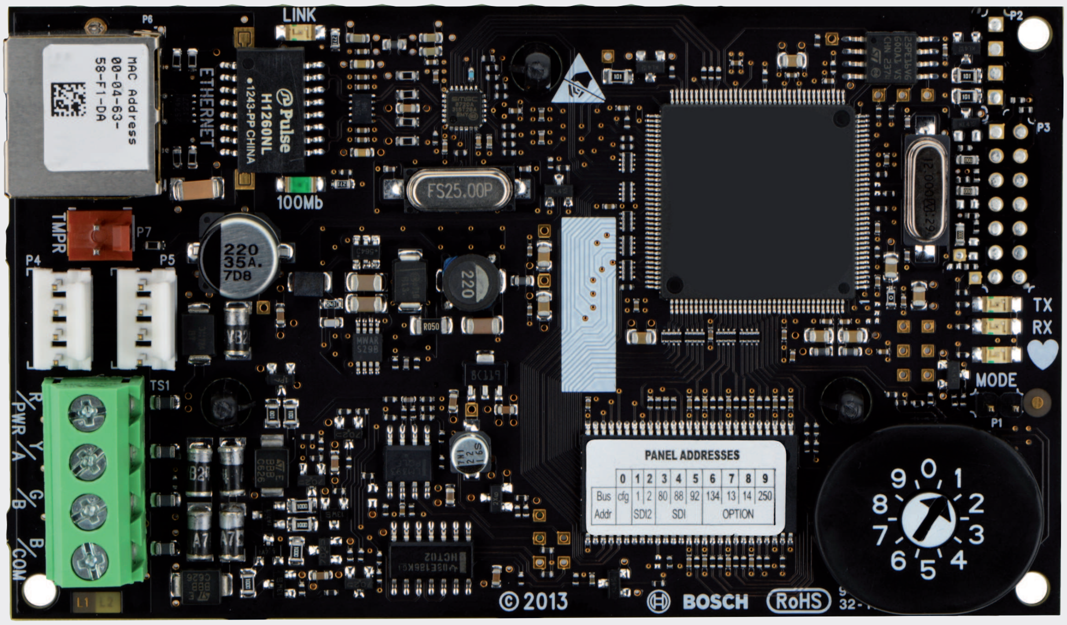


Conettix Ethernet Communication Module

B426

en Installation and Operation Guide

Table of contents

1 Safety

ESD Precaution

Please note that the B426 board comes without any case/box and all components are exposed for finger touches - therefore extra attention must be paid to ESD (electrostatic discharge) precaution. Make sure there is no static interference when using the board. Appropriate ESD protections must be taken and wearing electrostatic equipment is recommended, such as anti-static wrist strap.
ESD damage can range from subtle performance degradation to complete device failure.
Precision integrated circuits may be more susceptible to damage because very small parametric changes could cause the device not to meet its published specifications.

Warning!
Failure to follow these instructions can result in a failure to initiate alarm conditions. Bosch Security Systems, Inc. is not responsible for improperly installed, tested, or maintained devices. Follow these instructions to avoid personal injury and damage to the equipment.

Notice!
Inform the operator and the local authority having jurisdiction (AHJ) before installing the module in an existing system.
Disconnect all power to the control panel before installing the module.
Before installing a B426, refer to *Technical specifications, page 33*.

2 Introduction

This section includes basic documentation information and an installation checklist.

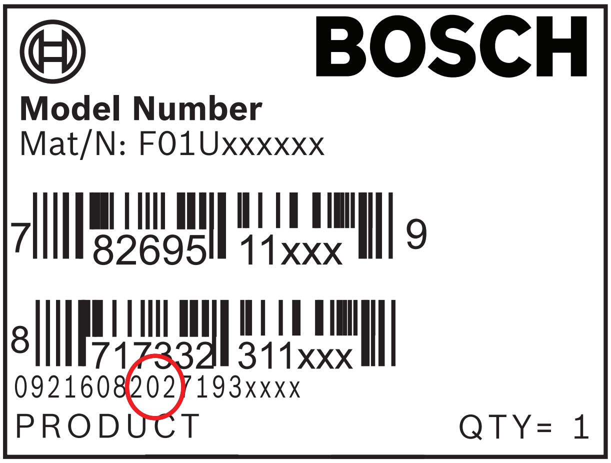
2.1 About documentation

Copyright
This document is the intellectual property of Bosch Security Systems, Inc. and is protected by copyright. All rights reserved.

Trademarks
All hardware and software product names used in this document are likely to be registered trademarks and must be treated accordingly.

2.2 Bosch Security Systems, Inc. product manufacturing dates

Use the serial number located on the product label and refer to the Bosch Security Systems, Inc. website at http://www.boschsecurity.com/datecodes/.
The following image shows an example of a product label and highlights where to find the manufacturing date within the serial number.



2.3 Installation workflow

To install and configure the module, use the workflow below. Follow in sequential order from top to bottom. Check off each box as you complete a step.

Caution!
Always power down the control panel when connecting a module. To power down the control panel, unplug the transformer and disconnect the battery.

□ Plan the installation. Refer to *System overview, page 7*.

□ Set the address switch. Refer to *Bus address settings, page 9*.

□ Install the module. Refer to *Mount the module in the enclosure, page 10*, *Mount and wire the tamper switch (optional), page 10*, and *Wire to the control panel, page 10*.

□ Configure the module. Refer to *Plug and Play configuration for SDI2 or option bus control panels, page 13*, or *Plug and Play configuration for SDI or option bus control panels, page 13*, or *Web-based configuration, page 13*.

□ Verify operation using the LEDs. Refer to *Maintenance and troubleshooting LEDs, page 30*.

3 System overview

Use the B426 for bi-directional communication over an Ethernet network.

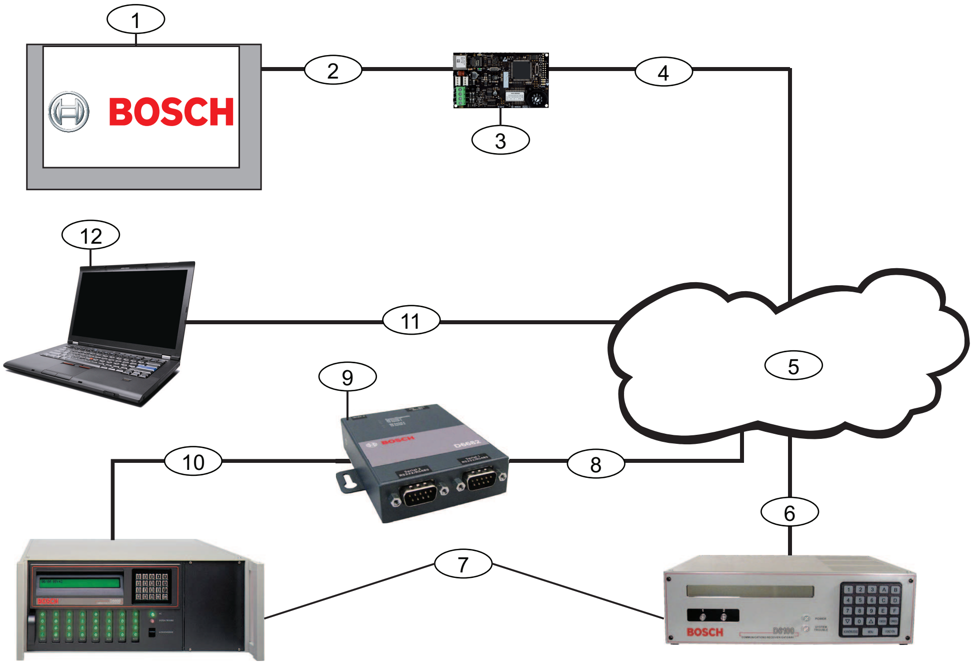


Figure 3.1: B426 system connections overview

Callout — Description	**Callout — Description**
1 — Compatible Bosch control panel	7 — Conettix D6100i Communications Receiver/Gateway and/or Conettix D6600 Communications Receiver/Gateway (Conettix D6600 Communications Receiver/Gateway requires 8, 9, and 10)
2 — Data bus connection between the control panel and the module	8 — Ethernet network connection to the Ethernet adapter (D6680/ITS-D6682/ITS-D6686) (ITS-D6682 shown) Ethernet Network Adapter
3 — B426	9 — Conettix Ethernet Network Adapter (ITS-D6682 shown)
4 — Ethernet connection between module and Ethernet network	10 — Connection from ITS-D6682 to the COM4 Port on the Conettix D6600 Communications Receiver/Gateway
5 — Ethernet network, Local Area Network (LAN), Metropolitan AreaNetwork (MAN), Wide Area Network (WAN), or Internet	11 — Ethernet network connection between the host computer Ethernet network interface card (NIC) and the Ethernet network
6 — Ethernet network connection to the D6100i Communications Receiver (D6100i/D6100IPv6)	12 — Host PC running Remote Programming Software, Automation, or the Conettix D6200 Programming/Administration Software

B426 module overview

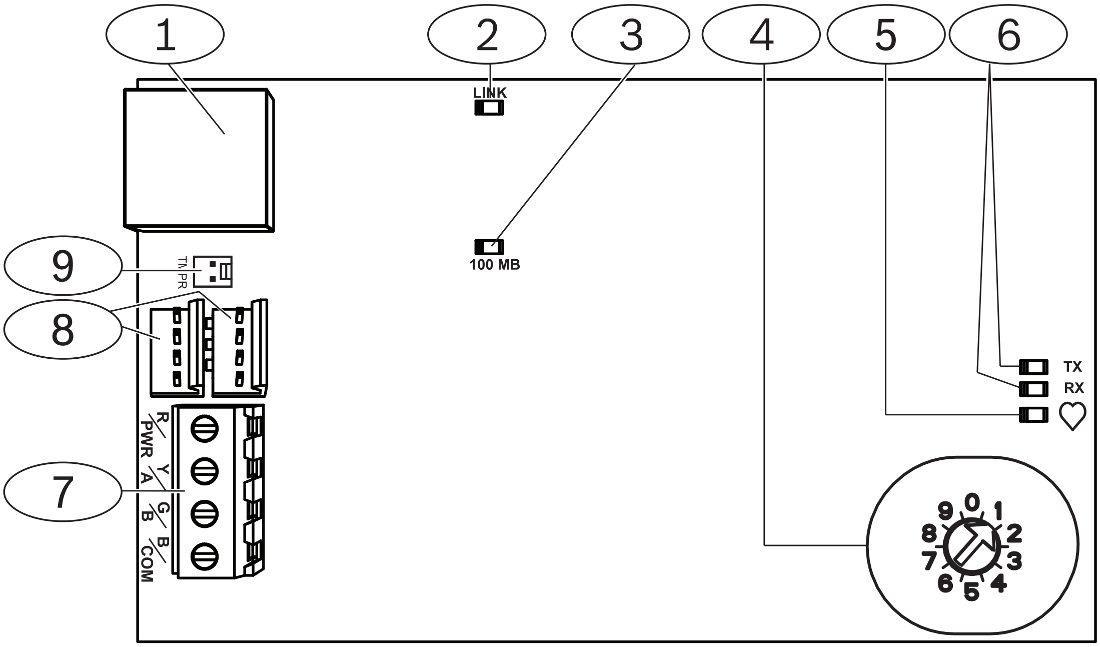


Figure 3.2: B426 Conettix Ethernet Communication Module

Callout — Description
1 — Ethernet RJ-45 port
2 — Yellow LINK LED
3 — Green 100MB LED
4 — Address switch
5 — Heartbeat LED
6 —TX and RX LEDs
7 — Terminal strip (to control panel)
8 — Interconnect wiring connectors (to control panel or other compatible modules)
9 — Tamper switch connector

3.1 Overview

The B426 Conettix Ethernet Communication Module is a four-wire powered SDI, SDI2, or option bus device that provides two-way communication with compatible control panels over IPv6 or IPv4 Ethernet networks.

