SAP Ariba

Feature at a Glance

Configure mutual TLS authentication certificates for inbound communications

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

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.

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.

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

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

Implementation information

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

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

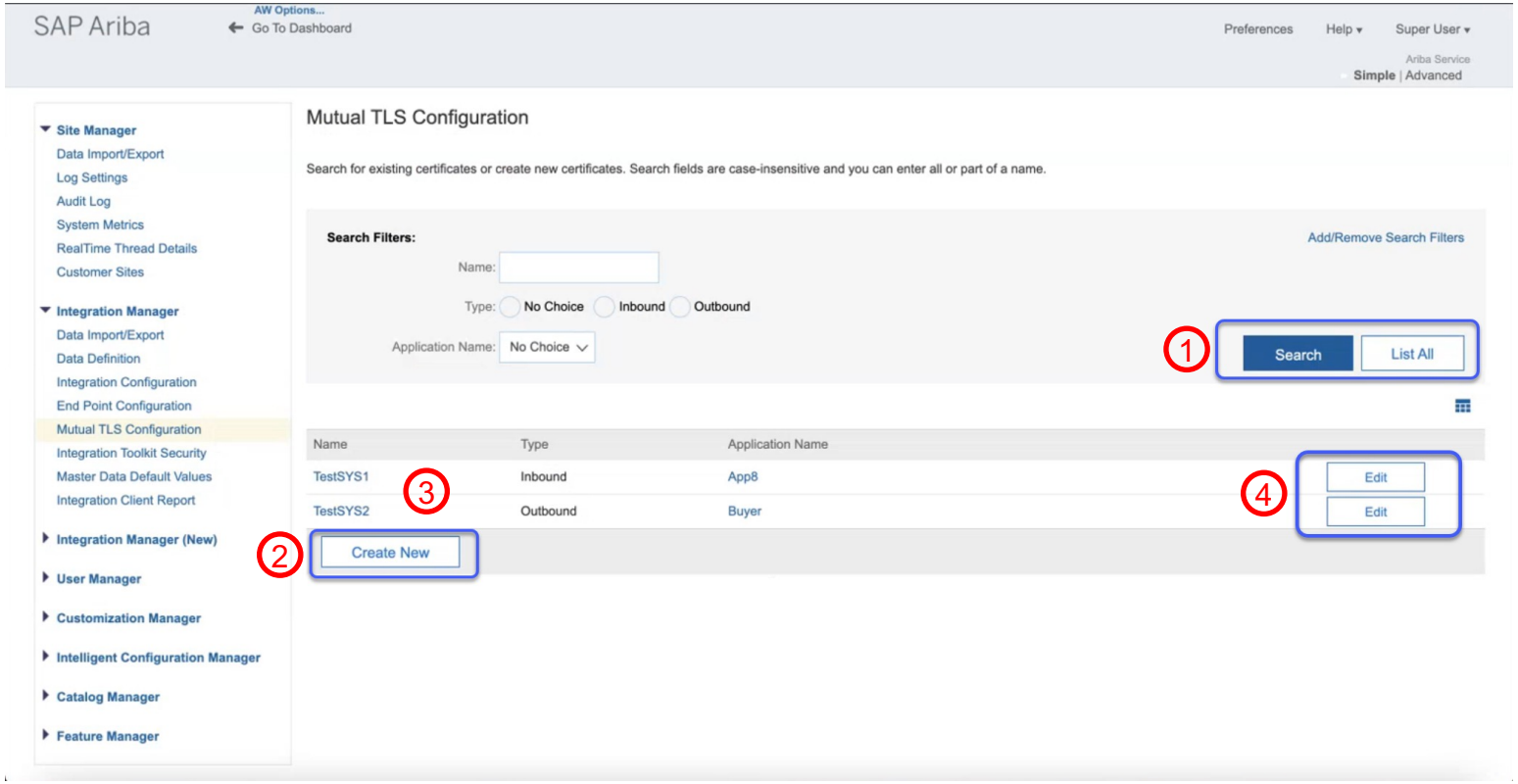
Introducing: **Configure mutual TLS authentication certificates for inbound communications**

