Single Sign On (SSO) in Intelligent Configuration Manager (ICM)

Suresh, Prem, Ankita
August, 2024

Agenda

1 Metadata Download

2 Enabling SSO

3 Updating SSO

4 Debugging SSO

5 FAQ’s

6 Q&A

Download / Upload Metadata

SAML Authentication in Intelligent Configuration Manager

- Users with role Customer administrators can configure SAML authentication settings for their site in the Intelligent Configuration Manager workspace without having to request assistance from SAP Ariba representatives.

- End users no longer have to wrestle with multiple unique logins or contend with forgotten passwords.

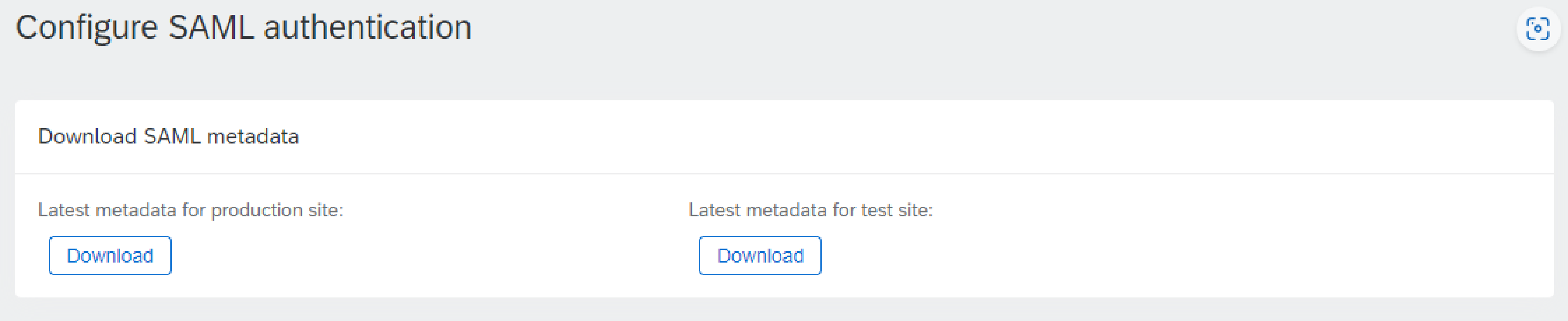
- All SAP Ariba solutions have the ability to integrate with an existing Single Sign-On (SSO) solution to securely authenticate users once.

- Security Assertion Markup Language (SAML) is an XML standard for exchanging authentication and authorization data between security domains.

- SAP Ariba supports SAML 2.0 style SAML HTTP POST binding authentication protocols for all enterprise users in the **Intelligent Configuration Manager** workspace.

Configuring SAML Authentication

The **Download SAML metadata** section provides the metadata download option from SAP Ariba for test and production sites. Customer can upload the metadata to the service provider system.



Configure SAML authentication

Download SAML metadata

Latest metadata for production site:

Latest metadata for test site:

The **Production site authentication** section lets you configure the SAML authentication in your production site and he **Test site authentication** section lets you configure the SAML authentication in your test site.

If the SAML authentication is configured in your test site, this section shows the existing certificate information with status.

Limitations

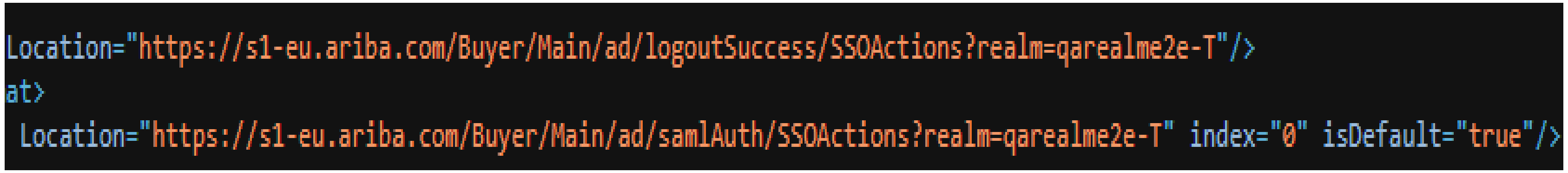
In line with our commitment to enhance your experience, we are rolling out our URL uniformity program.

