



# ShareTech UTM Solution

Website  
www.sharetech.com.tw/en-us

Sales Info  
sales@sharetech.com.tw

Tech Support  
help@sharetech.com.tw



## Implementing Zero Trust in Enterprises, ShareTech UTM Supports Multi-Factor Authentication (MFA)

(Administrator Account / Internet Authentication / SSL VPN / ZTA VPN)

Unlike traditional network services that rely on single-factor authentication (password only), **Multi-Factor Authentication (MFA)** requires users to pass **two or more authentication mechanisms** before being authorized to access system resources. Common verification methods include PIN codes, fingerprints, QR code scanning, and one-time passwords (OTPs). The goal is to provide higher security protection for user accounts.

The MFA feature integrates with **Google Authenticator**, **Microsoft Authenticator**, or a **third-party authenticator** for verification, and supports **passwordless authentication** performing QR code scanning or biometric identification.

By default, this feature is disabled. After enabling it, the system will prompt for both a password and a one-time code before allowing account access.

	Features	Two-Step Verification	Passwordless Authentication (ShareTech Authenticator App)
UTM Series	Administrator Account	○	○
	Authentication (Local/POP3,IMAP/RADIUS/AD Server)	○	○ (Available for Local and AD Server only)
	SSL VPN	○	×
	ZTA VPN	○	△ (Will be supported later)

**Note:** For HiGuard Series (firmware HX 9.0.2.3 and above) / NU Series (NU 9.0.2.4 and above), newly added two-step verification for RADIUS and AD authentication.

## 1. Administrator Account

Go to [Configuration](#) → [Administration](#) → [Administrator](#) → [Add](#) and add **two-step verification** or **Passwordless Authentication** for administrator accounts.

**Note:** For ShareTech UTM devices running firmware v9.0.2.2 or above, administrator can use their mobile phone as the second authentication factor.

Administrator										
Account and Privilege										
Account	Privilege	User Defined Menu	Enable	Account Expiration Date	Password Alter Date	Require Password Change	Notes	2-Step Verification	Passwordless Authentication	
<input type="checkbox"/>	yo	All Privileges	<input checked="" type="checkbox"/>	--	2025-02-14			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	KHH	All Privileges	<input checked="" type="checkbox"/>	--	2025-02-14			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

▲ Figure 1

**Example 1:** Require two-step verification the administrator logs in.

**Administrator** | Account Security Setting | IP Address | Clear Data | USB Backup Log

**Add New Administrator**

Enable

Account

Password  (Please input 3 to 64 characters, not the same with account)

Password Strength:  Weak  Fair  Strong

Confirm Password

Change their passwords the next time they sign in

Change password every  day(s) (0 means no limit)

PSWD cannot be the same as old one(s)  times

Account Expiration Date

Notes

**2-Step Verification**  Enable  Key Information : Is Not Enabled

Passwordless Authentication  Enable

Privilege

User Defined Menu

◀ Figure 2

**NU-6000**

Account

Password

Remember Account and Password

English

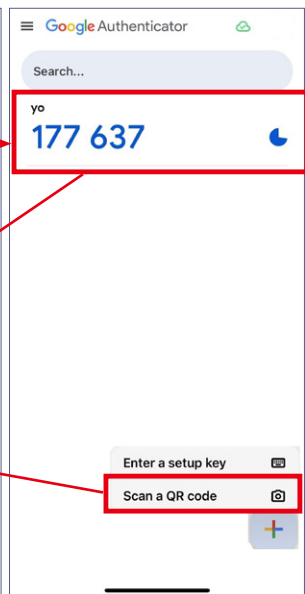
◀ Figure 3

The initial binding [2-Step Verification](#) screen.

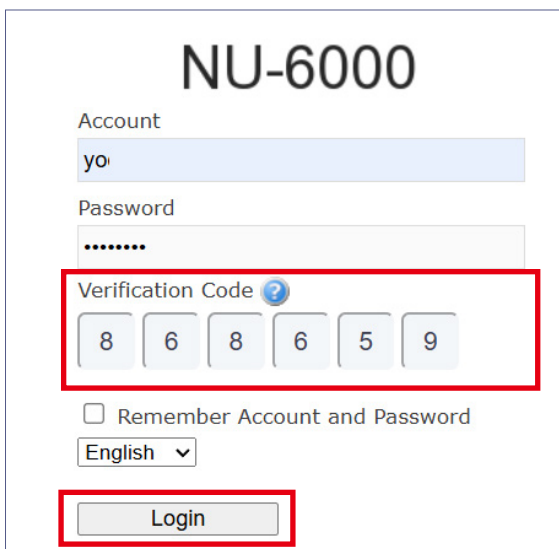
You can use Microsoft Authenticator, Google Authenticator, or a third-party authenticator app.



▲ Figure 4



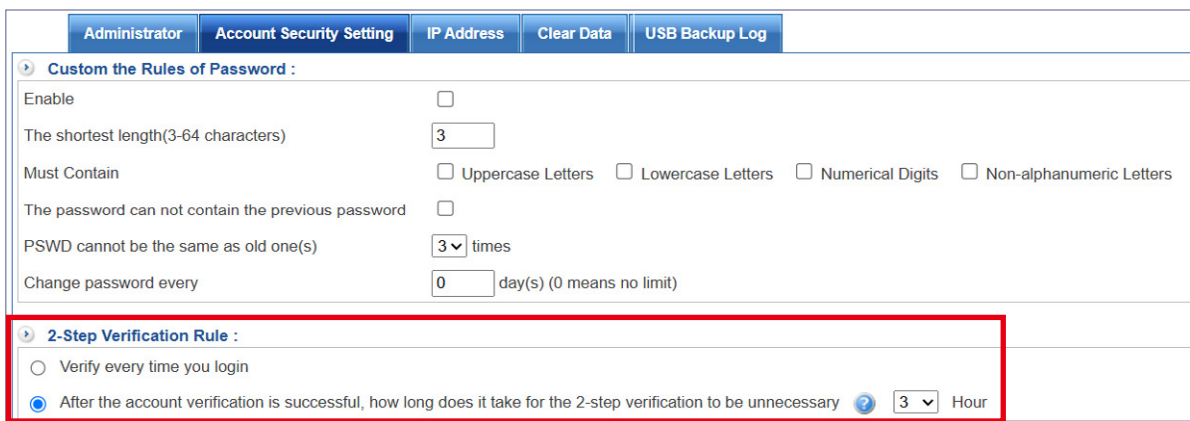
▲ Figure 5



◀ Figure 6

Besides, administrators can choose:

- to perform two-step verification [every login](#), or
- to skip secondary verification for a specific time period after a successful login.



