AN-193

Troubleshooting Protege GX Controller Connectivity

Application Note

Last Published: 18-Jul-22 2:49 PM

Contents

Introduction

When the correct procedure is followed, you should have little to no issues bringing your Protege GX controller online. However, if your controller is not coming online, you need to follow some basic troubleshooting steps as outlined here.

Please complete all of these steps before you contact technical support.

Communication Requirements

For the server and controller to communicate, the following are required:

1. The controller must be physically networked to the server, or connected over the web.
2. The Protege GX services must be running.
3. The server must have the correct IP address for the controller.
4. The server must have the correct controller serial number to properly identify incoming messages from it.
5. The controller must have the event server IP address and port set correctly (port 22000 by default).
6. The controller must be contactable on the download and control ports (ports 21000 and 21001 by default).
7. Protege GX must have the correct computer name configured for the download and event servers.
8. The Protege GX software and databases must have the same database version.
9. Encryption must either be disabled at both ends or enabled at both ends with the correct encryption key.

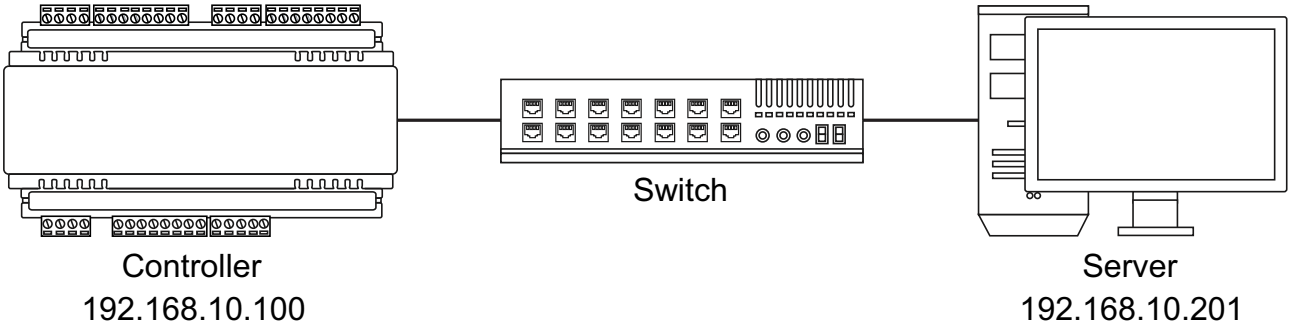
Physical Networking

The first step is to establish what is **between** the server and controller.

How you go about troubleshooting depends on whether the controller and server are on the same sub network or not.

Simple Networks

If the server and controller are on the same sub network, troubleshooting the network path is somewhat easier.

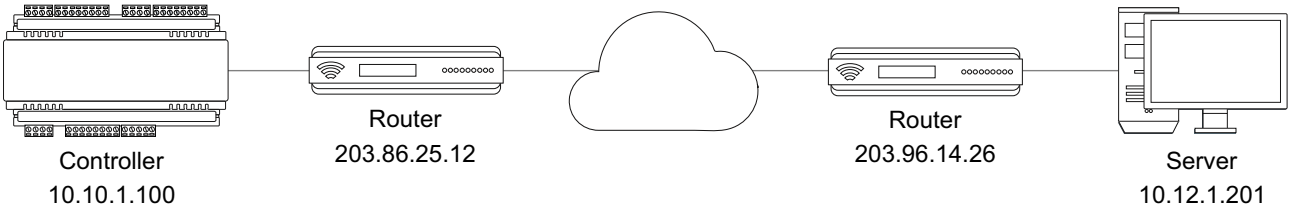


Devices on the same sub network have only switches or hubs connecting them.

This means the server and controller should be able to communicate directly if they are both physically connected to the network.

Complex Networks

If your network has routers between the controller and server, troubleshooting can be more difficult. You will need to ensure that any necessary firewall permissions and port forwarding have been set up correctly.



Troubleshooting networks such as these is beyond the scope of this document. However, the problem points outlined here may still be useful to guide you.

Troubleshooting Steps

Check that the Services are Running

The simplest and first thing to check is that the Protege GX services are running.

