Access Control User Manual

Introduction

1 Introduction

Sentinel Series by Defendas is a powerful, yet intuitive, electronic door access-control system supporting the latest innovations in physical security and biometric access. Sentinel Series provides:

- Secure and convenient fingerprint access using Defendas' industry-leading biometric technology (Biometric Sentinel Series models only)
- Support for industry-standard OSDP and Wiegand card readers, with flexible card format definitions
- Powerful, intuitive, Web Management Application built into the Controller — all you need is a web browser; no PC software to install or maintain.
- Scalability up to 84 Doors by adding Secondary Controllers, quickly and easily using network-based discovery
- Critical emergency functions: global lockdown, global emergency unlock, alarm management, duress PINs, emergency codes, and muster reporting
- Mobile app for iOS and Android

Defendas' Sentinel Series is z9/op=n certified, powered by Z9 Security.

Using this Guide

The topics in this Introduction explain how to use the Web Management Application generally.

The four main sections correspond to the four main navigation menus: Monitoring, Access Control, Configuration, and Administration. These topics provide general guidance, and have a sub-topic for each menu item.

Features and Tasks describes special features that are not centralized, and explains tasks that are common to several screens.

Reference includes the Glossary and other reference material.

Getting Started

Your Primary Controller should already be installed and configured. (If the Setup Wizard appears when you log in, configuration is not complete. Complete the configuration before continuing.)

To get started:

1. Open a web browser and log in to the Web Management Application.
2. Register the product and add any additional licenses you purchased. Registration is required if you ever need to reset your system password, and optionally allows Defendas to contact you about software updates and other information. Additional licenses expand the capacity of your system.
3. Review the Home Screen and Menus.
4. Understand List Views and Property Views. Most screens use one of these views.
5. Take a look at the configuration of your Doors, particularly the **Default Mode** and the **Door Mode Schedule.**
6. Learn about the different ways you can assign door access to Users.

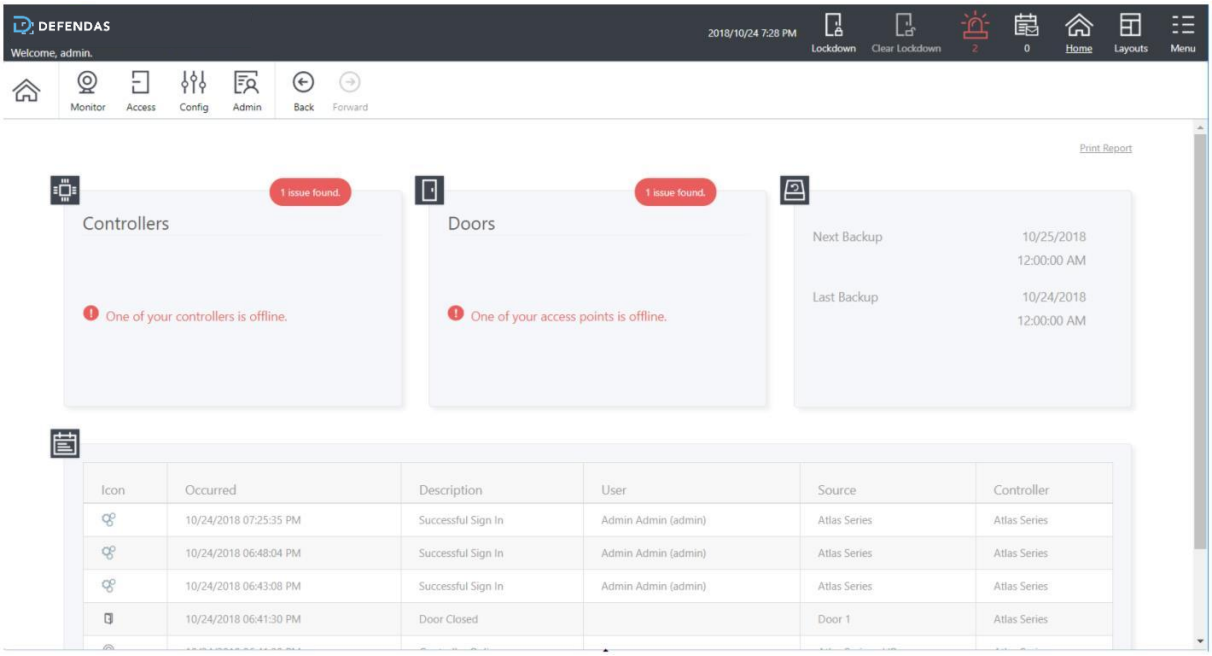
You now have a fully functioning access control system. Read about Monitoring and Notifications so you can see what's going on in your system.

Important: After getting started, learn to use the Sentinel Series Emergency Features. Some of these require significant setup before you can use them to protect your Users.

1.1 Home Screen and Menus

The Home Screen displays a dashboard-style summary of your system, including recent Event activity. The Menu Bar is available on this screen, as it is on every screen in the application.

Home Screen Dashboard



click to enlarge

Potential security issues and problems are highlighted in red, including Lockdown and Emergency Unlock counts. You can click the links for more information. You can always return to this screen using the **Home** button towards the upper right on the Main Menu.

The dashboard summary squares include:

- Controllers status summary — link takes you to Hardware
- Doors status summary — link takes you to Door Status
- Backup status (next scheduled backup, most recent backup) — link takes you to Backup and Restore
- Web/Mobile connected client count, and whether the Admin password has been secured (Go to the Users module and change the Admin password to secure it.)
- Recent Events — **+ View More** link takes you to Events

The exact summary squares visible depend on your User Role. Also note that when logging into a Secondary Controller, the summary squares are extremely limited due to the fact that the Secondary Controller gets its data from the Primary Controller.

Main Menu

The Main Menu bar is at the top right of all screens.

Lockdown and Clear Lockdown		Click **Lockdown** to quickly lock all Doors in an emergency situation. When a global lockdown is in effect, a message is displayed prominently in the Menu Bar. Note that initiating a lockdown will create an Alarm by default. Click **Clear Lockdown** to re-enable access and return Doors to their default or Scheduled Door Mode. See Lockdown for more information.
Alarms		When there are active Alarms, this icon will be red or yellow and show the number of current Alarms. Click to go to the Alarms screen.
Notifications		Click to view the Notifications you have subscribed to. The number of Notifications waiting for you is displayed under the icon.
Home		Return to the Home Screen.
Layouts		Layouts allow you to view multiple features or screens

at a time. For example, select a 3-panel layout to work on Access Levels and Schedules while viewing live Events. Each panel has its own navigation menu.

Select the single-panel layout to return to the standard view.

Menu 

Opens a menu showing several miscellaneous options. See below.

The exact Main Menu items available depend on your User Role. Also note that when logging into a Secondary Controller, the menu items are extremely limited, because it is mostly managed by the Primary Controller.

Navigation Menu

The Navigation Menu contains items for all of the main screens in the application, organized under four subject buttons. The Navigation Menu is repeated in every panel of multiple-panel layouts. This help manual is organized like the menu—four main sections containing a subtopic for each menu item.

The subjects are Monitoring, Access Control, Configuration, and Administration.

Use the **Back** and **Forward** buttons to navigate through your own history of accessing the screens. (The browser's navigation buttons do not work inside the Web Management Application).

The exact Navigation Menu items available depend on your User Role. Also note that when logging into a Secondary Controller, the menu items are extremely limited, because it is mostly managed by the Primary Controller.

Menu Button Items

Language Sets the language for the current User. Saved as the default for this User.

Available languages depend on your software license. Contact your authorized LTS representative for license upgrades.

Preferences Sets the preferences for the current User. Saved as the default for this User. The preferences are

- "Items per Page", the number of items shown in one page of a list, and
- "Card Enrollment Point."

Save Logs Creates a file containing program logs and other information for investigating problems. Use when asked to by technical support. If possible, save the logs right after you see a problem, and have it available when contacting technical support.

Help Opens this Help.

About Opens a window showing product information, including your current version and licenses. Register or add licenses on this screen.

Sign Out Log out of the Web Management Application, returning to the Login Screen.

1.2 Using List Views

List Views show a list of items in columns. In many cases, the columns can be changed, moved around, and searched.

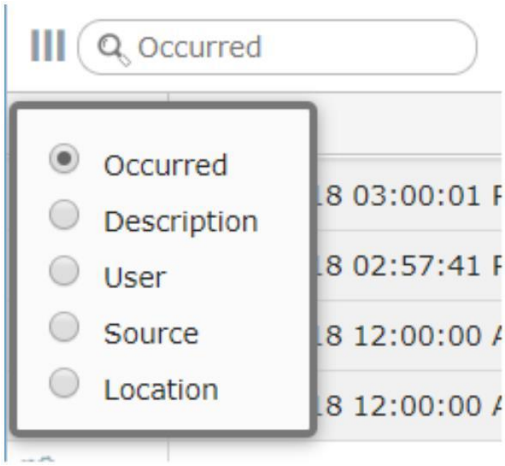
Note that Property Views also display a list on the left, which has the same controls.

Some List Views have an enhanced filter or search feature instead of the following controls.

Searching

To search in a column, enter the text in the box at the top of the list.

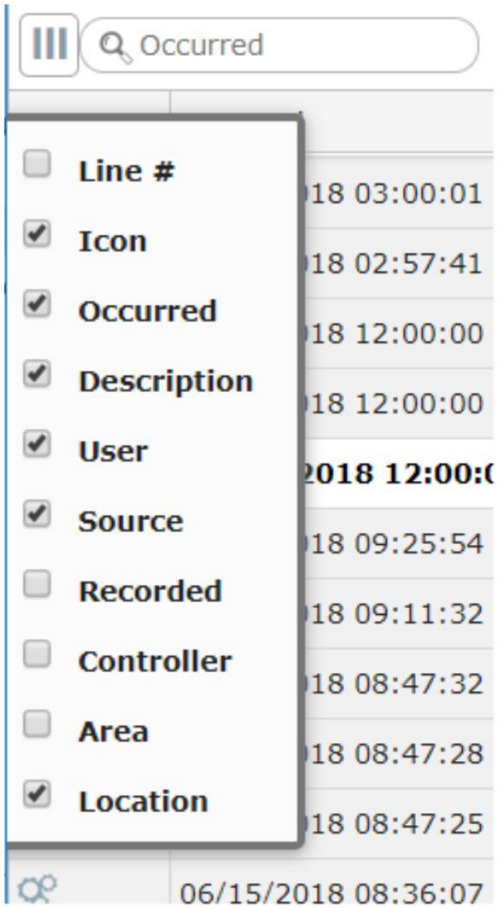
The default, gray text is the column that will be searched. Click the magnifying glass to change the column.



Column Selection

You can move the displayed columns by clicking and dragging on the column title.

Click the triple bar icon to select which columns to show.



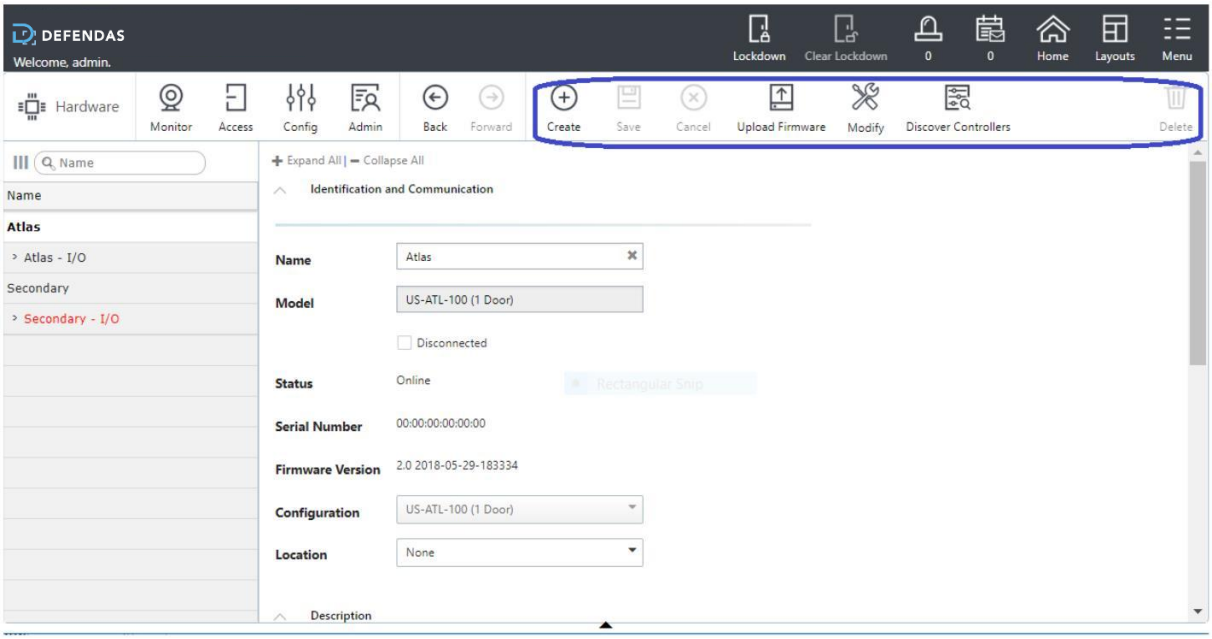
Paging

Lists run to extra pages when the number of items exceed your personal **Items per Page** set in Menu: Preferences.

This box appears at the bottom of the list when there are pages. You can go forward or back a page, go to the end or beginning, or enter a page number.

1.3 Using Property Views

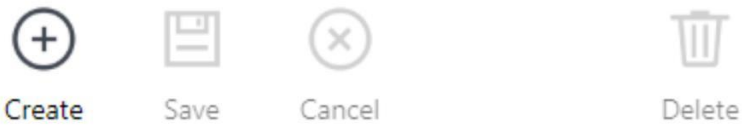
Most configuration is viewed or changed in Property Views. These screens display a list of items you have created on the left, with their properties on the right.



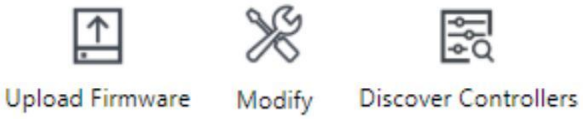
click to enlarge

The list can be searched using the same tools as in List Views.

Use the buttons above the properties to create new items, save changes, or delete items.



Many Property Views add additional action buttons to the menu bar. These are generally specific to the screen they are displayed on, and their functions are described in the documentation for the specific screens. These are shown in gray if they don't apply to the currently selected item.



1.4 Logging In and Passwords

To access the Web Management Application, open a web browser and enter the address of the Primary Controller provided by your Sentinel Series administrator. (In some browsers, you must type "https://" before the address.) You should bookmark this link.

Your browser might display an insecure site warning. The means to bypass this varies among browser applications, but should be shown on the error page as a link labeled "Advanced", "Details", "More Information", or something similar. You can prevent this warning for all Users by installing a signed HTTPS certificate.

Enter the username and password provided by your administrator. If you have lost the password for the "admin" user, see Password Reset.

Note: you cannot change your password unless you have access privileges to edit Users. Ask your administrator for password changes.

1.5 Product Registration and Licenses

Registration is required for full system functionality, including access to the **Access Control** and **Monitoring** menus. It is also required if you ever need to reset your system password. It also optionally allows LTS to contact you about software updates and other information.

Additional licenses let you increase the capacity of your Sentinel Series system. You can

- increase the number of Doors or Secondary Controllers allowed,
- increase the number of mobile device connections, and
- add to the languages the system supports.

(Note that "Out" Doors are not counted towards your maximum authorized doors.)

Contact your authorized LTS representative for license upgrades. Current license information can be viewed on the About screen.

How to Register

Follow these steps to register for the first time or to update your registration information.

1. Registration can be started in two ways:
    a. When you log in the first time, click **Register Now** in the Register Your Product pop-up window, or
    b. Select **Menu: About,** and click the **Register** button. (If you have previously registered, the link is **Update Registration.**)
2. Click the **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.*
4. Submit your registration automatically or by email.
    a. For automatic registration, click the **Submit Online** button. You will see a progress window followed by a success message.
    b. For email registration:
        i. Click the **Offline Registration** button. Read the instructions in the following window.
        ii. Click the **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 the **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.

How to Add Licenses

When you acquire an additional license, you will receive a license file from LTS. Save this file on your computer, then:

1. Select **Menu: About.**
2. Click the **Upload Additional Licenses** button.
3. Click on the **Browse** button, and **Open** the license file you received.
4. Click **OK.** Your new capabilities should be listed on the About screen.

Related Topics

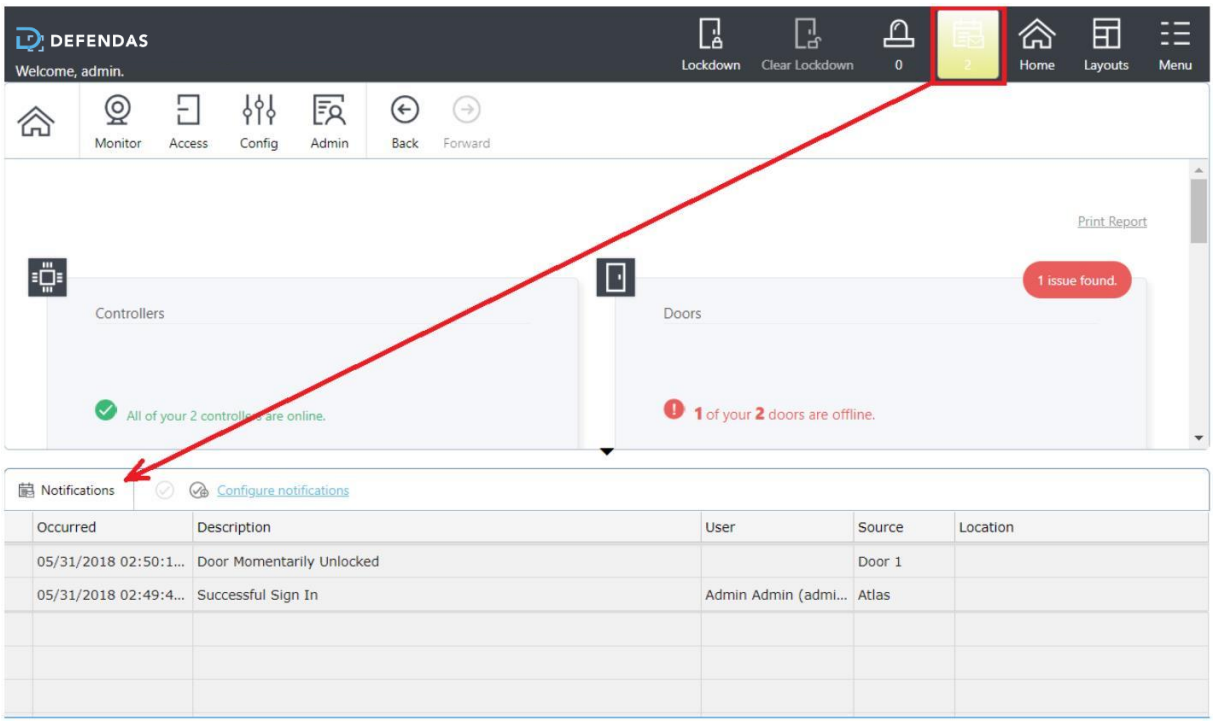
- Home Screen and Menus
- Password Reset

1.6 Notifications

Notifications allow each user to select certain Events they wish brought to their attention. When one of these Events occurs, it will appear in the Notification window of that User, and remain there until acknowledged.

Notifications can be copied to you by email.

Click the **Notifications** icon in the Menu Bar to open and close the Notifications Window at the bottom of the screen.



click to enlarge

Configuring Notifications

Configure Notifications to select the Events that generate Notifications for the current User. No Notifications are created unless you select them.

1. Click **Notifications** on the Menu Bar.
2. Click the **Configure notifications** link in the Notifications Window.
3. If desired, check **Send a Copy of Notifications by Email**.
   - You must have a valid email address configured in Users. You may need an administrator to set this, if you do not have permissions. There must also be an email server configured in Email Settings.
4. Check the Event categories and types you wish to receive Notifications for.
   - Select a category to receive Notifications for all Event Types in that category, or
   - Expand the category and select specific Event Types.
5. Click **Save**.

Clearing Notifications

To clear Notifications in the list, click one of the buttons next to **Configure notifications**.

— Select one or more Notifications and click this to clear them.

— Click to clear all Notifications.

Note that since Notifications are on a per-User basis, if one User clears a Notification, other Users' Notifications are unaffected.

Maximum Number of Notifications

To define the maximum number of Notifications per User:

1. Go to System Settings.
2. Enter the **Maximum Notifications per User**.
3. Click **Save**.

The oldest Notifications are deleted when the maximum number is reached.

Related Topics

- Users
- Events
- Email Settings
- System Settings

1.7 Emergency Features

Your Sentinel Series system is designed with a number of important features used to aid in a variety of emergency situations.

- Lockdown can be configured and used to secure facilities against an active intruder or threat.

- Emergency unlock can be configured and used to aid access by emergency personnel in the event of an active emergency condition signaled from another system.
- Duress PINs can be used to allow users to signal a duress condition during their otherwise normal access.
- Emergency Codes can be configured and used to allow access to emergency or security personnel using a PIN-code only, regardless of Door Mode (including lockdown), or Multi-User Access Rules.
- Muster can be used to aid in the tracking of users during an evacuation, or evacuation drill
- Alarms and Notifications can be configured and used to make sure the correct personnel are aware of potential emergency situations

Important: All emergency functions intended to be used in your system should be tested ahead of time, to ensure that everything is configured and working correctly.

Important: These emergency functions are designed as a supplement to, but not a replacement for, life-safety infrastructure for your facility. Life-safety functions are regulated by country- and region-specific fire codes. Please refer to these when designing and configuring your system to ensure compliance.

Monitoring

2 Monitoring

Monitoring gives you live views of what's occurring in the system, and printable reports of configuration and history.

Live Monitoring

Events is a live view of everything that happens in the system.

Alarms shows Events that you have determined should be immediately reviewed and action taken. Each Alarm must be acknowledged and cleared by someone who has resolved the problem. Note that Events do not become Alarms until you set up Alarm Triggers.

Door Status shows the real-time status of all Doors, including whether they are online/offline, locked/unlocked, open/closed, and any errors or alarms.

Controller Status shows the real-time status of all Controllers, including whether they are online/offline.

Sub-Controller Status shows the real-time status of Sub-Controllers, including whether they are online/offline.

