infrastructure
protection

TZ Centurion™ Server

Product Manual

Powered by

Microsoft® Silverlight®

A TZ Business | ixp.tz.net | © 2015

Date: December 2015
Document Number: 112521-01_D

About TZ

Telezygology, Inc. (TZ) is a wholly owned subsidiary of publicly listed intellectual property and technology development company, TZ Limited, with design and engineering operations throughout the United States, Europe and Australia.

TZ is a leader in the integration of intelligence and software control into everyday objects to enable new levels of functionality. Supported by a full product development capability, TZ Technology is a platform on which many different solutions can be created by third parties seeking to integrate remote controlled intelligent locking and sensory devices to add functionality to their products.

TZ solutions fuse software controlled remote locking and fastening, environmental sensing, real time analysis and measurement to provide adopters with compelling benefits for their products and businesses.

Disclaimer

This document is intended to provide basic technical information related to the TZ Centurion Server Foundation.

This document is not meant to be an exhaustive statement of all relevant data. By using this document, however, you agree to accept and comply with the terms, conditions, notices and disclaimer contained in this document.

While TZ has used all due care and skill to ensure that the information contained in this document is accurate, correct, and current at the time of publication, it does not warrant or represent that the information is free from errors or omissions, and does not accept responsibility for any defect in the information.

Use of Information Contained in This Document

The correct operation of the TZ Centurion Server foundation will require consideration of installation and system integration issues such as networking for power and data, and subsequent programming for functionality.

The TZ Centurion Server foundation described has not been tested or qualified for a specific application other than for compliance to the specification outlined. Specific qualification testing may be required for fit-for-purpose application design.

Caution

Changes or modifications not expressly approved by TZ could void the user's authority to operate the equipment (FCC Code of Federal Regulations Title 47 Part 15.21).

Contents

infrastructure
protection

TZ Centurion™ Server

1. Introduction

Telezygology, Inc. (TZ) is the inventor of intelligent fastening, locking and actuation devices that in combination with TZ software and communication gateways provide a networked platform that extends traditional access control networks to asset level protection and creates compelling security, locking, monitoring and control applications across a number of market segments.

TZ control networks consist of TZ Radial and other locking devices, interconnect modules, physical and environmental sensors, and industry standard access control input translators, all of which can be connected to and controlled from stand-alone control devices and computers via the internet.

This manual only provides detailed technical information about the TZ Centurion Server.

2. System Example

Figure 1 below portrays an example of a TZ network system used to control and monitor multiple computer racks and provide the appropriate level of access to authorised parties.

The TZ network allows only those people with proper authority – on or off-site – to monitor and control cabinets and other areas secured with TZ intelligent locks and devices. The system administrator assigns different roles and permission levels to users to grant –physical access to equipment using RFID cards or remote access to view and control specific subsets of locks via a web browser.

These devices are controlled by the TZ Centurion Bridge, allowing activity and measurement by any device in the network to be viewed on the embedded administration web interface. The TZ Centurion Bridge communicates and synchronizes with a server running the TZ Centurion Server software, which coordinates, records, organizes, and displays the status of all devices.

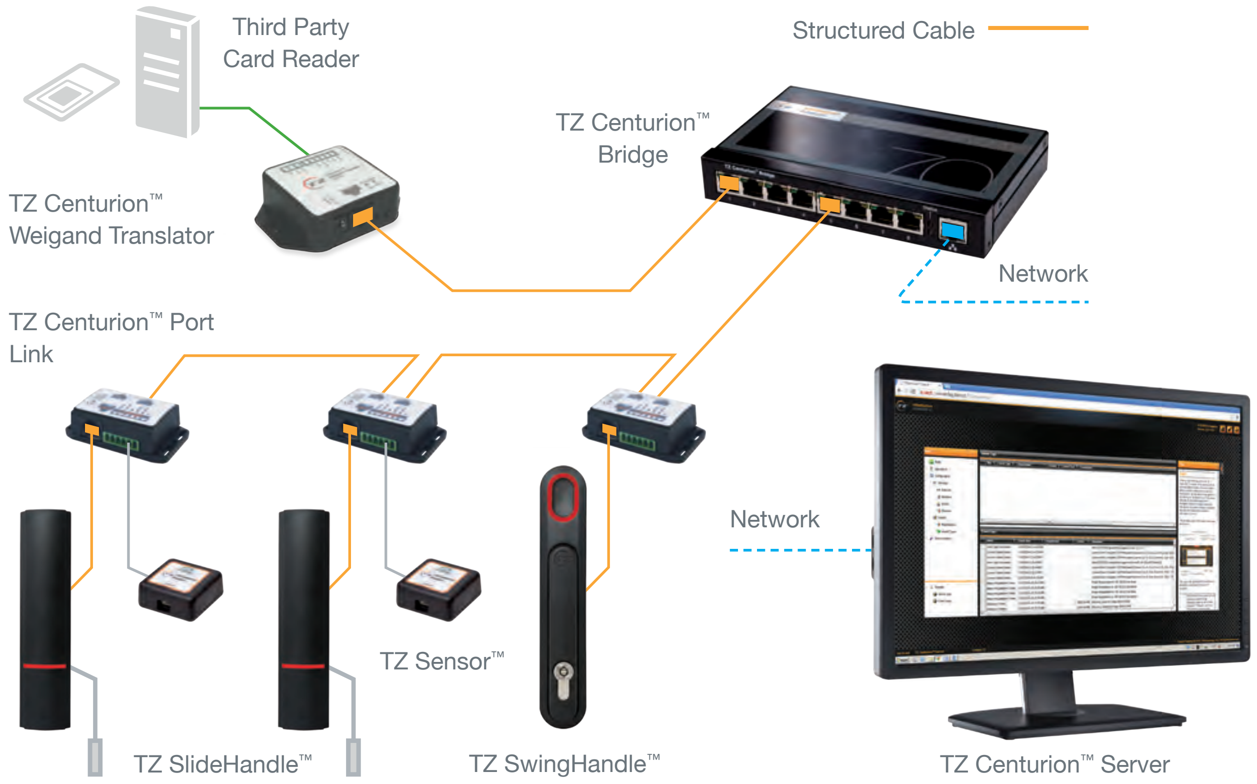


Figure 1: TZ Network System

3. Physical Connections

The server running the TZ Centurion™ Server software and all of the TZ Centurion Bridges must be plugged into an Ethernet connection. The other Internet access requirements for the TZ Centurion are described in the section on Firewall Settings.

TZ SlideHandle, TZ Radial Intelligent locks, TZ Centurion Wiegand Translators and RFID Readers, and other devices are plugged directly into any of the eight RJ45/RS485 ports on the TZ Centurion Bridge. The individual TZ devices can be connected to a TZ Centurion Bridge with up to 100 metres of standard CAT5e/6 cable.

Although TZ devices are connected to a TZ Centurion Bridge with the same Category 5e/6 (Cat 5e/6) cabling used in Ethernet connections, the TZ Centurion™ Bridge communicates to devices attached to it (locks and readers) via RS485 serial communications, not 802.3 Ethernet. Only the cabling from TZ devices should be connected to any of the eight RS485 ports on the front of the unit. TZ recommends using a different color of CAT5e/6 cabling for the devices connected to the TZ Centurion Bridge than is used for Ethernet throughout the environment (e.g.: blue for Ethernet, orange for TZ Centurion devices).

More than one device can be connected to any leg coming from the TZ Centurion Bridge by daisy-chaining the connection and using a TZ Centurion Port Link or Multi Port Link device. If the device is farther than 100m from the TZ Centurion Bridge, it is necessary to use a TZ Centurion Multi Port Link to connect a power supply physically closer to the device. If the TZ Centurion Bridge is powered via PoE (Power over Ethernet), the maximum amount of cable and devices that can be used is 7m and 8 devices unless additional power is added.

More details can be found in the TZ Centurion Bridge manual.

