

ADFS RFP Requirements

Definitions

Container – A segregated environment for delivering a cloud based solution to a customer or group of customers.

Federated SSO – Allows a user's existing identity to be used when accessing applications external to the organization without disclosing authentication credentials to the third party.

Identity Provider – One of two roles in a federation. Software that leverages cryptography and federated protocols such as SAML and Open ID to provide a security token that vouches for a user's identity to a Service Provider.

Service Provider – The second role in a federation that provides application functionality using the token issued by the Identity Provider as a basis for identity.

Cloud Solution Authentication and Deployment Scenarios

When assessing a Cloud vendor solution it is helpful to understand what authentication scenarios are supported for a deployment. Doing so will help ensure that key business requirements can be met for user access. Authentication options can also influence the decision to deploy a single tenant or multi-tenant solution. As a result, it is recommended that prospective cloud vendors be asked which of the following scenarios are approved for accessing their solution based on project business requirements:

- 1. Single tenant container, single Federated Identity Provider –**
This is the Enterprise Active Directory Only option accessing a shared application for the entire EAD. Access to the Cloud solution for an organization leverages Federated Single-sign-on by integrating with a single customer Identity Provider. All users that access the solution are authenticated and issued a token by the single Identity Provider.
- 2. Single tenant container, multiple Federated Identity Providers –**
This option is for EAD and other non-joined agencies accessing a shared application. Users from multiple customer organizations access a single tenant container using Federated Single-sign-on. To support more than one organization accessing the same cloud solution the vendor supports the implementation of more than one federation for access to the tenant container.
- 3. Single tenant container, local accounts –**
This option does not require ADFS and uses local accounts in the cloud solution sharing a single shared application. Federated Single-sign-on is not used for accessing the Cloud solution. User accounts are local to the application and provisioned and maintained by the Cloud provider.
- 4. Single tenant container, local accounts and one or more Federated Identity Providers –**
This option allows for multiple ADFS or other federation products, local accounts managed in the application with all users accessing a single shared application. The

cloud provider supports a mixed mode where some accounts are local to the application and federated SSO is also supported either for one or more organizations.

5. Multiple tenant containers with organization specific configurations for authentication –

This option described an application where there is no shared application and each agency would use their own ADFS or federation solution to access their own version of the application. No data would be shared between tenants. Each organization is treated as an independent entity which requires the configuration of multiple tenant containers by the cloud provider. This allows for custom solutions based on specific agency business requirements and technical capabilities such as the presence of an established Identity Provider function.

Suggested Requirements

The following two requirements would be sufficient if the application is only to be used by **Enterprise Active Directory joined agencies only:**

- Solution must support federated single sign-on (SSO) using Active Directory Federation Services 2.0 and above.
- ADFS claims can be used for roles-based authentication within the application. If not supported, describe how different levels of access to the application are controlled.

(If claims are supported for RBAC, this would allow local control of access through Active Directory ACLS. This could be a mandatory or desirable depending on customer requirements.)

For an enterprise application that will be accessed by agencies/entities that are not joined to the EAD, an additional requirement would be:

Single Container for the Enterprise (Shared Data and Application by all entities):

Vendor must support:

- Multiple identity providers; and/or
- Multiple identity providers and local accounts managed with the application simultaneously; and/or
- A single identity provider and local accounts managed within the application simultaneously.

Multiple Containers for the Enterprise (No shared data between agencies, each has their own version of the application and own ADFS installation or other federation solution):

Requirements would be dependent on the use of the application by each agency and would depend on the individual agency requirements and their federation solution. (See No. 5 above).