Mettl Single Sign On(SSO) Documentation

Document Version: v1.1

Document Release Date: 17th Feb ,2018

Please contact us on support@mettl.com for any queries.

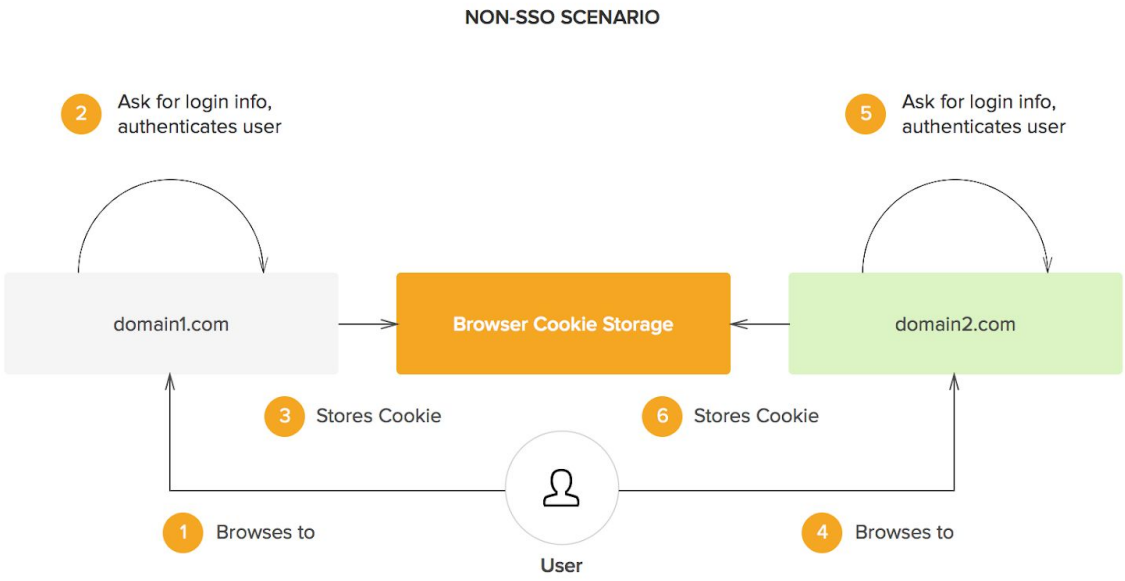
Table of Contents

1. SSO Introduction:

Mettl's platform supports smooth and quick integration of single sign-on (SSO) using Security Assertion Markup Language (SAML). SSO mitigates compliance and security risks for organisations by giving clients control over candidate authentication.

By configuring SSO client can use identity provider to authenticate candidates. It lets a candidate log in once and gain access to Mettl assessments without being prompted to log in again. SSO also enables application to share information about candidates.This is both convenient and secure practice for client.

2. NON SSO SCENARIO:



In a case when SSO is not enabled, when a user visits Mettl to take test from a platform he/she has to Re-register to start the test. Which is depicted in the above scenario.

3. SSO SCENARIO:

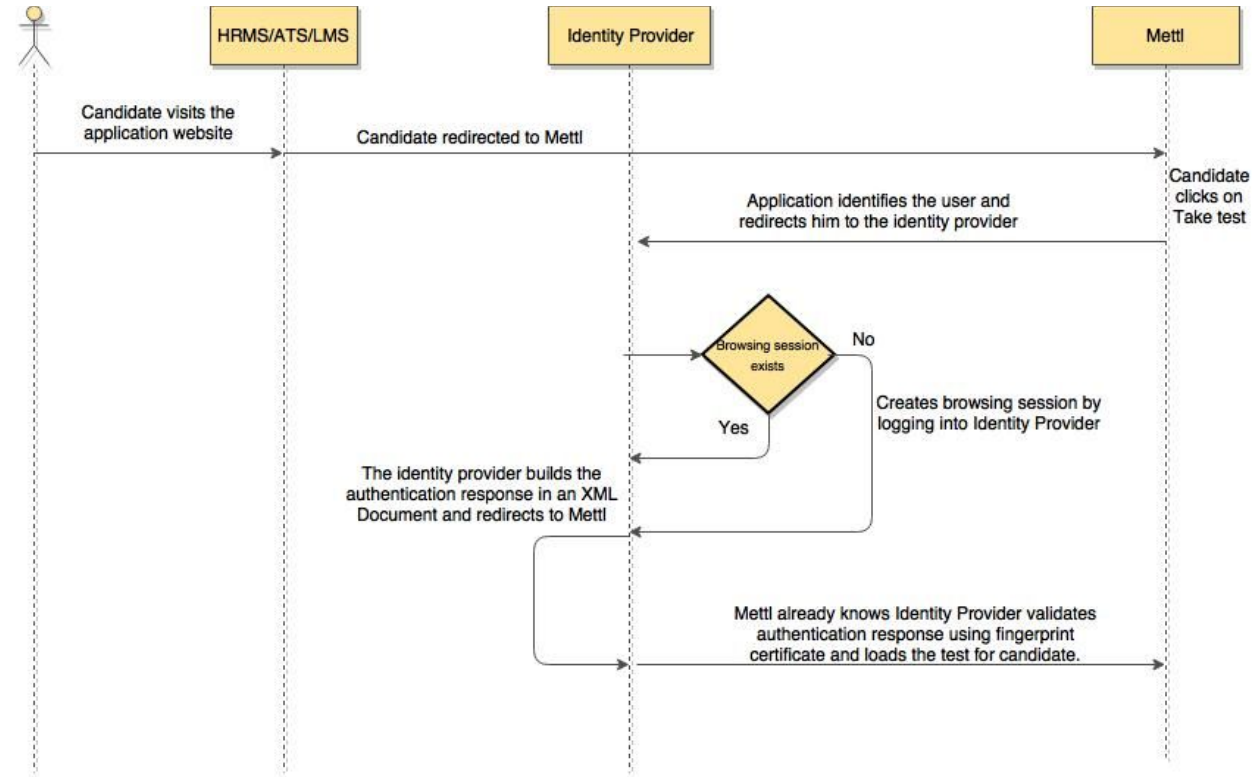
Here in SSO we are using SAML Protocol to implement it.

