



SAP SuccessFactors 

PUBLIC

Document Version: 1H 2025 – 2025-04-04

Using Security Center

Content

1	Security Center.	3
2	Setting Up Permissions for Security Center.	4
3	Importing a PGP File Encryption Key.	6
4	Creating OAuth Configurations.	8
4.1	OAuth 2.0 Settings Field Descriptions.	9
	OAuth 2.0 with SAML Flow.	10
	OAuth 2.0 with Grant Type as Password.	12
	OAuth 2.0 with Grant Type as Client Credential.	14
	OAuth 2.0 mTLS with Grant Type as Client Credential.	15
5	Generating X509 Certificates	17
5.1	X509 Certificates Field Descriptions.	18
6	Generating Other Keys.	22
7	Uploading HTTPS Trust Certificates.	25
7.1	Uploading Server Certificates.	25
7.2	Uploading Root CA Certificates	26
7.3	HTTPS Trust Certificate Field Descriptions.	27
8	Configuring Destination Settings.	29
8.1	Creating SFTP Destination Settings.	29
8.2	Creating REST Destination Settings.	31
9	Setting Up a LinkedIn Account.	34
10	Change History.	36

1 Security Center

Security Center allows you to create and manage keys, certificates and configurations that can be used in integrations.

You can access the Security Center from the Admin Center. The Security Center provides a dashboard that has the following tiles:

- [PGP File Encryption Keys](#) - Import a PGP Public Key to encrypt files generated using SFTP Outbound Integrations.
- [OAuth Configurations](#) - Configure OAuth 2.0 configurations for outbound connections to other systems.
- [X509 Certificates](#) - Generate and download X509 certificates for OAuth with SAML and mTLS authentication.
- [Other Keys](#) - Generate and download keys for file decryption, file signing and SFTP server authentication.
- [HTTPS Trust Certificates](#) - Pull certificates from servers or upload Root CA certificates to establish client-server trust.
- [Destination Settings](#) - Maintain SFTP and REST destination settings for Outbound Integrations.
- [LinkedIn Account Setup](#): Create customer LinkedIn accounts and select LinkedIn integrations.
- [X.509 Public Certificate Mapping](#): Register your X.509 public certificate for mTLS authentication.

You can view detailed change log information for [OAuth Configurations](#), [X509 Certificates](#), [Other Keys](#), [HTTPS Trust Certificates](#), and [Destination Settings](#). The change log contains the following information:

- Created By
- Created On
- Last Modified By
- Last Modified On

📌 Note

To access Security Center, you must have enabled access to any one of the tiles from [Manage Security Center](#).

Related Information

[Setting Up Permissions for Security Center \[page 4\]](#)

2 Setting Up Permissions for Security Center

Set up role-based permissions required to use Security Center.

Prerequisites

You're logged in as the RBP Admin.

Procedure

1. Go to ► [Admin Center](#) ► [Tools](#) ► [Manage Permission Roles](#) ►.
2. Select a Permission Role.
3. Under [Permission Settings](#), choose [Permission](#).
4. Set up the following role-based permissions:

Permission Location	Permission Name	Description
Manage Security Center	Access to PGP File Encryption Keys	Enables access to import PGP Public Keys for file encryption.
Manage Security Center	Access to OAuth Configurations	<p>Enables access to OAuth configurations for outbound connections to other systems.</p> <p>You can assign View or Create, Edit & Delete, or both access to this permission.</p> <p>You also need the ► Metadata Framework ► Access to non-secured objects ► permission for OAuth configurations.</p>
Manage Security Center	Access to X509 Certificates	<p>Enables access to X509 Certificates for OAuth with SAML and mTLS server authentication.</p> <p>You can assign View or Create, Edit & Delete, or both access to this permission.</p>

Permission Location	Permission Name	Description
Manage Security Center	Access to Other Keys	<p>Enables access to generate keys for file decryption, file signing and SFTP server authentication.</p> <p>You can assign View or Create, Edit & Delete, or both access to this permission.</p>
Manage Security Center	Access to HTTPS Trust Certificates	<p>Enables access to pull certificates from servers or upload Root CA certificates to establish client-server trust.</p> <p>You can assign View or Create & Delete, or both access to this permission.</p>
Manage Security Center	Access to Destination Settings	<p>Enables access to create and maintain SFTP and REST destination settings for outbound integrations.</p> <p>You can assign View or Create, Edit & Delete, or both access to this permission.</p>
Manage Integration Tools	Manage LinkedIn Account Setup	<p>Enables access to LinkedIn Account Setup.</p> <p>To access the LinkedIn Account Setup tile in Security Center, you also need the Metadata Framework > Access to non-secured objects permission.</p>

Related Information

[Using Role-Based Permissions](#)

3 Importing a PGP File Encryption Key

Import a PGP Public Key to encrypt files generated using SFTP Outbound Integrations.

Prerequisites

You must have generated a PGP key pair so that you can import the PGP public key.

Context

If you want to send sensitive data, it is always recommended to encrypt the data at message level. Security Center offers message level encryption using PGP (Pretty Good Privacy) encryption methodology.

Procedure

1. Go to ► [Admin Center](#) ► [Security Center](#) ► [PGP File Encryption Keys](#) ►.
2. To import your PGP Public key for encryption, select [Import a Key](#).

The [Import Key](#) dialog box opens.

3. Enter a name for your key in the [Name](#) field.
4. Choose [Choose File](#) to select your file.

Some common file formats used for PGP Public keys are: **.pub** and **.asc**.

