TEST REPORT FOR: ACM-1 – APPLICABILITY OF ACCESS CONTROL MECHANISMS

Product: TP-LINK Wi-Fi Router
Model No: Archer A10 AC2600 MU-MIMO
Test Report No: DLPL-20251801-01
Assessment: As per EN-18031-1 (ACM-1 – APPLICABILITY OF ACCESS CONTROL MECHANISMS)

DELTAPHI LABS PRIVATE LIMITED
606, Meadows, Sahar Plaza Andheri Kurla Road,
Mumbai 400059 Maharashtra, India

Test Report

■ **TSTL Name**	Deltaphi Labs Pvt Ltd (DLPL)
■ **Applicant Name**	Internal To (DLPL).
■ **Application Number**	Internal To (DLPL).
■ **Applicable ER**	As per EN-18031-1 (ACM-1 – APPLICABILITY OF ACCESS CONTROL MECHANISMS)
■ **TSTL Document ID**	DLPL-20251801-01
DUT Details: -	
■ **DUT Make**	TP-Link Wi-Fi Router
■ **DUT Model no**	ARCHER A10 AC2600 MU-MIMO
■ **DUT Serial Number**	2208134000657
■ **DUT Software Version**	1.0.2
■ **DUT Hardware Version**	Archer A10 v2.0
■ **OEM Supplied Document list:**	Not available (Internal test).
■ **Vendor Doc, File name, Page no**	NA
■ **Tools used and version**	Firefox v (136.0)
■ **DUT Firmware Hash**	d9257bed79f00f0e69132c04eeeca31f9663946c16a0808967fe0827f3656813
■ **Test Details: -**	
■ **Test Engineer**	Manojkumar S
■ **Authorized By**	Krishnan V
■ **Condition of SUT/DUT**	Working
■ **Location of Test Performed**	At LAB
■ **Date of Receipt of SUT/DUT**	NA
■ **Date of Commencement of Testing**	09/03/2025
■ **Date of Completion of Testing**	09/03/2025
■ **Test Report Issued Date**	09/03/2025
■ **Total Number of Pages**	19

Change log:

Date	-
Changed By	-
Change details	-

Report Summary

A sample unit of M/s **Deltaphi Labs Pvt Ltd**. Product: **TP-Link WI-FI Router** Model: **Archer A10 AC2600 MU-MIMO** Serial No. **2208134000657** with Interface - was tested **as per EN-18031-1.** The sample does not meet the requirement of standards as mentioned above and not Compliant. For details, please refer the test results.

Manojkumar S	Vasantha Kumar P	Krishnan V
Test Engineer	**Reviewed By**	**Authorized By**

Remarks:

1. DUT (Device Under Test).
2. This test report refers to the only particular item submitted for testing.
3. This test report shall not be reproduced except in full without the written permission of Lab Directors of DLPL.
4. DLPL is only responsible for the reported results of tested sample(s), test sample submitted by customers.
5. DLPL is not responsible for the accuracy of information provided by the customer.

INDEX

Table of Contents

Section 1: Product Assessed

1.1 ER Section No & Name:

Section: 1.1.1 Access Control Mechanisms

1.2 Security Requirement No & Name:

1.2.1 Applicability of Access Control Mechanisms

1.3 Requirement Description

The TP-Link Archer A10 Router employs Access Control Mechanisms (ACM) to secure its network and administrative functions, as per EN 18031-1:2024 guidelines. These mechanisms regulate user access to Wi-Fi networks, admin settings, and security assets, ensuring that only authorized users can configure or manage the router. Key security features include password-protected Wi-Fi, WPA2/WPA3 encryption, MAC filtering, guest network isolation, and admin authentication.

