. If more confidence in this data was desired, more application integrations could be routed to Azure AD. There are 9 open application integrations for UW Shibboleth which so far have an average elapsed time of 100.9 days, which suggests the

<sup>10</sup> Data based on UW Connect Requests with a short name beginning "Application Integration requested by", as of August 2021. An excel spreadsheet showing counts and elapsed time available from Brian Arkills.

average in the table is representative, not an anomaly. The only open application integration for UW Azure AD has only been open 19 days.

To explain this difference in fulfillment time, one might hypothesize that for most vendors and customers, Azure AD is a standard out-of-the box solution with custom attributes and claim mappings provided by the vendor by default, while those same custom attributes and claim mappings require more custom integration with Shibboleth. This is because Azure AD is widely adopted and very well documented. In contrast, Shibboleth is really only used in the Education sector and represents a learning curve for many vendors and customers. Microsoft's step-by-step application integration documentation for over 1000 applications is a concrete example of why fulfillment might take longer with Shibboleth than Azure AD. Testing the validity of this hypothesis would require a survey of customers and vendors.

## Capabilities

Table 3 - Supported capabilities of UW web identity providers

	UW Shibboleth	UW Azure AD
SAML	Yes	Yes <sup>11</sup>
OIDC	Yes <sup>12</sup>	Yes
OAuth 2.0	No	Yes
SCIM	No	Yes
WS-Fed	No	Yes
WebAuthN	No <sup>13</sup>	Yes
Verifiable Credentials	No	Yes
2FA	Yes	Yes
Conditional Access	Limited & custom	Yes
Terms of Service	Yes	Yes
Automated risk-based protections (CARTA)	No	Yes
Online Fraud Detection	No	Yes

<sup>11</sup> Azure AD does not support the full set of SAML capabilities. Of importance to the UW are: lack of support for custom IdP metadata (required for R&S category) and multilateral SAML federation (required for participation in InCommon and other global research and education federations).

<sup>12</sup> Shibboleth v4.1 supports OIDC via a plug-in.

<sup>13</sup> A third party dev module exists but is not natively supported by Shibboleth

(OFD)		
Per-application sign in logs for application owners	No	Yes
Pre-integrated application templates	No	Yes
Support for custom claims	Yes	Yes
Highly customizable	Yes	
Supports multilateral federation	Yes	No <sup>14</sup>
Custom IdP metadata	Yes	No
Supports <a href="#">Research &amp; Scholarship (R&amp;S) category</a>	Yes	No <sup>15</sup>

## Basic capabilities (protocol support)

Shibboleth is the reference SAML implementation provided by the Shibboleth Foundation. Its support for the SAML protocol is exceptional, but it lags behind in support of more modern protocols and capabilities. Shibboleth has released support for OIDC, and after testing the UW has deployed this to customers. Shibboleth does not support SCIM for automated user lifecycle provisioning to SaaS applications, nor OAuth 2.0 protocol support. Shibboleth also supports the MetaData Query (MDQ) protocol, which will be discussed in the ‘External Identity support’ section.

Azure AD is a mature, cloud-based identity provider, supporting all broadly adopted modern authentication related protocols, and active in proposing new standards in concert with the vendors of other commercial identity providers. Azure AD supports SAML, WS-Fed, OIDC, OAuth 2.0, and SCIM.

The SCIM protocol provides an automated way for an identity provider to automatically provision and deprovision user accounts to applications. 53.5%<sup>16</sup> of customers using the IAM application integration survey want this capability. It eliminates the need for an application administrator to manually provision and deprovision user accounts. Each application must provide SCIM support, but since it is a standard with broad adoption, it is unlike the UW’s homegrown subscription system in that it is more readily supported. Today, applications which use Shibboleth have no option other than asking UW-IT to support them via the UW subscription

<sup>14</sup> Azure AD provides guest accounts via B2B capabilities, which has its own unique benefits, like being able to centrally add additional access conditions on external accounts. Up to 1000 external IdPs can be federated via this.

<sup>15</sup> Azure AD supports custom claims, and can easily be configured to supply eduPersonPrincipalName and even the optional eduPersonScopedAffiliation, however, it can not meet the IdP metadata requirement (see #7, at <https://refeds.org/category/research-and-scholarship>).

