SAP SuccessFactors

PUBLIC

Document Version: 1H 2605 – 2026-07-15

Setting Up SAP SuccessFactors with Identity Authentication and Identity Provisioning Services

SAP

Content

1 When to Use SAP SuccessFactors with Identity Authentication

Determine if you have to set up your SAP SuccessFactors system to use Identity Authentication in SAP Cloud Identity Services.

> → Remember
>
> Identity Authentication is becoming the standard authentication method for SAP SuccessFactors. Basic authentication is being deprecated, and customers are expected to migrate to Identity Authentication before November 2026. If you're not already using Identity Authentication, you should plan to set it up.

There are two scenarios that require you to set up SAP SuccessFactors with the Identity Authentication service:

- **You want to integrate SAP SuccessFactors with other SAP applications.**
  For example, the Identity Authentication service is a prerequisite for using SAP Analytics Cloud and SAP Build Work Zone with SAP SuccessFactors. First, you have to set up the connection between SAP SuccessFactors and the Identity Authentication service. Then, you can connect to other dependent SAP applications, like SAP Analytics Cloud and SAP Build Work Zone.
- **You want your SAP SuccessFactors application to utilize time-saving functionalities that are possible with Identity Authentication.**
  For example, the Onboarding application can synchronize user-account changes in real time to Identity Authentication without having to manually run or wait for a scheduled job.
- **You need additional functionality that SAP SuccessFactors doesn't natively support.**
  Identity Authentication supports much more functionality than SAP SuccessFactors does natively. You want to take advantage of these features.

2 Important Notes About Using SAP SuccessFactors with Identity Authentication

Before you set up your SAP SuccessFactors system to use the Identity Authentication service, you should be aware of the following notes.

- **Data centers in different regions.** The Identity Authentication service has data centers in various global regions but they are not a one-for-one match with SAP SuccessFactors data centers. During authentication, some personal information is passed between SAP SuccessFactors and the service.
  When an Identity Authentication tenant is assigned to you, you're provided by email with details about your system, including the region of both your SAP SuccessFactors and Identity Authentication tenants.
  If you have any data protection and privacy concerns about the region your tenant is in, contact us to request a tenant in the appropriate region.
- **SAP NS2 support.** Eligible SAP SuccessFactors customers using SAP NS2 can migrate to the Identity Authentication service, however, the migration would be a manual process. Please contact SAP support to start this migration.
- **Changes to Company ID.** As with all integrations, the connection to the Identity Authentication service is impacted by a change in Company ID. If you ever need to change the Company ID of your SAP SuccessFactors system, you need to update the configurations in the Identity Authentication service accordingly. For more information, see the note: 2087436.
- **Username Case-Insensitivity**
  Identity Authentication uses case-insensitive usernames. To avoid login issues after upgrading, ensure that the *Enable Case-Insensitive Usernames* setting is enabled in *Admin Center* > *Company System and Logo Settings*. If this setting is not enabled, users must enter their username using the exact case stored in SAP SuccessFactors, which can lead to authentication failures.
- **Data Protection and Privacy.**
  If you use the Identity Authentication service, be sure to review the latest documentation to ensure that it meets your data protection and privacy requirements. For more information, see here.
- **Global Assignment and Concurrent Employment (GA/CE)** are supported for upgrade to the Identity Authentication service.
- **Integrated External Learners** and **Onboarding 2.0** are supported for upgrade to the Identity Authentication service.
- ⚠ Restriction

  After you've upgraded to the Identity Authentication service, you won't have the ability to turn on partial SSO in SAP SuccessFactors company Provisioning. By default, partial SSO is disabled after activating Identity Authentication. If needed, you can set up partial SSO in Identity Authentication.

  After you've upgraded to the Identity Authentication service, you won't have the ability to enable multiple SAML asserting parties in SAP SuccessFactors company provisioning. By default, Identity Authentication will be enabled as the single SAML asserting party in the SAP SuccessFactors provisioning setting after activating Identity Authentication. If you need multiple asserting parties, you can accomplish this by setting up conditional authentication.

> → Remember
>
> 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.

- **Removal of unique email address**: We do **not** recommend that you use the feature that allows you to create a non-unique, null, or blank emails. This feature is not supported by all SAP SuccessFactors product areas so we recommend that you do not use this functionality.
- *SHA-256* is the default hashing algorithm for signing certificates for all integrations. *SHA-1* is **not** recommended as *SHA-256* provides a higher level of security.
- When you are onboarding employees and you need to activate those users after you've migrated to the Identity Authentication service, follow the procedure described in **Activating an Account and Setting New Password After Identity Authentication Service is Enabled**. For more information, refer to this topic in Related Information section.

Related Information

Activating an Account and Setting New Password After Identity Authentication Service Is Enabled

3 Email Templates and Branding Themes

You can use email templates and branding themes to support your company's themes.

Email Templates

The Identity Authentication service has email templates for new users, password resets, etc. You'll want to review these and customize them to meet your needs. There are predefined email templates for user and administrator-related emails. You can also create a custom template set. Unless you have another way to communicate the initial logon URL to your users, we recommend you add a basic logon URL to the New User email.

When Identity Authentication is enabled, welcome and activation emails are handled by the Identity Authentication service. The welcome email from the SAP SuccessFactors email notification templates is no longer required. For more information, see 3321943.

Themes and Branding

The Identity Authentication service supports basic settings for themes and branding. You can add logos, change colors, etc. to the login page and others in Identity Authentication. You will want to review and set them up to meet your needs. For more information, see Related Information.

Related Information

Define an Email Template Set for an Application
Choose and Configure a Branding Style for an Application

4 Guidance on Migrating to Identity Authentication in SAP Cloud Identity Services

All SAP SuccessFactors systems can use the Identity Authentication service. While the SSO signing certificate used for authentication will expire on June 2, 2025, the final deadline for completing migration to Identity Authentication is November 2026..

> ⚠ Caution
>
> **For customers still using 3rd Party IDP or Basic Authentication (Username and Password)**:
>
> - The SSO signing certificate used by both Identity Authentication and 3rd party IDPs for authentication is set to expire on June 2, 2025. In addition, Google is phasing out support for third-party cookies in Chrome browsers in the second half of 2024.
> - Upon the expiration of this SSO certificate, if it is not updated, SSO authentication via IDP will not work, preventing users from access to your SAP SuccessFactors applications.
> - Customers still using basic authentication will also not be able to adopt the latest security and compliance requirements for cloud applications upon deprecation of 3rd party browser cookie support.
> - We **strongly** recommend that you migrate to Identity Authentication to avoid disruptions and for the best integration experience with SAP SuccessFactors.

> ⓘ Note
>
> **For customers who migrate to Identity Authentication**:
>
> - For customers/tenants using Identity Authentication (either as a real IDP or proxy IDP to a 3rd party coporate IDP, Identity Authentication will take care of their certificate update automatically.
> - If Identity Authentication is the real IDP for SuccessFactors, then SAP will handle the upgrade necessary to minimize the impact of 3rd party coookie deprecation. If Identity Authentication is proxy to a corporate IDP such as Microsoft Azure AD, Okta, Google, etc, SAP will provide automation to assist the upgrade necessary to minimize the impact of third party cookie deprecation. There could be further configuration needed.
> - When your SAP SuccessFactors is connected to the Identity Authentication service, it handles all logins (including password, two-factor authentication, risk-based authentication or corporate identity provider) for your SAP SuccessFactors system.
> - Identity Authentication allows HCM suite customers to complete a major Identity Authentication pre-requisite for some of the most important innovations of SAP SuccessFactors solutions i.e. Story Reports, Work Zone, Task Center, Internal Career Site, etc.
> - Faster innovation and better product quality/support with one unified authentication services to develop, maintain and innovate.
> - Better incorporation of new technologies and innovations in the security/authentication domain.
> - Streamlined user management across the enterprise and better user self-services.

For the latest announcements on migration dates and 3rd party cookie deprecation, refer to the Customer Community-Migration to Identity Authentication and Customer Community-Impact of Third-Party Cookie Deprecation..

5 Handling Customer Migration Scenarios in Identity Authentication

Learn how to handle different migration scenarios for SSO users authenticating with a corporate IDP (without Identity Authentication), partial SSO users, and Onboarding users undergoing a status change (e.g., new hires to alumni transitions).

When migrating to Identity Authentication, understanding the different migration behaviors for each customer group helps ensure a smooth transition. The following approaches outline best practices for managing each migration scenario.

1. **SSO Users Authenticating Through Corporate IDP**
    - **Current Setup**: These users authenticate through their company's corporate Identity Provider (IDP) (e.g., Azure AD, Okta).
    - **Migration Behavior**:
        - **Before Identity Authentication is activated**, these users continue to authenticate directly through their corporate IDP.
        - **After Identity Authentication is activated**, it can serve as the proxy IDP, but users can still choose to authenticate via the corporate IDP if preferred.

          > ⚠ Caution
          >
          > Direct integration with SAP SuccessFactors through the corporate IDP will be deprecated in November 2026, so users should plan to transition to using Identity Authentication as the proxy IDP before this date.

        - No need to include these users in the Identity Provisioning sync job unless they require access to features such as SAP Analytics Cloud or People Stories in Analytics. For these features, Identity Authentication must first be activated, and the relevant IPS sync job must be run to sync the users' data to Identity Authentication.

2. Partial SSO Users Using SAP SuccessFactors Username and Password Authentication

- **Current Setup**: These users log into SAP SuccessFactors directly with their username and password, which means they are still using basic authentication.
- **Migration Scenario**:
    - These users must migrate to Identity Authentication before the deprecation of basic authentication. Once synced using Identity Provisioning, the Identity Authentication service will manage their authentication.
    - Define conditional authentication rules in Identity Authentication:
        - Full SSO users (those who authenticate through the corporate IDP) will continue to be routed to the corporate IDP for authentication.
        - Partial SSO users (who still use SAP SuccessFactors username and password) will authenticate via the Identity Authentication login screen, rather than using basic authentication.

          > → Remember
          >
          > Partial SSO will be disabled in November 2026 to ensure all authentication requests go through Identity Authentication for consistency. After the deprecation, users still relying on basic

> authentication must authenticate using this service, and they will no longer be able use SAP SuccessFactors directly for login.

3. Users in Onboarding Undergoing a Status Change (e.g., Employees, New Hires, Alumni)

- **Scenario**: Users may undergo a status change, such as transitioning from an employee to an alumni.
- **Migration Behavior**:
  - **New Hires**: Onboarding customers can enable Identity Authentication for new hires by integrating with the SCIM API and completing the upgrade from the OData V2 API if their migration to Identity Authentication was prior to December 9, 2022. Once configured, both employees and new hires are authenticated using Identity Authentication. For more details and prerequisites, refer to the **Authenticating New Hires with Identity Authentication in SAP Cloud Identity Services** in the **Related Information** section.
  - **Existing Employees**: For current employees, upgrade to/enable Identity Authentication. If your system is still utilizing the OData V2 API, upgrading to the SCIM API is required to ensure consistent authentication processes across all user types. This upgrade facilitates seamless synchronization and authentication via Identity Authentication. For more information, refer to Initiating the Upgrade to Identity Authentication and **Upgrade from ODATA Identity Provisioning Connector to SCIM Connector with SAP SuccessFactors HCM Suite** in the **Related Information** section.
  - **Alumni**: Once you've completed the steps in Enabling Alumni Access, you can initiate or schedule a delta sync job in Identity Provisioning to update the former employee's status to *Alumni* in Identity Authentication. This will initiate an activation email that the alumni user can use to authenticate back into SAP SuccessFactors with Identity Authentication so they can access important company materials after leaving the organization. Refer to Configuring the Alumni Activation Email Template in Identity Authentication.

Related Information

Authenticating New Hires with Identity Authentication in SAP Cloud Identity Services [page 82]
Upgrade from ODATA Identity Provisioning Connector to SCIM Connector with SAP SuccessFactors [page 139]
Initiating the Upgrade to Identity Authentication in SAP Cloud Identity Services [page 40]

6 Benefits of Using Identity Authentication in SAP Cloud Identity Services

Here are some of the important benefits of setting up your SAP SuccessFactors system to use the Identity Authentication service.

- **Connection to other SAP solutions.** Using the Identity Authentication service as an identity provider is the first step to enabling future integrations with other SAP solutions.
- **More login options.** The Identity Authentication service supports username and password login and SAML 2.0 SSO login, just like SAP SuccessFactors does now. It also supports two-factor/token authentication, Social Sign On, SPNEGO, and some Corporate User Stores.
- **More security.** The Identity Authentication service supports SHA-256.
- **Better user experience.** The Identity Authentication service provides a better logon experience than the current SAP SuccessFactors Partial SSO option.
  - No password-specific URL required for first-time login.
  - If user clears cookies, they need to enter email or username again.
- **Conditional Authentication.** You can set up the Identity Authentication service to direct users to either a corporate identity provider or a password login option, based on conditional rules. You can use this feature to replace the current SAP SuccessFactors Partial SSO and Multiple Asserting Party Selection features.
- **Risk-Based Authentication.** You can set up the Identity Authentication service to require different login methods, such as password, two-factor authentication, or Social Sign On, based on risk-based rules.
- **Stand-alone Identity Provider.** As the Identity Authentication service is enhanced, you can use new features.
- **Self-service.** You can access common SSO settings from SAP SuccessFactors *Admin Center* and all other configuration options directly in administration console of your Identity Authentication tenant.
- SuccessFactors customers get Identity Authentication as part of their license, and this enterprise-grade Identity Access Management feature is included free of charge.

7 Single Sign-On for SAP SuccessFactors

Single Sign-On (SSO) is a property of access control of multiple related, but independent software systems. With this property, a user logs in once and gains access to all systems without being prompted to log in to each of them.

Single Sign-on allows users to access your SuccessFactors instance without entering their username and password each time. Instead of manually logging in to the SAP SuccessFactors application, users are authenticated by your Identity Provider (IdP) and then logged into SAP SuccessFactors automatically.

Single Sign-On can be enabled for all users of your system or for a partial subset of users (called "Partial SSO").

Most customers use the SAML 2.0 protocol to set up Single Sign-On for their instance, but we support a number of other SSO options as well.

SAML 2.0

Security Assertion Markup Language (SAML) is an XML-based, open-standard SSO protocol for exchanging authentication and authorization data between an identity provider (IdP) and a service provider (SP).

> → Remember
>
> SAML 2.0 is the recommended method of configuring Single Sign-On for SAP SuccessFactors.

7.1 How Does SAML 2.0 Work?

SAML 2.0 is the recommended method of configuring Single Sign-On for SAP SuccessFactors.

How does SAML 2.0 work?

SSO generally takes place between two parties, the identity provider (IdP) and the service provider (SP). The identity provider has information required to authenticate the users and generate SSO logins. The service provider offers a service that is accessible using with SSO.

The SP must be able to accept IdP-generated SSO logins and identify the user who wants to log in. In this case, SAP SuccessFactors is the service provider, or SP. You can use your own IdP to authenticate users and log them into SuccessFactors.

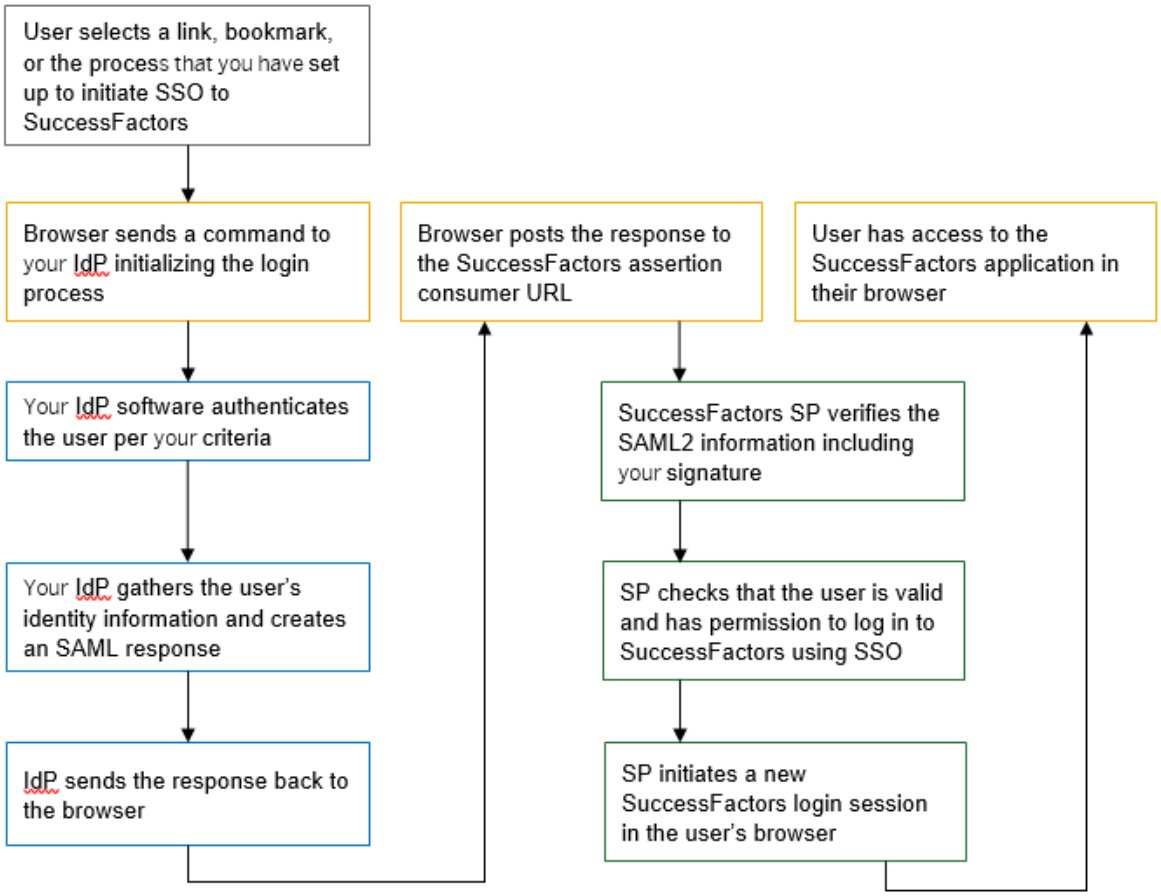
We support the following SAML2 protocols:

- IdP-initiated login, where a user starts the process internally.

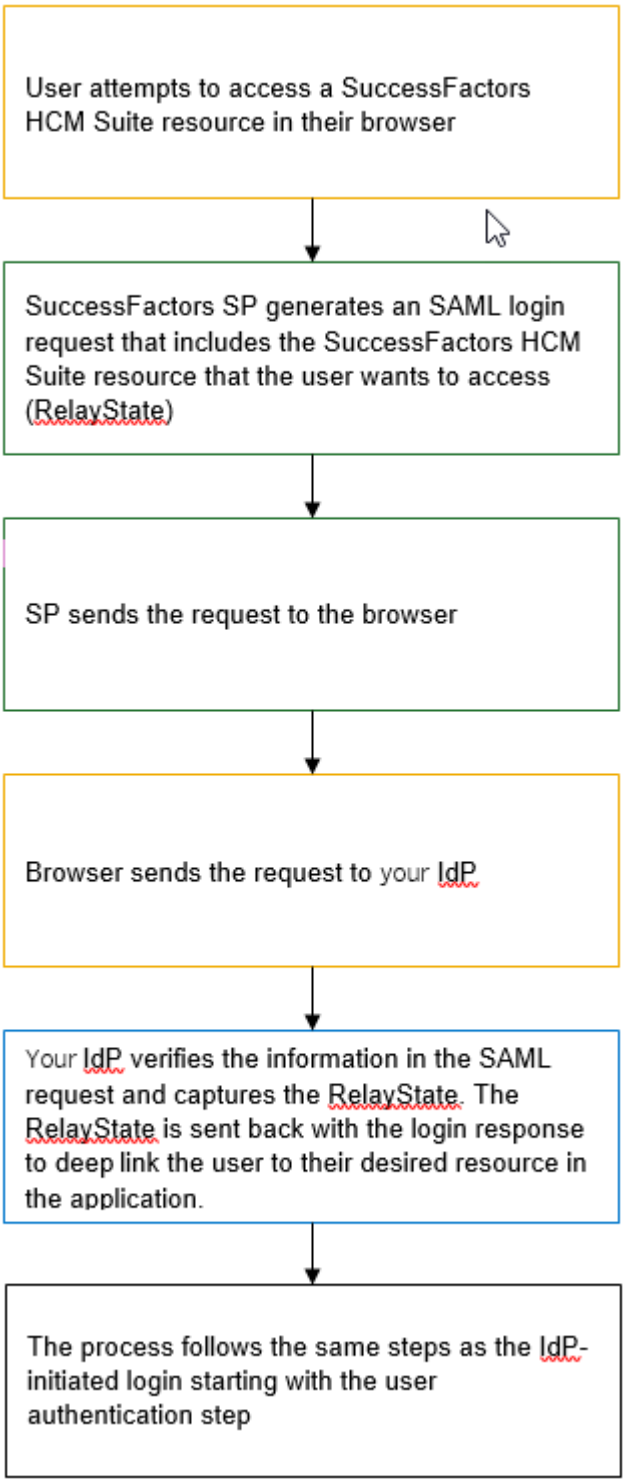
- SP-initiated login, where a user starts the process by attempting to connect to SAP SuccessFactors

Here's how these processes work:

Identity Provider (IdP) Initiated SAML Single Sign-On



Service Provider (SP) Initiated SAML Single Sign-On



7.2 SAP SuccessFactors Implementation of SAML 2.0

The SAML2 specification provides a general framework to ensure SAML identity providers (IdP) and service providers (SP) work together properly. Within that framework, service providers offer features that best support their application and their customers. SAP SuccessFactors offers the following:

IdP and SP Logins

You can connect using either or both. The default setup is for SP-initiated and this must be completed for all SSO customers. Additional settings need to be configured to allow the optional IdP-initiated logins.

Dynamic Deep Linking

The SP-initiated login option is designed to allow users to deep link to some place other than the default landing page after an SSO login. For example, the SAP SuccessFactors application typically sends users to our home page. With deep linking, they can land on their performance review or a course in SAP SuccessFactors Learning or countless other locations within the application. When a user is not logged in and tries to access SAP SuccessFactors, we send an SAML request to your identity provider URL. The response contains the login information and landing page details in an additional value called RelayState.

If you do not support SP-initiated SAML2, we offer a generic deep link feature. This accomplishes the same result (deep linking) as SP logins, but uses cookies. When a user is not logged in and tries to access SAP SuccessFactors, we send their browser to the IdP-initiated URL that you provided. This is typically the same URL that users use to log in directly from their internal systems. The user goes through the IDP-initiated login process. After they are logged in, we read a cookie that was stored with their initial destination, and place them there instead of on the home page.

If you have both deep linking and SP-initiated logins enabled from a single IdP, we use SP-initiated rather than deep linking.

Dynamic deep linking should work with all links sent out by the application itself. These include things sent in system emails, course links generated by SAP SuccessFactors Learning administrators, exported JAM links, and so on. We do not recommend copying the URLs directly from the browser and using them for bookmarks. There is no guarantee that a URL in the browser will create a valid link, or that a link will be valid in the future.

Static Deep Linking

If you use IdP-initiated logins, you can provide us with a RelayState value to send users somewhere other than the home page. We provide a list of supported RelayState values if you plan to use this option.

SP-Initiated Single Logout

You may want to perform some action in your home system when a user logs out of SAP SuccessFactors. If you provide us with the destination URL, we can send a logout request when a user ends a SAP SuccessFactors session.

Multiple Asserting Parties

If you have multiple identity providers, we can set up asserting parties for each one. This includes separate values for SAML issuer, signing certificate, and other settings. If one or more of the asserting parties is set to use SP-initiated logins, one of them can be set to be the default asserting party.

If you have multiple asserting parties and use deep linking, we need to identify to which IdP to send users for login information. If you have a default asserting party, we send them to that IdP. If not, we display a list of the available asserting parties and ask the user to select the appropriate one. Your administrator can configure the text identifying each available asserting party. After a user has logged on using a specific asserting party, we store a cookie in their browser. As long as they use the same browser and don't clear their cookies, they don't need to select the asserting party again.

> ### Note
>
> All SAP SuccessFactors tenants must migrate to Identity Authentication in SAP Cloud Identity Services by November 2026. Support for multiple asserting parties will also be deprecated by that date. If you currently use multiple asserting parties, please migrate to Identity Authentication and set up multiple corporate identity providers in Identity Authentication for the multiple asserting parties. Once migrated to Identity Authentication, there should be only one active asserting party in each SAP SuccessFactors tenant.

SSO Redirects

By default, the SAP SuccessFactors application shows users the login page when they log out, time out, or when certain login issues occur, unless custom redirect pages are configured. You can host your own pages for these use cases. If you provide us with the URL for each page, we configure our SSO system to send the users there instead of the home page. We can redirect for the following use cases:

Use Case	Description
Logout	When the user logs out, we send them to the customer-hosted page.
Timeout	After a 30-minute inactivity timeout, we send the user to this page. **Note** For Identity Authentication and Identity Provisioning timeout information, refer to the **Related Information** section.

Use Case	Description
Invalid login	If the SSO login fails, the application redirects users to a static invalid login page by default. If a customer-hosted page is configured for this use case, the system redirects to that page instead.
Invalid Login Path by External Users	The SAP SuccessFactors HCM suite application requires a valid login path. If the user's login path is inconsistent with the login method, we send the user to this page.
Missing credentials	If the SAP SuccessFactors application receives an SSO login with no user information, we send the user to this page.
Deep link	Your IdP login link goes here if you plan to deep link, but are not using SP-initiated SAML. **Note** Deep linking is not applicable when the SAP SuccessFactors tenant is integrated with Identity Authentication.

Partial Organization SSO

Partial Organization SSO will be deprecated by November 2026, with the deprecation of SAP SuccessFactors to corporate identity provider direct integration.

Enablement of partial organizational SSO when SAP SuccessFactors is directly integrated with a corporate identity provider allows some users to use SSO via the corporate identity provider while others log in with SAP SuccessFactors usernames and passwords. No single user can have access to both methods at the same time. When a SAP SuccessFactors tenant is integrated with Identity Authentication, partial organization SSO is disabled by default. SSO users are subject to the password policy and features specified on the corporate identity provider.

Related Information

SAP Cloud Identity Services - Identity Authentication-Configure Session Timeout
Session Management - Handling Session Timeout

7.3 SAP SuccessFactors SAML 2.0 Technical Details

The SAP SuccessFactors service provider is configured to accept a wide variety of SAML responses and assertions. However, your IdP must adhere to the following rules:

HTTPS Encryption and POST

All communication with the SAP SuccessFactors application must use HTTPS in the browser. SAML responses sent to SAP SuccessFactors must use POST. URLs sent to deep link into the application and SAML requests do not need to be POSTed.

User Identifier

SAP SuccessFactors accepts two values to identify the user logging in using SAML2. The most common is NameID. We also support the UserName attribute. Whichever method is used, the value is compared with the UserName in the SAP SuccessFactors application. If that user does not exist or does not have permission to log in, the user is unable to access the application.

The system checks for the UserName attribute first. In the assertion, the SAP SuccessFactors application expects something similar to the following:

Sample Code

```
<saml:AttributeStatement xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
<saml:Attribute Name="username"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
<saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string"> jdoe</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

If the UserName attribute is not found, the SAP SuccessFactors application looks for the NameID value. In the assertion, theSAP SuccessFactors application expects something like the following:

Sample Code

```
<Subject><NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified">jdoe</NameID><SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><SubjectConfirmationData
InResponseTo="_f6e21384-e33b-4a5f-a532-e58ce3f0a5e2"
NotOnOrAfter="2014-10-21T16:30:56.599Z" Recipient="https://
performancemanager4.successfactors.com/saml2/SAMLAssertionConsumer?
company=TestCompany"/></SubjectConfirmation></Subject>
```

Notice that in addition to NameID, there is nameid-format: unspecified. SAP SuccessFactors expects a nameid-format. Typically, you send the value unspecified. SAP SuccessFactors accepts other common values like

persistent or transient. However, there is no support for these other options. Irrespective of the nameid-format sent, SAP SuccessFactors simply compares the NameID from the login to the username in the application. The only exception is the UserName attribute that is sent. In that case, the NameID is ignored entirely.

Certificates and Signatures

SAP SuccessFactors expects the SAML logins to be signed by your certificate. The signature can be on the response, assertion, or both. To verify the signature, you need to provide SAP SuccessFactors with your X509 signing certificate. SAP SuccessFactors accepts both CA and self-signed certificates.

SAP SuccessFactors provides an X.509 certificate for you to encrypt assertion elements if desired. The same certificate is used to sign SP-initiated logout requests.

If you use SP-initiated logins, we provide the X.509 certificate used to sign the SAML login requests.

IP Address Restrictions

SAP SuccessFactors allows you to restrict logins to specific IP addresses or ranges. This feature does not require SSO. However, it applies to SSO logins if SSO is enabled.

Information Exchanged to Set Up SAML2

In order to set up SAML2 between SAP SuccessFactors and your applications/identity provider (IdP), the below sections list the information that would need to be exchanged. SAP SuccessFactors can provide and receive metadata files. SAP SuccessFactors does not provide an automated exchange of metadata files. To obtain an SAP SuccessFactors metadata file, refer to **Public API to Retrieve Customer SSO Service Provider Metadata** in the **Related Information** section.

SAP SuccessFactors provides:

- X.509 certificate that you can use to encrypt assertion values
- SAP SuccessFactors entity ID values

The SAP SuccessFactors entity ID is unique for each SAP SuccessFactors customer instance.

- Assertion consumer service URL

This URL is unique for each SAP SuccessFactors customer instance.

- Global logout response handler URL

This URL is unique for each SAP SuccessFactors customer instance.

You provide:

- X.509 certificate used to sign the response or assertion
- SAML issuer or IdP entity ID

• If you are using IdP-initiated logout, SAP SuccessFactors needs your global logout service URL

• If you are enabling IP address restrictions, SAP SuccessFactors needs the list of IPs

• If you are using the SAP SuccessFactors redirect pages (highly recommended), SAP SuccessFactors needs the URL for each

Timestamps and Server Synchronization

SAML2 requires you to send and SAP SuccessFactors to respect NotBefore and NotAfter values that define when a login is valid. These values are always sent in GMT/UTC. SAP SuccessFactors syncs server time to public time servers on a regular basis. You are expected to do the same. However, there still may be slight variances in the clocks. SAP SuccessFactors asks you to allow a small window of NotBefore time to prevent login failures if server time gets slightly out of sync.

RelayState

If you use IdP-initiated logins, you can specify a RelayState value to deep link your users to a specific page in the application. RelayState is optional. RelayState must be a relative URL, for example `/sf/admin`, not an absolute URL. You can see a list of examples that can be used as valid RelayState values on List of SAP SuccessFactors Deep Links under the **Deep Link** column.

Related Information

Public API to Retrieve Customer SSO Service Provider Metadata [page 122]

7.4 Example of Typical Login Response (Decoded)

SAP SuccessFactors accepts a wide variety of formats and values in the SAML2 response. The following is a typical example. Your provided responses may differ.

Sample Code

```
<samlp:Response ID="gf8b65pFRW3JOvrV9z8_fjCJJtO"
    IssueInstant="2009-02-09T11:52:09.484Z" Version="2.0"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
idp1.test.org</saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#" />
```

```
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1" />
            <ds:Reference URI="#gf8b65pFRW3JOvrV9z8_fjCJJtO">
                <ds:Transforms>
                    <ds:Transform
                        Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#">
                        <ec:InclusiveNamespaces PrefixList="ds saml samlp xs xsi"
                            xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#sha1" />
                <ds:DigestValue>8crrNj4pAptpLQKlAzbsS37tfOI=
                </ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
            bdmIryj5+K9tGsK7sO89j0UwBNQDRee8XpF/
aDY61ERrazaIC1NFwfXN6ETdz61gU5EKY5tJkaHR

YjYTTr8NG1JwSj8JCGePoabuh3KbjgNuE21nQ8JY0TcttPZGMysD4NOzkLIGOTKARp2BUVx7COJC
            egN9yX+SNphxlWD2vMQ=</ds:SignatureValue>
    </ds:Signature>
    <samlp:Status xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"
            xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" />
    </samlp:Status>
    <saml:Assertion ID="xv5BP-.Sl_aNbpsNwMX259HTgxL"
        IssueInstant="2009-02-09T11:52:09.500Z" Version="2.0"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
        <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">idp1.test.org
        </saml:Issuer>
        <saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
            <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"> lhadley</
saml:NameID>
            <saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                <saml:SubjectConfirmationData
                    InResponseTo="_F499B815F2BA7AB15F1207741929643"
NotOnOrAfter="2010-04-09T11:57:09.515Z"
                    Recipient=" https://performancemanager.successfactors.com /
saml2/SAMLAssertionConsumer" />
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions NotBefore="2009-02-09T11:47:09.500Z"
            NotOnOrAfter="2009-12-09T11:57:09.500Z"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
            <saml:AudienceRestriction
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                <saml:Audience>https://www.successfactors.com
                </saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement AuthnInstant="2009-02-09T11:52:09.500Z"
            SessionIndex="xv5BP-.Sl_aNbpsNwMX259HTgxL"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
            <saml:AuthnContext
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                <saml:AuthnContextClassRef>
                    urn:oasis:names:tc:SAML:2.0:ac:classes:Password
```

```
                </saml:AuthnContextClassRef>
            </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
            xmlns:xs="http://www.w3.org/2001/XMLSchema">
            <saml:Attribute Name="password"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"
                    xsi:type="xs:string"> lhadley</saml:AttributeValue>
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

8 Performing Single Sign-On Configuration Checks in SAP SuccessFactors

Learn how to use the new Single Sign-On (SSO) configuration checks in the Check Tool for SAP SuccessFactors. These checks assist with diagnosing, resolving, and ensuring the proper configuration and compliance of SSO settings.

Prerequisites

- You have enabled the Metadata Framework
- You have the following *Administrator* > *Check Tool* permissions:
  - *Access Check Tool* authorizes users to access the tool.
  - *Allow Check Tool Quick Fix* authorizes users to run quick fixes for the checks that have this feature. A quick fix can be used to immediately correct any issues found by that check.
  - *Allow Configuration Export* authorizes users to attach configuration information to a ticket.

Context

The new SSO configuration checks within the Check Tool help administrators identify their current authentication setup by determining whether tenants are using basic authentication, directly integrating with a corporate Identity Provider (IdP), or already utilizing Identity Authentication in SAP Cloud Identity Services.

These checks also validate that tenant SSO settings align with SAP SuccessFactors security and compliance requirements, offering assurance that configurations meet recommended standards. Where adjustments are necessary, the Check Tool provides guidance on migrating to Identity Authentication, enabling organizations to stay ahead of security requirements and transition smoothly to SAP SuccessFactors preferred authentication protocols.

Procedure

1. Go to *Admin Center* > *Check Tool*.

   The *Check Tool* page opens displaying the results of the first tab *System Health*.
2. Under the *Authentication / Single Sign-On (SSO)* section, select the particular checks that you want to run.

   You can also enter this section name in the search bar so that it gets displayed in the results table.
3. Choose *Run Checks* from the top right of the results table.

> **Note**
>
> If the check you selected requires one or more prechecks (checks that need to be run successfully first), the prechecks are run first even if you haven't selected them.

The *Results* column displays any issues found.

8.1 Check Results

After you run checks in the check tool, it returns the results of the checks so that you can resolve the issues found.

The results of a check are displayed in the *Result* column. If you run the checks multiple times to see how you're resolving issues, you can select a previous result from the *History* dropdown list.

> **Note**
>
> To display the *History* dropdown list, select a check. On the details screen that opens on the right side of the page, expand the header. The *History* dropdown list is directly below the check title.

Possible Results of Check Tool

Result	Action
No issues found	If the tool can't find issues, you see a green check mark in the *Result* column.
Issues found	If the tool finds issues, it reports the number of issues and a yellow ⚠ *(Warning)*icon or a red alarm icon. • The yellow icon indicates a low severity issue. The system proposes a solution. • The red icon indicates a high severity issue. You must take action, which could include creating a support ticket.
Pending migrations	If the tool finds pending migrations that need to be completed by the user, you can see a yellow warning icon or a red alarm icon in the *Status* column on the *Migration* tab.
Completed	If the tool finds no issues with migration, or the migration has already been completed, you see a green check mark in the *Status* column on the *Migration* tab.

> **Note**
>
> - Select the *Export Results* button to download the check results. Ensure you run the check before exporting the check results. If not you can view only the first 100 check results.
> - The downloaded check result table can display a maximum number of 10,000 rows.

8.1.1 Creating Technical Support Tickets from the Check Tool

When the check tool reports a serious issue that you can't solve, you might need to contact Technical Support. You can create a support ticket from within the check tool.

Prerequisites

You've run the check tool. You can find the check tool by going to *Admin Center* > *Check Tool*. You create the ticket from the details page of the tool.

Procedure

1. Select the check you can't solve.

   The detail view opens to the right side of the screen with more information on the check and on how to solve the issue.
2. On the *Result* tab, scroll down to the results table to look for the errors you want to report on.

   You usually contact Technical Support for high severity issues not low severity issues.
3. On the *Check Information* tab, under *Need Assistance?*, copy the component ID.

   For example, LOD-SF-EC is the component ID for Employee Central.
4. Create a customer case in the relevant category.
5. When you create the ticket, paste the component ID into the ticket.

9 Checking to See if You Already Have Identity Authentication Enabled

Confirm whether Identity Authentication is already enabled for your SAP SuccessFactors tenant.

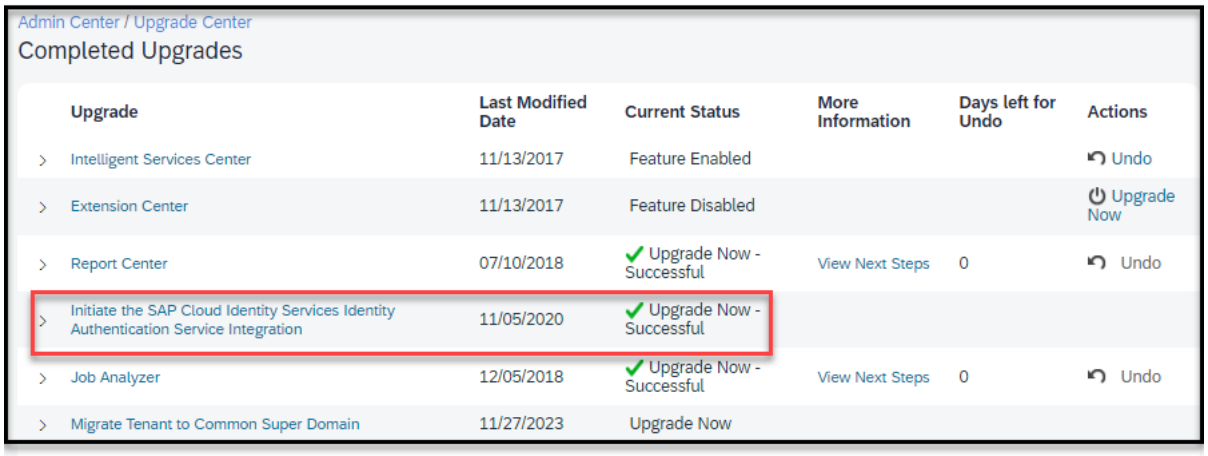
Context

Depending on when you've enabled Identity Authentication, you may already have received the new enhancements that come with this upgrade. These enhancemntes include X.509 certificate-based authentication in conjunction with the System for Cross-domain Identity Management (SCIM) API, which are the latest methods of authentication and integration with Identity Authentication and Identity Provisioning. These features are enabled automatically for upgrades to Identity Authentication that occur from December 9, 2022 onwards.

Complete the steps below to confirm if and when you've enabled this feature.

Procedure

1. Navigate to *Admin Center* > *Upgrade Center* > *View Recently Completed Upgrades*.
2. Look for the upgrade called *Initiate the* SAP Cloud Identity Services Identity Authentication *Service Integration*.
3. Under the *Current Status* column, look for the status *Upgrade Now - Successful*.



4. In the *Last Modified Date* column next to the status, confirm whether the date is before or after December 9, 2022.

> ### Note
>
> Customers who enabled Identity Authentication as of November 29, 2024 or later will already have a hybrid SAML/OpenID Connect application configured for their SAP SuccessFactors tenant. This hybrid application supports both SAML and OpenID Connect authentication flows. If you need to register or

manage your OpenID Connect client application, please refer to **Register Your Own Application to Communicate with SAP SuccessFactors HCM Suite** in the **Related Information** section.

Next Steps

If you've enabled Identity Authentication from December 9, 2022 or later, go to **Getting Started with Identity Authentication Already Enabled** in the **Related Information** section for next steps.

If you've enabled Identity Authentication **before** December 9, 2022, or have not enabled it at all, go to **Existing Customers (Before December 9, 2022) Start Here**.

Related Information

Getting Started with Identity Authentication Already Enabled [page 28]
Existing Customers (Before December 9, 2022) Start Here [page 30]
Register Your Own Application to Communicate with SAP SuccessFactors HCM Suite with OpenID Connect [page 125]

9.1 Getting Started with Identity Authentication Already Enabled

If you've already enabled Identity Authentication from December 9, 2022 onwards, you've already been set up with X.509 certificate-based authentication, the Workforce SCIM API, as well as the the option to authenticate both your Employees and New Hires with Identity Authentication because of the SCIM integration provided (refer to **Authenticating New Hires with Identity Authentication in SAP Cloud Identity Services** in the **Related Information** section).

Context

> **Note**
>
> For a list of commonly asked questions in 2H 2022 regarding the SAP SuccessFactors HCM suite to Identity Authentication/Identity Provisioning integration, refer to our Frequently Asked Questions page.

Having your Identity Authentication tenant already enabled means that you don't need to complete the steps to initiate the upgrade to Identity Authentication and have it activated. You should have already received your welcome email called **Access Information for your SAP SuccessFactors HCM suite**, as well as an activation email from the Identity Authentication service. Complete the below steps to login for the first time and access the Identity Authentication and Identity Provisioning administration consoles.

Procedure

1. Follow the steps in the activation email sent to you from the Identity Authentication service.
2. Click on the **SAP SuccessFactors HCM suite** URL in the welcome email called **Access Information for your SAP SuccessFactors HCM suite**.
3. On the login screen, enter the **Identity Authentication** username provided in the welcome email.
4. Enter the password you set up per the instructions in the **Identity Authentication activation email.**.

   You will then be redirected to the SAP SuccessFactors HCM suite homepage.
5. Next, you can click on either the **Identity Authentication** or **Identity Provisioning** URLs in the **Access Information for your SAP SuccessFactors HCM suite** welcome email to access these administration consoles and review their default configurations.

> ### Note
>
> To perform further configurations to each console as needed, refer to **Identity Authentication Service Administration Console Tasks** and **Identity Provisioning Service Administration Console Tasks** in the **Related Information** section.

> ### Note
>
> If you are a SAP SuccessFactors HCM suite user for an already existing Identity Authentication tenant and you have no administrative privileges, follow the instructions in the **Advanced Identity & Access Management** section of your welcome email to contact your Identity Authentication administrator to have you added as a user in the administration console or perform further configurations as needed.

Related Information

SAP Cloud Identity Services Administration Console Tasks [page 113]
Identity Provisioning Service Administration Console Tasks [page 135]
Authenticating New Hires with Identity Authentication in SAP Cloud Identity Services [page 82]

10 Existing Customers (Before December 9, 2022) Start Here

If you're an existing customer, depending on if and when you've completed the upgrade to Identity Authentication, there are a few upgrades you'll need to make based on your scenario (to confirm whether you've upgraded already and when, refer to **Checking to See if You Already Have Identity Authentication Enabled** in the **Related Information** section).

If you haven't yet upgraded to the Identity Authentication service, refer to **Initiating the Upgrade to Identity Authentication in SAP Cloud Identity Services** in the **Related Information** section to complete this upgrade.

If you've already completed this upgrade before December 9, 2022, it is possible that your Identity Authentication tenant is still using the OData API for use with the Identity Provisioning service, and that you are using Basic Authentication as your authentication method.

It is **highly** recommended that you upgrade from this API to the new **SCIM API** for use with Identity Provisioning, along with upgrading from basic authentication to **mutual Transport Layer Security (mTLS)** (certificate-based authentication) as this provides better security, better management of user data, and a more simplified experience with your Identity Authentication service. To make both of these upgrades, complete the steps in **Upgrade from OData Identity Provisioning Connector to SCIM Connector with SAP SuccessFactors HCM suite** in the **Related Information** section.

If you're already using the SCIM API, but have never upgraded to mTLS, then perform this upgrade by following the steps in **Upgrade to X.509 Certificate-based Authentication for Incoming Calls to SAP SuccessFactors HCM suite**.