1.4 Reference Number:

NA

Section 2: DUT Confirmation Details

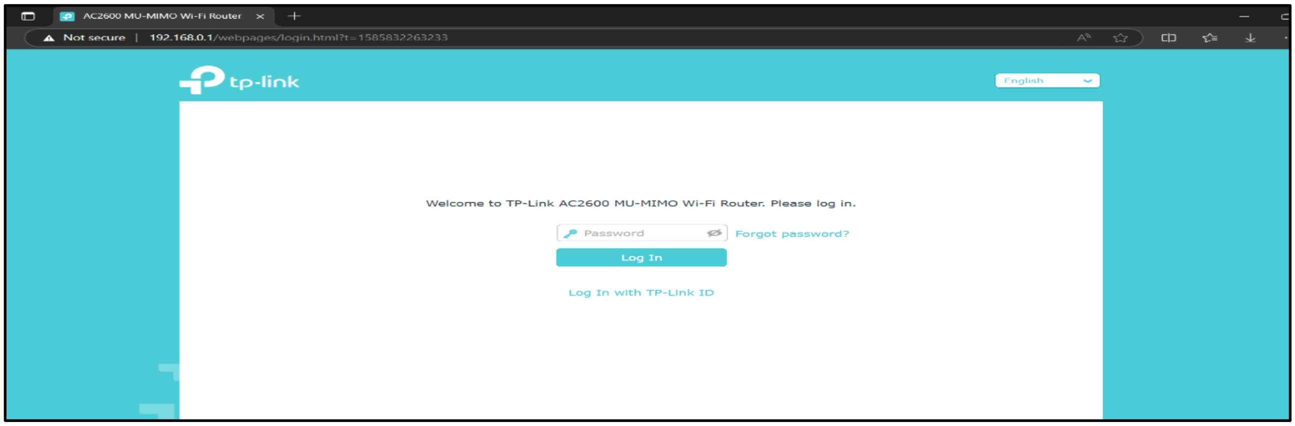
2.1 DUT:

TP-Link WI-FI Router Version 2.0

2.2 DUT General Information:

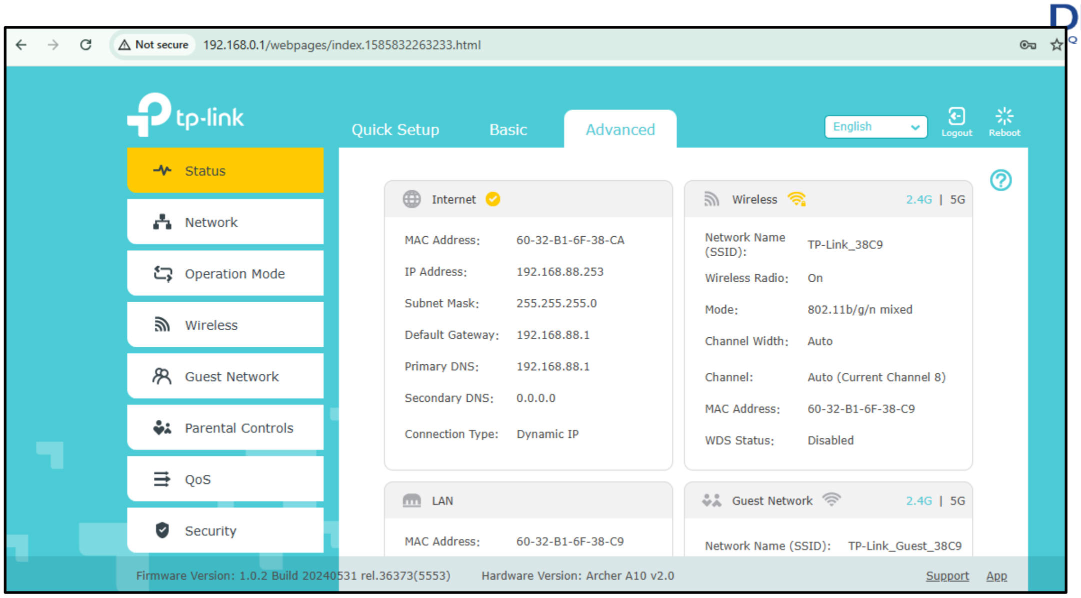
DUT Make	▪ TP-Link Wi-Fi Router
DUT Model no	▪ Archer A10 AC2600 MU-MIMO
DUT Serial Number	▪ 2208134000657
DUT Hardware Version	▪ 2.0

2.3 DUT Photographs:


AC2600 MU-MIMO Wi-Fi Router
Not secure | 192.168.0.1/webpages/login.html?t=1585832263233
tp-link
English
Password
Forgot password?
Log In
Log In with TP-Link ID

Welcome to TP-Link AC2600 MU-MIMO Wi-Fi Router. Please log in.

Figure 2.3.1 DUT Name and Model.



