Ads-tec-Industrial IT GmbH

IRF1xxx, IRF2xxx and IRF3xxx
Application Note -Firmware migration guide 2.0.0 and 5.0.0

© *Copyright* 2024

Table of contents

1 Introduction 3
1.1 Strong Passwords for Authentication 3
1.2 Session Timeout Management 3
2. Firmware update/downgrade 3
2.1 Firmware upgrade 3
2.2 Firmware downgrade 4
3 What's new? 5
3.1. HTTPS, Access the Web Interface 5
3.2 Migrate to secure passwords 6
3.2 HTTP/HTTPS web access 7
3.3 Activating Compatibility Mode for Downgrade or Legacy APIs 9
3.4. IoT Filter Integration 10
6 Document version management 11

© *Copyright* 2024

1 Introduction

ADS-TEC is pleased to announce the release of a new firmware update for the IRF1xxx, IRF2xxx, and IRF3xxx series devices. This documentation provides detailed information on the new firmware and the major changes compared to previous versions. It is important to read this document to understand how the changes will affect your system and ensure a smooth and secure transition.

Key Enhancements in Firmware Version 2.0.0 and 5.0.0

This update includes several significant improvements, particularly in terms of security and functionality. Some of the major changes in this release are as follows.

1.1 Strong Passwords for Authentication

One of the most important enhancements is the introduction of stronger password security for accessing the firewall's web interface. In previous firmware versions (prior to 2.0.0/5.0.0), device passwords were stored using the MD5 hash function, which is no longer considered secure.

New Password Hashing: Starting with firmware 2.0.0, passwords are stored using the Argon2 hashing algorithm, a much more secure method.

Compatibility with Older Versions: Due to the transition from MD5 to Argon2, compatibility between older versions of the firmware and 2.0.0 may cause issues, especially for users who are upgrading from firmware versions prior to 2.0.0. To ensure that older configurations continue to function properly, we have introduced a compatibility mode.

1.2 Session Timeout Management

Another key enhancement is the management of authenticated user sessions. In earlier versions, sessions remained open until manually terminated. With firmware 2.0.0, sessions now automatically time out after 300 seconds (5 minutes) of inactivity (user will be automatically logged out and asked for login).

Configurable Timeout: In future firmware releases, this session timeout will be configurable via the GUI.

2. Firmware update/downgrade

2.1 Firmware upgrade

The new firmware versions 2.0.0/5.0.0 require at least the following firmware version for update. If you are running an older version please update to the required version first.

Please note that after the update the device will run in the insecure password compatibility mode. The device will directly run with the improved password mode if you reset the device to factory defaults or run the migration wizard afterwards.

Variant	Required firmware version	New firmware version
IRF1xxx	1.6.9 or 1.6.10	2.0.x
IRF2xxx	4.5.8 or 4.5.9	5.0.x
IRF3xxx	1.3.9 or 1.3.10	2.0.x

© *Copyright* 2024

2.2 Firmware downgrade

Firmware downgrade from the new to older version requires compatibility mode (Please refer to compatibility mode part).

To make firmware downgrade to older versions than 2.0.0 and 5.0.0 by using strong password it is necessary to activate compatibility mode.

