onelogin

WHITEPAPER

Total Cost of Ownership Overview ADFS vs OneLogin

150 Spear Street, Suite 1400 San Francisco, CA 94105 877 979 0411 onelogin onelogin.com

Are you really going to double down on machines, software and professional services to extend Active Directory (AD)?

Executive Summary

Are you planning to federate Active Directory to Azure AD in order to secure your cloud apps? If so, the two TCO scenarios that follow show that this will cost you between $132k and $940k over 3 years (of course, your costs will vary depending on your specific inputs).

Why is the TCO of Active Directory Federation Services(ADFS) and Azure AD so high? Integrating your cloud apps with Active Directory using Microsoft's native solution set requires the setup and maintenance of a complex, dedicated infrastructure. Your cloud vendor SLAs are meaningless unless IT can maintain a highly available ADFS deployment – which is often predicated on load balancing multiple sets of servers, deploying SQL Server, a storage solution, and a global traffic management solution.

In contrast, OneLogin's zero-config, one-minute Active Directory Connector (ADC) installs via a simple click-through process that deploys the ADC as a Windows service, and the same ADC also enables Desktop SSO (Integrated Windows Authentication), further minimizing network complexity.

When combined with OneLogin, Active Directory takes on powerful new capabilities to control real-time access to SaaS, web, desktop, and mobile applications– and there's no need to embark on a complex Active Directory integration project for each new app. From single domain environments to complex directory infrastructures, OneLogin makes it easy to extend Active Directory to the Cloud.

CALCULATING THE TOTAL COST OF OWNERSHIP OF FEDERATING ACTIVE DIRECTORY TO AZURE AD AND YOUR CLOUD APPS

The AD TCO models below consider the hardware, software, cloud services consumption, and professional services costs that one might expect for both single datacenter and multiple datacenter architectures when federating Active Directory to Azure AD using ADFS.

AD TCO MODEL FOR HIGHLY AVAILABLE SINGLE DATACENTER ARCHITECTURE

Scenario A as shown below

- Users = 1,000
- Azure AD Premium = No
- Virtualized Infrastructure = No

NPV of Total AD Cost at 4% Interest = -$132,000

AD Total Cost of Ownership by Year

- Year 1 $84k
- Year 2 $24k
- Year 3 $24k
- 3 Year = $132k

AD TCO MODEL FOR HIGHLY AVAILABLE MULTIPLE DATACENTER ARCHITECTURE

Scenario B as shown below

- Users = 5,000
- Azure AD Premium = Yes
- Dedicated SQL Servers = Yes
- Virtualized Infrastructure = Yes

NPV of AD TCO at 4% Interest = -$940,000

AD Total Cost of Ownership by year

- Year 1 $410k
- Year 2 $270k
- Year 3 $270k
- 3 Year = $950k

Hardware	Quantity	Unit Cost	Total
ADFS Federation Server	4	$5,000	$20,000
ADFS Web Application Proxy	4	$5,000	$20,000
Dedicated SQL Servers	-	$7,500	-
Network Load Balancer	4	$6,990	$27,960
Dirsync Server	1	$5,000	$5,000
Hardware Subtotal			**$72,960**
Software	**Quantity**	**Unit Cost**	**Total**
SQL Server Standard	-	$3,570	-
Windows Server Standard	9	$882	$7,938
Software Subtotal			**$7,938**
Cloud Services Consumption	**Quantity**	**Unit Cost**	**Total**
Azure Active Directory Premium	5,000	-	-
Azure Multi–Factor Authentication	5,000	$24	$120,000
Cloud Services Consumption Subtotal			**$120,000**
Professional Services	**Days**	**Unit Cost**	**Total**
Design & Planning	3	$225	$5,400
Implementation	8	$225	$14,400
Testing/Pilot	10	$225	$18,000
Rollout	10	$225	$18,000
Training	3	$225	$5,400
Professional Services Subtotal	**34**		**$55,800**
	Year 1	**Year 2**	**Year 3**
Capital Costs	$136,698	-	-
Recurring Costs	$120,000	$120,000	$120,000
Total	**$256,698**	**$120,000**	**$120,000**

NOTE TO REQUEST A CUSTOMIZED TCO ANALYSIS, PLEASE SEND AN EMAIL TO SALES@ONELOGIN.COM

GENERAL INPUTS AND ASSUMPTIONS

General Inputs

The default inputs (which we can further customize for you) are shown below. For comparison, we've also included a column that shows the corresponding input values for OneLogin's solution.