5. To finish, choose [Import Key](#) to import your file.

Note

- The size of the file varies based on the key size that you have set on the tool to generate a PGP key. The size of the generated key is generally between 512 and 4096 bytes.
- You cannot upload PGP keys with same name.

Your imported PGP Key is encrypted and listed in the [Keys](#) table. To delete a key, choose  from [Actions](#).

Results

You can use these keys in various admin tools that support PGP encryption, such as [Integration Center](#) or [Change Audit Reports](#).

Related Information

[Information on PGP Message Format](#) ➡

4 Creating OAuth Configurations

Configure OAuth 2.0 configurations for outbound connections to other systems.

Prerequisites

- Ensure you have the [Create, Edit & Delete](#) access to the [Access to OAuth Configuration](#) permission.
- Ensure you have enabled [Metadata Framework](#) > [Access to non-secured objects](#) permission.
- Ensure you have the [View](#) access to the [Access to X509 Certificates](#) permission, when you are configuring an OAuth Configuration with [OAuth 2.0 with SAML Flow](#).

Procedure

1. In the [Security Center](#) dashboard, choose [OAuth Configurations](#) .

The OAuth Configurations page is displayed.

2. Choose [Add](#) to create a new OAuth configuration.
3. Enter details for fields under [OAuth 2.0 Settings](#).

Note

If you are configuring with [OAuth 2.0 with SAML Flow](#) and do not have an existing [X509 Certificate](#), then configure an X509 certificate by choosing [Click to manage X509 Certificates](#). For more information, refer [Generating X509 Certificates](#) in the related information.

For descriptions on each setting, refer OAuth 2.0 Settings Field Descriptions in the related information.

4. Choose [Save](#).

Remember

- To edit the OAuth Configuration, choose [Edit](#). Choose [Save](#) to save your changes.
- To delete the OAuth Configuration, choose [Delete](#) from the configuration settings window.

Results

A confirmation message appears. The newly created OAuth Configuration is saved and is displayed in the left pane.

You can search the OAuth configurations by name or sort them in a particular order to narrow down your search result.


Related Information

[Generating X509 Certificates \[page 17\]](#)

[OAuth 2.0 Settings Field Descriptions \[page 9\]](#)

4.1 OAuth 2.0 Settings Field Descriptions

Use the field descriptions in the table for [OAuth 2.0 Settings](#) to configure your [OAuth Configuration](#).

Fields	Description
Configuration Name	Name for the OAuth configuration. <div><div> Note</div><div>Make sure you select the same name when you model the integration.</div></div>
Description	Additional information about the configuration.
OAuth Type	<p>OAuth 2.0 has various types of flows that enable authentication and authorization with an OAuth 2.0 client at a back-end where you want to access resources. Currently Security Center offers configurations for the following OAuth 2.0 flows:</p> <ol style="list-style-type: none">1. OAuth 2.0 with SAML Flow: OAuth 2.0 with Security Assertion Markup Language (SAML) Flow is used to authenticate the client as well as to request the OAuth 2.0 access token from an OAuth 2.0 authorization server. For more information, refer to OAuth 2.0 with SAML Flow in the related information.2. OAuth 2.0: Supports OAuth authentication using a Grant Type. For more information on this OAuth type, refer to related information.<ul style="list-style-type: none">• The Grant Type is either using Password or Client_Credentials. You have the following Grant Types:<ol style="list-style-type: none">1. Password: Use this to exchange a user's credentials for an access token. The Password is encrypted and stored. For more information, refer to OAuth 2.0 with Grant Type as Password in the related information.2. Client_Credentials: Use this grant type when an application request an access token to access their own resources, not on behalf of a user.

Fields	Description
Label	<p>This field is populated by label values which are provided by the Administrator in the database using the Manage Data tool.</p> <p>In the Manage Data tool, the Administrator can use the IntegrationProcessOAuthCategory to create values which will appear in the Label field for OAuth Configurations in Security Center.</p> <p>For both new and existing OAuth Configurations, this field is set to Not Selected by default. You can select a value from the dropdown list in the Label field.</p> <p>This field can be used to allow filtering of specific types of OAuth configurations and set permissions for user.</p>

Based on the [OAuth Type](#) selected, the corresponding configuration fields are displayed. For more information, refer to **OAuth 2.0 with SAML Flow**, **OAuth 2.0 with Grant Type as Password** and **OAuth 2.0 with Grant Type as Client Credential** in the related information.

Related Information

[OAuth 2.0 with SAML Flow \[page 10\]](#)

[OAuth 2.0 with Grant Type as Password \[page 12\]](#)

[OAuth 2.0 with Grant Type as Client Credential \[page 14\]](#)

[Managing MDF Object Instance](#)

4.1.1 OAuth 2.0 with SAML Flow

OAuth 2.0 with Security Assertion Markup Language (SAML) Flow is used to authenticate the client as well as to request the OAuth 2.0 access token from an OAuth 2.0 authorization server.

When an integration initiates an HTTPS POST request to the authorization server in order to exchange the assertion, the authorization server performs client authorization and validation of the supplied data from the request. If the application is authorized and the assertion is validated, the authorization server responds with an access token. Using the access token, a call is made to the same service where it was originally fetched and the CSRF token is requested. If the assertion is validated the authorization server responds with a CSRF token. If any error occurs during the process, an error response is returned.

