



SAVANCE WORKPLACE

Brivo Integration

Savance Workplace Setup Guide

Revised August 21, 2026

Email: support@savance.com

www.savanceworkplace.com

Overview

This guide covers the setup and troubleshooting of the Brivo integration for Savance Workplace. It shows where to obtain the values you need to enter, explains what each setting does, and describes how the integration behaves once it is running.

At a high level, the integration does three things:

- **Receives access events.** Workplace registers a webhook subscription in Brivo. Brivo then forwards door events to a Workplace event-listener endpoint, and Workplace uses them to update each person's status and location.
- **Imports users and doors** from Brivo, either on demand or automatically as events arrive.
- **Optionally issues credentials** back into Brivo (credential activation and auto-credentialing), including randomly generated card numbers.

Terminology

Brivo's product is now branded **Brivo Access** at <https://access.brivo.com>. Older Savance documentation refers to it as "Brivo Onair." Both names refer to the same platform.

What You Will Need Before Starting

- A **Brivo Access** administrator login (<https://access.brivo.com>). If you do not have one, contact Brivo support.
- A **Brivo API key** (see Step One).
- An **administrator login** for the Savance Workplace site you are configuring.
- The **publicly reachable URL** of that Workplace site, for example <https://cloud.savanceworkplace.com/>, or your own domain if you are self-hosted. Brivo must be able to reach this URL to deliver events, and the same URL is used as the Brivo Redirect URI.

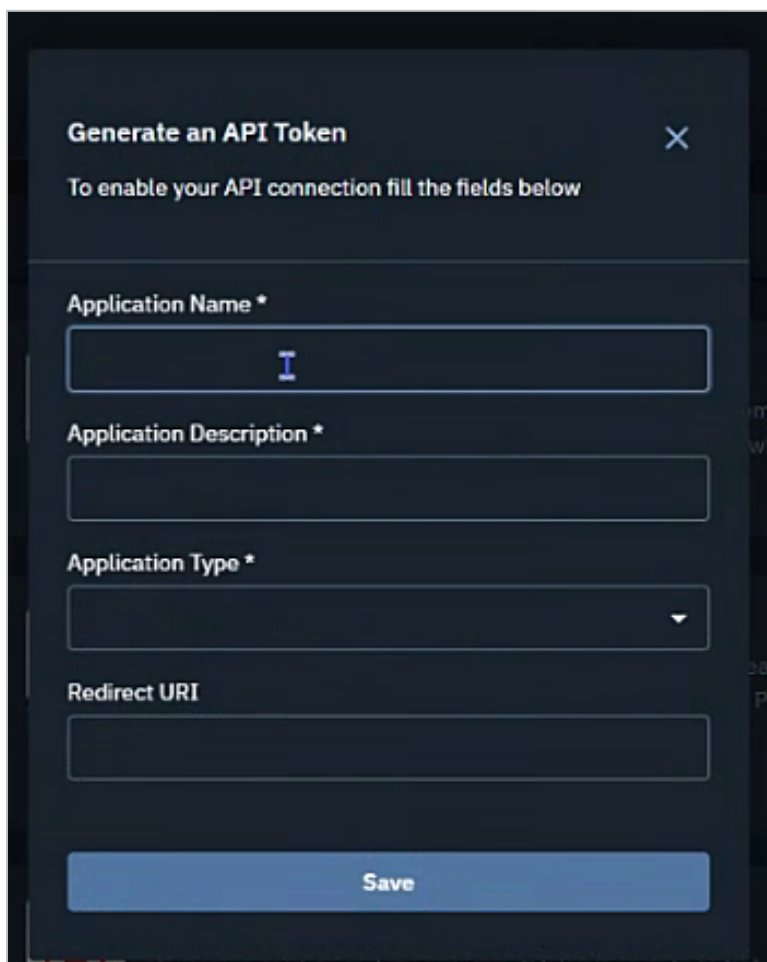
Step One: Obtain a Brivo API Key

The API key is issued by Brivo and is separate from the Client ID and Client Secret that you will generate in Step Two. An API key is unique per Brivo account. When a customer enables the Brivo API for use with Savance, a new production API key is added to the Savance developer account with Brivo.

To obtain the key for a deployment, contact Savance Workplace support at support@savanceworkplace.com (248-478-2555) and identify the Brivo account the integration will run against. Keep the key handy, because you will paste it into the **API Key** setting in Step Four.

Step Two: Generate an API Token in Brivo Access

1. Log in to <https://access.brivo.com>.
2. In the left navigation, open [Marketplace](#).
3. Click **Generate API Token** in the upper right. This button is not available until the API key has been obtained from Brivo.
4. Fill in the **Generate an API Token** dialog using the field guide below, then click **Save**.



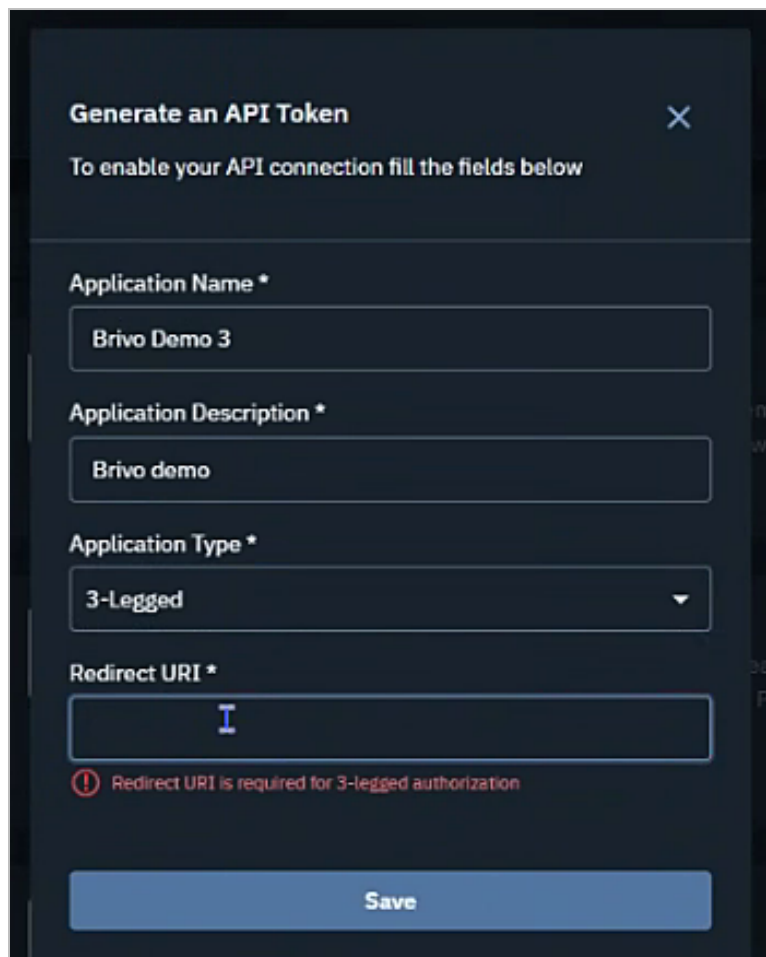
The Generate an API Token dialog, opened from the Marketplace page.

Field	What to enter
Application Name *	Anything you prefer. Use something that identifies the Workplace site, for example Savance Workplace – Cloud. This name is shown to the administrator on the Brivo authorization screen in Step Six.
Application Description *	Anything you prefer.
Application Type *	Select 3-Legged .

Field	What to enter
Redirect URI *	The root URL of the Workplace site you are setting the integration up from. Becomes required as soon as 3-Legged is selected. Brivo shows "Redirect URI is required for 3-legged authorization" if it is left blank.