This program aims to consolidate all our URLs under the Primary Front Door (PFD) for improved consistency and convenience.

When you download the metadata, please note the changes in the location URL:

- The location URL is s1.ariba.com.

- For sites s1-2.ariba.com, the location URL needs to manually amended to s1-2.ariba.com



```
Location="https://s1-eu.ariba.com/Buyer/Main/ad/logoutSuccess/SSOActions?realm=qarealme2e-T"/>
at>
 Location="https://s1-eu.ariba.com/Buyer/Main/ad/samlAuth/SSOActions?realm=qarealme2e-T" index="0" isDefault="true"/>
```

Demo

Enabling SSO

Single Sign-On

- SAP Ariba solutions have the ability to integrate with an existing Single Sign-On (SSO) solution to securely authenticate users once and then move from application to application transparently without requiring them to log in again.
- Security Assertion Markup Language (SAML) is an XML standard for exchanging authentication and authorization data between security domains.

Prerequisites

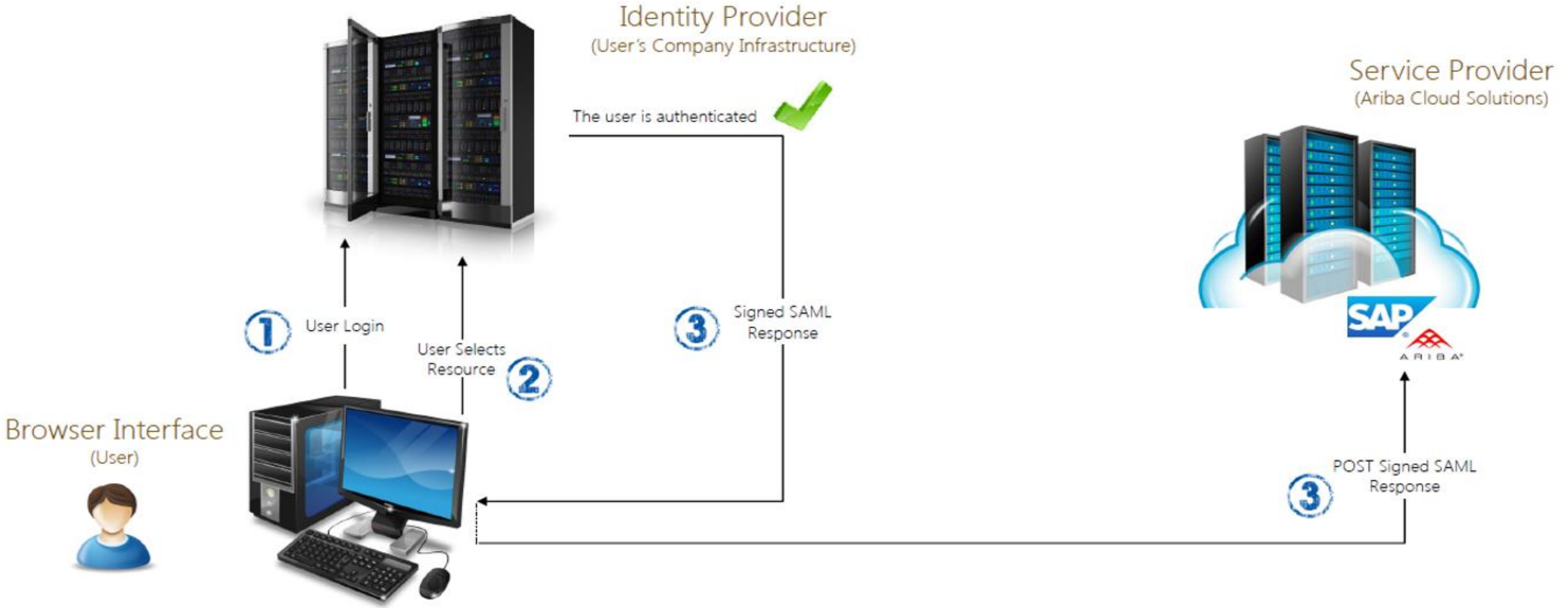
- You must be a member of the Customer Administrator group with Third Party Enterprise User (Ariba) type.
- You must sign in to the Intelligent Configuration Manager workspace with the third-party user access credentials to update the authentication configuration.
- Gather SAML metadata from your identity provider that you need to upload.