4. Initial Setup of Bridges

After the software is installed, the information required to configure and arrange the TZ network must be gathered and imported. Before beginning with the TZ Centurion Server software, a few settings on each of the TZ Centurion Bridges must be configured via the following steps:

1. Locate each of the TZ Centurion Bridges within the network. Use the TZ Centurion Console – a Windows utility that scans the local subnet and lists all connected TZ Centurion Bridges and the current default IP address. Since the TZ Centurion Console cannot see outside of the local subnet, it will be necessary to run it within each subnet that contains a TZ Centurion Bridge and firewalls must be opened to allow local communication on UDP port 30303.
2. Log in to each TZ Centurion Bridge with a browser using the following steps:
    a. Use the IP address as the URL in the browser. Use the default login name of “admin” and the password as “admin.”
    b. Navigate to the Users tab. Edit the admin user to set the administrator login and password combination to something safe and secure.
    c. Navigate to the Systems tab and the Settings sub-tab

1. Set the IP address to something that is pre-allocated, static, and appropriate within the network.
2. Set the Subnet Mask.
3. Optionally set the Primary DNS and Secondary DNS.
4. Uncheck the Enable DHCP checkbox.
5. Click Save. The browser will now log out because the browser is no longer pointing to the correct IP address.
6. Make a permanent note of the new IP address, login and password.

5. Firewall Settings

By default, communication between the TZ Centurion Server and the different TZ Centurion Bridges within a system is done (1) between the IP address of the server and the IP addresses of each Bridge, and (2) directly to the default TCP port 80*. (This port can be custom configured in the System Application Settings xml file.) Each bridge must be able to communicate with the server and vice versa.

Additionally, any user that requires login access to the TZ Centurion Server must be able to access the server via their browser of choice, and their access through firewall and/or an institution's Intranet must be set appropriately.

Note: **NB: Prior to TZ Centurion Server version 3.0.2.007 communication with TZ Centurion Bridge was performed using SSL (TCP/443). This behavior can be changed to HTTPS if required.*

6. Server Requirements

TZ Centurion™ Server provides centralized support for many TZ locking and sensor devices over a secure LAN or WAN connection. It includes web services and a Silverlight web client, and is designed to run on Windows Server® 2008 R2 64-bit with SQL Server® 2008 Express or better. The client is supported by major browsers including IE 8.0 or greater with JavaScript enabled. Silverlight 5.0 is required and will be installed from the Internet if it is not already installed for the user. Local and Domain Administrator rights are required for the installation.

6.1. Set up Requirements

> It has been benchmarked using network traffic throughput of at least 100mbit/s. Networks of 1gbit/s are recommended between bridges and their controlling TZ Centurion Server instance for large installations.

> TZ Centurion Server includes web services and a website that is designed to run on Windows Server® 2008 64-bit or later. Each should be on equipment certified for and exceeding the minimum requirements of the operating system (OS).

> Small scale environments of less than 64 devices on two to four TZ Centurion Bridges should generally run satisfactorily with 2GB of RAM on hardware exceeding Windows Server® 2008 64-bit minimums if that server is dedicated to TZ Centurion Server application. RAM should exceed that minimal amount if any other functionality is run on the server.

> Minimum 10GB Free hard drive space is required.

> If SQL Server® instance is hosted on the same server as the TZ Centurion™ Server, Microsoft's recommendation to install SQL Server® log files on a separate drive set from the data files should be followed. Failure to do so may impact real-time performance.

> The TZ Centurion Server uses Microsoft SQL Server® 2008 or newer as its data repository. If a full version is not available, an Express version must be loaded prior to installation.

> SSL is required for secure communication between the management browsers and the TZ Centurion Server web-interface.

> Local and Domain Administrator rights are required for the installation.

6.2. Prior to Installation, the following steps are recommended

> Plan a naming convention that will help you know where a device is located and transmit the naming convention clearly to your installers BEFORE they begin cabinet and hardware installation.

> As devices are installed, connect them to TZ Centurion Bridges. When all devices are attached to a Bridge, test to confirm all are discovered by the Bridge (refer to TZ Centurion Bridge User Guide), so you know connectivity and power to each is OK.

> Identify IP Address of each TZ Centurion Bridge.

> Confirm you can ping each TZ Centurion Bridge from the server.

> Confirm you can connect to port 8484 on the TZ Centurion Server from the TZ Centurion Bridge network.

6.3. Key TZ Centurion™ Server installation steps involve

1. SQL Server® installation
2. .NET 4.0 Framework
3. WCF Feature support activation, if required
4. IIS setup of the Web Service layer
5. IIS setup of the website
6. Configuration of devices using the TZ Centurion Server Silverlight client

Steps 2-5 are performed as part of the TZ Centurion Server installation program.

7. Organize Assets

Asset levels provide a method of grouping devices in order to locate and keep track of them. The specific asset levels are assigned string values which are intended to describe the superstructure, and the levels are hierarchical to allow for the logical deployment within enterprise infrastructure.

The best explanation of this concept is through an example. Suppose a business has assets deployed in two separate buildings, with TZ devices located throughout both buildings.

The first building (designated “Building 1”) has three floors (Floor 1, Floor 2, and Floor 3), and on each floor there can be different number of uniquely labeled rooms.

The second building has only one floor with two rooms on that floor. Within each room, there are varying numbers of rows of cabinets.

Because asset levels are hierarchical, for any particular member of the hierarchy there can be any number of sub-members, and the sub-members must have unique names (e.g. Floor 1 in Building 1 can *not* have two Room As). However, different members of the hierarchy can have similarly named sub-members. (e.g. Floor 3 in Building 1 has a Room 1 and a Room 2, and Building 2 has a Room 1 and a Room 2) For the TZ Centurion™ software, there is a limit of three asset levels within the software, plus primary and secondary names to distinguish devices. The Asset Management Module provides more levels and flexibility.

The hierarchical arrangement of these assets can be organized within TZ Centurion software as described in the section on Asset Types and Asset Registration.

8. Start

When a user first logs in to the TZ Centurion Server system, they are brought to the initial Start screen where the latest activity and the status of any alarms. This screen can always be navigated to by clicking on the Start icon in the upper left side of the screen above the navigation pane. The exact content is filtered per the user’s role as well as the devices and assets the user has permission to view.

The primary parts of the start screen are as follows:

The upper bar contains information and elements pertaining to the current session.

The center of the upper bar will display a bright orange message if alarms have been triggered. The user can view the alarms by going to the monitoring screen. Click on this message balloon to view the current active alarms. You can also hide these alarms for the current session by clicking the close control within the message balloon.

View the end-user license agreement and enter in Licensing information.

Change password.

Logout.

The information area is the central portion of the window. The exact format and presentation depend on the navigation node clicked by the user.

The navigation pane is located along the left side, and is used to jump between functional areas of the TZ Centurion™ Server. The functional areas available depend on the roles of the person who is logged in. The functional areas are:

Clicking the Start icon displays up-to-date tables for both the alarm logs and event logs.

The Operations area consists of operational cards (the assignment of access cards to people) remote access (the ability to open locks and grant access through via the server interface) and monitoring (the viewing of events and alarms present in the system).

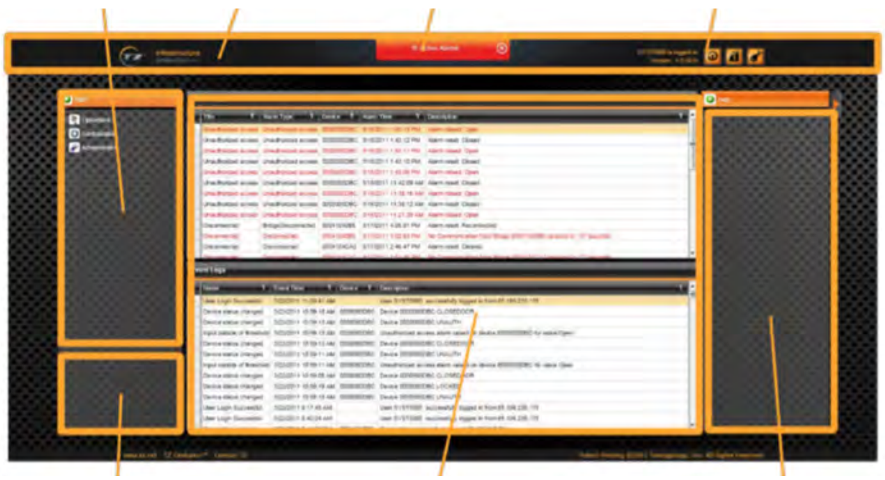
The Configuration node contains icons necessary to initially set up the TZ Centurion(TM) Server, connect and/or edit additional devices, and place them within a hierarchical asset structure. These functions include administering bridges, card readers, locks, and sensors as well defining asset types and registering assets.

The Administration node contains icons to define user accounts, manage user organizations, manage cards, and manage the settings of the system.

The Reports area is located just below the navigation area, and it displays links to up-to-date reports that are associated with the current screen.

