SAP Ariba

Feature at a Glance

Application Gateway: Supplier access to non-SAP Ariba applications via Single Sign On

Richard Vermeij and Chris Chase, SAP Ariba
Target GA: May 2020

PUBLIC

THE BEST RUN SAP

Feature at a Glance

Ease of implementation High touch
Geographic relevance Global

Introducing: **Application Gateway: Supplier access to non-SAP Ariba applications via Single Sign On**

Customer challenge

Some buying organizations that use Ariba Network may have additional supplier-facing applications that require supplier access.

Meet that challenge with SAP Ariba

- This release introduces Ariba Network as an Application Gateway providing suppliers with access to buyer managed applications through Single Sign On (SSO).
- Buyers may manage suppliers SSO access to each application via a csv upload.
- Buyers may refine supplier user access via Ariba Network supplier permissions.

Experience key benefits

- Suppliers have easy access to applications that complement Ariba Network.
- Supplier users have fewer credentials to remember.
- Buyer organization may consolidate supplier access into single supplier portal.
- Buyer organizations may lower supplier user management cost.

Solution area

Ariba Network, buying organizations

Implementation information

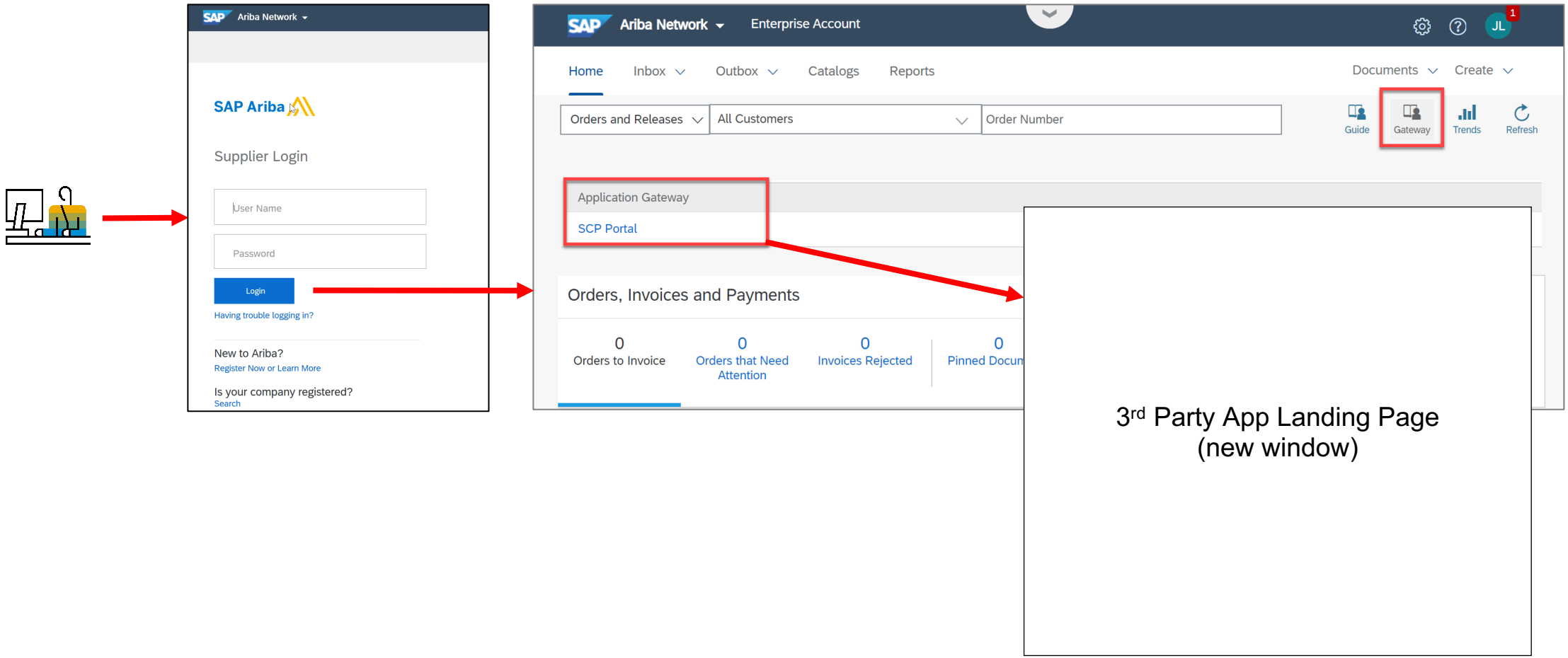
To have this feature enabled, please have your Designated Support Contact (DSC) submit a Commercial Request with your SAP Ariba Customer Engagement Executive or Services Sales Engagement Manager.

Prerequisites and Restrictions

- 3rd party application must accept Ariba Network as Identity Provider (SAML 2.0).
- Only static 3rd party application links are supported (i.e. no run-time parameters).
- Buyers must provision supplier users in the 3rd party application (with permissions).
- Ariba support will not process (i.e. close) service request from supplier users related to the 3rd party application itself.