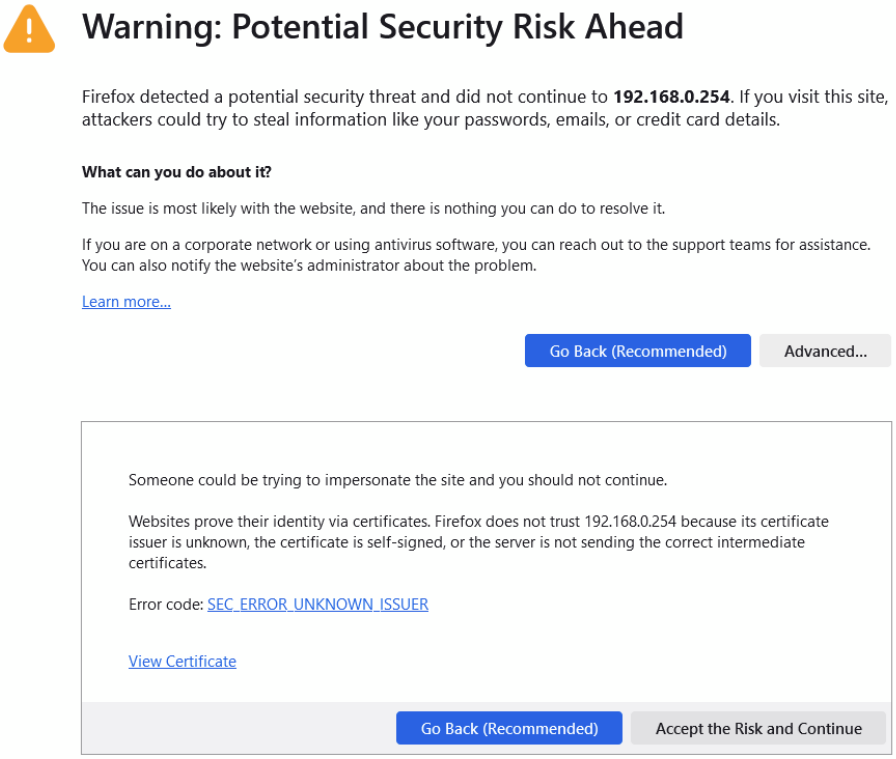
Otherwise, the firmware downgrade is blocked as the device would end without any passwords if running the old firmware version with an incompatible password storage.

© *Copyright* 2024

3 What's new?

3.1. HTTPS, Access the Web Interface

The Web Interface of the device is now reachable by HTTPS only. This implies that you will get a Security Warning from your browser:

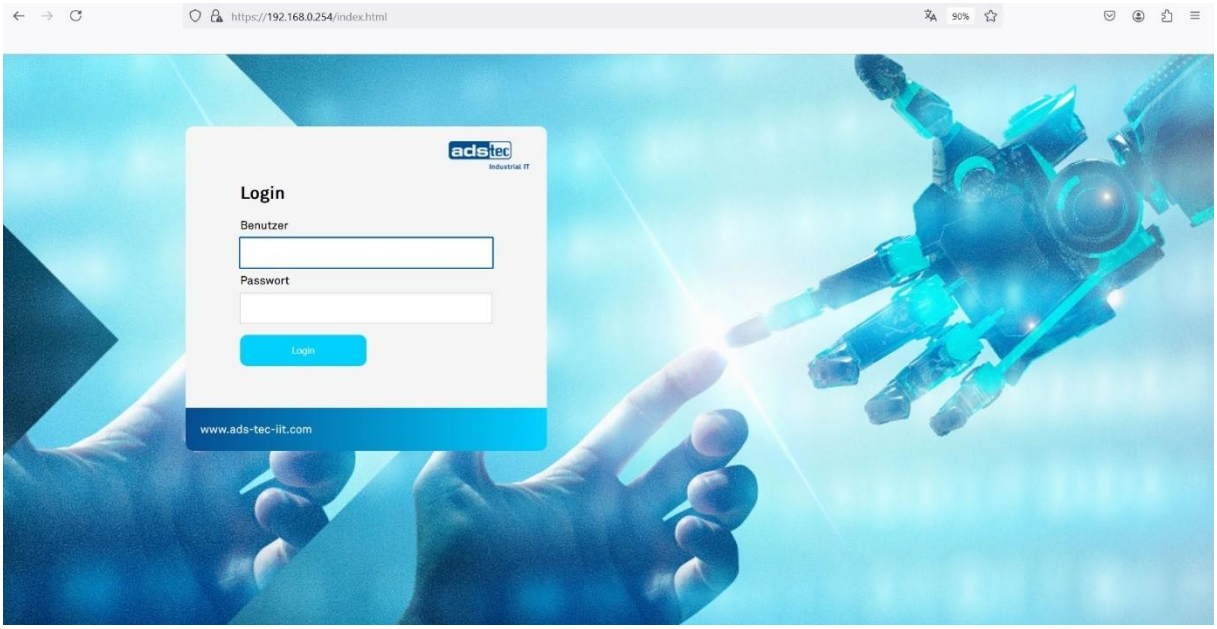


Example: With Firefox, please select "Advanced" and the "Accept the Risk and Continue".