Let us consider an example where calls are made when [POST](#) is selected as an option from [Token Method](#) menu:

❖ Example

For POST token method, the Token URL that uses SAML assertion: <https://cloud-service/oauth/token>. When using POST Token Method, the call is made to the same service where it was originally fetched and requests for the CSRF token. In the next call, the URL appears as: <https://cloud-service/core/oauth/api/v1/rest/csrf>

SAML Assertion

To prepare the SAML 2.0 assertion XML we must have the values of the following XML attributes and elements:

OAuth 2.0 with SAML SAML parameters	Description
Token URL	<p>The URL to get the access token.</p> <p>This is a mandatory parameter.</p>
Token Method	<p>The HTTP method - <i>POST</i> or <i>GET</i>, that must be used for the connection.</p>
Audience	<p>Intended audience for the assertion, which will be verified by the OAuth authorization server.</p> <p>This is a mandatory parameter.</p>
Recipient	<p>Specifies the authorization server's token URL on which the POST request will be executed.</p> <p>This is an optional parameter.</p>
Issuer	<p>Specifies the location of the SAML identity provider.</p> <p>This is a mandatory parameter.</p>
Subject Name ID	<p>Specifies the name ID format. You can set the format as <i>Email Address</i>, <i>X509 Subject Name</i> or <i>Unspecified</i>. If you choose <i>Unspecified</i>, your user ID is used as the Subject Name ID.</p> <p>This is an optional parameter.</p>
Subject Name ID Format	<p>Specifies an e-mail address of the user on whose behalf the flow is initiated.</p> <p>This is an optional parameter.</p>
X509 Certificates	<p>A self-signed certificate used for assertion that is digitally signed using standard XML Signature.</p> <p>This is a mandatory parameter.</p> <div><p>Note</p><ul style="list-style-type: none">If you do not have an existing <i>X509 Certificate</i>, then configure an X509 certificate by choosing Click to manage X509 Certificates. For more information, refer Generating X509 Certificates in the related information.Only <i>Self Signed</i> X509 certificates will be displayed in this list.</div>
Custom Attributes	<p>Custom attributes are mainly static values populated into the SAML Assertion. The attributes are defined as name-value pairs. You can add up to 6 attributes.</p> <p>This is an optional parameter.</p>

Requesting Authorization

Now that we have the assertion prepared, we have to prepare the POST request in order to execute it. The parameters that are used when constructing the request are the following:

Requesting Authorization Parameters	Description
Client ID	The authorization server provides a client ID to the registered client. The client id - a unique string representing the registration information provided by the client. This is an optional parameter.
Client Secret	Authorization information that is known only to the application and the authorization server. This is an optional parameter.

Successful Authorization

If the client is authenticated and the supplied fields and assertions are validated, the authorization server will respond with an access token.

Note

Refresh tokens usually are not issued when using this grant type. Client applications can try to refresh the expired access token by requesting a new one with the same assertion. If the assertion has expired then a new access token can be requested by executing the whole grant flow from the start.

Getting CSRF Token

It is possible that the Token URL is protected with Cross Site Request Forgery (CSRF) to prevent session riding. To make sure the CSRF Token is fetched before the call is made to get the Token, the relative URL is set in [Destination Settings](#). For example, `/core/oauth/api/v1/rest/csrf`.

Related Information

[Generating X509 Certificates \[page 17\]](#)

4.1.2 OAuth 2.0 with Grant Type as Password

The Password grant type is used by client to exchange a user's credentials for an access token.

After the user gives their credentials to the application, the application makes a call to the authorization server. If the call is valid, the authorization server generates an access token (and optional refresh token) and returns them to the client along with some additional properties about the authorization. If the call is invalid, for example, if the password is incorrect or if the user does not have access to the system, then the server returns an error response.

Note

As per the specification, passwords are used to get the Access Token and Refresh token and are not supposed to be stored in the client system. As certain self-signed certificate's implementation may have short lived

Access Tokens or Refresh Tokens, and can expire, the Security Center provides additional capability to store them encrypted.

The access token request will contain the following parameters.

Access Token Request parameters

Request Parameters	Description
Grant Type	<p>The grant type parameter is set to Password. Password is encrypted and stored.</p> <p>This is a mandatory parameter.</p>
Client ID	<p>The authorization server provides a client ID to the registered client. The client id - a unique string representing the registration information provided by the client.</p> <p>This is a mandatory parameter.</p>
Client Secret	<p>The Client Secret is a secret known only to the application and the authorization server.</p> <p>This is an optional parameter.</p>
Token URL	<p>The URL to get the access token.</p> <p>This is a mandatory parameter.</p>
Token Method	<p>Choose either <i>POST</i> or <i>GET</i> supported HTTP method for the connection.</p>
Username	<p>The username of the system that you are accessing.</p> <p>This is a mandatory parameter.</p>
Custom Header Parameters	<p>These are mainly static header values. You can add one or more headers using + (add) button.</p> <div><p>→ Remember</p><p>Two same keys cannot be added in custom header parameters. Also, you cannot add Content Type and Authentication Header types to custom header parameters.</p></div>

When you click save, you will see a Password dialog. When you enter the password, Security Center generates the refresh token, encrypts and stores it for future generation of access token.

If you select [Save Password](#), then Security Center stores the encrypted password in the database, else the password will be used only to generate the refresh token.

4.1.3 OAuth 2.0 with Grant Type as Client Credential

The Client Credentials grant is used when application requests an access token to access their own resources, not on behalf of a user.

The application makes a call by sending its credentials, its client ID and client secret, to the authorization server. If the call is valid, then the authorization server returns an access token to the application. If the call is invalid, then the authorization server returns an error response.

ⓘ Note

Currently, OAuth works with Integration Center only when you follow the standard. We don't support customized implementation as of now. For example, Integration Center supports only custom header and does not support custom body parameters.