<sup>16</sup> Data available upon request, based on review of UW Connect requests using the IAM form.

system if they want this kind of capability. The UW subscription system isn't generally provided to customers. SCIM represents a possible future opportunity for UW-IT to step away from its custom subscription system for internal use cases.

Token expiration and refresh is a standard mechanism associated with identity providers. How it works depends on the specifics of which protocol is being leveraged, but we will generalize for discussion purposes. Successful authentication generally results in an identity token, which can then be used to get an access token for each application. A refresh token is also issued which can be used to get a fresh access token without interactive sign in. Each of those 3 token types has a different lifetime, but the key one is the refresh token lifetime. This is because it is what determines whether the user is interrupted and must sign in again. Modern IdPs like Okta, OneLogin, Auth0, and Google<sup>17</sup> all have significantly longer token lifetimes than UW Shibboleth's 8 hour lifetime. Even emerging efforts supporting research and researchers like [Open Researcher and Contributor ID \(ORCID\) have chosen very long lifetimes](#). They have all chosen this longer lifetime because their research has shown this results in an improved user experience and a better security result due to users falling for fewer phishing attacks due to sign in fatigue. Azure AD takes this farther than most other modern IdPs--it has an indefinite refresh token lifetime. Azure AD has automatic security mitigations which invalidate a given token should a security event be detected, which forces a fresh interactive sign in. This type of modern approach to token expiration and refresh is something which is missing in UW Shibboleth but represents a strength of Azure AD.

Azure AD has a few gaps in its SAML capabilities which are of note to the UW: lack of support for custom IdP metadata which is required for the [Research & Scholarship category \(R&S\)](#) and multilateral SAML federation (required for participation in InCommon and other global research and education federations). The Research and Scholarship category is a bundle of claims which equate to the same claims which every major identity provider vendor includes by default, but with support for eduPerson specific variations--so R&S support is really about compatibility for the very few Education sector identity providers that are not using the NameID claims that all other vendors have standardized on. In other words, this is a case where Education has gone into the weeds, and expects everyone else to follow. Likewise, Microsoft and every other large cloud vendor providing identity provider products do not think multilateral SAML federation is a good idea, so whether this is a downside or an upside is debatable. The topic of multilateral federation and the ways that other universities who have adopted Azure AD have employed to address these gaps is discussed further in the 'External identity support' section.

With Shibboleth, you wait for modern basic capabilities. With Azure AD you get the modern basic capabilities and must work around those gaps which are considered significant.

## Reliability

Both UW Shibboleth and Azure AD have had several P1 or P2 incidents in the past 3 years.

---

<sup>17</sup> [Okta: 100 days](#), [OneLogin: 45 days](#), [Auth0: 30 days](#), [Google: 6 months](#)

Table 4 - Major incident over past 3 years

UW Shibboleth	UW Azure AD
INC1657779 (expired cert), INC1387192/INC1387913 (gws outage), INC1093030 (ELB expired cert)	INC1770359, INC1754770, INC1616817 <sup>18</sup>

The number is roughly comparable, but considerably less UW time was spent resolving the Azure AD incidents since the vendor was responsible to resolve them. With Shibboleth we have full configuration control, including the underlying platform. That control comes at the cost of providing the provisioning and maintenance of the full stack, as well as designing and maintaining critical aspects like continuity and capacity.

Despite these outages, Azure AD has a generally strong fault tolerance/disaster recovery story, with a global presence, significant engineering resources to improve resiliency, transparency in lessons learned and a documented roadmap for resiliency improvements. Earlier this year, Microsoft revealed the presence of a backup authentication service which can be leveraged on a per-tenant basis as needed. A few months ago, Microsoft completed implementation of a [cell-based architecture](#) for Azure AD, and redesigned their deployment practices to include modern verification in a multi-ring deployment model. Microsoft is investing heavily in resiliency.

