Panel Networking Guide

I Introduction

II ACS6000, ACS300, ACS5000, and IPDC

III ACS100

Legal Disclaimers

Federal Communications Commission (FCC) Compliance

You are cautioned that changes or modifications not expressly approved by the part responsible for compliance could void the user's authority to operate the equipment.

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 instruction manual, 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:

- Re-orient or relocate the receiving antenna.
- Increase the distance between the equipment and receiver.
- Connect the equipment to a circuit other than the one to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

These devices comply with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. These devices may not cause harmful interference and
2. These devices must accept any interference received, including interference that may cause undesired operation of the device.

FCC RF Radiation Exposure Statement (ACS6000 and ACS300 only)

1. The transmitter must not be co-located or operate in conjunction with any other antenna or transmitter.
2. This equipment complies with the FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

Underwriter Laboratories (UL) Compliance

Brivo controllers comply with the UL 294 Standard for access control units with the following restrictions:

- All models: The Ethernet port is for supplemental use only. The unit will continue to operate standalone if the network connection is interrupted.
- All models: The monitoring software is not UL evaluated.
- **ACS6000**/**ACS300**: Wi-Fi connection is supplemental and was not evaluated by UL.
- **ACS300**: Bluetooth capability was not verified by UL.

Canada-Underwriters Laboratories (C-UL) Compliance

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

Parts and Service

All Brivo controllers contain no user serviceable parts. The lithium battery is not serviceable and is to be replaced by qualified service technicians only.

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 https://partner.brivo.com/welcome and click Sign In to gain access to the Partner Portal.

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.

© 2021 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

Document Objectives

This Panel Networking Guide provides all the information needed to operate a Brivo control panel on a Local Area Network (LAN) connected to the Internet. The document covers the -E and -A versions of the control panels.

By default, the Brivo control panels automatically configure themselves upon power-up and contacts the Brivo Cloud Server (-E) or the Brivo Onsite Server (-A) with no intervention from the installer or IT personnel. This ease of installation is possible because the control panel:

- uses DHCP to configure network parameters
- does NOT require a static or routable IP address
- initiates all communications with the Brivo Cloud Server or Brivo Onsite Server
- for the –E panel, it uses only HTTPS (Port 443 Outbound) to communicate with the Brivo Cloud Server

The Panel Networking Guide's primary audience is trained access control installation technicians (Installers) and IT personnel, who should use this Guide in conjunction with the corresponding Installation Manual. This document may also be used by dealers and their sales professionals to help them conduct pre-sales, and to provide client support during the network configuration process. It may also be used for in-house training purposes and ongoing support.

Terminology

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 Manual, and certain terminology may not apply to all models.

- ***Control chassis***. The main chassis for a control panel. The control chassis contains the MAIN BOARD, and for the **ACS5000** and **ACS6000**, may also contain one expansion board, either a DOOR BOARD or an INPUT/OUTPUT BOARD (if using a standard chassis) or three expansion boards in any combination of DOOR BOARDs or INPUT/OUTPUT BOARDs (if using a large chassis).

- ***Expansion chassis***. **ACS5000 and ACS6000 only**. Additional chassis, containing one or two expansion boards, either DOOR BOARDs and/or INPUT OUTPUT BOARDs.

- ***Large expansion chassis***. **ACS5000 and ACS6000 only**. Additional chassis, containing up to four expansion boards, either DOOR BOARDs and/or INPUT OUTPUT BOARDs.

- ***Control panel***. The complete system of control chassis and possible expansion chassis for an account. A control panel will have the MAIN BOARD (contained in the control chassis) and (if using an **ACS5000** or **ACS6000**) a number of additional expansion chassis (standard or large) to hold a maximum of 14 additional DOOR BOARDs and/or INPUT OUTPUT BOARDs (for a total maximum of 15 boards).

- ***Access control system (ACS)***. The complete interaction between a control panel and the Brivo product (Access or Onsite 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.

- ***Brivo Onsite Server***. Brivo's appliance-based application which enables the end user to manage their Brivo Onsite Server account.

© 2021 Brivo Systems LLC. All rights reserved.

Registration

The control panel is considered “registered” when it is properly installed and configured through the Brivo Cloud Server (for the -E) or the Brivo Onsite Server (for the -A).

Additional Resources

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

- Installation Manuals
- Installation Worksheets
- https://www.brivo.com
- Technical Support: 1-866-BRIVO-4-U

Understanding the Network Environment

This section describes the basic operation of the control panel in an IP network environment.

Network Requirements

Requirements	Comments
Ethernet 10/100 Base T LAN	CAT5 Cabling with RJ45 Connectors
Ethernet Hub/Switch set to Auto-Negotiate	Most hubs and switches default to auto-negotiate, which is the preferred setting
LAN Connected to Internet	Minimal bandwidth; Cable/DSL compatible
Allow Outbound HTTPS	Allow Port 443 Outbound on Firewall
DHCP	DHCP Recommended
Proxy Server	SOCKS5 Proxy login supported
SNMP – Not supported/required	SNMP is a security vulnerability

Bandwidth Usage

The Brivo control panel has a virtually unnoticeable effect on your LAN environment. It requires very little bandwidth and no network management.

The control panel produces the following types of network traffic:

For both panel versions, in response to local events (credential authorization, alarms, timers, etc.), it posts HTTPS messages to the Brivo Cloud Server.

For the -E, it periodically polls the Brivo Cloud Server using HTTPS to query for new data that may be available.

NOTE: The polling period is set by default to a five-minute interval for the –E panel version.

For the -A, the panel will contact the Brivo Onsite Server each time it encounters a situation where the data is not in the panel's current database. Additionally, the Brivo Onsite Server appliance will push new data to the -A panel when there is a change in configuration.

For both panel versions, it downloads new data sets via HTTPS when available. Data sets consist of credentials, schedules, configuration parameters, etc. They may be anywhere from a few kilobytes to several tens of kilobytes, depending on the size of the user population, number of schedules, number of changes to the account, etc.

For the -E, the panel firmware is upgraded automatically when the hardware connects to the Brivo Cloud Server for the first time.

For the -A, when the panel first handshakes with the Brivo Onsite Server appliance, the firmware will automatically be updated. Additionally, the administrator of the Brivo Onsite Server appliance may manually update the firmware of all connected panels when the Brivo Onsite Server appliance receives a new upgrade file.

Firewall Considerations

The -E panel operates successfully through any firewall that is configured to allow OUTBOUND HTTPS traffic (Port 443). It does not require that any firewall ports be open to INBOUND traffic from outside your environment. This is because of the way that the HTTP(S) protocol operates with firewalls.

Data from the Brivo Cloud Server is downloaded to the control panel by virtue of the fact that firewalls allow the response to an HTTP(S) "POST" message to return through the firewall, provided the original POST message originated from within the firewall, as it does in the case of an installed –E panel.

-E Control Panels and Proxy Servers

If there is a proxy server on your network which ordinarily blocks outbound network traffic, please see your network administrator to obtain the required proxy server settings: login ID, password, port number, and IP address of the proxy server. The -E control panel requires this information to authenticate itself to the proxy server and gain access to the Internet.

Using a proxy server may also require that the -E control panel be configured to use a static IP address so that the proxy server can correctly identify the control panel as a "special case" and allow it to communicate to the Internet.

ACS6000, ACS300, ACS5000, & IPDC

This chapter is devoted to the **ACS6000**, **ACS300**, **ACS5000**, and **IPDC** control panels. For information on the **ACS100** control panel, refer to the following chapter.

Accessing the Local Administrative Interface

This section describes how to connect to the Brivo control panel local Administrative Interface (often described throughout this document as the **WebCLI**).

NOTE: In most cases, the Brivo control panel will self-configure its network settings without any input from the installer. You will only need to use access the Administrative Interface if you need to configure your network settings manually or for troubleshooting.

Connect a Laptop to the Admin Port

With your laptop powered down, connect a CAT 5 network cable with RJ45 jacks from the ADMIN port on the Main Board to the network jack on your laptop, as shown in the figures below.

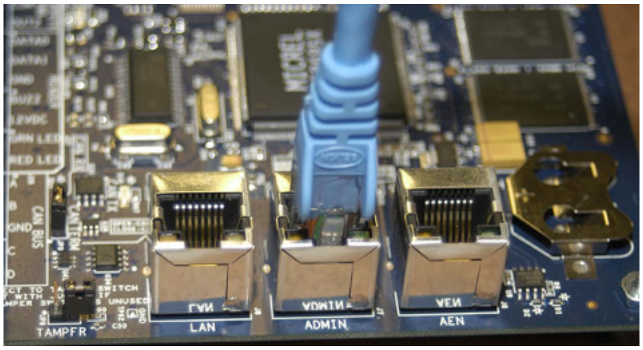


Figure 1: **ACS5000** - Connect laptop to the Admin port

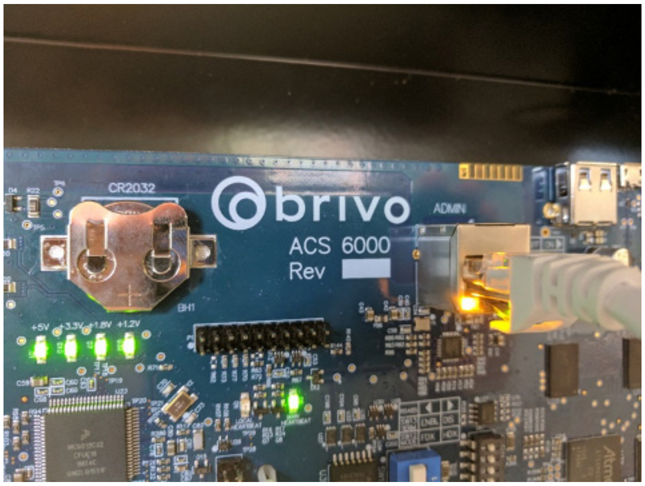


Figure 2: **ACS6000** - Connect laptop to the Admin port

© 2021 Brivo Systems LLC. All rights reserved.

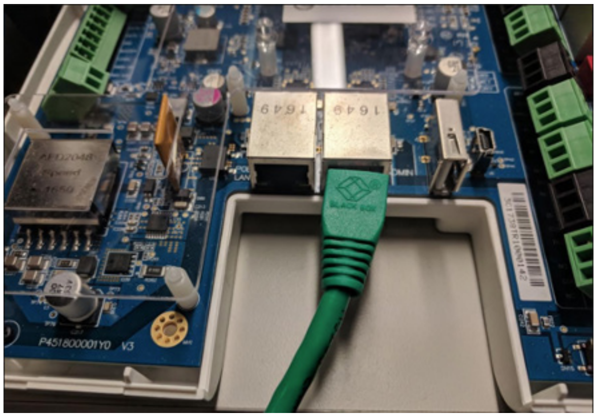


Figure 3: **ACS300** - Connect laptop to the Admin port

When the Ethernet connection is working properly, you will see a green LED illuminated on the right side of the socket. If the green light is not illuminated, check both the connection on the control panel and on the Ethernet hub to which the panel is wired.

Connect the Main Board to a LAN (both -E or- A)

Connect an Ethernet cable from a 10/100 Base T hub to the RJ45 LAN port located on the Main Board, as shown in the figures, below.

NOTE: Only the Main Board requires an Ethernet connection; any other boards that are slaved off the Main Board communicate via the CAN bus.

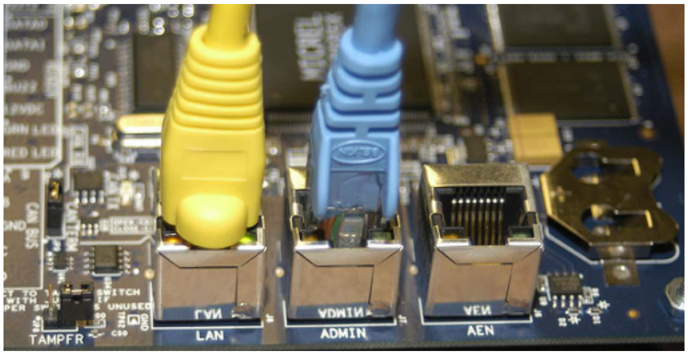


Figure 4: **ACS5000** - Connect Main Board to LAN

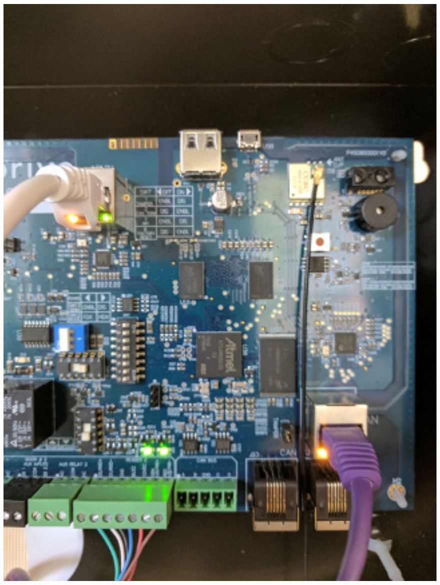


Figure 5: **ACS6000** - Connect Main Board to LAN

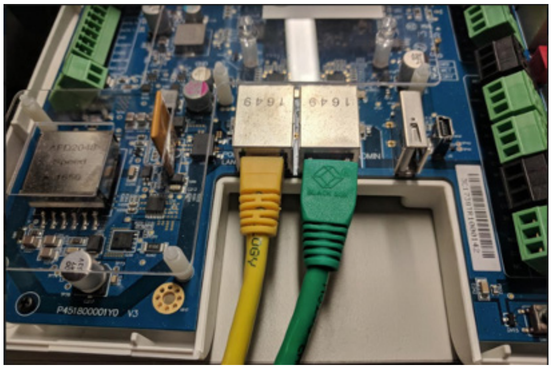


Figure 6: **ACS300** - Connect Main Board to LAN

When the Ethernet connection is working properly, you will see a green LED illuminated on the right side of the socket. If the green light is not illuminated, check the connection on the control panel as well as the connection on the Ethernet hub to which the panel is wired.

Power on the Laptop

Now that you have connected a cable from the laptop to the Main Board, power on your laptop.

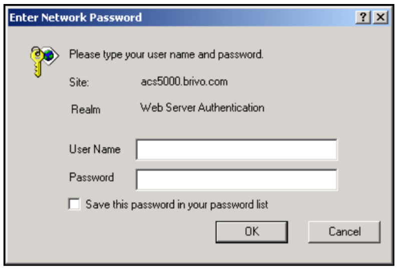
During the power-on sequence, your laptop will obtain local network settings from the Main Board, provided your laptop's network configuration is set to "Automatically Obtain IP Address." This is the most common setting for computers running Microsoft Windows.

If your laptop is not configured to obtain network settings automatically, use the Help utilities on your laptop to determine how to change the settings for your operating system.

Log in to the Administrative Interface

After your computer has finished booting up:

1. Open your web browser.
2. In the address bar, enter: http://192.168.207.1 A pop-up login screen similar to the one shown in the figure below will display.



Please type your user name and password.

Site: acs5000.brivo.com

Realm Web Server Authentication

Figure 7: Login Screen

3. Enter **cli** as the default user name and **new5cli** as the default password. You are now ready to begin configuring your Brivo control panel.

IMPORTANT NOTE: Brivo strongly recommends that you change the default password when you first access the Administrative Interface. Instructions on how to do this are found on the System tab under the Administration sub-tab.

© 2021 Brivo Systems LLC. All rights reserved.

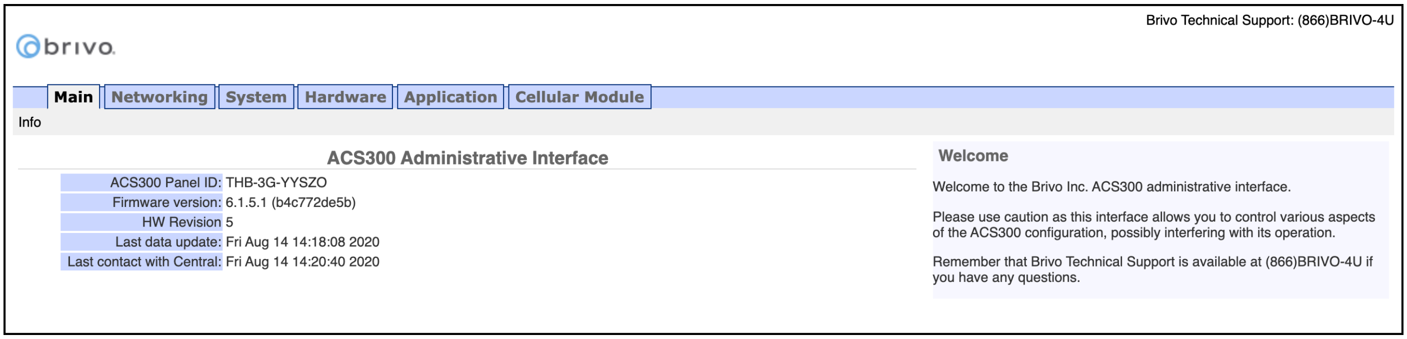
Main Tab

Info

The **Info** screen of the Main tab displays the control panel Administrative Interface.

NOTE: If you were **NOT** able to reach this page for any reason, see the *Troubleshooting* section at the end of this document.

NOTE: For ease of presentation, the screenshots below display **ACS6000** or **ACS300** as the model type. When you log in, the model that displays will match your device type.



ACS300 Administrative Interface

ACS300 Panel ID: THB-3G-YYSZO
Firmware version: 6.1.5.1 (b4c772de5b)
HW Revision 5
Last data update: Fri Aug 14 14:18:08 2020
Last contact with Central: Fri Aug 14 14:20:40 2020

Welcome

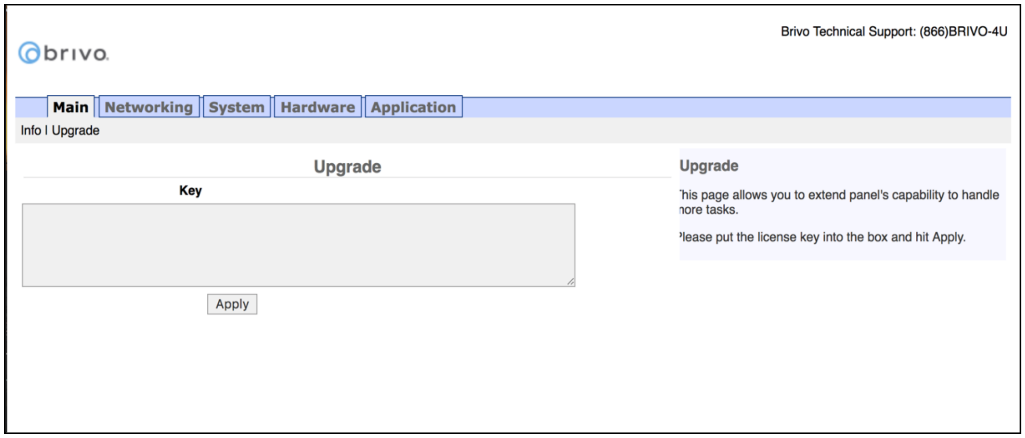
Welcome to the Brivo Inc. ACS300 administrative interface.

Please use caution as this interface allows you to control various aspects of the ACS300 configuration, possibly interfering with its operation.

Remember that Brivo Technical Support is available at (866)BRIVO-4U if you have any questions.

Figure 8: Info page of the Administrative Interface

4. **For IPDC only** - To upgrade the **IPDC** controller from a one-door controller to a two-door controller, click on the **Upgrade** link under the **Main** tab. To complete the upgrade process, contact Brivo Technical Support and follow their provided instructions.



Upgrade

Upgrade

his page allows you to extend panel's capability to handle nore tasks.

Please put the license key into the box and hit Apply.

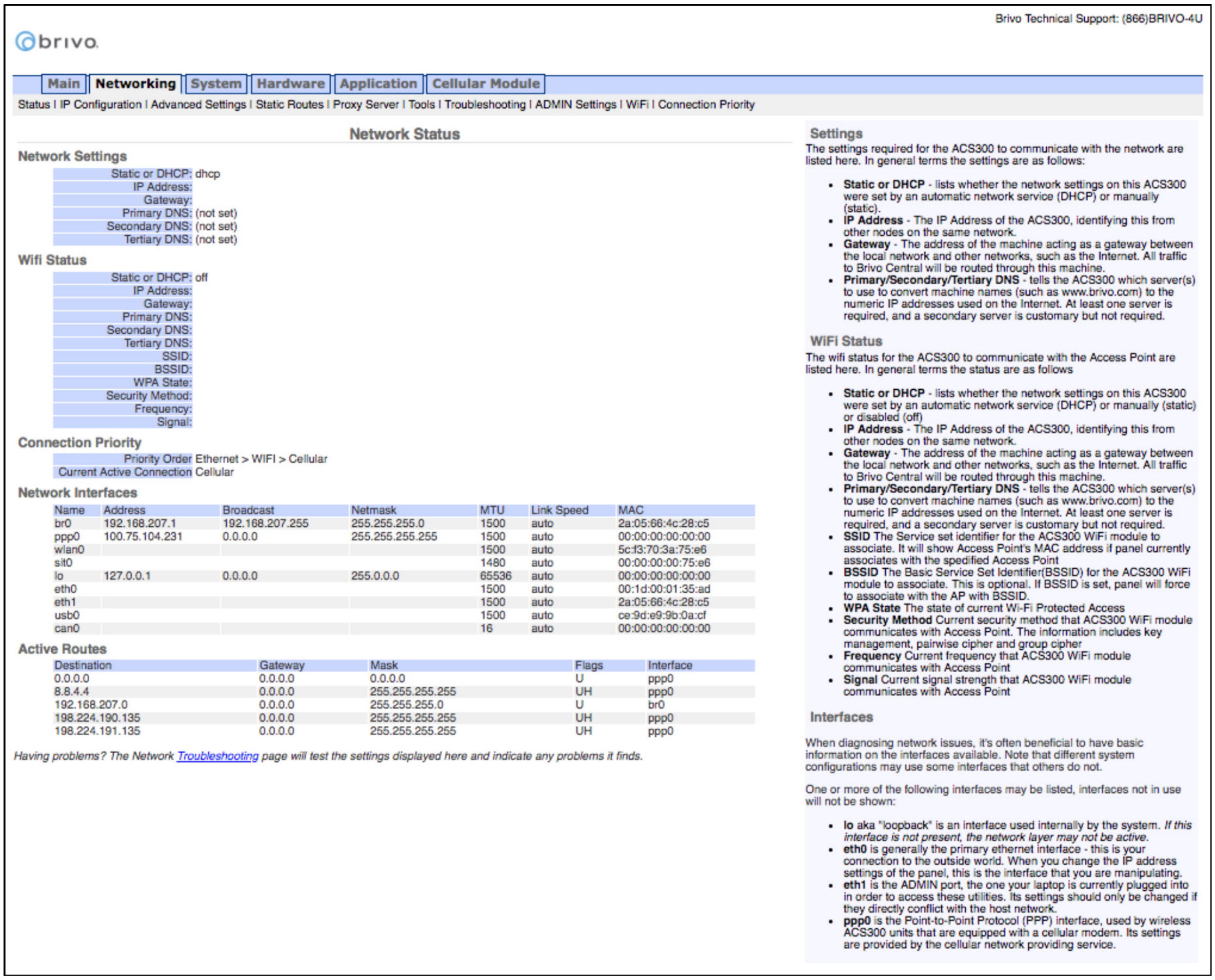
Figure 9: Upgrade page of the Main Administrative Interface

Networking Tab

Status

The Network Status page is useful for diagnosing various network conditions. To access this page:

1. Click **Networking** to access the Networking menu bar.
2. Click **Status** to access the Network Status page. Explanations of the various status fields are provided in the text on the right side of the page.


Brivo Technical Support: (866)BRIVO-4U
Main
Networking
System
Hardware
Application
Cellular Module
Status I IP Configuration I Advanced Settings I Static Routes I Proxy Server I Tools I Troubleshooting I ADMIN Settings I WiFi I Connection Priority

Network Status

Network Settings

Static or DHCP: dhcp
IP Address:
Gateway:
Primary DNS: (not set)
Secondary DNS: (not set)
Tertiary DNS: (not set)

Wifi Status

Static or DHCP: off
IP Address:
Gateway:
Primary DNS:
Secondary DNS:
Tertiary DNS:
SSID:
BSSID:
WPA State:
Security Method:
Frequency:
Signal:

Connection Priority

Priority Order Ethernet > WIFI > Cellular
Current Active Connection Cellular

Network Interfaces

Name	Address	Broadcast	Netmask	MTU	Link Speed	MAC
br0	192.168.207.1	192.168.207.255	255.255.255.0	1500	auto	2a:05:66:4c:28:c5
ppp0	100.75.104.231	0.0.0.0	255.255.255.255	1500	auto	00:00:00:00:00:00
wlan0				1500	auto	5c:f3:70:3a:75:e6
sit0				1480	auto	00:00:00:00:75:e6
lo	127.0.0.1	0.0.0.0	255.0.0.0	65536	auto	00:00:00:00:00:00
eth0				1500	auto	00:1d:00:01:35:ad
eth1				1500	auto	2a:05:66:4c:28:c5
usb0				1500	auto	ce:9d:e9:9b:0a:cf
can0				16	auto	00:00:00:00:00:00

Active Routes

Destination	Gateway	Mask	Flags	Interface
0.0.0.0	0.0.0.0	0.0.0.0	U	ppp0
8.8.4.4	0.0.0.0	255.255.255.255	UH	ppp0
192.168.207.0	0.0.0.0	255.255.255.0	U	br0
198.224.190.135	0.0.0.0	255.255.255.255	UH	ppp0
198.224.191.135	0.0.0.0	255.255.255.255	UH	ppp0

Having problems? The Network Troubleshooting page will test the settings displayed here and indicate any problems it finds.

Settings

The settings required for the ACS300 to communicate with the network are listed here. In general terms the settings are as follows:

- **Static or DHCP** - lists whether the network settings on this ACS300 were set by an automatic network service (DHCP) or manually (static).
- **IP Address** - The IP Address of the ACS300, identifying this from other nodes on the same network.
- **Gateway** - The address of the machine acting as a gateway between the local network and other networks, such as the Internet. All traffic to Brivo Central will be routed through this machine.
- **Primary/Secondary/Tertiary DNS** - tells the ACS300 which server(s) to use to convert machine names (such as www.brivo.com) to the numeric IP addresses used on the Internet. At least one server is required, and a secondary server is customary but not required.

WiFi Status

The wifi status for the ACS300 to communicate with the Access Point are listed here. In general terms the status are as follows

- **Static or DHCP** - lists whether the network settings on this ACS300 were set by an automatic network service (DHCP) or manually (static) or disabled (off)
- **IP Address** - The IP Address of the ACS300, identifying this from other nodes on the same network.
- **Gateway** - The address of the machine acting as a gateway between the local network and other networks, such as the Internet. All traffic to Brivo Central will be routed through this machine.
- **Primary/Secondary/Tertiary DNS** - tells the ACS300 which server(s) to use to convert machine names (such as www.brivo.com) to the numeric IP addresses used on the Internet. At least one server is required, and a secondary server is customary but not required.
- **SSID** The Service set identifier for the ACS300 WiFi module to associate. It will show Access Point's MAC address if panel currently associates with the spedified Access Point
- **BSSID** The Basic Service Set Identifier(BSSID) for the ACS300 WiFi module to associate. This is optional. If BSSID is set, panel will force to associate with the AP with BSSID.
- **WPA State** The state of current Wi-Fi Protected Access
- **Security Method** Current security method that ACS300 WiFi module communicates with Access Point. The information includes key management, pairwise cipher and group cipher
- **Frequency** Current frequency that ACS300 WiFi module communicates with Access Point
- **Signal** Current signal strength that ACS300 WiFi module communicates with Access Point

Interfaces

When diagnosing network issues, it's often beneficial to have basic information on the interfaces available. Note that different system configurations may use some interfaces that others do not.

One or more of the following interfaces may be listed, interfaces not in use will not be shown:

- **lo** aka "loopback" is an interface used internally by the system. *If this interface is not present, the network layer may not be active.*
- **eth0** is generally the primary ethernet interface - this is your connection to the outside world. When you change the IP address settings of the panel, this is the interface that you are manipulating.
- **eth1** is the ADMIN port, the one your laptop is currently plugged into in order to access these utilities. Its settings should only be changed if they directly conflict with the host network.
- **ppp0** is the Point-to-Point Protocol (PPP) interface, used by wireless ACS300 units that are equipped with a cellular modem. Its settings are provided by the cellular network providing service.

Figure 10: Network Status

© 2021 Brivo Systems LLC. All rights reserved.

IP Configuration

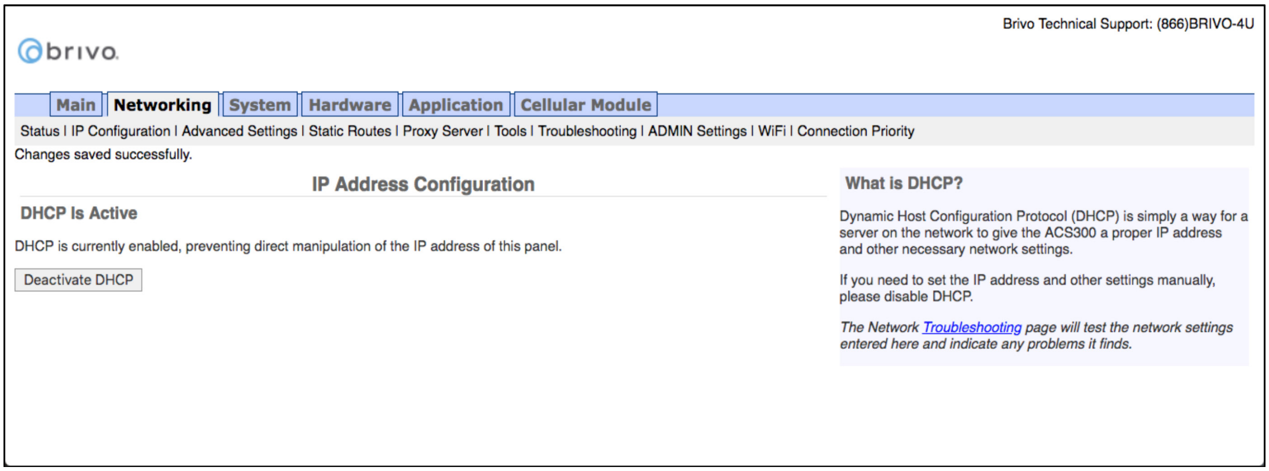
The Brivo control panel is shipped with DHCP enabled. This means that on most networks, the control panel will automatically acquire all the information it needs to communicate with Brivo. However, some networks may require custom settings, either by design or by policy. This section explains how to change network settings if you need to do so.

