Test Schedule and Test Procedure (TSTP)

ITSAR name: Wi-Fi CPEs 1.0.0	ITSAR No: ITSAR402122401

Disclaimer: **This TSTP is intended to serve as a guide for testing various clauses outlined in the relevant ITSAR. The test methods described in this TSTP are not exhaustive and should not be considered as the sole approach to test any clause. The actual testing process and results may vary depending on how the OEMs implemented the clause in their equipment.**

MTCTE के तहत जारी:
Issued under MTCTE by:

राष्ट्रीय संचार सुरक्षा केंद्र (रा.सं.सु.कें.)
दूरसंचार विभाग, संचार मंत्रालय
भारत सरकार
सिटी दूरभाष केंद्र, एसआर नगर, बैंगलोर-५६००२७, भारत

National Centre for Communication Security (NCCS)
Department of Telecommunications
Ministry of Communications
Government of India
City Telephone Exchange, SR Nagar, Bangalore-560027, India

Chapter 1: Common Security Requirement
Section 1.1: Access and Authorization

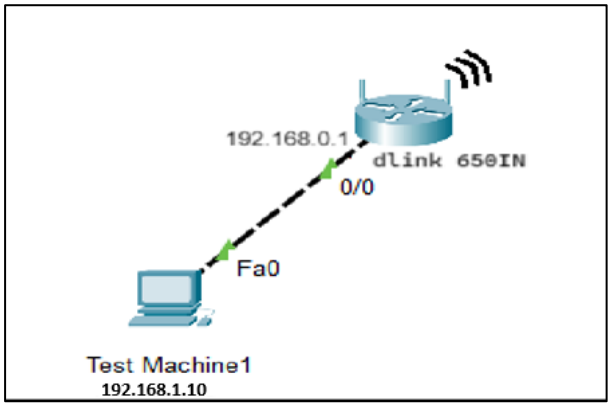
1.1.1 Authentication Policy

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.1: Access and Authorization**
2. **<Security Requirement No & Name > 1.1.1: Management Protocols Entity Mutual Authentication**
3. **<Requirement Description: > The** CPE shall communicate with authenticated management entities only. The protocols used for the CPE management shall support mutual authentication mechanisms, preferably with pre- shared key arrangements or by equivalent entity mutual authentication mechanisms. This shall be verified for all protocols used for CPE management. (This feature shall be supported on all WAN management interfaces).
4. **DUT Confirmation Details**:
5. **DUT Configuration:**
6. **Preconditions**
   - OEM shall provide details of all management or/and maintenance interfaces & respective protocols supported on those interfaces of the DUT
   - OEM shall support to configure management protocol such as TELNET, SSH, HTTP/HTTPS, TACACS+, SNMP v3 and SFTP) on Management Interface of DUT.
7. **Test Objective:-** To check if there is mutual authentication supported on the management protocols supported by DUT

8. **Test Plan**
   8.1. Number of Test Scenarios:
      8.1.1. Test Scenario to check the management protocols supported by DUT in comparison to the protocols given in the OEM document
      8.1.2. Test Scenario to check if mutual authentication supported on HTTPS
      8.1.3. Test Scenario to check if mutual authentication supported on RADIUS server (for wife access)

   8.2. Test Bed Diagram



8.3. Tools Required: - Only DUT needed

8.4. Test Execution Steps:-

- The tester shall run zenmap/nmap to check the management protocols supported by DUT.
- The tester should check if any mutual authentication supported for HTTPS and RADIUS

9. **Expected Results for Pass:** The DUT supports mutual authentication for the supported management protocols

10. **Expected Format of Evidence:** Screenshots of Terminal

11. **Test Execution:**

11.1 **Test Case Number:** 01

11.1.1 **Test Case Name:** Supported management protocols

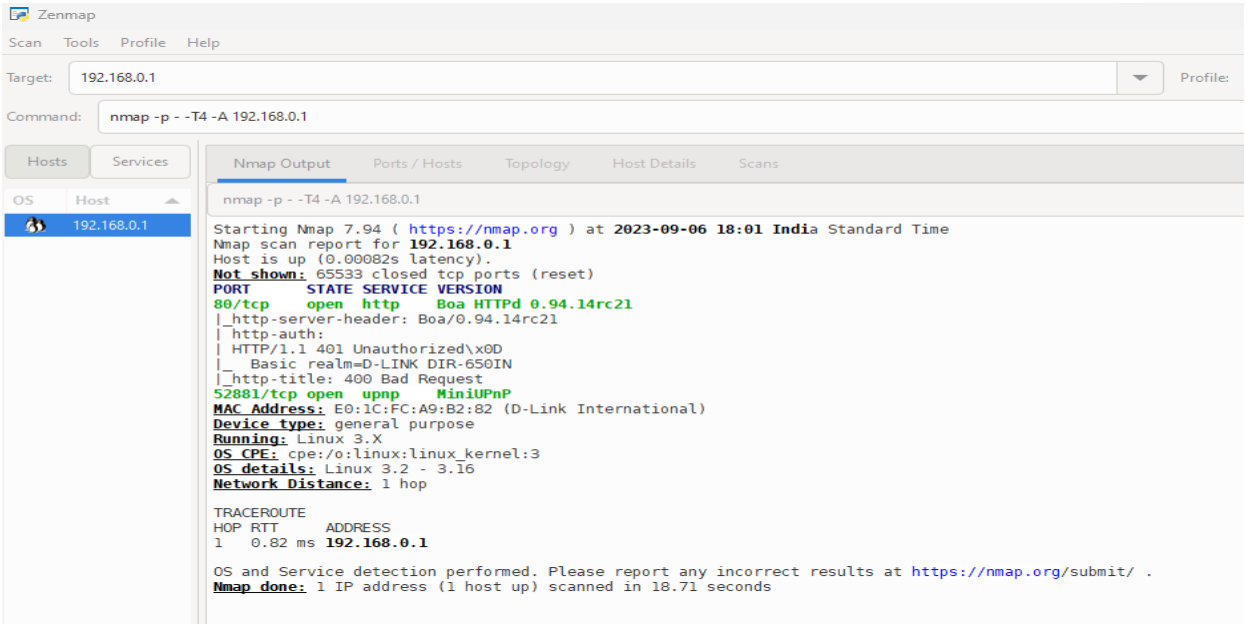
11.1.2 **Test Case Description:** The following testcase is done to check the supported management protocols.

11.1.3 **Execution Steps:**

PORT	Description
LAN 1	10/100 Mbps
LAN 2	10/100 Mbps

LAN 3	10/100 Mbps
WAN	10/100 Mbps
Power Connector	Input: 100 to 240 V AC, 50/60 Hz
Buttons	WPS/Reset , Power
Antenna	5dBi External

2.Run zenmap for port scanning



11.2 **Test Case Number:** 02

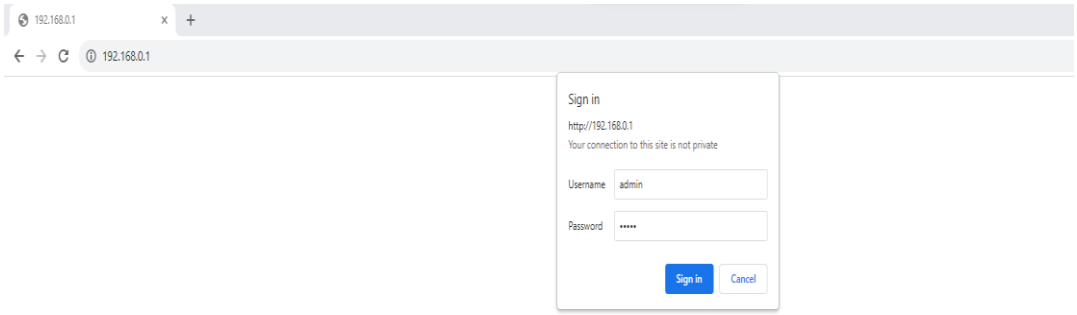
11.2.1 **Test Case Name:** Mutual authentication on HTTPS

11.2.2 **Test Case Description:** The following testcase is done to check the mutual authentication on HTTPS

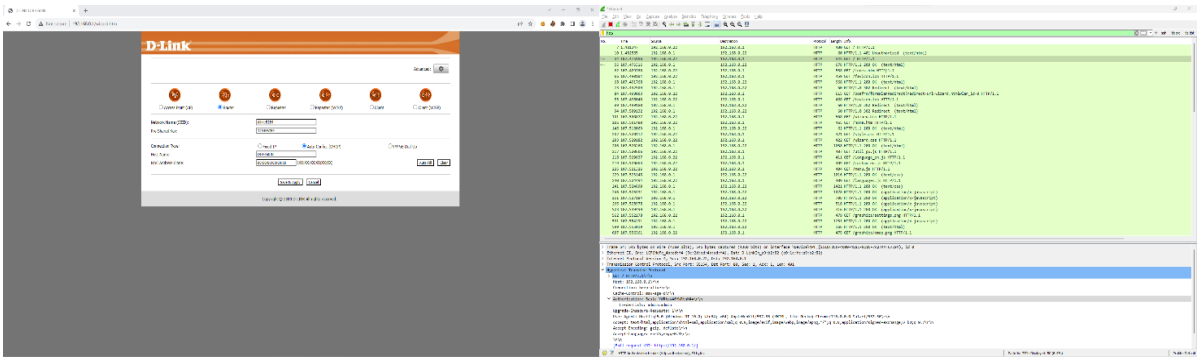
11.2.3 **Execution Steps:**

a. In DUT have preconfigured IP address on DUT. (192.168.0.1).

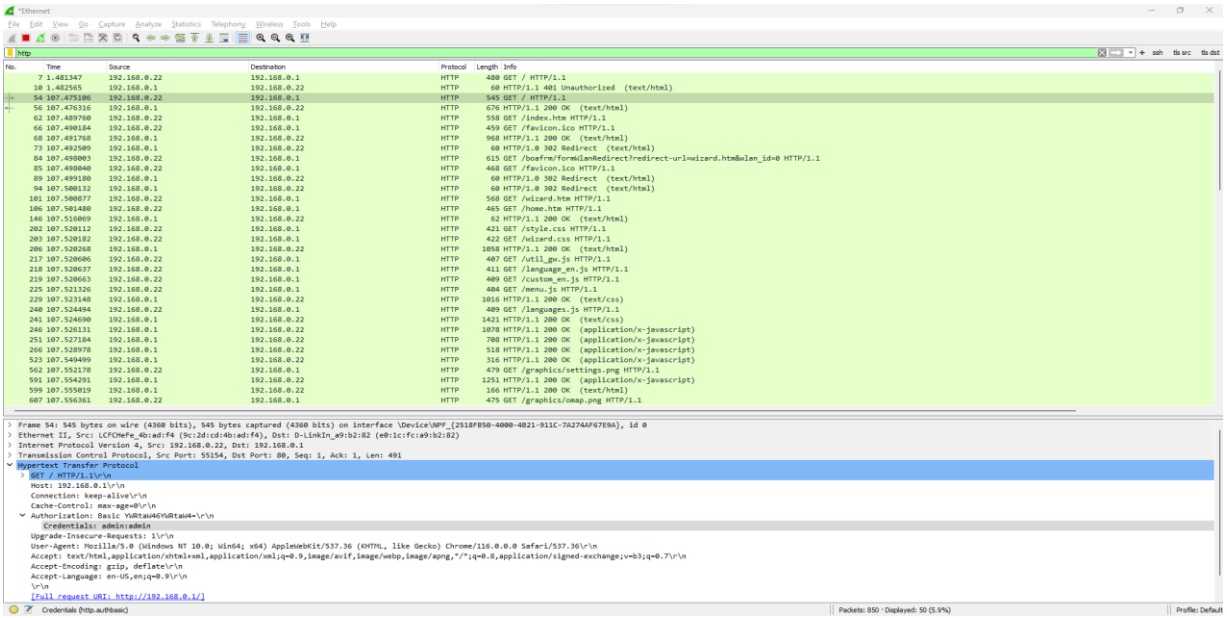
b. The Tester connects the DUT through LAN port and access HTTP using following http://192.168.0.1 on web browser of test machine (192.168.0.22).



c. The Tester captured traffic between DUT and test machine in Wireshark to verify whether there is any mutual authentication between both the entities.



d. The tester observed that there is no mutual authentication between DUT and Test machine established. In Wireshark, not able to see any key/certificate exchange between Server and client to authenticate and verify each other to establish mutual authentication.



11.3 **Test Case Number:** 03

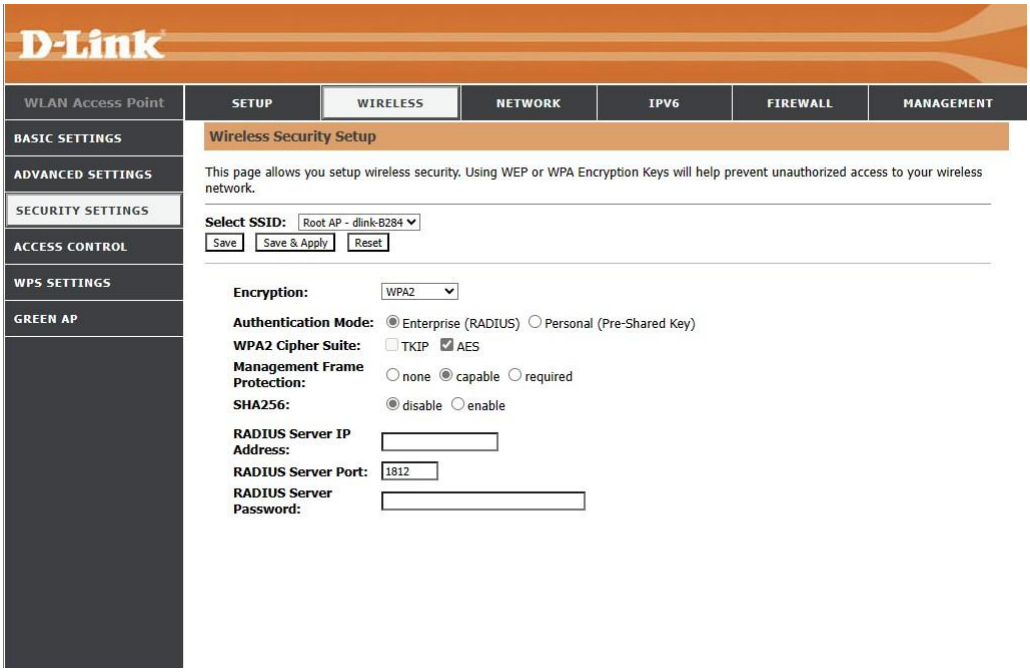
11.3.1 **Test Case Name:** Mutual authentication on RADIUS

11.3.2 **Test Case Description:** The following testcase is done to check the mutual authentication on HTTPS

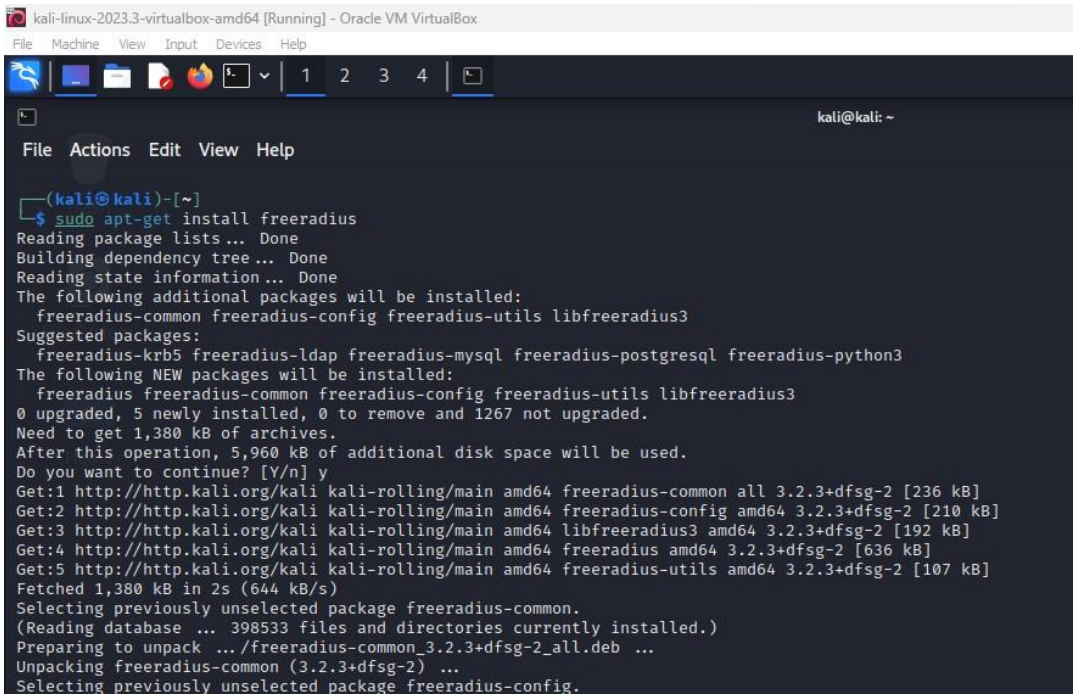
11.3.3 **Execution Steps:**

a. The tester observed DUT supports RADIUS protocol for WiFi Access.

b. In DUT, tester have manually configured to use IP address. (192.168.1.1).



c. Tester setup Freeradius server in Kali Linux testmachine using `apt-get install freeradius`

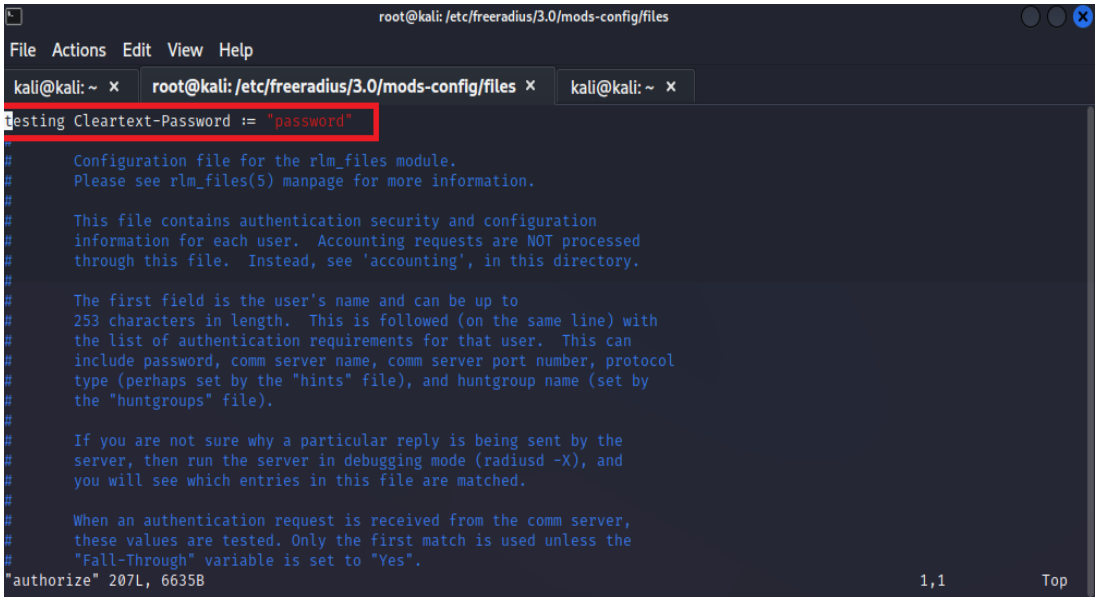


d. Tester adds client information to freeradius server in configuration file "/etc/freeradius/3.0/clients.conf" with ip address and secret (testing123).

e. Tester adds username and password for WiFi access to freeradius server in configuration file "/etc/freeradius/3.0/mods-config/files/authorize".

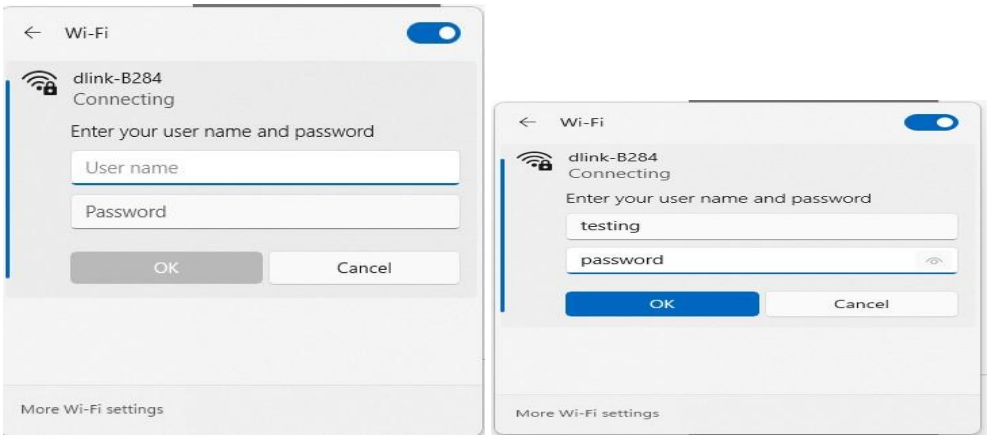
Username: testing

Password: password

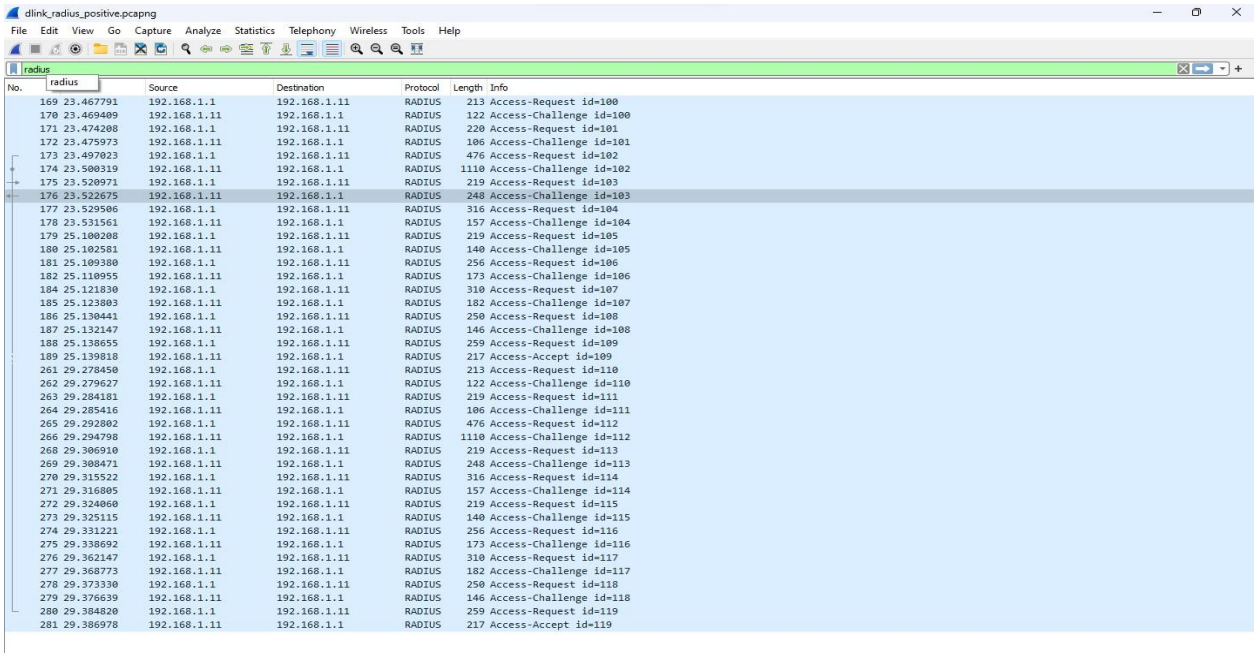


f. Tester configures CPE with RADIUS server information, i.e., IP address and secret.

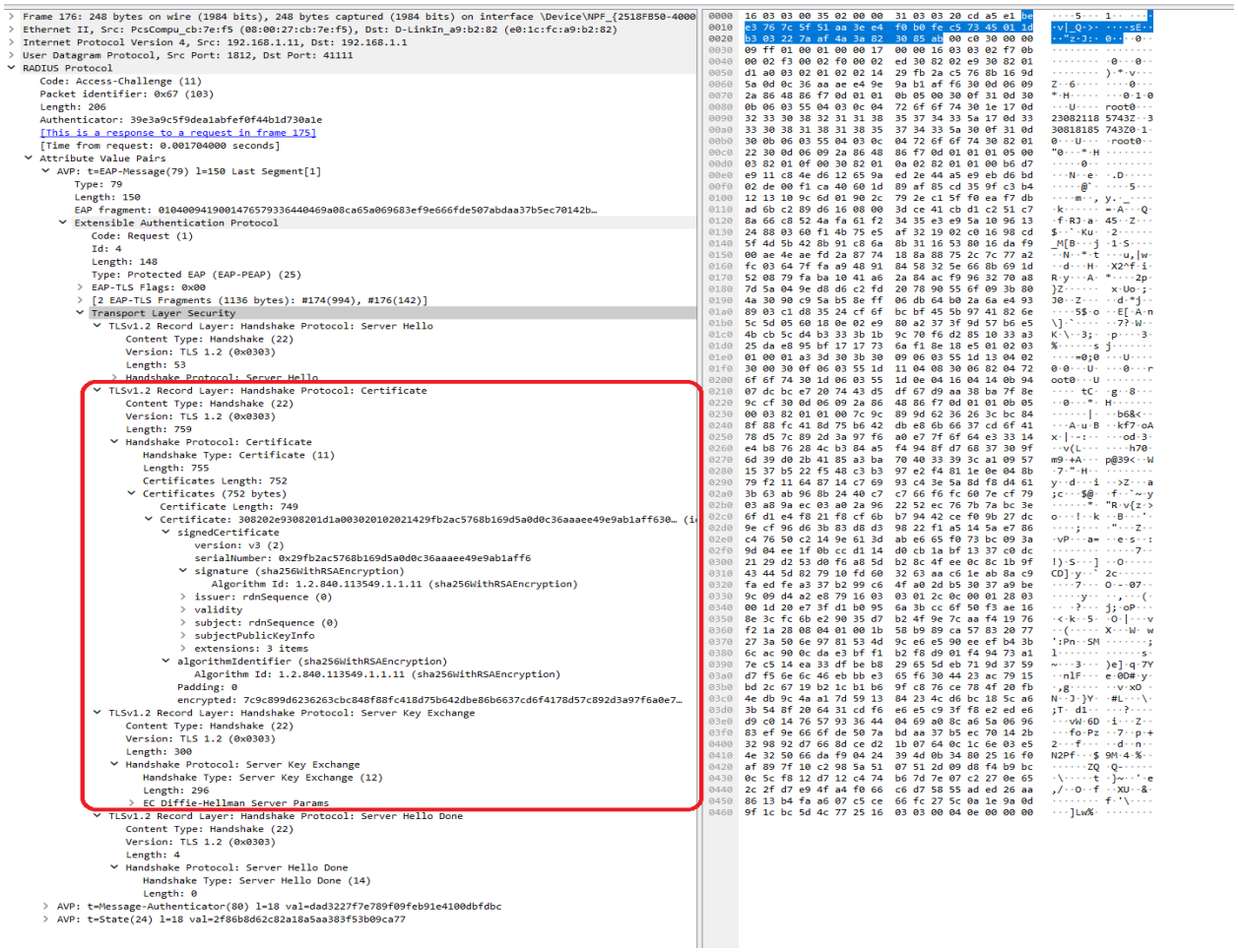
i. Tester attempts to capture the RADIUS traffic on Wireshark



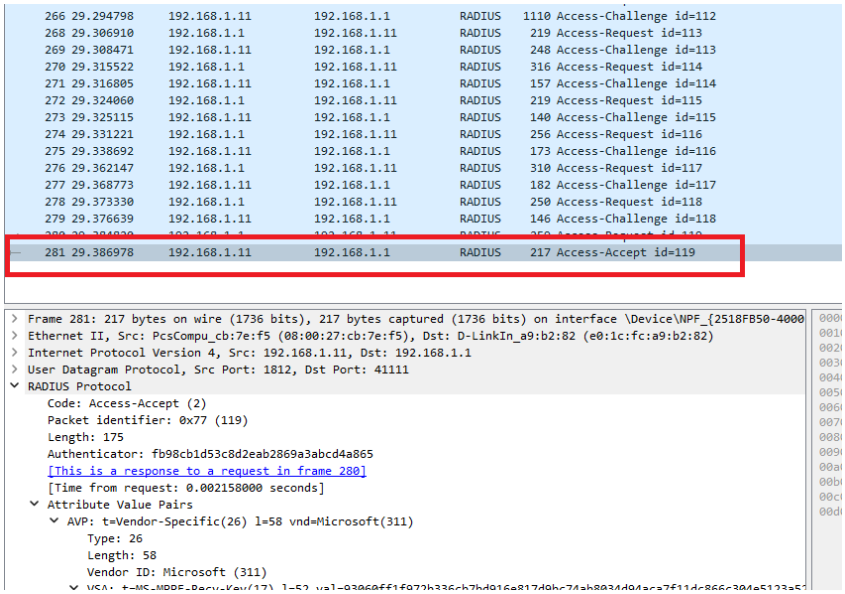
ii. While connection in progress, tester open the Wireshark to capture the traffic and starts capturing on the Ethernet interface of the test machine which CPE is connected to



iii.Tester observed that the communication between the CPE and the free radius server installed in test machine is mutually authenticated as the Certificate/Key exchange over EAP-TLS protocol has been verified in captured traffic in Wireshark



iv.Tester observed the test machine was able to connect to the CPE's WiFi successfully, also verified the "Access-Accept" message in the Wireshark trace.



v.Attached the Wireshark capture file below

Capture File: dlink_radius_positive.pcapng

11.3.4 **Test Observations:** Tester observed that the communication between the CPE and the free radius server installed in test machine is mutually authenticated as the Certificate/Key exchange over EAP-TLS protocol has been verified in captured traffic in Wireshark.

11.3.5 **Evidence Provided:** - Screenshots of Terminal

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Supported Management protocols	Pass	
2	HTTPS protocols	Fail	
3	RADIUS protocol	Pass	

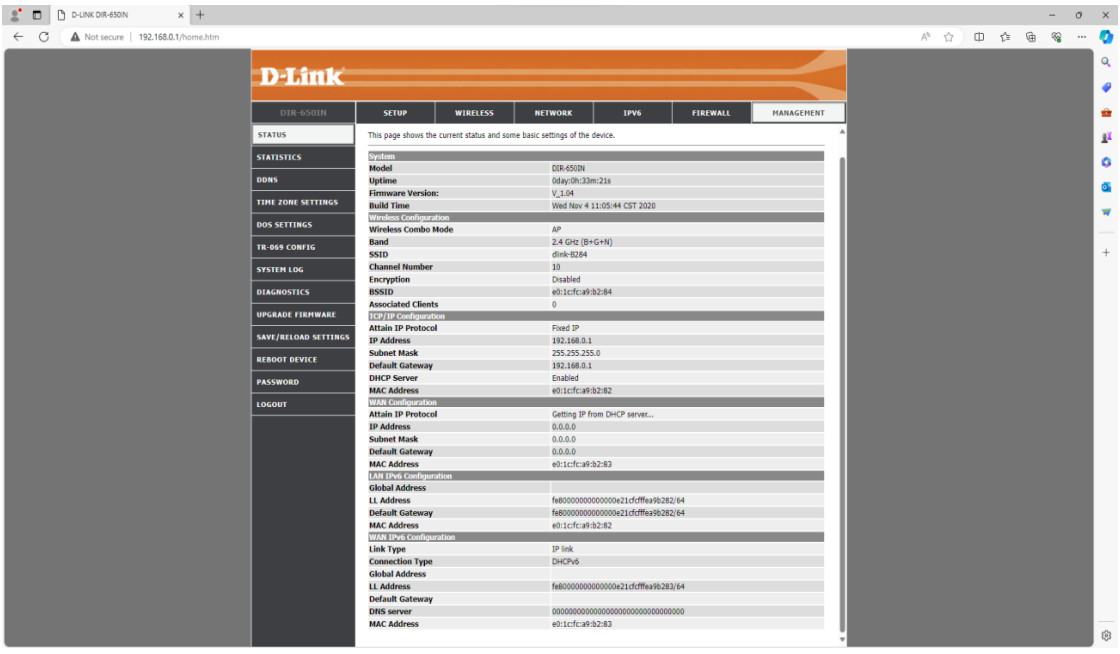
1.1.2 TSTP for Evaluation of Management Traffic Protection

ITSAR Name: Wi-Fi CPEs 2.0.0	ITSAR No: ITSAR40212YYMM	Clause No: 1.1.2

<DUT Details: > Wi-Fi CPE router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.1: Access and Authorization**
2. **<Security Requirement No & Name >12.1.2 : Management Traffic Protection**
3. **<Requirement Description: > All** management traffic shall be protected by integrity and encryption. Unprotected sessions shall not be accepted. The remote access methods can support traffic encryption using protocols such as HTTPS, SSHv2 or can be based on lower tunnelling protocols (IPsec VPN, TLS VPN, etc.).
   Secure cryptographic controls prescribed in Table 1 of the latest document "Indian Telecommunication Security Assurance Requirements (ITSAR) for Cryptographic Controls" shall only be used for system management.

4. **DUT Confirmation Details**:



5. **<u>DUT Configuration:</u>** The tester checks if the DUT is configured with the supported management protocols

6. **<u>Preconditions:-</u>** OEM shall provide detail management protocols supported by the DUT as well as the ciphers supported.

7. **Test Objective:-** To check if the DUT's all management traffic shall be protected by integrity and encryption as per secure cryptographic controls prescribed in Table 1 of the latest document "Indian Telecommunication Security Assurance Requirements (ITSAR) for Cryptographic Controls"

8. **Test Plan**

8.1. Number of Test Scenarios:

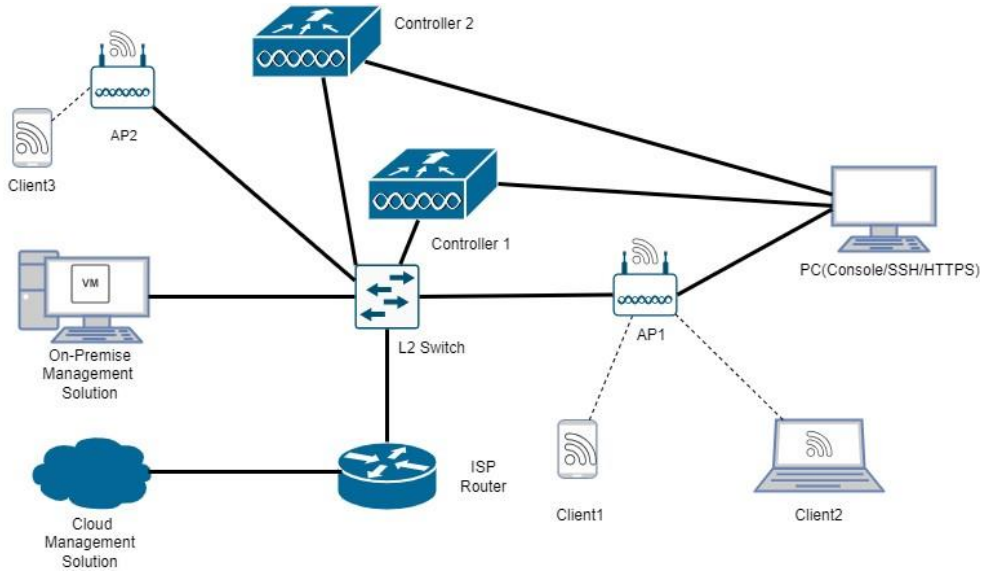
8.1.1. The Tester should check all the management protocols and the ciphers supported by the DUT described in OEM Documentation and make a note if any cipher is not permitted as per Crypto ITSAR Table-1 is present

8.1.2. Tester needs to verify that the traffic between DUT and Test Machine is protected via permitted cipher only. (like through SSH, SSL/TLS etc.)

8.1.3. The Tester shall verify that the traffic between DUT and test machine is not established with null or weak ciphers.

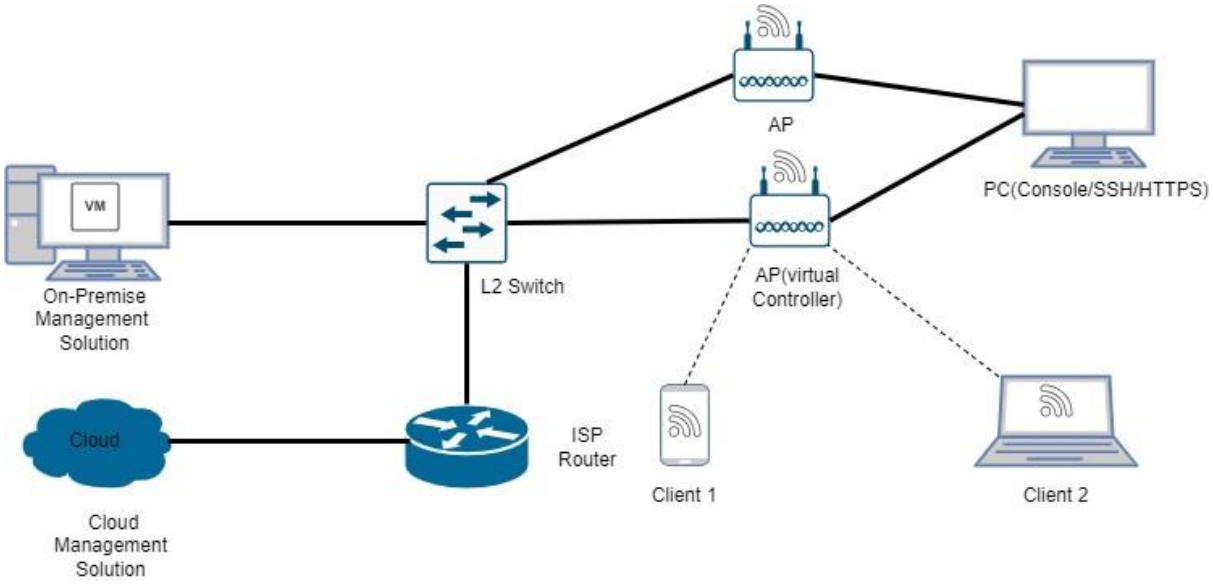
8.1.4. Secure traffic between AP and Controller (in case of split)(same procedure as explained above)

8.2. Test Bed Diagram



Note :. The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

8.3. Tools Required: - DUT , Wireshark

8.4. Test Execution Steps

- Tester shall check management protocols and cryptographic ciphers as per the OEM document.
- Tester shall capture the traffic on wireshark to check for the ciphers
- Tester shall attempt connection with weak/null ciphers
- Tester shall also follow the same test procedure for split mode/cloud managed/on-premise

9. **Expected Results for Pass:-** The DUT supports secure ciphers for the supported management protocols

10. **Expected Format of Evidence:** Screenshots of Terminal , pcap

11. **Test Execution:**

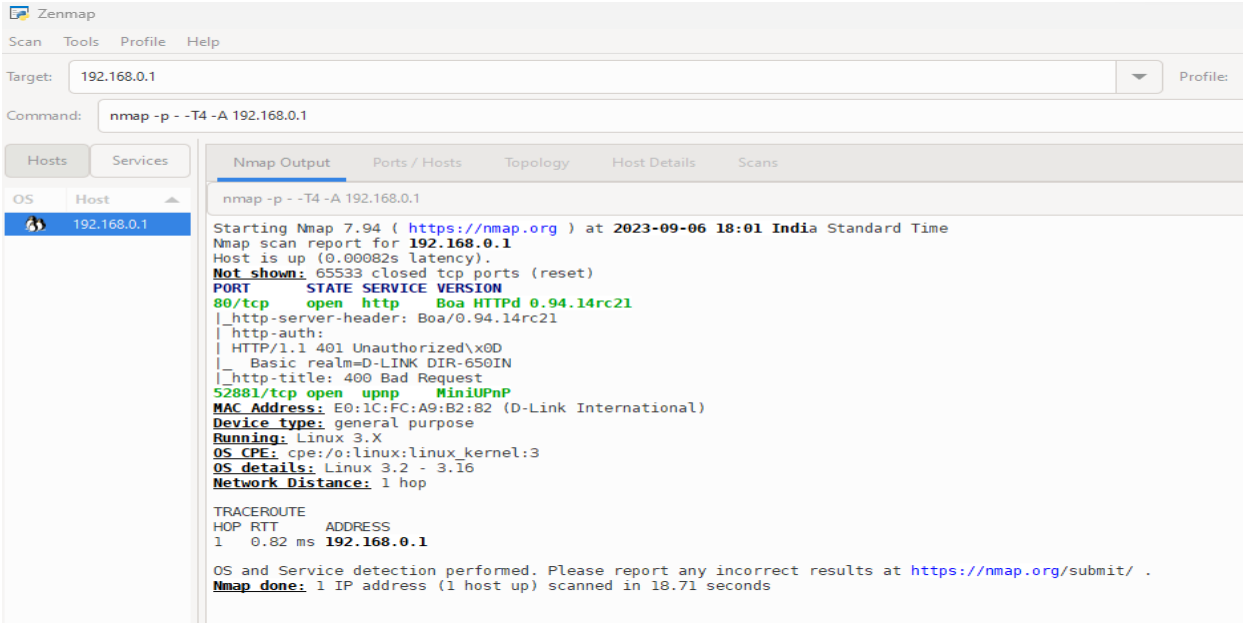
11.1 **Test Case Number:** 01

11.1.1 **Test Case Name:** Supported ciphers and management protocols

11.1.2 **Test Case Description:** The following testcase is done to check supported ciphers and management protocols as per the OEM document

11.1.3 **Execution Steps:**

Run zenmap for port scanning



<note ; NO OEM document available to check for secure ciphers>

11.2 **Test Case Number:** 02

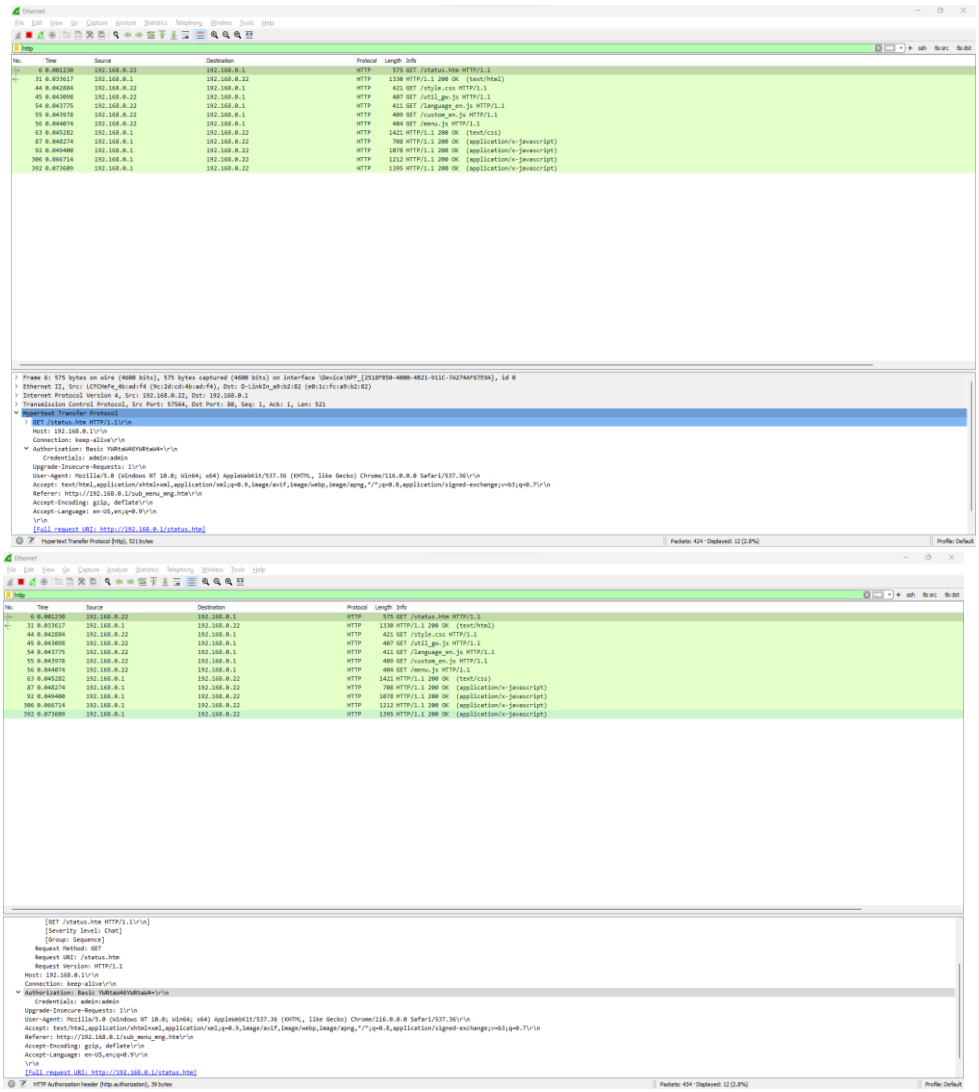
11.2.1 **Test Case Name:** Secure ciphers for HTTPS

11.2.2 **Test Case Description:** The following testcase is done to check for secure ciphers in HTTPS

11.2.3 **Execution Steps:**

- The Tester opens web browser in test machine (192.168.0.22) to connect DUT (https://192.168.0.1) through HTTP protocol
- The Tester attempts to login DUT using pre-defined “admin” account.
- The Tester supplies the correct password and reach to DUT’s web browser.
- The Tester attempt to customize dashboard and captured the network traffic between DUT and the Test machine in Wireshark.

- The Tester analyzed the Wireshark output and observed that traffic is going in unencrypted format on HTTP protocol.



11.2.4 **Test Observation:** - The Tester verified that the secure communication mechanism is not implemented for date transfer to and from the DUT

11.2.5 **Evidence provided**: - Screenshots above

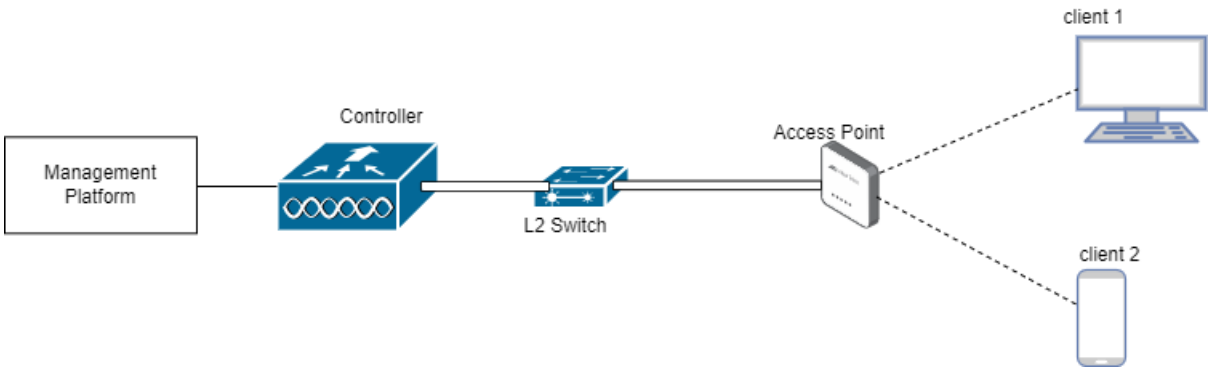
11.2.6 **Test Execution**:

11.3 **Test Case Number:** 03

11.3.1 **Test Case Name:** Secure traffic between Controller and AP

11.3.2 **Test Case Description:** The following testcase is done to check supported ciphers between AP and Controller (in case of split)

11.3.3 **Execution Steps:**



- The Tester shall refer the OEM documents to identify the management protocols running between AP and CONTROLLER
- The Tester shall configure the communication between AP and CONTROLLER
- The Tester shall capture the management traffic communication between AP and CONTROLLER using Wireshark and check for secure ciphers being used in traffic encryption

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Supported Secure ciphers		No OEM document available
2	Secure cipher HTTPS protocols	Pass	
3	Secure traffic between Controller and AP		Procedures explained

1.1.3 Role-Based Access Control

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.1: Access and Authorization**
2. **<Security Requirement No & Name > 1.1.3: Role-Based Access Control**
3. **<Requirement Description: > CPE** shall support Role-Based Access Control (RBAC) which provides at least two different access levels or domains to guarantee that individuals can only perform the operations that they are authorized for. The RBAC system controls how users are allowed access to the various domains and what type of operations.
4. **DUT Confirmation Details**:
5. **DUT Configuration:**
6. **Preconditions**
   - Documentation describing the role-based access control system including details on which user roles are defined.
   - Highest privilege user configured while initial set up and ensured that the tester has administrative i.e., read-write level access on DUT that all users with password authentications are configured.
7. **Test Objective: -** To check if roles based access control supported in the DUT
8. **Test Plan**

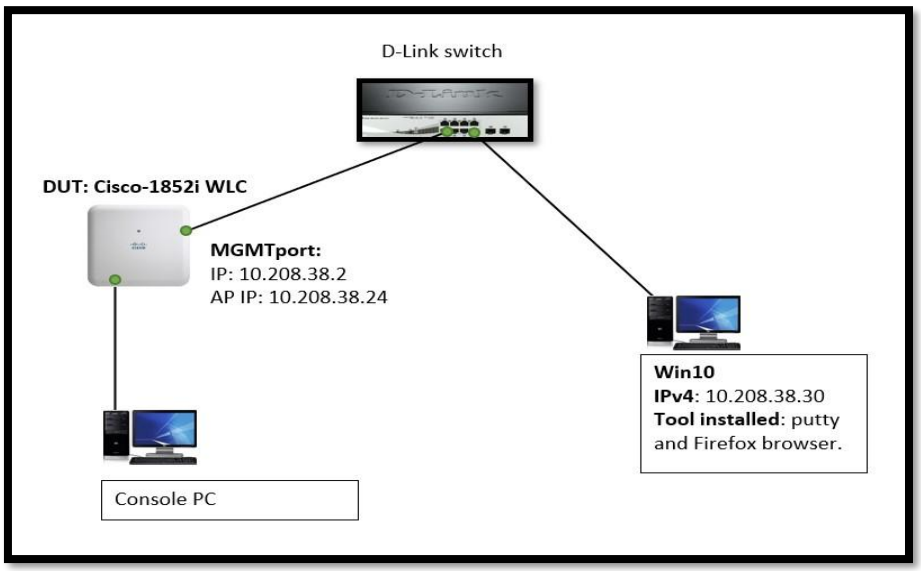
   8.1 Number of Test Scenarios:

   - CASE I: Creation of Read Only user type in DUT with an administrative account & Verification of the functionality supported by Read Only type.
   - CASE II: Creation of another Read/Write user type in DUT with an administrative account & Verification of the functionality supported by the Read/Write type.
   - CASE III: Creation of Lobby Ambassador user type in DUT with administrative account & Verification of the functionality supported by Lobby Ambassador type.

ON WEB-GUI

   - CASE IV: Creation of Read Only user type in DUT with the account user1 (read only type) logins on the web & verify the feature is not supportive.
   - CASE V: Creation of another Read/Write user type in DUT with user2 account (read/write type) logins & verify the user gets successfully created.
   - CASE VI: Creation of Lobby Ambassador user type in DUT with user4 account (lobby ambassador) & verify only the guest users get successfully created.

   8.2 Test Bed Diagram



- Test Tools:

DUT

8.3 Tools Required

- DUT,
- Wireshark

8.4 Test Execution Steps:- Tester shall attempt to test all the roles-based access supported in the DUT

9. **Expected Results for Pass:** The DUT supports secure ciphers for the supported management protocols
10. **Expected Format of Evidence:** Screenshots of Terminal, pcap
11. **Test Execution:**

11.1 **Test Case Number:** 01

11.1.1 **Test Case Name:** Read only user type

11.1.2 **Test Case Description:** Creation of Read Only user type in DUT with an administrative account & Verification of the functionality supported by Read Only type.

11.1.3 **Execution Steps:**

11.1.4 **Test Observation**: - The Tester verified that the secure communication mechanism is not implemented for date transfer to and from the DUT

11.1.5 Evidence provided: - Screenshots above

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Supported Secure ciphers		No OEM document available

1.1.4 User Authentication - Local/Remote

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.1**: **Access and Authorization**
2. **<Security Requirement No & Name > 1.1.4: User Authentication - Local/Remote**
3. **<Requirement Description: > Local**/Remote access to the CPE for configuration and maintenance purposes shall be granted only to authenticated users or machines using at least one authentication attribute. This authentication attribute when combined with the user's name shall enable unambiguous authentication and identification of the authorized user. No methods to exist providing authentication-bypass attacks to succeed under all combinations of interface / methods of authentication.
4. **DUT Confirmation Details**:

5. **DUT Configuration:**

6. **Preconditions**
   - The manufacturer shall supply the list of system functions which include network services, local access via a management console, local usage of operating system and applications.
   - The manufacturer shall supply the list of access entries for system functions

7. **Test Objective:-** To check if there is at least one authentication attribute to access the DUT

8. **Test Plan**
   8.1. Number of Test Scenarios:
   8.1.1. Test Scenario to check the authentication feature of the DUT (GUI)

   8.2. Test Bed Diagram

Tester machine
192.168.129.13

Wifi CPE
192.168.29.1

   8.3. Tools Required: - Only DUT needed
   8.4. Test Execution Steps

- The tester shall attempt to login into the DUT using its management interface (web GUI)
- The tester should check if any authentication attribute is checked before giving the access to the DUT

9. **Expected Results for Pass:** The DUT supports at-least one authentication attribute when attempting to access the DUT

10. **Expected Format of Evidence:** Screenshots of Terminal

11. **Test Execution:**

11.1 **Test Case Number:** 01

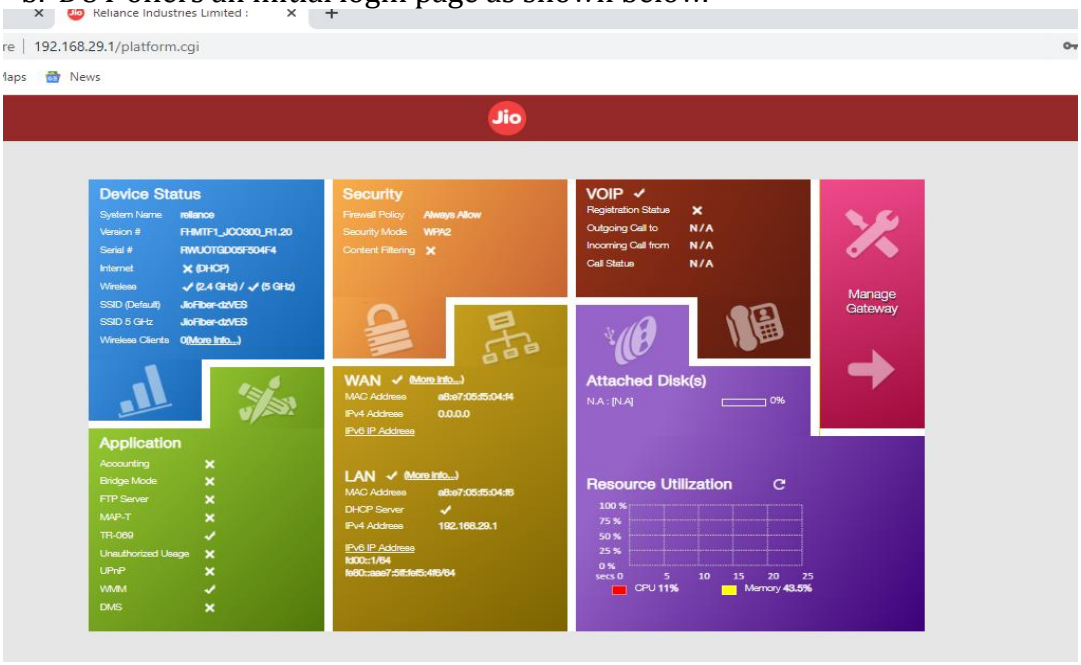
11.1.1 **Test Case Name:** Login with DUT's GUI

11.1.2 **Test Case Description:** The following testcase is done to login into the DUT to check for authentication attribute

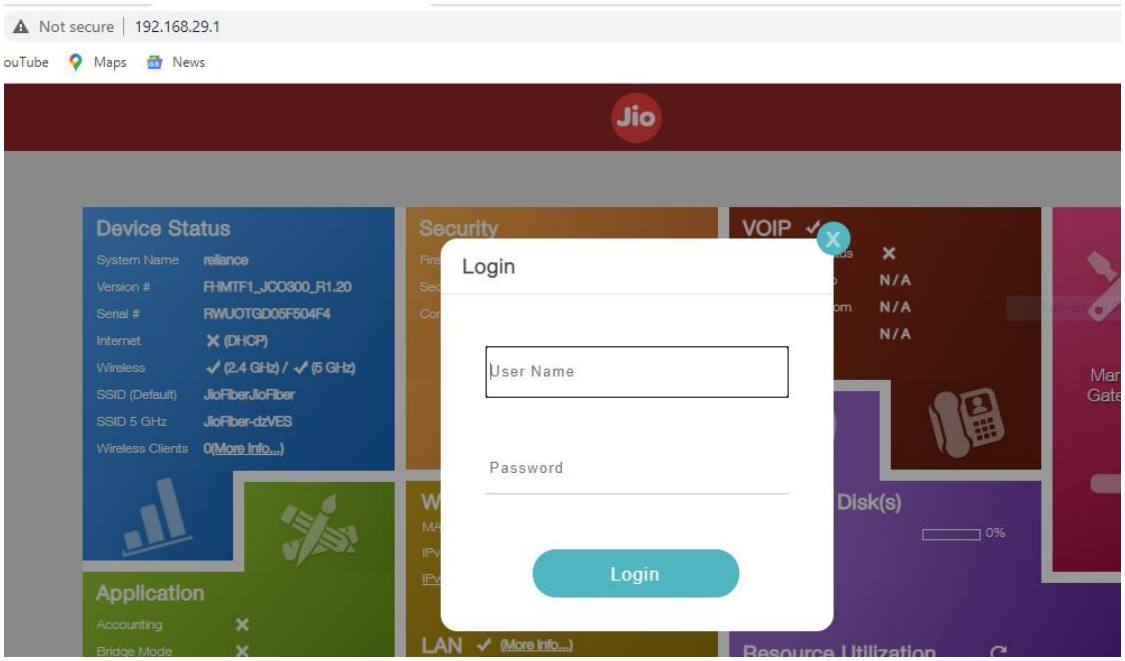
11.1.3 **Execution Steps:**

a. Access the web page of the DUT at 192.168.29.1

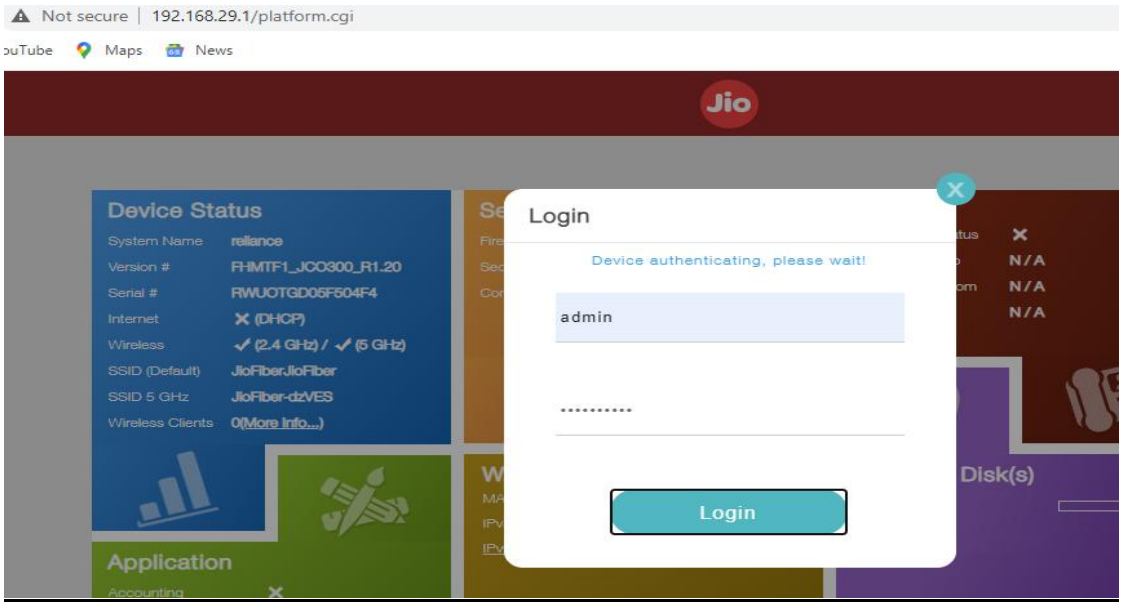
b. DUT offers an initial login page as shown below.



c. Click on the Manage gateway option for logging in to the Wi-Fi CPE modem. The login page as offered by Wi-Fi CPE modem will be prompting for a password in combination with username for logging in to the DUT.



d. The username and password are 'Admin' and 'Jiocentrum' respectively for the successful login. (as provided by the OEM)



11.1.4 **Test Observations:** It was observed that the tester attempting to login is asked for password authentication, upon which the tester gets the access to the DUT

11.1.5 **Evidence Provided: -** Screenshots of Terminal

12. **<u>Test Case Result:</u>**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Login to DUT (GUI)	Pass	

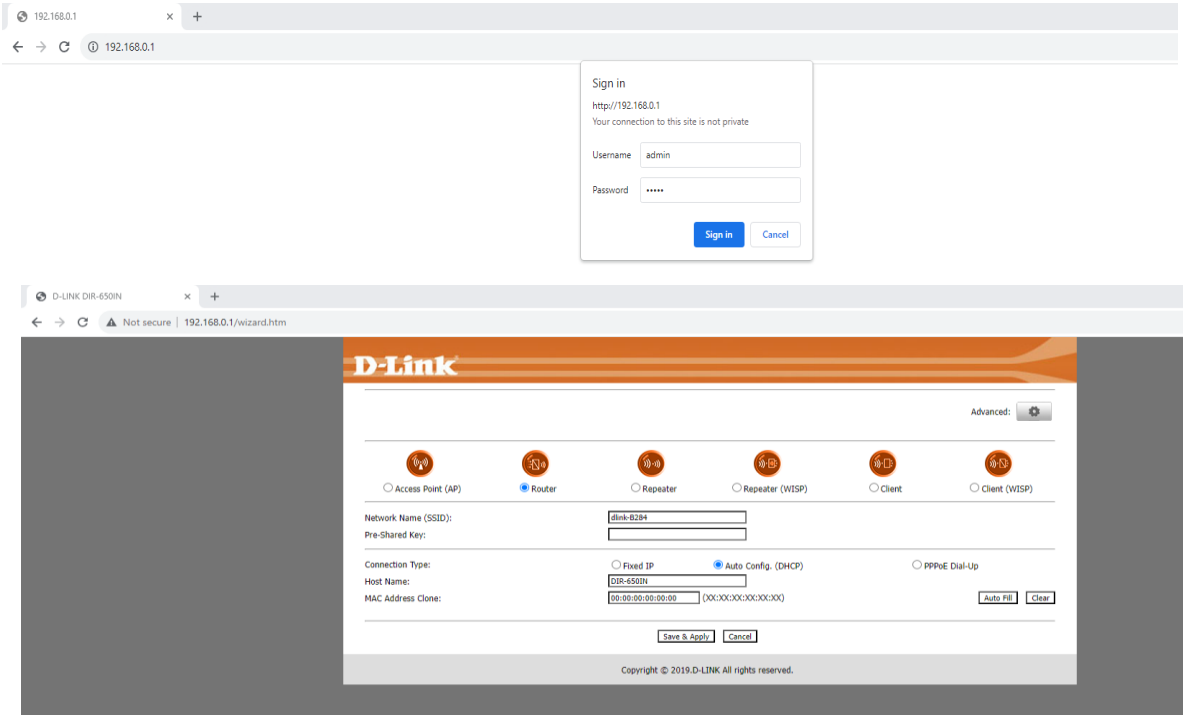
1.1.5 Remote Management Standards

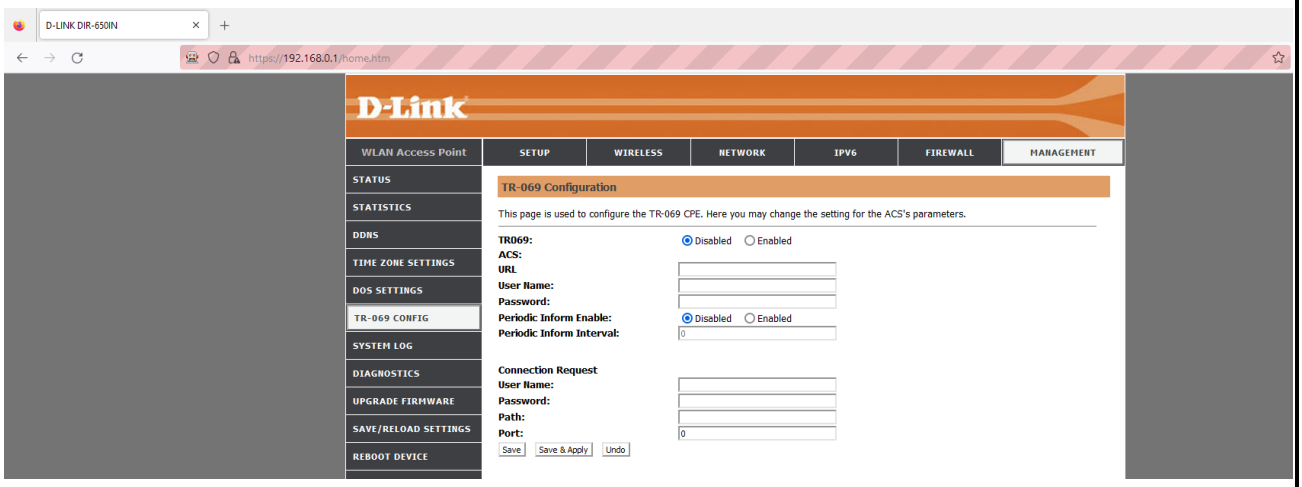
<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.1: Access and Authorization**
2. **<Security Requirement No & Name > 1.1.5: Remote Management Standards**
3. **<Requirement Description: >** The remote management mechanisms for CPE to be fully compliant with the remote management standards that the OEM chose to implement, example: TR-069 or any other relevant standards, such mechanisms to include entity mutual authentication, encryption of the management traffic.

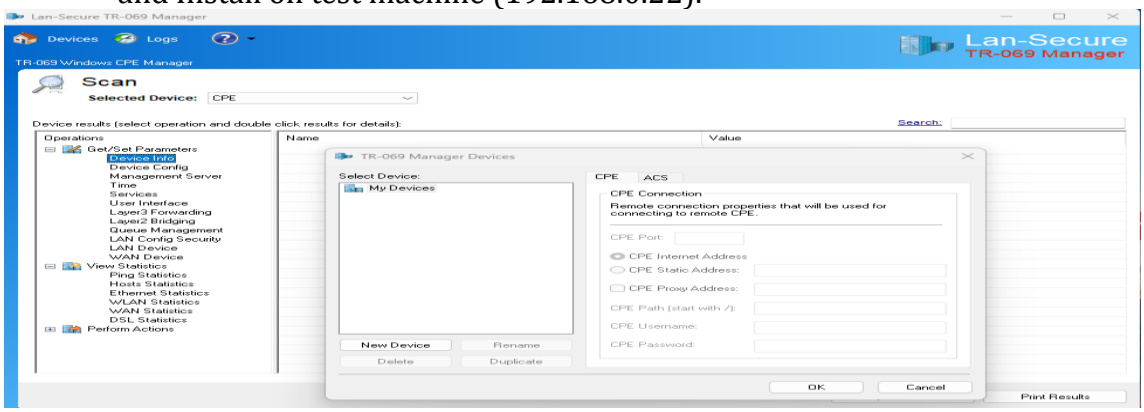
4. **DUT Confirmation Details**:

5. **DUT <u>Configuration:</u>** The tester shall login with physical console and configure TR-069 to remotely connect to DUT

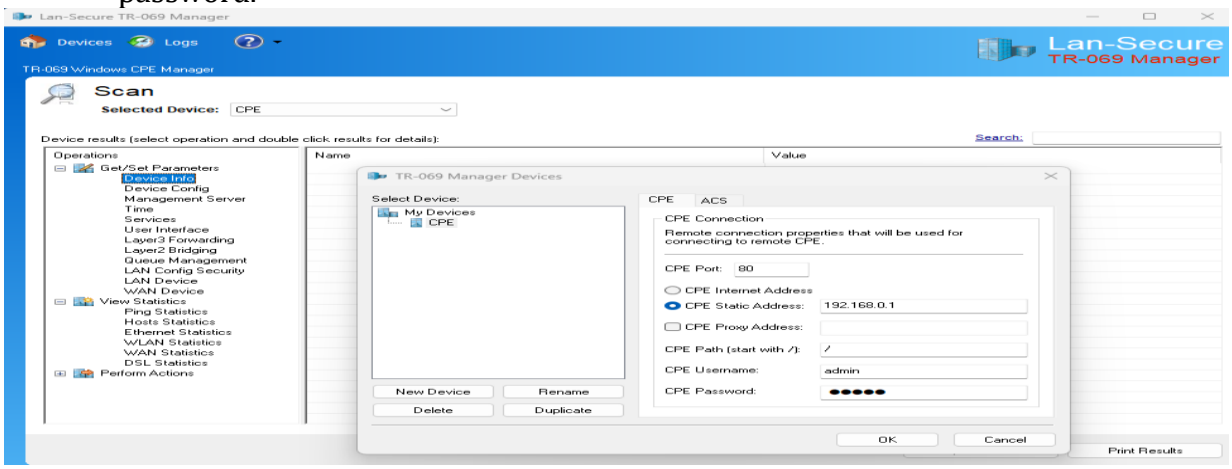




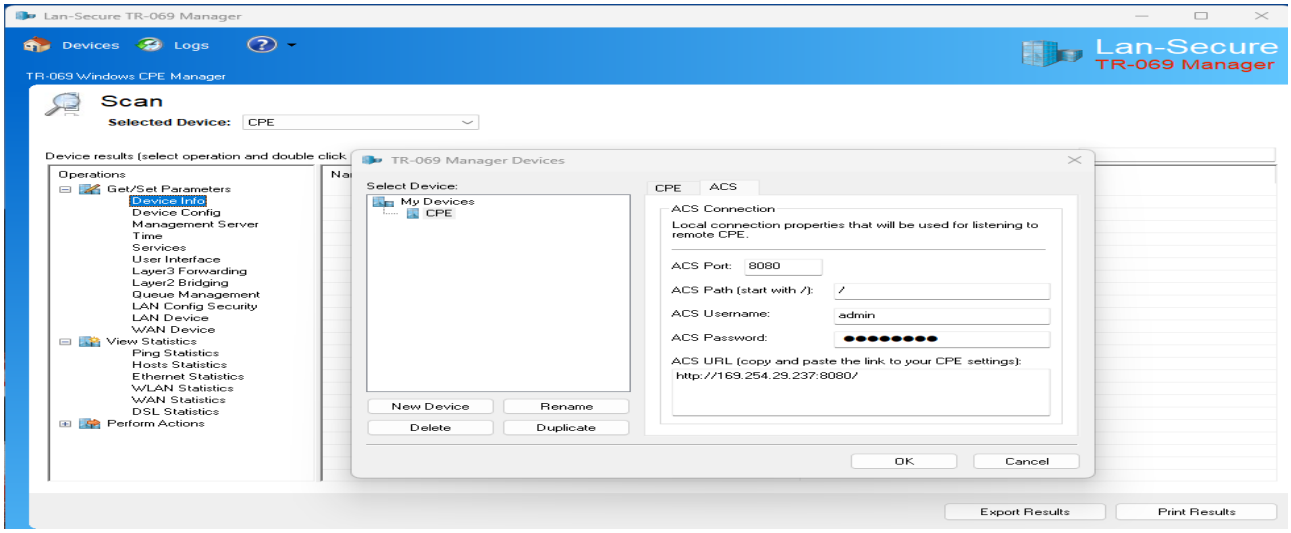
a. The Tester Download (https://www.lan-secure.com/TR-069-ACS-Windows.htm) and Install on test machine (192.168.0.22).

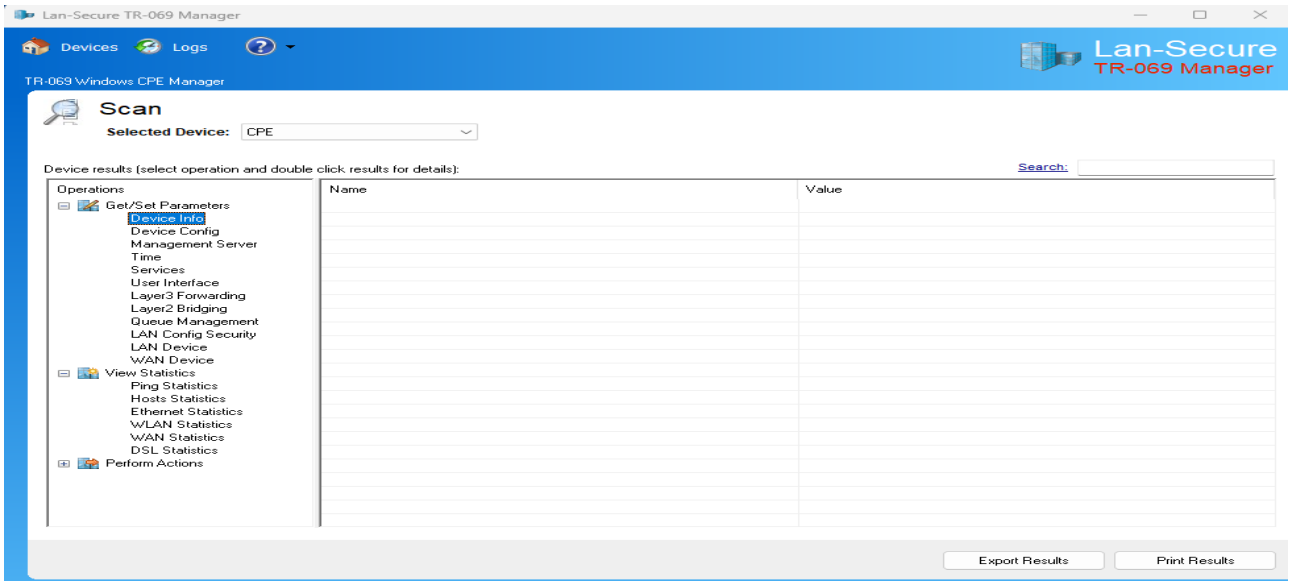


b. Tester filled CPE details such CPE Port, Static IP address , CPE path , username and password.

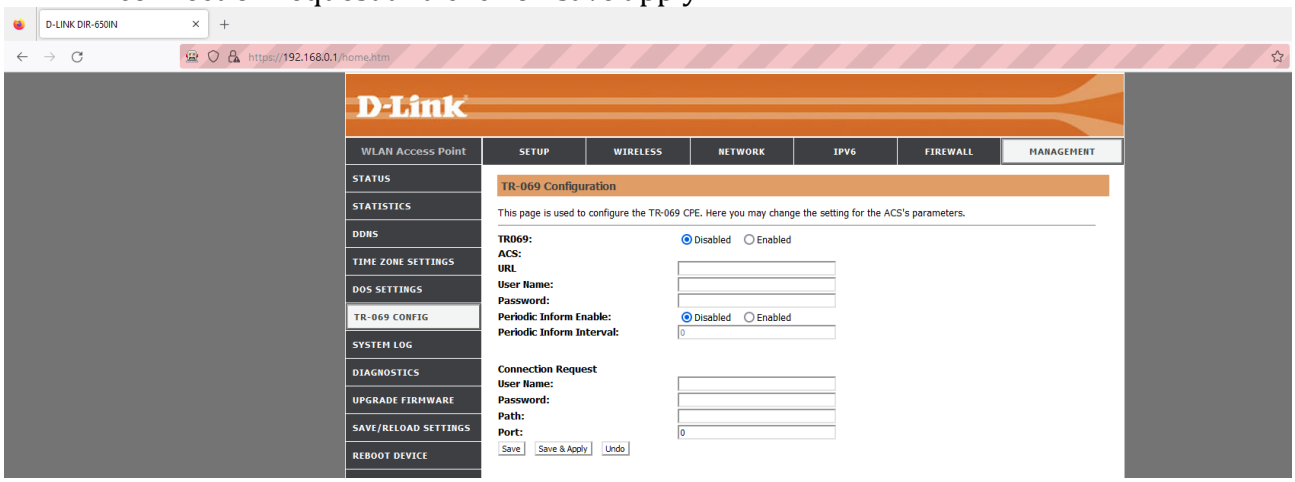


c. Tester filled ACS Details such ACS path, username, password and click on OK



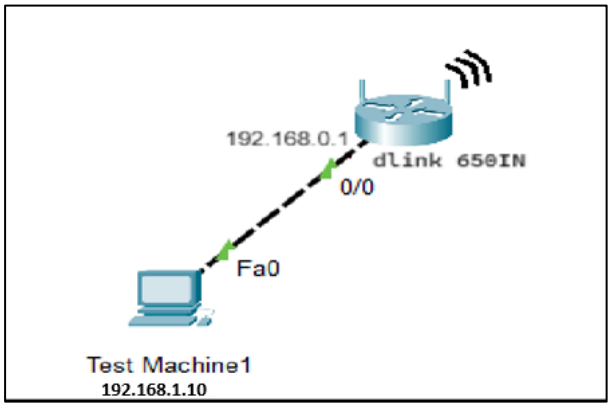


d. The Tester clicks on Management > TR-069 config and fill details ACS and connection request and click on save apply.



6. **Preconditions: -** OEM shall provide details of all DUT supporting TR-069 configuration
7. **Test Objective: -** To check if there is mutual authentication supported on remote interface connection to DUT

8. **Test Plan**
   - 8.1. Number of Test Scenarios:
   - 8.1.1. Test Scenario to check the mutual authentication is supported on the remote interface connection to DUT
   - 8.2. Test Bed Diagram



8.3. Tools Required

- DUT ,
- Wireshark

8.4. Test Execution Steps:- The tester shall attempt connection between TR-069 client and DUT to remotely connect to DUT and simultaneously capture the traffic on wireshark.

9. **Expected Results for Pass:** The DUT supports mutual authentication for the remote interface connection
10. **Expected Format of Evidence:** Screenshots of Terminal

11. **Test Execution:**

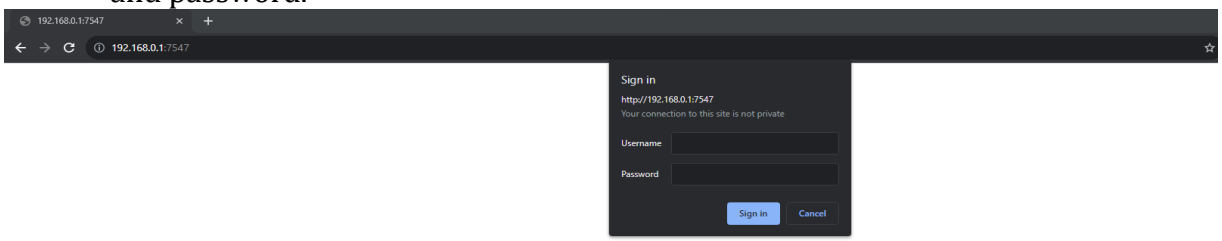
11.1 **Test Case Number:** 01

11.1.1 **Test Case Name:** Mutual authentication on remote interface(TR-069 connection)

11.1.2 **Test Case Description:** The following testcase is done to check if DUT supports mutual authentication for the remote interface connection

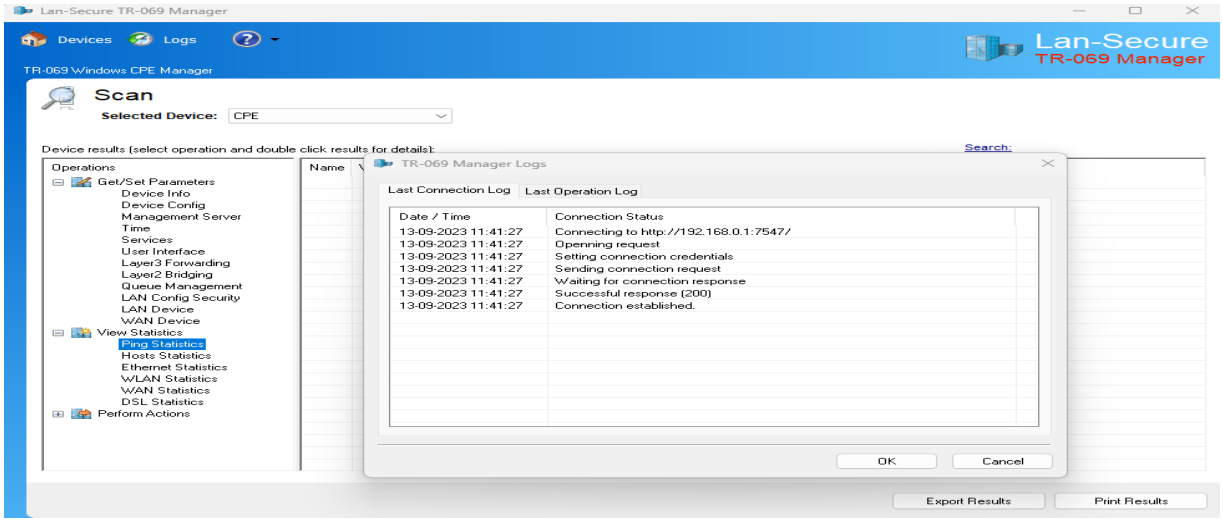
11.1.3 **Execution Steps:**

a. The Tester visit http://192.168.0.1:7547/ and login with username “admin” and password.

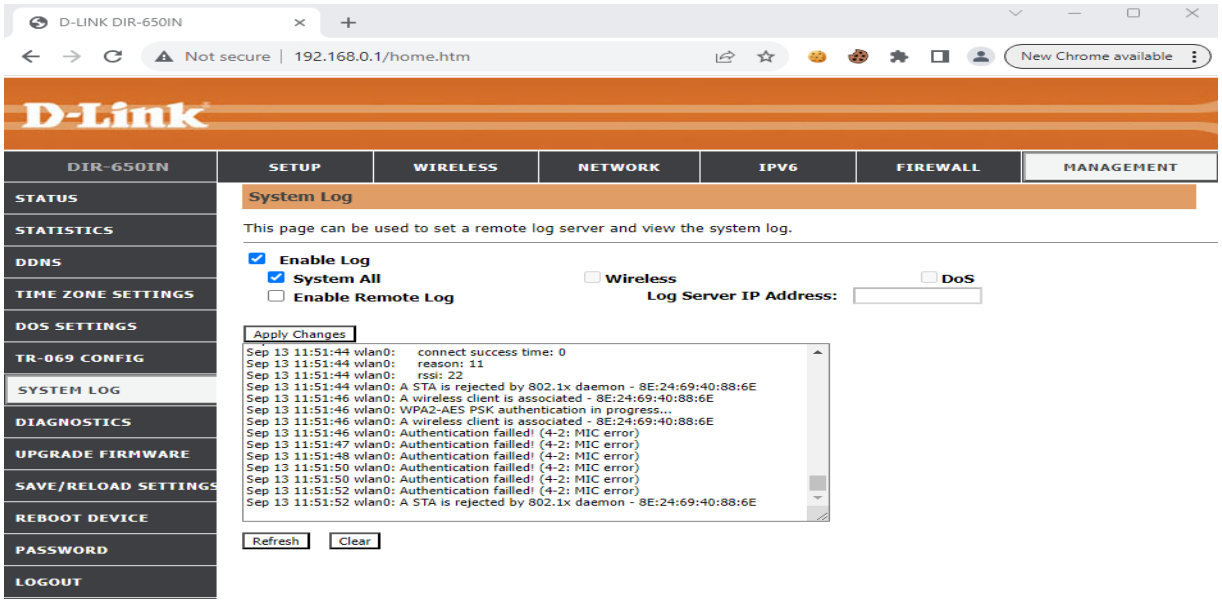


b. Tester verify TR-069 log and DUT log details.

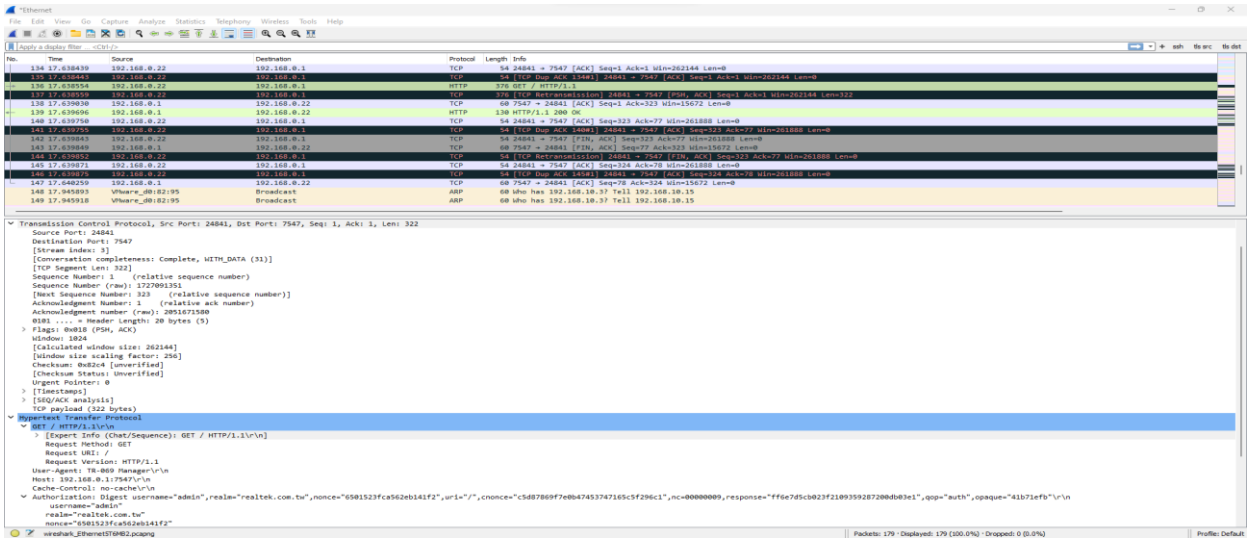
TR-069 log



DUT log



c. The Tester captured network traffic using Wireshark.



11.1.4 **Test Observations:** The Tester observed that there was NO mutual authentication or encryption of the management traffic between the DUT and connected entities remotely.

11.1.5 **Evidence Provided**: - Screenshots of Terminal

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Mutual Authentication on remote	Fail	

1.1.6 Remote Management Standards for Connected Devices, Additional Features

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.1: Access and Authorization**
2. **<Security Requirement No & Name > 1.1.6:** Remote Management Standards for Connected Devices, Additional Features
3. **<Requirement Description: >** The remote management mechanisms for devices connected to CPE, or for configuration of additional features of CPE like DDNS, UPnP etc., are to be compliant with the respective. Latest standards published at the time of commencement of security testing. These additional features are to be configured as disabled in the factory default settings, with provision for user to enable individual features on menu-selection. Such mechanisms to include entity mutual authentication, encryption of the management traffic

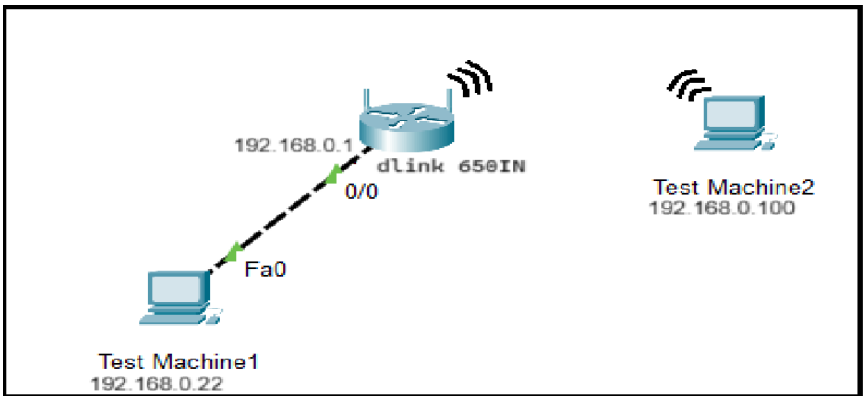
4. **DUT Confirmation Details**:

5. **DUT Configuration:**

6. **Preconditions**
   - Documentation describing the remote management defined for the system including configuration of additional features of CPE like DDNS, UPnP etc
   - OEM shall provide confirmation that additional features such as DDNS, UPnP etc. are configured as disabled in the factory default settings, with provision for user to enable individual features on menu-selection.
7. **Test Objective:-** To check if there is mutual authentication supported on remote interface connection to DUT

8. **Test Plan**
   8.1. Number of Test Scenarios:
   - 8.1.1 test shall review the OEM documentation which describes the availability of additional features such as DDNS, UPnP available on DUT.
   - 8.1.2 The Tester shall verify that DDNS, UPnP mechanisms include entity mutual authentication, encryption of the management traffic.

8.2. Test Bed Diagram



8.3. Tools Required

- DUT ,
- Wireshark

8.4. Test Execution Steps

9. **Expected Results for Pass:** The DUT supports mutual authentication for the remote interface connection
10. **Expected Format of Evidence:** Screenshots of Terminal

11. **Test Execution:**

11.1 **Test Case Number:** 01

11.1.1 **Test Case Name:** Review the OEM document to check additional features.

11.1.2 **Test Case Description:** This test shall review the OEM documentation which describes the availability of additional features such as DDNS, UPnP available on DUT.

11.1.3 **Execution Steps:**

i. At this stage OEM document is not available with the TSTL so this cannot be verified at this stage.
ii. The document available in the public domain confirms the availability of the features like DDNS and UPnP.

11.1.4 **Test Observations:** The tester reviewed the document available in the public domain confirms the availability of the features like DDNS and UPnP.

11.1.5 **Evidence Provided: -** None

11.2 **Test Case Number:** 02

11.2.1 **Test Case Name: -** Check the mutual authentication, encryption of the management traffic

11.2.2 **Test Case Description:** The Tester shall verify that DDNS, UPnP mechanisms

include entity mutual authentication, encryption of the management traffic

11.2.3 **Execution Steps:**

a. At this stage OEM document is not available with the TSTL to confirm that whether these service supports mutual authentication or not.

11.2.4 **Test Observation: -** The tester reviewed the document available in the public domain confirms the availability of the features like DDNS and UPnP.

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Review the OEM document to check additional features.		
2	Check the mutual authentication, encryption of the management traffic		

1.1.7 Unambiguous identification of the user & group

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.1: Access and Authorization**
2. **<Security Requirement No & Name > 1.1.7 Unambiguous identification of the user & group**
3. **<Requirement Description: > The** CPE shall identify each login user unambiguously. CPE shall be able to assign individual accounts per user, where a user could be a person, or, for Machine Accounts, an application, or a system. It is a desirable feature to configure user preferred USERID name in configuration menu instead of pre-configured ADMIN User ID. Use of group accounts or group credentials or sharing of the same account between several users shall not be enabled by CPE
4. **DUT Confirmation Details**:
5. **DUT Configuration:**
6. **Preconditions**

8.1.1 OEM shall provide all predefined accounts available on DUT as categorized below–

6.1.1 Machine Accounts: These will be used for authentication and authorization from system to system or between applications on a system and cannot be assigned to a single person or a group of persons.

6.1.2 Local access: The access from Console interface, from local Console network, from LMT (Local Maintenance Terminal interface) or from DUT local hardware interface.

6.1.3 Remote access: The access which is not Local access. This includes access from the EMS (Element Management System) network, and access that originates or passes through the internet.

8.1.2 OEM shall share configuration document to define unique identification (UID) to each user accounts.

7. **Test Objective: -** To check if the DUT can unambiguously identify individual accounts per user

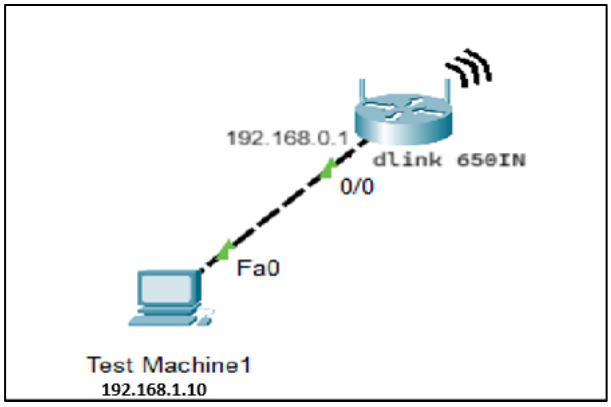
8. **Test Plan**

8.1. Number of Test Scenarios:

8.1.1 Test Scenario to check the multiple user account creation with existing user name

8.1.2 Test case to verify the AAA support
8.1.3 Test case to create a multiple user (duplicate user id)
8.1.4 Test Case to check concurrent session
8.1.5 Test Case to verify unique user ids assigned to user accounts

8.2. Test Bed Diagram



8.3. Tools Required

- DUT,
- Wireshark,
- Burp suite

8.4. Test Execution Steps:- The tester shall perform tests with duplicate usernames, duplicate user ids to prove the unambiguous identification of user accounts

9. **Expected Results for Pass:** The DUT supports the unambiguous identification of user accounts

10. **Expected Format of Evidence:** Screenshots of Terminal

11. **Test Execution:**

11.1 **Test Case Number:** 01

11.1.1 **Test Case Name:** multiple user account creation with existing user name

11.1.2 **Test Case Description:** The following testcase is done to check if DUT supports: multiple user account creation with existing user name

11.1.3 **Execution Steps:**

- The tester observed that CPE doesn't support multiple user accounts. It uses only one user account. Hence, ambiguity cannot be verified.

11.1.4 **Test Observations:** The tester observed that CPE doesn't support multiple user accounts. It uses only one user account. Hence, ambiguity cannot be verified

11.1.5 **Evidence Provided: -** Screenshots

11.2 **Test Case Number:** 02

11.2.1 **Test Case Name:** verify the AAA support

11.2.2 **Test Case Description:** The DUT may support independent user data bases for different access methods, e.g., one database for command shell access on OS level and another data base for GUI access. User data bases may be stored locally on the network product or on a central AAA system that the network product accesses for user authentication.

11.2.3 **Execution Steps:**

i. The Tester observed that DUT have one database for command shell access on OS level (user Id : root) and another data base for GUI access (user Id : admin).

11.2.4 **Test Observation: -** The Tester observed that DUT does not have mechanisms of central AAA system.

11.2.5 **Evidence provided: -** Screenshots

11.3 **Test Case Number:** 03

11.3.1 **Test Case Name:** Creation of multiple user and User ID verification

11.3.2 **Test Case Description:** The Tester shall verify that system should not allow creation of duplicate user IDs..

11.3.3 Execution steps:

11.3.4 **Test Observation:** Tester The Tester observed that in DUT there is no user creation feature.

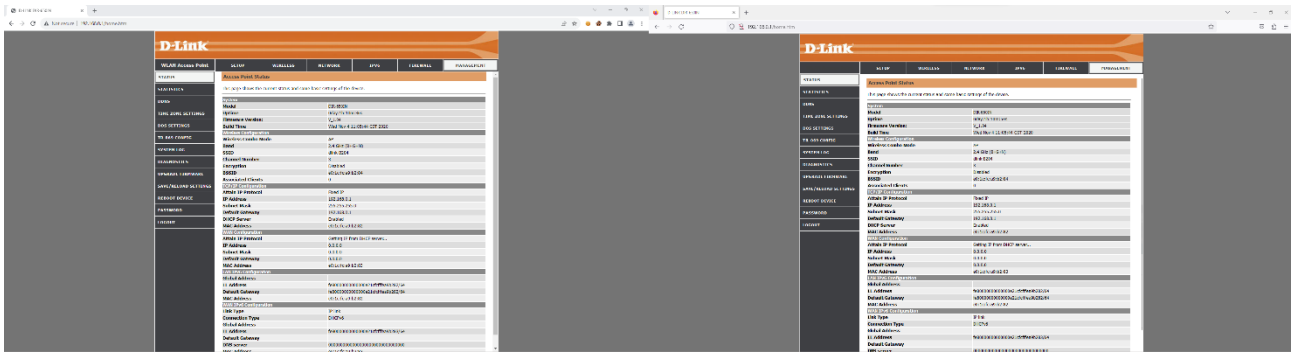
11.4 **Test Case Number:** 04

11.4.1 **Test Case Name**: Checking user concurrent sessions

11.4.2 **Test Case Description**: The Tester shall verify that simultaneous login is restricted to one session per user ID (concurrent sessions

11.4.3 **Execution Steps**

a. The Tester login simultaneous two different browser with user “admin”.



11.4.4 **Test Observation:** Tester Observed that the DUT is accepting multiple sessions with the same user or allows concurrent sessions.

11.5 **Test Case 05**

11.5.1 **Test case Name**: unique UIDs are assigned for each account.

11.5.2 **Test Case Description**: The Tester shall verify that unique UIDs are assigned for each account.

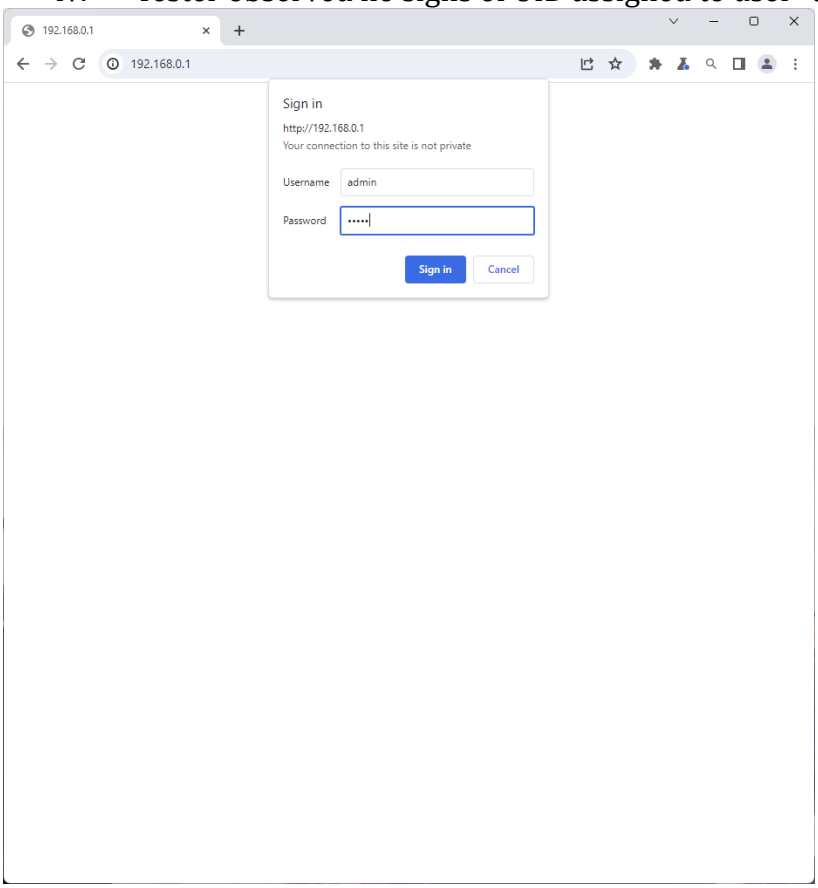
- Tool Used**:**
  - i. Burp suite

11.5.3 **Execution Steps:**

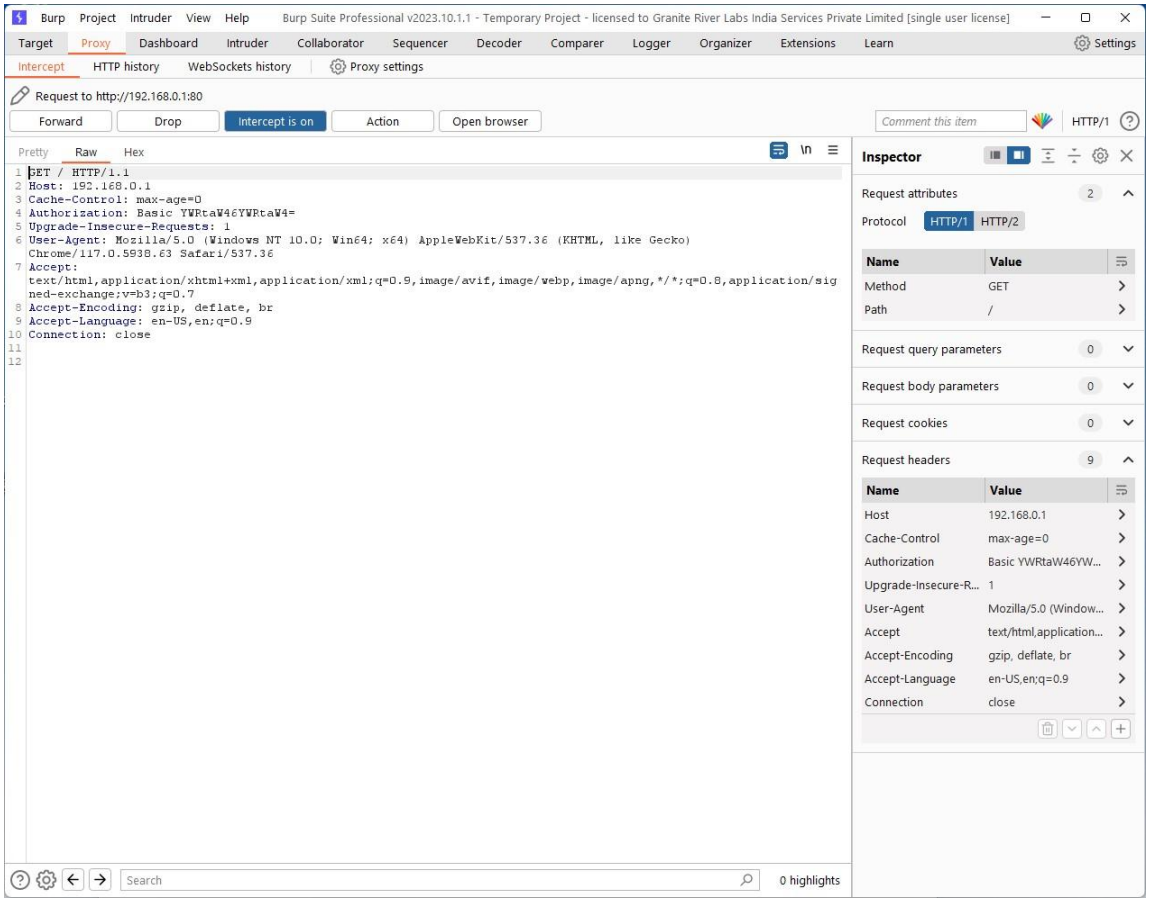
ii. Tester uses Burp suite to intercept the traffic during login via web browser.

iii. Tester login with default username and password, and intercepted immediate responses from CPE.

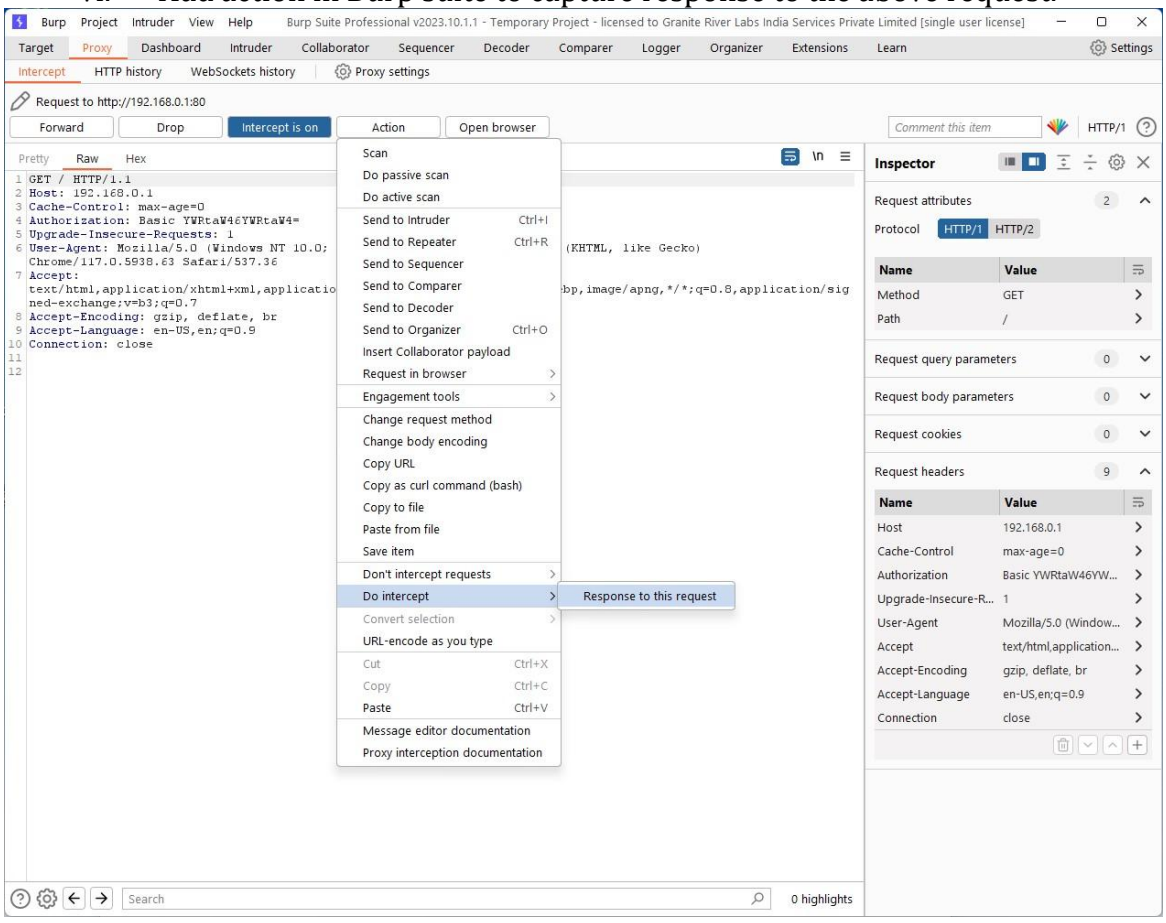
iv. Tester observed no signs of UID assigned to user “admin”



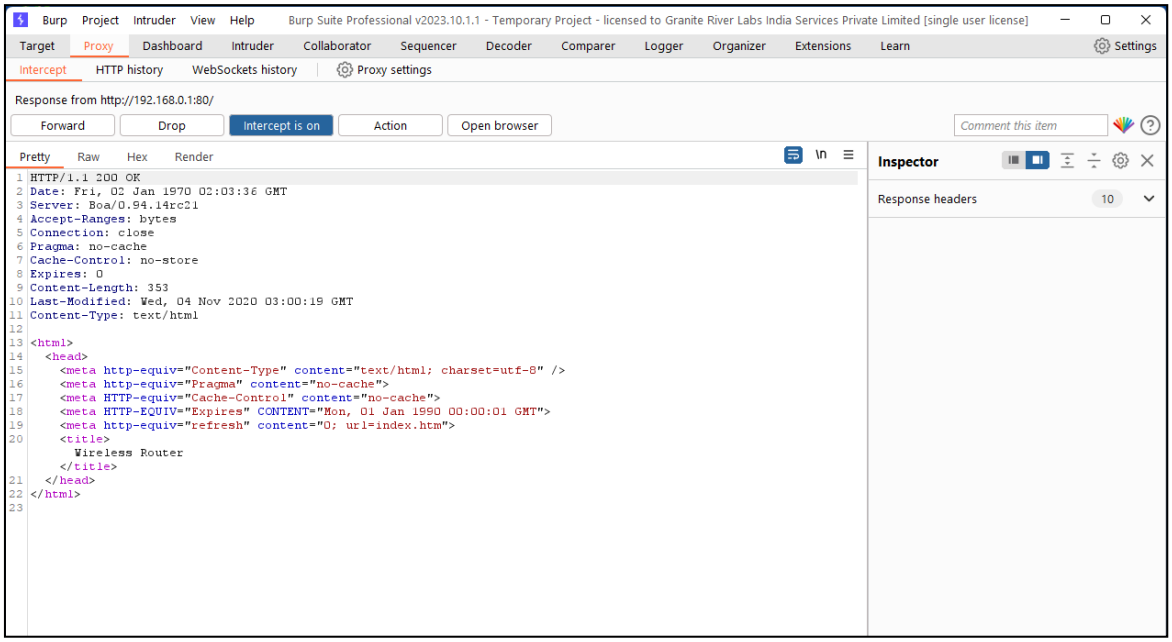
v. Intercepted request from browser to CPE.



vi. Add action in Burp suite to capture response to the above request.



vii. Response from the router is observed in HTML format without any identification of user UID.



11.5.4 **Test Observation:** Tester observed that the DUT is not assigning any user ID to the user admin.

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	multiple user account creation with existing user name		No feature exists of multiple account creation
2	verify the AAA support		No feature for AAA support
3	multiple user (duplicate user id)		No feature for multiple user creation
4	verify unique user ids assigned to user accounts	Pass	Not assigning any user id

Section 1.2: Authentication and Attribute Management

1.2.1 Authentication Policy

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.2** Authentication **and Attribute Management**
2. **<Security Requirement No & Name > 1.2.1: Authentication Policy**
3. **<Requirement Description: >** The usage of a system functions such as network services (like SSH, SFTP, Web services), management access, local usage of operating systems and applications shall be allowed only after successful authentication on the basis of the user identity and at least one authentication attribute (e.g., password, certificate). This requirement shall also be applied to accounts that are only used for communication between systems.

4. **DUT Confirmation Details**:

5. **DUT Configuration:**

6. **Preconditions**
   - The manufacturer shall supply the list of system functions which include network services, local access via a management console, local usage of operating system and applications.
   - The manufacturer shall supply the list of access entries for system functions
7. **Test Objective:-** To check if there is at least one authentication attribute to access the DUT

8. **Test Plan**
   - 8.1. Number of Test Scenarios:
     - 8.1.1. Test Scenario to check the authentication feature of the DUT (GUI)
   - 8.2. Test Bed Diagram

Tester machine
192.168.129.13

Wifi CPE
192.168.29.1

8.3. Tools Required

- Only DUT needed

8.4. Test Execution Steps

- The tester shall attempt to login into the DUt usin its management interface(web GUI)
- The tester should check if any authentication attribute is checked before giving the access to the DUT

9. **Expected Results for Pass:** The DUT supports at- least one authentication attribute when attempting to access the DUT

10. **Expected Format of Evidence:** Screenshots of Terminal

11. **Test Execution:**

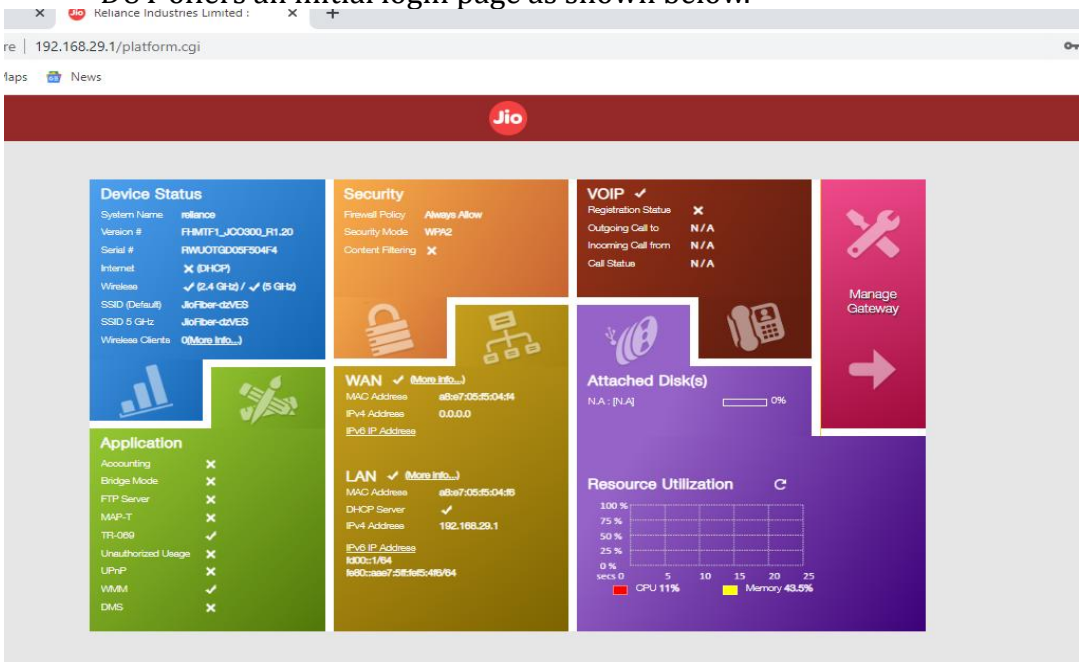
11.1 Test Case Number: 01

11.1.1 **Test Case Name:** Login with DUT's GUI

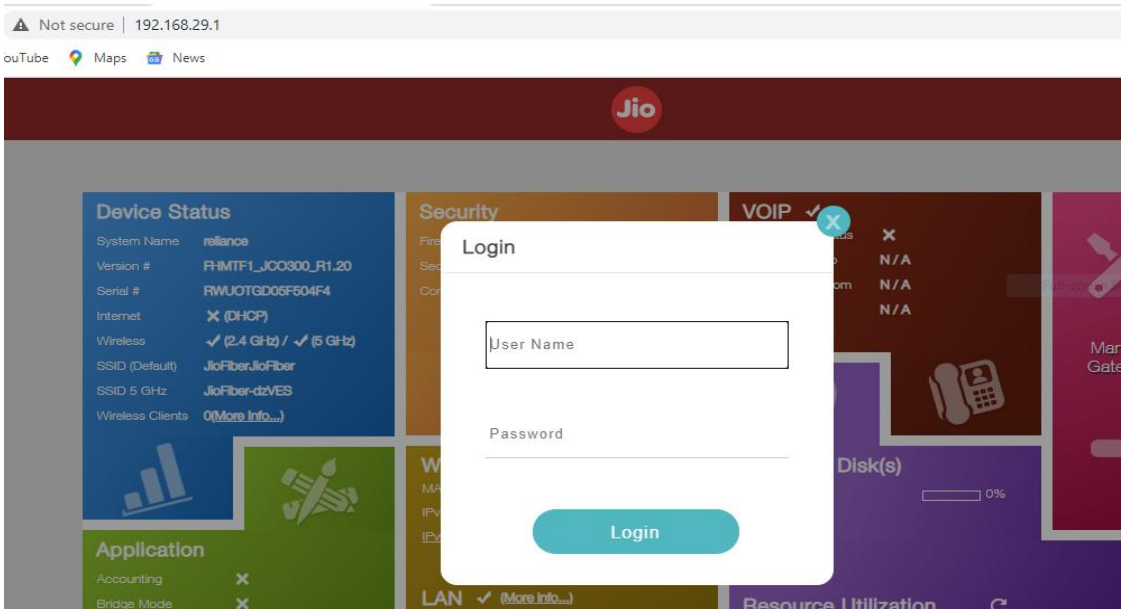
11.2.2 **Test Case Description:** The following testcase is done to login into the DUT to check for authentication attribute

11.2.3 **Execution Steps:**

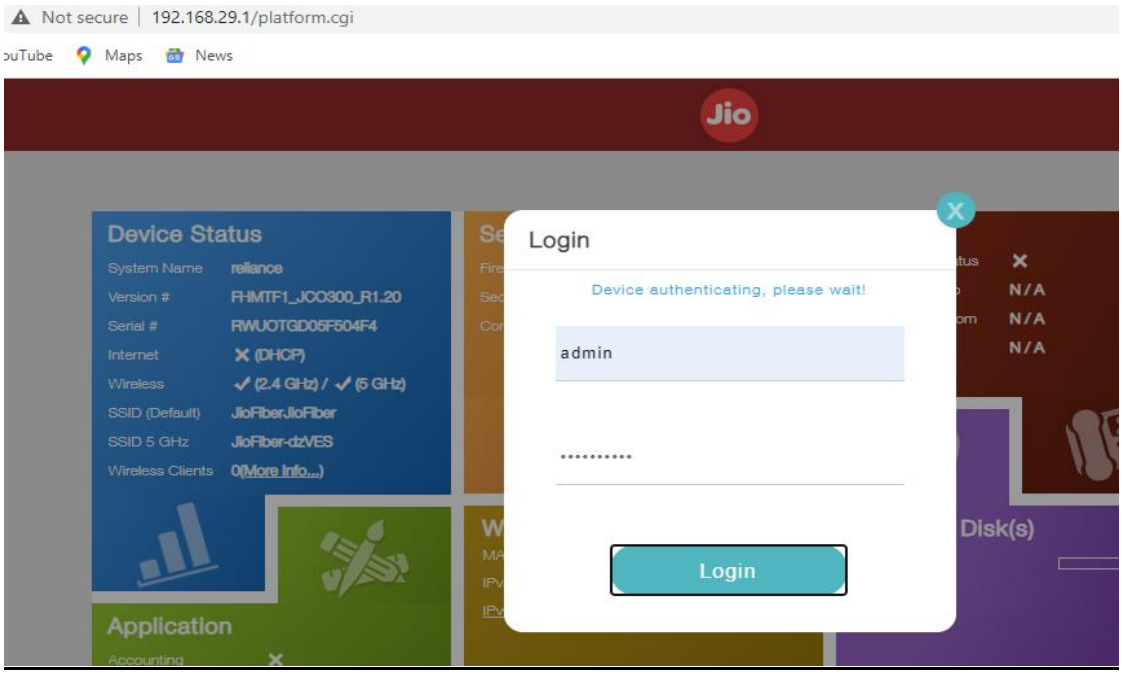
- Access the web page of the DUT at 192.168.29.1
- DUT offers an initial login page as shown below.



- Click on the Manage gateway option for logging in to the Wi-Fi CPE modem. The login page as offered by Wi-Fi CPE modem will be prompting for a password in combination with username for logging in to the DUT.



- The username and password are 'Admin' and 'Jiocentrum' respectively for the successful login. (as provided by the OEM)



11.2.4 **Test Observations:** It was observed that the tester attempting to login is asked for password authentication, upon which the tester gets the access to the DUT

11.2.5 **Evidence Provided: -** Screenshots of Terminal

12. **<u>Test Case Result:</u>**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Login to DUT (GUI)	Pass	

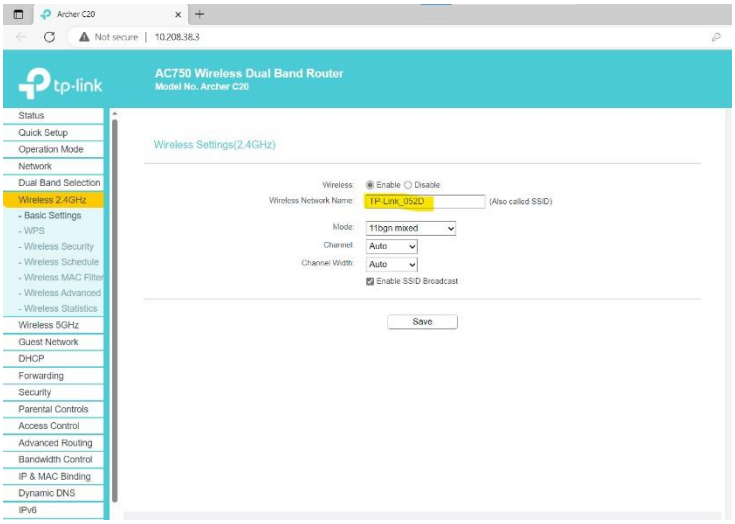
1.2.2 Authentication Support - External

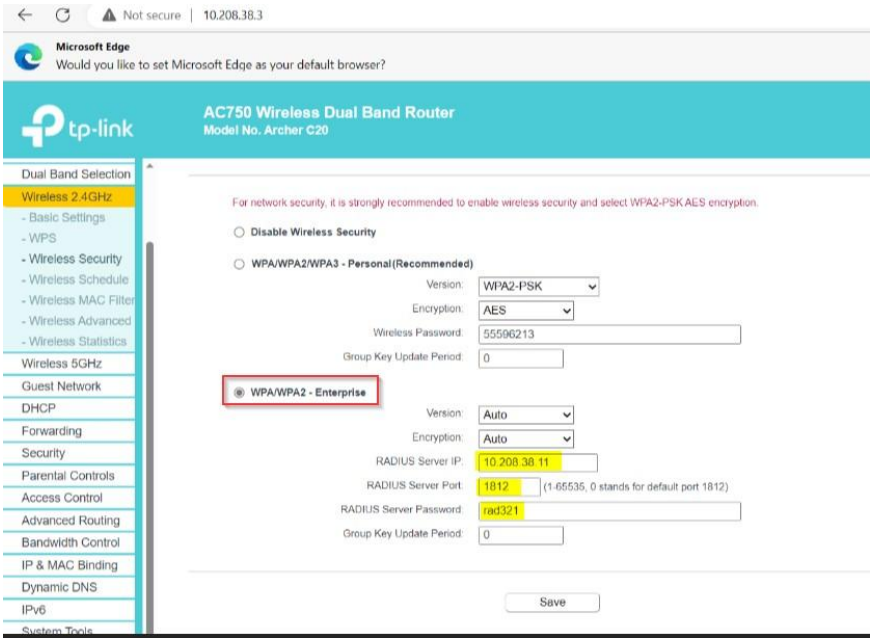
<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.2 Authentication and Attribute Management**

2. **<Security Requirement No & Name > 1.2.2: Authentication Support - External**
3. **<Requirement Description: >** If CPE supports external authentication (for the Cyber-Cafe use-case scenario), the user authentication credentials should be protected and securely communicated if the authentication credentials are managed by external authentication servers
4. **DUT Confirmation Details**:

5. **<u>DUT Configuration:</u>** Verify the configurations of the DUT for authentication and authorization using the radius server.





Verify the configurations of the radius server.

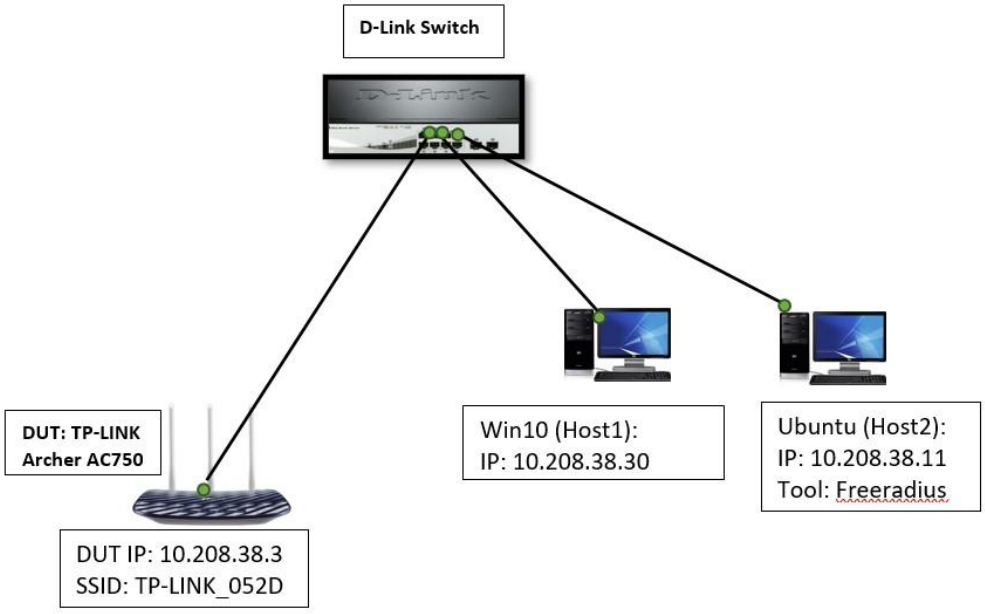
- Check the configurations of the clients. conf file to identify the hostname and shared secret:

The above screenshot shows the configured hostname and shares secret key 'rad321'.

o Check the "user" file to check the configurations file for allowed user to access the device.

The above screenshot shows the configured users in the user file of radius server to perform authentication and authorization.

6. **Preconditions:-** Documentation from vendor stating whether DUT utilizes External authentication server for its operation.
7. **Test Objective:**- To check if external authentication supported by DUT is secure or not
8. **Test Plan**
   - 8.1. Number of Test Scenarios:
     - 8.1.1. Test Scenario to check communication channel between external authentication server and DUT is encrypted.
   - 8.2. Test Bed Diagram



8.3. Tools Required

- DUT , freeradius

8.4. Test Execution Steps

- The tester shall attempt to login into the DUt using its management interface(web GUI)
- The tester should check if any authentication attribute is checked before giving the access to the DUT

9. **Expected Results for Pass:** The DUT supports secure communication with external authentication

10. **Expected Format of Evidence:** Screenshots of pcap

11. **Test Execution:**

11.1 Test Case Number: 01

11.1.1 **Test Case Name:** Secure communication of external authentication

11.1.2 **Test Case Description:** Verifying if communication channel between external authentication server and DUT is encrypted

11.1.3 **Execution Steps:**

- Check the freeradius server service status

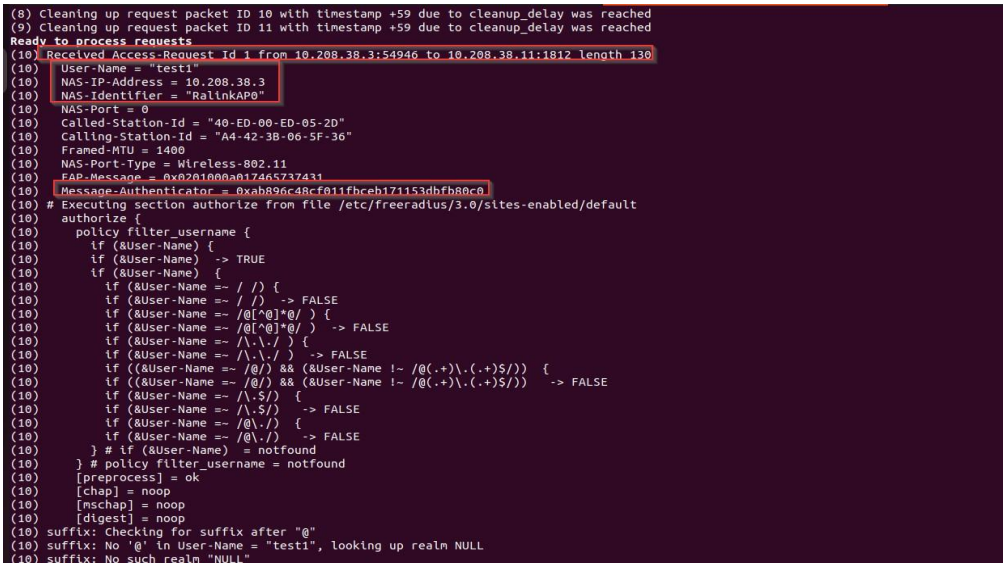
```
root@APMUMCSAE002D:/etc/freeradius/3.0# systemctl status freeradius service
Unit service.service could not be found.
● freeradius.service - FreeRADIUS multi-protocol policy server
     Loaded: loaded (/lib/systemd/system/freeradius.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-08-16 14:46:00 IST; 57s ago
       Docs: man:radiusd(8)
             man:radiusd.conf(5)
             http://wiki.freeradius.org/
             http://networkradius.com/doc/
    Process: 513279 ExecStartPre=/usr/sbin/freeradius $FREERADIUS_OPTIONS -Cx -lstdout (code=exited, status=0/SUCCESS)
   Main PID: 513280 (freeradius)
     Status: "Processing requests"
      Tasks: 6 (limit: 4600)
     Memory: 78.6M (limit: 2.0G)
        CPU: 427ms
     CGroup: /system.slice/freeradius.service
             └─513280 /usr/sbin/freeradius -f

Aug 16 14:45:59 APMUMCSAE002D freeradius[513279]: Compiling Auth-Type PAP for attr Auth-Type
Aug 16 14:45:59 APMUMCSAE002D freeradius[513279]: Compiling Auth-Type CHAP for attr Auth-Type
Aug 16 14:45:59 APMUMCSAE002D freeradius[513279]: Compiling Auth-Type MS-CHAP for attr Auth-Type
Aug 16 14:45:59 APMUMCSAE002D freeradius[513279]: Compiling Autz-Type New-TLS-Connection for attr Autz-Type
Aug 16 14:45:59 APMUMCSAE002D freeradius[513279]: Compiling Post-Auth-Type REJECT for attr Post-Auth-Type
Aug 16 14:45:59 APMUMCSAE002D freeradius[513279]: Compiling Post-Auth-Type Challenge for attr Post-Auth-Type
Aug 16 14:45:59 APMUMCSAE002D freeradius[513279]: Compiling Post-Auth-Type Client-Lost for attr Post-Auth-Type
Aug 16 14:45:59 APMUMCSAE002D freeradius[513279]: radiusd: #### Skipping IP addresses and Ports ####
Aug 16 14:45:59 APMUMCSAE002D freeradius[513279]: Configuration appears to be OK
Aug 16 14:46:00 APMUMCSAE002D systemd[1]: Started FreeRADIUS multi-protocol policy server.
root@APMUMCSAE002D:/etc/freeradius/3.0#
```

o Run the freeradius server service in debug mode.

```
root@APMUMCSAE002D:/etc/freeradius/3.0# freeradius -X
FreeRADIUS Version 3.0.26
Copyright (C) 1999-2021 The FreeRADIUS server project and contributors
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE
You may redistribute copies of FreeRADIUS under the terms of the
GNU General Public License
For more information about these matters, see the file named COPYRIGHT
Starting - reading configuration files ...
including dictionary file /usr/share/freeradius/dictionary
including dictionary file /usr/share/freeradius/dictionary.dhcp
including dictionary file /usr/share/freeradius/dictionary.vqp
including dictionary file /etc/freeradius/3.0/dictionary
including configuration file /etc/freeradius/3.0/radiusd.conf
including configuration file /etc/freeradius/3.0/proxy.conf
```

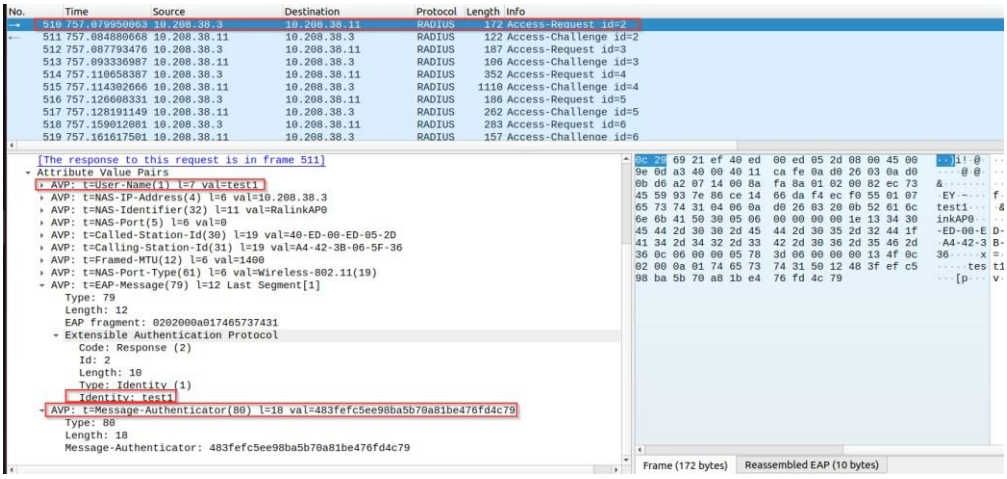
– Authenticate to DUT using radius server credentials.

- Check logs generated on radius server



The above screenshot shows the logs that are generated on radius server after successful login using credentials of user “test1”, which confirms DUT using radius server for authentication and authorization purpose.

• Verifying the communication channel between the external authentication server (radius server) is encrypted or not.



It is evident from the above screenshot that the request from DUT is not encrypted and requested data is visible in wire-capture.

11.1.4 **Test Observations:** It was observed that the communication channel between external authentication server is not encrypted. This does not meet the testing requirement

11.1.5 **Evidence Provided: -** Screenshots of Terminal , pcap

12. **<u>Test Case Result:</u>**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Secure communication of external authentication	Fail	

1.2.3 Protection against brute force and dictionary attacks

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.2** Authentication **and Attribute Management**

2. **<Security Requirement No & Name > 1.2.3: Protection against brute force and dictionary attacks**
3. **<Requirement Description: >** CPE shall have a mechanism that provides a protection against brute force and dictionary attacks which aim to use manual/automated guessing to obtain the passwords for user and machine accounts. CPE to detect repeated invalid attempts to sign into an account with incorrect passwords during a short period of time and it may implement at least one of the following most commonly used protection measures:
    - Increasing the delay (e.g., doubling) for each newly entered incorrect password.
    - Blocking an account after a specified number of incorrect attempts (typically 5) for a certain period of time.
    - Using CAPTCHA to prevent automated attempts.

This feature to be enabled for login attempts for CPE and on authentication attempts on WiFi access through SSID with PSK

4. **DUT Confirmation Details**:
5. **DUT Configuration:**
6. **Preconditions: -** The OEM shall provide the supported documents needed to configure the DUT to configure for protection against brute force attack
7. **Test Objective:-** To check if there if the DUT has the feature of protection against brute force attack and dictionary attack
8. **Test Plan**
    8.1. Number of Test Scenarios:
        8.1.1. Test Scenario to check the protection feature of the DUT against brute force attack
        8.1.2. Test Scenario to check protection feature of DUT against dictionary attack

    8.2. Test Bed Diagram

Tester machine
192.168.129.13

Wifi CPE
192.168.29.1

8.3. Tools Required:- Only DUT needed

8.4. Test Execution Steps:- The tester shall attempt to login into the DUT using its management interface multiple times with incorrect password and check the outcome

9. **Expected Results for Pass:** The DUT supports protection feature against brute force attack/dictionary attack

10. **Expected Format of Evidence:** Screenshots of Terminal

11. **Test Execution:**

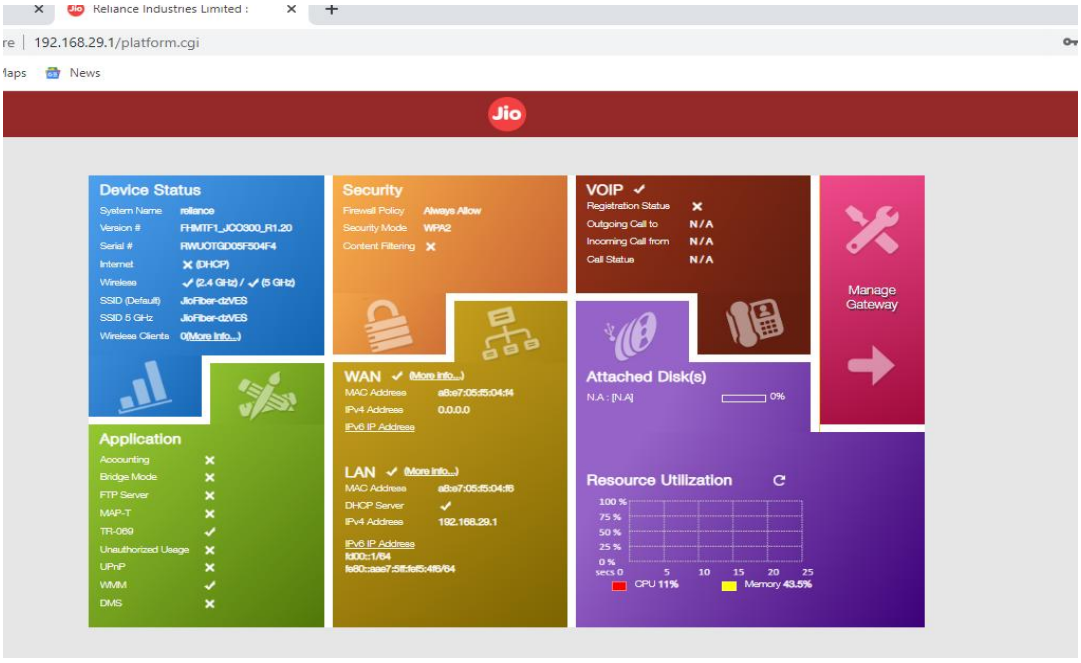
11.1 Test Case Number: 01

11.1.1 **Test Case Name:** Protection against brute force attack

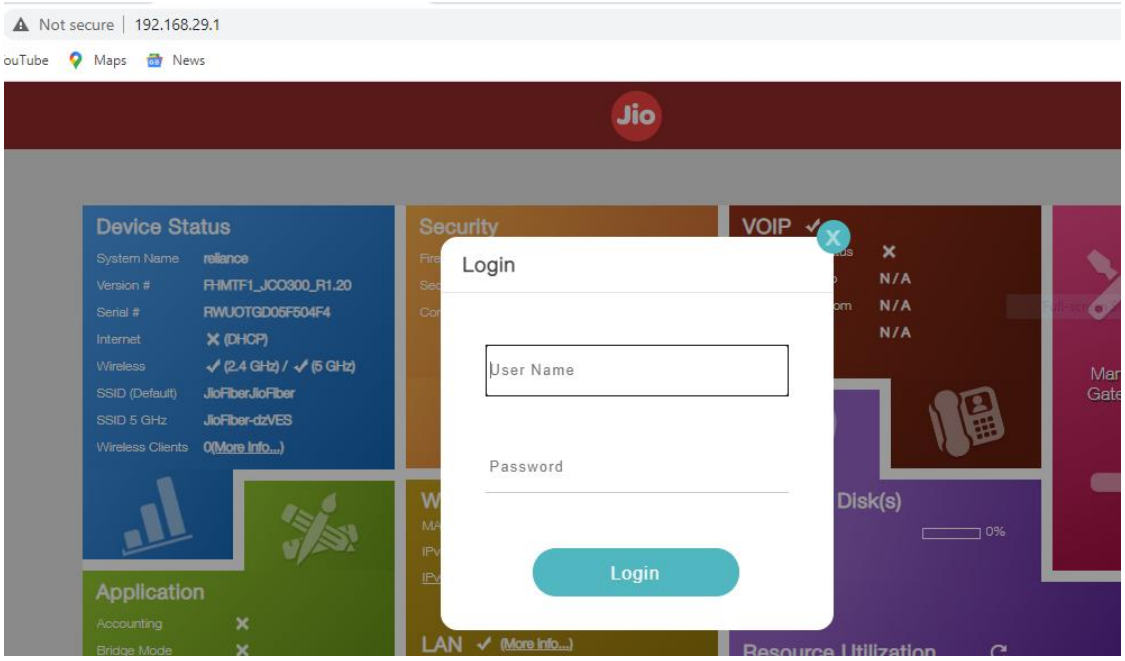
11.1.2 **Test Case Description:** The following testcase is done by attempting to login into the DUT multiple times with incorrect credentials.