The Help area is located on the far right side, and can be turned hidden or shown by clicking on the large orange triangle on the far right side.

Navigation Pane Upper Bar Alert Notification Logout, EULA and Password Change



Available Reports Information Area Help Area

9. Network (Bridges)

The Network screen displays all currently registered TZ Centurion™ bridges and is also the place where bridge-related details are edited and newly-connected bridges are be registered and configured.

The top portion displays all currently configured bridges. The bottom portion lists the details about any particular bridge that is selected in the upper portion.

There are two ways to work with the bridges. For first time set up of bridges, the Device Registration Wizard is recommended, as it can handle multiple bridges, incorporates the creation of an Asset Hierarchy, and can automatically map devices to assets, saving a lot of manual setup effort. To work with existing bridges in the system, or if you want to individually add new bridges without using the Wizard, then use the specific functions as described below after the Wizard section.

9.1. Device Registration Wizard

The Device Registration Wizard supports registering multiple Bridges and automatically mapping their associated Devices to an Asset Hierarchy. To begin using this Wizard, click the Device Registration Wizard button in the upper right portion of the screen. The screen progression for this Wizard is as follows:

1. ENTER BRIDGE INFORMATION TO START SCREEN -

On this screen you configure the bridges to work with, either by:

a. Adding them manually, with the Add Configuration button.

b. Automatically finding all the bridges visible to the server but not already registered, with the Discover Bridges button.

For each Bridge, you can also optionally provide a Primary and Secondary Name, which will be applied in the last step of the Wizard when the bridges are registered. Complete this step by ticking the bridges you want to be included in the bulk registration (maximum five at a time), then click Next.

2. ASSET HIERARCHY SCREEN -

This screen is optional. If you already have an existing asset hierarchy, or you are planning to import Device-Asset mappings via a CSV file in the next step of this Wizard, you can skip over this screen. This screen allows you to define an asset hierarchy with far fewer clicks than the normal (non-Wizard) method.

Add each leaf of your desired asset hierarchy one at a time by entering the asset name and clicking Add. If using more than one level of asset, separate them using the indicated separator, for example:

a. ‘HQ’ is an example of a top level asset

b. ‘HQ-room101’ is an example of a 2 level deep asset

c. ‘HQ-room102-cab1’ is an example of a 3 level deep asset

Note that Assets must be associated to an organization. Use the Organization drop-down list to select from the existing organizations. You cannot add a new organization from within this wizard.

When you have finished designing the asset hierarchy, or are skipping over this step, click Next.

3. MAP DEVICES TO ASSETS SCREEN -

This screen is optional. It allows you to define Device-Asset mappings. However, note that any existing Device-Asset mappings will NOT be overwritten by those you define here. To change existing mappings, use the normal manual methods rather than this Wizard.

Also note that any devices discovered during the last step of the Wizard when the bridges are registered and which are missing a Device-Asset mapping will be assigned to the ‘Unmapped’ Asset (which is what the normal non-Wizard method of Device discovery does) and will have to be manually mapped.

By default, any assets referred to by these mappings that don’t already exist will be created. If you want unknown Assets ignored, then uncheck the Create Asset hierarchy.

Note that to define mappings, you must already know the serial numbers of the devices to be mapped. Any mapping referring to a device which is not subsequently discovered is ignored.

You can define mappings either manually or using importing. Using the manual method, add them to the displayed table using the Add button. Using the importing method, use the Import button to import the mappings from a CSV file. Each mapping consists of five fields:

a. Device serial number

b. Organization the Device will belong to

c. The Primary Name to assign to the Device

d. The Secondary Name to assign to the Device

e. The parent Asset, in the form AssetLevel1 [-AssetLevel2][-AssetLevel3]

When you have finished adding the mappings, or are skipping over this step, click Next.

4. DEVICE DISCOVERY SCREEN -

Each bridge to be registered by the Wizard will be listed on its own row in the table. To finalize the process of bridge registration, device discovery and mapping of devices to assets, click the Start Discovery button.

The screen will update the status for each bridge as this step is progressing. The statuses are:

> Registered – bridge has been sent registration message

> Discovering – bridge is undergoing device discovery

> Online – bridge has completed discovery and is ready for use

Once all bridges are Online, or you have waited a reasonable period of time and the bridge status is not progressing, click the Finish button. In the case where a bridge has not come Online, the Event logs may provide a clue as to the cause.

If all bridges are online, check that the devices of each bridge have been correctly found and mapped to their expected asset, and that the asset hierarchy is as expected.

9.2. Registering Bridges (non-Wizard)

To add a new bridge to the TZ Centurion Server system, click the Register Bridge button in the upper right portion of the screen. Enter the IP address, username and password of the new bridge and click OK.

You should see the message “Registration has been sent to bridge,” and either an entry in the bridge table should appear in a few seconds or a message should appear stating the reason the bridge could not be found.

After registering a bridge, the bridge must be told to survey(discover) and find all of the TZ devices connected to that bridge, as discussed in the next section.

9.3. Re-Registration of offline Bridges

If the TZ Centurion Server detects that a Centurion Bridge is unreachable, it will automatically attempt to re-register the bridge. The TZ Centurion Server will attempt to re-register the bridge every 60 minutes. Discovery is not performed on the bridge after it has been re-registered; the entries that were previously loaded in the database will be restored against the bridge. This can be disabled in the instance that you have a testing server which is unable to reach a set of bridges by using the AutoRegisterUnreachableBridges configuration option.

This bridge re-registration is performed in a serial fashion (one bridge after another) rather than in parallel to prevent excessive load on the TZ Centurion server and network environment.

9.4. Discover (non-Wizard)

To discover all of the devices connected to a particular bridge, discover a device that is newly connected to a bridge, or check an Internet connection if for some reason a bridge appears off line, select the bridge and click on the Discover button in the upper right portion of the screen. The message “Discovery has been sent to bridge” should appear, and after a few seconds, the devices should appear under either the Locks or Readers screen, depending on the type of device.

9.5. Updating Bridge Firmware

To update bridge firmware, click on the Update Bridge Firmware button in the upper right portion of the screen. The Update Bridge Firmware screen will appear.

The latest firmware file known to the server will already be pre-populated, but if you have a later version .tar file, you can use this by clicking the magnifying glass icon, selecting the file in the browse dialog that appears, then clicking the Upload to Server button.

The table within the screen will list all the currently Online bridges that are registered to the server, together with details such as the current Firmware Version. Tick the bridges to be updated (maximum five at a time) and then click Update Selected Bridges. Updates typically take about one minute, during which, the bridge will make occasional beeping sounds.

The screen will update the status for each bridge as this step is progressing. The statuses are:

- Uploading – bridge is in the process of having the firmware uploaded
- Firmware Uploaded – bridge has finished uploading and is ready to use

Once all bridges have been updated, or you have waited a reasonable period of time and the bridge status is not progressing, click the Close button. In the case where a bridge has not successfully updated, the Event logs will provide a clue as to the cause.

9.6. Bridge Details

To edit the details of any particular bridge, select that bridge and modify the fields underneath any of the tabs in the bottom portion of the screen. Click Save before changing tabs, or information will not be saved.

The text fields should contain only numbers, letters, spaces, dashes, and underscores. The fields are used as follows:

- Primary Name: The name used to designate this device from other devices throughout this web interface. Using a meaningful and easily recognizable string in this field can simplify network set up and management. The initial default is a number assigned during the device discovery process. Note: TZ recommends using names that easily identify the location of the device in your environment
- Secondary Name: This is an additional text field that can be used to store additional info about the TZ Centurion™ Bridge (e.g. location, cabinet number, etc.). The initial default is the serial number of the device.
- Auxiliary Input Name: String used to describe the device attached to the auxiliary input. The Auxillary Inputs are simple digital contact closures
- Auxiliary Input Type: The type of input that is connected. This is either set to Contact Closure or Unconfigured.
- Auxiliary Output Name: String used to describe the device attached to the auxiliary outputs.
- Auxiliary Output Type:
- Alarm Output: The output will depend on an alarm, which will depend on the Auxiliary Input of some other TZ device.

The IP address, gateway address, subnet mask, primary and secondary DNS used by the selected bridge are all displayed under the Network Details tab. These details cannot be changed from the server.

9.7. Replacing Bridges

If for some reason a bridge is malfunctioning and needs to be physically replaced, the following procedure can be used to swap the bridge with a new one. This procedure will make all of the proper associations within the database, however, it will be necessary to redefine any alarms associated with any devices connected to the malfunctioning bridge. This procedure should only be done to physically replace a bridge.