If you are uncertain whether the network requires manual configuration of networks settings, contact the network administrator at the site.

Deactivating DHCP

Before you can set network parameters manually, you must first deactivate DHCP.

1. Select the **Networking** tab. The Networking menu bar displays.
2. Select **IP Configuration**. The IP Address Configuration page displays.
3. Click **Deactivate DHCP**.



Brivo Technical Support: (866)BRIVO-4U

Main
Networking
System
Hardware
Application
Cellular Module
Status | IP Configuration | Advanced Settings | Static Routes | Proxy Server | Tools | Troubleshooting | ADMIN Settings | WiFi | Connection Priority

Changes saved successfully.

IP Address Configuration

DHCP Is Active

DHCP is currently enabled, preventing direct manipulation of the IP address of this panel.

What is DHCP?

Dynamic Host Configuration Protocol (DHCP) is simply a way for a server on the network to give the ACS300 a proper IP address and other necessary network settings.

If you need to set the IP address and other settings manually, please disable DHCP.

The Network Troubleshooting page will test the network settings entered here and indicate any problems it finds.

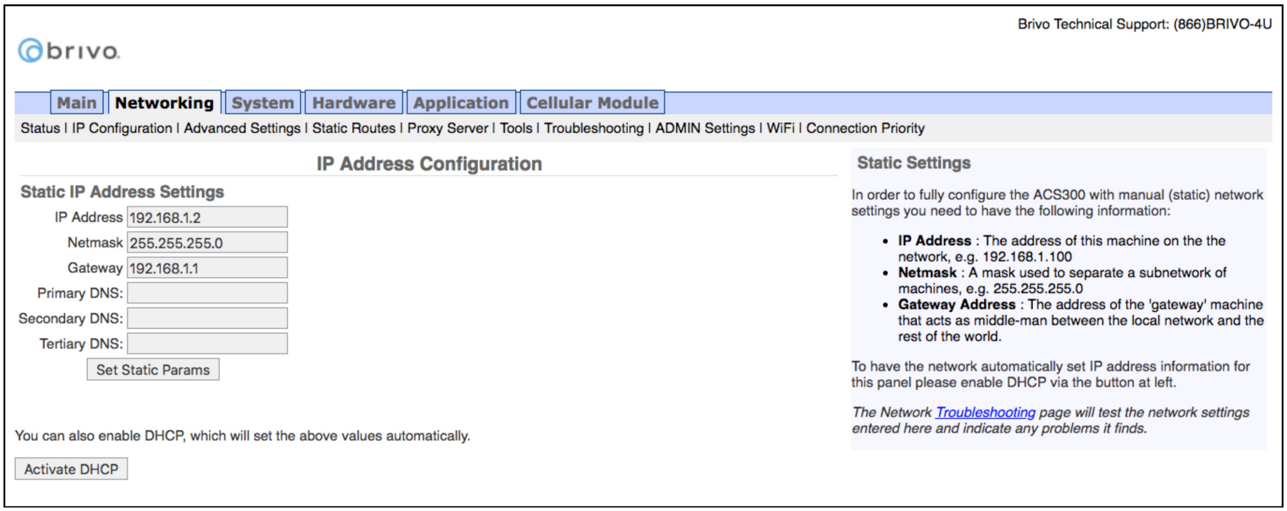
Figure 11: Deactivate DHCP

© 2021 Brivo Systems LLC. All rights reserved.

Entering Networking Parameters

Once DHCP is deactivated, you can enter IP configuration information on the IP Address Configuration page.

1. **IP Address**, **Netmask**, **Gateway**, and **Primary DNS** are required fields on this page.
2. **Secondary DNS** and **Tertiary DNS** are optional.
3. After entering the data, click **Set Static Params**.



brivo
Main
Networking
System
Hardware
Application
Cellular Module
Status | IP Configuration | Advanced Settings | Static Routes | Proxy Server | Tools | Troubleshooting | ADMIN Settings | WiFi | Connection Priority
Set Static Params
Activate DHCP

Brivo Technical Support: (866)BRIVO-4U

IP Address Configuration

Static IP Address Settings

IP Address 192.168.1.2

Netmask 255.255.255.0

Gateway 192.168.1.1

Primary DNS:

Secondary DNS:

Tertiary DNS:

You can also enable DHCP, which will set the above values automatically.

Static Settings

In order to fully configure the ACS300 with manual (static) network settings you need to have the following information:

- **IP Address** : The address of this machine on the the network, e.g. 192.168.1.100
- **Netmask** : A mask used to separate a subnetwork of machines, e.g. 255.255.255.0
- **Gateway Address** : The address of the 'gateway' machine that acts as middle-man between the local network and the rest of the world.

To have the network automatically set IP address information for this panel please enable DHCP via the button at left.

The Network Troubleshooting page will test the network settings entered here and indicate any problems it finds.

Figure 12: IP Address Configuration

NOTE: Incorrect parameters may prevent the control panel from communicating with the Brivo Cloud Server. Please confirm all settings with the LAN network administrator first.

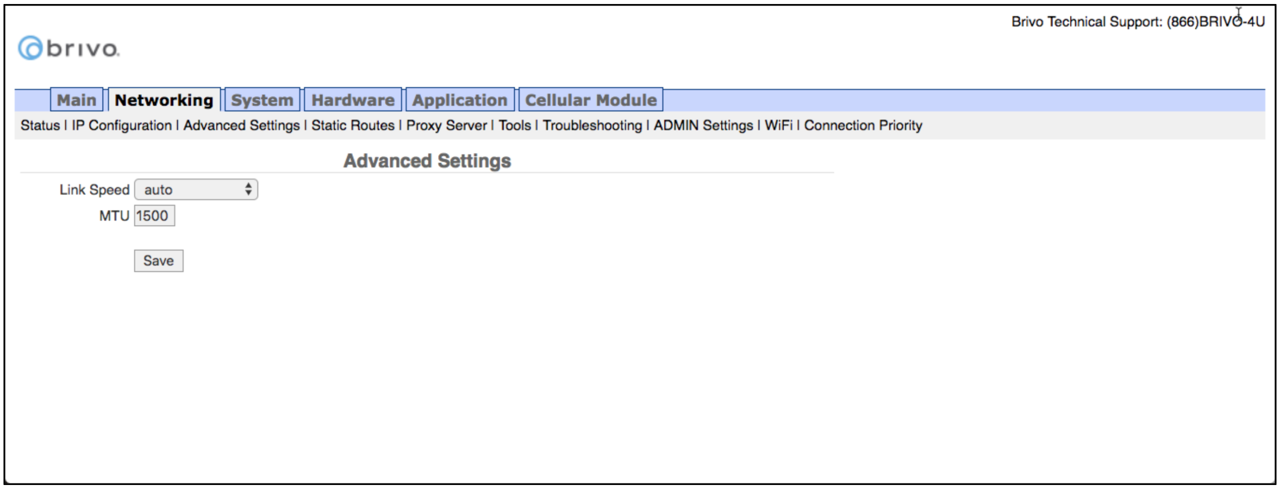
WARNING: LAN Port IP Address

The Admin port uses the IP address range 192.168.207.NNN; do NOT use this range on the LAN port. If you must use this IP range, first change the address of the ADMIN port to something other than 192.168.207.NNN. Do this BEFORE you connect the panel to the host network.

Advanced Settings

When configuring a network Link Speed, the Brivo control panel defaults to Auto when establishing a link speed between the panel and the network.

1. Click **Networking** to access the Networking menu bar.
2. Click **Advanced Settings** to access the Advanced Settings page.


Brivo Technical Support: (866)BRIVO-4U
brivo
Main | Networking | System | Hardware | Application | Cellular Module
Status | IP Configuration | Advanced Settings | Static Routes | Proxy Server | Tools | Troubleshooting | ADMIN Settings | WiFi | Connection Priority
Save

Advanced Settings

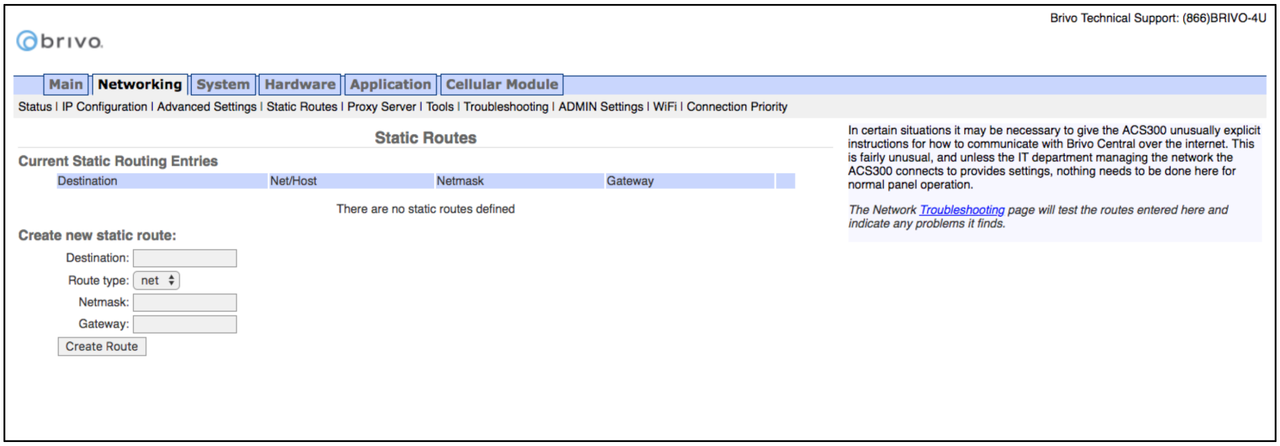
Link Speed: auto

MTU: 1500

Figure 13: Advanced Settings

Static Routes

Establishing static routes is rarely required and should be performed only with the advice of the network administrator for the site where the control panel is being installed.


Brivo Technical Support: (866)BRIVO-4U
brivo
Main | Networking | System | Hardware | Application | Cellular Module
Status | IP Configuration | Advanced Settings | Static Routes | Proxy Server | Tools | Troubleshooting | ADMIN Settings | WiFi | Connection Priority
Create Route

Static Routes

Current Static Routing Entries

Destination	Net/Host	Netmask	Gateway

There are no static routes defined

Create new static route:

Destination:

Route type: net

Netmask:

Gateway:

In certain situations it may be necessary to give the ACS300 unusually explicit instructions for how to communicate with Brivo Central over the internet. This is fairly unusual, and unless the IT department managing the network the ACS300 connects to provides settings, nothing needs to be done here for normal panel operation.

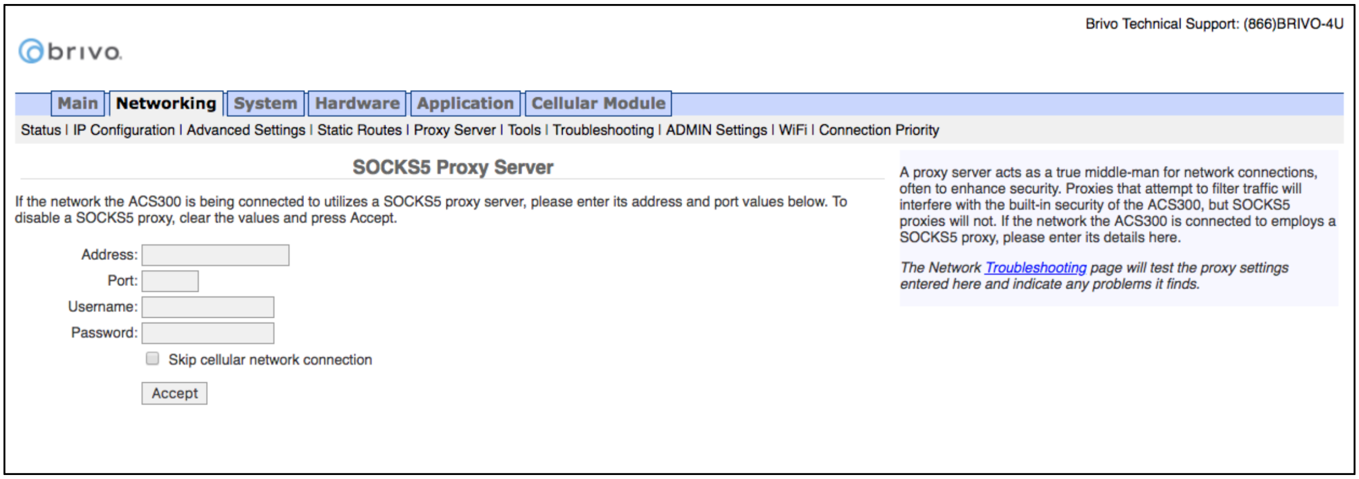
The Network Troubleshooting page will test the routes entered here and indicate any problems it finds.

Figure 14: Static Routes Configuration

Proxy Server

If your network uses a proxy server to control access to the internet, you will need to manually configure the proxy server settings. Before changing these settings, first work with the network administrator to determine valid values.

1. Click **Networking** to access the Networking menu bar.
2. Click **Proxy Server** to access the SOCKS5 Proxy Server page.



Brivo Technical Support: (866)BRIVO-4U
Main
Networking
System
Hardware
Application
Cellular Module
Status | IP Configuration | Advanced Settings | Static Routes | Proxy Server | Tools | Troubleshooting | ADMIN Settings | WiFi | Connection Priority
Accept

SOCKS5 Proxy Server

If the network the ACS300 is being connected to utilizes a SOCKS5 proxy server, please enter its address and port values below. To disable a SOCKS5 proxy, clear the values and press Accept.

Address:
Port:
Username:
Password:
□ Skip cellular network connection

A proxy server acts as a true middle-man for network connections, often to enhance security. Proxies that attempt to filter traffic will interfere with the built-in security of the ACS300, but SOCKS5 proxies will not. If the network the ACS300 is connected to employs a SOCKS5 proxy, please enter its details here.

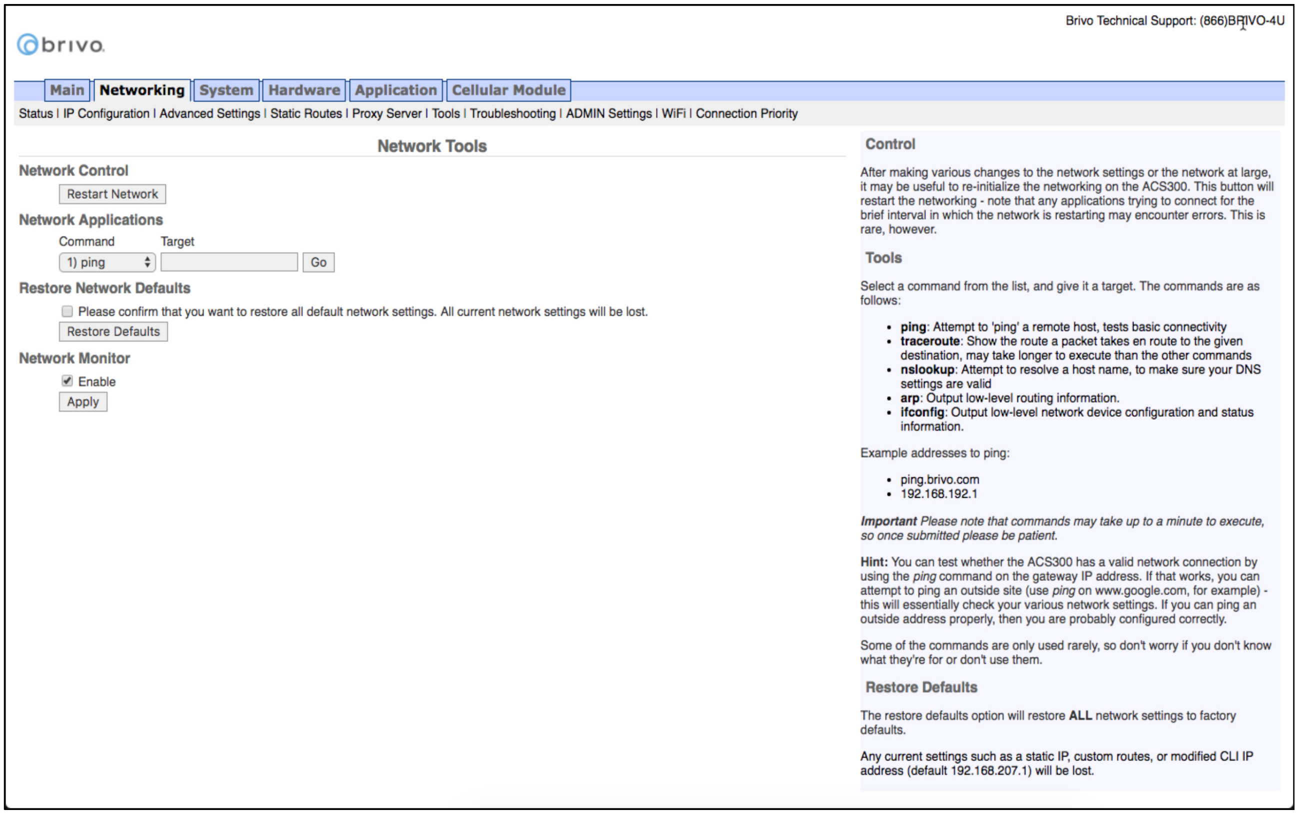
The Network Troubleshooting page will test the proxy settings entered here and indicate any problems it finds.

Figure 15: Proxy Server Configuration

Tools (Networking)

Diagnosing connectivity problems through use of the Network Tools page allows you to reinitialize the Brivo control panel networking setup or enter commands for diagnosing network connectivity problems. To access this page:

1. Click **Networking** to access the Networking menu bar.
2. Click **Tools** to access the Network Tools page.
3. If you want to reinitialize the Brivo control panel networking, click **Restart Network**.
4. To diagnose network connectivity problems, enter a valid **Command** and **Target**, then click **Go**. The system performs the specified command and displays the output. Descriptions of the valid commands are provided in the text on the right side of the page.


Brivo Technical Support: (866)BRIVO-4U
brivo
Main
Networking
System
Hardware
Application
Cellular Module
Status | IP Configuration | Advanced Settings | Static Routes | Proxy Server | Tools | Troubleshooting | ADMIN Settings | WiFi | Connection Priority
Restart Network
Go
Restore Defaults
Apply

Network Tools

Network Control

Network Applications

Command: 1) ping

Target:

Restore Network Defaults

□ Please confirm that you want to restore all default network settings. All current network settings will be lost.

Network Monitor

☑ Enable

Control

After making various changes to the network settings or the network at large, it may be useful to re-initialize the networking on the ACS300. This button will restart the networking - note that any applications trying to connect for the brief interval in which the network is restarting may encounter errors. This is rare, however.

Tools

Select a command from the list, and give it a target. The commands are as follows:

- **ping**: Attempt to 'ping' a remote host, tests basic connectivity
- **traceroute**: Show the route a packet takes en route to the given destination, may take longer to execute than the other commands
- **nslookup**: Attempt to resolve a host name, to make sure your DNS settings are valid
- **arp**: Output low-level routing information.
- **ifconfig**: Output low-level network device configuration and status information.

Example addresses to ping:

- ping.brivo.com
- 192.168.192.1

***Important** Please note that commands may take up to a minute to execute, so once submitted please be patient.*

Hint: You can test whether the ACS300 has a valid network connection by using the *ping* command on the gateway IP address. If that works, you can attempt to ping an outside site (use *ping* on www.google.com, for example) - this will essentially check your various network settings. If you can ping an outside address properly, then you are probably configured correctly.

Some of the commands are only used rarely, so don't worry if you don't know what they're for or don't use them.

Restore Defaults

The restore defaults option will restore **ALL** network settings to factory defaults.

Any current settings such as a static IP, custom routes, or modified CLI IP address (default 192.168.207.1) will be lost.

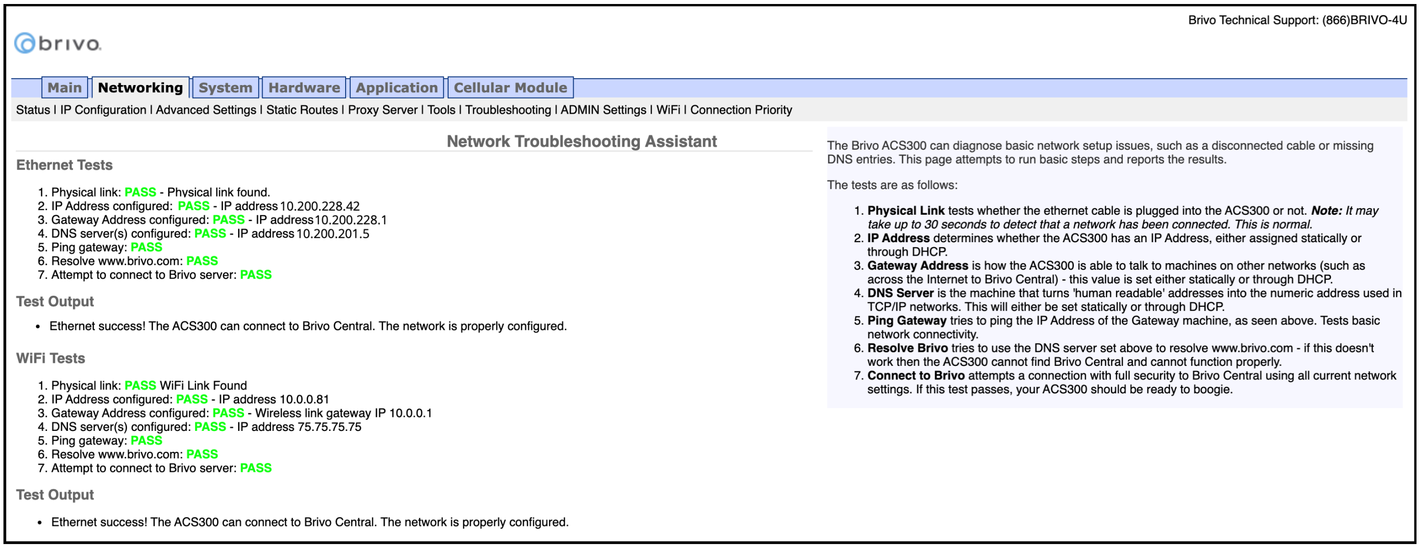
Figure 16: Network Tools

© 2021 Brivo Systems LLC. All rights reserved.

Troubleshooting

Troubleshooting network problems (for both -E or -A panel types) through the Administrative Interface uses a Network Troubleshooting assistant to determine if the Brivo control panel is connected to the local network and ultimately to the Brivo Cloud Server or Brivo Onsite Server. To access this tool:

1. Click **Networking** to access the Networking menu bar.
2. Click **Troubleshooting** to access the Network Troubleshooting Assistant.
3. If any one of the connectivity tests fails, a message displays describing the failure and offering suggestions for resolving it. Descriptions of the tests performed are provided in the text on the right side of the page.


Brivo Technical Support: (866)BRIVO-4U
brivo
Main
Networking
System
Hardware
Application
Cellular Module
Status | IP Configuration | Advanced Settings | Static Routes | Proxy Server | Tools | Troubleshooting | ADMIN Settings | WiFi | Connection Priority

Network Troubleshooting Assistant

Ethernet Tests

1. Physical link: **PASS** - Physical link found.
2. IP Address configured: **PASS** - IP address 10.200.228.42
3. Gateway Address configured: **PASS** - IP address 10.200.228.1
4. DNS server(s) configured: **PASS** - IP address 10.200.201.5
5. Ping gateway: **PASS**
6. Resolve www.brivo.com: **PASS**
7. Attempt to connect to Brivo server: **PASS**

Test Output

- Ethernet success! The ACS300 can connect to Brivo Central. The network is properly configured.

WiFi Tests

1. Physical link: **PASS** WiFi Link Found
2. IP Address configured: **PASS** - IP address 10.0.0.81
3. Gateway Address configured: **PASS** - Wireless link gateway IP 10.0.0.1
4. DNS server(s) configured: **PASS** - IP address 75.75.75.75
5. Ping gateway: **PASS**
6. Resolve www.brivo.com: **PASS**
7. Attempt to connect to Brivo server: **PASS**

Test Output

- Ethernet success! The ACS300 can connect to Brivo Central. The network is properly configured.

The Brivo ACS300 can diagnose basic network setup issues, such as a disconnected cable or missing DNS entries. This page attempts to run basic steps and reports the results.

The tests are as follows:

1. **Physical Link** tests whether the ethernet cable is plugged into the ACS300 or not. ***Note:*** *It may take up to 30 seconds to detect that a network has been connected. This is normal.*
2. **IP Address** determines whether the ACS300 has an IP Address, either assigned statically or through DHCP.
3. **Gateway Address** is how the ACS300 is able to talk to machines on other networks (such as across the Internet to Brivo Central) - this value is set either statically or through DHCP.
4. **DNS Server** is the machine that turns 'human readable' addresses into the numeric address used in TCP/IP networks. This will either be set statically or through DHCP.
5. **Ping Gateway** tries to ping the IP Address of the Gateway machine, as seen above. Tests basic network connectivity.
6. **Resolve Brivo** tries to use the DNS server set above to resolve www.brivo.com - if this doesn't work then the ACS300 cannot find Brivo Central and cannot function properly.
7. **Connect to Brivo** attempts a connection with full security to Brivo Central using all current network settings. If this test passes, your ACS300 should be ready to boogie.

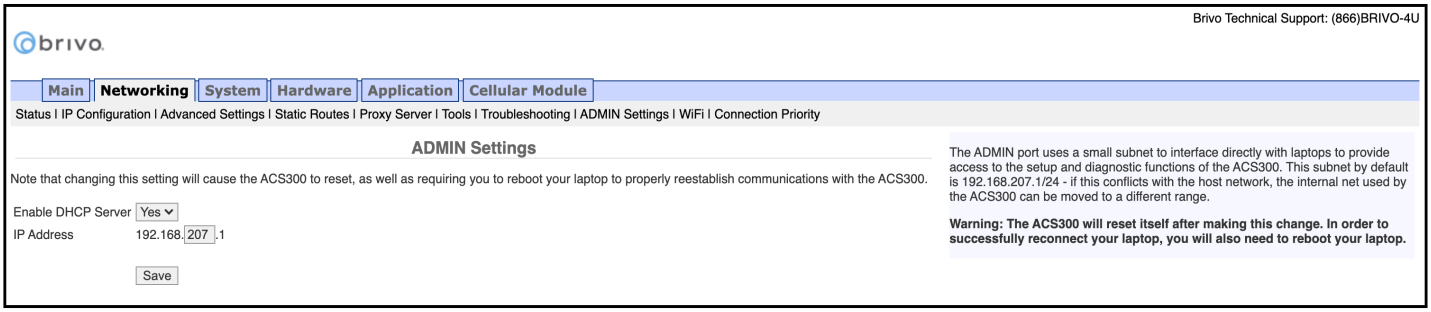
Figure 17: Network Troubleshooting Assistant

ADMIN Settings

The ADMIN port uses a small subnet to interface directly with laptops to provide access to the setup and diagnostic functions of the control panel. This subnet by default is 192.168.207.1 through 24. If this conflicts with the host network, the internal net used by the control panel can be moved to a different range.

WARNING: The control panel will reset itself after making this change. In order to successfully reconnect your laptop, you will also need to reboot your laptop.

1. Click **Networking** to access the Networking menu bar.
2. Click **ADMIN Settings** to access the settings page.
3. To enable or disable DHCP and/or change the IP address range, make the necessary changes and click **Save**. Details on this functionality is found on the right side of the page.


Brivo Technical Support: (866)BRIVO-4U
brivo
Main
Networking
System
Hardware
Application
Cellular Module
Status | IP Configuration | Advanced Settings | Static Routes | Proxy Server | Tools | Troubleshooting | ADMIN Settings | WiFi | Connection Priority
Save

ADMIN Settings

Note that changing this setting will cause the ACS300 to reset, as well as requiring you to reboot your laptop to properly reestablish communications with the ACS300.

Enable DHCP Server: Yes

IP Address: 192.168.207.1

The ADMIN port uses a small subnet to interface directly with laptops to provide access to the setup and diagnostic functions of the ACS300. This subnet by default is 192.168.207.1/24 - if this conflicts with the host network, the internal net used by the ACS300 can be moved to a different range.

Warning: The ACS300 will reset itself after making this change. In order to successfully reconnect your laptop, you will also need to reboot your laptop.

Figure 18: ADMIN Settings

© 2021 Brivo Systems LLC. All rights reserved.