## Application fulfillment and delegated support

Table 5 - Application support details

	UW Shibboleth	UW Azure AD
Basic application creation self-fulfillment	DNS contacts	Any UW AAD user
Federation enablement	Via UW-IT	Yes
Basic claims	Yes	Yes
Additional claims	Via UW-IT	Yes
2FA required configuration	Yes	Via UW-IT
Restrict access to a group	Yes	Yes
Restrict access based on device health, geo-location, sign-in or user risk, IP	Limited to IP address and group membership	Yes

<sup>18</sup> UW ADFS had INC1304347 during the past 3 years, but it is no longer part of our AAD architecture, so isn't being counted.

address, etc.		
Installation templates	Basic	1000+
Access to sign in logs	No	Yes
Provisioning setup	N/A	Via UW-IT
Provisioning maintenance	N/A	Yes

UW Shibboleth provides:

- basic [service provider installation guides](#) for the main web server platforms but no guides specific to an application,
- DNS authorized contacts can register their application or use a request process to get UW-IT to register the application for federation via InCommon,
- A basic set of claims is included and customers can request additional custom claims via UW-IT
- customers are in control of 2FA and group restrictions for their application.

Azure AD application capabilities include:

- more than 1,000 pre-integrated application templates to quickly get new applications integrated, with new ones being added regularly,
- any UW Azure AD user can register an application, including the ability to enable federated access and configure custom claims,
- customers can request a rich set of Conditional Access controls for their application via UW-IT,
- application user provisioning via SCIM can be requested via UW-IT with customers in control of ongoing maintenance,
- customers have access to sign in logs for their application

Azure AD represents a step forward in simplifying application on-boarding, additional delegated management, automatically provisioning application users, and easily getting access to sign-in logs and analysis. Access to sign in logs enables customers to troubleshoot without UW-IT assistance. The additional levels of delegation should result in support cost-savings for UW-IT as customers are able to do more without UW-IT assistance.

## External identity support

UW Shibboleth leverages multilateral SAML federation to provide the ability for users external to the UW the ability to access UW applications. This means that organizations with an identity provider that supports this capability can opt into sharing their application metadata with a larger federation of organizations. If an organization does not (or is unable to) opt in, they can't gain access. Multilateral SAML federation has significant design issues due to the size of the resulting metadata file. An application must either [support the MDQ protocol or manually](#)

[maintain the selective IdP metadata](#) it wants to enable. Without the MDQ protocol, there is no way for the application to automatically support every IdP in the federation. The MDQ protocol is not widely adopted by applications. Once a federated user is authenticated, it is solely up to the application to make access control decisions.

Azure AD instantiates external users as a guest user in the local Azure AD tenant. This approach provides the ability to centrally apply policies on external users such as lifecycle attestation, conditional access or other risk-based controls. All Azure AD tenants and Microsoft accounts are by default possible external identity providers for UW Azure AD. Additionally, we can add Google, Facebook, or any SAML or WS-Fed identity provider up to a maximum of 1000 additional IdPs. With the widespread adoption of Azure AD<sup>19</sup> by organizations in almost every sector, just the default set provides a much broader coverage than InCommon or even the combined set of all other Research and Education federations worldwide.

Shibboleth via EduGain has access to more than 5K IdPs<sup>20</sup>. Azure AD has access to more than 200K IdPs<sup>21</sup>. UW Azure AD can support social IdPs natively, whereas UW Shibboleth requires a 3rd party gateway service.

The UW has existing applications which rely on the InCommon federation. In most cases, these applications should be able to shift to Azure AD. But for those applications which pose problems, there are several workarounds:

- [Cirrus Identity Bridge](#) is recommended by the Microsoft Identity product team and is the most commonly used solution by university peers with this scenario. Cirrus Identity Bridge can be used to join the UW Azure AD to InCommon and also supports R&S category applications in Azure AD.
- UW Shibboleth can be kept and configured to use Azure AD for authentication via [Shibboleth's native SAML authentication proxy feature](#). A variation of this is to outsource management of UW Shibboleth to Overt Software, who provide their own proxy solution: [Overt Software Shibboleth Azure AD authentication module](#).

All of these workarounds have been successfully used by other universities who have adopted Azure AD as their primary identity provider.

Azure AD has significantly stronger external identity support than Shibboleth, both in terms of breadth and in terms of the business controls enabled.

