Part 1: Product Introduction

System Overview

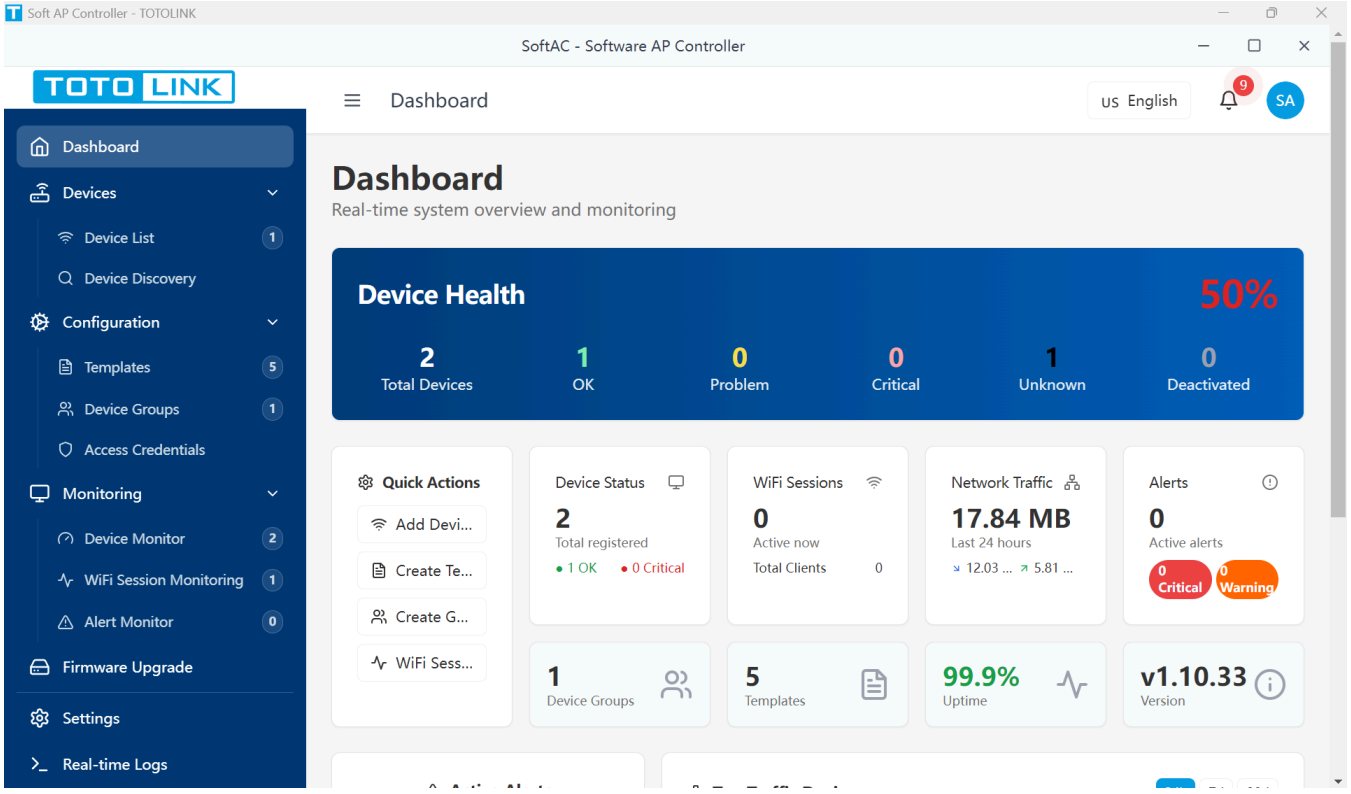
1.1 What is SoftAC

TOTOLINK SoftAC (Software Access Controller) is a centralized wireless network management system designed for businesses and organizations. It allows you to manage multiple TOTOLINK wireless access points (APs) and routers from a single, easy-to-use interface on your computer.

Think of SoftAC as the control center for your wireless network. Instead of configuring each device individually by logging into them one by one, you can manage all your network devices from one place, saving time and reducing complexity.

Key Benefits

- **Centralized Management**: Control all your network devices from one dashboard
- **Easy Setup**: Automatic device discovery and simple configuration wizards
- **Real-time Monitoring**: See device status and network performance at a glance
- **Batch Operations**: Apply settings to multiple devices simultaneously
- **Multi-platform**: Works on Windows, macOS and Linux computers

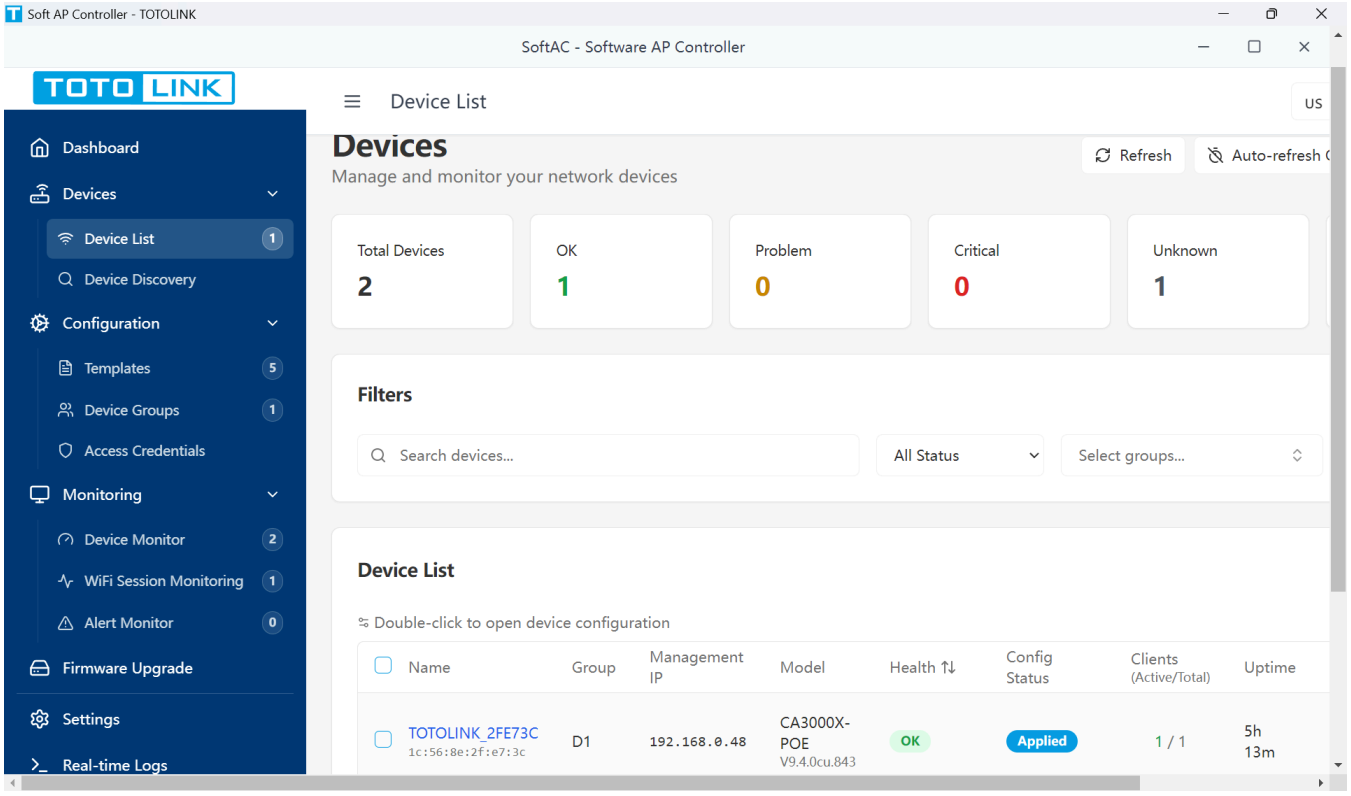


1.2 Main Features

TOTOLINK SoftAC provides comprehensive features to simplify your network management tasks:

Device Management

- **Add and Configure Devices**: Easily add new APs and routers to your network
- **Device Groups**: Organize devices by location, floor, or department
- **Batch Configuration**: Apply settings to multiple devices at once
- **Device Status Monitoring**: Real-time visibility of device health and connectivity

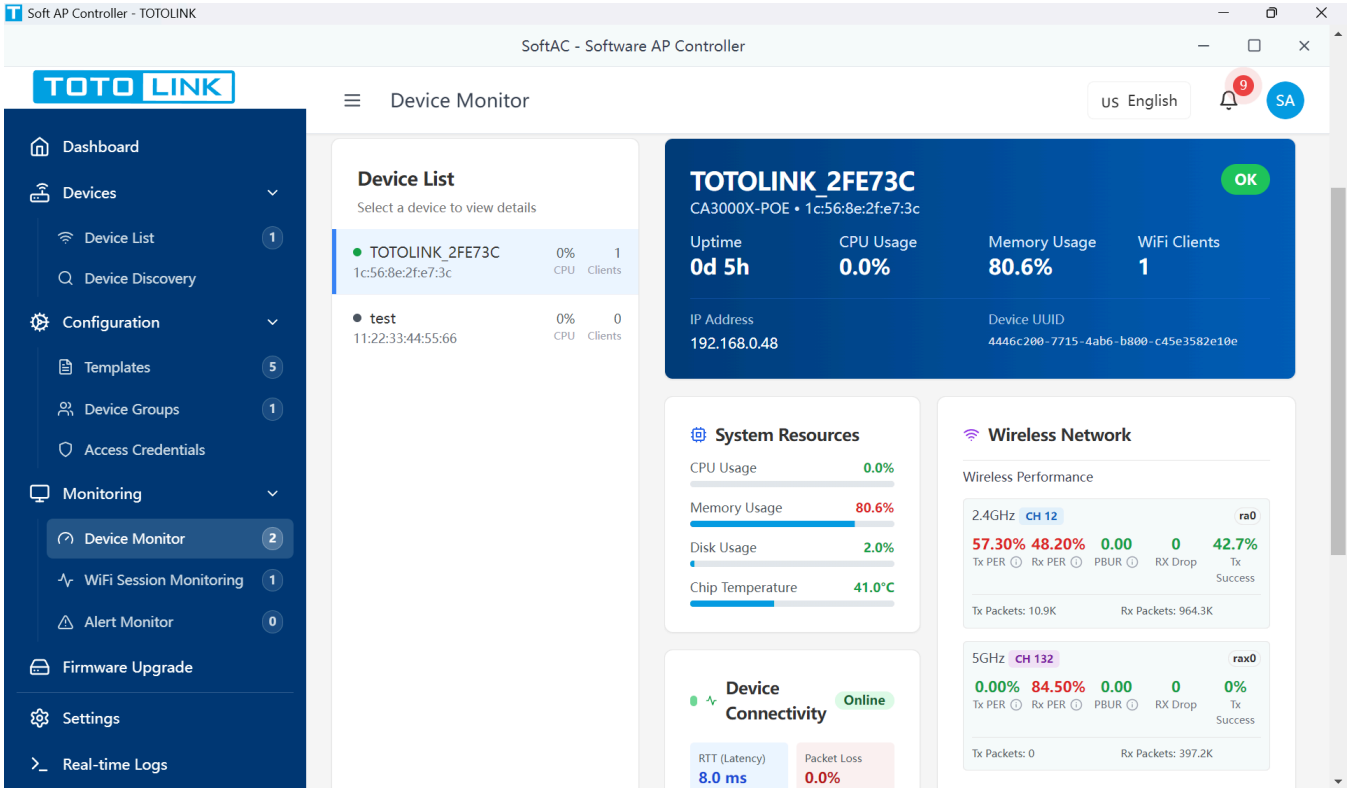


Configuration Templates

- **Pre-defined Templates**: Use ready-made configurations for common scenarios
- **Custom Templates**: Create your own templates for specific needs
- **Template Variables**: Customize settings without editing the entire template
- **Version Control**: Track changes and revert if needed

Network Monitoring

- **Real-time Dashboard**: View network statistics and performance metrics
- **WiFi Session Tracking**: Monitor connected users and their usage
- **Alert Management**: Receive notifications about network issues
- **Traffic Analysis**: Understand bandwidth usage patterns



Firmware Management

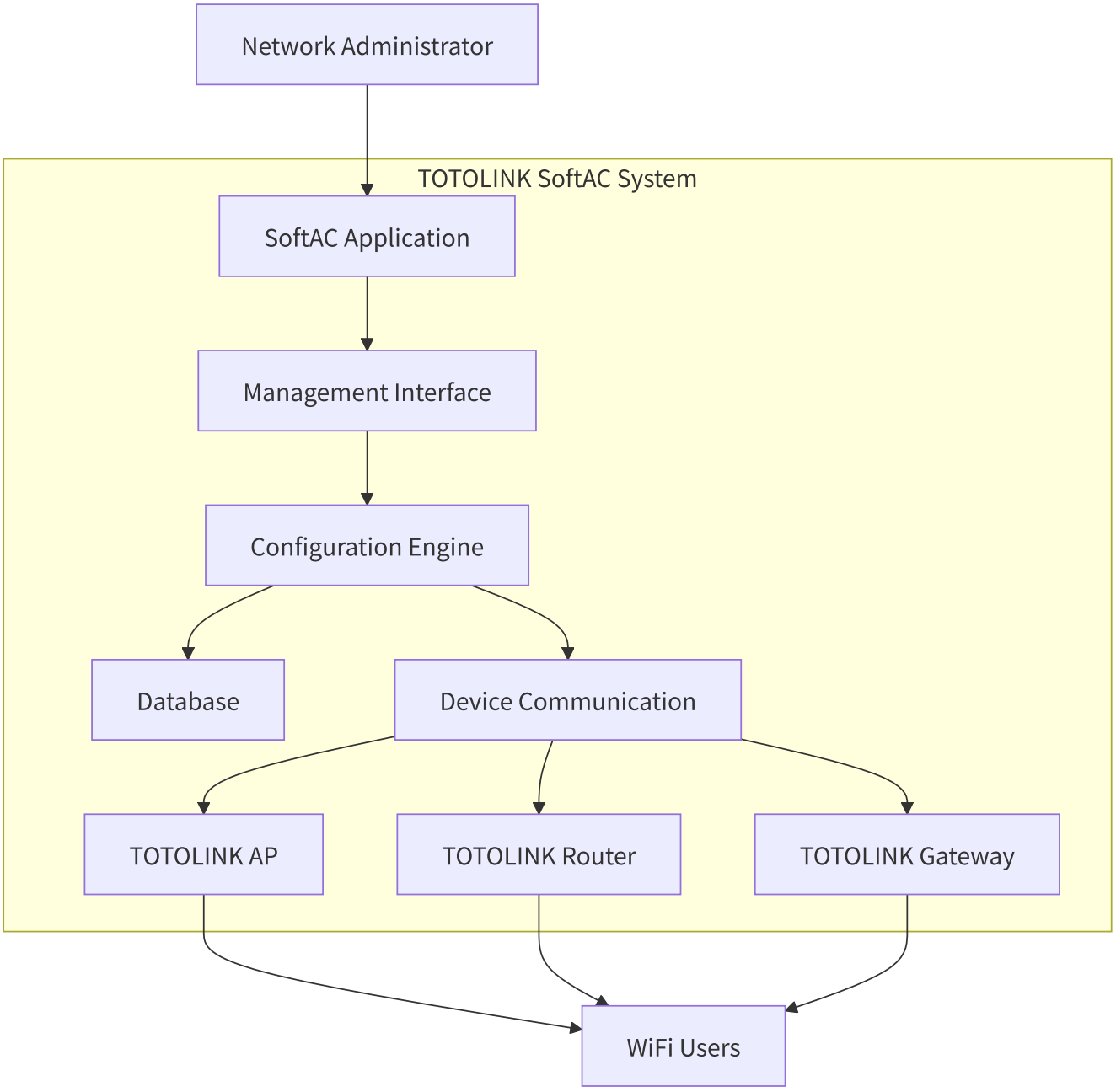
- **Centralized Updates**: Update device firmware from SoftAC
- **Batch Upgrades**: Update multiple devices simultaneously
- **Scheduled Updates**: Plan firmware updates during maintenance windows
- **Version Tracking**: Keep track of firmware versions across all devices

Security Features

- **Access Control**: Manage who can connect to your network
- **Credential Management**: Securely store device access credentials
- **User Authentication**: Control access to the SoftAC system
- **Audit Logs**: Track all configuration changes and system activities

1.3 System Architecture

Understanding how SoftAC works will help you better utilize its features:



Components Explained

1. **SoftAC Application**: The main software installed on your computer
2. **Management Interface**: The user-friendly dashboard you interact with
3. **Configuration Engine**: Processes and applies your settings to devices
4. **Database**: Stores all configurations, device information, and monitoring data
5. **Device Communication**: Handles secure communication with your network devices

How It Works

1. **Discovery**: SoftAC automatically finds TOTOLINK devices on your network
2. **Registration**: Devices are added to SoftAC with their unique identifiers
3. **Configuration**: You create or apply configurations through the interface
4. **Deployment**: Settings are securely sent to the devices

5. **Monitoring**: Devices report their status back to SoftAC continuously

1.4 Supported Devices

TOTOLINK SoftAC is compatible with a wide range of TOTOLINK network equipment:

Wireless Access Points (APs)

- **Indoor APs**: For office spaces, classrooms, and indoor venues
- **Outdoor APs**: Weather-resistant models for outdoor coverage
- **High-density APs**: For environments with many simultaneous users
- **Wall-plate APs**: Distributed in-wall mounting options

Device Requirements

For a device to be managed by SoftAC, it must satisfy:

Requirement	Description
Brand	TOTOLINK branded equipment
Firmware	Running compatible firmware version
Network Access	Reachable from the SoftAC computer
Authentication	Valid device key or credentials

> 📝 **Note**: Check the TOTOLINK website for the latest list of compatible models and firmware versions. To ensure the management on APs, firmwares of APs should be the ones published after ***1st Oct 2025***.

Scalability

SoftAC can manage networks of various sizes:

- **Small Business**: 1-10 devices
- **Medium Enterprise**: 10-50 devices
- **Large Organization**: 50+ devices

The system automatically adjusts its performance based on the number of managed devices, ensuring smooth operation regardless of network size.

> 💡 **Tip**: For optimal performance with large networks (50+ devices), we recommend running SoftAC on a dedicated computer with at least 8GB RAM.

Network Compatibility

SoftAC works with standard network configurations:

- **IPv4 Networks**: Full support for traditional IP addressing
- **VLAN Support**: Manage devices across different VLANs

- **Remote Management**: Access devices at branch offices via VPN
- **Mixed Networks**: Manage both wired and wireless devices

Getting Started

Now that you understand what TOTOLINK SoftAC can do, you're ready to proceed to the next section: **Quick Start**, where we'll guide you through installation and initial setup.

> 🚀 **Next Steps**:
>
> - Review system requirements for your computer
> - Prepare a list of devices you want to manage
> - Gather device information (MAC addresses, IP addresses)
> - Plan your network groups and organization structure

For technical support and additional resources, visit www.totolink.net

Part 2: Quick Start

Overview

This chapter will help you to get TOTOLINK SoftAC up and run it on your computer quickly and easily. We'll walk you through checking system requirements, installing the software, logging in for the first time, and completing the initial setup.

2.1 System Requirements

Before installing TOTOLINK SoftAC, please ensure your computer meets the following requirements:

Minimum System Requirements

Component	Windows	macOS	Linux
Operating System	Windows 10 or later (64-bit)	macOS 10.14 (Mojave) or later	Ubuntu 18.04+ / Debian 10+
Processor	Intel Core i3 or equivalent	Intel Core i3 or Apple Silicon (M1/M2/M3)	Intel Core i3 or equivalent
Memory (RAM)	4 GB	4 GB	4 GB
Storage Space	2 GB available	2 GB available	2 GB available
Network	Ethernet or WiFi connection	Ethernet or WiFi connection	Ethernet or WiFi connection
Display	1280×720 resolution	1280×720 resolution	1280×720 resolution

Recommended System Requirements

For the best experience, especially when managing 20 or more devices:

Component	Windows	macOS	Linux
Operating System	Windows 11 (64-bit)	macOS 12 (Monterey) or later	Ubuntu 22.04 LTS
Processor	Intel Core i5 or better	Intel Core i5 or Apple Silicon	Intel Core i5 or better
Memory (RAM)	8 GB or more	8 GB or more	8 GB or more
Storage Space	5 GB available	5 GB available	5 GB available
Network	Gigabit Ethernet	Gigabit Ethernet	Gigabit Ethernet
Display	1920×1080 resolution	1920×1080 resolution	1920×1080 resolution

> 📝 **Note**: SoftAC requires port 18580 to be available on your computer. If you have firewall software installed, you may need to allow SoftAC to pass through it.

Network Requirements

To manage your TOTOLINK devices, please ensure:

- Your computer can visit the devices on the network
- Devices are on the same network or accessible through routing
- No firewall blocks communication between SoftAC and your devices

2.2 Installation Guide

Follow the appropriate installation steps for your operating system.

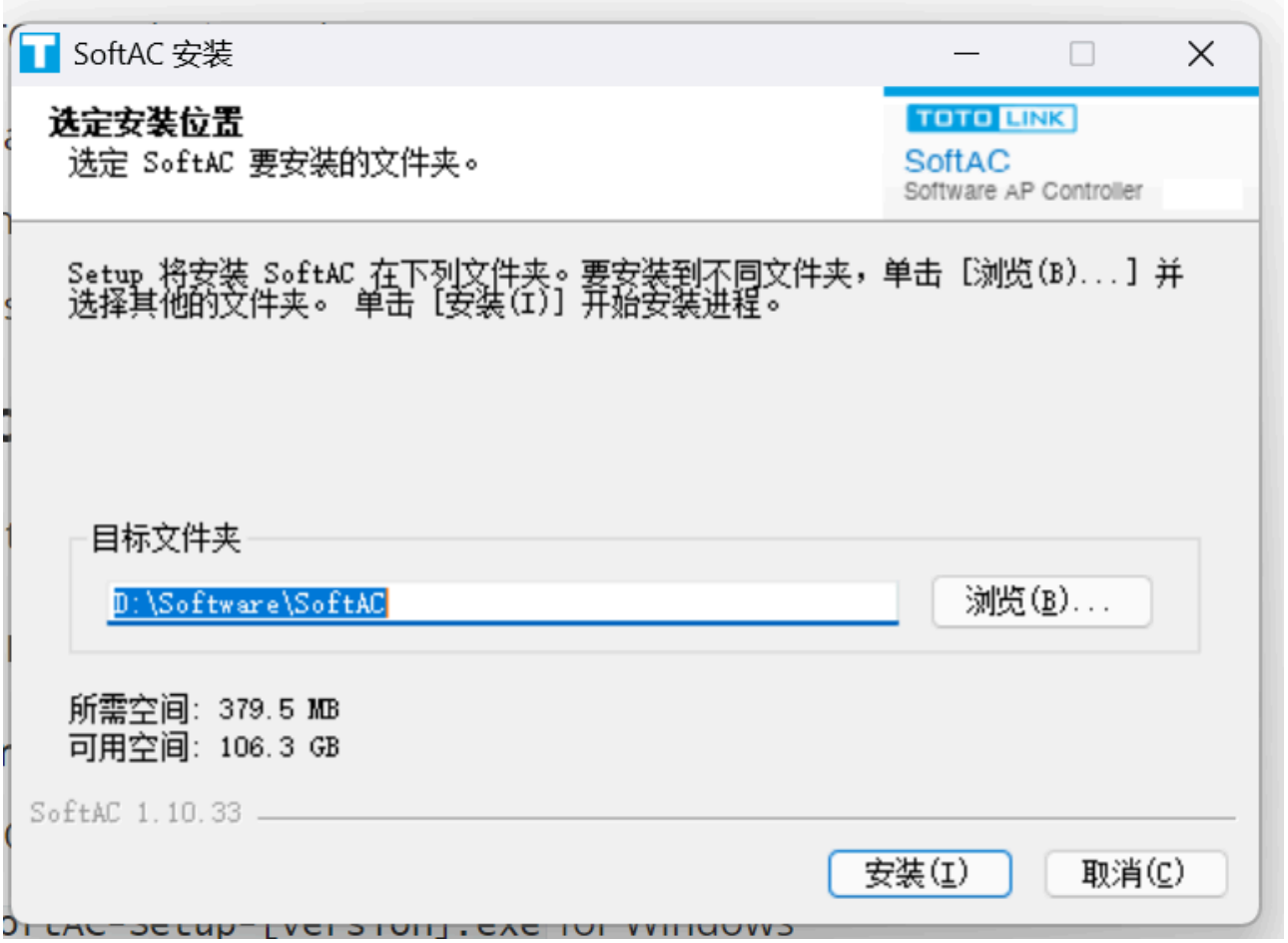
Installing on Windows

1. **Download the Installer**
   - Visit the TOTOLINK website or use the provided installation media
   - Download `SoftAC-Setup-[version].exe` for Windows

   Run the Installer
   - Locate the downloaded file in your folder
   - Double-click `SoftAC-Setup-[version].exe` to start installation
   - If Windows shows a security warning, click "Run anyway"

2. **Follow Installation Wizard**
   - Click "Next" on the welcome screen
   - Read and accept the license agreement
   - Choose installation location (default is recommended)
   - Select whether to create desktop shortcut

- Click "Install" to begin installation



3. **Complete Installation**
   - Wait for the installation to finish (usually takes 1-2 minutes)
   - Click "Finish" to complete
   - The application will launch automatically if you keep "Launch SoftAC" checked

> 💡 **Tip**: If you need to install SoftAC on multiple computers, you can use the same installer file on each one.

Installing on macOS

1. **Download the Installer**
   - Download the appropriate version for your Mac:
     - For Apple Silicon Macs (M1/M2/M3): `SoftAC-[version]-arm64.dmg`
     - For Intel Macs: `SoftAC-[version].dmg`

   [Screenshot: Download page showing both macOS versions]
2. **Open the DMG File**
   - Double-click the downloaded DMG file
   - A new window will open showing the SoftAC app and Applications folder

   [Screenshot: DMG window with SoftAC icon and Applications folder]
3. **Install the Application**
   - Drag the SoftAC icon to the Applications folder
   - Wait for the copy to complete
   - Eject the DMG by clicking the eject button in Finder

   [Screenshot: Dragging SoftAC to Applications folder]
4. **First Launch**
   - Open your Applications folder

- Right-click on SoftAC and select "Open"
- If macOS shows a security warning, click "Open" to confirm
- SoftAC will start and be available in your Dock

[Screenshot: macOS security dialog when first opening the app]

> ⚠️ **Important**: On first launch, macOS may require you to allow SoftAC in System Preferences > Security & Privacy if you see a message about an unidentified developer.

Installing on Linux

1. **Download the Package**
   - For Ubuntu/Debian: Download `softac_[version]_amd64.deb`
   - For other distributions: Download `SoftAC-[version].AppImage`

   [Screenshot: Linux download options]
2. **Install Using Package Manager (Ubuntu/Debian)**

   ```
   sudo dpkg -i softac_[version]_amd64.deb
   sudo apt-get install -f  # Install any missing dependencies
   ```

   Or double-click the .deb file to open in Software Center
3. **Using AppImage (Universal)**
   - Make the AppImage executable:

     ```
     chmod +x SoftAC-[version].AppImage
     ```

   - Double-click to run, or execute from terminal:

     ```
     ./SoftAC-[version].AppImage
     ```
4. **Launch the Application**
   - Find SoftAC in your application menu
   - Or launch from terminal: `softac`

   [Screenshot: SoftAC in Ubuntu application menu]

2.3 First Login

When you launch TOTOLINK SoftAC for the first time, you'll see the login screen.

Understanding the Login Screen

[Screenshot: SoftAC login screen with all elements visible]

The login screen contains:

- **TOTOLINK Logo**: Company brand at the top
- **Username Field**: Where you enter your username

- **Password Field**: Where you enter your password
- **Remember Me Checkbox**: Check this to save your username for next time
- **Login Button**: Click to log into the system
- **Forgot Password Link**: Use if you need to reset your password

Default Credentials

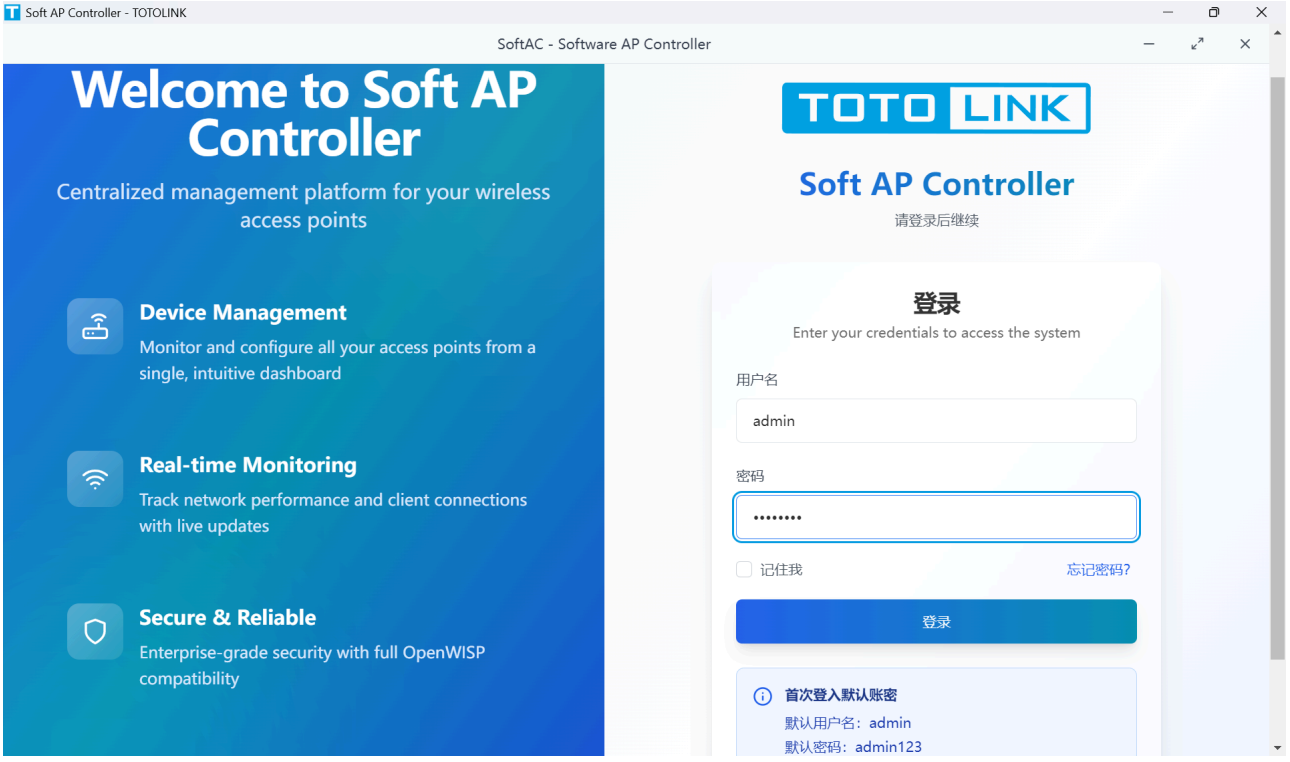
For first-time login, use these default credentials:

Field	Value
Username	admin
Password	admin123

> 🔴 **Important**: You will be required to change the default password immediately after your first login for security reasons.

Login Steps

1. **Enter Username**
   - Click in the username field
   - Type: `admin`
2. **Enter Password**
   - Click in the password field
   - Type: `admin123`
   - The password will appear as dots for security



3. **Optional: Remember Username**

- Check "Remember me" if you want the system to remember your username
- This saves time on future logins
- Only use this on your personal computer

4. **Click Login**
    - Click the blue "Login" button
    - Or press Enter on your keyboard

    [Screenshot: Clicking the Login button]

Troubleshooting Login Issues

If you cannot log in:

Problem: "Invalid credentials" error

- Check if Caps Lock is on (passwords are case-sensitive)
- Ensure you typed "admin" correctly for both username and password
- Try typing the password again slowly

[Screenshot: Login error message showing invalid credentials]

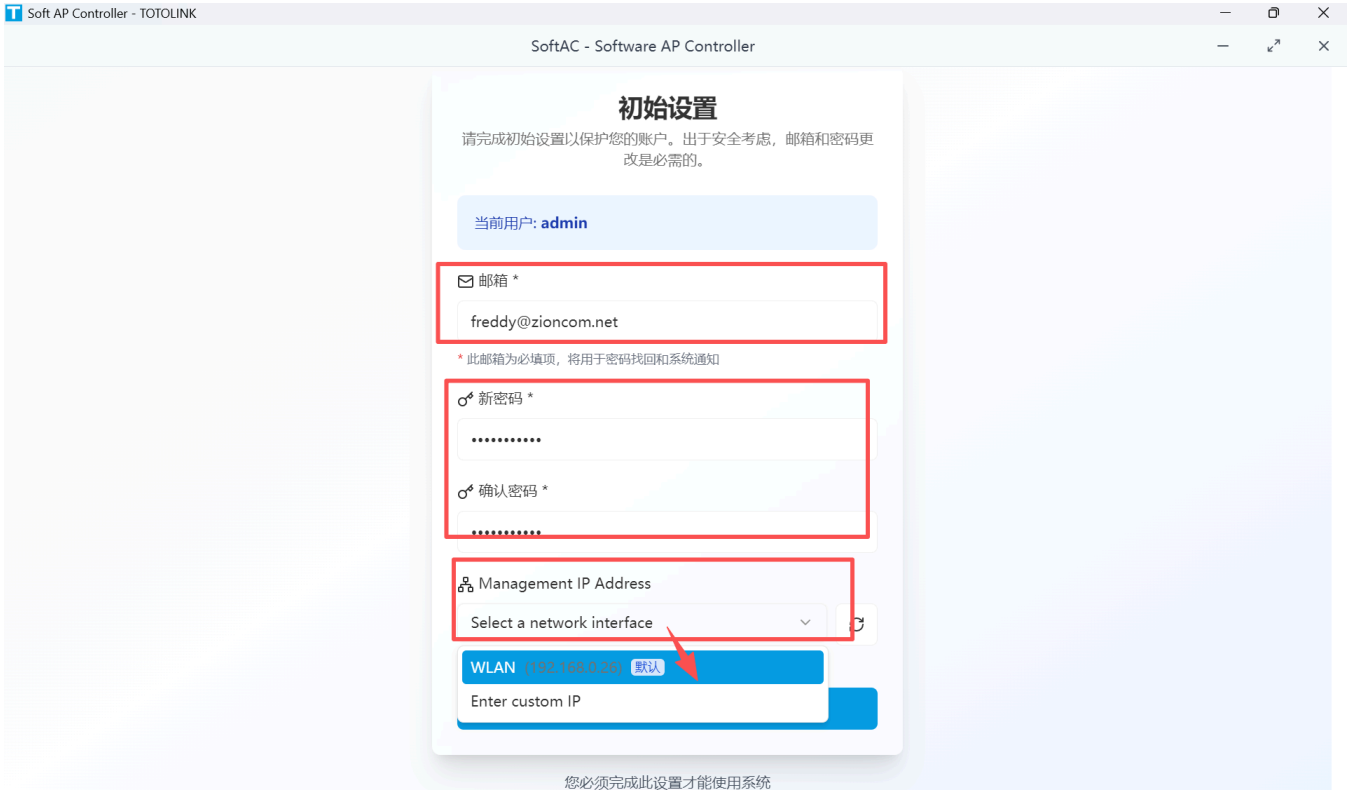
Problem: "Cannot connect to server" error

- Wait a moment for the backend service to start (especially after installation)
- Check if any antivirus software is blocking SoftAC
- Restart the SoftAC application

> 💡 **Tip**: If you see a yellow warning about Caps Lock being on, turn it off before typing your password.

2.4 Initial Setup Wizard

After your first successful login with default credentials, you'll be automatically directed to the Initial Setup Wizard. This wizard helps you to secure your system and configure basic settings.



Step 1: Security Configuration

The first and most important step is setting up your administrator account security.

Change Administrator Password

1. **Current User Display**
   - Shows you've logged in as "admin"
   - This confirms you've set up the main administrator account
2. **Enter Email Address**
   - Type your email address in the "Email" field
   - This email will be used for:
     - Password recovery if you forget your password
     - System notifications (if configured)
     - Security alerts

   Example: `john.smith@company.com`
3. **Create New Password**
   - Enter a strong password in the "New Password" field
   - Password requirements:
     - Minimum 6 characters
     - Mix of letters and numbers recommended
     - Case-sensitive (capitals and lowercase matter)
4. **Confirm Password**
   - Re-type the same password in "Confirm Password" field

- Must match exactly with the new password
- If they don't match, you'll see an error message

> 🔒 **Security Tips for Strong Passwords**:
>
> - Use at least 8 characters
> - Include uppercase and lowercase letters
> - Add numbers and special characters
> - Avoid common words or personal information
> - Consider using a passphrase like "Coffee@Morning2024!"

Step 2: Network Configuration (Optional)

Configure how SoftAC communicates with your network devices.

Management IP Address

The Management IP is the network address which SoftAC uses to communicate with your devices.

1. **Automatic Selection (Recommended)**
   - SoftAC automatically detects your network interfaces
   - Select from the dropdown list of available network adapters
   - The system will show the IP address for each adapter
2. **Manual Configuration (Advanced)**
   - Select "Custom IP" from the dropdown
   - Enter your preferred IP address
   - Format: XXX.XXX.XXX.XXX (e.g., 192.168.1.100)

> 📝 **Note**: Most users should use the automatic selection. Only choose custom IP if you have specific network requirements or multiple network interfaces.

When to Use Custom IP:

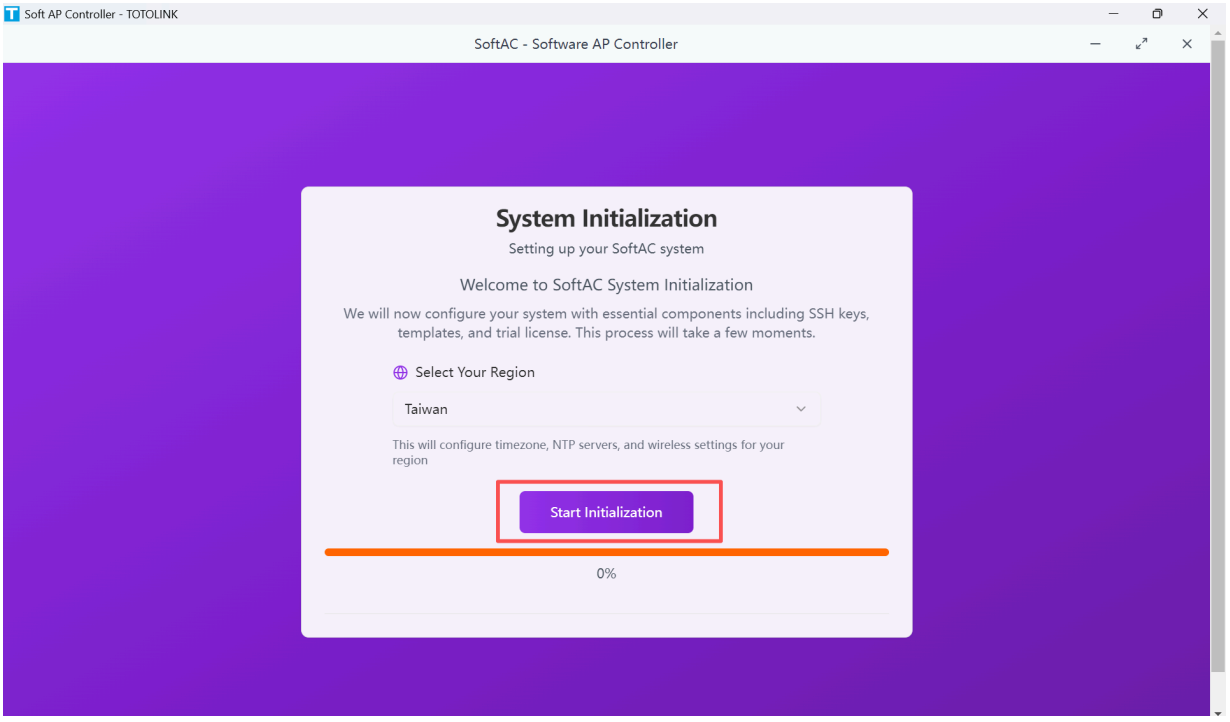
- Your computer has multiple network cards
- You want to manage devices on a specific network segment
- Your IT department requires a specific management IP

Step 3: Review and Complete

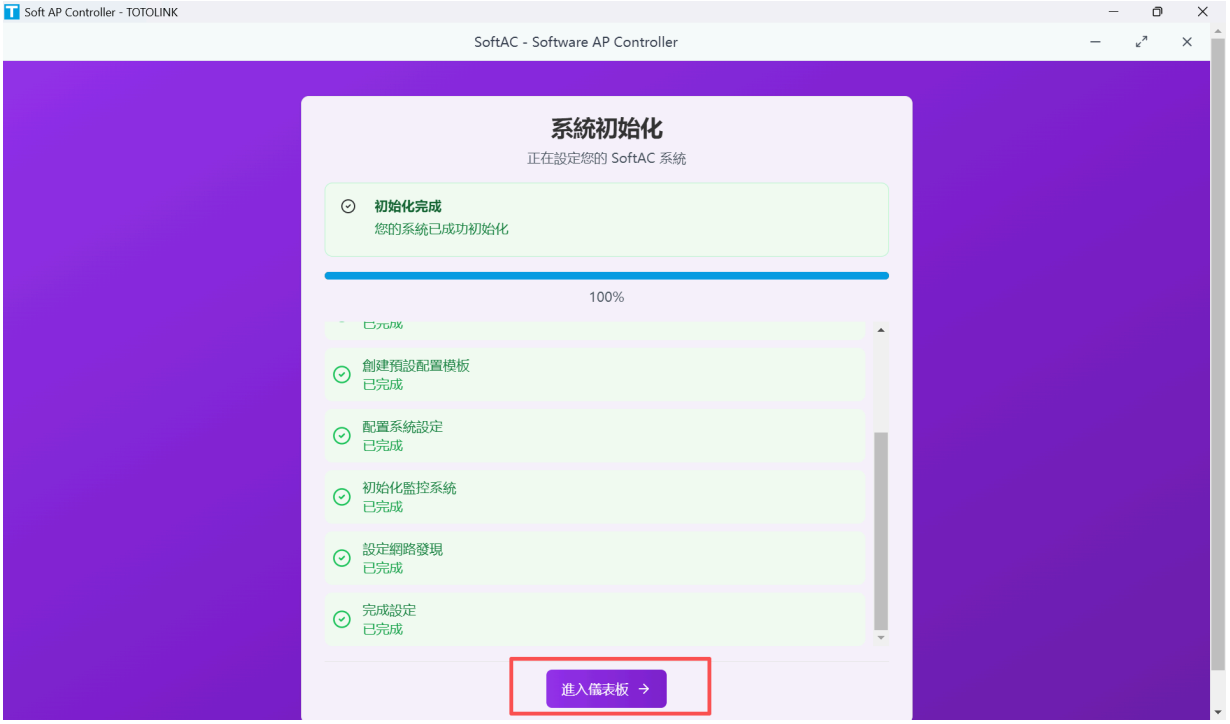
Before finalizing the setup:

1. **Review Your Settings**
   - Email address is correct and accessible
   - Password has been set (shown as dots)
   - Network configuration is appropriate
2. **Complete Setup**
   - Click the "Complete Setup" button

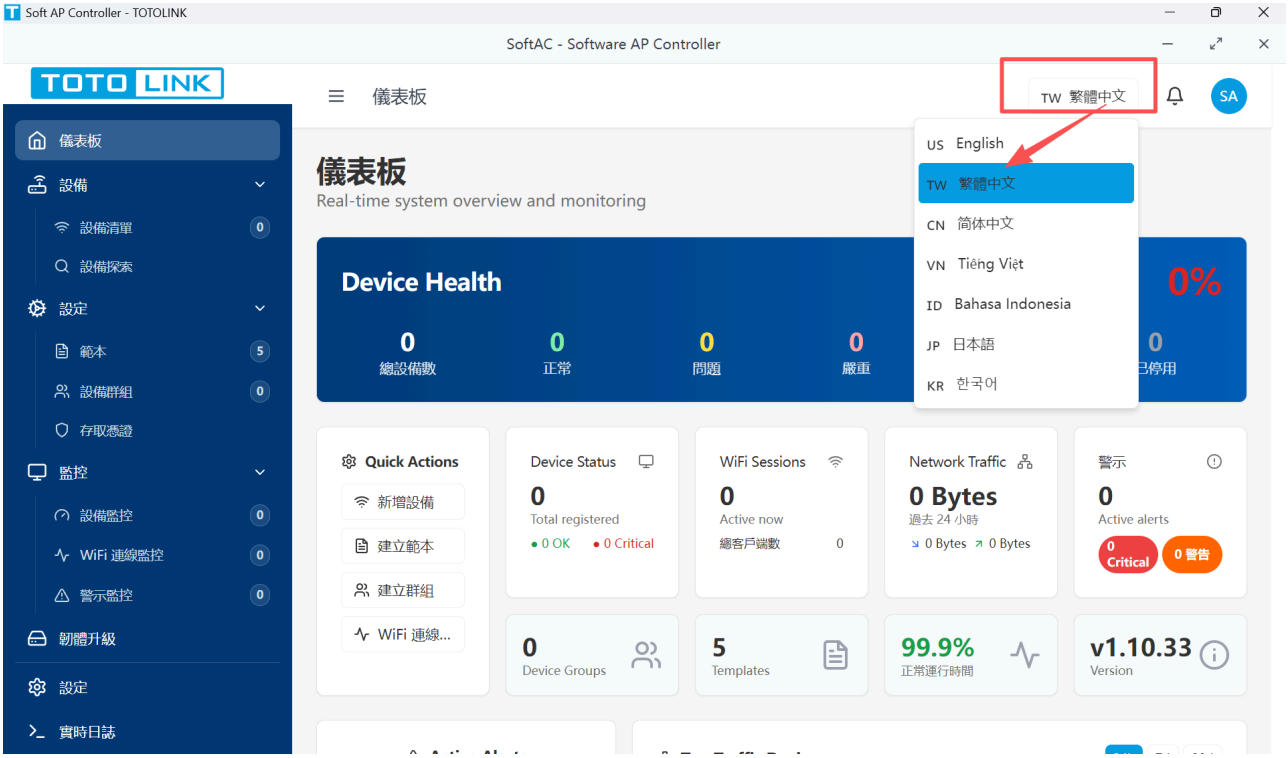
- You'll see the initialization page
- Click "Start Initialization"



- After successfully initializing the system, click "Enter Dashboard"



- The system will automatically redirect to the main dashboard, click the language option at the upper right corner to change the system language (currently, the initial language option is traditional Chinese, TW)



3. **What Will Happen Next**
    - Your new password is now active
    - Default "admin" password no longer works
    - System is ready for device management
    - You can now add your first device

Post-Setup Checklist

After completing initial setup, you're ready to start using SoftAC:

- [x] Administrator password changed from default
- [x] Recovery email configured
- [x] Network settings configured
- [ ] Ready to add first device
- [ ] Ready to create device groups
- [ ] Ready to configure templates

[Screenshot: Main dashboard after successful setup]

Important Security Reminders

> ⚠️ **Security Best Practices**:
>
> - Never share your administrator password
> - Change your password regularly (every 90 days recommended)
> - Use different passwords for SoftAC and your devices
> - Log out when finished, especially on shared computers
> - Keep your recovery email up to date

Getting Help

If you encounter issues during initial setup:

1. **Email Not Accepted**
   - Ensure email format is correct (name@domain.com)
   - Check for typos or extra spaces
2. **Password Not Accepted**
   - Ensure minimum 6 characters
   - Check that passwords match exactly
   - Remember passwords are case-sensitive
3. **Network Configuration Issues**
   - Try using automatic detection first
   - Consult your IT department for correct IP settings
   - Ensure your network adapter is active

> 💡 **Tip**: Write down your new password in a secure location until you're sure you've memorized it. Consider using a password manager for better security.

Next Steps

Congratulations! You've successfully installed and configured TOTOLINK SoftAC. You're now ready to:

1. **Add Your First Device** (Section 4.1)
   - Learn how to add TOTOLINK devices to your management system
2. **Explore the Dashboard** (Section 3)
   - Understand the main interface and navigation
3. **Create Device Groups** (Section 6)
   - Organize your devices for easier management
4. **Set Up Templates** (Section 5)
   - Create configuration templates for quick deployment

> 📚 **Quick Reference Card**
>
> **Default Login**: admin / admin123
> **Default Port**: 18580
> **Data Location Windows**: %APPDATA%\SoftAC
> **Data Location macOS**: ~/Library/Application Support/SoftAC
> **Data Location Linux**: ~/.config/SoftAC
> **Support Email**: support@totolink.net
> **Support Website**: https://www.totolink.net

Part 3: Dashboard

3.1 System Overview

Overview

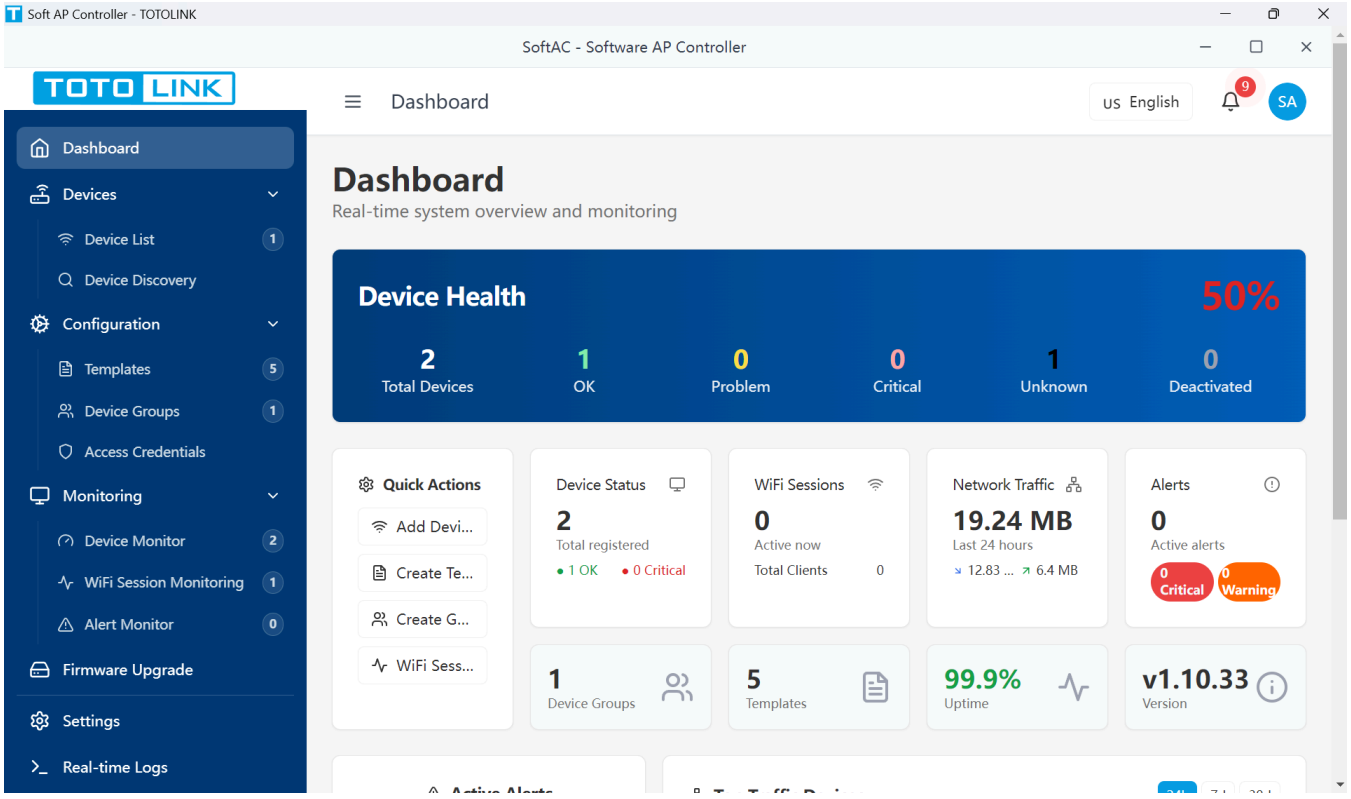
The Dashboard is your central command center for monitoring and managing your TOTOLINK SoftAC network. It provides real-time insights into device health, network performance, and system status at a glance.

Purpose

- Monitor overall network health instantly
- Identify issues before they impact users
- Access frequently used functions quickly
- Track network usage and performance trends

When to Use

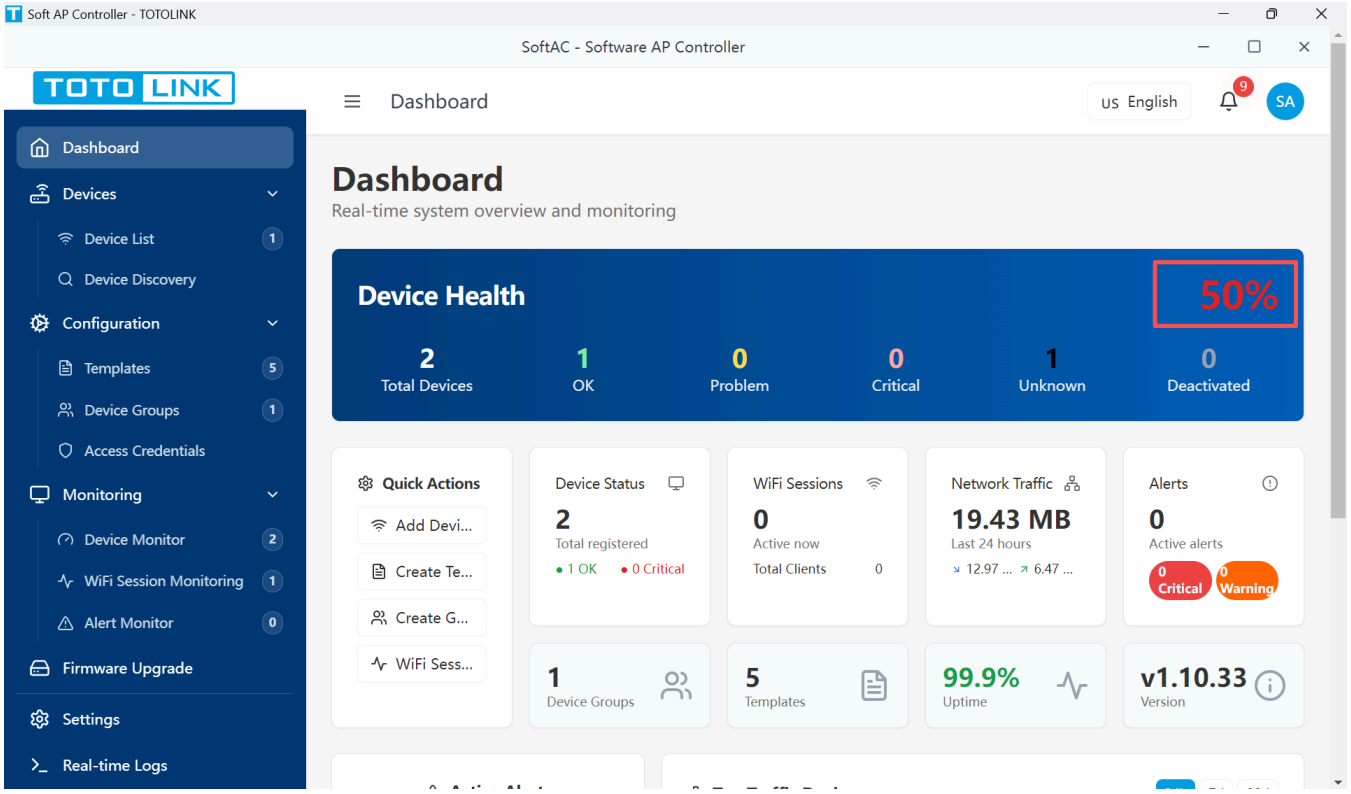
- **Daily monitoring**: Start your day by checking system health
- **Troubleshooting**: Quickly identify problem areas in your network
- **Performance review**: Monitor traffic patterns and usage trends
- **Alert management**: Respond to system notifications promptly



3.2 Real-time Monitoring Data

Device Health Score

The prominent health score at the top of the dashboard shows your network's overall health as a percentage.



Understanding the Health Score:

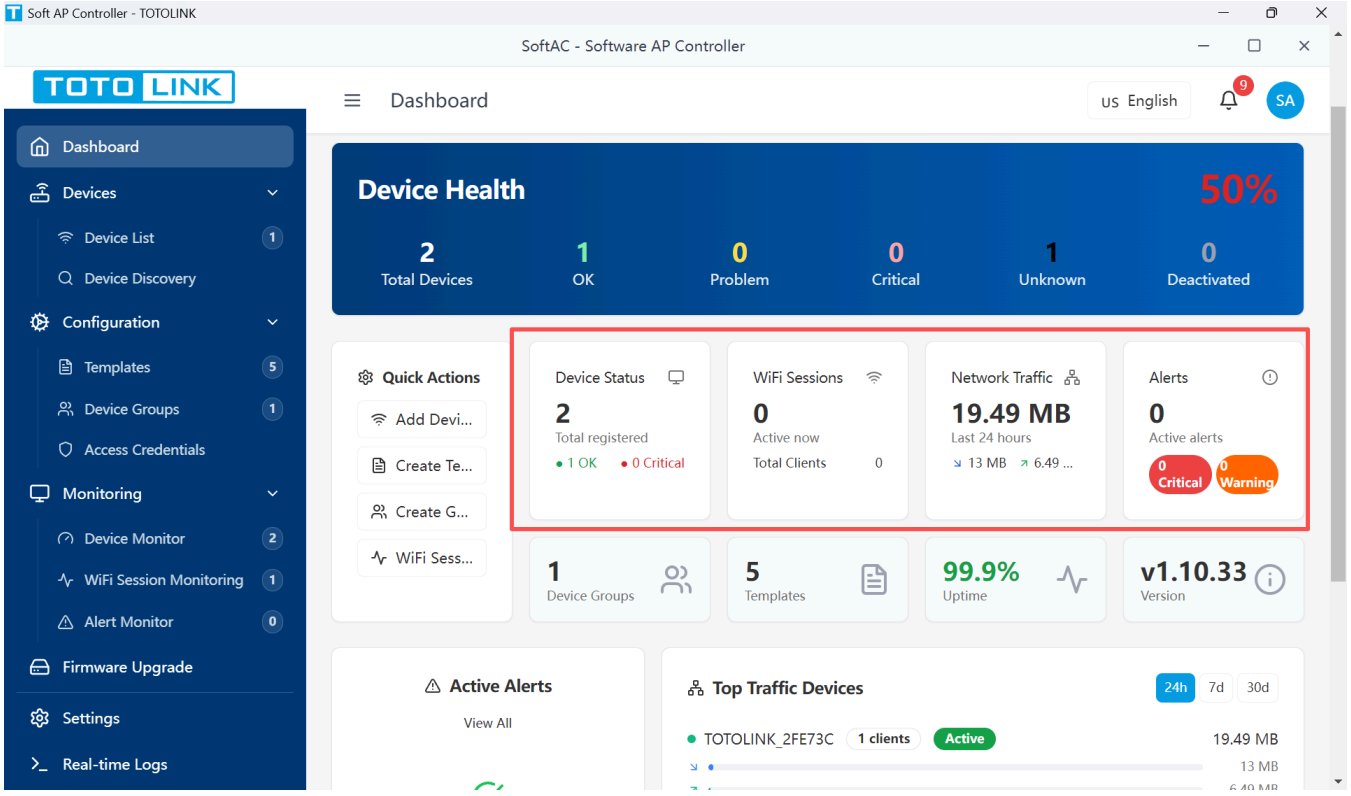
- **80-100%**: Excellent - System running optimally (Green)
- **60-79%**: Good - Minor issues present (Yellow)
- **Below 60%**: Attention needed - Multiple issues detected (Red)

The health card displays device status breakdown:

Status	Meaning	Action Required
OK	Device functioning normally	None
Problem	Minor issues detected	Monitor closely
Critical	Serious issues present	Immediate attention
Unknown	Connection lost	Check device connectivity
Deactivated	Device intentionally offline	None

Key Performance Indicators

The dashboard displays four main metric cards:



1. Device Status Card

Shows total registered devices and their current operational states.

- **Total count**: All devices in your network
- **OK devices**: Devices operating normally (green indicator)
- **Critical devices**: Devices requiring immediate attention (red indicator)

2. WiFi Sessions Card

Displays active wireless connections in real-time.

- **Active sessions**: Current connected users
- **Total clients**: All registered WiFi devices

> 💡 **Tip**: Click the session count to view detailed session information

3. Network Traffic Card

Shows cumulative data transfer in selected time period.

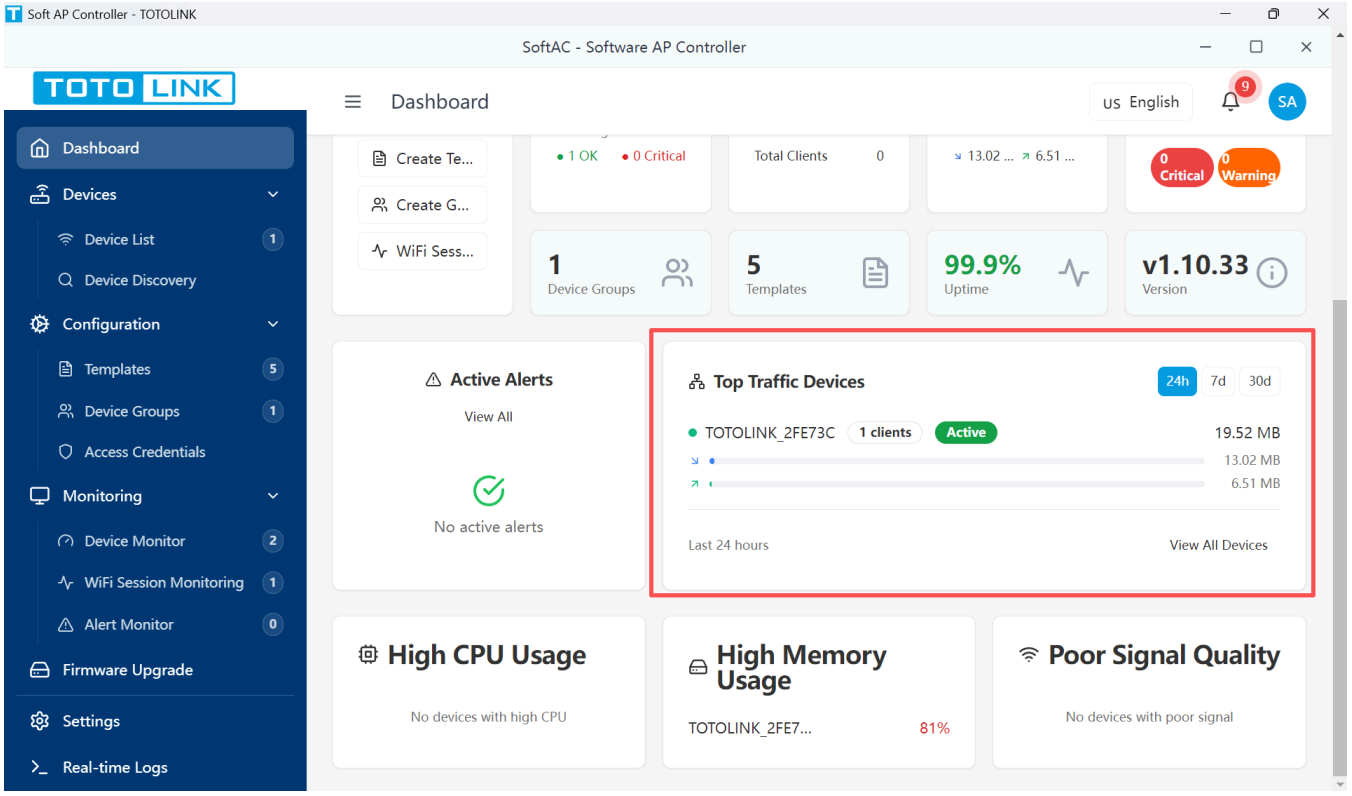
- **Total traffic**: Combined upload and download
- **Download volume**: Data received (blue arrow)
- **Upload volume**: Data sent (green arrow)
- **Time ranges**: 24 hours, 7 days, or 30 days

4. Alerts Card

Summarizes active system notifications.

- **Active count**: Unresolved issues requiring attention
- **Critical alerts**: High-priority issues (red badge)
- **Warnings**: Lower-priority notifications (grey badge)

Top Traffic Devices



This section identifies your highest bandwidth consumers:

Device Information Displayed:

- Device name and health status (colored indicator)
- Number of connected clients
- Activity status (Active/Inactive badge)
- Download/Upload traffic with visual progress bars
- Total traffic volume

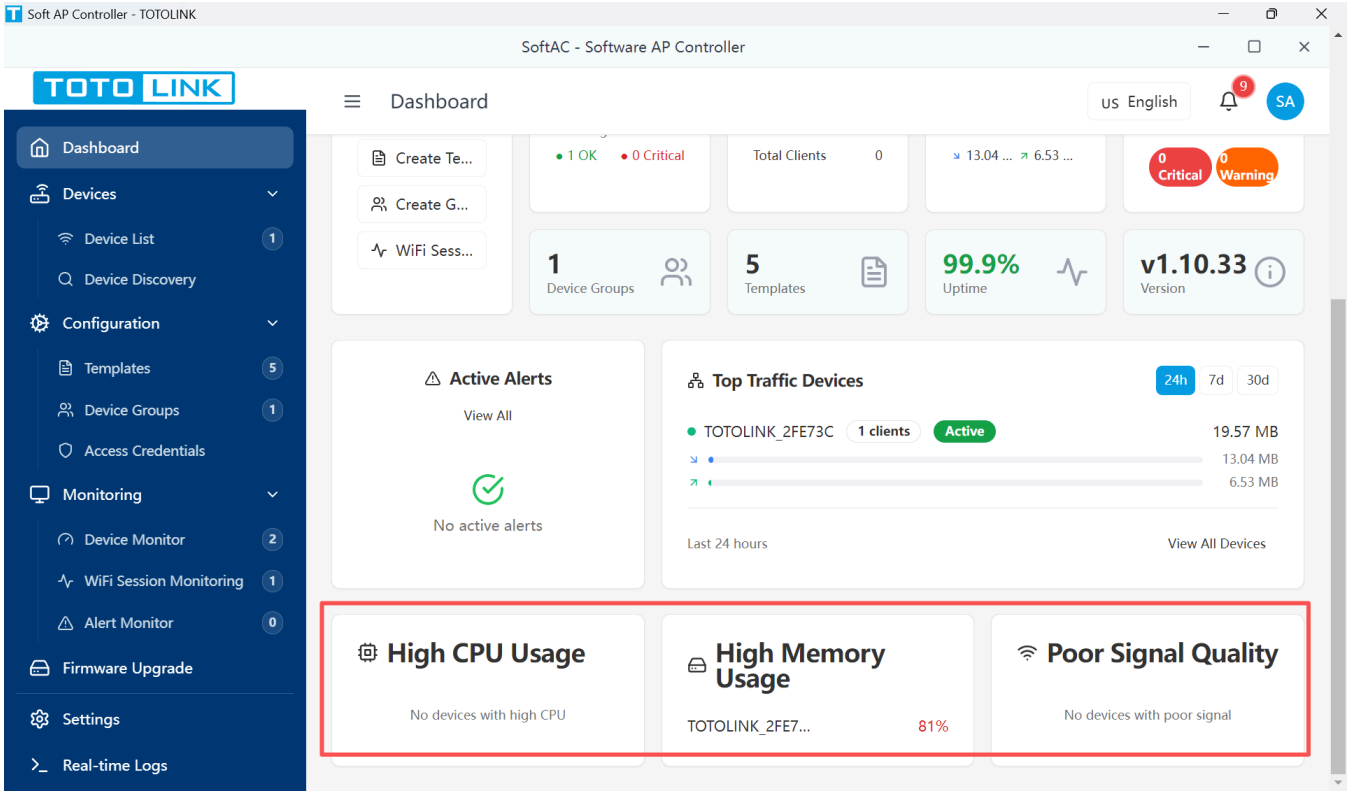
Time Range Selection:
Click the time buttons (24h, 7d, 30d) to adjust the monitoring period.

Traffic Visualization:

- Blue bar: Download traffic
- Green bar: Upload traffic
- Bar length represents relative usage

> ⚠️ **Important**: Devices marked "High Usage" may be experiencing performance issues

Performance Monitoring



Three cards monitor critical device performance:

High CPU Usage

Lists devices with CPU usage above 70%

- Device name
- Current CPU percentage
- Trend indicator (↑ increasing, ↓ decreasing)

High Memory Usage

Shows devices with memory usage above 70%

- Device name
- Memory usage percentage
- Usage trend

Poor Signal Quality

Identifies devices with weak wireless signals

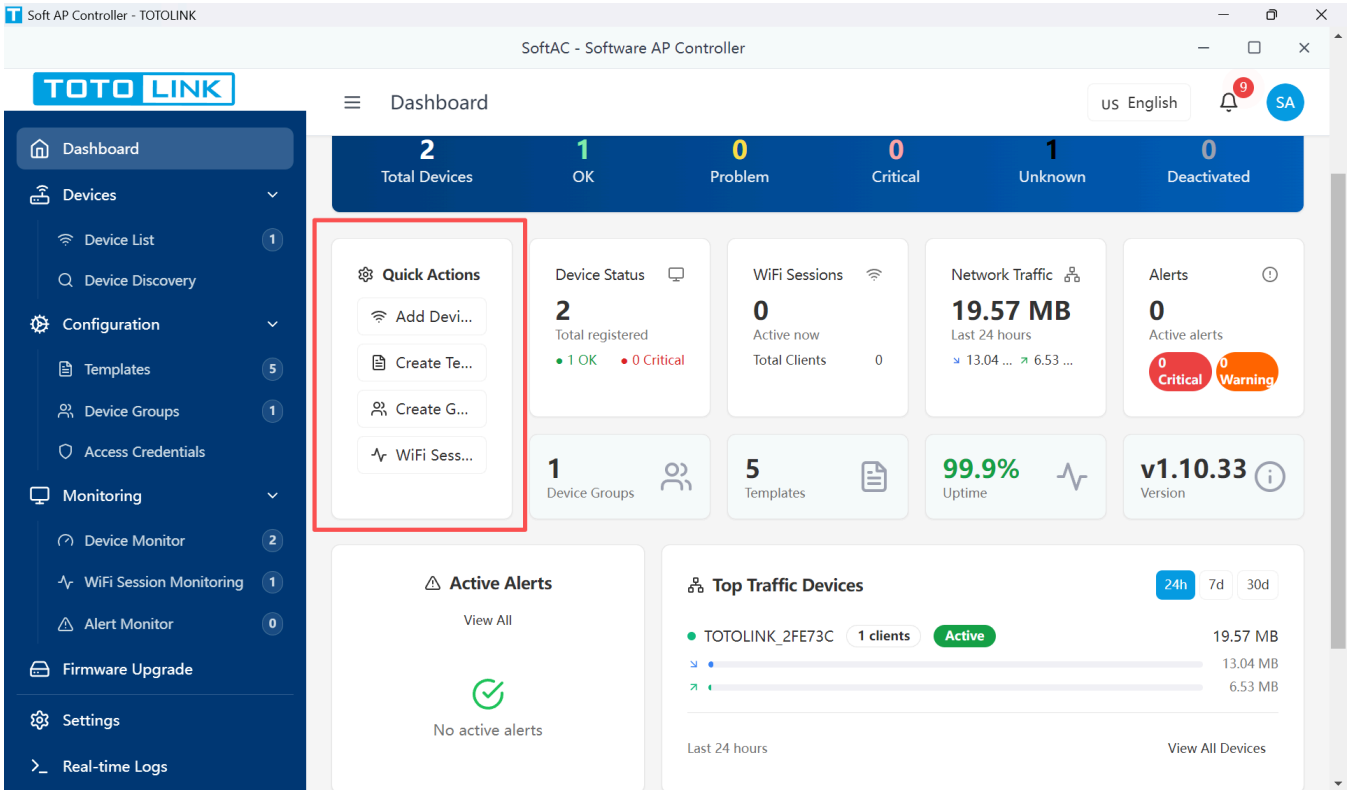
- Device name
- Signal strength in dBm
- Quality rating (Poor/Fair)

> 📝 **Note**: Signal strength below -70 dBm indicates poor connectivity

---

3.3 Quick Operation Entries

Quick Actions Panel



The Quick Actions panel provides one-click access to common tasks:

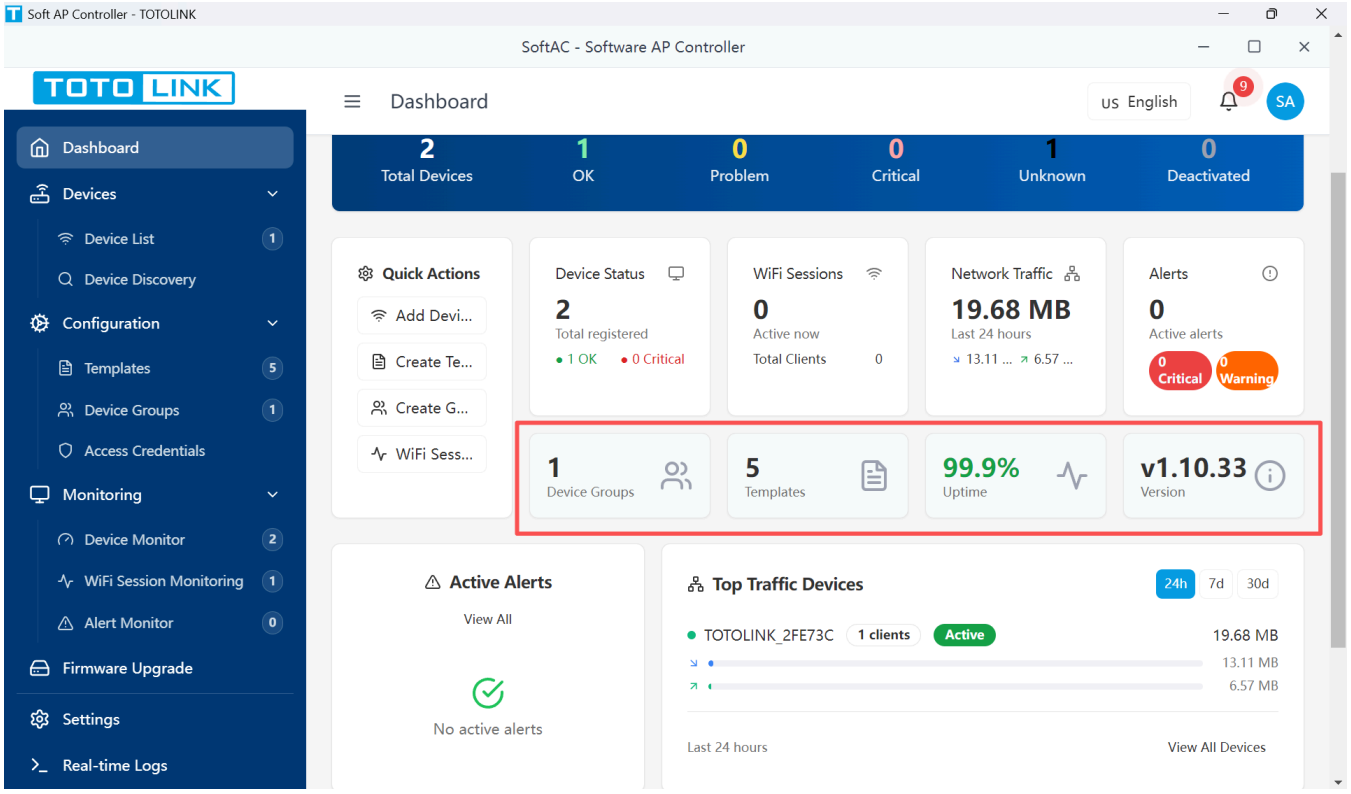
Button	Function	When to Use
Add Device	Open new device registration	Adding new access points
Create Template	Open template creation	Standardizing configurations
Create Group	Open group creation	Organizing devices
WiFi Sessions	Open session monitor	Viewing connected users

Using Quick Actions

1. **Locate the Quick Actions panel**
   Found in the upper-left section of the dashboard
2. **Click desired action**
   Each button opens the corresponding function directly
3. **Complete the operation**
   Follow the guided forms to complete your task

> 💡 **Best Practice**: Use Quick Actions for routine tasks to save navigation time

System Information Cards

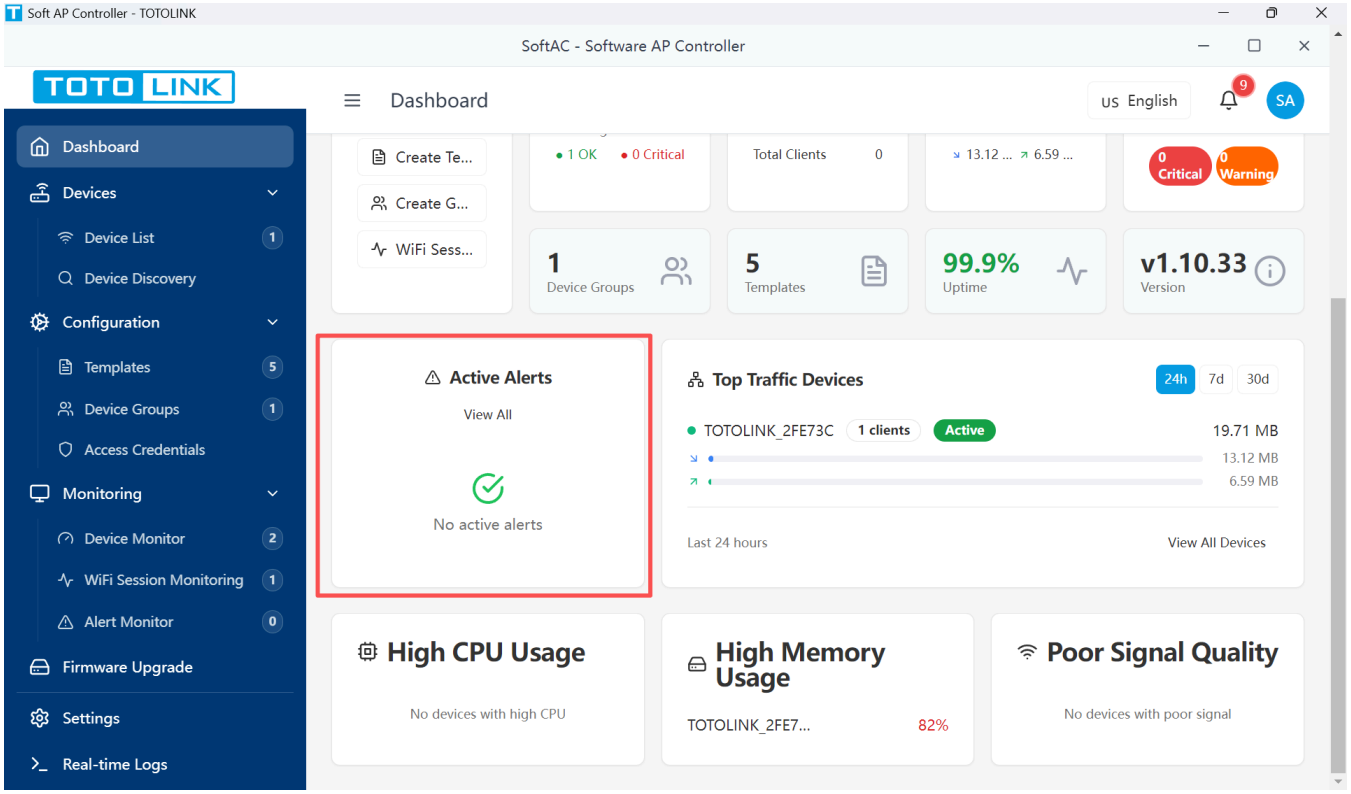


Additional system metrics display below the main indicators:

- **Device Groups**: Total number of configured groups
- **Templates**: Available configuration templates
- **Uptime**: System availability percentage
- **Version**: Current SoftAC software version

3.4 Alert Notifications

Active Alerts Panel



The Active Alerts panel displays current system notifications requiring attention.

Understanding Alert Types

Alert Indicators (in alert monitoring menu):

- 🔔 **Red bell**: Critical alerts requiring immediate action
- ⚠️ **Yellow triangle**: Warnings requiring monitoring

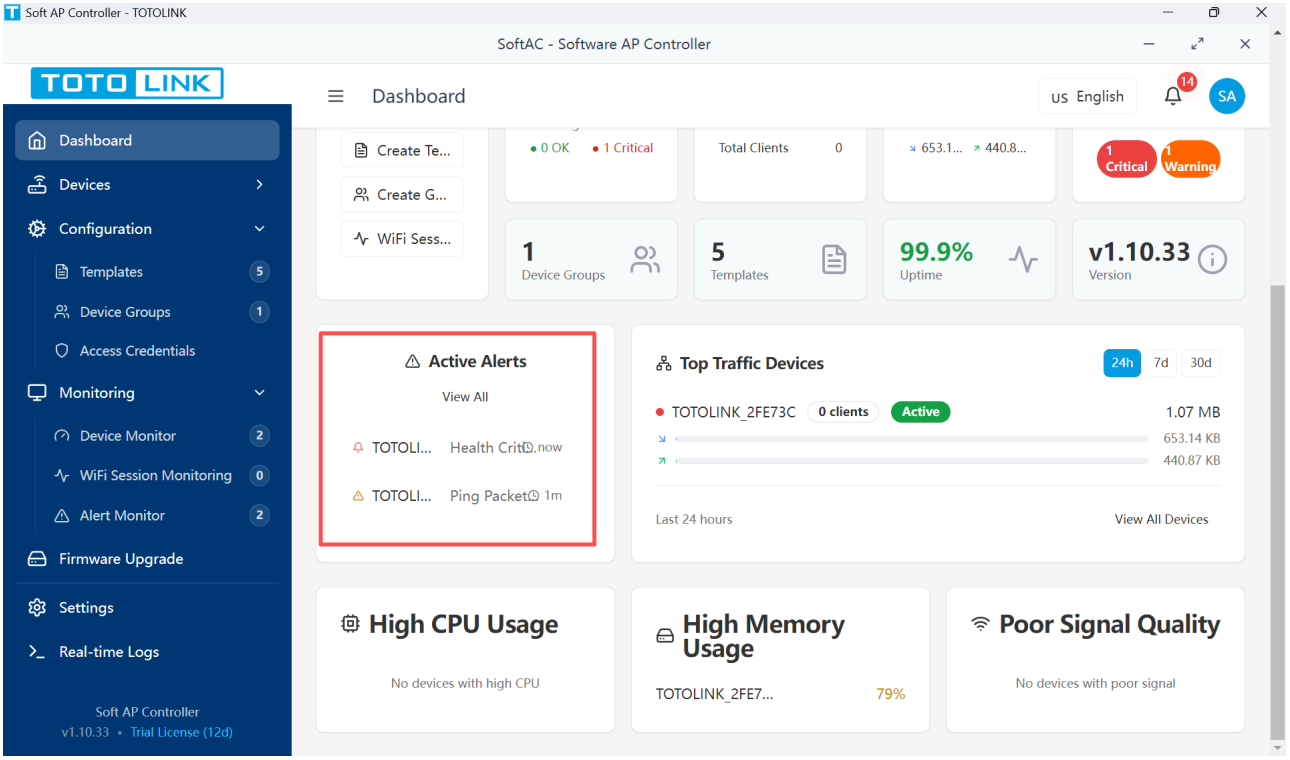
Alert Information:
Each alert displays:

- Device name affected
- Issue description
- Time elapsed since detection
- Clear button (X) for resolution

Managing Alerts

Viewing Alert Details

1. **Review the alert list**
   Alerts appear in chronological order

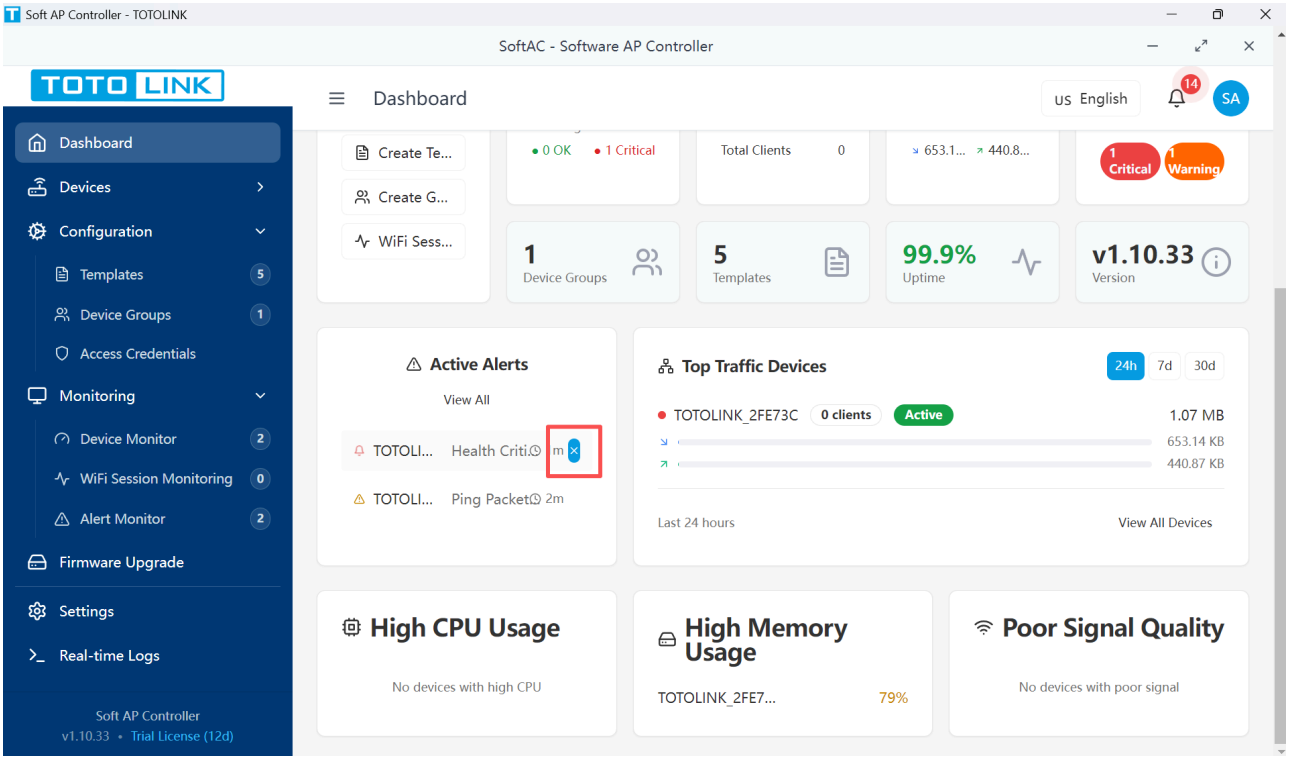


2. **Check alert severity**
   Icon color indicates priority level
3. **Note the time indicator**
   Shows how long the issue has persisted
   - "now": Just occurred
   - "5m": 5 minutes ago
   - "2h": 2 hours ago
   - "1d": 1 day ago

Clearing Alerts

1. **Hover over an alert**
   The clear button (X) appears on the right

2. **Click the X button**



3. **Confirm the action**
   Alert moves to resolved status

> ⚠️ **Warning**: Only clear alerts after verifying the issue is resolved

Viewing All Alerts

Click "View All" button to access the complete alerts page for:

- Historical alert data
- Detailed alert information
- Bulk alert management
- Alert filtering options

Best Practices in Response to Alerts

Priority Guidelines:

Alert Type	Response Time	Action
Critical (Red)	Immediate	Investigate and resolve promptly
Warning (Yellow)	Within 1 hour	Monitor and plan resolution
Info (Gray)	As convenient	Review during routine checks

Common Alert Scenarios

Device Offline:

- Check physical device power and connections
- Verify network connectivity
- Review device configuration

High Resource Usage:

- Check for unusual traffic patterns
- Review connected client count
- Consider load balancing

Poor Signal Quality:

- Check for physical obstructions
- Review device placement
- Consider signal strength adjustments

> 💡 **Tip**: Set up email notifications for critical alerts in System Settings

---

Navigation Tips

Dashboard Refresh

The dashboard automatically updates every 10 seconds. Look for the subtle data refresh in the metrics.

Drilling Down

Click on any metric card to navigate to detailed views:

- Device Status → Device Management page
- WiFi Sessions → WiFi Monitor page
- Alerts → Alert Management page

Customizing Time Ranges

Where available, use time range selectors to adjust the data period:

- 24h: Daily overview
- 7d: Weekly trends
- 30d: Monthly analysis

Troubleshooting Dashboard Issues

Dashboard Not Loading

If the dashboard fails to load:

1. **Check your connection**
   Ensure you're connected to the network
2. **Refresh the page**
   Press F5 or click the browser refresh button
3. **Clear browser cache**
   Clear cached data and reload
4. **Verify login status**
   Ensure your session hasn't expired

Missing or Incorrect Data

If metrics appear incorrect:

1. **Wait for auto-refresh**
   Data updates every 10 seconds
2. **Check device connectivity**
   Ensure all devices are properly connected
3. **Verify time settings**
   Confirm system time is correctly set

> 📝 **Note**: Contact support if dashboard issues persist

Related Features

- 4.1 Device Management - Manage individual devices
- 7.1 Device Monitoring - Detailed performance metrics
- 7.3 Alert Management - Comprehensive alert handling
- 11.1 System Settings - Configure dashboard preferences

Summary

The Dashboard provides essential real-time monitoring for your TOTOLINK SoftAC network. Regular dashboard monitoring helps maintain optimal network performance and enables proactive issue resolution. Use the Quick Actions for efficient task execution and respond promptly to alerts to ensure network reliability.

Remember to:

- Check the dashboard daily for system health
- Respond to critical alerts immediately
- Use quick actions for routine tasks

- Monitor traffic patterns for capacity planning

> 🚀 **Quick Start**: Begin each day by reviewing the health score and active alerts to ensure your network runs smoothly

Part 4. Device Management

Overview

Device Management is the core functionality of TOTOLINK SoftAC that enables you to centrally manage all your wireless access points and network devices. This module provides comprehensive tools for adding, configuring, monitoring, and maintaining your network devices from a single interface.