Related Information

Overview of the SAP SuccessFactors and Identity Authentication Service Integration (Video) [page 31]
Initiating the Upgrade to Identity Authentication in SAP Cloud Identity Services [page 40]
Upgrade from ODATA Identity Provisioning Connector to SCIM Connector with SAP SuccessFactors [page 139]
Upgrade to X.509 Certificate-Based Authentication for Incoming Calls [page 36]
Checking to See if You Already Have Identity Authentication Enabled [page 27]

10.1 Scenarios for Existing Customers with Identity Authentication Automatically Enabled

After December 9, 2022, there are certain scenarios in which existing customers may have Identity Authentication and Identity Provisioning automatically enabled.

Scenarios in which existing customers would have Identity Authentication and Identity Provisioning automatically enabled after December 9, 2022 are:

- If you're an existing customer with SAP SuccessFactors HCM suite tenants that **have already** completed the upgrade to Identity Authentication, **any additional** (new) SAP SuccessFactors HCM suite tenants will have the upgrade and activation of Identity Authentication with Identity Provisioning done for them automatically.
- If you're an existing customer with SAP SuccessFactors HCM suite production tenants that **have not** completed the upgrade to Identity Authentication, then those tenants **will not** be automatically upgraded and activated with Identity Authentication and Identity Provisioning.
- If you're an existing customer with **no** SAP SuccessFactors HCM suite production tenants available, then our automation process will create a **new** tenant for you and enable it with Identity Authentication and Identity Provisioning.

Related Information

Getting Started with Identity Authentication Already Enabled [page 28]
Initiating the Upgrade to Identity Authentication in SAP Cloud Identity Services [page 40]

10.2 Overview of the SAP SuccessFactors and Identity Authentication Service Integration (Video)

The process of migrating to the Identity Authentication service requires you to perform tasks in SAP SuccessFactors *Admin Center*, and in Identity Authentication and Identity Provisioning located within the SAP Cloud Identity Services administration console.

Identity Authentication Integration-The Overall Picture

Integrating SAP SuccessFactors with Identity Authentication involves the process described, at a high level, in the image. Select an image to find the topics associated with each task.

> → Tip
>
> If your company migrated to the Identity Authentication service, before April 24, 2020, you will need to make changes to your Identity Authentication Transformations. The changes that you need to make are described in detail in the guide linked below: **IPS Transformations Document**

- Initiating the Upgrade to Identity Authentication in SAP Cloud Identity Services [page 40]
- Configuring the Corporate Identity Provider in the Identity Authentication service (Video) [page 120]
- SAP Cloud Identity Services Administration Console Tasks [page 113]
- Identity Provisioning Service Administration Console Tasks [page 135]
- Testing and Activating the Upgrade to Identity Authentication [page 47]

Overview of the Identity Authentication Upgrade

Related Information

Step-by-Step Upgrade of SAP SuccessFactors to Identity Authentication (Video) [page 32]
Identity Provisioning Transformations Document

10.3 Step-by-Step Upgrade of SAP SuccessFactors to Identity Authentication (Video)

All SAP SuccessFactors systems can be set up to use Identity Authentication in SAP Cloud Identity Services.

The Identity Authentication service is a cloud solution for identity life-cycle management. It is used by SAP Cloud solutions like the SAP SuccessFactors HCM suite, as well as for SAP Business Technology Platform applications and on-premise applications. It provides services for authentication, single sign-on, and on-premising integration as well as self-services such as registration or password reset for employees, customer partners, and consumers.

You can use Identity Authentication services like SAML 2.0 single sign-on, username and password login, two-factor authentication, and other login options to control access yourSAP SuccessFactors system.

Step-by-Step Upgrade to Identity Authentication

Open this video in a new window

Related Information

Benefits of Using Identity Authentication in SAP Cloud Identity Services [page 12]
Guidance on Migrating to Identity Authentication in SAP Cloud Identity Services [page 8]
When to Use SAP SuccessFactors with Identity Authentication [page 4]
Important Notes About Using SAP SuccessFactors with Identity Authentication [page 5]
Getting Started with Identity Authentication and SAP SuccessFactors [page 33]

10.4 Getting Started with Identity Authentication and SAP SuccessFactors

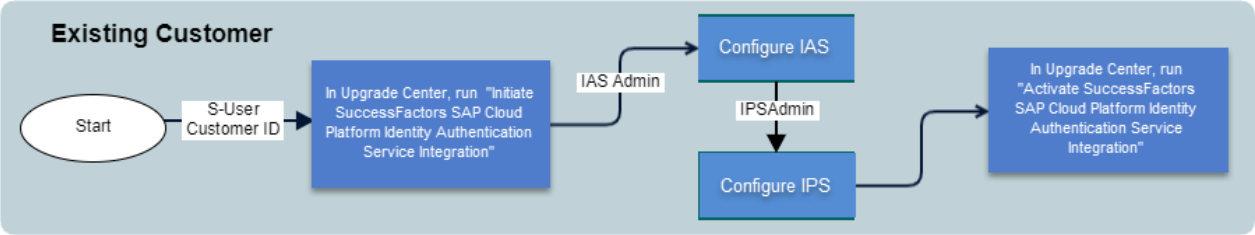
Learn about the overall process to set up your SAP SuccessFactors system and how to use Identity Authentication in SAP Cloud Identity Services.

> **Note**
>
> We are requesting for all systems to be migrated to Identity Authentication by June 2, 2025. For details about this migration, refer to **Guidance on Migration to Identity Authentication in SAP Cloud Identity Services** in the **Related Information** section.

> **Note**
>
> The below steps apply to SAP SuccessFactors HCM suite tenants created prior to December 9, 2022, If your tenant was created after this, it means you already have Identity Authentication enabled. Instead, go to **Getting Started with Identity Authentication Already Enabled** in the **Related Information** section for steps to log in and access Identity Authentication and Identity Provisioning.

> **Note**
>
> Identity Authentication is included natively in all partner paid demo tenants (i.e. Company ID starts with **SFCPART**) which is created from a template with “IAS” in the template description and version name. Selecting one of these templates automatically ensures that Identity Authentication is provisioned along with the demo tenant during the provisioning process, without the need to run any Identity Authentication process through the Upgrade Center. Additionally any Identity Authentication Initiate Upgrade or Change tasks, if available in the Upgrade Center, should not be run and is not supported by Technical Support.

Here is an overview of the process:



Understanding User Identity and Synchronization Before Migration

Identity Authentication uses the login name from SAP SuccessFactors as the user's unique identifier for authentication. This value is synchronized to Identity Authentication through Identity Provisioning and must remain consistent for a successful upgrade.

User synchronization is based on the user account record rather than employment level data. Identity Authentication reads identity attributes such as login name, locale, and account status from the user account record. Employment level values, such as job or position information, do not determine the identity used for login.

Identity Authentication also treats usernames as case insensitive. To ensure consistent login behavior and prevent authentication failures after the upgrade, turn on the *Enable Case-Insensitive Usernames* setting in *Admin Center* > *Company System and Logo Settings* before completing the upgrade.

For more information about how user attributes from SAP SuccessFactors map to Identity Authentication through SCIM, refer to **Mapping Between SCIM Users and OData User** in the Related Information section.

1. **Integrate SAP SuccessFactors with Identity Authentication.**
   - Initiate the process to upgrade your SAP SuccessFactors system using the *Upgrade Center*. You're notified by email when the connection is complete.
2. **Confirm that user sync is set up in Identity Provisioning in SAP Cloud Identity Services.**
   - Set up sync jobs with Identity Provisioning.
   - Ensure that the user that is configured in the Identity Provisioning service *Properties* tab (API User) has the necessary role-based permissions to export user data with OData API.

> ⚠ Caution
>
> You must sync **ALL** users to Identity Authentication service before you activate the service. User sync is critical when using the following services and features:
>
> - **Conditional Authentication:** To set up with rules that authenticate based on email, user type, or group.
> - **Story Reports, Internal Career Site, and other SAP SuccessFactors product areas:** User identifiers can change between product areas and Identity Authentication can only map these identifiers correctly when your users are in the Identity Authentication service.
> - **Global Assignment & Concurrent Employment:** when users log on from different sources, Identity Authentication service needs to convert their identifiers so that the Identity Authentication service understands them. That only happens when user sync has been done and the users are loaded into the Identity Authentication service.
> - **Enablement of Partial SSO:** If you intend to user partial sso, your users should exist in Identity Authentication service.
> - **Two-factor Authentication:** Your users need to exist in Identity Authentication service so that you can take advantage of two-factor security features.

> Do not manually create users in Identity Authentication, as all users must be synchronized from SAP SuccessFactors or other integrated systems to ensure accurate and consistent user management. Manual creation can result in synchronization issues, mismatched user data, and potential authentication failures.

3. **Review the default configurations.**
   Review the default configuration of the Identity Authentication service to determine if it meets your requirements or if additional configuration is required.
4. **Additional configuration optional features.**
   Configuration options in Identity Authentication include:
   - Password policy settings
   - Single sign-on (SSO)
   - Identity Authentication service user groups to configure multiple authentication methods
   - Conditional and risk-based authentication rules
   - Two-factor authentication
   - Email notification templates
   - Branding
5. **Turn on the Identity Authentication service.**
   - Enable Identity Authentication in the SAP SuccessFactors *Upgrade Center* after you're finished setting it up.

Related Information

Default Configuration of Identity Authentication with SAP SuccessFactors [page 50]
Process to Set Up Single Sign-On with Identity Authentication [page 119]
Initiating the Upgrade to Identity Authentication in SAP Cloud Identity Services [page 40]
Guidance on Migrating to Identity Authentication in SAP Cloud Identity Services [page 8]
Getting Started with Identity Authentication Already Enabled [page 28]
Mapping Between SCIM Users and ODATA User

10.4.1 Setting Up Authentication Between Identity Authentication and SAP SuccessFactors

10.4.1.1 Default Authentication Setup Between Identity Authentication and SAP SuccessFactors

By default, communication between Identity Authentication and SAP SuccessFactors uses X.509 certificate-based authentication (mTLS). This setup has been the standard since December 2022 and replaces the previous Basic Authentication method that relied on the IPSADMIN user.

The SCIM API (System for Cross-domain Identity Management) is used to automate user provisioning and lifecycle management, ensuring that user accounts in SAP SuccessFactors are securely and efficiently synchronized with Identity Authentication.

A system-created administrator entry appears in Identity Authentication to allow SAP SuccessFactors to retrieve corporate identity provider (IdP) information, which is displayed on the *Manage SAML SSO Settings* page in Admin Center.

> **Note**
>
> Basic Authentication for API communication is planned for deprecation. If your system is still using the IPSADMIN user for integration between SAP SuccessFactors and Identity Provisioning, migrate to X.509 certificate-based authentication before November 2026.

Related Information

Upgrade to X.509 Certificate-Based Authentication for Incoming Calls [page 36]
Default Configuration of Identity Authentication with SAP SuccessFactors [page 50]

10.4.1.2 Upgrade to X.509 Certificate-Based Authentication for Incoming Calls

X.509 certificate-based authentication is now supported in SAP SuccessFactors for incoming calls.

Prerequisites

You have the *Administrator Permissions* > *Manage Security Center* > *Access to X.509 Certificate Mapping* permission.

Context

Mutual Transport Layer Security (mTLS) establishes an encrypted TLS connection, in which both parties use X.509 certificates to authenticate and verify each other. mTLS prevents malicious third parties from imitating genuine applications, and provides a more secure authentication option to its users.

When an application attempts to establish a connection with another application's secure web server, the mTLS protocol protects their communications, and verifies that the incoming server truly belongs to the application being called. The application making the call can trust the identity of the application it's calling, because the Certificate Authority has created and issued an X.509 certificate to the application.

Your application's X.509 certificate can be uploaded to the Admin Center's *Security Center* for use in mTLS authentication.

> **Note**
>
> As of now, the *Security Center* supports the use cases for incoming calls to SAP SuccessFactors from **Identity Authentication**, **Identity Provisioning**, **Employee Central Payroll**, **Business Technology Platform**, **SAP Identity Management**, and **Business Data Cloud**.
>
> For information about your specific application's certificate (including how to obtain and set up notifications for expiring X.509 certificates), refer to the **Related Information** section.
>
> For Identity Authentication, certificate information is located in step 4 of **Configure Authentication Provider To Migrate User Passwords from SAP SuccessFactors Systems to Identity Authentication**. Make sure to check the *Automatic Renewal* checkbox option mentioned in this step to ensure that your certificate is regenerated automatically.
>
> Basic Authentication for API integrations is planned for deprecation. If your system still uses the **IPSADMIN** user for communication between SAP SuccessFactors and Identity Provisioning, migrate to X.509 certificate-based authentication before November 2026 to ensure uninterrupted integration.

Procedure

1. Go to *Admin Center* > *Security Center* > *X.509 Public Certificate Mapping*.
2. Click *Add*.
3. Complete the following fields:

Field	Description
Configuration Name	Example: New X.509 Certificate Mapping
Integration Name	Select the name of your application from the drop-down menu. The options available are: • Employee Central Payroll • Identity Authentication Service • Identity Provisioning Service • Business Technology Platform • SAP Identity Management • Business Data Cloud
Certificate File	Upload the corresponding file with a certificate file extension `cer, pem, crt` etc. and that follows the X.509 protocol.

Field	Description
Login Name	The login name of a user that has permission to consume the SAP SuccessFactors API for its respective application. **Note** If your *Integration Name* is Identity Authentication *Service* or Identity Provisioning *Service*, this field is optional, since a technical user is is already created in the background for these applications. The default technical user has the permissions required for standard SAP SuccessFactors–delivered data. Provide a different user only if your integration requires access to additional or customer-specific data (for example, extensions to standard entities such as EmpEmployment in Employee Central) or if your Business Technology Platform integration requires permissions beyond those of the default technical user.

4. Click *Save*.

Results

Going forward, your certificate is registered, and used for authentication.

Related Information

Configure Authentication Provider To Migrate Passwords from SAP SuccessFactors to Identity Authentication
Identity Provisioning - Generate and Manage Certificates for Outbound Connection
Business Technology Platform - Use Destination Certificates
X.509 Client Certificates-Employee Central Payroll

10.4.1.3 Manage Allowed IP Address Ranges for API Integration

To help ensure smooth API integration, tenants using Identity Authentication and Identity Provisioning should configure allowed IP address ranges so that API calls from these services are accepted by SAP SuccessFactors.

Context

Even if your system no longer uses the IPSADMIN user for API integration, setting up allowed IP ranges is still required for Identity Authentication and Identity Provisioning to communicate securely with your SAP SuccessFactors instance. Proper configuration helps maintain secure access and uninterrupted service.

Procedure

1. Log on to your SAP SuccessFactors system as an administrator.
2. Go to *Admin Center* > *Company Settings* > *Password & Login Policy Settings* > *API Login Exceptions*.
3. Select *Add*.
4. Enter your username if required (the **`IPSADMIN`** user is no longer needed for new configurations).
5. Set *Maximum Password Age* in days to **`-1`** (only if you are still using IPSADMIN).

   > ⚠ Caution
   >
   > For IPSADMIN: The password for this user should NOT expire until you migrate to X.509 certificate-based authentication.

6. Enter the IP address ranges for Identity Provisioning into the *IP Address Restrictions* field. Refer to **Regional Availability (Identity Provisioning)** in the **Related Information** section for these ranges.
7. Enter the IP address ranges for Identity Authentication into the *IP Address Restrictions* field. Refer to **Regional Availability (Identity Authentication)** in the **Related Information** section for these ranges.
8. Save your changes.

Results

The configured IP ranges allow Identity Authentication and Identity Provisioning API calls to be accepted by SAP SuccessFactors, ensuring secure communication and proper integration.

Related Information

Regional Availability (Identity Authentication)

Regional Availability (Identity Provisioning)

What Are Role-Based Permissions

Authenticating New Hires with Identity Authentication in SAP Cloud Identity Services [page 82]

Manage Real-Time Sync of Users from SAP SuccessFactors to Identity Authentication with Identity Provisioning [page 84]

Regions and Hosts Available for the Neo Environment

10.4.2 Initiating the Upgrade to Identity Authentication in SAP Cloud Identity Services

Initiate integration of your organization's SAP SuccessFactors system with the Identity Authentication service so that you can use it for identity management.

Prerequisites

> ⓘ Note
>
> If your SAP SuccessFactors tenant was created after December 9, 2022, Identity Authentication and Identity Provisioning **have already** been enabled and are using Mutual Transport Layer Security (mTLS) in conjunction with the System for Cross-domain Identity Management (SCIM) API, which are the latest methods of authentication and integration with Identity Authentication and Identity Provisioning. You **do not** need to complete the below steps to upgrade to Identity Authentication.
>
> This enablement also provides you the option to authenticate both your Employees and New Hires with Identity Authentication because of the SCIM integration provided (refer to **Authenticating New Hires with Identity Authentication in SAP Cloud Identity Services** in the **Related Information** section).

> ⓘ Note
>
> If you perform the below steps to initiate the upgrade to Identity Authentication after December 9, 2022, Identity Authentication and Identity Provisioning **will already** be configured to use Mutual Transport Layer Security (mTLS) in conjunction with the System for Cross-domain Identity Management (SCIM) API, which are the latest methods of authentication and integration with Identity Authentication and Identity Provisioning.

> ⓘ Note
>
> Identity Authentication is included natively in all partner paid demo tenants (i.e. Company ID starts with **SFCPART**) which is created from a template with "IAS" in the template description and version name. Selecting one of these templates automatically ensures that Identity Authentication is provisioned along with the demo tenant during the provisioning process, without the need to run any Identity Authentication process through the Upgrade Center. Additionally any Identity Authentication Initiate Upgrade or Change tasks, if available in the Upgrade Center, should not be run and is not supported by Technical Support.

- You have the SAP *S-User* user name and password.

- You want to be set up as an administrator of your organization's first Identity Authentication tenant in SAP Cloud Identity Services **or** you can gather the required information from the current administrators of your organization's existing Identity Authentication service tenant.
- You have access to theSAP SuccessFactors *Upgrade Center.*

Context

> ⚠ Caution
>
> Completing this task initiates the Identity Authentication service upgrade process, after configuring your authentication methods as described in this guide, you must then activate the Identity Authentication service to complete the migration.

This is a video overview of the steps to initiate the upgrade to the Identity Authentication service.

Procedure

1. Go to *Admin Center* > *Upgrade Center* > *Optional Upgrades*.

   > ⓘ Note
   >
   > The Upgrade Center can be searched for, but is also available in the *Release Center* tile under *See More*.

2. Find the upgrade *Initiate the* SAP Cloud Identity Services Identity Authentication Service *Integration* and click *Learn More & Upgrade Now*.
3. Click *Upgrade Now.*
4. Enter your *S-User* and password in the dialog and click *Validate*.

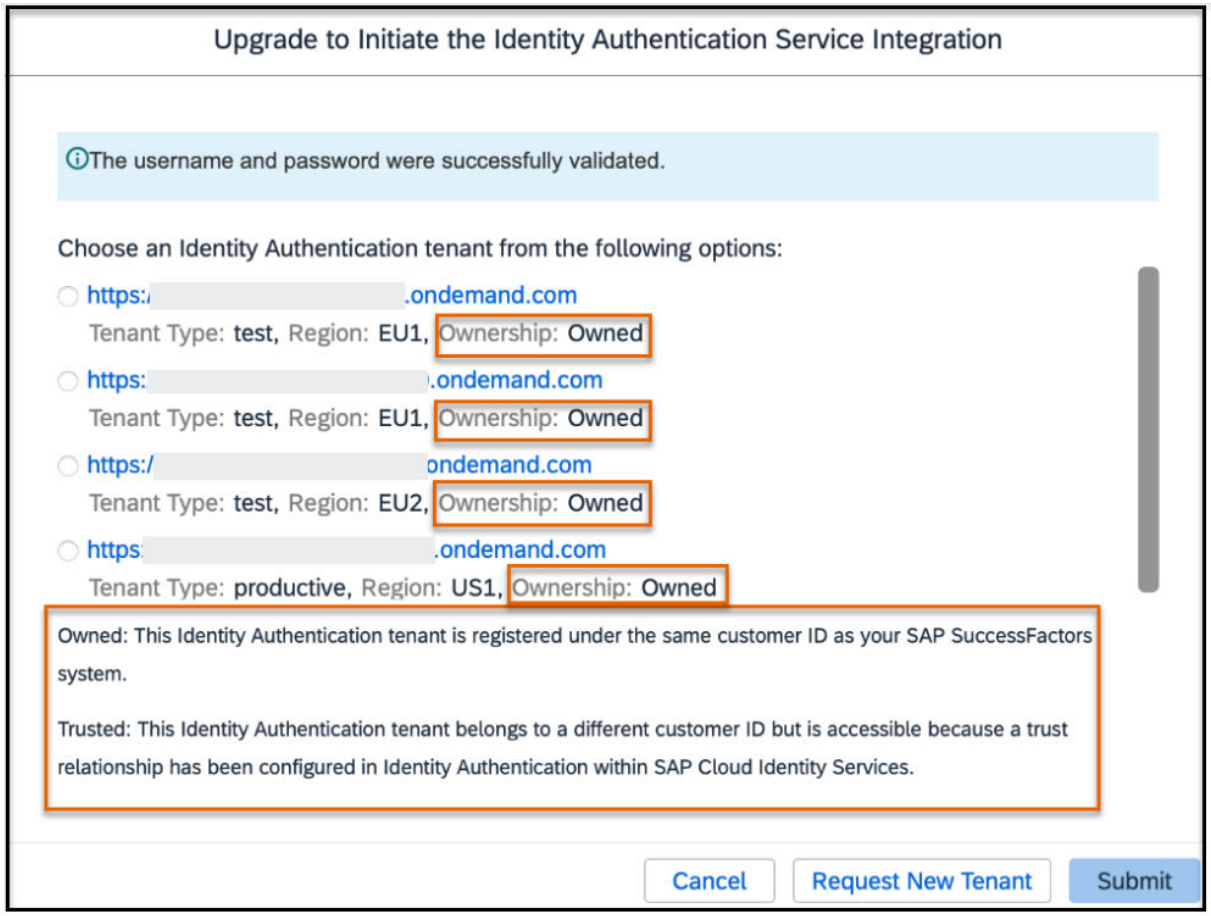
   We match the information you entered against our records to make sure it's correct. If you enter invalid credentials or you aren't part of the organization who owns the system you're working in, you can't proceed.

   > ⓘ Note
   >
   > If you encounter validation errors when logging in, refer to Identity Authentication Upgrade Error when Validating S-User Credentials: 2944990

5. Select a tenant from your list of displayed tenants or select *Request New Tenant* to the Identity Authentication service.

   The list now includes an *Ownership* field showing whether a tenant is:

   - *Owned*: registered under your organization's customer ID, or
   - *Trusted*: belongs to a different customer ID but is accessible because a trust relationship has been configured in Identity Authentication within SAP Cloud Identity Services.



This helps you identify the appropriate tenant for integration. For more information about how multiple customer IDs can reuse the same Identity Authentication tenant, see Reuse SAP Cloud Identity Services Tenants for Different Customer IDs.

If you're a Partner-Managed Cloud (PMC) customer, you can only request a new tenant.

> ⚠ Caution
>
> If your company is already using a productive tenant for Identity Authentication, we strongly recommend that you reuse it and migrate with that productive SAP SuccessFactors tenant. Using one Identity Authentication tenant for your SAP cloud applications is important for other integration scenarios between these applications. Starting with this simplified configuration can help to avoid the need to migrate the integrations and to redesign the landscape. If your company has a specific requirement (functional or legal) where existing Identity Authentication usage or users should not be mixed with the usage and users of SAP SuccessFactors, you can proceed to request an additional Identity Authentication tenant dedicated to SAP SuccessFactors.
>
> We do not recommend using the same Identity Authentication service tenant for multiple SAP SuccessFactors tenants, as the Identity Authentication service will not be able to identify if multiple SAP SuccessFactors tenants have the same login name of some users.
>
> We recommend, for test environments, that you have at least one Identity Authentication tenant that is shared with various SAP cloud applications so that you can test a production-like scenario. If you have additional SAP SuccessFactors test instances that cannot be mapped to a test tenant with multiple

applications, then you can request a dedicated Identity Authentication tenant for these instances so that they're managed separately.

> **Note**
>
> The tenants available for upgrade are listed according to the tenants in your region. If the tenant that you want to upgrade is located in a different region or you don't see the tenant that you want to upgrade, please contact your implementation partner or Account Executive so that they can enable the *Ignore region and type restrictions for Identity Authentication Service integration (Warning: This feature should be turned on only when an existing* Identity Authentication *tenant needs to be integrated).* setting.

> **Caution**
>
> Although this option is available, we recommend you retain the default settings, which limit the use of Identity Authentication to the appropriate region and corresponding tenant type of the SAP SuccessFactors tenant (for example, ensuring that production Identity Authentication tenants are used for production SAP SuccessFactors tenants, and test/preview Identity Authentication tenants are used for test/preview SAP SuccessFactors tenants). Only select the *Ignore region and type restrictions for Identity Authentication Service integration (Warning: This feature should be turned on only when an existing* Identity Authentication *tenant needs to be integrated).* setting when your company absolutely needs this configuration enabled, and you have evaluated and validated all the impacts and consequences.

6. Click *Yes* to confirm the upgrade and begin the integration process.

Results

The integration process runs in the background and can take up to 24 hours to complete. After the upgrade process completes, an email is sent with tenant details. You can monitor the progress of your upgrade using the Identity Authentication monitoring tool.

> **Note**
>
> The monitoring tool can be found by searching for **Monitoring Tool** in the *Tools* tile, or by using the Admin Center search bar.

If your organization did not have an Identity Authentication service tenant, we create one during the upgrade process and you're added as its administrator, based on your *S-User* information. You receive an e-mail notification to register your new account.

If you provided the URL of an existing Identity Authentication service tenant, the SAP SuccessFactors system you're working in is added to the Applications section of the Identity Authentication service tenant. You aren't added as a new administrator. Current administrators can go there to complete the configuration.

> **Note**
>
> The Identity Authentication service is **not** enabled and used by your system yet. You still have to configure it and then turn it on when you're ready.

Next Steps

After you receive notification that the process completed successfully, review default configuration settings in the Identity Authentication service tenant and confirm that the user sync is functioning properly.

If the upgrade fails for some reason, use the *Undo* option in *Upgrade Center*, within 30 days, to rerun the upgrade after you've resolved the cause of the failure. If you're not sure why the upgrade failed or how to fix it, contact SAP Cloud Support.

> ⓘ Note
>
> The *Undo* option in *Upgrade Center* only allows you rerun a failed upgrade. It can't undo a successful integration.

Related Information

Default Configuration of Identity Authentication with SAP SuccessFactors [page 50]
Process to Set Up Single Sign-On with Identity Authentication [page 119]
Opening the Identity Authentication Administration Console in SAP Cloud Identity Services [page 168]
Authenticating New Hires with Identity Authentication in SAP Cloud Identity Services [page 82]

10.4.2.1 Monitoring Tool for the Upgrade to Identity Authentication

When you initiate your upgrade to the Identity Authentication service, and while the upgrade is processing, you can track the status of your upgrade using the Monitoring Tool.

Upon initiating the upgrade, you're given a link to access the Monitoring Tool, but you can also access it by searching for **Monitoring Tool** in the *Admin Center* > *Tools* tile, or by using the Admin Center search bar.

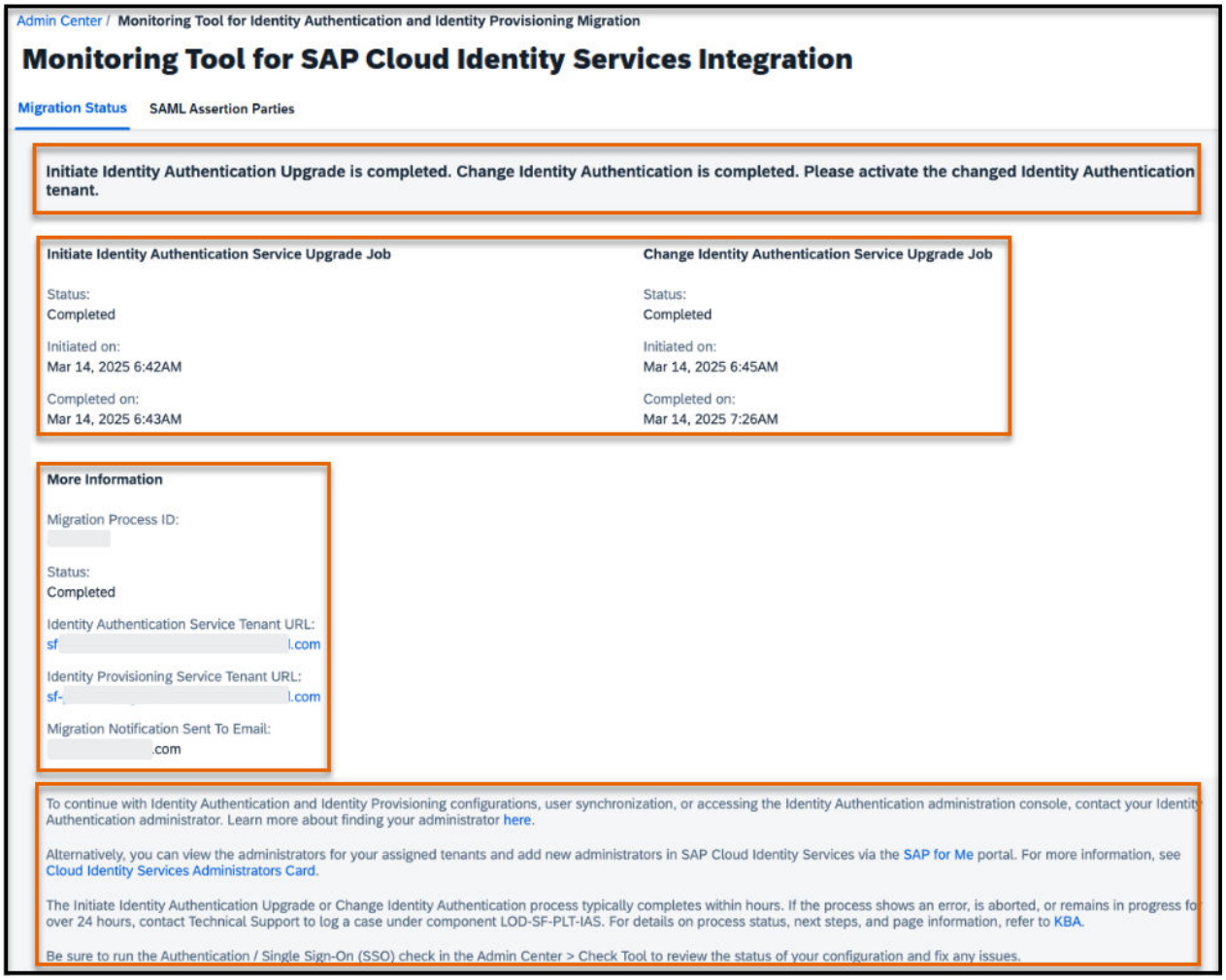
Under the *Migration Status* tab of the tool, you can:

- View the overall status of your Initiate and Change upgrades, and see which upgrades are complete or still need to be activated.
- See detailed information for each upgrade, including the date the upgrade was initiated and completed.
- Access the Migration Process ID, along with URLs for your Identity Authentication and Identity Provisioning tenants.
- View the email address of the user who received the migration notification or, when no user is available, a message indicating that an Identity Authentication administrator account was created with a link to set up the account.

  > ⓘ Note
  >
  > The *Migration Process ID*, *Identity Authentication Service Tenant URL*, *Identity Provisioning Service Tenant URL*, and *Migration Notification Sent to Email* are only displayed when the Initiate Identity Authentication Service Upgrade or Change Identity Authentication Service job is initiated from Upgrade Center and

completes successfully. If Identity Authentication is integrated manually or changes are made using Provisioning, this information might not be available in the Monitoring Tool.

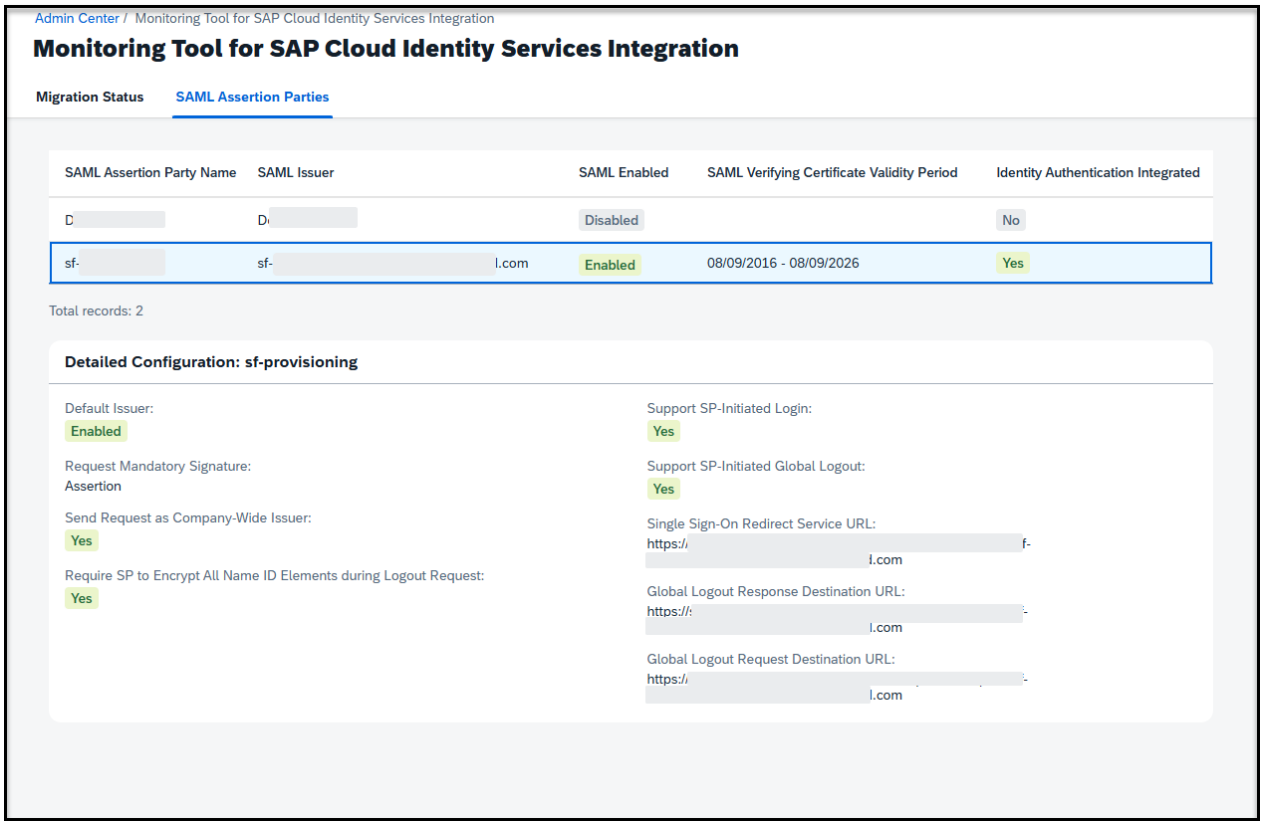
- Review additional guidance, such as how to contact administrators, access the Identity Authentication admin console, and view related resources.



SAML Assertion Parties

All relevant SAML assertion party information is now displayed in the tool. Administrators can view key details for each SAML assertion party, including the assertion party name, SAML issuer, and the SAML enabled flag. All displayed values come from Provisioning and are read-only.

Additional attributes are shown in the *Detailed Configuration* section when a row is highlighted. This section includes optional configuration details such as request signatures, single sign-on URLs, and other integration-specific information.



→ Tip

If you are reusing an Identity Authentication tenant, ensure that you have access to the admin user credentials.

→ Remember

- The Monitoring Tool will display the status and URL for the initial upgrade process, and will do the same for the Identity Authentication change upgrade process, if it has been completed.
- Even if the initial upgrade process has succeeded, if the change upgrade process is run later and fails,the Monitoring Tool will display the error for the failure on this same screen.
- It might not be able to display the execution details of upgrade processes completed a year or more ago.

ⓘ Note

- If an error occurs during the upgrade, take note of the *Migration Process ID* so that Technical Support can identify your issue.
- The Monitoring Tool only monitors the integration between SAP SuccessFactors and Identity Authentication, and does not monitor the SAP Analytics Cloud (SAC) or Learning Management Systems (LMS) integration process.
- If your Identity Authentication service was configured manually, or upgraded before the Monitoring Tool was implemented, the time stamp will not display and the **More Information** section will be empty.
- You can navigate to *Admin Center* > *Tools* > *SAML 2.0 Single Sign On* > *Advanced Settings* to be redirected to the Identity Authentication console in SAP Cloud Identity Services and go to *Tenant Settings* to get the information and configurations for your connected tenant.

- To view all of your tenants in one place, see **View All of Your Identity Authentication and Identity Provisioning Tentants** in the **Related Information** section.

Related Information

View All of Your Identity Authentication and Identity Provisioning Tenants

10.4.3 Testing and Activating the Upgrade to Identity Authentication

Test your Identity Authentication service configuration before activating your migration.

Prerequisites

- You've initiated your Identity Authentication service migration in the *Upgrade Center*.
- You've set up your authentication configurations in the Identity Authentication in SAP Cloud Identity Services.
- You've set up your source and target configurations in the Identity Provisioning in SAP Cloud Identity Services.
- You have the corporate identity provider log on information.

> **Note**
>
> - If you're using a third-party provider, ensure that you have the credentials to log on to the corporate IdP.
> - If the Identity Authentication service is your corporate IdP, ensure that you have the login credentials for your Identity Authentication user.

Context

This is a video overview of the steps to test your migration before activating the Identity Authentication service.

> **Restriction**
>
> After you've upgraded to the Identity Authentication service, you will not have the ability to turn on partial SSO in SAP SuccessFactors company Provisioning. By default, partial SSO is disabled after activating Identity Authentication. If needed, you can set up partial SSO in Identity Authentication.
>
> After you've upgraded to the Identity Authentication service, you will not have the ability to enable multiple SAML asserting parties in SAP SuccessFactors company Provisioning. By default, Identity Authentication will be enabled as the single SAML asserting party in the SAP SuccessFactors provisioning setting after

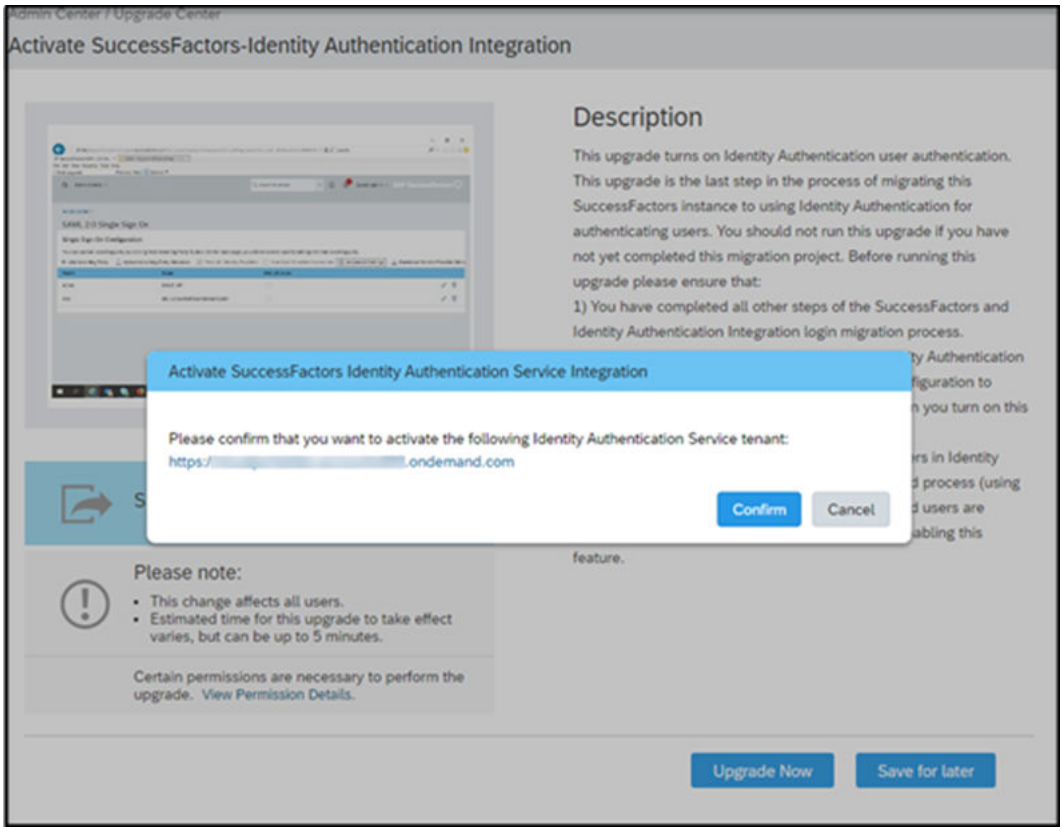
activating Identity Authentication. If you need multiple asserting parties, you can accomplish this by setting up conditional authentication.

→ Remember

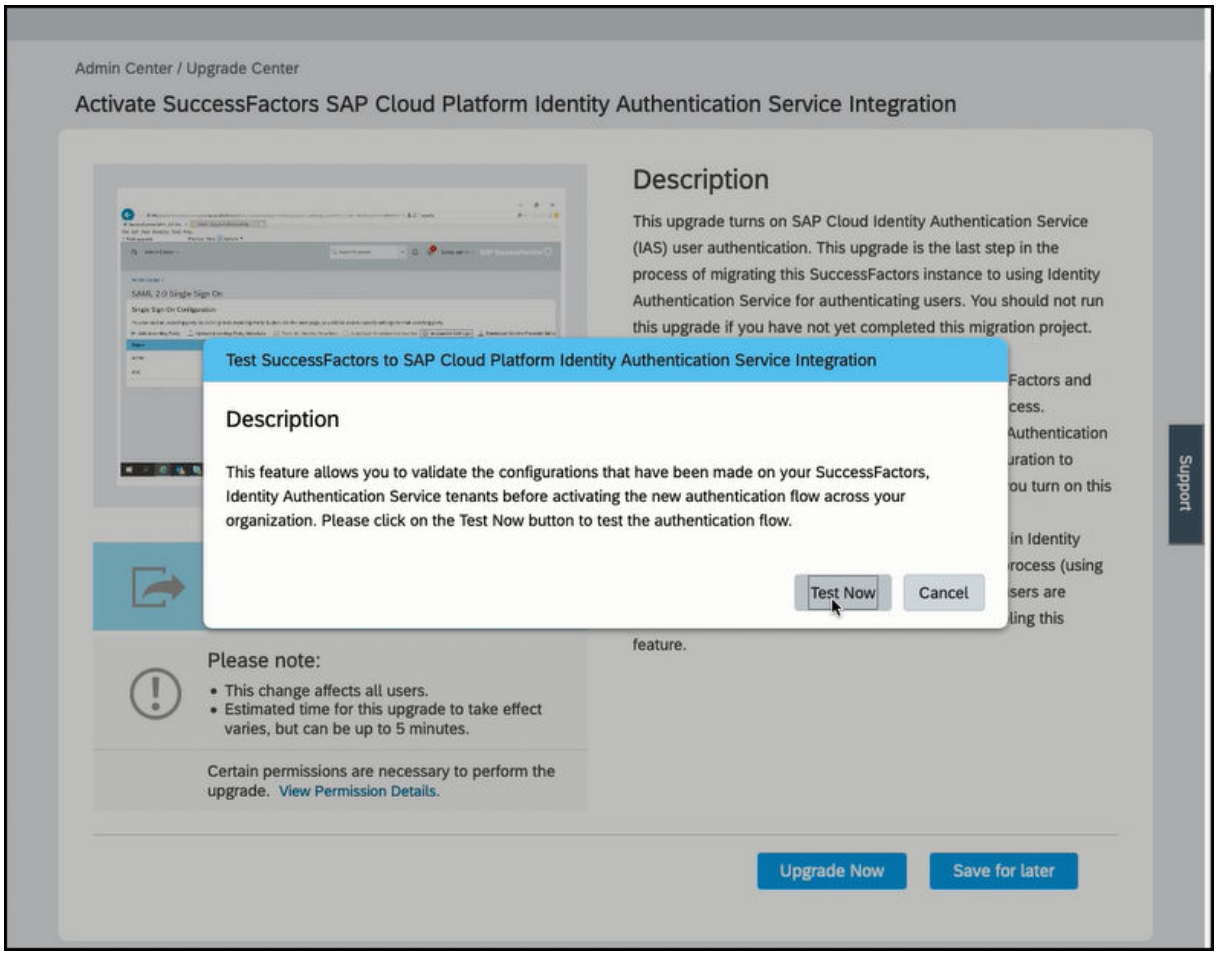
As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Technical Support.