Item	Input Value ADFS	Input Value OneLogin
Consulting Rate	$225	$0. No professional services
Server (Small)	$5,000	$0. No servers
Server (Large)	$7,500	$0. No servers
Network Load Balancer (Small)	$1,990	No additional hardware. HA Mode included free in Enterprise Plan and above
Network Load Balancer (Large)	$6,990	See above
Windows Server Standard	$882	$0. Not requried
Azure MFA Cost (Annualized)	$24	$0. Free MFA with all plans
Azure AD Premium User Cost (Annualized)	$54	Volume discounts start at just 100 users

General Assumptions for the AD FS Scenarios

In both AD FS scenarios, we assume that server costs are eliminated with a virtualized infrastructure. Why? Companies that virtualize infrastructure have already licensed Windows Server Datacenter for unlimited virtual guest instances. So, they often treat virtual infrastructure as a sunk cost, and virtual machines are "free" until they realize they are out of space.

If you are really mature in your processes and know your internal costs to operate a virtual machine then we can override the formulas in the spreadsheet as appropriate. For both scenarios, we assume that Microsoft MFA Server is co-located on ADFS servers.

Load balancers are popular in Microsoft environment, so you already have load balancers on your network then we can adjust those numbers accordingly.

All costs are quoted at full retail costs--but no one pays full retail prices for Microsoft software, so we can adjust those accordingly based on discount assumptions.

Professional services and training are considered upfront costs, with the assumption that once everything is up and running with your first two to five cloud apps, then you would be able to maintain and add new apps to the system on your own. Professional Services assumes no travel for out-of-state consultants.

How OneLogin Cuts Out the Costs and Complexity of Federating Active Directory to Your Cloud Apps

For most enterprises, Microsoft Active Directory (AD) is the official user directory for managing access to key business applications. Microsoft's Active Directory Federation Services (ADFS) can bridge AD with cloud applications and services, but its complexity hinders IT's ability to keep pace with the "now" mentality of business. ADFS also lacks key functionality like user provisioning and compliance reporting.

When combined with OneLogin, Active Directory takes on powerful new capabilities to control real-time access to SaaS, web, desktop, and mobile applications– and there's no need to embark on a complex Active Directory integration project for each new app. From single domain environments to complex directory infrastructures, OneLogin makes it easy to extend Active Directory to the Cloud. Here's how:

HIGH-PERFORMANCE ARCHITECTURE KEEPS EVERYTHING IN SYNC

OneLogin's Active Directory Connector (ADC) deploys in minutes, yet its superior architecture scales to support dozens of domains, tens of thousands of OUs (Organizational Units), and millions of users and security groups. The (ADC) installs as a simple Windows service that subscribes to change notifications instead of scanning the full directory. Updates appear in milliseconds and there's no need for a dedicated server.

While others claim "real-time", OneLogin offers true real-time bi-directional synchronization and authentication across Active Directory domains, trees and forests. A faster sync means increased security and greater peace of mind.

ZERO-CONFIG, ONE-MINUTE ACTIVE DIRECTORY INTEGRATION

OneLogin's Active Directory Connector installs via a simple click-through process that deploys the ADC as a Windows service– so you don't have to worry about manual restarts after a Windows reboot. No firewall changes are required as all communication is performed via an outbound SSL connection. To sync users, simply check off which OUs you'd like to import, and rest easy knowing that all passwords remain on-premises.

The outbound connection to OneLogin is also used to authenticate users against Active Directory from OneLogin's login page. This can be combined with PKI certificates, IP address restrictions and two-factor authentication.

INTEGRATED DESKTOP SINGLE SIGN-ON

OneLogin leverages Microsoft's Integrated Windows Authentication (IWA) to authenticate users to OneLogin when they are logged into their office computer. When employees are on the corporate network and signed in with their Windows credentials, they can use Desktop SSO (from a PC or Mac) to get one-click access to their web applications. There's no need for additional usernames or passwords, just like on-prem apps. To minimize network complexity, the same OneLogin ADC also enables Desktop SSO.