4.1 Adding Devices

Function Overview

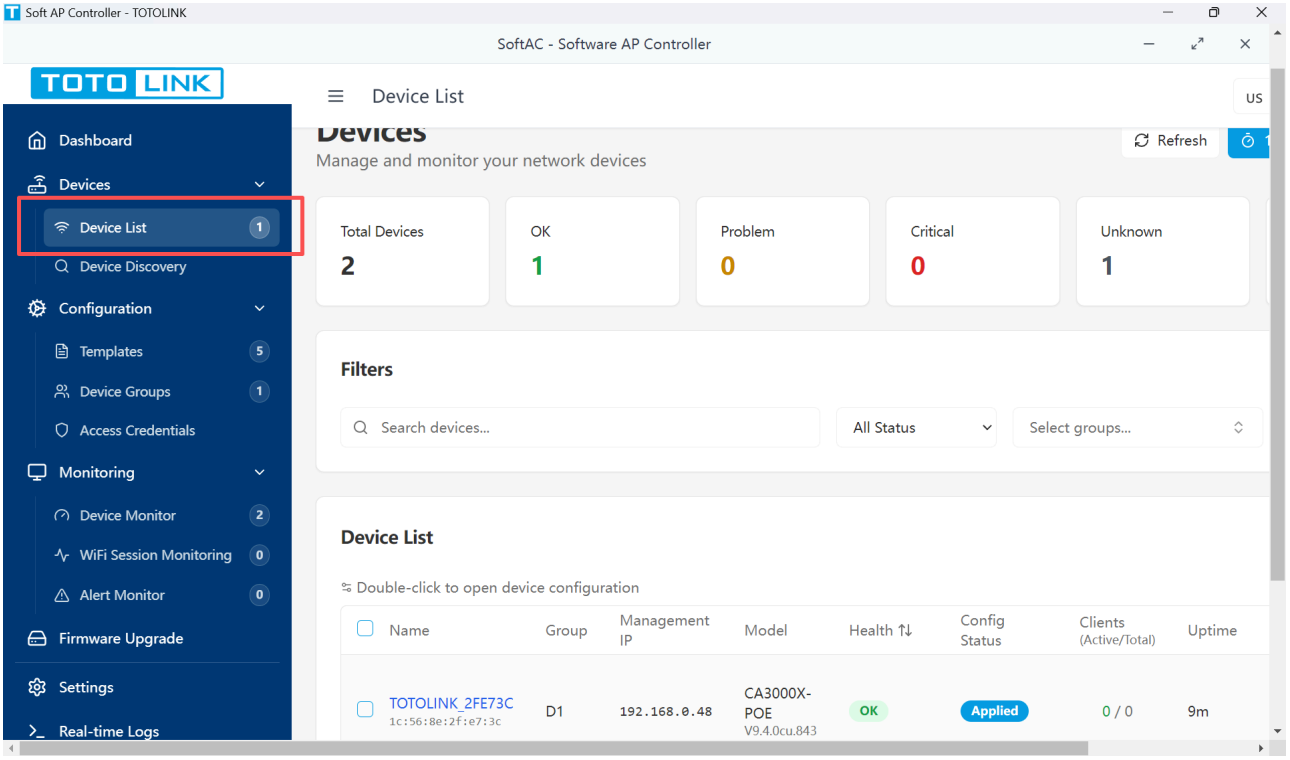
The Add Device feature allows you to register new TOTOLINK wireless access points and network devices into the SoftAC management system. Each device is uniquely identified by its MAC address and authenticated using a secure key.

Use Cases

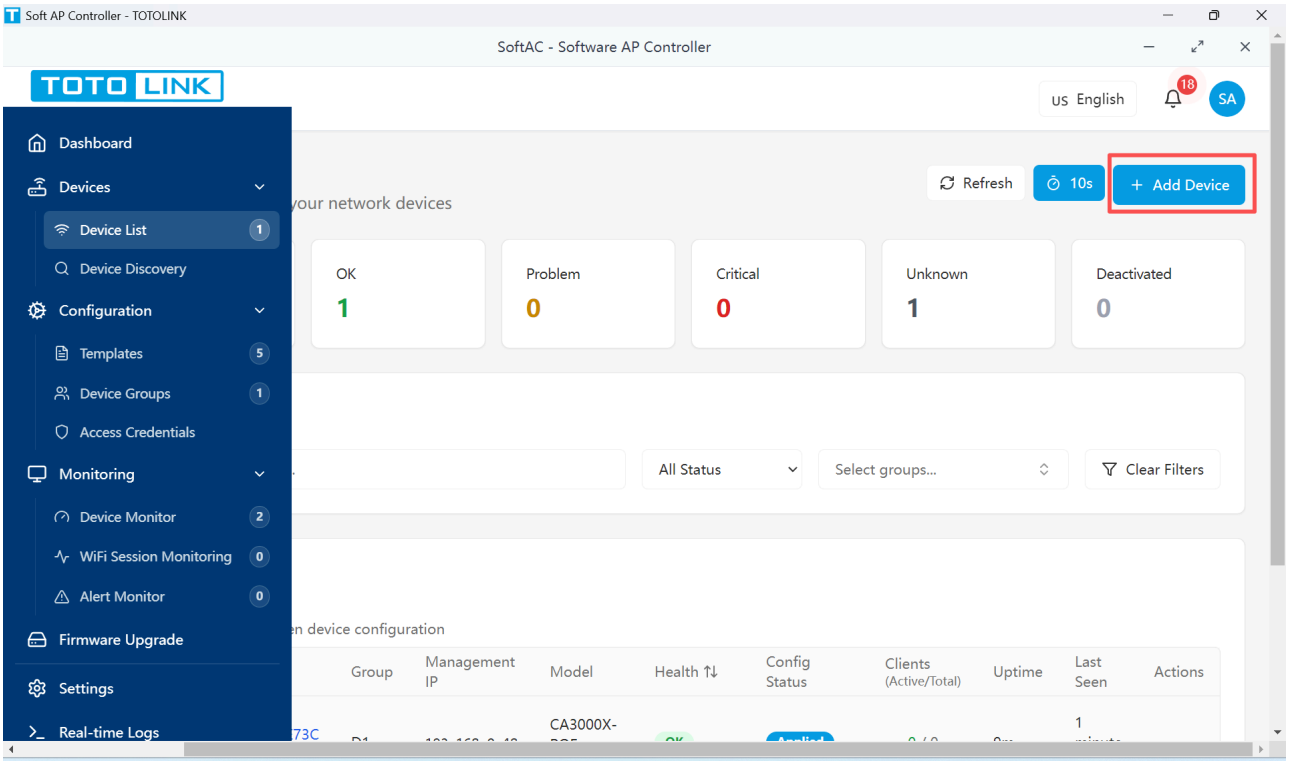
- **Initial Deployment**: Setting up new access points during network installation
- **Network Expansion**: Adding additional devices to extend wireless coverage
- **Device Replacement**: Registering replacement devices when upgrading hardware

Operating Steps

1. **Navigate to Device List**
   Click "Device List" in the left sidebar navigation menu.



2. **Open Add Device Dialog**
   Click the blue "+ Add Device" button in the top right corner of the device list page.

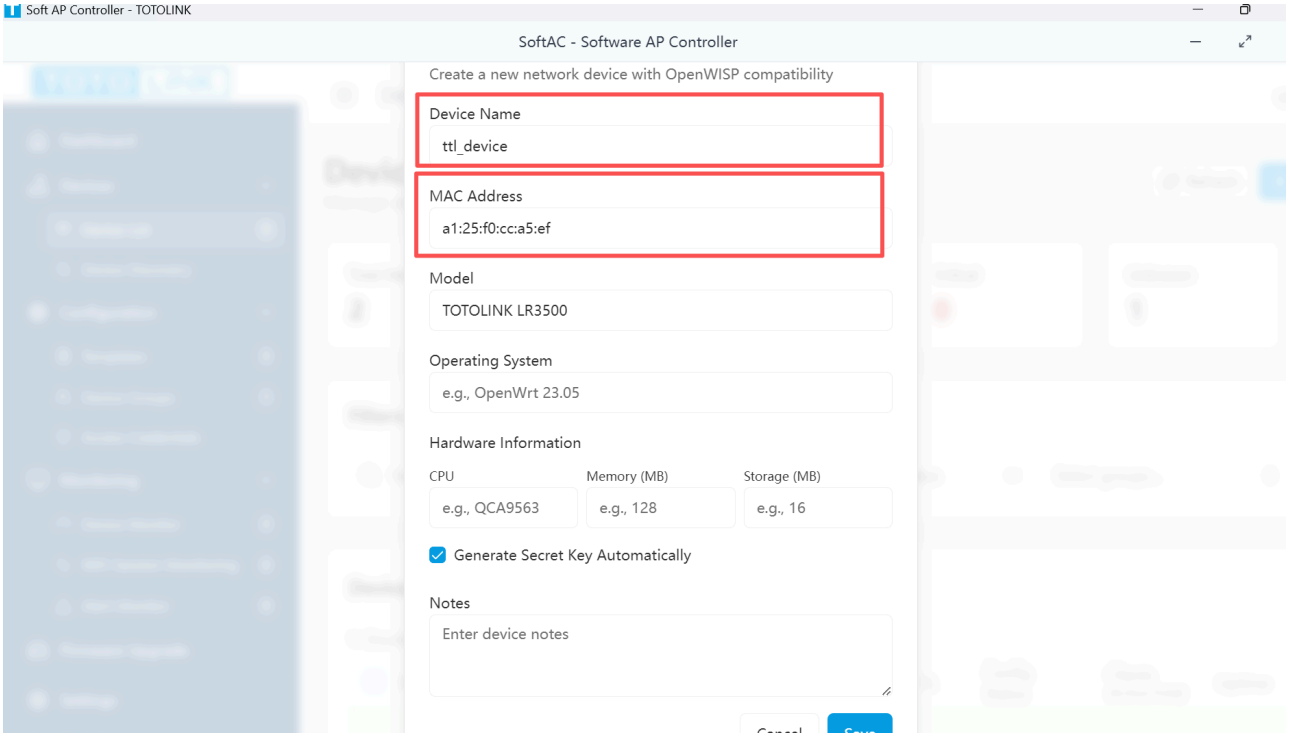


3. **Enter Device Information**
   Fill in the required device details in the dialog window:

Field	Description	Example
Device Name*	A descriptive name for easy identification	Office AP Floor 1
MAC Address*	The device's physical network address	00:11:22:33:44:55
Model	Device model number	A3002RU

Field	Description	Example
Operating System	Device firmware type	OpenWrt
Notes	Additional information or location details	Near conference room

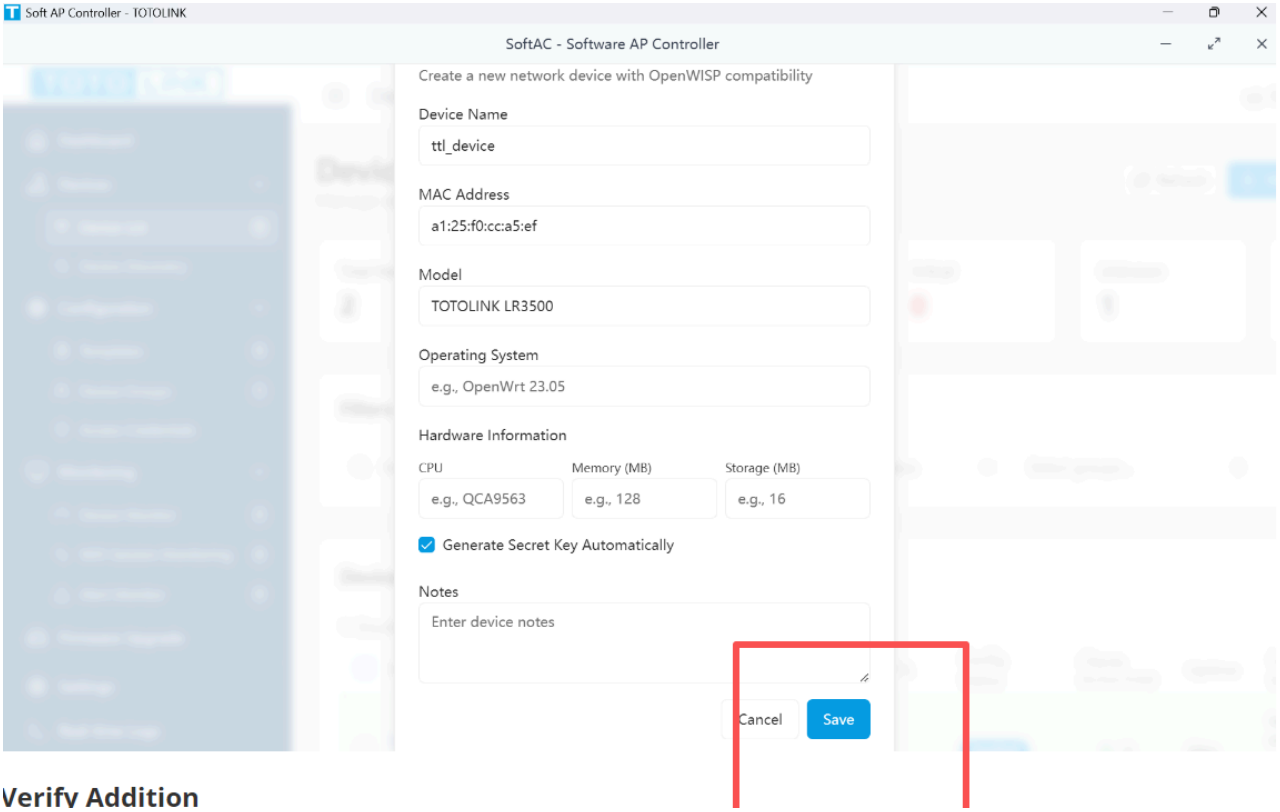
> 📝 **Note**: Fields marked with * are compulsory.



4. **Configure Security Settings**
   - Check "Generate Secret Key Automatically" for the system to create a secure key
   - Or manually enter a custom key if required by your security policy

> 🔒 **Security Tip**: Use auto-generated keys for better security. Store keys securely as they are required for device authentication.

5. **Save Device**
   Click the "Save" button to add the device to your system.



Verifv Addition

6. **Verify Addition**

   After successful addition:

   - A green success notification appears in the top right
   - The new device appears in the device list
   - Initial status shows as "Offline" until the device connects

Important Notes

> ⚠️ **Warning**:
>
> - Each MAC address must be unique in the system
> - Devices require proper network configuration to connect after registration
> - Keep device keys confidential to prevent unauthorized access

> 💡 **Tip**:
> You can prepare devices offline and add them in bulk using the import feature for large deployments.

Related Functions

- 4.2 Editing Device Information
- 4.3 Device Configuration
- 6.2 Creating Groups

4.2 Editing Device Information

Function Overview

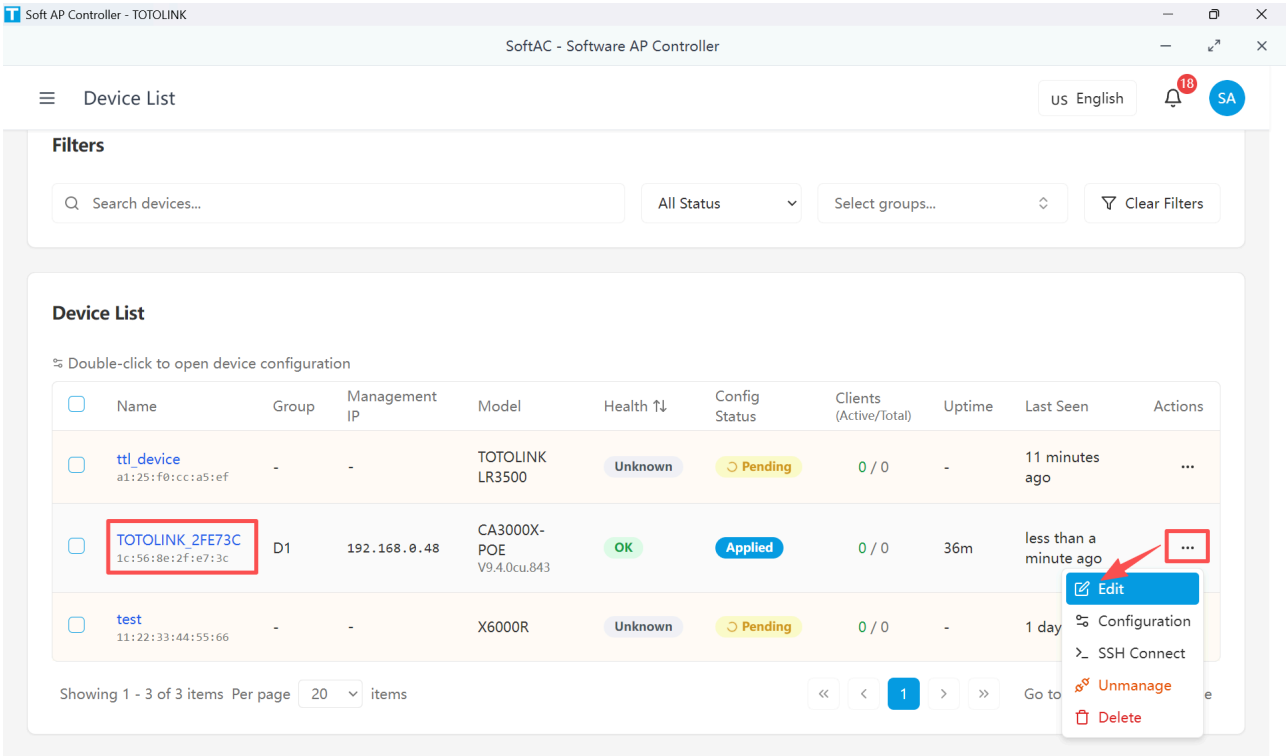
Edit Device Information allows you to update device details after initial registration. You can modify the device name and notes while hardware information remains read-only to maintain data integrity.

Use Cases

- **Renaming Devices**: Update device names to reflect new locations or purposes
- **Adding Notes**: Document maintenance history or special configurations
- **Updating Documentation**: Keep device information current with device changes

Operating Steps

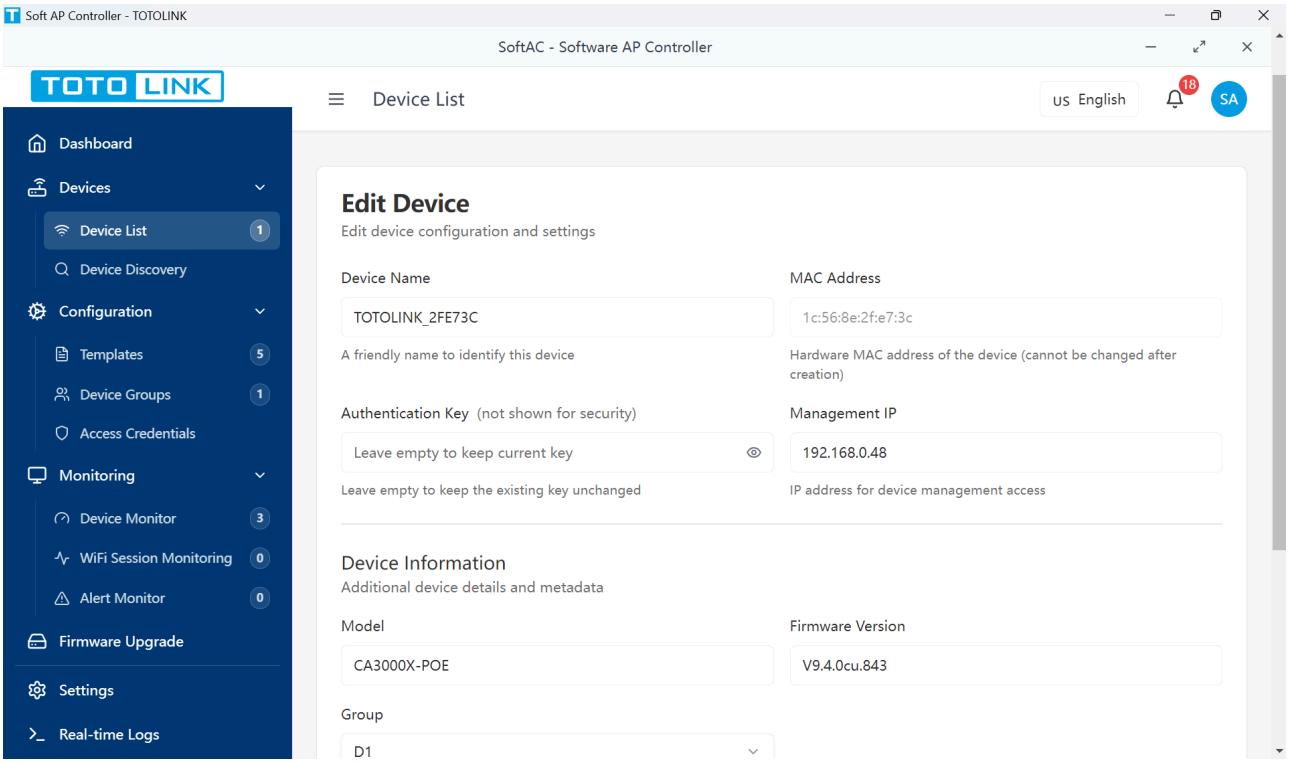
1. **Access Edit Options**
   There are two ways to edit device information:
   - Click the device name link in the device list
   - Click the three-dot menu and select "Edit"



2. **Modify Device Information**
   In the edit dialog, you can update:
   - **Device Name**: Change to a more descriptive identifier
   - **Notes**: Add or update operational notes

   Read-only fields (cannot be modified):
   - **MAC Address**
   - **Model**
   - **Operating System**

- **Hardware specifications**



3. **Save Changes**
   Click "Save" to save your modifications.

> ✅ **Success**: Changes are applied immediately without requiring device restart.

Important Notes

> 📝 **Note**: Hardware information is automatically detected during device registration and cannot be manually modified, in order to ensure accuracy.

> 💡 **Best Practice**: Use consistent naming conventions for devices (e.g., Building-Floor-Location format).

4.3 Device Configuration

Function Overview

Device Configuration provides comprehensive tools to manage device settings, apply configuration templates, set variables, and maintain configuration versions. This centralized approach ensures consistent network policies across all devices.

Use Cases

- **Initial Setup**: Configure newly added devices with standard settings
- **Policy Updates**: Apply new security or network policies across devices
- **Troubleshooting**: Adjust specific device settings to resolve issues
- **Standardization**: Apply templates to ensure configuration consistency

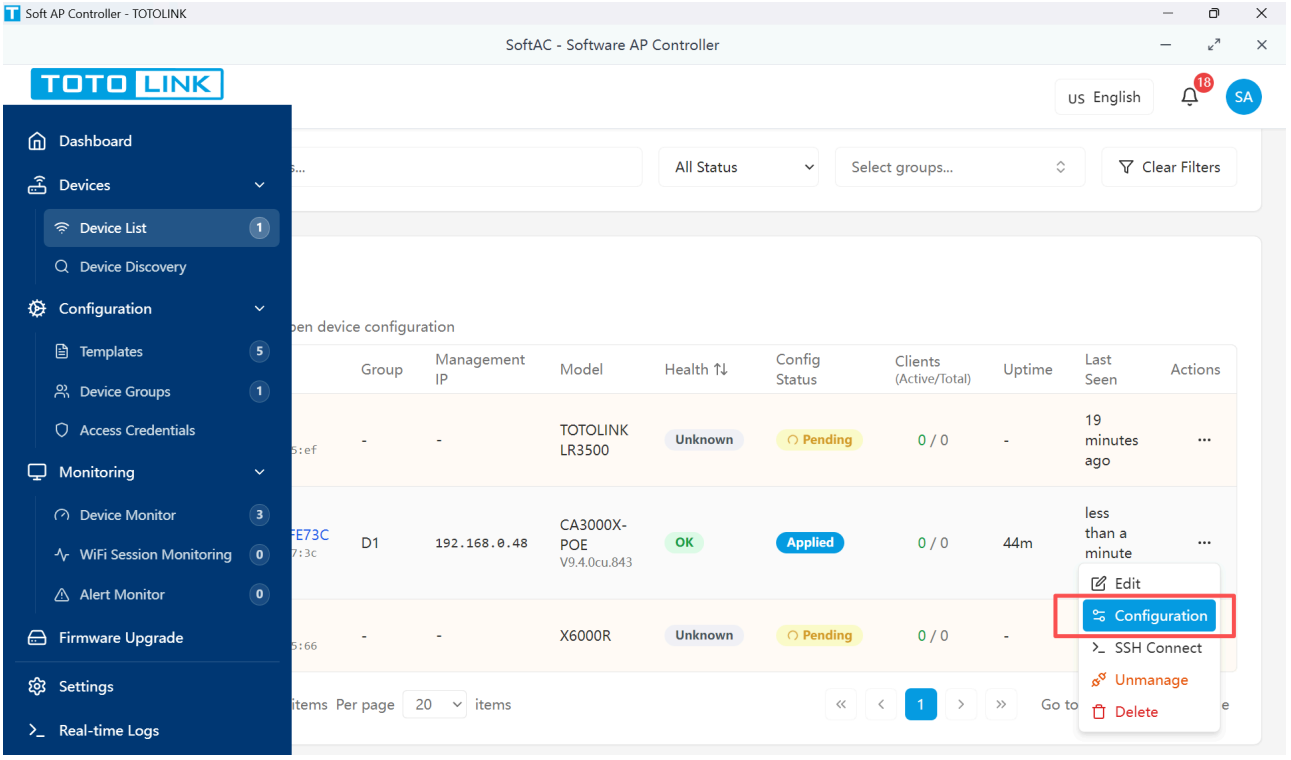
Operating Steps

Accessing Device Configuration

1. **Open Configuration Interface**

   There are two ways to open device configuration interface:

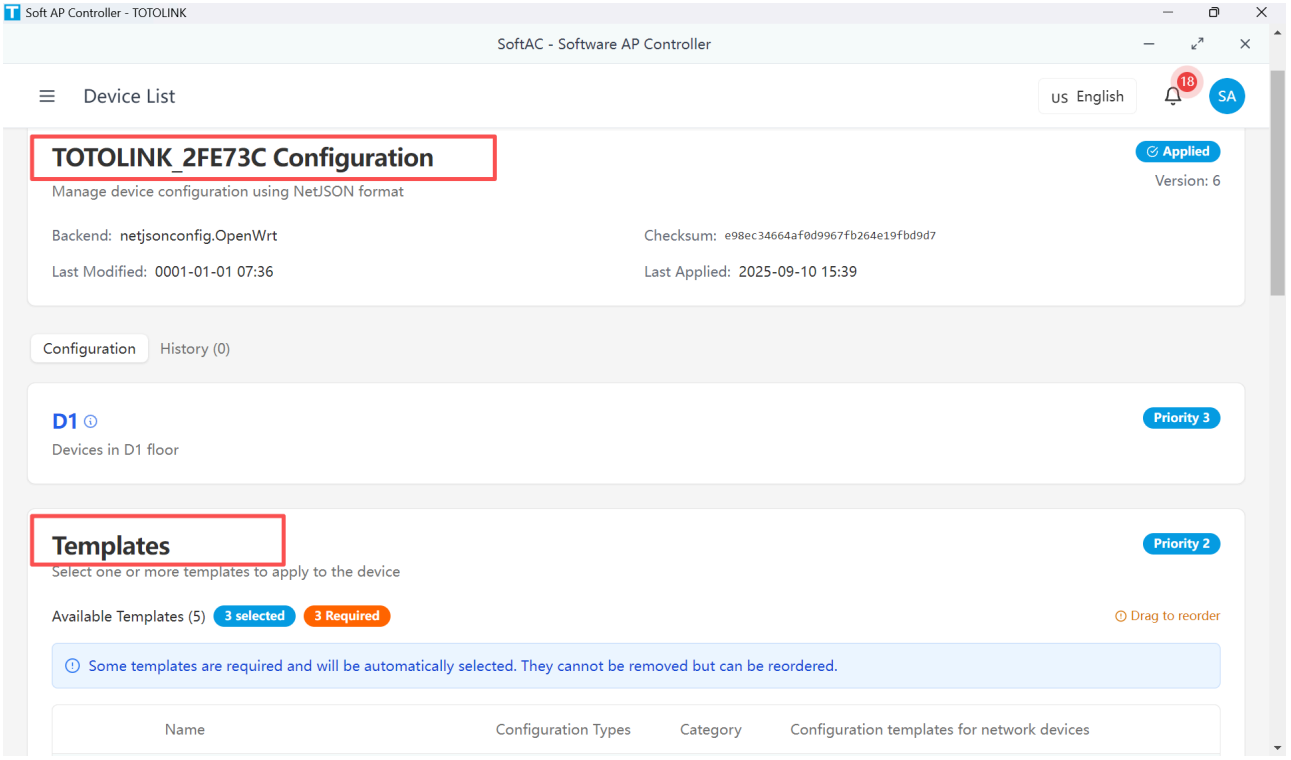
   - Double click the device row
   - Or select "Configuration" from the device's action menu

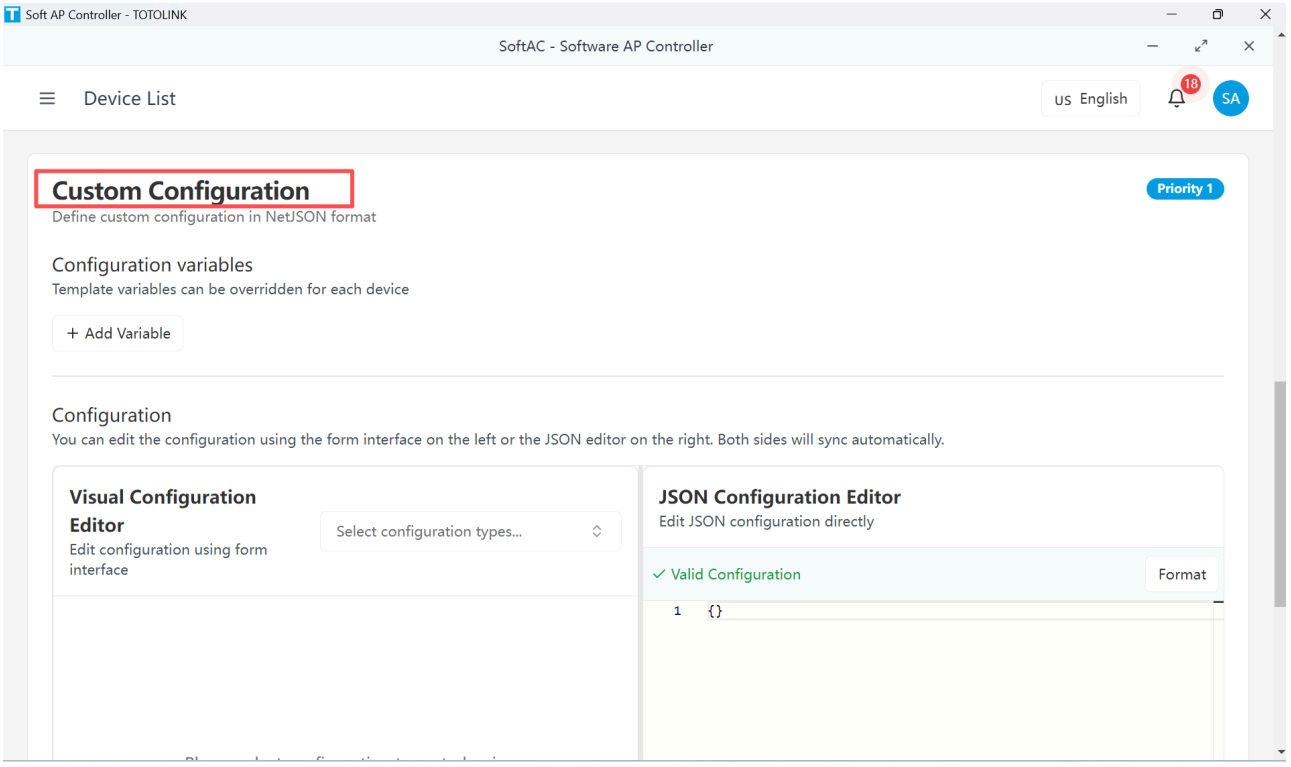


2. **Configuration Interface Overview**

   The configuration page contains three main tabs:

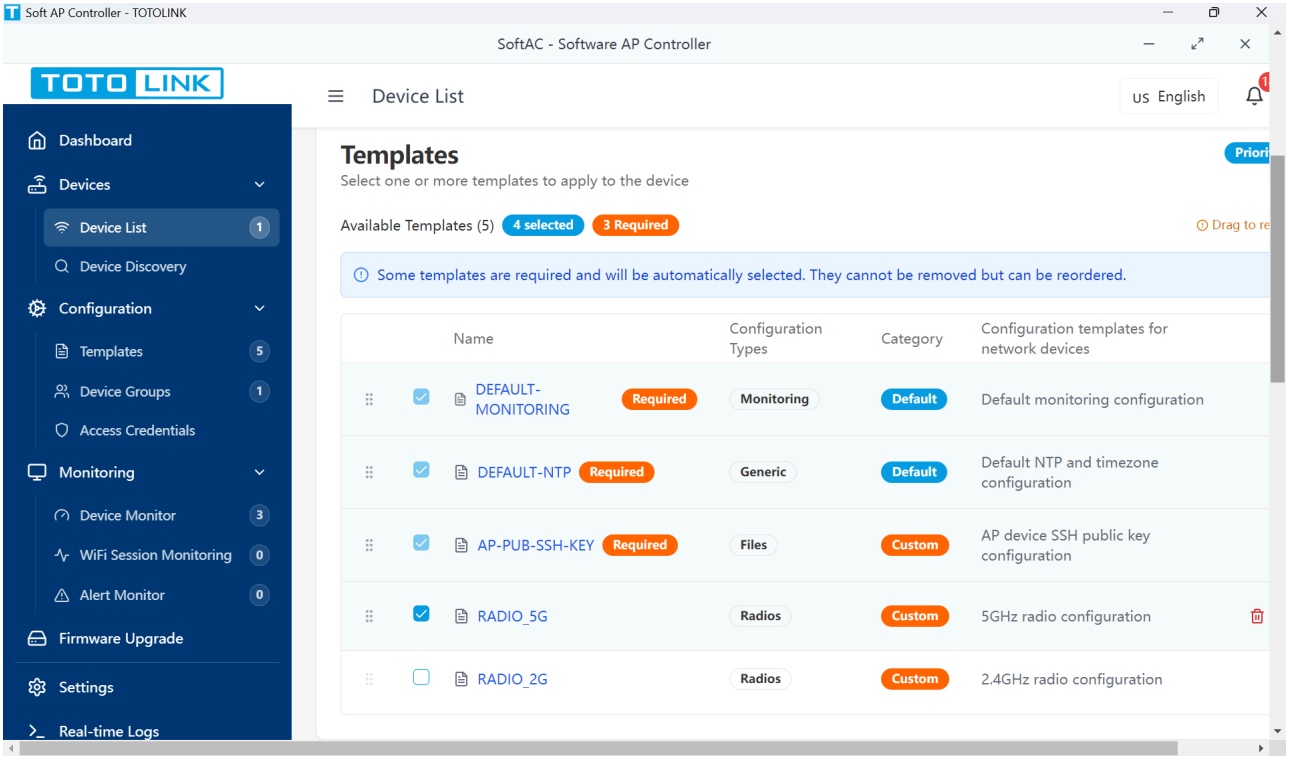
   - **Basic Configuration**: Template selection and general settings
   - **Templates**: Dynamic values for templates
   - **Custom Configuration**: JSON editor for detailed configuration





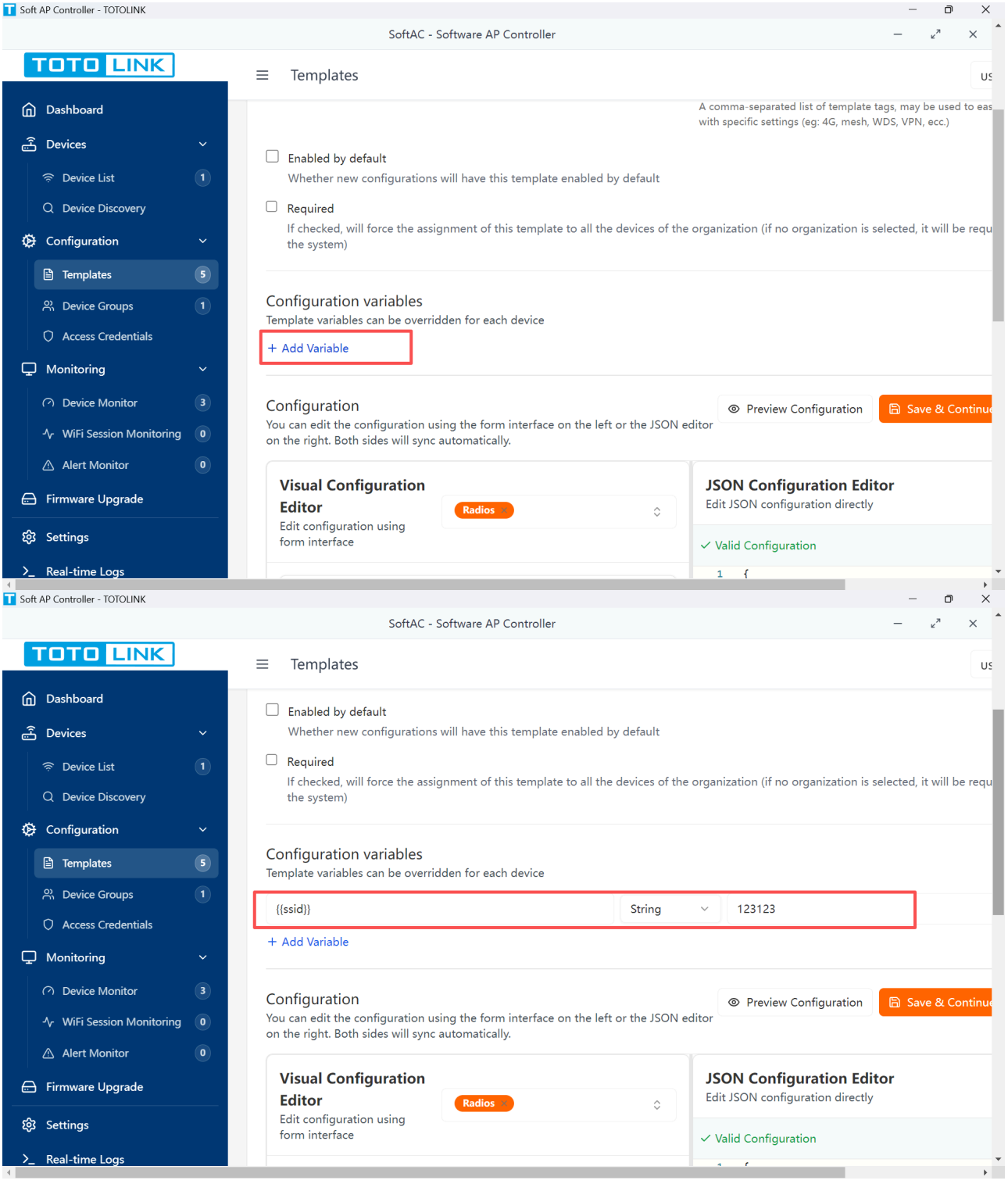
Applying Configuration Templates

1. **Select Templates**
   In the Template Selection area:
   - Browse available templates by category
   - Select one or more templates to apply
   - Templates are applied in order (top to bottom)

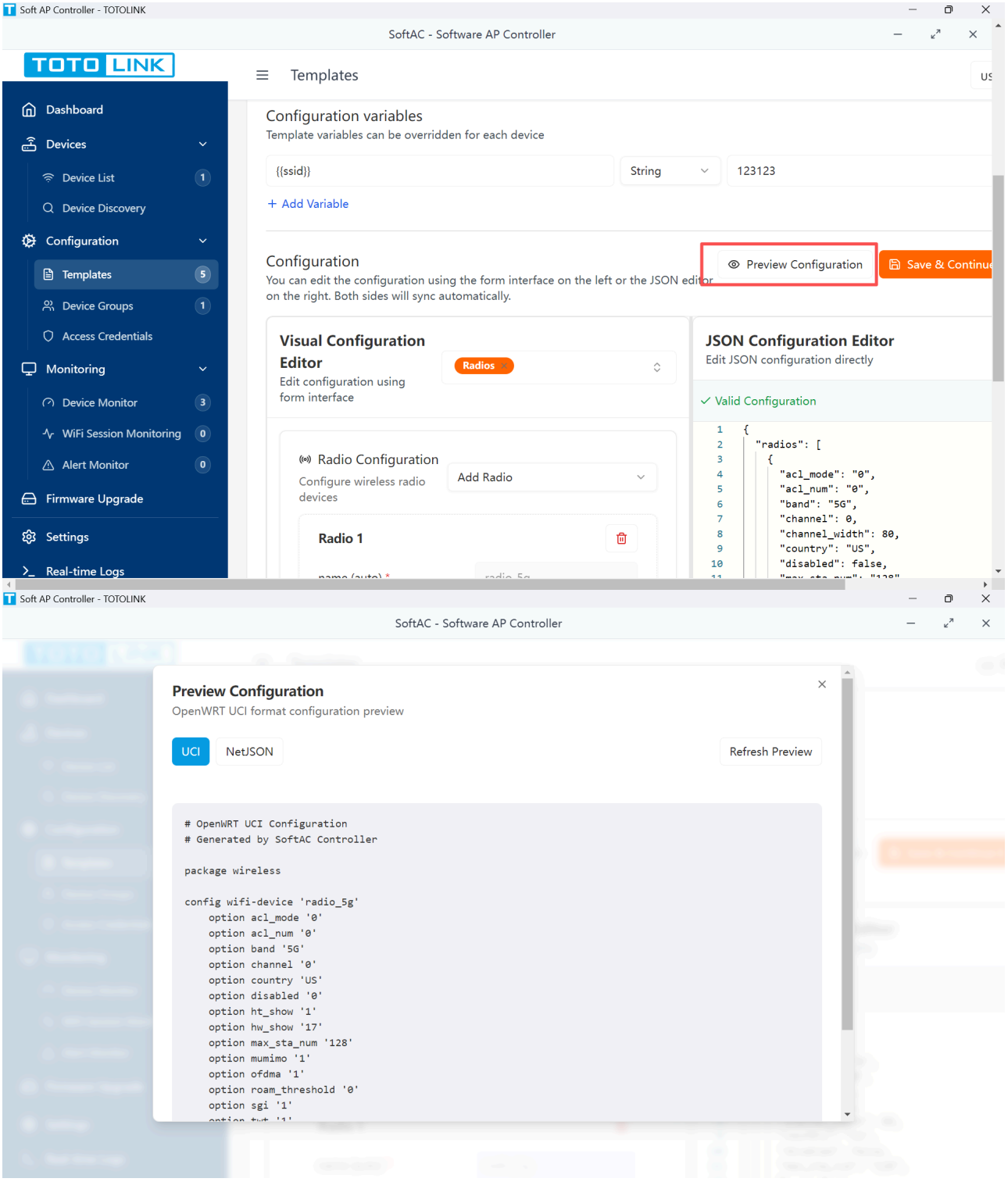


2. **Configure Variables**
   Click "Add Variables" tab to set dynamic values:

Variable	Type	Description	Example
ssid_name	String	Wireless network name	Office_WiFi
channel	Integer	Wireless channel	6
tx_power	Integer	Transmission power (dBm)	20
vlan_id	Integer	VLAN identifier	100



3. **Preview Configuration**
   Click "Preview Configuration" to see the merged configuration before applying:
   - Review all settings
   - Check for conflicts
   - Verify variable substitution

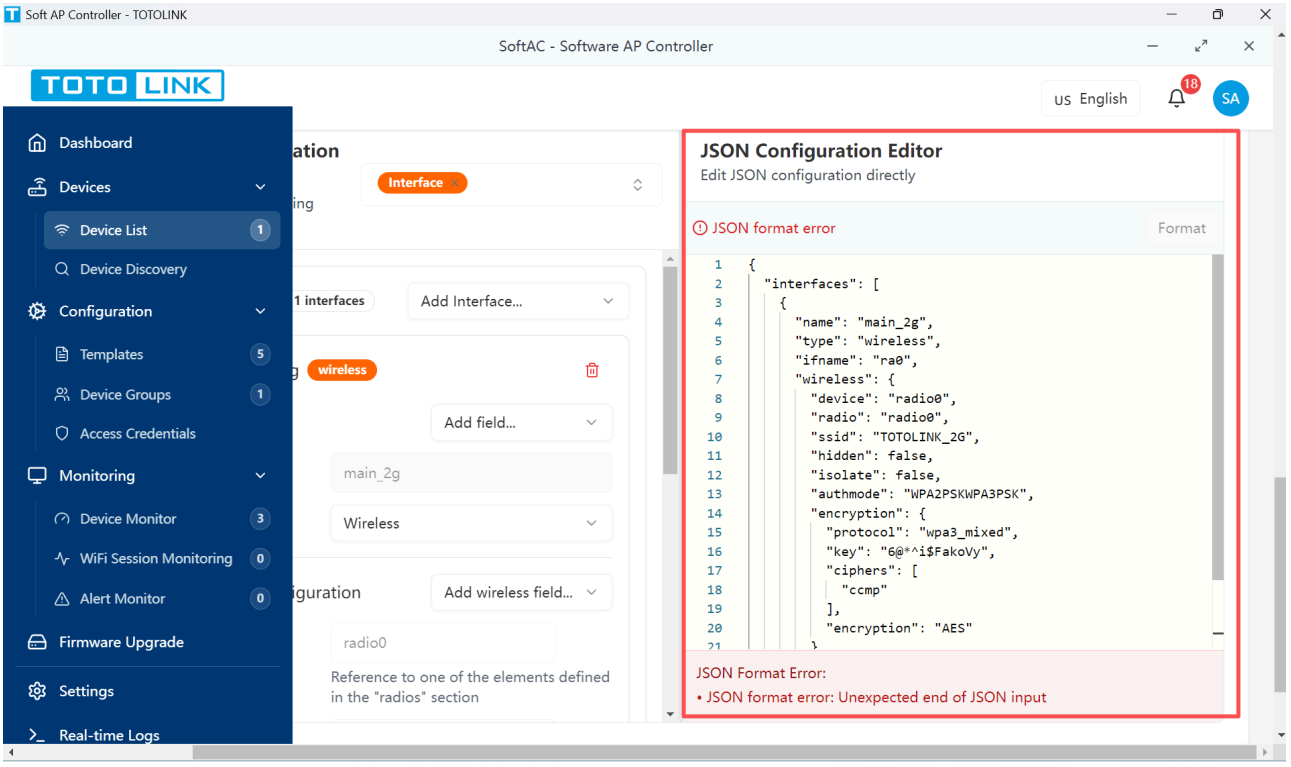


4. **Save and Apply**
   Click "Save Configuration" to apply settings:
   - Configuration is validated before sending
   - Device receives and applies new settings
   - Status updates to "Pending" then "Applied"

> **Note**: Configuration typically applies within 30-60 seconds.

Advanced Configuration Editor

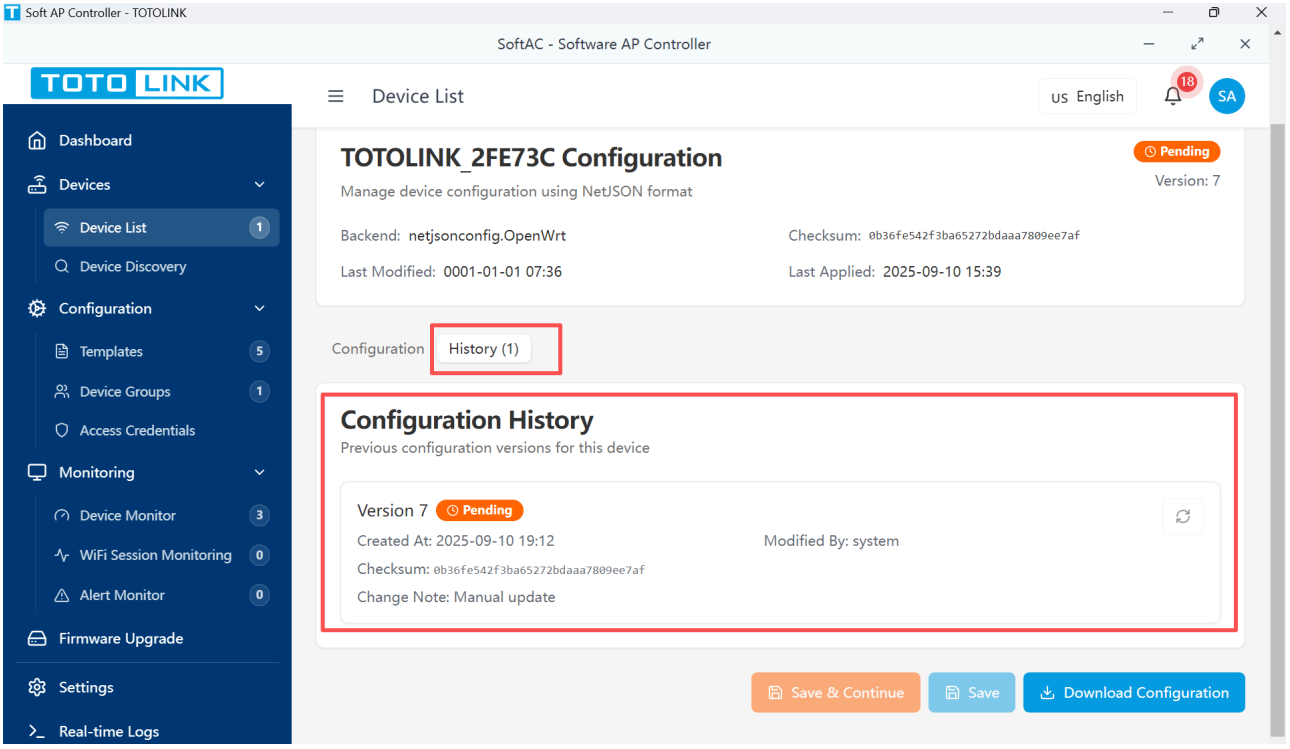
1. **Access JSON Editor**
   Edit JSON in "Custom Configuration" tab:
   - Modify JSON structure directly
   - Use syntax highlighting for clarity
   - Real-time validation shows errors



> ⚠️ **Warning**: Direct JSON editing requires knowledge of configuration schema. Incorrect settings may cause device malfunction.

Configuration History and Rollback

1. **View History**
   Access the configuration history panel to see:
   - Previous configuration versions
   - Timestamp of each change
   - User who made the change



2. **Rollback Configuration**
   To restore a previous configuration:
   - Select the desired version from history
   - Click "Rollback to this version"
   - Confirm the rollback action

> 🔄 **Note**: Rollback creates a new configuration version rather than deleting history.

Configuration Status Indicators

Status	Description	Action Required
Applied	Configuration successfully active	None
Pending	Configuration sent, awaiting application	Wait for device processing
Modified	Local changes not yet saved	Save configuration
Error	Configuration failed to apply	Check device connectivity and logs

Important Notes

> ⚠️ **Critical**: Always preview configuration changes before applying to production devices.

> 💡 **Best Practice**: Test configuration changes on a single device before applying to groups.

> 🔒 **Security**: Sensitive configuration data (passwords, keys) is encrypted during transmission.

Related Functions

- 5.2 Creating Templates
- 6.4 Group Configuration

4.4 Batch Operations

Function Overview

Batch Operations enable efficient management of multiple devices simultaneously, saving time and ensuring consistency across your network device. These tools are essential for large-scale deployments and maintenance tasks.

Use Cases

- **Group Assignment**: Organize multiple devices into logical groups
- **Bulk Deletion**: Remove multiple obsolete devices at once
- **Mass Configuration**: Apply settings to multiple devices simultaneously
- **Maintenance Tasks**: Perform updates or changes across device sets

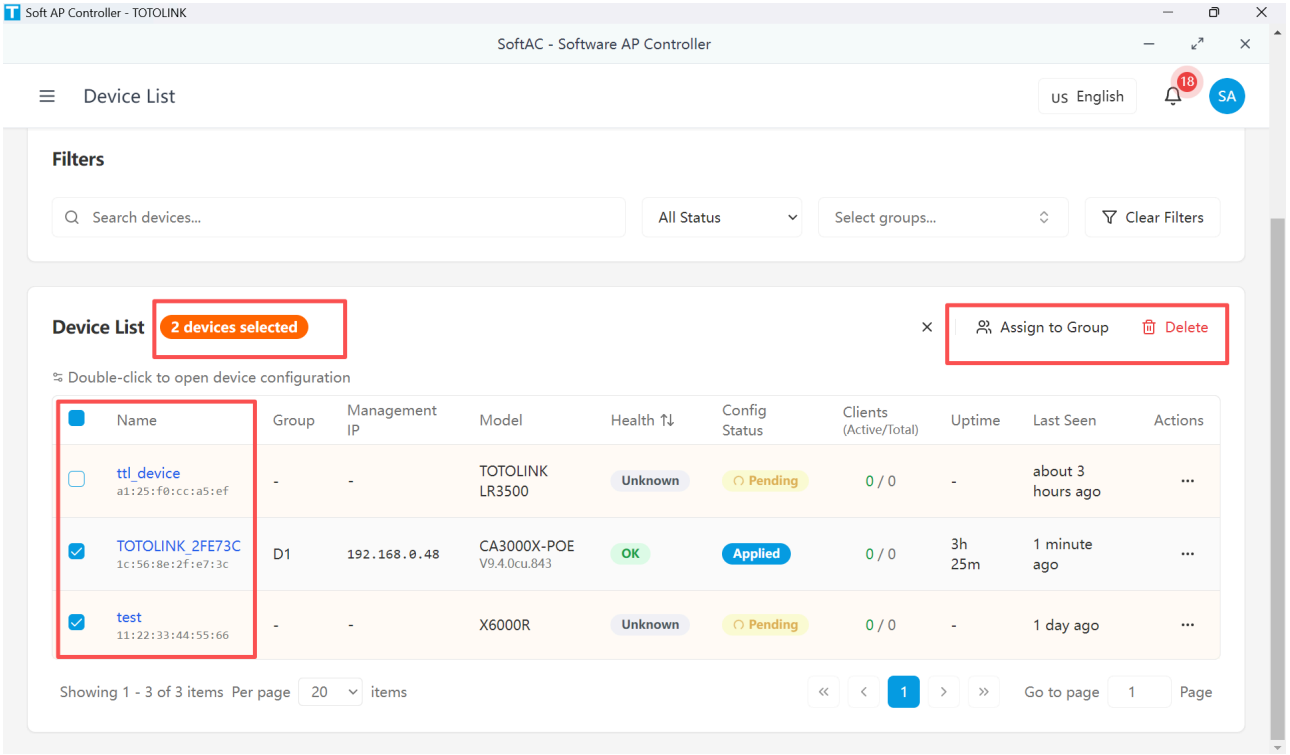
Operating Steps

Selecting Multiple Devices

1. **Enable Selection Mode**
   The checkbox column appears automatically in the device list.
2. **Select Devices**
   - Click individual checkboxes to select specific devices
   - Use the header checkbox to select/deselect all visible devices

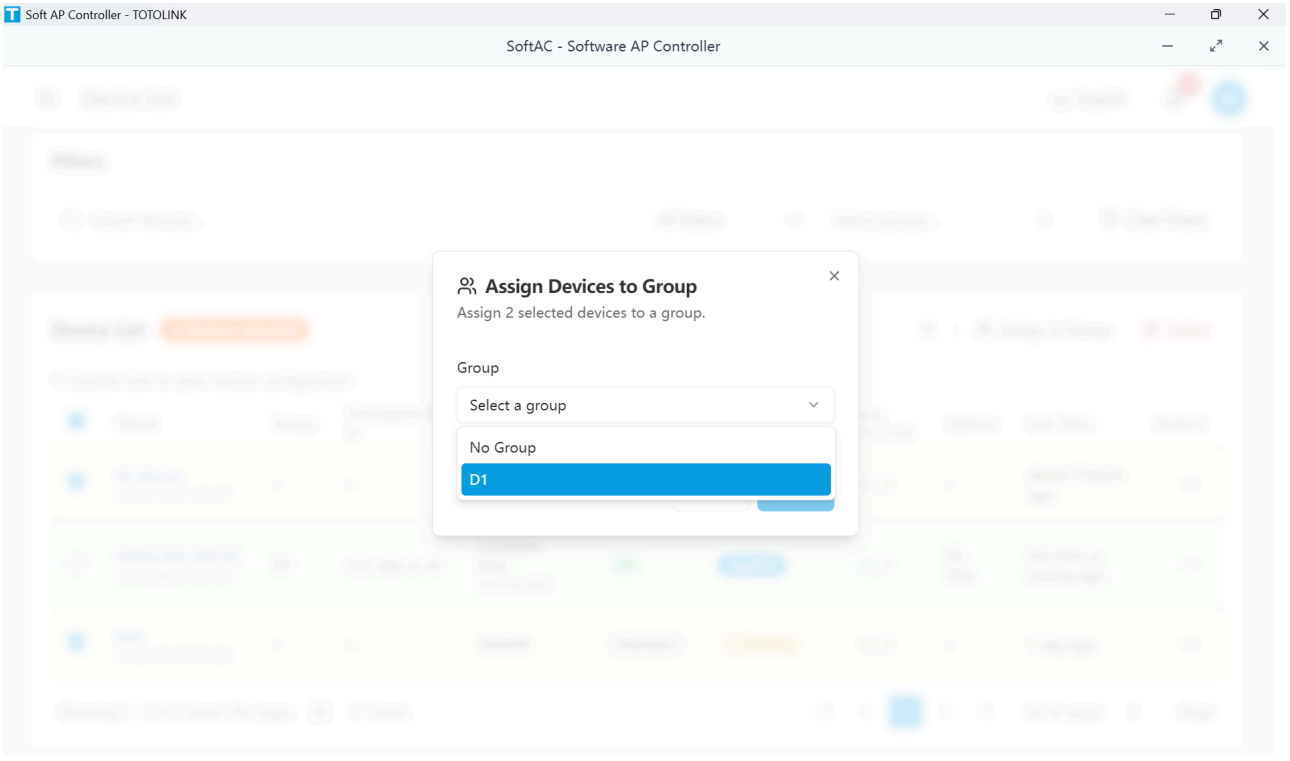
   > 💡 **Tip**: Use filters and search to display only the devices you want to select.

3. **View Selection Count**
   A selection toolbar appears showing:
   - Number of selected devices
   - Available batch actions



Bulk Assign to Group

1. **Initiate Group Assignment**
   With devices selected, click "Assign to Group" in the batch actions toolbar.
2. **Select Target Group**
   In the assignment dialog:
   - Choose the destination group from the dropdown
   - View the list of selected devices
   - Confirm the assignment scope

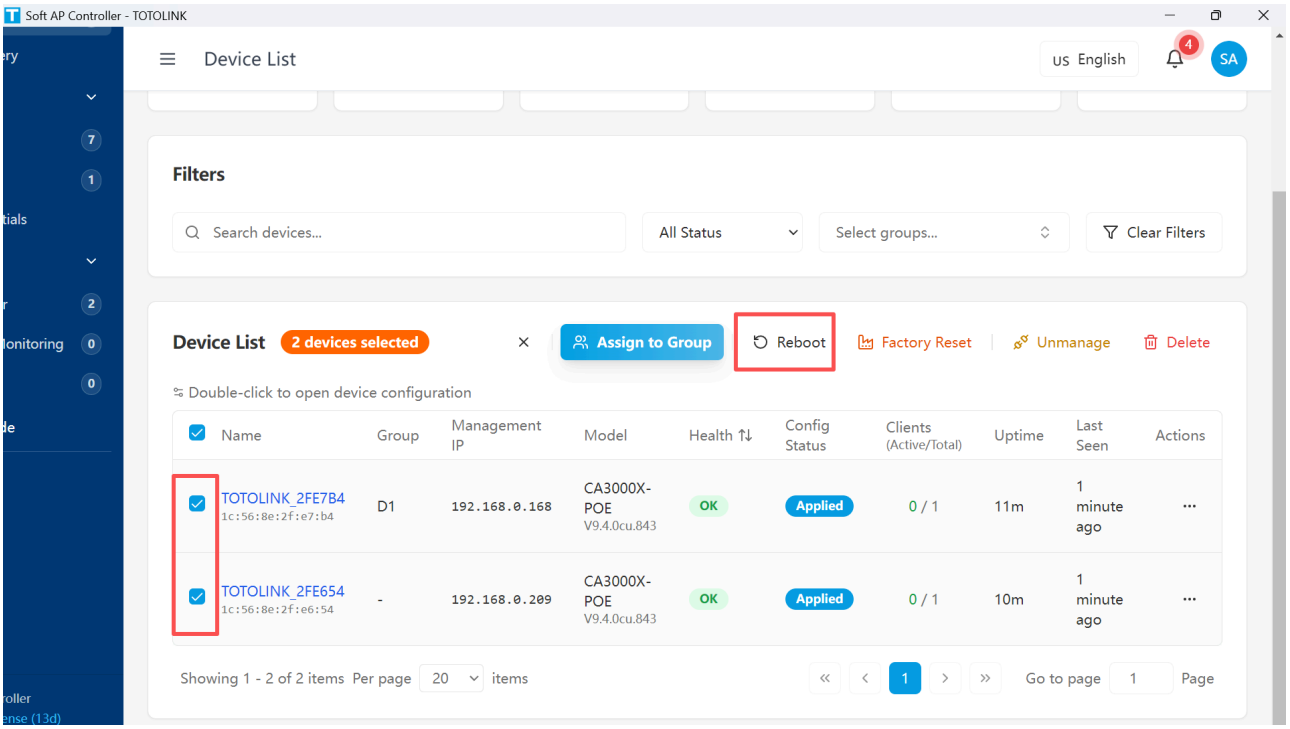


3. **Apply Assignment**
   Click "Assign" to move all selected devices to the chosen group.

> ✅ **Result**: All selected devices inherit the group's configuration templates and settings.

Bulk Reboot Devices

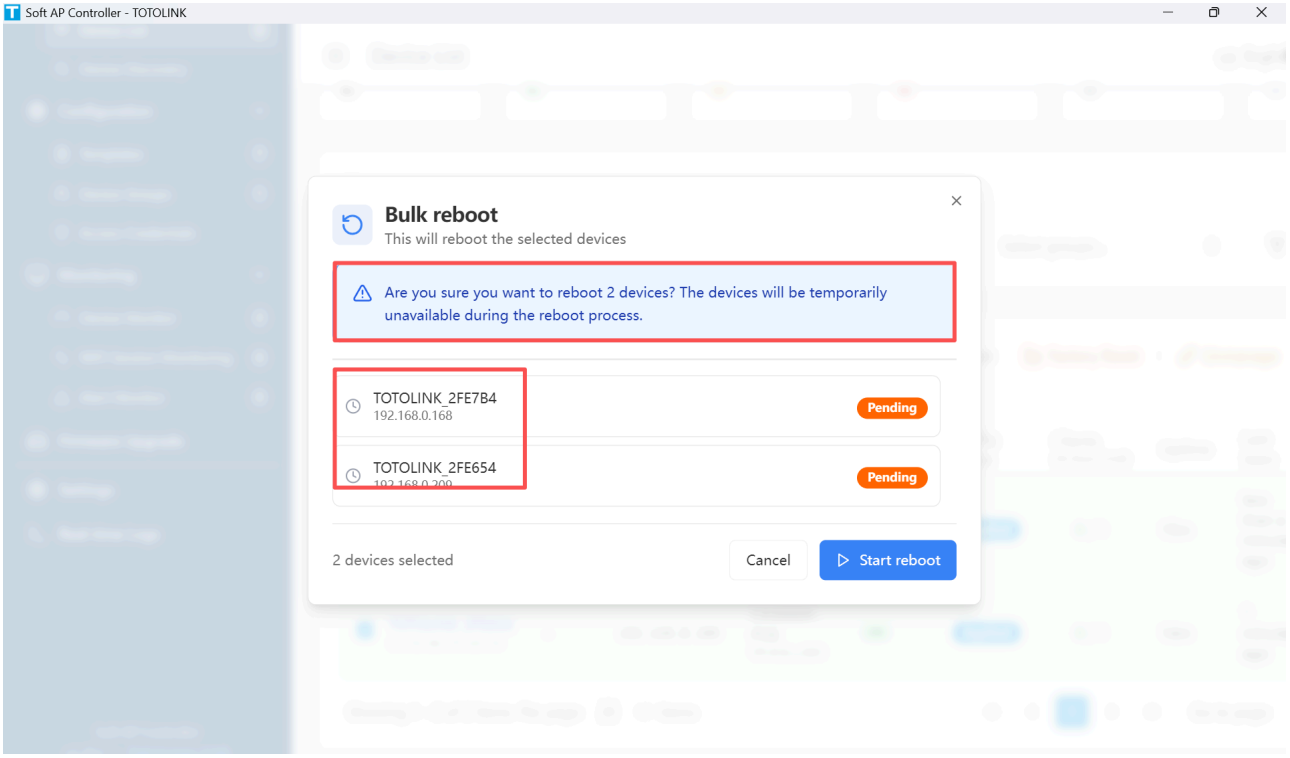
1. **Initiate Bulk Reboot**
   With devices selected, click "Delete".



2. **Review and Confirm**

   The confirmation dialog shows:

   - Number of devices to be rebooted
   - List of device names
   - Warning about reboot



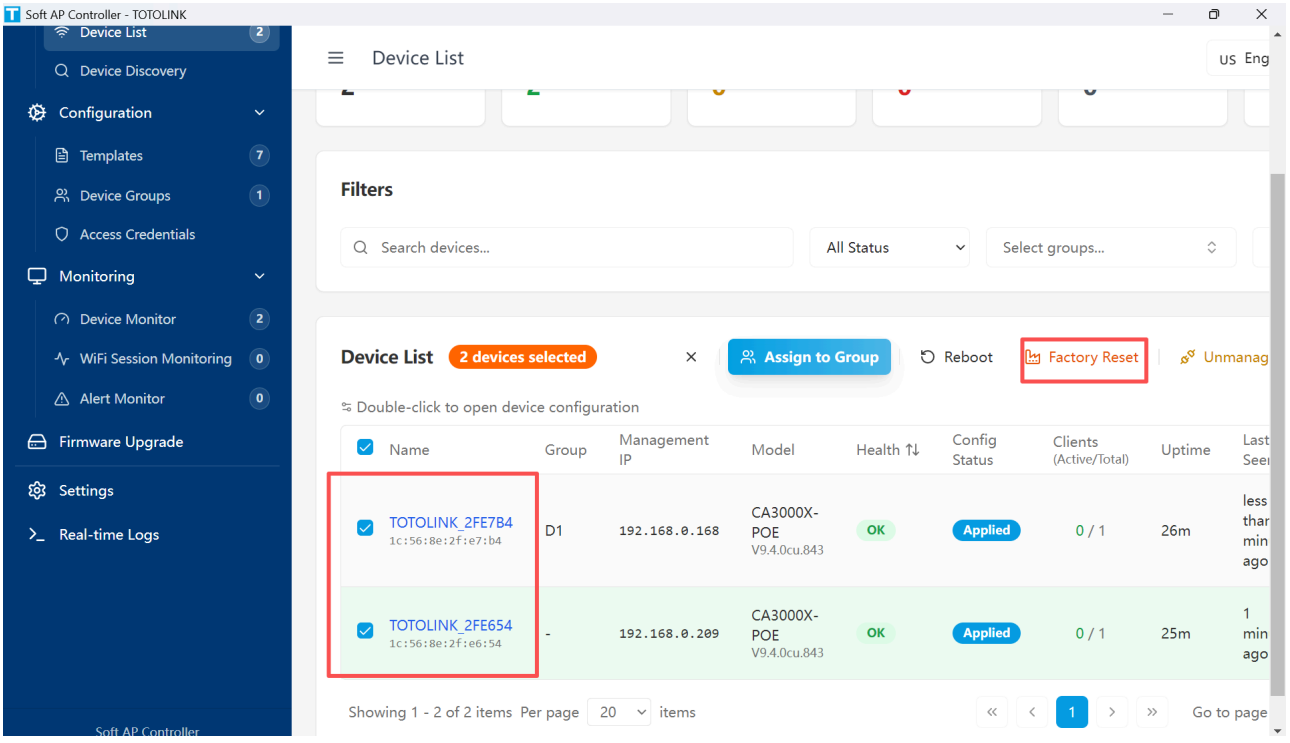
3.**Confirm Reboot**

Click "Start reboot" to proceed.

Bulk Factory Reset

1. **Initiate Bulk Factory Reset**

   With devices selected, click "Factory Reset".

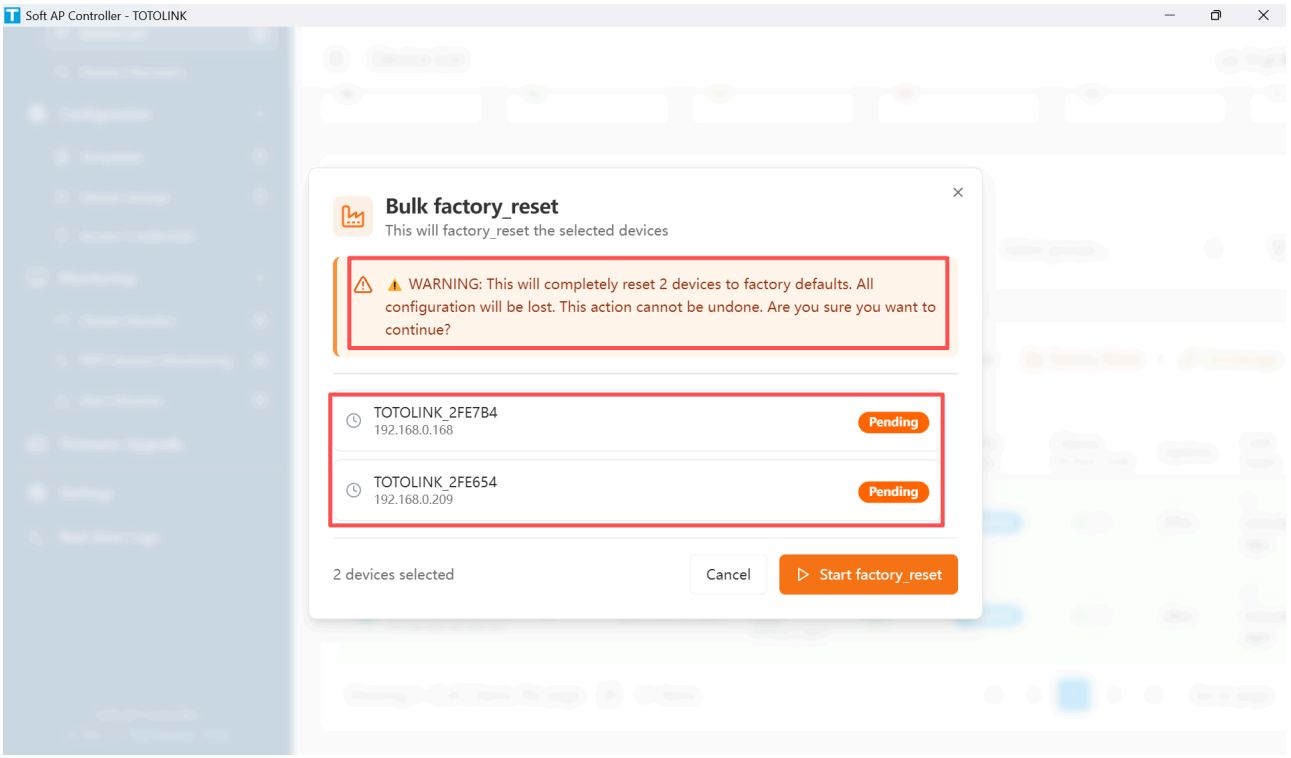


2. **Review and Confirm**

   The confirmation dialog shows:

   - Number of devices to be reset
   - List of device names

- Warning about reset



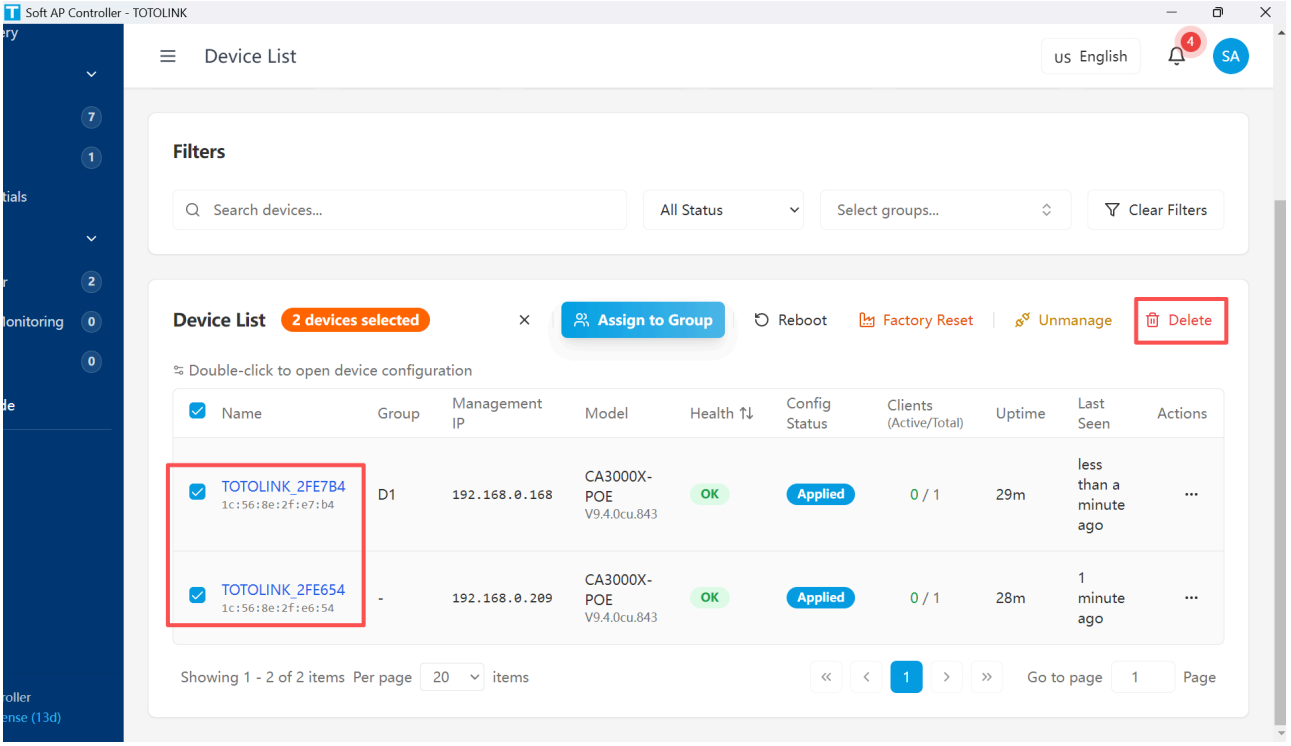
3.**Confirm Reset**

Click "Start factory reset" to proceed.

Bulk Delete Devices

1. **Initiate Bulk Delete**

With devices selected, click "Delete".

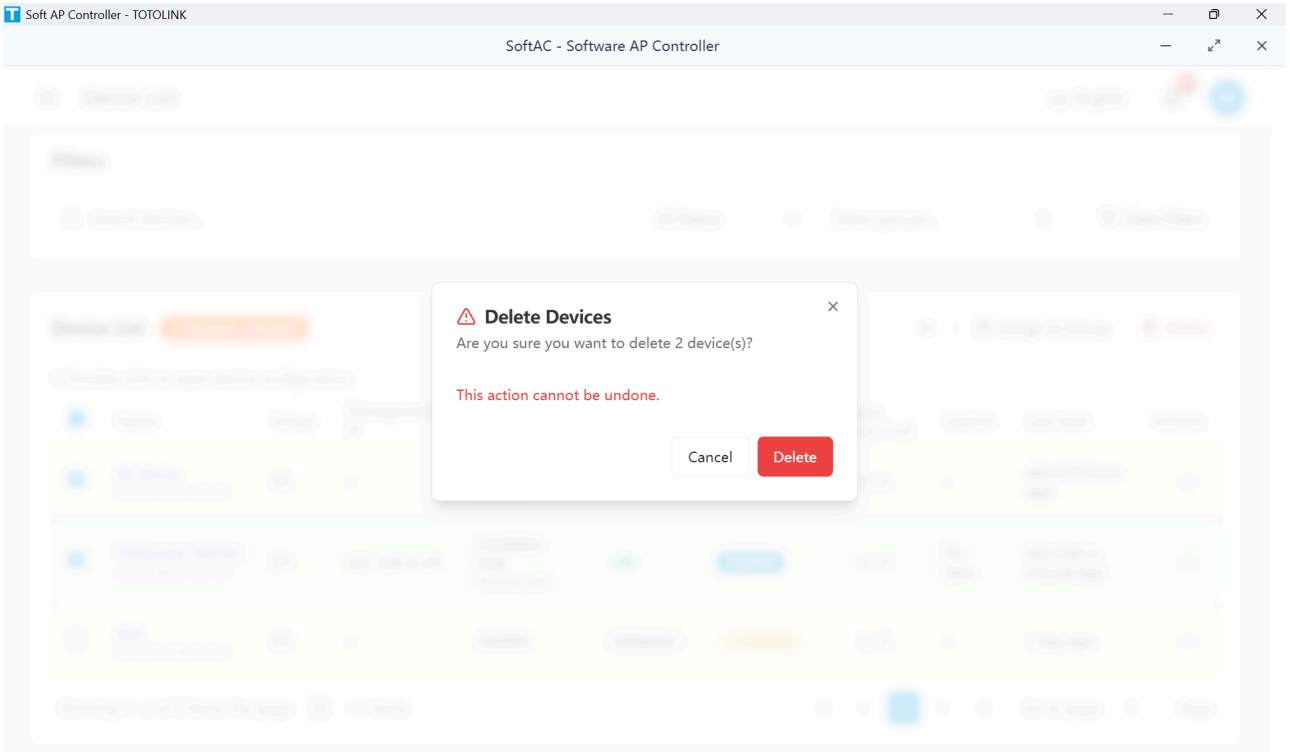


2. **Review and Confirm**

The confirmation dialog shows:

- Number of devices to be deleted

- List of device names
- Warning about permanent deletion



3. **Confirm Deletion**
   Click "Delete" to proceed.

> ⚠️ **Warning**: This action is permanent and cannot be undone. Deleted devices must be re-added manually.

Batch Operation Best Practices

> 💡 **Tips for Efficient Batch Operations**:
>
> - Use filters to narrow down device selection
> - Start with small batches when testing new configurations
> - Monitor the first few devices after batch updates
> - Schedule major batch operations during maintenance windows

Important Notes

> ⚠️ **Performance Consideration**: Large batch operations may take several minutes to complete.

> 🔒 **Safety Feature**: Batch operations require confirmation to prevent accidental changes.

> 📝 **Audit Trail**: All batch operations are logged for compliance and troubleshooting.

Related Functions

- 6.3 Managing Group Members
- 4.5 Device Status Monitoring

4.5 Device Status Monitoring

Function Overview

Device Status Monitoring provides real-time visibility into the health and performance of all managed devices. This comprehensive monitoring system helps identify issues proactively and maintain optimal network performance.

Use Cases

- **Health Monitoring**: Track device operational status and availability
- **Performance Analysis**: Monitor resource utilization and client connections
- **Troubleshooting**: Identify and diagnose device issues quickly
- **Capacity Planning**: Analyze usage patterns for device planning

Monitoring Dashboard

Status Overview

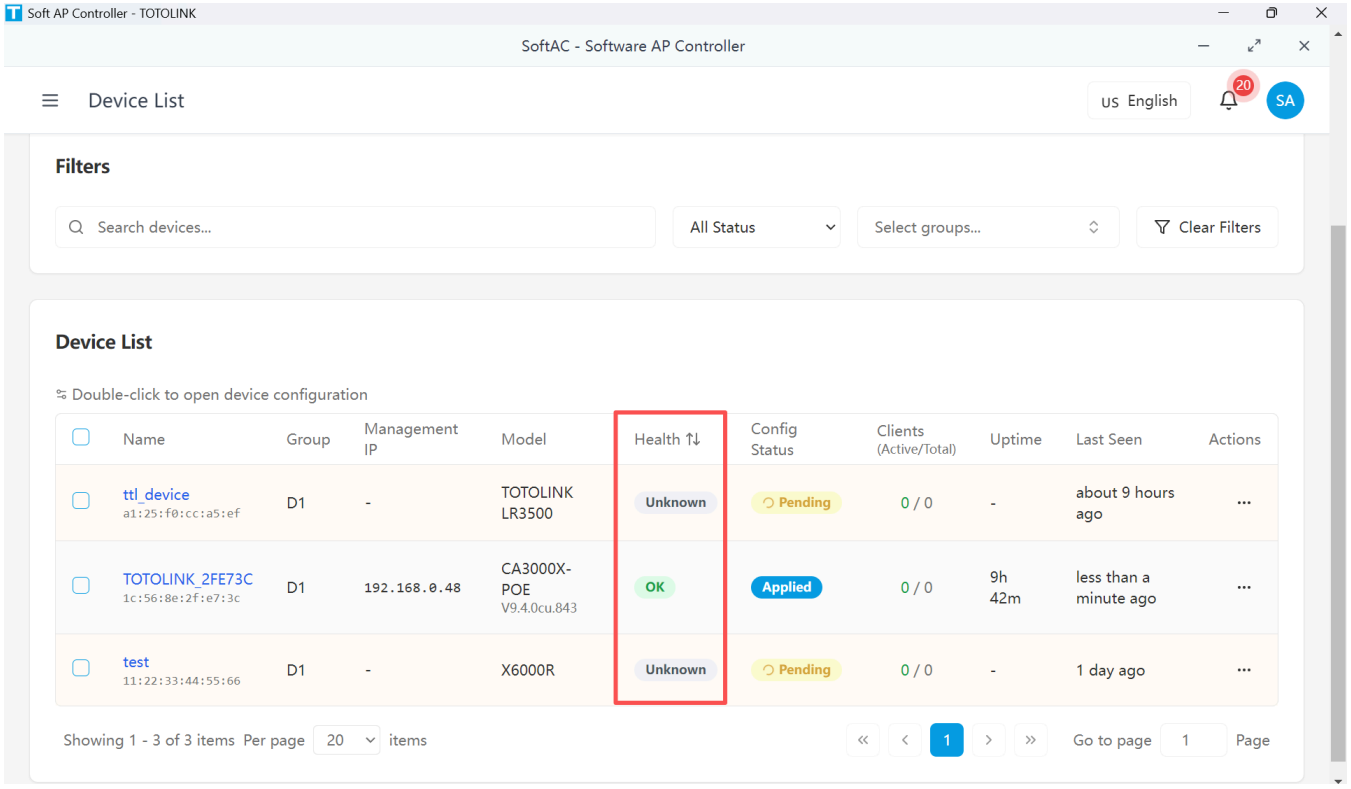
The device list displays real-time status information:

Indicator	Description	Visual Cue
Health Status	Overall device health	Color-coded badges
Configuration Status	Configuration deployment state	Status badges with icons
Client Count	Active/Total connected clients	Numeric display
Uptime	Time since last restart	Duration format
Last Seen	Last communication timestamp	Relative time

[Screenshot: Device list showing all status columns]

Health Status Indicators

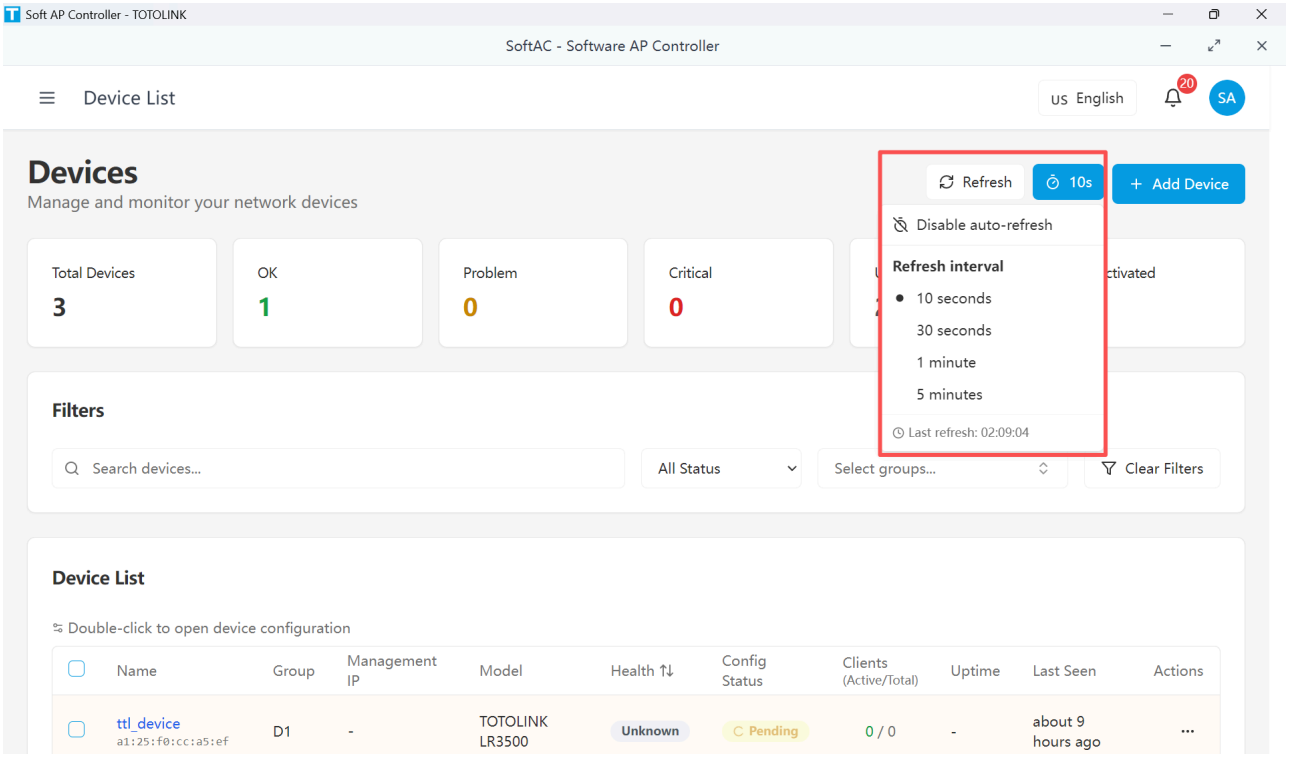
Status	Description	Typical Causes
🟢 OK	Device operating normally	All metrics within thresholds
🟡 Warning	Minor issues detected	High resource usage, minor alerts
🟠 Problem	Significant issues present	Connection issues, failed services
🔴 Critical	Severe problems requiring attention	Device offline, critical failures
⚫ Deactivated	Device manually disabled	Administrative action
⬜ Unknown	Status cannot be determined	New device, no data received



Real-Time Monitoring Features

Auto-Refresh Settings

1. **Enable Auto-Refresh**
   Click the timer icon in the toolbar to toggle auto-refresh.



Set Refresh Interval
Choose from preset intervals:

- 10 seconds (High frequency)
- 30 seconds (Default)

- 60 seconds (Standard)
- 5 minutes (Low frequency)

> 💡 **Tip**: Use shorter intervals during troubleshooting, longer intervals for general monitoring.

