



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

# 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

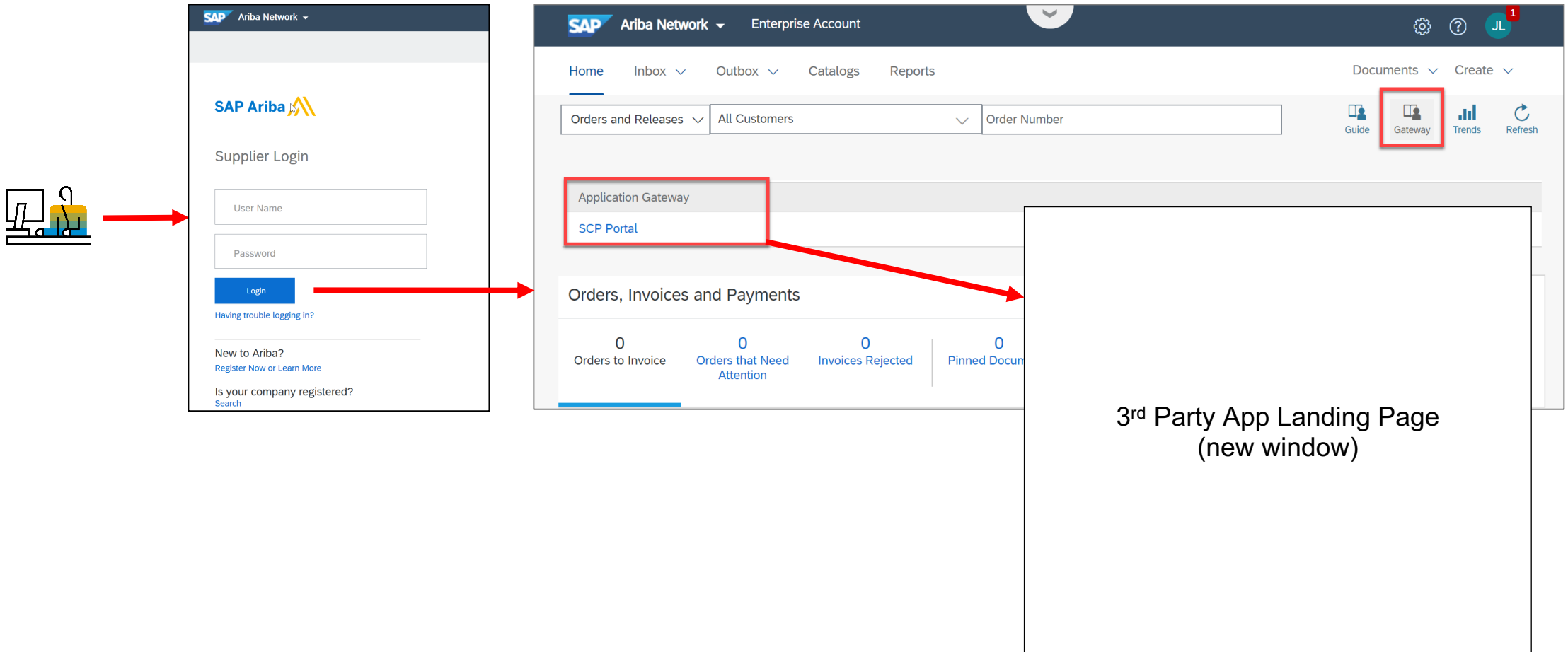
To have this feature enabled, please have your Designated Support Contact (DSC) submit a Commercial Request with your SAP Ariba Customer Engagement Executive or Services Sales Engagement Manager.