11.1.3 **Execution Steps:**

- Access the web page of the DUT at 192.168.29.1
- DUT offers an initial login page as shown below.



- Click on the Manage gateway option for logging in to the Wi-Fi CPE modem. The login page as offered by Wi-Fi CPE modem will be prompting for a password in combination with username for logging in to the DUT.



- Tester tries to login into the device with incorrect credentials continuously.

11.1.4 **Test Observations:** It was observed that the user credentials could not be blocked even after indefinite and continuous attempts of incorrect password login. Hence, the test case is failing.

11.2 Test Case Number: 02

11.2.1 **Test Case Name:** Protection against dictionary attack **<Same observed as above as there is no protection feature in the DUT against brute force and dictionary attack>**

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Protection against brute force attack	Fail	No protection feature available
2	Protection against dictionary attack	Fail	No protection feature available

1.2.4 Enforce Strong Password

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.2** Authentication **and Attribute Management**
2. **<Security Requirement No & Name > 1.2.4: Enforce Strong Password**
3. **<Requirement Description: >** CPE shall only accept passwords that comply with the following complexity criteria:
    - Password containing a minimum length of 8 characters are only permitted by default. Shorter lengths shall be rejected by the NE.
    - Minimum password length - the default minimum value of 8 characters.
    - Password comprises at least three of the following categories:
        - at least 1 uppercase character (A-Z)
        - at least 1 lowercase character (a-z)
        - at least 1 digit (0-9)
        - at least 1 special character (e.g., @; $.)
    - CPE shall support password field length of minimum 64 characters.

This Feature to be enabled for CPE Login-IDs as well as for the PSK key associated with SSID for Wi-Fi access.

4. **DUT Confirmation Details**:

5. **DUT Configuration:**

6. **Preconditions: -** The OEM shall provide the supported documents needed to configure the DUT to configure idle timeout (if present)

7. **Test Objective:** - To check if there if the DUT has strict password policy in accordance to the requirement

8. **Test Plan**
    8.1. Number of Test Scenarios:
    8.1.1. Test Scenario to check whether the DUT password supports min of 8 character
    8.1.2. Test Scenario to check whether DUT supports password policy as follows

- at least 1 uppercase character (A-Z)
- at least 1 lowercase character (a-z)
- at least 1 digit (0-9)
- at least 1 special character (e.g., @; $.)

8.2. Test Bed Diagram

Tester machine
192.168.129.13

Wifi CPE
192.168.29.1

8.3. Tools Required:- Only DUT needed

8.4. Test Execution Steps

- The tester shall attempt to login into the DUT using its management interface
- The tester sall attempt to create a user with password that opposes the password policy as mentioned in the requirement and check if DUT rejects that or not

9. **Expected Results for Pass:** The DUT supports the password policy as mentioned in the requirement

10. **Expected Format of Evidence:** Screenshots of Terminal

11. **Test Execution:**

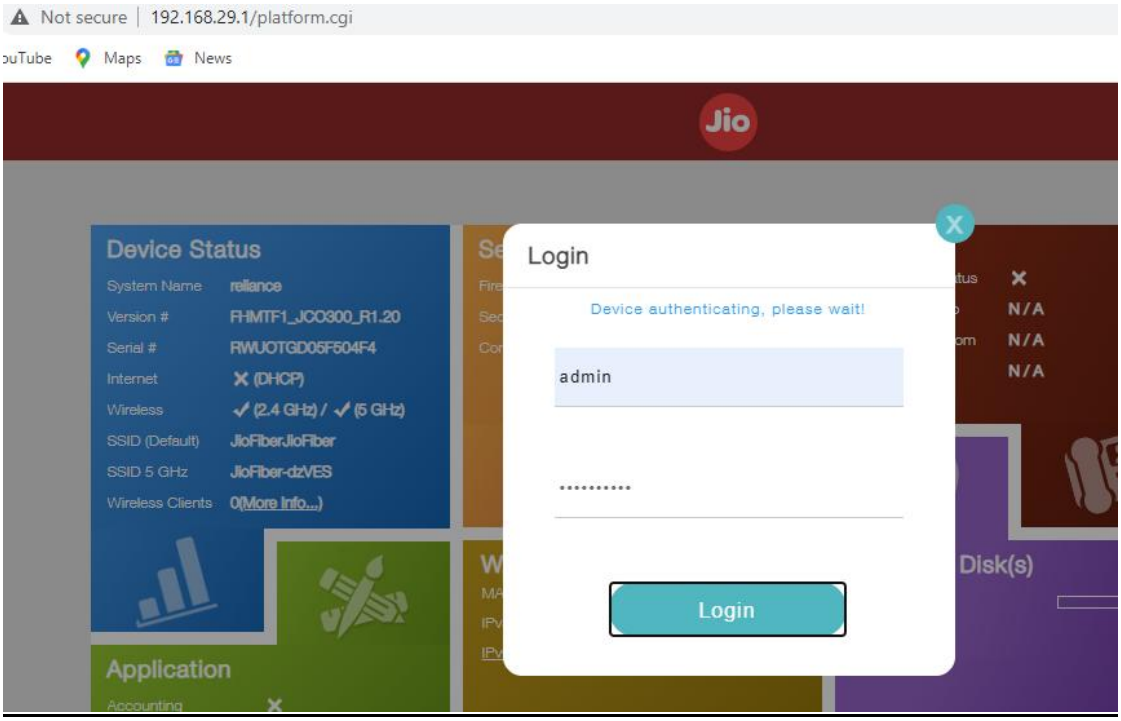
11.1 Test Case Number: 01

11.1.1 **Test Case Name:** Password min characters

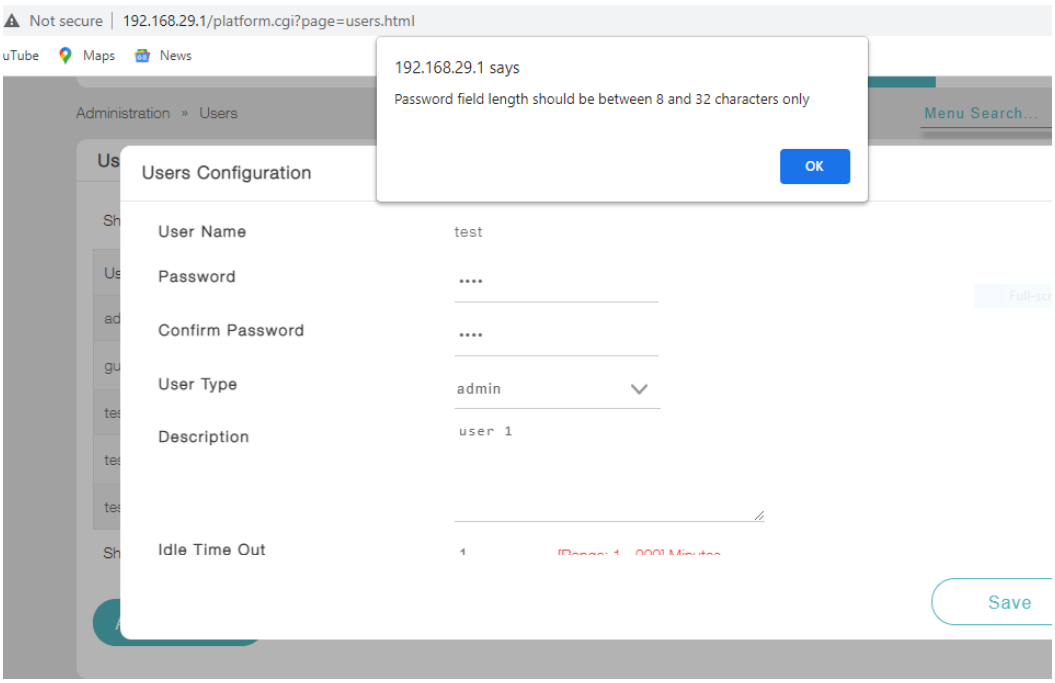
11.1.2 **Test Case Description:** The following testcase is done by attempting to check if the DUT supports min of 8 characters

11.1.3 **Execution Steps:**

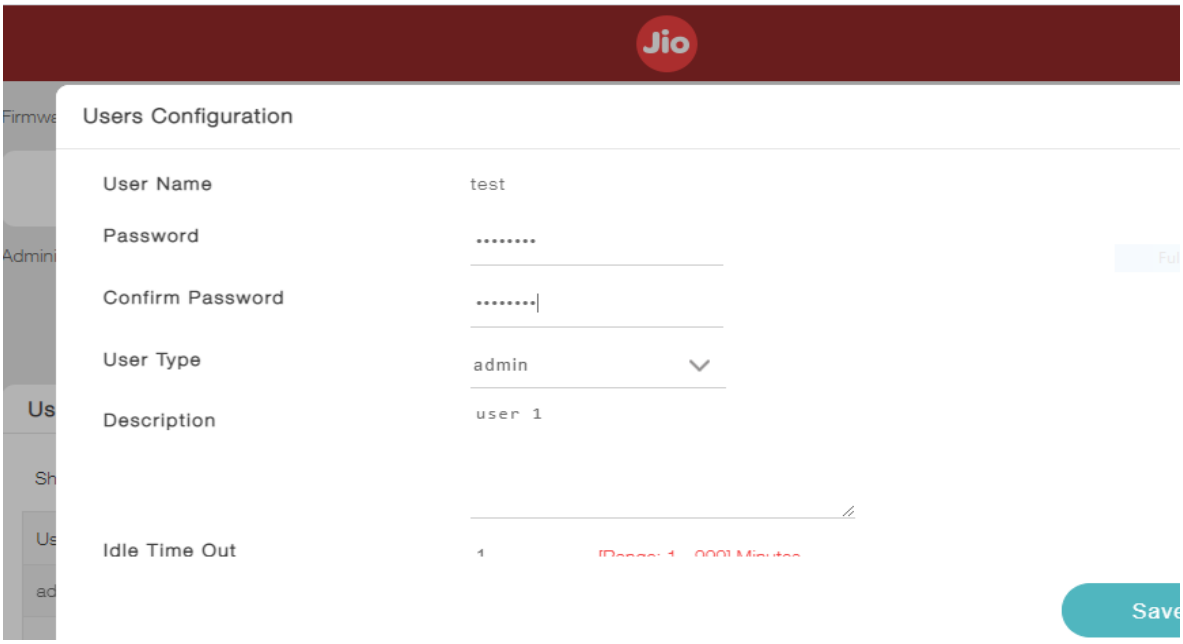
- Access the web page of the DUT at 192.168.29.1 and login with the admin credentials
- DUT offers an initial login page as shown below.

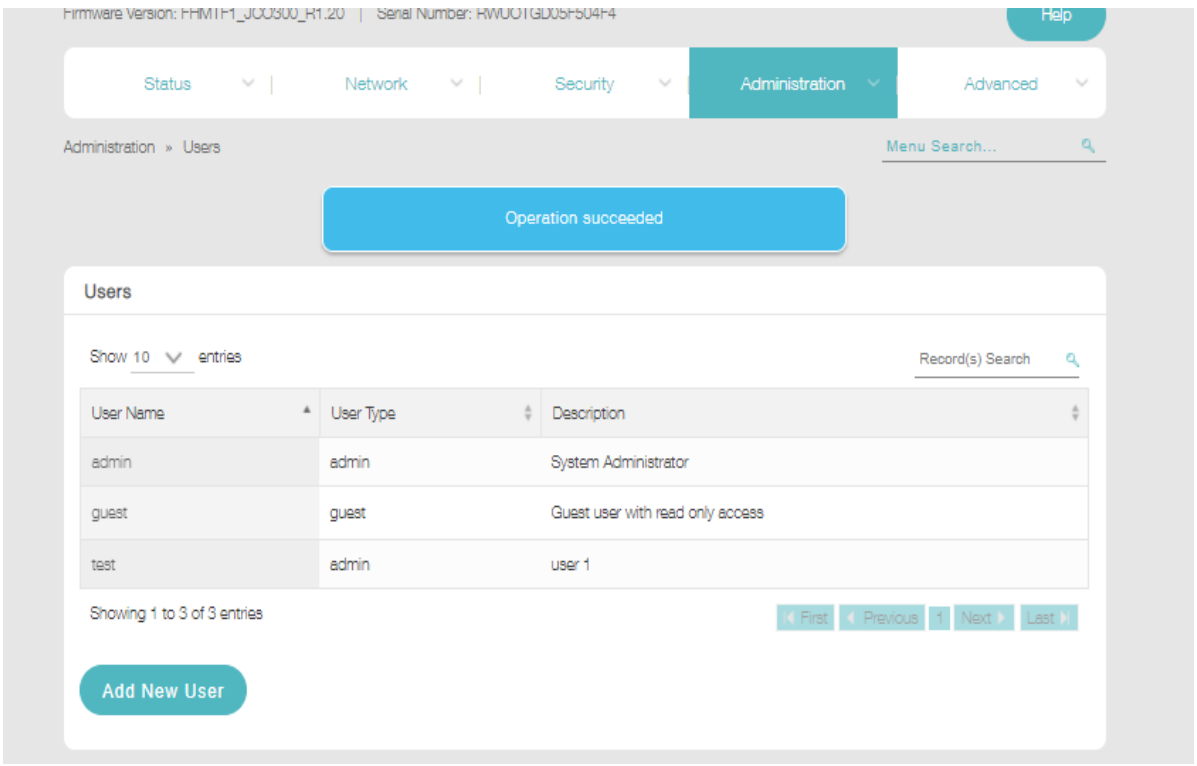


- Create a user with a weak password with the following credentials
  - username: test
  - password: 1234



- Create a user with a weak password with the following credentials
  - username: test
  - password: 12345678





11.1.4 **Test Observation:** It was observed that DUT doesn't accept password of length less than 8

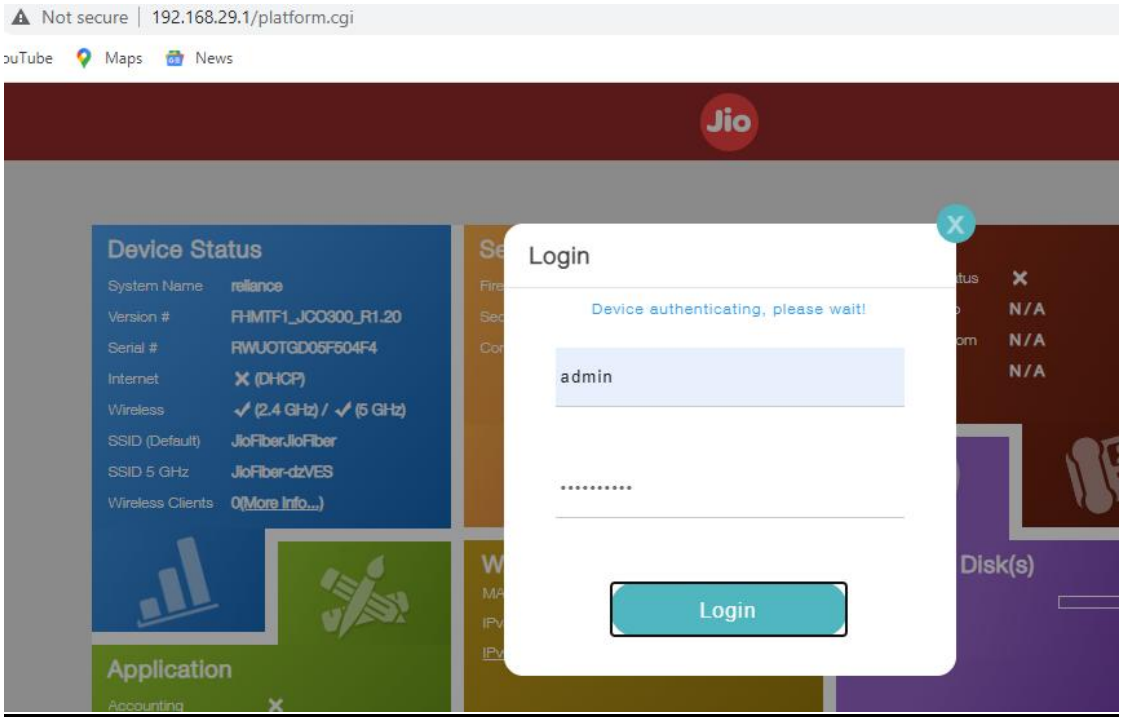
11.2 Test Case Number: 02

11.2.1 **Test Case Name:** Password policy

11.2.2 **Test Case Description:** The following testcase is done by attempting to check if the DUT supports password policy as per the requirement

11.2.3 **Execution Steps:**

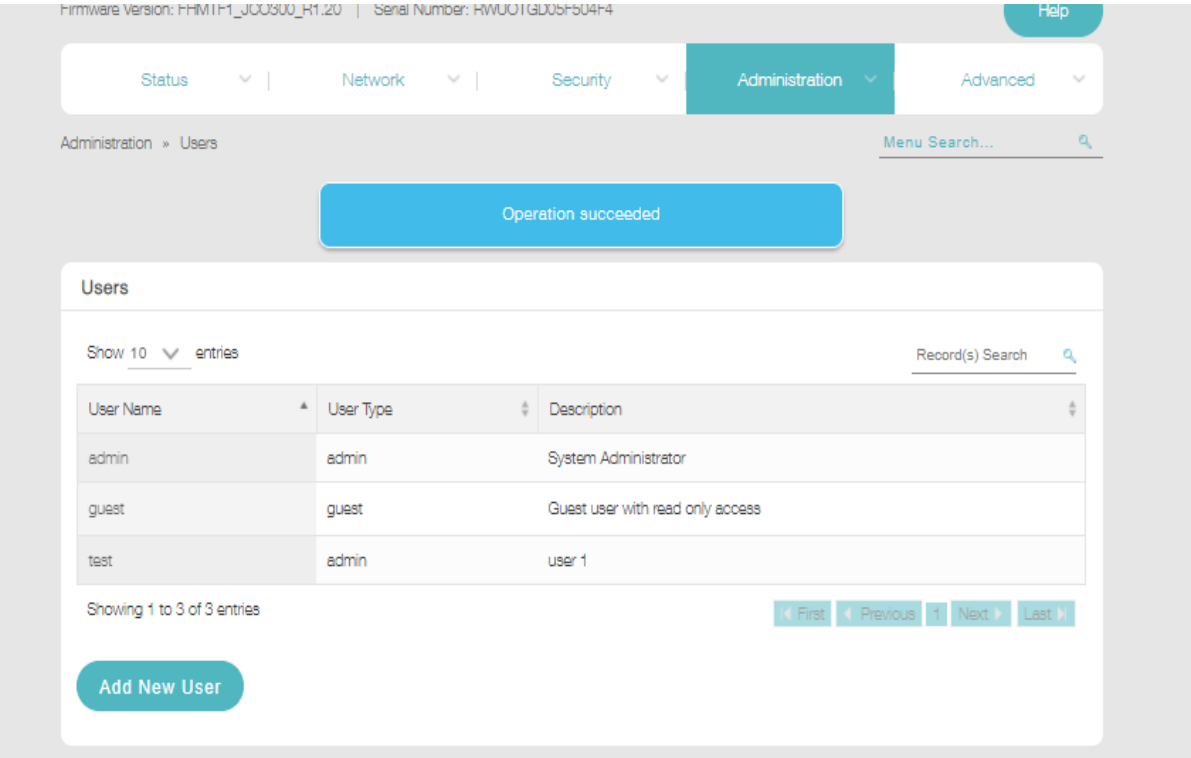
- Login into the DUT with admin credentials



- Attempt to create a user with a weak password violating the password policy
- Create a user with a weak password with the following credentials

  username: test

  password: 12345678



11.2.4 **Test Observations:-** It was observed that DUT accepts the password that violates the password policy(as per the requirement)

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Password min characters	Pass	
2	Password policy	Fail	DUT supports the password that violates the password policy

1.2.5 Inactive Session Timeout

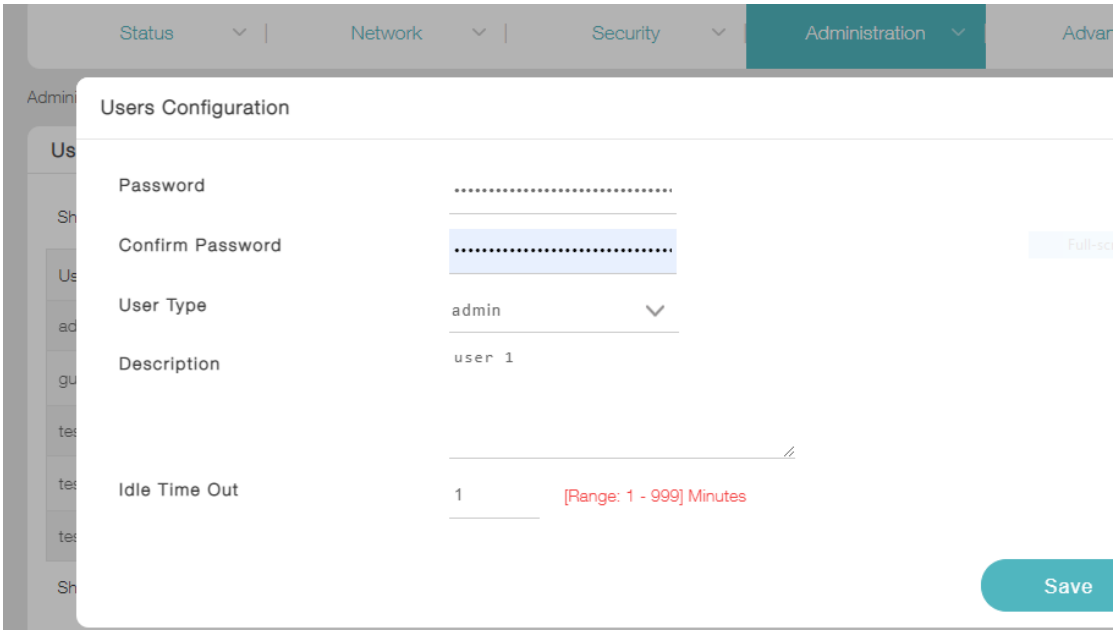
<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.2** Authentication **and Attribute Management**

2. **<Security Requirement No & Name > 1.2.5: Inactive Session Timeout**
3. **<Requirement Description: >** CPE shall monitor inactive sessions of administrative login users, Data users either on LAN or Wi-Fi and initiate session locking mechanism based on user configurable timers.

Unlocking the session shall be permissible only by authentication. If the inactivity period further continues for a defined period, Session /user ID time out must occur after this inactivity. The timer values can be admin configurable as per requirement. When the time out occurs, the same screen must be cleared of all displayed information.

4. **DUT Confirmation Details**:
5. **DUT <u>Configuration:</u>**
   - Login to router using the following admin credentials
   - Configure the timeout



6. **Preconditions:-** The OEM shall provide the supported documents needed to configure the DUT to configure idle timeout (if needed)
7. **Test Objective: -** To check if there if the DUT has the feature of idle timeout

8. **Test Plan**
   8.1. Number of Test Scenarios:
      8.1.1. Test Scenario to check whether the DUT has timeout upon inactivity
   8.2. Test Bed Diagram

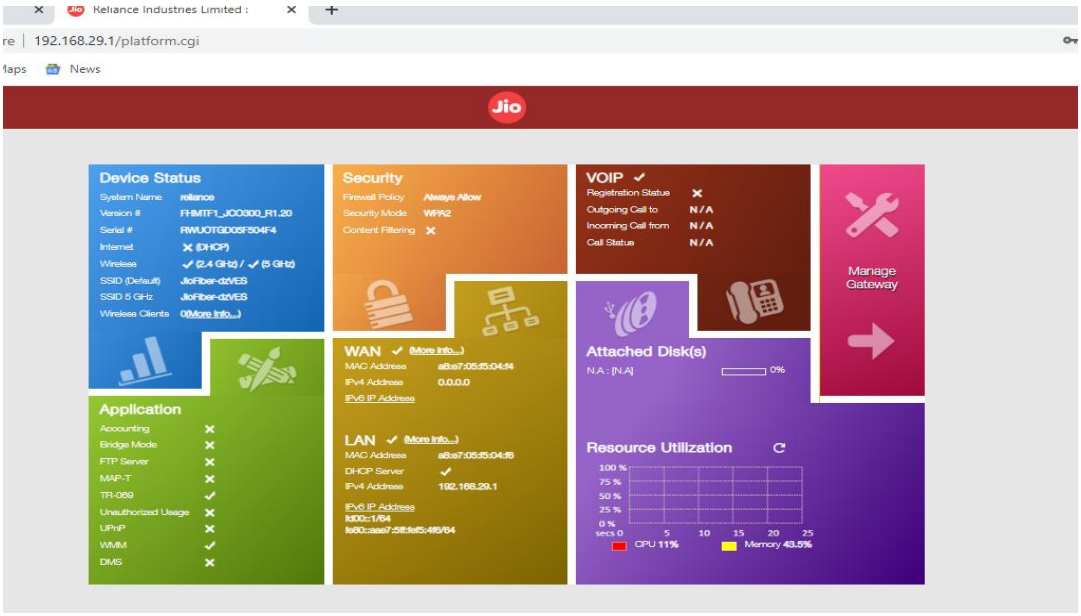
Tester machine
192.168.129.13

Wifi CPE
192.168.29.1

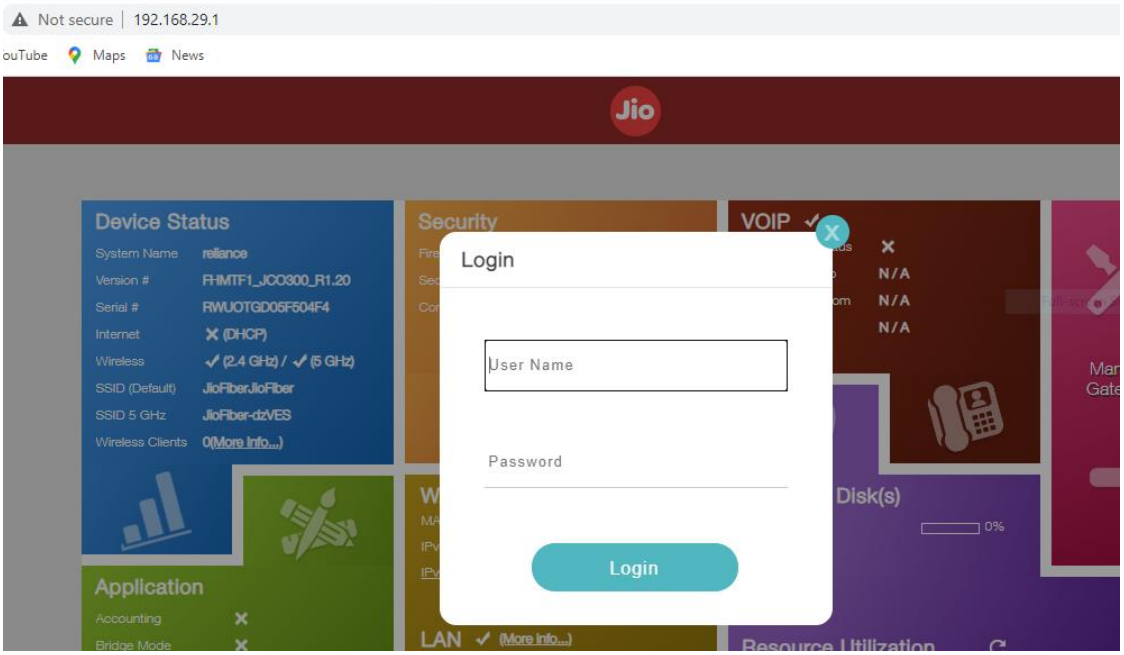
   8.3. Tools Required:- Only DUT needed
   8.4. Test Execution Steps
      - The tester shall attempt to login into the DUT using its management interface
      - The tester shall keep the DUT inactive until the certain (configured in the DUT) and checks the outcome
9. **Expected Results for Pass:** The DUT supports timeout feature upon inactivity

10. **Expected Format of Evidence:** Screenshots of Terminal

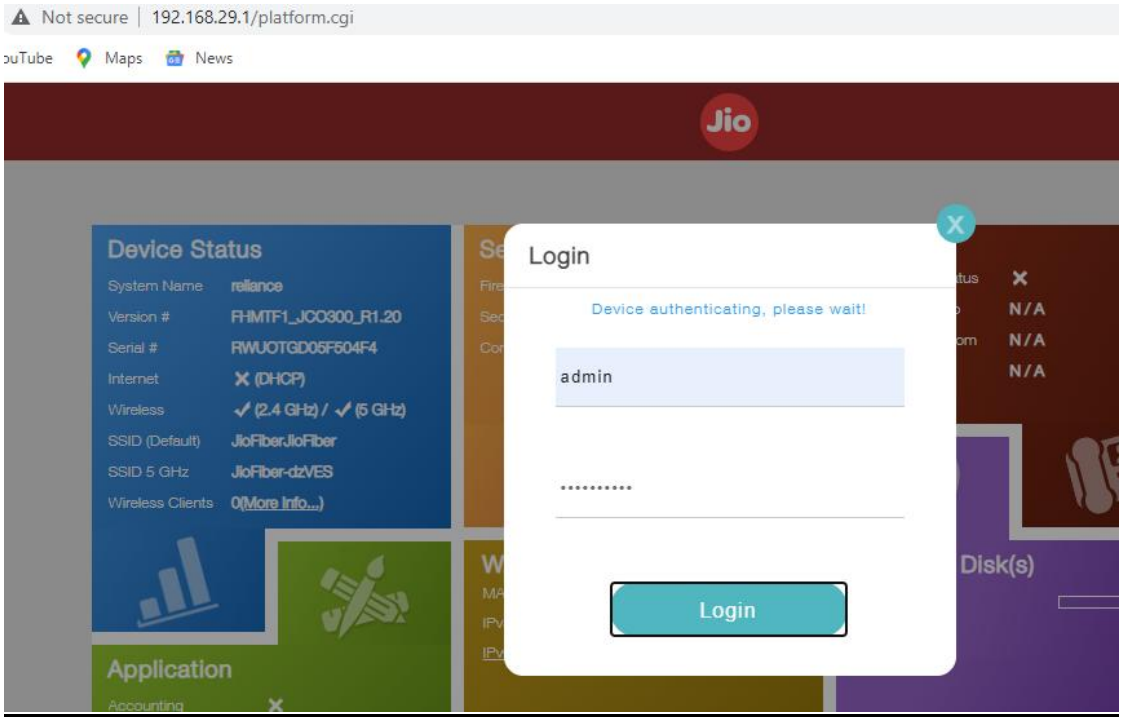
11. **Test Execution:**
   11.1 Test Case Number: 01
      11.1.1 **Test Case Name:** Inactivity logout
      11.1.2 **Test Case Description:** The following testcase is done by attempting to login into the DUT and checking if the DUT logs out upon inactivity
      11.1.3 **Execution Steps:**
         - Access the web page of the DUT at 192.168.29.1
         - DUT offers an initial login page as shown below.



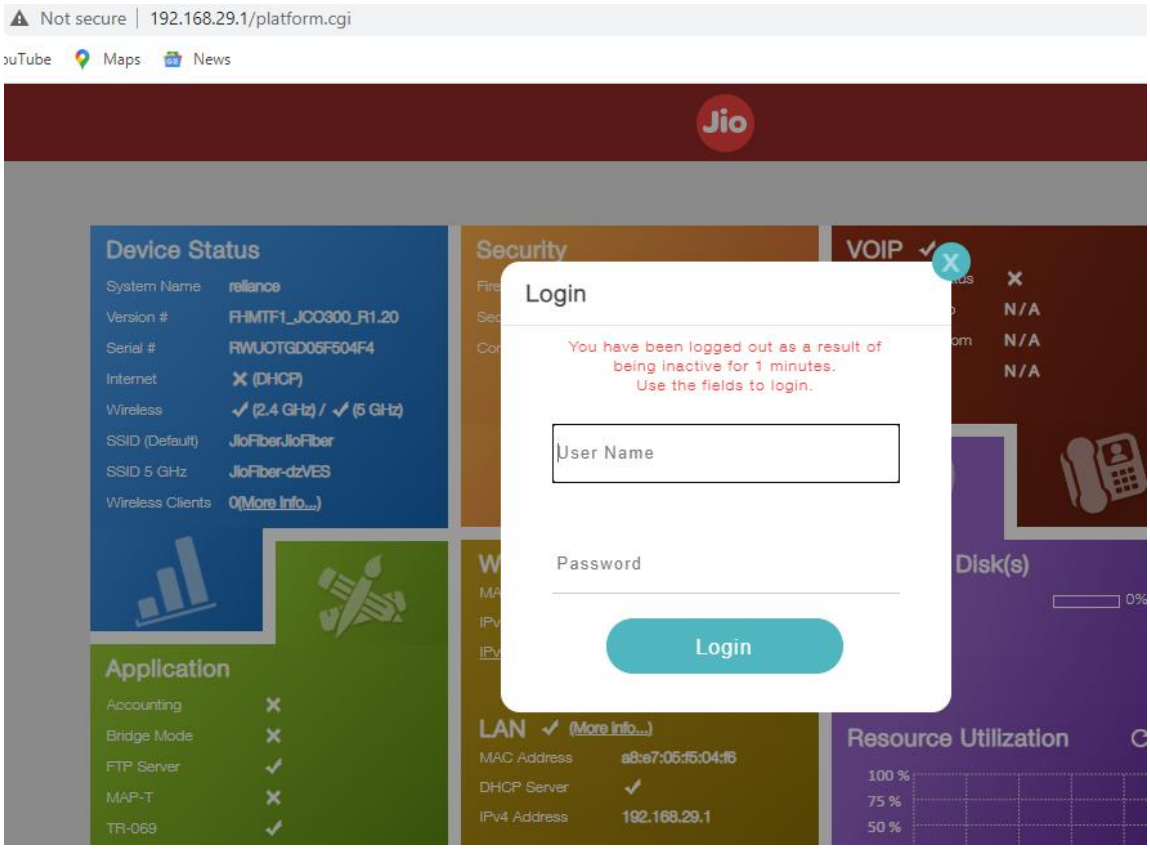
- Click on the Manage gateway option for logging in to the Wi-Fi CPE modem. The login page as offered by Wi-Fi CPE modem will be prompting for a password in combination with username for logging in to the DUT.



- Attempt to login



- Wait for a minute without performing any activity on the web GUI.



11.1.4 **Test Observations:**

- It was observed that after 1 minute of time out the user gets logged out of the device as shown in the screenshot above

- The test case is passing in the case of device management account login users. The test case is failing for the data users (LAN and Wi-Fi).

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Logout on inactivity	Pass	

1.2.6 Password Change facility, 1st Installation /Factory Reset

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.2** Authentication **and Attribute Management**
2. **<Security Requirement No & Name > 1.2.6: Password Change facility, 1st Installation /Factory Reset**
3. **<Requirement Description: >** CPE shall enforce change of authentication attribute (eg: - password) on 1st installation configuration or on factory reset conditions. If a password is used as an authentication attribute, then the CPE shall provide a function that facilitates the user to change his password at any time. However, the CPE shall not allow the previously used passwords up to a certain number (Password History)
4. **DUT Confirmation Details**:
5. **DUT Configuration:** No configuration needed
6. **Preconditions:** - The OEM shall provide the supported documents for credentials to access the admin and other features of DUT
7. **Test Objective:**- To check if there if the DUT enforces password change upon factory reset , at any other time and if previous passwords are disabled to be used
8. **Test Plan**
   - 8.1. Number of Test Scenarios:
     - 8.1.1. Test Scenario to check whether the DUT enforces the user to change the password upon 1st time login
     - 8.1.2. Test Scenario to check if DUT allows the user to change the password at any time
     - 8.1.3. Test Scenario to check if DUT allows user to use previous passwords upon password change
   - 8.2. Test Bed Diagram

Tester machine
192.168.129.13

Wifi CPE
192.168.29.1

   - 8.3. Tools Required: - Only DUT needed
   - 8.4. Test Execution Steps

- The tester shall attempt to reset the DUT and check if password is enforced to be changed from the default credentials
- The tester shall also attempt to change the credentials of a user account to a new password
- The tester will check if a previously used password can be used again

9. **Expected Results for Pass:** The DUT supports the features as mentioned in the requirement.
10. **Expected Format of Evidence:** Screenshots of Terminal
11. **Test Execution:**

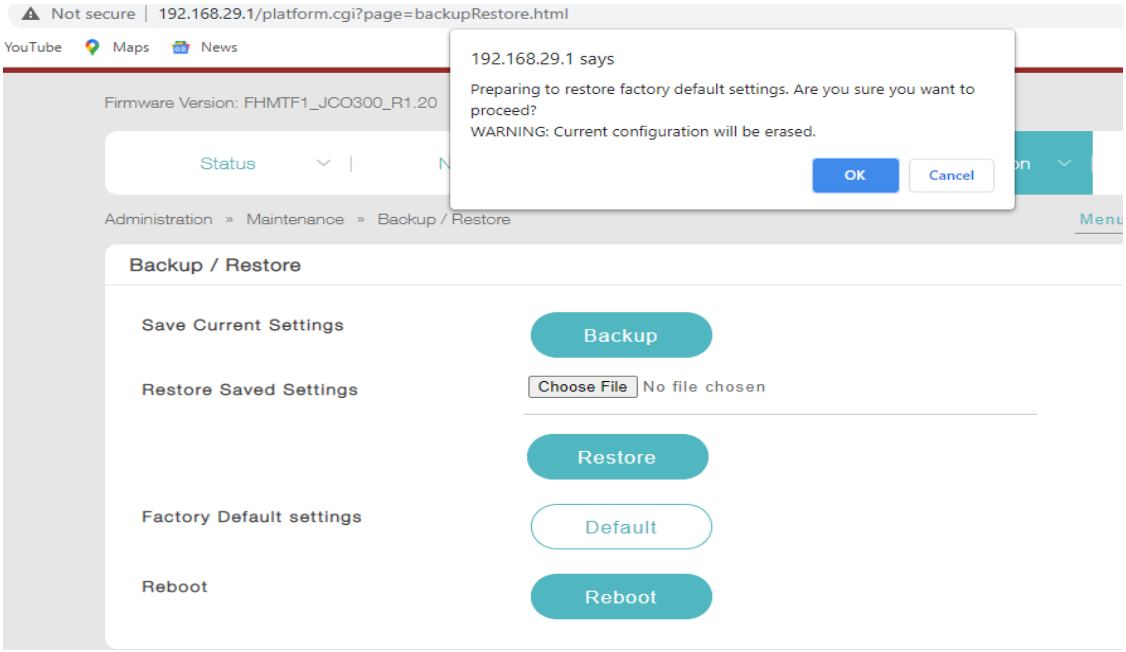
11.1 Test Case Number: 01

11.1.1 **Test Case Name:** Enforce Password change upon reset

11.1.2 **Test Case Description:** The following testcase is done by attempting to reset the DUT to check if password change is enforced for the user

11.1.3 **Execution Steps:**

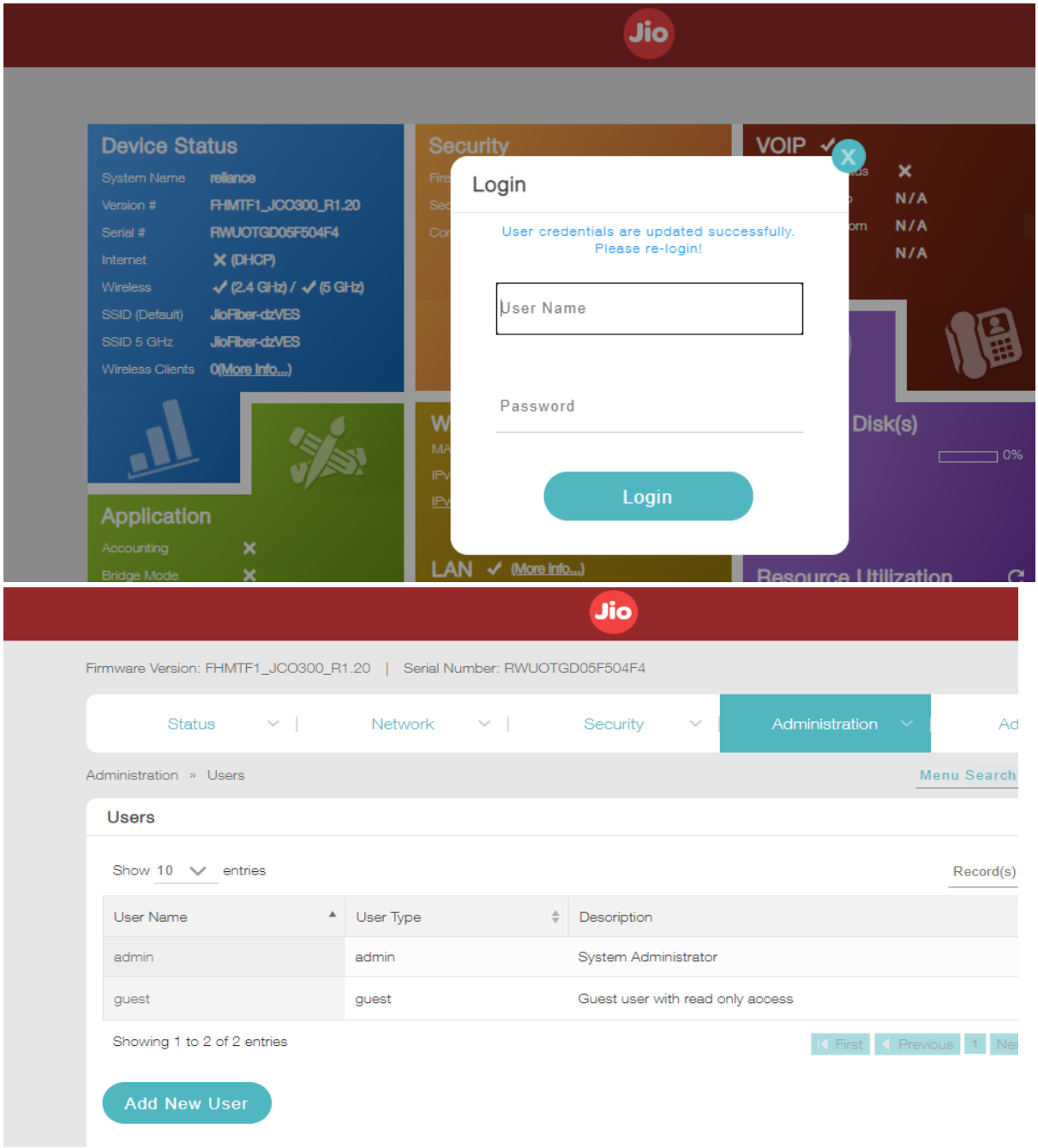
- Reset the DUT



- Login using default admin credentials. (Admin & Jiocentrum)

- Jio Wi-Fi CPE modem prompts to change the default password immediately after 1 login post factory reset as shown below.

- Tester changes the password for the default Admin user as well as guest user with the following passwords.
  New password for user admin: Ajio@1234
  New password for user guest: 12345678
  And attempts to login with the updated password



11.1.4 Test Observation:- It was observed that DUT enforces the user(admin) to change the password upon initial login

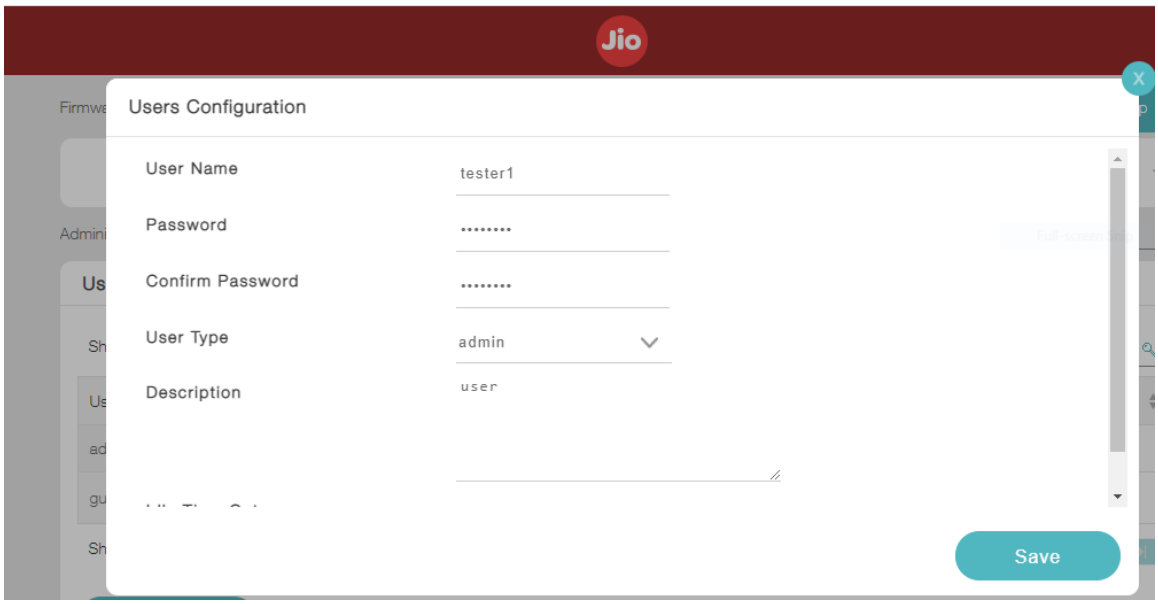
11.2 Test Case Number: 02

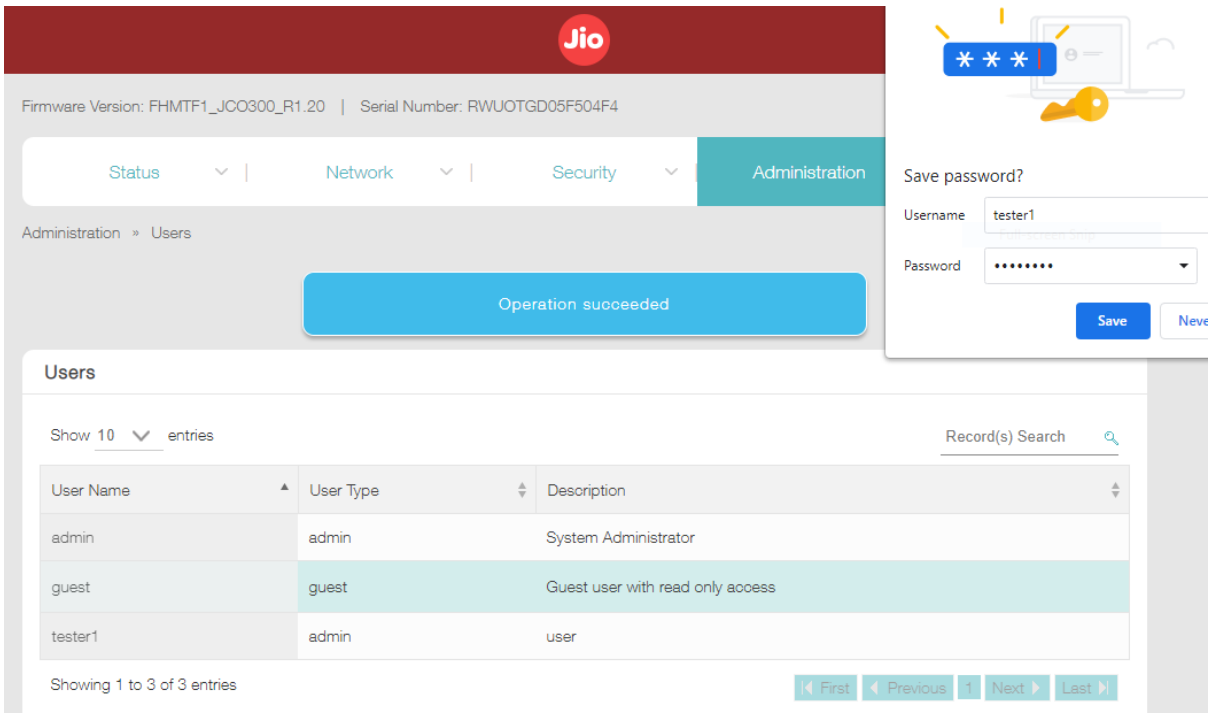
11.2.1 **Test Case Name:** Change password anytime

11.2.2 **Test Case Description:** The following testcase is done by changing the password of user to a new password

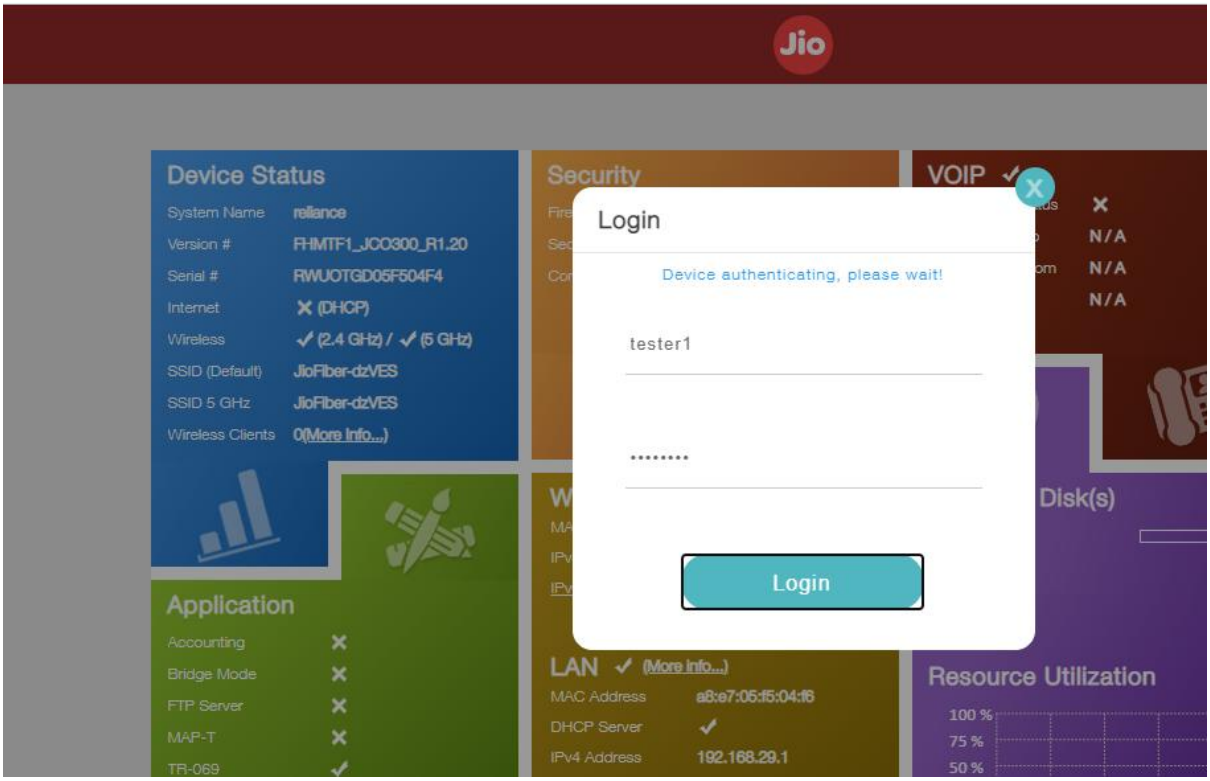
11.2.3 **Execution Steps:**

- Create a user with the following credentials,
  - User: tester1
  - Password: 12345678

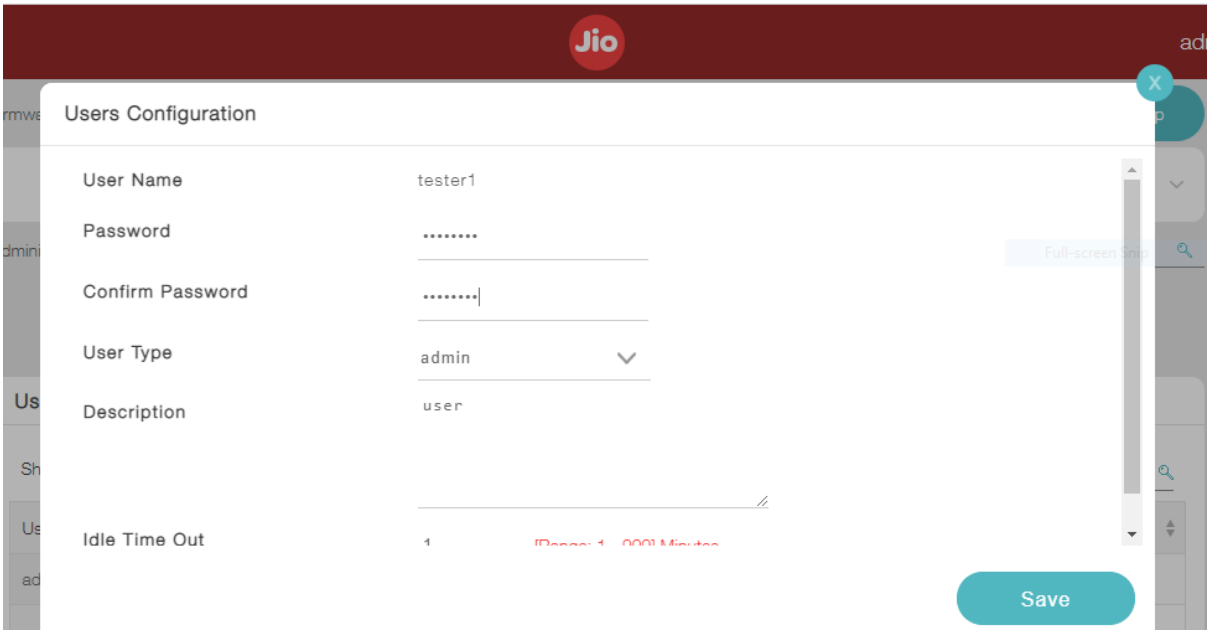


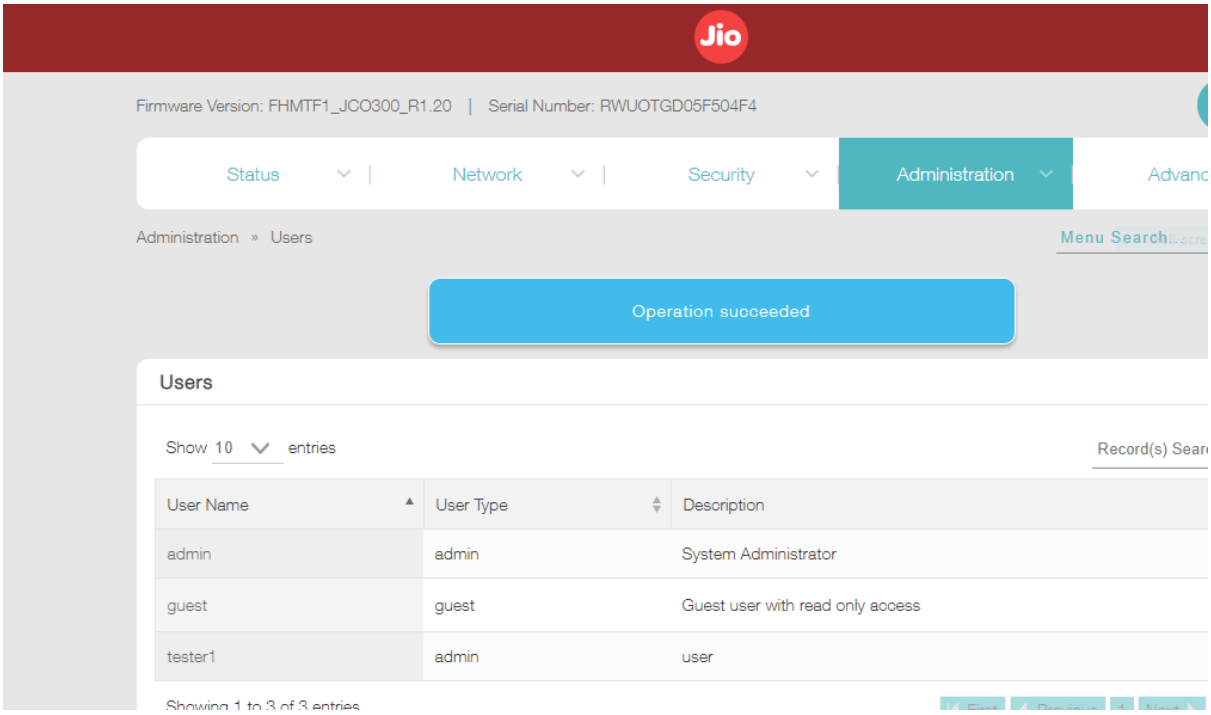


- Now login with the created user account



- Change the password of the tester1 account with the following credentials,
  Password: 87654321





- Attempt to login with the updated password

11.2.4 Test Observation:- It was observed that DUT supports password changing at any time

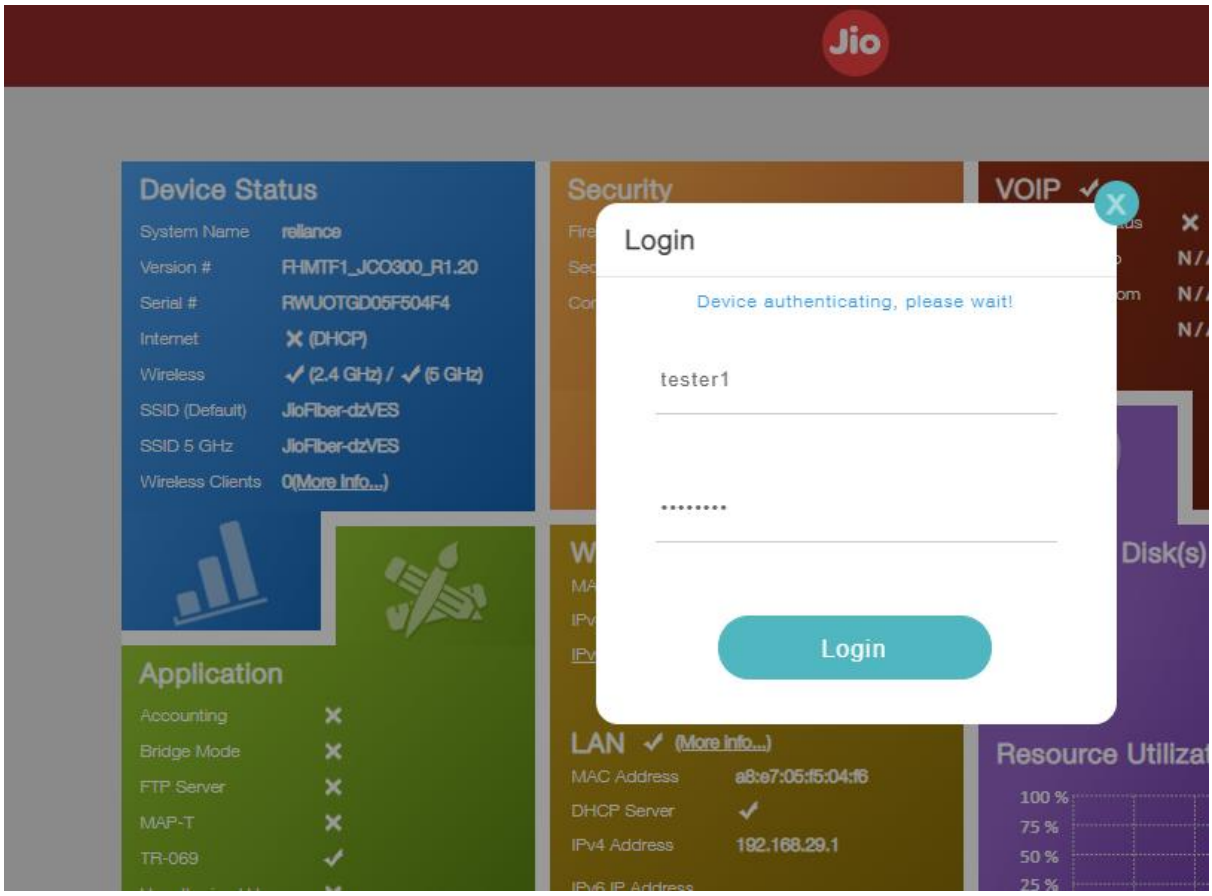
Test Case Number: 03

11.3.1 **Test Case Name:** Password History

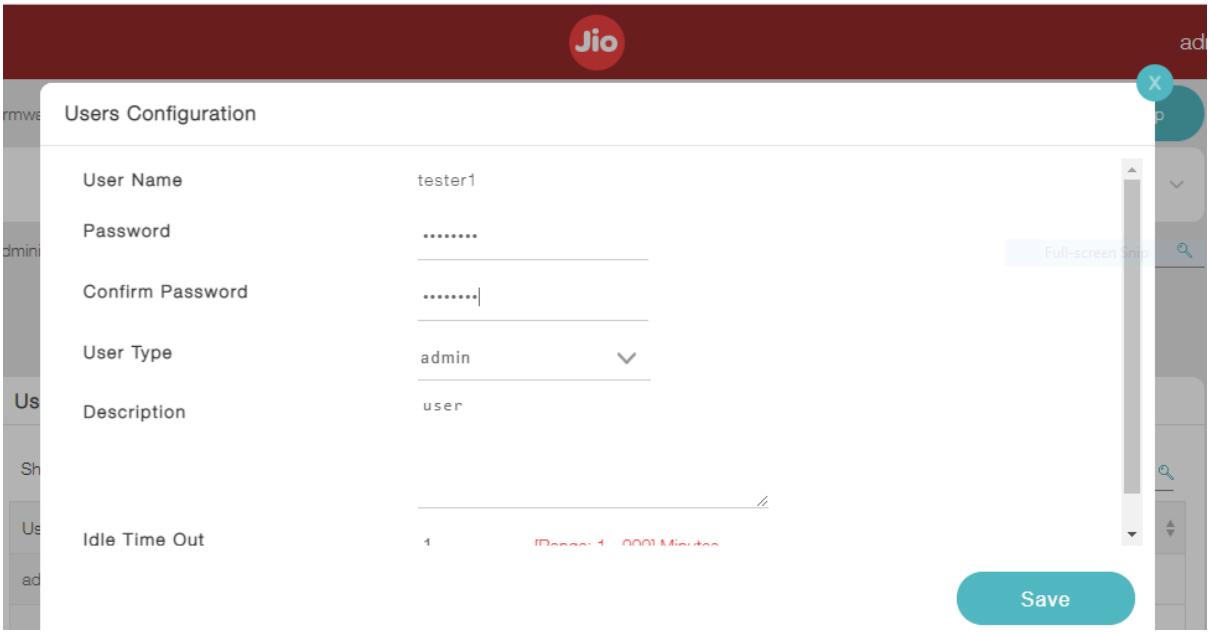
11.3.2 **Test Case Description:** The following testcase is done to check if previously used password can be used

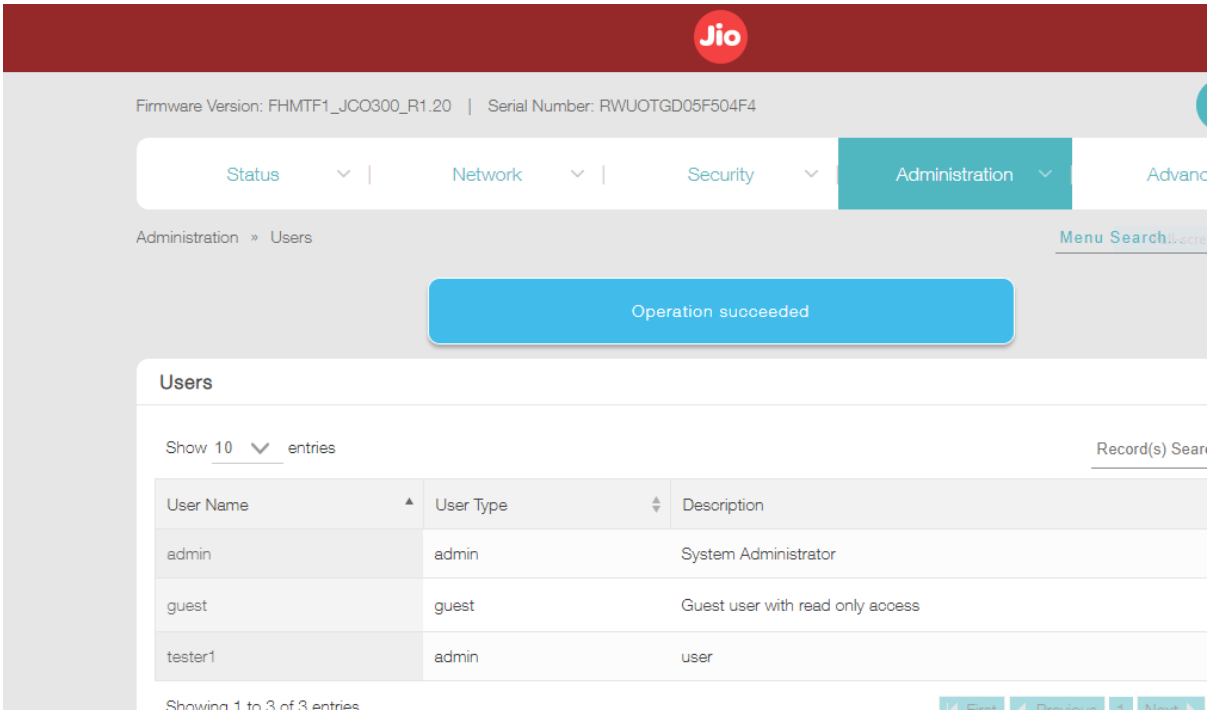
11.3.3 **Execution Steps:**

- Login with the tester account



- As seen from the Test Case : 02 , the tester account's password was changed from 12345678 to 87654321.
- Hence attempt to change the tester account's password again to 12345678





11.3.4 Test Observation: - It was observed that DUT allows previously used password to be used to update the password again

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Enforce Password change upon reset	Pass	
2	Change password anytime	Pass	
3	Password History	Fail	

1.2.7 Protected Authentication feedback

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.2** Authentication **and Attribute Management**

2. **<Security Requirement No & Name > 1.2.7: Protected Authentication feedback**

3. **<Requirement Description: >**
   When a user enters the password at the local console, local or remote management GUI, the CPE should give obscure feedback by displaying characters like "*".

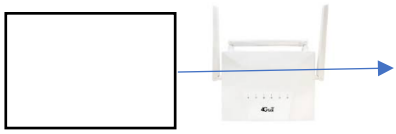
4. **DUT Confirmation Details**:

5. **DUT Configuration:** No configuration needed

6. **Preconditions**

7. **Test Objective**:- To check if there if the DUT obscures the password display with characters like "*".

8. **Test Plan**
   8.1. Number of Test Scenarios:
      8.1.1. Test Scenario to check whether the DUT obscures the password display with characters like "*" when user logs into the DUT
      8.1.2. Test Scenario to check whether the DUT obscures the password display with characters like "*" during new account creation
   8.2. Test Bed Diagram



Tester machine 192.168.129.13 — Wifi CPE 192.168.29.1

8.3. Tools Required:- Only DUT needed

8.4. Test Execution Steps

- The tester shall attempt to login into the DUT , entering the password to check how it is displayed
- The tester shall also attempt to create a new account entering the password to check the password display

9. **Expected Results for Pass:** The DUT obscures the password display during login and password change

10. **Expected Format of Evidence:** Screenshots of Terminal

11. **Test Execution:**

11.1 Test Case Number: 01

11.1.1 **Test Case Name:** Password during user login

11.1.2 **Test Case Description:** The following testcase is done by attempting to login into DUT by entering the password to check how it is displayed

11.1.3 **Execution Steps:**

- Login into DUT with admin credentials

11.1.4 Test Observation:- It was observed that DUT obscures the user password when entered during login

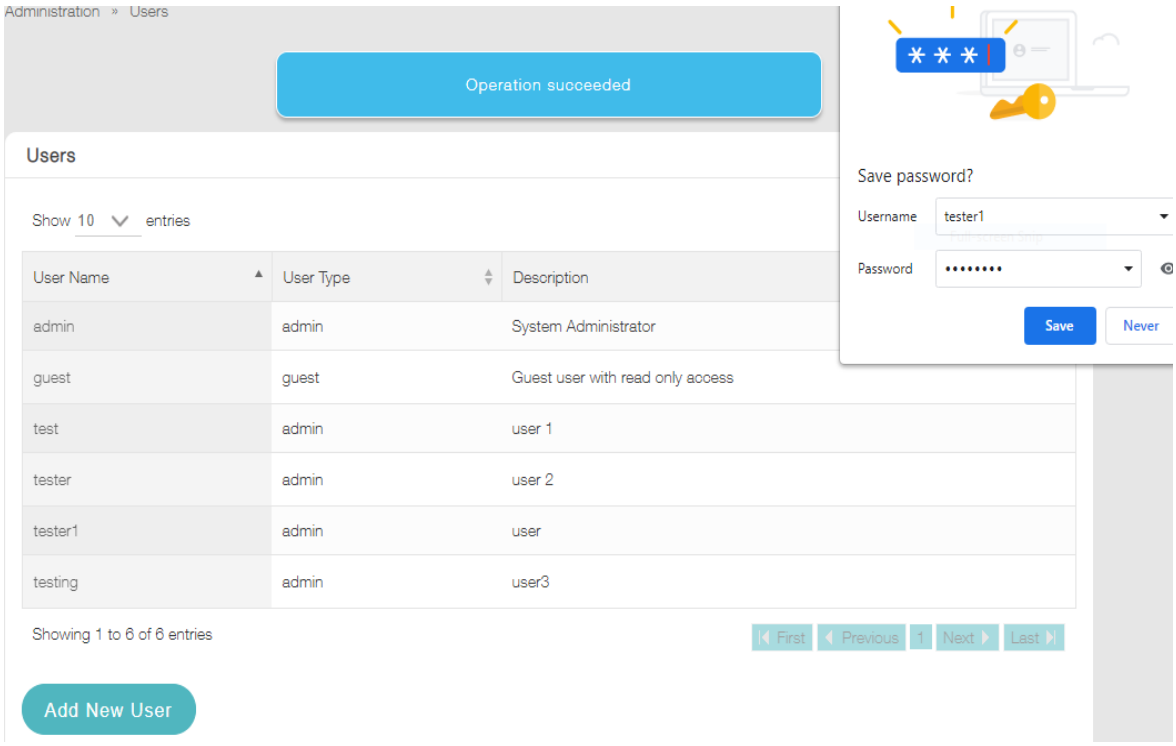
11.2 Test Case Number: 02

11.2.1 **Test Case Name:** Password during account creation

11.2.2 **Test Case Description:** The following testcase is done by attempting to create a new user account and entering the updated to check its display

11.2.3 **Execution Steps:**

- Create a user with the following credentials,
  User: tester1
  Password: 12345678



Relogin with the updated password

11.2.4 Test Observation: - It was observed that DUT obscures the password when entered during account creation

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Password during user login	Pass	
2	Change password anytime	Pass	

1.2.8 Removal of predefined or default authentication attributes

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.2** Authentication **and Attribute Management**

2. **<Security Requirement No & Name** > 1.2.8: Removal of predefined or default authentication attributes
3. **<Requirement Description: >** When a user enters the password at the local console, local or remote management GUI, the CPE should give obscure feedback by displaying characters like "*".

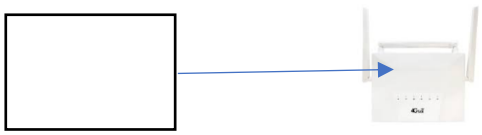
4. **DUT** Confirmation Details:

5. **DUT Configuration**: No configuration needed

6. **Preconditions**

7. **Test Objective**:- To check if there if the DUT obscures the password display with characters like "*".

8. **Test Plan**
   - 8.1. Number of Test Scenarios:
   - 8.1.1. Test Scenario to check whether the DUT obscures the password display with characters like "*" when user logs into the DUT
   - 8.1.2. Test Scenario to check whether the DUT obscures the password display with characters like "*" during new account creation
   - 8.2. Test Bed Diagram



Tester machine
192.168.129.13

Wifi CPE
192.168.29.1

   - 8.3. Tools Required:- Only DUT needed
   - 8.4. Test Execution Steps

- The tester shall attempt to login into the DUT , entering the password to check how it is displayed
- The tester shall also attempt to create a new account entering the password to check the password display

9. **Expected Results for Pass:** The DUT obscures the password display during login and password change

10. **Expected Format of Evidence:** Screenshots of Terminal

11. **Test Execution:**

11.1 Test Case Number: 01

11.1.1 **Test Case Name:** Password during user login

11.1.2 **Test Case Description:** The following testcase is done by attempting to login into DUT by entering the password to check how it is displayed

11.1.3 **Execution Steps:**

- Login into DUT with admin credentials

11.1.4 Test Observation :- It was observed that DUT obscures the user password when entered during login

11.2 Test Case Number: 02

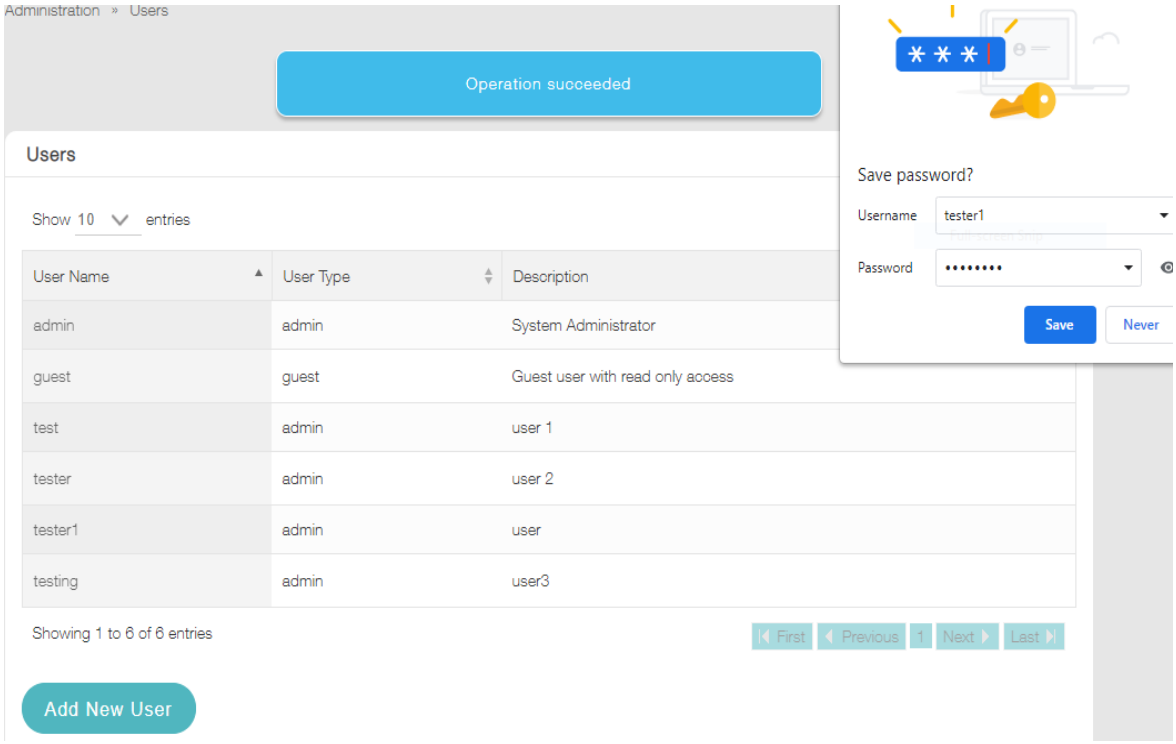
11.2.1 **Test Case Name:** Password during account creation

11.2.2 **Test Case Description:** The following testcase is done by attempting to create a new user account and entering the updated to check its display

11.2.3 **Execution Steps:**

- Create a user with the following credentials,
  User: tester1

Password: 12345678



Relogin with the updated password

11.2.4 **Test Observation: -** It was observed that DUT obscures the password when entered during account creation

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Password during user login	Pass	
2	Change password anytime	Pass	

1.2.9: Storage of Passwords in encrypted form

Section 1.3: Software Security

1.3.1 Secure Update

<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 3 - Software Security
2. **<Security Requirement No & Name >** 1.3.1 Secure Update
3. **<Requirement Description: >**
   The update process should verify the authenticity of the source repository and the integrity of the software patch preferably employing Digital Certificate for authenticity and hashing (example: SHA2) for integrity before updating the software in the CPE. The update mechanism should prevent illegal software patching.
4. **DUT Confirmation Details**:

- This section involves information about DUT like software/firmware version, Hardware version model.
- DUT Cisco WLC contains default boot image with version 8.10.183.0. The model is AIRAP1852I-E-K9. The inventory shows model serial no. & model description.

- Verification of DUT Cisco wireless LAN controller's HW product series information by running command *show inventory* on CLI.

```
(Cisco Controller) >show inventory

Burned-in MAC Address.............................. 38:ED:18:C8:10:60
Maximum number of APs supported..................... 50
NAME: "Mobility Express"    , DESCR: "Cisco Aironet 1850 Series Mobility Express"
PID: AIR-AP1852I-E-K9,  VID: V01,  SN: KWC193100UU
```

- Verification of DUT Cisco WLC's high-level system SW information by running command *show sysinfo* on CLI.

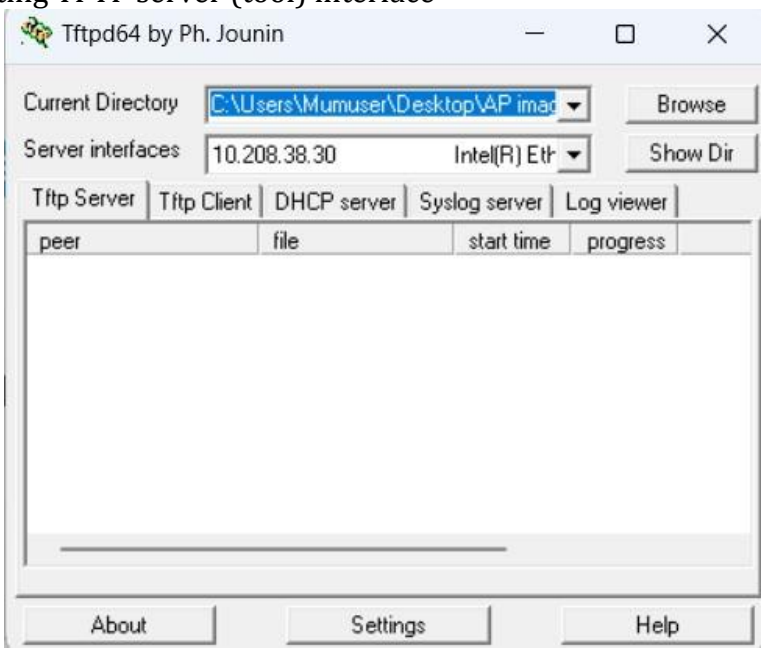
```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.10.183.0
OUI File Last Update Time........................ N/A

System Name...................................... Aironet-Controller
System Location..................................
System Contact...................................
System ObjectID.................................. 1.3.6.1.4.1.9.1.2250
IP Address....................................... 10.208.38.2
Last Reset....................................... 1: reload command

System Up Time................................... 0 days 3 hrs 33 mins 5 secs
System Timezone Location......................... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
System Stats Realtime Interval................... 5
System Stats Normal Interval..................... 180

Configured Country............................... IN  - India

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled

--More-- or (q)uit
```

- Verification of DUT Cisco WLC's system information on Web access.

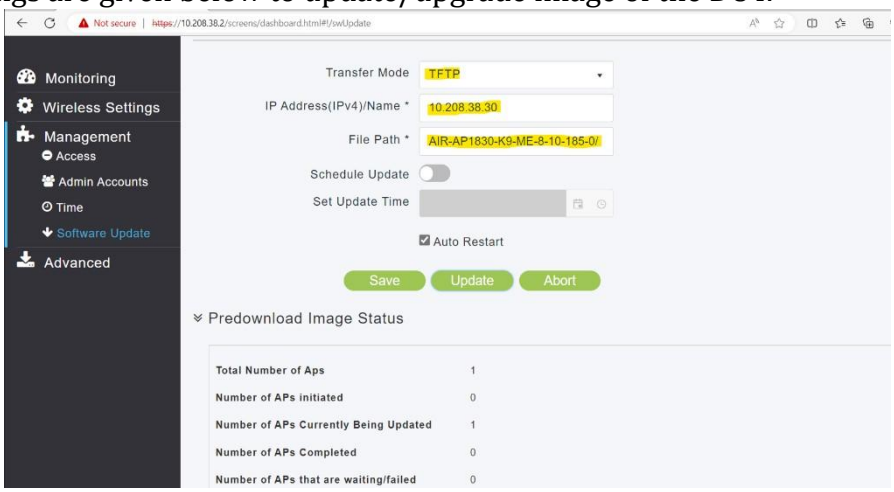
5. **DUT Configuration**: Configuration of DUT as per this test:

Case1: positive test case –

- Selecting TFTP server (tool) interface



- Settings are given below to update/upgrade image of the DUT.



6. **Preconditions:**

- A document containing information regarding the following:
- software package integrity checks.
- Including details of how the integrity check is carried out.
- Where public keys or certificates of sources authorized to sign software packages are stored on the DUT and who these sources are.
- What evidence is created to prove that the integrity check has been executed and what the result of the check was.
- Documentation which describes the installation procedure including how a user is authorized and authenticated to perform installation process.
- Valid package for installation/boot and one tampered image (tampered with hex edit).
- Hex Editor for modifying the DUT Image. - TFTP server for image transfer - Valid package for installation/boot.
- A network product document containing information regarding software package integrity checks, including details of how the integrity check is carried out.
- A valid network product software load/package and one that is not-valid.

7. **Test Objective:** To verify that DUT have mechanism that validates the software package integrity during installation/update stage

8. **Test Plan:**

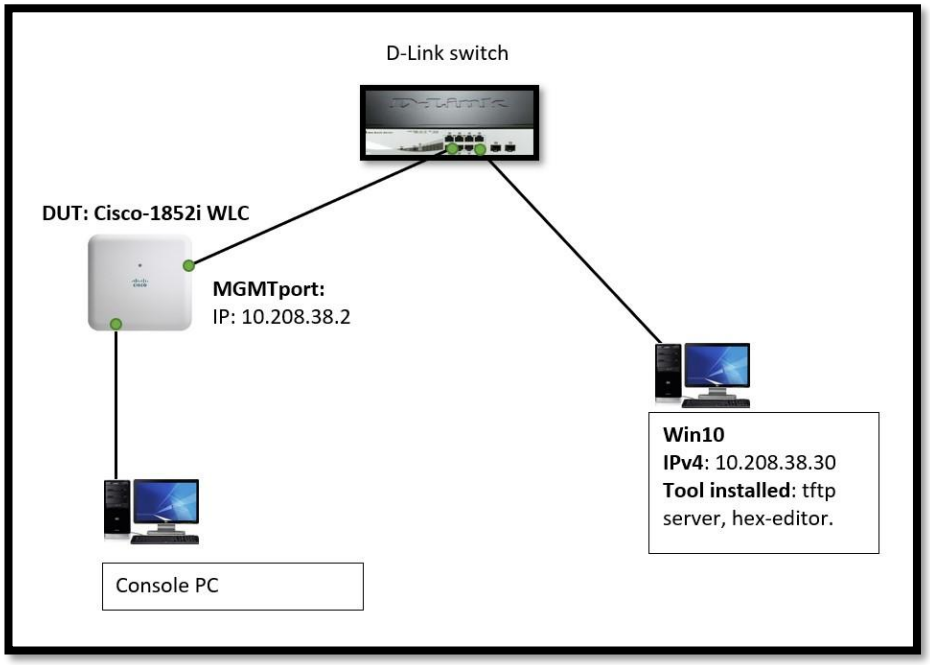
- Software package integrity shall be validated in the installation/upgrade stage.
- Network product shall support software package integrity validation via cryptographic means, e.g. Digital Certificate(digital signature). To this end, the network product has a list of public keys or certificates of authorised software sources, and uses the keys to verify that the software update is originated from only these sources.
- Tampered software shall not be executed or installed if integrity check fails.

- A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software update, and modify the list mentioned in bullet 2.

8.1 **Number of Test Scenarios:**

8.1.1 Software update in DUT verifying the integrity using digital certificate(digital signature)/public keys

8.2 **Test Setup Diagram**



8.3 **Tools Used:**

- Web browser(client) Win10, tftp-server, hex-editor, putty for console.

8.4 **Test Execution Steps:**

Below are the execution steps with evidence:

Case1: Positive testcase –

- The settings on tool i.e., TFTP server - Selecting image to be updated.
- Settings On DUT:
- Now login as user1 (ReadOnly privilege)
- Verifying user1 can't update/upgrade the image of DUT.
- Now login with Admin (ReadWrite privilege)
- Settings are given below to update/upgrade image of the DUT. (Current iOS image version is 8.10.183.0).
- After clicking on update transfer of image from TFTP to DUT starts - verification of image transfer on TFTP server.

- Uploading of image to DUT from TFTP server completed.
  - DUT auto restarts after completion of uploading image to DUT.
  - DUT starts boot process automatically.
  - DUT performing Image Signing verification while booting to new image.
  - DUT performing Cryptographic checks while starting image process –

- Verifying the version of the DUT Image updated – on controller after login with user Admin on console and GUI.

Case2: Negative testcase – (note: this test performed earlier before updating the image) - copy the boot image (part.bin) from DUT to terminal for tampering.

- Run Hexeditor of terminal machine and change certificate values in the boot image.
- After editing save the edited image and reboot the device with the tampered boot image over TFTP.
- Updating from rommon mode require IP to be change of TFTP server as per DUT ask for it.
- Verify the integrity of the boot image manually by command. Device failed to load the tampered image giving error message as Image signing verification failed.

9. **Expected Result for Pass:** Software package integrity shall be validated using cryptographic means, e.g. Digital certificate(digital signature) in the installation/upgrade stage. Tampered software shall not be executed or installed if integrity check fails. Only authorized person, can able to do software update.

10. **Expected Format of Evidence:** Screenshot of DUT webpage and terminal

11. Test Execution:

11.1 **Test Case Number:** 01

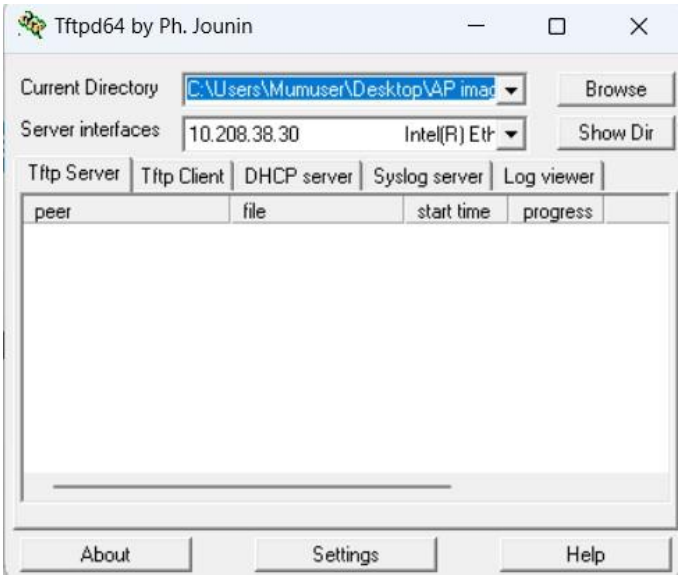
11.1.1 **Test Case Name:** TC_NO_SECURE_UPDATE

11.1.2 **Test Case Description:** In this test scenario tester will perform the positive test to update/upgrade the DUT image using the TFTP server and DUT settings were configured for an image update. The update will be verified by low privilege user and highest privilege user also image signing verification and cryptographic library will be checks during update/upgrade on console. In the negative test, tester will try to update on DUT and observed the process will get fail or not for image signing verification.

11.1.3 **Execution Steps:** Below are the execution steps with evidence:

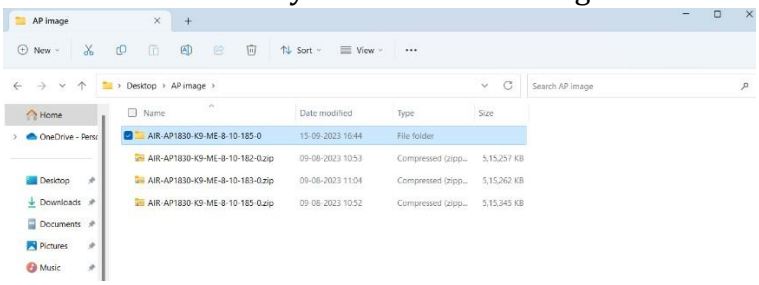
Case1: Positive testcase – Below are the settings on tool i.e., TFTP server:

Selecting server interface

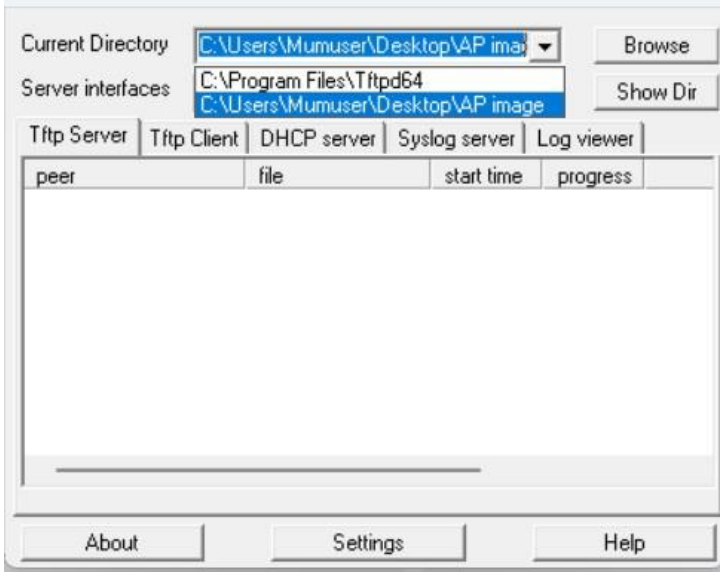


- Selecting image to be updated.

Browse to the directory where the new image downloaded.

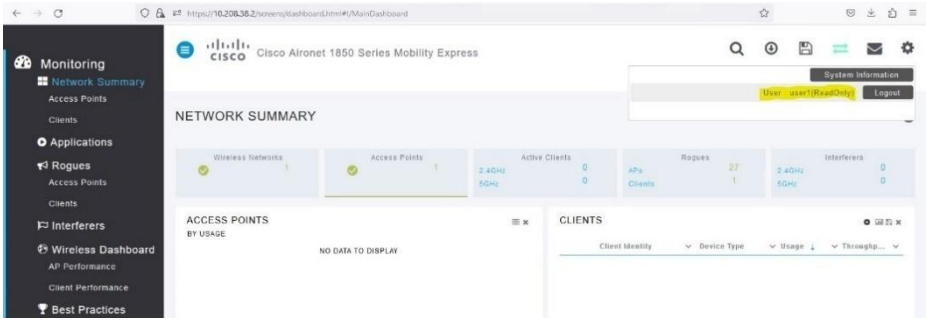


Browse correct path in current directory of TFTP server.

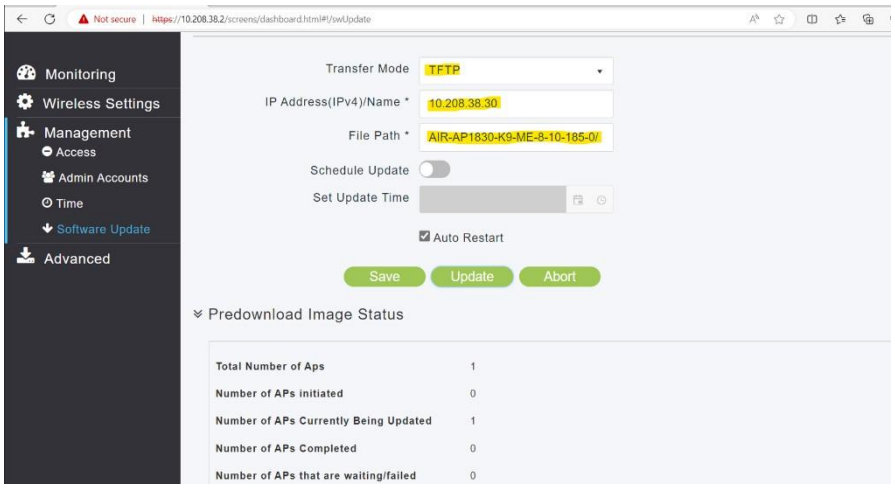


- Settings On DUT:

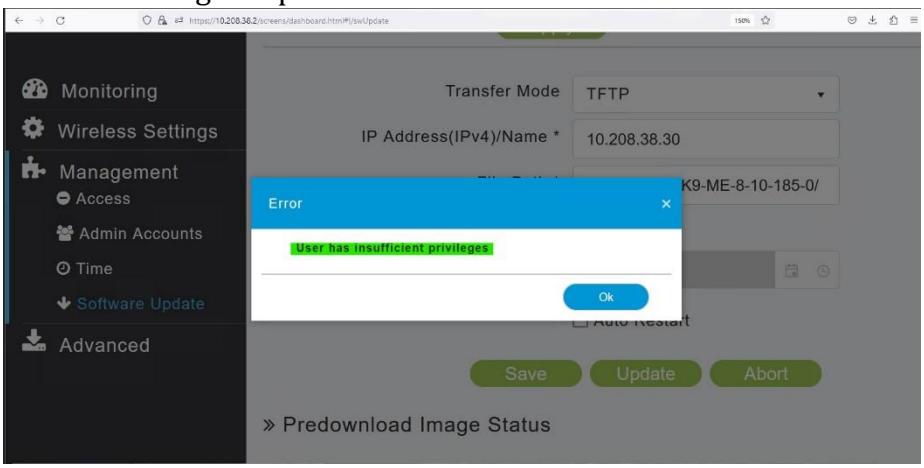
First Login as user1 (ReadOnly privilege)



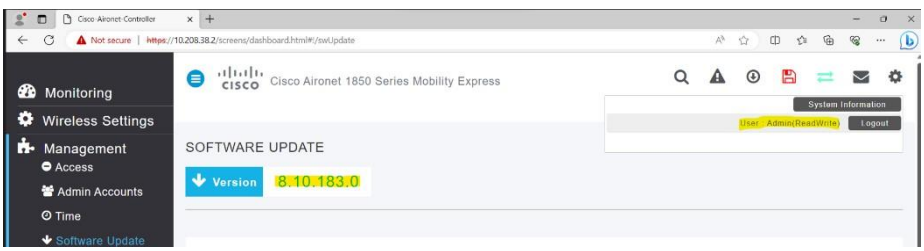
- Settings are given below to update/upgrade image of the DUT.



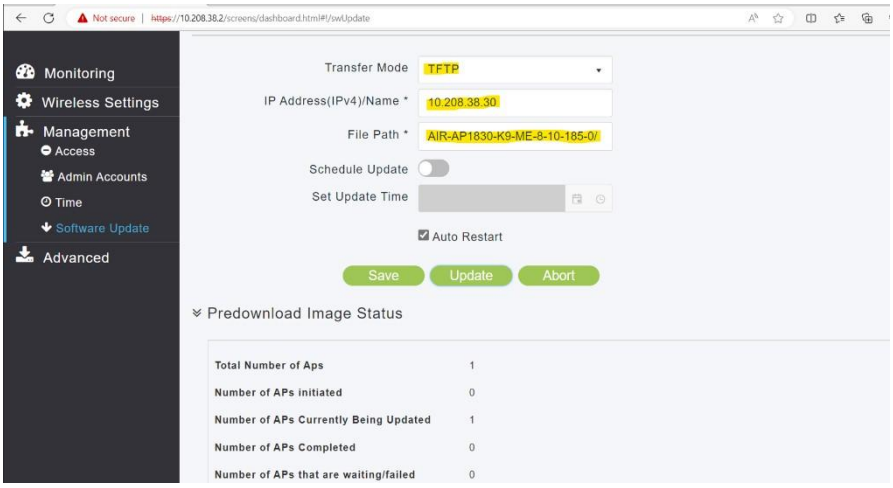
- After clicking on update error occurs.



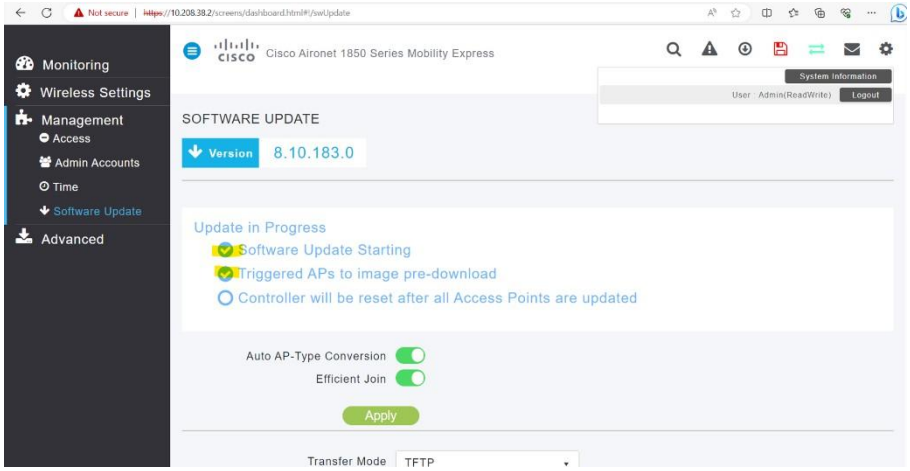
- Here it has been observed that User – "user1" does not have Readwrite privilege so can't update/upgrade. So, "insufficient privilege error occurred.
    - Note: Only users with Read-write privilege can update/update iOS image of DUT.
    - Now login as Admin (ReadWrite privilege)



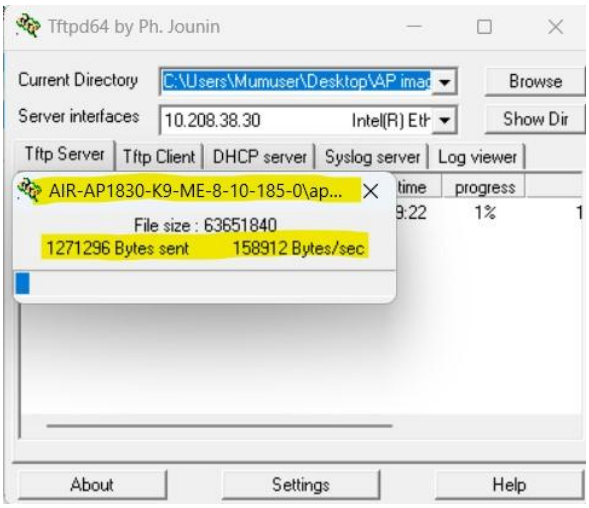
- Settings are given below to update/upgrade image of the DUT. (Current iOS image version is 8.10.183.0).



- After clicking on update transfer of image from TFTP to DUT starts

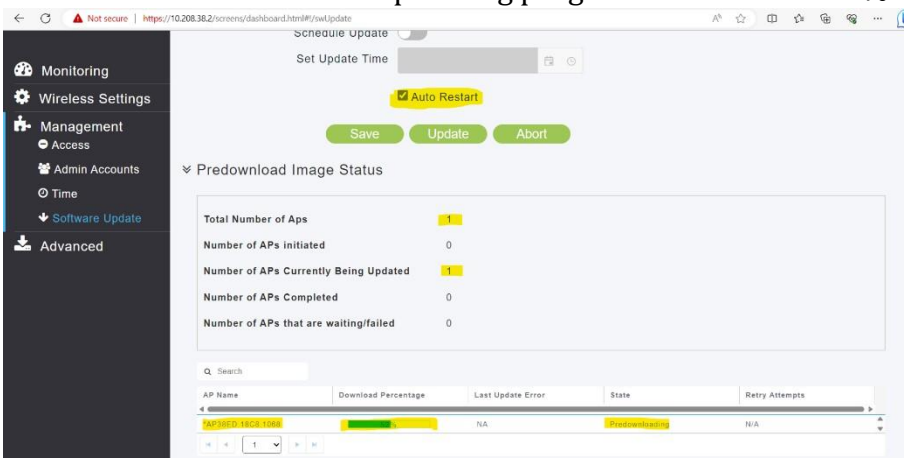


- On TFTP server



On tftp server it is seen that transfer of image from TFTP server to DUT has been started. Till this step it can be concluded that only Admin (mgmtuser with highest level of access i.e., read-write privilege)

- After some time on DUT- uploading progress is more than 50%



Here it can be noted that "Auto restart" is checked which means DUT auto restart after completion of image transfer to DUT.

- Uploading of image to DUT from TFTP server completed.

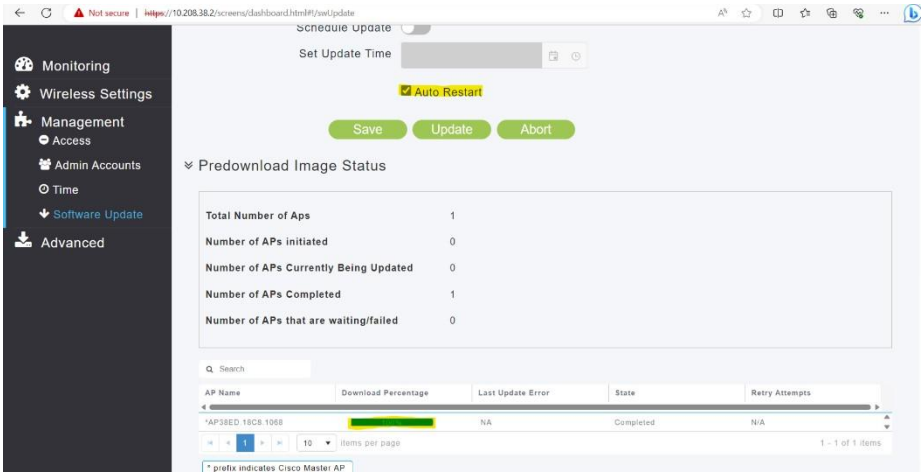
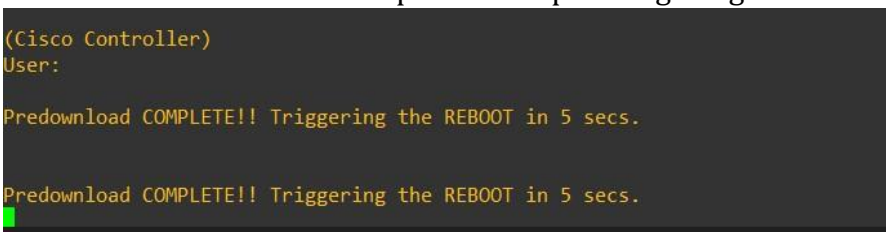


Image transfer completed 100%.

- DUT auto restart after completion of uploading image to DUT.



- DUT starts boot process automatically.

Continue booting process.

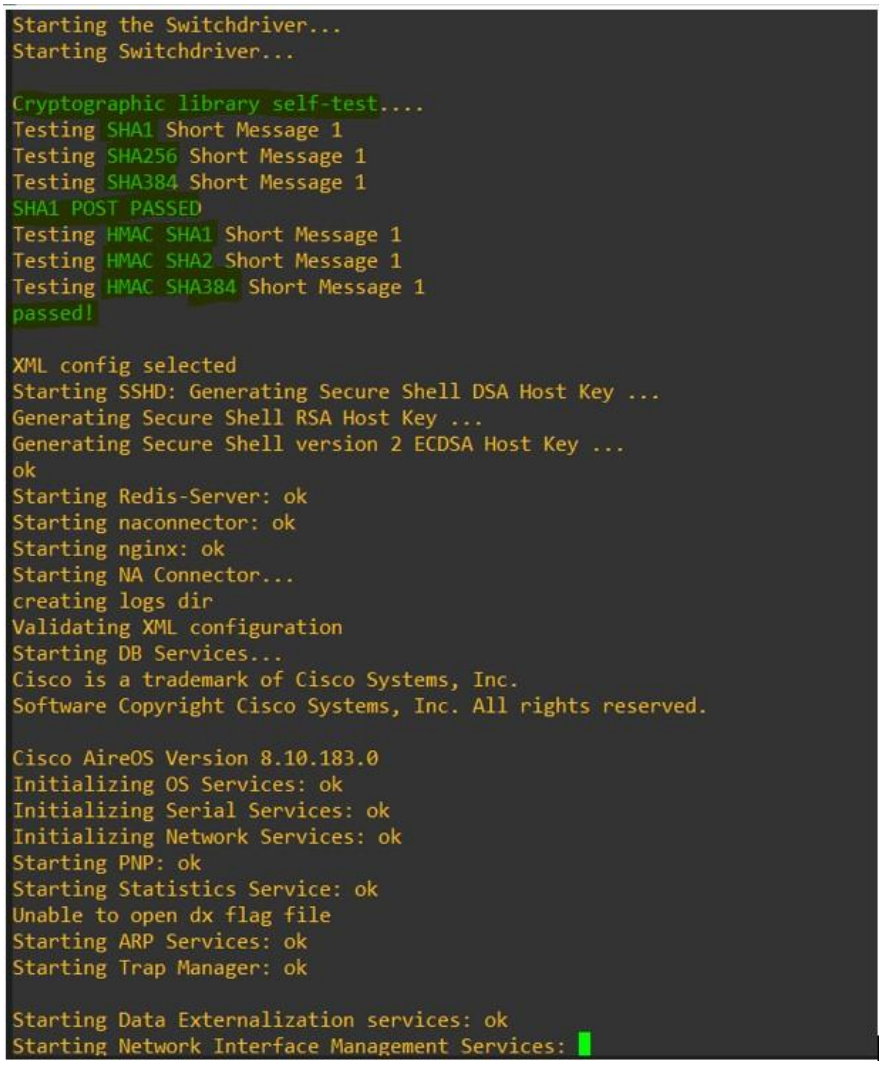
```
[  OK  ] Removed slice system.slice.
[  OK  ] Reached target Shutdown.
[09/13/2023 08:09:12.2512] sysctl link missing during unregister: /net/ipv4/neigh//vlan0
[09/13/2023 08:09:12.3311] sysctl link missing during unregister: /net/ipv6/neigh//vlan0
[09/13/2023 08:09:12.4211] sysctl link missing during unregister: /net/ipv4/neigh//vlan1
[09/13/2023 08:09:12.5111] sysctl link missing during unregister: /net/ipv6/neigh//vlan1
[09/13/2023 08:09:12.6510] sysctl link missing during unregister: /net/ipv4/neigh//vlan2
[09/13/2023 08:09:12.7310] sysctl link missing during unregister: /net/ipv6/neigh//vlan2
[09/13/2023 08:09:12.8210] Restarting system.
[09/13/2023 08:09:12.8210] sysctl link missing during unregister: /net/ipv4/neigh//vlan3
[09/13/2023 08:09:12.8210] sysctl link missing during unregister: /net/ipv6/neigh//vlan3


U-Boot 2012.07 (btldr release 41) (Jan 05 2021 - 13:03:00)

This product contains some software licensed under the
"GNU General Public License, version 2" provided with
ABSOLUTELY NO WARRANTY under the terms of
"GNU General Public License, version 2", available here:
http://www.gnu.org/licenses/old-licenses/gpl-2.0.html

DRAM:  1 GiB
NAND (ONFI): Detected SPANSION S34MS02G1 [256 MiB]
SF: Detected Macronix MX25U3235F [4 MiB]
MFG data loaded
Scanning shenv data blocks
Total valid parts=4
Active shenv part[1:0], write_counter=27
PCI0 Link Intialized
PCI1 Link Intialized
Net:
PHY ID = 0x4dd074, eth0 found AR8033 PHY
PHY ID = 0x4dd074, eth1 found AR8033 PHY
Valid I2C chip addresses: 51 52
AP 1832/1852 detected...
Power Type: 802.3af POE or Others detected...
Signature returns 0
BL signing verification success, continue to run...
Auto boot mode, use bootipq directly
Hit ESC key to stop autoboot:  4
```

- DUT performing Image Signing verification while booting to new image.

```
PHY ID = 0x4dd074, eth0 found AR8033 PHY
PHY ID = 0x4dd074, eth1 found AR8033 PHY
Valid I2C chip addresses: 51 52
AP 1832/1852 detected...
Power Type: 802.3af POE or Others detected...
Signature returns 0
BL signing verification success, continue to run...
Auto boot mode, use bootipq directly
Hit ESC key to stop autoboot:  0
Specified BOOT: part2

Booting from part2

Read 1024 bytes from volume part2 to 45000000
Read 63274950 bytes from volume part2 to 45000000
Signature returns 0
Image signing verification success, continue to run...
Using machid 0x1260 from environment

Starting image ...
```

Here it has been observed that image signing verification is success of the new image which means it is valid image and continue to run then continue to “starting image”.

- Here DUT performing Cryptographic checks while starting image process –



In above screenshot it has been observed that cryptographic library self-test passed!

Tested cryptographic library are - sha1, sha256, sha384, hmac-Sha1, hmac-sha256, hmac-sha384.

- After successful update/upgrade of the image and completion of all booting process DUT ask for login to controller with “enter username “dialog.

```
Starting Virtual AP Services: ok
Starting AireWave Director: open rrm: not able to ipv4 by pass rule ok
Starting Network Time Services: ok
Starting Cisco Discovery Protocol: ok
Starting Broadcast Services: ok
Starting Logging Services: ok
Starting DHCP Server: ok
Starting IDS Signature Manager: ok
Starting RFID Tag Tracking: ok
Starting RF Profiles: ok
Starting Mesh Services:  ok
Starting TSM: ok
Starting CIDS Services: ok
Starting DTLS server:  enabled in CAPWAP
Starting CleanAir: ok
Starting WIPS: ok
Starting SSHPM LSC PROV LIST: ok
Starting RRC Services: ok
Starting Alarm Services: ok
Starting FMC HS: ok
Starting FLEXEXPRESS ConfigSync Task: ok
Starting Hotspot Services: ok
Starting HTTP Image Download Task: ok
Starting Tunnel Services New: ok
Starting mDNS Services: ok
Starting Management Services:
Starting IPSec Profiles component: ok
   Web Server:    CLI:    Secure Web: ok

(Cisco Controller)

Enter User Name (or 'Recover-Config' this one-time only to reset configuration to factory defaults)

User:  Admin
Password:*********
 Warning: Missing TFTP/CCO params, Please Configure the Image Download Params

Welcome to the Cisco Mobility Express command line interface.
Only commands which are listed in the command reference guide for this release are supported.
http://www.cisco.com/c/en/us/support/wireless/mobility-express/products-command-reference-list.html

Warning:In SNMPV2 No Defaults Presents.
Please use command: config snmp community create <name>

Warning:In SNMPV3 No Defaults Presents.
Please use command: config snmp v3user create <username>

(Cisco Controller) >
```

Logged-in with user “Admin.”

Verifying the version of the Image on controller after login with user Admin:

Verifying sysinfo of the controller via console.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.10.185.0
OUI File Last Update Time........................ N/A

System Name...................................... Cisco-Aironet-Controller
System Location.................................
System Contact..................................
System ObjectID.................................. 1.3.6.1.4.1.9.1.2250
IP Address....................................... 10.208.38.2
Last Reset....................................... 0: unknown

System Up Time................................... 0 days 8 hrs 13 mins 46 secs
System Timezone Location........................
System Stats Realtime Interval................... 5
System Stats Normal Interval..................... 180

Configured Country............................... AL  - Albania

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
Number of WLANs.................................. 1

--More-- or (q)uit
```

Continue sysinfo

```
--More-- or (q)uit
Number of Active Clients..................... 0

OUI Classification Failure Count.............. 0

Memory Current Usage......................... 67
Memory Average Usage......................... 67
CPU Current Usage............................ 2
CPU Average Usage............................ 3

Flash Type................................... Compact Flash Card
Flash Size................................... 1073741824

Burned-in MAC Address........................ 38:ED:18:C8:10:60
Maximum number of APs supported.............. 50
System Nas-Id.....................................
WLC MIC Certificate Types.................... SHA1/SHA2

(Cisco Controller) >?
```

Here it has been observed that WLC-MIC certificate type is SHA1/SHA2

Verifying the running configuration on the controller with the following command: Cmd: Show running-config on controller.

```
(Cisco Controller) >show running-config

Notice: "show running-config" has been changed to be an alias to "show run-config".
Use "show run-config commands" to display the configuration commands.
Press Enter to continue or <Ctrl-Z> to abort...

System Inventory
NAME: "Mobility Express"    , DESCR: "Cisco Aironet 1850 Series Mobility Express"
PID: AIR-AP1852I-E-K9,  VID: V01,  SN: KWC193100UU

Burned-in MAC Address........................ 38:ED:18:C8:10:60
Maximum number of APs supported.............. 50
Press Enter to continue or <ctrl-z> to abort


System Information
Manufacturer's Name.......................... Cisco Systems Inc.
Product Name................................. Cisco Controller
Product Version.............................. 8.10.185.0
OUI File Last Update Time.................... N/A

System Name.................................. Cisco-Aironet-Controller
System Location...............................
System Contact................................
System ObjectID.............................. 1.3.6.1.4.1.9.1.2250
IP Address................................... 10.208.38.2
```

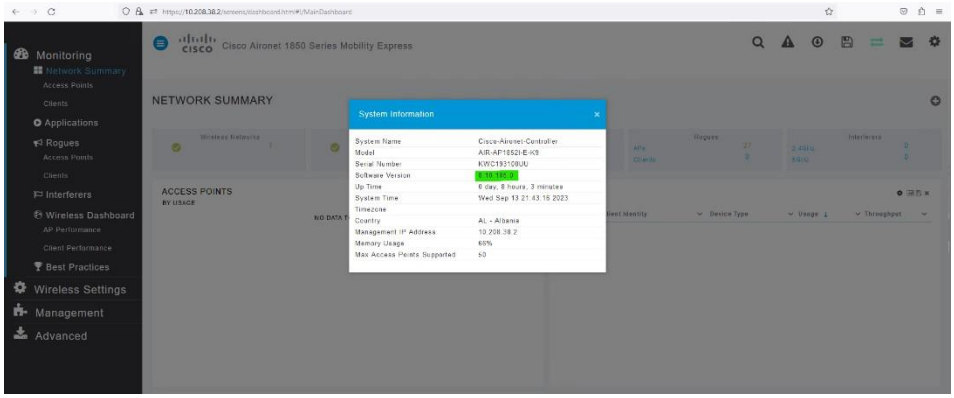
Here it has been observed that product version has been change. Now it is 8.10.185.0 (earlier it was 8.10.183 which can be verified in DUT confirmation details).

- Verification of image in AP mode:

```
cisco AIR-AP1852I-E-K9 ARMv7 Processor rev 0 (v71) with 996240/375964K bytes of memory.
Processor board ID KWC193100UU
AP Running Image     : 8.10.185.0
Primary Boot Image   : 8.10.185.0
Backup Boot Image    : 8.10.183.0
Primary Boot Image Hash: 6a09c7457bff3593d756fbca11edc2c8b79472c11ca9cd22b402c9253e964982acb47ecd9509cd11fd3c6b792da9fb39786746a90964014a3066aa5b7902c24c
Backup  Boot Image Hash:
AP Image type    : MOBILITY EXPRESS IMAGE
AP Configuration : MOBILITY EXPRESS CAPABLE
2 Gigabit Ethernet interfaces
2 802.11 Radios
Radio FW version : f39e59654a44b14dbeedf2603bab9cd0
NSS FW version : NSS.AK.C.CS-3-fix5

Base ethernet MAC Address          : 38:ED:18:C8:10:68
Part Number                        : 0-0000-00
PCA Assembly Number                : 074-13149-01
PCA Revision Number                : 01
PCB Serial Number                  : KWC193100UU
Top Assembly Part Number           : 000-00000-00
Top Assembly Serial Number         : KWC193100UU
Top Revision Number                : A0
Product/Model Number               : AIR-AP1852I-E-K9


CiscoAP1852i#
```

It has been observed that 8.10.183.0 becomes now a backup image after update/upgrade.

- Verifying on Web gui.

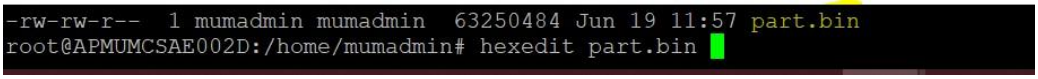


System information of the DUT.

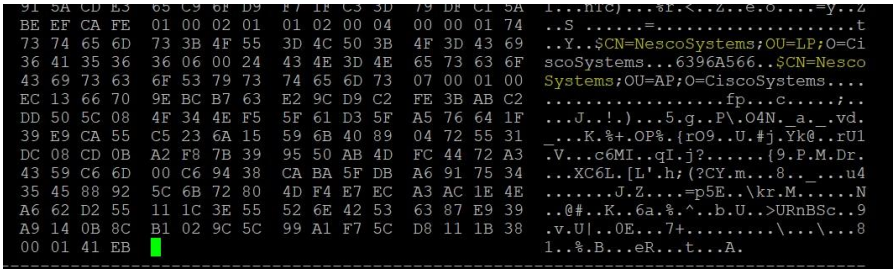
The image of the DUT successfully updated after cryptographic check of the new image. Now product version is 8.10.185.0 (earlier, before update, it was 8.10.183.0).

Case2: Negative testcase – (note: this test performed earlier before updating the image)

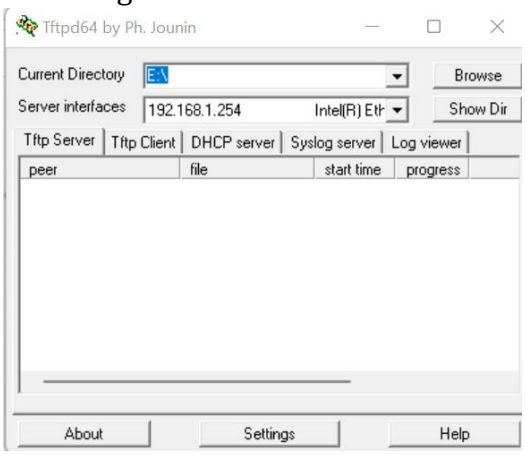
- copy the boot image (part.bin) from DUT to terminal for tampering.



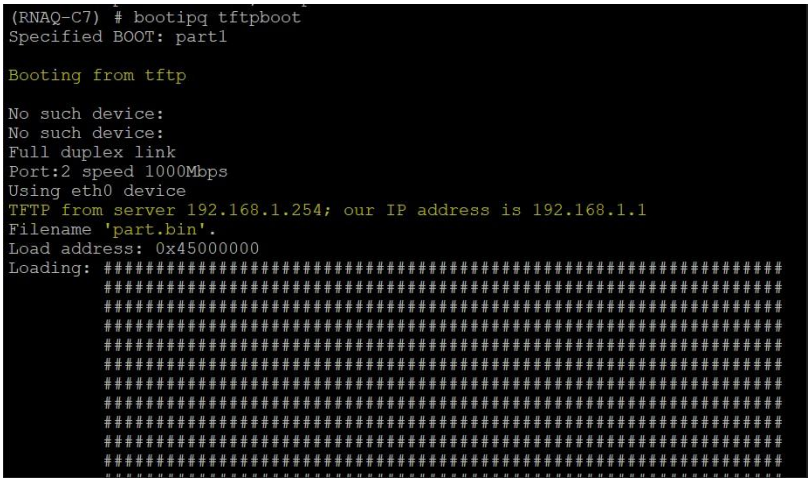
- Run Hexeditor of terminal machine and change certificate values in the boot image.



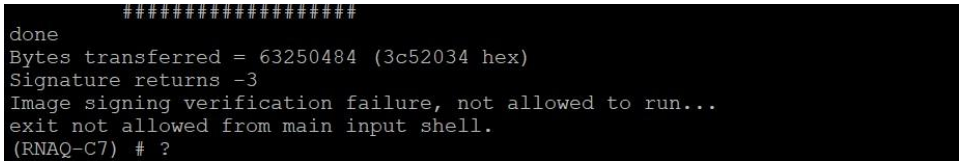
▪ After editing save the edited image and reboot the device with the tampered boot image over TFTP.



Updating from rommon mode require ip to be change of TFTP server as per DUT ask for it.



▪ Verify the integrity of the boot image manually by command. Device failed to load the tampered image giving error message as Image signing verification failed.



It has been observed that image signing verification of corrupted image return gives signature return "-3" means verification is failed. So it can be concluded that given image is not a valid image.

11.1.4 **Test Observations:**

- **Case1: Positive Test Case**
  - The TFTP server settings were configured and the image to be updated was selected. The DUT settings were adjusted, but an error occurred when attempting to update with a user that only had read-only privileges. After logging in as an admin with read-write privileges, the image transfer from the TFTP server to the DUT began. The DUT automatically restarted after the image transfer was completed. During the booting process, the DUT performed image signing verification and cryptographic checks. After successful login, the new image

version was verified on the controller. The image was also verified in AP mode and on the Web GUI.

- **Case2: Negative Test Case**
  - The boot image was copied from the DUT to the terminal for tampering. After editing and saving the image, the device was rebooted with the tampered boot image over TFTP. The integrity of the boot image was manually verified, and the device failed to load the tampered image, indicating that image signing verification had failed.

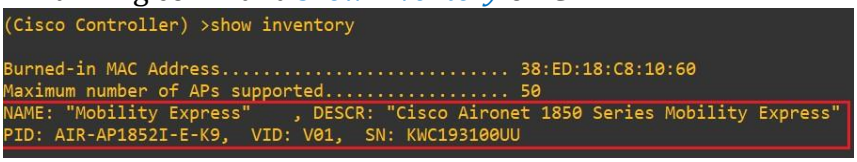
12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_SECURE_UPDATE	FAIL	

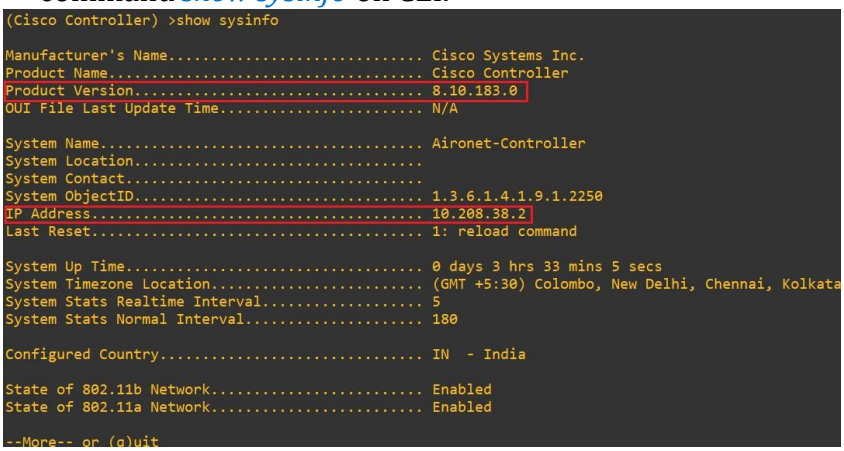
1.3.2 Secure Upgrade

<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 3 - Software Security
2. **<Security Requirement No & Name >** 1.3.2 Secure Upgrade
3. **<Requirement Description: >** CPE should support authenticity and integrity check while performing software upgrade Preferably employing Digital Certificate for authenticity and hashing (example: SHA2) for integrity software patching.
4. **DUT Confirmation Details**:
   - This section involves information about DUT like software/firmware version, Hardware version model.
   - DUT Cisco WLC contains default boot image with version 8.10.183.0. The model is AIRAP1852I-E-K9. The inventory shows model serial no. & model description.
   - Verification of DUT Cisco wireless LAN controller's HW product series information by running command *show inventory* on CLI.



   - Verification of DUT Cisco WLC's high-level system SW information by running command *show sysinfo* on CLI.

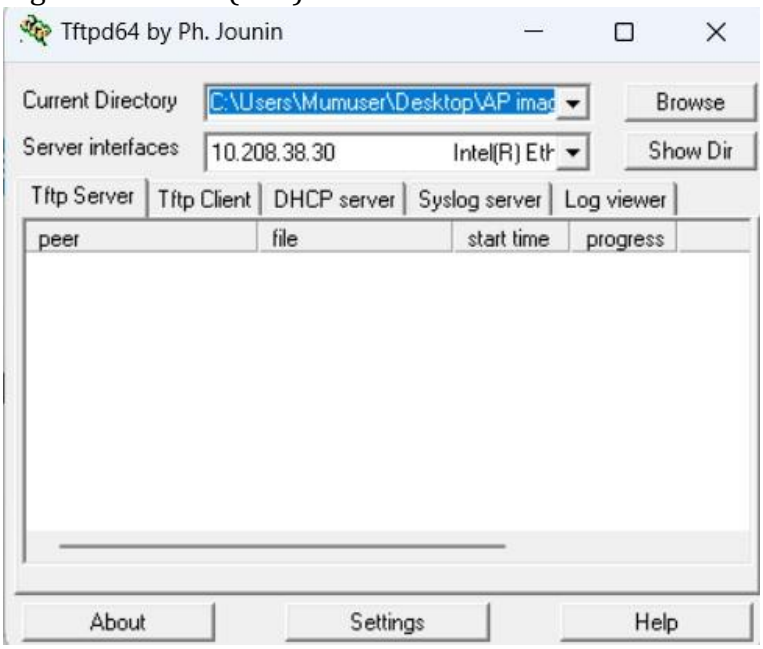


   - Verification of DUT Cisco WLC's system information on Web access.

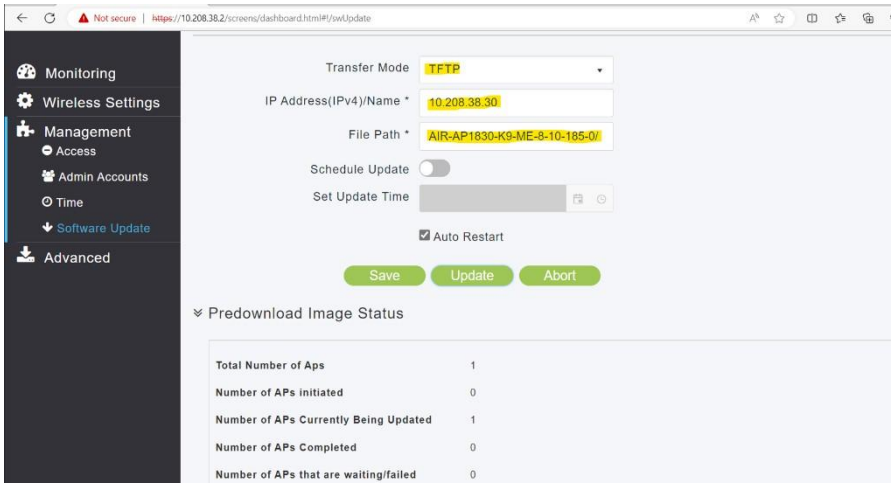
5. **<u>DUT Configuration</u>**: Configuration of DUT as per this test:

Case1: positive test case –

- Selecting TFTP server (tool) interface



- Settings are given below to Upgrade/upgrade image of the DUT.



6. Preconditions:

- A document containing information regarding the following:
- software package integrity checks.
- Including details of how the integrity check is carried out.
- Where public keys or certificates of sources authorized to sign software packages are stored on the DUT and who these sources are.
- What evidence is created to prove that the integrity check has been executed and what the result of the check was.
- Documentation which describes the installation procedure including how a user is authorized and authenticated to perform installation process.
- Valid package for installation/boot and one tampered image (tampered with hex edit).
- Hex Editor for modifying the DUT Image. - TFTP server for image transfer - Valid package for installation/boot.
- A network product document containing information regarding software package integrity checks, including details of how the integrity check is carried out.
- A valid network product software load/package and one that is not-valid.

7. Test Objective:

To verify that DUT have mechanism that validates the software package integrity during installation/Upgrade stage

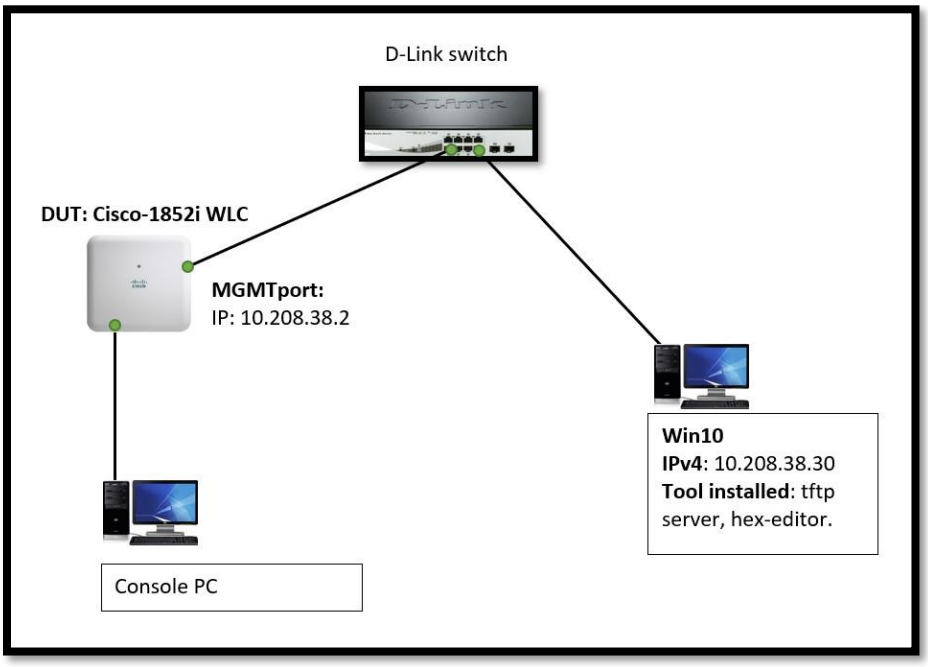
8. Test Plan:

- Software package integrity shall be validated in the installation/upgrade stage.
- Network product shall support software package integrity validation via cryptographic means, e.g. Digital Certificate(digital signature). To this end, the network product has a list of public keys or certificates of authorised software sources, and uses the keys to verify that the software Upgrade is originated from only these sources.
- Tampered software shall not be executed or installed if integrity check fails.
- A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software Upgrade, and modify the list mentioned in bullet 2.

8.1 Number of Test Scenarios:

8.1.1 Software Upgrade in DUT verifying the integrity and using digital certificate/public keys

8.2 **Test Setup Diagram**



8.3 **Tools Used:** Web browser(client) Win10, tftp-server, hex-editor, putty for console.

8.4 **Test Execution Steps:**

Below are the execution steps with evidence:

Case1: Positive testcase –

- The settings on tool i.e., TFTP server - Selecting image to be Upgraded.
- Settings On DUT:
- Now login as user1 (ReadOnly privilege)
- Verifying user1 can't Upgrade/upgrade the image of DUT.
- Now login with Admin (ReadWrite privilege)
- Settings are given below to Upgrade/upgrade image of the DUT. (Current iOS image version is 8.10.183.0).
- After clicking on Upgrade transfer of image from TFTP to DUT starts - verification of image transfer on TFTP server.

- Uploading of image to DUT from TFTP server completed.
  - DUT auto restarts after completion of uploading image to DUT.
  - DUT starts boot process automatically.
  - DUT performing Image Signing verification while booting to new image.
  - DUT performing Cryptographic checks while starting image process –
  - Verifying the version of the DUT Image Upgraded – on controller after login with user Admin on console and GUI.

Case2: Negative testcase – (note: this test performed earlier before updating the image) - copy the boot image (part.bin) from DUT to terminal for tampering.

- Run Hexeditor of terminal machine and change certificate values in the boot image.
- After editing save the edited image and reboot the device with the tampered boot image over TFTP.
- Updating from rommon mode require IP to be change of TFTP server as per DUT ask for it.
- Verify the integrity of the boot image manually by command. Device failed to load the tampered image giving error message as Image signing verification failed.

9. **Expected Result for Pass:** Software package integrity shall be validated using cryptographic means, e.g. digital certificate in the installation/upgrade stage. Tampered software shall not be executed or installed if integrity check fails. Only authorized person, can able to do software Upgrade.
10. **Expected Format of Evidence:** Screenshot of DUT webpage and terminal

11. **Test Execution:**

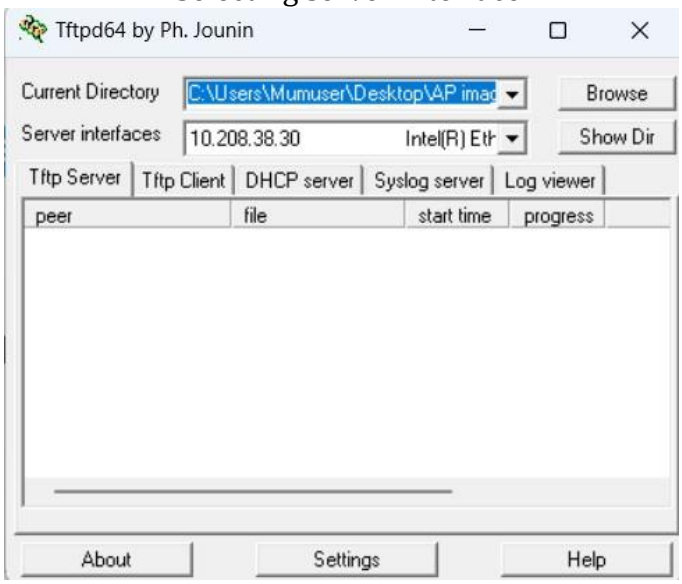
11.1.1 **Test Case Number:** 01
11.1.2 **Test Case Name:** TC_NO_SECURE_UPGRADE
11.1.3 **Test Case Description:** In this test scenario tester will perform the positive test to Upgrade/upgrade the DUT image using the TFTP server and DUT settings were configured for an image Upgrade. The Upgrade will be verified by low privilege user and highest privilege user also image signing verification and cryptographic library will be checks during Upgrade/upgrade on console. In the negative test, tester will try to Upgrade on DUT and observed the process will get fail or not for image signing verification.
11.1.4 **Execution Steps:**

Below are the execution steps with evidence:

Case1: Positive testcase –

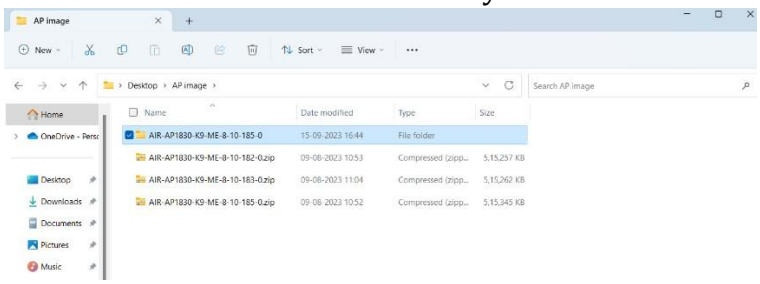
Below are the settings on tool i.e., TFTP server:

Selecting server interface

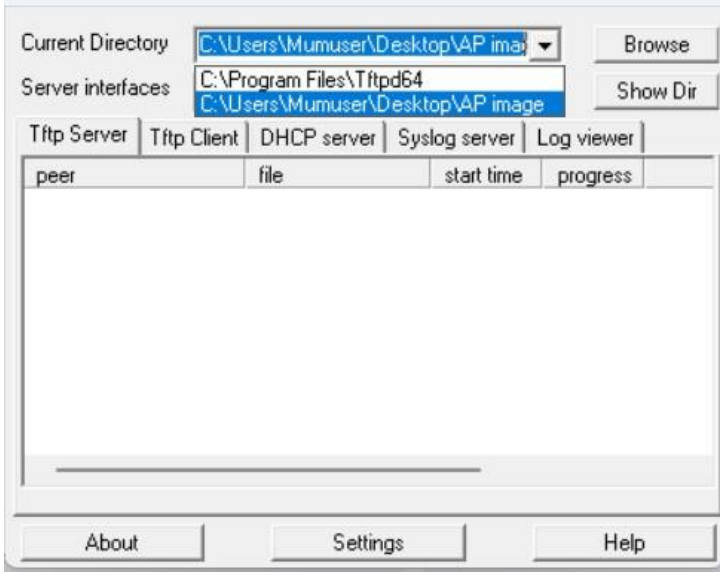


Selecting image to be Upgraded.

Browse to the directory where the new image downloaded.

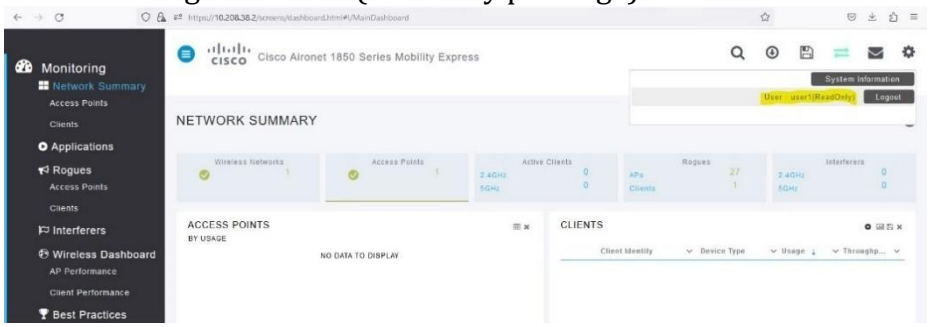


Browse correct path in current directory of TFTP server.

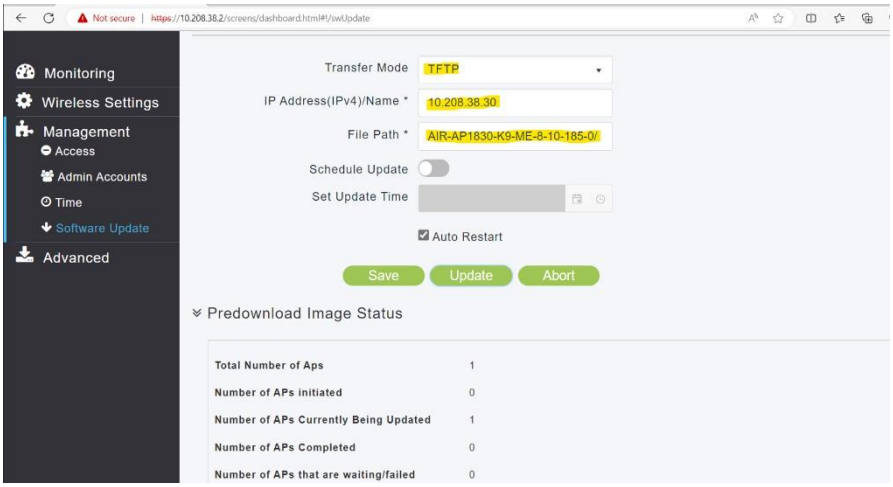


Settings On DUT:

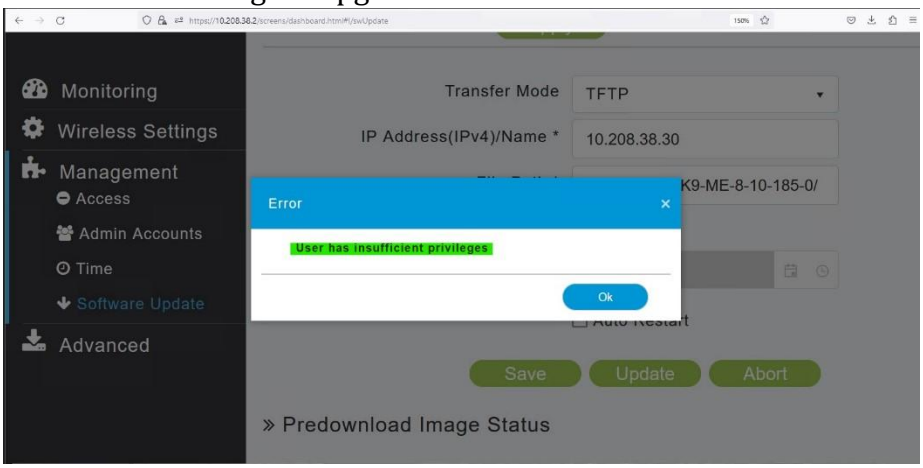
First Login as user1 (ReadOnly privilege)



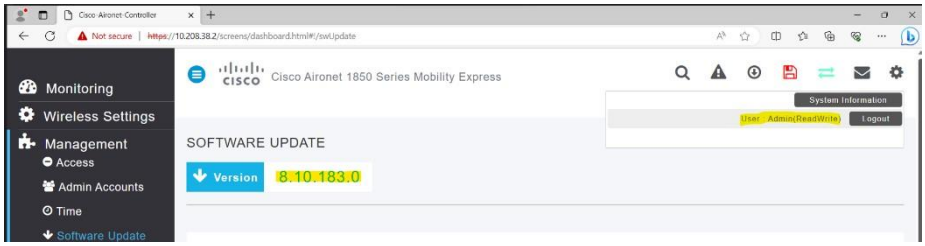
Settings are given below to Upgrade/upgrade image of the DUT.



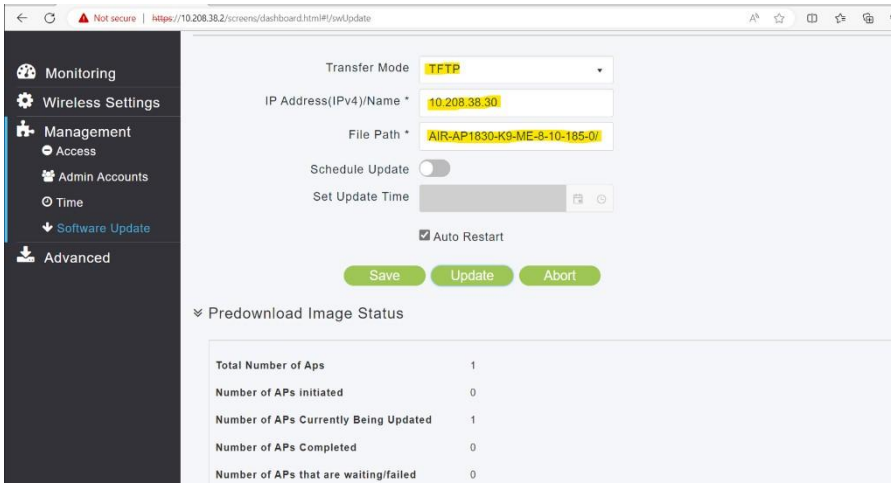
- After clicking on Upgrade error occurs.



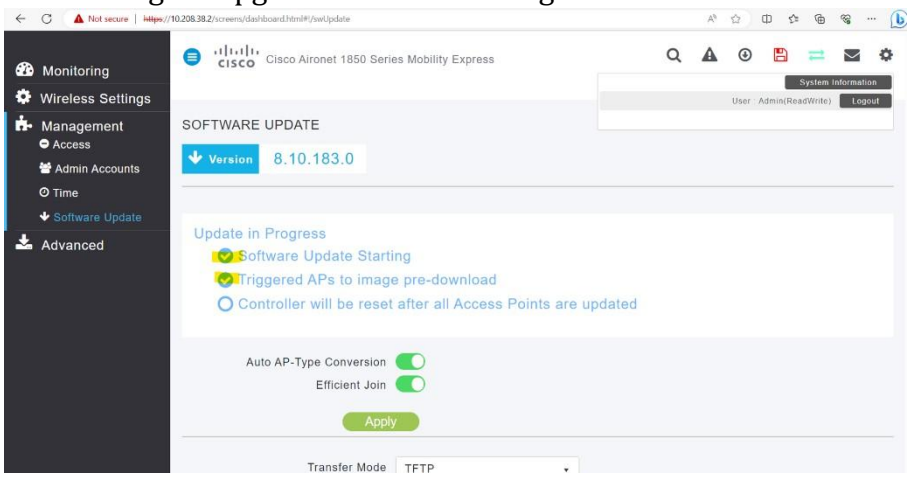
- Here it has been observed that User – “user1” does not have Readwrite privilege so can’t Upgrade/upgrade. So, “insufficient privilege error occurred.
- Note: Only users with Read-write privilege can Upgrade/Upgrade iOS image of DUT.
- Now login as Admin (ReadWrite privilege)



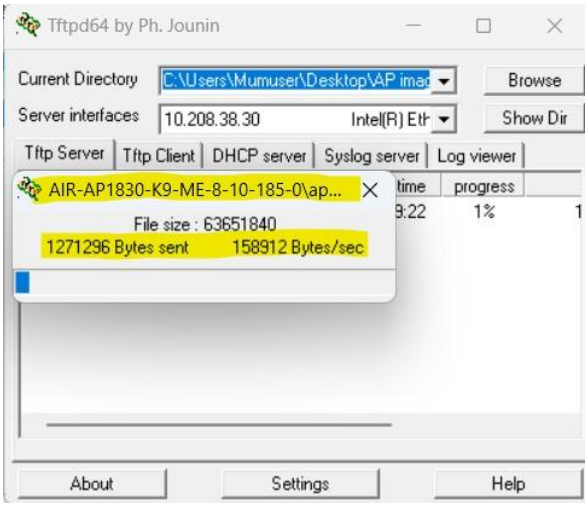
- Settings are given below to Upgrade/upgrade image of the DUT. (Current iOS image version is 8.10.183.0).



After clicking on Upgrade transfer of image from TFTP to DUT starts

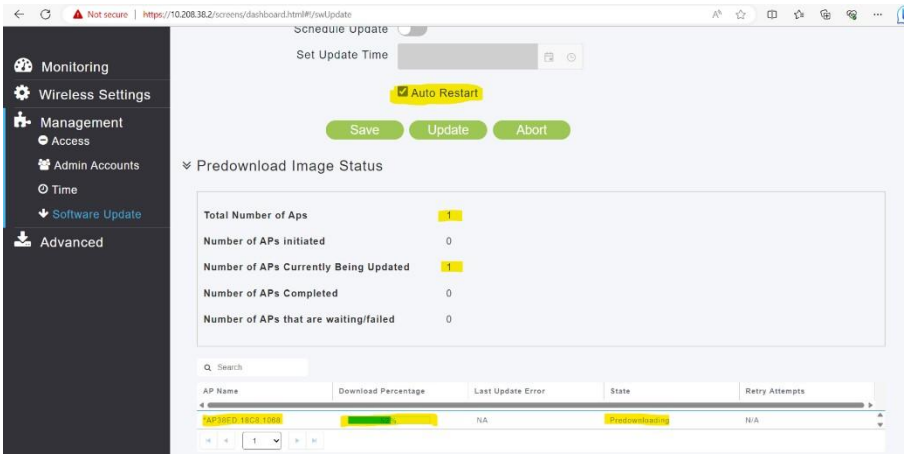


On TFTP server



On tftp server it is seen that transfer of image from TFTP server to DUT has been started. Till this step it can be concluded that only Admin (mgmtuser with highest level of access i.e., read-write privilege)

- After some time on DUT- uploading progress is more than 50%



Here it can be noted that "Auto restart" is checked which means DUT auto restart after completion of image transfer to DUT.

Uploading of image to DUT from TFTP server completed.

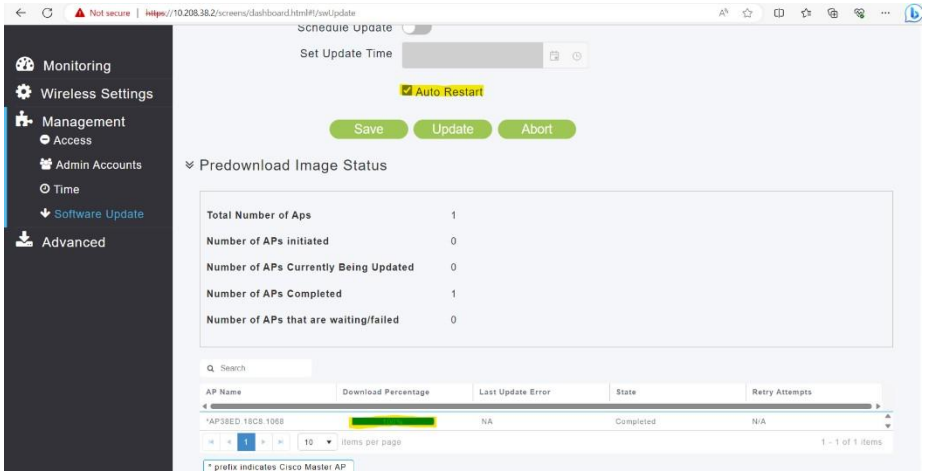
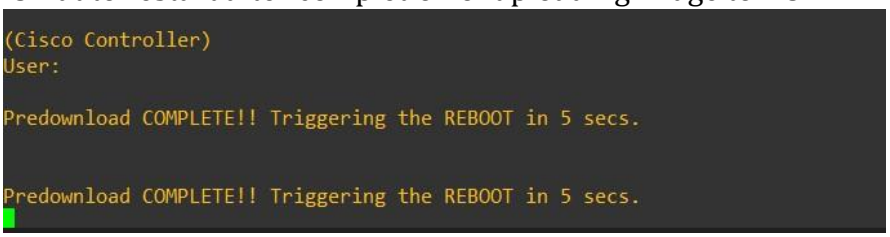


Image transfer completed 100%.

DUT auto restart after completion of uploading image to DUT.



DUT starts boot process automatically.

Continue booting process.

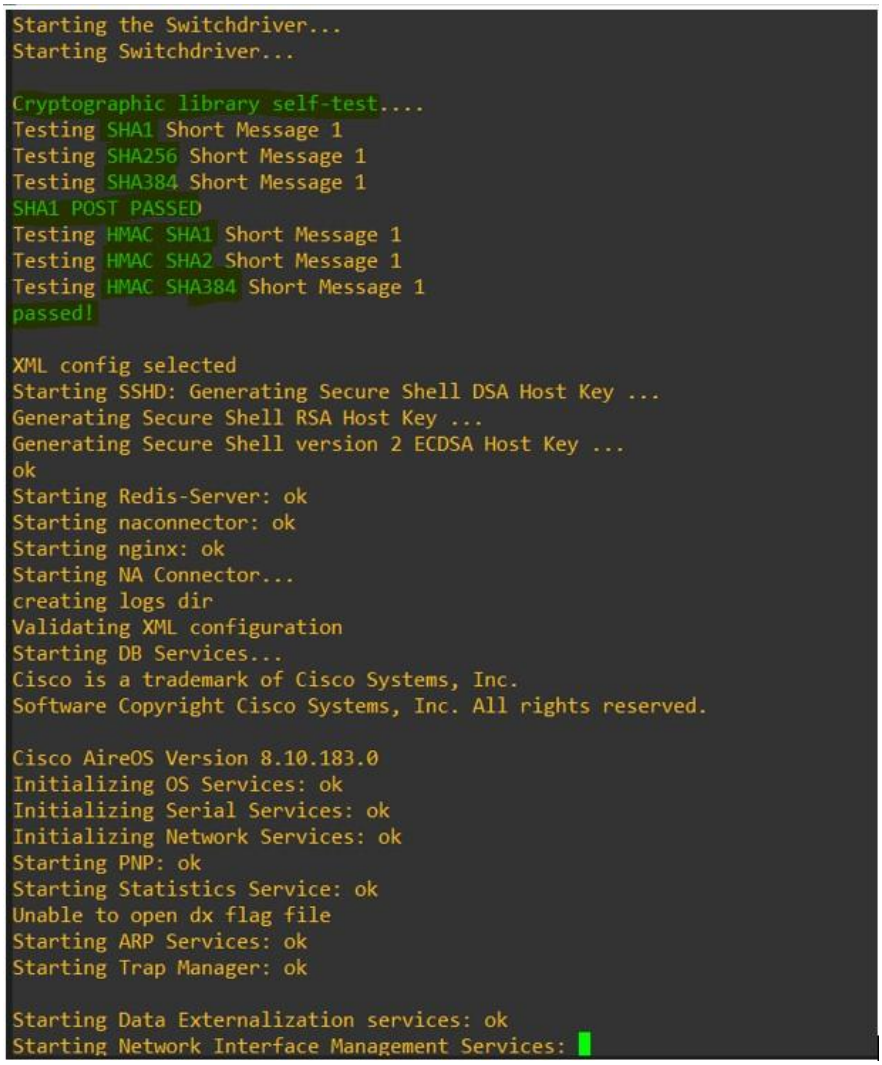
```
[  OK  ] Removed slice system.slice.
[  OK  ] Reached target Shutdown.
[09/13/2023 08:09:12.2512] sysctl link missing during unregister: /net/ipv4/neigh//vlan0
[09/13/2023 08:09:12.3311] sysctl link missing during unregister: /net/ipv6/neigh//vlan0
[09/13/2023 08:09:12.4211] sysctl link missing during unregister: /net/ipv4/neigh//vlan1
[09/13/2023 08:09:12.5111] sysctl link missing during unregister: /net/ipv6/neigh//vlan1
[09/13/2023 08:09:12.6510] sysctl link missing during unregister: /net/ipv4/neigh//vlan2
[09/13/2023 08:09:12.7310] sysctl link missing during unregister: /net/ipv6/neigh//vlan2
[09/13/2023 08:09:12.8210] Restarting system.
[09/13/2023 08:09:12.8210] sysctl link missing during unregister: /net/ipv4/neigh//vlan3
[09/13/2023 08:09:12.8210] sysctl link missing during unregister: /net/ipv6/neigh//vlan3


U-Boot 2012.07 (btldr release 41) (Jan 05 2021 - 13:03:00)

This product contains some software licensed under the
"GNU General Public License, version 2" provided with
ABSOLUTELY NO WARRANTY under the terms of
"GNU General Public License, version 2", available here:
http://www.gnu.org/licenses/old-licenses/gpl-2.0.html

DRAM:  1 GiB
NAND (ONFI): Detected SPANSION S34MS02G1 [256 MiB]
SF: Detected Macronix MX25U3235F [4 MiB]
MFG data loaded
Scanning shenv data blocks
Total valid parts=4
Active shenv part[1:0], write_counter=27
PCI0 Link Intialized
PCI1 Link Intialized
Net:
PHY ID = 0x4dd074, eth0 found AR8033 PHY
PHY ID = 0x4dd074, eth1 found AR8033 PHY
Valid I2C chip addresses: 51 52
AP 1832/1852 detected...
Power Type: 802.3af POE or Others detected...
Signature returns 0
BL signing verification success, continue to run...
Auto boot mode, use bootipq directly
Hit ESC key to stop autoboot:  4
```

DUT performing Image Signing verification while booting to new image.