Guidelines for Configuring SAML Authentication

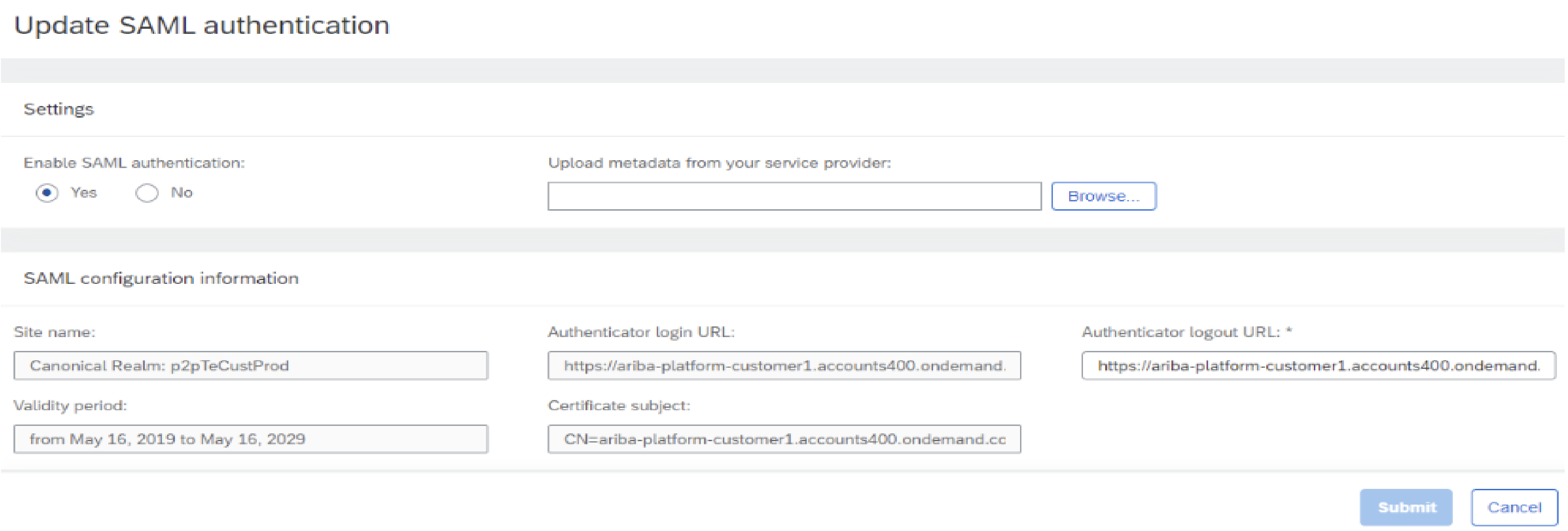
- **In suite-integrated configurations**, you need to update SAML authentication in the Buying and Invoicing site. The Sourcing and Contracts site inherits configuration changes made in the Buying and Invoicing site.
- **In multi-ERP configurations**, you must update SAML authentication in each site separately.
- To enable or update SAML authentication settings for your test and production sites, you must update them from the test site only. You can't update them directly in production sites.
- You must have the third-party user access credentials to update the authentication configuration in the Intelligent Configuration Manager workspace.
- If the site you're updating is configured for corporate authentication and you want to switch it to SAML authentication, you need to submit a case to SAP Ariba Support.

