DEFENDAS

Installation Guide

ST Series Access Controller

Version: 1.0

Safety Instruction

⚠ **Please note the following cautions. Mis-operation may lead to any injury or equipment failure:**

1. Do not power the system before installation is complete.
2. All peripheral devices must be grounded.
3. The conduits of wires under relay must be matched with metal conduits, other wires can use PVC conduits.
4. It is strongly recommended that the length of the exposed part of any connection cable should not be longer than 0.157"(4mm). Professional clamping tools may be used to avoid unintentional contact of exposed wires to avoid short-circuit or communication failure.
5. It is recommended that the card readers and the buttons should be installed at a height of 55"-59" (1.4m-1.5m) above ground.
6. It is recommended to use the power supply for the control panel, and external power supply for each lock.
7. The appliance shall be installed and wired in accordance with the national electrical code and by qualified personnel only.

Control Panel LED Indicators

There is 6 LED indicator present in the device, they are POWER(Red), RUN1(Green), COMM1 (Yellow), COMM2 (Yellow), WLAN (Green) & Door (Green).

When the STX00B is powered on, normally the **POWER** indicator (red) is lit constantly, the **RUN** indicator (green) shall flash slowly (indicating the system is normal), and other indicators are all off.

COMM1 indicator (yellow): It flashes when the system is communicating with upper-level devices (e.g., PC).

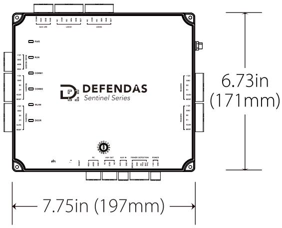
COMM2 indicator (yellow): It flashes when the system is communicating with lower-level devices (e.g. readers). When the indicator is flashing continuously, it indicates data transmission. When the indicator is flashing slowly, it indicates real-time monitoring status.

WLAM indicator (green): When the indicator is flashing continuously, it indicates the system is communicating in wireless (Wi-Fi) mode.

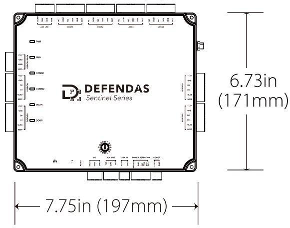
DOOR indicator (green): When the indicator is flashing continuously, it indicates a door opening signal (a door is opened).