1. Replace the malfunctioning TZ Centurion Bridge by:
    a. Physically disconnecting the old bridge from the TZ devices and from the Ethernet.
    b. Un-mount the malfunctioning TZ Centurion Bridge.
    c. Mount the new bridge in its place.
    d. Plug the new bridge into the network and connect all of the appropriate devices.
    e. Configure the new TZ Centurion Bridge with an IP Address reachable from the Centurion Server.
2. Select the malfunctioning TZ Centurion Bridge from the upper portion of the screen, and click the Replace Bridge button on the upper right.
3. Enter the IP address for the new bridge in the pop-up box and click OK.
4. Select the new bridge from the upper portion of the screen and click Discover.

When discovery is complete, all of the locks, readers, and other connected devices will be assigned within the asset hierarchy just as they were before. However, as mentioned above, it will be necessary to redefine any alarms associated with the devices connected to the malfunctioning bridge.

9.8. Bridge License Details

The current license details of the selected bridge are displayed on the Bridge License Details tab. If during a bridge firmware upgrade the TZ Centurion™ Bridge loses the associated device license this can be rectified by:

1. Contact your TZ sales representative to obtain a new bridge license (the license determines the number of devices that can be attached to the bridge, by default this is limited to eight devices).
2. Enter the new license key in the provided field on the Bridge License Details tab.
3. Enter the number of devices the new license allows (this is informational only, the number has no effect on the actual licensing).
4. Click Save.

9.9. Event Log

The Event Log tab displays all of the events associated with the bridge. Note that it does not display the events associated with the connected devices; it only displays the events associated with the bridge itself.

9.10. Alarm Log

The Alarm Log tab displays the alarms associated with the bridge as well as any alarms associated with the devices connected to the bridge.

9.11. Devices

The Devices tab displays a list of all the TZ devices connected to the bridge selected in the top portion of the screen. The devices cannot be edited in this screen, but they can be removed via the buttons on the right side.

9.12. Alarm Configuration

An alarm is a condition that the TZ Centurion Bridge can test for, and when the condition is true, the TZ Centurion Server can send a message to the browser, simply write the event in a special Alarms log, generate a syslog event or send an SNMP Trap.

By default, an alarm condition exists whenever a TZ SlideHandle, TZ Centurion Bridge, or other device is no longer in contact with the server.

Additional alarms are defined and edited under the Alarm Configuration tab. To define a new alarm, select the bridge that is connected to devices involved with the alarm, and click New. A window should appear that allows the user to enter the appropriate details.

In the Name text box, give the new alarm a descriptive title. This text is included in the Alarm Log entry that is recorded every time this alarm is triggered. This customised name can be used to quickly identify the source of the alarm.

From the Source dropdown list, select the device to be monitored by this alarm. This can be any TZ Radial, SlideHandle, or TZ Sensor. Alarms configured for sensors are triggered when the sensor reading falls above or below a specified acceptable range. Configuring these parameters is defined in more detail below.

From the Target dropdown list, a physical indicator (i.e., a warning light or audible alarm) can be set when the alarm is triggered. All alarm events are automatically logged in the Alarm Log. Select Log Only from the target list if no other notification is needed.

Click Save to complete the definition.

Alarms can be edited by selecting the appropriate alarm from the lower portion of the screen, clicking Modify, and following the same procedure. Alarms can be removed by selecting the appropriate alarm and clicking Remove.

9.13. Reports for Bridges

A report containing details of any particular bridge is available by selecting the specific bridge from the upper half of the screen and clicking on the Bridge Detail report in the lower left portion of the screen. The report will contain all the details of the bridge including IP address, DNS server, firmware version and a list of all of the devices connected directly to the bridge in question.

The information contained in any report can either be directly printed or exported into an Excel, Word, or PDF format by clicking the either the printer icon or the disc icon in the upper bar of the report.

10. Readers

The Readers screen displays all RFID Readers and Wiegand translators connected to the system. Global System Administrators may configure readers regardless of the organisation they are assigned to. Other users may configure only those within their own organisation and those that are still unmapped in Registration. All Available Locks displays only the locks within the selected reader's organisation. Since a Reader can be assigned to a different organisation after locks have been mapped, Mapped Locks displays all the locks mapped to that reader, regardless of their organisation. It is your responsibility to remove these locks from the reader if you choose to change the reader's organisation. The reader name can be changed on the Registration screen.

For access cards to work properly, the following elements must be set up correctly:

> RFID Reader/Wiegand Translator (card reader) must be connected to the system and discovered (see Registration in Network).

> A lock or set of locks must be mapped to the card reader as explained below.

> Personal information of the cardholder must be placed in the system using either the Accounts screen or the Operational Cards screen.

> The organization to which the cardholder belongs must be in the system, along with a proper start date, end date and access schedule. (This can also be done in the Operational Cards screen.)

> The access card must be associated with the cardholder, and then physically given to him or her using the Operational Cards screen.

The locks that are mapped to a particular card reader are the locks that will open when a valid access card is swiped at that reader. The mapping is accomplished via the following steps:

1. Select the card reader from the top portion of the screen. All of the available locks will appear on the lower left portion of the screen.
2. Select all of the locks that should open when an access card is presented to the card reader by clicking in the checkbox and then click on the rightward pointing triangle. The locks should move from the All Available Locks column on the left side of the screen to the Mapped Locks column on the right side of the screen. Locks can be unmapped from a reader by selecting them from the lower right section (mapped locks) and clicking the leftward pointing triangle. Note that if the lock being unmapped belonged to an organisation the reader no longer belongs to, it will not be available.

10.1. Reports for Readers

A report containing details of any particular card reader is available by selecting the specific reader from the upper half of the screen and clicking on the Card Reader Lock Mappings report in the lower left portion of the screen. The report will contain all the details of the reader including what bridge it is connected to as well as what locks the reader directly controls.

The information contained in any report can either be directly printed or exported into an Excel, Word, or PDF format by clicking the either the printer icon or the disc icon in the upper bar of the report.

11. Locks

The Locks section is used to display information pertaining to all of the TZ SlideHandles and TZ Radial Locks connected to the system. The upper portion of the screen displays all of the locks currently monitored by the system in a filterable, sortable list.

The locks can also be operated from this screen, and the device status is displayed (locked / unlocked, open / closed) as discussed in the Remote Access section.

To edit the details of any lock, simply select the lock from the upper portion of the screen and edit the information under the Device Details tab below. To save any changes, click on the Save button before selecting any other locks or any tabs.

The fields available are based on whether the lock is a TZ Radial or a TZ SlideHandle, but in general they are as follows:

> Primary Name: This is the name used to designate this device from other devices throughout this web interface. Using a meaningful and easily recognizable string in this field can simplify network set up and management. The initial default is the serial number of the lock assigned during manufaturing. Note: TZ recommends using names that easily identify the location of the device in your environment.

> Secondary Name: This is an additional text field that can be used to store additional info about the TZ Radial (e.g. location, cabinet number, etc.) The initial default is the serial number of the device.

> Unlock Duration: In some applications, the TZ Radial or TZ SlideHandle isn't unlocked directly. Rather, it is put into a mode (push-to-release) that waits to sense a push on the door to which the lock is attached. When the lock senses this pressure, it pops open and allows access to the secured assets. The Unlock Duration field defines how long the lock stays in this "ready" mode.

> Auxiliary Input Name: String used to describe the device attached to the auxiliary input (temp sensor, humidity sensor, etc.).

> Auxiliary Input Type: There are different types of sensors that can be attached to the auxiliary inputs of a TZ Radial or TZ SlideHandle lock. The choices are Temperature, Relative Humidity, Contact Closure, and a Liquid/ Leak sensor. Use this drop down to designate what type of sensor is connected to each lock. If the lock is a TZ SlideHandle the Auxilliary Input 2 is already assigned the included Door Sensor (contact closure) that is supplied with the lock.

> Auxiliary Output Name: String used to describe the device attached to the auxiliary output.

> Auxiliary Output Type:

> Locked Indicator: Will turn on (sink current) when the TZ SlideHandle or TZ Radial is locked.

> Unlocked Indicator: Will turn on (sink current) when the TZ SlideHandle or TZ Radial is unlocked.

> Open Indicator: Will turn on (sink current) when the associated Auxiliary Input is connected to a contact closure / door sensor, and the door is open.