SAML – Identity Provider (IDP)

End users can log into your Identity Provider's SSO page (e.g., Okta, OneLogin, or Microsoft Azure AD) and then access/click a Ariba application to log in using SSO and open the Ariba application.



SAML configuration information



Update SAML authentication

Settings

Enable SAML authentication: ● Yes ○ No

Upload metadata from your service provider:

SAML configuration information

Site name: Canonical Realm: p2pTeCustProd

Authenticator login URL: https://ariba-platform-customer1.accounts400.ondemand.

Authenticator logout URL: * https://ariba-platform-customer1.accounts400.ondemand.

Validity period: from May 16, 2019 to May 16, 2029

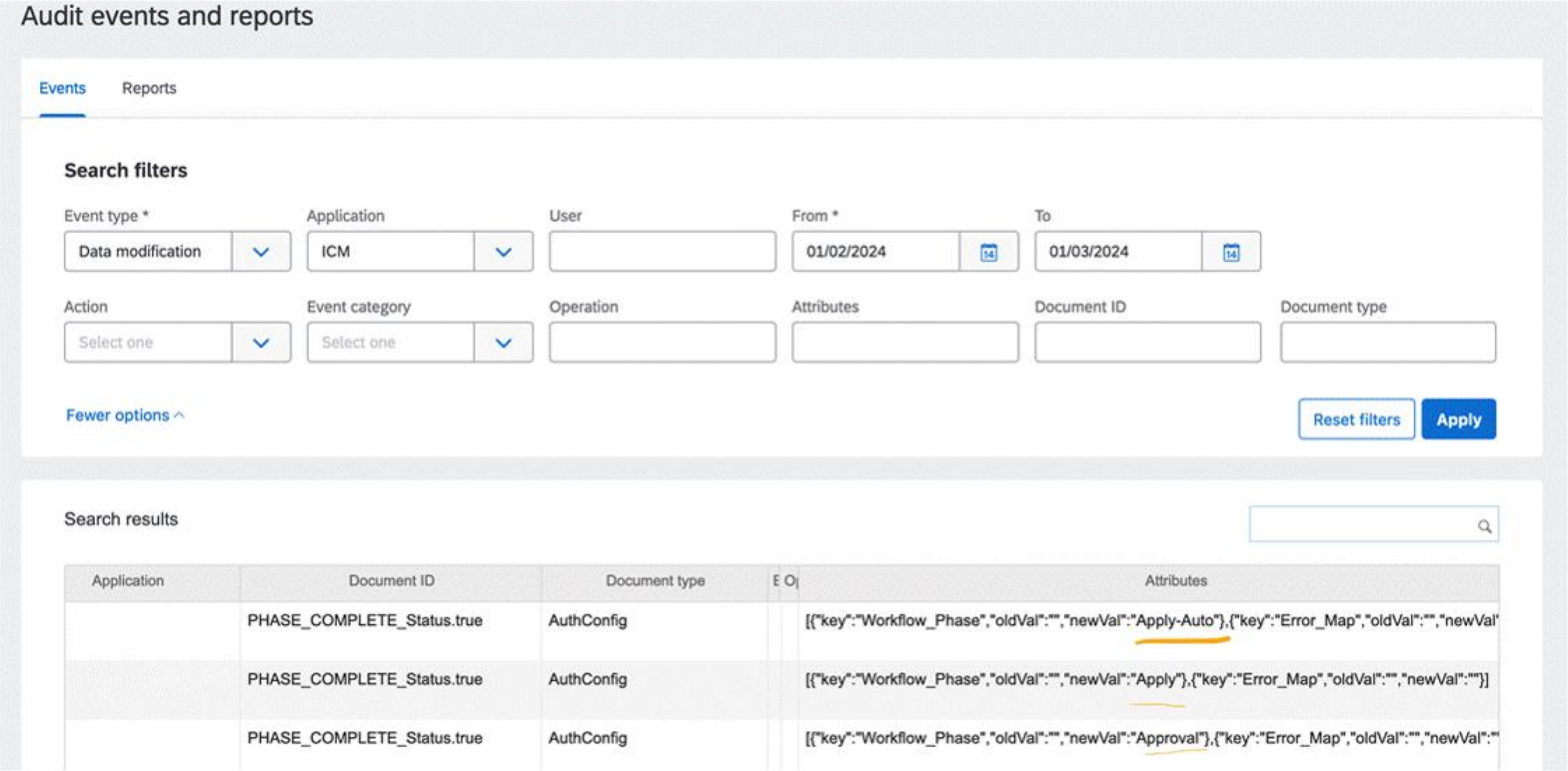
Certificate subject: CN=ariba-platform-customer1.accounts400.ondemand.cc