Product Dimension

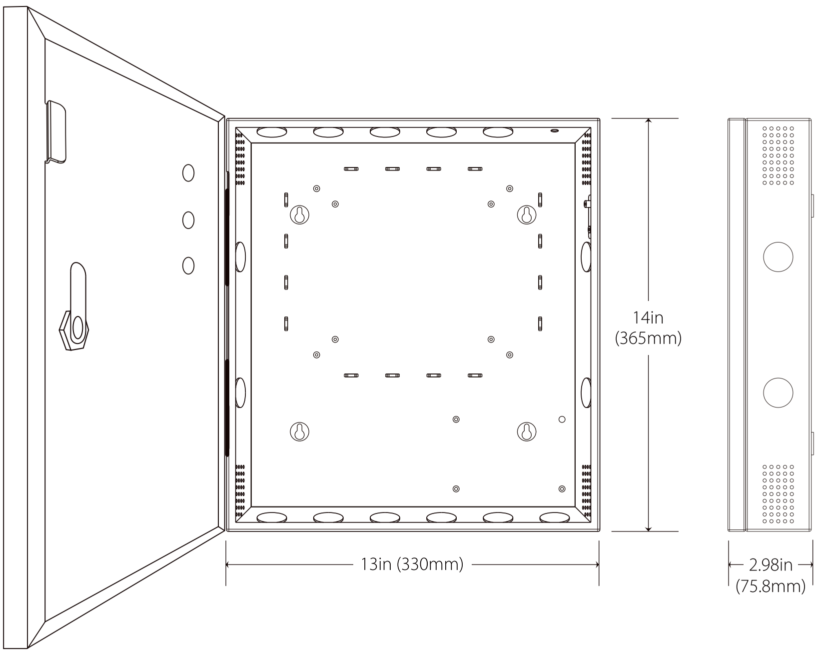
ST200B



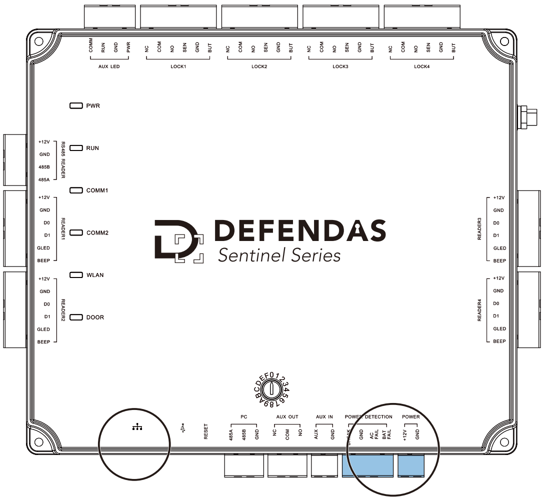
ST400B



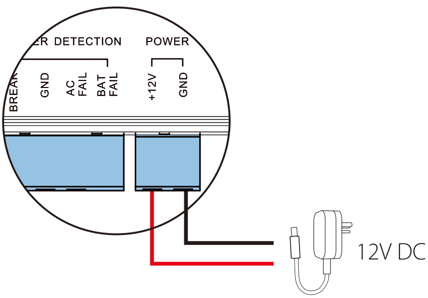
Metal Cabinet



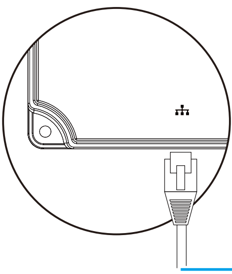
Internal Wiring Diagram



12V Power

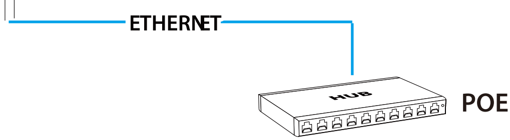


POE Power

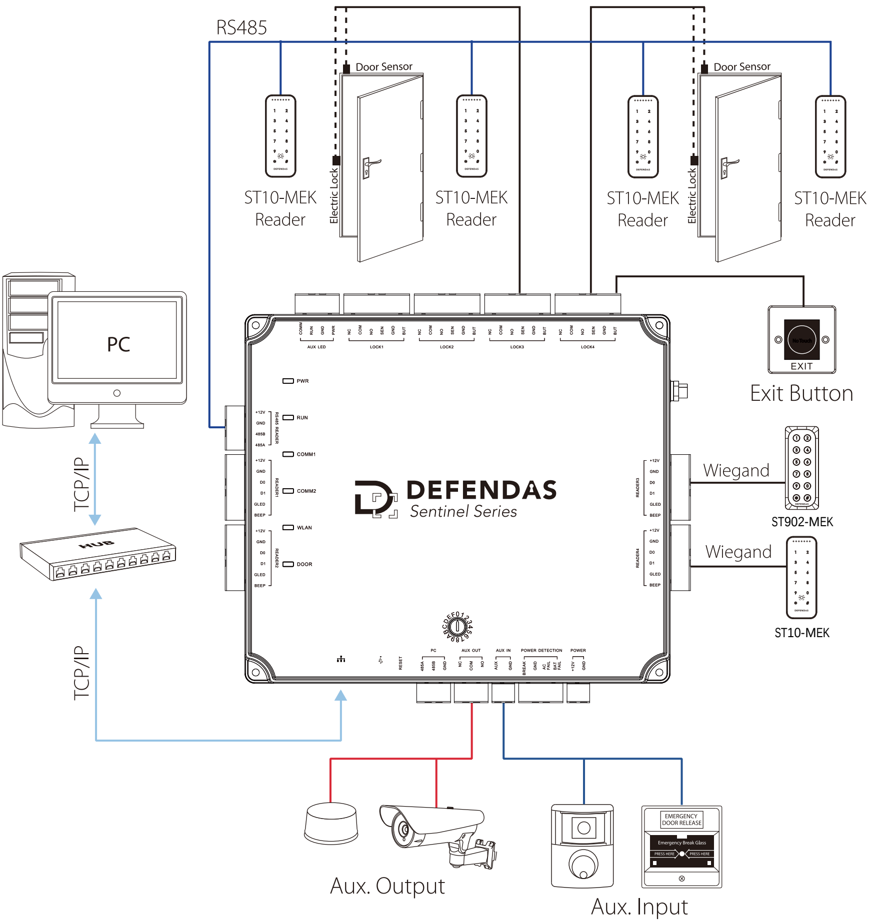


1) This product comes with a 12V DC surge protected Class 2 power supply.

2) This product comes with a POE cable source. This equipment is in compliance with section 34.7 of UL 294, 7th Edition.



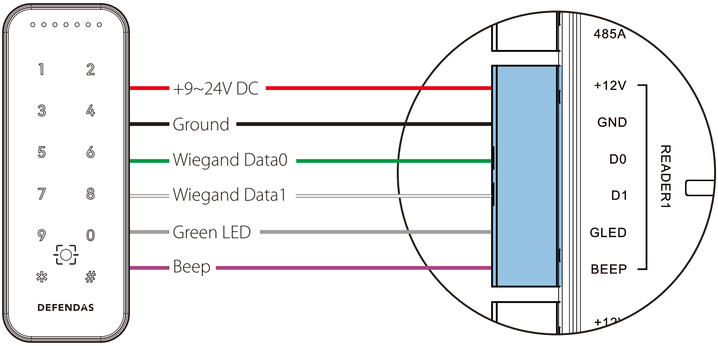
Wiring Legend



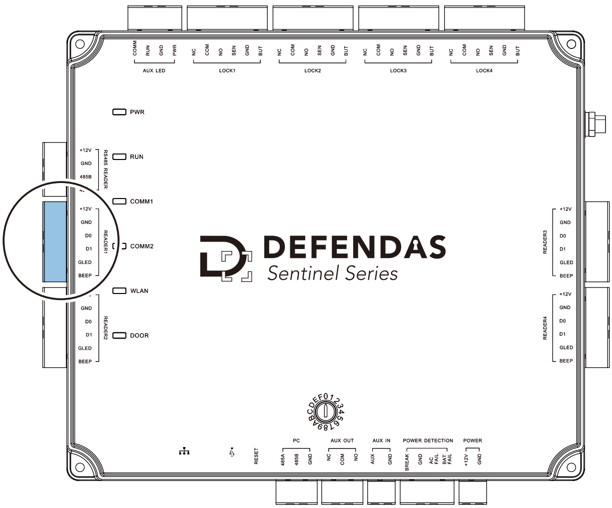
Notes:

1. The auxiliary input may connect to infrared body detectors, fire alarms, or smoke detectors.
2. The auxiliary output may connect to alarms, cameras or doorbells, etc.
3. The RS485 Reader port can be connected externally to RS485 reader.
4. The terminals above are set through the relevant access control software. Please see the respective software manual for further details.