WiFi (ACS6000 and ACS300 only)

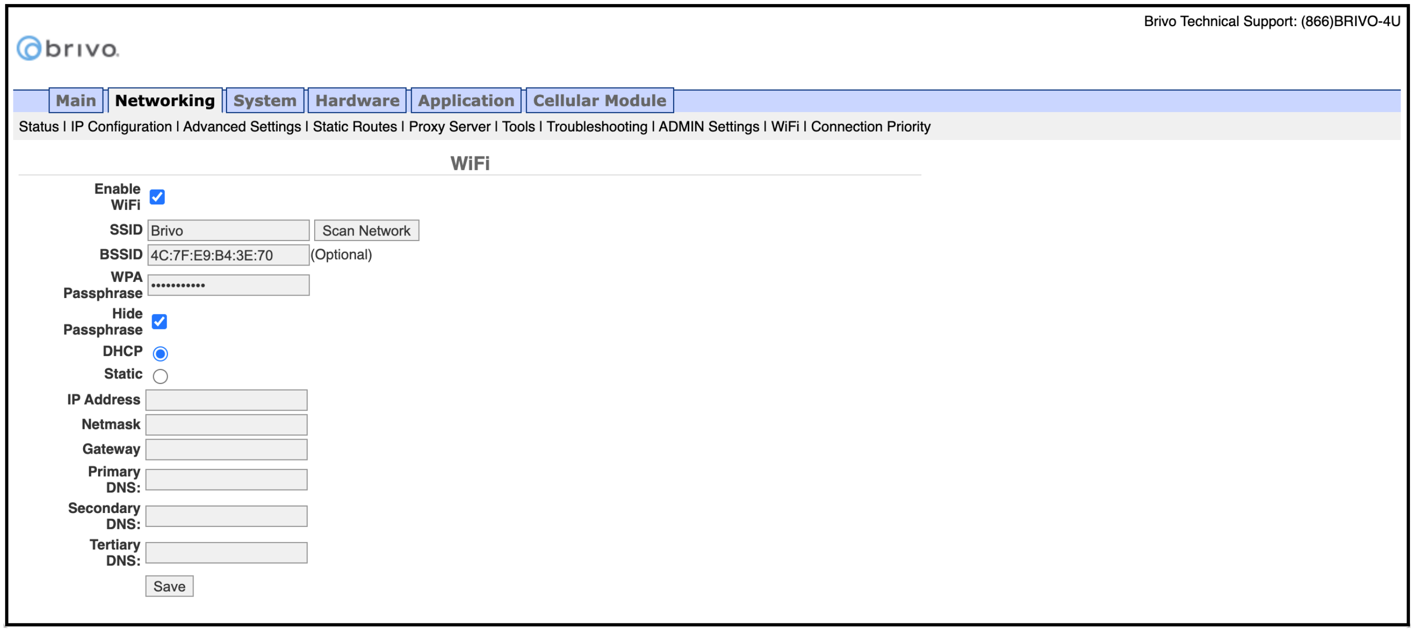
NOTE: For the **ACS6000**, to allow Wi-Fi functionality, Switch 7-8 MUST be in the Enabled position on the **ACS6000** control panel. Please refer to the **ACS6000** (A/E) Installation Manual (available at www.brivo.com) for instructions on configuration of the Wi-Fi hardware.

NOTE: For the **ACS300**, to allow Wi-Fi functionality, Switch 2-4 MUST be in the Enabled position on the **ACS300** control panel. Please refer to the **ACS300** Installation Manual (available at www.brivo.com) for instructions on configuration of the Wi-Fi hardware.

The **ACS6000** and **ACS300** have an internal Wi-Fi interface for communicating with either the Brivo Cloud Server or Brivo Onsite Server depending upon the panel type. Wi-Fi works in parallel with, or in replacement of, Ethernet functionality on the **ACS6000** and **ACS300** control panels. Wi-Fi can also function as a failover for Ethernet. If both Wi-Fi and Ethernet are enabled, the **ACS6000** and **ACS300** control panels will default to using the Ethernet connection.

The Administrative Interface includes a tab for configuring Wi-Fi network settings. To access this tool:

1. Click **Networking** to access the Networking menu bar.
2. Click **WiFi** to access the Wi-Fi settings page.
3. To configure **WiFi**, check the **Enable WiFi** checkbox.
4. Enter the **SSID** name of the wireless network to which the control panel will be connected.
5. Optionally, click the **Scan Network** button to scan for all available SSIDs which will provide a pop-up window with the available wireless networks. Click the **SSID** to which the control panel will be connected. You are returned to the **WiFi** page.
6. Optionally, enter the **BSSID** for the wireless network.
7. Enter the **WPA Passphrase** (Hide Passphrase is enabled by default).
8. Select **DHCP** or **Static** IP address. Please refer to the corresponding sections of this guide for instructions on configuration. If using **Static** IP selection, enter **IP address**, **Netmask**, **Gateway**, and **DNS** information.
9. Click **Save**.



Brivo Technical Support: (866)BRIVO-4U

brivo
Main
Networking
System
Hardware
Application
Cellular Module
Status I IP Configuration I Advanced Settings I Static Routes I Proxy Server I Tools I Troubleshooting I ADMIN Settings I WiFi I Connection Priority
Scan Network
Save

WiFi

Enable WiFi ☑

SSID Brivo

BSSID 4C:7F:E9:B4:3E:70 (Optional)

WPA Passphrase •••••••••••

Hide Passphrase ☑

DHCP ●

Static ○

IP Address

Netmask

Gateway

Primary DNS:

Secondary DNS:

Tertiary DNS:

Figure 19: WiFi

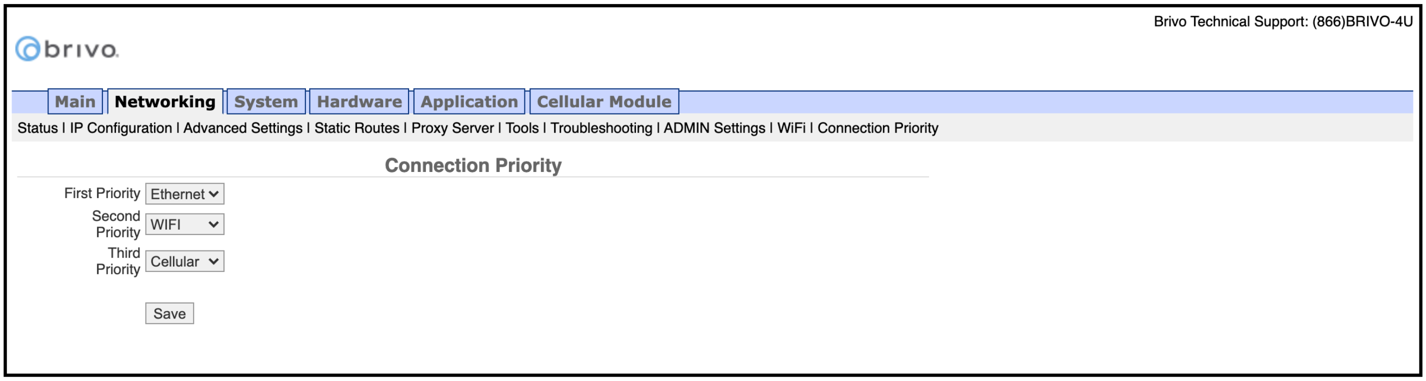
© 2021 Brivo Systems LLC. All rights reserved.

Connection Priority (ACS6000 and ACS300 only)

The **ACS6000** and **ACS300** allow for multiple connection methods to the Brivo Cloud Server or Brivo Onsite Server. The panel can connect via Ethernet, WiFi, or Cellular.

The Administrative Interface includes a tab for configuring the connection priority of the panel. To access this tool:

1. Click **Networking** to access the Networking menu bar.
2. Click **Connection Priority** to access the Connection Priority page.
3. To set the **First Priority**, select Ethernet, WiFi, or Cellular from the dropdown list.
4. Repeat this step for **Second Priority** and **Third Priority**. Do not choose the same connection type for more than one priority.
5. Click **Save**.


Brivo Technical Support: (866)BRIVO-4U
brivo
Main
Networking
System
Hardware
Application
Cellular Module
Status | IP Configuration | Advanced Settings | Static Routes | Proxy Server | Tools | Troubleshooting | ADMIN Settings | WiFi | Connection Priority
Save

Connection Priority

First Priority: Ethernet
Second Priority: WIFI
Third Priority: Cellular

Figure 20: Connection Priority

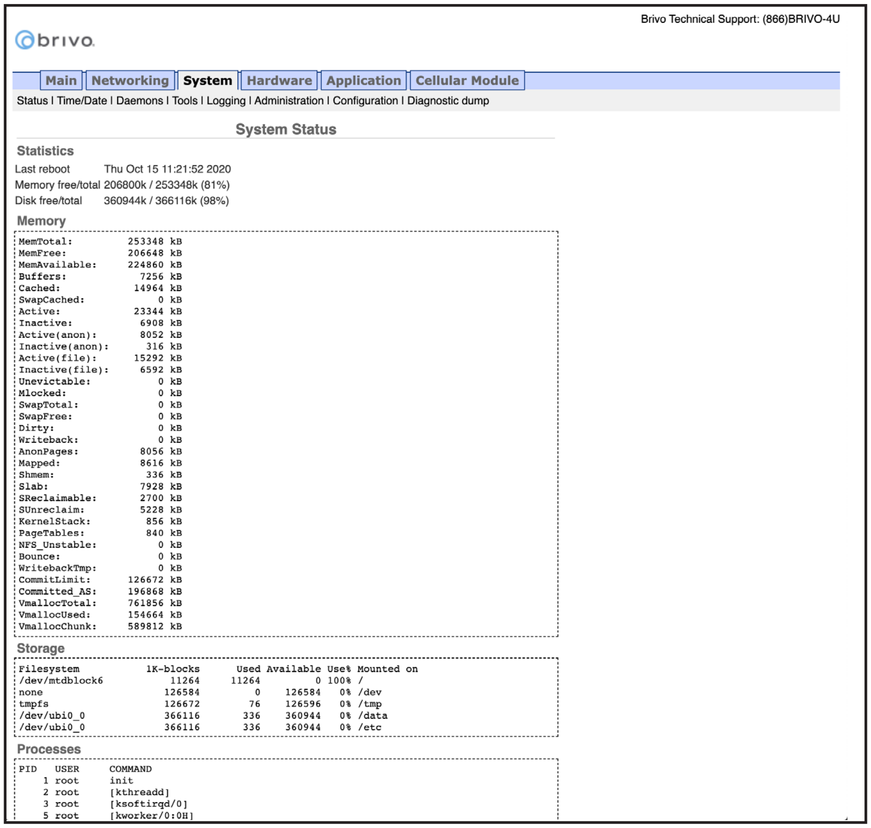
System Tab

WARNING: These tools are rarely required during normal operation of the panel and should be used only in conjunction with assistance from Brivo Technical Support.

Status

To view a status report of the performance and state of the control panel at the level of the operating system:

1. Click **System** to access the System menu bar.
2. Click **Status** to access the System Status page.


Brivo Technical Support: (866)BRIVO-4U
Main
Networking
System
Hardware
Application
Cellular Module
Status I Time/Date I Daemons I Tools I Logging I Administration I Configuration I Diagnostic dump

System Status

Statistics

Last reboot Thu Oct 15 11:21:52 2020
Memory free/total 206800k / 253348k (81%)
Disk free/total 360944k / 366116k (98%)

Memory

```
MemTotal:         253348 kB
MemFree:          206648 kB
MemAvailable:     224860 kB
Buffers:            7256 kB
Cached:            14964 kB
SwapCached:            0 kB
Active:            23344 kB
Inactive:           6908 kB
Active(anon):       8052 kB
Inactive(anon):      316 kB
Active(file):      15292 kB
Inactive(file):     6592 kB
Unevictable:           0 kB
Mlocked:               0 kB
SwapTotal:             0 kB
SwapFree:              0 kB
Dirty:                 0 kB
Writeback:             0 kB
AnonPages:          8056 kB
Mapped:             8616 kB
Shmem:               336 kB
Slab:               7928 kB
SReclaimable:       2700 kB
SUnreclaim:         5228 kB
KernelStack:         856 kB
PageTables:          840 kB
NFS_Unstable:          0 kB
Bounce:                0 kB
WritebackTmp:          0 kB
CommitLimit:      126672 kB
Committed_AS:     196868 kB
VmallocTotal:     761856 kB
VmallocUsed:      154664 kB
VmallocChunk:     589812 kB
```

Storage

```
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/mtdblock6           11264     11264         0 100% /
none                    126584         0    126584   0% /dev
tmpfs                   126672        76    126596   0% /tmp
/dev/ubi0_0             366116       336    360944   0% /data
/dev/ubi0_0             366116       336    360944   0% /etc
```

Processes

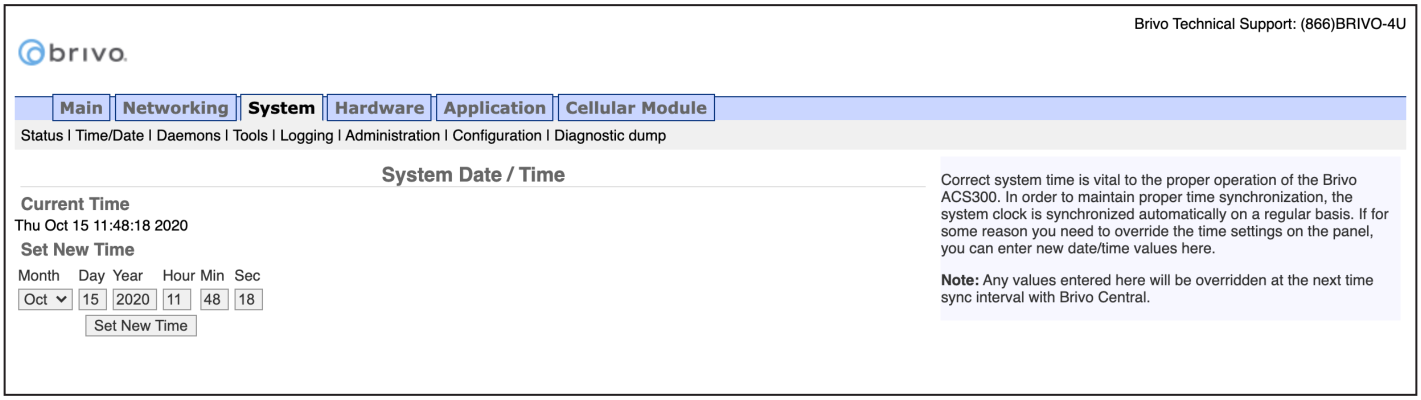
```
PID   USER     COMMAND
    1 root     init
    2 root     [kthreadd]
    3 root     [ksoftirqd/0]
    5 root     [kworker/0:0H]
```

Figure 21: System Status

Time/Date

To view or change the date and time settings in the control panel:

1. Click **System** to access the System menu bar.
2. Click **Time/Date** to access the System Date/Time page.



Brivo Technical Support: (866)BRIVO-4U
brivo
Main
Networking
System
Hardware
Application
Cellular Module
Status | Time/Date | Daemons | Tools | Logging | Administration | Configuration | Diagnostic dump

System Date / Time

Current Time

Thu Oct 15 11:48:18 2020

Set New Time

Month	Day	Year	Hour	Min	Sec
Oct	15	2020	11	48	18

Correct system time is vital to the proper operation of the Brivo ACS300. In order to maintain proper time synchronization, the system clock is synchronized automatically on a regular basis. If for some reason you need to override the time settings on the panel, you can enter new date/time values here.

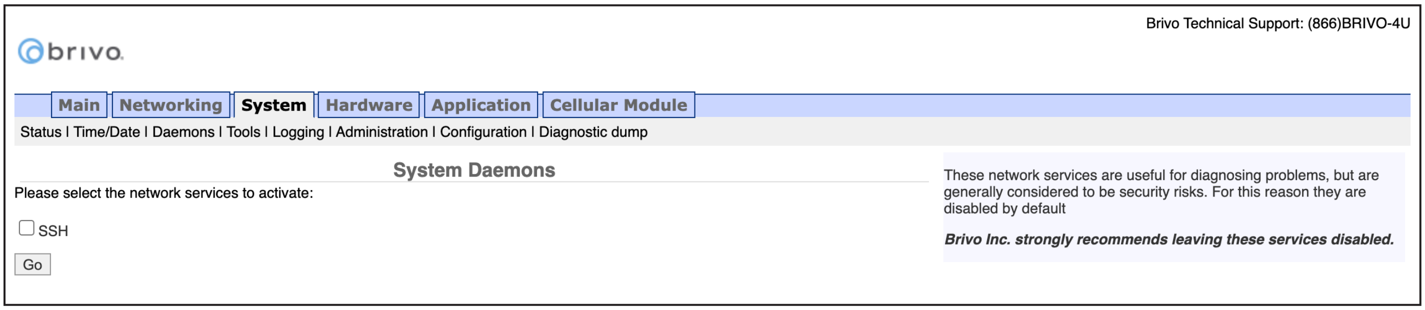
Note: Any values entered here will be overridden at the next time sync interval with Brivo Central.

Figure 22: System Date/Time

NOTE: A properly functioning control panel obtains its date and time information from the Brivo Cloud Server or Brivo Onsite Server. Setting the date and time manually should seldom be required, if ever.

Daemons

The Administrative Interface provides tools for enabling telnet access through the local interface only but is never used except for debugging purposes. This page should be accessed ONLY if requested by Brivo Technical Support.



Brivo Technical Support: (866)BRIVO-4U
brivo
Main
Networking
System
Hardware
Application
Cellular Module
Status | Time/Date | Daemons | Tools | Logging | Administration | Configuration | Diagnostic dump

System Daemons

Please select the network services to activate:

☐ SSH

These network services are useful for diagnosing problems, but are generally considered to be security risks. For this reason they are disabled by default

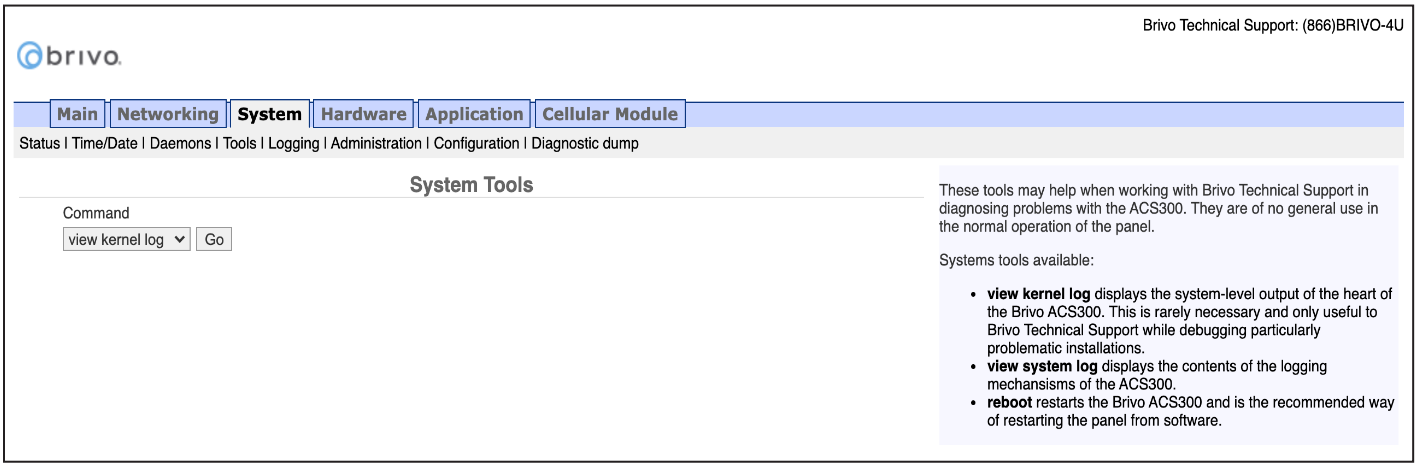
Brivo Inc. strongly recommends leaving these services disabled.

Figure 23: System Daemons

Tools (System)

The Administrative Interface provides access to low-level operations that are to be used only when troubleshooting a control panel with the assistance of Brivo Technical Support. If instructed to do so by Technical Support:

1. Click **System** to access the System menu bar.
2. Click **Tools** to access the System Tools page.



Brivo Technical Support: (866)BRIVO-4U

brivo
Main
Networking
System
Hardware
Application
Cellular Module
Status | Time/Date | Daemons | Tools | Logging | Administration | Configuration | Diagnostic dump
System Tools
Command
view kernel log
Go

These tools may help when working with Brivo Technical Support in diagnosing problems with the ACS300. They are of no general use in the normal operation of the panel.

Systems tools available:

- **view kernel log** displays the system-level output of the heart of the Brivo ACS300. This is rarely necessary and only useful to Brivo Technical Support while debugging particularly problematic installations.
- **view system log** displays the contents of the logging mechansisms of the ACS300.
- **reboot** restarts the Brivo ACS300 and is the recommended way of restarting the panel from software.

Figure 24: System Tools

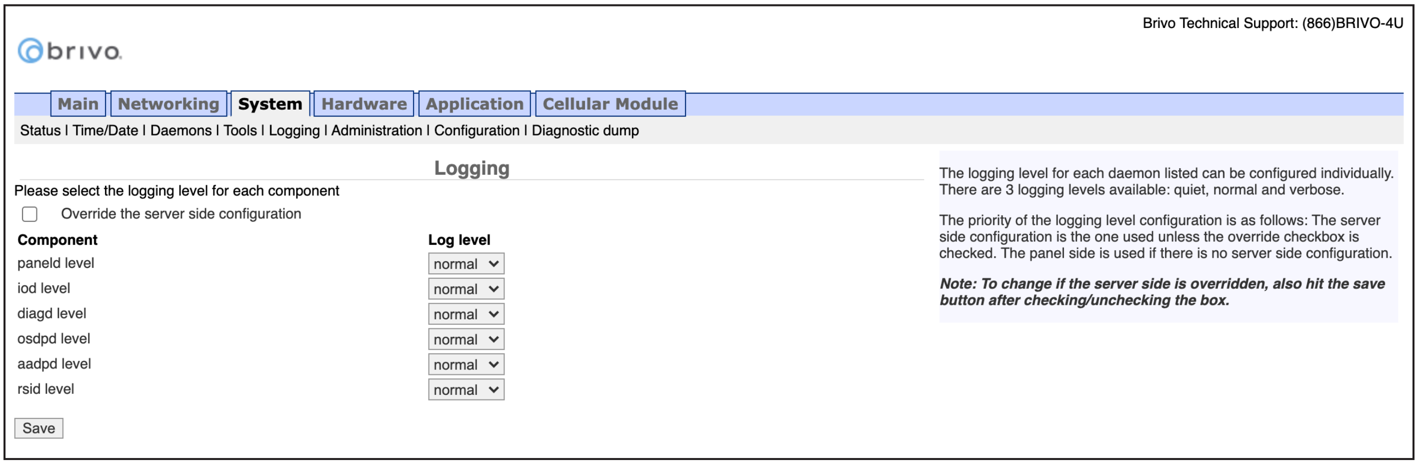
3. The three options from the **Command** dropdown menu are:
   a. **View Kernel Log** – this displays the system level output of the control panel. This is generally only useful to Brivo Technical Support.
   b. **View System Log** – this displays the contents of the various logging mechanisms in the control panel.
   c. **Reboot** – this restarts the control panel. This is the recommended method of restarting the panel from within the Administrative Interface. It is recommended that this function only be used if asked to by Brivo Technical Support.
4. Once you have selected your option, click the **Go** button.

© 2021 Brivo Systems LLC. All rights reserved.

Logging

The Administrative Interface allows the option to configure the level of logging for each daemon listed. By default, the levels are set on the server side, but may be overriden by checking the override checkbox and manually configured.

1. Click **System** to access the System menu bar.
2. Click **Logging** to access the System Tools page.



Brivo Technical Support: (866)BRIVO-4U

brivo
Main
Networking
System
Hardware
Application
Cellular Module
Status | Time/Date | Daemons | Tools | Logging | Administration | Configuration | Diagnostic dump

Logging

Please select the logging level for each component

□ Override the server side configuration

Component	Log level
paneld level	normal
iod level	normal
diagd level	normal
osdpd level	normal
aadpd level	normal
rsid level	normal

The logging level for each daemon listed can be configured individually. There are 3 logging levels available: quiet, normal and verbose.

The priority of the logging level configuration is as follows: The server side configuration is the one used unless the override checkbox is checked. The panel side is used if there is no server side configuration.

Note: To change if the server side is overridden, also hit the save button after checking/unchecking the box.

Figure 25: Logging

3. To change the log level, check the **Override the server side configuration** checkbox.
4. If desired, change the log level on each daemon from the dropdown list. The options are **Quiet**, **Normal**, and **Verbose**.
5. Once you are finished, click the **Save** button.

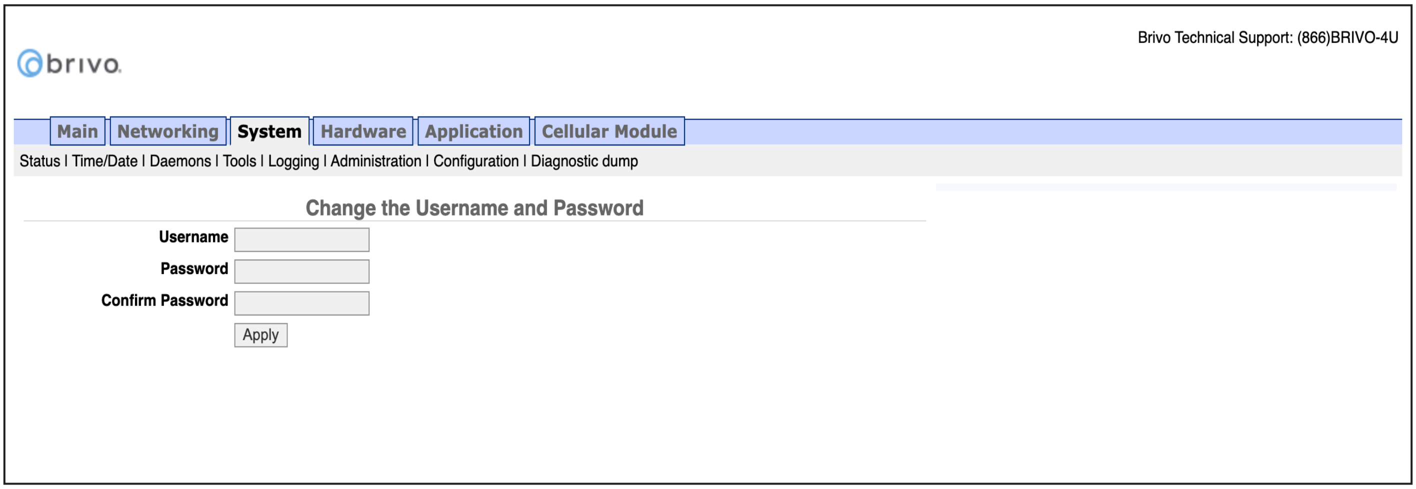
© 2021 Brivo Systems LLC. All rights reserved.

Administration

The Administrative Interface provides the administrator with the option to change the default Username and Password to the Administrative Interface. The default Username is **cli** and the default Password is **new5cli**.

IMPORTANT NOTE: Brivo strongly recommends that you change the default password when you first access the Administrative Interface.

1. Click **System** to access the System menu bar.
2. Click **Administration** to access the Change the Login Password page.
3. If desired, enter the new **Username**.
4. If desired, enter the new **Password**.
5. Enter the same Password in the **Confirm Password** field.
6. Click **Apply**.


Brivo Technical Support: (866)BRIVO-4U
brivo
Main
Networking
System
Hardware
Application
Cellular Module
Status I Time/Date I Daemons I Tools I Logging I Administration I Configuration I Diagnostic dump
Apply

Change the Username and Password

Username

Password

Confirm Password

Figure 26: Change the Username and Password

NOTE: New usernames and passwords must comply with the following rules:

- The minimum character length is six characters and the maximum character length is 1024 characters.
- All CAPS and the following non-alphanumeric characters are permitted:
  - ~`!@$%^&*()_+{}[]|\:;’”<,>.?/ (except # and space)

© 2021 Brivo Systems LLC. All rights reserved.

System Configuration (ACS6000 and ACS300 only)

The Administrative Interface allows an administrator to backup and/or restore the panel settings currently established on the control panel:

1. Click **System** to access the System menu bar.
2. Click **Configuration** to access the System Configuration page.

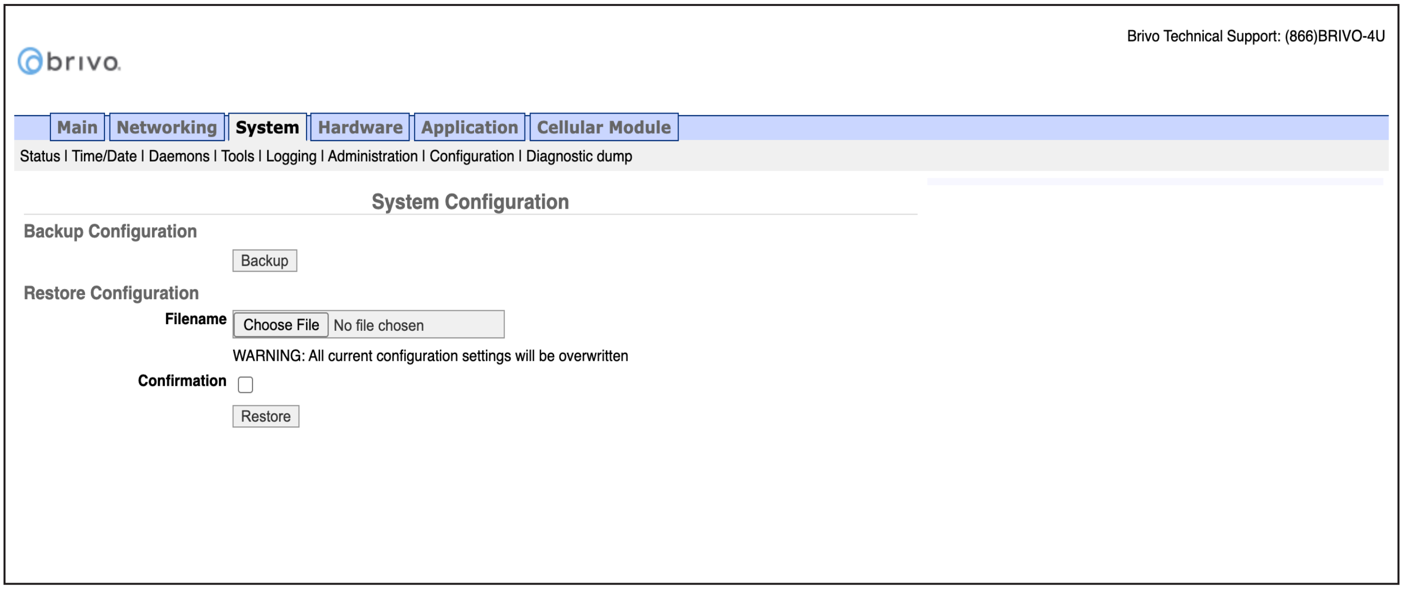

Brivo Technical Support: (866)BRIVO-4U
brivo
Main
Networking
System
Hardware
Application
Cellular Module
Status I Time/Date I Daemons I Tools I Logging I Administration I Configuration I Diagnostic dump
System Configuration
Backup Configuration
Backup
Restore Configuration
Filename
Choose File
No file chosen
WARNING: All current configuration settings will be overwritten
Confirmation
□
Restore

Figure 27: System Configuration

3. To back up the current panel settings, click on **Backup** to automatically backup current panel settings onto your local storage device. The file immediately and automatically saves to your local storage device.

