Before you Choose AD FS: 5 Considerations in Assessing an SSO Solution

Information and specifications described herein are true at the time of publication and are subject to change without notice.
Table of Contents

Executive Summary ................................................................................................................................................. 3
Introduction .............................................................................................................................................................. 3
Consideration #1: Costs .......................................................................................................................................... 4
Consideration #2: Automation ............................................................................................................................... 5
Consideration #3 Authentication ............................................................................................................................. 6
Consideration #4 Availability ................................................................................................................................ 7
Consideration #5 Security ....................................................................................................................................... 8
Conclusion .............................................................................................................................................................. 10
About SafeNet Trusted Access: The Smart Way to Manage Cloud Access ........................................................ 10
About Gemalto’s SafeNet Identity and Access Management Solutions ............................................................. 10
Appendix ................................................................................................................................................................. 11
References ............................................................................................................................................................. 11

Table of Figures

Table 1 AD FS Hard And Soft Costs ........................................................................................................................ 4
Table 2 AD FS Automation ....................................................................................................................................... 5
Table 3 AD FS Authentication Methods ................................................................................................................... 6
Table 4 AD FS Uptime And Service Levels ............................................................................................................. 7
Table 5 AD FS Security Comparison ....................................................................................................................... 8
Table 6 AD FS Enterprise Self-Assessment Tool: Microsoft AD FS vs. Gemalto SafeNet Trusted Access. .... 11
Executive Summary

As enterprises embrace cloud applications, their IT teams are seeking streamlined methods of centrally defining and enforcing access controls to manage security and compliance in a consistent manner across their cloud and web applications, and services. CISOs need to prevent password fatigue, simplify the life of their end users, and protect their organization, reducing the risk of identity theft with the goal of thwarting data breaches.

There are many factors to consider in how best to achieve these goals when assessing an access management and cloud single sign on solution. These include cost, authentication, automation, availability and security.

One of the available methods of achieving SSO is through Microsoft AD FS (Active Directory Federation Services). This paper will examine these criteria in depth and assess where Gemalto SafeNet Trusted Access can augment or be considered as an alternative to AD FS in order to best meet the business and security outcomes you need to achieve.

Introduction

Most IT ecosystems are based on Microsoft, so when looking to add single sign on, most IT departments consider Microsoft AD FS (Active Directory Federation Services) as a potential solution. At first glance, SSO using Microsoft AD FS would be a practical choice. Seemingly a natural choice for Microsoft IT environments, AD FS can be downloaded free of charge as a toolkit in the Windows Server Operating System/s, and is considered as a convenient first attempt at Single Sign On.

AD FS is a software component in the Microsoft Windows Server Operating system that lets identity information to be shared outside an enterprise’s network. It helps reduce the log on burden for end users by assessing claims rules and providing single sign on to applications or cloud services in an organization.

As an IT professional, you may be considering AD FS as a solution to simplify access to multiple applications. Although available from the Operating System/s of the Windows Server, AD FS integration may not ultimately be sufficient, simple or secure for all your SSO and cloud access management scenarios.

In this white paper we’ll assess Microsoft AD FS in relation to several factors that contribute to the overall efficacy of an access management solution, so that you are better informed about selecting an access management solution that meets your needs.

Before you choose AD FS: 5 Considerations in Assessing an SSO Solution

#1 Cost
When you calculate the total costs of a solution, do you take into account the real hard and soft costs such as licenses, infrastructure, maintenance and consulting?

#2 Automation
What automated workflows, templates and wizards does the prospective solution offer to save you time and effort when setting up and maintaining policies?

#3 Authentication
What assurance levels does your prospective solution offer in terms of multi-factor and contextual authentication methods?

#4 Availability
How does the prospective solution handle failover, redundancy, backup and security patching?

#5 Security
Does the potential solution provide the assurance levels and methods needed to comply with organizational security policies?
**Consideration #1: Costs**

When you calculate the total cost of a solution, do you take into account the real hard and soft costs such as licenses, infrastructure, maintenance and consulting?

Varied investments go into setting up and running an access management solution. Hard costs would be your subscriptions or license fees, ongoing support fee, and on-premises infrastructure that you need to purchase and maintain for initial setup and to ensure high availability and redundancy of your solution. Soft costs are the time and effort required to manage a solution on a daily basis. These include the time and personnel needed for ongoing operations such as security patching, backup, policy configuration and set up, policy updates, and third party application integration. You can also incur costs for IT personnel overtime and/or external consultants and other professional services related to reporting and integration.

Delivery model: Cloud services eliminate costs relating to initial and ongoing infrastructure investments, as well as costs relating to server and software upgrades, OS upgrades and security patching.