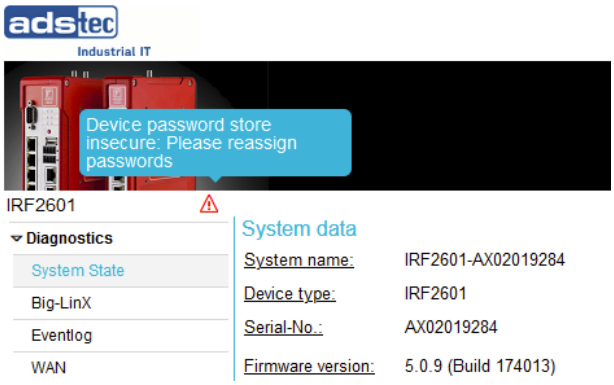
To proceed, you can use the workaround of accepting the risks and continuing. However, to avoid this warning permanently, you need to import the device's self generated CA certificate into the browser's certificate store or import your own device certificate into the device.

© *Copyright* 2024

The Device will now welcome you with a new login screen:



If you've updated the device from an older firmware, a symbol will indicate the security status of your password storage:



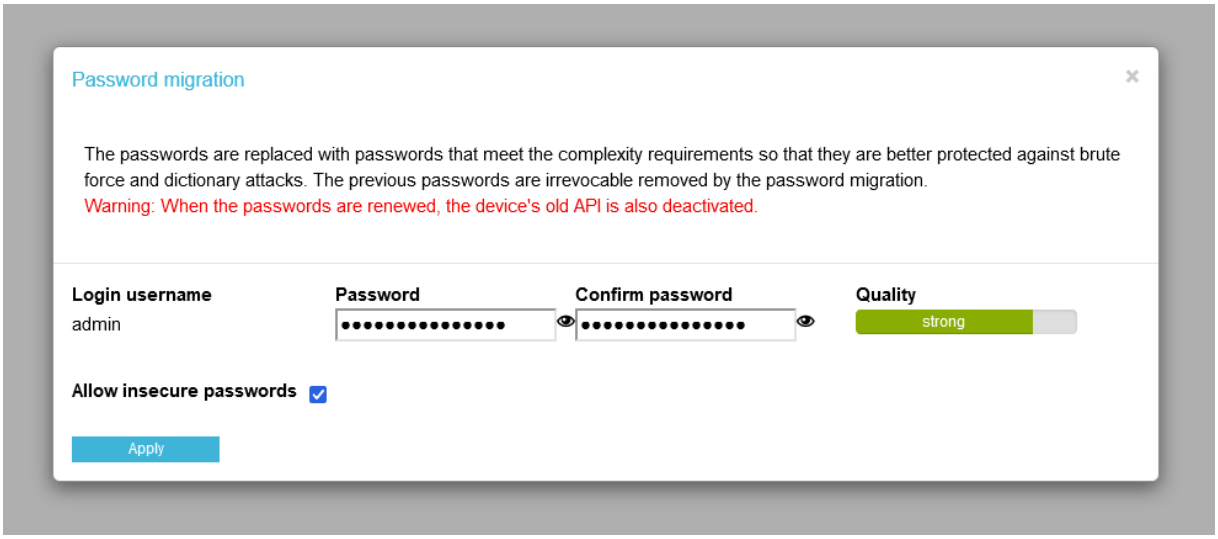
You can click on this icon to start the migration wizard. See next chapter.