## Security protections (CARTA & OFD)

UW Shibboleth has limited custom Conditional Access, supporting only group membership or IP address as conditions. Native support for market competitive CARTA or OFD capabilities such as robust Conditional Access is unlikely, because the richer set of data required (such as the trustworthiness of the client device) is not present in Shibboleth--its scope of functionality is too narrow. UW could extend its custom implementation further, but this would come at significant

---

<sup>19</sup> [Over 200K customer organizations use Azure AD with 425 million monthly active users](#)

<sup>20</sup> <https://edugain.org/>

<sup>21</sup> <https://www.microsoft.com/en-us/security/business/identity-access-management/azure-active-directory>



cost. Likewise, it is unlikely Shibboleth will add the risk-based OFD capabilities<sup>22</sup> expected in a modern authentication system.

Azure AD risk-based protections are provided via UW-owned licensing. CARTA capabilities are provided via a rich set of Conditional Access controls. These Conditional Access controls include:

- group membership,
- application,
- sign-in risk (OFD analysis level no/low/medium/high),
- device platform,
- location,
- client application,
- several client device state characteristics including joined and security compliance (typically indicates managed and patched), and
- application specific restrictions

Azure AD OFD capabilities are built on top of 8 trillion daily security signals<sup>23</sup>, including device and user location, device health, recent login history, application factors such as reputation, and hundreds of others. Microsoft's unique position as a leading provider of online services allows these signals to be analyzed by Azure compute resources, informed by a dedicated team of more than 3,500 cybersecurity professionals, including analysts, researchers, responders, engineers, and data scientists. The combination of the collected signals and corresponding analysis has placed Microsoft as the [Gartner 2020 Magic Quadrant leader for Access Control](#) based on the strength of its CARTA and OFD capabilities provided via Azure AD.

Azure AD clearly has exceptional modern security controls, whereas UW Shibboleth does not.

## Costs

Cost is a significant aspect of any solution which helps determine when it is viable or not--and how long it can continue to be viable. It is challenging to compare the costs of two different solutions, when the two solutions don't provide the same capabilities and qualities. There are also different types of cost: monetary cost, opportunity cost, risk and reputational cost, labor cost, and so on. And finally, cost tracking methodologies and measurements across these disciplines are rarely similar enough to allow for equitable comparison. In these cases, estimation has been used to provide a realistic comparison.

For the purposes of this analysis, we'll focus on the aspects that UW-IT budgets for: non-labor costs and labor costs. Where one solution has lower labor costs, we are not actually recommending that fewer people be employed, but instead that "saved labor" can then be used to prioritize other work.

---

<sup>22</sup> Gartner calls this "continuous adaptive risk and trust assessment" or CARTA. See [IAM Leaders Guide to User Authentication](#) (Dec 2020) and [Market Guide for User Authentication](#) (Jun 2020) for how this figures into modern expectations of user authentication.

<sup>23</sup> [Microsoft Digital Defense Report \(September 2020\)](#)

Table 4 shows the annual non-labor costs of the two IdP solutions, based on FY21 budgets. The non-labor costs are not significant.

Table 4 - Annual non-labor costs of IdPs at UW

	UW Shibboleth	UW Azure AD
Security token service servers	\$8,735.60	\$0
Licensing	\$0	\$0 <sup>24</sup>
<b>Total annual non-labor costs</b>	\$8,735.60	\$0

Table 5 shows the estimated labor costs for the two IdP solutions. Many estimates go into these numbers, so confidence in their accuracy is only moderate--review footnotes to understand what is behind them. Regardless of their absolute accuracy, there is a high degree of confidence that their magnitude is in the right ballpark.

Table 5 - Estimated annual labor costs<sup>25</sup> of IdPs at UW

	UW Shibboleth	UW Azure AD
Code development, server maintenance, debugging, release management	\$89,148.00 <sup>26</sup>	\$0
Application integration fulfillment (based on estimated 25 requests/year)	\$74,432.75 <sup>27</sup>	\$39,002.25 <sup>28</sup>
<b>Total annual labor costs</b>		

Developer and engineer time to maintain the two IdP solutions shows a huge contrast. For Azure AD, there are no labor costs to maintain -- Microsoft provides that labor as part of the

<sup>24</sup> Azure AD P2 licensing is provided to students and employees via central funding of the Microsoft 365 A5 license. This cost is required by UW business needs regardless of the choice of UW Shibboleth baseline support and/or preferred IdP. For that reason, the cost represented here is \$0. For Azure AD, the UW only needs to license risk-based capabilities for its core population. Identities sourced in another organization's IdP are outside UW responsibility--just as they are with Shibboleth federation.