```
PHY ID = 0x4dd074, eth0 found AR8033 PHY
PHY ID = 0x4dd074, eth1 found AR8033 PHY
Valid I2C chip addresses: 51 52
AP 1832/1852 detected...
Power Type: 802.3af POE or Others detected...
Signature returns 0
BL signing verification success, continue to run...
Auto boot mode, use bootipq directly
Hit ESC key to stop autoboot:  0
Specified BOOT: part2

Booting from part2

Read 1024 bytes from volume part2 to 45000000
Read 63274950 bytes from volume part2 to 45000000
Signature returns 0
Image signing verification success, continue to run...
Using machid 0x1260 from environment

Starting image ...
```

Here it has been observed that image signing verification is success of the new image which means it is valid image and continue to run then continue to “starting image”.

Here DUT performing Cryptographic checks while starting image process –



In above screenshot it has been observed that cryptographic library self-test passed! Tested cryptographic library are - sha1, sha256, sha384, hmac-Sha1, hmac-sha256, hmac-sha384.

After successful Upgrade/upgrade of the image and completion of all booting process DUT ask for login to controller with “enter username “dialog.

```
Starting Virtual AP Services: ok
Starting AireWave Director: open rrm: not able to ipv4 by pass rule ok
Starting Network Time Services: ok
Starting Cisco Discovery Protocol: ok
Starting Broadcast Services: ok
Starting Logging Services: ok
Starting DHCP Server: ok
Starting IDS Signature Manager: ok
Starting RFID Tag Tracking: ok
Starting RF Profiles: ok
Starting Mesh Services:  ok
Starting TSM: ok
Starting CIDS Services: ok
Starting DTLS server:  enabled in CAPWAP
Starting CleanAir: ok
Starting WIPS: ok
Starting SSHPM LSC PROV LIST: ok
Starting RRC Services: ok
Starting Alarm Services: ok
Starting FMC HS: ok
Starting FLEXEXPRESS ConfigSync Task: ok
Starting Hotspot Services: ok
Starting HTTP Image Download Task: ok
Starting Tunnel Services New: ok
Starting mDNS Services: ok
Starting Management Services:
Starting IPSec Profiles component: ok
   Web Server:    CLI:    Secure Web: ok

(Cisco Controller)

Enter User Name (or 'Recover-Config' this one-time only to reset configuration to factory defaults)

User:  Admin
Password:*********
 Warning: Missing TFTP/CCO params, Please Configure the Image Download Params

Welcome to the Cisco Mobility Express command line interface.
Only commands which are listed in the command reference guide for this release are supported.
http://www.cisco.com/c/en/us/support/wireless/mobility-express/products-command-reference-list.html

Warning:In SNMPV2 No Defaults Presents.
Please use command: config snmp community create <name>

Warning:In SNMPV3 No Defaults Presents.
Please use command: config snmp v3user create <username>

(Cisco Controller) >
```

Logged-in with user “Admin.”

Verifying the version of the Image on controller after login with user Admin:

Verifying sysinfo of the controller via console.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.10.185.0
OUI File Last Update Time........................ N/A

System Name...................................... Cisco-Aironet-Controller
System Location.................................
System Contact..................................
System ObjectID.................................. 1.3.6.1.4.1.9.1.2250
IP Address....................................... 10.208.38.2
Last Reset....................................... 0: unknown

System Up Time................................... 0 days 8 hrs 13 mins 46 secs
System Timezone Location........................
System Stats Realtime Interval................... 5
System Stats Normal Interval..................... 180

Configured Country............................... AL  - Albania

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
Number of WLANs.................................. 1

--More-- or (q)uit
```

Continue sysinfo

```
--More-- or (q)uit
Number of Active Clients..................... 0

OUI Classification Failure Count.............. 0

Memory Current Usage.......................... 67
Memory Average Usage.......................... 67
CPU Current Usage............................. 2
CPU Average Usage............................. 3

Flash Type.................................... Compact Flash Card
Flash Size.................................... 1073741824

Burned-in MAC Address......................... 38:ED:18:C8:10:60
Maximum number of APs supported.............. 50
System Nas-Id.................................
WLC MIC Certificate Types..................... SHA1/SHA2

(Cisco Controller) >?
```

Here it has been observed that WLC-MIC certificate type is SHA1/SHA2

Verifying the running configuration on the controller with the following command: Cmd: Show running-config on controller.

```
(Cisco Controller) >show running-config

Notice: "show running-config" has been changed to be an alias to "show run-config".
Use "show run-config commands" to display the configuration commands.
Press Enter to continue or <Ctrl-Z> to abort...

System Inventory
NAME: "Mobility Express"    , DESCR: "Cisco Aironet 1850 Series Mobility Express"
PID: AIR-AP1852I-E-K9,  VID: V01,  SN: KWC193100UU

Burned-in MAC Address......................... 38:ED:18:C8:10:60
Maximum number of APs supported.............. 50
Press Enter to continue or <ctrl-z> to abort


System Information
Manufacturer's Name........................... Cisco Systems Inc.
Product Name.................................. Cisco Controller
Product Version............................... 8.10.185.0
OUI File Last Update Time..................... N/A

System Name................................... Cisco-Aironet-Controller
System Location...............................
System Contact................................
System ObjectID............................... 1.3.6.1.4.1.9.1.2250
IP Address.................................... 10.208.38.2
```

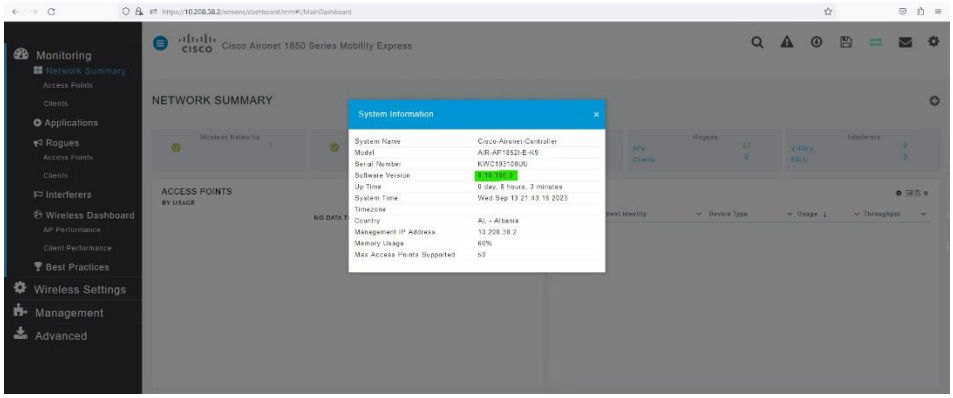
Here it has been observed that product version has been change. Now it is 8.10.185.0 (earlier it was 8.10.183 which can be verified in DUT confirmation details).

Verification of image in AP mode:

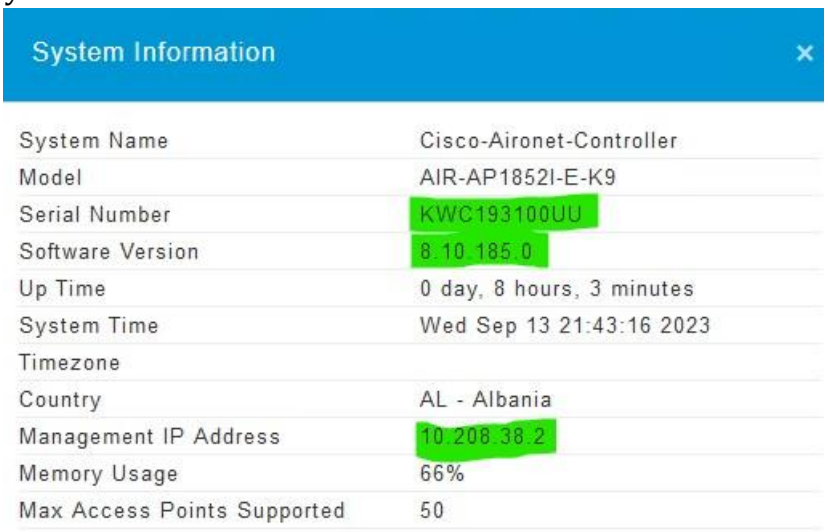
```
cisco AIR-AP1852I-E-K9 ARMv7 Processor rev 0 (v71) with 996240/375964K bytes of memory.
Processor board ID KWC193100UU
AP Running Image     : 8.10.185.0
Primary Boot Image   : 8.10.185.0
Backup Boot Image    : 8.10.183.0
Primary Boot Image Hash: 6a09c7457bff3593d756fbca11edc2c8b79472c11ca9cd22b402c9253e964982acb47ecd9509cd11fd3c6b792da9fb39786746a90964014a3066aa5b7902c24c
Backup  Boot Image Hash:
AP Image type    : MOBILITY EXPRESS IMAGE
AP Configuration : MOBILITY EXPRESS CAPABLE
2 Gigabit Ethernet interfaces
2 802.11 Radios
Radio FW version : f39e59654a44b14dbeedf2603bab9cd0
NSS FW version : NSS.AK.C.CS-3-fix5

Base ethernet MAC Address          : 38:ED:18:C8:10:68
Part Number                        : 0-0000-00
PCA Assembly Number                : 074-13149-01
PCA Revision Number                : 01
PCB Serial Number                  : KWC193100UU
Top Assembly Part Number           : 000-00000-00
Top Assembly Serial Number         : KWC193100UU
Top Revision Number                : A0
Product/Model Number               : AIR-AP1852I-E-K9


CiscoAP1852i#
```

It has been observed that 8.10.183.0 becomes now a backup image after Upgrade/upgrade.

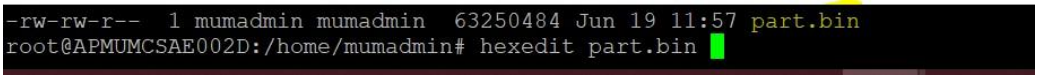
Verifying on Web gui.



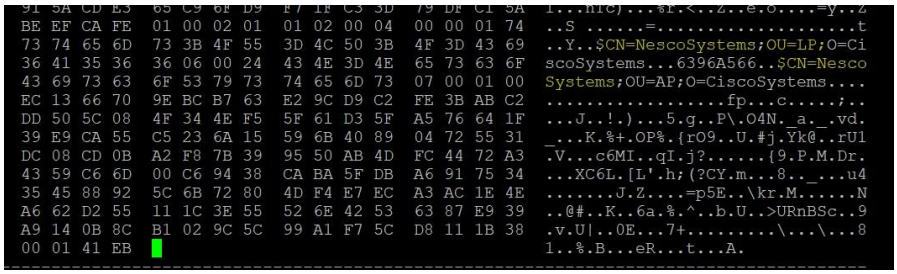
System information of the DUT.



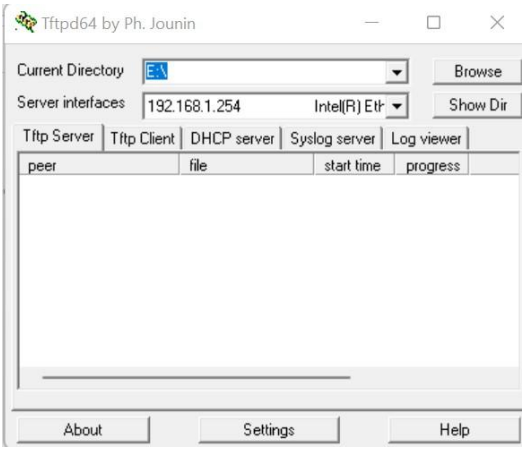
The image of the DUT successfully Upgraded after cryptographic check of the new image. Now product version is 8.10.185.0 (earlier, before Upgrade, it was 8.10.183.0).
Case2: Negative testcase – (note: this test performed earlier before updating the image) copy the boot image (part.bin) from DUT to terminal for tampering.



Run Hexeditor of terminal machine and change certificate values in the boot image.



After editing save the edited image and reboot the device with the tampered boot image over TFTP.



Updating from rommon mode require ip to be change of TFTP server as per DUT ask for it.

```
(RNAQ-C7) # bootipq tftpboot
Specified BOOT: part1

Booting from tftp

No such device:
No such device:
Full duplex link
Port:2 speed 1000Mbps
Using eth0 device
TFTP from server 192.168.1.254; our IP address is 192.168.1.1
Filename 'part.bin'.
Load address: 0x45000000
Loading: ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
```

Verify the integrity of the boot image manually by command. Device failed to load the tampered image giving error message as Image signing verification failed.

```
         ##################
done
Bytes transferred = 63250484 (3c52034 hex)
Signature returns -3
Image signing verification failure, not allowed to run...
exit not allowed from main input shell.
(RNAQ-C7) # ?
```

It has been observed that image signing verification of corrupted image return gives signature return “-3” means verification is failed. So it can be concluded that given image is not a valid image.

11.1.5 **Test Observations:**

- **Case1: Positive Test Case**
  The TFTP server settings were configured and the image to be Upgraded was selected. The DUT settings were adjusted, but an error occurred when attempting to Upgrade with a user that only had read-only privileges. After logging in as an admin with read-write privileges, the image transfer from the TFTP server to the DUT began. The DUT automatically restarted after the image transfer was completed. During the booting process, the DUT performed image signing verification and cryptographic checks. After successful login, the new image version was verified on the controller. The image was also verified in AP mode and on the Web GUI.
- **Case2: Negative Test Case**

The boot image was copied from the DUT to the terminal for tampering. After editing and saving the image, the device was rebooted with the tampered boot image over TFTP. The integrity of the boot image was manually verified, and the device failed to load the tampered image, indicating that image signing verification had failed.

12. Test Case Result:

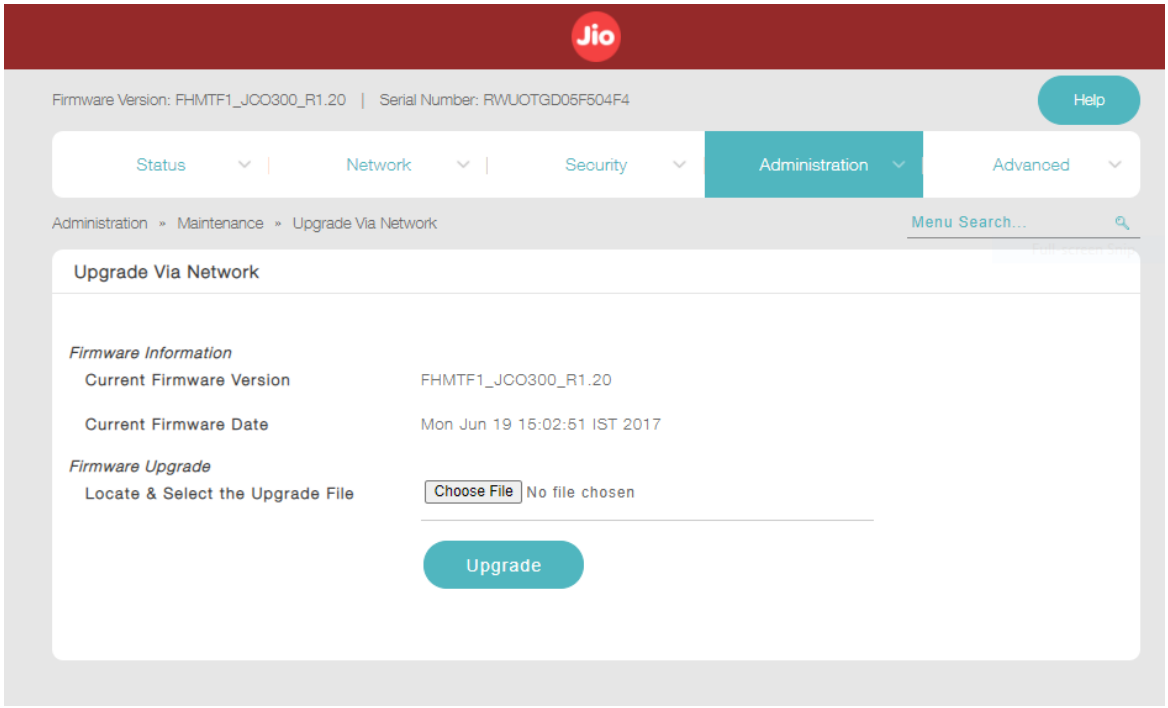
S. No	**TEST CASE NAME**	**PASS/FAIL**	**Remarks**
1	TC_NO_SECURE_UPGRADE	FAIL	

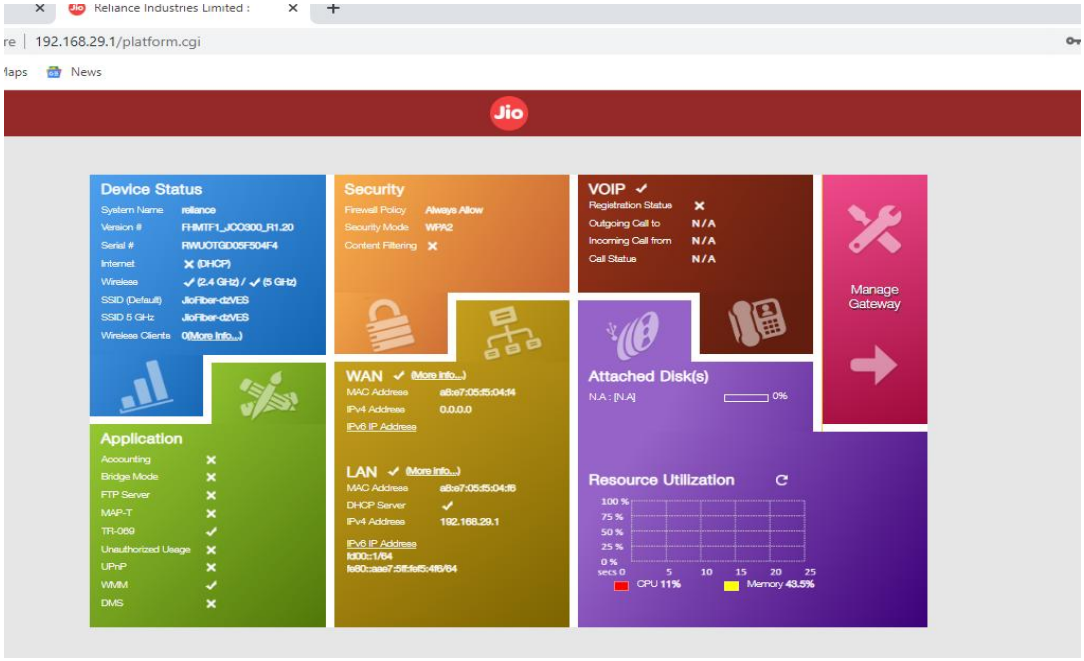
1.3.3 Source Code Security Assurance

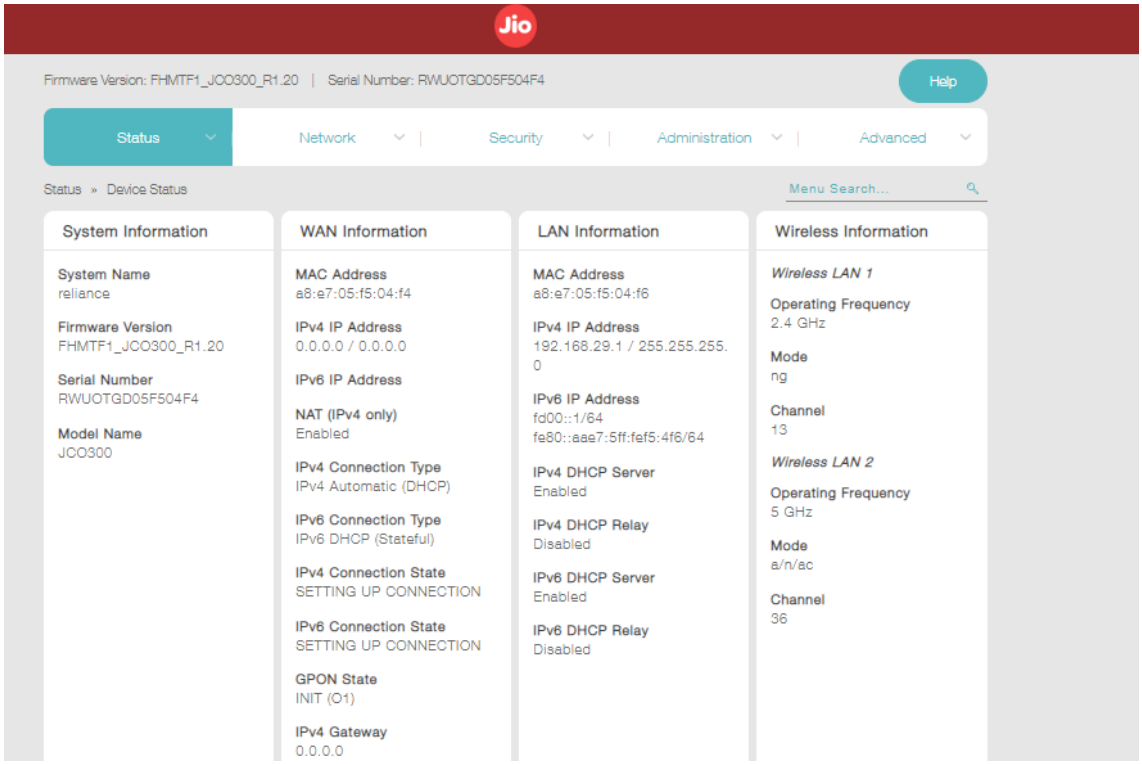
<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 3: Software Security
2. **<Security Requirement No & Name > 1**.3.3 Source Code Security Assurance
3. **<Requirement Description: >**
   Source code of the CPE (in high level programming language) shall be free from known security vulnerabilities, the high security critical weaknesses listed in the CWE database and all the exploitable security vulnerabilities listed in the latest SANS Top 25 and OWASP Top 10. OEM may provide Software Test Document (STD) in this regard.
4. **DUT Confirmation Details**:
   Use the command line/GUI interface to get details of the machine on which test is conducted.
   Use GUI to get Application No/Version No & hardware Info

   The below screenshot shows the firmware version of the DUT







5. **DUT Configuration:**
   Nil
6. **Preconditions:**
   Below are the preconditions for this test case:

   Vendor must provide documentation such as Software Development Lifecycle and evidence of Implemented processes (such as integrity of code base, management of code, etc.), and

Secure coding guidelines for the vendor developed code, and any third party and opensource software used/embedded in the product.

Vendor to provide SAST/SBA report for DUT that cover SANS Top 25 and OWASP Top 10, Also report of known security vulnerabilities, security weaknesses listed in the CWE database.

Vendor to provide Software Test Document (STD) stating that no known vulnerabilities exist and that Secure Software Life cycle practices were followed.

7. **Test Objective:** To Verify that:
   - Best security practices including secure coding are followed for software development.
   - software is free from CWE top 25 and OWASP top10 security weaknesses on the date of testing.
   - The binaries of DUT and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities.
8. **Test Plan:**
   Validating the STD document provided by OEM

8.1 Tools Used:
- A suitable source code analysis tool having support for the programming language of the source code & having capabilities to detect weaknesses/vulnerabilities as per the requirement clause.
- A suitable static binary analysis tool can be used to find the weakness/vulnerabilities in the DUT binary file.

8.2 Testbed Diagram: As per Vendor STD document

8.3 **Test Execution Steps:** verification of software test document submitted by OEM :
- Examine and authenticate the Software Test Document (STD) given by the Original Equipment Manufacturer (OEM).
- Verify that the source code of the Device Under Test (DUT) is free from all known security vulnerabilities and high-security critical weaknesses listed in the CWE database.
- Verify that the binary code of the Device Under Test (DUT) is free from known security vulnerabilities and high-security critical weaknesses listed in the CWE database.

9 **Expected Result to Pass:** Validate that source code and binary code in DUT are free from known security vulnerabilities and critical vulnerabilities from the CWE database, this can be validated from vendor-provided test reports such as Static Application Security Test (SAST) report.

10 **Expected Format of Evidence:** Tester validation of source code analysis/static binary analysis reports.

11 **Test Execution:**

11.1 Number of Test Cases: 1

11.1.1 **Test Case Number:** 1
11.1.2 **Test Case Name:** TC_VEIFY_STD_DOC
11.1.3 **Test Case Description:** To Verify the software test document provided by Vendor
11.1.4 **Execution Steps:**

Case 1: verification of software test document submitted by vendor

verification of software test document submitted by OEM :

- Examine and authenticate the Software Test Document (STD) given by the Original Equipment Manufacturer (OEM).
- Verify that the source code of the Device Under Test (DUT) is free from all known security vulnerabilities and high-security critical weaknesses listed in the CWE database.
- Verify that the binary code of the Device Under Test (DUT) is free from known security vulnerabilities and high-security critical weaknesses listed in the CWE database.

11.1.5 **Test Observations:** Based on Software Test Documentation submit by OEM the result will vary

12 **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1.	TC_VERIFY_STD_DOC		OEM dependent

1.3.4 Known Malware Check

<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 3 - Software Security
2. **<Security Requirement No & Name >** 1.3.4 Known Malware Check
3. **<Requirement Description: >**

The Operating System and the applications installed in the CPE shall be free from any known malware. The CPE shall support mechanism to carry out anti-malware checks. OEM to submit Software Test document (STD) to establish that the CPE is free from Known Malware.

4. **DUT Confirmation Details**:

- This section involves information about DUT like software/firmware version, Hardware version model.
- DUT Cisco WLC contains default boot image with version 8.10.183.0. The model is AIRAP1852I-E-K9. The inventory shows model serial no. & model description.
- Verification of DUT Cisco wireless LAN controller's HW product series information by running command *show inventory* on CLI.

```
(Cisco Controller) >show inventory

Burned-in MAC Address.............................. 38:ED:18:C8:10:60
Maximum number of APs supported.................... 50
NAME: "Mobility Express"    , DESCR: "Cisco Aironet 1850 Series Mobility Express"
PID: AIR-AP1852I-E-K9,  VID: V01,  SN: KWC193100UU
```

- Verification of DUT Cisco WLC's high-level system SW information by running command *show sysinfo* on CLI.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.10.183.0
OUI File Last Update Time........................ N/A

System Name...................................... Aironet-Controller
System Location.................................
System Contact..................................
System ObjectID.................................. 1.3.6.1.4.1.9.1.2250
IP Address....................................... 10.208.38.2
Last Reset....................................... 1: reload command

System Up Time................................... 0 days 3 hrs 33 mins 5 secs
System Timezone Location......................... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
System Stats Realtime Interval................... 5
System Stats Normal Interval..................... 180

Configured Country............................... IN  - India

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled

--More-- or (q)uit
```

- Verification of DUT Cisco WLC's system information on Web access.

5. **DUT Configuration**:
   OEM dependent
6. **Preconditions:**
   - Vendor to provide Software Test Document (STD) stating that software does not contain known malware and provide a mechanism to perform anti-malware check at certain lifecycle.
   - Binary (.bin file) of DUT copied to a win10 machine.

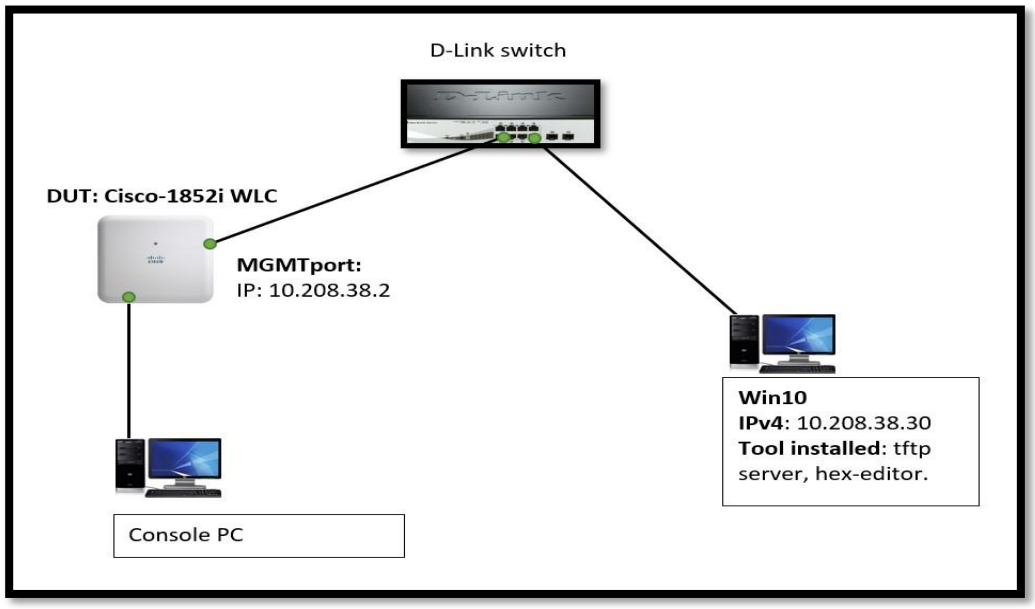
7. **Test Objective:** To verify that DUT don't have any known malware

8. **Test Plan:**

   8.1 **Number of Test Scenarios:**

   8.1.1 Validate that the DUT don't have any known malware

   8.2 **Test Setup Diagram**



8.3 **Tools Used:**

- clamAV tool

Note : Depending on vendor input the malware scan will vary(online or offline).

8.4 **Test Execution Steps:**

- Vendor shall submit Software Test Document (STD) of the network product proving that the network product is free from known malware/spyware to lab for scrutiny.
- Vendor to provide documentation for network product support mechanisms to carry out anti-malware checks.
- We will require binaries/packages to scan for malware.
- As tester, We will verify existence of malware using clamAV (prior to using clamAV, database will be updated such that latest malware are captured.)"

9. **Expected Result for Pass:** The DUT software should not have any known malware
10. **Expected Format of Evidence:** Screenshot of malware test report

11. **Test Execution:**

11.1.1 **Test Case Number:** 01

11.1.2 **Test Case Name:** TC_NO_KNOWN_MALWARE_CHECK

11.1.3 **Test Case Description:** In this test scenario tester will perform the positive test to Upgrade/upgrade the DUT image using the TFTP server and DUT settings were configured for an image Upgrade. The Upgrade will be verified by low privilege user and highest privilege user also image signing verification and cryptographic library will be checks during Upgrade/upgrade on console. In the negative test, tester will try to Upgrade on DUT and observed the process will get fail or not for image signing verification.

11.1.4 **Execution Steps:**

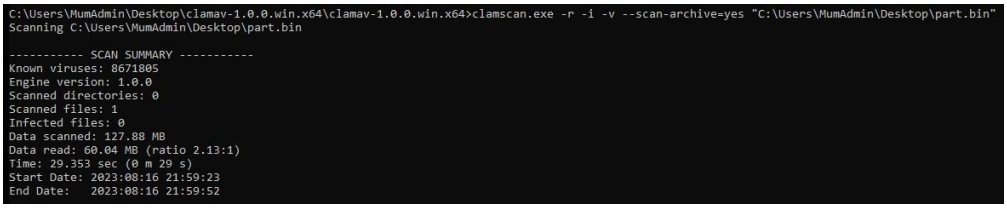
Below are the execution steps with evidence:

a. Vendor shall submit Software Test Document (STD) of the network product proving that the network product is free from known malware/spyware to lab for scrutiny.
b. Vendor to provide documentation for network product support mechanisms to carry out anti-malware checks.
c. We will require binaries/packages to scan for malware.

As tester,

-We will, verify existence of malware using clamAV (prior to using clamAV, database will be updated such that latest malware are captured.)"

• Validate that all the operating systems and the applications installed in the DUT shall be free from any known malware. Also, Identify the list of known malwares by running anti-malware checks using software.



It has been observed that the image of the DUT is free from known malware as per clam AV tool scanned image report. Its showing infected file is “0”.

Note : DUT don’t have anti-malware checks feature

11.1.5 **Test Observations:** The DUT software don’t have any known malware based on malware scan.

Note : DUT don’t have anti-malware checks feature

12. Test Case Result:

S. No	**TEST CASE NAME**	**PASS/FAIL**	**Remarks**
1	TC_NO_ KNOWN_MALWARE_CHECK		Depend on OEM

1.3.5 No unused software

<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 3 Software Security
2. **<Security Requirement No & Name >** 1.3.5 No unused software
3. **<Requirement Description: >**

Unused software components or parts of software which are not needed for operation or functionality of the CPE shall not be installed or shall be deleted after installation. This includes also parts of a software, which will be installed as examples but typically not be used (e.g., default web pages, example databases, test data). OEM to provide Software Test Document (STD) in this regard.

4. **DUT Confirmation Details**:

- This section involves information about DUT like software/firmware version, Hardware version model.
- DUT Cisco WLC contains default boot image with version 8.10.183.0. The model is AIRAP1852I-E-K9. The inventory shows model serial no. & model description.
- Verification of DUT Cisco wireless LAN controller's HW product series information by running command *show inventory* on CLI.

```
(Cisco Controller) >show inventory

Burned-in MAC Address.............................. 38:ED:18:C8:10:60
Maximum number of APs supported.................... 50
NAME: "Mobility Express"     , DESCR: "Cisco Aironet 1850 Series Mobility Express"
PID: AIR-AP1852I-E-K9,  VID: V01,  SN: KWC193100UU
```

- Verification of DUT Cisco WLC's high-level system SW information by running command *show sysinfo* on CLI.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.10.183.0
OUI File Last Update Time........................ N/A

System Name...................................... Aironet-Controller
System Location.................................
System Contact..................................
System ObjectID.................................. 1.3.6.1.4.1.9.1.2250
IP Address....................................... 10.208.38.2
Last Reset....................................... 1: reload command

System Up Time................................... 0 days 3 hrs 33 mins 5 secs
System Timezone Location......................... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
System Stats Realtime Interval................... 5
System Stats Normal Interval..................... 180

Configured Country............................... IN  - India

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled

--More-- or (q)uit
```

- Verification of DUT Cisco WLC's system information on Web access.

5. **DUT Configuration**: Depending on vendor inputs.
6. **Preconditions:**
   - Document provided by vendor should include the following details:
   - List of available software, Libraries, and components.
   - name of the software / library.
   - version of the software / library installed.
   - list of dependencies and versions.
   - any add-ons and functions.
   - any special hardware/debugging ports.
   - software support type.
   - licensing information.
   - brief description of their purpose.

7. **Test Objective:** Unused software components should not be present in the DUT

8. **Test Plan:** Validating the SBOM provided by the OEM
   - 8.1 **Number of Test Scenarios:**
     - 8.1.1 Validating the list of components provided by OEM
   - 8.2 **Test Setup Diagram :-** Depents on vendor input
   - 8.3 **Tools Used:** Syft, Blackduck SCA
   - 8.4 **Test Execution Steps:** Below are the execution steps:
     - This requirement is associated with Software Bill of Material (SBOM). It is assumed that vendor will be maintaining such list of software, libraries and associated components, and can provide for verification purpose.
     - Check the list of software, libraries and associated components provided by the vendor.
     - Identify how the software libraries or components can be modified.
     - Identify the software/libraries or components using tool like syft or blackduck.
     - Validate that there is no unnecessary software, libraries installed in the system apart from the ones that have been mentioned.
     - Identify the example webpages/documents in the DUT.

9. **Expected Result for Pass:** Unused software disabled/deleted in the DUT
10. **Expected Format of Evidence:** Screenshot of tools used
11. **Test Execution:**

11.1 **Test Case Number:** 01

11.1.1 **Test Case Name:** TC_NO_UNUSED_SOFTWARE

11.1.2 **Test Case Description:**

11.1.3 Verifying the DUT not have any unused software, default webpages and examples

11.1.4 **Execution Steps:**

- Identify the software/libraries or components using tool like syft (for demonstration purpose).

- Identify the example webpages/documents in the DUT

```
mumadmin@APMUMCSAE002D:~/Desktop/SDadhwal/syft$ ./bin/syft dir:/home/mumadmin/Desktop/SDadhwal/Image/
 ✔ Indexed /home/mumadmin/Desktop/SDadhwal/Image
 ✔ Cataloged packages      [156 packages]

NAME                           VERSION    TYPE
CherryPy                       3.2.5      python
PyYAML                         4.1        python
backports.ssl_match_hostname   3.4.0.2    python
busybox                        1.29.3     binary
certifi                        2017.11.5  python
cffi                           1.9.1      python
chardet                        3.0.2      python
cheroot                        5.4.0      python
cov-core                       1.7        python
coverage                       3.7.1      python
cryptography                   1.7.1      python
docker                         3.5.0      python
docker-pycreds                 0.3.0      python
email                          4.0.2      python
enum34                         1.0        python
falcon                         1.1.0      python
functools32                    3.2.3-2    python
futures                        2.1.6      python
idna                           2.1        python
ipaddress                      1.0.17     python
jsonschema                     2.5.1      python
libvirt-python                 1.2.2      python
libvirt-python                 1.3.4      python
mock                           0.8.0      python
mock                           1.0.1      python
mockito                        0.5.2      python
netaddr                        0.7.18     python
oauthlib                       1.0.3      python
pam                            0.1.4      python
pep8                           1.4.6      python
pexpect                        2.3        python
psutil                         2.0.0      python
py                             1.4.20     python
pyOpenSSL                      19.0.0     python
pyaes                          1.6.0      python
pyasn1                         0.1.9      python
```

11.1.5 **Test Observations:**

- List of software components present in the DUT(syft generated) compare with OEM SBOM.
- Example webpages/documents not verified due to OEM dependency.

12. Test Case Result:

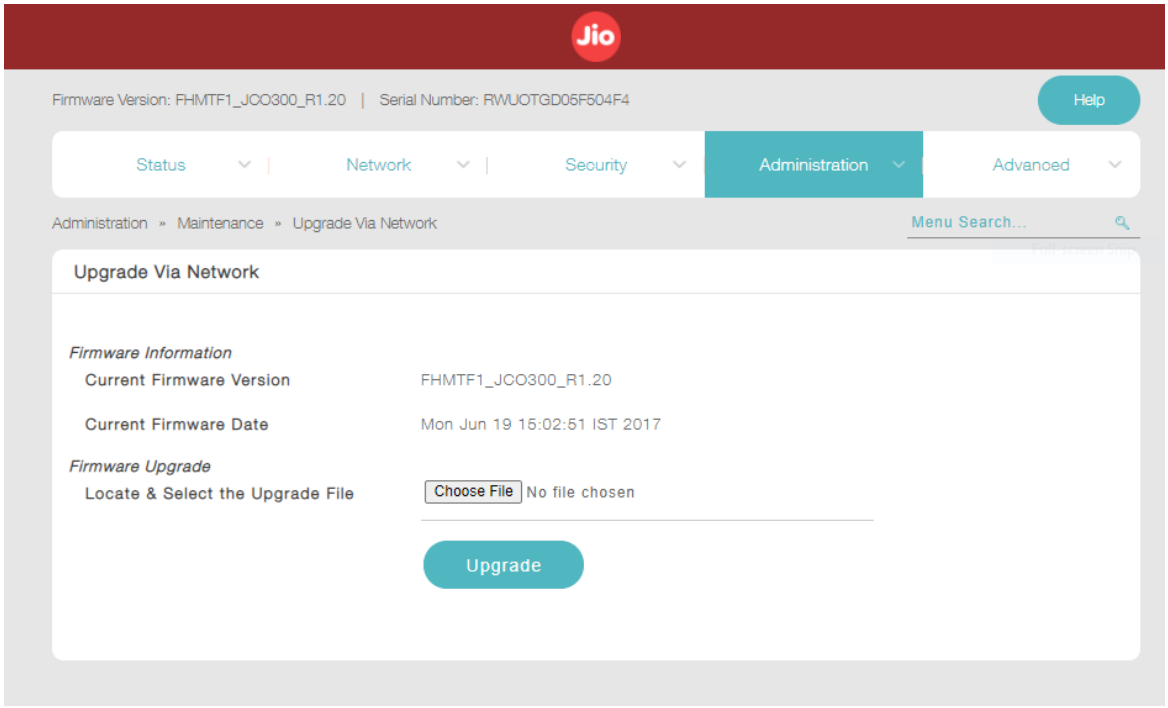
S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_UNUSED_SOFTWARE		Testcase is incomplete

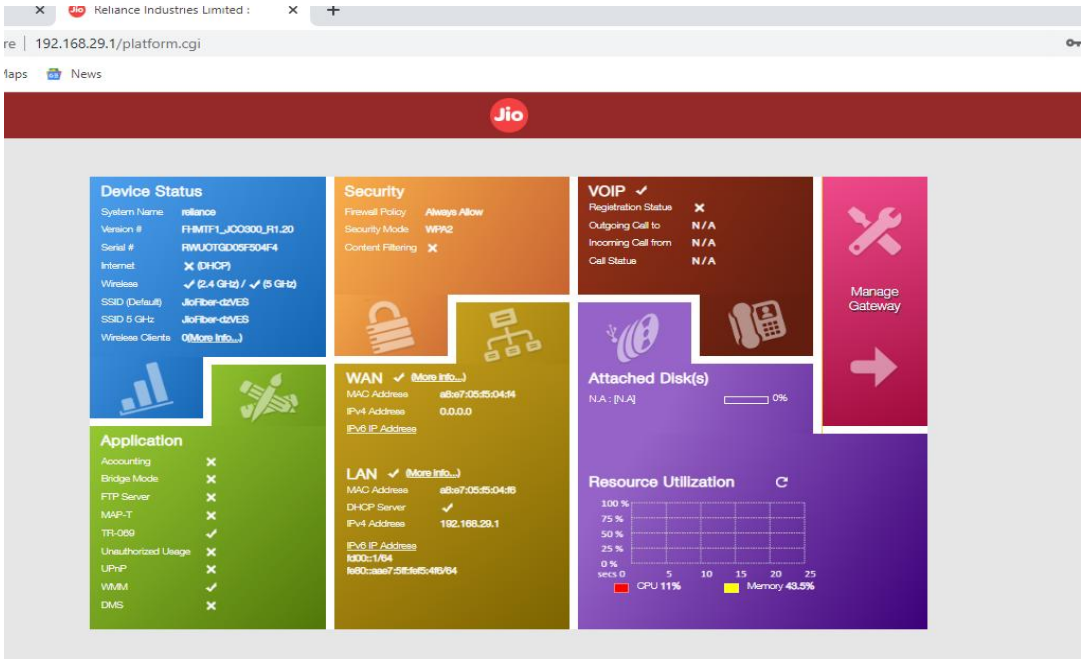
1.3.6 Unnecessary Services Removal

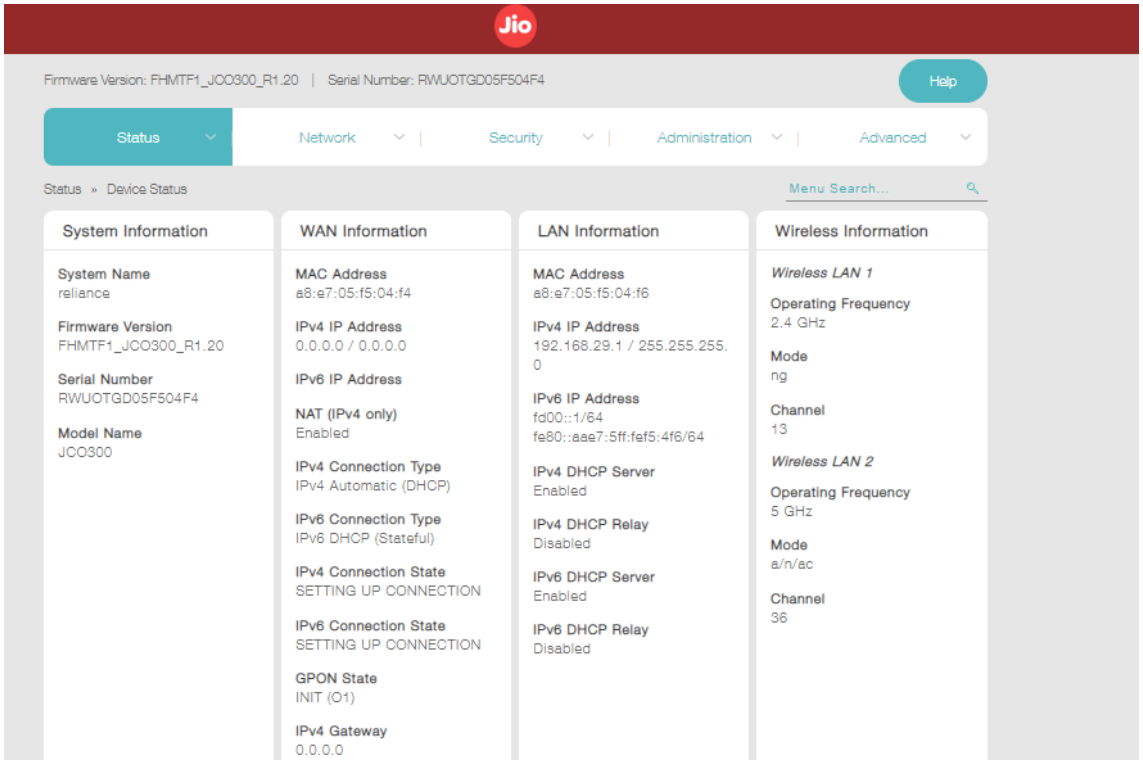
<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 3 - Software Security
2. **<Security Requirement No & Name >** 1.3.6 Unnecessary Services removal
3. **<Requirement Description: >** The OEM to provide list of essential services and the related ports required for functioning of CPE, list of optimal services supported by CPE and their related ports. The CPE shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities. In particular, by default the following services and their ports shall be initially configured to be disabled on the CPE by the vendor.
   - FTP
   - TFTP
   - Telnet
   - rlogin, RCP, RSH
   - HTTP - SNMPv1 and v2
   - SSHv1, HNAP
   - TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)
   - Finger - BOOTP server
   - Discovery protocols (CDP, LLDP)
   - IP Identification Service (Identd)
   - PAD
   - MOP
4. **DUT Confirmation Details**:
   - Use the command line/GUI interface to get details of the machine on which test is conducted.
   - Use GUI to get Application No/Version No & hardware Info

   The below screenshot shows the firmware version of the DUT

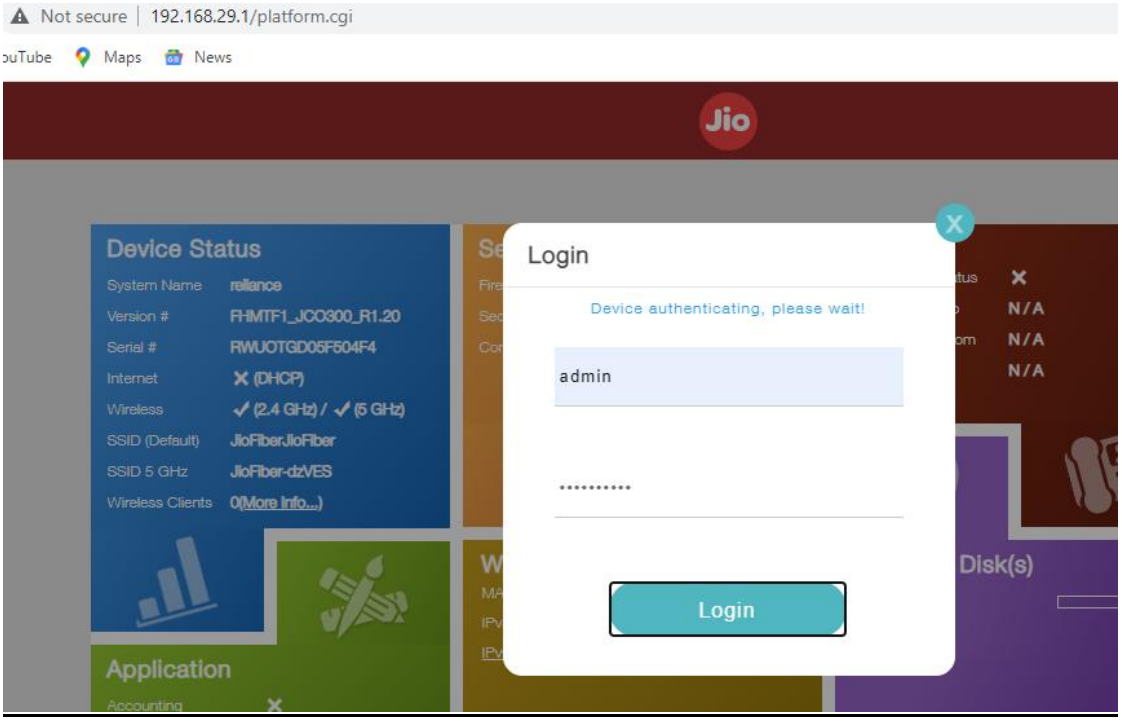

Jio
Firmware Version: FHMTF1_JCO300_R1.20 | Serial Number: RWUOTGD05F504F4
Help
Status
Network
Security
Administration
Advanced
Administration » Maintenance » Upgrade Via Network
Menu Search...
Upgrade Via Network
Firmware Information
Current Firmware Version
FHMTF1_JCO300_R1.20
Current Firmware Date
Mon Jun 19 15:02:51 IST 2017
Firmware Upgrade
Locate & Select the Upgrade File
Choose File
No file chosen
Upgrade


Reliance Industries Limited :
192.168.29.1/platform.cgi
News
Jio
Device Status
System Name reliance
Version # FHMTF1_JCO300_R1.20
Serial # RWUOTGD05F504F4
Internet (DHCP)
Wireless (2.4 GHz) / (5 GHz)
SSID (Default) JioFiber-dzVES
SSID 5 GHz JioFiber-dzVES
Wireless Clients 0(More Info...)
Security
Firewall Policy Always Allow
Security Mode WPA2
Content Filtering
VOIP
Registration Status
Outgoing Call to N/A
Incoming Call from N/A
Call Status N/A
Manage Gateway
Application
Accounting
Bridge Mode
FTP Server
MAP-T
TR-069
Unauthorized Usage
UPnP
WMM
DMS
WAN (More Info...)
MAC Address e8:e7:05:f5:04:f4
IPv4 Address 0.0.0.0
IPv6 IP Address
LAN (More Info...)
MAC Address e8:e7:05:f5:04:f5
DHCP Server
IPv4 Address 192.168.29.1
IPv6 IP Address
Attached Disk(s)
N.A : [N.A] 0%
Resource Utilization
100 %
75 %
50 %
25 %
0 %
secs 0 5 10 15 20 25
CPU 11%
Memory 43.5%



5. **DUT Configuration**:

- The Tester opens GUI(https) of DUT(192.168.29.1) in tester machine (192.168.29.118).



- The Tester attempts to login DUT using “admin” account.

6. **Preconditions:** A list of all required network protocols and services containing at least the following information shall be included in the documentation accompanying the Network Product, provided by the Vendor:
    - protocol handlers and services needed for the operation of network product;
    - Their open ports and associated services;
    - And a description of their purposes.

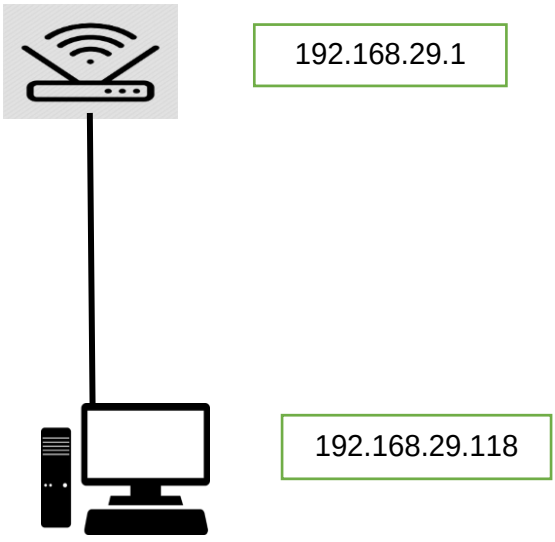
   The tester machine must be equipped with a port scanning tool, for scanning the ports of the DUT to get information required the status of the ports and the protocols/services running on them.
   The firewall on DUT must be disabled for allowing network traffic/requests from the tester machine.
7. **Test Objective:** To ensure that on all network interfaces, there are no unnecessary and unsecure services or protocols that might be running.

8. **Test Plan:**
    - The Tester shall identify what all services or protocols are running on DUT.
    - Verify identified protocols and services of the Network product and their purpose with documentation provided by OEM.
    - If any services or protocol running by default but that shall be initially configured to be disabled on the DUT by the OEM then check with OEM for justification.
    - The Tester shall record all above configurations steps and observations with evidences.

8.1 **Number of Test Scenarios:**

8.1.1 Based on the OEM document disable the unnecessary/unsecure services in the DUT

8.2 **Test Setup Diagram**



8.3 **Tools Used:** Zenmap (a Port scanning Tool)

8.4 **Test Execution Steps:**

a. The tester must verify for the compliance to the pre-requisites:
   - Verification that the list of available network services and protocol handlers is available in the documentation of the Network Product.
   - Validation that the entries in the list do not contain the prohibited protocols/services from the list mentioned above or any other protocol that is known to have security vulnerabilities, and it should be reasonably necessary for the operation of the Network Product class.

b. The tester must identify the protocols and services running on the DUT using an appropriate port scanning tool.
c. The tester must validate that there are no entries in the list of network services and handlers apart from the ones that have been mentioned and deemed necessary for the operation of the Network Product in the attached documentation.
d. The tester shall reboot the network product and re-execute execution steps 2 and 3 without further configuration.

9. **Expected Result for Pass:** The report will contain:
   - The names and version of the tool(s) used. - Information of all the protocol handlers and services running in the network product.

   Result will show:

   - There are no unnecessary services running in the network product except for the ones which are deemed necessary for its operation.

Any undocumented services running on the network product should be highlighted and brought out in the report. - The network product behaves the same after reboot as before.

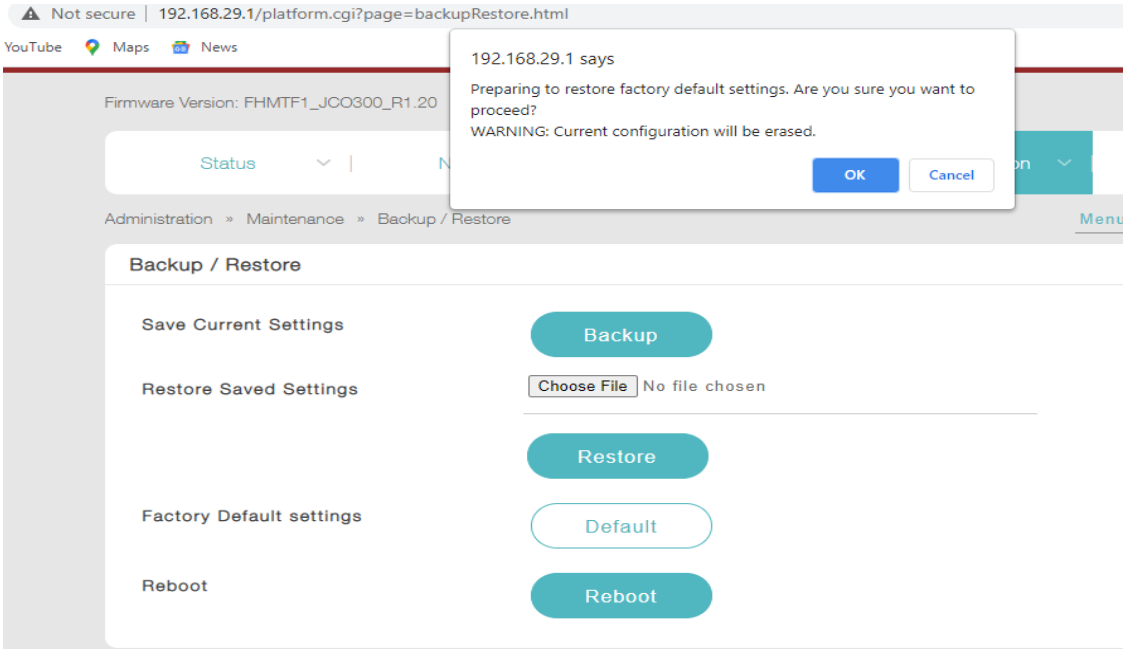
10. **Expected Format of Evidence:** Screenshot of Nmap scan, DUT CLI

11. **Test Execution:**

11.1.1 **Test Case Number:** 01
11.1.2 **Test Case Name:** TC_NO_UNNECESSARY_SERVICE
11.1.3 **Test Case Description:** Ensuring that on all network interfaces, there are no unnecessary and unsecure services or protocols that might be running.
11.1.4 **Execution Steps:**

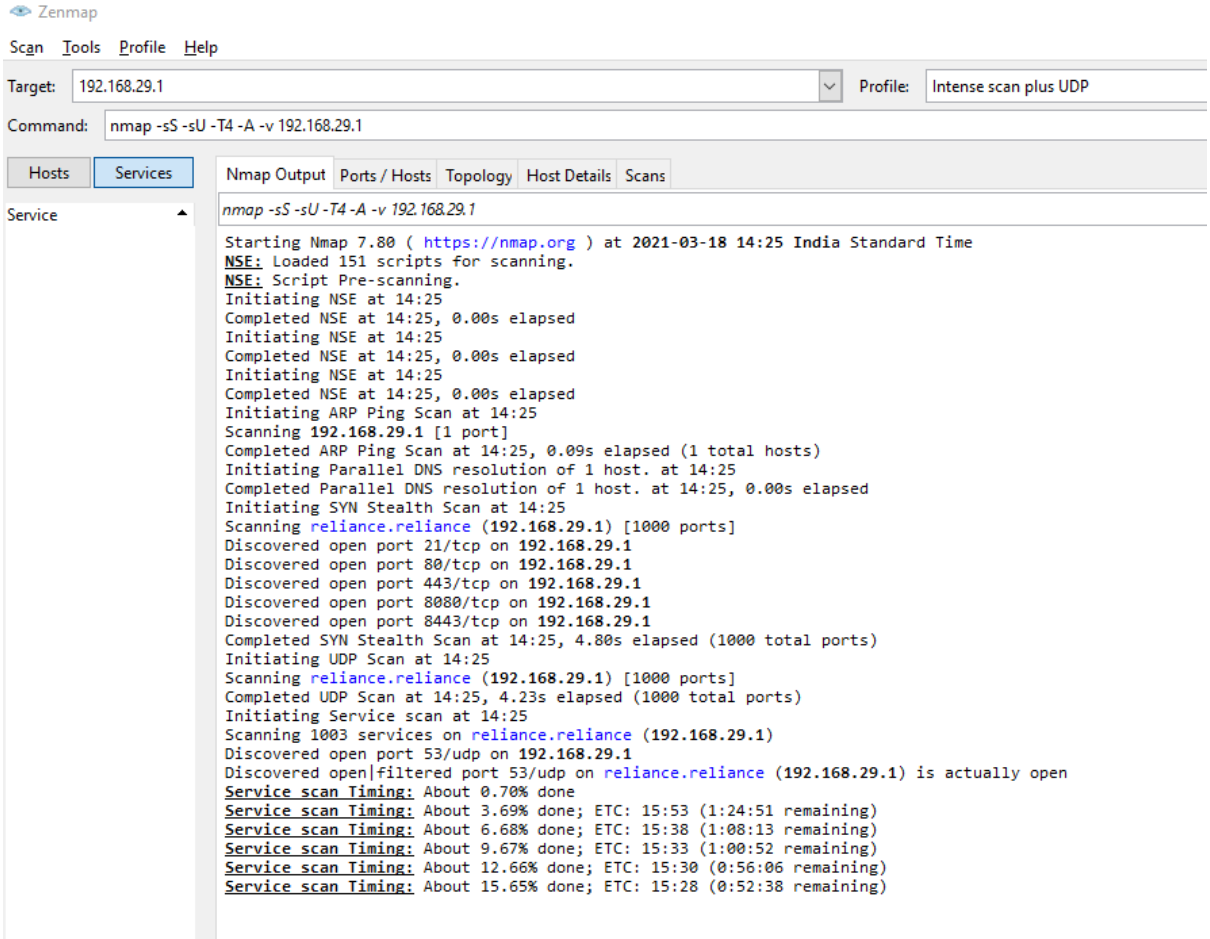
Test Case1: Identify what all by default services or protocols running on DUT.

- Login to the DUT
- Perform the factory reset of DUT



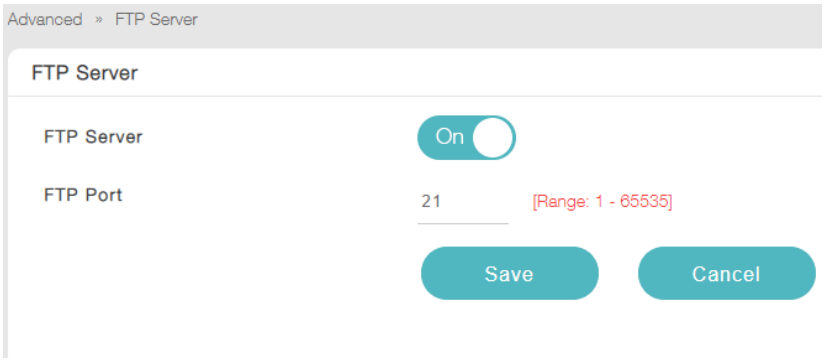
- Run the Zenmap port scanner tool to the DUT(192.168.29.1) by command **nmap -sS -sU -A -v 192.168.29.1** (-sS for TCP, -sU for UDP, -A for service Version info)

Note : SCTP protocol also need to be check in the DUT



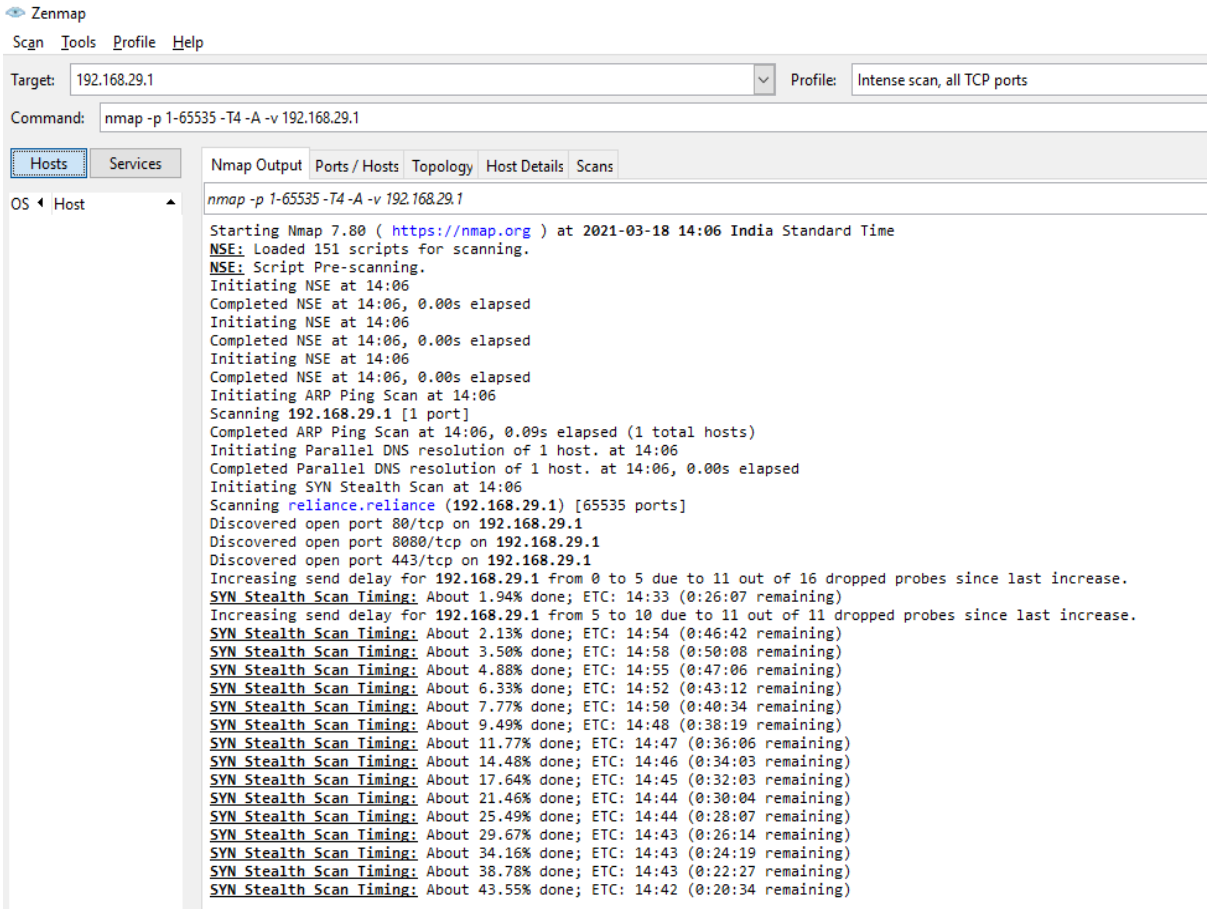
After factory reset, by default the unsecured(FTP,HTTP) protocols running in the DUT.

- Based on the OEM document disable the unnecessary/unsecure protocols running in the DUT.



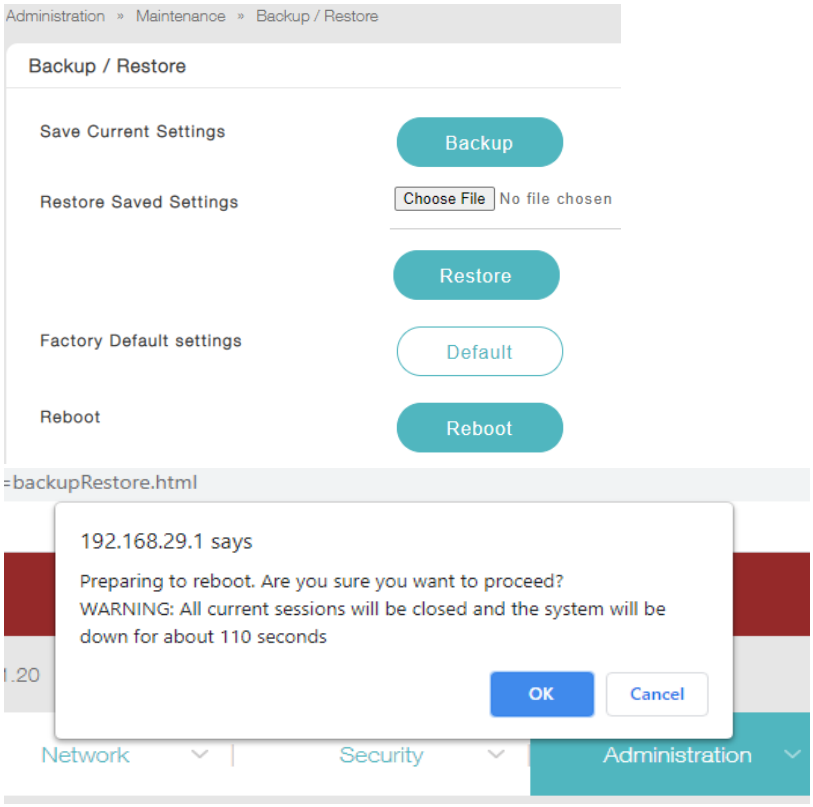
The above screenshot shows disable the FTP service(Port No :21) running in the DUT

- Run the Zenmap port scanner tool to the DUT(192.168.29.1), for validating the FTP service are disabled. The command is **nmap -p 1-65535 -T4 -A -v 192.168.29.1**

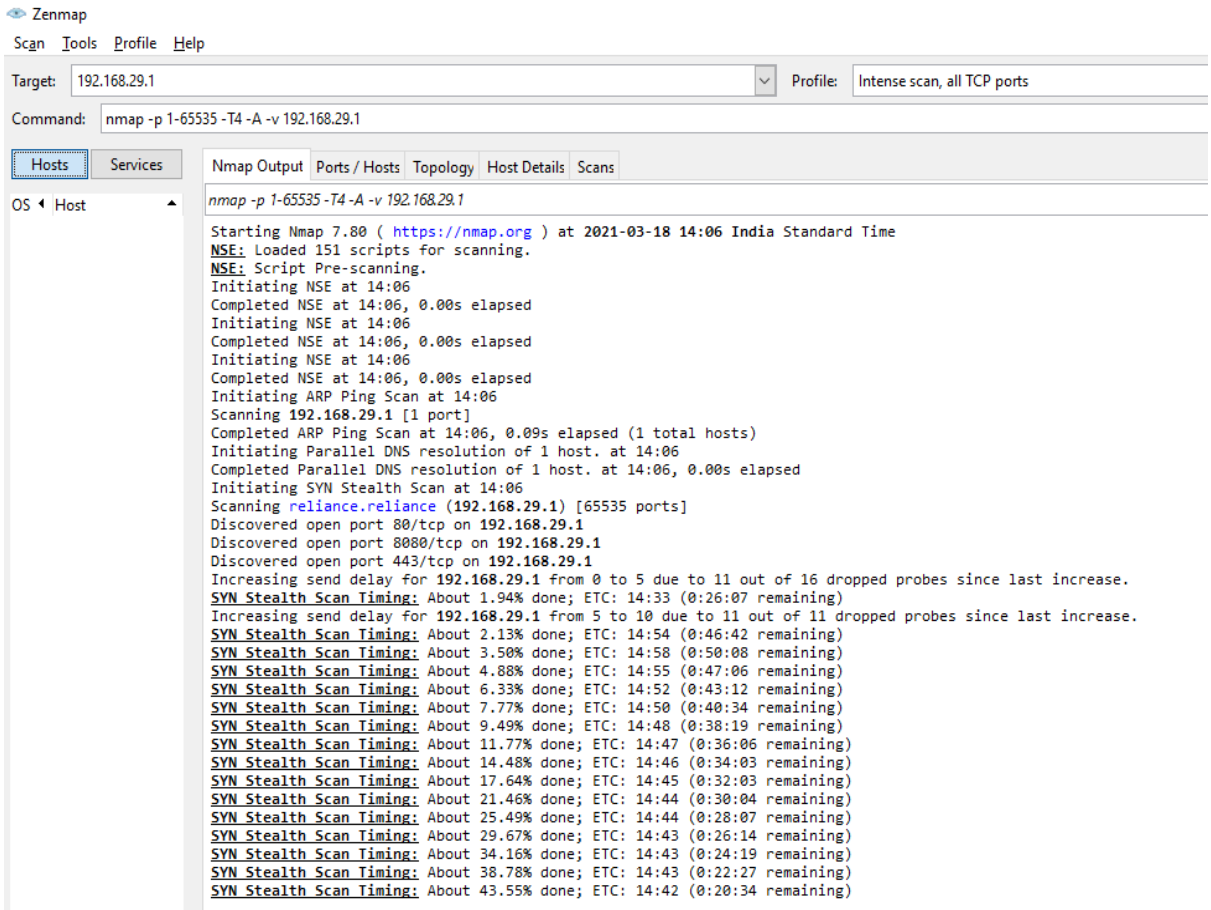


The above screenshot shows the FTP service is not active

- Reboot the DUT



- Run the Zenmap port scanner tool to the DUT(192.168.29.1), for validating the FTP service are disabled after reboot also. The command is **nmap -p 1-65535 -T4 -A -v 192.168.29.1**



11.1.5 **Test Observations:**

- The DUT by default running unsecure protocols/services(HTTP,FTP)
- Based on OEM documentation the tester able to disable the unsecure protocols/services
- disabled services remain disabled after reboot also.

12. Test Case Result:

S. No	**TEST CASE NAME**	**PASS/FAIL**	**Remarks**
1	TC_ NO_UNNECESSARY_SERVICE		Based on OEM document the result will vary

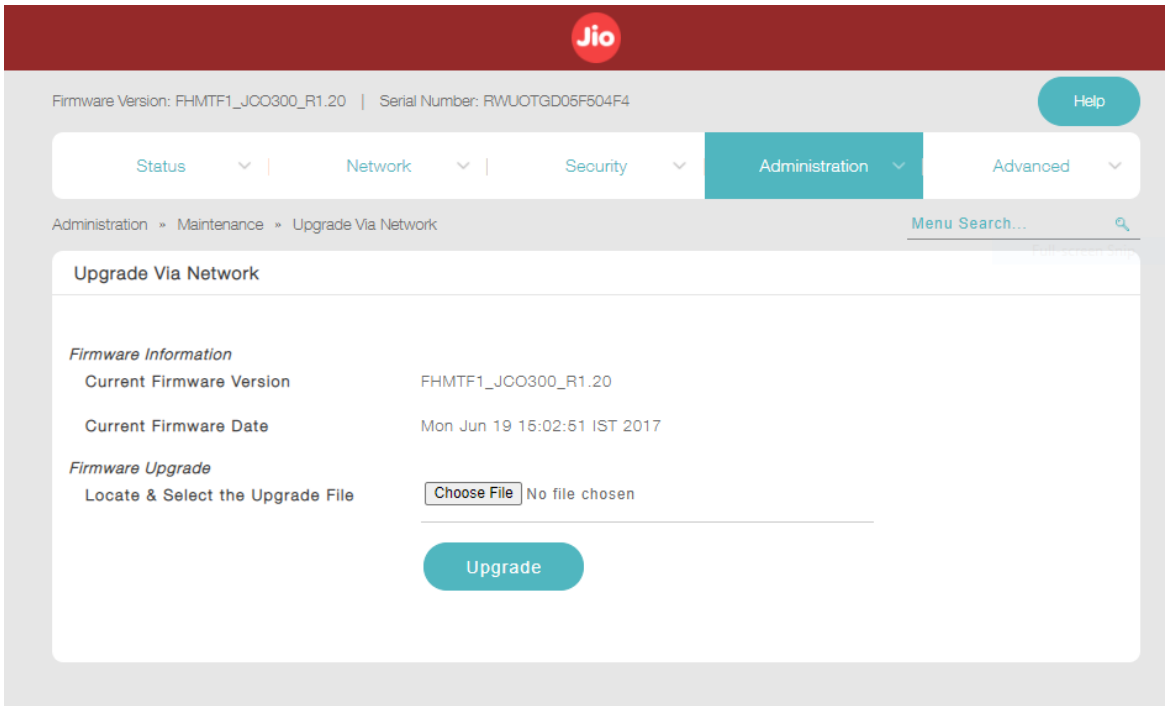
1.3.7 Secure Time Synchronization

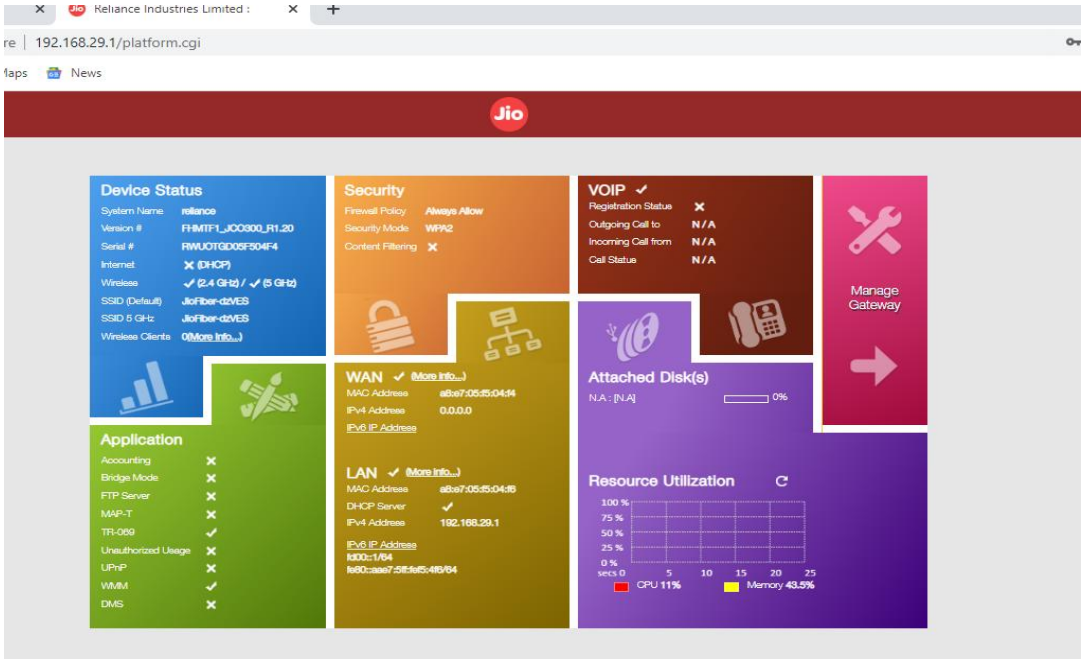
<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

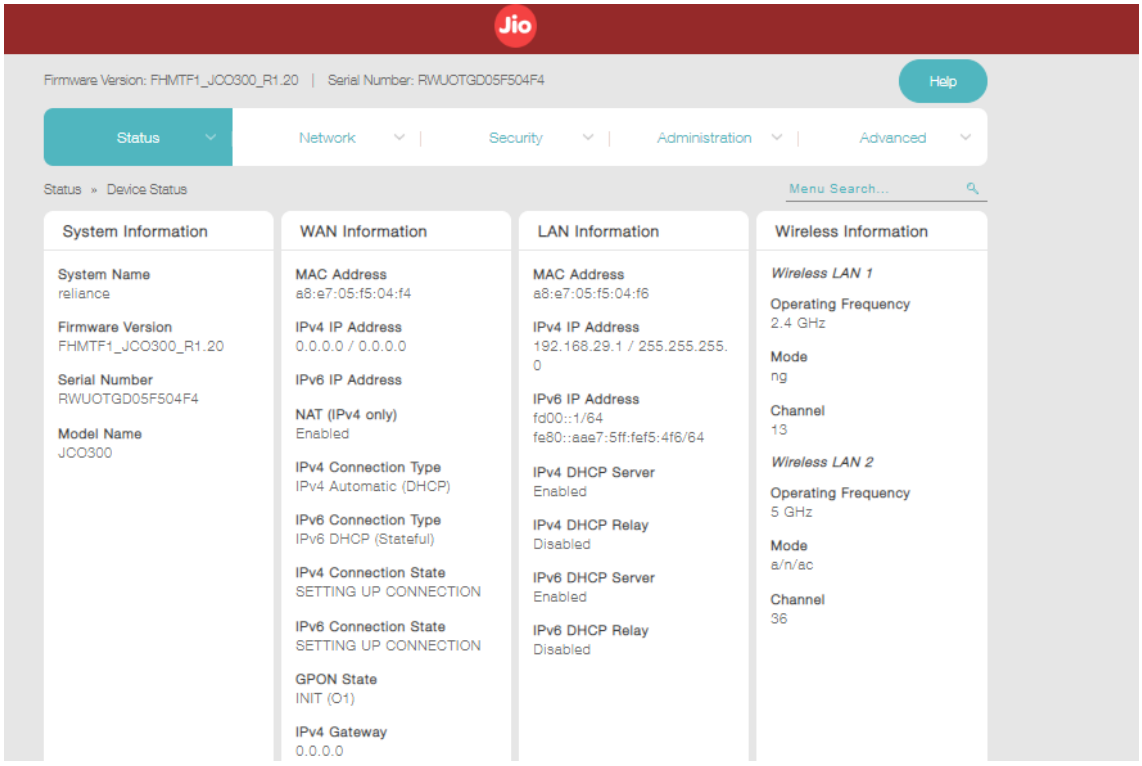
1. **<ITSAR Section No & Name>** Section 3 - Software Security
2. **<Security Requirement No & Name >** 1.3.7 Secure Time Synchronization
3. **<Requirement Description: >** The CPE shall support time synchronization feature for its core functionality or for the additional supported functionality. For CPEs that have time synchronization feature, it shall support the secure time synchronization feature preferably by using Network Time Protocol NTP. The CPE clock shall be synchronized with NTP server in a secure manner. The CPE client should be able to verify the authentication and authorization of the NTP Server. OEM shall plugin well known vulnerabilities, input validation vulnerabilities related to NTP feature.

4. **DUT <u>Confirmation Details</u>:**
   - Use the command line/GUI interface to get details of the machine on which test is conducted.
   - Use GUI to get Application No/Version No & hardware Info

The below screenshot shows the firmware version of the DUT

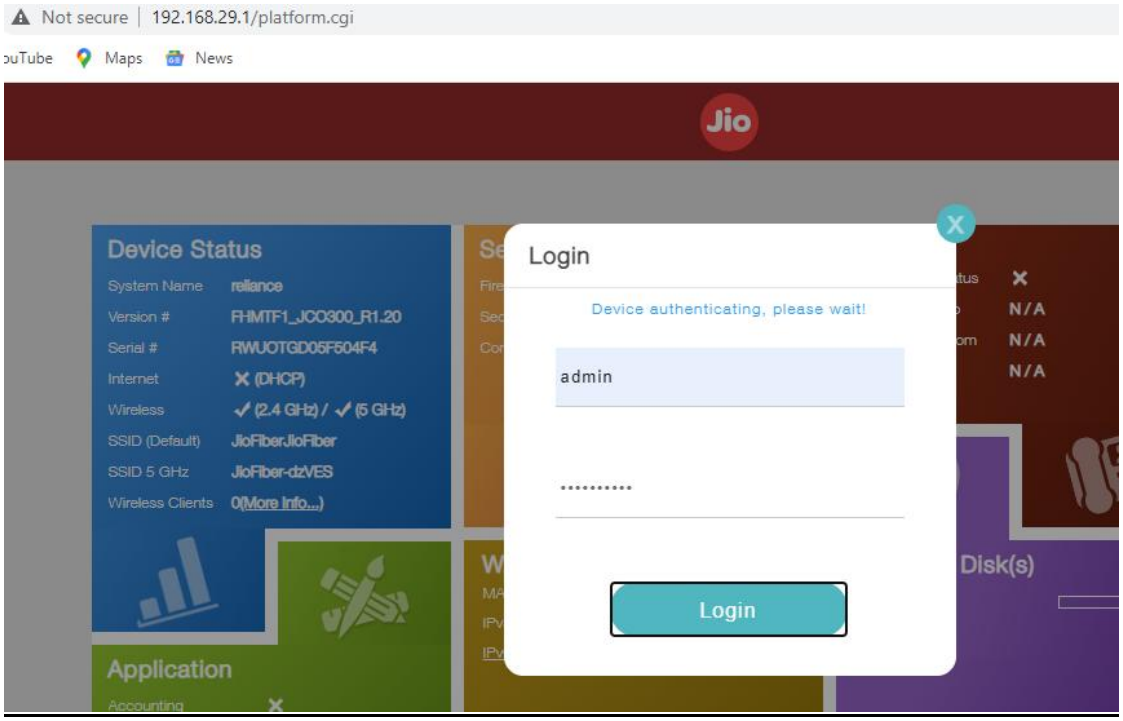






5. **DUT Configuration**:

- The Tester opens GUI(webpage) of DUT(192.168.29.1) in tester machine (192.168.29.118).



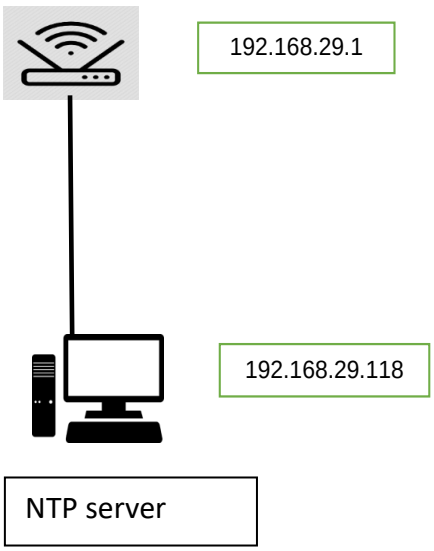
- The Tester attempts to login DUT using “admin” account.

6. **Preconditions:** The OEM need to provide documentation regarding on how to configure NTP in the DUT with securely
7. **Test Objective:** To ensure that DUT time sync with NTP server in a secure manner.
8. **Test Plan:**
    - The Tester configure the NTP services(client) on the DUT
    - Verify the DUT time sync with NTP server
    - Verify the DUT time sync with NTP server securely

    8.1 **Number of Test Scenarios:**

    8.1.1 DUT time sync with NTP server

    8.2 **Test Setup Diagram**



8.3 **Tools Used:** Wireshark (a Packet Capture Tool)

8.4 **Test Execution Steps:**

- The tester must verify for the compliance to the pre-requisites:
- Check the time/date of DUT
- Configure the NTP Server in the tester machine
- Configure the DUT(NTP client)
- Check the time/date of DUT
- Check the authentication of NTP packets

9. **Expected Result for Pass:** The DUT time sync with NTP server by securely

10. **Expected Format of Evidence:** Screenshot of Wireshark, DUT CLI

11. **Test Execution:**

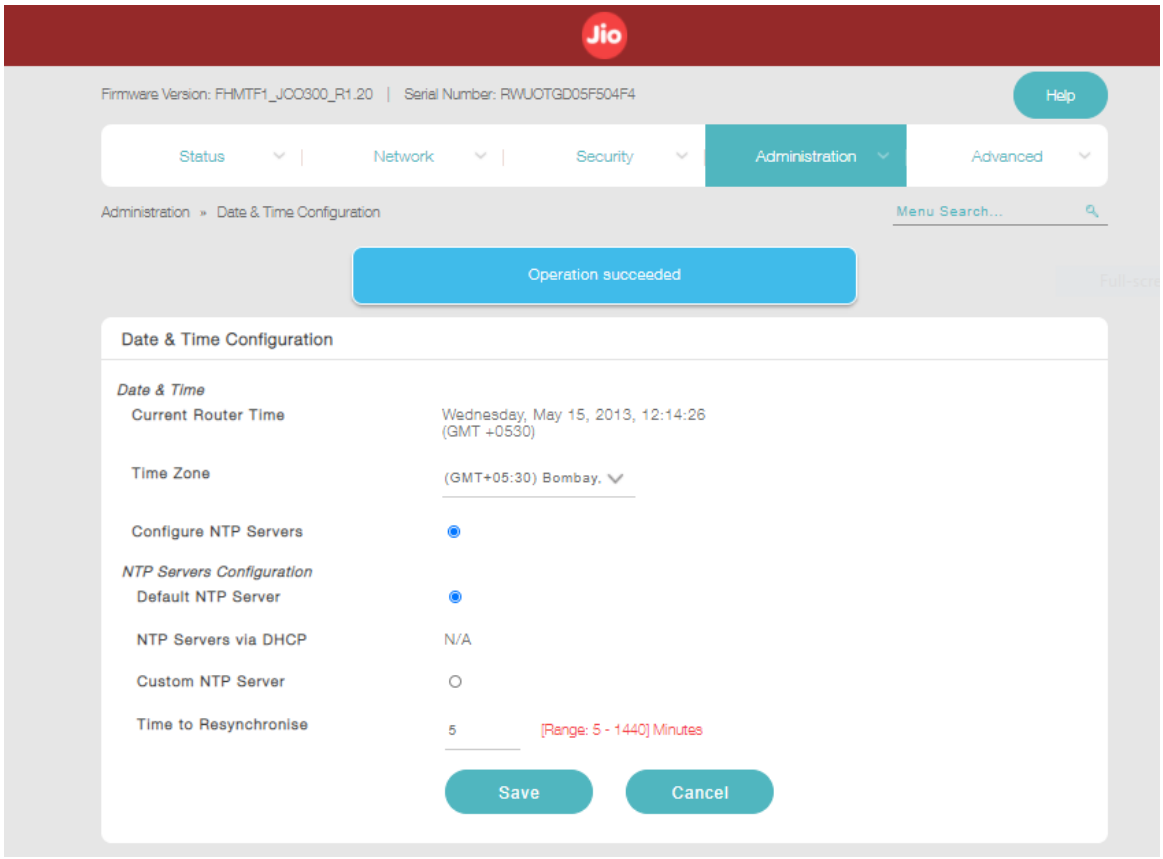
11.1.1 **Test Case Number:** 01

11.1.2 **Test Case Name:** TC_NO_SECURE_TIME_SYNCHRONIZATION

11.1.3 **Test Case Description:** Ensuring that DUT time sync with NTP server in a secure manner.

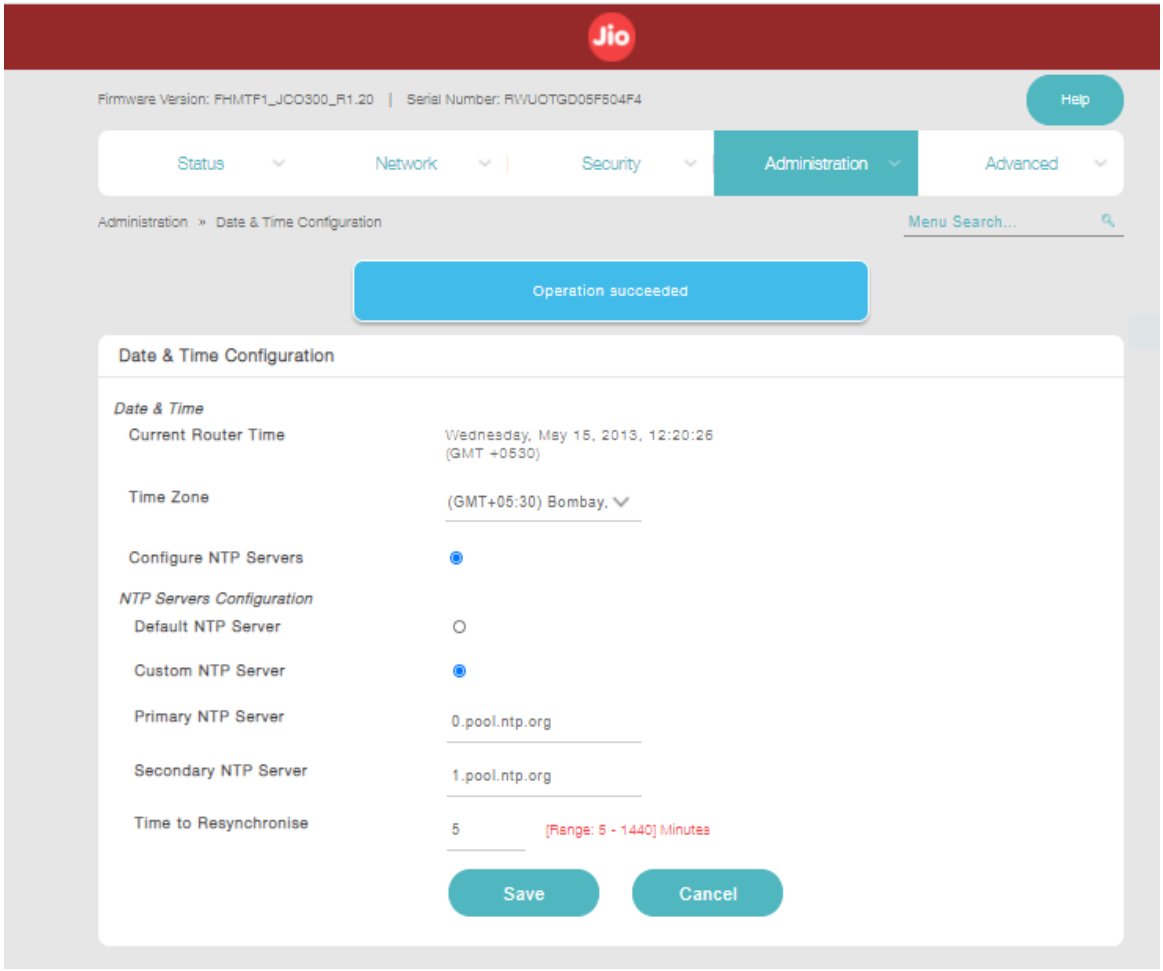
11.1.4 **Execution Steps:**

- Login to the DUT with Admin credentials
- Go to **Administration** in the GUI(webpage) and select **Date & Time Configuration**



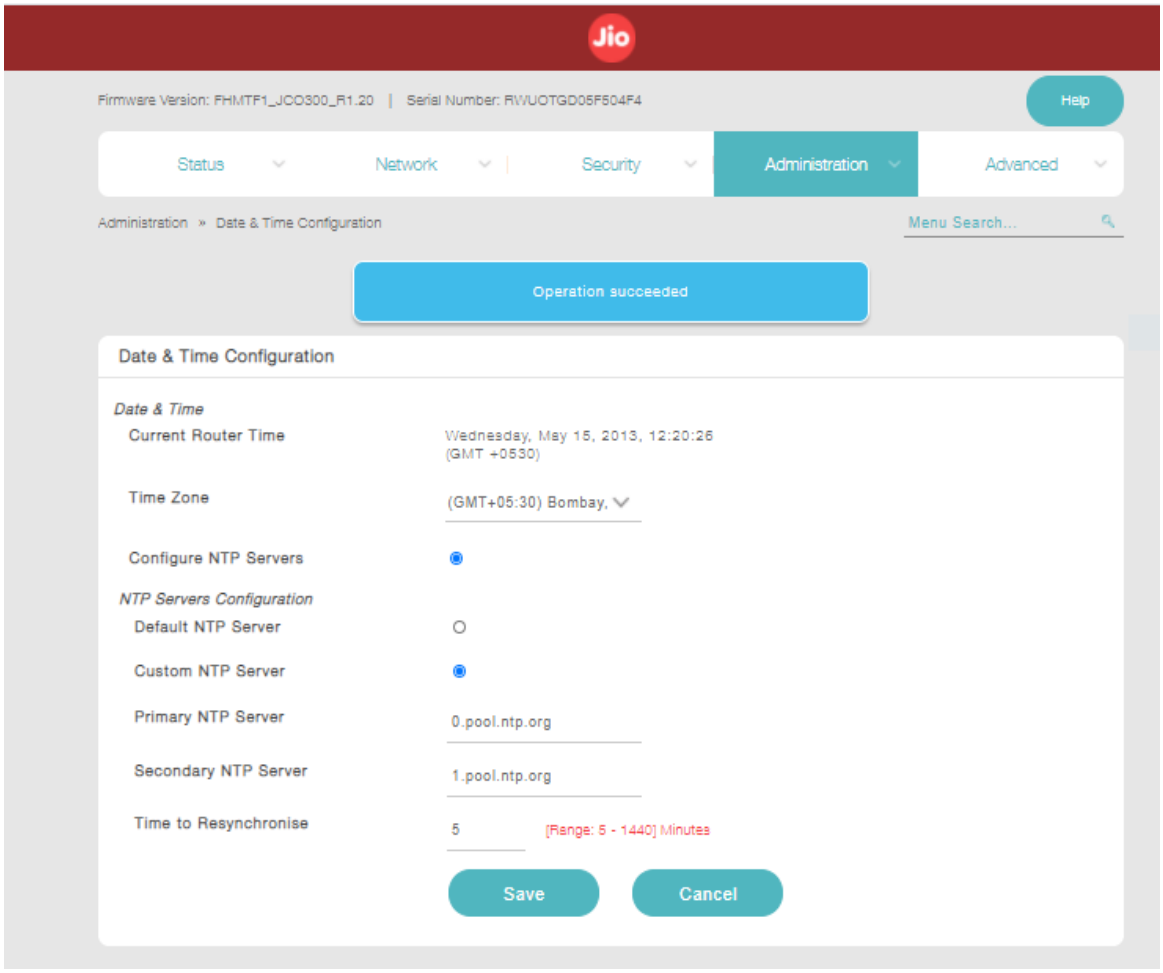
- In GUI option **Configure NTP Servers** select **Custom NTP Server** like below screenshot.

Configure NTP server IP address 192.168.29.118 in the DUT



Note : NTP server should be run locally

- Check time/date of DUT after NTP configuration
- Check the DUT have NTP server authentication option.



The above screenshot shows that there is no option mention regarding **NTP server authentication**. So, it's not possible to configure DUT with NTP server securely.

11.1.5 Test Observations:

- The DUT supports time sync with NTP server. But The DUT doesn't support secure time sync with NTP server.

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_ NO_SECURE_TIME_SYNCHRONIZATION	FAIL	DUT not supporting NTP authentication mechanism

1.3.8 Self-Testing

<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 3 - Software Security
2. **<Security Requirement No & Name >** 1.3.8 Self-Testing
3. **<Requirement Description: >**
   The CPE shall support the detection mechanism for identification of failure of underlying security mechanisms (such as software image integrity, runtime integrity, cryptographic modules etc.) used. The CPE to perform such self-tests periodically/at the time of booting, visual indication on failure is a desirable feature.
4. **DUT Confirmation Details**:
   - This section involves information about DUT like software/firmware version, Hardware version model.
   - DUT Cisco WLC contains default boot image with version 8.10.183.0. The model is AIRAP1852I-E-K9. The inventory shows model serial no. & model description.
   - Verification of DUT Cisco wireless LAN controller's HW product series information by running command *show inventory* on CLI.

```
(Cisco Controller) >show inventory

Burned-in MAC Address.............................. 38:ED:18:C8:10:60
Maximum number of APs supported.................... 50
NAME: "Mobility Express"    , DESCR: "Cisco Aironet 1850 Series Mobility Express"
PID: AIR-AP1852I-E-K9,  VID: V01,  SN: KWC193100UU
```

   - Verification of DUT Cisco WLC's high-level system SW information by running command *show sysinfo* on CLI.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name................................ Cisco Systems Inc.
Product Name....................................... Cisco Controller
Product Version.................................... 8.10.183.0
OUI File Last Update Time.......................... N/A

System Name........................................ Aironet-Controller
System Location.....................................
System Contact......................................
System ObjectID.................................... 1.3.6.1.4.1.9.1.2250
IP Address......................................... 10.208.38.2
Last Reset......................................... 1: reload command

System Up Time..................................... 0 days 3 hrs 33 mins 5 secs
System Timezone Location........................... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
System Stats Realtime Interval..................... 5
System Stats Normal Interval....................... 180

Configured Country................................. IN  - India

State of 802.11b Network........................... Enabled
State of 802.11a Network........................... Enabled

--More-- or (q)uit
```

- Verification of DUT Cisco WLC's system information on Web access.

5. **DUT Configuration**: No additional configuration required for this test case.

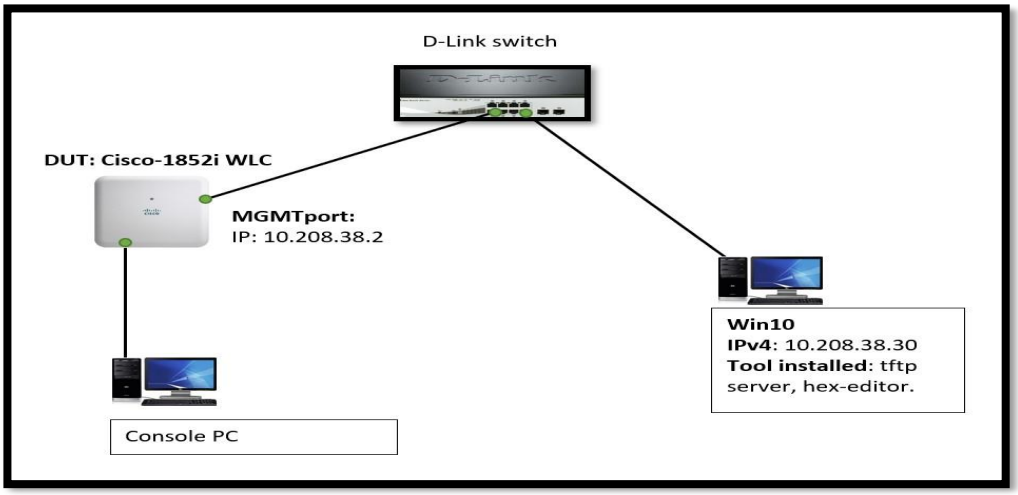
6. **Preconditions:**
   - Tester has the highest level of access to DUT.
   - Document from OEM having details of cryptographic modules implemented on DUT, self-testing mechanism and the evidence produced by DUT on self-test (start-up logs, any specific command to enable such logs etc.), command for initiating self-test by Admin etc.
7. **Test Objective:** To verify that DUT have mechanism that validates the cryptographic module when bootup

8. **Test Plan:**
   - Validating the DUT is performing POST in the device bootup stage
   - Validating the DUT software image when bootup

   8.1 **Number of Test Scenarios:**

   8.1.1 Verifying the integrity of DUT crypto modules and image

   8.2 **Test Setup Diagram**



8.3 **Tools Used:** DUT terminal (Console)

8.4 **Test Execution Steps:** Below are the execution steps,

Self-test for AP (1852i) – when Power On/restart.

Power on the DUT (AP 1852i) and verify the self-test to identify cryptographic functions security mechanism.

9. **Expected Result for Pass:** The DUT performing self-testing for crypto module and software image.
10. **Expected Format of Evidence:** Screenshot of DUT terminal (Console)
11. **Test Execution:**

11.1.1 **Test Case Number:** 01

11.1.2 **Test Case Name:** TC_NO_SELF_TESTING

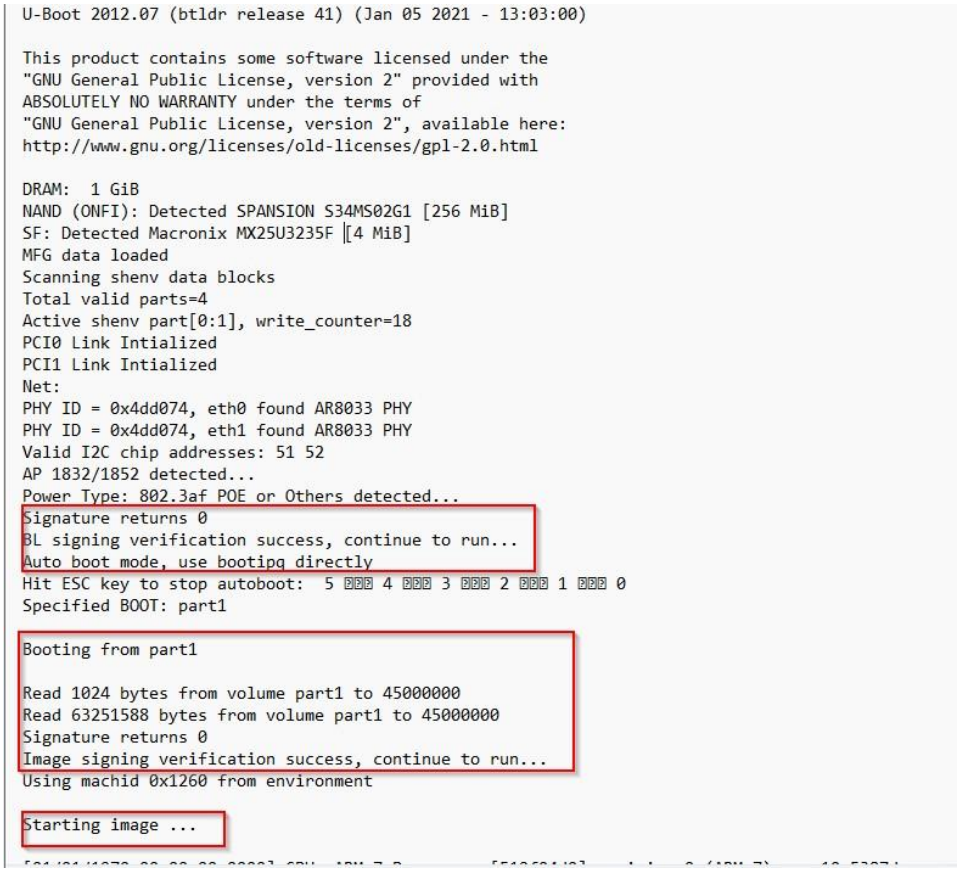
11.1.3 **Test Case Description:** Verifying the self-test when DUT boot up.

11.1.4 **Execution Steps:** Below are the execution steps with evidence:

When DUT powered on of restart firstly DUT Boot up at AP mode the after 2 to 3 minutes automatically boot up for controller mode.

-Tester powered on the DUT.

Verification under AP MODE are as follows.



For part1 image verification is success (above screenshot).

Above screenshots show starting Image after all checks done success and image is valid.

```
         Starting Cisco seed generation...
         Starting Cisco platform file generation...
         Starting Cisco fips check...
[[32m  OK  [0m] Started Cisco system time setup.
[[32m  OK  [0m] Started Cisco seed generation.
[*06/13/2023 05:39:17.4998] GCM-128 POST passed

[*06/13/2023 05:39:17.4998] GCM-256 POST passed

[[32m  OK  [0m] Started Cisco platform file generation.
[[32m  OK  [0m] Started Cisco fips check.
[[32m  OK  [0m] Reached target Local File Systems.
         Starting Cisco pkg install service...
         Starting Cisco S10 boot service...
[[32m  OK  [0m] Started Cisco system time saving.
         Starting Cisco system time saving...
```

Above screenshot evident that POST pass for GCM-128 and GCM-256.

- Verification under WLC MODE are as follows:
- Following screenshot is evident the Cryptographic self-test

```
Starting the Switchdriver...
Starting Switchdriver...

Cryptographic library self-test....
Testing SHA1 Short Message 1
Testing SHA256 Short Message 1
Testing SHA384 Short Message 1
SHA1 POST PASSED
Testing HMAC SHA1 Short Message 1
Testing HMAC SHA2 Short Message 1
Testing HMAC SHA384 Short Message 1
passed!
```

- SHA1 POST passed.

```
Cisco AireOS Version 8.10.183.0
Initializing OS Services: Starting DB Services...
ok
Initializing Serial Services: ok
Initializing Network Services: ok
Starting Statistics Service: ok
Unable to open dx flag file
Starting ARP Services: ok
Starting Trap Manager: Starting PNP: ok
ok
```

- - Various services check

11.1.5 **Test Observations:**

- Power on the DUT (AP 1852i) and verify the self-test to identify cryptographic functions security mechanism.
- It has been observed that cryptographic library all test passed which includes SHA1, SHA256, SHA384, HMAC SHA1, HMAC SHA2, HMAC SHA384.

12. Test Case Result:

S. No	**TEST CASE NAME**	**PASS/FAIL**	**Remarks**
1	TC_NO_SELF_TEST	FAIL	

1.3.9 Feature / Service Activation Policy

<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 3 - Software Security
2. **<Security Requirement No & Name >** 1.3.9 Feature / Service Activation Policy
3. **<Requirement Description: >**
   The CPE shall have factory default settings such that only the essential features / services and ports required for main operational needs of CPE are only enabled. Optional features, added services, futuristic service / applications are disabled by default. Such disabled services could only be enabled after successful authentication and selection by ADMIN user.
4. **DUT Confirmation Details**:
   - This section involves information about DUT like software/firmware version, Hardware version model.
   - DUT Cisco WLC contains default boot image with version 8.10.183.0. The model is AIRAP1852I-E-K9. The inventory shows model serial no. & model description.
   - Verification of DUT Cisco wireless LAN controller's HW product series information by running command *show inventory* on CLI.

```
(Cisco Controller) >show inventory

Burned-in MAC Address.............................. 38:ED:18:C8:10:60
Maximum number of APs supported.................... 50
NAME: "Mobility Express"    , DESCR: "Cisco Aironet 1850 Series Mobility Express"
PID: AIR-AP1852I-E-K9,  VID: V01,  SN: KWC193100UU
```

   - Verification of DUT Cisco WLC's high-level system SW information by running command *show sysinfo* on CLI.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name................................ Cisco Systems Inc.
Product Name....................................... Cisco Controller
Product Version.................................... 8.10.183.0
OUI File Last Update Time.......................... N/A

System Name........................................ Aironet-Controller
System Location.....................................
System Contact......................................
System ObjectID.................................... 1.3.6.1.4.1.9.1.2250
IP Address......................................... 10.208.38.2
Last Reset......................................... 1: reload command

System Up Time..................................... 0 days 3 hrs 33 mins 5 secs
System Timezone Location........................... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
System Stats Realtime Interval..................... 5
System Stats Normal Interval....................... 180

Configured Country................................. IN  - India

State of 802.11b Network........................... Enabled
State of 802.11a Network........................... Enabled

--More-- or (q)uit
```

   - Verification of DUT Cisco WLC's system information on Web access.

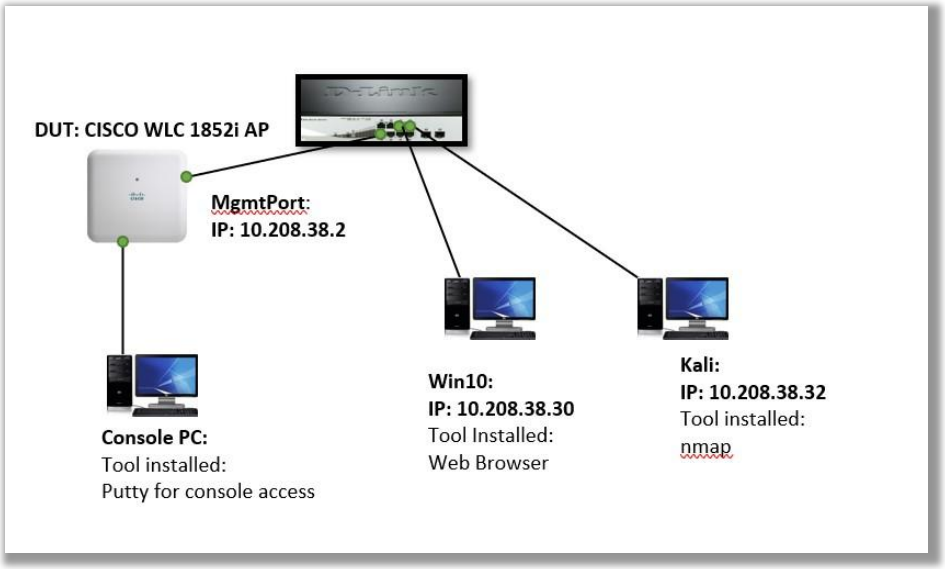
5. **DUT Configuration**: No additional configuration required as tester test this requirement on by default configuration (after initial setup done).
6. **Preconditions:**
   Below are the preconditions: -
   - Vendor/OEM documentation requires stating what are the essential service/feature and port which are required for operational of the DUT.
   - Vendor/OEM documentation require stating what are the service/feature or port are enabled and disabled.
   - Vendor/OEM documentation require how to disable or enabled the services.
   - Tester has the highest level of access to DUT.
     Connectivity is through as per diagram.
7. **Test Objective:** To verify that DUT have factory default settings such that only the essential features / services and ports required for main operational needs of CPE are only enabled.

8. **Test Plan:**
   - Validating the DUT have factory default settings
   - Validating the DUT disabled services only be enabled by ADMIN user.

8.1 **Number of Test Scenarios:**

8.1.1 Validating the default services enabled by DUT after factory reset.

8.2 **Test Setup Diagram**



8.3 **Tools Used:** DUT terminal(Console), DUT Webpage and Nmap

8.4 **Test Execution Steps:**

Below are the execution steps:

- Run nmap scan for tcp/udp and verify all those services have well defined in oem/vendor documentation about their enable or disable status by default.
- Restart the DUT and verify the services while booting the DUT and check all those services are listed in booting guide.
- Loging to DUT via web-interface and verify the services which are enable able disable by default.

9. **Expected Result for Pass:** Optional features, added services, futuristic service / applications are disabled by default. Such disabled services only enabled by ADMIN user.
10. **Expected Format of Evidence:** Screenshot of DUT terminal(Console), DUT Webpage and Nmap

11. **Test Execution:**

11.1.1 **Test Case Number:** 01

11.1.2 **Test Case Name:** TC_NO_FEATURE_ACTIVATION

11.1.3 **Test Case Description:**

In this requirement the tester use Nmap to scan TCP/UDP services and verifying their status against the vendor documentation. After restarting the DUT, the services are checked during the boot process to ensure they match the booting guide. Finally, by logging into the DUT via the web interface, the default status of the services is verified and all those services should enable or disable as per the admin guide or vendor document.

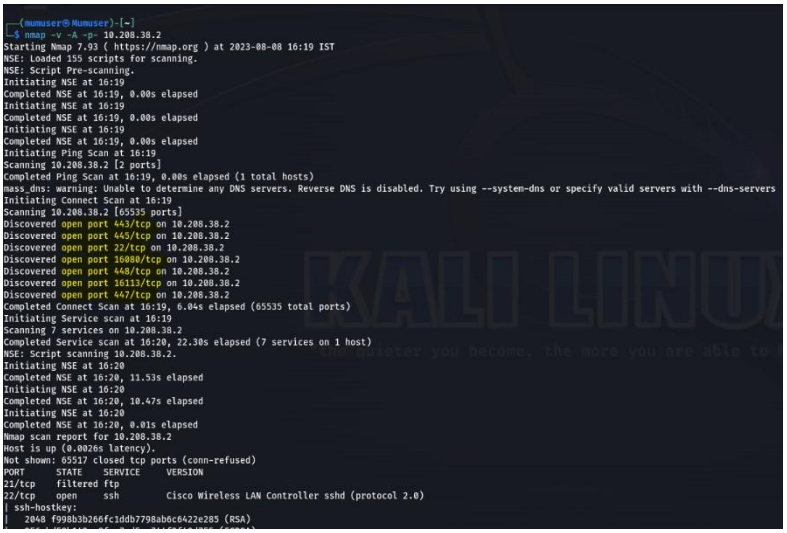
11.1.4 **Execution Steps:**

11.1.5 Evidence Provided

Below is the execution step with evidence:

1. Run nmap scan for tcp/udp and verify all those services have well defined in oem/vendor documentation about their enable or disable status by default.

- Perform nmap TCP scan on Cisco WLC.



- Perform nmap UDP scan on Cisco WLC.

- Result of UDP nmap scan

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-09 13:06 IST
Initiating ARP Ping Scan at 13:06
Scanning 10.208.38.2 [1 port]
Completed ARP Ping Scan at 13:06, 0.06s elapsed (1 total hosts)
Initiating UDP Scan at 13:06
Scanning 10.208.38.2 [65535 ports]
UDP Scan Timing: About 2.18% done; ETC: 13:29 (0:23:14 remaining)
UDP Scan Timing: About 4.82% done; ETC: 13:29 (0:22:02 remaining)
UDP Scan Timing: About 9.02% done; ETC: 13:29 (0:20:51 remaining)
UDP Scan Timing: About 13.87% done; ETC: 13:29 (0:19:40 remaining)
UDP Scan Timing: About 18.73% done; ETC: 13:28 (0:18:31 remaining)
Discovered open port 161/udp on 10.208.38.2
UDP Scan Timing: About 22.59% done; ETC: 13:27 (0:16:20 remaining)
UDP Scan Timing: About 44.33% done; ETC: 13:18 (0:06:37 remaining)
UDP Scan Timing: About 73.06% done; ETC: 13:14 (0:02:08 remaining)
Completed UDP Scan at 13:12, 369.37s elapsed (65535 total ports)
Nmap scan report for 10.208.38.2
Host is up (0.0021s latency).
Not shown: 65534 open|filtered udp ports (no-response)
PORT    STATE SERVICE
161/udp open  snmp
MAC Address: 00:00:5E:00:01:01 (Icann, Iana Department)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 369.62 seconds
           Raw packets sent: 131257 (6.339MB) | Rcvd: 379 (26.989KB)
```

After TCP nmap completion it has been observed that DUT has HTTP service enabled by default. To disable HTTP initially on DUT, vendor doc required.

After UDP nmap completion it has been observed that DUT has SNMP service enabled by default. To disable SNMP initially on DUT, vendor doc required.

2. Restart the DUT and verify the services while booting the DUT and check all those services are listed in booting guide or administrator guide.

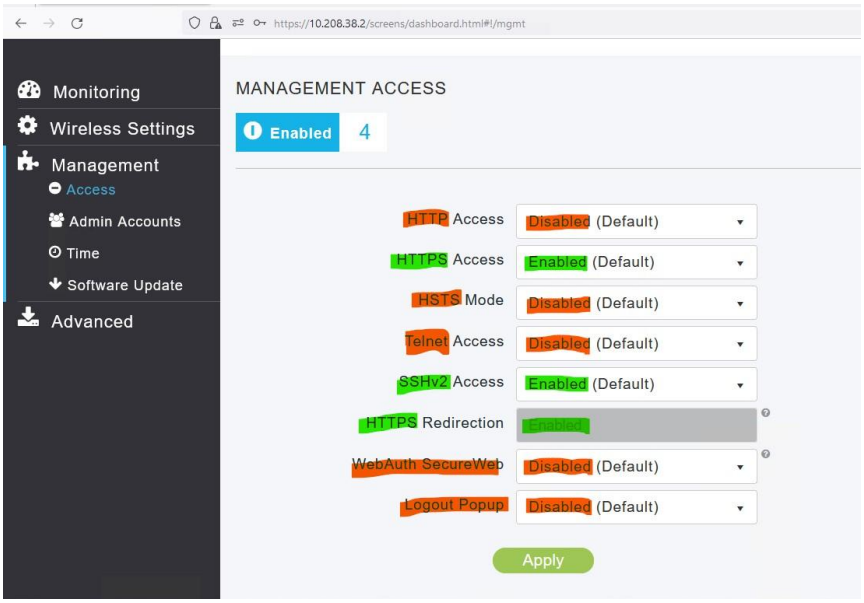
```
XML config selected
Starting SSHD: Generating Secure Shell DSA Host Key ...
Generating Secure Shell RSA Host Key ...
Generating Secure Shell version 2 ECDSA Host Key ...
ok
Starting Redis-Server: ok
Starting naconnector: ok
Starting nginx: ok
Starting NA Connector...
creating logs dir
Validating XML configuration
Cisco is a trademark of Cisco Systems, Inc.
Software Copyright Cisco Systems, Inc. All rights reserved.