▲ Figure 7

**Example 2:** Require Passwordless Authentication the administrator logs in.

The screenshot shows the 'Add New Administrator' configuration page. At the top, there are tabs for 'Administrator', 'Account Security Setting', 'IP Address', 'Clear Data', and 'USB Backup Log'. The 'Add New Administrator' section includes the following fields and options:

- Enable:**
- Account:**
- Password:**  ( Please input 3 to 64 characters, not the same with account )
- Password Strength:** Weak | Fair | Strong
- Confirm Password:**
- Change their passwords the next time they sign in:**
- Change password every:**  day(s) (0 means no limit)
- PSWD cannot be the same as old one(s):**  times
- Account Expiration Date:**
- Notes:**
- 2-Step Verification:**  Enable. Key Information : Is Not Enabled.
- Passwordless Authentication:**  Enable.  (This row is highlighted with a red box)
- Privilege:**
- User Defined Menu:**

At the bottom right, there is a  button.

◀ Figure 8

The screenshot shows the login screen for 'NU-6000'. It includes the following elements:

- Account:**  (This field is highlighted with a red box)
- Password:**
- Remember Account and Password:**
- Language:**
- Login:**
- Login Without Password:**  (This button is highlighted with a red box)

◀ Figure 9

The initial binding [Passwordless Authentication](#) screen.

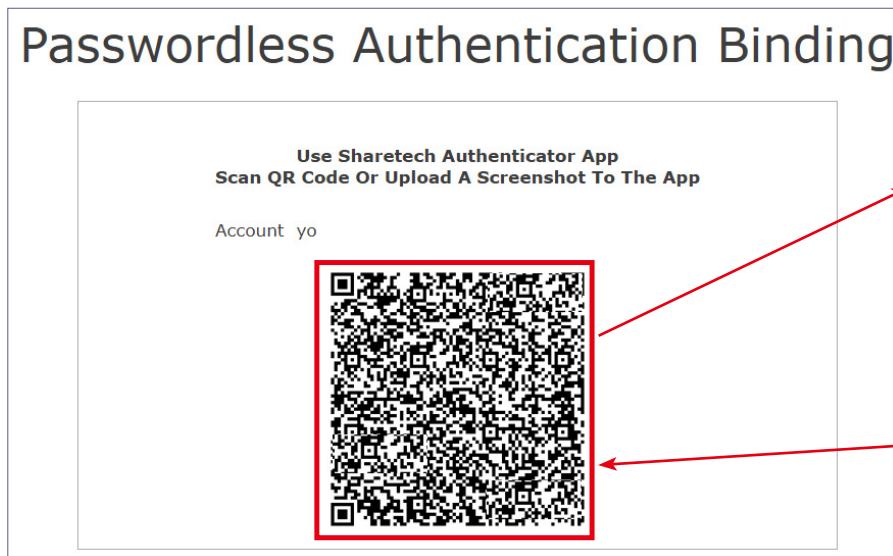
The screenshot shows a dialog box titled 'Passwordless Authentication Binding'. The message inside says 'Please enter the password to bind.' Below the message, there is a form with the following fields:

- Account:** yo
- Password:**  (This field is highlighted with a red box)

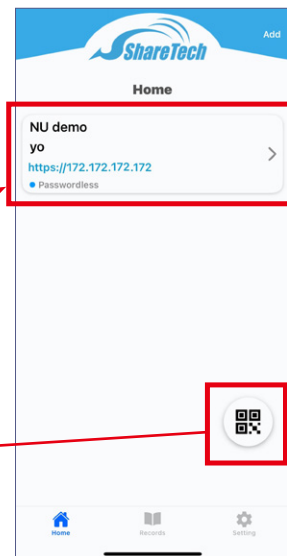
At the bottom of the dialog, there is an  button.

◀ Figure 10

Please download the [ShareTech Authenticator app](#) from the App Store.

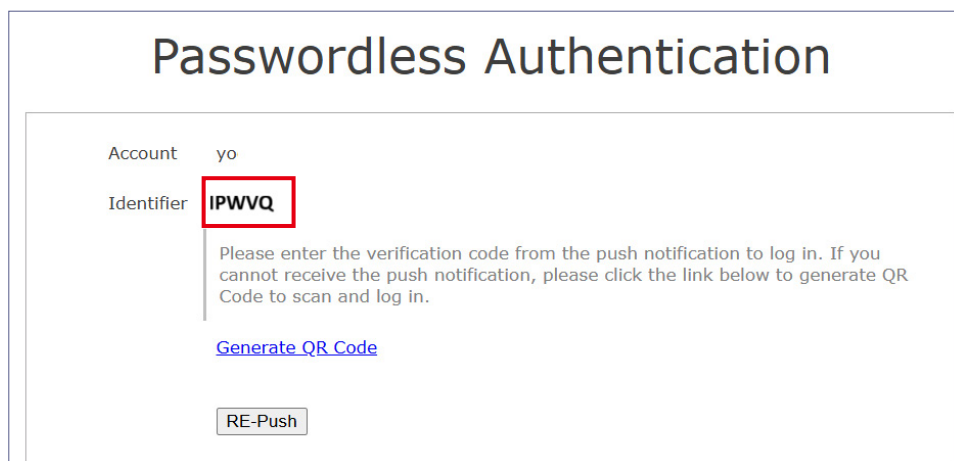


▲ Figure 11



▲ Figure 12

The login screen after binding [Passwordless Authentication](#).

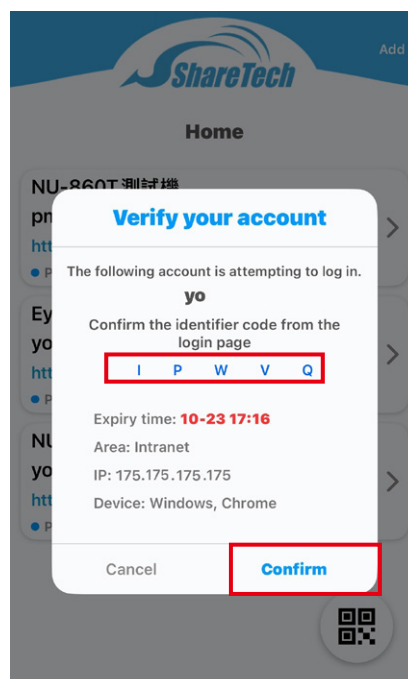


◀ Figure 13

A notification window will pop up on your phone and verify your account.