PRECISE USER PROVISIONING OF APPS AND SECURITY POLICIES

OneLogin performs real-time user provisioning, importing, matching and de-duplication as well as Just In Time Provisioning into the application user store. OneLogin also provides user provisioning with entitlements into a growing list of SaaS applications. For example, you can not only create a user in Salesforce, but actually restrict their access to that of a Standard User profile–all based on Active Directory attribute mappings and organizatinal structure, and business rules that you define in OneLogin.

OneLogin provides flexibility around Active Directory Groups while also adding in Roles as an additional administrative capability. For example, you can use any attribute in Active Directory as an indicator for assigning roles (groups of applications), group memberships (policies), as well as perform bulk operations (like activating users).

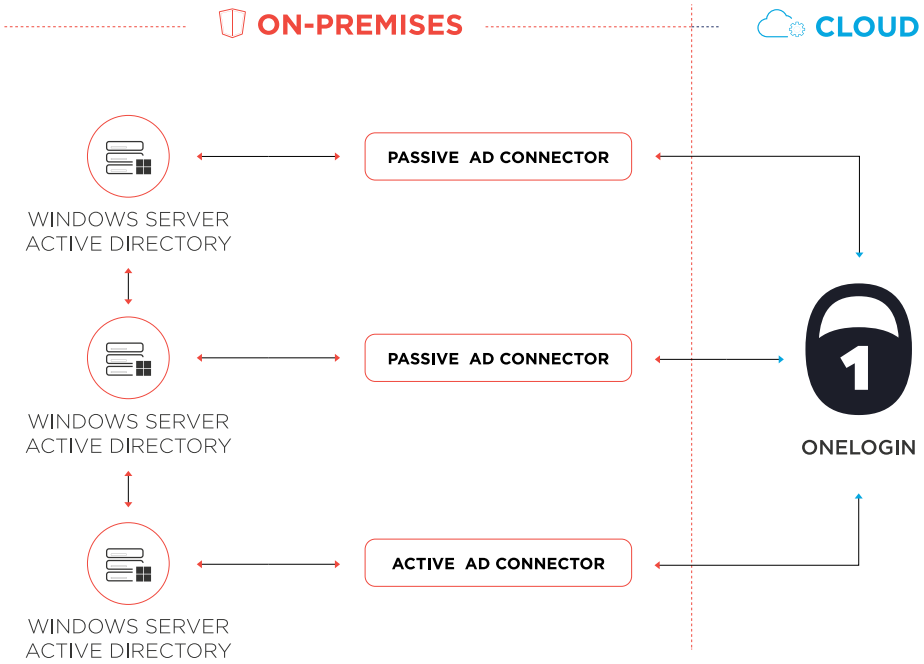
REAL-TIME DEPROVISIONING AND COMPLIANCE REPORTING

Real-time Active Directory integration is useful when people join an organization, or gain responsibilities, but absolutely critical when they leave or lose responsibilities. With OneLogin, you can instantly disable app access for leavers in real time by removing them from Active Directory, and there's no need to check back later.

Having a Windows service listening to events on your Active Directory (instead of periodic scans, or on-demand checks during an authentication event) ensures that the instant someone is terminated, the change is propagated through to OneLogin and connected services. This is critical when popular services like Google Apps allow back-door access through protocols like IMAP. Unless the user is immediately disabled, unwarranted access can occur. Best of all, all sign-in activity is recorded in a centralized audit trail, which simplifies compliance and enables cross-application analysis.

HIGH AVAILABILITY MODE

The ADC has a High Availability feature that allows customers to set multiple connectors to run in parallel. If a customer server hosting the primary ADC goes down, one of the secondary connectors is promoted to primary, automatically. Administrators can also manually promote ADCs or bring them online or offline from OneLogin.



GLOBAL INFRASTRUCTURE, EU HOSTING OPTION, AND A 99.99% UPTIME GUARANTEE

OneLogin supports complex directory infrastructures for some of the most demanding public companies in the world. No planned downtime means redundancy at every tier: DNS, data centers, application servers and database servers. OneLogin also provides customers with an EU hosting option that meets European data residency and compliance standards.