Procedure

1. Log on to your SAP SuccessFactors system as an admin.
2. Go to *Admin Center* > *Upgrade Center* > *Optional Upgrades*.
3. Find the upgrade *Activate SuccessFactors* Identity Authentication Service *Integration* and choose *Learn More & Upgrade Now*.
4. Click *Upgrade Now* on the *Activate SuccessFactors* Identity Authentication Service *Integration*.
5. Click *Confirm* on the *Activate SuccessFactors* Identity Authentication Service *Integration* pop up.



6. Click *Test Now* on the *Test SuccessFactors to* Identity Authentication Service *Integration* pop up, to test your migration.



After clicking *Test Now* a new tab opens to your corporate identity provider's log on screen.

7. Log on to your corporate identity provider based on your corporate IdP scenario.
    - If Identity Authentication is your corporate IdP, log on to Identity Authentication using any user's credentials. For a successful test, this user must exist in both Identity Authentication and SAP SuccessFactors.
    - If Identity Authentication is being used as a proxy to your corporate IdP, log on to your corporate IdP using your corporate IdP credentials. For a successful test, this user must exist in both Identity Authentication and SAP SuccessFactors.
8. Click *Yes* to activate Identity Authentication.

    If you're using Onboarding to activate employees, refer to the following topic: **Activating an Account and Setting a New Password After Identity Authentication is Enabled.**

Related Information

SAP Note 2954556

Activating an Account and Setting New Password After Identity Authentication Is Enabled

Configure the Corporate Identity Provider

10.4.4 First Time Login Experience for Migrated Users

After Identity Authentication is activated and user credentials are migrated, users experience one of two possible login flows, depending on their previous authentication method.

Users Previously Using SSO via a Corporate Identity Provider

If users were already signing in through your corporate identity provider (IdP) using single sign-on (SSO), their login experience doesn't change. After migration, Identity Authentication acts as a proxy IdP, forwarding authentication requests to your corporate IdP and completing the sign-in with SAP SuccessFactors.

Users Previously Using SAP SuccessFactors Username and Password

If users previously signed in with their SAP SuccessFactors username and password, they'll now use the Identity Authentication login page instead of the SAP SuccessFactors one. During their first login after migration, they enter the same credentials as before. Identity Authentication validates those credentials with SAP SuccessFactors, migrates them, and then manages all future logins. If a password doesn't meet the policy defined in Identity Authentication, the user is prompted to change it before continuing.

After the first successful login, all password changes and resets are handled directly in Identity Authentication.

10.4.5 Default Configuration of Identity Authentication with SAP SuccessFactors

When you upgrade to the Identity Authentication service, your users are configured to authenticate using passwords by default. You can customize these configurations for the needs or your organization.

The Identity Authentication service is the Identity Provider and performs the user authentication method you configure for your system, session management, and single sign-on for your integrated applications. This integrated process requires the synchronization of users from the SAP SuccessFactors instance to the Identity Authentication service.

Username Case-Insensitivity Behavior

Identity Authentication treats usernames as case-insensitive. This means that variations in letter casing (for example, john.doe, JOHN.DOE, or John.Doe) are treated as the same username during login and identity checks. Many corporate identity providers, such as Microsoft Entra ID, follow the same behavior.

To ensure consistent username handling between Identity Authentication, corporate identity providers, and SAP SuccessFactors, we recommend turning on the *Enable Case-Insensitive Usernames* setting in *Admin Center* > *Company System and Logo Settings*. If this setting is not enabled, users may experience login failures after Identity Authentication is activated, because the username sent by the identity provider must match the exact case stored in SAP SuccessFactors.

User Provisioning Behavior

When a new user is created in SAP SuccessFactors, they're provisioned in Identity Authentication and the provisioned user receives an activation email that they can use to set the password that they can use access their SAP SuccessFactors application.

→ Tip

Successfully syncing your users to Identity Authentication requires that the SAP SuccessFactors users MUST contain the following attributes:

- Last Name
- Unique Username
- Unique Email

These attributes are required in Identity Authentication. If you cannot ensure that all users have a unique email address, you may need to generate "dummy" emails for them.

⚠ Caution

The *sf.user.filter* in Identity Provisioning under the tabs *Source Systems* > *Properties*, contains place holder values called *'sf_username1_placeholder','sf_username2_placeholder'*. Replacing these place holders with a few users can help you to test user provisioning before performing the sync job that pulls in all of your SAP SuccessFactors users into Identity Authentication. Test your selected users by substituting the place holders with usernames from your SAP SuccessFactors system. After testing and ensuring that user provisioning is working correctly, remove the placeholder users and replace them with the value **`Active`**. This syncs all the active users in your system.

Identity Authentication is configured as follows:

- Password-based logins only
- Standard password policy
- Authentication rules configured to send all users to password-based logon
- No user groups configured
- No other corporate identity provider (IdP) configured, as Identity Authentication is the identity provider that handles single sign-on for SAP SuccessFactors.
- For newly provisioned Identity Authentication tenants created after February 2026, multifactor authentication (MFA) is automatically enabled for administrator access to the Identity Authentication administration console. The first time an administrator signs in, they are prompted to set up MFA by using either a mobile authenticator app (recommended) or a supported web or device authenticator. Administrators can defer this setup for up to 14 days. After 14 days, MFA setup is required to continue accessing the administration console. For more information, refer to Cloud Identity Services—Multi-Factor Authentication

Default Configuration for Identity Provisioning

Your Identity Provisioning system has the following default configurations:

- **Certificate-based authentication**: Mutual Transport Layer Security (mTLS) establishes an encrypted TLS connection, in which both parties use X.509 certificates to authenticate and verify each other. mTLS prevents malicious third parties from imitating genuine applications, and provides a more secure authentication option to its users.
- **Workforce SCIM API**: The System for Cross-domain Identity Management (SCIM) API is a preferred method to make user data more secure and simplify the user experience by automating the user identity lifecycle management process.

In *SAP Cloud Identity Services* > *Identity Provisioning* > *Source Systems* > *Your Source System* > *Properties* tab, this API is set by default by having the *sf.api.version = 2*.

- **sf.user.filter**: Also under the *Properties* tab, use this property to filter users from SAP SuccessFactors. This value is set by default to *sf.user.filter=active eq "true" and userName eq "sf_username_placeholder"*.
- **Transformations**: Located under the *Transformations* tab of your Source and Target systems.

Identity Provisioning's Default Transformations

The below transformations are provided by default by Identity Provisioning for the **OData API**, **Workforce SCIM API**, **Identity Authentication SCIM API Version 1**, and **Identity Authentication SCIM API Version 2**:

> → Tip
>
> The attribute mapping required for SAP Analytics Cloud (SAC) integration is included by default in the Identity Provisioning transformations for SAP SuccessFactors and Identity Authentication. You don't need to add or maintain any custom mappings for SAC.

Default Transformation for SAP SuccessFactors as the Source System - OData API:.

> {·} Code Syntax

```
// The value of entityIdSourceSystem is used for storing the unique ID of each
user.
       // You can change the default source attribute perPersonUuiD, but make
sure the new source attribute is also unique.
{
  "user": {
    "mappings": [
      {
        "sourcePath": "$.personKeyNav.perPersonUuid",
        "targetPath": "$.id",
        "targetVariable": "entityIdSourceSystem"
      },
      {
        "constant": false,
        "targetPath": "$.active"
      },
      {
        "condition": "$.personKeyNav.userAccountNav.accountStatus =='ACTIVE'",
        "constant": true,
        "targetPath": "$.active"
      },
      {
        "sourcePath": "$.personKeyNav.userAccountNav.username",
        "targetPath": "$.userName"
      },
      {
        "constant": "employee",
        "targetPath": "$.userType"
      },
      {
        "sourcePath": "$.firstName",
        "optional": true,
        "targetPath": "$.name.givenName"
      },
      {
        "sourcePath": "$.lastName",
        "targetPath": "$.name.familyName"
      },
// The email attribute is used as a first value for the emails array of the
intermediate JSON data.
      {
```

```
        "sourcePath": "$.email",
        "targetPath": "$.emails[0].value"
      },
      {
        "constant": "urn:ietf:params:scim:schemas:core:2.0:User",
        "targetPath": "$.schemas[0]"
      },
      {
        "constant": "urn:sap:cloud:scim:schemas:extension:sfsf:2.0:User",
        "targetPath": "$.schemas[1]"
      },
      {
        "constant": "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
        "targetPath": "$.schemas[2]"
      },
      {
        "sourcePath": "$.personKeyNav.perPersonUuid",
        "targetPath": "$['urn:sap:cloud:scim:schemas:extension:sfsf:2.0:User']
['personGUID']"
      },
      {
        "sourcePath": "$.userId",
        "targetPath": "$['urn:sap:cloud:scim:schemas:extension:sfsf:2.0:User']
['userSysID']"
      },
      {
        "sourcePath": "$.personKeyNav.personIdExternal",
        "optional": true,
        "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['employeeNumber']"
      }
    ]
  },
// By default, the group mapping is inactive (ignored) but groups are supported.
// To start provisioning groups, either delete the statement "ignore": true, or
set its value to false.
  "group": {
    "ignore": true,
    "mappings": [
      {
        "sourcePath": "$.groupID",
        "targetVariable": "entityIdSourceSystem"
      },
      {
        "sourcePath": "$.groupName",
        "targetPath": "$.displayName"
      },
      {
        "constant": "urn:ietf:params:scim:schemas:core:2.0:Group",
        "targetPath": "$.schemas[0]"
      },
      {
        "sourcePath": "$.users[*].personGUID",
        "preserveArrayWithSingleElement": true,
        "optional": true,
        "targetPath": "$.members[?(@.value)]"
      }
    ]
  }
}
```

Default Transformation for SAP SuccessFactors as the Source System - Workforce SCIM API:

Code Syntax

```
{
```

```
    "user": {
        "mappings": [
            {
                "sourcePath": "$.schemas",
                "targetPath": "$.schemas",
                "preserveArrayWithSingleElement": true
            },
            {
                "sourcePath": "$.id",
                "targetVariable": "entityIdSourceSystem"
            },
            {
                "sourcePath": "$.userName",
                "targetPath": "$.userName",
                "correlationAttribute": true
            },
            {
                "sourcePath": "$.active",
                "targetPath": "$.active"
            },
            {
                "sourcePath": "$.userType",
                "targetPath": "$.userType"
            },
            {
                "sourcePath": "$.name.familyName",
                "targetPath": "$.name.familyName",
                "optional": true
            },
            {
                "sourcePath": "$.name.givenName",
                "targetPath": "$.name.givenName",
                "optional": true
            },
            {
                "sourcePath": "$.name.middleName",
                "targetPath": "$.name.middleName",
                "optional": true
            },
            {
                "sourcePath": "$.name.honorificPrefix",
                "targetPath": "$.name.honorificPrefix",
                "optional": true
            },
            {
                "sourcePath": "$.name.honorificSuffix",
                "targetPath": "$.name.honorificSuffix",
                "optional": true
            },
            {
                "sourcePath": "$.name.formatted",
                "targetPath": "$.name.formatted",
                "optional": true
            },
            {
                "sourcePath": "$.nickName",
                "targetPath": "$.nickName",
                "optional": true
            },
            {
                "sourcePath": "$.title",
                "targetPath": "$.title",
                "optional": true
            },
            {
                "sourcePath": "$.displayName",
                "targetPath": "$.displayName",
                "optional": true
```

```
            },
            {
                "sourcePath": "$.emails",
                "targetPath": "$.emails",
                "optional": true,
                "preserveArrayWithSingleElement": true
            },
            {
                "sourcePath": "$.emails[?(@.primary== true)].value",
                "optional": true,
                "correlationAttribute": true
            },
            {
                "sourcePath": "$.phoneNumbers",
                "targetPath": "$.phoneNumbers",
                "optional": true,
                "preserveArrayWithSingleElement": true
            },
            {
                "sourcePath": "$.preferredLanguage",
                "targetPath": "$.preferredLanguage",
                "optional": true
            },
            {
                "sourcePath": "$.locale",
                "targetPath": "$.locale",
                "optional": true
            },
            {
                "sourcePath": "$.timezone",
                "targetPath": "$.timezone",
                "optional": true
            },
            {
                "sourcePath": "$.externalId",
                "targetPath": "$.externalId",
                "optional": true
            },
            {
                "sourcePath": "$.groups",
                "targetPath": "$.groups",
                "optional": true,
                "preserveArrayWithSingleElement": true
            },
            {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['employeeNumber']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['employeeNumber']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['department']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['department']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['division']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['division']",
                "optional": true
            },
            {
```

```
"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",
                "optional": true
            },
            {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['displayName']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['displayName']",
                "optional": true
            },
            {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['$ref']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['$ref']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['userUuid']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['userUuid']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['groupDomains']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['groupDomains']",
                "optional": true,
                "preserveArrayWithSingleElement": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['perPersonUuid']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['perPersonUuid']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['personIdExternal']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['personIdExternal']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['loginMethod']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['loginMethod']",
                "optional": true
            },
```

```
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']['isDraft']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']['isDraft']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['customFields']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['customFields']",
                "optional": true
            },
            {
                "targetPath": "$
['urn:sap:cloud:scim:schemas:extension:sap.ips.sfsf.sac:2.0:User']
['hasEmbeddedAnalyticsPermission']",
                "constant": false
            },
            {
                "targetPath": "$
['urn:sap:cloud:scim:schemas:extension:sap.ips.sfsf.sac:2.0:User']
['hasEmbeddedAnalyticsPermission']",

"condition": "$['urn:ietf:params:scim:schemas:extension:sap:2.0:User']
['groupDomains'][?(@.value == 'embeddedAnalyticsAccessPermission')] empty false",
                "constant": true
            }
        ]
    },
    "group": {
        "ignore": true,
        "mappings": [
            {
                "sourcePath": "$.id",
                "targetPath": "$.id",
                "targetVariable": "entityIdSourceSystem"
            },
            {
                "sourcePath": "$.schemas",
                "targetPath": "$.schemas"
            },
            {
                "sourcePath": "$.displayName",
                "targetPath": "$.displayName"
            },
            {
                "sourcePath": "$.members",
                "targetPath": "$.members",
                "optional": true,
                "preserveArrayWithSingleElement": true
            }
        ]
    }
}
```

Default Transformation for Identity Authentication as the Target System - Identity Authentication SCIM API Version 1:

Code Syntax

```
{
  "user": {
```

```
    "condition": "($.emails.length() > 0) && ($.name.familyName EMPTY false) &&
isValidEmail($.emails[0].value)",
    "mappings": [
      {
        "sourcePath": "$.groups",
        "preserveArrayWithSingleElement": true,
        "optional": true,
        "targetPath": "$.corporateGroups"
      },
      {
        "sourceVariable": "entityIdTargetSystem",
        "targetPath": "$.id"
      },
      {
        "constant": "urn:ietf:params:scim:schemas:core:2.0:User",
        "targetPath": "$.schemas[0]"
      },
      {
        "constant": "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
        "targetPath": "$.schemas[1]"
      },
      {
        "sourcePath": "$.userName",
        "targetPath": "$.userName",
        "optional": true
      },
      {
        "sourcePath": "$.emails[*].value",
        "preserveArrayWithSingleElement": true,
        "targetPath": "$.emails[?(@.value)]"
      },
      {
        "sourcePath": "$.userType",
        "targetPath": "$.userType",
        "optional": true
      },
      {
        "sourcePath": "$.name.givenName",
        "targetPath": "$.name.givenName",
        "optional": true
      },
      {
        "sourcePath": "$.name.middleName",
        "targetPath": "$.name.middleName",
        "optional": true
      },
      {
        "sourcePath": "$.name.familyName",
        "targetPath": "$.name.familyName",
        "optional": true
      },
      {
        "sourcePath": "$.name.honorificPrefix",
        "targetPath": "$.name.honorificPrefix",
        "optional": true
      },
      {
        "sourcePath": "$.addresses",
        "targetPath": "$.addresses",
        "preserveArrayWithSingleElement": true,
        "defaultValue": [],
        "optional": true,
        "functions": [
          {
            "function": "putIfAbsent",
            "key": "type",
            "defaultValue": "work"
          },
```

```
            {
              "condition": "(@.type NIN ['work', 'home'])",
              "function": "putIfPresent",
              "key": "type",
              "defaultValue": "work"
            }
          ]
        },
        {
          "sourcePath": "$.locale",
          "targetPath": "$.locale",
          "optional": true
        },
        {
          "sourcePath": "$.phoneNumbers",
          "targetPath": "$.phoneNumbers",
          "preserveArrayWithSingleElement": true,
          "optional": true
        },
        {
          "sourcePath": "$.displayName",
          "targetPath": "$.displayName",
          "optional": true
        },
        {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['employeeNumber']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['employeeNumber']",
          "optional" : true
        },
        {
          "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['costCenter']",
          "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['costCenter']",
          "optional" : true
        },
        {
          "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['organization']",
          "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['organization']",
          "optional" : true
        },
        {
          "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['division']",
          "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['division']",
          "optional" : true
        },
        {
          "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['department']",
          "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['department']",
          "optional" : true
        },
        {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",
```

```
        "optional" : true,
        "functions": [
            {
                "function": "resolveEntityIds"
            }
        ]
      },
      {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['displayName']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['displayName']",
        "optional" : true
      },
      {
        "sourcePath": "$.active",
        "targetPath": "$.active",
        "defaultValue": true,
        "optional": true
      },
      {
        "constant": "false",
        "targetPath": "$.sendMail",
        "scope": "createEntity"
      },
      {
        "constant": "true",
        "targetPath": "$.mailVerified",
        "scope": "createEntity"
      },
      {
        "constant": "disabled",
        "targetPath": "$.passwordStatus",
        "scope": "createEntity"
      },
      {
        "constant": "39",
        "targetPath": "$.sourceSystem",
        "scope": "createEntity"
      },
      {
        "constant": "employee",
        "targetPath": "$.userType"
      },
      {
        "sourcePath": "$.timezone",
        "targetPath": "$.timeZone",
        "optional": true
      }
    ]
  },
  "group": {
    "ignore": true,
    "mappings": [
      {
        "sourceVariable": "entityIdTargetSystem",
        "targetPath": "$.id"
      },
      {
        "sourcePath": "$.displayName",
        "targetPath": "$.displayName"
      },
      {
        "scope": "createEntity",
        "sourcePath": "$.displayName",
```

```
        "targetPath": "$['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']
['name']",
        "functions": [
          {
            "type": "replaceAllString",
            "regex": "[\\s\\p{Punct}]",
            "replacement": "_"
          }
        ]
      },
      {
        "scope": "createEntity",
        "optional": true,
        "sourcePath": "$['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']
['name']",
        "targetPath": "$['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']
['name']"
      },
      {
        "optional": true,
        "sourcePath": "$['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']
['description']",
        "targetPath": "$['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']
['description']"
      },
      {
        "optional": true,
        "preserveArrayWithSingleElement": true,
        "sourcePath": "$.members[*].value",
        "targetPath": "$.members[?(@.value)]",
        "functions": [
          {
            "type": "resolveEntityIds"
          }
        ]
      }
    ]
  }
}
```

Default Transformation for Identity Authentication as the Target System - Identity Authentication SCIM API Version 2:

Code Syntax

```
{
    "user": {
        "condition": "($.emails EMPTY false) && ($.userName EMPTY false) &&
isValidEmail($.emails[0].value)",
        "mappings": [
            {
                "sourceVariable": "entityIdTargetSystem",
                "targetPath": "$.id"
            },
            {
                "constant": [
                    "urn:ietf:params:scim:schemas:core:2.0:User",
                    "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
                    "urn:ietf:params:scim:schemas:extension:sap:2.0:User",
                    "urn:sap:cloud:scim:schemas:extension:custom:2.0:User"
                ],
                "targetPath": "$.schemas"
            },
            {
                "sourcePath": "$.active",
                "optional": true,
```

```
                "targetPath": "$.active"
            },
            {
                "sourcePath": "$.userName",
                "targetPath": "$.userName"
            },
            {
                "sourcePath": "$.emails",
                "preserveArrayWithSingleElement": true,
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['emails']",
                "scope": "createEntity",
                "functions": [
                    {
                        "function": "putIfAbsent",
                        "key": "verified",
                        "defaultValue": true
                    }
                ]
            },
            {
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['emails'][*]['type']",
                "type": "remove"
            },
            {
                "sourcePath": "$.emails[*].value",
                "preserveArrayWithSingleElement": true,
                "targetPath": "$.emails[?(@.value)]"
            },
            {
                "sourcePath": "$.userType",
                "optional": true,
                "targetPath": "$.userType",
                "defaultValue": "employee"
            },
            {
                "sourcePath": "$.name.givenName",
                "optional": true,
                "targetPath": "$.name.givenName"
            },
            {
                "sourcePath": "$.name.middleName",
                "optional": true,
                "targetPath": "$.name.middleName"
            },
            {
                "sourcePath": "$.name.familyName",
                "optional": true,
                "targetPath": "$.name.familyName"
            },
            {
                "sourcePath": "$.name.formatted",
                "targetPath": "$.name.formatted",
                "optional": true
            },
            {
                "ignore": true,
                "sourcePath": "$.name.honorificPrefix",
                "optional": true,
                "targetPath": "$.name.honorificPrefix"
            },
            {
                "sourcePath": "$.addresses",
                "preserveArrayWithSingleElement": true,
                "optional": true,
                "targetPath": "$.addresses",
                "functions": [
```

```
                    {
                        "function": "putIfAbsent",
                        "key": "type",
                        "defaultValue": "work"
                    },
                    {
                        "function": "putIfPresent",
                        "condition": "(@.type NIN ['work', 'home'])",
                        "key": "type",
                        "defaultValue": "work"
                    }
                ],
                "defaultValue": []
            },
            {
                "sourcePath": "$.preferredLanguage",
                "targetPath": "$.preferredLanguage",
                "optional": true
            },
            {
                "ignore": true,
                "sourcePath": "$.locale",
                "optional": true,
                "targetPath": "$.locale"
            },
            {
                "sourcePath": "$.phoneNumbers",
                "preserveArrayWithSingleElement": true,
                "optional": true,
                "targetPath": "$.phoneNumbers"
            },
            {
                "sourcePath": "$.displayName",
                "optional": true,
                "targetPath": "$.displayName"
            },
            {
                "sourcePath": "$.timezone",
                "optional": true,
                "targetPath": "$.timeZone"
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['validFrom']",
                "optional": true,
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['validFrom']"
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['validTo']",
                "optional": true,
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['validTo']"
            },
            {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['employeeNumber']",
                "optional": true,
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['employeeNumber']"
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['costCenter']",
                "optional": true,
```

```
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['costCenter']"
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['organization']",
                "optional": true,
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['organization']"
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['division']",
                "optional": true,
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['division']"
            },
            {
                "ignore": true,
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['department']",
                "optional": true,
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['department']"
            },
            {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",
                "optional": true,

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",
                "functions": [
                    {
                        "function": "resolveEntityIds"
                    }
                ]
            },
            {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['displayName']",
                "optional": true,

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['displayName']"
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['perPersonUuid']",
                "optional": true,

"targetPath": "$['urn:sap:cloud:scim:schemas:extension:custom:2.0:User']
['attributes'][0]['value']"
            },
            {

"condition": "$['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['perPersonUuid'] EMPTY false",
                "constant": "customAttribute1",

"targetPath": "$['urn:sap:cloud:scim:schemas:extension:custom:2.0:User']
['attributes'][0]['name']"
            },
            {
```

```
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['sourceSystem']",
                "optional": true,
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['sourceSystem']"
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['sourceSystemId']",
                "optional": true,
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['sourceSystemId']"
            },
            {
                "ignore": true,
                "constant": "%ias.initial.password.attribute%",
                "targetPath": "$.password",
                "scope": "createEntity"
            },
            {
                "constant": "disabled",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:sap:2.0:User']
['passwordDetails']['status']",
                "scope": "createEntity"
            },
            {
                "condition": "$.userType == 'ONBOARDEE'",
                "constant": "enabled",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:sap:2.0:User']
['passwordDetails']['status']",
                "scope": "createEntity"
            },
            {
                "condition": "$.userType == 'ALUMNI'",
                "constant": "enabled",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:sap:2.0:User']
['passwordDetails']['status']",
                "scope": "createEntity"
            },
            {
                "constant": false,
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['sendMail']",
                "scope": "createEntity"
            },
            {
                "condition": "$.userType == 'ONBOARDEE'",
                "constant": true,
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['sendMail']",
                "scope": "createEntity"
            },
            {
                "condition": "$.userType == 'ALUMNI'",
                "constant": true,
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['sendMail']",
                "scope": "createEntity"
            },
            {
                "constant": true,
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['mailVerified']",
                "scope": "createEntity"
            },
```

```
            {
                "condition": "$.userType == 'ONBOARDEE'",
                "constant": false,
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['mailVerified']",
                "scope": "createEntity"
            },
            {
                "condition": "$.userType == 'ALUMNI'",
                "constant": false,
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['mailVerified']",
                "scope": "createEntity"
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['applicationId']",
                "optional": true,
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['applicationId']",
                "scope": "createEntity"
            },
            {
                "condition": "($.userType == 'ONBOARDEE') &&
('%ias.onboardee.email.template.id.attribute%' !== 'null')",
                "constant": "%ias.onboardee.email.template.id.attribute%",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['emailTemplateSetId']",
                "scope": "createEntity"
            },
            {
                "condition": "($.userType == 'ALUMNI') &&
('%ias.alumni.email.template.id.attribute%' !== 'null')",
                "constant": "%ias.alumni.email.template.id.attribute%",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['emailTemplateSetId']",
                "scope": "createEntity"
            }
        ]
    },
    "group": {
        "mappings": [
            {
                "sourceVariable": "entityIdTargetSystem",
                "targetPath": "$.id"
            },
            {
                "constant": [
                    "urn:ietf:params:scim:schemas:core:2.0:Group",
                    "urn:ietf:params:scim:schemas:extension:sap:2.0:Group",
                    "urn:sap:cloud:scim:schemas:extension:custom:2.0:Group"
                ],
                "targetPath": "$.schemas"
            },
            {
                "sourcePath": "$.displayName",
                "targetPath": "$.displayName"
            },
            {
                "sourcePath": "$.displayName",
                "targetPath": "$
['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']['name']",
                "scope": "createEntity"
            },
            {
                "sourcePath": "$
['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']['name']",
                "optional": true,
```

```
                "targetPath": "$
['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']['name']",
                "scope": "createEntity"
            },
            {
                "sourcePath": "$
['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']['description']",
                "optional": true,
                "targetPath": "$
['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']['description']"
            },
            {
                "sourcePath": "$.members[*].value",
                "preserveArrayWithSingleElement": true,
                "optional": true,
                "targetPath": "$.members[?(@.value)]",
                "functions": [
                    {
                        "function": "resolveEntityIds",
                        "entityType": "user"
                    }
                ]
            },
            {
                "sourcePath": "$.members[*].value",
                "preserveArrayWithSingleElement": true,
                "optional": true,
                "targetPath": "$.members[?(@.value)]",
                "functions": [
                    {
                        "function": "resolveEntityIds",
                        "entityType": "group"
                    }
                ]
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:Group']",
                "optional": true,
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:Group']"
            }
        ]
    }
}
```

→ Tip

The default transformations for Identity Provisioning can also be found in their source document for both the Source and Target systems:

- To review the source document for the default **Source** transformations for SAP SuccessFactors provided by Identity Provisioning, refer to the section of their guide called Step 5 (Optional) Configure the Source transformations and click on Code Syntax to expand and review the transformation details.
- To review the source document for the default **Target** transformations for SAP SuccessFactors provided by Identity Provisioning, refer to Step 5 (Optional) Configure the Target transformations.

Related Information

Default Configuration of Identity Authentication with SAP SuccessFactors [page 50]

Opening the Identity Authentication Administration Console in SAP Cloud Identity Services [page 168]

10.4.6 Default Tenant Configurations for HCM Suite and Identity Authentication

When a new SAP SuccessFactors HCM suite tenant is provisioned, or when the *Initiate the* SAP Cloud Identity Services Identity Authentication Service *Integration* or *Change SuccessFactors* Identity Authentication Service *Integration* tasks are run in the Upgrade Center, the HCM suite tenant will be automatically configured for integration with the Identity Authentication tenant.

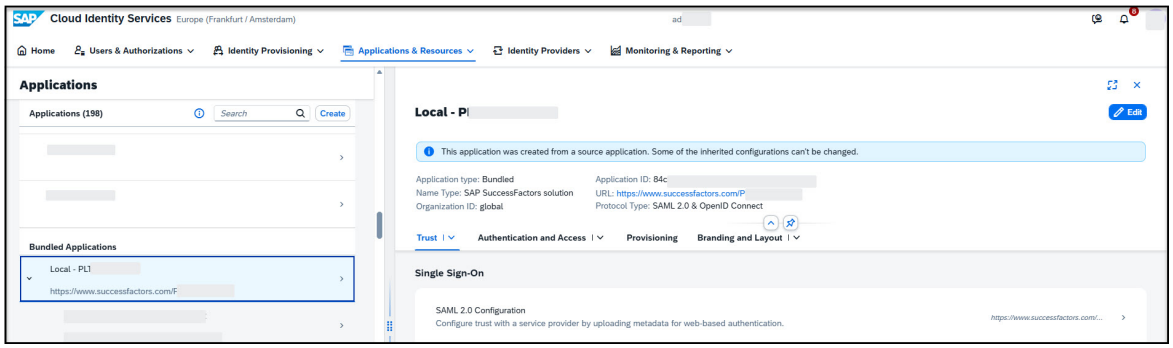
The following outlines the default configuration settings after this integration is completed:

1. In the SAP Cloud Identity Services admin console, under *Applications & Resources* > *Applications*, an application for the HCM suite tenant is created with the following attributes:

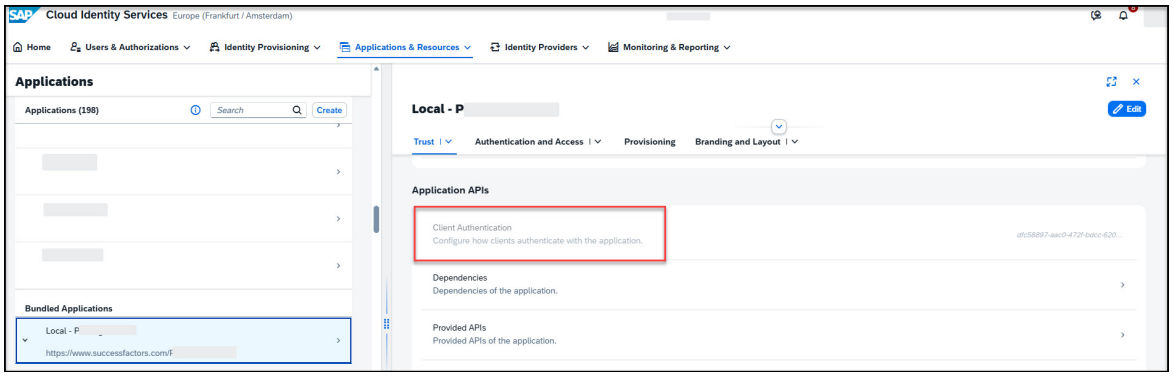
Name	Value
Application Type	Bundled
Name Type	SAP SuccessFactors Solutions
Protocol Type	SAML 2.0 & OpenID Connect
Organization	global
URL	• **Pattern**: `https://<SF Customer Facing Hostt>/login?company=<company_id>` • **Example**: `https://qacand.qa.hr.cloud.sap/login?company=xyz`

The application is configured as a hybrid application using both SAML 2.0 and OpenID Connect.
The following default behaviors apply to the application:

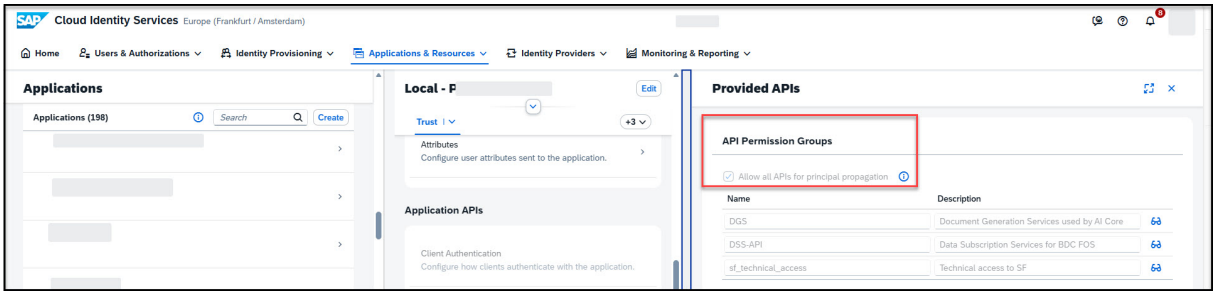
- A message indicates that the application was created from a source application and that some inherited configurations can't be changed.



- Under *Application APIs*, the *Client Authentication*section is grayed out.



- In the *Provided APIs* section, the *Allow all APIs for principal propagation* checkbox is checked and grayed out. The *sf_technical_access* provided API is also predefined and grayed out.



2. Under *Single Sign-On* > *SAML 2.0 Configuration*, this particular SAP SuccessFactors application will have the following SAML 2.0 attributes:

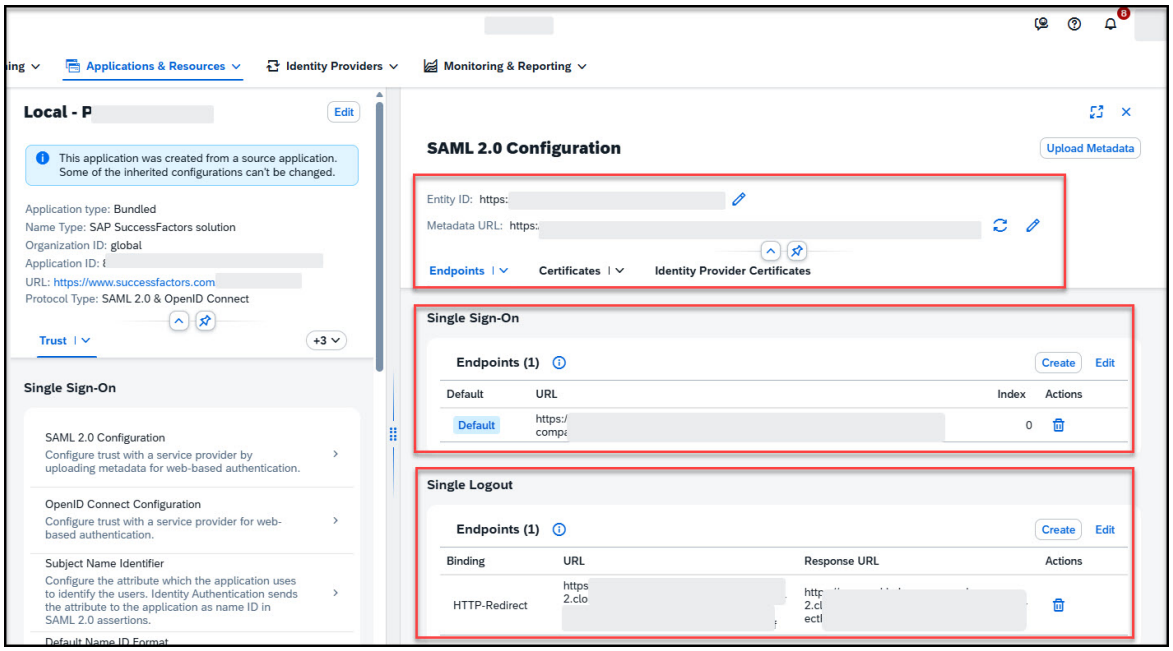
Name	Value
Entity ID	• **Pattern**: `https://<SF Customer Facing Host>//<company_id>` • **Example**: `https://www.successfactors.com/xyz`
Metadata URL	• **Pattern**: `https://<SF Customer Facing Host>/saml2/spmetadata?company=<company_id>` • **Example**: `https://qacand.qa.hr.cloud.sap/saml2/spmetadata?company=xyz`

- Under *Single Sign-On Endpoints*:

Name	Value
Default	Checked
URL	• **Pattern**: https://<SF Customer Facing Host>/saml2/SAMLAssertionConsumer?company=<company_id> • **Example**: https://qacand.qa.hr.cloud.sap/saml2/SAMLAssertionConsumer?company=xyz

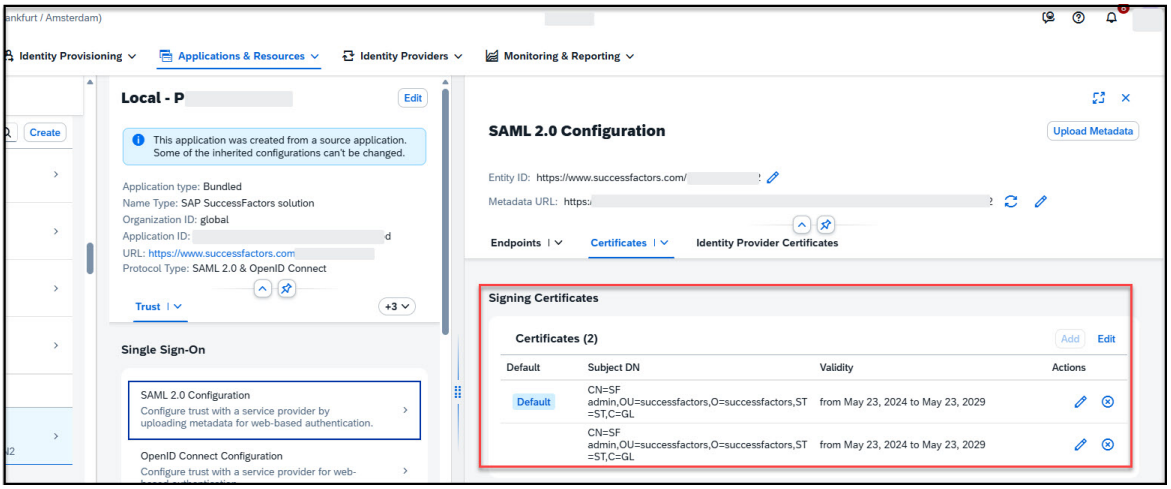
- Under *Single Logout Endpoints*:

Name	Value
Binding	HTTP-Redirect
URL	• **Pattern**: `https://<SF Customer Facing Host>/saml2/LogoutServiceHTTPRedirect?company=<company_id>&amp;RelayState=sf` • **Example**: `https://<SF Customer Facing Host>/saml2/LogoutServiceHTTPRedirect?company=<company_id>&amp;RelayState=sf`
Response URL	• **Pattern**: `http://<SF Customer Facing Host>/saml2/LogoutServiceHTTPRedirectResponse?company=<company_id>` • **Example**: `http://qacand.qa.hr.cloud.sap/saml2/LogoutServiceHTTPRedirectResponse?company=xyz`



- Under *Signing Certificate*:

Name	Value
Subject DN	`CN=SF admin,OU=successfactors,O=successfactors,ST=ST,C=GL`
Validity	Default date range should be a 5-year period.

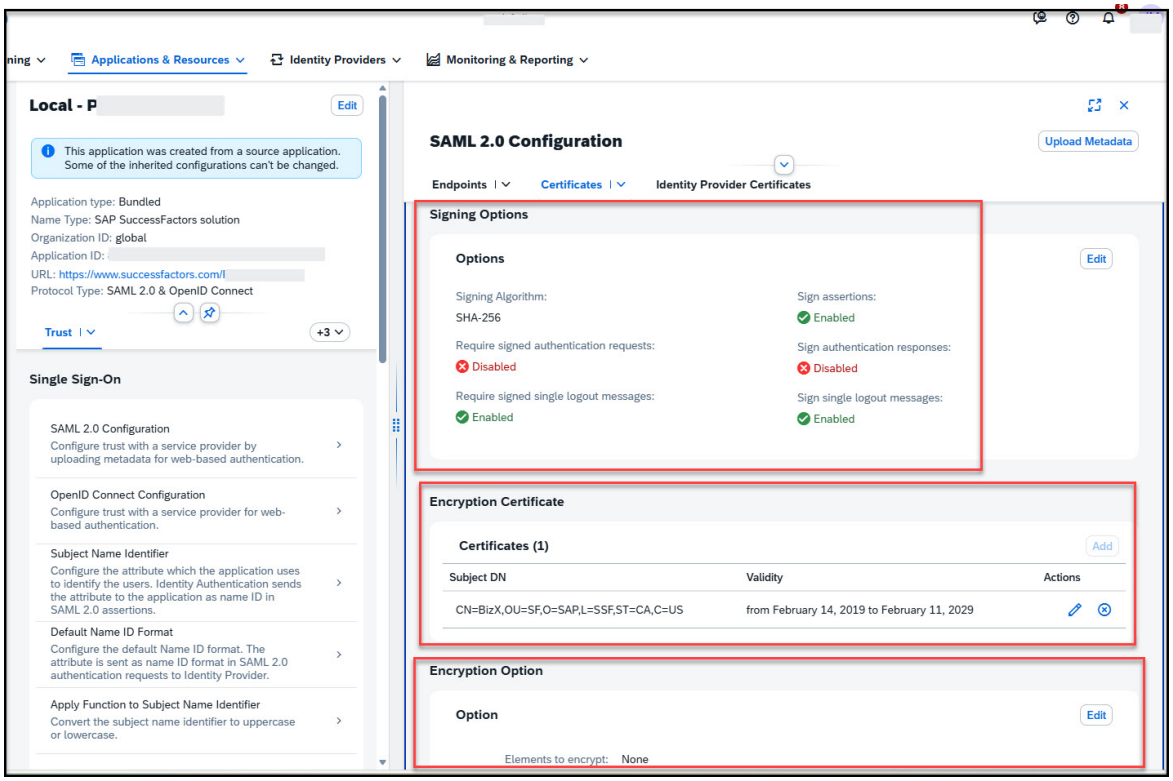


- Under *Signing Options*:

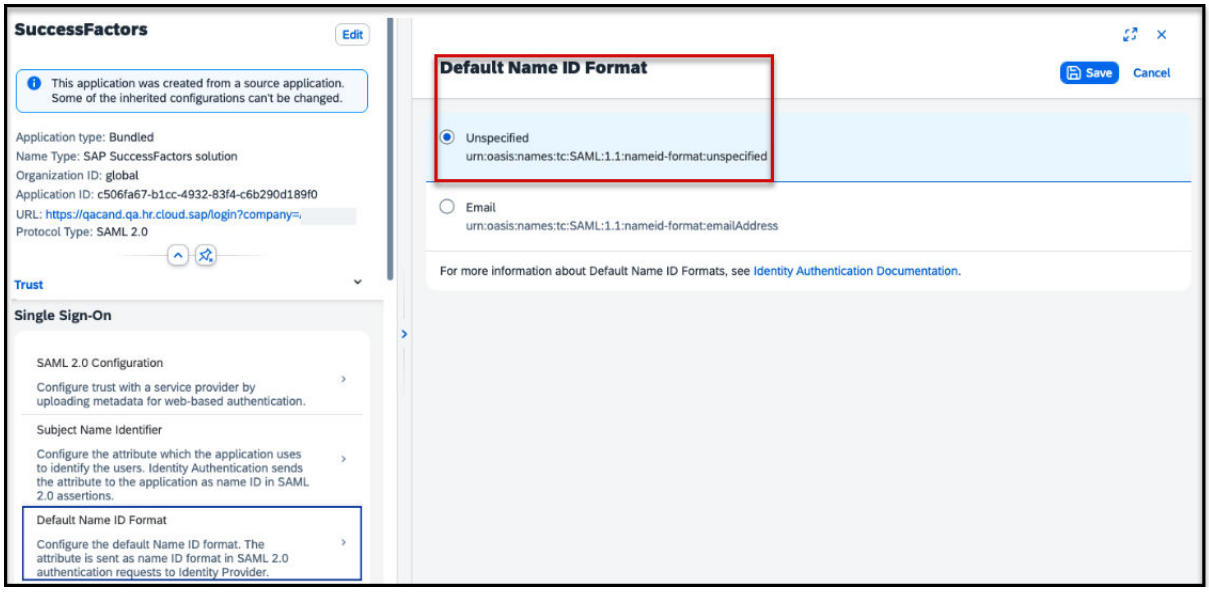
Name	Value
Signing Algorithm	SHA-256
Sign assertion	Checked (Enabled)
Sign single logout messages	Checked (Enabled)
Require signed single logout messages	Checked (Enabled)
Sign authentication responses	X (Disabled)
Require signed authentication requests	X (Disabled)

- Under *Encryption Certificate*: the *Subject DN* and *Validity* values below should be exactly the same as the corresponding values under the *Signing Certificate* section:

Name	Value
Subject DN	`CN=SF admin,OU=successfactors,O=successfactors,ST=ST,C=GL`
Validity	Default date range should be a 5-year period.
Elements to encrypt	None

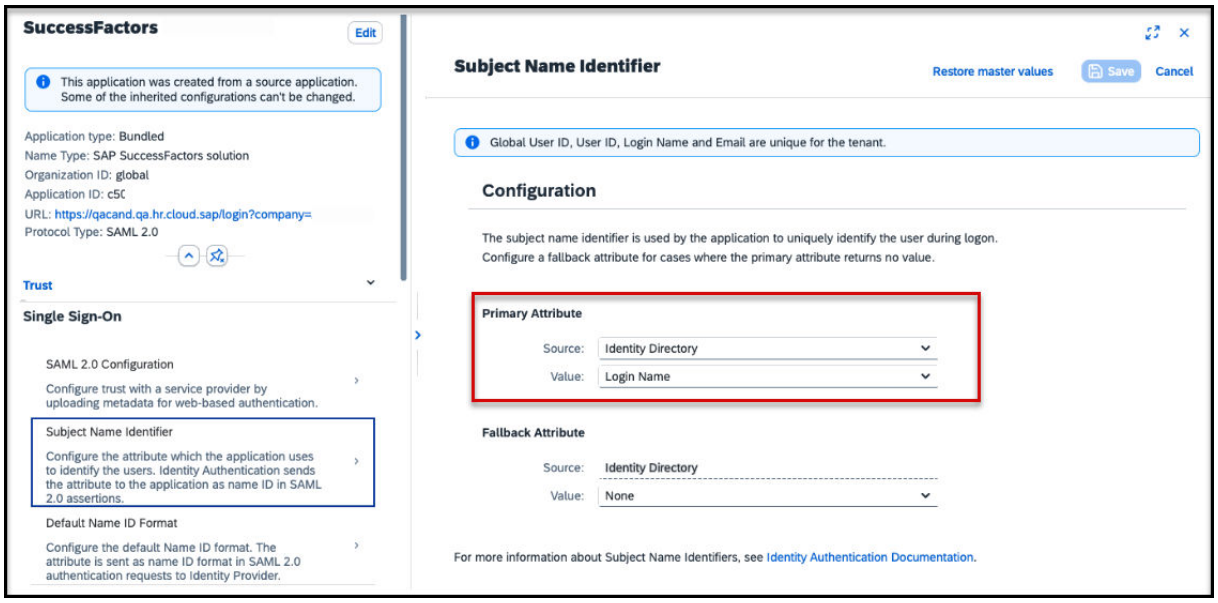


3. Under *Default Name ID Format*, the *Unspecified* radio button is checked.



4. Under *Subject Name Identifier*:

Name	Value
Source	Identity Directory
Value	Login Name



SAP SuccessFactors Mobile Service Application

We provide a preconfigured SAP SuccessFactors Mobile Service application in Identity Authentication for all tenants that have Identity Authentication enabled. This application supports OpenID Connect based authentication for the SAP SuccessFactors mobile app.

