SAML Single Sign-On

2024.2

February 12, 2025

this documentation and will not be responsible for any loss, costs, or damages incurred due to the use of this documentation.

If this document is in private pre-General Availability status:

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your pre-General Availability trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described in this document may change and remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Master Agreement, Oracle License and Services Agreement, Oracle PartnerNetwork Agreement, Oracle distribution agreement, or other license agreement which has been executed by you and Oracle and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Sample Code

Oracle may provide sample code in SuiteAnswers, the Help Center, User Guides, or elsewhere through help links. All such sample code is provided "as is” and “as available”, for use only with an authorized NetSuite Service account, and is made available as a SuiteCloud Technology subject to the SuiteCloud Terms of Service at www.netsuite.com/tos, where the term “Service” shall mean the SuiteProjects Pro Service.

Oracle may modify or remove sample code at any time without notice.

No Excessive Use of the Service

As the Service is a multi-tenant service offering on shared databases, Customer may not use the Service in excess of limits or thresholds that Oracle considers commercially reasonable for the Service. If Oracle reasonably concludes that a Customer’s use is excessive and/or will cause immediate or ongoing performance issues for one or more of Oracle’s other customers, Oracle may slow down or throttle Customer’s excess use until such time that Customer’s use stays within reasonable limits. If Customer’s particular usage pattern requires a higher limit or threshold, then the Customer should procure a subscription to the Service that accommodates a higher limit and/or threshold that more effectively aligns with the Customer’s actual usage pattern.

Table of Contents

SuiteProjects Pro SAML Single Sign-On Overview

The SuiteProjects Pro SAML Single Sign-On (SSO) feature lets you use an external identity provider service to manage user access to your SuiteProjects Pro account.

For more information about the SAML SSO feature, including a brief review of key terminology, feature requirements and limitations, see SAML Single Sign-On.

For best practice guidelines to ensure the seamless deployment of SAML SSO on your account, see SAML Deployment Best Practice Guidelines.

For an overview of steps required to set up and deploy SAML SSO on your SuiteProjects Pro account, see Deploying SAML Single Sign-On on Your SuiteProjects Pro Account.

SuiteProjects Pro Mobile supports SuiteProjects Pro single sign-on. See SuiteProjects Pro Mobile Apps and SAML Single Sign-On.

SAML Single Sign-On

Security Assertion Markup Language (SAML) is an OASIS open standard that supports secure communication of user authentication, entitlement and attribute information between different enterprise applications. It provides a method of secure integration with existing, on-site authentication infrastructures without exposing these services to direct public access, and enables federation of user identity across any number of additional services. SAML enables single sign-on (SSO), a scheme that allows users to sign in to one application — the identity provider — and automatically have access to separate applications — the service providers — without having to sign in to each of these other applications separately.

- The **identity provider (IdP)** validates the identity of the user and makes an SAML assertion to authorize access to a service provider. As a user, the IdP service is often a sign-in page where you enter your SSO sign-in details, or a dashboard you can use to access different enterprise applications.
- The **service provider (SP)** consumes the SAML assertion and grants the user access to the application.
- The **SAML assertion** uses a XML-based standard to send security information that applications working across security domain boundaries can trust.
- The SP and IdP use the **metadata** provided during configuration to establish a circle of trust.

The SuiteProjects Pro SAML SSO feature uses the SAML version 2.0 specifications. For information about the SAML standard, refer to the OASIS website.

⚠ **Important:** IdP services must support SAML 2.0 and allow custom assertions to be used with the SuiteProjects Pro SAML SSO feature.

The SuiteProjects Pro SAML SSO feature supports:

- IdP-initiated SSO — Typically, the user goes to the IdP service, signs in, and clicks a link or a button on the IdP page to access SuiteProjects Pro. The IdP service redirects the user to SuiteProjects Pro with a SAML assertion.
- SP-initiated SSO — Typically, the user goes to the SuiteProjects Pro sign-in page for SSO users, enters the company ID and user ID. SuiteProjects Pro redirects the user to the IdP service with an SAML

request. The IdP prompts the user to enter a password, validates the identity of the user and redirects the user to SuiteProjects Pro with an SAML assertion.

- Integration with multiple identity providers.

SuiteProjects Pro account administrators control who can use SAML SSO to access SuiteProjects Pro.

SAML Deployment Best Practice Guidelines

This section provides best practice guidelines for deploying SAML single sign-on (SSO) on your SuiteProjects Pro account.

- For an initial SAML deployment:
  - Test the SAML deployment on a sandbox account. Make sure it works as expected before you deploy SAML to your production account.
  - When you deploy SAML to your production account, only enable a small group of SuiteProjects Pro users to sign in using SAML SSO. Make sure it works as expected before you enable all users to login using SAML SSO.
- When changing over to a new identity provider (IdP):

  Test the new IdP configuration on a sandbox account. Make sure it works as expected before you change the IdP configuration on your production account. To discuss procuring a sandbox account for this purpose, contact your SuiteProjects Pro account manager.
- Always have at least one account administrator who can sign in to SuiteProjects Pro using password authentication. This will ensure an account administrator will be able to access your account in case there is an unexpected problem with SAML. If you enable a user to login using SAML SSO, this user can no longer use the default password authentication method to access SuiteProjects Pro.
- SuiteProjects Pro SAML certificates on sandbox and production environments have a finite lifetime. SuiteProjects Pro rotates SAML certificates that are about to expire. When SuiteProjects Pro rotates the SAML certificates, you must update the SAML signing and encryption certificates for the SuiteProjects Pro service provider profile in your identity provider product. See Updating the SuiteProjects Pro SAML Signing and Encryption Certificates in the Identity Provider Configuration.

  > **Note:** Before SuiteProjects Pro rotates the SAML certificates, you will receive a proactive feature change notification (PFCN) with information about the dates when new certificates will become available and previous certificates are due to expire.

Deploying SAML Single Sign-On on Your SuiteProjects Pro Account

This section gives an overview of steps required to set up and deploy SAML single sign-on (SSO) on your SuiteProjects Pro account.

> **Important:** Make sure you review the best practice guidelines before deploying SAML SSO on your SuiteProjects Pro account or changing over to a new identity provider (IdP) — See SAML Deployment Best Practice Guidelines.

To deploy SAML SSO on your SuiteProjects Pro account

1. **Configure the identity provider (IdP) for the SAML integration** — Import the SuiteProjects Pro service provider metadata XML file and configure the attributes required in the SAML assertion by the SuiteProjects Pro service provider. See Configuring the Identity Provider for the SAML Integration
2. **Configure the SAML Integration in SuiteProjects Pro** — Go to Administration > Global Settings > Account > Integration: SAML Single Sign-On and modify the settings are required. See Configuring the SAML Integration in SuiteProjects Pro.
3. **Test the SAML integration** — See Testing the SAML Integration.
4. **Enable employees to sign in using SAML single sign-on** — Create the `saml_auth` custom field associated with the Employee entity form and check the corresponding box on the employee demographic form for SAML SSO users. See Enabling Employees to Sign In Using SAML Single Sign-On.