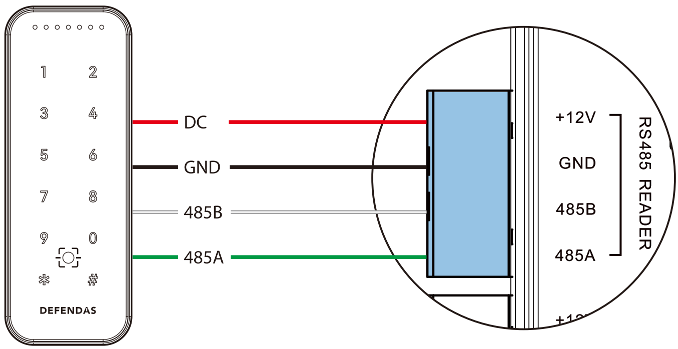
Wiegand Connection



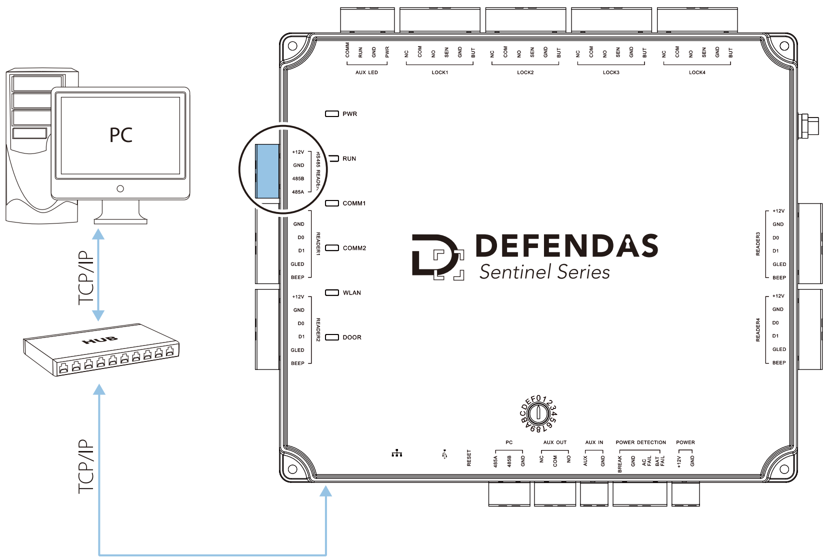
ST10-MEK Reader



OSDP Connection

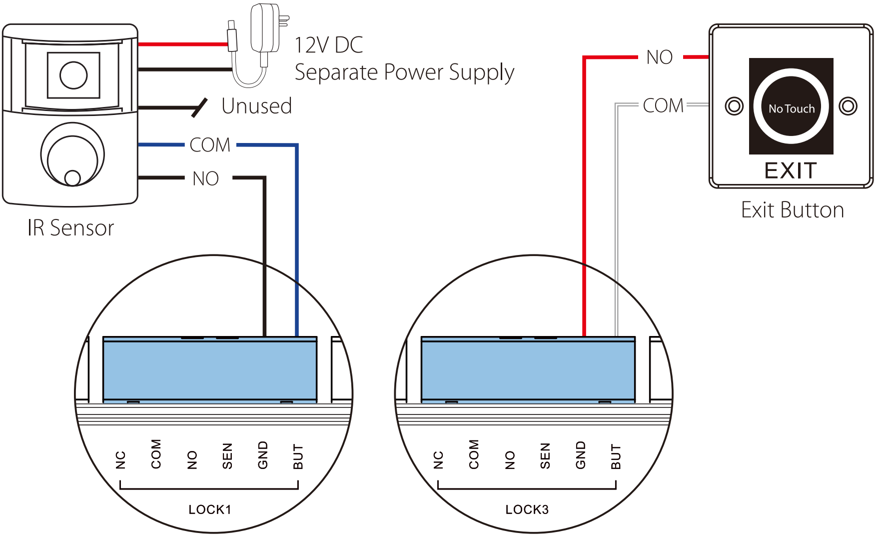


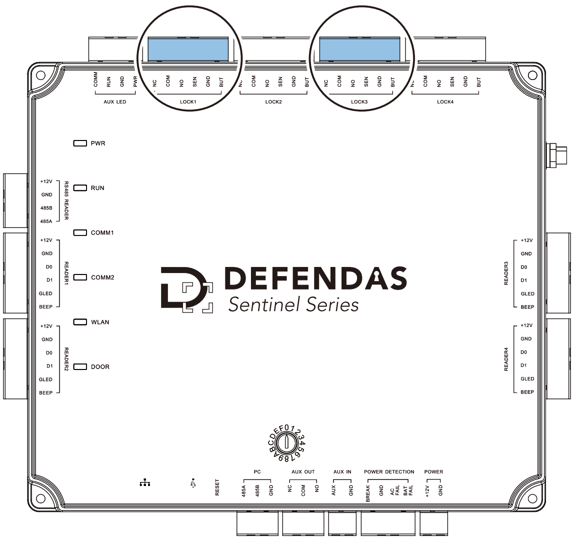
ST10-MEK Reader



Note: OSDP and RS485 cannot be connected to one control panel at the same time.

