

Brivo Door Station Pro Installation Guide

I

Introduction

Legal Disclaimers.....	2
Introduction	4

II

Pre-Installation Procedures

Understand the function of the Brivo Door Station Pro (B-DS-PRO)	6
Understand B-DS-PRO product compatibility	6
Verify client site is ready for installation.....	6
Verify shipping contents.....	7
Verify tools needed for installation.....	7
Verify Brivo control panel setup to accept Brivo Door Station Pro.....	8
Confirm Brivo Door Station Pro powers up successfully.....	8
Follow safety precautions	9

III

General Assembly Procedures

Wiring the cable to the Brivo Door Station Pro.....	10
Prepare the location to mount the Brivo Door Station Pro.....	11
Mounting the Brivo Door Station Pro	13

IV

Brivo Door Station Pro Configuration

Configure and test your Brivo Door Station Pro in Access	14
Configure Intercom call receiver in Brivo Access	15
Configure notifications for your Brivo Door Station Pro	15
Test your intercom call receiver in Brivo Access	16
Test your intercom to call a mobile phone using BMP	16
Configure and test a user with physical credentials	17
Configure and test a user with Bluetooth credentials	17
Reader LED Operations for Brivo Door Station Pro	18

V

Troubleshooting

Verify OSDP connection.....	19
Verify communication with Brivo cloud server	20
Verify WebUI works and firmware is up to date.....	21
Verify functionality through Troubleshooting Tool.....	22
Troubleshooting Live Video.....	23
Video Services for Brivo Door Station Pro	25

VI

Maintenance Mode Operations

Brivo Door Station Pro Maintenance Mode Operations.....	26
---	----

VII

Appendices

Ports and IP Addresses for the Brivo Door Station Pro	27
---	----

Legal Disclaimers

FCC

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment complies with the FCC requirements for RF exposure. This device should be installed with a minimum distance of 20cm between the device and your body.

Note:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation or when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Canada

This device complies with ISSED Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'ISDE Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1. l'appareil ne doit pas produire de brouillage;
2. l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Énoncé d'exposition aux rayonnements: Cet équipement est conforme aux limites d'exposition aux rayonnements ioniques RSS-102 Pour un environnement incontrôlé. Cet équipement doit être installé et utilisé avec un Distance minimale de 20 cm entre le radiateur et votre corps.

Canada-MET Labs (MET-C) Compliance (CSA C22.2 No. 205)

For MET-C Listed applications, the unit shall be installed in accordance with Part 1 of the Canadian Electrical Code.

UL294/ULC Listing Compliance

UL294 Performance Levels					
Model Number	Access Control Line Security Level	Destructive Attack Level	Endurance Level (13.56MHz)	Endurance Level (BLE)	Stand-by Power Level
Brivo Door Station Pro (B-DS-PRO)	Level 1	Level 1	Level 4	Level 1	Level 1

Parts and Service

The B-DS-PRO contains no user serviceable parts.

Documentation Disclaimer and Restrictions

Information in this document is subject to change without notice and does not represent a commitment on the part of Brivo Systems LLC. For the most up-to-date information, visit www.brivo.com.

This document and the data herein shall not be duplicated, used or disclosed to others for procurement or manufacturing, except as authorized with the written permission of Brivo Systems LLC. The information contained within this document or within the product itself is considered the exclusive property of Brivo Systems LLC. All information in this document or within the hardware and software product themselves is protected by the copyright and/or other intellectual property laws of the United States.

Product Support

All support for this product is provided by the third-party dealer. Please contact the dealer who installed the product with questions and support requests.

© 2025 Brivo Systems LLC. All rights reserved.

Brivo® is a trademark of Brivo Systems LLC. Brivo Systems LLC., 7700 Old Georgetown Road, Suite 300, Bethesda, MD 20814

Introduction

Document Objectives

This Installation Guide provides step-by-step instructions for installing the Brivo Door Station Pro (B-DS-PRO). Its primary audience is trained access control installation technicians (Installers) who are responsible for installing the Brivo Door Station Pros (B-DS-PRO) at client sites.

This version of the guide is also intended for IT personnel, who should use it in conjunction with the [Brivo Panel Networking Guide](#) and [Ports and IP Addresses by Product Category](#). It may be used by dealers and their sales professionals to help them conduct pre-sales, and to provide client support during the installation process. Finally, it may be used for in-house training purposes and ongoing support.

Document Layout

This guide is organized into a series of procedural checklists, detailing steps you must follow to ensure a safe, trouble free, and effective installation. The main sections of the guide are:

- Introduction
- Pre-Installation Procedures
- General Assembly Procedures
- Brivo Door Station Pro Configuration
- Maintenance Mode Operations

Terminology

The following is a list of terms that are used throughout this document. While some of these terms may have other meanings, the definitions provided below are the ones intended in this [Installation Guide](#).

- **Door Station.** The all-in-one intercom video reader that unlocks doors using facial authentication, captures video of every access event and connects to visitors.
- **Access control system (ACS).** The complete interaction between a door station, a control panel, Brivo Access, and the Brivo Cloud Server.
- **Brivo Access.** Brivo's cloud based software application which enables the end user to manage their Brivo account.
- **Brivo Cloud Server.** The off-site servers, hosted by Brivo, that are used to store an account's database. Configuration and maintenance of the control panel is managed through Brivo Access.
- **Brivo Security Suite.** Our unified, cloud-based security platform designed to provide comprehensive protection and operational efficiency for modern enterprises, multifamily properties, and commercial facilities. It brings together access control, video intelligence, visitor management, and intrusion detection into a single, centralized view—making it easier to manage security across one or thousands of locations.