Field	Description
Site name	The name of the site you're enabling authentication for.
Authenticator login URL	The URL to the customer’s third-party SSL application. The URL must be fully qualified, for example: https://www.sap.com.
Authenticator logout URL	Enter the URL to which users should be redirected after logging out of the SAP Ariba on-demand application. The URL must be fully qualified, for example: https://www.sap.com. This is a required field. **Note:** This URL is not updated after the metadata file upload if it's already added in the system. You need to update it manually.
Validity period	The validity period of the certificate.
Certificate subject	The subject of the certificate.

Status

Status	Description
Ready to approve	The authentication update is ready for approval.
Ready to apply	The authentication update is ready to apply in your site.
Enabled	The SAML authentication is enabled in your site.
Disabled	The SAML authentication is disabled in your site. This is visible in the production site only.

Audit log



Audit events and reports

Search filters

Event type *: Data modification

Application: ICM

User:

From *: 01/02/2024

To: 01/03/2024

Action: Select one

Event category: Select one

Operation:

Attributes:

Document ID:

Document type:

Search results

Application	Document ID	Document type	E	O	Attributes
	PHASE_COMPLETE_Status.true	AuthConfig			[{"key":"Workflow_Phase","oldVal":"","newVal":"Apply-Auto"},{"key":"Error_Map","oldVal":"","newVal'
	PHASE_COMPLETE_Status.true	AuthConfig			[{"key":"Workflow_Phase","oldVal":"","newVal":"Apply"},{"key":"Error_Map","oldVal":"","newVal":""}]
	PHASE_COMPLETE_Status.true	AuthConfig			[{"key":"Workflow_Phase","oldVal":"","newVal":"Approval"},{"key":"Error_Map","oldVal":"","newVal":"

Demo

SAP Ariba

Updating SSO

Updating SSO

- To update SAML authentication settings for your test and production sites, you must update them from the test site only.
- You can’t update them directly in production sites.
- The **Configure SAML authentication** page is in the read-only mode in your production site.
- If the SAML authentication is already configured, you can update the certificate information at any time. For example, upload a new certificate when the certificate validity period is expired, or update the logout URL.
- When updating authentication settings in your site, make sure to follow these 3 steps: Update, Approve, and Apply.

Prerequisites

- You must be a member of the Customer Administrator group with Third Party Enterprise User (Ariba) type.

- You must sign in to the Intelligent Configuration Manager workspace with the third-party user access credentials to update the authentication configuration.

- Gather SAML metadata from your identity provider that you need to upload.