> Red Locked or Green Locked (SlideHandle Only) the LED indicator on the front of the TZ SlideHandle will shine red or green when it is locked, depending on the value of this field.

11.1. Event Log

The Event Log tab displays all of the events associated with the current lock selected.

11.2. Alarm Log

The Alarm Log tab displays the alarms associated with the current lock selected.

11.3. Reports for Locks

A report containing details of any remote event (i.e., via the web interface) which caused a lock to open can be obtained by selecting the lock in question from the upper half of the screen and clicking on the Devices Opened Remotely report in the lower left portion of the screen.

A report containing details of any particular lock is also available by selecting the specific lock from the upper half of the screen and clicking on the Device Detail report in the lower left portion of the screen. The report will list all the events (openings, closings, and status changes) associated with the lock.

The information contained in any report can either be directly printed or exported into an Excel, Word, or PDF format by clicking the either the printer icon or the disc icon in the upper bar of the report.

12. Sensors

All of the sensors connected to the TZ Centurion system are displayed via the Sensors screen.

The upper portion of the screen displays the names, types, status and reading of each sensor in the system. Sensors may include temperature sensors, humidity sensors, leak sensors, and magnetic door sensors. The names that appear here are the same names that appear when alarms are defined under the Network screen. The names of sensors can be edited by selecting the sensor from the upper portion of the screen, editing the Primary Name or Secondary Name fields, and clicking Save. Events or alarms that the sensor has been involved with can be viewed by clicking on the Event Log or Alarm Log tabs.

Sensors must first be wired to a specific device, and then defined in the in the screen associated with that device. In most cases, this is a TZ Radial or TZ SlideHandle, but it may also be a TZ Centurion Bridge.

12.1. Event Log

The Event Log tab displays all of the events associated with the current sensor selected.

12.2. Alarm Log

The Alarm Log tab displays the alarms associated with the current sensor selected.

13. Device Age

The age of a device from when it was first registered against the TZ Centurion Server system can be determined by viewing the device under the relevant section.

> Bridges – This is Bridge Details tab when the relevant bridge has been selected on the Network configuration page.

> Locking Devices - This is Device Details tab when the relevant lock has been selected on the Locks configuration page.

> Card Readers – This is listed as a column entry on the Readers configuration page.

This data is required to be supplied as part of any warranty claim.

14. Registration

Individual assets as well as the hierarchical relationship between assets tracked by the TZ Centurion Server are defined here in the Registration screen. The type of the asset is either one of the TZ devices or it is a user-defined type which is defined in the Asset Types screen.

When TZ devices are first discovered in the Network screen, they are not mapped to any particular asset or organization, so they are placed in the Unmapped asset in the upper portion of the screen.

14.1. Creating Assets

Some of these concepts are best described by way of example. Suppose that there should be three asset types: (1) buildings, (2) rooms, and (3) cabinets. Logically, one or more locks would belong to a cabinet, one or more cabinets would belong within a room, and one or more rooms would belong within a building which belongs to an organization. To create an asset, use the following steps:

1. Click New in the upper right portion of the screen.
2. Type in a name of the asset to be created, and select the type of asset from the Type drop down list.
3. If you have Global System Administrator rights and there are other organizations available, click the magnifying glass next to the Organization text box to assign the asset to an organization. Note: If the asset has a parent, then it must be in that parent's organization, and this magnifying glass is disabled.
4. By default, discovered assets are not assigned to an organisation, and are unmapped. In order to update these assets, first click Remove to remove them from the unmapped folder, and then use the organisation picker, magnifying glass, to select the organization.

5. If it is the uppermost asset level, then click Remove near the Parent information. Otherwise, click on the magnifying glass and select the parent of the asset in question. Per the example, a Building is likely to be the uppermost asset type, so it would have no parent. However, when creating rooms, they would naturally belong in a particular building, so one would select the appropriate building here. (This also requires the upper level assets to be defined first.)
6. Click Save.

14.2. Assigning Devices to Assets

To map a device to the appropriate asset class, use the following steps for each device:

1. Select the device in question. The device may be in the Unmapped folder, so it may be necessary to click on the triangle next to the Unmapped folder to reveal it.
2. Under the asset information, select the asset to which the device belongs by clicking the magnifying glass next to the Parent information box. (In our example, a lock would belong within a cabinet, so this assumes that you have made at least one building, made at least one room and placed it within that building, and made the appropriate cabinet within the room, all according to the steps in the previous section.)
3. The device will then be assigned to that parent asset's organization.
4. Click Save.

14.3. Locks

It is possible to see all of the locks that belong to a particular asset (including all of its children) by selecting the asset in question, and then selecting the Locks tab on the lower portion of the screen.

14.4. Reports for Asset Registration

A report containing a list of all assets monitored by the system can be obtained by selecting the Asset List report in the lower left portion of the screen.

A report containing details of any particular asset is also available by selecting the specific asset from the upper half of the screen and clicking on the Asset Detail report in the lower left portion of the screen. The report will list all the basic data (location, parent name, type, and status) associated with the lock.

The information contained in any report can either be directly printed or exported into an Excel, Word, or PDF format by clicking the either the printer icon or the disc icon in the upper bar of the report.

15. Asset Types

The Asset Types screen is used to define classifications for assets. The actual instances of the assets and how they relate to a hierarchy are defined in Registration.

The TZ Centurion™ Server is installed with three default asset types that can be defined to organize the enterprise: Asset Level 1, Asset Level 2, and Asset Level 3. There are also asset types to reflect the TZ locks, readers, and other devices.

In order to edit the predefined asset types, select the appropriate line from the upper portion of the screen, and type in new values for the Name and Description fields. If it is conceivable that the asset type might contain other asset classes (or other asset classes may roll up into this asset class), then leave the Allow Children checkbox checked. Click Save to save these changes.

There are a total of three properties that can also be attributed to assets. Properties are essentially additional fields that can hold string values once the asset is actually instantiated in the Registration screen. The properties are defined under the Properties tab. To add a new property to an asset class, click New on the right side of the screen. A pop-up screen listing possible property types will appear. To give the property a meaningful name, click Modify, edit the appropriate field and click Save. Click Select to select the appropriate property and return to the Properties tab.

A maximum of three properties can be defined, and although different asset types can share the same property definition, the three property definitions must be allocated across all of the asset levels.

16. Sorting and Filtering Tables

Most tables and lists displayed by the TZ Centurion™ Server can be filtered and/or sorted by the criteria listed at the top of each table.

1. Click on the filter symbol ( ) next to the appropriate column heading to bring down a menu of sorting and filtering options.
2. Enter the appropriate criteria or click on the appropriate option.
3. Click Apply Filter if the drop down menu does not disappear automatically.
4. The filter symbol should turn orange, and the list should be filtered and sorted accordingly.

To remove the filter or apply another filter, simply click on the filter symbol again and repeat the process.

17. Operational Cards

Operational cards are any of a number of physical tokens (RFIDs, smart cards, iClass, PIC and similar) typically given to people to allow physical access to assets. The assignment of the operational card to the person is performed in the Operational Cards screen. The lower part of the screen has three tabs, each of which controls a different aspect of the access that a user has.

17.1. Contact Information

Before a card is assigned and physically given to a person, several procedures are usually performed in advance. Depending on the policies and practices of the institution, steps 1 and 2 may be done beforehand, so that only the steps 3 through 10 will be performed during day-to-day operation.

1. The system should be configured properly, with readers connected and mapped to specific locks.
2. A controlled number of cards are registered within the system via the Card Management screen.
3. When an individual is to be given a card, select the contact from the list on the top portion of the screen. In instances where a person may represent several organizations, they may have multiple entries. Select the entry that describes the use of the operational card. If the person is not listed in the top portion of the screen, select New from the upper right, and fill out the information below:
   a. Organisation: Select the organisation the user will be representing by clicking on the magnifying glass icon and choosing the organisation from the window that appears. With the TZ Centurion Server, only the organisation that actually owns and runs the system can be placed in this field.
   b. Person: Select the personal information of the user by clicking on the magnifying glass icon and choosing the correct person from the window that appears. If creating a new person within the system, click the magnifying glass icon and then click New button in the upper right portion of the screen.
   c. Association: From the drop down box, select the relationship of the person to the organisation.
   d. Start Date and End Date: Enter the range of time for which this contact information will be valid.
   e. Required Docs: This is an auxiliary field that can be used to hold identification numbers such as employee numbers, driver's license numbers, etc.
   f. All other fields in this screen are optional, but filling them out will help with the completeness and integrity of the data kept by the TZ Centurion™ Server.
   g. Click Save.
4. Select the card to be assigned to this person by clicking on the magnifying glass next to Card RFID.