The B426 on-board switch determines the bus address of the device. Perform configuration of the B426 through the B426 configuration web pages. Additional configuration options include:

- B9512G/B8512G, B6512/B5512/B4512/B3512, D9412GV4/D7412GV4 v2.xx. SDI2 keypad and Remote Programming Software (RPS) configuration.
- AMAX 2000/2100/3000/4000 . A-Link configuration.

The B426 Conettix Ethernet Communication Module is compatible with IPv6.

For ULC-S559, the B426 can be used for either active or passive communication. For passive communication, maximum check in is 24 hours. For active communication, maximum check in (heartbeat) is 89 seconds. NIST encryption is required.

3.2 Bus address settings

The address switch determines the bus type and the module’s address on the bus. The control panel uses the address for communications. Use a slotted screwdriver to set the address switch.

Notice!
The module reads the address switch setting only during module power up. If you change the setting after you apply power to the module, you must cycle the power to the module in order for the new setting to take effect.

The B426 address switch provides the value for the module's address. The figure below shows the address switch setting for address 1. Refer to the following table for panel-specific settings.

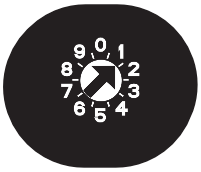


Figure 3.3: Address switch set to address 1

Control panels	Switch position	Control panel address	Bus type	Function
B9512G/B8512G, B6512/ B5512/B4512/B3512, GV4, Solution 2000/3000	1	1	SDI2	Automation, Remote Programming, or Reporting
B9512G/B8512G, GV4, Solution 2000/3000	2	2		
GV4, GV3, GV2, D9412G/ D7412G/D7212G v6.3 or higher	3	80	SDI	Automation
GV4, GV3, GV2, D9412G/ D7412G/D7212G v6.3 or higher	4	88		Reporting or Remote Programming
GV4, GV3	5	92		
FPD-7024 v1.06+, DS7240V2, DS7220V2, Easy Series V3+, AMAX Series, CMS Series	6	134	Option	
DS7400Xi	7	13		
DS7400Xi	8	14		Reporting
FPD-7024, AMAX Series, CMS Series	9	250		Reporting or Remote Programming

Tab. 3.1: B426 address switch settings

4 Installation

After you set the address switch for the proper address, install the module in the enclosure and then wire the module to the control panel and to the Ethernet connection.

4.1 Mount the module in the enclosure

Mount the B426 into the enclosure’s 3-hole mounting pattern using the supplied mounting screws and mounting bracket.
For UL certified systems, mount the module in the control panel enclosure or in a UL listed enclosure (for example, the D8103 Universal Enclosure).
House all communicators in tampered enclosures, compliant with the following clauses within Standard CAN/ULC-S304-06: 5.2.6; 5.2.9; 5.2.10 and 5.2.15.

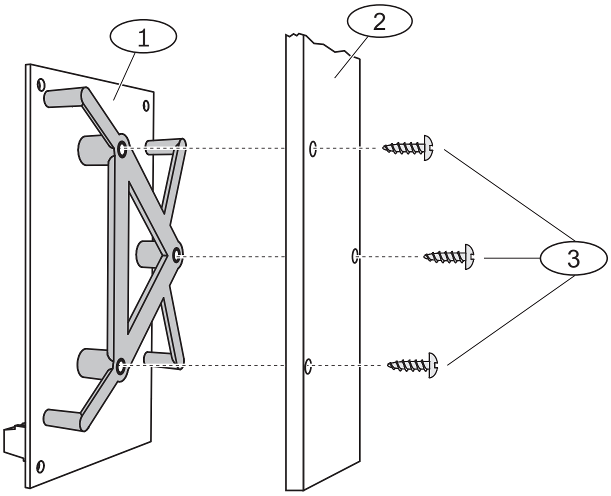


Figure 4.1: Mounting the module

Callout — Description
1 — B426 with mounting bracket installed
2 — Enclosure
3 — Mounting screws (3)

4.2 Mount and wire the tamper switch (optional)

For B9512G/B8512G, B6512/B5512/B4512/B3512, and GV4 v.2xx control panels, you can connect an enclosure door tamper switch for one module in an enclosure.

Installing the optional tamper switch for use with a B426:

1. Mount the ICP-EZTS Cover and Wall Tamper Switch (P/N: F01U009269) into the enclosure’s tamper switch mounting location. For complete instructions, refer to *the Cover and Wall Tamper Switch (ICP- EZTS) Installation Guide* (P/N: F01U003734).
2. Plug the tamper switch wire onto the module’s tamper switch connector. For the tamper switch connector location, refer to *B426 module overview, page 8*.

4.3 Wire to the control panel

When you wire a B426 to an SDI or SDI2 control panel, you can use either the module's terminal strip labeled R, Y, G, B (PWR, A, B, COM) or the module's interconnect wiring connectors (wire included). The figure below indicates the location of both the terminal strip and the interconnect wiring connectors on the module.

Notice!
Remove all power (AC and Battery) before making any connections. Failure to do so may result in personal injury and/or equipment damage.

Notice!
Use either the terminal strip wiring **or** interconnect cable to wire to the control panel. Do not use both. When connecting multiple modules, you can combine terminal strip and interconnect wiring connectors in series.

Run the wiring connections from the module to the data bus terminals on the compatible control panel. Connect the Ethernet cable to the Ethernet port on the module.

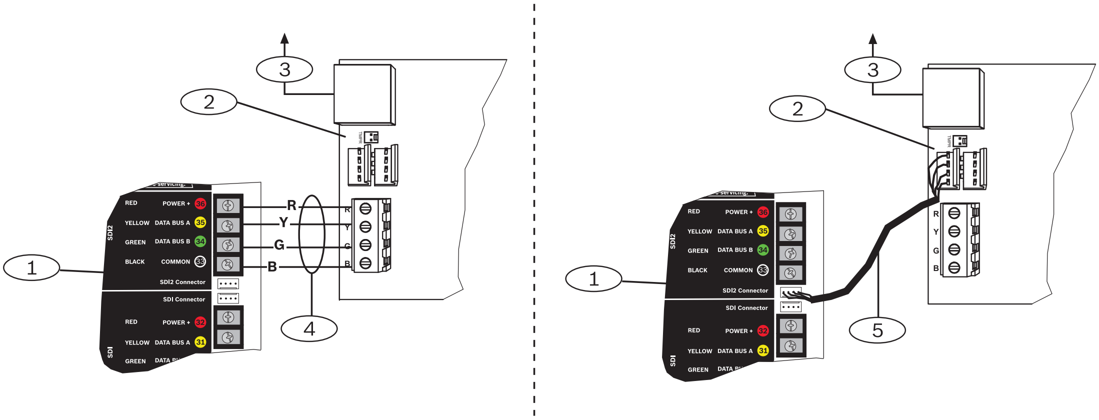


Figure 4.2: Using terminal strip or interconnect cable wiring (GV4 control panel shown)

Callout — Description
1 — SDI2 control panel. For SDI control panels, wire R, Y, G, B to the SDI bus.
2 — Module
3 — To Ethernet network
4 — Terminal strip wiring
5 — Interconnect cable (P/N: F01U079745) (included)

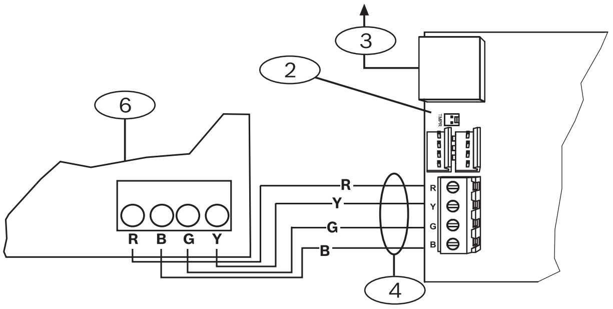


Figure 4.3: Wiring to an option bus terminal strip

Callout — Description
1 — Compatible control panel (FPD-7024 control panel shown)
2 — Module

3 — To Ethernet network
4 — Terminal strip wiring

For complete wiring instructions, refer to the control panel documentation.

5 Configuration

You can configure the B426 using one of the methods described in this section for your control panel type:

- *Plug and Play configuration for SDI2 or option bus control panels, page 13*
- *Plug and Play configuration for SDI or option bus control panels, page 13*
- *Web-based configuration, page 13* (all compatible control panel types)

5.1 Plug and Play configuration for SDI2 or option bus control panels

Notice!
Option bus control panels include AMAX 2100/3000/4000 firmware version v1.5 or higher.

By default, when connecting a field replacement B426 to an existing SDI2 or option bus control panel, the control panel overrides the module settings. To keep custom module settings when you connect a module to a configured control panel, you must disable Panel Programming Enable using web-based configuration, prior to connecting to the SDI2 or option bus.

When connected to a non-default SDI2 or option bus control panel, the control panel automatically configures a connected module.

1. Set the address switch to the correct address for the control panel if not already set (SDI2 control panels use address 1 or 2, option bus control panels use address 134 or 250).
2. Connect the module to the control panel bus and apply power.
3. Program the control panel communication settings using RPS for SDI2 control panels, A-Link for option bus control panels, or the keypad.

The control panel stores the module settings and automatically programs the connected module. To override automatic module programming, use the web configuration pages to set the Panel Programming Enable parameter to **NO** before installing.

5.2 Plug and Play configuration for SDI or option bus control panels

When installing under the following conditions, the B426 needs no further configuration:

- DHCP is available on your network.
- AES encryption is not required.
- Default B426 port settings (UDP on Port 7700) are permitted by the network administrator.

5.3 Web-based configuration

For installations requiring non-default configuration, use the B426 web-based configuration pages.

Notice!
When connected to a B9512G/B8512G, B6512/B5512/B4512/B3512, or D9412GV4/D7412GV4/D7212GV4 control panel, configuration for the module must have the Web Access Enable option set to Yes in order to access or configure the module over the web.