Contact SuiteProjects Pro Support if you have any questions or encounter any difficulties when deploying SAML SSO on your SuiteProjects Pro account. See Creating a Support Case.

SuiteProjects Pro Mobile Apps and SAML Single Sign-On

SuiteProjects Pro Mobile Apps, including SuiteProjects Pro Mobile for iPhone and SuiteProjects Pro Mobile for Android, support SAML single sign-on. Both service provider initiated single sign-on (SP-initiated SSO) and identity provider initiated single sign-on (IdP-initiated SSO) are supported.

For information about setting up SuiteProjects Pro Mobile to sign in using SAML single sign-on, see Mobile.

Configuring the Identity Provider for the SAML Integration

This section describes the information you need to configure your identity provider (IdP) product for the SAML integration.

⚠ **Important:** Note the following requirements:

- IdP services must support SAML 2.0. In particular IdP services must support Redirect/POST bindings, and POST responses containing the SAML authentication assertion must be digitally signed.
- IdP services must allow custom assertions.
- SAML assertion encryption is optional, but should be used.
- Make sure you review the best practice guidelines before deploying SAML SSO on your SuiteProjects Pro account or changing over to a new identity provider (IdP) — See SAML Deployment Best Practice Guidelines.

The following IdP configuration steps are required before SAML authentication assertions can be exchanged between the IdP and the SuiteProjects Pro service provider (SP). Specific IdP products may require custom configuration — refer to the IdP product documentation for details.

1. **Import the SuiteProjects Pro service provider (SP) metadata** — See SuiteProjects Pro SAML Metadata.
2. **Configure the assertion attributes required by the SuiteProjects Pro SP** — Either of the attribute `NameID` or `user_nickname` must be included in the SAML assertion. See SAML Assertion Attributes.
3. **Download the IdP metadata XML file** — You will need to upload the IdP metadata XML file when configuring SuiteProjects Pro to work with the IdP service, or when you need to update the metadata (after a new security certificate for your IdP service, for example).

SuiteProjects Pro SAML certificates on sandbox and production environments have a finite lifetime. SuiteProjects Pro rotates SAML certificates that are about to expire. When SuiteProjects Pro rotates the SAML certificates you must update the SAML signing and encryption certificates for the SuiteProjects Pro service provider profile in your identity provider product. See Updating the SuiteProjects Pro SAML Signing and Encryption Certificates in the Identity Provider Configuration.

This guide includes steps to set up Microsoft Entra ID with SuiteProjects Pro SAML SSO. See Configuring Microsoft Entra ID for the SAML Integration.

Important: **The third party product setup steps are given for illustration purposes only.** SuiteProjects Pro does not support specific identity provider products or product versions. Refer to the product documentation for your identity provider for detailed and updated instructions. For additional questions about setting up your identity provider, please contact the Support services for your identity provider product.

SuiteProjects Pro SAML Metadata

The first step in configuring the identity provider (IdP) service for the SAML integration is to create a service provider (SP) profile for SuiteProjects Pro.

SuiteProjects Pro generates a unique SAML **Entity ID** (metadata URL) and **Assertion Consumer Service URL** for each identity provider profile you create. To find the correct **Entity ID** and **Assertion Consumer Service URL** to use in the SP profile for SuiteProjects Pro, go to Administration > Global Settings > Account > Integration: SAML Single Sign-On and do one of the following:

- Click the name of the identity provider profile, if a profile exists for the identity provider.
- Add a profile for the identity provider, if a profile does not already exist. See Adding a New Identity Provider Profile.

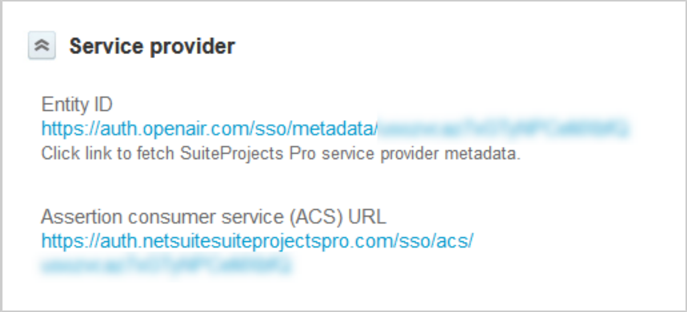
The Identity provider profile form appears and shows the **Entity ID** (metadata URL) and **Assertion Consumer Service URL** under the Service Provider section.

Note: OpenAir is now SuiteProjects Pro. As of 5 a.m. Eastern Time (UTC–5) on January 25, 2025, for your sandbox account, and on February 15, 2025, for your production account, service URLs with the `netsuitesuiteprojectspro.com` domain name replace URLs with the `openair.com` domain name.

Note that existing SAML single sign-on implementations are not expected to require any updates. The service provider entity IDs and assertion consumer service (ACS) URLs **have not changed** for existing identity provider profiles.

For identity provider profiles added after February 15, 2025, service provider entity IDs continue to use the `openair.com` domain name and ACS URLs use the `netsuitesuiteprojectspro.com` domain name.

For more information about the change, see the help topic Introducing SuiteProjects Pro (Action Required).



Service provider

Entity ID
https://auth.openair.com/sso/metadata/[redacted]
Click link to fetch SuiteProjects Pro service provider metadata.

Assertion consumer service (ACS) URL
https://auth.netsuitesuiteprojectspro.com/sso/acs/[redacted]

SAML Assertion Attributes

After you have created a service provider (SP) profile for SuiteProjects Pro and imported the SuiteProjects Pro SAML metadata into your IdP service, you need to ensure that SAML assertions contain the required attributes with the appropriate SuiteProjects Pro sign-in identifiers.

This following table lists both required and optional assertion attributes and the SuiteProjects Pro sign-in identifiers they map to.

Attribute	Required / Optional	Description
`NameID`	Required	SuiteProjects Pro User ID — The unique user identifier (**Employee ID** on the employee demographic form in SuiteProjects Pro). **Important:** Depending on your IdP configuration, you may not be able to map `NameID` to the source attribute containing the SuiteProjects Pro User ID. For example, the IdP service may use `NameID` as a transient identifier for session management. If this is the case: ▪ The assertion must contain both `NameID` and `user_nickname` attributes. ▪ Use `user_nickname` to send the SuiteProjects Pro User ID in the SAML assertion.
`user_nickname`	Optional	If specified, `user_nickname` takes precedence over `NameID` for identifying the user. You can use `user_nickname` to send the SuiteProjects Pro User ID in the SAML assertion if `NameID` cannot be used.

Note: The attribute `account_nickname` is no longer required. The SuiteProjects Pro SAML endpoint is unique to your SuiteProjects Pro account and to each IdP profile.

Updating the SuiteProjects Pro SAML Signing and Encryption Certificates in the Identity Provider Configuration

SAML signing and encryption certificates provide additional security when using SAML single sign-on (SSO) authentication to access SuiteProjects Pro. SAML signing and encryption uses public keys, or certificates, to verify data sent between the SuiteProjects Pro service provider (SP) and the identity provider (IdP). The IdP uses the signing certificate to verify the signature sent by the SuiteProjects Pro SP during the authentication request. The IdP uses the encryption certificate to conceal the content in the return response (assertion) to the SuiteProjects Pro SP.