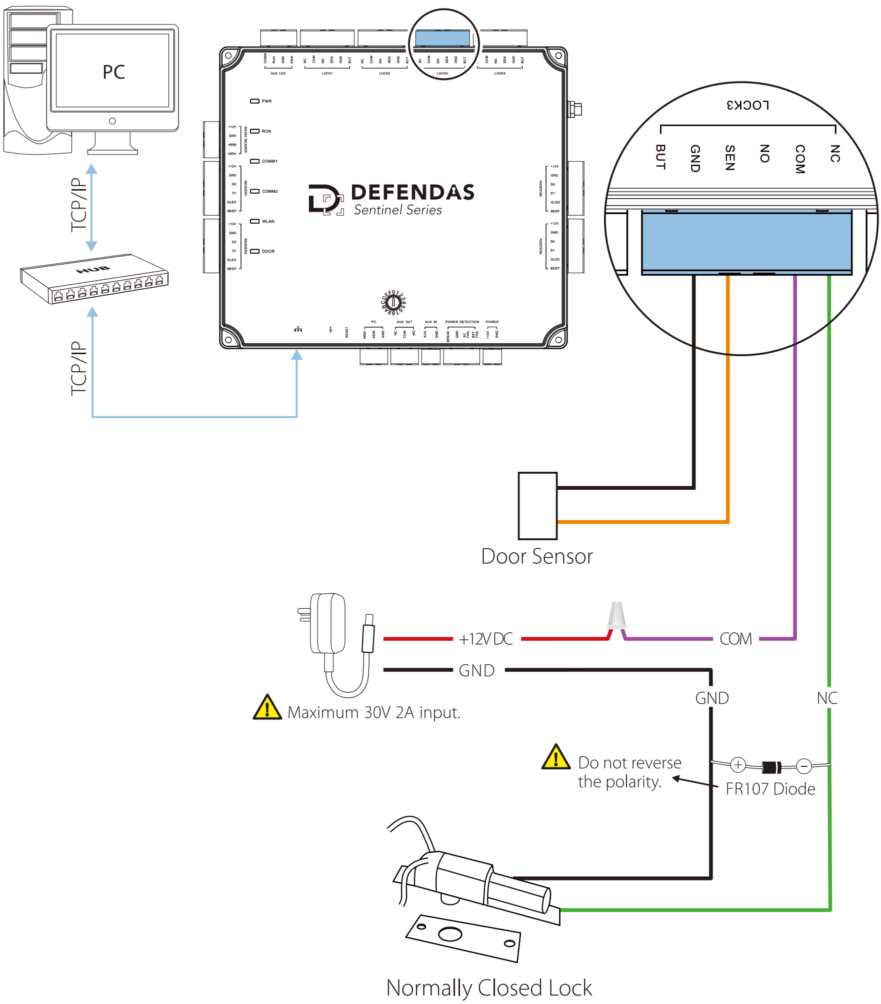
REX Connections



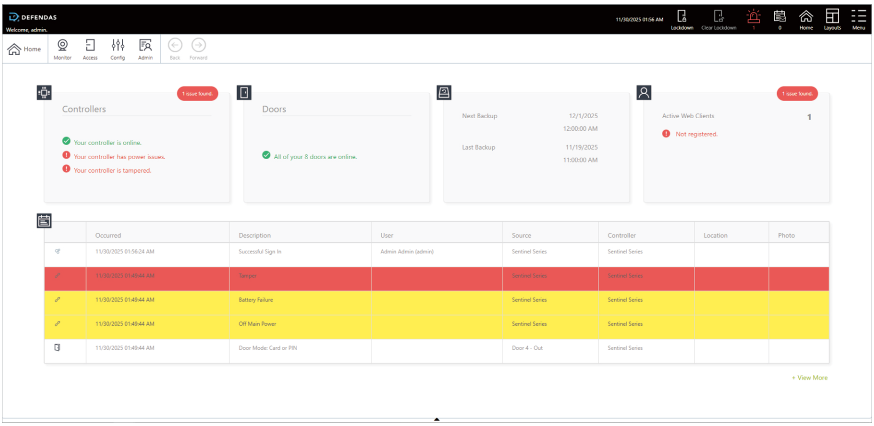


Lock Relay Connection

The system supports both **Normally Opened Lock** and **Normally Closed Lock**. The **NO Lock** (Normally Opened when powered) is connected with '**NO**' and '**COM**' terminals, and the **NC Lock** (Normally Closed when powered) is connected with '**NC**' and '**COM**' terminals. As shown in the example with NC Lock below.



ST Series Web Management Application



Introduction

Requirements

1. Obtain an available static IP address and configuration from the network administrator.
2. (Optional) Obtain a signed HTTPS certificate. This provides some additional security and avoids web browser warning messages. Supported certificate formats are PEM or PFX. See "Complete the Configuration," below.
3. Find out whether using network time protocol (NTP) to automatically update the controller clock over the Internet is possible and acceptable, as well as whether non-standard time servers are used (such as corporate time servers). With a typical small network, it is safe to assume NTP will work with default ST Series settings.

Procedure

1. Understand how a ST Series system networks together by reading the brief section, "Understanding the ST Series Network".
2. Connect a computer directly to a controller and run the initial configuration program. This step must be completed before the controller operates on the network.
3. Connect the controller to the local network.
4. Log in to the controller with a web browser and complete essential configuration.
5. Add a user and test door access.
6. Add any secondary controllers you are installing.

Help

This guide refers you to online help topics for more detailed information. The help is available once you have connected the first controller and logged in to the Web Management Application. Open it by selecting "Help" from the menu in the upper right corner.

Understanding the ST Series Network

Expected Browser Warnings

Your browser will display an insecure site warning each time you log in to the Web Management Application. The exact text of the warning, and the way to resolve it, varies among browser applications. You can prevent this warning by installing a signed HTTPS certificate when directed, below.

