Manage API settings

Updated: 2025-04-23

You can configure and export API settings in (company name) (product name).

API settings

To use (product name) (product name) APIs to develop integrations that leverage (company name) (product name), see *Use (product name) (product name) APIs*.

To configure ISO codes, leverage the **API Configuration** tab. See Configure ISO Codes.

To configure API settings, see Set up API settings.

To export API settings from an application to a CSV file, you can click **Export API Settings** on the **Owned Resources** tab of an application. See Add owned resources to an application (single owner).

If you select **Export API Settings**, or if there are some resources that have available API settings to configure, they display as a hyperlink in the **Resource** name list. If you click the hyperlink or select the application on the **API Configuration** tab, you can view the resource configuration.

If you do not see hyperlinks on the resources, check for errors. See Troubleshooting API settings.

Configure ISO Codes

Updated: 2025-02-24

You can set up ISO Codes on the **API Configuration** tab in (company name) (product name).

Procedure

1. Select **Tools > (product name) > Integration**, 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 (product name)** 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 **API Configuration**.

   Result: Applications that have settings that are available for configuration load and then are available in the **Application** drop-down list.

3. Select an application to configure from the **Application** drop-down.

   You can click the drop-down and see a list of applications that have settings available for configuration.

   Result: The **ISO Code Settings** and **Upgrade Actions** tabs display.

4. On the **ISO Code Settings** tab, select the following configuration values for the application. and then click **Save**.

   • Country

   • Currency

   • Language

   • Region

   • Subregion

5. On the **Upgrade Actions** tab, if the Base URI for applications with owned resources received upgrades, you are prompted to auto configure resources again for that application.

6. **Optional:** To export API settings from an application to a CSV file, go to the **Owned Resources** tab of an application and click **Export API Settings**.

   If you receive a 400 error, verify that your Base URI and credentials are correct and try the export again. See Add owned resources to an application (single owner).

Set up API settings

Updated: 2025-03-19

You can set up API settings on the application that has owned resources in (company name) (product name).

Procedure

1. Select **Tools > (product name) > Integration**, 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 (product name)** 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 application name that has owned resources.

   Use the **Search Applications** field to search for an application, if needed.
4. Click the **Owned Resources** tab.
5. Select an owned resource from the list.

   Result: The **Resource Defaults** tab displays.
6. Locate the row for the owned resource and click the edit button  .
7. Select a **Source Value** and then click **Save**.

   See *API Integration Configuration Settings* for the values you should configure for (product name) APIs.

Troubleshooting API settings

Updated: 2025-04-23

If you are unable to access the hyperlink to configure settings, consider conditions that may be the cause.

What if APIs have settings, but are not showing the hyperlink to configure settings or if I receive a 400 error when I export an API?

Within the (product name) UI or (product name) in (product name), the resource names that pass the conditions below are enabled with a hyperlink. This hyperlink provides the ability to modify the API settings for the resource configuration value(s). The resource needs to pass the following conditions:

1. The resource is listed inside the response payload of the *resources* API.
2. Update the Base URI and ensure the Accept header includes:

Source application URL	Accept header values
<baseUri>/mapping-settings	application/vnd.hedtech.integration.mapping-settings-options.v1.0.0+json
<baseUri>/default-settings	application/vnd.hedtech.integration.default-settings-options.v1.0.0+json

<baseUri>/configuration-settings	application/vnd.hedtech.integration.configuration-settings-options.v1.0.0+json
<baseUri>/compound-configuration-settings	application/vnd.hedtech.integration.compound-configuration-settings-options.v1.0.0+json
<baseUri>/collection-configuration-settings	application/vnd.hedtech.integration.collection-configuration-settings-options.v1.0.0+json

Note: If one of the endpoints above returns a status code that is not 2xx, no resources are hyperlinked. If all endpoints succeed, resources that meet the conditions above are hyperlinked.

Manage (product name) API keys

Updated: 2020-11-10

You can add or remove API keys for an application.

Applications integrating with (product name) are identified by their unique API keys, which serve as credentials. (product name) supports provisioning two types of API keys to an application:

- Unrestricted API Key - Accepts requests from any integrated applications with the appropriate credentials set up in (product name).
- Restricted API Key - Specify an IP address or range of IP addresses. Applications making requests using a restricted API key must make requests from the IP addresses within the specified range. If the request originates from an IP address outside the specified range, the request is denied and an error response is returned.

Related information
Best practices for securely using API keys.

Best practices for securely using API keys

Updated: 2026-01-06

Applications integrating with (product name) are identified by their unique API keys, which serve as credentials. It is important to keep your API keys secure.

To ensure your API keys are secure, follow the best practices below:

- Do not embed API keys directly in code. API keys that are embedded in code can be exposed if you share the code. Instead of embedding your API keys in your applications, store them in environment variables or in protected files outside of your application source tree.
- Do not store API keys in files inside your application source tree. If you store API keys in files, keep the files outside your application source tree to help ensure your keys do not end up in your source code control system. This is particularly important if you use a public source code management system, such as GitHub.
- Restrict your API keys to be used by only the IP addresses that need them. By restricting the IP addresses that can use each key, you can better ensure security. Refer to Modify API key restrictions.