SuiteProjects Pro SAML certificates on sandbox and production environments have a finite lifetime. SuiteProjects Pro rotates SAML certificates that are about to expire.

When SuiteProjects Pro rotates the SAML certificates, you must retrieve SAML certificate information from your SuiteProjects Pro account, save it in the correct format and import it in to your identity provider product on the service provider profile you created for this SuiteProjects Pro account.

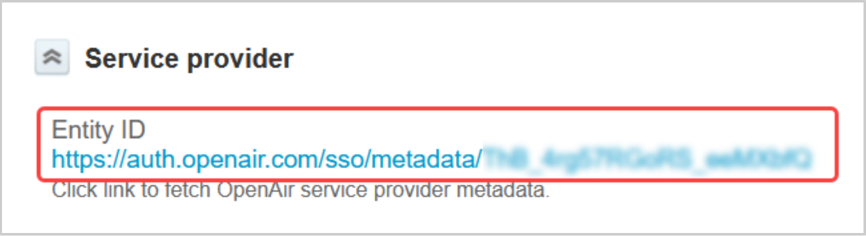
> ⚠ **Important:** Do not download the SSL certificate from your browser header. SAML certificates are distinct from SSL (TLS) certificates. SSL certificates apply to the browser you use to access SuiteProjects Pro and they are configured and maintained by the server.
>
> Before SuiteProjects Pro rotates the SAML certificates, you will receive a proactive feature change notification (PFCN) with information about the dates when new certificates will become available and previous certificates are due to expire.

To update the SuiteProjects Pro SAML signing and encryption certificates in your identity provider configuration:

1. In SuiteProjects Pro, go to Administration > Account> Integration: SAML Single Sign-On > [*Select the active identity provider profile*].

   The identity provider profile form opens.

2. Click the link under **Entity ID**.

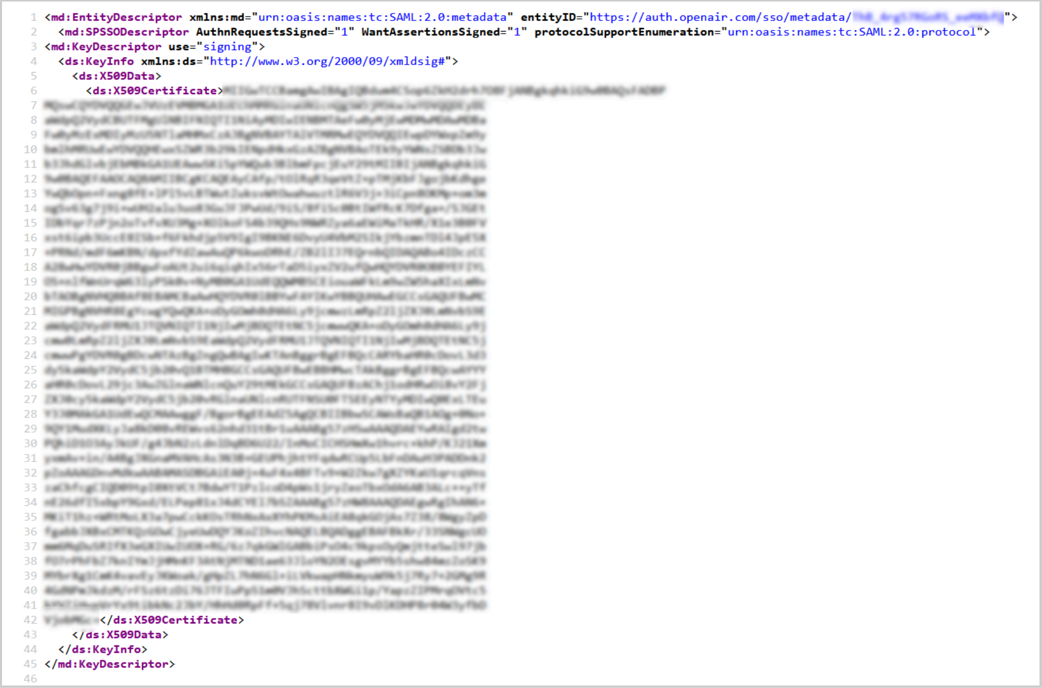
   

   Entity ID
   https://auth.openair.com/sso/metadata/[redacted]
   Click link to fetch OpenAir service provider metadata.

   The SuiteProjects Pro SAML metadata associated with the identity provider profile appears.

3. Right-click anywhere on the page and select **View Page Source** from the context menu.

   The page source appears.

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://auth.openair.com/sso/metadata/[redacted]">
  <md:SPSSODescriptor AuthnRequestsSigned="1" WantAssertionsSigned="1" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:X509Data>
      <ds:X509Certificate>[redacted]</ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</md:KeyDescriptor>
```

4. Copy the text between the `<ds:X509Certificate>` and `</ds:X509Certificate>` tags.

Make sure that you select the entire certificate text and only the certificate text before you copy it to your clipboard. Do not select any of the characters in the `<ds:X509Certificate>` and `</ds:X509Certificate>` tags.

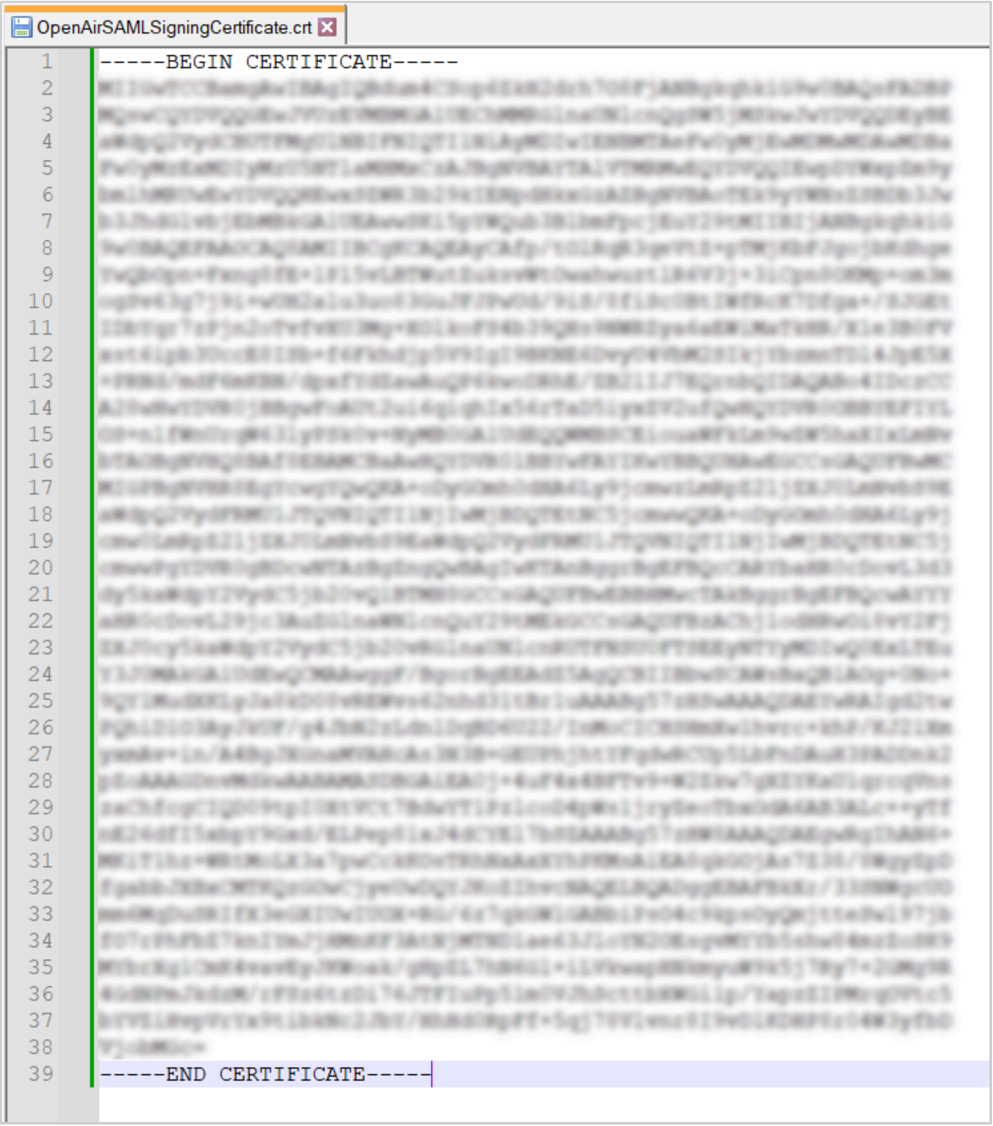
5. Paste the content of the clipboard into a text editor.
6. Insert the following certificate header on a separate line at the top.