Reader Status shows the real-time status of Readers, in particular OSDP Readers, including whether they are online/offline, and information on encryption, software version, and serial number.

Maps show similar status as Door Status, with visual indicators displayed on a Map of your facilities. The Maps must first be created in Maps (Configuration) .

Reports

Reports provides exportable/printable reports on Users, configuration, and history.

Related Topics

- Reports and Printing

2.1 Events

Events displays a real-time list of Events occurring within the system. Events that trigger Alarms are displayed in a configurable color.

To receive an email when important Events occur, see Notifications.

Up 1000 Events can be displayed. To view more Events, use Event History.

Menu Buttons

Filter Opens a panel where you can restrict the Events you wish to see in the list view. Your filters remain in place each time you log in.

Settings take effect when you click the **Search** button, at the bottom of the panel. The **Reset** button clears all filters.

User and Device Filters

The display shows only the Events that match *all* the filters you specify. Note that the **Name** filters are case-insensitive, and will find partial matches. For instance, if you enter "john", the display will also show Events for "John", or "Johnny".

Event Type Filter

The display shows Events that match *any* of the Event Types you have checked. If nothing is checked, all Events are displayed.

Clear Clear the current list of Events from the display, so only new Events appear. Events are hidden, but not deleted.

Events Columns

Some columns will be empty for certain types of Events.

Icon Category of Event

Occurred When the Event actually occurred (determined by the Controller on which it occurred)

Cameras	If a Camera is associated with the source of this event, then a link or links to view the recorded video are available here. Available only if video is licensed.
Description	Text of the Event
User	The User associated with the Event. This could also be a Shared Access Code, Emergency Code, or credential (card, PIN) that is not assigned to a single User.
Source	The device that recorded the Event. For door access Events, this is a Door. For other Events, this may be a Controller, input, output, or other device.
Recorded	(Hidden by default) The time the Event was received and recorded by the Primary Controller. This only differs from Occurred if the Secondary Controller where it occurred was offline with the Primary Controller at the time of the Event.
Controller	(Hidden by default) Controller where the Event occurred, or Controller managing the device where the Event occurred.
Area	(Hidden by default) If the Event is associated with an Area (for example a Door entering an Area), the Area is indicated here.
Location	(Hidden by default) If the source is associated with a Location, it is indicated here.

Event Archiving

The oldest Events are are automatically archived to CSV files on the Primary Controller when the maximum number is reached. To download the archived data, see Archive Downloads.

To change the maximum number of Events in the system, go to System Settings and set the **Maximum Events in Database**.

Related Topics

- Using List Views
- System Settings
- Event History
- Notifications

2.2 Alarms

Alarms are issues that may indicate a potential security threat or other problem. They cause a warning display on the Main Menu bar, and they remain in effect until they are resolved by a User.

Alarms are triggered by Events. Some Event Types are set to trigger Alarms by default. You can make more Events trigger Alarms, or change the defaults, in Alarm Triggers.

To receive an email when an Event causes an Alarm, see Notifications.

The color of an Alarm is determined by its state, which can be:

- New (Red) — this means the Alarm is active.
- Acknowledged (Yellow) — this means that some User has acknowledged the Alarm.

Resolved Alarms are removed from the list. They can be viewed in Alarm History.

Repeated Alarms are merged into a single Alarm. The **Count** column shows how many times it has occurred, and **Last Recorded** shows the most recent time it occurred. Alarms are merged when they are identical in all ways except for the date and time. Once resolved, any new occurrence will make a new Alarm.

Menu Buttons

Acknowledge	Acknowledges selected Alarms that are in the **New** state, changing the state to **Acknowledged**. Acknowledgment Indicates that the User is aware that the Alarm has occurred. Note that depending on the configuration of the corresponding Alarm Trigger, the Alarm may start off in the **Acknowledged** state instead of the **New** state.
Resolve	Resolves all Alarms that are in the **Acknowledged** state, changing the state to **Resolved**. Resolution Indicates that any underlying problem has been dealt with, or that the Alarm is of no consequence. The Alarm will be removed from this screen, but can be viewed in Alarm History. Alarms must be acknowledged before they can be resolved.

Alarms Columns

Description	Description of the triggering Event
Cameras	If a Camera is associated with the source of this alarm, then a link or links to view the recorded video are available here. Available only if video is licensed.
Source	The device that recorded the Event. For door access Events, this is a Door. For other Events, this may be a Controller, or other device.
Priority	The priority of this Alarm (as configured in Alarm Triggers)
Count	The number of times the triggering Event has occurred and merged into one Alarm
First Recorded	Time of the first triggering Event

Last Recorded	Time of the most recent duplicate triggering Event
State	"New" or "Acknowledged". The "Resolved" state is only visible in Alarm History. The state determines the color (see above).
Location	Location where the triggering Event occurred
Area	(hidden by default) Area where the triggering Event occurred

Related Topics

- Using List Views
- Alarm Triggers
- Alarm History
- Emergency Features

2.3 Door Status

Door Status displays a real-time list of all Doors and their status. You can also use Manual Commands to unlock a Door temporarily or change the Door Mode.

Menu Buttons

Manual Commands	Send a Manual Command to the selected Door, such as to temporarily unlock it or change its Door Mode.

Columns

Door	The name of the Door

Cameras	If a Camera is associated with this door, then a link or links to view the live video are available here. Available only if video is licensed.
Communications	**Online** or **Offline**
Door Mode	The Door Mode, such as **Card Only** or **Card and PIN**
Status	Whether the Door is **Locked** or **Unlocked**, and **Open** or **Closed**
Errors	Shows **Door Forced,** or **Door Held**, **Reader Offline**, and **Tamper** errors
Alarm	Indicates if an active Alarm exists for the Door
Type	The type of Door • **In** • **Out** • **Muster Point** • **Card Enrollment Point**
Location	The Door's Location

Related Topics

- Using List Views
- Manual Commands

2.4 Controller Status

Controller Status displays a real-time list of all Controllers and their status. This display does not include Sub-Controllers. You can perform certain maintenance tasks such as Resync, Reboot, and Software Updates.

Menu Buttons

Resync Resynchronizes the data on selected Controllers.

Reboot Reboots selected Controllers.

Resync All Resynchronizes the data on all Controllers. See Resync All.

Upload Software Update See Software Updates.

Update See Software Updates.Software

Status Columns

Name The name of the Controller

Status A summary of the status

Communications **Online** or **Offline**

Model	The model of the Controller
Software Version	The software version of the Controller
Serial Number	The serial number of the Controller
Location	The Controller's Location

Related Topics

- Using List Views
- Resync All
- Software Updates

2.5 Sub-Controller Status

Sub-Controller Status displays a real-time list of all Sub-Controllers and their status. This display does not include internal I/O Sub-Controllers. You can perform certain maintenance tasks such as Reboot.

Menu Buttons

Reboot	Reboots selected Sub-Controllers.

Status Columns

Name	The name of the Sub-Controller

Status	A summary of the status
Communications	**Online** or **Offline**
Model	The model of the Sub-Controller
Software Version	The software version of the Sub-Controller.
Serial Number	The serial number of the Sub-Controller
Location	The Sub-Controller's Location

Related Topics

- Using List Views

2.6 Reader Status

Reader Status displays a real-time list of all Readers and their status. It is primarily useful for OSDP Readers.

Menu Buttons

Configure	Opens the OSDP Reader Configuration Wizard. See OSDP Readers.

Columns

Name	The name of the Reader

Status	Status summary
Communications	**Online** or **Offline**, and encryption information
Address	The address of the Reader on the Sub-Controller (I/O)
OSDP/RS-485 Address	The "polling address" of the OSDP or LTS RS-485 reader.
Sub-Controller	The Sub-Controller (I/O) which this Reader is a part of.
Managed By	The Door that this Reader is managed by
Software Version	The Reader's software version, if known
Serial Number	The Reader's serial number, if known
Location	The Reader's Location

Related Topics

- OSDP Readers

2.7 Maps

The Maps view is used to show the status of your Doors and Controllers on graphical backgrounds, for example, on Maps of your building or campus. It highlights all problems in red, and allows sending commands to Doors. Maps may also have links to other Maps for easy navigation.

If Cameras are present on Maps, clicking on them shows the live video for that camera.

In this example there are four Doors and one Controller. One of the side doors is offline and should be checked on. Gray icons represent normal operation.

Click to enlarge.

Before they can be viewed, Maps must be created and configured in the Maps (Configuration) screen.

Menu Buttons

Manual Commands	Click on a Door to enable the Manual Commands button, allowing commands such as temporarily unlocking it, or changing its mode. See Manual Commands.
Zoom In / Zoom Out	Make the Map larger or smaller. When zoomed in, you can click and drag on the Map to see different areas.

Related Topics

- Using List Views
- Maps (Configuration)

- Manual Commands

2.8 Reports

Reports provides exportable/printable reports of Users, configuration and history.

There are several options which are common to many or all reports:

- **Orientation**: **Portrait**, or **Landscape**
- **Generate**: generates the report, viewable on the same screen
- **Export as PDF**: exports the report to PDF
- **Save as Custom Report**: saves the current settings to a Custom Report, available under **Custom Reports** (towards the bottom of the list of report types).

Reports

Audits shows configuration changes and actions performed by Users logged into the Web Management Application.

Muster is a special report that can show you where Users are in an emergency or an evacuation drill. To use the Muster report, you should first designate Muster Areas. Users must check in at the Muster Areas to indicate that they are safely out of the facility.

Users With Access Level shows which Users have a specific Access Level.

Users With Access to Door shows which Users have access to a specific Door. This report includes Doors directly assigned to the Users as well as those assigned via an Access Level.

Schedules is a report of Schedules and Door Mode Schedules.

Access Levels is a report of Access Levels.

Door Report is a report of Doors.

Users is a report of Users.

Event History is a report view of Events, with the ability to display a larger number Events and export to CSV and PDF.

Alarm History shows all Alarms, including those that have been resolved (resolved Alarms are not shown on the live Alarms screen).

Related Topics

- Reports and Printing

2.8.1 Audits

Audits lists configuration changes and actions performed by Users of the Web Management Application. Use these reports to see who unlocked a Door, gave access to a User, configured Access Levels, and other system operations.

When generating the report, you are prompted for the following options. Options vary based on the Audit Type selected. Click **Generate** to create the report.

Report Options

Orientation	Displays the report in "Portrait" or "Landscape" view
Audit Type	• **Database Change** — shows changes to items in the database (Users, Doors, Access Levels, etc.), and enables further filtering options. • **Manual Command** — shows Manual Commands executed on Doors, and enables further filtering options. • **Any/All** — both of the above
User	If selected, the report will only show actions taken by a specific User.
From / To	Limits the report to a date range
Change Type	For **Database Change,** which types of changes to include: • **Inserted** • **Updated** • **Deleted**

- **Any/All**

Object Type	For **Database Change,** which types of items to include (User, Door, etc.)
Manual Command	For **Manual Command,** limits the report to one command type.
Device	For **Manual Command,** limits the report to a single Door or Controller

Related Topics

- Reports and Printing
- Users
- Manual Commands

2.8.2 Muster

The **Muster** report shows the last known location of Users who are *not* registered in a safe Area. Use this report when evacuating a building or buildings or performing an evacuation drill. This lets security personnel know who is still inside the building(s).

Users counted as "safe" are

- Users who have exited to Global Out or reported at a Muster Point and
- Users who have not used any Door within 24 hours.

Muster reports may or may not include Users who have used a Shared Access Code or Emergency Code.

Creating a Muster Point

A Muster Point can be added at Controller creation time for 1-door Controller models.

1. Go to Hardware.
2. Select a 1-door model.
3. For **Configuration**, select an option which includes a Muster Point, such as **In Only + Muster Point**.

You can also modify Controllers after creation, to have Muster Points. For example:

1. Go to Hardware.
2. Select a Controller.
3. Turn the spare readers into Muster Points.

Generating a Muster Report

1. Go to **Muster**. A list of existing muster points is displayed at the bottom.
2. Select **List By** — **Last Name** or **Area**.
3. Select **Orientation** — **Landscape** or **Portrait**.
4. Click **Generate**.

Related Topics

- Reports and Printing
- Hardware
- Emergency Features

2.8.3 Users With Access Level

Users With Access Level creates a report of all Users who have a selected Access Level.

This report does not include Shared Access Codes or Emergency Codes.

Related Topics

- Reports and Printing

- Users
- Access Levels

2.8.4 Users With Access to Door

Users With Access to Door creates a report showing which Users have access to a specific Door. This report includes Doors directly assigned to the Users as well as those assigned via an Access Level.

This report does not include Shared Access Codes or Emergency Codes.

This report also excludes Users with no credentials (no cards, PIN, or biometrics).

Related Topics

- Reports and Printing
- Users
- Access Levels

2.8.5 Schedules

Schedules creates a report of all Schedules and Door Mode Schedules.

Related Topics

- Reports and Printing
- Schedules
- Door Mode Schedules

2.8.6 Access Levels

Access Levels creates a report of all Access Levels.

Related Topics

- Reports and Printing

- Access Levels

2.8.7 Doors

Doors creates a report of all Doors, or a selected Door.

Related Topics

- Reports and Printing
- Doors

2.8.8 Users

Users creates a report of all Users, or a selected User.

Related Topics

- Reports and Printing
- Users

2.8.9 Event History

Event History displays a list of Events according to a filter, and allows export to CSV and PDF. The maximum number of Events in this screen is limited only by the number of Events in the database. For a real-time view, see Events.

Menu Buttons

Export CSV	Export the displayed Events to a data file appropriate for importing into program like Excel. ("CSV" designates the "comma separated values" file format.)
Export PDF	Save the displayed Events as a printable report in PDF format.

Filter Pane

Settings take effect when you click the **Search** button, at the bottom of the panel. The **Reset** button clears all filters.

Date and Time Filter

Shows only Events from the specified time period.

User and Device Filters

The display shows only the Events that match *all* the filters you specify. Note that the **Name** filters are case-insensitive, and will find partial matches. For instance, if you enter "john", the display will also show Events for "John", or "Johnny".

Event Type Filter

The display shows Events that match *any* of the Event Types you have checked. If nothing is checked, all Events are displayed.

Events Columns

See Events.

Event Archiving

The oldest Events are automatically archived to CSV files on the Primary Controller when the maximum number is reached. To download the archived data, see Archive Downloads.

To define the maximum number of Events in the system, go to System Settings and set the **Maximum Events in Database**.

Related Topics

- Using List Views
- Reports and Printing
- System Settings
- Events

2.8.10 Alarm History

Alarm History displays all Alarms, including resolved ones. Resolved Alarms are hidden in the Alarms screen. This view does not update in real-time or allow you to acknowledge or resolve Alarms.

Menu Buttons

Filter Opens a panel where you can define the kind of Alarms you wish to see.

Settings take effect when you click the **Search** button, at the bottom of the panel. The **Reset** button clears all filters.

Date and Time Filter

Display Alarms from a range of dates and times.

User and Device Filters

The display shows only the Events that match *all* the filters you specify. Note that the **Name** filters are case-sensitive. For instance, if you enter "john," the display will not show Events for "John."

Event Type Filter

The display shows Alarms that match *any* of the Event Types you have checked. If nothing is checked, all Alarms are displayed.

Export PDF Save the displayed Alarms as a printable report in PDF format.

Alarms Columns

See Alarms.

Related Topics

- Using List Views
- Reports and Printing
- Alarms
- Alarm Triggers
- Emergency Features

Access Control

3 Access Control

The Access Control menu is primarily for determining who can open Doors, when, and how (cards, PINs, and biometrics).

You can also perform related tasks such as creating Users for the Web Management Application and creating Door Mode Schedules.

Access to Doors

Create Users to provide door access to individual Users who use a credential such as a card, a PIN, or a biometric fingerprint. This is the most common door access method and allows you to track who comes and goes. You can simply give each User unrestricted 24/7 access to Doors, or further restrict their access using the following features.

Set up Schedules to allow access only at certain times, such as during business hours.

Create Access Levels to predefine a set of Doors and Schedules that can be quickly assigned to multiple Users.

Specify Special Days to restrict access more than usual for holidays, corporate events, or other days when access rules should differ. Special Days are used in Schedules.

Create Shared Access Codes, which creates PIN codes that anyone can use to unlock designated Doors.

Special Features

The following features are used in special situations:

Emergency Codes are PIN codes that unlock Doors in an emergency.

Multi-User Access requires more than one User to present credentials to unlock sensitive areas. For example, a rule could be created such that three Users must present their card to open a Door.

Door Mode Schedules function like normal Schedules but are used in the Doors configuration to schedule Door Mode changes.

Access to the Web Management Application

Web Management Application Users are added in the same Users configuration screen. A User can have both Door access and web application access.

3.1 Users

Users can be created for the following purposes:

- Cardholders who can access Doors.
- Users who can log into the Web Management Application.

A single User can have both Door and application access.

Menu Buttons

Filter Displays a panel above the list where you can search for a User on several properties. Users are displayed if they match *all* filters.

Settings take effect when you click the **Search** button, at the bottom of the panel. The **Reset** button clears all filters.

Import See Importing Users from a CSV File.

Forgive Resets the selected User's anti-passback status. Use this when anti-passback rules are preventing a User's access, and this needs to be overridden.

Export All to CSV Exports all User (excluding the Admin User) to CSV file, in the same CSV format that is used for Importing Users from a CSV File.

Key Properties

For the complete list and more details see User Properties.

First Name and Last Name	The User's first and last name. Both required, maximum 32 characters each.
Photo	A photo of the User. This is shown here, and can be printed on a card. To add or change the photo, click the photo image and select an image from your computer. Supported image formats are PNG, JPEG, and GIF.
Role	**Cardholder Only** for cardholder. The other Roles provide access to the Web Management Application. Each Role provides a different level of access; see User Roles. Users with the ability to log in also can have Door access.
Username and Password	If **Role** is not **Cardholder Only**, this is the username/password used to log in to the web application.
Cards	Add any number of cards that will be used for access. You can use a Card Enrollment Point to add a card number. Adding a card does not provide access; the User will also need Access Levels or Doors assigned, below.
Fingerprints	Shows whether the User has any fingerprints enrolled, and allows them to be enrolled. (Fingerprints are only available if the Primary Controller supports biometrics.)
PIN	PIN (Personal Identification Number) for the User, numeric only. Click **Create New** to generate a random, unique PIN. The length must match the PIN length defined in System Settings. (The default is 4 characters).

Access Levels	•	Add Access Levels that have been defined, and/or
Door Access	•	Add **Door Access** entries to customize access for this User.

Card Design — Use to print cards.

Related Topics

- Using Property Views
- User Properties
- User Roles
- Duress
- Access Levels
- Anti-Passback
- Printing Cards

3.1.1 User Properties

The following are the properties available on the Users screen:

Identity

Status	Displays whether the current User's status is **Valid** or **Invalid**. The status will be **Invalid** if the current date is outside of the and **Valid To** range, or if **Disable User** is checked.
First Name and Last Name	The User's first and last name. Both required, maximum 32 characters each.

Photo	A photo of the User. This is shown here, and can be printed on a card. To add or change the photo, click the photo image and select an image from your computer. Supported image formats are PNG, JPEG, and GIF.
Personnel ID	A unique identifier, such as an employee ID. Maximum 32 characters.
Role	**Cardholder Only** for cardholder. For Users with the ability to log in, select another Role. See User Roles. Users with the ability to log in also can have cards.
User Group	Select a User Group which will be used when applying Multi-User Access rules. This is used if multiple Users are required to present their credentials to open a Door.
Language	The User's preferred language, which will be • displayed on card readers that support multiple languages (such as some OSDP readers), and • the User's default language in the Web Management Application. Available languages depend on your software license. Contact your authorized LTS representative for license upgrades.
Valid From	The date and time when access should begin. The default is the current date, at 00:00. This applies to both Door access and Web Management Application access.
Until Further Notice, Valid To	If **Until Further Notice** is checked, then the User's access never expires. If it is unchecked, then the **Valid To** date and time must be provided, which determines when the User's access expires. This applies to both Door access and Web Management Application access.

Note that the **Valid To** time takes effect at the end of the minute, not at the beginning.

Disable User	If checked, the User's access is disabled. This applies to both Door access and Web Management Application access.
Vacation From, Vacation To	If this date range is entered, it is a vacation date range during which the User's Door access is suspended. Web Management Application access is not affected by vacation dates.

Login

Username	If **Role** is not **Cardholder Only**, this is the username used to log in to the web application.
Password	If **Role** is not **Cardholder Only**, this is the password used to log in to the web application. The Password has the following minimum strength requirements: • At least 9 characters long • At least one uppercase letter • At least one lowercase letter • At least one number • At least one special character
Allow Mobile App Login	If checked, the User is may use the mobile app to log in to this system

Authorized Mobile Devices

A mobile device must be authorized for a specific User before it can connect to the Sentinel Series system.

To authorize a device for this User, create an authorization here. Then, after the User record is saved, click the **Share** button to view the QR code. Then then scan the QR code with the mobile application, or right click this image to save it for emailing to the User.

Each code can authorize only one mobile device. You may delete and add authorizations as needed to support several devices. The number of devices you can authorize is limited by your license. Contact your authorized LTS representative for license upgrades.

Additional Information

Email

The User's email address. This is required for the User to receive system emails such as Notifications.

Mobile Phone

The User's mobile phone number.

Custom 1-4

Custom fields corresponding to those configured in System Settings.

Access

Cards

Click **Add** to add card numbers for Door access. Click **Enabled** to enable or disable a card. To enter a card number by swiping the card, see Card Enrollment Points.

Each card has the following properties:

- **Type**:

- **Standard**: A standard card. This is the default type.
- **QR Code**: A QR Code credential to be used with the app. See QR Code Credentials.

- **Card Number**: the card number encoded within the credential, which uniquely identifies it.
- **Enabled**: if checked, the card is active. If unchecked, the card will be considered inactive, and denied access.
- **Share**: For QR Code credentials, once saved, this will contain a button to share the credential to the user's app.

Fingerprints

Shows whether the User has any fingerprints enrolled, and allows them to be enrolled.

Fingerprint enrollment requires a Defendas USB enrollment reader and its Fingerprint Driver software.

PIN

The PIN (Personal Identification Number) used for Door access. Numeric only. The length must match the PIN length defined in System Settings (default is 4 characters).

- PIN numbers must be unique, including **Duress PIN** codes, Shared Access Codes, and Emergency Access Codes.
- Click **Create New** to generate a random unique PIN number.
- Click **Clear** to clear the PIN.