The access token request will contain the following parameters.

Access Token Request parameters

Request Parameters	Description
Grant Type	The grant type parameter is set to Client_Credentials .
Client ID	<p>The authorization server issues the registered client, a client id - a unique string representing the registration information provided by the client.</p> <p>This is a mandatory parameter.</p>
Client Secret	<p>The Client Secret is a secret known only to the application and the authorization server.</p> <p>This is a mandatory parameter.</p>
Token URL	<p>The URL to get the access token.</p> <p>This is a mandatory parameter.</p>
Token Method	Choose either POST or GET supported HTTP method for the connection.
Custom Header Parameters	<p>These are mainly static header values. You can add one or more headers using + (add) button.</p> <div><p>→ Remember</p><p>Two same keys cannot be added in custom header parameters. Also, you cannot add Content Type and Authentication Header types to custom header parameters.</p></div>

4.1.4 OAuth 2.0 mTLS with Grant Type as Client Credential

The Client Credentials grant is used when application requests an access token to access their own resources, not on behalf of a user.

The application makes a call by sending its credentials, its client ID and client secret, to the authorization server. If the call is valid, then the authorization server returns an access token to the application. If the call is invalid, then the authorization server returns an error response.

Note

Currently, [OAuth 2.0 mTLS](#) authentication is supported only for REST integration.

The access token request will contain the following parameters.

Access Token Request parameters

Request Parameters	Description
Grant Type	The grant type parameter is set to Client_Credentials .
Client ID	<p>The authorization server issues the registered client, a client id - a unique string representing the registration information provided by the client.</p> <p>This is a mandatory parameter.</p>
X509 Client Certificate	<p>Choose an X.509 certificate from the dropdown. X.509 certificate is a digital certificate and is used to manage identity and security in internet communications.</p> <p>If you don't have an existing X509 Certificate, then configure an X509 certificate by choosing Click to manage X509 Certificates. For more information, refer Generating X509 Certificates in the related information.</p> <p>This is a mandatory parameter.</p>
Token URL	<p>The URL to get the access token.</p> <p>This is a mandatory parameter.</p>
Token Method	Choose either POST or GET supported HTTP method for the connection.
Custom Header Parameters	<p>These are mainly static header values. You can add one or more headers using + (add) button.</p> <div><p>→ Remember</p><p>Two same keys cannot be added in custom header parameters. Also, you cannot add Content Type and Authentication Header types to custom header parameters.</p></div>

Related Information

[Generating X509 Certificates \[page 17\]](#)

5 Generating X509 Certificates

Generate and download X509 certificates for OAuth with SAML and Mutual TLS (mTLS) authentication.

Prerequisites

You must have [Create, Edit & Delete](#) permission to [Access to X509 Certificates](#) permission.

Procedure

1. In the [Security Center](#) dashboard, choose [X509 Certificates](#) in the window.
2. Choose [Add](#) to create a new X509 certificate.
3. Enter details for fields in the [Certificate Settings](#) and [Certificate Subject](#).

Note

The [Certificate Subject](#) fields are optional.

Refer to X509 Certificate Field Descriptions in the related information.

4. Choose [Generate and Save](#).

Note

If you chose [External CA](#) under [Certificate Settings](#), then in the [Key Store](#) field, select a certificate using [Browse](#). Choose [Upload and Save](#) to upload the certificate.

Results

A confirmation message appears. The newly created [X509 Certificates](#) are saved and is displayed in the left pane.

You can search the [X509 Certificates](#) by name or sort them in a particular order to narrow down your search results.

Next Steps

You can edit or delete the certificate. To edit the certificate, choose [Edit](#). To save your changes, choose [Regenerate and Save](#). To delete the certificate, choose [Delete](#).

Choose [Download](#) button to download your [X509 certificate](#) or [CA Certificates](#). Your [X509 Certificate](#) is saved to your local drive as a `.cert` file. You can fetch both the intermediate and Root certificates when you download the CA certificate. The format of the downloaded file is PKCS#7 PEM (Privacy Enhanced Mail).

Related Information

[X509 Certificates Field Descriptions \[page 18\]](#)

5.1 X509 Certificates Field Descriptions

The following field descriptions will help you configure the [Certificate Settings](#) when you are generating a X509 Certificate.

X509 Certificate Configuration Fields	Description
Configuration Name	X509 certificate name.
Description	Description of your X509 certificate.
Certification Authority (CA)	The certifying authority to be used when generating a X509 certificate.

Certificate Authority Parameters

Certificate Authority	Description
Self Signed	<p>Set suitable values to the following fields to generate a self-signed certificate:</p> <ul style="list-style-type: none">Valid Until : Specifies the validity duration (in the UTC format) of the self-signed certificate. The maximum duration for the key's validity is 3 years. <div><p>→ Tip</p><p>Use shorter validity durations for enhanced security.</p></div> <p>This is a mandatory parameter.</p> <ul style="list-style-type: none">Signature Algorithm: SHA256WithRSA and SHA512WithRSA algorithm is used to generate the X509 certificate. These algorithms are a set of cryptographic hash functions that compares the computed hash to a known and expected hash value. The algorithm allows you to determine the integrity of the data. <p>This is a mandatory parameter.</p> <ul style="list-style-type: none">Issued By: Specifies the authority from where the certificate was issued.

Certificate Authority

Description

[SAP Cloud Root CA](#)

These are X509 Client Certificates signed by SAP Cloud Root CA and can be used in SAP to SAP Application integrations for mutual TLS authentication.