All ST Series systems have a single “primary” controller. Many “secondary” controllers may be added to support additional doors. All secondary controllers maintain a connection to the primary, and the primary provides all data and configuration the secondaries need to operate.

The primary controller provides a Web Management Application you can log into from a web browser. This application on the primary controller is where you will manage all configuration for the entire system.

Network Considerations

Ideally, all controllers should be networked on the same subnet. If you have a simple home or small office network, this will almost always be the case. For more complex networks, be sure to review the “Special Considerations” discussed at the end of this document before proceeding.

Initial Controller Setup

Connecting

1. Connect the controller to DC power.
2. Connect an ethernet cable directly from your computer to the controller.
3. If your computer is set to use a static IP address, you will need to temporarily change it to one in the range 169.254.202.xxx, or to DHCP. If you normally use DHCP, skip this step. If you do not know, try assuming you use DHCP, which is common.
4. Open a web browser and enter the default controller address: **169.254.202.242**. You should get an insecure site warning from the browser (see above). After resolving the warning, you will be directed to the Web Management Application login screen. Note that it might take a minute for the connection to become available.

Trouble Connecting: If at any point you find you cannot connect to the controller at the default IP address, or the address you configure, below, you can try a hard network reset. Find the small opening on the controller labeled "Reset." Insert a paperclip to depress the button for **5-20** seconds. The controller address will revert to the default, 169.254.202.242, until rebooted, reset, or the configuration is modified.

Running the Setup Wizard

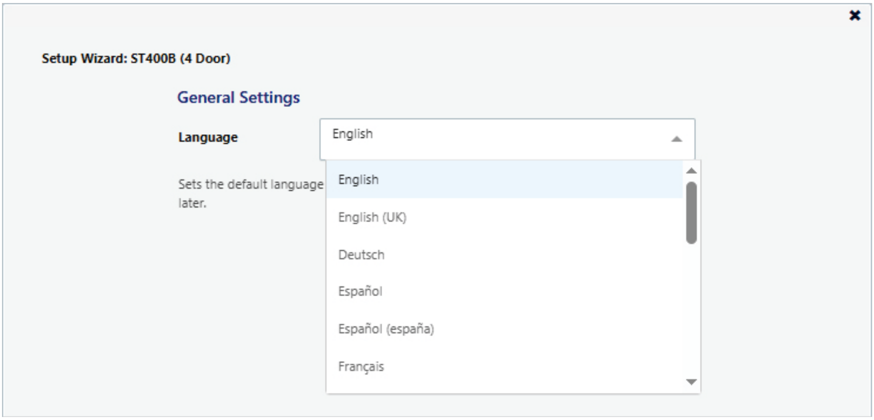
Log in using the default administrator account:

- User name: **admin**
- Password: **admin**

You will be directed to the Setup Wizard, where you will enter information required for the controller to operate.

Initial Controller Setup

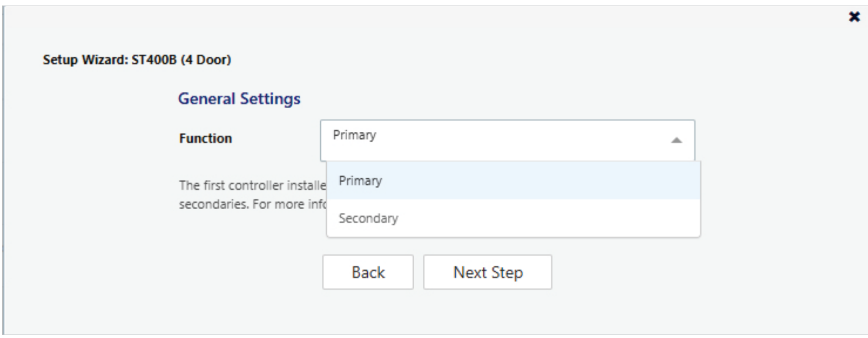
Page 1: Language



Choose a language. Your choice will be used for this wizard. It will also become the default language of the Web Management Application. This can be changed later in the hardware configuration of the primary controller.

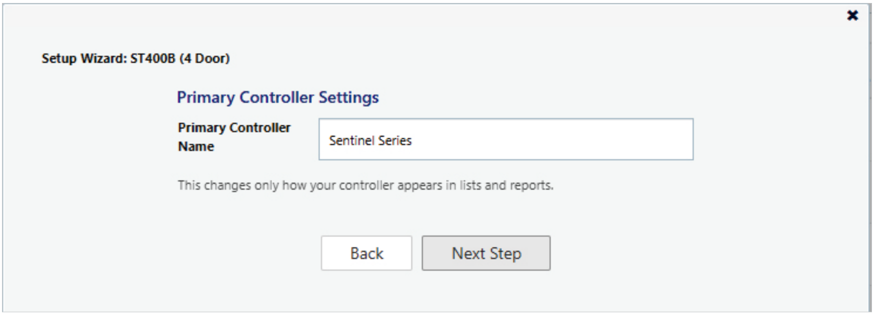
Note: For secondary controllers, Language does not affect the Web Management Application. It does set the language of the simplified management application on this controller, and can be changed later in the configuration of this controller.

Page 2: Function



Choose whether this controller will be a "Primary" or a "Secondary". Make sure you understand the ST Series network, discussed above. The first controller installed should be a primary, and all others should be secondaries.