Cisco AireOS Version 8.10.183.0
Initializing OS Services: Starting DB Services...
ok
Initializing Serial Services: ok
Initializing Network Services: ok
Starting Statistics Service: ok
Unable to open dx flag file
Starting ARP Services: ok
Starting Trap Manager: Starting PNP: ok
ok

Starting Data Externalization services: ok
Starting Network Interface Management Services: ok
Starting System Services: ok
Starting SNMP services: ok
Starting Fastpath Hardware Acceleration: Starting Switching Services: ok
Starting QoS Services: ok
Starting Policy Manager: ok
Starting Data Transport Link Layer: ok
Starting Access Control List Services: ok
Starting System Interfaces: ok
Starting Client Troubleshooting Service: ok
Starting Certificate Database: PnP config is saved to storage
Initializing Curl Globally..
ok
```

During boot process after image signing process, DUT start the abovementioned services.

Note: It is required that vendor should give all relevant documentation or guide so that tester can verify services for testing requirement.

3. Loging to DUT via web-interface and verify the services which are enable able disable by default.

Logged-in with Admin command. Below screenshot represent the services which are enable or disable by default.



By default, on web-gui interface of DUT it has been observed that HTTPS, sshv2, HTTPS redirection services are enabled by default.

11.1.6 **Test Observations:** It has been observed that after completion of Nmap scan for TCP/UDP services on the Cisco WLC, the results showed that the HTTP and SNMP services were enabled by default. To disable these services, vendor documentation is required. Upon restarting the DUT, the services were verified during the boot process. Logging into the DUT via the web interface showed that HTTPS, SSHv2, and HTTPS redirection were enabled by default. It's important to have all relevant vendor documentation for verification of services for testing requirements.

12. Test Case Result:

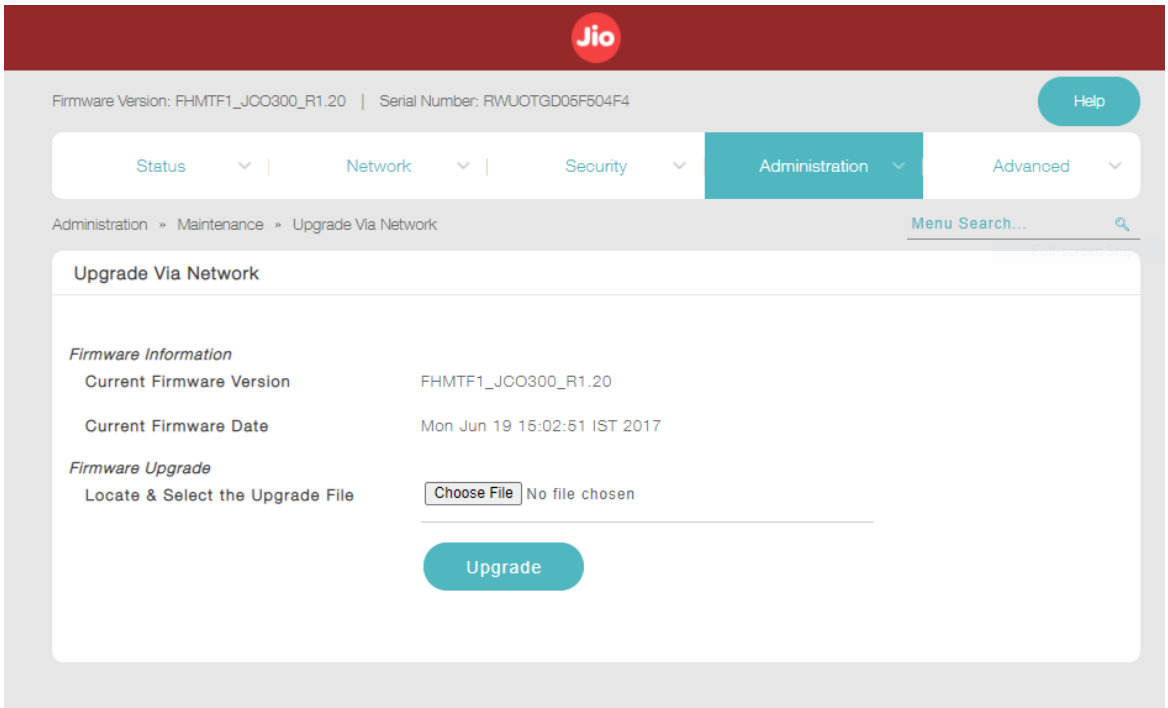
S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_SELF_TEST		Based on OEM document

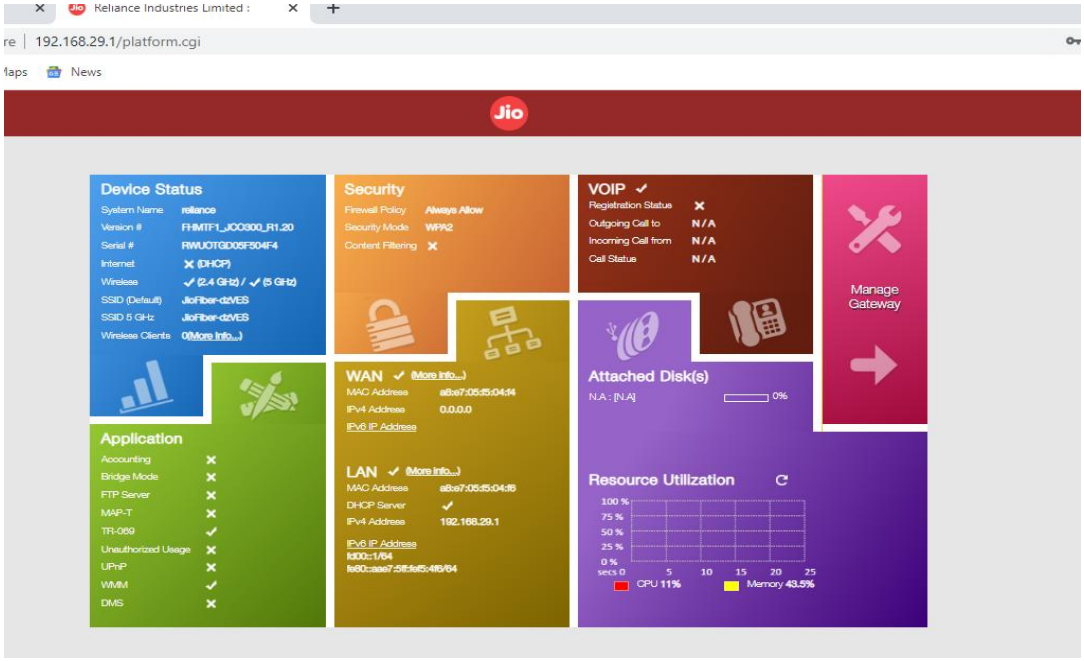
1.3.10 Restricted reachability of services

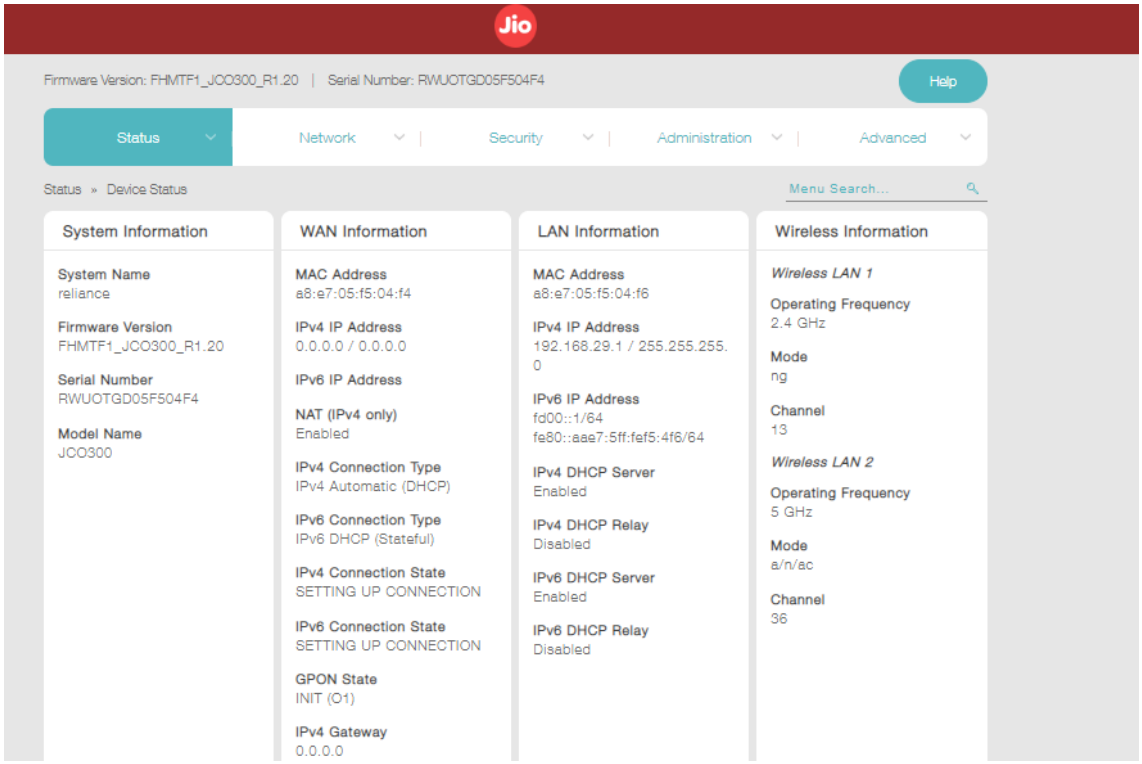
<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 3 - Software Security
2. **<Security Requirement No & Name >** 1.3.10 Restricted reachability of services
3. **<Requirement Description: >** The CPE shall restrict the reachability of services so that they can only be reached on interfaces where their usage is required. OEM to map the essential services required to be accessed from WAN side, LAN side to limit access to services only on need / functionality basis. For Interfaces on which services are active, the reachability to be limited to legitimate communication peers. One such Use-case scenario is to restrict web management access of CPE to only LAN ports and not to permit access on Wi-Fi, WAN side.
4. **DUT Confirmation Details**:
   - Use the command line/GUI interface to get details of the machine on which test is conducted.
   - Use GUI to get Application No/Version No & hardware Info

The below screenshot shows the firmware version of the DUT

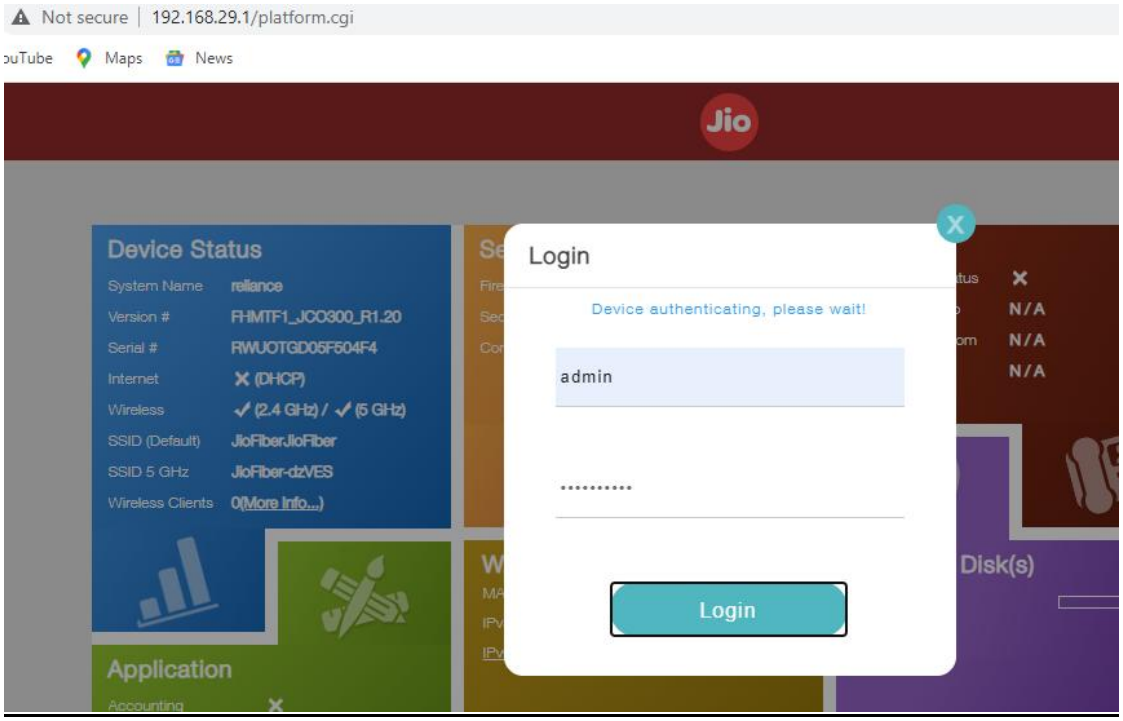






5. **<u>DUT Configuration</u>**:

- The Tester opens GUI(https) of DUT(192.168.29.1) in tester machine (192.168.29.118).



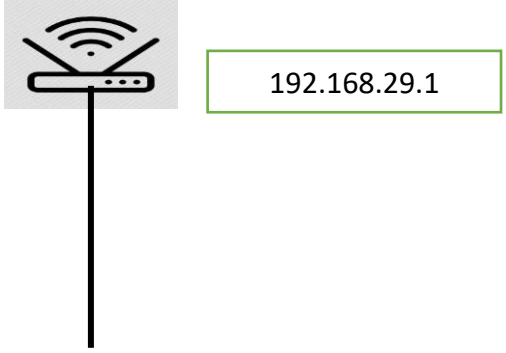
- The Tester attempts to login DUT using “admin” account.

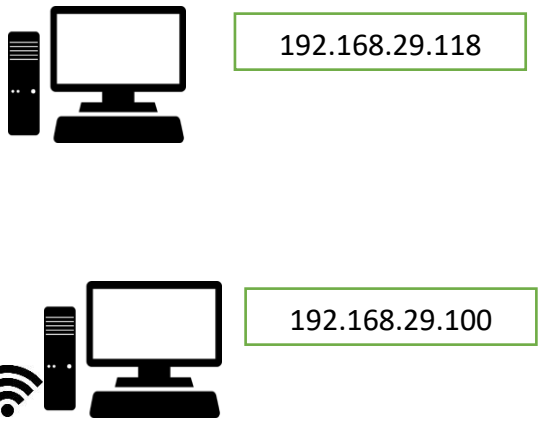
6. **Preconditions:** OEM need to provide documentation regarding how to restrict the services in the DUT

7. **Test Objective:** To verify that it is possible to bind the services only to the interfaces from which they are expected to be reachable.

8. **Test Plan:**
   - The tester shall identify what all interfaces available on the DUT.
   - Bind the services to particular interface, verify the services are active on that interface only (other interfaces should not get service)
   - Verify legitimate communication peers only getting services

   8.1 **Number of Test Scenarios:**
   8.1.1 Restricted reachability of services
   8.1.2 Legitimate communication peers
   8.2 **Test Setup Diagram**





8.3 **Tools Used:** Web browser(client)

Note : Nmap or Zenmap can be used to verify the services available to particular interfaces.

8.4 **Test Execution Steps:**

- The tester must verify for the compliance to the pre-requisites:
- Restricted reachability of services
- Bind the services to LAN(wired- 192.168.29.118) interface , verify the DUT webpage accessible on that interface only(other interfaces(wireless) should not load webpage)
- Legitimate communication peers
- Configure ACL in the DUT to allow access from ip address 192.168.29.1 and deny others. Verify legitimate communication peers only getting reachable(other than 192.168.29.1 should not reachable)

9. **Expected Result for Pass:**
Services can be enabled on per-interface basis.

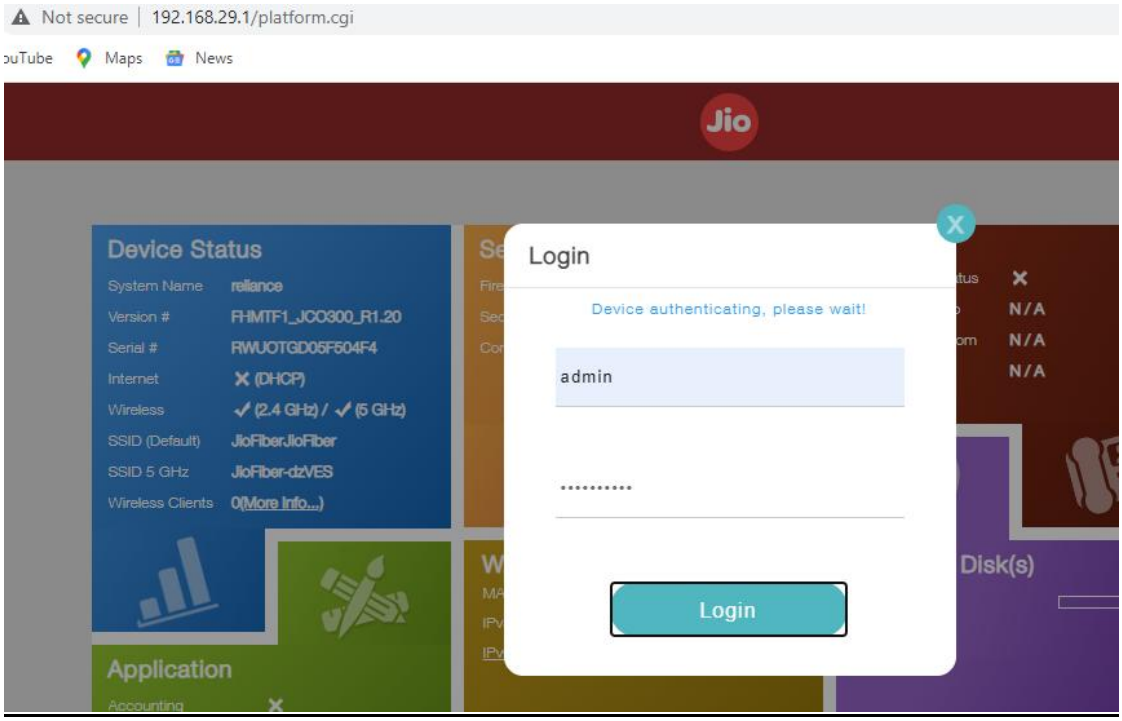
10. **Expected Format of Evidence:**

- Screenshot of DUT webpage

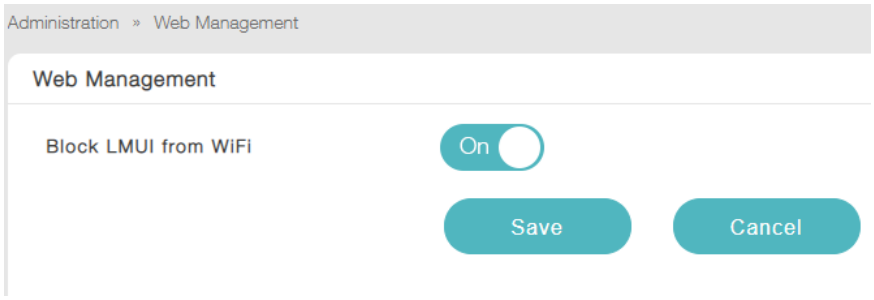
11. **Test Execution:**

11.1.1 **Test Case Number:** 01
11.1.2 **Test Case Name:** TC_NO_RESTRICTED_REACHABILITY_OF_SERVICES
11.1.3 **Test Case Description:** Ensuring that DUT can be accessible by configured interface only
11.1.4 **Execution Steps:**

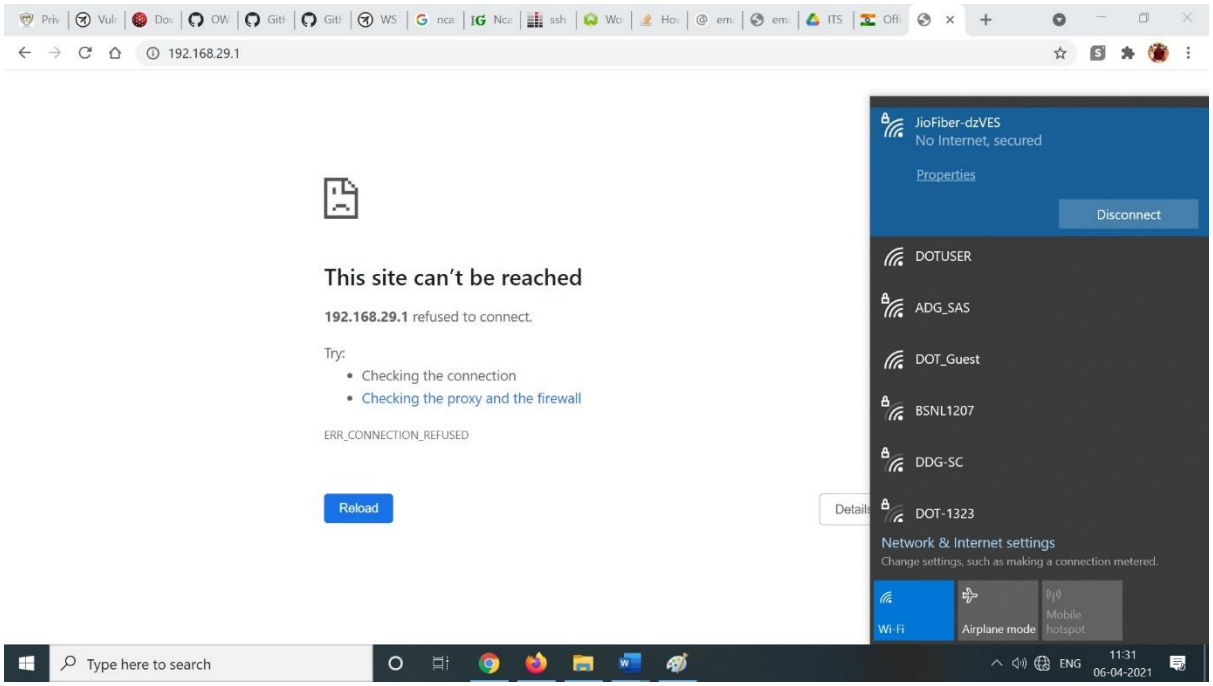
- Login to the DUT with admin credentials



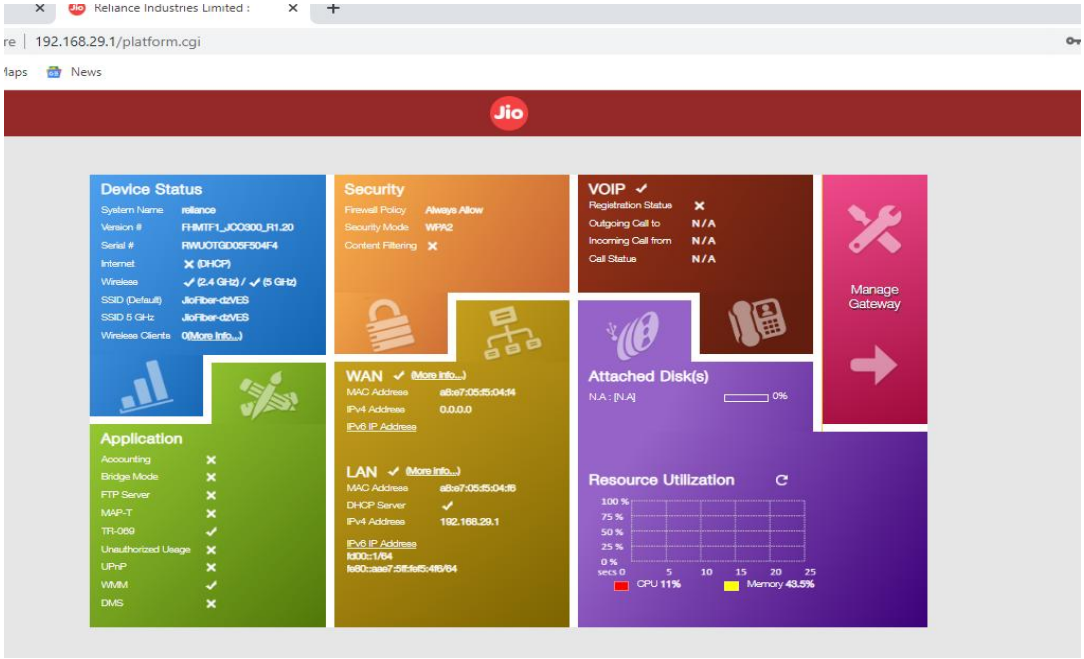
- Configure LMUI(Local Mode User Interface) option for restricting the DUT webpage access from WiFi interface(Wired allowed).



- Check the DUT access from wireless connected tester machine ip address 192.168.29.100.



- Access DUT from wired interface tester machine ip address 192.168.29.118



Note : The tester same need to be perform for WAN interface also.

11.1.5 **Test Observations:**

- The DUT only accessible from configured interface(wired) only. Not accessible from unconfigured interface(WiFi).

Test Case Number: 02

11.2.1 **Test Case Name:** TC_NO_LEGITIMATE_COMMUNICATION_PEERS

11.2.2 **Test Case Description:** Ensuring that DUT can be accessible by legitimate host only

11.2.3 **Execution Steps:**

Positive case :

- Configure the ACL rule to allow access from WiFi interface tester machine ip address 192.168.29.100
- Ping the DUT from tester machine ip address 192.168.29.100
- It should be reachable

Negative case :

- Configure the ACL rule to deny access from WiFi interface tester machine ip address 192.168.29.100
- Ping the DUT from tester machine ip address 192.168.29.100
- It shouldn't be reachable

12. Test Case Result:

S. No	**TEST CASE NAME**	**PASS/FAIL**	**Remarks**
1	TC_NO_RESTRICTED_REACHABILITY_OF_SERVICES	PASS	DUT accessible from Wired interface(LAN) and not accessible from wireless(LAN)
2	TC_NO_LEGITIMATE_COMMUNICATION_PEERS		Not performed

Section 1.4: System Secure Execution Environment

1.4.1 System Secure Execution Environment

<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 4 System Secure Execution Environment
2. **<Security Requirement No & Name >** 1.4.1 No unused functions
3. **<Requirement Description: >** Unused functions of the CPEs' software and hardware shall be deactivated. During installation of software and hardware often functions will be activated that are not required for operation or function of the system. If unused functions of software cannot be deleted or de-installed individually, such functions shall be deactivated in the configuration of the CPE in permanent manner. Also, hardware functions which are not required for operation or function of the system (e.g., unused interfaces) shall be permanently deactivated. Permanently means that they shall not be reactivated again after CPE reboot. OEM to provide report in this regard, List of the used functions of the CPE's software and hardware as given by the OEM shall match the list of used software and hardware functions that are necessary for the operation of the CPE.
4. **DUT Confirmation Details**:
   - This section involves information about DUT like software/firmware version, Hardware version model.
   - DUT Cisco WLC contains default boot image with version 8.10.183.0. The model is AIRAP1852I-E-K9. The inventory shows model serial no. & model description.
   - Verification of DUT Cisco wireless LAN controller's HW product series information by running command *show inventory* on CLI.

```
(Cisco Controller) >show inventory

Burned-in MAC Address.............................. 38:ED:18:C8:10:60
Maximum number of APs supported..................... 50
NAME: "Mobility Express"    , DESCR: "Cisco Aironet 1850 Series Mobility Express"
PID: AIR-AP1852I-E-K9,  VID: V01,  SN: KWC193100UU
```

   - Verification of DUT Cisco WLC's high-level system SW information by running command *show sysinfo* on CLI.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.10.183.0
OUI File Last Update Time........................ N/A

System Name...................................... Aironet-Controller
System Location..................................
System Contact...................................
System ObjectID.................................. 1.3.6.1.4.1.9.1.2250
IP Address....................................... 10.208.38.2
Last Reset....................................... 1: reload command

System Up Time................................... 0 days 3 hrs 33 mins 5 secs
System Timezone Location......................... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
System Stats Realtime Interval................... 5
System Stats Normal Interval..................... 180

Configured Country............................... IN  - India

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled

--More-- or (q)uit
```

- Verification of DUT Cisco WLC's system information on Web access.

5. **DUT Configuration**: Depending on vendor inputs.

6. **Preconditions:** The vendor shall provide the following list of requirements:

   a. A list of all software and hardware functions that are included in the product, with the identification of all necessary functions that are required for operation of system, along with their physical or logical interfaces.
   b. A list of all available software and associated components containing at least the following information shall be included in the documentation accompanying the Network Product:
      - Name of the software
      - Version of the software installed.
      - List of dependencies and versions
      - Any add-ons and functions
      - Any special hardware/debugging ports.
      - Software support type
      - Licensing information
      - Requirement during functioning of system
      - Brief description of their purpose

c. List of available software or Hardware and its associated components which are not required for operations should be mentioned with their physical & logical interfaces.
d. Process of how to disable unused software and hardware functions/interfaces permanently, with their detailed configurations.

7. **Test Objective:** Unused software and hardware components deleted/disabled in the DUT

8. **Test Plan:**
   - Identify the unused software and hardware components in the DUT
   - Delete/Disable the unused software and hardware components in the DUT
   - Reboot the DUT and check the status of Delete/Disable the unused software and hardware components in the DUT

   8.1 **Number of Test Scenarios:**

   8.1.1 Validating the unused software/hardware in the DUT

   8.2 **Test Setup Diagram**

Testing Terminal
Test Terminal OS: Linux Ubuntu 22.04.3
IP Address: 10.208.38.11
Putty V 0.76
OpenSSH_8.9p1

DUT
Cisco AP Aironet 1850
IP Address: 10.208.38.2

8.3 **Tools Used:**

- Syft, Blackduck SCA, Cmdline/GUI of DUT

8.4 **Test Execution Steps:**

(i) Identify from vendor's list all ports/interfaces which are required for operation and using the vendor documentation, perform the following steps:

- For Example: To verify the physical aux interface enter command "Show line aux0"

(ii) Identify from vendor's list all ports/interfaces which are not required for operation and using the vendor documentation, perform the following steps:

- Check document provided by vendor on how to disable the unused services/ interfaces.
- Attempt to perform disabling functions on interfaces as per documentation provided & verify that the interface is disabled.
- Verify the unused ports/services remains disabled on reboot of the DUT.

(iii) Identify the hardware and software functions installed in the DUT which might have been disabled by using any suitable command line tools or any other suitable means of determination.

(iv) Validate that there are no entries in the vendor provided list of 'hardware and software functions', apart from those that were identified as 'necessary for the operation of the wifi cpe'

(v) Verify the list of software, libraries and associated components, versions using Nessus, Black Duck from SBOM provided by vendor.

NOTE: When user will have root access following points will be considered

- Additional services/functionalities may get activated.
- Tester will run Nmap scan or Nessus scan to find any additional service/functionalities vulnerability.

9. **Expected Result for Pass:** Unused software/hardware will be disabled/deleted in the DUT
10. **Expected Format of Evidence:** Screenshot of tools used
11. **Test Execution:**

11.1.1 **Test Case Number:** 01

11.1.2 **Test Case Name:** TC_NO_UNUSED_SOFTWARE_HARDWARE

11.1.3 **Test Case Description:** Verifying the DUT not have any unused software/hardware will be deleted/disabled

11.1.4 **Execution Steps:**

Depending on the vendor inputs.

For one such hardware functions instance considered here for demo:

- Case 1: Vendor shall provide documentation to verify list of default used physical interfaces/ports.

  - To be completed after vendor provides documentation –

  - The evaluator has identified that there are 2 physical interfaces available on DUT.
    - POE/ management port: The POE port or the management port is used to provide power to DUT, this port cannot be disabled, as this port is only power supply available for DUT.
    - AUX port: it is designed to perform port Link Aggregation (LAG). The AUX port will be disabled by default.
      The AUX port is not manageable and is simply bridged back to the controller. Avoid connecting another AP to this port or devices such as switches/hubs or the same switch or uplink as the PoE port because it can create spanning tree loop issues.
- Case 2: DUT shall support the mechanism to identify all the physical interface and to disable them.
  - Login with 'admin' user and run command 'show interface summary' to check the management physical interface and its status.

```
User:Admin
Password:*********emWeb: Aug 28 19:12:06.087: %AAA-5-AAA_AUTH_ADMIN_USER: aaa.c:3334 Authentication succeeded f
*emWeb: Aug 28 19:12:06.115: %APF-5-COUNTRY_NOT_FOUND: apf_channel.c:3021 Country 'J2' not found in country dat

 Warning: Missing TFTP/CCO params, Please Configure the Image Download Params

Welcome to the Cisco Mobility Express command line interface.
Only commands which are listed in the command reference guide for this release are supported.
http://www.cisco.com/c/en/us/support/wireless/mobility-express/products-command-reference-list.html

Warning:In SNMPV2 No Defaults Presents.
Please use command: config snmp community create <name>
```

Screenshot showing the user admin logged in successfully.

```
(Cisco Controller) >show interface summary


 Number of Interfaces..... 2

Interface Name                   Port Vlan Id  IP Address      Type    Ap Mgr Gu
-------------------------------- ---- -------- --------------- ------- ------ --
management                       1    untagged 10.208.38.2     Static  Yes    N/
virtual                          N/A  N/A      192.0.2.1       Static  No     N/
```

Screenshot showing 1st physical interface management interface with is the POE interface as well.

- Run command. 'show ap lag-mode' to check the status of AUX port.

```
(Cisco Controller) >show ap lag-mode

LAG-Mode Support ..............................Disabled
```

Screenshot showing the link aggregation mode is by default disabled this is used by AUX port which is 2nd physical port, and this port is only used for lag-mode.

- Once interface list is displayed, evaluator found out that AUX port is an unused port, and it cannot be used as it poses threat of spanning tree loop. So, to shut the AUX port execute command.

```
(Cisco Controller) >config ap lag-mode support disable

Warning! All APs with LAG enabled will be rebooted.
And non lag APs will have DTLS connection teared down causing
 them to disjoin and rejoin again.
 Are you sure you want to continue? (y/n) y
```

Screenshot showing the command to disable the link aggregation mode which is used by AUX port it is same as disabling the physical AUX port.

Verify the status of the AUX port with command 'show ap lag-mode'.

```
(Cisco Controller) >show ap lag-mode

LAG-Mode Support ..............................Disabled
```

- Case 3: All the unused physically accessible interface shall remain disable after reboot.

Now reboot the device with 'restart' command. Screenshot showing the restart command executed and DUT has initiated restart.

```
(Cisco Controller) >restart

The system has unsaved changes.
Would you like to save them now? (y/N) y


Configuration Saved!
```

Once reload is complete login to DUT with 'admin' user. Screenshot showing the login successful with user admin.

```
User: Admin
Password:********
 Warning: Missing TFTP/CCO params, Please Configure the Image Download Params

Welcome to the Cisco Mobility Express command line interface.
Only commands which are listed in the command reference guide for this release ar
http://www.cisco.com/c/en/us/support/wireless/mobility-express/products-command-r
```

Verify the status of disabled interface. (It should remain disabled after reboot)

```
(Cisco Controller) >show ap lag-mode

LAG-Mode Support ..............................Disabled

(Cisco Controller) >
```

Screenshot showing the AUX port remained disabled after reboot.

11.1.6 **Test Observations:**

- Case 1: It is observed that the evaluator has identified there are 2 physical ports on DUT,
  - *POE/ management port: The POE port or the management port is used to provide power to DUT, this port cannot be disabled, as this port is only power supply available for DUT.*
  - *AUX port: it is designed to perform port Link Aggregation (LAG). The AUX port will be disabled by default. The AUX port is not manageable and is simply bridged back to the controller. Avoid connecting another AP to this port or devices such as switches/hubs or the same switch or uplink as the PoE port because it can create spanning tree loop issues.*
- Case 2: It is observed that the unused AUX port is by disabled by default, also it can be disabled manually with command. The unused physical aux port is not manageable directly, but it can be managed indirectly with lag mode commands, The AUX port remain disabled after reboot as well.

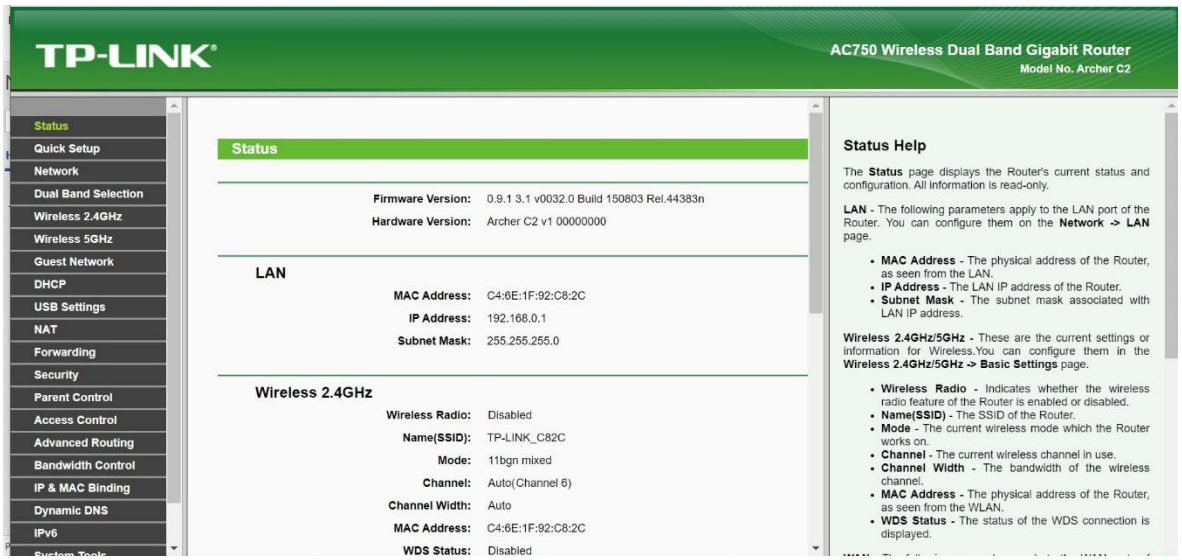
12. Test Case Result:

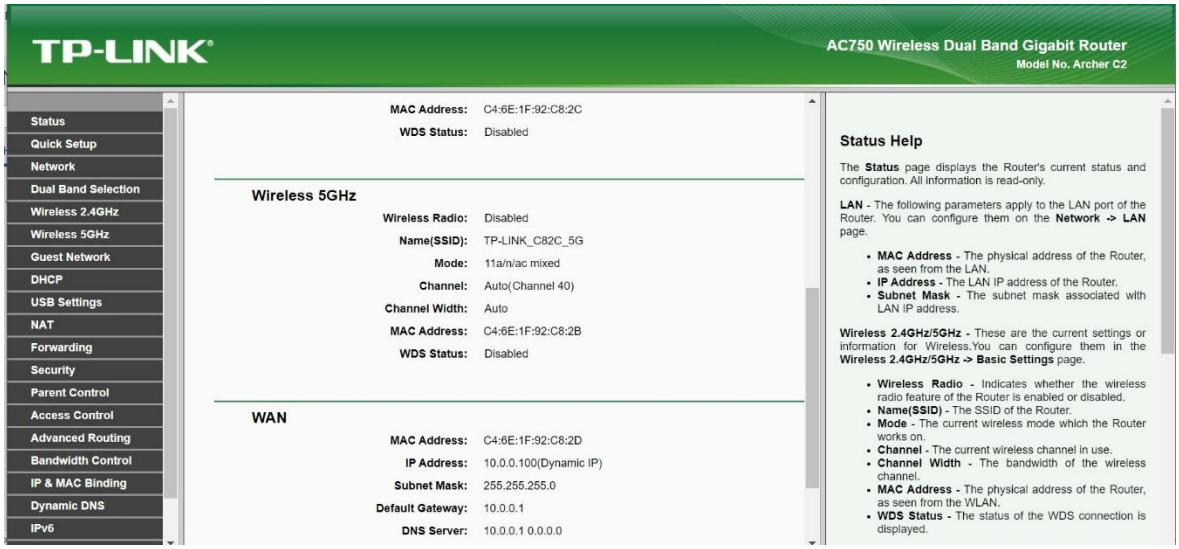
S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_UNUSED_SOFTWARE_HARDWARE		Testcase is incomplete

1.4.2 No unsupported components

<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 1.4 System Secure Execution Environment
2. **<Security Requirement No & Name >** 1.4.2 No unsupported components
3. **<Requirement Description: >** The CPE shall not contain software and hardware components that are no longer supported by their vendor, producer or developer, such as components that have reached end-of-life or end- of-support. Excluded are components that have a special support contract. This contract shall guarantee the correction of vulnerabilities over components' lifetime. OEM to provide report and declaration to this effect.
4. **DUT Confirmation Details**:
    - Use the command line/GUI interface to get details of the machine on which test is conducted.
    - Use GUI to get Application No/Version No & hardware Info





5. **DUT Configuration**: No additional configuration is required to perform this test case.
6. **Preconditions:**
   - OEM shall provide the testing report regarding network product shall not contain software and hardware components that are no longer supported by their vendor, producer, or developer, such as components that have reached end-of-life or end-of-support.
   - OEM need to provide supportive documents for how to check software and hardware components information on the DUT.

7. **Test Objective:** To verify that there is no EoL/EoS software and hardware components available in the DUT.
8. **Test Plan:**
   - The tester should verify the OEM providing composition analysis testing report for opensource(SCA) / third-party(SLA) / proprietary(OEM) software components
   - The tester should verify the EoL/EoS of hardware components like CPU(+chipset), Network and other components in the DUT.

   8.1 **Number of Test Scenarios:**

   8.1.1 Validate the composition analysis test report from OEM

   8.2 **Test Setup Diagram**

   8.3 **Tools Used:** Blackduck SCA tool

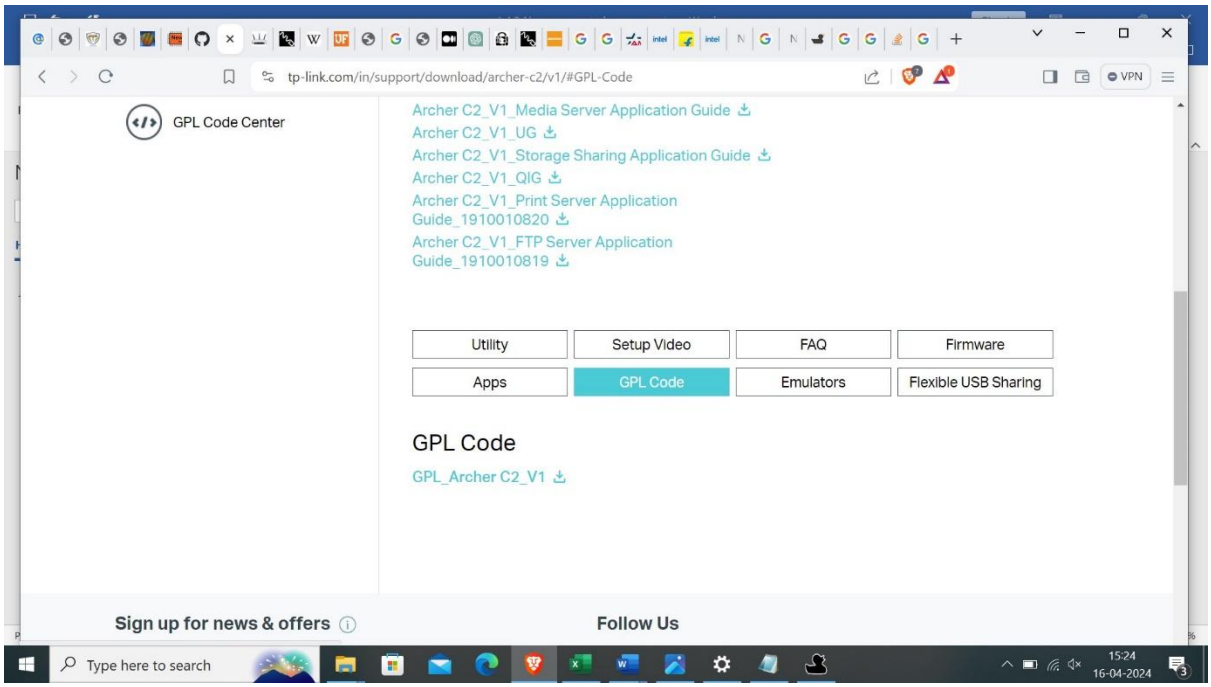
   8.4 **Test Execution Steps:**
   - Validate the software list provided by vendor
   - Validate the Hardware list provided by OEM

9. **Expected Result for Pass:** There should be no EoL/EoS components present in the DUT at the time of testing
10. **Expected Format of Evidence:** Screenshot of tool used for finding the EoL/EoS

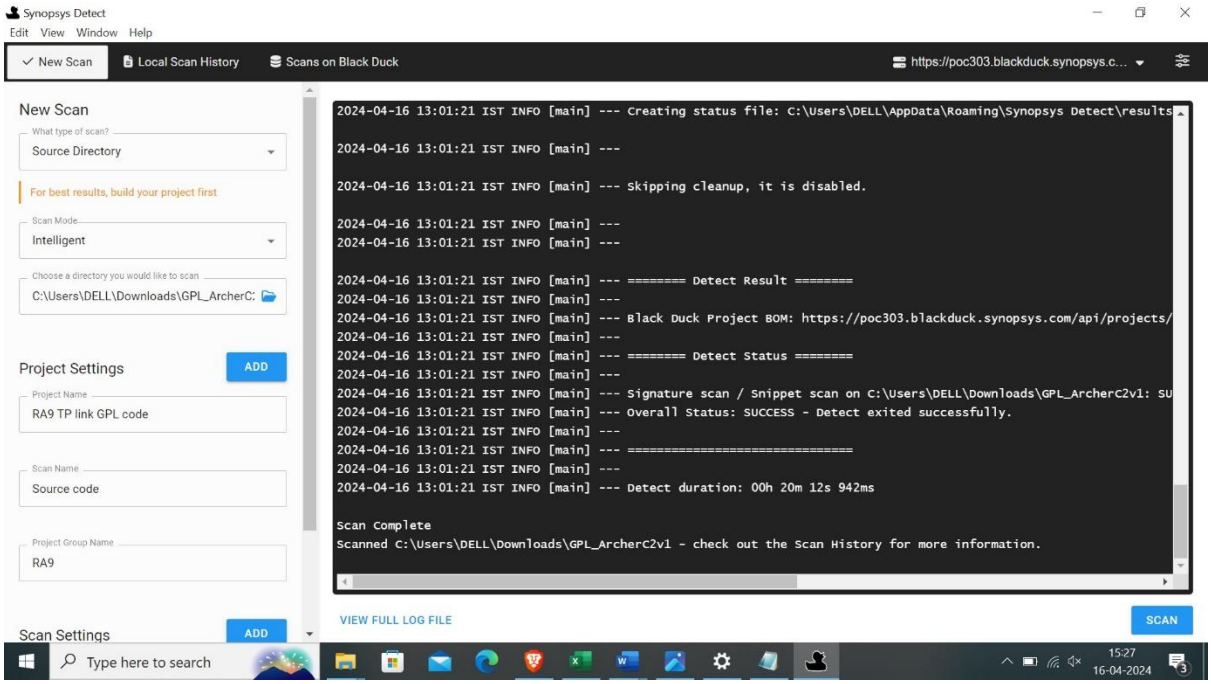
11. **Test Execution:**

11.1.1 **Test Case Number:** 01
11.1.2 **Test Case Name:** TC_NO_UNSUPPORTED_COMPONENTS
11.1.3 **Test Case Description:** Ensuring that DUT not have any EoL/EoS component present in the DUT.
11.1.4 **Execution Steps:**
Note : Currently, we don't have vendor support
Find Software components :

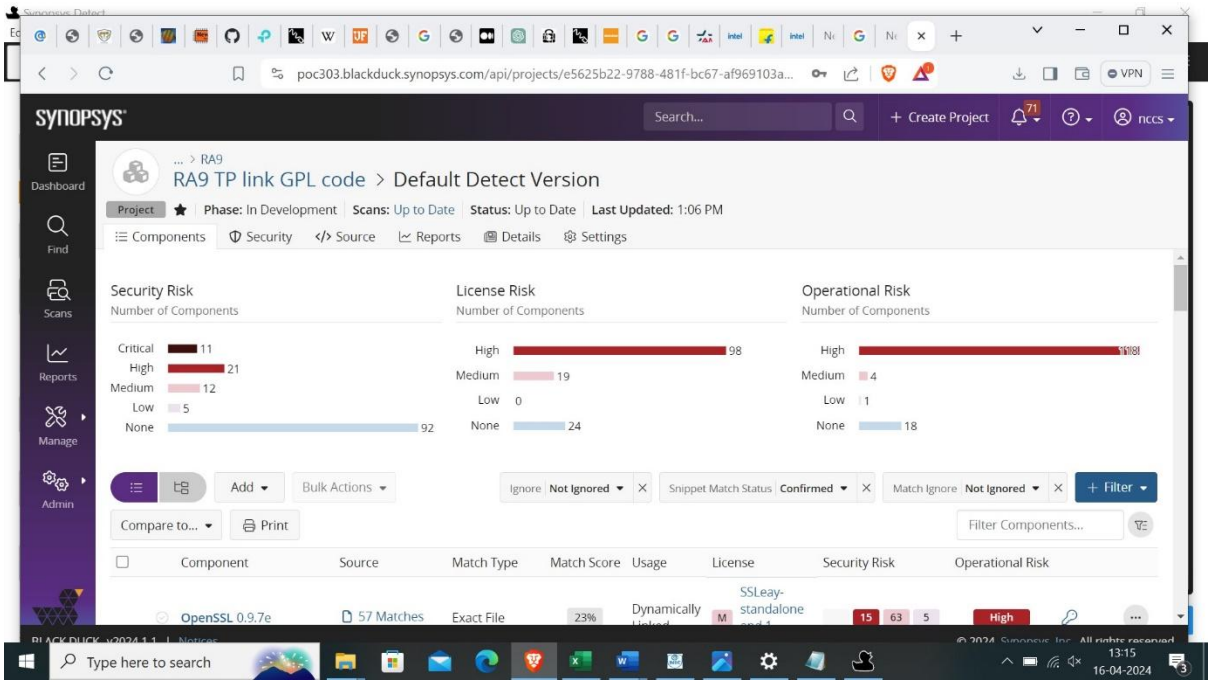
- Validate the Software composition analysis report shared by the OEM. SCA tool running in tester machine(192.168.29.118)
- Note : For demo purpose, I have taken source code of TP link WiFi CPE from their website. Suppose, If the DUT vendor not providing source code of DUT, then we need to ask binary code of DUT in unobstructed mode(No encryption).
- Download the source code(GPL code) of TP Link archer C2 in TPlink website.



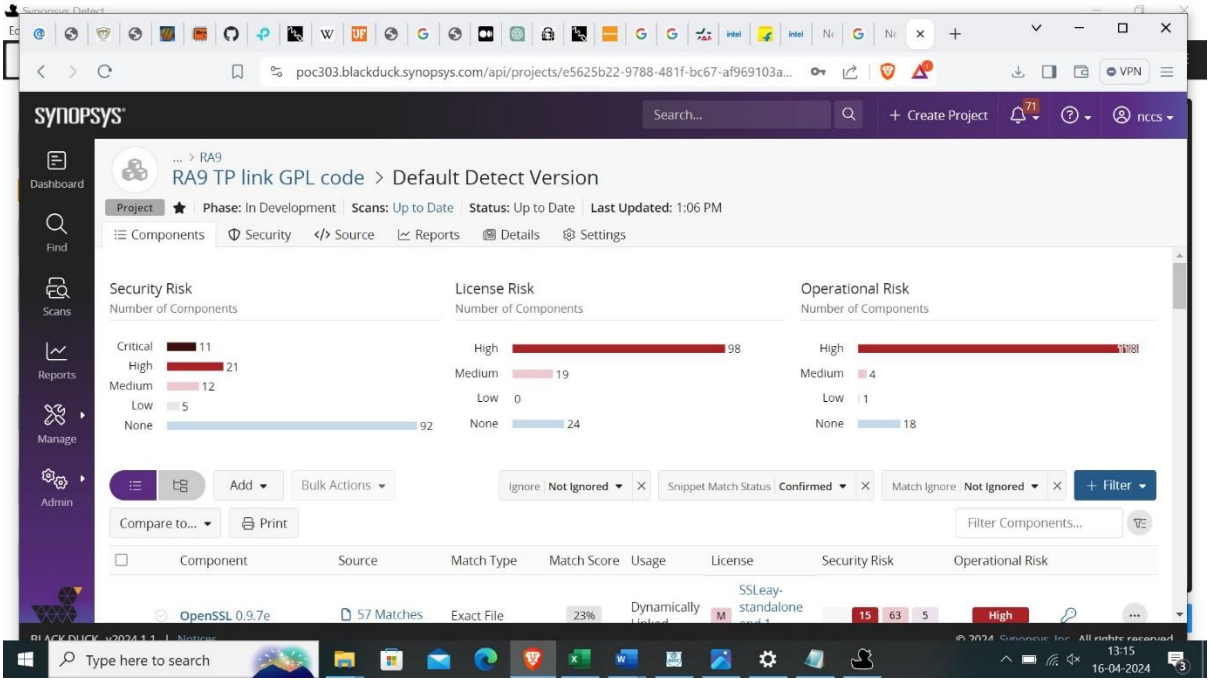
- Scan the TPlink source code using Blackduck SCA tool



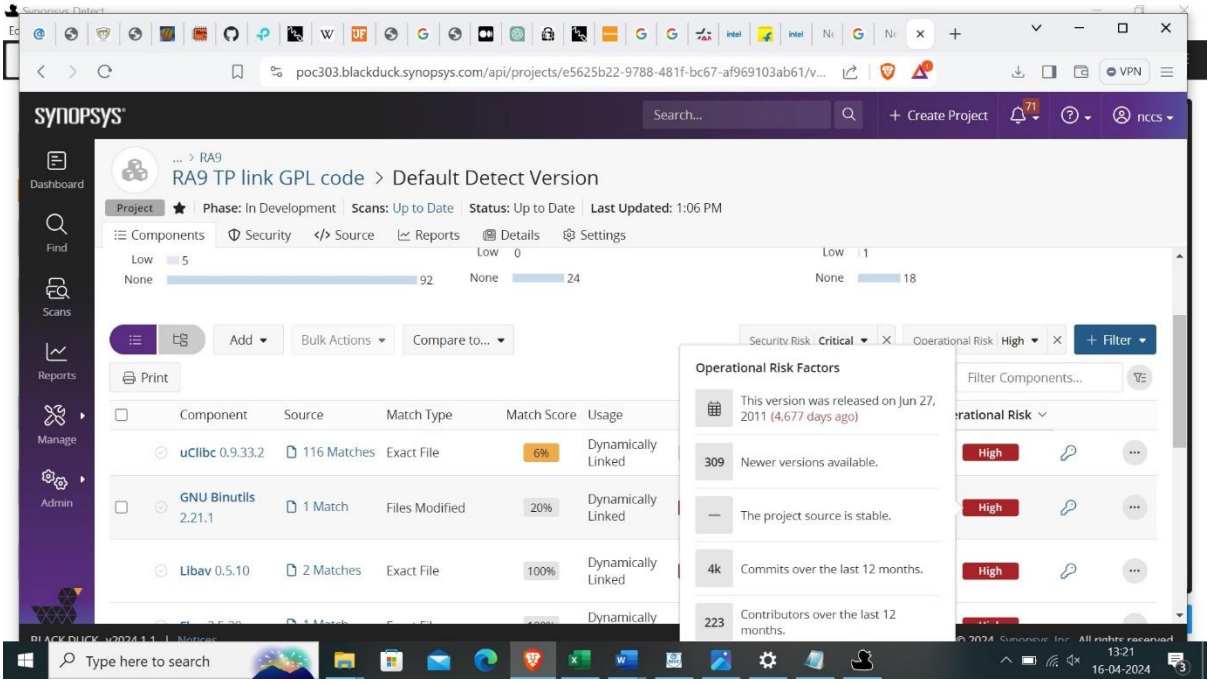
- verify the list of components with their vulnerabilities in the blackduck dashboard

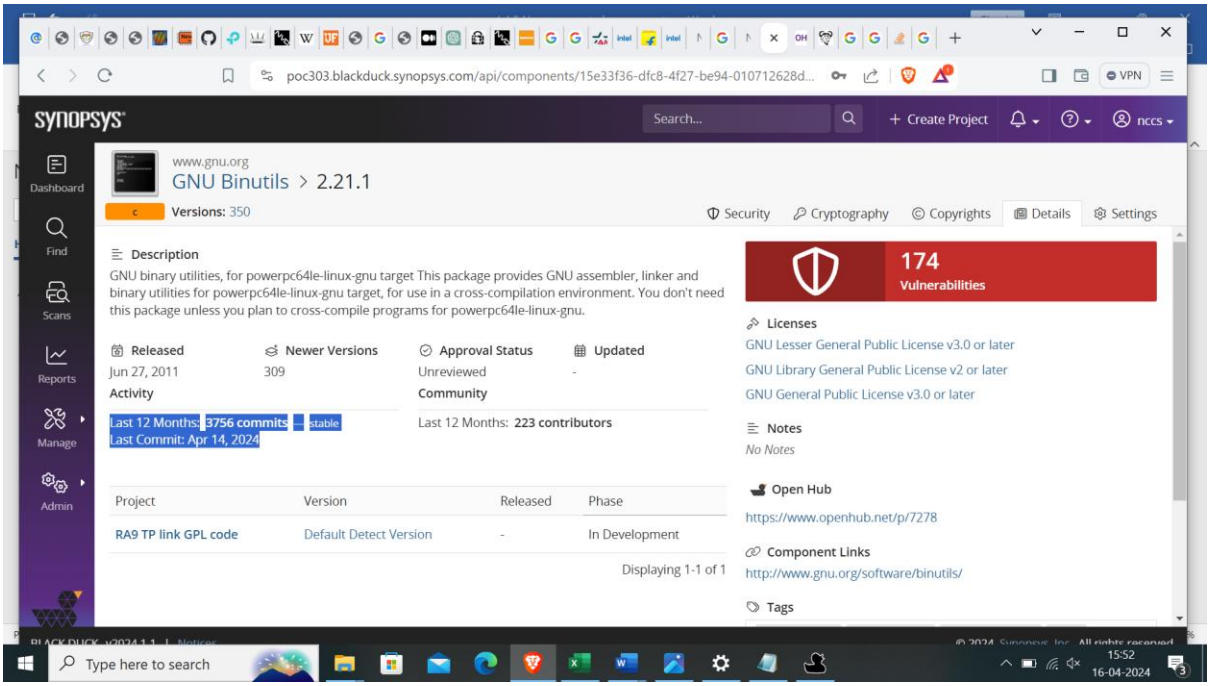


- Check vulnerability and operational risk for each component in the report. If component having vulnerability and it's not patched for longtime we consider as a EoL/EoS component.



6. I have selected “GNU Binutils 2.21.1” vulnerable component in the dashboard of blackduck. The vulnerable component have newer version for rectifying the vulnerability.



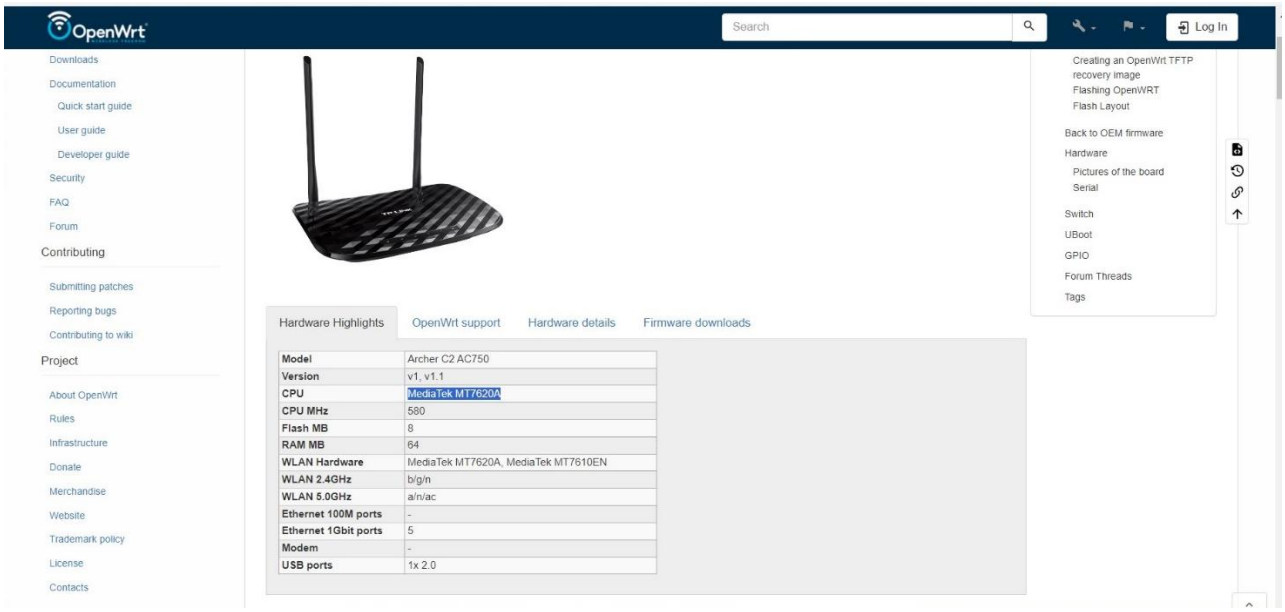


7.The above figure shows that the component providing organization have active commits.

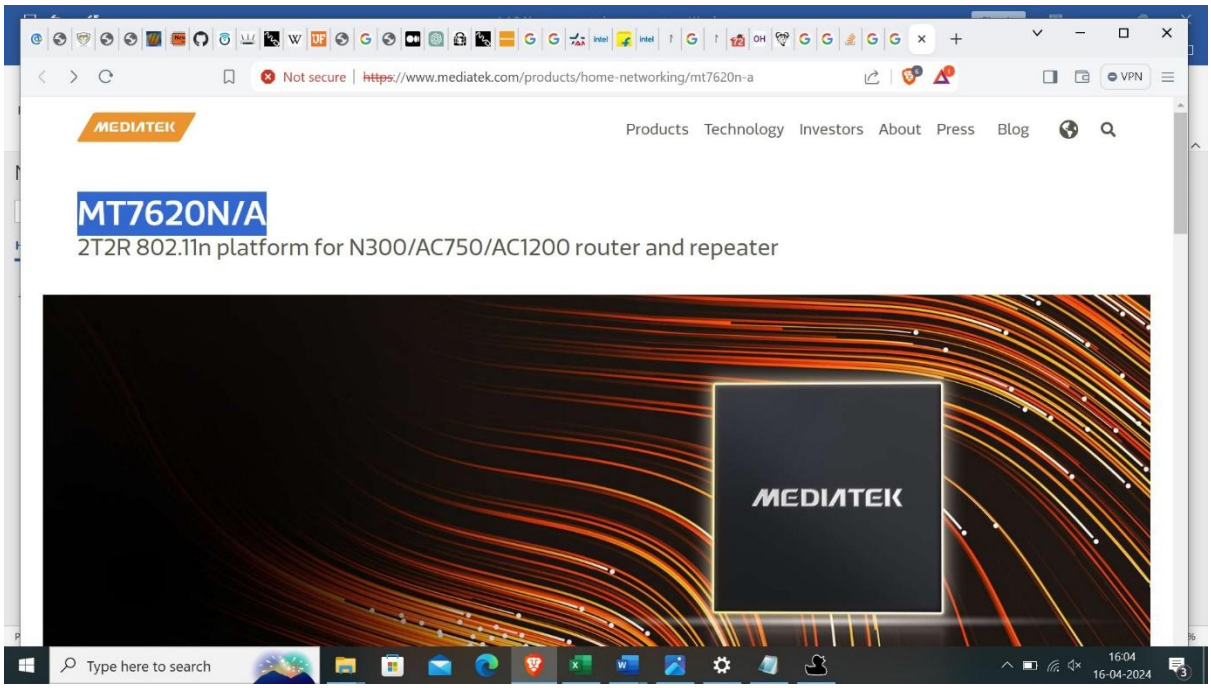
Note : For third party/proprietary software components, OEM need to give SLA and warranty support.

Find Hardware Components :

1. Through public search of TP-Link Archer C2 AC750 chipset details,



2. Check the CPU support status in the CPU vendor website



Note : Same thing need to be done for all hardware components available in the DUT

11.1.7 **Test Observations:**

- It was observed, the SCA scan shows the components with their security risk(vulnerability) and operation risk.
- For proprietary and third party software components not tested
- The hardware component vendor not showing supporting status of CPU used in DUT

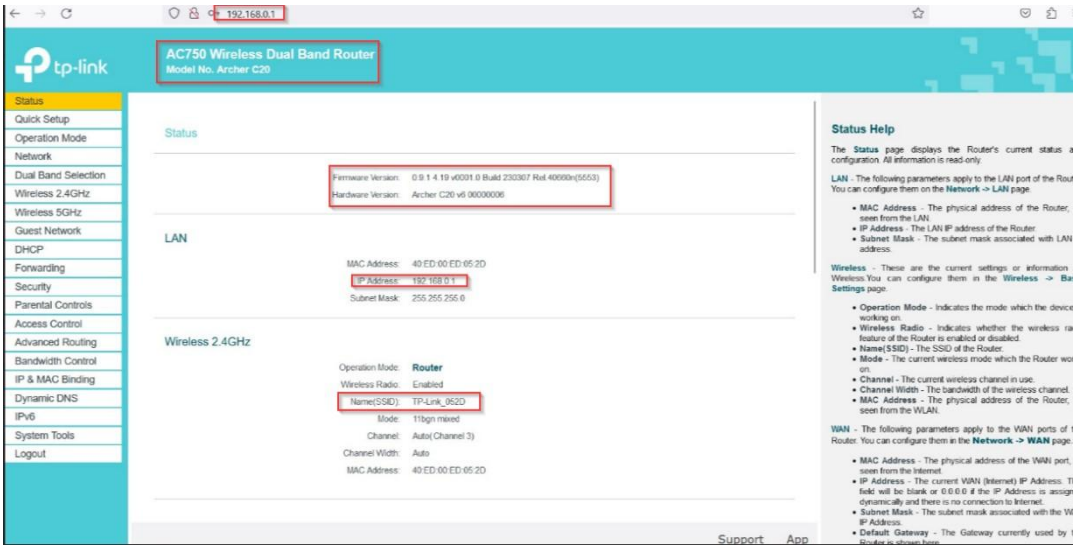
12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_UNSUPPORTED_COMPONENTS		Testcase incomplete

1.4.3 No Known Vulnerabilities in System on Chip (SOC) solution

<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 1.4 System Secure Execution Environment
2. **<Security Requirement No & Name >** 1.4.3 No Known Vulnerabilities in System on Chip (SOC) solution
3. **<Requirement Description: >**
   This test is applicable for such CPEs which have System on Chip solutions, where majority of CPE functions are realized in a VLSI chip. OEM to provide self-test / third-party / Chipvendor test report indicating that the SOC is free from malware, known-vulnerabilities.
4. **DUT Confirmation Details**:
   Use the command line/GUI interface to get details of the machine on which test is conducted.
   Use GUI to get Application No/Version No & hardware Info



5. **DUT Configuration**: Depending on the vendor input.

6. **Preconditions:** Note that the DUT in the lab does not have System on Chip solutions. OEM to provide selftest / third-party / Chip-vendor test report indicating that the SOC is free from malware, known-vulnerabilities. However, the test steps to be followed, in case we have a DUT with System on chip solutions have been listed down on Test Steps.

7. **Test Objective:** To verify that there is no malware and known vulnerability in the SoC of DUT(If applicable)

8. **Test Plan:** The tester should verify the OEM providing documents such as self-test / third-party / Chip vendor test report indicating that the SOC is free from malware, known-vulnerabilities

   8.1 **Number of Test Scenarios:**

   8.1.1 Validate the test report of SoC

   8.2 **Test Setup Diagram:-** Depending on the vendor input.

   8.3 **Tools Used:** Depending on the vendor input.

   8.4 **Test Execution Steps:**

   - For testing SOC, Fault induction testing can be performed using the simulation platform or command line tool/scripts to conduct a test campaign on specific board from a test PC.
   - On the software side, any of the following static analysis tools can be used to scan the code for vulnerabilities. These tools can pick up issues in code development such as buffer overflows and uninitialized variables.
   - Note: SAST tool can be used to detect vulnerabilities in the source code such as memory corruptions, buffer overruns, resources leaks, insecure data handling, use of resources that have been freed etc.

9. **Expected Result for Pass:** There should be no malware/ known vulnerability present on the SoC of DUT
10. **Expected Format of Evidence:** Screenshot of tool used for finding the malware/ vulnerability

11. **Test Execution:**

    11.1.1 **Test Case Number:** 01

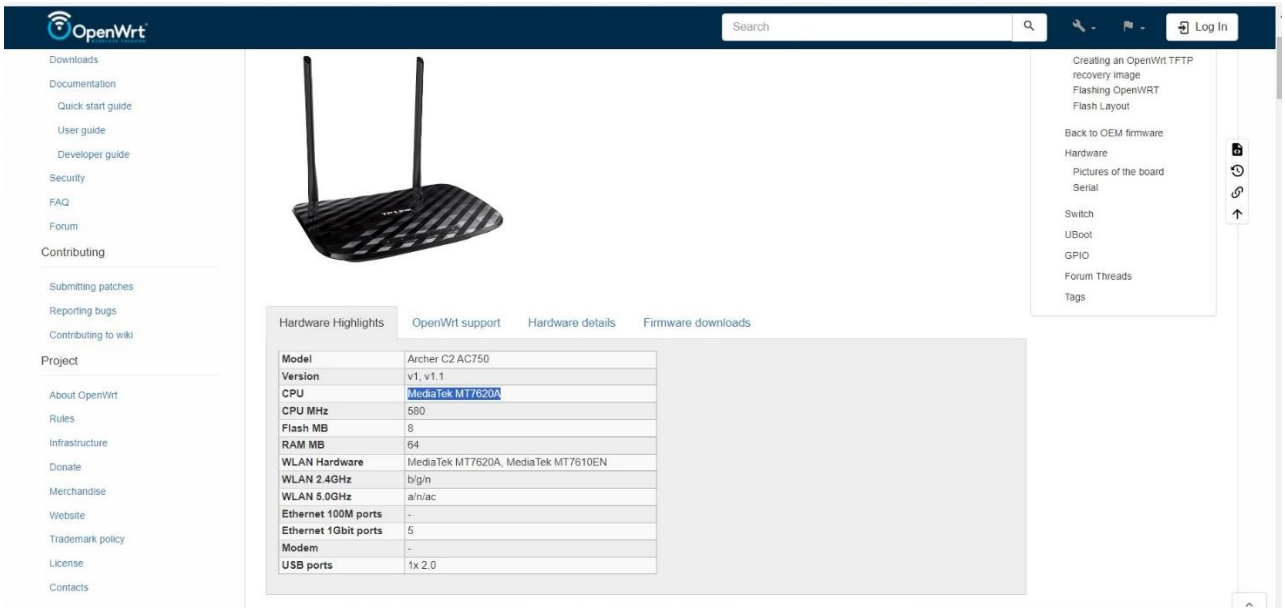
    11.1.2 **Test Case Name:** TC_NO_SoC_VULNERABILITIES

    11.1.3 **Test Case Description:** Ensuring that DUT SoC not have any known vulnerabilities/malware

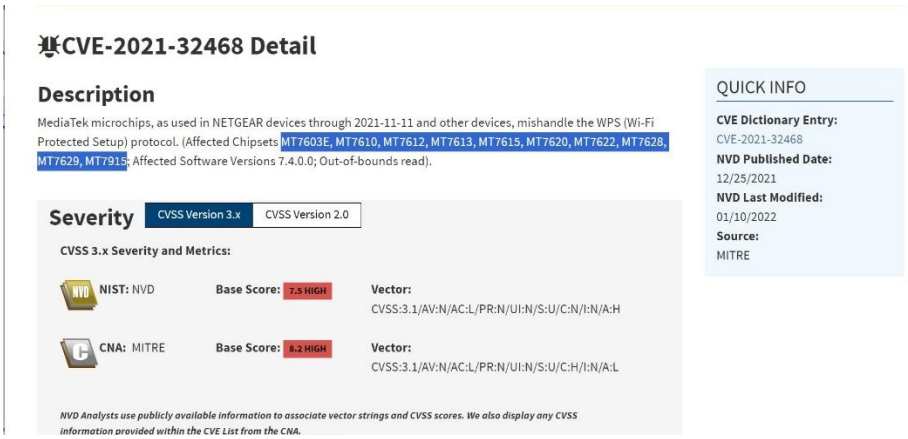
    11.1.4 **Execution Steps:**

    Note : If the DUT have SoC solutions then following execution steps will apply

    - Through public search of TP-Link Archer C2 AC750 chipset details,



- Tester validate the testing report provided from OEM for selftest/ third-party / Chipvendor test report of SoC.
- Tester need to check known vulnerability for SoC in NVD database



The above screenshot showing that the MT7620 chip affected by CVE-2021-32468 vulnerability.

11.1.5 **Test Observations:**

- Note that the DUT in the lab does not have System on Chip solutions. OEM to provide self-test / third-party / Chip-vendor test report indicating that the SOC is free from malware, known vulnerabilities. However, the test steps to be followed, in case we have a DUT with System on chip solutions have been covered on Test Steps.

12. **<u>Test Case Result:</u>**

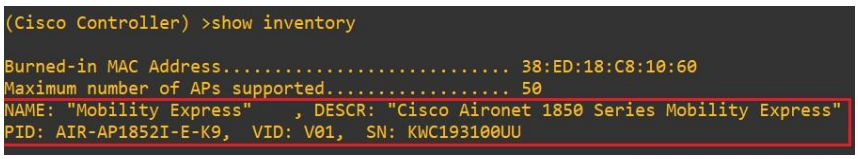
S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_SoC_VULNERABILITIES		OEM dependent

Section 1.5: User Audit

1.5.1 Audit Event Generation

<DUT Details: > Wi-Fi CPE
<DUT Software Version:> 8.10.183.0
<Digest Hash of OS> Hash of OS required
<Digest Hash of Configuration> Hash of configuration required.
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> ITSAR402122401 and Version: 1.0.1
<OEM Supplied Document list: > OEM Supplied Document list required

1. **<ITSAR Section No & Name>** Section 1.5: User Audit
2. **<Security Requirement No & Name >** 1.5.1 Audit Event Generation
3. **<Requirement Description: >**
   CPE to have capability to log important Security events. The audit logs may preferably be stored in non-volatile memory. If applicable (for cyber-cafe, Public Data Office usage scenario) provision for secure log export should exist and logs may capture unique System Reference such as website address, IP Address, MAC address, hostname, login attempts etc.
4. **DUT Confirmation Details**: This section involves information about DUT like software/firmware version, Hardware version model.
   DUT Cisco WLC contains default boot image with version 8.10.183.0. The model is AIR-AP1852I-E-K9. The inventory shows model serial no. & model description.
   Verification of DUT Cisco wireless LAN controller's HW product series information by running command show inventory on CLI.



Verification of DUT Cisco WLC's high-level system SW information by running command show sysinfo on CLI.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.10.183.0
OUI File Last Update Time........................ N/A

System Name...................................... Aironet-Controller
System Location.................................
System Contact..................................
System ObjectID.................................. 1.3.6.1.4.1.9.1.2250
IP Address....................................... 10.208.38.2
Last Reset....................................... 1: reload command

System Up Time................................... 0 days 3 hrs 33 mins 5 secs
System Timezone Location......................... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
System Stats Realtime Interval................... 5
System Stats Normal Interval..................... 180

Configured Country............................... IN  - India

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled

--More-- or (q)uit
```

Verification of DUT Cisco WLC's system information on Web access.

5. **DUT Configuration:** Config buffered logging on DUT.

```
(Cisco Controller) >config logging buffered ?

<0-7>          Set buffer logging message severity level.
alerts         Set buffer logging severity to 'alerts' (severity 1).
critical       Set buffer logging severity to 'critical' (severity 2).
debugging      Set buffer logging severity to 'debugging' (severity 7).
emergencies    Set buffer logging severity to 'emergencies' (severity 0).
errors         Set buffer logging severity to 'errors' (severity 3).
informational  Set buffer logging severity to 'informational' (severity 6).
notifications  Set buffer logging severity to 'notifications' (severity 5).
warnings       Set buffer logging severity to 'warnings' (severity 4).

(Cisco Controller) >config logging buffered 7
```

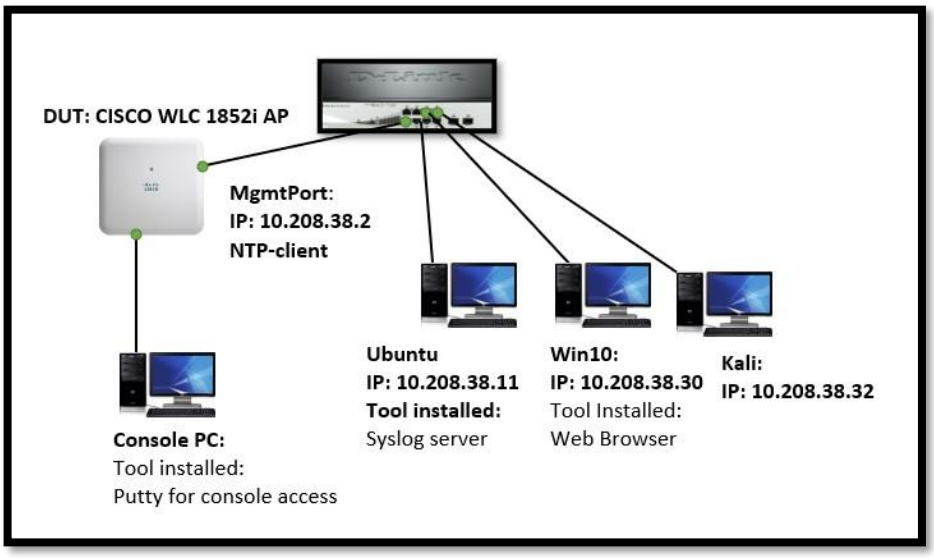
6. **Pre-Conditions:**
   - Vendor to provide documentation (administration guide or any other document) on how to configure audit logs to be access controlled for various privilege levels.
   - The following information shall be provided by the documentation (administration guide or any other document) accompanying the network product:
     - The log where the event is recorded and how it can be accessed (e.g., the complete path).
     - If the event type is enabled by default or how to enable it.

- Documentation (administration guide or any other document) describing where logs are stored and how these logs are accessed, and the Network Product interfaces that these logs can be accessed from.
- Tester has the highest level of access to DUT.

7. **Test Objective:** CPE to have capability to log important Security events. The audit logs may preferably be stored in non-volatile memory. If applicable (for cyber-cafe, Public Data Office usage scenario) provision for secure log export should exist and logs may capture unique System Reference such as website address, IP Address, MAC address, hostname, login attempts etc.

8. **Test Plan:**

8.1 **Test-Bed Diagram**



8.2 **Number of test scenarios/test cases: 2**

8.3 **Tools used:** Command line of DuT, syslog server , wireshark

8.4 **Test case Execution:**

- CASE I: Authenticate the client. Unsuccessful WLAN SSID client authentication
  - Attempt incorrect PSK for SSID
  - Verify system event generated.
- CASE II: Enabling communications between a pair of components.
  - Insert syslog server ip set up on Web GUI
  - Verify logs generated on syslog server.
  - Verify system event generated.
  - Verify packet capture syslog communication is encrypted or not

9. Expected Results for Pass: The tester checks CPE to have capability to log important Security events. The audit logs may preferably be stored in non-volatile memory. If applicable (for cyber-cafe, Public Data Office usage scenario) provision for secure log export should exist and logs may capture unique System Reference such as website address, IP Address, MAC address, hostname, login attempts etc.

10. Expected Format of Evidence: Screenshots

11. Test Execution:

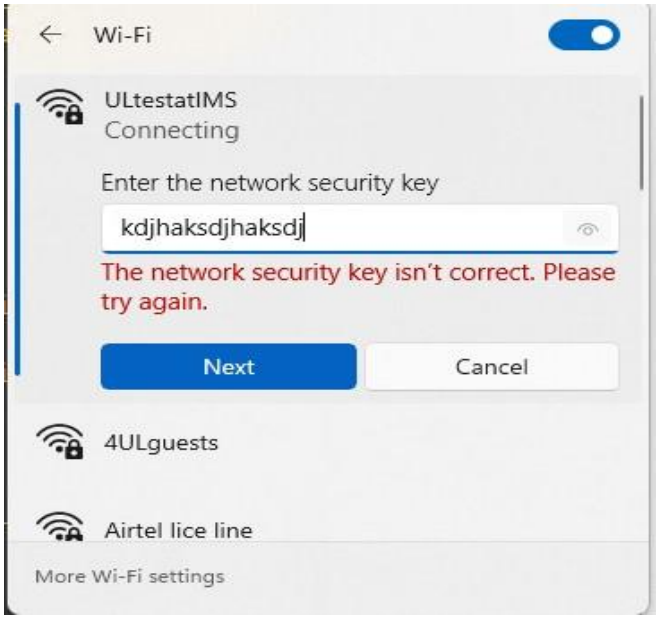
11.1 **Test Case Number:** 1

11.1.1 **Test Case Name:** TC_LOGGING_IMPORTANT_SECURITY_EVENTS

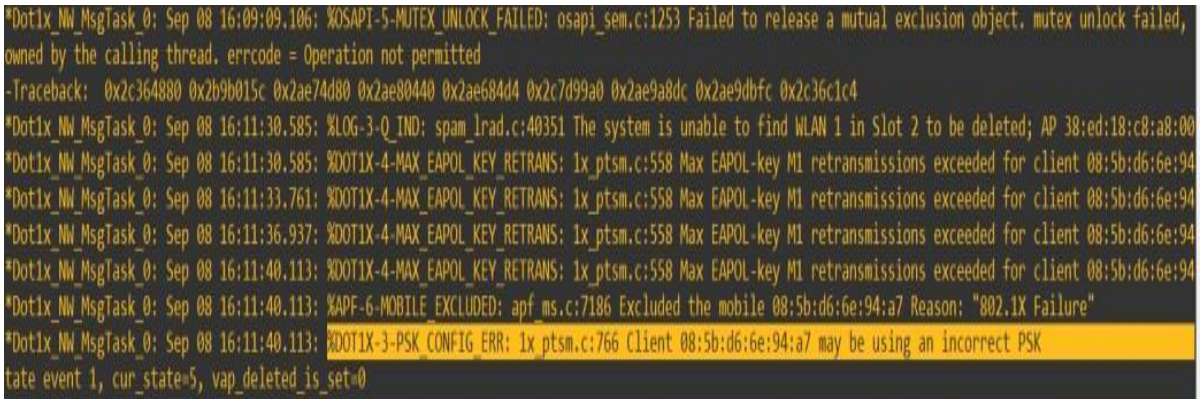
11.1.2 **Test Case Description:** The tester checks that DuT logs important security events.

11.1.3 **Test Execution:** Unsuccessful WLAN SSID client authentication

- Attempt incorrect PSK for SSID



Verify system event generated.



11.1.4 **Test Observations:** It is evident that system log has client MAC address and date references, as logs are enabled in debug mode.

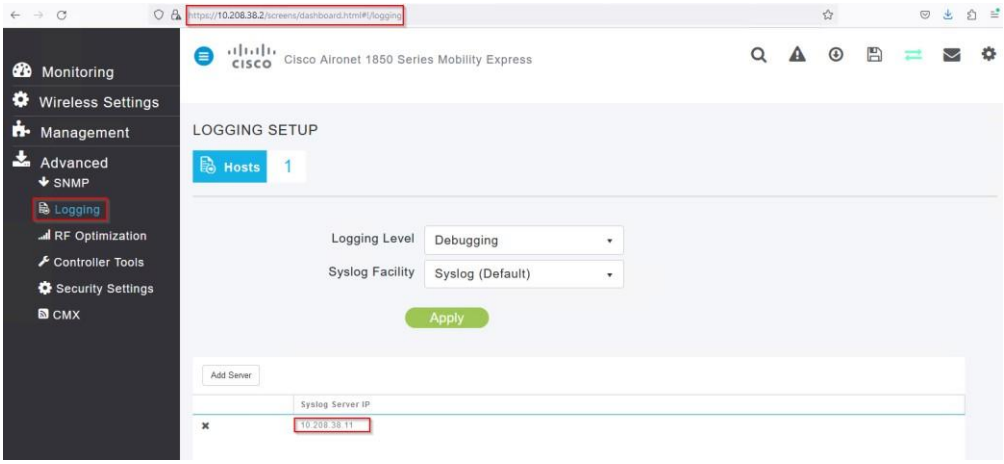
11.2 **Test Case Number:** 2

11.2.1 **Test Case Name:** TC_SECURE_LOG_EXPORT

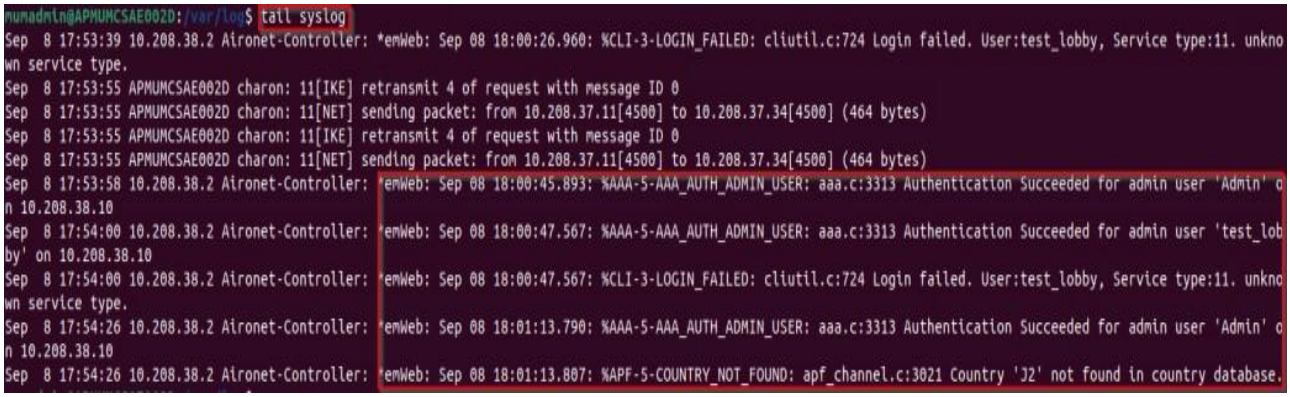
11.2.2 **Test Case Description:** The tester checks that DuT logs are securely exported.

11.2.3 **Test Execution:**

Add syslog server IP on DUT (Web GUI access)



Verify logs generated on syslog server.

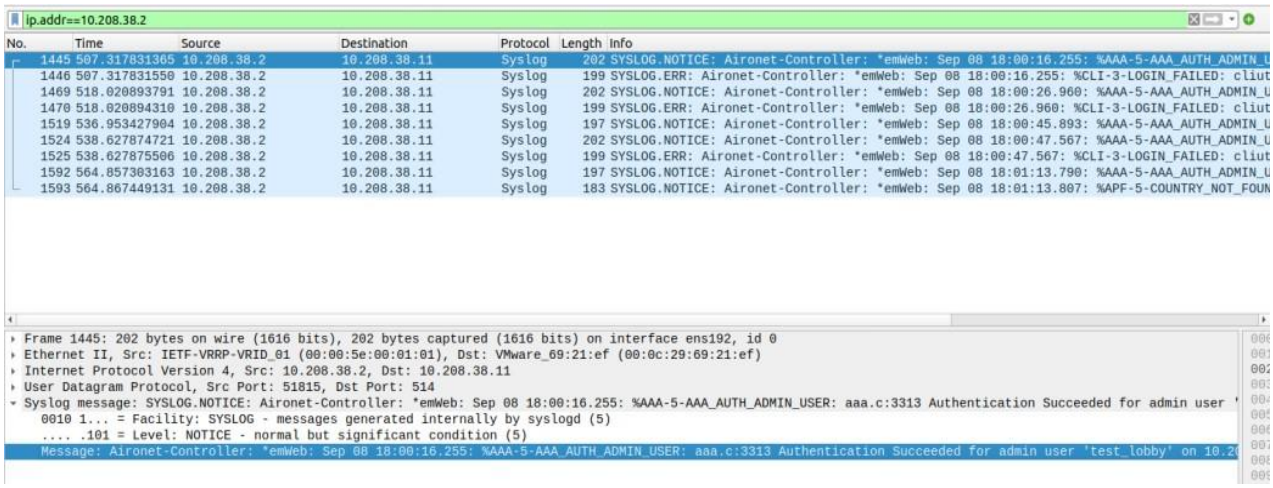


- Verify system event generated on DUT.

```
(Cisco Controller) >show msglog

Message Log Severity Level ..... DEBUGGING
*emWeb: Sep 08 18:01:13.807: %APF-5-COUNTRY_NOT_FOUND: apf_channel.c:3021 Country 'J2' not found in country database.
*emWeb: Sep 08 18:01:13.790: %AAA-5-AAA_AUTH_ADMIN_USER: aaa.c:3313 Authentication Succeeded for admin user 'Admin' on 10.208.38.10
*emWeb: Sep 08 18:00:47.567: %CLI-3-LOGIN_FAILED: cliutil.c:724 Login failed. User:test_lobby, Service type:11. unknown service type.
*emWeb: Sep 08 18:00:47.567: %AAA-5-AAA_AUTH_ADMIN_USER: aaa.c:3313 Authentication Succeeded for admin user 'test_lobby' on 10.208.38.10
*emWeb: Sep 08 18:00:45.893: %AAA-5-AAA_AUTH_ADMIN_USER: aaa.c:3313 Authentication Succeeded for admin user 'Admin' on 10.208.38.10
```

It is evident that DUT logs with all timestamps are fetched same & stored at the syslog server end too.

Verify packet capture syslog communication is encrypted or not.



11.2.4 **Test Observations:** It is evident that DUT system log is not communicated in encrypted manner to syslog server.

Note: Testing to be performed to check if the audit logs may preferably be stored in non-volatile memory. Testing to be also performed to check logging of all important security events in DuT. (above test scenario shows only one security event).

12 . Test Case Result:

S. No	OUTCOME OF RUNNING THE SCRIPT (CASE 1/CASE2)	PASS /FAIL	REMARKS
1	TC_LOGGING_IMPORTANT_SECURITY_EVENTS	Pass	It is evident that system log has client MAC address and date references, as logs are enabled in debug mode.
2	TC_SECURE_LOG_EXPORT	Fail	It is evident that DUT logs with all timestamps are fetched the same & stored at the syslog server end too and DUT system log are not

			communicated in an encrypted manner to the syslog server.

Section 1.6: Data Protection

1.6.1 Cryptographic Based Secure Communication

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name>** Section 1.6 Data Protection
2. **<Security Requirement No &** Name > 1.6.1: Cryptographic Based Secure Communication
3. **<Requirement Description: >** The communication security dimension ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points). The data is protected against well know attacks related to Sniffing, Disclosure, reconnaissance etc., The secure communication mechanisms between the CPE and connected entities shall use industry standard protocols such as IPSEC, VPN, SSH, TLS/SSL, etc., and NIST specified cryptographic algorithms with specific key sizes such as SHA, Diffie-Hellman, AES etc
4. **DUT Confirmation Details**:

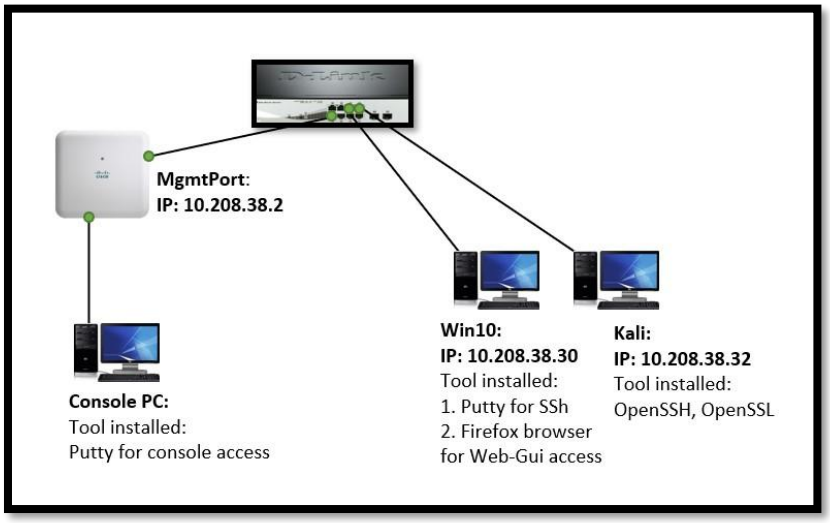
5. **DUT Configuration:** No configuration needed

6. **Preconditions**
   - The manufacturer shall supply the list of system functions which include network services, local access via a management console, local usage of operating system and applications.
   - The manufacturer shall supply the list of access entries for system functions

7. **Test Objective:-** To check if data communicated is protected with secure protocols (with secure ciphers)

8. **Test Plan**
   8.1. Number of Test Scenarios:
   8.1.1. Test Scenario to check the secure communication using SSH
   8.1.2. Test Scenario to check the secure communication using HTTPS

   8.2. Test Bed Diagram



8.3. Tools Required

- DUT , Wireshark

8.4. Test Execution Steps

- The tester shall attempt to login into the DUT using SSH and simultaneously capture the packets on wireshark
- Similarly while accessing through GUI

9. **Expected Results for Pass:** The DUT supports secure communication through SSH and GUI using secure ciphers

10. **Expected Format of Evidence:** Screenshots of Terminal and pcap file

11. **Test Execution:**

11.1 Test Case Number: 01

11.1.1 **Test Case Name:** Login into DUT through SSH

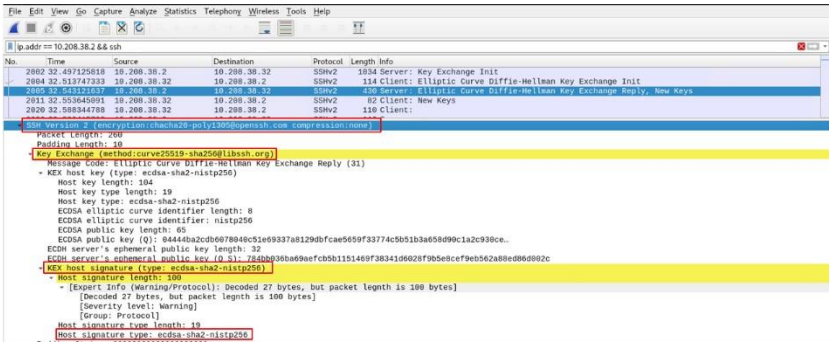
11.1.2 **Test Case Description:** The following testcase is done to login into the DUT through SSH

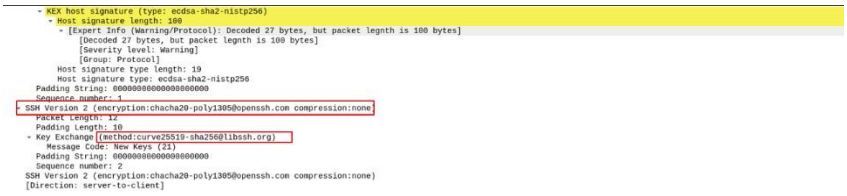
11.1.3 **Execution Steps:**

- Attempt to login into DUT

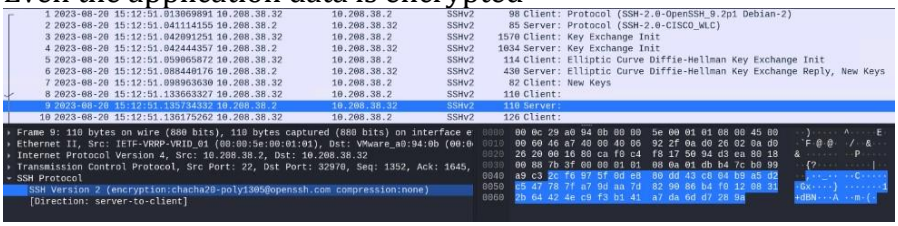
```
┌──(root㉿Mumuser)-[/home/mumuser]
└─# ssh 10.208.38.2


(Cisco Controller)
User: Admin
Password:********
Welcome to the Cisco Mobility Express command line interface.
Only commands which are listed in the command reference guide for this release are supported.
http://www.cisco.com/c/en/us/support/wireless/mobility-express/products-command-reference-list.html

Warning:In SNMPV2 No Defaults Presents.
Please use command: config snmp community create <name>

Warning:In SNMPV3 No Defaults Presents.
Please use command: config snmp v3user create <username>

(Cisco Controller) >
(Cisco Controller) >logoutConnection to 10.208.38.2 closed.

┌──(root㉿Mumuser)-[/home/mumuser]
└─#
```

- Analyze the captured packets on wireshark

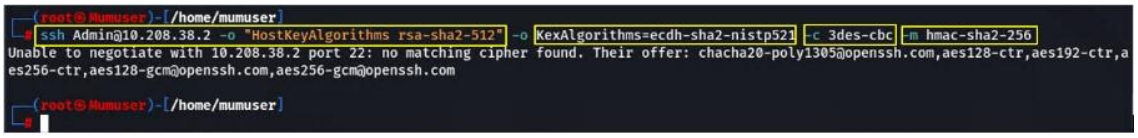




Even the application data is encrypted



- Also attempt to login into DUT using insecure ciphers



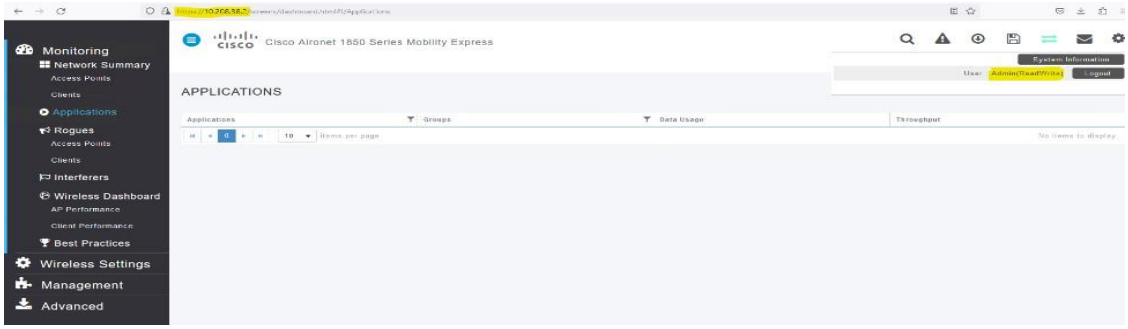
11.1.4 **Test Observations:** It was observed that the secure ciphers are used in the SSH connection. Also on attempting to connect with weak ciphers, DUT rejects the connection.

11.1.5 **Evidence Provided: -** Screenshots of Terminal

11.2 Test Case Number: 02

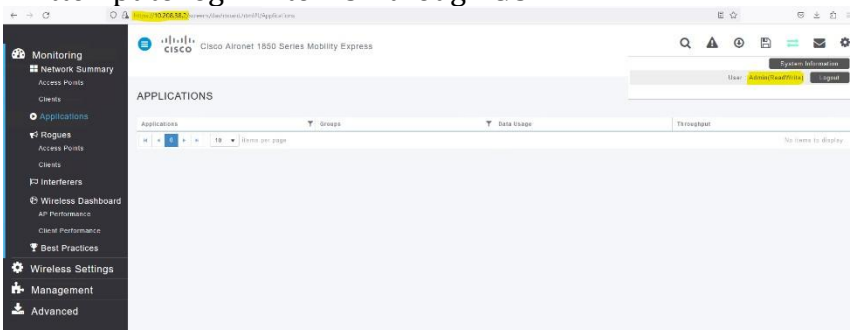
11.2.1 **Test Case Name:** Login into DUT through HTTPS

11.2.2 **Test Case Description:** The following testcase is done to login into the DUT through GUI

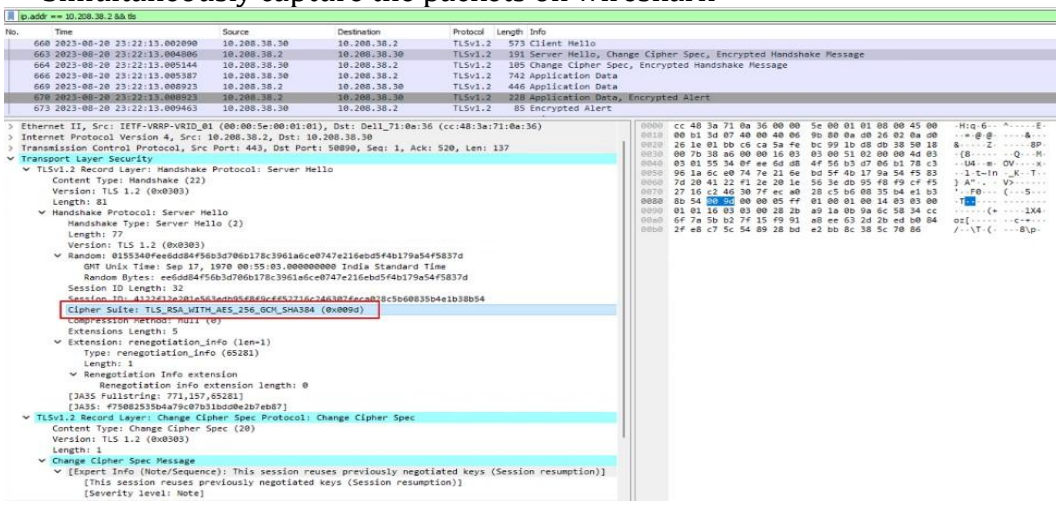


11.2.3 **Execution Steps:**

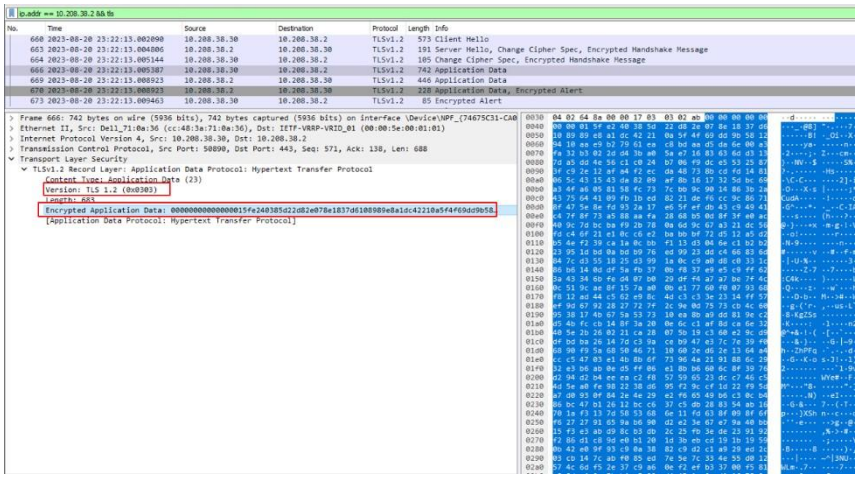
- Attempt to login into DUT though GUI



- Simultaneously capture the packets on wireshark



A secure cipher been observed to be used between server and client



Application data encrypted

11.2.4 Test Observation:- It was observed that GUI access to DUT is using secure cipher and application data is observed to be encrypted.

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	SSH connection	Pass	
2.	GUI connection	Pass	

1.6.2 Cryptographic Based Secure Communication on Wi-Fi Access

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.6** Data **Protection**
2. **<Security Requirement No & Name > 1.6.2: Cryptographic Based Secure Communication on Wi-Fi Access**
3. **<Requirement Description: > The** CPE to have protection mechanisms against access to keys in the CPE against Key disclosure, reconnaissance, re-installation attacks, nonce-resets, Zeroing blocks of key etc.

4. **DUT Confirmation Details**:

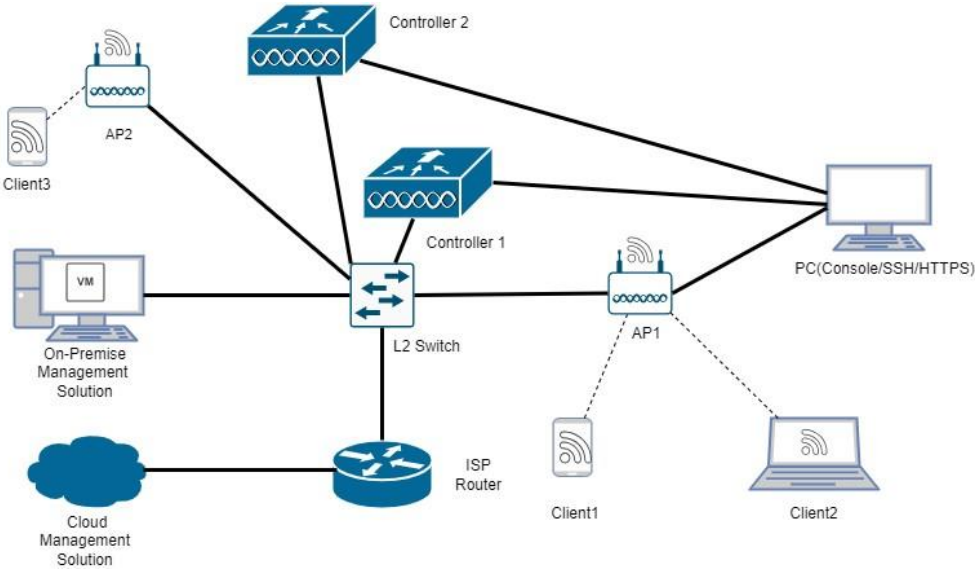
5. **DUT Configuration:** No configuration needed

6. **Preconditions:**- OEM shall provide documentation describing how confidential system internal information is handled by system functions.

7. **Test Objective:-** To verify that the DUT has protection against against Key disclosure, reconnaissance, re-installation attacks, nonce-resets, Zeroing blocks of key etc.

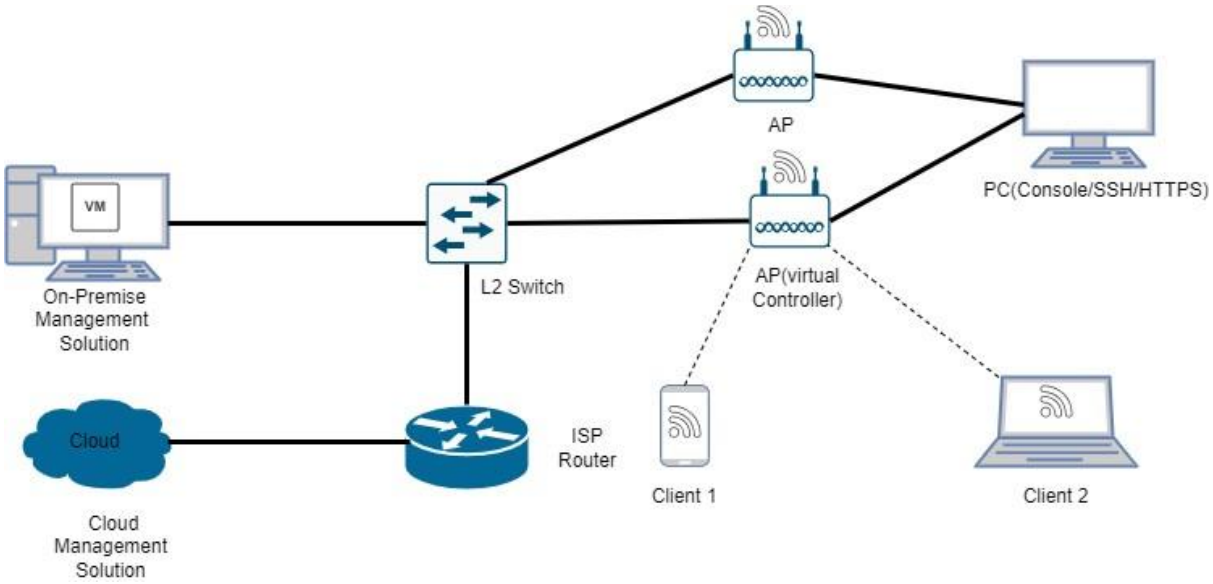
8. **Test Plan**
   8.1. Number of Test Scenarios:
   8.1.1. Test Scenario to review the documentation provided by the vendor describing how confidential system internal information is handled by system functions
   8.1.2. Test Scenario to try to gain access to the CPE and its configuration files to see if you can find any plaintext keys.
   8.1.3. Test Scenario to install malicious firmware on the CPE to see if it can be detected and prevented. This can be done by creating a fake firmware update and trying to install it on the device.

   8.2. Test Bed Diagram



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

8.3. Tools Required

- DUT ,
- Wireshark

8.4. Test Execution Steps:- The tester shall the mechanism to protect the keys in DUT by simulating attacks

9. **Expected Results for Pass:** The DUT has protection feature against Key disclosure, reconnaissance, re-installation attacks, nonce-resets, Zeroing blocks of key

10. **Expected Format of Evidence:** Screenshots of Terminal and pcap file

11. **Test Execution:**

11.1 Test Case Number: 01

11.1.1 **Test Case Name:** review the documentation provided by the vendor.

11.1.2 **Test Case Description:** The Tester shall review the documentation provided by the vendor describing how confidential system internal information is handled by system functions.

11.1.3 **Execution Steps:**

Note: The software test document is not available with the lab because this is the market-purchased product used for demo testing.

11.1.4 **Test Observations:**

Note: The software test document is not available with the lab because this is the market-purchased product used for demo testing.

11.1.5 **Evidence Provided**

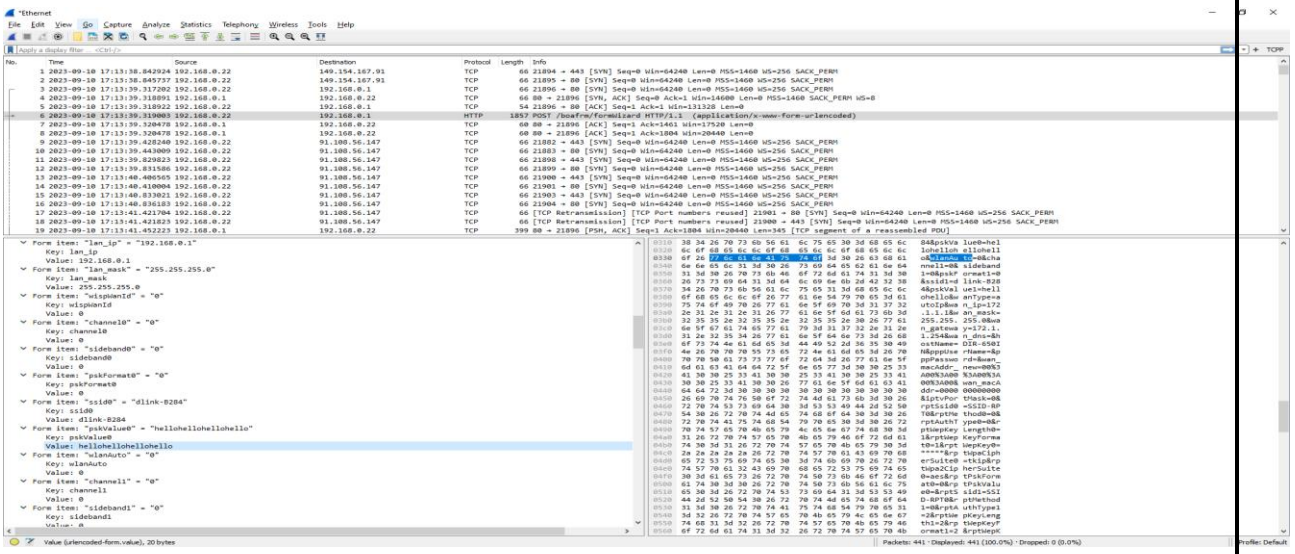
11.2 Test Case Number: 02

11.2.1 **Test Case Name:** try to gain access to the CPE and its configuration files to see if you can find any plaintext keys

11.2.2 **Test Case Description:** Key disclosure and reconnaissance: The Tester shall try to gain access to the CPE and its configuration files to see if you can find any plaintext keys. You can also use network scanning tools to see if any keys are transmitted in plaintext.

11.2.3 **Execution Steps:**

- The Tester logged into the DUT's Web GUI (http://192.168.0.1) in the web browser of the test machine (192.168.0.22) account "admin" using the respective authentication attribute (password).
- The Tester changes the Pre-Shared Key and captures the change request using Wireshark.
- The Tester observed Pre-Shared Key are transmitted in plaintext.



11.2.4 **Test Observations:** The Tester observed Pre-Shared Key are transmitted in plaintext.

11.2.5 **Evidence Provided:**- Screenshots of the Pre-Shared Key are transmitted in the plaintext.

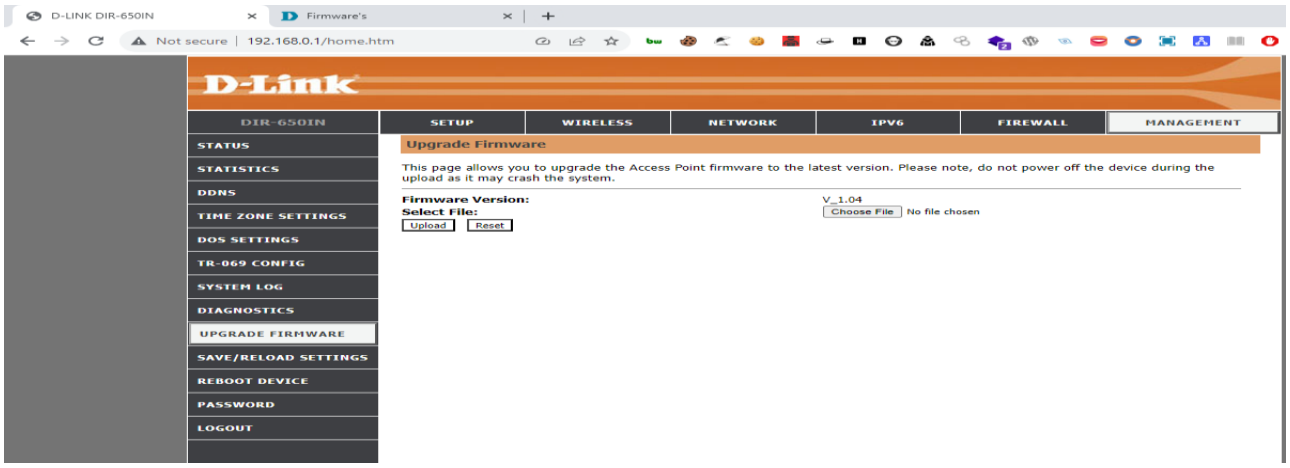
11.3 Test Case Number: 03

11.3.1 **Test Case Name:** attempt to install malicious firmware on the CPE to see if it can be detected and prevented

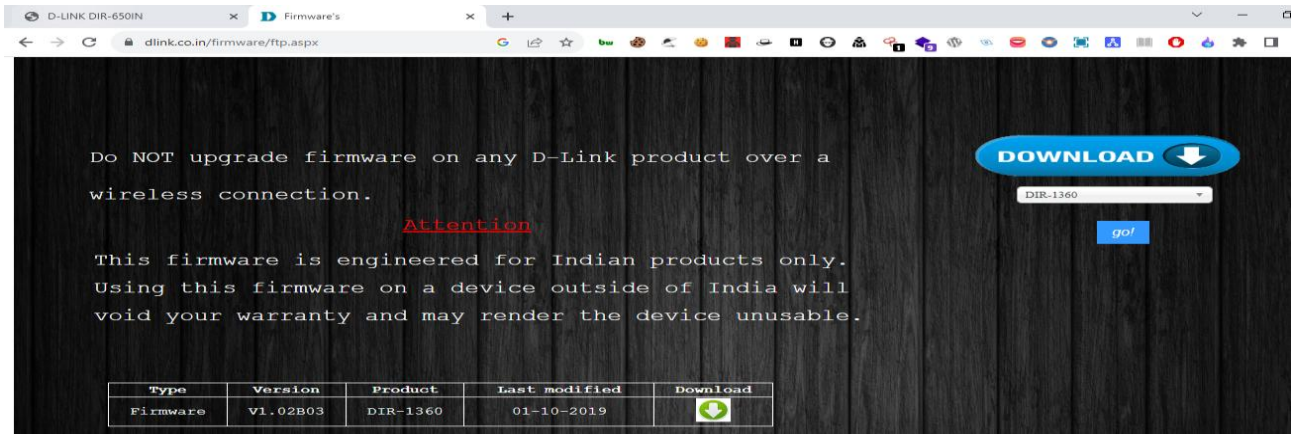
11.3.2 **Test Case Description:** Re-installation attacks: The Tester shall attempt to install malicious firmware on the CPE to see if it can be detected and prevented. This can be done by creating a fake firmware update and trying to install it on the device.

11.3.3 **Execution Steps**

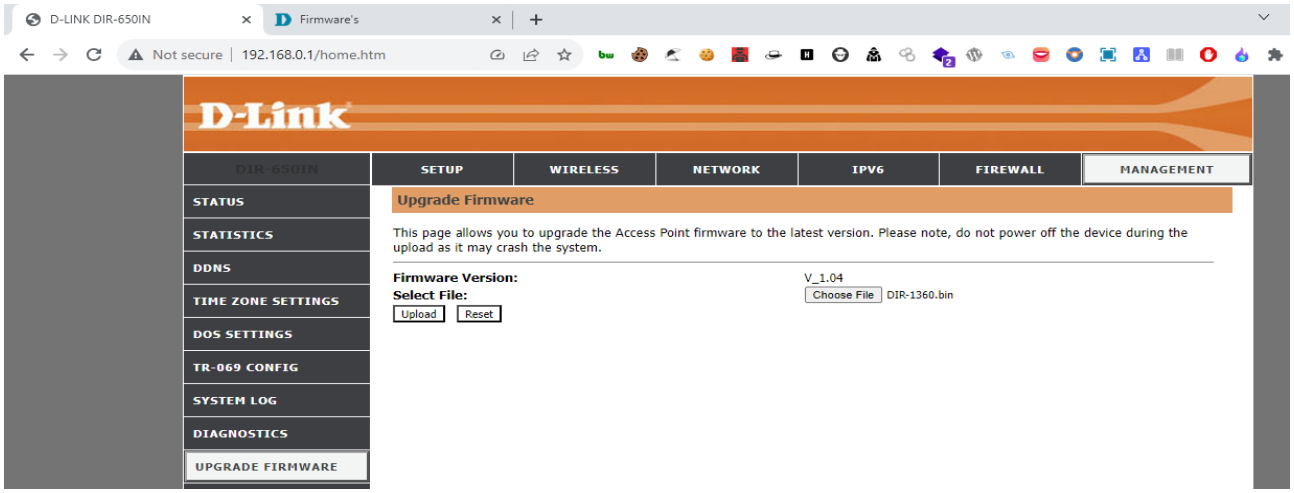
- The tester logs in to the DUT's Web GUI (http://192.168.0.1) in the web browser of the test machine (192.168.0.22) account "admin" using the respective authentication attribute (password).
- The tester clicked on MANAGEMENT > UPGRADE FIRMWARE and observed the current firmware version.



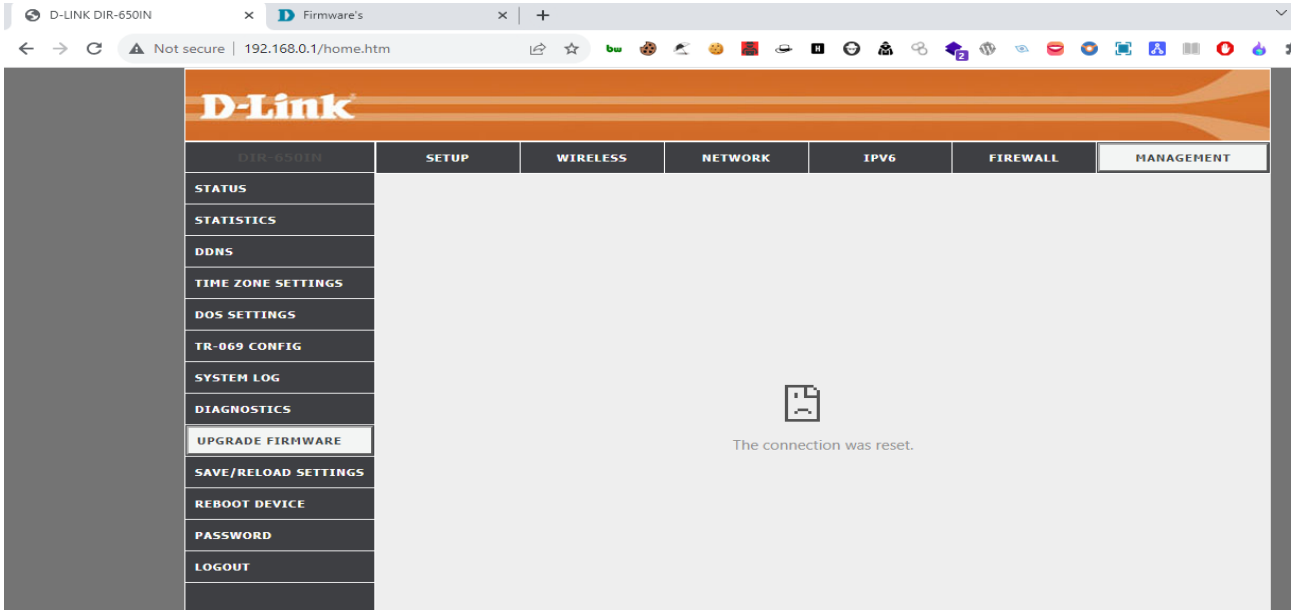
- The Tester downloaded different versions of firmware and attempted to upload them on DUT to verify if DUT has a detection feature or not.

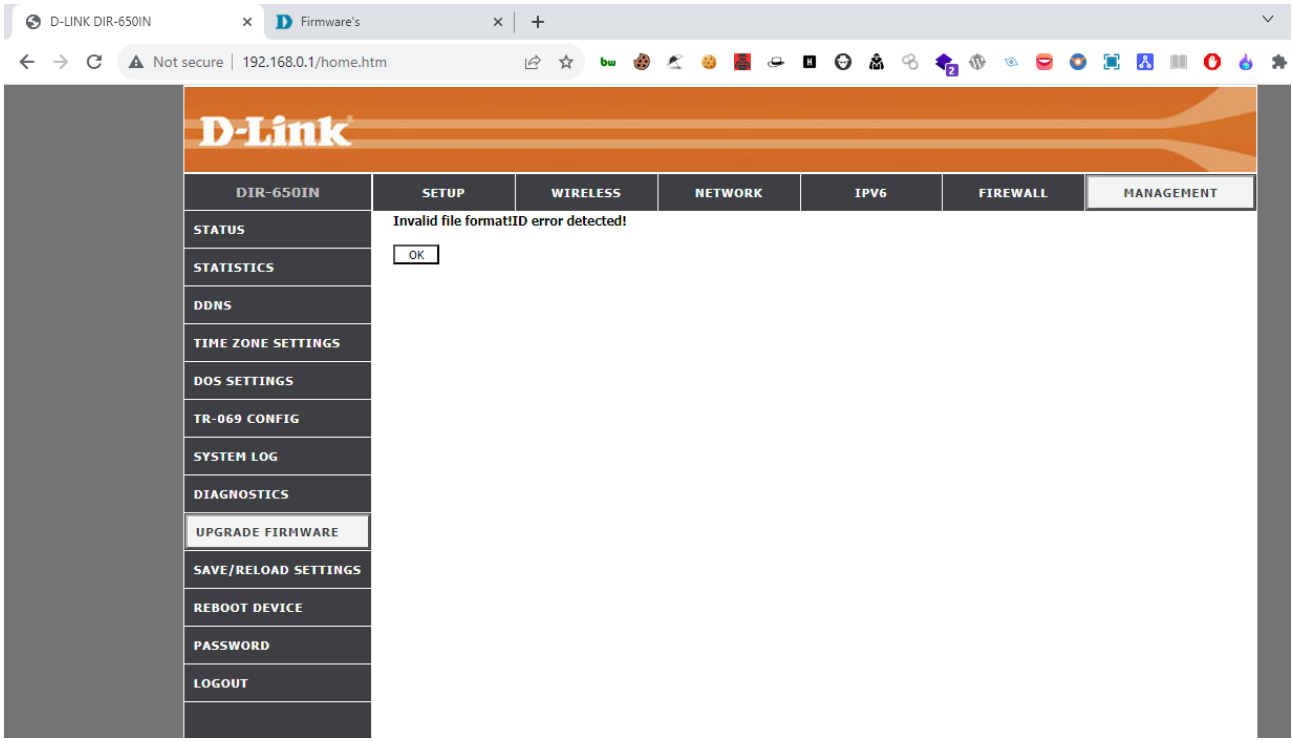


- The Tester clicked on the “Choose File” feature and uploaded the downloaded firmware and clicked on the upload button.



- The Tester observed that DUT has detected other version firmware so stop itself for update.





11.3.4 **Test Observations:** The Tester observed that DUT has detected other versions of firmware so stop itself for update.

11.3.5 **Evidence Provided**: - Screenshot of the DUT detecting other versions of firmware.

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	review the documentation provided by the vendor		No document available
2	try to gain access to the CPE and its configuration files to see if you can find any plaintext keys	FAIL	
3	attempt to install malicious firmware on the CPE to see if it can be detected and prevented	PASS	

1.6.3 Cryptographic Algorithm selection for Wi-Fi Access <DUT Details: > Ex: Router

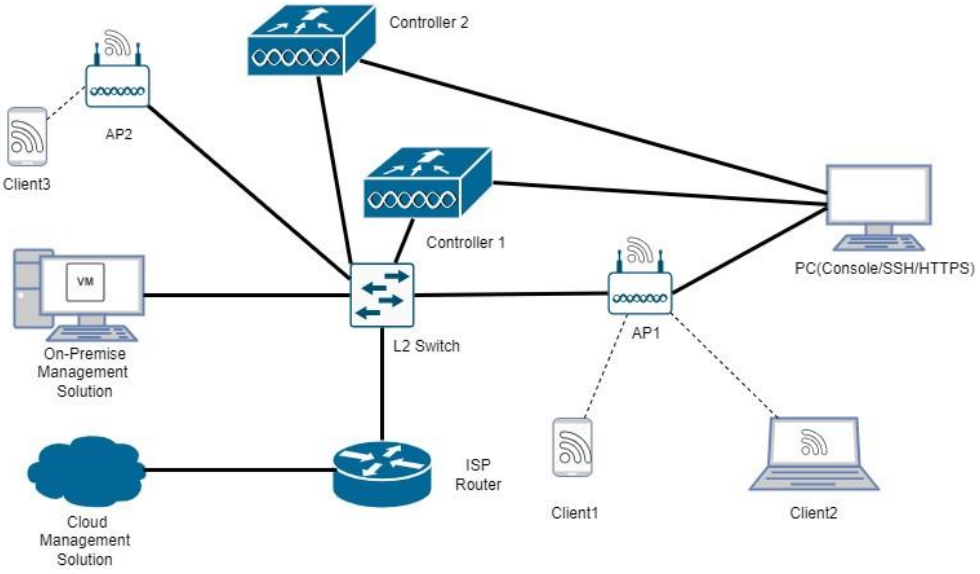
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name**> Section 2.6 Data Protection
2. **<Security Requirement No & Name >** 1.6.3 Cryptographic Algorithm selection for Wi-Fi Access **<Requirement Description: > When** Wi-Fi CPE is not in debug (maintenance) mode, there shall be no system function that reveals confidential system internal data in the clear to users and administrators. Such system functions could be, for example, local or remote OAM CLI or GUI, error messages, logging messages, alarms, configuration file exports etc. Confidential system internal data contains authentication data (i.e., PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration and could be of advantage to attackers (i.e., stack traces in error messages). Access to maintenance mode shall be restricted only to authorized privileged users.

3. **DUT Confirmation Details**:
4. **DUT Configuration:** No configuration needed
5. **Preconditions**
    - OEM shall provide documentation describing the supported functions
    - Also to review about the accessibility of debug mode of the DUT

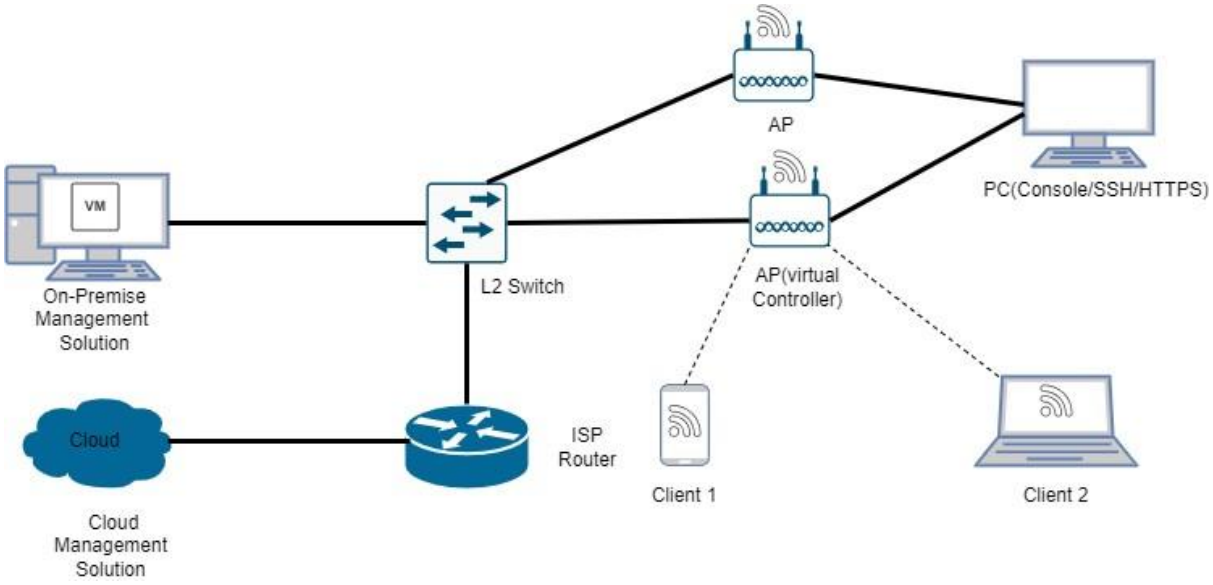
6. **Test Objective:-** To verify that DUT has no system function that exposes sensitive data in clear text in normal operational mode. Also the maintenance mode should be accessible to authorized users only
7. **Test Plan**
    7.1. Number of Test Scenarios:
    7.1.1. Test to verify confidentiality of sensitive data in system functions
    7.1.2. Test to verify confidentiality of sensitive data in logs
    7.1.3. Test to verify confidentiality of sensitive data in configuration file exports
    7.1.4. Test to verify access to maintenance mode by authorized users only

    7.2. Test Bed Diagram



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet

7.3. Tools Required

- DUT ,
- Wireshark

7.4. Test Execution Steps

- The tester shall access the DUT through the CLI and the GUI and check for password visibility

- The tester shall check for configuration files (startup and running config) for reveal of sensitive data in clear text as well as the logs
- The tester shall check in the config file exports for any sensitive data in clear text
- The tester shall check the authorized accessibility of maintenance mode of the DUT

8. **Expected Results for Pass:** The system functions of the DUT do not reveal the sensitive data in clear text and has authorized accessibility on maintenance mode

9. **Expected Format of Evidence:** Screenshots of cli and the GUI of the DUT

10. **Test Execution:**

11.1 **Test Case Number:** 01

11.1.1 **Test Case Name:** confidentiality of sensitive data in system functions

11.1.2 **Test Case Description:** The following test case is performed to check for sensitive data in system functions.

11.1.3 Execution steps

- Access the DUT in the GUI and check for the password visibility

- Similarly access the DUT at the console level and check for the password visibility
- Access the configuration files such as running-config to check for password/PINs/cryptographic key visibility
- Capture the 4-way wifi handshake and check if any KEY is found in the capture

11.1.4 **Test Observations:** It was observed that the password dis not visible in the GUI No KEY was found in the handshake capture

11.1.5 **Evidence Provided**

11.2 Test Case Number: 02

11.2.1 **Test Case Name:** Test to verify confidentiality of sensitive data in logs

11.2.2 **Test Case Description:** The following test case is to verify that confidentiality of sensitive data in logs (errors , auth, debug logs)

11.2.3 **Execution Steps:**

- Attempt to access the DUT with incorrect credentials to generate error logs
- Verify the error logs for any sensitive data in clear texts
- Access the DUT with correct credentials and verify from the session logs/auth logs for the sensitive data in clear texts
- Initiate debug session of a process and verify from debug logs for any sensitive data in clear texts

11.2.4 **Test Observations:**

11.2.5 **Evidence Provided:-** (check for screenshots)

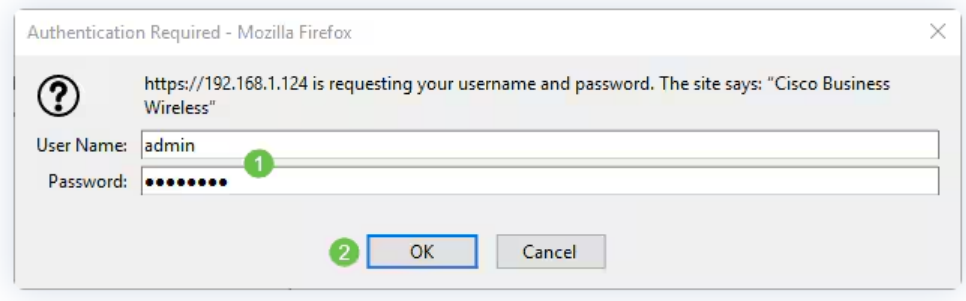
11.3 Test Case Number: 03

11.3.1 **Test Case Name:** confidentiality of sensitive data in configuration file exports

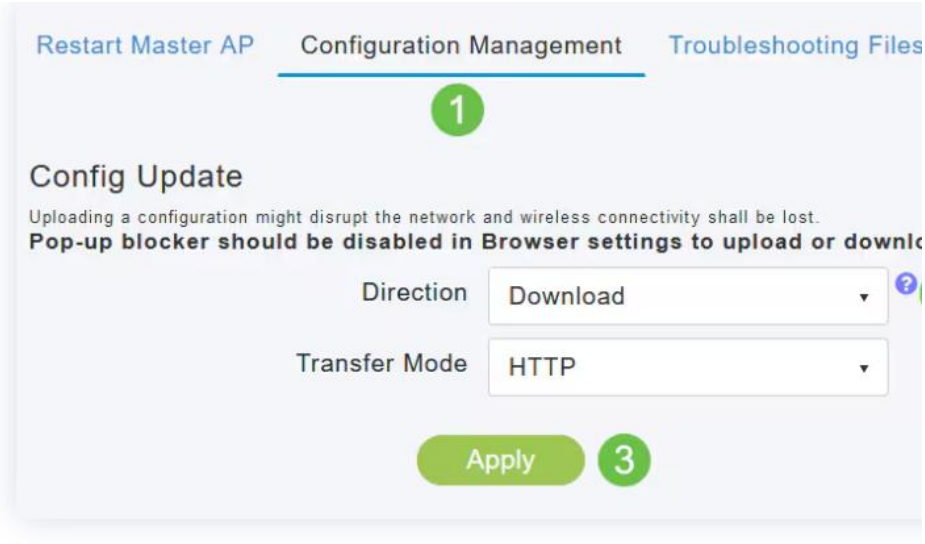
11.3.2 **Test Case Description:** The following test case is to verify the confidentiality of sensitive data in the configuration file exported from DUT

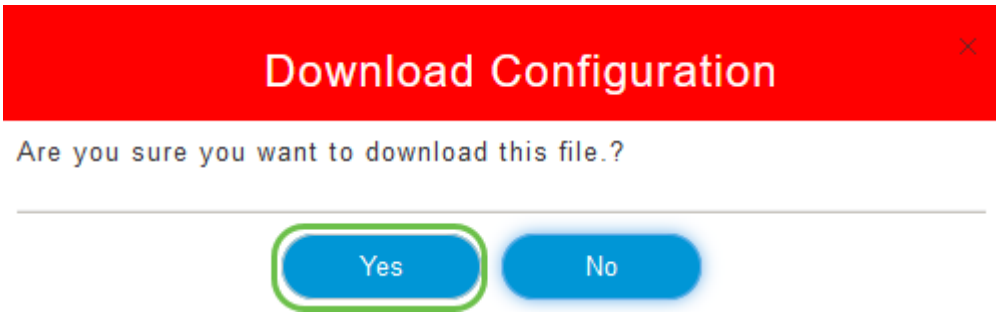
11.3.3 **Execution Steps: -** (the following test case is performed on Cisco AP AC-145)

- Access the DUT with appropriate credentials

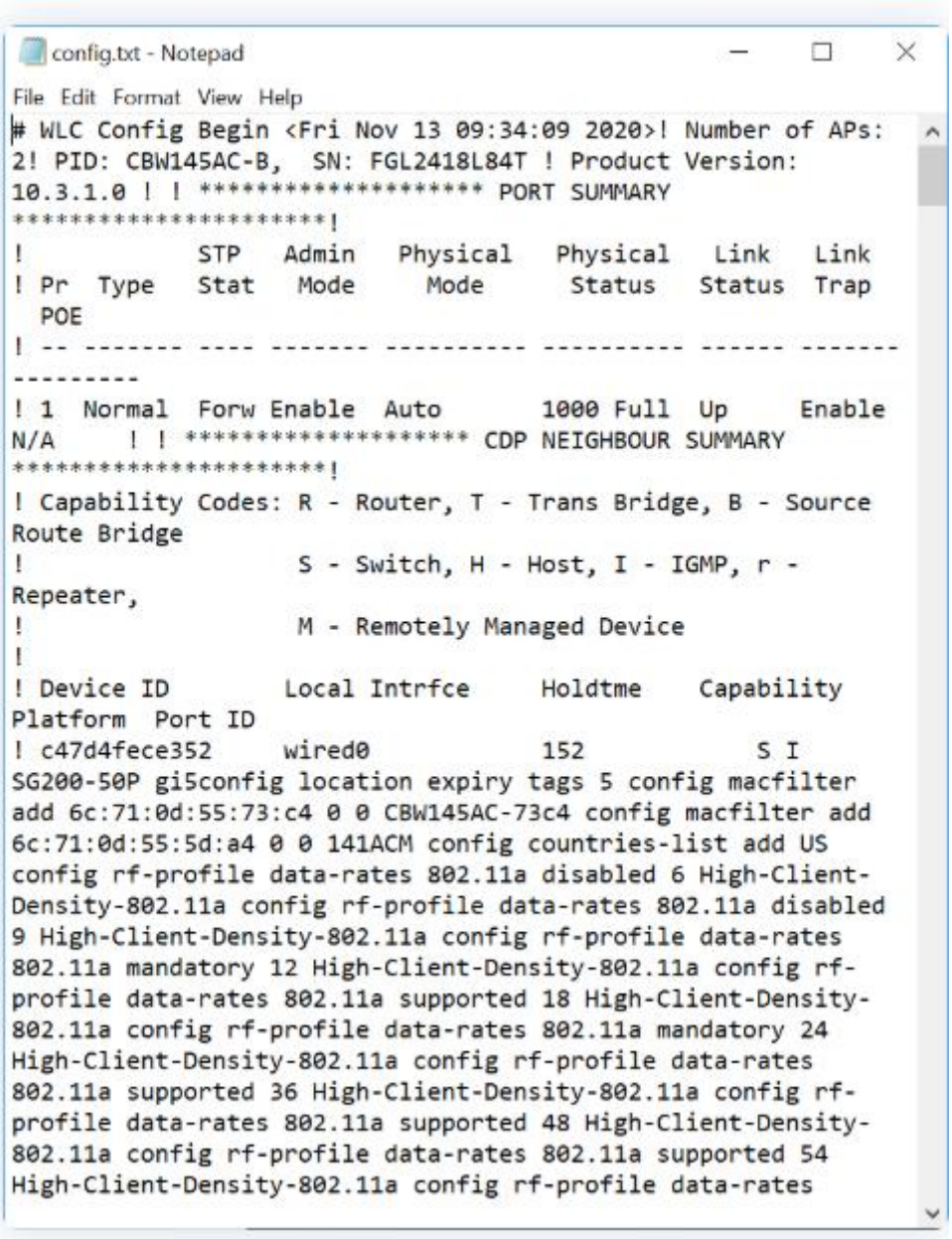


- Head to the directory of the configuration file of the DUT and attempt to download the same





- download the config file test machine where the management platform (GUI) of the DUT is running and access it



- **check for the confidentiality of any sensitive data**

11.4 Test Case Number: 04

11.4.1 **Test Case Name:** verify for access to maintenance mode

11.4.2 **Test Case Description:** The following test case is to verify the authorized access to maintenance mode

11.4.3 **Execution Steps**

- Review the OEM documentation for the availability/accessibility of maintenance mode
- Attempt to access the maintenance mode by a normal user(unauthorized user) and verify if its permitted or not

11.4.4 **Test Observation**

11.4.5 **Evidence Provided**

11. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	verify confidentiality of sensitive data in system functions		No document available
2	verify confidentiality of sensitive data in logs		
3	confidentiality of sensitive data in configuration file exports		
4.	verify for access to maintenance mode		

1.6.4 Crypto-Key Protection Mechanism

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 2.6 Data Protection**
2. **<Security Requirement No & Name > 2.6.4: Crypto-Key Protection Mechanism**
3. **<Requirement Description: >** For sensitive data (persistent or temporary) in storage, read access rights shall be restricted.
   a. Sensitive files of Wi-Fi CPE that are needed for the functionality shall be protected against manipulation strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" with appropriate non-repudiation controls.
   b. In addition, the following rules apply for:
      (i) Systems that need access to identification and authentication data in the clear/readable form e.g., in order to perform an activity/operation. Such systems shall not store this data in the clear/readable form, but scramble or encrypt it by implementation-specific means.
      (ii) Systems that do not need access to sensitive data (e.g., user passwords) in the clear. Such systems shall hash this sensitive data strictly using the cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.
      (iii) Stored files in the Wi-Fi CPE shall be protected against manipulation strictly using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only
4. **DUT Confirmation Details**:

5. **DUT <u>Configuration:</u>** No configuration needed

6. **Preconditions:** - OEM shall provide details of sensitive data (persistent or temporary) where it is stored and who all have access to read/ write.

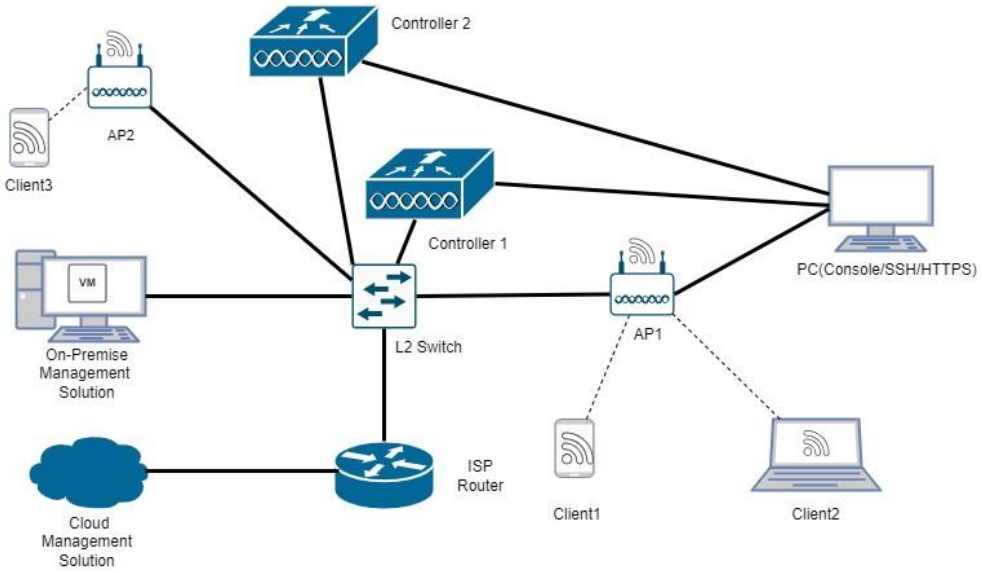
7. **<u>Test Objective:</u>** - To verify that sensitive data in storage is access restricted and protected against manipulation using the Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" with appropriate non-repudiation controls. To check DUT's protection mechanism against confidential data in storage being exposed
8. **<u>Test Plan</u>**

8.1. Number of Test Scenarios:

8.1.1. Test scenario to verify that user passwords/sensitive data are stored in encrypted form / one-way hash algorithm.

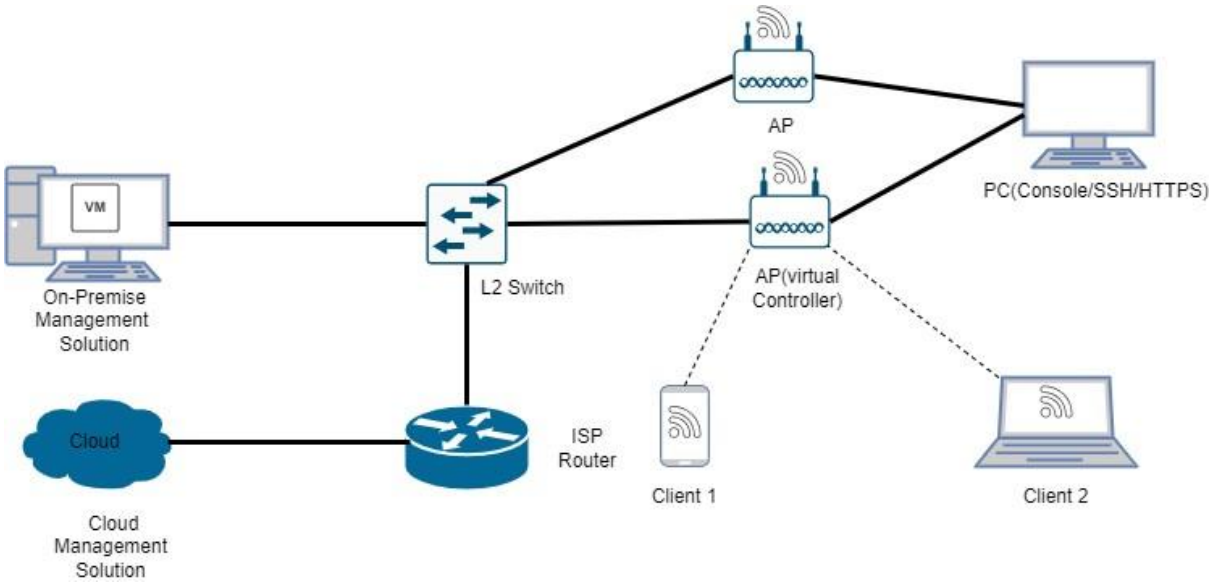
8.1.2. Test Scenario to check access control on such system functions where passwords/sensitive data is stored

8.2. Test Bed Diagram



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

8.3. Tools Required: - DUT

8.4. Test Execution Steps

- Access the directory of sensitive data/password in accordance to the OEM documentation. Verify the access rights
- Also verify if DUT has protection against manipulation of sensitive

9. **Expected Results for Pass:**

10. **Expected Format of Evidence:** Screenshots of Terminal and pcap file

11. **Test Execution:**

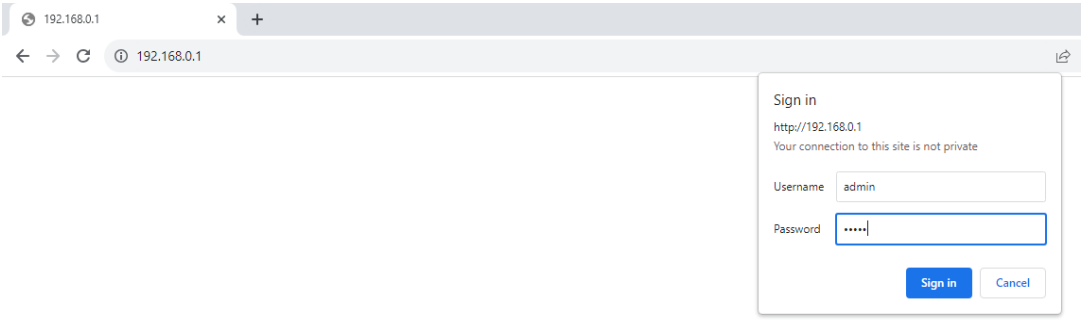
11.1 Test Case Number: 01

11.1.1 **Test Case Name:** verify that user passwords/sensitive data are stored in encrypted form / one-way hash algorithm.

11.1.2 **Test Case Description:** The Tester shall check the sensitive data/password is not stored in clear text

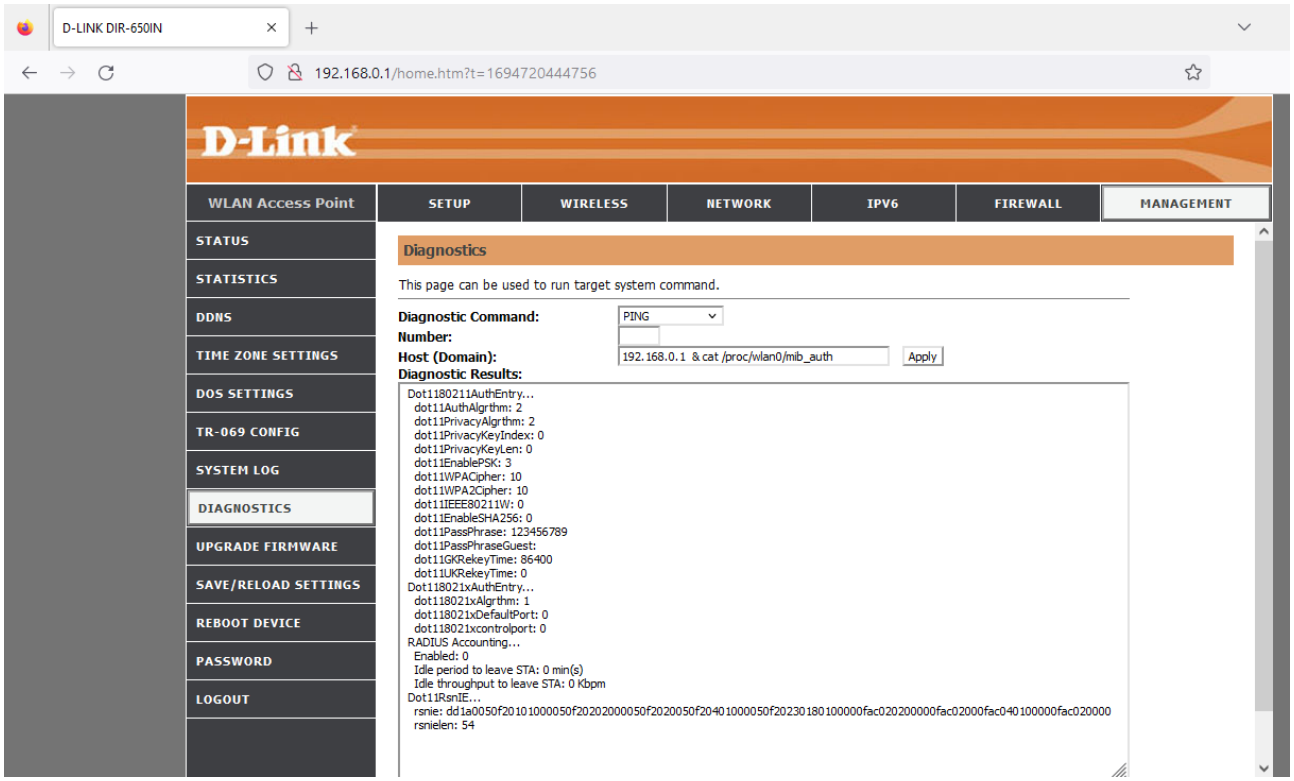
11.1.3 **Execution Steps:**

- The tester logged into the DUT's Web GUI (http://192.168.0.1) in the web browser of the test machine (192.168.0.22) account "admin" using the respective authentication attribute (password).



- The Tester clicked on Management > Diagnostics> Select ping

- Put command line injection payload in the Host (Domain) input field. i.e., payload =192.168.0.1 & cat /proc/wlan0/mib_auth to reveal the wireless password.



- After the execution of the command line injection payload, DUT revealed the wireless password in clear text.
- The Tester concludes that the data and information are not stored in encryption format.

11.1.4 **Test Observations:** The Tester concludes that the data and information are not stored in encryption format.

11.1.5 **Evidence Provided: -** Screenshots

11.2 Test Case Number: 02

11.2.1 **Test Case Name** check access control on such system functions where sensitive data/password is stored.

11.2.2 **Test Case Description:** The Tester shall check access control on such system functions where sensitive data is stored.

11.2.3 **Execution Steps:**

- In DUT, there is only one pre-defined “admin” account that has access to sensitive data stored in DUT.

- The tester shall verify the access control of a particular sensitive file of different user roles supported by the DUT (by appropriate commands or by OEM documentation)
- The tester shall check attempt to access the sensitive file(such as /cat/passwd where the password is stored) as normal user/non privileged user and verify if the DUT permits the same or not
- The tester shall access the same sensitive file as privileged user and verify if the DUT permits the access or not

11.2.4 **Test Observations**: - The Tester verified there is only one pre-defined "admin" account that has access to sensitive data stored in DUT.

11.2.5 **Evidence Provided**: - Screenshots

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	verify that user passwords are stored in encrypted form / one-way hash algorithm	FAIL	
2	check access control on such system functions where sensitive data is stored.		Procedures mentioned

1.6.5 Protecting data and information - Confidential System Internal Data <DUT Details: > Ex: Router

<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 2.6 Data Protection**
2. **<Security Requirement No & Name > 2.6.5: Protecting data and information - Confidential System Internal Data**
3. **<Requirement Description: >** CPE shall have protection against creating a copy of data in use / data in transit. Protective measures should exist against use of available system functions / software residing in CPE to create copy of data for illegal transmission. The software functions, components in the CPE for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

4. **DUT Confirmation Details**:

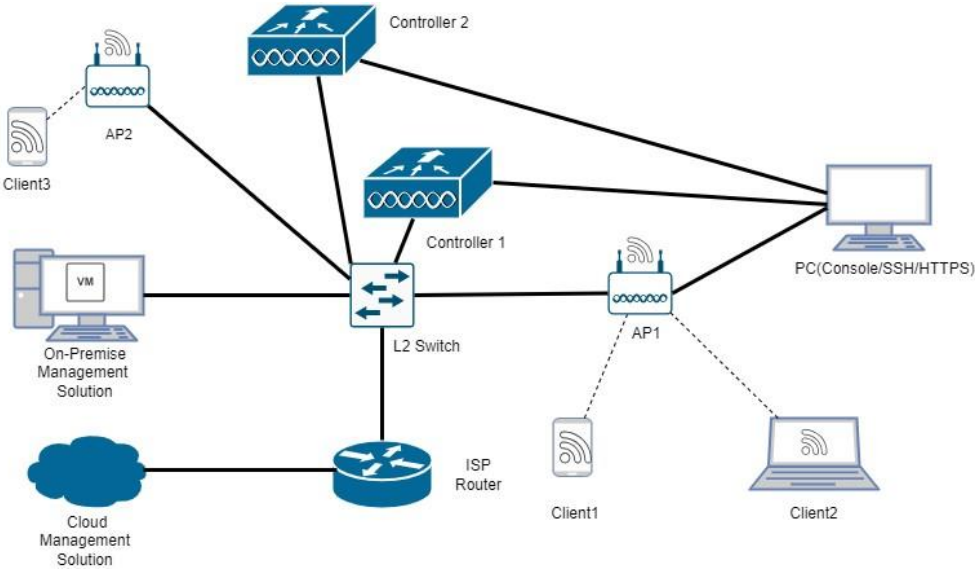
5. **DUT Configuration:** No configuration needed

6. **Preconditions:** - OEM shall provide details of available system functions/software supported by the DUT with which copy of data can be done and protective measures against using it

7. **Test Objective: -** To check DUT's protection mechanism against illegal copying of data in use and in transit

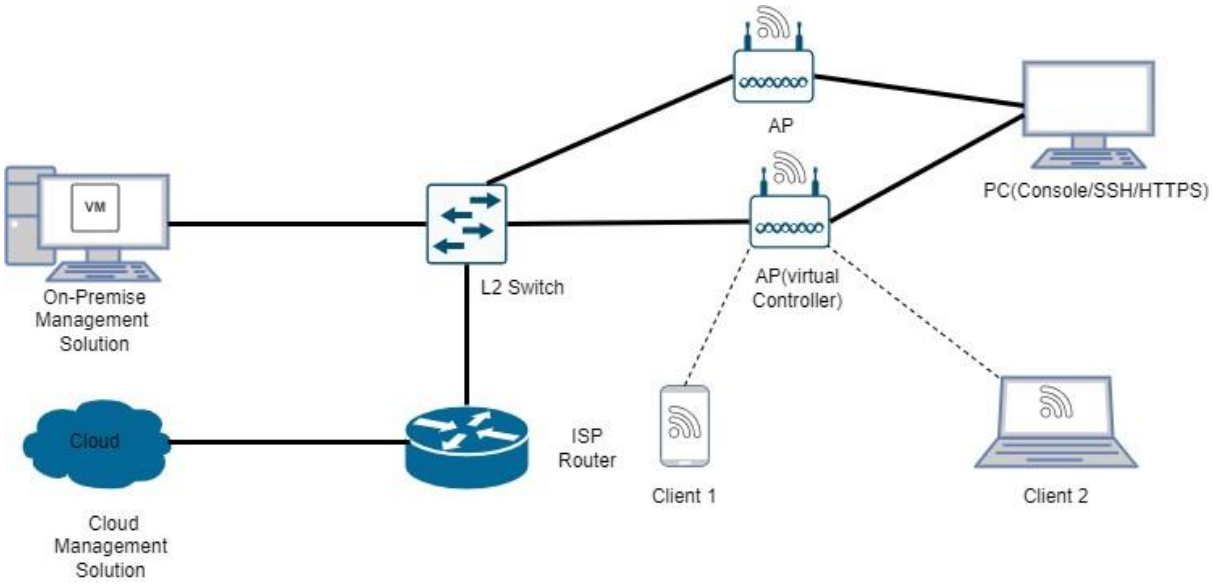
8. **Test Plan**
   8.1. Number of Test Scenarios:
      8.1.1. Test Scenario to verify protection against copy of data in use and data in transit
      8.1.2. Test Scenario to verify protection against copy of data in use and data in transit (in split mode)

   8.2. Test Bed Diagram



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

8.3. Tools Required

- DUT

8.4. Test Execution Steps

- The tester will perform copying of files with the supported communication protocols and check if they are secure
- The tester shall if the supported copy function are disabled or sufficiently secured

9. **Expected Results for Pass:**

- The DUT has copy functions disabled or sufficiently secured
- The DUT transfers file in encrypted format

10. **Expected Format of Evidence:** Screenshots of Terminal and pcap file

11. **Test Execution:**

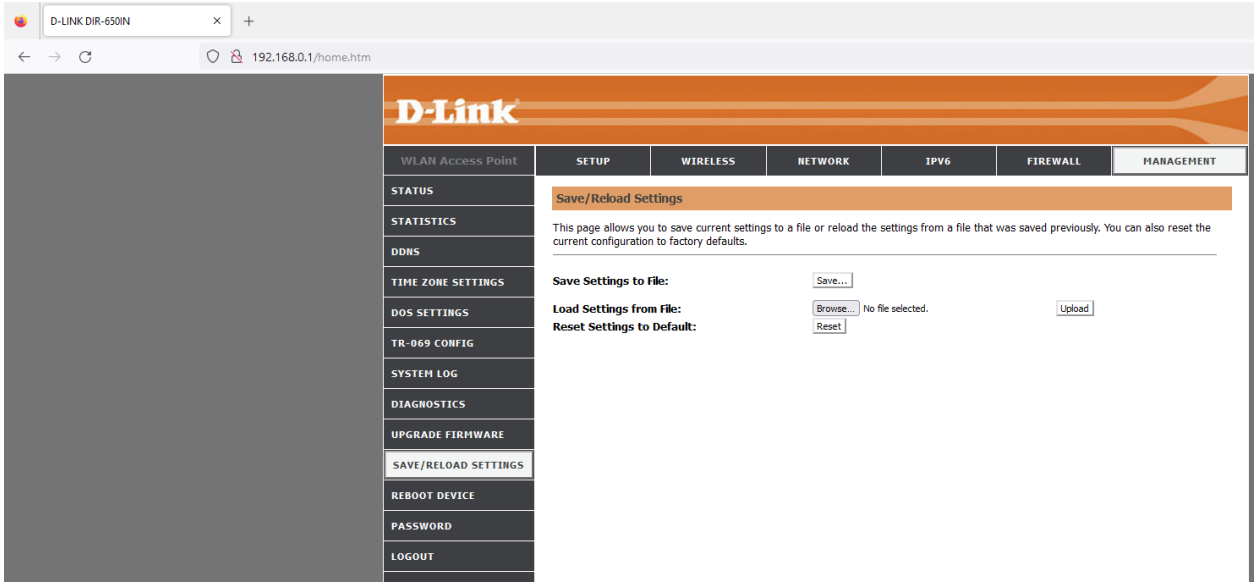
11.1 Test Case Number: 01

11.1.1 **Test Case Name:** verify protection against copy of data in use and data in transit

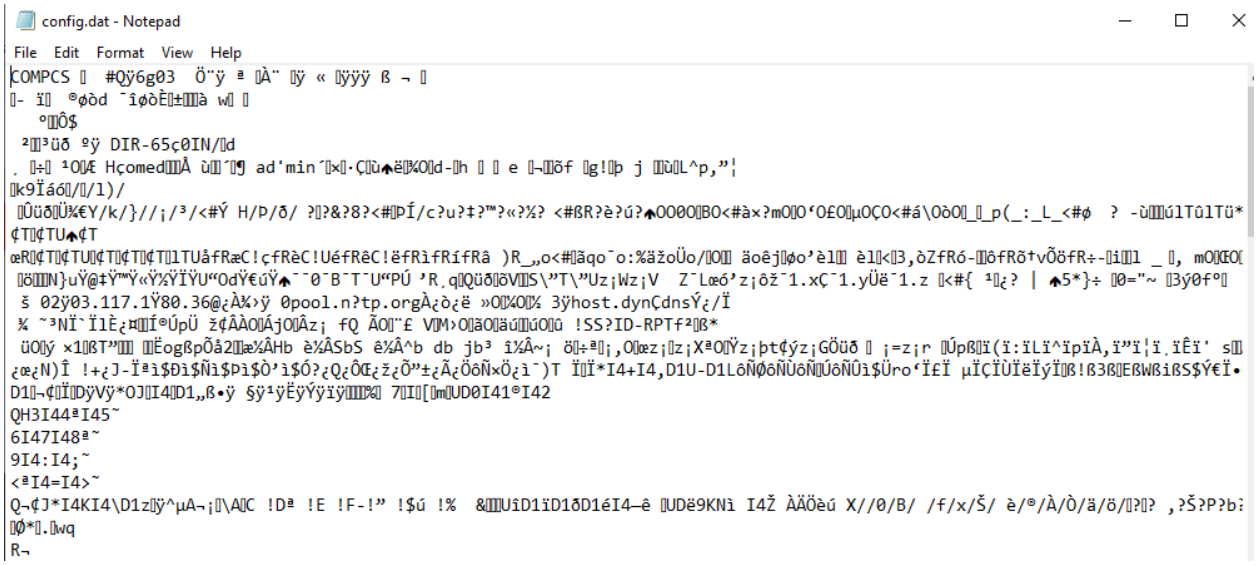
11.1.2 **Test Case Description:** The following test case to check if the DUT has protection against copy of data in use and data in transit

11.1.3 **Execution Steps:**

- The Tester shall review the OEM documentation regarding software functions, components, etc., in the AP that can create or copy data and ensure that the documentation explains the protective mechanisms to prevent illegal copying or transmission
- The tester logs in to the DUT's Web GUI (http://192.168.0.1) in the web browser of the test machine (192.168.0.100) account "admin" with using the respective authentication attribute (password).



- The Tester clicked on MANAGEMENT > Save/Reload Settings.
- The Tester found the "Save Settings to File" option to save the DUT configuration to the file system.
- The Tester clicks on the save button to save the configuration file to the local machine and attempts to read the config file but all data is in an unreadable format.



- Review the OEM documentation for the supported copy functions and verify it in the DUT