```
-----BEGIN CERTIFICATE-----
```

7. Insert the following certificate footer on a separate line at the bottom.

```
-----END CERTIFICATE-----
```

8. Save the file. Use the file extension `.pem` or `.crt` depending on the file extension required by the identity provider product for SAML certificates.



```
-----BEGIN CERTIFICATE-----
[redacted]
-----END CERTIFICATE-----
```

9. In your identity provider product, go to the service provider profile you set up for your SuiteProjects Pro account and import the PEM or CRT SAML certificate file for SuiteProjects Pro under both the Signing certificate and Encryption certificate sections.

Configuring Microsoft Entra ID for the SAML Integration

This section provides the steps to set up Microsoft Entra ID, formerly known as Microsoft Azure AD, to provide single sign-on (SSO) access to SuiteProjects Pro using the SuiteProjects Pro SAML SSO feature.

⚠ **Important: The following configuration steps are given for illustration purposes only.** SuiteProjects Pro does not support specific identity provider products or product versions. The following steps do not reflect the latest identity provider product version and still refer to the product name at the time these steps were written and tested. The Refer to Microsoft product documentation for detailed and updated instructions about Microsoft Entra ID. For additional questions about setting up Microsoft Entra ID, please contact Microsoft Support.

Make sure your Microsoft Entra ID plan supports custom attributes as well as preconfigured attributes in the SAML assertion. The free version, for example, may not let you define the custom attribute `user_nickname` required by the SuiteProjects Pro service provider.

ⓘ **Note:** OpenAir is now SuiteProjects Pro. As of 5 a.m. Eastern Time (UTC–5) on January 25, 2025, for your sandbox account, and on February 15, 2025, for your production account, service URLs with the `netsuitesuiteprojectspro.com` domain name replace URLs with the `openair.com` domain name.

Note that existing SAML single sign-on implementations are not expected to require any updates. The service provider entity IDs and assertion consumer service (ACS) URLs **have not changed** for existing identity provider profiles.

For identity provider profiles added after February 15, 2025, service provider entity IDs continue to use the `openair.com` domain name and ACS URLs use the `netsuitesuiteprojectspro.com` domain name.

For more information about the change, see the help topic Introducing SuiteProjects Pro (Action Required).

To configure Microsoft Entra ID for the SAML integration

1. Sign in to the Microsoft Entra admin center using your Microsoft Entra ID administrator account.
2. Go to Identity > Applications > Enterprise Applications.
3. Click **New application**.
4. Click **Create your own application**.
5. Enter a Name for the application (“SuiteProjects Pro Sandbox” or “SuiteProjects Pro Production”, for example).
6. Choose **Integrate any other application you don't find in the gallery (Non-gallery)**.
7. Click **Create**.

   The Application Overview page appears.

8. Click **Single sign-on** under Manage, and select **SAML**.

   The SAML-based sign-on configuration page displays.

9. Click the Edit icon in the Basic SAML Configuration section and enter the following information:

   - **Identifier (Entity ID)** — Click the **Add identifier** link and enter the Entity ID generated by SuiteProjects Pro on the identity provider profile you created for Microsoft Entra ID in your SuiteProjects Pro account.
     - `https://auth.sandbox.openair.com/sso/metadata/`*<unique_ref_generated_by_SuiteProjects Pro>* (Sandbox account)
     - `https://auth.openair.com/sso/metadata/`*<unique_ref_generated_by_SuiteProjects Pro>* (Production account)
   - **Reply URL (Assertion Consumer Service URL)** — Click the **Add reply URL** link and enter the Assertion Consumer Service URL generated by SuiteProjects Pro on the identity provider profile you created for Microsoft Entra ID in your SuiteProjects Pro account.
     - `https://auth.sandbox.netsuitesuiteprojectspro.com/sso/acs/`*<unique_ref_generated_by_SuiteProjects Pro>* (Sandbox account)
     - `https://auth.netsuitesuiteprojectspro.com/sso/acs/`*<unique_ref_generated_by_SuiteProjects Pro>* (Production account)

   > **Note:** Examples in this help topic use sample Entity ID and Assertion Consumer Service URL generated for a sandbox account. To set up Microsoft Entra ID with your production or sandbox account, replace the URLs with the unique **Entity ID** and **Assertion Consumer Service URL** generated by SuiteProjects Pro on the identity provider profile you created for Microsoft Entra ID on your SuiteProjects Pro account. See SuiteProjects Pro SAML Metadata.

   - Leave the optional fields **Sign on URL**, **Relay State** and **Logout Url** blank.

10. Click **Save** and close the Basic SAML Configuration pane.

11. Click the Edit icon in the Attributes & Claims section.

12. Add the **User Attributes & Claims** `user_nickname`. To do so:

    1. Click **Add new claim**.

       The Manage user claims page appears.

    2. Enter the **Name** `user_nickname`.
    3. Under **Source**, choose `Attribute`.
    4. Select the **Source attribute** where the claim is going to retrieve its value. This must be the source attribute containing the SuiteProjects Pro User ID.