- **Valid Until:** Specifies the validity duration (in the UTC format) of the SAP Cloud Root CA certificate. The maximum duration for the key's validity is 1 year.

Note

Use shorter validity durations for enhanced security.

This is a mandatory parameter.

- **Renew on Expiry:** Once you set the validity for the certificate, select this check box to enable the automatic renewal of the certificate. The check box is disabled by default. By default, the renewal happens for a period of one year, irrespective of what the validity was previously set to.
- **Signature Algorithm:** [SHA256WithRSA](#) and [SHA512WithRSA](#) algorithm is used to generate the X509 certificate. These algorithms are a set of cryptographic hash functions that compares the computed hash to a known and expected hash value. The algorithm allows you to determine the integrity of the data.
This is a mandatory parameter.
- **Email:** Include email IDs in this field to receive notifications for certificates that are nearing expiration date.

Certificate Authority

Description

External CA

These are external CA signed certificates that can be uploaded and stored as X509 Certificates. Upload a certificate using the [Key Store](#) field, by selecting a **.pem** file using [Browse](#).

You can generate a **.pem** file using **OpenSSL** or any open source tool. The file content must be inline with the following format:

Sample Code

```
Bag Attributes
subject=<X509 Certificate subject>
issuer=<X509 Certificate issuer>
-----BEGIN CERTIFICATE-----
<X509 Certificate>
-----END CERTIFICATE-----
Bag Attributes
subject=<X509 Intermediate CA
Certificate1 subject>
issuer=<X509 Certificate issuer [Root CA/
Intermediate CA]>
-----BEGIN CERTIFICATE-----
<X509 Intermediate CA Certificate1>
-----END CERTIFICATE-----
Bag Attributes
subject=<X509 Intermediate CA
Certificate2 subject>
issuer=<X509 Certificate issuer [Root CA/
Intermediate CA]>
-----BEGIN CERTIFICATE-----
<X509 Intermediate CA Certificate2>
-----END CERTIFICATE-----
Bag Attributes
subject=<X509 Root CA Certificate subject>
issuer=<X509 Root CA Certificate subject>
-----BEGIN CERTIFICATE-----
<X509 Root CA Certificate2>
-----END CERTIFICATE-----
Bag Attributes
Key Attributes
-----BEGIN PRIVATE KEY-----
<X509 Private Key>
-----END PRIVATE KEY-----
```

Certificate Subject

Certificate Subject

Description

Common Name (CN)

Common name attribute type specifies an identifier for an object.

This is an auto-generated field that appears once the X509 certificate is generated.

Certificate Subject	Description
<i>Organization (O)</i>	<p>Organization attribute type that specifies an organization.</p> <div> ❖ Example O = Scottish Telecommunications, tlc </div>
<i>Organizational Unit (OU)</i>	<p>The organizational unit attribute type that specifies an organizational unit.</p> <div> ❖ Example OU = Information Technology </div>
<i>Locality (L)</i>	<p>This field is auto-generated with the Company ID. This is applicable for self signed certificates.</p> <div> ❖ Example L = Edinburgh </div>
<i>State/Province (ST)</i>	<p>The state or province attribute type that specifies either a state or province.</p> <div> ❖ Example S = Ohio </div> <div> ❖ Example T = British Columbia </div>
<i>Country/Region (C)</i>	<p>This attribute specifies the country or region.</p>

6 Generating Other Keys

To generate keys for file decryption, file signing and SFTP server authentication.

Prerequisites


You must have [Create, Edit & Delete](#) permission to [Access to Other Keys](#) permission.

Procedure

1. In the [Security Center](#) dashboard, choose [Other Keys](#).
The [Other Keys](#) page is displayed.
2. In the [General Details](#) section, enter suitable values for the fields as described in the following table:

Field	Description
Type	Specifies the type of algorithm used. The key-pair is generated using RSA algorithm. <div><div><div><div><div></div><div>Note</div></div><div>The SSH keys are generated using the SHA-256 and SHA-512 algorithms with a RSA key size of 3072 and 4096. The existing SHA-1 keys are still supported, but we recommend migrating to the improved SSH key generation.</div></div></div></div>
Name	Enter a key alias/name for the key-pair. This is a mandatory parameter.
Description	Enter the description for the key-pair.

Field	Description
Category	<p>Select the key category from the drop-down list. The available keys are as follows:</p> <ul style="list-style-type: none"> • Authentication Key (SSH) - Use this key for SFTP server authentication. • Signing Key (PGP) - Use this key for signing outbound integration files only. • Decryption Key (PGP) - Use this key to decrypt files that are picked from the SFTP and are written to Metadata Framework. You can only decrypt inbound integration files.
Scheduled Job Key	<p>Generate PGP Decryption Keys that is used in scheduled jobs.</p> <div> <p>Note</p> <p>This feature is enabled in phases. If you can see the Scheduled Job Key checkbox when you select Decryption Key (PGP) from Category, then the feature is enabled in your instance. Meanwhile, the PGP Decryption Keys generation, test, and export features in Provisioning have been disabled.</p> </div> <p>If you have a PGP Decryption Key generated for scheduled jobs in Provisioning, you can find it listed in the Other Keys list. You could either continue to use this PGP Decryption Key, or generate a new one for scheduled jobs.</p> <div> <p>→ Remember</p> <p>As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Technical Support.</p> </div> <div> <p>⚠ Caution</p> <p>You can only have one active PGP Decryption Key used in scheduled jobs. If you already have a PGP Decryption Key used in scheduled jobs, creating a new key overrides the existing one.</p> </div>

Field	Description
Valid From	<div>  Note This field is displayed only for the Authentication Key (SSH) category. Specifies the date from which the key is valid. You can select a current date or a future effective date from the picker. </div>
Valid Until	Specifies the expiration date of the key.