1. Open the **Services** snap-in by:
   - Pressing the **Windows + R** keys
   - Typing **services.msc** into the search bar and pressing **Enter**
2. Scroll down to the Protege GX services. Ensure that the following services are running:
   - Protege GX Data Service
   - Protege GX Download Service
   - Protege GX Event Service
   - Protege GX Update Service
3. If any service is not running, right click on it and click **Start**.

If any services will not start there may be another issue with your installation. For example, the database version may be incompatible (see page 10).

Confirm Controller IP Address

For the server to be able to contact the controller it must have the correct IP address programmed and be able to reach that IP address.

1. In Protege GX, navigate to **Sites | Controllers**.
2. In the **General** tab, highlight and copy (CTRL + C) the **IP address**.
3. Paste (CTRL +V) the IP address into the address bar of a web browser on the server, with the prefix https:// (e.g. https://192.168.1.2).

   You may be presented with a certificate security warning on connection.
4. If you cannot connect, remove the https:// prefix and try again (e.g. 192.168.1.2) as your controller may not be configured for HTTPS.
5. If the controller is reachable using this IP address you should be presented with a simple login screen.
6. Log in to the controller using admin credentials.

If you are unable to web browse to the controller you may not have the correct IP address. If the IP address is unknown you will need to view/change it from a keypad or default the controller's IP address (see below).

If you do have the correct IP address then it is likely that you have a network problem. Ensure that the server and controller are on the same subnet, or have correct port forwarding configured at the router.

From firmware version 2.08.911 controller ping is disabled by default. If the controller is receiving downloads you can allow ping by adding the command `EnablePing = true` in the controller commands.

Setting the IP Address from a Keypad

If the current IP address of the controller is not known it can be viewed and changed using a Protege keypad.

1. Connect the keypad to the module network.
2. Log in to the keypad using any valid installer code. The default installer code is 000000.

If the default code has been overridden and you do not know the new codes you will need to default the controller (see Defaulting the Controller in this document) to reset the code.

Note that this will erase **all** existing programming as well as setting up the default installer code.

3. Once logged in select **Menu 4** (Install Menu) then **Menu 2** (IP Menu) and view or edit the IP address, network mask, and gateway as required.

Once the settings have been changed you must save the settings by pressing the **[Arm]** key. You will be prompted to confirm the changes by pressing **[Enter]**. You must then restart the controller, either through the menu **[4], [2], [2]** or by cycling the power, for the settings to take effect.

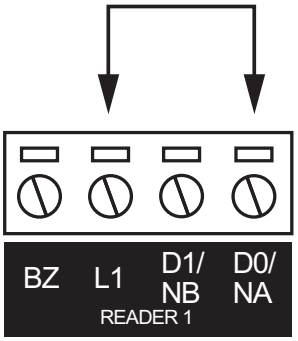
Defaulting the IP Address

If the currently configured IP address is unknown it can be temporarily set to 192.168.111.222 so that you can connect to the web interface to view and/or change it.

This defaults the IP address for as long as power is applied, but does not save the change permanently. Once the link is removed and power is cycled to the unit the configured IP address is used.

Defaulting a 2 Door Controller's IP Address

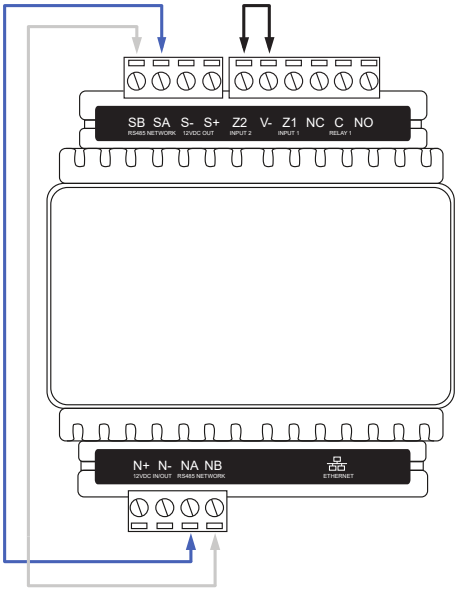
1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **Reader 1** D0 input and **Reader 1** L1 output.



4. Power up the controller. Wait for the status indicator to begin flashing steadily.

Defaulting a 1 Door Controller's IP Address

1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **NA** of the module network and **SA** of the reader network, and between **NB** of the module network and **SB** of the reader network.
4. Connect **Input 2** to ground.