Use the Redirect URI that matches your deployment:

- Savance cloud-hosted: <https://cloud.savanceworkplace.com/>
- Self-hosted: your own publicly available domain. Use `https` if an SSL certificate exists on the production server.



The completed dialog. Selecting 3-Legged makes Redirect URI required.

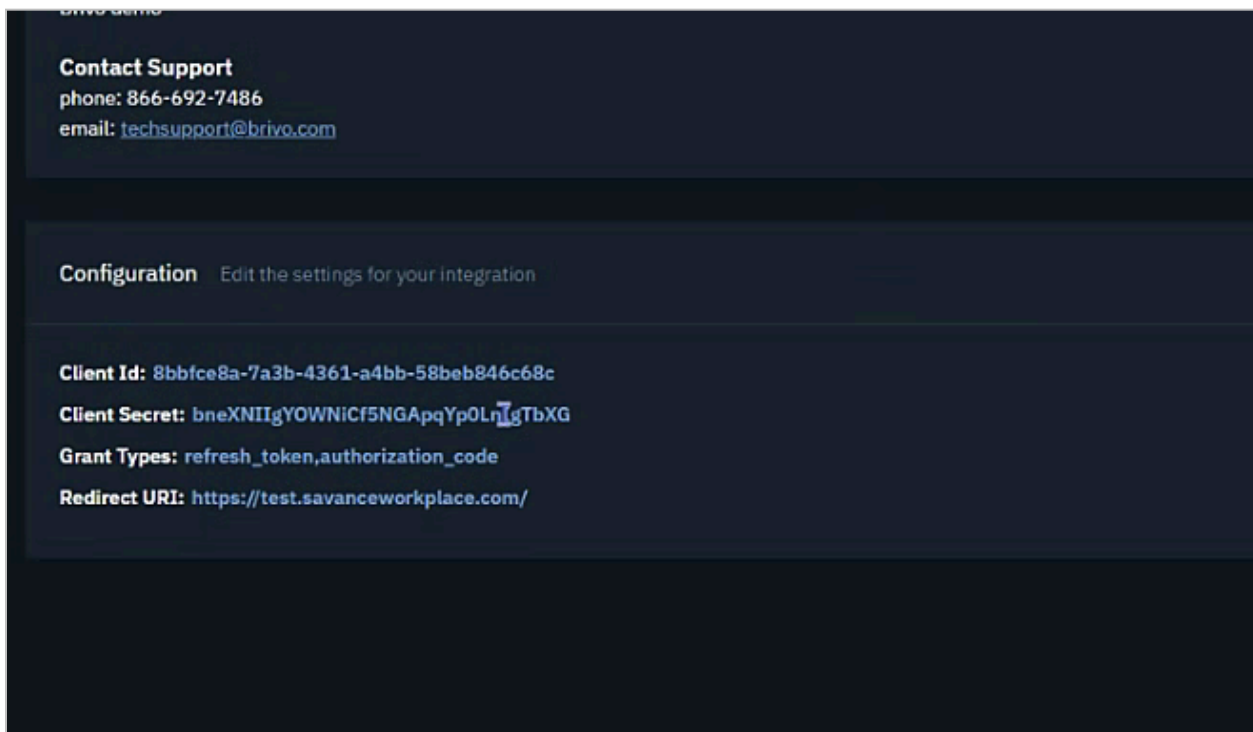
Note

The Redirect URI is used only while generating the Original Authorization Code from the Workplace integration page (Step Six). It is **not** the Event Subscription URI.

It must match the site you are actually working in. If the Redirect URI and the site you configure the integration from do not match, the authorization round-trip will fail.

After saving, retrieve the credentials Workplace needs:

1. In **Marketplace**, open the **Enabled** tab and click your new application.
2. Review the **Configuration** section. Copy the **Client Id** and **Client Secret**. Both are needed in Step Four. **Grant Types** should read `refresh_token, authorization_code`, and the **Redirect URI** should match what you entered.



The application's Details and Configuration panels, reached from the Enabled tab.

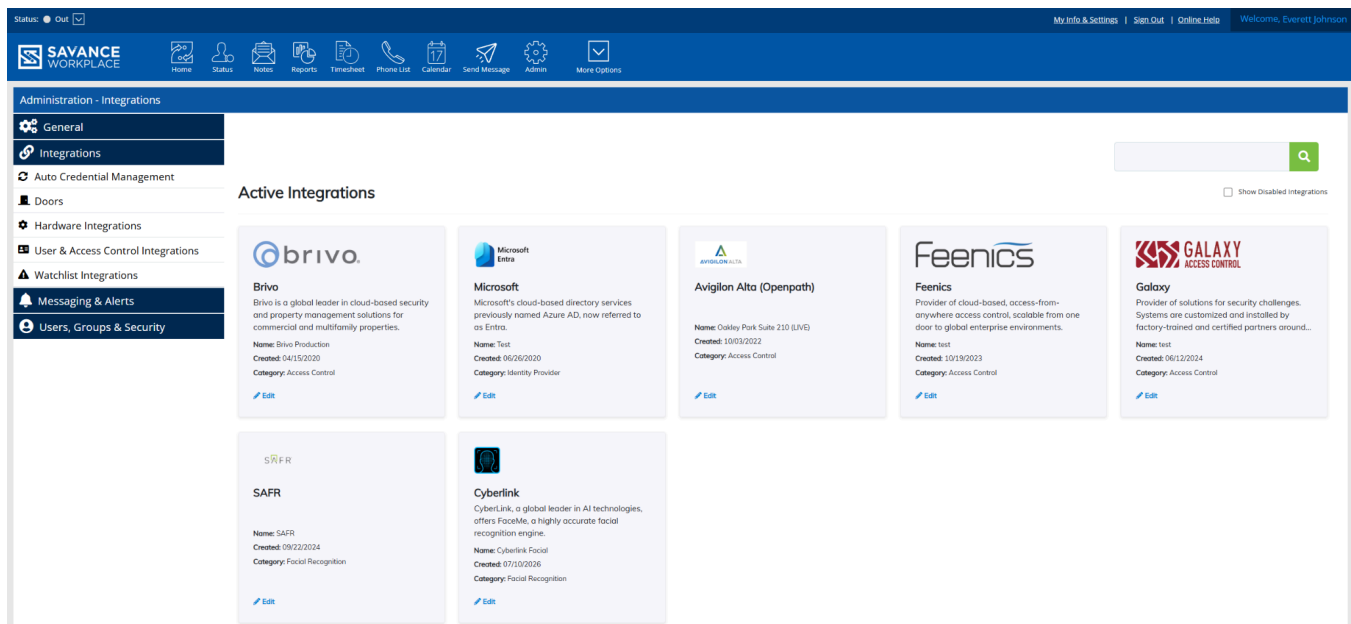
Changed

Earlier versions of this guide instructed you to click a blue “i” icon under “Application Detail.” That interface no longer exists. Use the **Enabled** tab and the **Configuration** section as described above.

