

Contents

Connect (product name) to (product name)	4
Prepare for (product name) with (product name).....	4
Learn about (product name).....	4
Install supporting (product name) software	5
Set up (product name) in (product name)	6
Create the (product name) application user for (product name).....	6
Create the application in (product name) for (product name)	6
Set up (product name) API key in the subscriber.....	7
Auto-configure resources that are owned by (product name).....	8
Update the (product name) owned resources after an (product) API upgrade	9
Create (product name) users for Proxy API requests	10
Create the API user	10
Define the role for the API user.....	10
Assign permissions to the API user role	10
Set up (product name) mapping	11

Connect (product name) to (product name)

Set up (product name) APIs and messaging components to support messaging between (product name) and other applications using (company name) (product name).

(product name) setup checklist

The checklist below lists the steps needed to set up (product name) in (product name), and identifies which steps are required to support each of the mechanisms by which other applications get data from (product name) through (product name): by making proxy API requests to (product name) or subscribing to changes published by (product name)

Step	Proxy API requests	Publish/subscribe
Prepare for (product name) with (product name)	X	X
Install supporting (product name) software	X	X
Set up (product name) in (product) Integration	X	X
Create (product name) users for Proxy API requests	X	X
Set up (product name) mapping	X	X

Prepare for (product name) with (product name)

Perform these steps before beginning the installation and the setup process.

Learn about (product name)

Use these resources to gain a general understanding of how to integrate (product name) with other applications using (product name).

Resource	Description
About (product name) link	Documentation describing (company name) (product) Platform.
(product name) link	Videos covering the (company name) (product) Platform and (product name).
About (product name)	Documentation describing (product name)

fundamentals.

Install supporting (product name) software

Before setting up (product name) with (product name), install the supporting software listed here.

Install or upgrade your (product name) database to 9.2.1

Before you connect (product name) to (product name), create a new (product name) database or upgrade your current (product name) database 9.0.0 or later to 9.2.1. For more information, see "Install or Upgrade your (product name) Database" in the *(product name) Install Guide*.

Install or upgrade your (product name) application to 9.2.1

For more information, see "Install or Upgrade (product name) application" in the *(product name) Install Guide*.

Install or upgrade your (product name) Identity database to 9.2.1

For more information on the Identity database installation, see "Install (product name) Identity database" in the *(product name) Self-Service Install Guide*.

If you have already installed a (product name) Identity database, then see "Upgrade (product name) Identity database" in the *(product name) Self-Service Upgrade Guide* to upgrade to 9.2.1.

Install or upgrade (product name) Service Bus to 9.2.1

Use (product name) Service Bus to transfer information between (product name) 9.2.1 and other applications. For more information, see "Install (product name) Service Bus" in the *(product name) Install Guide*.

Install (product name) API

Install (product name) (product) API. For more information, see "Install (product name) (product) API" in the *(product name) Self-Service Install Guide*.

The (product) API APIs allow (product) API applications to retrieve information from (product name).

Install (product name) Web Administration

Install (product name) Web Administration to map the Code table values to (product) values. To allow access to the application, set the Web Administration URL in (product name). See "(product name) Web Administration" in the *(product name) Web Administration Install Guide*.

Install (product name) User Management

The User Management application allows you to manage users, roles, and to assign permissions for (product) API. For more information, see "Install (product name) User Management" in the *(product name) Self-Service Install guide*.

Set up (product name) in (product name)

In (product name), create the (product) application for (product name) and add the resources for which (product name) is authoritative.

Create the (product name) application user for (product name)

Create a user in (product name) **User Management** and assign permissions to allow the user to access (product name) resources in (product name).

Procedure

1. Create a user for (product name) in (product name) > **User Management** > (product) API
2. Create a role for the new user. Then, under **Claims**, make sure you select the **Resources** API.
3. Check the **Get** claim.

For more information, see "(product name) product API" in the *(product name) Self-Service Administrator Guide*.

Create the application in (product name) for (product name)

The (product name) application records contain basic information about (product name), including the location of the (product name) APIs, the resources for which (product name) is the authoritative source, and the API key.

About this task

Perform this procedure to create one application for the (product name) authoritative source application in (product name).

Procedure

1. On the (product name) header bar, click the gear button, then select the environment where you want to perform this procedure.
When you log into (product name) for the first time, the **Enhance Your Experience** page displays. Decline or allow (company name) to enable cookies to track your usage in (product name) using Google Analytics.
2. In the (product name) header bar, click **Applications**.
3. In the **Applications** page, on the **Create New App** section, click **Manually**.

-
4. In the **Add Application** dialog box, create your application by clicking **Continue**.

Warning! Do not select any of the available options.

Result: (product name) displays the Add Application wizard.

5. On the **Application Details** page of the wizard, enter the information described below and then click **Next**.

Field	Entry
Application name	Enter a unique name for this application. Make sure that the name uniquely identifies this application. When you need to select an application elsewhere in the (product name) user interface, you will use the name to select the correct application. Examples: (product name) Integration API
Description	(Optional) Enter a description of this application.

6. Click **Skip**.
(product name) does not subscribe to changes published by other (product) applications.
7. Click **View Application** if you are ready to configure application-specific settings, or click **Back to Applications** if you want to just create the application now and configure settings later.