Note

The generated key's validity will begin based on the current date and time on which it was generated. Also, if the [Valid Until](#) field is left blank, the key will be generated without an expiry date.

- Choose [Save](#) and choose [Ok](#) when the success message is displayed.

→ Remember

- To download the key, choose [Download Public Key](#).
- To edit the key, choose [Edit](#). To save your changes, choose [Regenerate and Save](#).
- To delete the key, choose [Delete](#).
- Choose [Finger Print](#), if you want to verify the authenticity of the downloaded key.

Results

A confirmation message appears. The newly created key is saved and is displayed in the left pane.

You can search the key by name or sort them in a particular order to narrow down your search results.

Related Information

[PGP Keys Used in Scheduled Jobs](#)

7 Uploading HTTPS Trust Certificates

Pull certificates from servers or upload Root CA certificates to establish client-server trust.

You can upload a HTTP Trust Certificate using the following certificate types:

- Server Certificate
- Root CA Certificate

Related Information

[Uploading Server Certificates \[page 25\]](#)

[Uploading Root CA Certificates \[page 26\]](#)

7.1 Uploading Server Certificates

Pull certificates from a server and upload it to the SAP SuccessFactors tenants to establish client-server trust.

Prerequisites

You must have [Create & Delete](#) permission to [Access to HTTP Certificates](#) permission.

Procedure

1. In your [Security Center](#) dashboard, go to [HTTPS Trust Certificates](#).
2. Choose [Add](#) to upload a new HTTPS trust certificate.
3. Choose the [Certificate Type](#) as [Server](#).
4. Enter suitable values for the parameters based on your selection.
5. Enter a [Description](#) for the HTTPS trust certificate.
6. Choose [Pull and Upload Trust Certificate From Server](#) button to pull the certificate from the server and upload it to the SAP SuccessFactors tenants.

If the certificate already exists, then you will see a warning message. If you wish to override the certificate then click [Ok](#).

→ Remember

To delete a certificate, choose [Delete](#).

Results

You can see the newly added certificate in the [HTTPS Trust Certificates](#) section. You can view certificate details by choosing  in the [Details](#) field.

You can search the [server certificates](#) by name or sort them in a particular order to narrow down your search results.

Related Information

https://en.wikipedia.org/wiki/IDN_homograph_attack 

[HTTPS Trust Certificate Field Descriptions \[page 27\]](#)

7.2 Uploading Root CA Certificates

Upload a Root CA certificate to establish client-server trust.

Prerequisites

You must have [Create & Delete](#) permission to [Access to HTTP Certificates](#) permission.

Procedure

1. In your [Security Center](#) dashboard, go to [HTTPS Trust Certificates](#).
2. Choose [Add](#) to upload a new HTTPS trust certificate.
3. Choose the [Certificate Type](#) as [Root Certificate Authority \(CA\)](#).
4. Enter suitable values for the parameters based on your selection.
5. Enter a [Description](#) for the HTTPS trust certificate.
6. In the [Root CA Certificate](#) field, select a file from your local system using [Browse](#).

The supported file types are: [.pem](#), [.crt](#) and [.cer](#)

Note

In the above mentioned file types, for Root CA certificates, the file format supported is Base-64.

7. Choose [Upload and Save](#) to save your certificate as a HTTPS Trust Certificate.

If the certificate already exists, then you will see a warning message. If you wish to override the certificate then click [Ok](#).

Remember

To delete a certificate, choose [Delete](#).

Results

You can see the newly added certificate in the [HTTPS Trust Certificates](#) section. You can view certificate details by choosing  in the [Details](#) field.

You can search the [Root CA certificates](#) by name or sort them in a particular order to narrow down your search results.

Related Information

[HTTPS Trust Certificate Field Descriptions \[page 27\]](#)

7.3 HTTPS Trust Certificate Field Descriptions

Use the field descriptions in the table to set up your HTTPS Trust Certificate.

Certificate Type - Server

Parameters	Description
Server URL	URL to establish an SSL communication and fetch the server's trust certificate. This is a mandatory parameter.

Parameters	Description
Verify Server URL	<p>Validates the URL and also checks whether the URL entered is all-ASCII or not. When you choose this feature, a warning message is displayed, choose Ok to proceed.</p> <p>Use this optional feature to verify if the received server URL is from an untrusted or unknown source or if you think the URL is spoofed with their look alikes.</p> <p>To prevent homograph attack, Integration Center validates the entered Server URL and verifies whether the entered URL is a malicious URL (based on using non-latin or any agreed upon font set) and not a look alike. ASCII has several characters or pairs of characters that look alike, for example, 0 (the number) and O (the letter), "l" lowercase L, and "I" uppercase "i". Also, Cyrillic small letter a ("a"), can look identical to Latin small letter a, ("a") which is the lowercase "a" used in English. When the URL contains non-ASCII characters, the Punycode form of the URL is displayed to the user.</p> <div> <p>❖ Example</p> <p>Let us consider an example of www.alppe.com (the Cyrillic version), which looks like www.alppe.com (the latin version) in some fonts. In this case, when you click Verify Server URL, the punycode form of the URL is displayed in the dialog box as a warning message.</p> </div>

Certificate Type - Root Certificate Authority (CA)

Parameter	Description
Configuration Name	<p>Name for the HTTPS Trust Certificate.</p> <p>This is a mandatory parameter.</p>
Root CA Certificate	<p>External signed certificates that can be uploaded and stored as HTTPS Trust Certificates. Upload a certificate using the Root CA Certificate field, by selecting a .pem file using Browse.</p> <p>This is a mandatory parameter.</p>

8 Configuring Destination Settings

Create and maintain SFTP and REST destination settings for Outbound Integrations.