### Prerequisites and Restrictions

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

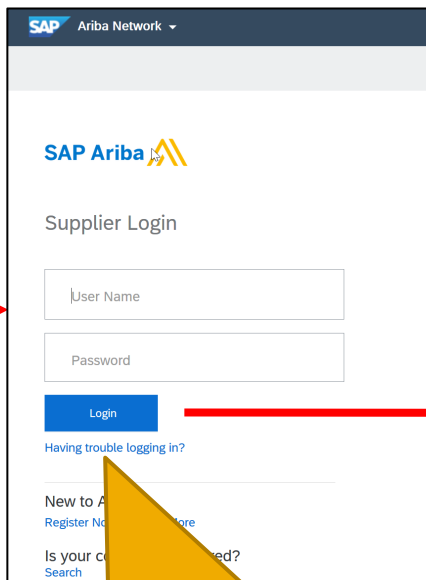
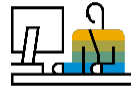
# Feature at a Glance

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

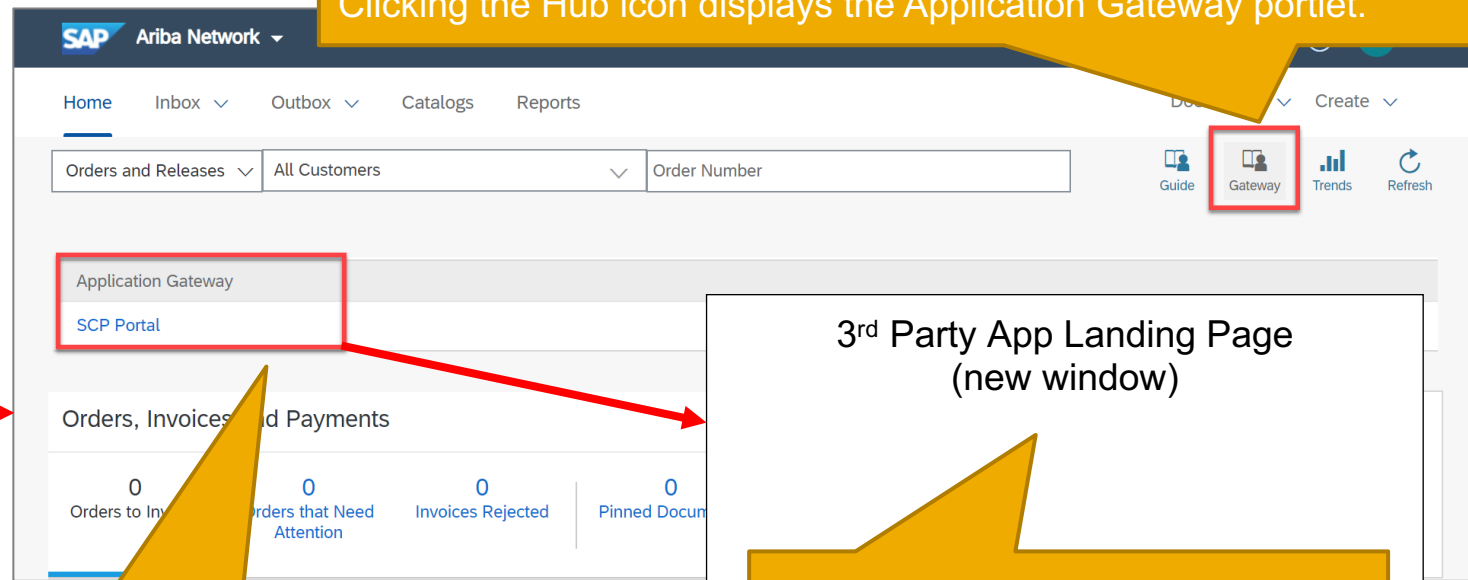


# Feature at a Glance

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



1. A supplier user logs in with its default Ariba Network login credentials.



2. Once a supplier is SSO-enabled for one or more 3rd party applications, the "Gateway" icon will show on the home page for all supplier users of that SSO-enabled supplier.

Clicking the Hub icon displays the Application Gateway portlet.