Duress PIN

The duress PIN generates a duress access Event when used in place of the normal PIN. Access is still granted if all other normal access conditions are met. See Duress for more details. For **Duress PIN Type**:

- Select **None** if the Duress PIN is not used.
- Select **Add 1 to Last Digit** to add one to the last digit, only, of the normal PIN. For example, a normal PIN of 1111 would then have a

duress PIN of 1112, and a normal PIN of 9999 would have a duress PIN of 9990.

- Select **Explicit** to enter an specific Duress PIN for this User. Numeric only. The length must match the PIN length defined in System Settings (default is 4 characters).

Access Levels	Access Levels assigned to the User for Door access.
Door Access	Grants this User access to individual Doors during the selected Schedule. This is in addition to any **Access Levels** assigned.
Use Extended Door Times	If checked, extended unlock and held times are used when this User is granted access. This is for Users requiring additional time to get through a Door, for example a person with a disability. The amount of extra time is set on each Door. **Important:** Accessibility functions are regulated by country- and region-specific codes. Please refer to these when designing and configuring your system to ensure compliance
Anti-passback Exempt	If checked, the User is not subject to anti-passback rules.
Access Doors in No Access	If checked, the User can access Doors in No Access mode. This is typically only for administrators and security personnel.
Access Doors in Lockdown Mode	If checked, the User can access Doors in Lockdown mode. This is typically only for administrators and security personnel.

Allow First Credential Unlock	If checked (or if the identical checkbox is checked on this user's User Group), and the User access a door in a "First Unlocks" Door Mode, then the door will stay unlocked after the access. See First Credential Unlock for details.

Card Design

Card Design	Select a card design. If selected, a preview is displayed. Click Print Card to print. When printing, if the card number is a part of the design, the card number must be selected. Click **Print Receipt** if the card is printed to a remote location, and the recipient must go pick it up.

Related Topics

- User Roles
- User Groups
- Card Enrollment Points
- Access Levels
- Printing Cards

3.1.2 Printing Cards

You can print to a specialized printer that writes ID cards. You can also print a paper receipt for your use as a record or to authorize pickup at a remote printer.

To do either, you must first create Card Designs.

To print, select a User, and:

1. Select a card design. (Your choice will be saved for this User.)
2. Click **Print Card** or **Print Receipt.**
3. Select a card number from the list.
4. Click **Print** and follow the prompts.

To complete the prompts, see Reports and Printing.

Related Topics

- Users
- Card Designs
- Reports and Printing

3.1.3 Importing Users from a CSV File

A CSV (comma-separated value) file can be add any number of Users using data from another software program. The other program must be able to export to CSV or a format you can convert to CSV. The CSV itself must be modified to exactly match the Sentinel Series import format using software such as a spreadsheet editor.

On the Users screen:

1. Click **Import.**
2. Click the link to download a template file that includes a header row with the column names pre-populated.
3. Review the import format, below.

In your own software:

4. Open the file, imported as UTF-8, with comma as the separator.
5. Create a copy of the file.
6. Modify the file, adding data for the users you want to create.
7. Save the file in CSV format, comma-delimited.

a. Make sure the file is in plain text and does not include any additional characters or encoding.

b. For example, if using any non-ASCII characters, the file must be encoded as UTF-8.

On the Users screen:

8. Click **Import.**

9. In the dialog, click **Import**.

10. Select the file from your computer. The file must have the ".csv" extension.

11. Click **Yes** to verify and import the file.

12. The number of imported Users is displayed. Click **OK**, and you will see the newly imported Users.

Import Format

File encoding must be UTF-8 (if using any non-ASCII characters), and the delimiter is comma.

Lines beginning with # are treated as comments, and ignored.

The header row, if present, should match exactly the column headers in the exported template.

The column values are defined as follows:

Column/Header	Type	Notes
First Name	Text	Required
Last Name	Text	Required
Personnel ID	Text	
Valid From	Date	See the note on accepted date formats.
Valid To	Date	See the note on accepted date formats.
Language	Text	This is a language code. See the language codes table below.

Email	Text	
Mobile Phone	Text	
Custom 1	Text	
Custom 2	Text	
Custom 3	Text	
Custom 4	Text	
User Enabled	Boolean	See the note on boolean values. Defaults to 1 (true).
Use Extended Door Times	Boolean	See the note on boolean values. Defaults to 0 (false).
Anti-passback Exempt	Boolean	See the note on boolean values. Defaults to 0 (false).
Card Number (1)	Number	
Card Enabled (1)	Boolean	See the note on boolean values. Defaults to 1 (true), if Card Number (1) is present.
Card Number (2)	Number	
Card Enabled (2)	Boolean	See the note on boolean values. Defaults to 1 (true), if Card Number (2) is present.
Card Number (3)	Number	
Card Enabled (3)	Boolean	See the note on boolean values. Defaults to 1 (true), if Card Number (3) is present.
Card Number (4)	Number	
Card Enabled (4)	Boolean	See the note on boolean values. Defaults to 1 (true), if Card Number (4) is present.
Card Number (5)	Number	

Card Enabled (5)	Boolean	See the note on boolean values. Defaults to 1 (true), if Card Number (5) is present.
Access Level (1)	Text	If specified, must match the name of an existing Access Level in the system
Access Level (2)	Text	If specified, must match the name of an existing Access Level in the system
Access Level (3)	Text	If specified, must match the name of an existing Access Level in the system
Access Level (4)	Text	If specified, must match the name of an existing Access Level in the system
Access Level (5)	Text	If specified, must match the name of an existing Access Level in the system
PIN	Number	May contain leading zeros

Dates should be in format YYYY-MM-DD or in the default format for the logged-in language (the language column in the CSV itself does not affect this):

- MM/DD/YYYY for English.
- DD/MM/YYYY for English (UK)/Spanish/French/Portuguese/Italian/Thai/Greek.
- DD.MM.YYYY for German/Turkish/Czech/Russian/Polish/Finnish/Norwegian.
- DD-MM-YYYY for Danish/Dutch.
- YYYY/MM/DD as well as the standard Chinese format with Chinese characters for Chinese.

Boolean fields use 0 for false; 1 for true.

Language codes:

Code	Language
en	English
en-GB	English (UK)
es	Spanish
es-ES	Spanish (Spain)
de	German
cs	Czech
da	Danish
el	Greek
fi	Finnish
fr	French
it	Italian
nl	Dutch
no	Norwegian
pl	Polish
pt	Portuguese
ru	Russian
sv	Swedish
zh	Chinese
zh-TW	Chinese (Traditional)
th	Thai
tr	Turkish
ro	Romanian

ja	Japanese
ko	Korean

Related Topics

- Users
- User Properties

3.2 Shared Access Codes

A Shared Access Code is a PIN that multiple people can use to access specified Doors.

These codes only work when the current Door Mode allows a PIN by itself to open the Door. For example, PIN-Only or any mode that says "or PIN", such as "Card or PIN".

Shared Access Codes do not work with:

- Doors that are in Card-only mode, Card and PIN, etc.
- Doors with Multi-User Access rules (because a user group cannot be assigned to a shared access code).

Shared Access Codes are always exempt from anti-passback.

Use of Shared Access Codes will impact the accuracy of a Muster report.

Shared Access Code Properties

Name	Required. Maximum 32 characters.
PIN	The Shared Access Code itself. Numeric only. Click **Create New** to generate a random, unique code.
Enabled	Checked to enable, unchecked to disable

Valid From	The date and time when access should begin. The default is the current date, at 00:00.
Until Further Notice, Valid To	If **Until Further Notice** is checked, then access never expires for this Shared Access Code. If it is unchecked, then the **Valid To** date and time must be provided, which determines when access expires for the Shared Access Code. Note that the **Valid To** time takes effect at the end of the minute, not at the beginning.
Usage Limit	If a **Usage Limit** is specified, then the Shared Access Code may only be used that number of times. Only Access Granted transactions count as a "use".
Usage Count	If a **Usage Limit** is specified, then the **Usage Count** shows how many times the credential has been used so far. The **Reset Usage** button resets the usage count back to 0.
Description	Description or comments
Access Rights	• Add Access Levels, and/or • add Door Access entries to directly assign Door/Schedule pairs for access.

Related Topics

- Using Property Views
- Emergency Codes
- Access Levels

3.3 Emergency Codes

An Emergency Code is a PIN that allows access to Doors regardless of other settings, including the Door Mode. (Compare to Shared Access Codes). It is intended to be used by emergency and security personnel to gain access in emergency situations.

This means that an Emergency Code can access a Door which is under Lockdown.

The successful use of an Emergency Code generates an Emergency Code Presented Event.

The Emergency Code Presented Event is configured as an Alarm Trigger by default, generating an Alarm. The Emergency Code Presented Event can also be used as a Linkage to trigger the activation of an auxiliary output on the Hardware screen.

Emergency Codes are exempt from anti-passback and Multi-User Access. (Compare to Shared Access Codes.)

Emergency Codes otherwise have the same properties as Shared Access Codes.

Use of Emergency Codes will impact the accuracy of a Muster report for the emergency personnel who use them.

Related Topics

- Using Property Views
- Shared Access Codes
- Access Levels
- Emergency Features

3.4 Access Levels

An Access Level is a list of Doors, each paired with a Schedule, during which access is to be allowed.

Access Levels can be applied to Users, Shared Access Codes, and Emergency Codes.

Using the Screen

*On the left-hand side (**Select one or more items**):*

- Select the **Default Schedule to Use** when adding Doors to **Selected items**.
- Page through Doors using the arrows, and/or search by name.
- Select Doors to add them to **Selected items**.

*On the right-hand side (**Selected items**):*

- Change the **Schedule** for individual Doors using the drop-down.
- Select a Door to remove it from **Selected items**.
- Use **Change all assigned schedules** to change the schedule associated with all Doors in **Selected items**.

Related Topics

- Using Property Views
- Schedules
- Users
- Shared Access Codes
- Emergency Codes

3.5 Schedules

Schedules are used to limit access to certain days and times. They can be used in Access Levels and anywhere Door access is assigned.

By default, access is *not* allowed on Special Days.

The built-in "24/7" Schedule allows access at all times, *including* Special Days.

Using the Screen

Access will be allowed during all the time periods you create. Click the **Add** and **Remove** buttons to add and remove time periods from the list.

Times (Start-Stop)	The left-side bar shows the time period access is allowed in green. You can drag the ends of the green bar to change the time range. You can also enter the exact times you want in the boxes under the bar. Times are entered and shown using a 24-hour clock (as opposed to "a.m". and "p.m.") Each bar can only have one time range; to have two time ranges on the same days, add another entry. The **All day** button is a convenience to reset the bar.
Days	The middle bar shows the days that access is allowed in green. You can click each day to change access, or you can use the convenience buttons to change the current selection. The convenience buttons are **Weekdays**, **All days**, and **Weekend**.
Special Days	The right bar appears green if you have included any Special Days for that time period. Click the bar to select Special Days to include. In the Special Days selection screen, you may check one or multiple Special Day types. Access is normally denied on Special Days. Access will be allowed if you include the Special Days in the Schedule. For more information, see Special Days.

Related Topics

- Using Property Views
- Special Days

3.6 Door Mode Schedules

Door Mode Schedules are used to change the mode of Doors at different times. For instance, they are commonly used to automatically unlock general-access Doors during business hours.

See Door Modes for a list of possible Door Modes.

Door Mode Schedules are assigned to Doors on the Doors screen.

A Door Mode Schedule can have multiple time intervals with different associated modes.

Note that emergency Door Modes cannot be scheduled.

Using the Screen

Click the **Add** and **Remove** buttons to add and remove time periods from the list.

In the left column, select a single Door Mode. A Door will automatically change to this mode during the time period defined.

The time periods are defined the same way they are for Schedules. See Schedules.

Related Topics

- Using Property Views
- Door Modes
- Special Days
- Schedules

3.7 Special Days

Special Days are single calendar days (such as May 5th) which are excluded from Schedules by default. A Special Day is only included in a Schedule if the corresponding Special Day Type is selected within the Schedule.

For a Schedule used for access, Users would be denied access by default on that day, even if access would otherwise be allowed based on the time of day, and day of week. If the Special Day Type is selected for that Schedule, those same Users would then have access on those days.

The same idea applies to Door Mode Schedules. For any given interval, the selected Door Mode applies for the time of day and day of week, except for on Special Days - unless the corresponding Special Day Type(s) are selected.

Special Days are used for holidays, corporate events, and other cases where you do not want your usual access to be granted, or usual scheduled door modes to apply. For instance, you might use Access Mode Schedules to automatically unlock Doors during business hours Monday-Friday, but you do not want to do that on holidays.

Special Day Types

Special Days are grouped into a number of Special Day Types. A type is essentially a calendar. For instance, one type might include all government holidays, while another might be teacher work days. You can then set different access rules for the different calendars.

Only Special Day Types can be added to a Schedule. So, you could add access on all government holidays, but not on a single one, unless you made a type with just that one day.

Using the Screen

In the first section, **Special Day Types**, you can change the names of the types to something useful, such as "Government Holidays" or "Teacher Workdays". You may also change the color assigned to each type. The color has no effect except on this screen.

The second section, **Special Days**, shows a calendar highlighting all Special Days of all types in their color. To add or remove a day, click on it.

The two options above the calendar change what happens when you next click on a day. They cannot change the properties of current Special Days.

- **Select Special Day Type:** days added on the calendar will be this type. You cannot add days if no type is selected.
- **Set as Repeating:** when checked, days added on the calendar will be repeating. This means they will occur every year on the same calendar date. They are displayed with a small "R", and can be seen on every year.

Note that any single day can only be in one Special Day Type.

Related Topics

- Schedules

- Door Mode Schedules

3.8 Multi-User Access

Multi-User Access is used to require multiple Users to present their credentials to open a Door. This is often used for high security areas. For example, an area might require two managers and one security guard to present their credentials. The credentials they may submit are those required by the Door's current Door Mode.

Shared Access Codes cannot access Doors with Multi-User Access rules in effect. Emergency Codes are exempt from Multi-User Access rules.

Using the Screen

You must first create one or more User Groups whose members can cooperate to access a specific Door.

Click the **Add** and **Remove** buttons to add and remove **User Groups** from the **Rules** list. If multiple rules are created, they all must be satisfied in order for access to be granted. If there are no **rules** in a specific Multi-User Access definition, associated Doors will behave as if they have no Multi-User Access restriction.

Apply the Multi-User Access rule on the Doors screen.

Related Topics

- Using Property Views
- User Groups
- Doors

Configuration

4 Configuration

Use the Configuration menu to:

- Connect and configure hardware and Doors.
- Organize your hardware into locations and Areas, and plot it on Maps.
- Configure general settings for the Monitor and Access Control features.

Users with the System Administration Role can add and configure Controllers and Doors. Access Control Management Users can only configure Doors. Other built-in User Roles can do neither.

See Administration for configuring system settings such as the time or network connection.

Configuring Hardware and Doors

Before doing any configuration, it's important to read the brief topic, Understanding Controllers and Doors. It is particularly useful for any Web Management Application User to understand the definition of "Door" in the Sentinel Series software.

Hardware is where the physical equipment (Controllers and their readers, inputs, and outputs) is added and configured. Hardware configuration is usually done by an expert who installs the system.

Door configuration is the starting point for all access control. Most importantly, this is where you specify if and when Doors are locked and how they can be opened. All Access Control settings are affected by Door configuration.

Hardware Templates and Door Templates can be used to quickly set up multiple Sub-controllers (I/O) or Doors with the same settings.

Organizing Hardware

Locations are labels that can be applied to Doors, Controllers, Maps, and other items. Locations appear in Events and Alarms.

Areas are used with anti-passback and airlock. They define physical regions where you can restrict access using those features. The Muster Report also relies on Areas to determine whether each User is at a known, safe Area (Muster or Global Out).

You can also create Maps of your buildings and campus. Monitor these Maps to watch the live status of Doors and Controllers on an actual map of your facility.

General Settings

Card Designs allows you to create the print layouts for Printing Cards.

Card Formats define the low-level details of how data is stored on the cards you use. Your Sentinel Series system includes all of the card formats you will likely need. Use this screen to create a format for another type of card, or to enter a "facility code" as instructed by your card vendor.

Create User Groups to use with Multi-User Access.

Set up Alarm Triggers to define which Events trigger Alarms.

4.1 Understanding Controllers and Doors

Controllers

Each system includes one Primary Controller. This is the one you log in to with your web browser to manage or monitor the entire system. It maintains all the data and configuration, and directs all Secondary Controllers.

Secondary Controllers are added to manage additional Doors. They receive their configuration from the Primary Controller. However, they keep a copy of the data, so they continue operate if the primary is not online. You can log in directly to a Secondary Controller through a link on its Hardware page, but only to change a few local values, such as the Network settings.

Important: The Primary Controller must support biometrics if any biometric Controller will be used in the system.

Sub-controllers (I/O)

Every Controller has a built-in Sub-controller (I/O). It is displayed under the Controller in Hardware with the additional label, "I/O", meaning "input/output". The Sub-controller manages the advanced details of the readers, inputs, and outputs of the hardware.

Additionally, separate physical Sub-controllers can be connected using RS-485/OSDP, to add additonal I/O. The following Sub-controller models are supported:

- LTS STEB-0808 I/O Expansion Board

Doors

Every card, PIN, and biometric reader in the system is represented as a Door — although this doesn't always correspond with what we think of as a door. A Door in the Web Management Application might represent one of many things:

- A real, physical door that can be entered
- A second reader that allows exit through a physical door. Notice that this means an In/Out physical door is represented by two Doors, one for "In", and one for "Out".
- Something that functions like a physical door, such as a turnstile or garage gate
- A reader by itself, with no physical door, used as a Muster Point or Card Enrollment Point

Doors are created on the Hardware screen, either automatically when the Controller is created, or by customizing the Controller.

Related Topics

- Hardware
- Doors

4.2 Hardware

Hardware represents the system's Controllers and all their physical connections to readers, locks, door sensors, and other inputs and outputs. This is where you configure electrical connections and Controller settings. Door behavior, such as Door Mode or opening times, are configured in Doors.

Hardware Topics

- Models and Configurations
- Modifying Controller Configuration
- LTS STEB-0808 I/O Expansion Board
- Hardware Properties
- Adding Controllers
- Software Updates
- Resync All

Related Topics

- Doors
- Hardware Templates

4.2.1 Models and Configurations

Sentinel Series Models

Model	Type	Wiegand Ports	RS-485 Slots	Number of “In” Doors	Max "Secondary" Doors	Default Reader Type	Default Type for Secondary Readers
ST200-B	2-Door	4	4 OSDP	2	2	Wiegand	Wiegand
ST400-B	4-Door	4	4 OSDP	4	4	Wiegand	OSDP

Important: The Primary Controller must support biometrics if any biometric Controller will be used in the system.

"In" Doors are automatically created and are permanent, though they need not be used.

Secondary Doors are Out Doors, Card Enrollment Points, and Muster Points. The Readers of Secondary Doors are always paired with the Readers of In Doors in a defined way.

Controller Type	"In" to "Secondary" Reader Pairings

2-door	1 to 3 2 to 4
4-door	1 to 5 2 to 6 3 to 7 4 to 8

For example, on a 4-door Controller, Door 2 always uses reader #2 and is an "In" Door. If it has an "Out" Door, that Door will always use reader #6.

The reader number is not necessarily the same as its address. For Wiegand, the reader number *is* the same as the labels on the hardware, but any reader can be changed to use any available RS-485 address.

Notice that 4-door Controllers only have enough Wiegand reader ports for the "In" Doors. Any secondary Doors must use RS-485.

Configuration Property

The Configuration property of a Controller determines what the Controller's Doors will be used for: authorizing Door entry, perhaps Door exit, or as special purpose readers.

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 biometric readers connected to the Controller.

In Only This 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).

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. See Card Enrollment Points.

The available options do not cover all possibilities. For instance, 2- and 4-Door Controllers do not offer Muster Points or Enrollment Points as standard Configurations. To tailor the configuration to your needs, see Modifying Controller Configuration. Modifying might be easier if you start with "In Only" as a baseline.

Related Topics

- Adding Controllers
- Modifying Controller Configuration

4.2.2 Modifying Controller Configuration

The "Modify" button on the menu bar is used to customize the Configuration property of a Controller, as well as add additional Sub-controllers. You will need to understand Models and Configuration to effectively customize a configuration.

Clicking "Modify" brings up a list of options. Some options will be disabled when they cannot be applied to the Controller as its readers are currently configured.

All options present a dialog to enter specifics for your change. The options are:

Change to In/Out	Select the number of the "In" **Door** which will have an "Out" Door paired with it.
Add Muster Point	Enter a **Name** for the new Door, and select the "In" **Door** number to pair it with.

Add Card Enrollment Point	Enter a **Name** for the new Door, and select the "In" **Door** number to pair it with.
Remove Secondary, Muster, or Card Enrollment Point	Select the number of the "In" **Door** that will have its paired Door removed.
Add Door (Monitor Open Only)	Reconfigure an available Input on a STEB-0808 to be a Monitor Open Only Door.
Remove Door (Monitor Open Only)	Remove a Monitor Open Only Door from a STEB-0808, making the Input available as a general Input.
Add STEB-0808	Add a STEB-0808 I/O Sub-controller.

Related Topics

- Models and Configuration

4.2.3 STEB-0808

The STEB-0808 I/O Expansion Board is connected to a Primary or Secondary Controller via RS-485/OSDP, and adds 8 Inputs and 8 Outputs.

Important note: the RS-485 port can only either be used for OSDP, or Defendas fingerprint readers. If fingerprint readers are in use, OSDP devices such as this one will not be able to be added.

The baud rate for the RS-485/OSDP connection is 9600.

The 8 inputs are supervised, with 1K/2K supervision.

The inputs and outputs can be used for linkages, very similarly to built-in I/O Sub-controllers.

The STEB-0808 does not support Wiegand or OSDP readers, but it can be used for Monitor Open Only Doors. A Monitor Open Only Door is a door with only a Door Sensor. When such a Door is being monitored, events and status are reported very similarly to Forced Open monitoring on a standard Door.

This monitoring can be masked or unmasked, both manually or according to a schedule. These doors also monitor for the Held Open condition, which can be similarly masked.

This type of Door is useful in situations where certain doors are not supposed to be opened at certain times, but, full electronic access control with a reader is not installed on them.

