Blackboard

The Blackboard REST API Framework

Date Published: Apr 26,2016 **Category:** Product:Installs_and_Configurations_Learn; Version:Learn_9_1_Q2_2016_3000_1_0_rel_52_991d   **Article No.:** 000053330

Product: Blackboard Learn

**Document Type:** Administrator Documentation

Document Summary:

Blackboard's new REST API Framework is a giant step forward for integrating with Blackboard Learn. By moving the integration from in-process code to a separate machine the health of your Blackboard Learn instance is dramatically improved by lowering complexity and reducing the amount of code running in a single location. The new REST API and Developer Portal are a work in progress and will continually grow in functionality as Blackboard Learn, the REST APIs, and the Developer Portal continue to mature. For additional information, please refer to docs.blackboard.com and community.blackboard.com/developers.

Information:

The Actors in REST API Use Cases

There are three actors in the REST API use case:

1. ***Developer:*** This is the person who writes an application that uses the new REST APIs. Through the application the developer manages authorization using the registered application's OAuth Key and Secret, any data sent to or received from Blackboard Learn, and tracks application entitlements required for operation. *Developers are limited to non-production testing pursuant to the applicable REST Developer Agreements.*

2. ***Blackboard Learn Administrator:*** By default, no Applications can access the REST APIs. A Blackboard Learn Administrator must enable each app from the Blackboard Learn Admin Panel before access is granted. This is done by creating an integration using the Blackboard Learn Admin REST API Integrations tool using the developer provided application Id and a User with the required entitlements as specified by the developer. *Important Note:* By default NO integrations are enabled and the Blackboard Learn server will not allow integrations without a Blackboard Learn Administrator taking action.

3. ***Blackboard Learn Administrator:*** The Developer Portal: This is a new website (https://developer.blackboard.com) where a developer can browse the REST API documentation, register as a REST Developer, and register application references for integrating with Blackboard Learn.
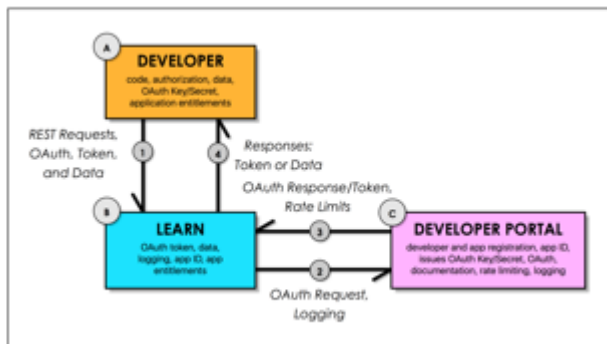
How These Three Actors Work Together to Enable Blackboard Learn REST Integrations

A developer (A) - or organization - decides that they want to create a new application which uses the Blackboard Learn REST APIs. She reviews the documentation and signs up inside the developer portal (C). Once she registers, she may create one to many applications. Creating an application provides an OAuth Key and Secret which is used to authorize Blackboard Learn REST API access and an Application ID that is used to approve Blackboard Learn instances.

The developer uses the Blackboard Learn Admin REST API Integrations tool on a Developer Virtual Machine (B) or their Test instance of Blackboard Learn (B) to enable access within Blackboard Learn by providing the application ID for the particular application in development. Once the Application has been enabled, the developer may now issue REST requests against the specific Learn server. These HTTPS requests are issued directly against the Learn instance and are secured by OAuth 2.0.

Once the application development and testing is completed, the developer shares the application Id and the required entitlements with the Blackboard Learn admin to enable access within Blackboard Learn for the particular application. The admin inputs the application Id provided by the developer and assigns a Blackboard Learn User that the integration will run as. The role for this user must have the entitlements as requested by the developer. This user can be an existing user or a newly created user specific to the application. The application will run as this user in Learn and will thus have all the rights that the user has in the system. If the admin wants to allow the application only READ access, this can be done with the security system already available in Learn by assigning the user role READ only entitlements.

Data Exchange between the Actors

The request BODY or response is *never* sent to the developer portal. Personal data is exchanged between the application and Blackboard Learn system only - no personally identifiable data is shared with the portal. Therefore, all data may remain within the Learn server and REST application regions.

Primary key identifiers (e.g. Learn PK1 for User or Course) are shared with the portal for purposes of request logging and error messages. Note that in an upcoming release of Learn these PK1s will also be anonymized so no PII information is ever communicated outside the bounds of Learn-to-application exchanges.

Data Flow
Pre-authorization

1. The developed application first makes an authorization request to their Learn server. This request contains the OAuth Key and Secret provisioned on application creation in the developer portal.
2. Learn receives the request and asks the Developer Portal for a TOKEN if the KEY/SECRET are correct and valid for that Learn instance.
3. The Developer Portal returns a response to Learn containing a TOKEN if validation was successful.
4. If validation is successful Learn caches and returns the TOKEN in the response to the application or returns a 401 Invalid client credentials.

Note: Tokens have a lifecycle of one hour and currently are not revocable.

Post-authorization

1. Once authorized, the application may then make data oriented requests to Learn by including the issued Token.
2. Developer data oriented requests are processed by Learn which returns response data to the requesting application.
    1. Learn checks the local cache to validate the TOKEN – if valid it runs and returns the request response.
    2. In a background thread Learn contacts the developer portal indicating a specified request was used by a TOKEN on a Learn server.
    3. The developer portal responds to Learn to indicate if the TOKEN is still valid (not revoked) and is still running under the rate limits.
        1. If the TOKEN has been revoked or rate limits have been reached, all future requests for that token will fail.

Note: Learn sends REST transaction and error log messages to the portal for purposes of API management and usage. The data sent to the portal includes the Learn Instance ID, Developer Application ID, and the REST API used (GET /users/ for instance).

Rate Limiting

In the background, the Learn instance securely communicates with the Developer Portal to enable rate limiting on the Developer Application. This is done by telling the Portal how many and which type of REST calls are being issued to Learn.

For the duration of the technical preview we have set the rate limit on a developers suite of applications to individual institution integrations at 10,000 requests per 24 hour period. As the Technical Preview progresses we will be collecting data on usage which will be analyzed to determine Customer and third party developer production grade rate limits when the Technical Preview is lifted.