Wire Recommendations

Signal	Belden # or Equivalent	AWG / mm	Twisted Pair	Shielded	Conductor	Max Length (ft / m)
RS-485 Comm (two wire)	9841	24 / .511	Yes	Yes	2	4000 ft / 1220 m
Power (18 gauge)	6300UE	18 / 1.024	No	No	2	500 ft / 150 m
RJ45-Ethernet	N/A	Cat5e or greater	Yes	No	8	328 ft / 100 m
CAN Bus	N/A	Cat5e or greater	Yes	No	5	1500 ft / 450 m
Fire Alarm Relay	6300FK	18 / 1.024	No	No	2	1500 ft / 450 m
Request-to-Exit	6502UE	22 / .644	No	No	4	500 ft / 150 m
	6300UE	18 / 1.024	No	No	2	500 ft / 150 m
Door Contact	6500UE	22 / .644	No	No	2	500 ft / 150 m
Transformer Block	6300UE	18 / 1.024	No	No	2	100 ft / 32 m
Power Connector	N/A	18 / 1.024	No	No	4	1 ft / .32 m
Earth Ground	N/A	12 / 2.058	No	No	1	40 ft / 12 m
Reader Option 1 (22 AWG)	6504FE	22 / .644	No	Yes	6	250 ft / 75 m
Reader Option 2 (18 AWG)	6304FE	18 / 1.024	No	Yes	6	500 ft / 150 m
Reader OSDP	6381MD	24 / .511 (Data)	Yes	Yes	2	500 ft / 150 m
		18 / .644 (Power)			2	500 ft / 150 m

Additional Resources

The following additional resources are available for the installer as well as the client.

- [Panel Networking Guide](#)
- Technical Support: 1-866-BRIVO-4-U
- www.brivo.com
- [Ports and IP Addresses by Product Category](#)
- Brivo Door Station Pro Quickstart Guide
- Additional Brivo Help Center articles at <https://support.brivo.com>

Pre-Installation Procedures

Before you begin installing the Brivo Door Station Pro, perform the following tasks to ensure a safe, speedy, and successful installation.

Understanding the function of the Brivo Door Station Pro (B-DS-PRO)

The Brivo Door Station Pro is an all-in-one intercom video reader that unlocks doors using facial authentication, captures video of every access event and connects to visitors. The Brivo Door Station Pro needs to be connected to a Brivo control panel in order to function. The Brivo Door Station Pro communicates with the Brivo control panel via OSDP using RS-485 wiring as detailed later in this guide.

Understanding Brivo Door Station Pro product compatibility

The Brivo Door Station Pro is supported on the following Brivo hardware: ACS100, ACS300, ACS6000-MBE, ACS6100-DB and ACS-SDC. For the Brivo Door Station Pro to function properly, ensure the Brivo control panel is running the latest version of firmware and that the Brivo Door Station Pro is running the latest version of firmware. If needed, please contact Brivo Technical Support at 866-274-8648 or email customer@brivo.com for assistance.

IMPORTANT NOTE: The ACS100 supports Brivo Door Station Pro faceprint credentials, but does not support Intercom functionality.

IMPORTANT NOTE: The Brivo Door Station Pro does not work with Mercury control panels.

Verify that the client site is ready to support the installation

1. Review the installation and note any needed LAN/Firewall settings with the Customer IT administrator before installation.
 - a. Make sure Customer site IT personnel are available during the installation.
 - b. Resellers and installers should review the IT requirements for installation of the Brivo Door Station Pro before site installation.
 - c. IT guidance and recommended settings can be found in Appendix 1 or in this Brivo Help Center article:
 - i. [Ports and IP Addresses by Product Category](#)
 - d. Additional installation documentation:
 - i. Brivo Door Station Pro Quick Reference Sheet
 - ii. [Panel Networking Guide](#)
 - iii. [Brivo Door Station Pro Quick Start Guide](#)
 - e. If needed, additional Help Center articles:
 - i. [Configuring a Brivo Door Station Pro](#)
 - ii. [How to setup Intercom for Brivo Door Station Pro](#)
 - iii. [How to use Intercom on a Brivo Door Station Pro](#)
 - iv. [How to setup notifications for Brivo Door Station Pro](#)
 - v. [How to view Live Video with the Brivo Door Station Pro](#)
 - vi. [How to use Talkdown with the Brivo Door Station Pro](#)
 - f. Verify that a Brivo Access account has been created and that a control panel is registered through Brivo Access to which the Brivo Door Station Pro can be assigned. If the control panel has not been registered by the reseller, the installer may either contact Brivo Technical Support for assistance or simply register the panel directly.

- g. Verify that the Primary Administrator and any other employee who will be accessing the system have Internet access on a computer equipped with a supported Web browser.