WORLDWIDE DATA CENTERS

UNIFY MULTIPLE DIRECTORIES

Most applications are only able to integrate with one directory per customer, but OneLogin overcomes this limitation. OneLogin can import users from an Active Directory domain in conjunction with other directories such as LDAP-based directories like OpenDirectory, or SaaS directories like Google Apps and Workday. OneLogin can combine mixed directory types and present them as a unified meta-directory to other applications for federation via SAML.

For example, you might have employees in Active Directory, customers in LDAP, and contractors in OneLogin. Use OneLogin to present them as a unified directory to your company's web applications.

SELF SERVICE PASSWORD RESET

OneLogin's self-service password reset functionality synchronizes password changes across Active Directory, the OneLogin portal, as well those web applications secured with OneLogin. When a user's password expires in Active Directory, they will be prompted to change their password the next time they log into OneLogin.

Users can also proactively change their Active Directory password through OneLogin by selecting Change Password in their OneLogin portal. When a user changes their password through their portal, OneLogin will keep the password synchronized with AD and any cloud applications where password provisioning is active.

Appendix

REFERENCE ARCHITECTURES FOR HIGHLY AVAILABLE ADFS

BACKGROUND

Microsoft Azure Active Directory is not a turnkey out of the box solution for the most common scenarios. In order to marry Azure AD with existing identities in an on-premises Active Directory Domain Services (AD DS) forest, organizations must first deploy the Azure AD Directory Synchronization appliance. To leverage single sign-on capabilities whereby user passwords are stored in the on-premises AD DS forest, Active Directory Federation Services (ADFS) must also be configured and deployed.

Federation with Azure AD is the elephant lurking in the back of the room. While deploying Azure AD Directory Synchronization is generally a trivial exercise, establishing and maintaining a highly available ADFS infrastructure is not trivial. Simply put, the service level agreements (SLAs) that cloud hosted services offer are a moot point if the ADFS infrastructure that brokers logins to these applications and services isn't running at the same service level (or higher).

DELIVERING HIGHLY AVAILABLE SERVICE WITH AD FS

Highly available ADFS is primarily predicated on load balancing multiple sets of servers. Figure 2 shows a typical highly available ADFS deployment in a single datacenter. For organizations with advanced requirements, SQL Server may be required, and ADFS will probably be deployed in multiple geographically dispersed datacenters with the addition of a global traffic management solution to manage requests across datacenters.