Adding a STEB-0808 I/O Expansion Board

1. Navigate to Hardware and select the Primary or Secondary Controller.
2. Press the **Modify** button and choose **Add STEB-0808**
3. Enter a **Name** of your choosing.
4. For **Serial Port**, select **COM1**.
5. For **OSDP Address**, select the OSDP address that corresponds to the DIP switches on the device. This address is from 0-15, and corresponds to DIP switches **AD1**, **AD2**, **AD3**, **AD4**.
6. Press **Add**
7. When the Sub-controller comes online, its status will be shown as Online here, as well as in Sub-Controller Status

Adding an Monitor Open Only Door

1. Navigate to Hardware and select the STEB-0808.
2. Press the **Modify** button and select **Add Door (Monitor Open Only)**

3. Enter a **Name** of your choosing.
4. Select the **Input** which is to be used to monitor the Door
5. Press the **Add** button.
6. The status of the Door can be monitored in Door Status

Monitoring STEB-0808 Status

STEB-0808 I/O Expansion Boards are Sub-Controllers, and therefore can be monitored in Sub-Controller Status.

Related Topics

- Hardware
- Door Status
- Sub-Controller Status
- Manual Commands

4.2.4 Hardware Properties

The body of the Hardware screen allows Controller configuration and displays data about the Controller. Each Controller is represented by two components: (1) the Controller itself for general configuration, and (2) a Sub-controller (I/O) for detailed settings of readers, locks, door sensors, and other inputs and outputs.

Sub-controllers can be configured to a saved group of settings using Hardware Templates.

Door behaviors, such as Door Modes and opening times, are configured in Doors.

Controller Properties

Name	The name of the Controller. Required, maximum 32 characters.
Model	The model of the Controller.

Host Address	(Secondary Controllers only) IP address or hostname of the Controller.
Port	(Secondary Controllers only) Port number for the Controller.
Disconnected	If checked, the Secondary Controller is treated as if it does not exist, and communication is not allowed. This cannot be checked on the Primary Controller. This can be useful during the installation or maintenance of hardware.
Status	Displays the current status of the device, including Online/Offline. If any tamper, power, or battery problems are present, these will be indicated here as well. Lockdown or Emergency Unlock will be indicated here, when active.
Serial Number	The serial number of the Controller. This is displayed only if the device is online.
Software Version	The software version of the Controller. This is displayed only if the device is online.
Configuration	See Models and Configuration.
Location	The Location of the Controller.
Description	Description or comments
Language	Sets the default language for • the Web Management Application on the Primary Controller,

- the simplified management application on a Secondary Controller, and
- multi-language OSDP readers connected to this Controller, if they have displays.

Available languages depend on your software license. Contact your authorized LTS representative for license upgrades.

Time Zone	(Secondary Controllers only) The time zone of the Secondary Controller. The time zone for the Primary Controller is set in Date and Time.
Managed Doors	A list of the Doors managed by the Controller, with links to their configuration screens.
Managed Sub-controllers	A list of Sub-controllers managed by this Controller, with links to their hardware configuration.
Software Update	(Secondary Controllers only) Select a previously uploaded software update file and download it to the Controller. Primary Controller software is updated under Software Settings.
Open Web Page	Click the link to log in directly to a Secondary Controller. You will enter a simplified web management application allowing limited Controller configuration options, such as Network settings.
Reboot Button	(Secondary Controllers only) Reboots the Controller
Resync Button	(Secondary Controllers only) Refreshes the configuration of this Secondary Controller.

Sub-controller (I/O) Properties

Name	(Read-only) The name of the Sub-controller.
Disconnected	(Read-only) Always unchecked and cannot be changed.
Status	(Read-only) Always Online for Sentinel Series built-in Sub-controllers.
Model	(Read-only) The device model.
Description	Description or comments
Hardware Template	Select an existing template and click **Apply Template**. Deselect **Apply Template** to edit the settings. Click **Create Hardware Template** to create a new template from the current settings. The template contains most of the Sub-controller configuration. See Hardware Templates.

Reader Properties

Address	If Wiegand, the address label printed on the Controller. Otherwise, **Address** is the address label which this reader replaces, or a virtual address which is above those printed on the board.
Managed By	The Door that the device is associated with
Model	The device model: • **Custom** — for Wiegand or OSDP readers • **LTS** — for RS-485 readers
Reader Type	• **Data0/Data1 (Wiegand)**

- **OSDP** — for model **Custom**
- **RS-485** — for model **LTS**. This is only available on biometric Controller models.

Keypad Type

For **Data0/Data1 (Wiegand)** readers only.

- If Auto, then PIN digits are accepted over Wiegand, automatically decoding the format.
- “None” is displayed for no PIN pad. (It generally makes sense to leave this on Auto, unless you want to specifically disable a PIN pad on a Wiegand reader.)
- OSDP and RS-485 readers send their PIN data differently, so this setting is not used for them.

Tamper

The type of tamper detection. Only **OSDP** is supported on OSDP readers.

LED Type

The LED control type:

- For Wiegand, this is either:
  - **None** — select this to disable LED control completely
  - **1-Wire (Green)** — one wire wired to the green LED (red LED generally lit when green is not)
  - **2-Wire (Red and Green)** — Biometric Controllers only
- For OSDP readers, this is **OSDP**.

OSDP/RS-485 Address

The "polling address" of the OSDP or LTS RS-485 reader.

For most OSDP readers the default is 0. See **Configure,** below, and installation instructions from the reader manufacturer, for how to change the address.

RS-485 readers have a DIP switch to configure the address. Please refer to the RS-485 reader installation instructions on how to set the address.

Configure

Configure opens the OSDP Reader Configuration Wizard, which can be used to:

- Change the OSDP address that the reader itself is configured to use. This is *not* the **OSDP/RS-485 Address** the Sub-controller is set to use, though they must ultimately have the same value.
- Manage the encryption key used to communicate with the reader.

See OSDP Readers for more details.

Input Properties

Address

The printed address on the board.

Name

The name of the input. Required, maximum 32 characters.

Enabled

Check to enable, uncheck to disable.

Normally Open

Whether the input is normally open (NO). Normally open inputs are active when the wires are normally not connected (open circuit). This is generally true for exit buttons. Most other inputs like tamper, power, and battery failure sensors are normally closed (NC).

Function

What the input is used for. Not all options are available for all inputs, and some cannot be changed. The **Functions** are:

- **Exit Button**
- **Door Sensor**

- **Tamper**
- **Power Monitor**
- **Battery Monitor**
- **Linkage**
- **Not Used**

Managed By

For exit buttons and door sensors, this is the Door that the input is a part of. For tamper, power monitor, and battery monitors, this is the Controller they are a part of. For Linkage inputs, this is the device affected by the linkage. (See **Linkage Type.)**

"Out" Doors cannot be used in linkages, nor to manage hardware.

Linkage Type

For **Linkage** inputs, this is an action to be performed when the input becomes active. The options depend on the **Managed By** setting

- **Input-Triggered Alarm** (Managed By: empty) — This will cause an Alarm to be generated when the input becomes active. Do not confuse this with a relay activating an audible alarm, which can be configured for an output, below.
- **Input-Triggered Lockdown** (Managed By: a Controller) — When the input is activated, a Global Lockdown is initiated. The lockdown will only end when a User clicks **Clear Lockdown** on the Main Menu (with some exceptions*).
- **Input-Driven Emergency Unlock** (Managed By: a Controller) — Whenever the input is active, a Global Emergency Unlock condition will be active. The emergency unlock will only end when the input returns to inactive (with some exceptions*).
- **Input-Triggered Momentary Unlock** (Managed By: a Door) — This will cause a momentary unlock of the Door when the input becomes active.

***Important:** As with all emergency functions, you should thoroughly understand the relevant topics before relying on lockdown and emergency unlock.

Schedule — (Linkage only) If a Schedule is selected here, the **Linkage** will only be applied during this Schedule.

Output Properties

Address — The printed address on the board.

Name — The name of the output. Required, maximum 32 characters.

Function — What the output is used for: Not all options are available for all outputs, and not all can be changed. The options are:

- **Reader Beeper**
- **Reader LED (Green)**
- **Reader LED (Red)**
- **Lock**
- **Linkage**
- **Not Used**

Managed By — For **Lock, Reader Beeper,** and LEDs this is the Door they are used for.

For **Linkage,** this is the device whose Events can trigger this output.

"Out" Doors cannot be used in linkages, nor to manage hardware.

Event / Condition — (**Linkage** only) Defines the Event or condition that triggers an output.

Controller triggers:

- **Tamper**

Door triggers:

- **Access Denied**
- **Access Granted**
- **Door Forced Open**
- **Door Held Open**
- **Duress**
- **Emergency Code Presented**

Input triggers:

- **Input Active**

Triggers when **Managed By** is blank:

- **Schedule Active**

Toggle / Pulse	(**Linkage** only) If **Pulse,** the Event activates this output briefly. If **Toggle,** this output is active until the Event is "ended" by its reverse Event. For example, "Door Held Open" is reversed by "Door Held Open Restored". **Toggle** is not an option when the Event has no reverse Event.
Pulse Time	(**Linkage** only) The pulse time in seconds.
Schedule	(**Linkage** only) If a Schedule is selected here, the **Linkage** will only be applied during this Schedule.

Related Topics

- Using Property Views
- Understanding Controllers and Doors

- Hardware Templates
- Models and Configuration
- Locations
- Doors

4.2.5 Adding Controllers

Secondary Controllers can be automatically found and added by the Web Management Application. This is called “Discovery.” When Discovery cannot be used, you can add Controllers manually. You can also use manual installation to add Controllers that have not yet been installed.

Once a Secondary Controller has been added, it cannot be reassigned to a new Primary Controller, or a factory reset Primary Controller, until the Secondary Controller itself has had a Factory Reset.

You can replace a Secondary Controller with a new Controller and transfer all of its configuration including its Doors.

The number of Secondary Controllers you can add and the number of Doors you can create are limited by your license. Contact your authorized LTS representative for license upgrades.

Discovering Secondary Controllers

There are two important qualifications about Discovery.

- When using Discovery, you should connect and discover Controllers one at a time. This is the best way to be able to tell which one is which.
- 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.

To Discover Controllers:

1. Click **Discover Controllers** on the menu bar.

2. In a few moments, a window will display all Controllers discovered.
3. Click the link to add a Controller. The create controller screen will appear.
   a. Select a Configuration.
   b. Enter a **Name,** and select **Custom Door Names** so you can name the doors in the box, below.
   c. Leave all other settings as they are. These are the settings that were discovered.
4. Click **Save** on the menu bar.

Manually Adding Secondary Controllers

To add a Controller manually:

1. Click **Create** on the menu bar. The create controller screen will appear.
2. Select a Model.
3. Select a Configuration.
4. Enter a **Name,** and select **Custom Door Names** so you can name the doors in the box, below.
5. Enter the Controller's **Host Address**.
6. Leave the **Port** number at the default, 443.
7. Click **Save** on the menu bar.

Replacing a Secondary Controller

If you need to replace a hardware panel that is functioning as a Secondary Controller, you can transfer all of its configuration to the new Controller. The Controller's Doors will be retained, along with the Access Levels, Maps, previous Events, emergency features, and any other configuration the Controller is involved in.

The new Controller must be the same model as the original Controller.

To replace a Secondary Controller:

1. Physically disconnect or turn off the original Secondary. Replacement will not work while it is active. *Do not disconnect or delete it on the Hardware screen.*
2. If the new Controller has been used before, perform a Factory Reset on that Controller.
3. Completely install the new Controller according to the instructions that came with it. Do complete the Setup Wizard for a Secondary as usual (see the note, below). ***Do not*** discover or manually add the Controller as described on this page.
4. Select the original Secondary on the Hardware screen.
5. Click the **Replace** button at the bottom of the properties, and confirm in the next window. You should see a message indicating that Replace has started.
6. If necessary, change the **Host Address** and click **Save.**

The Status of the Secondary should change to "Online" shortly.

Note about the Setup Wizard: If the original Secondary used a static IP address, use the same one and skip step 6, above. If the original was set to DHCP use that again, but you must later determine the new Controller's IP address and complete step 6. One way to find the address is to click **Discover Controllers** and look for the unconnected Controller. Then click **OK** to exit Discovery without adding it.

Related Topics

- Models and Configuration
- Modifying Controller Configuration

4.2.6 Software Updates

"Software" refers to all the software running on a Controller, including both the Web Management Application and the software that operates the Doors. Updating the software installs upgrades received from LTS.

You can update software in two different ways:

1. Log in to any Controller and update it directly
2. Use the Web Management Application to update any Secondary Controller remotely

Note that a Primary Controller can only be updated using the first method.

In either case, you must have an update file available on your own computer.

Both methods cause the updated Controller to reboot.

Updating the Software On The Controller You Are Logged Into

1. Go to Software Settings.
2. Click **Update Software**.
3. Click **Browse** and select the software update file from your computer.
4. Wait while the file transfers to the Controller.
5. When it completes, click **Ok.** There will be a delay while the update installs, then the Controller will go offline while it reboots.

Updating the Software of a Secondary Controller from the Primary

This method involves two steps: (1) send the update file to the Web Management Application, then (2) download the file to Secondary Controllers.

1. Go to Hardware.
2. Click **Upload Software Update** in the menu bar.
3. Click **Browse** and select the software update file from your computer.
4. Follow the prompts and the software update file will be uploaded, but *not applied to any Controller.*
5. Select a Secondary Controller.
6. Scroll down to **Software Update** and select the update file.
7. Click **Download.**
8. Follow the on-screen prompts to update the software on the Secondary Controller you selected.

Related Topics

- Software Settings

4.2.7 Resync All

The **Resync All** button on the menu bar causes a full resynchronization of data to all Secondary Controllers. All configuration from the Web Management Application (on the Primary Controller) is freshly updated on all Secondary Controllers. This includes all hardware, Door, and access configuration, including Users data. It does not include Network or Software version settings.

Individual Secondary Controllers can be resynchronized under **Maintenance** on their Hardware pages.

4.3 Doors

Every card, PIN, and biometric reader in the system is represented as a Door (see Understanding Controllers and Doors).

Doors are automatically created to match the **Configuration** property of Controllers in Hardware. The number of Doors you can create are limited by your license. Contact your authorized LTS representative for license upgrades.

Menu Buttons

Manual Commands	Allows direct control of the selected Door using Manual Commands to change Door Mode or unlock the Door.

Key Properties

For the complete list and details, see Door Properties.

Name	The name of the Door. Required, maximum 32 characters.

Type	Shows the Door's function: "In", "Out", "Card Enrollment Point", or "Muster Point". This is determined in Hardware.
Door Template	Used to configure this Door with a template, which overrides and disables some properties on this screen.
Default Mode	The Door Mode for this Door whenever not altered by a Schedule, manual command, or Event. Door Mode determines whether a Door is locked, and what kinds of access can unlock it.
Door Mode Schedule	Pick a Door Mode Schedule to change the Door Mode according to the day and time of day.
Multi-User Access	See Multi-User Access.
Areas and Anti-passback	See Areas.

Related Topics

- Using Property Views
- Door Properties
- Door Modes
- Door Templates
- Manual Commands
- Door Status

4.3.1 Door Properties

Door properties differ based on the door type. For example, Muster and Card Enrollment Points have far fewer properties since they do not control a door strike or have other door hardware.

Name The name of the Door. Required, maximum 32 characters.

Status The current status of the Door, including online/offline, Door Mode, locked/unlocked, open/closed, or errors such as forced, held, tamper, reader offline. Lockdown or Emergency Unlock will be indicated here, when active.

Alarm If any Alarm is pending at the Door, it is shown here.

Type How the Door is used:

- **In** — an entry Door. Either an entry-only Door, or an entry Door as a part of an entry/exit (in/out) Door pair.
- **Out** — an exit Door.
- **Muster Point** — used to check in during an emergency for the Muster report.
- **Card Enrollment Point** — used only to enroll cards.

Controller The Controller that this Door is managed by.

Sub-Controller The Sub-controller (I/O) which manages this Door's hardware.

Door Template A Door Template defines common parameters. Once a Door is linked to the template, the fields are read-only in the Door screen.

If the Door template is modified, the associated Doors are also updated.

Location	Location of the Door.
Description	Description or comments
Default Mode	The Door Mode for this Door whenever not altered by a Schedule, Manual Command, or Event. Door Mode determines whether a Door is locked, and what kinds of access can unlock it.
Door Mode Schedule	Pick a Door Mode Schedule to change the Door Mode according to the day and time of day.
Multi-User Access	The Multi-User Access configuration, if multiple Users are required to open a Door.
Unlock Time (s)	The amount of time the lock is activated for an access (access granted, exit requested, etc).
Default Forced Open Masking	• **Default - Unmasked** • **Unmasked** • **Masked**
Forced Open Masking Schedule	If selected, Forced Open will be masked during the selected Schedule.
Default Held Open Masking	• **Default - Unmasked** • **Unmasked** • **Masked**

Held Open Masking	If selected, Held Open will be masked during the selected Schedule.
Schedule Default	Only applicable to Monitor Open Only Doors:
Monitored Open Masking	• **Default - Unmasked** • **Unmasked** • **Masked**
Monitored Open Masking Schedule	If selected, Monitored Open will be masked during the selected Schedule. Only applicable to Monitor Open Only Doors.
Held Open Alarm Time (s)	The amount of time a Door can be held open before a held open Event is generated. This Event can be configured in the Sub-controller configuration to drive an aux output, for example, to sound a beeper.
Minimum Unlock Time (s)	If **Re-lock On** allows for the Door to be re-locked before the strike time is up, then this is the minimum time the Door will stay unlocked. This is to avoid an unlock pulse that is too brief, which can be a problem for some hardware.
Extended Unlock Time (s)	If a User has **Use Extended Door Times** checked, this time is used instead of **Unlock Time**. **Important:** Accessibility functions are regulated by country- and region-specific codes. Please refer to these when designing and configuring your system to ensure compliance.

Extended Held Time (s)	If a User has **Use Extended Door Times** checked, this time is used instead of **Held Open Alarm Time**. **Important:** Accessibility functions are regulated by country- and region-specific codes. Please refer to these when designing and configuring your system to ensure compliance.
Held Open Pre-Alarm Warning Time (s)	The amount of time before the **Held Open Alarm Time** is reached, when a held open pre-alarm warning Event is generated. This Event can be configured in the Sub-controller configuration to drive an aux output, for example, to sound a beeper.
Suppress Exit Button Events	When selected, exit requested Events are not created for this Door. This can be used if the number of these Events is considered too numerous and unimportant.
Unlock on Exit Button	If checked, the Door is unlocked when the exit button is pressed. This may not be required for systems where the exit button is wired directly to cut off power to the lock, for example. **Important:** Exit button functions are regulated by country- and region-specific fire codes. Please refer to these when designing and configuring your system to ensure compliance.
Re-lock On	When the lock should be re-locked after access is granted: • **End of Unlock Time** • **Door Open** • **Door Close** • **Door Close or End of Unlock Time** (whichever is sooner)
Exempt From Global Lockdown	If checked, the Door will not be affected by a global lockdown

Exempt From Global Emergency Unlock	If checked, the Door will not be affected by a global emergency unlock
Entering Area	The Area the Door leads into for anti-passback (and airlock) configurations.
Exiting Area	The Area the Door leads out of for anti-passback (and airlock) configurations.
Anti-passback	

None — no anti-passback enforced

	Method	• **Door-Based** — cannot use same credential within certain amount of time at the same Door.
		• **Area-Based** — checks that they are known to be in the correct Area before using a Door leading out of that Area, into another Area.

	Anti-passback Mode	Available if **Anti-passback Method** is **Area-Based**: whether to deny or grant access on an anti-passback violation:
		• **Hard (Deny Access)**
		• **Soft (Grant Access)**

Minutes Denied	Available if **Anti-passback Method** is **Door-Based**. The number of minutes before the same credential can be used at the Door. If blank, a default of 60 minutes is used.

Related Topics

See Anti-Passback.

- Doors
- Door Templates
- Door Status
- Door Modes
- Anti-Passback
- Manual Commands
- Hardware Properties
- Locations
- Areas

4.4 Video Systems

Video Systems, also known as NVRs, DVRs, and VMSs, are video recording systems which manage one or more Cameras.

Video integration is a licensed feature, including the maximum number of Video Systems. Contact your authorized LTS representative for license upgrades.

Once a Video System is created, the Cameras are auto-discovered and added to the system. It may take a moment for this to happen, therefore it may be necessary to refresh the page (for example by navigating to another screen, and navigating back) in order for the discovered Cameras to appear.

4.5 Cameras

Cameras allow the viewing of live and recorded video. Cameras are connected to and managed by Video Systems.

Video integration is a licensed feature, including the maximum number of Cameras. Contact your authorized LTS representative for license upgrades.

Cameras cannot be added manually, they are auto-discovered and added after a Video System is configured and online.

Cameras can be added to Maps.

Camera Properties

Name	The name of the Camera. Required, maximum 32 characters.
Status	The status of the Camera, either **Online** or **Offline**.
Video System	The Video System to which this Camera is connected.
Location	A Location to associate with the Camera
In View	Use **Add** and **Remove** to specify which Doors are in view of this Camera. When a Door is associated with a Camera in this manner, the live and recorded video is available in other screens where the Door is visible, such as Events, Alarms, Notifications, and Door Status.
Live Video	When available, this will show a still video frame preview. Clicking on it will pop up a live video window. Note: if your Video System has a self-signed HTTPS certificate, which most Video Systems have by default, you will be prompted to accept and bypass the browser warning for this certificate. This is required if live or recorded video is to be viewed on such a system.

Description	Description or comments

Related Topics

- Using Property Views
- Video Systems
- Events
- Alarms
- Notifications
- Door Status
- Maps

4.6 Locations

Locations are labels you can apply to organize Doors and hardware on lists and reports, particularly on Events and Alarms. Locations can be assigned to Doors, Controllers, Areas, and Maps.

Location Properties

Name	The name of the Location. Required, maximum 32 characters.
Type	Category by Location size. From large to small, they are: **Region > Campus > Building > Floor > Room**
Parent Location	Designates this Location as included in any *larger* Location. A **Building's** parent could be a **Campus** or **Region,** but not a **Floor** or **Room.** When you filter Events to a Location, all the smaller Locations that are included in it will also be displayed.

Related Topics

- Using Property Views
- Events
- Alarms

4.7 Areas

Areas are physical regions you define, and are used for Anti-Passback, Muster, and airlocks. A column to show the Area can be added on Events and Alarms.