3. All SSO-enabled applications from all buyers will show in the Customer Application Center portlet.

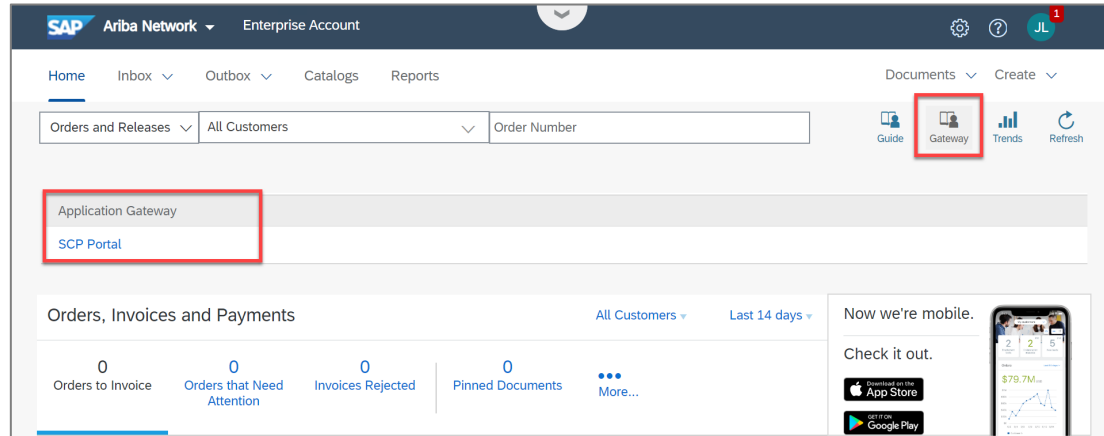
3rd Party App Landing Page  
(new window)

4. Once successfully authenticated via SSO, authorized supplier users are redirected to a pre-configured landing page in the buying organization's 3rd party application.