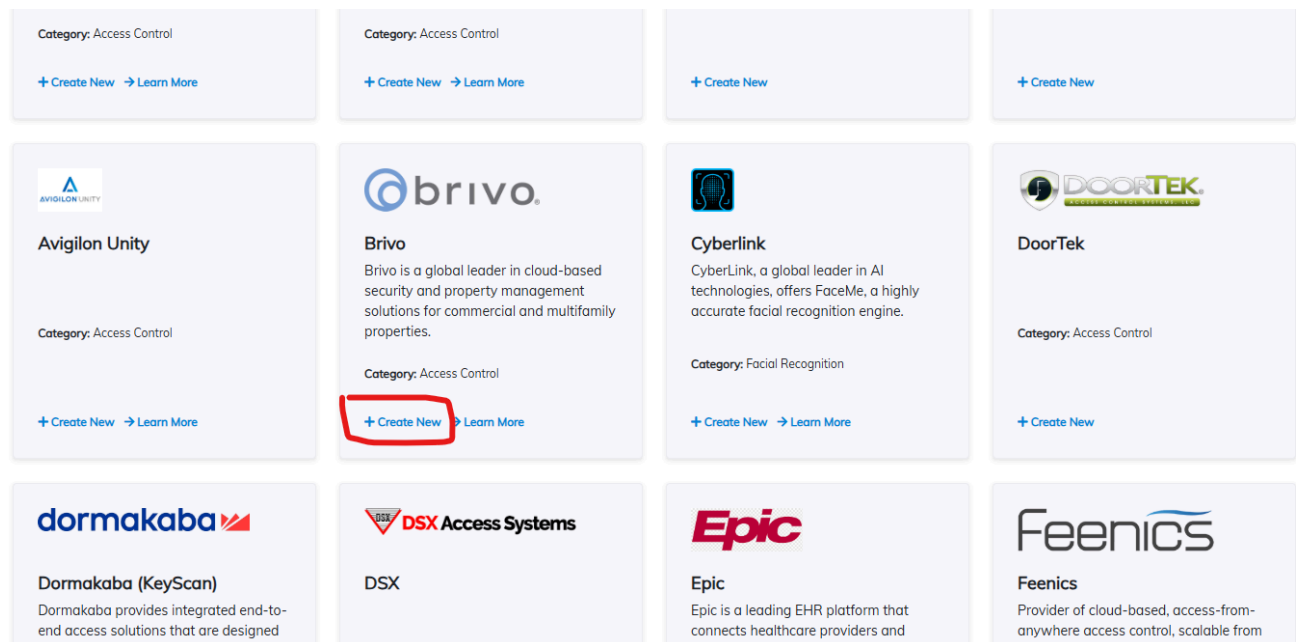
The application page also offers **Disable Integration** and a **Details** tab with Brivo support contact information.

Step Three: Create the Integration in Savance Workplace

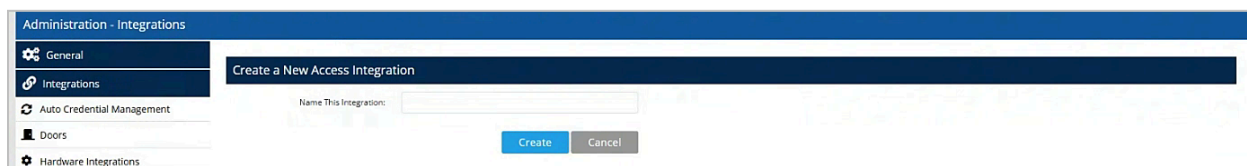
1. Log in to the Workplace website as an administrator.
2. Go to **Admin** → **Administration** → **User & Access Control Integrations**.
3. The top of the page lists **Active Integrations** as cards, each showing the integration name, created date and category, with an **Edit** link. A **Show Disabled Integrations** checkbox and a search box are available.
4. Below that is the provider catalog, filtered by the tabs **ALL / ACCESS CONTROL / IDENTITY PROVIDER / HARDWARE / FACIAL RECOGNITION / OTHER**.
5. Find the **Brivo** card and click + **Create New**.
6. On the **Create a New Access Integration** screen, type a name in **Name This Integration** and click **Create**.
7. You are taken to the integration page. Under **Integration Name**, note the **ID** (a GUID). It appears in the Event Subscription URI and in the Sync Users URL. **Edit Name** and **Delete this Integration** are also available here.



Administration → User & Access Control Integrations. Existing integrations appear as cards under Active Integrations.



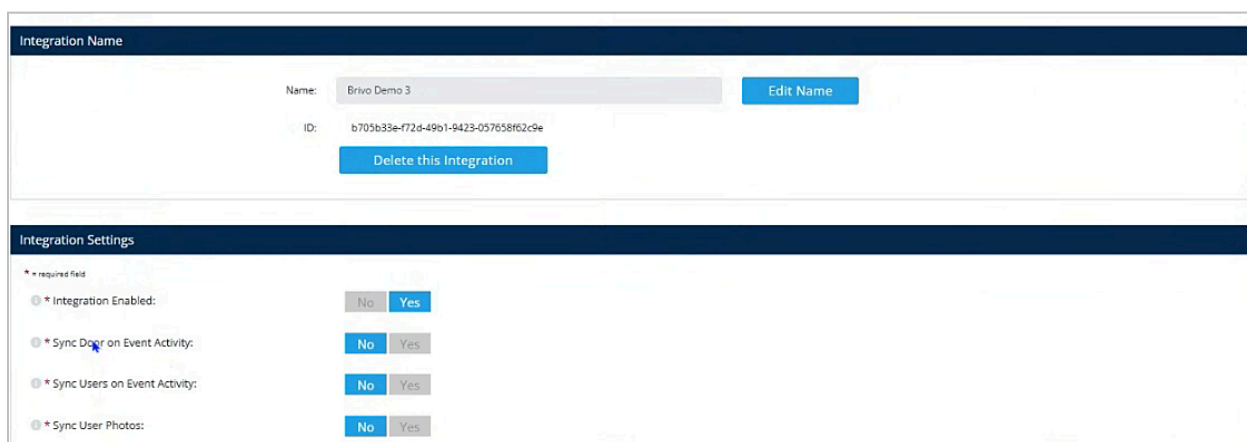
The provider catalog further down the same page. Click Create New on the Brivo card.



Name the integration and click Create.

Step Four: Complete the Integration Settings

Scroll to **Integration Settings**. Hover the “i” icon to the left of any setting for inline help. An asterisk (*) marks a field that is **required** in order to save. The settings appear in the order below.