Areas are actually nothing but a label. They serve no function until you define which Doors lead into and out of the Area. You do this by setting the **Entering Area** and **Exiting Area** of each relevant Door.

Predefined Areas

There are two Areas that are predefined by the system and cannot be edited or deleted:

- **Global Out** — Doors that enter from, or exit to, the "outside world" should use this as the **Exit Area** or **Entry Area,** respectively.
- **Muster** — An Area where all Muster Points "enter" to. Anyone who uses a Muster Point will have their last known Area set to the Muster Area and will be excluded from the Muster report.

Using the Screen

Name	The name of the Area. Required, maximum 32 characters.
Location	A Location to associate with the Area
Type	• **Local** — Used only on a single Controller. Can be used for airlock.

- **Global** — Can be used on multiple Controllers, for global anti-passback enforcement.

Managed By — (Local Areas only) The single Controller for this Area.

Airlock Mode — (Local Areas only)

- **No Exit During Entry** — A Door exiting the Area cannot be used while a Door entering the Area is open.
- **Strict Single Door** — No two Doors in the Area can be unlocked/opened at the same time.

Description — Description or comments

Related Topics

- Using Property Views
- Anti-Passback
- Muster

4.8 Maps

Maps configuration is used to create the screens for the Maps view.

The Maps view is used to show the status of your Doors and Controllers on graphical backgrounds, for example, on maps of your building or campus. It highlights all problems in red, and allows sending commands to Doors. Maps may also have links to other Maps for easy navigation.

Map Properties and Controls

Name — The name of the Map (required, maximum 32 characters)

Location	Optional Location of the Map.
Background	Click **Upload** to load an image from your computer. This will be the canvas on which you can place devices. Large images will shrink to fit the available space.
Elements	Elements, in multiple list boxes, can be clicked on and dragged to the Map. These elements can be: • **Custom Elements** • **Hardware** (Controllers) • **Doors** • **Cameras** (if video is licensed) When on the Map, their blue wrench icon provides options to • delete the element, or • set the destination of a "Link" element from a list of other Maps. Text entered in **search** filters all three element lists.

Related Topics

- Using Property Views
- Maps (Monitoring)

4.9 Card Designs

A Card Design is a print layout you create for use in Printing Cards. It can include User information such as the name and expiration date and images such as the User photo and logos.

Properties

Name	The name of the Card Design. Required, maximum 32 characters.
Description	Description or comments.

The Design Area

Center Column

The center area is your canvas to "draw" your card on. It shows a standard size access card, front and back sides.

Important: Review your card printer manual to understand its limitations, such as whether it can print both front and back and whether you are allowed to print to the edge of the card.

Left Column

Click and drag elements from the left panels onto the card area.

Click elements on the card area to select them. Shift-click to select multiple elements.

Drag selected elements to move them.

Images (only) can be sized by dragging on the corners.

Right Column

The first row of three icons performs standard delete, undo, and redo actions.

The second row has six options for aligning elements, followed by four options controlling which elements are on top of others. Hover over any icon to see its exact function. You must select more than one item to enable the alignment options.

The rest of this panel shows the properties of the currently selected item.

For **Images**, click **Select Image** to load an image file from your computer.

For **Text** and **User Fields,** enter the **Text**. Text between "{{" and "}}" will be replaced with the named property of the User. Additional text may be added outside the brackets, but the text inside must be a valid field name.

The remaining options for text set the font and color.

X Origin and **Y Origin** are properties of both images and text. They determine which direction the element will grow to fit the contents, *by choosing which corner will never move.* The default is top left, and the box will expand to the right and down when, for instance, the name field is long or its font size increases. If you change the origin to bottom right, the box will expand upwards and to the left, allowing you to place the box on the right or bottom edge of the card.

Notes

Supported image formats are PNG, JPEG, and GIF.

Text will print over of images (if on top), and transparency in images is supported.

Related Topics

- Using Property Views
- Users
- Printing Cards

4.10 Card Formats

Card Formats define the low-level details of how data is stored on the cards you use. Your Sentinel Series system includes all of the card formats you will likely need, although you might want to enter a "facility code" specified by your card vendor.

If you do use an uncommon type of card, you will have to create a custom card format. This is quite technical, and requires exact specifications from the card vendor.

Notes

You can use more than one card format in your system.

Card formats are neither associated with specific Doors nor specific Users—they all are used for all.

Two card formats with the same number of bits cannot be enabled at the same time, unless they both have facility codes and those codes are different.

Entering Your Facility Code

You must know which of the existing card formats matches your cards. Simply select that format, enter the **Facility Code** number, and save.

Card Format Properties

Note: Start and location fields are number of the bit, where the first bit on the card is number 0.

Name	The format name. Required, maximum 32 characters.
Bits	The total number of bits on the card, including parity bits, etc.
Enabled	Use or do not use the format.
Facility Code (optional)	If there is a facility code field (start/length specified), this is the value that the facility code must be equal to for the format to be matched.
Facility Code Start	The facility code start (bit number).
Facility Code Length	The facility code length (in bits).

Card Num Start	The card number start (bit number).
Card Num Length	The card number length (in bits).
Parity (1-4)	• **None/Even/Odd** — **None** to not use this parity field at all, **Even** or **Odd** for parity calculation method. • **Start** — The start bit of the parity source (the range of bits to be checked for parity). Does NOT include the location of the parity bit itself. • **Length** — The length in bits of the parity source. • **Location** — The bit number of the parity bit. • **Mask** — Normally, the entire source is used. If only some bits in a pattern are to be used in the source, this is entered here as the mask, as a string of 0s and 1s.

Related Topics

- Using Property Views

4.11 User Groups

User Groups are used in Multi-User Access. Members of the group are added in Users.

User Group Properties

Name	Required. Maximum 32 characters.
Description	Description or comments
Allow First Credential Unlock	If checked and a User in this group accesses a door in a "First Unlocks" Door Mode, then the door will stay unlocked after the access. See First Credential Unlock for details.

Related Topics

- Using Property Views
- Users
- Multi-User Access
- First Credential Unlock

4.12 Alarm Triggers

Alarms are triggered by Events, meaning that whenever an Event of a specified type occurs, an Alarm is also generated. The Alarm Triggers screen allows you to add to the Events that trigger Alarms and modify or remove the default triggers.

Alarm Trigger Properties

Triggering Event	The Event Type which will trigger an Alarm.
Priority	The importance of the Alarm created. The **Priority** can be used to sort the Alarms screen.

Color Triggering Event	The triggering Event will be in this color on the Events screen. This does not affect the Alarm color. (Some Event Types also have a color, whether or not they are Alarm triggers.)
Auto-acknowledge	If checked, the triggered Alarm will start off in the Acknowledged state.

Related Topics

- Using Property Views
- Alarms
- Events
- Event Categories and Types
- Emergency Features

4.13 Door Templates

Door Templates can be created from existing Door configurations, then applied to other Doors that require the same settings. Subsequent changes to the template are applied to every Door using it. Only certain Door properties are controlled by the Template (see below).

When a Door Template is applied to a Door, the properties which come from the template are no longer editable on the Doors screen. To change them, you must either edit the template, or remove the template from the Door.

A Door Template cannot be applied to a Door that has a different **Type** in its Door properties.

Creating a Door Template from an Existing Door

1. Go to the Doors screen.

2. Select a Door.
3. Click the **Create Door Template** button in the Door's properties.
4. Enter a name (required, maximum 32 characters), and optionally, a description.
5. Click **Save.**

Applying a Door Template to a Door

1. Go to the Doors screen.
2. Select a Door.
3. Select a **Door Template** in the Door's properties.
4. Check **Apply Template**. The Door will use the settings from the template only when this is checked. If you remove the check, the Door will keep the template settings unless you change them.
5. Click **Save**.

Door Template Properties

A Door Template overrides these Door Properties. Some Door types do not use all of these properties.

- **Manual Commands Enabled**
- **Unlock Time**
- **Held Open Alarm Time**
- **Minimum Unlock Time**
- **Extended Unlock Time**
- **Extended Held Time**
- **Held Open Pre-Alarm Warning Time**
- **Suppress Exit Button Events**
- **Unlock on Exit Button**

- **Re-lock On**

Related Topics

- Using Property Views
- Doors
- Hardware Templates

4.14 Hardware Templates

Hardware Templates can be created from existing Sub-controller (I/O) properties, then applied to other Sub-controllers that require the same settings. Subsequent changes to the template are applied to every Sub-controller using it. Only certain Sub-controller properties are controlled by the Template.

When a Hardware Template is "applied" to a Sub-controller, the properties which come from the template are no longer editable on the Sub-controller screen. To change them, you must either edit the template, or remove the template from the Sub-controller.

Creating a Hardware Template from an Existing Sub-controller

1. Go to the Hardware screen.
2. Select a Sub-controller.
3. Click the **Create Hardware Template** button in the Sub-controller's properties.
4. Enter a name (required, maximum 32 characters), and optionally, a description.
5. Click **Save**.

Applying a Hardware Template to a Sub-controller

1. Go to the Hardware screen.
2. Select a Sub-controller.

3. Select a **Hardware Template** in the Sub-controller's properties.
4. Check **Apply Template**. The Sub-controller will use the settings from the template only when this is checked. If you remove the check, the Sub-controller will keep the template settings unless you change them.
5. Click **Save**.

Related Topics

- Using Property Views
- Hardware
- Door Templates

Administration

5 Administration

The Admin menu includes a variety of settings for the whole system.

User Roles lets you see the definition of the built-in User Roles for Users logging into the web application and define new, custom roles.

Backup and Restore lets you backup and restore the system database and manage the scheduled backups.

System Settings provides control over the archiving settings and the custom field labels.

Network allows configuration of the networking settings.

Date and Time allows configuration of the time zone and network time settings.

Email Settings allows an SMTP mail server to be configured for the emailing of Notifications.

Archive Downloads allows the download of archive files generated according to the System Settings

Software Settings allows software update, factory reset, and reboot.

Web Server Settings allows the upload of an HTTPS certificate.

Communications is used to configure how primary and secondary controllers communicate.

Authorized Mobile Devices allows you to view and manage the mobile devices that have the mobile app installed.

5.1 User Roles

User Roles define what different Users can do within the Web Management Application. The system comes with a number of built-in User Roles which may not be modified or deleted. Custom User Roles can be created.

Here is a summary of the built-in User Roles.

System Administration	Unlimited; able to access all screens and functions.

Access Control Management	Provide access to Users and define the Doors, times, and other access control rules that allow or deny access. Able to configure Doors, but not Hardware. Able to execute all manual commands.
Basic Monitoring	Most monitoring functions. Able to view Alarms but not acknowledge or resolve them. Able to view Users but not create or edit them.
User and Credential Management	Add and manage Users and their associated credentials. Also able to perform some limited monitoring tasks. No Alarm management, and no hardware or Door configuration.
Alarm Monitoring	Similar to Basic Monitoring, but also able to acknowledge and resolve Alarms.

User Role Options - Menu Items

Option	System Administration	Access Control Management	Basic Monitoring	User and Credential Management	Alarm Monitoring
About: License	Yes				
Access Control: Access Levels	Yes	Yes			
Access Control: Door Mode Schedules	Yes	Yes			
Access Control: Emergency Codes	Yes	Yes			
Access Control: Multi-User Access	Yes	Yes		Yes	
Access Control: Schedules	Yes	Yes			

Option	System Administration	Access Control Management	Basic Monitoring	User and Credential Management	Alarm Monitoring
Access Control: Shared Access Codes	Yes	Yes		Yes	
Access Control: Special Days	Yes	Yes			
Access Control: Users	Yes	Yes		Yes	
Access Control: Users (Read-Only)	Yes	Yes	Yes	Yes	Yes
Administration: Archive Downloads	Yes				
Administration: Authorized Mobile Devices	Yes				
Administration: Backup and Restore	Yes				
Administration: Communications	Yes				
Administration: Date and Time	Yes				
Administration: Email Settings	Yes				
Administration: Software Settings	Yes				
Administration: Network	Yes				
Administration: System Settings	Yes				

Option	System Administration	Access Control Management	Basic Monitoring	User and Credential Management	Alarm Monitoring
Administration: User Roles	Yes				
Administration: Web Server Settings	Yes				
Configuration: Alarm Triggers	Yes				
Configuration: Areas	Yes	Yes			
Configuration: Card Designs	Yes	Yes			
Configuration: Card Formats	Yes				
Configuration: Door Templates	Yes	Yes			
Configuration: Doors	Yes	Yes			
Configuration: Hardware	Yes				
Configuration: Hardware Templates	Yes				
Configuration: Locations	Yes				
Configuration: Maps	Yes				
Configuration: User Groups	Yes				
Monitoring: Alarms	Yes				Yes
Monitoring: Alarms (Read-Only)	Yes	Yes	Yes		Yes

Option	System Administration	Access Control Management	Basic Monitoring	User and Credential Management	Alarm Monitoring
Monitoring: Door Status	Yes	Yes	Yes	Yes	Yes
Monitoring: Events	Yes	Yes	Yes	Yes	Yes
Monitoring: Maps	Yes	Yes	Yes	Yes	Yes
Monitoring: Reports	Yes	Yes	Yes	Yes	Yes
Monitoring: Reports: Access Levels	Yes	Yes			
Monitoring: Alarm History	Yes		Yes		
Monitoring: Reports: Audits	Yes	Yes			Yes
Monitoring: Reports: Doors	Yes	Yes			
Monitoring: Reports: Event History	Yes	Yes	Yes	Yes	Yes
Monitoring: Reports: Muster	Yes	Yes	Yes	Yes	Yes
Monitoring: Reports: Schedules	Yes	Yes			Yes
Monitoring: Reports: Users	Yes	Yes	Yes	Yes	Yes
Monitoring: Reports: Users With Access Level	Yes	Yes	Yes	Yes	Yes
Monitoring: Reports: Users With Access to Door	Yes	Yes	Yes	Yes	Yes

User Role Options - Manual Commands

Option	System Administration	Access Control Management	Basic Monitoring	User and Credential Management	Alarm Monitoring
Controller: Software Update	Yes				
Controller: Reboot	Yes				
Controller: Replace	Yes				
Controller: Resync	Yes				
Credential: Reset	Yes	Yes	Yes	Yes	Yes
Door: Momentary Access	Yes	Yes	Yes	Yes	Yes
Door: Set Door Mode	Yes	Yes			Yes
User: Forgive	Yes	Yes	Yes	Yes	Yes

User Role Options - Door Modes

Option	System Administration	Access Control Management	Basic Monitoring	User and Credential Management	Alarm Monitoring
Cancel/Clear	Yes	Yes			Yes
Unlocked	Yes	Yes			Yes
No Access	Yes	Yes			Yes
Card Only	Yes	Yes			
Card and PIN	Yes	Yes			
PIN Only	Yes	Yes			
Card or PIN	Yes	Yes			

Option	System Administration	Access Control Management	Basic Monitoring	User and Credential Management	Alarm Monitoring
Unlocked (Emergency)	Yes	Yes			Yes
Lockdown	Yes	Yes			Yes
Card Only (First Unlocks)	Yes	Yes			
Card and Biometric	Yes	Yes			
Card and Biometric and PIN	Yes	Yes			
Biometric Only	Yes	Yes			
Biometric and PIN	Yes	Yes			
Biometric or PIN	Yes	Yes			
Card or Biometric	Yes	Yes			
Biometric or Card or PIN	Yes	Yes			
No Access, No Exit Button	Yes	Yes			Yes
Card and PIN (First Unlocks)	Yes	Yes			
PIN Only (First Unlocks)	Yes	Yes			
Card or PIN (First Unlocks)	Yes	Yes			
Card and Biometric (First Unlocks)	Yes	Yes			
Card and Biometric and PIN (First	Yes	Yes			

Option	System Administration	Access Control Management	Basic Monitoring	User and Credential Management	Alarm Monitoring
Unlocks)					
Biometric Only (First Unlocks)	Yes	Yes			
Biometric and PIN (First Unlocks)	Yes	Yes			
Biometric or PIN (First Unlocks)	Yes	Yes			
Card or Biometric (First Unlocks)	Yes	Yes			
Biometric or Card or PIN (First Unlocks)	Yes	Yes			

Related Topics

- Using Property Views
- Users

5.2 Backup and Restore

Backup and Restore allows configuration of database backups, including scheduling. It also provides manual backup and restore of the database.

Backup files are saved encrypted, in the `.dbbackup` format. Up to three backups can be saved on the Controller. Older backups are automatically deleted. You can also download backup files to your computer.

By default, the database on a Primary Controller is automatically backed up every night at midnight. You can also schedule a backup on a custom schedule. If a scheduled backup is not enabled, the automatic backups do not occur.

Backup files are tied to the serial number of the Primary Controller from which they were made. If a backup from one controller must be restored to a different controller, the system will prompt for the source controller's serial number, to complete the restore.

Secondary Controllers do not create backups. Their data comes from the Primary Controller.

When the database is successfully backed up, a "Database Backed Up" event is generated. If there is any kind of failure backing up, a "Database Backup Failed" event is generated.

Sentinel Series controllers have a USB port which can accommodate a USB drive (FAT32 only). If the option "Copy Backups to USB Drive" is checked, then every time a backup is made, whether manual or scheduled, the backup will be copied to a folder called "backups" on the USB drive. If this folder does not exist, it will be created. A maximum of 10 backups will be stored in this folder. Older backups are automatically deleted. When the database is successfully copied to the USB drive, a "Database Backup Copied to USB Drive" event is generated. If this copy fails a "Database Backup Copy to USB Drive Failed" is generated. The USB drive not being connected is the most common cause of such a failure.

Changing the Backup Schedule

To schedule a backup to occur at a different time or frequency:

1. Under **Scheduled Backup,** leave the **Enabled** box checked (recommended).
2. Select **Daily**, **Weekly** or **Monthly**. **Daily** is recommended.
3. Select the time of day to perform scheduled backups.
4. Click **Save**.

Manually Backing Up the Database

Click **Backup Now** to backup the database to a file on the Controller, and optionally download the newly created backup to your computer.

Click **Download Now** to download the file to your computer.

Restoring a Backup

Backups can be restored from a file on the Controller or from an uploaded file.

Caution: Existing data will be erased if you choose to restore.

1. Under **Restore**, select the backup or select a `.dbbackup` file from your computer.
2. Click **Restore**, then click **Restore** again at the prompt to confirm. If the backup came from a different controller, you will be prompted for the source controller's serial number.
3. Wait for the restore process to complete. You will be logged out automatically.
4. Log back in to the Web Management Application.

5.3 System Settings

System settings define assorted settings used by the system, for database maintenance, custom fields, and PIN length.

Database Maintenance

These settings define the storage requirements for Notifications, Events, Audits and Alarms. The default settings are typically sufficient and do not need to be changed. Revise the following if necessary. The archive files generated according to these settings are available in Archive Downloads.

Maximum Notifications per User	Older Notifications are automatically deleted, even if they have not been cleared by the User, to keep the total per User at or under this limit
Maximum Events in Database	Older Events are archived, to keep the total number of Events in the database at or under this limit.
Maximum Event Archive Files	Events are archived to CSV files on the Controller. This is the maximum number of Event archive files to keep.

Maximum Event Archive File Size (Bytes)	The maximum size of any individual Event archive file.
Maximum Audits in Database	Older audits are archived, to keep the total number of audits in the database at or under this limit.
Maximum Audit Archive Files	Audits are archived to CSV files on the Controller. This is the maximum number of audit archive files to keep.
Maximum Audit Archive File Size (Bytes)	The maximum size of any individual audit archive file.
Maximum Alarms in Database	Older Alarms are archived, to keep the total number of Alarms in the database at or under this limit.
Maximum Alarms Archive Files	Alarms are archived to CSV files on the Controller. This is the maximum number of Alarm archive files to keep.
Maximum Alarm Archive File Size (Bytes)	The maximum size of any individual Alarm archive file.

Custom Fields

This section allows you to change the custom field labels which appear in the Users screen. Maximum 32 characters.

Shared Access/Emergency/PIN Codes

This section allows you to change the system-wide length of all Shared Access Codes, Emergency Codes, and PIN Codes (Users screen). The same length is used for all of these.

Changing the length will alter all existing PINs.

- Increasing PIN length will prepend zeros to existing shared access codes, emergency codes, and User PIN codes.
- Decreasing PIN length will randomly regenerate all shared access codes and emergency codes, and will clear all User PIN codes.

This length must be between 4 and 8 characters. The default length is 4.

Related Topics

- Users
- Notifications
- Events
- Audits
- Alarms
- Shared Access Codes
- Emergency Codes

5.4 Network

Use the Network screen to view or change a Controller's network settings. The settings apply only to the Controller you are logged into. To change networking for a Secondary Controller you must log in to that controller directly using the link on its Hardware page.

We recommend that your Primary Controller be assigned a static IP address. If a Primary Controller does not have a static IP address, and the IP address changes dynamically, then it may be difficult to find the correct address for connecting with a web browser, and Secondary Controllers may no longer be able to reach it.

In most cases, Secondary Controllers should use DHCP unless you cannot use Discovery.

Select **Ethernet** to change your wired connection or **WiFi** to set up wireless networking (on supported models). When Network settings are saved, the Controller will reboot, and might be at a different network address when it does so.

Network Properties

These properties apply to both wired and wireless connections.

	Configure IPv4	• **Manually** — The Controller will have a static IP address, and all settings must be entered in the remaining properties. • **Using DHCP** — The Controller will get all settings from the network. Its IP address will be essentially random, and can change from day to day. No other properties need to be entered.

IP Address — The static IP address to use for the Controller you are logged into

Subnet Mask — The mask for the network, usually "255.255.255.0"

Gateway — IP address of your Internet gateway, usually the address of your network router

DNS Servers — The IP address of your DNS server, usually specified by your IT department or provided by your Internet service provider. If you don't know, you may use a public DNS. (One such is "Google Public DNS" at "8.8.8.8" and "8.8.4.4".)

Search Domains — Only used as your network administrator directs

Setting Up WiFi

1. Select **WiFi** in the list.
2. Check **Active** to turn WiFi on.
3. Click the **Scan for Networks** button. In the results window, select a network to join.
4. Click the **Change** button to enter and confirm the network password.
5. Set the network properties.
6. Click **Save.**

Network Reset

If at any point you find you cannot connect to the Controller at the IP address you have defined, you can try a hard network reset.