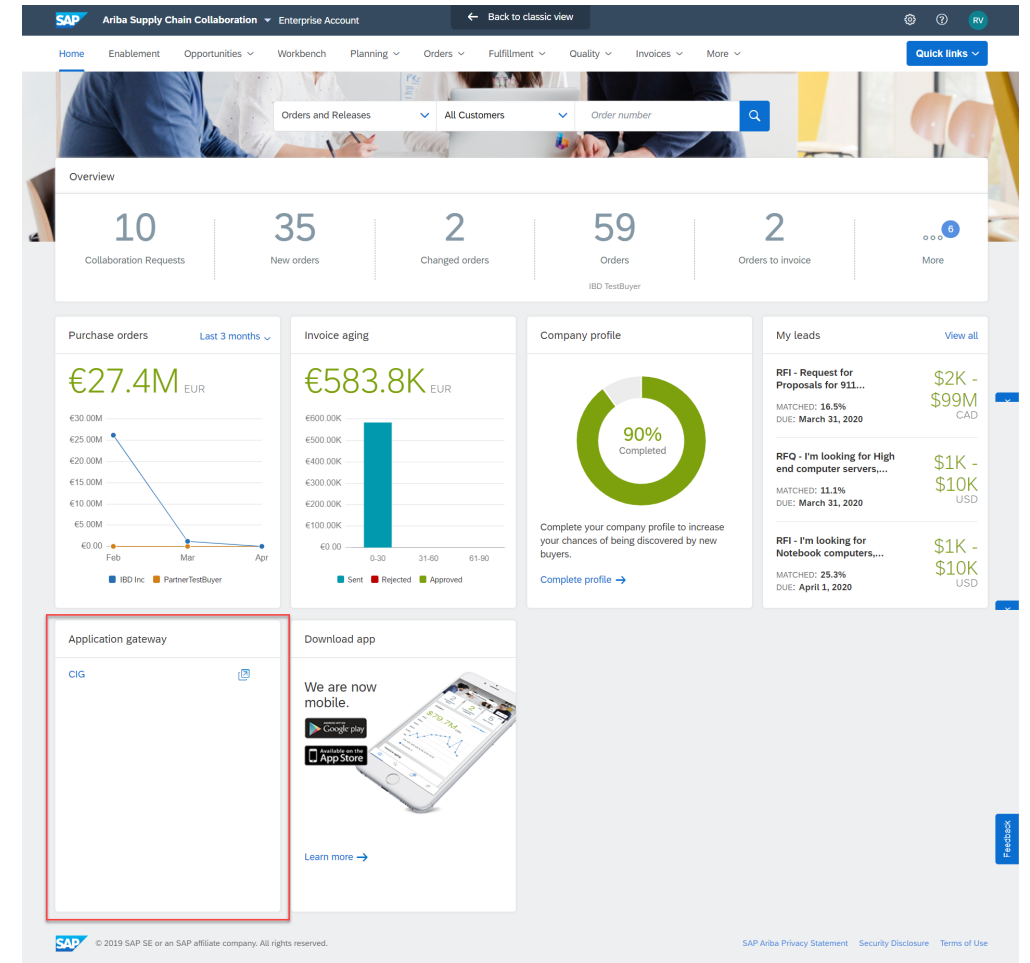
# Feature at a Glance

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 3<sup>rd</sup> 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 3<sup>rd</sup> party IdP to authenticate the supplier user.
- The 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> party business questions or functional problems.

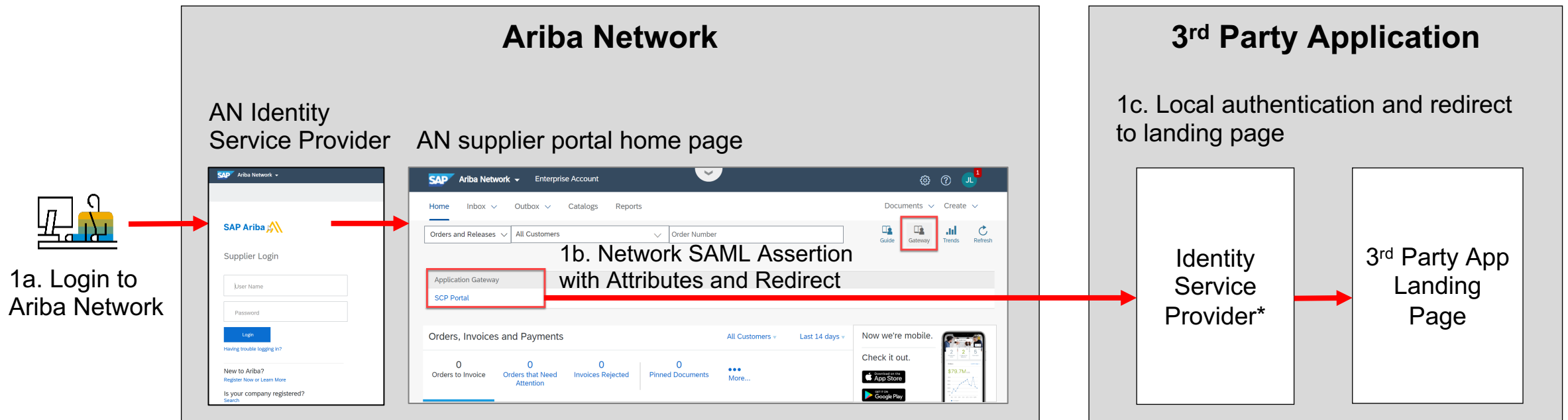
# Feature at a Glance

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 local Identity Service Provider. 1c) After automatic completion of local authentication, user is redirected to 3<sup>rd</sup> party app landing page (with 3<sup>rd</sup> party app roles/permissions).