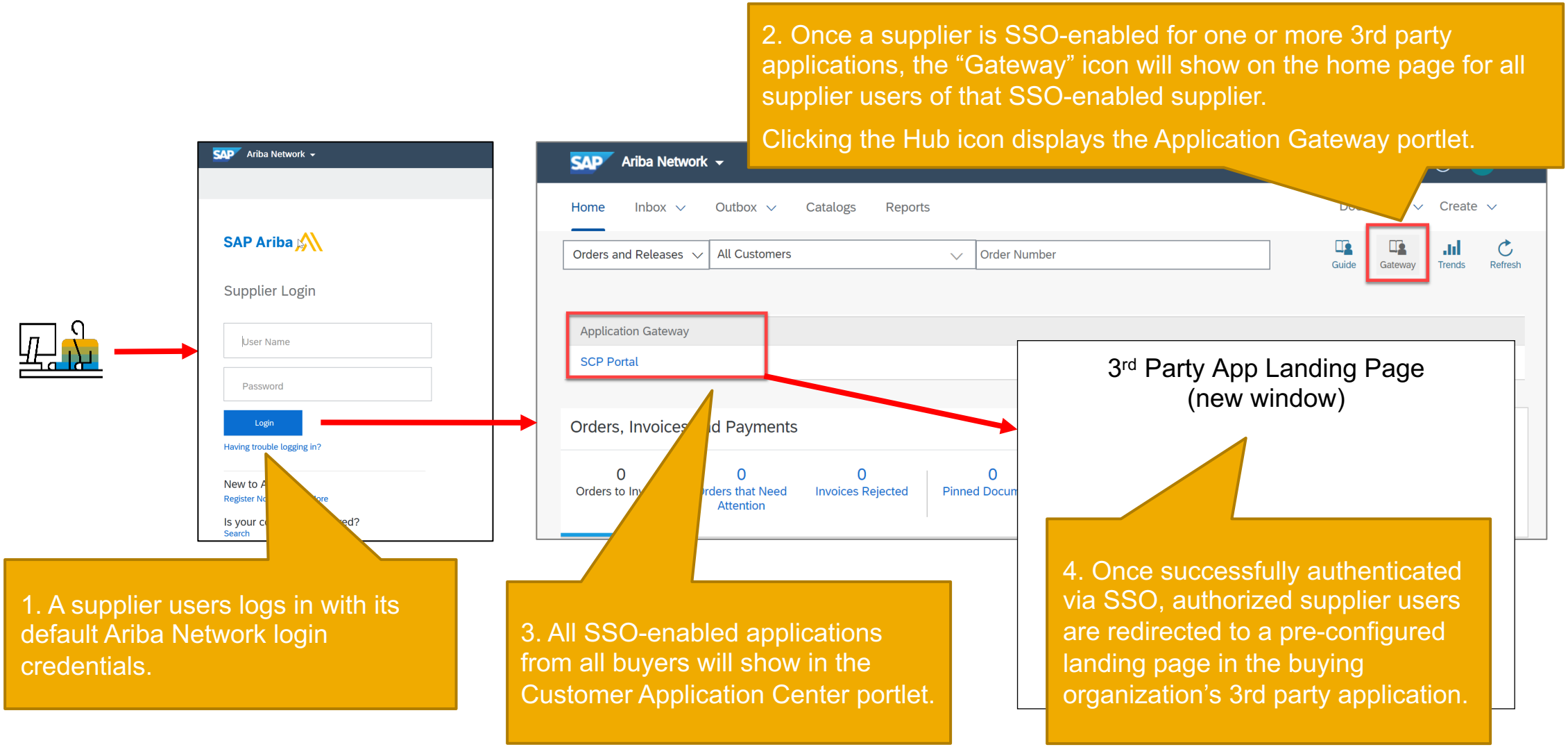
Feature at a Glance

Introducing: **Application Gateway: Supplier access to non-SAP Ariba applications via Single Sign On**



Feature at a Glance

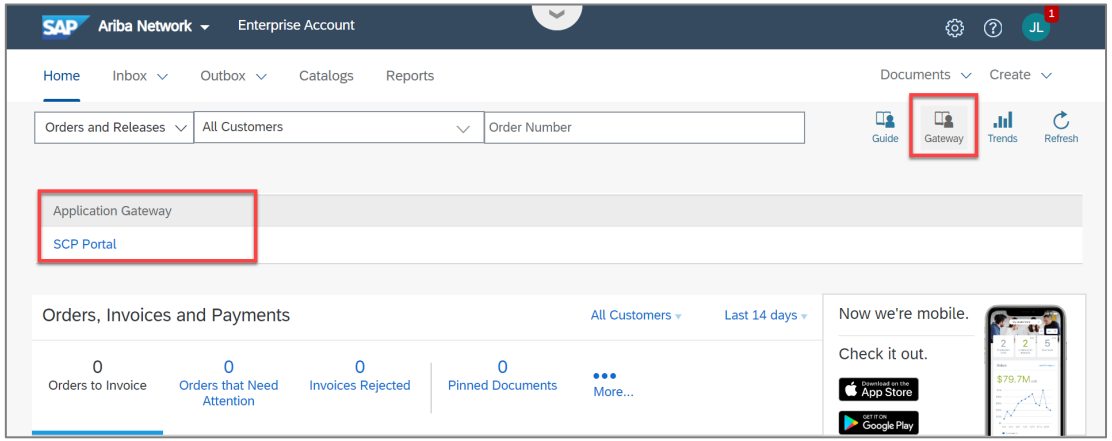
Introducing: **Application Gateway: Supplier access to non-SAP Ariba applications via Single Sign On**



