IBISTIC TECHNOLOGIES

ADFS integration with Ibistic Commerce Platform

A walkthrough of the feature and basic configuration

Magnus Akselvoll

19/02/2014

Change log

26/06/2012 – Initial document

19/02/2014 – Added paragraph “2.5 Certificate rollover”

ADFS provides a way to access Ibistic Commerce Platform authenticating against the local Active Directory. This document details out those features and provides a basic walk through for set-up.

1 Feature description

1.1 Overview

The web application for Ibistic Commerce Platform (ICP) is usually accessed through usernames and password. To help IT departments simplify their environments and lower support cost, Ibistic also offers access to the web site through Active Directory Federation Services 2.0, from how on referred to as ADFS.

After ADFS has been set up for an enterprise, customers access ICP through a custom link to Ibistic's servers. This link will redirect the browser to the customer's internal ADFS server. This server will, explicitly or implicitly, authenticate the user against the domain and post a signed message back to ICP with information regarding the user. The user's browser will be automatically redirected back to Ibistic and the platform will trust the information received from the ADFS server and let the user in to his or her account without any further authentication.

For the users this can be set up to be completely transparent. They click a link on e.g. a company intranet and automatically get into their Ibistic account without any password or other information required.

1.2 Details and requirements

While ADFS adds another way of authenticating to Ibistic Invoice System it does not invalidate usernames and passwords. If you wish to remove the options for users to set a password and thus get conventional access to ICP, please contact Ibistic as a separate implementation project may be required for this.

The ADFS integration is only supported on ADFS version 2.0 and has only been tested on Windows Server 2008 R2. Ibistic offers neither expertise nor assistance on ADFS deployment and configuration; this must be covered by the customer's IT department. This document will outline a basic setup of ADFS 2.0 with Ibistic though, to serve as a starting point for proper enterprise roll out of ADFS.

To access ICP through ADFS, the customer's users must access through a custom URL that will be provided by Ibistic. There is no button or other mechanism on the standard Ibistic login page to log on with ADFS. The ADFS server must be available through HTTPS to the user, not to Ibistic, in order to log in. Since ADFS servers are usually placed on the internal business network and protected behind firewalls, this usually means that roaming users must be connected through VPN if they want to access ICP through ADFS.

Finally, ADFS integration must be enabled or disabled to an entire security domain, i.e. the entire enterprise. Ibistic offers no granularity that enables customers to use this only for specific users or departments. Any detailed control of this should be done through ADFS.

The technical requirements are as follows:

1. Windows 2008 R2 environment with ADFS 2.0
2. The ADFS server must be configured to deliver a claim of type "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress".

3. The email address must be equal to the user name set up in Ibistic Commerce Platform. Any transformation etc. must be done on the customer's side.
4. The ADFS relaying party must be set up with only signing, not encryption. WS-Federation should be used (not SAML). ICP's identifier and endpoint is "https://services.ibistic.net/sso/adfs/signOn.request".
5. TLS access (https) is recommended to the ADFS server for encryption.
6. The ADFS server may use any certificate to sign its requests. The thumbprint for this certificate must be communicated to Ibistic together with the ADFS Entity ID and WS Federation Endpoint Url. Any changes to this must be rolled out in a synchronized fashion, e.g. on certificate expiry.
7. One certificate can only be used to authenticate one security domain in Ibistic. This means that if several Ibistic customers share IT infrastructure, a separate certificate and relying party must be set up for each customer.
8. Ibistic will try to keep the custom URL stable over time. In some circumstances however it might be necessary to create a new one, e.g. when rolling out certificate changes.

1.3 Security

An ADFS implementation will not provide any added security, as usernames and password will not be disabled. The security of the ADFS login relies entirely on the customer's enterprise environment.

Please note that the customized URL provided by Ibistic is not considered secret and that having access to it will reveal the endpoint URL for the ADFS server. It is therefore entirely up to the customer to properly limit access to their ADFS servers to its own users.

Ibistic recommends that all access to the ADFS 2.0 server is done through HTTPS for privacy and security.

2 Basic ADFS configuration walkthrough

This chapter provides a walkthrough to a simple ADFS setup against ICP. As previously noted, ADFS deployment and configuration is not offered by Ibistic, so any changes to this should be handled by the customer.

2.1 Server setup and preparation

ADFS 2.0 must be set up on a Windows 2008 R2 server. It can be downloaded here: http://technet.microsoft.com/en-us/evalcenter/ee476597.aspx

Please refer to Microsoft for instructions on how to set up ADFS 2.0.

2.2 Information to provide to Ibistic

For Ibistic to be able to enable ADFS on your security domain, we need the following:

1. The thumbprint for your signing certificate
2. ADFS Entity ID
3. WS Federation Endpoint Url

2.2.1 Thumbprint

On the ADFS console, go to *ADFS 2.0 -> Service -> Certificates*. Right-click the certificate under *Token-signing* and click *View certificate.* Go to the *Details* tab and scroll down to *Thumprint*. The entire contents of this field must be provided to Ibistic.

