

**Dual 10G Zero Trust Security Gateway with 4-Port
10/100/1000T**

ZT-800

ZeroTrust & Passkey & TOTP Configuration Guide

Table of Contents

1. INTRODUCTION.....	4
1.1 OVERVIEW	4
1.2 PRODUCT BENEFITS	5
1.3 ARCHITECTURE COMPARISON	5
2. SYSTEM PREPARATION	6
2.1 DOWNLOAD SYSTEM CERTIFICATE.....	6
2.2 INSTALL SYSTEM CERTIFICATE.....	7
2.3 ACCESS ZT-800 VIA DOMAIN NAME	8
3. ADMINISTRATOR PASSKEY SETUP.....	9
3.1 WINDOWS HELLO PASSKEY SETUP.....	9
3.2 MOBILE DEVICE PASSKEY SETUP	14
3.3 SECURITY KEY PASSKEY SETUP.....	20
4. ADMINISTRATOR TOTP SETUP	29
4.1 INSTALL AUTHENTICATOR APPLICATION	29
4.2 OPEN TOTP CONFIGURATION	30
4.3 GENERATE QR CODE	31
4.4 SCAN QR CODE	32
4.5 VERIFY TOTP	33
4.6 ENABLE TWO-FACTOR AUTHENTICATION.....	34
4.7 LOGIN WITH TOTP	35
5. VPN USER PASSKEY SETUP	36
5.1 CONFIGURE DNS RESOLUTION FOR ZT-800	36
5.2 CREATE A VPN USER ACCOUNT	37
5.3 CONFIGURE USER INFORMATION	38
5.4 REGISTER SECURITY KEY PASSKEY.....	39

Configuration Guide

5.5	TOUCH SECURITY KEY	40
6.	WIREGUARD VPN CONFIGURATION	41
7.	VPN PORTAL LOGIN	42
7.1	ACCESS VPN PORTAL	42
7.2	LOGIN USING PASSKEY	43
7.3	SELECT VPN TYPE	44
8.	WIREGUARD CLIENT CONNECTION	45
8.1	DOWNLOAD VPN PROFILE	45
8.2	IMPORT VPN PROFILE	46
8.3	VERIFY TUNNEL CONFIGURATION.....	47
9.	CUSTOMER SUPPORT	48

1. Introduction

1.1 OverView

ZT-800 is a Zero Trust Security Gateway designed to provide secure remote access through advanced identity verification and VPN technologies.

The system supports:

- Passkey Authentication (FIDO2)
- TOTP Two-Factor Authentication
- VPN Self-Service Portal
- WireGuard VPN
- OpenVPN VPN
- Zero Trust Access Control

Configuration Guide

1.2 Product Benefits

Zero Trust VPN Portal

ZT-800 provides identity-verified access through strong authentication mechanisms.

Features include:

- FIDO2 Passkey Authentication
- Multi-Factor Authentication (MFA)
- Dynamic Access Control
- Secure VPN Profile Provisioning

Secure Remote Access

ZT-800 protects enterprise resources by verifying every login request before access is granted.

Benefits:

- Secure remote connectivity
- VPN self-service portal
- Protection of internal resources
- Strong identity verification

1.3 Architecture Comparison

Item	ZT-800	Traditional Router
Security Model	Zero Trust	Perimeter Security
Authentication	MFA / Passkey	Password Only
Internal Access	Default Deny	Trust Internal Users
Lateral Movement	Blocked	Trust Internal Users

Configuration Guide

2. System Preparation

2.1 Download System Certificate

Log in to the ZT-800 Web UI and go to:

Security > Certificates

Click **Download** under **System CA Certificate** to download the certificate.

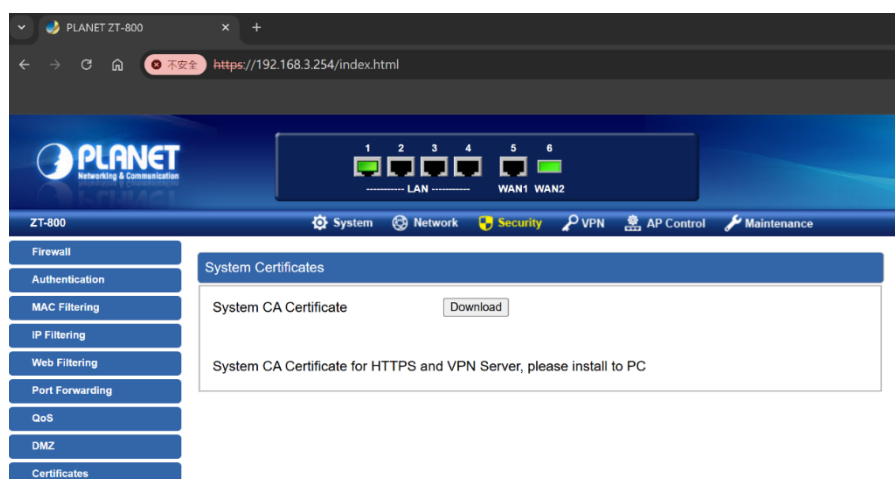


Figure 2-1 Download System Certificate

Configuration Guide

2.2 Install System Certificate

After downloading the certificate:

1. Launch Certificate Import Wizard.
2. Select:

Place all certificates in the following store

3. Choose:

Trusted Root Certification Authorities

4. Complete the import process.

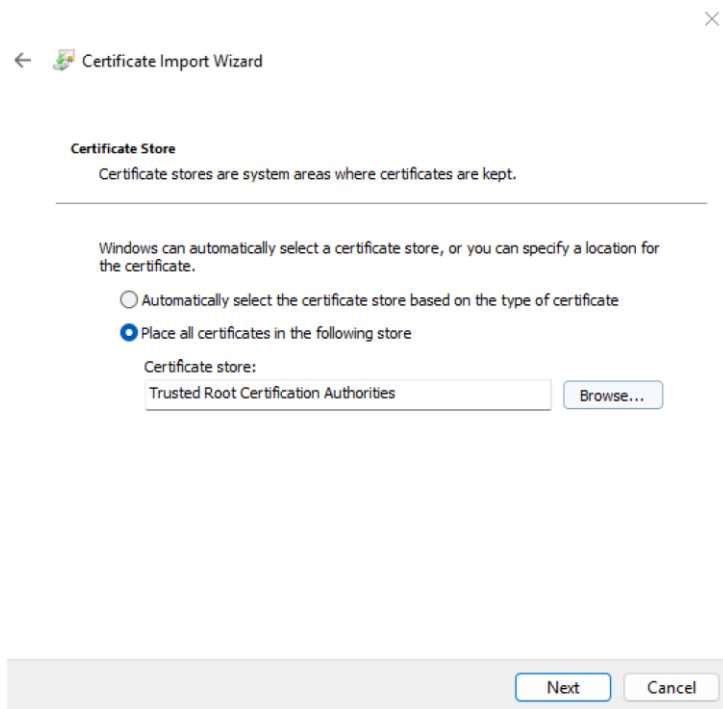


Figure 2-2 Certificate Import Wizard

Configuration Guide

2.3 Access ZT-800 via Domain Name

After the certificate installation is completed, please reopen the browser and access the ZT-800 using the following HTTPS domain format:

<https://zt-800/>

Do not use the IP address format such as:

<https://192.168.x.x>

Passkey registration and authentication require the browser domain information (Relying Party ID) to match the Passkey domain configuration. Therefore, Passkey setup and login must be performed using:

<https://zt-800/>



Figure 2-3 Access via Domain Name

Configuration Guide

3. Administrator Passkey Setup

3.1 Windows Hello Passkey Setup

Step 1 Enable Windows Hello

Open:

Settings → Accounts → Sign-in Options

Configure at least one authentication method:

- PIN
- Fingerprint
- Facial Recognition

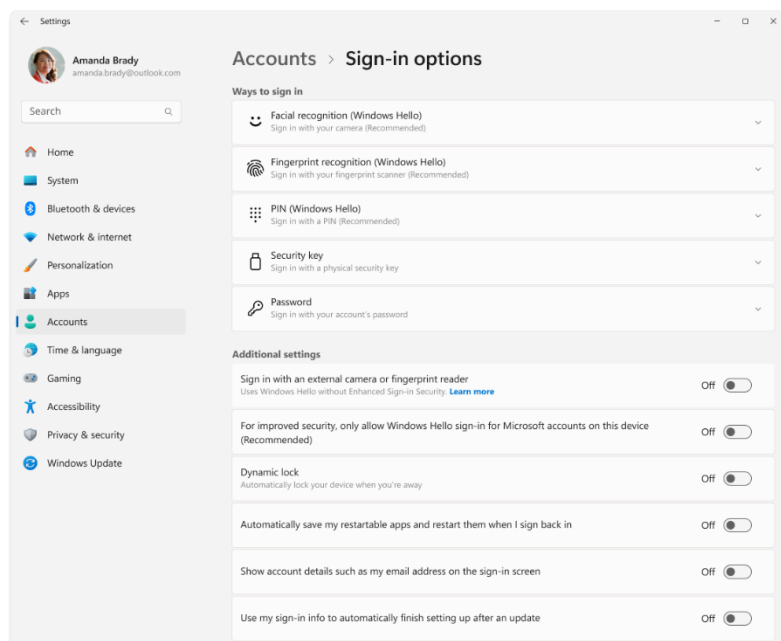


Figure 3-1 Windows Hello Configuration

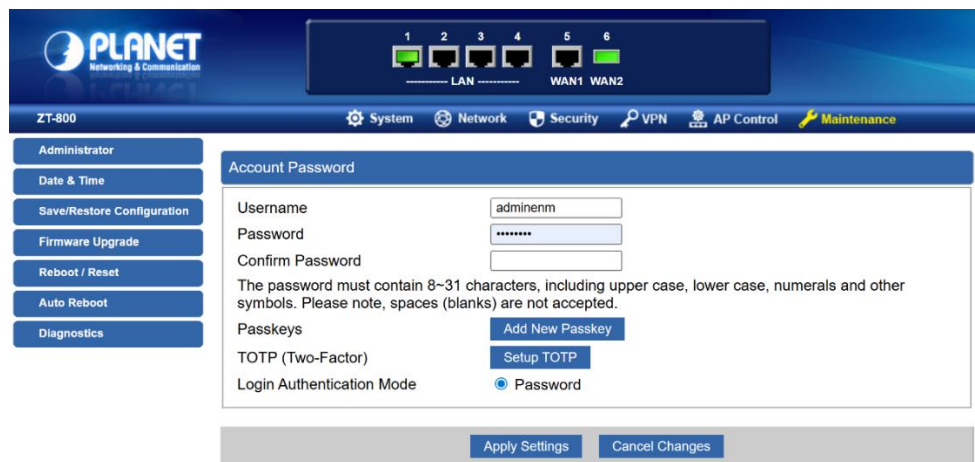
Configuration Guide

Step 2 Open Administrator Page

Login to ZT-800.