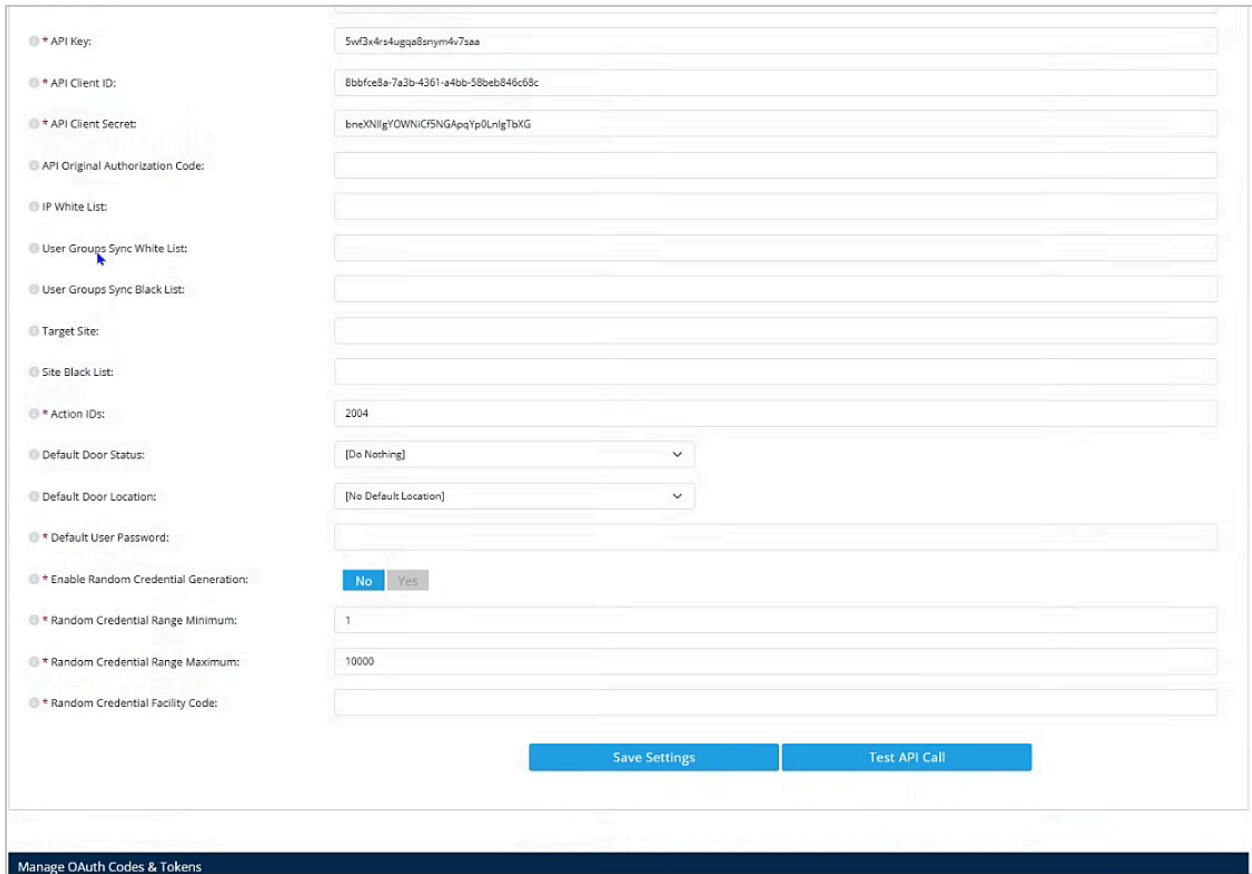


Integration Settings, upper half.

Setting	What it does / what to enter
* Integration Enabled	Set to Yes when all setup is complete. This turns the integration on.
* Sync Door on Event Activity	Yes , let Workplace create doors that do not yet exist as events for them arrive.
* Sync Users on Event Activity	Yes , let Workplace create users that do not yet exist as they scan their card. Users created this way are still subject to the user group whitelist and blacklist below.

Setting	What it does / what to enter
* Sync User Photos	Yes , makes Workplace also attempt to pull each user's photo from Brivo when users are synced.
* Event Subscription URI	<p>The URI Brivo will post events too. Auto-populated as <code>https://cloud.savanceworkplace.com/InboundEventListenerAsync.aspx?IntegrationId=[ID]</code>, where [ID] is the integration ID shown above the settings.</p> <p>If you are self-hosted, change the domain to your own. Workplace uses this value when it creates the webhook subscription in Brivo.</p>
* Error Email	The address Brivo error notifications are sent to.
* API Key	The Brivo-provided API key for this organization (Step One).
* API Client ID	The Client Id from the Brivo application (Step Two).
* API Client Secret	The Client Secret from the Brivo application (Step Two).
API Original Authorization Code	Leave blank for now. It is filled in automatically in Step Six. The integration will not sync until it is populated.
IP White List	Comma-separated list of IP addresses from which event submissions are allowed (xxx.xxx.xxx.xxx).
User Groups Sync White List	Comma-separated list of Brivo user groups. If a user is not in one of these groups, they are not synced.
User Groups Sync Black List	Comma-separated list of Brivo user groups. If a user is in one of these groups, they are not synced.
Target Site	Restricts the sync to a specific Brivo site. Leave blank to include all sites. Note: A Target Site cannot also be used with a site Black List.
Site Black List	Brivo sites to exclude from the sync. Due to the nature of the Brivo API, the site Black List cannot be used for manual event sync.
* Action IDs	Comma-separated list of Brivo action IDs Workplace should act on. Brivo assigns a different action ID to each kind of access event.

Setting	What it does / what to enter
	Defaults to 2004 ("Access Granted"), which is normally the only one needed, but the list can be customized.
Default Door Status	Dropdown of the organization's statuses; defaults to [Do Nothing] . Whatever you pick becomes the default status applied to doors newly synced from Brivo. Individual doors can be changed afterwards in Manage Doors .
Default Door Location	Dropdown of the organization's locations; defaults to [No Default Location] . Same behavior as Default Door Status.
* Default User Password	The password assigned to users created in Workplace by the Brivo sync. These users typically never log in, so the value mainly needs to satisfy the password requirement.
* Enable Random Credential Generation	Yes , lets Workplace generate and assign a random card number when a credential is activated, instead of requiring one to be typed in. Workplace avoids issuing the same number twice.
* Random Credential Range Minimum	Lowest number a generated credential may use. Default 1. We recommend setting this to 10,000 or 100,000 for 5 or 6 digit card numbers.
* Random Credential Range Maximum	Highest number a generated credential may use. Default 10000.
* Random Credential Facility Code	The facility code assigned to every randomly generated credential. This code comes from Brivo.



* API Key: 5wf3x4rs4ugqa8srym4v7saa
 * API Client ID: 8bbfce8a-7a3b-4361-a4bb-58beb846c68c
 * API Client Secret: bneXNllgYOWNiCF5NGAppqYp0LnlgtbXG
 API Original Authorization Code:
 IP White List:
 User Groups Sync White List:
 User Groups Sync Black List:
 Target Site:
 Site Black List:
 * Action IDs: 2004
 Default Door Status: [Do Nothing] v
 Default Door Location: [No Default Location] v
 * Default User Password:
 * Enable Random Credential Generation: No Yes
 * Random Credential Range Minimum: 1
 * Random Credential Range Maximum: 10000
 * Random Credential Facility Code:
 Save Settings Test API Call
 Manage OAuth Codes & Tokens

Integration Settings, lower half, ending with Save Settings and Test API Call.

Changed

The setting **Email Custom Field Name** described in earlier versions of this guide is no longer present on the integration settings page.

Workplace now reads the email address from the Brivo user record directly and uses it to match people; the sync notes will say “There is no email for this user in Brivo” when the record has none. See **How users and doors are matched** below.