2.2.2 ADFS Entity ID

If your ADFS server is called adfs.yourdomain.local, the Entity ID will by default be **"http://adfs.yourdomain.local/adfs/services/trust"**. To verify this, go to *ADFS 2.0 -> Service -> Endpoints*, and locate the entry of type *Federation Metadata* under *Metadata*. Append this *URL Path* to the ADFS full name and type it into a browser (using HTTPS). Typically this will give you something like "https://adfs.yourdomain.local/FederationMetadata/2007-06/FederationMetadata.xml".

Your *Entity ID* is the one shown as a parameter named *entityID* to the root tag (*EntityDescriptor)* of this document.

2.2.3 WS Federation Endpoint URL

Once again, if the ADFS server is called adfs.yourdomain.local, the WS Federation Endpoint URL will by default be **"https://adfs.yourdomain.local/adfs/ls"**. To check this go to *ADFS 2.0 -> Service -> Endpoints* and locate the endpoint of type *SAML 2.0/WS-Federation* under *Token Issuance*. This will give you the URL relative to your server name. Again, we recommend using HTTPS.

2.3 Setting up the relaying party

2.3.1 Basic properties

Go to *ADFS 2.0 -> Trust relationships -> Relaying Party Trusts* and click *Add Relaying Party Trust* in the right hand action menu. Click *Start*, select *Enter data about the relaying party manually* and click *Next.*

As *Display name* you may write *Ibistic Commerce Platform* or any other descriptive text you may choose. Click *Next*.

On the following page choose *AD FS 2.0 profile* and click *Next*. Click *Next* again to confirm that you don't wish to configure an encryption certificate.

On the *Configure URL* page, check *Enable support for the WS-Federation Passive protocol* and enter "https://services.ibistic.net/sso/adfs/signOn.request" as its URL (without the quotes). Click *Next* and on the following page click *Next* again to accept the same URL as *Relaying party trust identifier*.

Finally, to allow all users to use this connection, leave *Permit all users to access this relaying party* and click *Next* twice.

On the final page leave *Open the Edit Claims dialog..* checkbox checked and click close.

2.3.2 Claim rules

You should now be in a dialog called *Edit Claim Rules for Ibistic Commerce Platform*. If you are not, right click your newly created relaying party and select *Edit Claim Rules*.

Click *Add* and as template select *Send LDAP Attributes as Claims*. As *Claim rule name* write "Lookup email address" and select *Active Directory* as your *Attribute Store*.

In the mappings below select *E-Mail-Addresses* as the *LDAP Attribute* and *E-Mail Address* as the *Outgoing Claim Type*. Click *Finish*.

Your ADFS setup is now complete, but for it to work for the users, please check the steps below.

2.4 User setup

For users to be able to use the ADFS integration, two conditions must be true. First they must access Ibistic Commerce Platform using a special URL provided by Ibistic once the information from chapter "2.2 Information to provide to Ibistic" has been received. This URL will typically look something like "https://services.ibistic.net/sso/adfs/signOn.request?idp=82ec0337-ce83-4db7-9f14-f355820f40db" only with a different GUID at the end.

Second, the email address from Active Directory must be 100% the same as their username in Ibistic. Using the example from this document, the email address retrieved is the one from the *General* tab on a user in AD. For other data sources for the Ibistic Username, please refer to ADFS / AD expertize. Note that if the email address does not coincide with the Ibistic username, you may change either.

2.5 Certificate rollover

Please note that by default ADFS uses certificates with two year validity. Sometime before the signing certificate expires, a new one will be issued and set as Primary. When this happens, the integration with Ibistic will fail. To fix this Ibistic support must get the thumbprint for your new certificate to get this up again. Please note that this may take up to 24 hours to be effective.

Please be proactive to minimize downtime related to certificate rollover. Refer to Microsoft's technical documentation for resources on how to control how rollover is done.

3 Client software tip

As mentioned, ADFS deployment and setup is not part of the Ibistic offering. Our experience however is that ADFS works out of the box best with Internet Explorer, and that the ADFS server should be added to the users' *Local Intranet* zone to not have to provide any additional login when using an AD account to login to the computer itself.

We recommend that this is done through Group Policies or other enterprise configuration tools. To do this manually however, go to *Internet options* inside IE (or from the start menu) and then go to the *Security* tab. Click *Local intranet*, then *Sites* and then *Advanced*. If your ADFS server is called "adfs.yourdomain.local" enter "https://adfs.yourdomain.local" in the textbox and then click *Add*. Click *Close* and *OK* twice and the ADFS logon should now be completely transparant for the user.

4 Contact

For the project of setting up ADFS in your organization, please contact Ibistic Support (http://support.ibistic.com/ or support@ibistic.com) and a technical project manager will be assigned to help you through the process.