Navigate to:

Maintenance → Administrator



The screenshot displays the PLANET ZT-800 web interface. At the top, there is a header with the PLANET logo and a status bar showing network ports (LAN, WAN1, WAN2) and a navigation menu (System, Network, Security, VPN, AP Control, Maintenance). On the left side, a sidebar contains buttons for Administrator, Date & Time, Save/Restore Configuration, Firmware Upgrade, Reboot / Reset, Auto Reboot, and Diagnostics. The main content area is titled 'Account Password' and contains fields for Username (adminnm), Password (masked with asterisks), and Confirm Password. Below these fields, a note states: 'The password must contain 8-31 characters, including upper case, lower case, numerals and other symbols. Please note, spaces (blanks) are not accepted.' There are also buttons for 'Add New Passkey', 'Setup TOTP', and a radio button for 'Login Authentication Mode' set to 'Password'. At the bottom, there are 'Apply Settings' and 'Cancel Changes' buttons.

Figure 3-2 Administrator Page

Configuration Guide

Step 3 Add New Passkey

Under Passkeys section click:

Add New Passkey

Select:

Windows Hello or External Security Key

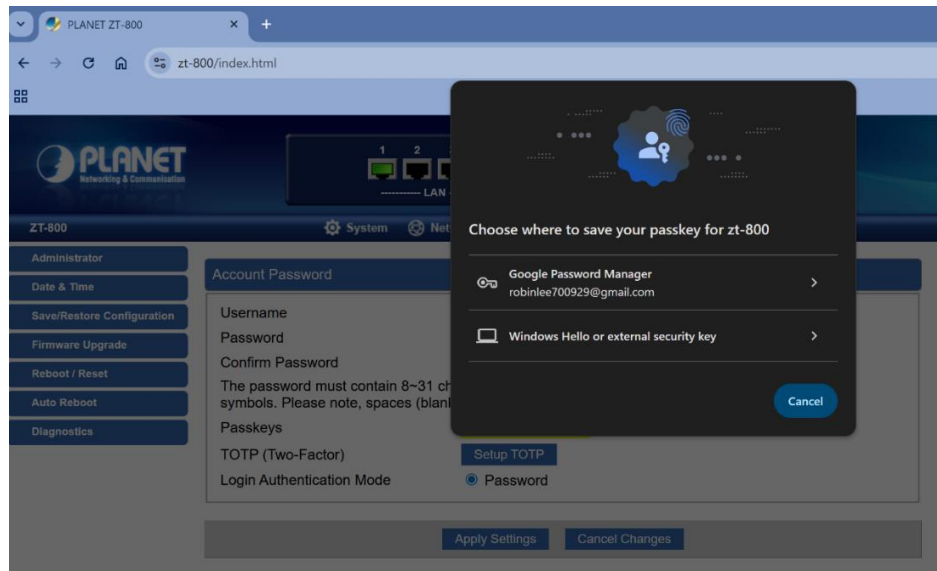


Figure 3-3 Add New Passkey

Configuration Guide

Step 4 Create Passkey

Windows Security will display:

Save Your Passkey

Enter Windows PIN.

The passkey will be stored locally on the Windows device.

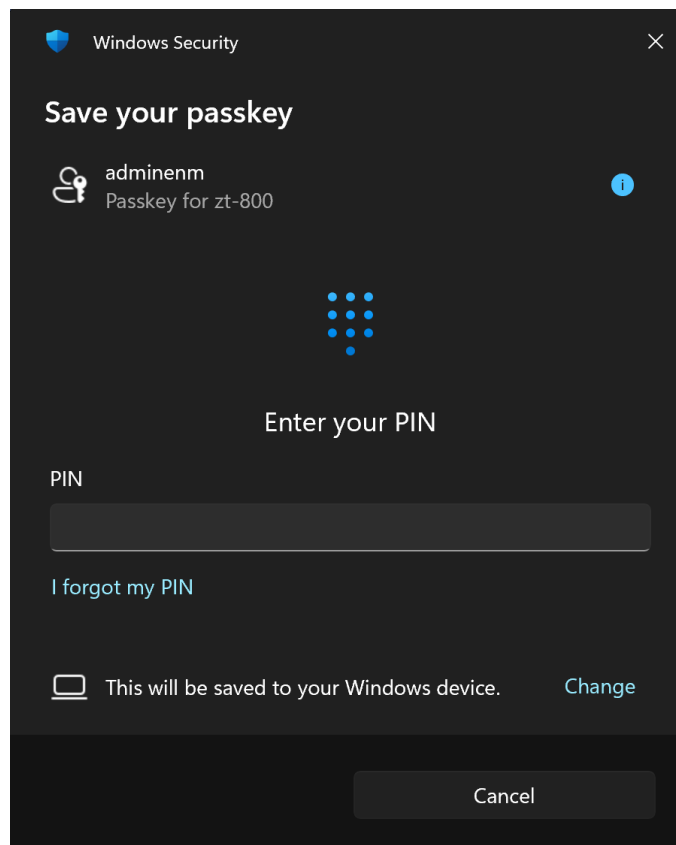


Figure 3-4 Save Passkey

Configuration Guide

Step 5 Login with Passkey

Return to Login Page.

Click:

Passkey Login

Select the stored Passkey.

Authenticate using:

- PIN
- Fingerprint
- Face Recognition

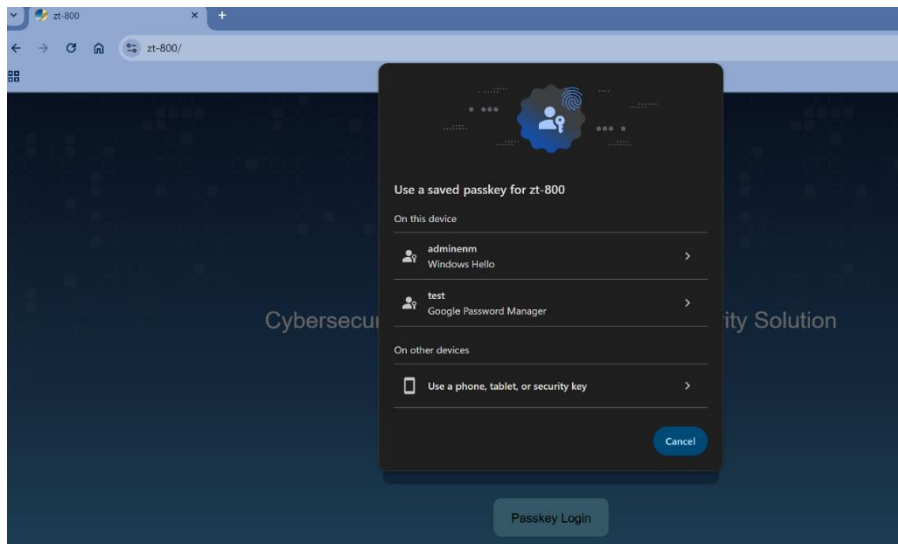


Figure 3-5 Passkey Login

Configuration Guide

3.2 Mobile Device Passkey Setup

Step 1 Add New Passkey

Navigate to:

Maintenance → Administrator

Click:

Add New Passkey

The screenshot shows the PLANET ZT-800 web interface. The top navigation bar includes links for System, Network, Security, VPN, AP Control, and Maintenance. The left sidebar contains a menu with options: Administrator, Date & Time, Save/Restore Configuration, Firmware Upgrade, Reboot / Reset, Auto Reboot, and Diagnostics. The main content area is titled 'Account Password' and contains the following fields and options:

- Username:
- Password:
- Confirm Password:
- Passkeys:
- TOTP (Two-Factor):
- Login Authentication Mode: ☒ Password

Below the form, there are two buttons: 'Apply Settings' and 'Cancel Changes'. A note states: 'The password must contain 8~31 characters, including upper case, lower case, numerals and other symbols. Please note, spaces (blanks) are not accepted.'

