



# Feature at a Glance

## Configure mutual TLS authentication certificates for inbound communications

Rajesh Shastry and Andy Rubinson, SAP Ariba  
Target GA: August, 2021

CONFIDENTIAL

# Feature at a Glance

Ease of implementation  High-touch  
Geographic relevance  Global

## Introducing: **Configure mutual TLS authentication certificates for inbound communications**

### Customer challenge

Until recently SAP Ariba applications provided user id/password and Web service security-based authentication for inbound calls. Although this helps ensure secure communication with external systems, it becomes an issue if the credentials are compromised for user id/password authentication. Also, the Web service security authentication requires additional coding to complete the certificate signing process. There is currently no authentication that ensures the communication is both secure and trusted in both directions between the client and server, opening customers to a potential security breach.

### Solution area

- SAP Ariba Buying
- SAP Ariba Buying and Invoicing
- SAP Ariba Invoice Management
- SAP Ariba Sourcing
- SAP Ariba Contracts
- SAP Ariba Supplier Lifecycle and Performance
- SAP Ariba Strategic Sourcing Suite

### Meet that challenge with **SAP Ariba**

This feature allows customers to configure certificates for mutual Transport Layer Security (TLS) authentication for inbound communications from external systems. Administrators in the customer organization can create new certificate configurations and also search for saved configurations on a new administrator page. In addition to the new page, the administrator page for end point configuration has been enhanced to allow administrators to configure mutual TLS authentication for end points.

### Implementation information

This feature is automatically on for all customers with the applicable solutions but requires **customer configuration**

### Experience key benefits

- Communication is both secure and trusted in both directions between a client and server
- Reduces the overhead of additional coding required for web-service security authentication
- Improves the security of access to SAP Ariba applications
- Ability to choose which configured mutual TLS certificates to use in end point configurations
- Create and manage certificate configuration for specific SAP Ariba applications, giving customers the ability to select the applications they wish to configure with mutual TLS
- Highly scalable
- Ability to add back-up certificates

### Prerequisites and Restrictions

- Mutual authentication works with client certificates issued by any valid certificate authority (CA).
- Ensure that the valid client certificates are stored in the server's truststore.

## Feature at a Glance

Introducing: **Configure mutual TLS authentication certificates for inbound communications**

### Detailed feature information – Brief description

#### Mutual Transport Layer Security (TLS) authentication for inbound SOAP web services

- If mutual authentication is turned on, the client (an SAP Ariba solution) and the server (an external system) exchange certificates over a TLS 1.2 connection to authenticate one another.
- Customer admins can create new certificate configurations per SAP Ariba application.
- Customer admins can add primary certificate to the configuration and also add a back-up certificate as part of the configuration, which will be used if the primary certificate fails.
- Customer admins can either paste or upload the new certificates.
- Certificates that are not expired and are issued by a valid certificate authority can be uploaded.
- Customer admins can select the configured certificate for mutual authentication in the inbound integration end point configuration.

# Feature at a Glance

## Introducing: **Configure mutual TLS authentication certificates for inbound communications**

### Detailed feature information – Create Mutual TLS authentication certificate configuration

Navigation Path: **Integration Manager** → **Mutual TLS Configuration**

The customer admin can do the following operations:

- 1. Search** for an existing inbound / outbound certificate configured for a specific application
- 2. Create new** certificate configuration for a specific application for an inbound certificate
- 3. View** existing inbound or outbound certificates configured for a specific application
- 4. Edit** an existing inbound certificate configured for a specific application

The screenshot shows the SAP Ariba Mutual TLS Configuration interface. The left sidebar contains a navigation menu with 'Integration Manager' and 'Mutual TLS Configuration' highlighted. The main content area is titled 'Mutual TLS Configuration' and includes a search section with filters for Name, Type (No Choice, Inbound, Outbound), and Application Name. Below the search filters is a table listing existing certificates. Red circles and blue boxes highlight specific UI elements: (1) Search and List All buttons, (2) Create New button, (3) TestSYS1 row, and (4) Edit buttons for TestSYS1 and TestSYS2 rows.

| Name     | Type     | Application Name |
|----------|----------|------------------|
| TestSYS1 | Inbound  | App8             |
| TestSYS2 | Outbound | Buyer            |

# Feature at a Glance

Introducing: **Configure mutual TLS authentication certificates for inbound communications**

## Detailed feature information – Create Mutual TLS authentication certificate configuration

Navigation Path: **Integration Manager** → **Mutual TLS Configuration** → **Create New**

The customer admin can create new certificate configuration for a specific application by entering

- **Name** of the certificate configuration which must be unique.
- **Type** of communication as 'Inbound'.
- **Application Name** for which the certificate configuration is created.
- **Primary certificate** is required and the admin can either paste the new certificate or upload it.
- **Backup certificate** is optional and is used when the primary certificate is unusable. The admin can paste the certificate or upload it.
- **Edit** an existing certificate configured for a specific application.