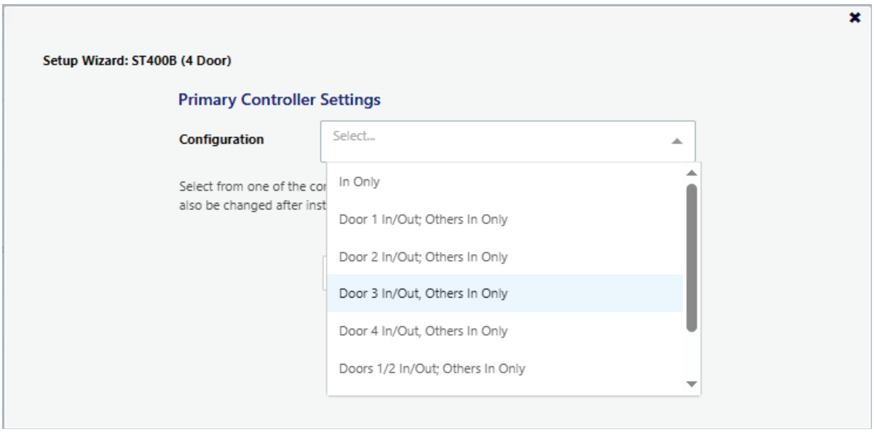
Page 3: Primary Controller Name (primaries only)



The name of the controller will be used for display in the Web Management Application and in reports.

Note: secondary controllers are named when they are connected to the system in the Web Management Application.

Page 4: Configuration (primaries only)



This determines what your controller will be used for: controlling door entry, perhaps door exit, or as special purpose readers.

Note: Secondary controllers are configured when they are connected to the system.

Initial Controller Setup

Configuration options available depend on the controller model. Each option will involve one or more of the following possibilities. Each possibility determines the function of the card, PIN, or readers connected to the controller. The configuration can be modified during "Complete the Configuration," below.

In Only - The most common configuration, where a reader is used to gain entry,but no credentials are required to exit (although an exit button may be configured for opening the door from the inside).

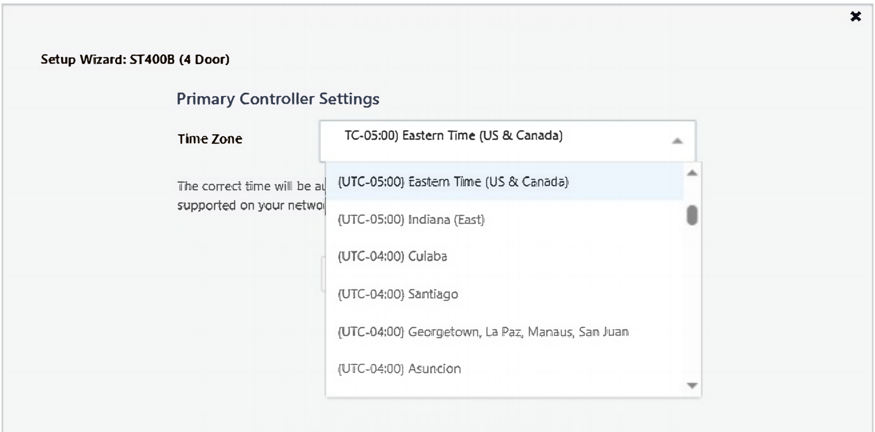
All controllers will have at least one "In" reader. It cannot be configured for another purpose, though you may choose not to use it.

In/Out - The physical door will have a reader both inside and outside. Authorization is required to pass either direction.

+ Muster Point - The second reader will serve as a muster point, where users can register that they have reached a safe location.

+ Card Enrollment Point - The second reader will be used to easily enter card numbers when adding users.

Page 5: Time Zone (primaries only)

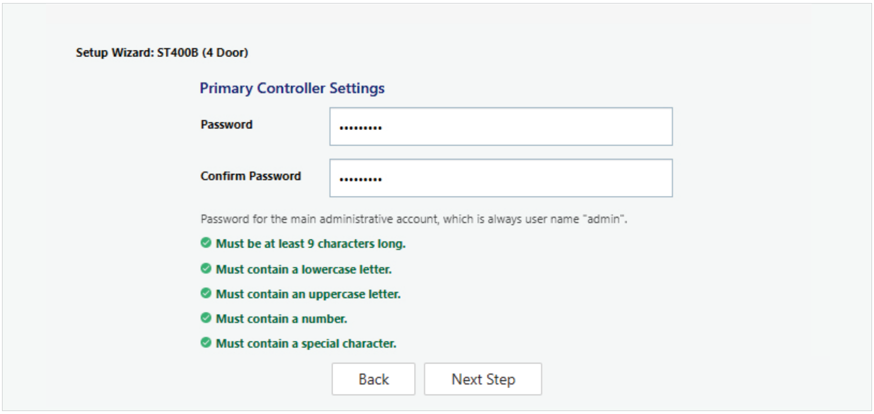


Select your time zone. In most cases you will never need to set the actual time; the controller will get the time from the internet using a technology called NTP. Other situations are discussed, below, under "Complete the Configuration."

Note: Secondary controllers get their time and time zone from the primary controller.