◀ Figure 14

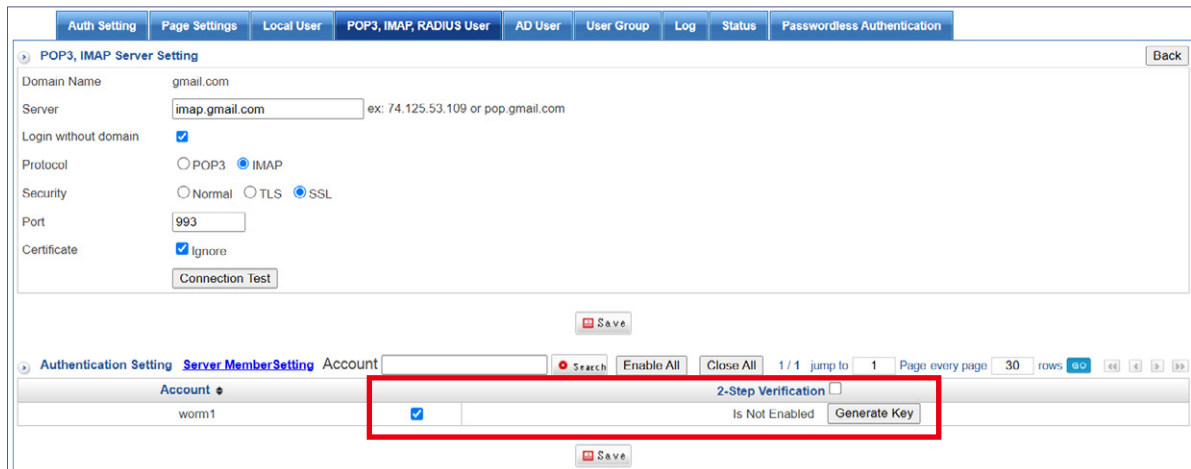


◀ Figure 15

## 2. Internet Authentication

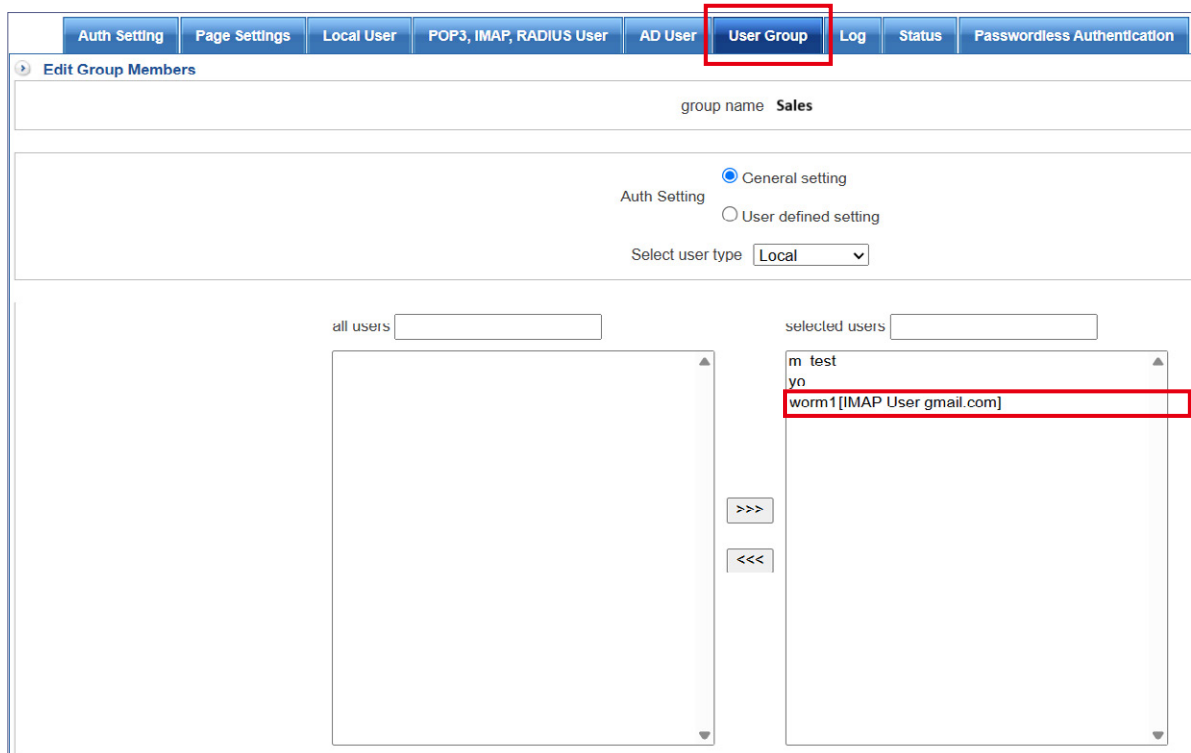
Go to [Object](#) → [Authentication](#) → Select authentication mode (Local User / POP3, IMAP / RADIUS / AD Server)

**Example 1:** Using the [IMAP Server](#) → [User Group](#) with **two-step verification**.



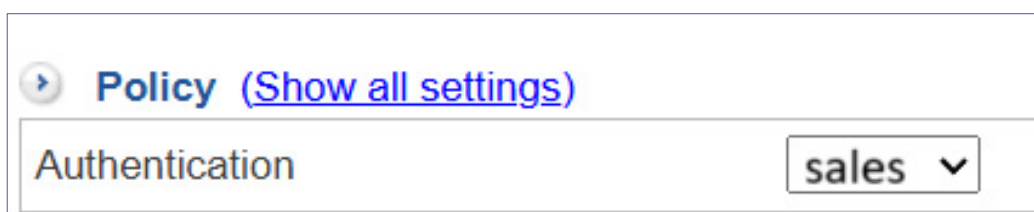
▲ Figure 16

Set up a User Group.



▲ Figure 17

[Policy](#) → [Security Policy](#) → [Outgoing](#)

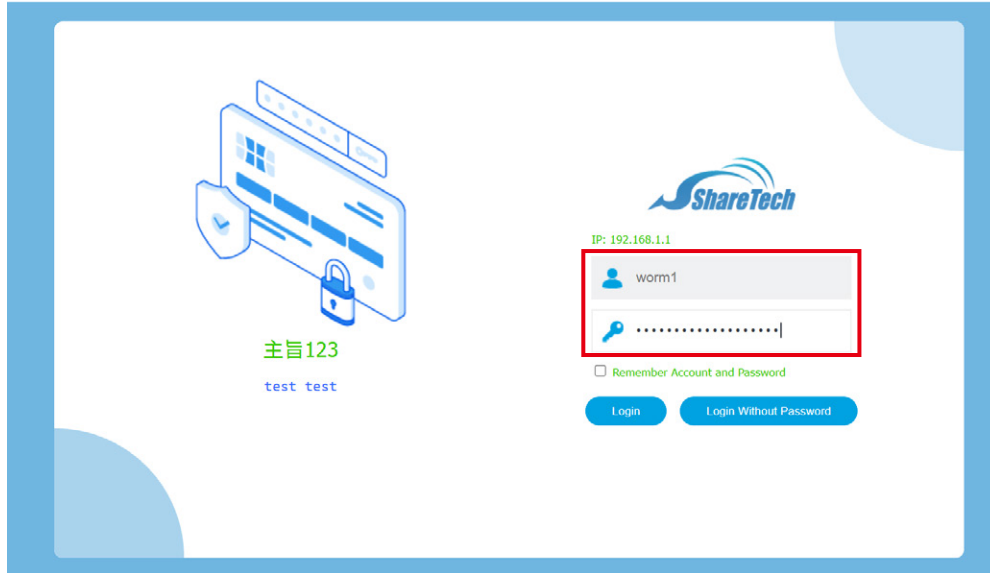


◀ Figure 18

After enabling **two-step verification**, users will be required to:

- 1. Enter **account and password**, and
- 2. Then input the **verification code generated by Microsoft Authenticator, Google Authenticator, or a third-party authenticator app.**

Only after both verifications are successful can users log in.