NOTE: In order to use **Restore** in System Configuration, you MUST insert a USB drive into the USB Host port prior to performing this operation.

WARNING: System Restore - All current configuration settings will be overwritten when the System Restore functionality is used.

4. To restore the current panel settings, click on **Choose File** and select the backup file you wish to restore to the control panel. The restoration begins immediately and automatically. To receive a confirmation message that the process is complete, check the **Confirmation** checkbox prior to beginning the restore process.

Diagnostic Dump

The Diagnostic Dump functionality has no particular screen, but simply downloads a log file to the local storage device.

NOTE: It is generally recommended that the Diagnostic Dump functionality be used only at the request of Brivo Technical Support.

1. Click **System** to access the System menu bar.
2. Click **Diagnostic Dump** to begin the download.
3. Once the file is downloaded, the process is complete.

© 2021 Brivo Systems LLC. All rights reserved.

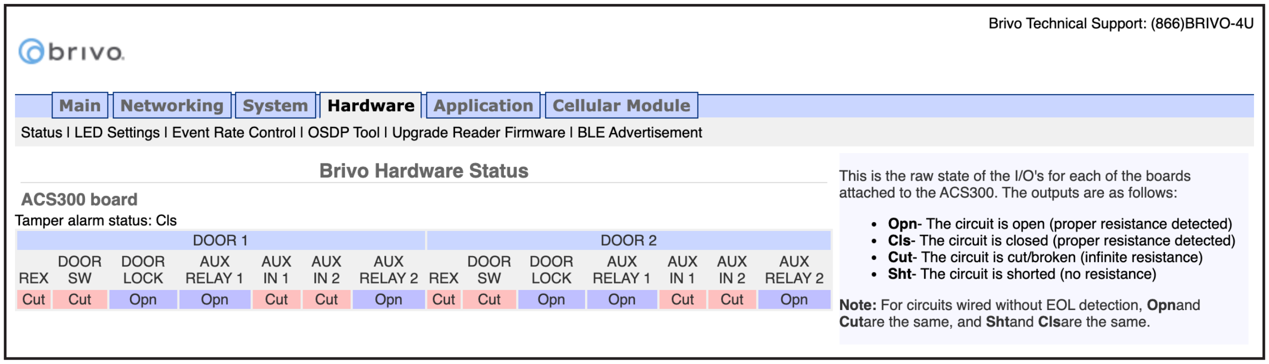
Hardware Tab

The Hardware tab of the Administrative Interface allows you to check the status of the control panel hardware, to change the LED settings for waiting state, to limit the number of notifications reported for certain events, to assign OSDP addressing to OSDP readers, and to upgrade firmware for OSDP readers.

Status

The Hardware Status page provides a complete view of the state of all major components of the control panel hardware. To access this page:

1. Click **Hardware** to access the Hardware menu bar.
2. Click **Status** to access the Brivo Hardware Status page. Status values are defined in the text on the right side of the page.


Brivo Technical Support: (866)BRIVO-4U
Main
Networking
System
Hardware
Application
Cellular Module
Status I LED Settings I Event Rate Control I OSDP Tool I Upgrade Reader Firmware I BLE Advertisement

Brivo Hardware Status

ACS300 board

Tamper alarm status: Cls

DOOR 1							DOOR 2						
REX	DOOR SW	DOOR LOCK	AUX RELAY 1	AUX IN 1	AUX IN 2	AUX RELAY 2	REX	DOOR SW	DOOR LOCK	AUX RELAY 1	AUX IN 1	AUX IN 2	AUX RELAY 2
Cut	Cut	Opn	Opn	Cut	Cut	Opn	Cut	Cut	Opn	Opn	Cut	Cut	Opn

This is the raw state of the I/O's for each of the boards attached to the ACS300. The outputs are as follows:

- **Opn**- The circuit is open (proper resistance detected)
- **Cls**- The circuit is closed (proper resistance detected)
- **Cut**- The circuit is cut/broken (infinite resistance)
- **Sht**- The circuit is shorted (no resistance)

Note: For circuits wired without EOL detection, **Opn**and **Cut**are the same, and **Sht**and **Cls**are the same.

Figure 28: Brivo Hardware Status

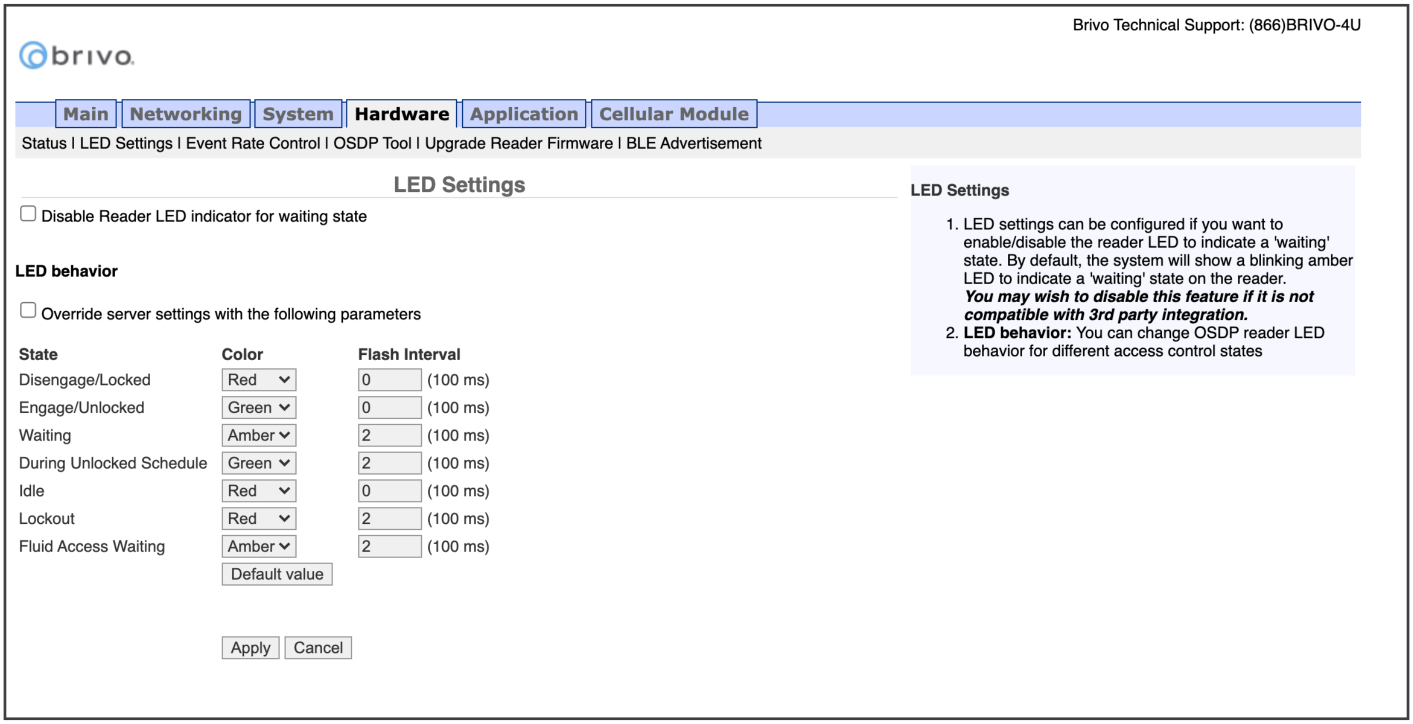
© 2021 Brivo Systems LLC. All rights reserved.

LED Settings

The LED Settings page allows the administrator to disable the Reader LED indicator for waiting state. LED settings can be configured if you want to enable/disable the reader LED to indicate a 'waiting' state. By default, the system will show a blinking amber LED to indicate a 'waiting' state on the reader. To access this page:

NOTE: You may wish to disable this feature if it is not compatible with 3rd party integration.

1. Click **Hardware** to access the Hardware menu bar.
2. Click **LED Settings** to access the LED Settings page.
3. Click the **Disable the Reader LED indicator for waiting state** checkbox if desired.
4. Click the **Override server settings with the following parameters** if you wish to change the OSDP reader LED behavior for various access control states.
5. Click **Apply** to complete the process.


Brivo Technical Support: (866)BRIVO-4U
brivo
Main | Networking | System | Hardware | Application | Cellular Module
Status I LED Settings I Event Rate Control I OSDP Tool I Upgrade Reader Firmware I BLE Advertisement

LED Settings

□ Disable Reader LED indicator for waiting state

LED behavior

□ Override server settings with the following parameters

State	Color	Flash Interval
Disengage/Locked	Red	0 (100 ms)
Engage/Unlocked	Green	0 (100 ms)
Waiting	Amber	2 (100 ms)
During Unlocked Schedule	Green	2 (100 ms)
Idle	Red	0 (100 ms)
Lockout	Red	2 (100 ms)
Fluid Access Waiting	Amber	2 (100 ms)

Default value
Apply
Cancel

LED Settings

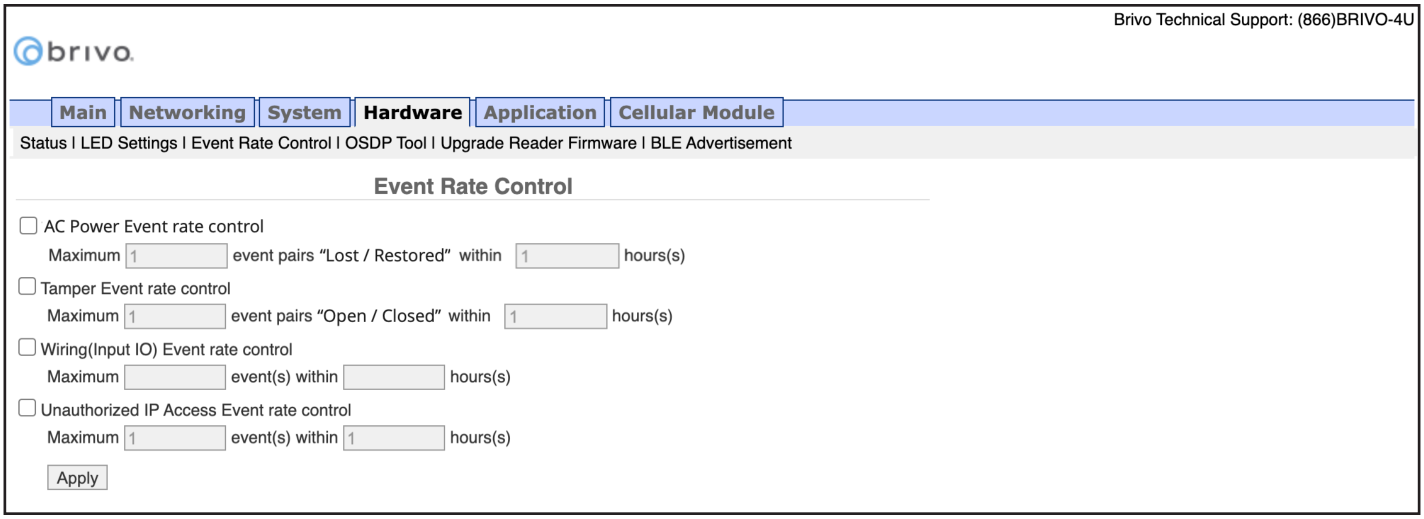
1. LED settings can be configured if you want to enable/disable the reader LED to indicate a 'waiting' state. By default, the system will show a blinking amber LED to indicate a 'waiting' state on the reader. ***You may wish to disable this feature if it is not compatible with 3rd party integration.***
2. **LED behavior:** You can change OSDP reader LED behavior for different access control states

Figure 29: LED Settings

Event Rate Control

The Event Rate Control page allows the administrator to limit the number of notifications reported for AC Power events, Tamper events, Wiring (Input/Output) events, and Unauthorized IP Access Events within a defined period of time.

1. Click **Hardware** to access the Hardware menu bar.
2. Click **Event Rate Control** to access the Event Rate Control page.
3. To limit AC Power event notifications, check the **AC Power Event** rate control checkbox.
4. Enter the maximum number of event pairs (Lost/Restored) and the number of hours (the default for each is one).
5. To limit Tamper event notifications, check the **Tamper Event** rate control checkbox.
6. Enter the maximum number of event pairs (Open/Closed) and the number of hours (the default for each is one).
7. To limit Wiring (Input/Output) event notifications, check the **Wiring (Input IO) Event** rate control checkbox.
8. Enter the maximum number of event(s) and the number of hours (the default for each is one).
9. To limit Unauthorized IP Access Event notifications, check the **Unauthorized IP Access Event** rate control checkbox.
10. Enter the maximum number of event(s) and the number of hours (the default for each is one).
11. Click **Apply** to complete the process.


Brivo Technical Support: (866)BRIVO-4U
brivo
Main
Networking
System
Hardware
Application
Cellular Module
Status I LED Settings I Event Rate Control I OSDP Tool I Upgrade Reader Firmware I BLE Advertisement

Event Rate Control

□ AC Power Event rate control

Maximum 1 event pairs "Lost / Restored" within 1 hours(s)

□ Tamper Event rate control

Maximum 1 event pairs "Open / Closed" within 1 hours(s)

□ Wiring(Input IO) Event rate control

Maximum event(s) within hours(s)

□ Unauthorized IP Access Event rate control

Maximum 1 event(s) within 1 hours(s)

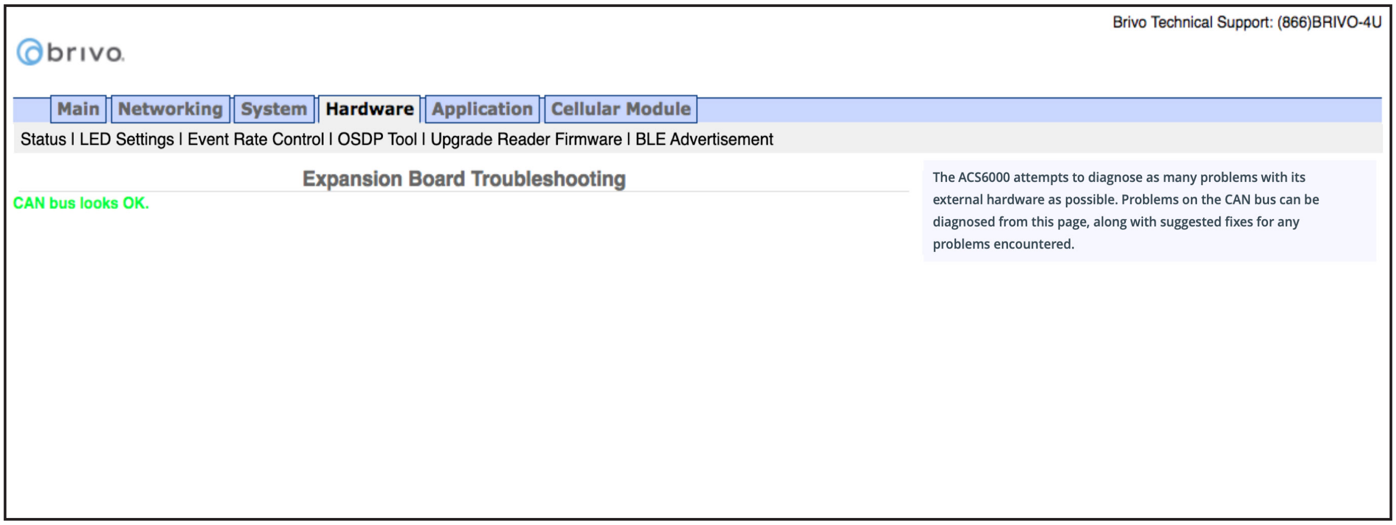
Apply

Figure 30: Event Rate Control

Troubleshooting (Hardware) (ACS5000 and ACS6000 only)

The Hardware Troubleshooting page provides a view of any hardware error conditions that the control panel is able to detect through self-diagnostics. To access this page:

1. Click **Hardware** to access the Hardware menu bar.
2. Click **Troubleshooting** to access the Hardware Troubleshooting page.



Brivo Technical Support: (866)BRIVO-4U
Main
Networking
System
Hardware
Application
Cellular Module
Status I LED Settings I Event Rate Control I OSDP Tool I Upgrade Reader Firmware I BLE Advertisement

Expansion Board Troubleshooting

CAN bus looks OK.

The ACS6000 attempts to diagnose as many problems with its external hardware as possible. Problems on the CAN bus can be diagnosed from this page, along with suggested fixes for any problems encountered.

Figure 31: Expansion Board Troubleshooting

© 2021 Brivo Systems LLC. All rights reserved.

OSDP Tool (ACS6000 and ACS300 only)

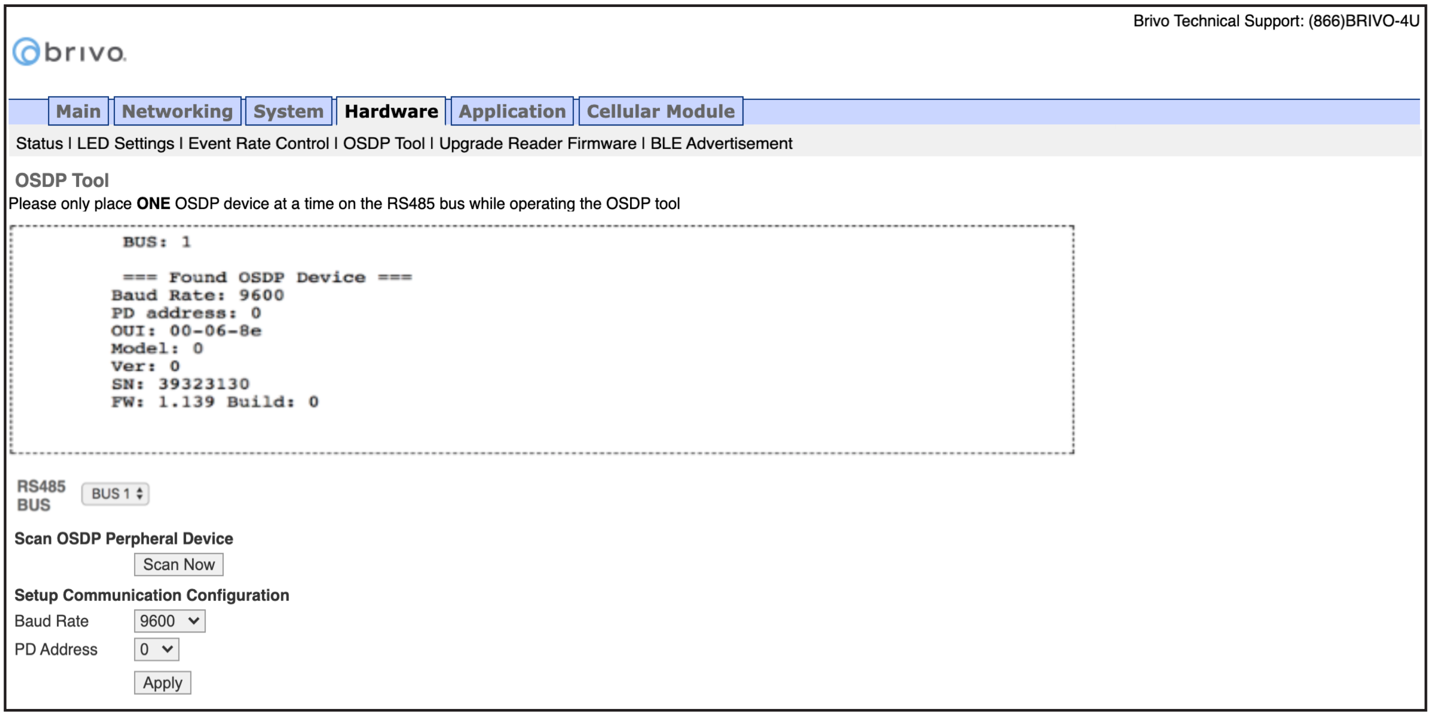
The OSDP Tool page allows the administrator to scan for OSDP peripheral devices attached to the control panel and to set up communication configurations including Baud Rate and Peripheral Device (PD) addressing.

NOTE: Place ONLY ONE OSDP device at a time on the RS485 bus while operating the OSDP tool.

To access this page:

1. Click **Hardware** to access the Hardware menu bar.
2. Click **OSDP Tool** to access the OSDP Tool page.
3. Select the RS485 Bus (**BUS 1** or **BUS 2**) from the dropdown list. **BUS 2** is only available on **ACS6000** control panels.
4. Click **Scan** to discover peripheral devices attached to the RS485 bus. When successful, the scan results will appear on the OSDP Tool page.
5. Choose the **Baud Rate** of the peripheral device from the Baud Rate dropdown list (the default is 9600).
6. Select the **PD Address** for the peripheral device from the available dropdown list. This choice assigns the selected PD Address to the peripheral device permanently once you click **Apply** below.
7. Click **Apply** to apply the PD address to the device and complete the process. Once a PD address number has been applied, it is no longer available for other peripheral devices.

NOTE: Once an OSDP reader has been addressed using the OSDP Tool, it is required that the OSDP address match the OSDP address assigned to the reader in Brivo Access or Brivo Onsite Server. If the OSDP addresses do not match, the OSDP reader will not function properly.


Brivo Technical Support: (866)BRIVO-4U
brivo
Main
Networking
System
Hardware
Application
Cellular Module
Status I LED Settings I Event Rate Control I OSDP Tool I Upgrade Reader Firmware I BLE Advertisement

OSDP Tool

Please only place **ONE** OSDP device at a time on the RS485 bus while operating the OSDP tool

```
   BUS: 1

   === Found OSDP Device ===
  Baud Rate: 9600
  PD address: 0
  OUI: 00-06-8e
  Model: 0
  Ver: 0
  SN: 39323130
  FW: 1.139 Build: 0
```

RS485 BUS: BUS 1

Scan OSDP Perpheral Device

Setup Communication Configuration

Baud Rate: 9600

PD Address: 0

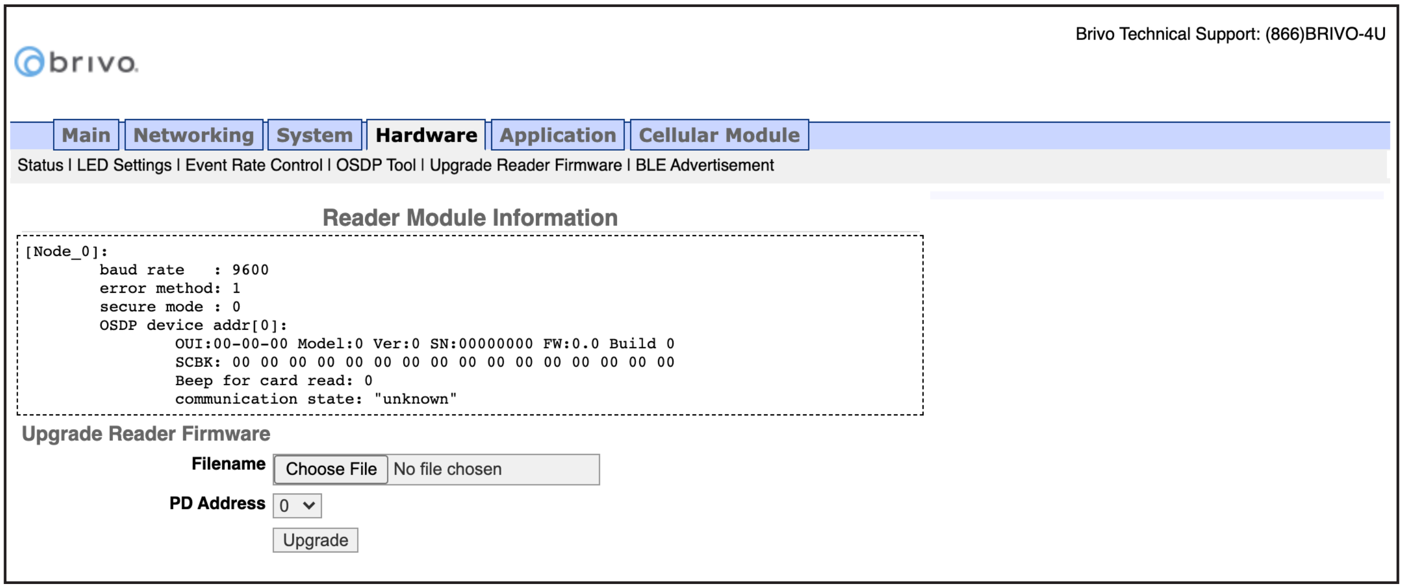
Figure 32: OSDP Tool

Upgrade Reader Firmware (ACS6000 and ACS300 only)

The Upgrade Reader Firmware page allows the administrator to upgrade the firmware for OSDP peripheral devices attached to the control panel. To access this page:

NOTE: The firmware upgrade file will ONLY be sent by Brivo to the administrator. Do not use any other firmware upgrades files provided from other sources.

1. Click **Hardware** to access the Hardware menu bar.
2. Click **Upgrade Reader Firmware** to access the Reader Module Information page.
3. To upgrade the firmware of a reader, click on **Choose File** and select the firmware upgrade file you wish to use from your local storage device. Select the appropriate **PD Address** from the dropdown menu and then click the **Upgrade** button to begin the firmware upgrade process.


brivo
Main
Networking
System
Hardware
Application
Cellular Module
Status | LED Settings | Event Rate Control | OSDP Tool | Upgrade Reader Firmware | BLE Advertisement
Choose File
Upgrade

Brivo Technical Support: (866)BRIVO-4U

Reader Module Information

```
[Node_0]:
        baud rate    : 9600
        error method: 1
        secure mode : 0
        OSDP device addr[0]:
                OUI:00-00-00 Model:0 Ver:0 SN:00000000 FW:0.0 Build 0
                SCBK: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                Beep for card read: 0
                communication state: "unknown"
```

Upgrade Reader Firmware

Filename: No file chosen

PD Address: 0

Figure 33: Upgrade Reader Firmware

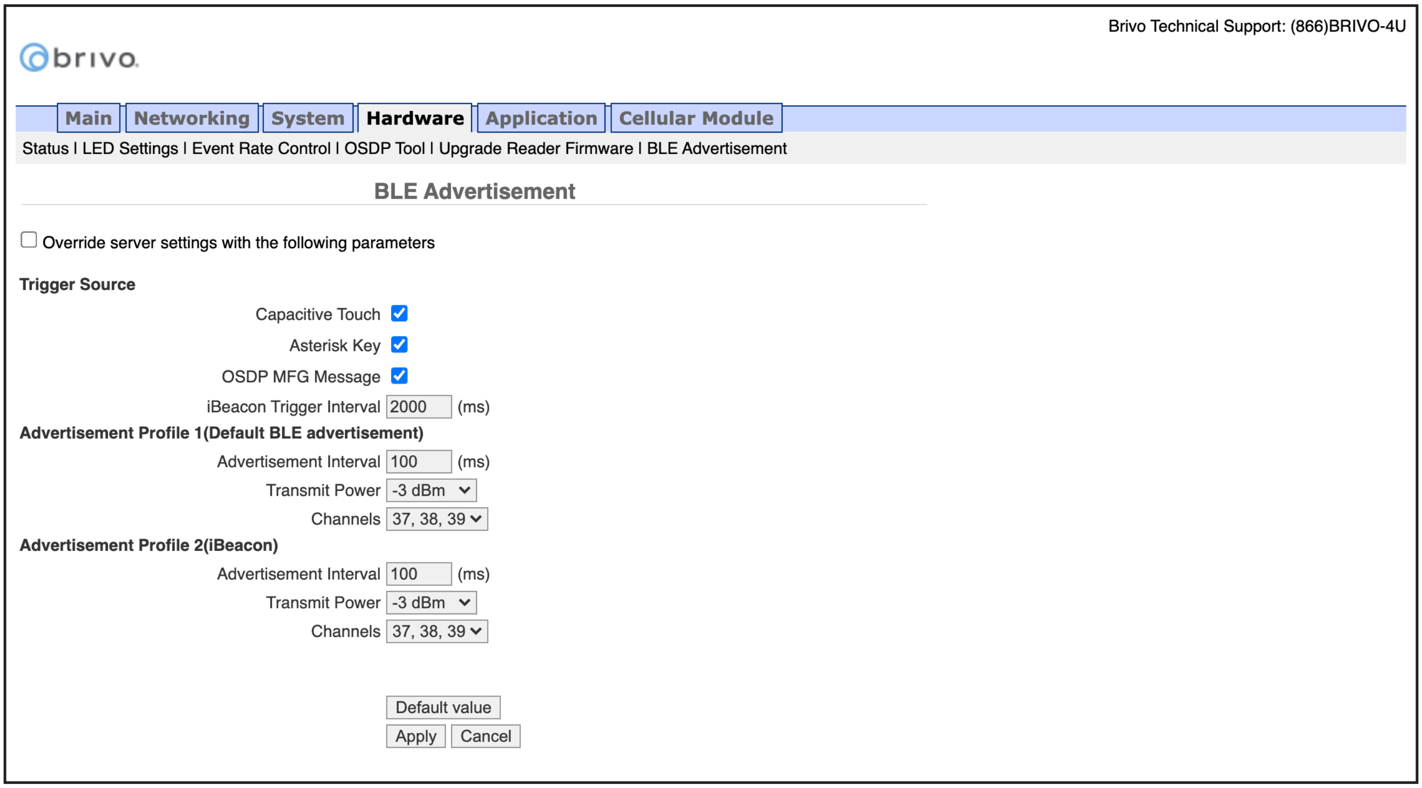
BLE Advertisement (ACS6000 and ACS300 only)

The BLE Advertisement page allows the administrator to manage fluid access and mobile credential functionality for Brivo Smart Readers and how the units are used by credential holders.