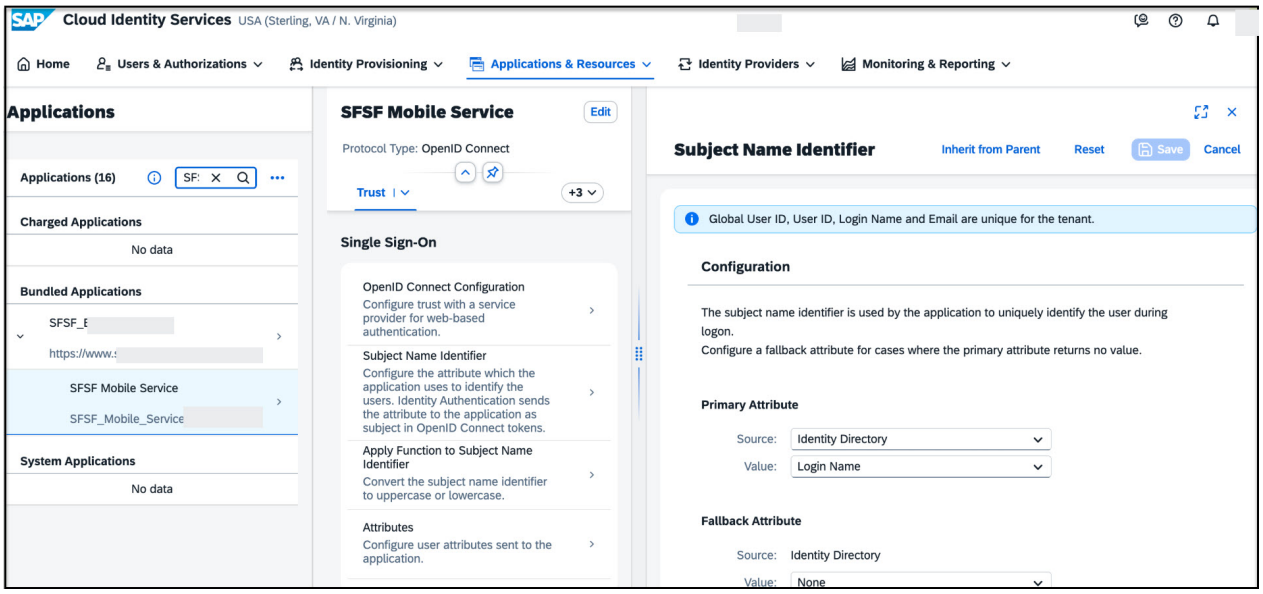
Default Configuration

In the Identity Authentication admin console, under *Applications & Resources* > *Applications*, the mobile service application is created with the following attributes:

Name	Value
Application Type	Bundled
Name Type	SAP BTP solution
Protocol Type	OpenID Connect
Organization	Global
Name	SFSF_Mobile_Service_<company_id>

Under *Subject Name Identifier:*

Name	Value
Source	Identity Directory
Value	Login Name



The mobile service application is automatically provisioned. You do not need to create or configure a mobile OIDC application. Do not modify or delete this application, as it is required for mobile authentication.

Since the 1H 2026 release, this application is automatically provisioned for all existing tenants.

> **Note**
>
> The presence of the mobile service application does not mean that authentication with SAP BTP Mobile Services is enabled. To enable BTP authentication, you must run the corresponding upgrade in Upgrade Center. For more information, see Enabling Authentication with BTP Mobile Services.

Auto-Created Technical Administrators in Identity Authentication

As part of the automatic configuration process, Identity Authentication creates two technical administrator users that support secure communication between SAP SuccessFactors, Identity Authentication, and Identity Provisioning. These accounts are system-managed and required for integration scenarios.

Both users appear in the SAP Cloud Identity Services admin console under *Users & Authorizations* > *Administrators* > **Do not modify or delete these users**.

1. **SAP IPS-SFSF – companyID**

This technical administrator supports certificate-based communication from SAP SuccessFactors to Identity Provisioning using X.509/mTLS authentication.

Created During:

- New SAP SuccessFactors tenant provisioning
- The *Initiate the SAP Cloud Identity Services Identity Authentication Service Integration* task
- The *Change SuccessFactors Identity Authentication Service Integration* task

Purpose:

- Required to support SAP SuccessFactors to Identity Provisioning integration using X.509/mTLS authentication
- Replaces Basic Authentication for backend Identity Provisioning communication
- Visible under *Users & Authorizations* > *Administrators* in Identity Authentication

2. **SF Admin Center**

Supports SAP SuccessFactors operations such as retrieving and updating corporate identity provider (IDP) configurations and enabling actions on the *Manage SAML SSO Settings* page.

Created During:

- New SAP SuccessFactors tenant provisioning
- *Initiate the SAP Cloud Identity Services Identity Authentication Service Integration* task
- *Change SuccessFactors Identity Authentication Service Integration* task

Purpose:

- Retrieves and updates corporate IDP configurations
- Supports metadata retrieval during SAML SSO setup
- Visible under *Users & Authorizations* > *Administrators* in Identity Authentication

> **Note**
>
> Starting with the SAP SuccessFactors 2605 release, the system no longer creates the *SF Admin Center* technical administrator. For Identity Authentication tenants provisioned before 2605, this user may still exist but is no longer used.

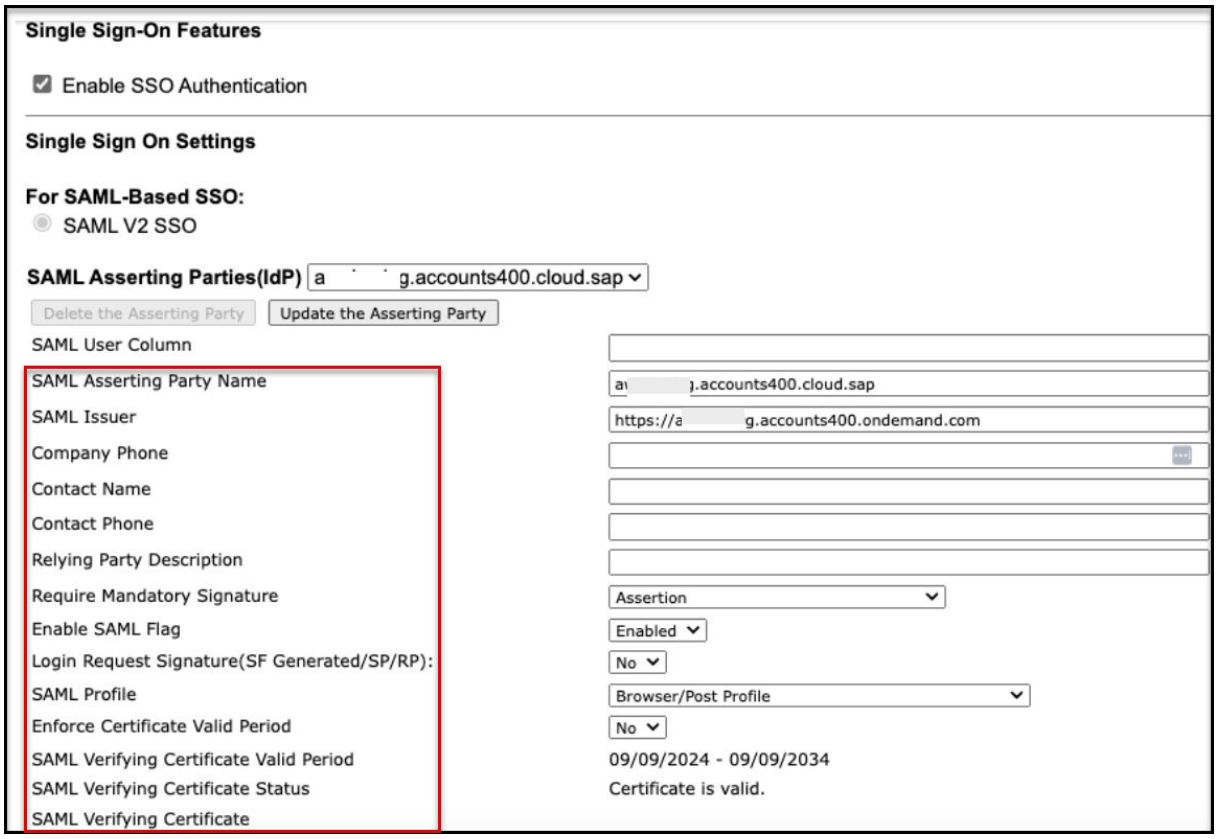
Default SAP SuccessFactors SSO Settings in Provisioning

In *Provisioning*, under the *Single Sign-On (SSO) Settings* page:

1. The *Enable SSO Authentication* checkbox is checked.
2. The *SAML V2 SSO* radio button is enabled.
3. The pre-configured Identity Authentication appears as a SAML Asserting Party (IdP) record in the drop-down list, with the following assertion party attributes:

Name	Value
SAML Asserting Party Name	Pattern is the Identity Authentication URL **without** "https": `xyz.accounts400.cloud.sap`
SAML Issuer	Pattern is the Identity Authentication URL **with** "https": `https://xyz.accounts400.cloud.sap`
Require Mandatory Signature	Assertion
Enable SAML Flag	Enabled
Login Request Signature (SF Generated/SP/RP)	No
SAML Profile	Browser/Post Profile

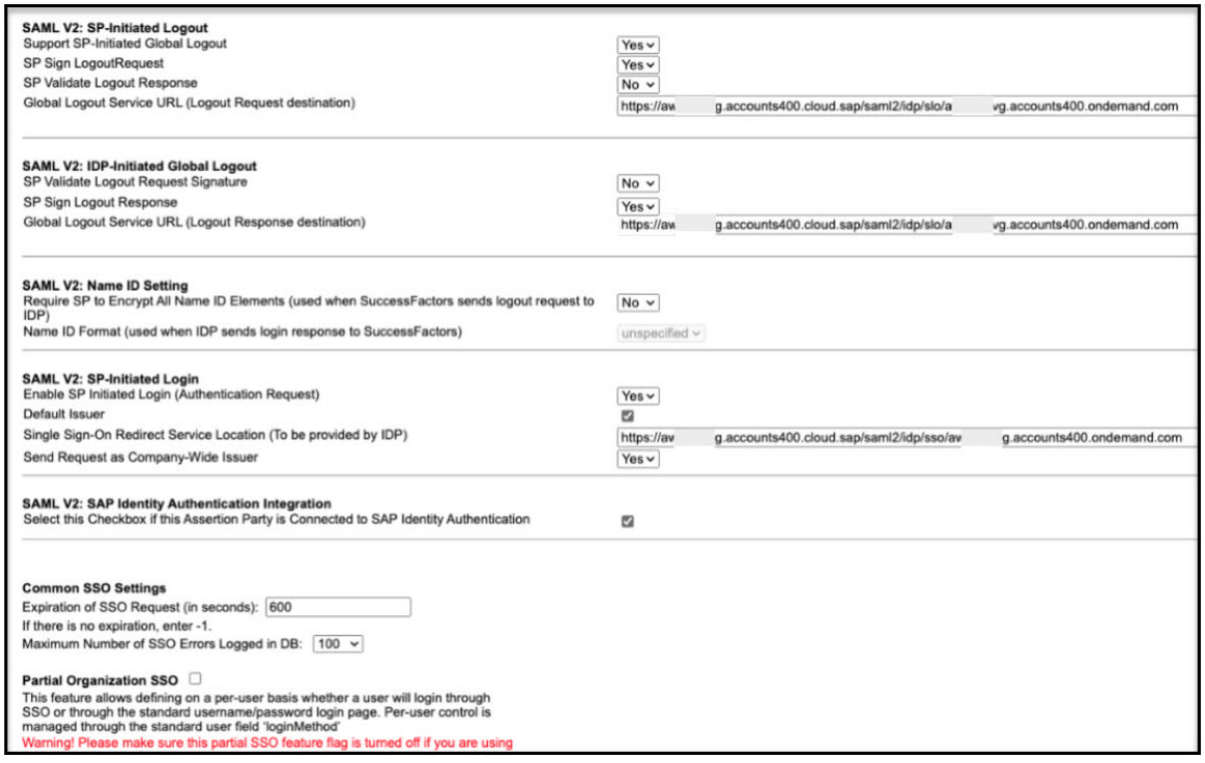
Name	Value
SAML Verifying Certificate Valid Period	Should be the same as *Identity Provider Certificate Validity Period* under the *SAML 2.0 Configuration* section for this HCM suite tenant in the Identity Authentication admin console.
SAML Verifying Certificate Status	Certificate is valid.



4. The SAML 2.0 configurations are as follows:

Name	Value
Support SP-Initiated Global Logout	Yes
SP Sign LogoutRequest	Yes
SP Validate Logout Response	No
Global Logout Service URL (Logout Request destination)	**Pattern**: `https://xyz.accounts400.cloud.sap/saml2/idp/slo/xyz.accounts400.ondemand.com` Global Logout Service URL (Logout Request destination)
SP Validate Logout Request Signature	No
SP Sign Logout Response	Yes

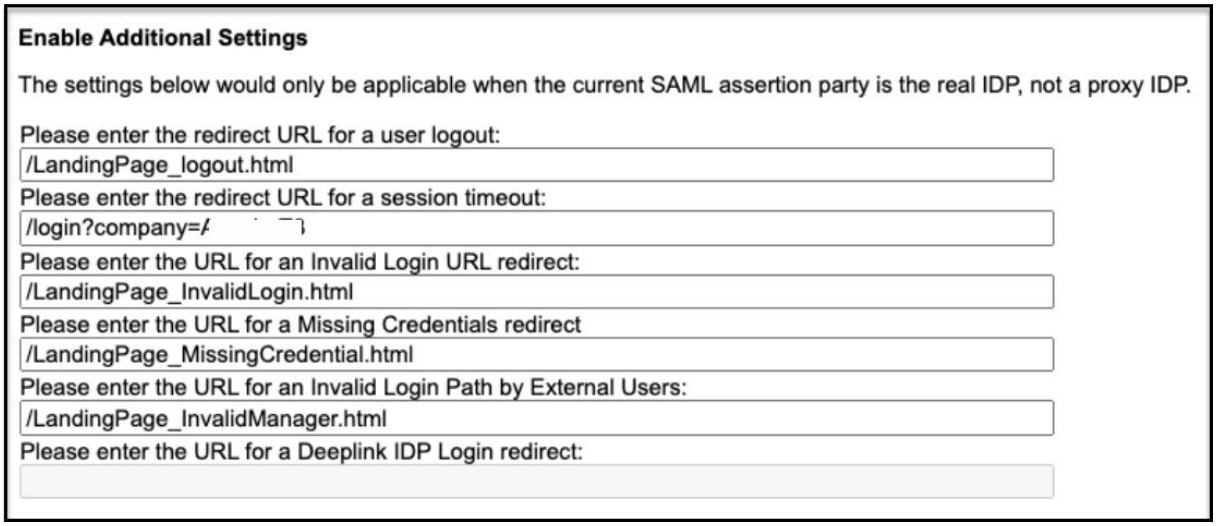
Name	Value
Global Logout Service URL (Logout Response destination)	**Pattern**: `https://xyz.accounts400.cloud.sap/saml2/idp/slo/xyz.accounts400.ondemand.com`
Require SP to Encrypt All Name ID Elements (used when SuccessFactors sends request to IDP)	No
Name ID Format (used when IDP sends login response to SuccessFactors)	Unspecified (this field is also grayed out and cannot be modified)
Enable SP Initiated Login (Authentication Request)	Yes
Default Issuer	Checked (Enabled)
Single Sign-On Redirect Service Location (To be provided by IDP)	**Pattern**: `https://xyz.accounts400.cloud.sap/saml2/idp/slo/xyz.accounts400.ondemand.com`
Send Request as Company-Wide Issuer	Yes
SAML V2: SAP Identity Authentication Integration	Checked (Enabled)
Partial Organization SSO	Unchecked (Disabled)



5. The *EnableAdditional Settings* section has the following Redirect URL values:

Name	Value
URL for a user logout	`/LandingPage_logout.html`

Name	Value
URL for a session timeout	• **Pattern**: `/login?company=<company_id>` • **Example**:`/login?company=xyz`
URL for an invalid Login URL redirect	`/LandingPage_InvalidLogin.html`
URL for Missing Credentials redirect	`/LandingPage_MissingCredential.html`
URL for an invalid Login Path by External Users	`/LandingPage_InvalidManager.html`
URL for a Deeplink IDP Login redirect	Empty and grayed out



11 Additional Configurations for SAP SuccessFactors HCM suite with SAP Cloud Identity Services

11.1 Remapping an Identity Authentication Tenant

You can remap or (or change) your existing Identity Authentication tenant using the Upgrade Center.

Context

In the Upgrade Center, you can remap tenants that have already been initiated, activated, or configured with Identity Authentication in SAP Cloud Identity Services. When you remap a tenant, your Identity Authentication and Identity Provisioning configurations don't automatically migrate - you must reconfigure them manually. In the SAP SuccessFactors Upgrade Center, you can start this process by selecting *Change SuccessFactors* Identity Authentication *Integration* .

> ⚠ Caution
>
> Before completing this step, consider the following:
>
> - Only perform this action if you have a legitimate business reason why the currently integrated Identity Authentication tenant cannot be used. Changing tenants may impact Single Sign-On (SSO) with other integrated applications and could require additional configuration in those applications. Exercise extreme caution.
> - Before proceeding, it is strongly recommended to check the current Initiate Identity Authentication upgrade status and the Identity Authentication/Identity Provisioning tenant information using the *Monitoring tool*. This helps ensure that the current integrated Identity Authentication/Identity Provisioning tenants cannot be reused. Refer to **Monitoring Tool for the Upgrade to Identity Authentication** in the **Related Information** section.
> - After completing the initial upgrade to Identity Authentication, each tenant can only perform the remap (change) action from the Upgrade Center one time.
> - Once the change is complete, and the remapped tenant is activated via the *Activate SuccessFactors* Identity Authentication Service *Integration* task in the Upgrade Center, this will be the only tenant that can be seen in your system.
> - Initial upgrades or remapping tasks performed by the Upgrade Center cannot be undone.
> - If you have requested an additional Identity Authentication tenant for an SAP SuccessFactors tenant, be aware that **its existence is tied to the associated SAP SuccessFactors tenant**. Decommissioning the SAP SuccessFactors tenant will also delete the additional Identity Authentication tenant, which may disrupt any other applications relying on it.

> ### Note
>
> If you perform the below steps to remap (or change) your existing Identity Authentication tenant using the Upgrade Center after December 9, 2022, Identity Authentication and Identity Provisioning will be configured to use Mutual Transport Layer Security (mTLS) in conjunction with the System for Cross-domain Identity Management (SCIM) API, which are the latest methods of authentication and integration with Identity Authentication and Identity Provisioning.

> ### Note
>
> Identity Authentication is included natively in all partner paid demo tenants (i.e. Company ID starts with **SFCPART**) which is created from a template with "IAS" in the template description and version name. Selecting one of these templates automatically ensures that Identity Authentication is provisioned along with the demo tenant during the provisioning process, without the need to run any Identity Authentication process through the Upgrade Center. Additionally any Identity Authentication Initiate Upgrade or Change tasks, if available in the Upgrade Center, should not be run and is not supported by Technical Support.

Procedure

1. Go to *Admin Center* > *Upgrade Center* > *Optional Upgrades*.
2. Find the upgrade *Change SuccessFactors* Identity Authentication Service *Integration* and click *Learn More & Upgrade Now*.
3. Click *Upgrade Now.*
4. Enter your *S-User* and password in the dialog and click *Validate*.

   > ### Note
   >
   > If you encounter validation errors, refer to this Knowledge Base Article 2944990

5. Select a tenant from your list of displayed tenants or select request a new tenant to the Identity Authentication service.

   The list now includes an *Ownership* field showing whether a tenant is:

   - *Owned*: registered under your organization's customer ID, or
   - *Trusted*: belongs to a different customer ID but is accessible because a trust relationship has been configured in Identity Authentication within SAP Cloud Identity Services.

   This helps you identify the appropriate tenant for integration. This view also displays the tenant that is currently enabled. For more information about how multiple customer IDs can reuse the same Identity Authentication tenant, see Reuse SAP Cloud Identity Services Tenants for Different Customer IDs.

   > ### Note
   >
   > The tenants available for remapping are listed according to the tenants in your region. If the tenant that you want to remap is located in a different region or you don't see the tenant that you want to upgrade, first check whether the tenant appears when searching for Identity Authentication tenants on the Cloud Identity Serices-Tenants page based on your current customer ID.

If the tenant desired still does not appear but is confirmed to be associated with your customer ID, please contact your implementation partner or Account Executive so that they can enable the *Ignore region and type restrictions for* Identity Authentication Service *integration (Warning: This feature should be turned on only when an existing* Identity Authentication *tenant needs to be integrated).* setting.

> ⚠ Caution
>
> Although this option is available, we recommend you retain the default settings, which limit the use of Identity Authentication to the appropriate region and corresponding tenant type of the SAP SuccessFactors tenant (for example, ensuring that production Identity Authentication tenants are used for production SAP SuccessFactors tenants, and test/preview Identity Authentication tenants are used for test/preview SAP SuccessFactors tenants). Only select the *Ignore region and type restrictions for* Identity Authentication Service *integration (Warning: This feature should be turned on only when an existing* Identity Authentication *tenant needs to be integrated).* setting when your company absolutely needs this configuration enabled, and you have evaluated and validated all the impacts and consequences.

6. Confirm your selection by choosing *Yes* when the confirmation dialog displays.

Results

> ⓘ Note
>
> Additional tenants can be requested by following the same steps for **Remapping an Identity Authentication Tenant** and selecting **Request New Tenant** *instead* of selecting an existing tenant from the list.

> ⚠ Caution
>
> If you've **already** selected an additional tenant using this process, and later decide to switch tenants **or** request another new tenant, the initial tenant may be deleted.

The integration process runs in the background and can take up to 24 hours to complete. After the upgrade process completes, an email is sent with tenant details. You can monitor the progress of your upgrade using the Identity Authentication Monitoring Tool.

Next Steps

When the upgrade completes, you can configure your new tenant.

Related Information

Monitoring Tool for the Upgrade to Identity Authentication [page 44]

11.2 Authenticating New Hires with Identity Authentication in SAP Cloud Identity Services

Onboarding customers can now select Identity Authentication in SAP Cloud Identity Services.

Prerequisites

- Onboarding is enabled with the **SCIM API** for integration based on the following:
  - You're provisioned with a new SAP SuccessFactors tenant with Identity Authentication and Identity Provisioning preconfigured.
  - Or the upgrade to the Identity Authentication service is fully completed with the SCIM API.
  - Or the manual upgrade from OData V2 to the SCIM API has been completed.

    > ⓘ Note
    >
    > For Onboarding customers performing the manual upgrade from OData V2 to the SCIM API, the *Provisioning* > *Company Settings* > *Onboardee* setting must also be enabled.
    >
    > > → Remember
    > >
    > > 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.

> ⓘ Note
>
> If you're an existing customer with the Identity Authentication service using OData V2 enabled, then the *Settings* tab under *Admin Center* > *Monitoring Tool for* Identity Authentication / Identity Provisioning *Service Upgrade* is currently unavailable. The ability to upgrade from OData V2 to System for Cross-domain Identity Management (SCIM) is available as of January 20, 2023. Refer to **Upgrade from OData Identity Provisioning Connector to SCIM Connector with SAP SuccessFactors HCM suite in the** in the **Related Information** section.

Context

Onboarding customers can now select Identity Authentication for new hires using the **Settings** tab.

Procedure

1. Search for *Monitoring Tool* in the *Tools* tile, or by using the Admin Center search bar.
2. Click the *Settings* tab.

   > ⓘ Note
   >
   > If you've enabled Onboarding, but **have not yet** initiated the upgrade to Identity Authentication, or the upgrade is **not yet complete**, you will **not** see the **Settings** tab. Please initiate and complete the upgrade first.

3. Click on *Apply to both Employee and Onboardee*.

   > ⚠ Caution
   >
   > Make sure you've completed all prerequisites before selecting this option, or you risk experiencing issues with integration functionality.

   > ⓘ Note
   >
   > If **you have already** initiated the upgrade to Identity Authentication, and the upgrade is complete, the option to select *Apply to both Employee and Onboardee* will only display if your Onboarding integration is using the **SCIM API**.
   >
   > If your SuccessFactors tenant is provisioned with the Identity Authentication service already preconfigured, then you will not see the option to select *Apply to both Employee and Onboardee*. Instead you will see *Employee and Onboardee Application Completed* displayed and grayed out, since the option has already been enabled by the tenant provisioning process automatically.
   >
   > You will also see *Employee and Onboardee Application Completed* displayed and grayed out, if your existing SAP SuccessFactors tenant has intitiated the upgrade to Identity Authentication after December 9, 2022 and the upgrade is complete.

4. Click *Approve* to confirm your changes.

Results

Going forward, both your employees and new hires will now be authenticated with the Identity Authentication service.

Next Steps

Next, complete the steps in the **Setting up Identity Authentication Service Support for New Hires Using System for Cross-domain Identity Management (SCIM) API** guide in the **Related Information** section.

If your organization also manages alumni users, see Enabling Alumni Access and Configuring the Alumni Activation Email Template in Identity Authentication for guidance on how to set up alumni access and implement Identity Authentication for these users.

Related Information

Initiating the Upgrade to Identity Authentication in SAP Cloud Identity Services [page 40]
Setting up Identity Authentication Service for New Hires Using System for Cross-domain Identity Management (SCIM) API
Upgrade from ODATA Identity Provisioning Connector to SCIM Connector with SAP SuccessFactors [page 139]

11.3 Manage Real-Time Sync of Users from SAP SuccessFactors to Identity Authentication with Identity Provisioning

You can enable or disable the real-time sync of user account changes from SAP SuccessFactors to Identity Authentication using Identity Provisioning. Both Onboardee and Employee user types are supported.

Prerequisites

- You have enabled Onboarding in *Provisioning* > *Company Settings* > *Onboarding (including Internal Hire Process)*.

  > → Remember
  >
  > 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.

- The SAP SuccessFactors Source System in Identity Provisioning must be using **sf.api.version = 2** (SCIM API).
- You've already configured SAP SuccessFactors as the **Source** system and Identity Authentication as your **Target** system in the Identity Provisioning administration console. Refer to **Setting Up the Identity Provisioning Source and Target Systems** in the **Related Information** section.

  > ⓘ Note
  >
  > If your Identity Authentication tenant was created after December 9, 2022, or your existing SAP SuccessFactors tenant has upgraded to Identity Authentication after December 9, 2022, your source and target systems have already been configured for you automatically, so you don't need to set them up manually.

- You have the *Administrator Permissions* > *Manage Security Center* > *Access to X.509 Certificates* permission and the *Create, Edit & Delete* box enabled.
- You have the *Administrator Permissions* > *Manage Identity Account and Group* > *Manage Identity Authentication/Identity Provisioning Real Time Sync* permission.
- You have the *Administrator Permissions* > *Manage Integration Tools* > *Access to Integration Service Registration Center UI* permission.

Context

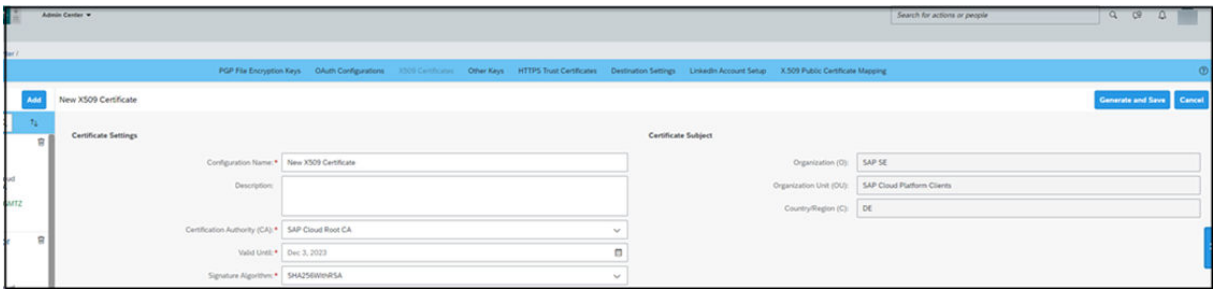
Real-time synchronization allows for the immediate update of user account data without having to manually run or wait for a scheduled job. This feature comes in handy for scenarios when updates to a user's information are made for immediate system access.

> **Note**
>
> The steps below apply only to Identity Provisioning tenants running on the **SAP Cloud Identity infrastructure** (you can recognize it by its URL as it uses the host of the corresponding Identity Authentication tenant and follows the pattern `https://<tenant-id>.accounts.ondemand.com` or `https://<tenant-id>.accounts.cloud.sap`).
>
> If you've completed the steps below and have since migrated your bundle or standalone tenant from the **SAP BTP, Neo environment** to the **SAP Cloud Identity infrastructure**, you will need to complete them again to use the real-time sync feature.
>
> If your Identity Provisioning tenant is running on the **SAP BTP, Neo environment**, we recommend that you migrate to the **SAP Cloud Identity infrastructure**. Refer to Migrate Identity Provisioning Bundle Tenants for more information on how to migrate your bundle or standalone tenant.

Procedure

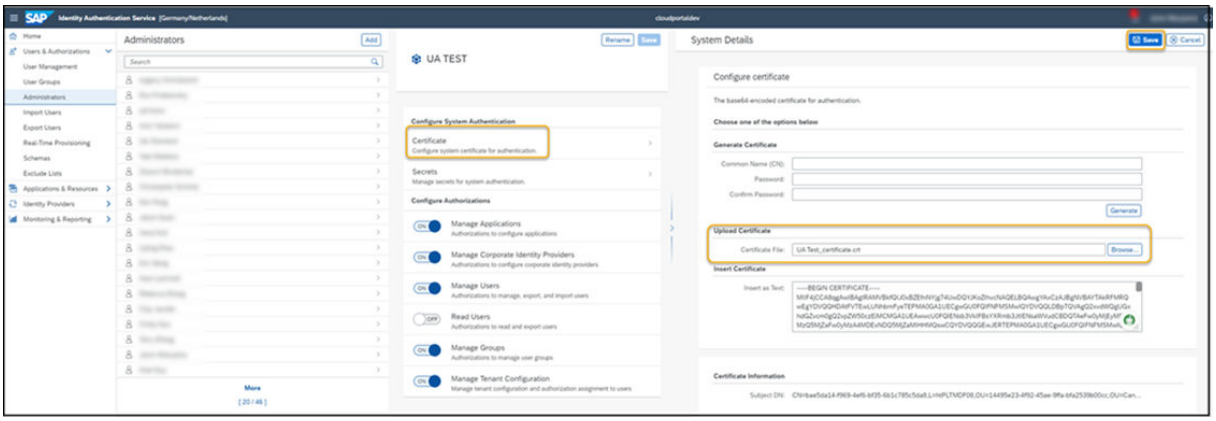
1. Navigate to the SAP SuccessFactors *Admin Center* > *Security Center* > *X.509 Certificates* screen.
2. Click *Add*.
3. Complete the following **required** fields:

Field	Description
Configuration Name	Example: New X.509 Certificate
Certificate Authority (CA)	Select either *SAP Cloud Root CA* or *External CA*.
Valid Until	Select an expiration date for the certificate. **Note** This field allows you to set the expiration date up to one year in advance. Make sure to update the date again before your certificate expires to avoid failure of the real-time sync.
Signature Algorithm	Keep defaulted value of `SHA256WithRSA`



4. Click *Generate and Save*.

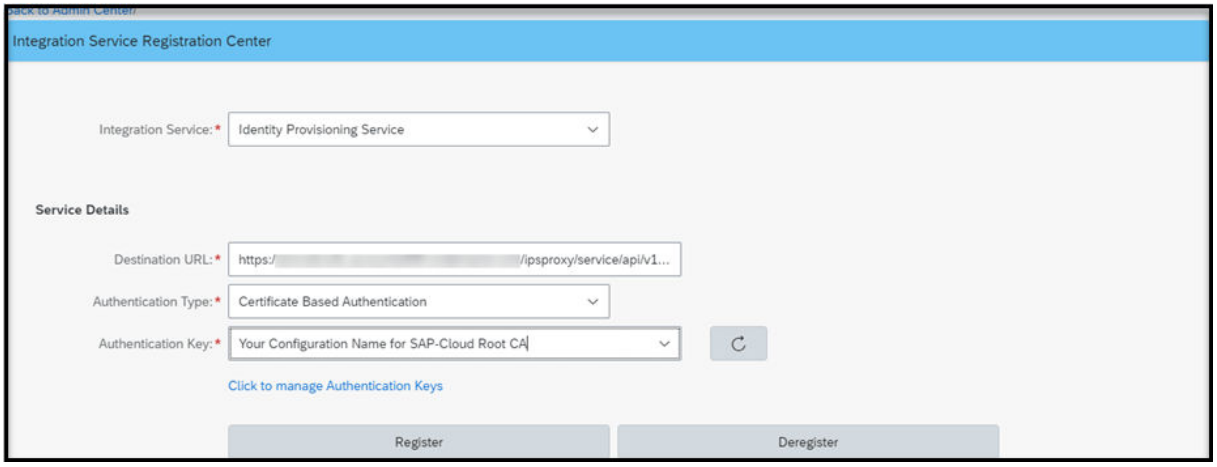
   A tile with the configuration name of your newly generated certificate will appear on the left side of the screen.
5. Click on the tile for your certificate.
6. Click *Download* > *X.509 Certificates* and save the certificate to your local file system.
7. Navigate to the administration console (the url for this console is found in your **Access Information for your** welcome email and has the following format: `https://<tenant ID>.accounts.ondemand.com/admin`).
8. Click *Users & Authorizations* > *Administrators* > *Add* > *System*.
9. On the *System Details* screen, enter a system name and click *Save*.
10. Next, click on *Certificate*.
11. In the *Upload Certificate* section, click *Browse* and upload the X.509 certificate you generated in **step 4**.



12. Under the *Configure Authorizations* section, set the *Access Real-Time Provisioning API* permission to *ON*
13. Save your changes.
14. Navigate to the SAP SuccessFactors *Admin Center* > *Integration Services Registration Center* screen.
15. Complete the following fields:

Field	Description
Integration Service	Select *Identity Provisionng Service* from the drop-down menu.

Field	Description
Destination URL	Enter the Identity Provisioning system URL: The URL format for the **SAP Cloud Identity infrastructure**: `https://<ips-tenant-host>/ipsproxy/service/api/v1/systems/<system-id>` **Note** The `<system-id>` is the ID of the **SAP SuccessFactors** source system you've added in the Identity Provisioning console and is displayed at the end of the system URL.
Authentication Type	Select *Certificate Based Authentication* from the drop-down menu.
Authentication Key	Select the configuration name of the X.509 certificate for SAP SuccessFactors from the drop-down menu. This is the **Configuration Name** that is tied to either the **SAP-Cloud Root CA** or **External CA** certificates, as these are currently the only Certificate Authorities supported. **Note** You can view the details of your X.509 certificates, as well as the *Configuration Name* and *Certificate Authority* they are tied to on the *Admin Center* > *Security Center* > *X.509 Certificates* screen. .



16. Click *Register*.
17. Navigate to the SAP SuccessFactors *Admin Center* > *Manage Identity Authentication/Identity Provisioning Real Time Sync* screen.
18. Set *Enable Real Time Sync* to *ON*.
19. Select the user account types you want to sync. Supported options are *Onboardee* and *Employee*.

20. Save your changes.

    You've successfully enabled the real-time user sync for Onboardee and Employee user types into Identity Authentication.

> ⓘ Note
>
> **Frequently Asked Questions**
>
> - **How can I check wether the New Hire is synced to Identity Authentication?**
>   The extension status indicates whether the new hire record is ready to be synced to Identity Authentication:
>   - **0-Active**: The new hire is synced to Identity Authentication.
>   - **1-Inactive**: The new hire is an inactive external user and will not be synced to Identity Authentication.
>   - **2-Pending**: The user would not be synced to Identity Authentication though they are an active user. This is applicable only for new hires. Employees would toggle between 0 and 1.
>   When the new hire is required to complete a personal data collection page, we set the status to 0 (Active) so that the user is synced to Identity Authentication and gets an Identity Authentication Activation email. So in this case, the new hire will be notified only when their inputs are required.
> - **How do I distinguish between an Employee and a New Hire in Identity Authentication?**
>   Identity Authentication uses the user types *Onboardee* and *Employee* to distinguish new hires from employees.
> - **If Identity Authentication is enabled, will all the external users be using Identity Authentication for login by default, or can we select a set of users that have Identity Authentication enabled?**
>   All external users should use Identity Authentication for login.
> - **How do I check whether a new hire is enabled with Identity Authentication?**
>   - This can be done by checking whether the customer is using Identity Authentication as its identity provider. Go to the *Admin Center* > *Monitoring Tool for Identity Authentication Service/Identity Provisioning Service Upgrade* page.
>   - Check the *Initiated On* date.
>   - For **Preview** environments, if the date is from **November 29, 2022** then the customer is using the 2211 Enhanced ONB-IAS SCIM integration.
>   - For **Production** environments, if the date is from **December 9, 2022** then the customer is using the 2211 Enhanced ONB-IAS SCIM integration.

Related Information

Setting Up the Identity Provisioning Source and Target Systems [page 137]
Integration Service Registration Center
Generating X509 Certificates
Manage Identity Authentication/Identity Provisioning Real Time Sync

11.4 Configure Transformations in Identity Provisioning

While the default transformations work well when using password-based logins, you may want to further control how data is read and received in Identity Authentication by updating the Identity Provisioning transformations. You can edit transformations to **remove test/dummy emails**, define your **sendmail** settings and to define the **password status** attribute.

> ### Note
>
> If your bundle or standalone tenant is running on the **SAP BTP Neo environment**, we recommend that you migrate them to the **SAP Cloud Identity infrastructure**. Sharing the same infrastructure with Identity Authentication brings a number of benefits as described in Tenant Infrastructure.

When updating your transformations, review both the *Source* and *Target* transformations in the console. These transformation areas have different configurations that you can update. Select the application that matches your SAP SuccessFactors instance (Note, for customers with multiple SAP SuccessFactors Instances using the same Identity Authentication. Typically, you will only sync users from one SAP SuccessFactors instance to the Identity Authentication service . No need to import the same people multiple times). Select the *Transformations* button. This shows you how data gathered from SAP SuccessFactors is transformed while being read into Identity Provisioning service. Typical edits you might make to your source transformations include fixing blank/duplicate emails, setting passwords, setting groups.

Upgrade Center's Default Transformations for SAP SuccessFactors

> ### Note
>
> By default, Identity Provisioning provides default transformations for your SAP SuccessFactors **Source** and **Target** systems, however, these are **not** the same transformations that are provided by the SAP SuccessFactors Upgrade Center.
>
> Please utilize the transformations listed below that were created by the **Upgrade Center**, as these are the most current.

> ### Note
>
> To review the default transformations provided by Identity Provisioning, refer to Default Configuration for Identity Provisioning.

> ### Note
>
> If you've migrated to Identity Authentication **before** April 24th,2020, the transformations for your Source and Target systems are different. You can review the guide that describes how to configure these transformations on Identity Provisioning Transformations Before April 24th, 2020.

Default transformation for SAP SuccessFactors as the Source System created by the Upgrade Center - Workforce SCIM API.