Figure 3-7 Add Mobile Passkey

Configuration Guide

Step 2 Select Device

Choose:

Use a Phone, Tablet or Security Key

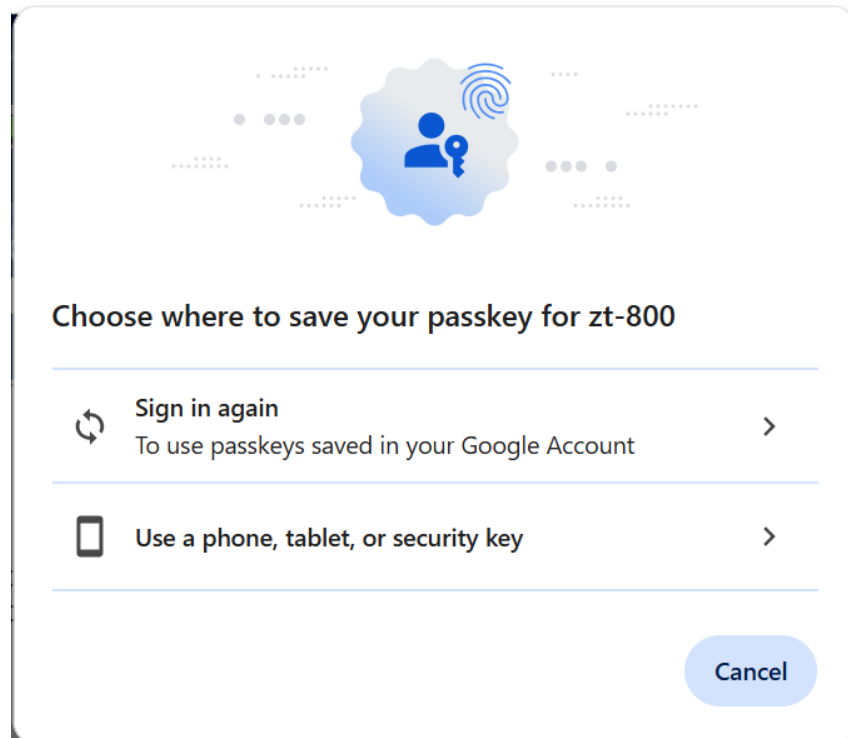


Figure 3-8 Select Device

Configuration Guide

Step 3 Scan QR Code

Windows Security displays a QR Code.

Use:

- Android
- iPhone
- iPad

to scan the code.

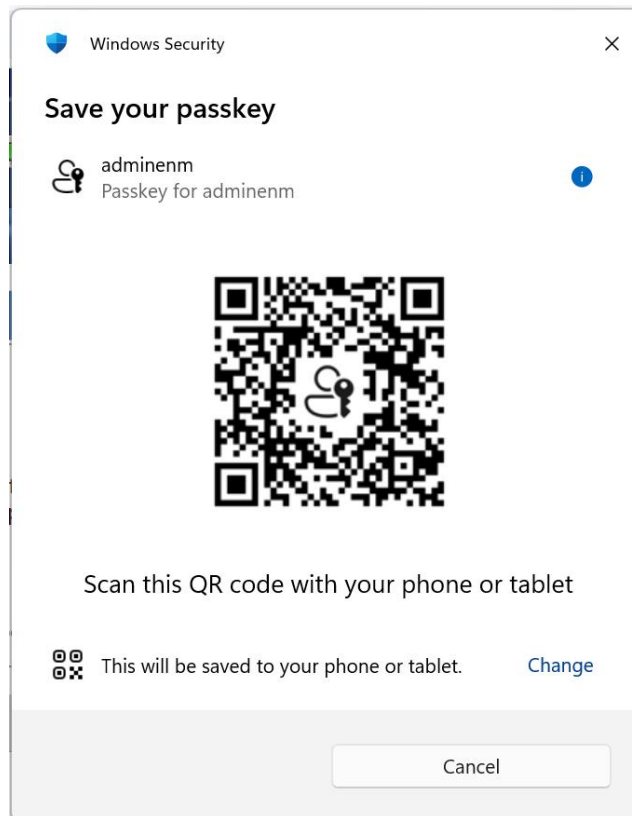


Figure 3-9 Scan QR Code

Configuration Guide

Step 4 Complete Registration

Follow the instructions on the mobile device.

Passkey registration will be completed automatically.

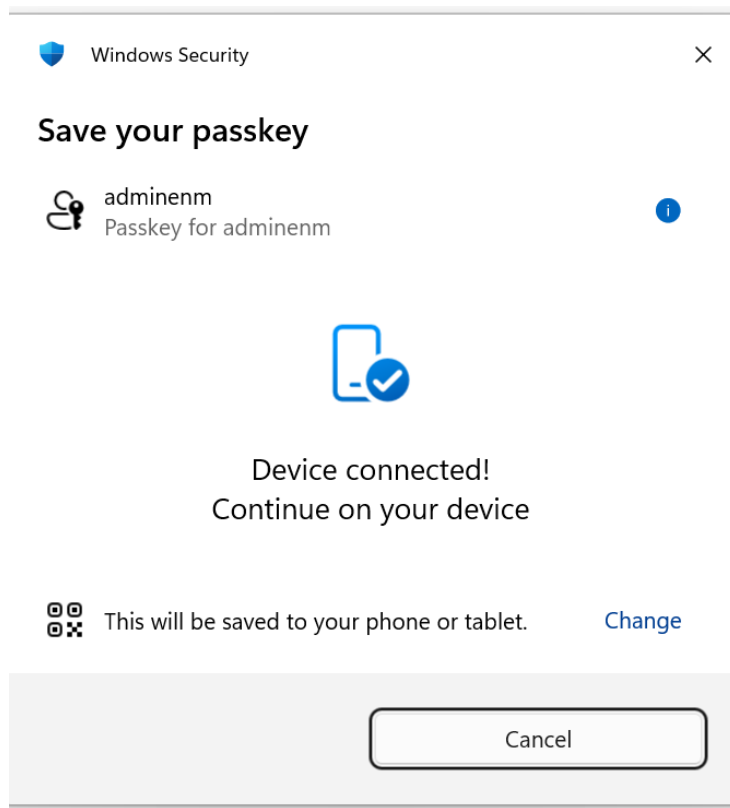


Figure 3-10 Registration Complete

Configuration Guide

Step 5 Login with Mobile Passkey

Click:

Passkey Login

Select:

iPhone, iPad, or Android device

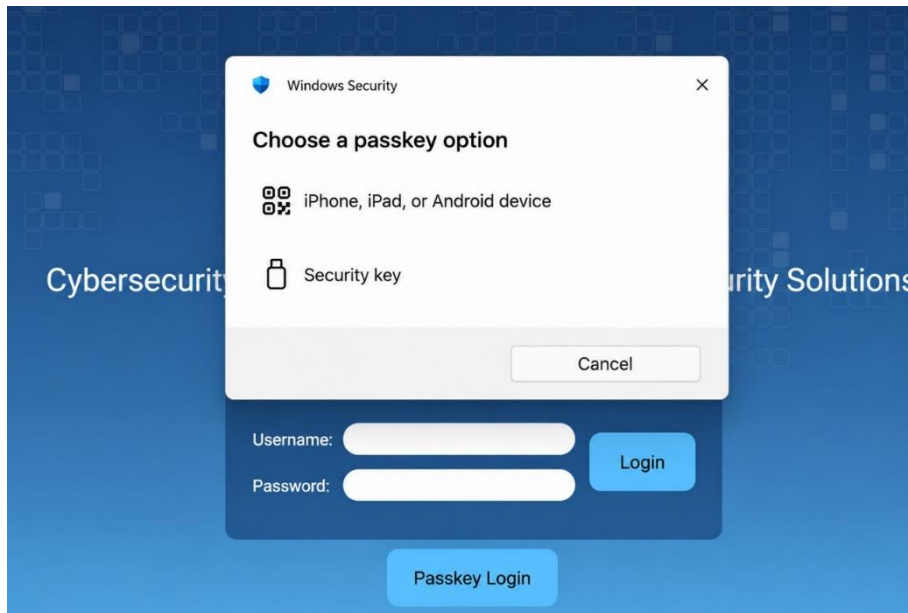


Figure 3-11 Mobile Passkey Login

Configuration Guide

Scan the displayed QR code using the registered device.

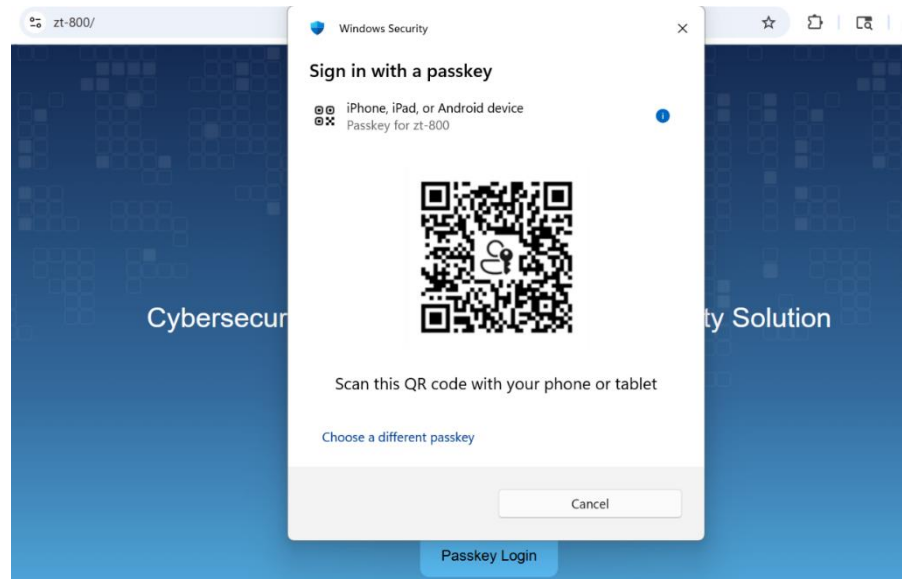


Figure 3-12 Scan the displayed QR code

Configuration Guide

3.3 Security Key Passkey Setup

Step 1 Configure Security Key PIN

Navigate to:

Settings → Accounts → Sign-in Options → Security Key

Click:

Manage

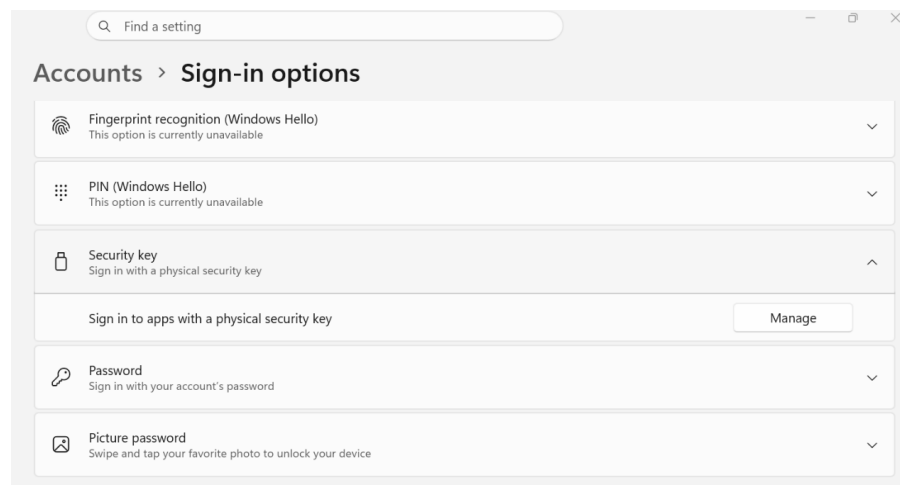


Figure 3-12 Security Key Settings

Configuration Guide

Step 2 Configure PIN

Select:

Change PIN

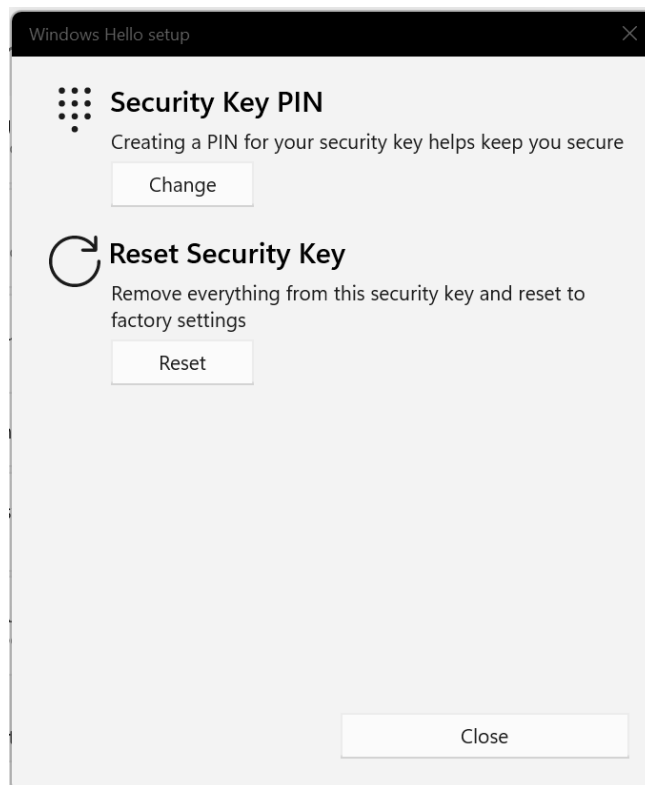


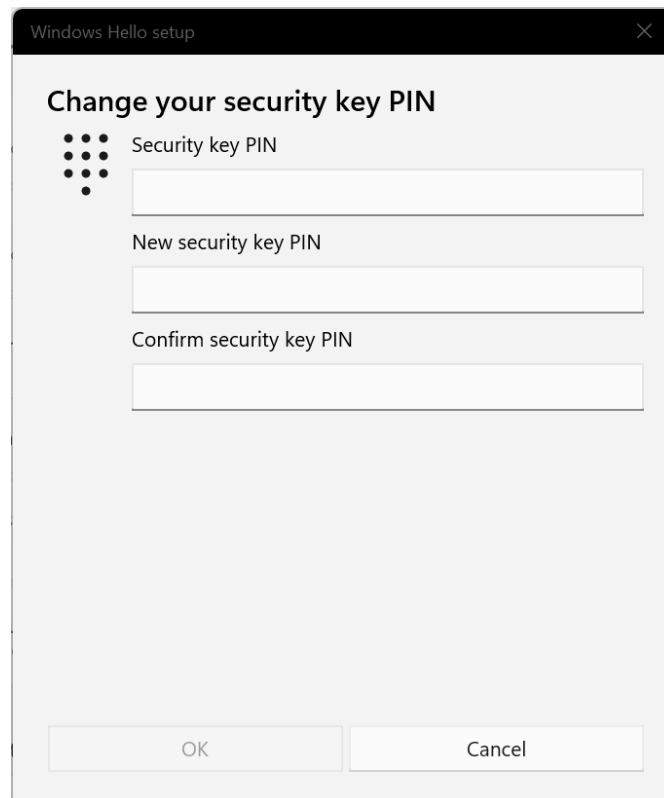
Figure 3-13 Configure PIN

Configuration Guide

Enter:

- Current PIN
- New PIN
- Confirm PIN

Click: OK



The image shows a Windows Hello setup window titled "Windows Hello setup" with a close button (X) in the top right corner. The main heading is "Change your security key PIN". To the left of the first input field is a security key icon (a grid of dots). The input fields are labeled "Security key PIN", "New security key PIN", and "Confirm security key PIN". At the bottom of the window are two buttons: "OK" and "Cancel".

Figure 3-14 Change security key PIN

Configuration Guide

Step 3 Register Security Key

Navigate to:

Maintenance → Administrator

Click:

Add New Passkey

The screenshot displays the PLANET ZT-800 web management interface. The top header shows the PLANET logo and network status indicators for LAN and WAN ports. The left sidebar contains a menu with options: Administrator, Date & Time, Save/Restore Configuration, Firmware Upgrade, Reboot / Reset, Auto Reboot, and Diagnostics. The main content area is titled 'Account Password' and contains the following fields and options:

- Username:** adminnm
- Password:** [masked with asterisks]
- Confirm Password:** [empty field]
- Passkeys:** Includes an 'Add New Passkey' button.
- TOTP (Two-Factor):** Includes a 'Setup TOTP' button.
- Login Authentication Mode:** Radio buttons for 'Password' (selected) and 'TOTP'.

At the bottom of the configuration area, there are two buttons: 'Apply Settings' and 'Cancel Changes'.

Figure 3-15 Register Security Key

Configuration Guide

Select:

Use a Phone, Tablet or Security Key → Security Key

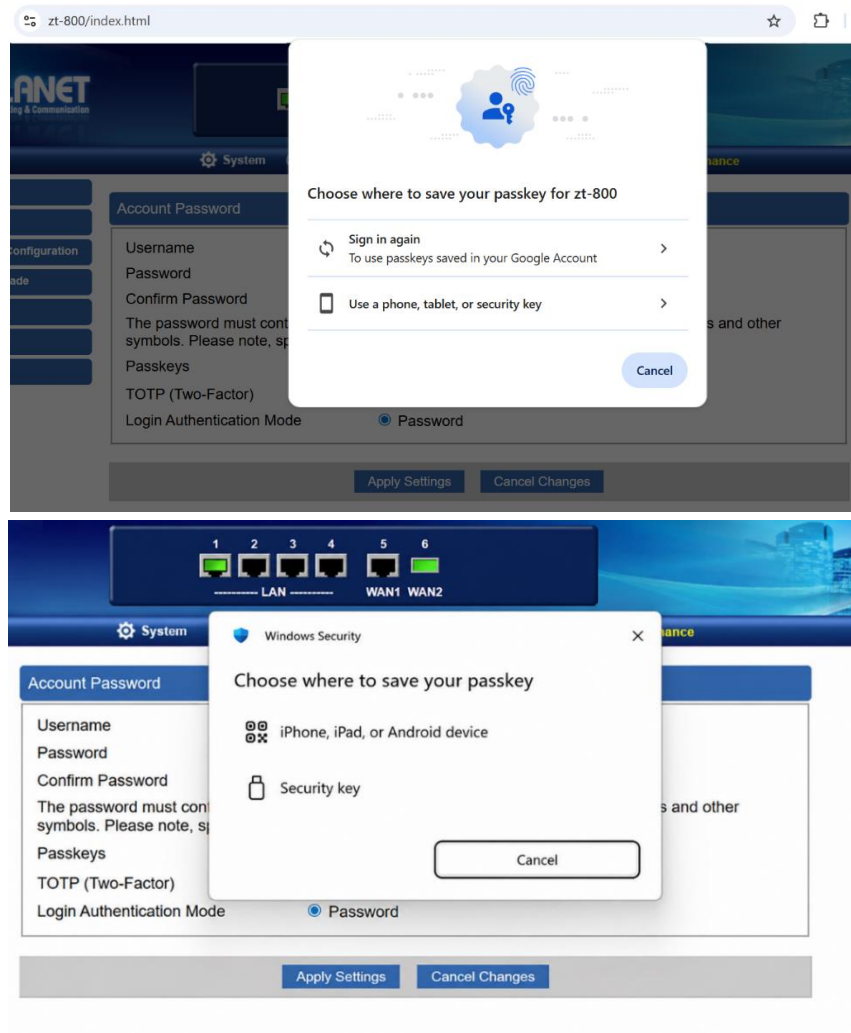


Figure 3-16 Select Device

Configuration Guide

Step 4 Enter Security Key PIN

Enter configured PIN.