The screenshot shows the SAP Ariba web interface for creating a Mutual TLS configuration. The page title is "Mutual TLS Configuration - Create" and it includes "Save" and "Cancel" buttons. The main heading is "Configure mutual TLS authentication for Inbound or Outbound connections." The form is divided into sections: "General", "Primary Certificate", and "Backup Certificate".

**General**  
Fields marked with \* are required.  
Name: \* [text input]  
Type: \* Inbound [dropdown]  
Application Name: \* SM [dropdown]

**Primary Certificate**  
Paste your Base64 encoded certificate here. It must begin with "-----BEGIN CERTIFICATE-----" and end with "-----END CERTIFICATE-----".  
Primary Certificate: \* [text area]  
[Choose File] No file chosen  
Issuer Name:  
Expiry Date:

**Backup Certificate**  
Paste your Base64 encoded certificate here. It must begin with "-----BEGIN CERTIFICATE-----" and end with "-----END CERTIFICATE-----".  
Backup Certificate: [text area]  
[Choose File] No file chosen  
Issuer Name:  
Expiry Date:

At the bottom right, there are "Save" and "Cancel" buttons.

# Feature at a Glance

Introducing: **Configure mutual TLS authentication certificates for inbound communications**

## Detailed feature information – Configure Mutual TLS Authentication for Inbound integration end point

Navigation Path: **Integration Manager** → **End Point Configuration**

The Customer admin can create new end point configuration or edit an existing entry to configure mutual TLS authentication.

The screenshot displays the SAP Ariba 'End Point Configuration' page. The left sidebar contains a navigation menu with categories like Site Manager, Integration Manager, Master Data Manager, User Manager, Customization Manager, Forms and Extensions Manager, Intelligent Configuration Manager, Email Notification Manager, Supplier Manager, Miscellaneous, and Dashboard Manager. The 'Integration Manager' section is expanded, and 'End Point Configuration' is selected. The main content area shows a search bar for existing endpoints, a search filter for 'Type' (No Choice, Inbound, Outbound), and a table of endpoints. A 'Create New' button is visible at the bottom left of the table area.

| Name           | Type     |      |
|----------------|----------|------|
| BasicOut       | Outbound | Edit |
| cadsadas       | Inbound  | Edit |
| dasdasd        | Inbound  | Edit |
| dhasjdas       | Inbound  | Edit |
| fasfd          | Inbound  | Edit |
| mutual         | Inbound  | Edit |
| mutual_1       | Inbound  | Edit |
| mutualauth     | Inbound  | Edit |
| mutualauth1    | Inbound  | Edit |
| RemittancePull | Inbound  | Edit |

# Feature at a Glance

Introducing: **Configure mutual TLS authentication certificates for inbound communications**

## Detailed feature information – Configure Mutual TLS Authentication for Inbound integration end point

Navigation Path: **Integration Manager** → **End Point Configuration** → **Create New**

The existing **End Point Configuration** page now has the **Requires Mutual Authentication** option to choose client authentication.

Default value of **Requires Mutual Authentication** is No. If this value is set to Yes, then the admin will be able to select the configured mutual authentication certificate.

The screenshot shows the SAP Ariba 'End Point Configuration - Create End Point' page. The 'Mutual TLS Authentication' section has 'Requires Mutual Authentication' set to 'Yes'. A modal dialog titled 'Choose Value for Inbound Certificate Configuration' is open, displaying a table of certificates. A blue arrow points from the 'Inbound Certificate Configuration' dropdown in the background to the 'Select' button for the 'final3' certificate in the modal.

| Name     | Application Name | Expiration Date  | Issuer Name     |        |
|----------|------------------|------------------|-----------------|--------|
| abcd1    | S4               | Fri, 1 Oct, 2021 | CN=c02y108bjgh5 | Select |
| abcdefg  | SM               | Fri, 1 Oct, 2021 | CN=c02y108bjgh5 | Select |
| abcdew   | Buyer            | Fri, 1 Oct, 2021 | CN=c02y108bjgh5 | Select |
| ffdsfd   | Buyer            | Fri, 1 Oct, 2021 | CN=c02y108bjgh5 | Select |
| final_1  | SM               | Fri, 1 Oct, 2021 | CN=c02y108bjgh5 | Select |
| final2   | SM               | Fri, 1 Oct, 2021 | CN=c02y108bjgh5 | Select |
| final3   | Buyer            | Fri, 1 Oct, 2021 | CN=c02y108bjgh5 | Select |
| ffsdfnfv | SM               | Fri, 1 Oct, 2021 | CN=c02y108bjgh5 | Select |
| gdhgfh   | Buyer            | Fri, 1 Oct, 2021 | CN=c02y108bjgh5 | Select |

Follow us



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

© 2021 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.

**THE BEST RUN**