Verify shipping contents

1. Locate and check the contents of the Brivo Door Station Pro kit.
The B-DS-PRO kit should contain the following parts:
 - a) Brivo Door Station Pro
 - 1 Brivo Door Station Pro Unit
 - 1 Mounting Plate for the Brivo Door Station Pro
 - 1 Pan Wedge for the Brivo Door Station Pro
 - 1 Single Gang Cover Plate for the Brivo Door Station Pro
 - 3 drywall anchors
 - 3 mounting screws 25mm
 - 3 mounting screws 10mm
 - 3 pan wedge mounting screws
 - 1 mounting screw, Torx security drive type
 - 1 Torx T10 security drive bit
 - b) 1 documentation set, including:
 - Quick Start Guide

Verify tools needed for installation

1. The following tools will be needed to install the Brivo Door Station Pro.
 - a) 1 Phillips screwdriver
 - c) 1 set of 1" (25mm) , 1/8" drill bits
 - d) 1 Screw driver or motorized driver accepting T10 security drive bit

Verify that the Brivo control panel is setup to accept the Brivo Door Station Pro

1. Verify that the control panel is talking to the Brivo cloud server.
 - a) Ensure the proper region (US or EU) has been set for the Brivo Door Station Pro. You do this by following the instructions in the Brivo Panel Networking Guide (refer to Region Selection).
 - b) Next, log into Brivo Access and verify that the control panel you're going to attach the Brivo Door Station Pro to shows that it is connected and online.
 - c) If not connected, follow normal installation steps to connect the Brivo control panel to the Brivo Cloud Service.
 - d) If still not working, contact Brivo Support at 866-BRIVO-4U or customercare@brivo.com.

NOTE: If using an ACS6000 series control panel, ensure the following dip switches are set properly:

- a) Set the RS485 switch to RS485 (SW3 or SW11)
 - b) Set the Duplex switch to Half-Duplex (SW4 and SW12)
 - c) Set Termination Switch (blue) to Disabled (SW5 and SW13)
2. Verify the control panel firmware is up to date.
 - a) The firmware for the Brivo control panel must be version 6.2.5.10 or later.
 - b) The control panel firmware can be viewed when logging into the WebCLI or via Brivo Access under the Access Devices page.
 - c) If the control panel doesn't have the correct firmware, use Partner Portal to update it or contact Brivo Support at 866-BRIVO-4U or customercare@brivo.com.

IMPORTANT NOTE: If the Brivo Door Station Pro is connected to the control panel via an ACS6100-DB door board node, verify door board MCU firmware on the ACS6100-DB is up to date.

- d) Use the WebCLI Hardware > Status or review the log from System > Diagnostic Dump to gather connected ACS6100 boards and MCU firmware versions.
 - e) If the first digit of door board firmware is 2, then it needs to be at 2.1.19 (or greater).
 - f) If the first digit of door boards firmware is 3, then it needs to be at 3.0.13 (or greater).
 - g) If the Door Board is not at the correct firmware level, contact Brivo Support at 866-BRIVO-4U or customercare@brivo.com.

Prior to installing the Brivo Door Station Pro, apply power to the unit to ensure it boots properly

1. Power the Brivo Door Station Pro unit via Power over Ethernet (PoE). The Brivo Door Station Pro is powered by PoE (802.3at Type 2) and uses up to 20W.
2. Once booted, the Brivo Door Station Pro will flash white and beep. If it does not, check that the Ethernet connection is PoE and is supplying power.
3. If the unit does not power up properly, check that your switch is providing PoE power. If the switch is providing power and the Brivo Door Station Pro is still not powering up, contact Brivo Support at 866-BRIVO-4U or customercare@brivo.com.

Follow safety precautions

WARNING: Fire Code

Never connect a keypad/reader or lock to doors without first consulting the applicable fire code. You must consult with, and get approval from, local fire officials before installing locks or devices on any doors that may be fire exits. Use of egress push buttons may not be legal. Single action exits may be required. Always obtain proper permits and approvals in writing before installing equipment

WARNING: Heat and Noise

Do not install the Brivo Door Station Pro in an area that could drop below 32 degrees FAHRENHEIT (0 degrees CELSIUS) or exceed 125 degrees FAHRENHEIT (52 degrees CELSIUS). Doing so can cause damage to components within the Brivo Door Station Pro. Do not install the Brivo Door Station Pro near or on the same circuit with devices that produce large amounts of electrical noise. This includes grinders, electric motors and blowers, electrical switch-gear and other electrically noisy equipment. Electrical noise can interfere with Brivo Door Station Pro operation. If it is not possible to install the Brivo Door Station Pro away from such sources of noise, it is advisable to isolate it by using a high-quality UPS (Uninterruptible Power Supply) between the AC Mains and the transformer.

WARNING: Humidity

Do not install the Brivo Door Station Pro in an area that could experience humidity greater than 85 percent non-condensing.

General Assembly Procedures

Wiring the cable to the Brivo Door Station Pro

IMPORTANT NOTE: The Brivo Door Station Pro does not support Wiegand wiring.

NOTE: Be sure to thread the wires through the wall plate and optional pan wedge prior to completing wiring up the Brivo Door Station Pro before mounting the wall plate and optional wedge.

1. Cut or tape the ends of any unused wires to prevent shorting.

Power over Ethernet (PoE) settings for both power and Ethernet.

- a) ~53VDC, 400mA via PoE (IEEE 802.3af) at 20W
- b) RJ45 Ethernet connector

2. Wire the Brivo Door Station Pro for OSDP / RS485.

- a) RS485A (RXD+ or D0) - Green wire
- b) RS485B (RXD- or D1) - White wire
- c) GND (Ground) - Black wire
- d) Verify the BDS Pro is communicating. Refer to Troubleshooting section of this guide for instructions.

IMPORTANT NOTE: Intercom functionality is not supported when the Brivo Door Station Pro is used as a secondary OSDP reader with the ACS100 control panel.