Click:

OK

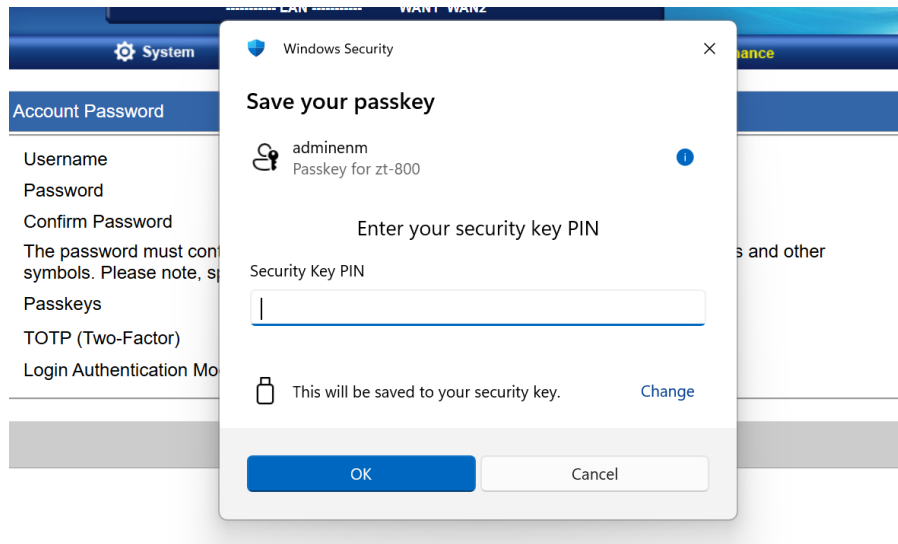


Figure 3-17 Enter PIN

Configuration Guide

Step 5 Touch Security Key

Touch the CoreTrust Key when prompted.

Passkey registration will be completed.

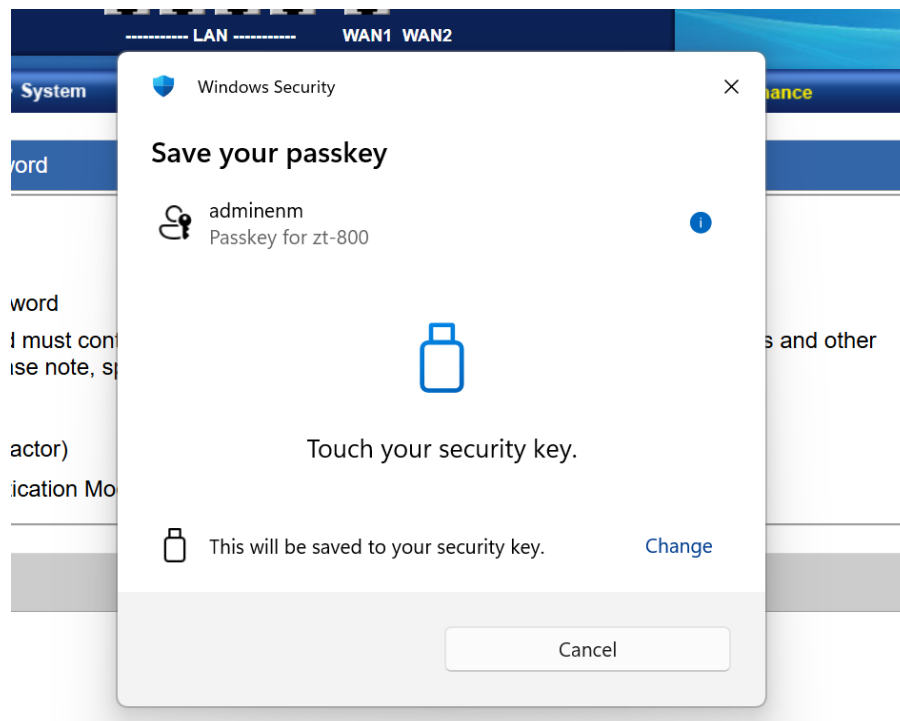


Figure 3-18 Touch Security Key

Configuration Guide

Step 6 Login Using Security Key

Click:

Passkey Login

Select:

Security Key

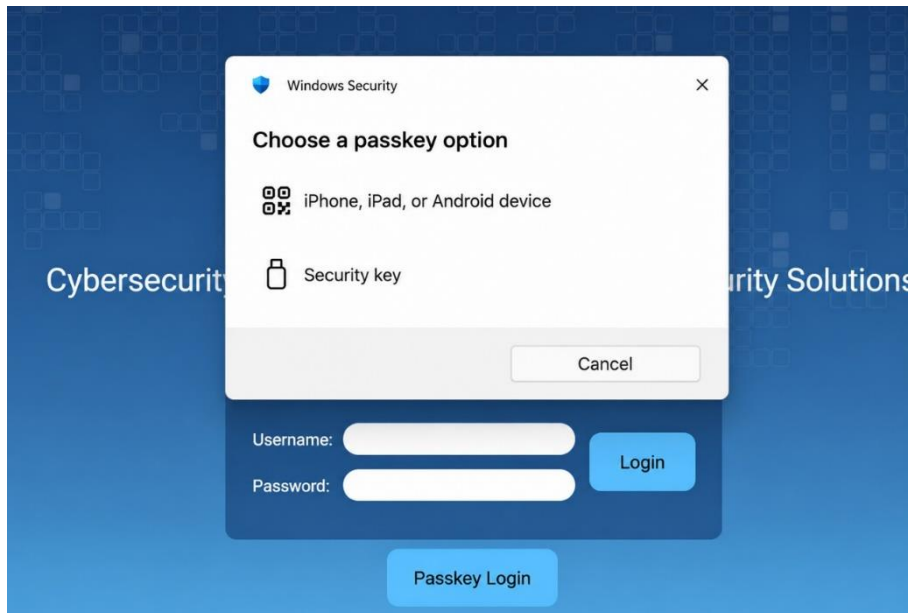


Figure 3-19 Security Key Login

Configuration Guide

Enter PIN.

Touch Security Key.

Login successful.

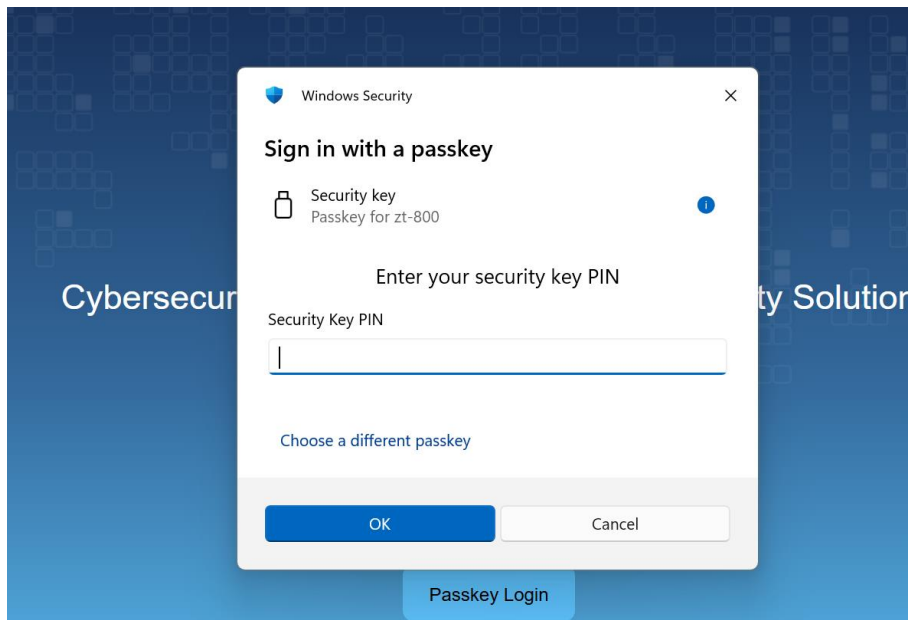


Figure 3-20 Enter security key PIN

4. Administrator TOTP Setup

4.1 Install Authenticator Application

Supported Applications:

- Google Authenticator
- Microsoft Authenticator
- Authy

Install and launch the application.

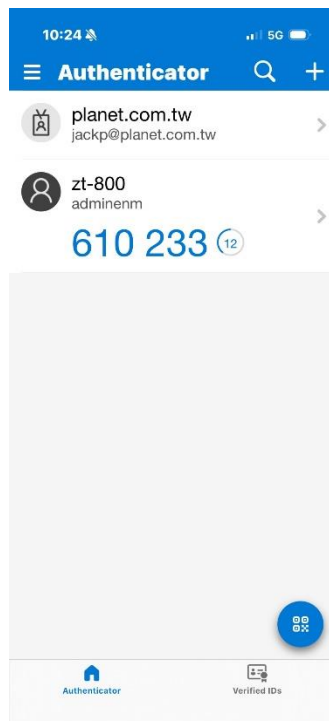


Figure 4-1 Authenticator Applications

Configuration Guide

4.2 Open TOTP Configuration

Navigate to:

Maintenance → Administrator

Click:

Setup TOTP



The screenshot displays the PLANET ZT-800 web management interface. The top navigation bar includes links for System, Network, Security, VPN, AP Control, and Maintenance. The left sidebar lists various system functions: Administrator, Date & Time, Save/Restore Configuration, Firmware Upgrade, Reboot / Reset, Auto Reboot, and Diagnostics. The main content area is titled 'Account Password' and contains the following fields and options:

- Username:** Input field containing 'adminnm'.
- Password:** Input field with masked characters (dots).
- Confirm Password:** Input field for password confirmation.
- Instructions:** A note stating, 'The password must contain 8~31 characters, including upper case, lower case, numerals and other symbols. Please note, spaces (blanks) are not accepted.'
- Passkeys:** A section with an 'Add New Passkey' button.
- TOTP (Two-Factor):** A section with a 'Setup TOTP' button.
- Login Authentication Mode:** A radio button selection with 'Password' selected.