    5. Click **Save**. The attribute `user_nickname` is now listed in the table.
    6. Delete all other attributes and claims that can be deleted.

13. Review the **SAML Signing Certificate** and download the **Metadata XML** file. You will need to upload the **Metadata XML** file to identity provider profile you created for Microsoft Entra ID in your SuiteProjects Pro account.

14. Click **Users and groups** on the left hand side pane and assign users and group to this SAML application. Microsoft Entra ID will not issue a token allowing a user to sign in to the application unless Microsoft Entra ID has granted access to the user. Users may be granted access directly, or through a group membership. To assign a user or group to your application, click the **Assign Users** button. Select the user or group you want to assign, and click the **Assign** button.

Configuring the SAML Integration in SuiteProjects Pro

The SAML integration administration page becomes available after the feature is enabled. To view or change the SAML integration settings for your SuiteProjects Pro account, go to Administration > Global Settings > Account > Integration: SAML Single Sign-On.

You can configure the SuiteProjects Pro SAML Single Sign-On feature to work with multiple identity providers. The list on the SAML integration administration page lets you manage the profile and upload the metadata for each identity provider.

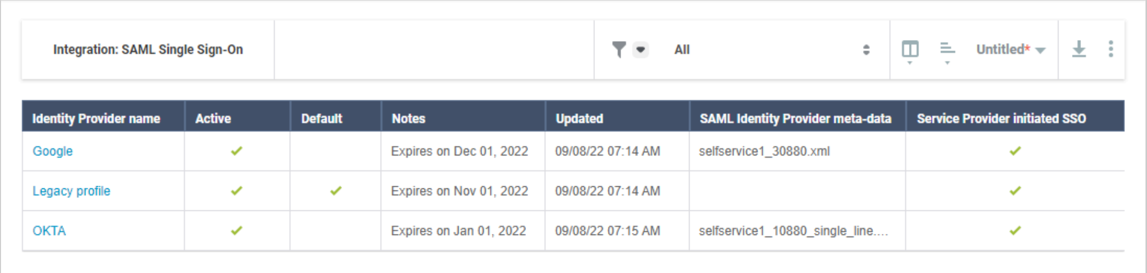
The SuiteProjects Pro SAML Single Sign-On feature lets you:

- Configure the SuiteProjects Pro SAML Single Sign-On feature to work with multiple identity providers.

  > **Important:** Multiple identity provider support is currently available only for identity provider initiated single sign-on.

- Review configured identity providers from a list. To view the list of identity provider profiles for your SuiteProjects Pro account, go to Administration > Global Settings > Account > Integration: SAML Single Sign-On.
- Add identity provider profiles. See Adding a New Identity Provider Profile.
- Delete identity provider profiles. See Deleting an Identity Provider Profile.
- Change identity provider profiles:
  - Set or change the profile details and upload the SAML metadata file for each identity provider as and when required.
  - Set any identity providers as active. Only active identity providers can be used for service provider or identity provider initiated single sign-on.
  - Select one default identity provider. If the default identity provider is configured to be used with service provider initiated single sign-on request, it will serve as the identity provider when using the SuiteProjects Pro sign-in page for single sign-on users.

  See Changing Profile Details or Upload the Metadata for an Identity Provider.
- View audit trail information for all identity provider profiles. See Viewing Audit Trail Information for Identity Provider Profiles.



Identity Provider name	Active	Default	Notes	Updated	SAML Identity Provider meta-data	Service Provider initiated SSO
Google	✓		Expires on Dec 01, 2022	09/08/22 07:14 AM	selfservice1_30880.xml	✓
Legacy profile	✓	✓	Expires on Nov 01, 2022	09/08/22 07:14 AM		✓
OKTA	✓		Expires on Jan 01, 2022	09/08/22 07:15 AM	selfservice1_10880_single_line....	✓

Adding a New Identity Provider Profile

You can add new identity provider profiles and configure the SuiteProjects Pro SAML Single Sign-On feature to work with multiple identity providers.

To add a new identity provider profile:

1. Go to Administration > Global Settings > Account > Integration: SAML Single Sign-On.
2. Click the Create button then New Identity provider.

   The Identity provider profile form appears.
3. Enter an **Identity provider name** and all other profile details. Upload the metadata for the identity provider. For more information about the profile details on the form, see Changing Profile Details or Upload the Metadata for an Identity Provider.

Deleting an Identity Provider Profile

You can delete obsolete identity provider profiles at any time.

⚠ **Important:** The identity provider profile marked as **Default**

To delete an identity provider profile:

1. Go to Administration > Global Settings > Account > Integration: SAML Single Sign-On.
2. Click the name of the identity provider profile you want to delete.

   The Identity provider profile form appears.
3. Click **Delete**.
4. Click **OK** to confirm

Changing Profile Details or Upload the Metadata for an Identity Provider

You can change the profile details and upload the metadata for each identity provider on the SAML single sign-on integration administration page at any time.

ⓘ **Note:** OpenAir is now SuiteProjects Pro. As of 5 a.m. Eastern Time (UTC–5) on January 25, 2025, for your sandbox account, and on February 15, 2025, for your production account, service URLs with the `netsuitesuiteprojectspro.com` domain name replace URLs with the `openair.com` domain name.

Note that existing SAML single sign-on implementations are not expected to require any updates. The service provider entity IDs and assertion consumer service (ACS) URLs **have not changed** for existing identity provider profiles.

For identity provider profiles added after February 15, 2025, service provider entity IDs continue to use the `openair.com` domain name and ACS URLs use the `netsuitesuiteprojectspro.com` domain name.

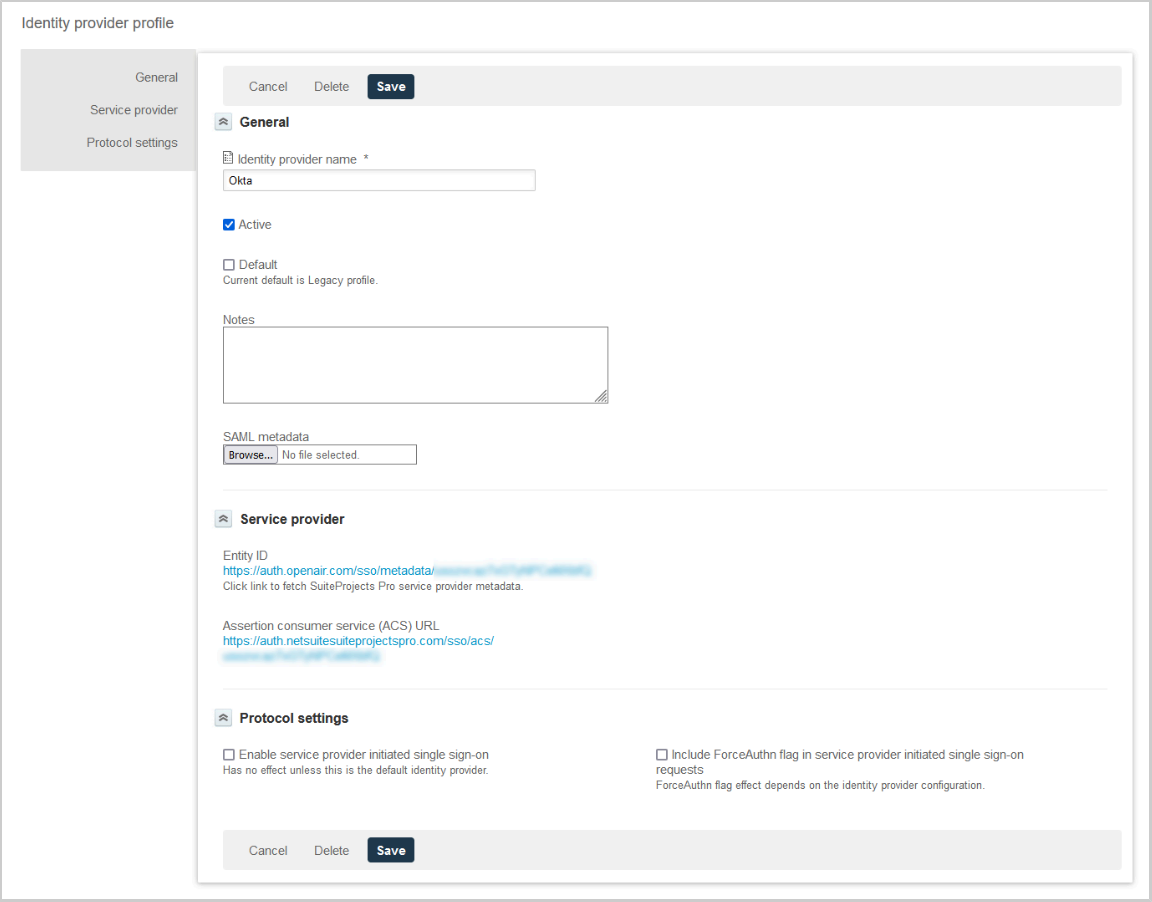