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



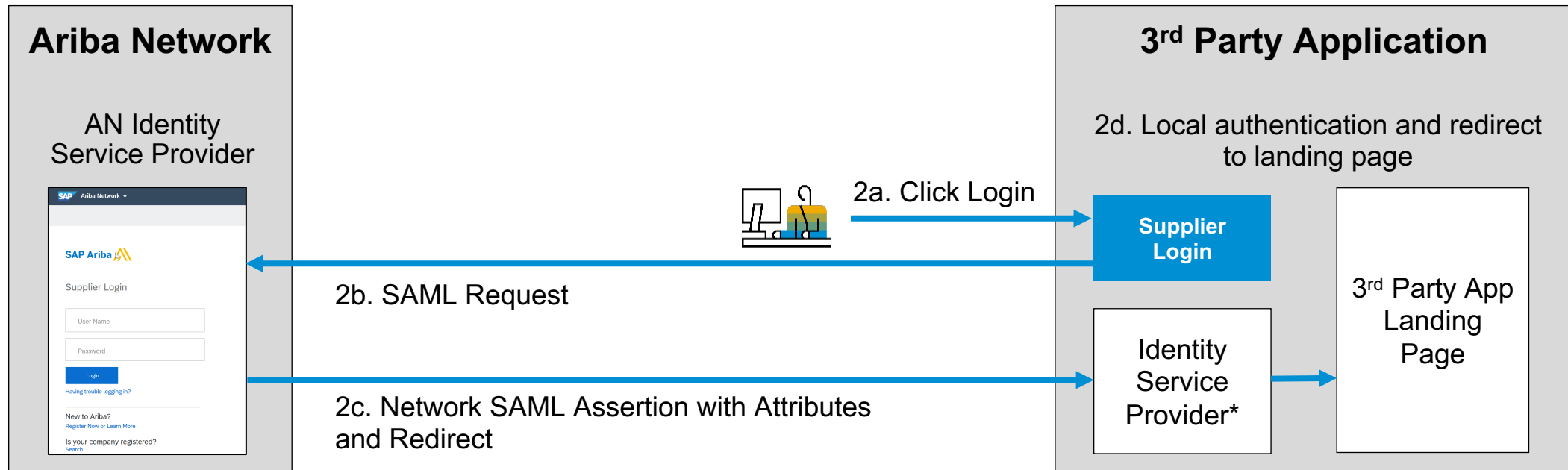
# Feature at a Glance

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 3<sup>rd</sup> 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 3<sup>rd</sup> party Identity Service Provider, which 2d) completes local authentication and redirects user to 3<sup>rd</sup> party application landing page.