At the bottom of the configuration area, there are two buttons: 'Apply Settings' and 'Cancel Changes'.

Figure 4-2 Setup TOTP

Configuration Guide

4.3 Generate QR Code

The **TOTP Two-Factor Authentication Setup** page will appear.

Click:

Generate QR Code

The ZT-800 will generate:

- A QR Code
- A Secret Key

for TOTP registration.

The screenshot displays the ZT-800 web management interface. At the top, a navigation bar includes 'ZT-800' and several menu items: 'System', 'Network', 'Security', 'VPN', 'AP Control', and 'Maintenance'. A left sidebar contains a list of administrative functions: 'Administrator', 'Date & Time', 'Save/Restore Configuration', 'Firmware Upgrade', 'Reboot / Reset', 'Auto Reboot', and 'Diagnostics'. The main content area is titled 'TOTP Two-Factor Authentication Setup'. It features a 'Username' field with the value 'adminnm'. Below this, a light blue box contains the instruction 'Step 1: Click "Generate QR Code" to create a new TOTP secret'. A 'Generate QR Code' button is positioned below the instruction box. At the bottom of the main area, a 'Back to user' button is visible.

Figure 4-3 Generate QR Code

Configuration Guide

4.4 Scan QR Code

Use the Authenticator application to scan the QR Code.
The application will generate a 6-digit verification code.



Figure 4-4 Scan QR Code

Configuration Guide

4.5 Verify TOTP

Enter the 6-digit code.

Click:

Verify & Enable TOTP

The screenshot shows the ZT-800 web interface. The top navigation bar includes links for System, Network, Security, VPN, AP Control, and Maintenance. The left sidebar lists various configuration options: Administrator, Date & Time, Save/Restore Configuration, Firmware Upgrade, Reboot / Reset, Auto Reboot, and Diagnostics. The main content area is titled "TOTP Two-Factor Authentication Setup". It contains a "Username" field with the value "adminnm". Below this, there are two steps: "Step 1: Click 'Generate QR Code' to create a new TOTP secret" and "Step 2: Scan the QR code on the right with your authenticator app (Google Authenticator, Microsoft Authenticator, Authy, etc.)". A "Generate QR Code" button is present, and a "QR Code generated" message is displayed. A "Verification Code" field shows "000000" with a prompt to "Enter the 6-digit code from your authenticator app". At the bottom, there are "Verify & Enable TOTP" and "Back to user" buttons. To the right of the main content area, there is a QR code and a "Secret Key" section with the text "Secret Key: M4EJD3Z74C4PYQD6SXSBMKJ GHPKZ1P9H0". Below the QR code, it says "Scan this QR code with your Authenticator App" and includes a "Regenerate Secret" button.

Figure 4-5 Verify TOTP

Configuration Guide

4.6 Enable Two-Factor Authentication

Select:

Password and TOTP (2FA)

Click:

Apply Settings

PLANET
Networking & Communication

ZT-800

System Network Security VPN AP Control Maintenance

Administrator
Date & Time
Save/Restore Configuration
Firmware Upgrade
Reboot / Reset
Auto Reboot
Diagnostics

Account Password

Username: adminnm

Password:

Confirm Password:

The password must contain 8~31 characters, including upper case, lower case, numerals and other symbols. Please note, spaces (blanks) are not accepted.

Passkeys: [Add New Passkey](#)

TOTP (Two-Factor): [Setup TOTP](#)

Login Authentication Mode:
☐ Password
☒ Password and TOTP (2FA)

TOTP Status

Username	Secrets Count	Created Time	Last Used	Action
adminnm	1	2026-05-19 10:19:44		

[Apply Settings](#) [Cancel Changes](#)

Figure 4-6 Enable 2FA

Configuration Guide

4.7 Login with TOTP

Login process:

1. Enter Username
2. Enter Password
3. Enter TOTP Code
4. Verify
5. Login Success

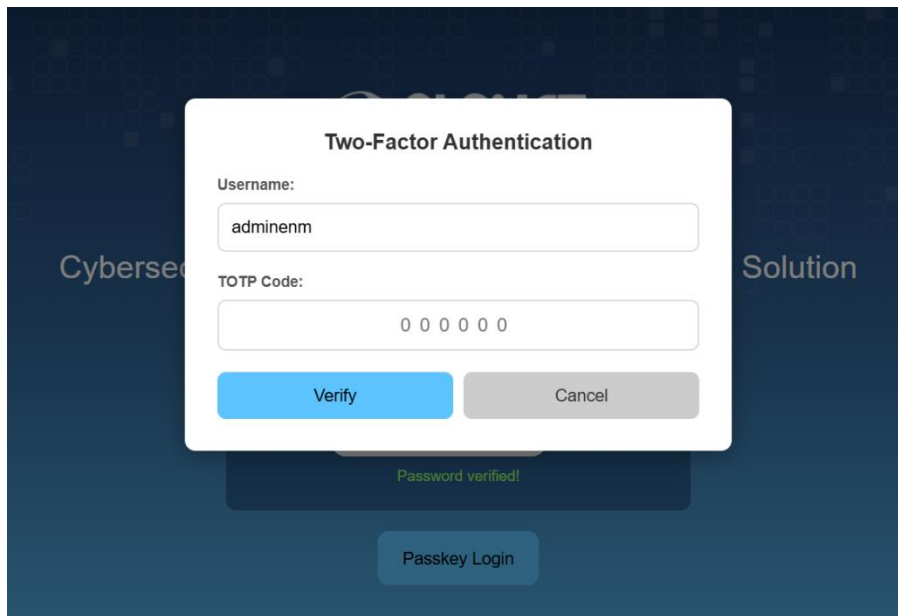


Figure 4-7 TOTP Login Workflow

Configuration Guide

5. VPN User Passkey Setup

5.1 Configure DNS Resolution for ZT-800

Before configuring VPN Passkey authentication, the client PC must be able to access the ZT-800 using a domain name.

Run Notepad as Administrator.

Open the hosts file:

C:\Windows\System32\drivers\etc\hosts

Add the following entry:

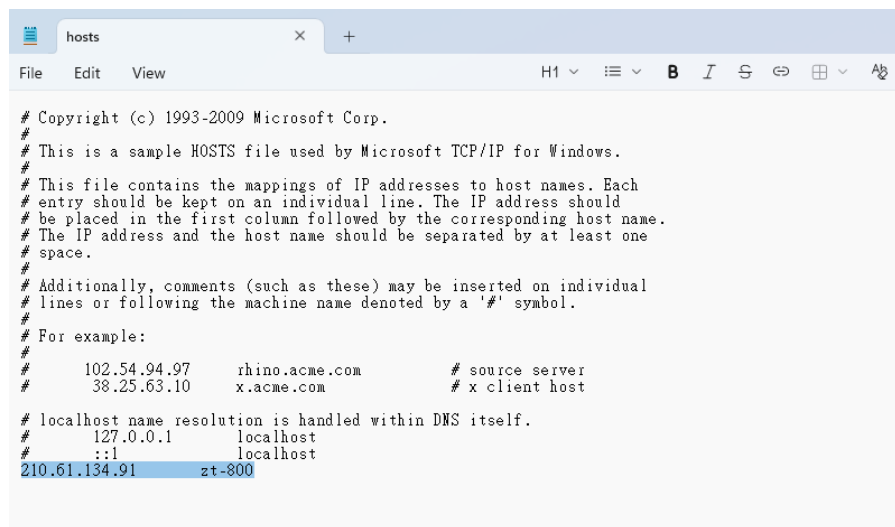
210.61.134.91 zt-800

Save the file.

Open a browser and verify access using:

<https://zt-800/>

Do not access the device using an IP address.