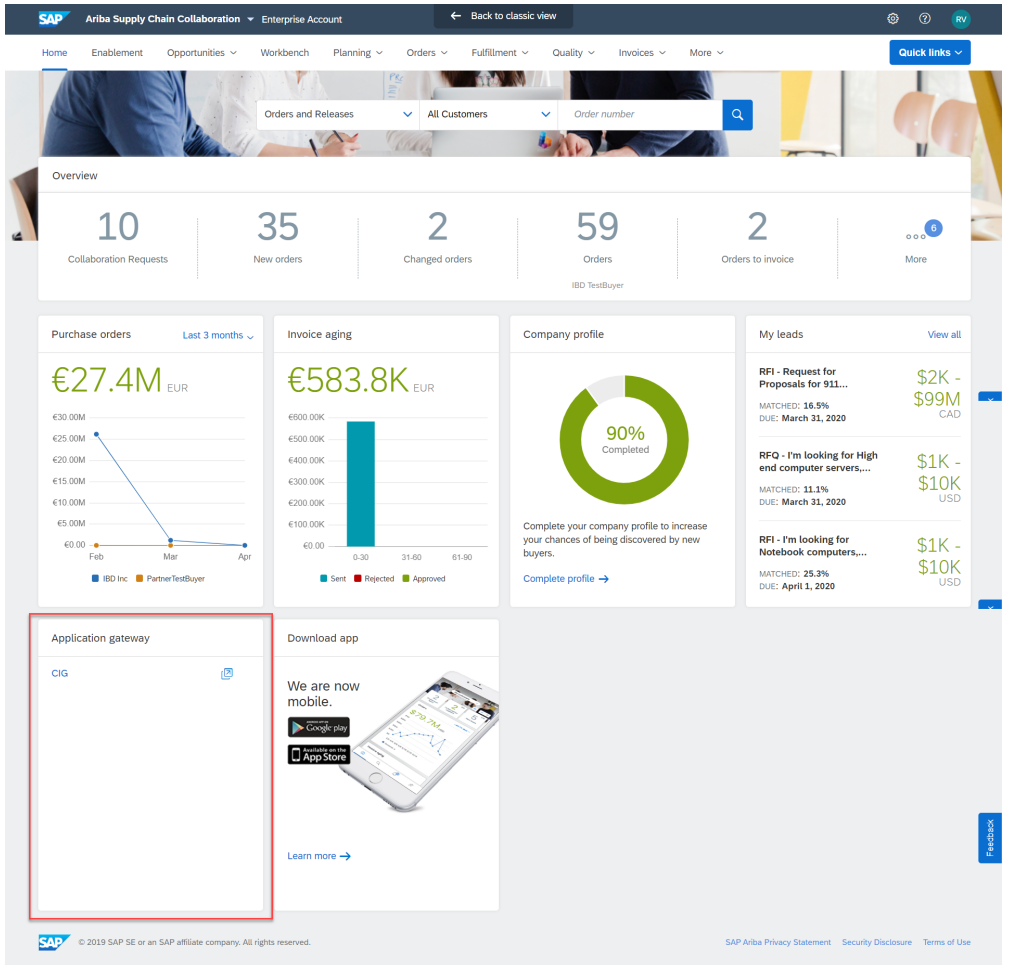
Feature at a Glance

Introducing: **Application Gateway: Supplier access to non-SAP Ariba applications via Single Sign On**

Current Supplier User Experience



Planned GA 3Q20: New Supplier Experience



Application Gateway is available in both supplier enterprise accounts and in standard accounts.

Feature at a Glance

Introducing: **Application Gateway: Supplier access to non-SAP Ariba applications via Single Sign On**

Detailed feature information

Commercial requirements

- To implement this feature, the customer needs to have a valid Ariba Network buyer license.

Enablement

- To have this feature enabled, a customer needs to submit a Commercial Request with the SAP Ariba Customer Engagement Executive or Services Sales Engagement Manager. Ariba Services will work with customer to scope out the configuration of the Ariba Network buyer account service and to support integration testing with customer's 3rd party applications. This results in a commercial service proposal.

Technical requirements

- This feature is solely designed for Ariba Network as Identity Provider (IdP) for supplier authentication; does not support architectures using a buying organization's or 3rd party IdP to authenticate the supplier user.
- The 3rd party system needs to be a cloud solution, i.e. accessible via a browser. The feature is not (yet) designed or tested for SSO to on-premises systems.
- The 3rd party system needs to support SAML 2.0 SSO authentication. Note: SAML 2.0 is not backwards compatible to SAML1.x.

Configuration & deployment

- Setup/configuration of this feature in the Ariba Network buyer account can only be performed by Ariba Services, based on the SOW in the commercial service proposal and configuration parameters provided by the customer.
- Setup/configuration of the 3rd party application for consumption of Ariba Network as Identity Service Provider is the responsibility of the customer or it's system integration partner.
- Testing is the responsibility of the customer, with help of Ariba services to verify the SAML assertion is posted.

