Feature at a Glance

Ability to Configure SAML Authentication Settings in Intelligent Configuration Manager (PLICM-871)

Content Owner: Justin Stephansky
Target GA: Q1, 2024

THE BEST RUN SAP

Introducing: **Ability to Configure SAML Authentication Settings in Intelligent Configuration Manager**

Feature Description

Customer administrators can now enable and update SAML authentication for their site in the Intelligent Configuration Manager workspace without having to request assistance from SAP Ariba representatives.

Key Benefits

Within Intelligent Configuration Manager, you were not able to enable or update your SAML SSO configuration. Customers would need to log a service request to enable or change their SAML SSO configuration in each of their workspaces. With this feature, customers can now enable and update their SAML SSO configuration in their site and promote the changes from test to production site.

Audience:

Buyer

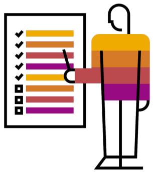
Enablement Model:

High Touch

Applicable Solutions:

SAP Ariba Buying
SAP Ariba Buying and Invoicing
SAP Ariba Contracts
SAP Ariba Contract Invoicing
SAP Ariba Catalog
SAP Ariba Invoice Management
SAP Ariba Sourcing
SAP Ariba Spend Analysis
SAP Ariba Strategic Sourcing Suite
SAP Ariba Supplier Information and Performance Management
SAP Ariba Supplier Lifecycle and Performance
SAP Ariba Supplier Risk

Prerequisites, Restrictions, Cautions



Prerequisites

- You must be a member of the **Customer Administrator** group with **Third Party Enterprise User (Ariba)** type
- Gather SAML metadata from your identity provider that you need to upload.

Restrictions

- 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.
- You can enable or update the SAML authentication settings from test sites only. You can't update them in production sites.

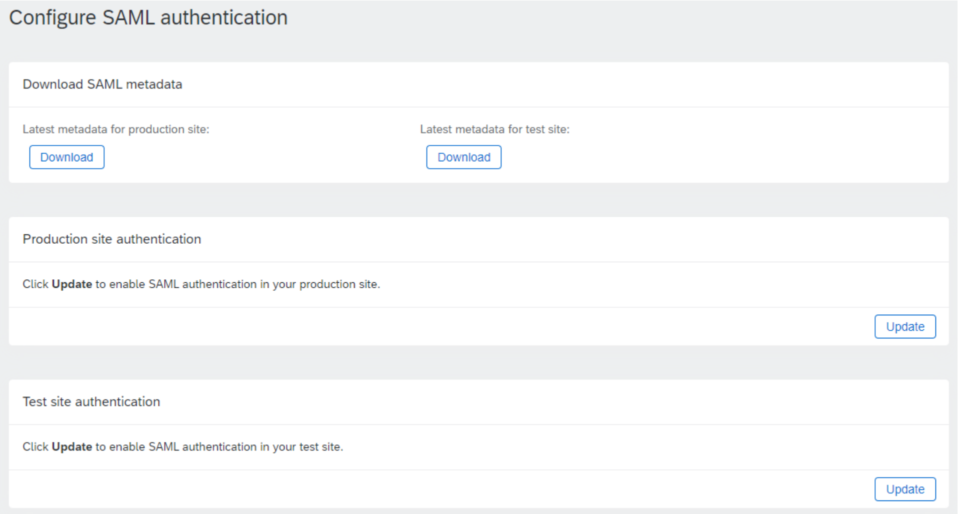
Cautions

- Before updating the authentication configuration, make sure you have the third-party user access credentials. For details about adding a third-party user, refer to Adding Users and Updating User Information.

User Story

User Story: As a customer administrator in my company, I need to be able enable, disable, configure and update my SAML authentication settings for my SAP Ariba applications.

Many organizations are implementing tougher security measures, such as user authentication policies that require strong passwords and frequent password changes. Remote authentication options such as those offered by the SAP Ariba Suite of on-demand solutions tackle the strong-authentication problem. 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 and then move from application to application transparently without requiring them to log in again.