▲ Figure 19

The initial binding **2-Step Verification** screen.

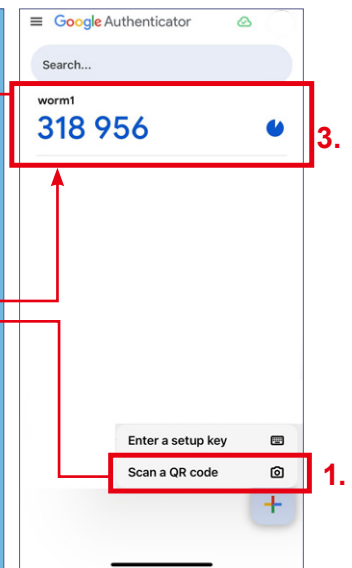
You can use **Microsoft Authenticator, Google Authenticator, or a third-party authenticator app.**

**Note:** The verification code allows for a time drift of up to one minute.

**Note:** When two-step verification is first enabled (no key generated yet) or when a key is changed, the verification screen will automatically generate a key for the user to configure.



▲ Figure 20



▲ Figure 21

The login screen after binding [2-Step Verification](#) screen and then enter the verification code to proceed to surf Internet.

**Note:** When a key has already been generated, the verification page (QR Code) will **not** display key information.



▲ Figure 22

Administrators can check the authentication connection status.

group name	Account	IP	MAC	Kick	Group Kick
sales	worm1	165.165.165.165	a8:a8:a8:a8:a8:a8	<a href="#">Kick</a>	<a href="#">Kick</a>

▲ Figure 23

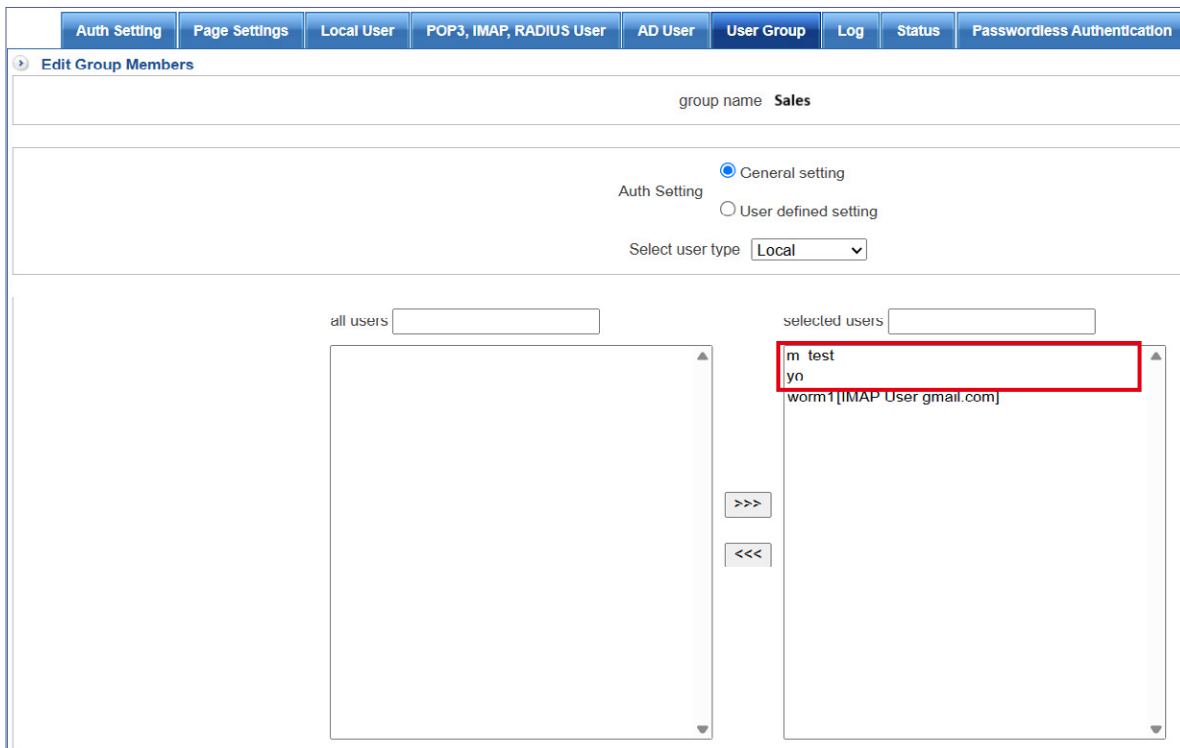
**Example 2:** Using the [Local User](#) → [User Group](#) with **passwordless authentication**.

**Note:** Accounts that enable passwordless authentication will not perform password authentication with the host. Only account status will be checked.

Name	Account	Require Password Change at Next Login	Account Expiration Date	2-Step Verification	Passwordless Authentication
yo	yo	No		✓	✓
m test	m	No	2025-05-31	✓	✓

▲ Figure 24

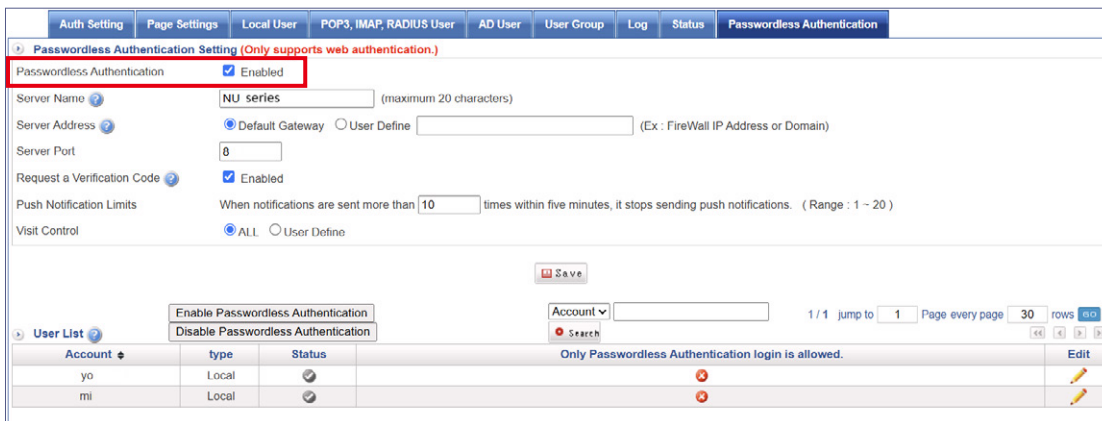
Set up a User Group.