OSDP / RS-485 Wiring Table

Hardware	Green Reader Wire	White Reader Wire
ACS6000/ACS6100	D0 / RXD +	D1 / RXD -
ACS300	RXD +	RXD -
ACS100	Green	White
ACS-SDC	RS485 +	RS485 -

Mount the Brivo Door Station Pro

1. The Brivo Door Station Pro has three mounting styles provided for with included hardware. Other mounting styles may be accomplished with custom adaptation.

Mount Type 1 - The Brivo Door Station Pro can be mounted directly to a wall or mullion using only the mounting plate and provide screw hardware.

Mount Type 2 - The Brivo Door Station Pro can be mounted over a single gang junction box using the included single gang cover and the mounting plate.

Mount Type 3 - The Brivo Door Station Pro can be mounted over a single gang junction box or directly to a wall using the include pan wedge cover and the mounting plate.

Brivo Door Station Pro Configuration

Configure and test your Brivo Door Station Pro in Brivo Access

The Brivo Door Station Pro is an advanced access control device that integrates video and audio intercom capabilities with facial authentication. It is designed to enhance security and streamline access management.

Prerequisites

Reseller Remote Access support admins have permission to view and manage control panels. Account administrators will need the **Configuration** role. Contact your reseller to enable the Configuration role on your account.

Steps to configure a Brivo Door Station Pro

1. Go to portal.brivo.com (US) or portal.eu.brivo.com (EU).
2. Enter your credentials and click **Sign In**.
3. Click **Customers** on the left navigation bar.
4. Search for the customer you wish to remotely access.
5. In the Remote Login section, click on **Account Config** to remotely log into the customer's account.
6. From the left navigation bar in Brivo Access, choose **Settings** and then click the **Sites** tab. The Site List displays.
7. Click the site to which you want to add a door. The **View Site** page displays.
8. Click **More Operations** and select **Add Door**. The **Add Door** page displays.
9. Enter a brief, descriptive name in the **Door Name** field.
10. Select a **Control Panel** from the dropdown list and click **Next**.
11. Select the **Board** then **Node**. The **Define Door** page displays.
12. Click a **Door Board/Node** combination from the **Board** and **Node** dropdown list. Only valid, available combinations are listed.

IMPORTANT NOTES:

- Verify that the address and baud rate of the Brivo Door Station Pro are configured properly for the panel type you are using. The **OSDP Device Address** and **Baud Rate** should match the expected door/panel settings.
- For ACS6000 and ACS300 panels only, the **Reader Interface** options are Wiegand and OSDP. The default setting is Wiegand, but needs to be changed to OSDP.
- For ACS6100 hardware, contact Brivo Technical Support (1-866-274-8648) to enable automatically updating of door board firmware.
- For ACS100 and ACS-SDC panels only, the Reader Interface is set to OSDP and cannot be changed.
- For ACS100 and ACS-SDC panels, you do not need to select the OSDP Device Address from the dropdown list.

13. Configure the remaining door settings as needed.
14. When finished, click **Save Door**.

Configure your Intercom call receiver in Brivo Access

1. On the left navigation bar, select **Devices**.
2. Once on the **Devices** page, select your **Brivo Door Station Pro**.
3. A pop-up window with your Brivo Door Station Pro details will appear. Click the **Manage** button next to **Notifications**. This will allow a credential user or Brivo Access administrator to receive notifications when the Intercom is activated.
4. Both credential **User** and **Access Administrators** will display in the User dropdown list.
5. **Access Administrators** will be notified while logged into Brivo Access.
6. **Credential Users** that are assigned will be notified through the Brivo Mobile Pass application.
7. Choose a **Schedule** from the dropdown list during which the recipient will receive notifications of an Intercom call.
8. Once a schedule has been selected, click on the **Add** button and the credential user or Brivo Access administrator will appear in the **Users** list along with the notification method (Access or Brivo Mobile Pass). To remove a User from the list, click on the **X** in the same row as the desired User.

Configure your notifications for your Brivo Door Station Pro in Brivo Access

1. On the left navigation bar, select **Devices**.
2. Once on the **Devices** page, select your **Brivo Door Station Pro**.
3. A pop-up window with your Brivo Door Station Pro details will appear. Click the **Manage** button next to **Notifications**. The **BDS Notification** pop-up window displays. The **Enable AI voice assistant** checkbox is off by default. Check the checkbox to enable the feature.
4. Select your user from the dropdown menu. The user list is sorted by **Last Name**.

IMPORTANT NOTE: Notifications for the Brivo Door Station Pro can be sent to Access Administrator OR Brivo Mobile Pass credential holders (who might not be an Access Administrator). If you are an administrator and have a Brivo Mobile Pass assigned to you, your name will appear twice in the User list. It is important to note that if you want to be notified through Brivo Access AND through your Brivo Mobile Pass app that you select BOTH your BMP and Admin names on the User list.

IMPORTANT NOTE: For a Brivo Mobile Pass user to show up in the notifications, that user must have access to the door with the Brivo Door Station Pro.

5. Once you have selected a user, select a **Schedule** from the dropdown menu. During this time, the users listed will receive notifications (either through **Brivo Access** or **Brivo Mobile Pass**) if someone uses the Intercom button on the Brivo Door Station Pro.
6. Once you have added your users and assigned your schedules, click the **Add** button to complete the process. Your selected user name will now appear on the list under the associated schedule.

