Embedded Web Server

User Guide

General usage guide lines to the ISONAS Embedded Web Server available on all ISONAS PowerNet™ reader-controllers

06/12/09
Contents
Revision history .................................................................................................................. 4
Scope .................................................................................................................................. 4
Introduction .......................................................................................................................... 4
  Supported Version .............................................................................................................. 5
  Connecting .......................................................................................................................... 5
Format of Pages .................................................................................................................... 5
  Standard Layout .................................................................................................................. 5
    Title Banner ...................................................................................................................... 6
    Time and Version Banner ................................................................................................. 6
    Menu bar for Navigation ................................................................................................... 6
Introduction to usage ............................................................................................................. 7
Login Page ............................................................................................................................. 7
Basic options ......................................................................................................................... 8
  LAN Page ............................................................................................................................ 9
Password Page ....................................................................................................................... 11
Set Time Page ....................................................................................................................... 11
User options .......................................................................................................................... 12
  Badges ................................................................................................................................. 13
  Time Zones .......................................................................................................................... 15
  Holidays ............................................................................................................................... 17
  Stored Events ..................................................................................................................... 18
Advanced options ................................................................................................................ 19
  Operations ............................................................................................................................ 20
Special ................................................................................................................................... 21
Keypad ................................................................................................................................... 22
Test Unit ............................................................................................................................... 24
Additional Pages ................................................................................................................... 25
  Timeout ................................................................................................................................. 25
  Logoff .................................................................................................................................. 25
Scope
Welcome to the ISONAS reader-controller-controller’s Embedded Web Server. The Embedded Web Server is designed to make it easy to configure many of popular ISONAS PowerNet™ reader-controller settings.

There are multiple ways to configure the ISONAS reader-controller, including via the Crystal Matrix™ Access Control Software System, or one of the utility programs such as Reader-controller, Plug And Play, or CTEST and now this; the Embedded Web Server.

All of methods of configuring the PowerNet™ reader-controller are compatible with one another, which allow the installer or administrator to use any one that he/she is comfortable with to achieve the same results. This document discusses only the Embedded Web Server.

Introduction
The Embedded Web Server is comprised of a group of web based pages that are stored on the reader-controller itself, allowing the set up and configuration of many of the PowerNet™ settings without the need for any other ISONAS products. Simply launch a web browser and connect to the reader-controller.

Note: These pages were specifically written and tested against Microsoft’s Internet Explorer 7 and Fire Fox 3.0; other compatible browsers may also work.

The two primary targets for use of the Embedded Web Server are:
1. During installation
2. For usage in a standalone system

1. **Installation** – During the install phase of the ISONAS reader-controllers it is very convenient to be able to configure the reader-controller without having to install any other software at the installation site. The Embedded Web Server is uniquely qualified for exactly this usage because the installer can use a web browser to connect to the reader-controller and then perform the configuration steps.
2. **Standalone systems** – A standalone system utilizing the ISONAS reader-controller can be any number of reader-controllers but will typically be ten (10) or fewer. For example, assume a small company that installs just 2 reader-controllers at their facility, one on the front door and another on the back door. Using the Embedded Web Server the user will be able to connect to each of the reader-controllers to configure and set up for their daily operations. The user will not need any other software and will only need to master a very small number of functions. The user will be able to add and delete credentials from the reader-controller, set up automatic unlock events and retrieve the history that is stored on the reader-controller. The Embedded Web Server provides a very easy and simplified way to set up and utilize the ISONAS access control system in a fully functional access control setting.

**Supported Version**

The Embedded Web Server is available on ISONAS reader-controllers with the ISONAS Freescale version 10.59 or higher. Any ISONAS PowerNet™ reader-controllers can be upgraded to have the Embedded Web Server. Contact the ISONAS Technical Support group at (303) 567-6516 for upgrade process information.

**Connecting**

Launch a supported browser, type in the address [http://address](http://address) where *address* is the IP address of the reader-controller to be connected with. Assuming the reader-controller’s firmware is up to date a Login screen will appear.

Note: If the reader-controller is currently connected to another product (ISONAS Crystal Matrix™ for example) it must be disconnected prior to accessing the Web Pages. In other words, only one product may connect to the reader-controller at anytime.

The factory IP address of the reader-controller is printed on the back label. Use this address to connect to the reader-controller from the browser unless it has been changed. If the address of the reader-controller is not known use one of the ISONAS supplied products such as the Plug N Play to search the network and locate the correct IP address. The reset button on the back of the reader-controller can also be pressed and held for 5 seconds to reset the reader-controller to its factory defaults (the reader-controller must be powered on during this process). The factory default IP address will reset automatically to 192.168.1.27.