Feature at a Glance

Introducing: **Application Gateway: Supplier access to non-SAP Ariba applications via Single Sign On**

Detailed feature information

Access and permission management

- The buying organization determines which suppliers are SSO enabled to which specific 3rd party application as part of the initial configuration.
- The supplier admin of the authorized supplier configures which supplier users are authorized to access the buying organization's 3rd party applications by assigning designated role(s) to applicable users.
- Assigning suppliers to each application is the responsibility of the buyer organization.

Supplier experience

- The Gateway / Application widget is displayed on the Ariba Network home page for all supplier users of a supplier that is SSO-enabled by one or more of its buyers. All buyers applications for which the supplier is SSO-enabled show within the Application Gateway.
- Unauthorized users from SSO-enabled suppliers will see an error message when trying to access an application link in the Application Gateway.

Best Practice

- To reduce user provisioning effort, your SSO enabled application may create new users on the fly when Ariba supplier users click on the application link on the Ariba Network. After your application creates the user with the default role and set of permissions, your 3rd party application administrator should refine the user's privileges according to your process in application.

Support

- Ariba provides L2 tech support for the SSO configuration and posting, by having your Designated Support Contact file a Service Request.
- Ariba support will close service requests logged by supplier users related to 3rd party business questions or functional problems.

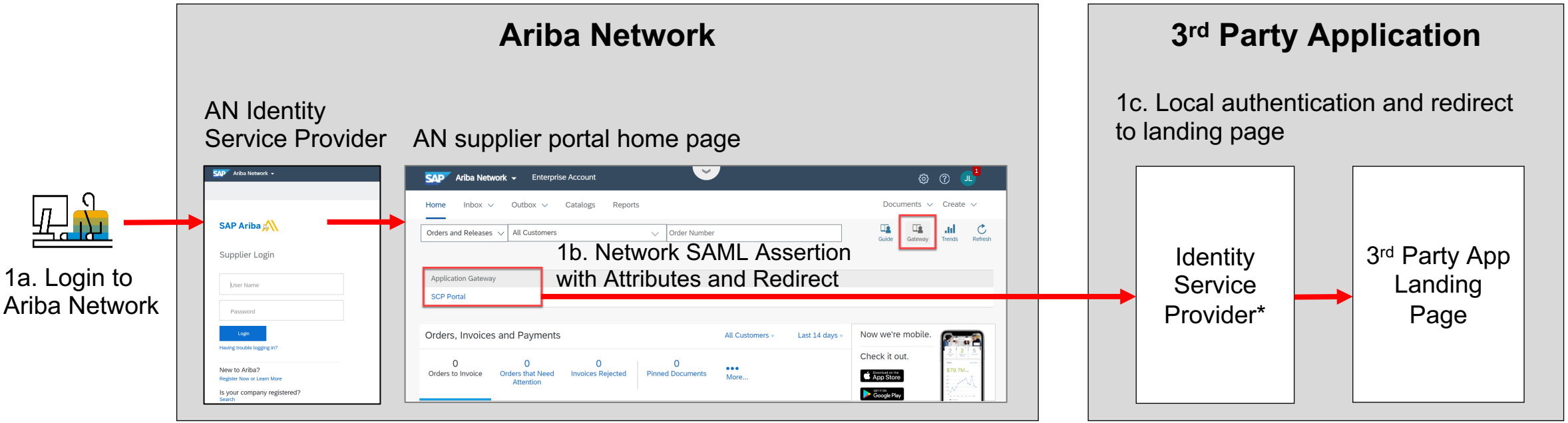
Feature at a Glance

Introducing: **Application Gateway: Supplier access to non-SAP Ariba applications via Single Sign On**

Solution Architecture Diagram

Scenario 1: Network Initiated Login

1a) Supplier user logs into Ariba Network (AN) via http://supplier.ariba.com with AN credentials. 1b) User clicks buyer's App URL in Application Gateway, which posts SAML assertion incl destination URL to localIdentity Service Provider. 1c) After automatic completion of local authentication, user is redirected to 3rd party app landing page (with 3rd party app roles/permissions).



*Local Identity Service Provider needs to support Ariba Network as Identity Provider using SAML 2.0