For more information about the change, see the help topic Introducing SuiteProjects Pro (Action Required).

To change profile details or upload the metadata for an identity provider:

1. Go to Administration > Global Settings > Account > Integration: SAML Single Sign-On.
2. Click the name of the identity provider profile.
3. Change all profile details and upload the metadata for the identity provider as required. The form includes the following information:
   - **Identity provider name** — (Required) Enter a name for the identity provider profile.
   - **SAML identity provider metadata** — To upload or change the metadata for the identity provider, click **Choose** and select the SAML metadata file from your computer. The selected document will be uploaded when you save the form. The file must be a valid XML document to be uploaded and must be a valid SAML 2.0 metadata file for SAML SSO to work.
   - **Active identity provider** — Check the box to mark the identity provider profile as active. Only active identity providers can be used for service provider or identity provider initiated single sign-on.
   - **Default identity provider** — Check the box to mark the identity provider profile as the new default profile. There can only be one default profile at any one time. If none of the existing profiles are marked as default, the legacy profile is the default profile.
   - **Notes** — Enter any relevant notes for the identity provider profile.
   - **Service Provider | Entity ID** — (Read only) This is generated automatically by SuiteProjects Pro. This is SuiteProjects Pro service provider Entity ID. Click the link to fetch the SAML metadata for SuiteProjects Pro service provider. You will need this information when configuring the identity provider service for the integration.
   - **Service Provider | Assertion consumer service (ACS) URL** — (Read only) This is generated automatically by SuiteProjects Pro. You will need this information when configuring the identity provider service for the integration.
   - **Protocol Settings | Enable service provider initiated SSO** — Check this box to enable this identity provider profile to be used for service provider initiated single sign-on (SP-initiated SSO). The identity provider profile must also be set as the default profile to be used for service provider initiated SSO.

     > ⚠ **Important:** An identity provider profile can only be used for service provider initiated single sign-on if both the following conditions are met:
     >
     > - The identity provider profile is the default identity provider profile.
     > - The **Enable service provider initiated SSO** box is checked.
     >
     > The SuiteProjects Pro sign-in page for single sign-on users cannot be used to sign in to SuiteProjects Pro otherwise.

   - **Protocol Settings | Enable Service Provider Initiated SSO ForceAuthn** — Check this box to include the `ForceAuthn` flag in service provider initiated requests. `ForceAuthn` is an optional SAML feature that acts as a signal to the identity provider to require some form of user interaction when handling the request, overriding the usual implicit assumption that it is acceptable to reuse authentication state from an earlier request. The effect depends on the identity provider service and configuration.



Identity provider profile

General

Identity provider name * Okta

☑ Active

□ Default
Current default is Legacy profile.

Notes

SAML metadata
Browse... No file selected.

Service provider

Entity ID
https://auth.openair.com/sso/metadata/[redacted]
Click link to fetch SuiteProjects Pro service provider metadata.

Assertion consumer service (ACS) URL
https://auth.netsuitesuiteprojectspro.com/sso/acs/[redacted]

Protocol settings

□ Enable service provider initiated single sign-on
Has no effect unless this is the default identity provider.

□ Include ForceAuthn flag in service provider initiated single sign-on requests
ForceAuthn flag effect depends on the identity provider configuration.

Viewing Audit Trail Information for Identity Provider Profiles

Account administrators can view audit trail information directly on the identity provider profile form. The audit information appears in a popup window. The audit log is in a plain text format displaying the user who made the change, what was changed, the date the change was made, and what the value was changed to.

Note: The audit trail information includes an `oa_uid` field. This is the internal ID of the user who made the change in the SuiteProjects Pro Identification Authentication Service, and is different from the internal ID of the user in SuiteProjects Pro.

Important: The audit trail information is available on the identity profile form only if the Quick Audit Trail for Global Settings feature is enabled for your account. To enable this feature, contact SuiteProjects Pro Support.

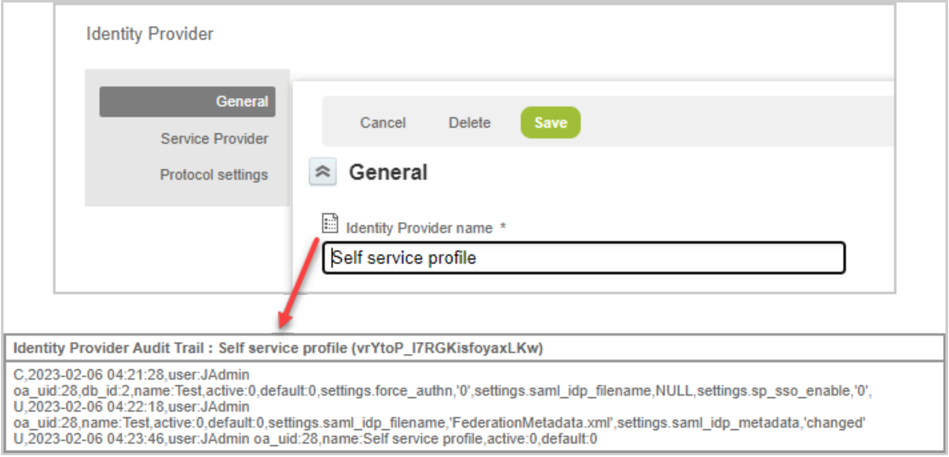
For more information about the Quick Audit Trail for Global Settings feature, see Optional Features and Security.

To view audit trail information for an identity provider profile:

1. Go to Administration > Global Settings > Account > Integration: SAML Single Sign-On.

2. Click the name of the identity provider profile.
3. Click the audit trail icon 🗎 next to the **Identity provider name** field.

   A popup window appears showing the audit trail information.



Self service profile

Identity Provider Audit Trail : Self service profile (vrYtoP_I7RGKisfoyaxLKw)