> ### Code Syntax

```
{
    "user": {
```

```
        "mappings": [
            {
                "sourcePath": "$.schemas",
                "targetPath": "$.schemas",
                "preserveArrayWithSingleElement": true
            },
            {
                "sourcePath": "$.id",
                "targetVariable": "entityIdSourceSystem"
            },
            {
                "sourcePath": "$.userName",
                "targetPath": "$.userName",
                "correlationAttribute": true
            },
            {
                "sourcePath": "$.active",
                "targetPath": "$.active"
            },
            {
                "sourcePath": "$.userType",
                "targetPath": "$.userType"
            },
            {
                "sourcePath": "$.name.familyName",
                "targetPath": "$.name.familyName",
                "optional": true
            },
            {
                "sourcePath": "$.name.givenName",
                "targetPath": "$.name.givenName",
                "optional": true
            },
            {
                "sourcePath": "$.name.middleName",
                "targetPath": "$.name.middleName",
                "optional": true
            },
            {
                "sourcePath": "$.name.honorificPrefix",
                "targetPath": "$.name.honorificPrefix",
                "optional": true
            },
            {
                "sourcePath": "$.name.honorificSuffix",
                "targetPath": "$.name.honorificSuffix",
                "optional": true
            },
            {
                "sourcePath": "$.name.formatted",
                "targetPath": "$.name.formatted",
                "optional": true
            },
            {
                "sourcePath": "$.nickName",
                "targetPath": "$.nickName",
                "optional": true
            },
            {
                "sourcePath": "$.title",
                "targetPath": "$.title",
                "optional": true
            },
            {
                "sourcePath": "$.displayName",
                "targetPath": "$.displayName",
                "optional": true
            },
```

```
            {
                "sourcePath": "$.emails",
                "targetPath": "$.emails",
                "optional": true,
                "preserveArrayWithSingleElement": true
            },
            {
                "sourcePath": "$.emails[?(@.primary== true)].value",
                "optional": true,
                "correlationAttribute": true
            },
            {
                "sourcePath": "$.phoneNumbers",
                "targetPath": "$.phoneNumbers",
                "optional": true,
                "preserveArrayWithSingleElement": true
            },
            {
                "sourcePath": "$.preferredLanguage",
                "targetPath": "$.preferredLanguage",
                "optional": true
            },
            {
                "sourcePath": "$.locale",
                "targetPath": "$.locale",
                "optional": true
            },
            {
                "sourcePath": "$.timezone",
                "targetPath": "$.timezone",
                "optional": true
            },
            {
                "sourcePath": "$.externalId",
                "targetPath": "$.externalId",
                "optional": true
            },
            {
                "sourcePath": "$.groups",
                "targetPath": "$.groups",
                "optional": true,
                "preserveArrayWithSingleElement": true
            },
            {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['employeeNumber']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['employeeNumber']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['department']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['department']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['division']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['division']",
                "optional": true
            },
            {
```

```
"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",
                "optional": true
            },
            {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['displayName']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['displayName']",
                "optional": true
            },
            {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['$ref']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['$ref']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['userUuid']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['userUuid']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['groupDomains']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['groupDomains']",
                "optional": true,
                "preserveArrayWithSingleElement": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['perPersonUuid']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['perPersonUuid']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['personIdExternal']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['personIdExternal']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['loginMethod']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['loginMethod']",
                "optional": true
            },
```

```
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']['isDraft']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']['isDraft']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['customFields']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['customFields']",
                "optional": true
            },
            {
                "targetPath": "$
['urn:sap:cloud:scim:schemas:extension:sap.ips.sfsf.sac:2.0:User']
['hasEmbeddedAnalyticsPermission']",
                "constant": false
            },
            {
                "targetPath": "$
['urn:sap:cloud:scim:schemas:extension:sap.ips.sfsf.sac:2.0:User']
['hasEmbeddedAnalyticsPermission']",

"condition": "$['urn:ietf:params:scim:schemas:extension:sap:2.0:User']
['groupDomains'][?(@.value == 'embeddedAnalyticsAccessPermission')] empty false",
                "constant": true
            }
        ]
    },
    "group": {
        "ignore": true,
        "mappings": [
            {
                "sourcePath": "$.id",
                "targetPath": "$.id",
                "targetVariable": "entityIdSourceSystem"
            },
            {
                "sourcePath": "$.schemas",
                "targetPath": "$.schemas"
            },
            {
                "sourcePath": "$.displayName",
                "targetPath": "$.displayName"
            },
            {
                "sourcePath": "$.members",
                "targetPath": "$.members",
                "optional": true,
                "preserveArrayWithSingleElement": true
            }
        ]
    }
}
```

Default Transformation for Identity Authentication as the Target System created by the Upgrade Center - Identity Authentication SCIM API Version 1.

Code Syntax

```
{
    "user": {
```

```
        "condition": "($.emails EMPTY false) && ($.name.familyName EMPTY false)",
        "mappings": [
            {
                "targetPath": "$.id",
                "sourceVariable": "entityIdTargetSystem"
            },
            {
                "targetPath": "$.schemas[0]",
                "constant": "urn:ietf:params:scim:schemas:core:2.0:User"
            },
            {
                "targetPath": "$.schemas[1]",
                "constant":
"urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"
            },
            {
                "targetPath": "$.schemas[2]",
                "constant":
"urn:sap:cloud:scim:schemas:extension:custom:2.0:User"
            },
            {
                "sourcePath": "$.active",
                "targetPath": "$.active",
                "optional": true
            },
            {
                "sourcePath": "$.userName",
                "targetPath": "$.userName",
                "optional": true
            },
            {
                "sourcePath": "$.emails[*].value",
                "targetPath": "$.emails[?(@.value)]",
                "preserveArrayWithSingleElement": true
            },
            {
                "sourcePath": "$.userType",
                "targetPath": "$.userType",
                "optional": true
            },
            {
                "sourcePath": "$.name.givenName",
                "targetPath": "$.name.givenName",
                "optional": true
            },
            {
                "sourcePath": "$.name.middleName",
                "targetPath": "$.name.middleName",
                "optional": true
            },
            {
                "sourcePath": "$.name.familyName",
                "targetPath": "$.name.familyName"
            },
            {
                "sourcePath": "$.name.honorificPrefix",
                "targetPath": "$.name.honorificPrefix",
                "optional": true,
                "ignore": true
            },
            {
                "sourcePath": "$.addresses",
                "targetPath": "$.addresses",
                "optional": true,
                "preserveArrayWithSingleElement": true
            },
            {
                "sourcePath": "$.locale",
```

```
                "targetPath": "$.locale",
                "optional": true,
                "ignore": true
            },
            {
                "sourcePath": "$.phoneNumbers",
                "targetPath": "$.phoneNumbers",
                "optional": true,
                "preserveArrayWithSingleElement": true
            },
            {
                "sourcePath": "$.telephoneVerified",
                "targetPath": "$.telephoneVerified",
                "optional": true
            },
            {
                "sourcePath": "$.displayName",
                "targetPath": "$.displayName",
                "optional": true
            },
            {
                "sourcePath": "$.timezone",
                "targetPath": "$.timeZone",
                "optional": true
            },
            {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['employeeNumber']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['employeeNumber']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['costCenter']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['costCenter']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['organization']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['organization']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['division']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['division']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['department']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['department']",
                "optional": true,
                "ignore": true
            },
            {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",
```

```
"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",
                "optional": true,
                "functions": [
                    {
                        "function": "resolveEntityIds"
                    }
                ]
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['perPersonUuid']",

"targetPath": "$['urn:sap:cloud:scim:schemas:extension:custom:2.0:User']
['attributes'][0]['value']",
                "optional": true
            },
            {

"targetPath": "$['urn:sap:cloud:scim:schemas:extension:custom:2.0:User']
['attributes'][0]['name']",

"condition": "$['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['perPersonUuid'] EMPTY false",
                "constant": "customAttribute1"
            },
            {
                "targetPath": "$.applicationId",
                "constant": "%ias.application.id.attribute%",
                "scope": "createEntity"
            },
            {
                "targetPath": "$.sendMail",
                "constant": "false",
                "scope": "createEntity"
            },
            {
                "targetPath": "$.sendMail",
                "condition": "$.userType == 'ONBOARDEE'",
                "constant": "true",
                "scope": "createEntity"
            },
            {
                "targetPath": "$.emailTemplateSetId",
                "condition": "$.userType == 'ONBOARDEE'",
                "ignore": true,
                "constant": "%ias.onboardee.email.template.id.attribute%",
                "scope": "createEntity"
            },
            {
                "targetPath": "$.mailVerified",
                "constant": "true",
                "scope": "createEntity"
            },
            {
                "targetPath": "$.mailVerified",
                "condition": "$.userType == 'ONBOARDEE'",
                "constant": "false",
                "scope": "createEntity"
            },
            {
                "targetPath": "$.passwordStatus",
                "constant": "disabled",
                "scope": "createEntity"
            },
            {
```

```
                "targetPath": "$.passwordStatus",
                "condition": "$.userType == 'ONBOARDEE'",
                "constant": "enabled",
                "scope": "createEntity"
            },
            {
                "targetPath": "$.password",
                "ignore": true,
                "constant": "%ias.initial.password.attribute%",
                "scope": "createEntity"
            },
            {
                "targetPath": "$.sourceSystem",

"condition": "$['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['loginMethod'] == 'PWD'",
                "ignore": true,
                "constant": "%ias.source.system.attribute%",
                "scope": "createEntity"
            },
            {
                "targetPath": "$.sourceSystemId",

"condition": "$['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['loginMethod'] == 'PWD'",
                "ignore": true,
                "constant": "%ias.source.system.id.attribute%",
                "scope": "createEntity"
            }
        ]
    },
    "group": {
        "mappings": [
            {
                "targetPath": "$.id",
                "sourceVariable": "entityIdTargetSystem"
            },
            {
                "sourcePath": "$.displayName",
                "targetPath": "$.displayName"
            },
            {
                "sourcePath": "$.displayName",
                "targetPath": "$
['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']['name']",
                "scope": "createEntity",
                "functions": [
                    {
                        "function": "replaceAllString",
                        "regex": "[\\s\\p{Punct}]",
                        "replacement": "_"
                    }
                ]
            },
            {
                "sourcePath": "$
['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']['name']",
                "targetPath": "$
['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']['name']",
                "optional": true,
                "scope": "createEntity"
            },
            {
                "sourcePath": "$
['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']['description']",
                "targetPath": "$
['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']['description']",
                "optional": true
```

```
            },
            {
                "sourcePath": "$.members[*].value",
                "targetPath": "$.members[?(@.value)]",
                "optional": true,
                "preserveArrayWithSingleElement": true,
                "functions": [
                    {
                        "function": "resolveEntityIds"
                    }
                ]
            }
        ]
    }
}
```

> ### Note
>
> After editing your transformations, run an sync job in the Identity Provisioning service so that your changes are loaded into your integration.

11.4.1 Migrating Passwords from SAP SuccessFactors to Identity Authentication in SAP Cloud Identity Services

Configure password migration from your SAP SuccessFactors instance to your Identity Authentication tenant.

Prerequisites

- You've provisioned the users from SAP SuccessFactors to the Identity Authentication service.
- Users provisioned to Identity Authentication have the sourceSystem attribute with value 100, and the sourceSystemId with value equal to theIdentity Authentication SAP SuccessFactors company ID.
- Configure your IP address ranges for both your service and Identity Provisioning service. Find the IP address ranges listed in the **Setting Up an API User for Sync Jobs in SAP SuccessFactors** topic. See the Related Information section below.

Context

Configure your SAP SuccessFactors passwords (authentication provider) to integrate with the Identity Authentication service (target system) so that your users will not need to create new passwords once the integration is complete.

Procedure

1. Configure SAP SuccessFactors instance as a password authentication provider in your Identity Authentication tenant as it is described in the **Configure Authentication Provider To Migrate User Passwords from SAP SuccessFactors Systems to Identity Authentication** topic in the Related Information section below.

   → Remember

   When completing the configuration in **step 1** above, once you navigate to *SAP Cloud Identity Services* > *Identity Providers* > *Authentication Providers* > *Create* > *Configuration* >:

   - If you choose the X.509 certificate as your *Authentication Type*, make sure the *Password Validation URL* field contains **.cert** right after the subdomain part of the regular URL according to the following pattern: `https://api22preview.cert.sapf.com/odata/v2/restricted/validateUser`.
   - You'll also need to upload that certificate into SAP SuccessFactors to register Identity Authentication for incoming calls using X.509 certificate-based authentication. Refer to **Upgrade to X.509 Certificate-Based Authentication for Incoming Calls** for the steps to complete the upload.

2. Modify the Identity Provisioning configuration responsible for writing users in Identity Authentication. Go to > > *Target Systems (your* Identity Authentication > *target system configuration)* > *Transformations* tab. In the > *Users* > *Mappings* section, include the following elements to map the **`sourceSystemId`** (where the **`SFCompanyID`** is your instance company ID).

Options	Sample Code
If SCIM API Version 1 is in use in Identity Provisioning	Sample Code `{ "constant": "SFCompanyID", "targetPath": "$.sourceSystemId", "scope": "createEntity" }, { "constant": "100", "targetPath": "$.sourceSystem", "scope": "createEntity" }`

   You also need to update the following elements, so the users don't receive activation emails:

   Sample Code

```
{
    "constant": "enabled",
    "targetPath": "$.passwordStatus",
    "scope": "createEntity"
},
{
    "constant": "false",
    "targetPath": "$.sendMail",
    "scope": "createEntity"
```

Options	Sample Code

	<pre>},
	{
	"constant": "true",
	"targetPath": "$.mailVerified",
	"scope": "createEntity"
	},</pre>

If SCIM API Version 2 is in use in Identity Provisioning	Sample Code
	<pre>{
	"constant": "<SF_Company_ID>",
	"targetPath":
	"$['urn:ietf:params:scim:schemas:extension:sap:2.0:User']
	['sourceSystemId']",
	"scope": "createEntity",
	"ignore": false
	},
	{
	"constant": 100,
	"targetPath":
	"$['urn:ietf:params:scim:schemas:extension:sap:2.0:User']
	['sourceSystem']",
	"scope": "createEntity",
	"ignore": false
	},</pre>
	You also need to update the following elements, so the users don't receive activation emails:
	Sample Code
	<pre>{
	"constant": "enabled",
	"targetPath":
	"$['urn:ietf:params:scim:schemas:extension:sap:2.0:User']
	['passwordDetails']['status']"
	
	},
	{
	"constant": false,
	"targetPath": "$
	['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['sendMail']",
	"scope": "createEntity"
	},
	{
	"constant": true,
	"targetPath":
	"$['urn:ietf:params:scim:schemas:extension:sap:2.0:User']
	['mailVerified']",
	"scope": "createEntity"
	},</pre>

> **Note**
>
> - To determine the API version you are using, refer to Identity Provisioning Service in the Neo Environment - Identity Authentication.
> - For both examples above, if you have users that were already synced into Identity Authentication, you'll need to remove the **`"scope": "createEntity"`** transformation from beneath either the *"targetPath": "$.passwordStatus"* or *"targetPath": "$['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['passwordDetails']['status']"* elements (depending on which SCIM API Version you are using), and then run the **Read** job. Once the job is complete, you can then add **`"scope": "createEntity"`** back to the respective password mapping. This ensures that on the next provisioning jobs, Identity Provisioning will always update the password status of your users, even if they get locked in Identity Authentication. It also ensures that the migrated passwords will be set first in Identity Authentication when a user logs in for the first time to one of their assigned applications (ex. *SAP SuccessFactors* or *User Profile*). For more information refer to Passwords are Migrated from SAP SuccessFactors.

Related Information

External Authentication Providers

Configure Authentication Provider To Migrate User Passwords from SAP SuccessFactors Systems to Identity Authentication

Setting Up an API User for Sync Jobs in SAP SuccessFactors

Upgrade to X.509 Certificate-Based Authentication for Incoming Calls [page 36]

List of SAP SuccessFactors API Servers

11.4.2 Remove Dummy Emails Transformation

If you have users with duplicated dummy emails, you need to implement the below transformation change to be able to sync those users.

Context

The following code sets email addresses to `username + @sap-test.de`. This guarantees that the email is unique. You are not required to use **sap-test .de**. However, we encourage you to use **sap-test.de**. This test email address does not route to an actual email server. If you use your own email domain, the server will need to reject all the emails.

Procedure

1. Navigate to *Identity Provisioining Administration Console* > *Target Systems* .
2. Select the target system for the Identity Authentication service that your SAP SuccessFactors instance is integrated with.
3. Click on the *Transformations* tab.
4. Find the code block that contains the code below:

   Sample Code

   ```
   {
                   "sourcePath": "$.email",
                   "targetPath": "$.emails[0].value"
               },
   ```

5. Add the dummy email transformation code below **underneath** the above email transformation:

   Note

   The following code below looks for emails in the format **no-email@test.com**. Replace this email with your own dummy email addresses. You can add multiple conditions by using the || (OR) operator.

   Sample Code

   ```
   {
                   "condition": "($.email == 'no-email@test.com')",
                   "sourcePath": "$.personKeyNav.userAccountNav.username",
                   "targetPath": "$.emails[0].value",
                   "functions": [
                       {
                           "type": "concatString",
                           "suffix": "@sap-test.de"
                       }
                   ]
               },
   ```

11.4.3 Define `SendMail` Transformation

Enable the `SendMail` transformation code if you want users receive email notifications when they're created in Identity Authentication.

Enter the following code on the *Identity Provisioning Administration Console* > *Target Systems* > *Your Identity Authentication Target System* > *Transformations* tab.

Sample Code

```
               "constant": "true",
                 "targetPath": "$.sendMail",
                 "scope": "createEntity"
```

Setting to false prevents the emails from being sent.

Sample Code

```
            "constant": "false",
               "targetPath": "$.sendMail",
               "scope": "createEntity"
```

11.4.4 Define `PasswordStatus` Transformation

When users first log in with their username and password, when enabled, the Identity Authentication Service does a one-time verification that the password entered matches the existing SAP SuccessFactors Password.

Enter the following code on the *Identity Provisioning Administration Console* > *Target Systems* > *Your Identity Authentication Target System* > *Transformations* tab.

Sample Code

```
             "constant": "enabled",
               "targetPath": "$.passwordStatus",
               "scope": "createEntity"
```

Set to disabled if your users are receiving welcome emails and resetting their passwords before first login.

Sample Code

```
            "constant": "disabled",
               "targetPath": "$.passwordStatus",
               "scope": "createEntity"
```

11.4.5 Define `PreferredLanguage` Transformation

Use the `PreferredLanguage` transformation code if you want to set the language to be used for the activation email you send to your users.

You can use the following transformation configuration to set the preferred language in the *Identity Provisioning Administration Console* > *Source Systems* > *Select your Source System* > *Transformations*.

Sample Code

Example

If you want to transfer the value from your SAP SuccessFactors system, add the following code in the `User` and `Mappings` section:

Sample Code

```
{
            "sourcePath": "$.preferredLanguage",
            "optional": true,
            "targetPath": "$.locale"
        },
```

Example

Setting the constant to a specific locale is useful if all your activation emails are for only one language. (See the link below for details on all supported locales.) If you want to set a constant value for all users, add the following code in the `User` and `Mappings` section:

Sample Code

```
{
            "constant": "es_ES",
            "targetPath": "$.locale"
        }
```

Remember

Unless you define another default locale for your company, U.S. English is the default locale for all users. If no translation is present, text appears in the company's default locale. Refer to the Related Information link below for the SAP SuccessFactors Languages and Locales topic in the *Managing Languages and UI Labels* guide.

Related Information

SAP SuccessFactors Languages and Locales
Configuring E-Mail Templates

11.4.6 Set Up Default Passwords Using Transformations

We recommend that you choose one of the recommended options for assigning an initial password:

- **Option 1**: You can use the password that's initially set up during the user sync in the Identity Provisioning service
- **Option 2**: You can use the SAP SuccessFactors user attribute value as a password
- **Option 3**: You can set an initial password by combining last name with an internal userID, something that only the employee aware of.

Password Set to an SAP SuccessFactors User Attribute

You can use the following transformation configuration to set the initial password to the SAP SuccessFactors Employee ID attribute under *SAP Cloud Identity Services* > *Identity Provisioning* > *Source Systems* > *(select your SAP SuccessFactors source system)* > *Transformations* > *Switch to JSON Editor(icon)* > *Edit*.

Note

To perform this operation when the **OData API** is in use in Identity Provisioning, use the elements below:

Sample Code

Example

In the *user* > *mappings* section of the JSON, add the following code:

Sample Code

```
{
 "sourcePath": "$.empId",
 "targetPath": "$['urn:sap:cloud:scim:schemas:extension:sfsf:2.0:User']
['empId']"
}
```

Sample Code

Example

In *Target Systems* > *(your Identity Authentication target system)* > *Switch to JSON Editor (icon)* > *Edit*, under the *user* > *mappings* section of the JSON, add the following code:

```
{
 "constant": "false",
 "targetPath": "$.sendMail",
 "scope": "createEntity"
 },
 {
  "constant": "true",
  "targetPath": "$.mailVerified",
  "scope": "createEntity"
 },
 {
  "constant": "initial",
  "targetPath": "$.passwordStatus",
  "scope": "createEntity"
 }
```

```
 {
  "sourcePath": "$['urn:sap:cloud:scim:schemas:extension:sfsf:2.0:User']
['empId']",
  "targetPath": "$.password",
  "scope": "createEntity"
 }
```

→ Tip

You can use a different SAP SuccessFactors user attribute by changing the attribute name **`empId`** to the name of the attribute that you want to use but you must use the name of the attribute as it's defined in the SAP SuccessFactors OData API or Workforce SCIM API, depending on which one you are using. Additionally, ensure that this attribute is part of the list in *sf.user.attributes* property.

To determine the API version you are using, check the *sf.api.version* parameter in the *Identity Provisioning* > *Source Systems* > *Properties* tab. Based on the parameter value:

- *1* = OData API
- *2* = SCIM API

Note

To perform this operation when the **SCIM API** is in use in Identity Provisioning, use the elements below:

Sample Code

In *Source Systems* > *(your SAP SuccessFactors source system)* > *Transformations* > *Switch to JSON Editor (icon)* > *Edit*, under the *user* > *mappings* section of the JSON, add the following code:

```
{
 "sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['employeeNumber']",
 "targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['employeeNumber']"
}
```

Sample Code

In *Target Systems* > *(your Identity Authentication target system)* > *Transformations* > *Switch to JSON Editor (icon)* > *Edit*, under the *user* > *mappings* section, add the following code:

```
{
 "constant": "false",
 "targetPath": "$.sendMail",
 "scope": "createEntity"
},
{
 "constant": "true",
 "targetPath": "$.mailVerified",
 "scope": "createEntity"
 },
 {
   "constant": "initial",
   "targetPath": "$.passwordStatus",
   "scope": "createEntity"
 },

 {
   "sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['employeeNumber']",
   "targetPath": "$.password",
   "scope": "createEntity"
 }
```

Password Set by Combining SAP SuccessFactors User Attributes

You can configure the Identity Provisioning transformation to set the user's initial password by combining multiple SAP SuccessFactors user attributes, such as their last name and employee number. This method increases password uniqueness and lowers the risk of using easily guessed passwords.

Before you begin, ensure that the attributes you want to use (for example, familyName and employeeNumber) are included in the *sf.user.attributes* property of your source system configuration.

The following example demonstrates how to create an initial password by concatenating the user's last name and employee number.

Example

In *Target Systems* > *(your Identity Authentication target system)* > *Transformations* > *Switch to JSON Editor (icon)* > *Edit*, under the *user* > *mappings* section of the JSON, add the following code:

Note

To perform this operation when the **OData API** is in use in Identity Provisioning, use the elements below:

Sample Code

```
{
  "sourcePath": "$.empId",
  "targetVariable": "employeeId"
},
{
  "sourcePath": "$.lastName",
  "targetPath": "$.password",
  "functions": [
    {
      "type": "concatString",
      "suffix": "${employeeId}"
    }
  ],
  "scope": "createEntity"
}
```

Note

To perform this operation when the **SCIM API** is in use in Identity Provisioning, use the elements below:

Sample Code

```
{
  "sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['employeeNumber']",
  "targetVariable": "empNum"
},
{
  "sourcePath": "$.name.familyName",
  "targetPath": "$.password",
  "functions": [
    {
      "type": "concatString",
```

```
      "suffix": "${empNum}"
    }
  ],
  "scope": "createEntity"
}
```

11.4.7 Instance Migration with SSO Login for Corporate Users

Migrate an SAP SuccessFactors Instance where SSO is configured with SAML-based Corporate Identity Provider (IDP).

After migration, users who log in using SSO will be redirected through the SAP Cloud Identity Services - Identity Authentication service tenant to the Corporate IDP to have the same user experience. If there are also password-based log in users (Partial SSO is enabled), they'll start using the Identity Authentication tenant for authentication.

Using the new Identity Authentication solution integrated with SAP SuccessFactors application you can configure delegated authentication to an existing Corporate Identity Provider (using SAML proxy approach). In doing this, the user accesses the SAP SuccessFactors application and will be redirected through the Identity Authentication service to the Corporate IDP, which will provide SSO authentication. Using this method allows you to keep your current user experience but allows you to also benefit from the advanced security features provided by Identity Authentication service, such as 2-factor authentication. Concurrently, you can use the Identity Authentication service tenant for authentication of users that are currently using password-based logins and are **not** part of the corporate environment, such as for partners, third parties, and consultants. In addition, you can configure Risk-Based authentication rules in Identity Authentication, so that under different conditions, access to the SAP SuccessFactors application could be denied, or second factor of authentication could be requested.

11.4.7.1 Pure SSO Scenario with One Corporate Identity Provider

Setup IPS Transformation rules for the scenario in which your Identity Authentication service tenant is integrated with only one Corporate Identity Provider (IdP) and SuccessFactors is only accessed through the IdP.

Prerequisites

Establishing a trust between the Corporate Identity Provider (IdP) and your Identity Authentication service tenant is a separate step that you need to complete. Refer to **Configure Trust with Corporate Identity Provider** in the **Related Information** section.

Procedure

1. In the Identity Provisioning configuration responsible for writing users in Identity Authentication, ensure that the transformation rules follow the sample below. Go to the *Identity Provisioning Administration* > *Target Systems (your Identity Authentication target system configuration)* > *Transformations* tab.
2. In the *Users* > *Mappings* section, make sure the transformation follows the pattern below, to have `sendMail` as **false** so that emails are not sent when users are created.

Sample Code

```
{
       "constant": "false",
       "targetPath": "$.sendMail",
       "scope": "createEntity"
      },
      {
       "constant": "true",
       "targetPath": "$.mailVerified",
       "scope": "createEntity"
      }
```

Related Information

Configure Trust with Corporate Identity Provider

11.4.7.2 Partial Single Sign-On (SSO) Login Using a Single Corporate Identity Provider (IdP)

Migrate your SAP SuccessFactors instance when some of your users have SSO-based login and you have external users with SAP SuccessFactors credentials for application access.

At this final step, you should have delegated authentication configured to your Corporate Identity Provider (IdP) for the SSO-based login users (Corporate Users). While your password-based login users (External Users) use the Identity Authentication service tenant for authentication. You have two options to configure this setup:

Option A: Define the Corporate Identity Provider as Default Authentication IdP for the SAP SuccessFactors Application

Option B: Conditional Authentication for Partial SSO Scenarios

As prerequisite for both options you should have established SAML trust between the Identity Authentication tenant and the Corporate IDP.

Option A: Define the Corporate Identity Provider as Default Authentication IdP for the SAP SuccessFactors Application

Using this option, your corporate users can use the SAP SuccessFactors application URL to access the instance. They're redirected automatically through Identity Authentication to the Corporate IdP. In addition, your external users can use a special link to Identity Authentication (for IdP-Initiated authentication flow) to log in with Identity Authentication credentials and to be redirected to the SAP SuccessFactors application.

Refer to the KBA for details on this option. 2954556

Option B: Set Up Conditional Authentication for Partial SSO with Identity Authentication Service as the Default Identity Provider (IdP)

When you upgrade to Identity Authentication, the flag for partial SSO is disabled, by default. You can use partial SSO by sending users in your system through the Identity Authentication Service.

1. Log on to your Identity Authentication console as an Identity Authentication Admin.
2. Select *Applications & Resources* > *Applications*.
3. Choose your SAP SuccessFactors application.
4. Choose *Conditional Authentication*.
5. Select *Allow users stored in Identity Authentication service to log on* in the *Allow Identity Authentication Users Log On* area.
6. Choose *Save*.
   The setting only appears if, by default you have the Identity Provider SSO set up, if you don't have SSO, you do not need this feature.
   If you are using Authentication Rules, you selected Identity Authentication as the *Default Authenticating Identity Provider* and you must change the *Default Authenticating Identity Provider* your SSO. After you've done this, the section *Allow Identity Authentication Users Log* displays.
7. Choose *Save*.
8. Copy the URL below the checkbox and provide that for your non-SSO users to log in.
   The URL looks similar to the following: **`https://<Identity Authentication tenant URL>/saml2/idp/sso?sp=<SF entity ID>&idp=https://<Identity Authentication tenant URL>`**.
9. If on Step 5, you changed the *Default Authenticating Identity Provider* to your SSO, you can change back and the URL will still work.

Related Information

Choose Default Identity Provider for an Application

11.4.8 Group Users Based on Login Method

Using this option, all users (corporate and external) can use the SAP SuccessFactors application URL to access the instance and based on conditional authentication rules some of them (corporate users) will be redirected to the Corporate IDP and others (externals) will authenticate in Identity Authentication with username and password.

Perform the following steps to configure this:

1. Configure in Identity Authentication conditional authentication rules for the SAP SuccessFactors application based on user group, user type or IP-range.
2. (optional) If you wish to use rules, based on user group or user type, modify the Identity Provisioning transformations to ensure that the corporate and external users can have been assigned different user groups or user types.

To differentiate the users in the Identity Provisioning transformation you can use SAP SuccessFactors user attributes, such as *loginMethod* user but you must first ensure that this attribute can be used in the Identity Authentication Target system configuration.

During user provisioning, you can assign different user types as listed:

> → Tip
>
> You can use a different SAP SuccessFactors user attribute by changing the attribute name **`empId`** to the name of the attribute that you want to use but you must use the name of the attribute as it's defined in the SAP SuccessFactors OData API or SCIM API, depending on which one you are using. Additionally, ensure that this attribute is part of the list in *sf.user.attributes* property.

The default Target SAP SuccessFactors system configuration in Identity Provisioning defines that all users are of type *employee* using the following element:

> {·} Sample Code

```
{
          "constant": "employee",
          "targetPath": "$.userType"
        },
```

The following element can be added after the default one in order to overwrite the user type if the *loginMethod* of the user is PWD:

> ⓘ Note
>
> The below elements will only work when the **Identity Authentication SCIM API Version 1** is in use in Identity Provisioning. They will **not** work when the **Identity Authentication SCIM API Version 2** is in use.
>
> To assign user groups when the **Identity Authentication SCIM API Version 2** is in use, refer to Enabling Group Assignment.
>
> To determine the API version you are using, refer to Identity Provisioning Service in the Neo Environment-Identity Authentication.

> {·} Sample Code

```
{
  "condition": "$.personKeyNav.userAccountNav.loginMethod =='PWD'",
```

```
  "constant": "partner",
  "targetPath": "$.userType"
},
```

External and Internal users can be assigned to an Identity Authentication user group, which can be used for conditional authentication rules.

> ⓘ Note
>
> The user group should exist already in the Identity Authentication tenant.

With the following element added in the Identity Authentication Target system configuration in Identity Provisioning, you will have assigned all users with *loginMethod* - **`PWD`** to a dedicated *Display Name* group in Identity Authentication:

> → Remember
>
> Make sure that the **constant** value matches the group *Display Name* that you've created in *SAP Cloud Identity Services* > *Groups* > *Display Name*. The group ID must **not** be used as the value. The example below is what would be entered if the group Display Name was **Password Login Users**.

> {·} Sample Code

```
{
                "condition": "$
['urn:sap:cloud:scim:schemas:extension:sfsf:2.0:User']['loginMethod'] == 'PWD'",
                "constant": "Password Login Users",
                "targetPath": "$.groups[0].value"
                },
```

11.4.9 Change the Redirect URL for Password Users in Identity Authentication Service

You can change the redirect URL for your users when you update the transformation code in your SAP Cloud Identity Services - Identity Provisioning service.

By default, user provisioning, in the Identity Provisioning service, replicates all SAP SuccessFactors active users in your system. For new users, who are created in SAP SuccessFactors, you must also create them in the Identity Authentication service so that they receive the activation email that will allow them to set a password and to access the SAP SuccessFactors application. With the default configurations to your Identity Provisioning service, any newly created users are redirected to the Identity Authentication service's User Profile page after they activate their account and reset their password. This URL, `https://<customer-tenant-id>.accounts.ondemand.com`, can be customized by adding the following code to your Identity Provisioning's Target System's Transformation.

Identity Provisioning Administration > *Target Systems* > *{your Identity Authentication target system configuration}* > *Transformations* > *User Mappings*

In the *Users* > *Mappings* section, include the following element if you are using the Identity Authentication API Version 1:

Sample Code

```
            {
            "constant": "https://custom.domain.net/landing_page",
            "targetPath": "$.targetUrl",
            "scope": "createEntity"
          }
```

For Identity Authentication API Version 2:

Sample Code

```
                  {
                    "constant": " https://custom.domain.net/landing_page",
                 "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['targetUrl']",
                 "scope": "createEntity"
                  }
```

In addition to updating the transformation, ensure that the following attributes contain the following values:

- `Target Transformations, $.sendMail attribute` = **`True`**
- `Target Transformations, $.mailVerified attribute` = **`False`**
- **Remove** from the Identity Authentication Target System Transformations: `$.passwordStatus attribute`
- Ensure that you add the target URL as a trusted domain in the Identity Authentication Administration console. For more information, review the topic **Configure Trusted Domains**, linked in the Related Information section.

Related Information

Configure Trusted Domains

11.5 SAP Cloud Identity Services Administration Console Tasks

The Identity Authentication service in SAP Cloud Identity Services provides you with secure authentication and single sign-on for users in the cloud.

Identity Authentication provides you with simple and secure cloud-based access to business processes, applications, and data. It simplifies your user experience through state-of-the-art authentication mechanisms, secure single sign-on, on-premise integration, and convenient self-service options. The Identity Authentication service functions as both a Service Provider (a resource a user is logging in to) and as an Identity Provider (an Identity Management tool that can authenticate a user and send a logon to a Service Provider).

Note

If your Identity Authentication tenant was created before December 9, 2022, we **highly** recommend that you first upgrade to Mutual Transport Layer Security (mTLS) authentication between Identity Authentication

and SAP SuccessFactors before completing any console tasks, as this is our most secure method of authentication.. As the Identity Authentication Administrator, an email is sent to you with a link to log on to the administration console.

To complete this upgrade, refer to Upgrade to X.509 Certificate-Based Authentication for Incoming Calls

The Identity Authentication service Administrator system is created when you initiate the upgrade process in the SAP SuccessFactors *Upgrade Center*

> ⚠ Caution
>
> If you haven't received an email with a link to your Identity Provisioning system within approximately two hours, contact Technical Support.

> ⓘ Note
>
> In the Identity Authentication *Applications* configuration, there is a setting to choose *Signing Options* within the *SAML 2.0 Configuration*. After our 1H 2021 Production Release, SHA-256 will be selected as the signing mechanism for SAP SuccessFactors HCM suite, Story Reports, and Internal Career Site applications for better security. Please **don't** change the setting back to SHA-1. This change will get rolled out in a phased manner, on your behalf, after the 1H 2021 Production Release.

What to Configure in the Identity Authentication Console

The Identity Authentication service gives you access to the following login methods. Configuring these login methods are optional and depends on how you want your users to log into their SAP SuccessFactors systems.

Optional Task	Description	Documentation
Configure password policy settings.	If the default standard password policy doesn't meet your requirements, you can: • Change to the Enterprise password policy. • Create a custom password policy. For users of two-factor authentication, these password policy settings are still used. For users of single sign-on (SSO) or other nonpassword logon options (like social sign-on), these password policy settings are ignored.	About Password Policies in the Identity Authentication service

Optional Task	Description	Documentation
Set up single sign-on (SSO).	If you want some or all users to access your system using single sign-on (SSO), you need to set it up. You need to: • Set up trust between the Identity Authentication service and your corporate identity providers. • Set up conditional and/or risk-based authentication rules to determine which users are sent to single sign-on.	Process to Set Up Single Sign-On with Identity Authentication [page 119]
Create user groups	If needed, you can set up authentication filtering so that different groups of users are authenticated differently. Create user groups so that you can apply different authentication rules for each group. User groups can be assigned manually or during the user sync with Identity Provisioning service.	About User Groups in the Identity Authentication service
Configure conditional authentication	By default, conditional authentication is configured to send all users to Identity Authentication-based logon. To set up single sign-on, you need to configure conditional authentication rules to send users to your corporate identity provider (IdP).	About Conditional Authentication in the Identity Authentication service
Configure risk-based authentication	By default, risk-based authentication is configured to send all users with Identity Authentication-based logon to username/password logon. You can also configure risk-based authentication rules to send users to two-factor authentication.	About Risk-Based Authentication in the Identity Authentication service
Enable two-factor authentication	If needed, you can choose to enable two-factor authentication as part of your password-based logins.	About Two-Factor Authentication in Identity Authentication service
Configure email templates	You can change the default email templates used to generate email notifications for events such as new users or password reset.	About Email Notification Templates in Identity Authentication service

Optional Task	Description	Documentation
Branding and theming	You can change the default colors and theming used on Identity Authentication pages such as the logon and password reset pages.	About Branding in Identity Authentication

Related Information

Configure the Corporate Identity Provider
Maintaining Conditional Authentication (Video)
Maintaining Risk-Based Authentication (Video)

11.5.1 Adding Users to the SAP Cloud Identity Services - Identity Authentication Service

As a tenant administrator, you can create a new user in the administration console for Identity Authentication service.

Prerequisites

You're authorized as an admin with the *Manage Users* access in the *Identity Authentication Service*.

> **Note**
>
> Typically, you'll use the sync job in the Identity Provisioning Administration Console to add users to the system but you can add individual users to the Identity Authentication Service as well.

Procedure

1. Log on to the *Identity Authentication Service* using the link from your registration email.
2. Select *User Management*
3. Select *Add User*.
4. Enter *First Name*, *Last Name*, and *Email Address*.
5. Enter *Login Name*. This log on name must match the exact username of the user in the SAP SuccessFactors, including case, unless *Non Case Sensitive Usernames* is selected in the *Admin Center* > *Manage SAML SSO Settings* page.

6. Select the *Employee* as the *User Type*.
7. Select one of the following options:

Option	Description
Send activation e-mail	The user receives an e-mail with instructions how to activate the user account.
Set initial password	The tenant administrator sets the password for the user. **Note** The user is prompted to reset the password during the first authentication.

8. Save the changes.

Results

The new admin can access the SAP SuccessFactors instance using Identity Authentication service.

11.5.2 Creating User Groups in Identity Authentication (Video)

As a tenant administrator, optionally, you can create new user groups in the tenant using the administration console for *Identity Authentication Service*. You may want to do this if you intend to use multiple methods of authentication for your users.

Prerequisites

Your user is authorized with the *Manage Groups* access in the *Identity Authentication Service*.

Context

You may want to create groups and assign users according to the logon method you want each group to use.

Watch the video to learn how and when to create user groups in Identity Authentication.

Open this video in a new window

Procedure

1. Log on to the *Identity Authentication Service*.
2. Select *Users & Management* > *User Groups*.
3. Select *Add*.
4. Enter *Name*, *Display Name*, and *Description*.
5. Choose *Save*.
6. Manually add a user to one or more groups by selecting *User Management*.
7. Select a user.

   While you can add users to your groups individually, you can add users in bulk using Identity Provisioning Transformations.
8. Select *User Groups*.
9. Choose *Assign Groups*.
10. Select the groups you want to add the user to.
11. Save your changes.

Related Information

Edit Administrator Authorizations
Create a New User Group

11.5.3 Configure Password Based Logins (Video)

All SAP Cloud Identity Services - Identity Authentication instances are preconfigured with password-based logins by default. If you intend to use password or two-factor logins, review and update your password policy settings.

If the default standard password policy doesn't meet your requirements, you can:

- Change to the enterprise password policy.
- Create a custom password policy.

These settings also apply to two-factor authentication logins.

> **Note**
>
> If your organization uses single sign-on (SSO) or other nonpassword logon options, such as social sign-on, these password policy settings are ignored.

Watch the video to learn how to configure password policies.

Open this video in a new window

Related Information

Configuring Password Policies

11.5.4 Configure Two-Factor Authentication

You can set up two-factor authentication if you intend to use multiple layers of authentication for your users.

If you intend to use two-factor authentication, setup password policies and additional two-factor settings. You'll need to sort your users using risk-based authentication and to register their token generator. We support SAP Authenticator, Google Authenticator, and other apps that follow the same standard.

Related Information

About Two-Factor Authentication in Identity Authentication service
About Risk-Based Authentication in the Identity Authentication service
About setting up SAP Authenticator on your phone

11.5.5 Process to Set Up Single Sign-On with Identity Authentication

Learn what you need to do to set up single sign-on (SSO) for your SAP SuccessFactors system so that it uses the SAP Cloud Identity Services - Identity Authentication service.

Setting up single sign-on is a multistep process:

1. **Configure your corporate identity provider (IdP).**
   Work with the administrator of your IdP to make the required configurations, using metadata downloaded on the SAP SuccessFactors *SAML 2.0 Single Sign On* page.
2. **Add asserting parties in SAP SuccessFactors.**
   Add your corporate identity provider (IdP) in SAP SuccessFactors as an asserting party to the Identity Authentication service. You can use the SAP SuccessFactors *SAML 2.0 Single Sign On* page or configure it directly in the Identity Authentication administration console.
3. **Configure user groups and authentication rules.**
   Authentication rules determine which user groups use single-sign on and are configured directly in the Identity Authentication administration console.

Related Information

Configure IdP-Initiated SSO

11.5.5.1 Configuring the Corporate Identity Provider in the Identity Authentication service (Video)

Setting up your corporate IDP in SAP Cloud Identity Services - Identity Authentication service requires that you create a link to your corporate IDP. When you create the IDP, you must also and upload your metadata file so that the metadata exchange occurs between the SAP SuccessFactors Identity Authentication and the company IDP.

Prerequisites

You've received the customer metadata file from your company's Corporate IDP team.

Context

Watch the video or follow the procedure to configure third party Corporate IDP.

Open this video in a new window

Procedure

1. Log on to the *Identity Authentication Service* using the link from your registration email.
2. Go to *Identity Providers*.
3. Go to *Corporate Identity Providers*.
4. Choose + *Add*.
5. Provide a unique name for your corporate IDP and save your changes.
6. Choose *SAML 2.0 Configuration*.
7. Browse for the metadata from your corporate IDP.

   You should have received the metadata file from your company's corporate identity team.
8. Import the metadata.
9. Select the *SAML 2.0 Compliant* as your identity provider type by clicking *Identity Provider Type* from your *Identity Provider* screen.

   If your provider is ADFS or Azure AD, select *Microsoft ADFS/Azure AD*.
10. Save your changes.

Results

When you've uploaded your metadata file, the fields for *Name* (Issuer), *Single Logout Endpoint* , and *Certificate* are automatically populated.

11.5.5.1.1 Downloading and Exporting the Identity Authentication Service Metadata File

The metadata file that you upload should be given to your company's corporate identity provider (IdP) team in order to complete your Identity Authentication setup process.

Procedure

1. Log on to the *Identity Authentication* service using the link from your registration email.
2. Go to *Applications and Resources*.
3. Go to *Tenant Settings*.
4. Go to *SAML 2.0 Configuration*.
5. Select *Download MetaData File* and save the file.

   > ⓘ Note
   >
   > Download the metadata twice, once using the **.ondemand.com** domain and once using the **.cloud.sap** domain. To get the second file, change the domain in your browser to **.cloud.sap** and log in again.
   > Verify which domain your SAP SuccessFactors integration is using, and if your corporate identity provider supports it, add the **Assertion Consumer Service (ACS) URLs** from both metadata files into the IdP configuration to ensure a reliable connection.

6. Give this file(s) to your corporate identity provider team so that they can import it into your corporate identity provider. This enables a connection to your Identity Authentication service.
7. Set up the Identity Provider to send: Name ID Format Unspecified

   > ⓘ Note
   >
   > The value in the Name ID should match the SAP SuccessFactors Username.

11.5.6 Implementing Single Sign-On After Upgrading

When you upgrade to Identity Authentication, the flag for partial SSO is disabled, by default. You can use partial SSO by sending users in your system through the Identity Authentication Service.

Context

Procedure

1. Log on to your Identity Authentication console as an Identity Authentication Admin.
2. Select *Applications & Resources* > *Applications*.
3. Choose your SAP SuccessFactors application.
4. Choose *Conditional Authentication*.
5. Select *Allow users stored in Identity Authentication service to log on* in the *Allow Identity Authentication Users Log On* area.
6. Choose *Save*.

   The setting only appears if, by default you have the Identity Provider (SSO) set up, if you don't have Single Sign-on, you do not need this feature.

   If you are using Authentication Rules, you selected Identity Authentication as the *Default Authenticating Identity Provider* and you must change the *Default Authenticating Identity Provider* your SSO. After you've done this, the section *Allow Identity Authentication Users Log* displays.
7. Choose *Save*.
8. Copy the URL below the checkbox and provide that for your non-SSO users to log in.

   The URL look similar to the following: **`https://<Identity Authentication tenant URL>/saml2/idp/sso?sp=<SF entity ID>&idp=https://<Identity Authentication tenant URL>`**
9. If on step 5, you changed the *Default Authenticating Identity Provider* to your SSO, you can change back and the URL will still work.

11.6 Public API to Retrieve Customer SSO Service Provider Metadata

The SSO SAML signing certificate provided by SAP SuccessFactors HCM suite to other applications such as IDPs like Identity Authentication is due to expire on June 2, 2025. The SAP SuccessFactors HCM suite public API allows applications to retrieve the SAML Service Provider metadata for their company which also includes the renewed signing certifcate. When certificate expiration is detected, the API is called by the client to get the new certificate and update the SAML setting in the application.

GET SAML Service Provider Metadata

Retrieve Service Provider Metadata by company ID.

