Industrial Control

Z45x Series Industrial Controllers

User Manual – UM002R4
Revision B
December 23, 2020

1891 N. Gaffey St. Ste. E
San Pedro, CA 90731

p. 310.241.2973

support@ctekproducts.com
www.ctekproducts.com

Contents

1. **Introduction** **5**
2. **Applicable Models** **5**
   - Z4500XXX 5
   - Z4550XXX 5
   - Z44009XX 5
3. **Getting Started** **6**
   - Default Factory Settings 6
   - Administrative Access 7
4. **Controller Indication/Terminations/Switches** **9**
   - Digital Outputs 9
   - Wake-Up 9
   - Analog/Digital/Pulse Inputs 9
   - Power Input 11
   - RS-485 Serial Interface 11
   - RS-232 Serial Interface 11
   - Reset Switch 11
   - Default Switch 11
   - LAN Led 11
   - Service Led 11
   - Link Led 12
5. **Wireless Network Activation** **12**
   - Prerequisites 12
   - Activation 12
   - Installing Radio Network Specific Firmware 12
   - APN Selection and Account Provisioning 13
   - For Legacy CDMA Carriers 13
   - For Legacy GSM Carriers 13

6. **Security** **14**
User Accounts 14
Security Preferences 14
General Configuration 16
Web Administration 16
IP White List 16
SMS Management 16
White List Status (SMS) 16
SSH Access 16
Additional Security Features 17
Multiple Failed Login Attempts 17
Authlogread 17
Intrusion Detection 17
7. **Device Profile** **17**
Device Network Profile 17
Gateway Configuration 17
Client Configuration 17
Application Parameters 18
Location 18
Application Alarming 18
Application Logging 18
Email Configuration 18
Dashboard Groups 18
Dashboard Options 18
8. **Local Interfaces** **18**
Port Forwarding 18
RS232/RS485 Ports 19
RS232/RS485 Options 19
9. **Tunneling and Encryption** **20**
GRE Tunnels 20
IPsec Tunnels 21

System-Wide IPsec Tunnel Options 21
Individual IPsec Tunnel Options 21
10. **Time and Location Source 23**
Cellular Network 23
Network Time Protocol (NTP) Server 23
GPS Location 23
11. **Location Source 23**
12. **SkyCloud Services 23**
13. **Tools 24**
Flash Update Client 24
Backup and Restore 24
14. **Applications 24**

Introduction

Welcome to the Ctek Z-45 Series Controller User's Guide. The Z-45 Series is a gateway applications platform that provides advanced monitoring and control features over wired and wireless infrastructure and cellular 4G/LTE service on all North American networks with fallback 3G service appropriate for that network. This User's Guide will explain the basic operation of the application platform and router, and take you through the necessary settings to get your wireless application online securely. Additional information concerning many of the advanced features of the Z4550 is found in TechNotes available at www.ctekproducts.com.

Applicable Models

Z4500XXX

Z4550XXX

Z44009XX

Getting Started

Default Factory Settings

Factory default settings are defined in the table below. Factory settings can be restored any time by pressing and holding the default switch for 5 seconds and releasing it when the service and link LEDs begin a repetitive (red/orange) flashing routine. At that point the device will reboot (power-cycle) and will return to service with the factory defaults in place.

Setting or Parameter	Factory Default
Administrative User ID	ctek *** Change after first login ***
Administrative password	ctek *** Change after first login ***
Administrative IP address	192.168.1.10
Network Configuration	Gateway
DHCP Server	Enabled
Administrative LAN and WAN port	Port 80 – See security section below
Firewall Status	Enabled – See security section below
WAN Ping Response	Disabled – See security section below
NAT Traffic to WAN	Enabled – See security section below
XML Interface	Disabled – See security section below
IP White List	Disabled – See security section below
SMS Management	Disabled – See security section below
SMS White List	Disabled – See security section below
SSH (Secure Shell) Access	Disabled – See security section below
SSH User ID	root – See security section below
SSH Password	pass – See security section below
Enable HTTPS	Disabled – See security section below
Connection State (WAN)	Enabled
Time Source	Cellular Network
Location Source	GPS (Internal)
DNS Address Source	Acquire from Wireless Network
Radio module firmware	Verizon - SWI9X15C_05.05.63.01 or newer

Administrative Access

All administration and configuration is accomplished using the web UI, which can be accessed locally throughout the Ethernet connection or over the air through the WAN connection after the unit is connected to a cellular network.

To use the local interface connect a computer to the controller's Ethernet port using a standard Ethernet cable. Using a web browser connect to the login page using the administrative IP address and the default login and password. Once you are successfully logged in the **Quick Panel** display shown in Figure 1 will be presented.