5. Power up the controller. Wait for the status indicator to begin flashing steadily.

Accessing the Controller

6. When the controller starts up it will use the following temporary settings:
   - IP address : 192.168.111.222
   - Subnet Mask : 255.255.255.0
   - Gateway : 192.168.111.254
   - DHCP : disabled
7. Connect to the controller by entering https://192.168.111.222 into the address bar of your web browser, and view or change the IP address as required.

   Remember to change the subnet of your PC or laptop to match the subnet of the controller.
8. Remove the wire link(s) and power cycle the controller again.

   You can now connect to the controller using the configured IP address.

Confirm Controller Serial Number

Incoming messages from the controller to the server are identified by the controller's serial number.

1. In the controller web interface, navigate to the **Settings** page.
2. Highlight and copy the **Serial number**.
3. In Protege GX, navigate to **Sites | Controllers | General**.
4. Paste into the **Serial number** field.

Duplicate IP Address or Serial Number

Although the software warns you, it is possible to save two controllers with the same IP or serial number. In this case, the controller created first takes priority.

- Confirm you haven't created a controller with a duplicate IP address or serial number. Check all of your sites.
- If you have created a site for templates, these should be left with zero IP addresses and serial numbers.

If you have two controllers with the same IP address or serial number anywhere on your server, there will be communication problems with at least one of them.

Confirm the Event Server is Functioning

To confirm the event server is functioning and listening on the correct port for incoming events, open the event server diagnostic window.

1. In Protege GX, navigate to **Sites | Controllers | General** and expand the **Diagnostic windows** section.
2. Select **Open event server diagnostic window**. You should see a message that reads 'Listening on Port : 22000'.

   The default event server port is **22000**, but this can be changed in **Global | Event servers**.
3. If the event server diagnostic window shows messages about an unknown serial number, events are being received from a controller with the serial number listed in the message. This also means the event server is accepting incoming events.
4. In the controller web interface, ensure that the **Event Port** matches the port set in Protege GX.
5. If you change the event port you must **save** and **restart the controller** using the icons in the upper right before your changes will take effect.

If the event server diagnostic window contains no text there is a problem with the configuration of the event server. This means the event server is **not** accepting incoming events. This can sometimes be resolved by restarting the Protege GX Event Service:

1. Open the **Services** snap-in by:
   - Pressing the **Windows + R** keys
   - Typing **services.msc** into the search bar and pressing **Enter**
2. Locate the Protege GX Event Service. Right click on the service and select **Restart**.

Confirm Event Server IP Address

For messages to get from the controller to the server, the controller must have the correct IP address for the event server.

1. On the server computer, open a command prompt. Enter the command `ipconfig` and press **[Enter]**.
2. You will be presented with the status and details of the server on various sub networks. Locate and copy the **IPv4 Address** for the sub network that the controller is connected to.

   For more complex networks it may be preferable to open a command prompt on a machine the controller is directly connected to and use the `ping` command to ascertain the external IP address of the server.
3. In the controller web interface, on the **System Settings** page, check that **Event Server 1** has the correct IP address. Paste in the address located above if it does not match.

   There are three spaces for entering the event server IP. This is for situations where controllers have multiple paths to the server. In most cases the second and third event server IP addresses should be left as all zeros or all 255s.

Confirm Ports

Next, ensure that the download and control ports set on the server match those set in the controller interface.

1. In Protege GX, navigate to **Sites | Controllers | General** and check these values:
   - **Download port** (default 21000)
   - **Control and status request port** (default 21001)
2. In the controller web interface, on the **System Settings** page, ensure that the **Download Port** and **Control Port** match those defined in the software.

3. If you have changed any settings on the controller, save your changes and restart the controller for the changes to take effect.

Check Computer Name

The download and event servers must have a correct computer name that matches the server machine. This usually only changes when you have restored a database from a different PC.

IMPORTANT: The computer name must be no longer than **15 characters**, or downloads will fail.

1. On the server computer, open **Control Panel > All Control Panel Items > System** to view computer information.
2. Copy the **Computer Name**.
3. In Protege GX, navigate to **Global | Download server** and check that the **Computer name** matches the name of the server machine. If not, paste in the name copied earlier.
4. Navigate to **Global | Event server** and again check and correct the **Computer name**.
5. If you have changed the computer name for either server, you must restart the corresponding service.