Note: Pressing the reset to factory defaults button will reset the reader-controller’s internal settings for the IP address, subnet mask, connection port and the two passwords for Admin and User.

**Format of Pages**

There are multiple pages available through the Embedded Web Server and each page supports specific options; however, every page has the same basic layout which is described here.

**Standard Layout**

Every functional page has the following header which consists of a Title Banner, Time and Version Banner and a Menu Bar.
Title Banner

Section 1 is a blue banner at the top of every page which displays the type of reader-controller currently connected.

Time and Version Banner

Section 2 has two times displays; Reader Time and Time Remaining.

Reader Time is the actual time that is currently set on the reader-controller itself. If this time does not match the local time, it can be re-set using the Set Time page described later in this document.

Time remaining is the amount of time that the current session has left before it expires and automatically disconnects the reader-controller. This time resets back to 1 minute and 50 seconds every time a function is performed. If the session timer expires and logs off, the user will need to re-login.

In the Time and Version Banner there are also 3 fields labeled PIC, Freescale and Web. Each of these fields represents the version number of the 3 types of software that are currently loaded on the reader-controller. These fields are important information should technical support be required.

Menu bar for Navigation

Section 3 is the menu bar that will display all of the options the user is authorized to access. There are 3 dropdown boxes labeled Basic, User and Advanced. Each of these dropdown boxes has a page that can be accessed by clicking on the option.

There is also a log out button in the menu bar that can be clicked from any page to log off from the reader-controller.

Note: If you ever see the prompt

![The page at http://192.168.0.74 says:](image)

you must click the OK button and then resubmit the last command. This will occur on occasions where the reader is temporarily too busy to handle your request.
Introduction to usage

The basic layout of the Embedded Web Server is by feature usage. Functions have been group under Basic, User and Advanced which correspond with the dropdown boxes available on the menu bar. Each of these functional areas is described below.

For this section of the document it will be useful to set up a fictional reader-controller that has an initial IP address of 192.168.1.167. The session begins when the user accesses the reader-controller via a Microsoft Internet Explorer or Firefox browser and typing the IP address in to the address bar.

If the reader-controller is accessible and has the right version of software loaded onto it, the login page will be displayed.

Login Page

The login page will automatically appear every time a reader-controller is successfully connected. A valid user name and password, both of which are case sensitive are entered. The appearance of the page presented for the login is somewhat dependent upon the browser utilized so it may not look exactly like the one depicted below. The login form however will always have a user name and password.

The reader-controllers support just two levels of users that can login; these are Admin and User accounts. The Admin account will have access to all of the available functions whereas the User account will be limited. Either of the account passwords can be changed through this browser interface which will be described later on in this document.

Note: The passwords can be reset back to their defaults by pressing and holding the reset button on the back of the reader-controller for 5 seconds while it is powered on.

The default user name for the Admin user is “Admin” and the default password for this account is “Admin00”

The default user name for the account known as User is “User” and the default password is “User2009”.
The following table displays all of the menu groups available, the options within each menu group and the level of login required (Admin or User) to access the option.

<table>
<thead>
<tr>
<th>Menu Group</th>
<th>Level</th>
<th>Option Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td></td>
<td>LAN Admin Basic network setup, IP address, Subnet mask, etc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Password Admin Change the password to Admin or User</td>
</tr>
<tr>
<td></td>
<td>Admin</td>
<td>Set Time Admin Set the clock on the reader-controller to PC’s time</td>
</tr>
<tr>
<td></td>
<td>User</td>
<td>Badges User Manage the authorized badges on the reader-controller</td>
</tr>
<tr>
<td></td>
<td>User</td>
<td>Time Zones User Manage the authorized Time Zones on the reader-controller</td>
</tr>
<tr>
<td></td>
<td>User</td>
<td>Holidays User Manage the authorized Holidays on the reader-controller</td>
</tr>
<tr>
<td></td>
<td>User</td>
<td>Store Events User View and/or delete the stored events (history) on the reader-controller</td>
</tr>
<tr>
<td>Advanced</td>
<td>Admin</td>
<td>Operations Admin Review or change the reader-controllers latch interval, alarms, etc.</td>
</tr>
<tr>
<td></td>
<td>Admin</td>
<td>Special Admin Review or change the special badges used to toggle the reader-controller in and out of the special modes like Add, Void, etc.</td>
</tr>
<tr>
<td></td>
<td>Admin</td>
<td>Key Pad Admin Review or change the way key pad (if equipped) functions</td>
</tr>
<tr>
<td></td>
<td>Admin</td>
<td>Test Unit Admin Perform some simple test on the reader-controller</td>
</tr>
</tbody>
</table>