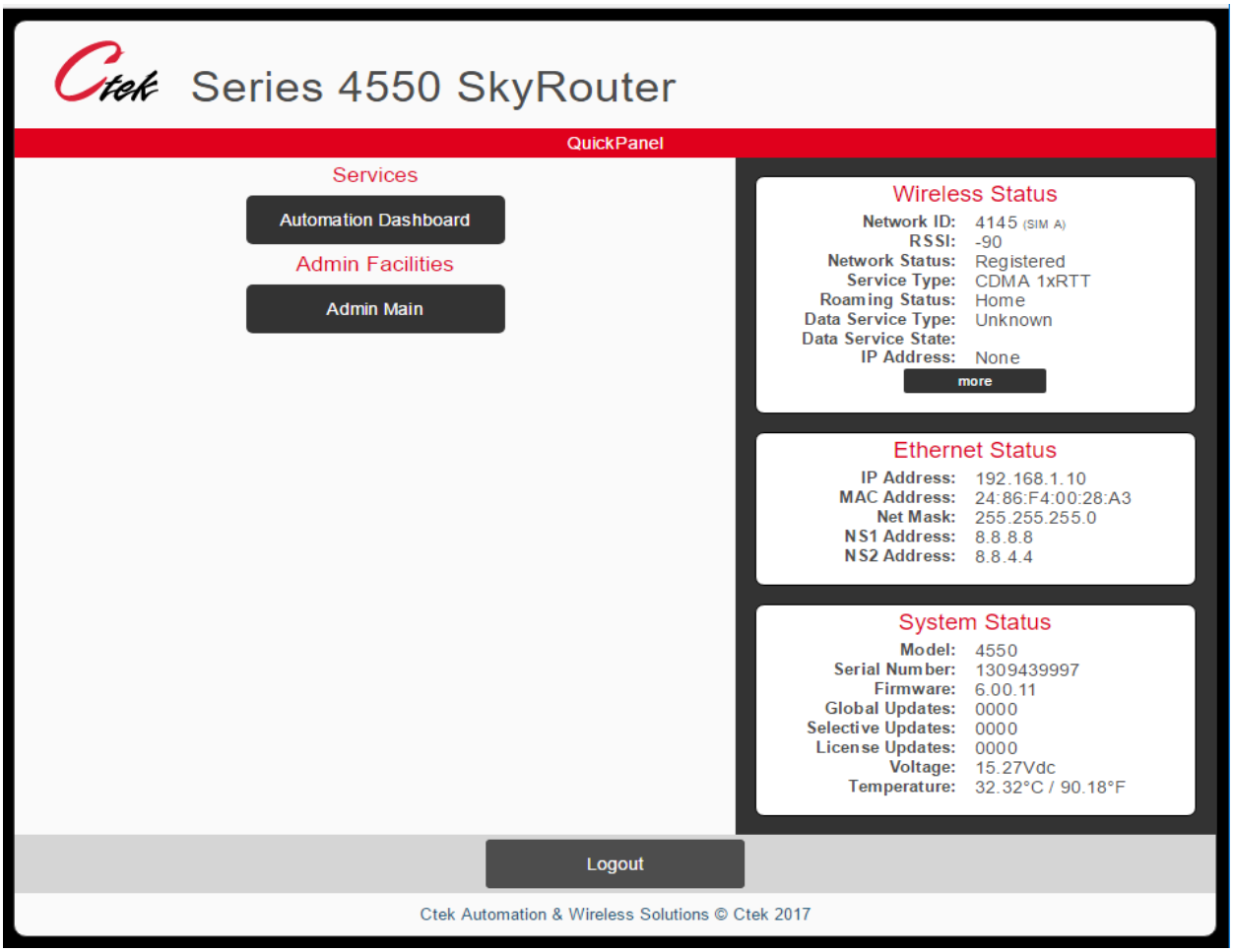


Figure 1

The Quick Panel display presents an overview of the network and equipment status, and provides navigation to the Administrative functions. The Quick Panel status information is a snapshot in time and must be refreshed to observe changes in dynamic parameters such as network connections or signal strength. The Admin Main button on the Quick Panel will display the main administrative screen as shown in Figure 2. Note that the main admin screen maintains the Quick Panel's status display, and offers navigation to all the controller's administrative functions.

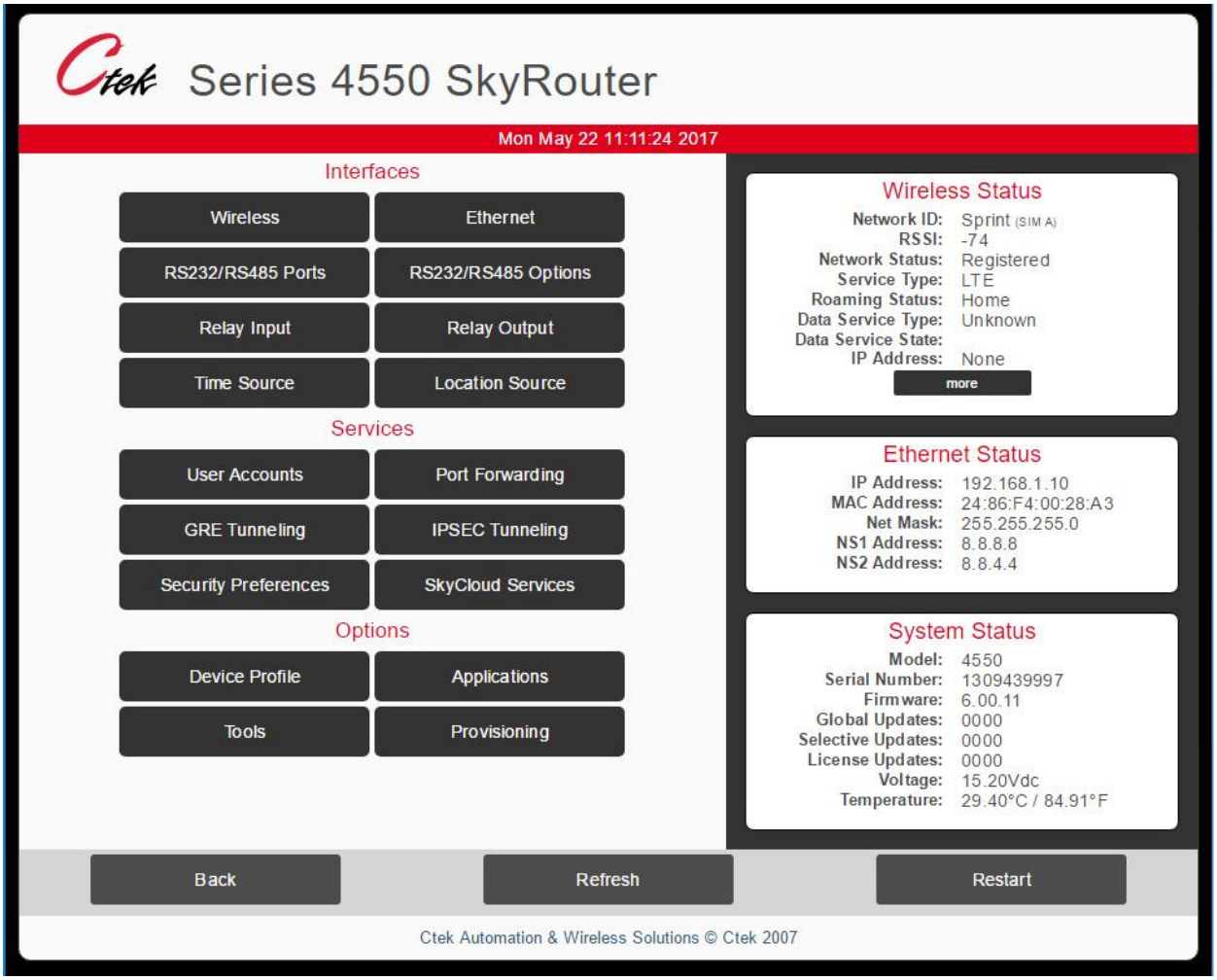
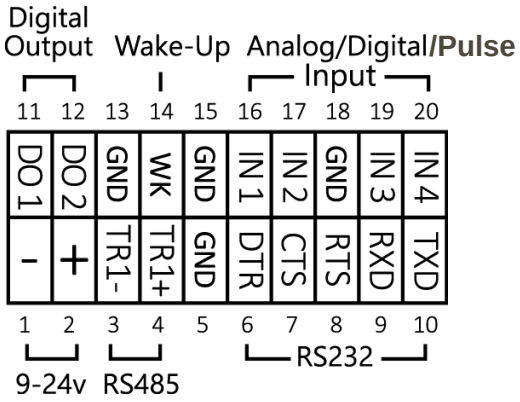