```
FortiWiFi-61F # copy
command parse error before 'copy'

FortiWiFi-61F #
config      Configure object.
get         Get dynamic and system information.
show        Show configuration.
diagnose    Diagnose facility.
execute     Execute static commands.
alias       Execute alias commands.
exit        Exit the CLI.

FortiWiFi-61F # alias
name    Alias command name.

FortiWiFi-61F # alias name
 <Enter>

FortiWiFi-61F # alias name
name is invalid alias command.

FortiWiFi-61F #
```

- Tester unable to copy the files in other location within the DUT (if the copy functions are supported by the DUT)
- Attempt to copy data in use (for eg. Running-config) to a removable media mounted location (as means of illegal transmission)
- Verify that data is allowed to copied or not
- If access roles are set on the copy functions attempt the above execution steps as an unauthorized user

11.1.4 **Test Observations:** The Tester observed that the data stays encrypted as a protection against copy of data. The data cannot be copied as copy functions are not supported by the DUT

11.1.5 **Evidence Provided:** - Screenshots are provided above

11.2 Test Case Number: 02

11.2.1 **Test Case Name:** verify protection against copy of data in use and data in transit (in split mode)

11.2.2 **Test Case Description:** The following test case to check if the AP has protection against copy of data in use and data in transit

11.2.3 **Execution Steps**

- Review the OEM documentation of the controller to check the access rights of the Controller users to manage the AP and its supported copy functions data
- Access the AP from the controller as a normal user and attempt to copy the data in use(running-config, logs)
- Verify if copy functions are sufficiently secured. Or if its disabled
- Attempt to connect to the AP with a different OS image version. Due to which the controller pushes its own image to be installed in the AP for upgrade. Capture this communication and verify that the data in transit is secure on the CAPWAP /equivalent channel

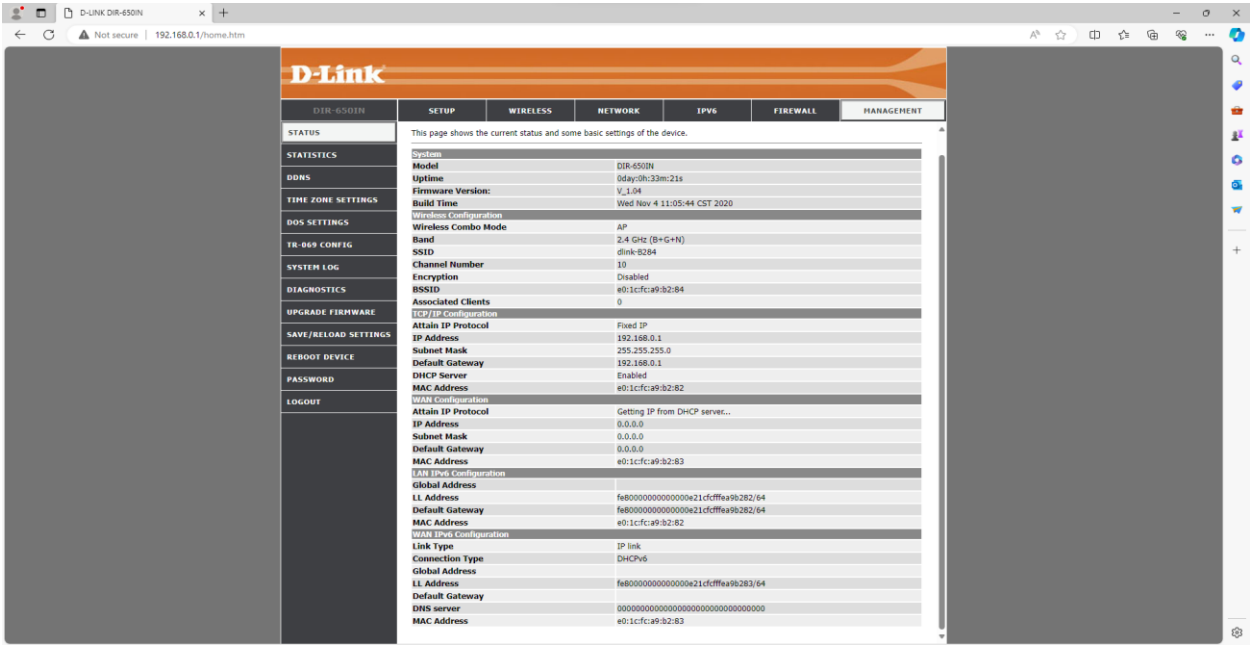
12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	verify protection against copy of data in use and data in transit		
2	verify protection against copy of data in use and data in transit(in split mode)		

1.6.6: Protecting data and information in storage

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name>** Section 2.6 Data Protection
2. **<Security Requirement No & Name >** 2.6.6: Protection against Data Exfiltration - Overt Channel
3. **<Requirement Description: >** Wi-Fi CPE shall have mechanisms to prevent data exfiltration attacks for theft of data in use /data in transit. Establishment of outbound overt channels such as FTP, HTTP, HTTPS IM, P2P, Email etc. are to be forbidden if they are initiated by / originate from the Wi-Fi CPE. Outbound-use of such services are to be disabled in the Wi-Fi CPE, if it is essential to have some of these services for outbound-use (remote management etc.,), facility to exist for monitoring anomalous channels. Session logs shall be generated for establishment of any session initiated by either user or Wi-Fi CPE
4. **DUT Confirmation Details**:



5. **<u>DUT Configuration:</u>**

6. **<u>Preconditions:-</u>** OEM documentation

7. **<u>Test Objective</u>**

- To check DUT's protection against establishment of overt channel for data exfiltration
- To verify if DUT monitors any anomalous channels
- To verify if DUT generates the session logs for every session established

8. **Test Plan**

8.1. Number of Test Scenarios:

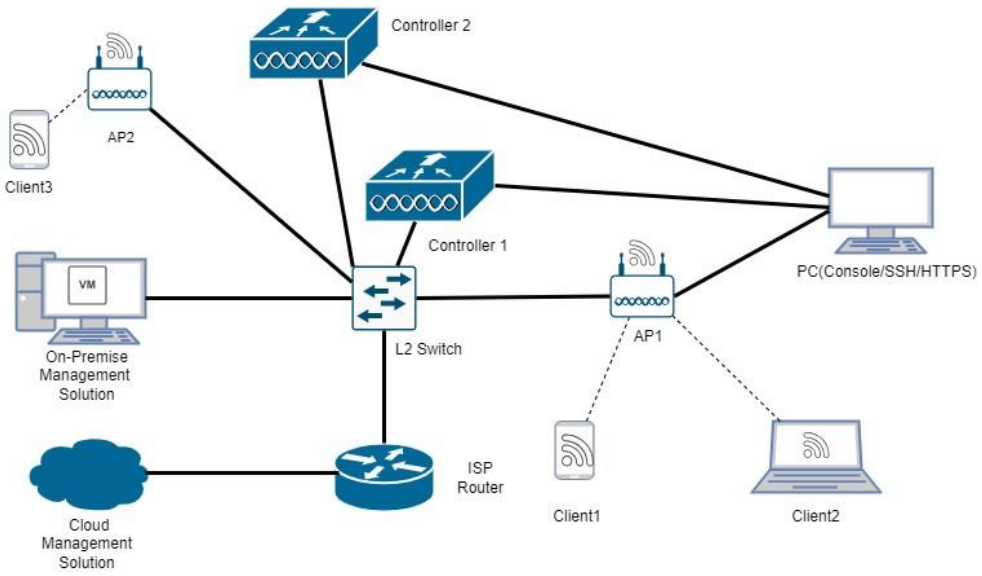
8.1.1. Test Scenario to review the OEM documentation to check for the overt channels mentioned

8.1.2. Test Scenario to Check if the outbound overt channels initiated by WiFi CPE is forbidden

8.1.3. Test Scenario to check if any monitoring system exists upon the establishment of outbound overt channel

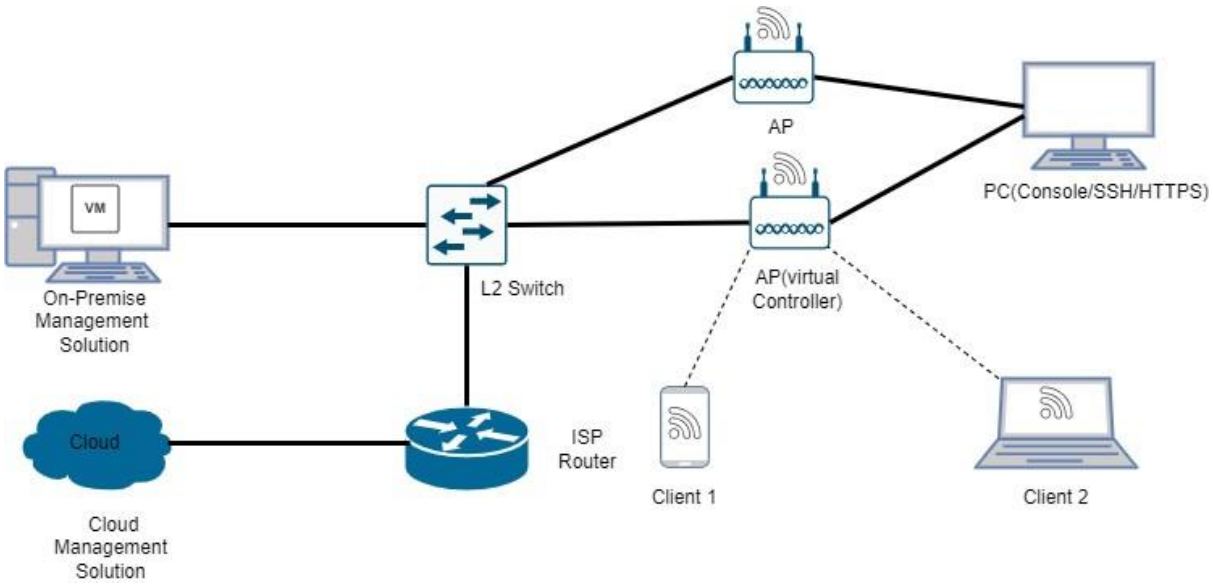
8.1.4. To verify if DUT generates the session logs for every session established

8.2. Test Bed Diagram



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

8.3. Tools Required

- DUT

8.4. Test Execution Steps

- The Tester shall review the document from OEM explaining the mechanism implemented to meet the clause and the default configuration
- The tester shall trigger scenarios for Wifi Cpe to initiate outbound overt channel and verify that its forbidden.
- The Tester shall check if any of the services are used for the Outbound channel by any unauthorized users
- The tester shall check if any monitoring system exists upon the establishment of outbound overt channel

9. **Expected Results for Pass:** The DUT prevent the use of outbound-overt channel, that is if they are initiated or originated by Wifi CPE. Also, the session logs are maintained for any outbound channel established

10. **Expected Format of Evidence:** Screenshots

11. **Test Execution:**

11.1 Test Case Number: 01

11.1.1 **Test Case Name:** Review the OEM documentation for outbound overt channels

11.1.2 **Test Case Description:** The Tester shall check if all of the services mentioned in the OEM documentation are used for the Outbound overt channel

11.1.3 **Execution Steps:** The Tester explored the DUT and didn't find any outbound overt channels such as FTP, HTTPS IM, P2P, Email, etc. other than HTTP. HTTP channel is used for the management/configuration of DUT.

However, Tester shall verify with OEM to conclude the verdict for this clause.

11.1.4 **Test Observations:** The Tester explored the DUT and didn't find any outbound overt channels such as FTP, HTTPS IM, P2P, Email, etc. other than HTTP. HTTP channel is used for the management/configuration of DUT.

However, Tester shall verify with OEM to conclude the verdict for this clause.

11.1.5 **Evidence Provided:**- Screenshots

11.2 Test Case Number: 02

11.2.1 **Test Case Name:** Check if the outbound overt channels initiated by WiFi CPE is forbidden

11.2.2 **Test Case Description:** the following test case is done to check if overt channel initiated by Wifi CPE is disabled

11.2.3 **Execution steps :**

- If the Wifi CPE supports scripting , the tester must integrate the script that will make Wifi CPE establish an outbound channel
  For eg Cisco IOS supports an inbult common scheduler called "kron" , using the tester may simulate the established of an TFTP channel by Wifi CPE

  kron policy-list TFTP_BACKUP
  cli show running-config | redirect tftp://10.0.0.5/cpe_config.txt
  exit
  Verify if the DUT forbids the establishment of this TFTP channel

- The tester needs to verify that the auto-update configuration that enables Wifi to automatically download and install new firmware updates without user intervention is disabled and must verify it in actual working.

- The tester must integrate an opensource malware that forces DUT to exfiltrate config data to an external entity and verify that its forbidden

11.3 Test Case Number: 03

11.3.1 **Test Case Name:** Scenario to check if any monitoring system exists upon the establishment of outbound overt channel

11.3.2 **Test Case Description:** the following test case is done to check if DUT monitors any anomalous activity happening in the established overt channel

11.3.3 **Execution steps :**

- Review the OEM documentation to check if there exists any monitoring system for anomalous channel

- Attempt to simulate this by sending data of various sizes/frequencies/patterns over the overt channel and verify if the DUT has detected/logged/alerted
  the same

11.4 Test Case Number: 04

11.4.1 **Test Case Name:** Check for session logs

11.4.2 **Test Case Description:** The Tester shall check if any monitoring system exists that can log upon the establishment of outbound overt channel

11.4.3 **Execution Steps:**

- The Tester shall establish an outbound overt channel from DUT to another connected entity(eg; using SFTP)
- The tester shall also trigger scenario to make wifi cpe initiate an outbound overt channel
- The tester shall check if any session log is maintained upon the establishment or closing the overt channel in both cases

11.4.4 **Test Observations:**

11.4.5 **Evidence Provided**

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Review the OEM documentation		No such protocols found
2	the outbound overt channels initiated by WiFi CPE is forbidden		
3	Scenario to check if any monitoring system exists upon the establishment of outbound overt channel		
4.	Check for session logs		

1.6.7: Protection against Copy of Data

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name>** Section 2.6 Data Protection
2. **<Security Requirement No & Name >** 1.6.7: Protection against Copy of Data
3. **<Requirement Description: >** Wi-Fi CPE shall have mechanisms to prevent data exfiltration attacks for theft of data in use /data in transit. Establishment of outbound covert channels and tunnels such as DNS Tunnel, HTTPS Tunnel, ICMP Tunnel, TLS, SSL, SSH, IPSEC VPN, RTP Encapsulation etc. are to be forbidden if they are initiated by / originate from the Wi-Fi CPE. Outbound use of such services are to be disabled in the Wi-Fi CPE, if it is essential to have some of these services for outbound-use (remote management etc.,), facility to exist for monitoring anomalous channels. Session logs shall be generated for establishment of any session initiated by either user or Wi-Fi CPE.

4. **DUT Confirmation Details**:

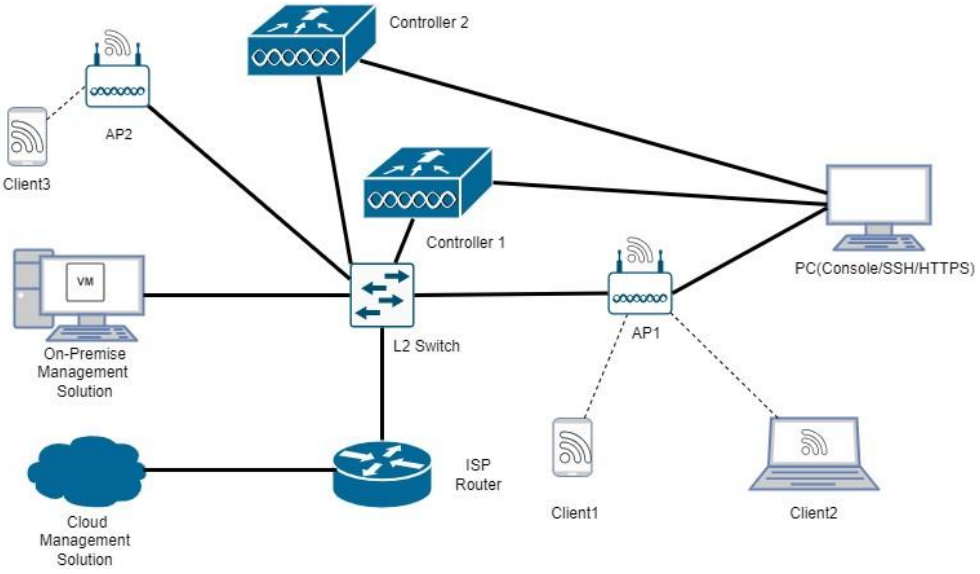
5. **DUT Configuration:** No configuration needed

6. **Preconditions: -** OEM shall provide details on what mechanisms are used to prevent data exfiltration attacks for theft of data in use/data in transit and Establishment of outbound covert channels and tunnels such as DNS Tunnel, HTTPS Tunnel, ICMP Tunnel, TLS, SSL, SSH, IPSEC VPN, RTP Encapsulation, etc. are to be forbidden, if they are initiated by CPE and how to monitor anomalous channels.

7. **Test Objective: -** To check DUT's protection against establishment of covert channel for data exfiltration and monitoring of anomalous channel

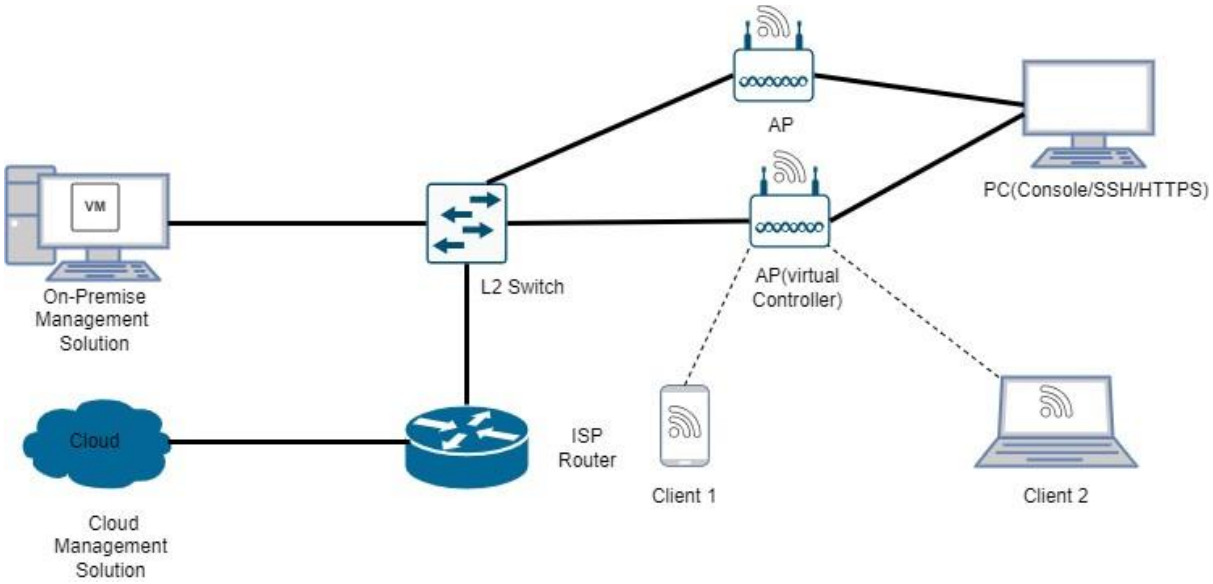
8. **Test Plan**
   - 8.1. Number of Test Scenarios:
     - 8.1.1. Test Scenario to review the OEM documentation and check if the mentioned covert channels are used in the DUT
     - 8.1.2. Test Scenario to check for the establishment of covert channel
     - 8.1.3. Test Scenario to check if any monitoring feature exists for channel establishment and data transfer
     - 8.1.4. Test Scenario to generate session logs for sessions established in the mentioned tunnels/channels

   - 8.2. Test Bed Diagram



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

8.3. Tools Required

- DUT

8.4. Test Execution Steps

- The Tester shall review the OEM documentation to check if any outbound covert channels are used in the DUT
- The Tester shall trigger the Wifi Cpe to initiate outbound covert channel and verify if DUT restricts it.
- The Tester shall check for any monitoring features present in DUT upon establishment of channel and data transfer
- The tester shall verify if the DUT generates session logs for sessions/channels established

9. **Expected Results for Pass:** The DUT prevent the use of outbound-covert channel, that is if they are initiated or originated by Wifi CPE. Also, the session logs are maintained for any outbound channel established and DUT monitors all the anomalous activities

10. **Expected Format of Evidence:** Screenshots

11. **Test Execution:**

11.1 Test Case Number: 01

11.2.1 **Test Case Name:** Review the OEM documentation

11.2.2 **Test Case Description:** The Tester shall ask for any available OEM documents, to verify the allowed outbound channels / tunnels.

11.2.3 **Execution Steps:** The Tester shall review the OEM documentation for the mentioned covert channels and figure out the possible covert channels and verify if it's disabled by default

11.2.4 **Test Observations:** OEM dependent

11.2.5 **Evidence Provided: -** Screenshots

11.2 Test Case Number: 02

11.2.1 **Test Case Name:** Monitoring anomalous activities

11.2.2 **Test Case Description:** The Tester shall attempt to establish the outbound channels from DUT to any other connected entity and verify that the DUT monitors the anomalous activities happening on the channel

11.2.3 **Execution Steps:**

- Dns tunnel
- Attempt to connect the WIFI CPE to a testing machine via ethernet and capture the same on wireshark
- filter the packets captured on port 53 and inspect the packet traces. Check if any dns tunnel query is found in the traces (looking for unusual characteristics like frequent, short queries with seemingly random domain names, large numbers of subdomains within a single domain, or unusual query types, which could indicate data being encoded within the DNS requests)
  - If the DUT supports the tool "iodine" or "dnscat2" , thesetools can be used to establish dns tunnel

- Tcp tunnel
  - Attempt to establish a tcp tunnel from wifi cpe to the testing machine (either by script or some malware)
  - Send the data from the wifi cpe in the tcp header (and not in the data field) and check if its received at the tester machine side
  - Verify if the DUT has monitored this entire above activity or maybe has logged it at some directory

  The Tester shall attempt to establish tcp tunnel (covert channel)
  Initiate a connection from the test machine

Send the data from the DUT

```
root@free5gc-af-b675c9d68-szdsr:/free5gc# echo "Covert channel Test Message" | nc 192.168.20.121 8080
```

Now check on the test machine side if the data sent from the DUT is received

```
afssr_kube@afssrkube:~$ nc -lvnp 8080
Listening on 0.0.0.0 8080
Connection received on 10.244.0.68 36610
Covert channel Test Message
```

Verify if the DUT has monitored this data transmission (in alerts, logs etc..)
(Similarly the tester can check for the establish of other covert channels from DUT using relevant commands/scripts)

11.2.4 **Test Observations:**

11.2.5 **Evidence Provided**: - Screenshots

11.3 Test Case Number: 03

11.3.1 **Test Case Name:** Covert channel initiated by WiFi

11.3.2 **Test Case Description:** The Tester shall trigger scenario to make WIFI initiate an outbound covert channel to verify if its forbidden by the DUT

11.3.3 **Execution Steps**

- The tester shall trigger a scenario to make wifi cpe self-initiate a covert channel with another entity and check if its forbidden
- This could either be done using a malware , script or scheduled task

11.4 Test Case Number: 04

11.4.1 **Test Case Name:** Verify the session logs

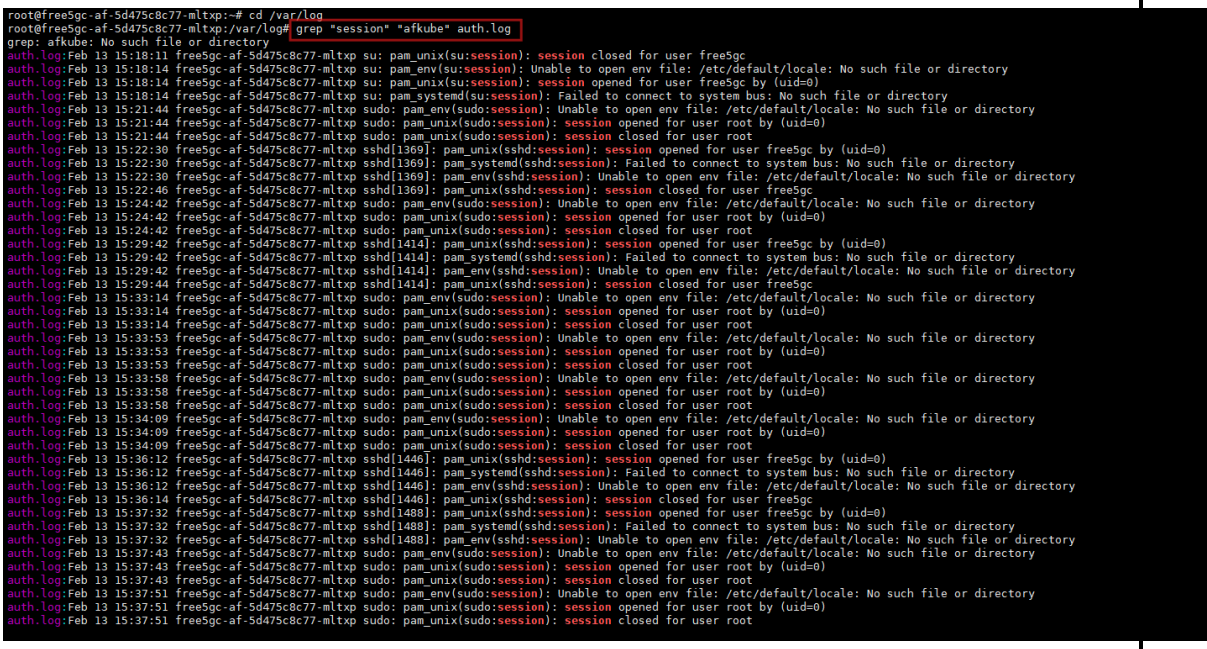
11.4.2 **Test Case Description:** The Tester shall check for any monitoring features present in DUT upon establishment of covert channel and verify that session logs are generated

11.4.3 **Execution Steps:**

- The Tester shall attempt to establish an outbound covert channel
- The tester shall also trigger the Wifi Cpe to initiate an outbound covert channel
- The Tester shall check if the session logs for the establishment of the covert channels in both the cases

  Attempt scp from DUT to an external enitity

```
root@free5gc-af-5d475c8c77-mltxp:/free5gc/config# scp -P 9091 afcfg.yaml afkube@192.168.20.120:/tmp/
The authenticity of host '[192.168.20.120]:9091 ([192.168.20.120]:9091)' can't be established.
ECDSA key fingerprint is SHA256:6TspAJL3zkIfHs0VtGp9RTaBQRZbzH79fEHFEoIYnHg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.20.120]:9091' (ECDSA) to the list of known hosts.
afkube@192.168.20.120's password:
afcfg.yaml                                    100%  931     4.7MB/s   00:00
root@free5gc-af-5d475c8c77-mltxp:/free5gc/config#
```



11.4.4 **Test Observations:** It was observed that DUT doesn't log the scp session
11.4.5 **Evidence Provided: -** Screenshots provided above

12. **<u>Test Case Result:</u>**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Review the OEM documentation		No such protocols found
2.	Covert channel establishment		
3.	Covert channel initiated by WiFi		Procedure mentioned
4.	Verify the session logs	Fail	Session logs not recorded

1.6.8: Protection against Data Exfiltration - Overt Channel

1.6.9: Protection against Data Exfiltration - Covert Channel

Section 1.7: Network Services

2.7.1 Traffic Filtering – Network Level

<DUT Details: > Wi-Fi CPE
<DUT Software Version:> 0.9.1 4.19
<Digest Hash of OS> Hash of OS required
<Digest Hash of Configuration> Hash of configuration required.
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPE
<ITSAR Version No:> ITSAR402122401 and Version: 1.0.1
<OEM Supplied Document list: > OEM Supplied Document list required

1. **<ITSAR Section No & Name>** Section 2.7: Network Services
2. **<Security Requirement No & Name >2.7.1 Traffic Filtering – Network Level**
3. **<Requirement Description: >**Wi-Fi CPE shall provide a mechanism to filter incoming IP packets on any interface (Refer to RFC 3871) In particular the Wi-Fi CPE shall provide a mechanism:
   a) To filter incoming IP packets on any IP interface at Network Layer and Transport layer of the stack ISO/Open Systems Interconnection (OSI).
   b) To allow specified actions to be taken when a filter rule matches. In particular at least the following actions should be supported:
      - Discard/Drop: the matching message is discarded; no subsequent rules are applied and no answer is sent back.
      - Accept: the matching message is accepted.
      - Account: the matching message is accounted for i.e. a counter for the rule is incremented. This action can be combined with the previous ones. This feature is useful to monitor traffic before its blocking.
   c) To enable/disable for each rule the logging for Dropped packets, i.e. details on messages matching the rule for troubleshooting.
   d) To filter on the basis of the value(s) of source IP, destination IP and port addresses of the protocol header
   e) To reset the accounting.
   f) Wi-Fi CPE shall provide a mechanism to disable/enable each defined rule.

   [Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.6.2.1]
   [Ref: RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

4. **DUT Confirmation Details**:

   - Use the command line interface to get details of the machine on which test is conducted.
   - Use command to get IP and Interfaces details
   - Use command to get OS Version/No

   Command used: Use the **show ip interface brief** command to display details of all network interfaces and associated IP addresses

```
C9300_TSTP1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES NVRAM  up                    up
Vlan21                 21.21.21.2      YES NVRAM  up                    up
Vlan22                 22.22.22.2      YES NVRAM  up                    up
Vlan23                 23.23.23.2      YES NVRAM  up                    up
Vlan83                 83.1.0.1        YES NVRAM  up                    up
Vlan84                 84.1.0.1        YES NVRAM  up                    up
Vlan85                 unassigned      YES unset  up                    up
Vlan250                10.136.250.254  YES NVRAM  up                    up
Vlan251                10.130.130.254  YES NVRAM  up                    up
Vlan252                10.137.1.254    YES NVRAM  up                    up
Vlan253                10.138.250.254  YES NVRAM  up                    up
Vlan2141               45.1.140.2      YES NVRAM  up                    up
Vlan2142               45.1.141.2      YES NVRAM  up                    up
Vlan2143               45.1.142.2      YES NVRAM  up                    up
Vlan2144               45.1.143.2      YES NVRAM  up                    up
VirtualPortGroup0      192.168.35.1    YES manual up                    up
GigabitEthernet0/0     192.168.20.140  YES NVRAM  up                    up
GigabitEthernet1/0/1   unassigned      YES unset  down                  down
GigabitEthernet1/0/2   172.16.10.1     YES NVRAM  down                  down
GigabitEthernet1/0/3   unassigned      YES unset  up                    up
GigabitEthernet1/0/4   unassigned      YES unset  down                  down
GigabitEthernet1/0/5   unassigned      YES unset  up                    up
GigabitEthernet1/0/6   unassigned      YES unset  down                  down
GigabitEthernet1/0/7   unassigned      YES unset  down                  down
GigabitEthernet1/0/8   unassigned      YES unset  down                  down
GigabitEthernet1/0/9   unassigned      YES unset  up                    up
GigabitEthernet1/0/10  unassigned      YES unset  down                  down
GigabitEthernet1/0/11  unassigned      YES unset  down                  down
```

Command used: **show version** (Use the following command to get the operating system version)

```
C9300_TSTP1#show version
Cisco IOS XE Software, Version 17.16.01
```

5. **DUT Configuration:** DUT network interfaces and IP details.

```
C9300_TSTP1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES NVRAM  up                    up
Vlan21                 21.21.21.2      YES NVRAM  up                    up
Vlan22                 22.22.22.2      YES NVRAM  up                    up
Vlan23                 23.23.23.2      YES NVRAM  up                    up
Vlan83                 83.1.0.1        YES NVRAM  up                    up
Vlan84                 84.1.0.1        YES NVRAM  up                    up
Vlan85                 unassigned      YES unset  up                    up
Vlan250                10.136.250.254  YES NVRAM  up                    up
Vlan251                10.130.130.254  YES NVRAM  up                    up
Vlan252                10.137.1.254    YES NVRAM  up                    up
Vlan253                10.138.250.254  YES NVRAM  up                    up
Vlan2141               45.1.140.2      YES NVRAM  up                    up
Vlan2142               45.1.141.2      YES NVRAM  up                    up
Vlan2143               45.1.142.2      YES NVRAM  up                    up
Vlan2144               45.1.143.2      YES NVRAM  up                    up
VirtualPortGroup0      192.168.35.1    YES manual up                    up
GigabitEthernet0/0     192.168.20.140  YES NVRAM  up                    up
GigabitEthernet1/0/1   unassigned      YES unset  down                  down
GigabitEthernet1/0/2   172.16.10.1     YES NVRAM  down                  down
GigabitEthernet1/0/3   unassigned      YES unset  up                    up
GigabitEthernet1/0/4   unassigned      YES unset  down                  down
GigabitEthernet1/0/5   unassigned      YES unset  up                    up
GigabitEthernet1/0/6   unassigned      YES unset  down                  down
GigabitEthernet1/0/7   unassigned      YES unset  down                  down
GigabitEthernet1/0/8   unassigned      YES unset  down                  down
GigabitEthernet1/0/9   unassigned      YES unset  up                    up
GigabitEthernet1/0/10  unassigned      YES unset  down                  down
GigabitEthernet1/0/11  unassigned      YES unset  down                  down
```

Host 1 and Host 2 details, make sure hosts and DUT are in the same subnet.

Host 1:

```
C9300_SW2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES NVRAM  up                    up
Vlan2141               45.1.140.3      YES NVRAM  up                    up
Vlan2142               45.1.141.3      YES NVRAM  up                    up
Vlan2143               45.1.142.3      YES NVRAM  up                    up
Vlan2144               45.1.143.3      YES NVRAM  up                    up
VirtualPortGroup0      192.168.100.1   YES NVRAM  up                    up
GigabitEthernet0/0     192.168.20.143  YES NVRAM  up                    up
GigabitEthernet1/0/1   unassigned      YES unset  down                  down
GigabitEthernet1/0/2   unassigned      YES unset  down                  down
GigabitEthernet1/0/3   unassigned      YES unset  down                  down
GigabitEthernet1/0/4   unassigned      YES unset  down                  down
GigabitEthernet1/0/5   unassigned      YES unset  down                  down
GigabitEthernet1/0/6   unassigned      YES unset  down                  down
GigabitEthernet1/0/7   unassigned      YES unset  down                  down
GigabitEthernet1/0/8   unassigned      YES unset  down                  down
GigabitEthernet1/0/9   unassigned      YES unset  up                    up
GigabitEthernet1/0/10  unassigned      YES unset  down                  down
GigabitEthernet1/0/11  unassigned      YES unset  down                  down
GigabitEthernet1/0/12  unassigned      YES unset  down                  down
GigabitEthernet1/0/13  unassigned      YES manual up                    up
```

Host 2:

```
csr@csr-virtual-machine:~$ ifconfig vlan2141
vlan2141: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 45.1.140.1  netmask 255.255.255.0  broadcast 45.1.140.255
        inet6 2001:45:140::1  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::20c:29ff:fe84:998f  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:84:99:8f  txqueuelen 1000  (Ethernet)
        RX packets 28317  bytes 1557952 (1.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 323499  bytes 30040492 (30.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Make sure the policy rules are configured in DUT.
Using ACL commands, configure the following rules for the network interface.
Create the extended ACL
ip access-list extended TRAFFIC_FILTERING

1. **Allow ICMP from Host 1 and log it**
   permit icmp host 45.1.140.3 any log

2. **Allow TCP and UDP from Host 1 and log it**
   permit tcp host 45.1.140.3 any log
   permit udp host 45.1.140.3 any log

3. **Deny ICMP from Host 2 and log it**
   deny icmp host 45.1.140.1 any log

4. **Deny TCP and UDP from Host 2 and log it**
   deny tcp host 45.1.140.1 any log
   deny udp host 45.1.140.1 any log

5. **Deny and log all other traffic from any host**
   deny ip any any log

Configured policies in DUT.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
C9300_TSTP1#
```

Configured policies in DUT Interface.

```
C9300_TSTP1(config)#interface Vlan2141
C9300_TSTP1(config-if)#ip access-group TRAFFIC_FILTERING in
C9300_TSTP1(config-if)#exit
C9300_TSTP1(config)#
```

```
C9300_TSTP1#show running-config interface Vlan2141
Building configuration...

Current configuration : 119 bytes
!
interface Vlan2141
 ip address 45.1.140.2 255.255.255.0
 ip access-group TRAFFIC_FILTERING in
 ip ospf 1 area 0
end

C9300_TSTP1#
```

Generating ICMP traffic from Host1 to DUT to get a successful response.

```
C9300_SW2#ping 45.1.140.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.1.140.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
C9300_SW2#
```

Generating TCP traffic from Host1 to DUT to get a successful response.

```
C9300_SW2#ssh -l csradmin 45.1.140.2

*************************************************************
* Welcome to the Lab Network!                               *
* Use your authorized credentials to log in.                *
* This system is monitored and controlled by law.           *
* Access is restricted to authorized personnel only.        *
* All activities are logged and subject to review.          *
*************************************************************

Password:



C9300_TSTP1>
```

6. **Preconditions:**
   - The Network Product has packet filtering enabled.
   - The Network Product has 2 different logical or physical Ethernet ports and each port is connected to a host.
   - Vendor to provide documentation (administration guide or any other document) on how to configure incoming IP packets filtering on any IP interface (LAN and wan port).
   - Tester has the highest privilege access to DUT to configure and monitor the DUT.
   - Before starting the test, connectivity should be through as per Test Bed diagram.
   - ACL rules defined.

7. **Test Objective:** Verify that the DUT provides functionality for incoming packet filtering.

8. **Test Plan:**

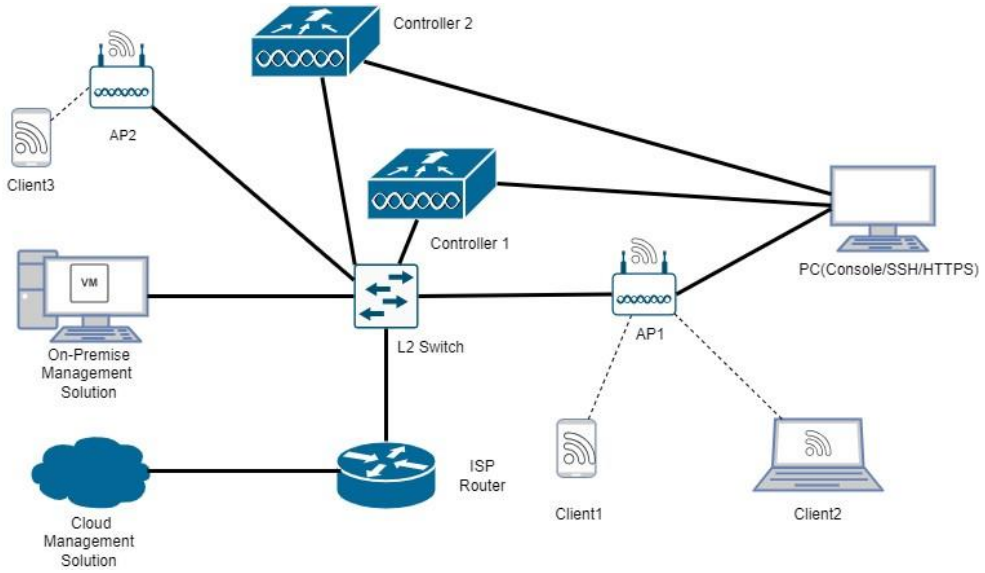
   NOTE: This plan has been executed on a vlan interface. Based on the available interface on the DUT, the tests can be conducted.

   8.1. Number of Test Scenarios: 9

8.1.1 TC_PACKET_FILTERING_NETWORKLAYER
8.1.2 TC_PACKET_FILTERING_TRANSPORTLAYER
8.1.3 TC_PACKET_FILTERING_RULE_LOGGING
8.1.4 TC_PACKET_FILTERING_ACCOUNTING
8.1.5 TC_PACKET_FILTERING_RESET_ACCOUNTING
8.1.6 TC_PACKET_FILTERING_HEADER_VALUE_NETWORKLAYER
8.1.7 TC_PACKET_FILTERING_HEADER_VALUE_TRANSPORTLAYER
8.1.8 TC_PACKET_FILTERING_ENABLE_RULE
8.1.9 TC_PACKET_FILTERING_DISABLE_RULE

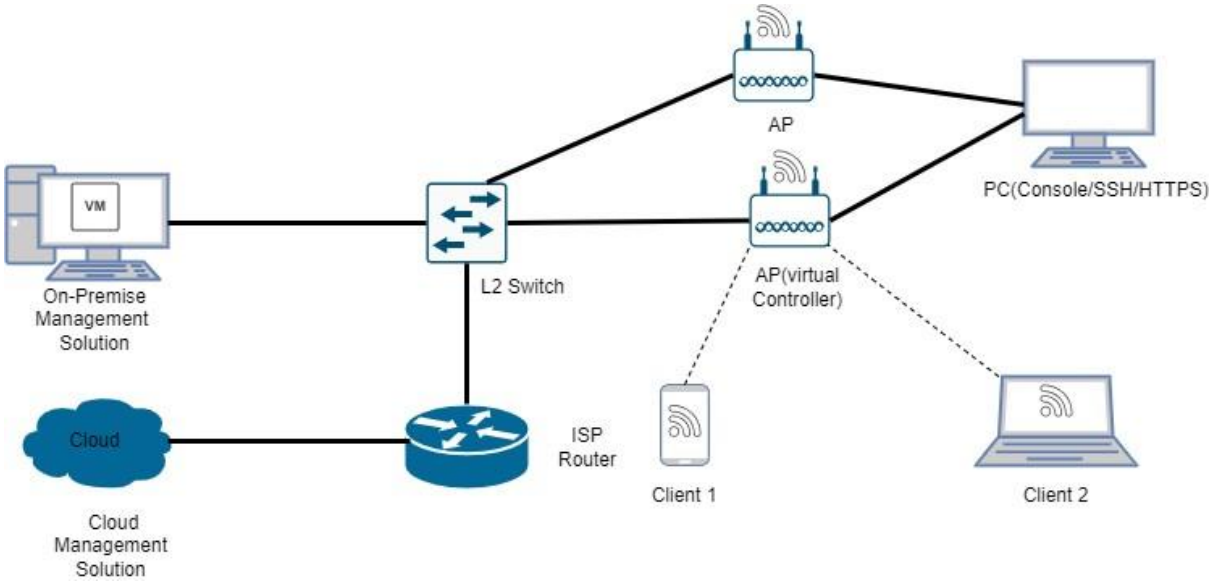
8.2 Testbed Diagram:

AP + Controller mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

8.3 Tools Required:

- Access control List.
- Ping
- SSH Client

8.4 Test Execution Steps

- The tester configures the Network Product to only allow any type of traffic (TCP/ICMP/SSH etc) from host 1.
- The tester initiates ping traffic from host 1.
- The tester initiates ping traffic from host 2.

9. Expected Results for Pass:

- Case 1: DUT receives a configured traffic and answers back to Host 1.
- Case 2: DUT blocks/receives the configured traffic and doesn't answer back from Host 2.
- Case 3: DUT drops the configured traffic and logging the traffic from Host 1 and Host 2.
- Case 4: DUT should account for the matching messages and increment the rule counter for each match.
- Case 5: DUT should reset the accounting.
- Case 6: DUT should be able to filter incoming IP packets on any IP interface at Network layer.
- Case 7: DUT should be able to filter incoming IP packets on any IP interface at the Transport layer.
- Case 8: DUT should provide a mechanism to enable each defined rule.
- Case 9: DUT should provide a mechanism to disable each defined rule.

10. **Expected Format of Evidence:** Analyse the Captured packet from DUT and put screenshots.

11. **Test Execution**

11.1 Test Case Number: 01

11.1.1 **Test Case Name:** TC_PACKET_FILTERING_NETWORKLAYER

11.1.2 **Test Case Description:** To filter incoming IP packets on the interfaces at the Network Layer of the ISO/OSI stack. To allow specified actions to be taken when a filter rule matches, such as accepting packets.

11.1.3 **Execution Steps:**

Step 1: Make sure the DUT is capable of configuring policies for Network interfaces. if the DUT supports, go through the DUT documentation and assign the policies for the selected host.

Configured policies in DUT to allow only ICMP traffic from Host1.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 2: In DUT, configure the policy to Allow any protocol from any one network interface of DUT from host1.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 3: Make sure the configuration other than Step 2, all protocols are blocked in all network interfaces.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 4: Generate network layer traffic (ICMP) from host1 to DUT and Analyse the DUT captures.

ICMP traffic is generated from HOST1. ICMP traffic is allowed in the DUT.

```
C9300_SW2#ping 45.1.140.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.1.140.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ICMP traffic is generated from HOST2. ICMP traffic is dropped in the DUT.

```
Apr 17 13:52:59.242: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(34660) -> 185.125.190.98(80), 1 packet
Apr 17 13:53:00.069: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(45962) -> 185.125.190.48(80), 1 packet
Apr 17 13:53:00.069: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(51948) -> 185.125.190.17(80), 1 packet
Apr 17 13:53:00.069: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(56208) -> 185.125.190.96(80), 1 packet
Apr 17 13:54:00.066: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(55442) -> 91.189.91.49(80), 2 packets
Apr 17 13:54:31.531: %SEC-6-IPACCESSLOGDP: list TRAFFIC_FILTERING denied icmp 45.1.140.1 -> 45.1.140.2 (8/0), 1 packet
```

11.1.5 Test Observations: DUT receives the configured traffic and answers back to Host 1.

11.2 Test Case Number: 02

11.2.1 **Test Case Name: TC_PACKET_FILTERING_TRANSPORTLAYER**

11.2.2 **Test Case Description:** To filter incoming IP packets on the interfaces at the Transport Layer of the ISO/OSI stack. To allow specified actions to be taken when a filter rule matches, such as discarding/dropping the packets.

11.2.3 **Execution Steps:**

Step 1: Make sure the DUT is capable of configuring policies for Network interfaces, if the DUT supports go through the DUT documentation and assign the policies for the Selected host.

Configured policies in DUT to allow TCP traffic from Host1.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 2: In DUT, configure the policy to Allow any protocol from any one network interface of DUT from host1.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 3: Make sure the configuration other than Step 2, all protocols are blocked in all network interfaces.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 4: Generate Transport Layer traffic (TCP) from the host to the DUT and Analyse the DUT captures.

Generating TCP traffic from Host 1 to DUT using SSH. Captured on the DUT side.

```
C9300_SW2#ssh -l csradmin 45.1.140.2

************************************************************
* Welcome to the Lab Network!                              *
* Use your authorized credentials to log in.               *
* This system is monitored and controlled by law.          *
* Access is restricted to authorized personnel only.       *
* All activities are logged and subject to review.         *
************************************************************

Password:



C9300_TSTP1>
```

Generating UDP traffic from Host 1 to DUT using the DNS. Captured on the DUT side.

```
C9300_SW2#ping section8.csrssr
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.1.140.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
C9300_SW2#
```

Generating TCP traffic from Host 2 to DUT using the SSH. Captured on the DUT side.

```
csr@csr-virtual-machine:~$ ssh csradmin@45.1.140.2
ssh: connect to host 45.1.140.2 port 22: No route
csr@csr-virtual-machine:~$
```

Generating UDP traffic from Host 2 to DUT. Captured on the DUT side.

```
csr@csr-virtual-machine:~$ ping section8.csrssr
PING section8.csrssr (45.1.140.2) 56(84) bytes of data.
From section8.csrssr (45.1.140.2) icmp_seq=1 Packet filtered
From section8.csrssr (45.1.140.2) icmp_seq=2 Packet filtered
From section8.csrssr (45.1.140.2) icmp_seq=3 Packet filtered
From section8.csrssr (45.1.140.2) icmp_seq=4 Packet filtered
^C
--- section8.csrssr ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3004ms

csr@csr-virtual-machine:~$
```

TCP traffic are generated from HOST1, TCP traffic are allowed in DUT.

```
May  6 19:19:26.521: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(52526) -> 91.189.91.97(80), 1 packet
May  6 19:19:26.521: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(35354) -> 185.125.190.48(80), 1 packet
May  6 19:19:26.522: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(33282) -> 185.125.190.49(80), 1 packet
May  6 19:19:26.522: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING permitted tcp 45.1.140.3(39432) -> 45.1.140.2(23), 1 packet
May  6 19:23:32.372: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(34128) -> 185.125.190.98(80), 1 packet
May  6 19:23:33.388: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(46962) -> 185.125.190.17(80), 1 packet
May  6 19:23:34.411: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(43318) -> 185.125.190.48(80), 1 packet
```

TCP traffic are generated from HOST2, TCP traffic are dropped in DUT.

```
May  6 20:18:42.622: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(51008) -> 91.189.91.98(80), 1 packet
May  6 20:21:15.253: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(59422) -> 45.1.140.2(23), 1 packet
May  6 20:22:15.557: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(58932) -> 45.1.140.2(23), 1 packet
May  6 20:22:57.286: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(50194) -> 45.1.140.2(22), 1 packet
May  6 20:23:32.357: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(49700) -> 91.189.91.49(80), 1 packet
May  6 20:23:33.373: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(35076) -> 91.189.91.98(80), 1 packet
```

UDP traffic are generated from HOST1, UDP traffic are allowed in DUT.

```
C9300_TSTP1#show logging | include udp
        Logging to 21.21.21.1  (udp port 514, audit disabled,
May  6 17:28:16.663: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied udp 45.1.140.1(5353) -> 224.0.0.251(5353), 1 packet
May  6 18:28:26.522: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied udp 45.1.140.1(5353) -> 224.0.0.251(5353), 1 packet
May  6 18:30:00.942: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied udp 45.1.140.1(38565) -> 8.8.4.4(53), 1 packet
May  6 18:33:26.523: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied udp 45.1.140.1(5353) -> 224.0.0.251(5353), 6 packets
May  6 18:35:26.522: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied udp 45.1.140.1(39951) -> 8.8.4.4(53), 1 packet
May  6 18:50:51.194: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING permitted udp 45.1.140.3(17166) -> 45.1.140.2(53), 1 packet
May  6 18:50:54.145: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING permitted udp 45.1.140.3(63342) -> 45.1.140.2(53), 1 packet
May  6 18:50:56.145: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING permitted udp 45.1.140.3(52710) -> 45.1.140.2(53), 1 packet
May  6 18:50:58.145: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING permitted udp 45.1.140.3(7557) -> 45.1.140.2(53), 1 packet
May  6 18:51:01.145: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING permitted udp 45.1.140.3(61984) -> 45.1.140.2(53), 1 packet
May  6 18:51:04.149: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING permitted udp 45.1.140.3(38954) -> 45.1.140.2(53), 1 packet
May  6 19:28:16.678: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied udp 45.1.140.1(5353) -> 224.0.0.251(5353), 1 packet
May  6 19:34:42.988: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING permitted udp 45.1.140.3(11421) -> 45.1.140.2(53), 1 packet
```

UDP traffic are generated from HOST2, UDP traffic are dropped in DUT.

```
C9300_TSTP1#show logging | include udp
        Logging to 21.21.21.1  (udp port 514, audit disabled,
May  6 17:28:16.663: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied udp 45.1.140.1(5353) -> 224.0.0.251(5353), 1 packet
May  6 18:28:26.522: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied udp 45.1.140.1(5353) -> 224.0.0.251(5353), 1 packet
May  6 18:30:00.942: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied udp 45.1.140.1(38565) -> 8.8.4.4(53), 1 packet
May  6 18:33:26.523: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied udp 45.1.140.1(5353) -> 224.0.0.251(5353), 6 packets
May  6 18:35:26.522: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied udp 45.1.140.1(39951) -> 8.8.4.4(53), 1 packet
May  6 18:50:51.194: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING permitted udp 45.1.140.3(17166) -> 45.1.140.2(53), 1 packet
May  6 18:50:54.145: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING permitted udp 45.1.140.3(63342) -> 45.1.140.2(53), 1 packet
May  6 18:50:56.145: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING permitted udp 45.1.140.3(52710) -> 45.1.140.2(53), 1 packet
May  6 18:50:58.145: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING permitted udp 45.1.140.3(7557) -> 45.1.140.2(53), 1 packet
May  6 18:51:01.145: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING permitted udp 45.1.140.3(61984) -> 45.1.140.2(53), 1 packet
May  6 18:51:04.149: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING permitted udp 45.1.140.3(38954) -> 45.1.140.2(53), 1 packet
May  6 19:28:16.678: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied udp 45.1.140.1(5353) -> 224.0.0.251(5353), 1 packet
May  6 19:34:42.988: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING permitted udp 45.1.140.3(11421) -> 45.1.140.2(53), 1 packet
```

11.2.4 **Test Observations:** DUT deny the configured traffic from Host 2 and doesn't answer back. DUT deny all other traffic from host1 and host2.

11.3 Test Case Number: 03

11.3.1 **Test Case Name:** TC_PACKET_FILTERING_RULE_LOGGING

11.3.2 **Test Case Description:** To filter incoming IP packets on the interfaces at the Network Layer and Transport Layer of the stack ISO/OSI. To enable/disable for each rule the logging for Dropped packets, i.e. details on messages matching the rule for troubleshooting.

11.3.3 **Execution Steps:**

Generating ICMP traffic from Host1 to DUT to get a successful response.

```
C9300_SW2#ping 45.1.140.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.1.140.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Generating TCP traffic from Host1 to DUT to get a successful response.

```
C9300_SW2#ssh -l csradmin 45.1.140.2

**************************************************************
* Welcome to the Lab Network!                                *
* Use your authorized credentials to log in.                 *
* This system is monitored and controlled by law.            *
* Access is restricted to authorized personnel only.         *
* All activities are logged and subject to review.           *
**************************************************************

Password:



C9300_TSTP1>
```

Step 2: Make sure the DUT is capable of configuring policies for Network interfaces, if the DUT supports go through the DUT documentation and assign the policies for the Selected host**.**

Configured policies in DUT to allow only ICMP traffic and TCP traffic from Host1.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 3: In DUT, configure the policy to Allow any protocol from any one network interface of DUT from host1**.**

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 4: Make sure the configuration other than Step 5, all protocols are blocked in all network interfaces.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 5: Other than host1, generate traffic from any host to DUT and Analyse the DUT captures. Generate traffic from host 2: Log captured from host 2 which generates ICMP and TCP traffic TCP

```
csr@csr-virtual-machine:~$ ssh csradmin@45.1.140.2
ssh: connect to host 45.1.140.2 port 22: No route
csr@csr-virtual-machine:~$
```

ICMP

```
csr@csr-virtual-machine:~$ ping 45.1.140.2
PING 45.1.140.2 (45.1.140.2) 56(84) bytes of data.
From 45.1.140.2 icmp_seq=1 Packet filtered
From 45.1.140.2 icmp_seq=2 Packet filtered
From 45.1.140.2 icmp_seq=3 Packet filtered
^C
--- 45.1.140.2 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2030ms
```

Step 6: Generating ICMP and TCP traffic from Host 2 to DUT two interfaces gets an unsuccessful response. Captured on the DUT side.

ICMP traffic are generated from HOST2. ICMP traffic is dropped in the DUT.

```
Apr 17 13:52:59.242: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(34660) -> 185.125.190.98(80), 1 packet
Apr 17 13:53:00.069: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(45962) -> 185.125.190.48(80), 1 packet
Apr 17 13:53:00.069: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(51948) -> 185.125.190.17(80), 1 packet
Apr 17 13:53:00.069: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(56208) -> 185.125.190.96(80), 1 packet
Apr 17 13:54:00.066: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(55442) -> 91.189.91.49(80), 2 packets
Apr 17 13:54:31.531: %SEC-6-IPACCESSLOGDP: list TRAFFIC_FILTERING denied icmp 45.1.140.1 -> 45.1.140.2 (8/0), 1 packet
```

TCP traffic are generated from HOST2, TCP traffic are dropped in DUT.

```
May  6 20:18:42.622: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(51008) -> 91.189.91.98(80), 1 packet
May  6 20:21:15.253: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(59422) -> 45.1.140.2(23), 1 packet
May  6 20:22:15.557: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(58932) -> 45.1.140.2(23), 1 packet
May  6 20:22:57.286: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(50194) -> 45.1.140.2(22), 1 packet
May  6 20:23:32.357: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(49700) -> 91.189.91.49(80), 1 packet
May  6 20:23:33.373: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(35076) -> 91.189.91.98(80), 1 packet
```

Step 7: Verify In DUT the rule for logging can be enable/disable**.**

In DUT able to disable logging rule.

```
C9300_TSTP1(config)#ip access-list extended TRAFFIC_FILTERING
C9300_TSTP1(config-ext-nacl)#no 10 permit tcp host 45.1.140.3 any log
C9300_TSTP1(config-ext-nacl)#exit
C9300_TSTP1(config)#
C9300_TSTP1(config)#
C9300_TSTP1(config)#exit
```

In DUT able to enable logging rule.

```
C9300_TSTP1#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
C9300_TSTP1(config)#ip access-list extended TRAFFIC_FILTERING
C9300_TSTP1(config-ext-nacl)#10 permit tcp host 45.1.140.3 any log
C9300_TSTP1(config-ext-nacl)#exit
C9300_TSTP1(config)#exit
C9300_TSTP1#
```

11.3.4 **Test Observations:** DUT drops the configured traffic and logging the traffic from Host 1 and Host 2.

11.4 Test Case Number: 04

11.4.1 **Test Case Name: TC_PACKET_FILTERING_ACCOUNTING**

11.4.2 **Test Case Description:** To filter incoming IP packets on the interfaces at the Network Layer and Transport Layer of the stack ISO/OSI. To allow specified actions to be taken when a filter rule matches. Account: the matching message is accounted for i.e. a counter for the rule is incremented. This action can be combined with the previous ones. This feature is useful to monitor traffic before its blocking.

11.4.3 **Execution Steps:**

Step 1: Make sure the DUT is capable of configuring policies for Network interfaces, if the DUT supports go through the DUT documentation and assign the policies for the Selected host.
Configured policies in DUT to allow only ICMP traffic and TCP traffic from Host1.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 2: In DUT, configure the policy to Allow any protocol from any one network interface of DUT from host1.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 3: Generate traffic from any host1 to DUT and Confirm whether the matching rules traffic is counted in DUT**.**
Configured policies in DUT to allow only ICMP traffic and TCP traffic from Host1.
In DUT the icmp traffic are allowed . The accountings have happened.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log (37 matches)
    20 permit icmp host 45.1.140.3 any log (80 matches)
    30 permit udp host 45.1.140.3 any log (27 matches)
    40 deny icmp host 45.1.140.1 any log (23 matches)
    50 deny tcp host 45.1.140.1 any log (4080 matches)
    60 deny udp host 45.1.140.1 any log (23 matches)
    70 deny ip any any log (8 matches)
C9300_TSTP1#
```

11.4.4 **Test Observations:** The matching messages are accounted and the counter for the rule is incremented.

11.5 Test Case Number: 05

11.5.1 **Test Case Name:** T**C_PACKET_FILTERING_RESET_ACCOUNTING**
11.5.2 **Test Case Description:** To filter incoming IP packets on the interfaces at the Network Layer and Transport Layer of the stack ISO/OSI. To reset the accounting.
11.5.3 Execution Steps:
Step 1: Make sure the DUT is capable of configuring policies for Network interfaces, if the DUT supports go through the DUT documentation and assign the policies for the Selected host**.**
Configured policies in DUT to allow only ICMP traffic and TCP traffic from Host1.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 2: In DUT, configure the policy to Allow any protocol from any one network interface of DUT from host1.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 3: Make sure the configuration other than Step 5, all protocols are blocked in all network interfaces.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 4: Other than host1, generate traffic from any host to DUT and Analyse the DUT captures.

Generate traffic from host 2: Log captured from host 2 which generates ICMP and TCP traffic

TCP

```
csr@csr-virtual-machine:~$ ssh csradmin@45.1.140.2
ssh: connect to host 45.1.140.2 port 22: No route
csr@csr-virtual-machine:~$
```

ICMP

```
csr@csr-virtual-machine:~$ ping 45.1.140.2
PING 45.1.140.2 (45.1.140.2) 56(84) bytes of data.
From 45.1.140.2 icmp_seq=1 Packet filtered
From 45.1.140.2 icmp_seq=2 Packet filtered
From 45.1.140.2 icmp_seq=3 Packet filtered
^C
--- 45.1.140.2 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2030ms
```

Generating ICMP and TCP traffic from Host 2 to DUT two interfaces gets an unsuccessful response. Captured on the DUT side.

ICMP traffic are generated from HOST2. ICMP traffic is dropped in the DUT.

```
Apr 17 13:52:59.242: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(34660) -> 185.125.190.98(80), 1 packet
Apr 17 13:53:00.069: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(45962) -> 185.125.190.48(80), 1 packet
Apr 17 13:53:00.069: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(51948) -> 185.125.190.17(80), 1 packet
Apr 17 13:53:00.069: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(56208) -> 185.125.190.96(80), 1 packet
Apr 17 13:54:00.066: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(55442) -> 91.189.91.49(80), 2 packets
Apr 17 13:54:31.531: %SEC-6-IPACCESSLOGDP: list TRAFFIC_FILTERING denied icmp 45.1.140.1 -> 45.1.140.2 (8/0), 1 packet
```

TCP traffic are generated from HOST2, TCP traffic are dropped in DUT.

```
May  6 20:18:42.622: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(51008) -> 91.189.91.98(80), 1 packet
May  6 20:21:15.253: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(59422) -> 45.1.140.2(23), 1 packet
May  6 20:22:15.557: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(58932) -> 45.1.140.2(23), 1 packet
May  6 20:22:57.286: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(50194) -> 45.1.140.2(22), 1 packet
May  6 20:23:32.357: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(49700) -> 91.189.91.49(80), 1 packet
May  6 20:23:33.373: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(35076) -> 91.189.91.98(80), 1 packet
```

Confirm the traffic accounted.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log (37 matches)
    20 permit icmp host 45.1.140.3 any log (80 matches)
    30 permit udp host 45.1.140.3 any log (27 matches)
    40 deny icmp host 45.1.140.1 any log (23 matches)
    50 deny tcp host 45.1.140.1 any log (4080 matches)
    60 deny udp host 45.1.140.1 any log (23 matches)
    70 deny ip any any log (8 matches)
C9300_TSTP1#
```

Step 5: Reset the counters in DUT and confirm the counter value is set to default.
Reset the accounting in DUT using command" sudo iptables -Z" and Confirm in DUT whether the counter values are set to default..

```
C9300_TSTP1#clear access-list counters TRAFFIC_FILTERING
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
C9300_TSTP1#
```

11.5.4 **Test Observations:** The counter is set to default when resetting the accounting

11.6 **Test Case Number: 06**

11.6.1 **Test Case Name:** TC_PACKET_FILTERING_HEADER_VALUE_NETWORKLAYER

11.6.2 **Test Case Description:** To filter the incoming IP Packets on any IP interfaces at the Network layer of ISO/OSI Stack.

11.6.3 **Execution Steps:**

Step 1: Make sure the DUT is capable of configuring policies for Network interfaces, if the DUT supports go through the DUT documentation and assign the policies for the Selected host.
Configured policies in DUT to allow only ICMP traffic and TCP traffic from Host1.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 2: In DUT, configure the policy to Allow any protocol from any one network interface of DUT from host1**.**

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 3: Generate traffic from any hosts to DUT and Confirm whether the matching rules traffic is filtered in DUT.

In DUT, configure the policy to Allow host src IP 45.1.140.3 traffic from the host.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Generate ICMP traffic from Host to DUT.

```
C9300_SW2#ping 45.1.140.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.1.140.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Confirm that in DUT the configured rule traffic is filtered.

```
C9300_TSTP1#show logging | include TRAFFIC_FILTERING
Apr 17 10:40:52.472: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied udp 45.1.140.1(5353) -> 224.0.0.251(5353), 1 packet
Apr 17 10:42:50.025: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(33856) -> 185.125.190.96(80), 1 packet
Apr 17 10:42:51.051: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(48160) -> 91.189.91.96(80), 1 packet
Apr 17 10:42:52.074: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(54074) -> 185.125.190.49(80), 1 packet
Apr 17 10:42:53.098: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(58280) -> 185.125.190.18(80), 1 packet
Apr 17 10:42:54.123: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(52140) -> 185.125.190.17(80), 1 packet
Apr 17 10:42:55.147: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(35672) -> 91.189.91.98(80), 1 packet
Apr 17 10:42:56.170: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(37674) -> 185.125.190.98(80), 1 packet
Apr 17 10:42:57.194: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(53078) -> 91.189.91.97(80), 1 packet
Apr 17 10:42:58.218: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(60912) -> 91.189.91.49(80), 1 packet
Apr 17 10:42:59.243: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(33966) -> 185.125.190.48(80), 1 packet
Apr 17 10:43:00.266: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(52324) -> 185.125.190.97(80), 1 packet
Apr 17 10:44:46.578: %SEC-6-IPACCESSLOGDP: list TRAFFIC_FILTERING permitted icmp 45.1.140.3 -> 45.1.140.2 (8/0), 1 packet
Apr 17 10:46:00.068: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied udp 45.1.140.1(5353) -> 224.0.0.251(5353), 49 packets
Apr 17 10:47:50.017: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(33982) -> 185.125.190.49(80), 1 packet
Apr 17 10:47:51.083: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(43300) -> 91.189.91.96(80), 1 packet
Apr 17 10:47:52.106: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(52386) -> 185.125.190.18(80), 1 packet
Apr 17 10:47:53.131: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(58534) -> 91.189.91.97(80), 1 packet
Apr 17 10:47:54.155: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(39086) -> 185.125.190.17(80), 1 packet
Apr 17 10:47:55.179: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(43360) -> 91.189.91.48(80), 1 packet
Apr 17 10:47:56.203: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(45780) -> 91.189.91.98(80), 1 packet
Apr 17 10:47:57.226: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(54308) -> 185.125.190.97(80), 1 packet
Apr 17 10:47:58.251: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(54856) -> 185.125.190.48(80), 1 packet
Apr 17 10:47:59.274: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(36344) -> 91.189.91.49(80), 1 packet
Apr 17 10:48:00.067: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(60912) -> 91.189.91.49(80), 1 packet
Apr 17 10:48:00.067: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(33966) -> 185.125.190.48(80), 1 packet
Apr 17 10:48:15.628: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING permitted tcp 45.1.140.3(20481) -> 45.1.140.2(80), 1 packet
Apr 17 10:48:31.262: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING permitted tcp 45.1.140.3(31745) -> 45.1.140.2(23), 1 packet
Apr 17 10:49:13.049: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING permitted tcp 45.1.140.3(44545) -> 45.1.140.2(23), 1 packet
```

11.6.4 **Test Observations:** DUT receives the IP Packets on any IP interfaces and able to filter the Network layer traffic.

11.7 **Test Case Number: 07**

11.7.1 **Test Case Name:** TC_PACKET_FILTERING_HEADER_VALUE_TRANSPORTLAYER

11.7.2 **Test Case Description:** To filter the incoming IP Packets on any IP interfaces at the Transport layer of ISO/OSI Stack.

11.7.3 **Execution Steps:**

Step 1: Make sure the DUT is capable of configuring policies for Network interfaces, if the DUT supports go through the DUT documentation and assign the policies for the Selected host.

Configured policies in DUT to allow only ICMP traffic and TCP traffic from Host1.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 2: In DUT, configure the policy to Allow any protocol from any one network interface of DUT from host1**.**

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 3: Generate traffic from any hosts to DUT and Confirm whether the matching rules traffic is filtered in DUT.
In DUT, configure the policy to deny port 23 telnet for host1 45.1.140.3 traffic from the host.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    5 deny tcp host 45.1.140.3 any eq telnet log
    10 permit tcp host 45.1.140.3 any log (37 matches)
    20 permit icmp host 45.1.140.3 any log (32 matches)
    30 permit udp host 45.1.140.3 any log (4 matches)
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log (276 matches)
    60 deny udp host 45.1.140.1 any log (1 match)
```

Generate port 23 traffic from Host to DUT.

```
C9300_SW2#telnet 45.1.140.2
Trying 45.1.140.2 ...
% Destination unreachable; gateway or host down
```

Confirm that in DUT the configured rule traffic is filtered.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    5 deny tcp host 45.1.140.3 any eq telnet log (14 matches)
    10 permit tcp host 45.1.140.3 any log (37 matches)
    20 permit icmp host 45.1.140.3 any log (42 matches)
    30 permit udp host 45.1.140.3 any log (4 matches)
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log (276 matches)
    60 deny udp host 45.1.140.1 any log (1 match)
```

```
May  6 23:28:40.541: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(40480) -> 185.125.190.17(80), 1 packet
May  6 23:28:41.566: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(45620) -> 185.125.190.98(80), 1 packet
May  6 23:28:42.589: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(44614) -> 91.189.91.49(80), 1 packet
May  6 23:33:26.523: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.3(30215) -> 45.1.140.2(23), 20 packets
May  6 23:33:32.326: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(41668) -> 91.189.91.97(80), 1 packet
May  6 23:33:33.340: %SEC-6-IPACCESSLOGP: list TRAFFIC_FILTERING denied tcp 45.1.140.1(34546) -> 91.189.91.49(80), 1 packet
```

11.7.4 **Test Observations:** DUT receives the IP Packets on any IP interfaces and able to filter the Transport layer traffic.

11.8 **Test Case Number: 08**

11.8.1 **Test Case Name:** TC_PACKET_FILTERING_ENABLE_RULE

11.8.2 **Test Case Description:** The DUT shall provide a mechanism to enable each defined rule.

11.8.3 **Execution Steps:**

Step 1: Make sure the DUT is capable of configuring rules for Network interfaces, if the DUT supports go through the DUT documentation and assign the rules for the Selected host.
In DUT configure policy to Allow ICMP traffic from the host.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 2: In DUT, define the rule for any one network interface.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 3: Enable the rule on any one interface.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 4: Check the rule-enabled network interface configuration to verify whether the rule is enabled or not.

Before enabling the rule in the DUT interface confirm whether the host can able to generate ICMP traffic to the DUT.

```
csr@csr-virtual-machine:~$ ping 45.1.140.2
PING 45.1.140.2 (45.1.140.2) 56(84) bytes of data.
64 bytes from 45.1.140.2: icmp_seq=1 ttl=254 time=0.958 ms
64 bytes from 45.1.140.2: icmp_seq=2 ttl=254 time=1.29 ms
64 bytes from 45.1.140.2: icmp_seq=3 ttl=254 time=1.32 ms
64 bytes from 45.1.140.2: icmp_seq=4 ttl=254 time=1.12 ms
^C
--- 45.1.140.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3067ms
rtt min/avg/max/mdev = 0.958/1.169/1.316/0.143 ms
csr@csr-virtual-machine:~$
```

Confirm whether the rule is enabled in the DUT network interface

```
C9300_TSTP1(config)#interface Vlan2141
C9300_TSTP1(config-if)#ip access-group TRAFFIC_FILTERING in
C9300_TSTP1(config-if)#exit
C9300_TSTP1(config)#
```

Host is denied after the rule is enabled

```
csr@csr-virtual-machine:~$ ping 45.1.140.2
PING 45.1.140.2 (45.1.140.2) 56(84) bytes of data.
From 45.1.140.2 icmp_seq=1 Packet filtered
From 45.1.140.2 icmp_seq=2 Packet filtered
From 45.1.140.2 icmp_seq=3 Packet filtered
From 45.1.140.2 icmp_seq=4 Packet filtered
^C
--- 45.1.140.2 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3063ms

csr@csr-virtual-machine:~$
```

11.8.4 **Test Observations:** Network Interface applies the configured rules when the rule is enabled.

11.9 Test Case Number: 09

11.9.1 Test Case Name: TC_PACKET_FILTERING_DISABLE_RULE

11.9.2 Test Case Description:The DUT shall provide a mechanism to disable each defined rule.

11.9.3 Execution Steps:

Step 1: Make sure the DUT is capable of configuring rules for Network interfaces, if the DUT supports go through the DUT documentation and assign the rules for the Selected host.

In DUT configure policy to Allow TCP traffic from the host.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 2: In DUT, define the rule for any one network interface.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 3: Enable the rule on any one interface.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Step 4: Check the rule-enabled network interface configuration to verify whether the rule is enabled or not.

In DUT configure policy to allow ICMP traffic from the host.

```
C9300_TSTP1#show access-lists TRAFFIC_FILTERING
Extended IP access list TRAFFIC_FILTERING
    10 permit tcp host 45.1.140.3 any log
    20 permit icmp host 45.1.140.3 any log
    30 permit udp host 45.1.140.3 any log
    40 deny icmp host 45.1.140.1 any log
    50 deny tcp host 45.1.140.1 any log
    60 deny udp host 45.1.140.1 any log
    70 deny ip any any log
```

Before disabling the rule in the DUT interface, confirm whether the host can able to generate ICMP traffic to the DUT.

```
csr@csr-virtual-machine:~$ ping 45.1.140.2
PING 45.1.140.2 (45.1.140.2) 56(84) bytes of data.
From 45.1.140.2 icmp_seq=1 Packet filtered
From 45.1.140.2 icmp_seq=2 Packet filtered
From 45.1.140.2 icmp_seq=3 Packet filtered
From 45.1.140.2 icmp_seq=4 Packet filtered
^C
--- 45.1.140.2 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3063ms

csr@csr-virtual-machine:~$
```

Step 5: Disable the rule on rule configured interface.
Disable the rule in the DUT network interface.

```
C9300_TSTP1(config)#interface vlan2141
C9300_TSTP1(config-if)#no ip
C9300_TSTP1(config-if)#no ip ac
C9300_TSTP1(config-if)#no ip acce
C9300_TSTP1(config-if)#no ip access-g
C9300_TSTP1(config-if)#no ip access-group TRAFFIC_FILTERING in
C9300_TSTP1(config-if)#exit
C9300_TSTP1(config)#
```

Step 6: Check the rule-disabled network interface configuration to verify whether the rule is disabled or not.
After disabling the rule in DUT cross check whether the host can able to generate TCP traffic to DUT.

```
csr@csr-virtual-machine:~$ ping 45.1.140.2
PING 45.1.140.2 (45.1.140.2) 56(84) bytes of data.
64 bytes from 45.1.140.2: icmp_seq=1 ttl=254 time=0.958 ms
64 bytes from 45.1.140.2: icmp_seq=2 ttl=254 time=1.29 ms
64 bytes from 45.1.140.2: icmp_seq=3 ttl=254 time=1.32 ms
64 bytes from 45.1.140.2: icmp_seq=4 ttl=254 time=1.12 ms
^C
--- 45.1.140.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3067ms
rtt min/avg/max/mdev = 0.958/1.169/1.316/0.143 ms
csr@csr-virtual-machine:~$
```

11.9.4 **Test Observations:** DUT removed the configured rules when the rule is disabled.

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_PACKET_FILTERING_NETWORKLAYER	PASS	DUT receives the configured traffic and answers back to Host 1.
2	TC_PACKET_FILTERING_TRANSPORTLAYER	PASS	DUT deny the configured traffic from Host 2 and doesn't answer back. DUT deny all other traffic from host1 and host2.
3	TC_PACKET_FILTERING_RULE_LOGGING	PASS	DUT drops the configured traffic and logging the traffic from Host 1 and Host 2.
4	TC_PACKET_FILTERING_ACCOUNTING	PASS	The matching messages are accounted and the counter for the rule is incremented.
5	TC_PACKET_FILTERING_RESET_ACCOUNTING	PASS	The counter is set to default when resetting the accounting
6	TC_PACKET_FILTERING_HEADER_VALUE_NETWORKLAYER	PASS	DUT receives the IP Packets on any IP interfaces and able to filter the Network layer traffic.
7	TC_PACKET_FILTERING_HEADER_VALUE_TRANSPORTLAYER	PASS	DUT receives the IP Packets on any IP interfaces and able to filter the Transport layer traffic.
8	TC_PACKET_FILTERING_ENABLE_RULE	PASS	Network Interface applies the configured rules when the rule is enabled.
9	TC_PACKET_FILTERING_DISABLE_RULE	PASS	DUT removed the configured rules when the rule is disabled.

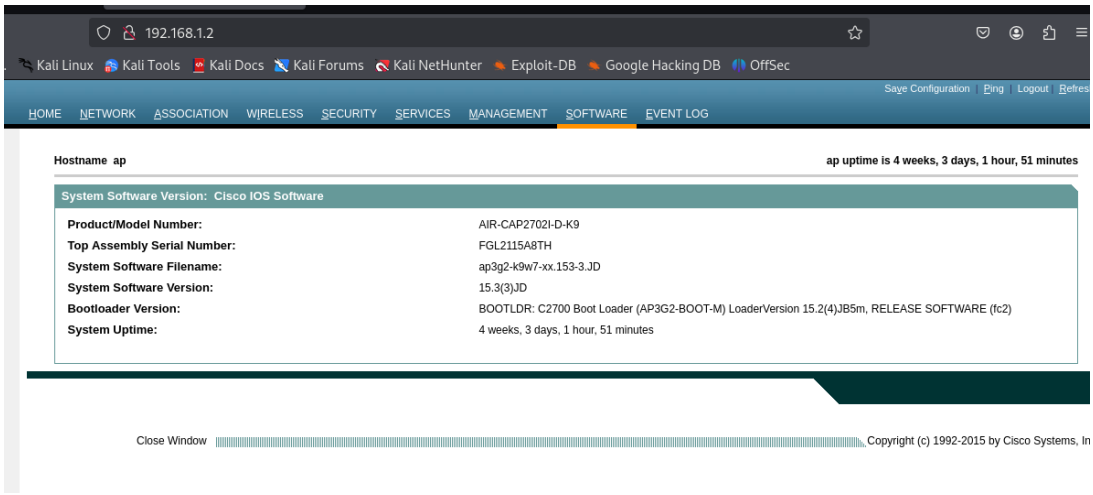
2.7.2 Traffic Separation

<DUT Details: > WiFi CPE
<DUT Software Version:> cisco
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 2.0.0
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name> Section 7: Network Services**
2. **<Security Requirement No & Name > 2.7.2 Traffic separation**
3. **<Requirement Description: >** (applicable for both split configuration and cloud hosted/managed configuration) The Network product shall support physical or logical separation of O&M and control plane traffic. See RFC 3871 [3] for further information.

[Ref: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.5.1]

4. **DUT Confirmation Details**:



5. **<u>DUT Configuration:</u>**

<u>ACL Configurations-</u>

ip access-list extended BLOCK_OAM

deny ip any host <OAM IP>

permit ip any any

<u>exit</u>

Bind ACL with corresponding interface:

ip access-group BLOCK_OAM in

ip access-list extended BLOCK_CONTROL

deny ip any host <CONTROL IP>

permit ip any any

<u>exit</u>

Bind ACL with corresponding interface:

ip access-group BLOCK_CONTROL in

6. **Preconditions**

NOTE: This test applies if the network product is meant to handle both O&M and control plane traffic.

The network product has at least one separate (logical) interface dedicated to O&M traffic and at least one (logical) interface for control plane traffic. Network products for which the test applies and that fail to meet this precondition fail the test by definition.

7. **Test Objective:-** To verify if traffic separation of DUT's O&M and control plane traffic is supported.

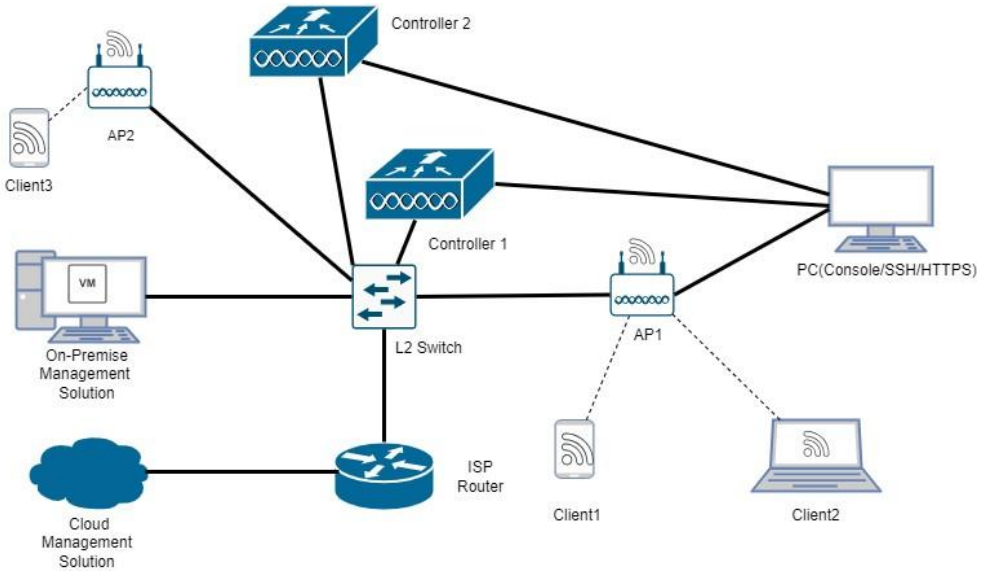
8. **Test Plan**

8.1. Number of Test Scenarios:

8.1.1 TC_PHYSICAL_SEPARATION (OPTIONAL)
8.1.2 TC_LOGICAL_BLOCK_OAM_INTERFACE_TO_CONTROL_PLANE
8.1.3 TC_LOGICAL_BLOCK _CONTROL_PLANE_TO_OAM_INTERFACE

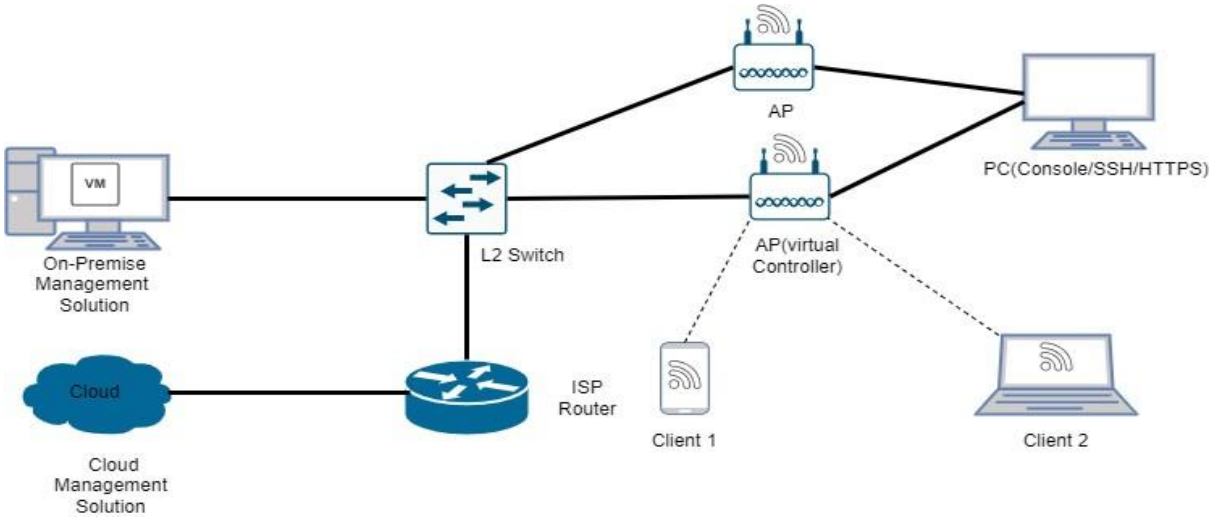
8.2. Test Bed Diagram

AP + Controller mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

8.3. Tools Required

CLI

8.4. Test Execution Step

- The tester checks whether the network product refuses O&M traffic on all interfaces meant for control plane traffic.
- The tester checks whether the network product refuses control plane traffic on all O&M interfaces.

9. **Expected Results for Pass:** The Device Under Test (DUT) shall correctly perform traffic filtering between the Management plane and Control plane, ensuring only authorized traffic is allowed between OAM, Management, and Control plane interfaces as per ITSAR requirement.

10. **Expected Format of Evidence:** Screenshots of Terminal (ACL Logs, pcap in case of VLAN based separation)

11. **Test Execution:**

11.1 Test Case Number: 01

Note: This case is applicable only if DUT supports physical separation

11.1.1 **Test Case Name:** TC_PHYSICAL_SEPARATION (OPTIONAL)

11.1.2 **Test Case Description:** To verify physical separation between OAM (Operations, Administration & Management) and Control Plane Interfaces.

11.1.3 **Execution Steps:** Tester should identify physical interfaces used for management (OAM) and control plane functions on the DUT and attach picture of DUT highlighting interface separation.

11.1.4 **Test Observations:** Tester should verify physical separation in DUT.

11.2 Test Case Number: 02

11.2.1 **Test Case Name:** TC_LOGICAL_BLOCK_OAM_TRAFFIC _TO_CONTROL_PLANE

11.2.2 **Test Case Description:** Verify the logical separation between the OAM

(Operations, Administration & Management) interface and the Control Plane interface by ensuring that:

- Traffic originating from the OAM interface cannot access or reach the Control Plane.
- Traffic intended for the Control Plane is correctly delivered without interference.

11.2.3 **Execution Steps:**

- Verify the appropriate ACL are applied on interface.

[NOTE: VLAN also can be considered as a traffic separation mechanism. In that case Wireshark trace can be used as evidence.]

- Tester will generate traffic from OAM interface to control plane interface and check the traffic filtering.

11.2.4 **Test Observations:** Tester shall verify that traffic originating from OAM plane to control plane is rejected by DUT.

11.3 Test Case Number: 03

11.3.1 **Test Case Name:**
TC_LOGICAL_BLOCK _CONTROL_PLANE_TRAFFIC_TO_OAM_INTERFACE

11.3.2 **Test Case Description:** Verify the logical separation between the Control Plane interface and the OAM (Operations, Administration & Management) interface by ensuring that:

- Traffic originating from the Control Plane cannot access or interact with OAM plane functions.
- Traffic intended for the Management Plane is correctly transmitted and delivered

11.3.3 **Execution Steps:**

- Verify the appropriate ACL are applied on interface.

[NOTE: VLAN also can be considered as a traffic separation mechanism. In that case Wireshark trace can be used as evidence.]

- Tester will generate traffic from control interface to OAM plane interface and check the traffic filtering.

11.3.4 **Test Observations:** Tester shall verify that traffic originating from control plane to OAM plane is rejected by DUT.

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_PHYSICAL_SEPARATION (OPTIONAL)		Procedure Explained
2	TC_LOGICAL_BLOCK_OAM_INTERFACE_TO_CONTROL_PLANE		Procedure Explained
3	TC_LOGICAL_BLOCK_CONTROL_INTERFACE_TO_OAM_PLANE		Procedure Explained

2.7.3 TSTP for Traffic Protection – Anti-Spoofing

<DUT Details: > WiFi CPE
<DUT Software Version:> cisco 10.5.2.0
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 2.0.0
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 2.7: Network Services
2. **<Security Requirement No & Name >** 2.7.3 Traffic Protection – Anti-Spoofing
3. **<Requirement Description: >**
   Wi-Fi CPE shall not process IP packets if their source address is not reachable via the incoming interface. Implementation example: Use of "Reverse Path Filter" (RPF) provides this function.

   [Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.3.3.1.1]

4. **DUT Confirmation Details**: This section involves information about DUT like software/firmware version, Hardware version model.

```
ap#show version
Cisco IOS Software, C2700 Software (AP3G2-K9W7-M), Version 15.3(3)JD, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Fri 29-Jul-16 03:58 by prod_rel_team

ROM: Bootstrap program is C2700 boot loader
BOOTLDR: C2700 Boot Loader (AP3G2-BOOT-M) LoaderVersion 15.2(4)JB5m, RELEASE SOFTWARE (fc2)

ap uptime is 6 minutes
System returned to ROM by power-on
System image file is "flash:/ap3g2-k9w7-mx.153-3.JD/ap3g2-k9w7-xx.153-3.JD"
Last reload reason:



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco AIR-SAP2702I-D-K9 (PowerPC) processor (revision A0) with 376814K/134656K bytes of memory.
Processor board ID FGL2115A8SZ
PowerPC CPU at 800Mhz, revision number 0x2151
Last reset from power-on
1 Gigabit Ethernet interface
2 802.11 Radios

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 70:DB:98:B6:0F:98
Part Number                          : 73-15824-04
PCB Serial Number                    : FOC211355R7
Top Assembly Part Number             : 800-41174-04
 --More--
```

```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco AIR-SAP2702I-D-K9 (PowerPC) processor (revision A0) with 376814K/134656K bytes of memory.
Processor board ID FGL2115A8SZ
PowerPC CPU at 800Mhz, revision number 0x2151
Last reset from power-on
1 Gigabit Ethernet interface
2 802.11 Radios

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 70:DB:98:B6:0F:98
Part Number                          : 73-15824-04
PCB Serial Number                    : FOC211355R7
Top Assembly Part Number             : 800-41174-04
Top Assembly Serial Number           : FGL2115A8SZ
Top Revision Number                  : A0
Product/Model Number                 : AIR-CAP2702I-D-K9



Configuration register is 0xF

ap#
```

The below screenshot shows the available interface details of DUT

```
ap#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
BVI1                       192.168.1.2     YES NVRAM  up                    up
Dot11Radio0                unassigned      YES NVRAM  administratively down down
Dot11Radio1                unassigned      YES NVRAM  administratively down down
GigabitEthernet0           unassigned      YES NVRAM  up                    up
GigabitEthernet1           unassigned      YES NVRAM  administratively down down
ap#
```

5. **DUT Configuration:**

```
File  Actions  Edit  View  Help
nccs@NCCS: ~ ×  nccs@NCCS: ~ ×  nccs@NCCS: ~ ×  nccs@NCCS: ~ ×
ap#show conf
ap#show configuration
Using 3318 out of 32768 bytes
!
! Last configuration change at 22:16:03 UTC Fri Mar 26 1993 by authorized_user
version 15.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
logging userinfo
logging buffered 51200
logging rate-limit console 9
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login webauth group radius
aaa authorization exec default local
!
!
!
!
!
aaa session-id common
no ip source-route
no ip cef
ip domain name nccs
!
!
!
!
dot11 pause-time 100
dot11 syslog
!

ap#
```

```
ap(config)#do show ip
ap(config)#do show ip in
ap(config)#do show ip int
ap(config)#do show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
BVI1                       192.168.1.2     YES NVRAM  up                    up
Dot11Radio0                unassigned      YES NVRAM  administratively down down
Dot11Radio1                unassigned      YES NVRAM  administratively down down
GigabitEthernet0           192.168.2.100   YES manual up                    up
GigabitEthernet1           192.168.2.2     YES manual up                    down
ap(config)#
```

6. **Preconditions**
   - Tester should have privileged access to the DUT for RPF configuration and verification.
   - WiFi CPE should have atleast one layer3 interface (for eg - management)

7. **Test Objective**:

- To verify that the network product provides anti-spoofing function that is, before a packet is processed, the network product checks whether the source IP of the received packet is reachable through the interface it comes in.
- To verify that if the received packet source address is not routable through the interface on which it comes, then the network product drops this packet.

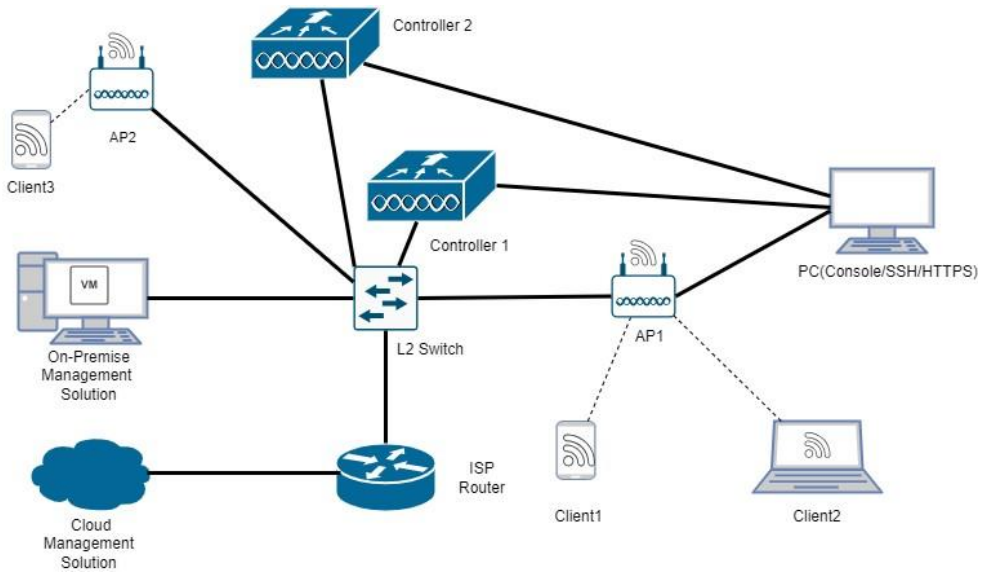
8. **Test Plan:**

8.1 Number of Test Scenarios:

8.1.1. TC_IP_SPOOFING_MITIGATION_VERIFY_RPF_ENABLED/DISABLED.
8.1.2. TC_ ANTI_SPOOFING_WITHOUT_RPF

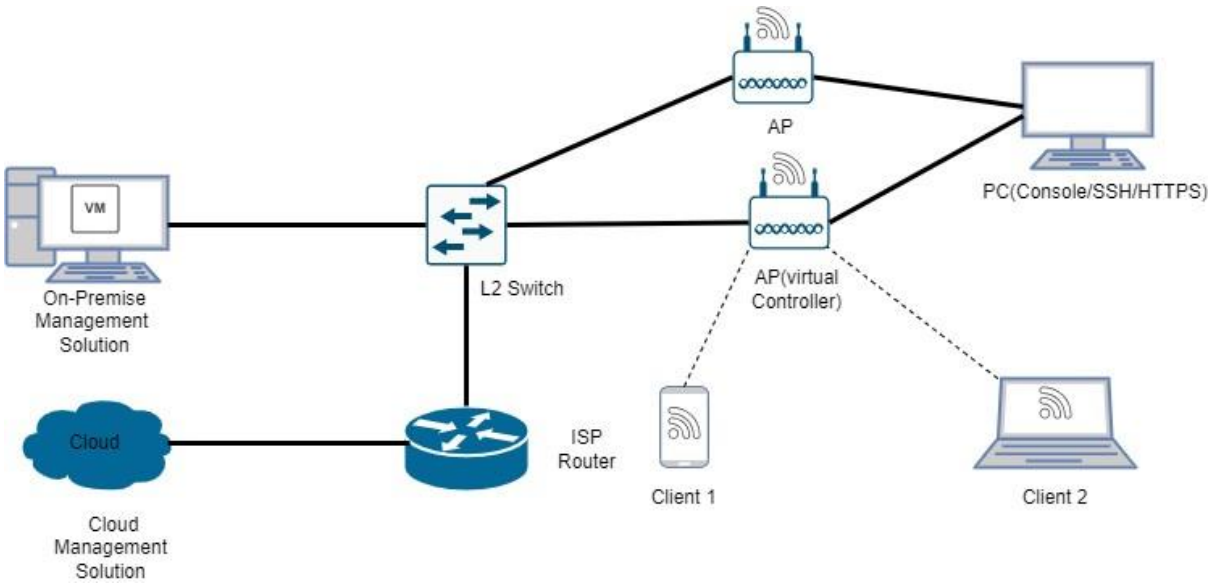
8.2 Test Bed Diagram

AP + Controller mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

.2 Tools Required

- CLI,
- Scapy,
- Wireshark

.3 Test Execution Steps:

- Tester should check for the RPF functionality in the DUT. If this feature is enabled then tester must verify enabled RPF options.
- If RPF feature is not available with the DUT then tester should alternate configuration metods inside DUT (eg- ACL) to identify the spoofed packet and check for DUT's response.

9. **Expected Results for Pass:**

- **Case 1:** The DUT supports RPF feature.
- **Case 2:** If the DUT does not support RPF then tester should check for alternate anti-spoofing mechanism (eg - ACL)

10. **Expected Format of Evidence:** A testing report provided by the testing agency which will consist of the following information:
    - The user settings and configurations
    - PCAP files
    - Log file if available
    - Test result (Passed or not)
11. **Test Execution:**

11.1 Test Case Number: 01

11.1.1 **Test Case Name:** TC_ ANTI_SPOOFING_WITH_RPF

11.1.2 **Test Case Description:**

11.1.3 **Execution Steps:**

- Detect whether RPF is configurable.

Command: *show running-config | include ip verify unicast.*

OR

- Tester can verify RPF functionality based on the options which are displayed as output of the above command:

  - *ip verify unicast source reachable-via rx → strict mode (option 2).*
  - *ip verify unicast source reachable-via any → loose mode (option 1).*
  - *None → disabled (option 0).*

11.1.4 **Test Observations:** Tester should verify the presence of RPF functionality.

11.2 **Test Case Number:** 02

11.2.1 **Test Case Name:** TC_ ANTI_SPOOFING_WITHOUT_RPF

11.2.2 **Test Case Description:**

11.2.3 **Execution Steps:**

- If RPF is not present then tester needs to configure ACL and **simulate a scenario where spoofed packets** are sent to DUT and check if device processes/drops them.
- Use **Scapy** to send packets with **invalid source IPs** via a specific interface.

Commands:

- sudo python3 -c "from scapy.all import *; send(IP(src=<'spoofed src IP>',dst='<DUT IP>')/TCP(sport=12345,dport=22,flags='S'),count=5,iface='eth0') "
- sudo python3 -c "from scapy.all import *; send(IP(src='<spoofed src IP >',dst=<DUT IP>')/ICMP(),count=3,iface='eth0')".

- Observe the response of the DUT that whether the DUT forwards/respond or drops the packet. Tester can verify this using any packet capturing tools.

11.2.4 **Test Observations:** Tester should verify the response of DUT when encountered with spoofed packet.

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_ ANTI_SPOOFING_WITH_RPF		Procedure Explained
2	TC_ ANTI_SPOOFING_WITHOUT_RPF		Procedure Explained

Section 1.8: Attack Prevention Mechanism

1.8.1 Excessive Overload Protection

<DUT Details: > Wi-Fi CPE
<DUT Software Version:> 8.10.183.0
<Digest Hash of OS> Hash of OS required
<Digest Hash of Configuration> Hash of configuration required.
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPE
<ITSAR Version No:> ITSAR402122401 and Version: 1.0.1
<OEM Supplied Document list: > OEM Supplied Document list required

1. **<ITSAR Section No & Name>** Section 1.8: Attack Prevention Mechanism
2. **<Security Requirement No & Name >** 1.8.1 Excessive Overload Protection
3. **<Requirement Description: >** Wi-Fi CPE shall act in a predictable way if an overload situation cannot be prevented. WiFi CPE shall be built in such a way that it can react to an overload situation in a controlled way. However, it is possible that a situation happens where the security measures are no longer sufficient. In such a case it shall be ensured that Wi-Fi CPE cannot reach an undefined and thus potentially insecure, state. In an extreme case this means that a controlled system shutdown is preferable to uncontrolled failure of the security functions and thus loss of system protection. OEM shall provide a technical description of the Wi-Fi CPE 's overload control mechanisms. (especially whether these mechanisms rely on cooperation of other network elements)

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.3]

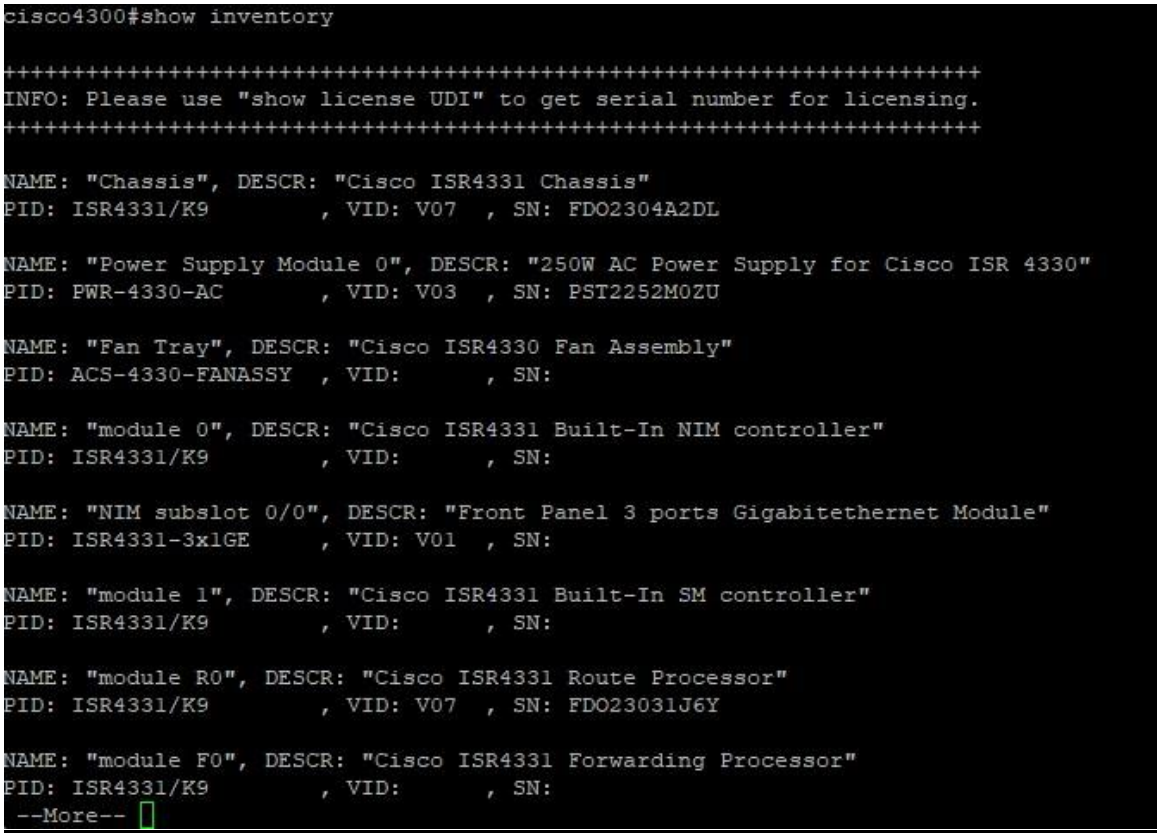
4. **DUT Confirmation Details**:
    - Use the command line interface to get details of the machine on which test is conducted.
    - Use command: show interface summary to get Interfaces details Use command to get Application No/Version No & Kernel Info Verification of DUT by running command: show version on CLI.
    - Use command for show interface: Sh version

```
cisco4300#show version
Cisco IOS XE Software, Version 17.06.08a
Cisco IOS Software [Bengaluru], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Version 17.6.8a, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2024 by Cisco Systems, Inc.
Compiled Mon 14-Oct-24 08:01 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2024 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: (c)

cisco4300 uptime is 1 hour, 34 minutes
Uptime for this control processor is 1 hour, 36 minutes
 --More--
```

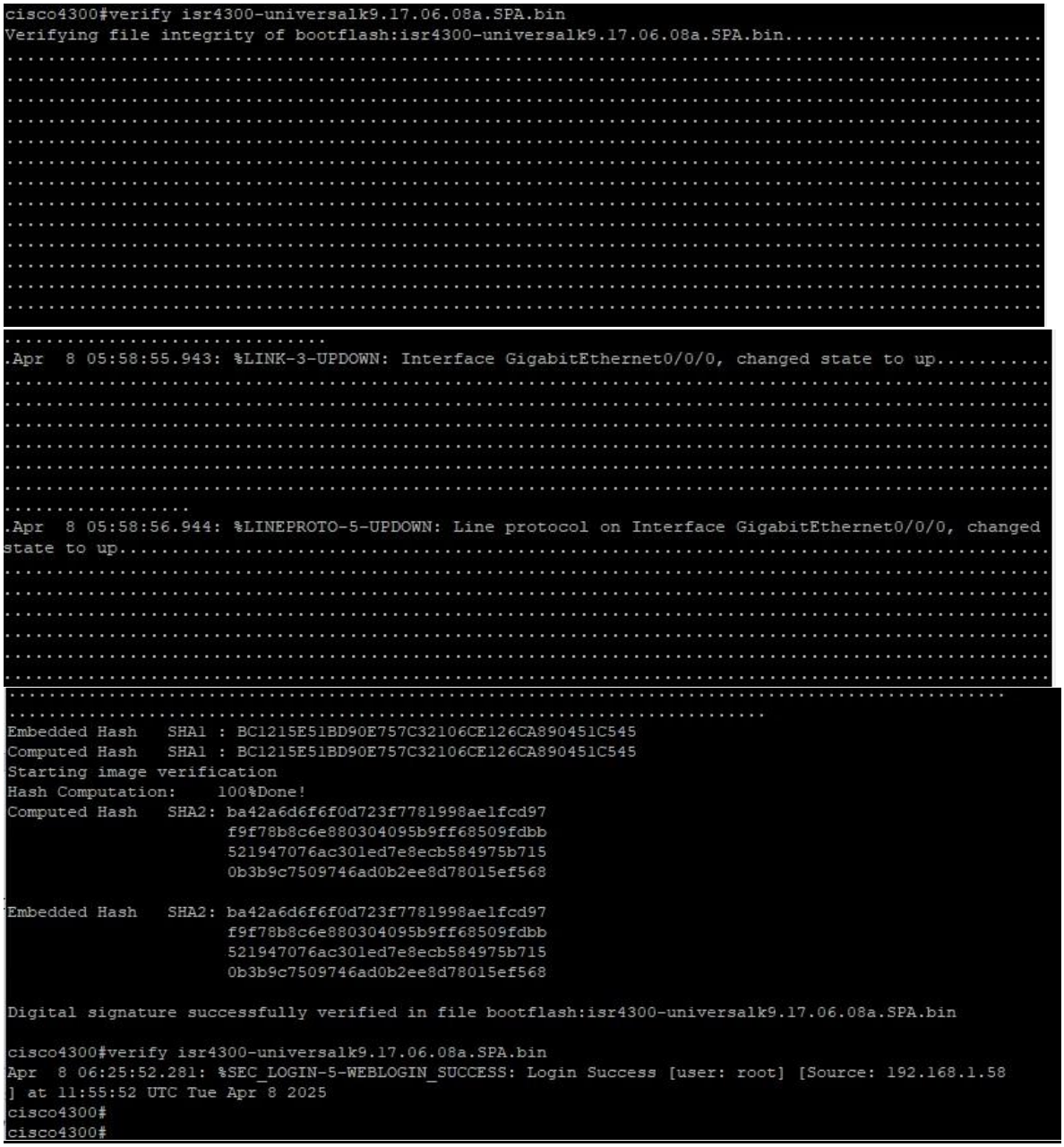
- Use command for show interface: Sh int summary

```
cisco4300#show interfaces summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface                   IHQ       IQD       OHQ       OQD      RXBS      RXPS
    TXBS      TXPS      TRTL
------------------------------------------------------------------------------------
---------------------------
* GigabitEthernet0/0/0          0         0         0         0     13000         3
       0         0         0
  GigabitEthernet0/0/1          0         0         0         0         0         0
       0         0         0
  GigabitEthernet0/0/2          0         0         0         0         0         0
       0         0         0
  GigabitEthernet0              0         0         0         0         0         0
       0         0         0
cisco4300#
cisco4300#
```

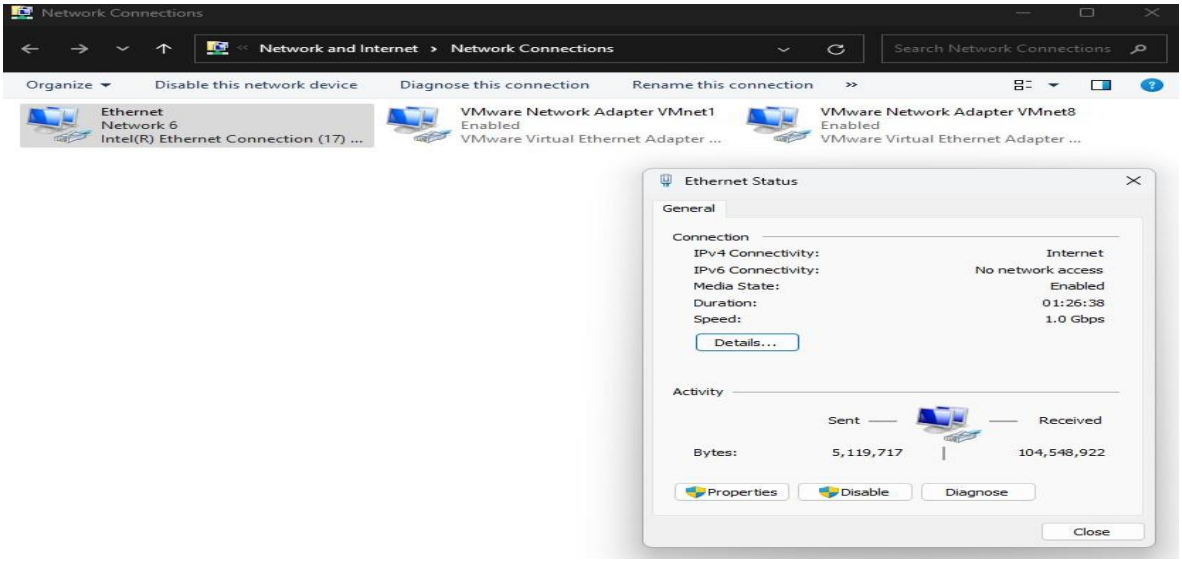
Command: show inventory



Verification of Integrity on DUT by running command verify software authentication on CLI verify: isr4300-universalk9.17.06.08a.SPA.bin



5. **DUT Configuration**: System Ethernet interface capacity is 1.0 Gbps



DUT Maximum capacity of interface eg. GigabitEthernet1 is showing below:

6. **Preconditions:**
   - A document which provides a detailed technical description of the overload control mechanisms.
   - Test results from a test execution phase of overload control mechanism testing.