192.168.0.1/webpages/index.1585832263233.html

Internet

MAC Address: 60-32-B1-6F-38-CA
IP Address: 192.168.88.253
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.88.1
Primary DNS: 192.168.88.1
Secondary DNS: 0.0.0.0
Connection Type: Dynamic IP

Wireless

Network Name (SSID): TP-Link_38C9
Wireless Radio: On
Mode: 802.11b/g/n mixed
Channel Width: Auto
Channel: Auto (Current Channel 8)
MAC Address: 60-32-B1-6F-38-C9
WDS Status: Disabled

LAN

MAC Address: 60-32-B1-6F-38-C9

Guest Network

Network Name (SSID): TP-Link_Guest_38C9

Firmware Version: 1.0.2 Build 20240531 rel.36373(5553) Hardware Version: Archer A10 v2.0

Figure 2.3.2 DUT System Information and Software Version.

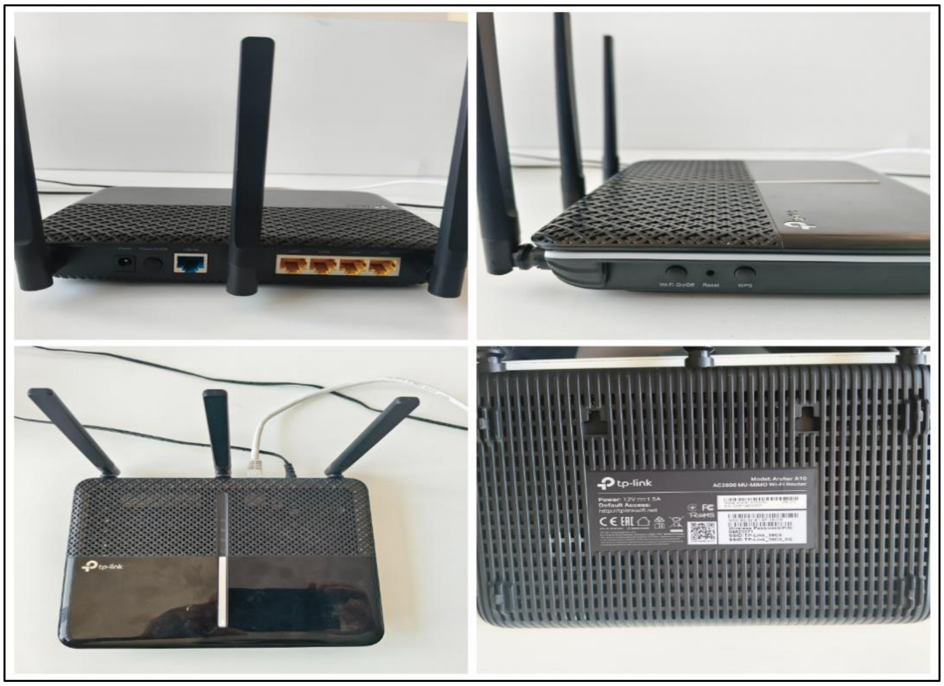


Figure 2.3.3 - DUT Images

2.4 DUT Access Credentials:

Username of the Account	Password of the Account	Group	Privileges
admin	infected@2020	Administrator	Admin – Highest Privilege

Table 2.4.1 DUT Access Credentials

Username of the Account	Password of the Account	Group	Privileges
test1@gmail.com	infected@2022	Administrator	Admin – Highest Privilege
test2@gmail.com	infected@2023	User	User – Low Privilege