**Basic options**
Under this set of options are settings that typically are used to set up the reader-controller at its location and then seldom need to be accessed again.
The LAN page allows the input of typical IP address settings that are required to successfully put an ISONAS reader-controller on the network. These settings are all critical and should not be changed unless the user is familiar with how they will affect the ability to access the reader-controller over the network.

It should further be noted that if the reader-controller will be utilized only in standalone mode and there are no immediate plans to install the Crystal Matrix™ software, then the only field of interest on this page is the IP address, and it is only of interest if the reader-controller cannot connect via the web browser.

MAC Id cannot be changed, this is a unique number assigned to this reader-controller by the factory.

DHCP allows the user to configure the reader to use Dynamic Host Configuration Protocol (DHCP) to obtain its IP address rather than specifying a static IP address. When DHCP is enabled, the fields IP Address, Subnet Mask and Gateway are disabled. If you switch your reader to use DHCP and click the Save button, you will be prompted about the likely consequences; which are: the reader will reboot and then make a request from your DHCP server for an IP address, if one is returned then that will become your reader’s new IP address. If the reader does not get a response from the DHCP request, it will revert back to the default address from the factory. If you switch to DHCP then you will need to find out what address has been assigned to your reader in order to connect again. You can find the reader’s DHCP...
assigned IP address by using the ISONAS PlugNplay program or you can ask your system administrator to find the address within your systems DHCP server.

**IP Address** is the current IP address assigned to this reader-controller. It may be changed to any valid IP address. If the IP address of the reader is changed to one that is not accessible by the attached PC, then immediately upon saving the change the reader-controller will be disconnected and it will not be possible to re-login using the web browser. If this happens please refer to the Trouble Shooting guide for resolution.

**Connect Port** is the current port number that is required for other products to directly connect to the reader-controller. For example, the Crystal Matrix™ application uses a combination of the IP address and this Connect port to control the reader-controller. This port assignment has no affect on connections established through the web browser and this port number should not be changed unless there is a compelling need to do so; such as, the default port that ISONAS used is blocked by your internal router.

**Subnet Mask** is the standard subnet mask required for all IP devices and the meaning and values of the subnet mask are beyond the scope of this document. The default setting is 255.255.0.0 and is set up to allow a wide range of accessibility from any point on most networks.

**Gateway** is an IP address that is an advanced feature typically set up on network devices that are located on a network but are accessed through a Gateway device. If a hardware gateway is utilized the IP address of the Gateway device is automatically populated into the supplied field.

**ACS DSN Name or IP Address** is a field that is only used if you have DHCP enabled and you are running the Crystal Matrix program. When DHCP is enabled the reader will attempt to notify the Crystal Matrix software about the DHCP assigned IP address to the reader, this is crucial in order for Crystal Matrix to maintain communications to the reader. This field can have 1 of 4 values, which are:

- **The text string SrvrAcs** which is the default DNS name that ISONAS uses to locate the Crystal Matrix program. **IF** you have a DNS server on your network and you have defined a name SrvrAcs with an IP address that the Crystal Matrix program is running on, then the reader will use that DNS name to connect with the Crystal Matrix program and send it the new IP address of the reader.

- **Any name** that you configured within your DNS server with the correct IP address of where Crystal Matrix is running.

- **The direct IP address** of the machine running Crystal Matrix.

- **Leave it blank** which means the reader will not make any attempt to find the Crystal Matrix software.
Save button will save any changes to the reader-controller AND will cause the reader-controller to reboot. While the reader-controller is rebooting the Redirect Page will be presented (described later in this document) and the user will be required to login again.

**Password Page**

![Password Page Screenshot](https://www.isonas.com)

This page allows the password settings for the two accounts Admin and User to be changed. The account to be changed is selected from the dropdown box and the new password is input and confirmed. Once all 3 fields have been filled in the Change Password button must be clicked to send the information to the reader-controller.

- **Username** is either Admin or User; one must be selected.
- **Password** is the new password of the account to be changed.
- **Confirm Password** must match the value placed in Password.