To access this page:

1. Click **Hardware** to access the Hardware menu bar.
2. Click **BLE Advertisement** to access the BLE Advertisement page.
3. To disable Fluid Access by touch functionality, make sure the **Capacitive Touch** checkbox is unchecked.
4. To disable Fluid Access by pressing the * key, make sure the **Asterisk Key** checkbox is unchecked.
5. If mobile credential devices are not being detected in a pocket or purse, increase the **Transmit Power** DB value.
6. If mobile credential holders are experiencing interference from other Brivo Smart Readers, decrease the **Transmit Power** DB value.
7. Click **Apply** when finished.

NOTE: Other than the options listed above, other changes to this page should be made ONLY if requested by Brivo Technical Support.


Brivo Technical Support: (866)BRIVO-4U
Main
Networking
System
Hardware
Application
Cellular Module
Status I LED Settings I Event Rate Control I OSDP Tool I Upgrade Reader Firmware I BLE Advertisement

BLE Advertisement

□ Override server settings with the following parameters

Trigger Source

Capacitive Touch ☑

Asterisk Key ☑

OSDP MFG Message ☑

iBeacon Trigger Interval 2000 (ms)

Advertisement Profile 1(Default BLE advertisement)

Advertisement Interval 100 (ms)

Transmit Power -3 dBm

Channels 37, 38, 39

Advertisement Profile 2(iBeacon)

Advertisement Interval 100 (ms)

Transmit Power -3 dBm

Channels 37, 38, 39

Figure 34: BLE Advertisement

Application Tab

The Application tab of the Administrative Interface gives you access to log of control panel events, the ability to activate Office Mode for Allegion LE wireless locks, and a set of tools used for diagnosing control panel problems.

Log

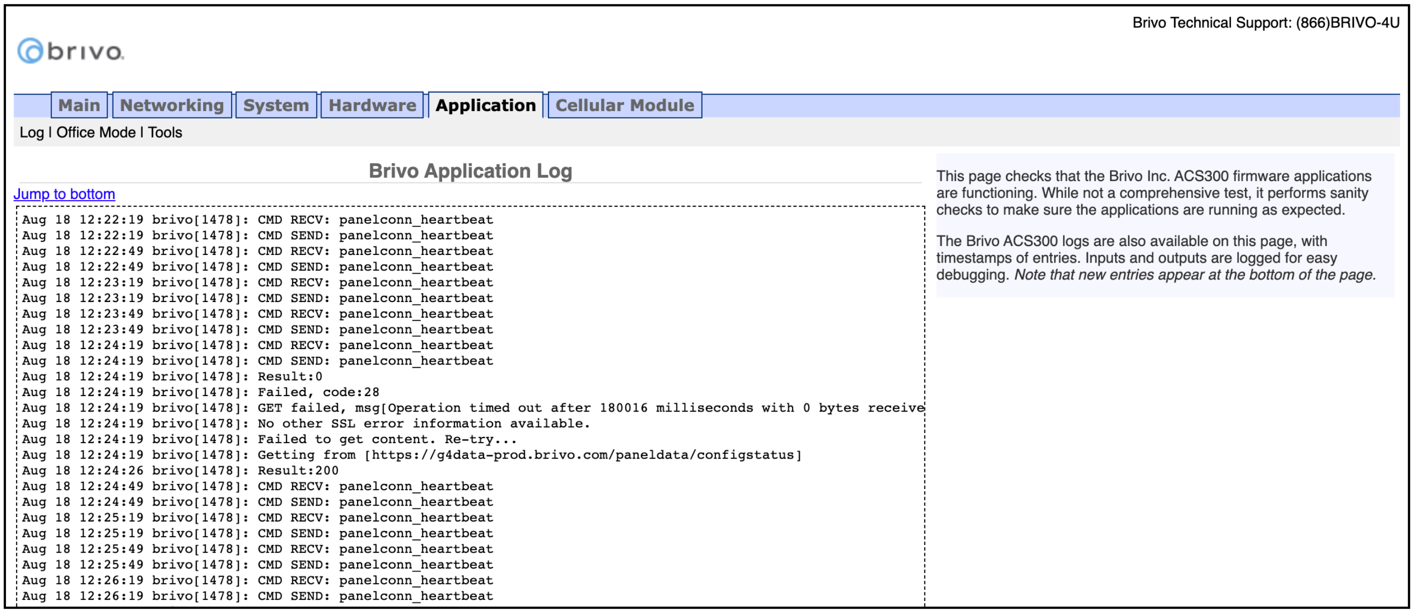
The Application Log contains an entry for every major event that occurs in the control panel. For example, it can answer such questions as:

Did the control panel receive a Wiegand value from the card reader?

Did the control panel detect the door closure switch change of state?

To access this page:

1. Click **Application** to access the Application menu bar.
2. Click **Log** to view the Brivo Application Log.



Brivo Application Log

```
Aug 18 12:22:19 brivo[1478]: CMD RECV: panelconn_heartbeat
Aug 18 12:22:19 brivo[1478]: CMD SEND: panelconn_heartbeat
Aug 18 12:22:49 brivo[1478]: CMD RECV: panelconn_heartbeat
Aug 18 12:22:49 brivo[1478]: CMD SEND: panelconn_heartbeat
Aug 18 12:23:19 brivo[1478]: CMD RECV: panelconn_heartbeat
Aug 18 12:23:19 brivo[1478]: CMD SEND: panelconn_heartbeat
Aug 18 12:23:49 brivo[1478]: CMD RECV: panelconn_heartbeat
Aug 18 12:23:49 brivo[1478]: CMD SEND: panelconn_heartbeat
Aug 18 12:24:19 brivo[1478]: CMD RECV: panelconn_heartbeat
Aug 18 12:24:19 brivo[1478]: CMD SEND: panelconn_heartbeat
Aug 18 12:24:19 brivo[1478]: Result:0
Aug 18 12:24:19 brivo[1478]: Failed, code:28
Aug 18 12:24:19 brivo[1478]: GET failed, msg[Operation timed out after 180016 milliseconds with 0 bytes receive
Aug 18 12:24:19 brivo[1478]: No other SSL error information available.
Aug 18 12:24:19 brivo[1478]: Failed to get content. Re-try...
Aug 18 12:24:19 brivo[1478]: Getting from [https://g4data-prod.brivo.com/paneldata/configstatus]
Aug 18 12:24:26 brivo[1478]: Result:200
Aug 18 12:24:49 brivo[1478]: CMD RECV: panelconn_heartbeat
Aug 18 12:24:49 brivo[1478]: CMD SEND: panelconn_heartbeat
Aug 18 12:25:19 brivo[1478]: CMD RECV: panelconn_heartbeat
Aug 18 12:25:19 brivo[1478]: CMD SEND: panelconn_heartbeat
Aug 18 12:25:49 brivo[1478]: CMD RECV: panelconn_heartbeat
Aug 18 12:25:49 brivo[1478]: CMD SEND: panelconn_heartbeat
Aug 18 12:26:19 brivo[1478]: CMD RECV: panelconn_heartbeat
Aug 18 12:26:19 brivo[1478]: CMD SEND: panelconn_heartbeat
```

This page checks that the Brivo Inc. ACS300 firmware applications are functioning. While not a comprehensive test, it performs sanity checks to make sure the applications are running as expected.

The Brivo ACS300 logs are also available on this page, with timestamps of entries. Inputs and outputs are logged for easy debugging. *Note that new entries appear at the bottom of the page.*

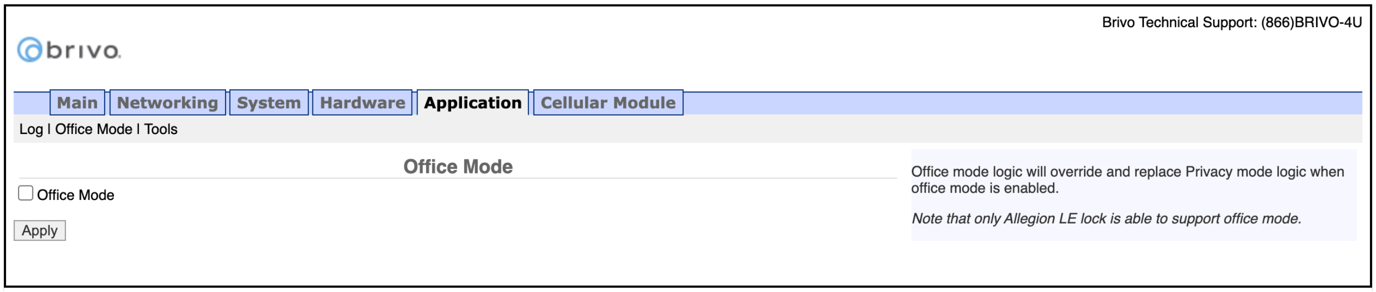
Figure 35: Brivo Application Log

Office Mode

The Office Mode page allows the administrator to activate Office Mode. Office Mode logic will override and replace Privacy mode logic when office mode is enabled.

NOTE: ONLY Allegion LE wireless locks are able to support Office Mode.

1. Click **Application** to access the Application menu bar.
2. Click **Office Mode** to view the Office Mode page.
3. To enable **Office Mode**, click the **Office Mode** checkbox.
4. To complete the process, click **Apply**.



Brivo Technical Support: (866)BRIVO-4U

Office Mode

☐ Office Mode

Office mode logic will override and replace Privacy mode logic when office mode is enabled.

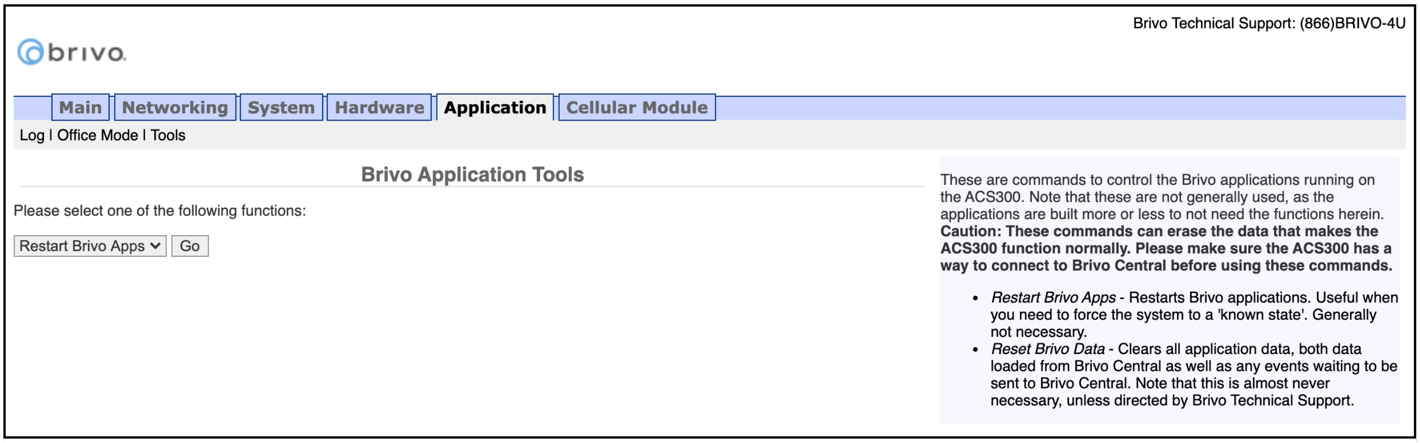
Note that only Allegion LE lock is able to support office mode.

Figure 36: Office Mode

Tools (Application)

The Brivo Application Tools page provides access to two commands that are used only as part of diagnostic procedures where you might suspect that the panel is not operating correctly or data may have been corrupted. To access this page:

1. Click **Application** to access the Application menu bar.
2. Click **Tools** to access the Brivo Application Tools page.
3. From the pull-down menu, select:
   a. **Restart Brivo Apps** to shut down the access control applications on the control panel, and then restart them. Generally, this command should be used only when Brivo Technical Support requests that you do so.
   b. **Reset Brivo Data** to erase the local database of credentials, schedules, door settings, etc., and forces the control panel to reacquire all this information from the Brivo Cloud Server or Brivo Onsite Server. This command should be used only if you suspect that the local data has been corrupted, or if requested by Brivo Technical Support.



Brivo Technical Support: (866)BRIVO-4U

Brivo Application Tools

Please select one of the following functions:

These are commands to control the Brivo applications running on the ACS300. Note that these are not generally used, as the applications are built more or less to not need the functions herein. **Caution: These commands can erase the data that makes the ACS300 function normally. Please make sure the ACS300 has a way to connect to Brivo Central before using these commands.**

- *Restart Brivo Apps* - Restarts Brivo applications. Useful when you need to force the system to a 'known state'. Generally not necessary.
- *Reset Brivo Data* - Clears all application data, both data loaded from Brivo Central as well as any events waiting to be sent to Brivo Central. Note that this is almost never necessary, unless directed by Brivo Technical Support.

Figure 37: Brivo Application Tools

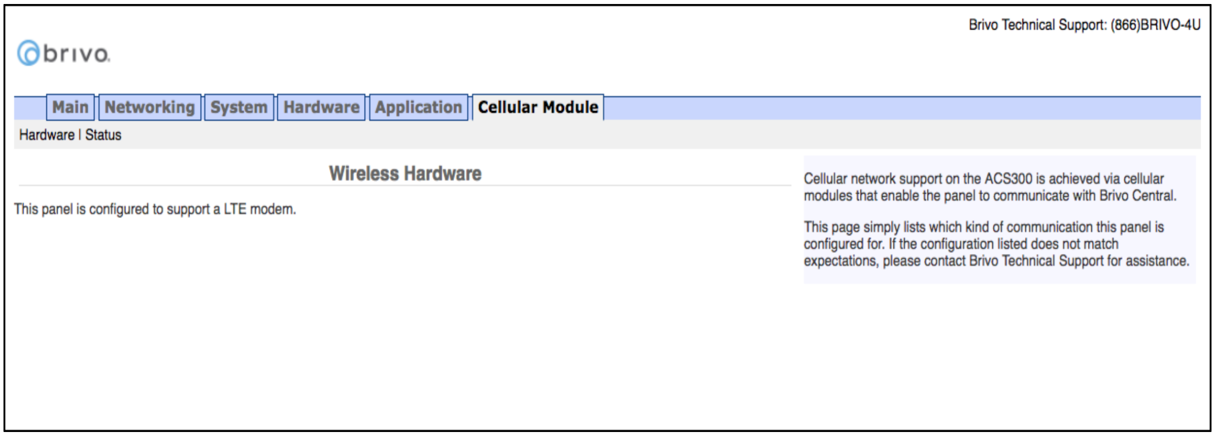
Cellular Module Tab (ACS6000 or ACS300 only)

The Cellular Module tab of the Administrative Interface provides instructions for using a cellular network module for internet connectivity and to verify that the cellular network module is operating properly.

NOTE: Firmware Requirement
In order to use a cellular network module, a minimum firmware version of 6.0.0 for Brivo Access and 3.4.6 for Brivo Onsite Server is required.

Hardware

The Administrative Interface provides a simple list for which kind of communication this panel is configured. If the configuration listed does not match expectations, contact Brivo Technical Support for assistance.



Wireless Hardware

This panel is configured to support a LTE modem.

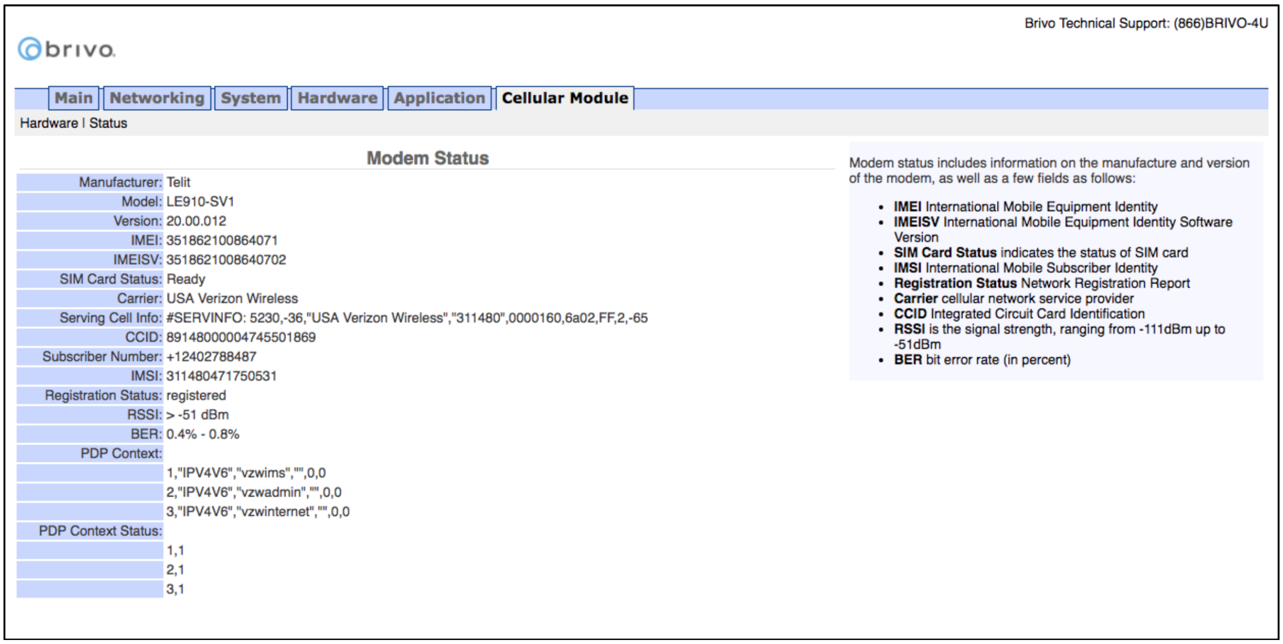
Cellular network support on the ACS300 is achieved via cellular modules that enable the panel to communicate with Brivo Central.

This page simply lists which kind of communication this panel is configured for. If the configuration listed does not match expectations, please contact Brivo Technical Support for assistance.

Figure 38: Wireless Hardware

Status

The Administrative Interface provides modem status information on the manufacturer and version of the modem. Additional modem status information is defined in the text on the right side of the page.



Modem Status

Manufacturer:	Telit
Model:	LE910-SV1
Version:	20.00.012
IMEI:	351862100864071
IMEISV:	3518621008640702
SIM Card Status:	Ready
Carrier:	USA Verizon Wireless
Serving Cell Info:	#SERVINFO: 5230,-36,"USA Verizon Wireless","311480",0000160,6a02,FF,2,-65
CCID:	89148000004745501869
Subscriber Number:	+12402788487
IMSI:	311480471750531
Registration Status:	registered
RSSI:	> -51 dBm
BER:	0.4% - 0.8%
PDP Context:	
	1,"IPV4V6","vzwims","",0,0
	2,"IPV4V6","vzwadmin","",0,0
	3,"IPV4V6","vzwinternet","",0,0
PDP Context Status:	
	1,1
	2,1
	3,1

Modem status includes information on the manufacture and version of the modem, as well as a few fields as follows:

- **IMEI** International Mobile Equipment Identity
- **IMEISV** International Mobile Equipment Identity Software Version
- **SIM Card Status** indicates the status of SIM card
- **IMSI** International Mobile Subscriber Identity
- **Registration Status** Network Registration Report
- **Carrier** cellular network service provider
- **CCID** Integrated Circuit Card Identification
- **RSSI** is the signal strength, ranging from -111dBm up to -51dBm
- **BER** bit error rate (in percent)

Figure 39: Modem Status

Troubleshooting (ACS6000, ACS300, ACS5000, & IPDC)

The following sections provide material to help ensure that the Brivo control panel networking is operating properly.

Network Connectivity

If your Brivo control panel is properly configured for the network, your network administrator should be able to see that it has received an IP address from the local DHCP server. Ask your network administrator to check the “DHCP Clients Table” on the DHCP server. There should be one entry for each control panel you have installed.

Pinging the Control Panel from another Computer

Your network administrator may use the “ping” utility on another computer on the network to test connectivity to the Brivo control panel. To use ping on a Windows computer, follow these steps:

1. In the **Start** menu, select **Run**.
2. When the Run dialog box opens, enter **command** in the Open field. A DOS window displays.
3. Type **ping NNN.NNN.NNN.NNN** where the N’s stand for the IP address of the Brivo control panel. You can get this address from the DHCP server or from the Network Status page of the Administrative Interface on the control panel itself.
4. Read the results of the ping command.
5. If successful, it will provide packet response times and other information.
6. If not, it will say that the node could not be reached.

Pinging another Computer from the Control Panel

You may also wish to verify correct network operation by using the command line interface to ping another computer on your network or on the Internet.

1. Log into the control panel’s Administrative Interface as described in “Accessing the Administrative Interface.”
2. Click **Networking**, and then click **Tools** from the Networking men bar.
3. Enter the **IP address** or full network name of another computer that is known to have network connectivity in the **Target** field and click **Go**.
4. If successful, you should see a response like the following within a few seconds:

```
PING 192.168.192.107 (192.168.192.107): 56 data bytes
64 bytes from 192.168.192.107: icmp_seq=0 ttl=128 time=0.9 ms
64 bytes from 192.168.192.107: icmp_seq=1 ttl=128 time=0.8 ms
64 bytes from 192.168.192.107: icmp_seq=2 ttl=128 time=0.8 ms
64 bytes from 192.168.192.107: icmp_seq=3 ttl=128 time=0.8 ms
64 bytes from 192.168.192.107: icmp_seq=4 ttl=128 time=0.9 ms
--- 192.168.192.107 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.8/0.8/0.9 ms
```

© 2021 Brivo Systems LLC. All rights reserved.

Connectivity to Brivo Cloud Server (-E panels only)

Follow the steps in the Brivo Quick Start Guide to make sure that you have performed all the tasks necessary to set up your account. In particular, you should at least have registered the control panel you are testing.

Connectivity to the Brivo Cloud Server can be verified by using the Network Troubleshooting Assistant.

1. Log into the control panel's Administrative Interface as described in "Accessing the Administrative Interface."
2. Click **Networking**, and then click **Troubleshooting** on the Networking menu bar.
3. If all the tests listed on that page show a green "**PASS**," the control panel is connected to the Brivo Cloud Server.

Connectivity to Brivo Onsite Server (-A panels only)

Follow the steps in the Brivo Onsite Server Quick Start Guide to make sure that you have performed all the tasks necessary to set up your account. In particular, you should at least have registered the control panel you are testing.

Connectivity to the Brivo Onsite Server can be verified by using the Network Troubleshooting Assistant.

1. Log into the control panel's Administrative Interface as described in "Accessing the Administrative Interface."
2. Click **Networking**, and then click **Troubleshooting** on the Networking menu bar.
3. If all the tests listed on that page show a green "**PASS**," the control panel is connected to the Brivo Onsite Server.

Additional Troubleshooting

For additional assistance to questions not answered in this troubleshooting section, please refer to www.brivo.com or contact Brivo Technical Support.

ACS100

This chapter is devoted to the **ACS100** control panel. For information on the **ACS6000**, **ACS300**, **ACS5000**, and **IPDC** control panels, refer to the previous chapter.

Accessing the Local Administrative Interface

This section describes how to connect to the Brivo control panel local Administrative Interface (often described throughout this document as the **WebCLI**).

NOTE: In most cases, the Brivo control panel will self-configure its network settings without any input from the installer. You will only need to use access the Administrative Interface if you need to configure your network settings manually or for troubleshooting.

Connect a Laptop to the same subnet as the ACS100

Accessing the **ACS100** local administrative interface is similar to other control panels (**ACS300**/**ACS6000**) except there is only one LAN port. Therefore, instead of connecting your laptop directly to the control panel, 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 **ACS100** (usually through a PoE switch) as shown in the figure below.

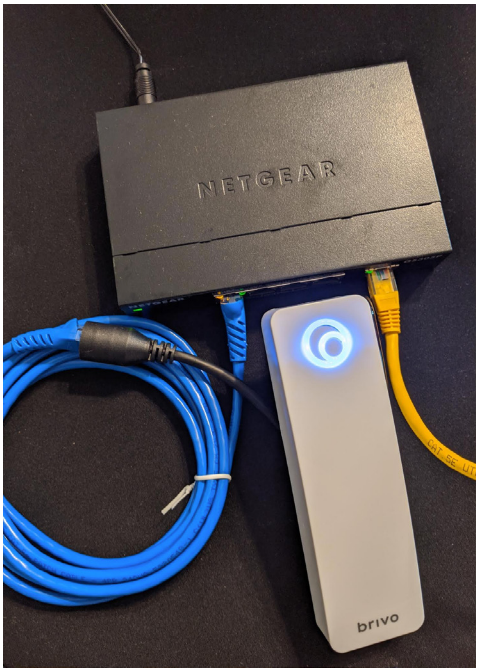


Figure 40: **ACS100** - Connect laptop to control panel through switch

When the Ethernet connection is working properly, you will see a blue Brivo logo illuminated on the front of the **ACS100**. If the logo is not illuminated, check the connection on the **ACS100** as well as the connection to the switch to which the panel is connected.

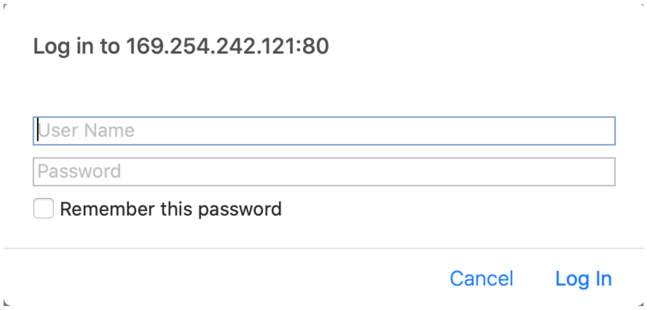
© 2021 Brivo Systems LLC. All rights reserved.

Log in to the Administrative Interface

NOTE: The process for logging into the local Administrative Interface on an ACS100 is different than other Brivo control panels.

After your computer finishes booting up:

1. Go to your laptop's/PC's networking settings page and manually set your IP address on your laptop/PC to **169.254.242.122** and net mask **255.255.255.0**. If asked for subnet length instead of net mask, enter **24**.
2. Open your web browser and navigate to **169.254.242.121** .
3. A pop-up login screen similar to the one shown in the figure below will display.



Log in to 169.254.242.121:80

User Name

Password

□ Remember this password

Figure 41: Login Screen

4. Enter **cli** as the default user name and **new5cli** as the default password. You are now ready to begin configuring your Brivo control panel.

© 2021 Brivo Systems LLC. All rights reserved.

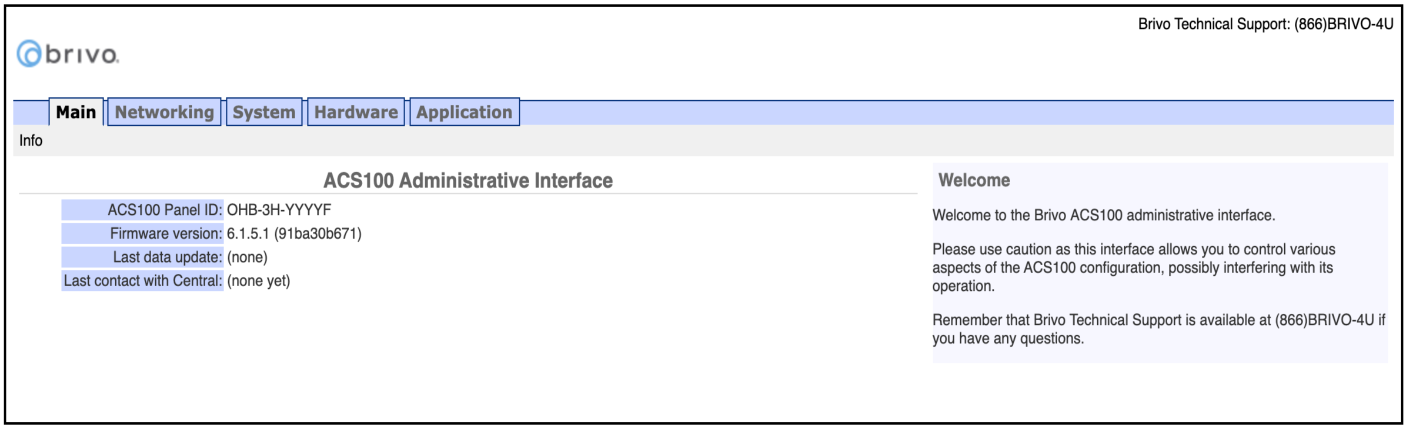
Main Tab

Info

The **Info** screen of the Main tab displays the control panel Administrative Interface.

NOTE: If you were **NOT** able to reach this page for any reason, see the *Troubleshooting* section at the end of this document.

NOTE: For ease of presentation, the screenshots below display **ACS100** as the model type. When you log in, the model that displays will match your device type.



ACS100 Administrative Interface

ACS100 Panel ID:	OHB-3H-YYYYF
Firmware version:	6.1.5.1 (91ba30b671)
Last data update:	(none)
Last contact with Central:	(none yet)

Welcome

Welcome to the Brivo ACS100 administrative interface.

Please use caution as this interface allows you to control various aspects of the ACS100 configuration, possibly interfering with its operation.

Remember that Brivo Technical Support is available at (866)BRIVO-4U if you have any questions.