   Open the **Services** snap-in by:
   - Pressing the **Windows + R** keys
   - Typing **services.msc** into the search bar and pressing **Enter**
6. Locate the Protege GX services. Right click on the download service and/or event service and click **Restart**.

Repair Database Compatibility

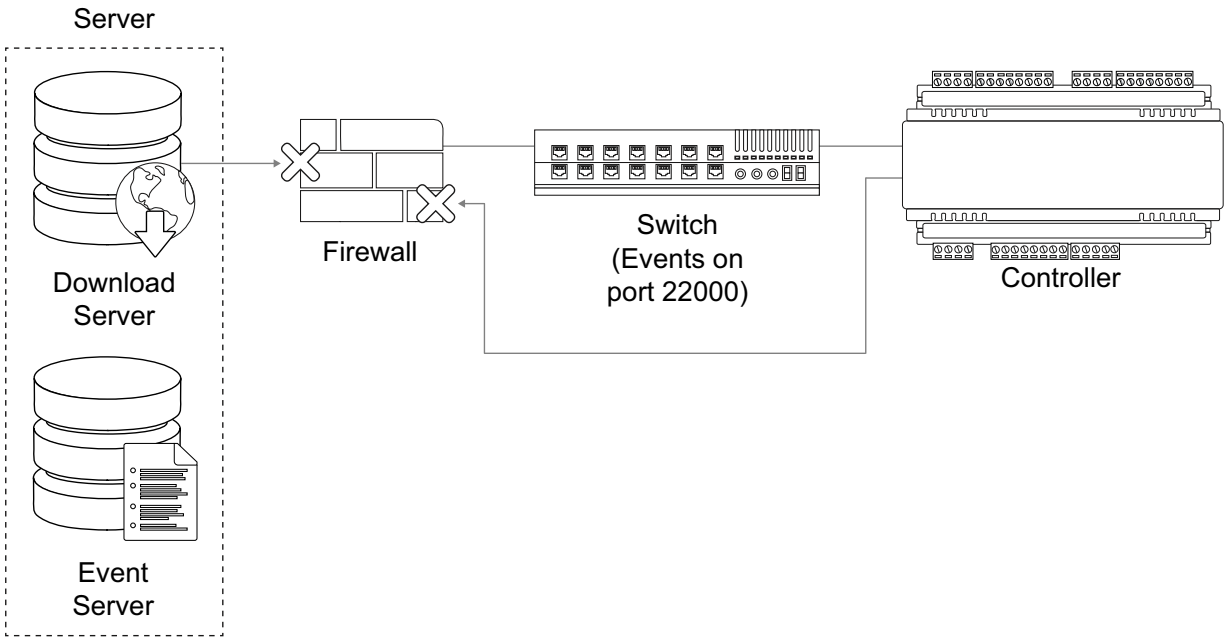
If you have restored a database from an older version of Protege GX, there may be a mismatch between the software and database versions. In this case the Protege GX Data Service will fail to start, the download and event server diagnostic windows will both remain blank, and no downloads will be passed to the controller.

To resolve this issue you must **uninstall and reinstall** Protege GX. This will prompt a database upgrade.

A backup taken from a newer version of Protege GX cannot be restored to an older version.

Windows Firewall

When the controller and server are on the same local network the only place a firewall can be blocking messages is on the server machine itself. This is called the Windows Firewall.



1. Open the Windows Firewall settings at **Control Panel > All Control Panel Items > Windows Firewall**. If the firewall is on, it is shown in green.
2. To eliminate the Windows Firewall as a cause of communication problems, turn it off temporarily by clicking **Turn Windows Defender on or off** at the left of the screen. Disable the firewall for each network location.

   Check whether this resolves the issue. If so, you can turn the Firewall back on and allow the Protege GX services through the Firewall.
3. Click the **Allow an app or feature through Windows Defender Firewall** link on the left of the screen.

   Third-party antivirus or firewall software may prevent modification of Windows Firewall rules. If this is the case, refer to the third-party manufacturer for details on allowing programs through the firewall.
4. Select **Allow another app...** to add a program as an exception.
5. Click **Browse...**, then navigate to the Protege GX installation directory.