To use the B426 configuration pages, you need the module's IP address or hostname. Refer to either:

- *Module hostname, page 35*

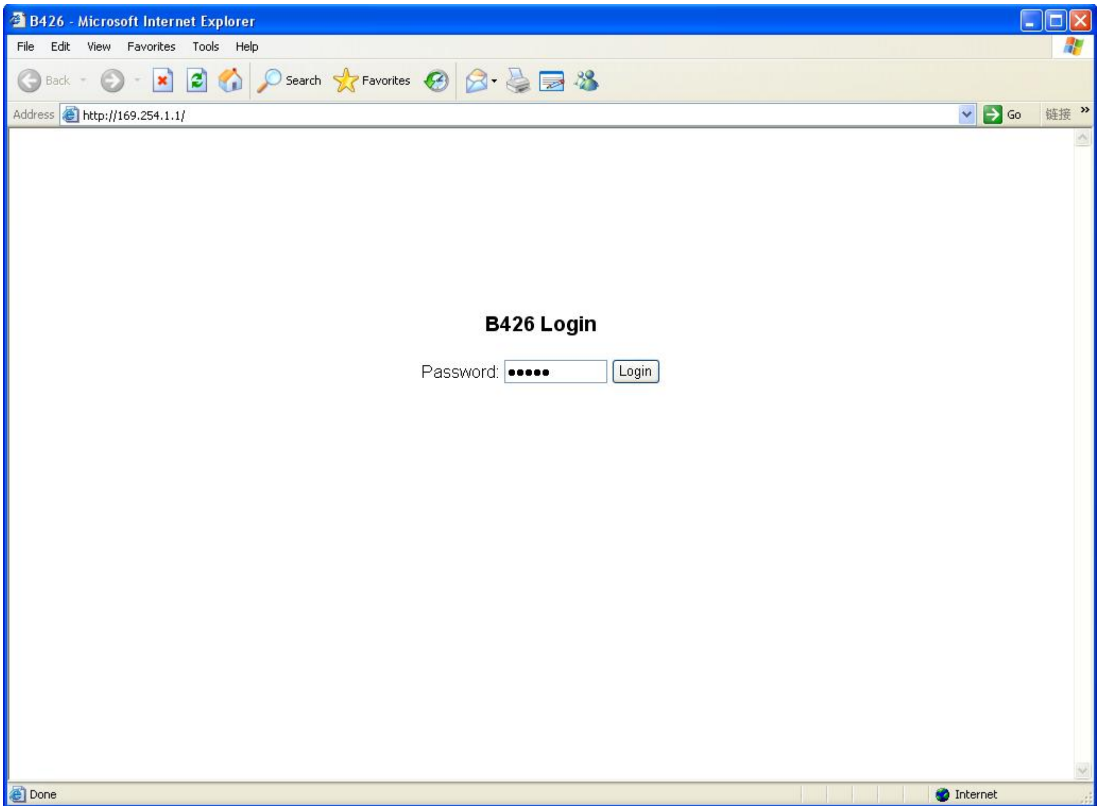
– *Module IP address, page 35*

5.3.1 Web-based configuration log in and use

Notice!
If you cannot connect to the module, you might need to change the web browser configuration so that it does not use a proxy server. Refer to the browser’s online help for instructions on disabling proxy service.

Using web-based configuration (B426 Configuration Pages):

1. Open an internet browser (Microsoft Internet Explorer 6 or higher, or Mozilla Firefox 3 or higher), type in the B426’s IP address or hostname, and press [Enter]. (If Web and Automation Security is enabled on the B426, you must type **https://** instead of **http://**). The B426’s **Login** page opens.


B426 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://169.254.1.1/
Go
链接
Done
Internet

B426 Login

Password: ●●●●● Login

Figure 5.1: B426 Login page

2. Enter the password (default is *B42V2*) and click **Login**. The **Device Information** home page opens. (Refer to *Device Information (home) page , page 15*.)
3. Browse to the desired settings page.
4. When you’ve finished making changes on the page, click **OK**.

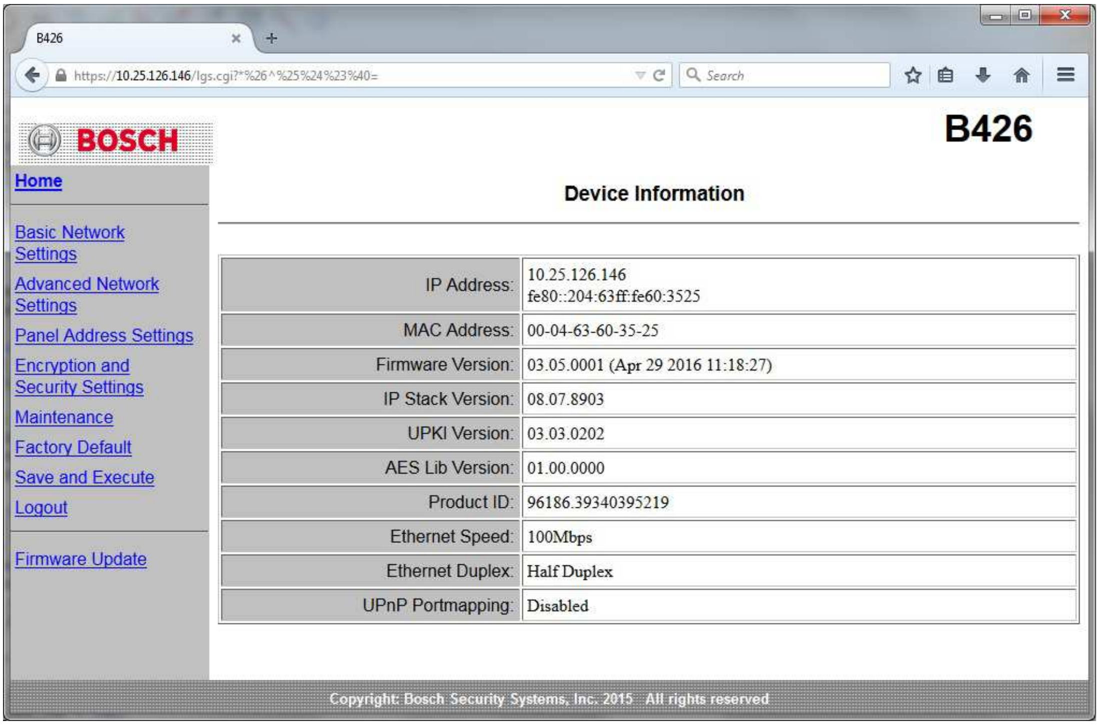
Notice!
Before browsing to a new settings page, you must click **OK** to save edited values.

5. Click **Save & Execute** to save and apply all changes to the device.

You should change your password from the default to secure module configuration. Change the Web Access Password using the **Maintenance** page.

5.3.2 Device Information (home) page

The **Device Information** page shows basic information for the module in its main pane, and provides links to the configuration web pages along the left-hand side.


B426
https://10.25.126.146/lgs.cgi?*%26^%25%24%23%40=
Search
BOSCH
Home
Basic Network Settings
Advanced Network Settings
Panel Address Settings
Encryption and Security Settings
Maintenance
Factory Default
Save and Execute
Logout
Firmware Update
Copyright: Bosch Security Systems, Inc. 2015 All rights reserved

B426

Device Information

IP Address:	10.25.126.146 fe80::204:63ff:fe60:3525
MAC Address:	00-04-63-60-35-25
Firmware Version:	03.05.0001 (Apr 29 2016 11:18:27)
IP Stack Version:	08.07.8903
UPKI Version:	03.03.0202
AES Lib Version:	01.00.0000
Product ID:	96186.39340395219
Ethernet Speed:	100Mbps
Ethernet Duplex:	Half Duplex
UPnP Portmapping:	Disabled

Figure 5.2: Device Information page

5.3.3 Change and save settings using the web

The settings for the module are grouped by topic in the left column of the web interface in the module menu structure.

Some settings (menu options) might be unavailable if:

- The setting conflicts with another configured setting (for example, the **Static IP** setting is unavailable when DHCP is enabled).
- The setting conflicts with the address setting (for example, the **Panel Address** setting is read-only if the address switch is set to anything but 0).
- The setting is unavailable in the current product release.

Saving settings using the Web

To preserve edited values, click the **OK** button on each page before navigating to a different setting page (menu).

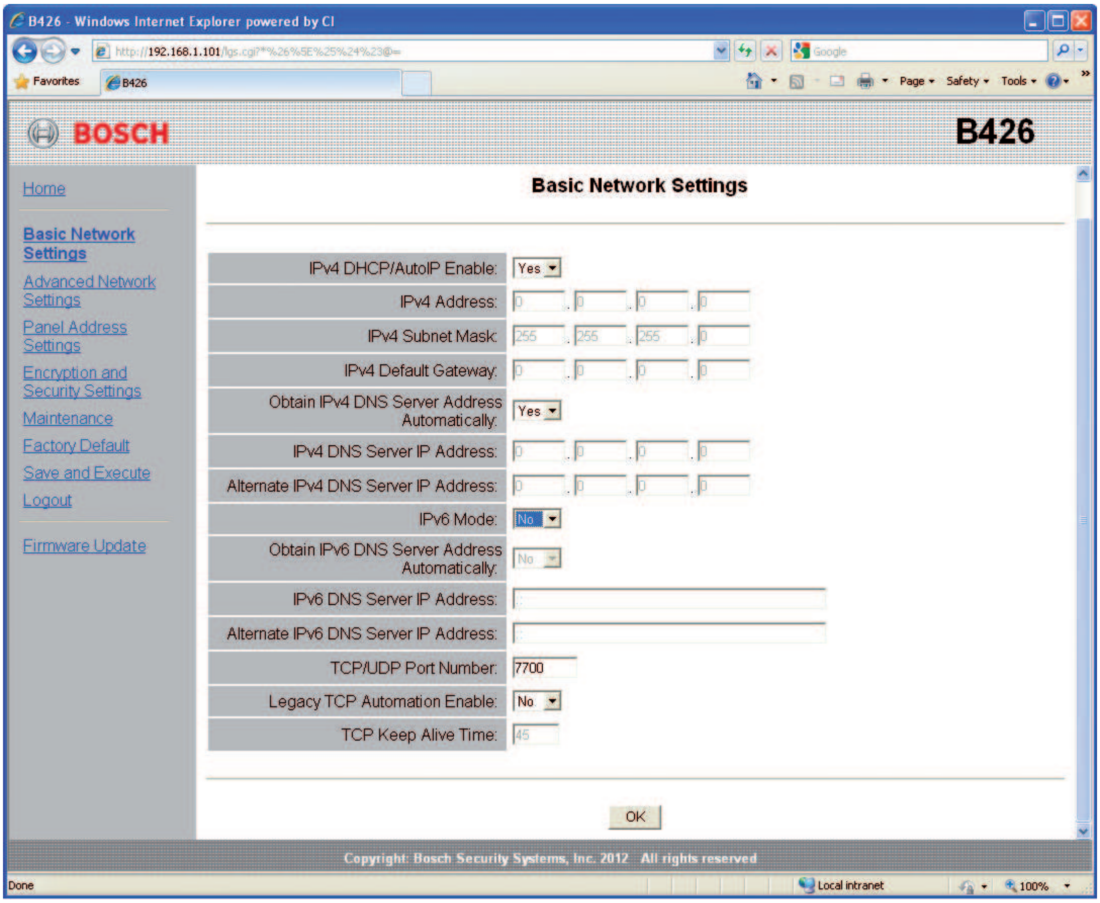
To save all edited values and apply them to the module, click the **Save and Execute** link.