▲ Figure 25

Object → Authentication → Passwordless Authentication

Enable “Passwordless Authentication.”



▲ Figure 26

Policy → Security Policy → Outgoing



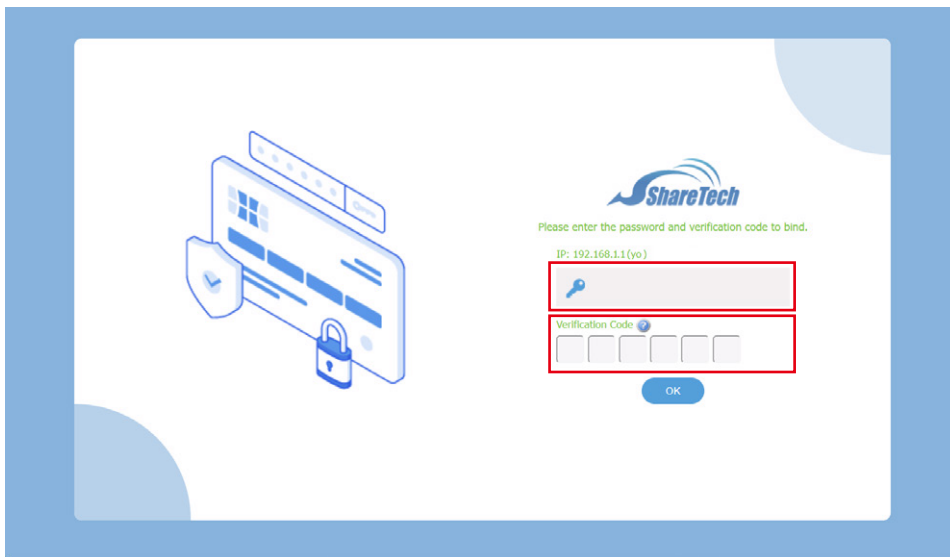
◀ Figure 27

After enabling **passwordless authentication**, users will be required to:

- 1. Enter **username only**, and
- 2. Then input the **verification code** generated by **two-step verification**.
- 3. User use(download) **ShareTech Authenticator App** scan QR Code.



◀ Figure 28



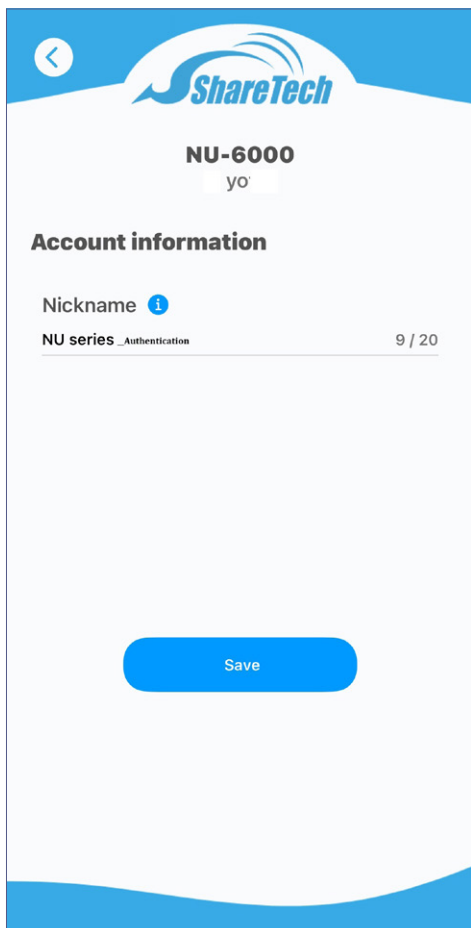
◀ Figure 29



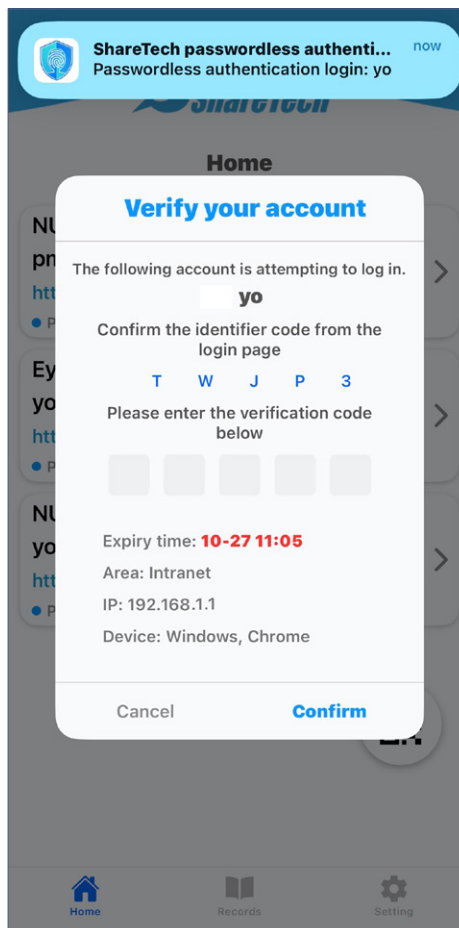
▲ Figure 30



▲ Figure 31

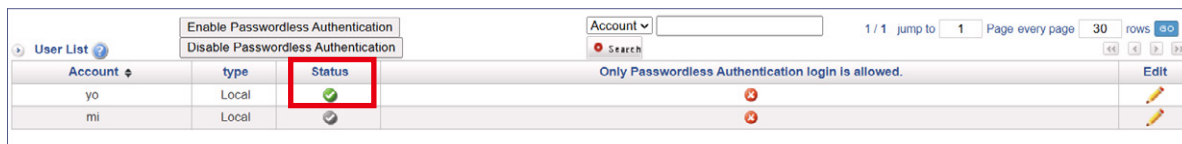


▲ Figure 32



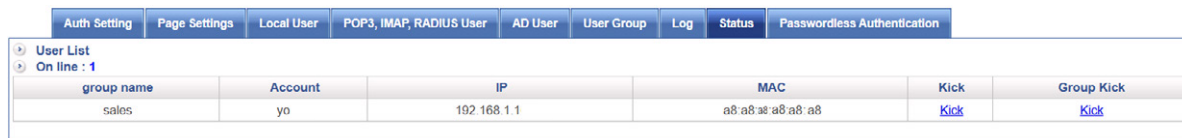
▲ Figure 33

After user use **passwordless authentication** through QR code scanning or biometric identification.