   The default installation directory is C:\Program Files (x86)\Integrated Control Technology\Protege GX.
6. Select (double click or select and **Open**) the executable that you want to allow, then click **Add**.

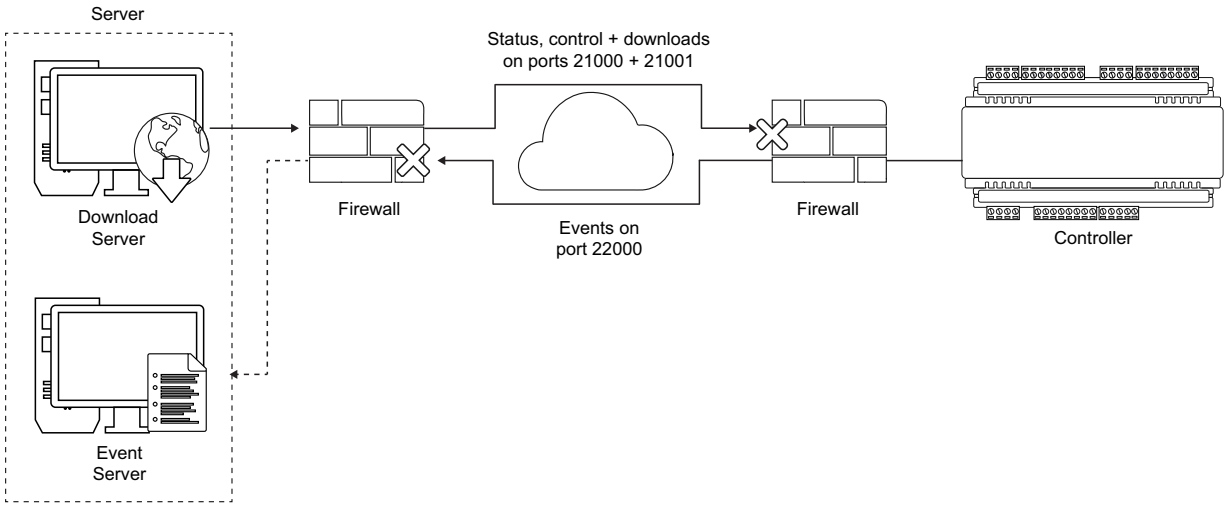
   Add the following Protege GX executables, one by one:
   - GXSV.exe
   - GXSV2.exe
   - GXSV3.exe
   - GXPI.exe
   - GXEvtSvr.exe
   - GXDVR1.exe
   - GXDVR2.exe

   This allows the necessary Protege GX services access through the Windows firewall.

   The above process will only allow access through your primary network connection. If you have multiple networks connected you will need to manually allow access (tick the checkbox in the network column) for each additional network that the Protege GX executable requires access through.

Multiple Firewalls

On corporate networks there can be multiple firewalls.

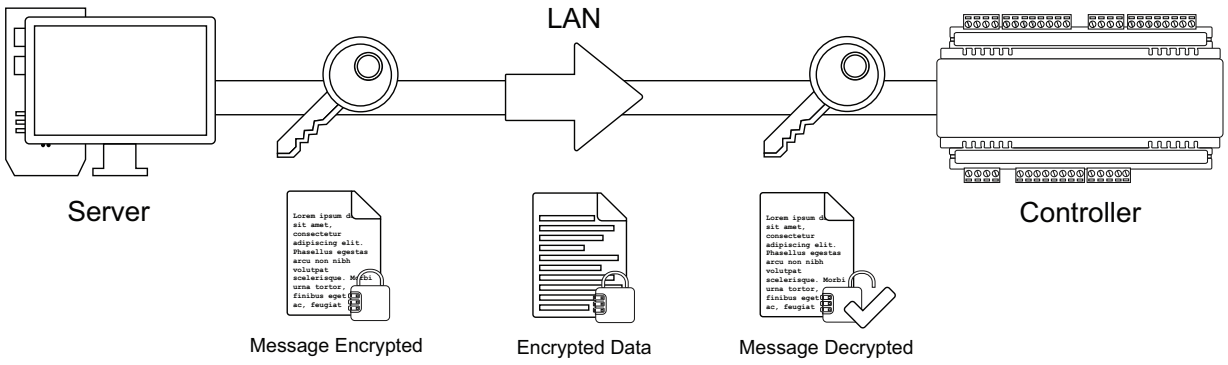


To ensure these are configured correctly, provide the Protege GX Network Administrators Guide to the appropriate IT staff member. This document is included in the software installation pack.