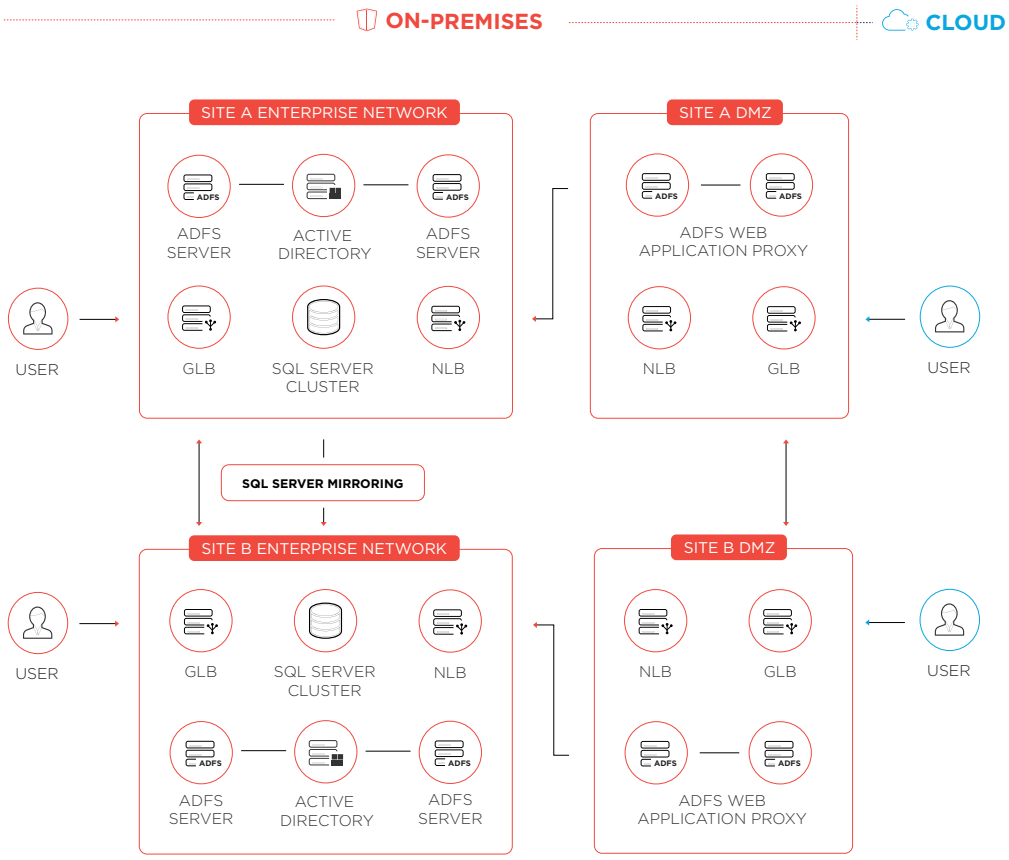


FIGURE 2 HIGHLY AVAILABLE SINGLE DATACENTER AD FS REFERENCE ARCHITECTURE

These dependencies add several layers of complexity to ADFS, and require collaboration across multiple teams. For example, in many enterprises, load balancers and global traffic management solutions (e.g. F5 Global Traffic Managers or Cisco Global Site Selectors) are generally managed by dedicated networking teams. SQL Server may require support from a database administration team, and the addition of SQL Server clustering will add a dependency on a storage management team as well.

Figure 3 shows one approach to highly available ADFS across multiple datacenters with the addition of SQL Server to take advantage of advanced ADFS features like token replay detection and SAML artifact resolution.

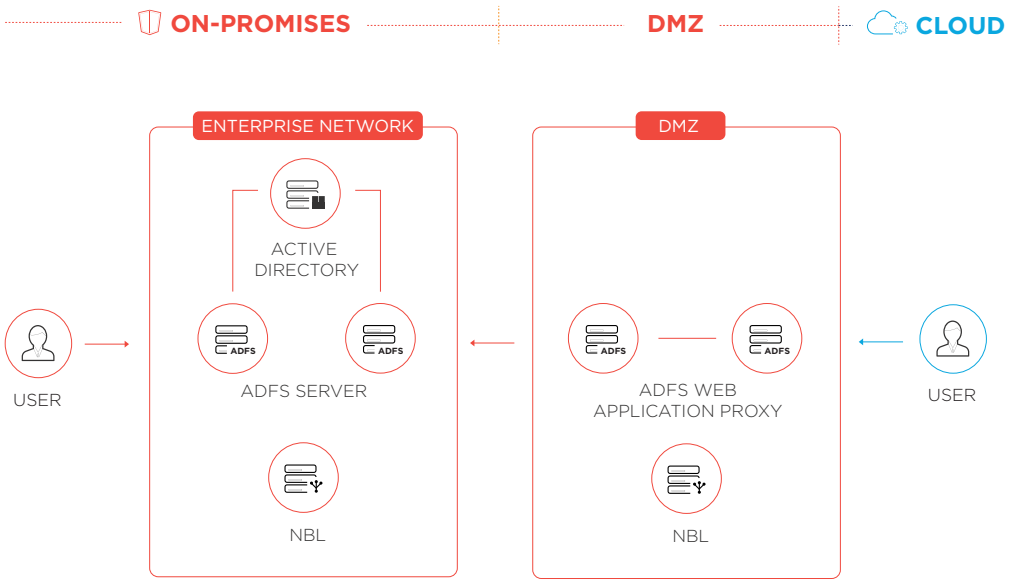


FIGURE 3 HIGHLY AVAILABLE MULTIPLE DATACENTER AD FS REFERENCE ARCHITECTURE

Bringing all of these teams together to deliver on a service level is a goal that large enterprises achieve at varying levels, but the coordination and complexity always exists. Smaller organizations that need to deliver the same level of availability that a solution such as the one in Figure 2 shows may not have the same number of teams or individuals involved, but they probably will also not have the same level of technical expertise across all functions available.

Comparing Microsoft Azure Active Directory with OneLogin

The table below highlights the capabilities of the Microsoft platform for integrating with a cloud application portfolio as well as capabilities from OneLogin.

	Microsoft Azure Active Directory	Microsoft Azure Active Directory Premium Edition	OneLogin
Application Support			
Application Catalog	1,000[1]	1,000[1]	7,400[1]
Office 365 Availability	✓	✓	✓
Hybrid Exchange Online	✓	✓	✓
Desktop Applications	✓	✓	✓
Integrate third–party SAML applications	✓	✓	✓
Integrate on–premises SAML applications	✓	✓	✓
Password Vaulting for form–based apps	✓	✓	✓
SAML Toolkits for custom apps			✓
Add your own form–based apps			✓
Directory Integration			
Active Directory directory synchronization	✓	✓	✓
High Availability	ADFS	ADFS	✓
Multi–Forest AD directory synchronization	FIM 2010 R2[2]	FIM 2010 R2[2]	✓
Generic LDAP directory synchronization	FIM 2010 R2[3]	FIM 2010 R2[3]	✓
Google directory synchronization			✓
Workday directory synchronization			✓
SAML Service Provder Interface	✓	✓	✓
Real–time bi–directional directory sync			✓
Unify mixed directory types (meta–directory)	FIM 2010 R2	FIM 2010 R2	✓
Manageability			
REST API	✓	✓	✓
VPN Integration		MFA Server	✓
RADIUS Support		MFA Server	✓
Group Based Access Control to Applications		✓	✓

[1] As of June 1, 2015

[2] Microsoft's Azure AD Directory Synchronization appliance only supports a single forest. Microsoft Makes an Azure AD connector available for Forefront Identity Manager 2010 R2 to enable multi–forest synchronization scenarios.

[3] The Azure AD connector for Forefront Identity Manager 2010 R2 can be used to synchronize generic LDAP directories

	Microsoft Azure Active Directory	Microsoft Azure Active Directory Premium Edition	OneLogin
Manageability (Continued)			
Provisioning with Entitlements[4]	✓	✓	✓
Just In Time Provisioning			✓
Delegated Authentication[5]			✓
Admin "Assume User" view			✓
Rules–based AD attribute mappings[6]			✓
End User Experience			
Desktop SSO to Cloud Apps (IWA)	ADFS	ADFS	✓
Active Directory Single–Sign–On	ADFS	ADFS	✓
Mobile SSO App Portal	✓	✓	✓
Self–Service Password Reset	✓	✓	✓
Branded Sign–On Page		✓	✓
Embeddable SSP App Portal (e.g. in an intranet)			✓
External Users SSO (customers and partners)			✓
Self–Registration Profiles			✓
Personal Apps			✓
Secure Notes			✓
Federated Search			✓
Security and Compliance			
User Password Synchronization	✓	✓	✓
Create custom password policies	✓	✓	✓
Combine AD Auth. w/ PKI Certificates	AD FS	AD FS	✓
Combine AD Auth. w/ IP address restrications	AD FS	AD FS	✓
Advanced Security Reporting		✓	✓
Role–based Access Control to Applications		✓	✓
Multi–Factor Authentication (MFA) Phone App		✓	✓
MFA via SMS		✓	✓
MFA Policies			✓
Pre–Integrated with 3rd Party MFA			✓
Choice of US or EU data residency			✓

ABOUT ONELOGIN

OneLogin is the innovator in enterprise identity management and provides the industry's fastest, easiest and most secure solution for managing internal and external users across all devices and applications.

Considered a "Major Player" in IAM by IDC, and Ranked #1 in Network World Magazine's review of SSO tools, OneLogin's cloud identity managment platform provides secure single sign–on, multi–factor authentication, integration with common directory infrastructures such as Active Directory and LDAP, user provisioning and more. OneLogin is SAML–enabled and pre–integrated with more than 4,000 applications commonly used by today's enterprises.

onelogin

150 Spear Street, Suite 1400 San Francisco, CA 94105 877 979 0411 onelogin onelogin.com