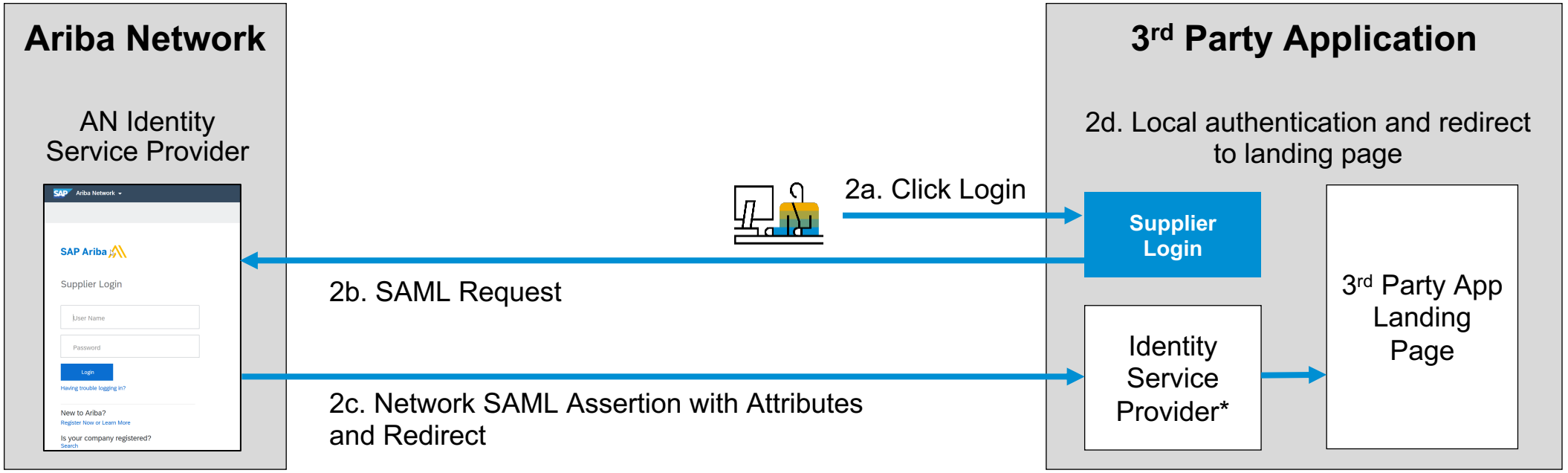
Feature at a Glance

Introducing: **Application Gateway: Supplier access to non-SAP Ariba applications via Single Sign On**

Solution Architecture Diagram

Scenario 2: Service Provider Initiated Login

2a) Supplier user initiates login in 3rd party application, which triggers SAML request to Ariba Network Identity Service Provider. 2b) User will be provided with AN login page and user enters Ariba Network login credentials. 2c) AN Identity Service Provider responds with SAML assertion to 3rd party Identity Service Provider, which 2d) completes local authentication and redirects user to 3rd party application landing page.



*Local Identity Service Provider needs to support Ariba Network as Identity Provider using SAML 2.0

Feature at a Glance

Introducing: **Application Gateway: Supplier access to non-SAP Ariba applications via Single Sign On**

Solution Deployment by Ariba Services – AN Buyer Acct Config

Ariba Application Gateway Configuration Request Form

1. ..
2. IdP end point URL
3. IdP Identity
4. IdP Certificate
5. Landing Page URL
6. ..

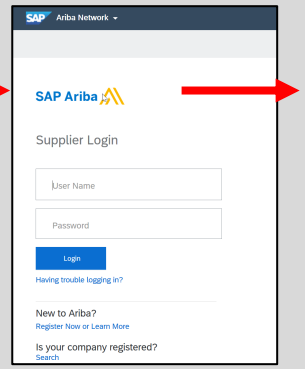
AN Buyer Acct configuration by Ariba Services