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

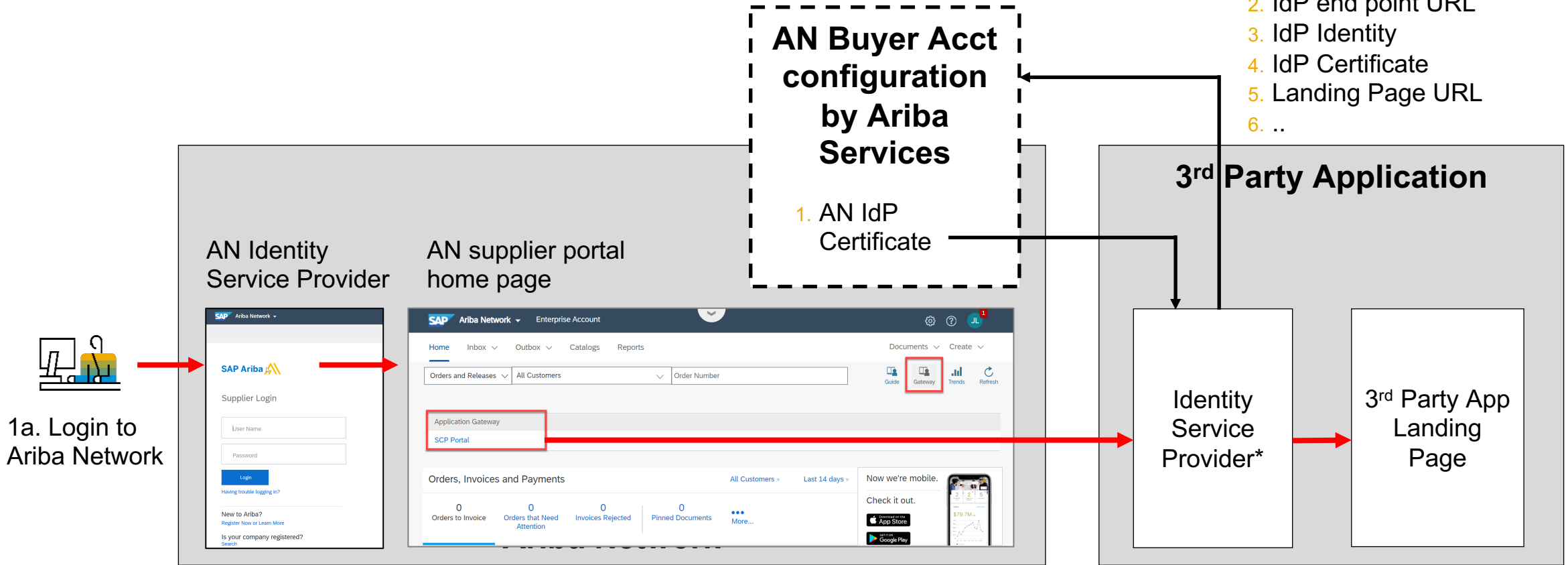
# Feature at a Glance

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. ..



\*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

Company Name: \*  Example

Other names, if any:

NetworkId: AN01009860685 ⓘ

Username: \*  ⓘ

[Change Password](#)

Email Address: \*

First Name: \*

Middle Name:

Last Name: \*

[Personal Information Change Log](#)

Business Role:  ▼

Preferred Language:  ▼ ⓘ

Preferred Timezone: \*  ▼ ⓘ

### 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	
<b>CompanyName</b>	<b>BeyPixels, LLC</b>
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
<b>AutoSubscribeTradingRelSuppliers</b>	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.
<b>AutoSubscribeSourcingRelSuppliers</b>	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.
<b>ViewAccess</b>	Set to an ariba network permission if role based authentication is necessary. For example,... <ul style="list-style-type: none"><li>• For SES - "OrderManagement_InboxAccess","Inbox and Order Access"</li><li>• For Quote - "Mkt_SupplierView","Respond to postings on Ariba Discovery"</li></ul>

### 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
<b>AutoSubscribeTradingRelSuppliers</b>	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.
<b>AutoSubscribeSourcingRelSuppliers</b>	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.
<b>ViewAccess</b>	Set to an ariba network permission if role based authentication is necessary. For example,... <ul style="list-style-type: none"> <li>• For SES - "OrderManagement_InboxAccess","Inbox and Order Access"</li> <li>• For Quote - "Mkt_SupplierView","Respond to postings on Ariba Discovery"</li> </ul>