- Restrict your API keys to be usable only for certain APIs. Integrated applications only to the APIs they need for integration functionality and no more. Or, if you are a (product name) customer, refer to Set up proxy API requests (multiple owners).
- Delete unneeded API keys. To minimize your exposure, delete any API keys that you no longer need.
- Change your API keys periodically. Refer to Change the API key.

Add an API key and manage IP restrictions

Updated: 2025-12-17

(company name) (product name) automatically creates one API key when you create an application. You can create additional API keys to use with the application.

About this task

Create a new API key and manage IP address restrictions.

Procedure

1. Select **Tools > (product name) > (product name)**, 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 (product name)** 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 application name.
4. On the **Application Overview** page, click the **API Keys** tab.
5. Click **Add API Key**.
6. Do one of the following:

a. The option to **Add API key to have IP address restrictions** is enabled by default.

i. Add a list of comma-separated IPv4 or IPv6 addresses that can use the API key.

b. Alternatively, select the **Add API key to have no IP address restrictions** option.

7. Click **Add**.

Change the API key

Updated: 2020-11-10

For security, you might want to periodically change the API key associated with an application.

About this task

To ensure that the application is available throughout the process, do the following:

- Create a new API key for the application. At this point, both the original API key and the new API key are active.
- In all places where you previously stored the API key (for example, in code or in a configuration form), update the stored API key to match the new API key.
- Remove the original API key.

Procedure

1. Select **Tools > (product name) > Integration**, 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 (product name)** page displays. Decline or allow (company name) to enable cookies to track your usage in (product name) using Google Analytics.

2. Create the new API key:

a. On the (product name) header bar, click **Applications**.

b. On the **Applications** page, locate and click the application name.

c. On the **Application Overview** page, click the **API Keys** tab.

d. Click **Add API Key**.

e. Locate the row for the new API key and click the copy button.

3. In all places where you previously stored the API key for this application (for example, in code or in a configuration form), update the stored API key by pasting in the new API key.

4. Remove the old API key:

a. On the (product name) header bar, click **Applications**.

b. On the **Applications** page, locate and click the application name.

c. On the **Application Overview** page, click the **API Keys** tab.

d. Locate the row for the old API key and click the delete button.

Note: When there is only one remaining API key for an application, you are unable to delete it, and the following message displays: `Each application has a minimum of one API Key.`

Create an application and modify API key restrictions

Updated: 2026-01-06

Create an application with API keys restricted by default and then add a IP address or multiple addresses to make them unrestricted.

About this task

When you create an application, by default, the API key is restricted for all IP addresses. You can add multiple IP addresses or make the API key unrestricted.

Procedure

1. Select **Tools > (product name) > Integration**, 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 (product name)** 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. In the **Create New App** area, click **Manually** or **From Catalog**.

4. Follow the wizard to create an application. For specific ERP/CRM wizard details, see Connect applications to (product name).

   Result: The **Finish** page of the wizard displays a message that says the application has been successfully added. By default, this API key is disabled for all IP addresses. To update this API key to unrestricted for all IP addresses or by IP addresses you have three options in the wizard:

   a. Select the **Edit your new API key to allow IP access** hyperlink.

      i. The option to **Set API key to have IP address restrictions** is enabled by default.

      ii. Add a list of comma-separated IPv4 or IPv6 addresses that can use the API key.

      iii. Alternatively, select the **Set API key to have no IP address restrictions** option.

      iv. Click **Save**.

   b. Click **View Application** and copy the API key for use.

When making an API key available for use for one or multiple (company name) products, use the following IP addresses:

(company name) (product name)	*(product name) domains and IP addresses*
(product name)	*ILP domains and IP addresses*
(company name) (product name)	*(company name) (product name) NAT gateway IP addresses*
(product name) (product name)	*Whitelist the (product name) IP addresses*

Note:

- To modify API key restrictions, see Modify API key restrictions.
- On the **Application Overview** page, API keys highlighted in yellow do not have IP restrictions.
- To add a new API key to an existing application, see Add an API key and manage IP restrictions.

Modify API key restrictions

Updated: 2026-01-06

For security, you can add IP address restrictions, or you can remove IP address restrictions.

Procedure

1. Select **Tools > (product name) > Integration**, 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 (product name)** 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 application name.
4. On the **Application Overview** page, click the **API Keys** tab.
5. Locate the row for the API key and click the edit button  .
6. To remove IP address restrictions, click **Set API key to have no IP address**

restrictions.

7. To add IP address restrictions, click **Set API key to have IP address restrictions**.

    a. Enter the **Source IP Address**, or a range of IP addresses.

    b. You can add multiple IP addresses, separated by commas.

    When you add IP addresses to an API key, only the IP addresses you add can be used for proxy calls that leverage that API key.

8. Click **Save**.