Single Sign-On – SAML 2.0

Your library can use single sign-on (SSO) where your users are signed onto a computer or account centrally managed by your organisation to bypass manual Infiniti authentication. Authorisation (role management) will still occur within Infiniti.

When configured, Infiniti will not prompt pre-authenticated SSO users for a username and password. If Infiniti is configured to opt for single sign-on as the first authentication strategy, unauthenticated users will be directed to their organisation's authentication server or prompting mechanism.

SAML 2.0 is an industry-standard cross-platform protocol for single sign-on between web sites and authentication sources. Ask your IT department or contractor if your organisation infrastructure supports SAML 2.0.

Key Concepts

Service Provider – This will be your Infiniti Library Management System.

Identity Provider – This is your centralised user directory.

SAML Metadata – Information that Infiniti and your Identity Provider will share to establish an ongoing trusted authentication relationship. Infiniti's metadata will be loaded into your Identity Provider; and your Identity Provider's metadata will be loaded into Infiniti.

Subject NameID – The SAML identifier that your Identity Provider will supply Infiniti over an encrypted channel for authenticated users. Infiniti will match this identifier against known enabled Infiniti users.

Quick Start – Infiniti Configuration

1. ***System Cog → Settings → Integration***
2. ***Reuse Webserver Certificate → On***
3. ***Service Provider → On → Save → [Input metadata URL into your Identity Provider]***
4. ***Wait 60 seconds***
5. ***Identity Provider (Internet) → Off***
6. ***Identity Provider (File) → On → [Upload file from your Identity Provider]***
7. ***Match NameID Against → Username***
8. ***Default Authentication Method → Off***
9. ***Logout Button → On***
10. ***Save***
11. ***Wait 60 seconds***
12. ***Test using https://[your Infiniti LMS]/welcome/sso***

For more detailed information, please read this documentation in-depth.

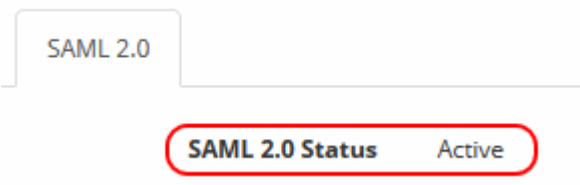
Quick Start – Identity Provider Configuration (examples)

Ping Identity	Cloud	https://goo.gl/Rc2kQI
ADFS 2.0	Microsoft	https://goo.gl/21YGX0
SimpleSAMLphp	Open Source	https://goo.gl/iPQziH

SAML 2.0 in Infiniti

A user with the *System Administrator* privilege can navigate to SAML 2.0 tab under the *System Settings* – *Integration* section.

An active SAML 2.0 relationship exists when Infiniti as a SAML Service Provider has been turned on and one of the Identity Provider origins (Internet or File) has been populated and turned on:



Note: An active SAML 2.0 relationship from Infiniti's perspective does not guarantee successful single sign-on, as the Identity Provider must also be correctly configured and the end-user's browser must correctly accept and mediate encrypted traffic between the Service and Identity Provider.

- - -

When you turn on the SAML Service Provider role for Infiniti and save your configuration, you will be supplied with a Service Provider metadata link that your Identity Provider can consume:

If your Identity Provider does not support metadata polling or has no access to the internet, you can click on and manually download Infiniti's SAML metadata file to upload to your Identity Provider server. Neither the metadata link nor the metadata file are confidential and can be freely shared with any applicable service or computer.

- - -

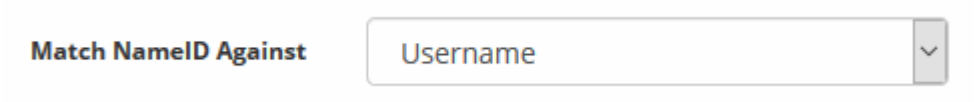
Infiniti will cryptographically sign its communication with your Identity Provider using either its commercial third-party webserver certificate or a custom certificate generated by Infiniti:

A custom certificate is more inline with SAML 2.0 specifications on isolated trust relationships. However, reusing the webserver certificate for SAML may require less configuration of new trust behaviour in some Identity Providers, like ADFS. The webserver certificate will expire more frequently (1 year) than the custom certificate (3 years). Both are equally secure.

As Infiniti's metadata contains X.509 server certificates that can expire; if your Identity Provider checks the expiration validity of the SAML service provider server certificates, you will either need to configure your Identity Provider to auto-update from the Infiniti metadata link supplied or periodically re-upload Infiniti's metadata file to your Identity Provider. Switching between custom and webserver signed certificates will also update the metadata your Identity Provider must use.