Table 2.4.1 DUT Cloud Access Credentials

- **Wireless Access Credentials:**

SSID	Password	Frequency	Security
Tp-Link_38C9	infected@123	2.4 GHz	WPA2-Personal

Table 2.4.2 DUT WIFI Credentials

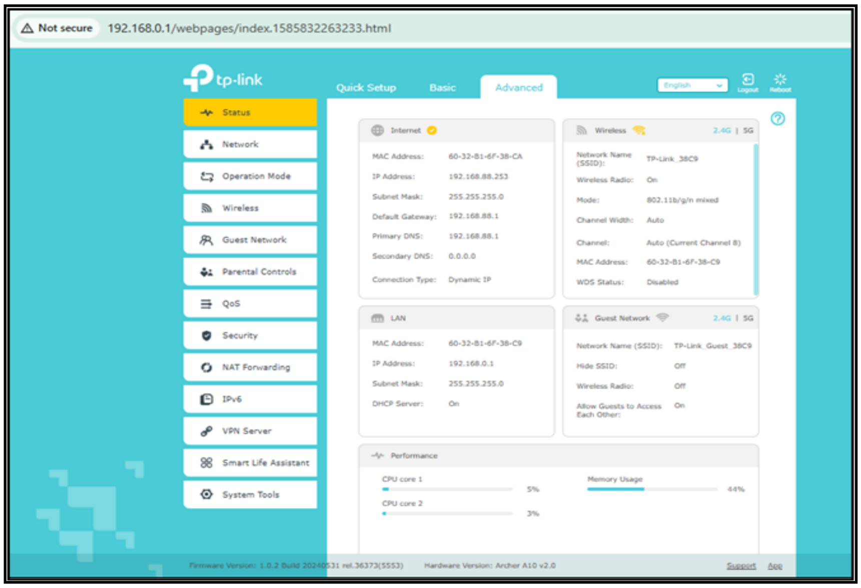
2.5 DUT Interface Information:

Interfaces	No.of Ports	Interface Type	Interface Name
LAN	4 Port(s)	Physical	LAN1, LAN2, LAN3, LAN4,
WAN	1 Port(s)	Physical	Internet 1

2.6 DUT Configuration:

- The router's admin interface (192.168.0.1) is protected with username/password authentication to prevent unauthorized configuration changes.
- A testing machine (192.168.0.173) is connected to the Archer A10 via Ethernet for security assessments.

- DUT is preconfigured with a web-based management interface for configuration and monitoring. The firmware version is 1.0.2.



192.168.0.1/webpages/index.1585832263233.html

Internet

MAC Address: 60-32-B1-6F-38-CA
IP Address: 192.168.88.253
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.88.1
Primary DNS: 192.168.88.1
Secondary DNS: 0.0.0.0
Connection Type: Dynamic IP

Wireless

Network Name (SSID): TP-Link_38C9
Wireless Radio: On
Mode: 802.11b/g/n mixed
Channel Width: Auto
Channel: Auto (Current Channel 8)
MAC Address: 60-32-B1-6F-38-C9
WDS Status: Disabled

LAN

MAC Address: 60-32-B1-6F-38-C9
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
DHCP Server: On

Guest Network

Network Name (SSID): TP-Link_Guest_38C9
Hide SSID: Off
Wireless Radio: Off
Allow Guests to Access Each Other: On

Performance

CPU core 1 5%
CPU core 2 3%
Memory Usage 44%

Firmware Version: 1.0.2 Build 20240531 rel.36373(5553) Hardware Version: Archer A10 v2.0

Section 3: Test Plan

3.1 No. of Test Scenarios/Test-Case required.

3.1.1 Test Scenario 1.1.1.1:

To verify that the TP-Link Archer A10 AC2600 MU-MIMO v2.0 Wi-Fi Router supports the applicability of access control mechanisms.

3.1.1 Test Scenario 1.1.1.2:

Verify if physical or logical measures restrict access to authorized entities in the targeted environment.

3.1.1 Test Scenario 1.1.1.3:

Check whether legal implications prevent the implementation of access control mechanisms.

3.1.1 Test Scenario 1.1.1.4:

Verify if access control mechanisms exist to manage entities' access to security and network assets.

3.2 Pre-conditions

None

- **DUT login Credential:**

Username of the Account	Password of the Account	Group	Privileges
admin	infected@2020	Administrator	Admin – Highest Privilege

- **DUT web login Credential:**

Web GUI URL	▪ https://192.168.0.1
Username	▪ admin
Password	▪ infected@2020

3.3 Execution Steps per Scenario/Test-Case

3.1.1 Test Scenario 1.1.1.1: To verify that the router supports the applicability of access control mechanisms.

1. Connect to the router via a wired or wireless connection and open a web browser and enter the router's IP address (default: 192.168.0.1) and log in with the admin credentials.
2. Navigate to Advanced Settings → Security → Access Control and verify that Access Control is enabled.
3. Check if the router supports role-based access or different user privilege levels.
4. Try to access the router from an unauthorized device.

3.1.1 Test Scenario 1.1.1.2: Verify if physical or logical measures restrict access to authorized entities in the targeted environment.