1. AN IdP Certificate

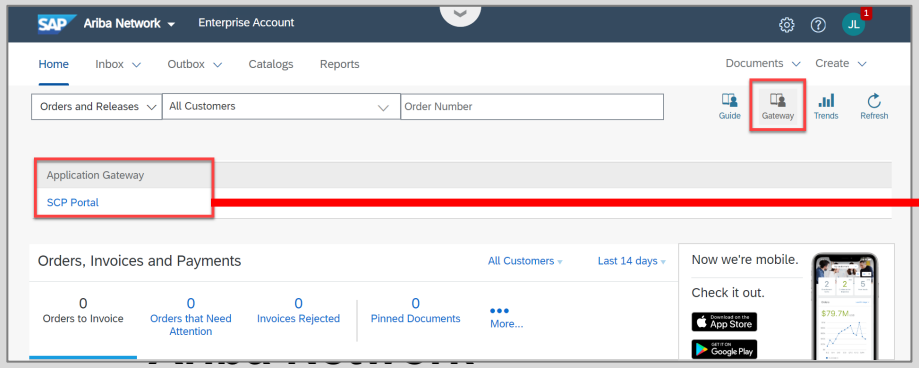
3rd Party Application

1a. Login to Ariba Network

AN Identity Service Provider



AN supplier portal home page



Identity Service Provider*

3rd Party App Landing Page

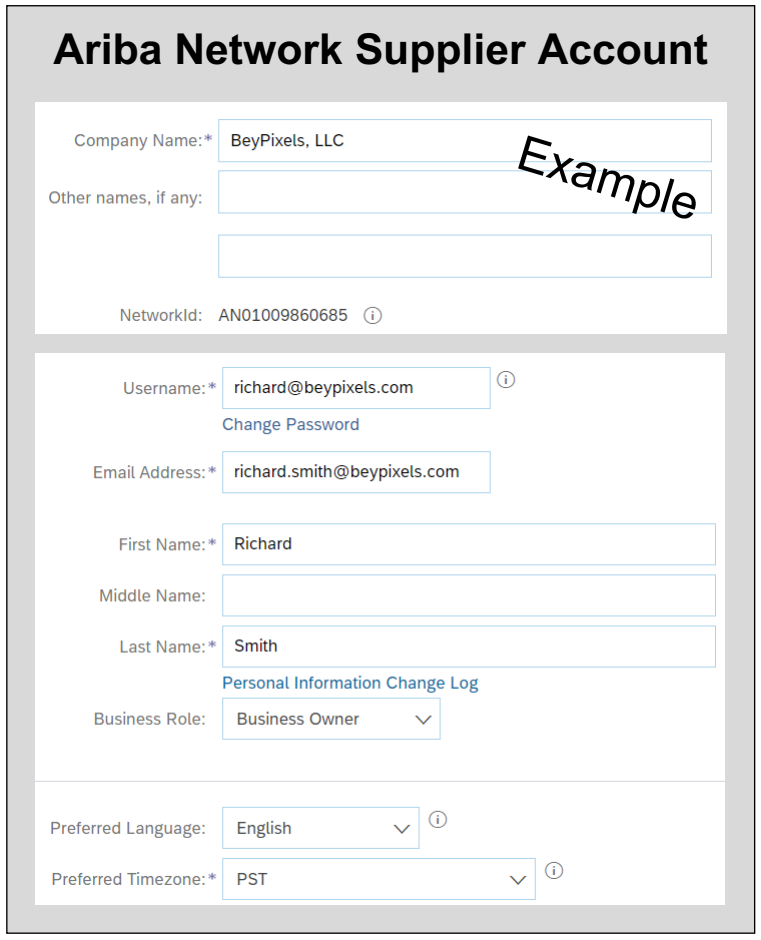
*Local Identity Service Provider needs to support Ariba Network as Identity Provider using SAML 2.0

Feature at a Glance

Introducing: **Application Gateway: Supplier access to non-SAP Ariba applications via Single Sign On**

Solution Deployment by Ariba Service – Available SAML Assertion Attributes + Example

Ariba Network Supplier Account



AN Buyer Acct Config Parameters

Config Parameter	Example XML Value
ANID	AN01009860685
Name	(first+SPACE+last name)
ContactEmail	richard.smith@beypixels.com
UserID	richard@beypixels.com
ContactFirstName	Richard
ContactLastName	Smith
ContactPhone	
CompanyName	BeyPixels, LLC
UserTimeZone	America/Los_Angeles
Permissions	(in AN supplier account)
DunsNumber	(supplier entered DUNS)
MktDunsNumber	(supplier entered DUNS)

Ariba Network SAML Assertion

```
samlp:Response
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol“
Destination=https://xxxxxx.accounts.ondemand.com/
ID="_1111148449520-398041260975918169.10.162.97.207"
IssueInstant="2020-03-26T18:47:29.520Z“ Version="2.0“>

<saml:Issuerxmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://service.ariba.com</saml:Issuer>

[…]

<saml:AttributeStatement>

    <saml:Attribute Name="CompanyName“
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">

        <saml:AttributeValue
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:type="xs:string">BeyPixels, LLC
        </saml:AttributeValue>

    </saml:Attribute>

</saml:AttributeStatement>

[…]
```

Feature at a Glance

Introducing: **Application Gateway: Supplier access to non-SAP Ariba applications via Single Sign On**

Solution Deployment by Ariba Service – Auto-Subscribing suppliers by ANID

AN Buyer Acct Config Parameters

Parameter Name	Description
AutoSubscribeTradingRelSuppliers	Set to “True” if all Ariba Network transacting suppliers should have access to the application. Suppliers Relationships created prior to setting this parameter still require the buyer to establish a relationship between application and supplier ANID through the csv load.
AutoSubscribeSourcingRelSuppliers	Set to “True” if all Ariba Sourcing / SLP / Risk suppliers should have access to the application. Suppliers Relationships created prior to setting this parameter still require the buyer to establish a relationship between application and supplier ANID through the csv load.
ViewAccess	Set to an ariba network permission if role based authentication is necessary. For example,… • For SES - "OrderManagement_InboxAccess","Inbox and Order Access" • For Quote - "Mkt_SupplierView","Respond to postings on Ariba Discovery"

Example best practice – Auto Subscribe

Buyer wants all user of all suppliers to have access to App1, only all supplier users enabled for Commerce Automation to App2, and only all user of select suppliers to App3

1. For App1, use cvs to enable all current suppliers (E.g. pull ANIDs from AN supplier enablement status report) + set AutoSubscribeTradingRelSuppliers=True + set AutoSubscribeSourcingRelSuppliers=True
2. For App2, use cvs to enable all current suppliers + set AutoSubscribeTradingRelSuppliers=True
3. For App3, use cvs to enable all selected suppliers

Feature at a Glance

Introducing: **Application Gateway: Supplier access to non-SAP Ariba applications via Single Sign On**

Solution Deployment by Ariba Service – ViewAccess for Supplier User Access Control