#### Example best practice - ViewAccess

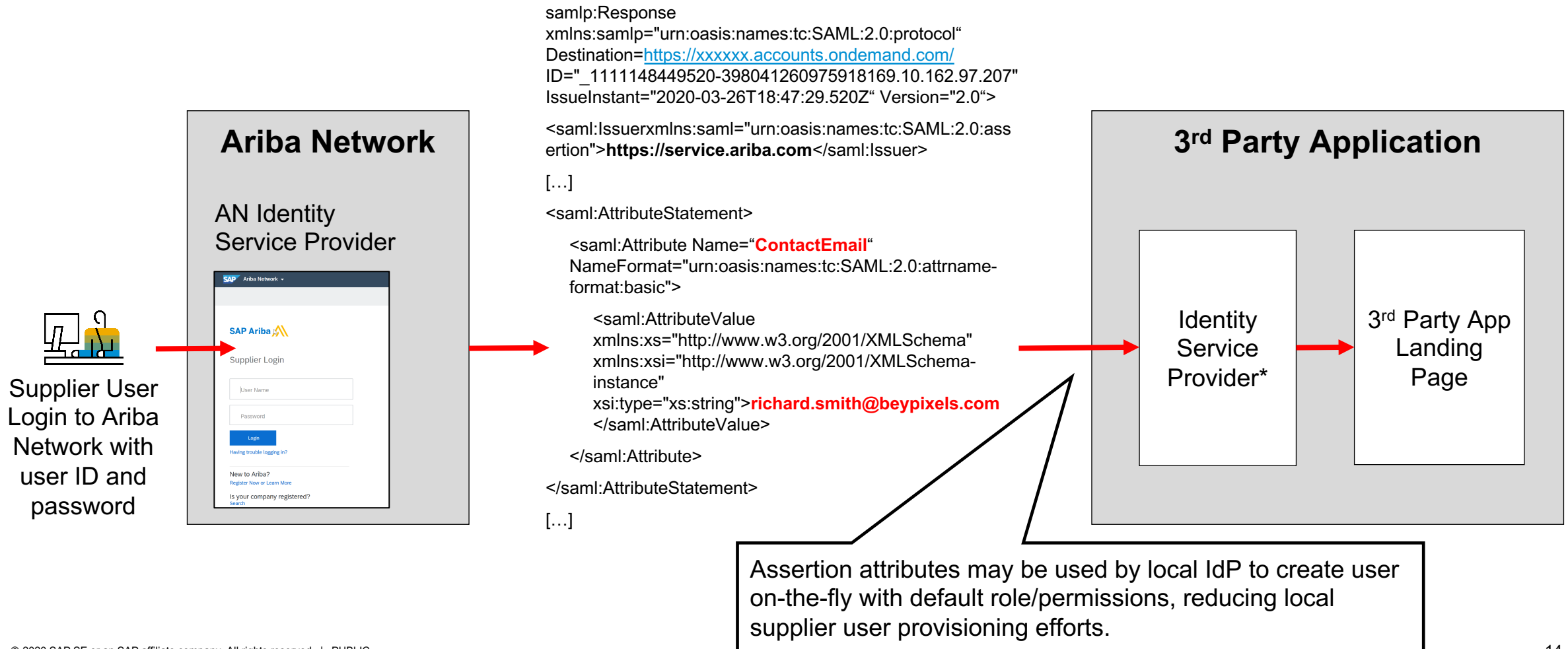
Buyer wants to provide all subscribed suppliers admin the ability to further limit buyer App1 SSO access to QM users, and App2 SSO to QM users and SCC users.

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

Configuration Done

Review and update company settings such as contact information, order routing [More](#)

- Personal Information
- Locale Settings
- Business Application IDs and End Points (cXML and OData Setup)
- Cloud
- Compa
- Compa
- Uploa
- Extend
- Addit
- Notific
- Defaul
- Curren
- Countr
- Suppli
- Payme
- Catalog Validation F
- Document Number
- Tax IDs
- Manage Business Us
- Supply Chain Financing Enablement
- API Client ID Configuration
- Third Party SSO Service Subscriptions Configuration**

Done

**Your admin must assign you the Supplier Management permission to enable/disable suppliers**

Third Party SSO Service Subscriptions Configuration

Upload Service Subscriptions Upload

Upload a CSV file with the Third Party SSO Service Subscriptions you want to update.

Upload File

Name:

CSV File:  No file chosen

[Download latest template version](#)

Note: After you click Upload, do not use your Web browser until your Third Party SSO Service Subscriptions file is uploaded. Large files can take several minutes to upload.

By submitting this personal data, you acknowledge that you have the authority to allow transfer of your personal data to SAP.

Upload Details

► Search Filters

Showing 1 - 18 of 18 Refresh Status

Name	Last Updated By	Date Created	Last Updated ↓	Status
NP-21437Test	i_buy@b.c	5 Dec 2019	5 Dec 2019	Errors Found
demo_01	i_buy@b.c	3 Dec 2019	3 Dec 2019	Successfully updated Third Party SS
03/12_01	i_buy@b.c	2 Dec 2019	2 Dec 2019	Errors Found

**You may enable / disable suppliers per application through a csv file**

**Sample file**

**Audit trail of each load attempt**

## 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



Follow us



[www.sap.com/contactsap](http://www.sap.com/contactsap)

© 2020 SAP SE or an SAP affiliate company. All rights reserved.

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/copyright](http://www.sap.com/copyright) for additional trademark information and notices.