Figure 2

Controller Indication/Terminations/Switches

The updated Z45x Series controllers have a few I/O changes that make it a more versatile package for a wide range of applications. Below is a diagram of the new block terminations.



Digital Outputs

The controller supports 2 digital outputs. Each output is an open drain configuration rated for 250ma at 24Vdc.

Wake-Up

A wake-up signal allows the device to come out of low power state on trigger.

Analog/Digital/Pulse Inputs

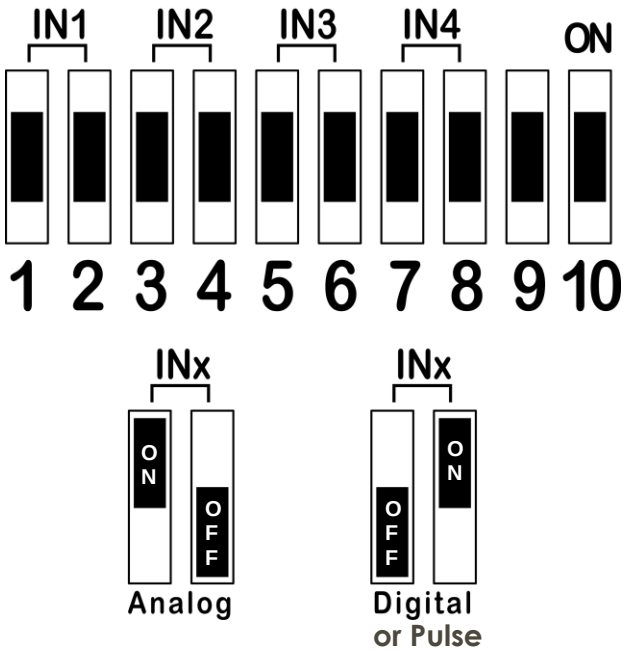
The controller has 4 available inputs that can be configured as either digital, pulse or analog. Configuration options associated with the 4 inputs differ between Revision A units and Revision B units. The mode of operation is user selectable using the dip switches on the bottom of the device. The images below show the dip switch configuration for Revision A and Revision B units.

Digital/Pulse Input Configuration on Revision A and B Units - In digital/pulse mode, an internal pull up to 3.3Vdc allows for direct connect of dry contacts. You may also configure an external pull up or digital source of up to 24Vdc if required.

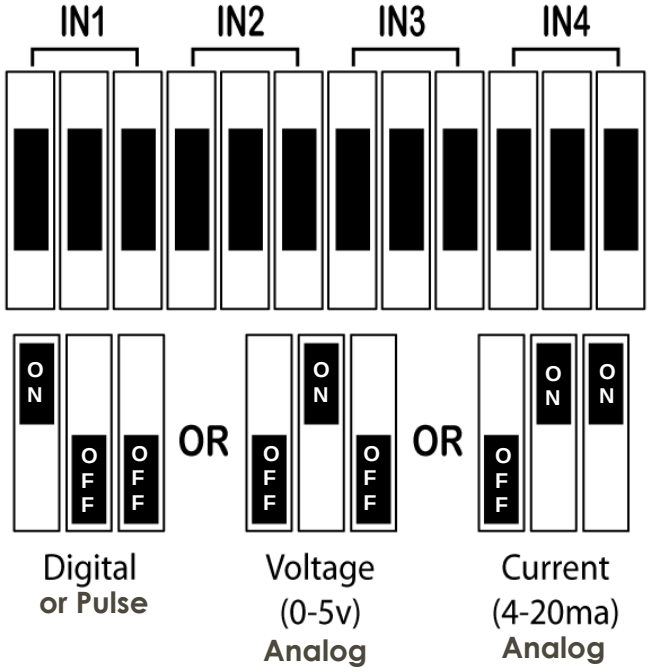
Analog Inputs on Revision A Units - In analog mode, inputs may be configured for sensing standard 0-5Vdc sources.