Table 1 below will help you assess the costs associated with MS AD FS and Gemalto’s SafeNet Trusted Access.

### Table 1 AD FS Hard and Soft Costs

<table>
<thead>
<tr>
<th>Hard Costs</th>
<th>Microsoft AD FS</th>
<th>SafeNet Trusted Access</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Infrastructure Investment</strong></td>
<td>Minimum of 5 servers needed in order to achieve a redundant environment.</td>
<td>No servers needed. Service is delivered from the cloud in a SaaS model.</td>
</tr>
<tr>
<td><strong>Server Maintenance</strong></td>
<td>Dedicated personnel required for server maintenance and support.</td>
<td>No personnel needed for server maintenance since the service is maintained in the cloud by Gemalto.</td>
</tr>
<tr>
<td><strong>Support Costs</strong></td>
<td>Microsoft license is not included in the basic license.</td>
<td>Support is included with the service subscription so no additional budget allocation is needed.</td>
</tr>
<tr>
<td><strong>Service Availability</strong></td>
<td>IT is responsible for server available and would need to set up a redundant environment consisting of at least 5 servers: 1 AD FS server, 1 AD FS proxy, 2 additional servers for high availability and one DirSync server for connecting Office 365.</td>
<td>Gemalto offers high availability for its service that can translate into no more than 1 hour of unexpected downtime per year.</td>
</tr>
<tr>
<td><strong>Pricing Model</strong></td>
<td>AD FS is available as a toolkit to be downloaded from the Windows Server Operating System and would need to integrate with several additional Microsoft components each of which have separate licensing, delivery and support costs. For example, an organization would have to take into account separate costs for multi-factor authentication. This pricing complexity means that there may be many hidden costs, making it difficult to forecast costs and assess expenditure over time.</td>
<td>SafeNet Trusted Access is offered as a simple subscription service which includes all the components of an advanced access management solution. It offers SSO, a policy engine and integrated multi-factor authentication in a simple and transparent per user per month pricing model which allows you to accurately estimate costs over time.</td>
</tr>
<tr>
<td><strong>Server Maintenance (staff support)</strong></td>
<td>Dedicated personnel are needed to maintain AD FS servers.</td>
<td>Since SafeNet Trusted Access is a cloud service, no dedicated personnel are needed to maintain infrastructure or servers.</td>
</tr>
<tr>
<td><strong>Solution Time to Live</strong></td>
<td>Factors that affect solution time to live include purchasing dedicated hardware, installing OS, setting up servers, installing, configuring and implementing AD FS itself on local infrastructure. This type of set up may accumulate into hours and even days and would also require time allocated to testing.</td>
<td>Setup and configuration time for a basic configuration of SafeNet Trusted Access (2-3 apps protected) ranges between 3-5 hours. A more complex IT environment with numerous app federations would require several hours more.</td>
</tr>
</tbody>
</table>
Consideration #2: Automation
Does the prospective solution offer automated workflows and a UX experience that saves you time and effort on setup and admin tasks?

Ease of use and automated workflows contribute to a user experience that can have a significant impact on how long it takes an IT admin to manage and run an access management solution. The more manual and unfriendly the UI, the more time consuming and complex it’ll be for the solution administrator to set up the service and maintain it. This in turn will reduce the efficacy of your access management solution and add up to additional personnel costs.

Table 2 below summarizes how Microsoft AD FS and SafeNet Trusted Access address ongoing admin tasks.

### Table 2 AD FS Automation

<table>
<thead>
<tr>
<th></th>
<th>Microsoft AD FS</th>
<th>SafeNet Trusted Access</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication</strong></td>
<td>AD FS does not support multifactor authentication natively or provisioning MFA tokens to users. It can be configured to leverage MS Azure MFA, a separate add-on solution offered by Microsoft. This has additional licensing requirements. AD FS also supports third party authenticators like Gemalto.</td>
<td>Users can be automatically provisioned a variety of authentication methods based on group membership. The platform supports a wide range of form factor authentication methods and deploys with your current infrastructure. SafeNet Trusted Access supports OATH and 3rd party tokens and easily scales with your organization.</td>
</tr>
<tr>
<td><strong>SAML</strong></td>
<td>AD FS supports session SSO, persistent SSO and application specific SSO. Claims rules need to be manually defined for each application set up as a relying party trust Core pipeline for policy processing has three phases: authentication, authorization and claim issuance.</td>
<td>By default all applications configured will fall under the Global Policy defined in STA. Additional Access policies can be configured in a matter of minutes on a group, users and app level and will automatically be implemented upon clicking save.</td>
</tr>
</tbody>
</table>

Table 1 AD FS Hard and Soft Costs, continued
Organizations that want to achieve effective risk management for different groups of users and access scenarios should take into account that this can be best achieved through support of broad authentication capabilities which are inherent to the service. This approach is more cost efficient and reduces complexity since it save you from having to purchase, integrate and maintain a separate authentication solution.