Encryption

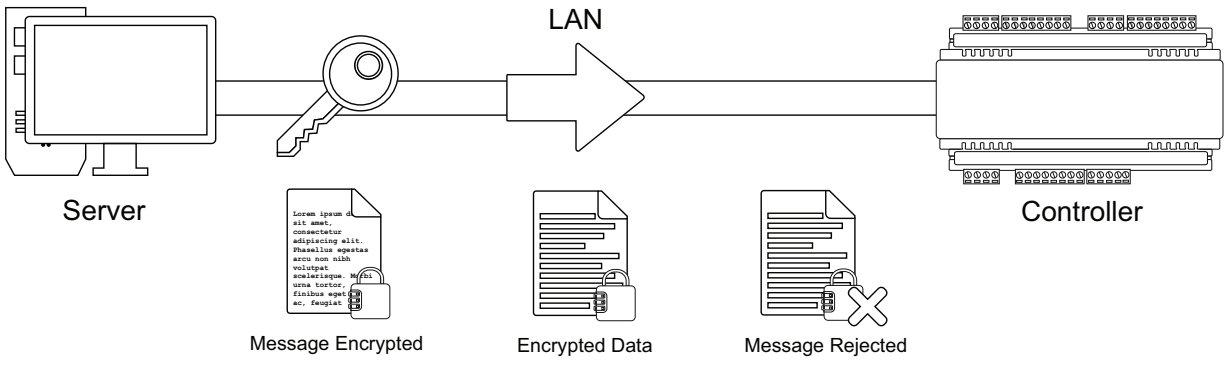
Both Server and Controller Encryption Enabled

Encryption relies on a shared key that both the sender and receiver of a message know. The message is encrypted using the key, then decrypted by the receiver using the same key. If the message is intercepted, it will make no sense to anyone without the encryption key.



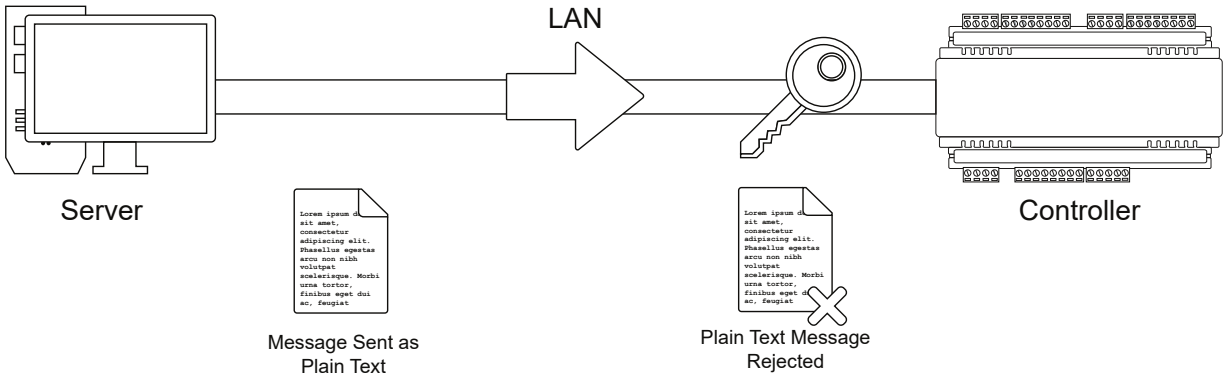
Server Enabled, Controller Disabled

If the receiver loses the key it is unable to decrypt incoming messages. In this case, the message is rejected.