Notice!

Saving the settings might cause the module to terminate the current web browsing session.

5.3.4 Basic Network Settings page

The **Basic Network Settings** page provides the applicable options, depending on whether IPv6 mode is enabled or disabled.


B426 - Windows Internet Explorer powered by CI
http://192.168.1.101/lgs.cgi?*%26%5E%25%24%23@=
Google
Favorites
B426
Page
Safety
Tools
BOSCH
B426
Home
Basic Network Settings
Advanced Network Settings
Panel Address Settings
Encryption and Security Settings
Maintenance
Factory Default
Save and Execute
Logout
Firmware Update
OK
Copyright: Bosch Security Systems, Inc. 2012 All rights reserved
Done
Local intranet
100%

Basic Network Settings

IPv4 DHCP/AutoIP Enable:	Yes
IPv4 Address:	0 . 0 . 0 . 0
IPv4 Subnet Mask:	255 . 255 . 255 . 0
IPv4 Default Gateway:	0 . 0 . 0 . 0
Obtain IPv4 DNS Server Address Automatically:	Yes
IPv4 DNS Server IP Address:	0 . 0 . 0 . 0
Alternate IPv4 DNS Server IP Address:	0 . 0 . 0 . 0
IPv6 Mode:	No
Obtain IPv6 DNS Server Address Automatically:	No
IPv6 DNS Server IP Address:	::
Alternate IPv6 DNS Server IP Address:	::
TCP/UDP Port Number:	7700
Legacy TCP Automation Enable:	No
TCP Keep Alive Time:	45

Figure 5.3: Basic Network Settings default web page

IPv4 DHCP/AutoIP Enable

Default: Yes

Selections: Yes, No

Yes: DHCP /AutoIP is enabled.

No: DHCP/AutoIP is disabled.

DHCP is an auto configuration protocol that allows a computer to be automatically configured, which eliminates the need for interaction by a network administrator. DHCP also provides a central database that tracks computers that connect to the network, which prevents two computers from accidentally being configured with the same IP address.

AutoIP enables dynamic IP addresses to be assigned to a device when the device is started up. Whereas DHCP requires a DHCP server, AutoIP does not require a server when selecting an IP address. A host configured with AutoIP receives an IP address of 169.254.xxx.xxx.

Notice!

When you enable DHCP /AutoIP, the module does not use the IPv4 address, subnet mask, or gateway. The corresponding fields on the page are disabled, but previously entered values show and cannot be changed. If you disable DHCP/AutoIP, you must set the IPv4 address, subnet mask, and gateway.

IPv4 Address

Default: 0.0.0.0

Selection: 0.0.0.0 to 255.255.255.255
This parameter sets a static IPv4 address for the module if DHCP is disabled.

IPv4 Subnet Mask

Default: 255.255.255.0
Selection: 0.0.0.0 to 255.255.255.255
Subnetting is used to break the network into smaller, more efficient subnets to prevent excessive rates of Ethernet packet collision in the large network. A significant feature of subnetting is the subnet mask. Applying a subnet mask to an IP address allows you to identify the network and node parts of the address. When DHCP/AutoIP Enabled is set to **Yes**, this parameter cannot be changed.

IPv4 Default Gateway

Default: 0.0.0.0
Selection: 0.0.0.0 to 255.255.255.255
A gateway is a point (typically a router) on a TCP/IP network that serves as an access point to another network. A host uses a default gateway when an IP packet's destination address belongs to someplace outside the local subnet. The default gateway address is usually an interface belonging to the LAN's border router. In DHCP mode, the default gateway is usually resolved automatically. When DHCP/AutoIP Enable is set to Yes, this parameter cannot be changed.

Obtain IPv4 DNS Server Address Automatically

Default: Yes
Selection: Yes, No
Setting this parameter to No allows entering the server address. Setting this parameter to Yes clears addresses and prevents address entry.

IPv4 DNS Server IP Address

Default: 0.0.0.0
Selection: 0.0.0.0 to 255.255.255.255
A Domain Name Server (DNS) converts internet domain names or hostnames to their corresponding IP addresses. This setting is used to configure a DNS server address in Static IP mode. In DHCP mode, the default value of 0.0.0.0 indicates the DHCP server’s default DNS is used. To use a custom DNS server in DHCP mode, change the parameter to the specified DNS server’s IP address.
The address has a dot decimal notation, which consists of the four octets of the address expressed separately in decimal and separated by periods. Each octet has a value 0-255.

Alternate IPv4 DNS Server IP Address

Default: 0.0.0.0
Selection: 0.0.0.0 to 255.255.255.255
This parameter provides an alternate IPv4 DNS server IP address.
The address has a dot decimal notation, which consists of the four octets of the address expressed separately in decimal and separated by periods. Each octet has a value 0-255.

If the module fails to obtain an address from the primary server, the alternate DNS server is used, if specified. To use the alternate address, you must specify a primary address.

IPv6 Mode

Default: Disable
Selections: Enable, Disable
Enable: IPv6 enabled; module works with both IPv6 and IPv4 addressing.
Disable: IPv6 disabled; module works only with IPv4 addressing.
IP Version 6 (IPv6) is a new version of Internet Protocol. Select whether the module works with IPv6 in addition to IPv4 addressing.

Obtain IPv6 DNS Server Address Automatically

Default: Yes
Selection: Yes, No
Setting this parameter to No allows entering the server address. Setting this parameter to Yes clears addresses and prevents address entry. In DHCP mode, the default value of 0.0.0.0 indicates that the DHCP server’s default DNS is used. To use a custom DNS server in DHCP mode, change the parameter to No and enter the specified DNS server’s IP address.

IPv6 DNS Server IP Address

Default: ::
Selection: 0:0:0:0:0:0:0:0 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
This parameter configures the IPv6 DNS server address.
A DNS server converts internet domain names or hostnames to their corresponding IP addresses. In DHCP mode, the default value indicates the DHCP server’s default DNS is used. To use a custom DNS server in DHCP mode, change the parameter to the specified DNS server’s IP address.

The IPv6 DNS address has a hexadecimal notation, which consists of the eight groups of the address expressed separately in hexadecimal and separated by colons. Each group can have a value between 0000-FFFF. When this is defined through the DHCP service, leave the default value.

Alternate IPv6 DNS Server IP Address

Default: ::
Selection: 0:0:0:0:0:0:0:0 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
This parameter provides an alternate IPv6 DNS server IP address.
The Alternate IPv6 DNS address has a hexadecimal notation, which consists of the eight groups of the address expressed separately in hexadecimal and separated by colons. Each group has a value between 0000-FFFF.
When this is defined through the DHCP service, leave the default value. If the module fails to obtain an address from the primary server, the Alternate IPv6 DNS server is used, if specified. The module can use the Alternate IPv6 DNS server address only when the Primary address is not the default address.

TCP/UDP Port Number

Default: 7700

Selection: 0 to 65535

This parameter sets the local port number on which the module listens for in-coming network traffic. This port is also the source port for outgoing communication.

The TCP/UDP Port is typically configured as 7700 when the control panel is communicating with a central station receiver, RPS, Automation or Remote Security Control. Port numbers are assigned in various ways based on three ranges:

– System Ports: 0 to 1023
– User Ports: 1024 to 49151
– Dynamic or Private Ports: 49152 to 65535

Note: In order to limit unwanted traffic, select a number above 1023.

Legacy TCP Automation Enable

Default: No

Selection: Yes, No

When enabled, a single TCP connection with no security is allowed.

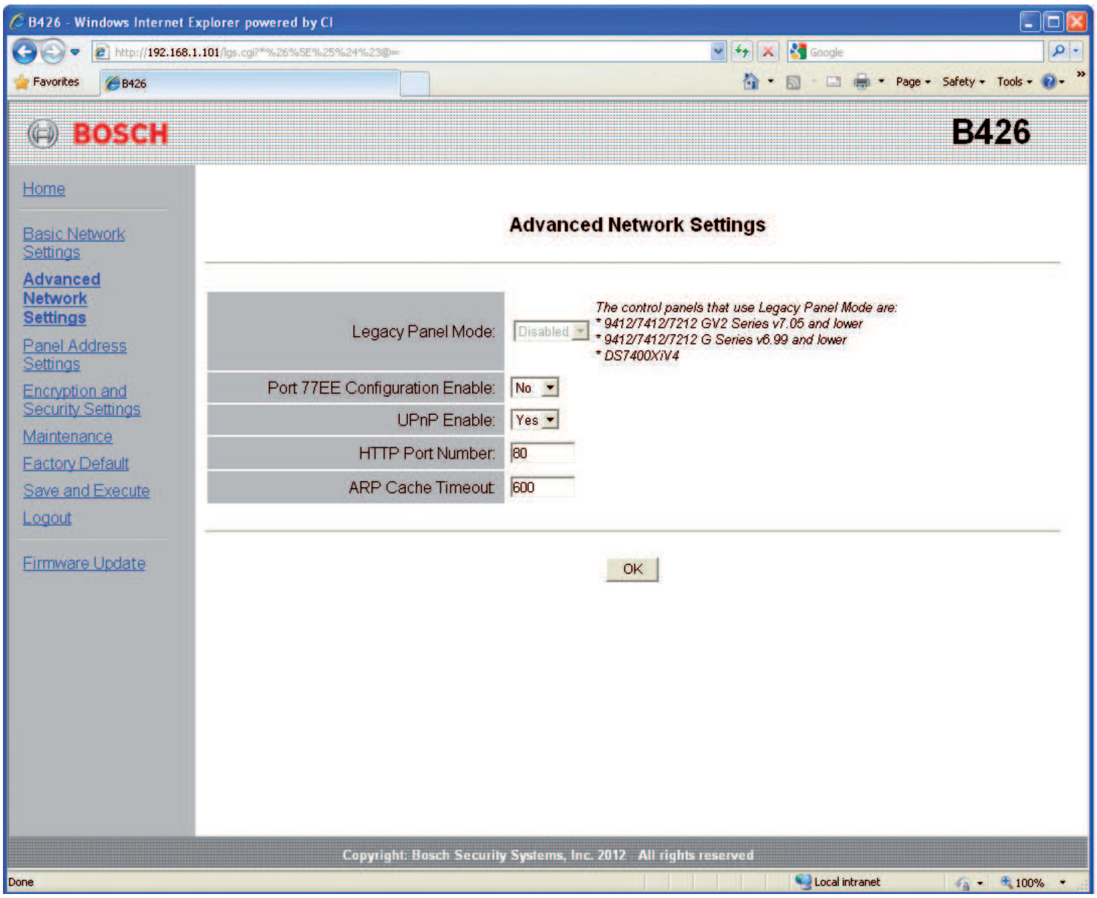
TCP Keep Alive Time

Default: 45

Selection: 0 – 65 (0: Disable, 1 - 65: Keepalive Time in sec)

Select how many seconds the unit waits during a silent connection before attempting to see if the currently connected network device is still on the network. If there is no response, it drops the connection.