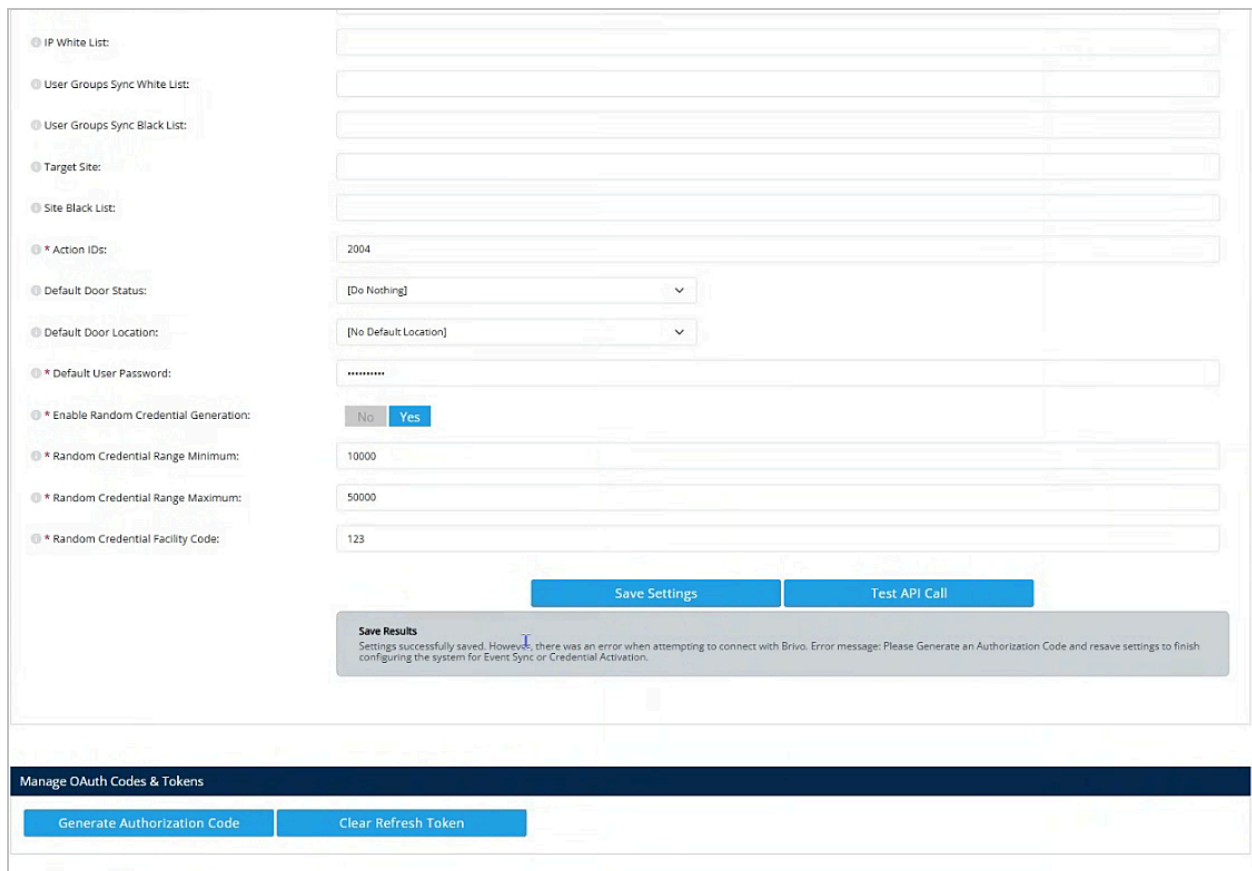
Step Five: Save the Settings (First Save)

Click **Save Settings**. Because the authorization code has not been generated yet, expect this message under the buttons:

Save Results

Settings successfully saved. However, there was an error when attempting to connect with Brivo. Error message: Please Generate an Authorization Code and resave settings to finish configuring the system for Event Sync or Credential Activation.

This is expected at this point. Continue to Step Six.

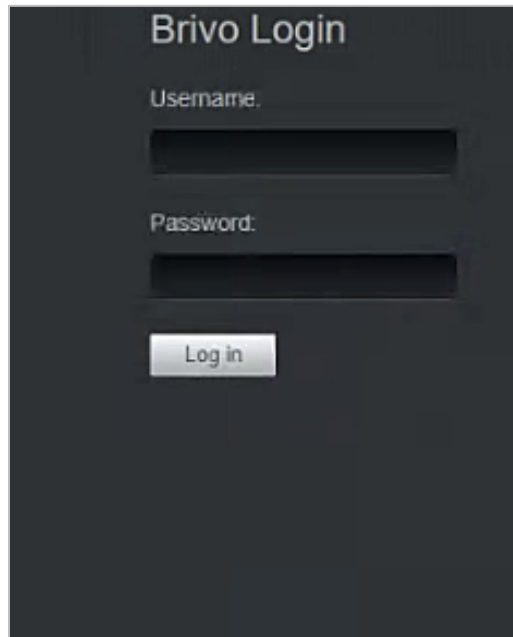


The screenshot displays the 'Save Settings' interface. On the left, a list of settings is shown with corresponding input fields on the right. The settings include IP White List, User Groups Sync White List, User Groups Sync Black List, Target Site, Site Black List, Action IDs (set to 2004), Default Door Status (set to [Do Nothing]), Default Door Location (set to [No Default Location]), Default User Password (masked with asterisks), Enable Random Credential Generation (set to Yes), Random Credential Range Minimum (set to 10000), Random Credential Range Maximum (set to 50000), and Random Credential Facility Code (set to 123). Below the settings list are two buttons: 'Save Settings' and 'Test API Call'. A 'Save Results' message box is visible below the buttons, stating: 'Settings successfully saved. However, there was an error when attempting to connect with Brivo. Error message: Please Generate an Authorization Code and resave settings to finish configuring the system for Event Sync or Credential Activation.' At the bottom of the interface, there is a section titled 'Manage OAuth Codes & Tokens' with two buttons: 'Generate Authorization Code' and 'Clear Refresh Token'.

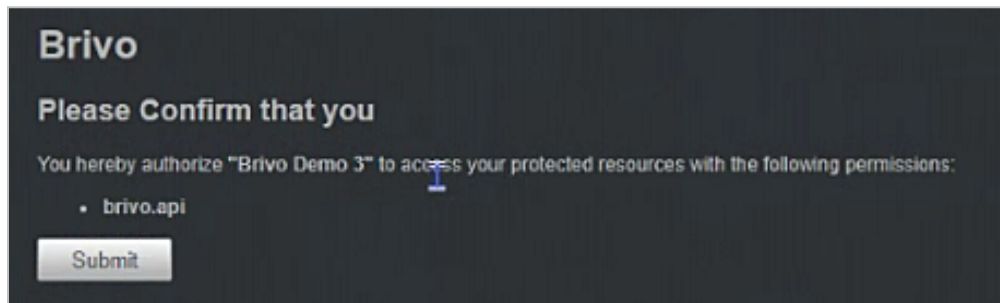
The expected result of the first save.

Step Six: Generate the API Authorization Code

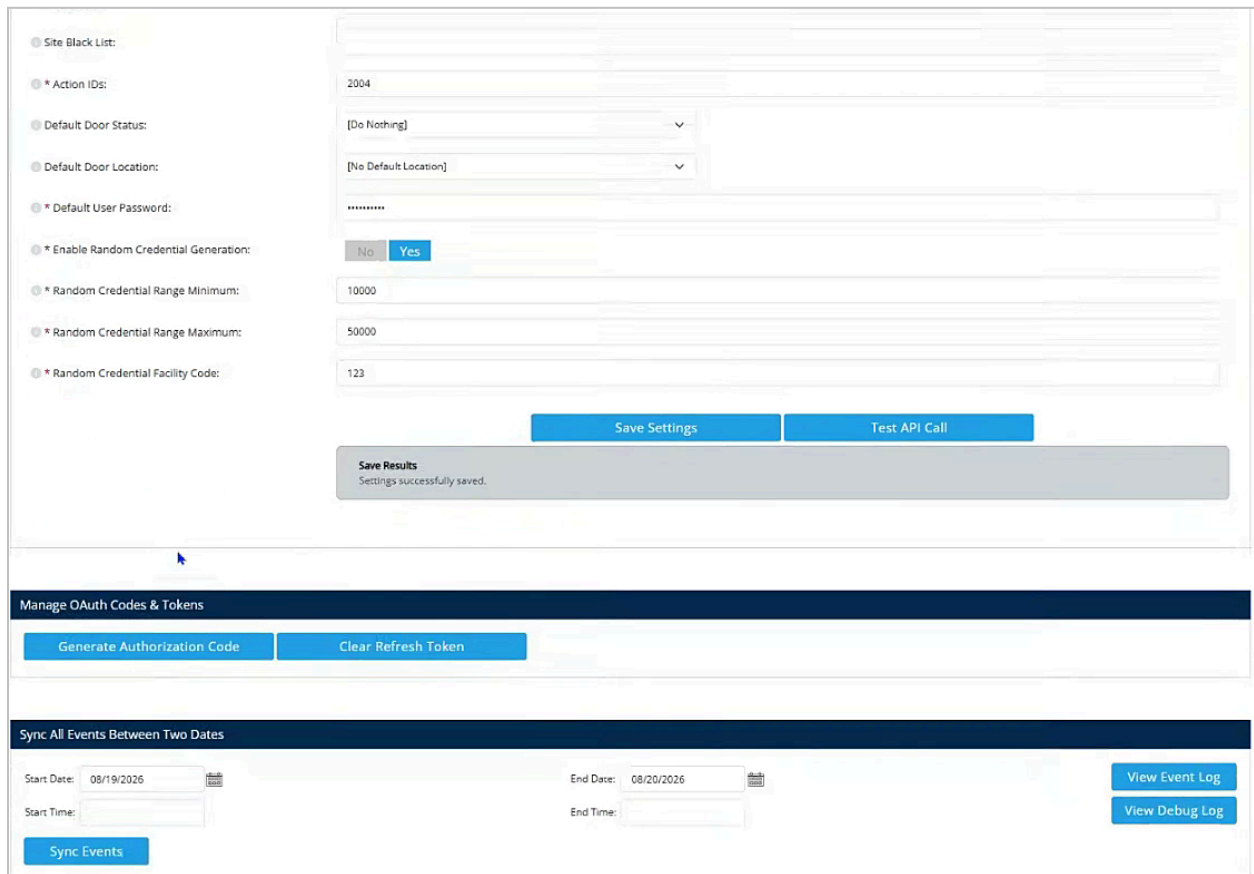
1. Below the settings, find the **Manage OAuth Codes & Tokens** section and click **Generate Authorization Code**.
2. A Brivo login page opens (<https://auth.brivo.com/login.jsp>). Enter your Brivo credentials and click **Log in**. You may need to use the **Admin ID** rather than the administrator email address as the Username.
3. Brivo then shows a grant-access screen headed "Please Confirm that you," followed by "You hereby authorize <your application name> to access your protected resources with the following permissions: brivo.api." Click **Submit**.
4. You are redirected back to the integration page, with the authorization code appended to the URL ([.../AccessIntegration.aspx?code=...](#)) and the **API Original Authorization Code** field filled in automatically.
5. Click **Save Settings** again. This second save is what actually creates the webhook subscription in Brivo. The message should now read simply "Settings successfully saved."