3.2 Migrate to secure passwords

This process is needed if you upgraded from older firmware. You can either start this by clicking on the warning in the menu icon or by using the menu and navigate to Configuration-> Access Control -> User accounts. Click on the "Start Password migration" button there.

© *Copyright* 2024

The password migration wizard is needed to configure the passwords of all user accounts at once. The system will switch to the new password storage afterwards.

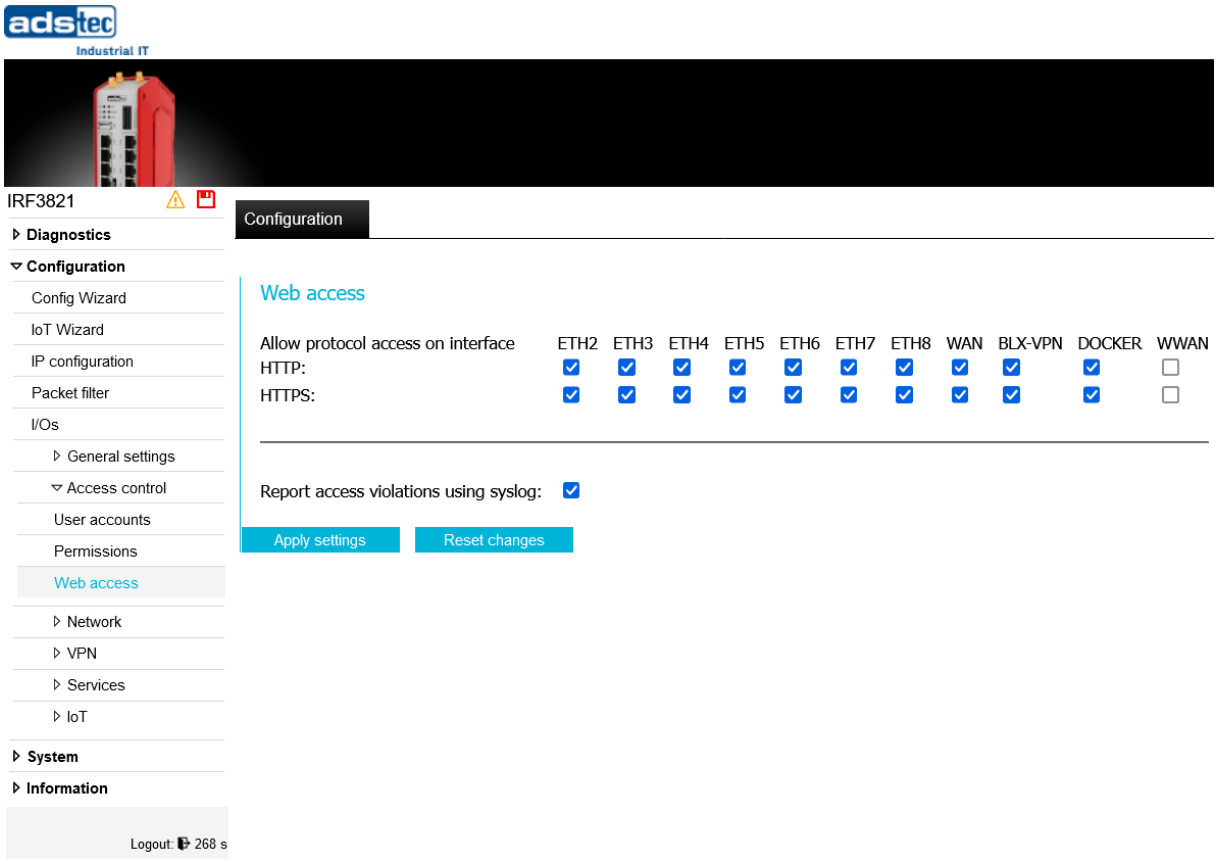


The classic HTTP API will get disabled as well. Please see the ADS-TEC document “Application Note - HTTP API Migration Guide” for details if you’re using this API.