```
C,2023-02-06 04:21:28,user:JAdmin
oa_uid:28,db_id:2,name:Test,active:0,default:0,settings.force_authn,'0',settings.saml_idp_filename,NULL,settings.sp_sso_enable,'0',
U,2023-02-06 04:22:18,user:JAdmin
oa_uid:28,name:Test,active:0,default:0,settings.saml_idp_filename,'FederationMetadata.xml',settings.saml_idp_metadata,'changed'
U,2023-02-06 04:23:46,user:JAdmin oa_uid:28,name:Self service profile,active:0,default:0
```

Testing the SAML Integration

After you enable the SAML Single Sign-On (SSO) feature for your SuiteProjects Pro account and you configure at least one identity provider (IdP) service, create an identity provider profile in SuiteProjects Pro, and upload the identity provider metadata, use the following steps to test the SAML integration.

To test the SAML integration:

1. Go to Administration > Global Settings > Account > Integration: SAML Single Sign-On.
2. Click the name of the identity provider profile you want to test.
3. Click the Tips menu, then click the following links:
   - **Test <IdP_profile_name> SP-initiated SSO** — Click this link to test the service provider initiated SSO

     > **Note:** This link only shows if the **Active identity provider**, **Default identity provider**, and **Enable service provider initiated SSO** boxes are all checked.

   - **Test <IdP_profile_name> IdP-initiated SSO** — Click this link to test the identity provider initiated SSO. A window appears. Enter the **URL for IdP-initiated SSO** and click **Test IdP SSO**.

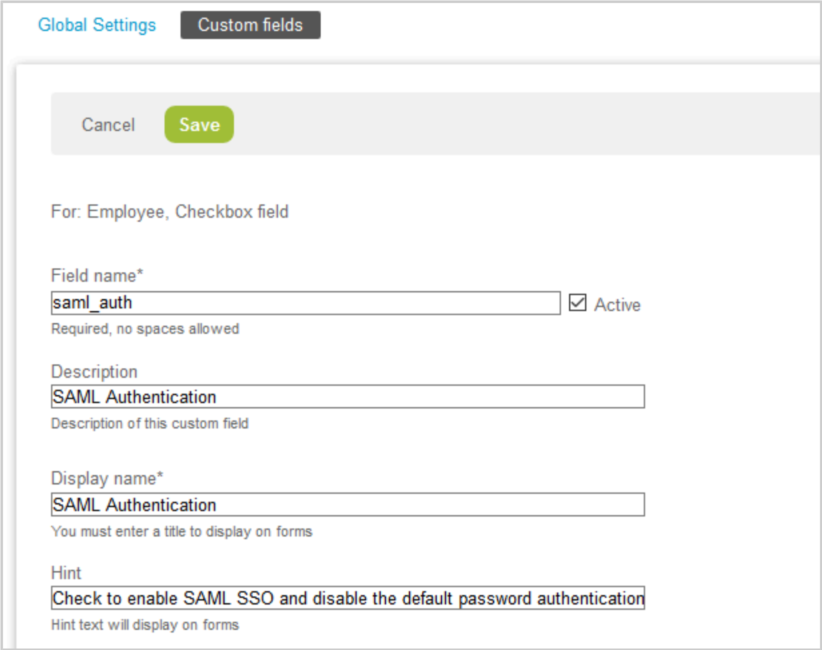
     > **Note:** This link only shows if the **Active identity provider** box is checked.

Enabling Employees to Sign In Using SAML Single Sign-On

After the SAML Single Sign-On (SSO) feature is enabled for your SuiteProjects Pro account and you have configured the identity provider (IdP) service and SuiteProjects Pro, you can enable your users to login using SAML Single Sign-on (SSO). To do so, you need to add a setting on the employee demographic form using a custom field.

To enable employees to sign in using SAML single sign-on:

1. In SuiteProjects Pro, go to Administration > Global settings > Custom fields.
2. Click the Create button and select New Custom field. The New Custom field form appears.
3. Select 'Employee' from the **Add a custom field to** dropdown list and 'Checkbox' from the **Type of field to add** dropdown list. Click **Continue**.
4. Enter the **Field name** `saml_auth`, check the **Active** box, enter the **Display name** `SAML Authentication`. Enter a **Description** and **Hint** if required. Click **Save**.



For: Employee, Checkbox field

Field name*
saml_auth ☑ Active
Required, no spaces allowed

Description
SAML Authentication
Description of this custom field

Display name*
SAML Authentication
You must enter a title to display on forms

Hint
Check to enable SAML SSO and disable the default password authentication
Hint text will display on forms

> ⚠ **Important:** The **Field name** must be set to `saml_auth`.

5. Go to Administration > Global Settings > Users > Employees > [*Select an Employee*]. The Employee Demographic form should now include the **SAML Authentication** box.
6. To enable SAML Authentication for an employee, check the **SAML Authentication** box on the employee demographic form.

⚠ **Important:** After you have enabled SAML Authentication for an employee, this employee will no longer be able to use the standard password authentication method to access SuiteProjects Pro. Make sure you keep the SAML Authentication disabled for at least one administrator account for troubleshooting purposes.

SAML authentication is mutually exclusive with two-factor authentication (2FA). Saving the form returns an error if both the **Two-factor authentication required** and **SAML Authentication** [saml_auth] boxes are checked. For more information about 2FA, see the help topic Two-Factor Authentication.

✓ **Tip:** You can use the bulk employee change wizard to copy the value of the saml_auth field to other user records on your SuiteProjects Pro account.

See Administrator Guide under Home > Home > Wizards > Making Changes to Multiple Employee Records at the Same Time.

Creating a Support Case

If you are experiencing difficulties with SuiteProjects Pro or would like to enable an optional feature, go to SuiteAnswers through the Support page in SuiteProjects Pro and create a support case.

Our support staff and engineers will work with you to find a solution to your problem.

> ⚠ **Important:** Be sure to review the Support Usage Best Practice Guidelines, Case Severity Definitions and Case Resolution Overview before you submit a support case or call the Support team.
>
> As a part of the support case creation process you will be presented with existing answers that may solve your problem. Take a moment to view the available answers before proceeding to create a support case.

To create a support case:

1. Sign in to your company's SuiteProjects Pro account.
2. Go to the user menu in the SuiteProjects Pro application. To access the user menu, click your profile pictures or initials in the upper-right corner.
3. Select **Support**.
4. Click **Explore SuiteAnswers**
5. In SuiteAnswers, click **Contact Support** in the top bar.