Analog Inputs on Revision B Units - In analog mode, inputs may be configured for sensing standard 0-5Vdc or 4-20ma sources.

Revision A Configuration Switches



Revision B Configuration Switches



Power Input

The device requires 9-24v DC. The power input also has reverse polarity protection.

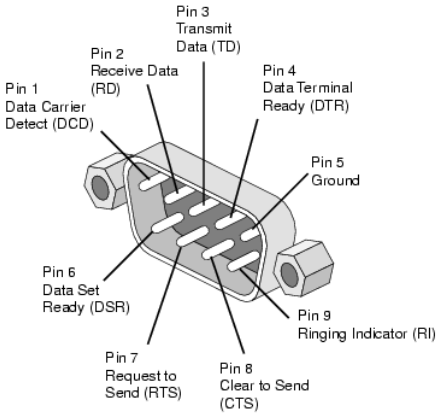
RS-485 Serial Interface

A two-wire RS485 interface is available. TR1- for data coming in and TR1+ for data going out. It is also recommended to use the one of the available ground pins (GND) to minimize signal interference.

RS-232 Serial Interface

A complete RS-232 DCE type interface is provided on pins 6-10. The table below shows the pins and signal direction. To avoid confusion, the corresponding pins for a standard DB9 connector are also shown.

Signal (Z45x Pin)	DB9 Pin	Direction
DTR (6)	4	Input
CTS (7)	8	Output
RTS (8)	7	Input
RXD (9)	2	Output
TXD (10)	3	Input



Reset Switch

The reset switch provides a software reboot of the device.

Default Switch

Perform a factory default by holding the default button for 5 seconds, until the Service and Link LEDs blink Orange/Red in unison and release. The device will be set to factory defaults and reboot.

LAN Led

The LAN LED will blink to indicate traffic on the Ethernet port of the device. If there is no traffic or no cable is plugged-in, then the LED will remain off.

Service Led

The service LED will blink Orange while it attempts to connect with a cellular tower. Upon success the LED will remain solid. A solid Green LED indicates a good signal level of -88 dBi or better. Anything less than -88 dBi will result in a Yellow LED to indicate poor signal.

Link Led

The Link LED will remain solid if the unit has established a data connection. A Red LED indicates LTE service. A Yellow LED indicates that the device has a low speed data connection. In other cases the LED may blink to indicate a process is being performed or it will remain off.

Wireless Network Activation

Ctek's Z-45 Series Controllers are capable of operating on North American LTE networks on bands 2, 4, 5, 13, 17, and 25 with fallback to the appropriate 3G network for the selected carrier. It will also operate globally on HSPA (UMTS) networks on bands 1,2,4,5, and 8

Prerequisites

Before you start, you must have:

1. A cellular data account with your selected carrier
2. A SIM card issued by that carrier that conforms to the 2FF form factor
3. At least one antenna suitable for the bands that will be used
4. A source of DC power between 9 and 24VDC

Activation

1. Insert the SIM card
2. Connect the DC power source to the Z4550 and power up
3. Connect a computer to the Ctek controller using an Ethernet cable, a browser, and the default administrative IP address
4. On the Provisioning/Radio Update screen verify that the radio firmware is correct for the network you are using
5. If the firmware is correct, proceed to APN Selection and Account Provisioning, otherwise install the correct firmware using direction in the following section.

Installing Radio Network Specific Firmware

1. On the Provisioning/Radio Update screen, select the correct firmware for the network you are using
2. Press the Update Radio button – This process will take between 2 and 3 minutes to complete
3. The SVC and Link LEDs will begin an alternating green pattern
4. The Status button on the Radio Update screen will display the network firmware that is being loaded
5. After a 2 – 3 minute delay the Status button will indicate that the radio programming has completed
6. The LEDs will simultaneously blink green indicating that the programming was successful
7. If the programming step encountered a problem the LEDs will simultaneously blink red/yellow

8. Restart or power cycle the unit

APN Selection and Account Provisioning

Important Note:

For the purposes of this manual, we divide the carriers (network operators) into two groups, legacy CDMA carriers, e.g. Sprint and Verizon, and the legacy GSM group, which is comprised of all other networks. In terms of provisioning the wireless account, especially APNs, these two groups present very different behaviors.

Legacy CDMA carriers use an over-the-air provisioning mechanism to "push" the appropriate APNs and settings to the radio module when it connects to the network. Under normal operation, this process is automatic and there should be no need to manually configure an APN. Legacy CDMA carriers currently use APN profile configuration (slot) 3 for the operational APN.

Legacy GSM carriers do not use an over-the-air provisioning mechanism. You must enter the carrier provided APN in APN profile configuration (slot) 1. Some legacy GSM carriers may also require you to enter a User Name, Password, and authentication type along with the APN.

For Legacy CDMA Carriers

On power-up, when the correct firmware is loaded, will automatically provision over the air, obtain an IP address from the network, and light the Link LED. This process will take between 1 and two minutes. If the Link LED is red it indicates an LTE connection, if the Link LED is green it indicates 3G connection.