3.2 HTTP/HTTPS web access

The firewall web interface in 2.0.0 will automatically redirect HTTP requests to HTTPS, ensuring secure web access. However, if your previous configuration used HTTP (port 80), this will now be redirected to HTTPS (port 443).

© Copyright 2024



Notice: all HTTP requests from the allowed interfaces will be automatically redirected to HTTPS if HTTP is allowed on the Web access page.

If you disable HTTP on the Web access page, then you now effectively disable the redirect as well.

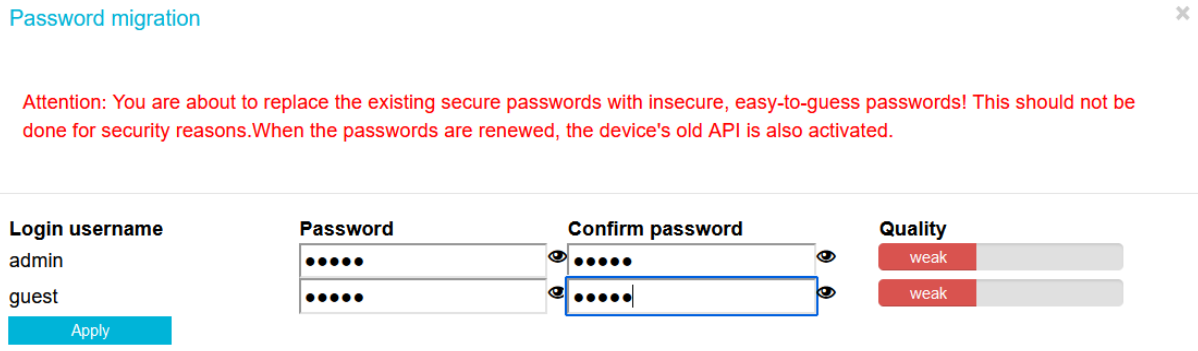
© *Copyright* 2024

3.3 Activating Compatibility Mode for Downgrade or Legacy APIs

To activate compatibility mode and ensure that legacy features continue to function, or downgrades are possible, follow these steps:

Navigate to the GUI: Go to Configuration -> Access Control -> User Accounts.

Click on “Password Migration to Insecure Password Storage” (Compatibility Mode): This allows legacy MD5 passwords to be accepted.



Notice: if different users are activated be sure to update all passwords for each user.