Request

Operation	Query
HTTP Method	GET
URI	`https://<SF Customer Facing Host>/saml2/spmetadata?company=<company_id>`

Response

Sample Code

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" entityID="https://
www.successfactors.com/<company_id>">
<md:SPSSODescriptor AuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIICDTCCAXagAwIBAgIETAl/
KDANBgkqhkiG9w0BAQUFADBLMQswCQYDVQQGEwJVUzEbMBkGA1UEChMSU3VjY2Vzc2ZhY3RvcnMuY29tM
QwwCgYDVQQLEwNPcHMxETAPBgNVBAMTCFNGIEFkbWluMB4XDTEwMDYwNDIyMzMxMloXDTI1MDYwMjIyMz
MxMlowSzELMAkGA1UEBhMCVVMxGzAZBgNVBAoTElN1Y2Nlc3NmYWN0b3JzLmNvbTEMMAoGA1UECxMDT3B
zMREwDwYDVQQDEwhTRiBBZG1pbjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAkS3xlwL9v/
5kHmfnW0fy2JzIDvHKK4TmkZYHN+JHBLRRzNtlGo1f4yUseMjVn4RF1W11uEqnBySokXv5FYoPd1guJ1X
t3u2Xnj52l/
lG4S7ichsPwF3ddDk+pWbKF29Ixt0iBN+keknSRyNGdh9jtOekCg6xq4i4YndwKCucABUCAwEAATANBgk
qhkiG9w0BAQUFAAOBgQBzhTmtBbnXpT1aTWDa3PRUx8fWTx/
oPjL7xP+WeoTJZmeY4N1c6Q3aZ+u+MhxvmhyDTGo43pyyFVBQjiFzrZUEAAPUrLr7M0e4kGULhxE1p2jn
BNfzmVYK397+QPHD2kN/BIzVcMBFsrS+fpdDGWnzj1hjuGLNO/XuPO9eSBRkZA==</
ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://hcm68sales.successfactors.com/saml2/LogoutServiceHTTPRedirect?
company=<company_id>&amp;RelayState=sf" ResponseLocation="https://
hcm68sales.successfactors.com/saml2/LogoutServiceHTTPRedirectResponse?
company=<company_id>"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST" Location="https://hcm68sales.successfactors.com/saml2/
SAMLAssertionConsumer?company=<company_id>" index="0" isDefault="true"/>
</md:SPSSODescriptor>
<md:Organization>
<md:OrganizationName xml:lang="en">SuccessFactors</md:OrganizationName>
<md:OrganizationURL xml:lang="en">https://www.successfactors.com</
md:OrganizationURL>
</md:Organization>
</md:EntityDescriptor>
```

Note

- No authentication is needed for this API request.
- The API will return the SPMetaData, with the **company schema metadata URL** in the Single Log Out (SLO) and Assertion Consumer Services (ACS) fields.

- If the company has reverse proxy enabled in *Provisioning* > *Company Settings*, the API will return the SPMetaData with the reverse proxy URL in the Single Log Out (SLO) and Assertion Consumer Services (ACS) fields.

→ Remember

After you've renewed your SSO signing certificate, go to the *Admin Center* > *Manage SAML SSO Settings* page and select the *SSO Certificate Renewed* checkbox to record your certificate renewal in the SAP SuccessFactors HCM suite.

11.7 Public API to Retrieve New Customer SSO Certificate

The SSO SAML signing certificate provided by SAP SuccessFactors HCM suite to other applications such as IDPs like Identity Authentication is due to expire on June 2, 2025. The SAP SuccessFactors HCM suite public API allows applications to retrieve the renewed signing certifcate, without the additional SAML metadata. When certificate expiration is detected, the API is called by the client to get the new certificate and update the SAML setting in the application.

GET New Customer SSO Certificate

Retrieve a new customer SSO certificate by company ID.

Request

Operation	Query
HTTP Method	GET
URI	`https://<SF Customer Facing Host>/saml2/spnewcert?company=<company_id>`

Response

{·} Sample Code

```
----BEGIN CERTIFICATE-----
MIIEnzCCAwegAwIBAgIUYc7W+jjs1h6YpLzq+dIMvGvfT6gwDQYJKoZIhvcNAQELBQAwXzELMAkG
A1UEBhMCR0wxCzAJBgNVBAgMAlNUMRcwFQYDVQQKDA5zdWNjZXNzZmFjdG9yczEXMBUGA1UECwwO
c3VjY2Vzc2ZhY3RvcnMxETAPBgNVBAMMCFNGIGFkbWluMB4XDTI0MDUyMzA0MTIzMFoXDTI5MDUy
MzA0MTIzMFowXzELMAkGA1UEBhMCR0wxCzAJBgNVBAgMAlNUMRcwFQYDVQQKDA5zdWNjZXNzZmFj
dG9yczEXMBUGA1UECwwOc3VjY2Vzc2ZhY3RvcnMxETAPBgNVBAMMCFNGIGFkbWluMIIBojANBgkq
hkiG9w0BAQEFAAOCAY8AMIIBigKCAYEArH9ASYbzhJqEdqpmzF30NTRJsmDo0+QzBni1hXa85WBm
aSTF+hVYsmxOQKCKGRhVOdGhybpzyzG2vKrcwdP4NGyZDMmORikPiXkwswwfqDjh+g/9YsFBGQBY
TI6M9/4K4t4XH1OR5m7e86iUGQOWXu9XqZSCDRb2y7eryU53wA2fZegXhN+sV5BL522edei3NW21
XFFJvUr02P+K0Mer+WkIztXDQ75vnzREy0cNjf6zuVr7CGlluUQPjJatZb8VIjWWUAAoQAOKxLPE
cPbzHUceO3yMsOqEYgA2XgMLGabmZ0kOHef5Ls3slDshyV5PjJeQ/j7R4M2ICGKzWyKuhiLwumrA
IH02znJ/pJUGBxnMBhK2F+ww/rx/4uKGSAG9NPpH+uFshPReKhlQppUHQ3FeCHbmxwtuDbnCczCH
R82vugzOnGQjR74lW0tB/rT5j2FYpRcHYdpZySVBFrpdqLQ8NNDIXyhuTrq0PIjYr2uDEL2yQK8C
nzTKJLY3kzWVAgMBAAGjUzBRMB0GA1UdDgQWBBR7XY2xGkVdP27blhwp6nnRy5ymjDAfBgNVHSME
GDAWgBR7XY2xGkVdP27blhwp6nnRy5ymjDAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUA
```

```
A4IBgQAuk89TS/voBA2my983KOU7Ey3fbw5pllfuD8YAkmCNNwH6KCjx/QbQGnK445+XtSqbZGXz
m275sBqlqB+gSOGpj9Bt9wU7iiecCK1JI215N3YhZrRO/lVfcxOh9L45rxOx3cHbHNJMV3Xg5jIl
6pwFUGaBw9DakVN15lwEIH+xplmaWLKqmX/do5KWVAnjSDdrFztjWPEw4En/2Te2xldEvDi0J3Je
m2E96dgKPcf/Y7A722DFu78aP/TDqr4kk2a950EbEF4Jhtxp71cN1IdxypD2MU3St8hFySaChFUl
S9Z26nfqjLhRWed3cJ+ZGq7V+o4fOdd4qjmlwhgK0fHRDCetXKhvaiVurFwqEdw7aTC0KdCv5wqX
wBrYtcmXa7JZ3Ug+Bod5J9OLfOXiWasCfoN9/6/0/hBxuyGCkZpkeAT6f0nNklWvaedz9ooAyPwU
hTnrOUwNe2fbStAqJrgzp1q6JHvrazHUKBDMMrBx6xw/OYKtFrJl7nO6JZnkWDI=
-----END CERTIFICATE-----
```

> **Note**
>
> No authentication is needed for this API request.

> **→ Remember**
>
> After you've renewed your SSO signing certificate, go to the *Admin Center* > *Manage SAML SSO Settings* page and select the *SSO Certificate Renewed* checkbox to record your certificate renewal in the SAP SuccessFactors HCM suite.

> **⚠ Caution**
>
> Ensure that the new SAP SuccessFactors SSO certificate is updated in your corporate IDP **before** selecting the *SSO Certificate Renewed* checkbox. Selecting the checkbox activates the new certificate for SSO integration. If the corporate IDP is not updated first, SSO will fail for all affected users.

11.8 Register Your Own Application to Communicate with SAP SuccessFactors HCM Suite with OpenID Connect

Set up your application to commnicate with SAP SuccessFactors HCM suite using the OpenID Connect (OIDC) authentication protocol.

Prerequisites

- You have the *Administrator Permissions* > *Manage Security* > *Manage SAML SSO Settings* permission.
- You have the *Administrator Permissions* > *Manage Security* > *Manage Application Security Feature Settings* permission.
- You already have an SAP SuccessFactors HCM suite hybrid SAML/OIDC application set up in Identity Authentication.

  > **→ Tip**
  >
  > To confirm that the application is correctly set up in Identity Authentication, go to the *Applications & Resources* > *Applications* page in the Identity Authentication administration console and select your SAP SuccessFactors application. If a banner appears that says “This application was created from a source

application. Some of the inherited configurations can't be changed.", the setup is complete. If the banner is missing, contact Technical Support for assistance.

→ Remember

The SAP SuccessFactors application in Identity Authentication is provisioned and managed by SAP. You must not modify its OpenID Connect settings.

The steps in this topic apply only when you are setting up a separate client application that needs to call SAP SuccessFactors APIs using OpenID Connect, such as a custom integration, Postman, or another SAP system.

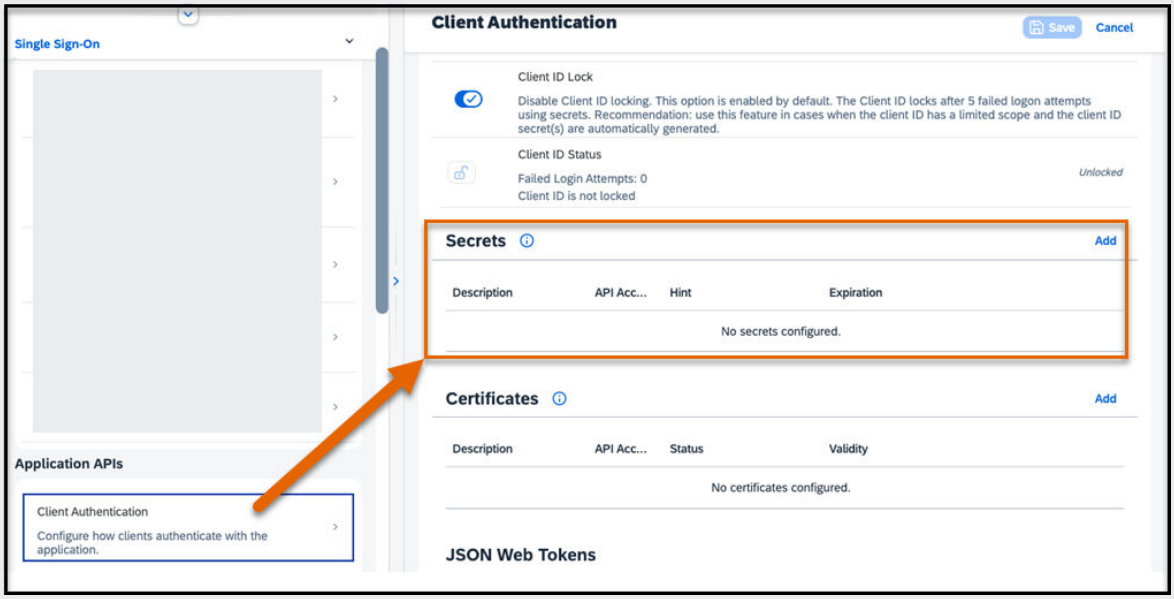
SAP managed services that already integrate with SAP SuccessFactors through Identity Authentication, such as Joule, do not require you to create or configure an OIDC client using this procedure.

ⓘ Note

If the hybrid SAML/OIDC setup is not complete (for example, the banner is missing), a common cause is the existence of one or more client secrets on the Identity Authentication application.

To check for existing client secrets that could prevent the SAML/OIDC setup banner from appearing:

1. In Identity Authentication, choose *Applications & Resources* > *Applications*.
2. Select the SAP SuccessFactors application created by Identity Authentication for your tenant.
3. Navigate to *Client Authentication* > *Secrets*.
   If any secrets are present, the hybrid setup cannot complete successfully. Client secrets are not secure and must not be used for API authentication. Delete all existing secrets and contact Technical Support to rerun the SAML/OIDC setup automation.



- The other application:
  - Is integrated with Identity Authentication on the same Identity Authentication tenant.
  - If system to system integration is set up, has a technical user in SAP SuccessFactors HCM suite with the required permissions.

Context

The OIDC protocol is one of the most popular and widespread methods of authentication across the web, mobile, and on-premise spaces. This procedure applies to scenarios where SAP SuccessFactors HCM suite is integrated with Identity Authentication using a hybrid SAML/OIDC application, enabling cohesive API authentication via OpenID Connect while maintaining browser-based single sign-on through SAML. With this feature, HCM suite integrations can use OAuth and OIDC with Identity Authentication as the central authentication provider.

Follow the steps below to set up your other application to communicate with SAP SuccessFactors HCM suite using the OIDC protocol.

Procedure

Create an OpenID Connect Client Application in Identity Authentication:

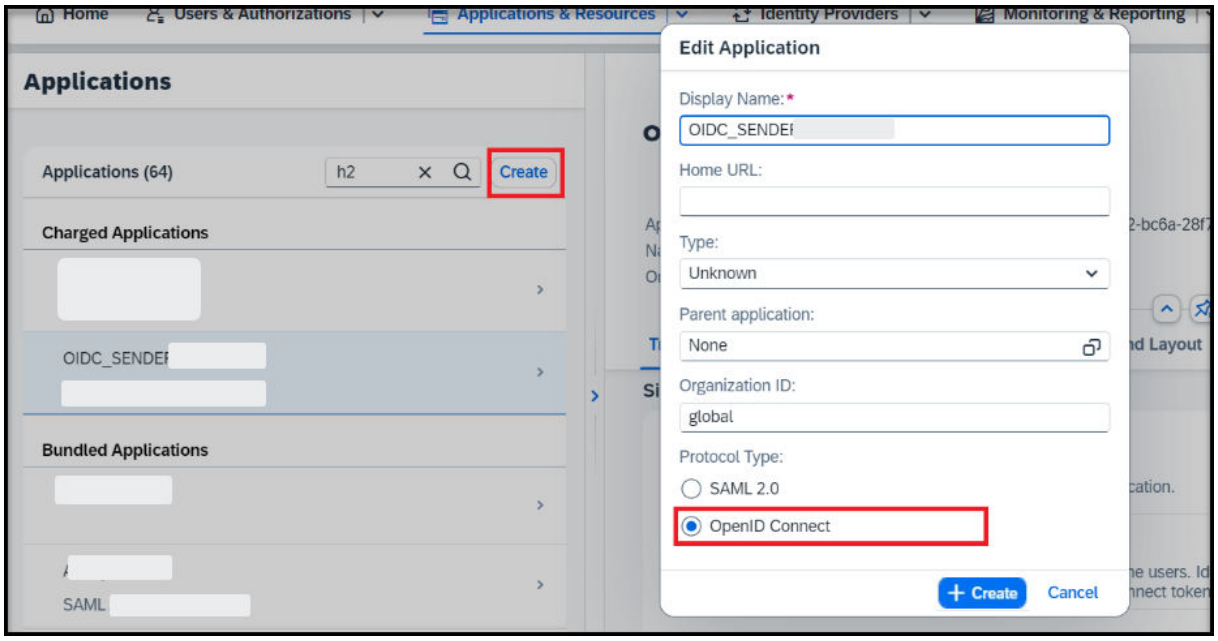
1. Sign in to the administration console for SAP Cloud Identity Services.
2. Under *Applications and Resources*, choose the *Applications* tile.

   > → Tip
   >
   > (Optional) You can use the Identity Authentication wizard to quickly create dependent applications and generate client credentials. For more information, see Generate Credentials to Access the APIs of an Application.
   >
   > If you use the wizard, you can skip the manual creation steps (Steps 3–5) and resume at Step 6: **Provided APIs**.

3. Click the *Create* button on the left-hand panel and fill in the information in the dialog box.
4. Provide the following information:

Field	Notes
Display Name	(Required) The display name of the application appears on the logon and registration pages.
Home URL	(Optional) Users are redirected to the `Home URL` after activating their accounts, when they are created via a CSV file import or the user registration service of Identity Authentication.
Type	(Optional)
Parent Application	Optional) → Remember Newly created applications with an assigned parent application will inherit all the configurations from the parent except for the `Client ID` and `Secrets`. The inherited configurations will be marked as such.
Protocol Type	Select the *OpenID Connect* radio-button.

Field	Notes
	→ Remember Newly created applications with an assigned parent application will inherit the protocol from the parent. To change the protocol, first create the new application and then edit it.

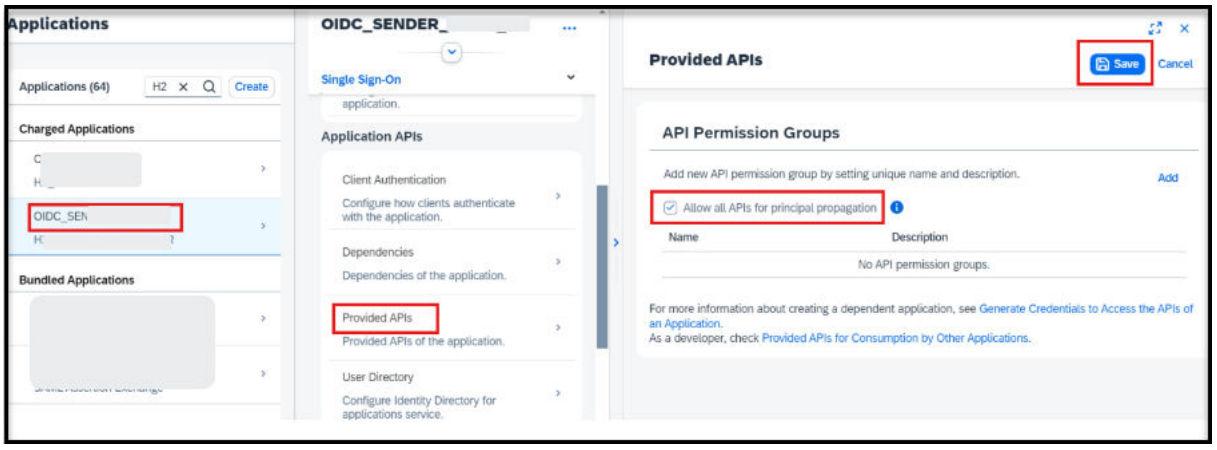


5. Choose *+Create*.

   Once the application has been created, the system displays the message **Application <name of application> created**.

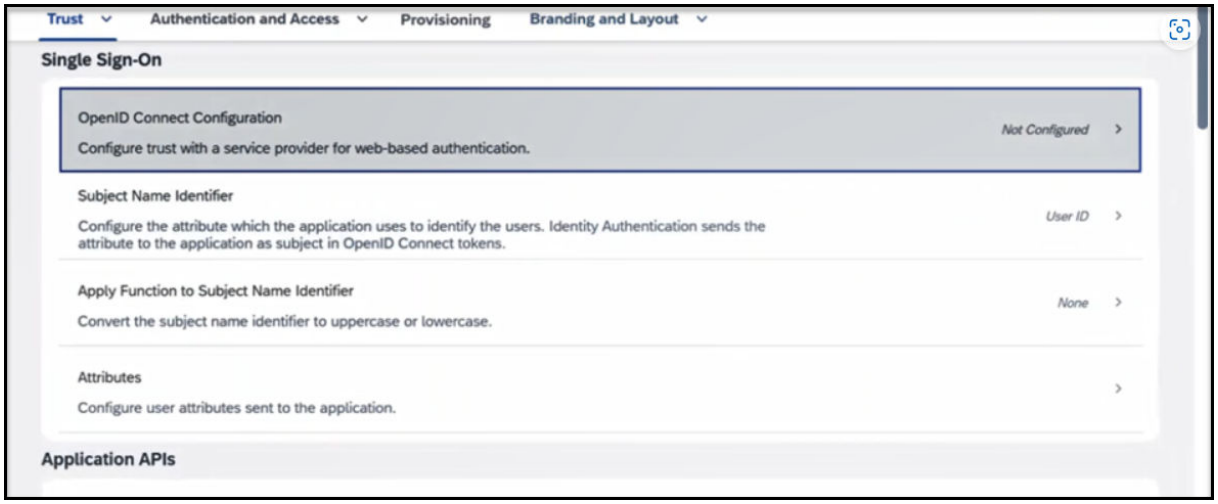
   The newly created application appears on the list with the applications on the left.

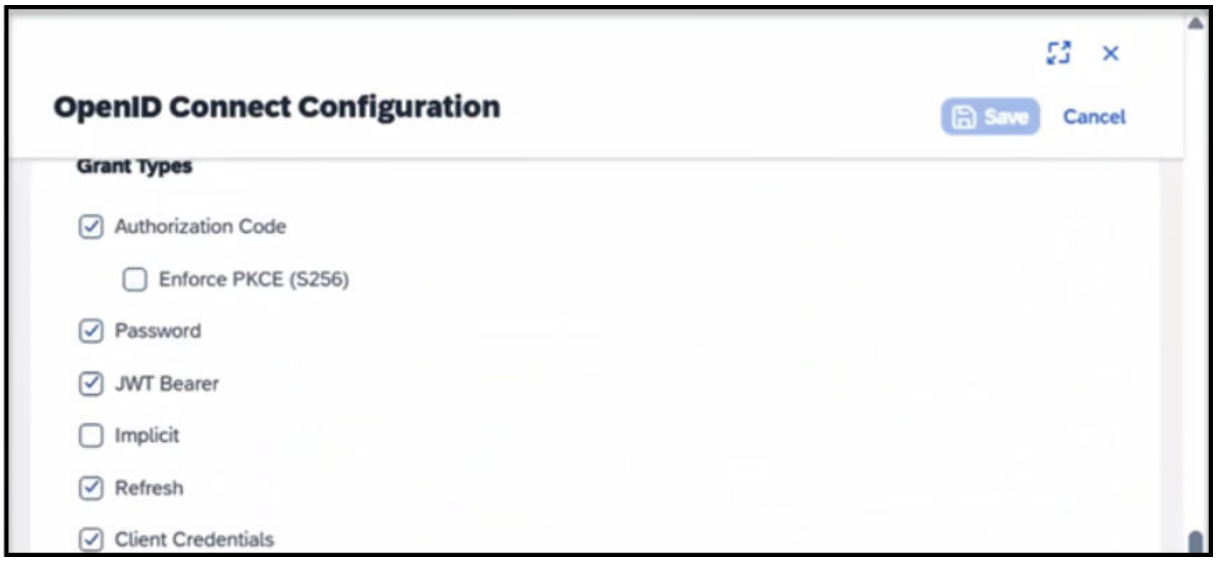
6. With your new application selected on the left panel, navigate to *Provided APIs* and make sure that *Allow all APIs for principal propagation* is enabled. If it's not, check this box and click *Save*.



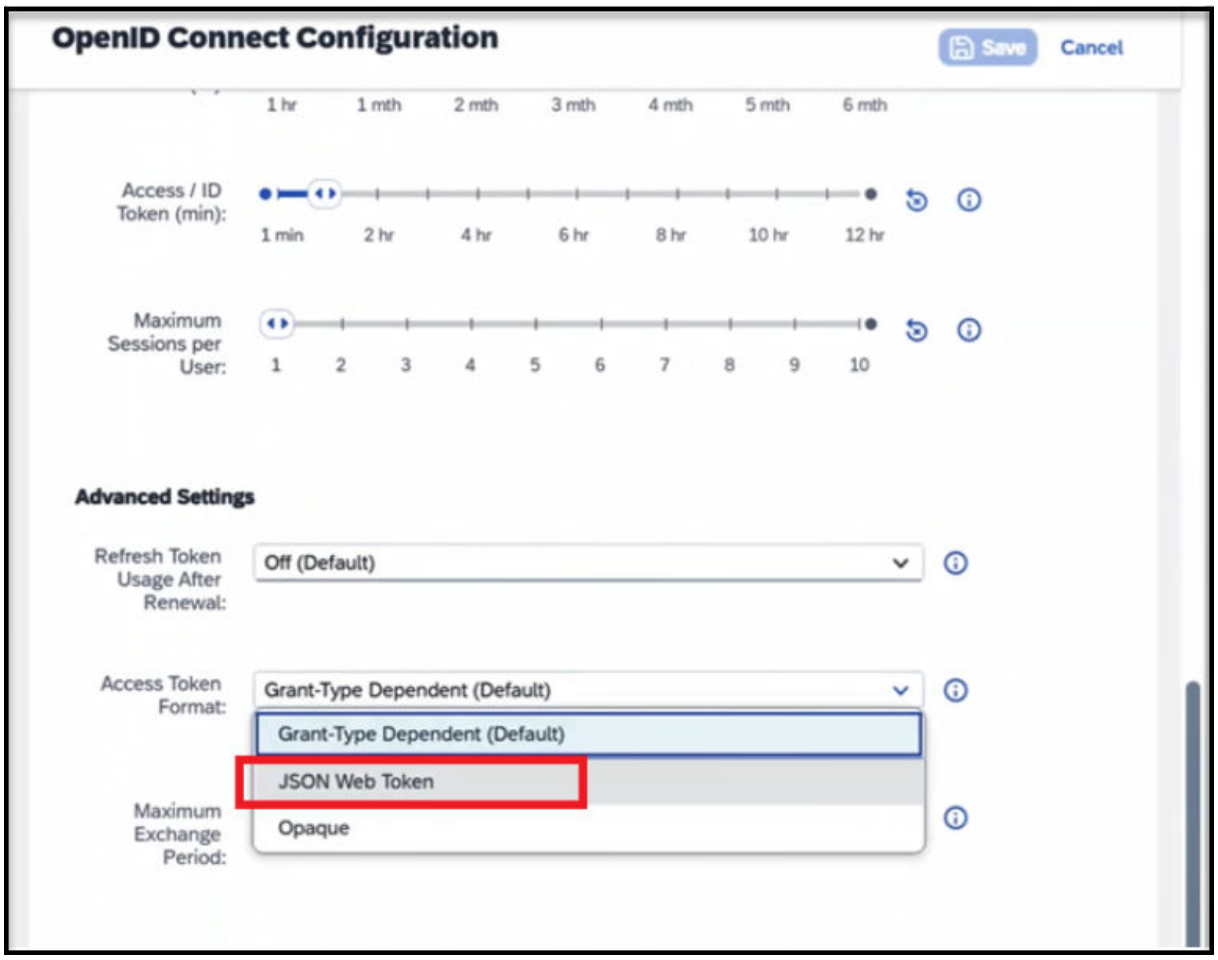
7. Next, go to *Single Sign-On* > *Grant Types* and verify that the following settings are configured as shown:

Grant Types	Setting
Authorization Code	Enable
Enforce PKCE (S256)	Disable
Password	Enable
JWT Bearer	Enable
Implicit	Disable
Refresh	Enable
Client Credentials	Enable

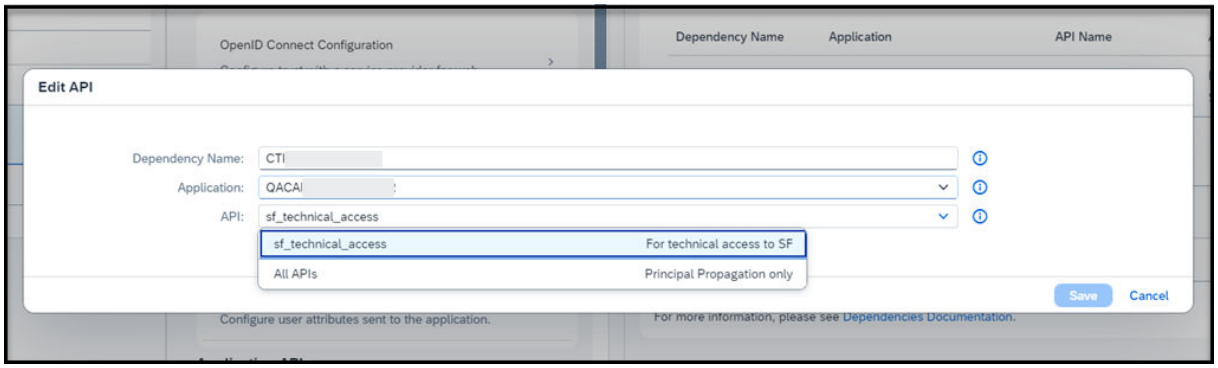


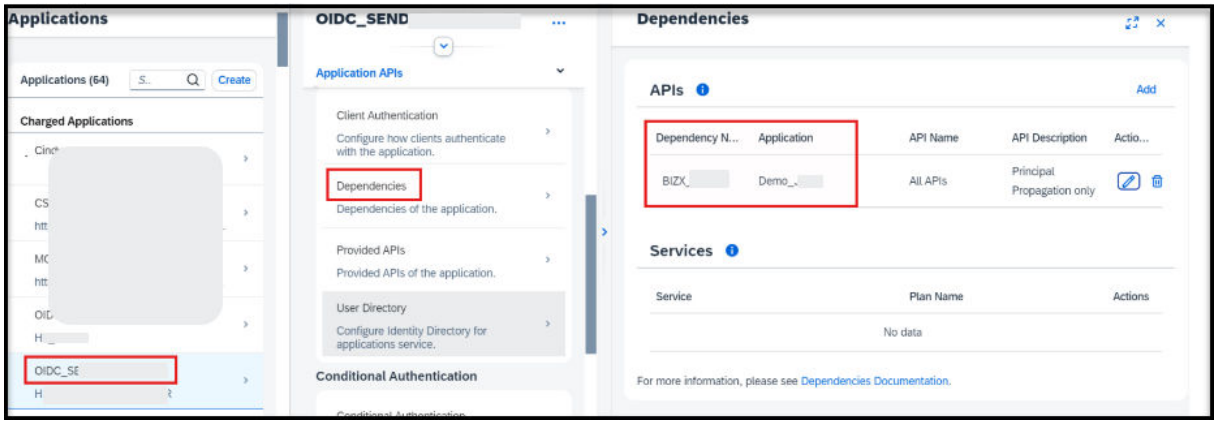


8. Scroll down to *Advanced Settings*, and under *Access Token Format*, select *JSON Web Token*.



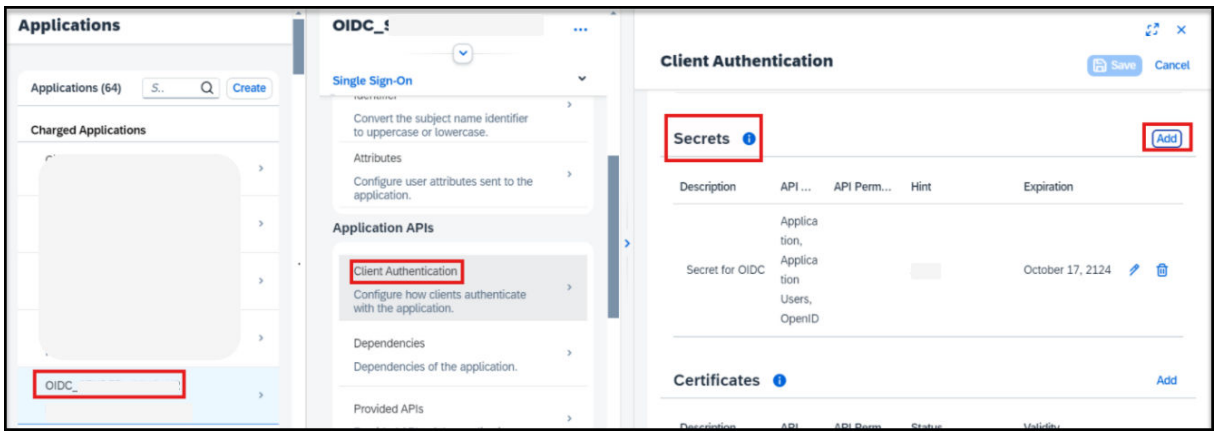
9. Navigate to *Dependencies* and click *Add*.
10. Under *Dependency Name*, define a dependency name of your choice, and under *Application* select your SAP SuccessFactors application.
11. Depending on which access method you want to use, select the appropriate value in the *API* drop-down:
    - For **Principal Propagation:** Select the *All APIs* option.
    - For **Technical User Access:** Select the *sf_technical_access* option.



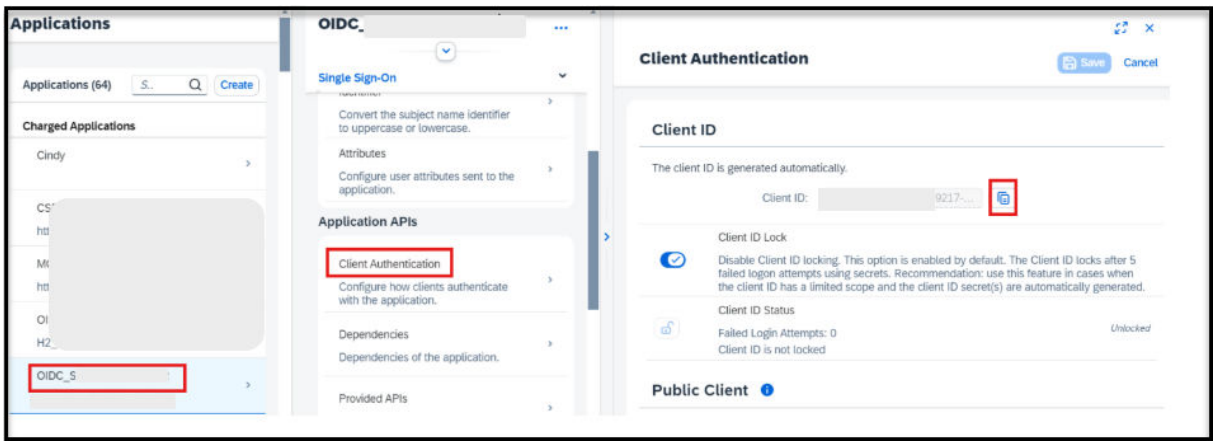


12. Click *Save*.

> → Tip
>
> (Optional) To test your OIDC configuration using an API tool such as Postman, or if requested by Technical Support, you can create a client secret:
>
> 1. Go to *Client Authentication* > *Secrets*
> 2. Click *Add* to create a new secret.
> 3. In the dialog box, enter the following:
>
> | Name | Value |
> |---|---|
> | Description | Enter a name for your client secret to be used for internal reference. |
> | Expire in | Choose a validity period before the secret expires. |
> | API Access | Select *Application* and *OpenID*. |
>
> 4. Click *Save*.
> 5. Copy the generated Client and Secret ID and store it for later use.



13. Navigate to *Client Authentication*, scroll up in the page and copy the *Client ID* (you'll need this later for use in step 19).



Create a Custom Applicaton Type Which Will Be Used to Sync Your OIDC OAuth Client Application to your SAP SuccessFactors HCM suite Hybrid SAML/OIDC Application:

> ### Note
>
> Starting with the 1H 2026 release, registering the incoming application in SAP SuccessFactors is no longer required for integrations that use Principal Propagation. If your integration uses Principal Propagation, you can skip Steps 14–20 in this procedure. These steps are only required for integrations that use Technical User Access.

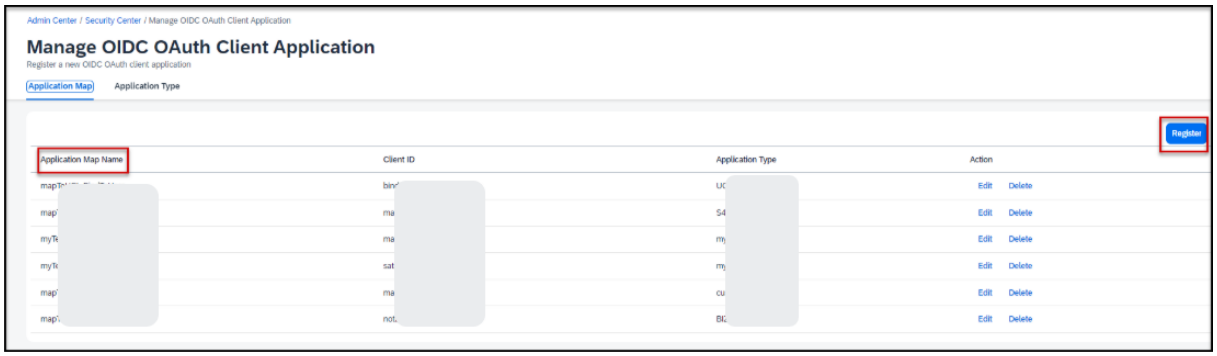
> ### Note
>
> For SAP applications that have already integrated with SAP SuccessFactors, a predefined *Application Type* is already pre-configured within the application. Typically, you won't need to create a new Application Type if the existing one already meets your integration needs.
>
> If you need to create your own custom Application Type, you may do so by following steps 14-16 below. Keep in mind that each Application Type can only be linked to one OIDC OAuth client application.

14. Navigate to the *Admin Center* > *Security Center* > *Manage OIDC OAuth Client Application* > *Application Type* > tab and click *Register*.
15. On the *Register a New Application Type* dialog box, enter your application's name in the *Application Type Name* field.

16. Click *Register*.

Map Your OIDC OAuth Client Application to Your SAP SuccessFactors HCM Suite Hybrid SAML/OIDC Application:

17. Click on the *Application Map* tab.



18. Click *Register*.
19. Complete the fields on the *Register a New Application Map* dialog box.

Field	Description
Application Map Name	(Required) The unique name of your OIDC OAuth client application in SAP SuccessFactors
Client ID	(Required) The unique ID of your OIDC OAuth client application (this is the Client ID created in step 13).
Bind to User	(Optional) • **If unchecked**: The system uses the **default technical user** (a backend-managed account for SAP SuccessFactors integrations, not visible to customers). This account is internally mapped to the predefined *Application Type* `BIZX`. In this case, ensure *sf_technical_access* is selected in the *API* field drop-down (Step 11) for proper system-to-system communication. • **If checked**: A specific user is used, based on the *User ID* you enter. **⚠ Caution** Keep *Bind to User* unchecked in most cases. Select it only if an advanced user is required and you are certain of the configuration.
User ID	(Required if *Bind to User* is enabled) This is the ID of the specific user that would always be used for communication to SAP SuccessFactors from the other application.

Field	Description
Application Type	(Required if *Bind to User* is left unchecked) If a technical user is used, the Application Type is the unique value associated with that technical user. **Note** For applications that have already integrated with SAP SuccessFactors, a predefined Application Type `BIZX` is already mapped in the backend. If you try to register this application type manually, you may see an error message about a duplicate mapping. This is expected and can be safely ignored. There is no need to register the `BIZX` application type again. **Note** If OIDC is used to authenticate requests to the OData API, they appear in the *OData API Audit Log*, where the default technical user in use can be verified (for example, `TECHNICAL_USER_ECTIME_S4HANA_CTR_<2A5BD013>`).

20. Click *Register*.

Note

If multi-factor authentication (MFA) is enabled for critical transactions, a verification prompt will appear before the registration is completed. Users must enter a one-time code from their registered authenticator app to proceed. For more information, refer to **Enable Transactional Verification for Critical Transactions** in the Related Information section.

Results

You've now registered your application to commuicate with SAP SuccessFactors HCM suite with OpenID Connect using Identity Authentication.

Next Steps

To learn how to authenticate and use OpenID Connect in your API calls, refer to **Authentication Using OpenID Connect** in the **Related Information** section.

To test your OIDC setup, refer to 3532791 in the **SAP for Me** portal to use the sample API testing package.

Related Information

Enable Transactional Verification for Critical Transactions Using Multi-Factor Authentication [page 162]
Authentication Using OpenID Connect (OIDC)

11.9 Identity Provisioning Service Administration Console Tasks

The Identity Provisioning service allows you to manage the transfer of user data from Source Systems (SAP SuccessFactors) to Target Systems (service). You can use this service to define how your data is read from the Identity Provisioning service into the Identity Authentication service.

> **Note**
>
> If your bundle or standalone tenant is running on the **SAP BTP Neo environment**, we recommend that you migrate them to the **SAP Cloud Identity Services infrastructure**. Sharing the same infrastructure with Identity Authentication brings a number of benefits as described in Tenant Infrastructure.

Your Identity Provisioning service system is created when you initiate your upgrade to Identity Authentication, in the SAP SuccessFactors *Upgrade Center* and the Identity Provisioning administrator receives an email with the link to the *Identity Provisioning Administration* console in SAP Cloud Identity Services.

> **→ Remember**
>
> If your SAP SuccessFactors tenant was created after December 9, 2022, Identity Authentication and Identity Provisioning have already been enabled. You do not need to complete the steps to upgrade and to Identity Authentication.

> **⚠ Caution**
>
> If you haven't received an email with a link to your Identity Provisioning system within two hours, contact Technical Support.

The Identity Provisioning service contains access to your *Source Systems* and *Target Systems* and ensures the synchronization of the entities between the two systems or multiple target systems.

You can configure the required provisioning entities in order to ensure proper synchronization between source and target systems. You can also use proxy systems for indirect connections between a system supported by the

Identity Provisioning service and an external application that uses a SCIM 2.0 API to consume identities from the proxy system. For example, you can use Identity Provisioning service as an external consuming application.

Properties help you to customize the way your identities are read from a source system or provisioned to the target one. They can also filter which entities and attributes to be read or skipped during the provisioning job.

For every system supported by the Identity Provisioning service, there's an initial (default) transformation logic that converts the system-specific JSON representation of the entities from/to one common JSON. You can keep the default transformation, or modify the mapping rules to reflect the current setup of entities from your source or target system.

- *Source* – a system, where the company is currently managing the corporate identities.
- *Target* – a system that needs to be populated with corporate users and other entities.

What to Configure in the Identity Provisioning Console

After upgrading to the Identity Authentication service in the SAP SuccessFactors *Upgrade Center*, you'll need to perform some configurations in the Identity Provisioning console.

> → Remember
>
> If your SAP SuccessFactors tenant was created after December 9, 2022, Identity Authentication and Identity Provisioning have already been enabled. You do not need to complete the steps to upgrade to Identity Authentication.

- Review and Edit the Settings Populated During the Upgrade Process.
- Default Configuration for SAP SuccessFactors as a Source System.
  When SAP SuccessFactors is configured as a source system in the Identity Provisioning service, the following default settings are applied:

Property	Default Value
Authentication	ClientCertificateAuthentication
sp.api.version	2
sf.group.members.paging.enabled	true
URL	Certificate API endpoint

  The default *sp.api.version = 2* ensures that the SCIM version transformation is applied for provisioning data from SAP SuccessFactors to Identity Authentication.

- Configure Transformations to control how your data is read into the Identity Authentication service.
- Create a password for the API user (IPSADMIN).

> ⓘ Note
>
> This *IPSADMIN* user is created during the upgrade process. As such, you must create a password for this user and grant them the permissions required to perform integration tasks in your SAP SuccessFactors.

> → Remember
>
> If your SAP SuccessFactors tenant was created after December 9, 2022, you are **not** using the IPSADMIN API user, since your configuration is already enabled with a technical user in the background to communicate between Identity Authentication and Identity Provisioning using mTLS and the SCIM API.

- Run sync jobs.

> ⓘ Note
>
> Access to Identity Provisioning is managed in the SAP Cloud Identity Services administration console in the *Administrators* section (previously, in the Neo environment, this was controlled in the Identity Provisioning console itself. For more information please refer to **Manage Authorizations in SAP Cloud Identity Infrastructure** under **Related Information** below).

Related Information

Manage Authorizations in Neo Environment
Configure Transformations in Identity Provisioning [page 89]

11.9.1 Setting Up the Identity Provisioning Source and Target Systems

Initiating the Identity Authentication upgrade automatically configures most of your Identity Provisioning settings but some settings made need edits to ensure that your connections are properly set and your tests sync runs properly.

Prerequisites

- The Identity Authentication upgrade is complete
- You created a password for the newly created API User: *IPSADMIN*

Context

> ⓘ Note
>
> If your SAP SuccessFactors tenant was created after December 9, 2022, you are **not** using the IPSADMIN API user, since your configuration is already enabled with a technical user in the background to communicate between Identity Authentication and Identity Provisioning using Mutual Transport Layer Security (mTLS) in

conjunction with the System for Cross-domain Identity Management (SCIM) API, which are the latest methods of authentication and integration with Identity Authentication and Identity Provisioning.

Also, if you have already initiated the upgrade to Identity Authentication after December 9, 2022, Identity Authentication and Identity Provisioning **will already** be configured to use Mutual Transport Layer Security (mTLS) in conjunction with the System for Cross-domain Identity Management (SCIM) API.

If you have manually upgraded to Mutual Transport Layer Security (mTLS) as your authentication method, a technical user will also be created for you in the background for communication between SAP SuccessFactors and Identity Authentication and Identity Provisioning.

You **do not** need to complete **steps 5 and 6** in the below procedure.

For more information on upgrading to mTLS authentication as well as upgrading to the SCIM API, refer to **Upgrade to X.509 Certificate-Based Authentication for Incoming Calls** and **Upgrade from OData Identity Provisioning Connector to SCIM Connector with SAP SuccessFactors HCM suite** in the **Related Information** section.

When you initiate the Identity Authentication upgrade, that process creates and configures your Identity Provisioning *Source* and *Target* systems.

Procedure

1. Log into *SAP Cloud Identity Services* > *Identity Provisioning*.
2. Go to *Source Systems*.
3. Select the source that reflects the name of your SAP SuccessFactors instance.
4. Go to *Properties*.
5. Scroll down to *User*. Your exact SAP SuccessFactors instance name is to the right of the API user name. For example, **`apiuser@instanceName`**

   If your instance name is not displayed in the source system that you selected, select a different source system until you find the instance that contains the name of your instance in the *User* field.
6. Enter the password you set for your API user in the *Password* field.
7. Review and edit the types of users you want to sync in the *sf.user.filter* field

   ⚠ Caution

   The *sf.user.filter* in the *Identity Provisioning Service Administration Console* under the tabs *Source Systems* > *Properties*, contains place holder values called, *'sf_username1_placeholder','sf_username2_placeholder'*. Replacing these place holders with a few users can help you to test user provisioning before performing the sync job that pulls in all of your SAP SuccessFactors users into Identity Authentication. Test your selected users by substituting the place holders with usernames from your SAP SuccessFactors system. After testing and ensuring that user provisioning is working correctly, remove the placeholder users and replace them with the value **`Active`**. This syncs all the active users in your system.

   If you change this filter **AFTER** running the user sync, any users not found using the new filter is deleted from the Identity Authentication Service.

8. Ensure that the value in *Source Systems* > *Details* > *System Name* **and** the value in *Source* > *Properties* > *User* contain the same instance name.
9. Go to *Target Systems*.
10. Select the source that reflects the name of your SAP SuccessFactors instance.
11. Ensure that the URL in *Properties* matches the URL to your Identity Authentication Service.

    The URL is listed in the Identity Authentication email you received after upgrading your system.
12. From the *Target System*, in the *Details* tab, ensure that the *Source Systems* value matches the value from the *Source System*, noted in Step 8.

    If the source is not listed, choose *Edit* and select your source from the list.

    > ⚠ Caution
    >
    > Use the dropdown list to check on your source. DO NOT uncheck any existing sources.
13. Save your changes.

Results

If you've reviewed or configured your Identity Authentication settings and you've completed your Identity Provisioning configurations, you can set up your sync jobs as described in the topic: **Running and Scheduling Jobs**

11.9.2 Upgrade from ODATA Identity Provisioning Connector to SCIM Connector with SAP SuccessFactors

Existing Identity Authentication customers can now switch from the ODATA API to the SCIM API for use with Identity Provisioning.

Prerequisites

You have the *Administrator Permissions* > *Manage Security Center* > *Access to X.509 Certificate Mapping* permission.

Context

The System for Cross-domain Identity Management (SCIM) API is a preferred method to make user data more secure and simplify the user experience by automating the user identity lifecycle management process. The below steps set up communication between Identity Provisioning and SAP SuccessFactors HCM suite and configure the authentication method.

> ### Note
>
> If you're an existing Identity Authentication customer, and would like to enable Onboarding to authenticate your users with Identity Authentication and Identity Provisioning, switching to the SCIM API is **required**.

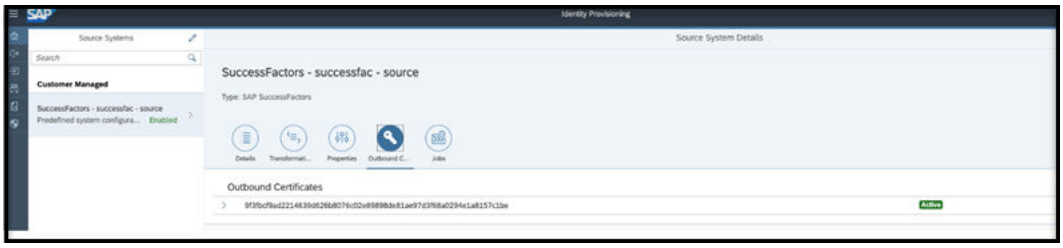
> ### Caution
>
> Do not start the upgrade procedure if your SAP SuccessFactors instance was recently refreshed and the post-refresh activities have not been completed. Performing the upgrade before Identity Provisioning successfully syncs after the instance refresh can cause provisioning issues with integrated systems such as Identity Authentication and SAP Analytics Cloud.

> ### Caution
>
> Before starting the upgrade, cancel all active Identity Provisioning user sync jobs with SAP SuccessFactors as the source system. This will prevent conflicts and ensure the new SCIM API configuration works correctly.

Procedure

1. > ### Caution
   >
   > Steps **1–7** walk you through setting up Mutual Transport Layer Security (mTLS) as your authentication method between Identity Provisioning and SAP SuccessFactors.
   >
   > Migration to Mutual Transport Layer Security (mTLS) for Identity Provisioning to SAP SuccessFactors integration is required before the deprecation of HTTP API Basic Authentication in 2H 2027.
   >
   > If your integration still uses HTTP API Basic Authentication, you must migrate to mTLS before the 2H 2027 deadline. After HTTP API Basic Authentication is removed, integrations that have not migrated to mTLS will no longer function.

   Go to *SAP Cloud Identity Services* > *Identity Provisioning* > *Source Systems*.
2. From the list of source systems, select the desired SAP SuccessFactors tenant record.
3. Click on the *Outbound Certificate* tab.



4. If there's no active certificate, click *Generate* and *Download*. If there's already an active certificate, just click *Download*.
5. Navigate to the SAP SuccessFactors *Admin Center* > *Security Center* > *X.509 Public Certificate Mapping* tab and choose *Add*.
6. Register your X.509 public certificate for mTLS communication by providing the required information and upload the certificate file. Make sure you select Identity Provisioning Service in the *Integration Name* field.

7. Save your changes.
8. > ⓘ Note
   >
   > The below steps configure SAP SuccessFactors as a **Source System** to use the SCIM API and are configured in your Identity Provisioning administration console.

   Go to *SAP Cloud Identity Services* > *Identity Provisioning* > *Source Systems*.
9. From the list of source systems, select the desired SAP SuccessFactors tenant record.
10. Click on the *Properties* tab to configure the property parameters, and set the *sf.api.version* parameter to **2** for the SCIM API to be used. Also update the *URL* field with the certificate-based authentication URL for your API. Refer to List of SAP SuccessFactors API Servers under the **mTLS Certificate Server** column.

    Refer to the table below for a list of the properties:

    > ⓘ Note
    >
    > The following properties are **mandatory** unless specified as Optional in the **Property Name** column.

    Mandatory Properties Table

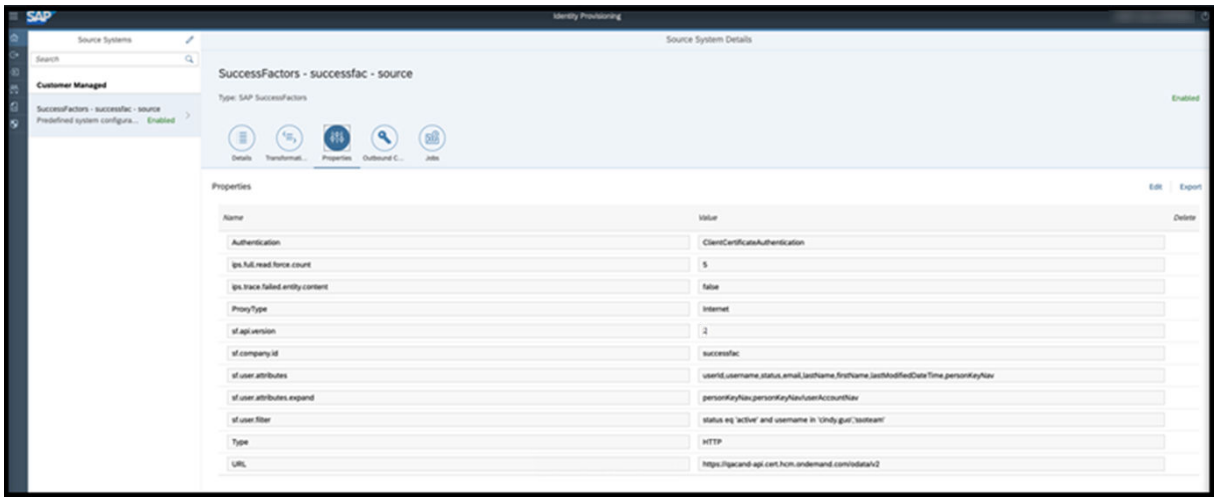
Property Name	Description & Value
Type	Enter: **HTTP**
URL	Specify the mTLS URL to your SAP SuccessFactors API. Refer to List of SAP SuccessFactors API Servers under the **mTLS Certificate Server** column.
Proxy Type	Enter: **Internet**
Authentication	Enter: **ClientCertificateAuthentication**
sf.api.version	Enter: **2**- Indicates that SAP SuccessFactors Workforce SCIM API (in short, SCIM API) is used.
sf.company.id	Valid if ClientCertificateAuthentication is configured as the authentication method. Enter the Company ID of your SAP SuccessFactors system. The Company ID is a short string of characters that identifies each SAP SuccessFactors system. It is like a username for your organization. All users of the same system share the same Company ID.

Property Name	Description & Value
(Optional)sf.group.members.paging.enabled	This property enables paging of group members. The maximum number of group members returned per request is 100. To read more than 100 group members, paging must be enabled. Possible values: **true** - Paging is enabled. **false** - Paging is disabled. Default value: **false**. **Connector version** SAP SuccessFactors version 2 (SCIM API)
(Optional) sf.user.filter	The possible values of this property depend on the API version which your SAP SuccessFactors system consumes. Use this property to filter users from SAP SuccessFactors. The filter obtains values as described in the OData 2.0 syntax, except any statements with attribute `lastModifiedDateTime`. Find below examples syntax for filtering users depending on the API version: • OData API - userName eq "cbraun" • SCIM API - userName eq "cbraun" To learn more, see: • OData Version 2 → **4.5. Filter System Query Option ($filter).** • SAP SuccessFactors HCM suite OData API:Reference Guide (V2) • SAP SuccessFactors Workforce SCIM API and System for Cross-domain Identity Management for Workforce in SuccessFactors

Property Name	Description & Value
(Optional) sf.user.read.deactivatedafter	This property filters SAP SuccessFactors inactive users from a particular date on. It is an optional property which does not appear by default at system creation. It accepts a value in the yyyy-MM-dd format. For example: **2023-07-17**. The `sf.user.read.deactivatedafter` property works together with the sf.user.filter property which is added at system creation with the default value: **active eq true**. Using it can further narrow down the filtering results. To filter active users along with inactive ones from a particular date on, the following configuration must be in place: Set the sf.user.read.deactivatedafter value to a date in the expected format. For example: 2023-07-17 `sf.user.filter`=**active eq true** As a result, Identity Provisioning reads SAP SuccessFactors active users and the users set to inactive from that date on using the 2023-07-17T00:00:00Z date-time format. Depending on the value you define for `sf.user.filter`, expect the following results: `sf.user.filter`=**active eq false** All inactive users will be returned. `sf.user.filter`=**active eq false and userName sw "Test_"** All inactive users with username starting with Test_ will be returned. **Note** When you filter by sf.user.filter = **active eq false** along with the property `sf.user.read.deactivatedafter`, the users that match the two critera will be read twice.

Property Name	Description & Value
(Optional) sf.group.filter	The possible values of this property depend on the API version which your SAP SuccessFactors system consumes. Use this property to filter users from SAP SuccessFactors. The filter obtains values as described in the OData 2.0 syntax, except any statements with attribute `lastModifiedDateTime`. To learn more, see: • OData Version 2 → **4.5. Filter System Query Option ($filter).** • SAP SuccessFactors HCM suite OData API:Reference Guide (V2)→**DynamicGroup** • SAP SuccessFactors Workforce SCIM API and System for Cross-domain Identity Management for Workforce in SuccessFactors
(Optional) sf.group.prefix	This property distinguishes SAP SuccessFactors groups by specific prefix. It is an optional property which does not appear by default at system creation. Example value: SF_ You can use the example value or provide your own. When **set in the source system**, the prefix will be prepended to the name of the groups that are read from the SAP SuccessFactors source system and will be provisioned to the target system with the following name pattern: SF_<GroupDisplayName>. This way SAP SuccessFactors groups in the target system will be distinguished from groups provisioned from other applications. If the property is not set, the SAP SuccessFactors groups will be read and provisioned to the target system with their actual display names. **Connector version**: SAP SuccessFactors version 2 (SCIM API)

To learn what additional properties are relevant to SAP SuccessFactors, refer to List of Properties. You can use the main search, or filter properties by the Name or System Type columns.



11. **Note**

    The below steps allow you to view and update the transformations for the SCIM API.

    By default, Identity Provisioning provides default transformations for your SAP SuccessFactors **Source** and **Target** systems, however, these are **not** the same transformations that are provided by the SAP SuccessFactors Upgrade Center.

    You'll need to therefore update these default transformations to the **Source** and **Target** transformations provided in the steps below.

    From the *SAP Cloud Identity Services* > *Identity Provisioning* > *Source Systems* page, ensure you have the desired SAP SuccessFactors tenant record selected from the list of source systems.

12. Click on the *Transformations* tab to view the default transformation provided by Identity Provisioning for your SAP SuccessFactors **source** system.
13. Click *Edit* to update the source transformation for the SCIM API to the following:

    Default transformation for SCIM API for SAP SuccessFactors Source System:

    Code Syntax

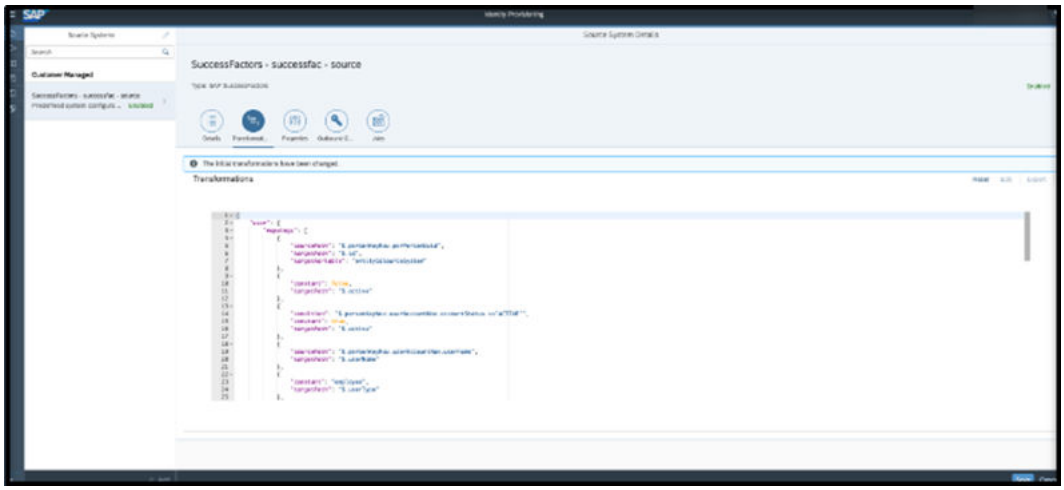
```
{
    "user": {
        "mappings": [
            {
                "sourcePath": "$.schemas",
                "targetPath": "$.schemas",
                "preserveArrayWithSingleElement": true
            },
            {
                "sourcePath": "$.id",
                "targetVariable": "entityIdSourceSystem"
            },
            {
                "sourcePath": "$.userName",
                "targetPath": "$.userName",
                "correlationAttribute": true
            },
            {
                "sourcePath": "$.active",
                "targetPath": "$.active"
```

