safewhere

Safewhere*Identify

Identify and AD FS 2.0

A comparison

safewhere

Contents

safewhere

Safewhere Identify and AD FS 2.0: Competitive summary

Often, it is not an either-or situation when it comes to Safewhere Identify and AD FS 2.0.

In many cases where Microsoft architecture is involved, the design often ends up including AD FS 2.0 as well as Safewhere Identify since Safewhere Identify usually steps in when AD FS 2.0 just does not cut it. AD FS 2.0, on the other hand, comes virtually free of charge when used beside the pre-existing Active Directory on the intranet, when all your users are already covered by CAL licenses.

So while it might not be an either-or in regard to AD FS 2.0 and Safewhere Identify, it still makes a lot of sense to compare the two products with each other so as to gain a better understanding of just how much more it becomes possible with Safewhere Identify compared to AD FS 2.0.

The highlights

Safewhere Identify	**Microsoft AD FS 2.0**
Includes a full-fledged user and role database and supports a varied set of out-of-the-box authentication options, including: Facebook, Google, Twitter, LinkedIn, OpenID, Live ID, Active Directory, LDAP-based directories, a generic provider for external authentication, username/password for the built-in user directory as well as One Time Password, mobile device-based login, SAML 2.0, and WS-Federation. You're able to combine any two login providers into a single login. Plus, you are free to add more login providers as you see fit due to Identify's open and modular login provider architecture.	Is only able to authenticate users that are stored in Active Directory, either based on username/password or certificates that are issued from a CA, which is configured as an Enterprise CA. Also, it is not a bit user-friendly if the authentication fails, and there are no options for improving on this. AD FS 2.0 is not able to combine logins (that is, you are either logged in or not). You might want to take note that Safewhere has developed an add-on solution (ADFSXLogin) that adds two-factor login and password reset functionality to AD FS 2.0 as well as improved user-friendliness in terms of the authentication and home realm discovery, among other things.
Can be placed on the intranet as well as in the DMZ, depending upon the needs at hand. The AD login provider includes a proxy component that ensures that you are free to choose where to place Identify.	Is built to be placed on the intranet. AD FS 2.0 includes a special version (the AD FS 2.0 proxy) that operates as a proxy for use in the DMZ.
Allows you to control which logins are available for accessing a particular application.	There is only very few options for controlling the logins available to each application.
You can implement multiple Identity Providers (and/or Service Providers) on the same server since Identify is built on a multitenant architecture. Each of these services (and user stores) is totally isolated from one another.	You can only have one Identity Provider (and/or Service Provider) per server.
Non-redundant installation: 1 or 2 servers, depending upon whether or not you wish to host the SQL database on the same server as Identify.	Non-redundant installation: 3 or 4 servers, depending upon whether you wish to host the SQL database on the AD FS 2.0 server since best practice always calls for two AD DCs at the

Redundant installation: 2 or 4 servers.	minimum. Redundant installation: 4 or 6 servers per installation.
Controlled and operated from a full-fledged web-based UI. It is possible to delegate the authority for creation and administration based on object types and/or objects as needed. It is even possible to create separate objects that are only accessible to a certain part of the organization.	Administered through an MMC-based console, which is supplemented by PowerShell scripts. The MMC console only provides access to a part of the AD FS 2.0 functionality. The rest is only accessible via PowerShell. The administrator(s) has access to all settings. Safewhere has developed an application (ADFS2WebAdmin) that put a web-based interface on AD FS 2.0.
Can be adapted to virtually any and all needs. Identify comes with a lot of options out of the box, including support for different pages based on web browser and device type as well as customization of text and error pages. In the next release of Safewhere Identify, which is scheduled in June 2013, we will also be adding some very sophisticated features for automatic home realm detection features that allow you to configure Identify to automatically choose the user's home realm based on source IP address, the providers that they are already logged in at etc.	It usually takes a fair deal of work to get AD FS 2.0 to work with the more special-use cases. Also, in a fair deal of cases, it is simply not possible to wring the needed functionality out of AD FS 2.0. So you are faced with changing the specifications to be in line with what is available on AD FS 2.0 or being left between a rock and a hard place.
Allows you to process and transform claims in virtually whatever way you see fit, by using the built-in filtering functionality. You are able to add claims and claims transformations using the modules for SQL, Active Directory, and external claims transformations (a DLL) as well as developing your own specialized custom transformation modules. You might also want to take note of the fact that Identify, by default, will do a pass-through of all claims, which eases the setup in many cases (especially compared to AD FS 2.0, which calls for you to define claim rules for everything you wish to pass-through). Also, Identify includes a sensitivity option that can be set on claims, which ensures that the content of the claims will not be logged. This feature will come in very handy when you need to meet such kind of security policies. Identify is able to generate exactly the same tokens, no matter which login is used, if that is what you are after.	Allows you to control the processing and transformation of claims using the built-in claims rule language. You are able to add claims and claims transformations based on information in Active Directory (and other LDAP-compatible directories) and SQL as well as by developing your own specialized custom attribute store. The claims rule language only allows control of the claims. That is, you do not have any control over how the token is generated. Also, there are some limitations on what claims can be produced by AD FS 2.0.
Allows for more end points to be added along the way so that we can cater for the needs and situations that may arise going forward. A set of Web Service end points is forthcoming in the next release of Safewhere Identify, which is	Comes with a variety of end points that include Web Services. The setup and configuration of the AD FS 2.0 end points (which each comprises an endpoint type, a client credential type, and a security mode) are fixed, and there is no option