Network reset changes the Controller to a "link local" IP address, which allows connecting directly to your computer. Using this connection you can enter the Web Management Application to fix the network settings.

1. Find the small opening on the Controller labeled “Reset.” Insert a paperclip to depress the button for 5-10 seconds. The wired address of the Controller will revert to the default, 169.254.202.242, until rebooted, reset, or the configuration is modified.
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 already 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 be directed to the Web Management Application login screen. Note that it might take a minute for the connection to become available.

Related Topics

- Using Property Views

5.5 Date and Time

Date and Time is used to set the Primary Controller's time zone and network time settings (NTP).

To set the Primary Controller's time zone, select the time zone where the Primary Controller is installed. By default, Controllers are set to the **Eastern Time (US & Canada)** time zone.

The **Use Daylight Savings** checkbox determines whether daylight savings is applied.

Date and Time shows the time on the Controller. **Browser Time** is the time on your computer.

The option **Set Server Time to Current Browser Time** may be used if NTP is not in use, for a one-time synchronization of the Controller's time to the browser time. Note that this does not synchronize the browser's time zone, only the absolute underlying time.

The **Update Date And Time Automatically From Network** checkbox determines whether NTP is used.

By default, Primary Controllers are configured to use NTP to get time from the network, and they are pre-configured with a default set of NTP servers. These defaults assume that your Controller has access to the Internet. If this is not the case, you may wish to use NTP servers within your network, or turn off NTP entirely if it is not available.

5.6 Email Settings

Email Settings are used to configure an SMTP server for sending copies of Notifications by email, if configured by any Users. The emails are sent to the email address associated with the specific User in the Users screen.

These settings are below. These settings usually come from an Internet provider, a mail service provider, or a company IT department. Be sure to test the settings with the **Send Test Mail** button.

Active	Enable or disable the email settings.
Send Mail From	Enter the “from” email address for email Notifications. The emails will be “from” this email address.

SMTP Mail Server	The SMTP mail server hostname to send the mail messages through.
Port	SMTP mail server port.
Username	username for the SMTP mail server account.
Password	password for the SMTP mail server account.
Use SSL/TLS	Check to use a secure encrypted connection when communicating with the mail server.

Under **Test Mail**, enter an email address to send to, and click **Send Test Mail** to test the settings.

Related Topics

- Users
- Notifications

5.7 Archive Downloads

Events, Audits and Alarms are archived after the system has been running long enough to exceed the limits defined in System Settings. This list will be empty until those limits have been reached.

Files are archived in CSV format. You may select any of them, and download them.

Related Topics

- System Settings
- Events

- Audits
- Alarms

5.8 Software Settings

Software

This section shows the current software version, and allows it to be updated. See Software Update.

Factory Reset

This section allows a Factory Reset as well as a button to reboot the device.

5.9 Web Server Settings

Web Server Settings is used to upload a signed HTTPS certificate, for more secure connections, as well as configure other settings such as the **Web Server Port**.

HTTPS Certificate

This section is used to upload a signed HTTPS certificate..

Note: If a certificate is not uploaded, a self-signed certificate will be used, which results in a browser warning. Your IT department can optionally provide a signed certificate for HTTPS, which is not required for encrypted HTTPS communication but provides additional security and prevents the browser warnings.

1. Obtain a ".pem" or ".pfx" certificate file, and copy it to your computer.
2. Click **Upload Certificate**.
3. Complete the online prompts to select and upload the certificate file.

Changing the certificate results in a reboot of the Controller.

Settings

The **Web Server Port** determines which networking port the Web Management Application is available on. This defaults to 443, the standard HTTPS port.

This port does not normally need to be changed, except for advanced network environments or IT requirements. If this port is changed, the controller will reboot, and you will be logged out. You will need to then log in at the new https:// URL which includes the port, preceded by a colon. All users who log in will need to do likewise.

Note that regardless of what port is chosen, HTTPS will be in use.

5.10 Communications

Communications is used to configure how primary and secondary controllers communicate.

When a secondary controller is initially added, the primary controller contacts it, and the primary gives the secondary the primary's own IP address, for the secondary to "call back". After this point, all communications is initiated by the secondary controller.

For local Ethernet and WiFi networks, the primary's actual IP address for the Ethernet and/or WiFi network interface is given to the secondary. This works correctly for local networks.

However, for wide-area networks involving hostnames, port forwarding, firewalls, dynamic DNS services, and other advanced networking techniques, the secondary may need to be given an alternate IP address, or perhaps a hostname. If it is a hostname, it must be resolvable by the secondary, that is, the secondary must have the correct networking settings, including DNS for hostname resolution.

Important: because this setting is only sent to secondary controllers when they are first linked to the primary, if these values are changed, they will not take effect on existing secondary controllers until the **Replace** operation is applied.

For these advanced configurations, the following properties may be set:

Secondary controllers connect back to primary at	The address (hostname or IP address) that the primary controller is reachable by, given to secondary controllers when they are first linked with the primary. If not specified, this defaults to the primary controller's Ethernet IP address.
Secondary controllers connect back to primary at (alternate)	If the first address is not reachable for any reason, the alternate address, if specified, will be tried. If not specified, and WiFi is enabled, this defaults to the primary controller's WiFi IP address.

Advanced Networking Considerations and Examples

In order to get primary and secondary controllers to communicate in advanced networking situations, it is important to be aware of which network ports need to be accessible from one controller to another, and in which direction. This is essential for correctly configuring firewalls, and any kind of port forwarding.

It is also important to understand that both the primary controller and the secondary controller need to be able to reach each other, although on different ports.

Primary Controller to Secondary

The primary controller needs to be able to access the secondary controller on its (HTTPS) Web Server Port, which is 443, by default, for initial linking. This port can be changed on the secondary controller (logged in to the secondary controller's web application) under Web Server Settings. If this port is changed to a non-default port, the primary controller needs to be able to access the secondary controller on this non-default port, instead.

This connection from the primary controller to the secondary is only used when a secondary is first added to the system, to link the secondary controller back to the primary. Once the secondary controller has been linked (and comes online), all connections after that are from the secondary controller back to the primary (see below).

If port forwarding from a router or firewall is needed to access the secondary controller, a port on this router/firewall needs to be forwarded to the actual (HTTPS) Web Server Port on the secondary controller. In this case, when adding a secondary controller to a primary, on

the primary, the address and port to be entered are as follows: the reachable (public) address or hostname of the router/firewall, and the source port on the router/firewall.

Secondary Controller to Primary

The secondary controller is told by the primary controller, in the initial setup/linking step (see above), what address to use to call back to the primary controller. The port, however, is fixed at 9723. So if a router/firewall is in the path of the secondary controller connecting to the primary, port 9723 needs to be open on the router/firewall, forwarded to port 9723 on the primary controller, at the primary's local IP address.

Example 1 - Default Ports

A secondary controller, local IP 192.168.0.1, is behind a firewall with public IP 1.2.3.4. Public port 443 on the secondary's firewall is configured to forward to 192.168.0.1:443.

The primary controller, local IP 192.168.1.1, is on a different LAN, behind a firewall with public IP 5.6.7.8. Port 9723 on the primary's firewall is configured to forward to 192.168.1.1:9723

Before adding the secondary controller to the primary, configure the primary controller to have **Secondary controllers connect back to primary at** set to 5.6.7.8.

Then, add the secondary controller to the primary, with address 1.2.3.4, and use the default port.

Example 2 - Non-Default Public Secondary Port

A secondary controller, local IP 192.168.0.1, is behind a firewall with public IP 1.2.3.4. Public port *9999* on the secondary's firewall is configured to forward to 192.168.0.1:443.

The primary controller, local IP 192.168.1.1, is on a different LAN, behind a firewall with public IP 5.6.7.8. Port 9723 on the primary's firewall is configured to forward to 192.168.1.1:9723

Before adding the secondary controller to the primary, configure the primary controller to have **Secondary controllers connect back to primary at** set to 5.6.7.8.

Then, add the secondary controller to the primary, with address 1.2.3.4, and use port *9999*.

Example 3 - Non-Default Public Secondary Port, and Non-Default Local Secondary Web Server Port.

A secondary controller, local IP 192.168.0.1, is behind a firewall with public IP 1.2.3.4. *The Web Server Port has been configured on the secondary controller to be 5000, instead of 443*. Public port *9999* on the secondary's firewall is configured to forward to 192.168.0.1:*5000*.

The primary controller, local IP 192.168.1.1, is on a different LAN, behind a firewall with public IP 5.6.7.8. Port 9723 on the primary's firewall is configured to forward to 192.168.1.1:9723

Before adding the secondary controller to the primary, configure the primary controller to have **Secondary controllers connect back to primary at** set to 5.6.7.8.

Then, add the secondary controller to the primary, with address 1.2.3.4, and use port *9999*.

5.11 Authorized Mobile Devices

A mobile device must be authorized before it can connect to the Sentinel Series system.

Mobile devices are authorized in the Users screen, including adding, updating, and removing authorizations. See User Properties. The Authorized Mobile Device screen allows you to view all of these authorizations in a single place, and delete them if necessary.

Each code can authorize only one mobile device. You may delete and add authorizations as needed to support several devices. The number of devices you can authorize is limited by your license. Contact your authorized LTS representative for license upgrades.

Authorized Mobile Devices Properties

Name The name of the authorization.

Enabled	Whether this authorization is enabled.
Valid From	The date when authorization begins.
Until Further Notice, Valid To	At the beginning, if Until Further Notice is checked, then the device authorization never expires. If it is unchecked, then the Valid To date determines when the authorization expires. Note that the Valid To time takes effect at the end of the minute, not Signing in from a Mobile Device.

1. Install and run the ***Defendas*** mobile app, available in Apple's App Store and in Google Play.
2. Press **Scan QR Code**.
3. You might have to confirm that the mobile application may use the camera.
4. The photo viewfinder will appear. Point the square scanning box at any copy of the authorization QR code. A picture will be taken automatically when a QR code is within the box, showing the message, "Authorization code successfully located."
5. The **Sign In** screen is next. Enter the **Server Address** of the primary Sentinel Series controller. Enter your Sentinel Series **Username** and **Password**. Press **Sign In**.
6. Once signed in you will see a list of everything you can do, including viewing alarms or status and initiating emergency lockdown.

Important: To connect locally, the mobile device must be connected by WiFi to the same local network as the Sentinel Series controllers. To connect from a distance, your network administrator must in some way open access from the Internet (such as by using a NAT) and provide the necessary **Server Address**.

Related Topics

- Using List Views

- Users
- User Properties

Features and Tasks

6 Features and Tasks

This section provides information on features which span multiple screens and information on common tasks.

Lockdown, Emergency Unlock, and Duress are used to handle emergency situations.

Reports and Printing explains how to print from the Web Management Application

Operators use Manual Commands to directly unlock Doors or temporarily change their Door Mode.

First Credential Unlock allows the first arriving individual to completely unlock a Door.

Manage the address and encryption key of OSDP Readers.

Use Card Enrollment Points to enroll a User's cards by swiping the card.

QR Code Credentials are credentials to be used with the app, and the LTS QR500 Series Reader.

Anti-passback discourages individuals from loaning or sharing their access card.

You can reset your password if you have registered the product.

Factory Reset returns your Controller to factory settings and removes all configuration and data.

The Setup Wizard must be completed one time during installation and after a Factory Reset.

6.1 Lockdown

Global lockdown is a feature to be used in emergency situations to lock all Doors in the system, such that no access is allowed. Scheduled and manually commanded Door Mode changes have no effect during lockdown.

There are exceptions:

- Doors with **Exempt From Global Lockdown** checked are not affected.
- Emergency Codes, and Users with **Access Doors in Lockdown Mode** checked are able to access Doors in the lockdown state.
- Exit Buttons continue to work during lockdown.

- Lockdown versus Emergency Unlock:
  - An emergency unlock will override a lockdown if the emergency unlock occurs after the lockdown.
  - A lockdown will override an emergency unlock if the lockdown occurs after the emergency unlock.
  - An emergency unlock condition will return when a lockdown is cleared, if its triggering condition is still active.

Global lockdown can be initiated through the web application, with the button on the top toolbar. It can also be initiated through the mobile application. There is also a button to clear the lockdown, next to it.

In Sub-controller (I/O) properties an auxiliary input can be configured with a Linkage to initiate a lockdown if the input becomes active. This can be used to create a physical lockdown button. Note that if a lockdown is initiated by an input, it can only be cleared using the web or mobile application.

When lockdown is initiated, an Event is generated. There is a default Alarm Trigger which generates an Alarm based on this Event.

If active, the lockdown status of the system is clearly shown at the top of the screen (regardless of what is being viewed) - "**SYSTEM UNDER LOCKDOWN!**", in red. Also, counts of locked down Controllers and Doors are shown in the dashboard statistics on the home screen. Note that when a Controller is in a lockdown state, that really just means all of the Doors on the Controller are in a lockdown state (apart from the exceptions above). Any screens which show Door or Controller status will show this state (Door Status, Maps, etc).

In a system with a Primary and Secondary Controllers, when the Primary Controller initiates lockdown, it also initiates lockdown for all Secondary Controllers, allowing for a total system lockdown.

Individual Doors may be manually put into lockdown mode using Manual Commands. Note that a Door cannot have a default or scheduled mode of lockdown.

Important: As with all emergency functions, lockdown should be tested ahead of time, to ensure that everything is configured and working correctly.

Important: Emergency exit functions are regulated by country- and region-specific fire codes. Please refer to these when designing and configuring your system to ensure compliance.

Related Topics

- Emergency Features
- Emergency Unlock

6.2 Emergency Unlock

Global emergency unlock is a feature to be used in emergency situations to unlock all Doors in the system. Scheduled and manual command Door Mode changes have no effect during the emergency unlock.

There are exceptions:

- Doors with **Exempt From Global Emergency Unlock** checked are not affected.
- Lockdown versus Emergency Unlock
  - An emergency unlock will override a lockdown if the emergency unlock occurs after the lockdown.
  - A lockdown will override an emergency unlock if the lockdown occurs after the emergency unlock.
  - An emergency unlock condition will return when a lockdown is cleared, if its triggering condition is still active.

In the Hardware screen, an auxiliary input must be configured to trigger an emergency unlock of all Doors. These Doors are kept unlocked as long as the input is active.

Global emergency unlock can only be triggered by an auxiliary input. Clearing the emergency is also governed by the input.

When a global emergency unlock is initiated, an Event is generated. There is a default Alarm Trigger which generates an Alarm based on this Event.

Counts of emergency unlocked Controllers and Doors are shown in the dashboard statistics on the Home Screen. Note that when a Controller is in an emergency unlock state, that really just means all of the Doors on the Controller are in an emergency unlock state (apart from the exceptions above). Any screens which show Door or Controller status will show this state (Door Status, Maps, etc).

In a system with a Primary and Secondary Controllers, when the Primary Controller initiates emergency unlock, it also initiates emergency unlock for all Secondary Controllers, allowing for a total system unlock.

Individual Doors may be manually put into emergency unlocked mode using Manual Commands. Note that a Door cannot have a default or scheduled mode of emergency unlocked.

Important: As with all emergency functions, emergency unlock should be tested ahead of time, to ensure that everything is configured and working correctly.

Important: Emergency exit functions are regulated by country- and region-specific fire codes. Please refer to these when designing and configuring your system to ensure compliance. Emergency unlock is intended as a supplement to, but not a replacement for, Doors correctly wired for emergency egress in compliance with fire codes.

Related Topics

- Emergency Features
- Lockdown

6.3 Duress

A Duress PIN is an alternate PIN that a User can enter in place of their normal PIN to discreetly indicate duress during Door access (for example, being threatened by an intruder). Access works as normal from the User's point of view, without any indication that anything is different at the Door. The User is granted or denied access according to the same rules as usual. In the system, however, an additional Event, **Duress**, is recorded under these conditions.

The Duress Event is configured as an Alarm Trigger by default, generating an Alarm.

Furthermore, the duress Event is one of the options that can be used as a Linkage to trigger the activation of an auxiliary output in the Hardware screen.

A **Duress PIN** is configured in the Users screen on a per-user basis.

The **Duress PIN** can be derived from the normal PIN automatically using the **Add 1 to Last Digit** method: For example, a normal PIN of 1111 would then correspond to a duress PIN of 1112, and a normal PIN of 9999 would then correspond to a duress PIN of 9990.

Alternatively, the **Duress PIN** can be explicitly specified.

Note that the **Duress PIN** value must be unique, also with respect to all normal PIN codes, Shared Access Codes, and Emergency Access Codes.

Related Topics

- Emergency Features

6.4 Reports and Printing

Printing from the Web Management Application is available in two situations.

- "Export PDF" Menu Buttons: Some list views include this button on the menu. Wherever this option appears, you can create a report of everything in the currently displayed list.
- Screen buttons with labels such as "Generate" or "Print Card." These buttons appear directly on screens that are devoted to printing special documents.

Printing of reports and other documents is performed via the web browser. In all cases, the application creates a formatted document called a PDF file. Depending on which brand of browser you use, you will have either or both of two options. Both are activated by controls in the browser, not in the Web Management Application.

- Save the file to your computer. You can then view or print the report using a PDF viewer program.
- Open the file immediately, where you can view and print it with the capabilities of the browser.

6.5 Manual Commands

Manual Commands is a menu button that directly commands Doors to unlock or change Door Mode. The button appears on any screen where Doors are listed. The command options are:

Momentary Access	Unlocks the Door momentarily for a single access
Set Door Mode	Changes the Door Mode.

- If **Until canceled or next scheduled change** is checked, the mode will be applied until canceled or until the next scheduled change.
- Otherwise, enter a **Duration**, specifying how long the mode change will last.

Cancel — Cancels a previous manual Door Mode change that was made on this screen

Related Topics

- Door Status
- Maps (Monitoring)
- Doors
- Door Modes

6.6 First Credential Unlock

Door Modes with “First Unlocks” stay locked only until the next valid access by a User with the **Allow First Credential Unlock** option checked (or with the same option on the User's User Group). The Door will then unlock and stay unlocked until the next scheduled mode change (or a mode change from a Manual Command).

First credential unlock is available anywhere where Door Modes are selected.

Once a valid Card and PIN is presented, the Door will change to **Unlocked** mode. This will be visible anywhere the Door status is shown. The mode can be changed later using Manual Commands.

Related Topics

- Doors
- Door Mode Schedules

- Manual Commands
- Door Status

6.7 OSDP Readers

OSDP Readers have 2 important features which require special attention when configuring a system:

- an address ("polling address") which must match between the reader and the controller it is connected to.
- encryption, with a configurable encryption key - which must also match between the reader and the controller it is connected to.

For this configuration, the OSDP Reader Configuration Wizard is available from the Hardware Properties and Reader Status screens.

Address

Each OSDP Reader must have a unique address. When setting up multiple OSDP Readers, which generally default to address 0, the most straightforward process is to get the first reader online at address 0, then change the address to a unique nonzero address. Then repeat with the next reader.

Encryption

By default, the Controller will use the default encryption key to communicate with OSDP readers (the only exception is OSDP readers which do not support encryption at all). Because this key is the same for all OSDP readers manufactured, a unique encryption key should be generated and used for each OSDP reader.

For OSDP Readers in the factory default state, this default encryption key will be used on the reader side as well, and the reader will come online. Once online, the OSDP Reader Configuration Wizard can be used to upload and switch to a new, unique encryption key for the reader.

Before reconfiguring encryption, it is worth reviewing the OSDP Reader manufacturer's instructions on how to perform a factory reset on the reader, in case there are any issues and the reader becomes unreachable due to an encryption key mismatch, etc.

Once an encryption key is transferred to a reader, the default encryption key can no longer be used with that reader, unless the reader is reset to the factory defaults.

OSDP Reader Configuration Wizard

With either of these features (address or encryption), there may be an OSDP Reader which is already itself configured to use a given address or encryption key, and offline, and the Controller simply needs to know the correct value in order to bring it online and communicate with it.

Or, the OSDP Reader is online with a given address or encryption key, and the goal is to switch to a new address or encryption key, updating both the Reader and Controller to use the new value.

To assist with this process, the OSDP Reader Configuration Wizard, shows the current status of the Reader throughout the process. This includes:

- whether the Reader is online or offline
- whether encryption is in use, and if so, whether the default encryption key is in use.

Set Polling Address

Note: some OSDP Readers might not support this operation.

Use this option to change the OSDP address that the reader itself is configured to use. This is *not* the **OSDP/RS-485 Address** the Sub-controller is set to use, though they must ultimately have the same value - see below.

The Reader must be online for this operation, because the new address must be communicated to the reader over the existing address.

After this operation has been performed, the actual OSDP/RS-485 Address in the Hardware Properties must be set to the same new value, and the hardware configuration saved.

After this final change, the OSDP Reader should come back online at the new address.

Upload and Switch to Encryption Key

Use this option to transfer a (new) encryption key to the OSDP Reader, and have the Controller start using it for communications with the Reader.

The Reader must be online for this operation, because the new key must be communicated to the reader.

Upload and Use Encryption Key

Use this option if the OSDP Reader already has an encryption key set up, but is offline because the controller does not have the matching key.

Revert to Default Encryption Key

Use this option if the OSDP Reader has no encryption key loaded in it, but is offline because the controller is attempting to use an encryption key. This may occur when a replacement OSDP Reader is connected in place of a previously connected OSDP Reader, or when the existing OSDP Reader has had a factory reset.

Related Topics

Hardware Properties

Reader Status

6.8 Card Enrollment Points

You can designate readers to use for adding cards to a User without typing in a card number. You might not even know the card number. These are called Card Enrollment Points and are a type of Door. You can also use any card reader at all to create cards for new Users.

Set Up a Card Enrollment Point

You need a Controller with a Configuration that includes "+ Card Enrollment Point". You can do this when you add a Controller, or you can modify an existing Controller. When this is done, one of the Controller's Doors will be an Card Enrollment Point.

Each User may select one Card Enrollment Point to use. Select your choice under Menu: Preferences.

Using a Card Enrollment Point

While on the Users screen,

1. Click "Add" next to the "Cards" box.
2. Click in the "Card Number" field.
3. Swipe the card at the Card Enrollment Point.

Using Any Reader to Enroll

Any card reader in the system can be used to enroll a completely new User, or to find out the number of a card.

1. Swipe the card at any reader.
2. Go to the Events screen.
3. Find the corresponding **Access Denied (Unknown Card Number)** Event. The card number is shown in the User column.
4. Click the card number to create a new User having this card.