Table 3 below summarizes the various authentication methods available in Microsoft AD FS and SafeNet Trusted Access.

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Microsoft AD FS</th>
<th>SafeNet Trusted Access</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication Token Provisioning</strong></td>
<td>AD FS authenticates using Windows credentials.</td>
<td>SafeNet Trusted Access supports numerous authentication methods and allows you to leverage authentication schemes already deployed in your organization.</td>
</tr>
<tr>
<td><strong>Contextual Authentication</strong></td>
<td>No native support</td>
<td>Supported</td>
</tr>
<tr>
<td><strong>Push Authentication</strong></td>
<td>No native support</td>
<td>Supported</td>
</tr>
<tr>
<td><strong>SMS Authentication</strong></td>
<td>No native support</td>
<td>Supported</td>
</tr>
<tr>
<td><strong>OTP Hardware Support</strong></td>
<td>No native support</td>
<td>Supported</td>
</tr>
<tr>
<td><strong>OTP App</strong></td>
<td>No native support</td>
<td>Supported</td>
</tr>
<tr>
<td><strong>Pattern-based authentication</strong></td>
<td>No native support</td>
<td>Supported</td>
</tr>
<tr>
<td><strong>PKI credential support</strong></td>
<td>No native support</td>
<td>Supported**</td>
</tr>
<tr>
<td><strong>FIPS certified authentication</strong></td>
<td>No native support</td>
<td>Supported</td>
</tr>
<tr>
<td><strong>Kerberos Authentication</strong></td>
<td>Natively Supported</td>
<td>Supported (Kerberos)**</td>
</tr>
<tr>
<td><strong>3rd Party authenticators</strong></td>
<td>Supported*</td>
<td>Supported</td>
</tr>
</tbody>
</table>

*NOTE: Gemalto is listed as a trusted provider of third-party additional authentication methods - **As of 2018 H2
Consideration #4 Availability
How does the prospective solution handle failover, redundancy, backup and security patching?

The need for users in your organization to access applications at any time is a fundamental part of an enterprise's ability to function smoothly. Hence, the ability to maintain a high level of service and ensure service uptime is an important aspect to consider when evaluating a potential solution.

An efficient service would support a multi-tenant/multi-tier architecture, ensuring data separation between tenants of the service. For example, using a redundant architecture service ensures high availability and disaster recovery. A prospective solution should strongly protect end user data to guaranty its privacy.

Uptime

Does the access management solution you are considering offer any assurances regarding uptime? Since your users rely on this type of solution to access the very resources they need to do their job, this is an important aspect to consider when evaluating a potential solution.

Access management service providers, who deliver identity-as-a-service (IDaaS), state the amount of uptime they expect their solution to provide in a service level agreement, or SLA.

Since IDaaS providers, such as Gemalto's SafeNet Trusted Access, employ dedicated teams that ensure redundancy and failover via multiple datacenters, and given that their backend operations team is accountable for ensuring the solution is available around the clock, these cloud-based access management services may offer a higher uptime than your own in-house team.

In contrast, on-premises solutions may offer lower uptime due to potential operational issues, expensive and time-consuming updates, maintenance and on-site troubleshooting.

When considering this aspect, note that AD FS requires two additional servers for high availability on top of the AD FS server and AD FS proxy, and one DirSync server for connecting to Office 365.

Table 4 below assesses the factors needed to achieve acceptable uptime and service levels with AD FS and SafeNet Trusted Access.

<table>
<thead>
<tr>
<th></th>
<th>Microsoft AD FS</th>
<th>SafeNet Trusted Access</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Redundancy and</strong></td>
<td>On-premises solutions may offer lower uptime due to potential operational issues, expensive and time-consuming updates, maintenance and on-site troubleshooting. Redundancy and fail over are not guaranteed unless organization sets up a high availability environment.</td>
<td>Offered as a cloud service which means that there is no need to account for high availability, load balancing and BC/DR.</td>
</tr>
<tr>
<td><strong>Fail Over</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Solution Back Up</strong></td>
<td>Requires AD FS Rapid Restore tool which needs PowerShell knowledge.</td>
<td>Cloud-based backup and restore are handled by Gemalto.</td>
</tr>
<tr>
<td><strong>Security Patching</strong></td>
<td>May encounter downtime during patching, dependent on configuration and infrastructure.</td>
<td>Security patches are applied on a scheduled basis during maintenance windows and cause no interruption of services.</td>
</tr>
</tbody>
</table>
Consideration #5 Security

Does the potential solution meet the security policies your organization needs to minimize breaches and identity theft?