- - -

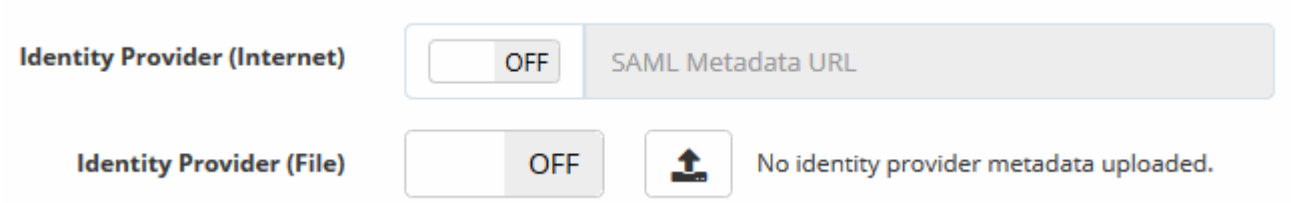
Your Identity Provider must supply for authenticated users a SAML security assertion that contains a Subject NameID. This is a user identifier from your central user directory that Infiniti will match against its internal database of known enabled users:



Users are matched on the selected field case-insensitively. Infiniti users that are disabled, lacking a System Group, or sharing the same identifier are not logged in. Note: You can use an Infiniti API to automatically import and update users; or you can manually manage users within Infiniti as an administrator.

- - -

Once you have configured your Identity Provider you will need to either provide Infiniti with a URL to the Identity Provider's SAML metadata or upload a copy of the metadata XML file:



If you use a metadata URL, the Identity Provider must be internet accessible. If the link is HTTPS the Identity Provider's web server certificate must be signed by a commonly recognised third-party Root CA. The X.509 certificates *within* the Identity Provider 's SAML metadata can be self-signed and unrelated to the Identity Provider's web server certificates. Infiniti will poll the Identity Provider with an interval of between 5 minutes and 4 hours. The exact polling rate depends on parameters within the metadata; prior retrieval success; and network latency.

- - -

SAML single sign-on can be made the default authentication method for Infiniti or an alternate authentication channel for a sub-set of users:

It is recommended to thoroughly test single sign-on both inside and outside your organisation before enabling federated single sign-on as the default.

When SAML 2.0 is active but not the default authentication method, users assigned single sign-on rights at the Identity Provider may access Infiniti via *https://[your Infiniti LMS]/welcome/sso* or through any custom portal link supplied by your Identity Provider.

When SAML 2.0 is active and is the default authentication method, users can (if made aware of this option) fall back to other manual Infiniti authentication methods via *https://[your Infiniti LMS]/login.* As such the login page itself should not be the default bookmark or intranet link to Infiniti when SAML SSO is being used.

- - -

When SAML SSO is the default authentication channel, user may never see a manual Infiniti login page or even be aware that it exists. A new option becomes available to hide the logout button or change the logout destination to somewhere other than Infiniti:

Hiding the login-logout paradigm in Infiniti is restricted to libraries using implicit single sign-in as only this arrangement has adequately hidden authentication from the user.

Logging out of Infiniti does not log the user out of their federated session. As such if a person forgets to logout of their federated session (computer asset, browser, VPN, etc); another person using the same computer may be automatically logged in as the previous user. This is a common vulnerability of single sign-on; both Cloud (Google+, Facebook) and Enterprise (SAML).

Commonly Encountered Identity Provider Caveats

SHA-1 Deprecation

Infiniti only supports the SHA-256 signature algorithm for SAML 2.0; as SHA-1 has been deprecated by NIST. Very old SAML identity providers may default to SHA-1 signatures, and must be changed to SHA-256 to communicate with Infiniti. Any self-signed or corporate PKI certificates and their certificate chains must have been generated with SHA-256 signatures. Commercially signed certificates already use SHA-256.

GoDaddy G2 Root Certificate

The GoDaddy G2 Root Certificate used by Infiniti is relatively recent as far as root certificates go, and may not be installed by default on all mature server ecologies. If you are reusing the Infiniti webserver certificate for signing SAML Service Provider assertions and metadata, you may encounter this problem. You will either need to install the root certificate (https://certs.godaddy.com/repository) or switch off webserver certificate reuse.

Forgetting a "NameID" claim rule for your Infiniti Relying Party in ADFS

Infiniti requires ADFS to send a Subject NameID assertion when authenticating a federated user. Useful Active Directory attributes to map to "Name ID" (only need one such claim) include UPN, SAM-Account and Email.

Having two instances of Infiniti configured as Relying Parties in ADFS

ADFS will not only treat two EntityIDs as the same effective Relying Party but also two equal signing certificates as the same Relying Party. Only one of the instances will be established correctly; the other will fail. This may occur even if one of the configuration instances is disabled.

A situation where this may occur is organisations with more than one Infiniti library federating all Infiniti instances through the same ADFS farm and reusing the Infiniti webserver certificate for SAML signing and trust convenience. Switching to the Infiniti PKI will resolve the issue as each Infiniti library has a unique signing certificate generated by the Infiniti PKI.

Using ADFS + IIS 7.0 and Chrome

Chrome does not automatically support IIS "extended protection" used by ADFS. In later versions of IIS (7.5+) an option exists to disable extended protection if your end-users prefer Chrome; for IIS 7.0 this option is not available and adjustments will either need to be made to each Chrome browser installation or discourage