You can create the following destination settings:

- SFTP Destination Settings
- REST Destination Settings

Related Information

[Creating SFTP Destination Settings \[page 29\]](#)

[Creating REST Destination Settings \[page 31\]](#)

8.1 Creating SFTP Destination Settings

Create SFTP destinations in Security Center. Here, you can create destination settings independent of an integration definition.

Prerequisites

You must have the [Create, Edit & Delete](#) access to [Access to Destination Settings](#) permission.

Procedure

1. In the [Security Center](#) dashboard, choose [Destination Settings](#).
2. Choose [Add](#) to create a new SFTP Destination Setting
3. Enter suitable values for the fields in settings window as described in the following table:

Field	Description
Name	Name of the SFTP destination setting. This is a mandatory parameter.

Field	Description
Type	Specify the type of connection. Choose SFTP from the dropdown.
SFTP Server Host Address	Address of the SFTP server. This is a mandatory parameter.
Port	By default, the port is set to 22. You can edit the SFTP port, if your security requirements make a different SFTP port necessary. The port must be between 0 and 65535. Only encrypted SFTP or port 22 file transfer protocol is supported. Security Center does not support data to be transmitted on the public internet FTP/port 21 channel because this would expose your sensitive data to the public internet.
File Folder	Specify folder and the file information in the SFTP destination. This is a mandatory parameter.
Authentication Type	<p>Select an authentication type from the dropdown:</p> <ul style="list-style-type: none"> • Certificate based Authentication: Allows you to connect to the server using the user name and the key. <ul style="list-style-type: none"> • SFTP User Name: Enter the user name of system you want to access. This is a mandatory parameter. • Authentication Key: This key is used for authentication while connecting to the destination. Select the key from the dropdown for SFTP server authentication. If you want to generate a new SSH authentication key, select Click to manage Authentication Keys. For more information, refer to Generating Other Keys in the related information. <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin-top: 10px;"> <p>Note</p> <p>To access X509 certificates, you must have the View access to Access to X509 Certificates permission.</p> </div> <ul style="list-style-type: none"> • Basic Authentication: Allows you to connect to the server using the username and password combination. <ul style="list-style-type: none"> • SFTP User Name: Enter the user name of the system you want to access. This is a mandatory parameter. • SFTP Password: Enter the SFTP Password of the system you want to access. The SFTP Password

Field	Description
	field supports alphanumeric characters that are case sensitive. This field does not support special character (+) and non-ascii characters. This is a mandatory parameter.

4. Choose [Save](#) to save your SFTP settings.

Note

You can delete an existing setting by clicking on the [Delete](#) button. However, if the SFTP destination (Destination Name) is used in any of the outbound integration, you will not be able to delete that setting.

Results

The newly created SFTP destination setting is added to the [Destination Settings](#) list.

You can search the [SFTP destination settings](#) by name or sort them in a particular order to narrow down your search results.

Related Information

[SFTP Settings](#)

[Generating Other Keys \[page 22\]](#)

8.2 Creating REST Destination Settings

Create SFTP destinations in Security Center. Here, you can create destination settings independent of an integration definition.

Prerequisites

You must have the [Create, Edit & Delete](#) access to [Access to Destination Settings](#) permission.

Procedure

1. Go to ► [Security Center](#) ► [Destination Settings](#) ►.
2. Click [Add](#) to create a new REST destination setting.
3. Enter suitable values for the fields in the settings window as described in the following table:

Field	Description
Name	Name of the REST destination settings. This is a mandatory parameter.
Type	Specifies the type of connection. Choose REST from the dropdown.
Endpoint URL	URL of the endpoint you want to connect. This is a mandatory parameter.
Authentication Type	Select the following authentication type from the dropdown: <ul style="list-style-type: none">• Certificate Based Authentication: Authentication is established with the endpoint using X509 certificates. X509 Certificates can be selected from the dropdown list.

Note

- To access X509 certificates, you must have the [View](#) access to [Access to X509 Certificates](#) permission.
Only [External CA](#) X509 certificates will be displayed in this list.
 - To generate a new X509 certificate, select [Click to manage X509 Certificates](#). For more information, refer to Generating X509 Certificates in the related information.
- [Basic Authentication](#): Allows you to connect to the endpoint using the username and password combination.
 - [User Name](#): Enter the user name of the system you want to access.
 - [Password](#): Enter the Password to access the system.

Note

Security Center does not support non-ascii characters in the password field.

Field	Description
	<ul style="list-style-type: none"> OAuth: OAuth specifies a process for resource owners to authorize third-party access to their server resources without sharing their credentials. When you select OAuth from the dropdown, you will see a list of configured OAuth 2.0 with SAML Flow and OAuth 2.0 with Grant type as Password and Client Credential configurations. <div> <p>Note</p> <ul style="list-style-type: none"> To access the list of OAuth Configurations from the dropdown list, you must have the View access to Access to OAuth Configurations permission. If you want to generate a new OAuth Configuration, select Click to manage OAuth Configurations For more information, refer to Creating OAuth Configurations in the related information. </div>

- Choose [Save](#) to save the REST settings.
- You can delete an existing setting by clicking on the [Delete](#) button.