Device Details View

1. **Access Detailed Monitoring**
   Click on a device row to view expanded monitoring information:

   [Screenshot: Expanded device monitoring view]

2. **Performance Metrics**

Metric	Description	Normal Range
CPU Usage	Processor utilization	< 70%
Memory Usage	RAM consumption	< 80%
Disk Usage	Storage utilization	< 85%
Temperature	Device temperature	< 70°C
WiFi Clients	Connected wireless devices	Varies by model
Traffic Rate	Network throughput	Varies by connection

   [Screenshot: Performance metrics graphs]

3. **Historical Data**
   View trends over time:
   - 1 hour
   - 24 hours
   - 7 days
   - 30 days

   [Screenshot: Historical performance charts]

Client Monitoring

1. **View Connected Clients**
   The client count shows:
   - **Active Clients**: Currently transmitting data
   - **Total Clients**: All associated devices

   [Screenshot: Client count display]

2. **Client Details**
   Click the client count to see:
   - Client MAC addresses
   - Connection duration
   - Signal strength

- Data usage

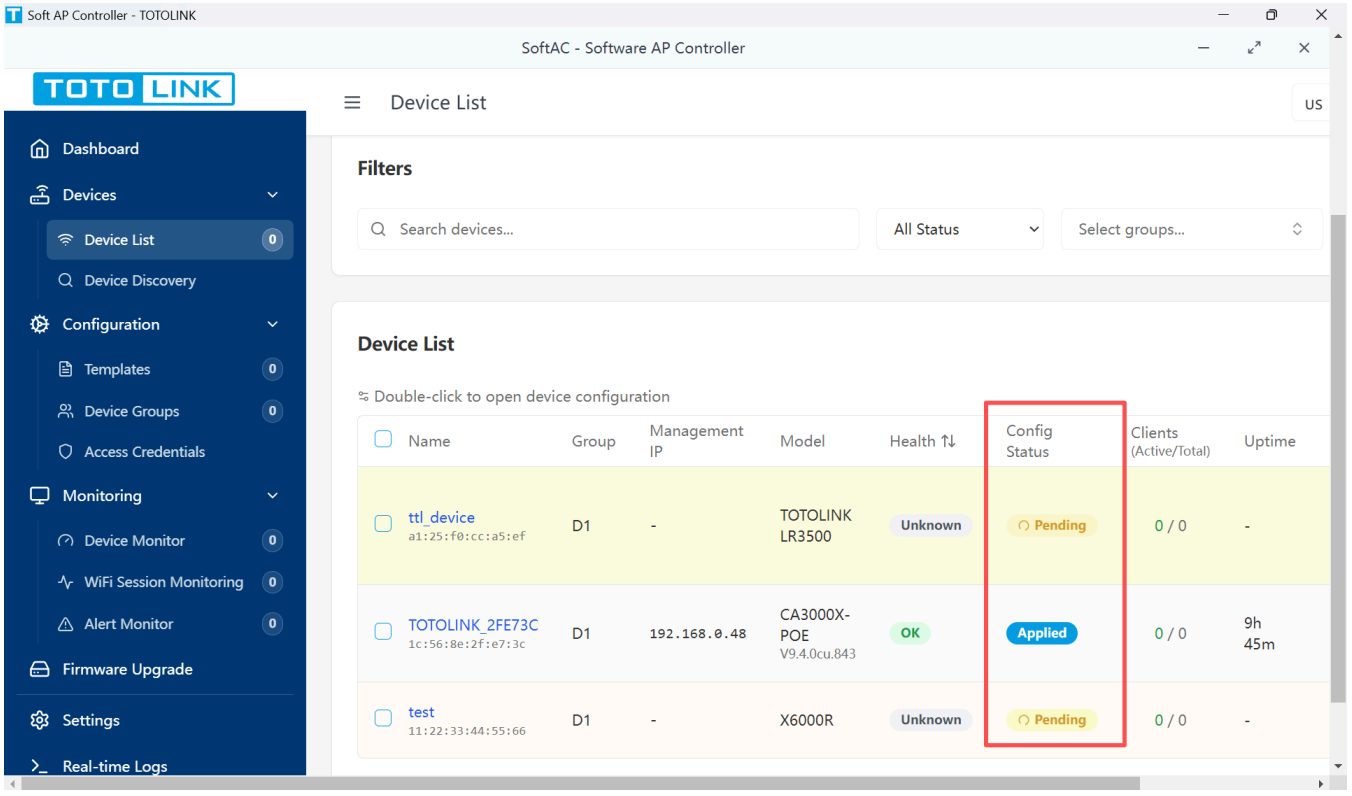
[Screenshot: Client details popup]

Alert Indicators

Visual Alerts

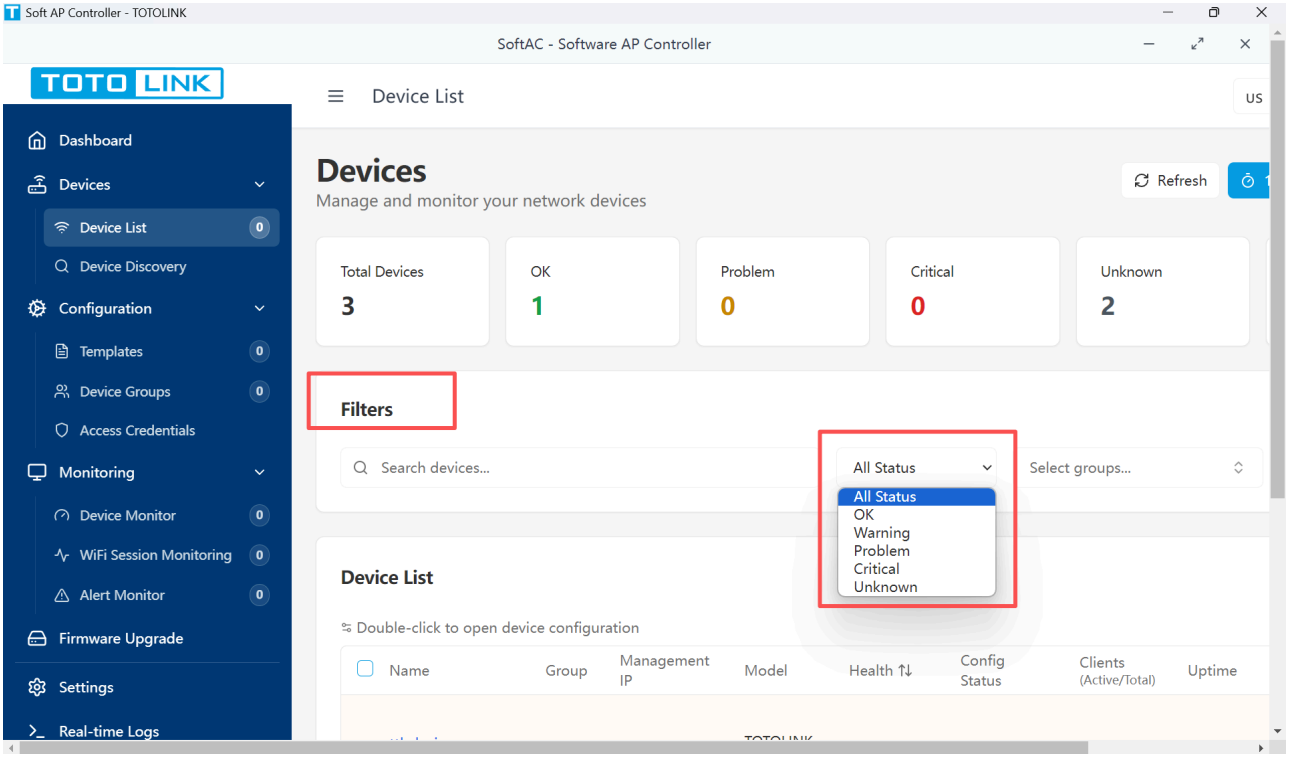
Devices requiring attention are highlighted:

- 🟡 Yellow background: Configuration pending
- 🟠 Orange background: Warning state
- 🔴 Red background: Critical issues
- 🔄 Pulsing animation: Active configuration deployment



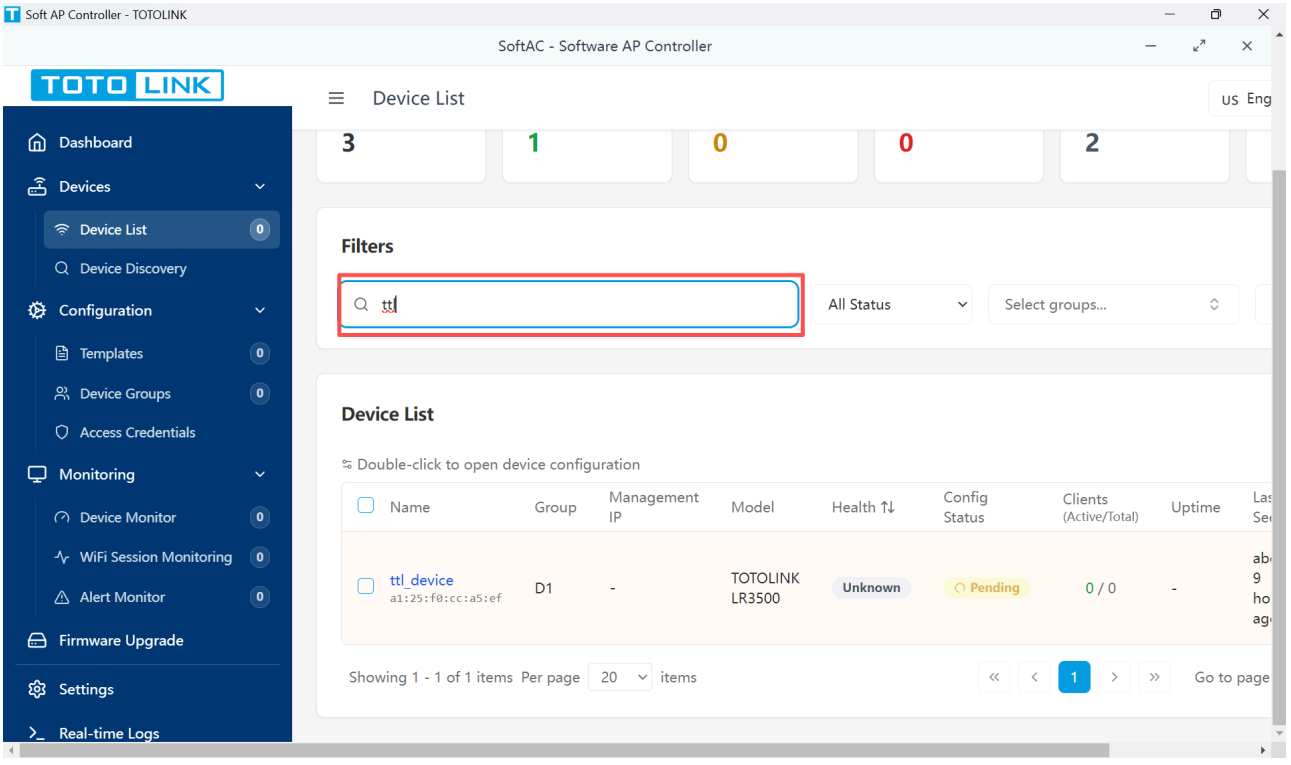
Status Filters

1. **Filter by Status**
   Use the status dropdown to show only:
   - All status
   - OK only
   - Warning
   - Problems
   - Critical
   - Unknown



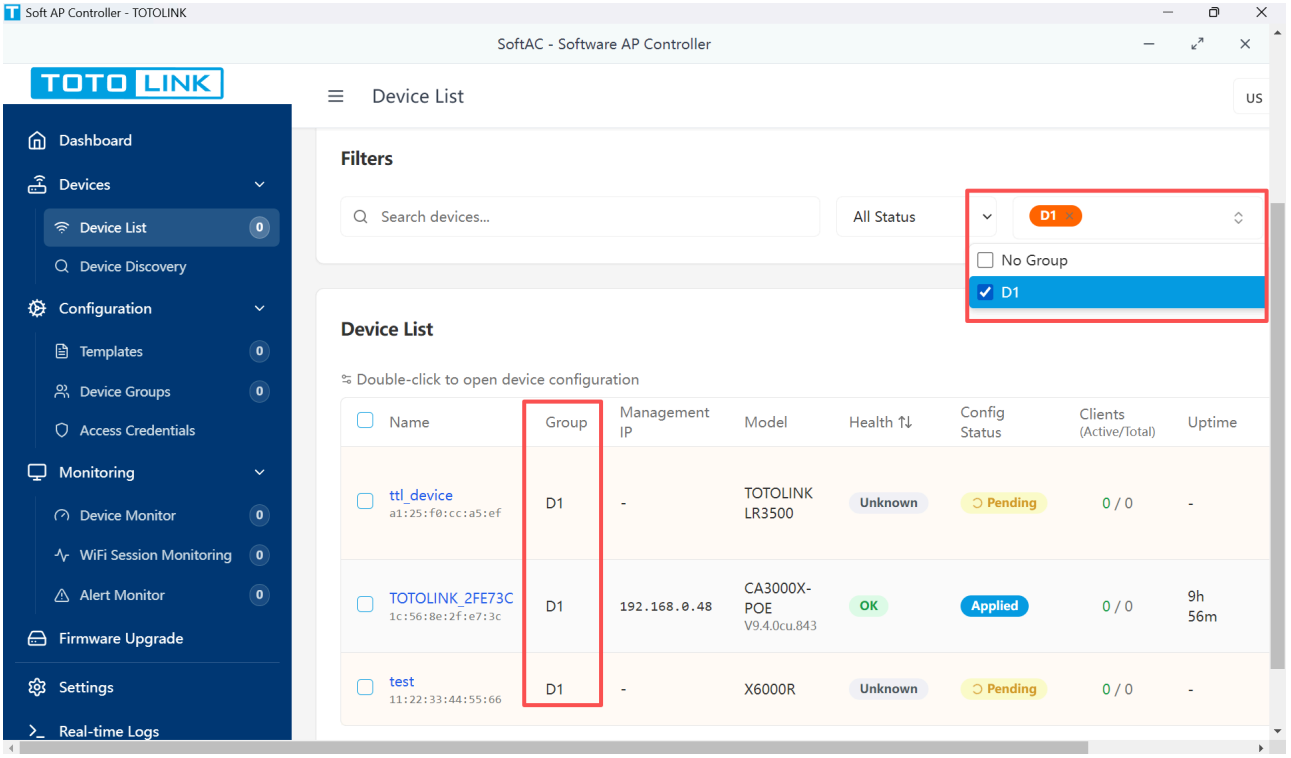
2. **Filter by Keyword**

   Input some keywords to match device names



3. **Filter by Group**

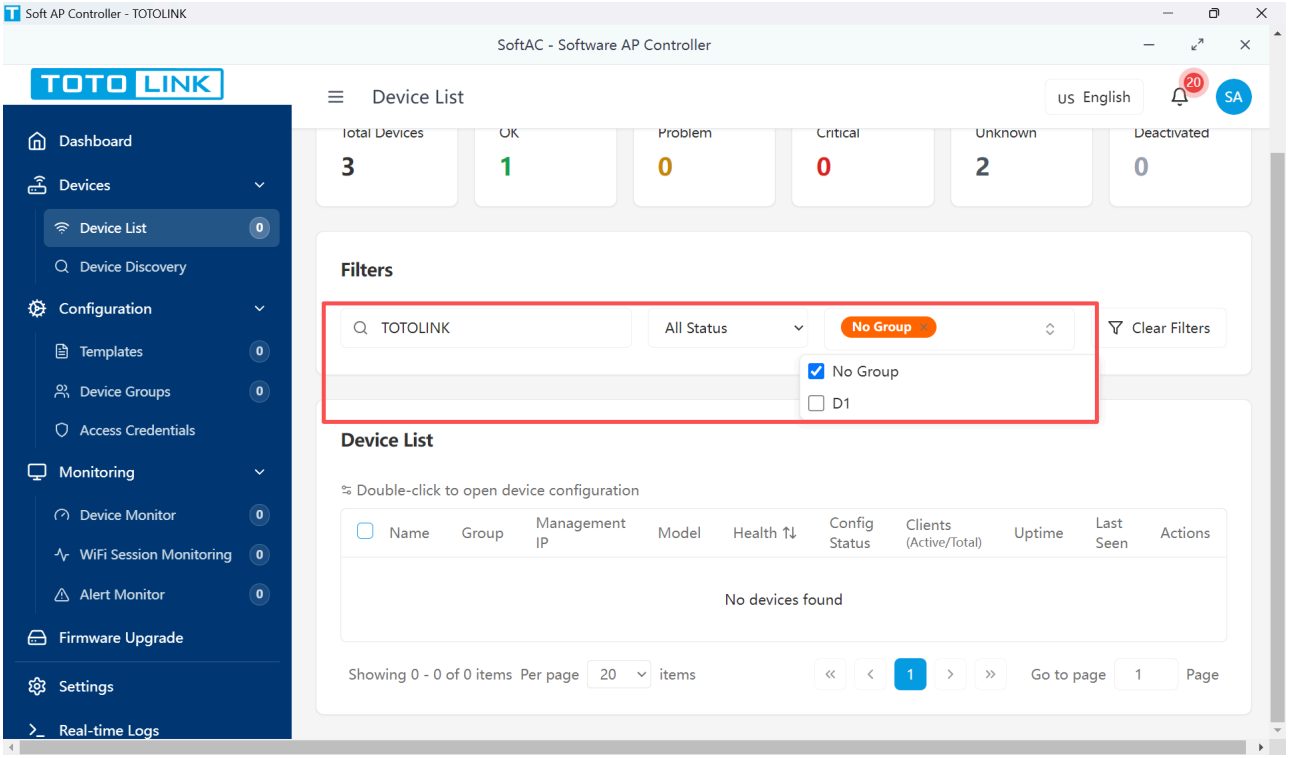
   Filter devices according to their group



4. **Combined Filters**

   Apply multiple filters simultaneously:

   - Search term | Status | Group



Best Practices for Monitoring

> 💡 **Monitoring Tips**:
>
> - Set up a monitoring dashboard on a dedicated display
> - Configure auto-refresh based on network criticality

> - Use filters to focus on problem devices
> - Export monitoring data for reporting

> 📊 **Performance Optimization**:
>
> - Monitor during peak usage hours
> - Identify devices consistently at high utilization
> - Plan upgrades based on historical trends

Troubleshooting with Monitoring

Quick Diagnostics

1. **Identify Problem Devices**
   - Sort by health status
   - Filter for critical/problem states
   - Check last seen timestamps
2. **Analyze Patterns**
   - Multiple devices offline: Check network connectivity
   - High CPU across devices: Review configuration
   - Client connection issues: Verify wireless settings
3. **Take Action**
   - Access device configuration
   - Initiate SSH session for direct access
   - Review device logs
   - Restart device if necessary

[Screenshot: Troubleshooting workflow in monitoring interface]

Important Notes

> ⚠️ **Data Accuracy**: Monitoring data updates based on device reporting intervals (typically 30-60 seconds).

> 🔄 **Auto-Recovery**: Devices automatically attempt reconnection if communication is lost.

> 📝 **Historical Data**: Monitoring history is retained for 30 days for trend analysis.

Related Functions

- 7.1 Device Monitoring
- 7.3 Alert Management
- 14.1 Connection Issues

Summary

Device Management in TOTOLINK SoftAC provides comprehensive tools for managing your network device efficiently. From adding individual devices to performing bulk operations and real-time monitoring, these features ensure your network operates optimally.

Key Takeaways

- **Centralized Management**: Control all devices from a single interface
- **Flexible Configuration**: Apply templates or custom settings as needed
- **Efficient Operations**: Use batch tools for large-scale management
- **Proactive Monitoring**: Identify and resolve issues before they impact users
- **Comprehensive Tracking**: Maintain complete visibility of device status and performance

Next Steps

- Continue to 5. Template Management to learn about configuration templates
- Explore 6. Device Groups for organizing devices logically
- Review 7. Network Monitoring for advanced monitoring features

Part 5. Template Management

5.1 Understanding Configuration Templates

Overview

Configuration templates in TOTOLINK SoftAC are reusable configuration presets that streamline device management. Templates allow you to define standard configurations once and apply them to multiple devices, ensuring consistency across your network infrastructure.

Use Cases

- **Standardized Deployments**: Apply uniform settings across multiple access points
- **Quick Configuration**: Set up new devices rapidly using pre-defined templates
- **Environment-Specific Settings**: Create templates for different locations (office, warehouse, guest areas)
- **Compliance Management**: Ensure all devices meet security and network policies

Template Components

Templates consist of three main elements:

Component	Description	Example
Configuration Data	The actual network settings	WiFi parameters, IP addresses, security settings

Component	Description	Example
Variables	Placeholders for device-specific values	Device name, location identifier, IP address
Metadata	Template information and settings	Name, type, version, tags

Template Types

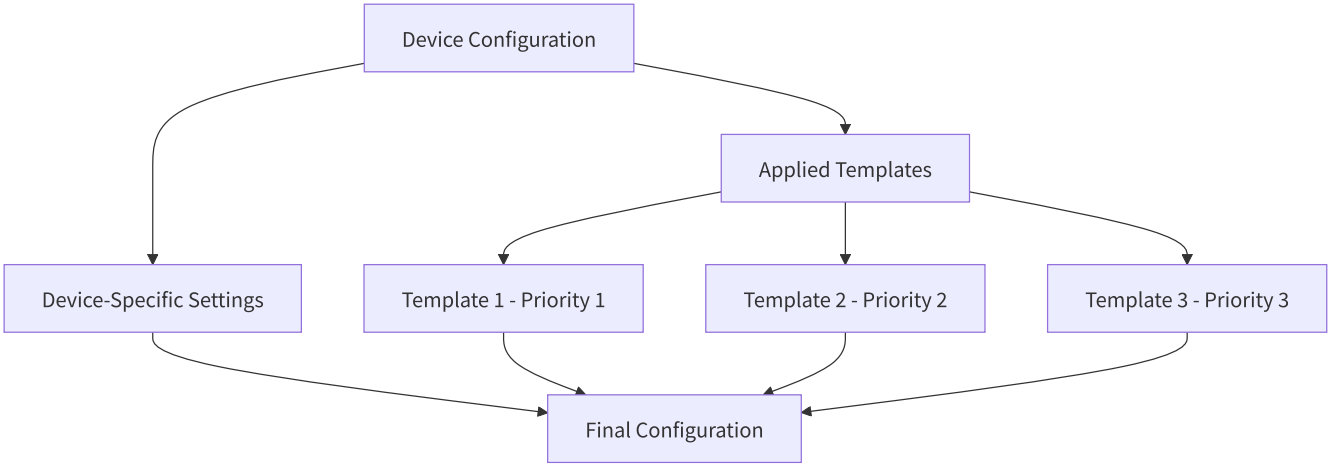
TOTOLINK SoftAC supports various template types for different configuration aspects:

Type	Purpose	Configurable Settings
Generic	Full configuration access	All device settings
General	Basic device settings	Timezone, hostname, system settings
Interface	Network interface configuration	LAN/WAN settings, VLANs
Radios	Wireless radio settings	Channels, power, country codes
DNS Configuration	DNS server settings	Primary/secondary DNS servers
NTP Settings	Time synchronization	NTP servers, time zones
Firewall	Security rules	Access control, port forwarding

> 📝 **Note**: Generic templates provide the most flexibility, allowing configuration of all device aspects.

Template Hierarchy

When multiple templates are applied to a device, they follow a priority order:



> 💡 **Tip**: Templates with higher priority (lower numbers) override settings from lower priority templates.

5.2 Creating Templates

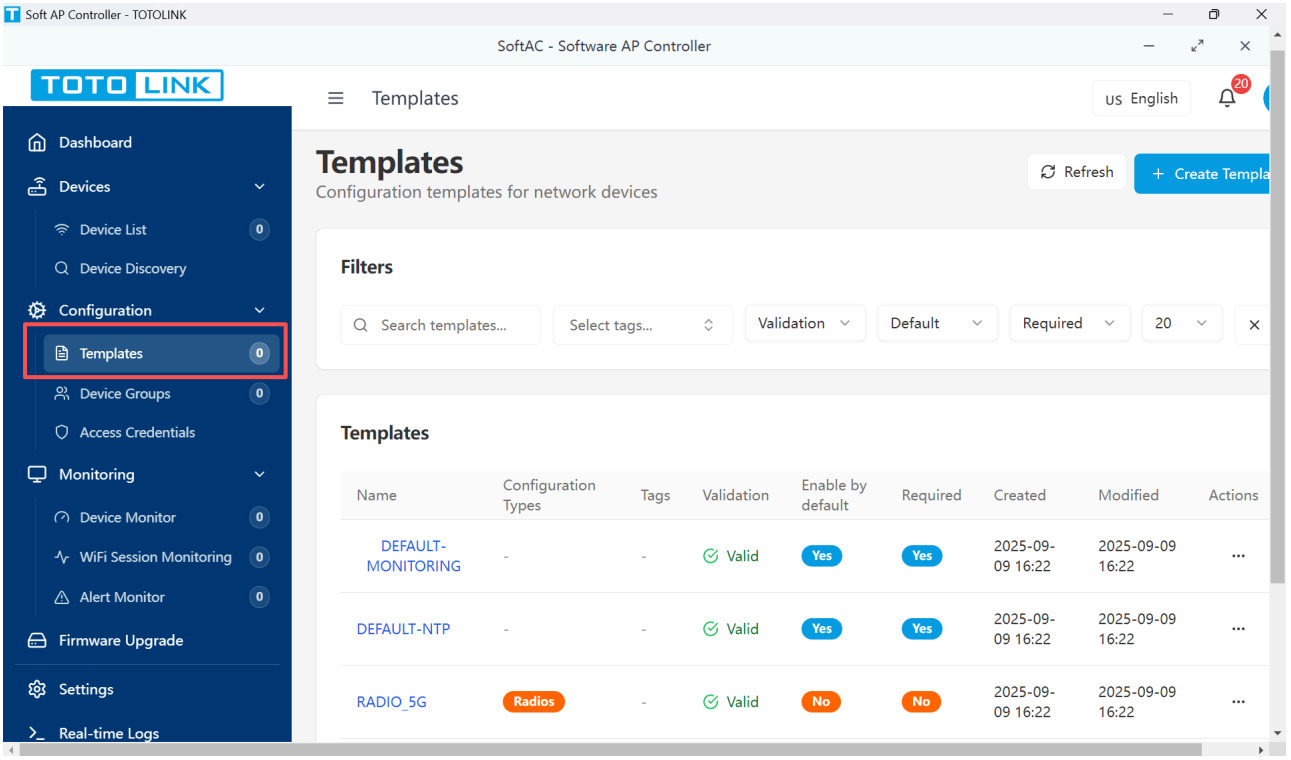
Prerequisites

Before creating a template, ensure you have:

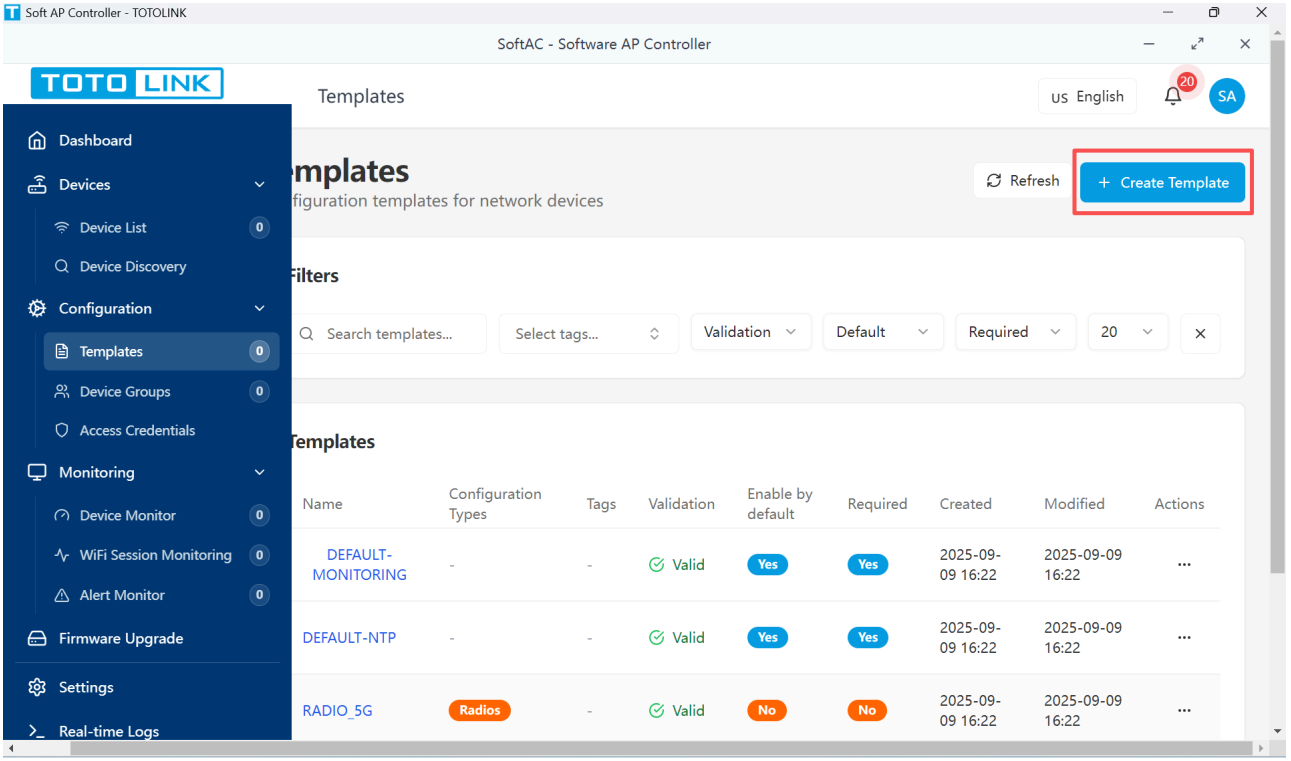
- Administrator or operator privileges
- Clear understanding of desired configuration
- Knowledge of target device capabilities

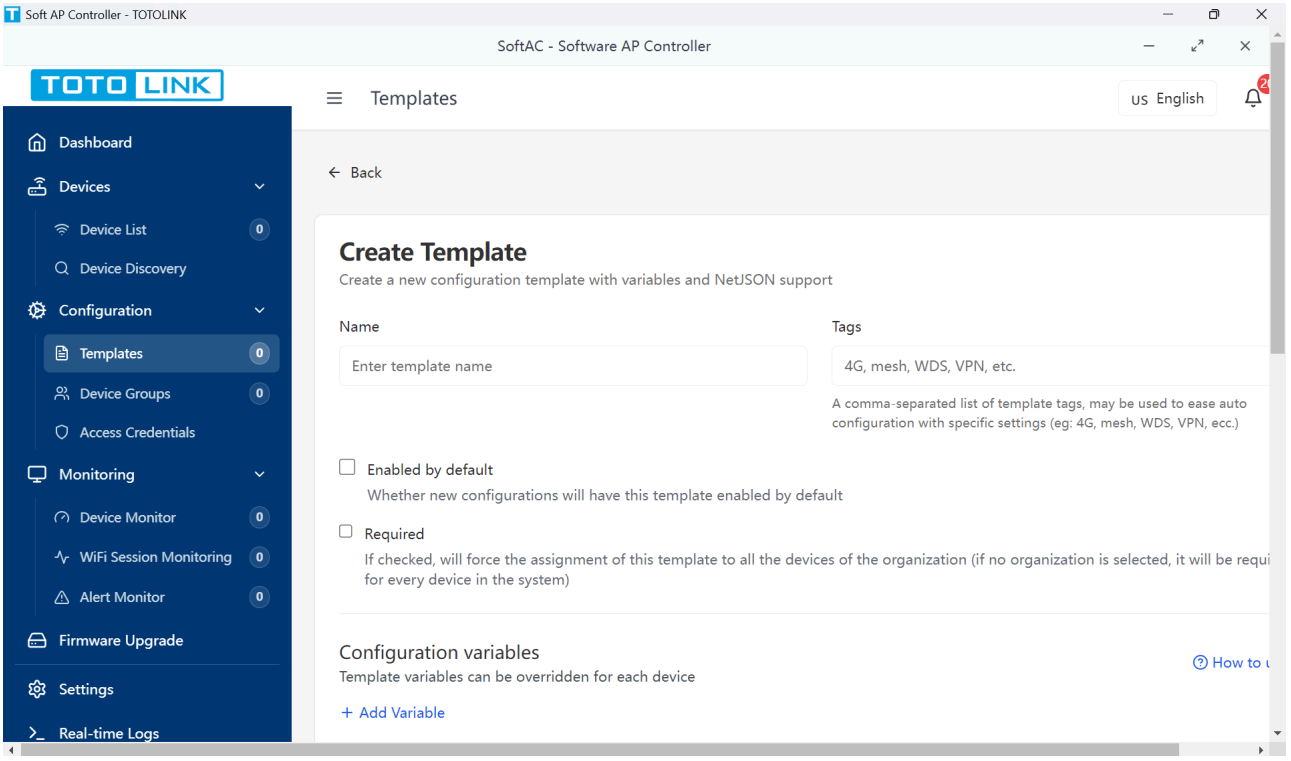
Step-by-Step Creation Process

1. **Access Template Management**
   Navigate to the Templates section from the main menu.



2. **Initiate Template Creation**
   Click the "Create Template" button in the upper right corner.

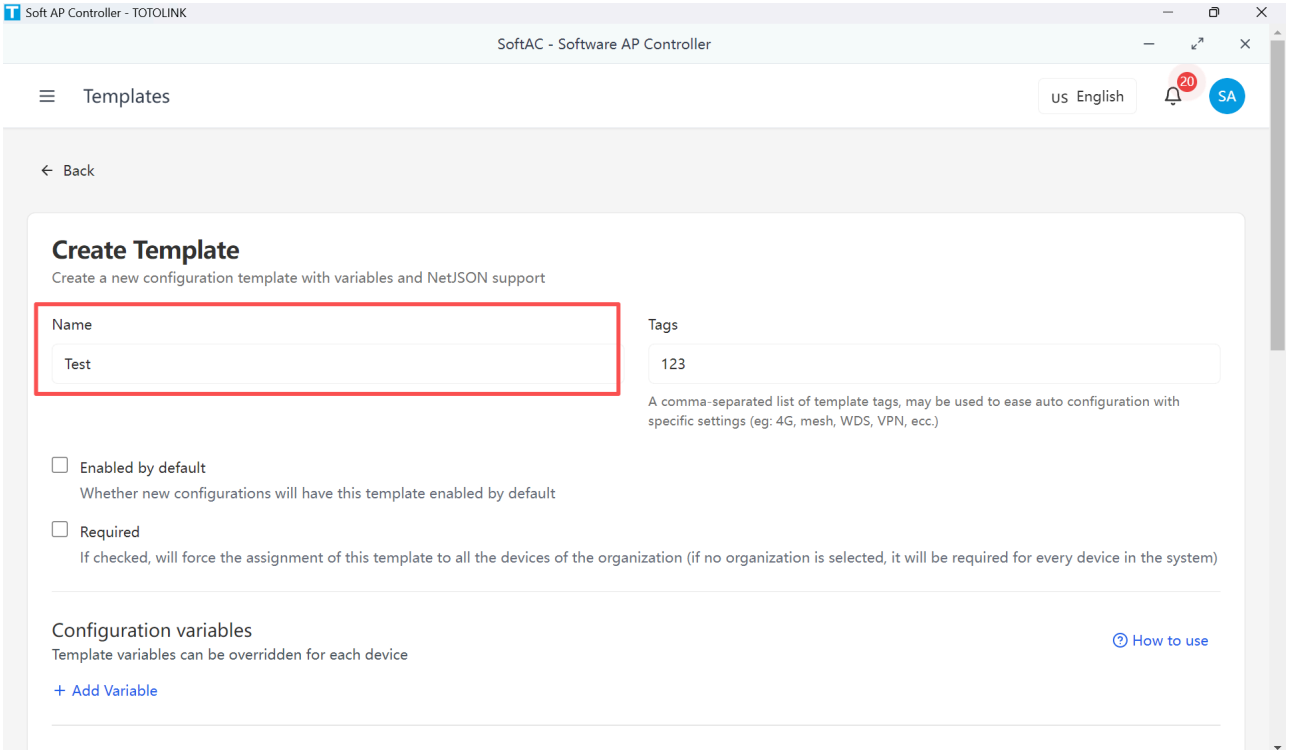


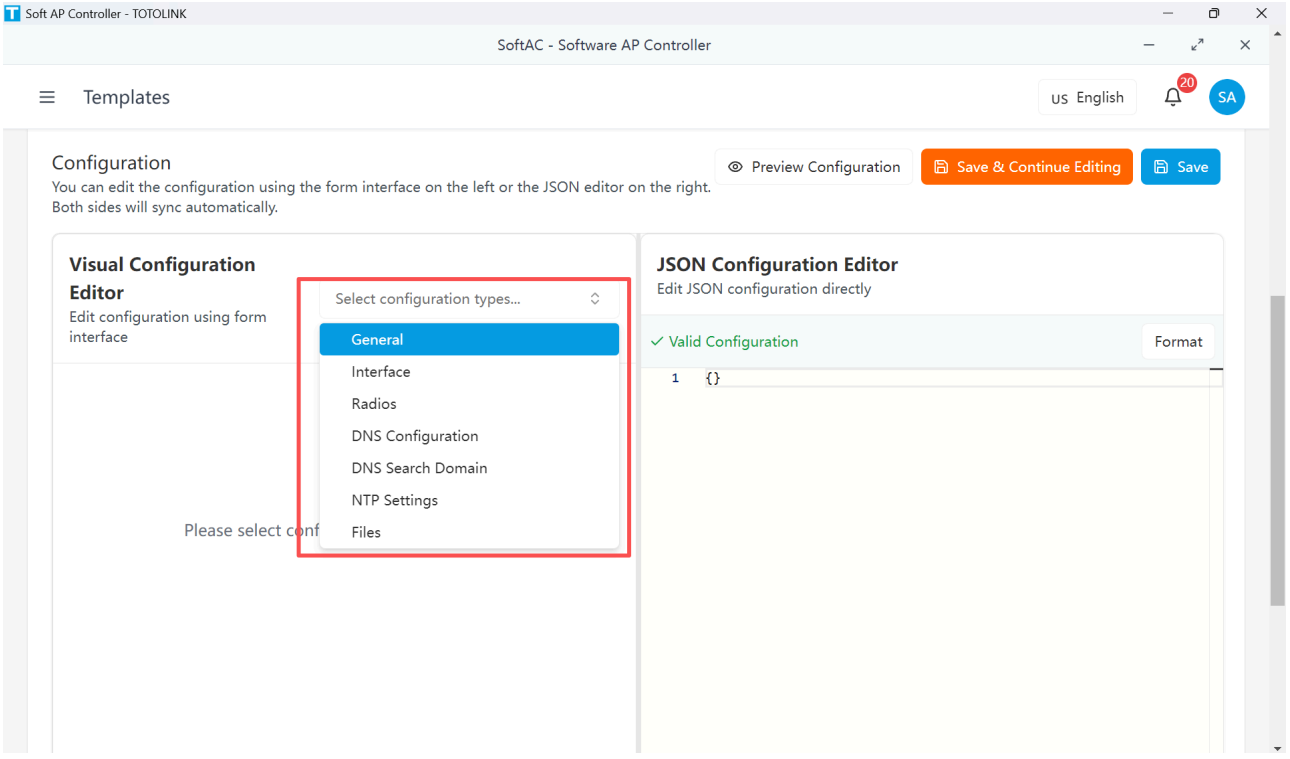


3. **Configure Basic Information**

   Fill in the template details:

Field	Description	Required
Template Name	Descriptive name for identification	Yes
Configuration Type	Configuration scope (Generic, Interface, etc.)	Yes
Tags	Labels for organization	No





4. **Define Configuration Settings**

   Use the configuration editor to specify settings:

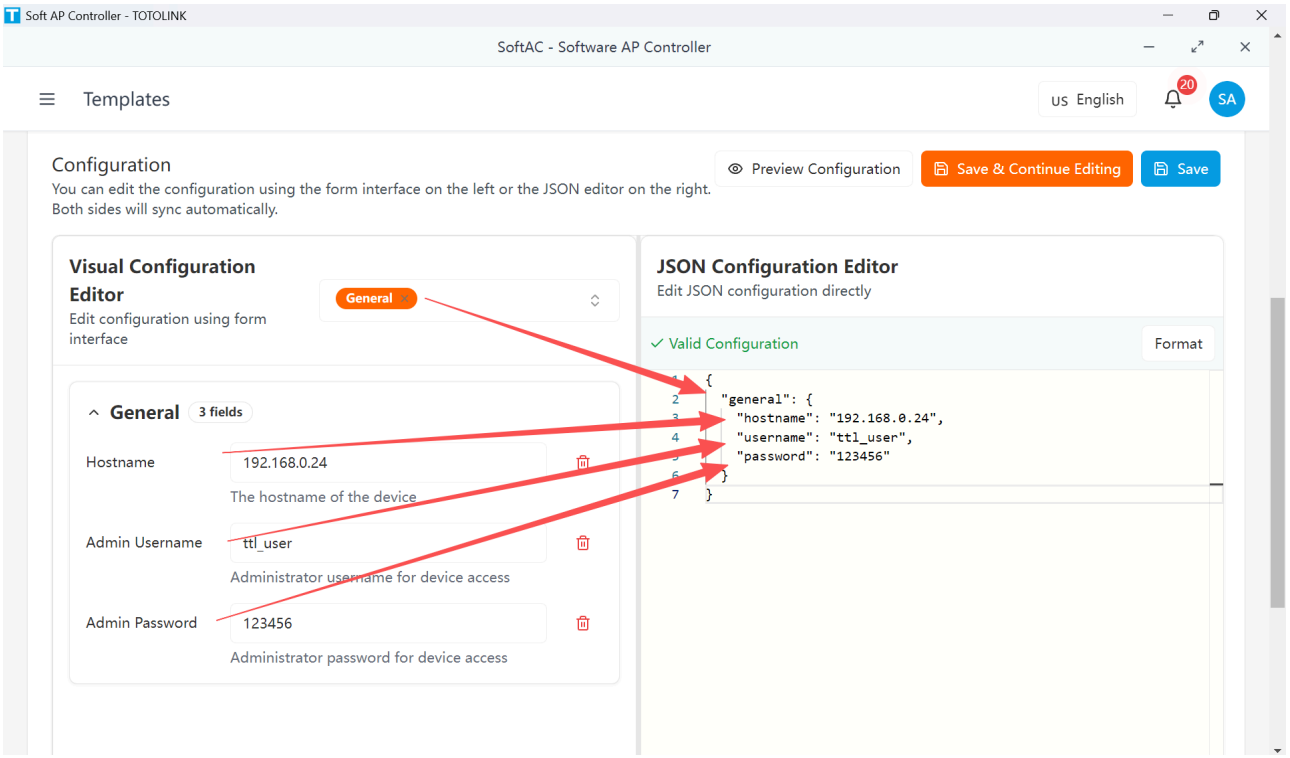
   Visual Editor Mode (Recommended for beginners):

   - Navigate through configuration categories
   - Fill in forms for each setting
   - Use tooltips for guidance

   JSON Editor Mode (For advanced users):

   - Direct JSON configuration input
   - Syntax highlighting and validation

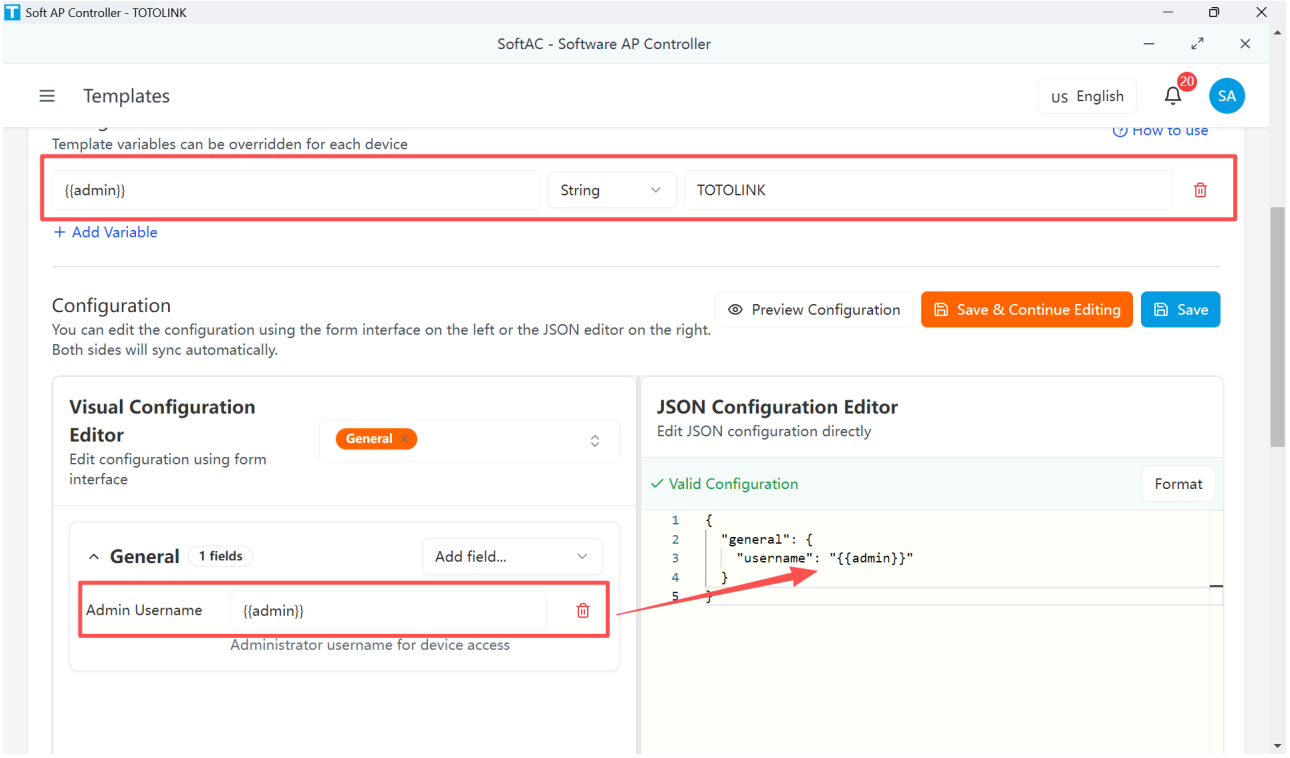
- Import/export capabilities

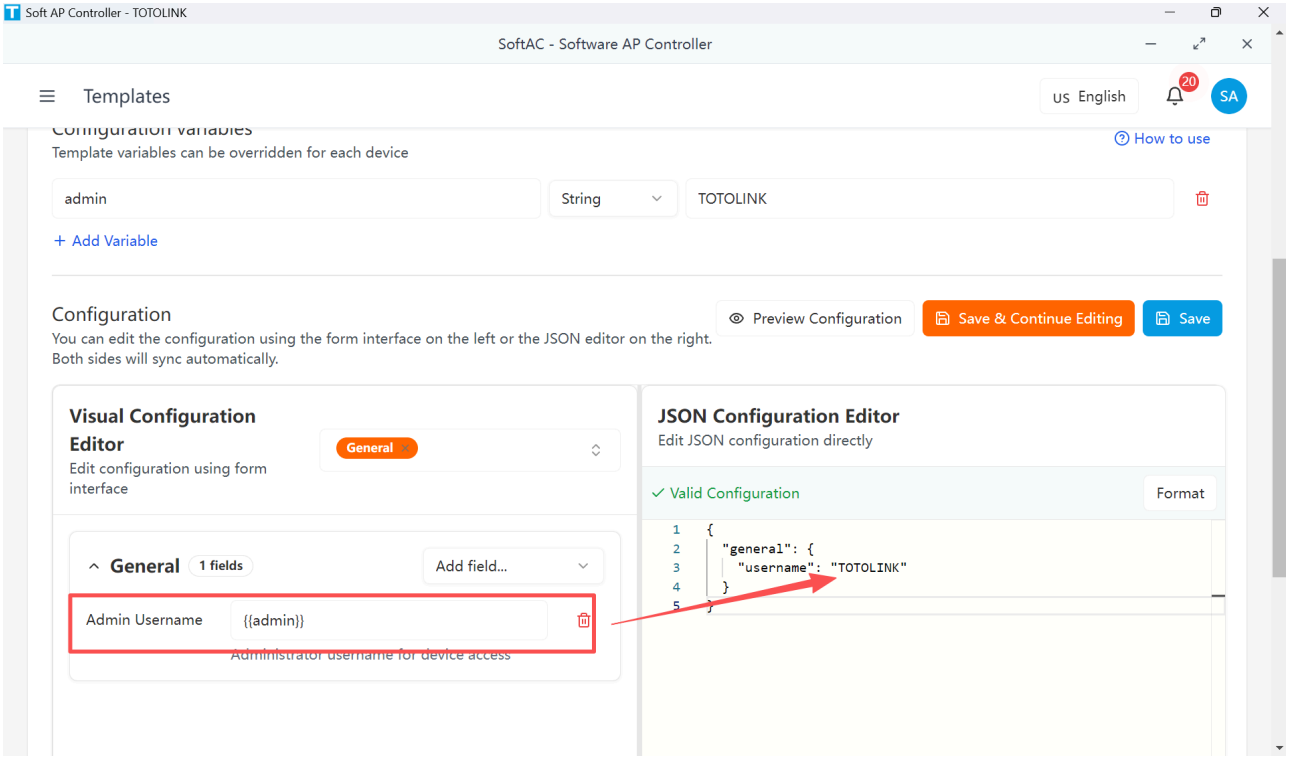


5. **Add Template Variables** (Optional)

   Define placeholders for device-specific values:

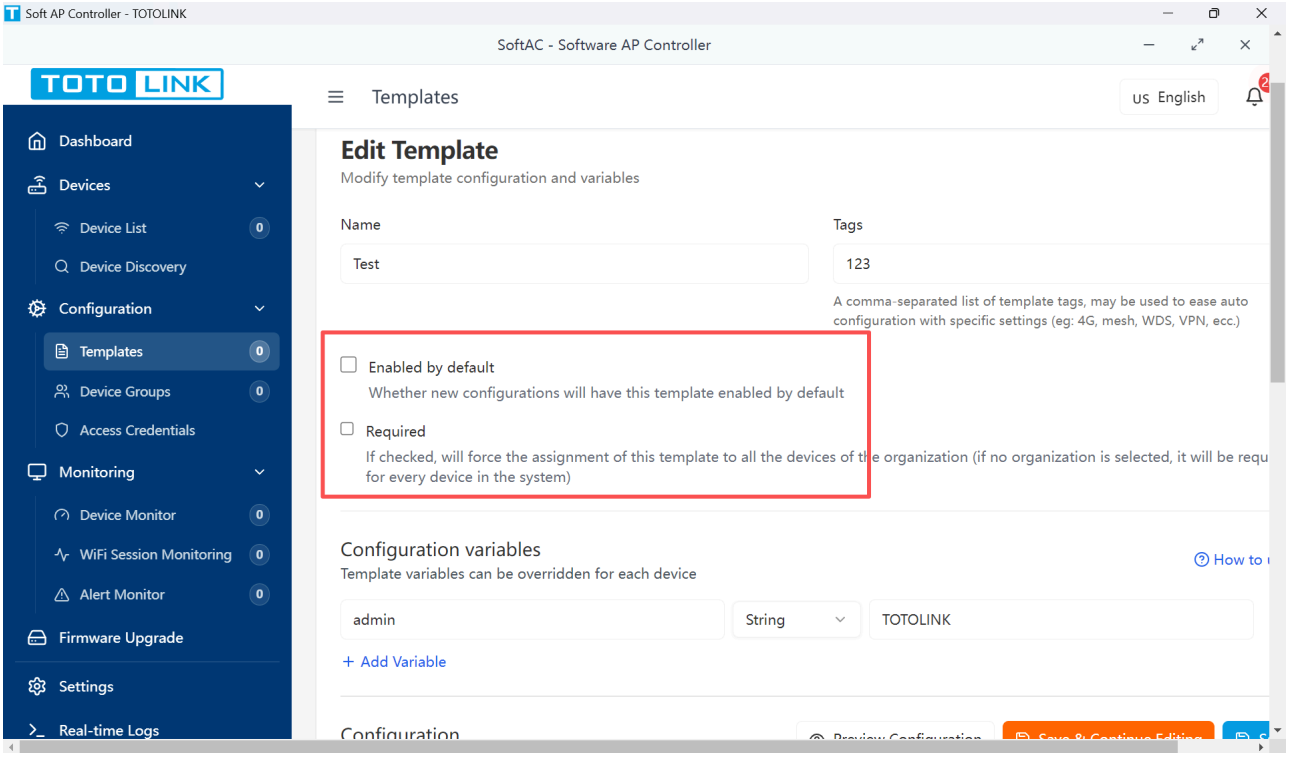
```
Variable Name: device_location
Variable Key: {{location}}
Type: String
Default Value: Main Office
Required: Yes
```





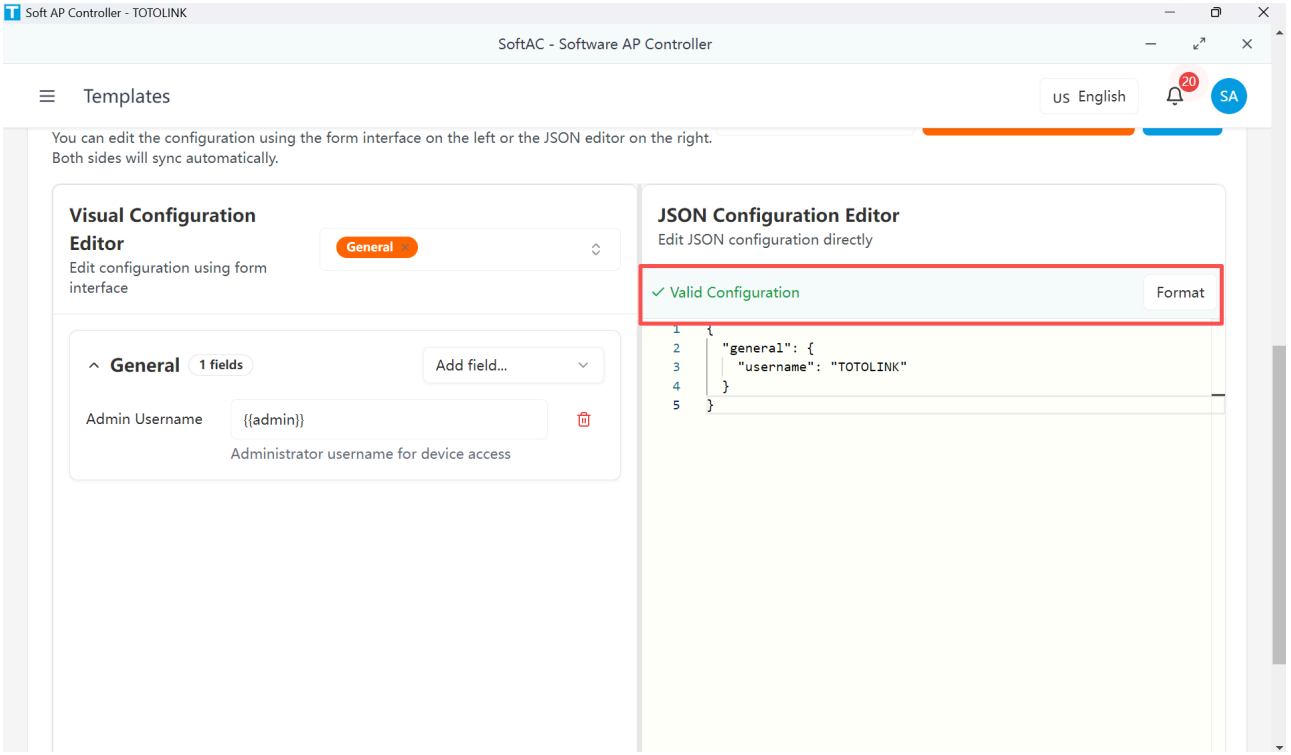
6. **Configure Template Options**

Option	Description	Default
Required	Template must be applied to devices	No
Enabled by Default	Automatically apply to new devices	No



7. **Validate Configuration**

Automatically check the validation of template configuration



8. **Save Template**

   Click "Save" to create the template.

   > ✅ **Success**: Template will appear in the templates list immediately.

Configuration Examples

WiFi Template Example

```
{
  "interfaces": [
    {
      "name": "wlan0",
      "type": "wireless",
      "wireless": {
        "mode": "access_point",
        "ssid": "{{wifi_name}}",
        "channel": "auto",
        "encryption": {
          "protocol": "wpa2_personal",
          "key": "{{wifi_password}}"
        }
      }
    }
  ]
}
```

Network Interface Template Example

```
{
  "interfaces": [
    {
      "name": "lan",
      "type": "bridge",
      "addresses": [
        {
          "proto": "static",
          "address": "{{lan_ip}}",
          "mask": 24
        }
      ]
    }
  ]
}
```

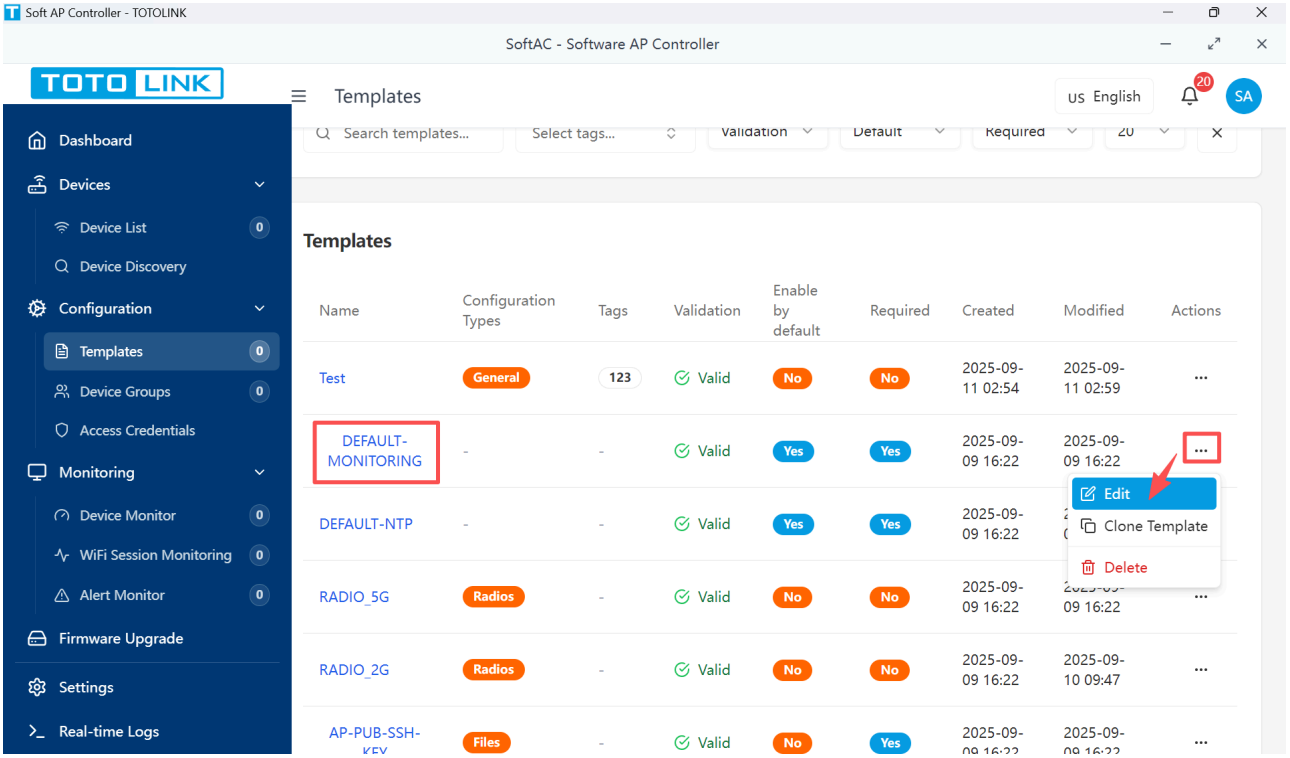
Best Practices

> 💡 **Best Practices**:
>
> - Use descriptive template names indicating purpose and environment
> - Document template purpose in the description field
> - Test templates on a single device before mass deployment
> - Version your templates by including version numbers in names
> - Use tags for easy filtering and organization

5.3 Editing Templates

Accessing Template Editor

1. **Navigate to Templates List**
   Go to Templates section from the main menu.
2. **Select Template to Edit**
   Click on the template name or use the action menu (⋮) and select "Edit".



Change Tracking

> 📝 **Note**: All template modifications are logged for audit purposes:
>
> - Timestamp of change
> - User who made the change
> - Description of modifications
> - Affected devices count

5.4 Applying Templates to Devices

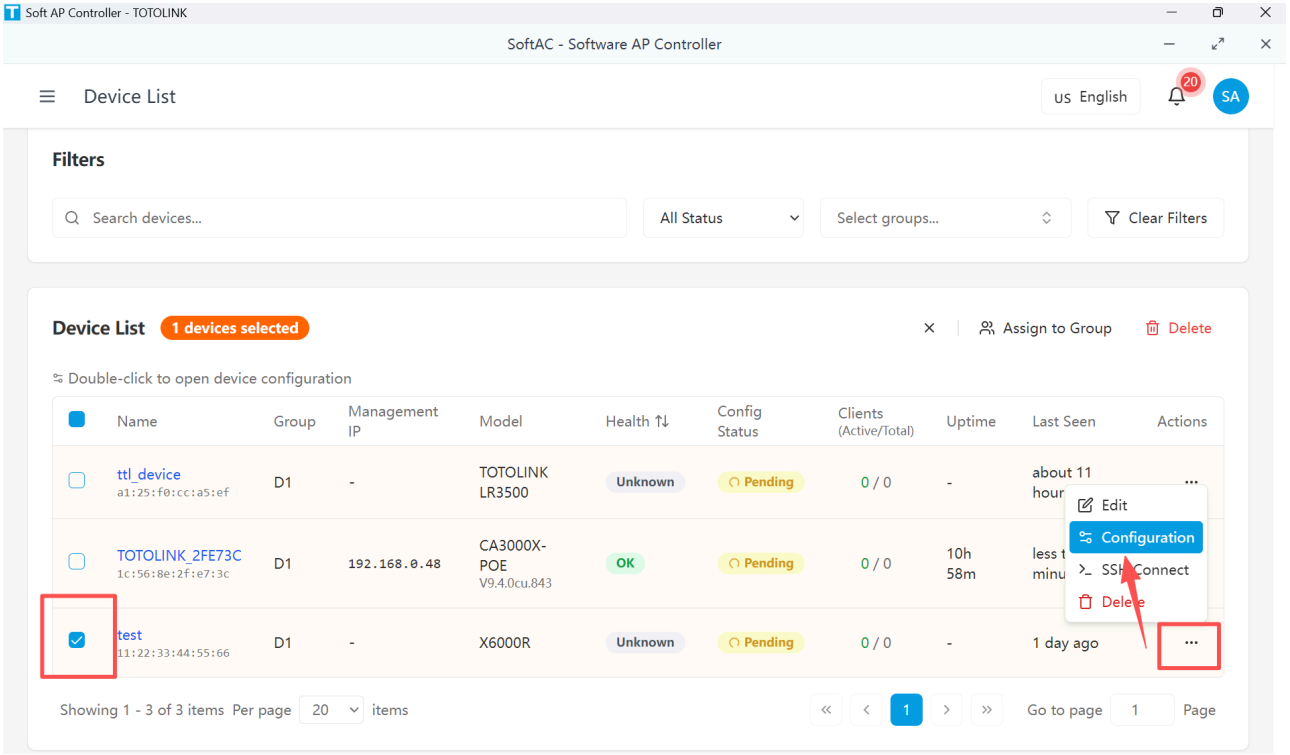
Application Methods

TOTOLINK SoftAC provides multiple ways to apply templates:

Method	Use Case	Devices Affected
Individual Application	Single device configuration	One
Group Application	Department or location-wide settings	All group members

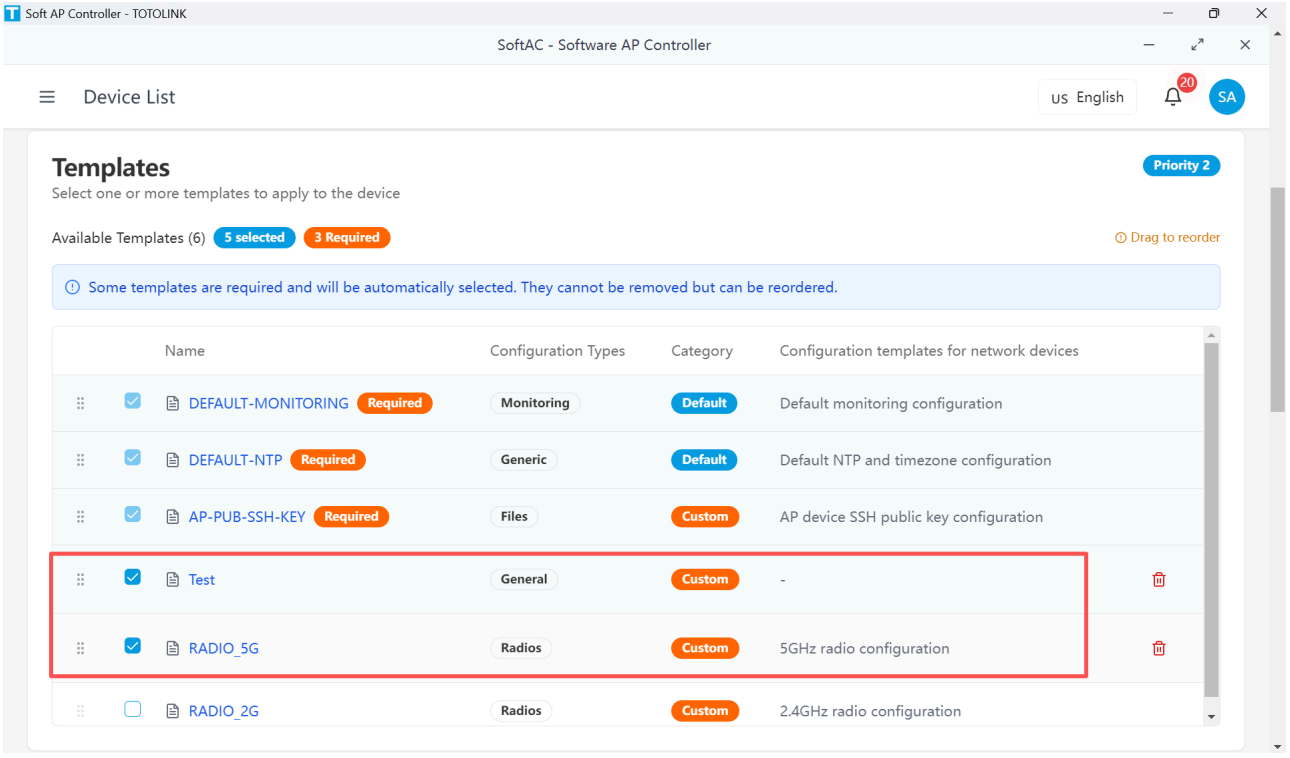
Individual Device Application

1. **Navigate to Device Configuration**
   Go to Devices List→ Select device → Configuration tab



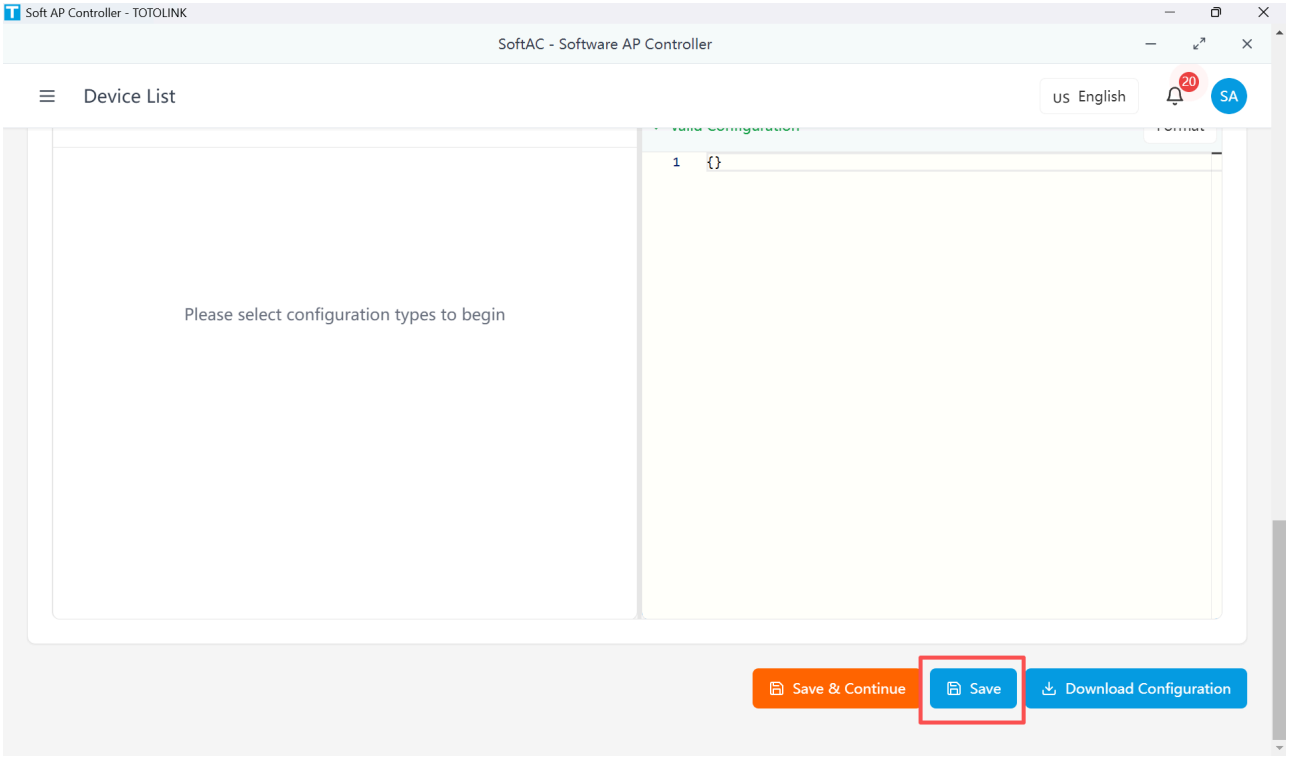
2. **Select Template**

   Select the templates you want in "Apply Template" tab.



3. **Save Configuration**

   Click "Save" button:

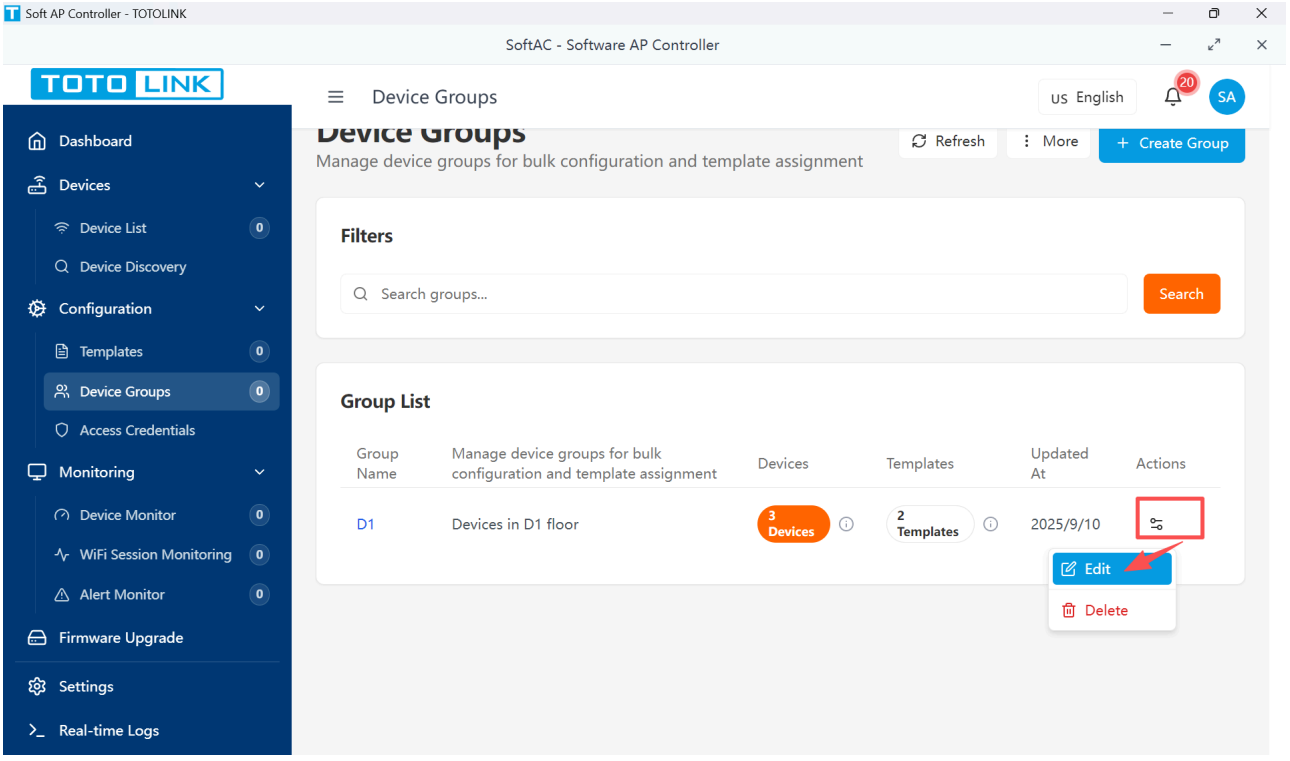


Group-Based Application

1. **Access Device Group**

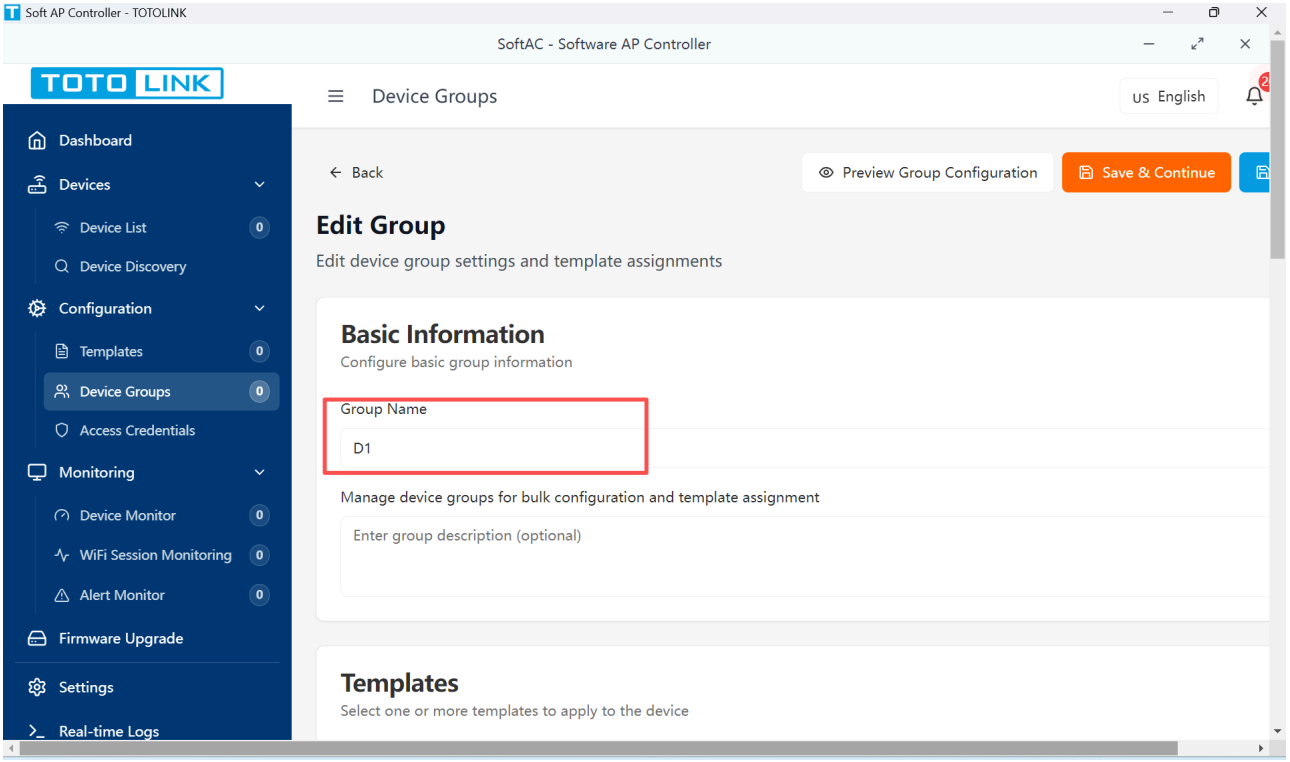
   Navigate to Device Groups → Group List

   - Select the group you want to add templates
   - Click "Edit"



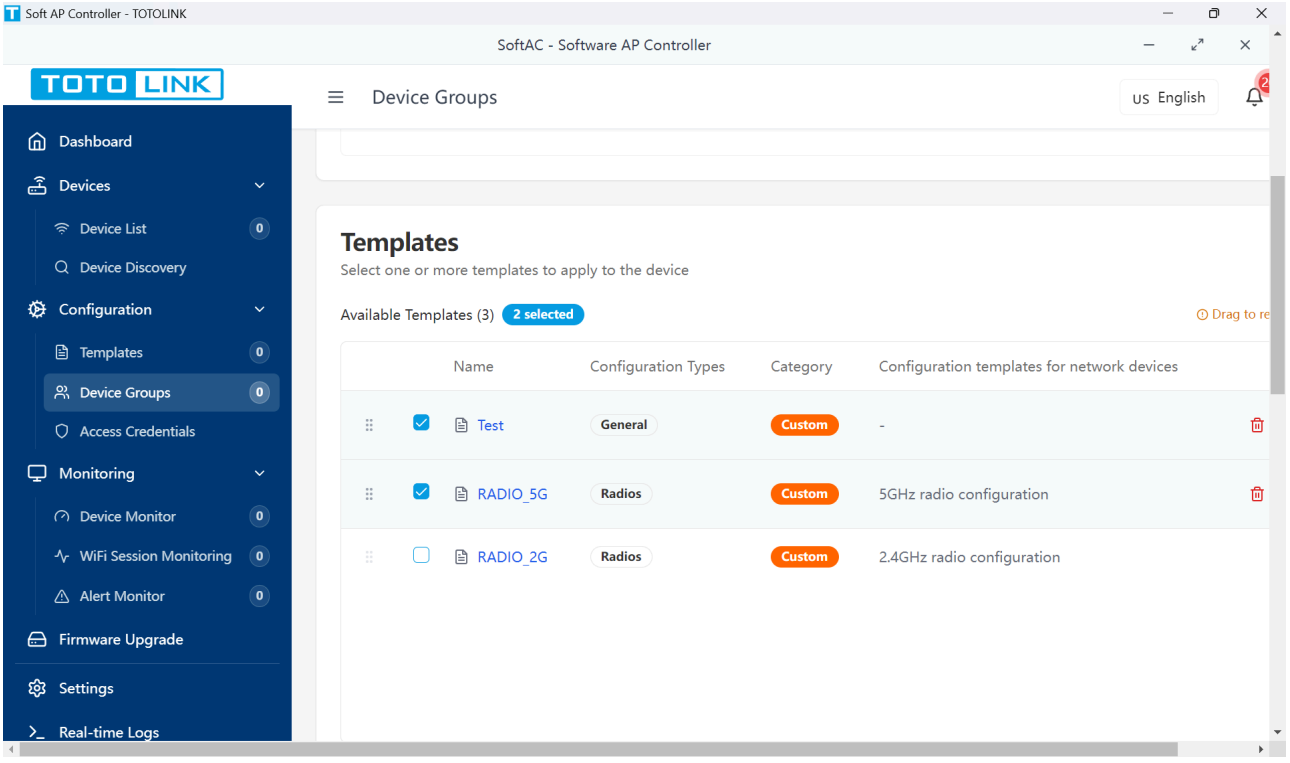
2. **Input Group Name**

   Input the group name in "Basic Information" tab



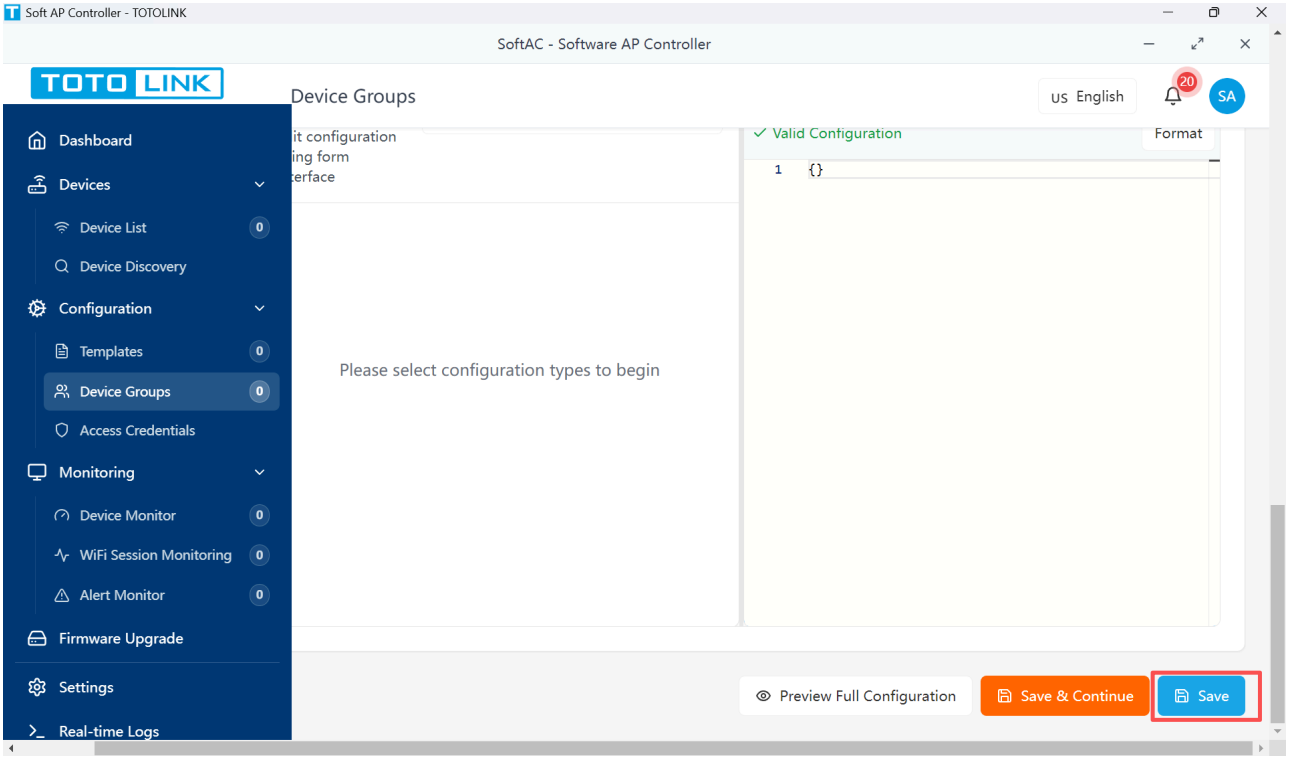
3. **Select Templates**

   Select the templates you want in "Templates" tab.



4. **Apply to Group Members**

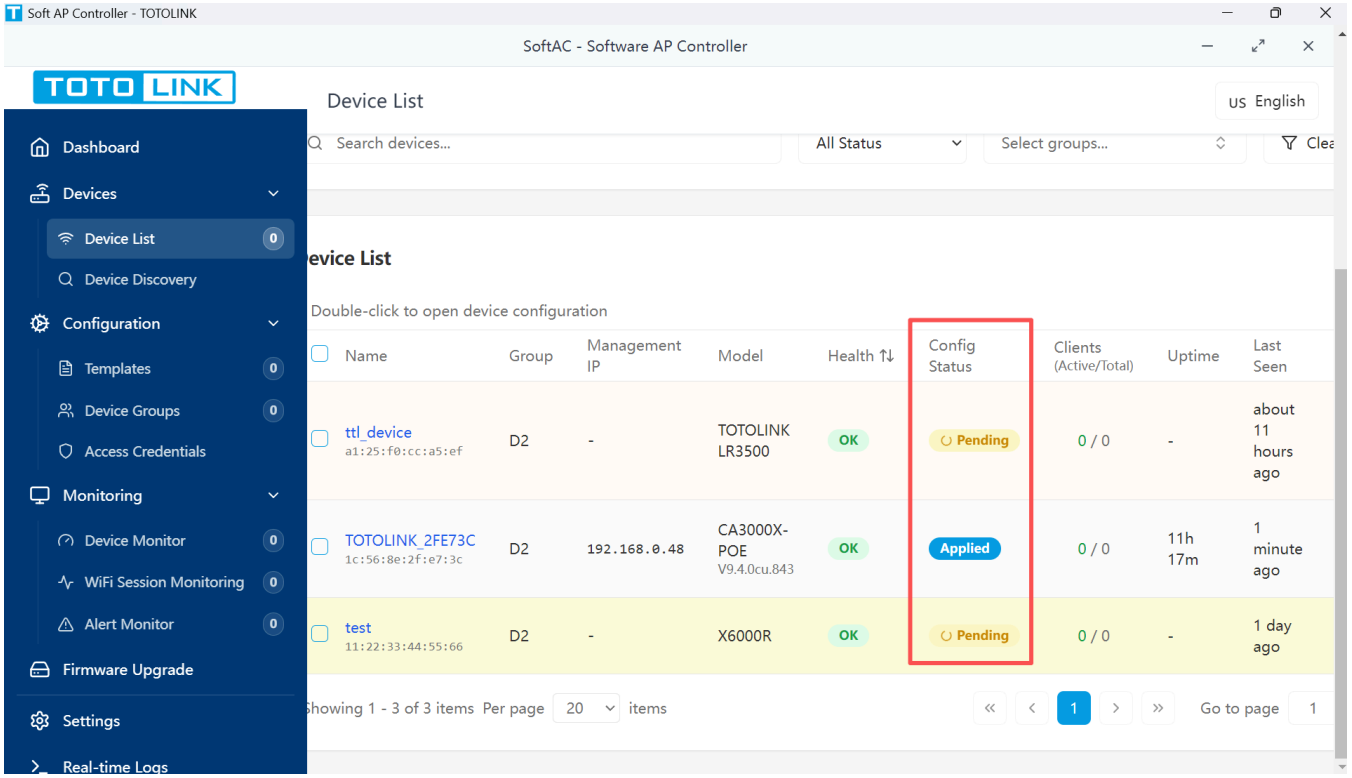
   Click "Save" to push configuration to all devices.



Application Monitoring

Track template application status:

Status	Description	Action Required
Applied	Successfully configured	None
Pending	Waiting for device connection	Wait or retry
Failed	Application error	Check logs and retry



Troubleshooting Application Issues

Common Issues and Solutions:

Problem: Template variables not replaced

- Verify variable names match exactly
- Check variable values are provided
- Ensure proper syntax: {{variable_name}}

Problem: Configuration conflicts

- Review template priority order
- Check device-specific overrides
- Use conflict resolution tool

Problem: Device not accepting configuration

- Verify device firmware compatibility
- Check network connectivity
- Review device logs for errors

5.5 Template Version Management

Version Control System

TOTOLINK SoftAC automatically tracks template versions to ensure configuration consistency and enable rollback capabilities.

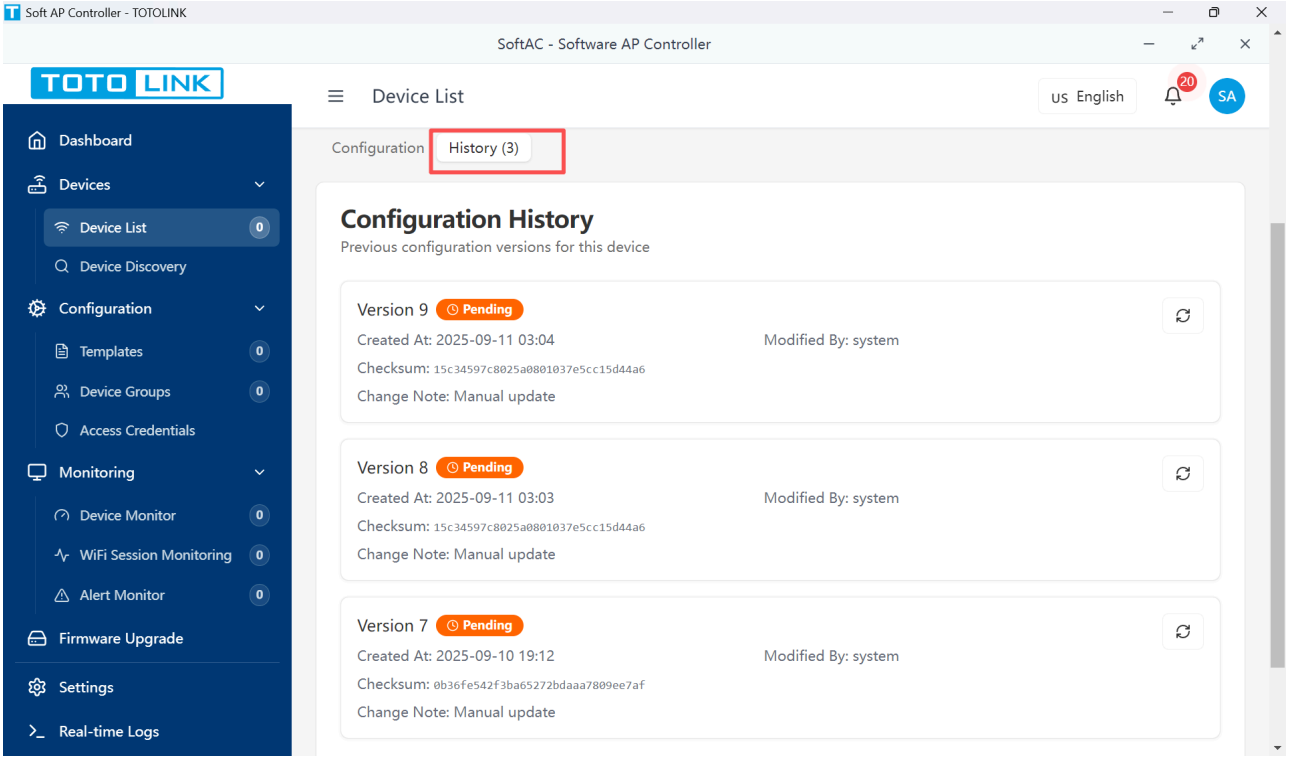
Version Tracking

Each template modification creates a new version with:

Information	Description	Example
Version Number	Auto-incremented identifier	v1, v2, v3
Timestamp	Creation date and time	2024-01-15 14:30:00
Author	User who made changes	admin@company.com
Change Summary	Description of modifications	Added guest network configuration
Configuration Hash	Unique identifier for configuration	abc123def456...

Viewing Version History

1. **Access Device Configuration**
   Access configuration in Device List.
2. **Configuration History**
   Select "History".

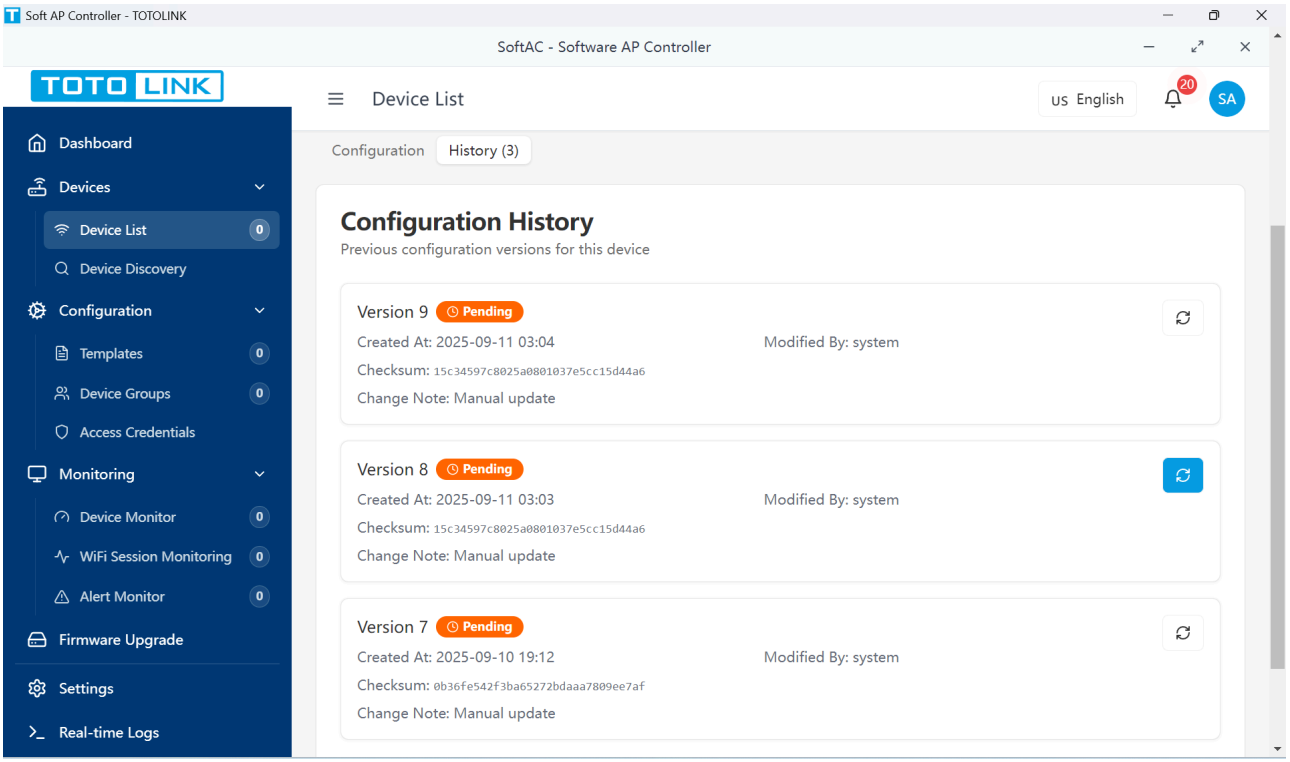


3. **Review Version List**
   View all template versions.

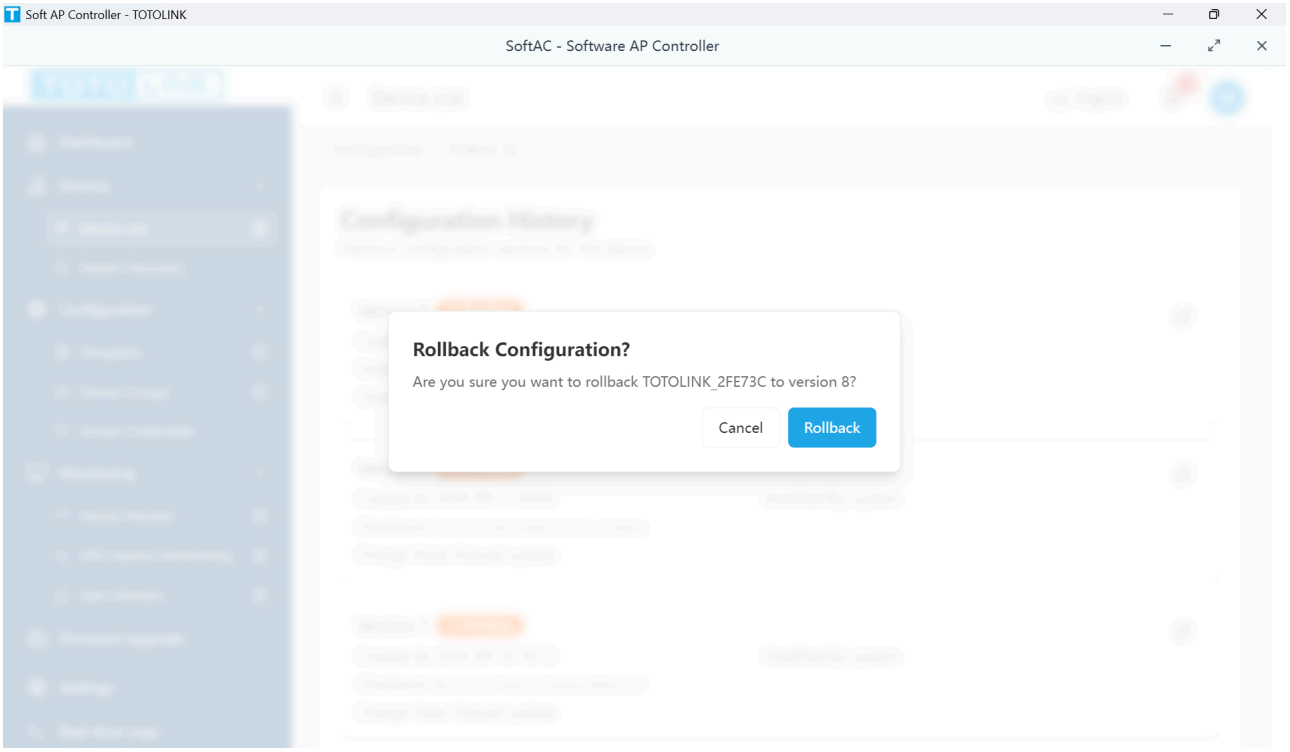
Version Operations

Rollback to Previous Version

1. **Select Target Version**
   Click the return arrow logo at the top left corner of version tab.



2. **Confirm Rollback**
   Click "Rollback".



> 📝 **Note**: Rollback creates a new version rather than deleting history.

