SAML F.A.Q.

What is SAML? (Security Assertion Markup Language)

SAML is an internet standard that provides SSO (Single-Sign On) capability. The client maintains a SAML 'hub' that applications can be configured to authenticate with. Users within a district can log into the 'hub' and then have authenticated access to all the applications that are configured to work with that SAML instance.

Analogy: SAML is like a shopping mall. One you gain access to the mall; you will then have access to all the stores within it.

How does SAML differ from LDAP?

LDAP allows for centralized authentication- users can sign-in with one set of credentials at all sites making use of the same directory server. That isn't quite the same as SSO because you must sign-on with those credentials at each site you visit. Under SAML, you normally have to provide your credentials only once, making it true SSO.

Requirements

Since SAML is mostly self-configured and administered, the client's network team should have a solid understanding of how to implement, secure, monitor, and manage a SAML system. Blackboard WCM Support cannot assist with the setup and configuration of a SAML system as this would pose an inherent security risk for the client.

The SAML standard also closely controls what error information and diagnostic data can be seen outside the central "hub" so it is critical that the client's server administrators be the primary participant in any investigation. We are available to assist with requests they provide, but we cannot see enough to make the diagnosis.

Also, the client's sign-in must be protected under SSL. For AWS clients, this won't be an issue. For Expedient-hosted client, you will need to verify that the client has SSL activated. If not, you will need to discuss moving to AWS vs getting a new certificate for their site.

What does the setup process consist of?

NOTE - It is highly suggested the client waits until the "Go Public" process has finished. See below.

We will assist client with getting SSL activated if they do not have it already.

Client will need to have SAML configured on their network. For assistance with adding WCM to their SAML, they can review the documentation noted below.

If the client has purchased SAML and it's been activated by Hosting, the client should be able to manage the rest of the set-up process by themselves using the documentation noted at the end of this FAQ.

Can we help set up the client side of SAML?

No, this imposes a security risk. We cannot supply any technical information regarding the client side setup. The client will need to handle their own SAML configuration.

Best time to implement SAML

We suggest setting up SAML after the “Go Public” process has finished. Implementation of SAML before this process has finished can yield unwanted results.

Can SAML be implemented before the “Go Public” process has started?

Yes, but we advise against it.

Because of what SAML is and how it works, there is very little value and no assurance that a test under the incubation domain will translate to a successful public domain. SAML relationships are established based on trusted server identities. Once that trusted relationship is in place, the identity server sends a command of "this is user X, let them in" and our server follows that instruction.

That trusted relationship is based entirely upon domain names, so changing the domain name after it is set up means eliminating the original (working) relationship and building a fresh one. Clients will want to be authenticating against their public domain as this influences where they are redirected to upon authentication, so they should wait until their site is using that public domain.

The primary issue clients will run into if they implement prior to going public will be inability to authenticate after going public. User accounts are flagged as SAML after the first successful SAML login. After that, those user accounts must authenticate via SAML. If they implement using the incubation domain, when the client goes public and that server identity trust is broken, any users flagged as SAML will not be able to authenticate. Each account will need to be manually reverted to local authentication. If they must revoke SAML access to 500 users so they can temporarily authenticate locally, that's 500 manual edits.

On the other hand, if they authenticate locally before going public and then any time after going public they decide to deploy SAML, all those users remain non-SAML until they experience a successful SAML assertion on that account. That means no disruption until everything's verified as functional.

Can the client test SAML before the “Go Public” process has started?

Yes, but it doesn't yield accurate results and highly we advise against it.

SAML establishes a relationship based on trusted server identities. The server identity will change after you have “Gone Public”. This is where most the issues will arise. Since SAML functionality relies on trusted relationships between domains, SAML will fail or redirect users to the old archived version of the incubation after login, potentially frustrating users.

What if the client is still insisting on testing SAML?

An early rollout can be achieved, but the client must be aware of the issues noted above. They will want to do a limited rollout and not rely on SAML before “Going Public”. We recommend testing with 1 or 2 disposable test accounts. They can then test the accounts and then delete all settings on both sides (the ADFS server and WCM) and re-implement after going public. The client will want to be sure to set any accounts that were used for SAML testing back to local authentication before going public.

After “Going Public” the client can schedule a time to implement SAML on their public domain. They should not assume that it will roll out the same way on their public domain that it did with the incubation domain.

Example of a failed early SAML rollout

A client had rolled out SAML prior to going public. After going public, all SAML users errored out on the authentication attempt. The client then tried to build new SAML relationship to their public domain. Internal network DNS issues conflicted with requests to the new domain, resulting in delays in the rollout. As an interim solution, the administrator needed to switch 500+ users back to local authentication. Then those 500+ user needed to reset their password before they could access the site. The total downtime was 3 weeks.

Had the client waited until they were public, all 500 clients would have been local authentication, would not have been disrupted, and even if they tried to do SAML and failed, would NOT have been flagged as a SAML authentication until they successfully were passed in from the SAML sever, resulting in no outage.

SAML Documentation Links

Set Up Active Directory Federation Services (ADFS):
http://insight.dev.schoolwires.com/HelpAssets/C2Assets/C2Guides/SWADFSSetUp.pdf

Security Assertion Markup Language (SAML) Site Manager Setup:
http://insight.dev.schoolwires.com/HelpAssets/C2Assets/C2Guides/SWSAMLSetUp.pdf

Once we go live will local authentication still exist along with the option to log into SAML?

Yes. We recommend creating a non-SAML connected administrator account for trouble shooting purposes.