Configure SAML authentication

Download SAML metadata

Latest metadata for production site:

Download

Latest metadata for test site:

Download

Production site authentication

Click **Update** to enable SAML authentication in your production site.

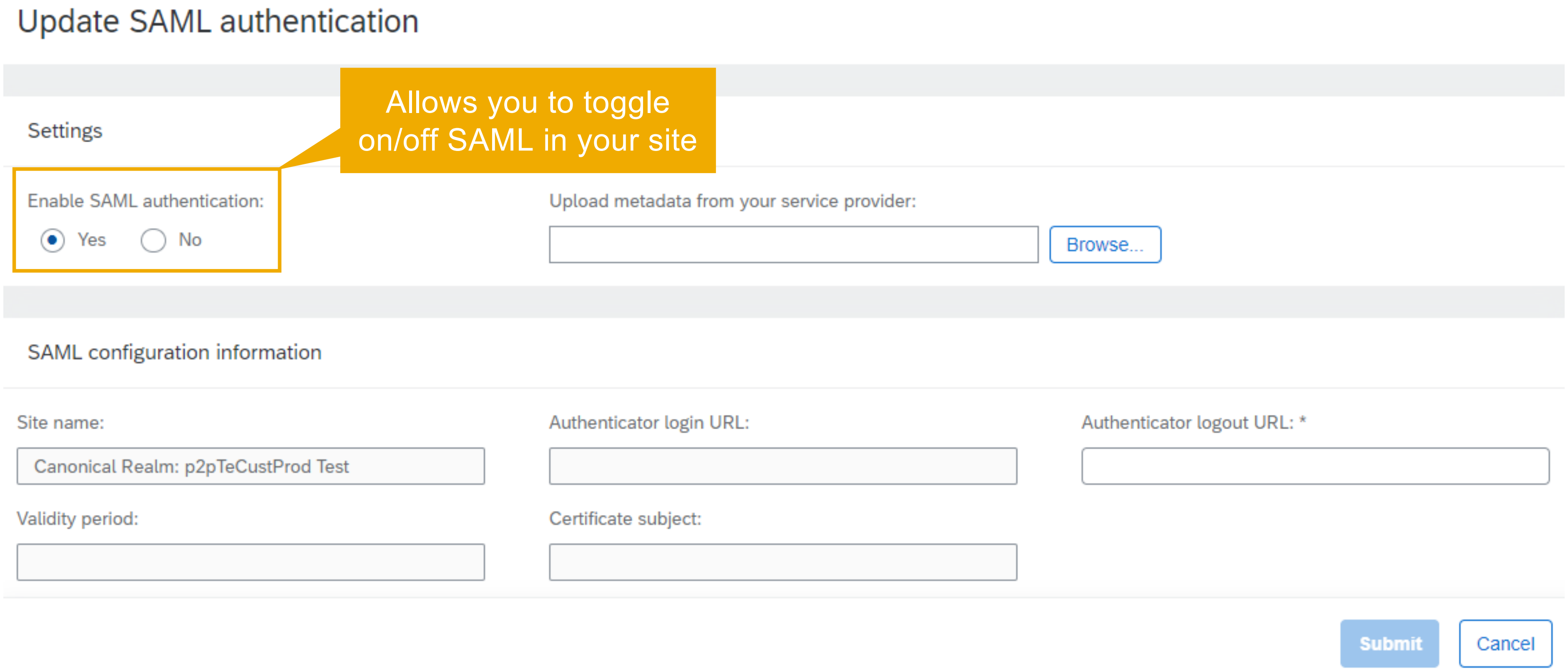
Update

Test site authentication

Click **Update** to enable SAML authentication in your test site.