5.3.5 Advanced Network Settings page


B426 - Windows Internet Explorer powered by CI
http://192.168.1.101/lgs.cgi?*%26%5E%25%24%23@=
Google
Favorites
B426
Page
Safety
Tools
BOSCH
B426
Home
Basic Network Settings
Advanced Network Settings
Panel Address Settings
Encryption and Security Settings
Maintenance
Factory Default
Save and Execute
Logout
Firmware Update
Copyright: Bosch Security Systems, Inc. 2012 All rights reserved
Done
Local intranet
100%

Advanced Network Settings

Legacy Panel Mode: Disabled

The control panels that use Legacy Panel Mode are:
** 9412/7412/7212 GV2 Series v7.05 and lower*
** 9412/7412/7212 G Series v6.99 and lower*
** DS7400XiV4*

Port 77EE Configuration Enable: No

UPnP Enable: Yes

HTTP Port Number: 80

ARP Cache Timeout: 600

OK

Figure 5.4: Advanced Network Settings page

Legacy Panel Mode

Default: 0 (Disable)

Selections: 0, 1

0: Legacy Panel Mode is disabled.

1: Legacy Panel Mode is enabled.

This option allows the module to support legacy control panels that communicate using Datagram Mode 0. When Legacy Panel Mode is enabled, the module uses the Local Port parameter as both the source port and destination port for communication.

The control panels that use Legacy Panel Mode are:

– GV2 v7.05 and lower
– D9412G/D7412G/D7212G v6.99 and lower
– DS7400XiV4

Port 77EE Configuration Enable

Default: No

Selections: Yes, No

Yes: The network configuration port is enabled.

No: The network configuration port is disabled.

The Conettix D6200 Programming/Administration Software uses this port to find devices on its local network.

UPnP Enable

Default: Yes
Selections: Yes, No
Yes: UPnP is enabled.
No: UPnP is disabled.
Universal Plug and Play (UPnP) allows devices to connect seamlessly and simplifies the implementation of personal and corporate networks. When enabled in the premises router, this feature is used to automatically setup port forwarding rules for Remote Programming traffic to the control panel.

HTTP Port Number

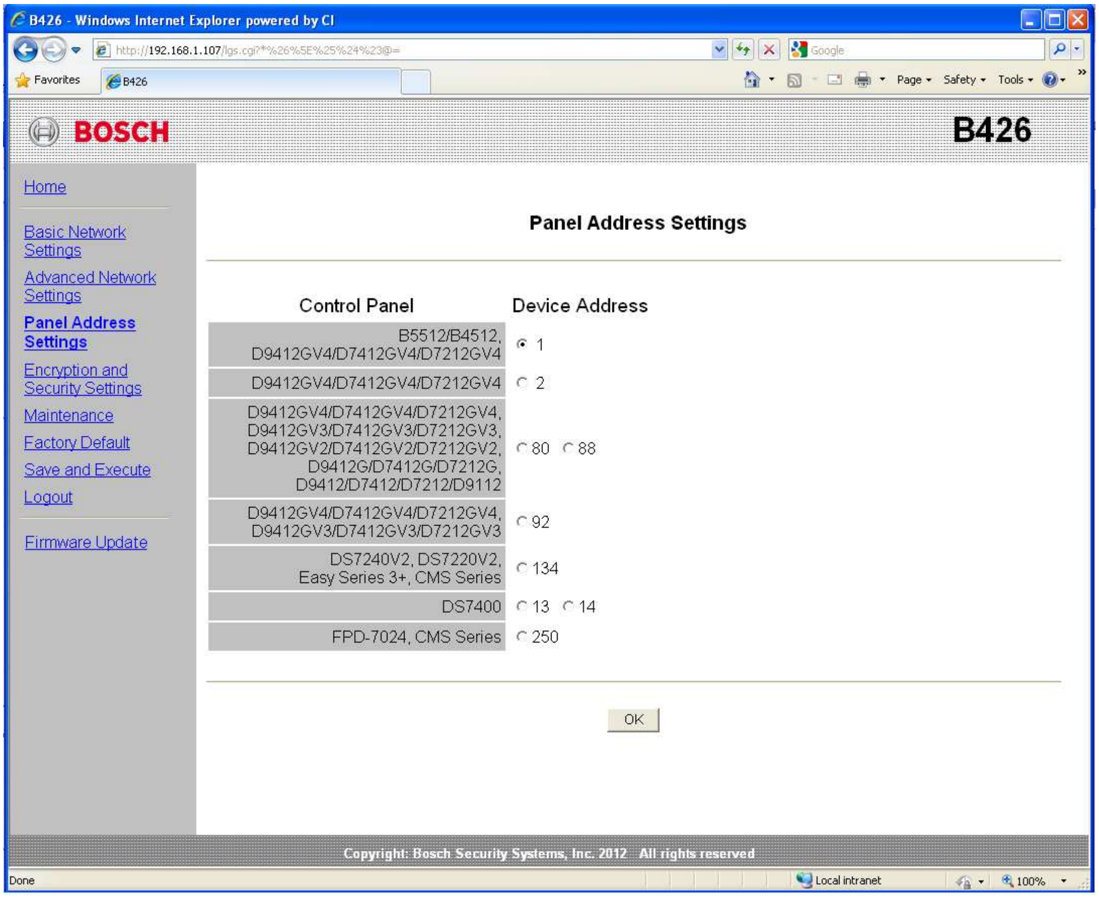
Default: 80
Selections: 1 to 65535
Use this option to configure the port number for the module web server.

ARP Cache Timeout

Default: 600
Selections: 1 to 600 (in 1-sec increments)
When the module communicates with any device on a network, an entry is added to its ARP table for each of those devices. The ARP Cache Timeout defines the number of seconds (1 to 600) before the ARP table of the module is refreshed.

5.3.6 Panel Address Settings page

The **Panel Address Setting** page only allows configuration when the address switch on the module is set to 0. If the address switch is set to a position other than 0, the set address is displayed.


B426 - Windows Internet Explorer powered by CI
http://192.168.1.107/lgs.cgi?*%26%5E%25%24%23@=
Google
Favorites
B426
Page
Safety
Tools
BOSCH
B426
Home
Basic Network Settings
Advanced Network Settings
Panel Address Settings
Encryption and Security Settings
Maintenance
Factory Default
Save and Execute
Logout
Firmware Update
OK
Copyright: Bosch Security Systems, Inc. 2012 All rights reserved
Done
Local intranet
100%

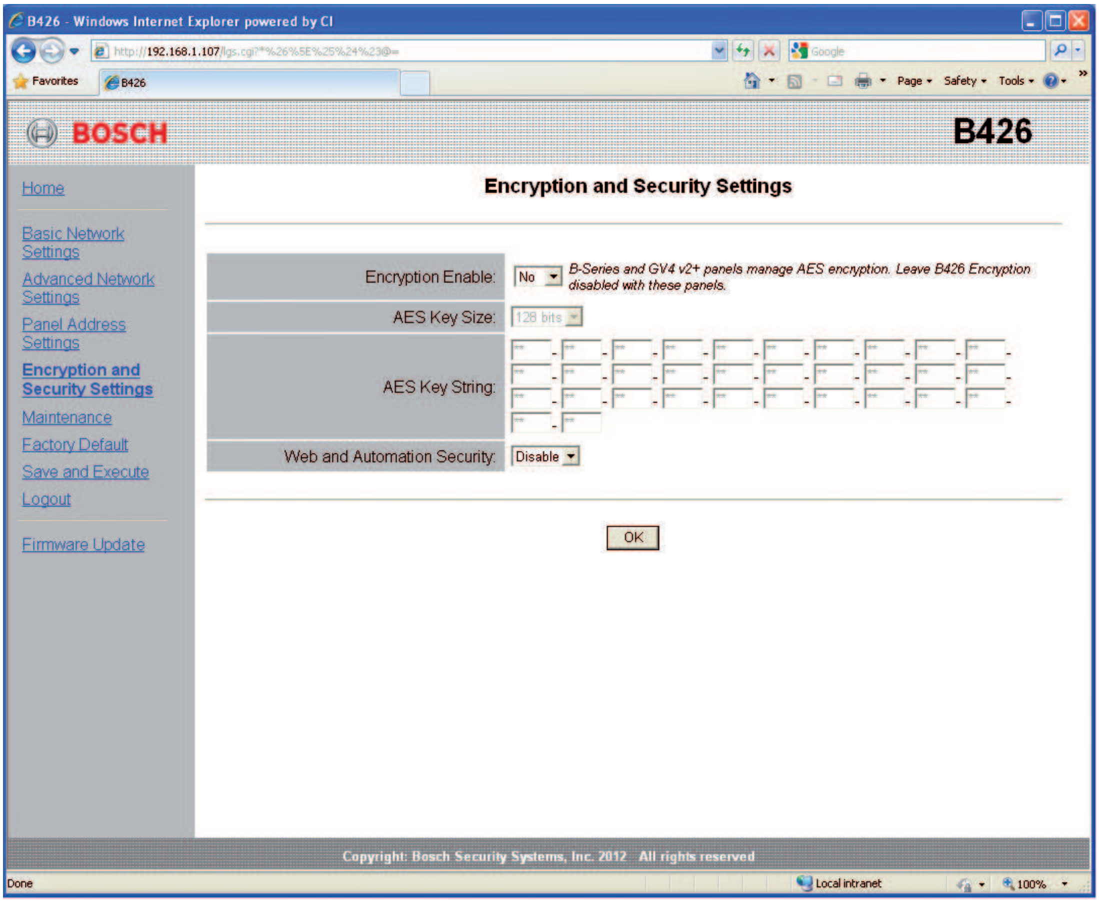
Panel Address Settings

Control Panel	Device Address
B5512/B4512, D9412GV4/D7412GV4/D7212GV4	● 1
D9412GV4/D7412GV4/D7212GV4	○ 2
D9412GV4/D7412GV4/D7212GV4, D9412GV3/D7412GV3/D7212GV3, D9412GV2/D7412GV2/D7212GV2, D9412G/D7412G/D7212G, D9412/D7412/D7212/D9112	○ 80 ○ 88
D9412GV4/D7412GV4/D7212GV4, D9412GV3/D7412GV3/D7212GV3	○ 92
DS7240V2, DS7220V2, Easy Series 3+, CMS Series	○ 134
DS7400	○ 13 ○ 14
FPD-7024, CMS Series	○ 250

Figure 5.5: Panel Address Settings page

Use this option to select the bus address for the control panel type to which the module is connected.