<sup>25</sup> All labor costs use the [ITI Consulting rate](#): \$148.58/hour

<sup>26</sup> This represents an estimate of 600 total hours. Data sources are needed to improve this estimate.

<sup>27</sup> 19.5h/integration, 1/5th the average elapsed time established in 'Customer Application Integration Request Fulfillment'. Presumes 25 application integrations per year, the annual average since 2016.

<sup>28</sup> 10.5h/integration, 1/5th the average elapsed time established in 'Customer Application Integration Request Fulfillment'. Presumes 25 application integrations per year, the annual average since 2016.

service. For the UW Shibboleth, there are several releases each year, each requiring multiple team members time to develop, debug, coordinate, and deploy. As in Table 2, Azure AD application integrations take less UW-IT time, and the labor costs here reflect that.

The annual labor costs of UW Shibboleth are significantly higher than UW Azure AD. Table 6 shows another aspect of an identity provider--the costs associated with 2FA. The table shows the current state of UW 2-factor authentication, UW Shibboleth paired with Duo compared to a potential future solution where UW Azure AD is paired with Azure MFA to provide this service. While there are differences in capabilities between Duo and Azure MFA, this comparison tries to be equitable in terms of the capabilities it is comparing. Moving the enterprise 2FA solution to Azure MFA represents a significant cost savings because this capability is included in the Microsoft licensing the UW must purchase to meet other business requirements.

Table 6 - Potential 2FA costs related to IdPs at UW

	UW Shibboleth + Duo	UW Azure AD + Azure MFA
Enterprise 2FA licensing costs	\$120,000	\$0 <sup>29</sup>
Enterprise 2FA telephony costs	\$44,000	\$0 <sup>30</sup>
Enterprise 2FA token costs	\$2,000	\$2,000
<b>Total costs</b>	<b>\$168,000</b>	<b>\$2,000</b>

## Ability to customize

When a compelling business need arises which a product doesn't meet out of the box, the ability to customize is an important quality. The ability to customize the capabilities and experience is also a double edged sword--you incur maintenance costs, increase the risk to stability and security, need to regularly update your user experience to match modern expectations, and need governance regarding what are reasonable business needs that justify customization. Using an out of the box solution, i.e. losing the ability to customize, has the benefits of lower maintenance costs, better stability and security, and so on.

<sup>29</sup> Azure MFA licensing is included in the Microsoft 365 A5 or A3 license which all employees and students receive. This is the same eligibility population for 2FA at the UW. The Microsoft 365 licenses are funded separately, so there is no additional cost.

<sup>30</sup> Azure MFA licensing includes telephony.

Because Shibboleth is open-source, the UW can add its own custom code and fully control the behavior and user experience. With UW Shibboleth, UW-IT has only chosen to exercise the ability to customize where the product doesn't natively meet UW needs and there is a compelling business need. The need to customize is only an issue if the product doesn't meet our needs.

UW Shibboleth has quite a few customizations to meet UW business needs. These include:

- Sign in experience
- automation to pull data from our custom SP registration site into the IdP metadata
- automated claims data query to PDS and GDS
- implementation of ["Auto 2FA", "Conditional 2FA" and "Conditional Access" features](#)
- custom 2FA for Workday--which can't otherwise force reauthentication
- custom claims transforms from existing data
- other customizations?

Azure AD supports the following out of the box abilities:

- Ability to brand the sign in experience using multiple settings
- Ability to add custom attributes to Azure AD and supply values via API
- Support for what UW calls "Auto 2FA", "conditional 2FA", and "Conditional Access" and more via Azure AD Conditional Access
- Support for forced re-authentication via Azure AD Conditional Access Session Sign-in Frequency
- Support for custom claims transformations<sup>31</sup>

Azure AD does not support:

- Claims data source outside Azure AD, such as PDS or GDS
- Full customization of the user sign in experience
- Customization of sign in error messages
- The ability to assert an entityId or customize almost any of the IdP metadata

The last bullet point has been addressed as an issue in other sections, with workarounds such as Cirrus Identity Bridge. The other bullets are either not significant or have workarounds.