6. Click **Create Support Case** under Online Support.

   > ⓘ **Note:** Depending on your support services subscription level, you may be able to access Support by phone. In this case, the page lets you select your country and shows a phone number that you can use to access Support by phone. The page also shows your SuiteProjects Pro account ID and your support services subscription level.
   >
   > The page also includes a link to the SuiteProjects Pro user group. Click **Ask an Expert from the SuiteProjects Pro Support Community** to go to the SuiteProjects Pro user group.

   The Create a Support Case page appears.
7. Follow the onscreen instructions to create a Support case:
   a. Step 1 – Enter a search term to check for existing answers to your query.

      The first 5 search results appear. The list shows the number of articles matching your search. Oftentimes, an answer to your query already exists in SuiteAnswers. Review the search results and click **View all search results** to view other search results.
   b. Step 2 – Click and select the type of case you want to create.
   c. Step 3 – Choose a case severity. For more information about case severity levels, see the help topic Case Severity Definitions.

      > ⚠ **Important:** Always use the appropriate case severity when submitting a case. Using the appropriate case severity helps SuiteProjects Pro Support prioritize between cases. Otherwise, SuiteProjects Pro Support need to evaluate the true urgency of each case, which slows down the response time to all cases.
   d. Step 4 – Click and select the feature that your query relates to. Click the caret to expand options under each categories in the list. If you want to change the option selected, you need to delete the text first before you can select a different option.

e. Step 5 – Enter your question or a description of the problem you encountered.

f. (Optional) Attach files. Either click and select the files you want to attach or drag the files to the form.

g. Enter or verify your email address.

h. (Optional) Enter or verify your telephone number, including the country code and without any spaces, if you prefer to be contacted by telephone.

- Do not enter anything into the “Attach Document” field.
- In the “Email” field, type your email.

> **Note:** Requests to enable or disable account-wide features in SuiteProjects Pro can only be processed when an administrator’s email address is entered in this field.

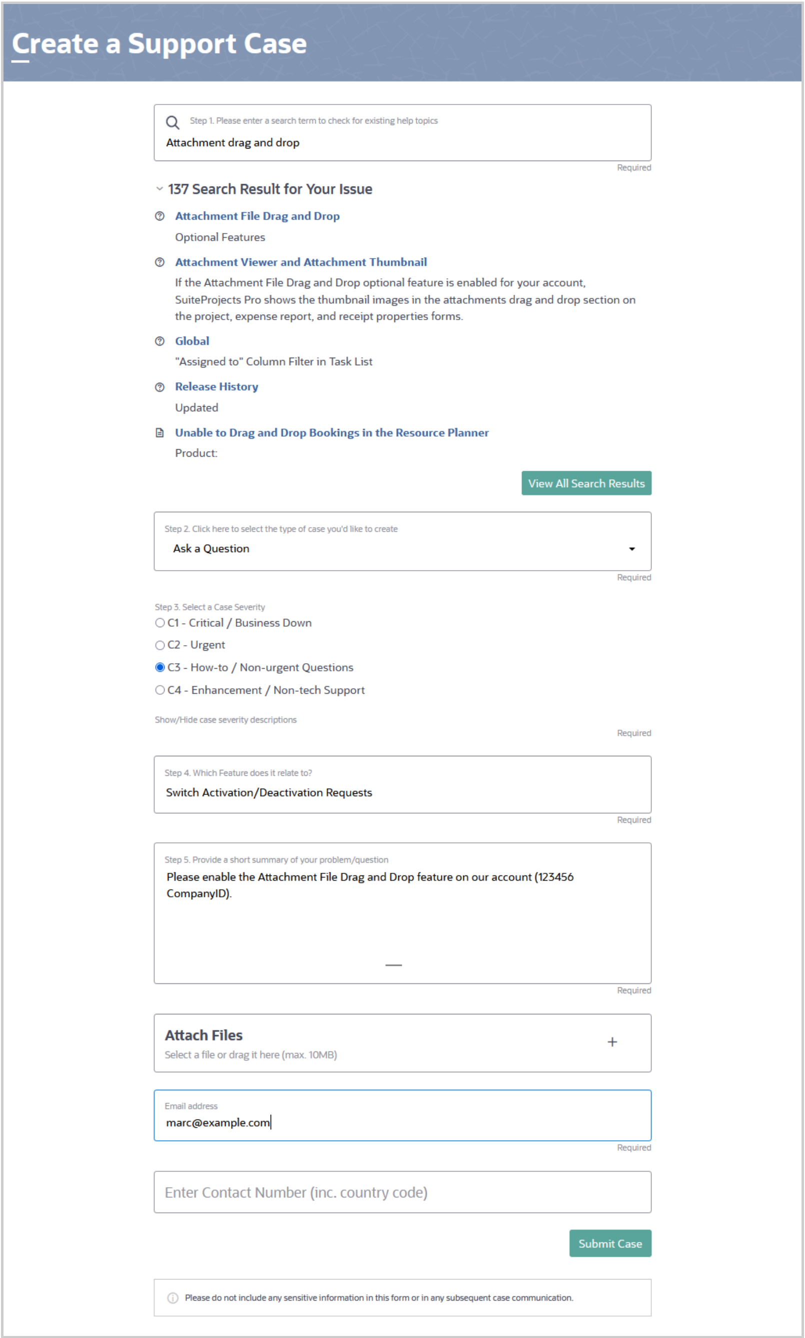
- In the “Phone (Optional)” field, type a phone number where you can be contacted if you would prefer contacts you by telephone. Please include your country code and enter the number without any spaces.

> **Note:** If you are creating a support case to enable an optional feature controlled by SuiteProjects Pro Support, enter the following details:
>
> - In **Step 2. Click here to select the type of case you'd like to create**, select “Ask a question”.
> - In **Step 3. Select a case severity**, select “C3 — How To / Non Urgent questions”.
> - In **Step 4. Which Feature does it relate to?**, select "Switch Activation/Deactivation Requests” under the category "SuiteProjects Pro Web Application".
> - In **Step 5. Provide a short summary of your problem/question**, enter the name of the optional feature you want to enable or disable, the type of account (production or sandbox) and the Company ID for the account you want to enable or disable it for.

8. Click **Submit case**.

An email confirmation with your support case reference (SuiteProjects Pro Customer Care #) is sent to your email address.

SuiteProjects Pro Support will contact you to request additional information if necessary or guide you through any steps required to resolve the support case.



Create a Support Case

Step 1. Please enter a search term to check for existing help topics

Attachment drag and drop

Required

137 Search Result for Your Issue

Attachment File Drag and Drop

Optional Features

Attachment Viewer and Attachment Thumbnail

If the Attachment File Drag and Drop optional feature is enabled for your account, SuiteProjects Pro shows the thumbnail images in the attachments drag and drop section on the project, expense report, and receipt properties forms.

Global

"Assigned to" Column Filter in Task List

Release History

Updated

Unable to Drag and Drop Bookings in the Resource Planner

Product:

Step 2. Click here to select the type of case you'd like to create

Ask a Question

Required

Step 3. Select a Case Severity

○ C1 - Critical / Business Down

○ C2 - Urgent

● C3 - How-to / Non-urgent Questions

○ C4 - Enhancement / Non-tech Support

Show/Hide case severity descriptions

Required

Step 4. Which Feature does it relate to?

Switch Activation/Deactivation Requests

Required

Step 5. Provide a short summary of your problem/question

Please enable the Attachment File Drag and Drop feature on our account (123456 CompanyID).

Required

Attach Files

Select a file or drag it here (max. 10MB)

Email address

marc@example.com

Required

Enter Contact Number (inc. country code)

Please do not include any sensitive information in this form or in any subsequent case communication.