```
            },
            {
                "sourcePath": "$.userType",
                "targetPath": "$.userType"
            },
            {
                "sourcePath": "$.name.familyName",
                "targetPath": "$.name.familyName",
                "optional": true
            },
            {
                "sourcePath": "$.name.givenName",
                "targetPath": "$.name.givenName",
                "optional": true
            },
            {
                "sourcePath": "$.name.middleName",
                "targetPath": "$.name.middleName",
                "optional": true
            },
            {
                "sourcePath": "$.name.honorificPrefix",
                "targetPath": "$.name.honorificPrefix",
                "optional": true
            },
            {
                "sourcePath": "$.name.honorificSuffix",
                "targetPath": "$.name.honorificSuffix",
                "optional": true
            },
            {
                "sourcePath": "$.name.formatted",
                "targetPath": "$.name.formatted",
                "optional": true
            },
            {
                "sourcePath": "$.nickName",
                "targetPath": "$.nickName",
                "optional": true
            },
            {
                "sourcePath": "$.title",
                "targetPath": "$.title",
                "optional": true
            },
            {
                "sourcePath": "$.displayName",
                "targetPath": "$.displayName",
                "optional": true
            },
            {
                "sourcePath": "$.emails",
                "targetPath": "$.emails",
                "optional": true,
                "preserveArrayWithSingleElement": true
            },
            {
                "sourcePath": "$.emails[?(@.primary== true)].value",
                "optional": true,
                "correlationAttribute": true
            },
            {
                "sourcePath": "$.phoneNumbers",
                "targetPath": "$.phoneNumbers",
                "optional": true,
                "preserveArrayWithSingleElement": true
            },
            {
```

```
                "sourcePath": "$.preferredLanguage",
                "targetPath": "$.preferredLanguage",
                "optional": true
            },
            {
                "sourcePath": "$.locale",
                "targetPath": "$.locale",
                "optional": true
            },
            {
                "sourcePath": "$.timezone",
                "targetPath": "$.timezone",
                "optional": true
            },
            {
                "sourcePath": "$.externalId",
                "targetPath": "$.externalId",
                "optional": true
            },
            {
                "sourcePath": "$.groups",
                "targetPath": "$.groups",
                "optional": true,
                "preserveArrayWithSingleElement": true
            },
            {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['employeeNumber']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['employeeNumber']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['department']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['department']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['division']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['division']",
                "optional": true
            },
            {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",
                "optional": true
            },
            {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['displayName']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['displayName']",
                "optional": true
            },
            {
```

```
"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['$ref']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['$ref']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['userUuid']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['userUuid']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['groupDomains']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:sap:2.0:User']['groupDomains']",
                "optional": true,
                "preserveArrayWithSingleElement": true
            },
            {
                "sourcePath":
"$['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['perPersonUuid']",
                "targetPath":
"$['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['perPersonUuid']",
                "optional": true
            },
            {
                "sourcePath":
"$['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['personIdExternal']",
                "targetPath":
"$['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['personIdExternal']",
                "optional": true
            },
            {
                "sourcePath":
"$['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['loginMethod']",
                "targetPath":
"$['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['loginMethod']",
                "optional": true
            },
            {
                "sourcePath":
"$['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['isDraft']",
                "targetPath":
"$['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['isDraft']",
                "optional": true
            },
            {
                "sourcePath":
"$['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['customFields']",
                "targetPath":
"$['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['customFields']",
                "optional": true
            },
```

```
            {
                "targetPath":
"$['urn:sap:cloud:scim:schemas:extension:sap.ips.sfsf.sac:2.0:User']
['hasEmbeddedAnalyticsPermission']",
                "constant": false
            },
            {
                "targetPath":
"$['urn:sap:cloud:scim:schemas:extension:sap.ips.sfsf.sac:2.0:User']
['hasEmbeddedAnalyticsPermission']",

"condition": "$['urn:ietf:params:scim:schemas:extension:sap:2.0:User']
['groupDomains'][?(@.value == 'embeddedAnalyticsAccessPermission')] empty
false",
                "constant": true
            }
        ]
    },
    "group": {
        "ignore": true,
        "mappings": [
            {
                "sourcePath": "$.id",
                "targetPath": "$.id",
                "targetVariable": "entityIdSourceSystem"
            },
            {
                "sourcePath": "$.schemas",
                "targetPath": "$.schemas"
            },
            {
                "sourcePath": "$.displayName",
                "targetPath": "$.displayName"
            },
            {
                "sourcePath": "$.members",
                "targetPath": "$.members",
                "optional": true,
                "preserveArrayWithSingleElement": true
            }
        ]
    }
}
```



14. Go to *SAP Cloud Identity Services* > *Identity Provisioning* > *Target Systems* > *(your Identity Authentication target system)*.

15. Click on the **Transformations** tab to view the default transformation provided by Identity Provisioning for your Identity Authentication **target** system.
16. Click *Edit* to update the target transformation for the SCIM API to the following:

    Default transformation for SCIM API for the Identity Authentication Target System:

Code Syntax

```
{
    "user": {
        "condition": "($.emails EMPTY false) && ($.name.familyName EMPTY
false)",
        "mappings": [
            {
                "targetPath": "$.id",
                "sourceVariable": "entityIdTargetSystem"
            },
            {
                "targetPath": "$.schemas[0]",
                "constant": "urn:ietf:params:scim:schemas:core:2.0:User"
            },
            {
                "targetPath": "$.schemas[1]",
                "constant":
"urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"
            },
            {
                "targetPath": "$.schemas[2]",
                "constant":
"urn:sap:cloud:scim:schemas:extension:custom:2.0:User"
            },
            {
                "sourcePath": "$.active",
                "targetPath": "$.active",
                "optional": true
            },
            {
                "sourcePath": "$.userName",
                "targetPath": "$.userName",
                "optional": true
            },
            {
                "sourcePath": "$.emails[*].value",
                "targetPath": "$.emails[?(@.value)]",
                "preserveArrayWithSingleElement": true
            },
            {
                "sourcePath": "$.userType",
                "targetPath": "$.userType",
                "optional": true
            },
            {
                "sourcePath": "$.name.givenName",
                "targetPath": "$.name.givenName",
                "optional": true
            },
            {
                "sourcePath": "$.name.middleName",
                "targetPath": "$.name.middleName",
                "optional": true
            },
            {
                "sourcePath": "$.name.familyName",
                "targetPath": "$.name.familyName"
            },
            {
```

```
                "sourcePath": "$.name.honorificPrefix",
                "targetPath": "$.name.honorificPrefix",
                "optional": true,
                "ignore": true
            },
            {
                "sourcePath": "$.addresses",
                "targetPath": "$.addresses",
                "optional": true,
                "preserveArrayWithSingleElement": true
            },
            {
                "sourcePath": "$.locale",
                "targetPath": "$.locale",
                "optional": true,
                "ignore": true
            },
            {
                "sourcePath": "$.phoneNumbers",
                "targetPath": "$.phoneNumbers",
                "optional": true,
                "preserveArrayWithSingleElement": true
            },
            {
                "sourcePath": "$.telephoneVerified",
                "targetPath": "$.telephoneVerified",
                "optional": true
            },
            {
                "sourcePath": "$.displayName",
                "targetPath": "$.displayName",
                "optional": true
            },
            {
                "sourcePath": "$.timezone",
                "targetPath": "$.timeZone",
                "optional": true
            },
            {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['employeeNumber']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['employeeNumber']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['costCenter']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['costCenter']",
                "optional": true
            },
            {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['organization']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['organization']",
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['division']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['division']",
```

```
                "optional": true
            },
            {
                "sourcePath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['department']",
                "targetPath": "$
['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']['department']",
                "optional": true,
                "ignore": true
            },
            {

"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",

"targetPath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",
                "optional": true,
                "functions": [
                    {
                        "function": "resolveEntityIds"
                    }
                ]
            },
            {
                "sourcePath":
"$['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['perPersonUuid']",

"targetPath": "$['urn:sap:cloud:scim:schemas:extension:custom:2.0:User']
['attributes'][0]['value']",
                "optional": true
            },
            {

"targetPath": "$['urn:sap:cloud:scim:schemas:extension:custom:2.0:User']
['attributes'][0]['name']",
                "condition":
"$['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['perPersonUuid'] EMPTY false",
                "constant": "customAttribute1"
            },
            {
                "targetPath": "$.applicationId",
                "constant": "%ias.application.id.attribute%",
                "scope": "createEntity"
            },
            {
                "targetPath": "$.sendMail",
                "constant": "false",
                "scope": "createEntity"
            },
            {
                "targetPath": "$.sendMail",
                "condition": "$.userType == 'ONBOARDEE'",
                "constant": "true",
                "scope": "createEntity"
            },
            {
                "targetPath": "$.emailTemplateSetId",
                "condition": "$.userType == 'ONBOARDEE'",
                "ignore": true,
                "constant": "%ias.onboardee.email.template.id.attribute%",
                "scope": "createEntity"
            },
            {
                "targetPath": "$.mailVerified",
                "constant": "true",
```

```
                "scope": "createEntity"
            },
            {
                "targetPath": "$.mailVerified",
                "condition": "$.userType == 'ONBOARDEE'",
                "constant": "false",
                "scope": "createEntity"
            },
            {
                "targetPath": "$.passwordStatus",
                "constant": "disabled",
                "scope": "createEntity"
            },
            {
                "targetPath": "$.passwordStatus",
                "condition": "$.userType == 'ONBOARDEE'",
                "constant": "enabled",
                "scope": "createEntity"
            },
            {
                "targetPath": "$.password",
                "ignore": true,
                "constant": "%ias.initial.password.attribute%",
                "scope": "createEntity"
            },
            {
                "targetPath": "$.sourceSystem",
                "condition":
"$['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['loginMethod'] == 'PWD'",
                "ignore": true,
                "constant": "%ias.source.system.attribute%",
                "scope": "createEntity"
            },
            {
                "targetPath": "$.sourceSystemId",
                "condition":
"$['urn:ietf:params:scim:schemas:extension:successfactors:2.0:User']
['loginMethod'] == 'PWD'",
                "ignore": true,
                "constant": "%ias.source.system.id.attribute%",
                "scope": "createEntity"
            }
        ]
    },
    "group": {
        "mappings": [
            {
                "targetPath": "$.id",
                "sourceVariable": "entityIdTargetSystem"
            },
            {
                "sourcePath": "$.displayName",
                "targetPath": "$.displayName"
            },
            {
                "sourcePath": "$.displayName",
                "targetPath": "$
['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']['name']",
                "scope": "createEntity",
                "functions": [
                    {
                        "function": "replaceAllString",
                        "regex": "[\\s\\p{Punct}]",
                        "replacement": "_"
                    }
                ]
            },
```