For Legacy GSM Carriers

After the restart performed in step 8 of section 3.3 the unit will complete its reboot cycle. When the unit completes its boot cycle reconnect with a browser. On the Wireless Interfaces screen enter the APN specified by your carrier. Optionally, you may also need to enter a User Name, Password, and select an authentication type. When the required information has been entered perform a restart or power cycle. When the unit completes its reboot cycle it will obtain an IP address from the network, and light the Link LED. This process will take between 1 and 2 minutes. If the Link LED is red it indicates an LTE connection, if the Link LED is green it indicates 3G connection.

Security

Properly configured, Ctek hardware is the most secure cellular router and controller available in the marketplace. However, the security provided is only as good as the thought given to its administration. Factory default settings disable all access mechanisms with the exception of HTTP access on port 80. Configure User Accounts and Security Preferences as a first line to secure your system.

User Accounts

Selecting User Accounts brings the screen shown in Figure 3 below.

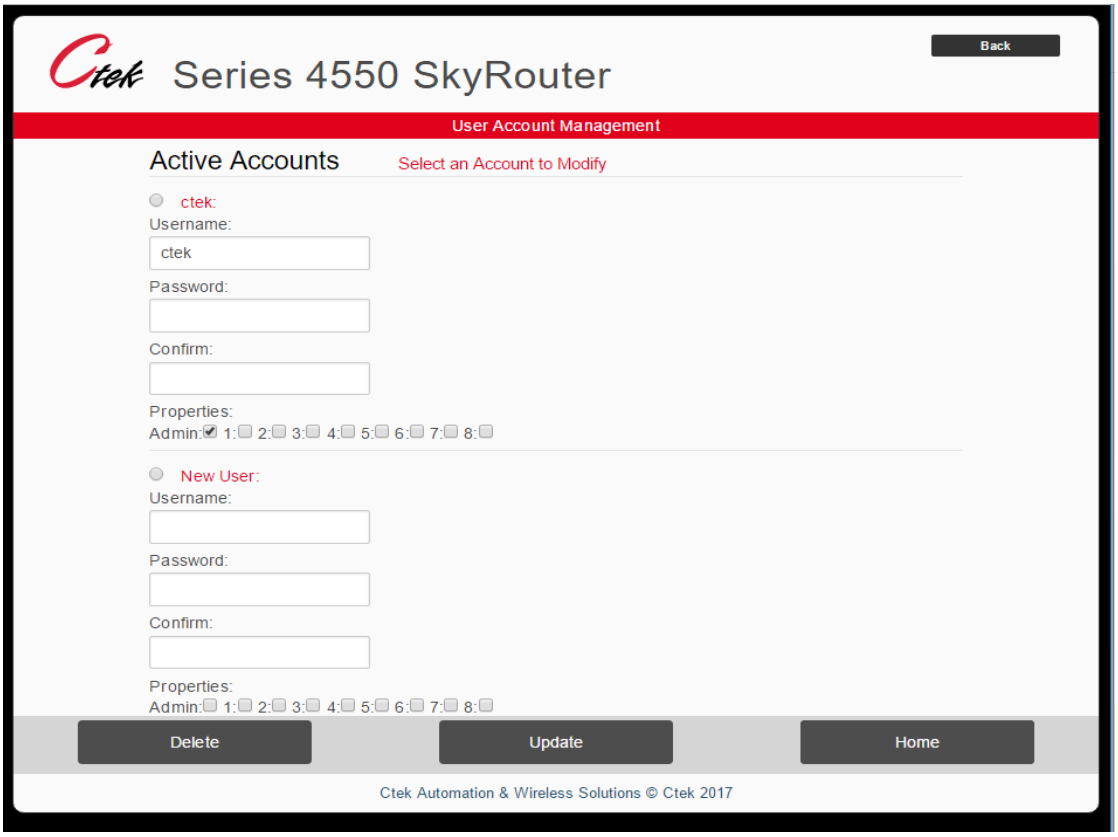


Figure 3

The default account can be modified but cannot be deleted. Ensure that at least 1 user has **Admin** privileges.

NOTE - The default User ID and password for Ctek's controllers is well known. Failure to perform this step exposes the user's equipment to unauthorized access and tampering.

Security Preferences

Selecting Security Preferences displays screen shown in Figure 4.