Best Practices for Version Management

> 💡 **Best Practices**:
>
> - Document changes in version description
> - Test new versions on single device first
> - Maintain version naming convention (e.g., v1.0, v1.1, v2.0)
> - Archive old unused versions periodically
> - Review version history before major updates

Version Deployment Strategies

Strategy	Description	Use Case
Immediate	Deploy to all devices instantly	Critical security updates
Phased	Gradual rollout to device groups	Major configuration changes
Scheduled	Deploy at specific time	Maintenance windows
Manual	Require manual approval per device	High-risk changes

Version Audit Trail

All version operations are logged:

Action	Logged Information	Retention
Create	User, timestamp, configuration	Permanent
Modify	Changes, reason, affected devices	Permanent
Rollback	Source/target versions, user	Permanent
Delete	Version details, authorization	Permanent

[Screenshot: Audit log viewer]

Related Features

- 4.3 Device Configuration
- 6.2 Creating Groups
- 6.4 Group Configuration
- 11.1 Basic Settings

Next Steps

After mastering template management:

1. Create your first template for common device configurations
2. Apply templates to test devices
3. Set up template versioning policies
4. Configure group-based template deployment

> 🚀 **Quick Start**: Begin with a simple WiFi configuration template to familiarize yourself with the template system before creating complex configurations.

Part 6. Device Groups

6.1 Group Concept

Overview

Device Groups in TOTOLINK SoftAC enable you to manage multiple access points as a single unit. Instead of configuring each device individually, you can apply settings, templates, and configurations to an entire group simultaneously, significantly reducing management time and ensuring consistency across your network.

Use Cases

- **Location-based Management**: Group all devices on the same floor or building for unified management
- **Function-based Organization**: Separate guest network APs from corporate network APs
- **Department Segmentation**: Organize devices by department for targeted configuration
- **Maintenance Scheduling**: Group devices that require the same maintenance window

Key Benefits

Benefit	Description
Time Efficiency	Configure multiple devices with a single action
Consistency	Ensure uniform settings across similar devices
Simplified Management	View and monitor grouped devices together
Template Application	Apply configuration templates to entire groups
Batch Operations	Perform firmware updates and restarts on multiple devices

> 💡 **Best Practice**: Create groups based on your organization's structure or network topology for easier management and troubleshooting.

6.2 Creating Groups

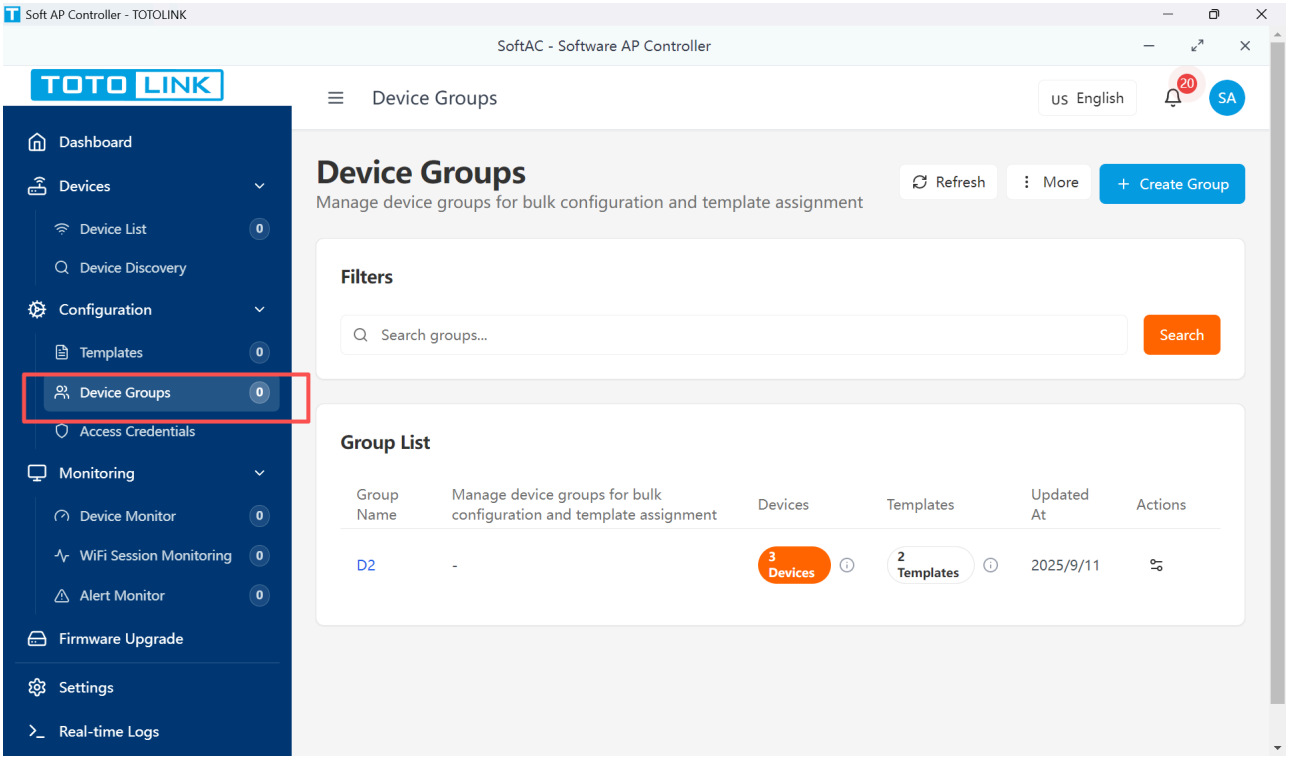
Prerequisites

Before creating a device group, ensure you have:

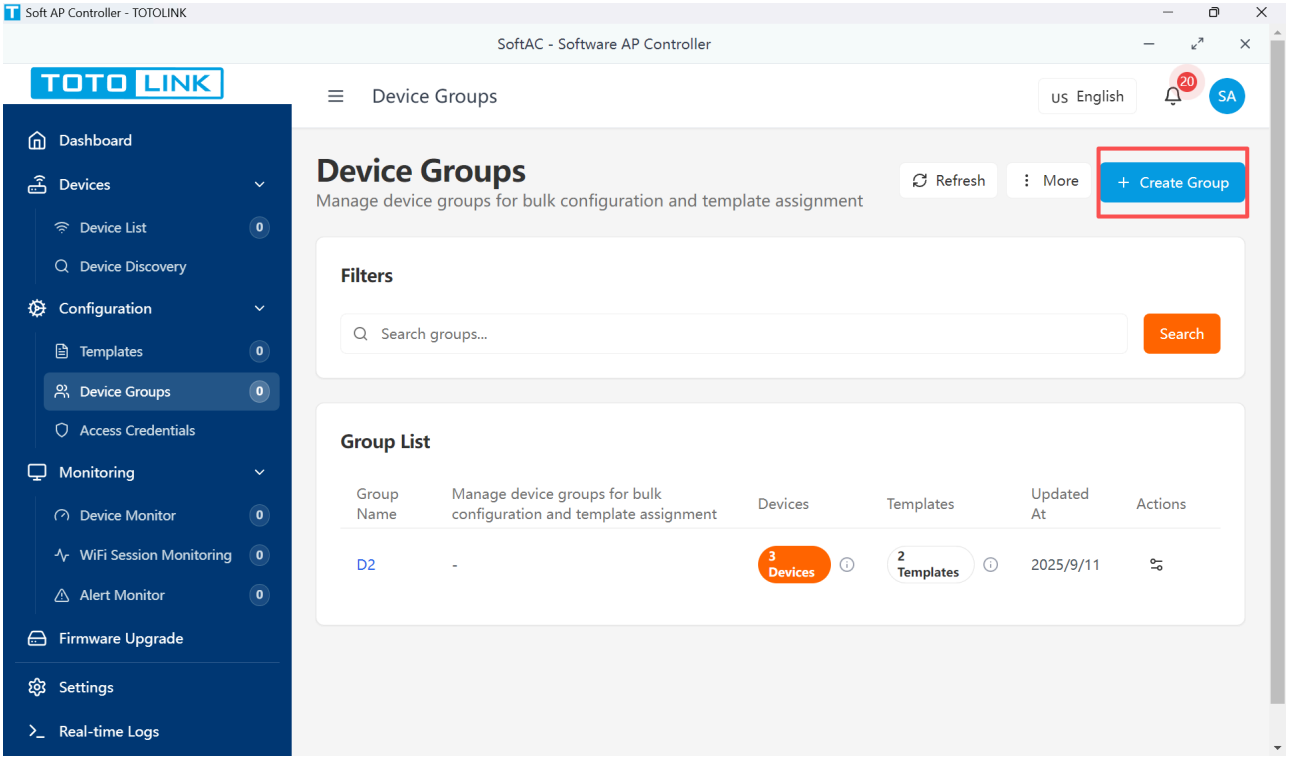
- Administrator access to the system
- At least one device added to the system (optional but recommended)
- Configuration templates prepared (optional)

Step-by-Step Instructions

1. **Navigate to Device Groups**
   Click "Device Groups" in the left navigation menu.

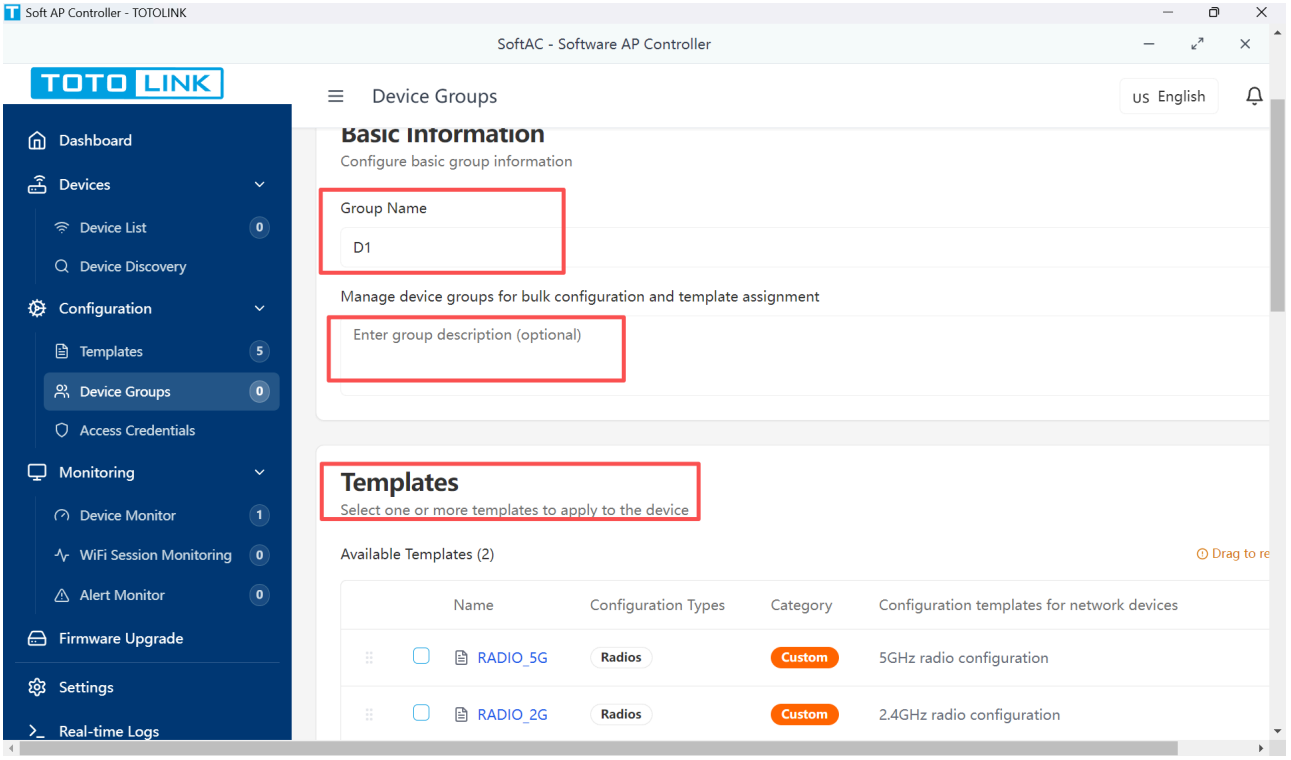


2. **Start Group Creation**
   Click the blue "+ Create Group" button in the top-right corner of the Device Groups page.



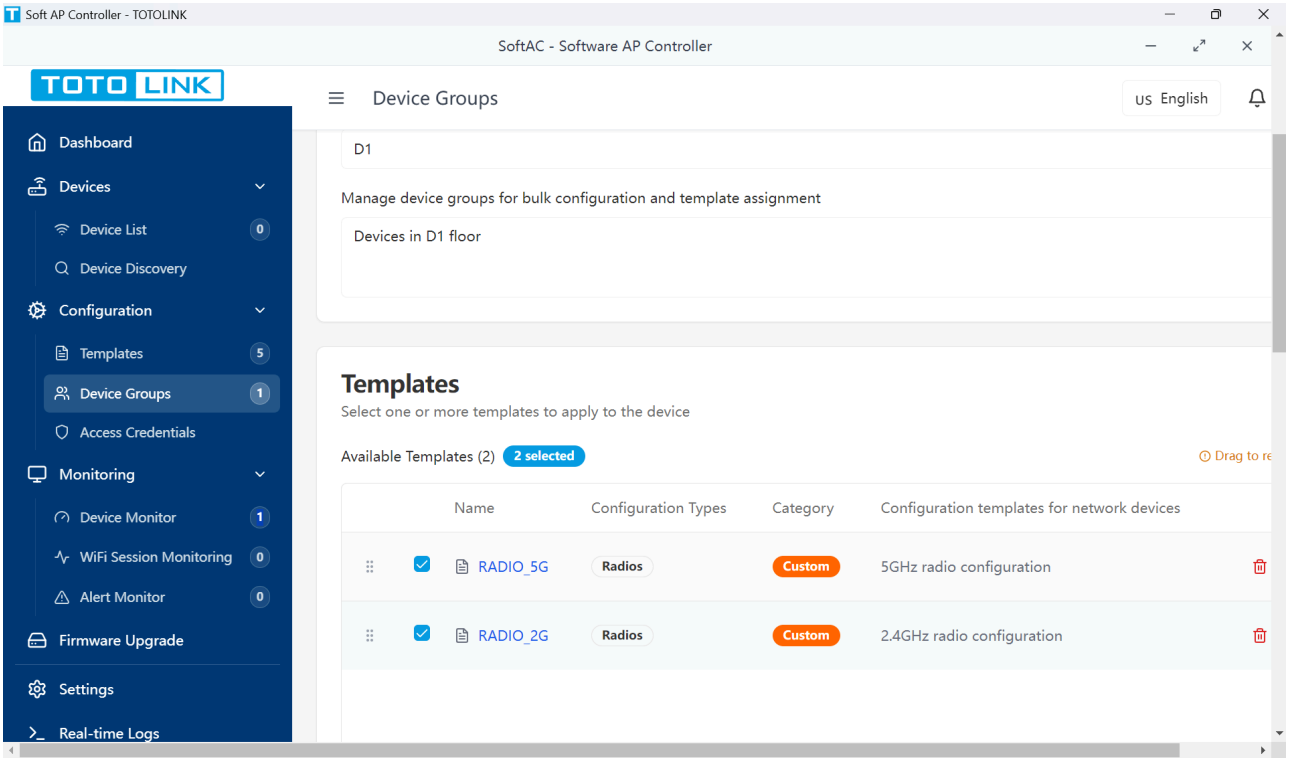
3. **Enter Group Information**
   Fill in the required and optional fields in the group creation form:

Field	Description	Required	Example
Group Name	Unique identifier for the group	Yes	"First Floor APs"
Description	Additional details about the group	No	"All access points on the first floor"
Templates	Configuration templates to apply	No	Select from dropdown



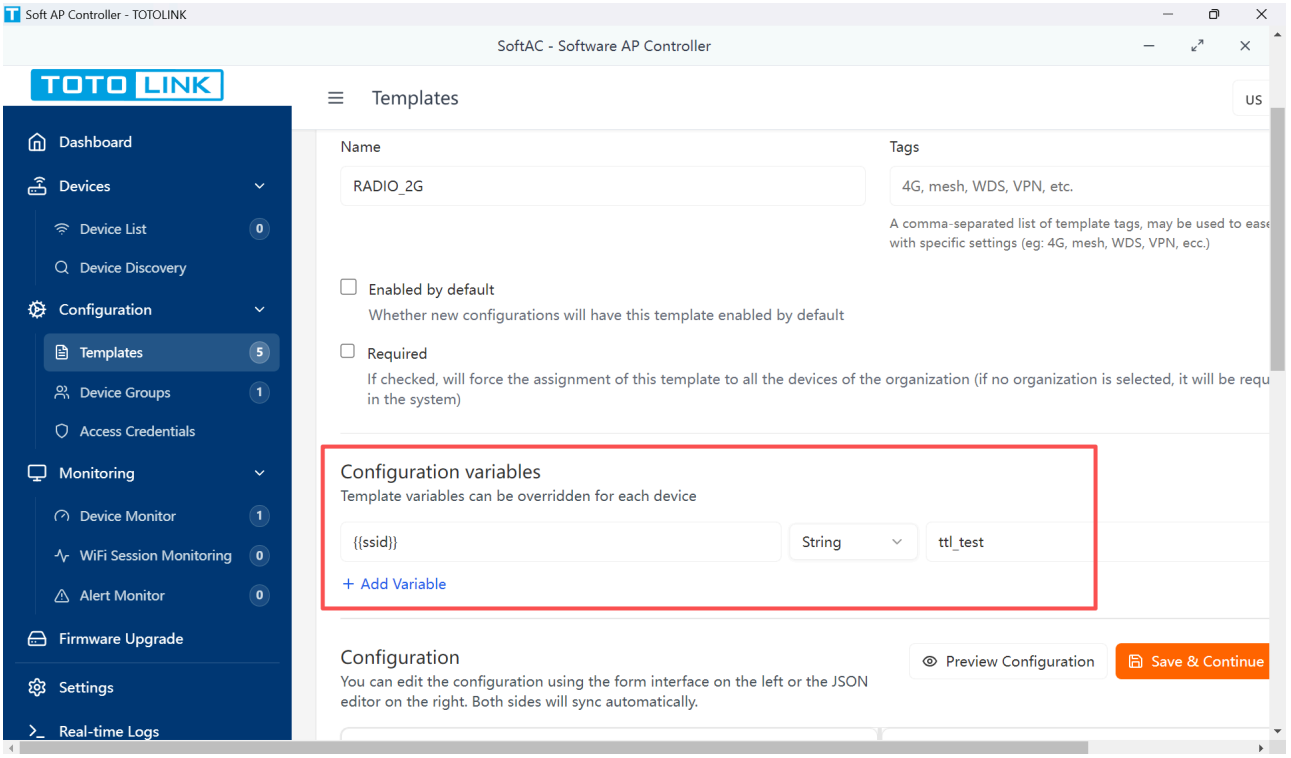
4. **Select Configuration Templates** (Optional)
   If you have created configuration templates:
   - Click the "Templates" dropdown
   - Select one or more templates to apply to this group
   - Templates will be applied in the order selected

> **Note**: You can add or modify templates later if needed.



5. **Configure Variables** (Optional)
   If your templates use variables:
   - Click "Add Variable" to define custom variables

- Enter variable name and value
- These variables will be available to all devices in the group



6. **Save the Group**
   Click the "Save" button to create the group.

> ✅ **Success**: The group will appear in your Device Groups list immediately.

After Creating a Group

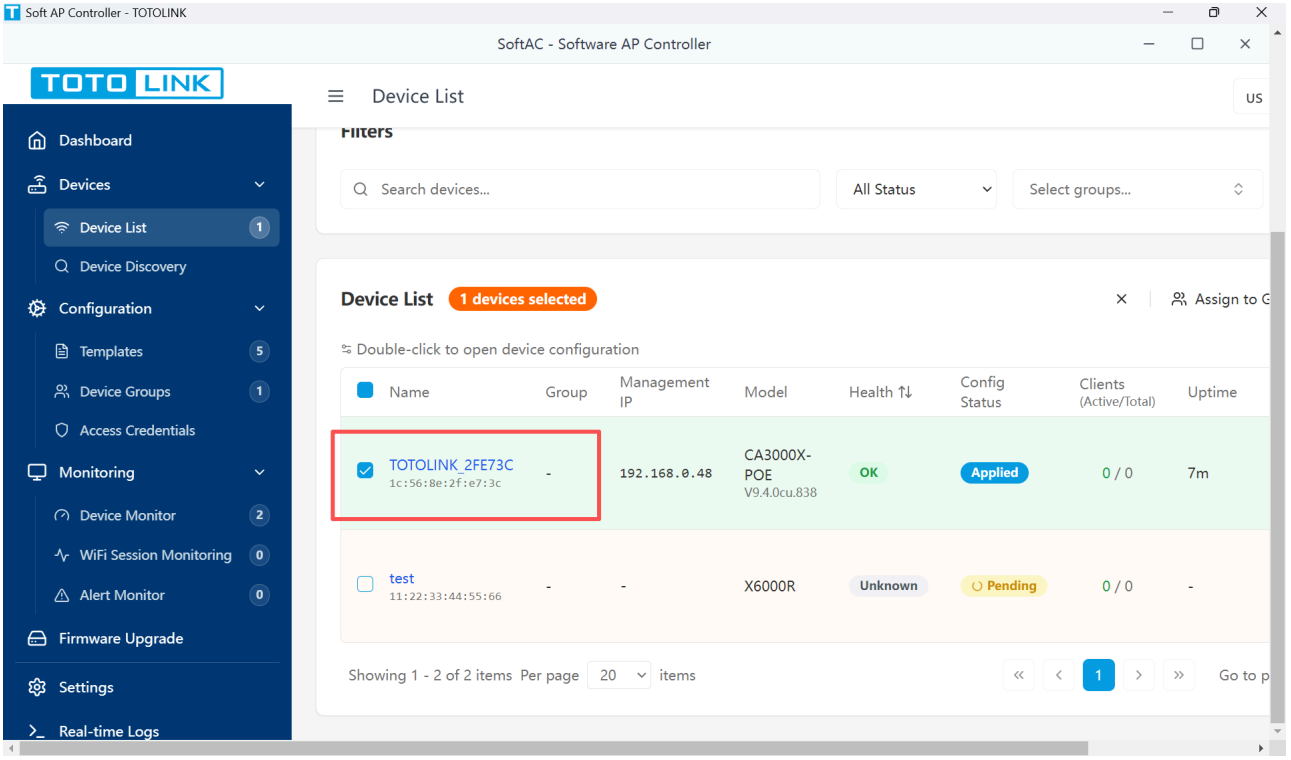
Once your group is created, you can:

- Add devices to the group
- Apply configuration templates
- Monitor group status from the dashboard
- Perform batch operations on all group members

6.3 Managing Group Members

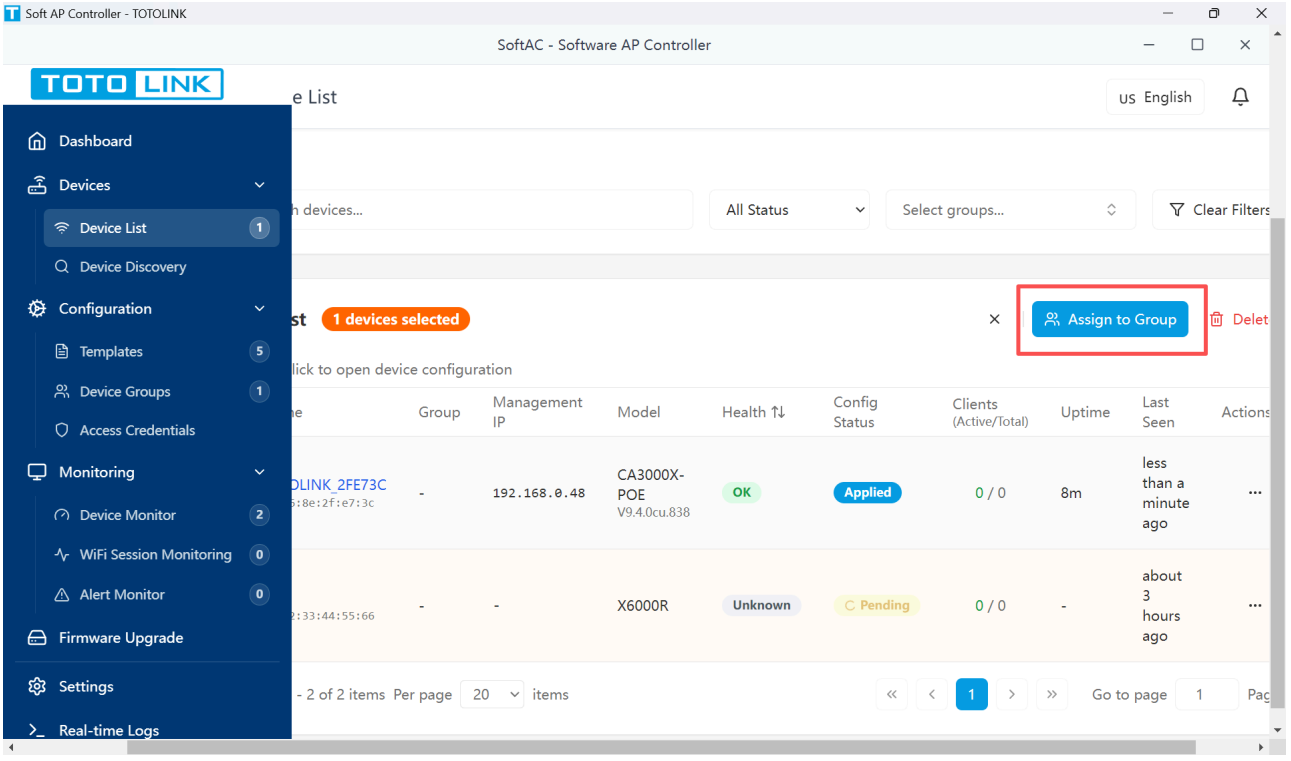
Adding Devices to a Group

1. **Open Device List**
   Select the devices you want in the Device List.



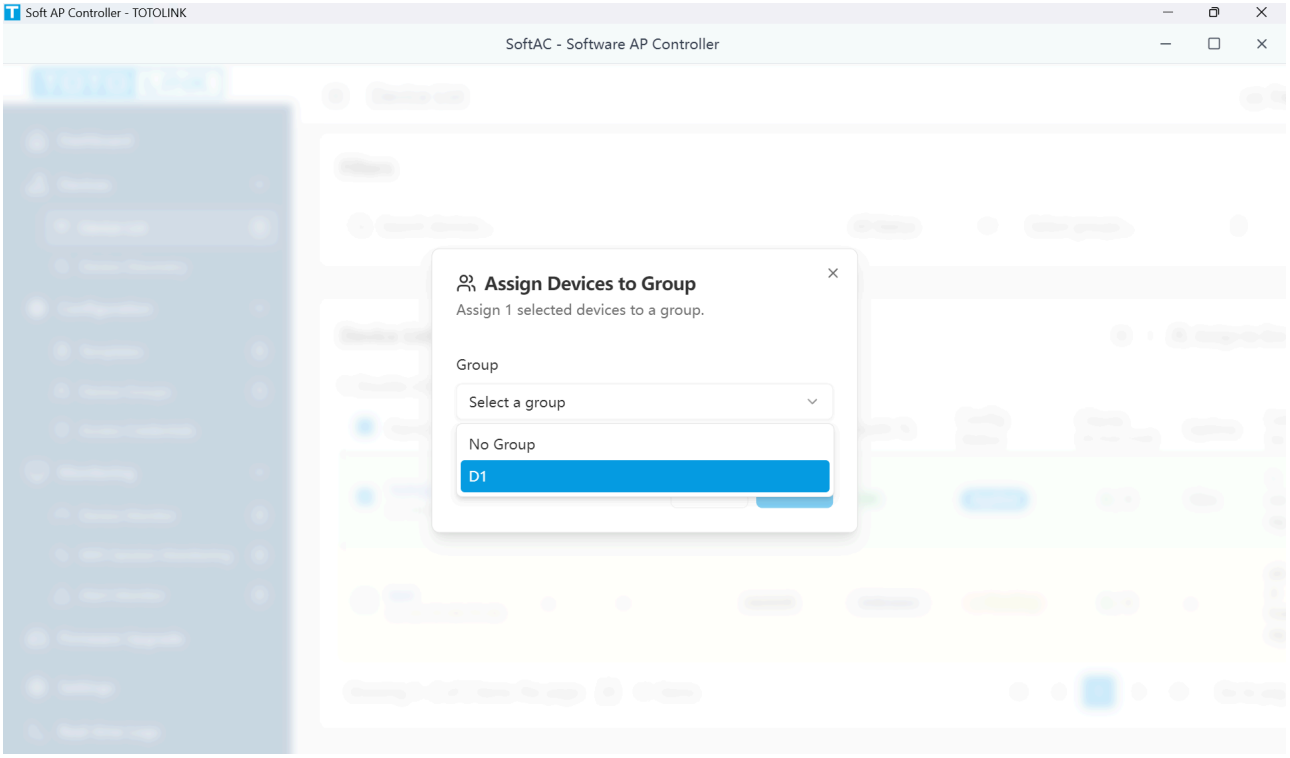
2. **Assign to Group**

   Click the "Assign to Group" tab at the upper right corner of the Device List.

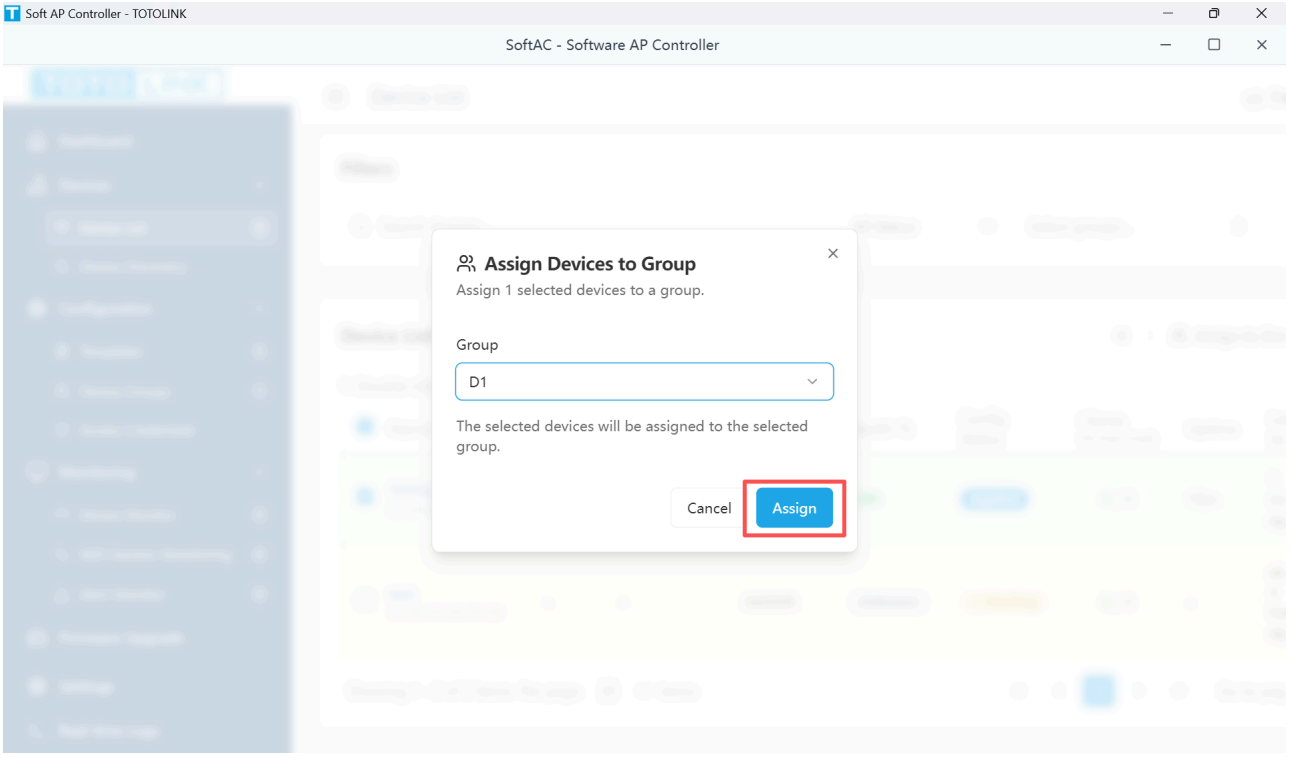


3. **Select a Group**

   Click "Select a Group" and select the group you want.

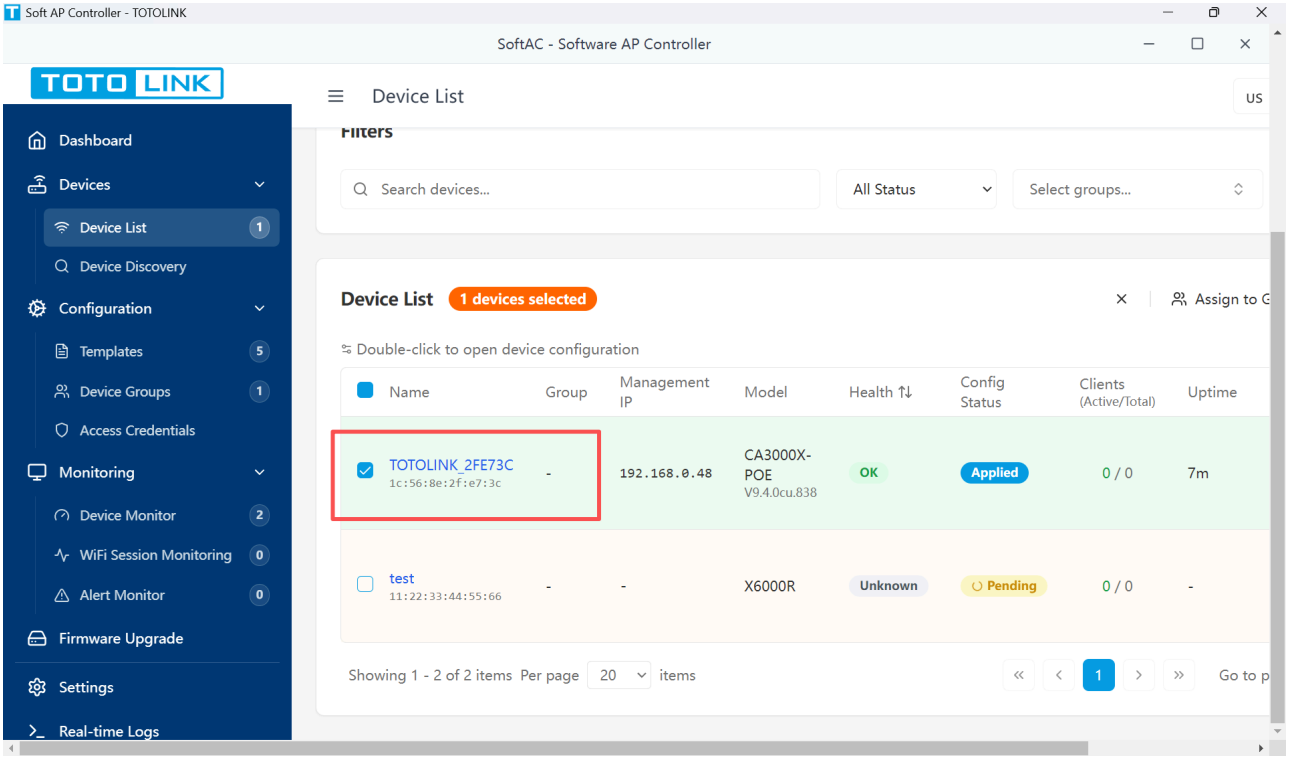


4. **Assign**
   Click the "Assign" button.



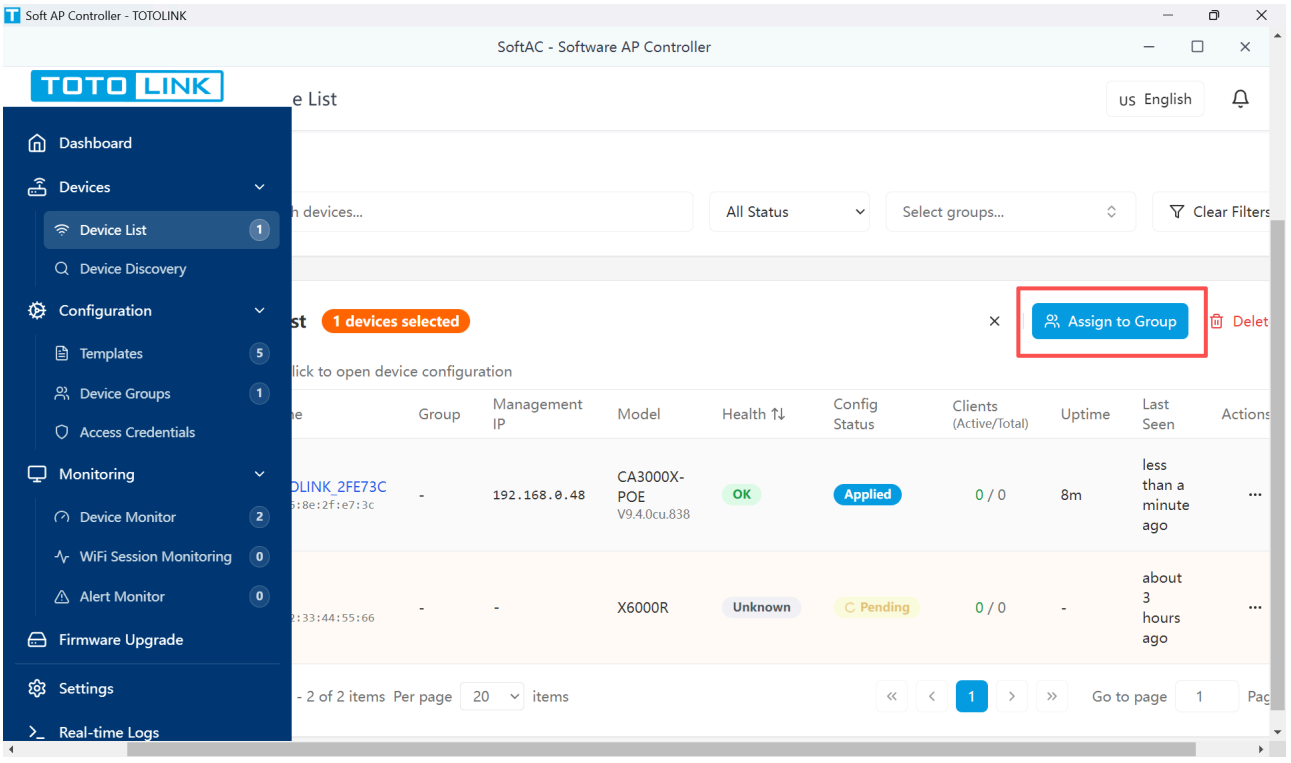
Removing Devices from a Group

1. **Open Device List**
   Select the devices you want in the Device List.



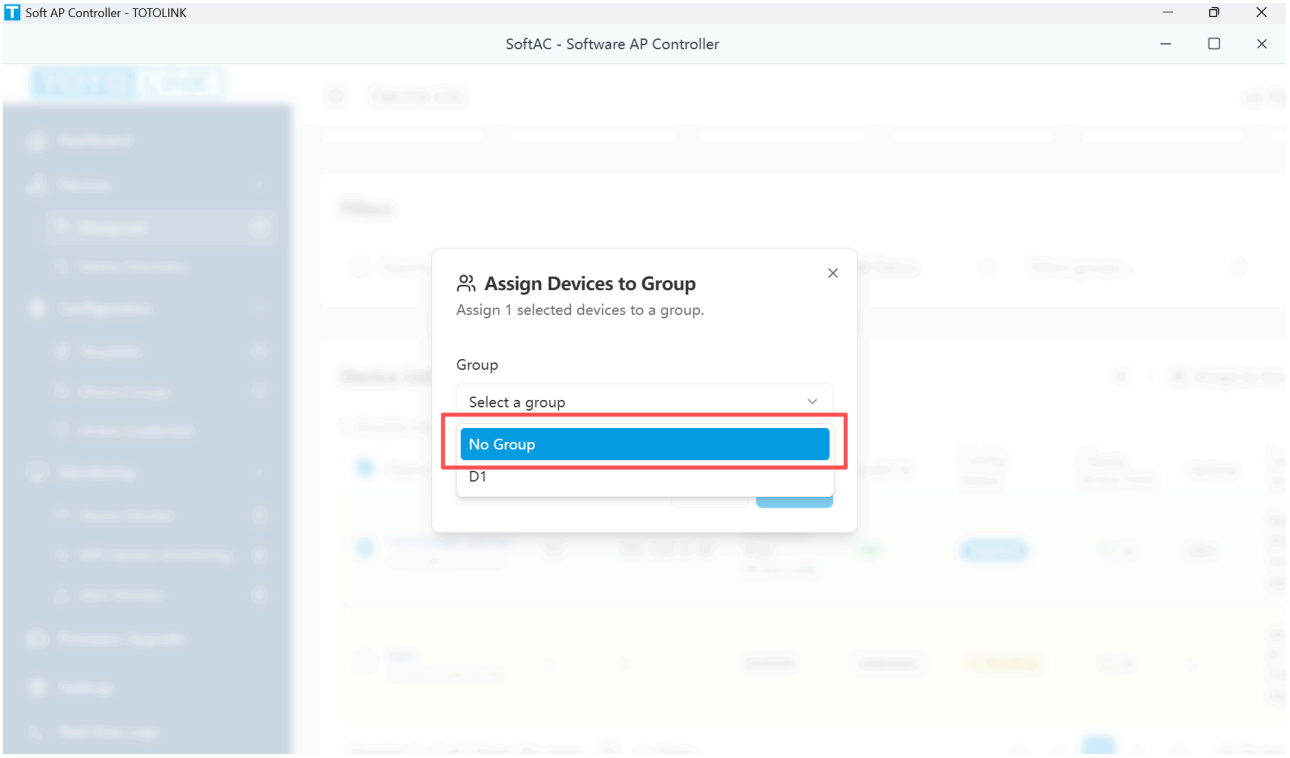
2. **Assign to Group**

   Click the "Assign to Group" tab at the upper right corner of the Device List.

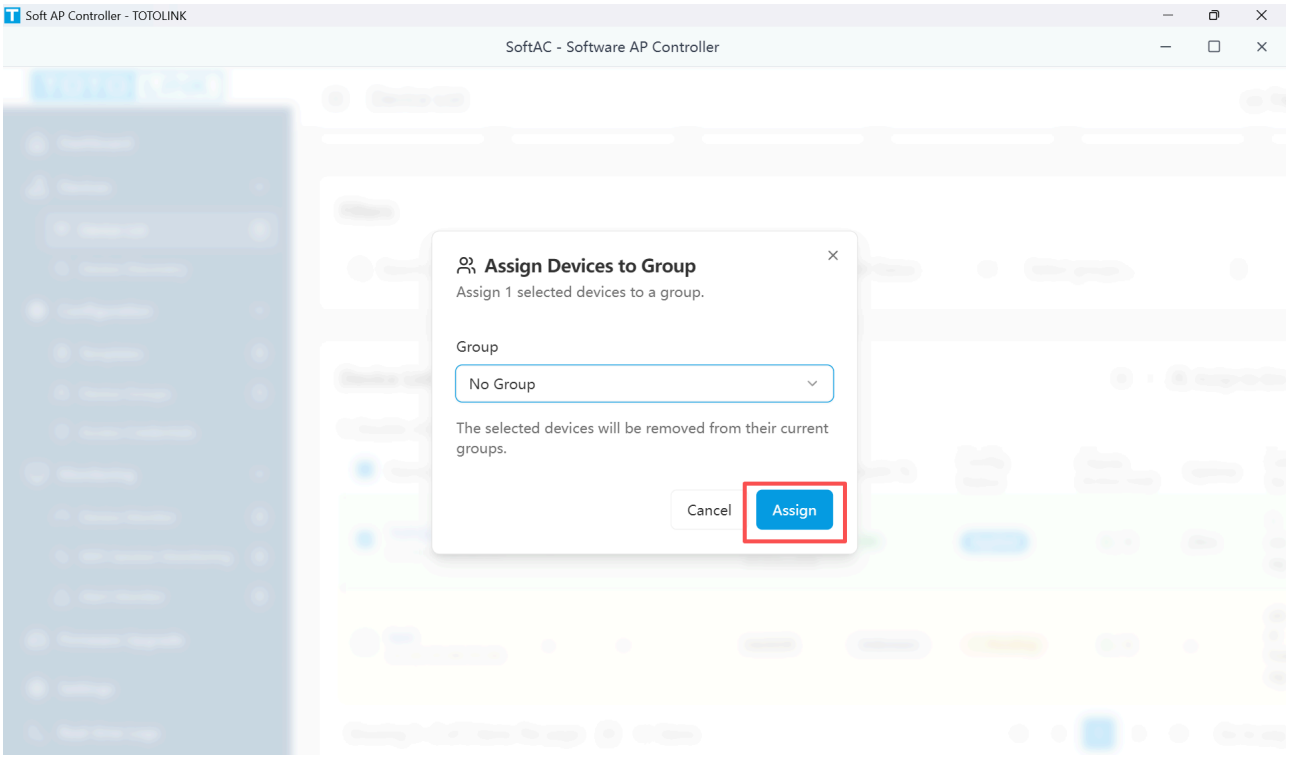


3. **Select a Group**

   Click "Select a Group" and select "No Group".



4. **Assign**
   Click the "Assign" button.



> ⚠️ **Important**: Removing a device from a group does not delete the device from the system. The device will retain its current configuration but will no longer receive group updates.

6.4 Group Configuration

Understanding Group Configuration Hierarchy

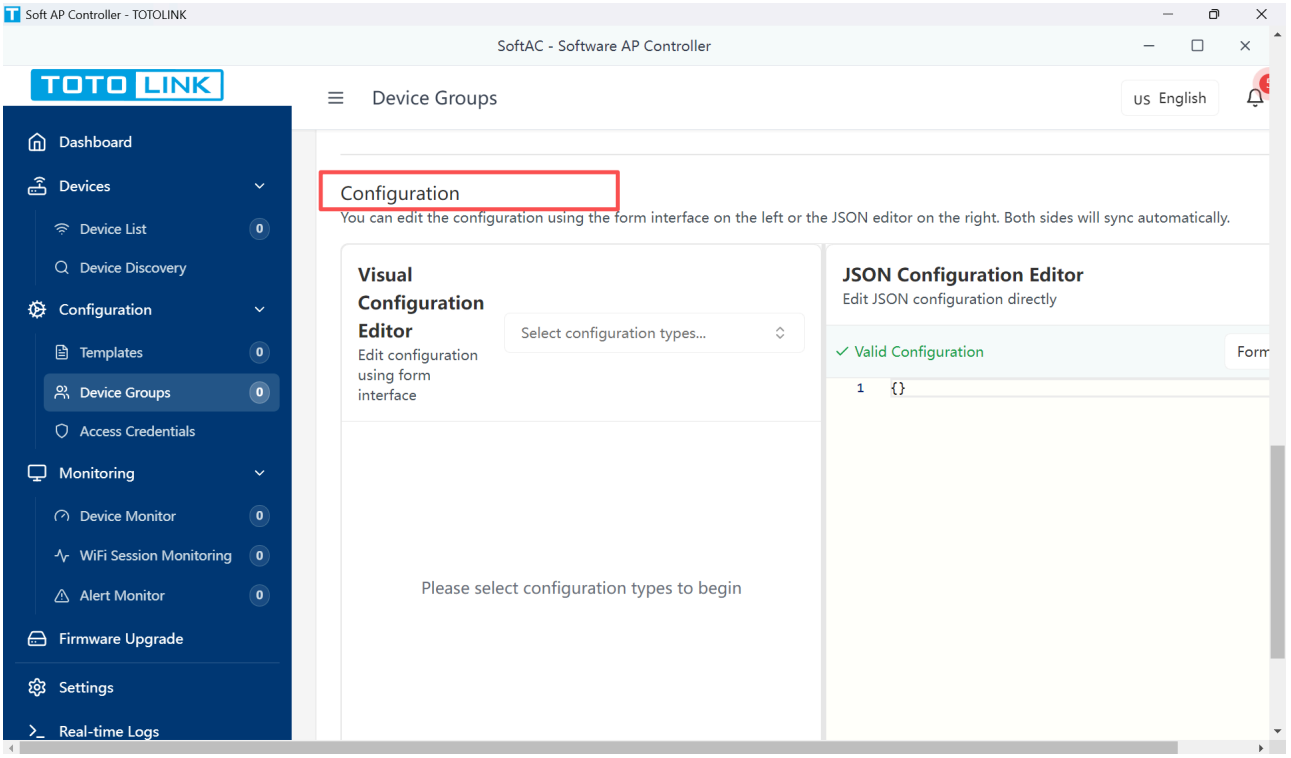
TOTOLINK SoftAC applies configurations in the following order:

1. **Default Settings**: System-wide defaults
2. **Group Configuration**: Settings applied to all group members
3. **Template Configuration**: Settings from assigned templates
4. **Device-Specific Configuration**: Individual device overrides

> 💡 **Tip**: More specific configurations override general ones. Device settings override group settings.

Configuring Group Settings

1. **Access Group Configuration**
   - Open the Device Groups page
   - Click a group you want in the group list
   - Find the "Configuration" tab



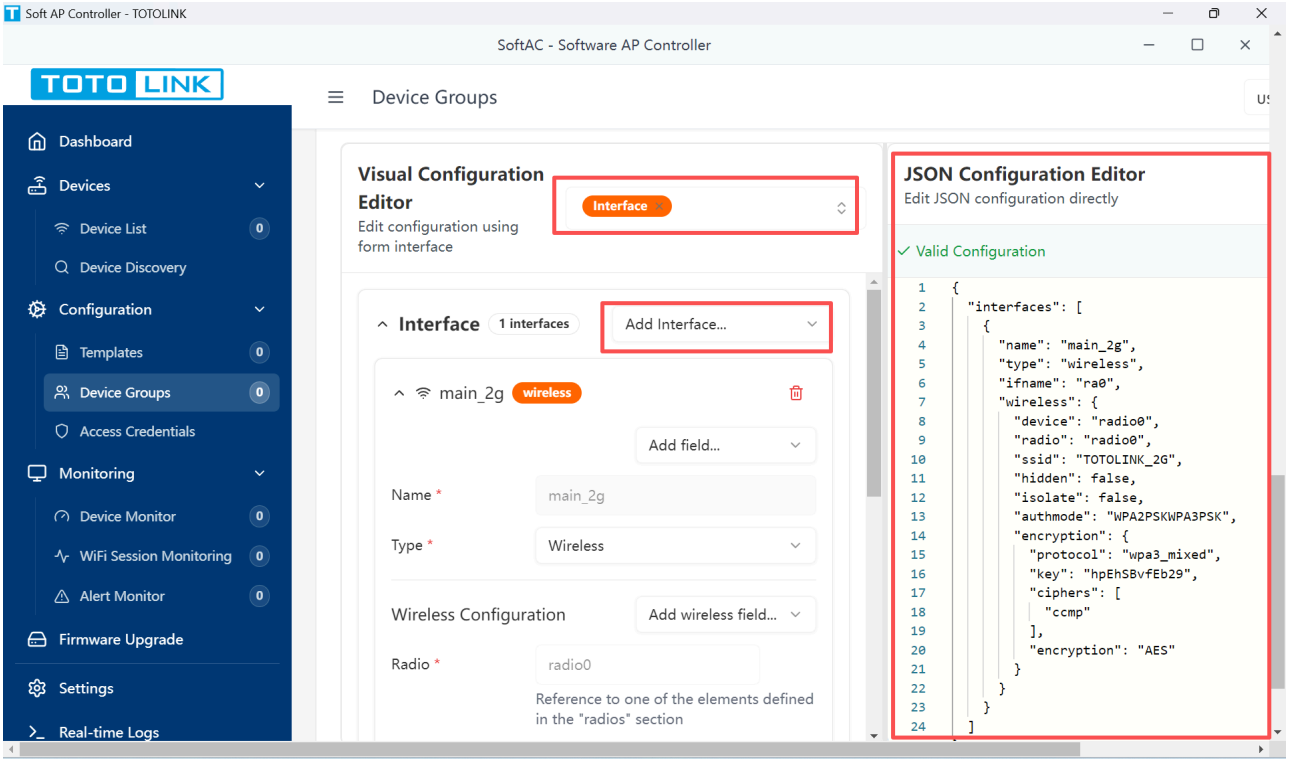
2. **Edit Configuration**
   The configuration editor provides two views:

   JSON View: For advanced users familiar with configuration syntax

```
{
  "interfaces": [
    {
      "name": "main_2g",
      "type": "wireless",
      "ifname": "ra0",
```

```
      "wireless": {
        "device": "radio0",
        "radio": "radio0",
        "ssid": "TOTOLINK_2G",
        "hidden": false,
        "isolate": false,
        "authmode": "WPA2PSKWPA3PSK",
        "encryption": {
          "protocol": "wpa3_mixed",
          "key": "FlUY@D^7KFZL",
          "ciphers": [
            "ccmp"
          ],
          "encryption": "AES"
        }
      }
    }
  ]
}
```


Form View: User-friendly interface for common settings



3. **Configure Common Settings**

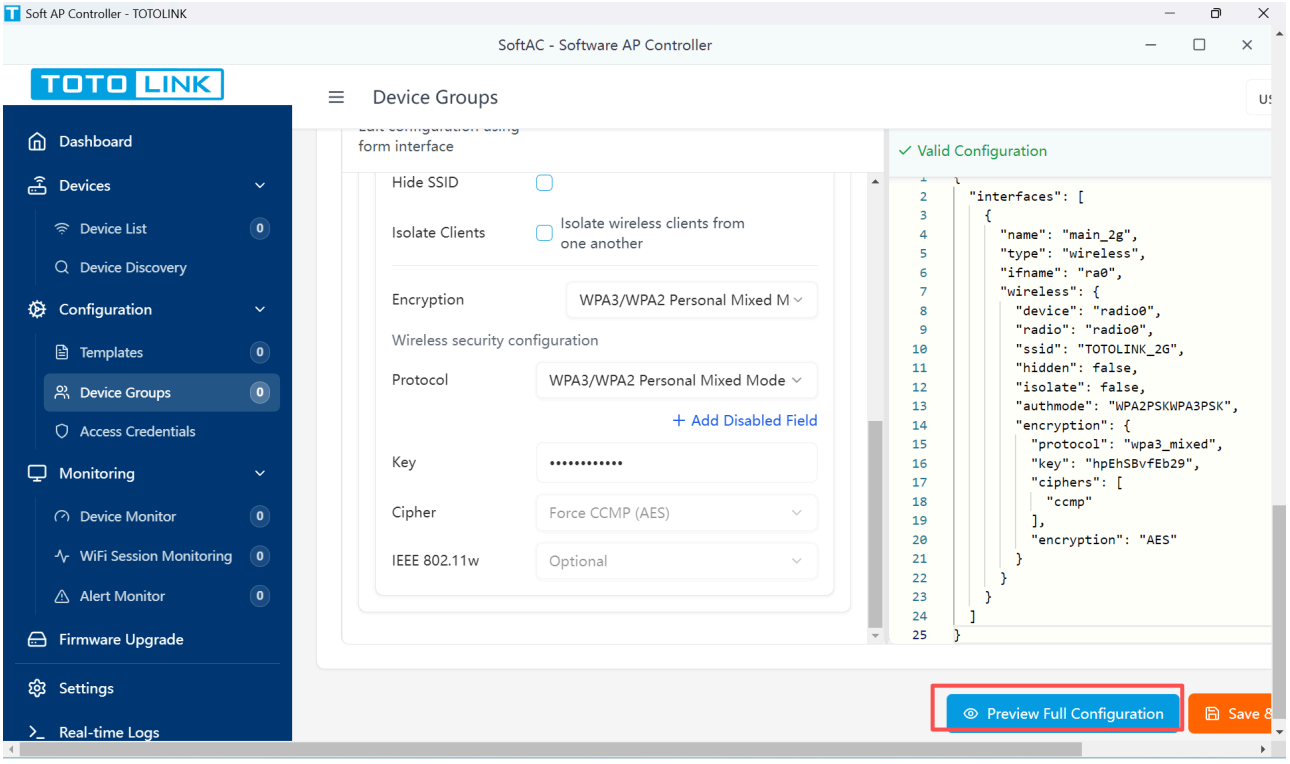
Setting Category	Common Options
Wireless	SSID, Channel, Power, Security Mode
Network	VLAN, IP Configuration, DNS
Security	Encryption, Authentication, Access Control
System	Timezone, NTP Server, Logging

4. **Use Configuration Variables**
   Variables allow dynamic configuration:
   - Reference variables using `{{variable_name}}` syntax
   - Variables are replaced with actual values when applied to devices

   Example:

```
{
  "wireless": {
    "ssid": "{{location}}-WiFi",
    "channel": "{{channel}}"
  }
}
```

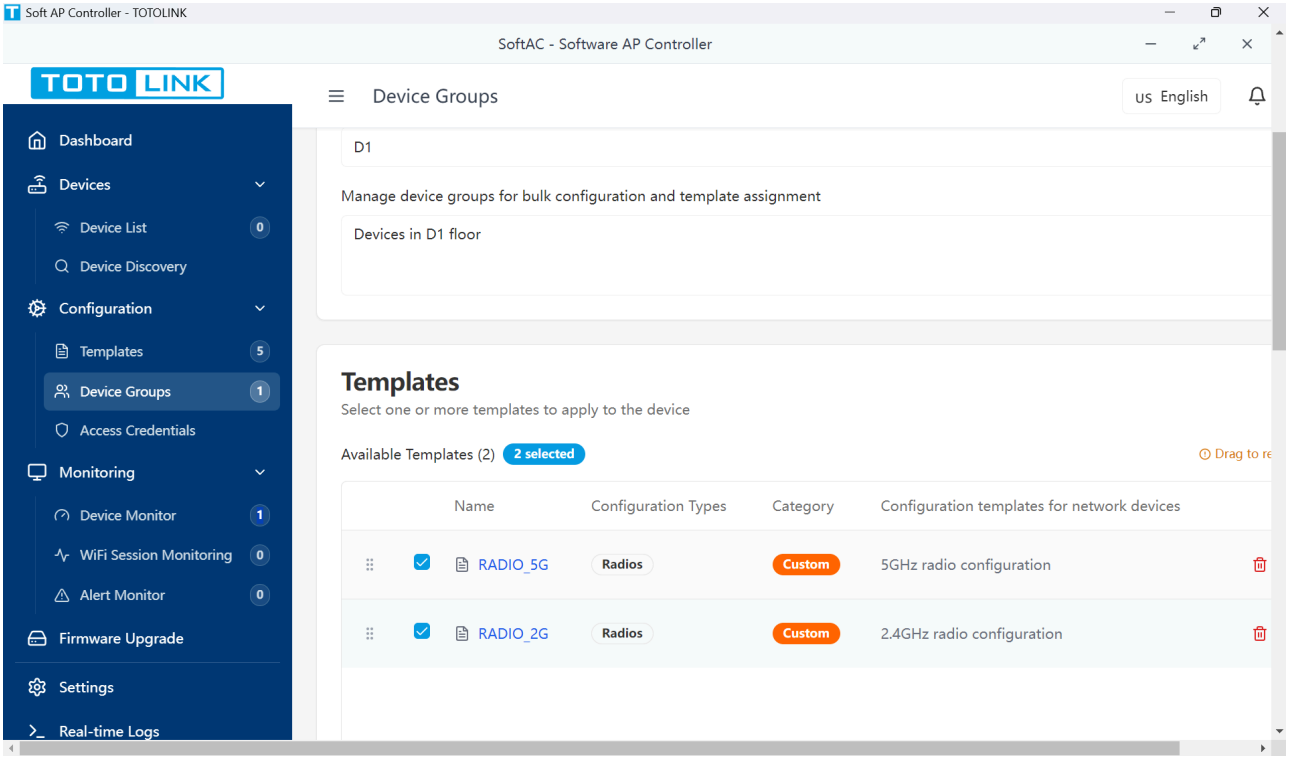
5. **Preview Configuration**
   Click "Preview" to see how the configuration will appear when applied to devices.

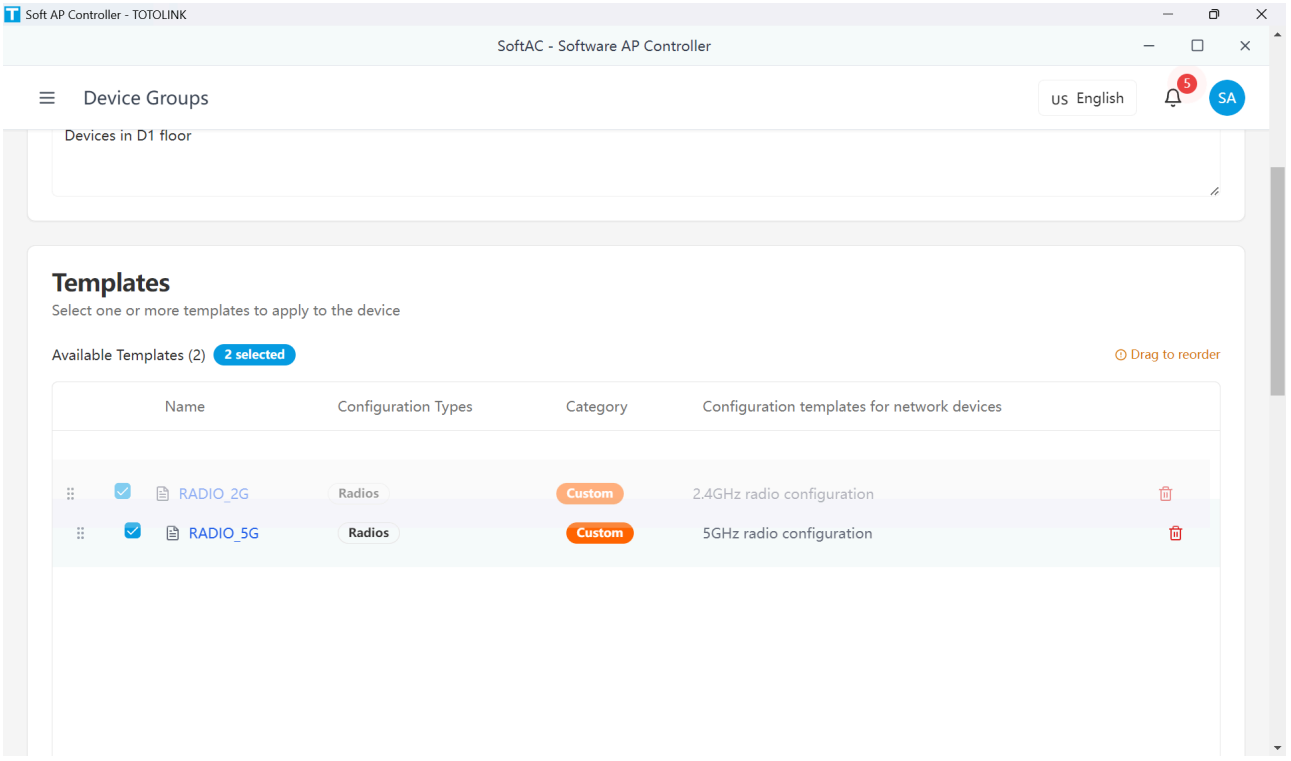


6. **Save Configuration**
   Click "Save" to store the configuration. Changes are not automatically applied to devices.

Template Management for Groups

1. **Assign Templates**
   - Open the Device Groups page
   - Click a group you want in the group list
   - Find the "Templates" tab
   - Drag to reorder template priority





2. **Template Order**
   Templates are applied in the specified order. Later templates override earlier ones for conflicting settings.

> 📝 **Note**: Template order is crucial. Place general templates first and specific ones last.

Related Features

- 4.3 Device Configuration - Configure individual devices
- 5.2 Creating Templates - Create reusable configuration templates
- 7.1 Device Monitoring - Monitor grouped devices

- 8.3 Batch Upgrade - Upgrade firmware for device groups

Quick Reference

Common Group Operations

Task	Location	Action
Create group	Device Groups page	Click "+ New Group"
Add devices	Group details > Members	Click "Add Devices"
Apply templates	Group details > Configuration	Click "Manage Templates"
Deploy config	Group details	Click "Deploy Configuration"
View history	Group details > History	Review deployment log

Keyboard Shortcuts

Shortcut	Action
Ctrl+S	Save configuration
Ctrl+P	Preview configuration
Ctrl+D	Deploy configuration
Esc	Cancel current dialog

> 📝 **Need Help?**: Contact TOTOLINK support for assistance with device group management.

Part 7. Network Monitoring

Overview

TOTOLINK SoftAC's Network Monitoring feature provides real-time visibility into your network's health and performance. Monitor all your devices from a single dashboard, track network usage patterns, and receive alerts when issues arise. This comprehensive monitoring system helps you maintain optimal network performance and quickly identify problems before they affect users.

Use Cases

- **Daily Operations**: Monitor device status and network performance during business hours
- **Troubleshooting**: Quickly identify which devices are experiencing issues
- **Capacity Planning**: Track usage trends to plan network expansion
- **Performance Optimization**: Identify bottlenecks and optimize network settings
- **Proactive Maintenance**: Receive alerts before problems become critical

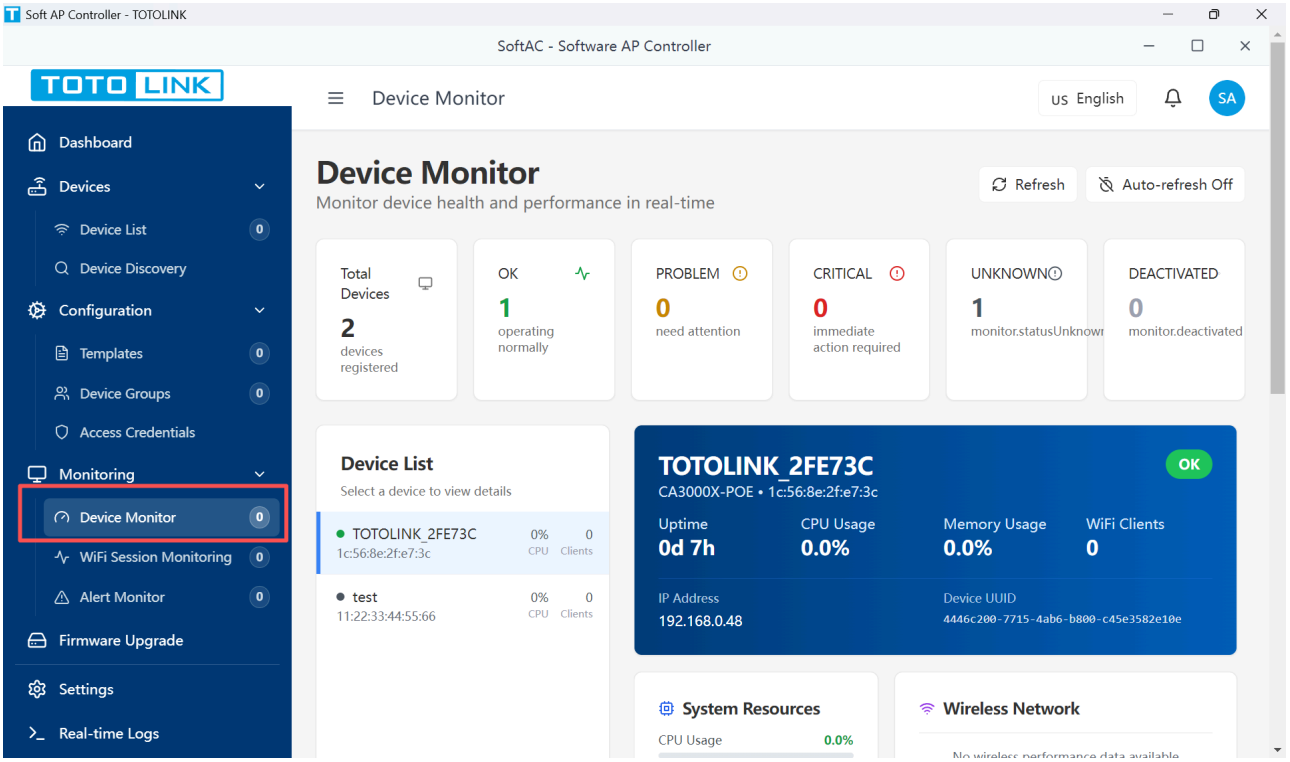
7.1 Device Monitoring

Feature Overview

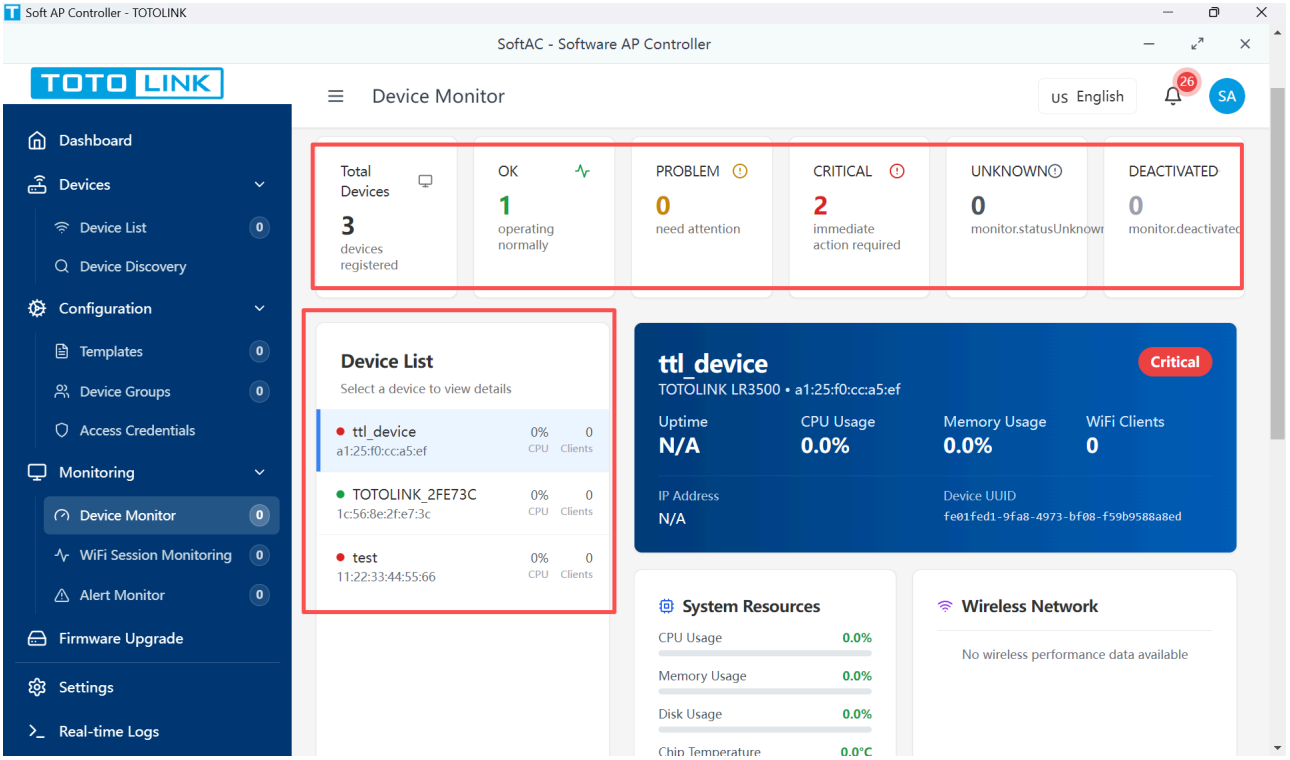
Device Monitoring gives you complete visibility into each device's operational status, performance metrics, and connection quality. View real-time data for all managed devices, track their health over time, and quickly identify any devices that need attention.

How to Access Device Monitoring

1. **Navigate to Monitoring Section**
   Click "Device Monitor" in the left navigation menu.



2. **View Device List**
   The main monitoring page displays all your devices with their current status.



7.1.1 Real-time Status

Understanding Device Status

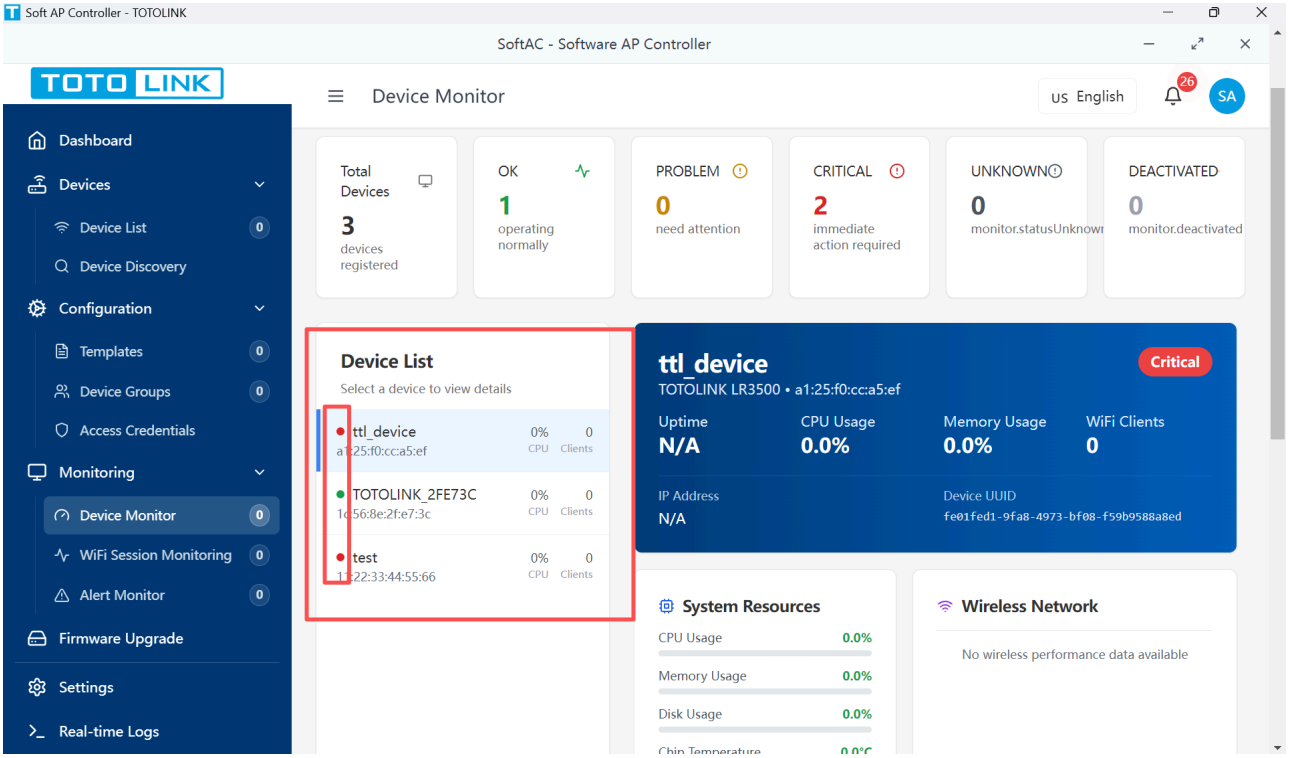
Real-time status monitoring shows the current operational state of each device in your network. The system continuously checks device health and updates the display automatically.

Status Indicators

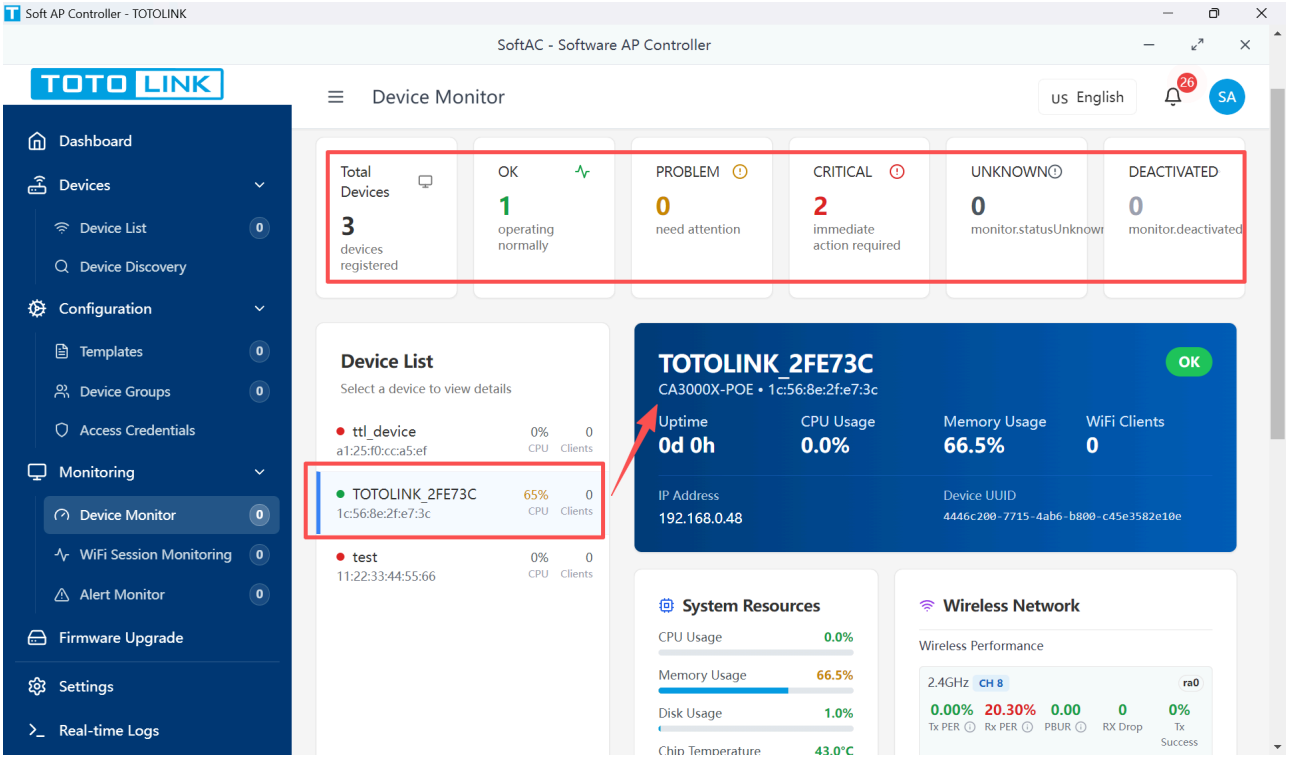
Status	Icon	Description	Action Required
Online	🟢	Device is connected and responding normally	None
Offline	🔴	Device is not responding to health checks	Check device power and network connection
Problem	🟡	Device is online but experiencing issues	Review alerts for specific problems
Unknown	⚫	Device status cannot be determined	Wait for next health check

Viewing Real-time Status

1. **Main Status View**
   The device list shows each device's current status with color-coded indicators.

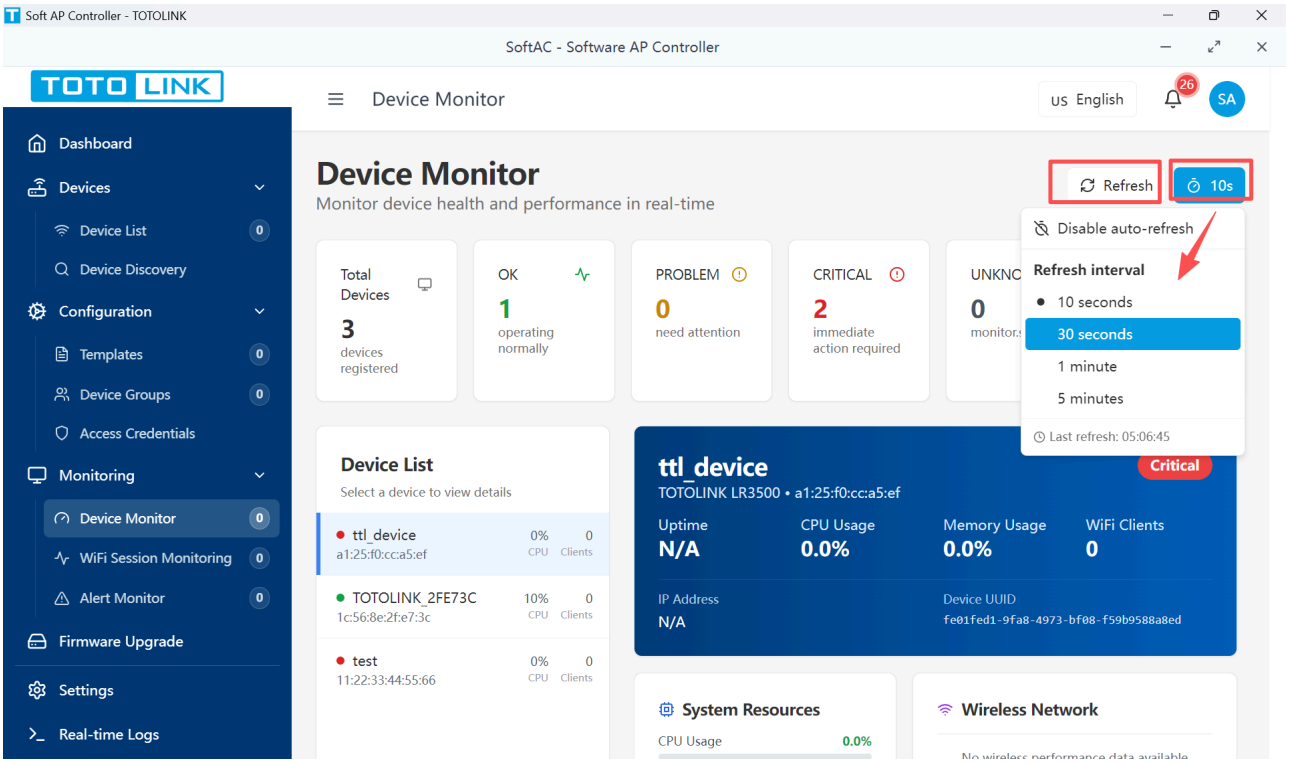


2. **Detailed Status Information**
   Click on any device name to view detailed status information:
   - **Uptime**: How long the device has been running
   - **CPU Usage**: The percentage of CPU used currently
   - **Memory Usage**: The percentage of memory used currently
   - **WiFi Clients**: Number of connected WiFi users



3. **Auto-refresh Settings**
   The status display refreshes automatically every 30 seconds. You can also:
   - Click the refresh button for immediate update

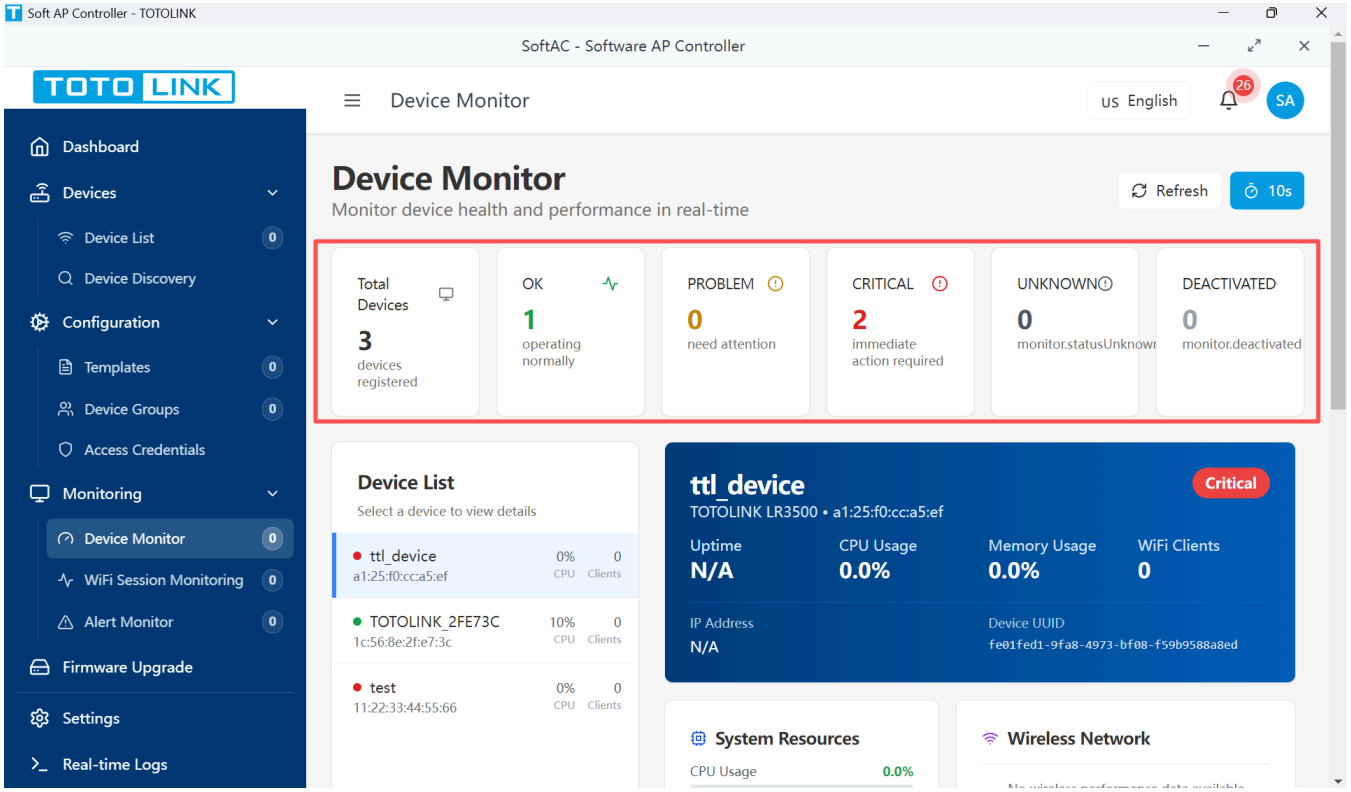
- Adjust refresh interval in settings



Quick Status Overview

The dashboard header provides an at-a-glance summary:

- **Total Devices**: Number of devices being monitored
- **OK**: Devices currently operational
- **PROBLEM**: Number of issues which need attention
- **CRITICAL**: Number of issues which need immediate action
- **UNKNOWN**: Devices which can not be identified
- **DEACTIVATED**: Devices currently offline



> 💡 **Tip**: Set up email notifications to be alerted immediately when a device goes offline. This helps you respond quickly to network issues.