1. Review authentication methods (e.g., password protection).
2. Ensure the router's admin panel is not accessible from the WAN (remote management disabled by default).
3. Try accessing the router's admin panel from a different subnet or unlisted MAC address.

3.1.1 Test Scenario 1.1.1.3: Check whether legal implications prevent the implementation of access control mechanisms.

1. Check if any local laws restrict access control mechanisms (e.g., GDPR, IT Act compliance).
2. Verify if the router's firmware has any region-specific restrictions on access control features.
3. Navigate Advanced System Tools → Firmware Upgrade and compare the firmware settings to TP-Link's regional firmware documentation.

3.1.1 Test Scenario 1.1.1.3: Verify if access control mechanisms exist to manage entities' access to security and network assets.

1. Log in to the router's admin panel and go to Advanced → Security → Access Control.
2. Verify the access management features by checking if the router provides the features like,
   - Device-based Access Control (Blacklist/Whitelist specific devices).
   - MAC Address Filtering (Block or allow devices based on MAC address).
   - Manual Device Management (Add or remove devices from the list).
3. Block a test device using MAC filtering and try to access the network and check if internet access is denied for blocked devices.

3.4 Test-Bed set-up Diagram Per Scenario

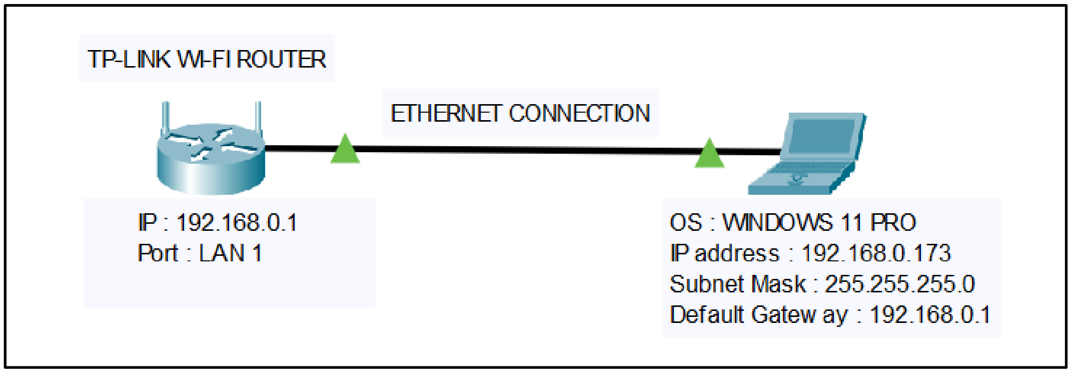


Figure 3.4.1 Test-Bed Set-up Diagram Per Scenario

3.5 Test Tools required Per Scenario

Command/Options Used	Execution Step	Tool Information
Firefox Browser	1.1.5.1	Firefox is a popular web browser developed by Mozilla. It offers features such as tabbed browsing, private browsing, built-in security and privacy protections, customizable themes and extensions, and synchronization of bookmarks, passwords, and browsing history across devices.