## Conclusions

Azure AD has strong support of modern protocols, while Shibboleth lags behind. Azure AD has significantly stronger external identity support than Shibboleth, both in terms of breadth and in terms of the business controls enabled. Azure AD has significantly stronger CARTA and OFD capabilities, reflected via Gartner, while Shibboleth natively has no CARTA or OFD capabilities, UW Shibboleth's CARTA or OFD capabilities are basic and subject to in-house maintenance.

---

<sup>31</sup>Certain kinds of regex replacements on data are not currently possible

Azure AD has a major vendor deeply invested in ensuring its reliability, while the UW has limited resources to invest in this, which must be spread across many competing priorities. Azure AD application integration and delegation features provide customers value more quickly and at a lower cost to UW-IT--in many cases, even the least technically savvy customers only need perform a web search and quickly get to vendor-provided step-by-step documentation telling them exactly how to get integrated, whereas Shibboleth integration generally requires IT.

The significant degree to which the UW can save money (or prioritize other needs) by choosing Azure AD as the enterprise IdP may come as a surprise to some. UW Shibboleth is a customized solution we maintain, whereas Azure AD is a commodity solution which Microsoft requires as a prerequisite for use of other products which are funded through separate licenses. Since our business needs to utilize those other Microsoft products, and Azure AD is positioned to provide for our ongoing IdP needs, the most cost effective solution for the University's ongoing IdP needs is to leverage Azure AD.

In summary, Shibboleth has been a solid "starter" solution for the UW, but it lacks the ability to reasonably provide modern capabilities. The longer we stay with Shibboleth the more significant the overall capability gap will become and the more expensive Shibboleth will become to maintain. In contrast, Azure AD represents a significant opportunity for the UW to realize greater capabilities without investing further resources in custom development of features that the Shibboleth Consortium is unlikely or unable to provide.

It is worth noting that by moving to a vendor provided and hosted solution, the additional benefits and capabilities of Azure AD come at the cost of some loss of control. We can't add customizations, something which our existing IAM developers could add to Shibboleth. But there's a flip-side to that--we also gain the stability and security that a centrally maintained solution provides, with significant gains in our risk management and mitigation capabilities. Arguably, all existing enterprise product choices including Shibboleth should have an exit plan to help mitigate future risk, but unfortunately when we have greater control of the product we tend to view such plans as a lower priority. As the provider of authentication at the UW, UW Shibboleth should have an exit strategy, just as UW Azure AD should if it becomes the preferred identity provider.

## Exit Strategy

Switching from Shibboleth to Azure AD for the preferred enterprise IdP represents a shift from being fully in control of an IdP solution to being dependent on a vendor. If the vendor relaxes their continuity targets, makes capability decisions which don't align with our future needs, or even chooses to abandon their product the UW could be in a very difficult position where we have to act quickly and broadly impact UW business. However we would not be alone in this given the number of other companies and institutions, including Microsoft itself, that rely on Azure AD. Gartner notes that "[banks are becoming increasingly comfortable with using vendor-hosted](#)" for "OFD capability that has traditionally been deployed on-premises". Banks

have a rigorous risk management practice, and they are increasingly turning to commercial solutions.

The fact that there are currently several other strong cloud-based identity providers, such as Okta and Google, in the marketplace is a good thing, and the further fact that many of these identity providers are leveraging the same standards as Azure AD makes coming up with a plan significantly easier. Okta is another commercial product a few universities in recent years have chosen to adopt instead of the typical “home-grown” identity providers that much of the higher education community uses--Shibboleth or Apereo Central Authentication Service (CAS)<sup>32</sup>. Okta would represent a larger price tag to the UW than Azure AD due to licensing costs, as well as needing to build expertise in-house, but an exit plan which took those variables into account would provide some peace of mind. Other companies and universities have moved all their web applications to a different identity provider in a short period of time, so such moves are doable even in a short time period. Of course, a rapid exit is undesirable but in this case the risk is also less likely given the large number of customers depending on Microsoft.

An exit strategy should be a deliverable of any project to change the UW’s preferred IdP.