AN Buyer Acct Config Parameters

Parameter Name	Description
AutoSubscribeTradingRelSuppliers	Set to “True” if all Ariba Network transacting suppliers should have access to the application. Suppliers Relationships created prior to setting this parameter still require the buyer to establish a relationship between application and supplier ANID through the csv load.
AutoSubscribeSourcingRelSuppliers	Set to “True” if all Ariba Sourcing / SLP / Risk suppliers should have access to the application. Suppliers Relationships created prior to setting this parameter still require the buyer to establish a relationship between application and supplier ANID through the csv load.
ViewAccess	Set to an ariba network permission if role based authentication is necessary. For example,… • For SES - "OrderManagement_InboxAccess","Inbox and Order Access" • For Quote - "Mkt_SupplierView","Respond to postings on Ariba Discovery"

Example best practice - ViewAccess

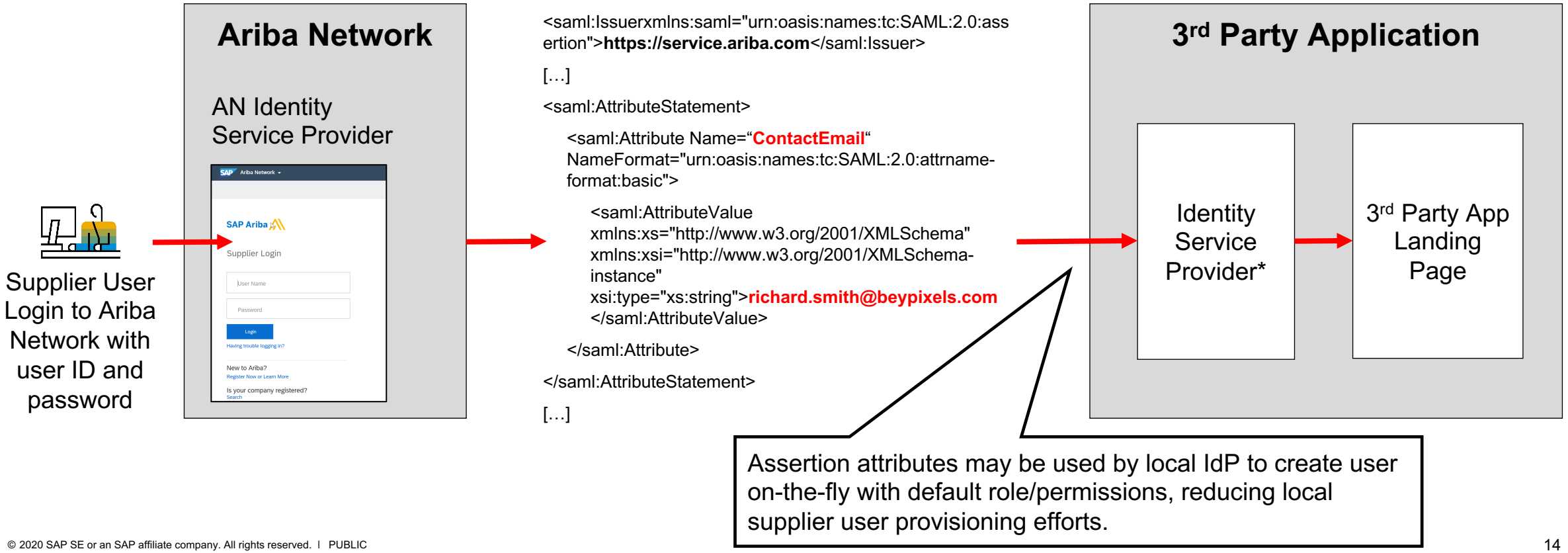
Buyer wants to provide all subscribed suppliers admins the ability to further limit buyer App1 SSO access to QM users, and App2 SSO to QM users and SCC users.

1. For App1, set ViewAccess= Quality_Notification_Create and instruct all subscribed suppliers to assign “Quality_Notification_Create” permission to role of their internal QM users who need access.
2. For App2, set ViewAccess= Quality_Notification_Create, Inventory_Collaboration_Visibility and instruct all subscribed suppliers to assign “Quality_Notification_Create” permission to QM user role, and assign “Inventory_Collaboration_Visibility” to SCC user role.

Feature at a Glance

Introducing: **Application Gateway: Supplier access to non-SAP Ariba applications via Single Sign On**

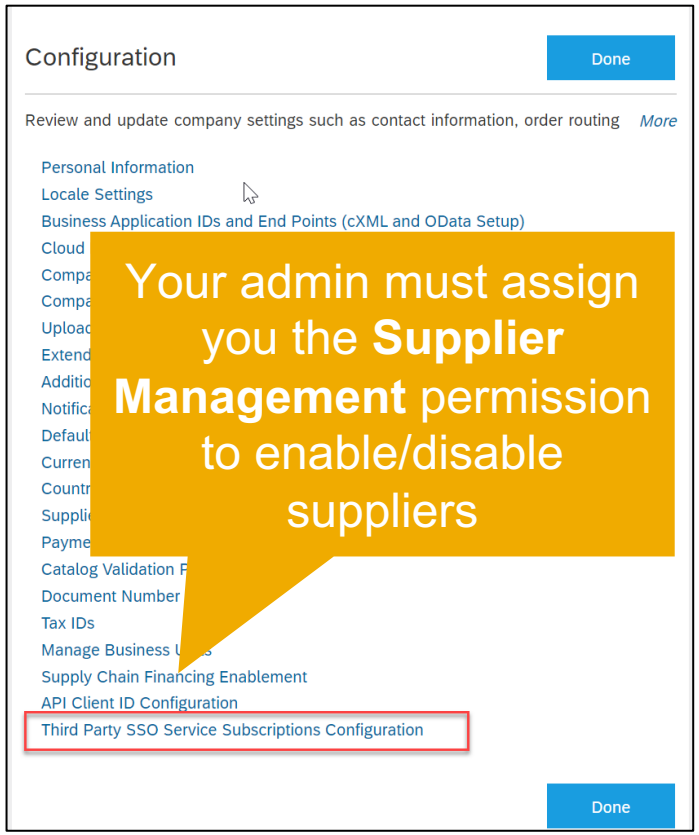
Solution Deployment – Buyer May Implement On-The-Fly User Creation w default Role/Permissions