5.3.7 Encryption and Security Settings page



Encryption and Security Settings

Encryption Enable: No — B-Series and GV4 v2+ panels manage AES encryption. Leave B426 Encryption disabled with these panels.

AES Key Size: 128 bits

AES Key String:

Web and Automation Security: Disable

Copyright: Bosch Security Systems, Inc. 2012 All rights reserved

Figure 5.6: Encryption and Security Settings Page

Encryption Enable

Default: No

Selections: Yes, No

Yes: All UDP communication (RPS and event reports) through the network module is encrypted. AES encryption must also be set at the central station receiver and the PC running RPS.

No: All communication through the network module is unencrypted.

Use this option to enable or disable Advanced Encryption Standard (AES) encryption on the module.

For B9512G/B8512G, B6512/B5512/B4512/B3512, and GV4 v2.xx control panels with Panel Programming Enable set to **Yes**, the module does not enable encryption regardless of the setting.

AES Key Size

Default: 128

Selections: 128, 192, 256

Use this option to select the AES key size. The AES key size must match the key size used in RPS and the receiver.

AES Key String

Default: The default varies by key size.

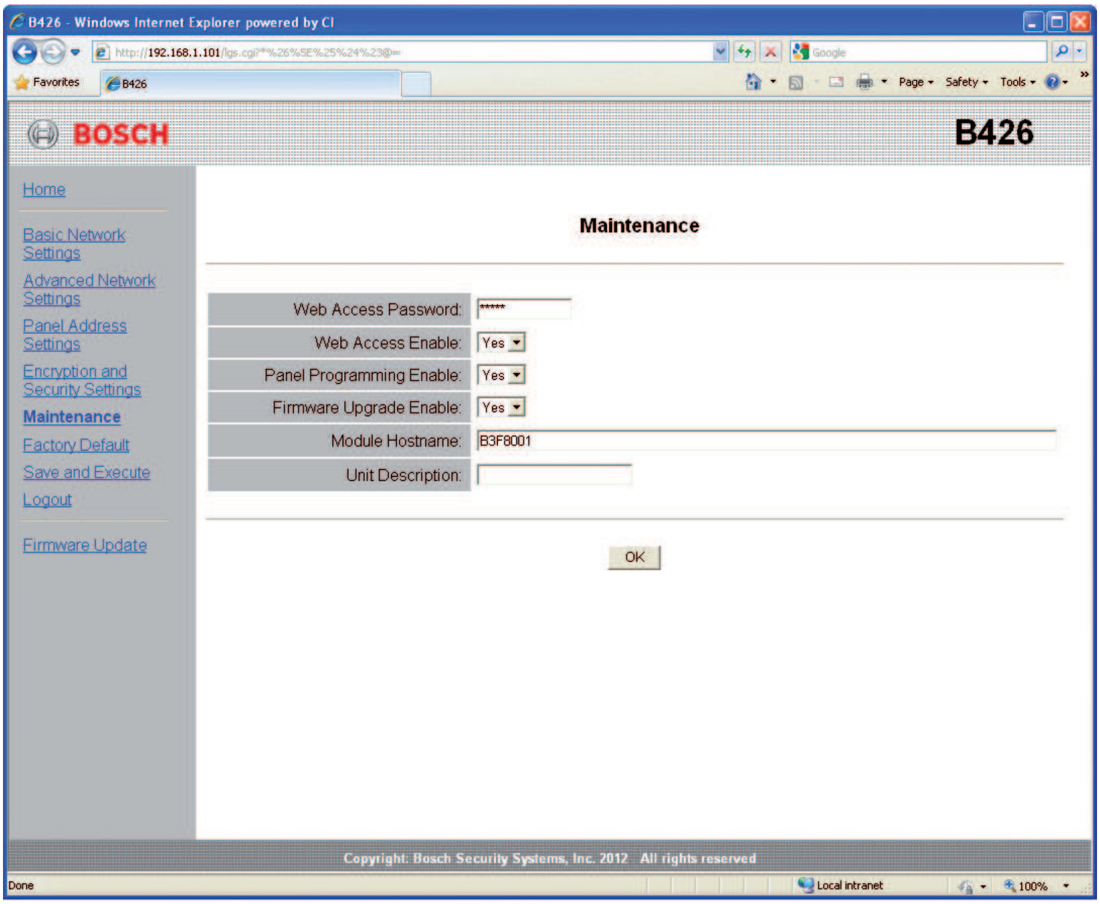
Selections: Sixty-four hexadecimal characters represented in up to 32 fields (2 hexadecimal characters per field)

- 128 bit key length is 16 bytes (16 fields displaying 2 ASCII [0-9, A-F] characters).
- 192 bit key length is 24 bytes (24 fields displaying 2 ASCII [0-9, A-F] characters).
- 256 bit key length is 32 bytes. (32 fields displaying 2 ASCII [0-9, A-F] characters).

Web and Automation Security

Default: Enable for B9512G/B8512G, B6512/B5512/B4512/B3512, and GV4 v2.xx control panels, Disable for all other control panels.
Selections: Disable, Enable
This parameter enables enhanced security for Automation and B426 Web Access.
When enabled, HTTPS is applied to B426 Web Access changing the default value of the HTTP port number parameter. This setting also enables TLS Security for Automation.

5.3.8 Maintenance page


B426 - Windows Internet Explorer powered by CI
http://192.168.1.101/lgs.cgi?*%26%5E%25%24%23@=
Google
Favorites
B426
Page
Safety
Tools
BOSCH
B426
Home
Basic Network Settings
Advanced Network Settings
Panel Address Settings
Encryption and Security Settings
Maintenance
Factory Default
Save and Execute
Logout
Firmware Update
Copyright: Bosch Security Systems, Inc. 2012 All rights reserved
Done
Local intranet
100%

Maintenance

Web Access Password:	*****
Web Access Enable:	Yes
Panel Programming Enable:	Yes
Firmware Upgrade Enable:	Yes
Module Hostname:	B3F8001
Unit Description:	

OK

Figure 5.7: Maintenance page

Web Access Password

Default: B42V2
Selections: Four to ten case sensitive alphanumeric characters
Enter the password to log in to the configuration web pages. It is recommended to change the default login password to secure of the module configuration.

Web Access Enable

Default: No for B6512/B5512/B4512/B3512 and GV4 v2.xx or higher control panels, Yes for all other control panels
Selections: Yes, No
Yes: Web configuration is enabled
No: Web configuration is disabled
Enable or disable access to the configuration web pages.
Do NOT disable web access unless you are on a SDI2 panel and AMAX 2100/ 3000/ 4000 with Panel Programming Enable enabled. With SDI and option control panels, the module can only be configured via the web interface.

Panel Programming Enable

Default: Yes
Selections: Yes, No
Yes: Control panel programming is enabled.
No: Control panel programming is disabled.
Enable or disable control panel programming of the module with compatible (SDI2-only) control panels and AMAX 2100/ 3000/ 4000.
Do not disable Web Access Enable and Panel Programming Enable. If both are disabled, you cannot configure the module.

Firmware Upgrade Enable

Default: No
Selections: Yes, No
Yes: Allows firmware upgrades to the B426.
No: Prevents firmware upgrades.
Enable or disable the ability to upgrade the module's firmware from the **Firmware Upgrade** configuration page.

Module Hostname

Default: Blank
Selections: Sixty-four alphanumeric characters
Blank: Blank restores the default hostname Bxxxxxx, where as xxxxxx is the last six digits of the module's MAC address.
Use this parameter to create or change a module hostname. This is the hostname that represents the module on the network. Optionally use the hostname to contact the control panel via RPS over network, for Remote Security Control, or for module web configuration and diagnostics.

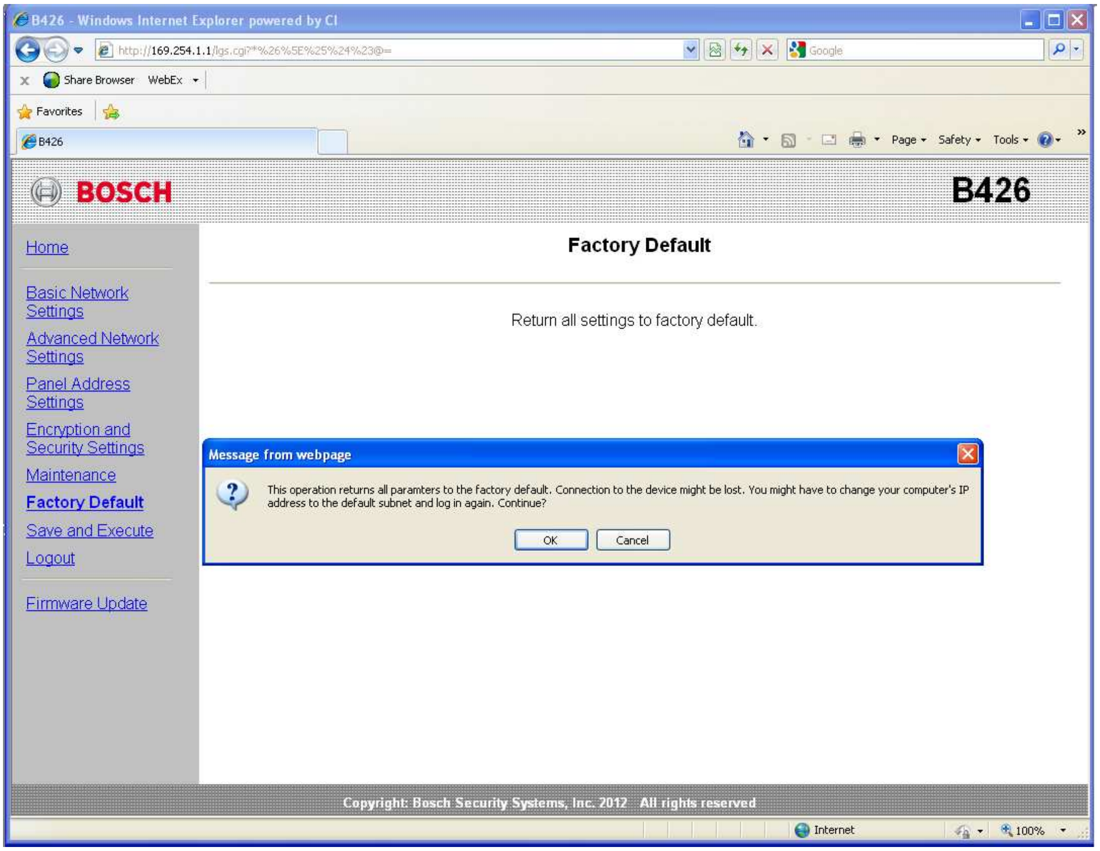
Notice!
Use the hostname on a local network using DHCP . To use the hostname externally, enter the hostname in the DNS server.