The image shows a dark-themed login interface for Brivo. At the top, the text "Brivo Login" is displayed. Below it, there are two input fields: "Username:" and "Password:". Each field has a dark rectangular input area. At the bottom of the form is a "Log in" button with a light-colored background and dark text.

The Brivo login page. Try the Admin ID if the email address is rejected.

The image shows a dark-themed grant-access screen for Brivo. At the top, the word "Brivo" is displayed. Below it, the text "Please Confirm that you" is shown. The main text reads: "You hereby authorize 'Brivo Demo 3' to access your protected resources with the following permissions:". Below this text is a bulleted list containing the item "• brivo.api". At the bottom left is a "Submit" button with a light-colored background and dark text.

The grant-access screen. The requested permission is *brivo.api*.



The screenshot shows the Brivo Integration Setup page. On the left, there is a sidebar with the following options: Site Black List, * Action IDs, Default Door Status, Default Door Location, * Default User Password, * Enable Random Credential Generation, * Random Credential Range Minimum, * Random Credential Range Maximum, and * Random Credential Facility Code. The main area contains input fields for these settings. For example, Action IDs is set to 2004, Default Door Status is [Do Nothing], Default Door Location is [No Default Location], Default User Password is masked with asterisks, and the random credential range is set from 10000 to 50000 with a facility code of 123. There are 'No' and 'Yes' buttons for 'Enable Random Credential Generation'. At the bottom of the main area are 'Save Settings' and 'Test API Call' buttons. Below these is a 'Save Results' box with the message 'Settings successfully saved.' Below the main area is a 'Manage OAuth Codes & Tokens' section with 'Generate Authorization Code' and 'Clear Refresh Token' buttons. At the bottom is a 'Sync All Events Between Two Dates' section with 'Start Date' (08/19/2026), 'End Date' (08/20/2026), 'Start Time', 'End Time', and 'Sync Events' buttons. There are also 'View Event Log' and 'View Debug Log' buttons.

After authorizing and saving again: "Settings successfully saved."

Clear Refresh Token, next to Generate Authorization Code, discards the stored refresh token. Use it when you need to re-authorize the integration from scratch, for example after the Brivo application or its credentials change.

Troubleshooting

During this process you may land on the Workplace home page instead of back on the Access Integration page. This usually means IIS is configured to redirect the browser to a default page (for example /default.aspx). See **Troubleshooting** for how to recover the code by hand.

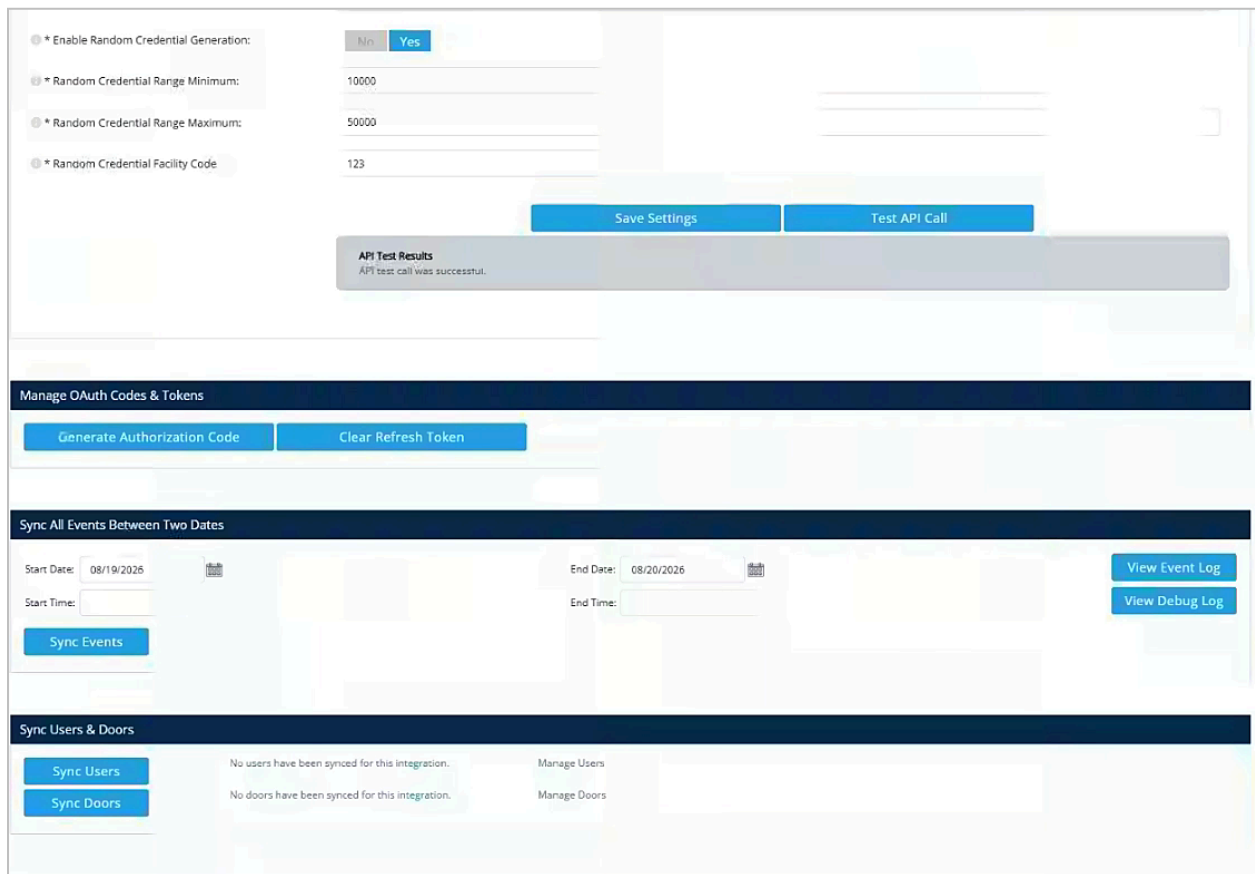
Step Seven: Test the API

Click **Test API Call**. You should see:

API Test Results

API test call was successful.