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



Feature at a Glance

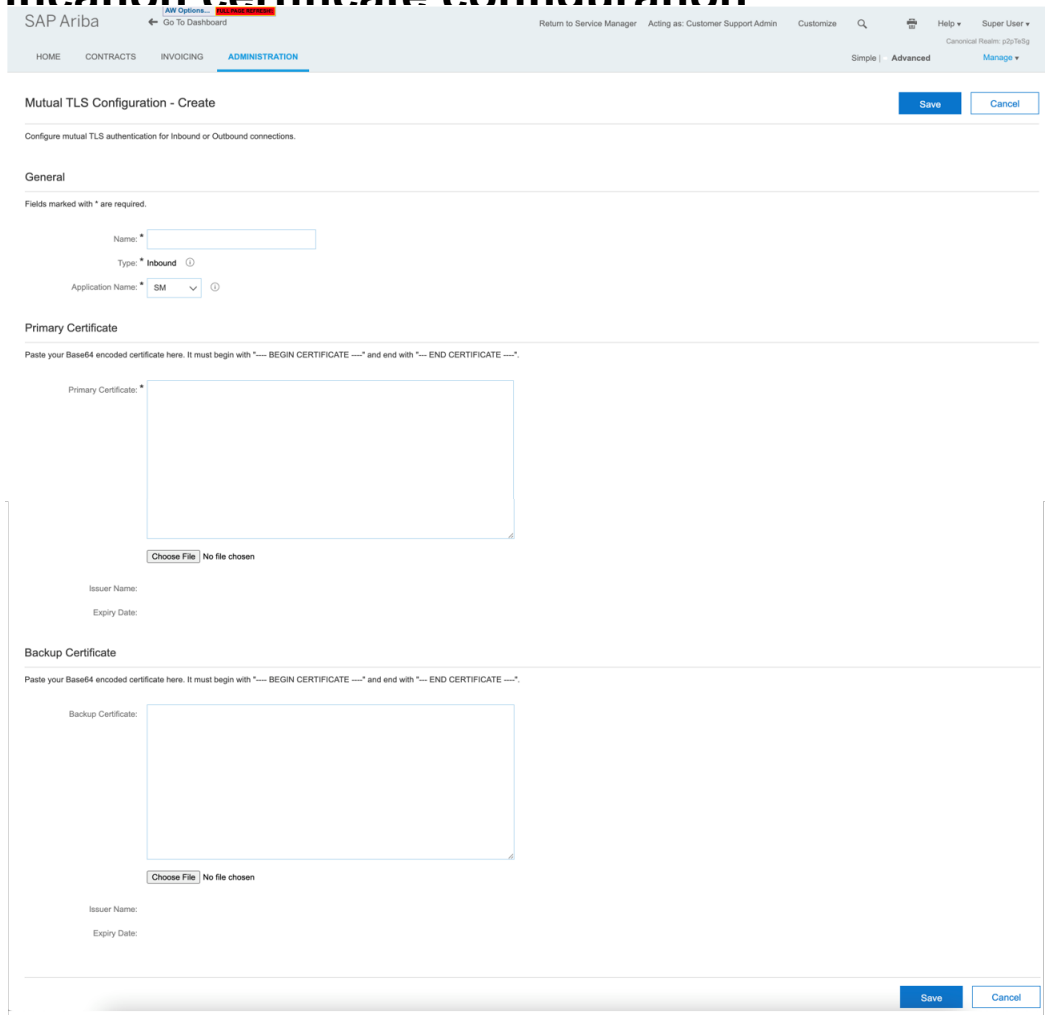
Introducing: **Configure mutual TLS authentication certificates for inbound communications**

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.



