Active Directory Federation Services (AD FS) is a software component developed by Microsoft that can be installed on Windows Server operating systems to provide users with single sign-on access to systems and applications located across organizational boundaries. It uses a claims-based access control authorization model to maintain application security and implement federated identity.[1]

Claims-based authentication is the process of authenticating a user based on a set of claims about its identity contained in a trusted token. Such a token is often issued and signed by an entity that is able to authenticate the user by other means, and that is trusted by the entity doing the claims-based authentication.

In AD FS, identity federation is established between two organizations by establishing trust between two security realms. A federation server on one side (the Accounts side) authenticates the user through the standard means in Active Directory Domain Services and then issues a token containing a series of claims about the user, including its identity. On the other side, the Resources side, another federation server validates the token and issues another token for the local servers to accept the claimed identity. This allows a system to provide controlled access to its resources or services to a user that belongs to another security realm without requiring the user to authenticate directly to the system and without the two systems sharing a database of user identities or passwords.

In practice this approach is typically perceived by the user as follows:

- The user logs into their local PC (as they typically would when commencing work in the morning)
- The user needs to obtain information on a partner company's extranet website - for example to obtain pricing or product details
- The user navigates to the partner company extranet site - for example: http://example.com
- The partner website now does not require any password to be typed in - instead, the user credentials are passed to the partner extranet site using AD FS
- The user is now logged into the partner website and can interact with the website 'logged in'

AD FS integrates with Active Directory Domain Services, using it as an identity provider. AD FS can interact with other WS-* and SAML 2.0 compliant federation services as federation partners.