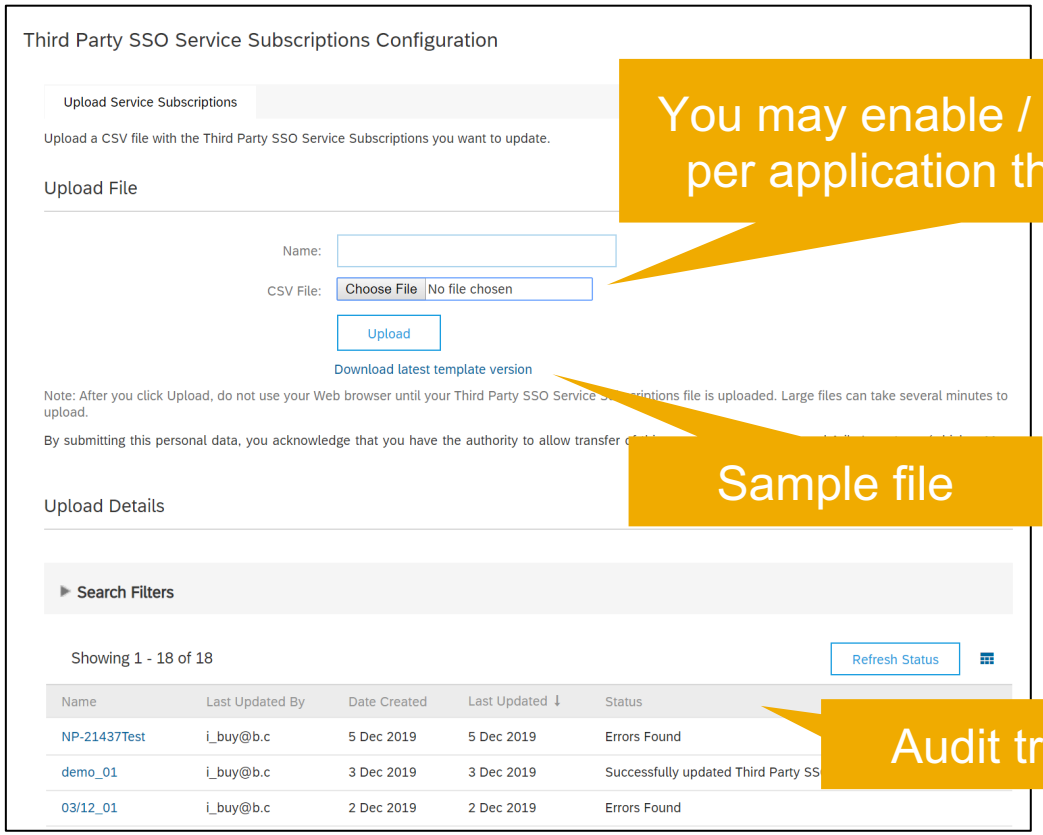


Feature at a Glance

Introducing: **Application Gateway: Supplier access to non-SAP Ariba applications via Single Sign On**

Access and Permission Management – Subscribing suppliers by ANID in Buyer Ariba Network Account





Feature at a Glance

Introducing: **Application Gateway: Supplier access to non-SAP Ariba applications via Single Sign On**

Access and Permission Management – Subscribing suppliers by ANID in Buyer Ariba Network Account

	A	B	C
1	UTF-8		
2	Service Id	Supplier ANID	Operation
3	Required	Required	Required
4	String 150	AN01999999999	String (must match pre-configured value)
5	ACME_QM1	AN02000844410	Enabled
6	ACME_INV1	AN02000844410	Enabled
7	ACME_QM1	AN03000934523	Enabled
8	ACME_INV1	AN03000934523	Disabled

There are 3 columns required to load

- ServiceID is your application
- Supplier ANID
- Operation: You may either Enable or Disable the supplier by ANID

After successfully uploading above CVS file, the supplier SSO subscription status is as follows:

- All users of supplier 1 with ANID:AN02000844410 see the App links associated w SSO service ACME_QM1 and ACME_INV1
- All users of supplier 2 with ANID:AN03000934523 see the App link associated w SSO service ACME_QM1 but not/no longer SSO service ACME_INV1

SAP Ariba

Follow us

www.sap.com/contactsap

THE BEST RUN SAP