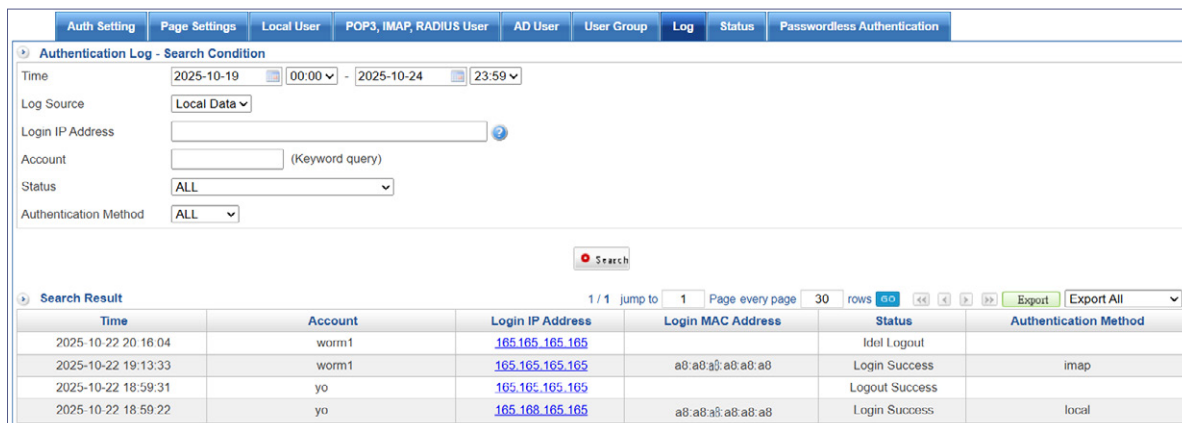


▲ Figure 34

Administrators can check the authentication connection status and search for historical logs.



▲ Figure 35



▲ Figure 36

**Example 3:** Using the AD Server with passwordless authentication.

▲ Figure 37

**Note:** Accounts that enable passwordless authentication will not perform password authentication with the host. Only account status will be checked.

▲ Figure 38

### 3. SSL VPN

Go to **VPN** → **SSLVPN Server** → **SSL VPN Setup** → Start “SSL VPN”

▲ Figure 39

Go to [VPN](#) → [SSLVPN Server](#) → [SSL Client List](#)

Before adding a new SSL VPN client, it is necessary to create an authentication group and select the group members for online authentication. (see the earlier Object → Authentication screen example).

Users can access it directly via a download URL that the administrator must preconfigure:

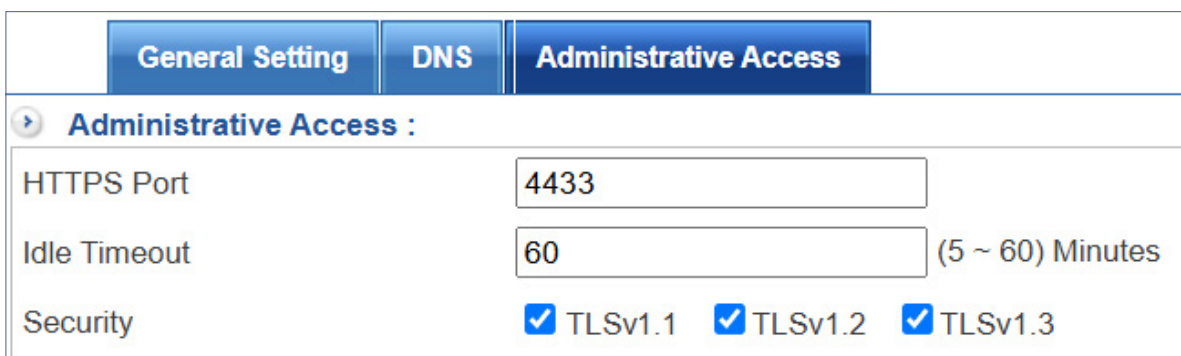
[https://\[interface\\_IP\\_or\\_domain\]:\[HTTPS\\_port\]/sslvpn.php](https://[interface_IP_or_domain]:[HTTPS_port]/sslvpn.php)

**Example:** <https://168.168.168.168:4433/sslvpn.php> or <https://domain:4433/sslvpn.php>

**Note:** When two-step verification is enabled, users can refer to the [SSL VPN for User Guide \(Two-Step Verification\)](#) for detailed instructions. (Windows, iOS, Android, macOS)

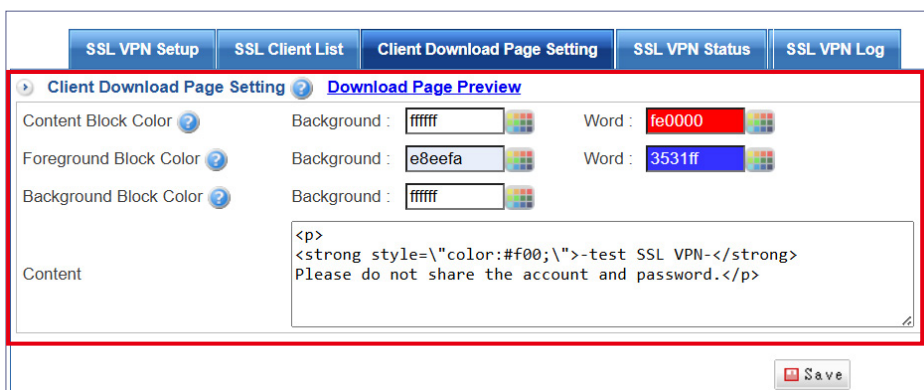


▲ Figure 40



▲ Figure 41

Go to [VPN](#) → [SSLVPN Server](#) → [Client Download Page Setting](#)



◀ Figure 42



◀ Figure 43

The initial binding **2-Step Verification** screen.

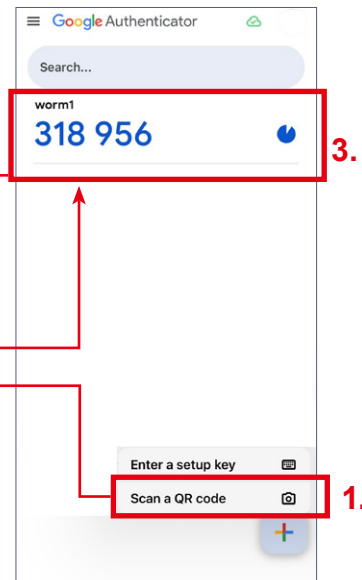
You can use [Microsoft Authenticator](#), [Google Authenticator](#), or [a third-party authenticator app](#).

**Note:** The verification code allows for a time drift of up to one minute.

**Note:** When two-step verification is first enabled (no key generated yet) or when a key is changed, the verification screen will automatically generate a key for the user to configure.



▲ Figure 44



▲ Figure 45

The login screen after binding **2-Step Verification** screen and then enter the verification code to proceed to the download SSL VPN software page.

**Note:** When a key has already been generated, the verification page (QR Code) will not display key information.



▲ Figure 46

Besides, if this feature is enabled, the validity of two-step verification can be extended for **1-24 hours**.