Microsoft AD FS provides basic single sign on capabilities for cloud and web-based apps. Single sign on (SSO) provides the capability to authenticate once with a static password, and be subsequently and automatically authenticated when accessing various resources. SSO enhances end user convenience since it eliminates the need to separately log in and authenticate to individual applications and systems.

While basic SSO simplifies the user experience, it also poses a security risk: If the credentials [user name and password] used universally to log into all apps is stolen or compromised – all apps will ultimately be at risk.

The way of overcoming this challenge is to incorporate SSO into a broader access management scheme, which allows organizations to set access policies for different scenarios. In this way, organizations can mitigate the risk of a ‘buffet style’ SSO, while still offering a convenient login experience to their users.

This ability to manage risk through access management policies depends on policy configuration capabilities, conditional access, the range of authentication methods supported and SSO session management.

Table 5 below provides an overview of MS AD FS and SafeNet Trusted Access.

<table>
<thead>
<tr>
<th>SSO</th>
<th>Microsoft AD FS</th>
<th>SafeNet Trusted Access</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Supports several types of SSO, session SSO, Persistent SSO (PSSO), Application Specific SSO. SSO native forms based authentication, certificate based authentication or integrated windows authentication [password] Third Party Authentication methods can be integrated but this requires additional connectors.</td>
<td>Supports session SSO through Global Policies which can be set to initiate SSO requiring a single, or multiple factors of authentication – supporting universal authentication options. The duration of an SSO session can be determined depending on the desired level of risk management.</td>
</tr>
<tr>
<td>Conditional Access</td>
<td>Access control in AD FS is implemented with issuance authorization claim rules that are used to issue a permit or deny claims that will determine whether a user or a group of users will be allowed to access AD FS-secured resources or not. Authorization rules can only be set on relying party trusts. This can be configured to consider multiple factors, including user, device, location, and authentication data.</td>
<td>Setting policies with risk-based scenarios enables organizations to easily augment security around protected resources. By applying scenario-based access policies, you can determine access controls for privileged user groups, sensitive apps, by evaluating specific contextual conditions including user, device, application, location, and network source. Further you have the ability to deny access if certain risk criteria are met, or require step-up authentication to provide a higher level of user assurance.</td>
</tr>
<tr>
<td>Session Management</td>
<td>For session-based SSO, the lifetime is up to 8 hours and is configurable. Sessions are secured using an authentication cookie and stored in the browser and are terminated when the browser is closed. For PSSO the lifetime is from 24 hours to 7 days and is configurable (*note that PSSO requires that the device be registered using DRS and written back to AD DS) Sessions are secured by writing cookies to WPJ. The lifetime of a default security token for a claims-based authentication deployment using AD FS is 60 minutes.</td>
<td>The lifetime of the SSO session is configurable up to 8 hours and can evaluate risk conditions against applications or groups of users to require additional authentication factors or deny access passed on the parameters set during the lifetime of the SSO session.</td>
</tr>
<tr>
<td>Session Encryption</td>
<td>AD FS acts as a Security Token Service (STS) when leveraging native authentication methods6.</td>
<td>SSO sessions are secured using JSON web tokens [JWT].</td>
</tr>
</tbody>
</table>
Before you Choose AD FS: 5 Considerations in Assessing an SSO Solution - White Paper

Support for MFA with AD FS requires third party integrations. Otherwise AD FS will use form-based or windows based authentication. AD FS, when it receives an authentication request, first determines whether or not there is an SSO context (such as a cookie) and then, if MFA is required (such as if the request is coming in from outside) it will assess whether or not the SSO context contains MFA. If not, MFA is prompted.

Policies can be configured to enforce the use of only Multi-factor authentication once per session or for each access attempt, this is configurable. Additionally policies can be designed to require more than one form of authentication for additional layers of security and identity validation. When a resource is accessed the access policies are evaluated and it is determined if there is an SSO context in place and as per the policy assess if the SSO context satisfies the rule or not. If not, then MFA is required.

Server security is at the discretion of the organization as this deployment is hosted on premise. Most organizations do not expose their AD FS servers to the DMZ, but they will be required to allow firewall exceptions to extend protection to applications that are web-based or external to an organizations infrastructure. It is recommended to follow best practices around securing the deployment.