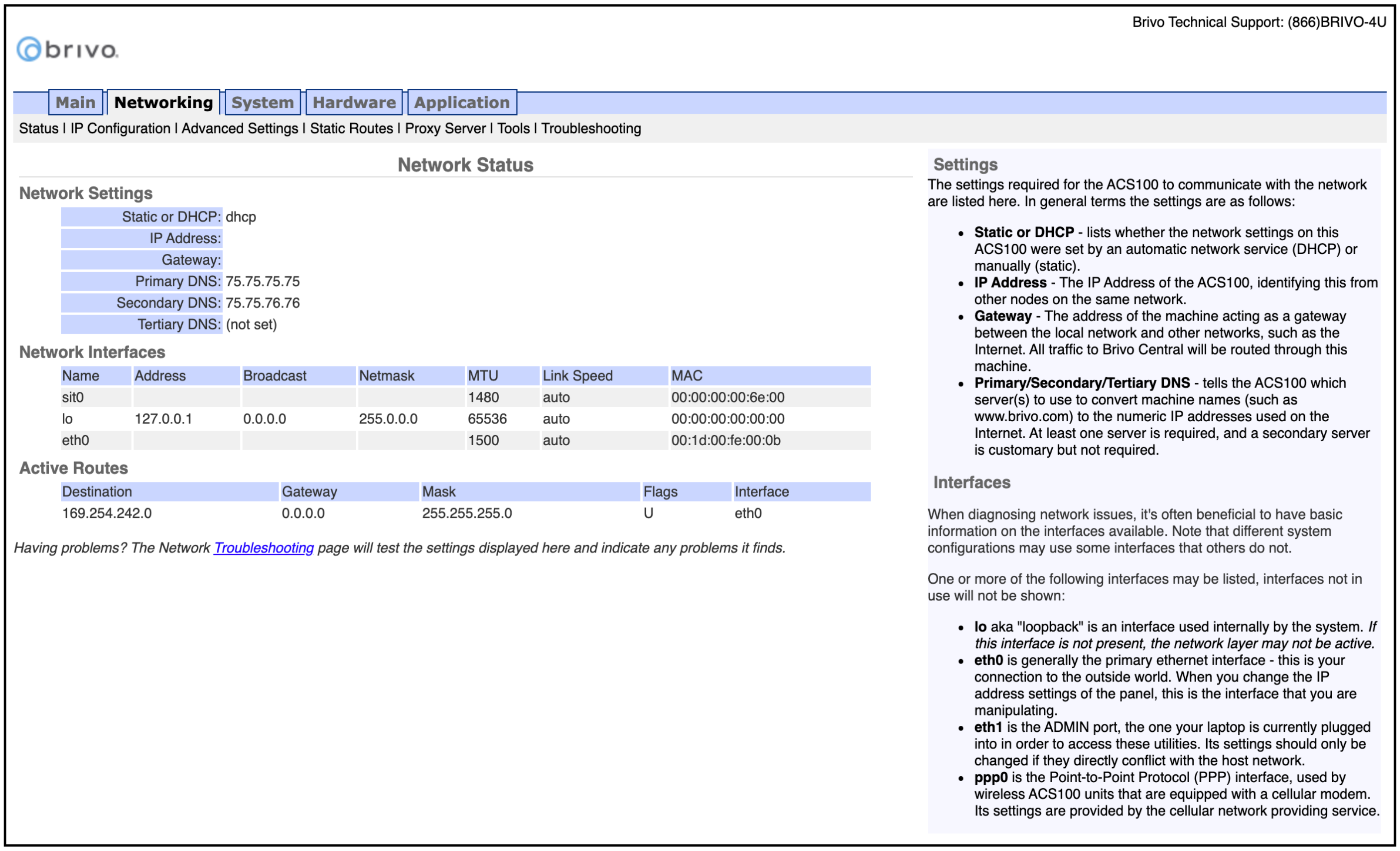
Figure 42: Administrative Interface

Networking Tab

Status

The Network Status page is useful for diagnosing various network conditions. To access this page:

1. Click **Networking** to access the Networking menu bar.
2. Click **Status** to access the Network Status page. Explanations of the various status fields are provided in the text on the right side of the page.


Brivo Technical Support: (866)BRIVO-4U
Main
Networking
System
Hardware
Application
Status | IP Configuration | Advanced Settings | Static Routes | Proxy Server | Tools | Troubleshooting

Network Status

Network Settings

Static or DHCP:	dhcp
IP Address:	
Gateway:	
Primary DNS:	75.75.75.75
Secondary DNS:	75.75.76.76
Tertiary DNS:	(not set)

Network Interfaces

Name	Address	Broadcast	Netmask	MTU	Link Speed	MAC
sit0				1480	auto	00:00:00:00:6e:00
lo	127.0.0.1	0.0.0.0	255.0.0.0	65536	auto	00:00:00:00:00:00
eth0				1500	auto	00:1d:00:fe:00:0b

Active Routes

Destination	Gateway	Mask	Flags	Interface
169.254.242.0	0.0.0.0	255.255.255.0	U	eth0

Having problems? The Network Troubleshooting page will test the settings displayed here and indicate any problems it finds.

Settings

The settings required for the ACS100 to communicate with the network are listed here. In general terms the settings are as follows:

- **Static or DHCP** - lists whether the network settings on this ACS100 were set by an automatic network service (DHCP) or manually (static).
- **IP Address** - The IP Address of the ACS100, identifying this from other nodes on the same network.
- **Gateway** - The address of the machine acting as a gateway between the local network and other networks, such as the Internet. All traffic to Brivo Central will be routed through this machine.
- **Primary/Secondary/Tertiary DNS** - tells the ACS100 which server(s) to use to convert machine names (such as www.brivo.com) to the numeric IP addresses used on the Internet. At least one server is required, and a secondary server is customary but not required.

Interfaces

When diagnosing network issues, it's often beneficial to have basic information on the interfaces available. Note that different system configurations may use some interfaces that others do not.

One or more of the following interfaces may be listed, interfaces not in use will not be shown:

- **lo** aka "loopback" is an interface used internally by the system. *If this interface is not present, the network layer may not be active.*
- **eth0** is generally the primary ethernet interface - this is your connection to the outside world. When you change the IP address settings of the panel, this is the interface that you are manipulating.
- **eth1** is the ADMIN port, the one your laptop is currently plugged into in order to access these utilities. Its settings should only be changed if they directly conflict with the host network.
- **ppp0** is the Point-to-Point Protocol (PPP) interface, used by wireless ACS100 units that are equipped with a cellular modem. Its settings are provided by the cellular network providing service.

Figure 43: Network Status

IP Configuration

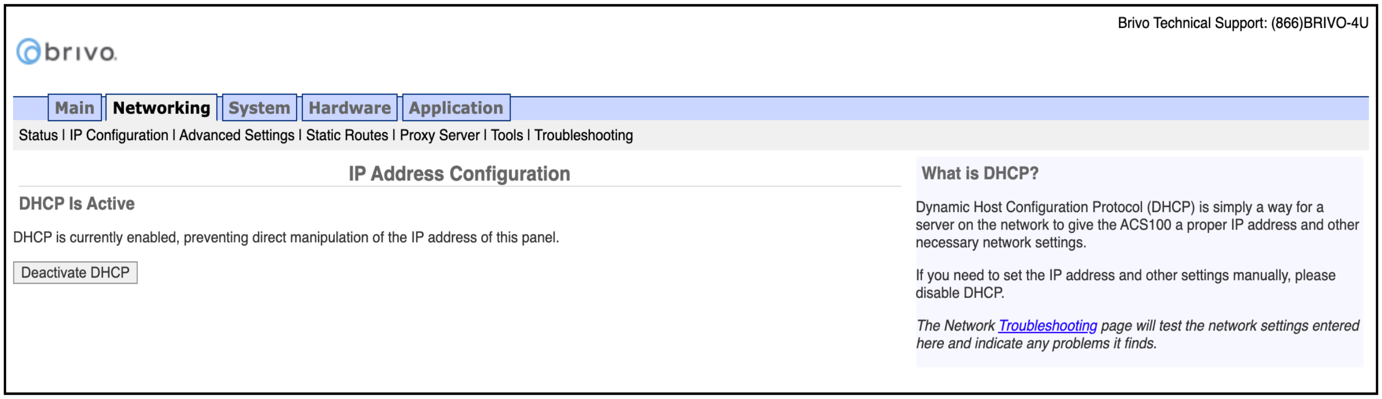
The Brivo control panel is shipped with DHCP enabled. This means that on most networks, the control panel will automatically acquire all the information it needs to communicate with Brivo. However, some networks may require custom settings, either by design or by policy. This section explains how to change network settings if you need to do so.

If you are uncertain whether the network requires manual configuration of networks settings, contact the network administrator at the site.

Deactivating DHCP

Before you can set network parameters manually, you must first deactivate DHCP.

1. Select the **Networking** tab. The Networking menu bar displays.
2. Select **IP Configuration**. The IP Address Configuration page displays.
3. Click **Deactivate DHCP**.


Brivo Technical Support: (866)BRIVO-4U
brivo
Main
Networking
System
Hardware
Application
Status | IP Configuration | Advanced Settings | Static Routes | Proxy Server | Tools | Troubleshooting
Deactivate DHCP

IP Address Configuration

DHCP Is Active

DHCP is currently enabled, preventing direct manipulation of the IP address of this panel.

What is DHCP?

Dynamic Host Configuration Protocol (DHCP) is simply a way for a server on the network to give the ACS100 a proper IP address and other necessary network settings.

If you need to set the IP address and other settings manually, please disable DHCP.

The Network Troubleshooting page will test the network settings entered here and indicate any problems it finds.

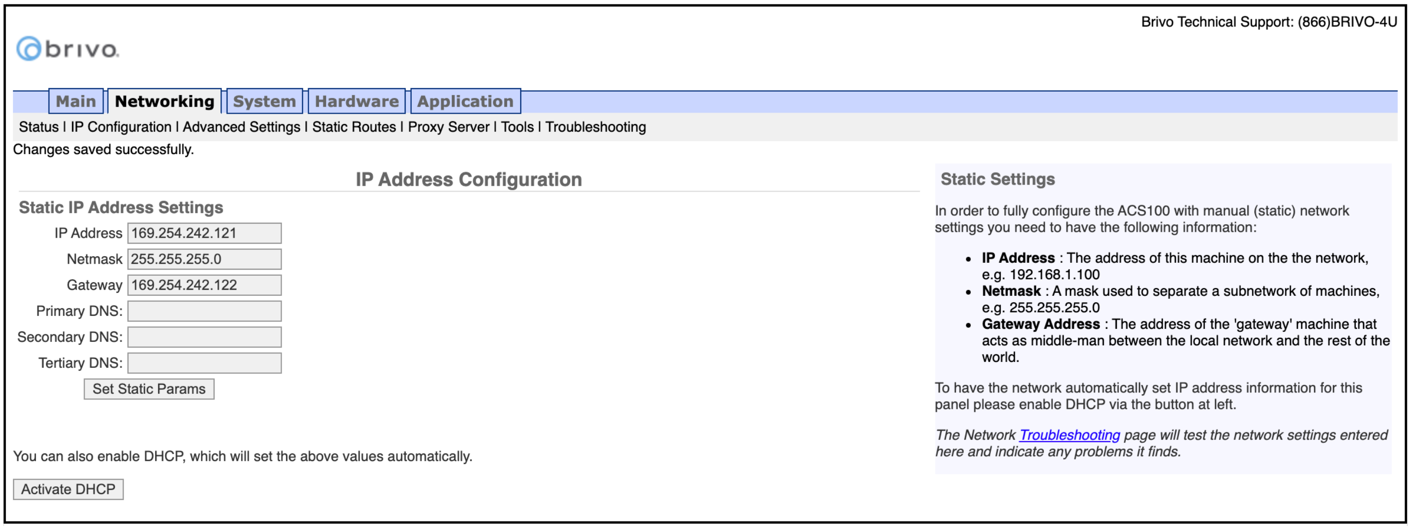
Figure 44: Deactivate DHCP

© 2021 Brivo Systems LLC. All rights reserved.

Entering Networking Parameters

Once DHCP is deactivated, you can enter IP configuration information on the IP Address Configuration page.

1. **IP Address**, **Netmask**, **Gateway**, and **Primary DNS** are required fields on this page.
2. **Secondary DNS** and **Tertiary DNS** are optional.
3. After entering the data, click **Set Static Params**.



Brivo Technical Support: (866)BRIVO-4U
brivo
Main
Networking
System
Hardware
Application
Status | IP Configuration | Advanced Settings | Static Routes | Proxy Server | Tools | Troubleshooting

Changes saved successfully.

IP Address Configuration

Static IP Address Settings

IP Address	169.254.242.121
Netmask	255.255.255.0
Gateway	169.254.242.122
Primary DNS:	
Secondary DNS:	
Tertiary DNS:	

You can also enable DHCP, which will set the above values automatically.

Static Settings

In order to fully configure the ACS100 with manual (static) network settings you need to have the following information:

- **IP Address** : The address of this machine on the the network, e.g. 192.168.1.100
- **Netmask** : A mask used to separate a subnetwork of machines, e.g. 255.255.255.0
- **Gateway Address** : The address of the 'gateway' machine that acts as middle-man between the local network and the rest of the world.

To have the network automatically set IP address information for this panel please enable DHCP via the button at left.

The Network Troubleshooting page will test the network settings entered here and indicate any problems it finds.

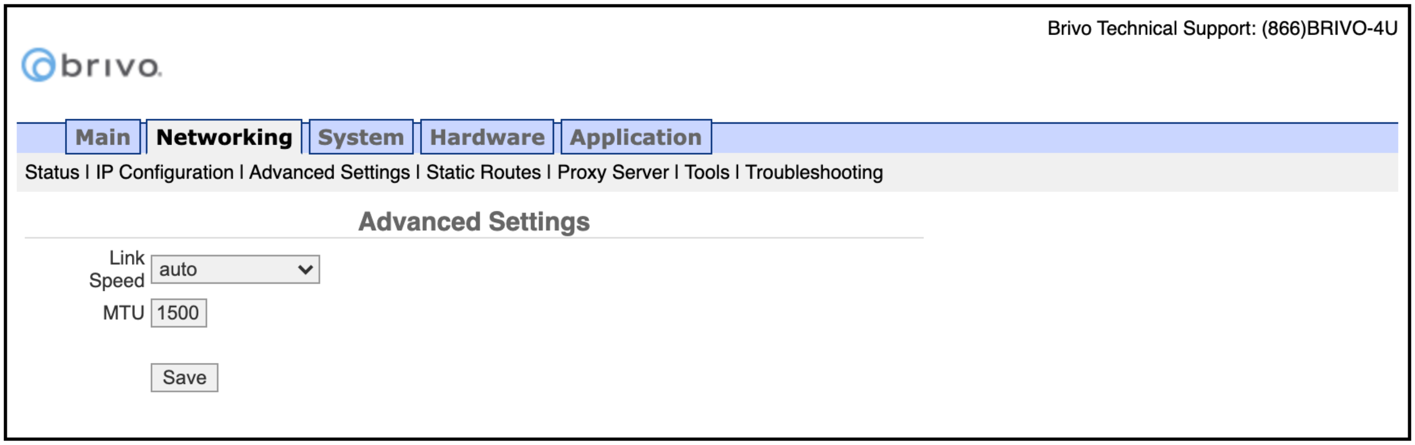
Figure 45: IP Address Configuration

NOTE: Incorrect parameters may prevent the control panel from communicating with the Brivo Cloud Server. Please confirm all settings with the LAN network administrator first.

Advanced Settings

When configuring a network Link Speed, the Brivo control panel defaults to Auto when establishing a link speed between the panel and the network.

1. Click **Networking** to access the Networking menu bar.
2. Click **Advanced Settings** to access the Advanced Settings page.



brivo
Main
Networking
System
Hardware
Application
Status | IP Configuration | Advanced Settings | Static Routes | Proxy Server | Tools | Troubleshooting
Save

Brivo Technical Support: (866)BRIVO-4U

Advanced Settings

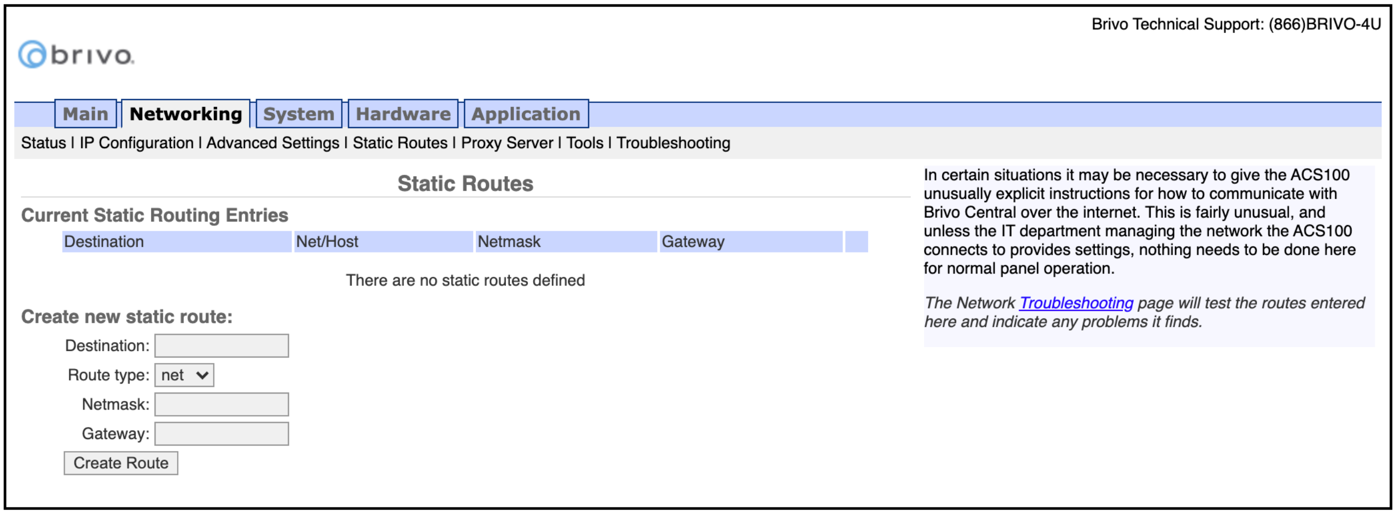
Link Speed: auto

MTU: 1500

Figure 46: Advanced Settings

Static Routes

Establishing static routes is rarely required and should be performed only with the advice of the network administrator for the site where the control panel is being installed.



brivo
Main
Networking
System
Hardware
Application
Status | IP Configuration | Advanced Settings | Static Routes | Proxy Server | Tools | Troubleshooting
Create Route

Brivo Technical Support: (866)BRIVO-4U

Static Routes

Current Static Routing Entries

Destination	Net/Host	Netmask	Gateway

There are no static routes defined

Create new static route:

Destination:

Route type: net

Netmask:

Gateway:

In certain situations it may be necessary to give the ACS100 unusually explicit instructions for how to communicate with Brivo Central over the internet. This is fairly unusual, and unless the IT department managing the network the ACS100 connects to provides settings, nothing needs to be done here for normal panel operation.

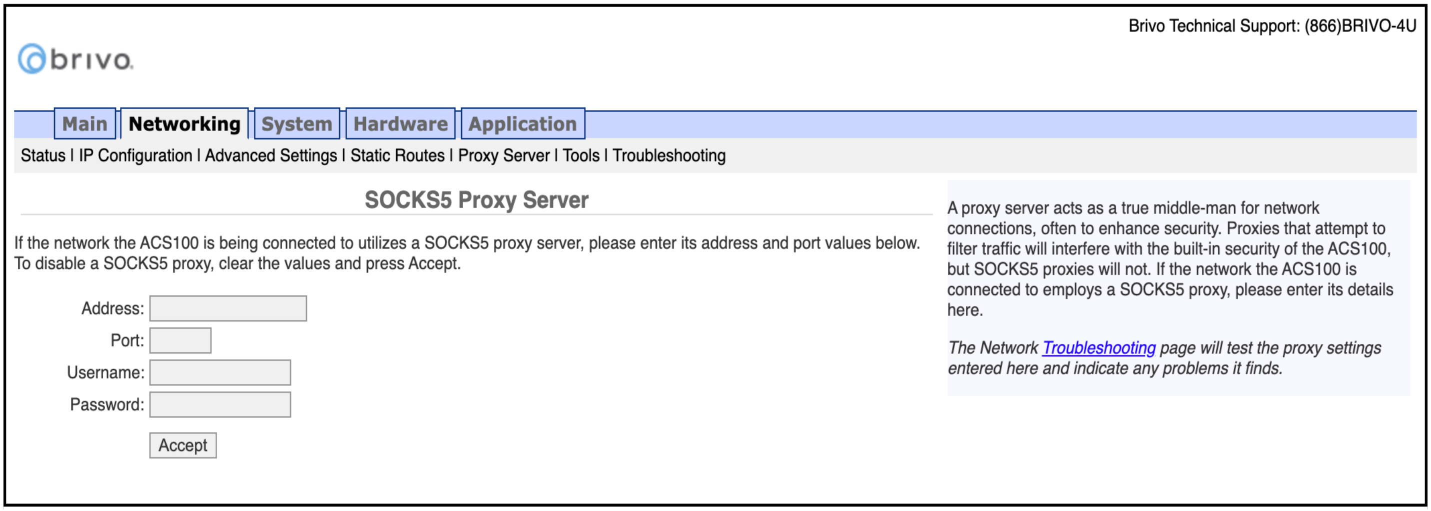
The Network Troubleshooting page will test the routes entered here and indicate any problems it finds.

Figure 47: Static Routes Configuration

Proxy Server

If your network uses a proxy server to control access to the internet, you will need to manually configure the proxy server settings. Before changing these settings, first work with the network administrator to determine valid values.

1. Click **Networking** to access the Networking menu bar.
2. Click **Proxy Server** to access the SOCKS5 Proxy Server page.


Brivo Technical Support: (866)BRIVO-4U
Main
Networking
System
Hardware
Application
Status | IP Configuration | Advanced Settings | Static Routes | Proxy Server | Tools | Troubleshooting
Address:
Port:
Username:
Password:
Accept

SOCKS5 Proxy Server

If the network the ACS100 is being connected to utilizes a SOCKS5 proxy server, please enter its address and port values below. To disable a SOCKS5 proxy, clear the values and press Accept.

A proxy server acts as a true middle-man for network connections, often to enhance security. Proxies that attempt to filter traffic will interfere with the built-in security of the ACS100, but SOCKS5 proxies will not. If the network the ACS100 is connected to employs a SOCKS5 proxy, please enter its details here.

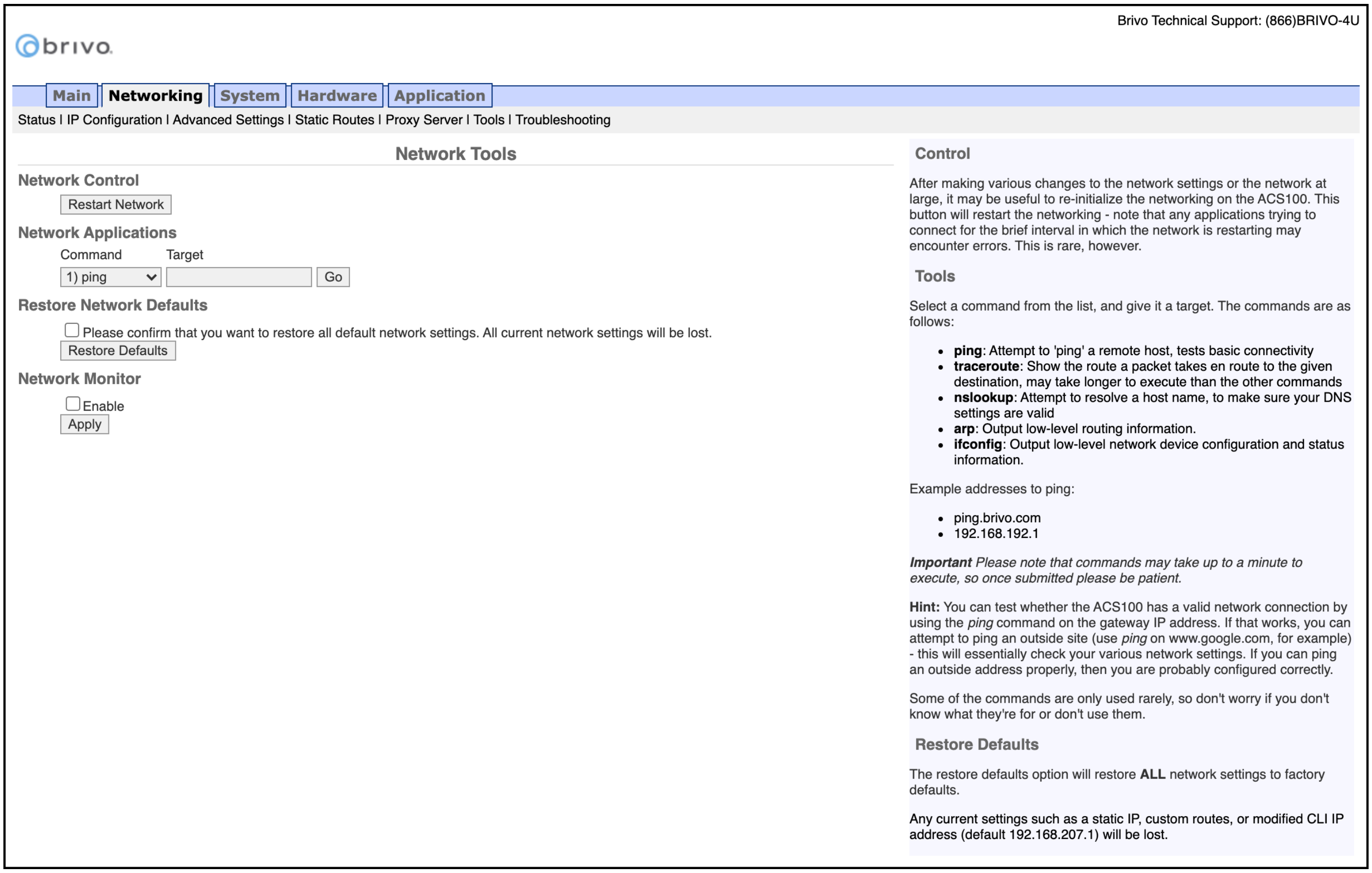
The Network Troubleshooting page will test the proxy settings entered here and indicate any problems it finds.

Figure 48: Proxy Server Configuration

Tools (Networking)

Diagnosing connectivity problems through use of the Network Tools page allows you to reinitialize the Brivo control panel networking setup or enter commands for diagnosing network connectivity problems. To access this page:

1. Click **Networking** to access the Networking menu bar.
2. Click **Tools** to access the Network Tools page.
3. If you want to reinitialize the Brivo control panel networking, click **Restart Network**.
4. To diagnose network connectivity problems, enter a valid **Command** and **Target**, then click **Go**. The system performs the specified command and displays the output. Descriptions of the valid commands are provided in the text on the right side of the page.


Brivo Technical Support: (866)BRIVO-4U
brivo
Main
Networking
System
Hardware
Application
Status | IP Configuration | Advanced Settings | Static Routes | Proxy Server | Tools | Troubleshooting
Restart Network
Command
Target
1) ping
Go
Restore Defaults
Apply

Network Tools

Network Control

Network Applications

Restore Network Defaults

□ Please confirm that you want to restore all default network settings. All current network settings will be lost.

Network Monitor

□ Enable

Control

After making various changes to the network settings or the network at large, it may be useful to re-initialize the networking on the ACS100. This button will restart the networking - note that any applications trying to connect for the brief interval in which the network is restarting may encounter errors. This is rare, however.

Tools

Select a command from the list, and give it a target. The commands are as follows:

- **ping**: Attempt to 'ping' a remote host, tests basic connectivity
- **traceroute**: Show the route a packet takes en route to the given destination, may take longer to execute than the other commands
- **nslookup**: Attempt to resolve a host name, to make sure your DNS settings are valid
- **arp**: Output low-level routing information.
- **ifconfig**: Output low-level network device configuration and status information.

Example addresses to ping:

- ping.brivo.com
- 192.168.192.1

Important *Please note that commands may take up to a minute to execute, so once submitted please be patient.*

Hint: You can test whether the ACS100 has a valid network connection by using the *ping* command on the gateway IP address. If that works, you can attempt to ping an outside site (use *ping* on www.google.com, for example) - this will essentially check your various network settings. If you can ping an outside address properly, then you are probably configured correctly.

Some of the commands are only used rarely, so don't worry if you don't know what they're for or don't use them.

Restore Defaults

The restore defaults option will restore **ALL** network settings to factory defaults.

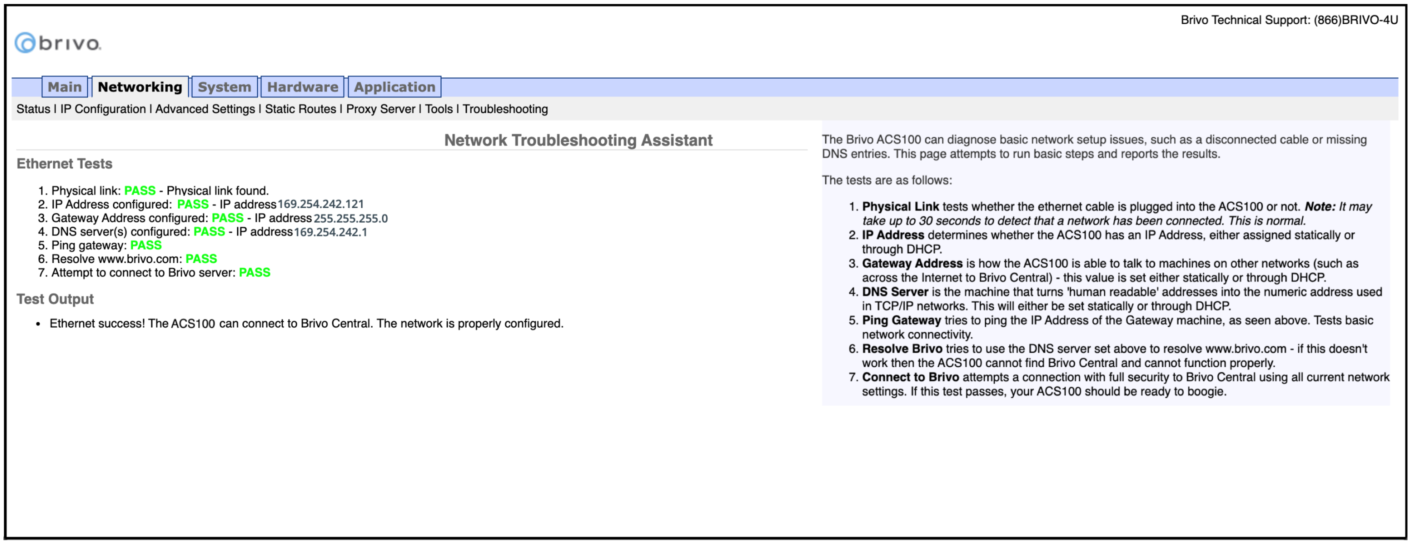
Any current settings such as a static IP, custom routes, or modified CLI IP address (default 192.168.207.1) will be lost.