© Copyright 2024

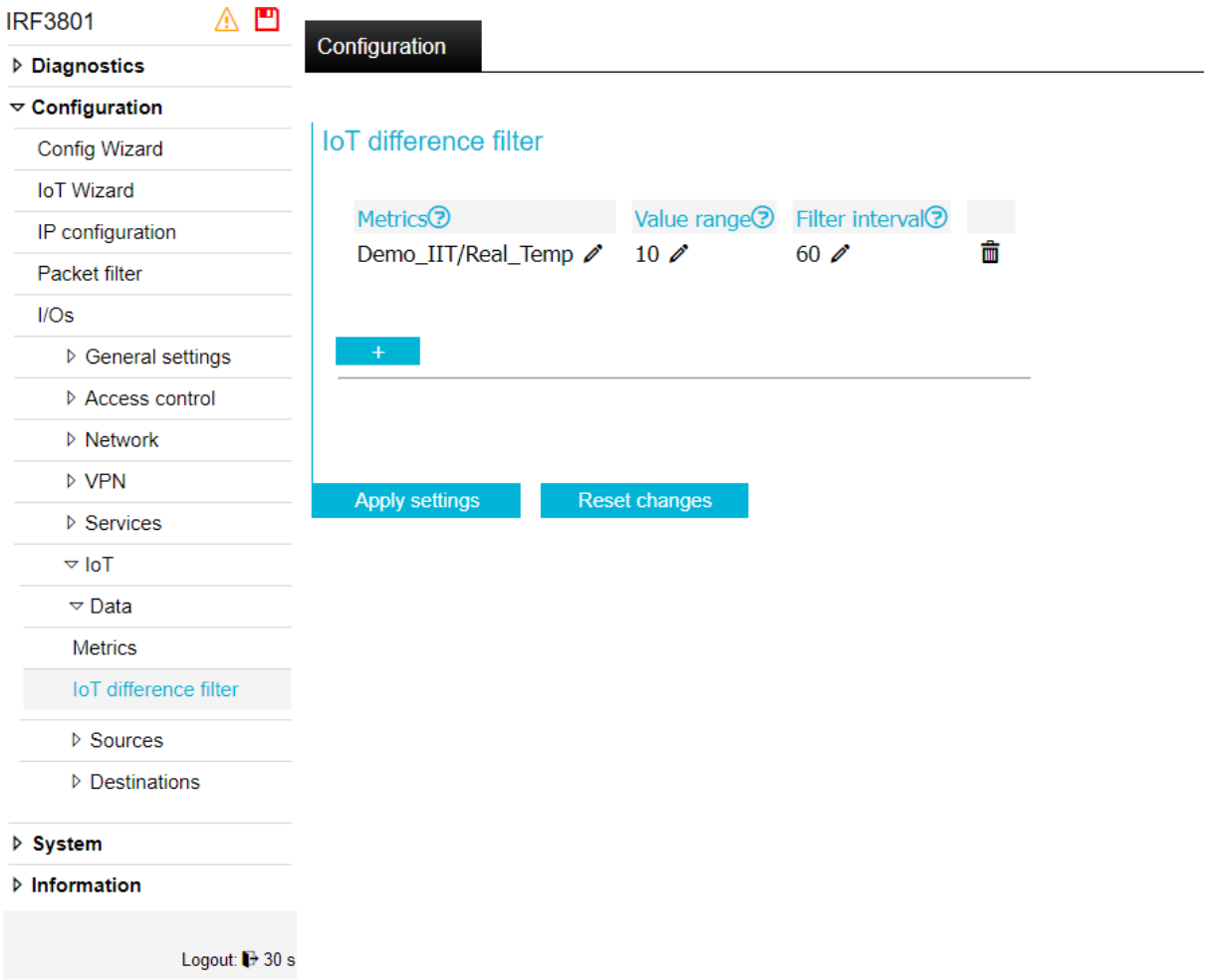
3.4. IoT Filter Integration

Older firmware than 2.0.0/5.0.0 includes transmission cycle time to push IoT-data into the cloud, this is not needed any more starting within the 2.0.0/5.0.0 Firmware versions. To have a better scalable and perfect filter option to push IoT data we included a new IoT service features that allow you to set up a filter for transmitting IoT data. These features enable each IoT data such as OPC UA, Modbus TCP, and Modbus RTU, to be individually filtered. This can save costs for mobile providers.

Configuration -> Services -> IoT ->Data ->IoT Filter Difference:

Under the IoT Difference Filter, you can now define "ranges" for each individual value. When a value remains within the defined range, no data is sent. Additionally, a time-based filter can be set for sending data.

Example:



Temperature Value Base Value: 30

Range: ±10

Interval: 60 minutes

If the value stays within the range of ±10 around the base value (e.g., between 20 and 40), no data will be sent until the 60-minute interval has passed. However, if the value exceeds the range (e.g., reaches 50), the value will be sent immediately. This functionality provides greater

© Copyright 2024

flexibility to define thresholds for individual values and ensures timely reactions when a value exceeds the specified range.

If you have any questions or need assistance, please feel free to contact our support team.

Mail : support.iit@ads-tec.de
Web: www.ads-tec-iit.com/support/

6 Document version management

Version	Date	Content	Author
V 1.0	09.12.2024	First document version	SiSm
V1.1	16.12.2024	Review	SnPr

© *Copyright* 2024