## Transition scenarios

A strong argument has been made that Shibboleth meets only a subset of the overall UW business needs, while being much more costly. The conclusions reached above strongly suggest UW Azure AD should be the preferred UW identity provider. Here we’ll briefly explore a couple transition issues and other impacts to outline whether there is a reasonable path forward. The topics we’ll explore are:

1. What do we do with UW Shibboleth?
2. How would we go about switching from Duo to Azure MFA?
3. What approaches can we use for existing UW Shibboleth applications?
4. Other implications

### What do we do with UW Shibboleth?

There are three scenarios of significance. In scenario 1, UW Shibboleth continues, but in a reduced role with costs contained. In scenario 2, UW Shibboleth is retired and the UW utilizes Cirrus to extend UW Azure AD to meet the missing capabilities the UW needs. In scenario 3, UW Shibboleth is kept and left in baseline support, but Azure AD becomes the preferred IdP.

#### Scenario 1

Azure AD becomes the preferred UW IdP. We keep Shibboleth as a tactical solution, supporting applications that need the R&S category or otherwise need InCommon federation, or for existing UW Shibboleth applications which need more time before migration. Shibboleth is configured to

---

<sup>32</sup> CAS is both a protocol and identity provider which was originally developed at Yale. See <https://apereo.github.io/cas/6.4.x/index.html> for more info. Pubcookie is another example of a homegrown identity provider, but UW has retired its use.

use Azure AD via [Shibboleth's native SAML authentication proxy feature](#) to unify the user sign in experience and provide the Azure AD security benefits which can be provided in this configuration.

This Shibboleth reconfiguration also eliminates dependence on the u.washington.edu Kerberos realm, which may allow UW-IT to consider retiring it too.

With this scenario, some automated risk-based protections would be available, but only broadly applicable Conditional Access would be possible, since from Azure AD's perspective, it would see UW Shibboleth as a single application and all of the service providers utilizing Shibboleth would be invisible to it.

In this scenario, future customizations of UW Shibboleth are kept to a minimum<sup>33</sup>. Existing Shibboleth service providers (applications) that do not need R&S or InCommon federation are migrated to Azure AD over the course of a 6-12 month project. Note: Of the universities who have moved their preferred IdP to a commercial IdP from Shibboleth, many have chosen this approach.

## Scenario 2

Azure AD becomes the preferred IdP. UW purchases [Cirrus Identity Bridge](#), recommended by the Microsoft Identity product team, to join the UW Azure AD to InCommon and support R&S category applications from Azure AD. Shibboleth is moved to retirement, after a complete migration of existing Shibboleth applications to Azure AD.

## Scenario 3

UW keeps Shibboleth and leaves it in baseline support, but Azure AD becomes the preferred IdP. This maintains the status quo for existing applications, but all new application integrations are directed to Azure AD. Long term, this is the most costly of the 3 scenarios, and puts off the inevitable need to migrate existing applications.

This scenario might make sense if one of the following was considered significant:

- there is a belief the Shibboleth Consortium will rally with a strong set of new capabilities
- the UW felt one of the other commercial identity providers might become more dominant with equivalent low costs for the UW as Azure AD does
- the UW is not ready for the costs or impacts of scenario 2 or 3

This scenario would require the UW to re-assess on some recurring basis when UW Shibboleth should move to tactical or retirement status, and it represents a larger risk especially due to reliability as existing staff skills dwindle.

---

<sup>33</sup> One variation on this scenario is the one University of Dundee took. They outsourced management of their Shibboleth IdP to Overt Software, who provide their own proxy solution: [Overt Software Shibboleth Azure AD authentication module](#). This further minimized their costs to a very predictable number.

NOTE: UW Google Workspaces uses UW Shibboleth currently, but Azure AD provides excellent support for the Google Suite. UW Google Apps is already integrated with Microsoft Log Analytics and Microsoft Cloud App Security, so shifting it to Azure AD would simplify and provide greater value to UW Google Workspaces.

## How to switch from Duo to Azure MFA

This topic is highly dependent on which of the 3 scenarios is chosen.

With scenario #1, Azure MFA can be solely used as soon as UW Shibboleth proxies authentication to Azure AD. At the point we switch to solely using Azure MFA, any Shibboleth application using any of our custom 2FA solutions<sup>34</sup> would lose those. At that point, applications dependent on those features would need to be evaluated to find another solution--of which, the best would be migration to Azure AD. Azure MFA and Duo can continue to coexist indefinitely (with the custom 2FA options at UW Shibboleth), but you then continue to pay for Duo licensing and introduce increased customer support due to multiple 2FA solutions.