7.1.2 Performance Metrics

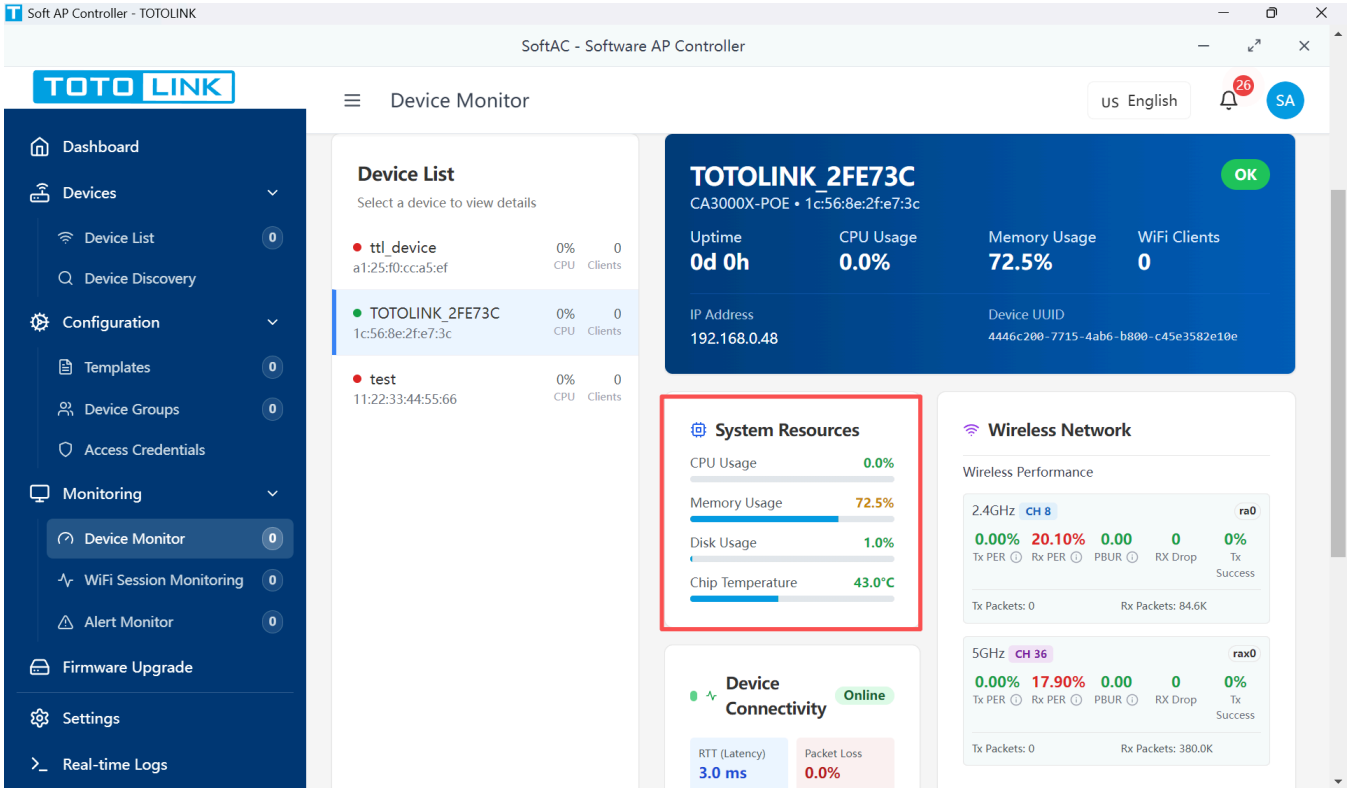
Available Metrics

TOTOLINK SoftAC monitors key performance indicators that affect network quality and user experience:

System Resources

Monitor device hardware utilization to prevent performance issues:

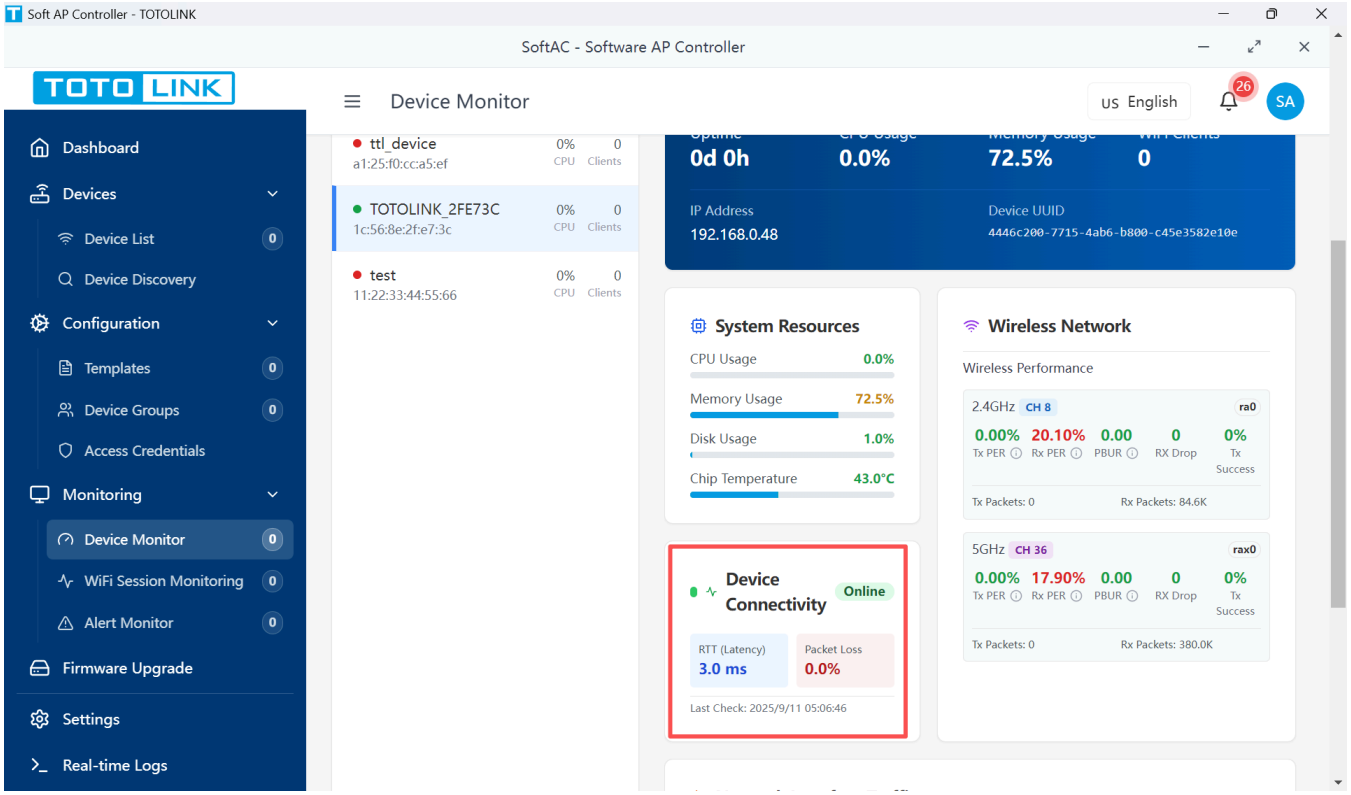
Metric	Description	Healthy Range	Alert Threshold
CPU Usage	Processor utilization percentage	0-60%	Above 80%
Memory Usage	RAM utilization percentage	0-70%	Above 85%
Disk Usage	Storage space utilization	0-80%	Above 90%
Chip Temperature	Device operating temperature	20-60°C	Above 70°C



Device Connectivity

Track network quality and throughput:

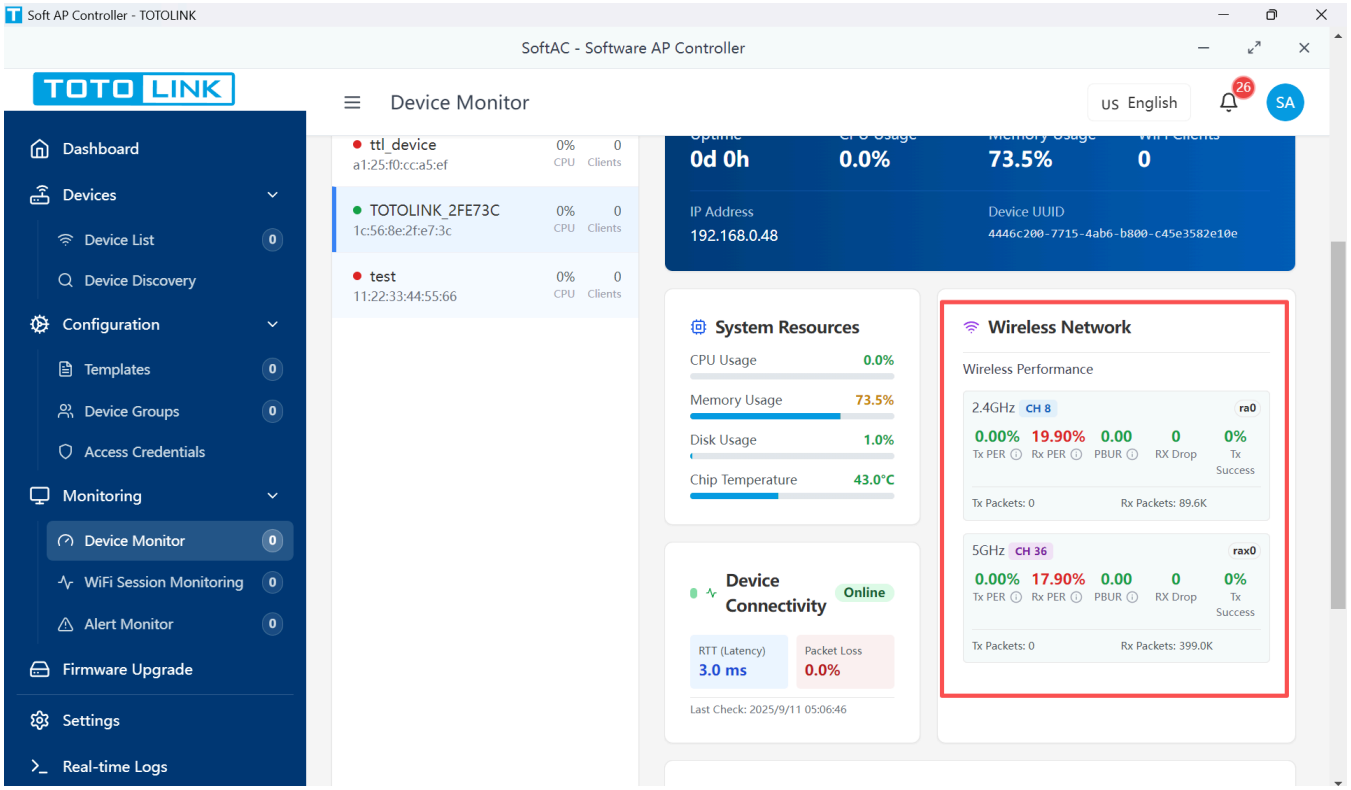
Metric	Description	What to Watch
RTT(Latency)	Current transmission interval per packet	Should be below 50ms
Packet Loss	Percentage of lost data packets	Should be below 1%



Wireless Network

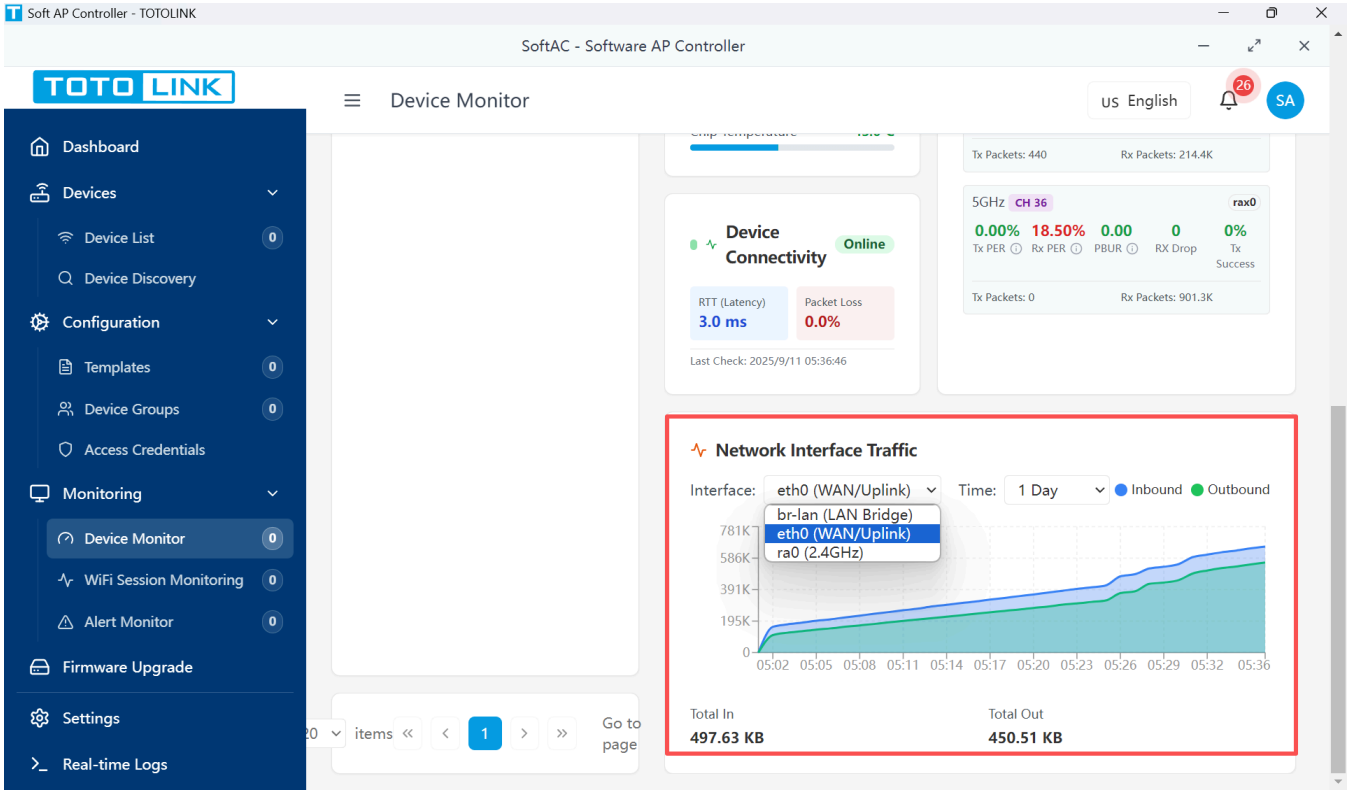
Monitor wireless network quality:

Metric	Description	Optimal Value
Tx PER	Transmit Packet Error Rate	Less than 1%
Rx PER	Receive Packet Error Rate	Less than 1%
PBUR	Physical Bandwidth Utilization Ratio	Less than 0.1
Rx Drop	Dropped packets in reception direction	--
Tx Success	Transmit Packet Success Rate	More than 99%



Network Interface Traffic

Record the traffic statistics of device's interface in a period.



##

Troubleshooting

Issue: Device shows offline but is working

- Check network connectivity between SoftAC and device
- Verify device monitoring service is enabled
- Ensure correct monitoring interval is set

Issue: Missing historical data

- Check data retention settings
- Verify device was online during the period
- Ensure monitoring service has sufficient storage

Issue: Performance metrics not updating

- Refresh the page manually
- Check auto-refresh settings
- Verify device is reporting metrics correctly

Best Practices

1. **Regular Monitoring**
    - Check dashboard daily for offline devices
    - Review performance alerts weekly
    - Analyze historical trends monthly

2. **Proactive Maintenance**
    - Set appropriate alert thresholds
    - Schedule regular device restarts
    - Keep firmware updated
3. **Documentation**
    - Export monthly reports for records
    - Document network changes and their impact
    - Track recurring issues and resolutions

Related Features

- 7.2 WiFi Session Management - Monitor connected users
- 7.3 Alert Management - Configure and manage alerts
- 8. Firmware Management - Keep devices updated
- 11. System Settings - Configure monitoring preferences

Next Steps

Now that you understand device monitoring, learn how to:

- Monitor WiFi sessions and user activity
- Set up custom alerts for critical events
- Configure automated responses to common issues

Continue to 7.2 WiFi Session Management →

7.2 WiFi Session Management

Feature Overview

WiFi Session Management provides comprehensive visibility into all wireless client connections across your network. Monitor active users in real-time, review connection history, and track user behavior patterns to optimize your WiFi network performance. This powerful feature helps you understand network usage, identify connection issues, and ensure quality service for all users.

Use Cases

- **Guest WiFi Management**: Monitor guest network usage and identify unauthorized access attempts
- **Troubleshooting Connection Issues**: Review session details to diagnose why specific clients experience connectivity problems
- **Network Capacity Planning**: Analyze peak usage times and client distribution across access points
- **Security Monitoring**: Track unusual connection patterns or suspicious client behavior
- **Bandwidth Management**: Identify heavy network users and optimize resource allocation

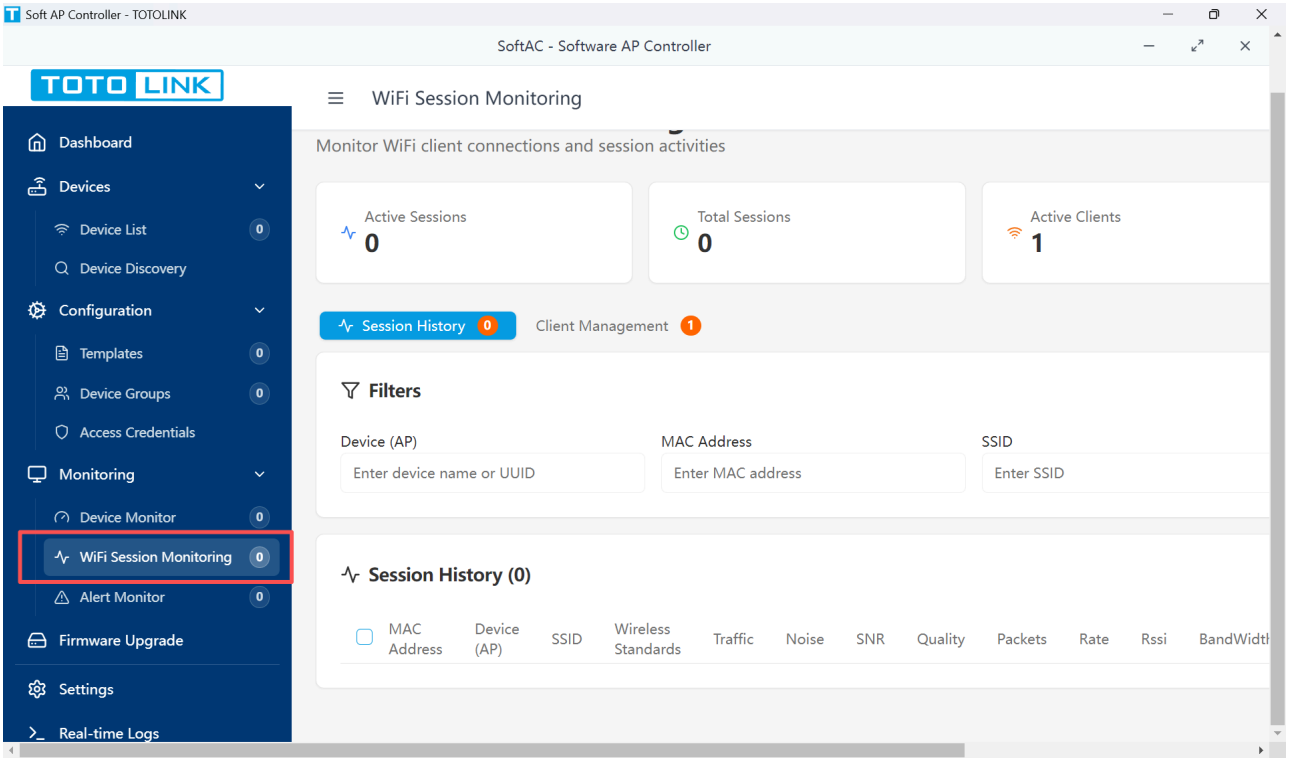
7.2.1 Online Users

Understanding Online Users

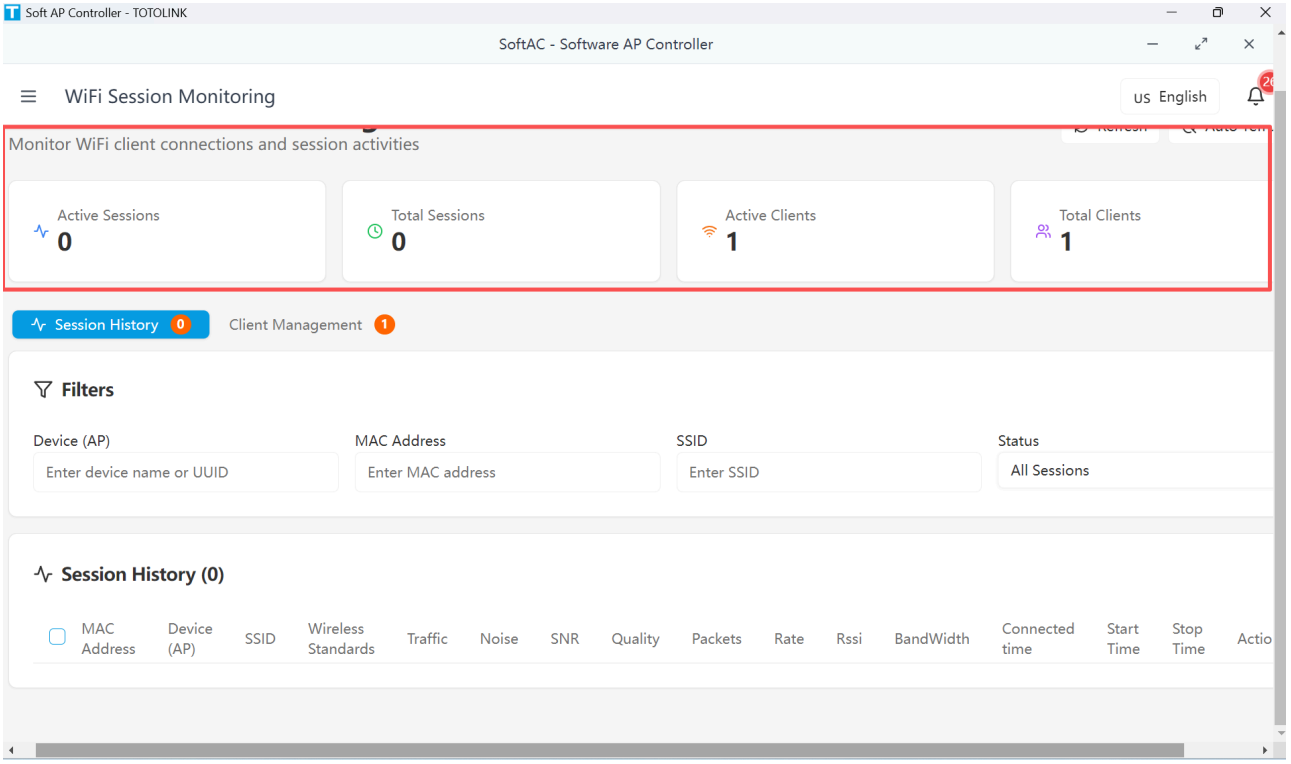
The Online Users view displays all currently connected WiFi clients across your network in real-time. This gives you instant visibility into who is using your network, which access points they're connected to, and their connection quality.

Accessing Online Users

1. **Navigate to WiFi Sessions**
   Click "WiFi Sessions Monitoring" in the left navigation menu under the Network Monitoring section.



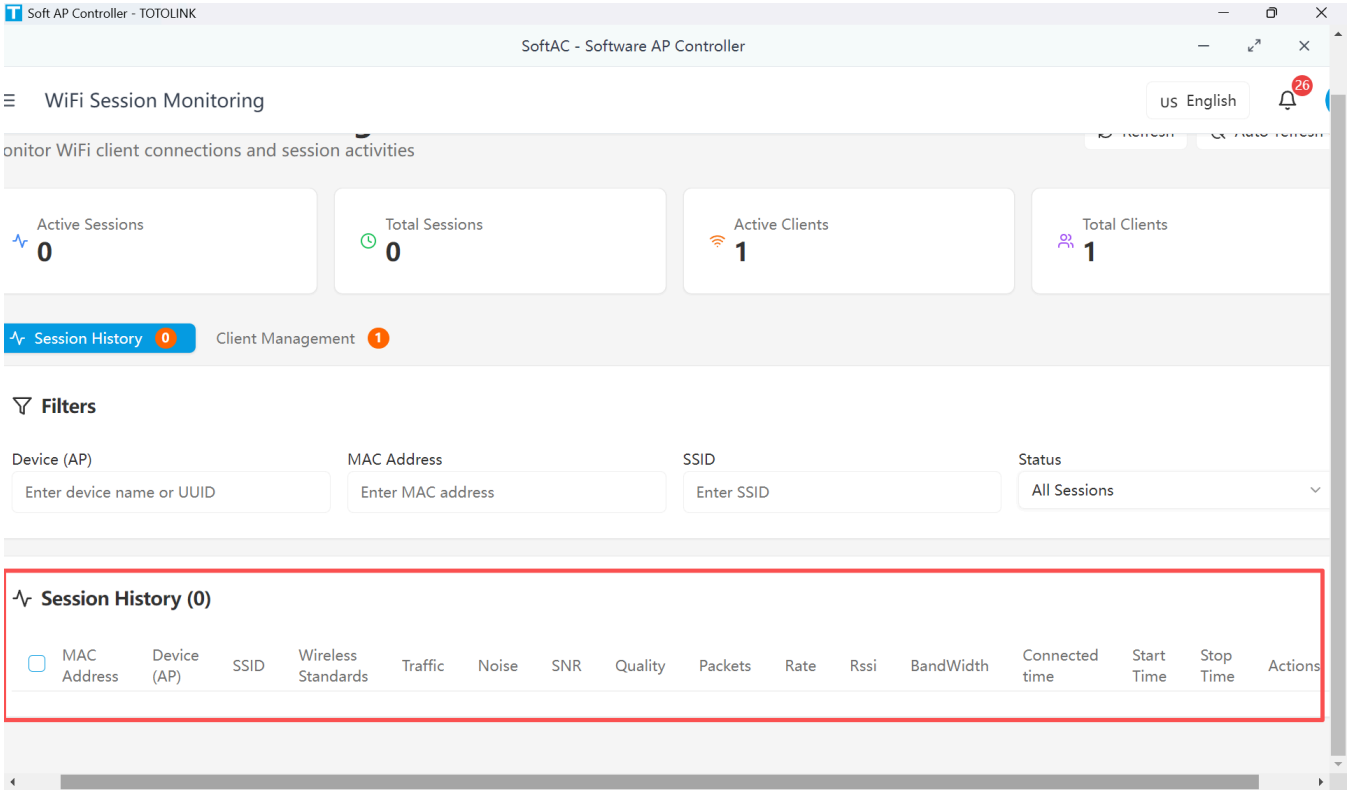
2. **View Active Sessions**
   The main page displays summary cards showing:
   - **Active Sessions**: Number of current connections
   - **Total Sessions**: Historical connection count
   - **Active Clients**: Unique devices currently online
   - **Total Clients**: All devices that have connected



Online User Information

The sessions table displays comprehensive information for each connected client:

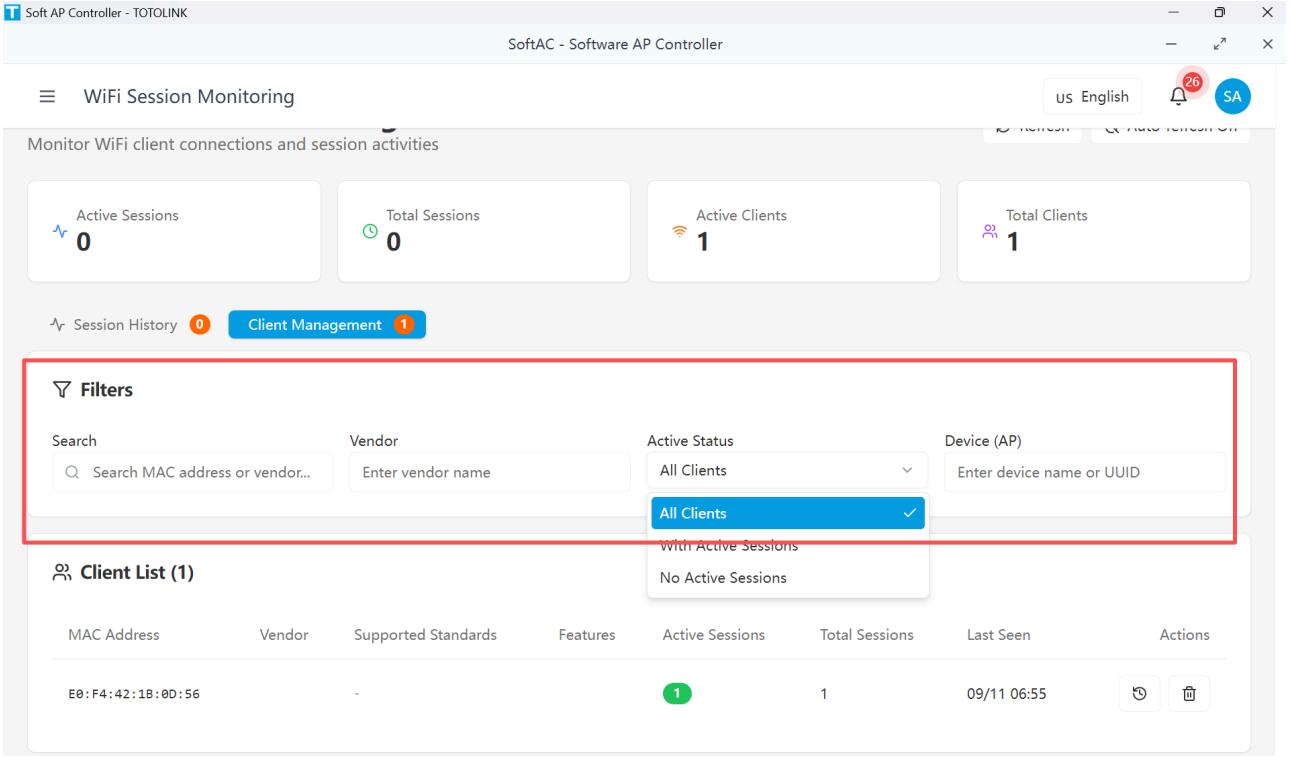
Column	Description	Use for Troubleshooting
MAC Address	Unique hardware identifier of the client device	Identify specific devices
Device (AP)	Access point the client is connected to	Check AP load distribution
SSID	Network name the client is using	Verify correct network access
Signal Strength	Connection quality in dBm	Identify weak connections
Traffic	Upload/download data volumes	Monitor bandwidth usage
Connected Time	Duration of current session	Track long-running connections
Wireless Standard	WiFi technology (WiFi 4/5/6)	Ensure optimal performance



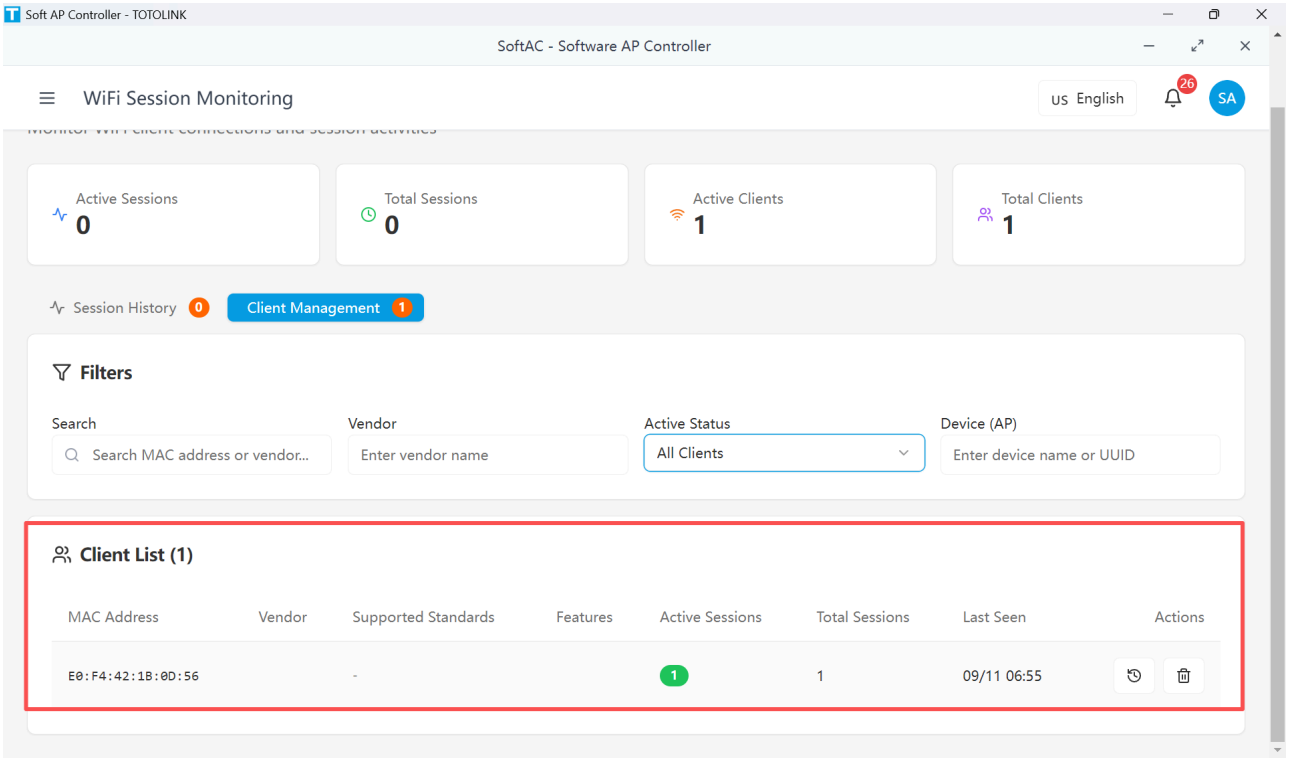
Filtering Online Users

Use filters to find specific clients or connection patterns:

1. **Apply Filters**
    - **Device**: Filter by specific access point
    - **MAC Address**: Search for a specific client
    - **SSID**: Show only clients on specific networks
    - **Status**: View active or inactive sessions



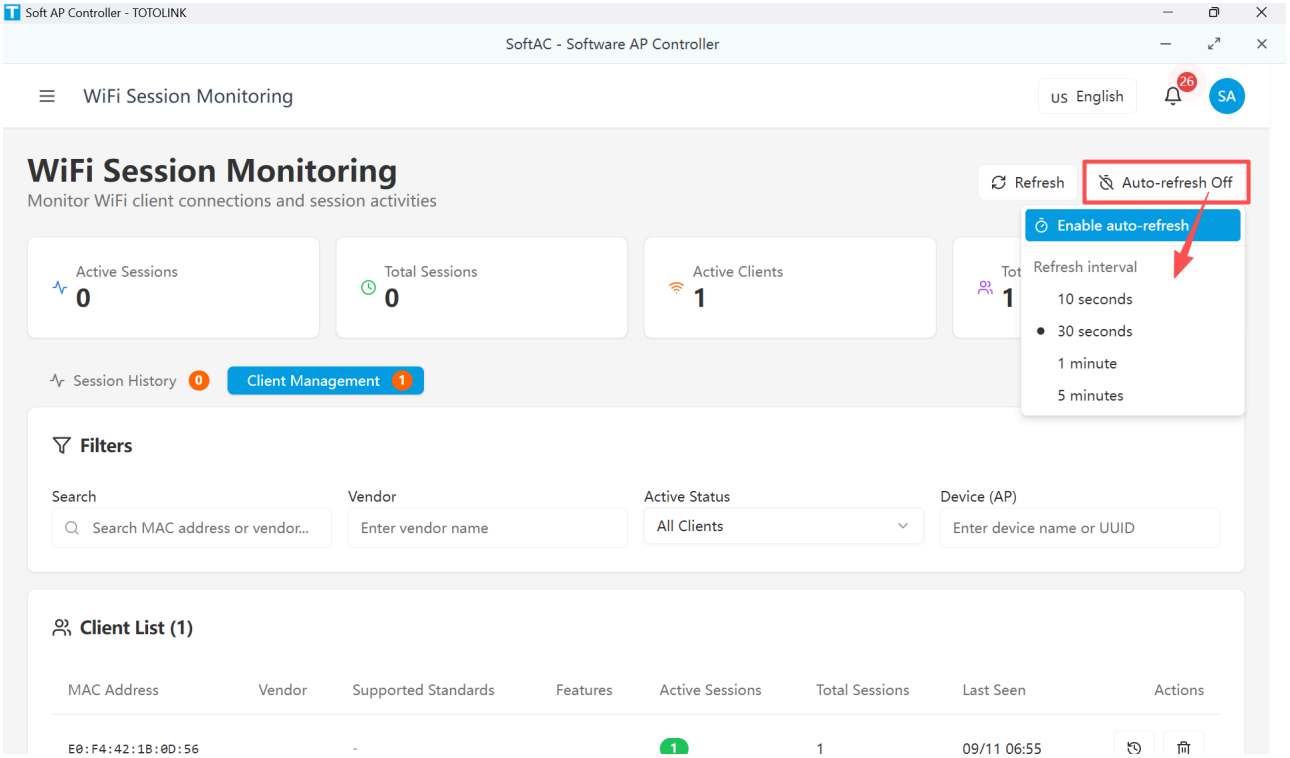
2. **Search Clients**
   Use the search box to quickly find clients by:
   - MAC address
   - Vendor name (e.g., "Apple", "Samsung")
   - Device hostname



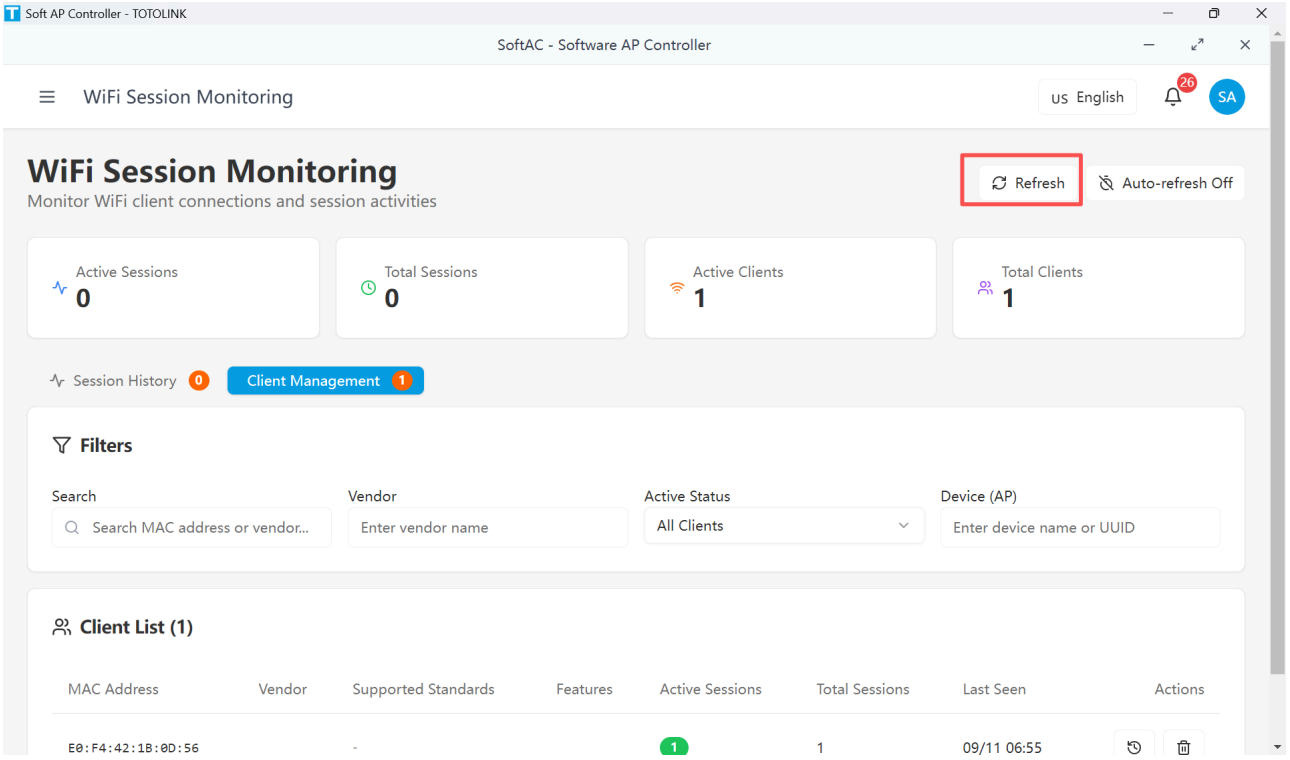
Real-time Updates

The online users display supports automatic refresh:

1. **Enable Auto-refresh**
   Click the timer icon in the top-right corner and select your preferred interval:
   - 10 seconds (for active monitoring)
   - 30 seconds (default)
   - 1 minute (for general monitoring)
   - 5 minutes (for low-traffic networks)



2. **Manual Refresh**
   Click the refresh button at any time for immediate update.



> 💡 **Best Practice**: Use 10-second refresh during troubleshooting to see real-time changes, but switch to longer intervals during normal operation to reduce system load.

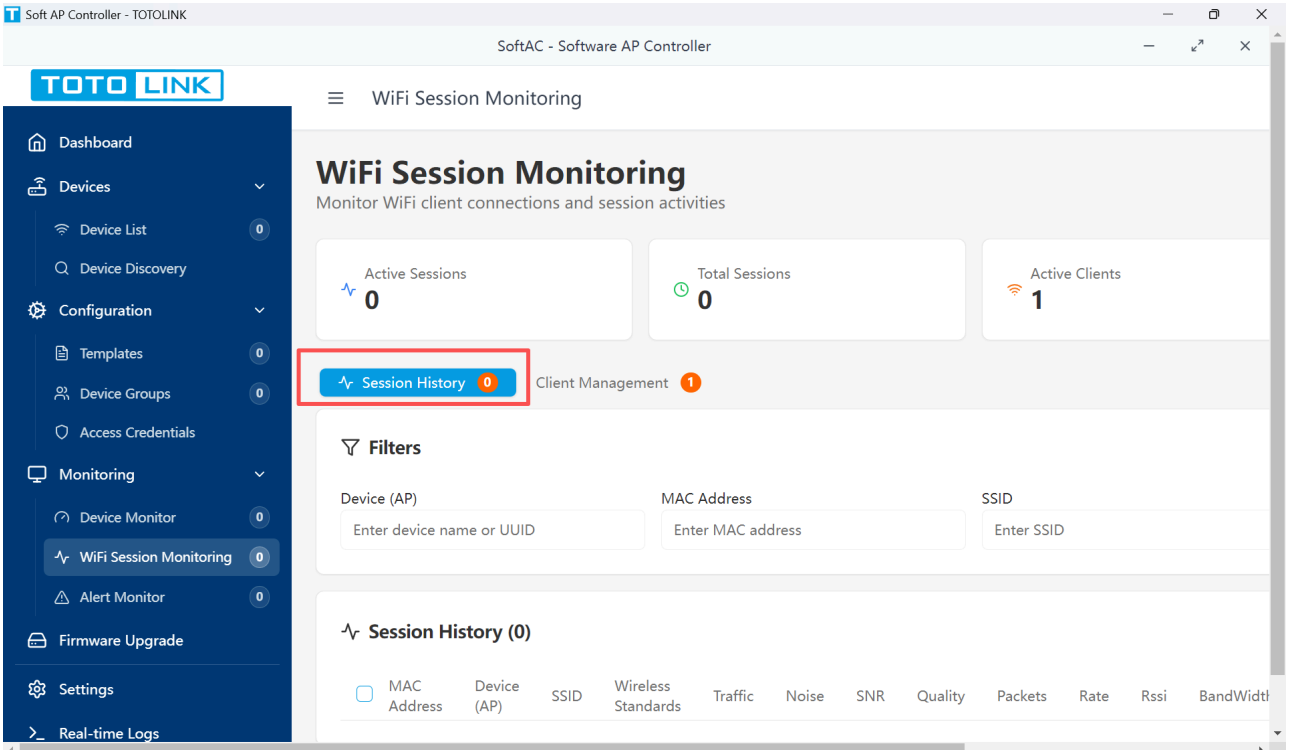
7.2.2 Session Details

Understanding Session Information

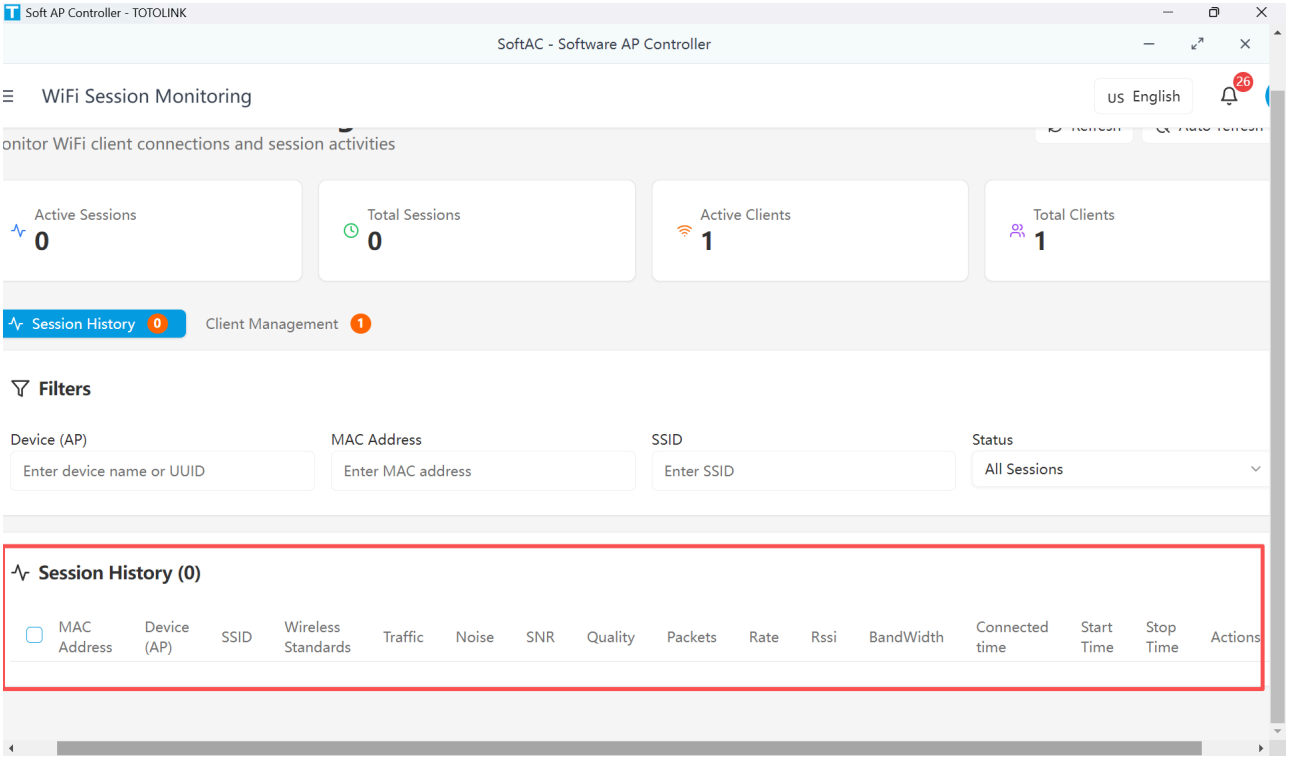
Each WiFi session contains detailed technical information that helps you understand connection quality, diagnose issues, and optimize network performance. TOTOLINK SoftAC captures comprehensive data for every client connection.

Viewing Session Details

1. **Access Session History**
   In the WiFi Sessions page, click the "Session History" tab to view all sessions (active and completed).



2. **Session Information Table**
   The detailed view shows extensive technical data for each session:



Technical Metrics Explained

Connection Metrics

Metric	Description	What It Tells You
RSSI	Received Signal Strength Indicator	Client's signal reception quality
Noise	Background RF interference level	Environmental interference affecting connection
SNR	Signal-to-Noise Ratio	Overall connection quality (higher is better)
Quality	Connection quality percentage	Quick assessment of link reliability

Performance Metrics

Metric	Description	Typical Values
TX Rate	Transmission speed in Mbps	150-1200 Mbps depending on WiFi standard
Bandwidth	Channel width (20/40/80 MHz)	Wider channels = higher potential speed
Packets	TX/RX packet counts	High packet loss indicates problems

Troubleshooting with Session Details

Use session information to diagnose common issues:

Poor Performance Checklist

- [ ] Check RSSI (should be above -70 dBm)
- [ ] Review SNR (should be above 20 dB)
- [ ] Verify TX Rate matches client capabilities
- [ ] Look for high packet counts with retransmissions
- [ ] Check if multiple clients on same AP

Connection Drops Checklist

- [ ] Review signal strength over time
- [ ] Check for noise spikes
- [ ] Verify session duration patterns
- [ ] Look for authentication issues

Best Practices

Daily Monitoring Routine

1. **Morning Check** (5 minutes)
    - Review overnight alerts
    - Check active user count
    - Verify all APs online
2. **Midday Review** (10 minutes)
    - Monitor peak usage
    - Check for connection issues
    - Review any user complaints
3. **End of Day** (5 minutes)
    - Note any recurring issues
    - Export daily statistics
    - Plan next day's maintenance

Performance Optimization

> 💡 **Pro Tip**: Use WiFi session data to make informed decisions about network configuration:

1. **Load Balancing**
    - Identify overloaded access points
    - Redistribute clients using band steering
    - Adjust AP power levels
2. **Coverage Optimization**

    - Find areas with weak signals
    - Add APs where needed
    - Adjust antenna orientation
3. **Channel Planning**
    - Identify interference patterns
    - Optimize channel allocation
    - Implement DFS channels if supported

Troubleshooting Guide

Problem	Check in Session Management	Solution
Slow speeds	TX Rate, Signal Strength	Move closer to AP or add repeater
Frequent disconnects	Session duration, Signal quality	Check for interference, update drivers
Can't connect	Client not in list	Verify credentials, check MAC filtering
High latency	Packet statistics, SNR	Reduce interference, check AP load

---

Related Features

- 7.1 Device Monitoring - Monitor access point health
- 7.3 Alert Management - Set up notifications for WiFi issues
- 8. Firmware Management - Keep devices updated for best performance
- 11.4 Backup & Recovery - Backup session data and configurations

---

Summary

WiFi Session Management in TOTOLINK SoftAC provides powerful tools to monitor, analyze, and optimize your wireless network. By understanding online users, analyzing session details, and tracking user behavior, you can ensure reliable connectivity and superior user experience across your entire network.

7.3 Alert Management

Overview

The Alert Management feature in TOTOLINK SoftAC helps you proactively monitor your network devices and receive timely notifications when issues arise. This system automatically detects problems, sends alerts, and helps you maintain a healthy network infrastructure without constant manual monitoring.

Key Benefits

- **24/7 Automated Monitoring**: The system continuously monitors your devices even when you're away
- **Early Problem Detection**: Catch issues before they become critical failures

- **Customizable Notifications**: Choose how you want to be notified about network events
- **Historical Tracking**: Review past alerts to identify patterns and recurring issues

---

7.3.1 Alert Rules

Understanding Alert Rules

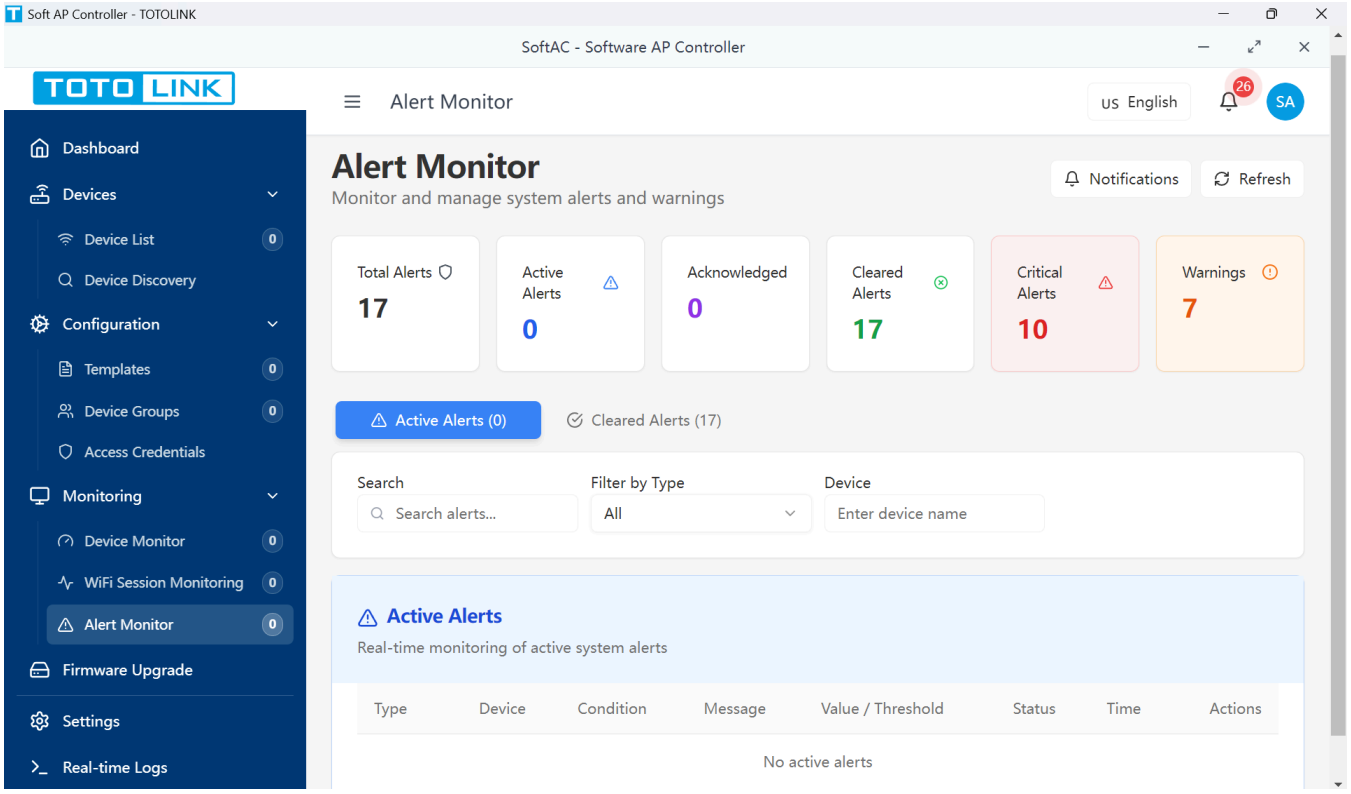
Alert rules are pre-configured conditions that trigger notifications when specific thresholds are exceeded. TOTOLINK SoftAC monitors your devices continuously and automatically generates alerts based on these rules.

Available Alert Types

The system monitors the following conditions and generates alerts accordingly:

Device Health Alerts

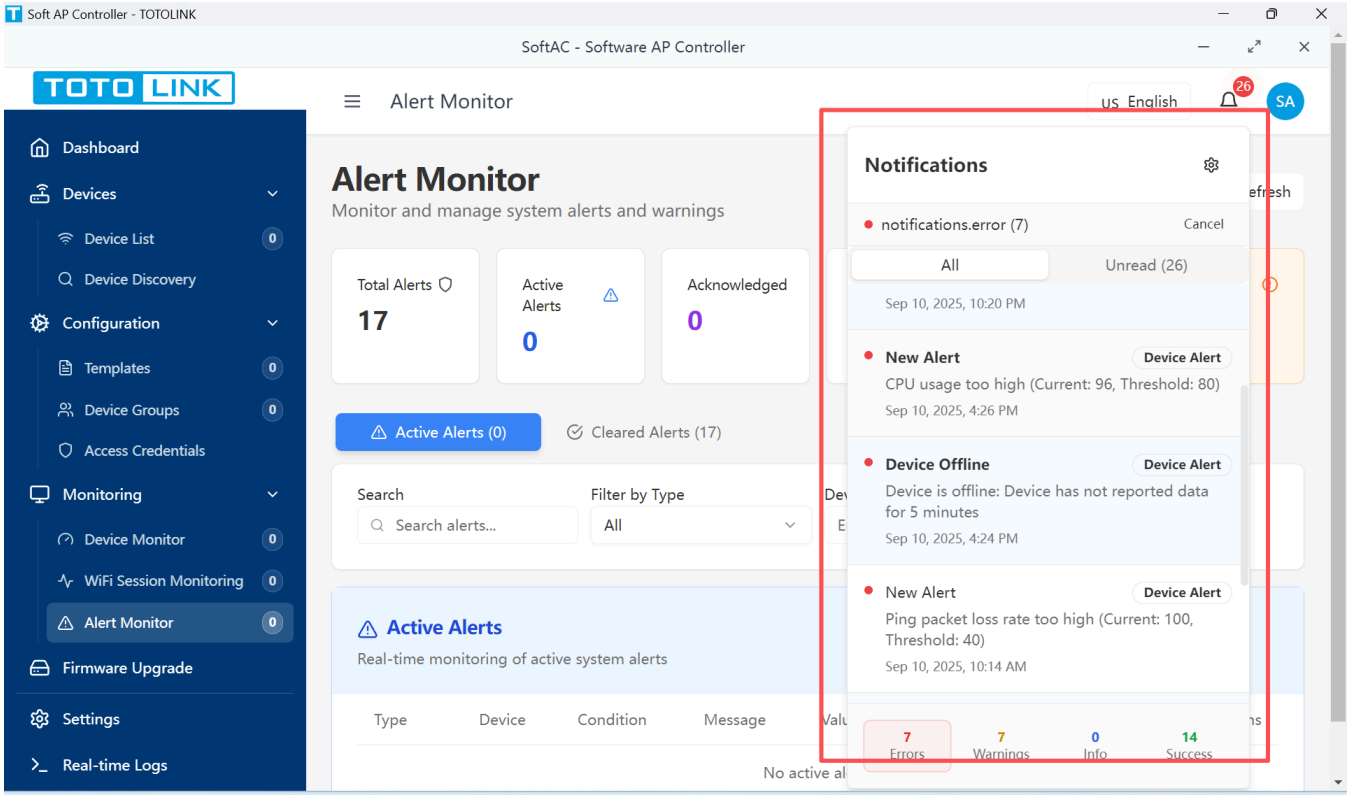
Alert Type	Description	When It Triggers
Device Offline	Device has stopped responding	No data received for 5+ minutes
Device Problem	Device experiencing issues	Delayed reporting or resource problems



Performance Alerts

Alert Type	Default Threshold	Severity	Description
High CPU Usage	80%	Critical	Device processor is overloaded
High Memory Usage	92%	Critical	Device running out of memory

Alert Type	Default Threshold	Severity	Description
Network Packet Loss	40%	Warning	Poor network connectivity
Low Signal Strength	-70 dBm	Warning	Weak WiFi signal quality
High Client Count	100 devices	Warning	Too many connected clients



How Alert Rules Work

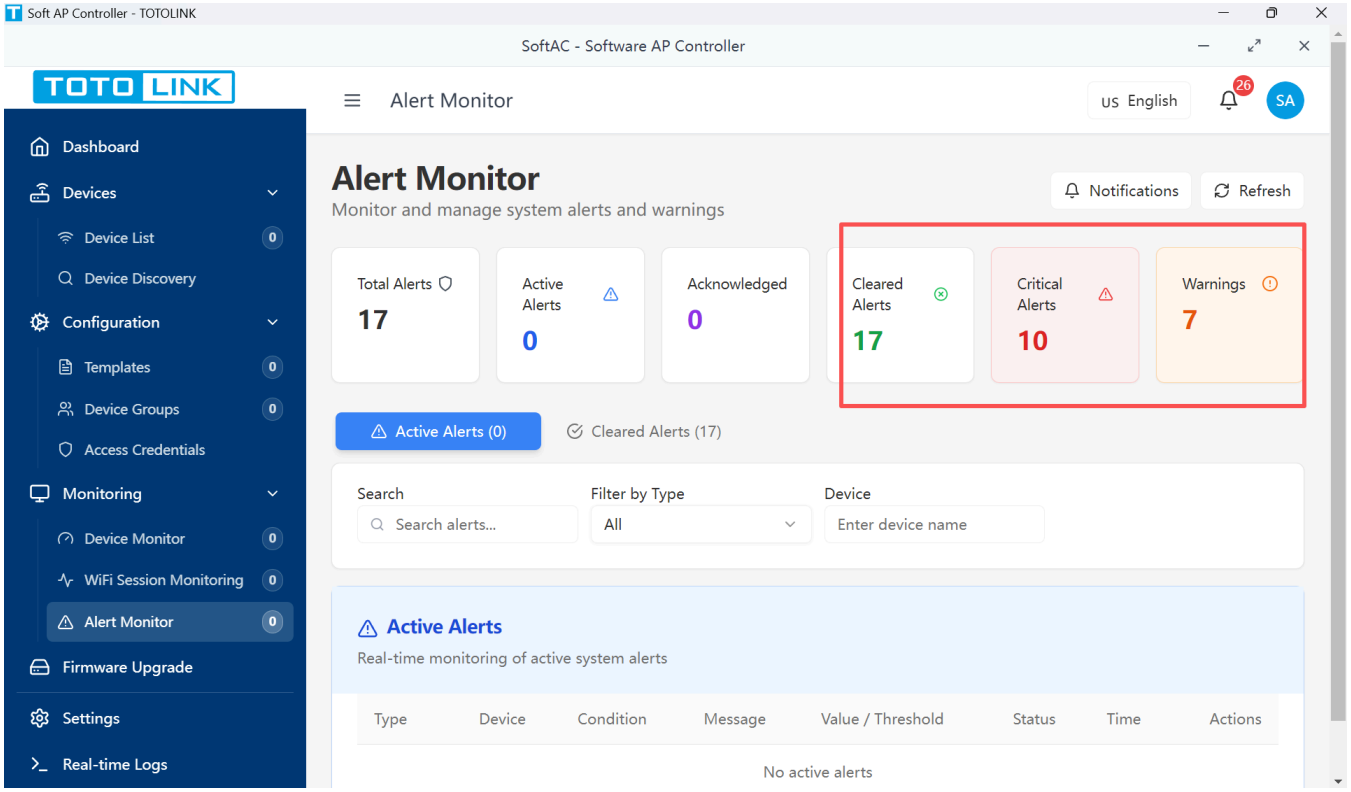
1. **Continuous Monitoring**
   The system checks device metrics every 2-3 minutes
2. **Threshold Comparison**
   Current values are compared against configured thresholds
3. **Alert Generation**
   When a threshold is exceeded, an alert is automatically created
4. **Auto-Recovery Detection**
   Alerts are automatically cleared when conditions return to normal

> 💡 **Tip**: Alert thresholds are optimized for typical network environments. Most users won't need to adjust these settings.

Alert Severity Levels

Alerts are categorized by severity to help you prioritize responses:

- 🔴 **Critical**: Immediate attention required (device offline, very high resource usage)
- 🟡 **Warning**: Monitor closely, may need action soon (moderate issues)
- 🟢 **Cleared**: Previously active alert that has been resolved



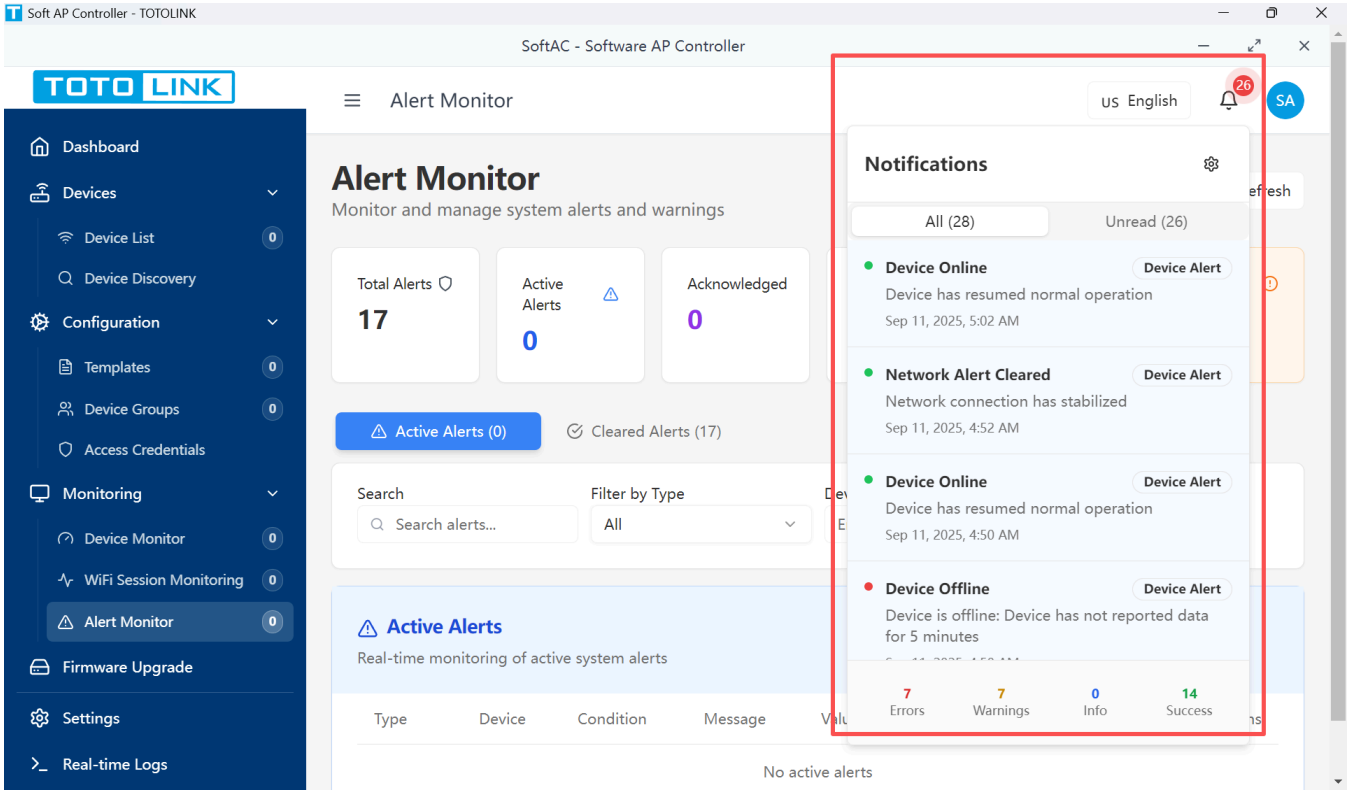
7.3.2 Alert Notifications

Notification Channels

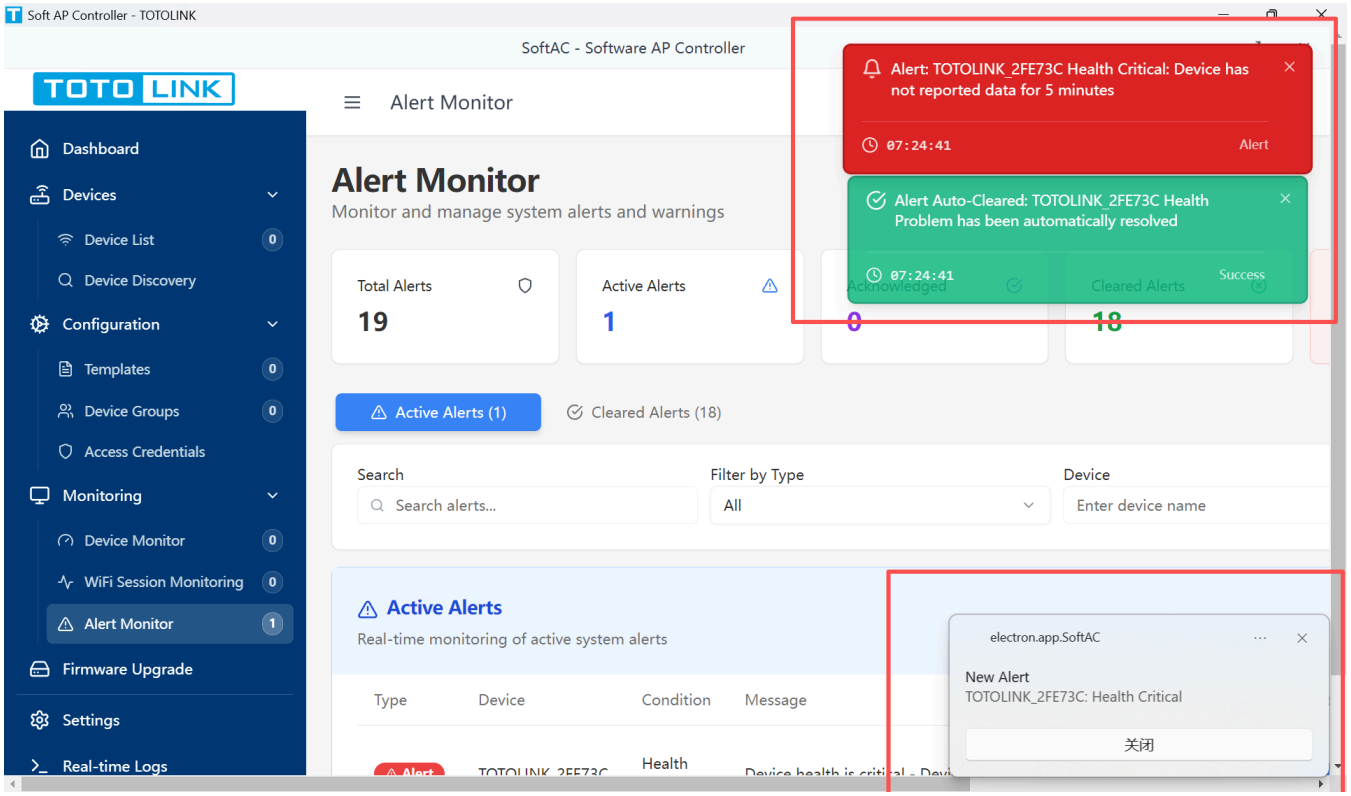
TOTOLINK SoftAC provides multiple ways to notify you about alerts, ensuring you never miss critical network events.

Available Notification Methods

1. **In-Application Notifications**
    - Bell icon in the top navigation shows unread count
    - Real-time updates without page refresh
    - Click to view full alert details



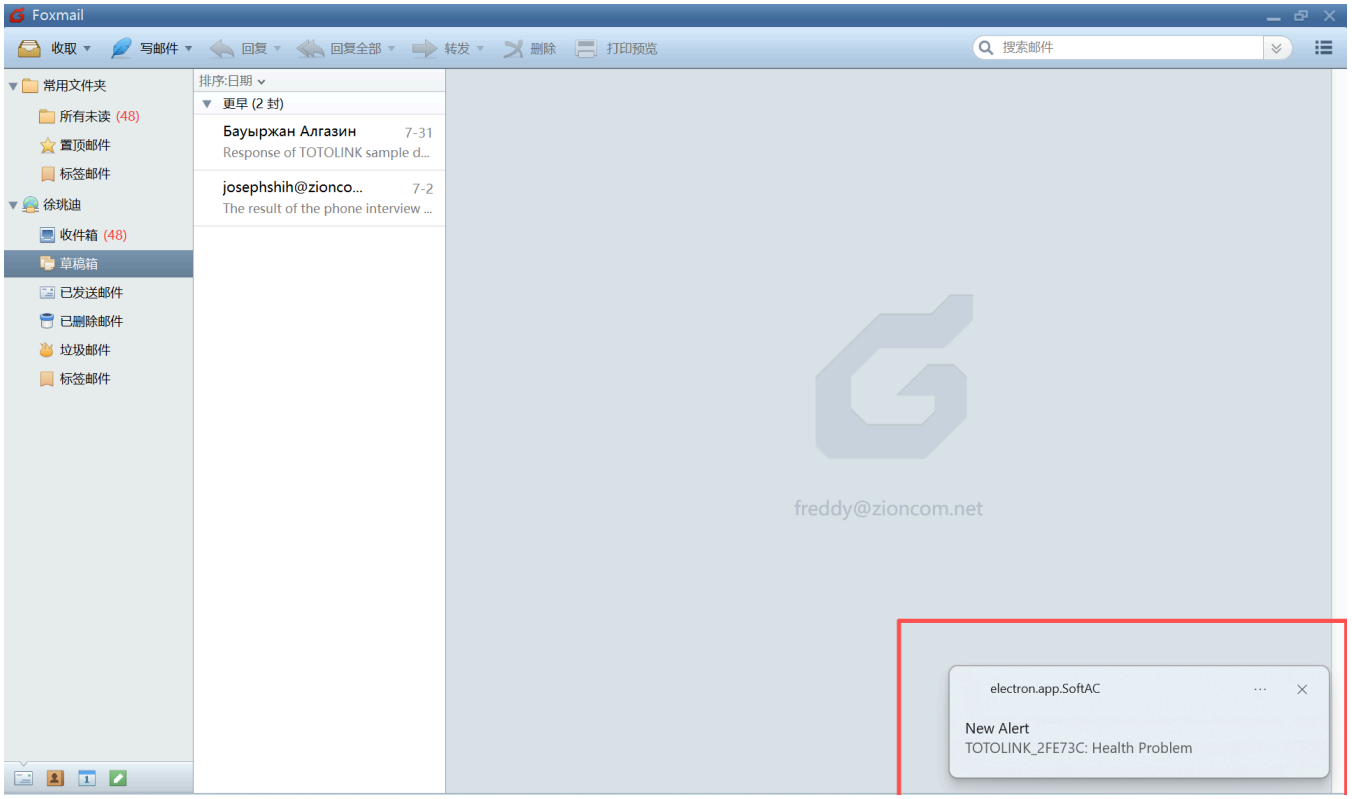
2. **Toast Notifications**
   - Pop-up messages appear in the corner of your screen
   - Shows alert summary with device name and issue
   - Click to navigate directly to the alert



3. **Sound Alerts**
   - Audible notification when new alerts arrive
   - Different sounds for different severity levels

- Can be muted during presentations or meetings

4. **Desktop Notifications**
   - System-level notifications outside the browser
   - Works even when SoftAC is minimized
   - Requires one-time browser permission

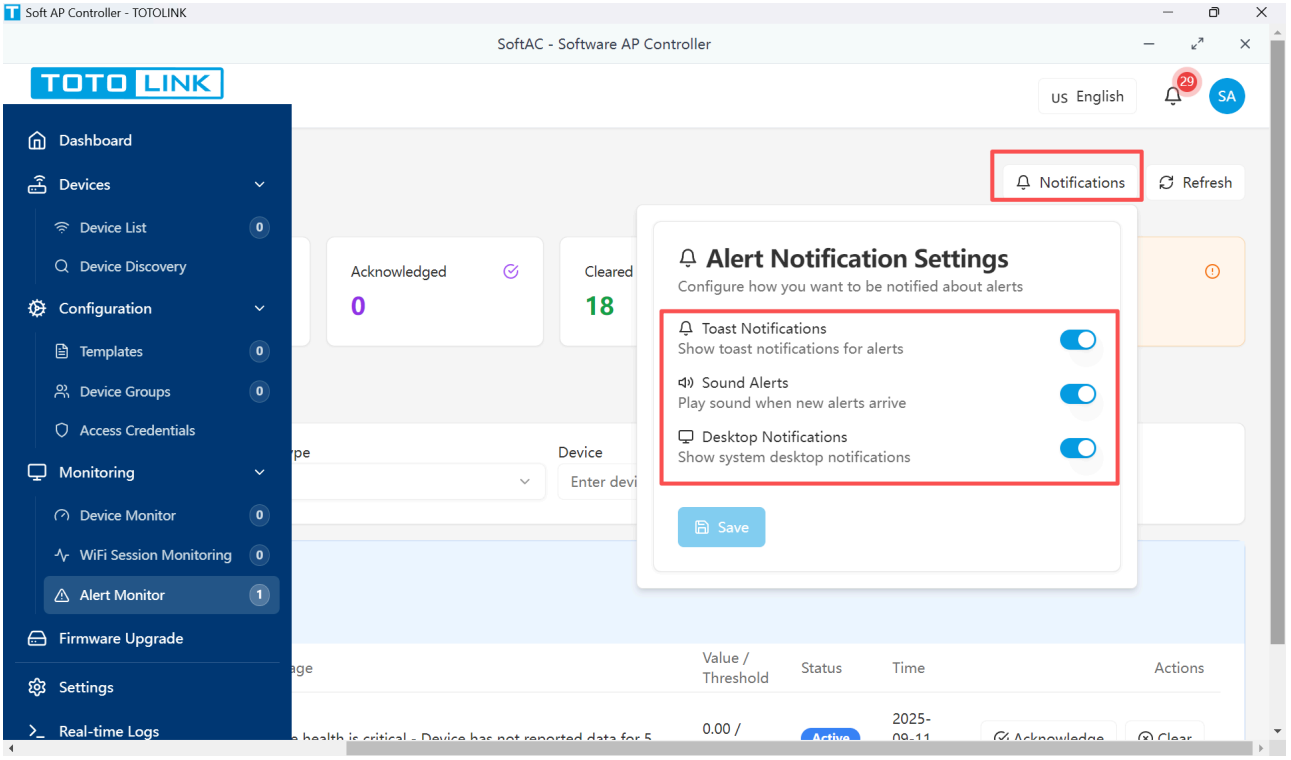


5. **Email Notifications** (when configured)
   - Sent to administrator email address
   - Includes alert details and direct link to system
   - Useful for after-hours monitoring

Configuring Notification Preferences

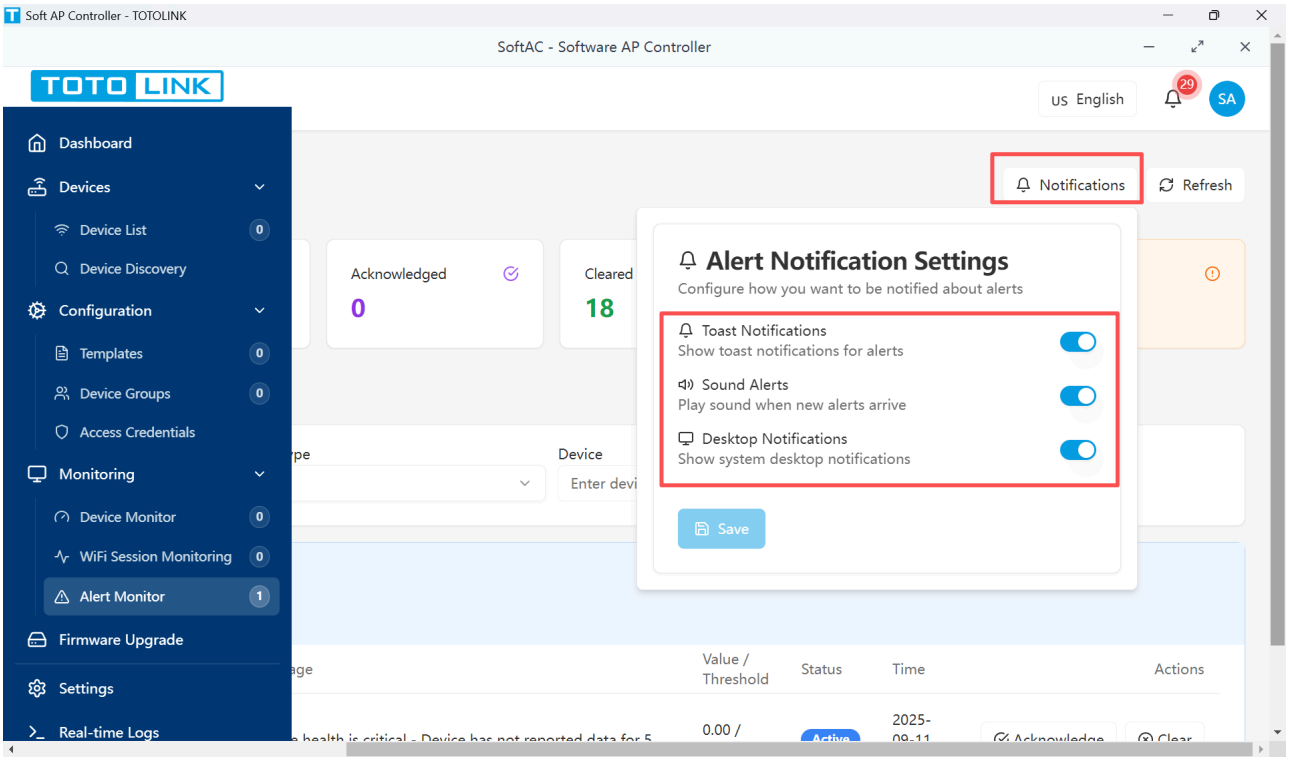
To customize how you receive alerts:

1. **Access Notification Settings**
   Click the bell icon in the alert monitor page.



2. **Toggle Notification Types**
   Enable or disable each notification method according to your preferences:

Setting	Description	Recommended
Toast Notifications	Pop-up messages in the app	✅ Always On
Sound Alerts	Audio notifications	✅ During work hours
Desktop Notifications	System notifications	✅ For critical alerts



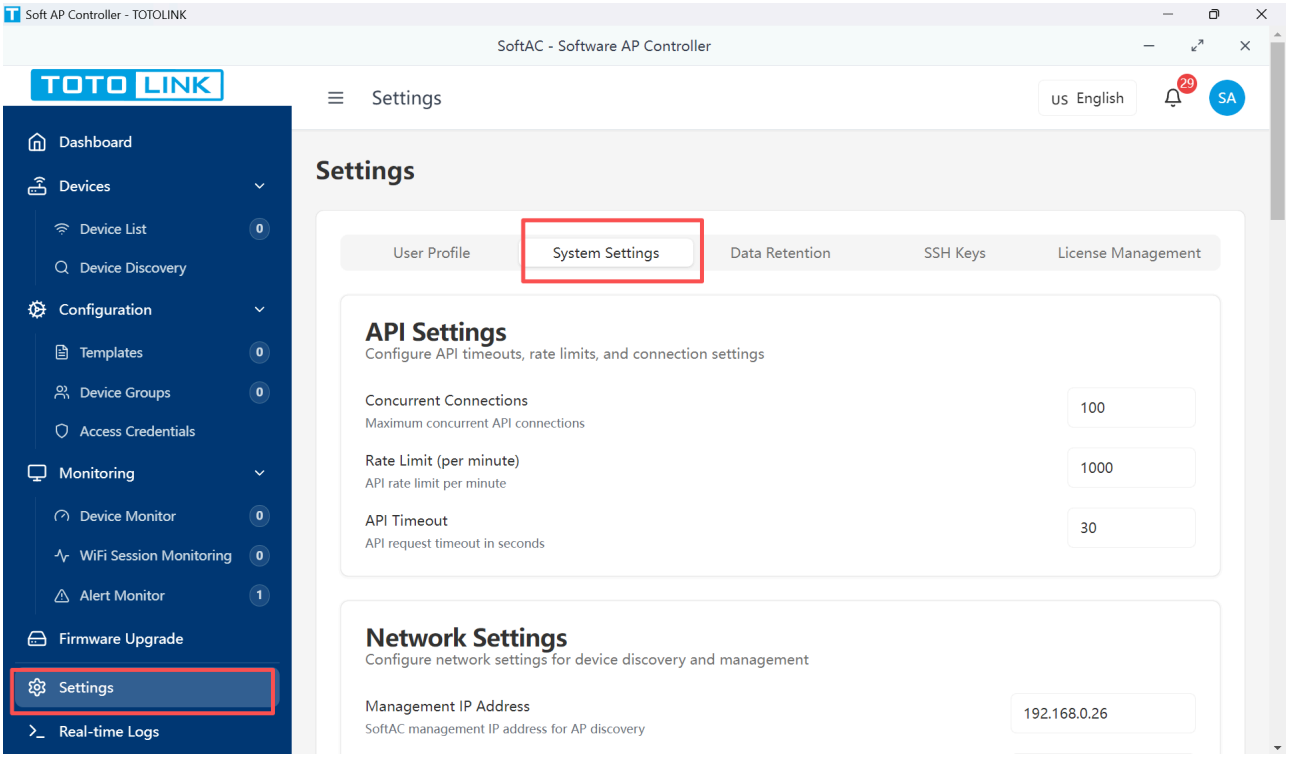
3. **Save Your Preferences**
   Click "Save" to apply your notification settings

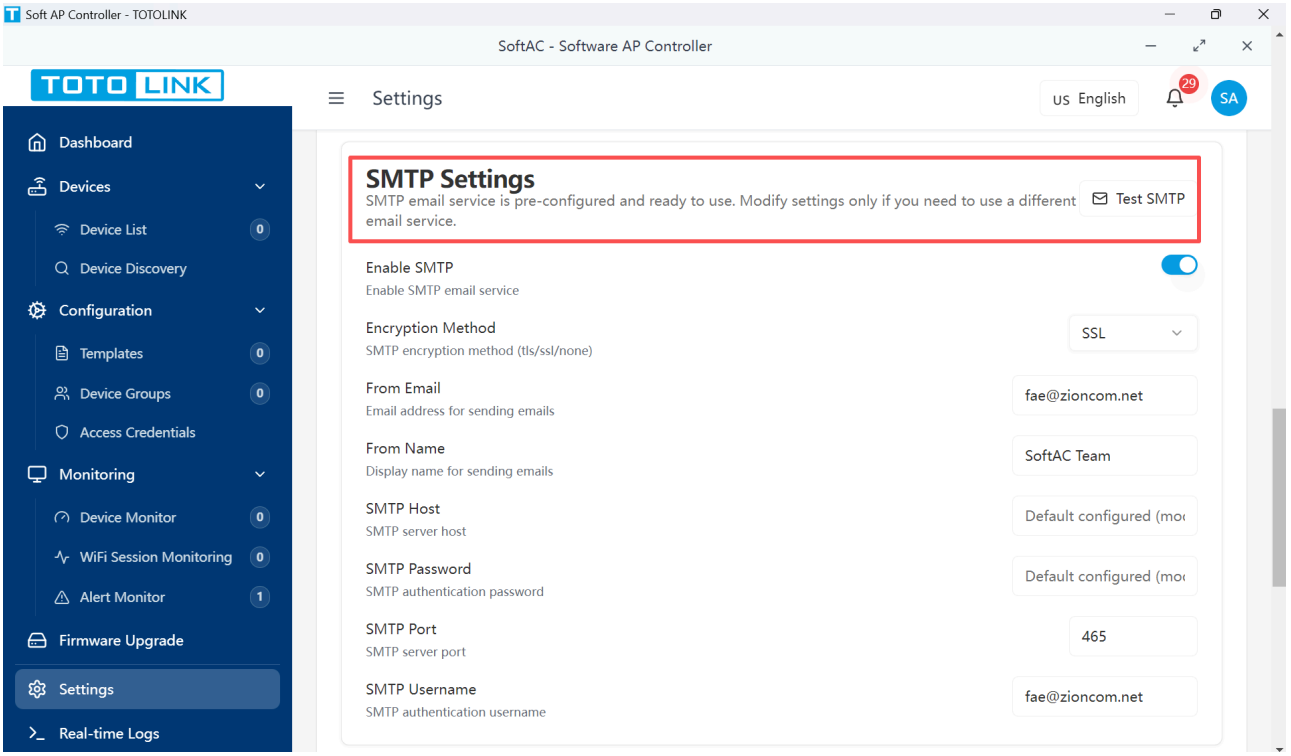
> ✅ **Success**: Your preferences are saved locally and will persist across sessions

Setting Up Email Notifications

For 24/7 monitoring, configure email alerts:

1. **Navigate to System Settings**
   Go to Settings → System Settings → SMTP Settings

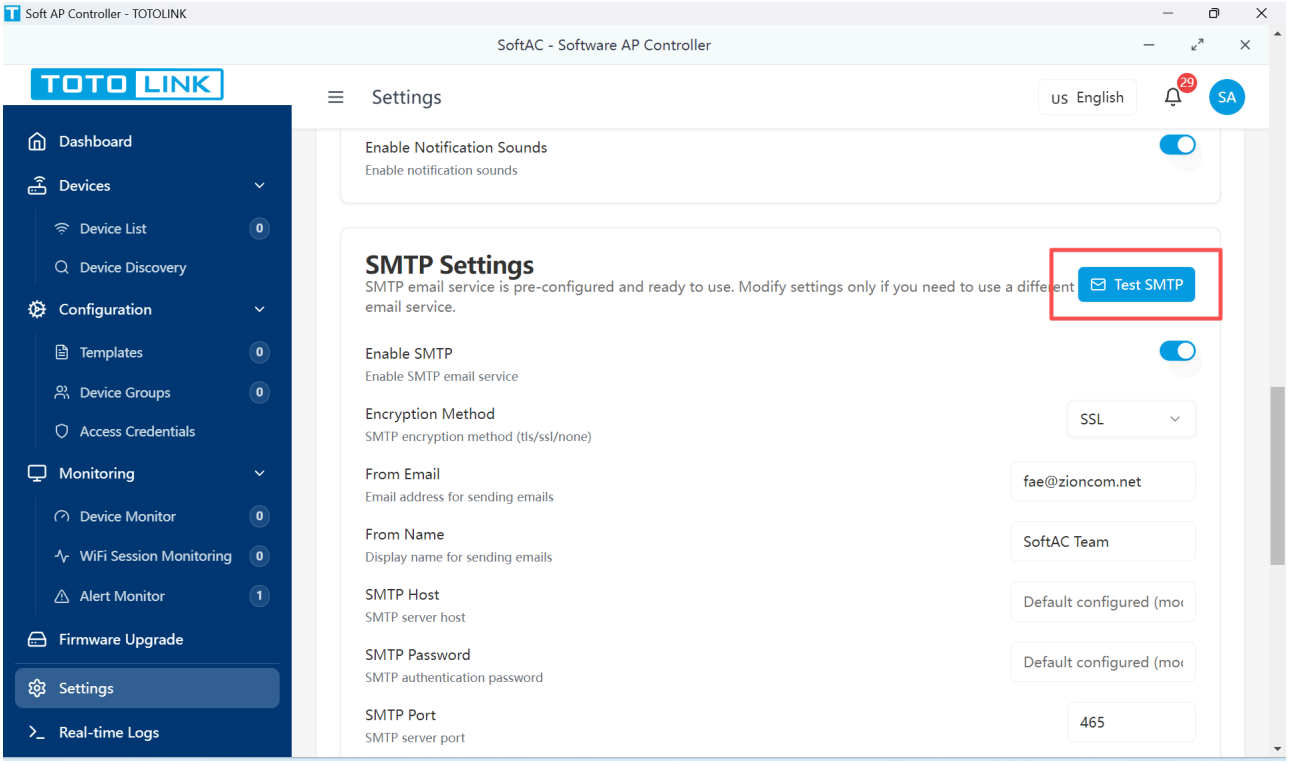




2. **Enter SMTP Details**
   Fill in your email server information:

Field	Description	Example
SMTP Server	Your mail server address	smtp.gmail.com
Port	Mail server port	587 (TLS) or 465 (SSL)
Username	Email account username	admin@company.com
Password	Email account password	••••••••
From Email	Sender address	noreply@company.com
Encryption	Security method	TLS/SSL

3. **Test Configuration**
   Click "Test SMTP" to verify settings



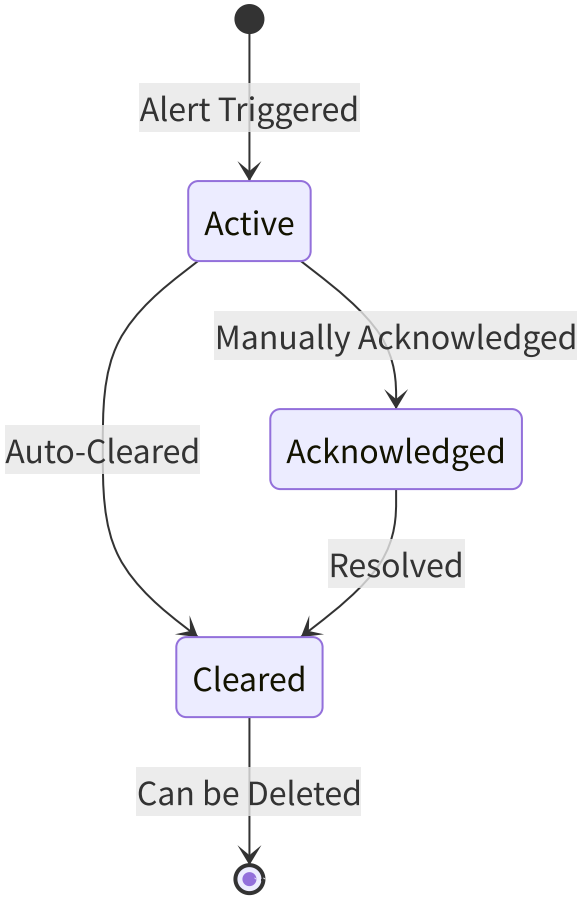
4. **Enable Email Alerts**
   Toggle "Enable Email Notifications" to activate

> ⚠️ **Important**: Email notifications require valid SMTP credentials. Contact your IT administrator if you need assistance with mail server settings.