If the card is currently assigned to another User, you will get some different Event.

Related Topics

Hardware

Users

6.9 QR Code Credentials

QR Code credentials are a type of credential that can be used with the app, and the LTS QR500 Series Reader. The app is available from Google Play, and the Apple App Store. The LTS QR500 must be properly installed and configured (see below).

To add a QR Code credential:

1. Add a card in User Properties.
2. Select **QR Code** as the **Type**.
3. Enter a **Card Number** that is unique within your system, and that would not conflict with the range of non-QR Code cards being used in your system. The maximum card number value for a QR Code is 65535.
4. Leave **Enabled** checked to ensure the credential is active.
5. Enter any other User properties, and then **Save**. The credential must be saved before it can be shared with a user's app.
6. Click the **Share** icon to obtain the registration code (available as a QR code, which is different from the QR code used for door access), for sharing with the app.

To use a QR Code credential:

1. Within the app, select the credential, if it is not already selected by default.
2. Present the QR code to the LTS QR500 Series Reader
3. If the app is still open and showing the same QR code, but is to be used with (same or another) QR500, tap the option to refresh the QR code. The same exact QR code cannot be used more than once.

QR500 Configuration

The LTS QR500 must be wired as a Wiegand reader to the Sentinel Series Controller where it will be used, according to the wiring instructions for both the Sentinel Series Controller, and the QR500.

Your QR500 comes preconfigured by LTS with the correct settings for Sentinel Series controllers.

If this is not the case, or if there is any question about whether the settings have been changed, then you must ensure that the following settings are correct in the configuration application for the QR500.

The **Wiegand parameter settings** must be configured as follows:

- **Wiegand mode**: **WG66**

- **Output format**: **Positive output**
- **Whether to check: Open**

Other **Wiegand parameter settings** should be left at the defaults.

Above that, in the **QR code parameter settings**, **QR code mode** must be set to **Not encrypted**.

Related Topics

- User Properties

6.10 Anti-Passback

Use anti-passback to prevent or detect Users going through the same Door twice in a row, without either exiting from the Area or waiting for the specified time period. For example, Users can enter through an Area with security screening, but must exit through a different Area.

Anti-passback is intended to prevent someone from "passing back" a credential for another person to use it at the same Door, or to another Door entering the same Area. This is commonly used with turnstiles and other special entry devices. Area-based anti-passback can also help prevent sharing of PINs. However, with a normal Door there is no way to prevent one User from simply holding it open for another.

If an access attempt is made which violates anti-passback rules, this will always create an Event. The User may or may not be denied access depending on the configuration.

There are two methods of anti-passback enforcement.

- Door-based — A Door can be opened by the same credential only once during a set time period.
- Area-based — Area-based anti-passback tracks the location of a User and generates a violation if their credential is used somewhere else. For example, if Door 1 exits Area A and enters Area B, and Door 2 exits Area B and enters Area C, then presenting the same credential at Door 1, then Door 2, then Door 1 again is an anti-passback violation, because the User is known to be in Area C when attempting to use a Door which exits Area A.

Note: Anti-passback does not apply to Shared Access Codes, Emergency Codes or anti-passback exempt Users (see below).

Defining Anti-passback Areas

In the Areas screen, you can define the Areas to use for anti-passback. You can also use the predefined Areas, such as Global Out.

Configuring Anti-passback Doors

In the Doors screen, you can define the entering and exiting Areas and the anti-passback settings.

1. Go to Doors.
2. Under Areas and Anti-passback:
   a. Select the **Entering Area**. This is the Area that the Door enters into
   b. Select the **Existing Area**. This is the Area that the Door exits from.
3. Select the Anti-passback Method:
   a. **Area-Based** — Anti-passback is enforced at this Door using any entry to or exit from the Area. Select an anti-passback mode to grant or deny access.
   b. **Door-Based** — Anti-passback is enforced solely based on access to this Door. Enter the number of minutes the anti-passback status is reset after the User enters the Door.
4. Click **Save**.

Anti-passback Exempt Users

To exclude Users from anti-passback rules, check the **Anti-passback Exempt** box on the Users screen.

Forgiving Anti-passback Violations

The **Forgive** button on the Users screen resets the selected User's anti-passback status. Use this when anti-passback rules are preventing a User's access, and you determine to forgive the violation.

Related Topics

- Users
- Areas
- Doors

6.11 Password Reset

If you lose the passwords for all Users with the Administrator Role, you can apply to LTS for a password reset authorization over the Internet. This is only available if you have previously registered with LTS, so we can confirm your email address.

How to Reset the Admin Password

1. On the login screen, click **Reset Password**.
2. Click the **Request Password Reset** button.
3. If successful you will see the message, "A password reset authorization file has been emailed to...."

When you receive the reply email:

1. Open the mail and save the attachment ("password.reset") to your computer.
2. Return to **Reset Password.**
3. Click the **Upload Authorization File** button.
4. Find and open the emailed file you saved.
5. In the following window, enter and **Submit** a new password for the User, "admin".

Related Topics

- Product Registration

6.12 Factory Reset

Factory Reset is used to reset a Controller to its initial configuration.

Warnings and Important Info:

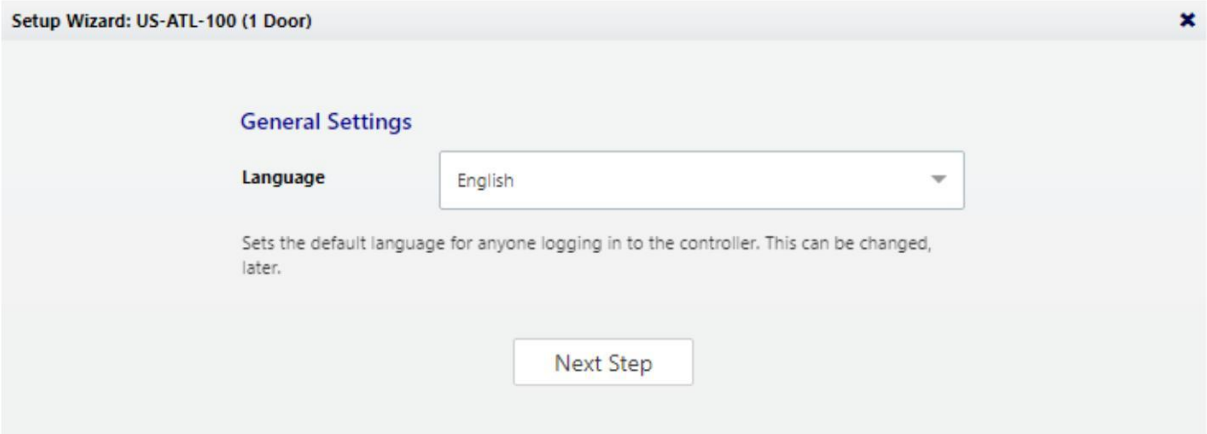
- This operation will erase your database. All existing data and configurations will be erased.
- The admin password will reset to the default, "admin".
- Product Registration information will be lost, although you will still be registered with LTS.
- The Network settings will *not* be reset. If the Controller has a static IP address, it will not change. If it is set for DHCP, it will probably reboot at the same address.
- If an HTTPS certificate has been installed, it will *not* be removed.
- The Date and Time settings will *not* be reset.
- Backups and Archives are *not* deleted.

1. Go to Software Settings and expand the **Factory Reset** section.
2. Click **Factory Reset.**
3. You will be logged out. Wait for the Controller to restart, and then log in.
4. You will be directed to the Setup Wizard, which must be completed.

6.13 Setup Wizard

The Setup Wizard appears when logging in for the first time and after a Factory Reset. It must be completed. However, you may exit at any time and complete it later.

Page 1: Language



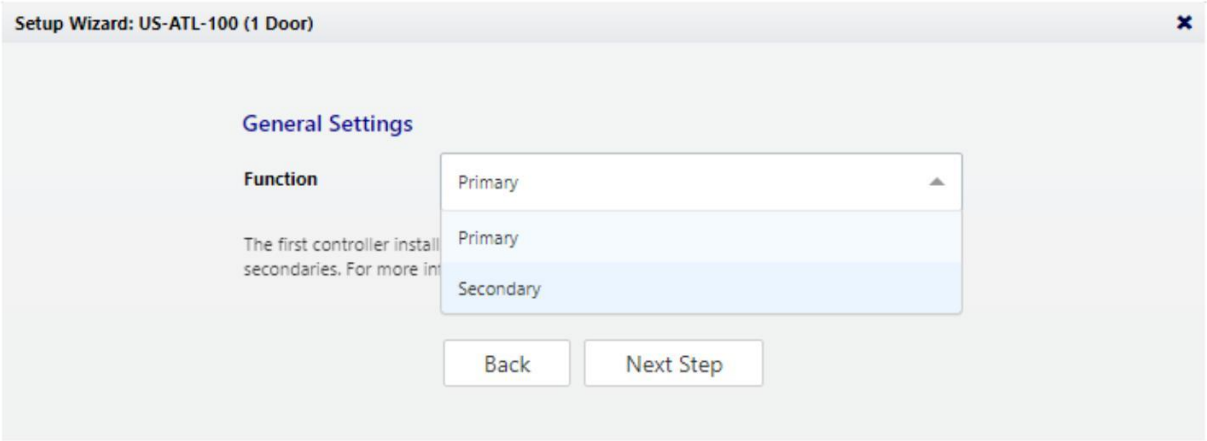
click to enlarge

Choose a language. Your choice will be used for this wizard. If this is a Primary Controller, it will also become the default language of the Web Management Application. If this is a Secondary Controller, it will become the default language of the simplified management application on this Controller.

Available languages depend on your software license. Contact your authorized LTS representative for license upgrades.

This can be changed in the Hardware Properties of the Controller.

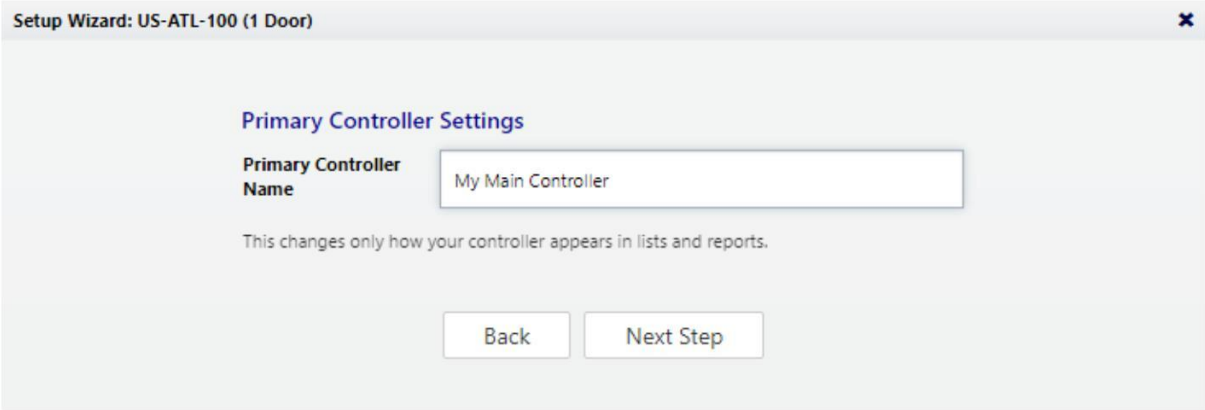
Page 2: Function



click to enlarge

Choose whether this Controller will be a Primary or a Secondary, as discussed at Understanding Controllers and Doors

Page 3: Primary Controller Name (primaries only)

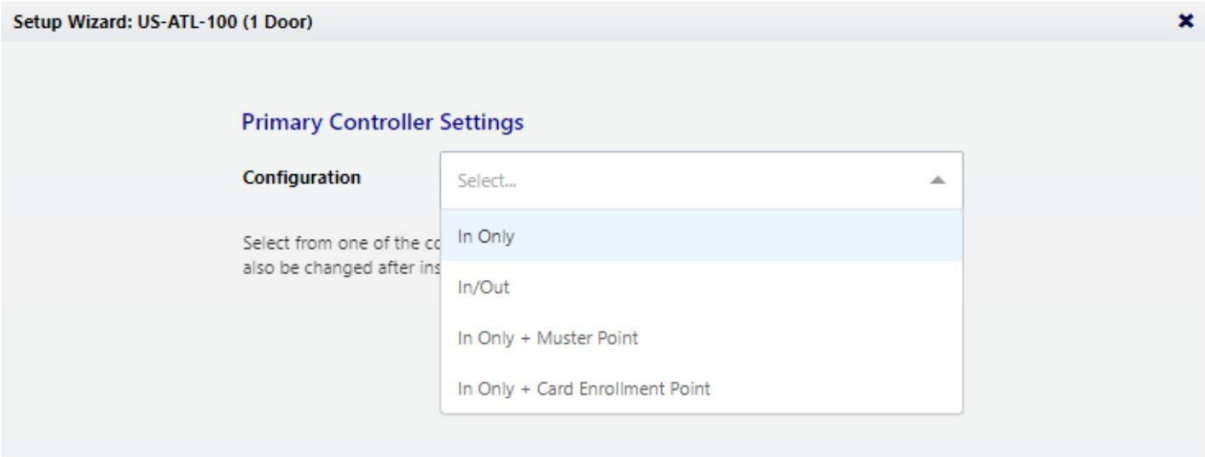


click to enlarge

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)

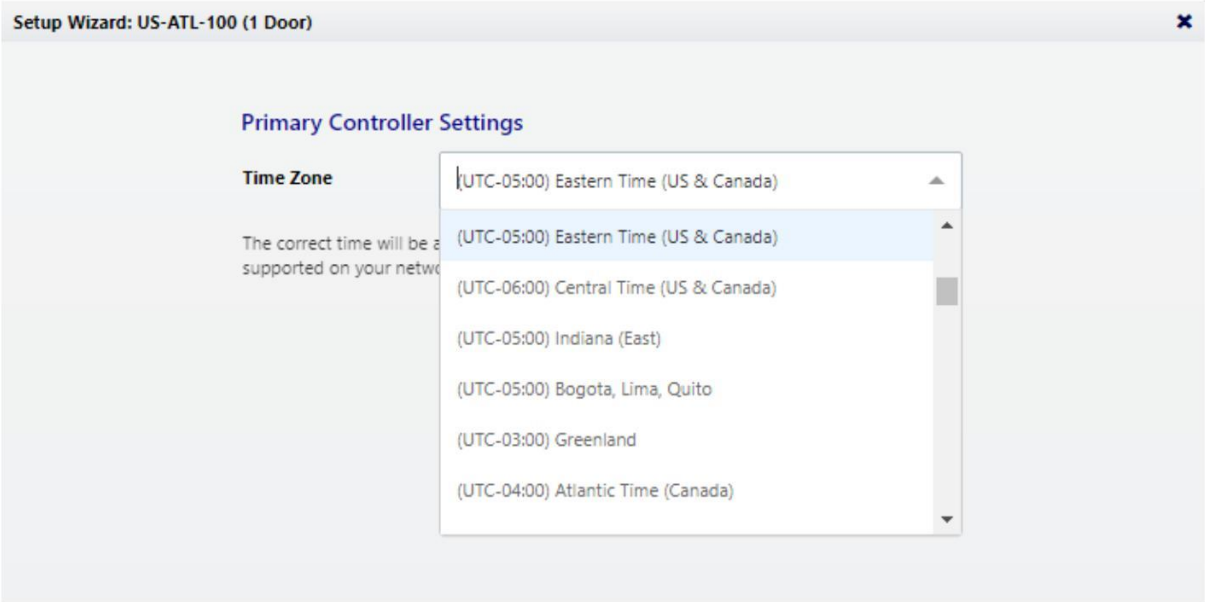


click to enlarge

See Controller Configuration Property.

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

Page 5: Time Zone (primaries only)

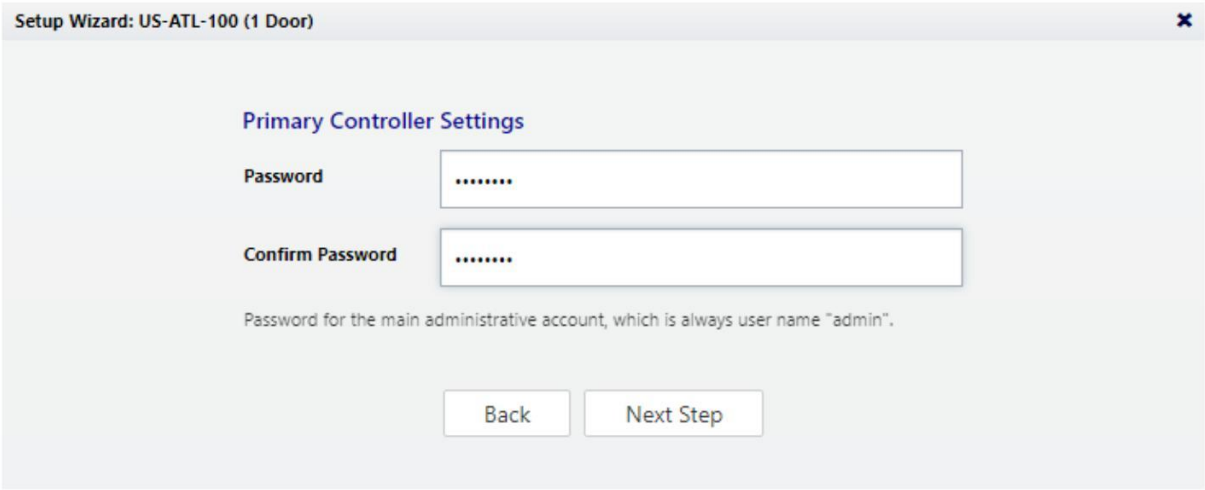


click to enlarge

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. In some cases NTP will not work due to firewalls or network policy. In that case, see Date and Time after completing the wizard.

Note: Secondary Controllers get their time and time zone from the Primary Controller.

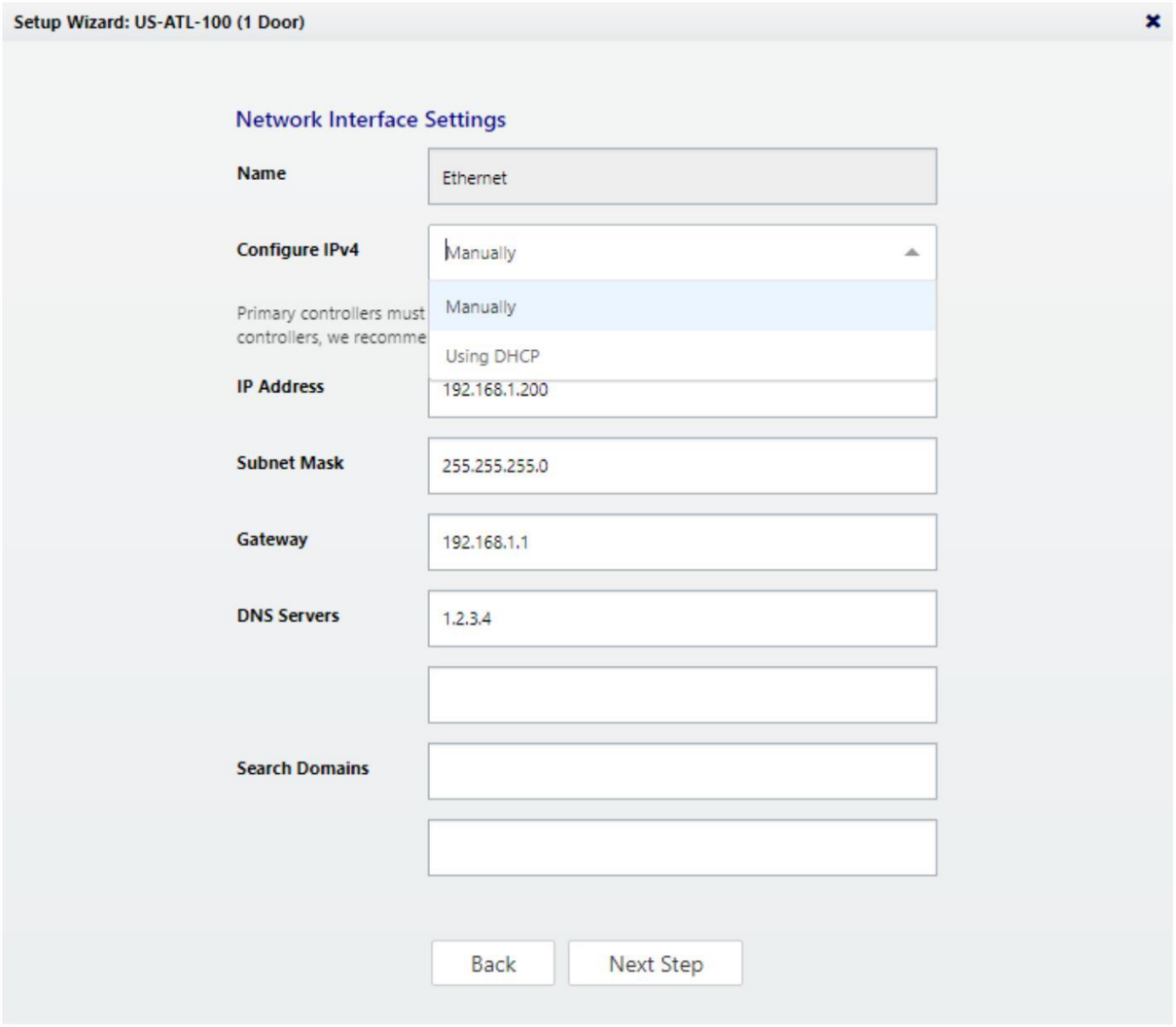
Page 6: Password (primaries only)



click to enlarge

Enter a strong password for the primary administrator account. The username for this account is “admin” and cannot be changed.

Page 7: Network Interface Settings



click to enlarge

If you have just performed a Factory Reset, these settings should already be set to what they were before the reset.

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 all Controllers cannot be located on one network subnet, or if Discovery is blocked by network restrictions. In that case:

- Assign these Controllers static IP addresses.
- Manually add these Secondary Controllers in the Web Management Application instead of using Discovery.

See Network for more information or to make changes later.

Page 8: Review

All your entries are displayed for review. Click either "Back" or "Complete Setup."

