Rest and Learn

Mark O'Neil

Managing REST Integrations in Learn: The REST Integrations Tool for System Administrators

Overview of the REST API Integrations Tool

For the other tasks related in this document, use the REST API Integrations.

To navigate to the REST API Integrations tool:

1. Select **System Admin** in the main screen of Learn.
2. Select the **REST API Integrations** link is in the Building Blocks section:

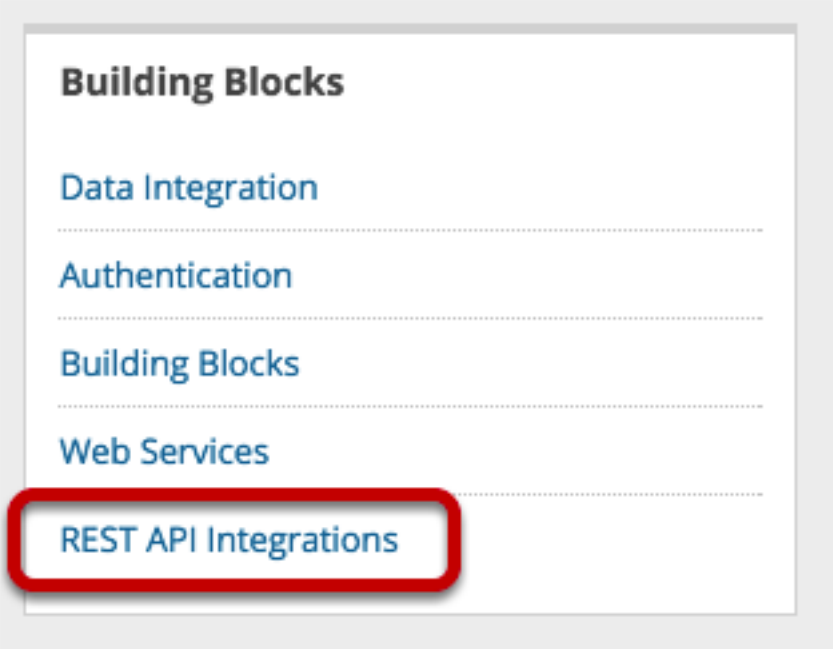

Figure 1: REST API Integrations

The main page for the REST API Integrations tool:

- Lists existing integrations
- Allows you to manage existing integrations
- Allows you to create new integrations

This list will be empty if you have not created any integrations.

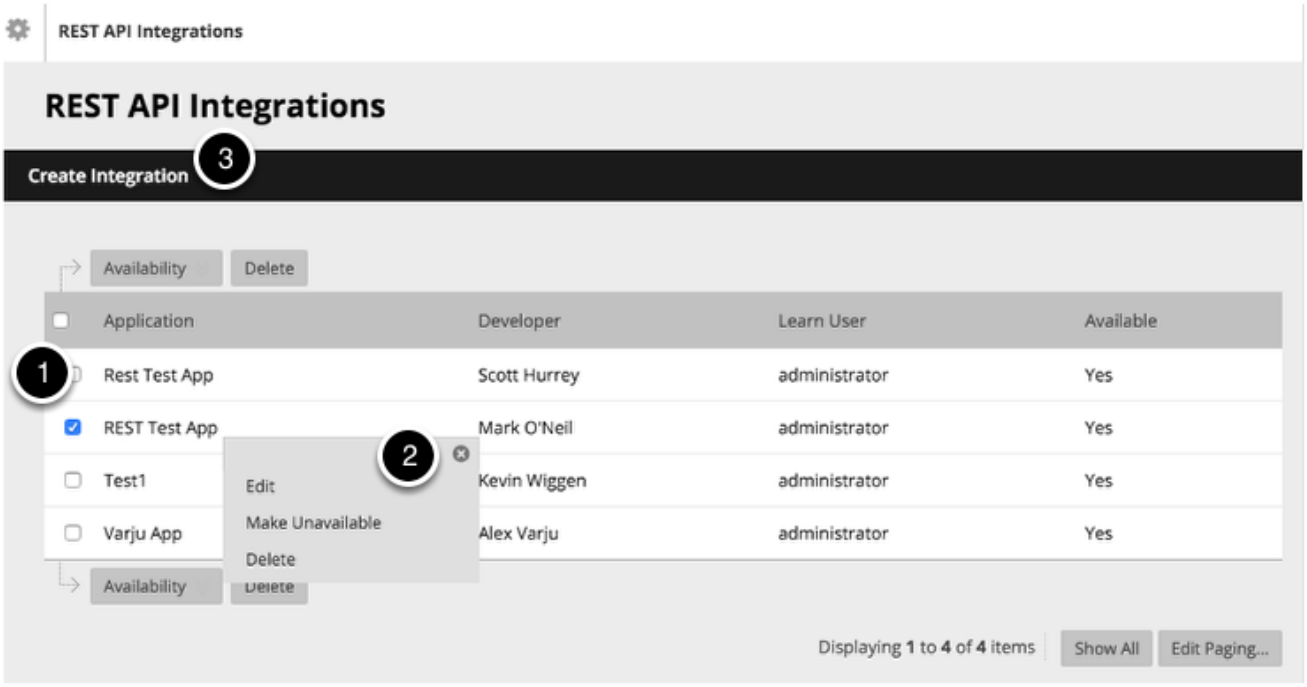

Figure 2: REST API Integrations

Create an Integration

An integration, here, refers to an external REST application being registered to work in conjunction with Learn. Before you create an integration, the best practice is to create a Learn user with entitlements that match those required by the REST application.

To create an integration and thereby allow an application to work with your instance of Learn:

1. On the REST API Integrations page, select **Create Integration**.
2. In the **Application ID** space, enter the application ID proved by the integration's developers.
3. Select **Browse** next to Learn User. Search through the list of Learn users to find the user that the integration should act as.
   Select a user that you specially create for the application and that has only the permissions that the integration needs to function properly.
4. For third-party integration, set **End User Access** to Yes. End users will sign in with their own Learn ID to use the integration. Each user's access is then limited to his or her own permissions. If you set End User Access to No, the integration always has access as if it were the Learn user indicated on the form.
5. **Submit** to save your settings for the integration.
6. Select the Learn user in whose name the application acts. This user must have the entitlements required by the REST Application. For more information about identifying required entitlements, see *Converting Documented Entitlements to GUI Privileges*, below. Note that the Institution role of this user has no impact on the entitlements, only the privileges on the user's System role.

Learn user entitlements are allow a REST application to act in your Learn environment. The best practice is to restrict these except as necessary to allow the REST Application to function. The vendor or developer of the REST application should provide a list of required entitlements.

NEVER configure a REST application to act as a System Admin user. Doing so gives the REST application full access to all data and operations of your Learn environment possibly resulting in IRREPARABLE harm. If a vendor requests a System Admin user for their application, do not allow it. In such a case, please provide the vendor's

contact and application information to developers@blackboard.com so that we can help the vendor correct the situation.

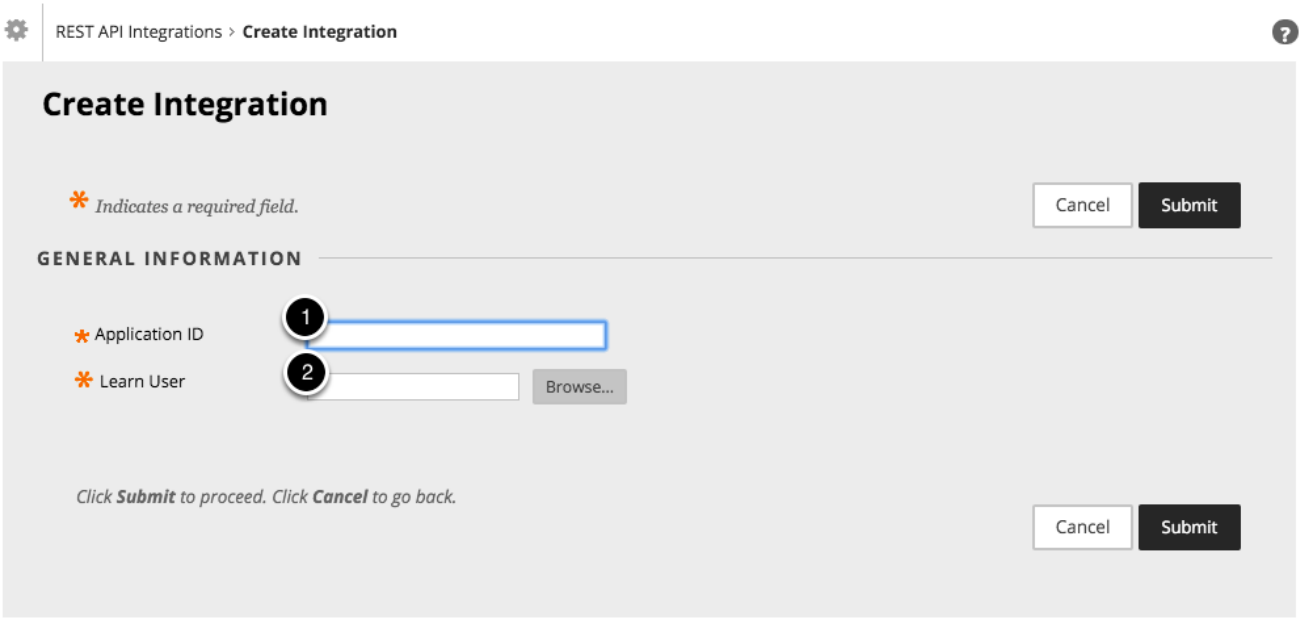

Figure 3: Create REST integration

Note: If you are an Anthology client, an Anthology Partner / Vendor / Developer of an LTI or REST Application should NEVER tell you to go to the developer portal and create an App ID with the associated key/secret to install their application. They should never tell you to apply for a Rate/Site increase for their application. Anthology DOES NOT support that model. Every REST Application developer should give you an App ID to install their REST App and tell you how to configure a system role for its use. Period. The REST Application developer needs to request the increases they need to run their application themselves. If they ask you to go to developer.anthology.com and get an App ID/Key/Secret, please tell them that is wrong. They should have exactly one App ID for their production REST application that they are asking you to install.

Contractors are an exception to this policy as they are producing an integration on your, the Anthology client, behalf. Questions regarding the policy and whether you are impacted may be asked here, or posted to developers @blackboard.com.

Managing your REST Integration

Once you have created a REST integration, you can manage it:

1. Edit the integration settings
2. Set the integration availability
3. Delete the integration

Edit a REST Integration

The editor displays information about the integration and allows you to change the Learn user that the integration runs as. This allows you to manage the permissions on the integration.

To edit an application's settings, navigate to the REST API Integrations tool. Select **Edit** from the context menu of the integration that you want to edit. A screen opens like one below.

You may use the standard Learn user and role tools to create an integration- specific user.

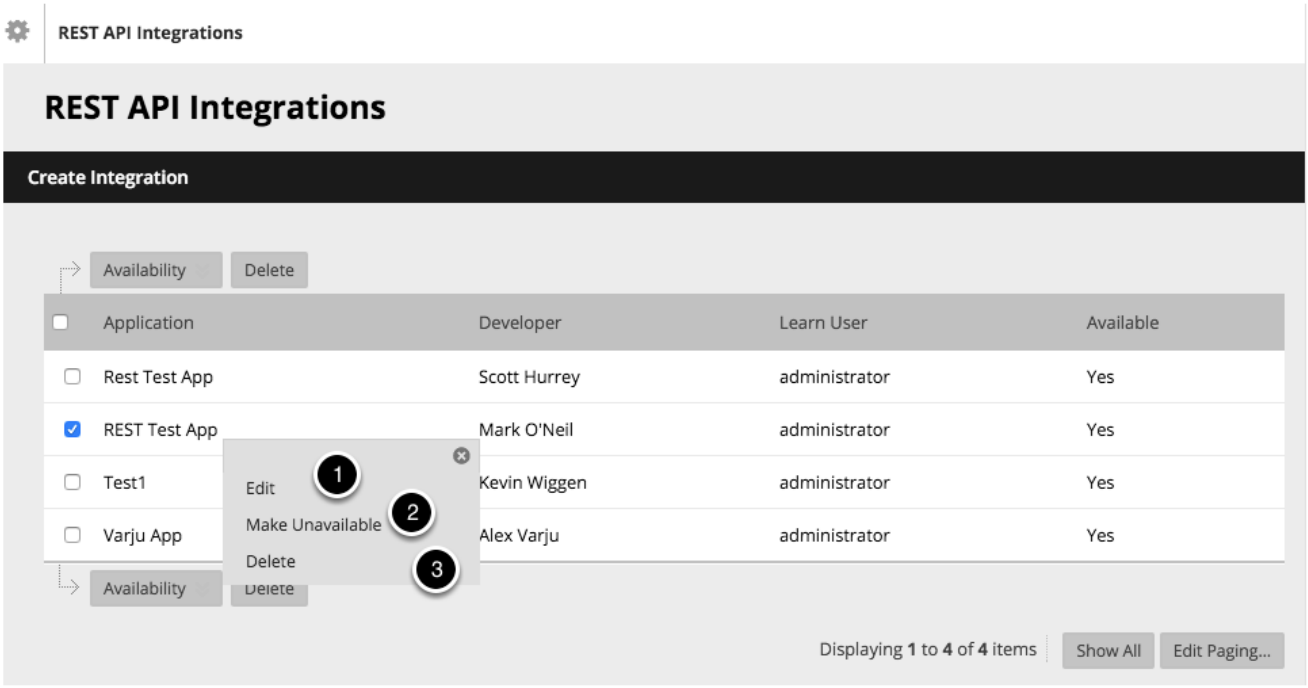

Figure 4: managing your rest integration

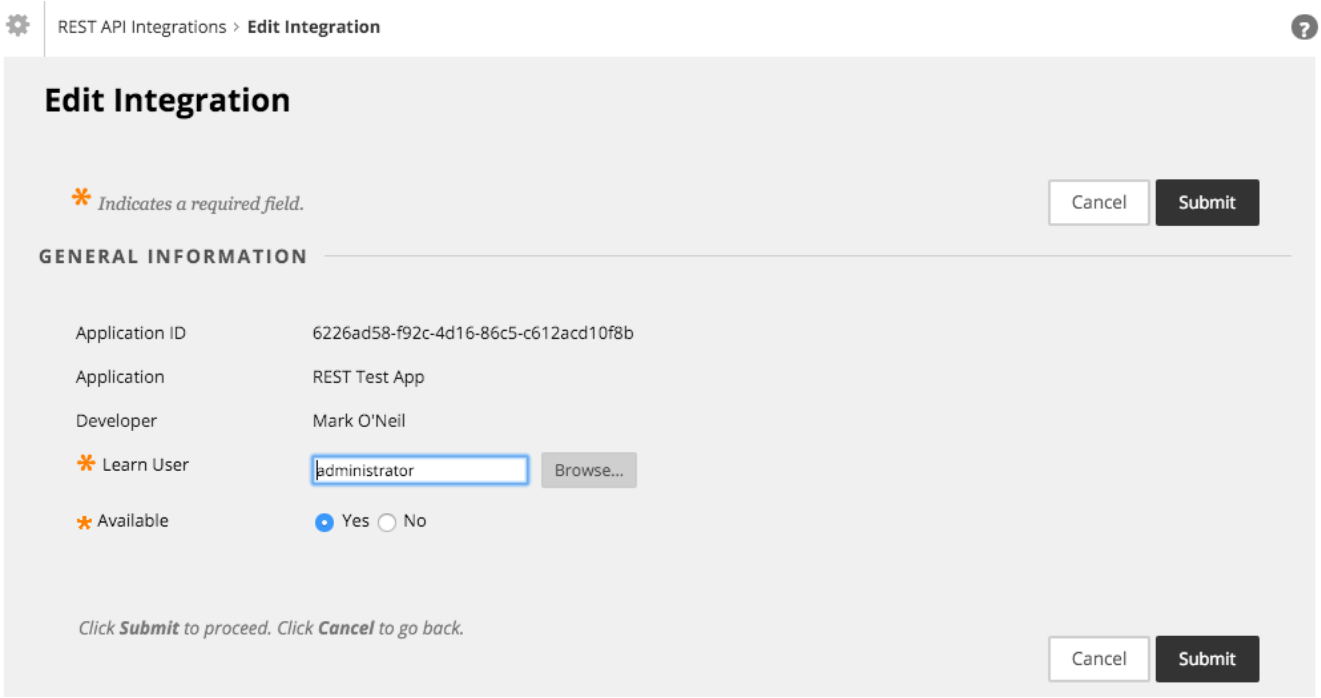

Figure 5: edit a rest integration

Running an Integration

An REST integration can be run in two ways. In both cases, the application is actually remote to the Learn environment.

1. A user selects a link within Learn which calls the remote application
2. A remote system call from the REST application

Converting Entitlements to GUI Privileges

There are a number of ways to accomplish this.

- Check out this blog, Bookmarklet To Help Map Entitlements to Permissions
- Check out this JSHack contributed by Matthew Deeprose.
- The EntitlementsToAdminGUI worksheet (updated 08/10/2019 9:57 AM) helps identify the **entitlements** to a string which may be searched on in the role **privilege** selection page when creating the role for your REST Application user. Paste the documented **entitlement** from the REST API documentation to column A and the **privilege** will appear in column B.
  - Here's a video demonstration.
- Should the spreadsheet not have what you're looking for, here's the way to find these manually: Dropbox - 2018-10-30_13-39-25.FindingPrivilegeForGivenEntitlement.mp4

Delivering your REST Integration

For a more detailed process please see Releasing your REST Integration

Step 1: NEVER USE OR REQUIRE SYSTEM ADMINISTRATOR as your REST application user.

Step 2: You determine from the API Docs which Entitlements are required for the integration.

Step 3: You set up a non-System Administrator User associated with the your REST API integration on your test system.

Step 4: You utilize your test system and the API Docs to identify the list of Learn Privileges required for the integration.

Step 5: You configure your test system integration user appropriately and validate successful integration operation using your identified Learn Privileges

Step 6: You provide the client the REST Application Id, a preferred/suggested user and role name (E.G.: Integration User, Integration Role), and a list of required Privileges for the Integration User Role.

Step 7: Include information from Step 6 in your client facing documentation.

Key takeaway: Providing the required Privileges to Learn Admins reduces the risk of a failure in integration installation and operation. Anthology nor you should want to burden clients with figuring out from the API Docs which Entitlements are needed and look up these Privileges on their own so that your application works as expected.