7.3.3 Alert Handling

Understanding Alert States

Each alert progresses through different states during its lifecycle:

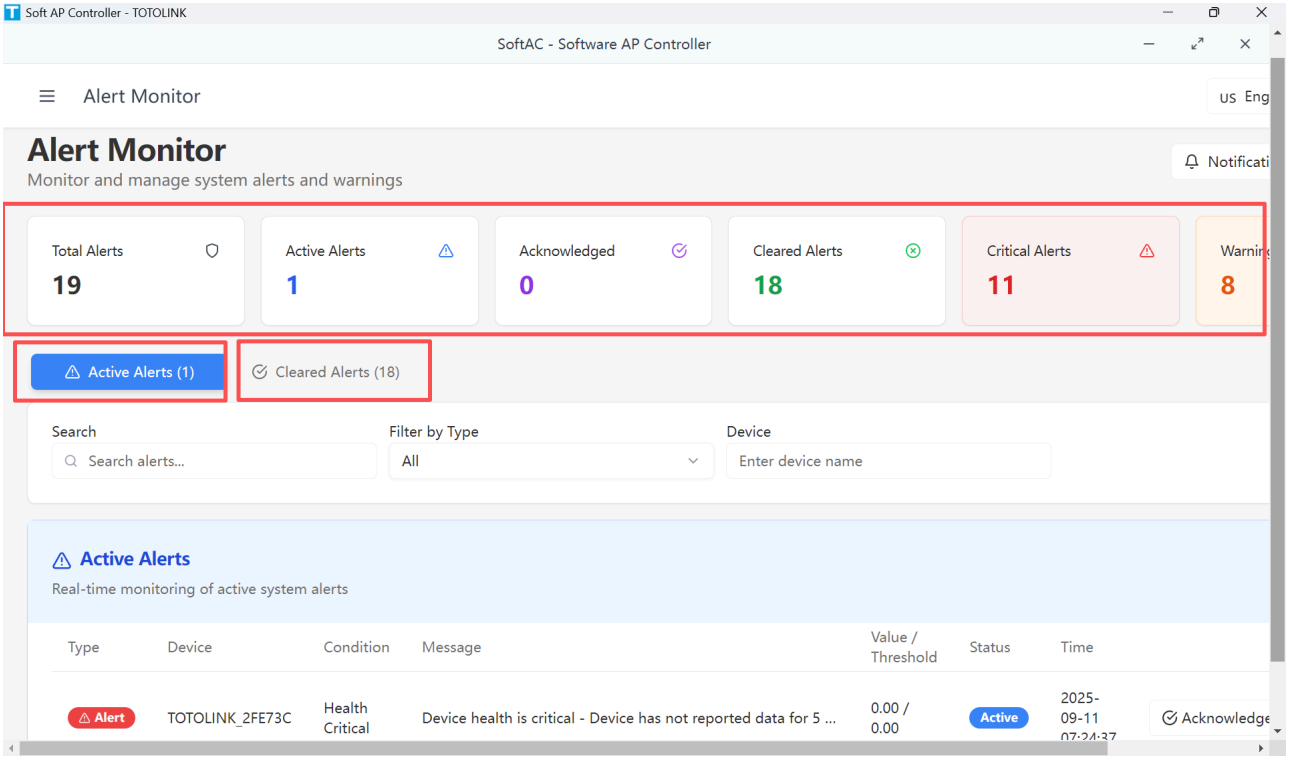


State	Description	Action Required
Active	New alert requiring attention	Review and acknowledge
Acknowledged	Alert seen but not yet resolved	Monitor and resolve issue
Cleared	Issue has been resolved	No action needed

Viewing and Managing Alerts

Accessing the Alert Monitor

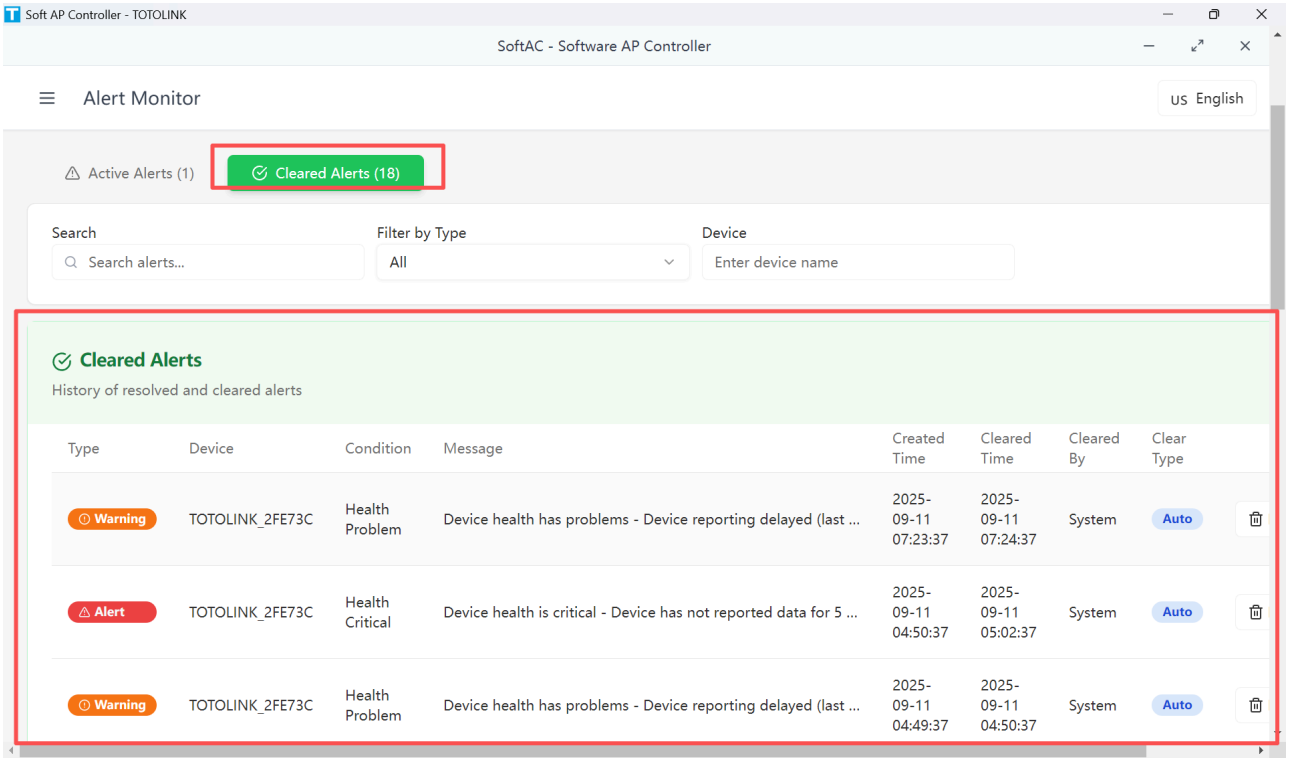
1. Click "Alert Monitor" in the main navigation menu
2. The Alert Monitor dashboard displays:
    - **Alert Statistics**: Overview cards showing total, active, and cleared alerts
    - **Active Alerts Tab**: Current issues requiring attention
    - **Cleared Alerts Tab**: Historical resolved alerts



Managing Alert History

Reviewing Cleared Alerts

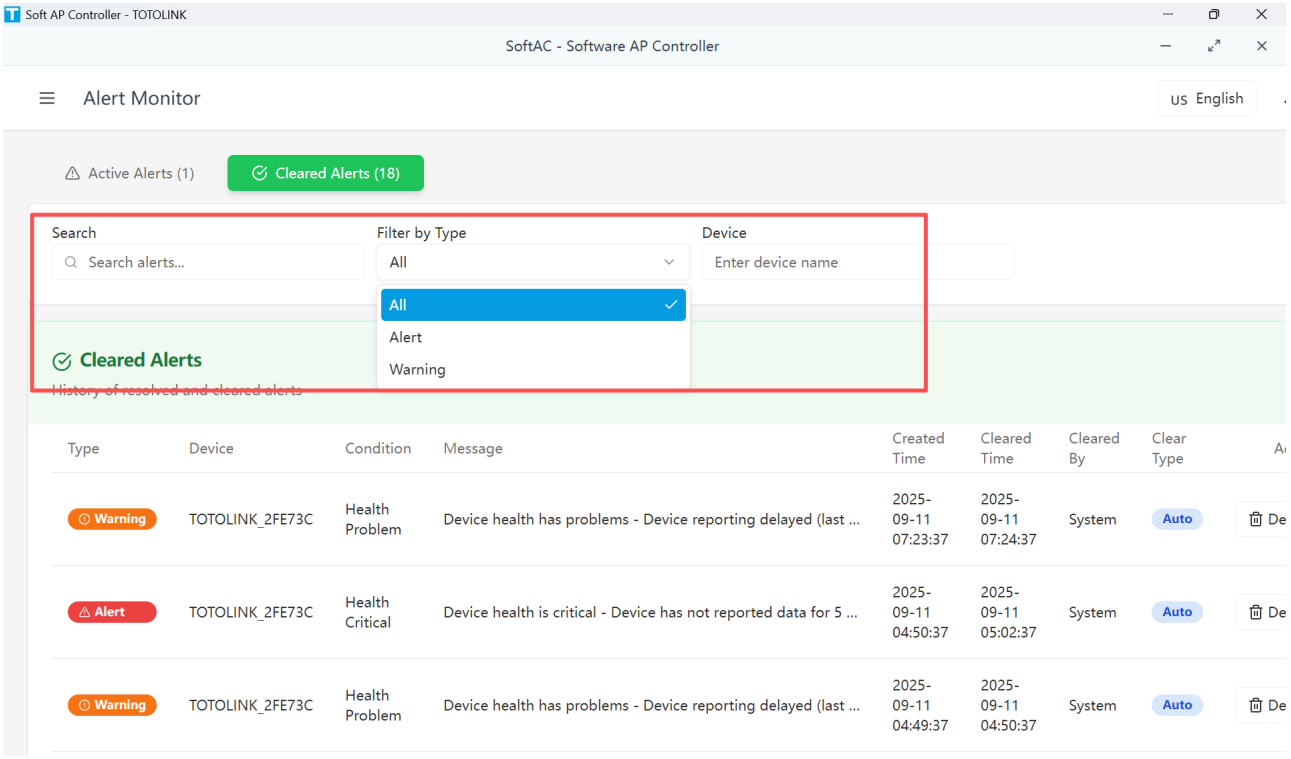
1. Click the "Cleared" tab in Alert Monitor
2. View historical alerts with:
    - Resolution time
    - Clear type (Auto/Manual)
    - Duration of the issue



Filtering and Searching

Find specific alerts quickly:

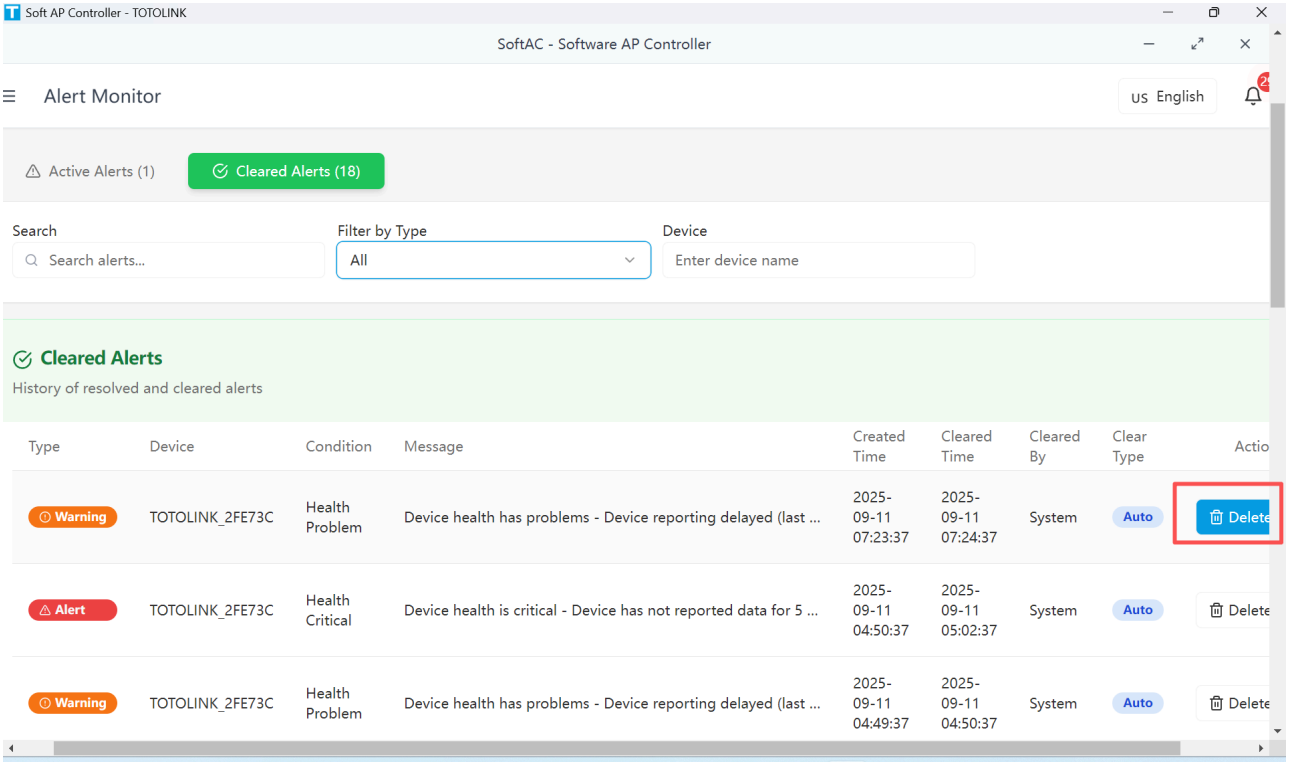
1. **Search Box**: Type device name or alert message
2. **Type Filter**: Show only specific alert types
3. **Date Range**: View alerts from specific time periods



Deleting Old Alerts

To clean up resolved alerts:

1. Select alerts in the "Cleared" tab
2. Click the trash icon
3. Confirm deletion



> ⚠️ **Warning**: Deleted alerts cannot be recovered. Only delete alerts you're certain you won't need for reporting.

Alert Response Best Practices

Priority Response Guide

Follow this guide to handle alerts effectively:

Alert Type	Response Time	Recommended Action
Device Offline	Immediate	1. Check network connectivity 2. Verify device power 3. Restart if necessary
High CPU/Memory	Within 15 min	1. Check running processes 2. Review connected clients 3. Schedule restart if needed
Packet Loss	Within 30 min	1. Check cable connections 2. Review interference 3. Adjust channel settings
High Client Count	Within 1 hour	1. Review client list 2. Check for unauthorized access 3. Consider load balancing

Creating Standard Operating Procedures

Develop response procedures for common alerts:

1. **Document Common Issues**
   Keep notes on frequently occurring alerts and their solutions
2. **Create Quick Actions**
   Prepare standard responses for typical problems
3. **Train Team Members**
   Ensure all administrators know how to handle alerts

Troubleshooting Alert Issues

Not Receiving Notifications?

- Check notification settings are enabled
- Verify browser permissions for desktop notifications
- Ensure email configuration is correct (if using email alerts)
- Check that devices are reporting data regularly

Too Many False Alerts?

- Review if thresholds match your environment
- Check for network instability causing intermittent issues
- Ensure devices have stable power supply
- Verify time synchronization across devices

Alerts Not Clearing Automatically?

- Confirm the issue has actually been resolved
- Check device is reporting current data
- Wait 5-10 minutes for the system to detect recovery
- Manually clear if the issue is confirmed resolved

Summary

The Alert Management system in TOTOLINK SoftAC provides comprehensive monitoring and notification capabilities to help you maintain a healthy network. By understanding alert rules, configuring appropriate notifications, and following proper alert handling procedures, you can quickly identify and resolve network issues before they impact your users.

Quick Reference

- **Alert Rules**: Automatically monitor device health, performance, and connectivity
- **Notifications**: Multiple channels including in-app, sound, desktop, and email
- **Alert States**: Active → Acknowledged → Cleared
- **Best Practice**: Acknowledge alerts promptly and document recurring issues

> 🚀 **Next Steps**: Configure your notification preferences and set up email alerts for 24/7 monitoring coverage.

Related Topics

- 7.1 Device Monitoring - Real-time device status monitoring
- 7.2 WiFi Session Management - Track connected clients
- 11.3 Notification Settings - System-wide notification configuration
- 14.1 Troubleshooting Connection Issues - Resolving device connectivity problems

Part 8: Firmware Upgrade

Feature Overview

The Firmware Upgrade feature in TOTOLINK SoftAC allows you to centrally manage, distribute, and upgrade firmware across all your network devices. This ensures your devices run the latest software with improved features, security patches, and bug fixes. The system provides a safe and controlled upgrade process with monitoring capabilities and rollback options.

Use Cases

- **Security Updates**: Deploy critical security patches across all devices to protect your network
- **Feature Rollout**: Upgrade devices to access new functionality and improvements
- **Standardization**: Ensure all devices in a network segment run the same firmware version
- **Maintenance Windows**: Schedule upgrades during off-peak hours to minimize disruption
- **Testing Deployment**: Test new firmware on select devices before network-wide rollout

---

8.1 Firmware Version Viewing

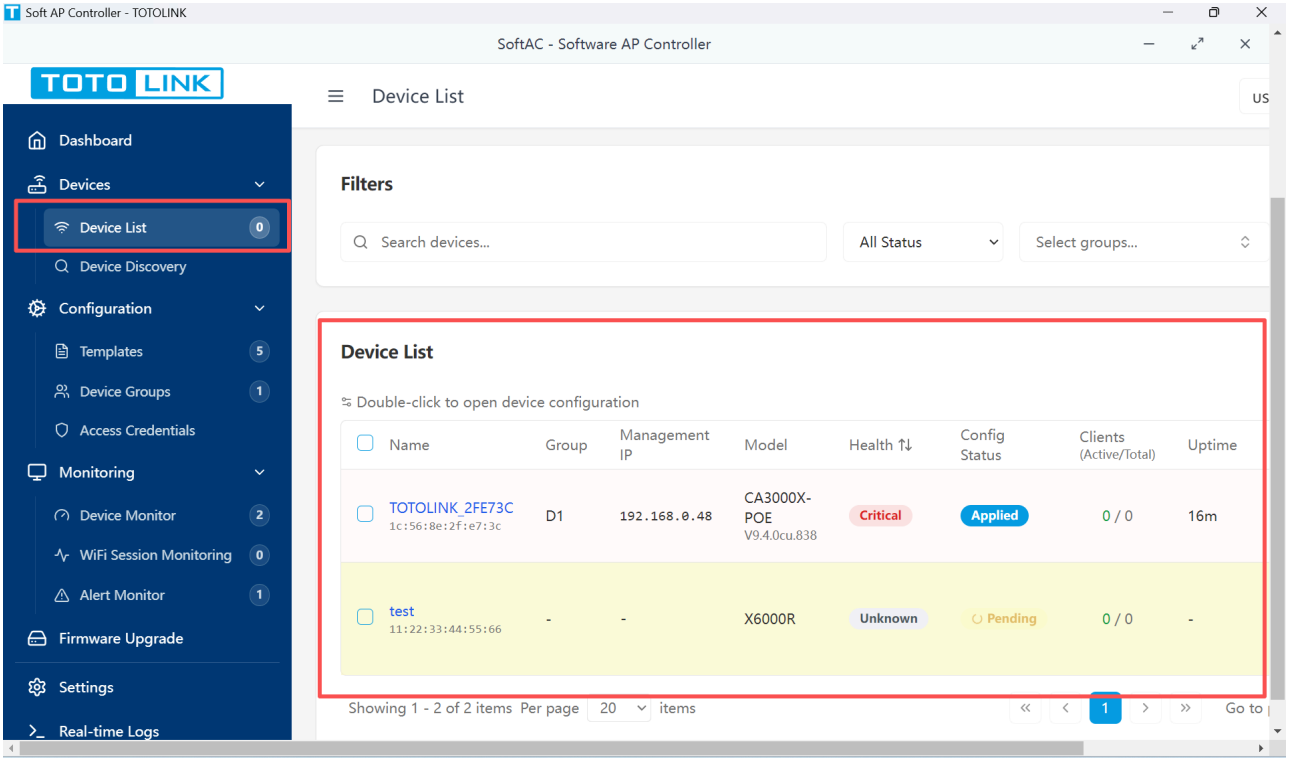
Feature Overview

View and monitor the current firmware versions running on all your devices from a centralized dashboard. This helps you identify outdated devices and plan upgrade strategies.

Accessing Firmware Information

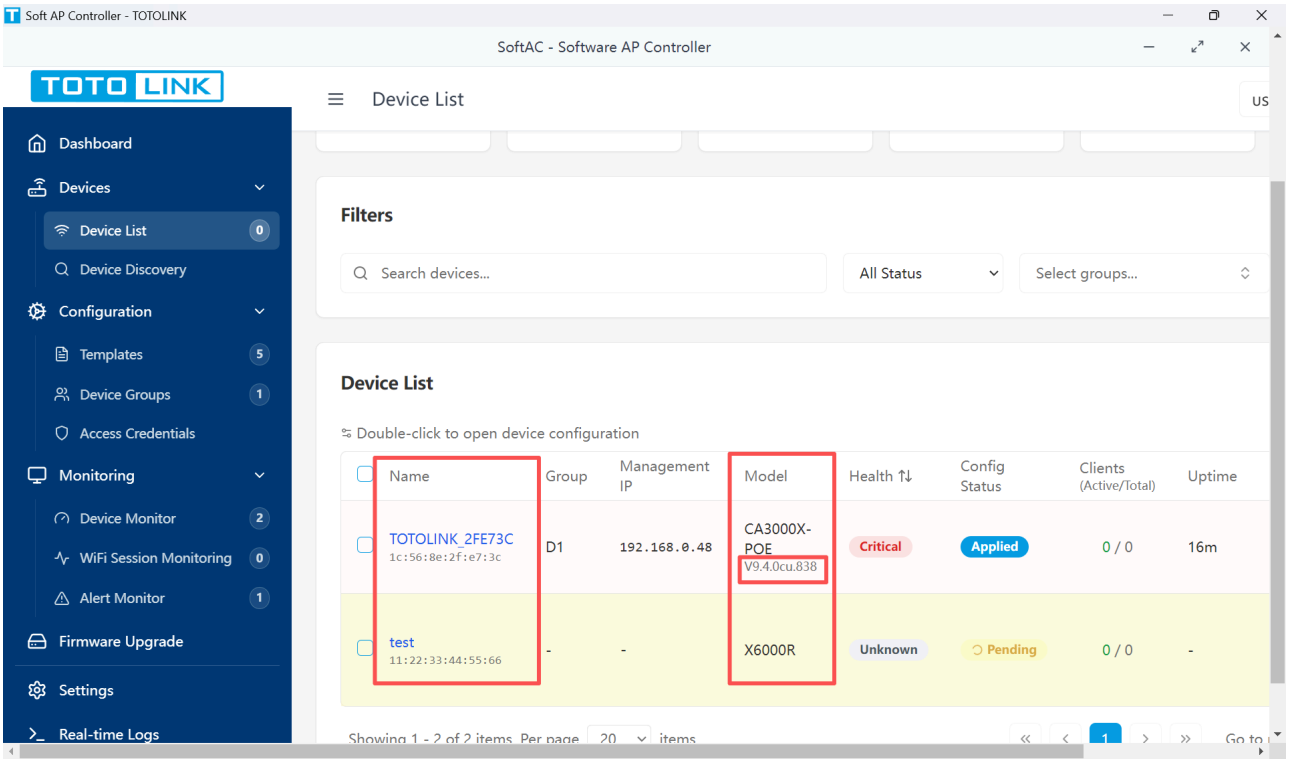
From Device List

1. **Navigate to Device List**
   Click "Device List" in the left navigation menu.



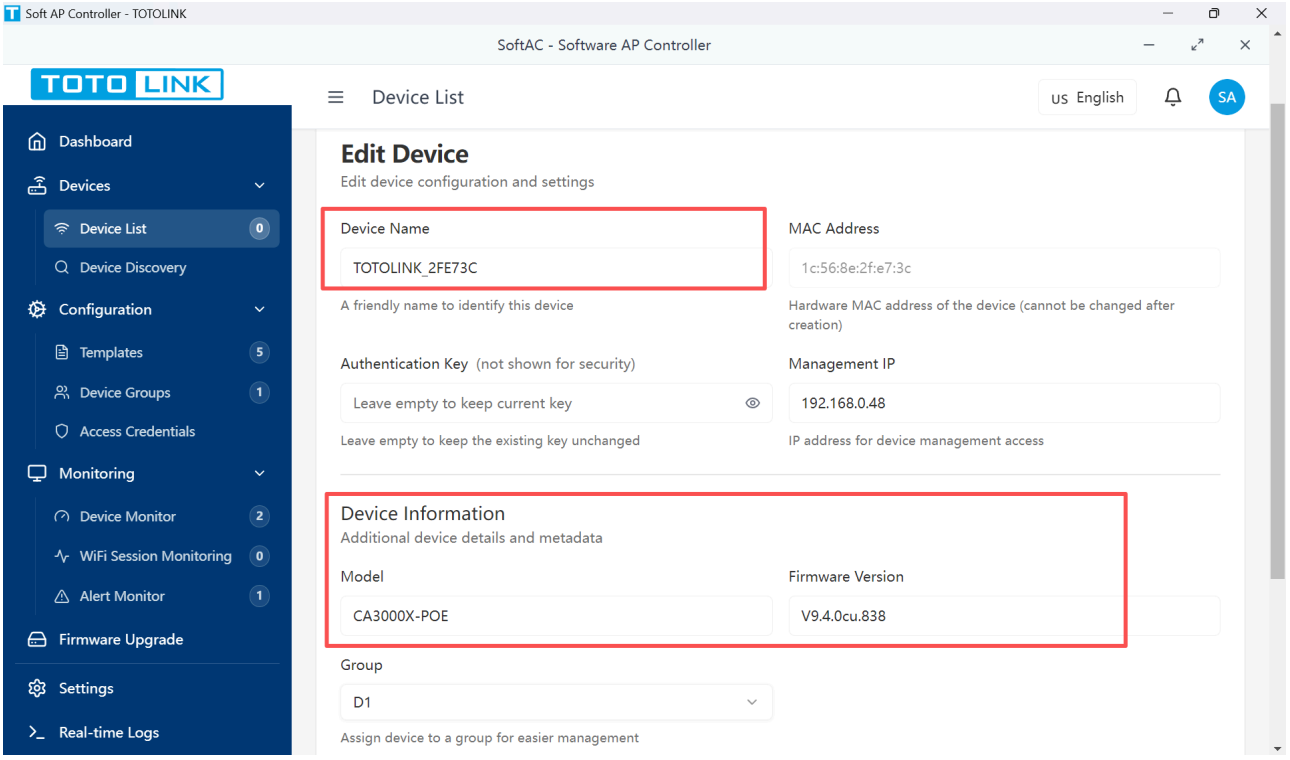
2. **View Firmware Column**
   The device list displays the current firmware version for each device.

Column	Information	Example
Device Name	Device identifier	Office-AP-01
Model	Device model number	TOTOLINK A7000R
Firmware Version (shown in Model)	Current installed version	v2.1.3



From Device Details

1. **Click on Device Name**
   Select any device from the list to open its detail view.
2. **Review System Information**
   The firmware version appears in the System Information section.



Firmware Status Indicators

The system uses visual indicators to help you quickly identify firmware status:

Indicator	Meaning	Action Required
🟢 Green badge	Latest version installed	None
🟡 Yellow badge	Update available	Consider upgrading
🔴 Red badge	Critical update available	Upgrade recommended
⚫ Gray badge	Version unknown	Check device connectivity

8.2 Uploading Firmware Files

Feature Overview

Upload new firmware files to the SoftAC system for distribution to your devices. The system validates files and stores them securely for deployment.

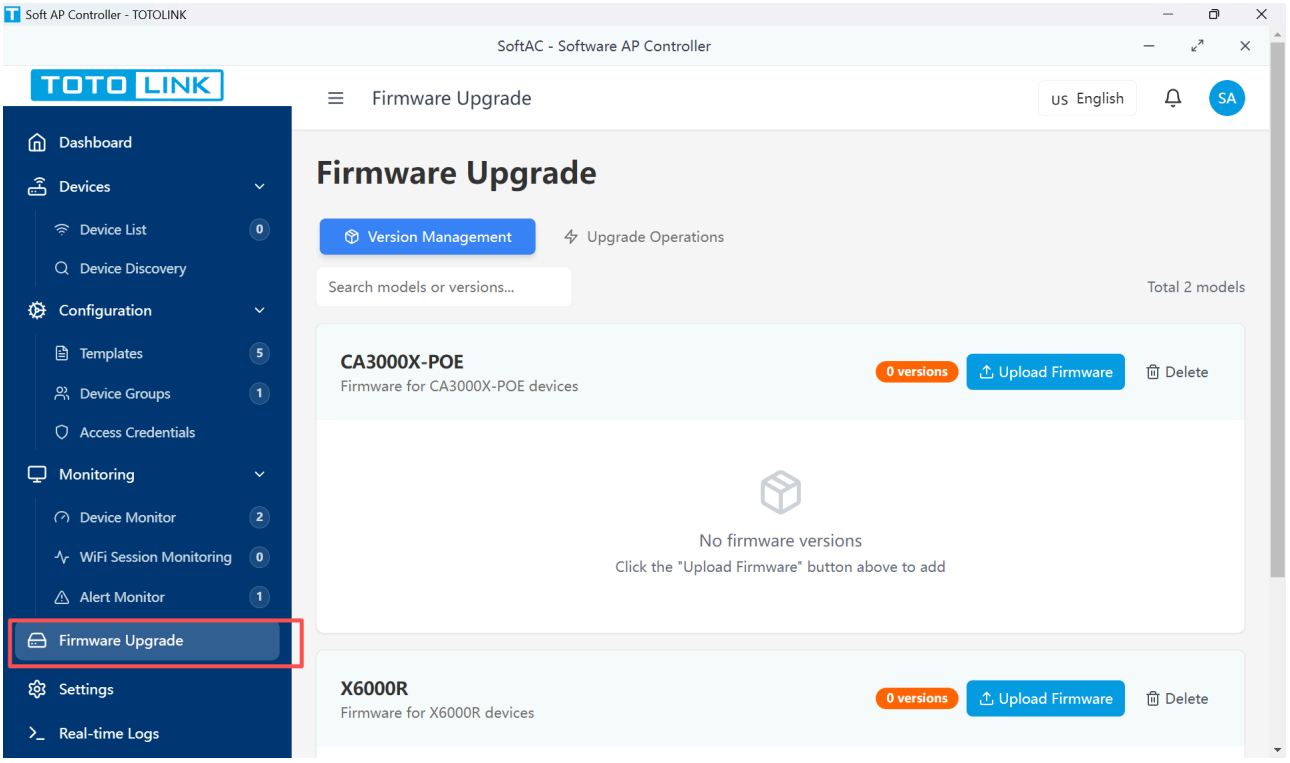
Prerequisites

Before uploading firmware:

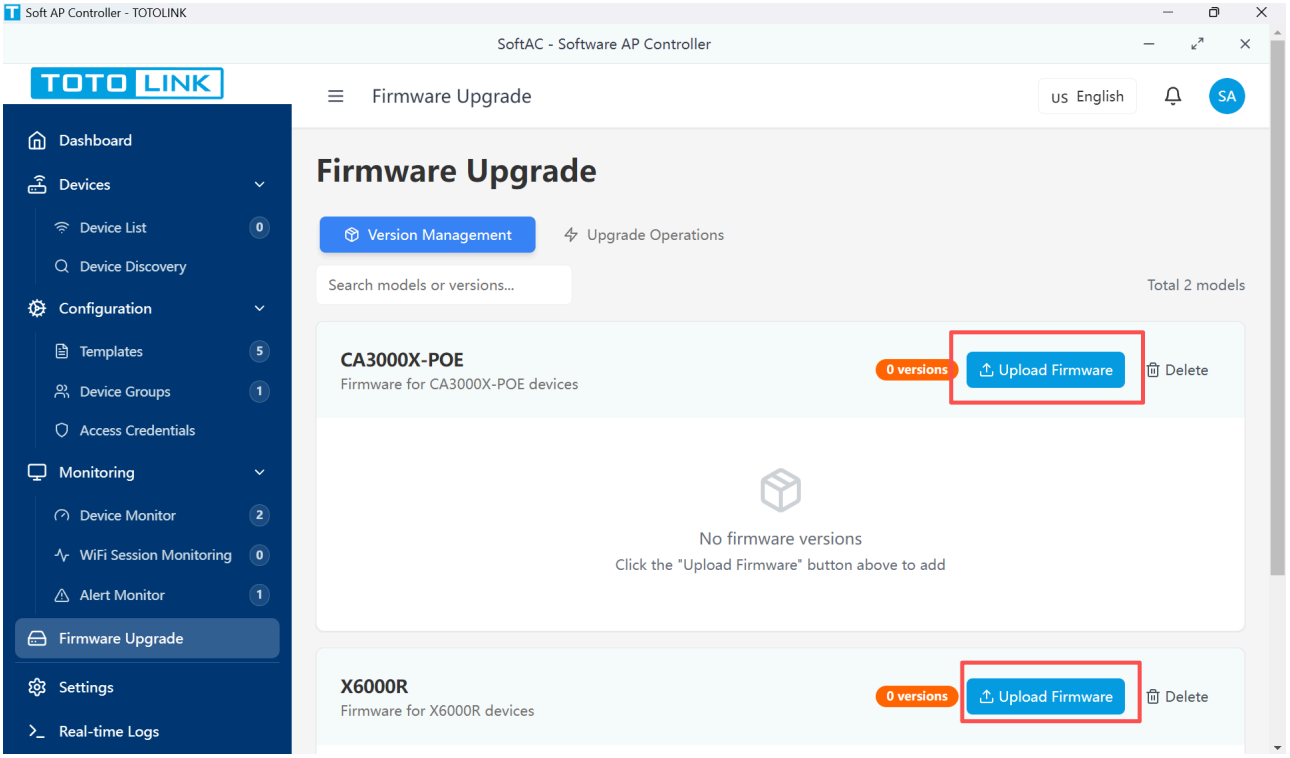
- Obtain firmware files from TOTOLINK official sources
- Verify file compatibility with your device models
- Check available storage space in the system

Upload Process

1. **Access Firmware Upgrade**
   Navigate to "Firmware Upgrade" from the main menu.

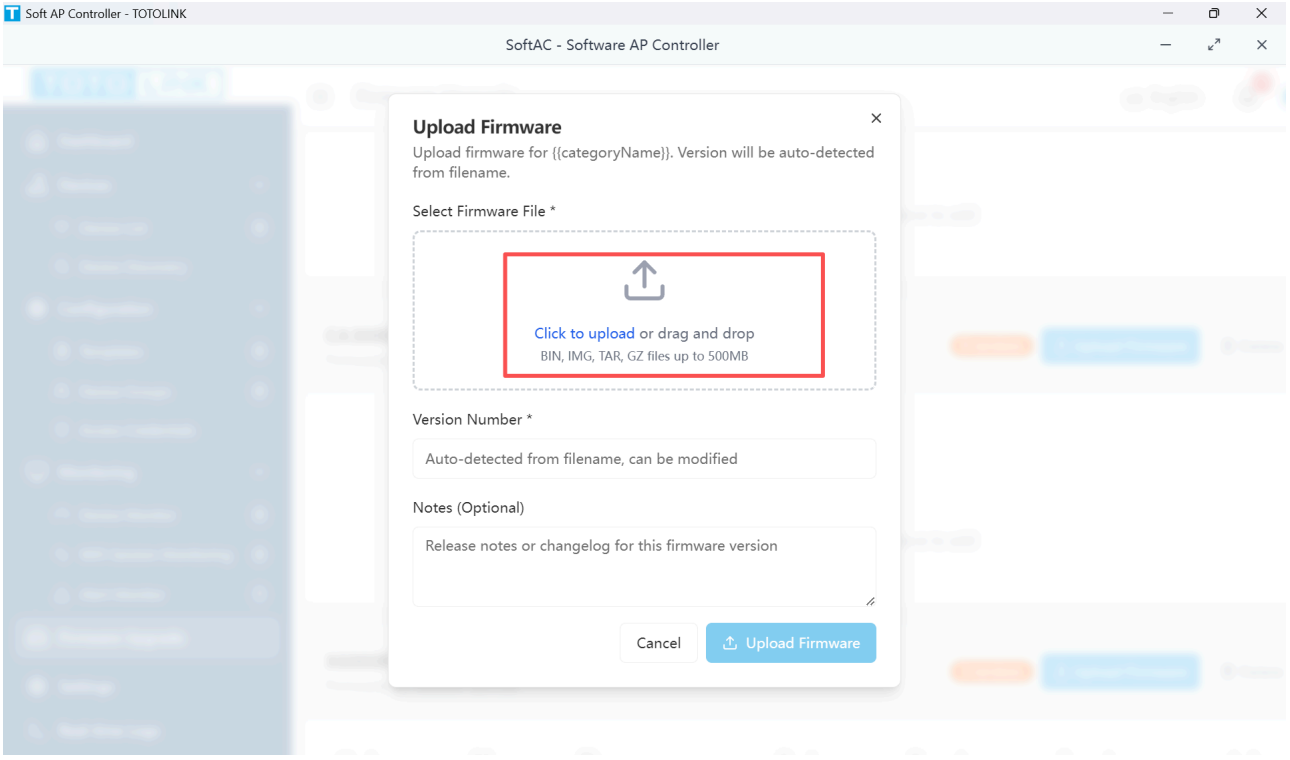


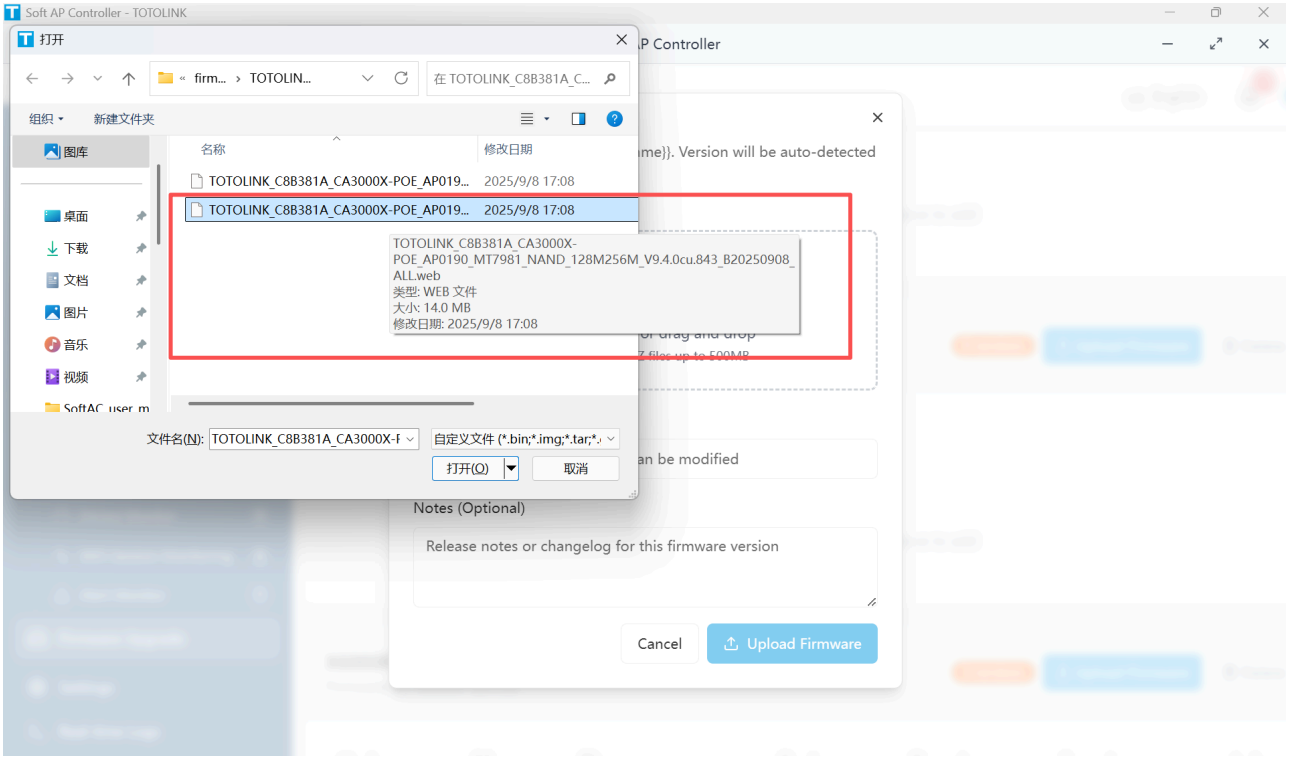
2. **Open Upload Interface**
   Click the "Upload Firmware" button in the top-right corner.



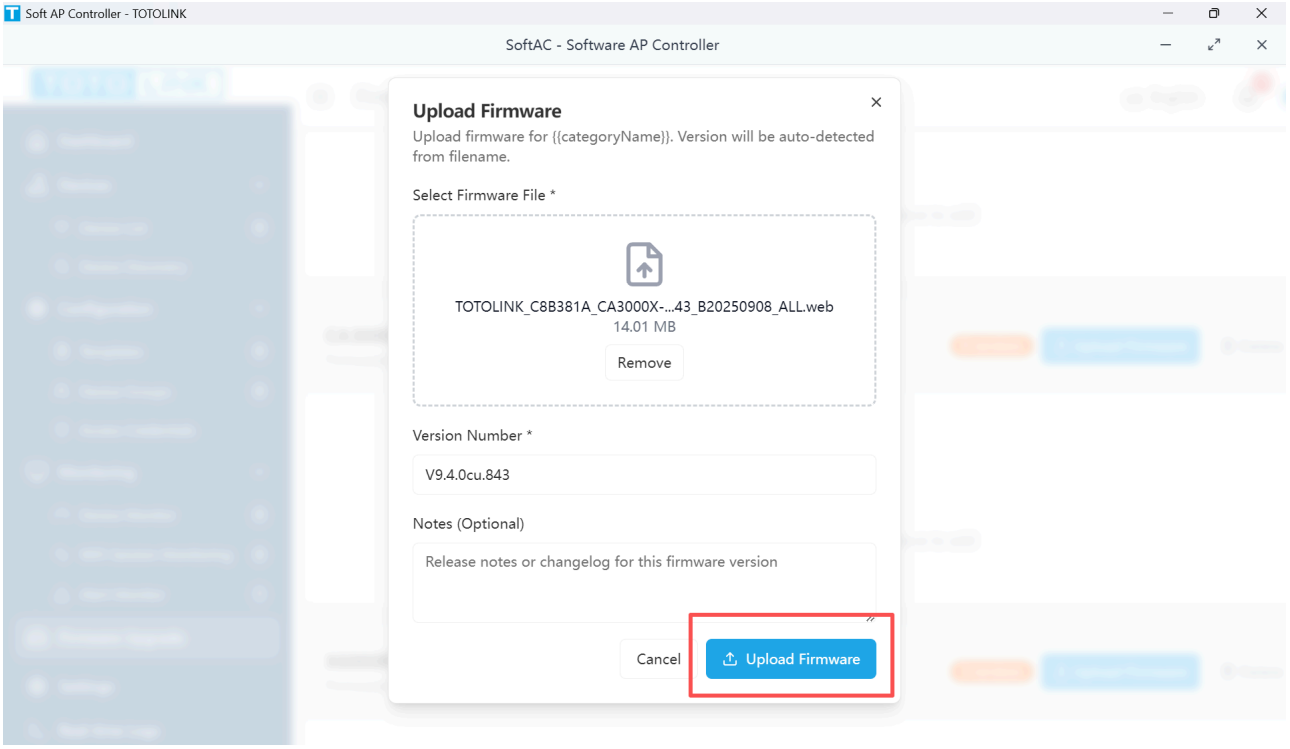
3. **Select Firmware Category**

   Select the firmware you prepared for upgrade:





Confirm Upload
Click "Upload Firmware" to start the transfer.



> 📝 **Note**: Upload progress is shown with a progress bar. Do not close the browser during upload.

File Validation

The system automatically validates uploaded files:

Validation Check	Description	Action if Failed
File Format	Checks for valid firmware extensions	Upload rejected

Validation Check	Description	Action if Failed
File Size	Ensures file isn't corrupted (too small/large)	Warning displayed
Checksum	Verifies file integrity	Upload rejected

Managing Uploaded Firmware

File Actions

For each uploaded firmware, you can:

- **Download**: Retrieve the original file
- **View Details**: Check metadata and compatibility
- **Delete**: Remove unused firmware files
- **Deploy**: Start upgrade process for devices

> ⚠️ **Warning**: Only delete firmware files that are not currently deployed or scheduled for deployment.

Best Practices

> 💡 **Best Practice**:
>
> - Always maintain at least two previous firmware versions for rollback purposes
> - Create descriptive version notes to track changes
> - Test firmware on a single device before batch deployment

8.3 Batch Upgrade

Feature Overview

Batch upgrade allows you to update firmware on multiple devices simultaneously, saving time and ensuring consistency across your network. The system manages the upgrade queue and monitors progress for each device.

Planning a Batch Upgrade

Pre-Upgrade Checklist

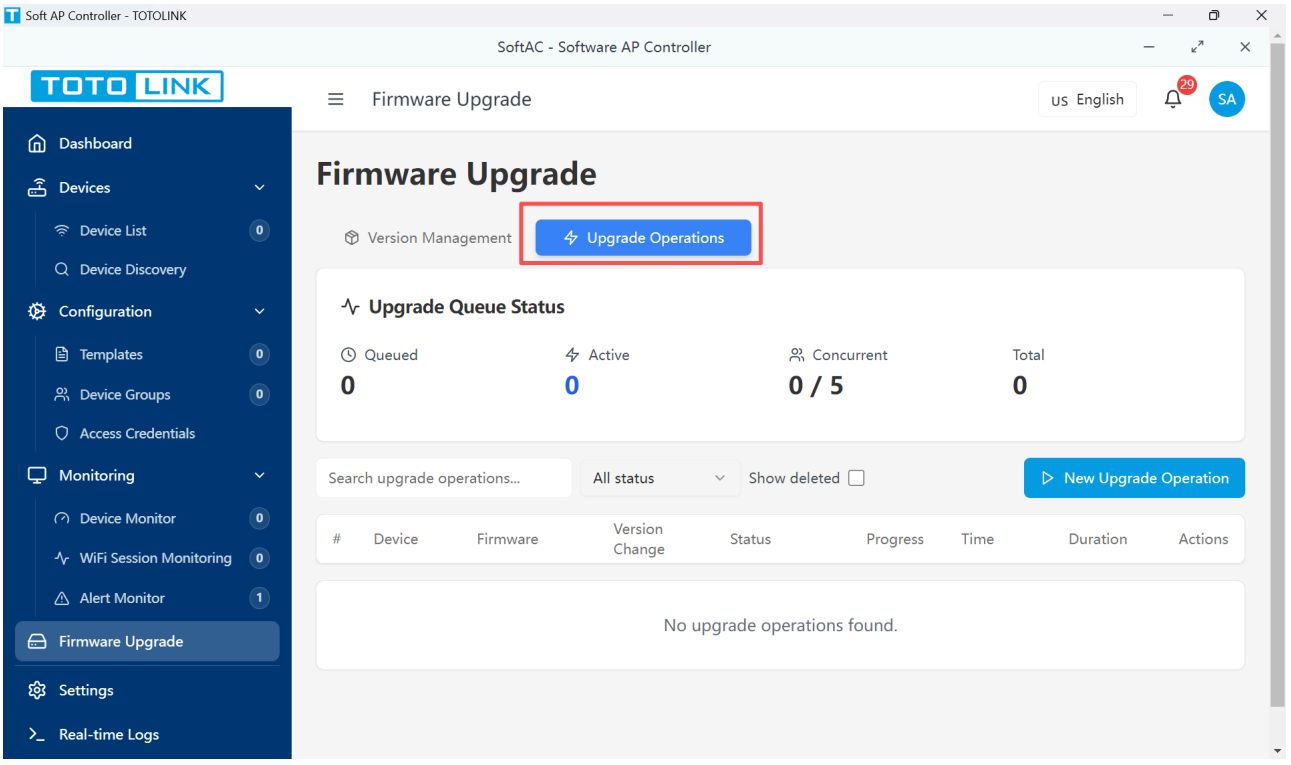
Before starting a batch upgrade:

- [ ] Verify all target devices are online
- [ ] Ensure devices have sufficient storage space
- [ ] Schedule during maintenance window
- [ ] Backup current configurations
- [ ] Notify users of potential service interruption

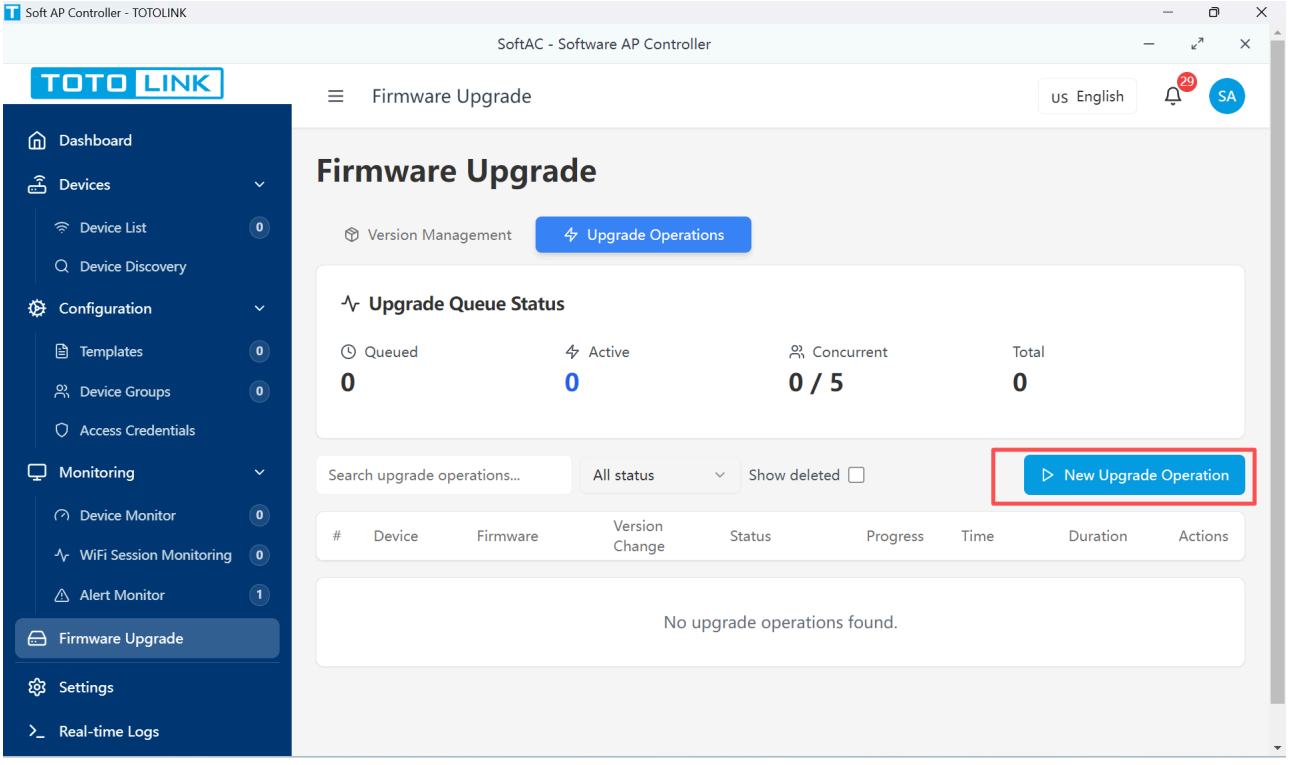
Starting a Batch Upgrade

1. **Access Batch Upgrade Wizard**

   From Firmware Upgrade, click "Upgrade Operations" button.

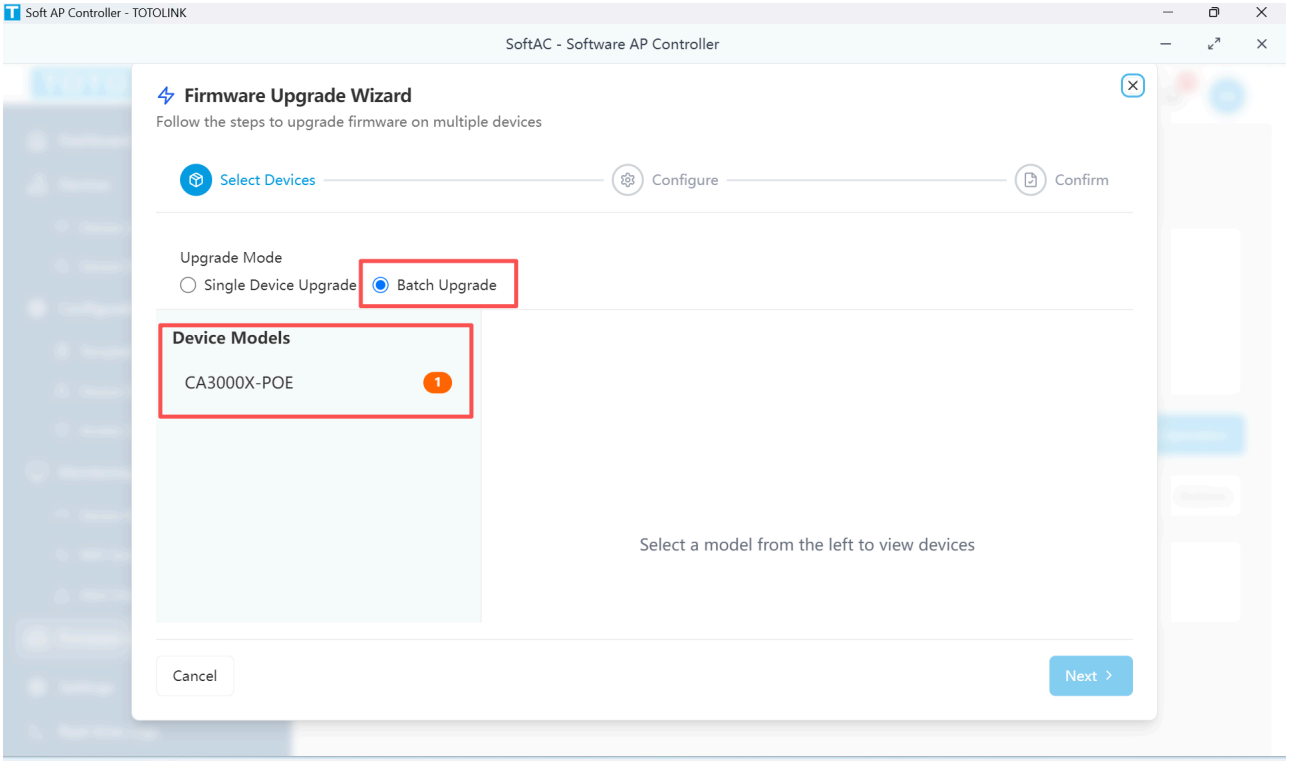


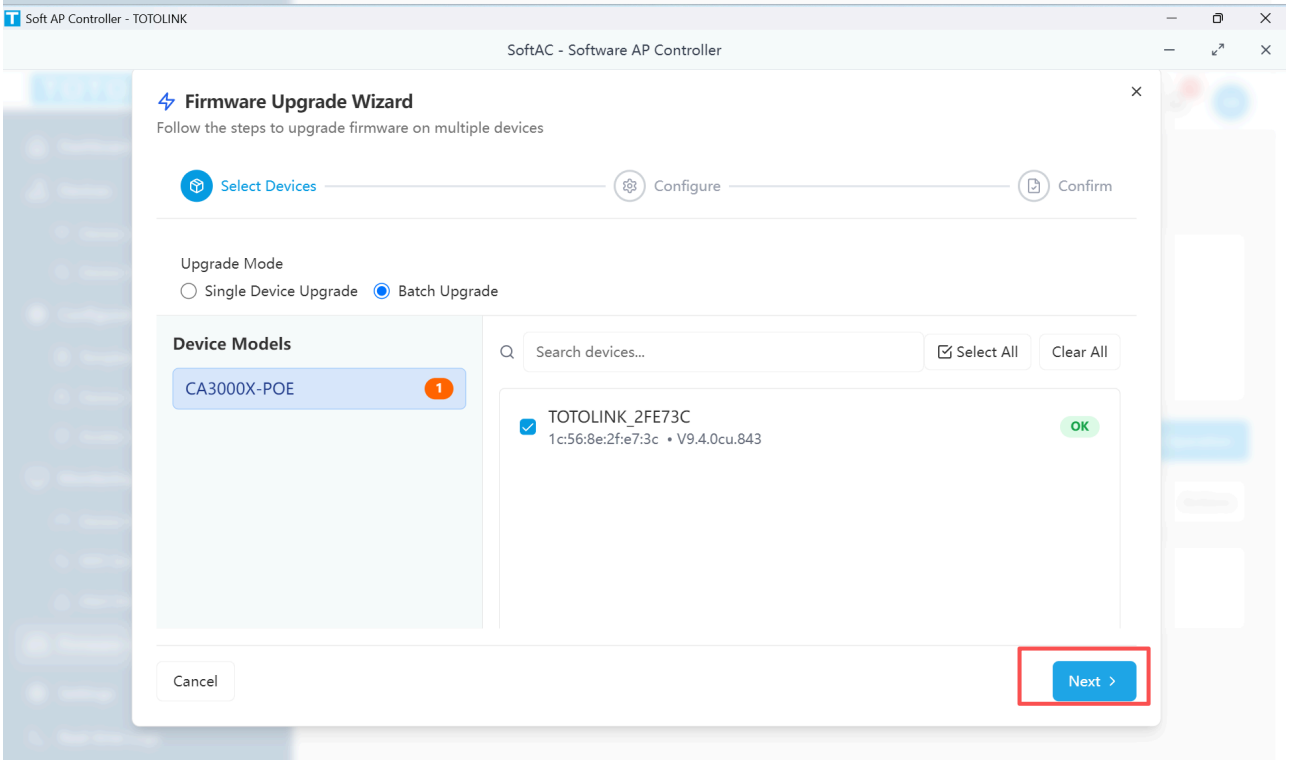
   Click "New Upgrade Operation" button.



2. **Select Target Devices**

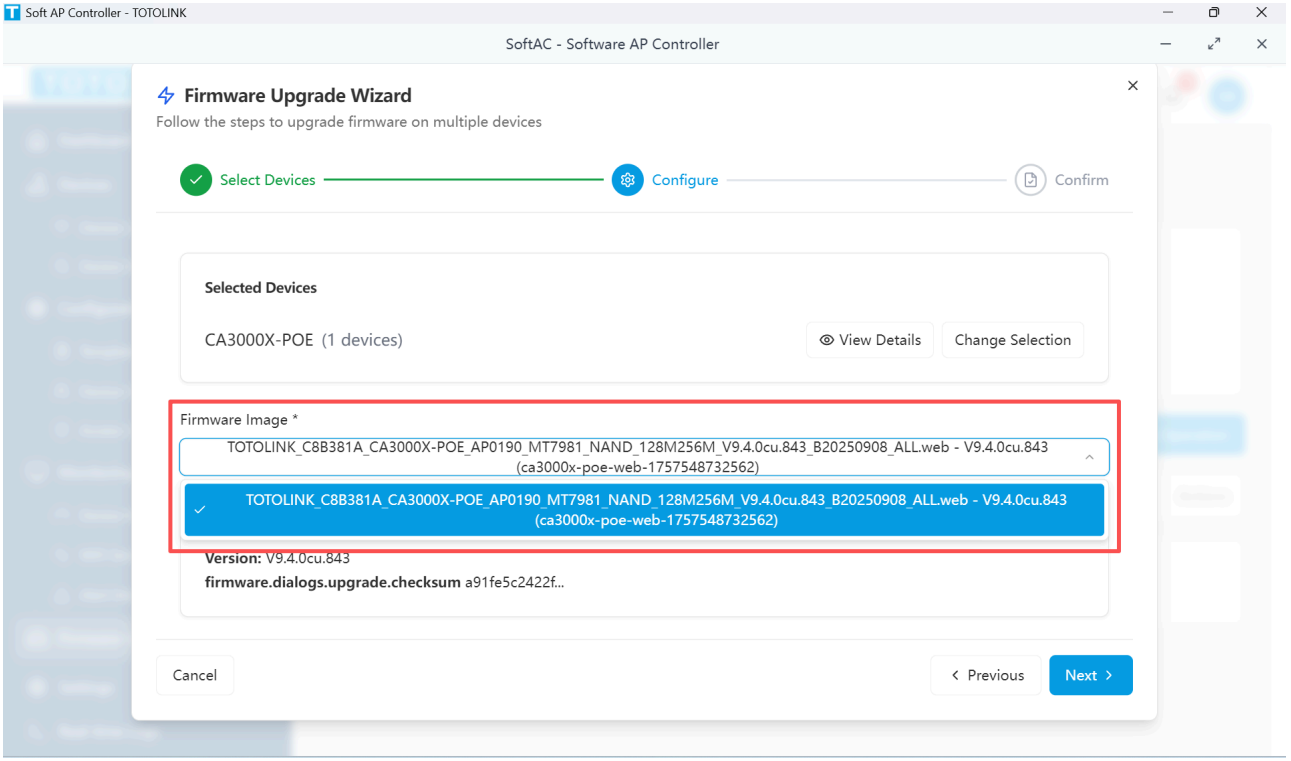
   Click "Batch Upgrade" (default option), then select the model you want.



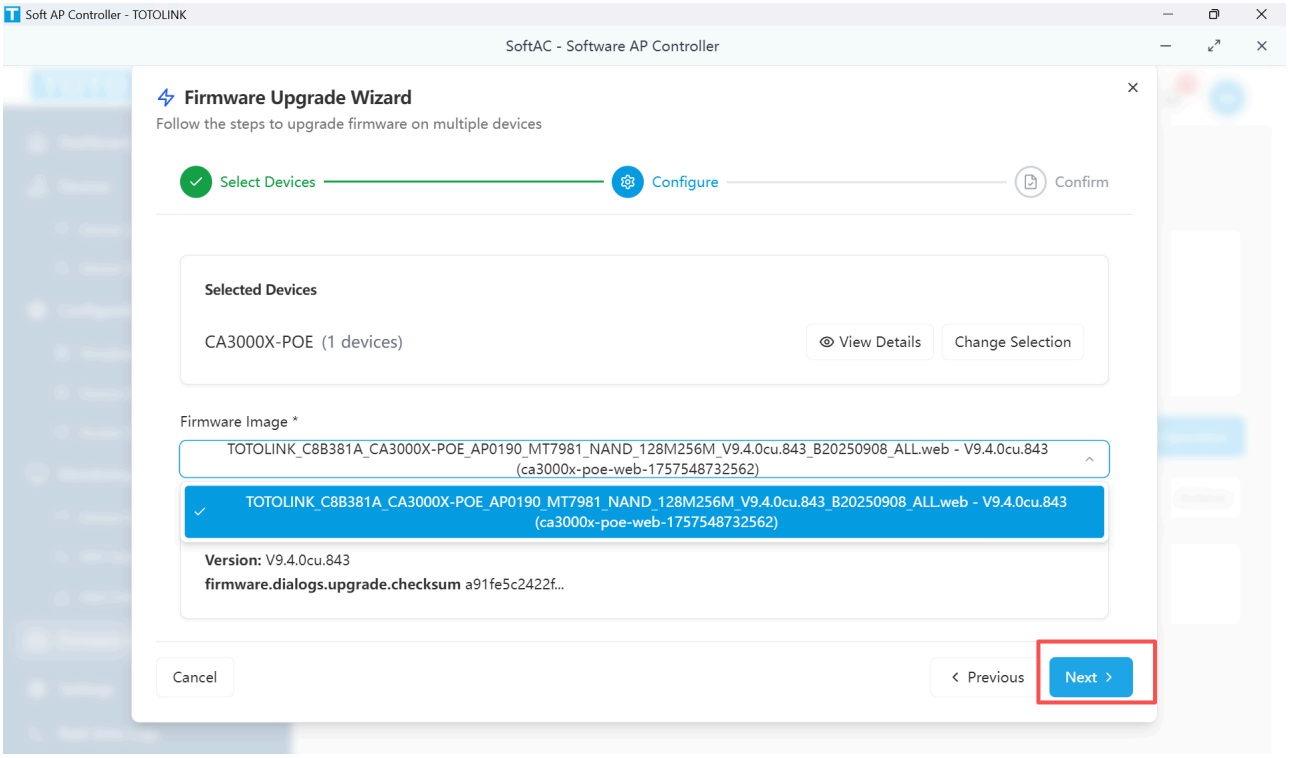


3. **Select Target Firmware**

   Click the blank below "Firmware Image", then select the firmware you want.

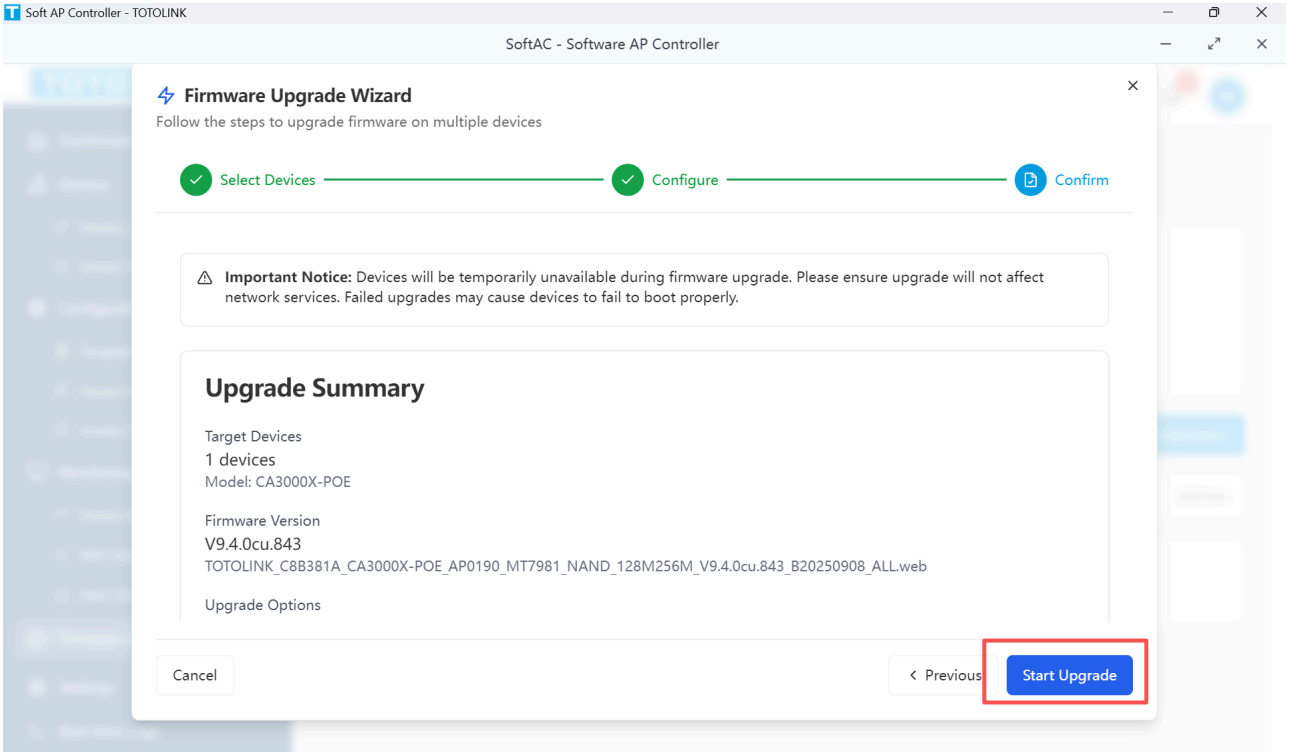


Click "Next"

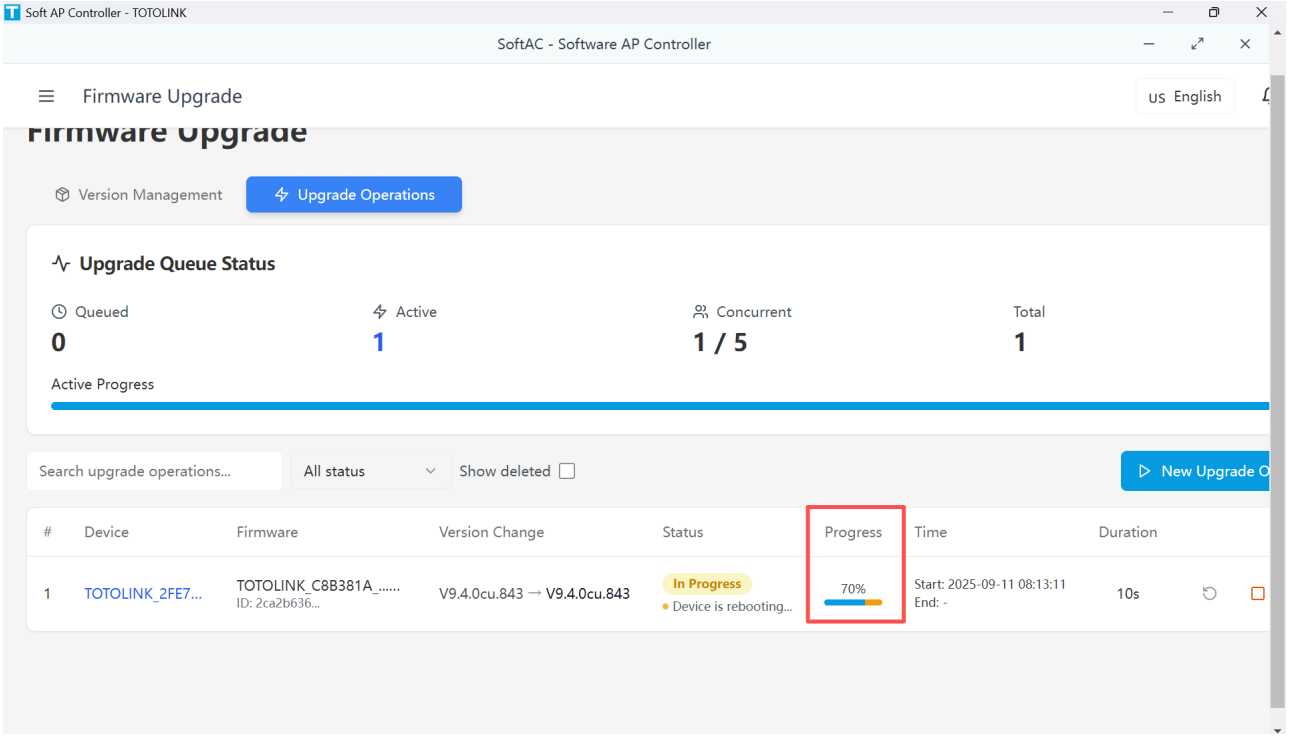


4. **Submit Upgrade Operation**

   Click "Start Upgrade".



The progress is shown in the page:



Related Features

- 4. Device List - Managing individual devices
- 6. Device Groups - Organizing devices for batch operations
- 7.3 Alert Management - Firmware-related alerts
- 11.4 Backup and Recovery - System backup before upgrades

Part 9. Device Discovery

Overview

The Device Discovery feature in TOTOLINK SoftAC automatically finds and identifies network devices, making it easy to add new access points to your management system. Instead of manually entering device information one by one, the discovery system can detect multiple devices simultaneously, saving time and reducing configuration errors.

Key Benefits

- **Automatic Detection**: Find all TOTOLINK devices on your network without manual searching
- **Time Savings**: Add multiple devices at once instead of individual manual entry
- **Error Reduction**: Automatically captures accurate device information
- **Network Visibility**: See all devices, both managed and unmanaged

---

9.1 Automatic Discovery

Understanding Automatic Discovery

Automatic discovery uses network broadcast and scanning technologies to find TOTOLINK devices on your network. The system sends out discovery messages and listens for responses from compatible devices.

How Automatic Discovery Works

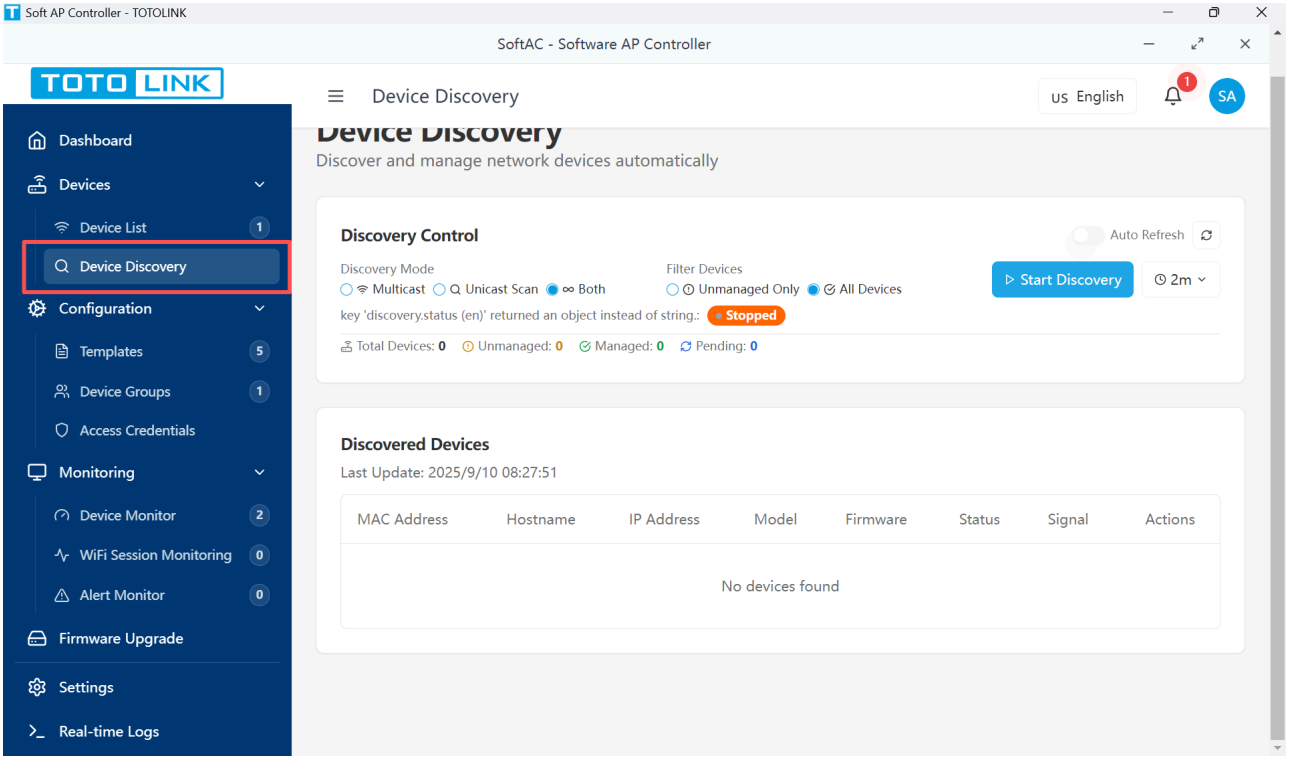
The discovery process uses three methods to find devices:

1. **Multicast Discovery**: Sends broadcast messages that all devices on the local network can hear
2. **Unicast Discovery**: Directly contacts devices at known IP addresses
3. **Network Scanning**: Systematically checks IP ranges for responsive devices

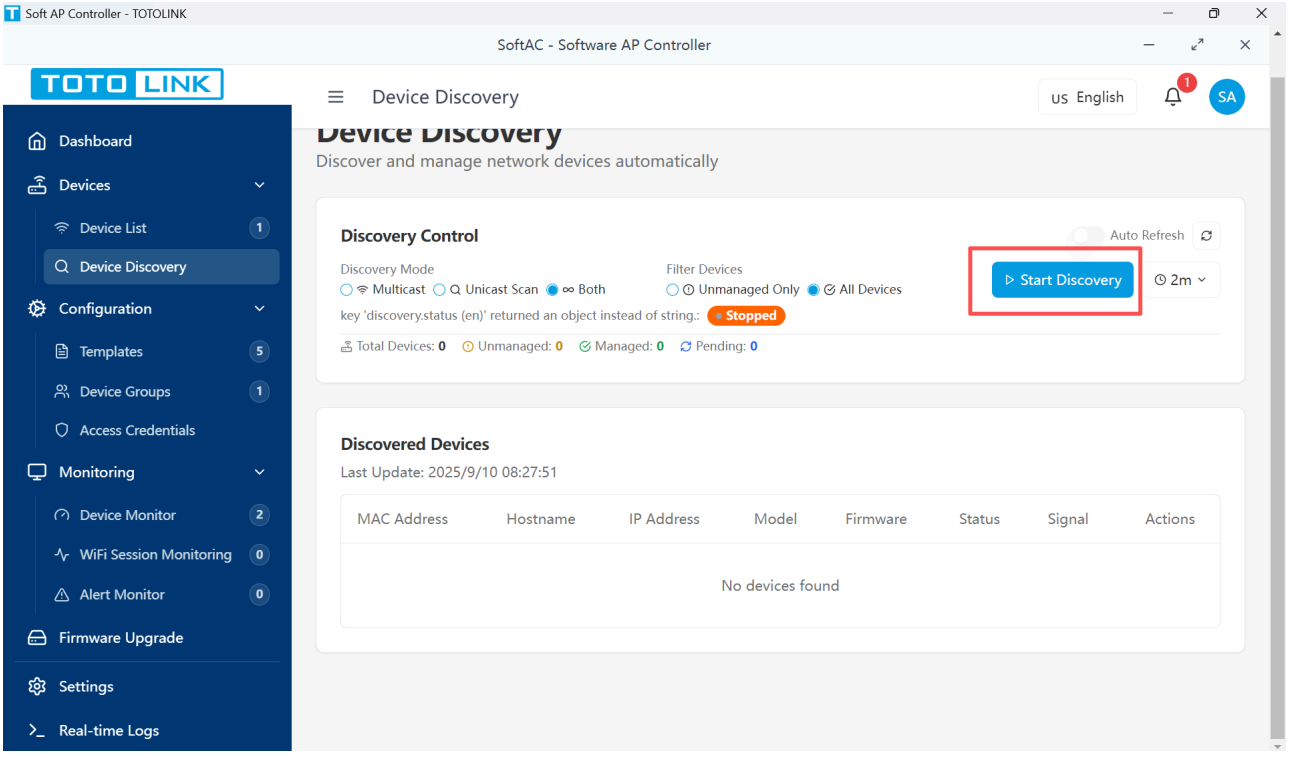
Starting Automatic Discovery

Quick Start Method

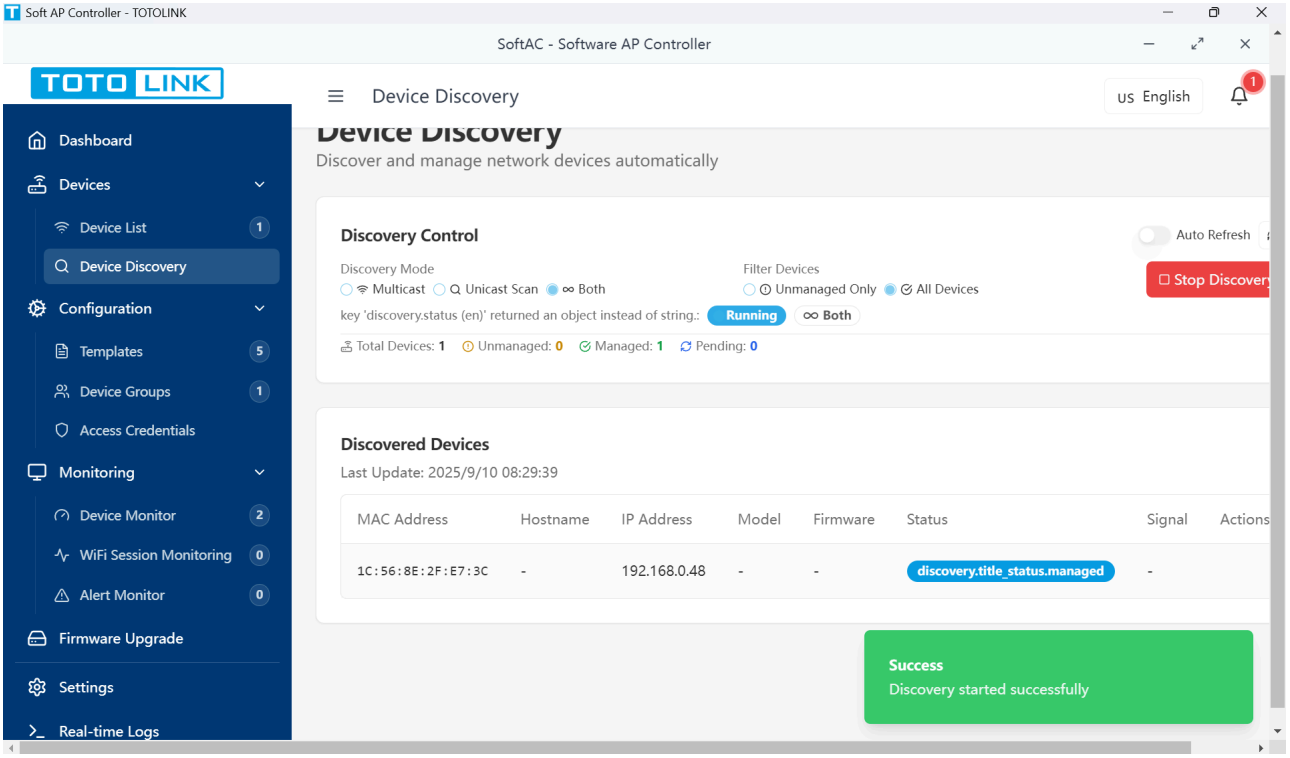
1. **Navigate to Discovery Page**
   Click "Device Discovery" in the main navigation menu



2. **Start Discovery**
   Click the large "Start Discovery" button in the control panel



3. **Monitor Progress**
   Watch as devices appear in the discovered devices list
   - The system automatically refreshes every 3 seconds
   - New devices appear with an "Unmanaged" status badge

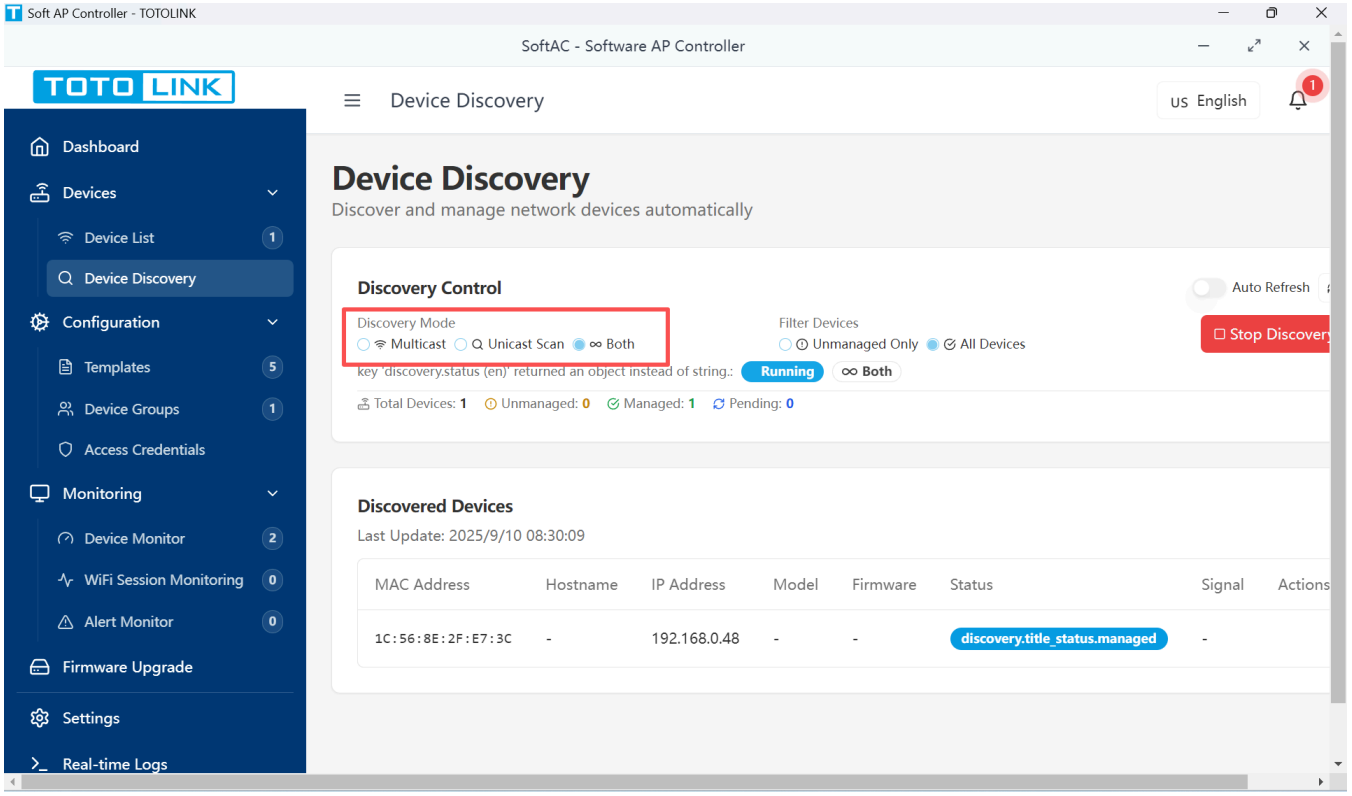


Advanced Discovery Options

Before starting discovery, you can configure:

Discovery Mode Selection

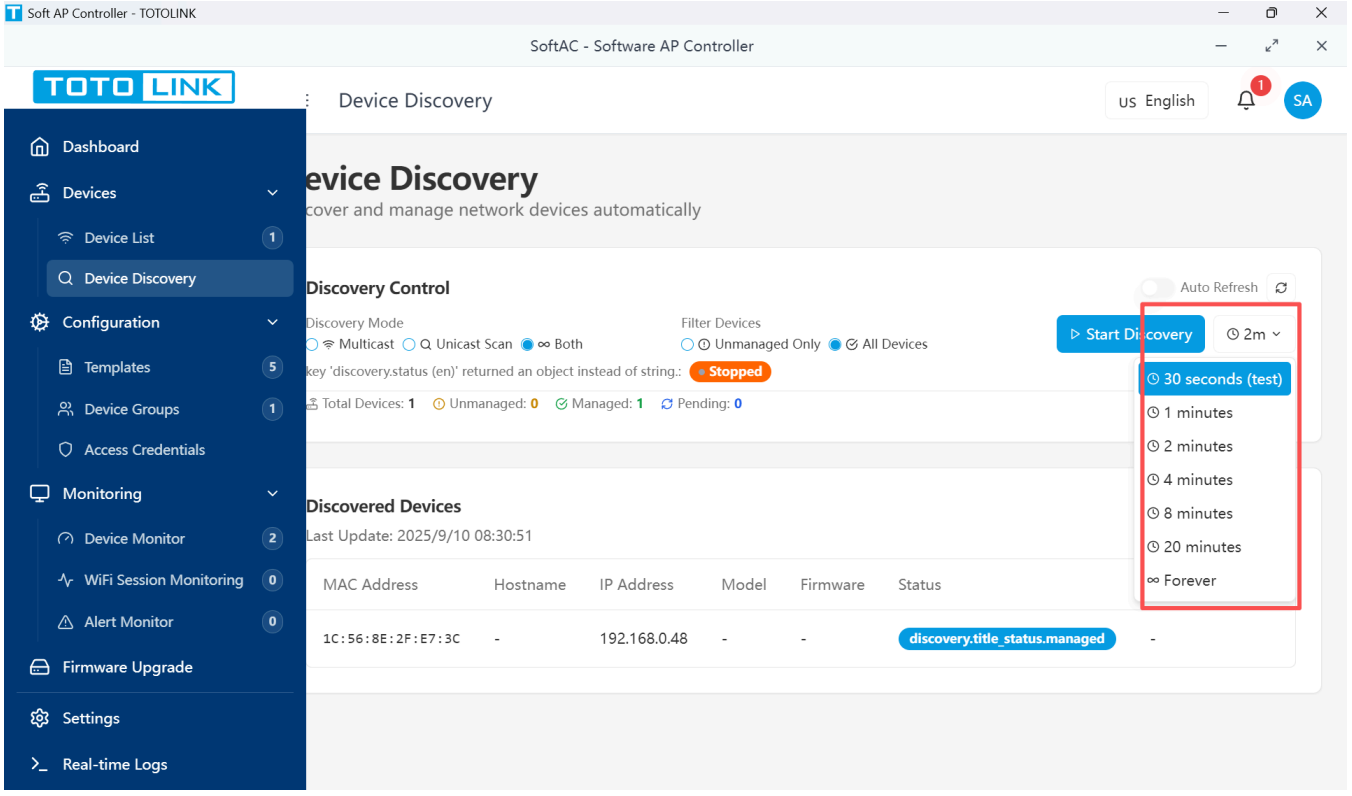
Mode	Description	Best For
Both (Default)	Uses all discovery methods	Most comprehensive search
Multicast Only	Broadcast messages only	Quick local network scan
Unicast Only	Direct IP contact	Targeted device search



Discovery Duration

Set how long the discovery should run:

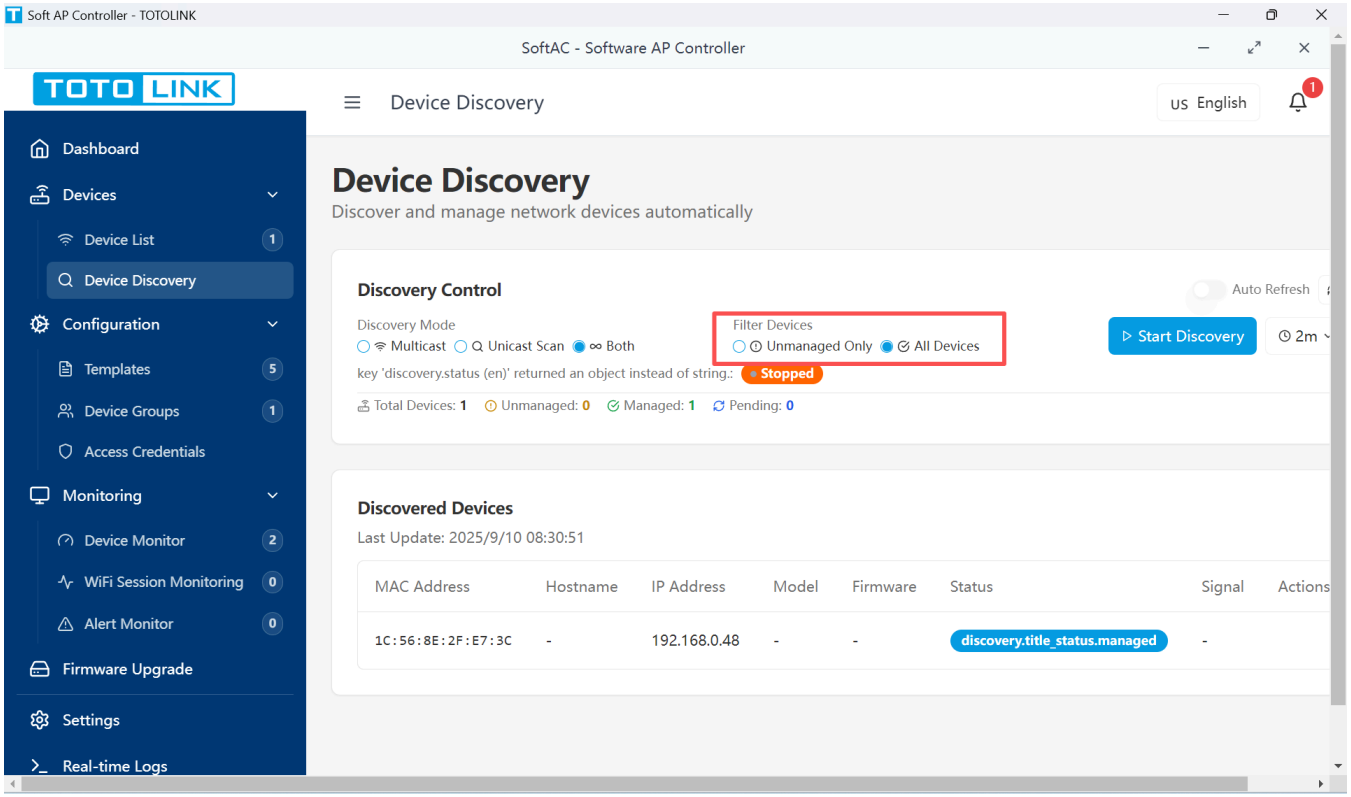
- **2 minutes** (Default) - Quick scan for most networks
- **5 minutes** - Thorough scan for larger networks
- **10 minutes** - Complete scan for complex networks
- **Forever** - Continuous discovery until manually stopped



Filter Options

Choose which devices to display:

- **All Devices** - Shows both managed and unmanaged devices
- **Unmanaged Only** - Shows only new devices not yet added to system



Understanding Discovery Results

The discovered devices list shows:

Column	Description
Status	Device management state (Unmanaged/Managed/Pending)
Device Info	MAC address, hostname, and model
Network	IP address and connection status
Firmware	Current firmware version
Action	Quick actions like Add Device

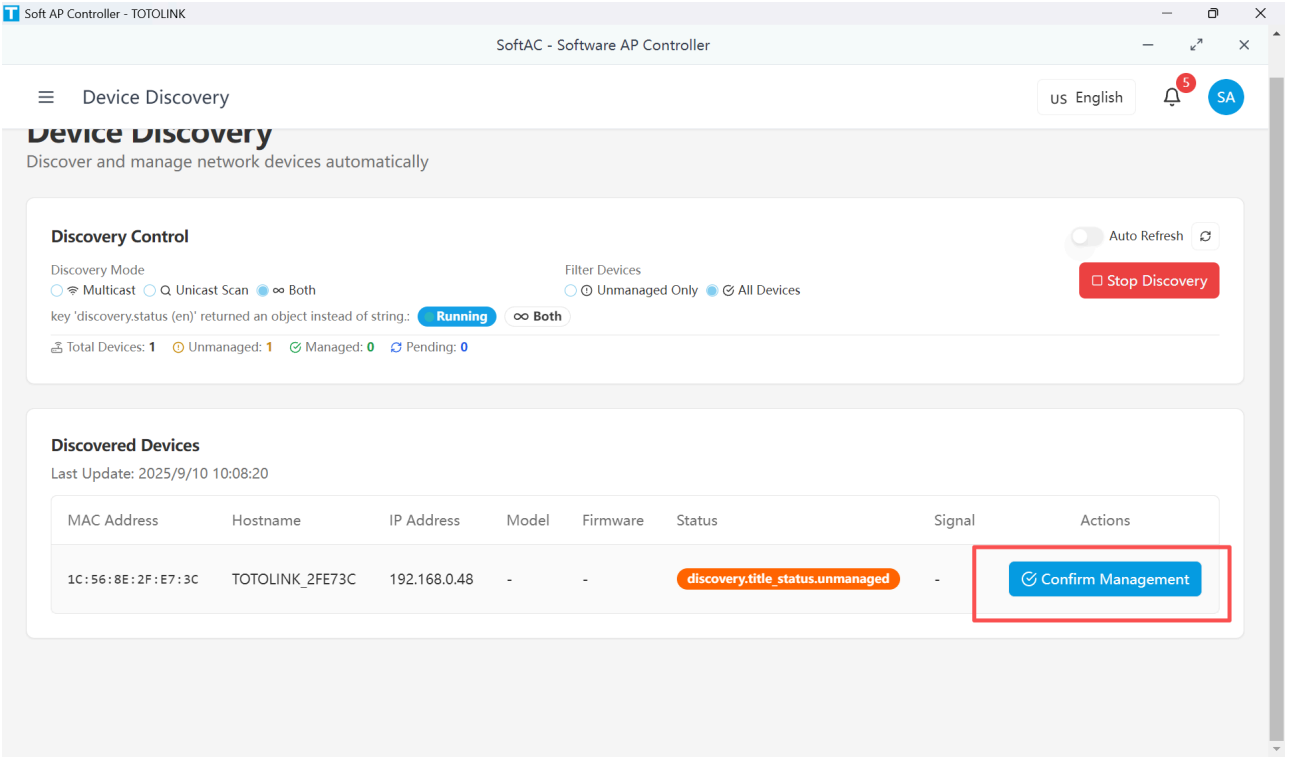
Device Status Indicators

- 🔴 **Unmanaged**: New device found, not yet added to system
- 🟡 **Pending**: Device confirmation in progress
- 🟢 **Managed**: Device already managed by SoftAC
- ⚫ **Registering**: Device being added to system

Adding Discovered Devices

To add a discovered device to your system:

1. **Locate the Device**
   Find the unmanaged device in the discovery list
2. **Click Add Button**
   Click the "Confirm Management" button in the Actions column



3. **Confirm Addition**
   The device status changes to "Registering" then "Managed"

> ✅ **Success**: Device will appear in your main device list within seconds

Troubleshooting Discovery Issues

No Devices Found?