Results

The newly created REST destination setting is added to the [Destination Settings](#) list.

You can search the [REST destination settings](#) by name or sort them in a particular order to narrow down your search results.

Related Information

[Creating OAuth Configurations \[page 8\]](#)

[Generating X509 Certificates \[page 17\]](#)

9 Setting Up a LinkedIn Account

Apply with LinkedIn is a feature that allows candidates to start the application process using their LinkedIn credentials. Use this tile to create customer LinkedIn account and select LinkedIn integrations.

Prerequisites

Before you use the new LinkedIn integrations, you need to:

1. Contact LinkedIn to set up an account with them.
2. Enable third party cookie in the browser.
3. Disable Popup blocker (to prompt the LinkedIn authorization username/password popup)
4. Make sure you have the following role-based permissions enabled to access [LinkedIn Account Setup](#):
 1. ► [Administrator](#) ► [Manage Integration Tools](#) ► [Manage LinkedIn Account Setup](#) ►.
 2. ► [Administrator](#) ► [Metadata Framework](#) ► [Access to non-secured objects](#) ► permission.

Context

LinkedIn is providing a new set of Integration points. When candidates apply with LinkedIn, an authentication window is displayed for them to enter their LinkedIn credentials. The authentication pop-up is a standard LinkedIn window and cannot be customized. Once the candidates authenticate with LinkedIn, they are logged into the application, and must exit it separately. Once the authentication with LinkedIn has been granted to a user, the user does not have to log in again for subsequent visits unless the user logs out or deletes the login cookie.

Procedure

1. On the [Security Center](#) dashboard, choose [LinkedIn Account Setup](#).
2. Select the [Enable Customer LinkedIn Account](#) checkbox.

You will be asked to sign-in to LinkedIn account, if you haven't signed-in to LinkedIn already.

3. Choose [Sign in](#) to sign-in to LinkedIn.
4. Create your LinkedIn account.

Once the account is created, you can see a list of contract signed in with LinkedIn which helps you to integrate and exchange data.

5. Choose the [Request](#) button to enable the integration.

A popup message is displayed, after the integration is enabled successfully.

Disabling the LinkedIn 2.0 Integration

6. The LinkedIn integration can be disabled or switched off by un-checking the [Enable Customer LinkedIn Account](#) checkbox. This will update the field [isLinkedInIntegrationEnabled](#) of the MDF object with value [No](#).

To activate the LinkedIn integration again, select the [Enable Customer LinkedIn Account](#) checkbox again. This will update the field [isLinkedInIntegrationEnabled](#) of the MDF object with value [Yes](#).

Note

Deactivating LinkedIn integration won't be communicated to LinkedIn.

Next Steps

Verifying successful LinkedIn Integrations

On the popup dialog of successful integrations, choose [Go back](#) to view the list of integration types which are enabled.

You can also verify the integration by checking the data in ► [Admin Center](#) ► [Manage Data](#) ► [search for LinkedInIntegrationConfiguration](#) ►. The [integrationStatus](#) should show [Active](#) along with [clientId](#), [clientSecret](#), [linkedinKey](#), [integrationContext](#) and so on.

Note

Integration may stop working if you alter any data manually.

10 Change History

Learn about changes to the documentation for Security Center in recent releases.

2H 2023

Type of Change	Description	More Info
Changed	We have moved the Change History to the end of the guide.	Security Center [page 3]

1H 2023

Type of Change	Description	More Info
New	Security Center contains detailed log information for <i>OAuth Configurations</i> , <i>X509 Certificates</i> , <i>Other Keys</i> , <i>HTTPS Trust Certificates</i> , and <i>Destination Settings</i> .	Security Center [page 3]

2H 2022

Type of Change	Description	More Info
New	Security Center supports OAuth 2.0 TLS Mutual Authentication.	OAuth 2.0 mTLS with Grant Type as Client Credential [page 15]
New	You can add custom parameters in the body of OAuth configurations.	OAuth 2.0 Settings Field Descriptions [page 9]
New	You have an option in <i>Security Center</i> to download the <i>Intermediate CA Certificate</i> .	Generating X509 Certificates [page 17]

1H 2022

Type of Change	Description	More Info
New	You can now search for the <i>Security Center</i> artifacts by name or sort them in a particular order to narrow down your search result.	Creating OAuth Configurations [page 8] Generating X509 Certificates [page 17] Generating Other Keys [page 22] Uploading HTTPS Trust Certificates [page 25] Configuring Destination Settings [page 29]

1H 2021



Type of Change	Description	More Info
July 09, 2021		
Added	Added information on an MDF permission that is required for <i>OAuth Configurations</i> .	Setting Up Permissions for Security Center [page 4]
May 28, 2021		
Added	Added a note for HTTPS Trust Certificates using <i>Root Certificate Authority (CA)</i> as the certificate type - the file format uploaded must be Base-64.	Uploading Root CA Certificates [page 26]
May 21, 2021		
New	We moved Security Center from Integration Center to Admin Center .	
New	<i>External CA</i> signed certificates and <i>SAP Cloud Root CA</i> certificates are supported for generating X509 Certificates.	Generating X509 Certificates [page 17]
New	<i>Root CA</i> certificates can be imported for HTTPS Trust Certificates.	Uploading Root CA Certificates [page 26]
New	<i>Scheduled Job Key</i> support for Decryption Key (PGP) generation.	Generating Other Keys [page 22]
New	<i>Certificate Based Authentication</i> is supported for REST-based integrations.	Creating REST Destination Settings [page 31]

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.

About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
 - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
 - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

© 2025 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.

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.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.