Set up (product name) API key in the subscriber

Enable the messaging between the authoritative source application created in (product name) and (product name) through Service Bus.

Procedure

1. In the (product name) header bar, click **Applications**.
2. In the **Applications** page, locate and click the **(product name)** application name.
3. In the **API Keys** tab, select the **Copy** button to copy the API key of the (product name) application.
4. Paste this API key in the `Message.config` of Service Bus.
For more information, see "Configure Subscriber for (product name)" in the *(product name) Install Guide*.

Auto-configure resources that are owned by (product name)

Procedure

1. On the (product name) header bar, click the gear button, and then select the environment where you want to perform this procedure.
When you log into (product name) for the first time, the **Enhance Your Experience** page displays. Decline or allow (company name) to enable cookies to track your usage in (product name) using Google Analytics.
2. On the (product name) header bar, click **Applications**.
3. On the **Applications** page, locate and click the (product name) application name.
4. On the **Application Overview** page, click the **Owned Resources** tab.
Result: Major versions of the resources display. An asterisk displays in the Major Versions column if a resource is deprecated.
5. In the **Authentication Type** field, accept the default of **Basic Authentication**.
(product name) uses basic authentication (username and password) to authenticate proxy API requests from other applications.
6. Enter the Base URI for the (product name) (product) API website then click **Save**.

Field	Entry
BaseURI	Enter the base URI of the (product name) (product) API website, in the following form: <code>https://<hostname>:<port>/<(product)>API/api</code> where <hostname> is the name of the web server hosting the (product name) (product) API, and <port> is the port number you specified when you created the website.

7. Click **Auto-configure resources**.
8. In the **Request Resources from Application** dialog box, enter your username and password. These credentials are the ones you set up in section "Create the (product name) application user for (product name)", then click **Next**.
9. Click **Close**.

Update the (product name) owned resources after an (product) API upgrade

Update the (product) applications for (product name) with any changes to (product name)' owned resources resulting from a new version of the (product name) (product) APIs.

About this task

When you originally created the (product) applications for (product name), you added the resources that (product name) owns. A new version of the (product name) (product) APIs might include changes to the resources owned by (product name). Perform the following procedure to update the (product) applications for (product name) with any changes to (product name) owned resources.

Perform this procedure for each (product) application that you created for (product name).

Procedure

1. On the (product name) header bar, click the gear button, and then select the environment where you want to perform this procedure

When you log into (product name) for the first time, the **Enhance Your Experience** page displays. Decline or allow (company name) to enable cookies to track your usage in (product name) using Google Analytics.
2. On the (product name) header bar, click **Applications**.
3. On the **Applications** page, locate and click the (product name) application name.
4. On the **Application Overview** page, click the **Owned Resources** tab.

Result: Major versions of the resources display. An asterisk displays in the Major Versions column if a resource is deprecated.
5. Click **Auto-Configure Resources**.
6. In the **Requests Resources from Application** dialog box, enter the username and password for (product name) account with access to the (product name) (product) API.
7. Click **Next**.

The list of resources owned by (product name) is automatically updated to reflect changes in the new version of the APIs.
8. Click **Close**.

Create (product name) users for Proxy API requests

Create a user in your ERP to support proxy API requests from (company name) applications

Create administrative users in (product name) and assign the appropriate API permissions, to allow those users to make proxy API calls to (product name).

Use the same procedures to set up a user for each proxy application you create. Assign the user permissions to the (product) API that corresponds to each application.

Create the API user

The Users option allows you to create and edit users, reset password, generate tokens, list the user's tokens, and delete accounts for (product name) (product) API.

For more information on how to create users in (product) API see "Users in (product) API" in the *Self-Service Administrator Guide*.

Define the role for the API user

Assign a role to a user.

First, you need to create roles in (product) API, for more information, see "Roles in (product) API". Then, you can assign the role to a user, for more information, see "Edit (product) API user account" in the (product name) *Self-Service Administrator Guide*.

Assign permissions to the API user role

The (product name) (product) API provides some claims that you can map to a role. You can add claims or change the existing mapping to a role

To set up a user with access to ILP resources, assign the claims for the APIs located in ([link](#)).

To set up a user with access to Experience resources, assign the claims for the APIs located in ([link](#)).

If the API requires **Read** permissions, in claims, select `Get` and `Get.id`

If the API requires **Update** permissions, in claims, select `Post` and `Put`

For more information about how to assign claims in (product) API, see "Configure claim mapping to an (product) API role" in the (product name) *Self-Service Administrator Guide*.

Set up (product name) mapping

Add mapping records allows to integrate (product name) values with (product) enumerations.

Create mappings for the code values on each code table, for the application you want to integrate with.

Code Table name	(product) API	ILP	Experience
Address type	address-types	X	X
Curriculum	academic-disciplines		X
Degree	academic-credentials		X
Email type	email-types	X	X
Institution type	educational-institutions	X	X
Person phone type	phone-types	X	X
Record type	persons	X	X
Release information	privacy-statuses		X
Stop list	person-hold-types		X

For more information about how to add ethos mappings, see "Configure Code values with (product) mapping" in the *(product name) Web Administration Handbook*.