With scenario #2, Azure MFA can solely be used as soon as application migration is complete.

With scenario #3, you are unable to lose Duo.

Azure AD has added support for forced re-authentication so applications which have a valid business need for that could be given a Conditional Access policy. Azure AD also supports requiring 2FA on a per-application basis, so any Shibboleth application using the "Auto 2FA" feature can be supported.

## Existing UW Shibboleth applications

Migrating existing UW Shibboleth applications feels like a daunting task even if it is a one-time cost. Shibboleth applications generally require someone with some IT experience to initially setup, so in most cases we can expect a partnership on the customer end which will be able to follow a migration document. As with almost all infrastructure retirement projects, there's a repeatable process involved:

1. Analysis of existing uses
2. Documentation of actions to take, which covers all common use cases
3. Notification to customers, including a deadline
4. Assist customers with problems
5. Review of use
6. Repeat steps #3-6 until done
7. Retire

---

<sup>34</sup> "Auto 2FA" and "Conditional 2FA" features described at <https://wiki.cac.washington.edu/display/infra/Request+Conditional+Access+and+Automatic+or+Conditional+Two-Factor+Authentication>. Also custom forced reAuthN implemented \*only\* for Workday.



UW Shibboleth is fortunate to have an application registry with clear contact information, as well as some indication of the use cases represented by each application's metadata. This can be analyzed to produce migration documentation for common use cases.

In addition to explicit application contact notification, we could also choose to notify application users: for a similar migration project, one university displayed a message on their Shibboleth IdP to the effect of "This application is using an outdated sign-in process that is no longer maintained" to encourage users to pressure application owners to transition to Azure AD.

A project which followed the approach noted above could be a P2 or P3 project, depending on the desired timeframe--a shorter timeframe would make it a P2, while a longer running project could take some concerted initial effort then hum along as a P3 with very little UW-IT IAM effort. Each customer might have to spend a couple hours making the transition, with some IT teams with heavy UW Shibboleth use being more impacted than others.

## Other implications

Any scenario where Azure AD becomes the primary authenticator for UW applications means that the [MI Inactive Users policy](#) has a broader impact and becomes the de facto policy for UW NetIDs. Extending Inactive Users beyond the UW Microsoft Infrastructure to the UW NetID level has been on the UW IAM Roadmap for some time so this isn't necessarily a major obstacle and might help UW IAM take another small step forward before implementing such a policy at a higher level in the UW IAM source systems. Doing this mitigates risks associated with unused accounts, some of which haven't had passwords changed in more than 20 years, and eliminates a major source of compromised accounts that result in spamming/phishing and other nefarious activities, requiring considerable work from the UW CISO to remediate.

A top customer issue with Husky OnNet is the custom authentication integration to UW Shibboleth chosen over the vendor's (F5) out-of-the-box VPN client configuration of Active Directory. Removing Shibboleth would force a reevaluation of overall business needs and presuming AD was chosen, could lead to elimination of other UW VPN services like the MWS VPN.

## Recommendation

For the reasons discussed above, Azure AD should become the preferred UW enterprise IdP. A project to decide between scenarios #1 & 2 should be initiated with a focus on determining a migration strategy for existing uses, followed by a project to implement and migrate existing Shibboleth service providers (applications). Ideally, the first project would also document and publish customer support expectations for the various lifecycle designations in the [Web Authentication Brick](#), so customers and UW-IT can work from the same set of expectations.

# Landing place for thoughts which don't yet have a good place

Put your thoughts here if you don't yet know where they should go. We'll get rid of this section eventually

- Migration of things like
  - Workday
  -
- Multilateral federation resources:
  - [https://spaces.at.internet2.edu/download/attachments/47154101/Multilateral Federation\\_2014-03.pdf](https://spaces.at.internet2.edu/download/attachments/47154101/Multilateral_Federation_2014-03.pdf)
  - Kantara Federation Interoperability working group (multilateral federation) is comatose/dead: <https://kantarainitiative.org/confluence/display/fiwg/Home>
  - <https://blog.cirrusidentity.com/multilateral-federations-and-azure-ad>