1. Check network connectivity between SoftAC and devices
2. Verify devices are powered on and connected to network
3. Ensure firewall allows discovery traffic (UDP port 5683)
4. Try increasing discovery duration

Network Configuration Warning?

If you see a network configuration warning:

1. Go to Settings → System Settings
2. Update the Management IP address
3. Restart discovery with correct network settings

Discovery Modes Explained

Multicast Mode

How it works:

- Sends UDP broadcast messages on port 5683
- All devices on local network receive message
- Compatible devices respond with their information

Best for:

- Local network discovery
- Finding all devices quickly
- Initial network setup

Limitations:

- Doesn't cross network segments
- May be blocked by some switches
- Requires multicast support

Unicast Mode

How it works:

- Directly contacts devices at specific IPs
- Sends targeted discovery messages
- Works across network segments

Best for:

- Known device locations
- Cross-subnet discovery
- Precise device targeting

Limitations:

- Slower for many devices
- Requires IP information
- May miss dynamic IPs

Combined Mode (Both)

How it works:

- Uses both multicast and unicast simultaneously
- Provides most comprehensive coverage
- Balances speed and completeness

Best for:

- Most discovery scenarios
- Unknown network layouts
- Maximum device detection

Optimizing Discovery

For Best Results

1. **Update Management IP**
    - Always set correct server IP before discovery
    - Update if server IP changes
2. **Choose Appropriate Duration**
    - Start with 2 minutes for small networks
    - Use 5-10 minutes for larger networks
    - Use continuous for ongoing monitoring
3. **Select Correct Mode**
    - Use "Both" for initial discovery
    - Switch to specific mode if needed
    - Consider network topology
4. **Monitor Discovery Status**
    - Check statistics panel regularly
    - Watch for network warnings
    - Verify all expected devices found

Common Issues and Solutions

Issue	Cause	Solution
No devices found	Incorrect network config	Update management IP
Partial discovery	Firewall blocking	Allow UDP 5683
Slow discovery	Large network	Increase duration, use filters
Duplicate devices	Multiple interfaces	Check device network settings

Security Considerations

Discovery Security

- Discovery uses secure tokens for device verification
- Each discovery session has unique identifiers
- Devices must respond with valid credentials

Best Practices

1. **Run Discovery As Needed**
   - Don't leave continuous discovery running unnecessarily
   - Stop discovery after adding all devices
2. **Verify Devices Before Adding**
   - Check MAC addresses match physical devices
   - Confirm device models are correct
   - Validate IP addresses are expected
3. **Document Discovery Sessions**
   - Note when discovery was run
   - Record number of devices found
   - Track any unusual findings

Summary

The Device Discovery feature in TOTOLINK SoftAC streamlines network device management through:

- **Automatic Discovery**: Find all compatible devices with one click
- **Manual Search**: Target specific devices when needed
- **Batch Management**: Handle multiple devices efficiently
- **Flexible Configuration**: Customize discovery for your network

Quick Reference

Task	Method	Time Required
Find all local devices	Automatic discovery (Both mode)	2-5 minutes
Add specific device	Manual search by IP	< 1 minute
Organize devices	Batch assign to groups	2-3 minutes
Configure discovery	Update network settings	1-2 minutes

> 🚀 **Next Steps**: Run your first discovery session to find all network devices, then organize them into logical groups for easier management.

Related Topics

- 4. Device Management - Managing discovered devices
- 6. Device Groups - Organizing devices into groups
- 11. System Settings - Configuring network parameters
- 14. Troubleshooting - Solving discovery issues

Part 10. Credential Management

Overview

Credential Management in TOTOLINK SoftAC provides secure authentication methods for accessing and managing network devices. The system uses industry-standard encryption to protect sensitive information like passwords and keys, ensuring only authorized administrators can access device configurations and perform management tasks.

Key Benefits

- **Secure Access**: Encrypted storage of all credentials protects against unauthorized access
- **Centralized Management**: Store and manage all device access credentials in one place
- **Automated Authentication**: System automatically uses stored credentials for device operations
- **Audit Trail**: Track credential usage and modifications for security compliance

---

10.1 SSH Credentials

Understanding SSH Credentials

SSH (Secure Shell) credentials allow TOTOLINK SoftAC to securely connect to network devices for configuration, monitoring, and management tasks. Instead of using passwords which can be intercepted or guessed, SSH uses cryptographic key pairs for authentication.

How SSH Keys Work

SSH authentication uses a pair of mathematically related keys:

1. **Private Key**: Kept secret on the SoftAC server, never shared
2. **Public Key**: Installed on network devices to verify identity

When SoftAC connects to a device:

- The device challenges SoftAC with its public key
- SoftAC proves its identity using the private key
- A secure encrypted connection is established

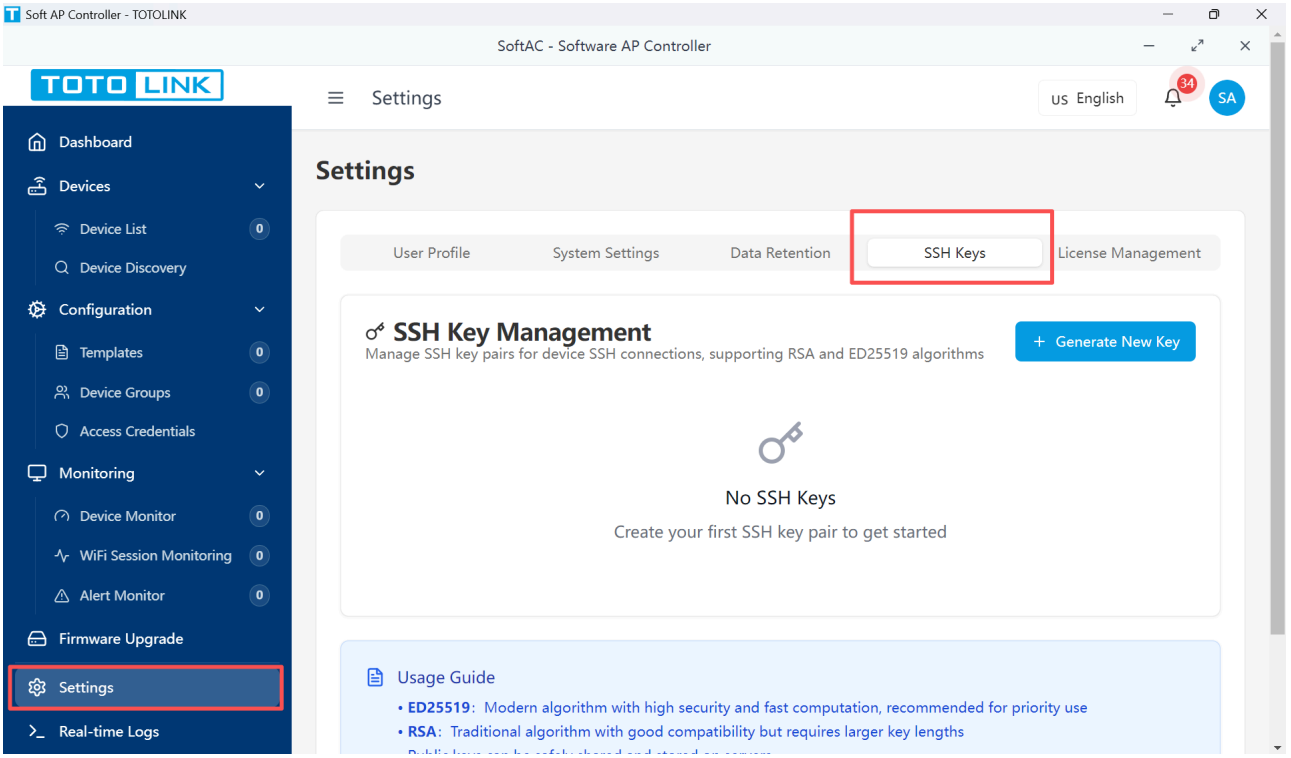
Creating SSH Credentials

Initial Setup

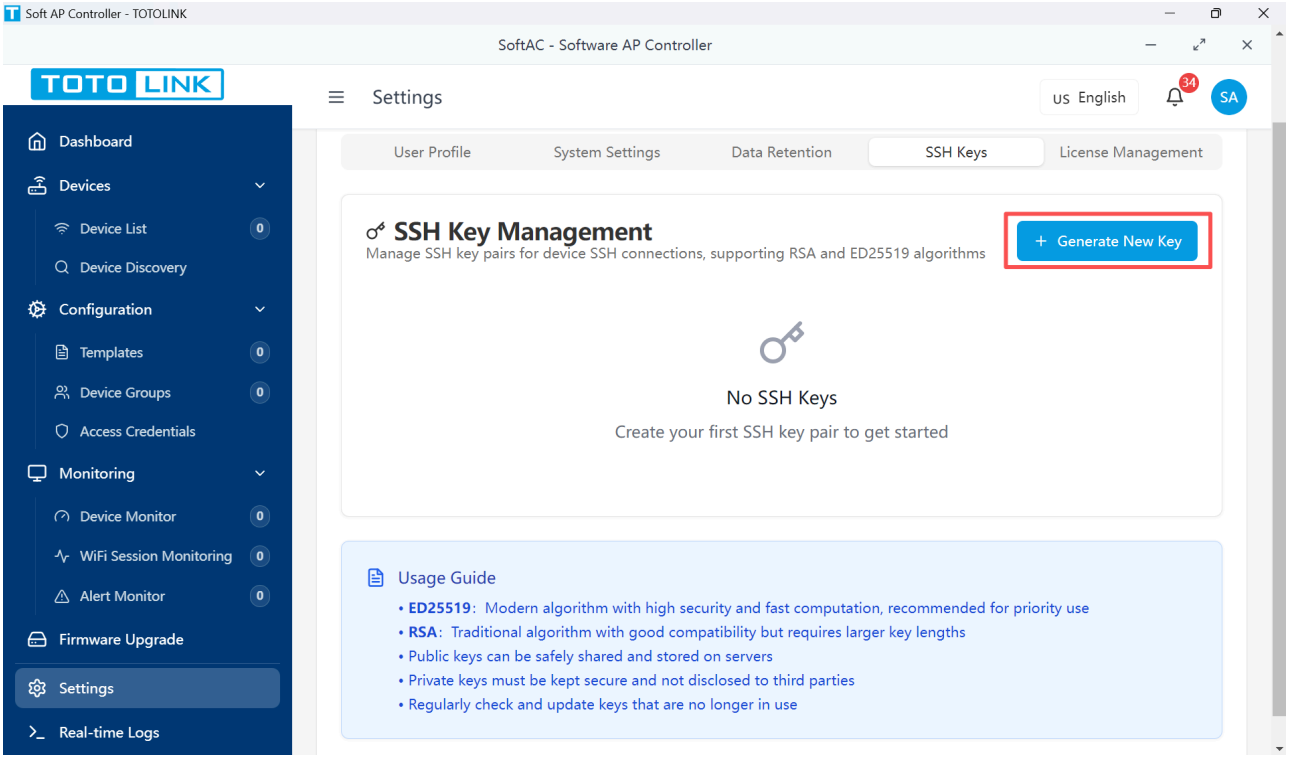
During system initialization, SoftAC automatically creates a default SSH key pair. For additional security or specific device requirements, you can create custom SSH credentials.

Creating New SSH Keys

1. **Navigate to SSH Key Management**
   Go to Settings → SSH Key Manager



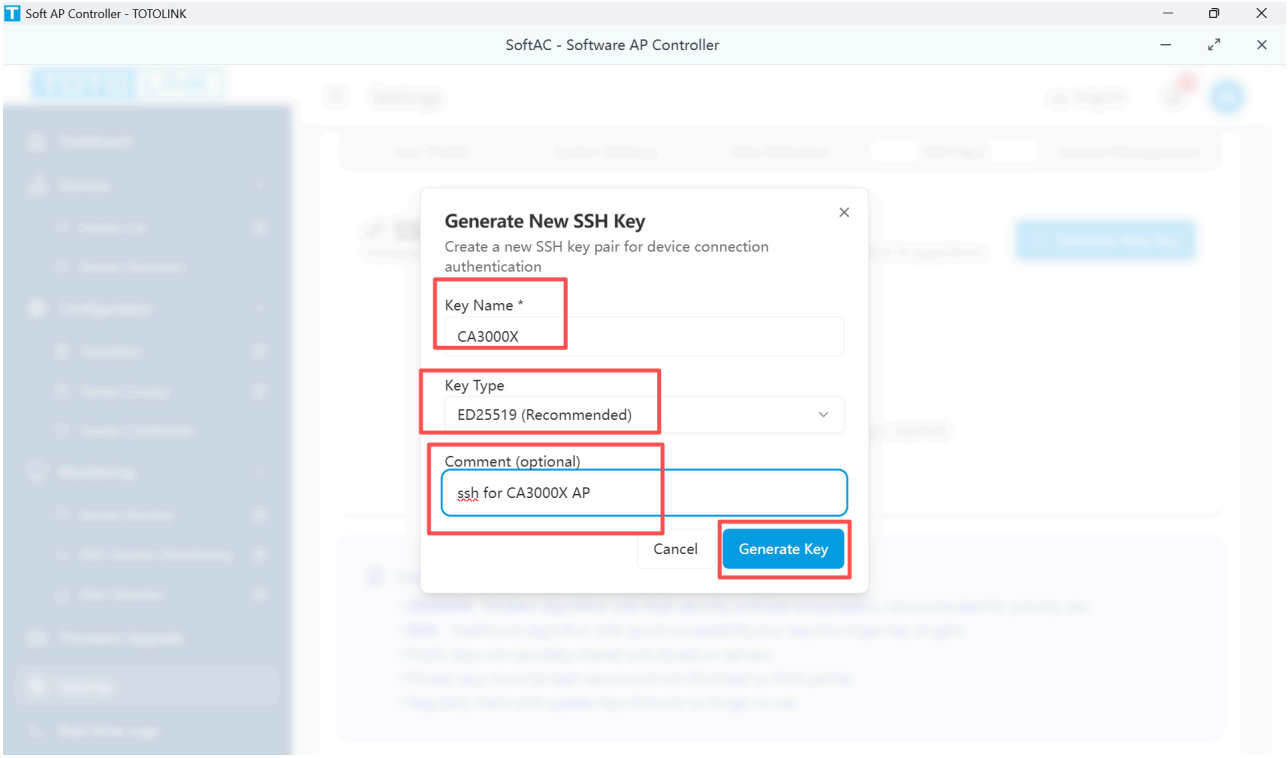
2. **Start Key Generation**
   Click the "Generate New Key" button



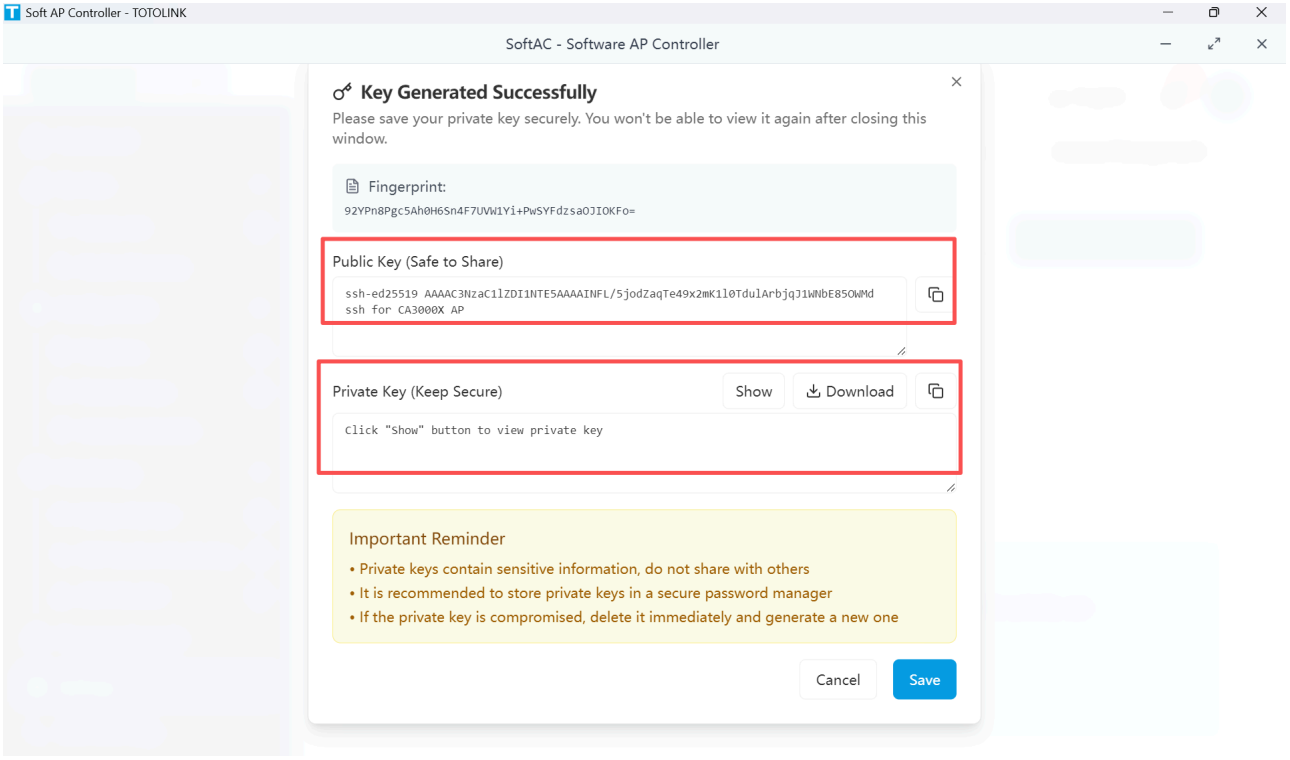
3. **Configure Key Parameters**

Parameter	Options	Recommendation
Key Name	Custom text	Use descriptive names (e.g., "Production-APs-2024")

Parameter	Options	Recommendation
Key Type	ED25519 or RSA	ED25519 (faster and more secure)
Key Size	2048, 3072, 4096 bits	2048 for RSA (if chosen)
Comment	Optional text	Add description for identification



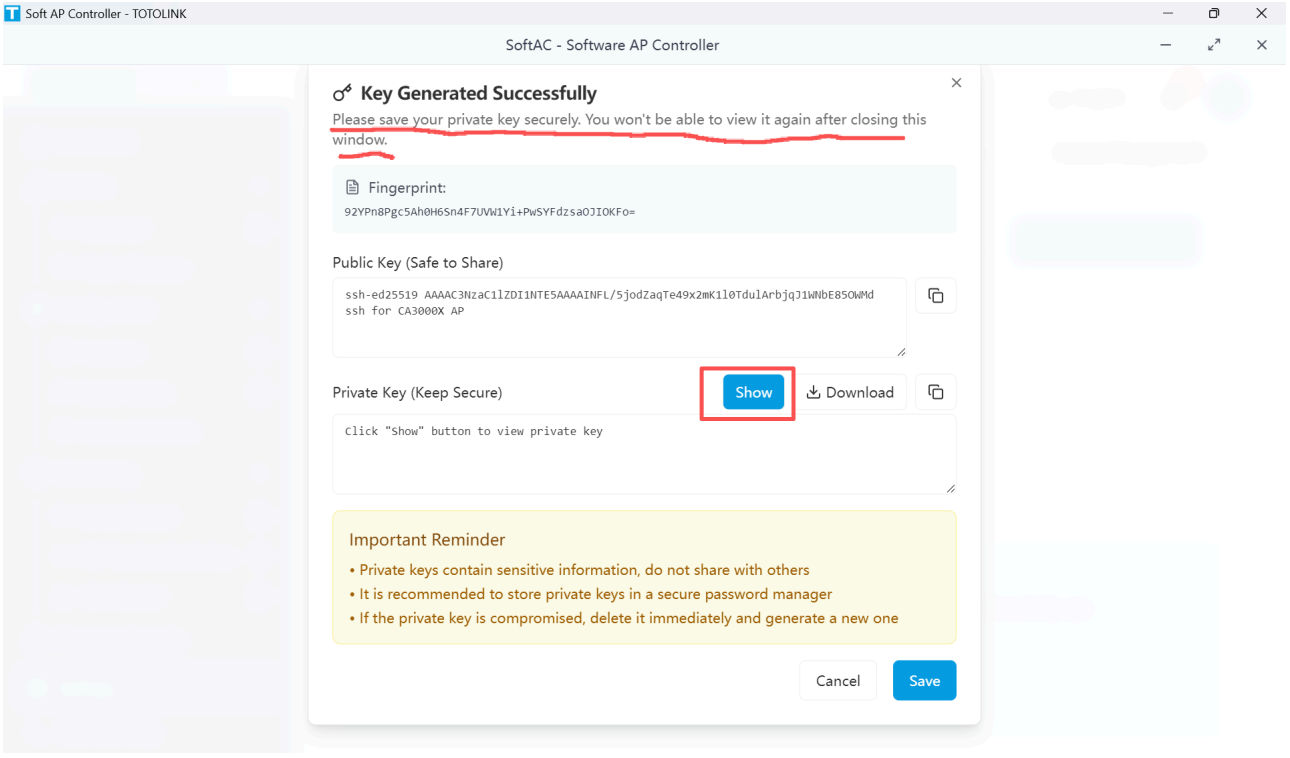
4. **Generate the Key Pair**
   Click "Generate" to create the key pair
   - The system generates both private and public keys
   - A unique fingerprint identifies this key pair



5. **Save the Keys**

   Important Actions:

   - **Download Private Key**: Save it securely - you cannot retrieve it later
   - **Copy Public Key**: You'll need this for device configuration
   - **Note the Fingerprint**: Use for verification



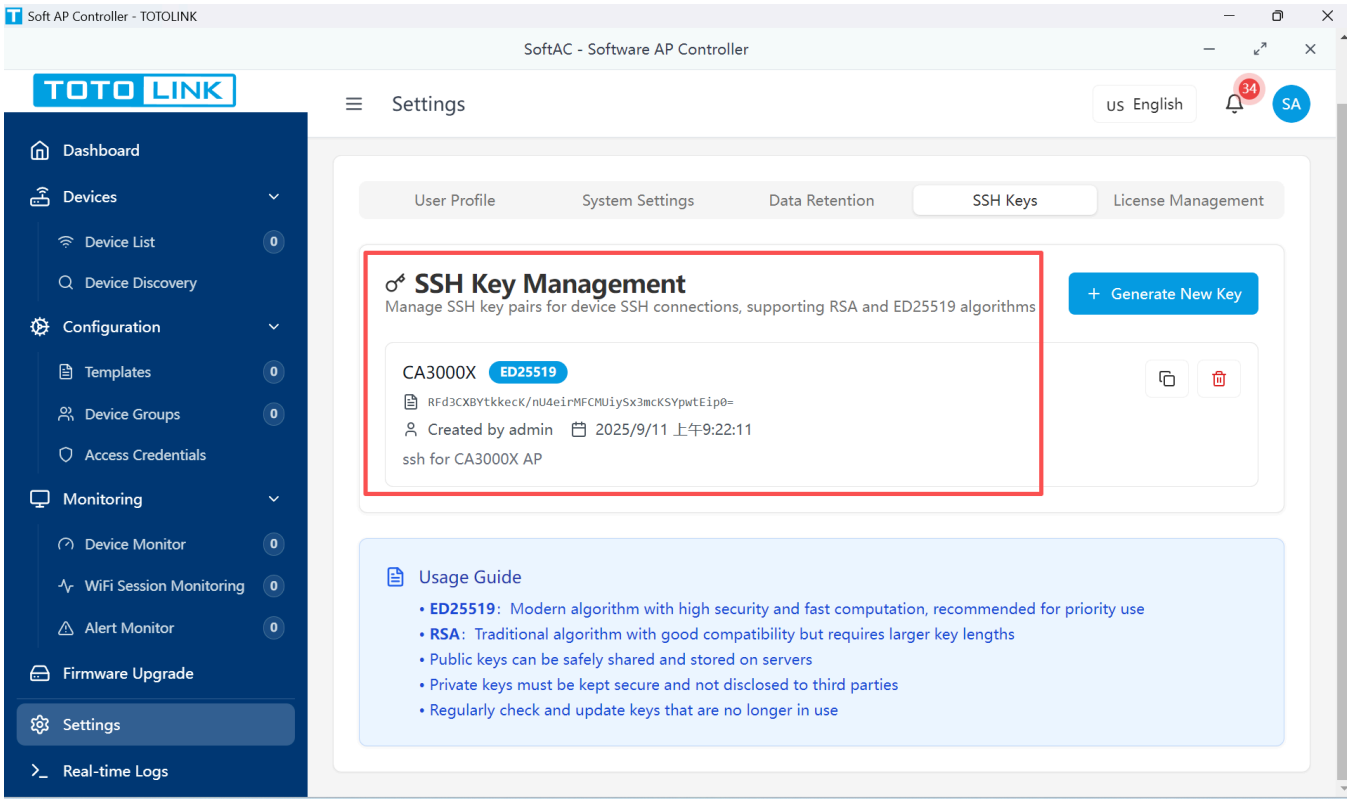
> ⚠️ **Critical Security**: Download and securely store the private key immediately. Once you close this dialog, the private key cannot be recovered.

Managing SSH Keys

Viewing Existing Keys

The SSH Key Manager displays all configured keys:

Column	Description
Name	Identifier for the key pair
Type	ED25519 or RSA
Fingerprint	Unique identifier for verification
Created	When the key was generated



Key Operations

Copy Public Key

1. Click the copy icon next to any key
2. Paste into device SSH configuration
3. The key is now ready for use

View Details

1. Click on the key name
2. See full public key content
3. Review usage statistics

Delete Key

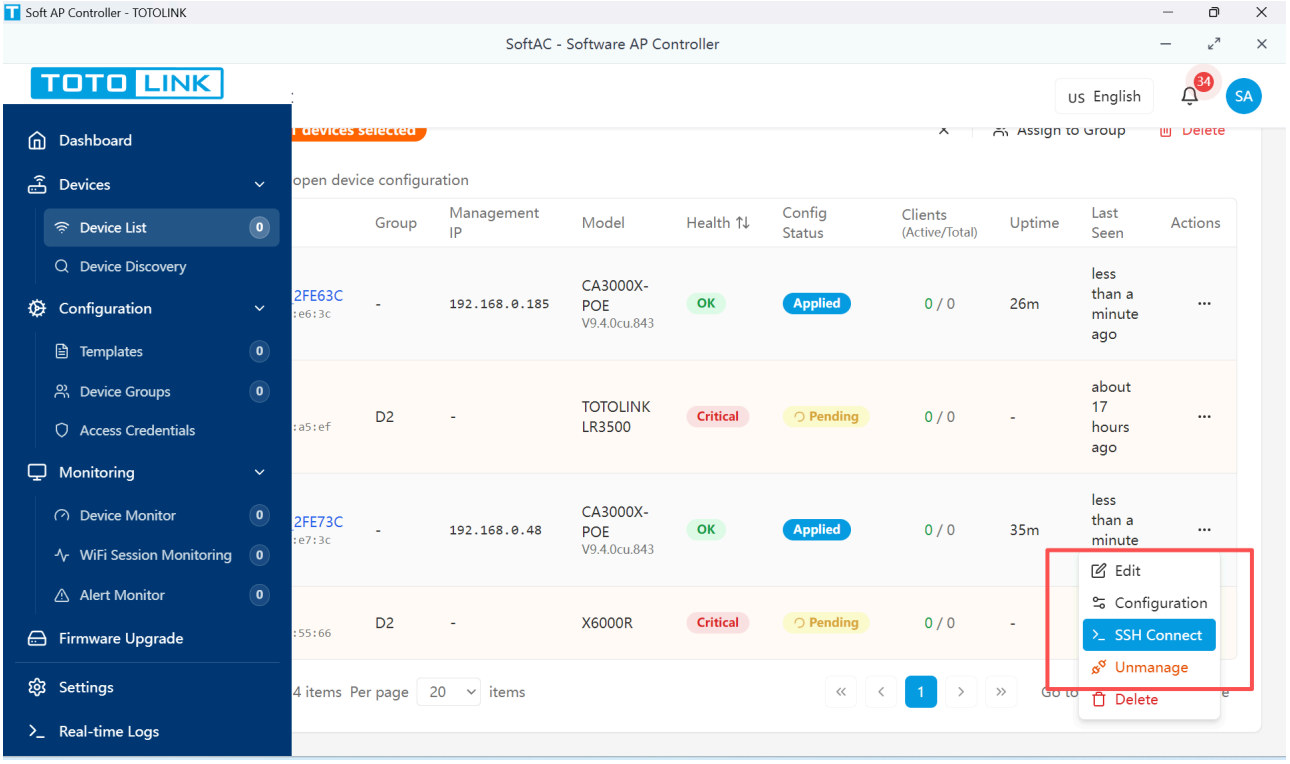
1. Click the delete icon
2. Confirm deletion
3. Note: Cannot delete if currently in use by devices

> 💡 **Tip**: Keep at least one backup SSH key pair in case the primary key is compromised or lost.

Using SSH Credentials with Devices

Associating Keys with Devices

1. **During Device Addition**
   When adding a new device:
   - Select "SSH" as the access method
   - Choose from available SSH credentials
   - Enter SSH username (usually "root" or "admin")
   - Specify SSH port (default: 22)



SSH Terminal Access

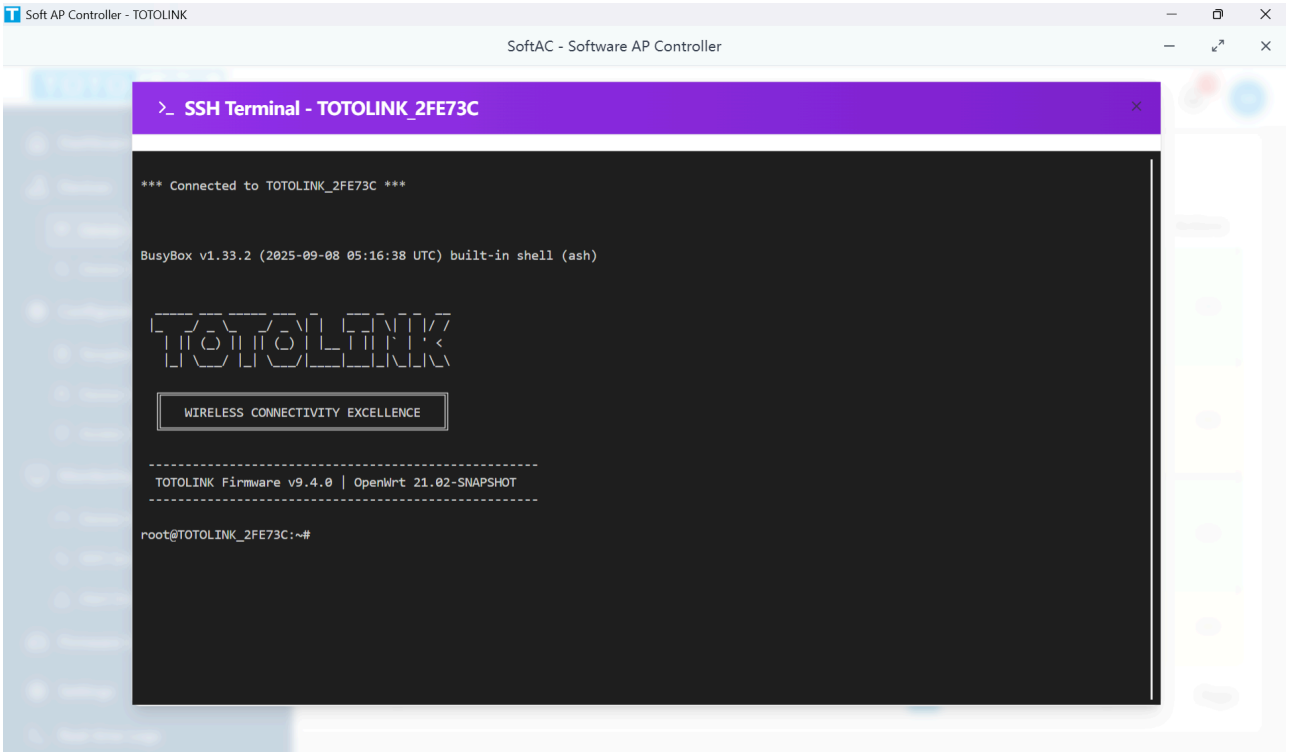
SoftAC provides direct SSH terminal access to devices:

1. **Open SSH Terminal**
   - Navigate to device details
   - Click "SSH Connect" button
   - System automatically authenticates

   [Screenshot: SSH Terminal button on device page]

2. **Terminal Features**
   - Full command-line access

- Copy/paste support
- Session logging
- Multiple tabs for different devices



10.3 Credential Security

Security Best Practices

Password and Key Management

Strong Credentials

- Use SSH keys instead of passwords when possible
- Generate keys with maximum supported length
- Use ED25519 keys for better security and performance

Regular Rotation

- Change credentials periodically (every 90 days recommended)
- Immediately rotate compromised credentials
- Keep audit logs of credential changes

Access Control

- Limit credential access to authorized administrators
- Use role-based permissions for credential management
- Implement two-factor authentication for sensitive operations

Credential Storage Security

Encryption at Rest

All credentials in SoftAC are protected:

Credential Type	Storage Method	Encryption
SSH Private Keys	Database	AES-256 encrypted
API Keys	Database	Salted hash
User Passwords	Database	Bcrypt hashed
Device Secrets	Database	AES-256 encrypted

Encryption in Transit

Data protection during transmission:

1. **HTTPS/TLS**
    - All web interface traffic encrypted
    - TLS 1.2 minimum version
    - Strong cipher suites only
2. **SSH Connections**
    - End-to-end encryption
    - Key exchange algorithms
    - Perfect forward secrecy
3. **API Communications**
    - HTTPS required for all API calls
    - Certificate validation
    - Encrypted payloads

Security Monitoring

Audit Logging

Track all credential-related activities:

Event	Logged Information
Credential Creation	Who, when, what type
Key Usage	Device, time, success/failure
Credential Modification	Changes made, by whom
Failed Authentications	Source, credential used, reason

Event	Logged Information
Credential Deletion	Who deleted, when, which credential

Security Alerts

Configure alerts for security events:

1. **Failed Authentication Attempts**
    - Multiple failures from same source
    - Attempts with invalid credentials
    - Brute force patterns detected
2. **Unusual Access Patterns**
    - Access from new locations
    - Outside normal hours
    - Rapid credential changes
3. **System Security Events**
    - Credential database access
    - Encryption key operations
    - Security setting changes

Compliance and Standards

Industry Standards

SoftAC credential management follows:

- **NIST Guidelines**: Key management best practices
- **PCI DSS**: If handling payment card data
- **ISO 27001**: Information security management
- **GDPR**: Data protection for EU users

Regular Security Tasks

Maintain credential security with:

Task	Frequency	Purpose
Review Access Logs	Daily	Detect anomalies
Verify Active Credentials	Weekly	Remove unused
Test Backup Keys	Monthly	Ensure recovery
Security Audit	Quarterly	Compliance check
Update Credentials	Annually	Prevent aging attacks

Emergency Procedures

Credential Compromise Response

If credentials are compromised:

1. **Immediate Actions**
   - Disable compromised credential
   - Generate new credentials
   - Update all affected devices
2. **Investigation**
   - Review access logs
   - Identify breach source
   - Check for unauthorized changes
3. **Recovery**
   - Reset all related credentials
   - Verify system integrity
   - Document incident

Backup and Recovery

Protect against credential loss:

1. **Backup Strategies**
   - Export encrypted credential backup
   - Store in secure, separate location
   - Test restoration procedures
2. **Recovery Procedures**
   - Import credential backup
   - Verify all credentials working
   - Update device configurations

> 🔒 **Security Reminder**: Store credential backups separately from system backups and encrypt with a different key.

Security Checklist

Regular security verification:

- [ ] All default credentials changed
- [ ] SSH keys using recommended algorithms
- [ ] API keys rotated within policy period
- [ ] No plaintext credentials in configurations
- [ ] Audit logs reviewed regularly

- [ ] Failed authentication alerts configured
- [ ] Backup credentials tested and secure
- [ ] Team trained on security procedures

Summary

TOTOLINK SoftAC's Credential Management system provides comprehensive security for device access:

- **SSH Credentials**: Secure key-based authentication for device management
- **API Keys**: Unique identifiers for automated device communication
- **Security Features**: Encryption, audit logging, and monitoring protect credentials

Quick Reference

Task	Location	Security Level
Generate SSH keys	Settings → SSH Key Manager	High (private key encrypted)
View device API key	Devices → Device Details	Medium (password required)
Check credential logs	Settings → System Logs	Audit trail maintained
Rotate credentials	Device/Settings pages	Immediate effect

> 🚀 **Next Steps**: Review your current credentials, ensure all default passwords are changed, and set up regular credential rotation schedules.

Related Topics

- 4. Device Management - Configuring device access
- 11. System Settings - Security configuration
- 12. User Management - Access control
- 14. Troubleshooting - Solving authentication issues

Part 11: System Settings

Overview

The System Settings module in TOTOLINK SoftAC allows you to configure and manage the fundamental operational parameters of your network management system. This chapter guides you through the various settings that control how your system operates, stores data, sends notifications, and maintains security.

Think of System Settings as the control center for your entire SoftAC installation - similar to the settings app on your smartphone, but specifically designed for network management.

Why System Settings Matter

Properly configured system settings ensure:

- **Reliable Operation**: Your network runs smoothly with appropriate timeouts and limits
- **Data Protection**: Important data is backed up and retained according to your needs
- **Timely Alerts**: You receive notifications when network issues arise
- **Storage Efficiency**: Old data is cleaned up automatically to save disk space
- **Security**: Your system remains protected with proper authentication settings

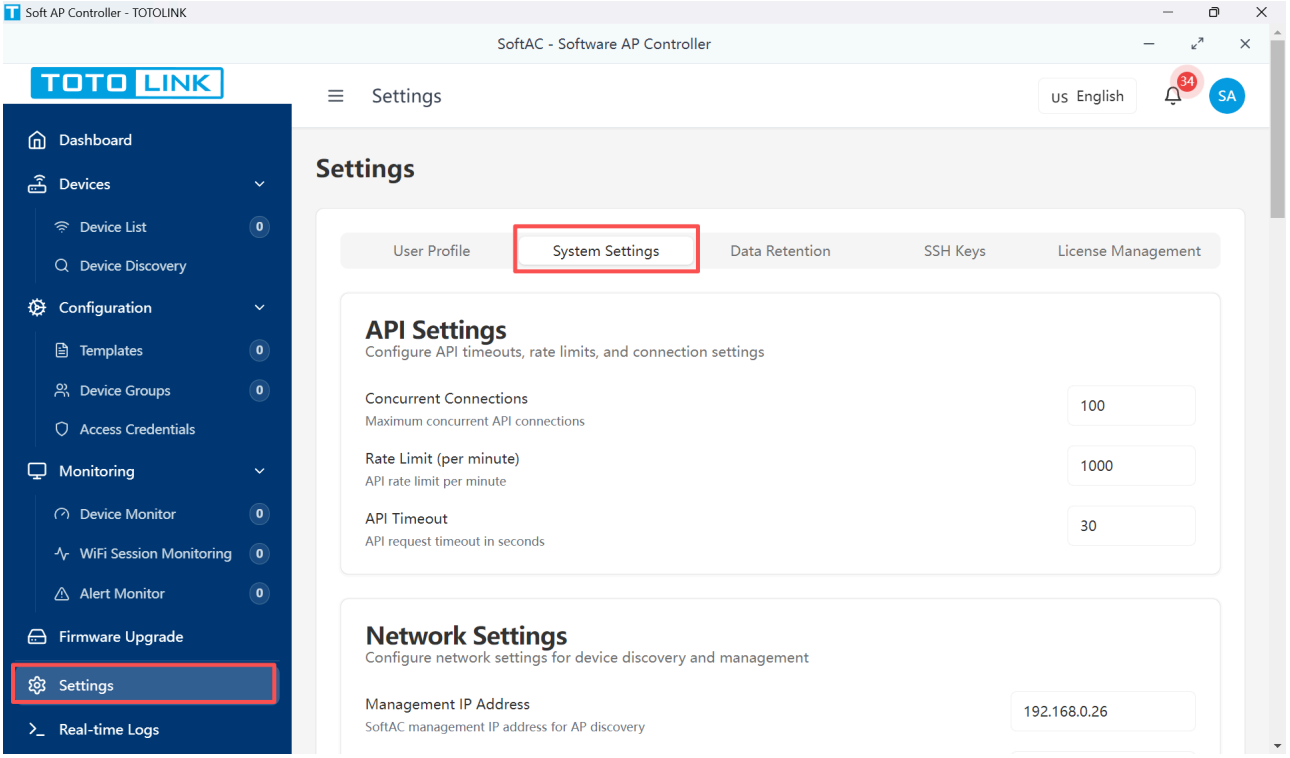
---

11.1 Basic Settings

Basic settings control the fundamental behavior of your SoftAC system. These settings affect how the system connects to devices, handles requests, and manages resources.

Accessing Basic Settings

1. **Navigate to Settings**
   Click on "Settings" in the left navigation menu.
2. **Select System Settings Tab**
   Click on the "System Settings" tab in the settings page.

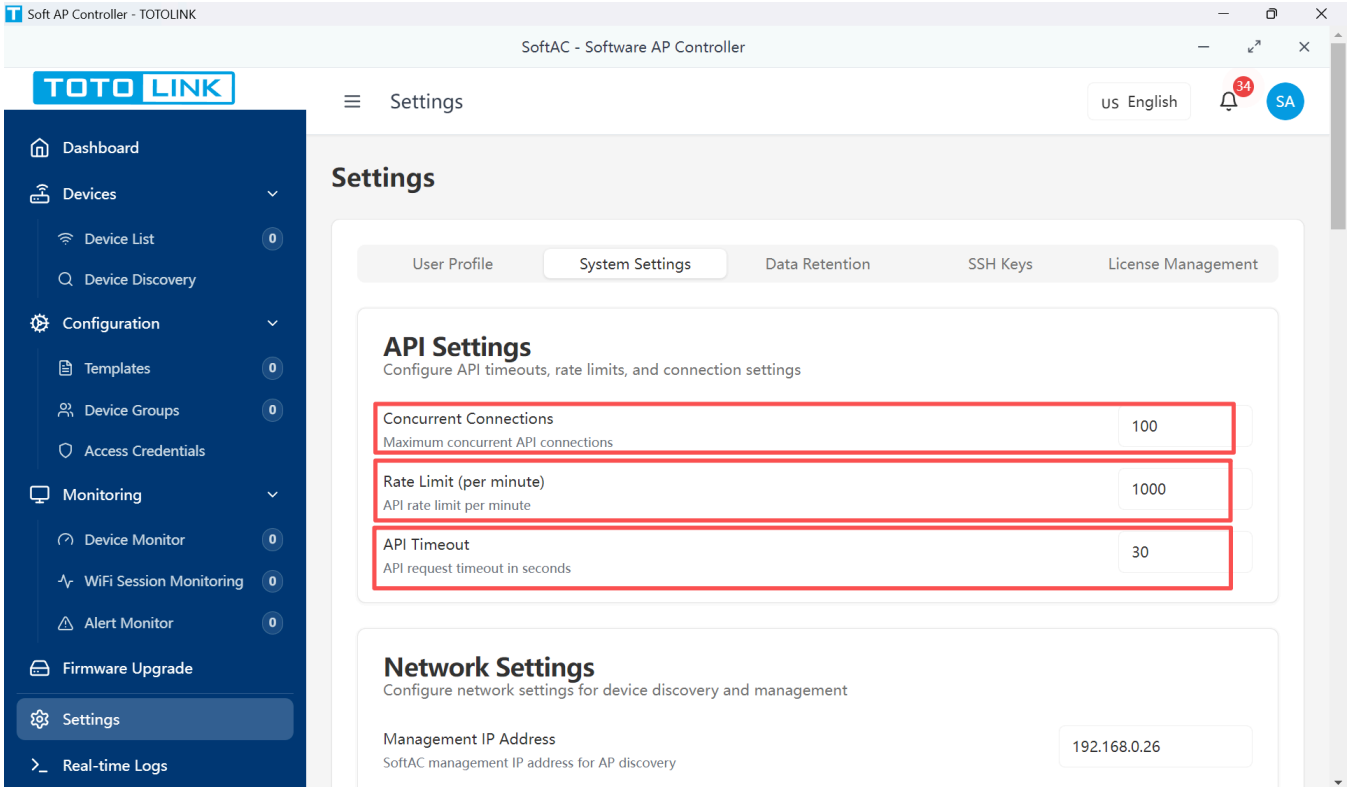


API Configuration

The API (Application Programming Interface) settings control how your system communicates with network devices.

Key API Settings

Setting	Description	Recommended Value
API Timeout	How long to wait for device responses	30 seconds
Concurrent Connections	Number of devices that can connect simultaneously	100
Rate Limit	Maximum requests per minute	1000



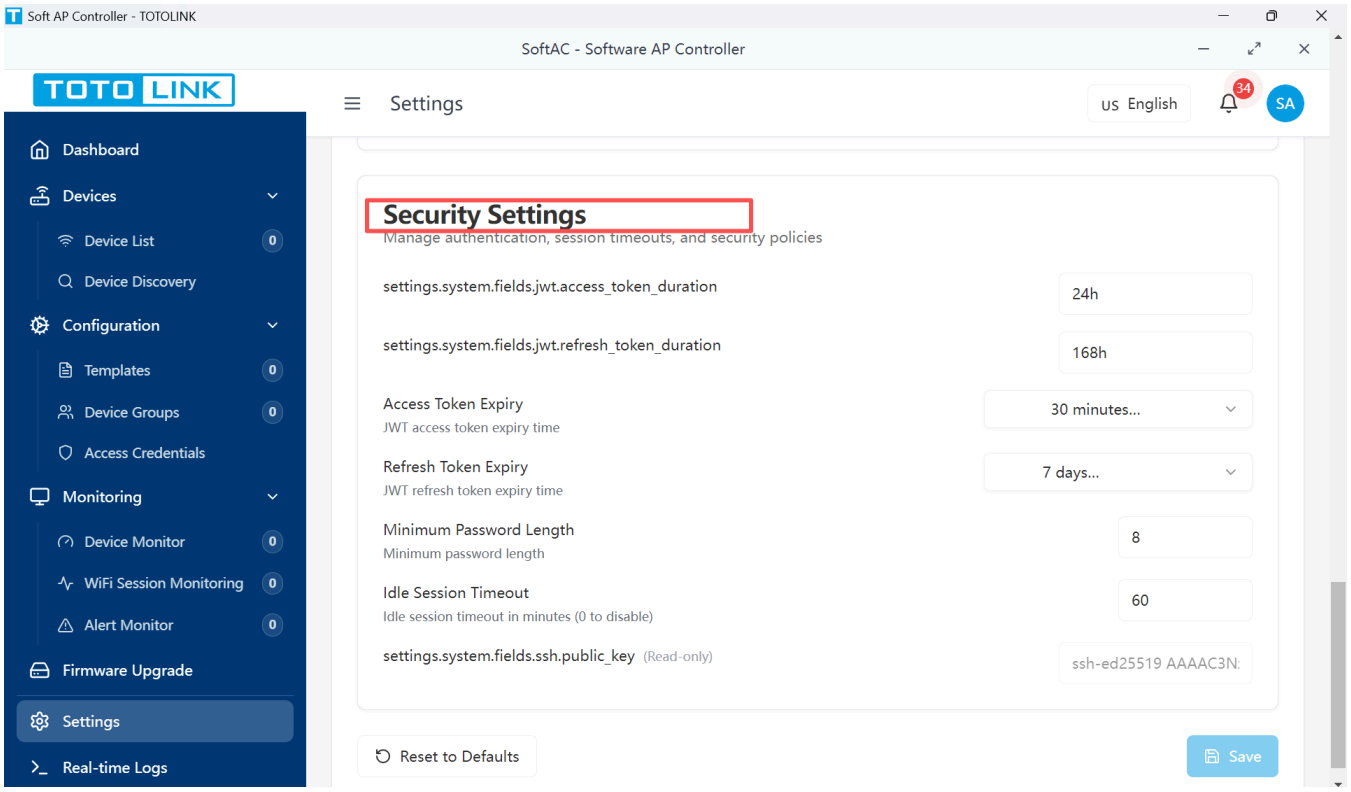
How to Configure API Settings

1. **API Timeout**
   - Increase this value if devices are far away or on slow connections
   - Decrease for faster response times on local networks
   - Default: 30 seconds
2. **Concurrent Connections**
   - Set based on your network size
   - Small networks (< 50 devices): 50-100
   - Medium networks (50-200 devices): 100-200
   - Large networks (> 200 devices): 200-500
3. **Rate Limit**
   - Prevents system overload
   - Leave at default unless experiencing performance issues

> 💡 **Tip**: Start with default values and adjust based on your network's performance. If devices frequently timeout, increase the API Timeout value.

Security Settings

Security settings protect your system from unauthorized access and define session behaviors.



Important Security Parameters

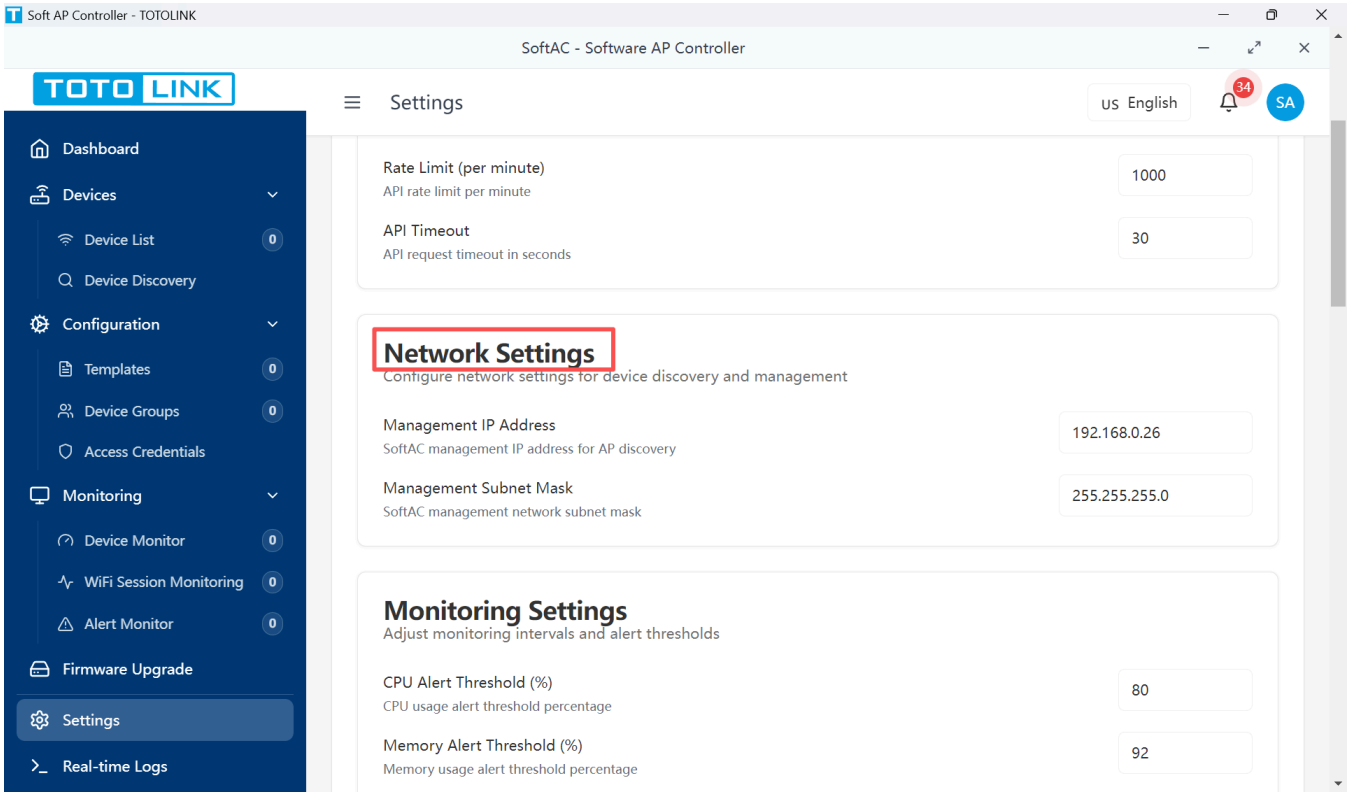
1. **Access Token Expiry**
   - How long you stay logged in while active
   - Default: 15 minutes
   - Longer times are more convenient but less secure
2. **Refresh Token Expiry**
   - How long your login session can be renewed
   - Default: 7 days
   - After this period, you must log in again
3. **Idle Session Timeout**
   - Automatic logout after inactivity
   - Default: 30 minutes
   - Protects against unauthorized access if you forget to log out
4. **Minimum Password Length**
   - Enforces strong passwords
   - Default: 8 characters
   - Recommended: At least 8-12 characters

> 🔒 **Security Best Practice**: Use shorter session timeouts in shared environments and longer timeouts for dedicated management stations.

11.2 Network Configuration

Network configuration determines how SoftAC discovers and manages devices on your network.

Management Network Settings



The management network is the network segment where SoftAC communicates with your devices.

Configuring Management IP

1. **Management IP Address**
   - The IP address SoftAC uses to communicate with devices
   - Example: 192.168.1.100
   - Must be on the same network as your managed devices
2. **Management Subnet Mask**
   - Defines the network range
   - Common values:
     - 255.255.255.0 (manages 254 devices)
     - 255.255.0.0 (manages 65,534 devices)

11.3 Notification Settings

Notification settings control how SoftAC alerts you about important events and system status changes.

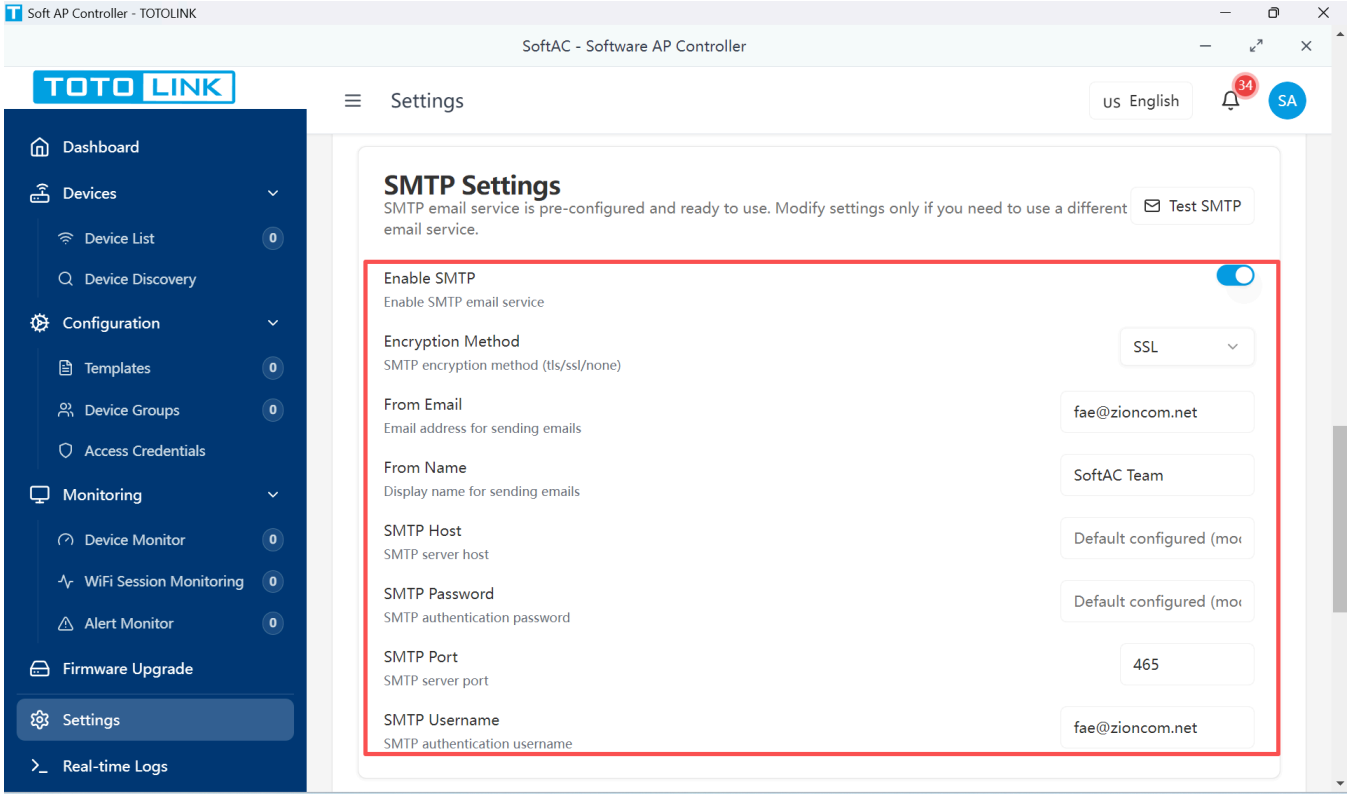
Email Notifications (SMTP Configuration)

SMTP (Simple Mail Transfer Protocol) settings enable SoftAC to send email alerts.

Setting Up Email Notifications

1. **Enable SMTP**
   Toggle the switch to activate email notifications.
2. **Configure Mail Server**

Setting	Description	Example
SMTP Host	Your email server address	smtp.gmail.com
SMTP Port	Server port number	587 (TLS) or 465 (SSL)
Encryption	Security method	TLS recommended
Username	Your email account	admin@company.com
Password	Email password or app password	Use app-specific password
From Email	Sender address	alerts@company.com
From Name	Sender display name	SoftAC Alerts



Common Email Providers Settings

Gmail

- Host: smtp.gmail.com
- Port: 587
- Encryption: TLS
- Note: Requires app-specific password

Outlook/Office 365

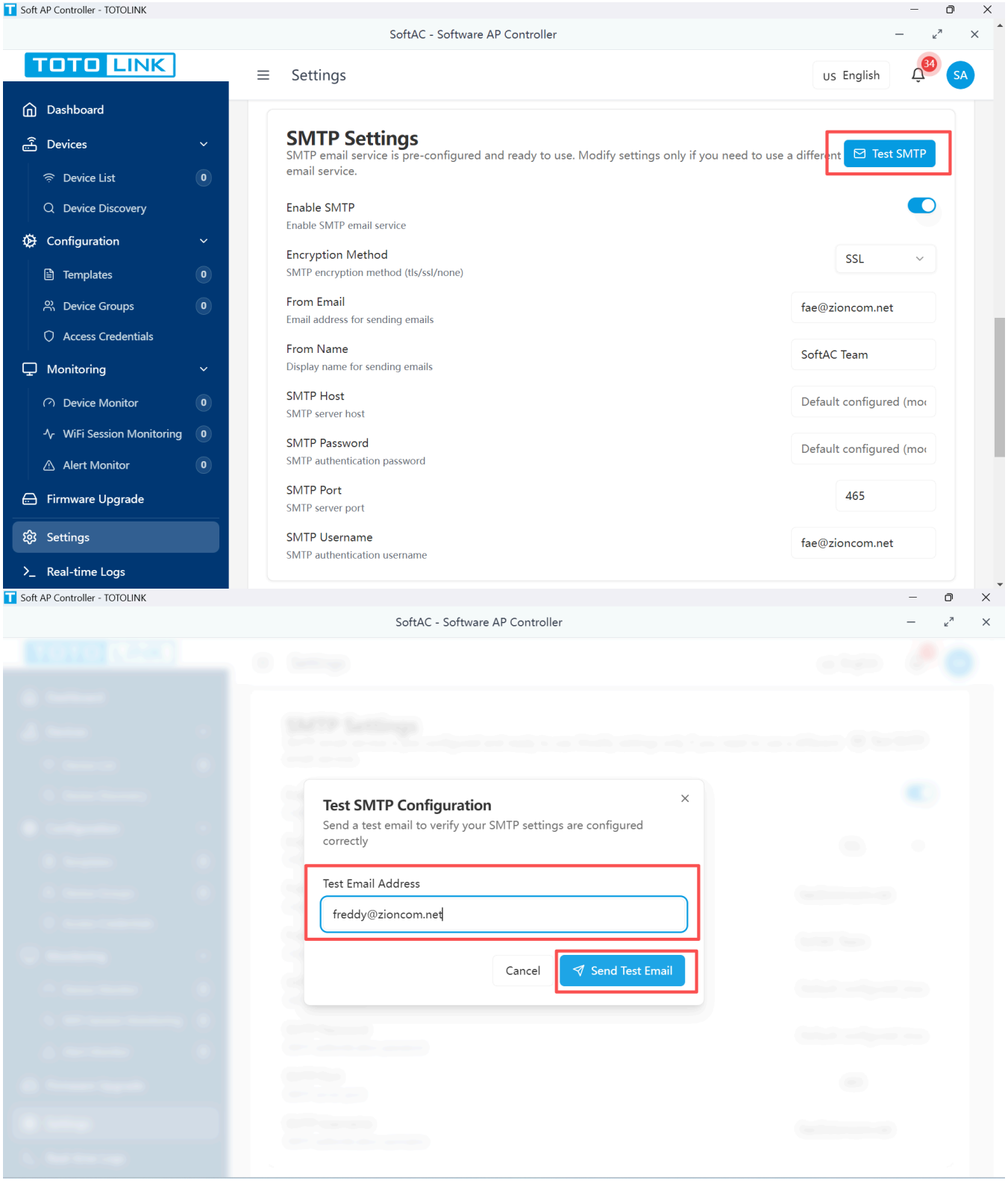
- Host: smtp.office365.com
- Port: 587
- Encryption: TLS

Yahoo Mail

- Host: smtp.mail.yahoo.com
- Port: 587 or 465
- Encryption: TLS or SSL

Testing Email Configuration

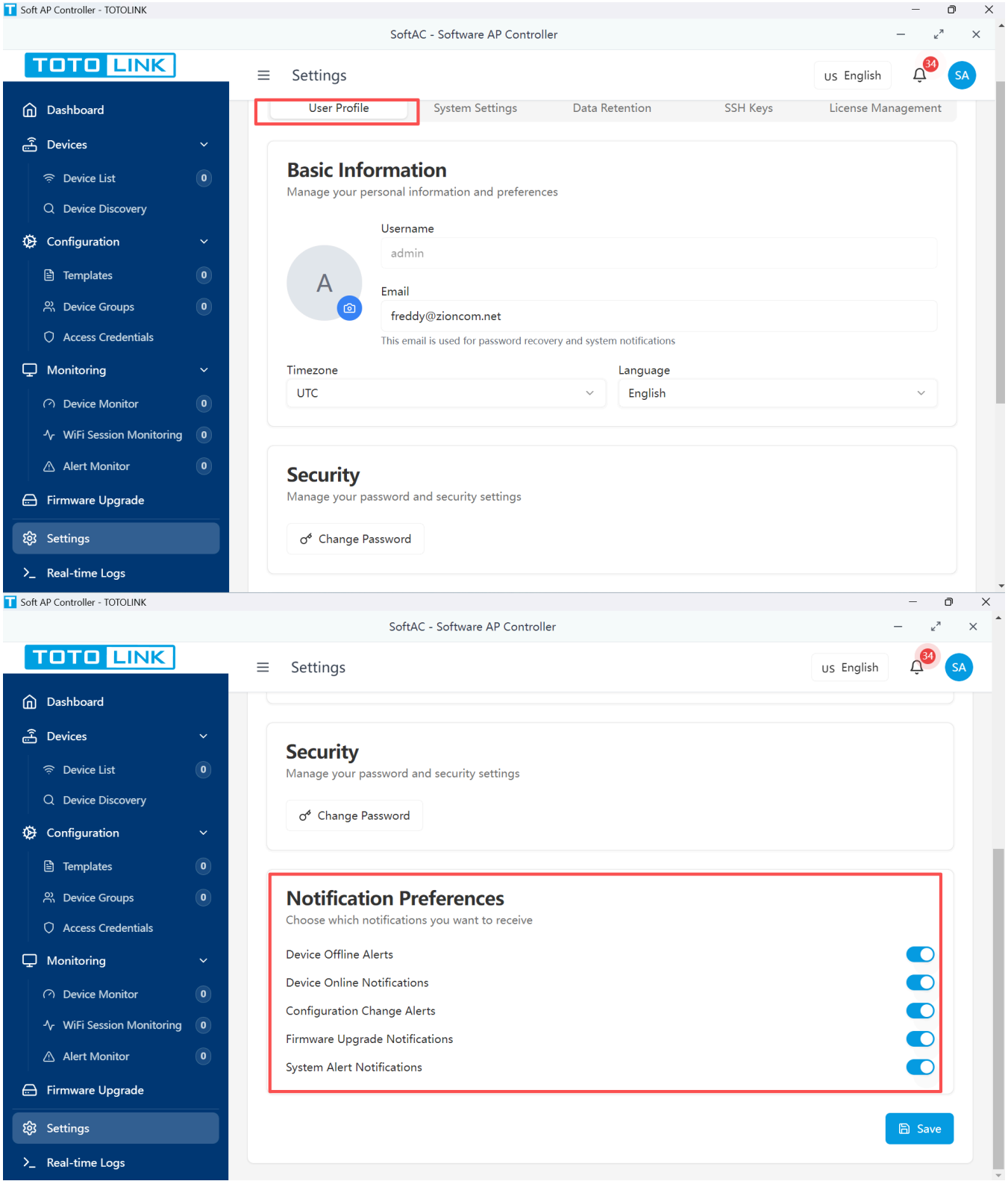
1. Click the **Test SMTP** button
2. Enter a test email address
3. Click **Send Test Email**
4. Check your inbox for the test message



> ⚠️ **Important**: For Gmail and other secure providers, use an app-specific password instead of your regular password. Enable 2-factor authentication and generate an app password in your email security settings.

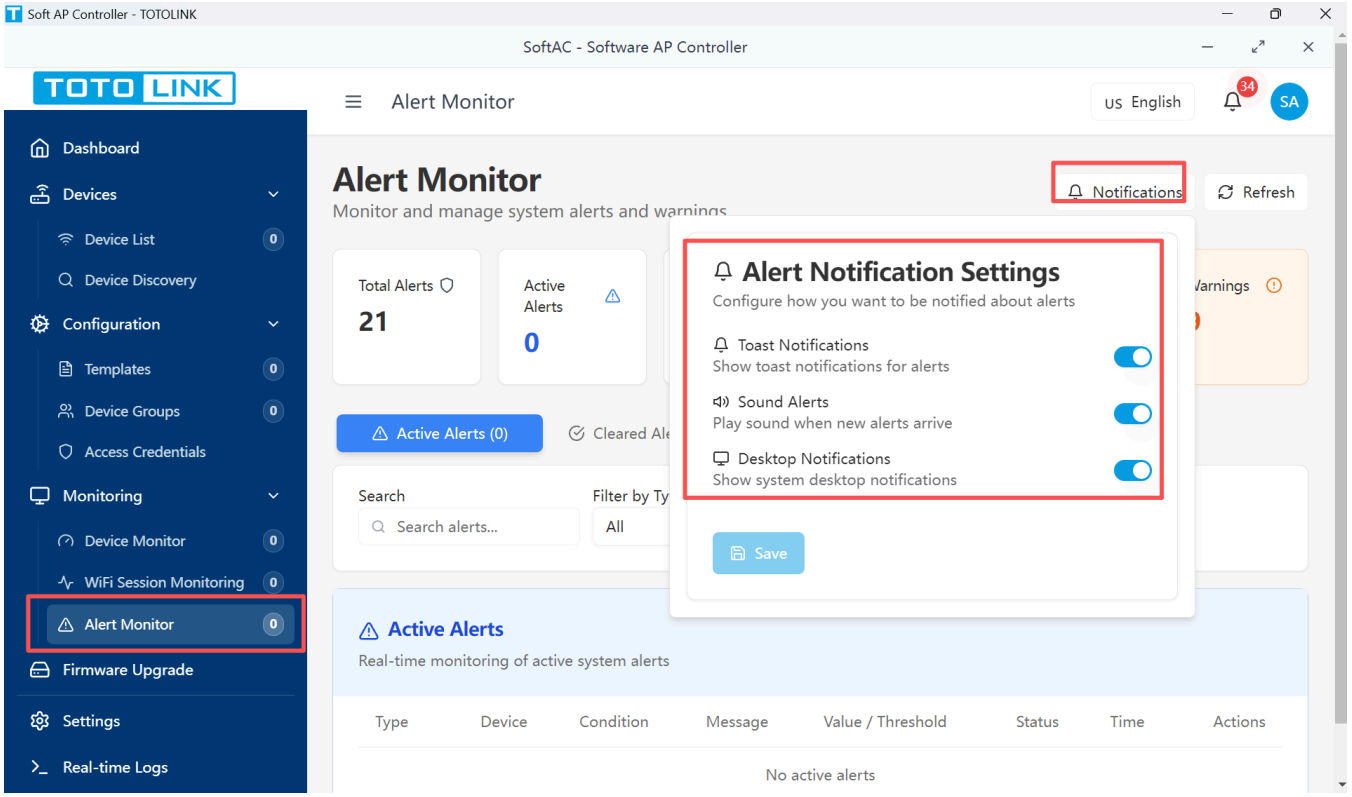
Alert Notification Preferences

Configure which types of alerts trigger notifications:



- **Device Offline Alerts**: Notified when devices disconnect
- **Configuration Changes**: Alerts for device configuration modifications
- **Firmware Updates**: Notifications about available firmware updates
- **System Alerts**: Critical system events and errors
- **Performance Warnings**: CPU, memory, or disk usage alerts

Notification Delivery Methods



1. **Toast Notifications**
    - Pop-up messages within the SoftAC interface
    - Immediate visibility while using the system
2. **Sound Alerts**
    - Audio alerts for critical events
    - Useful when monitoring multiple screens
3. **Desktop Notifications**
    - System-level notifications
    - Visible even when SoftAC is minimized

11.4 Backup and Recovery

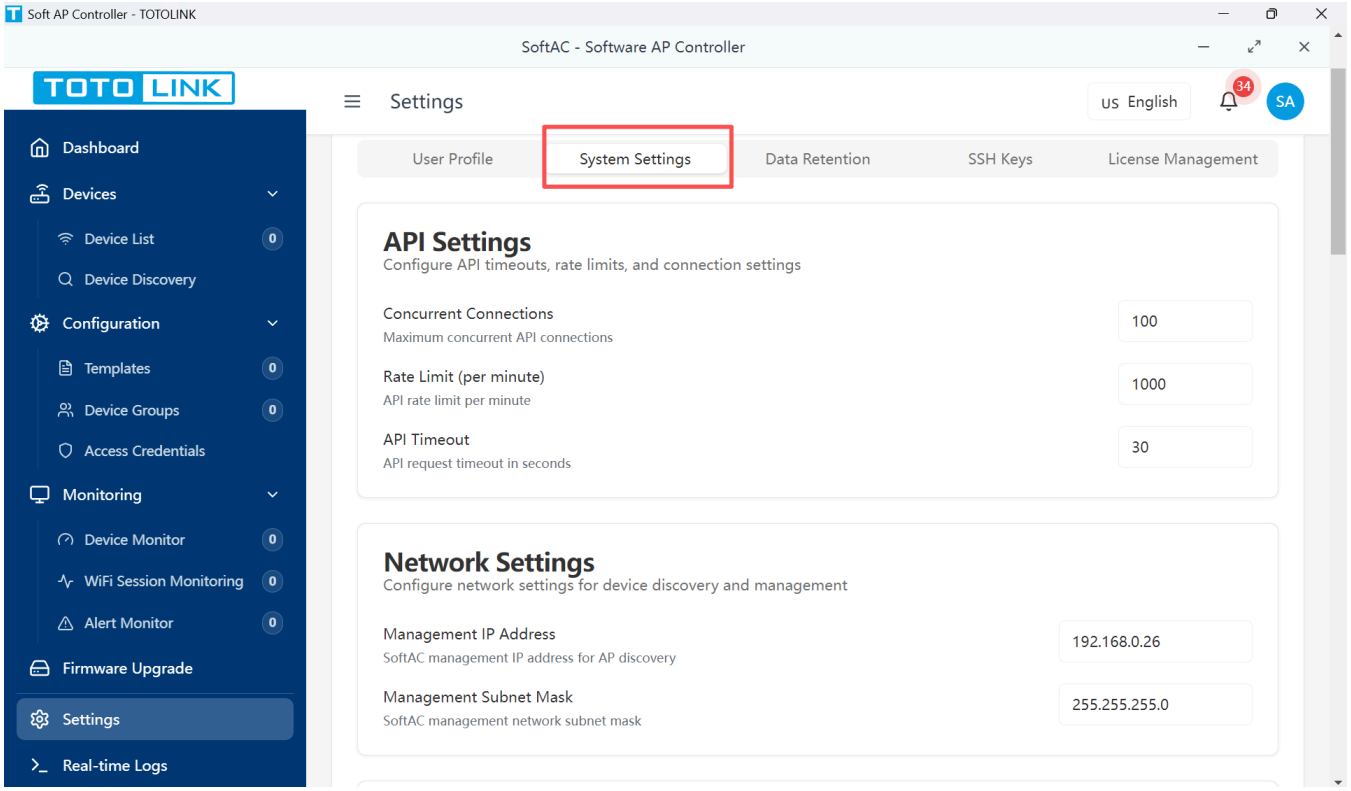
Regular backups protect your configuration and ensure quick recovery from system failures.

Understanding Backups

SoftAC backups include:

- Device configurations
- User settings and preferences
- Alert rules and thresholds
- System configuration
- Historical data (optional)

Automatic Backup Configuration

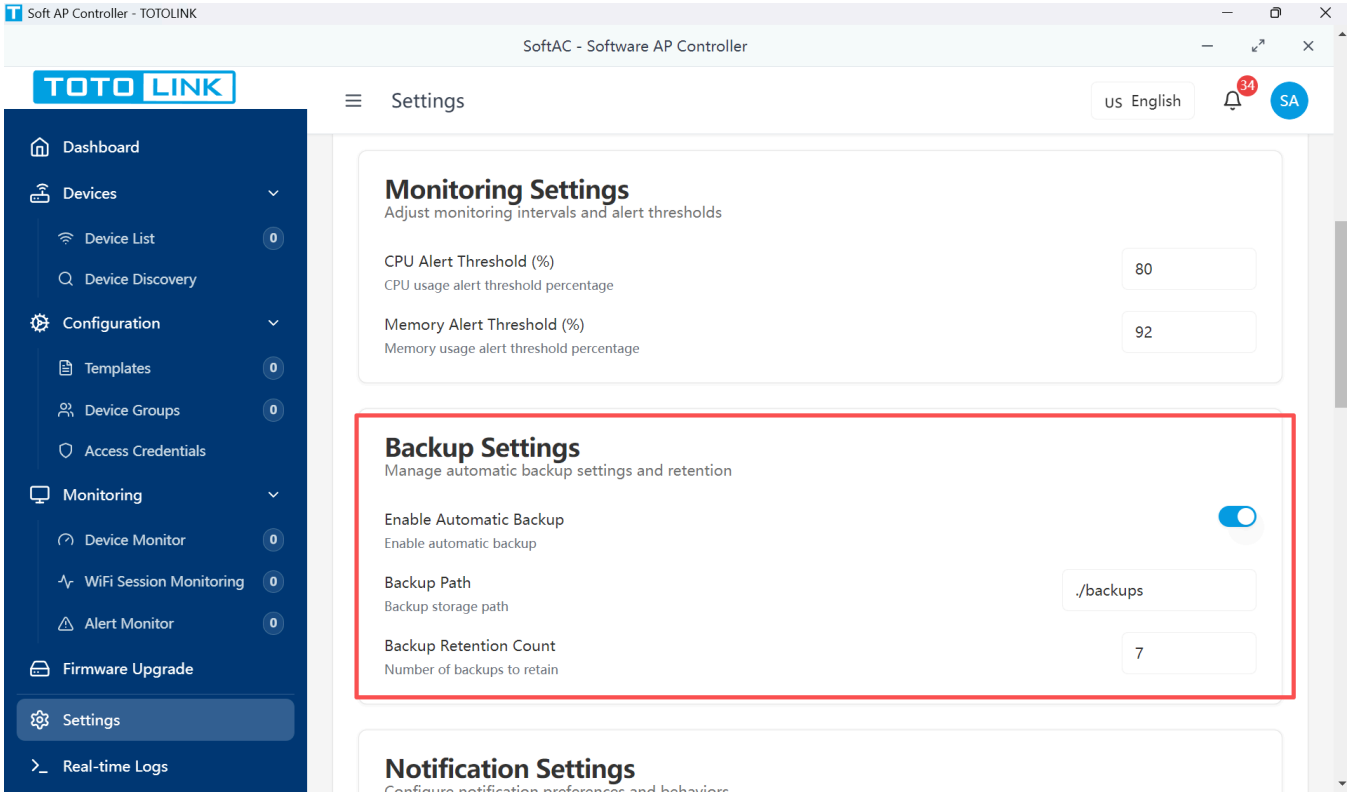


Setting Up Automatic Backups

1. **Enable Automatic Backup**
   Toggle the switch to activate scheduled backups.
2. **Backup Path**

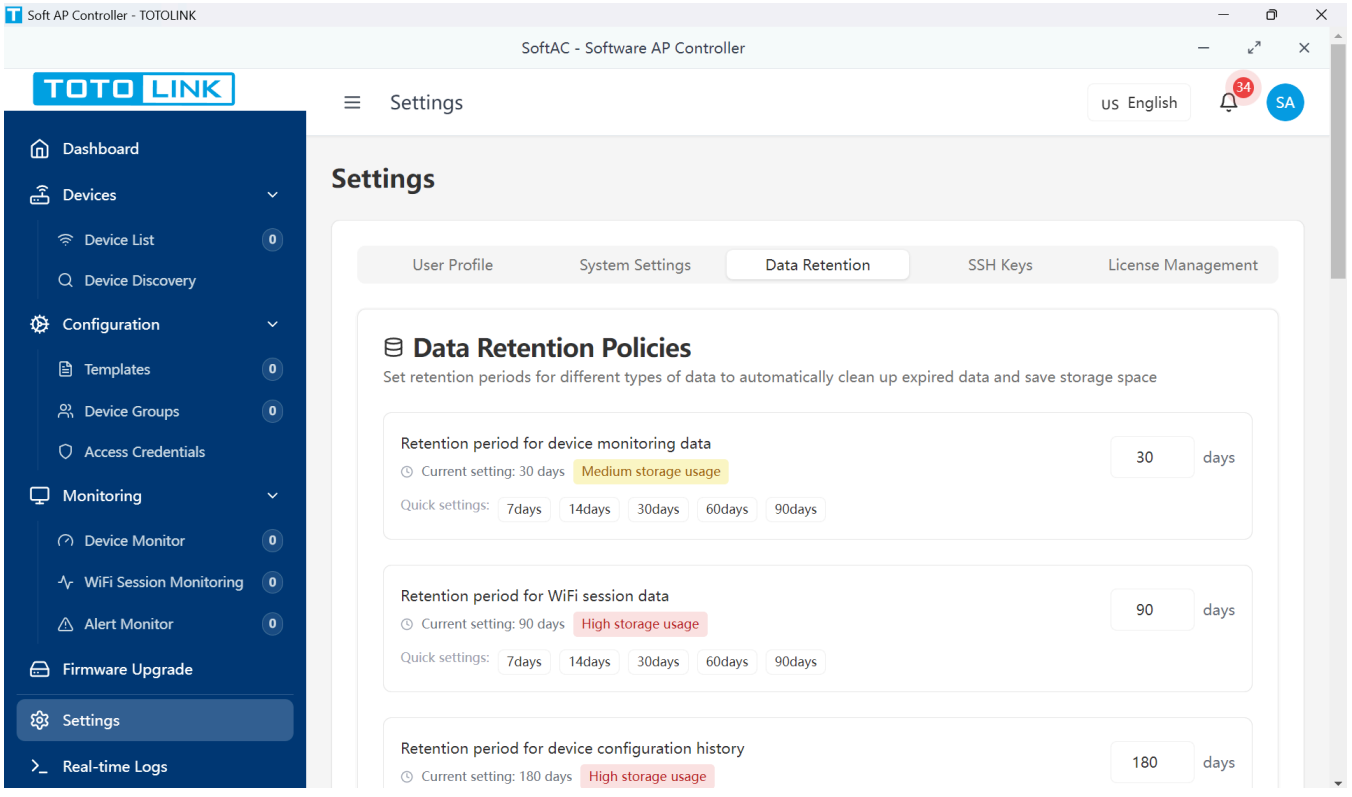
   Backup storage files will be created in this path.
3. **Backup Retention Count**

   Number of backups to retain.



Data Retention Policies

Data retention policies automatically clean up old data to save storage space.

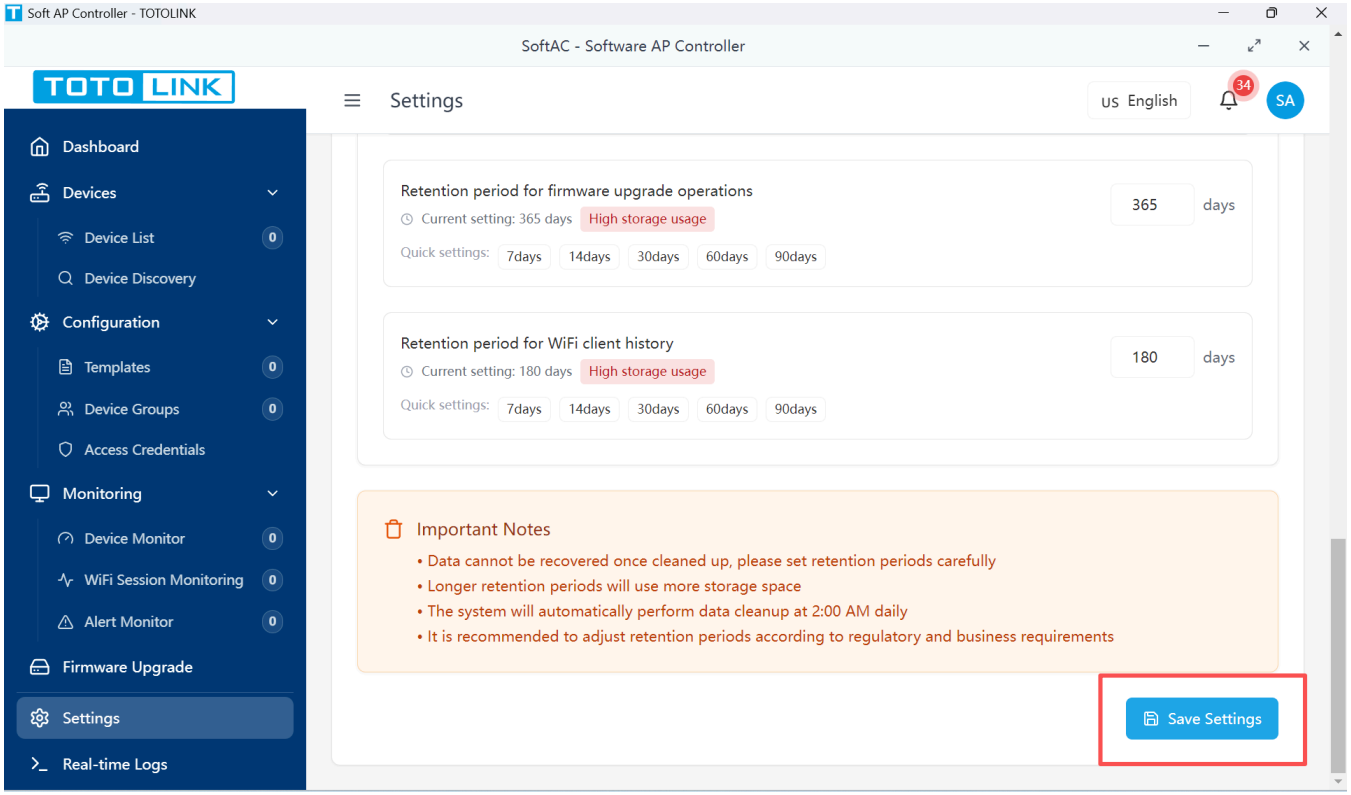


Configurable Retention Periods

Data Type	Description	Default	Recommended
Monitoring Data	CPU, memory, disk usage	30 days	30-90 days
WiFi Sessions	Connection records	90 days	7-30 days
Configuration History	Change logs	180 days	90-365 days
Cleared Alert	Past alerts	30 days	30-90 days
Upgrade Logs	Upgrade records	30 days	30-60 days
Upgrade Operations	Detailed upgrade data	365 days	365-730 days
Acknowledged Alerts	All alerts received currently	90 days	30-90 days
Operation Logs	Operation records	90 days	30-90 days
System Logs	System records	30 days	7-30 days
Firmware Upgrade Operations	Upgrade history	365 days	7-90 days
WiFi Client History	Records of WiFi accessing	180 days	7-90 days

Setting Retention Policies

1. Navigate to **Data Retention** tab
2. Adjust days for each data type
3. Use quick settings buttons for common values
4. Monitor storage impact indicator:
    - 🟢 Green: Low storage usage
    - 🟡 Yellow: Medium storage usage
    - 🔴 Red: High storage usage
5. Click **Save Settings**



> 💡 **Tip**: Balance between data availability and storage costs. Keep critical data longer (configuration history, upgrade operations) and routine data shorter (WiFi sessions, monitoring data).

Summary

Proper system settings configuration is essential for optimal SoftAC performance. Key takeaways:

- **Start with defaults**: Begin with recommended settings and adjust based on experience
- **Regular backups**: Enable automatic backups to protect your configuration
- **Monitor storage**: Use data retention policies to balance history and disk space
- **Test changes**: Always test significant changes during maintenance windows

Next Steps

- Configure email notifications for critical alerts
- Set up automatic backups
- Review and adjust data retention policies
- Check for available system updates

Related Topics

- Chapter 12: User Management - Managing user accounts and permissions
- Chapter 13: Log Management - System and audit log configuration
- Chapter 9: Device Discovery - Automatic device detection settings

- Chapter 7.3: Alert Management - Configuring alert thresholds

---

For additional support, contact TOTOLINK technical support or consult the online knowledge base.

Part 12: User Management

Overview

TOTOLINK SoftAC operates with a single administrator account system, providing centralized control over your network management platform. This chapter covers how to manage your administrator account, maintain security, and track system activities through comprehensive audit logging.

Unlike multi-user systems, SoftAC's single-admin design ensures maximum security and simplified management - perfect for small to medium-sized networks where one trusted administrator handles all network operations.

Why Single Administrator Design?

The single administrator model provides:

- **Maximum Security**: No risk of privilege escalation or unauthorized user creation
- **Simplified Management**: No complex permission systems to configure
- **Clear Accountability**: All actions traced to one responsible administrator
- **Reduced Attack Surface**: Fewer accounts mean fewer potential security vulnerabilities
- **Streamlined Operation**: No user conflicts or permission issues

---

12.1 Administrator Account

The administrator account is the master key to your SoftAC system. It has complete control over all network management functions.

Understanding the Admin Account

Your SoftAC system has exactly one administrator account with:

- Full system access and control
- Complete device management capabilities
- All configuration permissions
- System maintenance privileges

Initial Setup Process

When you first install SoftAC, you must complete the mandatory initial setup

Default Credentials (First Login Only)

```
Username: admin
Password: admin123
```

> 🔴 **Critical Security**: These default credentials work only for the first login. You MUST change them immediately.

Mandatory Setup Steps

1. **First Login**
   - Enter default username: `admin`
   - Enter default password: `admin123`
   - System detects first-time login
2. **Security Configuration**

   Required Changes:
   - **New Password**: Must be different from default
     - Minimum 8 characters
     - Include letters and numbers
     - Remember this - there's only one account!
   - **Email Address**: Critical for account recovery
     - Must be valid and accessible
     - Used for password reset codes
     - Receives system notifications
3. **Complete Setup**
   - Click "Complete Setup"
   - System saves new credentials
   - Default password permanently disabled
   - Redirected to main dashboard

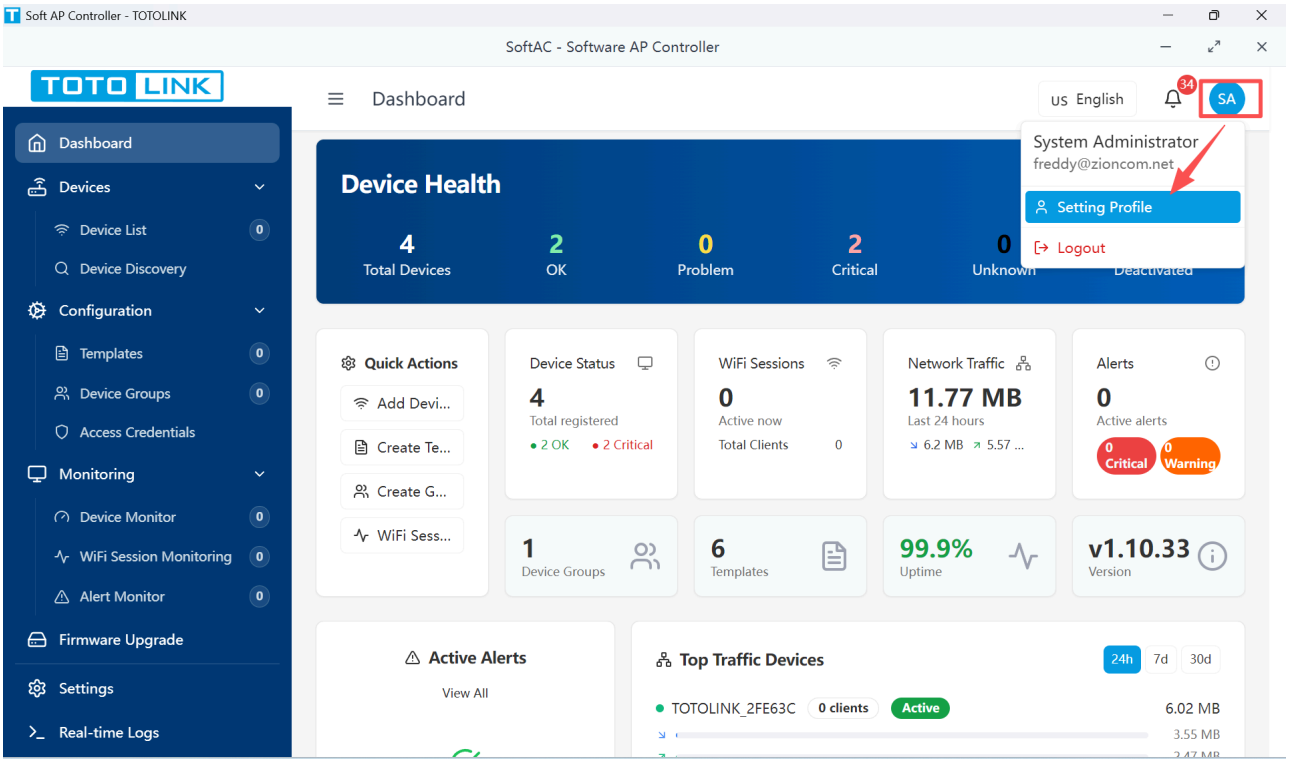
> ⚠️ **Warning**: You cannot skip initial setup. The system will not function until you secure the admin account.