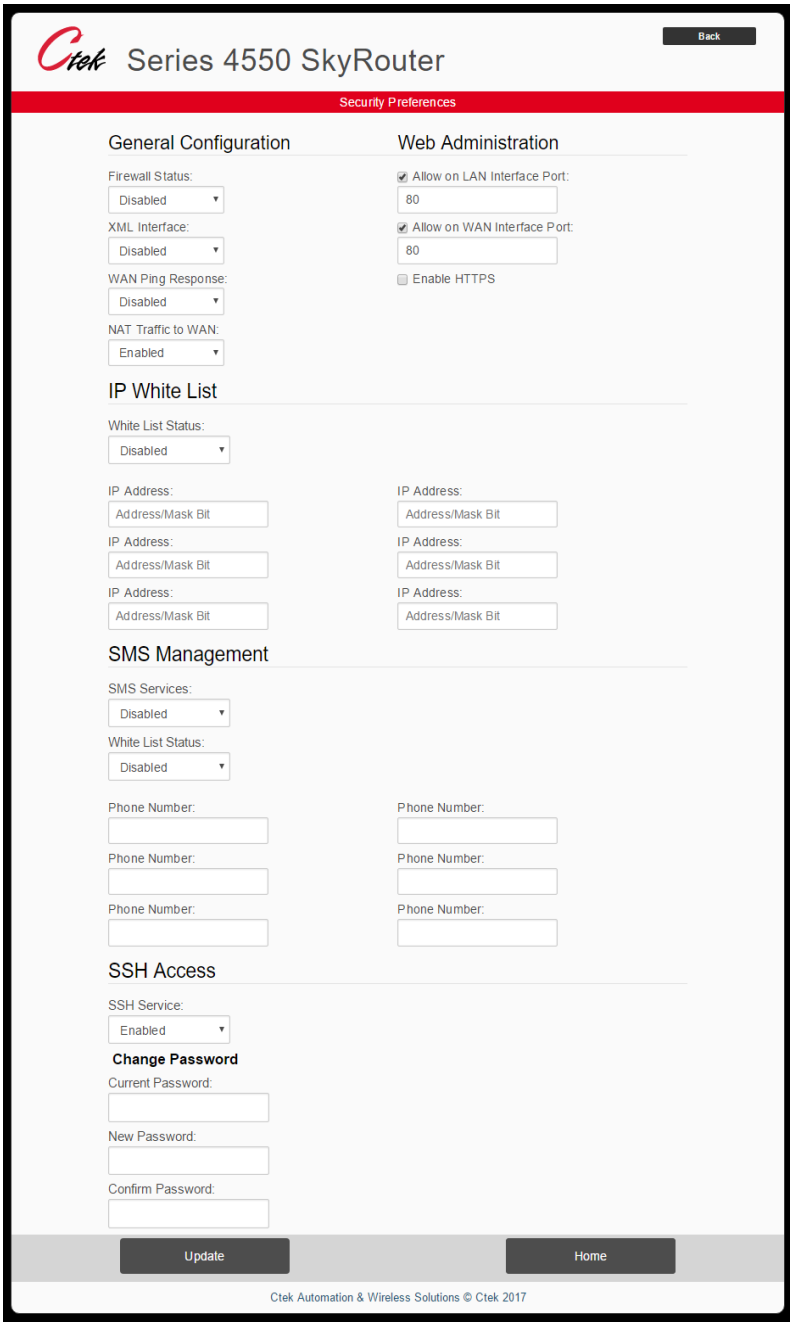

Series 4550 SkyRouter
Back
Security Preferences
General Configuration
Firewall Status:
Disabled
XML Interface:
Disabled
WAN Ping Response:
Disabled
NAT Traffic to WAN:
Enabled
Web Administration
Allow on LAN Interface Port:
80
Allow on WAN Interface Port:
80
Enable HTTPS
IP White List
White List Status:
Disabled
IP Address:
Address/Mask Bit
SMS Management
SMS Services:
Disabled
White List Status:
Disabled
Phone Number:
SSH Access
SSH Service:
Enabled
Change Password
Current Password:
New Password:
Confirm Password:
Update
Home
Ctek Automation & Wireless Solutions © Ctek 2017

Figure 4

General Configuration

- Firewall Status - When enabled the firewall blocks all WAN traffic except for port 80 and the serial pad port if, and only if the serial pad is active. Since an SMS command (TechNote TN009) can be used to temporarily open ports for ad-hoc maintenance there are very few reasons to ever disable the firewall.
- XML Interface: Can be enabled to open port 5070 for XML applications
- WAN Ping Response – When Disabled ICMP Ping requests will be ignored
- NAT Traffic to WAN - Must be Enabled for normal operation

Web Administration

Provides a mechanism to enable or disable HTTP access through the WAN, LAN, or both. Also provides a mechanism to specify an IP port number other than 80 for HTTP access through the WAN, LAN, or both.

IP White List

Enable to limit access to specified addresses or ranges of address. The White list applies to both WAN and LAN side connections.

IP Address (for white list) – specified as an address followed by a netmask in the Classless Inter-Domain Routing (CIDR) format as in 192.168.1.0/24 to allow the entire class C range beginning at 192.168.1.0 for LAN administration

Note: If enabled, be sure to create an entry for LAN access.

SMS Management

Enable to allow SMS management commands as defined in TechNote TN009

White List Status (SMS)

Enable to limit SMS access to specified phone numbers

SSH Access

Enable to allow SSH access from LAN Only, WAN Only, or both

Note: The SSH password can and should be changed if SSH is enabled. For file transfers, the Secure Copy (SCP) utility can be used with the same login credentials as SSH

Additional Security Features

Multiple Failed Login Attempts

Three (3) consecutive failed login attempts on either the LAN or the WAN interface will cause subsequent login attempts to see a "Locked" screen. Once the "Locked" condition occurs the user must wait for 30 minutes with no further login attempts before it clears.

Authlogread

Using SSH the command line utility authlogread can be used to determine the last 20 login attempts since the unit was last rebooted.

Intrusion Detection

If the Z4550 has the TCOPlus management option (APN001) installed, the intrusion detection feature under Tools/Wan Management can be used to alarm 3 consecutive failed login attempts, and if desired to lockout any subsequent login activity until the unit receives administrative attention.

Device Profile

The Device Profile screen performs two key functions. First, it is used to configure the Z4550's LAN for either network gateway or network client operation. Second, it is used to configure a number of parameters used by controller's resident applications for alarming, reporting, and formatting the dashboard display.

Device Network Profile

Gateway Configuration

In the Gateway mode of operation the Z4550 Controller connects with the cellular network, obtains an IP address from the cellular network, and routes traffic to and from LAN side connections using Network Address Translation (NAT). Gateway mode is the default method of operation.

Client Configuration

The Client mode of operation allows the Z4550 to be connected, via Ethernet to an enterprise or home network. In this mode of operation, the Z4550 can be set up to operate either as a DHCP client or with a static address on an established network. Client mode can be a useful tool for loading updates or applications since in the client mode of operation traffic moves through the corporate network instead of over the wireless network.