```
            {
                "sourcePath": "$
['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']['name']",
                "targetPath": "$
['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']['name']",
                "optional": true,
                "scope": "createEntity"
            },
            {
                "sourcePath": "$
['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']['description']",
                "targetPath": "$
['urn:sap:cloud:scim:schemas:extension:custom:2.0:Group']['description']",
                "optional": true
            },
            {
                "sourcePath": "$.members[*].value",
                "targetPath": "$.members[?(@.value)]",
                "optional": true,
                "preserveArrayWithSingleElement": true,
                "functions": [
                    {
                        "function": "resolveEntityIds"
                    }
                ]
            }
        ]
    }
}
```

17. Reset Identity Provisioning for the current SAP SuccessFactors tenant Source System by following the steps in Reset Identity Provisioning System.

> ⚠ Caution
>
> This step is mandatory. If you skip it, Identity Provisioning may fail with errors such as **409 – Email address is already used for <ID>**. These errors occur because entities from the old OData configuration conflict with the new SCIM configuration.

> ⓘ Note
>
> For the relevant target systems (e.g. Identity Authentication and SAP Analytics Cloud) that would use the user data from SAP SuccessFactors, add the following property: *ips.delete.existedbefore.entities* with value **true**. This allows Identity Provisioning to delete users created before the reset.

18. Go to *Identity Provisioning* > *Source Systems* > *Jobs* > *(your SAP SuccessFactors source system)* and resume your scheduled sync jobs, or run a new *Read Job*, if you did not have one scheduled.

> ⓘ Note
>
> Please note that the sync job after the Reset will always be a full sync that covers all the users from the source. It takes more time.

Related Information

Setting Up SAP SuccessFactors as a Source System with Identity Provisioning with SCIM API Option

Mapping Between SCIM User and OData User

11.9.3 Running and Scheduling Jobs (User Sync)

When changes occur to your users data, a sync job synchronizes the changes to your system. Run sync jobs to load users into your Identity Authentication service, after editing the transformations (how data reads into the Identity Authentication service), anytime changes occur in your data.

Prerequisites

Ensure that you've performed the tasks in: **Setting up the Identity Provisioning Source and Target System**.

> ⓘ Note
>
> If you have both SAP SuccessFactors and Reporting, you'll want to configure both before running the user Re-Sync job.

Context

It's important that you set up user sync so that your users exist in the Identity Authentication service. User sync is critical when using the following services and features:

> ⚠ Caution
>
> - **Conditional Authentication:** To set up with rules that authenticate based on email, user type, or group.
> - **Reporting, Internal Career Site and other SAP SuccessFactors product areas:** User identifiers can change between product areas and the Identity Authentication service can only map these identifiers correctly when your users are in Identity Authentication.
> - **Global Assignment & Concurrent Employment:** when users log on from different sources, Identity Authentication needs to convert their identifiers so that Identity Authentication understands them. That only happens when user sync has been done and the users are loaded into Identity Authentication.
> - **Enablement of Partial SSO:** If you intend to user partial sso,your users should exist in Identity Authentication.
> - **Two-factor Authentication:** Your users need to exist in Identity Authentication so that you can take advantage of two-factor security features.

Run a provisioning job manually, or set a time interval for automatic (scheduled) jobs. Also, you can choose whether to run a complete read job or a synchronized one. The sync job reads and provisions only the new and updated entities.

If you have a large user population, this may take a long time. The jobs process is set up with basic transformations that load data for all users fromSAP SuccessFactors to the Identity Authentication tenant. You may want to modify these transformations before running the full reload or *Resync Job*. Common changes include syncing passwords

for migrating users and replacing blank or dummy email addresses with unique ones. Once the initial user load is completed, you will need to enable the job to run on a schedule.

Procedure

1. In the *Identity Provisioning Administration Console*, select *Source*.
2. From your *Source Settings*, select *Jobs*.
3. Choose a sync job.

   In the *Read Job* section you can do three things:
   - **Run Job**: This runs the delta job that finds changed records only.
   - **Schedule**: You can set the run schedule in minutes. If you schedule more than once a day, make the schedule long enough to insure each run completes before another starts.
   - **Pause/Resume**: Use this to stop and start the schedule.

   In the *Resync Job* section, you can choose *Run Now* to do a full reload.

> ⚠ Caution
>
> The **full reload** deletes any users that were previously loaded by this job but are not found in the current data. The **read job** deletes users if there's a change to the *sf.user.filter* setting, as suggested should be done for testing. If you test with one user and then test with another, the first will be deleted. Users manually added to the Identity Authentication tenant will never be deleted by the jobs process (an exception to this is if you set the property *ips.delete.existedbefore.entities = true* in the target system. For more information see **Manage Deleted Entities** under **Related Information** below).

> → Tip
>
> By default, only active users are synced to the Identity Authentication Service, so when an employee is deactivated or deleted in SAP SuccessFactors, the user will be deleted with the next *Resync Job* (full sync). However, you can decide to provision all the users (both active and inactive), so that once a user is deactivated in SAP SuccessFactors, they will also be deactivated in the Identity Authentication Service with the next sync, either by a *Run Job* (delta sync) or *Resync Job* (full sync). The full sync job keeps your source and target systems synchronized. To run a scheduled sync between your source and target systems, we recommend that you enforce full reads from time to time. To achieve this, you need to set up the following source system property: `ips.full.read.force.count`.
>
> For example, `ips.full.read.force.count=10` results in alternating full reads after every 10 delta reads are performed. This property only impacts scheduled runs; manually triggered runs are ignored.

> → Tip
>
> To ensure that inactive users are continually deleted in a timely manner, we suggest that you keep the following in mind:
> - Make sure to use the system property *sf.user.filter = status eq 'active'*. This way when a user becomes inactive, they will no longer be read by the Identity Provisioning job, and any record missing from the read will be deleted.

- In the *Resync Job*, use the property *ips.full.read.force.count = 1* to ensure that the job does a full read of **active** users each time a delta read is performed, and deletes the inactive users. Alternatively, you may also run the *Resync Job* manually for a full read of active users.
- Ensure that your job run is free of errors. If the particular error does not allow Identity Provisioning to properly calculate the entities that are no longer present in the source system, the delete operation will be skipped.
- Note that the same job that provisions a user in Identity Provisioning is also the one that is used to delete that same user. If a user from a previous job is made inactive, and a new job is created or the existing job is reset, it will not affect the users from the previous job, and they will not be deleted.
- If you create conditions within the Identity Provisioning *Target* or *Source* transformations, while they will cause **unprovisioned** users to be skipped that don't meet these conditions, users that have **already been provisioned**, but also do not meet these conditions will get deleted.

→ Tip

You can download the execution logs for all running jobs by navigating to *Job Logs* > *Down arrow icon (at the top-right of the screen)* > *Download* button on the *Download Execution Logs for All Jobs* modal. This feature also allows you to download all the execution logs in real-time while the jobs are still running.

Related Information

Manage Full and Delta Read
Manage Deleted Entities

11.10 Configure Single Sign-On in Admin Center

11.10.1 Manage SAML SSO Settings in SAP SuccessFactors

Use the Manage SAML SSO Settings (SAML 2.0 Single Sign-On) page in Admin Center to configure and maintain Identity Authentication SAML Single Sign-On (SSO) settings. This feature supports Identity Authentication in both proxy Identity Provider (IDP) and primary IDP scenarios. It enables customer admins to self-service core SAML SSO settings such as redirect URLs, identity provider metadata, and certificate renewals.

The Manage SAML SSO Settings screen provides a centralized interface for configuring SAML 2.0-based SSO between SAP SuccessFactors and Identity Authentication. It supports the following actions:

- View Identity Authentication corporate identity providers (IDPs)
- Maintain redirect URLs for login scenarios
- Download service provider (SP) metadata for Identity Authentication
- View options like Trust All Identity Providers and Case-Insensitive Usernames
- Launch the Identity Authentication Admin Console directly from the screen
- Enable Transactional Verification for critical transactions using multi-factor authentication (MFA)

- View SSO enablement settings such as *Enable SSO Authentication* and *Partial Organization SSO*

> → Remember
>
> This screen reflects Identity Authentication corporate identity provider configurations from the Identity Authentication tenant, but **only** if your SAP SuccessFactors company's SAML Issuer is set correctly in Provisioning. To view assertion records for a specific company, you must log in to SAP SuccessFactors using that company's Company ID, and ensure the SAML Issuer in Provisioning matches the Identity Authentication tenant.

The *Single Sign-On Configuration* section displays core SSO settings and related options, while corporate identity providers are displayed under a separate *Corporate IDPs* section. Admins can edit existing identity provider entries.

Single Sign-On Configuration Settings

Setting	Description
Enable SSO Authentication	Displays whether SSO authentication is enabled for the instance. This setting is shown as read-only on this page.
Partial Organization SSO	Controls whether specific users sign in using SSO or the SAP SuccessFactors login page (username and password). This setting is editable when applicable and read-only when not.
Trust All Identity Providers	Identity Authentication setting that allows IDP-initiated login from any configured corporate IDP or assertion party.
Enable Transactional Verification	Enables an additional verification step for critical transactions using multi-factor authentication (MFA) through Identity Authentication. When enabled, users performing critical actions are prompted for MFA verification. → Remember Before enabling this feature, ensure you've completed the prerequisite steps outlined in **Enable Transactional Verification for Critical Transactions Using Multi-Factor Authentication** in the **Related Information** section. ⓘ Note The transactional MFA check is currently supported for: • Updating payment information in Employee Central (primary scenario) • Registering new OpenID Connect (OIDC) clients in SAP SuccessFactors (optional scenario for testing MFA setup) For more information, refer to the *Related Information* section. Support for additional critical transactions are planned for future releases.

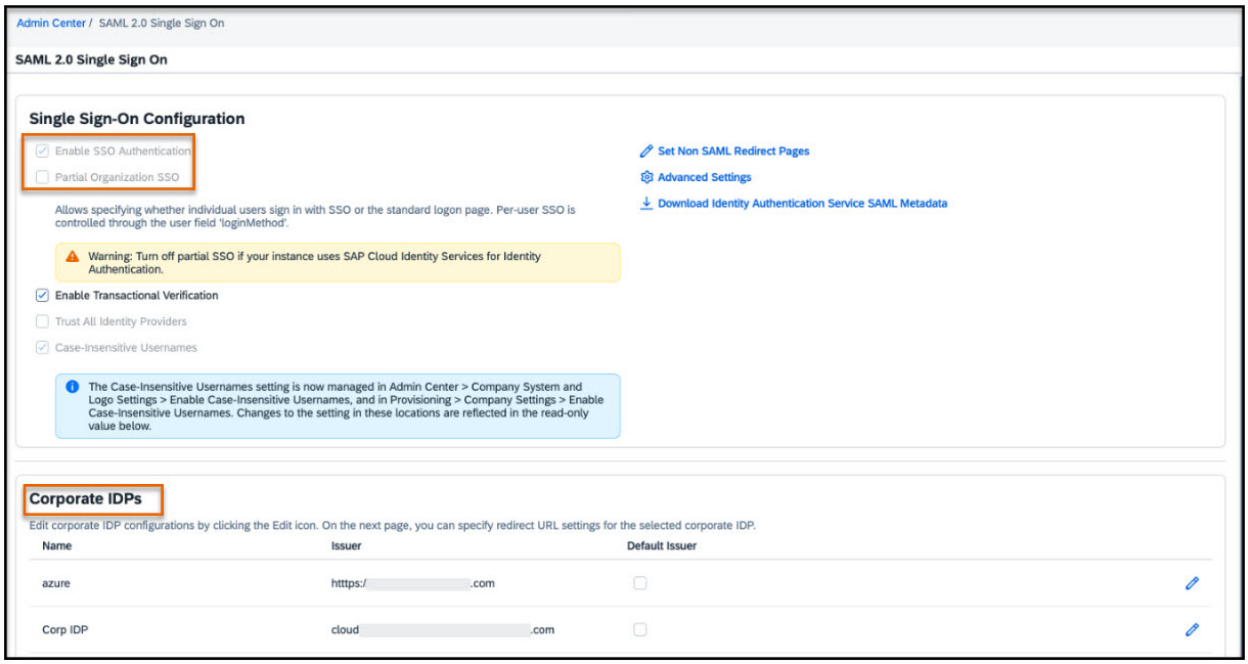
Setting	Description
Case-Insensitive Usernames	Feature that allows usernames to be validated without case sensitivity. It is shown as read-only on this page. Go to *Admin Center* > *Company and System Logo Settings* > to set this parameter. A message on the page indicates where this setting is managed. **→ Remember** For integration with Identity Authentication, this setting must be enabled, as the service only supports case-insensitive usernames. **ⓘ Note** If your system doesn't contain usernames that differ only by upper or lowercase letters (e.g., "John.Doe" vs. "john.doe"), SAP SuccessFactors will automatically turn on the case-insensitive setting for you.
Set Non-SAML Redirect Pages	Used for users who log in directly via the Identity Authentication login screen using credentials, rather than through an external corporate identity provider. **ⓘ Note** These settings are only applicable when Identity Authentication is acting as the main corporate IDP.
Advanced Settings	Opens the *SAP Cloud Identity Services* Identity Authentication admin console login page for further configuration of SAML settings and user attributes.
Download Service Provider Metadata	Downloads Identity Authentication service provider metadata for use when setting up trust in the *SAP Cloud Identity Services* Identity Authentication admin console.

The following columns appear in the *Corporate IDPs* section of the Manage SAML SSO Settings (SAML 2.0 Single Sign-On) page. They help identify corporate identity providers and route authentication through the correct configuration:

Corporate IDPs Columns

Column Name	Description
Name	A label to identify the corporate identity provider (IDP) configuration shown in the list. Used for internal reference and selection in the UI.
Issuer	The SAML Entity ID of the corporate identity provider. Whether Identity Authentication acts as the main IDP or as proxy, this value must match the *Name* field (Entity ID) defined in the SAML 2.0 Configuration of the relevant application in the Identity Authentication administration console. It determines where to route authentication requests.

Column Name	Description
Default Issuer	Designates this corporate IDP as the fallback for authentication requests that don't explicitly match another configured Issuer. Useful when multiple IDPs are present, and a default route is needed.



Enable Additional Settings

When you edit a corporate identity provider from the Manage SAML SSO Settings screen, a configuration view opens with additional sections:

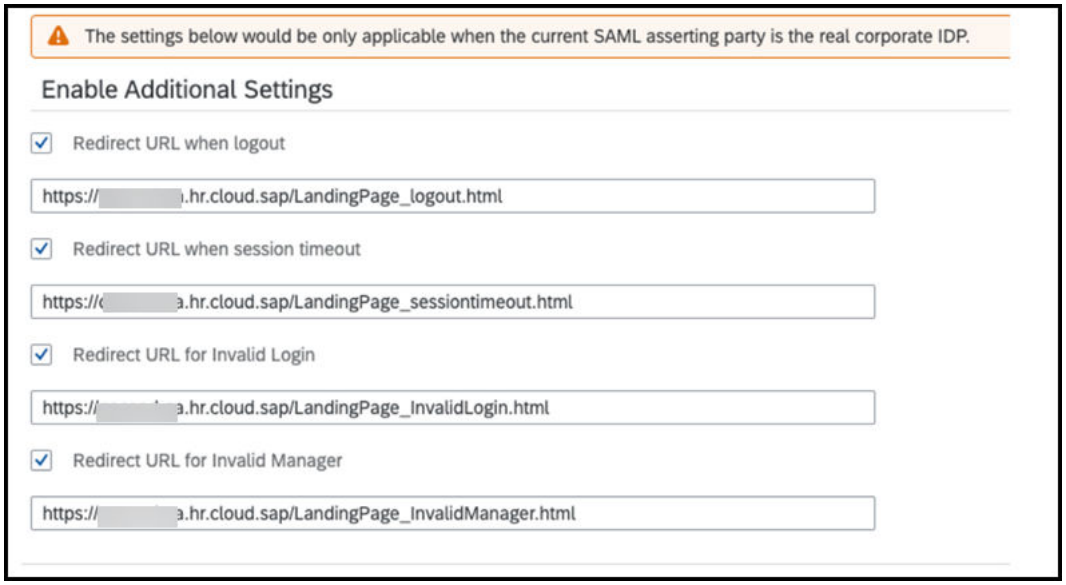
- **Base Configuration Settings**: Displays the same *SAML Asserting Party Name* and *SAML Issuer* information on the main screen.
- **Enable Additional Settings**: Allows you to configure redirect URLs that determine where users are sent after specific login-related events. These settings help improve the user experience by guiding users to appropriate landing pages when authentication issues occur:

> ### Note
>
> These settings are only applicable when Identity Authentication is acting as proxy to the real corporate IDP.

Enable Additional Settings

Setting	Description
Redirect URL when logout	Specifies where to redirect users after a logout.

Setting	Description
Redirect URL when session timeout	Defines the landing page users see when their session expires due to inactivity.
Redirect URL for Invalid Login	URL used when login fails due to incorrect credentials or unexpected authentication issues. Helps deliver a clear message or next steps.
Redirect URL for an Invalid Login Path by External Users	Used for scenarios where an external user attempts to log in via an invalid path (e.g., not authorized or misrouted). Directs them to a dedicated page explaining the issue.



Related Information

Public API to Retrieve New Customer SSO Certificate [page 124]

Enable Transactional Verification for Critical Transactions Using Multi-Factor Authentication [page 162]

Register Your Own Application to Communicate with SAP SuccessFactors HCM Suite with OpenID Connect [page 125]

11.10.1.1 Enable Transactional Verification for Critical Transactions Using Multi-Factor Authentication

Enable additional multi-factor authentication (MFA) verification for critical transactions in SAP SuccessFactors using Identity Authentication.

Prerequisites

- Your Identity Authentication tenant is already integrated with SAP SuccessFactors in SAP Cloud Identity Services. For more information, refer to **Checking to See if You Aready Have Identity Authentication Enabled** in the **Related Information** section.
- You have the *Manage SAML SSO Settings* permission.

Context

Enabling this feature prompts users to enter a one-time verification code from their registered TOTP authenticator app before completing a critical transaction. This adds an extra layer of protection to sensitive actions in your SAP SuccessFactors system.

Currently, the multi-factor authentication (MFA) prompt is supported for the following scenarios:

- Updating payment information in Employee Central
- Registering new OpenID Connect (OIDC) OAuth clients in Security Center, after the Application Map information is submitted

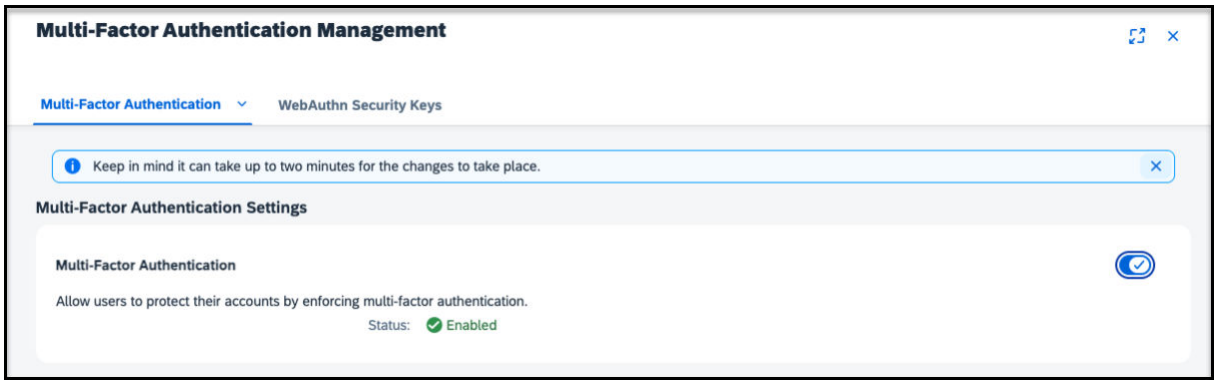
For more details, refer to the **Related Information** section.

> **Note**
>
> Only Identity Authentication is supported for this verification check, even when it's used as a proxy for a corporate identity provider.

Procedure

1. > **Note**
   >
   > The below steps will enable MFA at the Identity Authentication tenant level.

   Navigate to *SAP Cloud Identity Services* > *Identity Authentication* > *Applications & Resources* > *Tenant Settings* > *Authentication*.
2. Go to the *Multi-Factor Authentication Management* section and enable the *Multi-Factor Authentication* radio button to enable MFA for the Identity Authentication tenant.



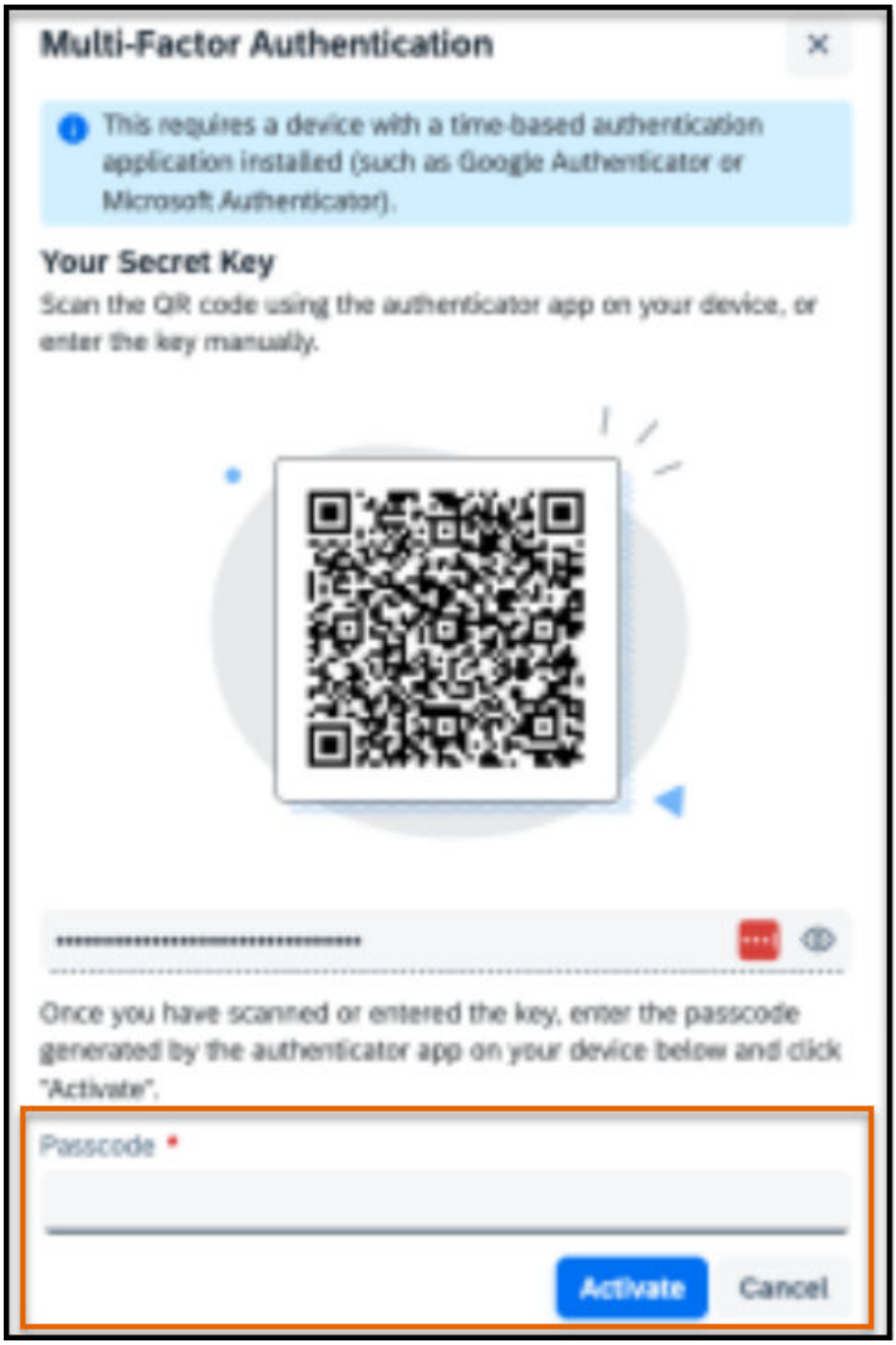
3. Note

   The below steps enable MFA for end users.

   Login to your Identity Authentication *User Profile Page* (e.g., `https://<IAS tenant>.accounts.ondemand.com/`) with a user account.

4. Next to *TOTP Two-Factor Authentication*, select *Activate*.

5. Using the authentication application on your mobile device, scan the QR code, enter the code from your authentication app, and click *Activate*.



6. Note

   Optional: Complete the following steps if you also want *Two-Factor Authentication* to always be required for the current user.

   Next to *Two-Factor Authentication*, select *Enable*.

7. Enter the MFA code from your authentication app to enable Two-Factor Authentication for all applications that this user would access via Identity Authentication.
8. > **Note**
   >
   > The below steps Enable MFA Transactional Verification in the Admin Center.

   Go to *Admin Center* > *Manage SAML SSO Settings*.
9. Select the *Enable Transactional Verification* setting.
10. Save your changes.

Results

Once enabled, a prompt appears asking users to enter a one-time verification code from their registered authenticator app whenever they perform a supported critical transaction. Examples include updating payment information in Employee Central or registering a new OpenID Connect client. The transaction proceeds only after successful verification.

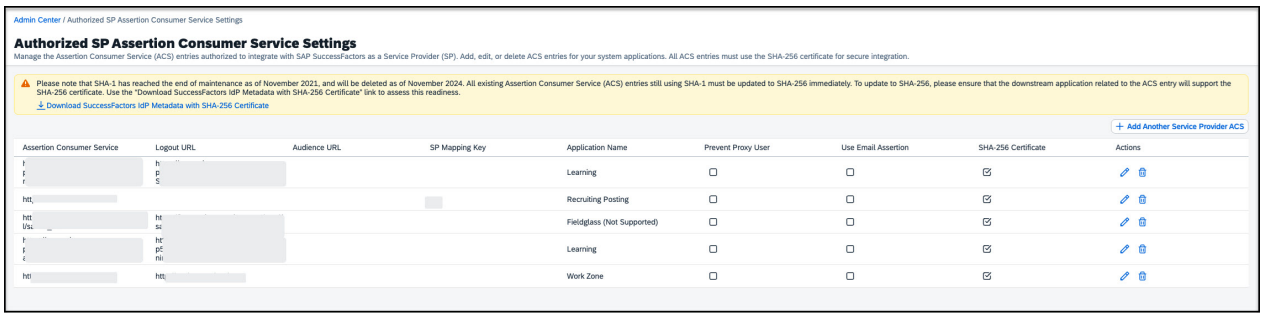
Related Information

Register Your Own Application to Communicate with SAP SuccessFactors HCM Suite with OpenID Connect [page 125]
Checking to See if You Already Have Identity Authentication Enabled [page 27]
(Recommended) Transactional MFA Check

11.10.2 Authorized SP Assertion Consumer Service Settings in SAP SuccessFactors

Use the *Authorized SP Assertion Consumer Service Settings* page in Admin Center to configure and maintain Assertion Consumer Service (ACS) records for SAML based single sign-on scenarios. This page enables administrators to fully manage ACS records directly in Admin Center without using Provisioning.

ACS records define the service provider endpoints that receive SAML assertions from an identity provider during authentication. These records are used to route authentication responses correctly for SAP SuccessFactors applications and supported integration scenarios.



What You Can Do on This Page

The *Authorized SP Assertion Consumer Service Settings* page provides a centralized interface for managing ACS records. Administrators can perform the following actions:

- View existing ACS records configured for the SAP SuccessFactors tenant
- Create new ACS records directly in Admin Center
- Edit supported fields for existing ACS records
- Delete ACS records that are no longer required

The page also includes built-in validations and guidance to help ensure that ACS entries are complete, correctly formatted, and unique.

> ### ⓘ Note
>
> For SAML based single sign-on (SSO) integrations, we recommend using Identity Authentication in SAP Cloud Identity Services as the primary identity provider for SAP SuccessFactors integrations and applications. To review details about the Identity Authentication tenant integrated with SAP SuccessFactors, including administrator information, see **Monitoring Tool for the Upgrade to Identity Authentication.** in the Related Information section.
>
> Using ACS records for SAML based SSO scenarios where SAP SuccessFactors acts as the identity provider has functional limitations because SAP SuccessFactors isn't intended to serve as a full featured identity provider. For example, these scenarios don't support advanced identity and access management capabilities such as multifactor authentication, conditional authentication policies, or risk based authentication rules.
>
> SAP SuccessFactors currently has no planned functional enhancements for these ACS based scenarios. Identity Authentication based integrations are the recommended approach for new implementations.

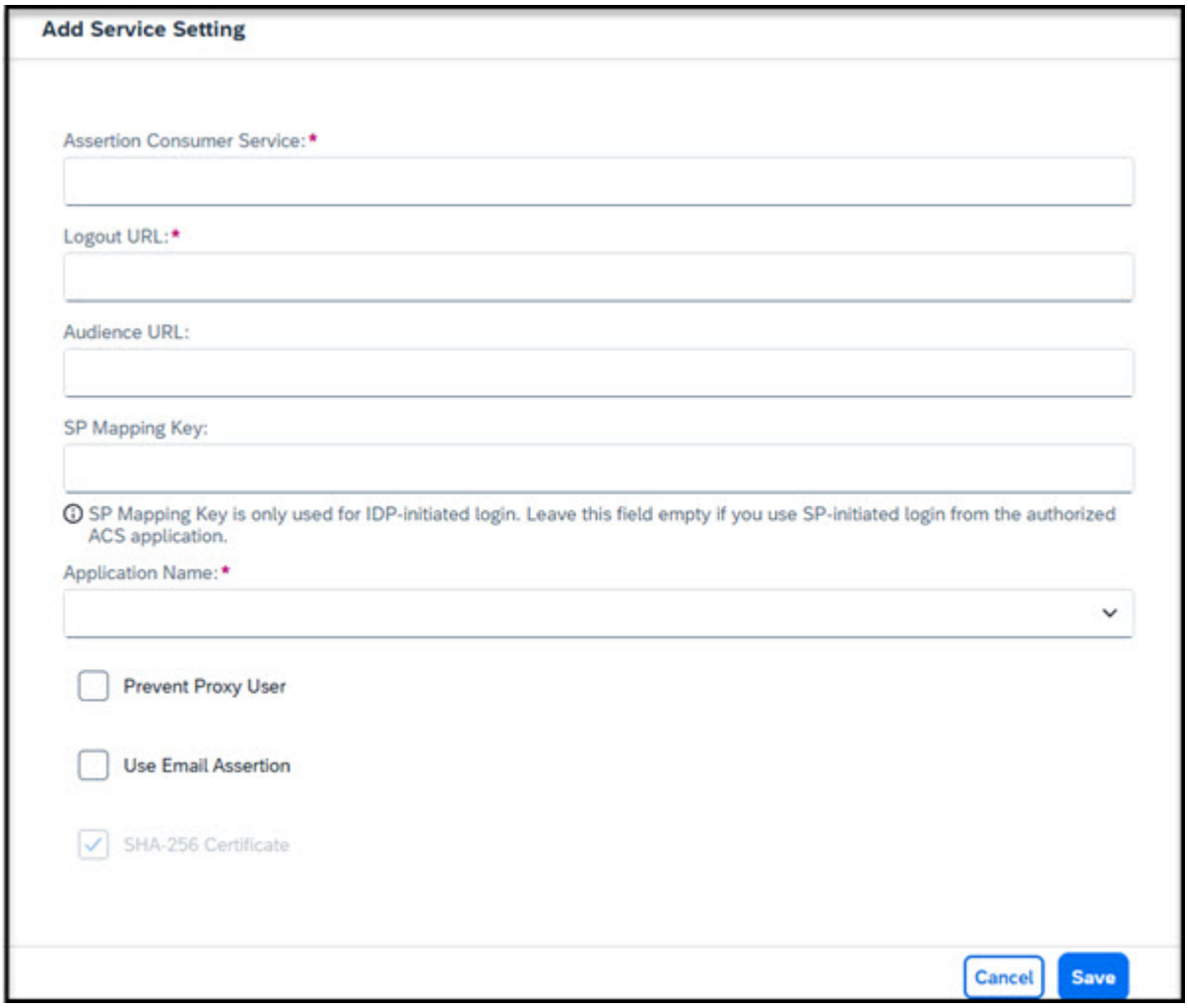
> ### → Remember
>
> Provisioning access is no longer required to create, edit, or delete Authorized Service Provider ACS records. All supported ACS management tasks can be completed from this page in Admin Center.

Maintain ACS Records in Admin Center

Based on these capabilities, you can perform the following tasks directly in Admin Center.

1. Go to *Admin Center* > *Authorized SP Assertion Consumer Service Settings*.
2. To create a new ACS record, choose *Add Another Service Provider ACS*.
3. Enter the required fields, such as *Assertion Consumer Service*, *Logout URL*, *Application Name* and provide additional details as needed.
4. Choose *Save*.

Add Service Setting Dialog



When creating a new ACS record, administrators use the *Add Service Setting* dialog, which guides them through required and optional fields, captures the information needed to define how SAML assertions are received and processed, and enforces validation rules to help prevent configuration errors.

Authorized SP Assertion Consumer Service Fields

The following fields are available when creating or editing an ACS record.

Field Name	Description
Assertion Consumer Service	URL endpoint that receives SAML assertions from the identity provider
Logout URL	Endpoint used for single logout scenarios
Audience URL	Audience restriction value used to validate SAML assertions
SP Mapping Key	Used for identity provider initiated login scenarios to route authentication correctly
Application Name	Identifies the SAP SuccessFactors application associated with the ACS record
Prevent Proxy User	Restricts the use of proxy access for the ACS entry

Field Name	Description
Use Email Assertion	Uses the email address as the user identifier in the SAML assertion
SHA 256 Certificate	Indicates whether the SHA 256 certificate is applied to the ACS record

Validation and Limits

The page enforces the following rules to ensure consistent and supported configurations:

- Required fields must be completed before saving
- URLs are validated for correct format
- ACS names must be unique within the tenant
- A maximum of 20 ACS records can be created per tenant

If more than 20 ACS records exist, administrators can continue to edit existing records but cannot create additional ones.

11.10.3 Opening the Identity Authentication Administration Console in SAP Cloud Identity Services

Navigate from the SAP SuccessFactors *SAML 2.0 Single Sign On* page to the Identity Authentication administration console so that you can configure advanced SAML SSO settings.

Prerequisites

- You have an Identity Authentication service tenant and SAML trust is set up between it and your SAP SuccessFactors system.
- You have the *Manage SAML SSO Settings* permission.

Procedure

1. Go to *Admin Center* > *Tools* > *SAML 2.0 Single Sign On*.
2. Click *Advanced Settings*.

Results

The Identity Authentication administration console opens in a new tab in your browser.

Related Information

Default Configuration of Identity Authentication with SAP SuccessFactors [page 50]
Opening the Identity Authentication Administration Console in SAP Cloud Identity Services [page 168]
More about SAP Cloud Identity Services - Identity Authentication Service

11.10.3.1 Configure Your Corporate Identity Provider

Configure your corporate identity provider with service provider metadata from the SAP Cloud Identity Services - Identity Authentication service.

Prerequisites

- Your SAP SuccessFactors system is connected to the Identity Authentication service.
- You have the *Manage SAML SSO Settings* permission.

Context

This is the first step in the process of setting up single sign-on for SAP SuccessFactors with Identity Authentication service. In this step, you are setting up Identity Authentication as the service provider that is configured in your corporate identity provider. Configuration is done by the administrator of your corporate identity provider.

About Corporate Identity Providers in the Identity Authentication service

Procedure

1. Download service provider metadata for your Identity Authentication tenant:
   a. Go to *Admin Center* > *Manage SAML SSO Settings*.
   b. Click *Download Identity Authentication Service SAML Metadata*.
2. Register Identity Authentication service as a service provider for your corporate identity provider.

   > → Tip
   >
   > For information about how to do this, consult documentation of your corporate identity provider.

3. (Optional) If you are using IdP-initiated SSO, add the `sp=<sp_name>` parameter to the assertion consumer service (ACS) endpoint URL in your corporate identity provider, replacing the `sp_name` with the `Entity ID` of your Identity Authentication service tenant.

This parameter is needed for Identity Authentication to know where to redirect the user to after successful authentication.

> → Tip
>
> The ACS endpoint URL should have the following format: `https://<the current ACS endpoint URL>?sp=<sp_name>`.
>
> How to request the Entity ID of the service provider from the tenant administrator of Identity Authentication.

4. Configure your corporate identity provider to send the `Name-ID` and `NameIDFormat` that are expected by SAP SuccessFactors:

   `Name-ID`: username

   `NameIDFormat`: unspecified

> ⓘ Note
>
> If it is not possible to send this information to SAP SuccessFactors and the attributes should be modified by Identity Authentication, you should enable *Identity Federation*.
>
> More about Identity Federation.

> → Remember
>
> When enabling *Identity Federation* with SAP SuccessFactors, make sure that you've also enabled the *Use Identity Authentication user store* option. This step is necessary to ensure that the data for users stored in the Identity Authentication user store are taken and their attributes are sent to the application.

5. Use the following fields in the *SAML Single Sign On* > *Edit icon* > *Enable Additional Settings* section to redirect URLs based on different scenarios:

> → Remember
>
> The following fields are only applicable when Identity Authentication is enabled and acting as a proxy IdP for your Corporate IdP.

Field	Description
Redirect URL when logout	Enter the URL of the page users should see when they logout of the service provider.
Redirect URL when session timeout	Enter the redirect URL when the session times out.
Redirect URL for Invalid Login	Enter the URL for Invalid Login URL redirect.
Redirect URL for Invalid Manager	Enter the URL for Invalid Manager URL redirect.

Next Steps

Proceed to add your corporate identity provider (IdP) as an asserting party to the Identity Authentication service.

11.10.3.2 Adding an Asserting Party

Add your corporate identity provider (IdP) as an asserting party to the Identity Authentication service.

Prerequisites

> **Note**
>
> We are requesting for all systems to be migrated to Identity Authentication by November 2026. For details about this migration refer to Guidance on Migrating to Identity Authentication in SAP Cloud Identity Services

- You have configured your corporate identity provider with service provider metadata from the Identity Authentication service.
- You have SAML metadata for your corporate identity provider. If you do not have this, contact the administrator of your corporate identity provider.

Context

This is a necessary step in the process of setting up single sign-on for SAP SuccessFactors with the Identity Authentication service. In this step, your corporate identity provider is the asserting party that is configured in Identity Authentication.

You can complete this task from the Identity Authentication administration console. Refer to **Configure Trust with SAML 2.0 Coprporate Identity Provider** in the **Related Information** section.

> **Restriction**
>
> It is important that Identity Authentication is the **only** SAML asserting party that is enabled after you've activated your upgrade to Identity Authentication. If you add more than one asserting party, that's not Identity Authentication, we recommend that you do **not** enable it. If you enable multiple asserting parties, you will not be able to upgrade to Story Reports.

Next Steps

Configure user groups and authentication rules in the Identity Authentication administration console to determine which users are sent to single-sign on.

If you choose, you can also configure additional SSO configuration options.

Related Information

Opening the Identity Authentication Administration Console in SAP Cloud Identity Services [page 168]
Configure Trust with SAML 2.0 Corporate Identity Provider

11.10.3.3 Additional Single Sign-On Configurations

Additional single sign-on options can be configured in the SAP Cloud Identity Services - Identity Authentication administration console.

Here are some common use cases and links to relevant documentation.

Use Case	Documentation
Set up authentication rules for sending users to corporate IdP or for multiple asserting party selection.	Conditional Authentication
Set up authentication rules for sending users to two-factor/token authentication, password-based login, or other login options.	Risk Based Authentication
Have the Identity Authentication service send a different value to SAP SuccessFactors than it used to authenticate the user. For example, Identity Authentication can contain a login using an email address but send SAP SuccessFactors the login name for that user.	Name ID Settings
Add asserting parties using Metadata Import in the Identity Authentication Administration Console, instead of using the SAP SuccessFactors *SAML 2.0 Single Sign On* page.	Configure Trust with Corporate IdP

Related Information

Opening the Identity Authentication Administration Console in SAP Cloud Identity Services [page 168]

11.10.4 Single Sign-On without SAP Cloud Identity Services - Identity Authentication

To configure single sign-on **without** SAP Cloud Identity Services - Identity Authentication, using other authentication services or identity providers, use the Provisioning application.

> → Remember
>
> 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.

⚠ Caution

We strongly advise against using the **Business Execution Suite Provisioning** platform as the identity provider by which you authenticate to SAP SuccessFactors, as this method of authentication is not supported by engineering or Technical Support, and is planned to be deprecated in the future.

Please also note that on this platorm, applications in the *Application Name* field that fall under the *Other Application* category are also not supported by engineering or Technical Support.

To avoid authentication issues, we recommend that you use SAP Cloud Identity Services - Identity Authentication as your solution for authentication instead.

⚠ Caution

Please note that any direct integration between SAP SuccessFactors and corporate identity providers (IDP) will be deprecated. Customers currently using corporate IDP directly with SAP SuccessFactors are required to migrate to Identity Authentication, with this service acting as a proxy to the corporate IDP.

Additionally, the creation of new corporate IDP to SAP SuccessFactors direct integrations in Provisioning is no longer supported. To ensure compliance and proper integration, please integrate with Identity Authentication first, and then connect your corporate IDP to Identity Authentication as a proxy.

Change History

Learn about changes to the documentation for setting up SAP SuccessFactors with SAP Cloud Identity Services - Identity Authentication service and Identity Provisioning service in recent releases.

1H 2026

Type of Change	Description	More Info
Change	Updated the "SP Sign Logout" value to "Yes" on the "Default SAP SuccessFactors Provisioning SSO Settings in Provisioning" section.	Default Tenant Configurations for HCM Suite and Identity Authentication [page 68]

2H 2025

Type of Change	Description	More Info
Change	Added information about user identity synchronization based on the user account record.	Getting Started with Identity Authentication and SAP SuccessFactors [page 33]
Change	Added information about case-insensitive username behavior in Identity Authentication and SAP SuccessFactors	Default Configuration of Identity Authentication with SAP SuccessFactors [page 50] Important Notes About Using SAP SuccessFactors with Identity Authentication [page 5]
Change	Added information about automatically created technical administrator accounts in Identity Authentication.	Default Tenant Configurations for HCM Suite and Identity Authentication [page 68]
Change	Renamed the old “Setting Up an API User for Sync Jobs in SAP SuccessFactors” topic to “Manage Allowed IP Address Ranges for Identity Authentication API Calls” and clarified that IP ranges must be configured even if IPSADMIN is no longer used. Added a caution about selecting the correct regional ranges.	Manage Allowed IP Address Ranges for API Integration [page 39]

Type of Change	Description	More Info
New	Added “Default Authentication Setup Between Identity Authentication and SAP SuccessFactors” to describe the current setup using X.509 certificates (mTLS + SCIM) and the technical user automatically added in Identity Authentication.	Default Authentication Setup Between Identity Authentication and SAP SuccessFactors [page 35]
New	Added “First Time Login Experience for Migrated Users” to explain how users previously using SSO or SAP SuccessFactors username/password authenticate after IAS migration.	First Time Login Experience for Migrated Users [page 50]
Change	We added a note to the "Login Name" row to clarify when a different user is required for integrations.	Initiating the Upgrade to Identity Authentication in SAP Cloud Identity Services [page 40]
Change	We updated step 5 for the initial upgrade and remap topics to add details about the new "Ownership" field that displays on each upgrade dialog.	Initiating the Upgrade to Identity Authentication in SAP Cloud Identity Services [page 40] Remapping an Identity Authentication Tenant [page 79]
Change	Added new Employee user type to the real time sync setup.	Manage Real-Time Sync of Users from SAP SuccessFactors to Identity Authentication with Identity Provisioning [page 84]
New	We added a new topic for enabling transactional verification using Multifactor Authentication.	Manage SAML SSO Settings in SAP SuccessFactors [page 157]
Change	We added details about the new display of SAML assertion party information on the Monitoring Tool page.	Monitoring Tool for the Upgrade to Identity Authentication [page 44]
Change	We added default configurations for SAP SuccessFactors as a source system in Identity Provisioning.	Identity Provisioning Service Administration Console Tasks [page 135]

1H 2025

Type of Change	Description	More Info
Changed	We added a note to the Prerequisites section with guidance on how to confirm if your SAP SuccessFactors appplication is already set up with OpenID Connect. We added steps for verifying Grant Types, selecting the JSON Web token, and references to perform API testing using OpenID Connect.	Register Your Own Application to Communicate with SAP SuccessFactors HCM Suite with OpenID Connect [page 125]
Changed	We added cautions to warn against performing the upgrade to the SCIM connector if SAP SuccessFactors post refresh activities haven't been completed, or existing user sync jobs are still running.	Upgrade from ODATA Identity Provisioning Connector to SCIM Connector with SAP SuccessFactors [page 139]
Changed	We updated old references of "Source System" to "Authentication Provider(s)" in reference to the *SAP Cloud Identity Services* > *Identity Providers* > *Authentication Providers* area of the Identity Authentication admin console.	
Changed	• We updated the path to the "Access to X.509 Certificate Mapping" permission. • We added "Business Data Cloud" as an application that is supported for making incoming calls to SAP SuccessFactors using X.509 authentication.	Upgrade from ODATA Identity Provisioning Connector to SCIM Connector with SAP SuccessFactors [page 139] Upgrade to X.509 Certificate-Based Authentication for Incoming Calls [page 36]
Changed	We added a reference to enabling Alumni access and configuring the Identity Authentication email template.	Authenticating New Hires with Identity Authentication in SAP Cloud Identity Services [page 82]
New	We added a new topic to cover the different migration sceanrios in Identity Authentication	Handling Customer Migration Scenarios in Identity Authentication [page 10]
Changed	We added a Caution note to remind users to update their SAP SuccessFactors SSO Certificate before checking the SSO Certificate Renewed box on the Manage SAML SSO Settings page.	Public API to Retrieve New Customer SSO Certificate [page 124]
Changed	We updated the Monitoring Tool details to reflect the new changes to the UI.	Monitoring Tool for the Upgrade to Identity Authentication [page 44]
Changed	We added additional considerations before performing a remap of your SAP SuccessFactors tenant to a new Identity Authentication tenant.	Remapping an Identity Authentication Tenant [page 79]

Type of Change	Description	More Info
Changed	We added a waring about the deprecation of corporate IDP direct integration with SAP SuccessFactors.	Single Sign-On without SAP Cloud Identity Services - Identity Authentication [page 172]

2H 2024

Type of Change	Description	More Info
Changed	We updated the "Information Exchanged to Set Up SAML2" section and referenced a topic for the API to retrieve the SAP SuccessFactors metadata file.	SAP SuccessFactors SAML 2.0 Technical Details [page 19]
Changed	We added a topic "Default Tenant Configurations for HCM Suite and Identity Authentication".	Default Tenant Configurations for HCM Suite and Identity Authentication [page 68]
Changed	We updated the "Caution" note to warn against manual user creation in Identity Authentication.	Default Configuration of Identity Authentication with SAP SuccessFactors [page 50]

1H 2024

Type of Change	Description	More Info
New	We created a new topic "Existing Customers (Before December 9,2022) Start Here".	Existing Customers (Before December 9, 2022) Start Here [page 30]
New	We created a new topic "Checking to See If You Already Have Identity Authentication Enabled".	Checking to See if You Already Have Identity Authentication Enabled [page 27]
Change	We added a Remember note to clarify how the Monitoring Tool displays the status and URL for the Upgrade and Change processes.	Monitoring Tool for the Upgrade to Identity Authentication [page 44]
Change	We restructured the Table of Contents for better navigation.	
Change	We added the path for the transformation code.	Define SendMail Transformation [page 102] Define PasswordStatus Transformation [page 103]
Change	We added the transformations produced by the Upgrade CenteSAP SuccessFactorsr for and Identity Authentication	Configure Transformations in Identity Provisioning [page 89]

Type of Change	Description	More Info
Change	We've added the default transformations for provided by Identity Provisioning for SAP SuccessFactors and Identity Authentication	Default Configuration of Identity Authentication with SAP SuccessFactors [page 50]
February 6, 2024		
Change	We updated references to "IAS" with Identity Authentication.	
January 24, 2024		
Changed	We fixed an invalid character ” in the sample code for "loginMethod" and updated it to correctly display as ".	Group Users Based on Login Method [page 111]
January 19, 2024		
Changed	We added to the last sentence of the note, a reminder to check the "Automatic Renewal" feature to ensure certificate automatic regeneration.	Upgrade to X.509 Certificate-Based Authentication for Incoming Calls [page 36]
January 9, 2024		
Changed	We updated the section "Relay State" and added a link to examples of valid RelayState values.	SAP SuccessFactors SAML 2.0 Technical Details [page 19]
January 10, 2024		
Changed	We added transformations code for SAP SuccessFactors, as they are different from the default transformations provided by Identity Provisioning Service.	Upgrade from ODATA Identity Provisioning Connector to SCIM Connector with SAP SuccessFactors [page 139]

2H 2023

Type of Change	Description	More Info
November 9, 2023		
Changed	We removed the note under "step 6" and added a note advising that the real-time sync instructions pertain to tenants under the "SAP Cloud Identity Services" environment. We also added a link to the steps to perform the migration from the Neo environment to the "SAP Cloud Identity Services" infrastructure.	Manage Real-Time Sync of Users from SAP SuccessFactors to Identity Authentication with Identity Provisioning [page 84]
November 8, 2023		

Type of Change	Description	More Info
Changed	We updated the "Invalid Manager" and description use-case to "Invalid Login Path by External Users".	SAP SuccessFactors Implementation of SAML 2.0 [page 16]
October 13, 2023		
Changed	We added SCIM API examples for setting up default passwords.	Set Up Default Passwords Using Transformations [page 104]
September 18, 2023		
Changed	We updated the Identity Authentication overview video.	Overview of the SAP SuccessFactors and Identity Authentication Service Integration (Video) [page 31]
September 11, 2023		
Changed	We added an FAQ section to the **Manage Real-time Sync of New Hires from SAP SuccessFactors to Identity Authentication with Identity Provisioning** topic.	Manage Real-Time Sync of Users from SAP SuccessFactors to Identity Authentication with Identity Provisioning [page 84]
August 18, 2023		
Changed	We added a topic with public API information to retrieve service provider metadata.	Public API to Retrieve Customer SSO Service Provider Metadata [page 122]
May 11, 2023		
Changed	We have moved the Change History to the end of the guide.	Overview of the SAP SuccessFactors and Identity Authentication Service Integration (Video) [page 31]

1H 2023

Type of Change	Description	More Info
April 11, 2023		
Change	Added note that real-time sync steps need to be redone if you've upgraded from the **SAP BTP, Neo environment** to the **SAP Cloud Identity infrastructure**.	Manage Real-Time Sync of Users from SAP SuccessFactors to Identity Authentication with Identity Provisioning [page 84]
March 29, 2023		
Change	Added note that its possible to download job execution logs while the jobs are still running.	Running and Scheduling Jobs (User Sync) [page 155]
March 28, 2023		
Change	Added note to *Valid Until* field as a reminder to extend the expiration date before the certificate expires.	Manage Real-Time Sync of Users from SAP SuccessFactors to Identity Authentication with Identity Provisioning [page 84]

Type of Change	Description	More Info
March 20, 2023		
Change	Updated note to point to new Identity Provisioning documentation on adding user groups when the SCIM API Version 2 is in use.	Group Users Based on Login Method [page 111]
January 30, 2023		
Change	• Updated note to include information about how to update the *Password Validation URL* field when using X.509 certificate authentication. • Updated the Identity Authentication Upgrade Video.	Migrating Passwords from SAP SuccessFactors to Identity Authentication in SAP Cloud Identity Services [page 98] Step-by-Step Upgrade of SAP SuccessFactors to Identity Authentication (Video) [page 32]
January 20, 2023		
Change	Updated step 5 referencing login names needing to be an exact match to the username including case, to include the exception for when *Non Case Usernames* is selected in the *Manage SAML SSO Settings* page.	Adding Users to the SAP Cloud Identity Services - Identity Authentication Service [page 116]
January 19, 2023		
Change	• Updated **Upgrade to X.509 Certificate-Based Authentication for Incoming Calls**. Added note to *Login Name* field advising that this field is optional for the Identity Authentication and Identity Provisioning applications. • Updated **Setting Up the Identity Provisioning Source and Target Systems**. Added note that steps 5 and 6 are not applicable when using X,509 certificate-based authentication.	Upgrade to X.509 Certificate-Based Authentication for Incoming Calls [page 36] Setting Up the Identity Provisioning Source and Target Systems [page 137]
January 18, 2023		

Type of Change	Description	More Info
Change	• Updated Step 3 on **Authenticating New Hires with SAP Cloud Identity Services - Identity Authentication** to instruct users to click on the button *Apply to both Employee and Onboardee* and updated note to advise that manual migration from OData to SCIM API is now available. • Added note to **Migrating Passwords from SAP SuccessFactors to the SAP Cloud Identity Services - Identity Authentication** with a reminder to follow steps to upload the X.509 certificate after generating it in the Identity Authentication admin console. • Updated **When to Use SAP SuccessFactors with SAP Cloud Identity Services - Identity Authentication** with additional scenarios for when you would want to set up SAP SuccessFactors with Identity Authentication. • Updated **Default Configuration of Identity Authentication Service with SAP SuccessFactors** to emphasize that Identity Authentication is the default identity provider for single-sign on with SAP SuccessFactors. • Updated Tip on **Set Up Default Passwords Using Transformations** to include both the OData and SCIM API. • Updated Tip on **Group Users Based on Login Method** to include both the OData and SCIM API.	Authenticating New Hires with Identity Authentication in SAP Cloud Identity Services [page 82] Migrating Passwords from SAP SuccessFactors to Identity Authentication in SAP Cloud Identity Services [page 98] When to Use SAP SuccessFactors with Identity Authentication [page 4] Default Configuration of Identity Authentication with SAP SuccessFactors [page 50] Set Up Default Passwords Using Transformations [page 104] Group Users Based on Login Method [page 111]
January 13, 2023		
Change	Added to Tip to advise that default transformations in Identity Provisioning can be viewed in the Identity Provisioning help guide, with link to the guide.	Configure Transformations in Identity Provisioning [page 89]
January 11, 2023		
Change	Added to Tip to advise that default transformations in Identity Provisioning can be viewed in the Identity Provisioning help guide, with link to the guide.	Configure Transformations in Identity Provisioning [page 89]
January 3, 2023		

Type of Change	Description	More Info
Change	Added note recommending the upgrade to mTLS authentication and SCIM API integration as an easier alternative to setting up the IPSADMIN user.	Manage Allowed IP Address Ranges for API Integration [page 39]

2H 2022

Type of Change	Description	More Info
December 29, 2022		
Change	Added note advising that mTLS authentication and SCIM API integration are automatically applied to remapped Identity Authentication tenants.	Remapping an Identity Authentication Tenant [page 79]
December 13, 2022		
New	Created new topic **Scenarios for Existing Customers with Identity Authentication Already Enabled**	Scenarios for Existing Customers with Identity Authentication Automatically Enabled [page 31]
December 12, 2022		
Change	Removed topic **Uploading Asserting Party**, since the option to use this setting has been deprecated.	
December 6, 2022		
Change	Added notes advising that new customers after December 3, 2022 will already have Identity Authentication/Identity Provisioning enabled with mTLS and SCIM API integration, with an option to also authenticate employees and new hires with Identity Authentication.	Initiating the Upgrade to Identity Authentication in SAP Cloud Identity Services [page 40]
December 1, 2022		
New	Added new topic **Manage Real-Time Sync of New Hires from SAP SuccessFactors to Identity Authentication with Identity Provisioning**	Manage Real-Time Sync of Users from SAP SuccessFactors to Identity Authentication with Identity Provisioning [page 84]
November 29, 2022		
Change	Added note recommending the upgrade to mTLS authentication between Identity Authentication and SAP SuccessFactors.	SAP Cloud Identity Services Administration Console Tasks [page 113]
November 26, 2022		

Type of Change	Description	More Info
Change	Added reminders that new customers after December 3, 2022 already have Identity Authentication and Identity Provisioning enabled and do not need to complete manual upgrade steps to obtain Identity Authentication or use IPSADMIN user with Identity Provisioning.	Identity Provisioning Service Administration Console Tasks [page 135]
November 23, 2022		
Change	Added note pointing customers with newly created SAP SuccessFactors HCM suite tenants to instructions to get started.	Getting Started with Identity Authentication and SAP SuccessFactors [page 33]
November 23, 2022		
New	Added new topic **Getting Started with Identity Authentication Aready Enabled with SAP SuccessFactors HCM suite**	Getting Started with Identity Authentication Already Enabled [page 28]
November 16, 2022		
Change	Added note with reminder to enable the *Identity Authentication user store* when setting up **Identity Federation**	Configure Your Corporate Identity Provider [page 169]
November 15, 2022		
Change	Added description of URL redirect fields in the *Manage SAML SSO Settings* > *SAML Single Sign On* > *Enable Additional Settings* section.	Configure Your Corporate Identity Provider [page 169]
September 22, 2022		
Change	Added note linking to KBA for troubleshooting S-User validation errors.	Initiating the Upgrade to Identity Authentication in SAP Cloud Identity Services [page 40] Remapping an Identity Authentication Tenant [page 79]
August 3, 2022		
Change	Added note advising of scenarios when time stamps and **More Information** section on the Monitoring Tool will not display data.	Monitoring Tool for the Upgrade to Identity Authentication [page 44]
August 1, 2022		

Type of Change	Description	More Info
Change	Removed steps to add Corporate IDP as an asserting party from **Manage SAML SSO Settings** page, as this option has been deprecated. Updated topic with note to complete this task from the Identity Authentication administration console.	Adding an Asserting Party [page 171]
June 30, 2022		
New	Added topic **Upgrade to X.509 Certificate-Based (mTLS) Authentication in SAP SuccessFactors**	Upgrade to X.509 Certificate-Based Authentication for Incoming Calls [page 36]
June 10, 2022		
New	Added topic **Authenticating New Hires with SAP Cloud Identity Services - Identity Authentication**	Authenticating New Hires with Identity Authentication in SAP Cloud Identity Services [page 82]

1H 2022

Type of Change	Description	More Info
June 12, 2022		
Change	Added missing comma and quotation mark to JSON code samples	Group Users Based on Login Method [page 111]
June 4, 2022		
Change	Added note to topic Setting Up an API User for Sync Jobs in SAP SuccessFactors advising which IP ranges to check based on whether Identity Authentication and Identity Provisioning infrastrucures are using the same environment.	Manage Allowed IP Address Ranges for API Integration [page 39]
February 14, 2022		

Type of Change	Description	More Info
Change	Updated topic Monitoring Tool for the Upgrade to SAP Cloud Identity Services-Identity Authentication • Added clear path to the Monitoring Tool • Added note explaining the way that tenant urls and upgrade processes are displayed in the monitoring tool. • Added link to SAP blog with instructions for customers to view all of their Identity Authentication/Identity Provisioning tenants.	Monitoring Tool for the Upgrade to Identity Authentication [page 44]
Februrary 11, 2022		
Change	Updated topic Initiating the Upgrade to SAP Cloud Identity Services - Identity Authentication Service • Corrected UI label name for button to Request New Tenant in step 5 • Added to Caution note the recommendation to avoid using the same Identity Authentication Service tenant for multiple SAP SuccessFactors tenants • Added clear path to the Monitoring Tool	Initiating the Upgrade to Identity Authentication in SAP Cloud Identity Services [page 40]
Februrary 3, 2022		
Change	Updated procedure step 2 to reflect the current UI label Change SuccessFactors Identity Authentication Service Integration	Remapping an Identity Authentication Tenant [page 79]
January 20, 2022		
Change	Updated the topic Initiating the Upgrade to SAP Cloud Identity Services - Identity Authentication Service • Updated procedure step 2 to reflect the current UI label SAP Cloud Identity Services Identity Authentication Service Integration • Added new screenshot to step 5 reflecting the current UI label Upgrade to Initiate the Identity Authentication Service Integration.	Initiating the Upgrade to Identity Authentication in SAP Cloud Identity Services [page 40]
January 10, 2022		

Type of Change	Description	More Info
Change	Updated the topic Testing and Activating the Upgrade to SAP Cloud Platform Identity Services - Identity Authentication • Updated procedure steps to clarify that the option to test the migration follows the activation confirmation prompt. • Added new screenshot for the activation confirmation pop up.	Testing and Activating the Upgrade to Identity Authentication [page 47]

2H 2021

Type of Change	Description	More Info
November 22, 2021		
New	Added the topic remapping an Identity Authentication Tenant	Remapping an Identity Authentication Tenant [page 79]

1H 2021

> **Note**
>
> Refer to the Related Information links below to view all updates to these products:
>
> - SAP Cloud Identity Services - Identity Authentication
> - SAP Cloud Identity Services - Identity Provisioning

Type of Change	Description	More Info
June 25, 2021		
Change	This topic was removed, but the content was added to an existing topic within the same guide. • Removed: Implementing Single Sign-On After Upgrading • Content added to: Partial Single Sign-On (SSO) Login Using a Single Corporate Identity Provider (IdP)	Partial Single Sign-On (SSO) Login Using a Single Corporate Identity Provider (IdP) [page 109]
Change	A KBA has been added in the Option A section.	Partial Single Sign-On (SSO) Login Using a Single Corporate Identity Provider (IdP) [page 109]

Type of Change	Description	More Info
June 4, 2021		
Added	A note is added to describe a change that will be rolled out, after the 1H 2021 Production Release. The SAML 2.0 Configuration Signing Option will be set to SHA-256.	SAP Cloud Identity Services Administration Console Tasks [page 113]
May 21, 2021		
Change	This guide has been updated to reflect the new names for these SAP products: • SAP Cloud Identity Services - Identity Authentication service (previously, SAP Cloud Platform Identity Authentication Service • SAP Cloud Identity Services - Identity Provisioning service (previously, SAP Cloud Platform Identity Provisioning Service Identity Authentication service and Identity Provisioning service are two main components within SAP Cloud Identity Services.	
New	A new topic to provide details about setting a preferred language for activation emails sent to your users.	Define PreferredLanguage Transformation [page 103]

2H 2020

Type of Change	Description	More Info
November 20, 2020		
Changed	You can use the monitoring tool track the progress of your upgrade.	Monitoring Tool for the Upgrade to Identity Authentication [page 44]Monitoring Tool for the Upgrade to SAP Cloud Platform Identity Authentication
Changed	Updated information around Dummy email, SendMail, and Password status transformations.	Configure Transformations in Identity Provisioning [page 89]Configure Transformations in Identity Provisioning
Changed	Added information around setting up a default password transformation for nonemail users.	Set Up Default Passwords Using Transformations [page 104]Set Up Default Passwords Using Transformations
October 16, 2020		

Type of Change	Description	More Info
Changed	We've enhanced the process for upgrading your tenants. When you upgrade, you can select the tenant to upgrade to.	Initiating the Upgrade to Identity Authentication in SAP Cloud Identity Services [page 40]Initiating the Upgrade to SAP Cloud Platform Identity Authentication

Related Information

SAP Cloud Identity Services - Identity Authentication
SAP Cloud Identity Services - Identity Provisioning

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.

www.sap.com/contactsap