Figure 49: Network Tools

Troubleshooting

Troubleshooting network problems (for the **ACS100**) through the Administrative Interface uses a Network Troubleshooting assistant to determine if the Brivo control panel is connected to the local network and ultimately to the Brivo Cloud Server. To access this tool:

1. Click **Networking** to access the Networking menu bar.
2. Click **Troubleshooting** to access the Network Troubleshooting Assistant.
3. If any one of the connectivity tests fails, a message displays describing the failure and offering suggestions for resolving it. Descriptions of the tests performed are provided in the text on the right side of the page.


Brivo Technical Support: (866)BRIVO-4U
Main
Networking
System
Hardware
Application
Status | IP Configuration | Advanced Settings | Static Routes | Proxy Server | Tools | Troubleshooting

Network Troubleshooting Assistant

Ethernet Tests

1. Physical link: PASS - Physical link found.
2. IP Address configured: PASS - IP address 169.254.242.121
3. Gateway Address configured: PASS - IP address 255.255.255.0
4. DNS server(s) configured: PASS - IP address 169.254.242.1
5. Ping gateway: PASS
6. Resolve www.brivo.com: PASS
7. Attempt to connect to Brivo server: PASS

Test Output

- Ethernet success! The ACS100 can connect to Brivo Central. The network is properly configured.

The Brivo ACS100 can diagnose basic network setup issues, such as a disconnected cable or missing DNS entries. This page attempts to run basic steps and reports the results.

The tests are as follows:

1. **Physical Link** tests whether the ethernet cable is plugged into the ACS100 or not. ***Note:*** *It may take up to 30 seconds to detect that a network has been connected. This is normal.*
2. **IP Address** determines whether the ACS100 has an IP Address, either assigned statically or through DHCP.
3. **Gateway Address** is how the ACS100 is able to talk to machines on other networks (such as across the Internet to Brivo Central) - this value is set either statically or through DHCP.
4. **DNS Server** is the machine that turns 'human readable' addresses into the numeric address used in TCP/IP networks. This will either be set statically or through DHCP.
5. **Ping Gateway** tries to ping the IP Address of the Gateway machine, as seen above. Tests basic network connectivity.
6. **Resolve Brivo** tries to use the DNS server set above to resolve www.brivo.com - if this doesn't work then the ACS100 cannot find Brivo Central and cannot function properly.
7. **Connect to Brivo** attempts a connection with full security to Brivo Central using all current network settings. If this test passes, your ACS100 should be ready to boogie.

Figure 50: Network Troubleshooting Assistant

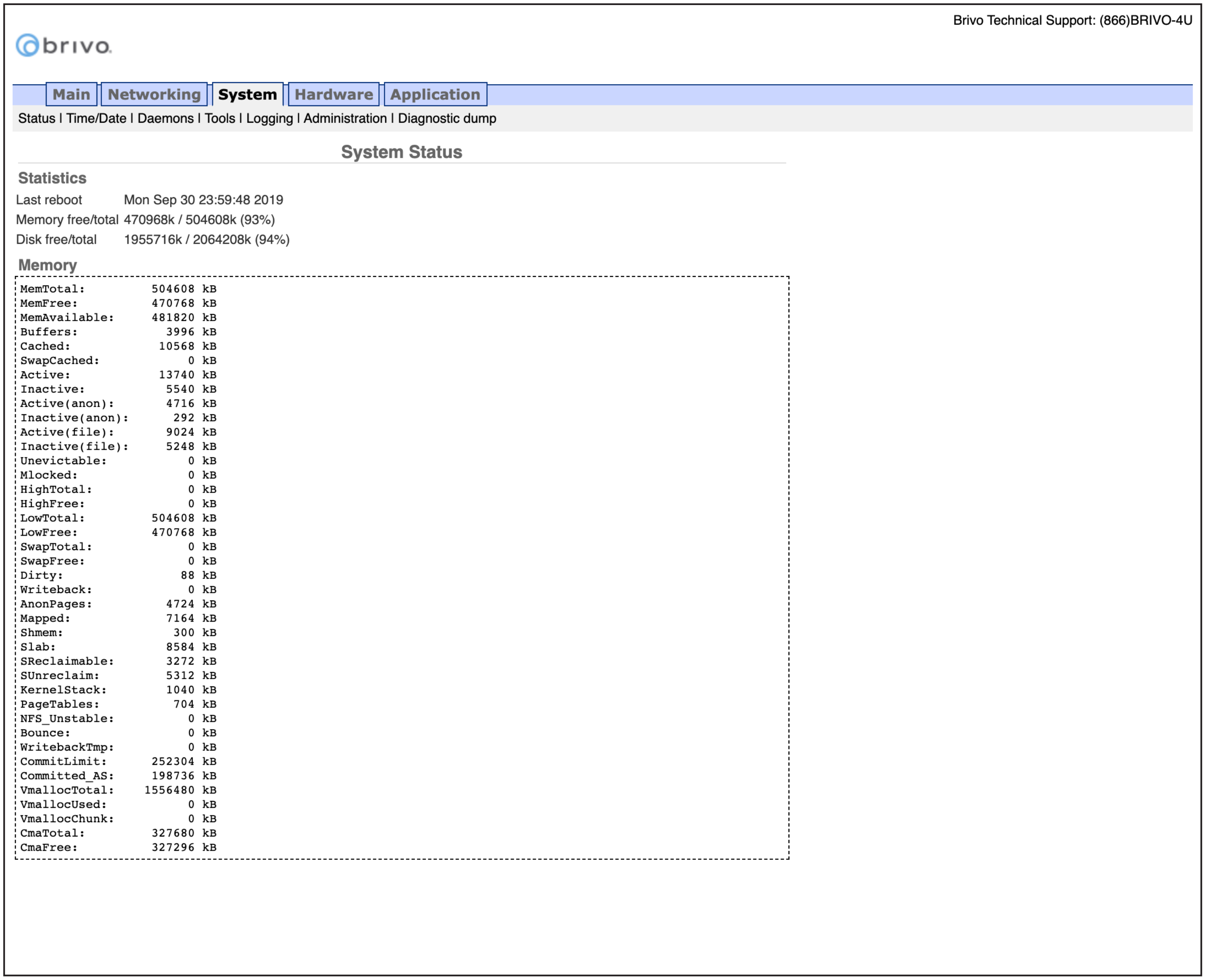
System Tab

WARNING: These tools are rarely required during normal operation of the panel and should be used only in conjunction with assistance from Brivo Technical Support.

Status

To view a status report of the performance and state of the control panel at the level of the operating system:

1. Click **System** to access the System menu bar.
2. Click **Status** to access the System Status page.


Brivo Technical Support: (866)BRIVO-4U
Main
Networking
System
Hardware
Application
Status | Time/Date | Daemons | Tools | Logging | Administration | Diagnostic dump

System Status

Statistics

```
Last reboot        Mon Sep 30 23:59:48 2019
Memory free/total  470968k / 504608k (93%)
Disk free/total    1955716k / 2064208k (94%)
```

Memory

```
MemTotal:         504608 kB
MemFree:          470768 kB
MemAvailable:     481820 kB
Buffers:            3996 kB
Cached:            10568 kB
SwapCached:            0 kB
Active:            13740 kB
Inactive:           5540 kB
Active(anon):       4716 kB
Inactive(anon):      292 kB
Active(file):       9024 kB
Inactive(file):     5248 kB
Unevictable:           0 kB
Mlocked:               0 kB
HighTotal:             0 kB
HighFree:              0 kB
LowTotal:         504608 kB
LowFree:          470768 kB
SwapTotal:             0 kB
SwapFree:              0 kB
Dirty:                88 kB
Writeback:             0 kB
AnonPages:          4724 kB
Mapped:             7164 kB
Shmem:               300 kB
Slab:               8584 kB
SReclaimable:       3272 kB
SUnreclaim:         5312 kB
KernelStack:        1040 kB
PageTables:          704 kB
NFS_Unstable:          0 kB
Bounce:                0 kB
WritebackTmp:          0 kB
CommitLimit:      252304 kB
Committed_AS:     198736 kB
VmallocTotal:    1556480 kB
VmallocUsed:           0 kB
VmallocChunk:          0 kB
CmaTotal:         327680 kB
CmaFree:          327296 kB
```

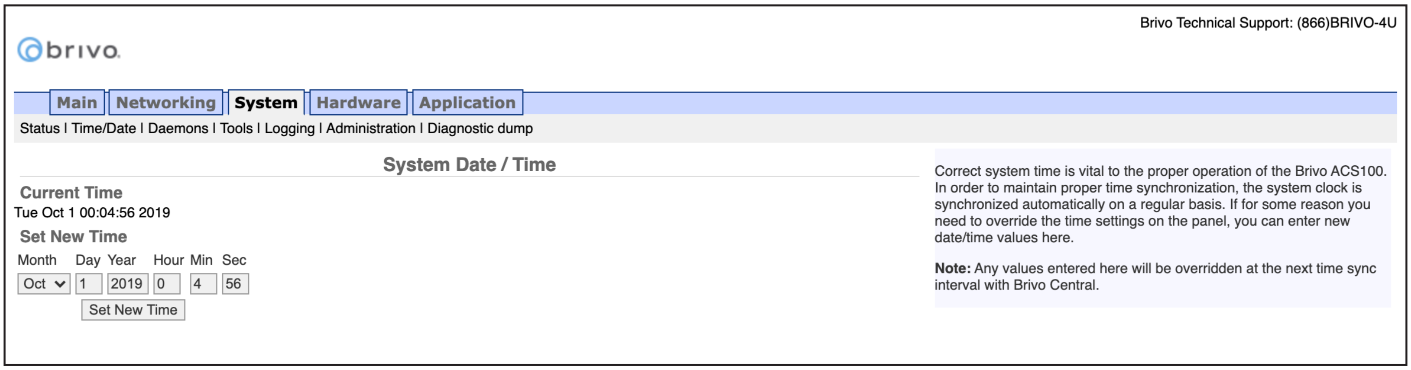
Figure 51: System Status

© 2021 Brivo Systems LLC. All rights reserved.

Time/Date

To view or change the date and time settings in the control panel:

1. Click **System** to access the System menu bar.
2. Click **Time/Date** to access the System Date/Time page.


Brivo Technical Support: (866)BRIVO-4U
Main
Networking
System
Hardware
Application
Status I Time/Date I Daemons I Tools I Logging I Administration I Diagnostic dump
Set New Time

System Date / Time

Current Time
Tue Oct 1 00:04:56 2019

Set New Time

Month	Day	Year	Hour	Min	Sec
Oct	1	2019	0	4	56

Correct system time is vital to the proper operation of the Brivo ACS100. In order to maintain proper time synchronization, the system clock is synchronized automatically on a regular basis. If for some reason you need to override the time settings on the panel, you can enter new date/time values here.

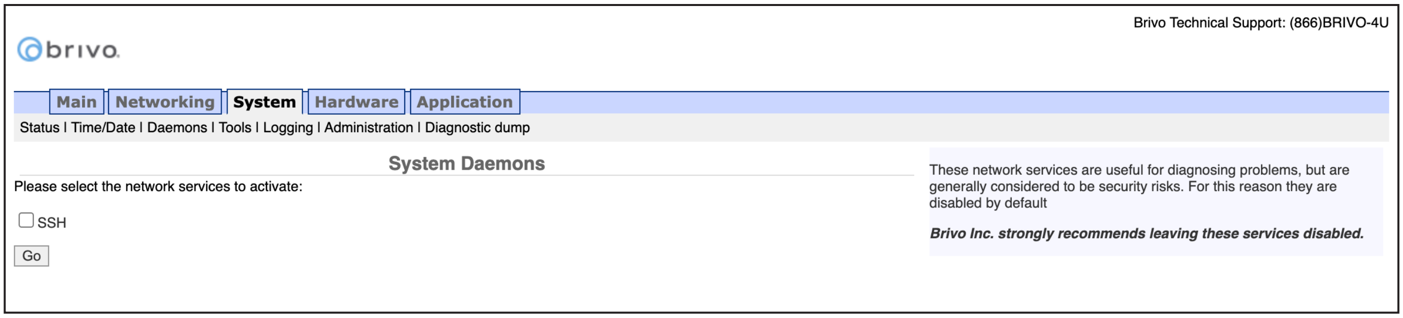
Note: Any values entered here will be overridden at the next time sync interval with Brivo Central.

Figure 52: System Date/Time

NOTE: A properly functioning control panel obtains its date and time information from the Brivo Cloud Server. Setting the date and time manually should seldom be required, if ever.

Daemons

The Administrative Interface provides tools for enabling telnet access through the local interface only but is never used except for debugging purposes. This page should be accessed ONLY if requested by Brivo Technical Support.


Brivo Technical Support: (866)BRIVO-4U
Main
Networking
System
Hardware
Application
Status I Time/Date I Daemons I Tools I Logging I Administration I Diagnostic dump
Go

System Daemons

Please select the network services to activate:

□ SSH

These network services are useful for diagnosing problems, but are generally considered to be security risks. For this reason they are disabled by default

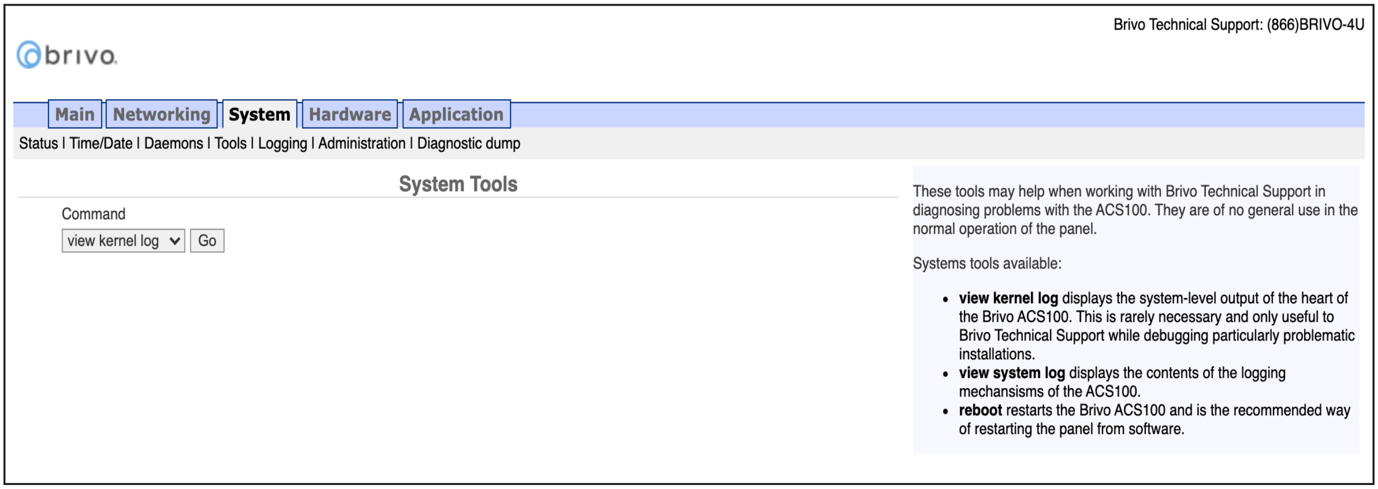
Brivo Inc. strongly recommends leaving these services disabled.

Figure 53: System Daemons

Tools (System)

The Administrative Interface provides access to low-level operations that are to be used only when troubleshooting a control panel with the assistance of Brivo Technical Support. If instructed to do so by Technical Support:

1. Click **System** to access the System menu bar.
2. Click **Tools** to access the System Tools page.



brivo
Main
Networking
System
Hardware
Application
Status | Time/Date | Daemons | Tools | Logging | Administration | Diagnostic dump
Go

Brivo Technical Support: (866)BRIVO-4U

System Tools

Command: view kernel log

These tools may help when working with Brivo Technical Support in diagnosing problems with the ACS100. They are of no general use in the normal operation of the panel.

Systems tools available:

- **view kernel log** displays the system-level output of the heart of the Brivo ACS100. This is rarely necessary and only useful to Brivo Technical Support while debugging particularly problematic installations.
- **view system log** displays the contents of the logging mechansisms of the ACS100.
- **reboot** restarts the Brivo ACS100 and is the recommended way of restarting the panel from software.

Figure 54: System Tools

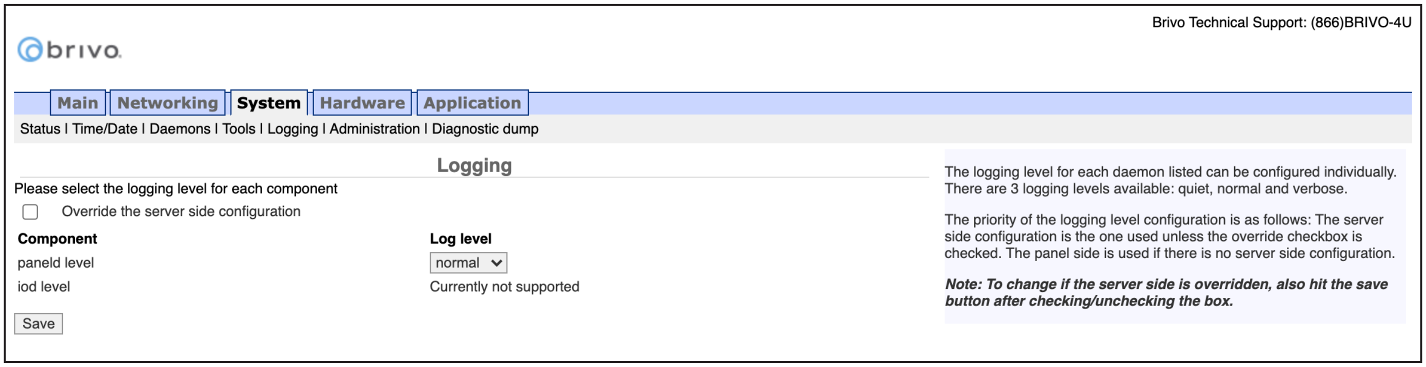
3. The three options from the **Command** dropdown menu are:
   a. **View Kernel Log** – this displays the system level output of the control panel. This is generally only useful to Brivo Technical Support.
   b. **View System Log** – this displays the contents of the various logging mechanisms in the control panel.
   c. **Reboot** – this restarts the control panel. This is the recommended method of restarting the panel from within the Administrative Interface. It is recommended that this function only be used if asked to by Brivo Technical Support.
4. Once you have selected your option, click the **Go** button.

© 2021 Brivo Systems LLC. All rights reserved.

Logging

The Administrative Interface allows the option to configure the level of logging for each daemon listed. By default, the levels are set on the server side, but may be overriden by checking the override checkbox and manually configured.

1. Click **System** to access the System menu bar.
2. Click **Logging** to access the System Tools page.


Brivo Technical Support: (866)BRIVO-4U
brivo
Main
Networking
System
Hardware
Application
Status | Time/Date | Daemons | Tools | Logging | Administration | Diagnostic dump
Save

Logging

Please select the logging level for each component

□ Override the server side configuration

Component	Log level
paneld level	normal
iod level	Currently not supported

The logging level for each daemon listed can be configured individually. There are 3 logging levels available: quiet, normal and verbose.

The priority of the logging level configuration is as follows: The server side configuration is the one used unless the override checkbox is checked. The panel side is used if there is no server side configuration.

Note: To change if the server side is overridden, also hit the save button after checking/unchecking the box.

Figure 55: Logging

3. To change the log level, check the **Override the server side configuration** checkbox.
4. If desired, change the log level on each daemon from the dropdown list. The options are **Quiet**, **Normal**, and **Verbose**.
5. Once you are finished, click the **Save** button.

© 2021 Brivo Systems LLC. All rights reserved.

Administration

The Administrative Interface provides the administrator with the option to change the default Username and Password to the Administrative Interface. The default Username is **cli** and the default Password is **new5cli**.

IMPORTANT NOTE: Brivo recommends that you change the default password when you first access the Administrative Interface.

1. Click **System** to access the System menu bar.
2. Click **Administration** to access the Change the Login Password page.
3. If desired, enter the new **Username**.
4. If desired, enter the new **Password**.
5. Enter the same Password in the **Confirm Password** field.
6. Click **Apply**.

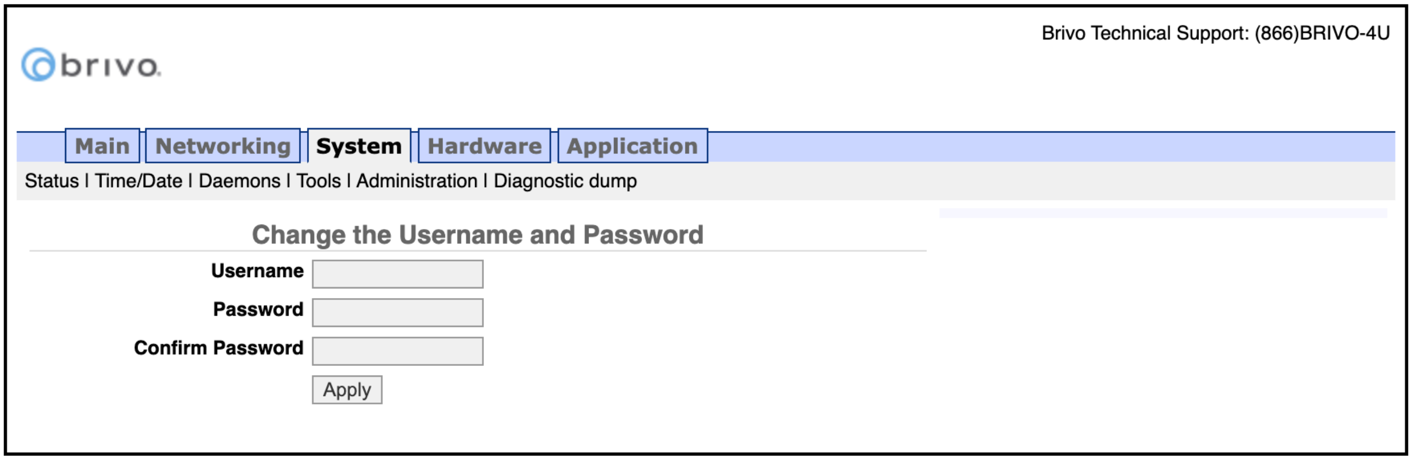

Brivo Technical Support: (866)BRIVO-4U
brivo
Main
Networking
System
Hardware
Application
Status I Time/Date I Daemons I Tools I Administration I Diagnostic dump
Change the Username and Password
Username
Password
Confirm Password
Apply

Figure 56: Change the Username and Password

NOTE: New usernames and passwords must comply with the following rules:

- The minimum character length is six characters and the maximum character length is 1024 characters.
- All CAPS and the following non-alphanumeric characters are permitted:
  - ~`!@$%^&*()_+{}[]|\:;’”<,>.?/ (except # and space)

Diagnostic Dump

The Diagnostic Dump functionality has no particular screen, but simply downloads a log file to the local storage device.

NOTE: It is generally recommended that the Diagnostic Dump functionality be used only at the request of Brivo Technical Support.

1. Click **System** to access the System menu bar.
2. Click **Diagnostic Dump** to begin the download.
3. Once the file is downloaded, the process is complete.

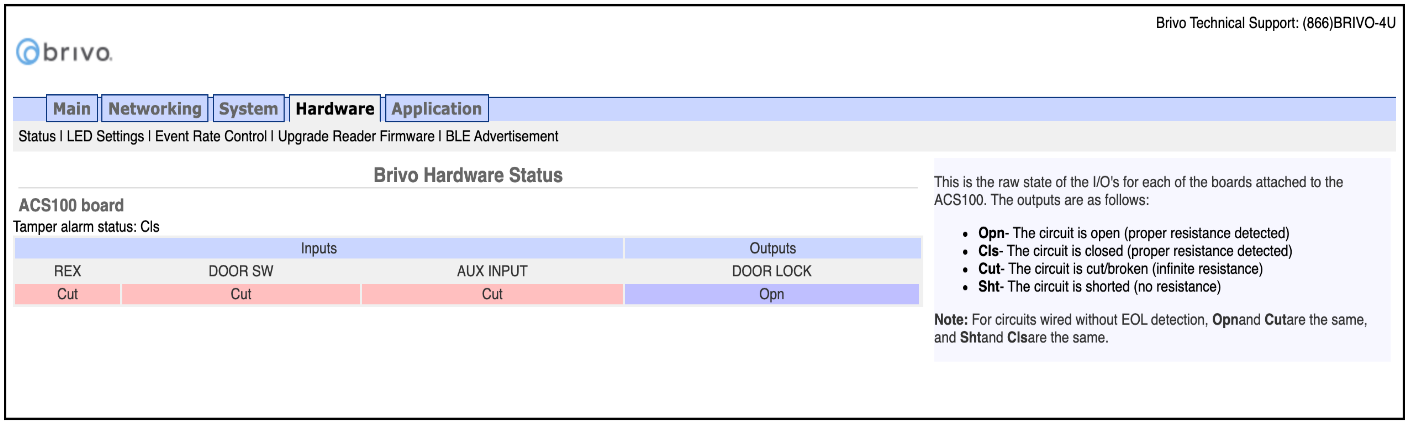
Hardware Tab

The Hardware tab of the Administrative Interface allows you to check the status of the control panel hardware, to change the LED settings for waiting state, to limit the number of notifications reported for certain events, to upgrade firmware for OSDP readers, and manage fluid access and mobile credential functionality.

Status

The Hardware Status page provides a complete view of the state of all major components of the control panel hardware. To access this page:

1. Click **Hardware** to access the Hardware menu bar.
2. Click **Status** to access the Brivo Hardware Status page. Status values are defined in the text on the right side of the page.


brivo
Main
Networking
System
Hardware
Application
Status I LED Settings I Event Rate Control I Upgrade Reader Firmware I BLE Advertisement

Brivo Technical Support: (866)BRIVO-4U

Brivo Hardware Status

ACS100 board

Tamper alarm status: Cls

Inputs			Outputs
REX	DOOR SW	AUX INPUT	DOOR LOCK
Cut	Cut	Cut	Opn

This is the raw state of the I/O's for each of the boards attached to the ACS100. The outputs are as follows:

- **Opn**- The circuit is open (proper resistance detected)
- **Cls**- The circuit is closed (proper resistance detected)
- **Cut**- The circuit is cut/broken (infinite resistance)
- **Sht**- The circuit is shorted (no resistance)

Note: For circuits wired without EOL detection, **Opn**and **Cut**are the same, and **Sht**and **Cls**are the same.

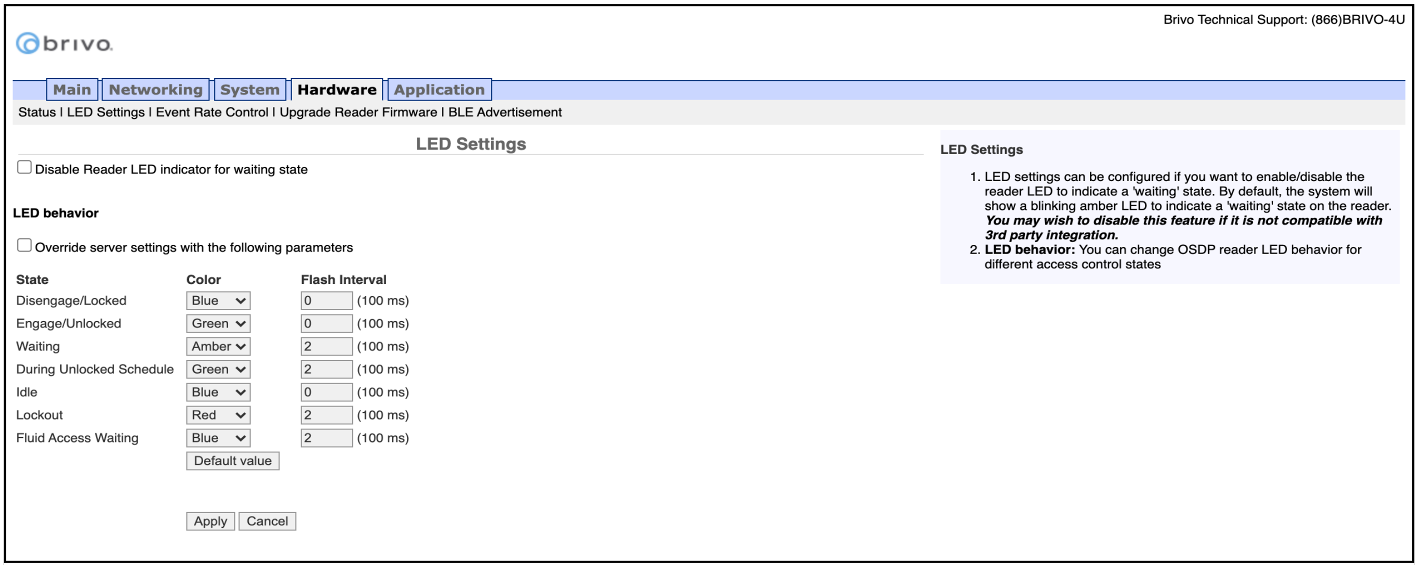
Figure 57: Brivo Hardware Status

LED Settings

The LED Settings page allows the administrator to disable the Reader LED indicator for waiting state. LED settings can be configured if you want to enable/disable the reader LED to indicate a 'waiting' state. By default, the system will show a blinking amber LED to indicate a 'waiting' state on the reader. To access this page:

NOTE: You may wish to disable this feature if it is not compatible with 3rd party integration.

1. Click **Hardware** to access the Hardware menu bar.
2. Click **LED Settings** to access the LED Settings page.
3. Click the **checkbox** to disable the Reader LED indicator for waiting state.
4. Click **Apply** to complete the process.