scheduled in June 2013.	for modifications.
Includes very rigorous logging and a base set of reports for the logging. Can also log to the security event log.	Includes limited logging functionality, which is spread out over two logs (a separate AD FS 2.0 log and the security event log).

Safewhere also markets a SAML 2.0 protocol implementation for .Net applications, which is derived from Safewhere Identify. SAML 2.0 for WIF is the only SAML 2.0 protocol implementation that is built for WIF.

Safewhere has developed a number of add-on products for AD FS 2.0, which strives to remedy some of the product's limitations. The add-ons include a group mapping attribute store, an AD user mapping attribute store, an extended logging feature, ADFS2WebAdmin (a web-based front-end for managing AD FS 2.0), and ADFSXLogin (password reset, two-factor login, and a number of other additions to the login functionality). We also have a number of enhancements to Active Directory that are applicable for many federation scenarios.

When to pick which solution?

We have outlined our general principles for when to pick which solution below. Please bear in mind that no rule is without exception.

Intranet	**Internet/Extranet**
AD FS 2.0 will usually be the inexpensive choice since it is a server role, which is covered by the Windows Server license. Thus, if you can do with the functionality offered by AD FS 2.0, it will usually be the most cost-effective choice when Active Directory is already employed for all users and the organization has purchased CAL licenses for all of them.	**AD FS 2.0** might be a good choice for Internet/extranet, provided that the current strategy calls for creating an externally facing Active Directory (which will have to store all external users that are not logging in from parties that already carry their own federation service). Please note that AD FS 2.0 demands that you purchase either an External Connector license for all the Windows servers involved or CAL licenses for each and every user (CAL licenses are usually not an option when dealing with externally facing solutions).
Identify is a very interesting alternative to AD FS 2.0 if the organization wishes to allow access for a number of users that are not covered by existing CAL licenses. This could be their own users (for instance, blue-collar users) as well as external users.	**Identify** is uniquely well-positioned for use on the internet/extranet due to its features and flexibility in terms of login providers, claims transformations, login page features etc. Also, the very fact that Identify was designed as a web-based solution plays well in that direction. Also, the server footprint of Identify is quite a deal lower than what is the case for AD FS 2.0, which means that it is usually highly competitive with AD FS 2.0 for extranet use.
Identify is your only choice if you employ a directory service other than Active Directory since AD FS 2.0 is closely intertwined with AD FS 2.0. Also, in many cases, Identify proves a very	**Identify** is uniquely positioned for uses that call for more than one federation service due to its multitenant architecture. Identify looks even better if the design at hand calls for full separation between the federation

attractive choice due to its calling for a reduced number of servers.	services since AD FS 2.0 will not be able to meet that need without the creation of fully separate Active Directories.
Identify includes a lot of additional functionality (and flexibilities) compared to AD FS 2.0, which might prove to make it the only choice for many of the more advanced uses. Even for the simple case, Identify will prove an advantage to AD FS 2.0 since it almost per definition will bring a smaller, simpler setup and calls for less customization.	