7. **Test Objective/ Purpose:** Verify that the network product:
   - has a detailed technical description of the overload control mechanisms used to deal with overload scenarios;
   - has test results verifying the operation of the overload control mechanisms.
   - To validate the DUT (router's) performance and overload protection mechanisms against ICMP flooding, TCP SYN/RST flooding, HTTP application overloading, and maximum capacity throughput testing using iperf.

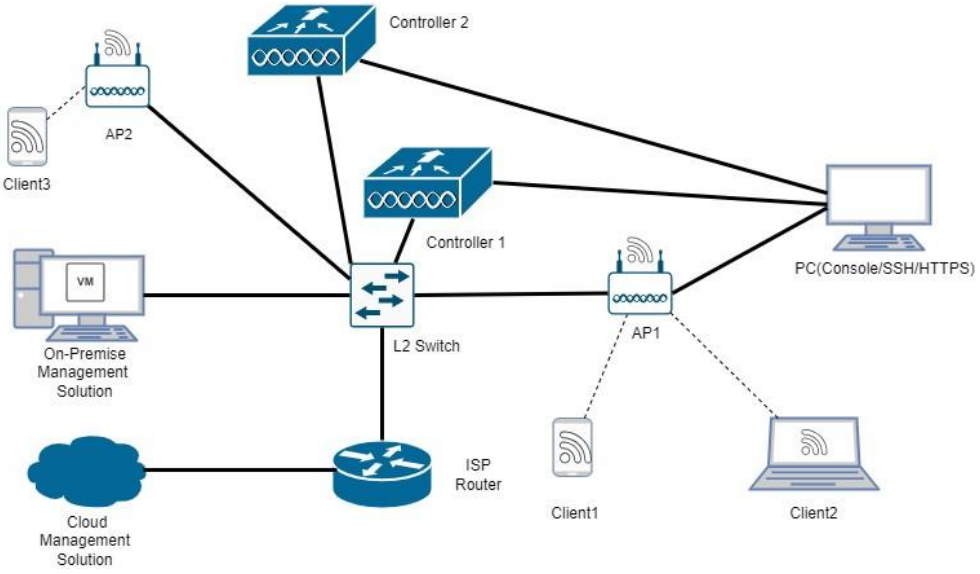
8. **Test Plan:**

8.1 Number of Test Scenarios: 5

8.1.1 TC_ICMP_FLOODING
8.1.2 TC_TCP_SYN_RST_FLOODING
8.1.3 TC_ Throughput Testing Using iperf
8.1.4 TC_HTTP_APPLICATION_OVERLOADING_TRAFFIC
8.1.5 TC_TRAFFIC_GENERATOR

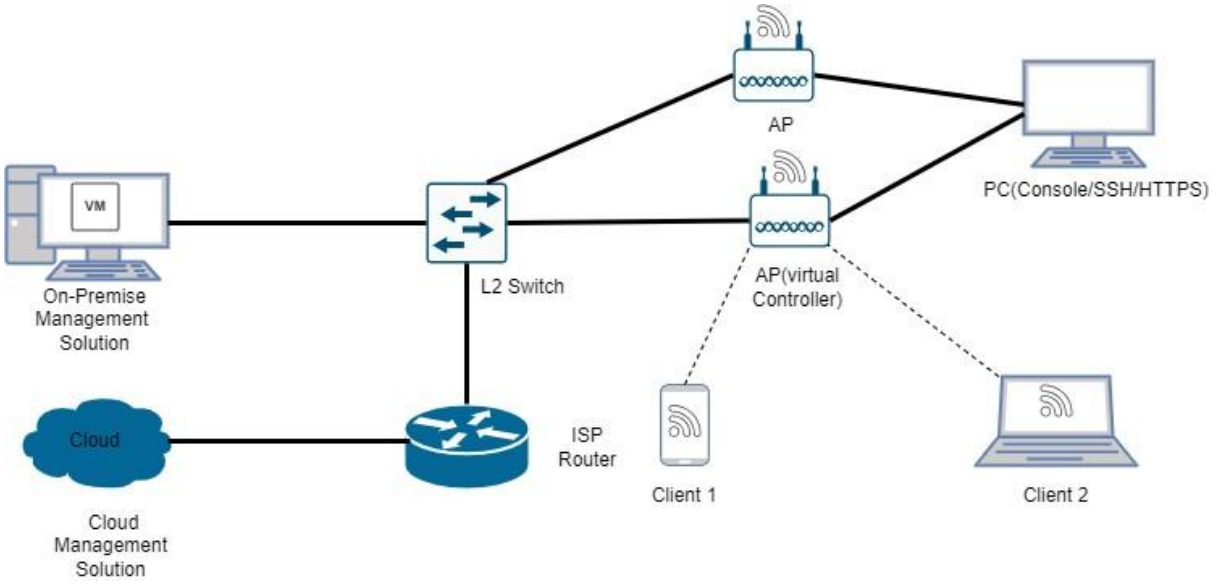
8.2 Testbed Diagram:

AP + Controller mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

8.3 Tools required:

- Traffic Generation: hping3, iperf, Apache Benchmark (ab), slowloris. § Packet Capture and Analysis: Wireshark § VeEX traffic generator.
- Router Monitoring: CLI commands (show processes cpu, show interface Gig0/0/0)

8.4 Test Execution Steps: The tester verifies that there is:

- A technical description providing a high-level overview of the overload control design.
- An overview of the types of overload scenarios that the network product overload control mechanisms are expected to handle.
- An overview of the overload control thresholds that the network product uses to trigger overload control mechanisms.
- Description of the types of attacks that may cause an overload to the network product and how these are handled.
- A description of how the network product discards or handles input during various overload situations including excessive overloads. i.e. where the overload is significantly greater than the thresholds where overload detection is triggered.
- A description of how the network product security functions operate and perform during overload.
- A description of how the network product shuts down or performs or takes other abatement or corrective actions during excessive overload conditions.

The tester verifies that the test results:

- Contain details of the overload conditions used in the test execution that are consistent with the technical description document.
- Describe test procedures used to verify the overload control mechanisms.
- Contain data which demonstrates/indicates that the overload control mechanisms described in the technical description document have been implemented.
- Contain details of the test set-up including the mechanisms for creating the overload. Where simulators and/or scripts are used to artificially create a load then details of these should also be included

9. **Expected Results:**

- A technical description provides a high-level overview of the overload control design.
- An overview of the types of overload scenarios and overload control thresholds that are considered.
- Description on the types of attacks that may cause an overload to the system and how these are handled.
- A description of how the network product discards or handles input during various overload situations.
- Describes if or how the network product security functions operate and perform during overload.
- If parts of the system shutdown or take other abatement or corrective actions these should be described.

Note: If some of the items listed above are not applicable to a network product then, in those cases, it should be clarified by the vendor why these items are not applicable.

The test results should:

- Contain details of the overload conditions used in the test execution that are consistent with the technical description document.
- Describe the test procedures used to verify the overload control mechanisms.
- Contain data which demonstrates/indicates that the overload control mechanisms described in the technical description document have been implemented.
- Contain details of the test set-up including the mechanisms for creating the overload.

10. **Expected Format of Evidence:**
    - **Wireshark Packet Captures:** Save capture files named after each scenario (ICMP_Flood.pcap, TCP_SYN_Flood.pcap, UDP_Flood.pcap, HTTP_Flood.pcap and traffic generate from VeEX traffic generator).
    - **CPU Utilization Logs:** Record output from show processes cpu every minute during tests.
    - **Traffic Rate Logs:** Record output from show interface GigabitEthernet0/0/0 every minute.
11. **Test Execution:**

11.1 **Test Case Number: 01**

11.1.1 **Test Case Name:** TC1_ICMP_FLOODING

11.1.2 **Test Case Description:** Generate ICMP flood traffic to test maximum bandwidth handling.

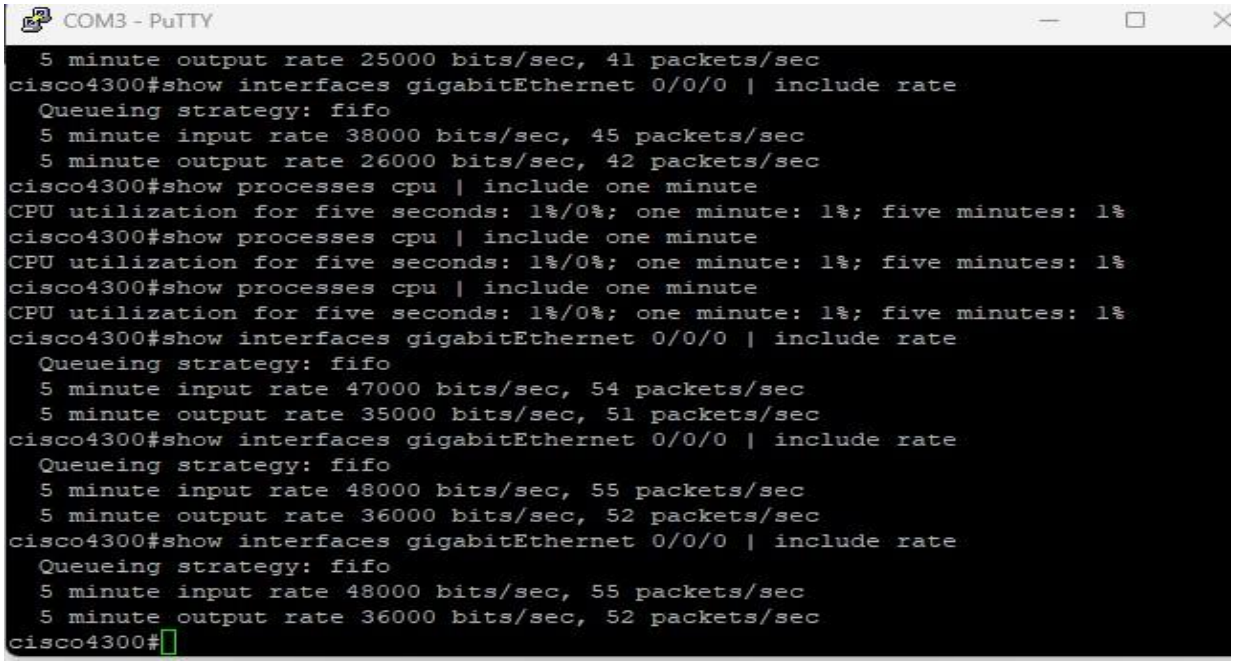
11.1.3 **Execution Steps:**

(i) Start Wireshark on the test system and set a capture filter for host 192.168.1.51.

(ii) Generate ICMP flood traffic using hping3:

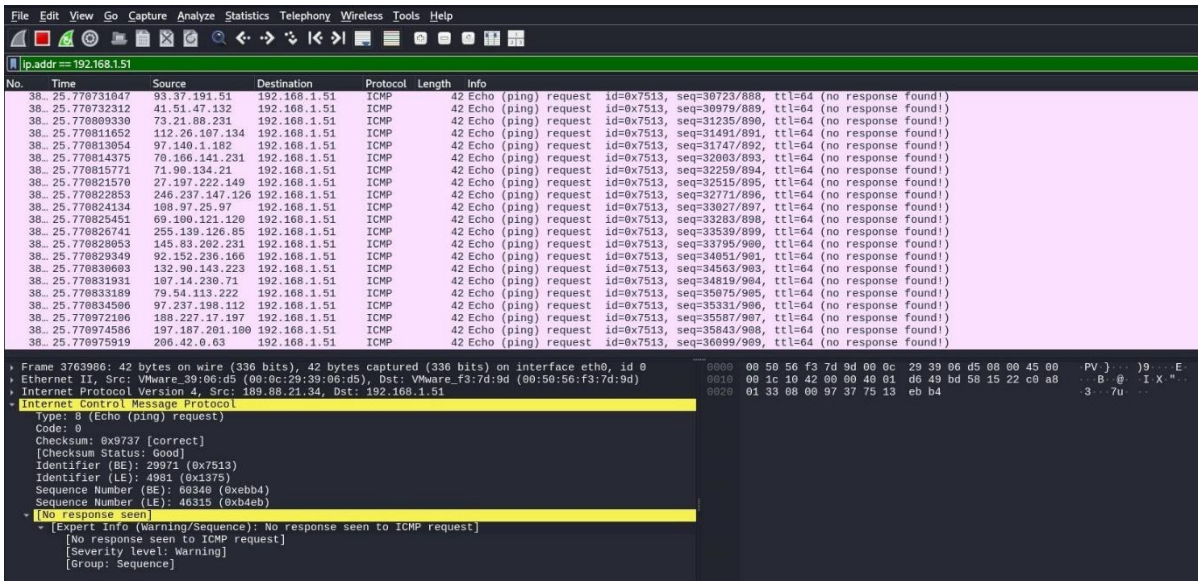
" sudo hping3 -I eth0 -1 192.168.1.51 --flood --rand-source"

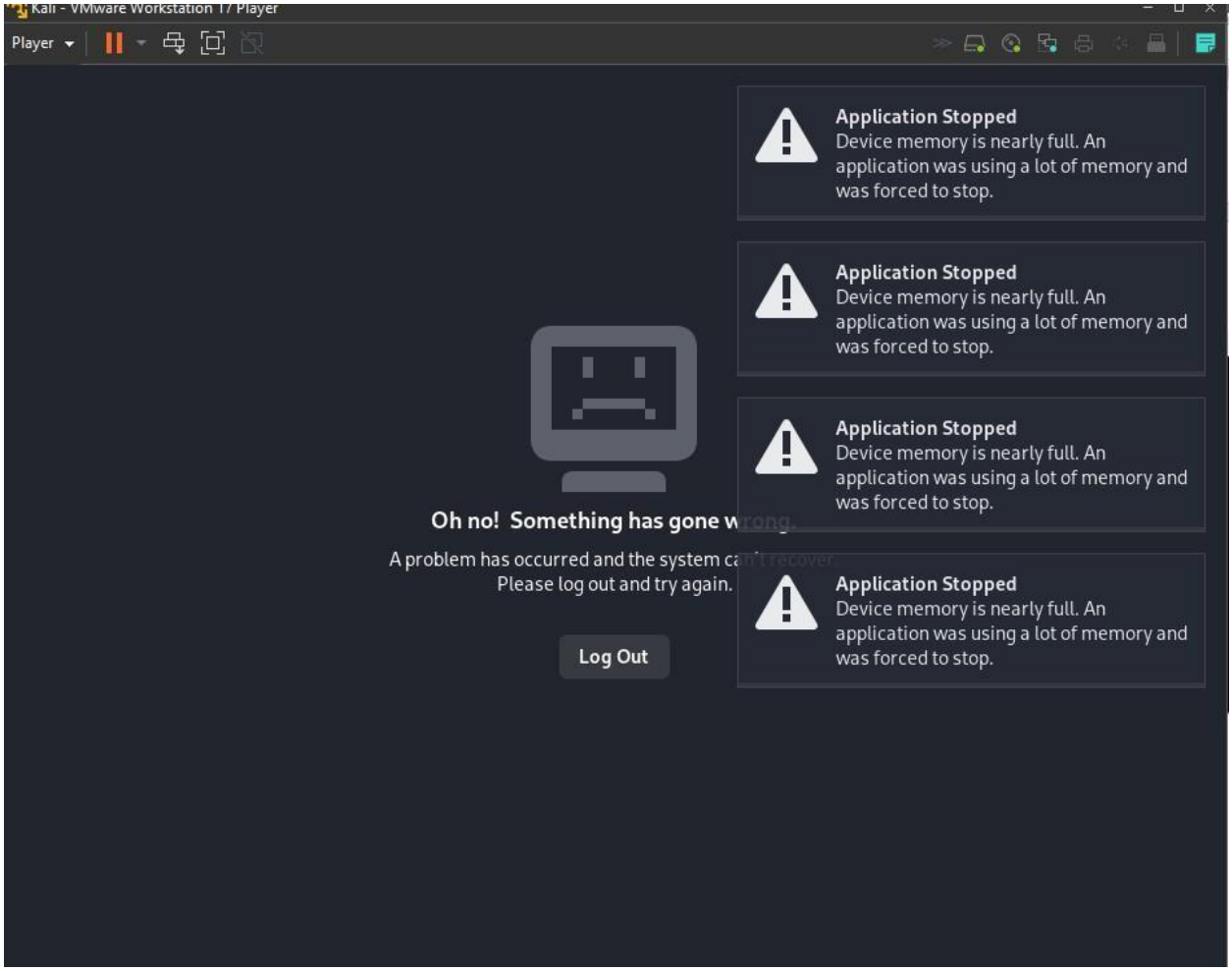
(iii) Monitor Router: On the Cisco 4300, run: "show processes cpu | include one minute" "show interface GigabitEthernet0/0/0 | include rate"



(iv) Stop after 10 minutes and save Wireshark capture.

Record observations: Check CPU usage, packet drops, and any syslog messages indicating overload protection activation.





11.1.4 **Test Observation:** Note the maximum CPU utilization observed during each test.

11.1.5 **Evidence Provided:** Screenshots of testing steps and Wireshark pcap files.

11.2 Test Case Number: 02

11.2.1 **Test Case Name:** TC2_TCP_SYN_RST_FLOODING

11.2.2 **Test Case Description:** Generate TCP SYN flood traffic to evaluate connection handling under high load.

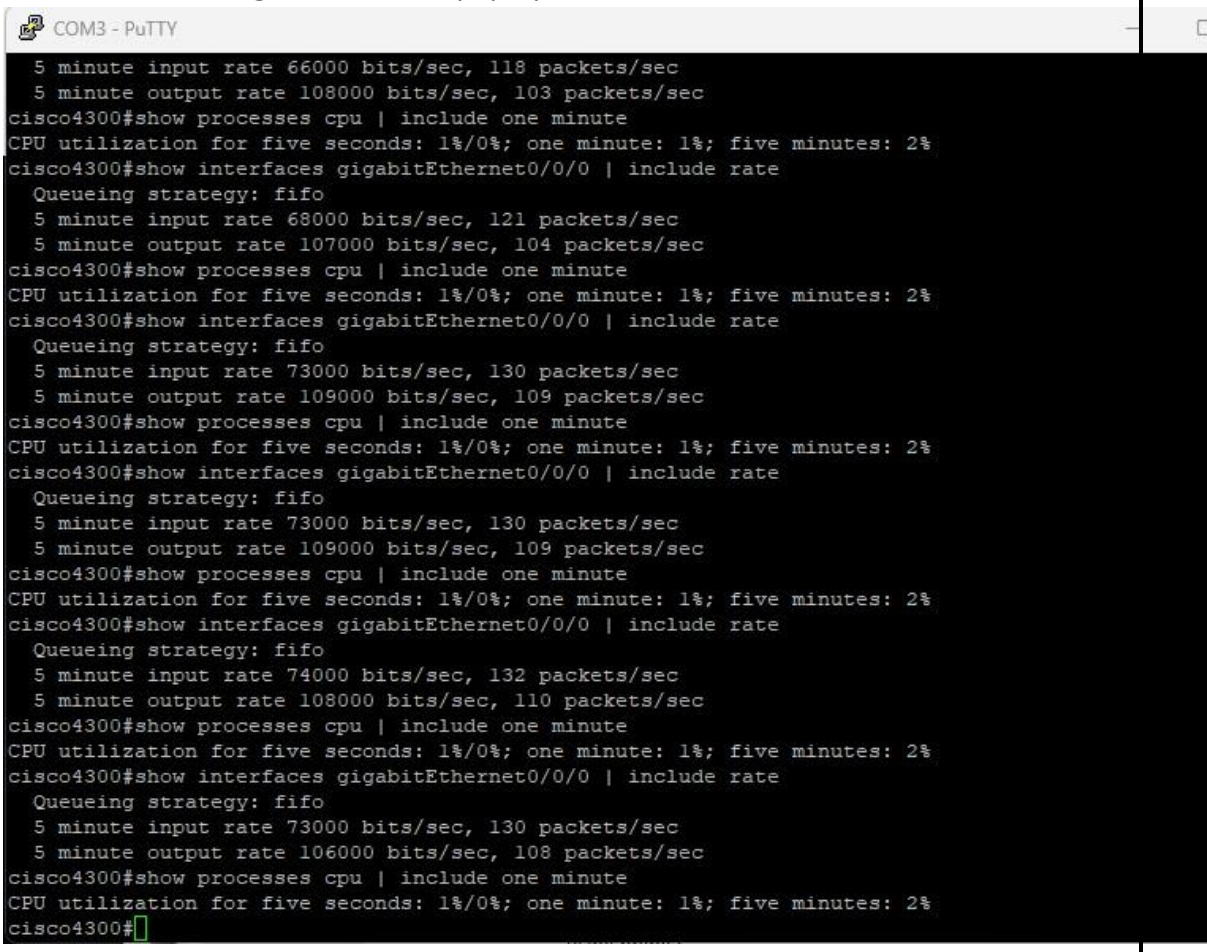
11.2.3 **Execution Steps:**

(i) Generate TCP SYN flood traffic:
"sudo hping3 -I eth0 -S 192.168.1.51 -p 80 --flood --rand-source"

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -I eth0 -S 192.168.1.51 -p 80 --flood --rand-source
[sudo] password for kali:
HPING 192.168.1.51 (eth0 192.168.1.51): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

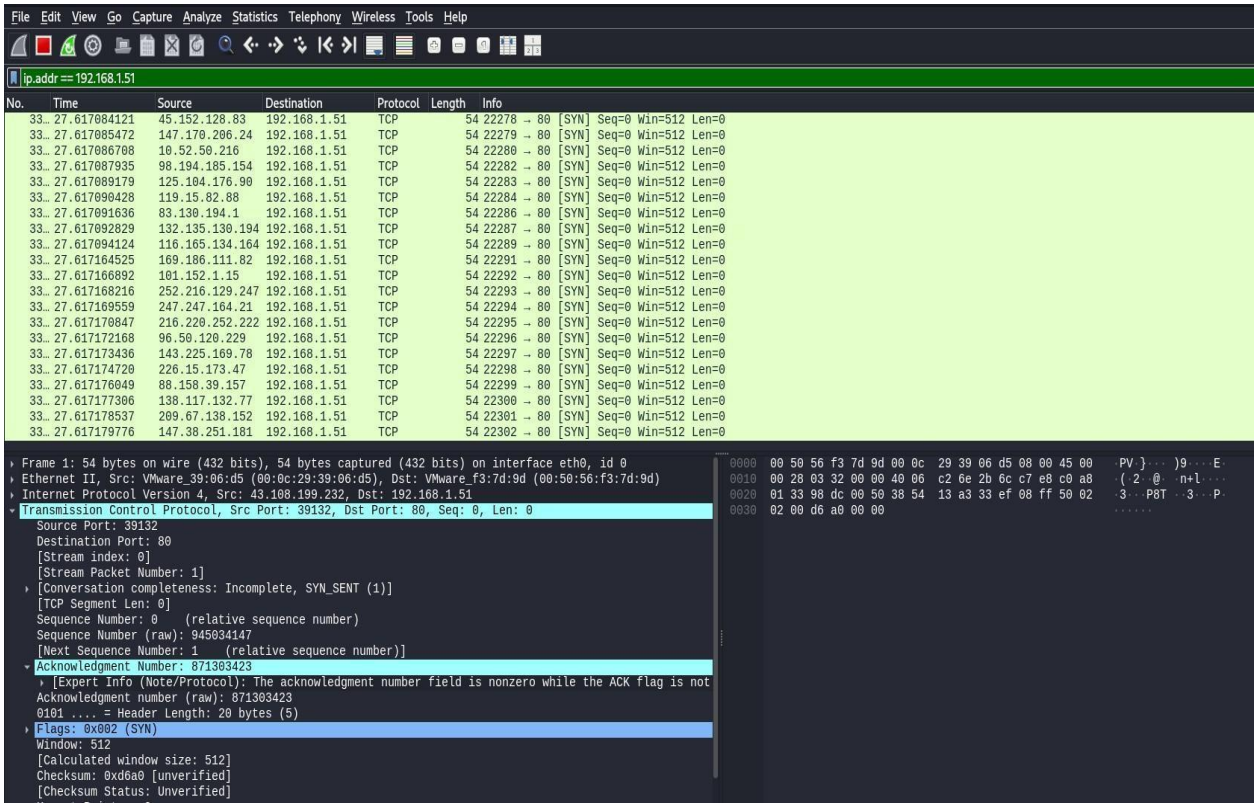
(ii) Monitor Router: On the router,

run: “show processes cpu | include one minute”
“show interface GigabitEthernet0/0/0 | include rate”



(iii) Stop after 10 minutes and save Wireshark capture.

Record observations: Check CPU usage, packet drops, and any syslog messages indicating overload protection activation.



11.2.4 **Test Observation:** Observe any packet drops, errors logged by the router, or signs of overload protection mechanisms.

11.2.5 **Evidence Provided:** Screenshots of testing steps and Wireshark pcap files.

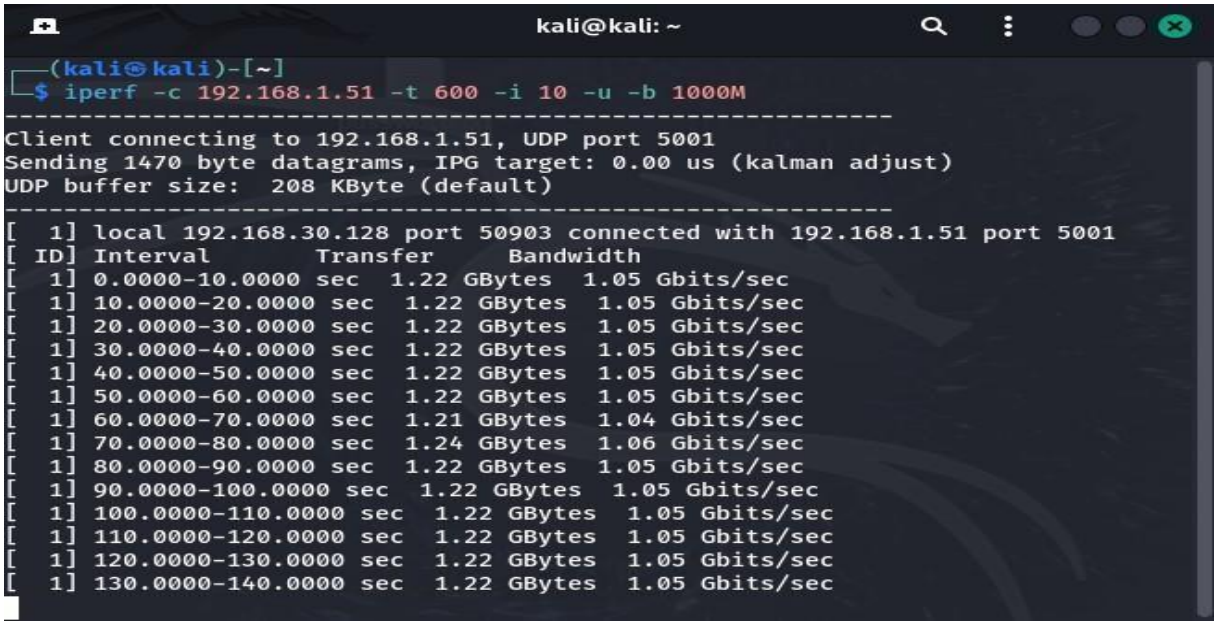
11.3 Test Case Number: 3

11.3.1 **Test Case Name:** TC_Throughput Testing Using iperf

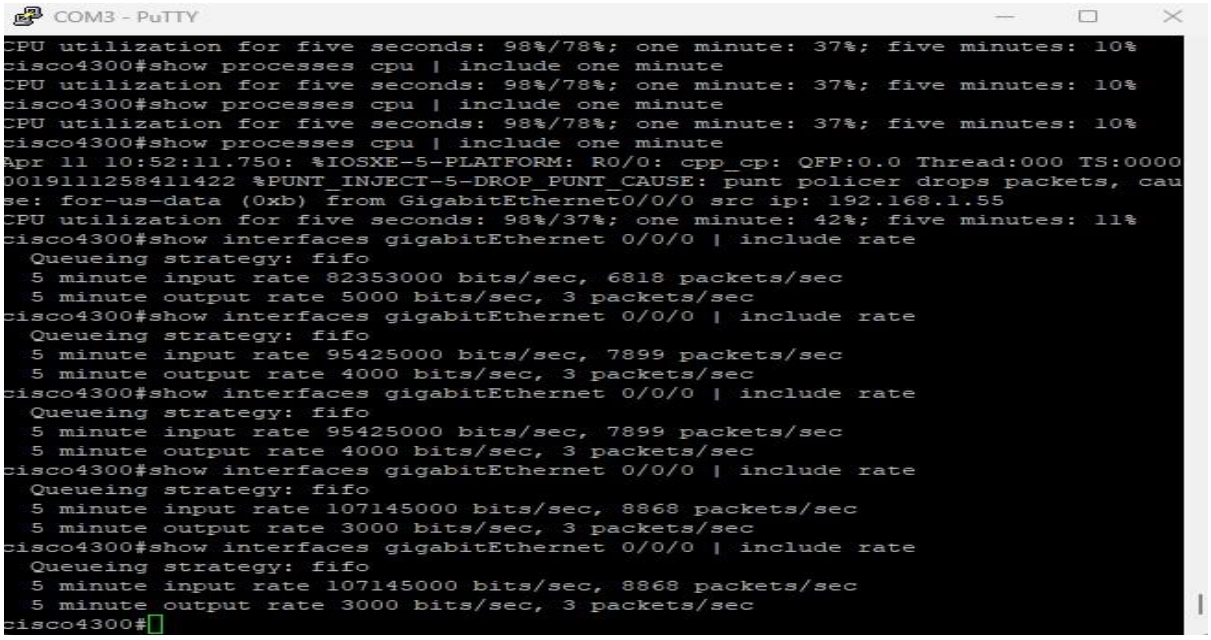
11.3.2 **Test Case description:** Generate TCP SYN flood traffic to evaluate connection handling under high load.

11.3.3 **Execution Steps:**

(i) Set up iperf server on the router or another system in the same network. run: Run iperf client on the test system (Kali Linux): **iperf -c 192.168.1.51 -t 600 -i 10 -u -b 1000M**

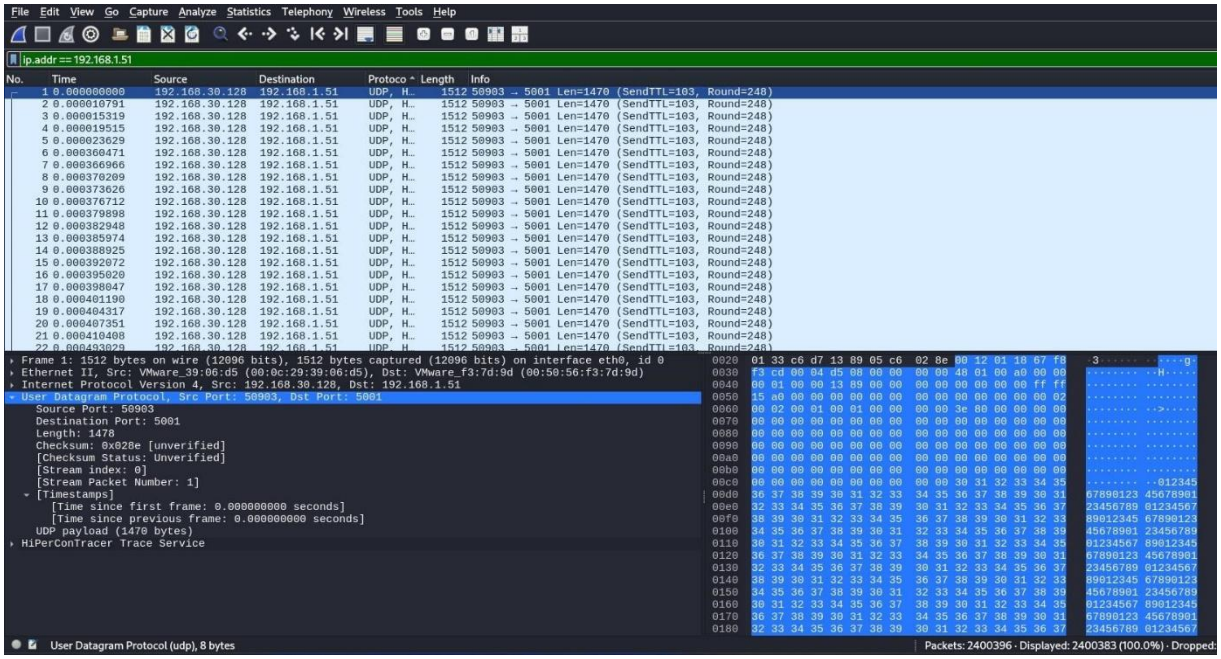


(ii) Monitor Router: On the router, run: **"show processes cpu | include one minute"** **"show interface GigabitEthernet0/0/0 | include rate**



(iii) Stop **after 10 minutes** and save Wireshark capture.

Record observations: Observe throughput, packet loss, CPU usage, and any overload protection activation.



11.3.4 **Test Observation:** Measure the throughput achieved using iperf and compare it to the maximum capacity of the interface.

11.3.5 **Evidence Provided:** Screenshots of testing steps and Wireshark pcap files.

11.4 Test Case Number: 4

11.4.1 **Test Case Name:** TC_HTTP_APPLICATION_OVERLOADING_TRAFFIC

11.4.2 **Test Case description:** Generate TCP SYN flood traffic to evaluate connection handling under high load.

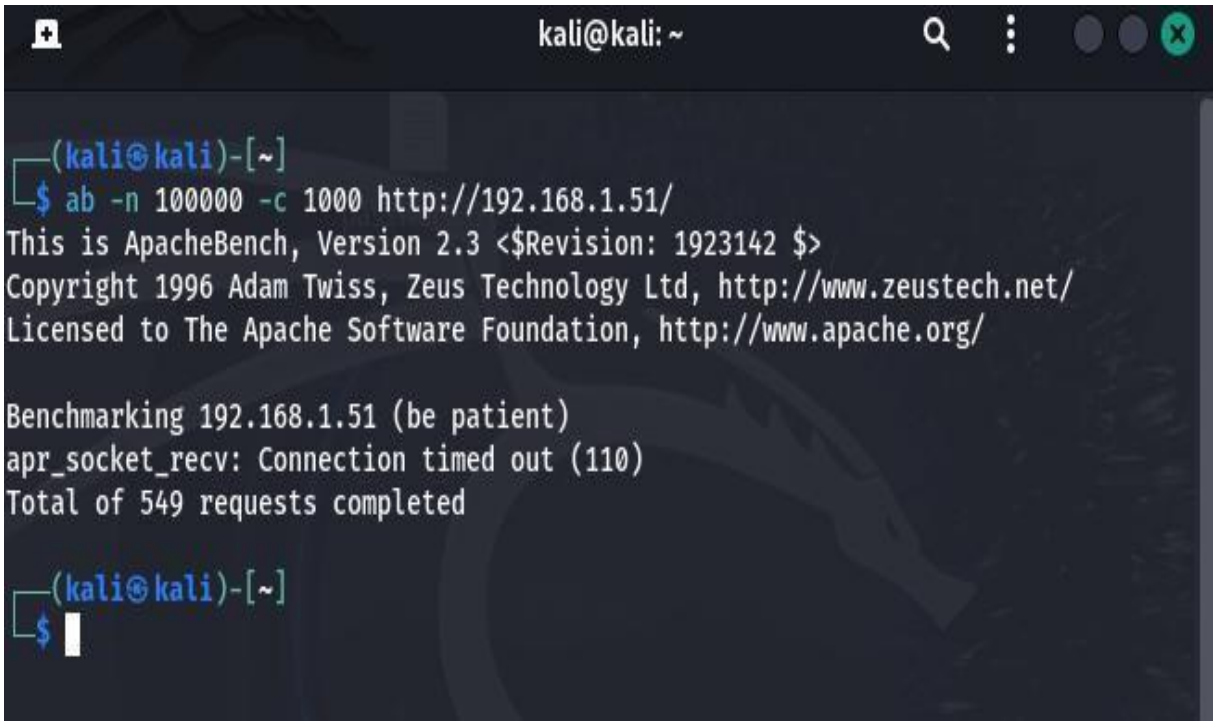
11.4.3 **Execution Steps:**

(i) Set Up Web Server: Ensure that there is a web server running on the router or another system reachable through the router on port 80. This will serve as the target for HTTP requests.

(ii) Start Wireshark on the test system and set a capture filter for host 192.168.1.51. **(iii)** Use Apache Benchmark (ab) to simulate HTTP overload:

Run ab to generate HTTP requests:

ab -n 100000 -c 1000 http://192.168.1.51/



Using slowloris:

slowloris http://192.168.1.51

slowloris is specifically designed to send partial HTTP requests slowly, to tie up resources

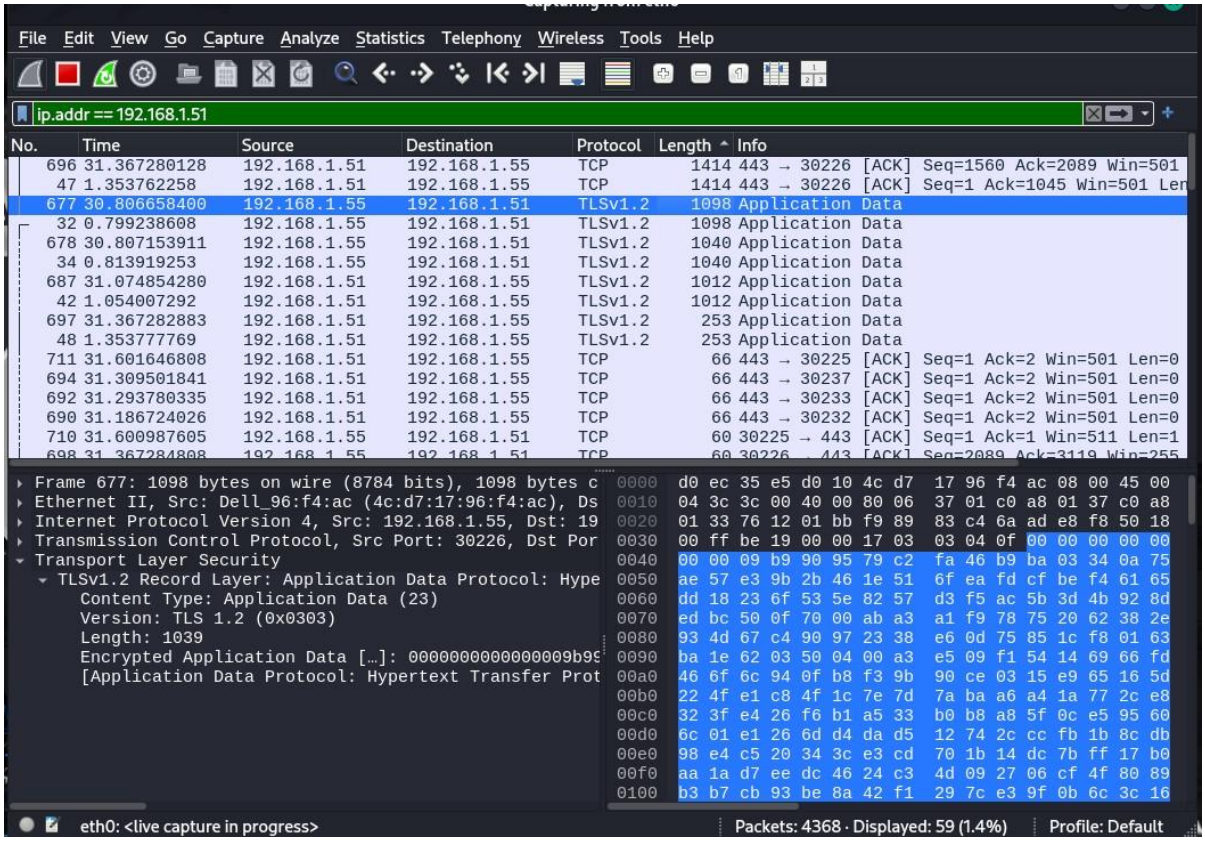
```
┌──(kali㉿kali)-[~]
└─$ slowloris http://192.168.1.51
[11-04-2025 16:35:35] Attacking http://192.168.1.51 with 150 sockets.
[11-04-2025 16:35:35] Creating sockets...
[11-04-2025 16:35:35] Sending keep-alive headers...
[11-04-2025 16:35:35] Socket count: 0
[11-04-2025 16:35:35] Creating 150 new sockets...
[11-04-2025 16:35:50] Sending keep-alive headers...
[11-04-2025 16:35:50] Socket count: 0
[11-04-2025 16:35:50] Creating 150 new sockets...
[11-04-2025 16:36:05] Sending keep-alive headers...
[11-04-2025 16:36:05] Socket count: 0
[11-04-2025 16:36:05] Creating 150 new sockets...
[11-04-2025 16:36:20] Sending keep-alive headers...
[11-04-2025 16:36:20] Socket count: 0
[11-04-2025 16:36:20] Creating 150 new sockets...
[11-04-2025 16:36:35] Sending keep-alive headers...
[11-04-2025 16:36:35] Socket count: 0
[11-04-2025 16:36:35] Creating 150 new sockets...
[11-04-2025 16:36:50] Sending keep-alive headers...
[11-04-2025 16:36:50] Socket count: 0
[11-04-2025 16:36:50] Creating 150 new sockets...
```

(iii) Monitor Router: On the router, run: **"show processes cpu | include one minute"**
"show interface GigabitEthernet0/0/0 | include rate

```
cisco4300#show interfaces gigabitEthernet 0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 113943000 bits/sec, 9409 packets/sec
  5 minute output rate 3000 bits/sec, 2 packets/sec
cisco4300#show interfaces gigabitEthernet 0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 113943000 bits/sec, 9409 packets/sec
  5 minute output rate 3000 bits/sec, 2 packets/sec
cisco4300#show interfaces gigabitEthernet 0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 113943000 bits/sec, 9409 packets/sec
  5 minute output rate 3000 bits/sec, 2 packets/sec
cisco4300#show interfaces gigabitEthernet 0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 112051000 bits/sec, 9252 packets/sec
  5 minute output rate 2000 bits/sec, 1 packets/sec
cisco4300#show processes cpu | include one minute
CPU utilization for five seconds: 1%/0%; one minute: 2%; five minutes: 14%
cisco4300#show processes cpu | include one minute
CPU utilization for five seconds: 1%/0%; one minute: 2%; five minutes: 14%
cisco4300#show processes cpu | include one minute
CPU utilization for five seconds: 1%/0%; one minute: 2%; five minutes: 14%
cisco4300#show processes cpu | include one minute
CPU utilization for five seconds: 1%/0%; one minute: 2%; five minutes: 14%
cisco4300#
```

(iv) **Stop after 10 minutes** and save Wireshark capture.

Record observations: Check CPU usage, response time, packet handling, and any syslog messages indicating overload protection activation.



11.4.4 **Test Observation:** CPU utilization observed during the HTTP overload test.

11.4.5 **Evidence Provided:** Screenshots of testing steps and Wireshark pcap files.

11.5 Test Case Number: 5

11.5.1 **Test Case Name:** TC_TRAFFIC_GENERATOR

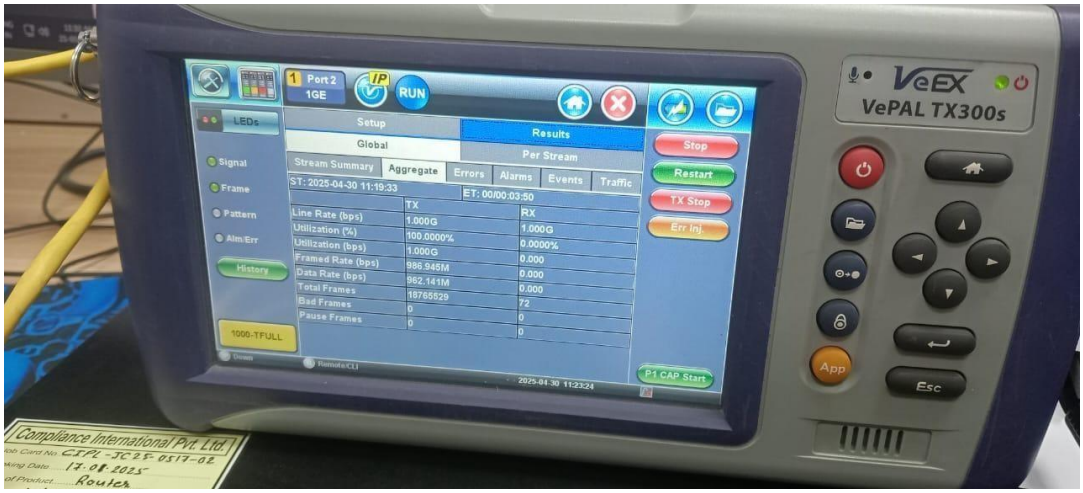
11.5.2 **Test Case description**: Test case to verify maximum capacity to reached while performing excessive overloading protection.

11.5.3 **Execution Steps:** Check the DUT interface capacity input rate.

```
cisco4300#show interfaces gigabitEthernet 0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Hardware is ISR4331-3x1GE, address is d0ec.35e5.d011 (bia d0ec.35e5.d011)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:17, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     8 packets output, 3296 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
cisco4300#
cisco4300#
cisco4300#
cisco4300#
cisco4300#
cisco4300#
cisco4300#show interfaces gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4331-3x1GE, address is d0ec.35e5.d010 (bia d0ec.35e5.d010)
  Internet address is 192.168.1.51/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:04:04, output 00:00:10, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     93108 packets input, 16102639 bytes, 0 no buffer
     Received 8711 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 80436 multicast, 0 pause input

cisco4300#
```

Above screenshot verify that the interface capacity is 100000 kbit/sec i.e 1 Gbps and input rate is 0 bit/sec before sending the traffic.

Generate the 1 Gbps traffic from VeEX traffic generator tool to DUT.



Monitor Router: On the router,
run: “show processes cpu | include one minute” “show interface GigabitEthernet0/0/0 | include rate

```
cisco4300#show interfaces gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4331-3x1GE, address is d0ec.35e5.d010 (bia d0ec.35e5.d010)
  Internet address is 192.168.1.51/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 248/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 376/375/1863033/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 974916000 bits/sec, 80510 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
     116923169 packets input, 176896790611 bytes, 2794 no buffer
     Received 8711 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 80452 multicast, 0 pause input

cisco4300#show interfaces gigabitEthernet 0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Hardware is ISR4331-3x1GE, address is d0ec.35e5.d011 (bia d0ec.35e5.d011)
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 248/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 376/375/1051969/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 975886000 bits/sec, 80910 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     118071169 packets input, 178051311436 bytes, 22342 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 8 multicast, 0 pause input

cisco4300#show processes cpu | include five minute
CPU utilization for five seconds: 98%/2%; one minute: 98%; five minutes: 98%
cisco4300#
```

Above screenshot the verify the input rate approx. 100% and cpu utilization is 98% the DUT handled overload effectively. CPU usage increased but remained stable. No significant degradation in DUT availability was observed, indicating robust handling of DDoS attacks.

11.5.4 **Test Observation:** The DUT managed the Traffic flood traffic effectively, demonstrating its capability to handle 1 Gbps DDoS attacks. CPU utilization increased as expected, but the system remained stable, with no critical performance issues or disruptions.

11.5.5 **Evidence Provided:** Screenshots of testing steps.

12. Test Case Result:

S. No.	Test Case Name	Pass/ Fail	Remarks
1	TC_ICMP_FLOODING	Pass	DUT handled ICMP flooding with overload protection showing stable CPU utilization and packet handling. No significant packet loss or service disruption occurred. Overload protection mechanisms were effective.
2	TC_TCP_SYN_RST_FLOODING	Pass	DUT demonstrated effective handling of TCP SYN/RST flooding with slight increase in CPU utilization. Overload protection mechanisms were successfully activated, and no service disruption occurred.
3	TC_UDP_FLOODING	Pass	DUT maintained high throughput during 'iperf' test, achieving near maximum interface capacity. CPU usage was higher but within acceptable limits, and no significant packet loss was observed. Overload protection was not triggered, indicating the router's capacity to handle expected traffic loads.
4	TC_HTTP_APPLICATION_ OVERLOADIN_ TRAFFIC	Pass	DUT handled HTTP overload effectively. CPU usage increased but remained stable. No significant degradation in HTTP response time or server availability was observed, indicating robust handling of application-level DDoS attacks. moderately but did not cause disruption.
5.	TC_TRAFFIC_GENERATOR	Pass	The DUT managed the Traffic flood traffic effectively, demonstrating its capability to handle 1 Gbps DDoS attacks. CPU utilization increased as expected, but the system remained stable, with no critical performance issues or disruptions.

1.8.2: Filtering IP Options

<DUT Details: > Wi-Fi CPE
<DUT Software Version:> 8.10.183.0
<Digest Hash of OS> Hash of OS required
<Digest Hash of Configuration> Hash of configuration required.
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> ITSAR402122401 and Version: 1.0.1
<OEM Supplied Document list: > OEM Supplied Document list required

1. **<ITSAR Section No & Name>** Section 1.8: Attack Prevention Mechanism
2. **<Security Requirement No & Name >** 1.8.2: Filtering IP Options
3. **<Requirement Description: >** Wi-Fi CPE shall have protection mechanisms against Network-level and Application-level Distributed Denial of Service (DDoS) attacks. Wi-Fi CPE shall provide security measures to deal with overload situations which may occur as a result of a denial-of-service attack or during periods of increased traffic. In particular, partial or complete impairment of system availability shall be avoided. Potential protective measures may include:
    - Restricting available RAM per application
    - Restricting maximum sessions for a Web/Database application
    - Defining the maximum size of a dataset
    - Restricting Central Processing Unit (CPU) resources per process
    - Prioritizing processes
    - Limiting amount or size of transactions of a user or from an IP address in a specific time range
    - Limiting amount or size of transactions to an IP address/Port Address in a specific time range

    [Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.3.1]

4. **<u>DUT Confirmation Details</u>**:
    - This section involves information about DUT like software/firmware version, Hardware version model.
    - DUT Cisco WLC contains default boot image with version 8.10.183.0. The model is AIRAP1852I-E-K9. The inventory shows model serial no. & model description.

Verification of DUT Cisco wireless LAN controller's HW product series information by running command show inventory on CLI.

Verification of DUT Cisco WLC's high-level system SW information by running command show sysinfo on CLI.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.10.183.0
OUI File Last Update Time........................ N/A

System Name...................................... Aironet-Controller
System Location..................................
System Contact...................................
System ObjectID.................................. 1.3.6.1.4.1.9.1.2250
IP Address....................................... 10.208.38.2
Last Reset....................................... 1: reload command

System Up Time................................... 0 days 3 hrs 33 mins 5 secs
System Timezone Location......................... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
System Stats Realtime Interval................... 5
System Stats Normal Interval..................... 180

Configured Country............................... IN  - India

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled

--More-- or (q)uit
```

Verification of DUT Cisco WLC's system information on Web access.

5. **DUT Configuration**:

Initial IP configuration set up in DUT as captured from the console.

```
(Cisco Controller) >show run-config

Press Enter to continue...

System Inventory
NAME: "Mobility Express"    , DESCR: "Cisco Aironet 1850 Series Mobility Express"
PID: AIR-AP1852I-E-K9,  VID: V01,  SN: KWC193100UU

Burned-in MAC Address............................ 38:ED:18:C8:10:60
Maximum number of APs supported.................. 50
Press Enter to continue or <ctrl-z> to abort


System Information
Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.10.183.0
OUI File Last Update Time........................ N/A

System Name...................................... Aironet-Controller
System Location..................................
System Contact...................................
System ObjectID.................................. 1.3.6.1.4.1.9.1.2250
IP Address....................................... 10.208.38.2
Last Reset....................................... 1: reload command

System Up Time................................... 2 days 6 hrs 5 mins 33 secs
System Timezone Location......................... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
System Stats Realtime Interval................... 5
System Stats Normal Interval..................... 180

Configured Country............................... IN  - India

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled

--More or (q)uit current module or <ctrl-z> to abort
```

LAN connection to DUT from tester machine. No additional configuration required, as the tester tests this requirement by default cases.

6. **Preconditions:**
   - A document which provides a detailed technical description of the overload control mechanisms.
   - Test results from a test execution phase of overload control mechanism testing.

7. **Test Objective/ Purpose:** Verify that the network product:
   - has a detailed technical description of the overload control mechanisms used to deal with overload scenarios;
   - has test results verifying the operation of the overload control mechanisms.

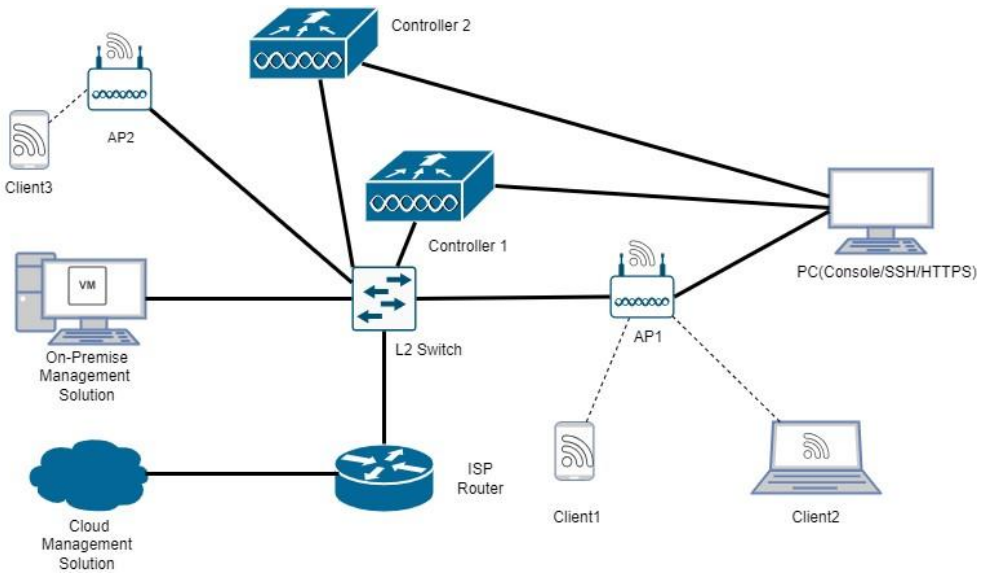
8. **Test Plan:**

8.1 Number of Test Scenarios:

8.1.1 TC_OVERLOAD_CONTROL_MECHANISM_DDOS_AVOIDANCE_VERIFICATION
8.1.2 TC_ICMP_FLOODING
8.1.3 TC_TCP_SYN_RST_FLOODING
8.1.4 TC_UDP_FLOODING
8.1.5 TC_HTTP_APPLICATION_FLOODING
8.1.6 TC_SSH_FLOODING
8.1.7 TC_TRAFFIC_GENERATOR

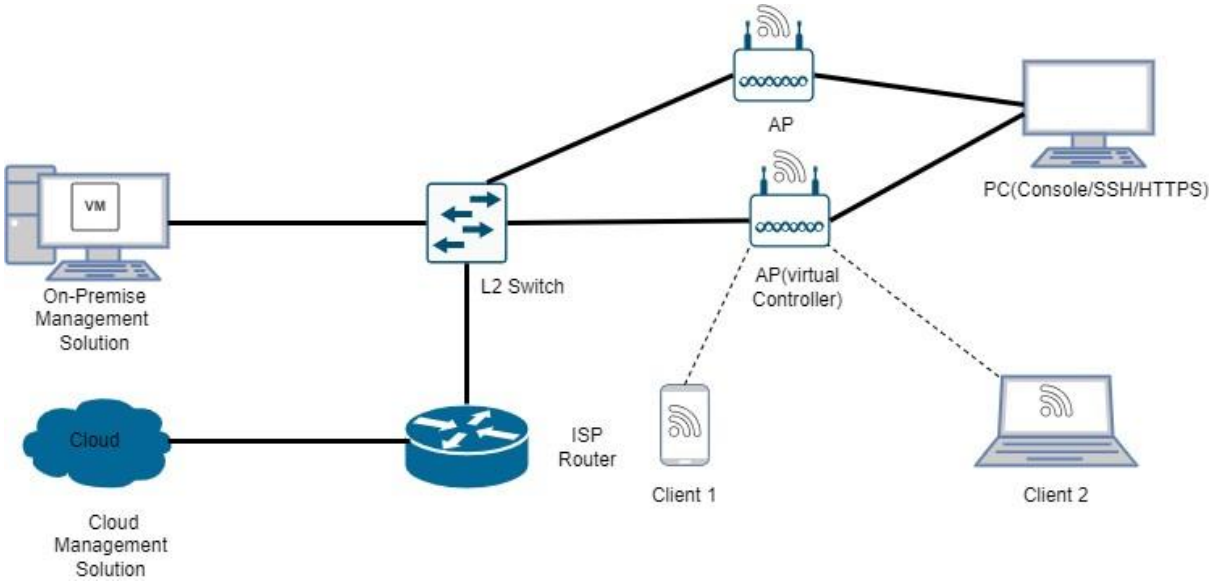
8.2 Testbed Diagram:

AP + Controller mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

8.3 Tools required:

Wireshark, ubuntu, kali, hping3 (for icmp flooding and tcp syn-rst flooding), yersinia (for CDP flooding), nload (monitor network traffic on interface), ostinato (icmp traffic generator.

.4 Test Execution Steps:

Case Tester should verify DDoS prevention mechanism provided in OEM documentation

- Case No. 1 – Network level DDoS - ICMP flooding.
  - Step1: Before applying ICMP flooding, tester login to DUT via ssh and verify CPU usage of DUT.
  - Step2: Starting ICMP flooding.
  - Step3: Observing DUT behaviour while ICMP flooding.
  - Step4: Stopping ICMP flooding and verifying DUT behaviour.
- Case No. 2 – Transport level DDoS - TCP SYN-RST Flood.
  - Step1: Before applying TCP SYN-RST Flooding, tester login to DUT via ssh and verify CPU usage of DUT.
  - Step2: Starting TCP SYN-RST Flooding.
  - Step3: Observing DUT behaviour while TCP SYN-RST Flooding.
  - Step4: Stopping TCP SYN-RST Flooding and verifying DUT behaviour.

The tester verifies that there is:

- A technical description providing a high-level overview of the overload control design.

- An overview of the types of overload scenarios that the network product overload control mechanisms are expected to handle.
- An overview of the overload control thresholds that the network product uses to trigger overload control mechanisms.
- Description of the types of attacks that may cause an overload to the network product and how these are handled.
- A description of how the network product discards or handles input during various overload situations including excessive overloads. i.e. where the overload is significantly greater than the thresholds where overload detection is triggered.
- A description of how the network product security functions operate and perform during overload.
- A description of how the network product shuts down or performs or takes other abatement or corrective actions during excessive overload conditions.

The tester verifies that the test results:

- Contain details of the overload conditions used in the test execution that are consistent with the technical description document.
- Describe test procedures used to verify the overload control mechanisms.
- Contain data which demonstrates/indicates that the overload control mechanisms described in the technical description document have been implemented.
- Contain details of the test set-up including the mechanisms for creating the overload. Where simulators and/or scripts are used to artificially create a load then details of these should also be included.

9. **Expected Results:**

- A technical description provides a high-level overview of the overload control design.
- An overview of the types of overload scenarios and overload control thresholds that are considered.
- Description on the types of attacks that may cause an overload to the system and how these are handled.
- A description of how the network product discards or handles input during various overload situations.
- Describes if or how the network product security functions operate and perform during overload.
- If parts of the system shutdown or take other abatement or corrective actions these should be described.

Note: If some of the items listed above are not applicable to a network product then, in those cases, it should be clarified by the vendor why these items are not applicable.

The test results should:

- Contain details of the overload conditions used in the test execution that are consistent with the technical description document.
- Describe the test procedures used to verify the overload control mechanisms.
- Contain data which demonstrates/indicates that the overload control mechanisms described in the technical description document have been implemented.
- Contain details of the test set-up including the mechanisms for creating the overload.

10. **Expected Format of Evidence:** Documentation showing each of the points in the results sections and screenshots of test performed.

11. **Test Execution:**

11.1 **Test Case Number: 01**

11.1.1 **Test Case Name:**
TC_OVERLOAD_CONTROL_MECHANISM_DDOS_AVOIDANCE_VERIFICATION

11.1.2 **Test Case Description:** To verify whether the PCF system has documented and implemented DDoS avoidance mechanisms, including overload control and protective measures, ensuring consistency between the OEM-provided documentation and system behavior.

11.1.3 **Execution Steps:**

(i) Review the technical and test result documentation provided by the OEM, ensuring it includes:
- A high-level overview of the overload control design.
- Details of overload scenarios handled by the DUT.
- Defined thresholds for triggering overload control mechanisms.
- Descriptions of potential DDoS attacks and corresponding mitigation strategies.
- Methods for discarding or handling excessive overload situations.
- Security functions and their performance under overload conditions.
- Overload conditions used in testing, consistent with the technical documentation.
- Test procedures used to verify the overload control mechanisms.
- Evidence demonstrating that the documented overload control mechanisms are implemented.
- Details of the test setup, including mechanisms for simulating overload conditions.

(ii) Verify protective measures implemented in the PCF system:
- Configure iptables to limit connections per IP.
- Configure resource limits (CPU, Memory, Sessions) to restrict excessive usage.

- Simulate network-level DDoS attacks (Flooding) using hping3.
- Monitor system logs to verify mitigation responses.
- Test application-layer overload scenarios by generating multiple HTTP sessions.

11.1.4 **Test Observations:** Documentation and system behavior align, demonstrating that DDoS mitigation mechanisms are effectively implemented.

11.1.5 **Evidence Provided:**

(iii) Review the technical and test result documentation provided by the OEM, ensuring it includes:

- A high-level overview of the overload control design.
- Details of overload scenarios handled by the DUT.
- Defined thresholds for triggering overload control mechanisms.
- Descriptions of potential DDoS attacks and corresponding mitigation strategies.
- Methods for discarding or handling excessive overload situations.
- Security functions and their performance under overload conditions.

11.2 Test Case Number: 02

11.2.1 **Test Case Name**: TC_ICMP_FLOODING

11.2.2 **Test Case Description:** Generate ICMP flood traffic to test maximum bandwidth handling.

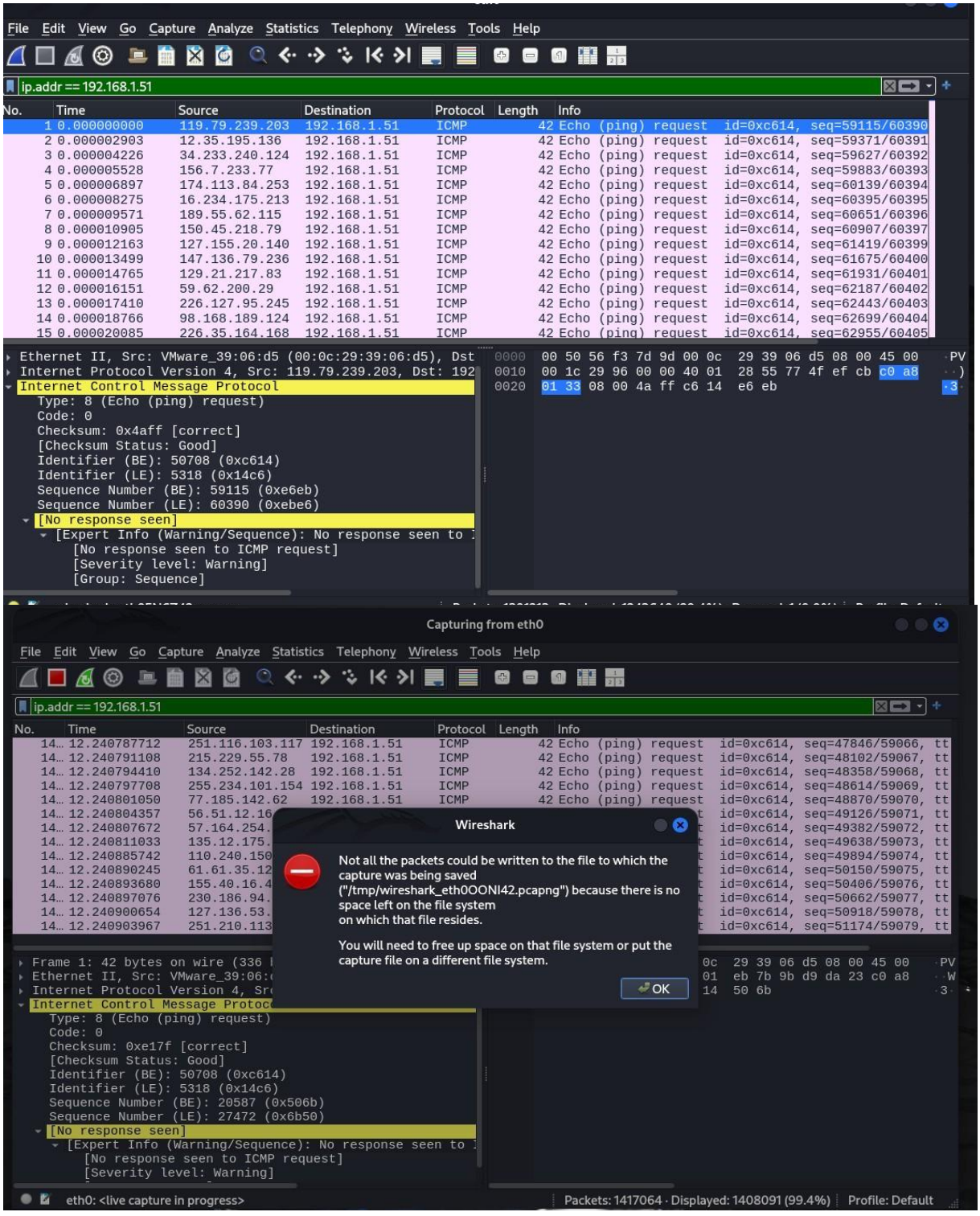
11.2.3 **Execution Steps:**

(i) Start Wireshark on the test system and set a capture filter for host 192.168.1.51.

(ii) Generate ICMP flood traffic using hping3:

" sudo hping3 -I eth0 -1 192.168.1.51 --flood --rand-source"

Now packet capture by wireshark:



hping3-8.1.pcapng

(iii) Monitor Router: On the Router, run:“show processes cpu | include one minute” “show interface GigabitEthernet0/0/0 | include rate”

```
cisco4300#show processes cpu | include one minute
CPU utilization for five seconds: 1%/0%; one minute: 1%; five minutes: 1%
cisco4300#show interfaces gigabitEthernet0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 182000 bits/sec, 352 packets/sec
  5 minute output rate 301000 bits/sec, 355 packets/sec
cisco4300#show processes cpu | include one minute
CPU utilization for five seconds: 0%/0%; one minute: 1%; five minutes: 1%
cisco4300#show interfaces gigabitEthernet0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 176000 bits/sec, 343 packets/sec
  5 minute output rate 286000 bits/sec, 345 packets/sec
cisco4300#show processes cpu | include one minute
CPU utilization for five seconds: 1%/0%; one minute: 1%; five minutes: 1%
cisco4300#show interfaces gigabitEthernet0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 176000 bits/sec, 343 packets/sec
  5 minute output rate 286000 bits/sec, 345 packets/sec
cisco4300#show interfaces gigabitEthernet0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 173000 bits/sec, 339 packets/sec
  5 minute output rate 280000 bits/sec, 340 packets/sec
cisco4300#show processes cpu | include one minute
CPU utilization for five seconds: 1%/0%; one minute: 1%; five minutes: 1%
cisco4300#show interfaces gigabitEthernet0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 172000 bits/sec, 337 packets/sec
  5 minute output rate 277000 bits/sec, 337 packets/sec
cisco4300#
```

(iv) Stop after 10 minutes and save Wireshark capture.

11.2.4 **Test Observation:** The router handled the ICMP flood traffic well, showing stable CPU usage. The applied ACLs effectively filtered unnecessary ICMP requests, preventing any overload.

11.2.5 **Evidence Provided:** Screenshots of testing steps and Wireshark pcap files**.**

11.**3 Test Case Number:** 3

11.3.1 **Test Case Name:** TC_ TCP_SYN_RST_FLOODING

11.3.2 **Test Case description:** Generate TCP SYN flood traffic to evaluate connection handling under high load.

11.3.3 **Execution Steps:**

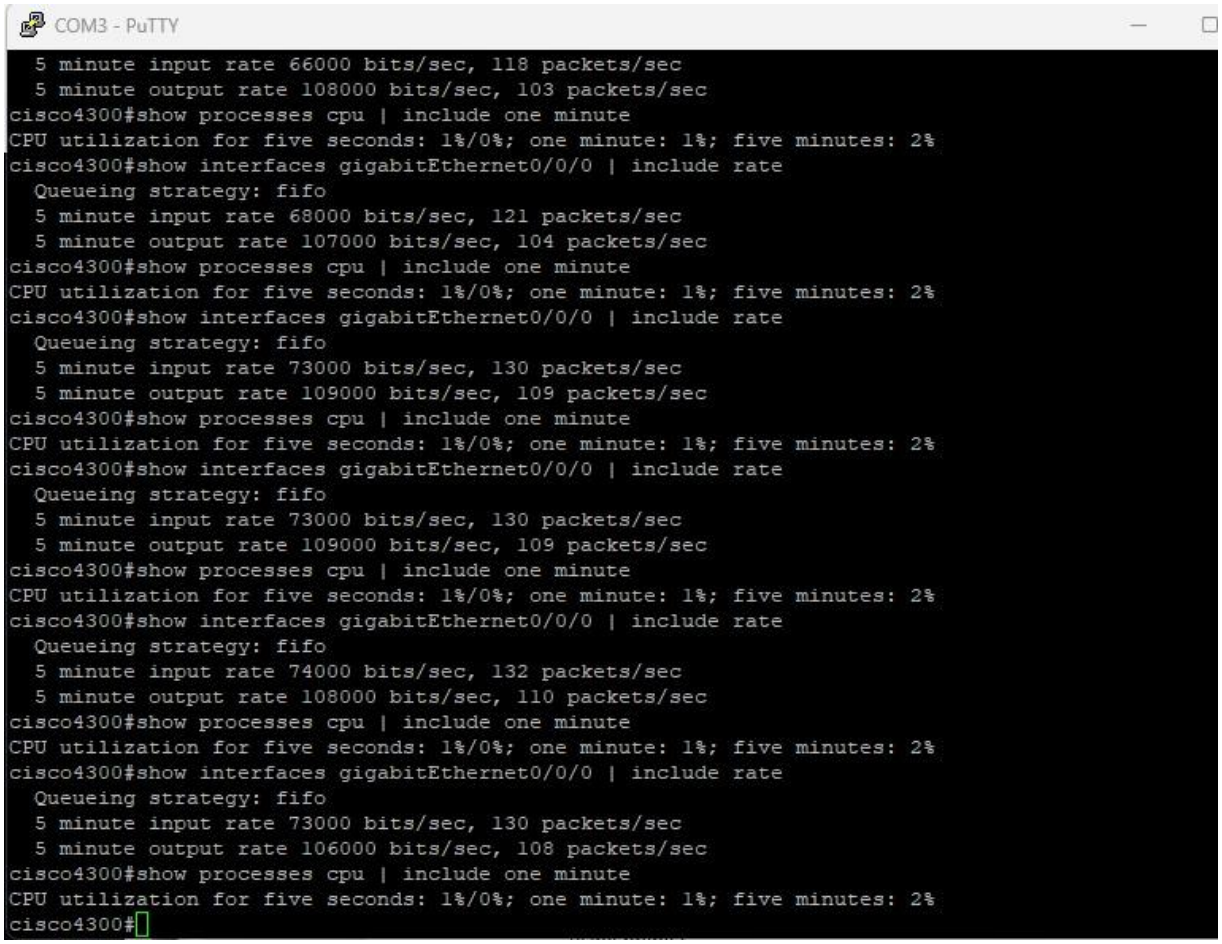
(i) Generate TCP SYN flood traffic:

"sudo hping3 -I eth0 -S 192.168.1.51 -p 80 --flood --rand-source"

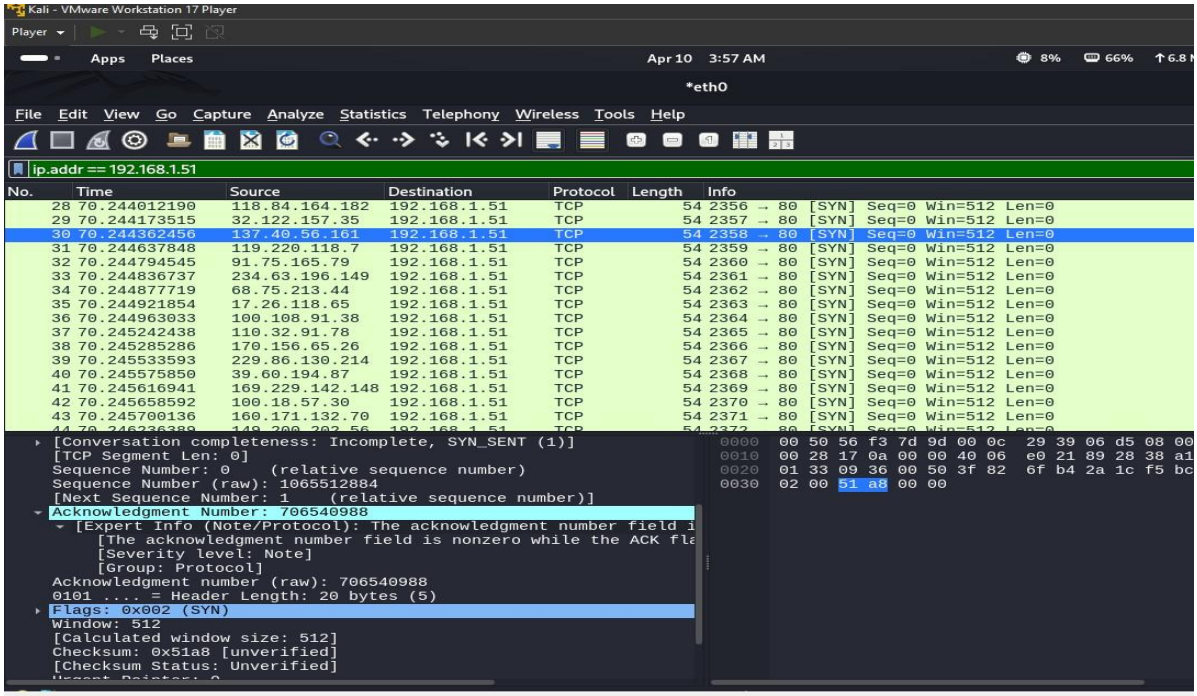
```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -I eth0 -S 192.168.1.51 -p 80 --flood --rand-source
[sudo] password for kali:
HPING 192.168.1.51 (eth0 192.168.1.51): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

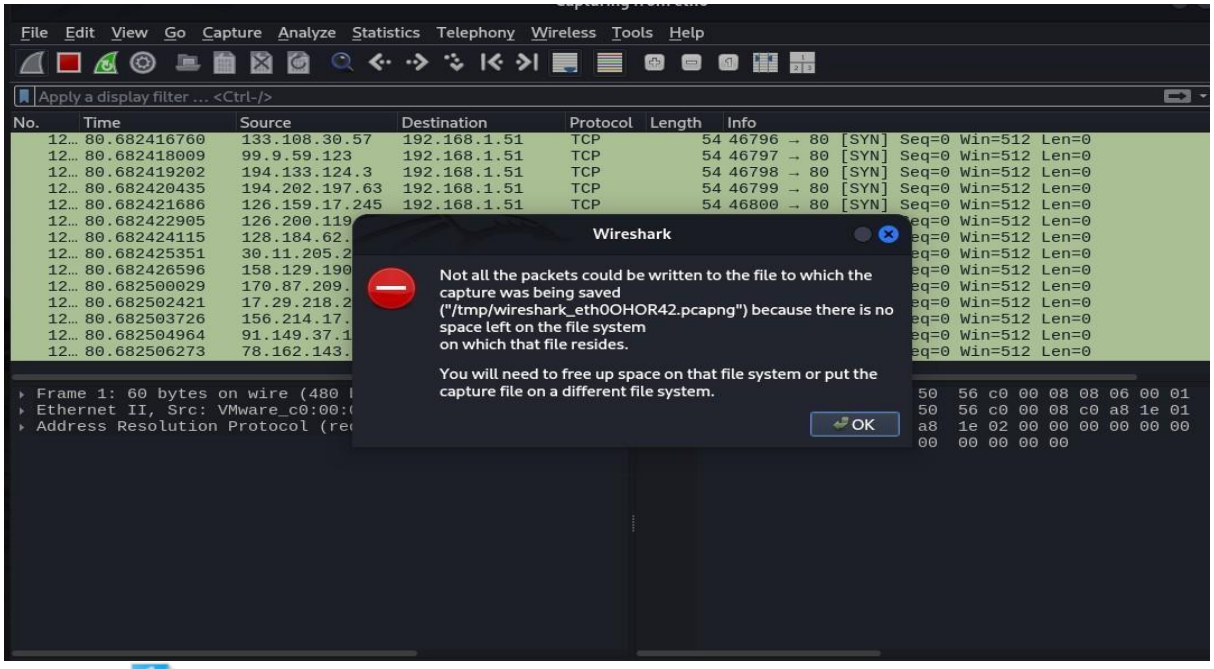
(ii) Monitor Router: On the router, run: **"show processes cpu | include one minute"**

"show interface GigabitEthernet0/0/0 | include rate"



(iii) Stop after 10 minutes and save Wireshark capture.





hping3-8.1 tcp.pcapng

11.3.4 **Test Observation:** During the TCP SYN flood test, the router managed to maintain a reasonable CPU usage level, indicating good resilience to connection-oriented flooding. The router's inherent SYN- flood protection mechanisms were effective.

11.3.5 **Evidence Provided:** Screenshots of testing steps and Wireshark pcap files.

11.4 Test Case Number: 4

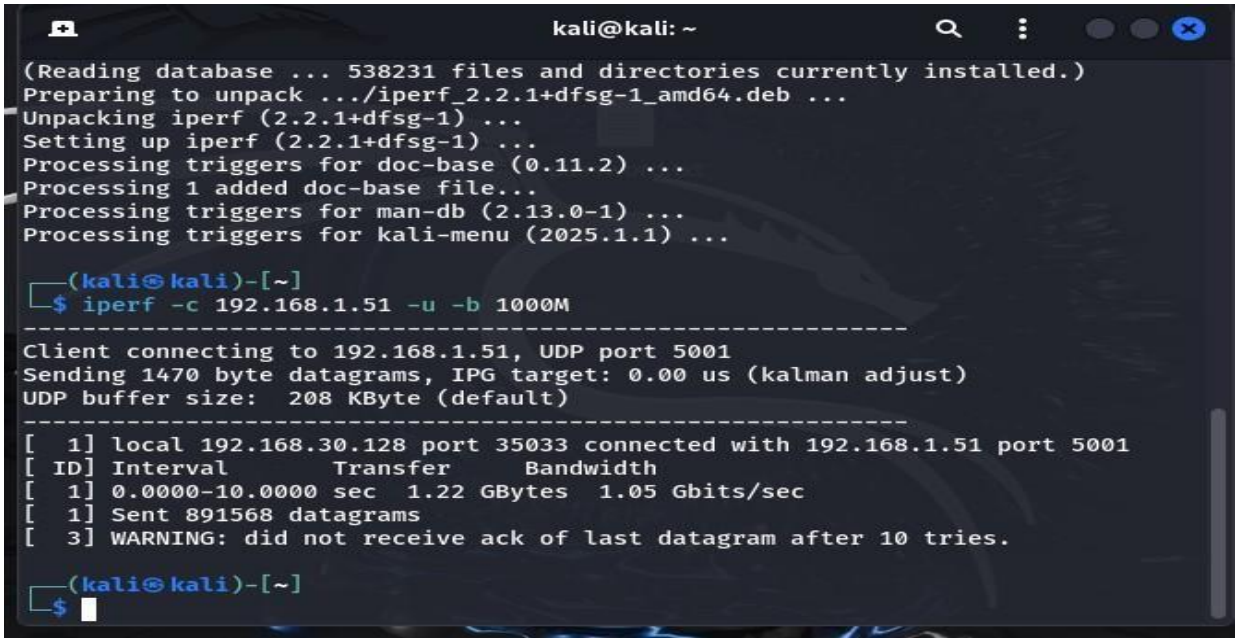
11.4.1 **Test Case Name:** TC_ UDP_FLOODING

11.4.2 **Test Case description:** Generate UDP flood traffic to test datagram processing capability.

11.4.3 **Execution Steps:**

(i) **Run iperf server** on another system if needed: iperf -s -u -i 1

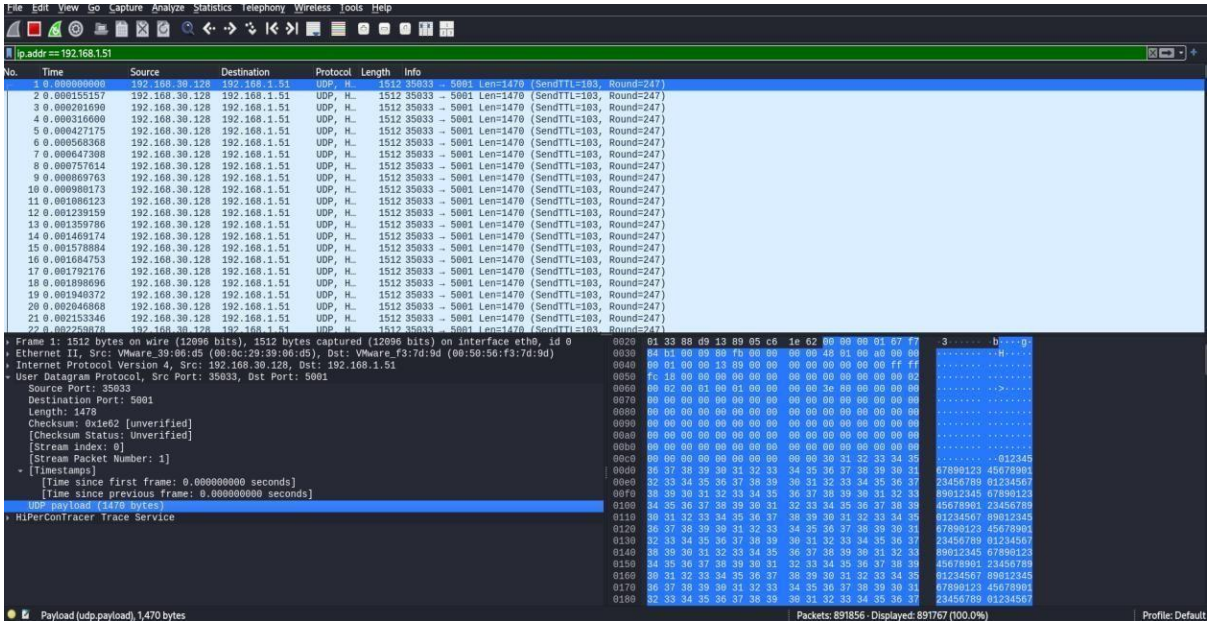
(ii) **Generate UDP flood:** As interface Max Capacity “iperf -c 192.168.1.51 -u -b 1000M



(iii) **Monitor Router:** On the DUT(Router), run:

```
cisco4300#show interfaces gigabitEthernet0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 27121000 bits/sec, 2245 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
cisco4300#show processes cpu | include one minute
CPU utilization for five seconds: 1%/0%; one minute: 14%; five minutes: 4%
cisco4300#show interfaces gigabitEthernet0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 27121000 bits/sec, 2245 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
cisco4300#show processes cpu | include one minute
CPU utilization for five seconds: 1%/0%; one minute: 13%; five minutes: 4%
cisco4300#show interfaces gigabitEthernet0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 26670000 bits/sec, 2207 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
cisco4300#show processes cpu | include one minute
CPU utilization for five seconds: 1%/0%; one minute: 13%; five minutes: 4%
cisco4300#show interfaces gigabitEthernet0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 26227000 bits/sec, 2170 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
cisco4300#show processes cpu | include one minute
CPU utilization for five seconds: 1%/0%; one minute: 12%; five minutes: 4%
cisco4300#show interfaces gigabitEthernet0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 26227000 bits/sec, 2170 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
cisco4300#show processes cpu | include one minute
CPU utilization for five seconds: 1%/0%; one minute: 11%; five minutes: 3%
cisco4300#show interfaces gigabitEthernet0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 25791000 bits/sec, 2134 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
cisco4300#show interfaces gigabitEthernet0/0/0 | include rate
```

(iv) **Stop after 10 minutes** and save Wireshark capture.



11.4.4 **Test Observation:** The router handled the UDP flood scenario efficiently. The CPUusage showed only a slight increase, indicating that the router could manage a high volume of datagram traffic without significant performance degradation.

11.4.5 **Evidence Provided:** Screenshots of testing steps and Wireshark pcap files.

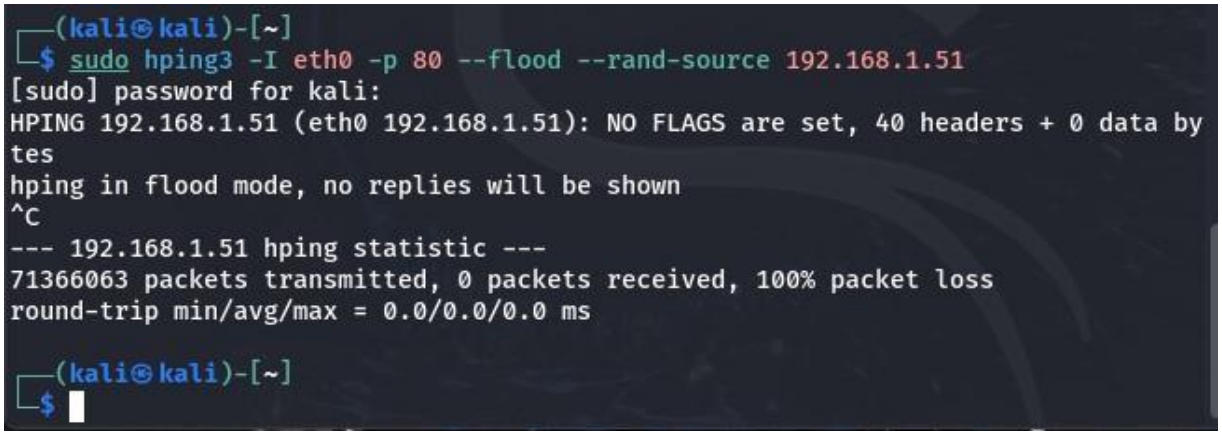
11.5 Test Case Number: 5

11.5.1 **Test Case Name:** TC_APPLICATION_HTTP_FLOODING

11.5.2 **Test Case description**: Perform application-level HTTP flooding to simulate a high volume of web requests.

11.5.3 **Execution Steps:**

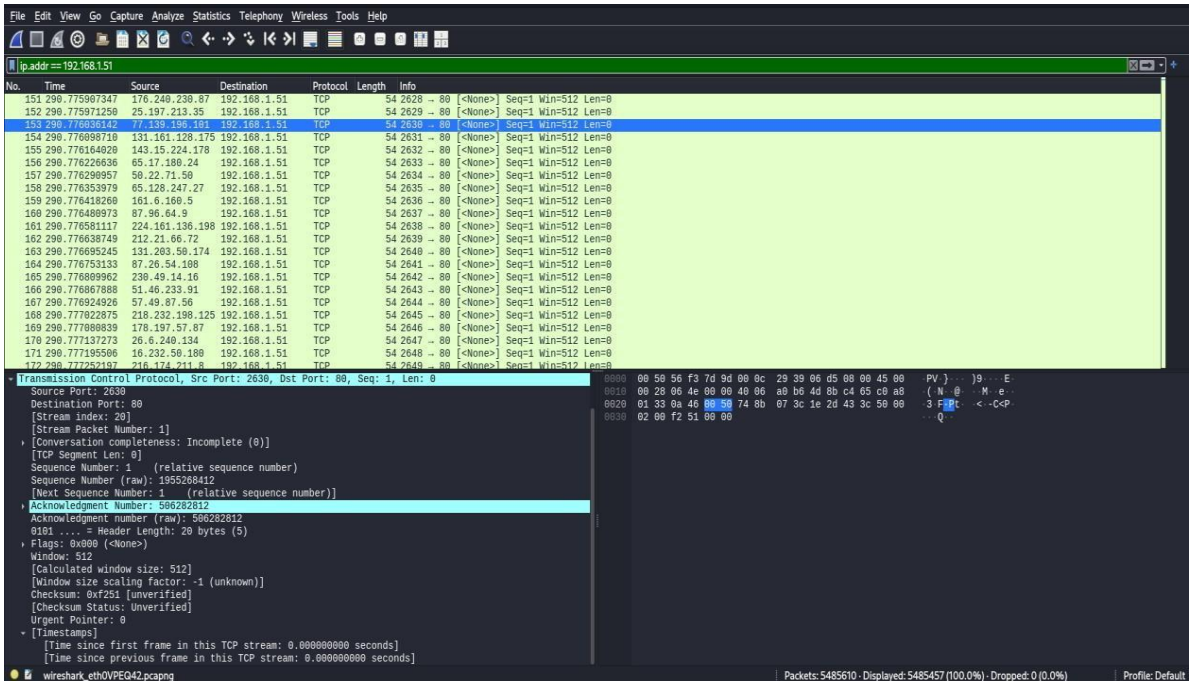
(i) Simulate HTTP flood using a script or tool to send HTTP GET requests rapidly: "sudo hping3 -I eth0 -p 80 --flood --rand-source 192.168.1.51



(ii)Monitor Router: On the DUT (router), run: show processes cpu | include one minute show interface GigabitEthernet1 | include rate

```
CPU utilization for five seconds: 4%/0%; one minute: 4%; five minutes: 3%
cisco4300#show interfaces gigabitEthernet0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 1386000 bits/sec, 93 packets/sec
  5 minute output rate 127000 bits/sec, 2 packets/sec
cisco4300#show processes cpu | include one minute
CPU utilization for five seconds: 4%/0%; one minute: 4%; five minutes: 3%
cisco4300#show interfaces gigabitEthernet0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 1363000 bits/sec, 91 packets/sec
  5 minute output rate 124000 bits/sec, 1 packets/sec
cisco4300#show processes cpu | include one minute
CPU utilization for five seconds: 1%/0%; one minute: 4%; five minutes: 3%
cisco4300#show interfaces gigabitEthernet0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 1363000 bits/sec, 91 packets/sec
  5 minute output rate 124000 bits/sec, 1 packets/sec
cisco4300#show processes cpu | include one minute
*Apr 10 09:00:27.500: %SYS-6-LOGOUT: User hari has exited tty session 866(10.10.10.50)
cisco4300#show processes cpu | include one minute
CPU utilization for five seconds: 1%/0%; one minute: 4%; five minutes: 3%
cisco4300#show interfaces gigabitEthernet0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 1340000 bits/sec, 89 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
cisco4300#show processes cpu | include one minute
CPU utilization for five seconds: 1%/0%; one minute: 4%; five minutes: 3%
cisco4300#show interfaces gigabitEthernet0/0/0 | include rate
  Queueing strategy: fifo
  5 minute input rate 1340000 bits/sec, 89 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
cisco4300#
*Apr 10 09:00:39.131: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http fro
m console as hari on vty1
cisco4300#
```

(iii) Stop after 5 minutes and save Wireshark capture.



11.5.4 **Test Observation:** The router managed the HTTP flood traffic effectively, demonstrating its capability to handle application-level DDoS attacks. CPU utilization increased as expected, but the system remained stable, with no critical performance issues or disruptions.

11.5.5 **Evidence Provided:** Screenshots of testing steps and Wireshark pcap files.

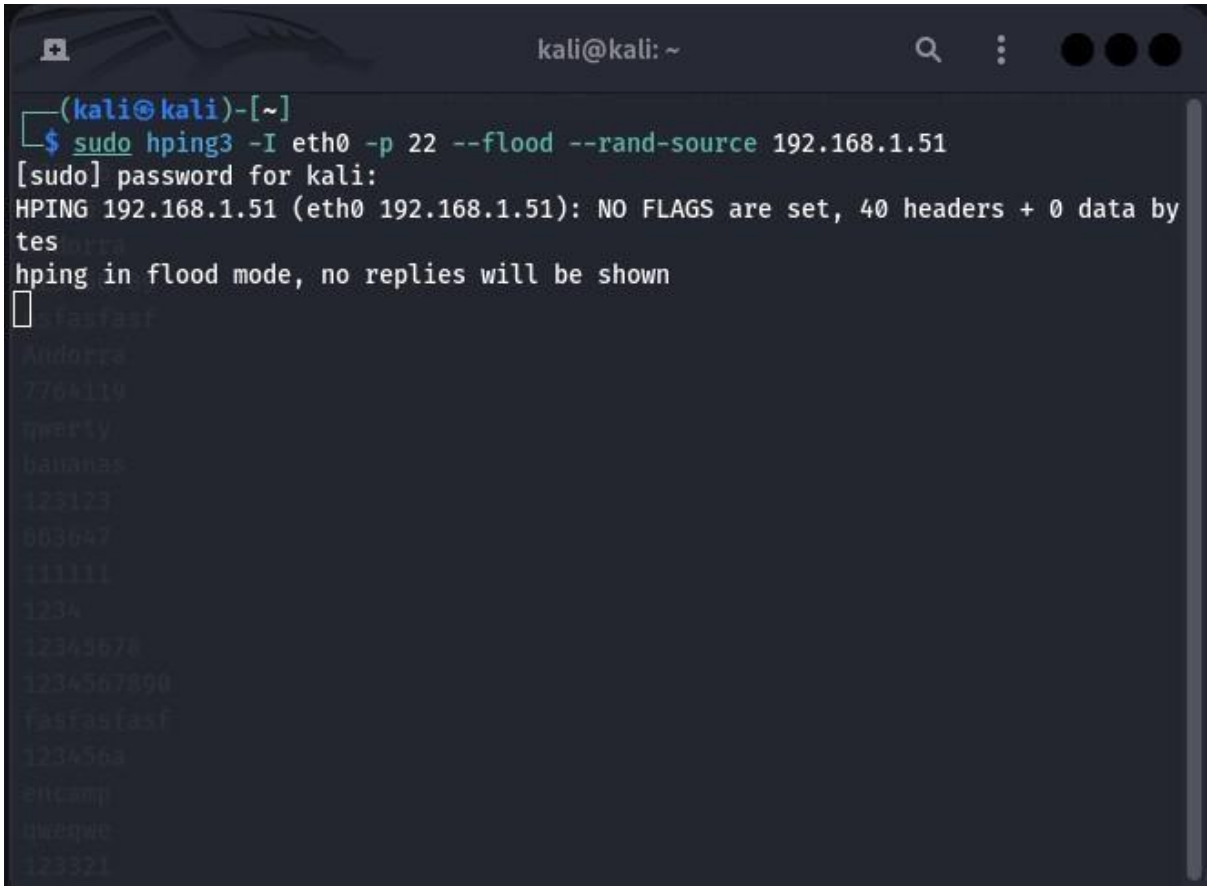
11.6 Test Case Number: 6

11.6.1 **Test Case Name:** TC_SSH_FLOODING

11.6.2 **Test Case description**: Perform SSH flooding to simulate a high volume of web requests.

11.6.3 **Execution Steps:**

Simulate SSHflood using a tool to send SSH GET requests rapidly: “sudo hping3 -I eth0 -p 22 --flood --rand-source 192.168.1.51



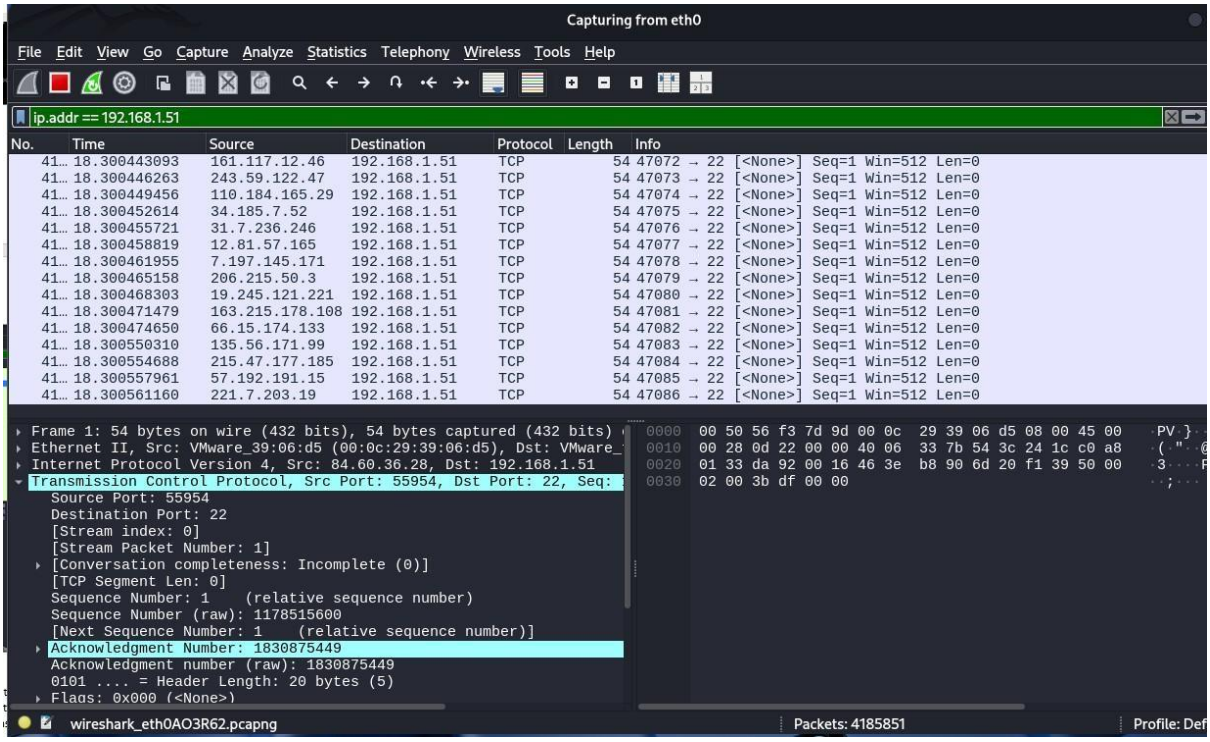
(ii) Monitor Router: On the DUT (router),

```
cisco4300#show interfaces gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4331-3x1GE, address is d0ec.35e5.d010 (bia d0ec.35e5.d010)
  Internet address is 192.168.1.51/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 57/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:29, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/1949494/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 225987000 bits/sec, 18652 packets/sec
  5 minute output rate 176000 bits/sec, 387 packets/sec
     246508952 packets input, 373082439878 bytes, 2794 no buffer
     Received 9477 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     196701 input errors, 0 CRC, 0 frame, 196701 overrun, 0 ignored
     0 watchdog, 84923 multicast, 0 pause input
     2668580 packets output, 160660234 bytes, 0 underruns
     Output 366 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 1 interface resets
     6234 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     5 lost carrier, 0 no carrier, 358802 pause output
     0 output buffer failures, 0 output buffers swapped out
cisco4300#
```

run: show processes cpu | include one minute show interface GigabitEthernet1 | include rate

```
cisco4300#show processes cpu | include five minute
CPU utilization for five seconds: 2%/0%; one minute: 1%; five minutes: 1%
cisco4300#show processes cpu
CPU utilization for five seconds: 1%/0%; one minute: 1%; five minutes: 1%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0          12          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2        1068        2413        442  0.00%  0.00%  0.00%   0 Load Meter
   3         311         277       1122  0.39%  0.18%  0.08%   0 Exec
   4           0           1          0  0.00%  0.00%  0.00%   0 Retransmission o
   5           0           1          0  0.00%  0.00%  0.00%   0 IPC ISSU Dispatc
   6          26          13       2000  0.00%  0.00%  0.00%   0 RF Slave Main Th
   7           0           1          0  0.00%  0.00%  0.00%   0 EDDRI_MAIN
   8           0           1          0  0.00%  0.00%  0.00%   0 RO Notify Timers
   9        7630        1801       4236  0.00%  0.08%  0.06%   0 Check heaps
  10         628       12207         51  0.00%  0.00%  0.00%   0 Pool Manager
  11           0           1          0  0.00%  0.00%  0.00%   0 DiscardQ Backgro
  12           0           2          0  0.00%  0.00%  0.00%   0 Timers
  13           4         327         12  0.00%  0.00%  0.00%   0 WATCH_AFS
  14           0           1          0  0.00%  0.00%  0.00%   0 MEMLEAK PROCESS
  15         641        4038        158  0.00%  0.00%  0.00%   0 ARP Input
  16         418       12478         33  0.00%  0.00%  0.00%   0 ARP Background
  17           0           2          0  0.00%  0.00%  0.00%   0 ATM Idle Timer
  18           0           1          0  0.00%  0.00%  0.00%   0 ATM ASYNC PROC
  19           0           1          0  0.00%  0.00%  0.00%   0 CEF MIB API
  20           0           3          0  0.00%  0.00%  0.00%   0 AAA_SERVER_DEADT
  21           0           1          0  0.00%  0.00%  0.00%   0 Policy Manager
  22           0           2          0  0.00%  0.00%  0.00%   0 DDR Timers
  23         199          12      16583  0.00%  0.00%  0.00%   0 Entity MIB API
  24          89          49       1816  0.00%  0.00%  0.00%   0 PrstVbl
  25           0           2          0  0.00%  0.00%  0.00%   0 Serial Backgroun
  26           0           1          0  0.00%  0.00%  0.00%   0 RMI RM Notify Wa
  27           0           2          0  0.00%  0.00%  0.00%   0 ATM AutoVC Perio
  28           0           2          0  0.00%  0.00%  0.00%   0 ATM VC Auto Crea
  29         200        5985         33  0.00%  0.00%  0.00%   0 IOSXE heartbeat
  30           3          22        136  0.00%  0.00%  0.00%   0 Btrace time base
  31           0           7          0  0.00%  0.00%  0.00%   0 DB Lock Manager
  32         271       11983         22  0.00%  0.00%  0.00%   0 GraphIt
  33           0           1          0  0.00%  0.00%  0.00%   0 DB Notification
 --More--
```

(iv) Stop after 5 minutes and save Wireshark capture.



11.6.4 **Test Observation:** The router managed the SSH flood traffic effectively, demonstrating its capability to handle application-level DDoS attacks. CPU utilization increased as expected, but the system remained stable, with no critical performance issues or disruptions.

11.6.5 **Evidence Provided:** Screenshots of testing steps and Wireshark pcap files.

11.7 **Test Case Number:** 7

11.7.1 **Test Case Name:** TC_TRAFFIC_GENERATOR

11.7.2 **Test Case description**: Test case to verify maximum capacity to reached while performing excessive overloading protection.

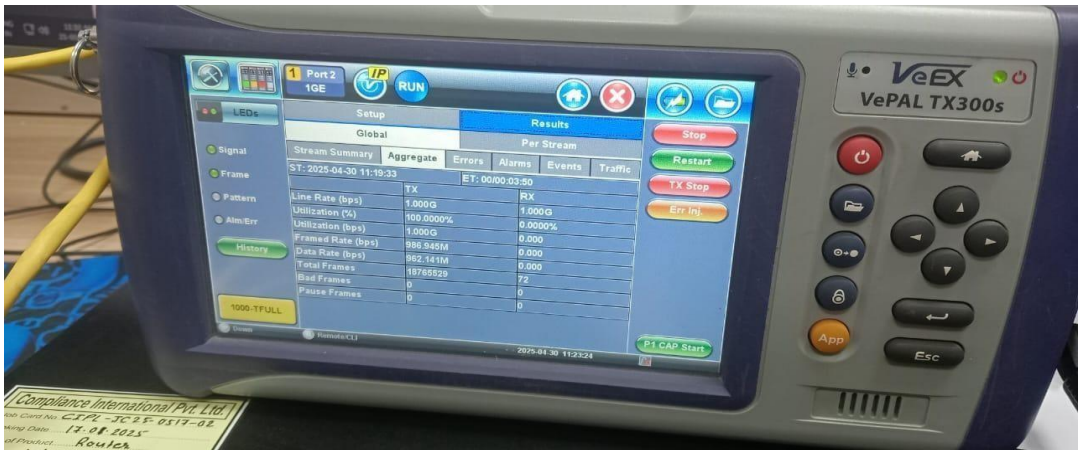
11.7.3 **Execution Steps:**

Check the DUT interface capacity input rate.

```
cisco4300#show interfaces gigabitEthernet 0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Hardware is ISR4331-3x1GE, address is d0ec.35e5.d011 (bia d0ec.35e5.d011)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:17, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     8 packets output, 3296 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
cisco4300#
cisco4300#
cisco4300#
cisco4300#
cisco4300#
cisco4300#
cisco4300#show interfaces gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4331-3x1GE, address is d0ec.35e5.d010 (bia d0ec.35e5.d010)
  Internet address is 192.168.1.51/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:04:04, output 00:00:10, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     93108 packets input, 16102639 bytes, 0 no buffer
     Received 8711 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 80436 multicast, 0 pause input

cisco4300#
```

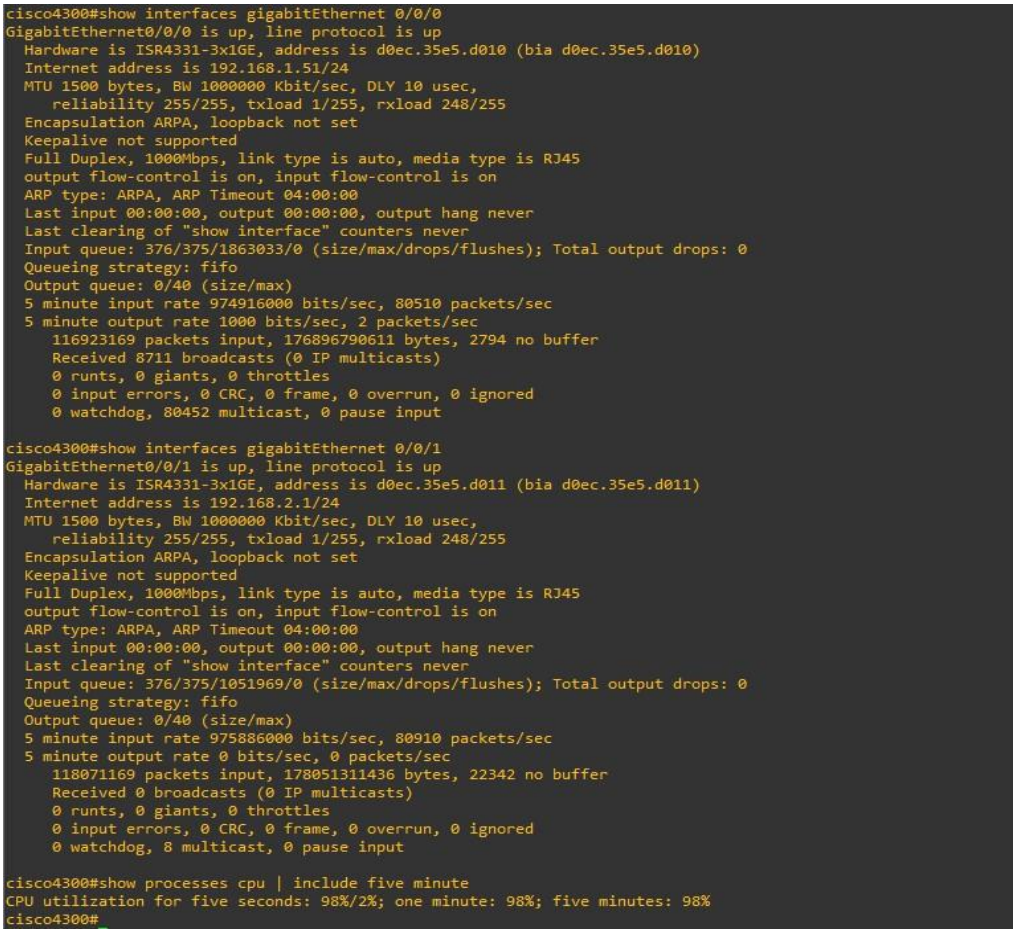
Above screenshot verify that the interface capacity is 100000 kbit/sec i.e 1 Gbps and input rate is 0 bit/sec before sending the traffic.

Generate the 1 Gbps traffic from VeEX traffic generator tool to DUT.



Monitor Router: On the router,

run: “show processes cpu | include one minute” “show interface GigabitEthernet0/0/0 | include rate



Above screenshot the verify the input rate approx. 100% and cpu utilization is 98% the DUT handled overload effectively. CPU usage increased but remained stable. No significant degradation in DUT availability was observed, indicating robust handling of DDoS attacks.

11.7.4 **Test Observation:** The DUT managed the Traffic flood traffic effectively, demonstrating its capability to handle 1 Gbps DDoS attacks. CPU utilization increased as expected, but the system remained stable, with no critical performance issues or disruptions.

11.7.5 **Evidence Provided:** Screenshots of testing steps and Wireshark pcap files.

12. **Test Case Result:**

S. No.	Test Case Name	Pass/Fail	Remarks
1	TC_OVERLOAD_CONTROL_MECHANISM_DDOS_AVOIDANCE_VERIFICATION	OEM Dependent	Documentation and system behavior should align, demonstrating that DDoS mitigation mechanisms are effectively implemented.
2	TC_ICMP_FLOODING	Pass	DUT maintained normal behaviour during the ICMP flood attack, CPU usage remained stable, and no significant packet loss or service disruption occurred. The ACL configuration on the router successfully mitigated the flooding impact.
3	TC_TCP_SYN_RST_FLOODING	Pass	DUT handled the TCP SYN flooding attack without significant degradation. CPU usage increased but remained within acceptable limits. The router's performance and stability were maintained.
4	TC_UDP_FLOODING	Pass	DUT exhibited normal behaviour during the UDP flood attack. CPU utilization was stable, and no significant packet loss or performance degradation was observed.
5	TC_HTTP_APPLICATION_FLOODING	Pass	DUT successfully managed the HTTP flood attack, demonstrating effective handling of high-volume application-level requests. CPU usage increased moderately but did not cause disruption.
6	TC_SSH_FLOODING	Pass	The router managed the SSH flood traffic effectively, demonstrating its capability to handle application-level DDoS attacks. CPU utilization increased as expected, but the system remained stable, with no critical performance issues or disruptions.
7	TC_TRAFFIC_GENERATOR	Pass	The DUT managed the Traffic flood traffic effectively, demonstrating its capability to handle 1 Gbps DDoS attacks. CPU utilization increased as expected, but the system remained stable, with no critical performance issues or disruptions.

2.8.3 TSTP for Filtering IP Options

<DUT Details: > WiFi CPE
<DUT Software Version:> cisco
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 2.0.0
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 2.8: Attack Prevention Mechanism
2. **<Security Requirement No & Name >** 2.8.3 Filtering IP Options
3. **<Requirement Description: >** IP packets with unnecessary options or extension headers shall not be processed. IP options and extension headers (e.g., source routing) are only required in exceptional cases. So, all packets with enabled IP options or extension headers shall be filtered.

4. **DUT Confirmation Details**:

- Use the command line interface to get details of the machine on which test is conducted.
- Use command: **show interface summary** to get Interfaces details
- Use command to get Application No/Version No & Kernel Info Verification of DUT by running command: **show version** on CLI.

Use command for show interface**: Sh int summary**

```
cisco4300#show version
Cisco IOS XE Software, Version 17.06.08a
Cisco IOS Software [Bengaluru], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Version 17.6.8a, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2024 by Cisco Systems, Inc.
Compiled Mon 14-Oct-24 08:01 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2024 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: (c)

cisco4300 uptime is 1 hour, 34 minutes
Uptime for this control processor is 1 hour, 36 minutes
 --More--
```

Use command for show interface**: Sh int summary**

```
cisco4300#show interfaces summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface                   IHQ       IQD       OHQ       OQD      RXBS      RXPS
    TXBS      TXPS      TRTL
------------------------------------------------------------------------------------
----------------------------
* GigabitEthernet0/0/0          0         0         0         0     13000         3
      0         0         0
  GigabitEthernet0/0/1          0         0         0         0         0         0
      0         0         0
  GigabitEthernet0/0/2          0         0         0         0         0         0
      0         0         0
  GigabitEthernet0              0         0         0         0         0         0
      0         0         0
cisco4300#
cisco4300#
```

Command: **show inventory**

```
cisco4300#show inventory

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

NAME: "Chassis", DESCR: "Cisco ISR4331 Chassis"
PID: ISR4331/K9        , VID: V07  , SN: FDO2304A2DL

NAME: "Power Supply Module 0", DESCR: "250W AC Power Supply for Cisco ISR 4330"
PID: PWR-4330-AC       , VID: V03  , SN: PST2252M0ZU

NAME: "Fan Tray", DESCR: "Cisco ISR4330 Fan Assembly"
PID: ACS-4330-FANASSY  , VID:      , SN:

NAME: "module 0", DESCR: "Cisco ISR4331 Built-In NIM controller"
PID: ISR4331/K9        , VID:      , SN:

NAME: "NIM subslot 0/0", DESCR: "Front Panel 3 ports Gigabitethernet Module"
PID: ISR4331-3x1GE     , VID: V01  , SN:

NAME: "module 1", DESCR: "Cisco ISR4331 Built-In SM controller"
PID: ISR4331/K9        , VID:      , SN:

NAME: "module R0", DESCR: "Cisco ISR4331 Route Processor"
PID: ISR4331/K9        , VID: V07  , SN: FDO23031J6Y

NAME: "module F0", DESCR: "Cisco ISR4331 Forwarding Processor"
PID: ISR4331/K9        , VID:      , SN:
 --More--
```

5. **<u>DUT Configuration:</u>**

Handling IPv4 option using ACL.

ACL configuration on DUT to filter IPv4 options:

```
cisco4300#c
Enter configuration commands, one per line.  End with CNTL/Z.
cisco4300(config)#ip acc
cisco4300(config)#ip access-list ex
cisco4300(config)#ip access-list extended option
cisco4300(config-ext-nacl)#deny ip any any option reco
cisco4300(config-ext-nacl)#deny ip any any option record-route log-input
cisco4300(config-ext-nacl)#end
cisco4300#
```

Acl deny rule is to reject or filter the ipv4-option enable with record route. Acl's permit rule is to accept all other options.

Applying ACL on interface Gigabit Ethernet 0/0/0

```
cisco4300(config)#interface gigabitEthernet 0/0/0
cisco4300(config-if)#ip acc
cisco4300(config-if)#ip access-group option in
cisco4300(config-if)#
```

Handling of ipv6-extension header:

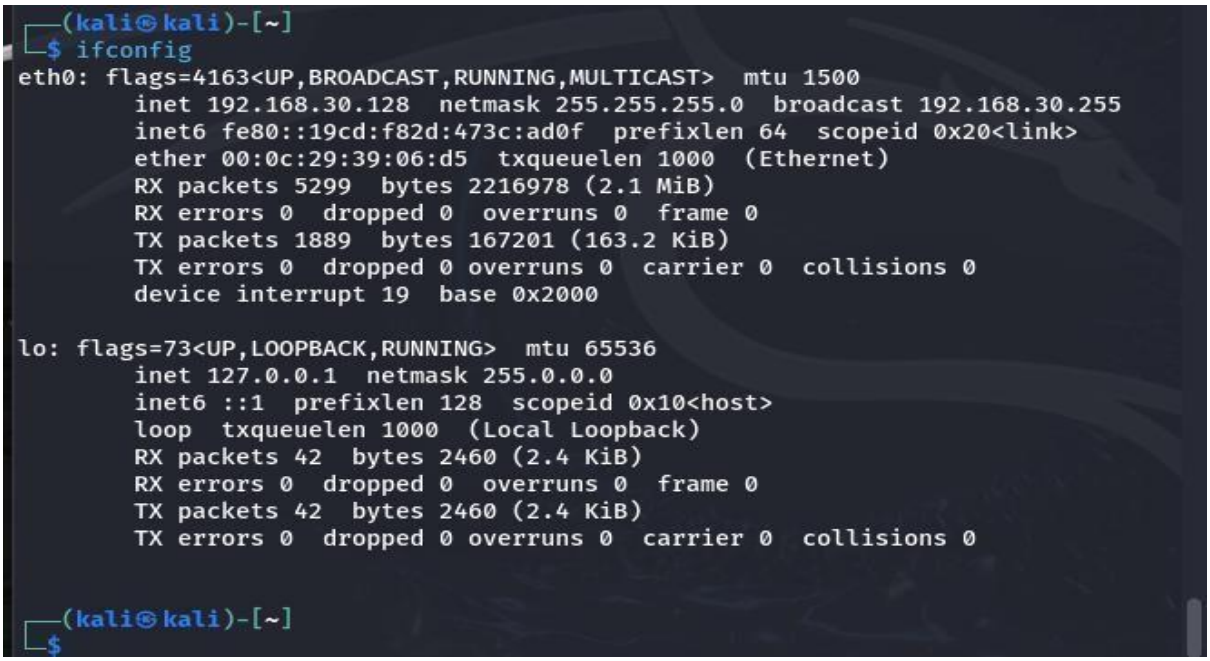
Configure acl to filter Extension Header9 (Hop by-Hop) ipv6-option. Acl to deny ExtHdr-hbh and permit all other.

Acl to deny tcp host and permit tcp eq telnet

```
cisco4300(config)#ipv6 access-list DENY_HBH_OPIONS
cisco4300(config-ipv6-acl)#per
cisco4300(config-ipv6-acl)#permit any any log-
cisco4300(config-ipv6-acl)#permit any any log-input hbh
cisco4300(config-ipv6-acl)#deny
cisco4300(config-ipv6-acl)#deny an
cisco4300(config-ipv6-acl)#deny any an
cisco4300(config-ipv6-acl)#deny any any log
cisco4300(config-ipv6-acl)#deny any any log-
cisco4300(config-ipv6-acl)#deny any any log-input hbh
cisco4300(config-ipv6-acl)#end
cisco4300#
*Apr 10 10:54:17.967: %SYS-5-CONFIG_I: Configured from console by root on consol
e
cisco4300#sh
cisco4300#show ipv
cisco4300#show ipv6 acc
cisco4300#show ipv6 access-list
IPv6 access list DENY_HBH_OPIONS
    permit ipv6 any any log-input hbh sequence 10
    deny ipv6 any any log-input hbh sequence 20
cisco4300#
```

```
cisco4300(config)#interface gigabitEthernet 0/0/0
cisco4300(config-if)#ipv
cisco4300(config-if)#ipv6 tra
cisco4300(config-if)#ipv6 traffic-filter deny
cisco4300(config-if)#ipv6 traffic-filter deny-hbh-options in
cisco4300(config-if)#
```

VMware(Kali) Machine IP details mention in below screenshot.



6. **<u>Preconditions</u>**
   - The manufacturer declares in the documentation accompanying the network product at least the following information:
   - The support of filtering capability for IP packets with unnecessary options or extensions headers.
   - The actions performed by the network product when an IP packet with unnecessary options or extensions headers is received (e.g. the packet is dropped, the options or extensions are ignored and the packet is treated as if it has no IP options, etc.) .
   - Guidelines on how to enable and configure this filtering capability.
   - The network product has at least one physical interface named if1 supporting both IPv4 and IPv6. If the network product does not support IPv6 then IPv6 related steps and checks may be skipped.
   - A network traffic analyser on the network product (e.g. TCPDUMP) or an external traffic analyser directly connected to the network product is available .
   - The tester has administrative privileges.
   - A tester machine is available with a tool able to send IPv4 packets with the IP Options and IPv6 packets (if supported by the network product) with Extension Header set (e.g. Scapy).

7. **<u>Test Objective</u>**: To verify that the network product provides functionality to filter out IP packets with unnecessary options or extension headers.

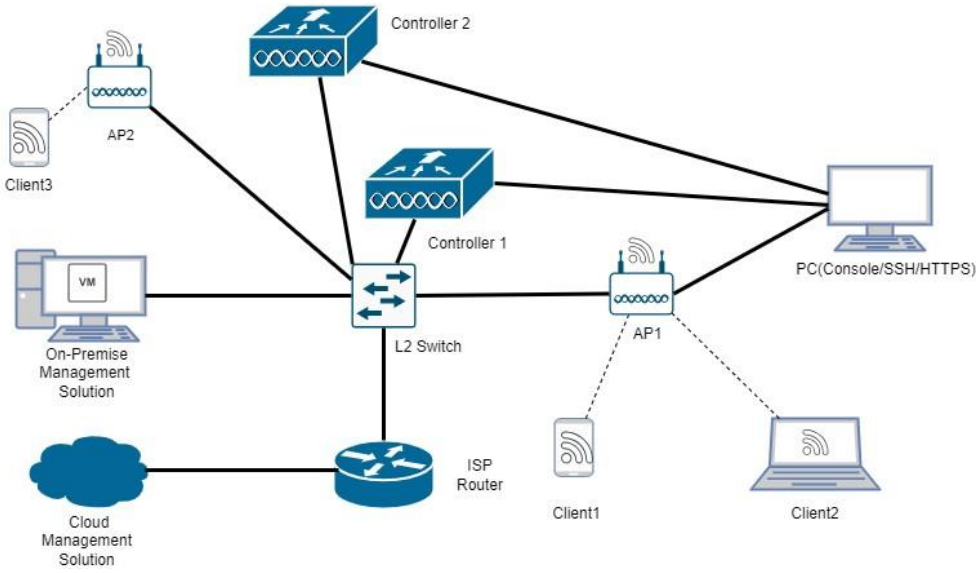
8. **<u>Test Plan:</u>**

   8.1. **Number of Test Scenarios: 3**

8.1.1 IP_OPTIONS_FILTERING
8.1.2 EXTENSION_HEADERS_FILTERING
8.1.3 EXCEPTIONAL_FILTERING

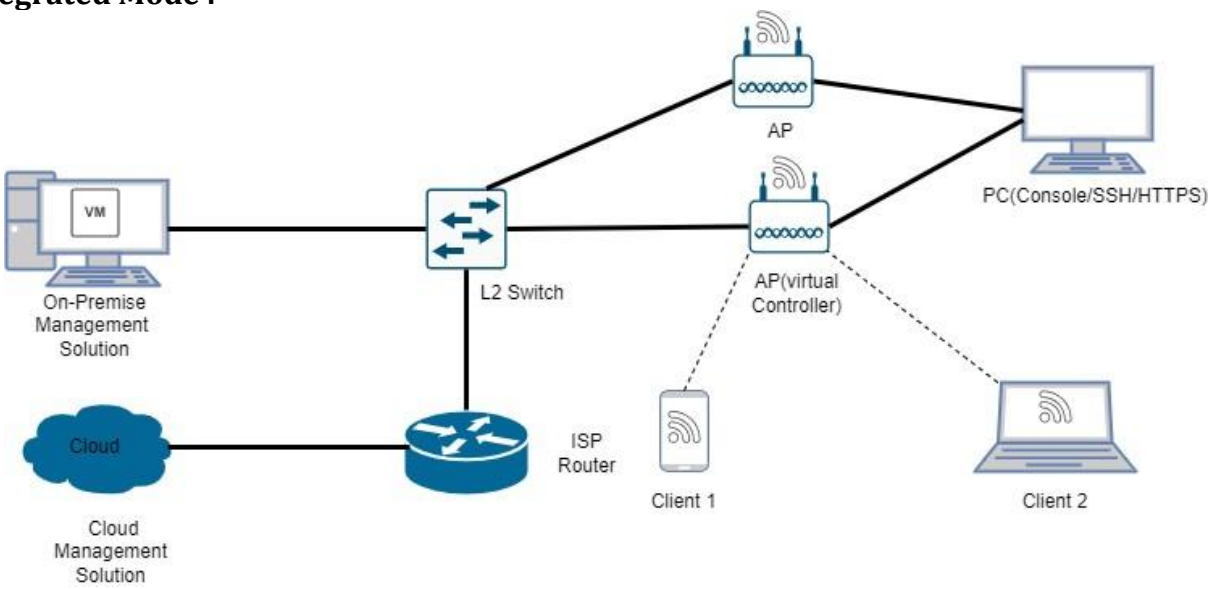
8.2. **Test Setup Diagram:**

AP + Controller mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

8.3 **Tools Used:**

- Scapy-python,
- wireshark,
- Putty

8.4 **Test Execution Steps**

1. The tester logs in the network product.
2. The tester configures on the network product a filtering rule to drop all IP packets containing an IP Option set
    a. The tester establishes an O&M session on if1 interface
    b. Using the tool (e.g. Scapy) the tester sends from the tester machine an IPv4 TCP SYN packet with an appropriate destination port to if1 interface without setting any IP Options
    c. Using the network traffic analyser, the tester verifies that the IP packet is received by the network product and the tester verifies that the corresponding ACK message is sent back.
    d. Using the tool (e.g. Scapy) the tester sends an IPv4 TCP SYN packet with an appropriate destination port and an IP Option set to the if1 interface
    e. Using the network traffic analyser, the tester verifies that the IP packet is received by the network product but no ACK message is sent back. This confirms the packet is dropped as expected from the filtering rule.
3. The tester configures on the network product a filtering rule to drop all incoming packets based on specific Extension Header Types, e.g. packets with the Routing Header extension. Step 3 may be skipped if the network product does not support IPv6.
    a. Using the tool (e.g. Scapy) the tester sends from the tester machine an IPv6 TCP SYN packet with an appropriate destination port to if1 interface without setting any extension header
    b. Using the network traffic analyser, the tester verifies that the IP packet is received by the network product and the tester verifies that the corresponding ACK message is sent back.
    c. Using the tool (e.g. Scapy) the tester sends an IPv6 TCP SYN packet with an appropriate destination port and an extension header set to the if1 interface
    d. Using the network traffic analyser, the tester verifies that the IP packet is received by the network product but no ACK message is sent back. This confirms the packet is dropped as expected from the filtering rule.

9. **Expected Results for Pass:** The network product discards IPv4 packets with unnecessary options or IPv6 packets (assuming the network product supports IPv6) with extension header.

10. **Expected Format of Evidence:**
    - Pcap trace
    - Screenshot

11. **Test Execution:**

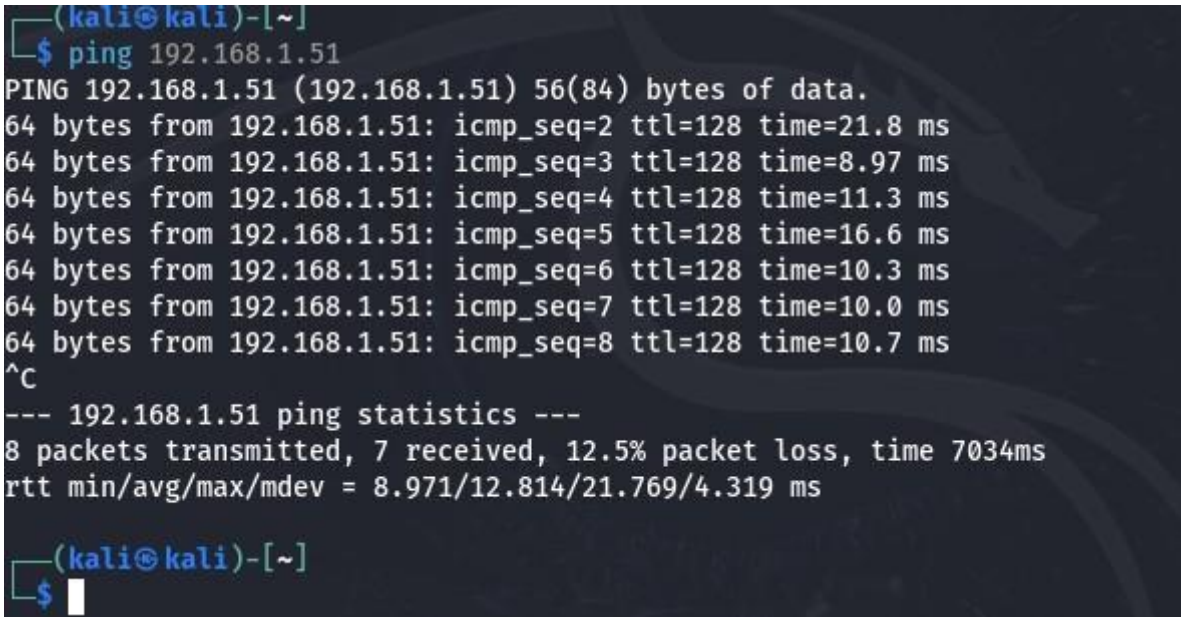
11.1 Test Case Number: 01

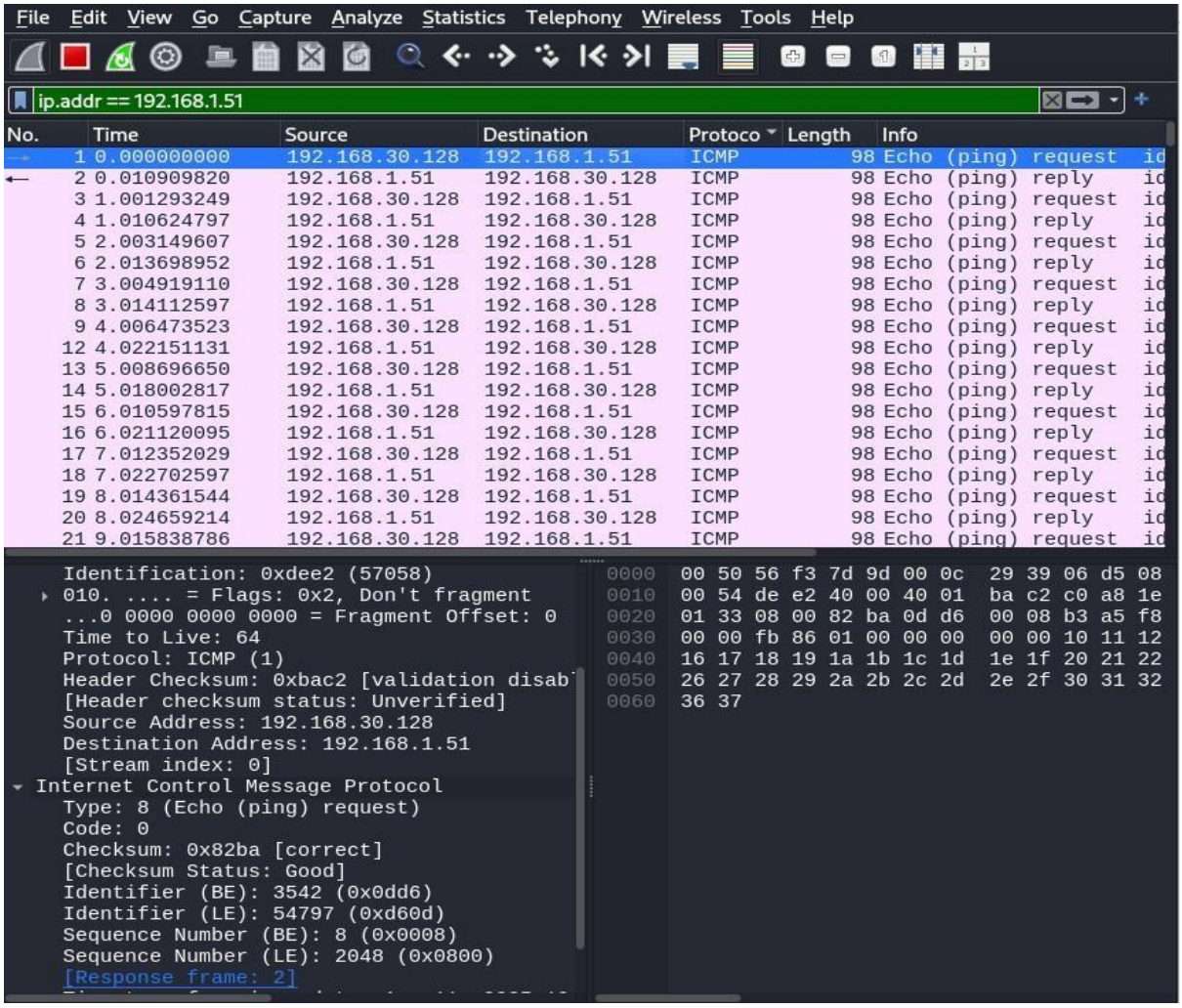
11.1.1 **Test Case Name:** IP_OPTIONS_FILTERING

11.1.2 **Test Case Description:** Verify that IP packets with unnecessary options shall not be processed.

11.1.3 **Execution Steps:**

DUT ping from tester machine: Before ACL apply.



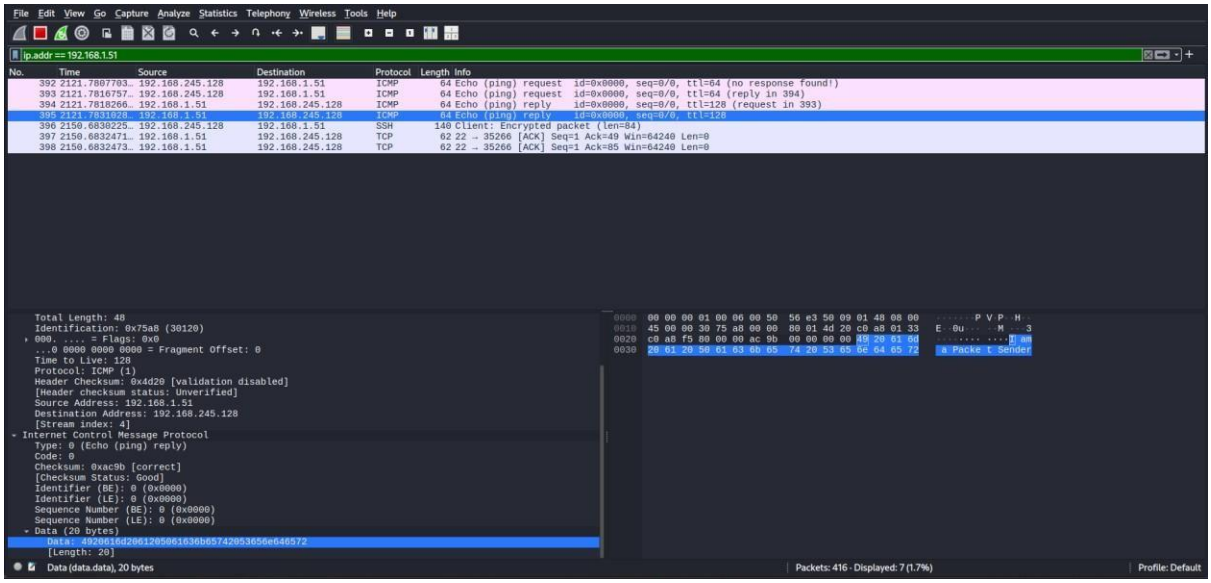


Above screenshot showing that tester machine, can getting ping reply from DUT.

Send ICMP Packet Using Scapy: Before ACL apply

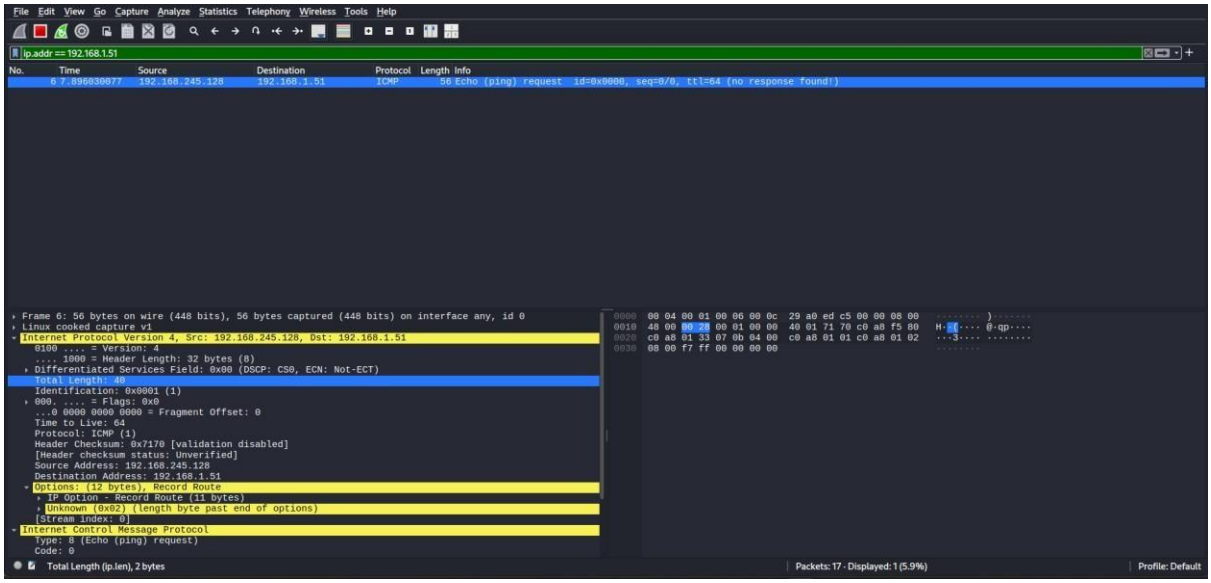
```
┌──(kali㉿kali)-[/home/kali]
└─PS> sudo scapy
[sudo] password for kali:
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().

                     aSPY//YASa
             apyyyyCY//////////YCa       |
            sY//////YSpcs  scpCY//Pp     | Welcome to Scapy
 ayp ayyyyyyySCP//Pp           syY//C    | Version 2.6.1
 AYAsAYYYYYYYY///Ps              cY//S   |
         pCCCCY//p          cSSps y//Y   | https://github.com/secdev/scapy
         SPPPP///a          pP///AC//Y   |
              A//A            cyP////C   | Have fun!
              p///Ac            sC///a   |
              P////YCpc           A//A   | Craft packets before they craft
       scccccp///pSP///p          p//Y   | you.
      sY/////////y  caa           S//P   |                     -- Socrate
       cayCyayP//Ya              pY/Ya   |
        sY/PsY////YCc          aC//Yp
         sc  sccaCY//PCypaapyCP//YSs
                  spCPY//////YPSps
                       ccaacs

                                       using IPython 8.30.0

>>> x=IP(ttl=64)
>>> x.src="192.168.245.128"
>>> x.dst="192.168.1.51"
>>> x=x/ICMP()/"I am a Packet Sender"
>>> send(x,count=2)
..
Sent 2 packets.
>>>
```

Packet is captured via Wireshark on kali, to see the packets running from kali as source (192.168.245.128) & DUT interface as destination (192.168.1.51)



Sent the packet with IP options by scapy: Before ACL apply

```
>>> rr_option = IPOption(b'\x07\x0B\x04\x00' + b'\xc0\xa8\x01\x01' + b'\xc0\xa8\x01\x02')
>>> pkt = IP(dst="192.168.1.51", options=[rr_option]) / ICMP()
>>> send(pkt)
.
Sent 1 packets.
>>>
```



The DUT does not respond to IP packets containing the Record Route (RR) option because, by default, Cisco IOS XE ignores IP packets with IP options for performance and security reasons

Create ACL on DUT.