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com             # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
210.61.134.91            zt-800
```

Figure 5-1 Configure Hosts File

Configuration Guide

5.2 Create a VPN User Account

Login to the ZT-800 Web Interface.

Navigate to:

System → RADIUS → User Account

Click:

Add or edit an existing user account.

The screenshot shows the ZT-800 Web Interface. The top navigation bar includes links for System, Network, Security, VPN, AP Control, and Maintenance. The sidebar menu on the left lists various system functions. The main content area is titled 'RADIUS' and has tabs for Local Server, Remote Server, Client, and User Account. The 'User Account' tab is active, displaying a table of user accounts. The table has columns for Index, Username, Description, Account Type, Validation Period, Valid Date From, Expiration Date, and Action. There are 9 rows of data. Below the table, there are links for 'Accounts Export' and 'Accounts Import'. At the bottom of the page, there are 'Apply Settings' and 'Cancel Changes' buttons.

Index	Username	Description	Account Type	Validation Period	Valid Date From	Expiration Date	Action
1	adminnm		All	Disable	mm/dd/yyyy	mm/dd/yyyy	
2	zxvrb		All	Disable	mm/dd/yyyy	mm/dd/yyyy	
3	stevanh@planet.co		Normal User	Disable	mm/dd/yyyy	mm/dd/yyyy	
4	test	login	All	Enable	04/01/2025 01:00 AM	04/04/2030 04:44 AM	
5	daniel	test	All	Disable	mm/dd/yyyy 12:00 AM	mm/dd/yyyy 12:00 AM	
6	Senab155	Enable Authentication	All	Disable	mm/dd/yyyy	mm/dd/yyyy	
7	2		All	Disable	mm/dd/yyyy 12:00 AM	mm/dd/yyyy 12:00 AM	
8	kent	Kent_Test	Admin User	Disable	mm/dd/yyyy	mm/dd/yyyy	
9	fae	fae_test	Normal User	Disable	mm/dd/yyyy	mm/dd/yyyy	

(up to 99 users)

Accounts Export: [Export](#)

Accounts Import: [Choose File](#) No file chosen

[Add](#)

[Apply Settings](#) [Cancel Changes](#)

Figure 5-2 User Account Configuration

Configuration Guide

5.3 Configure User Information

Configure the following information:

Username: test0529

Password: User Password

Description: VPN Test

Account Type: All

Validation Period: Disable

Click:

Add New Passkey

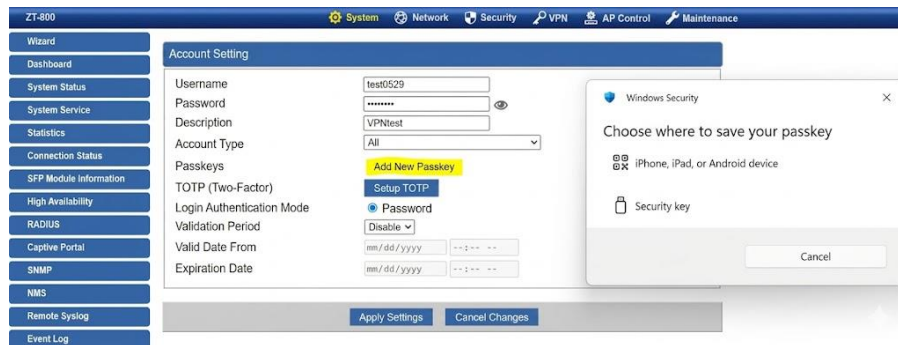


Figure 5-3 User Account Parameters

Configuration Guide

5.4 Register Security Key Passkey

When Windows Security appears:

Select:

Security Key

Enter the Security Key PIN.

Click:

OK

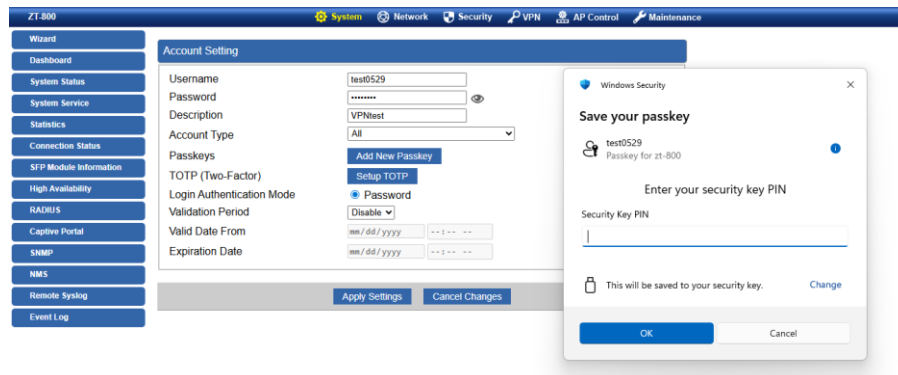


Figure 5-4 Security Key Selection

Configuration Guide

5.5 Touch Security Key

Touch the CoreTrust Security Key when prompted.
Wait for registration to complete.

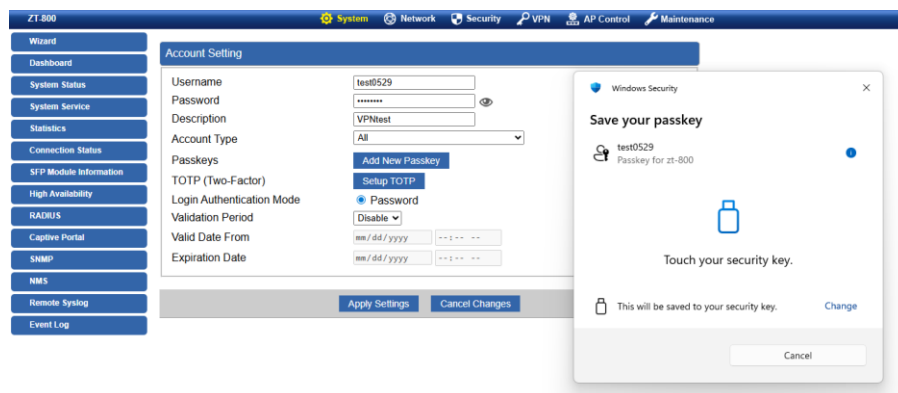


Figure 5-5 Touch Security Key

Configuration Guide

6. WireGuard VPN Configuration

Log in to the ZT-800 Web UI.

Navigate to:

VPN > WireGuard VPN Server

Enable the WireGuard VPN Server.

Configure the WireGuard server parameters:

WireGuard: Enable

Listen Port: 51820

Address (CIDR): 10.10.10.1/24

MTU: 1420

DNS: 8.8.8.8

Interface: LAN

The screenshot displays the ZT-800 Web UI configuration page for the WireGuard VPN Server. The top navigation bar includes links for System, Network, Security, VPN, AP Control, and Maintenance. The left sidebar lists various VPN and network settings. The main configuration area for the WireGuard VPN Server includes the following fields:

- WireGuard: ☒ Enable ☐ Disable
- Listen Port: 51820 (range 1024-65535)
- Address(CIDR): 10.10.10.1/24
- MTU: 1420 (range min: 1280, max: 1500)
- DNS: 8.8.8.8
- Interface: LAN (dropdown menu)
- Public Key: [Redacted]
- Private Key: [Redacted]
- Generate Keypairs button

