

Single Sign-On and Active Directory Integration

This document describes ways that Project Hosts can integrate a customer's online solution with a corporate Active Directory in order to enable single sign-on for users and to simplify user administration. The costs quoted here are in addition to any other hosting costs associated with a deployment. The four methods described here are

- Windows Credential Manager (default)
- Argon (a Project Hosts solution)
- Federation Services

Definitions:

A **Single Sign-On (SSO)** solution allows users to access online applications without having to enter a username and password each time.

Active Directory Integration means that when a customer's corporate Active Directory is changed, corresponding changes are made to the online solution. For example if a new user is added to the customer's Active Directory, an account for that user will be created in the online solution. Similarly, if a user is disabled from the customer's Active Directory, access for that user will automatically be removed from the online solution. Also, mappings can be set up to determine for example if a user is in a particular department in a customer's Active Directory, then that user should be in a certain security group or given a particular role in the online solution.

Feature	Credential Manager	ARGON	Federation Services
SSO access to SharePoint and SharePoint apps: Project Web Access, Excel Services, SQL Reporting Services, etc.)	X	X	X
SSO access to other online apps (PH user portal, CRM, etc.)	X	X	
Access to Project Server from Project Professional on user's PC	X	X*	X
Ability to open Excel Services Reports in Excel on a user's PC	X	X*	
People-picker functionality (e.g. for Issues, Risks, alerts, etc.)	X	X	X**
SSO for Remote Desktop (e.g. for developing reports)	X	X	
Users can access apps from anywhere	X	X	X***
Automated provisioning of new users		X	
Active Directory Integration		X	X
Code must be deployed by customer		X	X
Setup fee	\$0	\$1,000	\$1,000
Monthly fee	\$0	\$250	\$250

*Using ARGON, access from PC-based applications like Project Pro or Excel requires an additional logon using a Project Hosts-provided password. This can be saved in Credential Manager to avoid future logins

** With ADFS, People picker usage (e.g. assigning someone to an Issue) requires a couple of extra steps

*** With ADFS, access is limited to a company's corporate IP range. Users can connect from anywhere if they first remote into their corporate network.

Windows Credential Manager

Universal single sign-on after first login.

Description:

There are a number of single sign-on solutions that enable access to browser-based applications. These solutions use technologies like Microsoft Live ID, Active Directory Federation Services, SAML, or even Project Hosts' own ARGON solution. They are great as long as all you want to do is to access web applications via your browser. But they typically do not work for access using Excel (connecting to Excel Services), and some do not work for Project Professional connecting to Project Server, or from other local applications running on your PC.

A single sign-on solution that works not only for browsers but also for all Office applications is Windows Credential Manager, an encrypted store built into each user's Windows PC. More than 90% of our customers have chosen this solution. The solution does require us to issue a username and password for each user, but the first time a user logs in, he or she can simply check the box "Remember my password" to store them in the Credential manager on their PC. As long as users have trusted our site in their browsers, they never have to log in again. They can connect using a browser, they can view an Excel Services report online then open it in Excel on their PC, they can launch Project Professional on their PC and have it automatically connect in the background to Project Server – it provides a completely seamless experience with no additional logins necessary. None of the other single sign-on solutions mentioned above work for all of these access methods.

User requirement:

Users must have a Windows PC (XP or higher) and the ability to trust a site.

Customer IT requirement:

None.

Project Hosts cost and timeline:

\$0. This is the default authentication method.

ARGON Single Sign-On with PH Sync AD Integration

Best web-based single-sign on solution for large organizations.

Description:

Project Hosts' Authorization Reconciliation Gateway Online (ARGON) system is a single sign-on solution for hosted web applications that use Windows Integrated Authentication.