Update

Feature Details – Enabling SAML



Update SAML authentication

Settings

Enable SAML authentication:

● Yes ○ No

Allows you to toggle on/off SAML in your site

Upload metadata from your service provider:

SAML configuration information

Site name: Canonical Realm: p2pTeCustProd Test

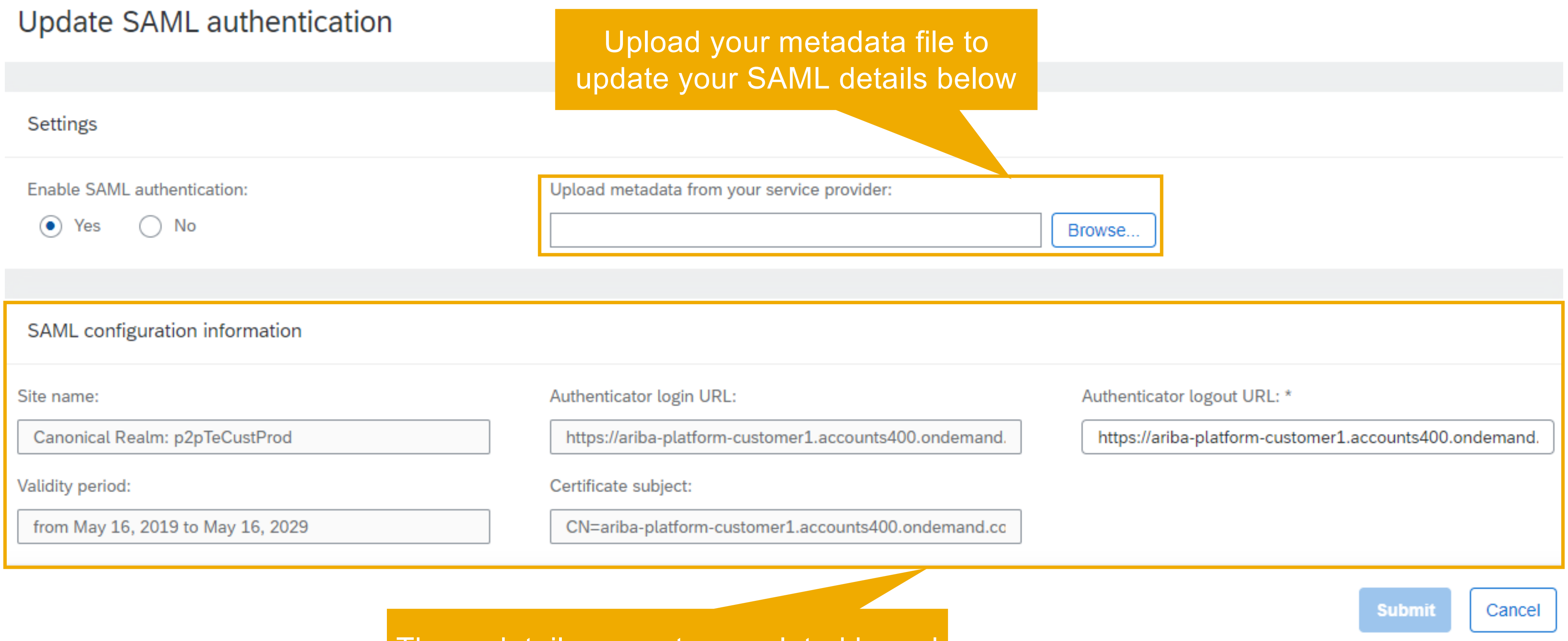
Authenticator login URL:

Authenticator logout URL: *

Validity period:

Certificate subject:

Feature Details – Updating SAML



Update SAML authentication

Settings

Enable SAML authentication:

● Yes ○ No

Upload metadata from your service provider:

Upload your metadata file to update your SAML details below

SAML configuration information

Site name:	Authenticator login URL:	Authenticator logout URL: *
Canonical Realm: p2pTeCustProd	https://ariba-platform-customer1.accounts400.ondemand.	https://ariba-platform-customer1.accounts400.ondemand.
Validity period:	Certificate subject:	
from May 16, 2019 to May 16, 2029	CN=ariba-platform-customer1.accounts400.ondemand.cc	

These details are auto-populated based on the file that is uploaded above

THE BEST RUN

Follow us

www.sap.com/contactsap

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary. These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.   In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions. SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. See www.sap.com/trademark for additional trademark information and notices.

THE BEST RUN SAP