Table 3.5.1 Test Tool Details

Section 4: Test Execution

4.1.1 Test Case Number:
1.1.5.1 ITSAR WIFI-CPE

4.1.2 Test Case Name:
To verify that the router supports the applicability of access control mechanisms.

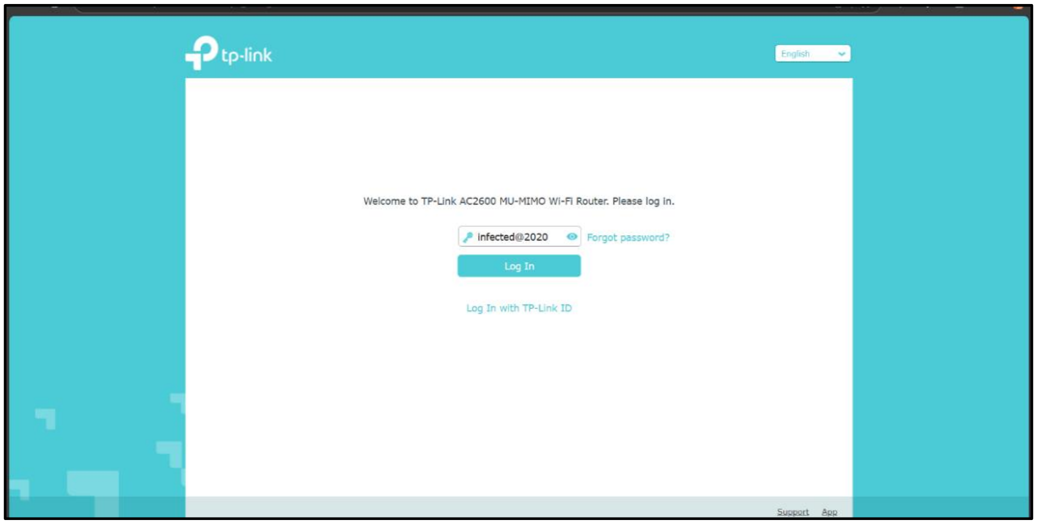
4.1.3 Test Case Description:
Ensure the router provides access control features like MAC filtering, IP restrictions, and user authentication. Verify that these mechanisms effectively restrict or allow access as configured.

4.1.4 Test-bed Diagram:
Refer the Test Bed Diagram on the Test-Plan above

4.1.5 Tools Used:
Refer the Tool used on the Test-Plan above

4.1.6 Execution Steps:

1. Log in to the router's admin panel (192.168.0.1).

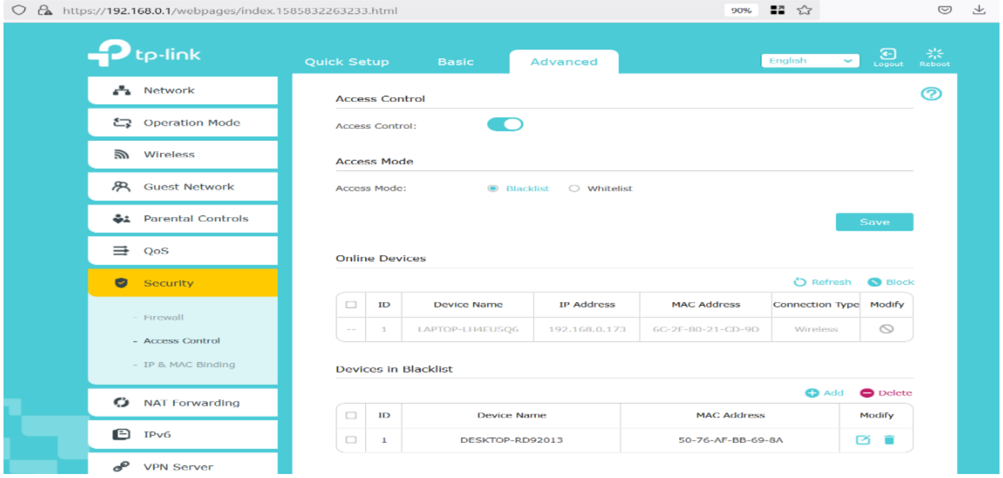


Welcome to TP-Link AC2600 MU-MIMO Wi-Fi Router. Please log in.