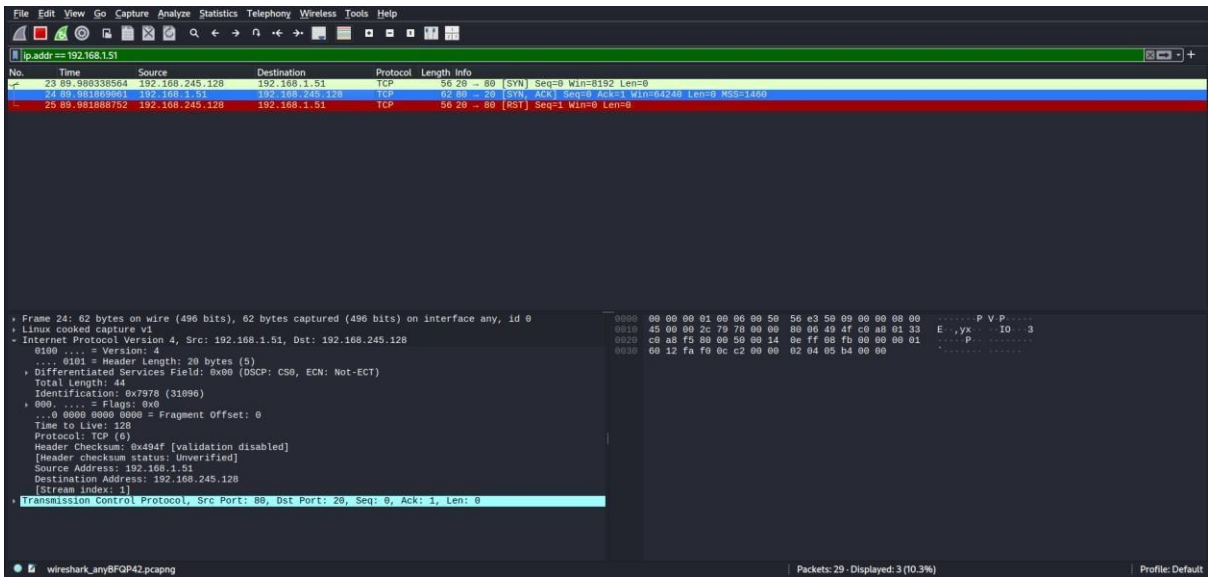
```
cisco4300(config)#ip access-list extended BLOCK_IP_OPTIONS
cisco4300(config-ext-nacl)# deny ip any any option any-options
cisco4300(config-ext-nacl)#permit ip any any
```

Applying ACL on interface GigabitEthernet0/0/0

```
cisco4300(config)#ip access-list extended BLOCK_IP_OPTIONS
cisco4300(config-ext-nacl)# deny ip any any option any-options
cisco4300(config-ext-nacl)#permit ip any any
cisco4300(config-ext-nacl)#interface GigabitEthernet0/0/0
cisco4300(config-if)#ip access-group BLOCK_IP_OPTIONS in
cisco4300(config-if)#
```

After ACL applied Sent the packet without IP options by scapy and captured the Wireshark packets

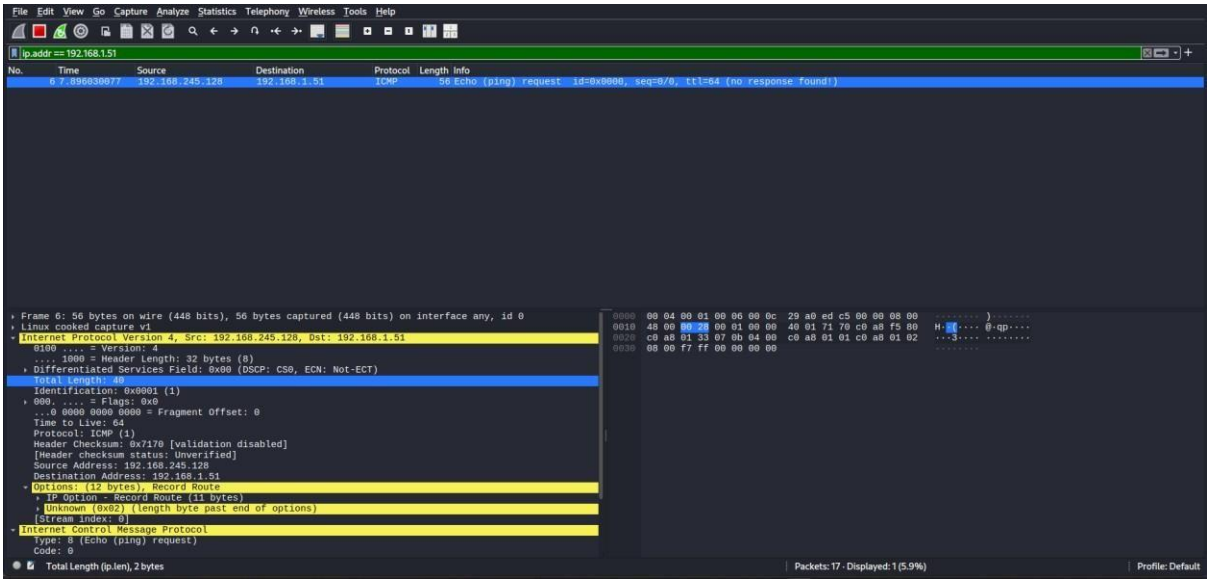
```
┌──(kali㉿kali)-[/home/kali]
└─PS> sudo scapy
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().

                     aSPY//YASa
             apyyyyCY//////////YCa       |
            sY//////YSpcs  scpCY//Pp     | Welcome to Scapy
 ayp ayyyyyyySCP//Pp           syY//C    | Version 2.6.1
 AYAsAYYYYYYYY///Ps              cY//S   |
         pCCCCY//p          cSSps y//Y   | https://github.com/secdev/scapy
         SPPPP///a          pP///AC//Y   |
              A//A            cyP////C   | Have fun!
              p///Ac            sC///a   |
              P////YCpc           A//A   | I'll be back.
       scccccp///pSP///p          p//Y   |                      -- Python 2
      sY/////////y  caa           S//P   |
       cayCyayP//Ya              pY/Ya
        sY/PsY////YCc           aC//Yp
         sc  sccaCY//PCypaapyCP//YSs
                  spCPY//////YPSps
                       ccaacs

                                       using IPython 8.30.0
>>> pkt = IP(dst="192.168.1.51") / TCP(dport=80, flags='S')
>>> send(pkt)
.
Sent 1 packets.
>>>
```



The screenshot above confirms that the DUT successfully received an IP packet without any IP options, and an ACK response was generated accordingly.

After ACL applied Sent the packet with IP options by scapy and captured the Wireshark packets

```
>>> rr_option = IPOption(b'\x07\x0B\x04\x00' + b'\xc0\xa8\x01\x01' + b'\xc0\xa8\x01\x02')
>>> pkt = IP(dst="192.168.1.51", options=[rr_option]) / ICMP()
>>> send(pkt)
.
Sent 1 packets.
>>>
```



The screenshot above confirms that the DUT received an IP packet containing an IP option, and no corresponding ACK message was sent in response.

11.1.4 **Test Observations:** It is observed from the Wireshark output that DUT drops IPv4 packet with IP option set and there is no response seen from DUT. This is also the default behaviour of DUT without ACL.

11.2 Test Case Number: 2

11.2.1 **Test Case Name:** EXTENSION_HEADERS_FILTERING

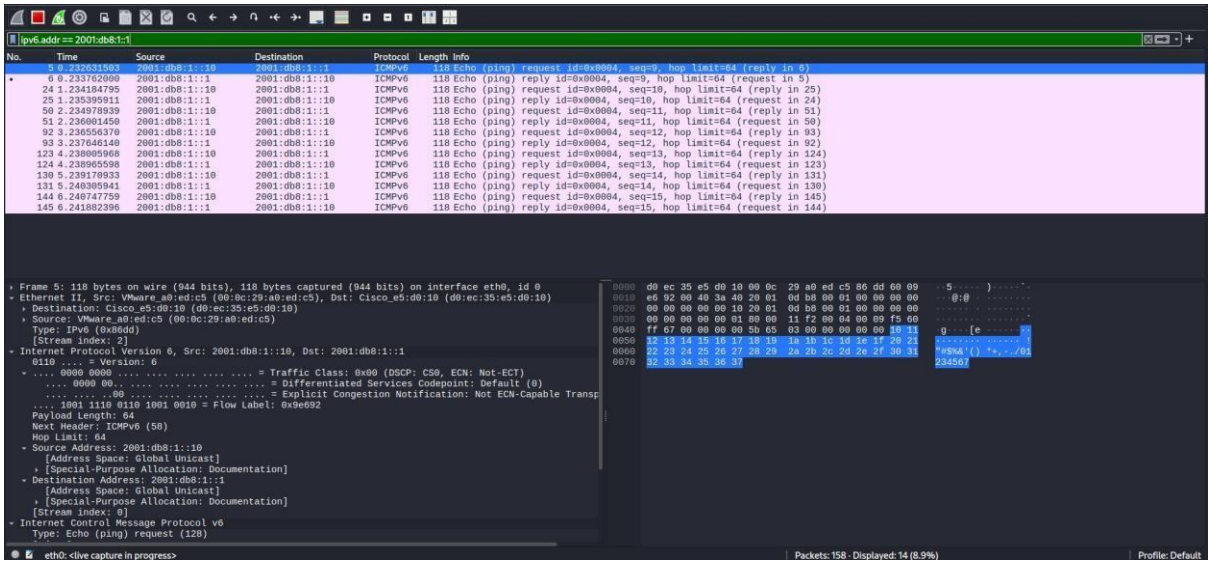
11.2.2 **Test Case Description:** Verify that IP packets (ipv6) with unnecessary extension headers shall not be processed.

11.2.3 **Execution Steps:**

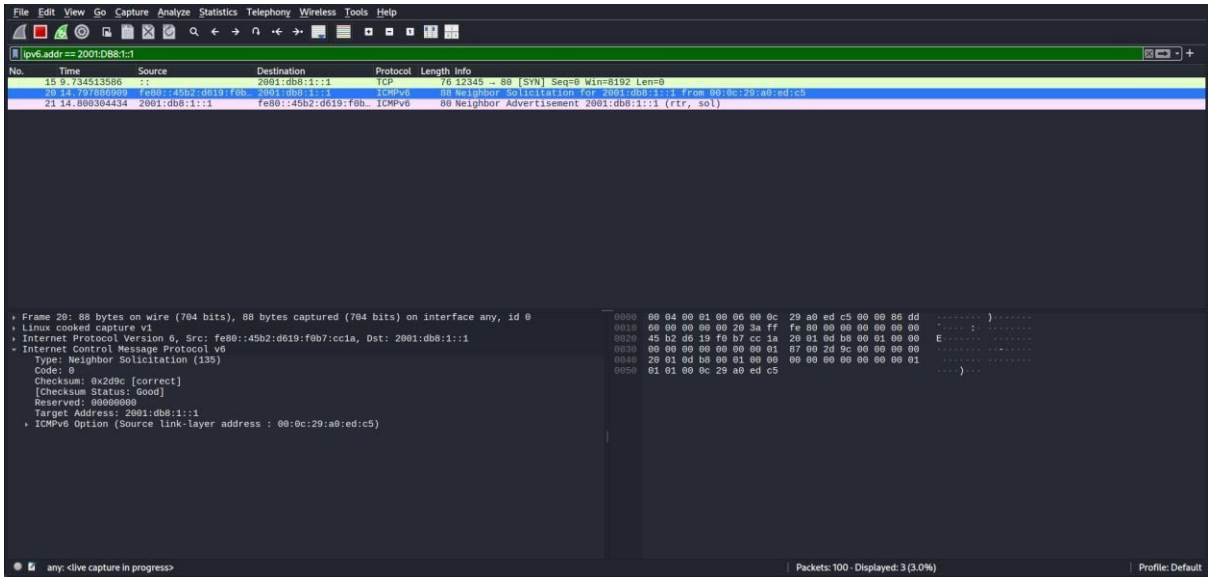
"ICMP –Ipv6"

DUT ping from tester machine: Before ACL apply.

```
┌──(kali㉿kali)-[~]
└─$ ping 2001:db8:1::1
PING 2001:db8:1::1 (2001:db8:1::1) 56 data bytes
64 bytes from 2001:db8:1::1: icmp_seq=1 ttl=64 time=3.40 ms
64 bytes from 2001:db8:1::1: icmp_seq=2 ttl=64 time=1.17 ms
64 bytes from 2001:db8:1::1: icmp_seq=3 ttl=64 time=1.17 ms
64 bytes from 2001:db8:1::1: icmp_seq=4 ttl=64 time=1.09 ms
64 bytes from 2001:db8:1::1: icmp_seq=5 ttl=64 time=1.13 ms
64 bytes from 2001:db8:1::1: icmp_seq=6 ttl=64 time=1.27 ms
64 bytes from 2001:db8:1::1: icmp_seq=7 ttl=64 time=1.30 ms
64 bytes from 2001:db8:1::1: icmp_seq=8 ttl=64 time=1.05 ms
64 bytes from 2001:db8:1::1: icmp_seq=9 ttl=64 time=1.15 ms
64 bytes from 2001:db8:1::1: icmp_seq=10 ttl=64 time=1.23 ms
64 bytes from 2001:db8:1::1: icmp_seq=11 ttl=64 time=1.05 ms
64 bytes from 2001:db8:1::1: icmp_seq=12 ttl=64 time=1.11 ms
64 bytes from 2001:db8:1::1: icmp_seq=13 ttl=64 time=0.984 ms
64 bytes from 2001:db8:1::1: icmp_seq=14 ttl=64 time=1.16 ms
64 bytes from 2001:db8:1::1: icmp_seq=15 ttl=64 time=1.15 ms
64 bytes from 2001:db8:1::1: icmp_seq=16 ttl=64 time=1.07 ms
64 bytes from 2001:db8:1::1: icmp_seq=17 ttl=64 time=1.05 ms
64 bytes from 2001:db8:1::1: icmp_seq=18 ttl=64 time=1.14 ms
64 bytes from 2001:db8:1::1: icmp_seq=19 ttl=64 time=1.08 ms
64 bytes from 2001:db8:1::1: icmp_seq=20 ttl=64 time=0.984 ms
64 bytes from 2001:db8:1::1: icmp_seq=21 ttl=64 time=1.22 ms
64 bytes from 2001:db8:1::1: icmp_seq=22 ttl=64 time=1.22 ms
64 bytes from 2001:db8:1::1: icmp_seq=23 ttl=64 time=1.18 ms
64 bytes from 2001:db8:1::1: icmp_seq=24 ttl=64 time=1.70 ms
64 bytes from 2001:db8:1::1: icmp_seq=25 ttl=64 time=1.14 ms
64 bytes from 2001:db8:1::1: icmp_seq=26 ttl=64 time=1.18 ms
64 bytes from 2001:db8:1::1: icmp_seq=27 ttl=64 time=1.05 ms
64 bytes from 2001:db8:1::1: icmp_seq=28 ttl=64 time=1.02 ms
64 bytes from 2001:db8:1::1: icmp_seq=29 ttl=64 time=1.34 ms
64 bytes from 2001:db8:1::1: icmp_seq=30 ttl=64 time=1.46 ms
64 bytes from 2001:db8:1::1: icmp_seq=31 ttl=64 time=1.31 ms
64 bytes from 2001:db8:1::1: icmp_seq=32 ttl=64 time=1.41 ms
```




```
>>> pkt = IPv6(dst="2001:DB8:1::1") / TCP(dport=80, sport=12345, flags='S')
>>> send(pkt)
WARNING: No route found for IPv6 destination 2001:db8:1::1 (no default route?)
WARNING: No route found for IPv6 destination 2001:db8:1::1 (no default route?)
WARNING: more No route found for IPv6 destination 2001:db8:1::1 (no default route?)
.
Sent 1 packets.
>>>
```



Create ACL on DUT.

```
cisco4300(config)#
cisco4300(config)#ipv6 access-list BLOCK-EXT-HDR
cisco4300(config-ipv6-acl)#deny ipv6 any any routing
cisco4300(config-ipv6-acl)# deny ipv6 any any hbh
cisco4300(config-ipv6-acl)# deny ipv6 any any dest-option
cisco4300(config-ipv6-acl)# deny ipv6 any any fragments
cisco4300(config-ipv6-acl)# deny ipv6 any any auth
cisco4300(config-ipv6-acl)#
cisco4300(config-ipv6-acl)# deny ipv6 any any mobility
cisco4300(config-ipv6-acl)# permit ipv6 any any
cisco4300(config-ipv6-acl)#
```

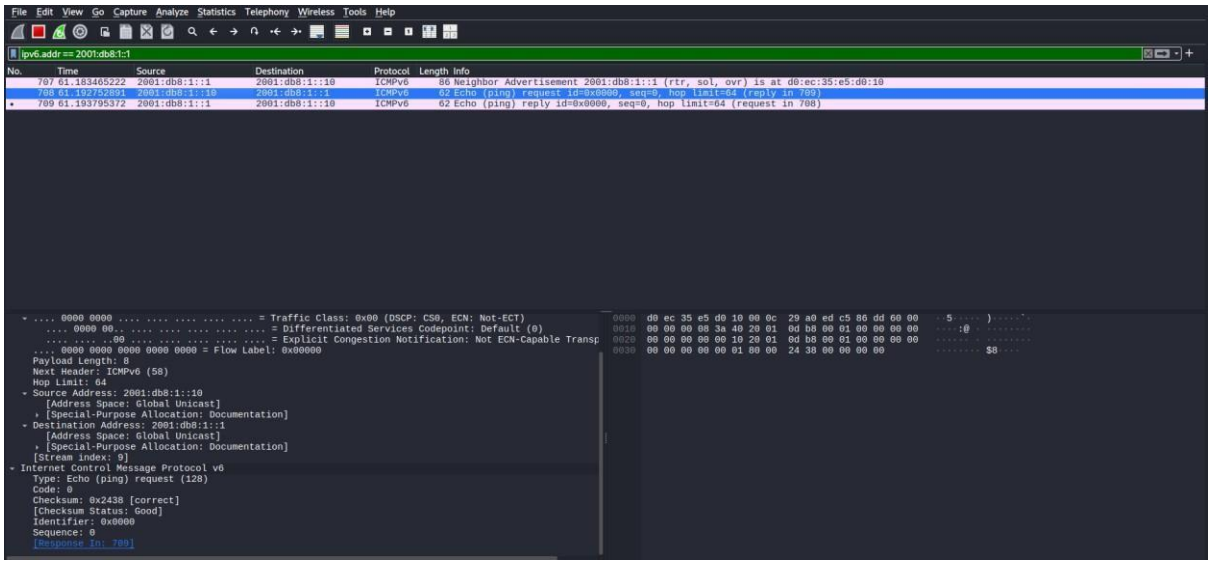
```
cisco4300(config-ipv6-acl)#deny ipv6 any any ?
  auth                  Match on authentication header
  dest-option           Destination Option header (all types)
  dest-option-type      Destination Option header with type
  dscp                  Match packets with given dscp value
  flow-label            Flow label
  fragments             Check non-initial fragments
  hbh                   Match on hop-by-hop option
  log                   Log matches against this entry
  log-input             Log matches against this entry, including input
  mobility              Mobility header (all types)
  mobility-type         Mobility header with type
  routing               Routing header (all types)
  routing-type          Routing header with type
  sequence              Sequence number for this entry
  time-range            Specify a time-range
  undetermined-transport  Transport cannot be determined or is missing
  <cr>                  <cr>
```

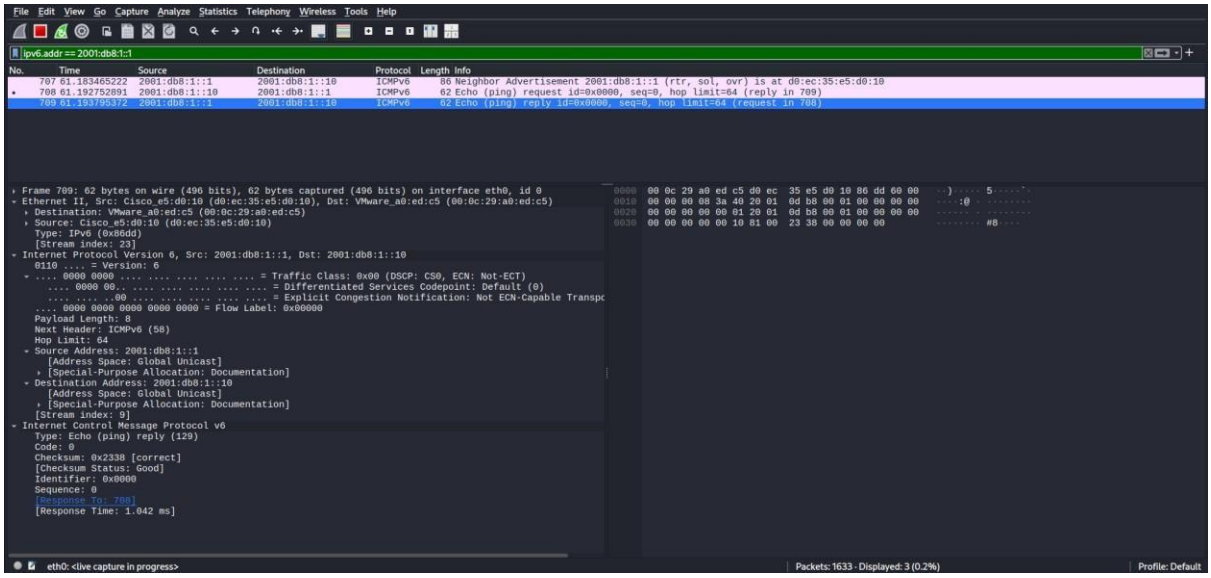
Applying ACL on interface GigabitEthernet0/0/0

```
cisco4300(config-if)#interface GigabitEthernet0/0/0
cisco4300(config-if)#ipv6 traffic-filter BLOCK-EXT-HDR in
cisco4300(config-if)#
```

After ACL applied Sent the packet without extension headers by scapy and captured the Wireshark packets

```
┌──(kali㉿kali)-[~]
└─$ sudo scapy
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().

                     aSPY//YASa
                apyyyyCY//////////YCa       |
               sY//////YSpcs  scpCY//Pp     | Welcome to Scapy
 ayp ayyyyyyySCP//Pp           syY//C      | Version 2.6.1
 AYAsAYYYYYYYY///Ps              cY//S     |
         pCCCCY//p          cSSps y//Y     | https://github.com/secdev/scapy
         SPPPP///a          pP///AC//Y     |
              A//A            cyP////C     | Have fun!
              p///Ac            sC///a     |
              P////YCpc           A//A     | Craft packets like I craft my beer.
       scccccp///pSP///p          p//Y     |                  -- Jean De Clerck
      sY/////////y  caa           S//P     |
       cayCyayP//Ya              pY/Ya
        sY/PsY////YCc           aC//Yp
         sc  sccaCY//PCypaapyCP//YSs
                  spCPY//////YPSps
                       ccaacs

                                       using IPython 8.30.0
>>> send(IPv6(dst="2001:db8:1::1")/ICMPv6EchoRequest())
.
Sent 1 packets.
>>>
```

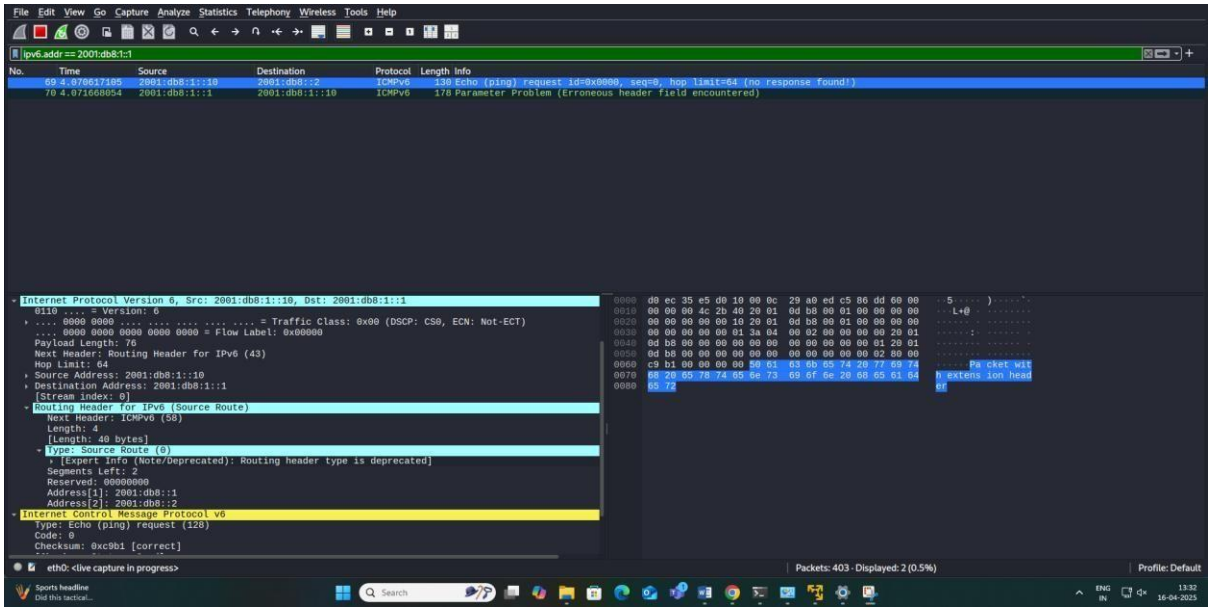


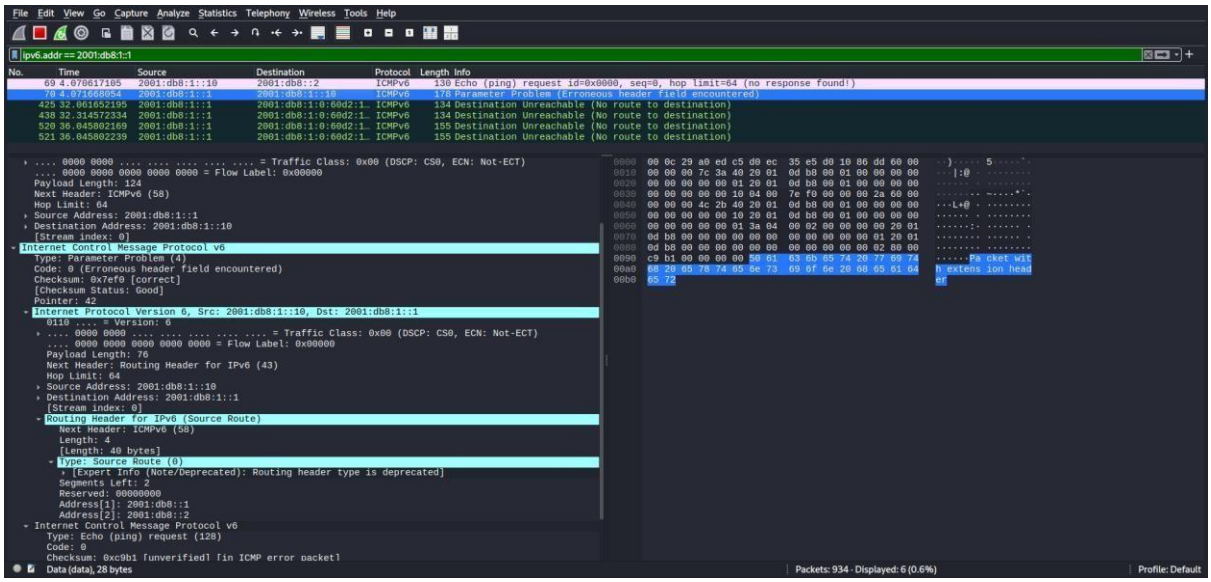


The screenshot above confirms that the DUT successfully received an IP packet without any extension headers, and an reply was generated accordingly.

After ACL applied Sent the packet with extension headers by scapy and captured the Wireshark packets

```
>>> routing_header = IPv6ExtHdrRouting(addresses=["2001:db8::1", "2001:db8::2"])
>>> pkt_with_options = IPv6(dst="2001:db8:1::1") / routing_header / ICMPv6EchoRequest() / Raw(load="Packet with extension header")
>>> pkt_with_options.show()
###[ IPv6 ]###
  version   = 6
  tc        = 0
  fl        = 0
  plen      = None
  nh        = Routing Header
  hlim      = 64
  src       = 2001:db8:1::10
  dst       = 2001:db8:1::1
###[ IPv6 Option Header Routing ]###
     nh        = ICMPv6
     len       = None
     type      = 0
     segleft   = None
     reserved  = 0
     addresses = [ 2001:db8::1, 2001:db8::2 ]
###[ ICMPv6 Echo Request ]###
        type      = Echo Request
        code      = 0
        cksum     = None
        id        = 0x0
        seq       = 0x0
        data      = b''
###[ Raw ]###
           load      = b'Packet with extension header'

>>> send(pkt_with_options)
.
Sent 1 packets.
>>>
```





The screenshot above confirms that the DUT received an IP packet containing an extension headers, and DUT responds with an **ICMPv6 Parameter Problem** message to inform the sender that the packet was invalid.

11.2.4 **Test Observations**: It is observed from the Wireshark output that DUT drops IPv6 packet with unnecessary extension headers set and DUT responds with an **ICMPv6 Parameter Problem** message to inform the sender that the packet was invalid.

11.3 Test Case Number: 3

11.3.1 **Test Case Name:** EXCEPTIONAL_FILTERING

11.3.2 **Test Case Description:** Test case to Configure and apply ACL for handling exceptional requirement of allowing IP options and extension headers

11.3.3 **Execution Steps:**

- Modify ACL on DUT for Exceptions

```
cisco4300(config)#ipv6 access-list BLOCK-EXT-HDR
cisco4300(config-ipv6-acl)#permit ipv6 any any routing
cisco4300(config-ipv6-acl)#exit
cisco4300(config)#interface GigabitEthernet0/0/0
cisco4300(config-if)#ipv6 traffic-filter BLOCK-EXT-HDR in
```

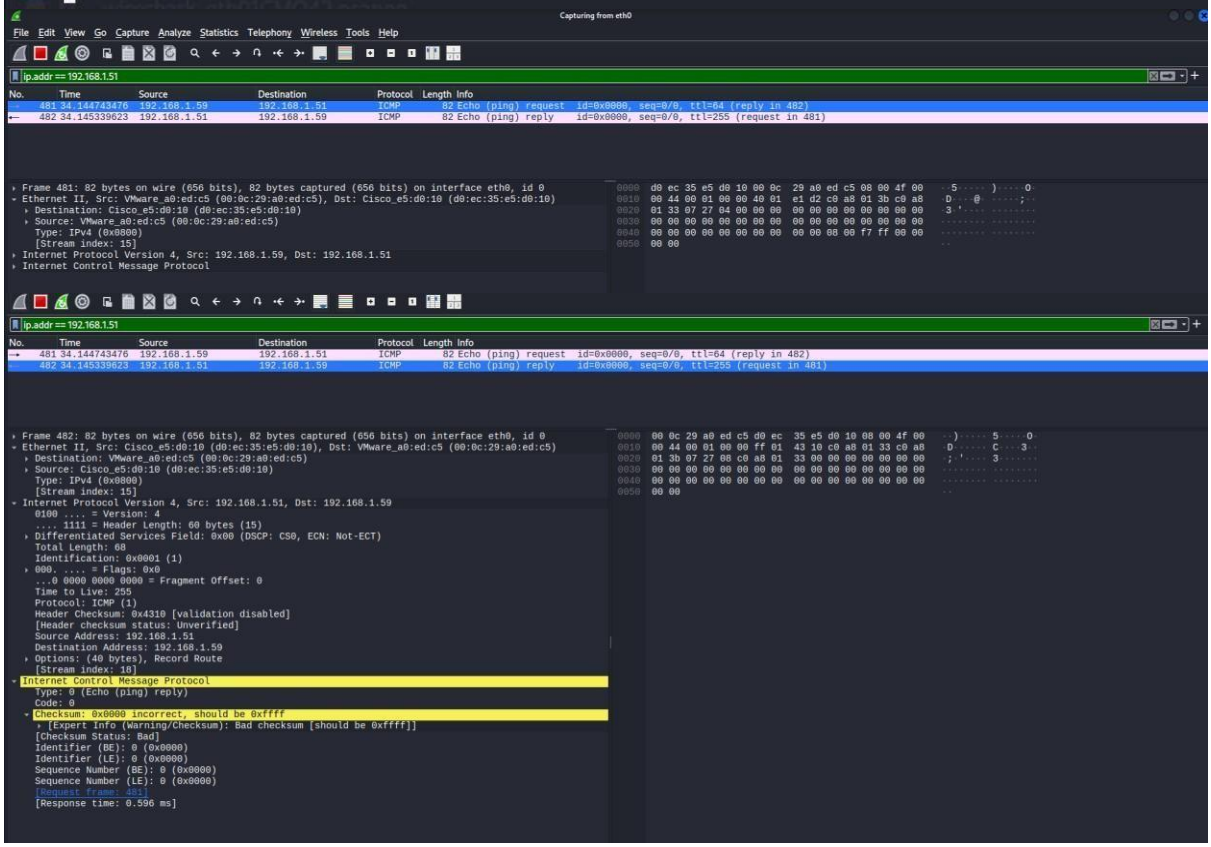
In above screenshots, the tester modified the ACL to allow for exceptional extension headers.

```
cisco4300#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cisco4300(config)#ip acc
cisco4300(config)#ip access-list exte
cisco4300(config)#ip access-list extended BLOCK_IP_OPTION
cisco4300(config-ext-nacl)#permit ip any any option re
cisco4300(config-ext-nacl)#permit ip any any option record-route
cisco4300(config-ext-nacl)#deny ip any any option any-
cisco4300(config-ext-nacl)#deny ip any any option any-options
cisco4300(config-ext-nacl)#permit ip any any
cisco4300(config-ext-nacl)#interf
cisco4300(config-ext-nacl)#exit
cisco4300(config)#interface GigabitEthernet0/0/0
cisco4300(config-if)#ip acc
cisco4300(config-if)#ip access-group BLO
cisco4300(config-if)#ip access-group BLOCK_IP_OPTION in
cisco4300(config-if)#
```

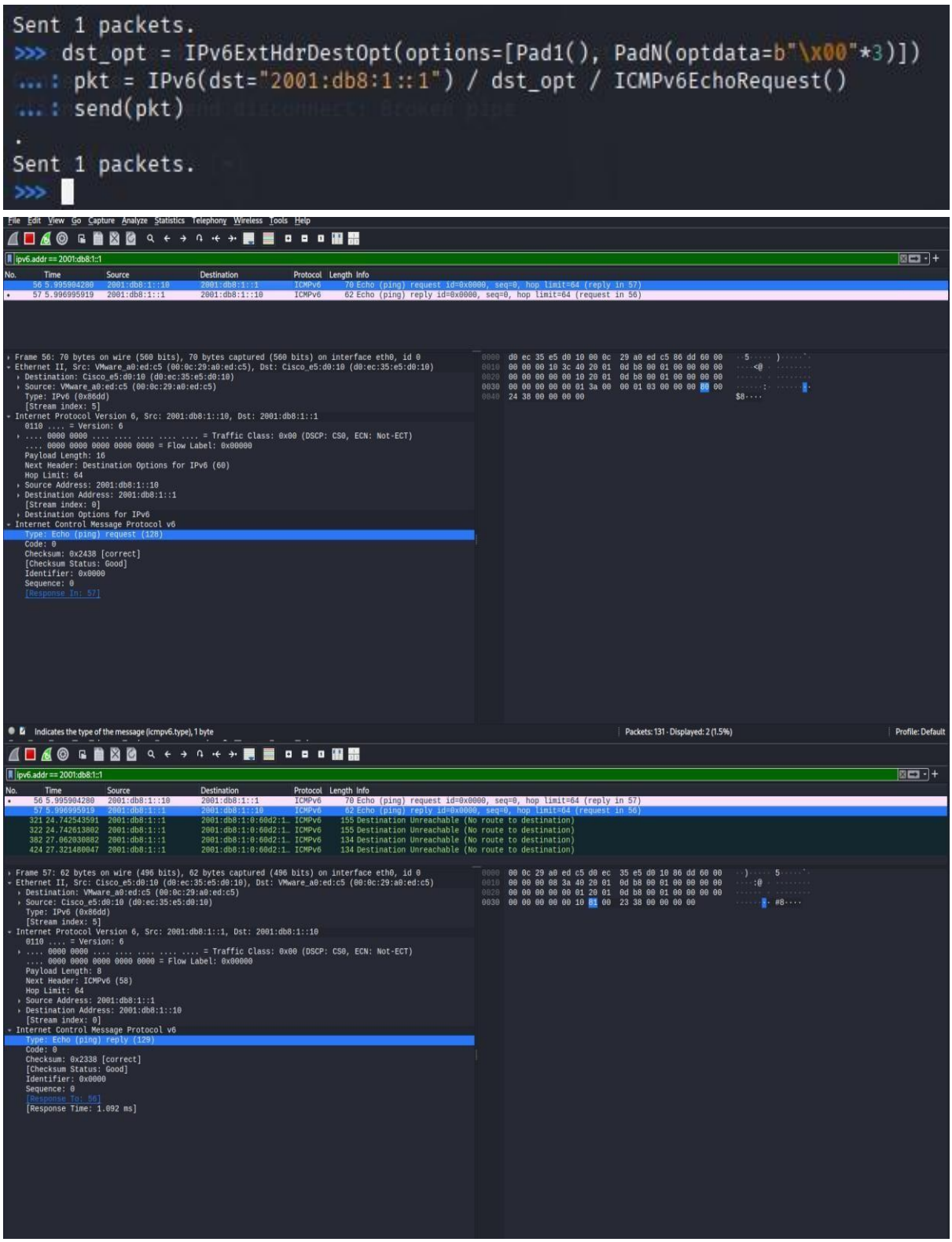
In above screenshots, the tester modified the ACL to allow for exceptional IP Option.

- After Exceptions ACL applied Sent the packet with exceptional IP options header by scapy and captured the Wireshark packets

```
Sent 1 packets.
>>> rr_option = IPOption(bytes([0x07, 0x27, 0x04] + [0x00] * 36))
...:
...: # Build the IP packet with the RR option
...: packet = IP(dst="192.168.1.51", options=[rr_option]) / ICMP()
...:
...: # Show the packet structure
...: packet.show()
...:
...: # Send the packet (without waiting for a response)
...: send(packet)
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = icmp
  chksum    = None
  src       = 192.168.1.59
  dst       = 192.168.1.51
  \options   \
   |###[ IP Option Record Route ]###
   |  copy_flag = 0
   |  optclass  = control
   |  option    = record_route
   |  length    = 39
   |  pointer   = 4
   |  routers   = [0.0.0.0, 0.0.0.0, 0.0.0.0, 0.0.0.0, 0.0.0.0, 0.0.0.0, 0.0.0.0, 0.0.0.0, 0.0.0.0]
###[ ICMP ]###
     type      = echo-request
     code      = 0
     chksum    = None
     id        = 0x0
     seq       = 0x0
     unused    = b''

.
Sent 1 packets.
>>>
```



- After Exceptions ACL applied Sent the packet with extension headers by scapy and captured the Wireshark packets



11.3.4 **Test Observations**: The tester observed that the DUT correctly handles the exceptional requirement of allowing IP options and extension headers

12. <u>Test Case Result:</u>

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_IP_OPTIONS_FILTERING	Pass	As ACL was applied for filtering of IPv4 packets with unnecessary options, the ipv4 packets with unnecessary options are being filtered.
2	EXTENSION_HEADERS_FILTERING	Pass	As ACL was applied for filtering of IPv6 packets with unnecessary extension headers, the ipv6 packets with unnecessary options are being filtered.
3	EXCEPTIONAL_ FILTERING	Pass	The tester observed that the DUT correctly handles the exceptional requirement of allowing IP options and extension headers

Section 1.9 Vulnerability Testing Requirements

2.9.1 Fuzzing – Network and Application Level

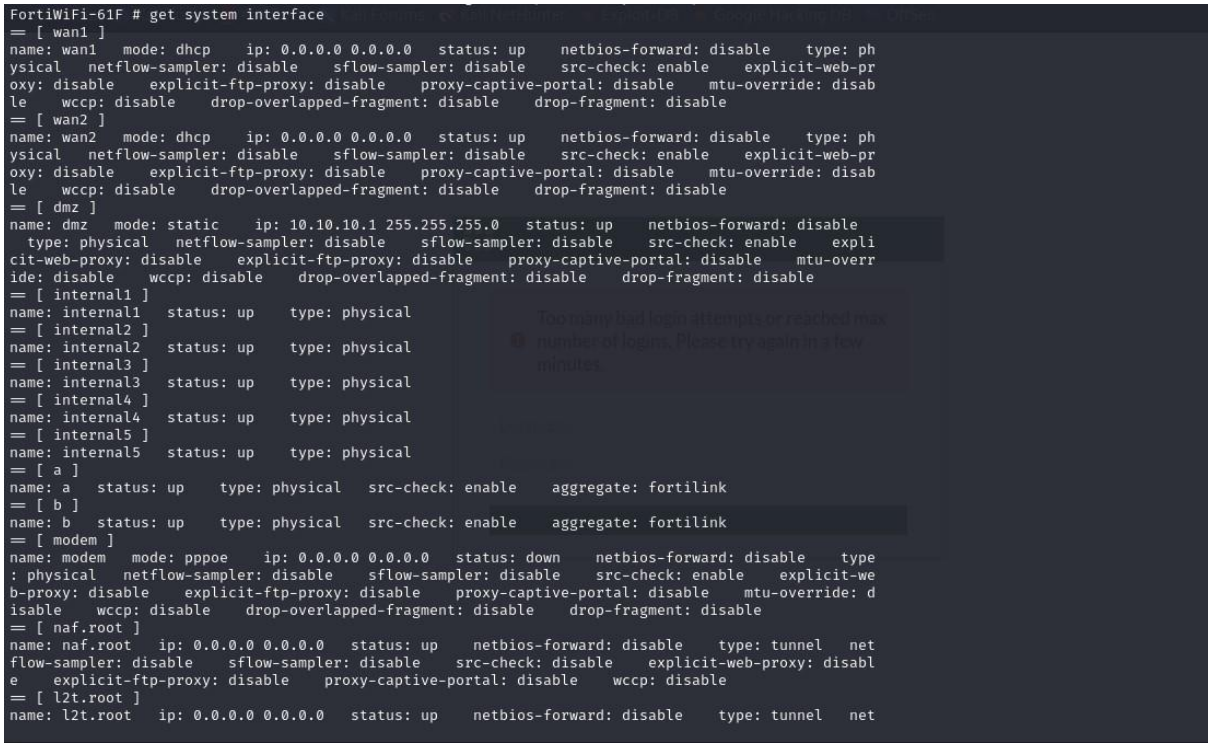
<DUT Details: > Wi-Fi CPE (Physical Wi-Fi)
<DUT Software Version:> FortiWiFi-61F v7.0.12, build0523,230606
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration>
a98153fbb034b4a45ea72d179cc737e6108c3f1d1c009705630c93dea3b0b76977cad074 0ab8c a503cd7a743f7a9cd23772223b227658cc80920aa570a27d73d(SHA512)
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> ITSAR402122401 and Version: 1.0.1
<OEM Supplied Document list: > Hash of DUT configuration is required

1. **<ITSAR Section No & Name>** Section 1.9: Vulnerability Testing Requirements
2. **<Security Requirement No & Name > 1**.9.1 Fuzzing – Network and Application Level
3. **<Requirement Description:>** The protocols supported by the Wi-Fi CPE shall be robust when receiving unexpected or malformed inputs. This requirement shall be applicable for both network level as well as application-level protocols supported by the equipment.

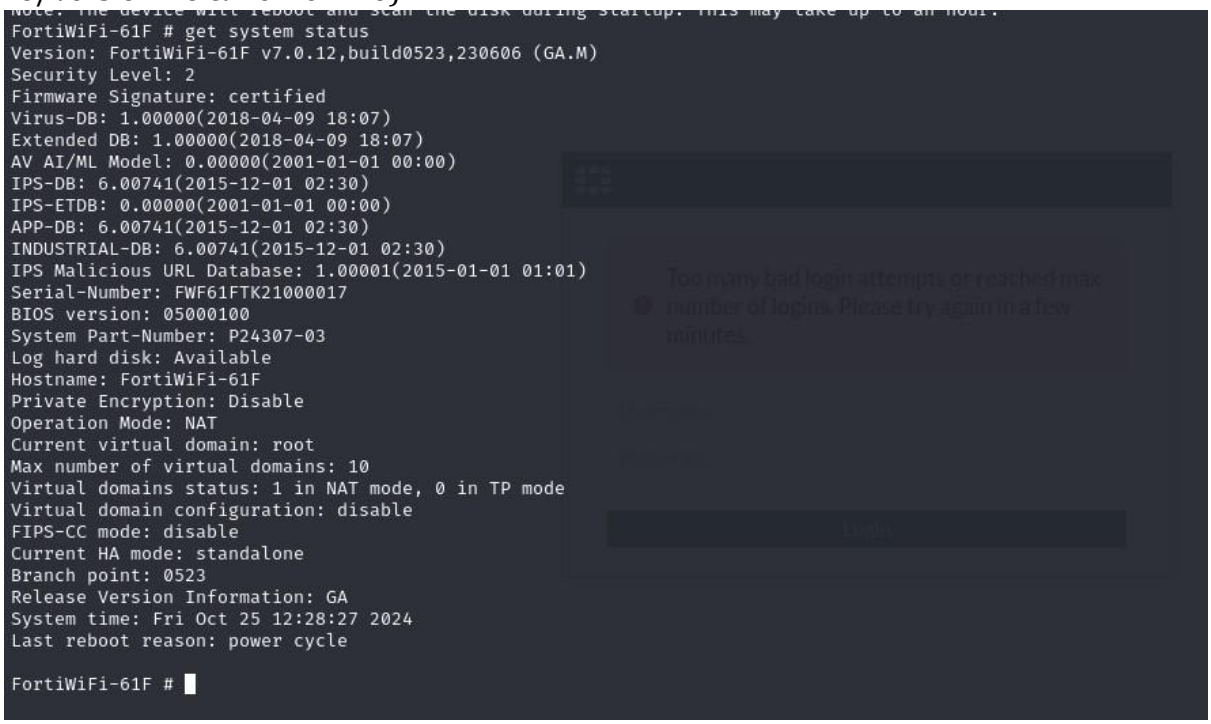
[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.4.4]

4. **DUT Confirmation Details**:
   - Use the command line interface to get details of the machine on which test is conducted
   - Use command to get Interfaces details
   - Use command to get Application No/Version No & Kernel Info

Command used: **get system interface** (To find all interfaces in the DUT)



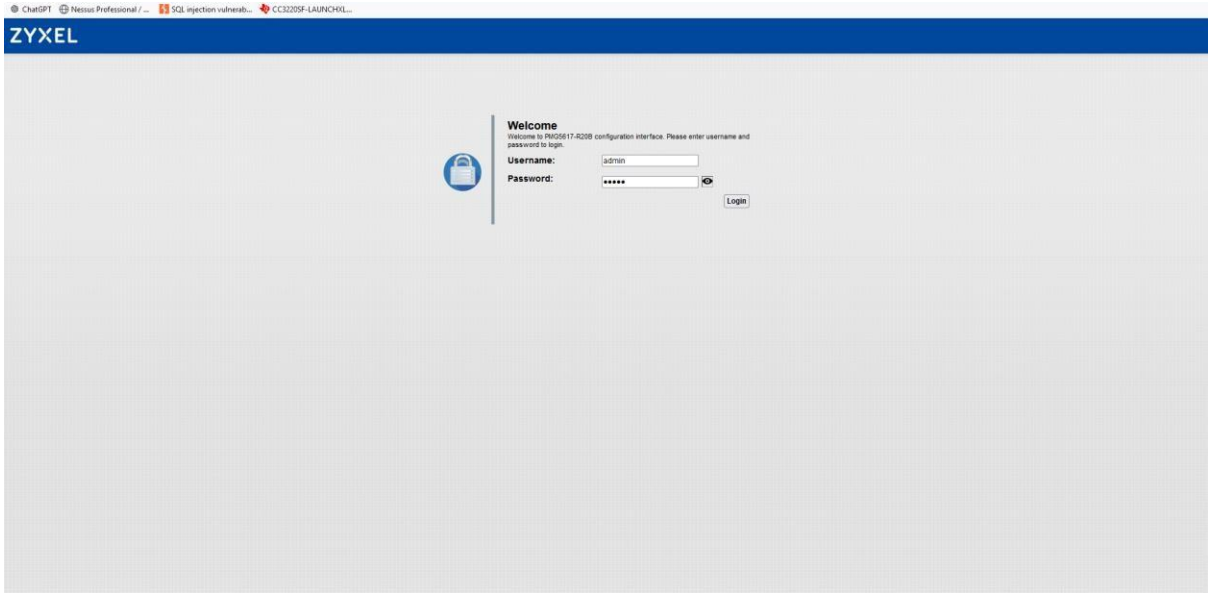
Command used: **show system status** (To get Application No/Version No & Kernel Info)



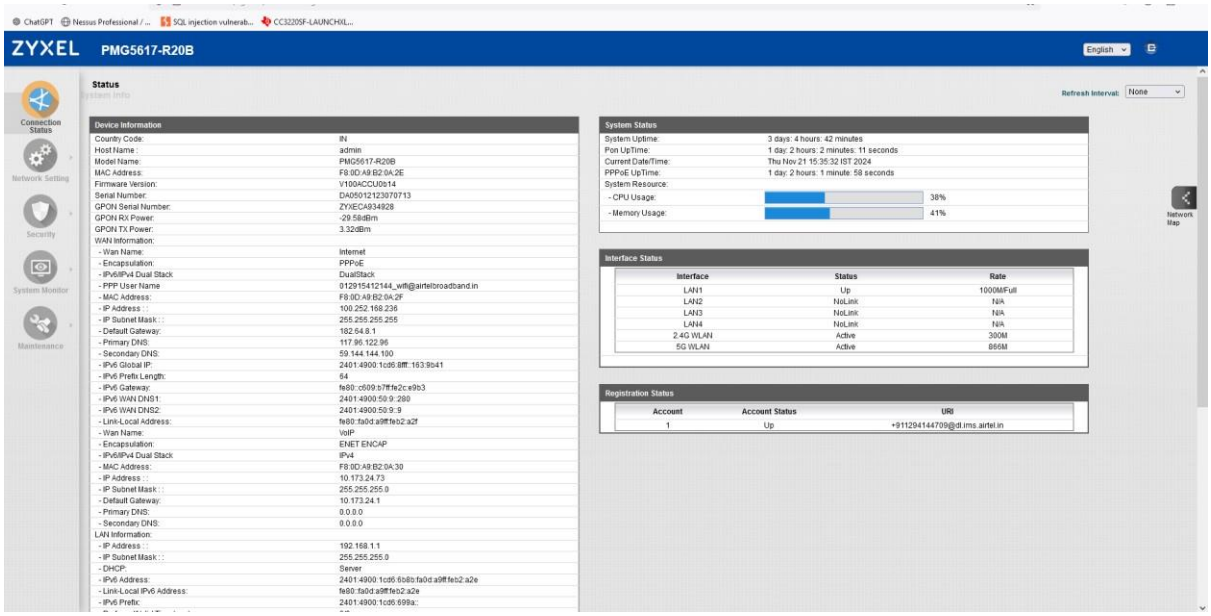
Note: Tester have used Zyxel PMG5617-R20B DUT for the Test Case 6

Login into the DUT with IP 192.168.1.1

By entering the correct credentials



Access the Zyxel PMG5617-R20B management interface (usually via web GUI).



5. **DUT Configuration:**

- Test Machine with Fuzzing tool loaded should be connected to the DUT. The DUT is connected to the fuzzing tool via LAN cable.
- Load the Fuzzing tool and input the protocol specific parameters of DUT on the tool.

6. **Preconditions**

- The tester has the privileges to log in the network product and to access all system resources (e.g. log files)
- A list of all available network services containing at least the following information shall be included in the documentation accompanying the Network Product:
    - all interfaces providing IP-based protocols;
    - the available transport layer protocols on these interfaces;

- their open ports and associated services;
- and a free-form description of their purposes.

NOTE: This list is to be validated as part of the BVT port scanning activity.

- The robustness and fuzzing tools that are selected for this test shall utilize state-of-the-art technology to identify input which causes the Network Product to behave in an unspecified, undocumented, or unexpected manner.
- Fuzz testing tools are a highly sophisticated technology and adaptation to the individual protocols in question is needed to be effective. Therefore, there is a lack of available effective fuzz testing tools available especially for protocols proprietary to the Telco industry. Taking into account note 4 of TR 33.916's clause 7.2.4, test labs shall acquire fuzz testing tools for those protocols where commercially feasible.
- It needs to be taken into account that fuzz testing tools might show drastic differences in terms of effectiveness. The accredited test lab is expected to have sufficient expertise to recognize the level of effectiveness of the available tools.
- A network traffic analyser on the network product (e.g. TCPDUMP) or an external traffic analyser directly connected to the network product and on a tester machine is available.

7. Test Objective: - To verify that the network product provides externally reachable services which are robust against unexpected input.
8. Test Plan

NOTE: Tester should perform fuzzing in full mode on each protocol. In case, if the completion of fuzzing is not possible in reasonable period (as notified by NCCS) then tester can opt for balanced mode fuzzing for such protocols.

8.1. Number of Test Scenarios: [Separate Testcase for each protocol as notified by NCCS.]

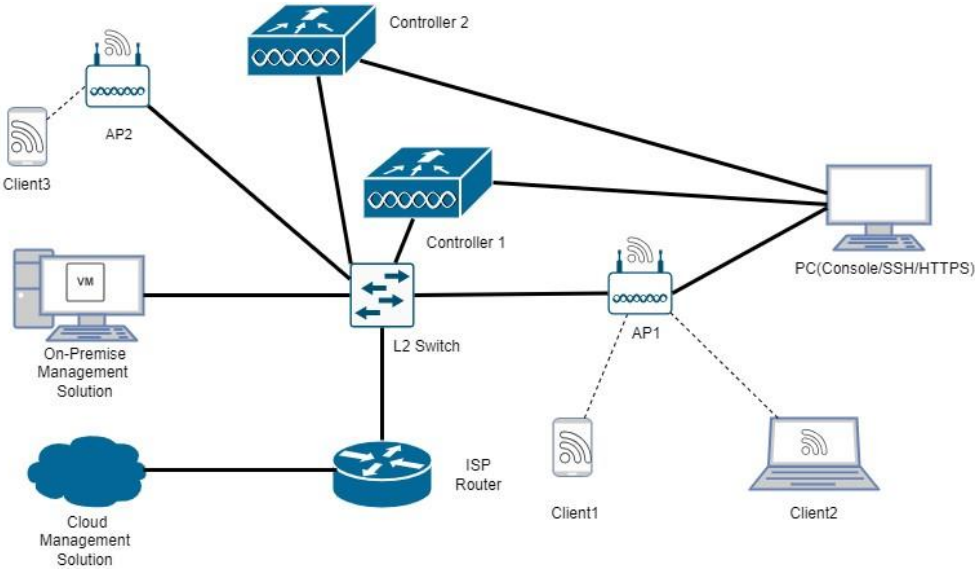
8.1.1 Test Case:01

8.1.2 Test Name: ARP Fuzz Test

8.1.3 Test Description: Tester to perform the ARP fuzzing test on the DUT

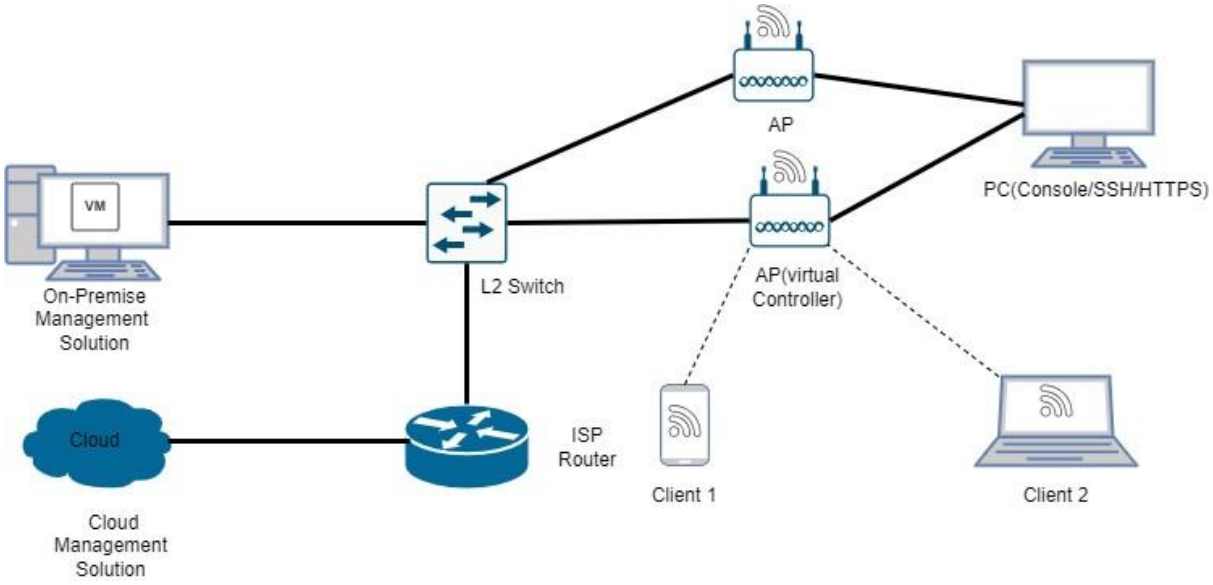
8.2 Test Bed Diagram

AP + Controller mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

Note: Here selecting ARP server test suite in the Defensics means Tool will act as an ARP client and DUT will act as ARP server.

8.3 Tools Required: - Black Duck (Defences) Fuzzing Tool

8.4 Test Execution Steps

1. Execution of available effective fuzzing tools against the protocols available via interfaces providing Application-based protocols of the Network Product for an amount of time sufficient to be effective.

2. Execution of available effective robustness test tools against the protocols available via interfaces providing IP-based protocols of the Network Product for an amount of time sufficient to be effective. (Use of TCP/UDP Packets with underlying IP packets also works)
3. For both step 1 and 2:
    - Using a network traffic analyser on the network product (e.g. TCPDUMP/Wireshark) or an external traffic analyser directly connected to the network product, the tester verifies that the packets are correctly processed by the network product.
    - The testers verifies that the network product and any running network service does not crash.
    - The execution of tests shall run sufficient times.

Note: Fuzz testing to be performed with direct connection between the tool and DUT. Also, any IDS/IP, firewall to be disabled if present on the DUT during fuzzing.

9. **Expected Results for Pass:-** A list of all of the protocols of the network product reachable externally on an IP-based interface, together with an indication whether effective available robustness and fuzz testing tools have been used against them, shall be part of the testing documentation. If no tool can be acquired for a protocol, a free form statement should explain why not.

The used tool(s) name, their unambiguous version (also for plug-ins if applicable), used settings, and the relevant output is evidence and shall be part of the testing documentation. Any input causing unspecified, undocumented, or unexpected behaviour, and a description of this behaviour shall be highlighted in the testing documentation.

COTS fuzzing tools, by their nature, may have an acceptable failure rate (e.g. 0.1%) due to different non-deterministic variables in their implementation. At some point the tool's documentation may even mention that the failing test shall be repeated to check whether it is really a recurring problem or not. The tester shall make best effort to determine if there is an issue with NE or the test tool and if necessary, work with the vendor of the network product to come to a consensus on the test result outcome.

10. **Expected Form of Evidence:-** A testing report which will consist of the following information:
    - The used tool(s) name and version information,
    - Settings and configurations used
    - The output log file of the chosen tool that displays the results (passed/failed).
    - Screenshot
    - Test result (Passed or not)
    - Log/evidence tracing possible crashes
    - Any input causing unspecified, undocumented, or unexpected behaviour.

11. **Test Execution**

Note: Testing to be performed for all externally reachable network and application layer protocols supported by the DUT on externally reachable interface. Following general instruction needs to be followed by the tester while performing fuzz test:

- **Timeout** – Acceptable response time before DUT is considered in DOS. This affects pass/fail criteria for the test-cases. It should be a value that is mutually agreeable between tester and the DUT vendor.
- **TCP Timeout** - Time that the test driver will wait for a request to be sent to the tested implementation when using TCP transport, provided in milliseconds
- **Fail limit** defines the number of consecutive instrumentations that need to be unsuccessful for a testcase to be regarded as "Failed". Typically, a value of either 2 or 3 is recommended.
- **Instrumentation Frequency** determines after how many test cases are run before instrumentation is executed. →Recommended value is 1.
- Collect DUT logs and packet captures and attach them with test-report for issue reporting.

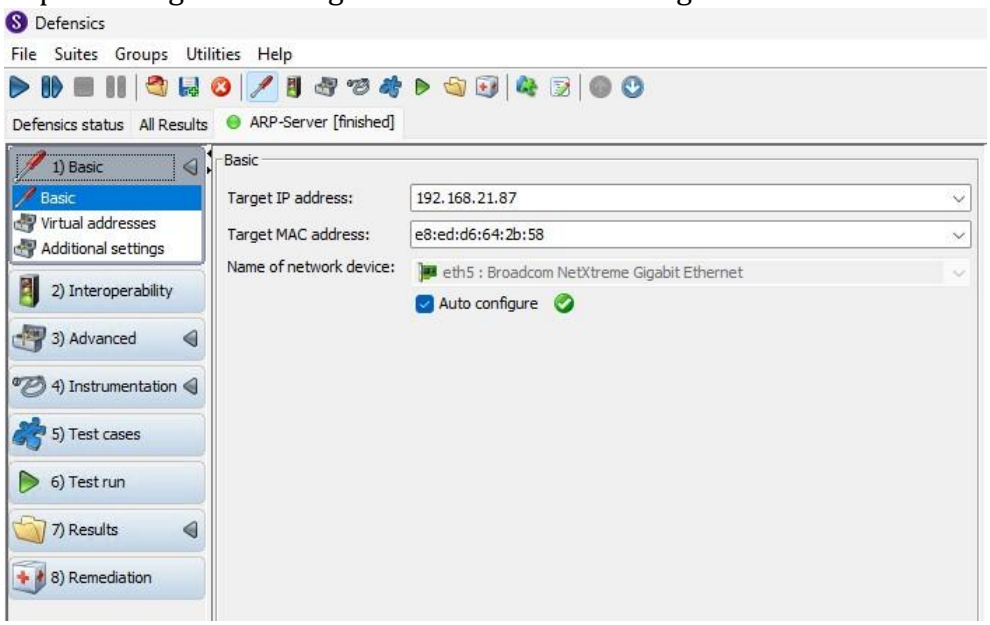
11.1 Test Case Number: 01

11.1.1 **Test Case Name:** ARP Fuzz Test

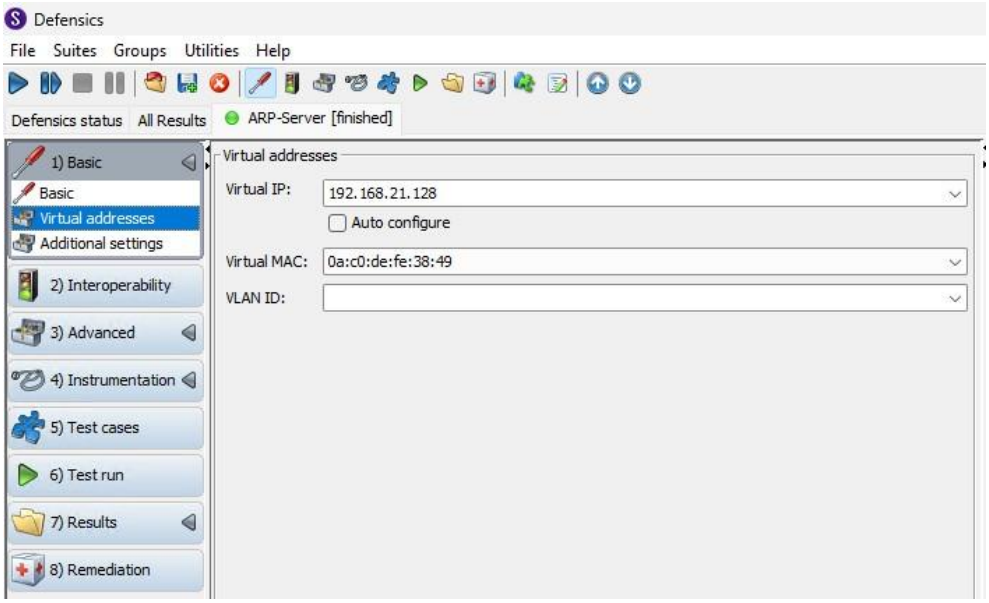
11.1.2 **Test Case Description:** Tester to perform the ARP fuzzing test on the DUT

11.1.3 **Execution Steps:**

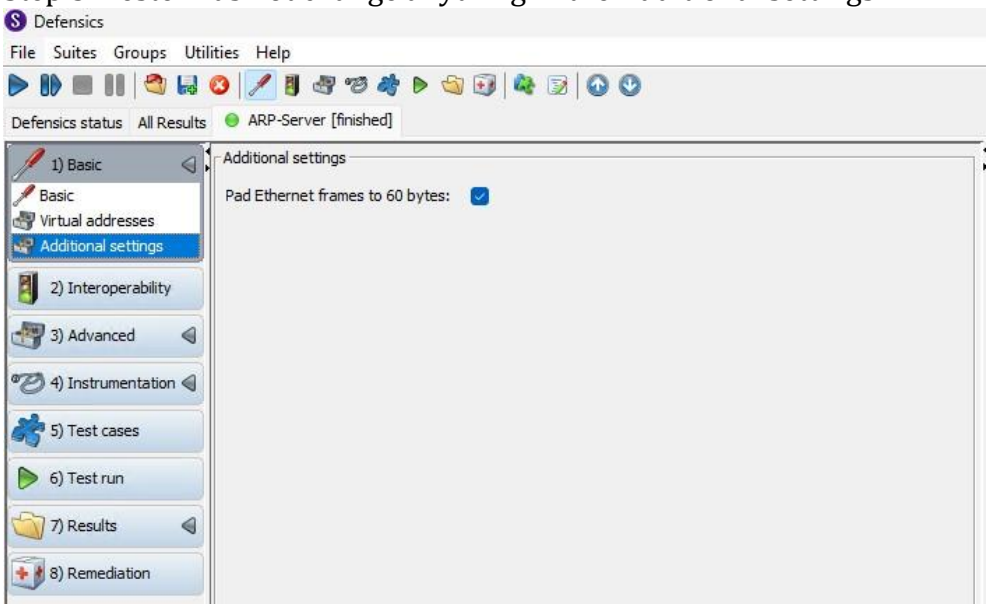
Step 1: Configure the target IP address and the target MAC address



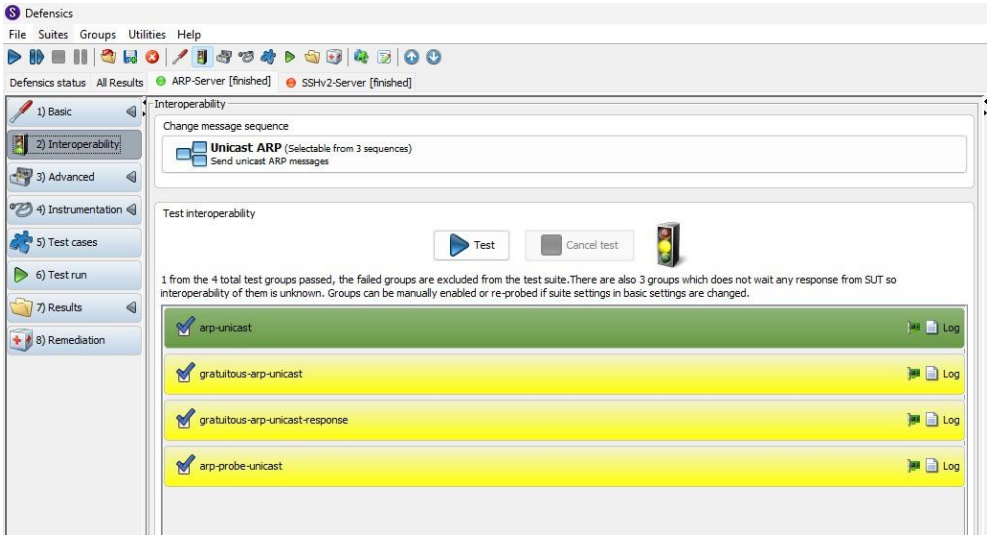
Step 2: Defensics automatically taken the Virtual IP address as 192.168.21.128.



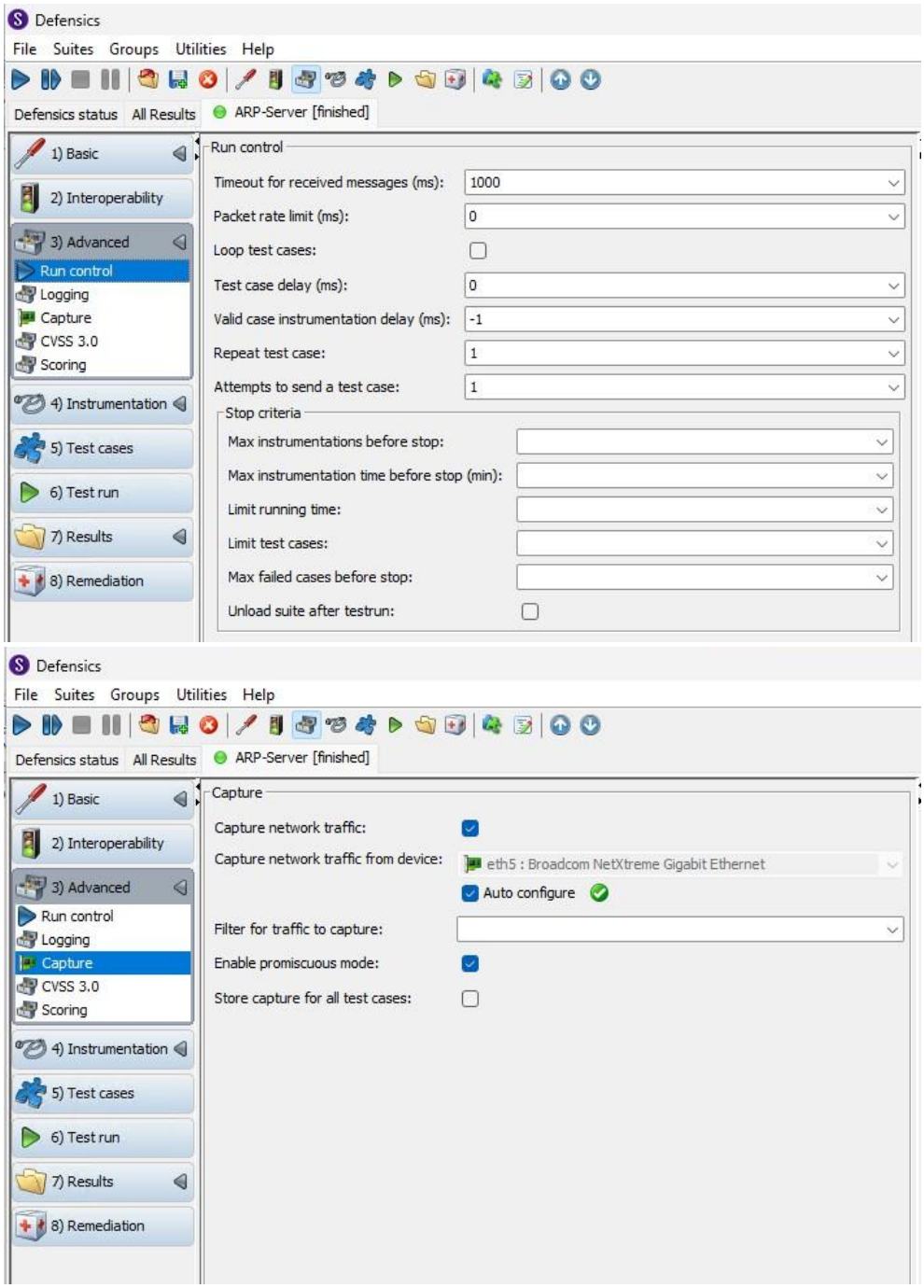
Step 3: Tester has not change anything in the Additional settings



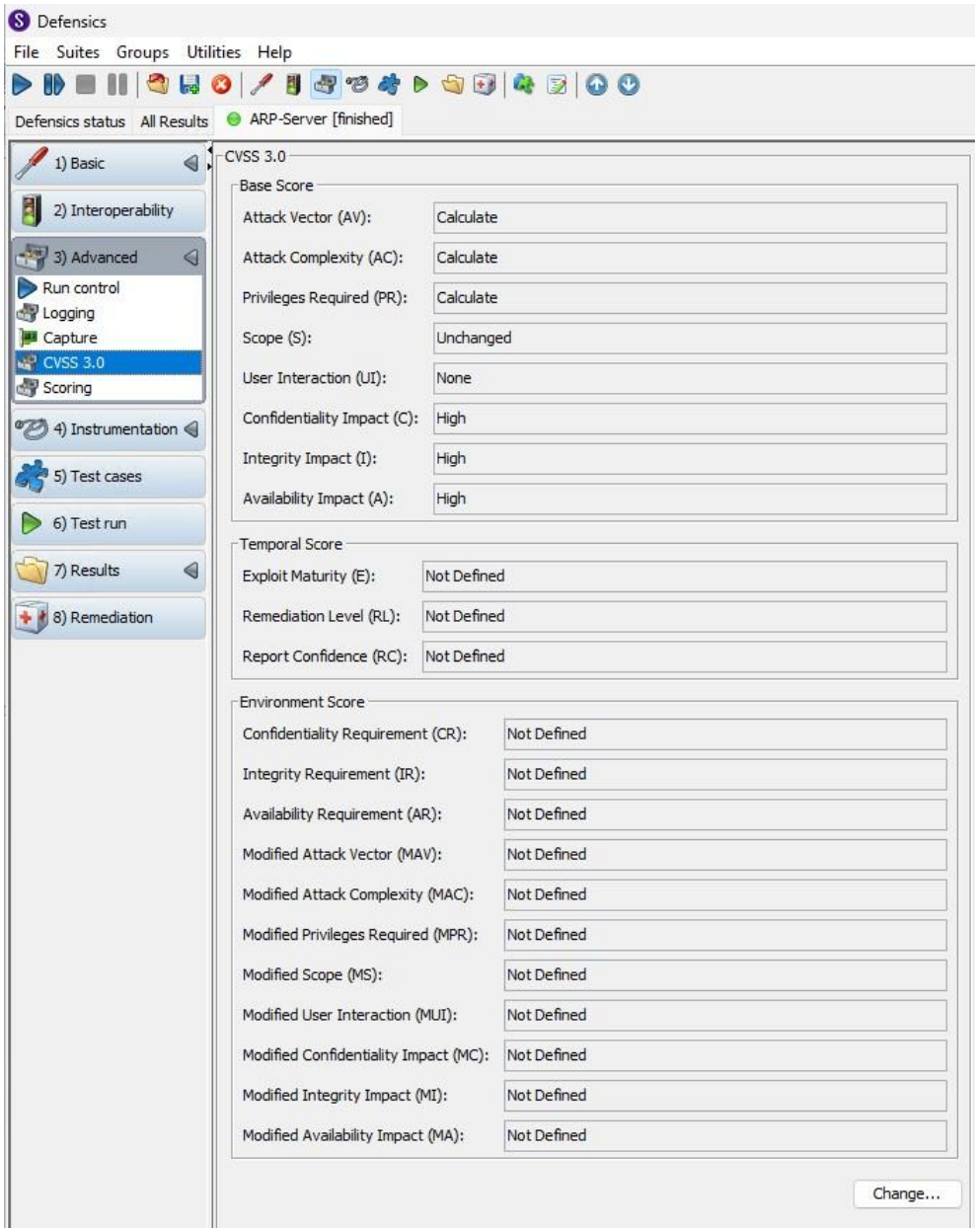
Step 4: Then Tester navigate to the Interoperability and test the compatibility.

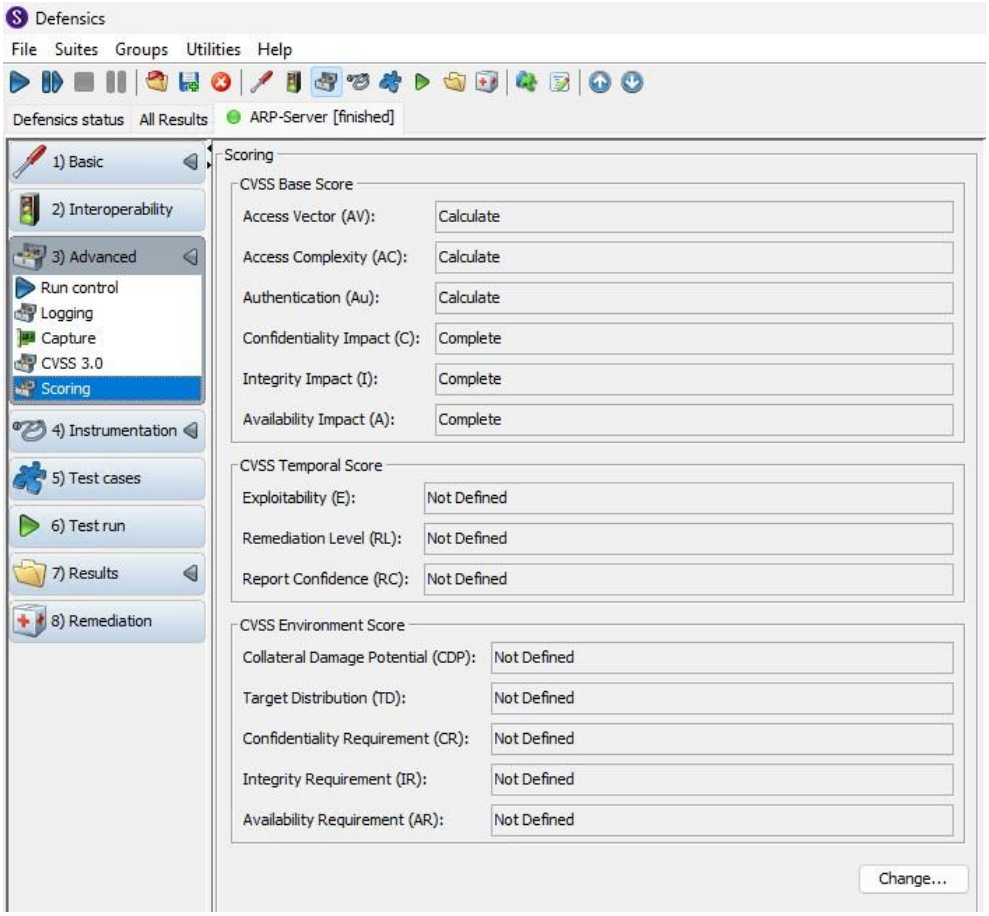


Tester have not changed any thing in the Run control.

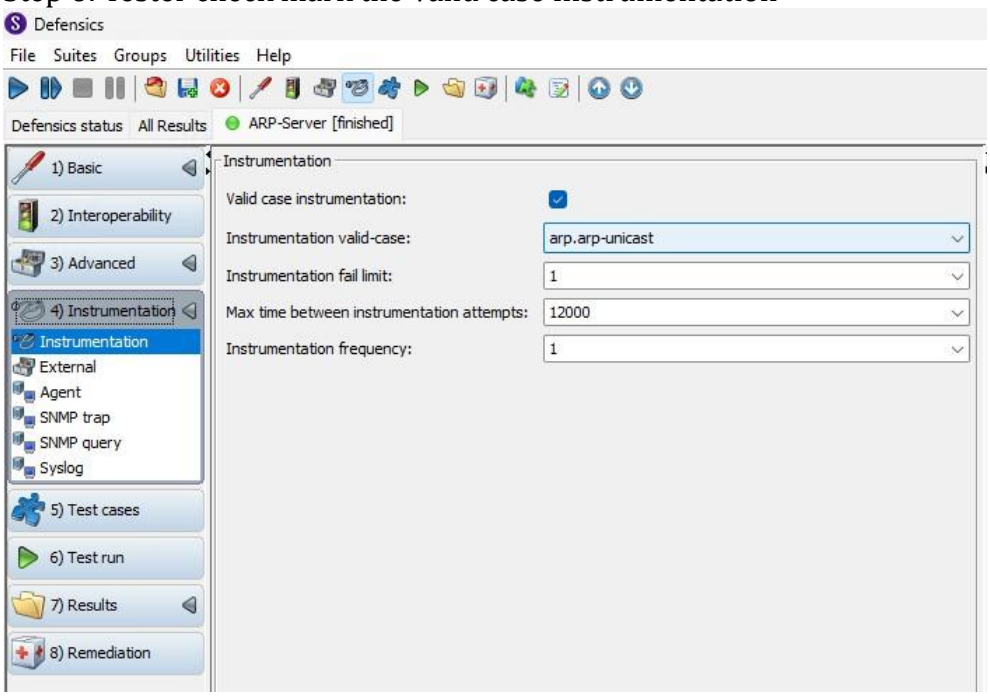


Step 5: Tester remains the by-default settings of the CVSS 3.0 section of the Defensics.

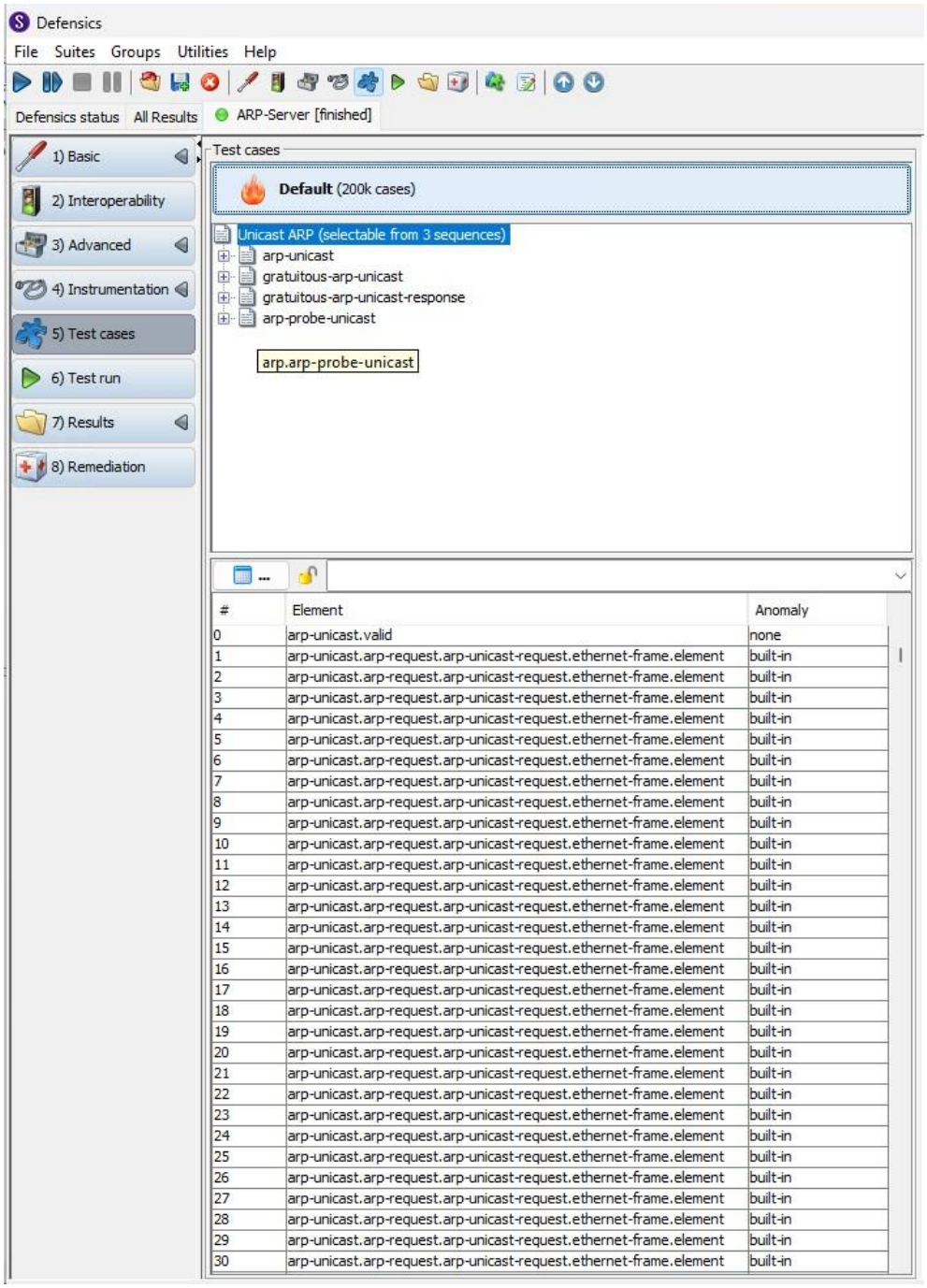

Defensics
File Suites Groups Utilities Help
Defensics status
All Results
ARP-Server [finished]
1) Basic
2) Interoperability
3) Advanced
Run control
Logging
Capture
CVSS 3.0
Scoring
4) Instrumentation
5) Test cases
6) Test run
7) Results
8) Remediation
CVSS 3.0
Base Score
Attack Vector (AV): Calculate
Attack Complexity (AC): Calculate
Privileges Required (PR): Calculate
Scope (S): Unchanged
User Interaction (UI): None
Confidentiality Impact (C): High
Integrity Impact (I): High
Availability Impact (A): High
Temporal Score
Exploit Maturity (E): Not Defined
Remediation Level (RL): Not Defined
Report Confidence (RC): Not Defined
Environment Score
Confidentiality Requirement (CR): Not Defined
Integrity Requirement (IR): Not Defined
Availability Requirement (AR): Not Defined
Modified Attack Vector (MAV): Not Defined
Modified Attack Complexity (MAC): Not Defined
Modified Privileges Required (MPR): Not Defined
Modified Scope (MS): Not Defined
Modified User Interaction (MUI): Not Defined
Modified Confidentiality Impact (MC): Not Defined
Modified Integrity Impact (MI): Not Defined
Modified Availability Impact (MA): Not Defined
Change...



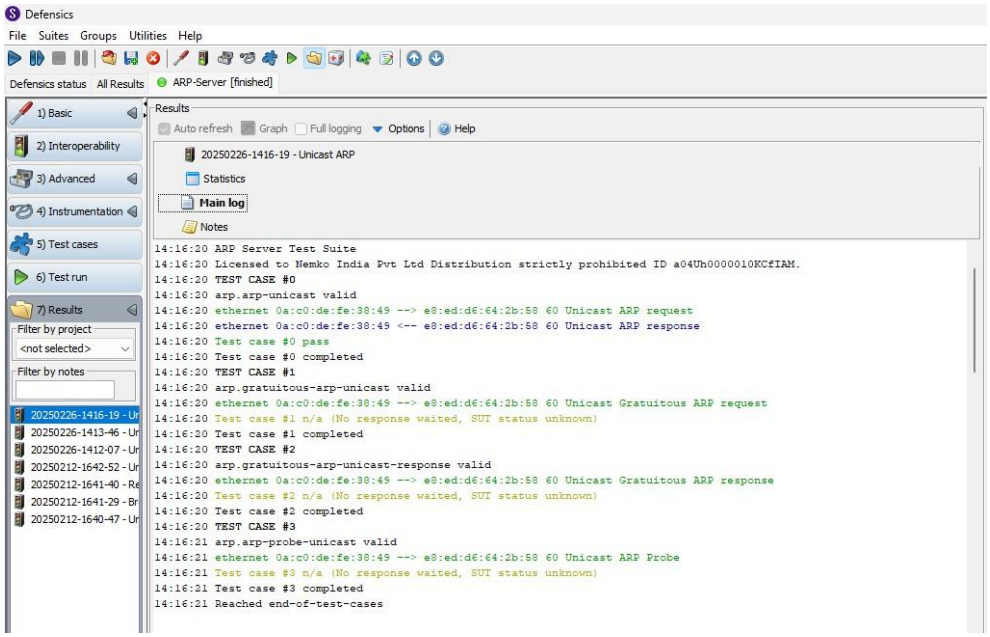
Step 6: Tester check mark the Valid case Instrumentation



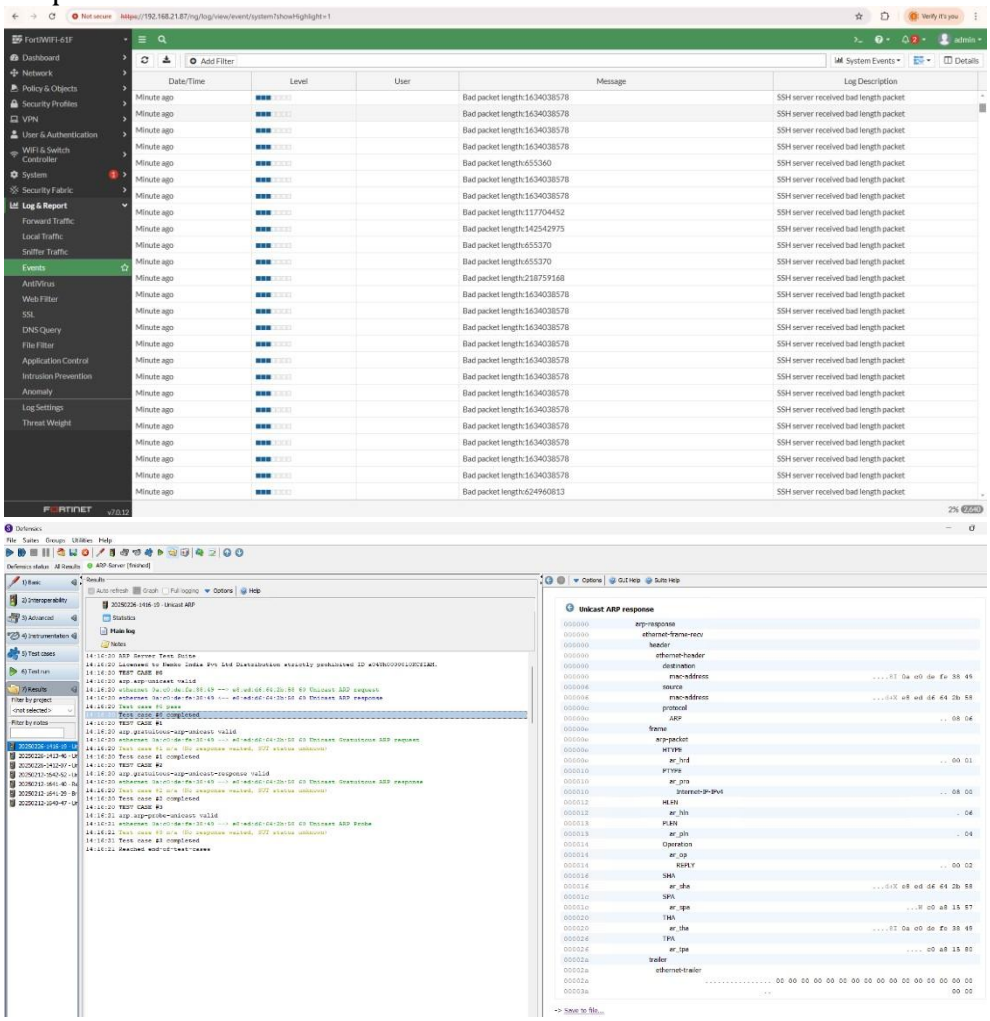
Step 7: Tester then chooses the Default test suite with 200k test cases



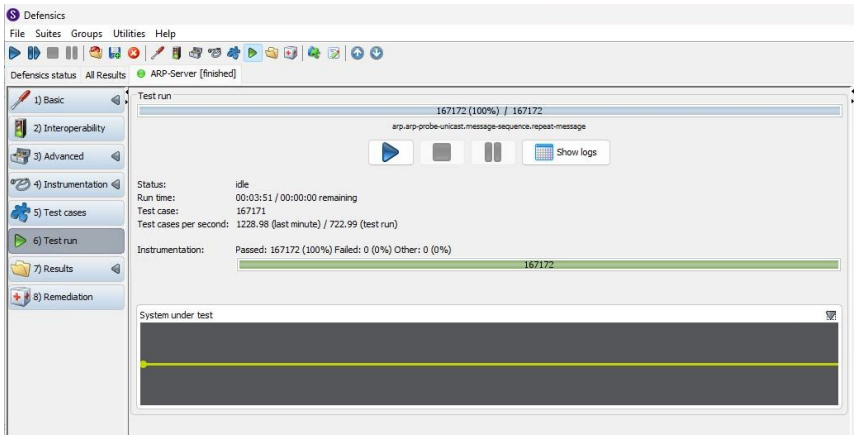
Step 8: Tester then clicks on the run to start the test and after that tester can clearly see the logs in the Defences

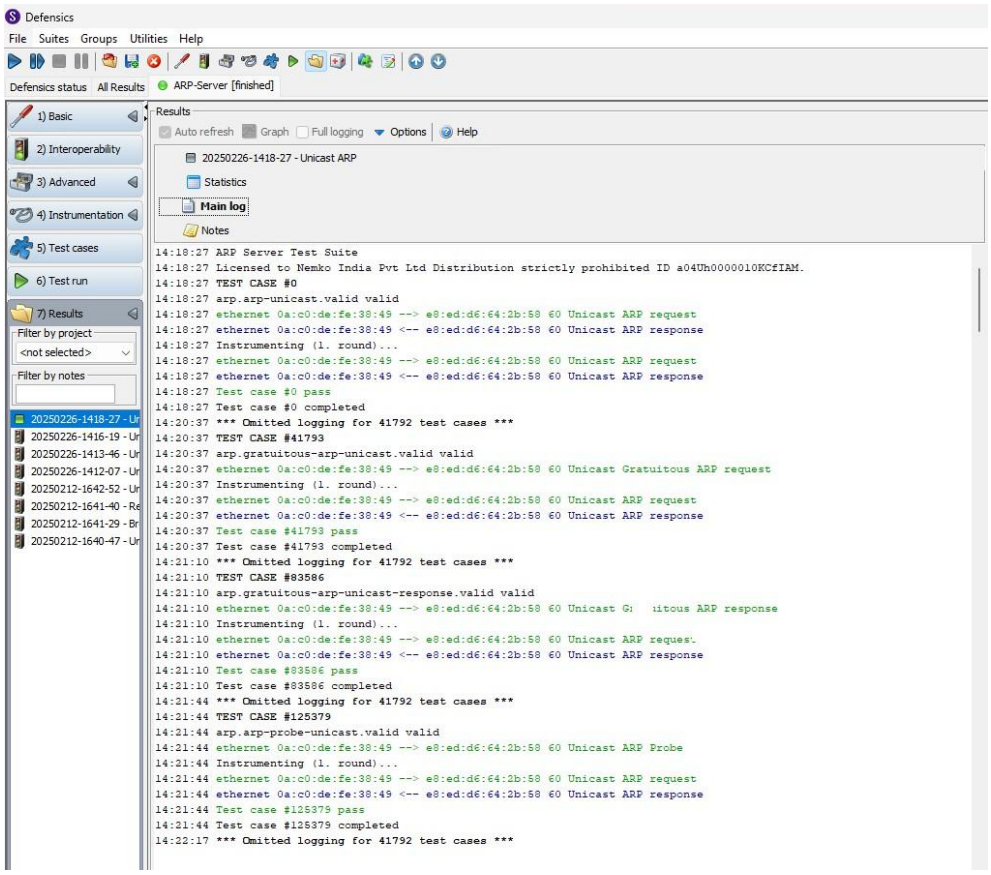


During Fuzzing of the ARP server test suite tester verified the logs on the DUT in the below snap-shot.

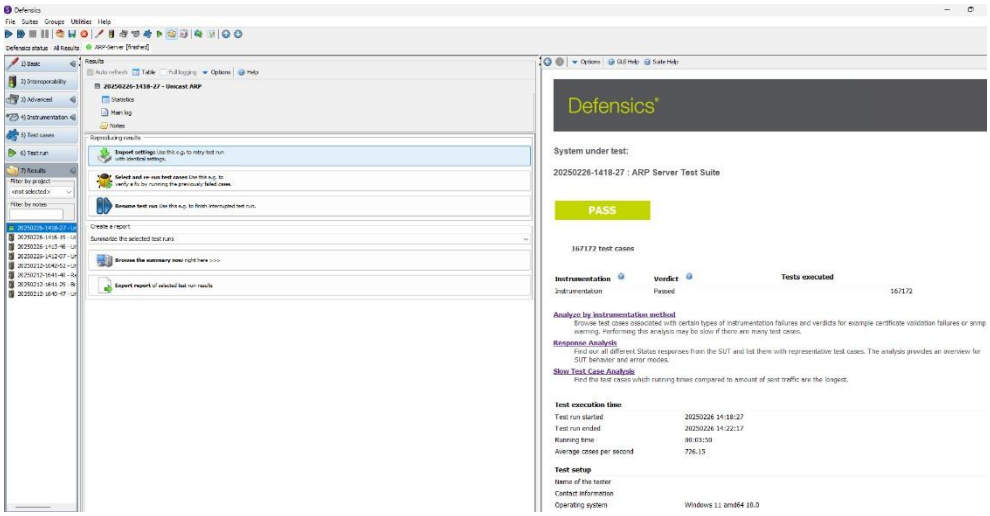


Step 9: After running 167172 test cases tester completed the ARP fuzzing test on DUT

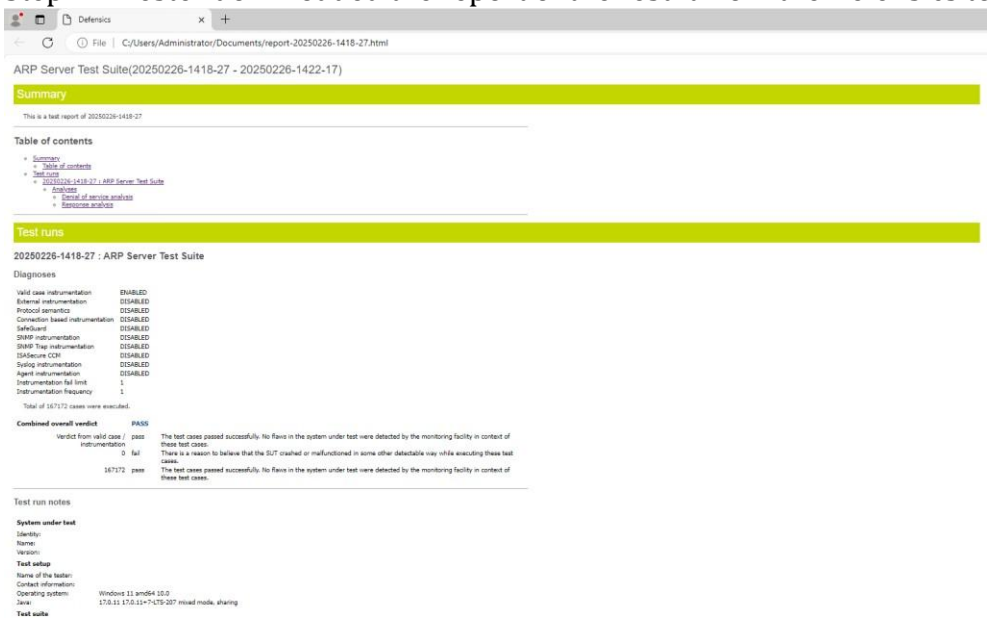




Step 10: Tester checked the result of the fuzzing test of ARP on the DUT



Step 11: Tester downloaded the report of the result from the Defensics to verify the results



Step 12: Tester verified from the below screen-shot that the final verdict of this test case is PASS

ARP Server Test Suite(20250226-1418-27 - 20250226-1422-17)

Summary

This is a test report of 20250226-1418-27

Table of contents

Test runs

20250226-1418-27 : ARP Server Test Suite

Diagnoses

Valid case instrumentation	ENABLED
External instrumentation	DISABLED
Protocol semantics	DISABLED
Connection based instrumentation	DISABLED
SafeGuard	DISABLED
SNMP instrumentation	DISABLED
SNMP Trap instrumentation	DISABLED
ISASecure CCM	DISABLED
Syslog instrumentation	DISABLED
Agent instrumentation	DISABLED
Instrumentation fail limit	1
Instrumentation frequency	1

Total of 167172 cases were executed.

Combined overall verdict	**PASS**	
Verdict from valid case / instrumentation	pass	The test cases passed successfully. No flaws in the system under test were detected by the monitoring facility in context of these test cases.
0	fail	There is a reason to believe that the SUT crashed or malfunctioned in some other detectable way while executing these test cases.
167172	pass	The test cases passed successfully. No flaws in the system under test were detected by the monitoring facility in context of these test cases.

Test run notes

System under test

Identity:
Name:
Version:

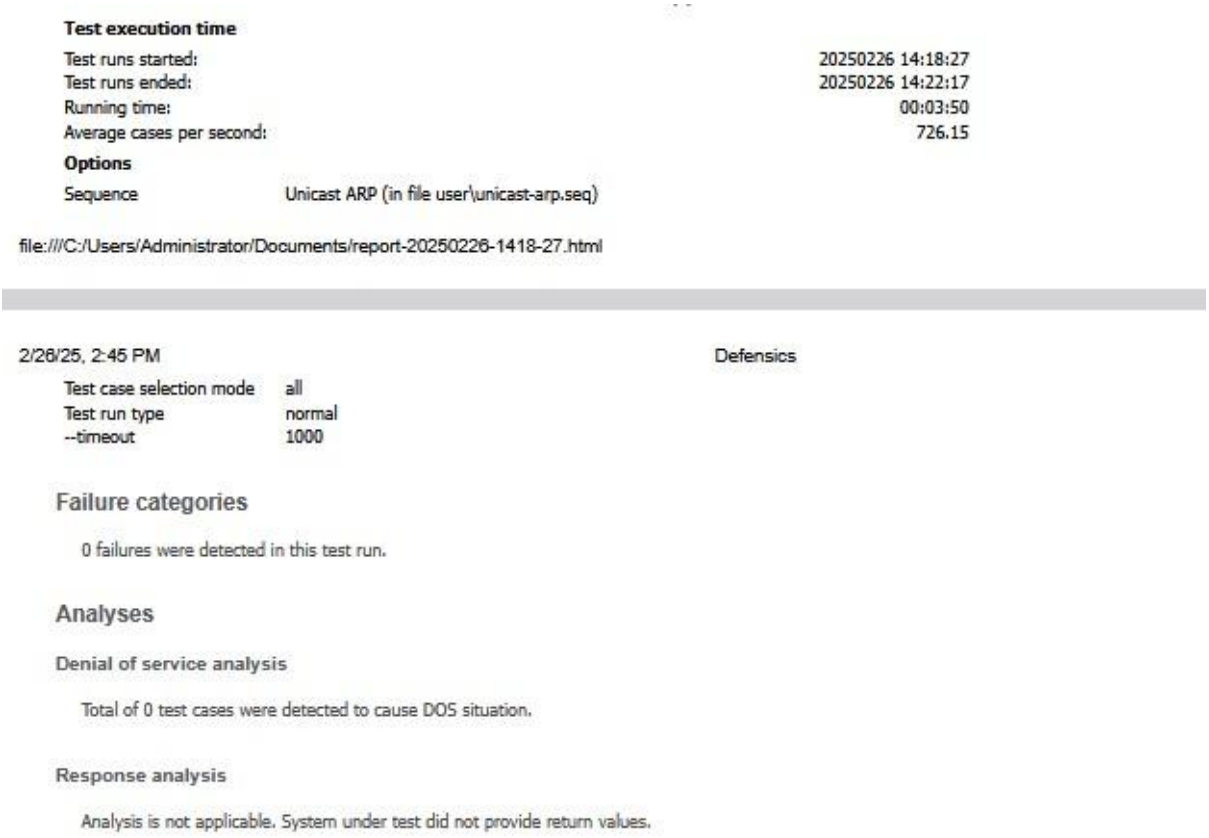
Test setup

Name of the tester:
Contact information:
Operating system: Windows 11 amd64 10.0
Java: 17.0.11 17.0.11+7-LTS-207 mixed mode, sharing

Test suite

Name: ARP Server Test Suite
Version: 7.5.1 20241114 2023.9.4
License: Licensed to Nemko India Pvt Ltd Distribution strictly prohibited ID a04Uh0000010KCfIAM.

Test execution time



Test execution time

Test runs started:	20250226 14:18:27
Test runs ended:	20250226 14:22:17
Running time:	00:03:50
Average cases per second:	726.15

Options

Sequence	Unicast ARP (in file user\unicast-arp.seq)

file:///C:/Users/Administrator/Documents/report-20250226-1418-27.html

2/26/25, 2:45 PM Defensics

Test case selection mode	all
Test run type	normal
--timeout	1000

Failure categories

0 failures were detected in this test run.

Analyses

Denial of service analysis

Total of 0 test cases were detected to cause DOS situation.

Response analysis

Analysis is not applicable. System under test did not provide return values.

11.1.4 **Test Observations**: While testing DUT it was observed that DUT fuzzing test for ARP protocol is Passed by Defences tool.

11.1.5 **Evidence Provided:** Screenshot attached and DUT logs.

(Tester should follow same steps to fuzz all the required protocols).

12 Test Case Results

S.No.	TEST CASE NAME	PASS/FAIL	REMARKS
1	ARP protocol Fuzzing	Pass	While testing DUT it was observed that DUT fuzzing test for ARP protocol is Passed by Defences tool.

2.9.2 Port Scanning

<DUT Details: > Wi-Fi CPE
<DUT Software Version:>
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> ITSAR402122401 and Version: 2.0.0
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 1.9: Vulnerability Testing Requirements
2. **<Security Requirement No & Name > 1**.9.2 Port Scanning
3. **<Requirement Description:>** It shall be ensured that on all network interfaces, only vendor documented/identified ports on the transport layer respond to requests from outside the system.

List of the identified open ports shall match the list of network services that are necessary for the operation of the CPE.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.4.2]

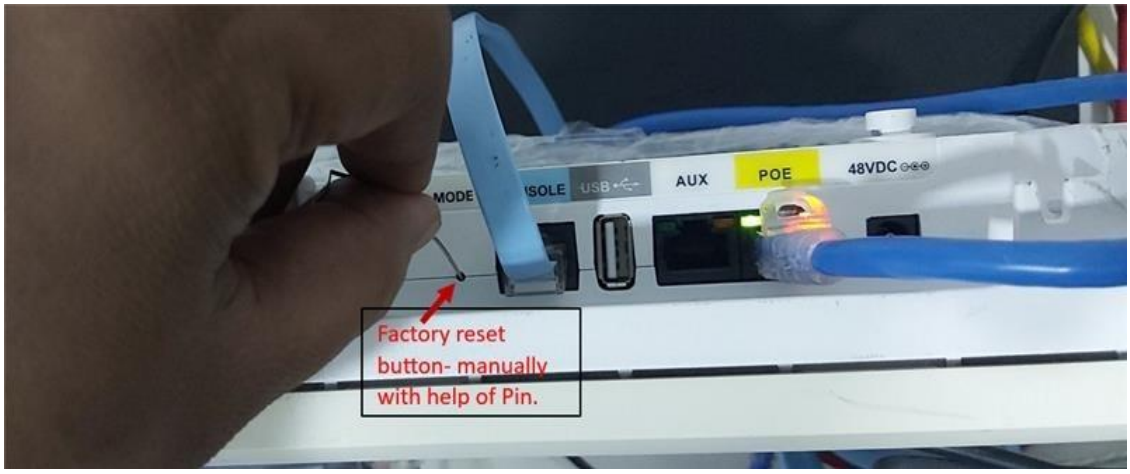
4. **DUT Confirmation Details**:
   - This section involves information about DUT like software/firmware version, Hardware version model.
   - DUT Cisco WLC contains default boot image with version 8.10.183.0. The model is AIR-AP1852I-E-K9. The inventory shows model serial no. & model description.
   - DUT TP-Link contains 3.16.9 build firmware version. The model is WR841N. The status tab displays LAN IP & wireless SSID information.
   - Verification of DUT Cisco wireless LAN controller's HW product series information by running command *show inventory* on CLI.

   - Verification of DUT Cisco WLC's high-level system SW information by running command *show sysinfo* on CLI.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.10.183.0
OUI File Last Update Time........................ N/A

System Name...................................... Aironet-Controller
System Location.................................
System Contact..................................
System ObjectID.................................. 1.3.6.1.4.1.9.1.2250
IP Address....................................... 10.208.38.2
Last Reset....................................... 1: reload command

System Up Time................................... 0 days 3 hrs 33 mins 5 secs
System Timezone Location......................... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
System Stats Realtime Interval................... 5
System Stats Normal Interval..................... 180

Configured Country............................... IN  - India

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled

--More-- or (q)uit
```

- Verification of DUT Cisco WLC's system information on Web access.

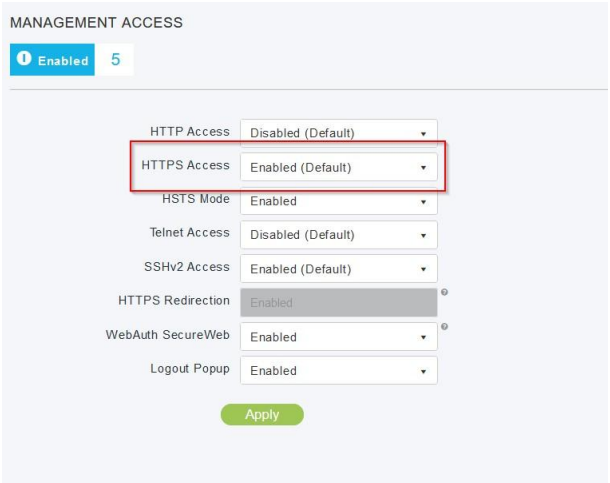
5. **DUT Configuration:-** Performing manual factory-reset on DUT with the help of pin as below image depicts:



After performing factory-reset & configuring management interface on Cisco WLC on DUT. Command "Show run-config" is run on DUT to check the interface ips configured:

```
(Cisco Controller) >show run-config

Press Enter to continue...

System Inventory
NAME: "Mobility Express"    , DESCR: "Cisco Aironet 1850 Series Mobility Express"
PID: AIR-AP1852I-E-K9,  VID: V01,  SN: KWC193100UU

Burned-in MAC Address.............................. 38:ED:18:C8:10:60
Maximum number of APs supported..................... 50
Press Enter to continue or <ctrl-z> to abort


System Information
Manufacturer's Name................................ Cisco Systems Inc.
Product Name....................................... Cisco Controller
Product Version.................................... 8.10.183.0
OUI File Last Update Time.......................... N/A

System Name........................................ Aironet-Controller
System Location.....................................
System Contact......................................
System ObjectID.................................... 1.3.6.1.4.1.9.1.2250
IP Address......................................... 10.208.38.2
Last Reset......................................... 1: reload command

System Up Time..................................... 2 days 6 hrs 5 mins 33 secs
System Timezone Location........................... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
System Stats Realtime Interval..................... 5
System Stats Normal Interval....................... 180

Configured Country................................. IN  - India

State of 802.11b Network........................... Enabled
State of 802.11a Network........................... Enabled

--More or (q)uit current module or <ctrl-z> to abort
```

- **HTTPS access is enabled by default in DUT as captured on WEB-GUI.**



6. **<u>Preconditions</u>**

- A list of all available network services containing at least the following information shall be included in the documentation accompanying the Network Product:
    - all interfaces providing IP-based protocols;
    - the available transport layer protocols on these interfaces;
    - their open ports and associated services per transport layer protocol;
    - and a free-form description of their purposes.
- The port scanning tool that is used shall be capable to detect open ports on the relevant transport layer protocols.
- NOTE: It might not be possible for certain transport layer protocols (like UDP) to unambiguously detect whether a port is open or not by means of external port

scanning. Also in some circumstances it might not be efficient to do external port scanning, e.g. if there are security measures to limit the rate a system can be probed. In those cases the accredited evaluator's test laboratory determines another means suitable to verify which ports are open.

7. **Test Objective:-** To ensured that on all network interfaces, only documented ports on the transport layer respond to requests from outside the system

8. **Test Plan**

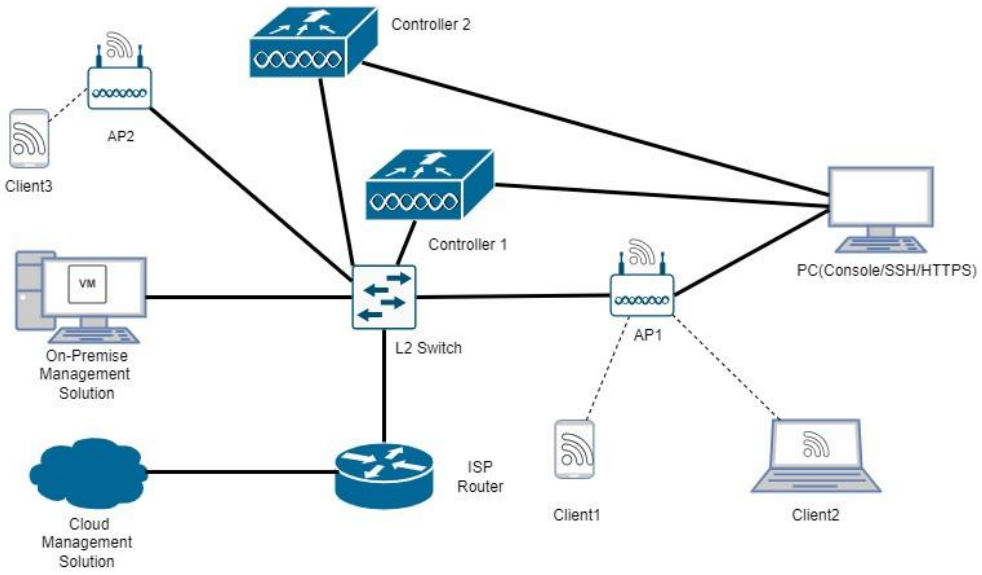
8.1. Number of Test Scenarios: 1

8.1.1. Test Scenario for Port Scanning using Nmap

- All the ports on all available interfaces should be scanned using Nmap.(Additional test scenarios are to be taken into consideration if tools like lsof, netstat are used)

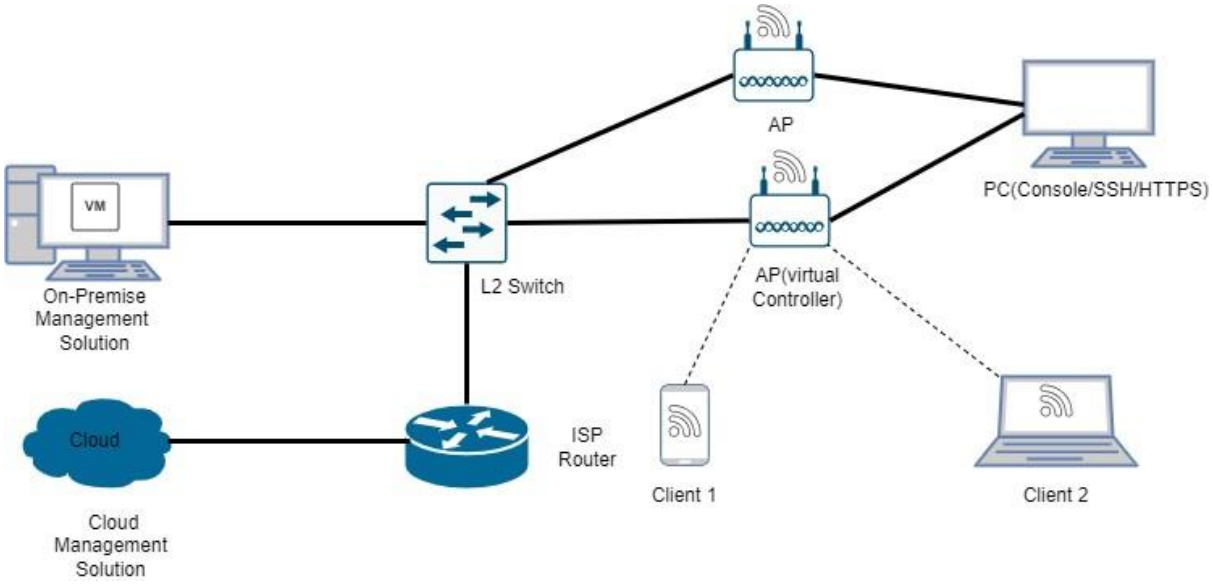
8.2. Test Bed Diagram

AP + Controller mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

8.3. Tools Required

Nmap

8.4. Test Execution Steps

1. Verification of the compliance to the prerequisites:
   a. Verification that the list of available network services is available in the documentation of the Network Product.
   b. Validation that all entries in the list of services are meaningful and reasonably necessary for the operation of the Network Product class
2. Identification of the open ports by means of capable port scanning tools or other suitable testing means.
3. Verification that the list of identified open ports matches the list of available network services in the documentation of the Network Product

9. **Expected Results :-** The used tool(s) name, their unambiguous version (also for plug-ins if applicable), used settings, and the relevant output containing all the technically relevant information about test results is evidence and shall be part of the testing documentation.
   All discrepancies between the list of identified open ports and the list of available network services in the documentation shall be highlighted in the testing documentation.

10. **Expected Form of Evidence:-** Output of ports can and list of identified discrepancies.

11. **Test Execution**

11.1 Test Case Number: 01

11.1.1 **Test Case Name:** TC_BVT_PORT_SCANNING_NMAP

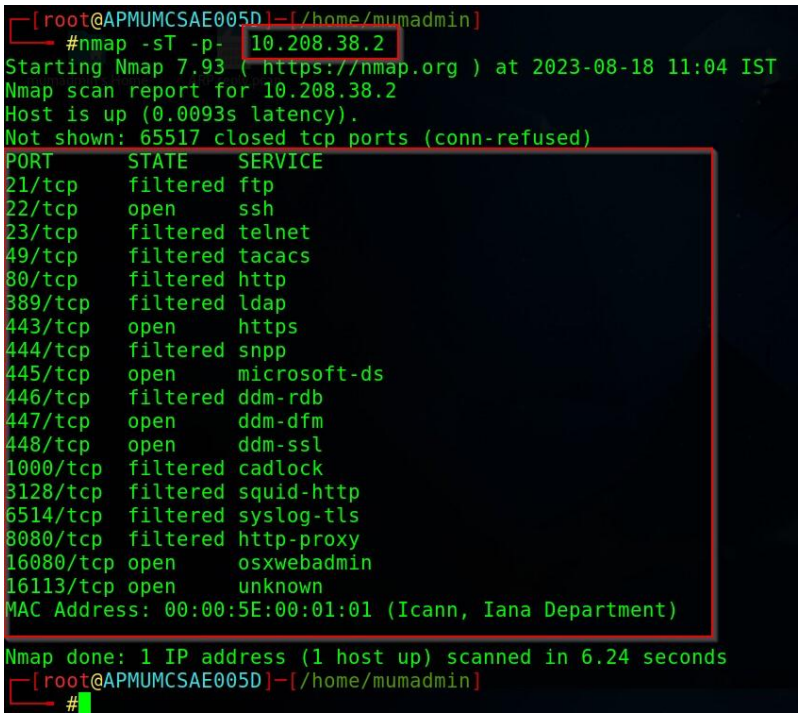
11.1.2 **Test Case Description:** On all network interfaces of DUT, only documented ports on the transport layer respond to requests from outside the system

11.1.3 **Execution Steps:**

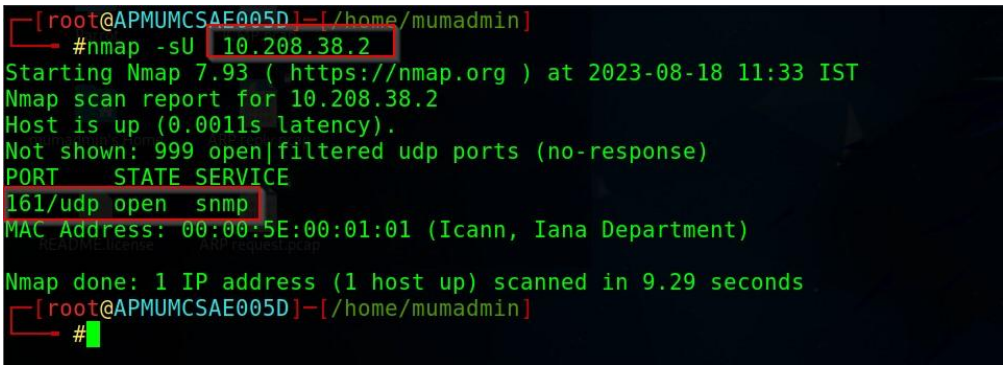
- Tester shall scan all the available transport layer protocols ports of the DUT using nmap with the following command

  For Example

  - For scanning TCP Ports, use below command.
    - ***sudo nmap -sT -PN -n -sV -T4 -p- -oN <DUT_IP>***
    - ***sudo nmap -p 1-65535 -T4 -A -v <DUT IP> (Default scan of TCP ports only)***
  - For scanning UDP Ports, use below command.
    - ***sudo nmap -sU -PN -n -sV -T4 -p- -oN <DUT_IP>***
  - For scanning SCTP Ports, use below command.
    - ***sudo nmap -sY -PN -n -sV -T4 -p- -oN <DUT_IP>***
  - -sT : TCP connect scan.
  - -sU : UDP scan
  - -sY : SCTP scan
  - -PN : Don't ping
  - -n : Disable reverse DNS
  - -p : Scan all ports
  - -oN : Output scan is normal. File specification , requests normal output be directed to given filename.
  - -T4: Faster Execution
  - -sV : Service Version
- Verify the result of the TCP PORT Scan



- Verify the result of the UDP PORT Scan



- Tester then shall verify if the ports mentioned as open by nmap on all the interfaces match the list provided by the vendor and also verify that no extra port is opened. (Note: This step has OEM dependancy).

11.1.4 **Test Observations:**

- **Case 1:** All the ports discovered to be open by port scanning tool match exactly to the list provided by the OEM

11.1.5 **Evidence Provided: -** Output of port scan.

12. **<u>Test Case Results</u>**

S. No	TEST CASS NAME	PASS/FAIL	Remarks
1	TC_BVT_PORT_SCANNING_NMAP	OEM Dependent	Port scan results to be verified against OEM document for list of open ports.

1.9.3: SSID Scanning

1.9.4: Vulnerability Scanning

Section 1.10: Operating System

1.10.1: Handling of ICMP

<DUT Details: > Ex: Router
<DUT Software Version:> : to be filled up
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

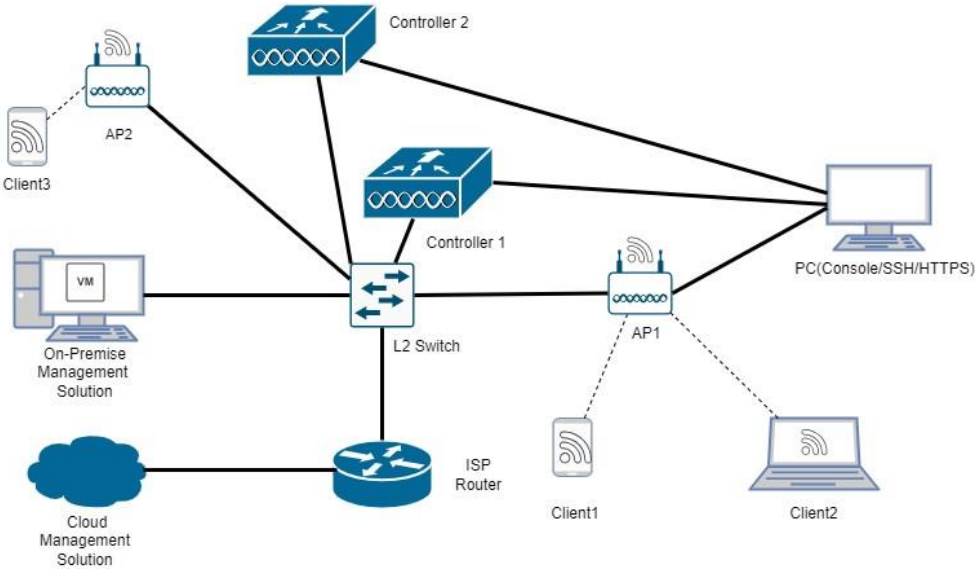
1. **<ITSAR Section No & Name> Section 1.10** Operating System
2. **<Security Requirement No & Name > 1.10.1: Growing Content Handling**
3. **<Requirement Description: >**
   a) Growing or dynamic content shall not influence system functions.
   b) A file system that reaches its maximum capacity shall lead to an event getting logged with appropriate message parameters and shall not stop Wi-Fi CPE from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided. The countermeasures are usage of dedicated filesystems, separated from main system functions, or quotas, or at least a file system monitoring
4. **DUT Confirmation Details**:
   <screenshot>
5. **DUT Configuration:** To configure the DUT for handling mechanism for log over flow and file system reaching max capacity

6. **Preconditions**:- OEM shall provide instruction to verify the DUT protection mechanism against log overflow(or any growing content) and file max capacity. The tester shall need the OS access level of the DUT

7. **Test Objective**:- DUT filesystem reaching its maximum capacity is to be logged with appropriate message parameters and shall not stop the CPE from functioning properly. Also there should exist countermeasures.

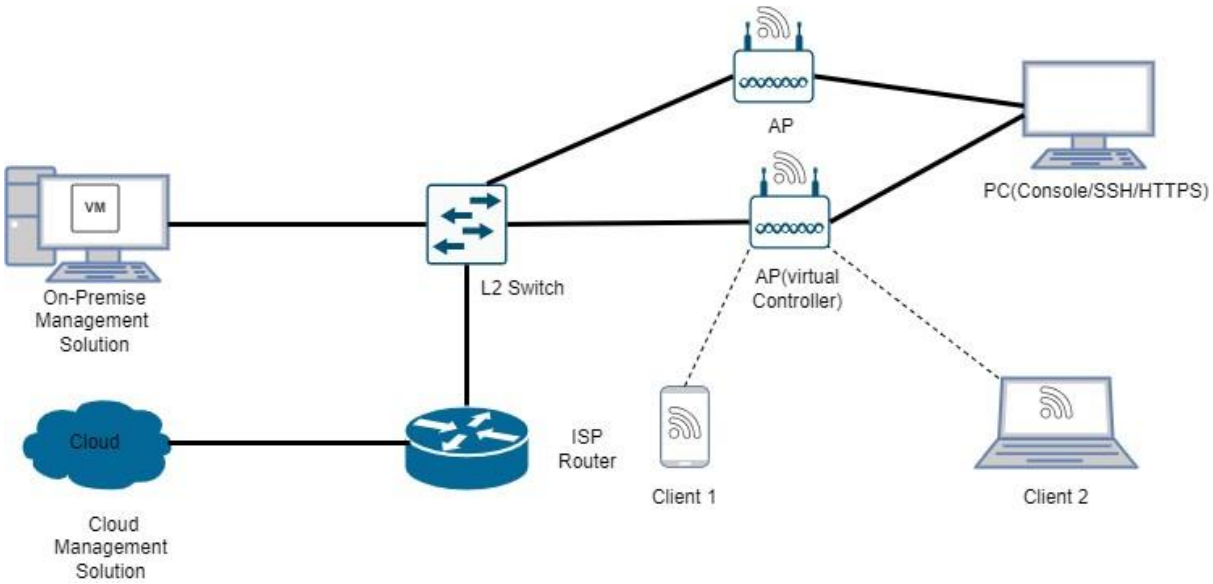
8. **Test Plan**
   8.1. Number of Test Scenarios:
   8.1.1. Test Scenario to check DUT's handling mechanism for log overflow
   8.1.2. Test Scenario to check DUT's handling mechanism for file max capacity

   8.2. Test Bed Diagram



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

8.3. Tools Required

- DUT

8.4. Test Execution Steps

- The tester shall verify from the OEM documentation for the supported protection mechanism for log overflow
- The tester shall generate logs to fill up the threshold to verify the DUT's supported mechanism to handle it

- The tester shall also check the working condition of the DUT
- The tester shall create a file directory and attempt to fill up the storage space exceeding threshold and verify DUT's protection mechanism against it, also verifying the DUT's status

9. **Expected Results for Pass:** DUT handles the log overflow and file max capacity without affecting its the working condition

10. **Expected Format of Evidence:** Screenshots of DUT CLI (at OS level)

11. **Test Execution:**

11.1 Test Case Number: 01

11.1.1 **Test Case Name** check DUT's handling mechanism for log overflow

11.1.2 **Test Case Description:** The following test case is done to verify the DUT's handling mechanism for log overflow

11.1.3 **Execution Steps:**

- Access the DUT's CLI and access the config mode
- Enter "sh logs" to see the log entries

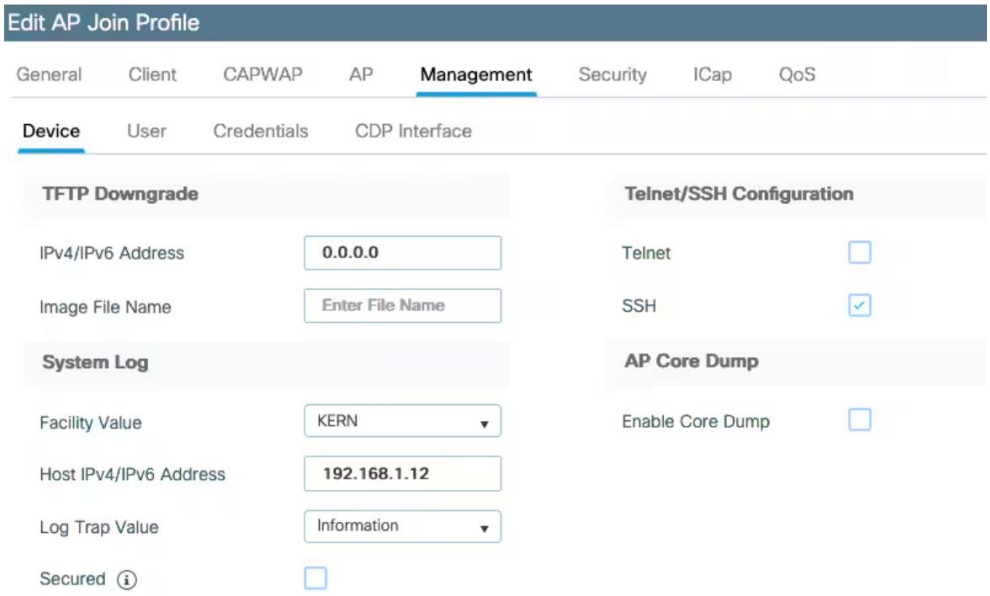
```
CM4500-Acumen (config) #
CM4500-Acumen (config) # show log files
INDEX   START TIME            END TIME              FILE SIZE  UNCOMPRESSED SIZE
                                                      (MB)         (MB)
main    2020/07/14 06:00:01   2020/07/14 11:55:30   0.665        0.665
1       2020/07/10 22:40:57   2020/07/14 06:00:01   0.219        5.000
2       2020/07/10 18:51:03   2020/07/10 22:40:57   0.116        5.000
3       2020/07/10 14:55:47   2020/07/10 18:51:03   0.118        5.000
4       2020/07/10 11:00:01   2020/07/10 14:55:47   0.116        5.000
5       2020/07/10 07:06:01   2020/07/10 11:00:01   0.119        5.000
6       2020/07/10 03:14:04   2020/07/10 07:06:01   0.121        5.000
7       2020/07/09 23:25:21   2020/07/10 03:14:04   0.121        5.000
8       2020/07/09 19:38:23   2020/07/09 23:25:21   0.119        5.000
9       2020/07/09 15:50:08   2020/07/09 19:38:23   0.120        5.000
10      2020/07/09 11:58:39   2020/07/09 15:50:08   0.120        5.000
CM4500-Acumen (config) #
CM4500-Acumen (config) #
CM4500-Acumen (config) #
```

Here when we generate logs , the main file upon reaching the threshold of 5MB(in uncompressed format) , it starts making archives of it (from 1 – 10), once the 10th archive of the main file reaches , it gets deleted and a new log entry is appended at the start

```
CM4500-Acumen (config) #
CM4500-Acumen (config) #
CM4500-Acumen (config) # show log file
INDEX   START TIME            END TIME              FILE SIZE  UNCOMPRESSED SIZE
                                                      (MB)         (MB)
main    2020/07/16 02:54:30   2020/07/16 03:50:52   0.126        0.126
1       2020/07/14 06:00:01   2020/07/16 02:54:30   0.309        5.000
2       2020/07/10 22:40:57   2020/07/14 06:00:01   0.219        5.000
3       2020/07/10 18:51:03   2020/07/10 22:40:57   0.116        5.000
4       2020/07/10 14:55:47   2020/07/10 18:51:03   0.118        5.000
5       2020/07/10 11:00:01   2020/07/10 14:55:47   0.116        5.000
6       2020/07/10 07:06:01   2020/07/10 11:00:01   0.119        5.000
7       2020/07/10 03:14:04   2020/07/10 07:06:01   0.121        5.000
8       2020/07/09 23:25:21   2020/07/10 03:14:04   0.121        5.000
9       2020/07/09 19:38:23   2020/07/09 23:25:21   0.119        5.000
10      2020/07/09 15:50:08   2020/07/09 19:38:23   0.120        5.000
CM4500-Acumen (config) #
CM4500-Acumen (config) #
CM4500-Acumen (config) #
```

(in case of split)

On 9800 Controller, you can change these parameters in the Configuration -> AP Join profile, under Management.



This will ensure that the AP syslogs the log output to the external syslog server

11.1.4 **Test Observations:**

- It was observed that in log overwriting is used to handle logs
- The AP can also be configured through the controller to unicast the syslog to a specific server

11.1.5 **Evidence Provided**: - Screenshots provided above

11.2 **Test Case Number:** 02

11.2.1 **Test Case Name** check DUT's handling mechanism file max capacity

11.2.2 **Test Case Description:** The following test case is done to verify the DUT's handling mechanism for file max capacity

11.2.3 Execution steps

- Initially logged into the test machine by providing the right credentials and created a large file as described in the below screenshots by providing the command **dd if=/dev/zero of=demo2.txt bs=1M count=5120** within the test machine terminal. A large file of 5.4 GB will be created as shown below in the screenshot.

```
sravani@sravani-dotra:~$ dd if=/dev/zero of=demo2.txt bs=1M count=5120
5120+0 records in
5120+0 records out
5368709120 bytes (5.4 GB, 5.0 GiB) copied, 45.0217 s, 119 MB/s
```

Fig 2: Creation of large file.

- The screenshot below displays the exact directory location where the created demo.txt file is stored after listing the directories within the system.