**Set Time Page**

![Set Time Page Screenshot](https://www.isonas.com)

Every ISONAS reader-controller has an internal clock set at the factory which may or may not match the local time. The Set Time page allows the reader-controller time to be set to that of the connected PC.
Current Time is the time currently set on the local PC. If this time does not match the Reader-controller Time in the header; use this page to correct that discrepancy. Since the value displayed in Current Time comes directly from the clock setting of the PC this field cannot be changed.

Seconds offset is an optional number of seconds that are added to the Current Time and sent to the reader-controller. This is sometimes necessary to get the reader-controller and the PC time exactly synchronized. The suggested manner of using this page is as follows:

1. Do not fill in the Seconds offset, click the Set Time button.
2. Note the difference between the Current Time and the Reader-controller Time in the header.
3. Do not fill in the Seconds offset yet, click the Set Time button a second time.
4. Note the difference between the Current Time and the Reader-controller Time in the header again.
5. Fill in the Seconds offset field with the average number of seconds noted in steps 2 and 4; it will typically be in the range of 2 to 8 seconds.
6. Click the Set Time button. The Current Time and Reader-controller Time should now be very close to one another, they do not need to be exact.

User options

At the heart of any access control system there are 3 main objectives, who, when and where. This translates to what badge holder is allowed in during specific hours and what doors they are allowed to open. The ‘who’ in this system is the ‘badges’, the ‘when’ is the ‘time zones’ and the “where” is the reader-controller that is being configuring. Badges, Cards, Credentials are all used synonymously when talking about access control systems.

PIN codes are also a form of credential for an access control system. PIN codes are typically manually input by a user on the available keypad and PIN codes and badges are treated exactly the same way by the reader-controller. If the reader-controller has a keypad, then PIN codes are assigned using this badge screen as they will behave exactly the same way as a badge. It is NOT a good practice to use a badge number as a PIN code because badge numbers are often printed on the credential which makes it easily accessible to any observer.
Badges

The Badges screen is designed to allow the administrator to Add, Change or Delete a badge from a door. If a badge is deleted from the door then it is not possible for that badge to open the door, it will be rejected anytime it is presented to the reader-controller.

Although this section of the document is dedicated to badges, it is impossible to talk about them without talking about Time Zones at the same time. Please consult the Time Zones section of this document before continuing.

When a badge is added to a door, that badge will only open the door during the Time Zone selected. A badge can be added to multiple Time Zones.

Some examples here should help clarify the relationship between a Badge, Time Zone and the door’s access.

If badge number 1010 belongs to the business owner and he/she needs access through the door at all times, then that badge is added to the door and the predefined time zone ‘Always’ is selected.

If badge 2001 belongs to an employee that needs to have access through the door Monday – Friday between the hours 8 am and 5 Pm, then that badge is added to the door and the predefined time zone ‘Business Hours’ is selected.
If badge 3001 that belongs to the cleaning crew they are required to have access through the door on Saturdays between the hours of 3 pm through 6 pm, then the administrator must first set up one of the user defined Time Zones with the Saturday flag selected and the hours 15:00:00 through 16:00:00 filled in. For the sake of this example let’s say the Time Zone is set up using the user defined zone named User3, then badge 3001 is added and the user defined Time Zone User3 is selected.

In the last example someone with badge number 4001 and needs to have access through the door during the normal business hours and during the cleaning crew hours that were previously defined. In this case badge number 4001 is added to the door and both the Business Hours and the user defined User3 Time Zones.

**Action** defines an operation performed against a specified badge. A new badge can have Add, Delete applied or Change can be applied to an existing badge. When an existing badge is changed, the badge number cannot be changed. To effectively change a badge number, first Delete it and then Add a new one with the correct number.

**Badge** is only active when the Action is set to Add, then a badge number may be typed in. The badge number must be a positive numeric value.

**Time Zone** indicates the times that the badge is allowed access through the door. Multiple Time Zones may be selected. If the All option is selected then all of the Time Zones will be selected. If then None option is selected then all of the Time Zones will be deselected.

**Note:** If a badge is added and no Time Zones are selected, then the badge will be accepted but it will not be authorized through the door at any time.

**Note:** If a badge is added to a Time Zone that has not yet been configured, the badge will be accepted but it will not be authorized through the door at any time; however, if at a later time the Time Zone is configured then the badge will be authorized through the door at the configured times.

**Origin** is a setting that instructs the reader-controller ‘how’ to accept the number. The choices are PROX, PIN or All. If PROX is selected, then the number is only accepted when it is presented to the reader-controller from a valid physical card. If PIN is selected, then the number is only accepted if it is manually typed in on the reader-controller’s keypad. If both PROX and PIN are selected, then the number is accepted from either a card or keypad entry.