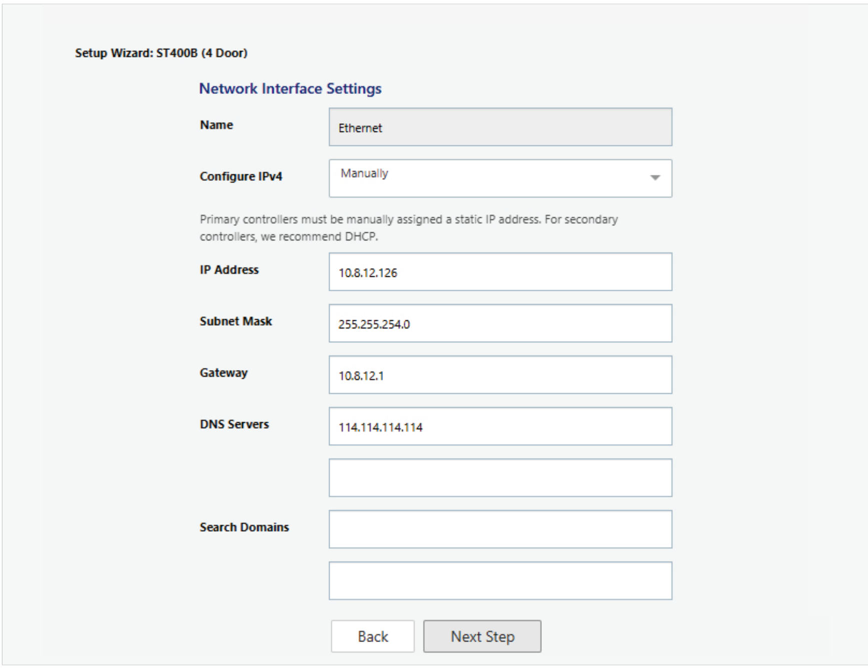
Initial Controller Setup

Page 6: Password (primaries only)



Enter a strong password for the primary administrator account. The user name for this account is "admin" and cannot be changed.

Page 7: Network Interface Settings



Initial Controller Setup

The important choice here is "Configure IPv4."

A primary controller must have a static IP address. This is because secondary controllers need to know how to find the primary on the network. Additionally, the users need a consistent address to log in to the Web Management Application.

To assign a static IP address, choose "Manually" and enter the IP address and configuration specified by the network administrator.

"Using DHCP" is probably the right choice for secondary controllers, unless you have a complicated network discussed below under "Special Considerations for Complex Networks."

> **Wireless Networking:** If your controller model supports WiFi, you still need to set up a wired connection, here. You can add your wireless connection once you are logged in to the Web Management Application. See the online help topic, "Administration: Network".

Page 8: Review

All your entries are displayed for review. Click either "Back" or "Complete Setup." After completing setup, you may disconnect the direct ethernet cable.

Connect the Controller to the Network

When you "Complete Setup," the controller will reboot itself automatically. If it is already installed, then simply reconnect its ethernet port to the local area network.

Otherwise, disconnect the controller and complete the physical installation. Connect it to the local area network via ethernet.

Complete the Configuration

Open a web browser and enter the IP address you specified in Network Interface Settings during initial setup. This will direct you to the login screen of the Web Management Application. Enter "admin" as the user, and use the password you set during initial configuration. The application Dashboard will appear. Expect to see green status, indicating everything has completed correctly to this point.

Review Time Settings (optional)

By default, the primary controller will use network time protocol (NTP) to automatically update the controller clock over the internet. This might not work due to local policies or because your controller does not have internet access.

If you need to change this configuration go to "**Admin → Date and Time**."

- To disable NTP, uncheck "Update Date and Time Automatically." When this box is not checked, you can manually set the time by checking "Set Server Time to Current Browser Time" and clicking Save.
- If you wish to use NTP, but with customized NTP servers, there is space to enter those server addresses. The default servers are: "0.pool.ntp.org," "1.pool.ntp.org," "1.pool.ntp.org," and "3.pool.ntp.org."
- You can also turn off the use of Daylight Savings Time.

Registration (optional)

Registration is required if you ever need to reset your system password, and optionally allows LT Security to contact you about software updates and other information. Follow these steps to register for the first time or to update your registration information.

1. Registration can be started in two ways:
   - When you log in the first time, click Register Now in the "Register Your Product" pop-up window, or
   - Select "**Menu → About**," and click the Register button. (If you have previously registered, the link is "Update Registration.")
2. Click New Registration button in the next pop-up window. (If you have previously registered, the button is "View/Update Registration.")
3. Fill in the registration information. Asterisks indicate required information. The email address you enter must be able to receive your registration information.

Complete the Configuration

4. Submit your registration automatically or by email.

   a. For automatic registration, click Submit Online button. You will see a progress window followed by a success message.

   b. For email registration:

      i. Click Offline Registration button. Read the instructions in the following window.

      ii. Click Download registration file link, and save the registration data file to your computer.

      iii. Create and send an email message by clicking the email link or entering it in your email program. Your email must contain the registration data file as an attachment, with its original name. The subject and text of the email do not matter.

You will receive a registration confirmation file by reply email. When you do,

1. Open the email and save the attachment to your computer.
2. Click Upload Confirmation button. (If you have already exited from registration, then return to this option by selecting "**Menu → About**" and clicking the Register button.)
3. Find and open the registration confirmation file you saved.

You should see a "Registration successful" message window.

Fine Tune Hardware Configuration

Configuration is discussed in detail in the online help topic, "Configuration: Hardware." Topics mentioned below are found within that section.

Go to "**Config → Hardware**." The list on the left shows all controllers. (At this point, you should see one, the primary.) Each controller has an "I/O" sub-controller listed beneath it. The controller item manages general controller configuration, while the sub-controller manages detailed configuration of the readers, inputs, and outputs.