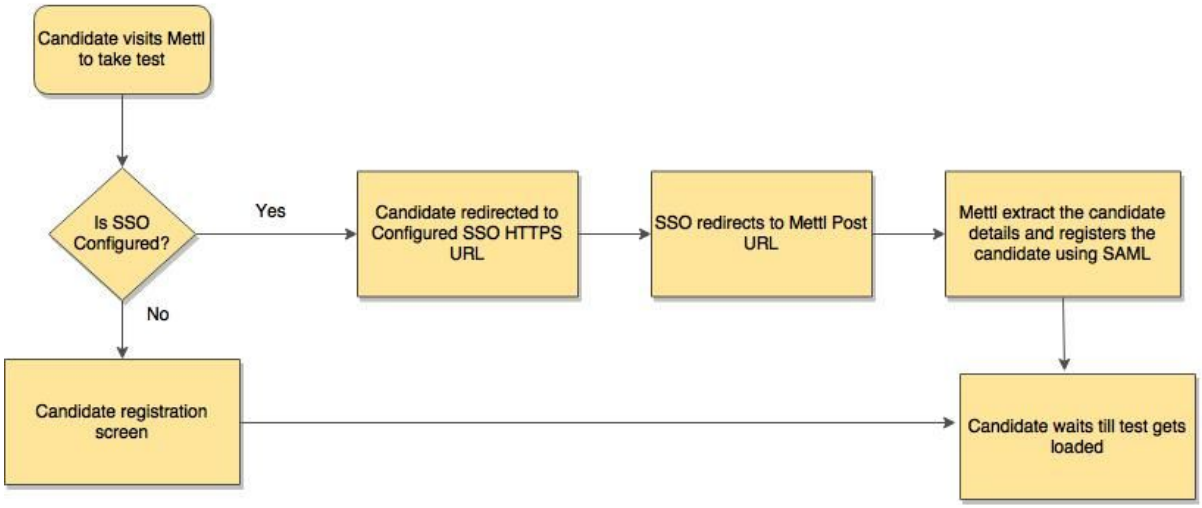
Security Assertion Markup Language (SAML) is a standard protocol for web browser Single Sign-On (SSO) using secure tokens. SAML completely eliminates all passwords and instead uses standard cryptography and digital signatures to pass a secure sign-in token from an identity provider to a SaaS application.

SAML SSO works by transferring the user's identity from one place (the identity provider) to another (the service provider). This is done through an exchange of digitally signed XML documents.

Consider the following scenario: A user is logged into a system that acts as an identity provider. The user wants to log in to a remote application, such as a support or accounting application (the service provider). The following happens:

1. To begin the process of SSO, clients needs to append '**tests.mettl.com/test-window/<key>**' URL to the 'Take Test' button of their application
2. User clicks on Take test button on Application.
3. The application identifies the user's origin (by application subdomain, user IP address, or similar) and redirects the user back to the identity provider, asking for authentication. This is the authentication request.
4. The user either has an existing active browser session with the identity provider or establishes one by logging into the identity provider.
5. The identity provider builds the authentication response in the form of an XML-document containing the user's username and email address, signs it using an X.509 certificate, and posts this information to the service provider.
6. The service provider(Mettl test), which already knows the identity provider and has a certificate fingerprint, retrieves the authentication response and validates it using the certificate fingerprint. Encrypted SAML response is not supported by Mettl in this scenario.
7. The identity of the user is established and test gets loaded for candidate.


HRMS/ATS/LMS
Identity Provider
Mettl
Candidate visits the application website
Candidate redirected to Mettl
Candidate clicks on Take test
Application identifies the user and redirects him to the identity provider
Browsing session exists
No
Yes
Creates browsing session by logging into Identity Provider
The identity provider builds the authentication response in an XML Document and redirects to Mettl
Mettl already knows Identity Provider validates authentication response using fingerprint certificate and loads the test for candidate.


Candidate visits Mettl to take test
Is SSO Configured?
Yes
No
Candidate redirected to Configured SSO HTTPS URL
SSO redirects to Mettl Post URL
Mettl extract the candidate details and registers the candidate using SAML
Candidate registration screen
Candidate waits till test gets loaded

End of Mettl's SSO Document

Please contact us on support@mettl.com for any queries.

Mettl.com – Online Assessments Made Easy