Search button will search the reader for the badge ID entered in the search field and then display the page with the badge if it is found. If the badge is not found, then the current page is redisplayed.

**Note:** The located badge may not be the top one on the list, is will be somewhere on the page.

Previous page and Next page buttons allow the administrator to page back and forth through the configured badges already store on the reader-controller. If there are less badges remaining to be displayed than the page can hold, then the remaining slots will be left blank and they can used to Add new badges.
Clear Page button will clear the information on the page ONLY, it will NOT affect any of the information already stored on the reader-controller. This button can be used to clear all the slots and allow the ability to Add multiple badges at one time.

Process badges button will process the information contained on the page. If the Add action is selected on a slot, then that badge will be added. If the action is set to Delete or Change, then the card will be deleted or changed.

Delete all button will delete all of the stored badges from the reader after prompting the user to confirm the action.

It is recommended that the Badges worksheet located at the end of this document be used to keep track of the badges and PIN codes that are stored on the reader-controller.

Time Zones

A Time Zone defines the days of a week and the hours within those days that the door can be:

- unlocked with a valid credential (badge or PIN code)
- will automatically unlock if configured to do so

As each Time Zone is displayed on the page, the title ‘Time Zone: name’ refreshes with the correct name of the Time Zone, these names cannot be changed. There are 7 Time Zones available through the
Embedded Web Server and they are numbered 1 – 7. The names of the Time Zones are Always, Business Hours, User1, User2, User3, User4 and User5 and they cannot be changed.

The Time Zones ‘Always’ and ‘Business Hours’ are strongly suggested to be set up as follows:

- The Always time zone should be configured so that a badge that is assigned to this time zone will be allowed access through the door 24 hours per day, 7 days per week including holidays.
- The Business hours time zone should be configured so that a badge that is assigned to this time zone will be allowed access through the door Monday – Friday during the hours 8 AM until 5 PM on or whatever your normal business hours are.

**Start time** is the starting hour of the Time Zone (format is 24 hours).

**End time** is the ending hour of the Time Zone (format is 24 hours).

**Day** is a flag that lets the reader-controller know whether the Time Zone is valid on that day at all. If the flag is not set, then despite any times being entered in the start or end time, the Time Zone will NOT be valid on that day.

**Normal** or **Holiday** flag lets the reader-controller know whether or not the Time Zone is valid on Normal (non holidays), Holidays only or both. Normal or Holiday must be selected. The possible selection of the Normal and Holiday flags are:

- Normal ON, Holiday OFF: the Time Zone will be valid on normal days (non holiday) but will not be valid on Holidays as they are defined on the Holiday page.
- Normal ON, Holiday ON: the Time Zone will be valid on all days.
- Normal OFF, Holiday ON: the Time Zone will only be active on Holidays as they are defined on the Holiday page.

**Auto Unlock**, **Badge Unlock** or **No Unlock** flag is an advanced but useful feature of the reader-controller. This flag can instruct the reader-controller to either automatically unlock during the specified times OR unlock during the specified times IF a valid badge is presented. Some examples are called for here.

If it is desired that the door be unlocked during the hours 9 am through 3 pm Monday – Friday on Normal days only, the selections would be:

- Day flags Mon – Fri
- Fill in the times for those days to be 09:00:00 through 15:00:00
- Select the Normal option
- Select the Auto Unlock

The above settings would result in the door automatically unlocking during the specified times. There are cases where this is acceptable such as common bathrooms shared in an office complex; however in many cases having the door automatically unlock even if no one is present is not acceptable. In these cases the Badge Unlock option is highly desirable. The Badge Unlock is essentially the same as the
Automatic Unlock but the door will not go into the unlock state until at least one valid badge is presented.

Fill Times radio button has two options, Always and Business Hours. These options can be used as a shortcut to fill all the times and days. If you click on Always, then the screen will pre-fill with a start time of 00:00:00, end time of 23:59:59 for 7 days per week. If you click Business Hours then the screen will pre-fill with a start time of 08:00:00, end time of 17:00:00 for the days Monday through Friday. Note, after clicking one of these two options you must still click the “Same Time Zone” button to update the reader.

Previous and Next page buttons allow displaying of either the previous or next Time Zone.

Save Time Zone will save the settings onto the reader-controller.