infected@2020

Figure 4.1.6.3.1 TP-Link web interface login

2. Go to Advanced → Security → Access Control and try blocking a device and check if access is denied.



Access Control

Access Control: ON

Access Mode

Access Mode: ● Blacklist ○ Whitelist

Online Devices

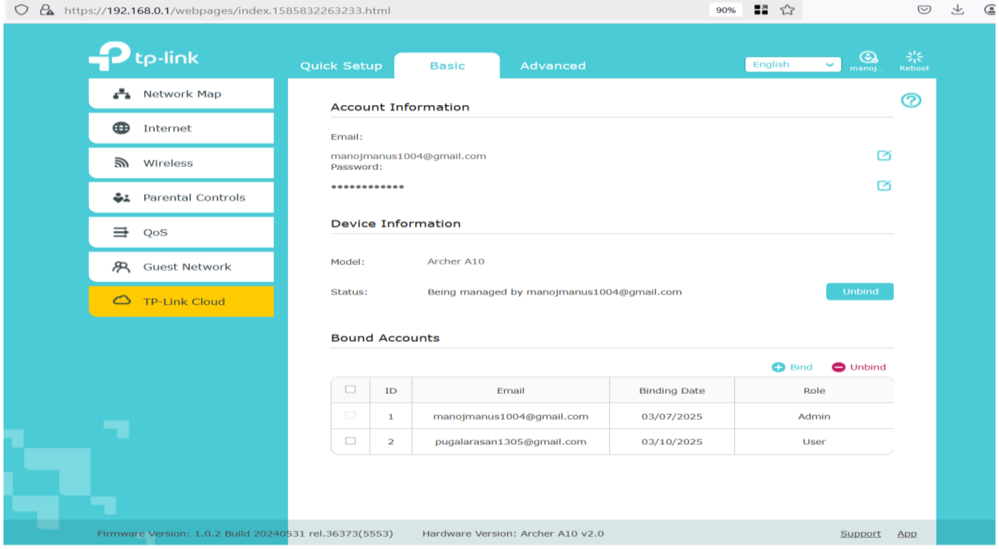
□	ID	Device Name	IP Address	MAC Address	Connection Type	Modify
--	1	LAPTOP-LH4EU5Q6	192.168.0.173	6C-2F-80-21-CD-9D	Wireless	⃠

Devices in Blacklist

□	ID	Device Name	MAC Address	Modify
□	1	DESKTOP-RD92013	50-76-AF-BB-69-8A	

Figure 4.1.6.3.1 TP-Link Access Control

3. Check if access control options like MAC filtering, IP restrictions, or user roles are available.



Account Information

Email:
manojmanus1004@gmail.com
Password:
•••••••••••••

Device Information

Model: Archer A10

Status: Being managed by manojmanus1004@gmail.com

Bound Accounts

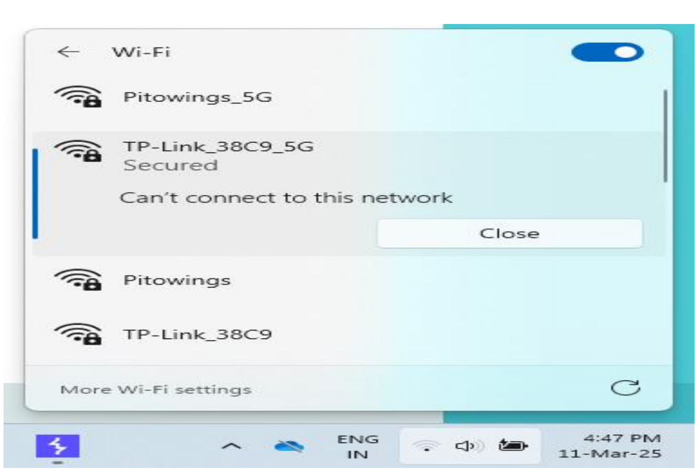
□	ID	Email	Binding Date	Role
□	1	manojmanus1004@gmail.com	03/07/2025	Admin
□	2	pugalarasan1305@gmail.com	03/10/2025	User

Firmware Version: 1.0.2 Build 20240531 rel.36373(5553) Hardware Version: Archer A10 v2.0

Figure 4.1.6.3.1 TP-Link User Roles

4.1.7 Evidence Provided:

- DUT enforces proper access control mechanisms. Unauthorized devices are blocked from connecting based on predefined access control rules.



Section 5: Test Observation and Result

5.1 Test Observation:

5.1.1 Test Scenario 1.1.5.1:

- During testing, the tester discovered that the (DUT) is not supported with server-side authentication. Therefore, mutual authentication is not possible. However, the communication between server and client is encrypted as per crypto ITSAR.

5.2 Test Case Result

ER No.	Test name	Actual Result
1.1.5.1	To verify that the TP-Link Archer A10 AC2600 MU-MIMO v2.0 Wi-Fi Router supports the applicability of access control mechanisms	FAIL

1.1.5.2	Verify if physical or logical measures restrict access to authorized entities in the targeted environment.	
1.1.5.3	Check whether legal implications prevent the implementation of access control mechanisms	
1.1.5.4	Verify if access control mechanisms exist to manage entities' access to security and network assets.	

Section 6: Raw Logs

These logs provide evidence that the specific tester executed the test at a specific date and time on the mentioned DUT.

- SS_4.1.6.3.1, SS_4.1.6.4.1, SS_4.1.6.5.1
- Networklog-1.1.1.5. pcap
- DUTlog-1.1.1.5.txt