Brivo Technical Support: (866)BRIVO-4U
Main
Networking
System
Hardware
Application
Status I LED Settings I Event Rate Control I Upgrade Reader Firmware I BLE Advertisement

LED Settings

□ Disable Reader LED indicator for waiting state

LED behavior

□ Override server settings with the following parameters

State	Color	Flash Interval
Disengage/Locked	Blue	0 (100 ms)
Engage/Unlocked	Green	0 (100 ms)
Waiting	Amber	2 (100 ms)
During Unlocked Schedule	Green	2 (100 ms)
Idle	Blue	0 (100 ms)
Lockout	Red	2 (100 ms)
Fluid Access Waiting	Blue	2 (100 ms)

Default value
Apply
Cancel

LED Settings

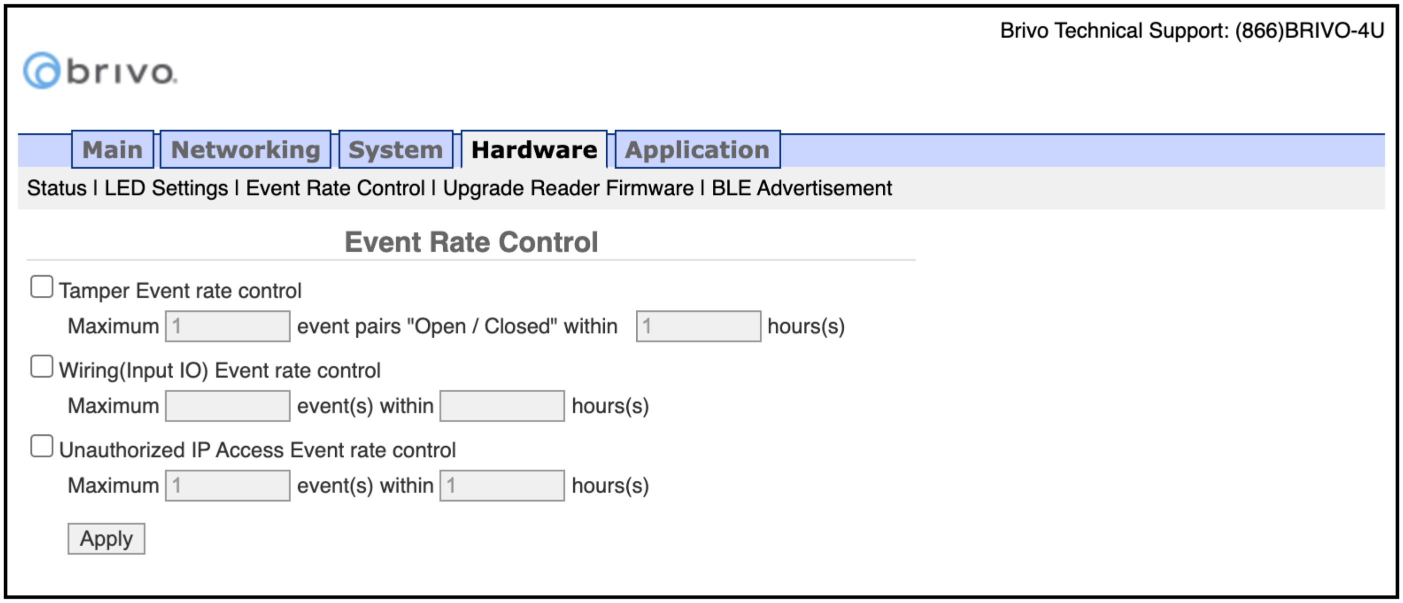
1. LED settings can be configured if you want to enable/disable the reader LED to indicate a 'waiting' state. By default, the system will show a blinking amber LED to indicate a 'waiting' state on the reader. ***You may wish to disable this feature if it is not compatible with 3rd party integration.***
2. **LED behavior:** You can change OSDP reader LED behavior for different access control states

Figure 58: LED Settings

Event Rate Control

The Event Rate Control page allows the administrator to limit the number of notifications reported for Tamper events, Wiring (Input/Output) events, and Unauthorized IP Access Events within a defined period of time.

1. Click **Hardware** to access the Hardware menu bar.
2. Click **Event Rate Control** to access the Event Rate Control page.
3. To limit Tamper event notifications, check the **Tamper Event** rate control checkbox.
4. Enter the maximum number of event pairs (Open/Closed) and the number of hours (the default for each is one).
5. To limit Wiring (Input/Output) event notifications, check the **Wiring (Input IO) Event** rate control checkbox.
6. Enter the maximum number of event(s) and the number of hours (the default for each is one).
7. To limit Unauthorized IP Access Event notifications, check the **Unauthorized IP Access Event** rate control checkbox.
8. Enter the maximum number of event(s) and the number of hours (the default for each is one).
9. Click **Apply** to complete the process.


Brivo Technical Support: (866)BRIVO-4U
brivo
Main
Networking
System
Hardware
Application
Status | LED Settings | Event Rate Control | Upgrade Reader Firmware | BLE Advertisement

Event Rate Control

□ Tamper Event rate control

Maximum 1 event pairs "Open / Closed" within 1 hours(s)

□ Wiring(Input IO) Event rate control

Maximum event(s) within hours(s)

□ Unauthorized IP Access Event rate control

Maximum 1 event(s) within 1 hours(s)

Figure 59: Event Rate Control

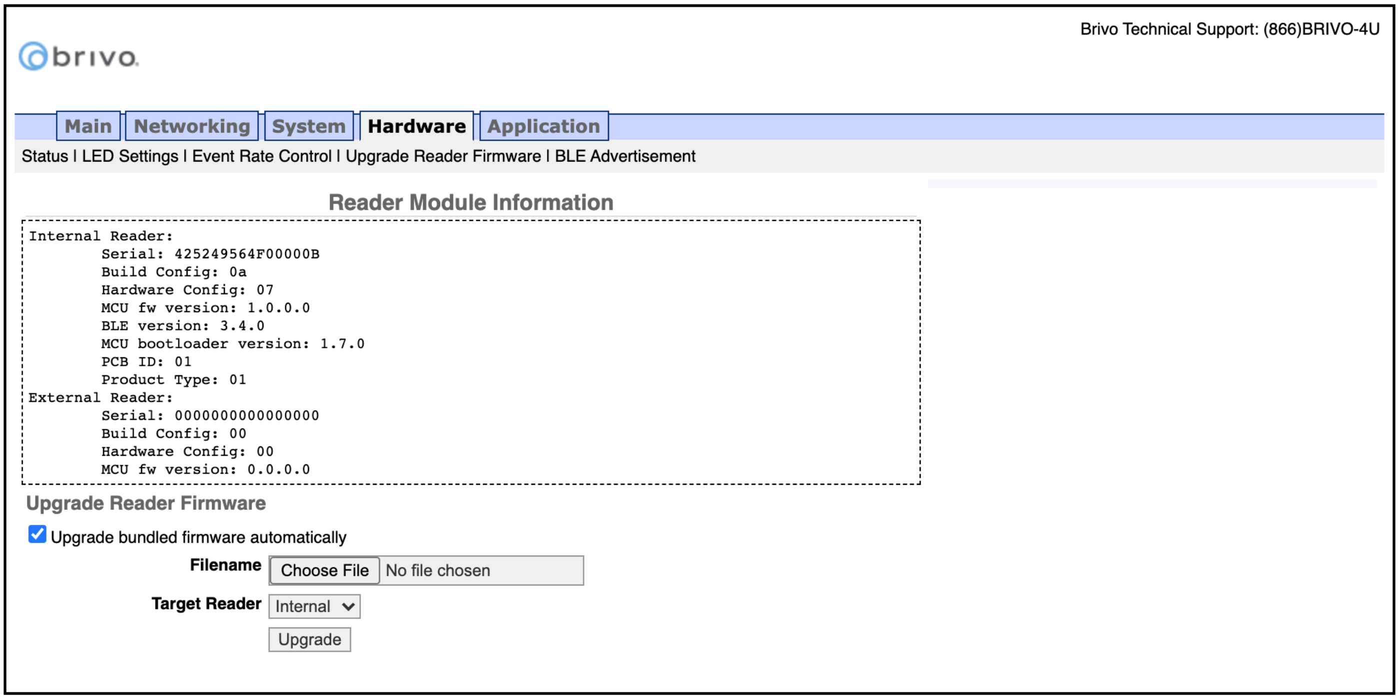
© 2021 Brivo Systems LLC. All rights reserved.

Upgrade Reader Firmware

The Upgrade Reader Firmware page allows the administrator to upgrade the firmware for the built-in OSDP reader and optional OSDP peripheral device attached to the control panel. To access this page:

NOTE: The firmware upgrade file will ONLY be sent by Brivo to the administrator. Do not use any other firmware upgrades files provided from other sources.

1. Click **Hardware** to access the Hardware menu bar.
2. Click **Upgrade Reader Firmware** to access the Reader Module Information page.
3. Firmware upgrades to the **ACS100** may also include firmware upgrades to the OSDP reader(s). To enable the automatic upgrade of bundled firmware, check the **Upgrade bundled firmware automatically** checkbox.
4. To upgrade the firmware of a reader manually, click on **Choose File** and select the firmware upgrade file you wish to use from your local storage device. Select the **Target Reader** from the dropdown menu and then click the **Upgrade** button to begin the firmware upgrade process.


Brivo Technical Support: (866)BRIVO-4U
Main
Networking
System
Hardware
Application
Status I LED Settings I Event Rate Control I Upgrade Reader Firmware I BLE Advertisement

Reader Module Information

```
Internal Reader:
        Serial: 425249564F00000B
        Build Config: 0a
        Hardware Config: 07
        MCU fw version: 1.0.0.0
        BLE version: 3.4.0
        MCU bootloader version: 1.7.0
        PCB ID: 01
        Product Type: 01
External Reader:
        Serial: 0000000000000000
        Build Config: 00
        Hardware Config: 00
        MCU fw version: 0.0.0.0
```

Upgrade Reader Firmware

☑ Upgrade bundled firmware automatically

Filename: No file chosen

Target Reader: Internal

Figure 60: Upgrade Reader Firmware

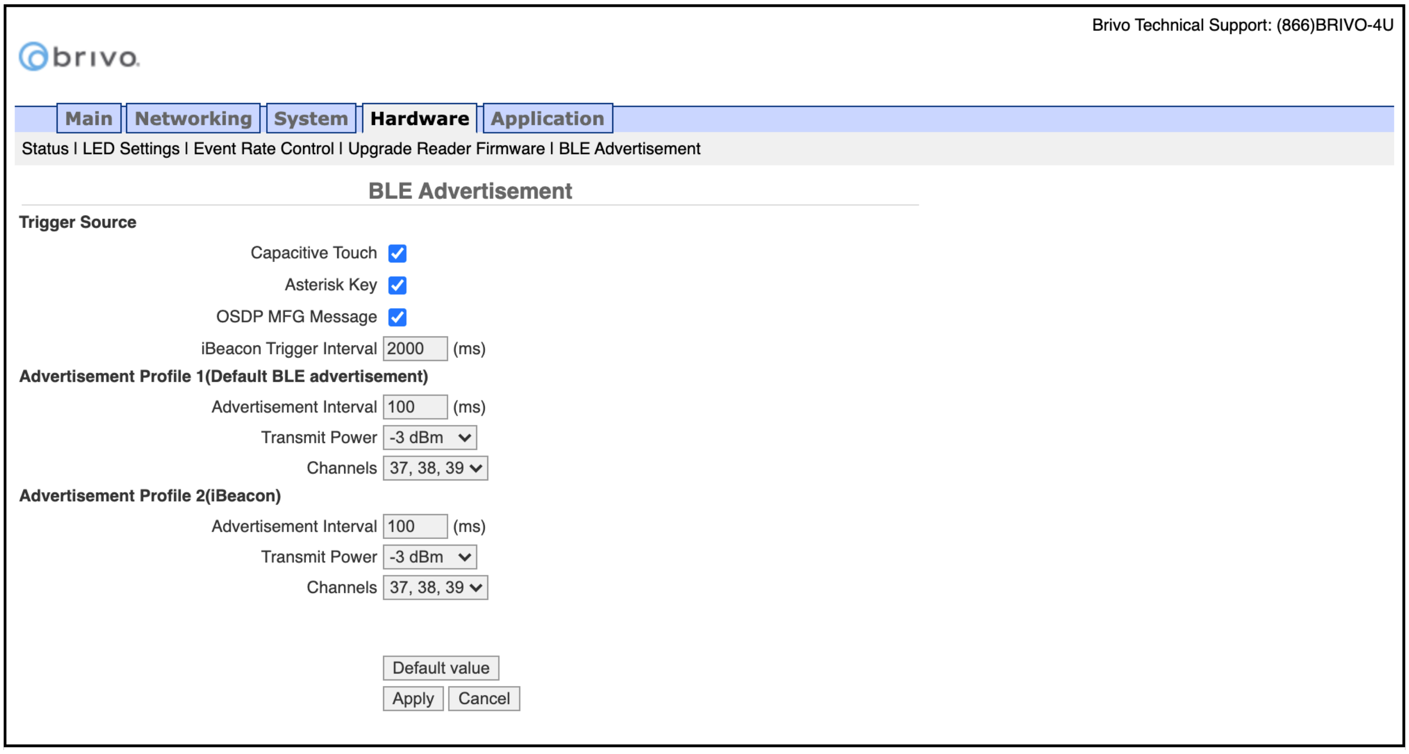
BLE Advertisement

The BLE Advertisement page allows the administrator to manage fluid access and mobile credential functionality of the ACS100 unit and how the unit is used by credential holders.

To access this page:

1. Click **Hardware** to access the Hardware menu bar.
2. Click **BLE Advertisement** to access the BLE Advertisement page.
3. To disable Fluid Access by touch functionality, make sure the **Capacitive Touch** checkbox is unchecked.
4. To disable Fluid Access by pressing the * key (available only on **ACS100** units with keypads), make sure the **Asterisk Key** checkbox is unchecked.
5. If mobile credential devices are not being detected in a pocket or purse, increase the **Transmit Power** DB value.
6. If mobile credential holders are experiencing interference from other Brivo Smart readers or **ACS100** units, decrease the **Transmit Power** DB value.
7. Click **Apply** when finished.

NOTE: Other than the options listed above, other changes to this page should be made ONLY if requested by Brivo Technical Support.


Brivo Technical Support: (866)BRIVO-4U
brivo
Main
Networking
System
Hardware
Application
Status I LED Settings I Event Rate Control I Upgrade Reader Firmware I BLE Advertisement
Default value
Apply
Cancel

BLE Advertisement

Trigger Source

Capacitive Touch ☑

Asterisk Key ☑

OSDP MFG Message ☑

iBeacon Trigger Interval 2000 (ms)

Advertisement Profile 1(Default BLE advertisement)

Advertisement Interval 100 (ms)

Transmit Power -3 dBm

Channels 37, 38, 39

Advertisement Profile 2(iBeacon)

Advertisement Interval 100 (ms)

Transmit Power -3 dBm

Channels 37, 38, 39

Figure 61: BLE Advertisement

Application Tab

The Application tab of the Administrative Interface gives you access to log of control panel events and a set of tools used for diagnosing control panel problems.

Log

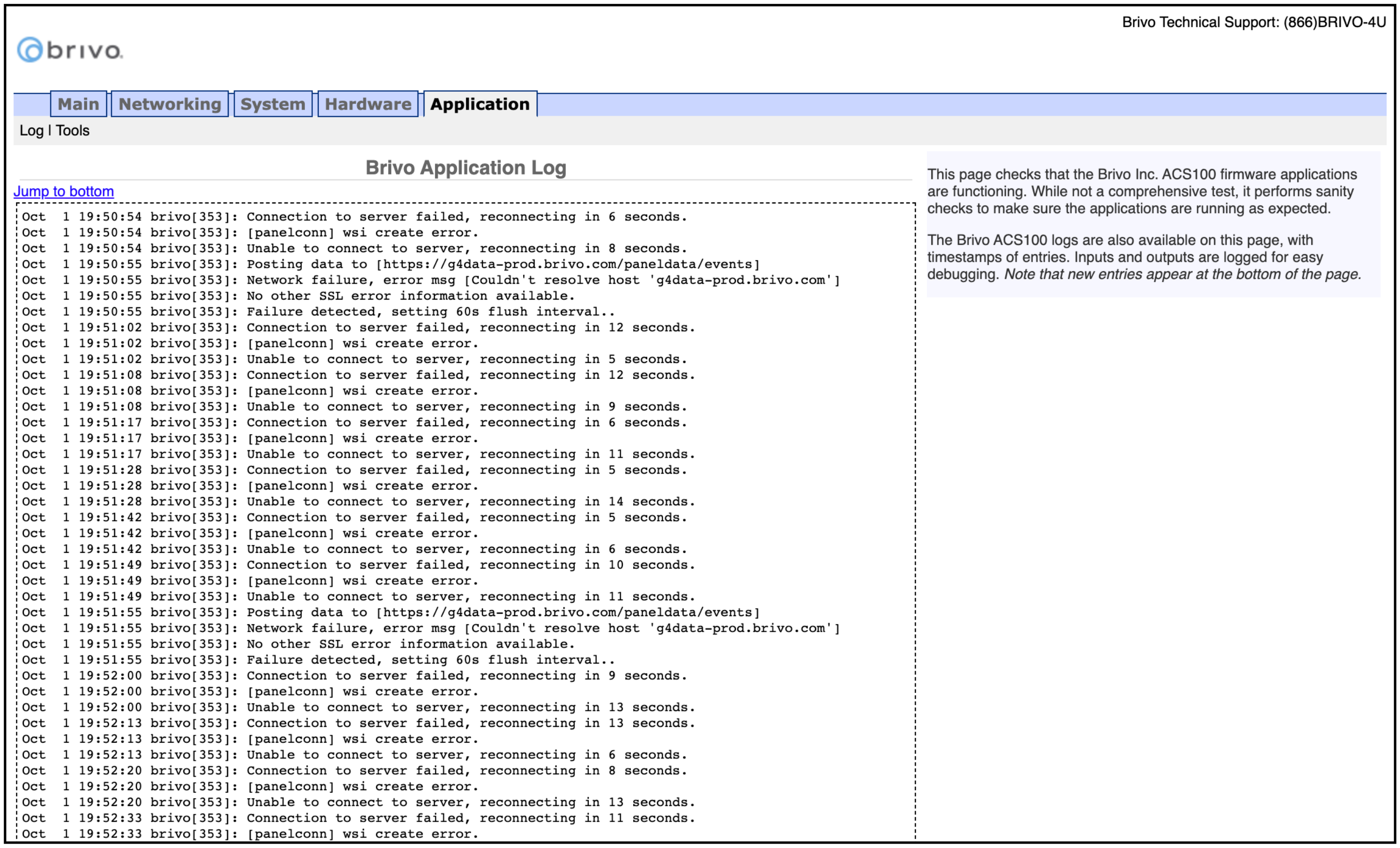
The Application Log contains an entry for every major event that occurs in the control panel. For example, it can answer such questions as:

Did the control panel receive a Wiegand value from the card reader?

Did the control panel detect the door closure switch change of state?

To access this page:

1. Click **Application** to access the Application menu bar.
2. Click **Log** to view the Brivo Application Log.



Brivo Application Log

Jump to bottom

```
Oct  1 19:50:54 brivo[353]: Connection to server failed, reconnecting in 6 seconds.
Oct  1 19:50:54 brivo[353]: [panelconn] wsi create error.
Oct  1 19:50:54 brivo[353]: Unable to connect to server, reconnecting in 8 seconds.
Oct  1 19:50:55 brivo[353]: Posting data to [https://g4data-prod.brivo.com/paneldata/events]
Oct  1 19:50:55 brivo[353]: Network failure, error msg [Couldn't resolve host 'g4data-prod.brivo.com']
Oct  1 19:50:55 brivo[353]: No other SSL error information available.
Oct  1 19:50:55 brivo[353]: Failure detected, setting 60s flush interval..
Oct  1 19:51:02 brivo[353]: Connection to server failed, reconnecting in 12 seconds.
Oct  1 19:51:02 brivo[353]: [panelconn] wsi create error.
Oct  1 19:51:02 brivo[353]: Unable to connect to server, reconnecting in 5 seconds.
Oct  1 19:51:08 brivo[353]: Connection to server failed, reconnecting in 12 seconds.
Oct  1 19:51:08 brivo[353]: [panelconn] wsi create error.
Oct  1 19:51:08 brivo[353]: Unable to connect to server, reconnecting in 9 seconds.
Oct  1 19:51:17 brivo[353]: Connection to server failed, reconnecting in 6 seconds.
Oct  1 19:51:17 brivo[353]: [panelconn] wsi create error.
Oct  1 19:51:17 brivo[353]: Unable to connect to server, reconnecting in 11 seconds.
Oct  1 19:51:28 brivo[353]: Connection to server failed, reconnecting in 5 seconds.
Oct  1 19:51:28 brivo[353]: [panelconn] wsi create error.
Oct  1 19:51:28 brivo[353]: Unable to connect to server, reconnecting in 14 seconds.
Oct  1 19:51:42 brivo[353]: Connection to server failed, reconnecting in 5 seconds.
Oct  1 19:51:42 brivo[353]: [panelconn] wsi create error.
Oct  1 19:51:42 brivo[353]: Unable to connect to server, reconnecting in 6 seconds.
Oct  1 19:51:49 brivo[353]: Connection to server failed, reconnecting in 10 seconds.
Oct  1 19:51:49 brivo[353]: [panelconn] wsi create error.
Oct  1 19:51:49 brivo[353]: Unable to connect to server, reconnecting in 11 seconds.
Oct  1 19:51:55 brivo[353]: Posting data to [https://g4data-prod.brivo.com/paneldata/events]
Oct  1 19:51:55 brivo[353]: Network failure, error msg [Couldn't resolve host 'g4data-prod.brivo.com']
Oct  1 19:51:55 brivo[353]: No other SSL error information available.
Oct  1 19:51:55 brivo[353]: Failure detected, setting 60s flush interval..
Oct  1 19:52:00 brivo[353]: Connection to server failed, reconnecting in 9 seconds.
Oct  1 19:52:00 brivo[353]: [panelconn] wsi create error.
Oct  1 19:52:00 brivo[353]: Unable to connect to server, reconnecting in 13 seconds.
Oct  1 19:52:13 brivo[353]: Connection to server failed, reconnecting in 13 seconds.
Oct  1 19:52:13 brivo[353]: [panelconn] wsi create error.
Oct  1 19:52:13 brivo[353]: Unable to connect to server, reconnecting in 6 seconds.
Oct  1 19:52:20 brivo[353]: Connection to server failed, reconnecting in 8 seconds.
Oct  1 19:52:20 brivo[353]: [panelconn] wsi create error.
Oct  1 19:52:20 brivo[353]: Unable to connect to server, reconnecting in 13 seconds.
Oct  1 19:52:33 brivo[353]: Connection to server failed, reconnecting in 11 seconds.
Oct  1 19:52:33 brivo[353]: [panelconn] wsi create error.
```

This page checks that the Brivo Inc. ACS100 firmware applications are functioning. While not a comprehensive test, it performs sanity checks to make sure the applications are running as expected.

The Brivo ACS100 logs are also available on this page, with timestamps of entries. Inputs and outputs are logged for easy debugging. *Note that new entries appear at the bottom of the page.*

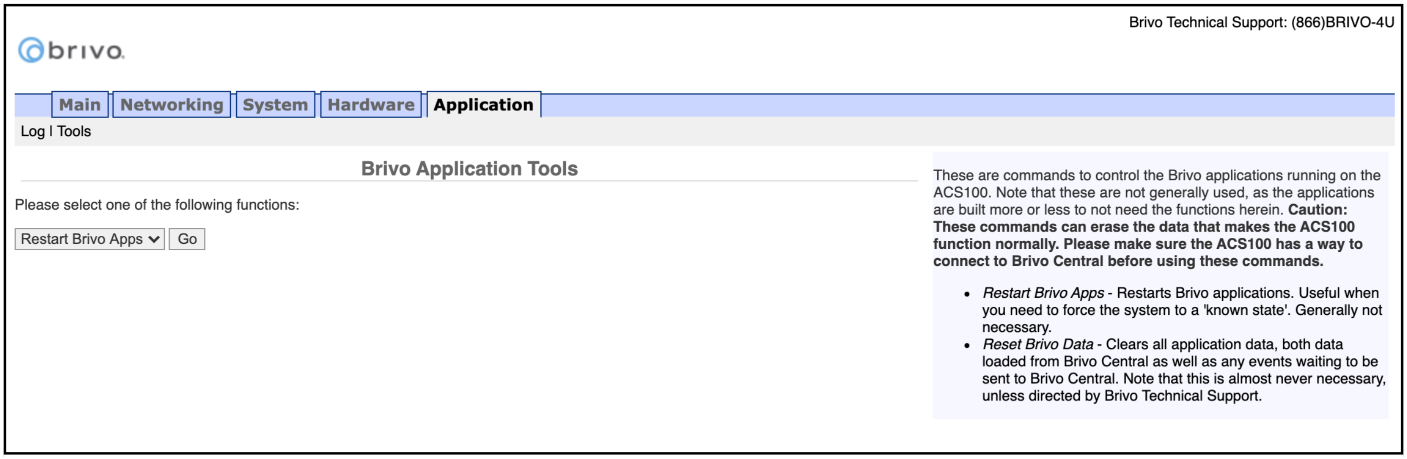
Figure 62: Brivo Application Log

© 2021 Brivo Systems LLC. All rights reserved.

Tools (Application)

The Brivo Application Tools page provides access to two commands that are used only as part of diagnostic procedures where you might suspect that the panel is not operating correctly or data may have been corrupted. To access this page:

1. Click **Application** to access the Application menu bar.
2. Click **Tools** to access the Brivo Application Tools page.
3. From the pull-down menu, select:
   a. **Restart Brivo Apps** to shut down the access control applications on the control panel, and then restart them. Generally, this command should be used only when Brivo Technical Support requests that you do so.
   b. **Reset Brivo Data** to erase the local database of credentials, schedules, door settings, etc., and forces the control panel to reacquire all this information from the Brivo Cloud Server. This
   command should be used only if you suspect that the local data has been corrupted, or if requested by Brivo Technical Support.



Brivo Application Tools

Please select one of the following functions:

Restart Brivo Apps ▾ Go

These are commands to control the Brivo applications running on the ACS100. Note that these are not generally used, as the applications are built more or less to not need the functions herein. **Caution: These commands can erase the data that makes the ACS100 function normally. Please make sure the ACS100 has a way to connect to Brivo Central before using these commands.**

- *Restart Brivo Apps* - Restarts Brivo applications. Useful when you need to force the system to a 'known state'. Generally not necessary.
- *Reset Brivo Data* - Clears all application data, both data loaded from Brivo Central as well as any events waiting to be sent to Brivo Central. Note that this is almost never necessary, unless directed by Brivo Technical Support.

Figure 63: Brivo Application Tools

Troubleshooting (ACS100)

The following sections provide material to help ensure that the Brivo control panel networking is operating properly.

Network Connectivity

If your Brivo control panel is properly configured for the network, your network administrator should be able to see that it has received an IP address from the local DHCP server. Ask your network administrator to check the "DHCP Clients Table" on the DHCP server. There should be one entry for each control panel you have installed.

Pinging the Control Panel from another Computer

Your network administrator may use the "ping" utility on another computer on the network to test connectivity to the Brivo control panel. To use ping on a Windows computer, follow these steps:

1. In the **Start** menu, select **Run**.
2. When the Run dialog box opens, enter **command** in the Open field. A DOS window displays.
3. Type **ping NNN.NNN.NNN.NNN** where the N's stand for the IP address of the Brivo control panel. You can get this address from the DHCP server or from the Network Status page of the Administrative Interface on the control panel itself.
4. Read the results of the ping command.
5. If successful, it will provide packet response times and other information.
6. If not, it will say that the node could not be reached.

Pinging another Computer from the Control Panel

You may also wish to verify correct network operation by using the command line interface to ping another computer on your network or on the Internet.

1. Log into the control panel's Administrative Interface as described in "Accessing the Administrative Interface."
2. Click **Networking**, and then click **Tools** from the Networking men bar.
3. Enter the **IP address** or full network name of another computer that is known to have network connectivity in the **Target** field and click **Go**.
4. If successful, you should see a response like the following within a few seconds:

```
PING 192.168.192.107 (192.168.192.107): 56 data bytes
64 bytes from 192.168.192.107: icmp_seq=0 ttl=128 time=0.9 ms
64 bytes from 192.168.192.107: icmp_seq=1 ttl=128 time=0.8 ms
64 bytes from 192.168.192.107: icmp_seq=2 ttl=128 time=0.8 ms
64 bytes from 192.168.192.107: icmp_seq=3 ttl=128 time=0.8 ms
64 bytes from 192.168.192.107: icmp_seq=4 ttl=128 time=0.9 ms
--- 192.168.192.107 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.8/0.8/0.9 ms
```

© 2021 Brivo Systems LLC. All rights reserved.

Connectivity to Brivo Cloud Server

Follow the steps in the Brivo Quick Start Guide to make sure that you have performed all the tasks necessary to set up your account. In particular, you should at least have registered the control panel you are testing.

Connectivity to the Brivo Cloud Server can be verified by using the Network Troubleshooting Assistant.

1. Log into the control panel's Administrative Interface as described in "Accessing the Administrative Interface."
2. Click **Networking**, and then click **Troubleshooting** on the Networking menu bar.
3. If all the tests listed on that page show a green "**PASS**," the control panel is connected to the Brivo Cloud Server.

Additional Troubleshooting

For additional assistance to questions not answered in this troubleshooting section, please refer to www.brivo.com or contact Brivo Technical Support.

© 2021 Brivo Systems LLC. All rights reserved.

Revision Table

Revision Number	Author	Date	Description
1.0	LMW	10/09/15	Original draft
1.1	LMW	03/06/17	Incorporated -A panel language
1.2	LMW	03/27/17	Added Wi-Fi configuration
1.3	LMW	05/04/17	Updated screenshots
1.4	LMW	05/24/17	Added System Configuration and Diagnostic Dump instructions
1.5	LMW	10/11/17	Corrected error on page 20
1.6	LMW	11/30/17	Updated Wi-Fi section to describe Scan Network functionality
1.7	LMW	02/02/18	Added username/password change functionality
1.8	LMW	02/13/19	Added cellular network module, connection priority functionality, and proxy server options for cellular connectivity
1.9	LMW	080/6/20	Added OSDP addressing clarification
1.10	LMW	08/19/20	Added ACS100 chapter
1.11	LMW	10/15/20	Added Logging feature
1.12	LMW	04/20/21	Added BLE Advertisement to ACS6000/ACS300 section and updated LED Controls section
1.13	LMW	07/15/21	Replaced Onair references with Access and updated password change recommendations on first login.

PUB-Panel Networking Guide_v1.13