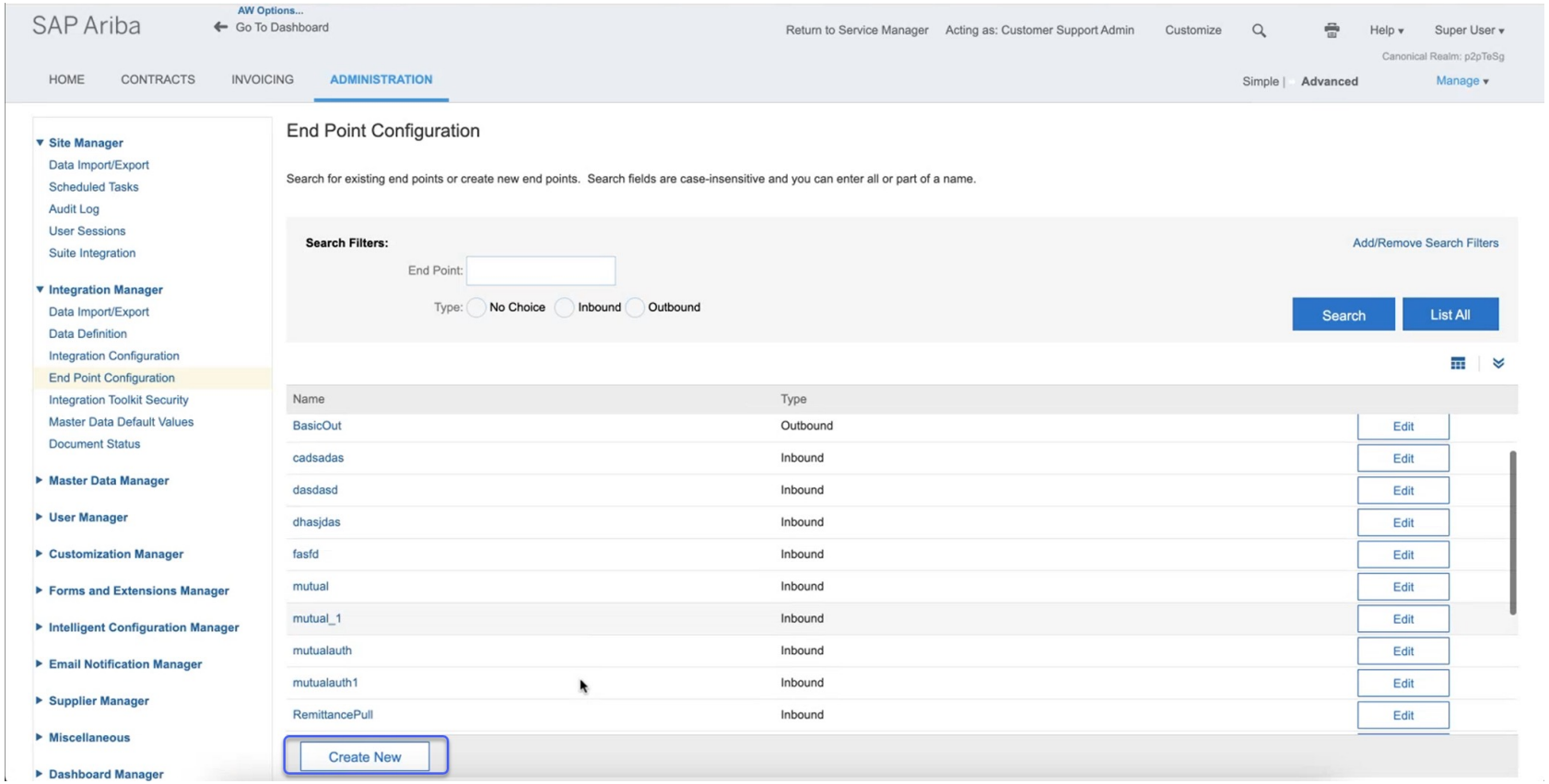
Feature at a Glance

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.



Feature at a Glance

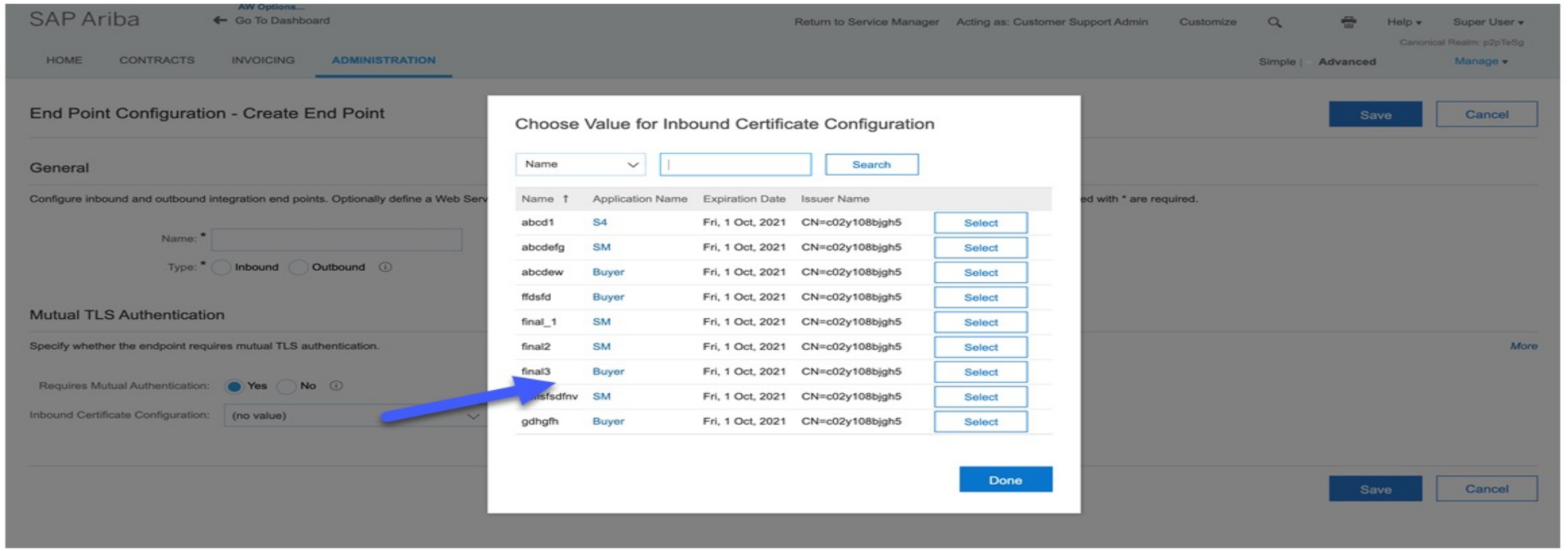
Introducing: **Configure mutual TLS authentication certificates for inbound communications**

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.



SAP Ariba

Follow us

www.sap.com/contactsap

THE BEST RUN SAP