7. To delete a user from the notification list, click on the **X** next to their name. Remember, if you are receiving notifications both as an Admin and BMP credential holder, you will need to remove both to stop receiving notifications.
8. To close the window, click the **X** in the upper right-hand corner.

Test your Intercom call receiver in Brivo Access

1. Verify browser settings are set correctly for granting microphone access for the site
 - a) Browser settings are dependent on the browser and usually defined per site. Please refer to browser documentation.
 - b) Generally the URL bar will have a microphone access permission icon. In chrome (chrome://settings), go to Site Settings > Microphone. Ensure the site being accessed has been granted permission. Note that some browsers may hide notification about microphone permission if the site was previously blocked.
2. Test **Intercom** to Access
 - a) Verify video.
 - i. With everything completed and working above. Press the intercom button located on the Brivo Door Station Pro.
 - ii. Administrators logged into Access will see a pop-up notification and hear a chime.



- iii. Administrators will click on the **Answer Call** button to receive the call.
- iv. After the Administrator answers the call, the Administrator should see and hear the person standing in front of the Brivo Door Station Pro unit.
- v. The person in front of the unit should hear a chime after pressing the **Intercom** button, until someone answers the call or it times out after 30 seconds. If answered, the person will hear the voice of the recipient of the intercom call.
- vi. The Administrator will be able to unlock the door for the person requesting entry.
- vii. If there are video/audio problems or the door will not unlock, contact Brivo Support.

Test Intercom to call a mobile phone using Brivo Mobile Pass

NOTE: The Brivo Mobile Pass user must have door access in order to be granted call notification, as the user will be able to unlock the door on the call.

1. Verify the phone settings are set correctly for granting microphone access for Brivo Mobile Pass.
 - a) Select the **hamburger icon** in the top right corner within the Brivo Mobile Pass app, and ensure the proper account is selected in Brivo Mobile Pass.
 - b) Select **My Settings**. Ensure **Push Notifications** and **Intercom** permissions are enabled.
 - c) In the phone settings, ensure that the Brivo Mobile Pass app has microphone access.

Configure and test a user with physical credentials

NOTE: The Brivo Door Station Pro does not work with low-frequency Prox (125kHz) cards

1. Ensure a user is in a group that has access to the door or add them.
2. Ensure a user has a credential assigned to them or assign one to them. Ensure it is using the proper credential format compared to an unknown credential type.
3. Present the credential.
4. Verify that the user can use a physical credential to enter. The Brivo Door Station Pro should beep and flash green for credential presentation, while the panel should unlock the door and then drive the Brivo Door Station LED operation.

Configure and test a user with Bluetooth credentials

1. Ensure a user is in a group that has access to the door or add them.
2. Ensure the user has a **Brivo Mobile Pass** or assign one to them.
3. If not done so previously, have the user accept and add the mobile pass to **Brivo Mobile Pass**.
4. Verify that the user can use Bluetooth to enter using the magic button. The user needs to be within BLE range (approximately six feet) of the Brivo Door Station Pro and make sure Bluetooth is turned on for the phone. The Brivo Door Station Pro should beep and flash green for credential presentation, while the panel should unlock the door and then drive the Brivo Door Station Pro LED operation.
 - a) If there are issues, consider:
 - i. Reloading the **Brivo Mobile Pass** App can expedite the process to accelerate onsite testing and ensure the credential was added for the **Brivo Mobile Pass** App.
 - ii. Ensure the door shows up if you look for it manually. Selecting it directly versus using the Magic Button can assist in troubleshooting or if there are multiple Bluetooth readers nearby.
 - iii. If the user was added to a new group for this test, ensure that BMP has been updated (synced) with the Brivo cloud server.
 - a. Normally this is unnecessary, as a panel will query the server if it does not recognize a credential. Updates are usually sent down immediately, but frequent updates on an account can cause updates to be buffered to avoid constantly flushing panel updates.
 - b. Panel logs can be reviewed to ensure recent configuration updates are downloaded after being applied on the server.

Reader LED Operations for the Brivo Door Station Pro

At startup, the Brivo Door Station Pro LED will flash a white LED.

For OSDP operations, the Brivo control panel drives the LED operations of the Brivo Door Station Pro.

For credential presentation, card swipes, successful use of BLE Brivo Mobile Pass, and successful face recognition cause the Brivo Door Station Pro LED to flash green and beep once before returning to OSDP control.

For face detection, as the user approaches the Brivo Door Station Pro, the unit will begin to flash yellow once a face is detected. If the user continues and is known, a facial recognition will be made and the LED will respond as shown above.

Troubleshooting

Troubleshooting the Brivo Door Station Pro is not merely a technical exercise; it can be a critical process that underpins the security, efficiency, and cost-effectiveness of Brivo's ecosystem. Issues with your Brivo Door Station Pro can cause installation delays and lead to frustrated users and administrators. By systematically identifying and resolving issues, you can ensure seamless access and prevent potential future issues. Therefore, understanding the value of troubleshooting is paramount for maintaining a robust and reliable security infrastructure. This section of the Installation Guide provides you with a number of troubleshooting options if you encounter issues with the installation and configuration of your Brivo Door Station Pro. These steps may not be necessary during your installation process but are provided here as a courtesy.