Application Parameters

Location

The location name that will be displayed on the dashboard, on SkyCloud, and in reports and alarms

Application Alarming

Enables or disables alarms, selects alarm delivery mechanisms, assigns email addresses and phone numbers for alarm delivery, and assigns GPS/Location coordinates to alarms

Application Logging

Enables or disables application logging, enables or disables log deliver via email, selects a log delivery schedule, and assigns email addresses of log recipients

Email Configuration

The Z4550 has a resident POP3 email server that is used to deliver alarms and logs. This panel is used to configure the controller with email account information. This set up should be identical to setting up any email client such as Outlook or Thunderbird.

Dashboard Groups

This panel is used to assign names to the display groups shown on the automation dashboard

Dashboard Options

This function is used to configure the number (1-5) of named display groups that will appear on a single row of the dashboard.

Local Interfaces

Port Forwarding

In the gateway mode of operation (see section 5.1) the Z4550 Controller routes data to and from the wireless network IP connection to a class C range of local (private) IP addresses available on the RJ45 Ethernet connector. To accomplish this the Port Forwarding screen allows you to forward WAN side IP traffic arriving on a specific IP Port to a specific Port at a designated LAN side address. In addition, this screen also allows you to make a named (advertised) service available over the WAN interface.

Each forwarding rules consists of the following field:

Service Name – A name that will be associated with a service advertised on the Quick Panel of the WAN interface

Forwarding From – The inbound (WAN side) port number managing the traffic

Local Port – The port number on the LAN side that the traffic will be routed to

Local IP – The IP address on the LAN side that the traffic will be routed to. Must be part of the class C range defined in the Ethernet Interface screen.

Advertise – Yes or no

Protocol – TCP, UDP, or both

Enable – Make the rule active (Yes/No)

RS232/RS485 Ports

The RS232/RS485 screen is used to configure the physical (electrical and timing) characteristics of the serial ports. The serial ports can be connected to the TCP/UDP PAD function for WAN transmission or to various protocols used by Automation Control. See TN039 for details.

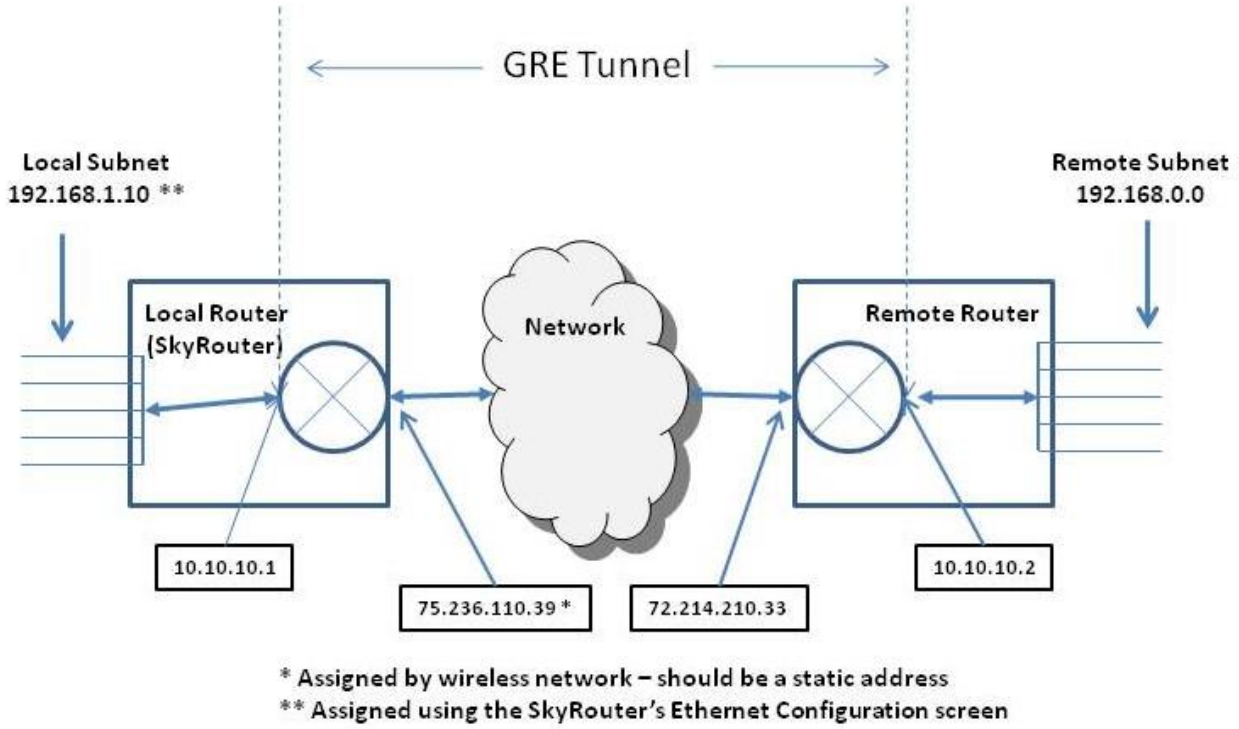
RS232/RS485 Options

The screens under this function are used to configure the serial (TCP/UDP/PPP) pad function. For details see TechNote TN-007

Tunneling and Encryption

GRE Tunnels

The Z4550 Controller allows for the configuration of up 2 GRE tunnels over the cellular wireless interface. The figure below shows the mode of operation



Parameter	Options
Tunnel Select	None/1/2/Both
WAN MTU/MRU	Increase for tunnel overhead (Yes/No)
TTL Value	Time for a packet to live in a tunnel (seconds)
Multicast Support	Enable/Disable
GRE Tunnel Definition (1/2)	**Remote Router IP** - Routable address of the remote router) **Remote Tunnel IP** - Address used for the remote end of the tunnel) **Remote Subnet IP/Netmask** - Base address of the subnet connected through the tunnel **Local Tunnel IP/Netmask** – Address used to construct local end of the tunnel

IPsec Tunnels

The Z4550 Controller supports 8 concurrent IPsec tunnels. For each tunnel the configuration options below are available.