Reference

7 Reference

Reference material:

- Glossary
- Event Categories and Types
- Door Modes

7.1 Glossary

Access Level	A set of Door/Schedule pairings defining access to those Doors during the associated Schedules.
Acknowledged	When a User is aware of an Alarm, but nothing has necessarily been done about it
Airlock	A rule applying to multiple Doors in an Area restricting which Doors can be opened at the same time
Alarm	Triggered by an Event, an Alarm is like a copy of the Event which can change state from New to Acknowledged to Resolved, for the purposes of Users being made aware of the issue and keeping track of whether and which ones have been Resolved
Alarm Trigger	Triggers an Alarm from an Event
Anti-passback	A rule preventing or detecting the "passing-back" of a credential from one person to another, using the same credential twice in a row at the same Door or entering into the same Area
Audit	A record of a change made in the system by a User, or of a manual command executed by a User
Battery Monitor	An Input on a Controller configured to detect whether a battery is connected
Biometric	A feature of a person which can be used as a credential for identification or verification purposes, like a fingerprint
Card	A Card is a credential encoded with a number used for electronic access control. These can come in other form factors like a fob. Also known as a "Badge"

Card Design	A graphical design, including image and text elements, some of which come from a User's record, which can be used to print on the surface of a Card. Also known as a "Badge Design"
Card Enrollment Point	A Reader configured not for access control, but rather to obtain the card number for enrollment purposes
Card Format	A technical specification of the format of the data bits encoded onto a Card, including Card Number, Facility Code, Parity. Different vendors supply different Cards encoded using different Card Formats.
Card Number	The portion of the data bits encoded on a Card corresponding to a unique, identifying number.
Controller	A physical electronic device which controls input and output for access-control. Sentinel Series Controllers can be either Primary Controllers or Secondary Controllers.
CSV	Comma Separated Values. A text file format which is able to be imported into or exported from Microsoft Excel and other office spreadsheet programs
DHCP	Dynamic Host Configuration Protocol. A network option where a device obtains its IP Address and other networking settings automatically from a router, gateway, or other network device.
Door	A combination of Reader(s), Input(s), and Output(s) which electronically controls access to a physical door, or something functionally similar to a door, like a parking gate. Also known as an "Access Point", or "Portal"
Door Mode	The mode of operation of a Door, specifying whether the Door is simply unlocked, whether it is locked and unavailable for access, or locked and requiring the presentation of credentials to unlock it. The mode also includes which types of credentials (Card, PIN, Biometric) are required.
Door Mode Schedule	A schedule with a set of time intervals (including days of the week and Special Day types), where each time interval can be associated with a Door Mode. The Door Mode Schedule can be associated with a Door to change the Door Mode automatically, according to the schedule.

Door Sensor	An Input wired to detect whether a Door is opened or closed. Also known as a "Door Contact" or "Door Position Switch".
Door Template	A set of Door properties which can be associated with multiple Doors to re-use common combinations of properties without re-entering them. Also used to change the properties of multiple Doors at once, by simply changing the associated Door Template
Duress PIN	An alternate PIN code which is used to signal a duress condition. Access is granted and denied normally as if the normal PIN was used. When access is granted using a Duress PIN, an Access Granted (Duress) Event is generated, which triggers an Alarm within the software, by default.
Emergency Code	A PIN code to be used by emergency or high-security personnel in an emergency situation to gain access to a Door, regardless of Door Mode (including Lockdown)
Event	A record of an occurrence within the system. Includes hardware and access activity. Also known as a "Transaction"
Exit Button	An Input wired to detect that the Door is being opened, or needs to be unlocked, for exit purposes. Generally located on the insecure side of the Door (the side you face when exiting). May be a button, or may be another kind of device such as a motion sensor. Also known as a "Request to Exit (REX)"
Facility Code	A number encoded onto a Card in addition to Card Number, which is used to identify a facility, customer, or batch of cards. A single company will often order Cards with the same Facility Code. The exact length and location of the Facility Code within the data bits of the card can be specified in Card Formats, and the actual Facility Code value expected can be specified there as well.
Fire Code	Laws and rules in a given country or region which specify how buildings, fire alarm systems, and other electronic systems must be designed, built, configured, and operated for life-safety purposes.
Firmware	Software which runs on an embedded device such as a Controller
Forced Open	A condition where a Door has been physically opened (according to the Door Sensor), but is also still locked. That is, it has been opened

	without any valid access, exit request, manual command, or Door Mode allowing it to be opened.
Hardware Template	A set of Controller properties which can be associated with multiple Controllers to re-use common combinations of properties without re-entering them. Also used to change the properties of multiple Controllers at once, by simply changing the associated Controller Template
Held Open	A condition where a Door was opened, but not closed within a set amount of time
HTTPS	A protocol for communicating between a web browser and a web server which is secured through encryption
In (Door)	A Door configured to enter (In). May be paired with an Out Door, in which case the In Door controls the shared Inputs and Outputs
In/Out	A configuration on a Controller with 2 Doors, one for entry (In), and one for exit (Out). These 2 Doors represent 2 sides of the physical door.
Input	An electronic input on a Controller which can detect a circuit being active or inactive.
IP Address	A numeric address for devices and computers on a network
Linkage	A rule linking Events and conditions to actions or outputs. Also known as a "Policy"
Location	A label indicating a Location name, which can be arranged in a hierarchy, to organize Hardware, Doors, Areas, and Maps.
Lock	An Output on a Controller configured to connect to a physical electronic door lock. Also known as a "Door Strike"
Lockdown	An emergency state for a Door or Controller where the Door (or all Doors associated with the Controller) are locked and deny access to all credentials (with some exceptions). Lockdown is unaffected by scheduled Door Mode changes as well as normal Manual Commands.
Manual Command	A command executed by a User in the web application or mobile app which affects a Door or Controller. Examples include momentarily allowing access to a Door, changing the Door Mode of a Door.

Map	A graphical layout of a facility, often with a floor plan, showing the location of Doors and Controllers, with their status.
Multi-User Access	Rules that require multiple Users from multiple User Groups to access a Door.
Muster	A report showing the last-known access of each User, if that access is not to the Global Out or Muster Areas.
Muster Point	A Door which is used simply to record that a User has reached the Muster Area, for Muster report purposes
Normally Closed (NC)	A type of Input configuration where the normal, "Inactive" condition of the input is where the circuit is open. Inputs which are typically Normally Closed are Door Sensor, Tamper, Power Monitor, Battery Monitor
Normally Open (NO)	A type of Input configuration where the normal, "Inactive" condition of the input is where the circuit is closed. Inputs which are typically Normally Closed are Door Sensor, Tamper, Power Monitor, Battery Monitor
Notification	An in-application copy of certain Events subscribed to by each User. A copy of Notifications can also be configured to be sent via email.
NTP	Network Time Protocol. A protocol for synchronizing time to computers and devices on a network or the Internet. NTP Servers provide reliable, accurate time to devices and computers which subscribe to their services.
OSDP	Open Supervised Device Protocol. A standard protocol for connecting Readers to Controllers using RS-485.
Out (Door)	A Door configured to exit (Out), which is always paired with a Door for entry (In). The In Door is the one controlling the shared Inputs and Outputs.
Output	An electronic output on a Controller which functions as an electronic switch, and can control other devices, like a Lock
Parity	A type of data bit within a Card Format which is used to ensure the integrity of the data read. A parity bit acts as a check on a set of binary values, calculated in such a way that the number of 1s in the

	set plus the parity bit should always be even (or occasionally, should always be odd).
PDF	Portable Document Format. A format used for documents or reports which can be easily viewed or printed on a PC.
PIN	Personal Identification Number. A credential consisting of a numeric code to be entered on a reader's keypad for identification or verification purposes.
Policy	A rule linking Events and conditions to actions or outputs. Also known as a "Linkage"
Power Monitor	An Input on a Controller configured to detect whether the main power is connected
Primary Controller	The Sentinel Series Controller in the system which maintains the entire system configuration, and hosts the web application used to access, configure, and monitor it. A Primary Controller can manage multiple Secondary Controllers.
Reader	Reads cards or credentials, including possibly Card, PIN, or Biometrics.
Resolved	The state of an Alarm which means that it has been fully resolved, that is, it is no longer an issue that needs attention or needs to be visible.
REX	Request to Exit. Another term for Exit Button.
RS-485	A serial communications protocol used for communications between devices, including between Controllers and Readers. OSDP uses the RS-485 protocol, for example.
Schedule	A set of time intervals (including days of the week and Special Day types), used to regulate Door access by time
Secondary Controller	An Sentinel Series Controller which obtains its configuration from a Primary Controller
Shared Access Code	A PIN code shared by a group of people, used gain access to a Door.
SMTP Server	An email server for sending email

Special Day	A day on the calendar (for example a holiday) where normal Door access is to be disallowed by default, unless the Schedule explicitly indicates that Special Days are allowed
Special Day Type	A category or grouping of Special Days.
SSL	Another term for TLS, a networking encryption protocol
Sub-controller	A type of Controller which manages inputs and outputs (I/O) but does not make access or other decisions by itself. In some systems, these Sub-controllers are separate physical devices. In Sentinel Series, they are built-in to the Controllers.
Tamper	An Input on a Controller configured to detect physical tampering with a case, enclosure, etc.
TLS	A networking encryption protocol
User Role	A set of permissions for what a User can and cannot do when logged into the web application or mobile app.
User Group	A classification or grouping of Users used for Multi-User Access.
Wiegand	A standard protocol for connecting Readers to Controllers

7.2 Event Categories and Types

Event Colors:

- Red: Event is also an Alarm Trigger by default. If you create additional alarm triggers, those events will appear red in the Web Management Application. If you remove built-in triggers, those events will appear yellow.
- Yellow: Warnings
- Green: Normal access granted
- White: Informational

System

Card Read (Enrollment)	A Card has been read on an Enrollment Point

Controller Resync	Data resynchronized to a Controller
Controller Startup	Controller started up
Database Backup Copied to USB Drive	Database backup copied to USB drive
Database Backup Copy to USB Drive Failed	Database backup copy to USB drive failed
Database Backed Up	Database backed up
Database Backup Failed	Database backup failed
Software Update Failed	Software update failed
Software Updated	Software updated
Schedule Active	Schedule became active
Schedule Inactive	Schedule became inactive
Signed Out	A User signed out of the application
Successful Sign In	A User signed in successfully to the application
Unsuccessful Sign In	A User unsuccessfully attempted to sign in to the application - generic
Unsuccessful Sign In (Connected Mobile Device Limit Reached)	A User unsuccessfully attempted to sign in to the application - license limit of connected mobile devices reached
Unsuccessful Sign In (Expired)	A User unsuccessfully attempted to sign in to the application - expired
Unsuccessful Sign In (Inactive)	A User unsuccessfully attempted to sign in to the application - inactive login
Unsuccessful Sign In (Inactive User)	A User unsuccessfully attempted to sign in to the application - inactive User
Unsuccessful Sign In (Incorrect Mobile Device)	A User unsuccessfully attempted to sign in to the application - incorrect mobile device was used

Unsuccessful Sign In (Incorrect Password)	A User unsuccessfully attempted to sign in to the application - incorrect password
Unsuccessful Sign In (Mobile Device Expired)	A User unsuccessfully attempted to sign in to the application - Mobile device not authorized - expired
Unsuccessful Sign In (Mobile Device Inactive)	A User unsuccessfully attempted to sign in to the application - Mobile device not authorized
Unsuccessful Sign In (Mobile Device Not Yet Effective)	A User unsuccessfully attempted to sign in to the application - Mobile device not authorized - not yet effective
Unsuccessful Sign In (No Privileges)	A User unsuccessfully attempted to sign in to the application - no User Roles
Unsuccessful Sign In (Not Yet Effective)	A User unsuccessfully attempted to sign in to the application - not yet effective
Unsuccessful Sign In (Outside Schedule)	A User unsuccessfully attempted to sign in to the application - outside schedule
Unsuccessful Sign In (Too Many Denied Attempts)	A User unsuccessfully attempted to sign in to the application - too many denied attempts
Unsuccessful Sign In (Too Many Incorrect Password Attempts)	A User unsuccessfully attempted to sign in to the application - too many incorrect password attempts
Unsuccessful Sign In (Unauthorized Mobile Device)	A User unsuccessfully attempted to sign in to the application - unknown or unauthorized mobile device
Unsuccessful Sign In (User Expired)	A User unsuccessfully attempted to sign in to the application - After Valid To of User
Unsuccessful Sign In (User Not Yet Effective)	A User unsuccessfully attempted to sign in to the application - Before Valid From of User

Access Granted

Access Granted	Generic
Access Granted (Door Already Open)	Door already open

Access Denied

Access Denied	Generic
Access Denied (Airlock Busy)	Airlock rules would be violated by the access (another Door in the Airlock-configured Area is unlocked/open)
Access Denied (Anti-passback)	Anti-passback violation
Access Denied (Bad Biometric Read)	A biometric was presented, but could not be read/processed
Access Denied (Expired)	After Valid To of Card or other credential
Access Denied (Inactive)	Card Inactive
Access Denied (Inactive User)	User is inactive
Access Denied (Incomplete)	Credentials incompletely presented (for example partial PIN digits)
Access Denied (Incorrect Biometric)	Incorrect or invalid biometric presented (one to one biometric verification)
Access Denied (Incorrect Card)	Door Mode requires/allows Card to be presented after PIN or biometric, but the Card does not match that PIN or biometric
Access Denied (Incorrect Confirming PIN)	Door Mode requires confirming PIN, but confirming PIN entered does not match
Access Denied (Incorrect Facility Code)	Card Format recognized, but Facility Code does not match
Access Denied (Lockdown)	Door Mode is Lockdown

Access Denied (No Access)	Door Mode is No Access
Access Denied (No Biometric Access)	Door Mode does not allow biometrics, but biometric presented
Access Denied (No Biometric Defined)	Door Mode requires biometric, but User has no biometric enrolled
Access Denied (No Biometric Presented)	Door Mode requires biometric, but no biometric presented.
Access Denied (No Card Access)	Door Mode does not allow Card, but Card presented
Access Denied (No Card Presented)	Door Mode requires Card, but no Card presented.
Access Denied (No Confirming PIN Defined)	Door Mode requires PIN, but User has no PIN defined
Access Denied (No Multi-User Access Credential Presented)	Multi-Credential rule in effect, but the additional credential(s) were not presented
Access Denied (No PIN Access)	Door Mode does not allow PIN, but PIN presented
Access Denied (No PIN Presented)	Door Mode requires PIN, but no PIN presented
Access Denied (No Privileges)	No matching Access Level or Door/Schedule assignment
Access Denied (Not Yet Effective)	Before Valid From of Card or other credential
Access Denied (Outside Schedule)	Matching Access Level or Door assignment, but Schedule is inactive
Access Denied (QR Code Invalid)	QR Code is not valid
Access Denied (QR Code Needs Refresh)	QR Code needs to be refreshed within the Defendas app before being used again
Access Denied (Unknown Biometric)	Unknown biometric presented in biometric-only mode, or biometric presented first (one to many biometric verification)

Access Denied (Unknown Card Number)	Unknown card number
Access Denied (Unknown Format)	Bit pattern of data bits on card does not match any defined, enabled Card Format
Access Denied (Unknown Unique PIN)	Unknown PIN used for PIN-only or PIN-first access
Access Denied (User Expired)	After Valid To of User
Access Denied (User Not Yet Effective)	Before Valid From of User

Communications

Controller Offline	Controller offline (Secondary Controller, Sub-controller (I/O)
Controller Online	Controller online (Secondary Controller, Sub-controller (I/O)
Reader Offline	Reader offline (OSDP, LTS RS-485)
Reader Online	Reader online (OSDP, LTS RS-485)
Video System Offline	Video System offline. Only applicable if video is licensed.
Video System Online	Video System online. Only applicable if video is licensed.

Door

Controller Access Mode: Lockdown	Lockdown at the Controller level
Controller Access Mode: None	Emergency Unlock or Lockdown at the Controller level cleared
Controller Access Mode: Unlocked (Emergency)	Emergency Unlock at the Controller level
Door Closed	Door closed (according to Door Sensor)

Door Forced Masked	Door Forced Open condition being masked (no indication as to whether the underlying condition is present or not)
Door Forced Open	Door opened while not unlocked
Door Forced Open Restored	Door Forced Open condition not present or no longer present
Door Forced Unmasked	Door Forced Open condition not being masked (condition will be reported if present)
Door Held Masked	Door Held Open condition being masked (no indication as to whether the underlying condition is present or not)
Door Held Open	Door held open too long after being opened
Door Held Open Restored	Door Held Open condition not present or no longer present
Door Held Open Warning	Warning prior to Door held open too long after being opened
Door Held Unmasked	Door Held Open condition not being masked (condition will be reported if present)
Door Mode: Biometric and PIN	Door Mode indication
Door Mode: Biometric and PIN (First Unlocks)	Door Mode indication
Door Mode: Biometric Only	Door Mode indication
Door Mode: Biometric Only (First Unlocks)	Door Mode indication
Door Mode: Biometric or Card or PIN	Door Mode indication
Door Mode: Biometric or Card or PIN (First Unlocks)	Door Mode indication
Door Mode: Biometric or PIN	Door Mode indication
Door Mode: Biometric or PIN (First Unlocks)	Door Mode indication

Door Mode: Card and Biometric	Door Mode indication
Door Mode: Card and Biometric (First Unlocks)	Door Mode indication
Door Mode: Card and Biometric and PIN	Door Mode indication
Door Mode: Card and Biometric and PIN (First Unlocks)	Door Mode indication
Door Mode: Card and PIN	Door Mode indication
Door Mode: Card and PIN (First Unlocks)	Door Mode indication
Door Mode: Card Only	Door Mode indication
Door Mode: Card Only (First Unlocks)	Door Mode indication
Door Mode: Card or Biometric	Door Mode indication
Door Mode: Card or Biometric (First Unlocks)	Door Mode indication
Door Mode: Card or PIN	Door Mode indication
Door Mode: Card or PIN (First Unlocks)	Door Mode indication
Door Mode: Lockdown	Door Mode indication
Door Mode: No Access	Door Mode indication
Door Mode: No Access, No Exit Button	Door Mode indication
Door Mode: PIN Only	Door Mode indication
Door Mode: PIN Only (First Unlocks)	Door Mode indication
Door Mode: Unlocked	Door Mode indication
Door Mode: Unlocked (Emergency)	Door Mode indication
Door Momentarily Unlocked	Momentary Access Manual Command sent from application
Door Momentary Access Denied	Momentary Access Manual Command sent from application - not executed (denied) - generic

Door Momentary Access Denied (Airlock Busy)	Momentary Access Manual Command sent from application - not executed (denied), because it would violate Airlock rules (another Door in the Airlock-configured Area is unlocked/open)
Door Monitored Open	Monitor Open Only Door: open while monitored
Door Monitored Open Masked	Monitor Open Only Door: Door Monitored Open condition being masked (no indication as to whether the underlying condition is present or not)
Door Monitored Open Unmasked	Monitor Open Only Door: Door Monitored Open condition not being masked (condition will be reported if present)
Door Not Monitored Open	Monitor Open Only Door: closed while monitored (or no longer being monitored)
Door Opened	Door opened (according to Door Sensor)
Duress	Duress (Duress PIN was entered)
Emergency Code Presented	Emergency Code Presented
Exit Request Denied	Exit Button active, but exit access not triggered - generic
Exit Request Denied (Airlock Busy)	Exit Button active, but exit access not triggered, because it would violate Airlock rules (another Door in the Airlock-configured Area is unlocked/open)
Exit Requested	Exit Button active, triggering exit access
Exit Requested (Door Already Open)	Exit Button active, triggering exit access - Door is already open
Door Momentarily Unlocked (Door Already Open)	Momentary Access Manual Command sent from application - Door is already open
Global Access Mode: Lockdown	Lockdown at the Global level

Global Access Mode: None	Emergency Unlock or Lockdown at the Global level cleared
Global Access Mode: Unlocked (Emergency)	Emergency Unlock at the Global level

Input/Output

Input Active	Input inactive
Input Inactive	Output inactive
Output Active	Output active
Output Inactive	Output inactive

Tamper/Power

Battery Failure	Battery Monitor Input is active
Battery Restored	Battery Monitor Input is inactive
Off Main Power	Power Monitor Input is active
On Main Power	Power Monitor Input is inactive
Tamper	Tamper Input is active
Tamper Restored	Tamper Input is inactive

7.3 Door Modes

The Door Mode determines whether or not the Door in an unchanging state (Unlocked, Unlocked (Emergency), No Access, Lockdown), or in an access-controlled state, requiring credential presentation for access. When credentials are required, the Door Mode also determines which types of credentials are required.

When the Door Mode is initially set for a Door, or it changes, a corresponding Event is generated (See: Event Categories and Types). For example, if the Door Mode becomes **Card Only**, an Event will be generated: **Door Mode: Card Only**.

The default Door Mode for a Door is set in the Doors screen.

Door Mode Schedules can be used to automatically change Door Modes according to a schedule.

Manual Commands can be used to set the Door Mode.

The Door Mode is also shown in Door Status and anywhere the status of a Door is shown (Doors, Maps).

Most access-controlled Door Modes have a **(First Unlocks)** variant. See First Credential Unlock for details.

The following is a list of all Door Modes for a Door:

Unlocked

Unlocked (Emergency)

No Access

Lockdown

No Access, No Exit Button

Card Only

Card Only (First Unlocks)

Card and PIN

Card and PIN (First Unlocks)

PIN Only

Pin Only (First Unlocks)

Card or PIN

Card or PIN (First Unlocks)

Card and Biometric

Card and Biometric (First Unlocks)

Card and Biometric and PIN

Card and Biometric and PIN (First Unlocks)

Biometric Only

Biometric Only (First Unlocks)

Biometric and PIN

Biometric and PIN (First Unlocks)

Biometric or PIN

Biometric or PIN (First Unlocks)

Card or Biometric

Card or Biometric (First Unlocks)

Biometric or Card or PIN

Biometric or Card or PIN (First Unlocks)

Note that a Controller can be placed in a special Door Mode during global Lockdown and Emergency Unlock. The Events generated for this at the global level are:

- **Global Access Mode: Unlocked (Emergency)**
- **Global Access Mode: Lockdown**
- **Global Access Mode: None**

The Events generated for this at the (secondary) Controller level are:

- **Controller Access Mode: Unlocked (Emergency)**
- **Controller Access Mode: Lockdown**
- **Controller Access Mode: None**

Related Topics

- Doors
- Door Mode Schedules
- Manual Commands
- First Credential Unlock

- Lockdown
- Emergency Unlock
- Events
- Event Categories and Types