Steps to Follow

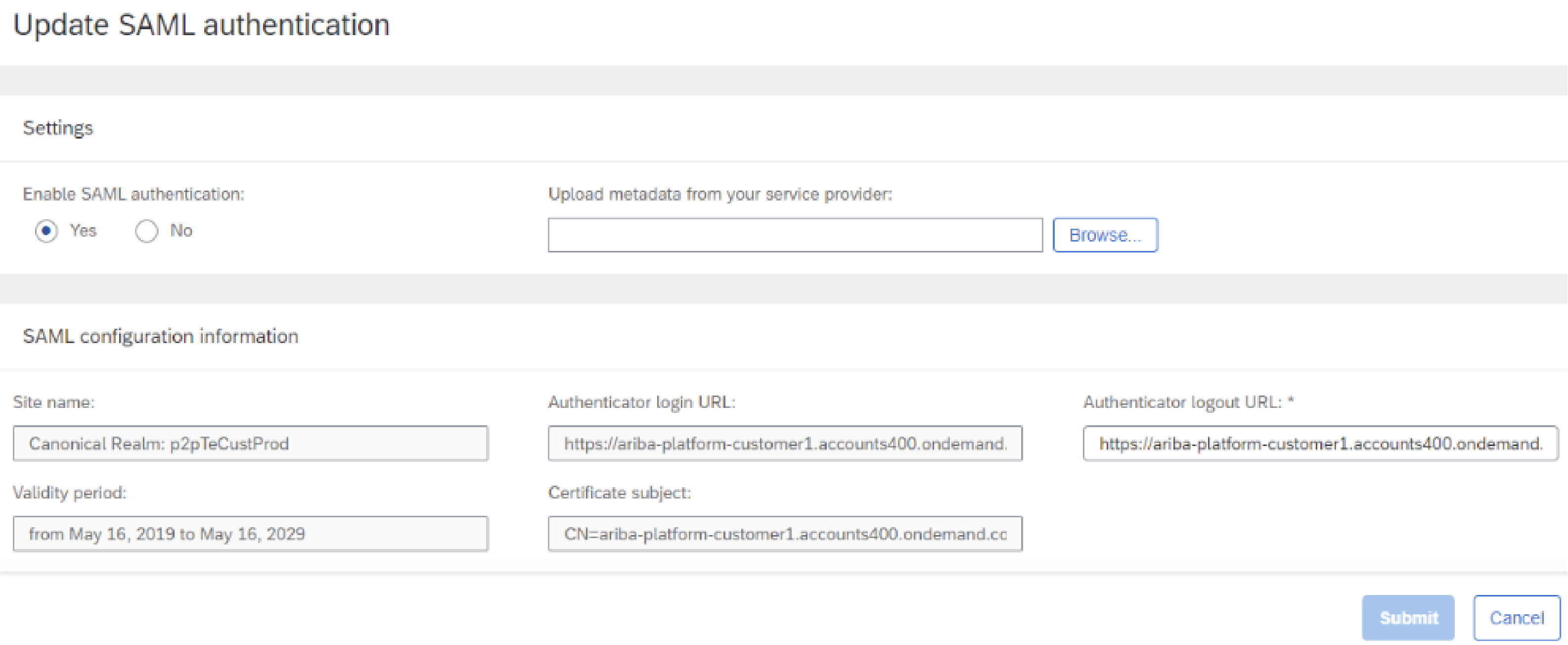
1. Go to the **Intelligent Configuration Manager** workspace. For detailed steps, see Accessing Intelligent Configuration Manager Workspace.

2. From the menu bar, click **Authentication** to open the **Configure SAML authentication** page. Define if you're configuring authentication for test or production site and choose the related section.

3. Optionally, in the **Download SAML metadata** section, click **Download** to download the latest metadata from SAP Ariba.

Steps to Follow Cont...

4. Click **Update** to update the authentication settings in your site.



Update SAML authentication

Settings

Enable SAML authentication: ● Yes ○ No

Upload metadata from your service provider:

SAML configuration information

Site name: Canonical Realm: p2pTeCustProd

Authenticator login URL: https://ariba-platform-customer1.accounts400.ondemand.

Authenticator logout URL: * https://ariba-platform-customer1.accounts400.ondemand.

Validity period: from May 16, 2019 to May 16, 2029

Certificate subject: CN=ariba-platform-customer1.accounts400.ondemand.cc

Steps to Follow Cont..

5. In the **Enable SAML authentication** field, choose **Yes** to enable the SAML authentication in your site.

6. Click **Browse** to choose a file to upload metadata from your service provider. You can upload only one XML file. It must be a valid XML file. The maximum size allowed for a single file is 10 MB.