   If there is no spare card, then cancel this card assignment step, create a new card via the Card Management screen or remove a card from someone else who no longer requires it via the Operational Cards screen and then return back to this step.
5. Click Save, then move onto setting the access rights and schedule for this contact as described in the next sections.

17.2. Access Rights

Access rights are granted in conjunction with the role an individual has with an organization. To set these:

1. Click on the Access Rights tab.
2. To grant a new set of access rights, click the New button at the top of the tab. To edit an existing set of access rights, select the appropriate line from the displayed list.
3. In this context, the only role that can be set is Asset Access (use the User Accounts Screen if you need to set other roles).
4. Set appropriate start and end dates for this set of access rights.
5. Select the set of assets to which the access rights will apply.
6. Click Save, then repeat the previous steps if more than one set of access rights is to apply to this contact.

17.3. Schedule

The schedule tab defines the days and times, along with the start and end date which a user can physically access assets via his or her card. Edit the information under this tab, including the start and end date along with the days of the week, and click Save.

18. Override Card

In most situations, when a card is scanned by a reader, the reader sends the corresponding information to the bridge, and ultimately to the server, where a decision is made to grant or deny access. An override card is a special card where the information is pushed to and kept at the bridge level, so that access can be given even during times of network outage for cases where the bridge may not be able to communicate with the TZ Centurion Server.

An override card is not subjected to the rules that are applied against the cardholder in the TZ Centurion Server and will open all locks that are mapped against a reader at the bridge level.

19. Remote Access

The Remote Access screen displays and controls the devices that monitor the assets of concern.

The top portion of the screen is used to locate the assets of concern. This list can be sorted and filtered by clicking on the funnel icon in the heading of the appropriate column or columns.

Once a set of assets is selected, all of the locks associated with the assets are listed in the bottom portion of the screen. This list can also be sorted and filtered by clicking on the funnel icon in the heading of the appropriate column or columns.

The correlation between the status icons and the color displayed by the TZ SlideHandle Indicator is shown in the table below.

TZ SlideHandle™	Device Status	Door State	Description
Solid Red 	Locked	Closed	Handle is down, unlocking is not enabled, door is closed
Solid Green 	Locked	Open	Handle is up (via authorised access), unlocking has timed out, door is open
	Unlocked *Push down on top of handle to unlock*	Open	Handle is up (via authorised access), unlocking is enabled, door is open
Flashing Orange 	Unlocked *Push down on top of handle to unlock*	Closed	Handle is down, unlocking is enabled, door is closed
		Open	Handle is down, unlcoking is enabled, door is open (For example, after handle was inadvertently closed with the door open)
Flashing Red 	Locked	Open	Handle is down, unlcoking is not enabled, door is open
	Error	Error	Handle opended with key
			Communication problem

In order to unlock a door from the user interface, click on the locked icon. If the lock is a TZ SlideHandle, the door should change to the unlocked state (flashing orange), and the user can physically open the door after pushing lightly on the top of the TZ SlideHandle. If the lock is a TZ Radial, the radial will be placed in the push-to-release mode.

In order to open a door from the user interface, click the closed door icon. If the lock is a TZ SlideHandle, the top will pop up and turn green. If the lock is a radial, the radial will eject the stud and the door will swing open.

Note that there is a subtle difference between the definition of unlocked (where a door or enclosure is physically closed, but is accessible by pressing a button, a door, or otherwise gaining access without further authentication), and open.

20. Monitoring

The Monitoring screen is used to view all active alarms and events within the system.

The alarms are presented in the top portion of the window. An alarm is a predefined condition that when violated results in a notification to some entity. The notification might be through a SNMP Trap, email or simply a prominent banner at the top of the page. An alarm will also be active if a TZ device (SlideHandle, Bridge, Wiegand translator) goes off line or is otherwise not in contact with the server. The definition of the alarms is discussed in the section on the network.

The events within the system are displayed in the bottom portion of the window. An event is any change in status of any component within the TZ Centurion System. This includes, but is not limited to, user's logging in to or out of the system, access cards being swiped and locks being open or closed. For most purposes, events are the everyday occurrences within the TZ system, but they do not include the alarms which are viewed separately in the top part of the screen.

The table and events can be sorted and filtered by clicking on the funnel icon in the heading of the appropriate column or columns.

20.1. Alarm Acknowledgement

When viewing alarms through Alarm monitoring page of the red flashing alarm panel at the top of the TZ Centurion Server interface, it is possible to acknowledge the alarms. This will prevent the acknowledged alarms from triggering the flashing red alarm box being displayed until they have been cleared and generated once again. This allows security departments who are constantly monitoring the server to ensure they have attended to all security and system error events.

20.2. Reports for Monitoring

A report that lists all of the alarm activity within the system can be obtained by selecting the Alarm Logs report in the lower left portion of the screen. When the report appears, it can be further filtered by entering the start and end dates in the appropriate fields and selecting OK.

A report that lists all of the events (card swipes, door openings and closings, users logging in, etc.) within the system can be obtained by selecting the Event Logs report in the lower left portion of the screen. When the report appears, it can be further filtered by entering the start and end dates in the appropriate fields and selecting OK.

The information contained in any report can either be directly printed or exported into an Excel, Word, or PDF format by clicking the either the printer icon or the disc icon in the upper bar of the report.

21. User Organisation

The general management of organisations to the TZ Centurion Server is done through the User Organisation screen. The User Organisation screen contains all the contact information of the organisation running Centurion Server. For Global System Administrators, it contains all the contact information of all the organisations, and the means to create, delete, or inactivate other organisations.

To make an organisation, or to edit information about an existing organisation, use the following steps:

1. If editing an existing organisation, select the organisation from the upper portion of the screen. If adding a new organisation, click New from the upper right portion of the screen. To add a new organisation, you must have Global System Administrator rights.

2. Enter the following fields:

Name: Enter the name of the organisation.

All other fields in this screen are optional, but filling them out will help with the completeness and integrity of the data recorded by the TZ Centurion Server.

Global System Administrators may delete and/or deactivate non-primary organisations. Once an organisation has been deleted, all its contacts are deleted from the system and will no longer be accessible. Therefore, a confirmation message is displayed. Deactivating an organisation similarly deactivates all its contacts. However inactive organisations and contacts are still accessible. If you decide to re-activate an organisation, you must manually re-activate all its contacts from the User Accounts screen.

21.1. Organisation Information

The basic contact information for the organisation can be reviewed and edited under the Organisation Information tab. Simply edit the appropriate fields and click Save.

21.2. Contacts

The Contacts tab lists all of the accounts that belong to the organisation. Similar to the User Accounts screen, it is possible to edit existing accounts or add new accounts. However, it is not possible to modify or add access rights, credentials, or schedules. That information must be explicitly added through the User Accounts screen.

To add a new account or edit an existing account, use the following steps:

1. If editing an existing account, select the appropriate line. If the list is large or unwieldy, it is possible to sort and filter the list to find the correct entry. If adding a new account, click the New button on the right side of the screen. A new line should appear in the table on the bottom portion of the screen.
2. Click the rectangle under the Person column to make a magnifying glass appear. Click on the magnifying glass in order to select which person to add or edit.
3. Modify the start date, end date, work phone, work email, and contact status as appropriate.
4. Click Save to save the changes.

21.3. Notifications

The information under the Notifications tab defines who, how, and when a notification is sent. A notification can be sent when an event or alarm takes place or when a card is issued. Events are sent as an Email.

To add a new notification or edit an existing notification, use the following steps:

1. If editing an existing notification, select the appropriate line. If adding a new notification, click the New button on the right side of the screen. A new line should appear in the table on the bottom portion of the screen.
2. Click the rectangle under the Method column and select Email.
3. Under the Notification column, select what type of condition will cause a notification to be sent. The options are Alarm, Event, or Card Issue.
4. In the address field, enter the Email address the notification is to be delivered to.
5. Click Save to save the changes.

21.4. SNMP

TZ Centurion™ Server supports SNMP v1 and v2 to integrate access control into network management systems.

The individual notifications (i.e., traps) are defined under the SNMP (Simple Network Management Protocol) tab. To add a notification, click New in the center portion of the screen, and then select the notification type by clicking the gray box underneath the Trap Type heading.