This confirms the API integration with Brivo is properly configured and working.



The screenshot displays the Brivo integration setup interface. At the top, there are settings for random credential generation:

- * Enable Random Credential Generation: ☒ Yes
- * Random Credential Range Minimum: 10000
- * Random Credential Range Maximum: 50000
- * Random Credential Facility Code: 123

 Below these settings are two buttons: "Save Settings" and "Test API Call". A grey notification box below the buttons displays "API Test Results" and "API test call was successful."

Below the notification box are three main sections:

- Manage OAuth Codes & Tokens:** Contains two buttons: "Generate Authorization Code" and "Clear Refresh Token".
- Sync All Events Between Two Dates:** Contains date and time pickers for "Start Date" (08/19/2026) and "End Date" (08/20/2026), along with "Start Time" and "End Time" fields. It includes a "Sync Events" button and two links: "View Event Log" and "View Debug Log".
- Sync Users & Doors:** Contains "Sync Users" and "Sync Doors" buttons. It also displays status messages: "No users have been synced for this integration." and "No doors have been synced for this integration.", along with "Manage Users" and "Manage Doors" links.

A successful API test, with the Sync panels below it.

Step Eight: Sync Users and Doors

At the bottom of the integration page, the **Sync Users & Doors** section holds the **Sync Users** and **Sync Doors** buttons. Beside them, Workplace reports the last sync (“No users have been synced for this integration.” until the first run) along with **Manage Users** and **Manage Doors** links.

Syncing users

1. Click **Sync Users**. Workplace gathers user information from Brivo and opens the sync wizard (/Administration/UserSync.aspx?id=[ID]), confirming “Gather Users Info Success!”
2. **Step 3 of 4: Select Users to Sync** reports the totals (for example “Active Brivo users found: 169. New Brivo users not already in Workplace: 14.”) along with the running count of users selected to be synced.
3. Use **Show New**, **Show Existing** or **Show Both** to filter the list, **Select All / Deselect All** and the A–Z index to narrow it, and the **Sync to EIOBoard** checkbox in each row to choose individuals. The **Existing EIOBoard User** column marks people Workplace already knows about.
4. Click **Sync Selected Users**. **Step 4 of 4** shows the results (for example “1 new users were added. 0 existing users were modified. 0 users were unchanged. 0 errors occurred”), with a row per user (Name, User Name, Email, Created, Changed, Notes, Edit). Hover **notes** to see exactly what the sync did: whether an email was found in Brivo, which card number was matched, and whether credentials were changed.
5. Click **Return to Integration Settings** when finished.

Users that are **suspended** in Brivo are not synced, and neither are users excluded by the group whitelist or blacklist.

Sync Users for Brivo Demo 3

✓ Gather Users Info Success!

Step 3 of 4: Select Users to Sync to EIOBoard

Active Brivo users found: 169. New Brivo users not already in Workplace: 14.

Sync Selected Users

Number of users selected to be synced: 155

Show New

Show Existing

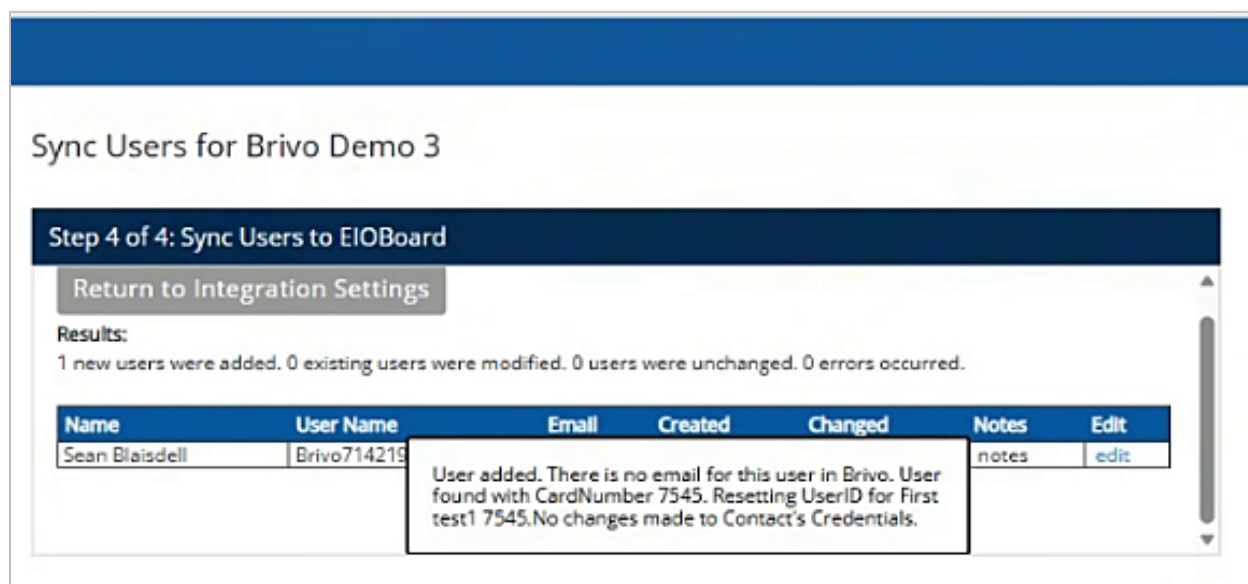
Show Both

Select All

Deselect All

All	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	123
Name	Existing EIOBoard User																		Sync to EIOBoard								
a, a																											
Akerley, Brian																											
arun4, test																											
Badgetest, Brivo																											
Bane, Cad																											
Banton, Boujou																											
Bardocz, Steve																											
Bates, Norman																											
Belushi, John																											
Berkson, Test																											
Berkson, Dan																											
Best, Alan																											
Bobob, Timmy																											
Boob, Preregisterd																											
Bourne, Jason																											
BrivoUser, EnosisTest																											
Brosef, Robert																											
Cage, Johnny																											
Caldwell, Andy																											
Calrissian, Lando																											
Carter, Derrick																											
Chapman, Joe																											
Chappelle, Dave																											
Choi, Andy																											
Collins, Tom																											
Curley, Jason																											

Step 3 of 4: selecting which Brivo users to bring into Workplace.



Step 4 of 4: sync results, with a Notes column explaining each decision.

UI note

Some labels in the sync wizard still read “EIOBoard” (the former product name) rather than “Workplace.” They refer to the same thing.

Syncing doors

Click **Sync Doors** to import the Brivo devices as doors. Synced doors then appear under **Administration** → **Doors** → **Manage Doors** (/Administration/ManageDoors.aspx), which lists **Door ID**, **Door Name**, **Status**, **Toggle**, **Alt Status**, **Status Location**, **Source**, **Integration**, plus Edit and Delete actions, an **Add New Door** button, and a search by door name or ID.

Edit a door to control what happens when someone badges at it: the **Status** applied on a scan, an **Alt Status** with the **Toggle** option for in/out style readers, and a **Status Location**. For example, a “Driver Entry” door can sign a person in while a “Driver Exit” door signs them out, so the status board reflects who is on site. Doors left at **[Do Nothing]** record the

event without changing anyone's status, which is useful for sites with a large number of doors where only a few should drive status.