Verify that the OSDP connection between the panel and the Brivo Door Station Pro is working

1. Using the WebCLI of the control panel, go to Hardware > OSDP Tool to check that the Brivo Door Station Pro can be detected via OSDP and it has the correct PD address and baud rate (9600 is the default), matching Brivo Access settings.
2. Using the WebCLI of the control panel, go to Hardware > OSDP Tool to adjust the Brivo Door Station Pro PD address and baud rate as necessary.
3. If the Brivo Door Station Pro is not detected, check the wiring and OSDP termination.
4. Gather the Brivo Door Station Pro information via panel WebCLI: Hardware > Upgrade Reader Firmware
 - a) The IP address, Serial Number, and Brivo Door Station Pro firmware version are available if the Brivo Door Station Pro is connected via OSDP.
5. The reported information will include status about Connection to PDS and JWT status.

JWT status must be Valid. If the Brivo Door Station Pro is using DHCP, and the Brivo Door Station Pro is connected, and the JWT status is valid, and there are no other settings to configure, then the next step can be skipped.

 - a) Generally it takes a minute or two for panel and Brivo Door Station Pro to boot and communicate sufficiently to get an Access Token and JWT.
 - b) If specific network settings are required for the Brivo Door Station Pro, continue to the next step. After setting specific network settings, ensure the Brivo Door Station Pro is able to get a JWT and talk to Brivo servers.



Verify that the Brivo Door Station Pro is communicating with the Brivo cloud server

1. Make sure the Brivo Door Station Pro unit is connected via Power over Ethernet (PoE) and powered.
2. Connect to the Brivo Door Station Pro using the built in WebUI tool. For details, refer to the Brivo Door Station Pro chapter of the [Panel Networking Guide](#).
 - a) Option 1: Use the IP from the panel. (See steps above for finding the IP address).
 - b) Option 2: Use local IT, network tools, or the panel log file to determine the IP otherwise. The MAC address on the back of the Brivo Door Station Pro can be used to find the device. The MAC address starts with the Brivo OUI 00:1D:00.
 - i. IT often has access to network equipment that can report the devices on the network by IP and MAC address.
 - ii. With IT approval, tools like arp can generally be used if the discovery computer is on the same subnet and/or switch as the Brivo Door Station Pro.
 - c) Option 3: Isolate the Brivo Door Station Pro on a switch and set the IP of the discovering device to 169.254.17.2 (anything but 169.254.17.1) and connect to it using the IP 169.254.17.1
3. Adjust network settings as directed by the customer's IT administrator.
 - a) DHCP or static.
 - b) DNS (recommend 8.8.8.8 or 8.8.4.4).
4. If necessary, reconnect the Brivo Door Station Pro to the target network.
5. Verify that the Brivo Door Station Pro is talking to the Brivo cloud server. You can do this in one of two ways:
 - a) Via Access: Door Device Page: Reader and Network Status: Online.
 - b) Via Panel WebCLI: Step 5 on page 14 will show "Connection to PDS: connected".
6. If the Brivo Door Station Pro is not showing connected to the Brivo PDS (Panel Data Service):
 - a) Ensure the OSDP connection is working as expected. You may do this by reviewing the Panel and Brivo Door Station Pro data logs.
 - b) Ensure the Brivo Door Station Pro has general network connectivity by reviewing the Brivo Door Station Pro logs.
 - c) Ensure enough time has been permitted for an Access Token and JWT to be granted by reviewing the Brivo Door Station Pro logs for Access Token and JWT messages.
 - i. Generally it takes a minute or two for panel and Brivo Door Station Pro to boot and communicate sufficiently to get an Access Token and JWT.
 - d) If the Brivo Door Station Pro is not receiving an Access Token:
 - i. Check the Door settings in Access contain the Brivo Door Station Pro SN. For troubleshooting, the SN can be cleared and the door pulsed to ensure it auto-populates.
 - ii. Review the Panel logs to see if the panel is getting an Access Token from the server.
 - e) If the Panel is getting repeated 401's when getting a JWT get a JWT.
 - i. Ensure the OSDP communication is reliable by reviewing Panel and Brivo Door Station Pro logs for OSDP communication resets. This might be messages about OSDP packet drop or in the panel log messages about disconnect and returning to clear text for OSDP.
 - ii. If the issue persists, contact Brivo Support at 866-BRIVO-4U or customercare@brivo.com.

Verify that you can connect to the Brivo Door Station Pro's built-in WebUI interface and that the Brivo Door Station Pro firmware is up to date

IMPORTANT NOTE: Accessing the Brivo Door Station Pro local administrative interface is similar to other control panels (ACS100 and ACS-SDC) in that there is only one LAN port. Instead of connecting your laptop directly to the Brivo Door Station Pro, you need to connect a CAT 5 network cable with RJ45 jacks from the network jack on your laptop to the same network as the Brivo Door Station Pro (usually through a PoE switch).

1. Obtain your Brivo Door Station Pro IP address from the control panel attached to the Brivo Door Station Pro by viewing the Hardware/Upgrade Reader firmware tab if connected over OSDP or from the Network Admin/Router administration for the associated MAC address of the reader.
2. Open your web browser and navigate to your Brivo Door Station Pro's IP address.
3. A login screen similar to the one shown here will display.



4. Click on the center icon and enter administrator as the default user name and bds5cli as the default password in the pop-up window and click Sign In.
5. Once in the Brivo Door Station Pro WebUI interface, click on the Status tab on the menu bar. In the System section of the Status page, the firmware version of the Brivo Door Station Pro will be displayed. The firmware version must be version 1.0.7 or later. If it is not, contact Brivo Support at 866-BRIVO-4U or customercare@brivo.com.
6. While still connected to the Brivo Door Station Pro WebUI, proceed to the next section.