The system and network information (e.g. IP addresses and public/private strings) required to set up SNMP is configured in the System Settings screen.

21.5. SYSLOG

TZ Centurion Server supports sending all logging details to a third-party syslog server. This allows for external auditing and logging of all events that occur on the TZ Centurion Server and connected devices.

To enable this functionality the Syslog server IP address and port need to be set in the System Settings page.

21.6. Reports for User Organisation

A report containing a list of all organisations which either have assets in the system or have contacts within the system can be obtained by selecting the Organisation List report in the lower left portion of the screen.

A report containing details of any specific organisation is also available by selecting the specific contact from the upper half of the screen and clicking on the Contact Detail report in the lower left portion of the screen. The report will list the organisation along with any and all contacts associated with that organisation.

A report containing all of the assets belonging to a particular organisation can be obtained by selecting the specific contact from the upper half of the screen and clicking on the Organisation Assets report in the lower left portion of the screen. The report will list all of the times the person has been issued and/or used a card.

The information contained in any report can either be directly printed or exported into an Excel, Word, or PDF format by clicking the either the printer icon or the disc icon in the upper bar of the report.

22. Card Management

Physical access to any asset is granted in one of two ways: Either an authorized user gives a command via the TZ Centurion™ Server Remote Access page, or a person is issued an Operational Card that can be swiped at a reader associated with the asset. The management of operational cards has two separate elements: First, the management (registration and cataloging) of the cards themselves is performed here in the Card Management screen. Second, the assignment of a card to a person is performed from:

a. the Operational Cards screen if you are an operator, or

b. the User Accounts screen if you are an administrator.

The complete list of operational cards registered within the system is displayed in the top portion of the screen. The list can be sorted and filtered by clicking on the funnel icon in the heading of the appropriate column or columns. To view the details associated with any card, simply select that card from the list. Note: Unless you are a Global System Administrator, cards assigned to contacts outside your organisation will not be displayed.

The details of a card are displayed on the bottom part of the screen under the three separate tabs.

> Under the Card Information tab, the card number and card status is displayed. Card status can be either active, stolen, inactive, malfunctioning, or destroyed. If this field is changed from anything except active, the card will be immediately unusable. If the card is an override card, then the corresponding box will be checked.

> Any activity associated with a card can be viewed under the Card Activity tab.

> The current owner of the card can be viewed under the Card Owner tab.

To register a single card with the system, perform the following steps:

1. Select the card reader at which the card will first be swiped.
   a. Click Set Card Reader on the upper right portion of the screen.
   b. Select the appropriate card reader from the list that appears,
   c. Click Select.
2. Click New in the upper right portion of the screen. The information on the lower portion of the page should be cleared.
3. Swipe the card at the reader. The card number should appear within a few seconds in the Card Number field.
4. Enter a value under Card Alias. Because systems differ in how the card numbers are transmitted and decoded, if a number is written on a card it may appear differently than what appears in the Card Number field. The string entered here will appear on reports and records instead of the string that appears in the Card Number field.
5. Click Save on the upper right portion of the lower half of the screen. The card information should appear in the list in the upper portion of the screen, and the card is now ready to be assigned to someone via the operational card screen.

To register many cards within the system, perform the following steps:

1. Select the card reader at which the card will first be swiped.
    a. Click Set Card Reader on the upper right portion of the screen.
    b. Select the appropriate card reader from the list that appears,
    c. Click Select.
2. Click Register Cards from the upper right portion of the screen. The information on the lower portion of the page should be cleared.
3. Swipe the first card at the reader. The card number should appear within a few seconds, and will automatically be saved by the system. The card information should appear in the list in the upper portion of the screen.
4. Repeat step 3 for all cards, and click End Registration. All cards are now ready to be assigned to someone via the operational card screen.

22.1. Reports for Card Management

A report containing a list of all active cards within the system can be obtained by selecting the Card List report in the lower left portion of the screen.

A report containing all the details and activity associated with any card is also available by selecting the specific card from the upper half of the screen and clicking on the Card Detail report in the lower left portion of the screen.

A report listing all the activity associated with any card is also available by clicking on the All Card Activity report in the lower left portion of the screen.

A report containing all of the cards associated with a particular organisation can be obtained by selecting the specific contact from the upper half of the screen and clicking on the All Cards in Organisation report in the lower left portion of the screen.

The information contained in any report can either be directly printed or exported into an Excel, Word, or PDF format by clicking the either the printer icon or the disc icon in the upper bar of the report.

23. User Accounts

The general, unrestricted management of users to the TZ Centurion™ Server is done through the User Accounts screen. More restricted and controlled management of physical visits is accomplished via the Operational Cards screen.

Every user within the system must have three critical elements:

- A set of personal information (name, home phone number, personal e-mail and personal cell phone) which is unique to that person.
- At least one set of contact information associated with an organisation he or she currently represents.
- One or more sets of access rights.

The upper portion of the User Accounts screen lists all of the contacts currently registered in the system. (A contact is almost synonymous with the concept of an account in that a person can have several accounts with different companies at the same time)

For creating new users, it is recommended to use the User Registration Wizard, which simplifies the process of associating any newly created user with a new or existing card, as well as granting the new user the appropriate access rights and schedules. For editing existing users, or if you want to add new users without using the Wizard, then use the specific functions as described below after the Wizard section.

23.1. User Registration Wizard

To begin using this Wizard, click the User Registration Wizard button in the upper right portion of the screen. The screen progression for this Wizard is as follows:

1. Contact Details screen -

On this screen, fill out the fields as appropriate for the new contact. Apart from the personal details (most of which are optional), the following additional fields are provided:

a. Organisation: From the drop down box, select the organisation the contact will be representing.

b. Association: From the drop down box, select the relationship of the contact to the organisation.

c. Start Date and End Date: Enter the range of time for which this contact will be valid.

d. Enable Credentials: If this user will be assigned a role that allows login privileges to the server, tick this box and then enter a User Name and initial Password for the user.

Once the information has been entered, click Next.

2. Card Information screen -

This screen is optional. It allows an existing or newly created card to be assigned to the contact.

a. If you are creating a new card, select the radio button labeled New, then use the associated fields to enter the new card details. Note that the card number can be automatically entered by swiping the new card at a previously selected RFID Reader (use the Set Card Reader button to set this reader).

b. If you are assigning an existing card, select the radio button labeled Existing, then use the associated controls to select the card to be assigned.

When you have finished assigning a card, or are skipping over this step, click Next.

3. Access Rights screen

This screen is optional. It allows access rights and/or schedules to be set for the Contact.

Access rights are granted in conjunction with the role an individual has with an organisation. To set these:

a. In the table within this screen, click in the Role field and select from the list of roles. A complete description of roles is discussed here.

b. Set appropriate start and end dates for this set of access rights.

c. Select the set of assets to which the access rights will apply to.

d. Repeat the previous three steps if more than one set of access rights is to apply to this contact

Below the access rights table are the schedule-related fields. These define the days and times, along with the start and end date which a user can physically access assets via his or her card. Set these fields as required.

When you have finished setting access rights and/or schedules, or are skipping over this step, click Finish

23.2. Adding or Editing Users (non-Wizard)

To make a user and give access, or to edit information about an existing user, use the following steps:

1. If editing an existing user, select the user from the upper portion of the screen. Because some users may have multiple entries (at least one entry per organisation that they represent), be careful to select the right item. If adding a new contact, click New from the upper right portion of the screen.

2. Enter the following fields:

   a. Organisation: Select the organisation the user will be representing by clicking on the magnifying glass icon and choosing the organisation from the window that appears.

   b. Person: Select the personal information of the user by clicking on the magnifying glass icon and choosing the correct person from the window that appears. If creating a new person within the system, click the magnifying glass icon and then click New button in the upper right portion of the screen.

   c. Association: From the drop down box, select the relationship of the person to the organisation.

   d. Start Date and End Date: Enter the range of time for which this contact will be valid.

   e. Required Docs: This is an auxiliary field that can be used to hold identification numbers such as employee numbers, drivers license numbers, etc.

   f. All other fields in this screen are optional, but filling them out will help with the completeness and integrity of the data recorded by the TZ Centurion Server.

   g. Click Save.