Manage Doors

[Add New Door](#)

Search by Door Name or ID

Door ID	Door Name	Status	Toggle	Alt Status	Status Location	Source	Integration	Edit	Delete
☒ 8ba5f977-9e49-460b-8a1a-6d2775f29689	AC12 - NEXP-KYAP-9TQ7 Door	In	☐		USA				
☒ 1	BlankDoor	In	☒	Out	India				
☒ 161	QA Door 01-D	Testing Task	☐	Testing	Bangladesh				
☒ 856	Testcase Door	Testing Task	☐	In					
☒ 2	870-Keypad		☐			AMAG	basdfire		
☒ 1	ProxPointPlus1		☐			AMAG	basdfire		
☒ 2	870-Keypad	Sales Call	☐			AMAG	Maggie_10-3-43		
☒ 1	ProxPointPlus1	Meeting	☐	Business Trip		AMAG	Maggie_10-3-43		
☒ 51597	Kiosk Entry (Demo)	In	☒	Out	Bangalore	Avigilon Alta (Openpath)	Openpath test		
☒ 5542	Main Office	In	☒	Out	Bangalore	Avigilon Alta (Openpath)	Openpath test		
☒ 10476	Test Entry (Dev)	In	☒	Out	Bangalore	Avigilon Alta (Openpath)	Openpath test		
☒ 283330	A1 Control East Door Inbound Entry	In	☐		Alderan	Avigilon Alta (Openpath)	openPathTestAminul		
☒ 283333	A1 Control East Door Outbound Entry	In	☐		Alderan	Avigilon Alta (Openpath)	openPathTestAminul		
☒ 283336	A1 Control South west Door Inbound Entry	In	☐		Alderan	Avigilon Alta	openPathTestAminul		

Manage Doors. The Source and Integration columns show where each door came from.

How users and doors are matched

- **Doors** are matched on the Brivo door ID, which corresponds to the primary key of the record in Brivo.
- **Users** are matched on email address. If Workplace already has a person with the same email, that person is treated as already synced rather than duplicated, which is what allows one person to be synced from more than one integration.
- A newly synced user gets a Workplace username, and their **User ID** is set from their card number. Email address and photo are imported when they exist in Brivo (photos require **Sync User Photos**).

- Workplace stores **all** of a person's credentials, not just one. If someone has a card and a key fob, an event from either at a Brivo panel identifies the person and updates their status.

Step Nine: Sync Historical Events (Optional)

The **Sync All Events Between Two Dates** section lets you pull events Workplace may have missed. Enter a **Start Date / Start Time** and **End Date / End Time** and click **Sync Events**. The **View Event Log** and **View Debug Log** buttons in this section open the logs described below.

Ready to Begin

With **Integration Enabled** set to Yes, Workplace is ready to receive access events from Brivo. Scan a few cards at various door readers and confirm the process works end to end. The event should appear in the Event Log and the person's status should change on the status board.

Logs

Open the logs from the **View Event Log** and **View Debug Log** buttons on the integration page.

Event Log

The Event Log catalogs all successful events that reach Workplace from Brivo. For each event it displays:

- Date and time of the event
- The user's full name
- The card number that was used

- The user's Workplace status before and after the scan
- The user's Workplace location before and after the scan
- The door where the card was scanned
- Whether the user was pre-existing or created in Workplace as a result of the scan
- Whether the door was pre-existing or created in Workplace as a result of the scan
- Hovering over "notes" shows the logic flow followed for the import, including how the status and location were determined

Debug Log

The Debug Log is a lower-level log capturing the underlying data and logic around each event. It is meant for tracking down problems with recent access events, not for long-term retention, so entries older than 60 days are deleted automatically. It displays:

- Date and time of the event
- A Log Id: a random number that ties together multiple log entries for the same access event
- Log Type (see below)
- Log Data: a JSON string, or notes pertaining to the event
- Source Query String: for Raw Data entries, all key-value pairs that were part of the incoming event call. Empty for other types.
- Source IP: for Raw Data entries, the external IP address the call came from. Empty for other types.

Debug Log event types:

- **Raw Data:** a JSON string of the raw data sent by the remote access provider.
- **Access Event:** a JSON string representing the object Workplace created after processing the raw data.
- **User Sync:** data explaining why a user was or was not synced.

- **Internal Stop:** processing stopped by internal Workplace logic. For example, the incoming event's IP address was not on the IP White List.
- **Api Call Fail:** a message from Brivo explaining why a call to their API failed.
- **Error:** an internal Workplace error.

Troubleshooting

“Please Generate an Authorization Code and resave settings”

Expected on the first save. Complete Step Six and save again. If it persists after generating a code, confirm the API Key, Client ID and Client Secret are correct and that the Redirect URI on the Brivo application matches the Workplace site you are working in.

Redirect URI problems

- The Redirect URI simply brings you back from Brivo so Workplace can capture the authorization code. It must be the same URI through which you are setting up the integration.
- If the redirect lands on the site's `default.aspx` instead of the integration page, try entering the full URI, for example `yourdomain.com/eioboard` rather than `yourdomain.com`.
- If the redirect does not error but lands on a page that throws an error, look at the browser's address bar and copy the value after `code=`. That value is your authorization code. Paste it into **API Original Authorization Code**, save the settings, and the API call should work.

Missed events

The externally available Workplace server is the primary source of missed Brivo events. Confirm the Workplace website is browsable from outside and is receiving Brivo events

before hardening security. If an **IP White List** is in use, verify Brivo's source addresses are included. Blocked events appear in the Debug Log as **Internal Stop**.

Events arrive but nobody's status changes

Check that the door's **Status** is not left at **[Do Nothing]** in Manage Doors, and that the event's action ID is included in the **Action IDs** setting (2004 = Access Granted).

Appendix: What Changed in This Revision

Recorded here so reviewers can spot-check the corrections. Sourced from the Brivo Demo 3 walkthrough of August 20, 2026.

- **Brivo application fields renamed.** The dialog is *Generate an API Token* with **Application Name**, **Application Description**, **Application Type** (not “Authentication Type”) and **Redirect URI**.
- **Retrieving Client ID / Secret rewritten.** The “blue icon under Application Detail” no longer exists; use Marketplace → Enabled → the application → Configuration.
- **Workplace navigation rewritten.** Brivo is created from the provider catalog on Administration → Integrations via the Brivo card’s **Create New** link, not from “User & Access Control Integrations → Access Control → a provider dropdown.”
- **Settings table rebuilt in UI order** and corrected: *Sync Door on Event Activity* (singular), plus three settings that were missing: **Sync User Photos**, **Target Site** and **Site Black List**.
- **Email Custom Field Name removed.** The setting is not present in the current UI, and the old “User Emails from Brivo” section has been replaced by “How users and doors are matched.”
- **Event Subscription URI warning added.** It defaults to the cloud domain and must be edited for self-hosted sites.
- **Two-save sequence documented** with the exact first-save message, since the webhook subscription is only created on the save that follows authorization.
- **Authorization flow updated** with the actual Brivo login and grant-access screens, the `brivo.api` permission, and the `?code=` redirect.
- **New sections for Manage OAuth Codes & Tokens** (including *Clear Refresh Token*) and **Sync All Events Between Two Dates**.
- **Sync Users wizard documented** as it now appears (Step 3 of 4 / Step 4 of 4, counts, filters, results and notes), and door/user matching behavior described.

- **Manage Doors** columns and the Status / Alt Status / Toggle behavior documented.
- **Log access corrected.** The logs open from *View Event Log* and *View Debug Log*, not from a “Last sync performed” link.
- **Screenshots replaced** throughout with captures from the current interface.

Still open: the API key request procedure in Step One, and confirmation that email no longer requires a Brivo custom field.