Single sign-on is achieved by running the ARGON Validation Service on a corporate intranet site and the ARGON Authorization Service on the hosted web application server. The ARGON Validation Service

validates that the user is a valid corporate user and then uses a Pre-Shared Security Key to securely communicate the Authorization Key to the ARGON Authorization Service. Once the Client is authorized, the ARGON Authorization Service automatically logs the Client in to the Target Application using Windows Integrated Authentication. Once the Client is authenticated, all future requests proceed directly between the Client and the Target Application imposing no addition overhead on the application traffic. The security of the ARGON Authorization Service is maintained by validating the Pre-Shared Security Key from the ARGON Validation Service and also by validating the Client IP address range. Please see the diagram below.

The Client experience is completely seamless. The client clicks on a link on the corporate intranet site and is automatically directed into the hosted application without any prompts. The entire Client authentication for the hosted application is handled behind the scenes by the ARGON Seamless Application Logon system.

In addition to the ARGON Validation Service, the customer could provide an intranet based landing page for the application that could provide customer specific guidance for the application users.

The ARGON system can be configured for auto-enrollment. When a user who is validated against the corporate intranet accesses the ARGON system and it not in the Target Active Directory, the ARGON system can be configured to automatically provision the user in the Target Active Directory and application.

ARGON is usually deployed together with PH Sync code that can provide Active Directory Integration as defined at the beginning of this white paper.

User requirement:

Each user must have a browser that has Javascript enabled. This is true for most browsers out-of-the box.

Customer IT requirement:

The ARGON Validation Service must be deployed on a corporate Intranet Web Server that is authenticated and available to the Client. It is currently available as an .asp page that can be provided to the customer, but equivalent code could be developed by the customer on any platform. For the PH Sync AD Integration, customer must also provide a domain account to log into the customer domain, periodically read allowed AD information, then call a secure web service to pass that information to the Project Hosts domain.

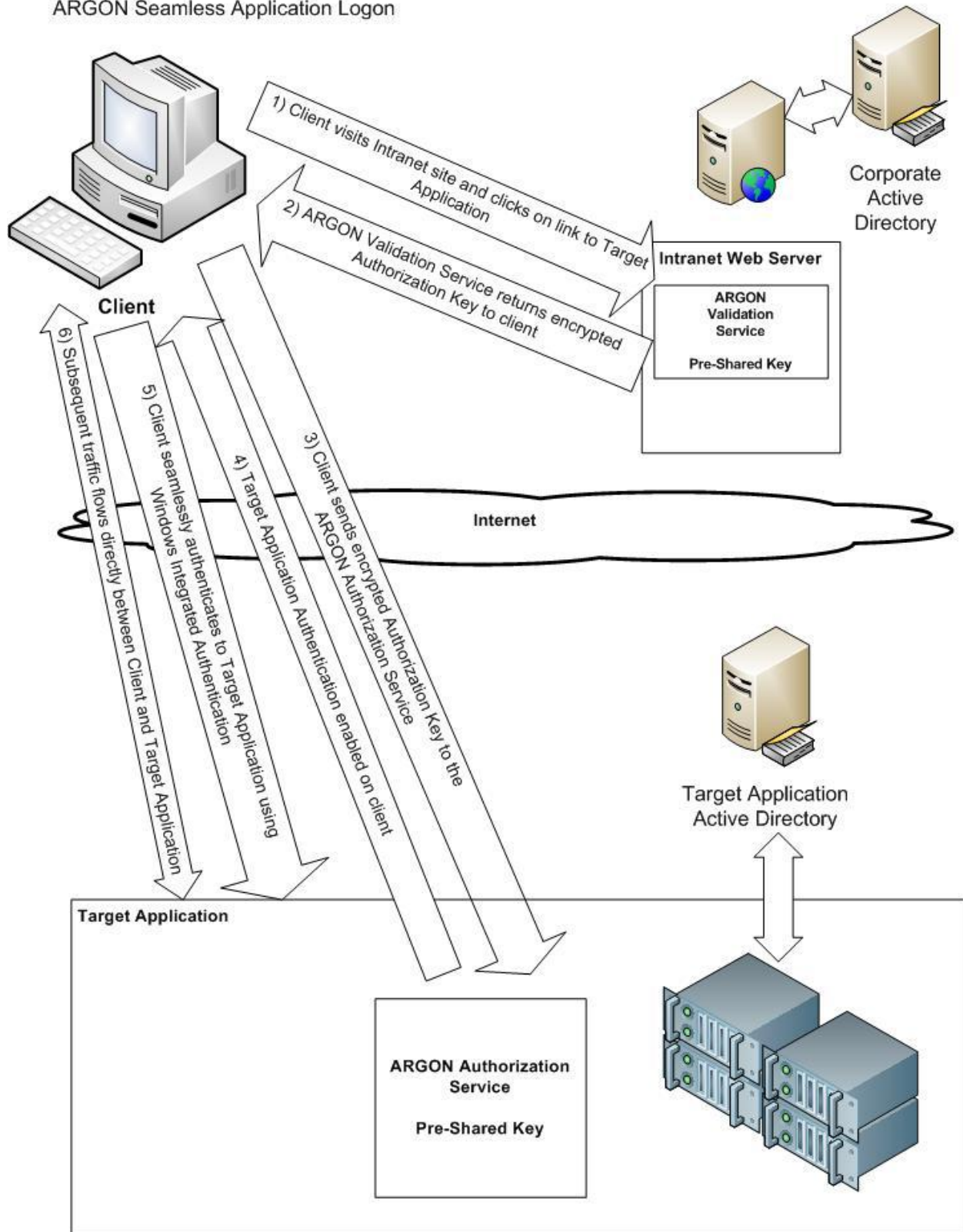
Project Hosts cost and timeline:

\$1,000 setup and \$250/month.

2 weeks required for setup assuming timely cooperation from customer IT.



ARGON Seamless Application Logon



Active Directory Federation Services

Microsoft's solution for Single Sign-On to SharePoint.

Description:

Active Directory Federation Services (ADFS) is a good SSO option for customers that only need to connect to SharePoint and who only want to deploy Microsoft code (ADFS 2.0) in their data center.

The other solutions described in this white paper use an Active Directory at Project Hosts in order to authenticate users. ADFS is different: it uses SharePoint to authenticate users. This means that each new user must first be set up with an account in SharePoint (and in each SharePoint application) before they can login. It also means that ADFS only provides Single Sign-On to SharePoint itself or to SharePoint applications like Project Server, Excel Services, or SQL Reporting Services in SharePoint mode.

In order to accommodate the SharePoint authentication, SharePoint must be set for Anonymous access. To maintain security while providing Anonymous access, Project Hosts requires IP blocking – users are only allowed access if they are coming from a limited IP range specified by the customer. This requires users that are traveling to first VPN into their corporate network then access applications from there.

ADFS does not provide any way to access the following applications:

- Non-SharePoint web applications (e.g. CRM, Project Hosts user portal, etc.)
- Dashboard Designer
- SQL Reporting Services in Native Mode (it does provide access in SharePoint mode)
- Remote Desktop
- Analysis Services over https
- People picker doesn't function (e.g. for use in Issues, Risks, and alerts)

One consequence of the last two above is that there is no way using only ADFS to create or edit an Excel Services report. To do so would require either access to Excel on a Remote Desktop in the Project Hosts data center or else the ability to open Excel on a user's local PC and connect to an Analysis Services data source over https. Since neither of these is available, if a customer wants to use ADFS and also create Excel Services reports, they will have to create separate accounts in the Project Hosts Active Directory for Excel Services report developers to allow them to access Remote Desktop or Analysis Services. These accounts can use the Windows Credential Manager version of SSO described earlier.

Customer IT requirement:

Customer must configure an ADFS 2.0 federation server that is accessible by HTTPS from the internet and provide a copy of the Token Signing Certificate. Each user must add the ADFS Sign-in URL and the URL for their hosted SharePoint applications into the Local Intranet Zone of their IE browser.

More information about ADFS configurations can be found at the site:

<http://connect.microsoft.com/site642/Downloads/DownloadDetails.aspx?DownloadID=25359>

Project Hosts cost and timeline:

\$1,000 setup and \$250/month.

1 week required for setup from the time that customer's ADFS has been configured.