Unit Description

Default: Blank
Selections: Twenty alphanumeric characters
Use this parameter to create a simple description for the unit, shown in the web configuration pages.

Notice!
Do not use the double quote character (") as it causes unexpected results.

5.3.9 Factory Default page


B426 - Windows Internet Explorer powered by CI
http://169.254.1.1/lgs.cgi?*%26%5E%25%24%23@=
Google
Share Browser
WebEx
Favorites
B426
Page
Safety
Tools
BOSCH
B426
Home
Basic Network Settings
Advanced Network Settings
Panel Address Settings
Encryption and Security Settings
Maintenance
Factory Default
Save and Execute
Logout
Firmware Update
Copyright: Bosch Security Systems, Inc. 2012 All rights reserved
Internet
100%

Factory Default

Return all settings to factory default.

Message from webpage

This operation returns all paramters to the factory default. Connection to the device might be lost. You might have to change your computer's IP address to the default subnet and log in again. Continue?

OK Cancel

Figure 5.8: Factory Default page

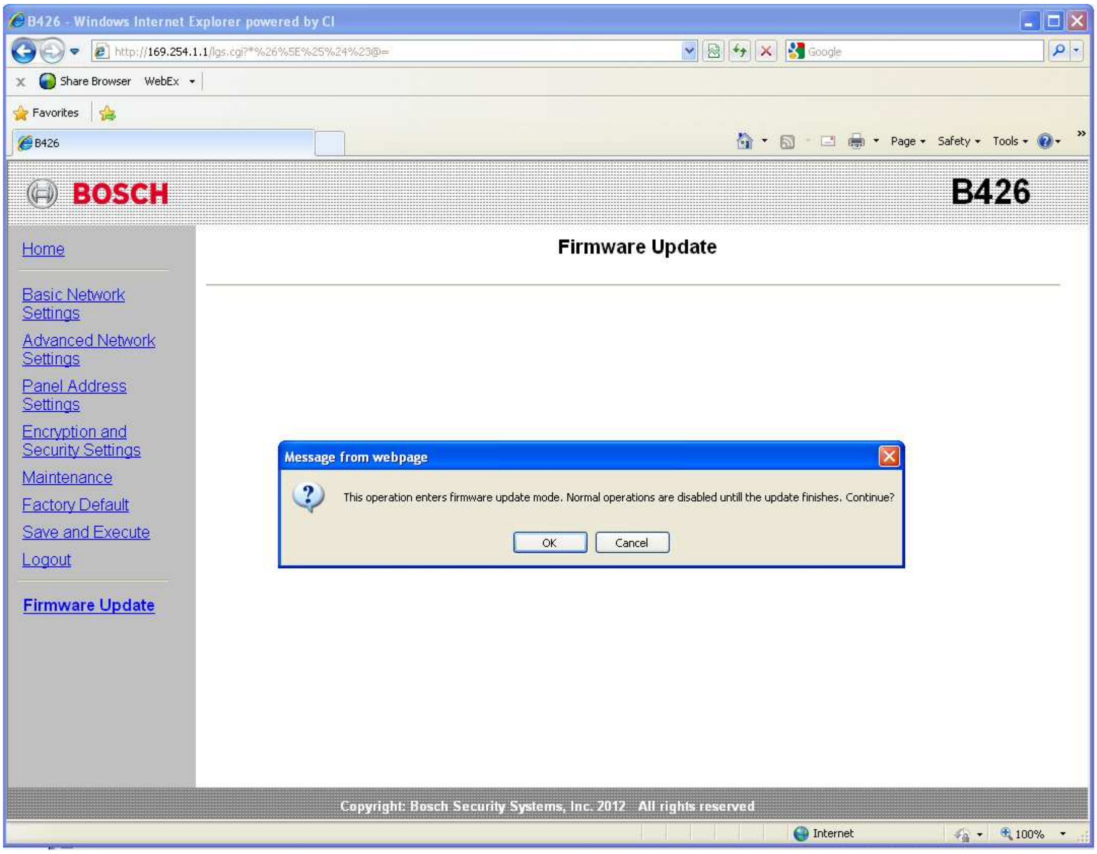
You can return the module to the factory default settings by clicking on the **Factory Default** menu.

Click **Cancel** to cancel the factory default reset. If you select **OK**, all configuration options are returned to the factory default settings.

Notice!
Returning the module to its factory default settings might cause the module to terminate the current web browsing session. If connected to a compatible SDI2 control panel, the control panel overwrites the factory default settings with the control panel's settings. To avoid the control panel settings overwriting **Configuration Page** settings, set Panel Programming Enable to No after restoring the module to factory default, but before pressing **Save and Execute**.

5.3.10 Firmware Update page

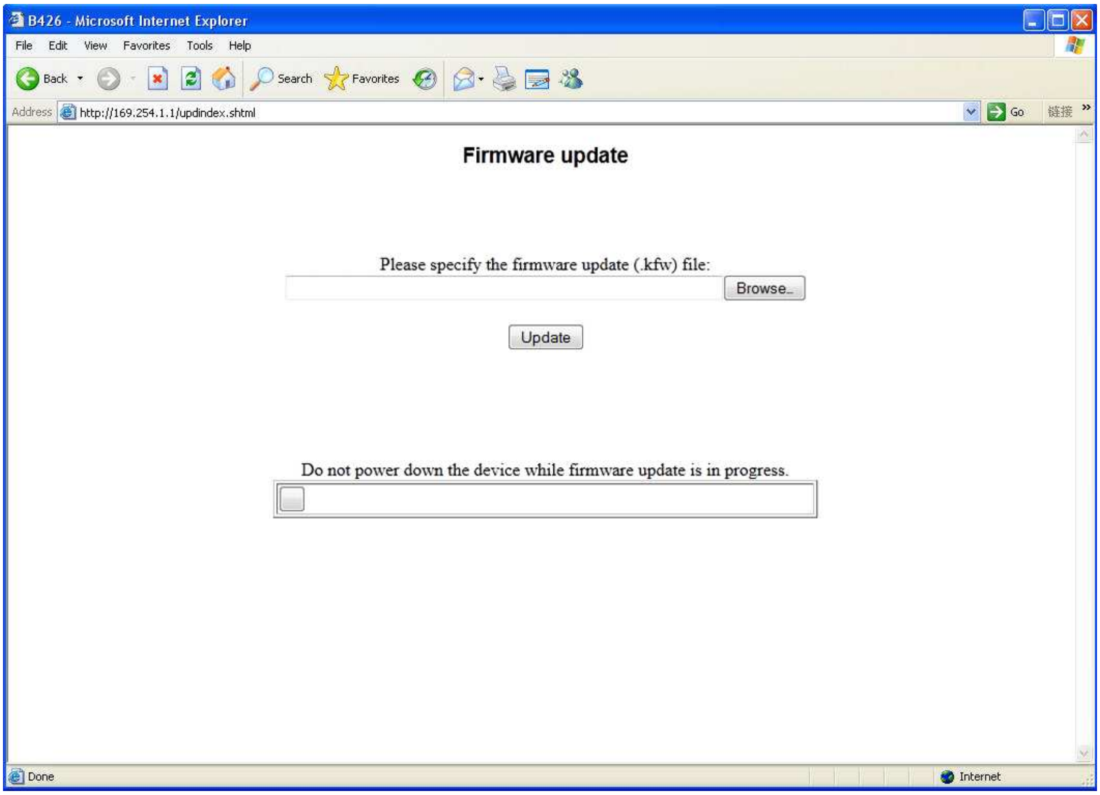
To upgrade the firmware in the module, select the **Firmware Update** option from the configuration home page. The **Firmware Update** page opens.



This operation enters firmware update mode. Normal operations are disabled untill the update finishes. Continue?

Figure 5.9: Firmware Update page

To proceed with the upgrade, click **OK**. A new web page opens that allows you to locate the firmware file and upload it to the module.


B426 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://169.254.1.1/updindex.shtml
Go 链接
Browse...
Update
Done
Internet

Firmware update

Please specify the firmware update (.kfw) file:

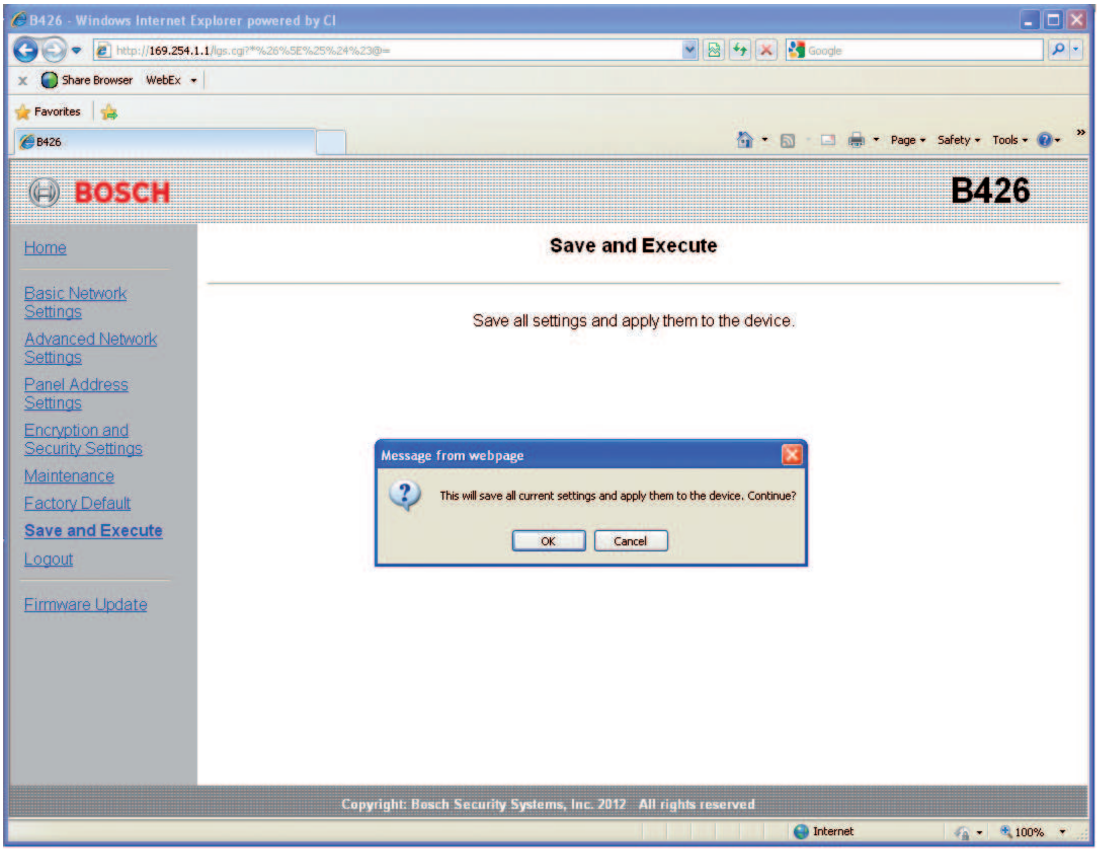
Do not power down the device while firmware update is in progress.