3. Give the contact access rights by clicking on the Access Rights tab. Access rights are granted in conjunction with the role an individual has with an organisation. To edit or make a new set of access rights, use the following steps:

   a. To grant a new set of access rights, click the New button on the right. To edit an existing set of access rights, select the appropriate line from the upper portion of the screen.

b. Select the appropriate role by clicking on the magnifying glass located in the role column. A complete description of roles is discussed here.

c. Set appropriate start and end dates for the set of access rights.

d. Select the set of assets that the access rights shall apply to.

e. Click the Save button on the left.

f. If the user has a role that allows login privileges, the login credentials and initial password are set under the Credential tab.

The user can now be given an operational card by an operator, or if the appropriate privileges have been set, the user should now be able to log in to the system.

To delete a user, click the Delete button, and click Yes to confirm. If the deleted contact was assigned an operational card, then the card will be made available to another user.

23.3. Reports for User Accounts

A report containing a list of all contacts can be obtained by selecting the Contact List report in the lower left portion of the screen.

A report containing details of any particular contact is also available by selecting the specific contact from the upper half of the screen and clicking on the Contact Detail report in the lower left portion of the screen. The report will list the first and last name of the contact as well as any and all of the contact information (city, state, email, and phone) associated with every company the person may represent.

A report containing all of the times that a contact has used an RFID or other card to access an asset can be obtained by selecting the specific contact from the upper half of the screen and clicking on the Card Usage report in the lower left portion of the screen. The report will list all of the times the person has been issued and/or used a card.

The information contained in any report can either be directly printed or exported into an Excel, Word, or PDF format by clicking the either the printer icon or the disc icon in the upper bar of the report.

24. Roles

A role defines the type of relationship between a person and an organisation, and any user that interacts with the system has a role. Note that in order to use login privileges, the user must have an association or contact with the main organisation. In the basic TZ Centurion Server, the following roles are defined:

24.1. Global System Administrator (GSA)

A global system administrator is a person responsible for maintaining the integrity of the overall TZ Centurion Server software. They have access to any and all screens within the system. They can view all assets. And they can be given operational cards. There must always be an individual with global system administrator privileges.

24.2. Administrator

An administrator is a person responsible for maintaining some subset of the assets monitored by the TZ Centurion Server software. They have access only to the screens located under the Administration navigation node. They can only view assets that are assigned to them. They can be given operational cards.

24.3. Operator

An operator is a person responsible for monitoring some subset of the assets, and assigning operational cards to other individuals. They have access only to the screens located under the operations navigation node. They can only view assets that are assigned to them. They can be given operational cards.

24.4. Configurator

A configurator is the person responsible for making the asset and data fields within the TZ Centurion Server reflect the physical reality of the application. They have access only to the screens located under the operations configuration node. They can only view assets that are assigned to them. They can be given operational cards.

24.5. Asset Access

A person whose role is asset access may be given an operational card, but will not have any login access to the system.

24.6. No Access

If an individual is ever given a role of no access, they will be denied access to the assets associated with their contact information. Since an individual may represent different organisations, and therefore may have multiple sets of contact information, this only applies to the current set of contact information.

25. Server Side Performance Enhancements

The TZ Centurion Server has several enhancements, which allow for a speedy and reliable operation of the system. Caching is performed on the server-side of the Card Access rules so that in the event that a card is swiped the data is retrieved from a high-speed in-memory database rather than a slower on-disk database. As a result, this in-memory database needs to be updated from the on-disk database. By default, this occurs every one minute, but can be tweaked using CacheUpdateInterval setting. As a result of the 1 minute cache update, changes to end users will not take affect for up to 90 seconds (60 seconds for update trigger and 30 seconds for processing).

The web browser data is also cached on the client side, to prevent repetitive requests for same data from the server. This cache can be cleared by press Shift+F5 on the web browser client access the TZ Centurion Server.

26. Centurion Server Troubleshooting

To assist with troubleshooting any errors that are experience with the TZ Centurion Server software, there is a troubleshooting logfile. This logfile specifically logs the following areas of action to a file:

- User Login
- License Management
- User Management
- Device Registration
- Device Discovery
- Access Card Swipe.

This logfile can be submitted to TZ Technical support for further analysis and will provide debugging information, which can be useful when the server is suffering database connectivity or performance issues. By default these logs will have a maximum size of 1MB and 20 rotations. This can be changed in the TZServerServices web.config file. The default location for the troubleshooting logfile is:

C:\inetpub\TZServerSite\TZServerServices\Log

27. System Settings

Parameters that define the operation and policy compliance of the TZ Centurion Server are located in the

System Settings screen. A description of each parameter is given below:

BridgeStreamingRate

The rate (number of seconds between consecutive values) at which bridges send sensor data to the server.

ContactTimeoutInMinutes

Number of minutes between sensor updates before a bridge is assumed to be unreachable. Note that this may need to be adjusted for exceptionally long BridgeStreamingRates.

DefaultContactScheduleToAlways

Newly created contact is a assigned schedule for every day, any time, for 10 years.

DiscoveryTimeoutInMinutes

Number of minutes until a discovery is assumed to have failed.

HumiditySensor Unit

Units for humidity sensor readings.

IsLicenseAccepted

Whether or not any user has accepted the EULA before first time application use.

LicenseType

Licensed product type: [Express, Server, Datacenter, etc.]

LoginFailedAttemptIntervalInMinutes

Number of minutes until login attempts reset. The number of failed attempts only locks a user out if they are within a configured amount of time.

LoginFailedAttemptLimit

Number of times before a login fails in the above specified period of time.

LogRefreshInSeconds

Number of seconds to wait before refreshing alarm and event logs.

OpenAllDevicesDuration

Default interval (in minutes) to open all devices for a visit configured to unlock devices right away, instead of by a card.

PasswordStrengthExpression

Regular expression for validating the password.

PasswordStrengthMessage

Used for password validation (corresponds with regular expression).

RemoteConfirmation

Designates whether or not a confirmation dialog is displayed when opening doors and unlocking locks.

ServerHostName

Hostname of server sent to bridge during registration so it knows where to call back, typically an IP address.

ServerPath

Path to hardware event handler on server, sent to bridge as part of registration so it knows where to send its events.

ServerPort

Port to send to bridges to call back server.

ServerUrl

The full URL path from where the Silverlight application is hosted.

SmtpFrom

The FROM field for outbound email notifications.

SmtpPassword

The password for authenticated SMTP email notifications.

SmtpPort

The mail server port.

SmtpSecurity

The security type (implicit, explicit, secure, or unsecure) used by the SMTP server.

Smtp Server

The SMTP server address.

SmtpUser

The username or login for authenticated SMTP email notifications.

SnmpServer

The IP address of the SNMP server address.

SnmpTrapPort

The SNMP trap port.

SyslogPort

The port the Syslog daemon is listening on.

SyslogServer

The IP address the Syslog server is listening on.

TempCardDuration

The enforced duration of an access right created by a viewer.

TempCardRole

The role a viewer can assign to an access right.

TemperatureSensorUnit

Intended to be units for temperature readings (Fahrenheit not implemented yet).

VisitorDummyEmailID

Filler email used when creating users of type “visitor.”

VisitorDummyPassword

Filler password used when creating users of type “visitor” (not used in TZ Centurion Express.)

To edit the values of the parameter, simply highlight the appropriate line from the top portion of the screen, edit the value of the field in the lower portion of the screen, and click Save.

28. System Application Settings

All of the TZ Centurion system application settings are initialized and defined in the following configuration file:

C:\inetpub\TZServerSite\TZServerServices\Web.config

Inside a xml block tagged <appSettings>.

CacheUpdateInterval

Default: 1 minute

Controls how often the internal cache is updated. A value of 0.5 will cause cache update every 30 seconds, so that events such as card swipes are reported in the event log closer to real time.

AutoRegisterUnreachableBridges

Default: true

Controls whether the server tries to automatically reconnect to bridges that are unreachable. If you set this False, then you will have to manually register bridges once they become reachable again in order to bring them online.

RebuildIndexFrequency

Default: 7 days

Controls how often the server's database has its index rebuilt. Consider reducing this period for a very large bridge network. To disable this feature, set the value to 0.

BridgeMessageProtocol

Default: True

Is used in all communications with bridges. This can be changed to https to make it more secure if really required. Please note that http will have better performance over https.

IncludeVerboseInTroubleshootingLog

Default: False

There will not be any messages from Bridge in the troubleshooting log. In case the messages have to be analysed, set this to True which will include all such verbose logging which are large in size.

infrastructure
protection

ixp.tz.net