Server Disabled, Controller Enabled

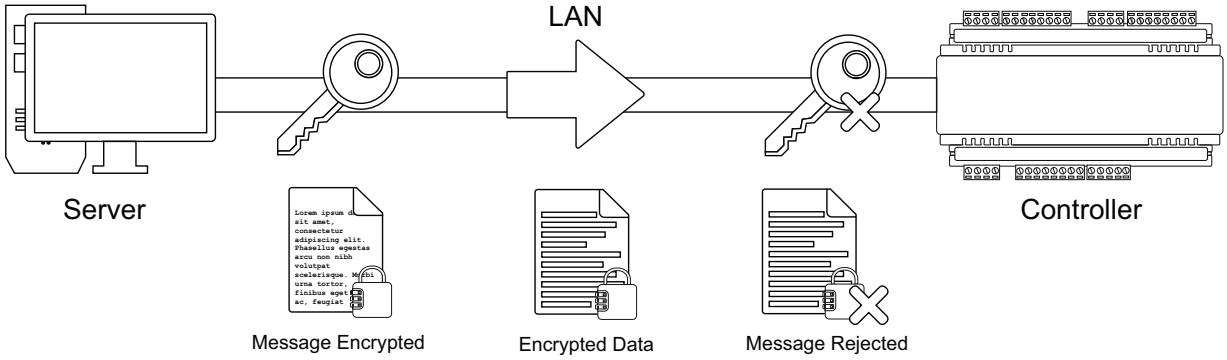
If the sender loses the key the message is sent in plain text. The receiver, expecting to receive encrypted events, will also reject the message as it may be of a malicious nature.



Server and Controller with Different Encryption Keys

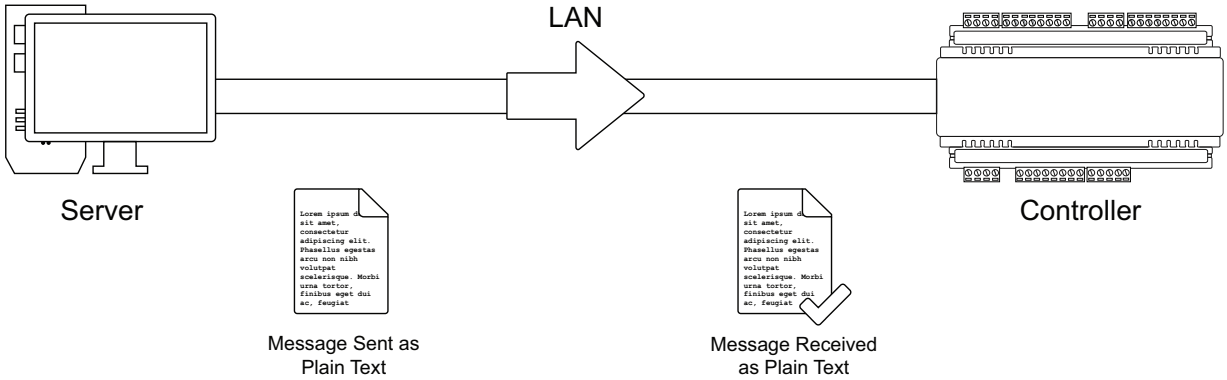
If the sender and receiver have different keys the message cannot be decrypted by the receiver. This also results in the receiver rejecting incoming messages.

Each time encryption is enabled at the server a new encryption key is generated. Each controller has a unique key, independent from all other controllers. If encryption for a controller is disabled, then enabled again, the key is changed. If encryption for a controller is disabled at the server, the controller must be defaulted. It is not possible to re-enable encryption without first defaulting the controller.



Both Server and Controller Encryption Disabled

If encryption is disabled at both the sender and receiver, received messages are accepted. The downside with this scenario is that anyone 'listening' between the sender and receiver can also receive the messages.



Disabling Encryption

Defaulting the controller is the only way to remove the encryption key. This is by design and intended as a security feature. It means that physical access to the controller must be gained before encryption can be disabled.

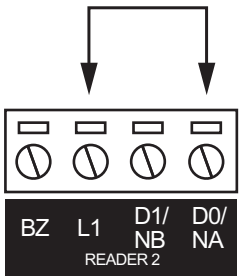
If you are unsure of the state of encryption of either the server or controller, disable encryption at the server, then default the controller. This ensures that neither is encrypted and rules this out as a cause of communications problems. Encryption should then be re-enabled once communications are established.

Disabling Encryption at the Server

If the controller is defaulted, encryption must be disabled at the server before communications can be established. Navigate to **Sites | Controllers | Configuration** and click **Disable controller encryption**. The software warns you prior to disabling encryption.