System-Wide IPsec Tunnel Options

Parameter	Options
Tunnel Select	Tunnel to be configured (up to 8)
IPSEC	System level Enable/Disable of IPSEC tunnels
Security Level	**Allow Internet and Secure Traffic** – In this mode IP traffic addressed for the IPsec tunnel will be transmitted through the tunnel. Other traffic will continue to route over the open IP network. This setting allows web type traffic to co-exist with secure traffic on the same Ctek controller. **Allow Only Secure Traffic** – In this mode only IP traffic addressed for the IPsec tunnel will be transmitted. Since this precludes the use of the standard routing feature the Routing button in the main menu is disabled in this mode of operation.

Individual IPsec Tunnel Options

The remaining portion of the IPsec configuration deals with tunnel specific parameters meaning that each parameter must be set for each tunnel deployed. The configurable options can be seen in the table below.

Phase 1 and Phase 2 under IPSec Key Exchange refer to IKE Phase 1 and IKE phase 2. During IKE phase 1 IKE authenticates IPSec peers and negotiates IKE Security Associations (SAs), setting up a secure channel for negotiating IPSec SAs in phase 2.During IKE phase 2 IKE negotiates IPSec SA parameters and sets up matching IPSec SAs in the peers. The selection choices with this panel for Phase 1 and Phase 2 are identical but repeated so that different choices can be applied to Phase 1 and Phase 2

Parameter	Options
Tunnel	Enable/Disable an individual tunnel
Auto-Connect	Sends ICMP request as the defined interval in seconds to the router subnet to maintain the tunnel connection alive
Local Router Definition	**Local Security Type** – Available option are FQDN, USER FQDN, KEY ID or NONE **Security ID** – The identifier corresponding to the selected security type **IP Address** – IP address of the remote router **Subnet IP Address/Netmask** – IP Address and netmask of remote router
Authentication/Encryption	**Pre-Shared Key** – Text string used by both ends of the tunnel for authentication **Exchange Mode** – Available settings are Main or Aggressive. Defines the number of exchanges used to complete IKE Phase 1. Main is the more robust setting while aggressive mode uses few exchanges and is therefore somewhat more risky. **Dead Peer Detection (DPD)** – Defines the intervals (in seconds) between DPD messages following idle periods. A zero (0) setting disables DPD.
IPSEC Key Exchange	**Encryption** – Choices are 3des, or aes128, aes192, ase256 **Authentication** – Choices are sha1, or md5 **DH Group** – Defines what size modulus to use for Diffie-Hellman calculation. Choices are 768,1024, 1536, or 2048 **PFS DH Group** – Choices are No PFS, 768, 1024, 1536, or 2048. You specify the Diffie – Hellman group in Phase 2 only when you select Perfect Forward Secrecy (PFS). PFS makes keys more secure because new keys are not made from previous keys. When you specify PFS during Phase 2, a Diffie-Hellman exchange occurs each time a new SA is negotiated. The DH group you choose for Phase 2 does not need to match the group you choose for Phase 1. **SA Lifetime (Phase 1 & Phase 2)** – The lifetime parameter controls the duration (in minutes) for which the SA is valid. A zero (0) setting disables SA Lifetime timeouts.

Time and Location Source

The Time Source screen allows the user to select from one of three mechanisms to synchronize the time reference on an individual Z4550 Controller.

Cellular Network

The controller retrieves and synchronizes to time provided by the cellular network

Network Time Protocol (NTP) Server

The controller retrieves and synchronizes to time provided by an NTP server. An IP address field for the NTP server is provided on the screen.

GPS Location

The controller retrieves and synchronizes to time provided by the GPS or GLONASS constellation. This option requires that GPS be enabled on the Location Source screen. GPS functionality also requires that a GPS capable antenna be connected to the secondary antenna connector in addition to the cellular antenna that is connected the primary antenna connector.

Location Source

The Controller's location source can be set to originate from the built-in GPS/GLONASS receiver, or by using user defined coordinates. User defined coordinates are especially useful for stationary installations that may not want to incur the expense of a GPS antenna.

The Location Source screen also supports the creation of two geo-fences. Geo-fencing applications are covered in detail in TechNote TN034.

SkyCloud Services

The SkyCloud Services screen serves two related purposes. It provides a method of selecting a Dynamic Domain Name Service (DDNS) for the Z4550. Secondly, it is used to configure the unit for operation on Ctek's cloud based visual access and management system, SkyCloud. See Technical Information Bulletin TIB006 for details.

Tools

The Z4550 comes standard with two tools installed.

Flash Update Client

The Flash Update client provides a mechanism to load over-the-air firmware update and to enable additional applications on the controller. The Flash Update client can be configured for periodic (daily/weekly/monthly) updates, or to perform the updates ad-hoc when the user initiates an update request.

Backup and Restore

Backup and Restore works in conjunction with a USB stick inserted in the type A USB connector. The USB stick should be formatted as FAT32. Types of backups possible include:

- Automation Control
- Navigation Services
- Entire System
- Product Branding
- Logs (WAN and System logs)

In addition to a restore option for each backup categories listed above, an additional type of restore allows update installer files to be applied to a Controller via the USB drive.

Applications

The Z4550 comes standard with the Automation-Light application installed. Automation-Lite is a scaled back version of the complete Automation application, which can be licensed from Ctek. See Application Note APN008 for details on the Automation application.