Verify Brivo Door Station Pro functionality by using the Troubleshooting Tool

IMPORTANT NOTE: The troubleshooting tool is only available on firmware version 1.0.7 or later.

1. Use the WebUI Troubleshooting Tool (WebUI > Gear Icon > Troubleshooting Tool) to:
 - a) If not done already, verify the Brivo Door Station Pro can connect to Brivo services. The test can be run by clicking the Start button under the Brivo Server Connectivity section and the Start button under the OSDP section.
 - b) Verify the Video service is properly running for Live Video and Intercom is properly running by clicking Start under the Video Service & WebRTC section. It also validates that the Brivo Door Station can get through Firewalls. It takes about 10 seconds to run while it observes the Video service and prints any failure messages. If there are any issues, review the steps below to help troubleshoot the issue.
 - i. Review the output of the Video Service NAT behavior.
 - 1) The Brivo Door Station Pro requires valid time from NTP to connect to the Amazon KVS services and properly stream video.
 - a. At boot up, it can take a minute or so to get valid time from NTP.
 - b. It is also possible the NTP service is blocked by IT/firewall rules.
 - 2) DNS or networking issues can prevent the routing to the Amazon KVS services.
 - a. Setting DNS to 8.8.8.8 or 8.8.4.4 from Google can be used to troubleshoot this issue.
 - b. Local DNS caches can occasionally be slow to cache Amazon KVS service updates as AWS scales or adjusts resources.
 3. If next gen firewalls are being used with URL whitelisting or reputation checking, it can create issues connecting to AWS services.
 4. While rare, issues with AWS IoT provisioning can prevent the BDS from connecting.
 - ii. When using DHCP with fixed DNS settings, DHCP provided DNS settings are prioritized over fixed DNS settings when the DHCP lease renewal occurs.
 - 1) The solution to this problem is to upgrade to BDS 1.0.8 (available soon) or use a static IP with fixed DNS settings
 - a. Fixed DNS settings are normally used when the local DNS is cached and does not update frequently to reflect Amazon KVS changes. Using fixed DNS settings (e.g., 8.8.8.8 or 8.8.4.4) are often used to resolve Live Video not working or being intermittent.
 - b. Without a solution, Live Video may begin working after initially setting fixed DNS settings before not working on DHCP lease renewal. This operation may be intermittent depending on updates to local DHCP provided DNS settings or it may require the BDS to be restarted after DHCP lease renewal. The customer report has been that the device needs to be restarted periodically. The period will be based on the frequency of DHCP renewal and the root cause can be confirmed by reviewing the device logs.
 - c) Verify the Status of Recent Connections by clicking the Start button under the WebRTC Recent Connections section.

NOTE: Viewing Live Video performing Intercom calls is covered in more detail later, but this step shows how the Troubleshooting Tool can assist in debugging issues. The test will review the recent WebRTC connections to report the number of connection attempts, successes, and failures. It reviews recent logs that can span from a few minutes to hours depending on what the Brivo Door Station Pro is doing.

- i. Firewall issues can generally be spotted with unsuccessful connections. Please review the Ports and IP Addresses in Appendix 1 or in the help article linked below.
 - 1) Common issues relate to denying UDP traffic, DNS delays, Next Gen Firewall settings (URL whitelisting, reputation checking etc).

- ii. Attempt connections and re-run the test. If there is no change in the number of connection attempts, it can be due to issues on the client device or firewall rules:
 - 1) The most common reason for not seeing incoming connections, is that the client has not enabled proper permission settings (e.g., microphone), the client device does not have a microphone, or the device does not have ability to play video (H.264 encoded). The location of settings can vary by browser and phone vendor. These settings can be hidden or difficult to find if previously denied by a user or as a default by IT policy.
 - 2) If the Video service is running as expected, it is not likely to service firewall issues here (no change in count vs. failed connections), but it is possible if the client is on a very restricted network. The connection to the signaling channel to negotiate a video stream happens via Amazon KVS using a TLS connection to port 443.
- d) See the [Ports and IP Addresses by Product Category](#) in Appendix 1 or click the link to read the Brivo help article for firewall configuration information and troubleshooting advanced firewall and port settings.

What are some troubleshooting steps for live video on the Brivo Door Station Pro?

General:

- No Live Video or Intermittent Live Video:
 - Ensure the BDS has firmware 1.0.7 or greater
 - Try opening all outbound traffic for the BDS and see if that resolves live video issues. More restrictive rules can be established to meet the desired security posture, but opening up outbound connections helps isolate and resolve issues.
 - If advanced firewalls are being deployed, review the notes below on the topic below.
 - If the firewall has the ability to monitor dropped and malformed packets, leverage the network tool to evaluate issues with network and firewall rules
 - Observe the location of the BDS and live video client. WebRTC will try to establish the best connection for low latency streaming. Local connections may avoid network firewalls, but sometimes there can be firewall rules between VLANs or subnet traffic.
- No Live Video:
 - Ensure UDP is enabled on port 443 for the device. It is included in the guidance, but it has been the issue for a few installations.
- Intermittent Live Video:
 - Try using Google DNS (8.8.8.8 / 8.8.4.4), some customers have reported intermittent live video when using local DNS. The cause relates to short caching by the local DNS or delays in propagation for Amazon KVS updates.