7. Click **Submit** to submit the certificate information.

8. As an approver, review the information. Choose one of the following options:

- To approve the authentication update, click **Approve**. Enter the comments before approving and click **Approve**.
- To reject the authentication update, click **Reject**. You must enter the comments before rejecting the authentication updates and click **Submit**. You can update the authentication configuration again.

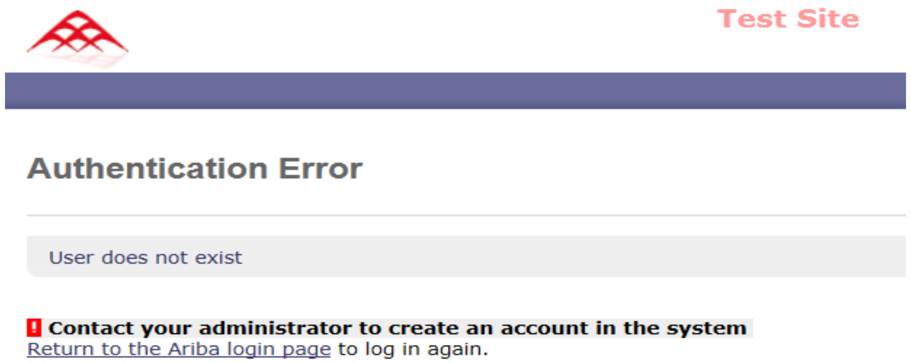
9. Click **Apply** to apply the SAML authentication in your site.

10. Click the checkboxes on the confirmation box and click **OK**.

Debugging SSO

We can avoid Service Requests (SRs) for?

- Download/update Metadata xml
- Enable/Disable SSO
- Updating the certificate
- Authentication error: User does not exist.
- Authentication Error - Failed to validate the user. Please contact your administrator for further assistance.



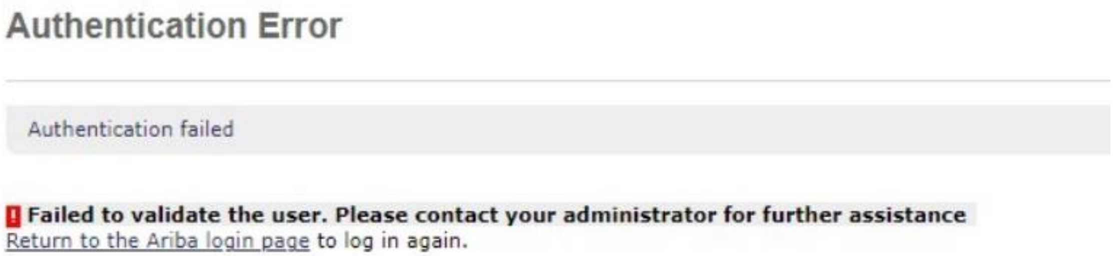
Test Site

Authentication Error

User does not exist

! Contact your administrator to create an account in the system

Return to the Ariba login page to log in again.



Authentication Error

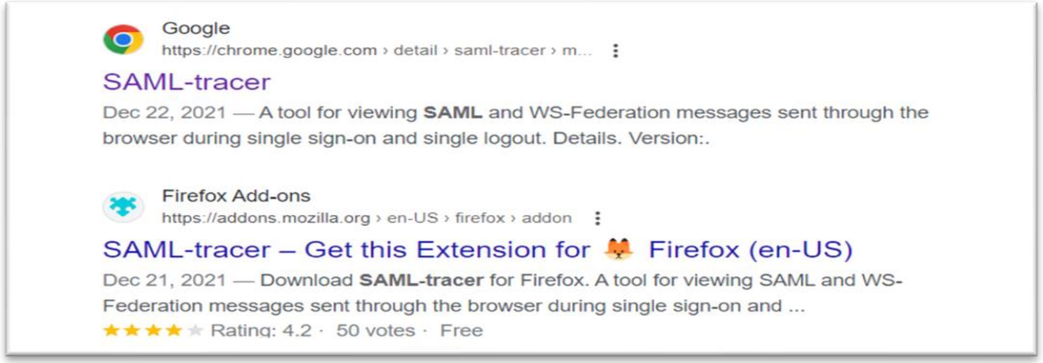
Authentication failed

! Failed to validate the user. Please contact your administrator for further assistance

Return to the Ariba login page to log in again.