Organization is responsible for maintaining and managing certificates in the environment.

Servers are hosted in a secure cloud environment which is in compliance to ISO 27001:2013 standards and SOC-2 guidelines.


Network security is at the discretion of the organization as this deployment is hosted on premise. It is recommended to follow best practices to protect against Man in the Middle attacks.

- All communication is encrypted using AES 256 encryption
- Neutral network connection to major ISPs
- Web facing services are protected by web application firewalls and all traffic goes over SSL (443)
- Run time servers are behind redundant firewalls.

## Table 5 AD FS Security Comparison, continued

<table>
<thead>
<tr>
<th>Multi-Factor Authentication (MFA) Enforcement</th>
<th>Microsoft AD FS</th>
<th>SafeNet Trusted Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for MFA with AD FS requires third party integrations. Otherwise AD FS will use form-based or windows based authentication. AD FS, when it receives an authentication request, first determines whether or not there is an SSO context (such as a cookie) and then, if MFA is required (such as if the request is coming in from outside) it will assess whether or not the SSO context contains MFA. If not, MFA is prompted.</td>
<td>Policies can be configured to enforce the use of only Multi-factor authentication once per session or for each access attempt, this is configurable. Additionally policies can be designed to require more than one form of authentication for additional layers of security and identity validation. When a resource is accessed the access policies are evaluated and it is determined if there is an SSO context in place and as per the policy assess if the SSO context satisfies the rule or not. If not, then MFA is required.</td>
<td></td>
</tr>
</tbody>
</table>
Conclusion
Organizations may face several factors regarding cloud application adoption, now and in the future: compliancy, growing number of cloud apps, appropriate risk management and the overall operational costs involved in setting up and managing cloud access.

By clearly defining business and security goals, and assessing them against the factors outlined in this paper, CISO, IT managers and risk management professionals have the power to make an informed decision about the Access Management solution that best meets their current and future needs.

Gemalto’s SafeNet Trusted Access can do more to help organizations build on existing deployments, including AD FS. Not only can the SafeNet Trusted Access solution add a layer of strong authentication, easily apply risk based access controls and protect an entire IT environment – it also enables organizations to protect more apps at no additional cost beyond the all-inclusive user subscription price.

To assess your organization’s needs, refer to Table 6: Enterprise Self-Assessment Tool, in the Appendix of this paper.

About SafeNet Trusted Access: The Smart Way to Manage Cloud Access
SafeNet Trusted Access is an intelligent access management service that allows customers to enforce the perfect balance between user convenience and secure access to all apps.

SafeNet Trusted Access offers flexible access management through a simple to use policy engine that gives customers real-time control over the ability to enforce policies at the individual user, group or application level. The policy engine supports a broad range of authentication methods, including ones already deployed, allowing organizations to leverage their current investments and use them to secure cloud and web-based services.

By combining SSO, risk-based policies and universal authentication methods, SafeNet Trusted Access gives organizations the power and flexibility to secure access to all apps, simplify the login experience, and effectively manage risk.

Key Benefits
Effective risk management
Address all use cases with flexible policies to accommodate diverse user groups, assurance levels and compliance considerations.

Balance convenience and security
Match authentication requirements to risk levels and create your own balance between user convenience and security, through a single, intuitive console. Create, manage and maintain the policies you need in real-time.

Universal authentication
Leverage the authentication scheme already deployed in your organization or use the broadest range of authentication methods and form factors supported out of the box.

About Gemalto’s SafeNet Identity and Access Management Solutions
Gemalto’s industry-leading Identity and Access Management solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy-based SSO and universal authentication methods, enterprises can effectively manage risk, maintain regulatory compliance, gain visibility into all access events and simplify the login experience for their users.

To learn more about access management from Gemalto, visit https://safenet.gemalto.com/access-management.
Appendix

Table 6: Enterprise Self-Assessment Tool

This tool will help your organization assess your priorities regarding basic SSO with AD FS vs. holistic SSO with SafeNet Trusted Access. In addition to the questions on page one of this paper, you may want to take into account the total cost of your operations, range of native authentication options, reporting, scenario-based options, conditional access, trust elevation and scope of third-party application integrations. You may also want to assess the benefits of a vendor whose core expertise is security and prefer an agnostic solution that provides segregated protection from the core resources it protects.

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Low Priority</th>
<th>Medium Priority</th>
<th>High Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

What do your results mean?

If you checked most of your answers in the Medium Priority and High Priority columns, then Gemalto’s SafeNet Trusted Access may be the best solution to address your enterprise’s SSO and Access Management needs.

References