Figure 5.10: Firmware upgrade specify upgrade file

Notice!
Upgrading the firmware in the module causes the module to terminate the current web browsing session.

5.3.11 Exiting the web-based configuration pages

When you are finished configuring the module, select the **Save and Execute** option. The **Save and Execute** web page opens.
To save the configuration changes that you made, click **OK**. A confirmation message appears.



Save and Execute

Save all settings and apply them to the device.

Message from webpage

This will save all current settings and apply them to the device. Continue?

Copyright: Bosch Security Systems, Inc. 2012 All rights reserved

Figure 5.11: Save and Execute confirmation

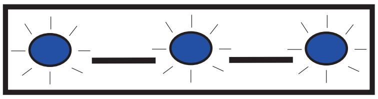
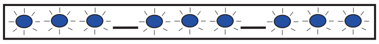
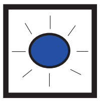
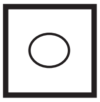
To exit the configuration web page, click **Logout**, and then close the internet browser window.

6 Maintenance and troubleshooting LEDs

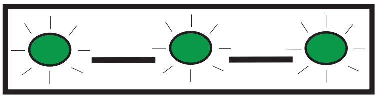
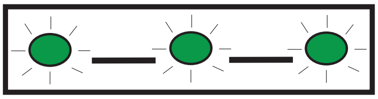
The B426 includes the following on-board LEDs to assist with troubleshooting:

- Heartbeat (system status).
- RX (receive).
- TX (transmit).

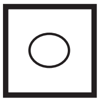
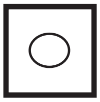
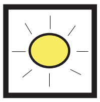
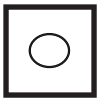
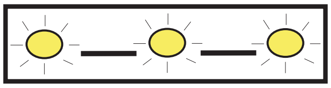
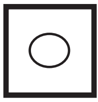
Refer to *B426 module overview, page 8* for Ethernet link LED locations.

Flash pattern	Function
 Flashes once every 1 sec	Normal state. Indicates normal operation state.
 3 quick flashes every 1 sec	Communication error state. Indicates a bus communication error. The module is not receiving commands from the control panel.
 On Steady	Trouble state. Indicates a trouble condition exists.
 Off	LED trouble state. Module is not powered, or some other trouble condition prohibits the module from controlling the heartbeat LED.

Tab. 6.2: Heartbeat LED descriptions

Flash pattern	Function
 RX (Receive) Flashing	Occurs when the module receives a message over the network connection – UPD, TCP, or DNS.
 TX (Transmit) Flashing	Occurs when the module sends a message over the network connection – UPD, TCP, or DNS.

Tab. 6.3: RX and TX LEDs descriptions

LINK (yellow) LED pattern	100Mb (green) LED pattern	Function
 Off	 Off	No Ethernet link
 On Steady	 Off	10Base-T link
 Flashing	 Off	10Base-T activity

LINK (yellow) LED pattern	100Mb (green) LED pattern	Function
● On Steady	● On Steady	100Base-TX link
●—●—● Flashing	● On Steady	100Base-TX activity

Tab. 6.4: Ethernet Link LEDs descriptions

Trouble conditions indicated through LEDs

Condition	Heartbeat	Transmit (TX)	Receive (RX)
Network cable disconnected	● On Steady	○ Off	●—●—● Flashes once every 1 sec
Obtaining an IP address	● On Steady	○ Off	●●—●●—●● 2 quick flashes every 1 sec
Low bus voltage	● On Steady	○ Off	●●●—●●●—●●● 3 quick flashes every 1 sec
Internal failure	● On Steady	○ Off	● On Steady

Tab. 6.5: Trouble conditions

Notice!
When the tamper switch is closed, all module LEDs are Off.

6.1 Show the firmware version

To show the firmware version using an LED flash pattern:

- If the optional tamper switch is installed:
  With the enclosure door open, activate the tamper switch.
- If the optional tamper switch is NOT installed:
  Momentarily short the tamper pins.

When the tamper switch is activated (open to closed), the heartbeat LED stays Off for 3 sec before indicating the firmware version. The LED pulses the major, minor, and micro digits of the firmware version, with a 1 sec pause after each digit.
The following is an example: The version 1.4.3 would show as LED flashes:
[3 second pause] *_****_*** [3 second pause, then normal operation].

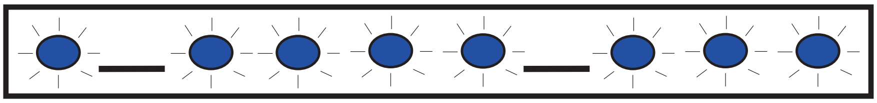


Figure 6.1: Firmware LED flash patterns example

7 Specifications

This section includes module specifications and compatibility.

7.1 Technical specifications

Environmental considerations

Relative humidity	Up to 93% non-condensing
Temperature (operating)	0° - +49°C (+32° - +120°F)

Properties

Board dimensions	59.5 mm x 108 mm x 16 mm (2.19 in x 4.25 in x 0.629 in)

Power requirements

Current (maximum)	100 mA max
Voltage	12 VDC nominal

Connectors

LAN/WAN	RJ-45 modular port (Ethernet)

Cabling

Ethernet cable	Category 5 or better unshielded twisted pair
Ethernet cable length	100 m (328 ft) max length

Wiring

Data bus wire gauge	18 AWG or 22 AWG
Data bus wire length	Maximum distance – Wire size : 150 m (500 ft) - 0.65 mm (22 AWG) 300 m (1000 ft) - 1.02 mm (18 AWG)

Browser support

Microsoft Internet Explorer (Microsoft Windows 7 and higher)
Mozilla Firefox

7.2 Compatibilities

Compatible control panels

AMAX 2000/2100/3000/4000
B9512G/B9512G-E
B8512G/B8512G-E
B6512
B5512/B5512E
B4512/B4512E
B3512/B3512E
D9412GV4/D7412GV4/D7212GV4
D9412GV3/D7412GV3/D7212GV3
D9412GV2/D7412GV2/D7212GV2 Version 7.06 or higher
DS7220 Version 2.10 or higher
DS7240 Version 2.10 or higher

DS7400XiV4 Version 4.10 or higher
Easy Series V3+
FPD-7024
Solution 2000/3000

8 Appendix

This section includes detailed instructions for module hostnames and IP addresses.

8.1 Module hostname

Determining the module's hostname:
The factory default configuration of the module allows the DHCP server to assign an IP address. A default hostname based on the MAC address is registered with the DHCP server if the module has not been programmed for a specific hostname. You can use the hostname for modules configured for dynamic DHCP or static IP addresses. Hostnames cannot be used when connecting directly using AutoIP. The default hostname for the module is the letter B followed by the last six alpha-numeric digits of its MAC address (for example, B3F603F).

8.2 Module IP address

Determining the module's IP address (with the address switch in any position), requires one of the following procedures:

- *Use DHCP to look up the IP address of a network-connected module, page 35*.
- *Use an SDI/SDI2 keypad to discover the IP address of a module, page 35*. (B9512G/B8512G, B6512/B5512/B4512/B3512, and GV4 only.)
- *Use Auto IP with a directly connected module, page 36*. Within 60 seconds, the B426 temporarily assumes address 169.254.1.1 for configuration.

Notice!
Outside access requires obtaining the public IP address and port mapping from the gateway.

8.2.1 Use DHCP to look up the IP address of a network-connected module

If the module is connected to a network, a DHCP (Dynamic Host Configuration Protocol) server assigns the IP address to the module.

Looking up the module’s IP address on the DHCP server:

1. Log into the DHCP server.
2. Locate the IP address table on the DHCP server.
3. Use the MAC address assigned to the module (indicated on the label on the Ethernet RJ-45 port), to find the IP address assigned to the module.

8.2.2 Use an SDI/SDI2 keypad to discover the IP address of a module

If the module is connected to a B9512G/B8512G, B6512/B5512/B4512/B3512, or GV4 control panel, you can use a connected keypad to look up the local (LAN) IP address.

Finding the module’s IP address using an SDI2 keypad (B920/B930 instructions):

1. Log in to the keypad with your installer passcode, and then go to the [1] Installer menu.
2. Go to the [3] Network > [1] B42x > [1] Settings menu option. The keypad scrolls through the following sub-categories, indicating the programming for: Hostname, IPv4 Source IP, IPv6 Source IP, MAC Address.
3. When the you finish viewing the information, press [ESC] to exit the menu.

Finding the module's IP address using an SDI keypad (D1255/D1260 instructions):

1. At the keypad, press [9] [9] [ENTER] and then press [NEXT].

2. At the Tools menu, press [ENTER]. The keypad prompts you to enter the installer passcode.
3. Enter the installer passcode and press [ENTER].
4. Go to the IP Diagnostics > B420 Module (1-2) > Settings menu option, and then press [NEXT] twice to access the IPaddress.
5. When the you finish viewing the information, press [ESC] to exit the menu.

8.2.3 Use Auto IP with a directly connected module

If the module is connected directly to a computer (laptop or PC) and is not connected to a network (no network hub, router, or switch is connected), you can use the module's AutoIP. to connect and program the module without knowing the IP.

Notice!
If you cannot connect with the AutoIP option, you might need to change the web browser configuration so that it does not use a proxy server. Also ensure the computer has AutoIP enabled. Refer to the browser’s online help for instructions on disabling proxy service.

If the module's IP address is not recorded in the host computer’s ARP table and you do not know the address, follow the steps below.
Using the AutoIP:

1. Remove power from the module.
2. Disconnect the module from the network.
3. Connect the B426 directly to the Ethernet port on a computer, power up, and wait 60 sec. If AutoIP service is enabled on your computer, a 169.254.XXX.XXX address should now be assigned to your computer.
4. Open an internet browser (Microsoft Internet Explorer 6 or higher, or Mozilla Firefox 3 or higher) and type in the default AutoIP address for the B426: **169.254.1.1**, and press [Enter].
5. Enter the password (default is *B42V2*) and click **Login**. The **Device Information** page opens.

If AutoIP does not work on the host computer, a new registry key might be required to enable AutoIP. Be sure to obtain permission from your company IT department before changing the registry.

Enabling AutoIP on the host computer with a new registry key:

1. Open Notepad and create a new file called **AutoIP.reg**.
2. In Notepad, include the following text:
   Windows Registry Editor Version 5.00
   [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
   "IPAutoconfigurationEnabled"=dword:00000001
3. Save the file to a location on the host computer that you can easily find.
4. Navigate to the saved file and double-click on it to add it to the host computer’s registry.
5. Restart the host computer.

Bosch Security Systems, Inc.
130 Perinton Parkway
Fairport, NY 14450
USA
www.boschsecurity.com

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany