

CASE STUDY · NOVEMBER 2021

From AD FS to Pass-Through Authentication: A College Identity Project

An anonymized project case study exploring Massive IT's November 2021 plan to replace a public community college's federated Microsoft 365 sign-in with pass-through authentication and Seamless SSO.



Conceptual illustration only; not the customer's production environment.

Project snapshot

Detail	Documented scope
Customer	A public community college (customer anonymized)
Project date	November 2021
Starting point	Federated Microsoft 365 authentication using Active Directory Federation Services (AD FS)
Target model	Azure Active Directory pass-through authentication (PTA) with Seamless Single Sign-on
Delivery approach	Plan, implement, test, manage, and establish monitoring and logging

This project case study is based on the November 15, 2021 statement of work. It describes the documented design and planned delivery, not independently verified completion or measured results. Customer identities and contact details have been omitted.

Executive summary

A public community college wanted to simplify its federated authentication infrastructure and improve the resilience of access to Microsoft 365. Its existing model relied on on-premises AD FS infrastructure, with the project brief highlighting concern about authentication availability during a power outage at the primary location.

Massive IT's statement of work defined a transition to Azure Active Directory managed authentication using pass-through authentication and Seamless SSO. The plan addressed more than a change in sign-in settings: it brought together agent placement, domain conversion, device preparation, compatibility review, user communications, validation, rollback, and ongoing support responsibilities.

Azure Active Directory is now known as Microsoft Entra ID. Historical product names are retained here to accurately describe the November 2021 project.

The challenge: simplify identity without losing control

Federation introduced dependencies on AD FS servers, certificates, load balancing, and local infrastructure. Replacing it required careful review of how people and applications authenticated, which federation customizations remained necessary, and how support teams would respond to a failed transition.

– **Infrastructure dependency:** The college sought a smaller authentication footprint and less reliance on its federation farm.

- **Continuity of access:** Primary-site availability was a planning concern, not a problem solved merely by changing a cloud setting.
- **Existing directory policies:** Password validation needed to continue against on-premises Active Directory.
- **User experience:** Domain-joined devices on the college network needed an appropriate single sign-on experience, while external devices still needed a tested sign-in path.
- **Safe transition:** Domain conversion required a maintenance window, compatibility checks, communication, and a credible rollback plan.

The proposed architecture

The target design replaced federated sign-in with cloud-managed sign-in backed by lightweight PTA agents. Those agents would validate credentials against on-premises Active Directory and communicate with Azure Active Directory over outbound connections, without exposing an inbound authentication listener to the internet.

Agent number and placement were planning decisions. The SOW called for placing agents close to domain controllers and considering multiple agents for availability and capacity. The final deployed server count and locations are not established by the supplied document.

PTA still depends on reachable authentication agents, domain controllers, and connectivity. A primary-site outage would only be mitigated if those dependencies remained available elsewhere. The SOW excluded deployment of an additional domain controller at a secondary site, so this case study does not claim site-outage immunity.

Seamless SSO would complement PTA for eligible domain-joined devices connected to the organizational network. Device Group Policy preparation and the required directory configuration were included in the plan; this was not a promise of password-free access from every device or location.

Massive IT's planned delivery

1. Review the federation environment and prerequisites

The plan began with review of AD FS usage, current federation settings, application dependencies, and customizations. Existing Azure AD Connect deployment, suitable agent servers, required outbound connectivity, administrative access, and modern authentication readiness were prerequisites.

2. Prepare devices and authentication agents

Device preparation included Group Policy changes for Seamless SSO. Agent planning addressed proximity to domain controllers, connectivity, registration, and availability. Preparing the client experience before switching sign-in methods was intended to reduce avoidable prompts during the transition.

3. Convert the sign-in model

The implementation scope included changing sign-in from federated to managed through Azure AD Connect, converting federated domains, installing PTA agents, and enabling Seamless SSO. The SOW documented alternative conversion procedures, with the applicable method dependent on the existing federation configuration.

4. Validate before retiring federation

The testing plan covered on-network Seamless SSO with and without a domain hint, external-device PTA sign-in, and relevant client scenarios. AD FS and its Microsoft 365 relying-party trust were to remain available until user and client authentication had been validated. Other applications using AD FS also needed review before any wider decommissioning.

5. Establish rollback and support readiness

Maintenance-window planning accounted for transitional authentication behavior. The plan included reverting to federation if a major issue could not be resolved promptly, communicating the change to users, and preparing support teams to troubleshoot PTA and Seamless SSO.

Validation and operational handoff

Workstream	Planned validation or responsibility
On-network access	Test eligible domain-joined devices with and without a domain hint
External access	Test cloud sign-in and PTA validation from devices outside the organizational network
Application dependencies	Confirm relevant clients and any remaining AD FS relying parties
Agent health	Monitor agent availability, authentication statistics, errors, and event logs
SSO maintenance	Plan recurring Kerberos key rollover for the Seamless SSO computer account
Audit visibility	Define sign-in log review, retention requirements, and any export needs
Recovery	Document when to roll back and how to restore federation

Scope boundaries

The engagement did not include a new Azure AD Connect deployment, a secondary-site domain controller, migration of custom AD FS claims rules to Conditional Access, MFA configuration, user license assignment, detailed AD FS backup and restoration procedures, or Hybrid Azure AD join. Password Hash Synchronization was discussed as a separate authentication option, not established as a deployed fallback in this project.

These boundaries matter: reviewing security capabilities or licensing considerations is not the same as implementing them. The case study therefore does not claim that MFA, Conditional Access policies, or a password-hash fallback were delivered.

Intended business value

- **Simpler operations:** Reduce the federation infrastructure and certificate-management burden associated with Microsoft 365 authentication.
- **More predictable user access:** Prepare and test an appropriate sign-in experience across supported network and device scenarios.
- **Controlled migration risk:** Pair the authentication change with explicit validation, rollback, and communications.
- **Clearer ownership:** Define support, monitoring, auditing, and key-maintenance responsibilities alongside implementation.

These are the objectives of the documented design, not measured outcomes. The supplied SOW does not establish actual downtime, cost savings, final acceptance, or completed deployment.

Why this project matters

An identity migration is an operational change as much as a technical one. This engagement's documented approach connected federation review, authentication architecture, endpoint preparation, testing, recovery, and long-term support rather than treating domain conversion as the entire project.

Modern identity choices should be reassessed against current Microsoft guidance, licensing, application requirements, and resilience needs. This historical case study is not a current deployment runbook.

Plan your identity modernization

Massive IT helps organizations assess Microsoft identity dependencies and plan migrations with clear scope, validation, and support ownership. Schedule a consultation or call (813) 518-5454.