Below the configuration fields is a 'Peer Info' table:

No.	Name	Address	Active	Action
1	TEST1	10.10.10.2/32		
2	Kent_WireGuard	10.10.10.3/32		

At the bottom of the page are three buttons: Add Peer, Apply Settings, and Cancel Changes.

Figure 6-1 WireGuard VPN Server

7. VPN Portal Login

7.1 Access VPN Portal

Open a browser and enter:

<https://zt-800:8443>

The VPN Self-Service Portal login page will appear.

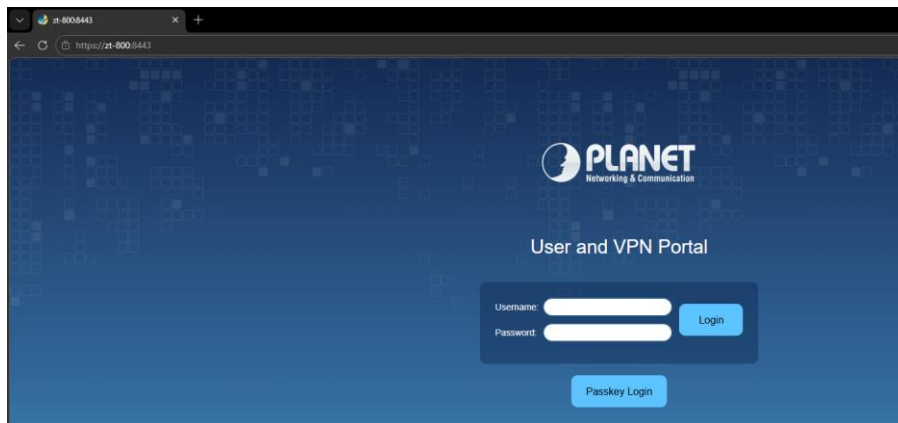


Figure 7-1 VPN Portal Login Page

Configuration Guide

7.2 Login Using Passkey

Click: Passkey Login

Windows Security will prompt for the Passkey authentication method.

Select: Security Key

Enter the Security Key PIN.

Click: OK

Touch the CoreTrust Security Key when prompted.

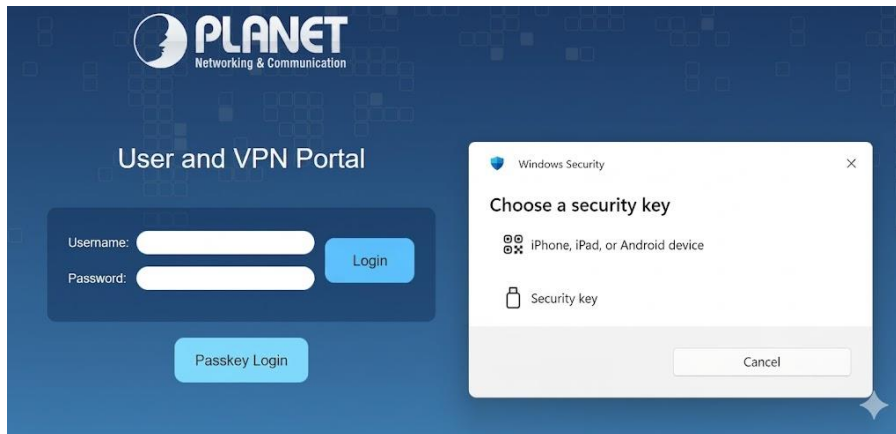


Figure 7-2 Passkey Login

Configuration Guide

7.3 Select VPN Type

After successful authentication, the VPN Self-Service Portal page appears.

Select:

WireGuard

Click:

Continue

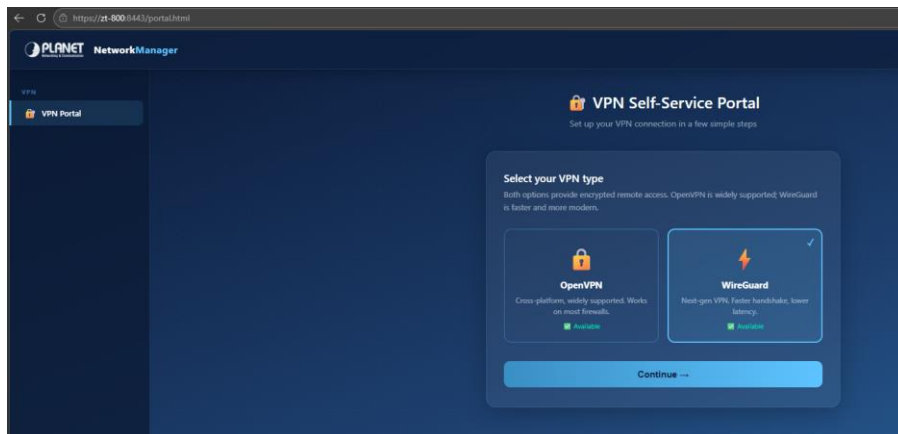


Figure 7-4 VPN Type Selection

Configuration Guide

8. WireGuard Client Connection

8.1 Download VPN Profile

Install and launch the **WireGuard** client software on your PC.

In the WireGuard main window, click:

Import tunnel(s) from file

Select the WireGuard configuration file downloaded from the **ZT-800 VPN Self-Service Portal**.

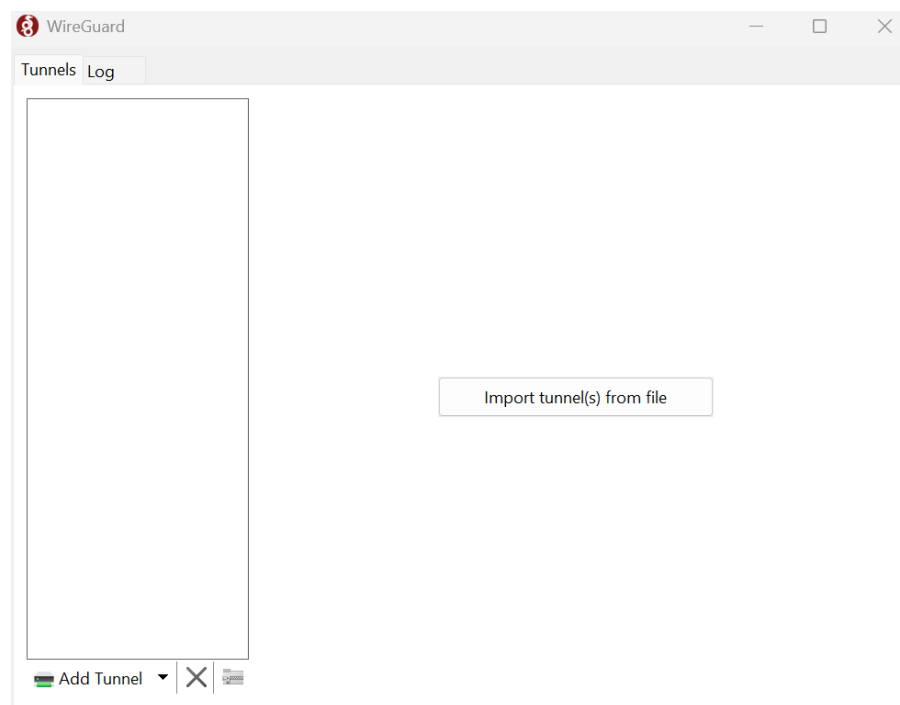


Figure 8-1 Download VPN Profile

Configuration Guide

8.2 Import VPN Profile

After the configuration file is imported successfully, a new tunnel profile (for example, **wireguard_client**) will appear in the tunnel list.

Verify that the imported profile contains the following information:

Tunnel Address: 10.10.10.2/32

DNS Server: 8.8.8.8

Endpoint: zt-800:51820

Select the imported WireGuard tunnel profile.

Click **Activate**.

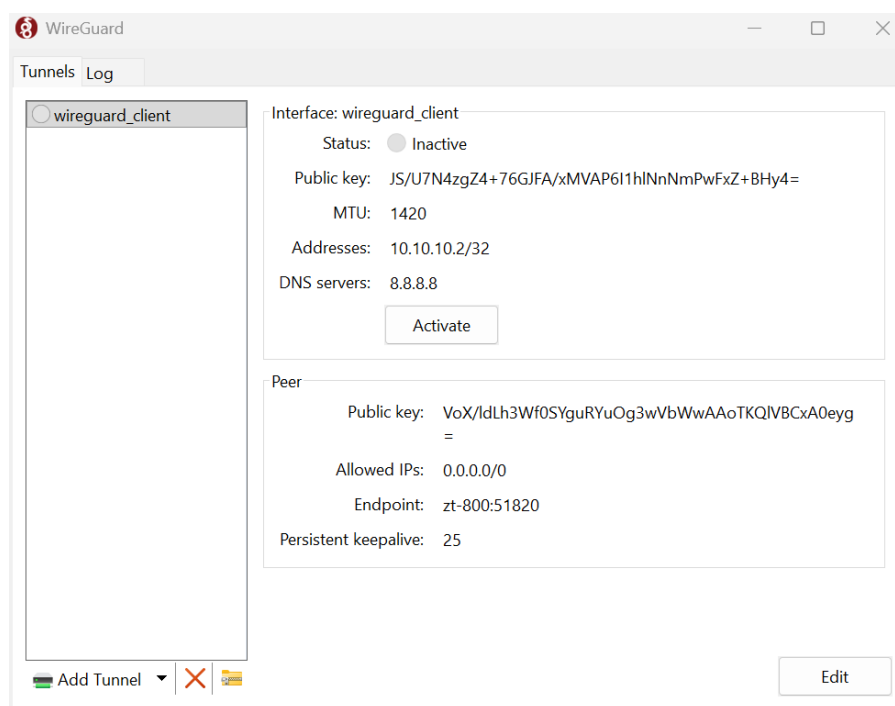


Figure 8-2 Import Tunnel

Configuration Guide

8.3 Verify Tunnel Configuration

Wait for the WireGuard client to establish the VPN connection.

When the connection is successful, the tunnel status will change from:

Inactive to:Active

Verify the connection status information:

Status: Active

Latest Handshake: Available

Transfer Statistics: Receiving and Sending Traffic

Confirm that the Endpoint has been resolved correctly and the VPN tunnel is operational.

Example:

Endpoint: 210.61.134.91:51820

The VPN connection is now established successfully, and the client can securely access resources behind the ZT-800 WireGuard VPN server.

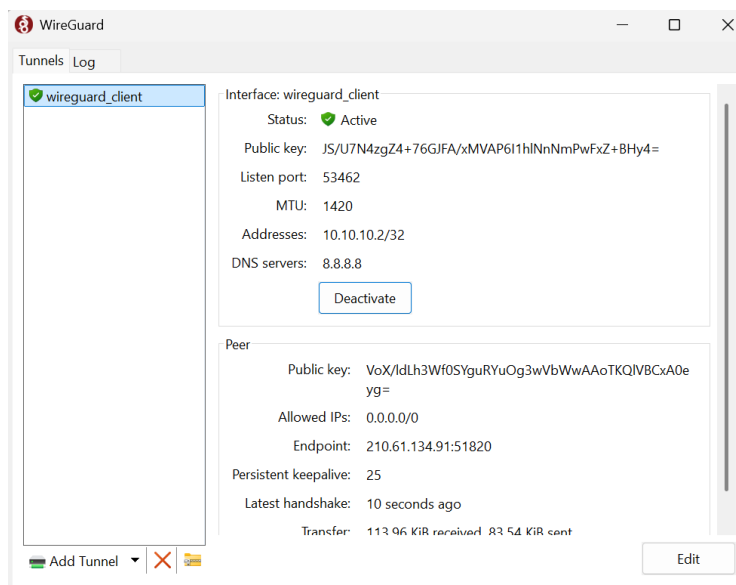


Figure 8-3 Tunnel Information

Configuration Guide

9. Customer Support

Thank you for purchasing PLANET products. You can browse our online FAQ resource and User's Manual on PLANET Web site first to check if it could solve your issue. If you need more support information, please contact PLANET support team.

PLANET online FAQs:

<https://www.planet.com.tw/en/support/faq>

Support team mail address:

support@planet.com.tw

ZT-800 User's Manual:

<https://www.planet.com.tw/en/support/download.php?&method=keyword&keyword=ZT-800&view=3#list>



(Please select your switch model name from Product Model drop-down menu)

Copyright © PLANET Technology Corp. 2026.

Contents are subject to revision without prior notice.

PLANET is a registered trademark of PLANET Technology Corp. All other trademarks belong to their respective owners.



Configuration Guide

EU Representative

PLANET Technology Europe B.V.

Address: Posthoornstraat 11, 3011 WD Rotterdam, NL

Email: eu_rep@planet.com.tw

URL: www.planet.com.tw