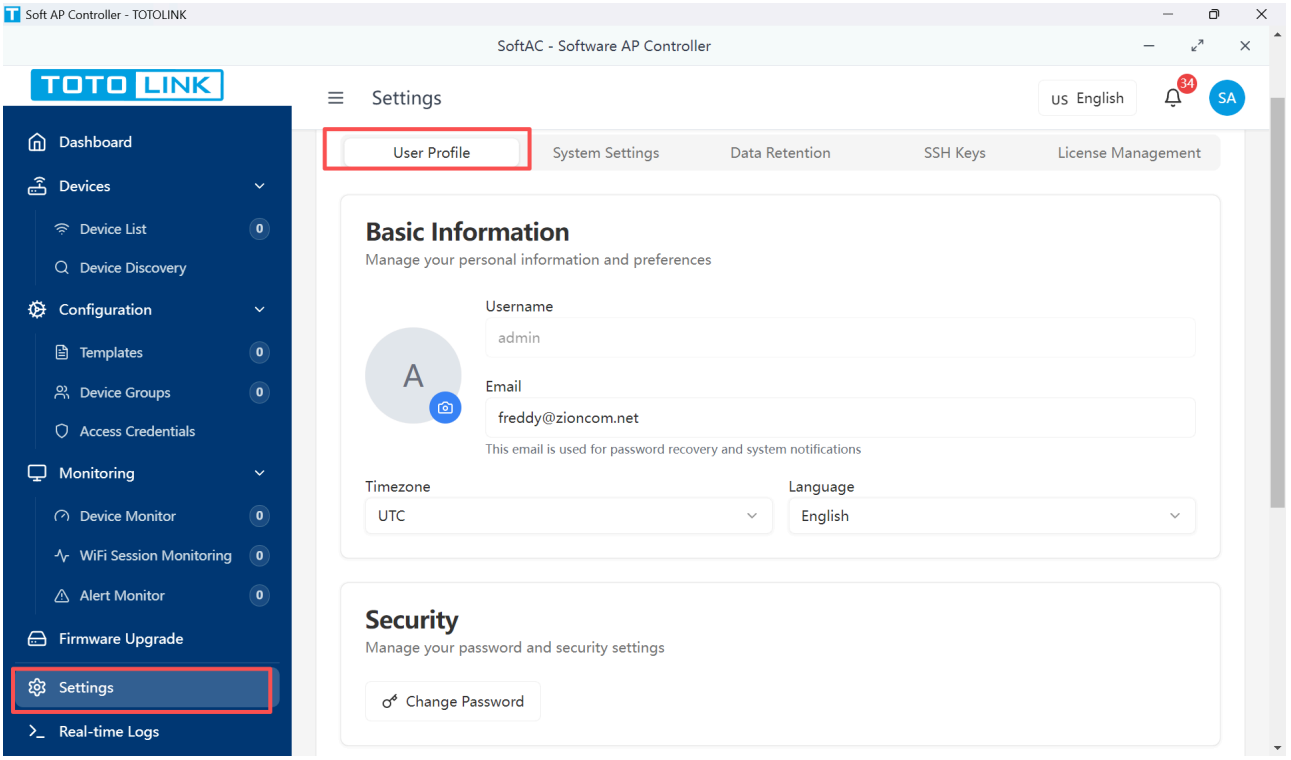
Managing Your Admin Profile

Access your profile settings to update account information

Accessing Profile Settings

1. Click your username in the top-right corner
2. Select "Setting Profile"
3. Or navigate to Settings → User Profile





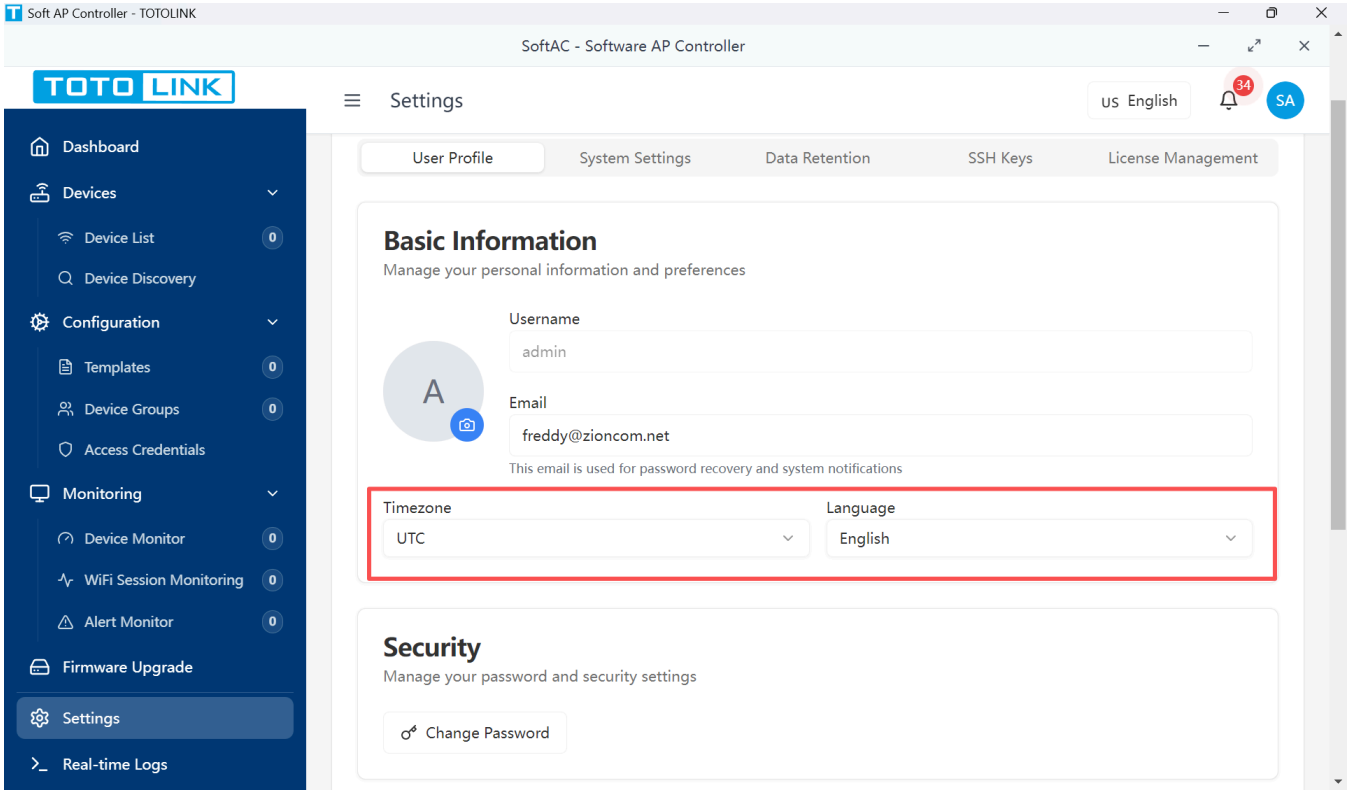
Updatable Information

Basic Information:

- **Email Address**
  - Required for password recovery
  - Must be valid email format
  - Test delivery before saving
- **Username**
  - Display name in interface
  - Appears in audit logs
  - Helps identify administrator in reports
- **Avatar**
  - Upload profile picture
  - JPG/PNG format
  - Maximum 2MB size

Preferences:

- **Language**
  - Interface language
  - Options: English, Chinese (Traditional/Simplified), Vietnamese, Indonesian, Japanese, Korean
- **Timezone**
  - Affects log timestamps
  - Report generation times
  - Scheduled task execution

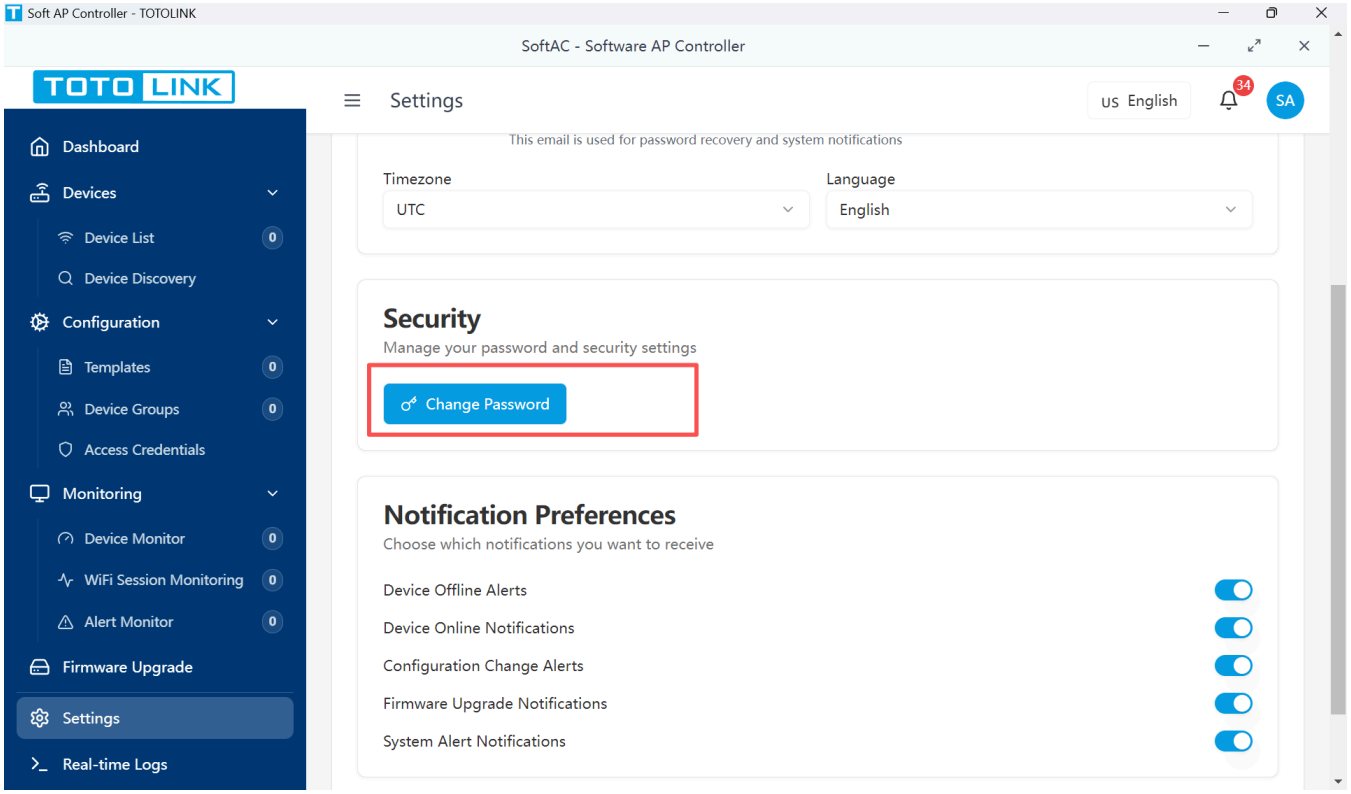


Saving Profile Changes

1. Make desired changes
2. Click "Save"
3. Some changes (like language) require page refresh
4. Email changes require verification

Password Management

Since there's only one account, password security is critical:



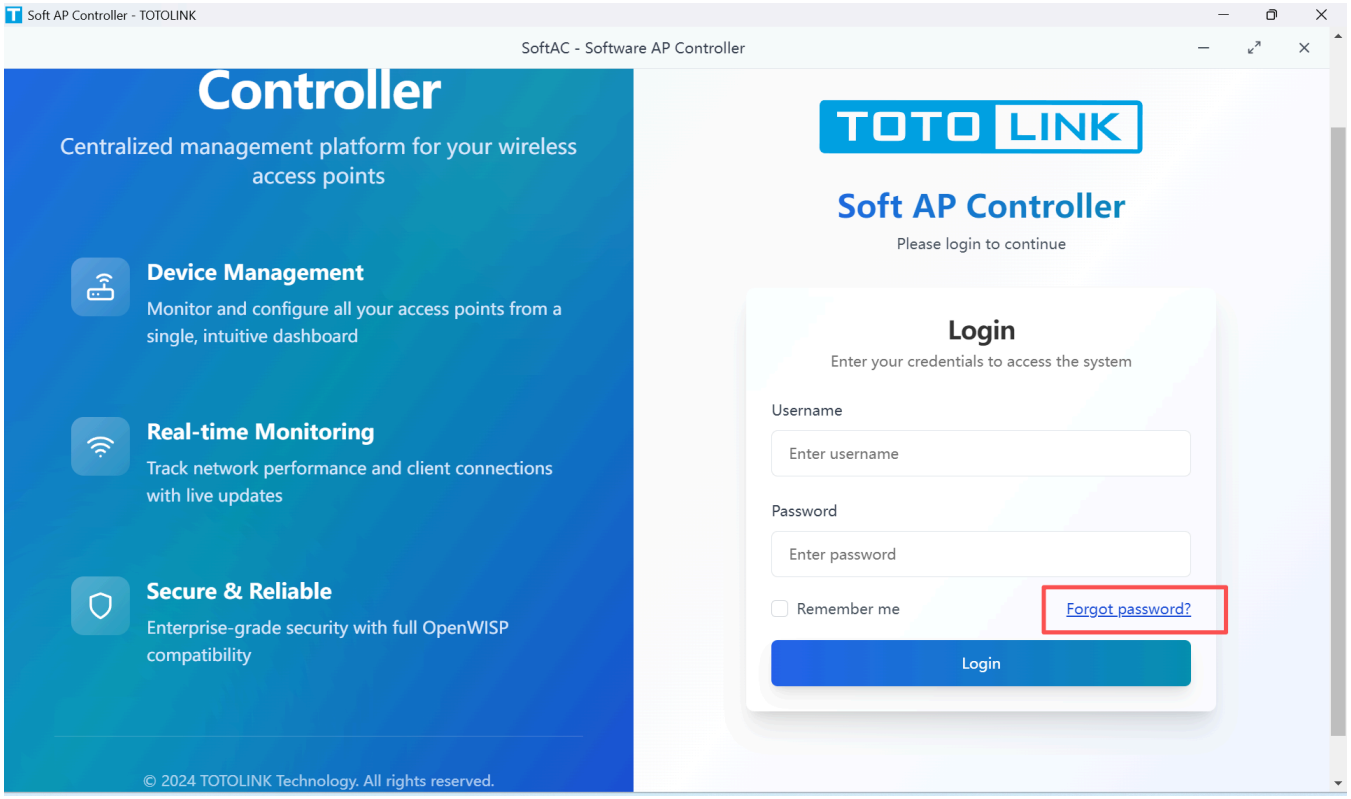
Changing Your Password

1. **Access Password Change**
   - Click "Change Password" in profile settings
   - Or use Security tab
2. **Enter Required Information**
   - Current password (for verification)
   - New password (meeting requirements)
   - Confirm new password (must match)
3. **Password Requirements**
   - Minimum 8 characters (configurable)
   - Must differ from current password
   - Should include mixed characters
   - Cannot be common passwords
4. **Complete Change**
   - Click "Update Password"
   - You'll be logged out
   - Log in with new password

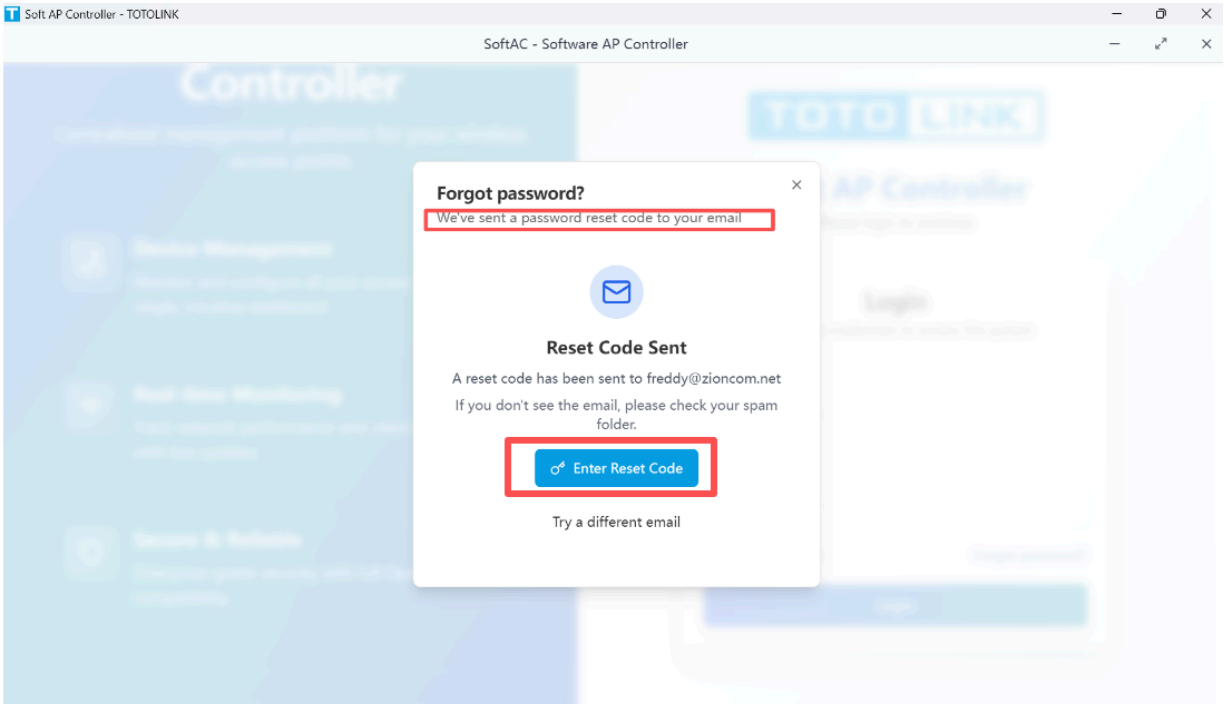
> 💡 **Best Practice**: Change your password every 90 days and use a password manager to store it securely.

Password Recovery

If you forget your password:

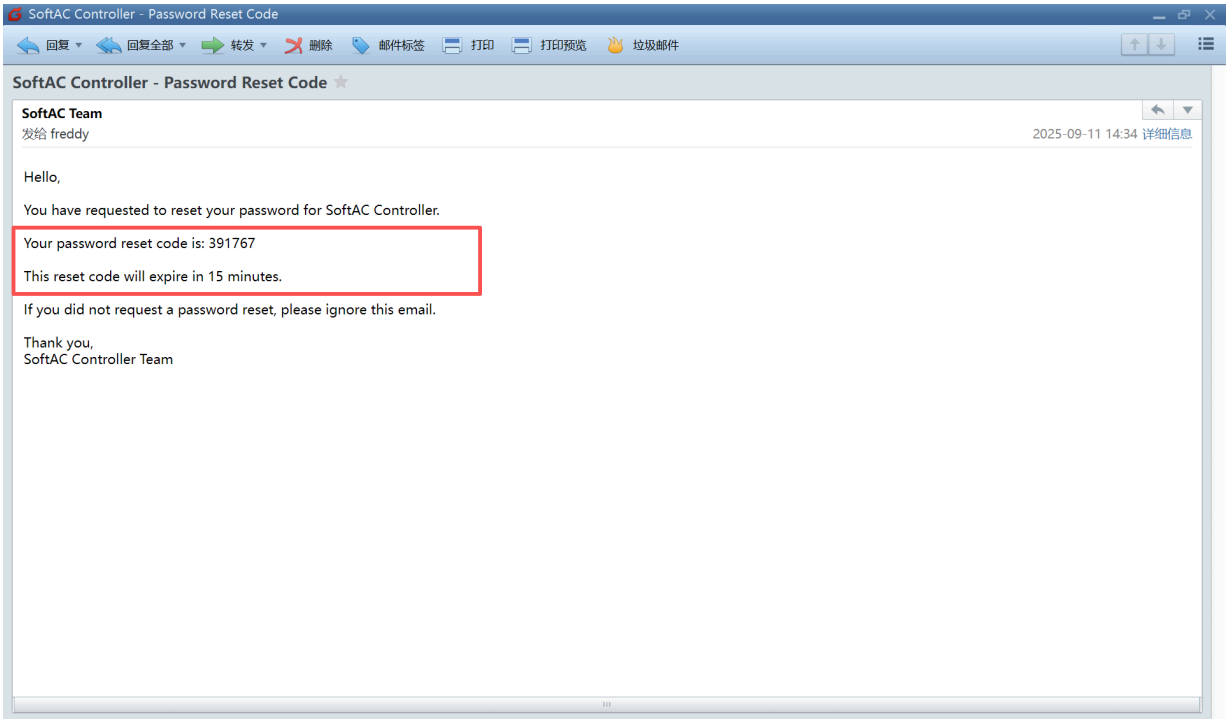


1. **Initiate Recovery**
    - Click "Forgot Password?" on login screen
    - Enter your registered email address
    - Click "Send Reset Code"

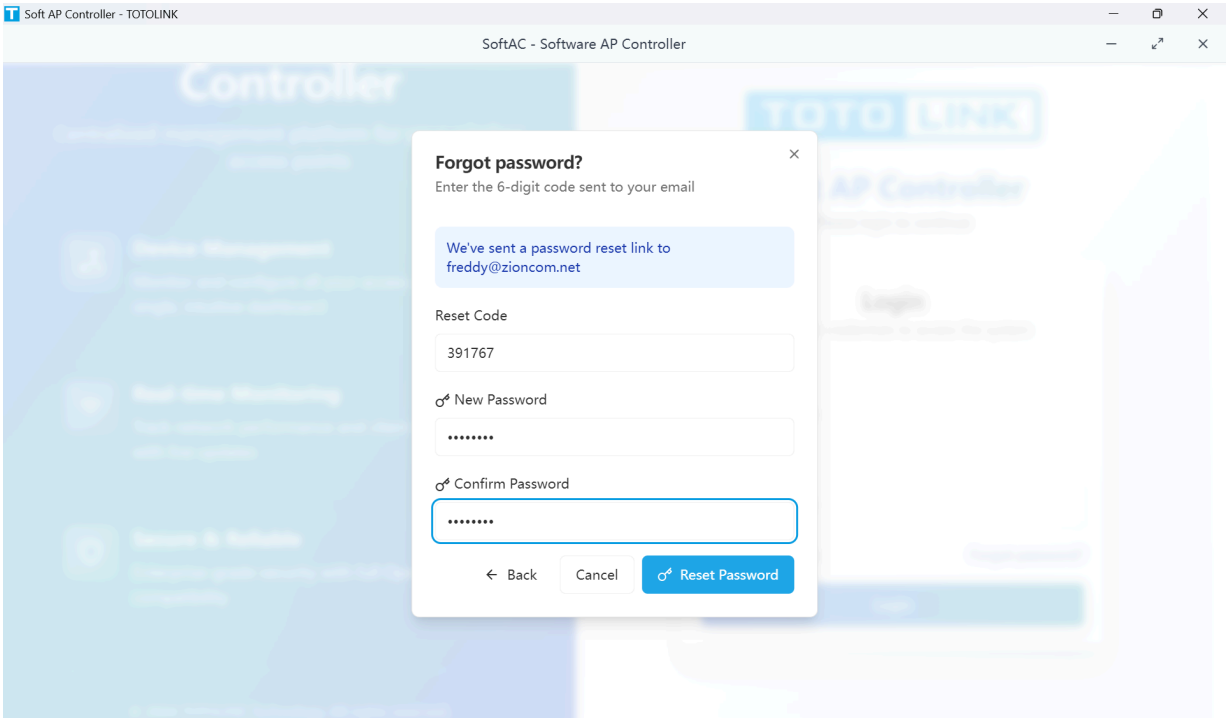


2. **Receive Reset Code**
    - Check your email (including spam folder)

- Find 6-digit reset code
- Code expires in 15 minutes



3. **Reset Password**
   - Enter reset code
   - Create new password
   - Confirm new password
   - Click "Reset Password"



4. **Login with New Password**
   - Return to login screen
   - Use username: `admin`

    - Enter new password

> ⚠️ **Important**: Password recovery requires a valid email address on file. Always keep your email updated and accessible.

Emergency Access Recovery

If you cannot access your account:

Scenario 1: Forgotten Password, No Email Access

- Contact TOTOLINK support with proof of ownership
- May require physical access to server
- Database password reset may be needed

Scenario 2: Account Locked

- Wait 15 minutes for automatic unlock
- Or restart SoftAC service to reset lockout

Scenario 3: Database Corruption

- Restore from recent backup
- Use emergency recovery procedure
- Contact technical support

12.2 Access Control

As the sole administrator, you have complete control over the SoftAC system.

Administrator Capabilities

Your admin account has unrestricted access to:

Device Management

- ✅ Add unlimited devices
- ✅ Modify all device configurations
- ✅ Delete devices
- ✅ Execute remote commands
- ✅ Apply firmware updates
- ✅ Manage device groups
- ✅ Control device discovery

Configuration Management

- ✅ Create and edit templates
- ✅ Apply configurations
- ✅ Backup configurations
- ✅ Restore previous settings
- ✅ Export/Import settings
- ✅ Manage configuration variables

System Administration

- ✅ Modify all system settings
- ✅ Configure network parameters
- ✅ Set up email notifications
- ✅ Manage SSL certificates
- ✅ Control system services
- ✅ Perform system updates

Monitoring & Alerts

- ✅ View all monitoring data
- ✅ Configure alert thresholds
- ✅ Set notification rules
- ✅ Access system logs
- ✅ Generate reports
- ✅ Export data

Security Functions

- ✅ Change security settings
- ✅ Manage SSH keys
- ✅ Configure firewall rules
- ✅ Set session timeouts
- ✅ Control API access
- ✅ Review audit logs

Protecting Admin Access

Since all control rests with one account:

Physical Security:

- Limit physical server access
- Use locked server rooms
- Control console access

- Secure backup media

Network Security:

- Use HTTPS only
- Implement firewall rules
- Restrict management IPs
- Use VPN for remote access

Operational Security:

- Never share credentials
- Log out when finished
- Lock workstation when away
- Use secure connections only

Administrative Best Practices

Practice	Recommendation	Reason
Strong Password	12+ characters with complexity	Only defense against unauthorized access
Regular Password Changes	Every 60-90 days	Limits exposure if compromised
Email Verification	Test monthly	Ensures password recovery works
Session Timeout	30 minutes or less	Prevents unauthorized access
Audit Review	Weekly checks	Detect any unusual activity
Backup Admin Access	Document recovery procedure	Emergency access plan

---

12.3 Login Security

Protecting the single administrator account is critical for system security.

Authentication Security Features

SoftAC implements multiple layers of login protection:

Password Policy Enforcement

Configure password requirements:

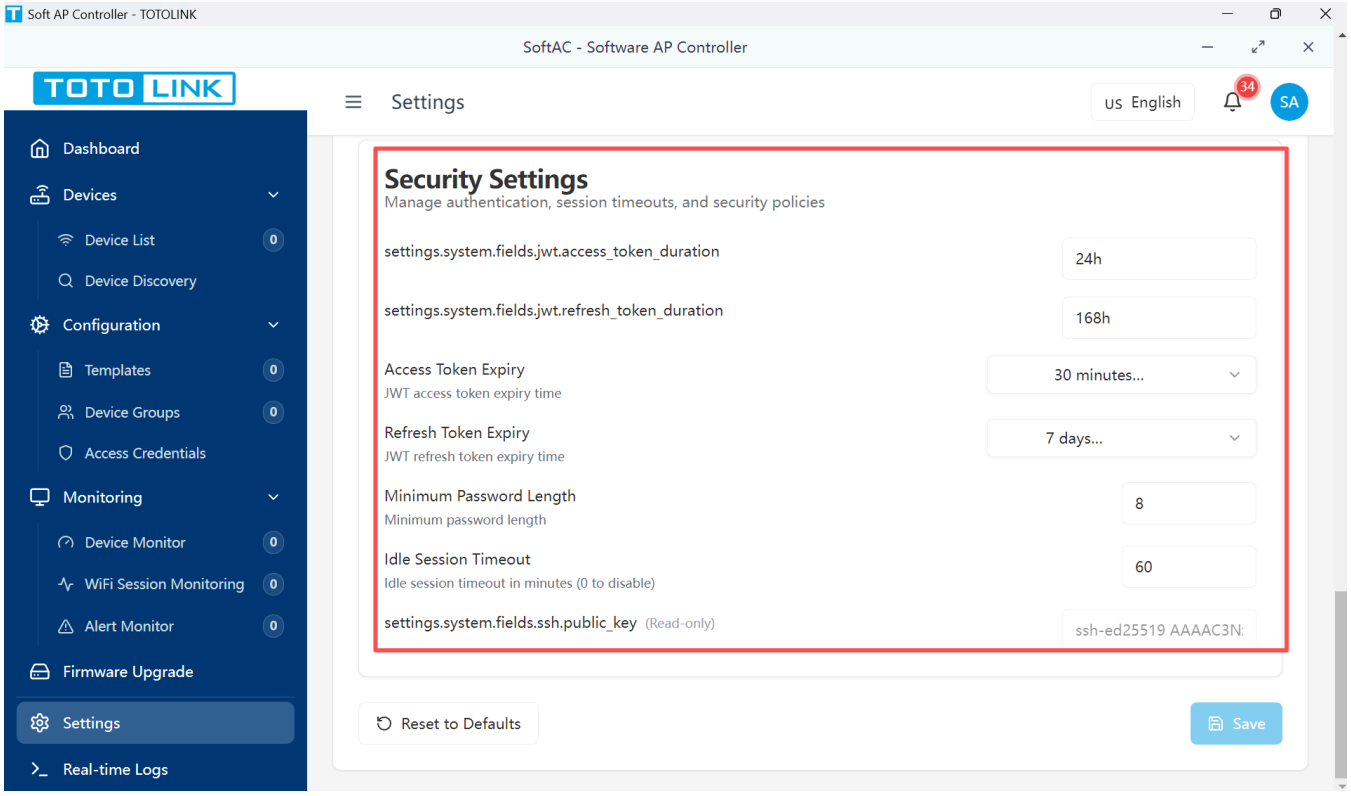
1. **Navigate to Security Settings**
   Settings → System Settings → Security
2. **Configure Password Rules**

- **Minimum Length**: 8-16 characters
- **Complexity**: Require mixed characters
- **History**: Prevent reuse of last 3 passwords
- **Expiration**: Optional expiration period

3. **Apply Settings**
   Click "Save" to enforce new rules

Session Management

Control how long you stay logged in:



Configurable Timeouts:

Setting	Purpose	Recommended
Access Token Expiry	Active session duration	15-60 minutes
Refresh Token Expiry	"Remember me" duration	1-7 days
Idle Timeout	Inactivity logout	15-30 minutes

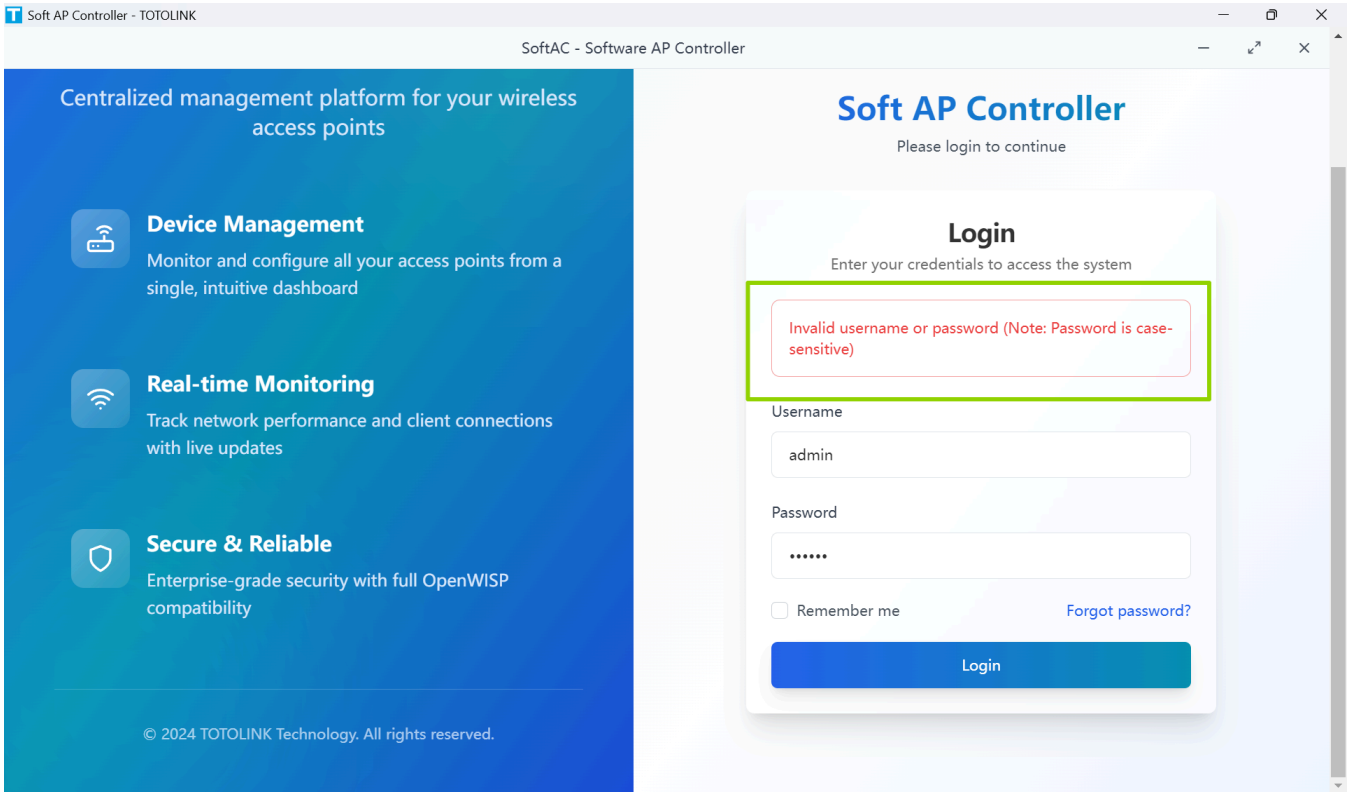
Setting Appropriate Timeouts:

1. **High Security Environment**
   - Access: 15 minutes
   - Idle: 15 minutes
   - Refresh: 1 day
   - Use for: Shared locations, compliance requirements

2. **Standard Security**
    - Access: 30 minutes
    - Idle: 30 minutes
    - Refresh: 7 days
    - Use for: Office environment
3. **Convenience Mode**
    - Access: 60 minutes
    - Idle: 60 minutes
    - Refresh: 30 days
    - Use for: Secure home office

Brute Force Protection

Automatic protection against password attacks:



Protection Mechanisms:

- Account locks after 5 failed attempts
- 15-minute lockout period
- Email alert on multiple failures
- IP-based rate limiting

After Account Lockout:

1. Wait 15 minutes for automatic unlock
2. Or restart SoftAC service
3. Check email for security alert

4. Review audit logs for attack source

Login Monitoring

Track all authentication attempts:

[Screenshot: Login history view]

What's Logged:

- Successful logins
- Failed attempts
- Password changes
- Session timeouts
- Password resets
- Account lockouts

Review Login Activity:

1. Navigate to Settings → Audit Logs
2. Filter by "Authentication" events
3. Check for:
    - Unusual login times
    - Multiple failed attempts
    - Logins from unknown IPs
    - Concurrent sessions

Security Recommendations

Password Best Practices:

- Use a passphrase: "MyNetwork&Secure@2024!"
- Avoid personal information
- Don't write it down
- Use a password manager
- Change if compromised

Session Security:

- Always log out when done
- Don't use "Remember Me" on shared computers
- Clear browser cache after use
- Use private/incognito mode when appropriate

Environmental Security:

- Use HTTPS only (never HTTP)
- Verify SSL certificate

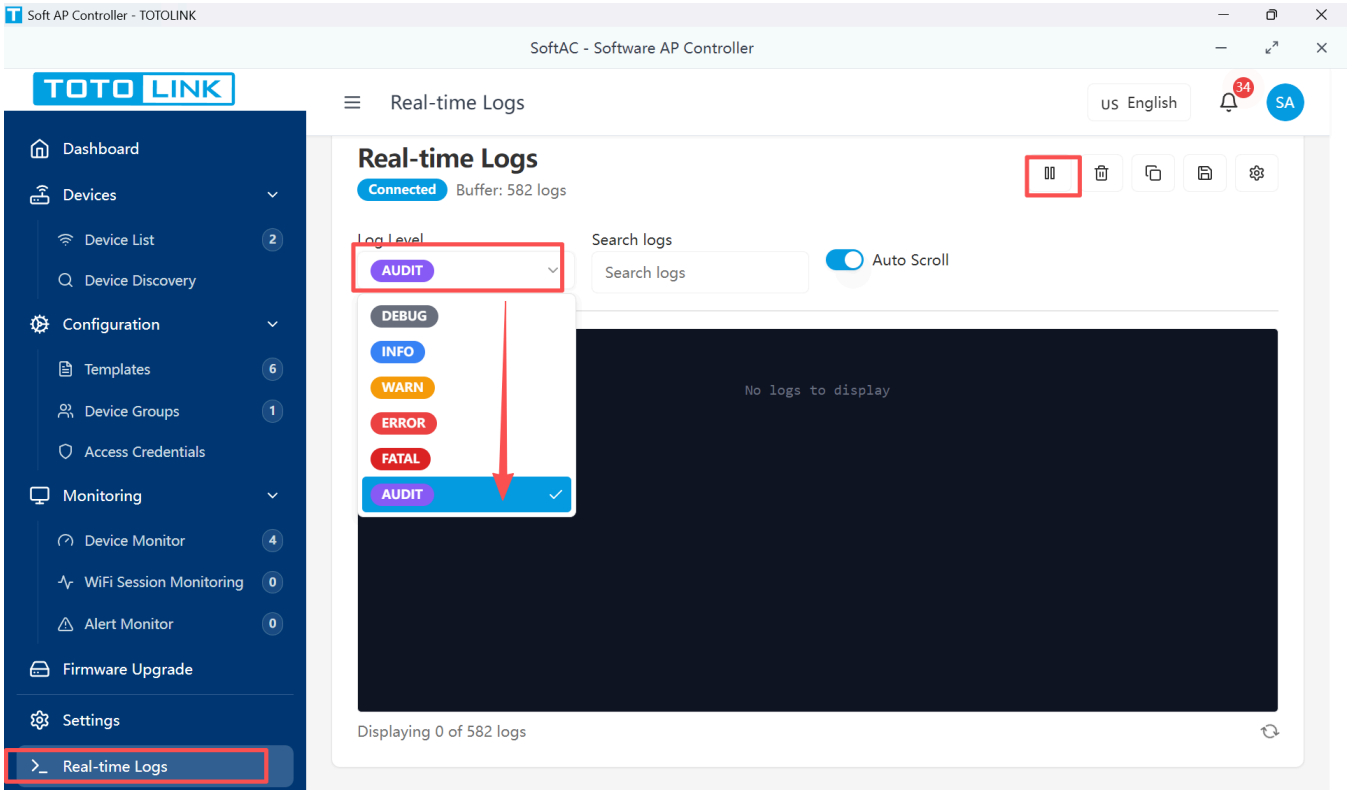
- Connect via VPN from remote locations
- Avoid public WiFi for admin access

12.4 Operation Audit

Comprehensive audit logging tracks all administrator activities for security, troubleshooting, and compliance.

Understanding Audit Logs

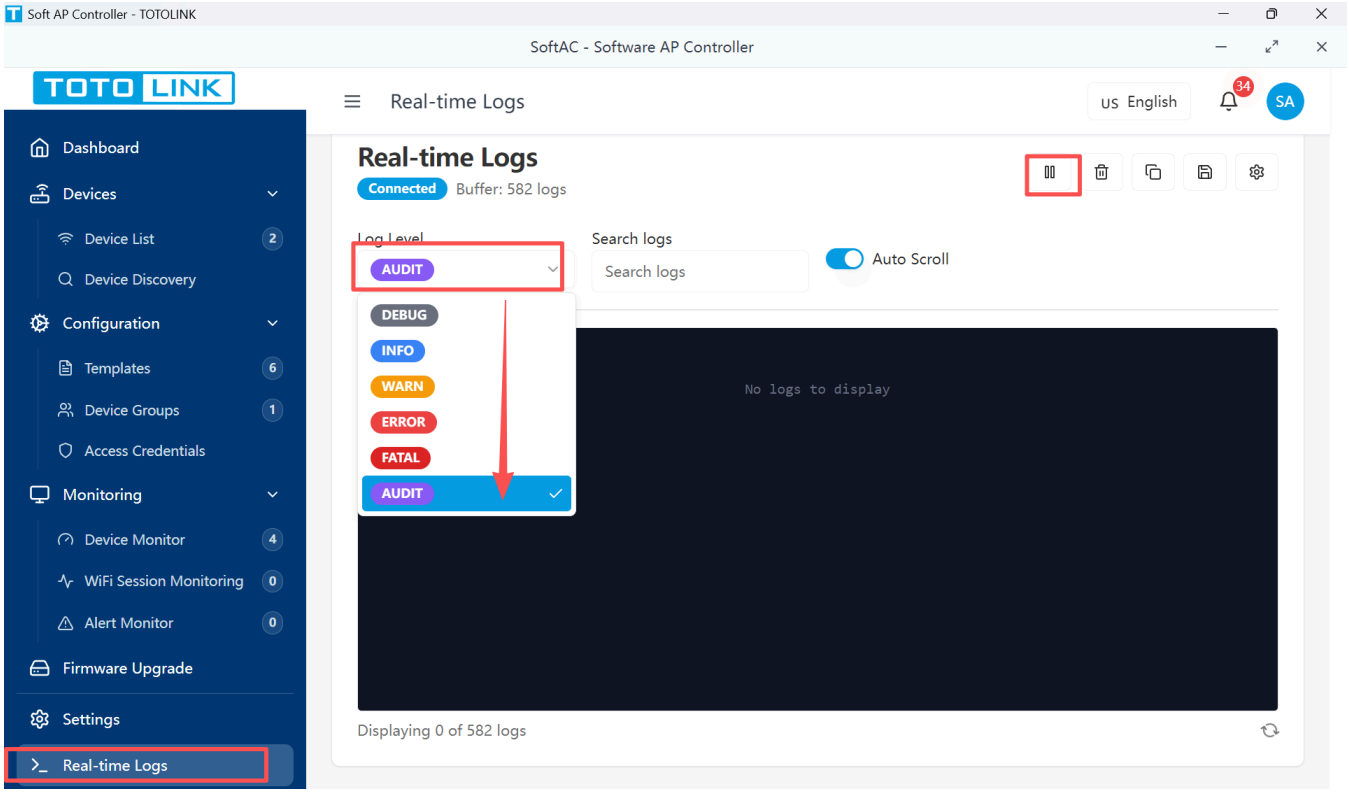
Every significant action is logged automatically:



Categories of Logged Events:

Category	Examples	Importance
Authentication	Login, logout, password changes	High - Security tracking
Configuration	Device settings, template changes	High - Change management
System Settings	Parameter updates, service changes	Medium - System stability
Device Operations	Add, delete, firmware updates	High - Network changes
Data Operations	Backup, restore, exports	Medium - Data handling
Security Events	Failed logins, permission denials	Critical - Threat detection

Accessing Audit Logs



Audit Log Details

Each log entry contains:

Field	Description	Example
Timestamp	Exact time of event	2024-03-15 14:23:45 UTC
Event Type	Category of action	Configuration Change
Action	Specific operation	Device Settings Updated
Target	Affected component	Device: AP-Floor2-01
Details	What changed	SSID: "Office" → "OfficeWiFi"
Result	Success or failure	Success
Duration	Operation time	245ms
IP Address	Source of action	192.168.1.100

Using Logs for Troubleshooting

Example scenarios:

Scenario 1: Device Configuration Issue

```
1. User reports device not working
2. Search audit logs for device name
3. Find recent configuration change
4. Review what was modified
5. Revert if necessary
```

Scenario 2: Security Investigation

```
1. Receive security alert
2. Filter logs by time period
3. Look for failed authentication
4. Check all actions after successful login
5. Assess if compromise occurred
```

[Screenshot: Troubleshooting with audit logs]

Audit Best Practices

1. **Regular Reviews**
   - Daily: Check for failures and errors
   - Weekly: Review all security events
   - Monthly: Analyze trends and patterns
2. **Set Up Alerts**
   - Email notification for failed logins
   - Alert on critical configuration changes
   - Notify on system errors
3. **Archive Important Logs**
   - Monthly exports for long-term storage
   - Secure offline backups
   - Encrypted storage for sensitive logs
4. **Document Significant Events**
   - Keep notes on major changes
   - Document incident responses
   - Track configuration decisions

Summary

SoftAC's single administrator model provides secure, simplified network management. Key points:

- **One Admin Account**: Complete control with maximum security
- **Mandatory Security Setup**: Cannot operate without securing admin account
- **Comprehensive Protection**: Multiple layers of login security
- **Full Audit Trail**: Every action is logged and searchable

- **Password Recovery**: Email-based recovery ensures account access

Security Checklist

- [ ] Initial setup completed with strong password
- [ ] Valid email address configured and tested
- [ ] Appropriate session timeouts configured
- [ ] Regular password changes scheduled
- [ ] Audit logs reviewed weekly
- [ ] Backup recovery procedure documented
- [ ] Emergency access plan in place

Next Steps

- Test password recovery process
- Configure session timeouts for your environment
- Set up audit log retention policies
- Document your emergency access procedures

Related Topics

- Chapter 11: System Settings - Configure security parameters
- Chapter 13: Log Management - System and device logs
- Chapter 2: Quick Start - Initial setup guide
- Chapter 14: Common Problems - Login troubleshooting

For additional support, contact TOTOLINK technical support or consult the online knowledge base.

Part 13: Log Management

Overview

TOTOLINK SoftAC's Log Management system provides comprehensive visibility into all system activities, device operations, and network events. This powerful diagnostic tool helps you monitor system health, troubleshoot issues, and maintain compliance records.

Think of the log system as your network's black box recorder - it captures everything that happens, allowing you to understand what occurred, when it happened, and why problems may have arisen.

Why Log Management Matters

Effective log management helps you:

- **Troubleshoot Issues**: Quickly identify and resolve network problems

- **Monitor Performance**: Track system and device performance over time
- **Ensure Security**: Detect unauthorized access attempts and security events
- **Maintain Compliance**: Keep required records for regulatory requirements
- **Analyze Trends**: Identify patterns and prevent future problems

---

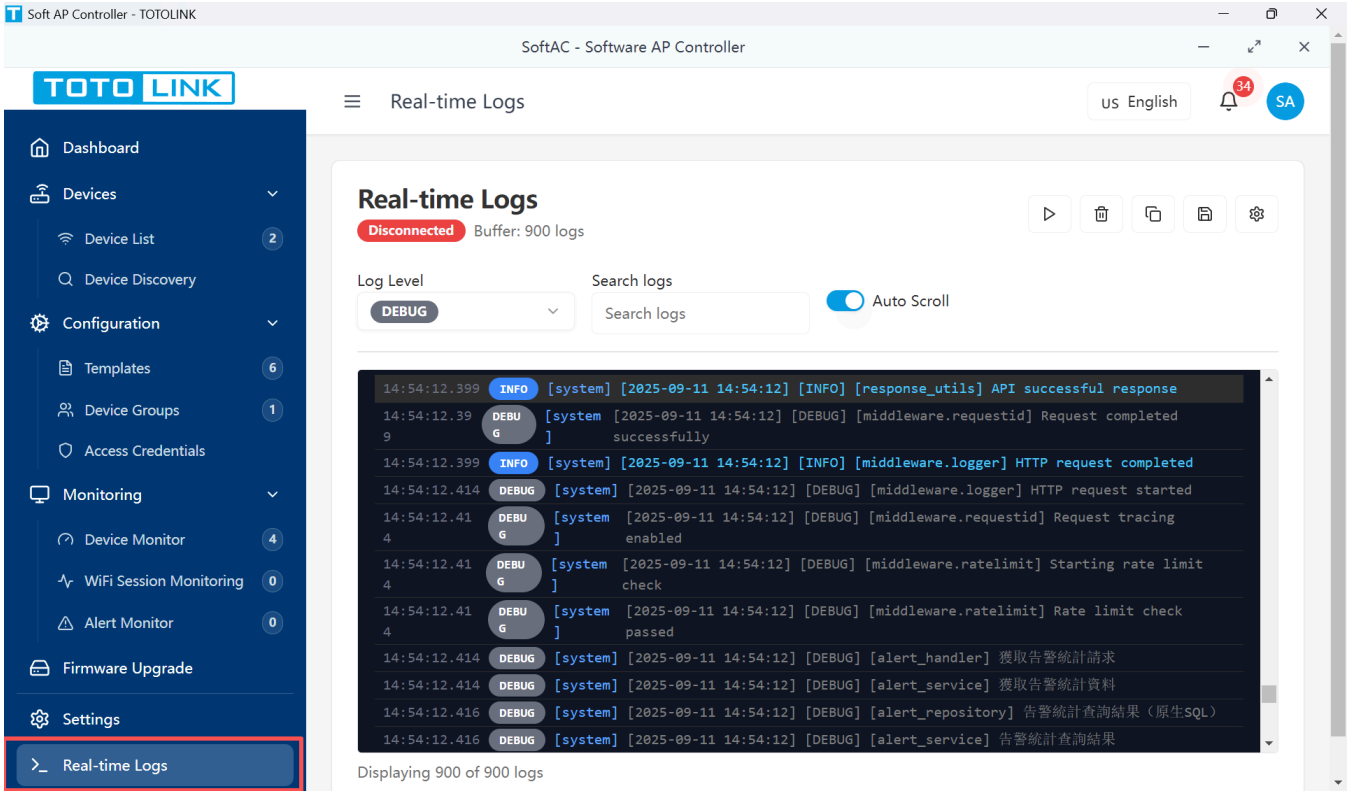
13.1 System Logs

System logs record all internal SoftAC operations, providing insight into the application's behavior and health.

Understanding System Logs

System logs capture:

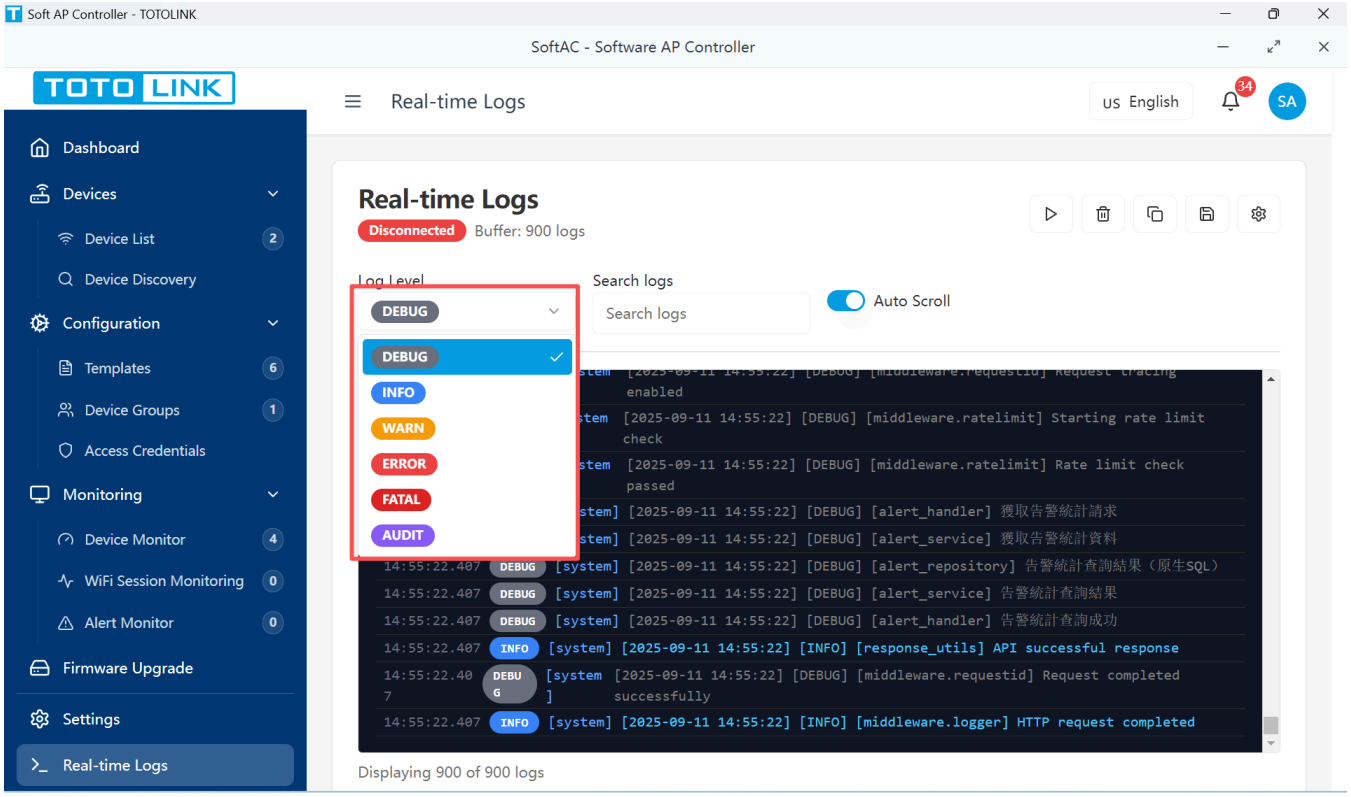
- Application startup and shutdown events
- Service status changes
- Configuration updates
- Database operations
- API requests and responses
- Background task execution



Log Levels Explained

SoftAC uses six log levels to categorize message importance:

Level	Color	Purpose	Examples
DEBUG	Gray	Detailed diagnostic information	Variable values, function calls
INFO	Blue	Normal operational messages	Service started, task completed
WARN	Yellow	Potential issues that don't stop operation	High memory usage, slow response
ERROR	Red	Problems that need attention	Connection failed, file not found
FATAL	Dark Red	Critical failures requiring immediate action	Database crash, out of memory
AUDIT	Purple	Security and compliance events	Login attempts, configuration changes



Accessing System Logs

Real-Time Log Viewer

1. **Navigate to Log Viewer**
   - Click Settings → Real-time Logs
2. **Understanding the Interface**

   [Screenshot: Log viewer interface with labeled components]

   Main Components:
   - **Log Stream**: Real-time display of log entries
   - **Filter Bar**: Level and module filtering

- **Search Box**: Text search across all logs
- **Control Buttons**: Start/pause streaming, clear, export
- **Status Indicator**: Connection status to log service

Filtering and Searching

Filter by Log Level

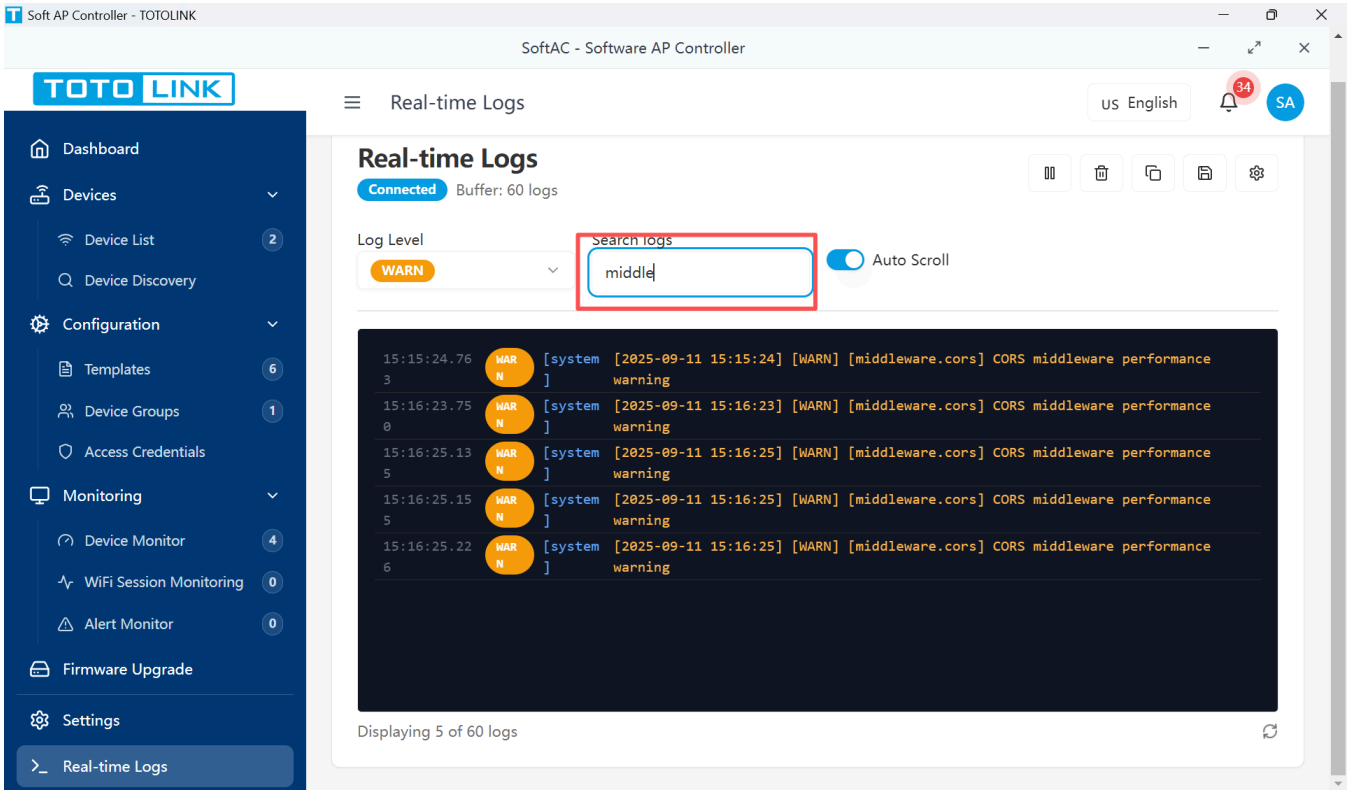
1. Click the level dropdown
2. Select minimum level to display
3. Higher levels include all lower levels

Example Filtering:

- Select "WARN" to see WARN, ERROR, and FATAL
- Select "DEBUG" to see all messages
- Select "ERROR" to see only errors and critical issues

Search Functionality

Use the search box for text-based filtering:



Search Examples:

```
"device offline" - Find device disconnection events
error AND config - Configuration errors
192.168.1.100 - Activities from specific IP
MAC:aa:bb:cc:dd:ee:ff - Device-specific logs
"failed to connect" - Connection failures
```

Real-Time Streaming

Watch logs as they're generated:

1. **Start Streaming**
   - Click "Play" button
   - New logs appear automatically
   - Auto-scroll follows latest entries
2. **Pause Streaming**
   - Click "Pause" button
   - Review specific entries
   - Resume when ready
3. **Auto-Scroll Toggle**
   - Enable: Always show newest logs
   - Disable: Stay at current position
   - Useful for detailed analysis

13.2 Operation Logs

Operation logs (audit logs) track all user actions and system changes for security and compliance.

What Gets Logged

Every significant action creates an audit entry:

[Screenshot: Operation log entries]

User Actions:

- Login and logout events
- Password changes
- Profile updates
- Configuration modifications
- Device management operations

System Operations:

- Scheduled task execution
- Automatic backups
- Data cleanup operations
- System updates

Security Events:

- Failed login attempts
- Session timeouts

- Permission denials
- Suspicious activities

Viewing Operation Logs

Access audit logs through multiple paths:

[Screenshot: Different ways to access audit logs]

1. **Via Settings Menu**
   Settings → Audit Logs
2. **Via Dashboard**
   Click "Recent Activities" widget
3. **Via User Menu**
   Click username → View Audit Logs

Operation Log Details

Each audit entry contains:

[Screenshot: Detailed audit log entry]

Field	Description	Example
Timestamp	Exact time of action	2024-03-15 14:23:45.123
User	Who performed action	admin
Operation	What was done	UPDATE_DEVICE_CONFIG
Target	What was affected	Device: Office-AP-01
Status	Success or failure	SUCCESS
Duration	Time taken	145ms
Details	Specific changes	Changed SSID from "Guest" to "Visitor"
Source IP	Where action originated	192.168.1.100

Security Monitoring

Use operation logs to detect security issues:

[Screenshot: Security event filtering]

Failed Login Monitoring

Watch for these patterns:

- Multiple failed attempts from same IP
- Failed attempts across many usernames
- Attempts at unusual hours

- Geographic anomalies

Setting Up Alerts:

1. Filter by "Authentication" category
2. Look for "FAILED" status
3. Check source IPs
4. Review timestamps for patterns

Configuration Change Tracking

Monitor critical changes:

[Screenshot: Configuration change logs]

- Who made changes
- What was changed
- When changes occurred
- Previous values (for rollback)

Compliance Reporting

Generate audit reports for compliance:

[Screenshot: Audit report generation]

1. **Select Report Type**
    - User activity summary
    - Configuration changes
    - Security events
    - Full audit trail
2. **Choose Time Period**
    - Last 24 hours
    - Last 7 days
    - Last 30 days
    - Custom range
3. **Export Format**
    - PDF for documentation
    - CSV for analysis
    - JSON for integration

13.3 Device Logs

Device logs capture events and status information from managed network devices.

Types of Device Logs

[Screenshot: Device log categories]

Status Logs:

- Device online/offline events
- Connection state changes
- Health status updates
- Resource utilization

Configuration Logs:

- Configuration applications
- Setting changes
- Template applications
- Rollback operations

Performance Logs:

- CPU usage statistics
- Memory utilization
- Network traffic data
- WiFi client connections

Firmware Logs:

- Upgrade attempts
- Version changes
- Success/failure status
- Rollback events

Accessing Device Logs

From Device List

1. Navigate to Devices page
2. Click on specific device
3. Select "Logs" tab

[Screenshot: Device logs tab]

From Log Viewer

1. Open Real-time Logs
2. Filter by device name or MAC
3. View all logs for that device

[Screenshot: Device-filtered logs]

Device Log Analysis

Connectivity Issues

Look for these patterns:

[Screenshot: Connectivity log patterns]

```
INFO: Device AA:BB:CC:DD:EE:FF came online
WARN: Device response time exceeded threshold (5000ms)
ERROR: Device AA:BB:CC:DD:EE:FF went offline
INFO: Attempting reconnection...
```

Troubleshooting Steps:

1. Check last online time
2. Review error messages before disconnect
3. Look for pattern in disconnections
4. Verify network path to device

Configuration Problems

Identify configuration issues:

[Screenshot: Configuration error logs]

```
INFO: Applying configuration to device
ERROR: Configuration validation failed: Invalid VLAN ID
WARN: Rolling back to previous configuration
INFO: Rollback completed successfully
```

Common Issues:

- Invalid parameter values
- Missing required fields
- Incompatible settings
- Template conflicts

Performance Monitoring

Track device performance:

[Screenshot: Performance metrics in logs]

```
INFO: Device CPU usage: 45%
WARN: Memory usage high: 85%
ERROR: CPU critical: 95% for 5 minutes
INFO: Alert triggered: High CPU usage
```

Performance Thresholds:

Metric	Normal	Warning	Critical
CPU	< 70%	70-85%	> 85%
Memory	< 75%	75-90%	> 90%
Disk	< 80%	80-90%	> 90%

Device Event Correlation

Correlate events across multiple devices:

[Screenshot: Multi-device event timeline]

Example: Network Outage Analysis

1. Filter logs by time range
2. Include all affected devices
3. Look for common patterns
4. Identify root cause

Pattern Recognition:

- Simultaneous disconnections → Network issue
- Sequential failures → Cascading problem
- Random disconnections → Individual device issues

13.4 Log Export

Export logs for external analysis, archival, or compliance requirements.

Export Options

[Screenshot: Log export dialog]

Export Formats

JSON Format:

- Machine-readable
- Preserves all fields
- Easy to import into analysis tools
- Ideal for automation

Text Format:

- Human-readable
- Formatted for reports
- Includes headers and summaries

- Good for documentation

CSV Format:

- Spreadsheet compatible
- Easy filtering and sorting
- Statistical analysis
- Trend identification

Exporting Logs

Quick Export

For immediate export of visible logs:

[Screenshot: Quick export button]

1. Apply desired filters
2. Click "Export" button
3. Choose format
4. Save file

Advanced Export

For comprehensive log extraction:

[Screenshot: Advanced export dialog]

1. **Click "Save Logs" Button**
2. **Configure Export Parameters:**

Parameter	Description	Options
Level	Minimum log level	DEBUG to FATAL
Modules	Specific components	Select multiple
Time Range	Period to export	Last hour to custom
Max Records	Limit entries	100 to 10,000
Format	Output format	JSON, Text, CSV
Filename	Output file name	Custom naming

3. **Set Filters:**
    - Log level threshold
    - Module selection
    - Date/time range
    - Search keywords
4. **Generate Export:**

- Click "Save & Download"
- Wait for processing
- File downloads automatically

Export File Structure

JSON Format Example

```
{
  "export_info": {
    "timestamp": "2024-03-15T10:30:00Z",
    "total_logs": 1523,
    "filters": {
      "level": "INFO",
      "modules": ["device_service"],
      "time_range": "24h"
    }
  },
  "logs": [
    {
      "id": "log_001",
      "timestamp": "2024-03-15T09:15:23.456Z",
      "level": "INFO",
      "module": "device_service",
      "message": "Device configuration updated",
      "fields": {
        "device_id": "dev_123",
        "changes": ["ssid", "password"]
      }
    }
  ]
}
```

Text Format Example

```
# SoftAC Log Export
# Export Time: 2024-03-15 10:30:00
# Total Logs: 1523
# Filters: Level=INFO, Module=device_service

[2024-03-15 09:15:23] INFO [device_service] Device configuration updated
  Device: dev_123
  Changes: ssid, password

[2024-03-15 09:16:45] WARN [device_service] Device response slow
  Device: dev_124
  Response Time: 5234ms
```

Log Archival

Best practices for log storage:

[Screenshot: Archive settings]

Archival Strategy

Log Type	Retention	Archive Format	Storage
System Logs	30 days	Compressed JSON	Local
Audit Logs	1 year	Encrypted JSON	Secure backup
Device Logs	90 days	Compressed CSV	Network storage
Security Events	2 years	Encrypted JSON	Offline backup

Automated Archival

Set up automatic log archival:

1. **Configure Schedule**
   - Daily: System logs
   - Weekly: Device logs
   - Monthly: Audit logs
2. **Set Destination**
   - Local directory
   - Network share
   - Cloud storage
3. **Enable Compression**
   - Reduces storage by 70-80%
   - Maintains searchability
   - Faster transfers

Log Analysis Tools

External tools for advanced analysis:

[Screenshot: Log analysis workflow]

Recommended Tools:

Tool	Purpose	Best For
Excel/Calc	Basic analysis	Small datasets, quick charts
Splunk	Enterprise analysis	Large-scale correlation

Tool	Purpose	Best For
ELK Stack	Open-source analytics	Custom dashboards
Python/R	Statistical analysis	Trend analysis, ML

Integration Steps:

1. Export logs in appropriate format
2. Import into analysis tool
3. Configure parsing rules
4. Create visualizations
5. Set up alerts

Export Best Practices

1. **Regular Exports**
   - Daily: Critical logs
   - Weekly: System logs
   - Monthly: Full archive
2. **Naming Convention**

   ```
   softac_[type]_[date]_[time].[format]
   Example: softac_audit_20240315_1030.json
   ```

3. **Storage Organization**

   ```
   /logs/
     /2024/
       /03/
         /system/
         /audit/
         /device/
   ```

4. **Security**
   - Encrypt sensitive logs
   - Restrict access
   - Audit log exports
   - Secure transmission
5. **Validation**
   - Verify export completeness
   - Check file integrity
   - Test restoration
   - Document procedures

Summary

Effective log management is essential for network operations and security. Key points:

- **System Logs**: Monitor application health and performance
- **Operation Logs**: Track all user actions for security and compliance
- **Device Logs**: Understand device behavior and issues
- **Log Export**: Archive and analyze logs for long-term insights

Best Practices Checklist

- [ ] Review logs daily for errors and warnings
- [ ] Set up filters for common troubleshooting scenarios
- [ ] Export audit logs monthly for compliance
- [ ] Archive logs according to retention policy
- [ ] Test log restoration procedures quarterly
- [ ] Document common log patterns and solutions
- [ ] Train team on log analysis techniques

Next Steps

- Configure log retention settings
- Set up automated exports
- Create custom filters for your environment
- Document troubleshooting procedures

Related Topics

- Chapter 12: User Management - Audit log configuration
- Chapter 7.3: Alert Management - Alert generation from logs
- Chapter 11: System Settings - Log retention policies
- Chapter 14: Common Problems - Using logs for troubleshooting

---

For additional support, contact TOTOLINK technical support or consult the online knowledge base.

Part 14. Common Problems

This chapter helps you solve common issues you might encounter while using TOTOLINK SoftAC. Each section provides simple, step-by-step solutions that anyone can follow.

14.1 Connection Problems

This section helps you fix problems when devices won't connect or stay connected to your network management system.

Device Shows "Offline" Status

When you add a new device but it won't come online:

What You'll See

- Red "Offline" indicator next to the device name
- No information available about the device
- Unable to manage or configure the device

[Screenshot: Device list showing a device with red "Offline" status]

How to Fix It

1. **Check if the Device is Powered On**
    - Look at the device's power LED (should be solid green)
    - Make sure the power cable is properly connected
    - Try unplugging and reconnecting the power cable
2. **Verify Network Cable Connection**
    - Check that the network cable is firmly plugged in
    - Look for a link LED near the network port (should be on or blinking)
    - Try using a different network cable if available
3. **Restart the Device**
    - Unplug the device power cable
    - Wait 30 seconds
    - Plug it back in
    - Wait 2-3 minutes for the device to fully start
4. **Check Device Information**

    [Screenshot: Edit device button in the device list]

    - Click on the device name in your list
    - Click the "Edit" button
    - Verify the device information is correct
    - Make sure the device password matches what's set on the actual device

> 💡 **Helpful Tip**: Most connection problems are solved by simply restarting the device. Always try this first!

Still Not Working?

Try these additional steps:

Step	What to Do	Why It Helps
1	Click "Rediscover Devices"	Searches for the device again
2	Delete and re-add the device	Clears any incorrect settings
3	Check with your network administrator	There may be network restrictions

---

Can't Access Device Settings

When clicking on a device doesn't open its settings:

What You'll See

- Clicking the device name does nothing
- "Loading" message that never completes
- Error message appears briefly

How to Fix It

1. **Refresh Your Browser**
    - Press F5 on your keyboard
    - Or click the refresh button in your browser
    - Wait for the page to fully reload
2. **Log Out and Back In**
    - Click your username in the top right corner
    - Select "Logout"
    - Log back in with your credentials
    - Try accessing the device again
3. **Clear Browser Data**
    - Press Ctrl+Shift+Delete (Windows) or Cmd+Shift+Delete (Mac)
    - Select "Last hour" for time range
    - Check "Cookies" and "Cached images"
    - Click "Clear data"

> 📝 **Note**: After clearing browser data, you'll need to log in again.

Dashboard Not Updating

When the main dashboard shows old information:

What You'll See

- Statistics don't change
- "Last updated" time is old
- Numbers seem frozen

Quick Fix Steps

1. **Check Your Internet Connection**
    - Make sure you're connected to the internet
    - Try opening a different website
    - If other sites work, continue to step 2
2. **Refresh the Dashboard**
    - Click the refresh icon on the dashboard
    - Or press F5 to reload the entire page
    - Wait 10-15 seconds for new data
3. **Check System Status**
    - Look at the top of the page for any warning messages
    - Yellow or red indicators mean the system is having issues
    - Green means everything is working normally

14.2 Configuration Problems

This section helps when device settings won't save or apply correctly.

Changes Not Saving

When you modify settings but they don't take effect:

What You'll See

- Settings revert to old values
- "Saving..." message never completes
- Device continues using old configuration

How to Fix It

1. **Save Changes Properly**
    - After making changes, always click "Save"
    - Wait for "Successfully saved" message
    - Don't navigate away until saving completes

2. **Apply Configuration to Device**
    - After saving, click "Apply Configuration"
    - You'll see a progress indicator
    - Wait for "Configuration applied successfully"
3. **Restart the Device**
   Some changes require a device restart:
    - Go to the device page
    - Click "Actions" → "Restart Device"
    - Wait 2-3 minutes for restart to complete

> ⚠️ **Important**: Restarting a device will briefly disconnect all connected users. Do this during low-usage times.

WiFi Network Not Appearing

When you create a WiFi network but devices can't see it:

What You'll See

- WiFi network name doesn't show up on phones/laptops
- Devices can't connect to your WiFi
- WiFi seems to be disabled

Step-by-Step Solution

1. **Check WiFi Settings**
    - Go to device settings
    - Click on "Wireless Settings"
    - Make sure "Enable WiFi" is checked
    - Verify the network name doesn't have special characters
2. **Verify Basic Settings**
   Check these essential settings:

Setting	Should Be	Common Mistake
WiFi Status	Enabled	Accidentally disabled
Network Name	Simple text	Using symbols like @#$
Hide Network	Unchecked	Network hidden from view
WiFi Password	8+ characters	Password too short

3. **Choose the Right WiFi Type**
    - **2.4GHz**: Better range, works with all devices

- **5GHz**: Faster speed, shorter range
- **Both**: Recommended for most users

4. **Save and Apply**
   - Click "Save Settings"
   - Click "Apply to Device"
   - Wait 1-2 minutes for WiFi to restart

> 💡 **Tip**: If you're unsure about settings, use the "Default Settings" button to restore recommended values.

Group Settings Not Working

When devices in a group don't receive group settings:

What You'll See

- Devices in group have different settings
- Group changes don't affect devices
- Some devices update, others don't

How to Solve

1. **Check Group Membership**
   - Go to "Device Groups"
   - Click on your group
   - Verify all intended devices are listed
   - Add missing devices if needed
2. **Apply Group Settings**
   - After changing group settings, click "Save"
   - Then click "Apply to All Devices"
   - A progress bar shows update status
   - Check the results summary
3. **Handle Individual Failures**
   If some devices fail to update:
   - Note which devices failed
   - Go to each device individually
   - Click "Sync with Group"
   - Or manually apply settings

14.3 Performance Problems

This section helps when the system runs slowly or becomes unresponsive.

Pages Loading Slowly

When it takes a long time to open pages or see information:

What You'll See

- Spinning loading circles
- Pages partially load then stop
- Clicking buttons has delayed response

Speed Things Up

1. **Close Unnecessary Browser Tabs**
    - Too many open tabs slow everything down
    - Keep only 2-3 SoftAC tabs open
    - Close other websites while working
2. **Use a Modern Browser**

    Recommended browsers:
    - Google Chrome (version 90 or newer)
    - Mozilla Firefox (version 88 or newer)
    - Microsoft Edge (version 90 or newer)
    - Safari (version 14 or newer)
3. **Reduce Display Options**
    - Click "Settings" → "Display Options"
    - Change "Devices per page" from 100 to 25
    - Disable "Auto-refresh" if not needed
    - Hide unused information columns

> 💡 **Quick Fix**: Log out, clear your browser cache, and log back in. This solves most speed issues!

System Becomes Unresponsive

When clicking buttons doesn't work or everything freezes:

What You'll See

- Clicking does nothing
- Page appears frozen
- "Not responding" message in browser

Recovery Steps

1. **Wait a Moment**
    - Sometimes the system is processing
    - Wait 30 seconds before taking action
    - Look for any progress indicators
2. **Refresh the Page**
    - Press F5 or click browser refresh
    - If that doesn't work, close the tab
    - Open a new tab and log in again
3. **Check System Notifications**
    - Click the bell icon (top right)
    - Look for system maintenance notices
    - Check for error messages
4. **Restart Your Browser**
    - Save any important work first
    - Close all browser windows
    - Open browser again and log in

Reports Taking Too Long

When generating reports or exports is very slow:

What You'll See

- "Generating report..." message stays for minutes
- Download never starts
- Browser may show timeout error

Solutions

1. **Reduce Report Scope**
    - Select shorter time period (week instead of month)
    - Choose fewer devices to include
    - Export only essential data fields
2. **Generate Reports During Off-Hours**
    - System is faster when fewer users are online
    - Try early morning or late evening
    - Schedule automatic reports if available
3. **Export in Smaller Chunks**
   Instead of one large export:

- Export by device group
- Export by date range
- Combine smaller exports later

14.4 Upgrade Problems

This section helps with issues when updating device software (firmware).

Can't Upload Firmware File

When trying to add new firmware for devices:

What You'll See

- "Invalid file" error message
- Upload fails immediately
- Progress bar doesn't move

How to Fix

1. **Check File Type**
   - Firmware files usually end in `.bin`
   - Make sure you have the correct file
   - Download from official TOTOLINK website only
2. **Verify File Size**
   - Files over 100MB may fail
   - Check if you have enough storage space
   - Delete old unused firmware files if needed
3. **Rename the File**
   - Remove special characters from filename
   - Use only letters and numbers
   - Keep the `.bin` extension

> 🔒 **Security Warning**: Only use firmware files from TOTOLINK official sources. Other files may damage your devices.

Device Upgrade Gets Stuck

When updating a device's firmware doesn't complete:

What You'll See

- Progress stays at same percentage
- "Upgrading..." message for over 30 minutes
- Device becomes unreachable

What to Do

1. **Be Patient**
    - Normal upgrades take 5-15 minutes
    - Large updates may take up to 30 minutes
    - Don't interrupt the process
2. **Check Device Status**

    Look at the physical device:
    - Power LED should be on
    - Status LED may blink during upgrade
    - Don't unplug the device!
3. **Wait for Automatic Recovery**
    - System will timeout after 30 minutes
    - Device should restart automatically
    - Status will update when device recovers
4. **If Still Stuck After 1 Hour**
    - Click "Cancel Upgrade"
    - Wait 5 minutes
    - Try upgrade again
    - Contact support if problem persists

> ⚠️ **Critical**: Never unplug a device during firmware upgrade! This can permanently damage the device.

Multiple Devices Upgrade Failing

When upgrading several devices at once:

What You'll See

- Some devices succeed, others fail
- Error messages for multiple devices
- Upgrade queue stops progressing

Best Practices

1. **Upgrade in Small Groups**
    - Select 5-10 devices at a time
    - Wait for each group to complete
    - Easier to track and fix problems
2. **Check Why Devices Failed**
    - Click "View Details" for failed devices
    - Common reasons:
        - Device offline
        - Wrong firmware version
        - Not enough device memory
3. **Retry Failed Devices**
    - Select only the failed devices
    - Click "Retry Upgrade"
    - Consider upgrading one at a time

Upgrade Checklist

Before starting upgrades:

Check	Ready?
All devices online	✓
Firmware file correct	✓
Backup settings saved	✓
Users notified of downtime	✓
Time allocated (5 min per device)	✓

Getting Help

If these solutions don't resolve your problem:

What Information to Gather

Before contacting support, note down:

1. **What you were trying to do**
    - Which menu or page you were on
    - What button you clicked
    - What you expected to happen

2. **What actually happened**
    - Any error messages (take a screenshot)
    - When the problem started
    - If it happens every time
3. **Your system information**
    - Found in "Help" → "About"
    - Your username
    - Device models having issues

How to Contact Support

1. **Check the Help Section**
    - Click "Help" in the menu
    - Search for your problem
    - Read suggested solutions
2. **Contact Your Administrator**
    - They may know about system maintenance
    - Can check your account permissions
    - May have seen the issue before
3. **TOTOLINK Support**
    - Email: support@totolink.net
    - Include screenshots and system information
    - Describe steps to reproduce the problem

> 💡 **Tip**: Taking screenshots of error messages helps support understand and solve your problem faster.

Quick Reference Card

Common Messages and What They Mean

You See	It Means	Do This
"Connection lost"	Lost contact with system	Refresh page (F5)
"Session expired"	Been logged in too long	Log in again
"Permission denied"	Not allowed to do this	Contact administrator
"Device busy"	Device doing something else	Wait 2 minutes and retry
"Invalid input"	Information entered incorrectly	Check for typos or special characters
"Timeout"	Taking too long	Try again with fewer devices/data

You See	It Means	Do This
"Offline"	Device not connected	Check device power and cables
"Pending"	Waiting to process	Wait or click "Apply" again
"Failed"	Didn't work	Check details and retry

Keyboard Shortcuts

- **F5**: Refresh page
- **Ctrl+F5**: Hard refresh (clears cache)
- **Ctrl+S**: Save settings
- **Esc**: Cancel/close dialog

Remember: Most problems are temporary and easily fixed. When in doubt, refresh the page or restart the device!

Part 15. Glossary

This glossary provides definitions for technical terms used throughout the TOTOLINK SoftAC system. Terms are arranged alphabetically for easy reference.

A

Access Point (AP)

A wireless networking device that allows Wi-Fi devices to connect to a wired network. TOTOLINK SoftAC manages multiple access points from a centralized location.

Alert

An automated notification triggered when specific conditions are met, such as device offline status or high memory usage. Alerts help administrators respond quickly to network issues.

API Key

A unique identifier used to authenticate and authorize access to the SoftAC system through its programming interface. Keep API keys secure and confidential.

Auto Discovery

The system's ability to automatically detect and identify TOTOLINK devices on the network without manual configuration.

B

Backup

A copy of system configuration and settings that can be restored if needed. Regular backups protect against data loss and allow quick recovery.

Bandwidth

The maximum rate of data transfer across a network connection, typically measured in Mbps (Megabits per second) or Gbps (Gigabits per second).

Batch Operation

The ability to perform the same action on multiple devices simultaneously, saving time when managing large networks.

C

Channel

A specific frequency range used for wireless communication. Wi-Fi networks use different channels to avoid interference between nearby networks.

Channel Width

The frequency bandwidth used by a Wi-Fi channel. Common widths are 20 MHz, 40 MHz, and 80 MHz. Wider channels provide higher speeds but may experience more interference.

Configuration Template

A pre-defined set of device settings that can be applied to multiple devices at once. Templates ensure consistent configuration across similar devices.

CPU Usage

The percentage of processing power being used by a device. High CPU usage may indicate performance issues or excessive load.

Credential

Authentication information such as usernames, passwords, or SSH keys used to access and manage devices securely.

D

Dashboard

The main overview screen that displays key system metrics, device status, and important notifications at a glance.

Device

A network hardware unit (such as an access point or router) managed by the SoftAC system.

Device Group

A collection of devices that can be managed together. Groups allow administrators to apply configurations and policies to multiple devices simultaneously.

DHCP (Dynamic Host Configuration Protocol)

A network protocol that automatically assigns IP addresses to devices on a network.

E

Encryption

The process of encoding data to prevent unauthorized access. Common Wi-Fi encryption standards include WPA2 and WPA3.

F

Firmware

The low-level software that controls a device's hardware. Firmware updates can add features, fix bugs, and improve security.

Frequency Band

The radio frequency range used for wireless communication. Common Wi-Fi bands are 2.4 GHz and 5 GHz.

G

Gateway

A network device that connects different networks and routes traffic between them. Often refers to the main router connecting a local network to the internet.

Guest Network

A separate wireless network for visitors that isolates guest traffic from the main network for security purposes.

H

Health Check

An automated test that verifies a device is functioning correctly and can communicate with the SoftAC controller.

Hostname

A human-readable name assigned to a device on the network, making it easier to identify than using IP addresses.

I

IP Address

A unique numerical identifier assigned to each device on a network. IPv4 addresses look like 192.168.1.1, while IPv6 addresses are longer and use hexadecimal notation.

L

LAN (Local Area Network)

A network that connects devices within a limited area, such as an office building or home.

Log

A record of system events, user actions, or device activities used for monitoring, troubleshooting, and security auditing.

M

MAC Address

A unique hardware identifier assigned to every network device. MAC addresses consist of six pairs of hexadecimal characters (e.g., 00:11:22:33:44:55).

Memory Usage

The amount of RAM (Random Access Memory) being used by a device. High memory usage can affect device performance.

Monitoring

The continuous observation of network devices and traffic to ensure optimal performance and identify issues.

N

Network Interface

A hardware or software component that connects a device to a network. Devices may have multiple interfaces (e.g., wired Ethernet and wireless Wi-Fi).

Network Topology

The arrangement and connection pattern of devices in a network.

O

Offline Status

Indicates that a device cannot communicate with the SoftAC controller, possibly due to network issues or device failure.

Online Status

Indicates that a device is connected and communicating normally with the SoftAC controller.

P

Port

A numerical identifier for specific services or applications. For example, web traffic typically uses port 80 (HTTP) or 443 (HTTPS).

Power Level

The transmission strength of a wireless signal. Higher power levels provide greater range but may cause interference.

R

Reboot

The process of restarting a device to apply changes or resolve issues.

Rollback

The ability to return to a previous firmware version or configuration if problems occur after an update.

S

SSID (Service Set Identifier)

The name of a wireless network that appears when scanning for available Wi-Fi connections.

SSH (Secure Shell)

A secure protocol for remotely accessing and managing network devices through a command-line interface.

SSL/TLS

Security protocols that encrypt data transmitted between devices and the SoftAC controller.

Status

The current operational state of a device or service (e.g., online, offline, warning, critical).

Subnet

A logical subdivision of an IP network, used to organize and secure network traffic.

T

Template

See Configuration Template.

Throughput

The actual amount of data successfully transferred over a network connection, usually less than the theoretical bandwidth.

Timezone

The geographical time zone setting for devices, important for accurate logging and scheduled operations.

Transmit Power

The strength of the radio signal transmitted by a wireless device, measured in dBm or milliwatts.

U

Uptime

The amount of time a device has been running continuously since its last restart.

UUID (Universally Unique Identifier)

A unique string of characters used to identify devices, templates, and groups within the SoftAC system.

V

VLAN (Virtual Local Area Network)

A logical network segment that groups devices together regardless of their physical location.

W

WAN (Wide Area Network)

A network that covers a broad geographical area, typically referring to the internet connection.

Wi-Fi Session

An active connection between a wireless client device (like a smartphone or laptop) and an access point.

Wireless Client

Any device that connects to a wireless network, such as smartphones, tablets, laptops, or IoT devices.

Wireless Standard

The technical specification for Wi-Fi communication. Common standards include 802.11n (Wi-Fi 4), 802.11ac (Wi-Fi 5), and 802.11ax (Wi-Fi 6).

WPA2/WPA3

Wi-Fi Protected Access security protocols that encrypt wireless communications. WPA3 is the newest and most secure standard.

> 📝 **Note**: This glossary covers the most common terms you'll encounter while using TOTOLINK SoftAC. For additional technical information or clarification, please refer to the relevant sections of this manual or contact technical support.

Part 16. Technical Support

TOTOLINK is committed to providing comprehensive support for all SoftAC users. This section provides information on how to get help, available support resources, and best practices for resolving issues quickly.

Getting Help

Before Contacting Support

To help us assist you more efficiently, please gather the following information before contacting support:

1. **System Information**
   - SoftAC version number
   - Operating system and version
   - Browser type and version (for web interface issues)
2. **Device Information**
   - Device model and firmware version
   - Number of devices affected
   - Device MAC addresses (if specific devices are affected)
3. **Issue Details**
   - Clear description of the problem
   - When the issue first occurred
   - Steps to reproduce the issue
   - Any error messages (exact wording or screenshots)
   - What troubleshooting steps you've already tried
4. **Log Files**
   - System logs from the time of the issue
   - Device logs if applicable

> 💡 **Tip**: You can export logs from the Log Management section (see Chapter 13).

Support Channels

1. Online Support Portal

Access our comprehensive online support resources:

Website: www.totolink.tw/support

Available resources include:

- Knowledge base articles

- Video tutorials
- FAQ section
- Software downloads
- Firmware updates
- User manual downloads

2. Email Support

For non-urgent technical issues and general inquiries:

Email: support@totolink.tw

Response Time:

- Business days: Within 24-48 hours
- Include your serial number and system information for faster service

3. Phone Support

For urgent issues requiring immediate assistance:

Taiwan Office

- Phone: +886-2-2659-1868
- Hours: Monday-Friday, 9:00 AM - 6:00 PM (GMT+8)
- Language: Mandarin, English

International Support

- Please visit our website for regional contact numbers
- Available in multiple languages based on region

4. Remote Assistance

For complex issues, our support team may request remote access to your system:

1. Support representative will provide a session ID
2. Download the remote assistance tool from our secure portal
3. Enter the session ID to establish connection
4. Support team can view and assist with configuration

> 🔒 **Security Note**: Only provide remote access to verified TOTOLINK support representatives. We will never ask for your passwords.

Self-Service Resources

Knowledge Base

Our online knowledge base contains hundreds of articles covering:

- Installation guides
- Configuration tutorials
- Troubleshooting guides
- Best practices
- Video demonstrations

Access: www.totolink.tw/kb

Community Forum

Connect with other SoftAC users and TOTOLINK experts:

- Share experiences and solutions
- Ask questions
- Get tips and best practices
- Participate in discussions

Access: community.totolink.tw

Video Tutorials

Step-by-step video guides for common tasks:

- Initial setup and configuration
- Adding and configuring devices
- Creating templates and groups
- Firmware updates
- Troubleshooting common issues

Access: Available on the support portal and YouTube channel

Warranty and Service

Standard Warranty

TOTOLINK SoftAC includes:

- **Software**: 1-year warranty from purchase date
- **Updates**: Security and bug fixes during warranty period
- **Support**: Email support during warranty period

Extended Support Plans

Enhanced support options available:

Professional Support

- Priority email and phone support
- Extended warranty coverage
- Advanced replacement options
- Dedicated support representative

Enterprise Support

- 24/7 phone support
- Guaranteed response times
- On-site assistance (select regions)
- Custom training sessions

Contact sales for pricing and availability: sales@totolink.tw

---

Reporting Issues

Bug Reports

If you discover a software bug:

1. Document the issue with detailed steps to reproduce
2. Include screenshots or screen recordings if possible
3. Note the exact error messages
4. Send report to: bugs@totolink.tw

Security Vulnerabilities

For security-related issues:

1. **Do not** post details publicly
2. Email security team directly: security@totolink.tw
3. Include detailed technical information
4. Allow 48 hours for initial response

We take security seriously and appreciate responsible disclosure.

Training and Certification

Online Training

Self-paced online courses available:

- SoftAC Basic Administration
- Advanced Configuration
- Network Optimization
- Troubleshooting Techniques

Webinars

Live online training sessions:

- Monthly feature highlights
- Best practices workshops
- Q&A sessions with experts

Register at: www.totolink.tw/training

Certification Program

Become a certified SoftAC administrator:

- Comprehensive curriculum
- Hands-on labs
- Industry-recognized certification
- Career advancement opportunities

Feedback and Suggestions

We value your input to improve SoftAC:

Product Feedback

- Email: feedback@totolink.tw
- Include specific feature requests or improvement suggestions
- Describe your use case and how the suggestion would help

Documentation Feedback

- Email: docs@totolink.tw
- Report errors or unclear sections
- Suggest additional topics to cover

Quick Reference

Important Links

Resource	URL
Support Portal	www.totolink.tw/support
Knowledge Base	www.totolink.tw/kb
Downloads	www.totolink.tw/downloads
Community Forum	community.totolink.tw
Training	www.totolink.tw/training

Contact Summary

Type	Contact	Hours
General Support	support@totolink.tw	24-48 hour response
Phone Support	+886-2-2659-1868	Mon-Fri, 9AM-6PM GMT+8
Bug Reports	bugs@totolink.tw	-
Security	security@totolink.tw	48 hour response
Sales	sales@totolink.tw	-

Emergency Support Checklist

When experiencing critical issues:

1. ✓ Check system status and error logs
2. ✓ Verify network connectivity
3. ✓ Review recent configuration changes
4. ✓ Check the knowledge base for known issues
5. ✓ Gather system information and logs
6. ✓ Contact phone support with details ready

Regional Offices

Asia Pacific Headquarters

TOTOLINK Technology Co., Ltd.
Taipei, Taiwan
Phone: +886-2-2659-1868
Email: info.tw@totolink.com

Additional Offices

For regional office information and local support contacts, please visit:
www.totolink.tw/contact

> 💡 **Best Practice**: Register your SoftAC installation on our support portal to receive important updates, security notifications, and access to premium support resources.

> 📝 **Note**: Support availability and response times may vary by region and support plan. Contact your local TOTOLINK representative for specific details about support in your area.

Thank you for choosing TOTOLINK SoftAC. We're committed to ensuring your success with our software access controller solution. Don't hesitate to reach out whenever you need assistance – we're here to help!

Support information is subject to change. Please visit our website for the most current contact information and support options.