Defaulting a Two Door Controller

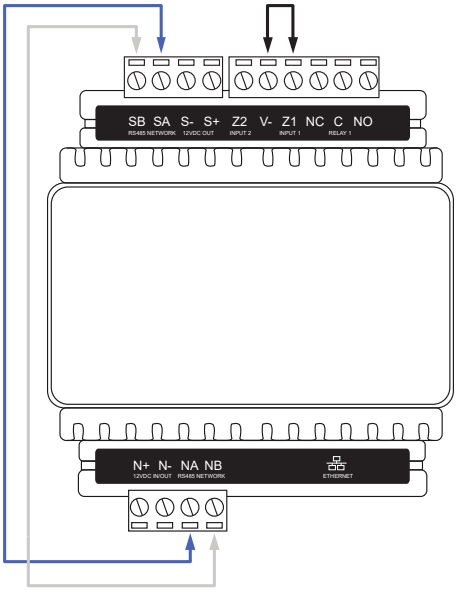
1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between the **Reader 2** D0 input and the **Reader 2** L1 output.



4. Power up the controller. Wait for the status indicator to begin flashing steadily.
5. Remove the wire link **before making any changes to the controller's configuration**.

Defaulting a One Door Controller

1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **NA** of the module network and **SA** of the reader network, and between **NB** of the module network and **SB** of the reader network.
4. Connect **Input 1** to ground.



5. Power up the controller. Wait for the status indicator to begin flashing steadily.
6. Remove the wire links **before making any changes to the controller's configuration**.

The system will now be defaulted with all programming and **System Settings** returned to factory configuration, including resetting the IP address and all network configuration, and removing all operator records.

- Defaulting the controller resets the IP address to the factory default IP of 192.168.1.2.

  Earlier versions of the controller firmware do not reset the IP address. If the controller is not available on 192.168.1.2 you will be able to connect to it via its previous IP address.

- Any configured system settings (e.g. **Default Gateway**, **Event Server**) are reset to their default values.
- Any custom HTTPS certificates are removed and the default certificate is reinstalled.

  Earlier versions of the controller do not have a default HTTPS certificate installed. If the controller is not available via HTTPS, connect to it via HTTP.

- All operator records are removed and the admin operator must be recreated.
- All other programming is removed.

After Defaulting a Controller

Before making any changes to the controller's configuration or upgrading the firmware, **remove the wire link used to default the controller**.

After defaulting a controller a number of essential steps will need to be performed to resume normal operation. Not all of the following steps will necessarily be required, depending on your site configuration:

1. Connect to the controller's web interface using HTTPS, unless it is an older controller with no default certificate loaded, then it will connect using HTTP.
2. Recreate the admin operator and log in to the controller's web interface.

   If you are not prompted to create the admin operator, the default username is admin with the password admin.

3. Reset the controller's IP address to its previous value.
4. Reconfigure any additional network settings.
5. Reinstall previously installed custom HTTPS certificates.
6. Restore any other system settings as required by your site configuration.

Telnet

To confirm a network path exists from the server to the controller and the correct ports are open, you can telnet to the controller on the download port (by default port 21000).

1. If the Telnet feature is not turned on, open the **Control Panel > All Control Panel Items > Programs and Features**.
2. Click **Turn Windows features on or off**. Locate the **Telnet Client**, check the box next to it and click **OK**.
3. Open a command prompt and attempt to telnet to the controller.
   For example, enter the command `telnet 192.168.1.2 21000`
   - If the controller can accept the connection, a clear screen appears with a cursor blinking in the top left corner.
   - If there is no connection, a message will advise there is still a problem between the server and controller. If you can web browse to the controller, it is likely a firewall is blocking the connection somewhere.

Finally, to confirm the event server is able to accept connections, configure a laptop with the same IP settings as the controller.

1. Remove the ethernet plug from the controller and plug into your laptop.
2. Try to telnet to the server IP address on the event server port (22000 by default):
   `telnet 192.168.1.100 22000`
   - If the server is able to accept connections, the clear screen and blinking cursor appear.
   - If the server is not reachable, a message will advise there is still a problem, indicating a firewall is blocking port 22000 to the server.

ICT Technical Support

If all the above options have been exhausted, contact ICT Technical Support. Ensure the results of all tests are at hand. If it is possible to get internet access on the server, a remote support session can be initiated.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.