Clear Time Zone will change all the Start and End times to 00:00:00, remove all the Day flags, set the No Unlock option and then save that Time Zone onto the reader-controller.

It is recommended that the Time Zone worksheet located at the end of this document be used to keep track of the user defined Time Zones that are set up.

Holidays

The Holidays page is used to set up to 10 holiday dates on the reader-controller. These dates are used in conjunction with Time Zones that have the Holiday flag set.

Here’s how it works:
Only the Normal flag is set on the Time Zone:
When the credential is entered, the reader-controller will make sure that the current date DOES NOT match one of the dates set in the Holiday list. If it does, then the credential will be rejected.

Only the Holiday flag is set on the Time Zone:
When the credential is entered, the reader-controller will make sure that the current date matches one of the dates set in the Holiday list. If does NOT, then the credential will be rejected.

Both Normal and Holiday flags are set on the Time Zone:
With this configuration, the reader-controller will not check the Holiday list when a credential is presented.

All or none of the Holidays can be filled in and then selected with the Process Dates button. Whatever appears on the page at the time the Process Dates button press is pressed will be sent to the reader-controller. If it is necessary to delete a date, it is cleared on the page and confirmed when Process Dates is pressed. To change one of the dates, simply type over the existing value and click Process Dates.

Holiday 1 – 10: Valid dates in the format mm/dd/yy.

Stored Events

As any action takes place on the reader-controller, such as a card being read, the reader-controller stores this information internally and then it becomes a Stored Event. The reader-controller has the ability save up to 5000 of these stored events and you use the Stored Events page to look at or clear them from the reader-controller.

Date is the date that the event took place. The events are displayed in reverse chronological order (newest to oldest).

Time is the time that the event took place. The events are displayed in reverse chronological order (newest to oldest).
Action is a text field which describes the event being displayed.

- **REX**: a button attached to the REX leads was pressed
- **AUX**: a button attached to the AUX leads was pressed
- **Auto Unlock (start)**: an auto unlock Time Zone activated
- **Auto Unlock (end)**: an auto unlock Time Zone ended
- **Accept**: either a badge or keypad entry was accepted
- **Reject**: either a badge or keypad entry was rejected
- **Reject (no time zone)**: the badge or keypad entry was rejected because it is not assigned to a Time Zone
- **Reject (lock down)**: the badge or keypad entry was rejected because the reader-controller is currently in Lock Down mode.
- **Tamper**: the optical sensor on the reader-controller detected that the reader-controller has been removed from the surface it was attached to.

Credential has several meanings depending on the Action displayed:

- If the action is an Accept or Reject, then the Credential will display the number entered either through a badge read or keypad.
- If the Action is a REX or AUX, then the Credential will display the card value associated with these two actions.
- If the Action is anything else then the Credential will be empty.

Origin is PROX, PIN or blank depending on the Action. If the Action is one of the credential read events then the Origin will display if the credential was a badge or entered manually through the keypad.

Next and Previous page buttons allow paging forward and backwards through the stored events.

Clear events button will delete all of the stored events on the reader-controller after prompting the user to confirm the action.

Advanced options

<table>
<thead>
<tr>
<th>Advanced</th>
<th>Operations</th>
<th>Special</th>
<th>Key Pad</th>
<th>Test Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
This page addresses many of the internal settings that affect the way a badge presenter interacts with the reader-controller.

**Network Time Out** is the number of seconds that the reader-controller will remain in HOST mode without any communications from the host software; once this time expires the reader-controller will fall into standalone mode. If the reader-controller is planned to be used in standalone mode, then this setting should always be 0 because there is not host.

**Latch Interval** is the number of seconds that the locking mechanism should remain unlocked after the presentation of a valid number to the reader-controller either by badge or keypad.

**Alarm Unauthorized Open** is a setting to determine whether or not the reader-controller is to initiate an alarm should the door be opened without the presentation of a valid number. In order for this to work, the reader-controller must be wired to a door sensor that can determine whether or not the door is currently open and some sort of alarm attached to the TTL2 lead of the reader-controller would additionally be needed.

**Beep On Reject** allows the reader-controller to give an audible sound anytime an **invalid** number is entered into the reader-controller either by a badge presentation or keypad.

**Beep On Accept** allows the reader-controller to give an audible sound anytime a **valid** number is entered the reader-controller either by a badge presentation or keypad. The audible sound can be set to either a short or long duration.