Within this period, the same IP source, account, or code remains valid which allowing users to reconnect without re-entering the verification code after temporary disconnections.

**Note:** For HiGuard Series firmware HX 9.0.2.3 and above / NU Series firmware NU 9.0.2.4 and above, a new Two-Step Verification Validity Extension feature is added.



◀ Figure 47

Administrators can check the authentication connection status and can search for historical logs.

Account	Status	Source IP Address	Local IP Address	Last Connection	Local Interface	Kick
yo				2025-10-23 15:18:51		<a href="#">Kickyo</a>
worm1		36.236.36.236.365	10.8.0.10	2025-10-24 12:12:11	WAN1 PPPOE (WAN1)	<a href="#">Kickworm1</a>
mi						<a href="#">Kickmi</a>

▲ Figure 48

**SSL VPN Log - Search Condition**

Time: 2025-09-07 00:00 - 2025-10-24 23:59

Log Source: Local Data

Account: [ ]

Source IP: [ ]

The machine dispensed IP: [ ]

Local Interface: All

Event: All

---

**Search Result**

Time	Account	Source IP	The machine dispensed IP	Local Interface	Event
2025-10-24 12:13:48	worm1	36.236.36.236	10.8.0.10	WAN1 PPPOE (WAN1)	Logout
2025-10-24 12:12:11	worm1	36.236.36.236	10.8.0.10	WAN1 PPPOE (WAN1)	Login
2025-10-23 15:18:51	yo	42.42.425.42	10.8.0.6	WAN1 PPPOE (WAN1)	Logout
2025-10-23 15:17:20	yo	42.42.425.42	10.8.0.6	WAN1 PPPOE (WAN1)	Login

▲ Figure 49

## 4. ZTA VPN

Go to [ZTA VPN](#) → [Client-to-Site](#) → [ZTA VPN Setup](#) → Start “ZTA VPN”

**ZTA VPN Setup** | Client List | Page Setting | Connection Status | Connection Log

**Server Setting** [Modify the Server Setting](#) \* means that after the configuration changes, you need to redownload the certificate to apply the new settings.

Service Status: **Start**

Enable:  Note . It will take a while to activate the ZTA VPN. Please wait patiently.

Local Interface:  Hide [Change](#)  
ppp4000

Client Linking Setting \* :  Hide [Change](#)  
ppp4000

Local Port \* :  (Use both TCP and UDP protocols)

Max concurrent connections:  ( Range: 20 ~ 200 )

Connection Timeout :  seconds ( Range: 30 ~ 180 )

2-Step Verification Expiry Time :  Minutes ( Range: 10 ~ 60, 0 means disabled. )

Client IP Range:  /  ( Client IP range need different with Zone interface. )

DNS Server 1:

DNS Server 2:

▲ Figure 50

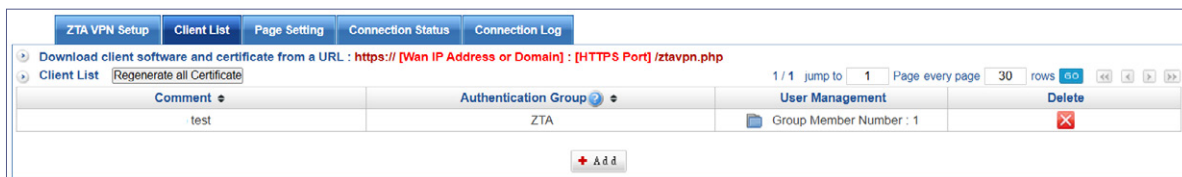
Go to [ZTA VPN](#) → [Client-to-Site](#) → [Client List](#)

Before adding a new ZTA VPN client, it is necessary to create an authentication group and select the group members for online authentication. (see the earlier Object → Authentication screen example).

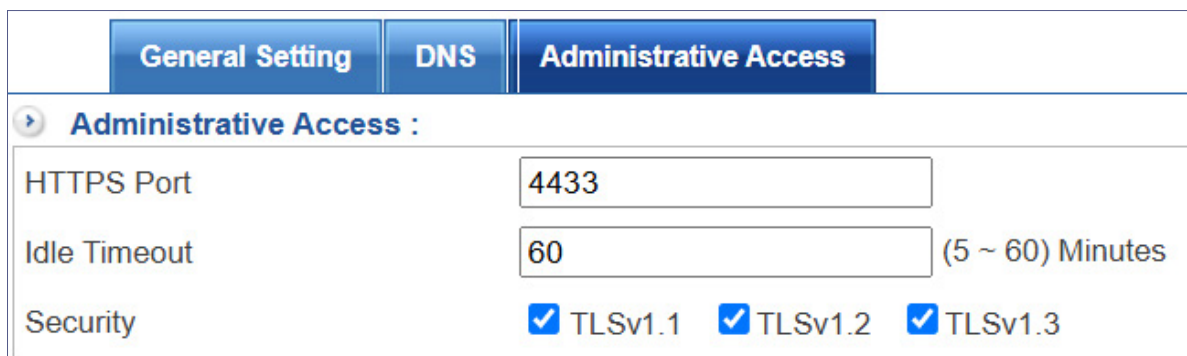
Users can access it directly via a download URL that the administrator must preconfigure:  
[https://\[interface\\_IP\\_or\\_domain\]:\[HTTPS\\_port\]/ztavpn.php](https://[interface_IP_or_domain]:[HTTPS_port]/ztavpn.php)

**Example:** <https://168.168.168.168:4433/ztavpn.php> or <https://domain:4433/ztavpn.php>

**Note:** When two-step verification is enabled, users can refer to the [ZTA VPN for User Guide \(Two-Step Verification\)](#) for detailed instructions. (Windows)

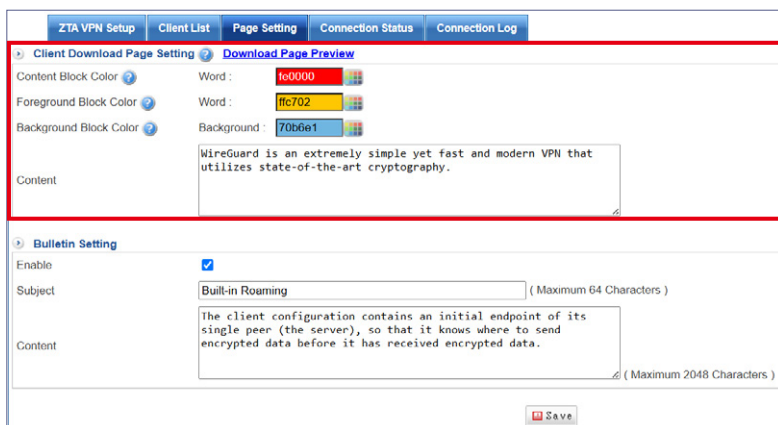


▲ Figure 51



▲ Figure 52

Go to [ZTA VPN](#) → [Client-to-Site](#) → [Page Setting](#)