Debugging SAML

- Chrome/Firefox browser extension – SAML Tracer extension
- The SAML Response is Base64-encoded
- Locate SAML Response
- Verify the NameID
  - NameID is case sensitive



Google
https://chrome.google.com › detail › saml-tracer › m...

SAML-tracer

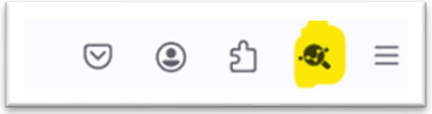
Dec 22, 2021 — A tool for viewing **SAML** and WS-Federation messages sent through the browser during single sign-on and single logout. Details. Version:.

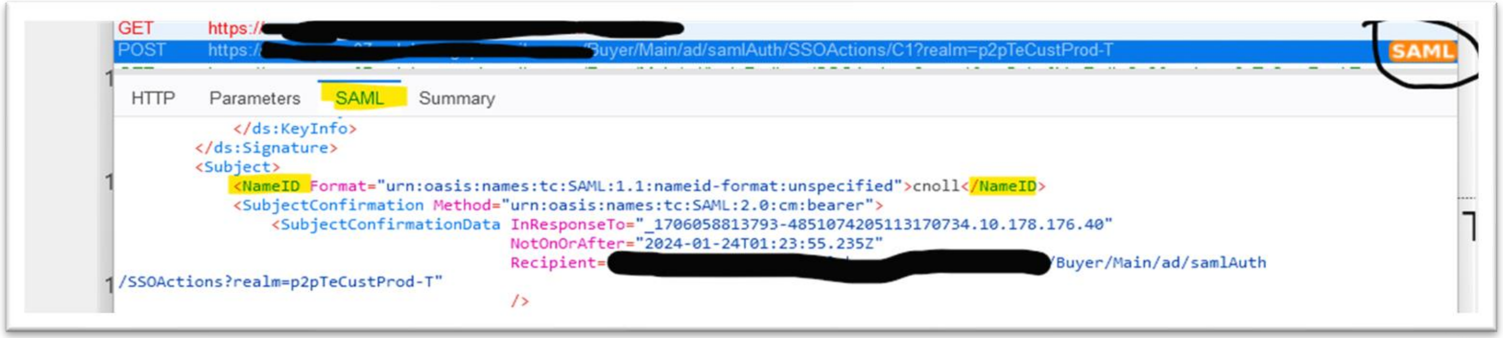
Firefox Add-ons
https://addons.mozilla.org › en-US › firefox › addon

SAML-tracer – Get this Extension for 🦊 Firefox (en-US)

Dec 21, 2021 — Download **SAML-tracer** for Firefox. A tool for viewing SAML and WS-Federation messages sent through the browser during single sign-on and ...

★★★★☆ Rating: 4.2 · 50 votes · Free





```
GET     https://[redacted]
POST    https://[redacted]Buyer/Main/ad/samlAuth/SSOActions/C1?realm=p2pTeCustProd-T          SAML
```

```
            </ds:KeyInfo>
        </ds:Signature>
        <Subject>
            <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">cnoll</NameID>
            <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <SubjectConfirmationData InResponseTo="_1706058813793-4851074205113170734.10.178.176.40"
                                         NotOnOrAfter="2024-01-24T01:23:55.235Z"
                                         Recipient=[redacted]Buyer/Main/ad/samlAuth
/SSOActions?realm=p2pTeCustProd-T"
                                         />
```

- Check the Valid From/To timestamps
- Verify the certificate sent in the XML

Demo

FAQ’s

QnA

Thank you.

Contact information: