



Brivo Technology Partner Program Overview

Welcome to the Program

We are excited to have you join the Brivo Technology Partner ecosystem

Why Work With Us?

Brivo is the global leader in mobile, cloud-based access control for commercial real estate, multifamily residential, and large distributed enterprises.

Our comprehensive product ecosystem and open API provide businesses with powerful digital tools to increase security automation, elevate employee and tenant experience, and improve the safety of all people and assets in the built environment.

2M

Mobile Credentials

+50K

Commercial Accounts

425K

Managed Entries

+450M

Sq Ft of Real Estate Protected

90K

Customer Sites

Global Reach
Securing Buildings in **60+** Countries

Let's Get Started

Below outlines the integration onboarding and certification process to help you get started with planning your engagement with Brivo

Quick Links

[Brivo API Integration Build Guide](#)

[Integration Application Checklist](#)

Brivo API Capabilities

Brivo Access is a consumer of the Brivo RESTful API. Brivo has exposed a significant number of capabilities in the API include, but not limited to:

- Provisioning users and user permissions
- Creating schedules
- Deploying credentials (including physical, PIN code and mobile)
- Subscribing to events subscriptions via webhook to extract events

Documentation & Registration

Brivo's open RESTful API and documentation is available at developer.brivo.com The first step in building your integration to Brivo is to set up a sandbox account. To do this, simply register at developer.brivo.com and send an email to BrivoAPI@brivo.com letting us know the purpose of your integration and application and requesting sandbox access.

We will either set up the sandbox upon receipt of the email or a member of the team will reach out to you to discuss if further information is needed.

Sandbox accounts are production accounts that do not have access control data. If you require gear to input access control data and/or to test your integration once complete you can purchase a demo kit or borrow one with an option to purchase or return. The Brivo Partnerships team can assist with this process.

Introductory call

Once the sandbox is set up and your integration team has conducted an initial review of the API documentation, we recommend you set up a call with the API Partnerships and Technical support team. The call lasts approximately 30 minutes. During the call, the team will review the Brivo application and the way the functions and naming conventions are reflected in the API. This will set your team up for success with the integration.

Build Guide

When building your integration, please follow the guidelines in the [API Build Guide](#) below. This will ensure that your integration is constructed with maximum efficiency.

Integration Completion

Upon completion of your integration, please submit the API integration partner intake form and arrange for a certification demonstration with the Brivo team including Brivo Partnerships, Product Marketing and API Support. This session will allow Brivo to confirm the correct operation of the integration and to get a basic understanding of the value proposition.

Upon certification, Brivo will provide following resources for all new integrations to support teams in the field:

- Simple sales collateral (1-pager)
- Sales slides for the Brivo API Information center. This information repository is the source for the Brivo global sales team about integrations
- Listing on [Brivo.com technology partner integrations](https://brivo.com/technology-partner-integrations)

There may be additional opportunities to do joint marketing and promotion activities. Those will be assessed individually.

Ongoing Partnership Management

Once certified and launched, the Brivo Partnerships team will be your main contacts at Brivo and will enlist other resources (marketing, sales, product, etc.) as needed.

Summary

We are excited to work with you and add you expand our world-class ecosystem of technology partners. For questions, please contact your Brivo Partnerships representative.

Brivo API Integration Build Guide

Authentication:

Which Authentication method should be used?

Developers should use OAuth2 3-legged authorization code workflow.

- You can use the same client id and client secret to simplify the configuration process.
- You should not have to store customers' login credentials.

For instances when your integration is a server to server interaction, you can contact API support for alternative authentication workflow.

Brivo requires each customer to use their own, unique API key for each application. If you are using authorization code workflow, it is best practice to include a field for the API key before sending the user to the authorize page.

API keys are added to the integration owner's developer account (developer.brivo.com).

What credentials should be used?

In Brivo Access, administrators are now required to log into Brivo Access with their email address. This has not changed the authentication process for the API. You are still required to use the administrator ID and password for the administrator being used to configure the integration.

For all new integrations, a service administrator should be created. This will help maintain clear audit logs and allow for setting permissions specific to the integration. This will also prevent accidental deletion.

To create a service administrator:[AMN1]

- 1 Log into Brivo Access with a primary or super administrator account.
- 2 On the left navigation bar, navigate to the Administrators tab.
- 3 Once you are on the Admin Management page, click on the Create Admin button.
- 4 If you would like to add assignments or roles to this administrator, you can do so now.
- 5 If you need more information on roles and assignments, please find our additional how-to videos or help guides.
- 6 Once done, scroll down to the bottom of the page and click the Create Admin button at the bottom of the page to complete the process.

To locate your administrator ID:

- 1 Log into your service account as the administrator.
- 2 Click the Onair Classic button on the navigation bar.
- 3 The administrator ID will be documented on the home screen of Onair Classic.

To locate your client id and secret:

- 1 While logged into Onair Classic, click on the Application Management tab on the Account Settings page.
- 2 The Create a New Application page displays.
- 3 To create a new application, enter the Application Name, Description, select an Authentication Type, and enter the Redirect URL and click the Create Application button. The information entered will appear in the Account Owned Applications field below. To view an existing application, click on the Application Detail button to reveal the Application Details popup window with a list of Client ID, Client Secret, Grant Types, and Redirect URL

[AMN1] It's better to make this part of the instructions rather than adding it as an afterthought.

Application Details:

Where to locate API keys?

API keys can be retrieved from the Brivo Developer portal, developer.brivo.com. You are free to create developer API keys for development purposes. Developer API keys have a monthly limit of 25,000 calls and a 25 call per second limiter. Please do not use developer keys for production deployments. This typically leads to integrations failing and having to troubleshoot and update code.

Production API keys are added to the developer account associated with the integration. This can only be done by a Brivo team member and is typically done when the API feature is enabled on a production account. API keys can be provided to the customer upon enabling the feature if an application is designed using an oAuth2 authorization code workflow.

Production API key limits have a 50 call per second limit and a tiered monthly limit:

Tier 0	Tier 1	Tier 2	Tier 3
100k	500k	1m	2m

How is the API Billed?

Brivo bills for the use of the API through the Brivo Authorized dealer unless otherwise agreed upon between Brivo and the API partner.

Note: For users of the Brivo Professional and Enterprise Editions, usage of any API tier is included and is not billed separately.

How is Usage Metered?

API usage is metered on a 30 day rolling window (ie. 30 days prior to today). All API calls received with a specific API key count toward this 30 day usage, including calls that result in an error and invalid calls.

Is Logging Available?

In some instances, Brivo can check logs if absolutely required. Our priority is to ensure that all changes on the account are logged for audit which is done in the administrative journal. It is your responsibility to ensure that your application has adequate logging and you are able to see what the application is doing.

Event Subscriptions vs Manual Event Polling

Brivo has provided a webhook in our API for getting events. There are great advantages to using the webhook as opposed to manually calling the events endpoint on a set interval.

Event Subscription

- One call to configure the subscription.
- Outbound POSTs to your API do not count toward the monthly API limit.
- Events are POSTed to your API in near real time.
- Subscriptions are available for both activity events as well as the administrative Journal.

Manual Event Polling

- Each GET counts toward the monthly quota.
- Delay between event posting and receiving the event.
- You will have to work with filters to get events over a large period of time.

Sandbox Accounts

Brivo will provide free sandbox accounts for development upon request. You will need to provide an outline of our application and indicate whether you are working with an existing Brivo customer.

Our sandbox accounts are empty accounts with no users/doors/devices. This will allow you to work through most basic flows such as Authentication and interacting with objects (ie. users, cards, schedules and groups). If you are building an application that requires events, you may purchase a demo kit which contains a control panel and reader as well as switches and buttons to simulate a request to exit and a door position switch.

You may continue to use your sandbox account for future development and maintenance.

Application Certification

Brivo provides a path to certification with API applications. Once certified, your application may be marketed on our product website and recommended by our sales team for customer use. Certification requires a demo of your application to be provided to the Brivo API and Business Development teams. We will also ask that you complete a checklist to make sure basic functions of the integration meet Brivo's requirements. Please see the checklist on the next page.

Demo Accounts

If your application is available to other customers, the Brivo team requests that you provide Brivo with a demo account to provide to our support team for familiarity and basic customer questions.

Application Integration Checklist

Authentication:

What authentication type is used?

- Credentials in body of Auth call
- Masked Password and client secret

Deployment:

Who will deploy the integration(API Partner/Customer/Brivo Dealer)?

Who does the customer contact for deployment support?

- Configuration guide
- Input for API key

Endpoint Usage:

What endpoints are you using most?

- Accounting for the per second limiter/queue
- Logging
- Error handling
- Who does Brivo contact for development questions?

Support:

Who should customers contact for support?



Contact us at
BrivoAPI@brivo.com