Base Setup:

Brivo recommends starting with a base setup to establish and validate live video before establishing more restrictive firewall rules as required for the installation. The BDS uses WebRTC with Amazon KVS to provide scale and availability, but it means that IP based whitelisting may limit live video capabilities.

- Firewall: Allow all out outbound connections for the BDS
 - Some installers have reported using static IPs can make opening outbound connections easier when working with the IT staff for an installation site. Other methods should work, but it improved communication with IT while validating the initial installation.
- DNS: 8.8.8.8 / 8.8.4.4
 - NOTE: Next generation firewalls may require use of local DNS or they will redirect queries and analyze them, but testing with 8.8.8.8 / 8.8.4.4 has helped isolate network issues.

Advanced Firewalls:

Firewalls with advanced features can require vendor unique programming and interfere with video services. The impact may be intermittent or less obvious than with legacy firewall rules. Below are some examples of the impacts observed:

URL Filtering:

Filtering capability can vary between network gear vendors, so it is important to ensure the rules are set as required for the specific device. Some vendors might only need a rule with `kinesisvideo.us-east-1.amazonaws.com` while others would also require `*.kinesisvideo.us-east-1.amazonaws.com` for subdomains.

Depending on the firewall, the device may build up a cache of associated IPs for URLs which can create disruptions if the filtering initially blocks requests while it does a lookup. Some firewalls will block initial TLS 1.2+ connections, in an attempt to force a reconnection at a lower TLS level where it can inspect the SNI.

Reputation Checking:

Unknown IPs can be rejected until the firewall can build a reputation score or get one from an online service. This delay can cause initial connections to be rejected or timeout. Connections to the Amazon KVS services are particularly impacted.

What does the Brivo Door Station Pro use for Video Services?

The BDS uses WebRTC for video streaming capabilities with Amazon KVS for scale and availability. The standard is briefly described below:

WebRTC:

WebRTC (Web Real-Time Communication) is an open framework that enables browsers and mobile applications to communicate directly in real time using audio, video, and data streams without requiring plugins or external software. It uses protocols like STUN, TURN, and ICE to establish peer-to-peer connections, even across NATs and firewalls. WebRTC is used for building applications like video conferencing and live streaming because it minimizes latency and provides a secure, high-quality communication experience. Its support for open standards and cross-platform compatibility makes it a powerful choice for modern real-time communication needs.

Wiki: <https://en.wikipedia.org/wiki/WebRTC>

Website: <https://webrtc.org/>

STUN:

STUN (Session Traversal Utilities for NAT) is a protocol that helps devices behind NATs (Network Address Translators) discover their public IP address and port, enabling peer-to-peer communication. It works by sending a request from a client to a STUN server, which responds with the client's public-facing information. This is crucial for establishing direct connections in protocols like WebRTC, as it allows devices to communicate across different network boundaries. While STUN facilitates connectivity, it doesn't handle scenarios where direct communication is impossible, so those cases require a TURN server.

TURN:

In WebRTC, TURN (Traversal Using Relays around NAT) is a protocol used to facilitate the transmission of media streams (such as audio and video) between peers in situations where direct peer-to-peer communication is not possible due to restrictive NAT (Network Address Translation) or firewall configurations.

Revision Table

Version	Date	Author	Content
0.1	11/21/2025	BRH	Original document - renamed Brivo Door Station Pro Quick Reference Sheet
0.2	2/5/2026	EMS	Updated the FCC and Canada legal disclaimer section

Appendix 1

Ports and IP Addresses for the Brivo Door Station Pro

This article shows which ports and IP addresses that need to be available for the Brivo Door Station Pro.

Q: What ports need to be open on the networking facing LAN port (firewall rules)?

Protocol	Port	Usage/Application Protocol	In / Out
UDP/TCP	53	DNS	OUT
UDP	123	NTP	OUT
TCP	443	WebRTC: KVS - HTTPS / WSS	OUT
UDP	443	WebRTC: TURN (Relay)	OUT

Q: What URLs will the Brivo Door Station Pro communicate with the US?

Port	URL	Protocol/Usage
443	access-api.prod.brivo.com	HTTPS (TCP)
443	bds.prod.brivo.com	HTTPS (TCP)
443	devices.prod.brivo.com	HTTPS (TCP)
123	*.pool.ntp.org	NTP (UDP)
443	*.credentials.iot.us-east-1.amazonaws.com	HTTPS (TCP)
443	kinesisvideo.us-east-1.amazonaws.com	WSS/HTTPS/STUN/TURN (TCP/UDP)
443	*.kinesisvideo.us-east-1.amazonaws.com	WSS/HTTPS/STUN/TURN (TCP/UDP)
443	*.amazontrust.com	HTTPS (TCP)

Q: What URLs will the Brivo Door Station Pro communicate with in Europe?

Port	URL	Protocol/Usage
443	access-api.eu.brivo.com	HTTPS (TCP)
443	bds.eu.brivo.com	HTTPS (TCP)
443	devices.eu.brivo.com	HTTPS (TCP)
123	*.pool.ntp.org	NTP (UDP)
443	*.credentials.iot.eu-east-1.amazonaws.com	HTTPS (TCP)
443	kinesisvideo.eu-east-1.amazonaws.com	WSS/HTTPS/STUN/TURN (TCP/UDP)
443	*.kinesisvideo.eu-east-1.amazonaws.com	WSS/HTTPS/STUN/TURN (TCP/UDP)
443	*.amazontrust.com	HTTPS (TCP)