Click the controller and review the configuration. Note under "Managed Doors" that doors were automatically created to match the controller configuration you chose earlier. Every reader is represented as a door, whether its function is in, out, card enrollment point, or muster point.You might need to:

Complete the Configuration

- Add more readers using the "Modify" button on the menu bar. Details about this operation are in the topic, "Modifying Controller Configuration". The Modify options are:
  - o "Change to In/Out"
  - o "Add Muster Point"
  - o "Add Card Enrollment Point"
  - o "Remove Secondary, Muster, or Card Enrollment Point"
- Change the default connection type for readers (Wiegand, OSDP). These settings are on the sub-controller, and are detailed in the topic, "Hardware Properties". The defaults vary by model and are listed in the topic, "Models and Configurations".
- Change the connection properties of inputs and outputs and configure optional functionality of auxiliary inputs and outputs. These settings are on the sub-controller, and are detailed in the topic, "Hardware Properties".

Configure Doors

Go to "**Config → Doors**". Every reader is represented as a door, whether its function is in, out, card enrollment point, or muster point.

For In and Out doors, change the "Default Mode" to set the door's normal locking state.

For In doors, review the lock timings and behaviors under "Operation".

Card enrollment and muster doors usually need little configuration.

Install a Signed Certificate (optional)

To provide extra security for the controller, and to avoid browser warnings when logging in, you might wish to install a signed HTTPS security certificate. For more information on what this means, and to get such a certificate, talk to your IT department.

Even if you do not install a signed certificate, all communications will still be encrypted.

To install a certificate:

1. Obtain a certificate file in .PEM or .PFX format and copy it to your computer.
2. Select "**Admin → Web Server Settings**."
3. Click Upload Certificate.
4. Complete the prompts to select and upload the certificate file.

Add a User and Test Access

1. Go to "**Access → Users.**"
2. Click **Create** on the menu bar.
3. Enter the following minimum required information:
   - First Name
   - Last Name
   - (To test cards) Scroll down to "Cards," click the **Add** button, then enter the number of a card.
4. Scroll down to "Door Access." Click the **Add** button and select 1 or more doors on the following screen.
5. Click **Save** on the menu bar.

The card and PIN you entered should now work to grant access at the specified doors, assuming you chose a compatible "Default Mode" during "Configure Doors."

To test access, you will (1) create an access level, (2) create a user, (3) give the user card, PIN, and (4) assign the access level to the user.

First:

1. Go to "**Access → Access Levels**."
2. Click "**Create**" on the menu bar.
3. Enter a "**Name**" for the access level.
4. Click the "**Add**" button.
5. In the pop-up window, select one or more doors that this access level will provide access to, and click "**OK**."
6. On the "Access Levels" screen, notice that each door has been added to the list with a schedule during which access will be granted. The default schedule, "24/7," provides access at all times. Schedules are explained further in the online help.
7. Click "**Save**" on the menu bar.

Then:

1. Go to "**Access → Users**."
2. Scroll down to "Access Levels." Click the **Add** button and select the access level you created, above.
3. Click **Save** on the menu bar.

Add a User and Test Access

The card and PIN you entered should now work to grant access to the specified doors during the specifed schedules, assuming you chose a compatible "Default Mode" during "Configure Doors."

Card formats that work out of the box are Wiegand (26, 34, 37, or 50 bits) and Corporate 1000 (35 bit). For other formats, see the online help topic, "Configuration: Card Formats."

More sophisticated ways to grant access to users are discussed in the online help under the main topic, "Access Control."

Card numbers can be more easily entered by using enrollment points. See the online help topic, "Features and Tasks: Card Enrollment Points."

The number of digits for PINs can be changed in "**Admin → System Settings**."

Adding Secondary Controllers

Step 1: Initial Setup

Follow the instructions under "Initial Controller Setup," above, for each controller. This will configure the controller for connection to the network.

Step 2: Add the Controller in the Web Management Application

Secondary controllers can be automatically found and added by the Web Management Application. This is called "Discovery."

There are two important qualifications about Discovery.

- When using Discovery, you should connect and discover controllers one at a time. This is the only way you can differentiate them.
- Discovery only works if all controllers are networked on the same subnet. If you have a simple network, this will almost always be true. In a larger corporate environment, you might need to add secondary controllers manually. See "Special Considerations…," below.

Adding Secondary Controllers

To discover secondary controllers:

1. Log in to the Web Management Application (on the primary controller).
2. Go to "**Config → Hardware**."
3. Click **Discover Controllers** on the menu bar.
4. In a few moments, a form will display all controllers discovered.
5. Click the link to add a controller. The create controller screen will appear.

    a. Select a "Configuration." (See "Initial Controller Setup", above.)

    b. Enter a "Name," and select "Custom Door Names" so you can name the doors.

    c. Leave all other settings as they are. These are the settings that were discovered.

    d. Click **Save** on the menu bar.

Special Considerations for Complex Networks

If all ST Series controllers cannot be located on one network subnet, or if Discovery is blocked by network restrictions, observe the following.

- There is no difference in the way you set up the primary controller.
- During "Initial Controller Setup" of secondary controllers on other subnets, do not select DHCP as normally recommended. Assign these controllers static IP addresses.
- Manually add these secondary controllers in the Web Management Application. Log in and read "Manually Adding Secondary Controllers" in the help topic, "Configuration: Hardware: Adding Controllers."

Where to Go Next

A complete user manual is available through the Management Application by selecting "Help" from the menu in the upper right corner.

The help's "Introduction" page will guide you to more information on operating the application, changing the configuration of controllers and doors, setting up door access, using emergency features, and more.

ETL Certification

Resistance to attack Level I;

Line security Level I;

Endurance Level I;

Standby Power Level I.