◀ Figure 53



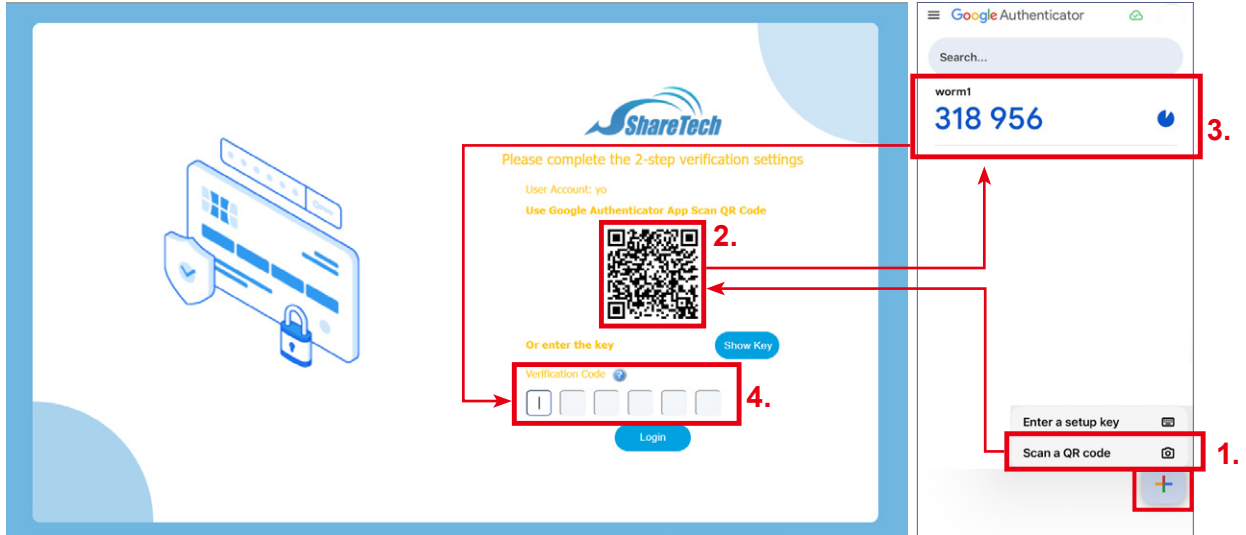
◀ Figure 54

The initial binding [2-Step Verification](#) screen.

You can use [Microsoft Authenticator](#), [Google Authenticator](#), or a [third-party authenticator app](#).

**Note:** The verification code allows for a time drift of up to one minute.

**Note:** When two-step verification is first enabled (no key generated yet) or when a key is changed, the verification screen will automatically generate a key for the user to configure.

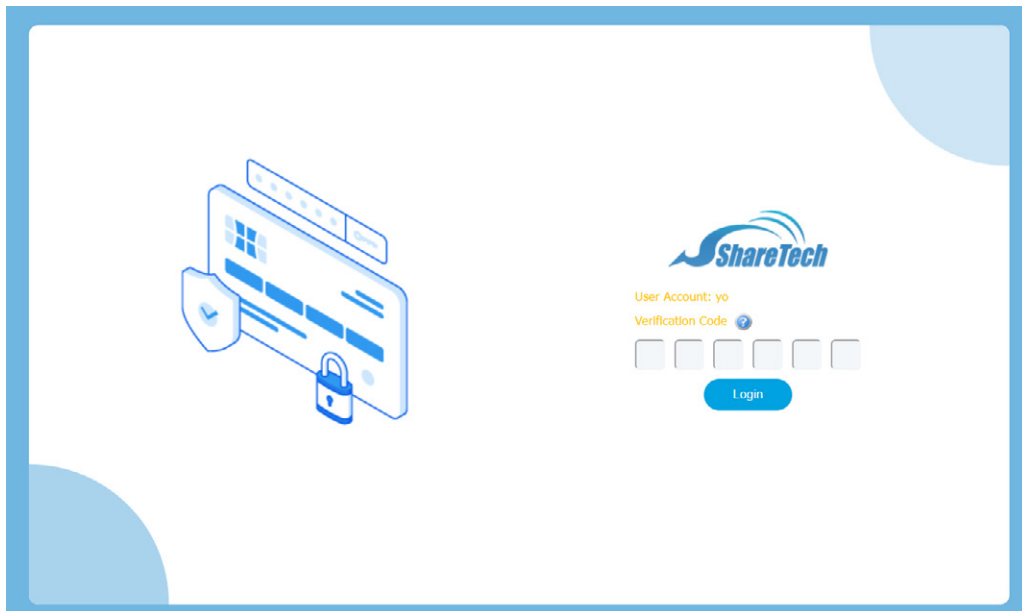


▲ Figure 55

▲ Figure 56

The login screen after binding [2-Step Verification](#) screen and then enter the verification code to proceed to surf Internet.

**Note:** When a key has already been generated, the verification page (QR Code) will **not** display key information.



▲ Figure 57

After a successful login, auto reconnection can bypass 2-step verification before the code expires.



▲ Figure 58

Administrators can check the authentication connection status and can search for historical logs.

Account	Status	Source IP Address	Local IP Address	MAC	Last Connection / Connection Duration	Local Interface	Kick
yo					2025-09-11 15:13:06		<a href="#">Kickyou</a>

▲ Figure 59

Time	Account	Source IP	Source Port	The machine dispensed IP	MAC	Local Interface	Event
2025-09-17 16:18:21	ist26	2'	3	34	10.0.1.101	WAN1 PPPOE (WAN1)	Logout
2025-09-17 16:05:29	esl8	6		33	10.0.1.146	WAN1 PPPOE (WAN1)	Logout
2025-09-17 16:01:04	ist38	6		70	10.0.1.5	WAN1 PPPOE (WAN1)	Logout (Connection Timeout)
2025-09-17 15:07:48	esl7	2'	3	32	10.0.1.169	WAN1 PPPOE (WAN1)	Logout
2025-09-17 14:44:15	ist18	;		37	10.0.1.236	WAN1 PPPOE (WAN1)	Logout
2025-09-17 14:36:45	est0	6		33	10.0.1.146	WAN1 PPPOE (WAN1)	Login
2025-09-17 14:30:58	esl4	2'	3	37	10.0.1.234	WAN1 PPPOE (WAN1)	Logout
2025-09-17 14:30:16	esl4	2'	3	37	10.0.1.234	WAN1 PPPOE (WAN1)	Login
2025-09-17 14:28:49	esl7	2'	3	32	10.0.1.169	WAN1 PPPOE (WAN1)	Login
2025-09-17 14:25:54	esl7	2'	3	39	10.0.1.203	WAN1 PPPOE (WAN1)	Logout

▲ Figure 60