**REX action (Request to Exit)** is used in concert with the **Alarm Unauthorized Open**. If the door is equipped with a door sensor AND the Alarm Unauthorized Open is active, then the user must have a way to exit the door without setting off the alarm. The REX wires on the reader-controller can be attached to what is commonly called a REX button, when the user presses the REX button the reader-controller will unlock the door thus bypassing any alarm condition. Once all of this is configured
correctly, the decision can be made as to whether or not one of the available actions will take place when the REX button is pushed. The actions are to set TTL2 high and/or an audible sound.

Tamper Action allows an action to be set up should a Tamper condition be detected. The Tamper switch is an optical sensor that can be seen by looking through the small window on the back of the reader-controller. When the reader-controller is attached to a surface correctly, the Tamper condition will not be active as long as the reflective surface of the wall is sufficient enough to reflect light (the reader-controller is shipped with a reflective sticker that can be used to ensure the optical sensor will work correctly). The actions that can be configured are to set TTL1 high and/or an audible sound.

Special

The reader-controller has a unique feature that allows the administrator to quickly enter or remove badges without the need to type anything in. The reader-controller is toggled into and out of this special mode by the presentation of one of the special cards, the special cards are configurable on this page.

An example here will help to clarify the usage of special cards. Let’s assume Special page depicted here has been successfully utilized the to set up the Add card as badge number 123456. What this will mean is that anytime the reader-controller sees the special badge number 123456 it will toggle into Add mode, the presentation of that same badge again will toggle the reader-controller out of Add mode. When the reader-controller is in Add mode any other badge can be presented and that badge will automatically be stored on the reader-controller into Time Zone 1 (the Always Time Zone).

The Void card and Void mode are the fundamentally the same as the Add card and Mode, however the cards are removed from the reader-controller rather than added.

Set card button is used to store the New Card Value on to the reader-controller and it will be associated with the special card selected in the dropdown box. Using the example above, if is desired to store the value 123456 X in the reader-controller as the Add mode badge, ‘Add’ in the dropdown box choose
would be chosen, and the value 123456 is input in the New Card Value field and the Set card button is clicked.

Add is the special badge number that will toggle the reader-controller in and out of Add mode.

Void is the special badge number that will toggle the reader-controller in and out of Void mode.

Void all is the special badge number that will put the reader-controller in to Void ALL mode, once the reader-controller is in Void ALL mode, the presentation of the Void All mode card a second time will remove all the badges from the reader-controller (acts like a confirmation that you really do want to remove all the cards). If the reader-controller is put into Void All mode but that action is not desired, simply wait 5 seconds and the reader-controller will come out of Void All mode on its own as long as the Void Mode card is not presented a second time.

Normal is the special badge number that will put the reader-controller back into Normal mode, this is used to take a reader-controller out of Lock down or Unlock mode and put it back into the mode where it will accept or reject badges and or keypad entries.

Lock down is the special badge number that will put the reader-controller into a lock down state where all badges will be rejected. The only way to get a reader-controller out of Lock down is to present either the Normal or Unlock special badge.

Unlock is the special badge number that will put the reader-controller into an unlock state. The only way to get a reader-controller out of the unlock state is to present either the Normal or Lock Down special badge.

Keypad

If the reader-controller has a keypad, then this page will allow the administrator to configure whether or not the keypad is active and if it is active, how it reacts to keypad entries.
**Mode** is either enabled or disabled, if it is enabled then the keypad is active otherwise it is not.

**Max Length** is the maximum number of digits the user can enter at the keypad, if the user goes beyond this limit then the entry is rejected.

**Entry Time Out** is the small amount of time that the reader-controller will wait before deciding that the user is finished entering their number. This field is in $1/16^{th}$ of a second which means that if the value of 16 is input, reader-controller will wait 1 full second before canceling the entry. The Entry Time Out has specific ramifications if the Starting and Ending chars are not set (see below). If the user is not using a starting and ending character to let the reader-controller know when the user is finished entering his/her PIN code, then the Entry Time Out takes over. Let’s assume that the starting and ending characters are not set and the Entry Time Out is set to 16 (1 second), then the user will enter his/her PIN number on the keypad and the reader-controller will wait for 1 second of no activity before deciding that the user is done. If the user starts entering their number and then stops for more than 1 second before finishing, then the reader-controller will attempt to process the partially entered number and it will be rejected. If this happens, the user will need to start over. If the reader-controller is not set to beep on reject, then the user will have no way of knowing that their partially entered entry has been rejected which can lead to frustration. For this reason it is advisable to have the beep on reject set at ON.

**Start Char #1** is the signal to the reader-controller that a keypad entry is about to be entered.

**End Char #1** is the signal to the reader-controller that the user is done entering their keypad entry.

If the Start Char is set to “*” and the End Char is set to “#”, then the correct sequence for the user to enter a PIN code of 123456 is to press the “*” key on the keypad, followed by the keys 1, 2, 3, 4, 5 and 6 followed by the “#”.

**Start Char #2** is exactly the same as Start Char #1.

**End Char #2** is exactly the same as Start Char #2.

Start and End char 2 are used to allow the user to enter his/her PIN code using either the “*” or “#” key to start the sequence followed by either the “#” or “*” to end it.
The Test Unit page is available to perform a small number of tests at the unit to ensure that it is operating correctly.

**Relay ON and OFF** will open and close the onboard relay and if it is attached correctly to a door lock, the door lock will activate on and off. If the relay is not attached to a door lock the onboard relay click can still be heard if the environment is quiet enough.

**Buzzer ON and OFF** will turn on and off the buzzer on the reader-controller. This noise will be a continuous sound until it is turned off.

**TTL1 ON and OFF** will activate and deactivate the TTL1 line but the only indication will be that this is working is IF the TTL1 is correctly wired to a device that will perform some action in response to the line activating and deactivating.

**TTL2 ON and OFF** will activate and deactivate the TTL2 line but the only indication that this is working will be is IF the TTL2 correctly is wired to a device that will perform some action in response to the line activating and deactivating.

**Set LED 1** will set the top LED on the reader-controller to the color specified in the dropdown box. The LED will remain in this color until either it is set to another color using this page or the user logs off and valid badges are presented to the reader-controller.

**Set LED 2** will set the bottom LED on the reader-controller to the color specified in the dropdown box. The LED will remain in this color until you either set it to another color using this page or you log off and valid badges are presented to the reader-controller.
Additional Pages
The following set of pages do not have any configurable options on them, they are pages generated by the reader-controller under normal operating circumstances.

Timeout

If the session timer is allowed to expire the reader-controller will automatically log you off and the Timeout page will be displayed. To log back in, click on the provided button from this page.

Logoff

PowerNet Session Complete!
You may now use this PowerNet unit in a normal fashion.
Thank You!

If the Log Out button is clicked this page will be displayed. If it is required to log in again the IP address will have to be put into the address field on the browser.

Redirect

Anytime an action is performed that causes the reader-controller to reboot this Redirect page will appear. The Redirect page will have a counter depicting the number of seconds before a new connection with the reader-controller will be attempted. When the counter reaches 0 a new connection will be established and the reader-controller must be logged into again.
**Trouble shooting**

**The IP address of the reader-controller is not known.** There are a number of options.

A. Press and hold the reset button on the back of the reader-controller for 5 seconds while it is powered on. The reader-controller will reset to the IP address of 192.168.1.27.

B. The reader-controller should have been delivered with a CD. The CD contains the Crystal Matrix™ access control administration program, which can also be downloaded from the ISONAS web site. When the program is installed several utility programs will be installed as well; Plug N Play is one of them.

**No login screen when connecting to the reader-controller.** If the reader-controller is operating under normal conditions then there is a good chance that the firmware on the reader-controller does not support the Embedded Web Server. Download the latest firmware from the ISONAS web site.

The Embedded Web Server pages fail to display correctly. The pages were written to support the Internet Explorer and Fire Fox browsers, other browsers **may** work correctly. If one of the two supported browsers are used and the pages are still failing, then try turning off the proxy server if one is being used.

I changed the IP address and now I cannot re-connect using my browser? ??

I do not remember the password for either Admin or User? If the reset button on the back of the reader-controller is pressed and held for 5 seconds while it is powered on, the reader-controller will reset the passwords to the defaults of Admin00 and User2009.
**Badges Worksheet**

Reader-controller location______________________  
Badge Number_______________________  
PROX (Yes or No)?  
PIN (Yes or No)?

Time Zones (put a check mark in the ones assigned to the badge)

<table>
<thead>
<tr>
<th>Always</th>
<th>Business Hours</th>
<th>User1</th>
<th>User2</th>
<th>User3</th>
<th>User4</th>
<th>User5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Time Zone Work Sheet**

Reader-controller location _______________________
Time Zone name: __________________________________
Normal (Yes or No)?
Holiday (Yes or No)?
Shift unlock (Yes or No)?
Badge unlock (Yes or No)?

<table>
<thead>
<tr>
<th>Day of week</th>
<th>Start time</th>
<th>End time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>