```
sravani@sravani-dotra:~$ ls
15dec.cfg           demo.txt
anoop               Desktop
capture1.pcap       Documents
cdot_audit.txt      Downloads
clients.conf        enable
Credential_CSON     etc
CSON_DB_3.6_NMAP    eth1_ntp.pcap
CSON_FW_3.6_NMAP    google-chrome-stable_current_amd64.deb
demo2.txt           hari2.txt
```

Fig3: Large file created and Stored within a directory.

- To display the command for the file system give the command show file-system summary. The provided screenshot describes the file system summary of the router, which includes the file paths of different directories.

```
CTX-2000# show file-system-summary | include ?
Possible completions:
  <Regular Expression - restricted subset>
  -a    The number of lines to include after the match
  -b    The number of lines to include before the match
  -c    The number of context lines to include
CTX-2000# show file-system-summary | include mnt
/dev/sda5        9.8G  1.7G  7.6G  19% /mnt/onl/images
/dev/sda6         14G   35M   13G   1% /mnt/onl/data
/dev/sda3        2.0G   48M  1.8G   3% /mnt/onl/boot
/dev/sda4        2.0G   66M  1.8G   4% /mnt/onl/config
CTX-2000# show file-system-summary | include /
devtmpfs         1.0M     0  1.0M   0% /dev
proc                0     0     0    - /proc
sysfs               0     0     0    - /sys
overlay          1.2G   14M  1.2G   2% /
/dev/sda5        9.8G  1.7G  7.6G  19% /mnt/onl/images
/dev/sda6         14G   35M   13G   1% /mnt/onl/data
/dev/sda3        2.0G   48M  1.8G   3% /mnt/onl/boot
/dev/sda4        2.0G   66M  1.8G   4% /mnt/onl/config
tmpfs            786M  1.4M  785M   1% /run
tmpfs            5.0M     0  5.0M   0% /run/lock
tmpfs            3.9G   27M  3.9G   1% /var/volatile
cgroup2             0     0     0    - /sys/fs/cgroup
tmpfs            1.6G   30M  1.6G   2% /dev/shm
devpts              0     0     0    - /dev/pts
binfmt_misc         0     0     0    - /proc/sys/fs/binfmt_misc
tmpfs            786M  1.4M  785M   1% /run/netns
nsfs                0     0     0    - /run/netns/vrf2
```

Fig 4: Displaying the file system within the memory before loading the file.

- Transfer the demo.txt file from the system to the storage unit of the router by files download URL **scp://192.168.129.13/home/sravani/demo2.txt user sravani vrf mgmt-vrf** and providing the accurate password when prompted. The below screenshot displays the DUT Response when the file size goes beyond the threshold value of the router memory space then the DUT responds Failure writing output to destination. The directory limit of /mnt/onl/images is 1.9GB

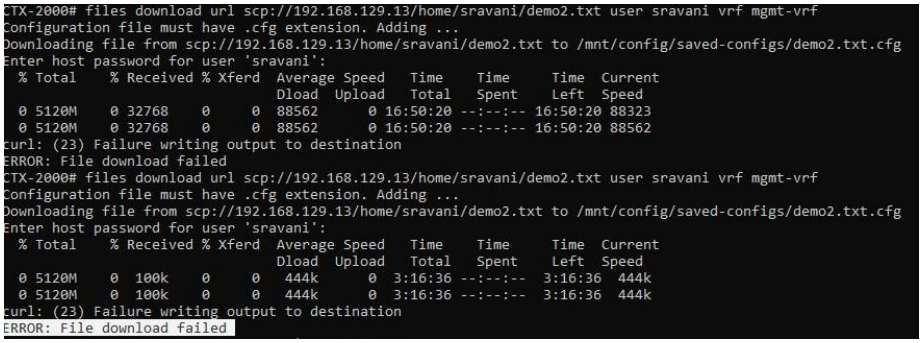


Fig 5: DUT response after loading the large file.

- The screenshot below displays the usage limit reached 100 per cent corresponding to the file path /mnt/onl/config where demo2.txt file was loaded to obtain a response from DUT on this action

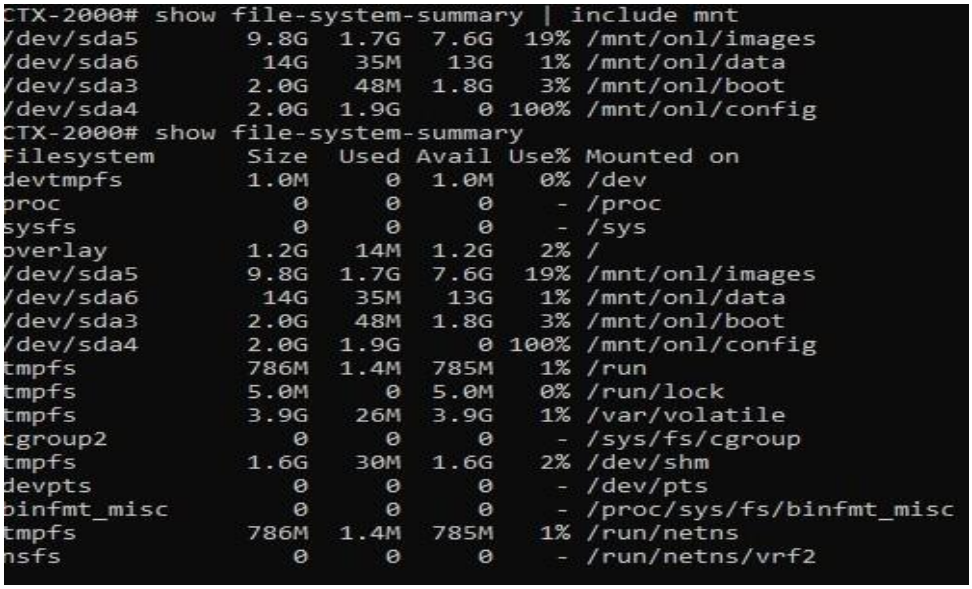


Fig 6: Shows file system within the memory after loading the file.

Even though there was more amount of file pending to be uploaded, the DUT didn't let the complete upload

11.2.4 Test Observations: - It was observed that the DUT does not allow mounting of files after a threshold

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	check DUT's handling mechanism for log overflow	FAIL	
2	check DUT's handling mechanism file max capacity	Pass	

1.10.2: Privilege Escalation

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.10** Operating **System**
2. **<Security Requirement No & Name > 1.10.2: Privilege Escalation**
3. **<Requirement Description: > Processing** of ICMP version 4 (ICMPv4) and ICMP version 6 (ICMPv6) packets which are not required for operation shall be disabled on the Wi-Fi CPE. There are certain types of ICMPv4 and ICMPv6 that are not used in most networks, but represent a risk. ICMP message types which on receipt lead to responses or to configuration changes are not mentioned in this requirement, but they may be necessary to support relevant and specified networking features. Those must be documented. Certain ICMP types are generally permitted and do not need to be specifically documented. Those are marked as "Permitted" in the table below.

Type (IPv4)	Type (IPv6)	Description	Send	Respond to
0	128	Echo Reply	Optional (i.e. as automatic reply to "Echo Request")	N/A
3	1	Destination Unreachable	Permitted	N/A
8	129	Echo Request	Permitted	Optional
11	3	Time Exceeded	Optional	N/A
12	4	Parameter Problem	Permitted	N/A
N/A	2	Packet Too Big	Permitted	N/A
N/A	135	Neigbor Solicitation	Permitted	Permitted
N/A	136	Neighbor Advertisement	Permitted	N/A

WiFi-CPE shall not respond to, or process (i.e., do changes to configuration) under any circumstances certain ICMP message types as marked in the below table.

Type (IPv4)	Type (IPv6)	Description	Send	Respond to	Process (i.e. do changes to configuration)
5	137	Redirect	N/A	N/A	Not Permitted
13	N/A	Timestamp	N/A	Not Permitted	N/A
14	N/A	Timestamp Reply	Not Permitted (i.e. as automatic reply to "Timestamp")	N/A	N/A
N/A	133	Router Solicitation	N/A	Not Permitted	Not Permitted
N/A	134	Router Advertisement	N/A	N/A	Not Permitted

4. **DUT Confirmation Details**:

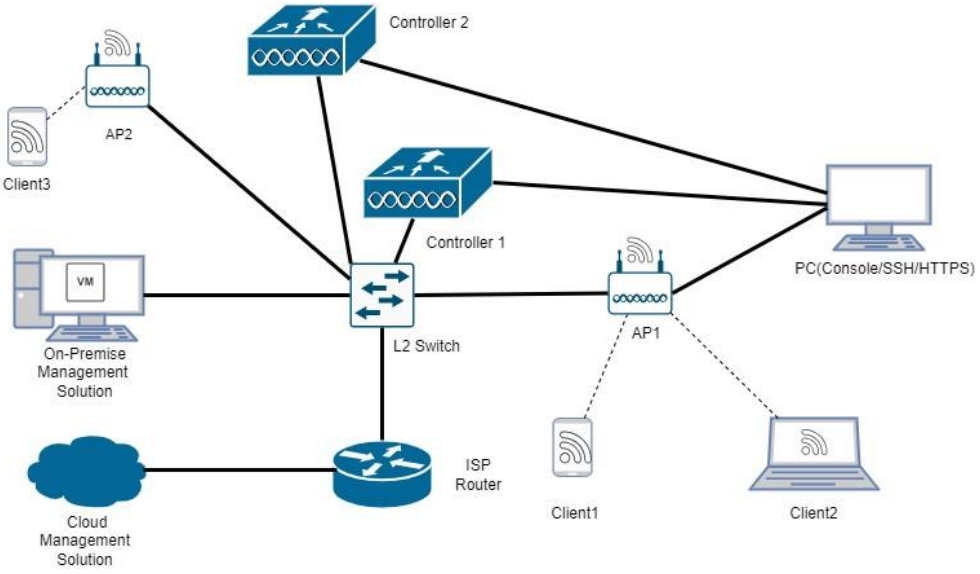
5. **DUT Configuration:** Configure the DUT to accept/deny/process/send/respond to certain ICMP types of messages as per the requirement

6. **Preconditions:**- OEM shall provide instruction to enable/disable ICMPv4 and ICMPv6 packets which are as per the requirement

7. **Test Objective:-** To check DUT to accept/deny/process/send/respond to certain ICMP types of messages as per the requirement

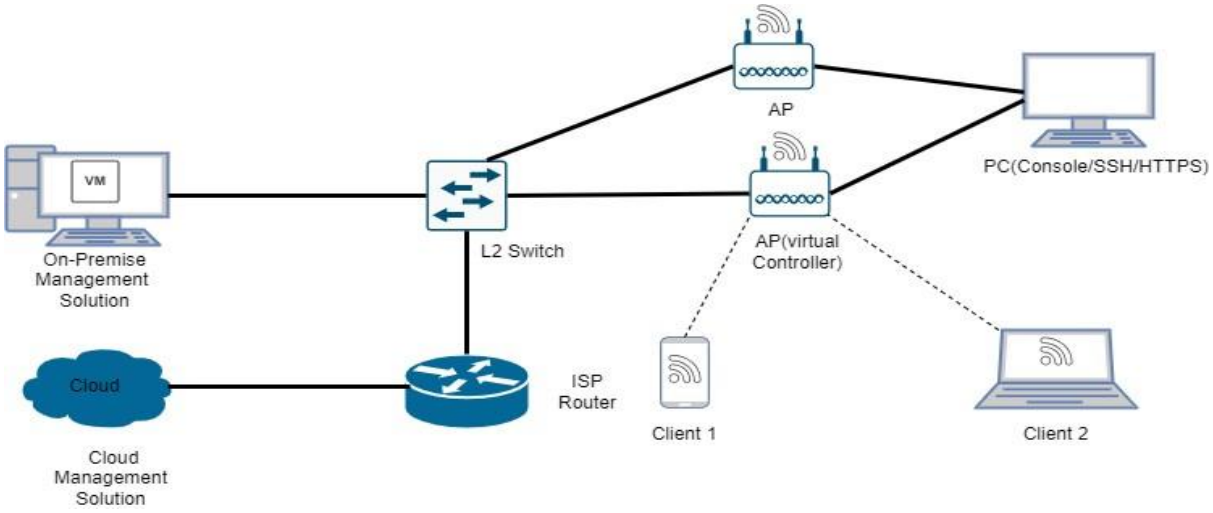
8. **Test Plan**
   - 8.1. Number of Test Scenarios:
     - 8.1.1. Test Scenario whether DUT denies the unallowed ICMP ipv4 and ipv6 type packets
     - 8.1.2. Test Scenario to check whether DUT's configuration changes after certain ICMP type packets
     - 8.1.3. Test Scenario to test whether DUT has optional type ICMP packets disabled by default

   - 8.2. Test Bed Diagram



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

8.3. Tools Required

- DUT

8.4. Test Execution Steps :- Initiate a factory reset to bring the DUT to its default state
The Tester Trigger samples of the certain ICMP types of messages from the tester machine (e.g., Scapy) to the DUT and verifies by appropriate means.
The Tester shall Capture the traffic between DUT and Test machine through Wireshark and do analysis the logs of DUT

9. **Expected Results for Pass:** DUT doesn't permit the unallowed ICMP packets as mentioned in the requirement , DUT doesn't change its core configuration after certain icmp packets

10. **Expected Format of Evidence:** Screenshots

11. **Test Execution:**

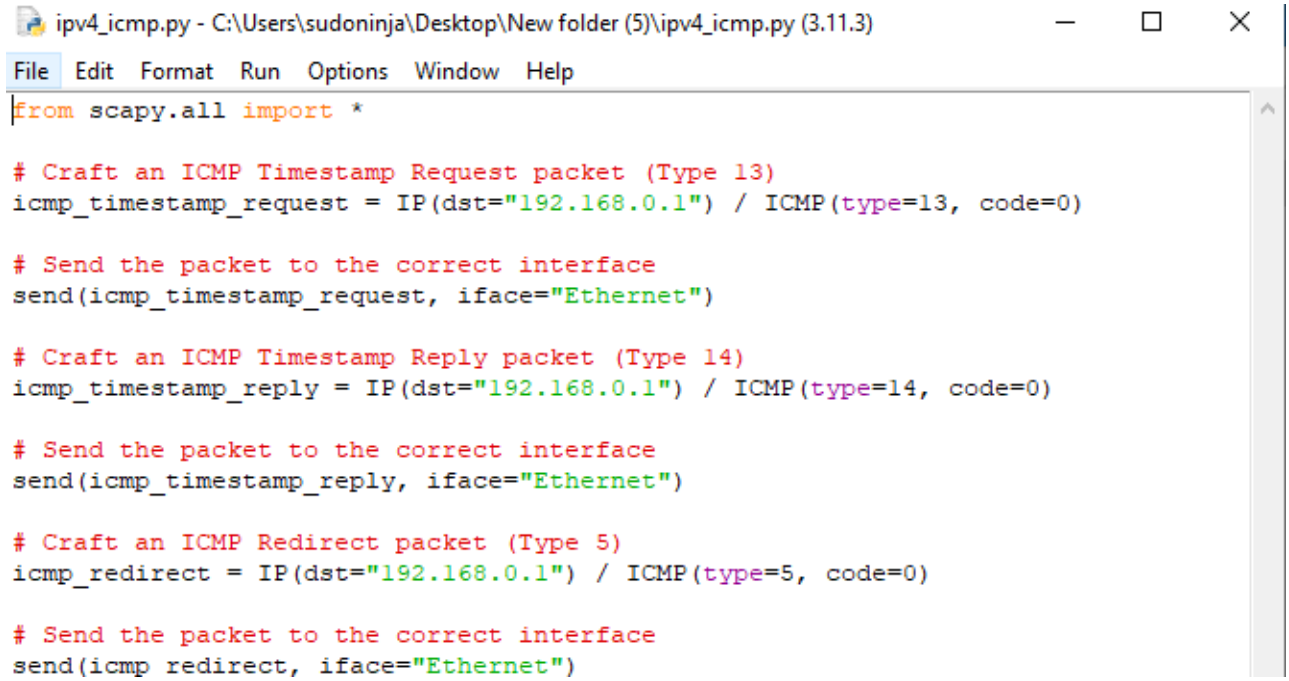
11.1 Test Case Number: 01

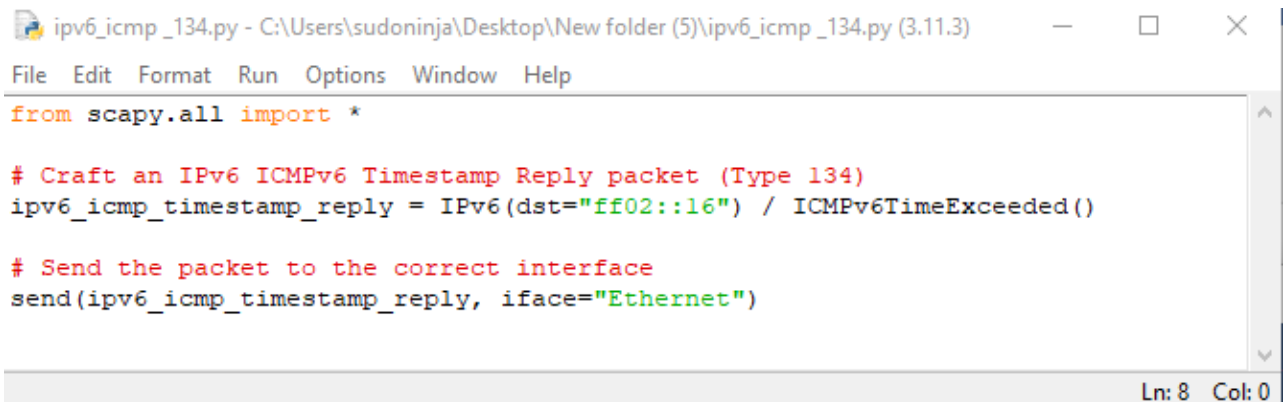
11.1.1 **Test Case Name:** DUT denies the unallowed ICMP ipv4 and ipv6 type packets

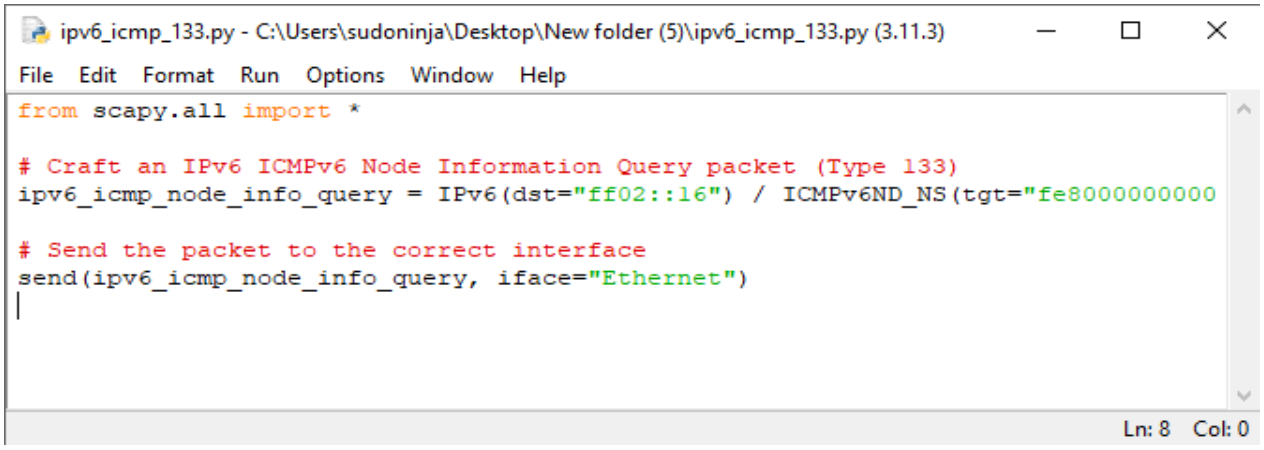
11.1.2 **Test Case Description:** The tester shall verify if the DUT doesn't allow the ICMP packets that are mentioned as Non permitted in the requirement

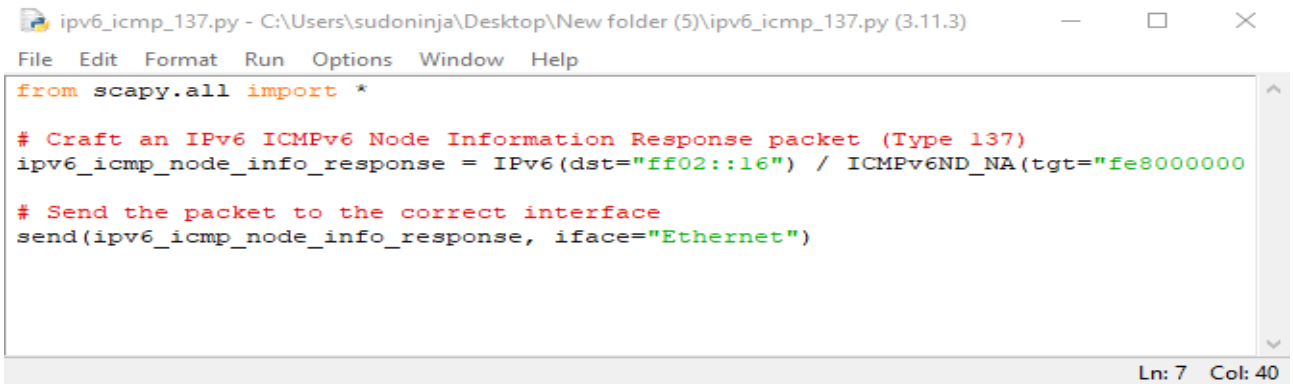
11.1.3 **Execution Steps:**

- The Tester creates the python script using Scapy to send specified types of ICMPv4 and ICMPv6 messages to DUT from Test machine. Screenshot of the python scripts attached below,

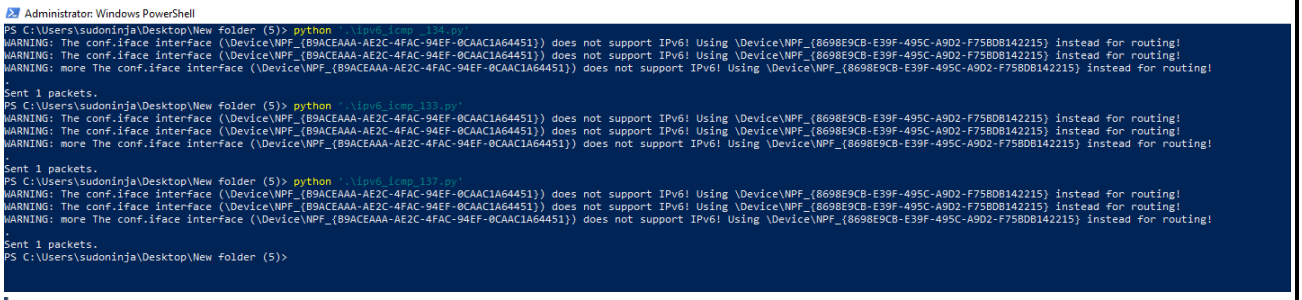


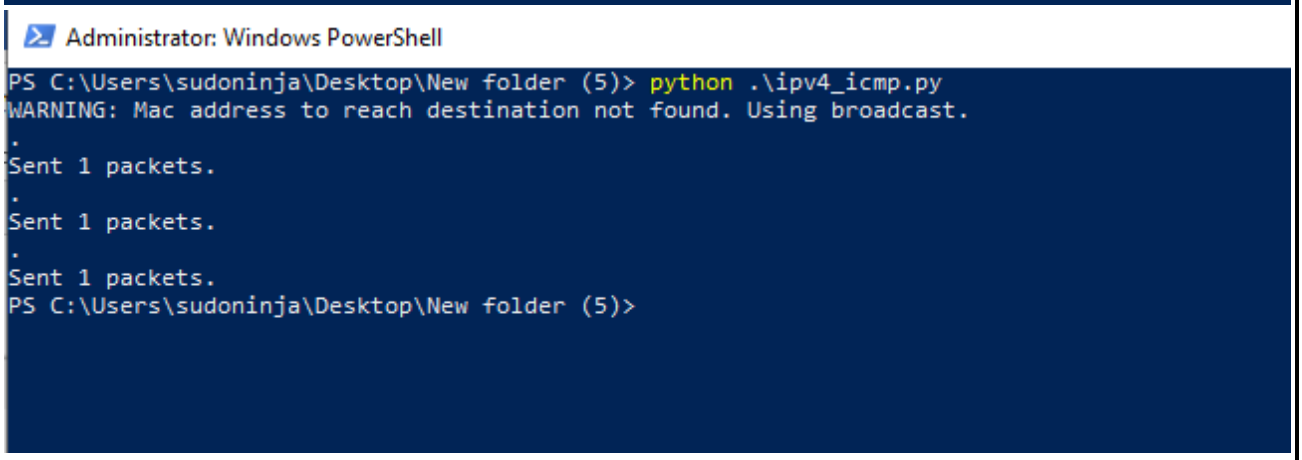






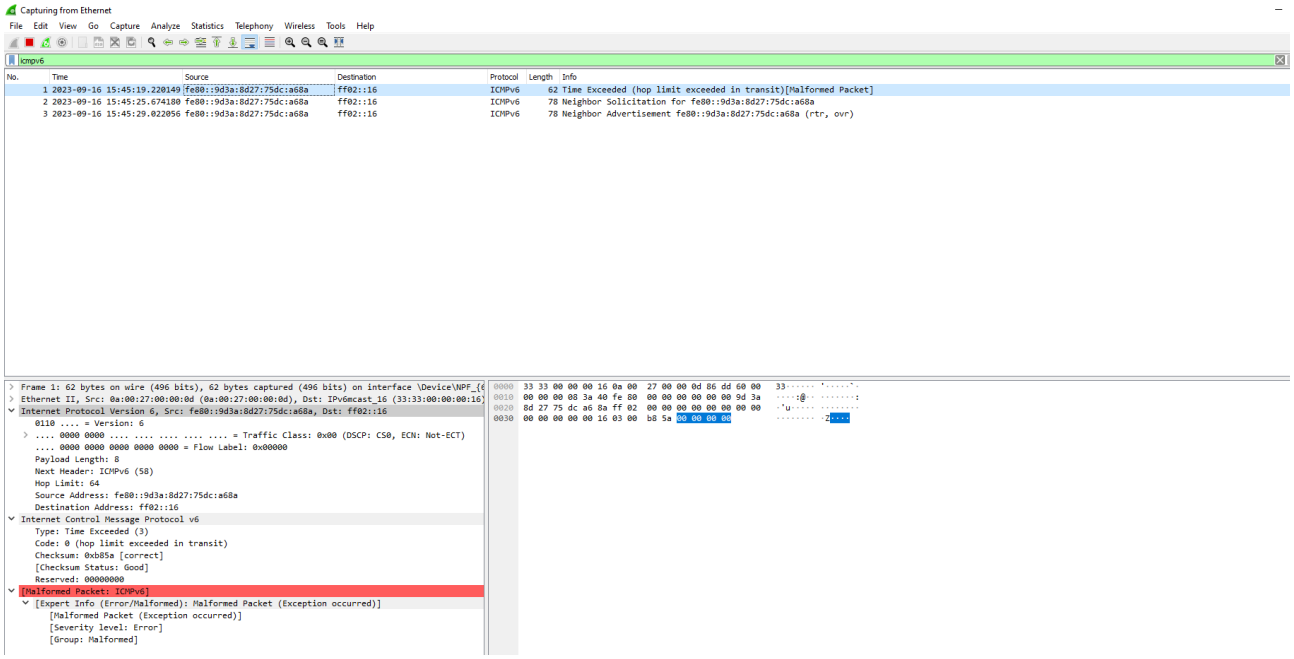
- The Tester initiates a ICMPv4 and ICMPv6 traffic using Python script



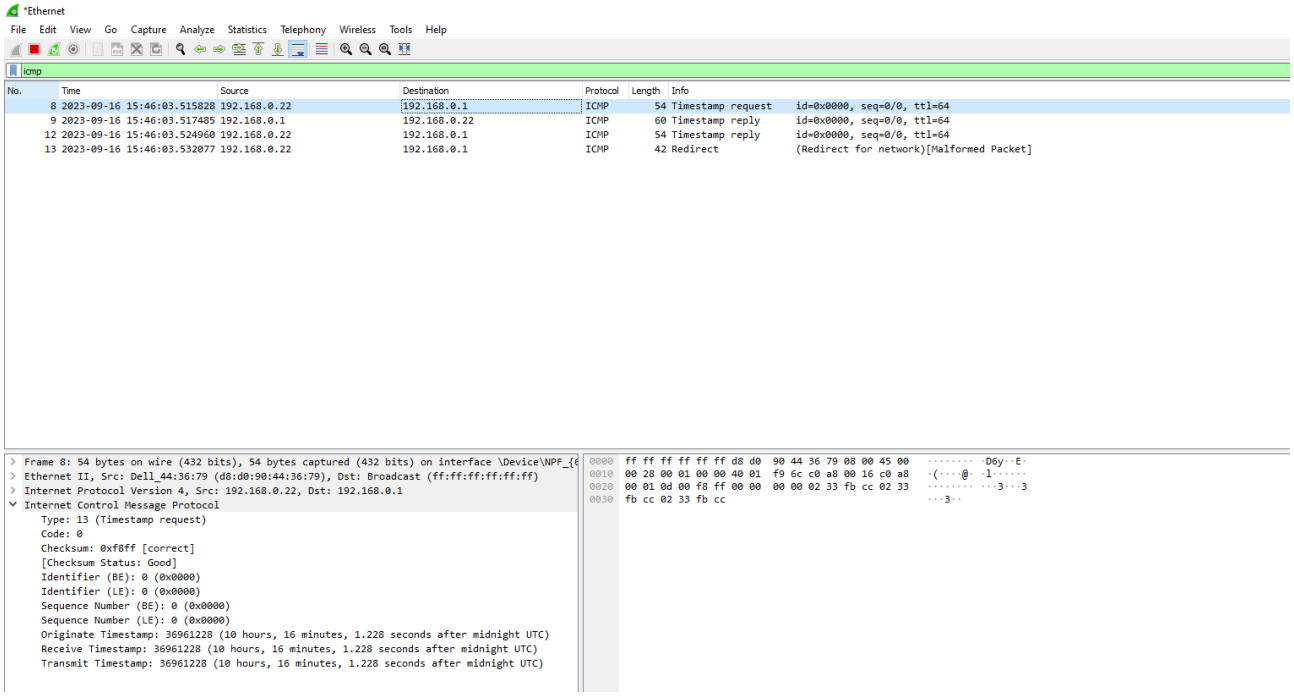


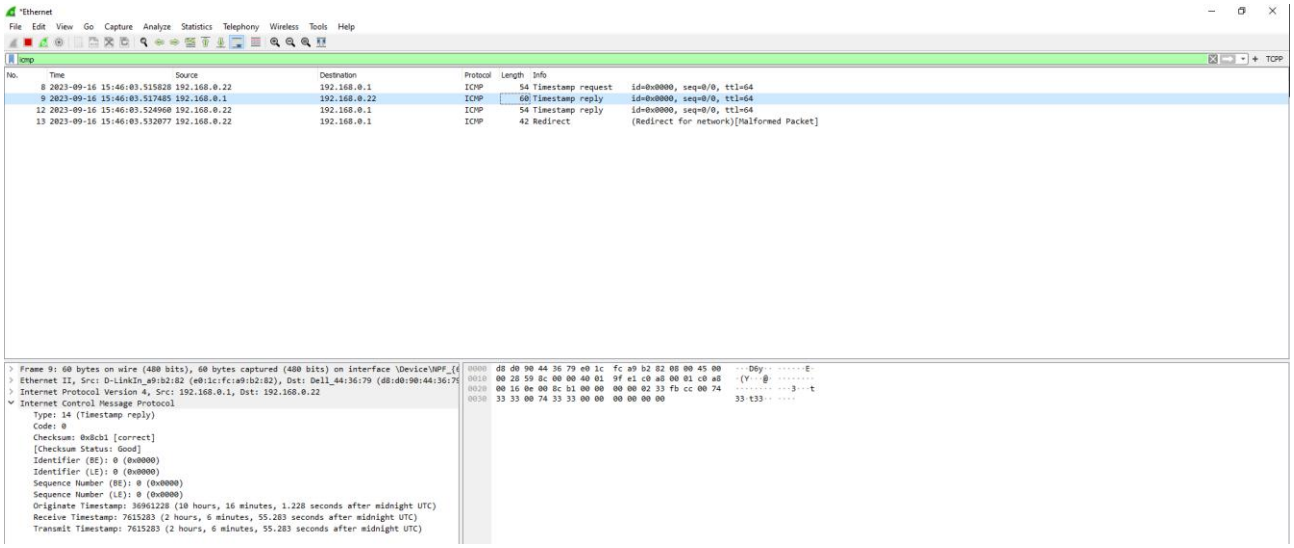
- The Tester captures the traffic between DUT and the Test Machine through Wireshark and analyze the output.

Neighbour Solicitation & Neighbour Advertisement

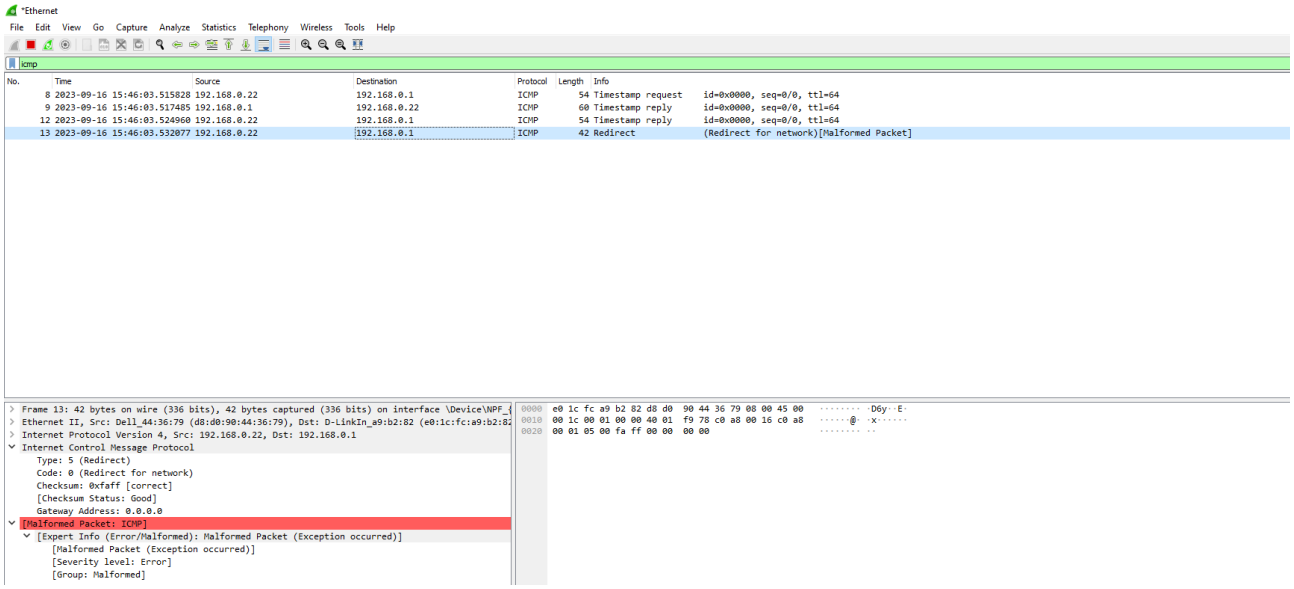


Time stamp & timestamp reply





Redirect



(here the tester must notice that the redirect packet sent here is the malformed redirect packet. The Dut may reject the packet due to its malformed nature rather than it being redirect. Hence the tester must send a legitimate Redirect packet as below)

- The Tester observed that DUT is dropping the blocked ICMP packets as shown in Wireshark.
- The Tester observed that the DUT doesn't reply to certain ICMP type messages which are not required for operation.

Note : As per mentioned in the 2nd part of the table , the requirement is to be tested without any packet filtering (eg. ACL) but in its default state

11.1.4 **Test Observations:**

- The ICMP messages which are "Not Permitted" or "Optional" to generate a response from the network product do not generate a response.

- The ICMP messages which are "Not Permitted" to change the configuration of the network element do not change the configuration.
- ICMP message types which lead to responses or to configuration changes on receipt, if neither mentioned in the requirement nor in the documentation are not enabled.

11.1.5 **Evidence Provided:-** Screenshots

12. **Test Case Result:**

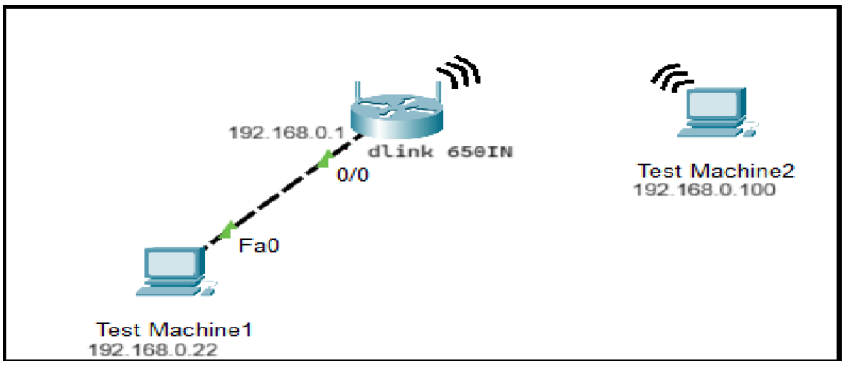
S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	to check the disabling of icmp packets not necessary	FAIL	

1.10.3 System account identification

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.10** Operating **System**
2. **<Security Requirement No & Name > 1.10.3: System account identification**
3. **<Requirement Description: >** Each system account in Operating system of the CPE shall have a unique identification, the OEM to provide information on implementation mechanism for this requirement.
4. **DUT Confirmation Details**:
5. **DUT Configuration:**
6. **Preconditions:-** OEM shall provide confirmation that each system account in Operating system of the CPE shall have a unique identification. OEM should share the supporting document.
7. **Test Objective**
   To check DUT's doesn't support/disable privilege escalation without authentication
8. **Test Plan**
   8.1. Number of Test Scenarios:
   8.1.1. Test Scenario to check whether all newly created system accounts having a unique identification (UID).

   8.2. Test Bed Diagram



   8.3. Tools Required
   - DUT

   8.4. Test Execution Steps
   - The Tester shall create multiple system accounts on DUT.

- The Tester shall check whether all newly created system accounts having a unique identification (UID).

9. **Expected Results for Pass:**

10. **Expected Format of Evidence:** Screenshots

11. **Test Execution:**

11.1 Test Case Number: 01

11.1.1 **Test Case Name:** Unique UID

11.1.2 **Test Case Description:** The Tester shall check whether all newly created system accounts having a unique identification (UID)..

11.1.3 **Execution Steps:** In DUT, there is no option to create any system or user account

11.1.4 **Test Observations:** The Tester verified the UIDs are not different and, in particular, only the root account should have UID = 0

11.1.5 **Evidence Provided:**- Screenshots

12. **Test Case Result:**

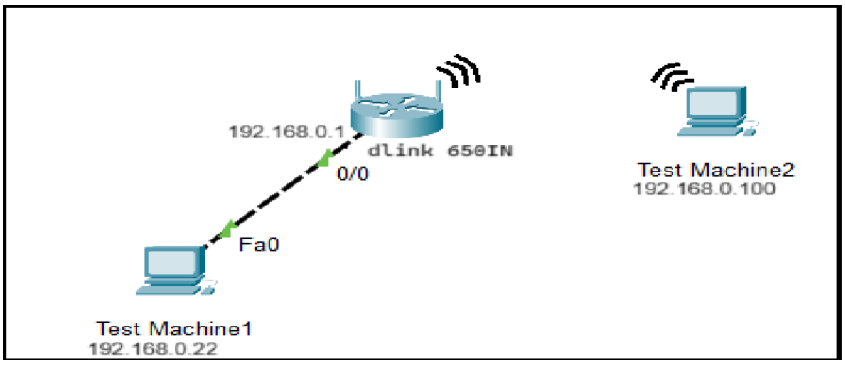
S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Unique UID	PASS	No feature to create a user account

2.10.4 OS-Hardening Kernel Security

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.10** Operating **System**
2. **<Security Requirement No & Name > 1.10.4: OS-Hardening Kernel Security**
3. **<Requirement Description: > OEM** may submit the process for OS Hardening undertaken to justify that the OS is sufficiently hardened and Kernel based applications / functions not needed for the operation of the CPE are deactivated. OEM to provide information on steps taken in this regard.

4. **DUT Confirmation Details**:
5. **DUT Configuration:**
6. **Preconditions: -** OEM shall provide OS Hardening undertaken and provide information on steps taken in this regard.
7. **Test Objective: -** To check DUT's support OS Hardening
8. **Test Plan**
   - 8.1. Number of Test Scenarios:
     - 8.1.1. Test Scenario to check DUT support OS Hardening from OEM documents
     - 8.1.2. Test Scenario to check OS Hardening functions of DUT
   - 8.2. Test Bed Diagram



   - 8.3. Tools Required
     - DUT
   - 8.4. Test Execution Steps
     - The Tester reviews the process for OS Hardening undertaken from OEM that justify that the OS is sufficiently hardened.
     - The Tester shall verify that IP Packet Forwarding / Proxy ARP / Directed broadcast / IP Multicast / Gratuitous ARP feature are disabled by default on the network product.
     - The Tester reviews the process for OS Hardening undertaken from OEM that justify that the OS is sufficiently hardened).

9. **Expected Results for Pass:**

10. **Expected Format of Evidence:** Screenshots

11. **Test Execution:**

11.1 Test Case Number: 01

11.1.1 **Test Case Name:** OS Hardening from OEM documents

11.1.2 **Test Case Description:** The Tester reviews the process for OS Hardening undertaken from OEM that justify that the OS is sufficiently hardened.

11.1.3 **Execution Steps:**

Note: Software test document is not available with lab because this is the market purchased product used for demo testing.

11.1.4 **Test Observations:**

Note: Software test document is not available with lab because this is the market purchased product used for demo testing.

11.1.5 **Evidence Provided:-** Screenshots

11.2 Test Case Number: 02

11.2.1 **Test Case Name:** OS Hardening of DUT

11.2.2 **Test Case Description:** The Tester shall verify that IP Packet Forwarding / Proxy ARP / Directed broadcast / IP Multicast / Gratuitous ARP feature are disabled by default on the network product.

11.2.3 **Execution Steps:** The Tester checked the DUT and found that there is no IP Packet Forwarding / Proxy ARP / Directed broadcast / IP Multicast / Gratuitous ARP feature shown in DUT.
The Tester shall review the OEM document to verify the OS hardening document.

11.2.4 **Test Observation**: - OEM Undertaking required Evidence

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	OS Hardening from OEM		No OEM document available
2	OS Hardening of DUT		No OS Hardening functions observed

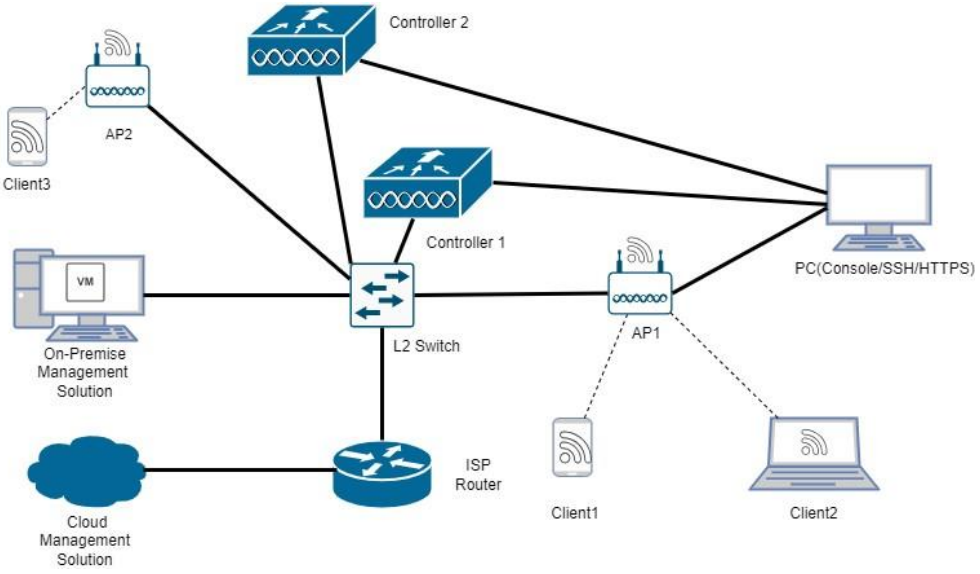
1.10.5: Protection from buffer overflows

<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 1.10** Operating **System**
2. **<Security Requirement No & Name > 1.10.5: Protection from buffer overflows**
3. **<Requirement Description: >** Kernel based network functions not needed for the operation of the network element shall be deactivated.
   In particular, the following ones shall be disabled by default:

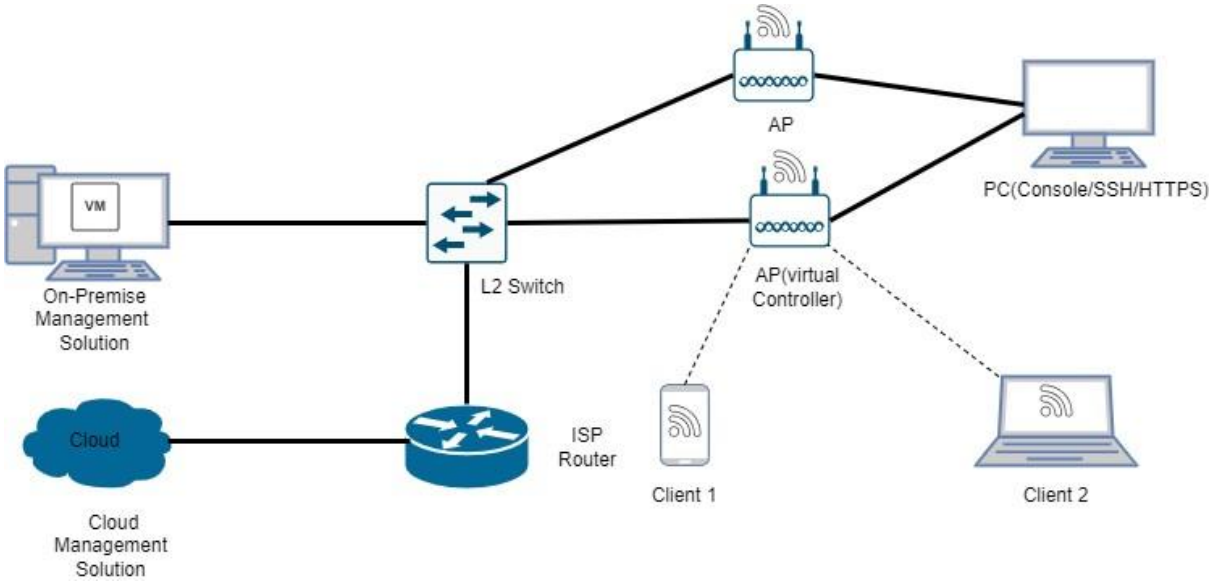
   a) Proxy Address Resolution Protocol (ARP) (to prevent resource exhaustion attack and man-in-the-middle attacks)
   b) Directed broadcast (to prevent attacks like Smurf, Denial of Service etc.,)
   c) IPv4 Multicast handling. In particular, all packets with IP source or destination address belonging to the multicast IP ranges (224.0.0.0 through 239.255.255.255) shall be discarded by default and multicast route caching and forwarding shall be disabled to prevent Smurf and Fraggle attacks. A configuration option shall be available to enable the IPv4 multicast handling if required.
   d) Gratuitous ARP messages (to prevent ARP Cache Poisoning attacks)

4. **DUT Confirmation Details**:
5. **DUT Configuration:** No configuration needed
6. **Preconditions** OEM shall provide OS Hardening undertaken and provide information on steps taken in this regard.
   The tester should do factory reset of the DUT.
7. **Test Objective:-** To check DUT support OS Hardening functions and verify the compliance as per the requirement
8. **Test Plan**
   8.1. Number of Test Scenarios:
      8.1.1. Test Scenario to check DUT support OS Hardening from OEM documents
      8.1.2. Test Scenario to check OS Hardening functions of DUT
   8.2. Test Bed Diagram



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

8.3. Tools Required

- DUT

8.4. Test Execution Steps

- The Tester reviews the process for OS Hardening undertaken from OEM that justify that the OS is sufficiently hardened.
- The Tester shall verify that ~~IP Packet Forwarding~~ / Proxy ARP / Directed broadcast / IP Multicast / Gratuitous ARP feature are disabled by default on the network product.

- The Tester reviews the process for OS Hardening undertaken from OEM that justify that the OS is sufficiently hardened).

9. **Expected Results for Pass:** The DUT has kernel based functions disabled which can harden the OS security
10. **Expected Format of Evidence:** Screenshots
11. **Test Execution:**

11.1 Test Case Number: 01

11.1.1 **Test Case Name:** OS Hardening from OEM documents

11.1.2 **Test Case Description:** The Tester reviews the process for OS Hardening undertaken from OEM that justify that the OS is sufficiently hardened.

11.1.3 **Execution Steps:**

- The tester reviews the OEM documents for the kernel based functions supported in the DUT
- The tester shall use the commands to check if the following kernel based functions are disabled- IP Packet Forwarding, Proxy Address Resolution Protocol (ARP), Directed broadcast, Gratuitous ARP messages, IPv4 Multicast handling.
- For proxy ARP verify that

net.ipv4.conf.all.proxy_arp = 0 in the linux sysctl.conf file.

For directed broadcast verify that

net.inet.ip.directed-broadcast=0

Similarly it can be checked for the other OS Hardening functions too if they are disabled as per the OEM documents

11.1.4 **Test Observations:**

Note: Software test document is not available with lab because this is the market purchased product used for demo testing.

11.1.5 **Evidence Provided**

11.2 Test Case Number: 02

11.2.1 **Test Case Name:** OS Hardening of DUT

11.2.2 **Test Case Description:** The Tester shall verify that ~~IP Packet Forwarding~~ / Proxy ARP / Directed broadcast / IP Multicast / Gratuitous ARP feature are disabled on the network product.

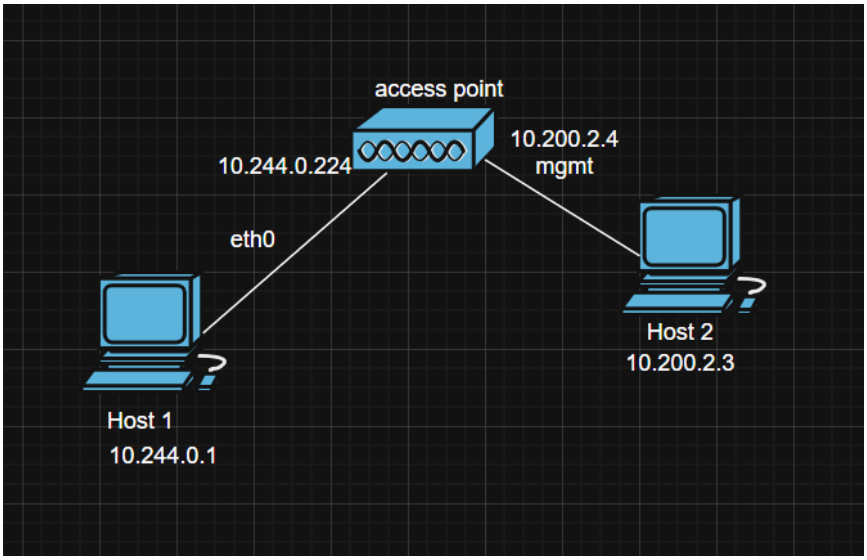
11.2.3 **Execution Steps:**

(a) (For Proxy ARP)

- The tester shall connect the DUT with the two test machines in two of its interfaces

  Host 1 is connected to IF1 on subnet A

  Host 2 is connected to IF2 on subnet B
- The network analyzer on the DUT is configured to capture all the packets through the DUT



- Host 1 is connected to DUT on interface eth0

```
root@free5gc-pcf-7cbdcd4444-ql7ds:/free5gc# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
        inet 10.244.0.224  netmask 255.255.255.0  broadcast 10.244.0.255
        inet6 fe80::d83a:99ff:fe7f:43c9  prefixlen 64  scopeid 0x20<link>
        ether da:3a:99:7f:43:c9  txqueuelen 0  (Ethernet)
        RX packets 198561  bytes 13166298 (13.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 198286  bytes 10481591 (10.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

mgnt: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
        inet 10.200.2.4  netmask 255.255.255.0  broadcast 10.200.2.255
        inet6 fe80::c8c:faff:fe68:9d94  prefixlen 64  scopeid 0x20<link>
        ether 0a:58:0a:c8:02:04  txqueuelen 0  (Ethernet)
        RX packets 132615  bytes 9244333 (9.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 132247  bytes 6897297 (6.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@free5gc-pcf-7cbdcd4444-ql7ds:/free5gc#
```

- **Host2 is connected to DUT on interface mgnt**

```
root@free5gc-pcf-7cbdcd4444-ql7ds:/free5gc# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
        inet 10.244.0.224  netmask 255.255.255.0  broadcast 10.244.0.255
        inet6 fe80::d83a:99ff:fe7f:43c9  prefixlen 64  scopeid 0x20<link>
        ether da:3a:99:7f:43:c9  txqueuelen 0  (Ethernet)
        RX packets 198561  bytes 13166298 (13.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 198286  bytes 10481591 (10.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

mgnt: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
        inet 10.200.2.4  netmask 255.255.255.0  broadcast 10.200.2.255
        inet6 fe80::c8c:faff:fe68:9d94  prefixlen 64  scopeid 0x20<link>
        ether 0a:58:0a:c8:02:04  txqueuelen 0  (Ethernet)
        RX packets 132615  bytes 9244333 (9.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 132247  bytes 6897297 (6.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@free5gc-pcf-7cbdcd4444-ql7ds:/free5gc#
```

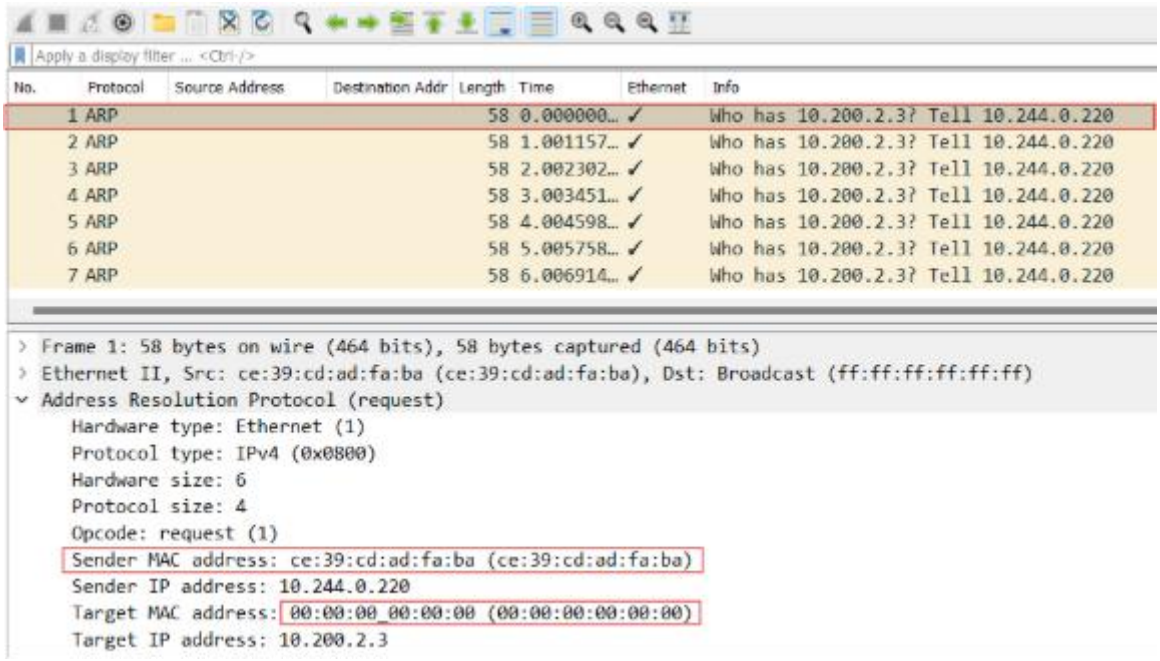
- Broadcast an ARP request from Host 1 on Subnet A to discover the MAC of Host 2 on subnet B. Since the ARP request is a broadcast, it reaches all nodes in the Subnet A, which include the IF1 interface of the network product, but it does not reach Host 2

```
root@free5gc-nrf-57b64b96f-tkxl9:/free5gc# arping -I eth0 10.200.2.3
ARPING 10.200.2.3
42 bytes from f2:4d:c3:71:ad:44 (10.200.2.3): index=0 time=4.581 usec
42 bytes from f2:4d:c3:71:ad:44 (10.200.2.3): index=1 time=3.608 usec
42 bytes from f2:4d:c3:71:ad:44 (10.200.2.3): index=2 time=3.652 usec
42 bytes from f2:4d:c3:71:ad:44 (10.200.2.3): index=3 time=3.437 usec
42 bytes from f2:4d:c3:71:ad:44 (10.200.2.3): index=4 time=4.077 usec
42 bytes from f2:4d:c3:71:ad:44 (10.200.2.3): index=5 time=3.853 usec
42 bytes from f2:4d:c3:71:ad:44 (10.200.2.3): index=6 time=3.809 usec
42 bytes from f2:4d:c3:71:ad:44 (10.200.2.3): index=7 time=3.665 usec
^C
--- 10.200.2.3 statistics ---
8 packets transmitted, 8 packets received,   0% unanswered (0 extra)
rtt min/avg/max/std-dev = 0.003/0.004/0.005/0.000 ms
root@free5gc-nrf-57b64b96f-tkxl9:/free5gc#
```

- Verify that the network product correctly receives this packet but that it does not send an ARP reply to Host 1 with its own MAC address.

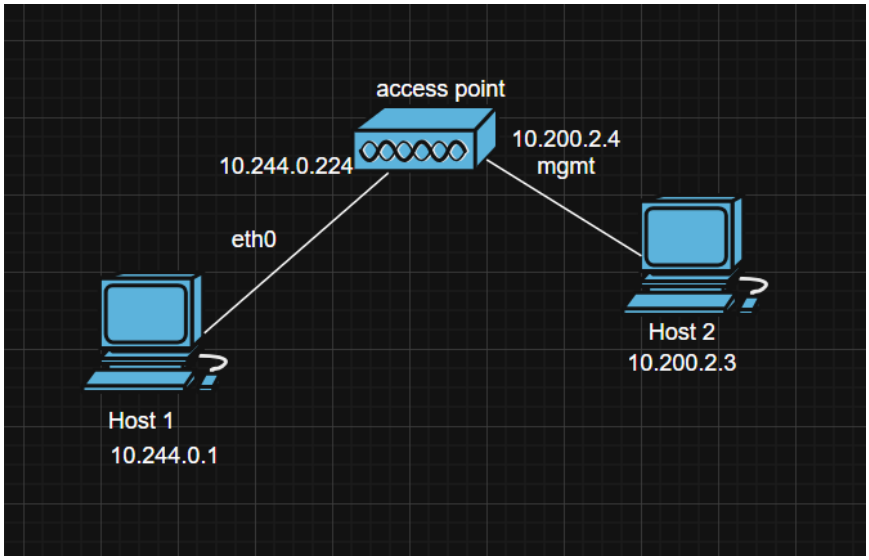
```
root@free5gc-pcf-7cbdcd4444-ql7ds:/free5gc# tcpdump -i eth0 -p arp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
18:53:39.263892 ARP, Request who-has 10.200.2.3 tell 10-244-0-220.nrf-nnrf.free5gc.svc.cluster.local, length 44
18:53:40.265050 ARP, Request who-has 10.200.2.3 tell 10-244-0-220.nrf-nnrf.free5gc.svc.cluster.local, length 44
18:53:41.266194 ARP, Request who-has 10.200.2.3 tell 10-244-0-220.nrf-nnrf.free5gc.svc.cluster.local, length 44
18:53:42.267199 ARP, Request who-has 10.200.2.3 tell 10-244-0-220.nrf-nnrf.free5gc.svc.cluster.local, length 44
18:53:43.268352 ARP, Request who-has 10.200.2.3 tell 10-244-0-220.nrf-nnrf.free5gc.svc.cluster.local, length 44
18:53:44.269500 ARP, Request who-has 10.200.2.3 tell 10-244-0-220.nrf-nnrf.free5gc.svc.cluster.local, length 44
```

The same can be checked on wireshark



(for IPV4 multicast handling)

- Here the tester verifies that ipv4 addresses (source and destination) aren't running on broadcast addresses
- Verify that none of the network product's interfaces is running Multicast (e.g. typing command ip maddr or ifconfig (for Unix embedded)



- Host 1 is connected to DUT on interface eth0

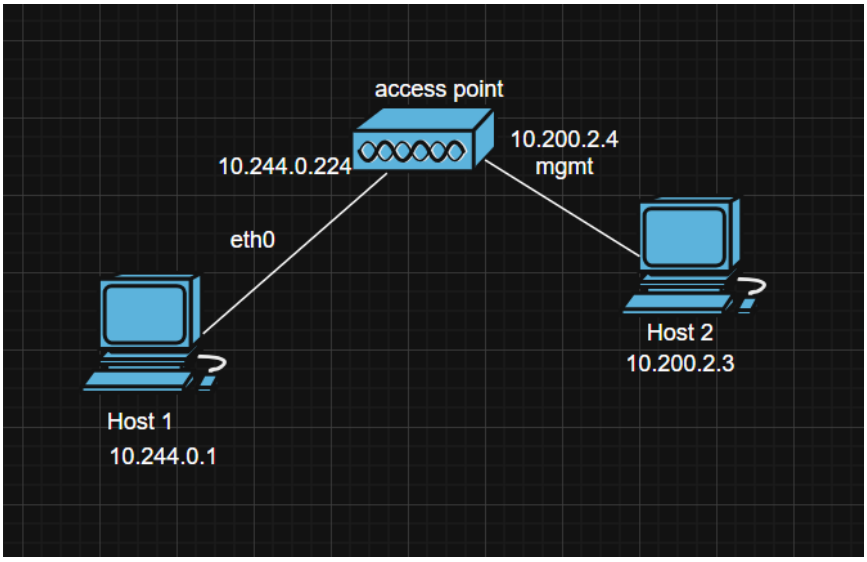
```
root@free5gc-pcf-7cbdcd4444-ql7ds:/free5gc# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
        inet 10.244.0.224  netmask 255.255.255.0  broadcast 10.244.0.255
        inet6 fe80::d83a:99ff:fe7f:43c9  prefixlen 64  scopeid 0x20<link>
        ether da:3a:99:7f:43:c9  txqueuelen 0  (Ethernet)
        RX packets 198561  bytes 13166298 (13.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 198286  bytes 10481591 (10.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

mgnt: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
        inet 10.200.2.4  netmask 255.255.255.0  broadcast 10.200.2.255
        inet6 fe80::c8c:faff:fe68:9d94  prefixlen 64  scopeid 0x20<link>
        ether 0a:58:0a:c8:02:04  txqueuelen 0  (Ethernet)
        RX packets 132615  bytes 9244333 (9.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 132247  bytes 6897297 (6.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@free5gc-pcf-7cbdcd4444-ql7ds:/free5gc#
```

- **Host2 is connected to DUT on interface mgnt**

```
root@free5gc-pcf-7cbdcd4444-ql7ds:/free5gc# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
        inet 10.244.0.224  netmask 255.255.255.0  broadcast 10.244.0.255
        inet6 fe80::d83a:99ff:fe7f:43c9  prefixlen 64  scopeid 0x20<link>
        ether da:3a:99:7f:43:c9  txqueuelen 0  (Ethernet)
        RX packets 198561  bytes 13166298 (13.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 198286  bytes 10481591 (10.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

mgnt: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
        inet 10.200.2.4  netmask 255.255.255.0  broadcast 10.200.2.255
        inet6 fe80::c8c:faff:fe68:9d94  prefixlen 64  scopeid 0x20<link>
        ether 0a:58:0a:c8:02:04  txqueuelen 0  (Ethernet)
        RX packets 132615  bytes 9244333 (9.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 132247  bytes 6897297 (6.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@free5gc-pcf-7cbdcd4444-ql7ds:/free5gc#
```

Its observed that both the interfaces on which Hosts are connected to the DUT have MULTICAST running

(for Gratuitous ARP)



- Craft a gratuitous ARP request

```
root@free5gc-nrf-57b64b96f-tkxl9:/free5gc# cat arp_request.py
from scapy.all import ARP, send

# Define spoofed IP and DUT MAC
spoofed_ip = "192.168.20.101"  # Spoofed Source IP
dut_mac = "da:3a:99:7f:43:c9"  # DUT MAC Address

# Gratuitous ARP Request Packet
arp_request = ARP(op=1,                    # ARP Request
                  psrc=spoofed_ip,          # Source IP (spoofed)
                  pdst=spoofed_ip,          # Target IP (same as Source IP)
                  hwsrc=dut_mac,            # DUT MAC Address (real)
                  hwdst="ff:ff:ff:ff:ff:ff")  # Broadcast MAC

# Send the ARP Request
send(arp_request)

print(f"Sent Gratuitous ARP Request for {spoofed_ip} ({dut_mac})")
```

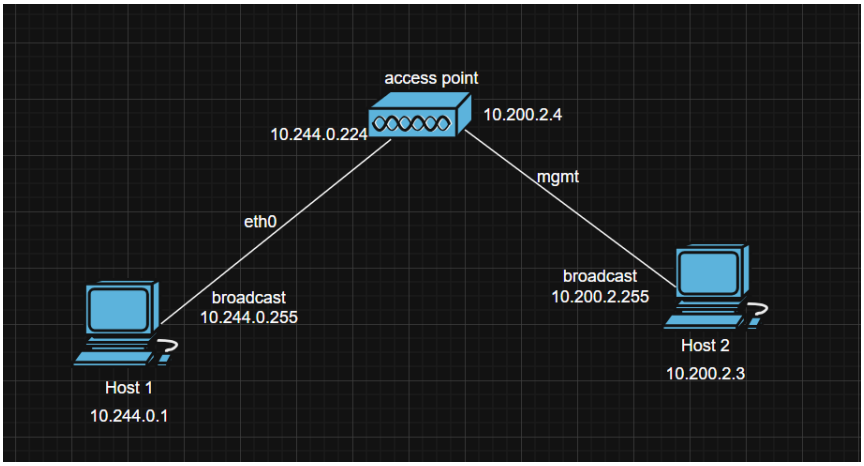
- Send a Gratuitous ARP request from Host 1, i.e. an ARP request where the source and destination IP are both set to an IP address different from the one already cached in the network product ARP Cache for Host 1 and the destination MAC is the broadcast address ff:ff:ff:ff:ff:ff.

```
root@free5gc-nrf-57b64b96f-tkxl9:/free5gc# python3 arp_request.py
.
Sent 1 packets.
Sent Gratuitous ARP Request for 192.168.20.101 (da:3a:99:7f:43:c9)
```

- Verify that the network product correctly receives this packet but discards it and that the ARP Cache is not updated.

```
root@free5gc-nrf-57b64b96f-tkxl9:/free5gc# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.244.0.97              ether   a2:e4:a1:aa:53:88   C                     eth0
10.244.0.80              ether   5e:e6:6f:58:36:87   C                     eth0
10.244.0.224             ether   da:3a:99:7f:43:c9   C                     eth0
10.244.0.221                     (incomplete)                              eth0
10.244.0.122             ether   96:59:4a:ac:30:12   C                     eth0
10.244.0.1               ether   d6:65:88:ee:44:ef   C                     eth0
root@free5gc-nrf-57b64b96f-tkxl9:/free5gc# arp -n | grep 192.168.20.101
root@free5gc-nrf-57b64b96f-tkxl9:/free5gc#
```

- The same can be observed on wireshark (packets captured at the DUT) (for broadcast handling)



- Host 1 is connected to DUT on interface eth0

```
root@free5gc-pcf-7cbdcd4444-ql7ds:/free5gc# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
        inet 10.244.0.224  netmask 255.255.255.0  broadcast 10.244.0.255
        inet6 fe80::d83a:99ff:fe7f:43c9  prefixlen 64  scopeid 0x20<link>
        ether da:3a:99:7f:43:c9  txqueuelen 0  (Ethernet)
        RX packets 198561  bytes 13166298 (13.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 198286  bytes 10481591 (10.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

mgnt: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
        inet 10.200.2.4  netmask 255.255.255.0  broadcast 10.200.2.255
        inet6 fe80::c8c:faff:fe68:9d94  prefixlen 64  scopeid 0x20<link>
        ether 0a:58:0a:c8:02:04  txqueuelen 0  (Ethernet)
        RX packets 132615  bytes 9244333 (9.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 132247  bytes 6897297 (6.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@free5gc-pcf-7cbdcd4444-ql7ds:/free5gc#
```

- **Host2 is connected to DUT on interface mgnt**

```
root@free5gc-pcf-7cbdcd4444-ql7ds:/free5gc# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
        inet 10.244.0.224  netmask 255.255.255.0  broadcast 10.244.0.255
        inet6 fe80::d83a:99ff:fe7f:43c9  prefixlen 64  scopeid 0x20<link>
        ether da:3a:99:7f:43:c9  txqueuelen 0  (Ethernet)
        RX packets 198561  bytes 13166298 (13.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 198286  bytes 10481591 (10.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

mgnt: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
        inet 10.200.2.4  netmask 255.255.255.0  broadcast 10.200.2.255
        inet6 fe80::c8c:faff:fe68:9d94  prefixlen 64  scopeid 0x20<link>
        ether 0a:58:0a:c8:02:04  txqueuelen 0  (Ethernet)
        RX packets 132615  bytes 9244333 (9.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 132247  bytes 6897297 (6.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@free5gc-pcf-7cbdcd4444-ql7ds:/free5gc#
```

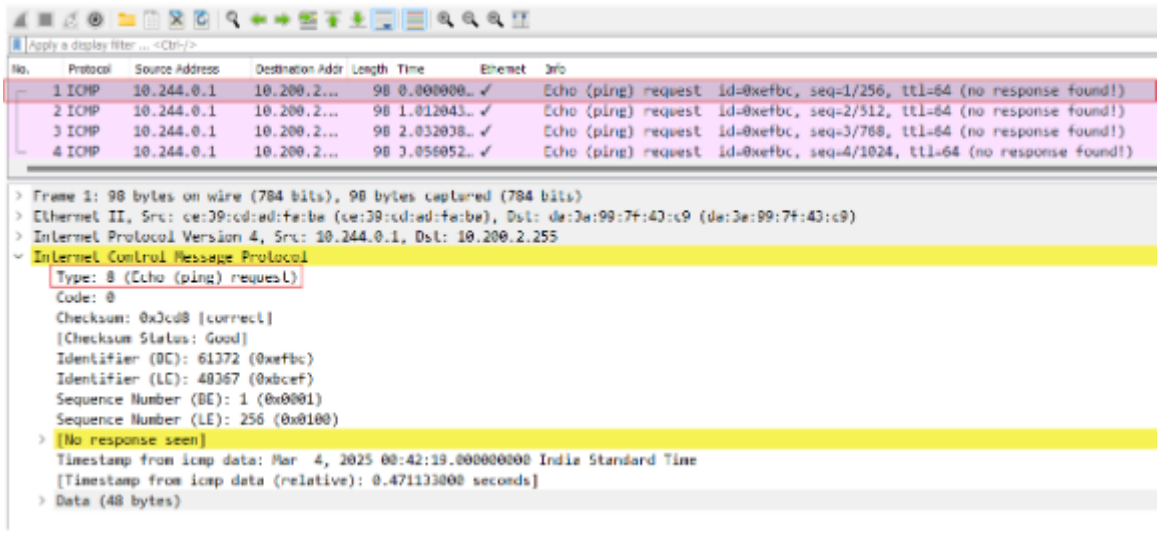
- Send an ICMP ECHO message from Host 1 to ping a broadcast address
  Host 1 (Subnet A) sends a packet with the destination broadcast address of Subnet B (10.200.2.255)

```
root@free5gc-nrf-57b64b96f-tkxl9:/free5gc# ping -b 10.200.2.255 -c 10 -I eth0
PING 10.200.2.255 (10.200.2.255) from 10.244.0.220 eth0: 56(84) bytes of data.
^C
--- 10.200.2.255 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7160ms
```

- Verify that the network product doesn't respond to the ping.
  Capture the same on tcpdump at the DUT

```
root@free5gc-pcf-7cbdcd4444-ql7ds:/free5gc# tcpdump -i eth0 -p icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
19:11:45.350726 IP 10.244.0.1 > 10.200.2.255: ICMP echo request, id 47650, seq 1, length 64
19:11:46.367165 IP 10.244.0.1 > 10.200.2.255: ICMP echo request, id 47650, seq 2, length 64
19:11:47.391162 IP 10.244.0.1 > 10.200.2.255: ICMP echo request, id 47650, seq 3, length 64
19:11:48.415164 IP 10.244.0.1 > 10.200.2.255: ICMP echo request, id 47650, seq 4, length 64
19:11:49.439166 IP 10.244.0.1 > 10.200.2.255: ICMP echo request, id 47650, seq 5, length 64
19:11:50.467162 IP 10.244.0.1 > 10.200.2.255: ICMP echo request, id 47650, seq 6, length 64
19:11:51.487158 IP 10.244.0.1 > 10.200.2.255: ICMP echo request, id 47650, seq 7, length 64
19:11:52.511173 IP 10.244.0.1 > 10.200.2.255: ICMP echo request, id 47650, seq 8, length 64
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel
```

The same can be seen on wireshark



- Send an ICMP timestamp request (ICMP type 13) from host 1 to a broadcast address
- Verify that the network product doesn't respond to the timestamp request

11.2.4 **Test Observation**

It was observed that DUT doesn't respond to the arp request from Host 1 on behalf of Host 2(proxy arp)

DUT does'nt respond to the directed broadcast request sent from Host 1

DUT does have MULTICAST running on the interfaces connected to the Hosts

DUT does not update the ARP cache upon receiving the Gratuitous ARP request from Host 1

11.2.5 **Evidence:-** Screenshots provided above

12. **<u>Test Case Result:</u>**

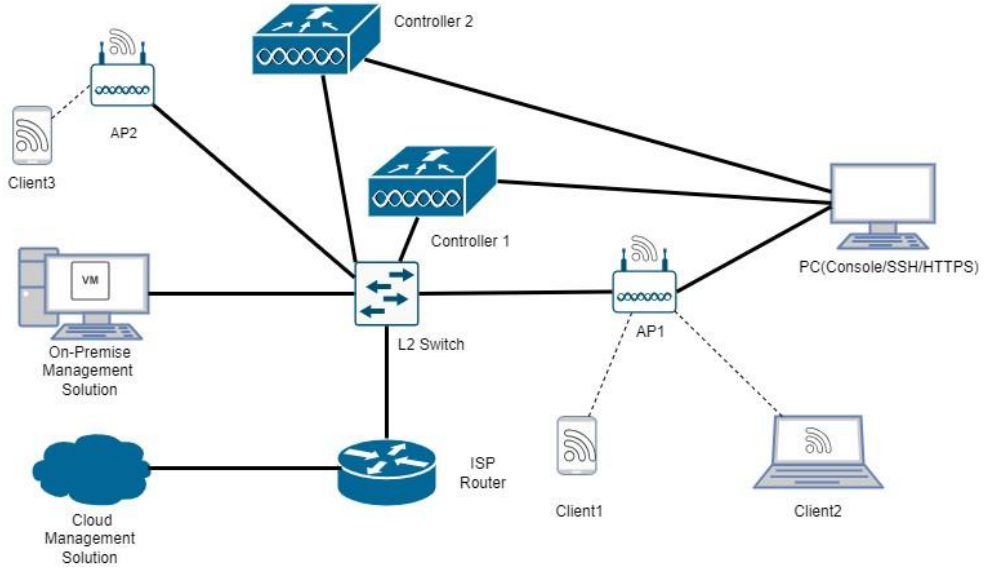
S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	OS Hardening from OEM		No OEM document available
2	OS Hardening of DUT	Fail	MULTICAST is running on the interfaces connected to the DUT

<test bed diagram with correct IP addr>

1.10.6: External file system mount restrictions

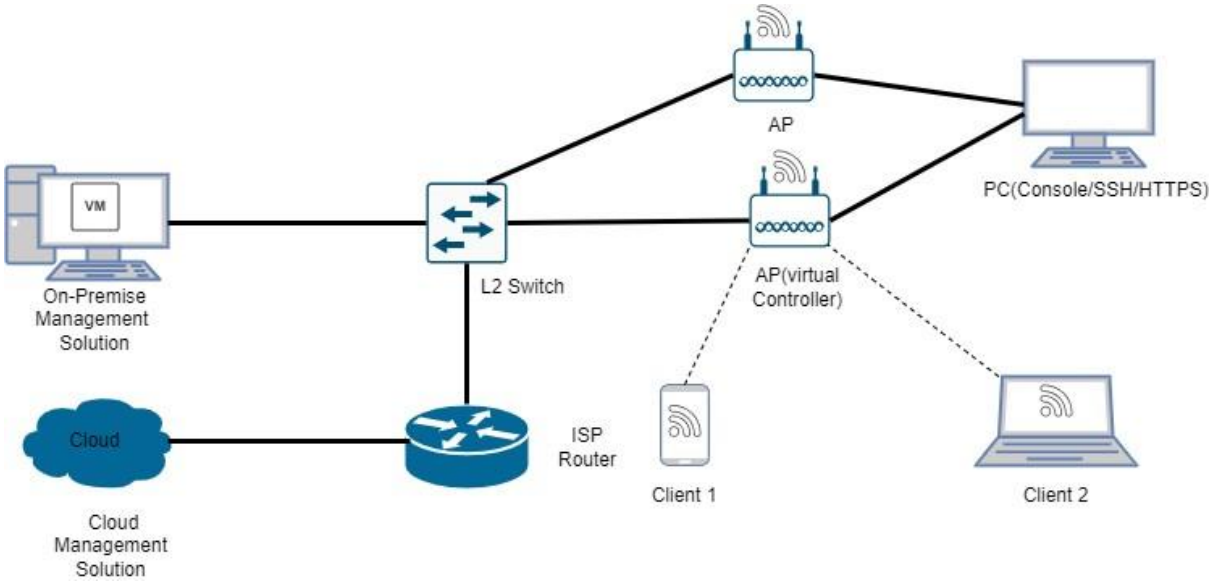
<DUT Details: > Ex: Router
<DUT Software Version:>
<Digest Hash of OS>
<Digest Hash of Configuration>
<Applicable ITSAR: >
<ITSAR Version No:>
<OEM Supplied Document list: >

1. **<ITSAR Section No & Name> Section 2.10 Operating System**
2. **<Security Requirement No & Name > 2.10.6 No automatic launch of removable media**
3. **<Requirement Description: >** The Network product shall not automatically launch any application when removable media device such as CD, DVD, USB-Sticks or USB-Storage drive is connected. If the operating system supports an automatic launch, it shall be deactivated unless it is required to support availability requirements.
4. **DUT Confirmation Details:**
5. **DUT Configuration: -**
6. **Preconditions:-** If the network product is provisioned with the necessary physical ports/drives (CD/DVD drive, USB port, etc.) then the test case applies.
7. **Test Objective:-** To test if DUT does'nt permits automatic launch of application when removable media is attached
8. Test Plan
   - 8.1. Number of test scenerios ; 01
     - 8.1.1. Test scenario to check if DUT permits launch application on its own
   - 8.2. Test Bed diagram



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

AP Integrated Mode :



Note : The execution steps remain same for all the above scenarios. Further scenarios please check OEM datasheet.

8.3. Test execution steps :

- Connect the removable media to DUT.
- Verify removable media does not automatically launch after connecting to DUT.
- Reload the DUT to verify if the removable drive is not accessible by default.

9. **Expected Results**: - DUT doesn't permit the mounting of removable media unless done manually
10. **<u>Expected Format of Evidence</u>**
11. **Test Execution**

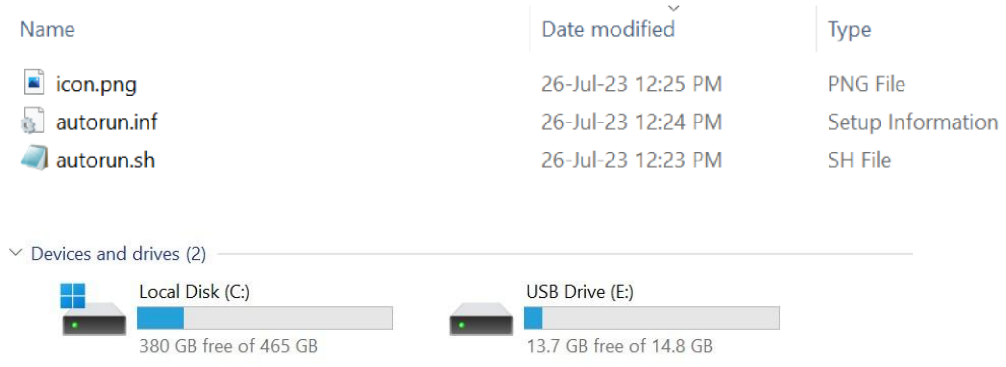
11.1 Test Case Number : 01

11.1.1 Test Case Name: Automatic launch from removable media

11.1.2 Test Case Description: To test if DUT permits automatic launch of application when removable media is attached

11.1.3 Execution Steps:

i) Load a removable drive with relevant files to DUT.



autorun.sh - Notepad

File Edit Format View Help

```
#! /bin/sh
xdg-open myDocument.odt
```

The removable media was formatted with FAT32 format, which supports Linux file system. The above script in autorun.sh will launch a new document .

ii)Connect the removable media to DUT and check if the DUt doesn't support the launch of the application

```
User:Admin
Password:*********
Welcome to the Cisco Mobility Express command line interface.
Only commands which are listed in the command reference guide for this release a
re supported.
http://www.cisco.com/c/en/us/support/wireless/mobility-express/products-command-
reference-list.html

Warning:In SNMPV2 No Defaults Presents.
Please use command: config snmp community create <name>

Warning:In SNMPV3 No Defaults Presents.
Please use command: config snmp v3user create <username>

(Cisco Controller) >
```

The script requires the access to bash shell to execute.

No popup or prompt message was observed after removable media (USB) is connected.

Reload the DUT to verify if the removable drive is not accessible by default

```
AP38ED.18C8.1068#show filesystems
Filesystem              Size      Used Available Use% Mounted on
devtmpfs               456.9M         0    456.9M   0% /dev
tmpfs                    1.0M     44.0K    980.0K   4% /dev/shm
none                     1.0M     44.0K    980.0K   4% /dev/shm
/dev/ubivol/storage     57.6M      1.3M     53.3M   2% /storage
tmpfs                  486.4M         0    486.4M   0% /run
none                    80.0M      1.8M     78.2M   2% /tmp
none                    80.0M      1.8M     78.2M   2% /tmp/var/run/netns
/dev/ubivol/storage2    40.0M     52.0K     37.9M   0% /storage2
/dev/ram5               29.0M    371.0K     27.2M   1% /mnt/core
AP38ED.18C8.1068#
```

The above screenshot shows that no USB was detected.

11.1.4 **Test Observation :-** It was observed that DUT doesn't launch any application

1. Test Result

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Automatic launch from removable media	PASS	

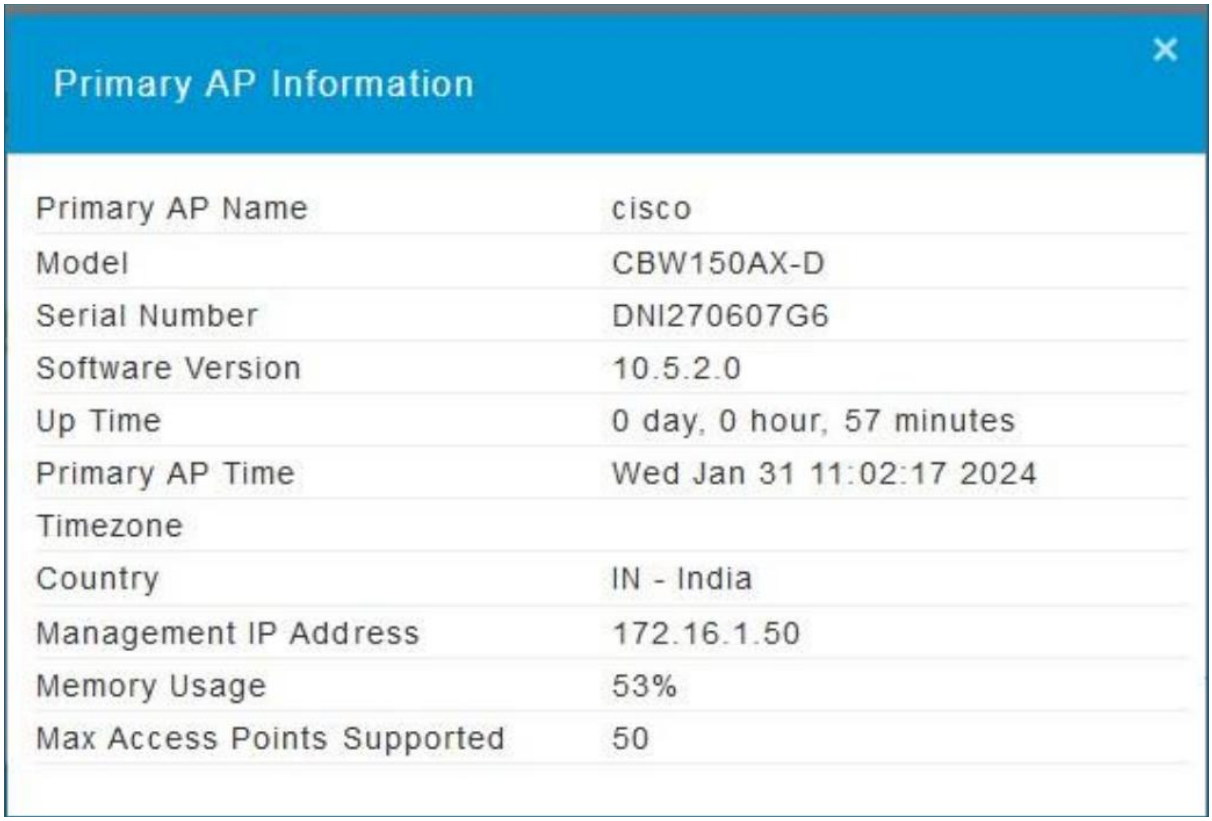
Section 1.11: Web Interface

1.11.1 HTTPS Support

<DUT Details: > WiFi CPE
<DUT Software Version:> cisco 10.5.2.0
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 11: Web Server
2. **<Security Requirement No & Name >** 1.11.1: HTTPS Support
3. **<Requirement Description: >**The communication between Web client and Web server to be protected using industry standard secured communication protocols TLS/HTTPS. Cipher suites with NULL encryption shall not be supported. CPE to be protected against sniffing and side jacking attacks.

4. **DUT Confirmation Details**: Screenshot below shows the DUT name (Primary AP Name) , Model number, Serial Number, Software Version.



DUT Configuration Checksum:

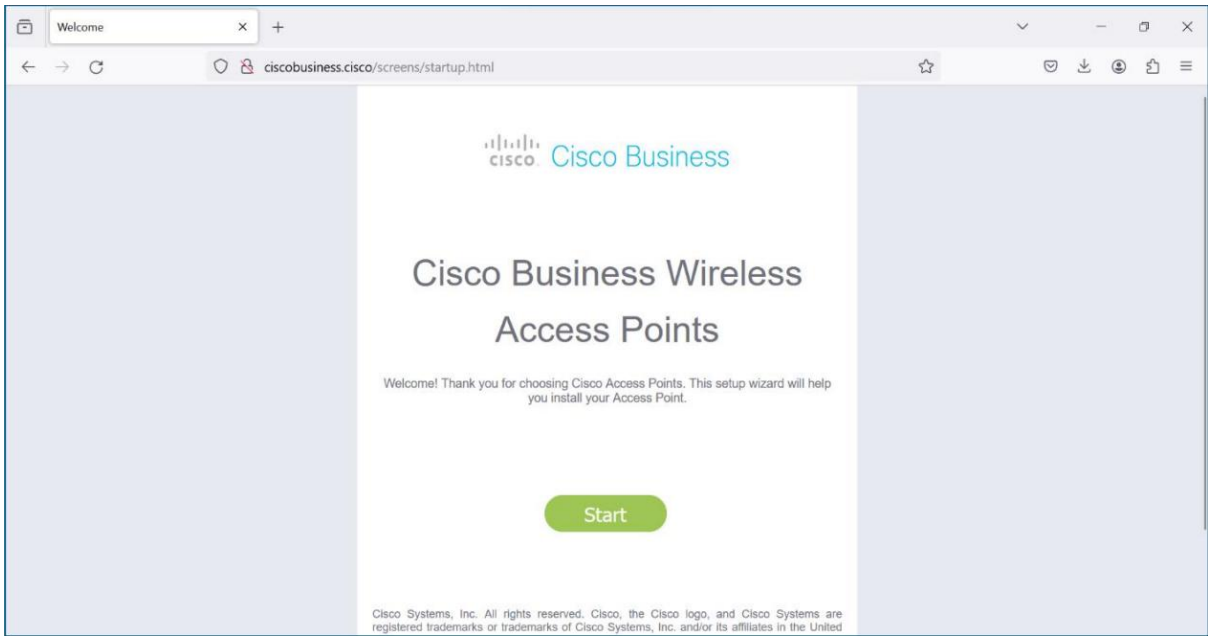
```
PS C:\> certutil -hashfile '.\Configuration files\Configuration 1.txt' SHA256
SHA256 hash of .\Configuration files\Configuration 1.txt:
fab585d185d316ad6c45b1d414d8bf55fa8ef0094173fe9a8a5fa2d3ddc2e43b
CertUtil: -hashfile command completed successfully.
```

5. **DUT Configuration:**

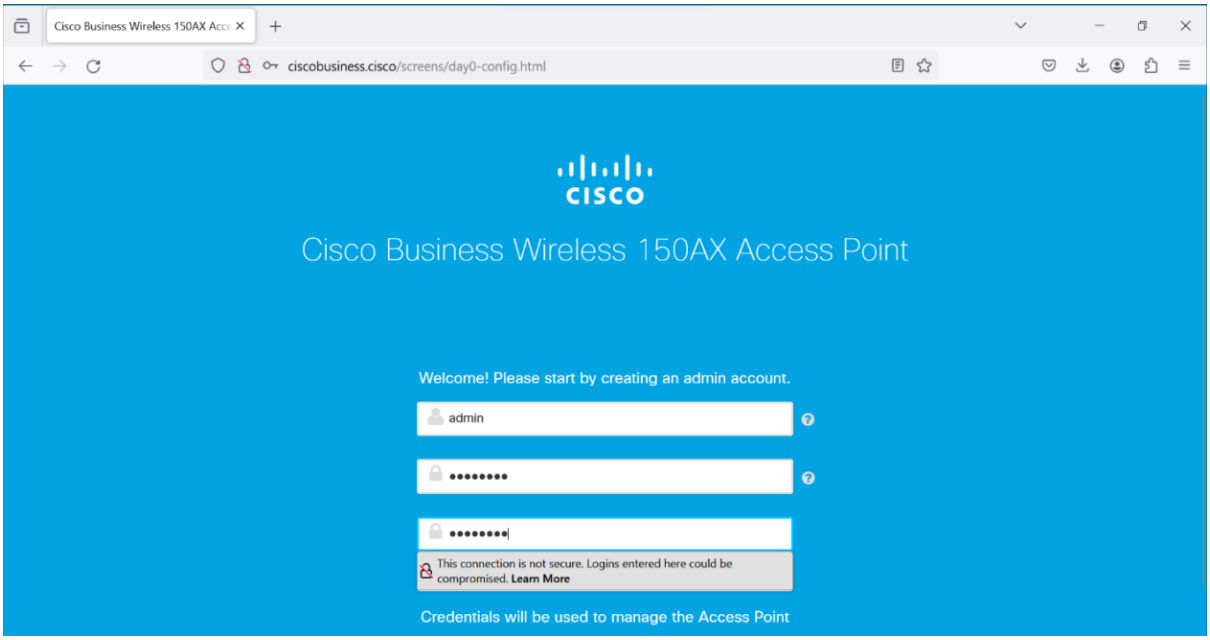
Initial Basic Configuration of CPE

Step 1: Power on the CPE and wait for the CPE to be visible on the Laptop Wi-Fi Scanning "Cisco Business-Setup" or Reset the CPE if not Visible

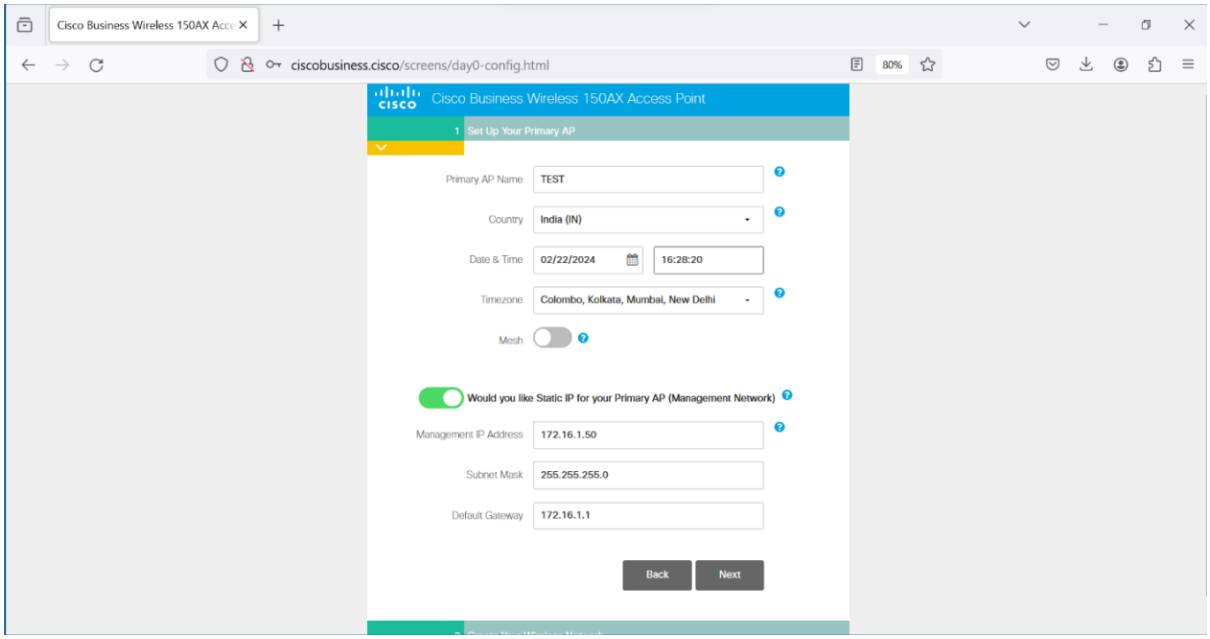
Step 2: Connect To the Wi-Fi Access Point using password " Cisco123" And Navigate to http://ciscobusiness.cisco/screens/startup.html and Click Start as Show in the below Screenshot.



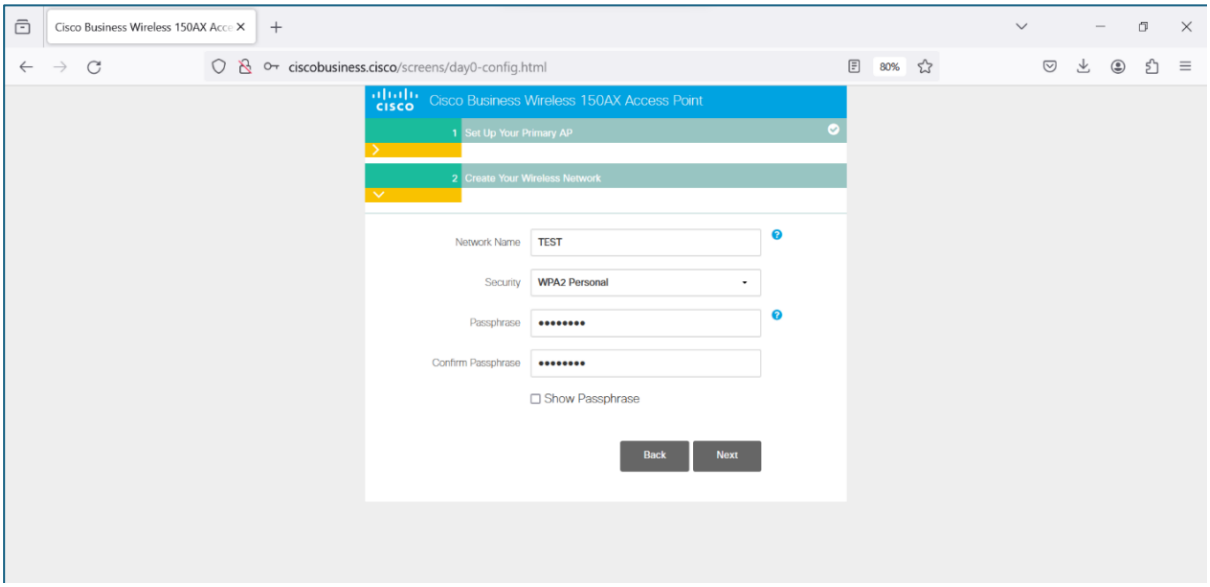
Step 3 : Enter the Desire Credentials for admin account creation and click start



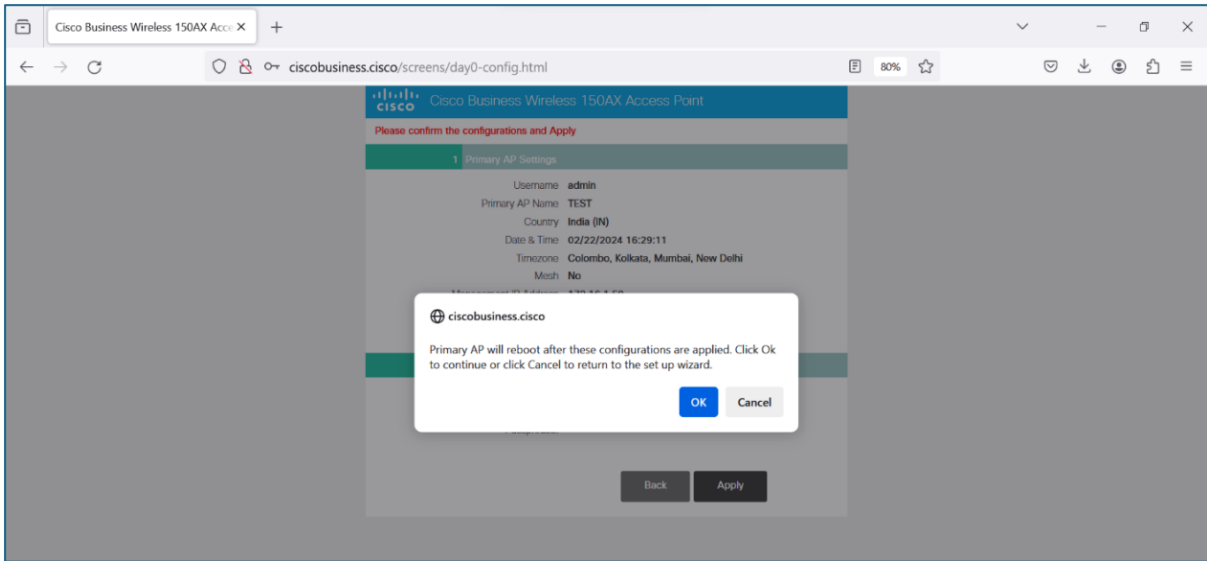
Step 4 : Enter the Desire AP Name and Select Static IP Configuration if required and click Next



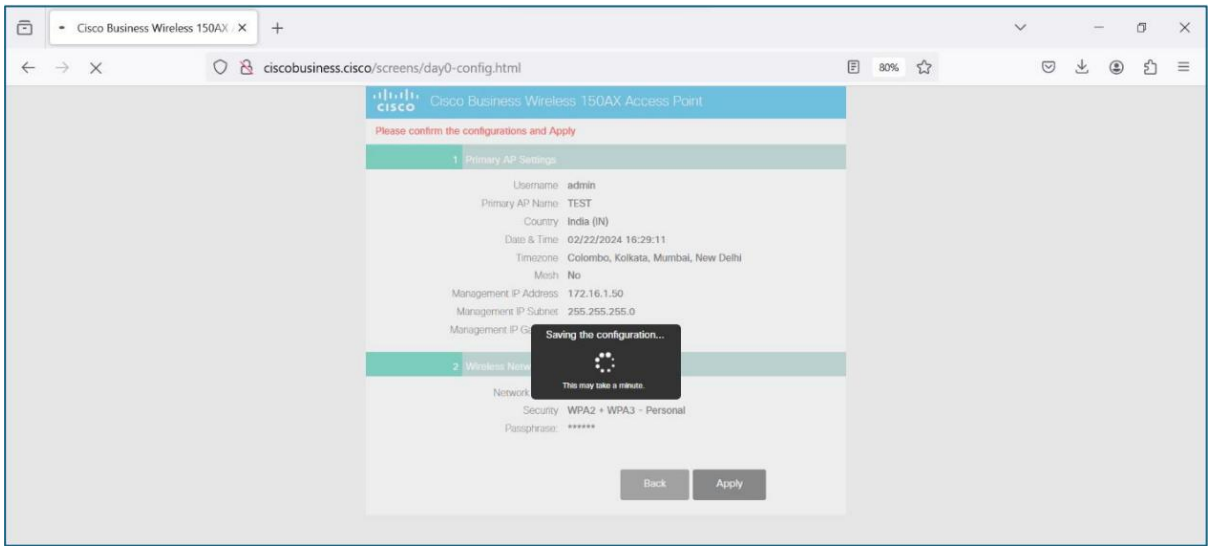
Step 5 : Enter the Desire Network Name and Passphrase and click Next

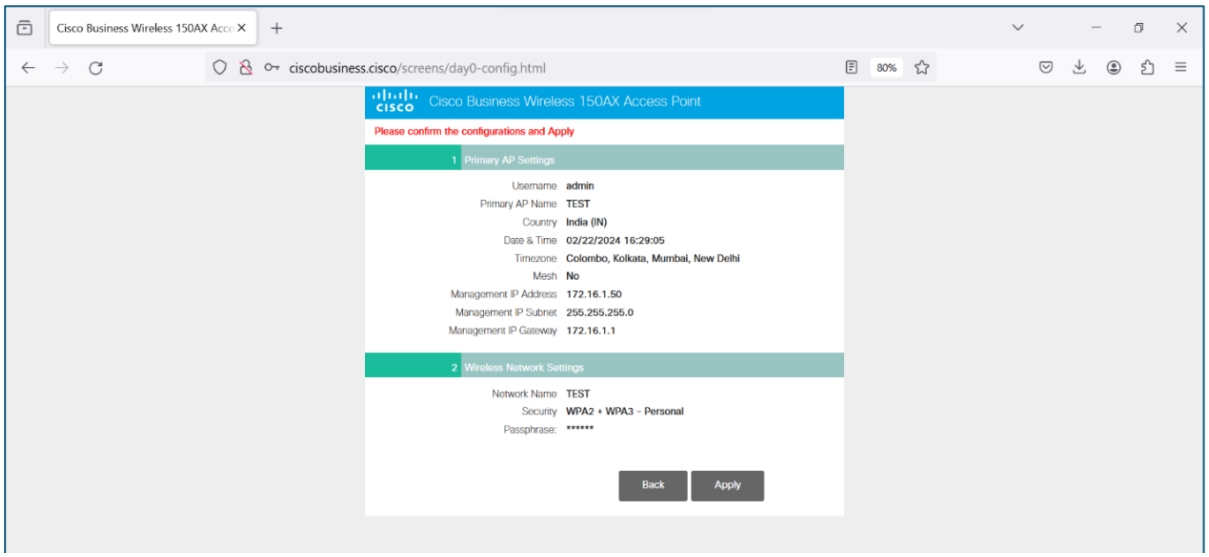


Step 6 : Verify the Configuration done and Click on Apply



Step 7 : A popup will appear on the screen “Primary AP will reboot after these configurations are applied. Click Ok to continue or click Cancel to return to the set-up wizard.”





Step 8: Finished Step Now the AP is Ready to Be used.

6. **Preconditions**
   - Network product documentation containing information about supported Web Servers and Protocol to communicate with the Web Server in the DUT is provided by the vendor.
   - A peer implementing the security protocol same as the one configured by the vendor on DUT for Web Server, (e.g., HTTPS client) shall be available.
   - Tester has HTTPS access to DUT.

7. **Test Objective**:
   - The communication between Web client and Web server shall be protected using TLS.
   - Cipher suites with NULL encryption shall not be supported.

8. **Test Plan:**

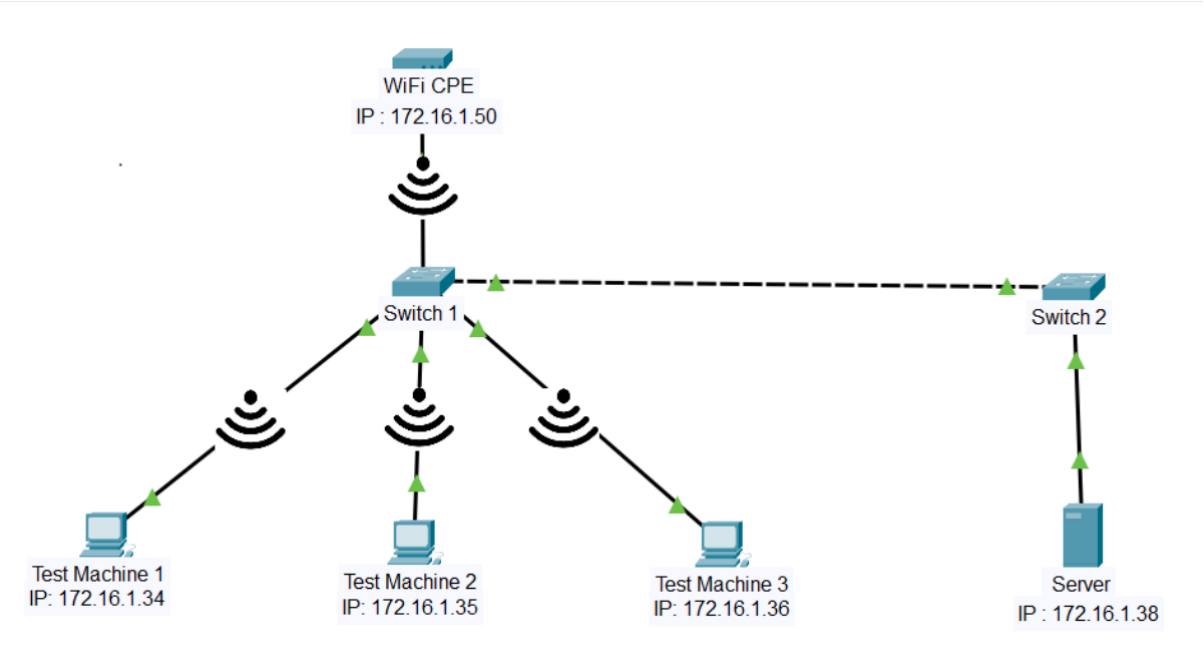
8.1 Number of Test Scenarios:

8.1.1 Test scenario to check whether the communication between the client and server is over http.

8.1.2 Test Scenario to check whether the DUT supports NULL encryption.

8.1.3 Test Scenario to check what are the ciphers supported by the DUT and which TLS version is being used.

8.2 Test Bed Diagram



8.3 Tools Required

- Testssl
- Browser

8.4 Test Execution Steps

- Open any web browser and initiate a connection to the target server using the HTTP protocol to verify whether the communication between the client and server occurs over HTTP.
- The tester initiates a connection to the target server using the SSL/TLS protocol, specifying a particular version (e.g., TLS 1.0, TLS 1.2).
- Take note of the cipher suites supported by the Device Under Test (DUT) during the SSL/TLS handshake.
- Follow the steps for each supported cipher suite, both secure and weak, to thoroughly test the server's configuration.

- Check all supported ciphers and verify that the DUT supports secure ciphers. Ensure that the server does not support null encryption.
  Note: Utilize an automated tool such as **Testssl** to streamline and automate the testing process.
- Verify CPE is protected against sniffing and sidejacking attacks.

9. **Expected Results for Pass:**

Case 1: The Device Under Test (DUT) should not support HTTP; instead, communication between the client and web server should exclusively utilize the HTTPS protocol.

Case 2: The ciphers supported by the Device Under Test (DUT) should align with the recommendations outlined in the Cryptography ITSAR.

10. **Expected Format of Evidence:** Screenshots of Testing
11. **Test Execution:**

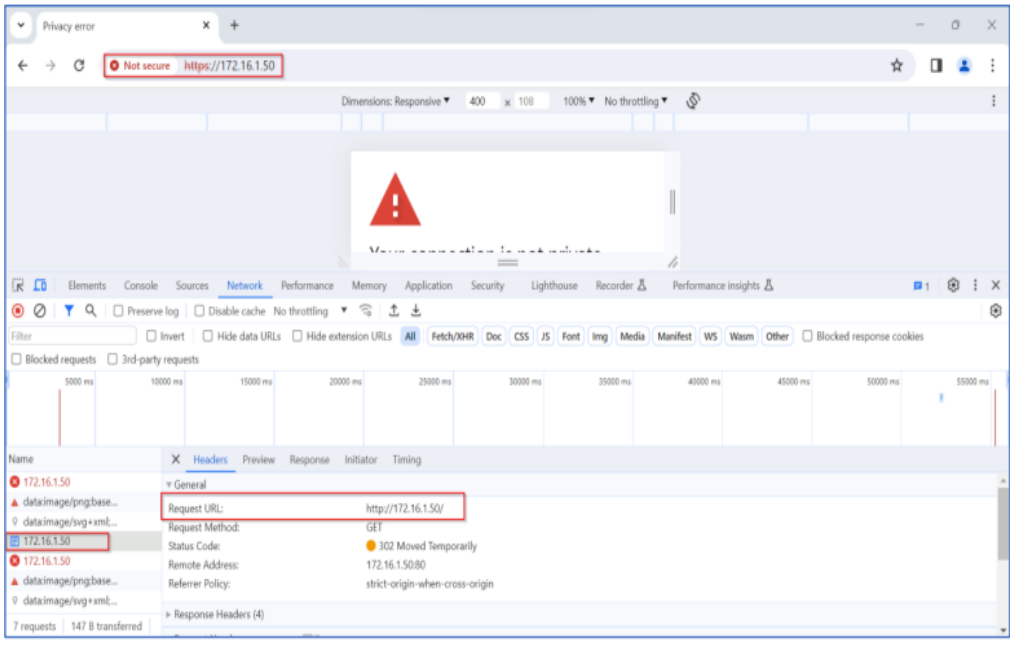
11.1 Test Case Number: 01

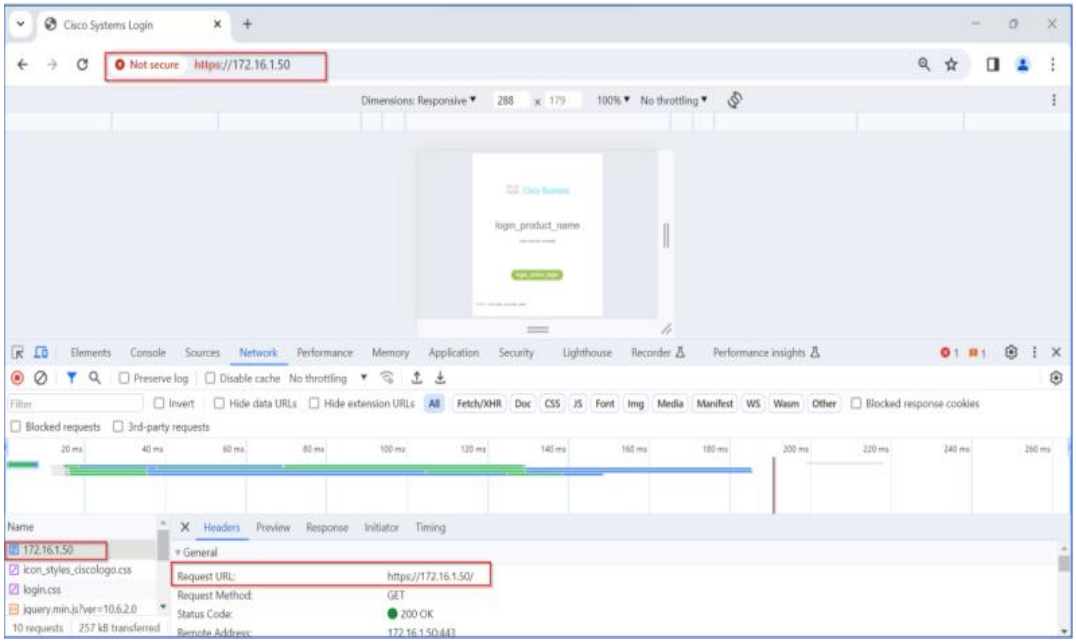
11.1.1 **Test Case Name:** TC1_HTTPS

11.1.2 **Test Case Description:** verify that Device Under Test (DUT) should not support HTTP

11.1.3 **Execution Steps:**

Step 1: Open browser and navigate to http://172.16.1.50 and observe that it is redirected to https://172.16.1.50.





11.1.4 **Test Observations:** DUT has successfully redirected a user to secure channel.

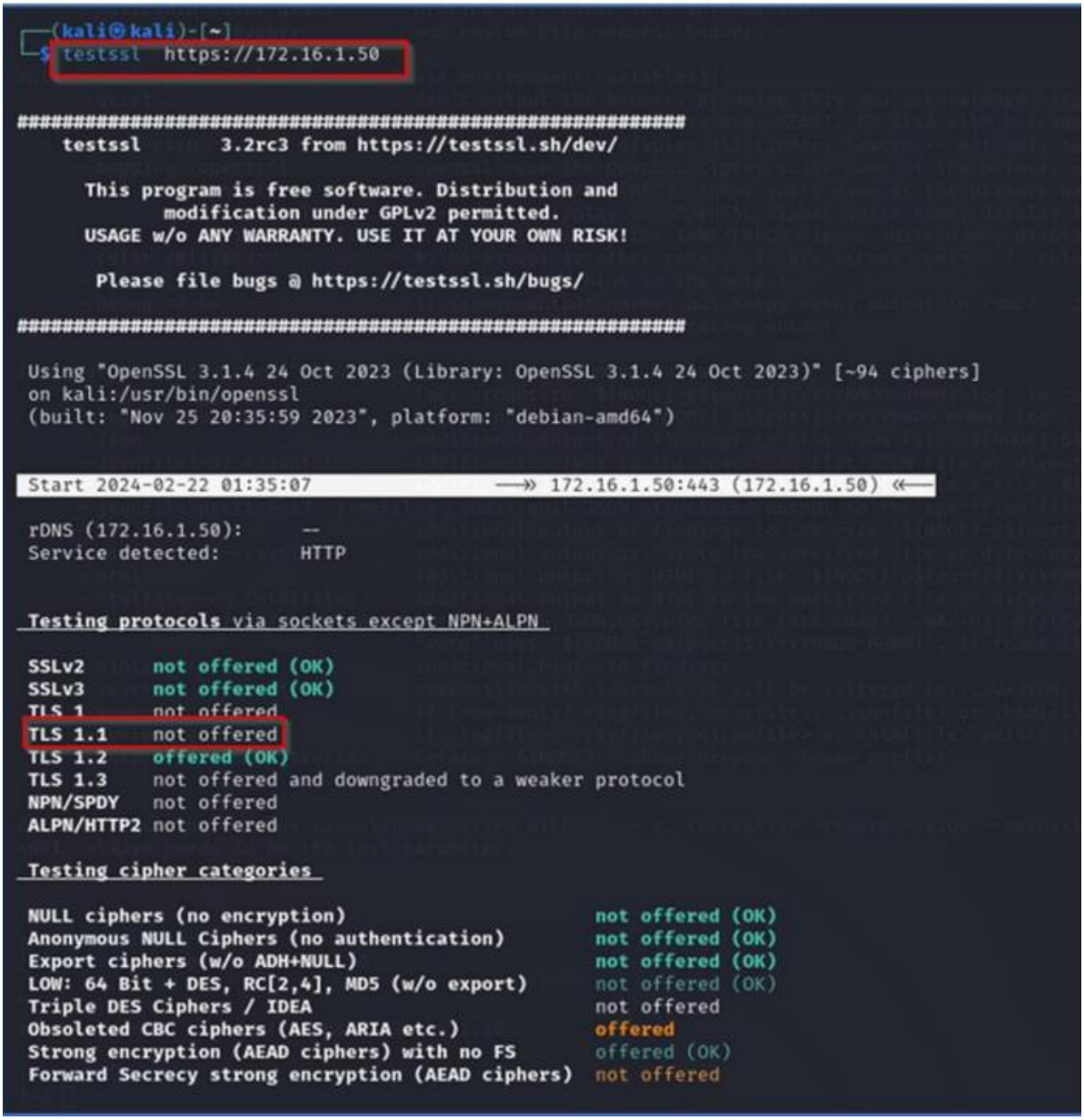
11.2 Test Case Number: 02

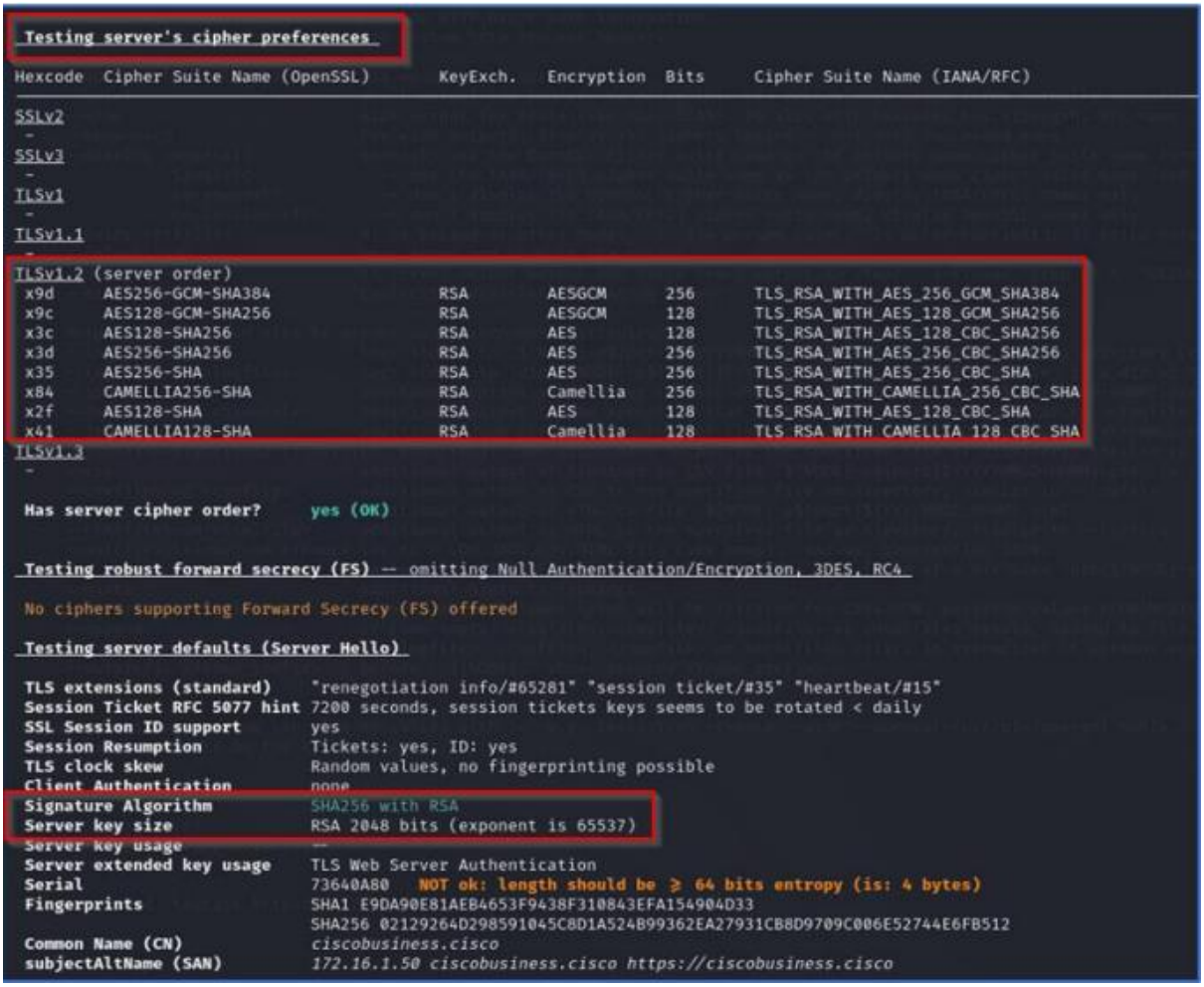
11.2.1 **Test Case Name:** TC2_ SUPPORT_ CIPHERS

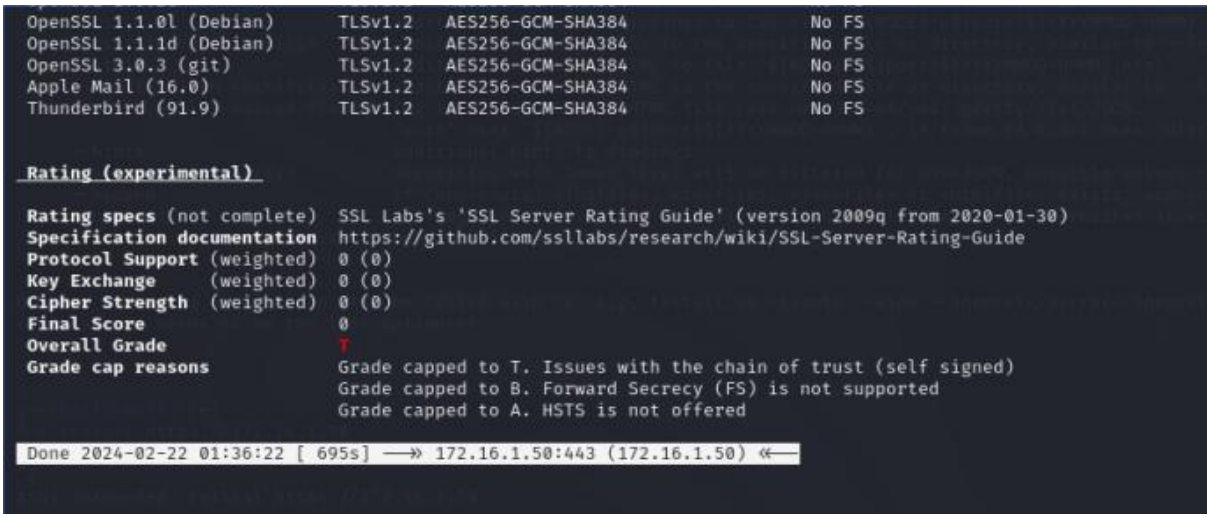
11.2.2 **Test Case Description:** The communication between Web client and Web server shall be protected using TLS.

11.2.3 **Execution Steps:**

Step 1: Open kali Linux and type the command “testssl https://172.16.1.50” and observe the response


(kali㉿kali)-[~]
$ testssl https://172.16.1.50
testssl 3.2rc3 from https://testssl.sh/dev/
This program is free software. Distribution and
modification under GPLv2 permitted.
USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!
Please file bugs @ https://testssl.sh/bugs/
Using "OpenSSL 3.1.4 24 Oct 2023 (Library: OpenSSL 3.1.4 24 Oct 2023)" [~94 ciphers]
on kali:/usr/bin/openssl
(built: "Nov 25 20:35:59 2023", platform: "debian-amd64")
Start 2024-02-22 01:35:07 -->> 172.16.1.50:443 (172.16.1.50) <<--
rDNS (172.16.1.50): --
Service detected: HTTP
Testing protocols via sockets except NPN+ALPN
SSLv2 not offered (OK)
SSLv3 not offered (OK)
TLS 1 not offered
TLS 1.1 not offered
TLS 1.2 offered (OK)
TLS 1.3 not offered and downgraded to a weaker protocol
NPN/SPDY not offered
ALPN/HTTP2 not offered
Testing cipher categories
NULL ciphers (no encryption) not offered (OK)
Anonymous NULL Ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADH+NULL) not offered (OK)
LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export) not offered (OK)
Triple DES Ciphers / IDEA not offered
Obsoleted CBC ciphers (AES, ARIA etc.) offered
Strong encryption (AEAD ciphers) with no FS offered (OK)
Forward Secrecy strong encryption (AEAD ciphers) not offered





From the above image, we verified the fingerprints, signature, TLS version, supported cipher and null encryption by the server.

11.2.4 **Test Observations:**

- The communication channel between the Network product and its client is encrypted using TLSv1.2,
- The DUT supported the weak cipher, Fingerprint and signature algorithm

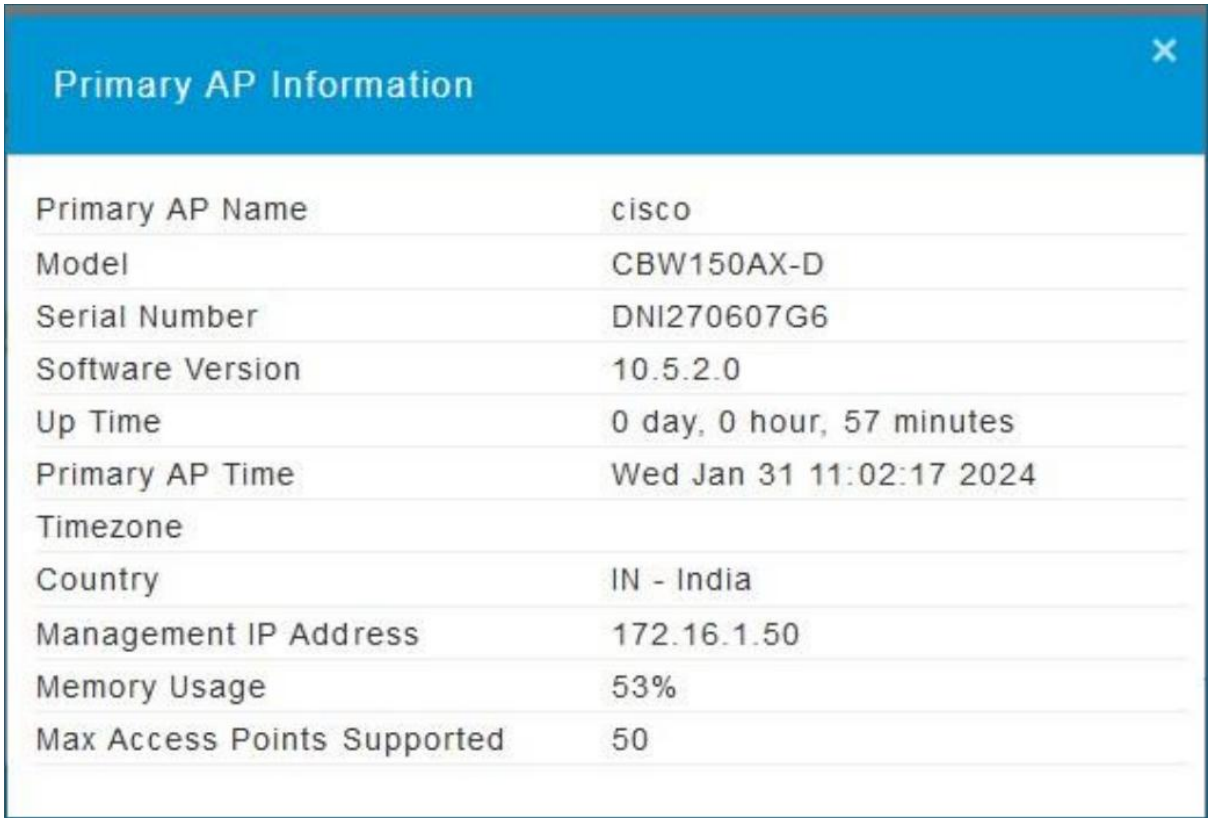
12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC1_HTTPS	PASS	
2	TC2_ SUPPORT_ CIPHERS	Fail	DUT supported the weak cipher, Fingerprint and signature algorithm

1.11.2: logging

<DUT Details: > WiFi CPE
<DUT Software Version:> cisco 10.5.2.0
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 11: Web Server
2. **<Security Requirement No & Name >** 1.11.2 logging
3. **<Requirement Description: >** Access to the webserver (both successful as well as failed attempts) shall be logged. The web server log shall contain the following information:
    - Access timestamp
    - Source (IP address)
    - Account (if known)
    - Attempted login name (if the associated account does not exist)
    - Relevant fields in http request. The URL should be included whenever possible.
    - Status code of web server response
4. **DUT Confirmation Details**: Screenshot below shows the DUT name (Primary AP Name) , Model number, Serial Number, Software Version.



DUT Configuration Checksum:

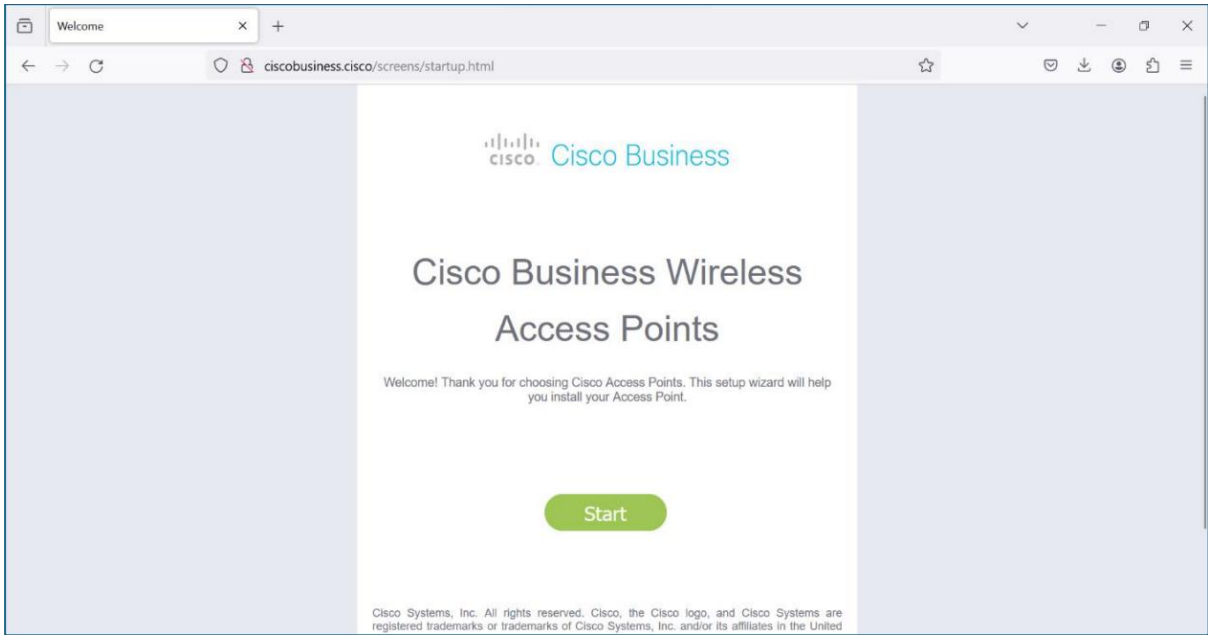
```
PS C:\> certutil -hashfile '.\Configuration files\Configuration 1.txt' SHA256
SHA256 hash of .\Configuration files\Configuration 1.txt:
fab585d185d316ad6c45b1d414d8bf55fa8ef0094173fe9a8a5fa2d3ddc2e43b
CertUtil: -hashfile command completed successfully.
```

5. **DUT Configuration:**

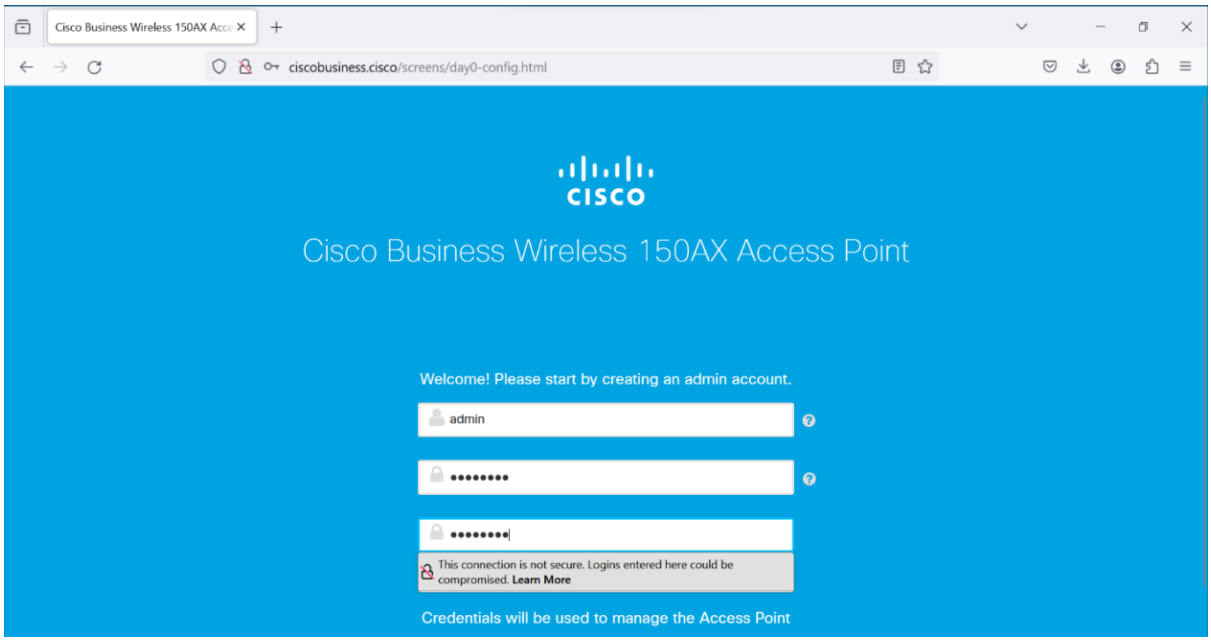
Initial Basic Configuration of CPE

Step 1: Power on the CPE and wait for the CPE to be visible on the Laptop Wi-Fi Scanning “Cisco Business-Setup” or Reset the CPE if not Visible

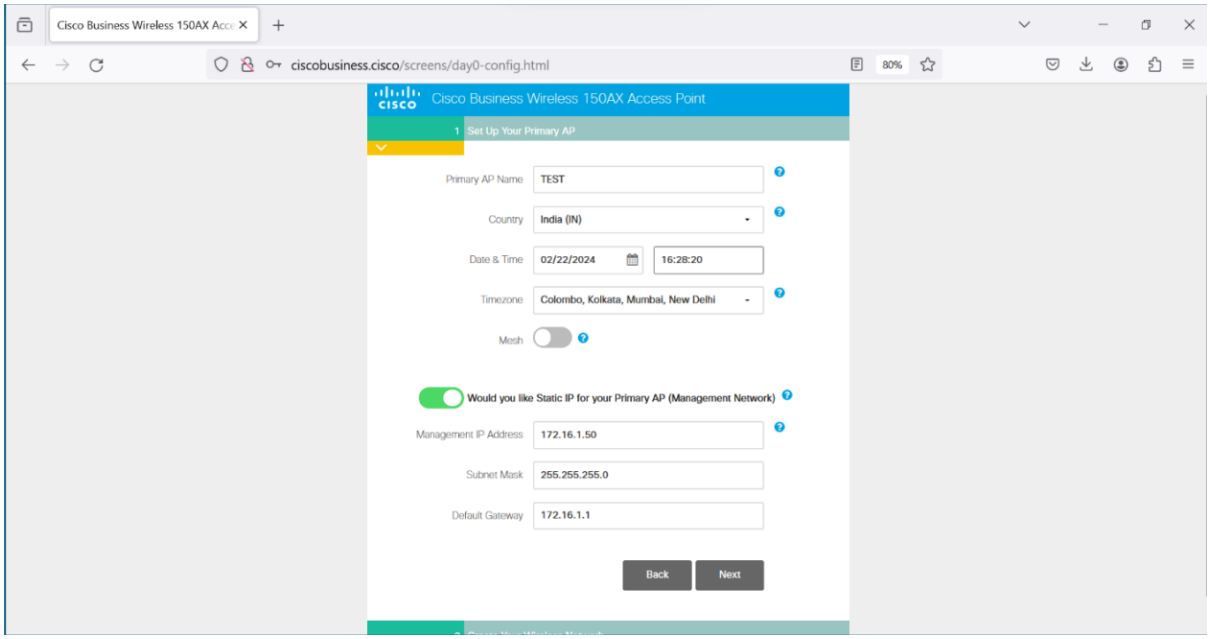
Step 2: Connect To the Wi-Fi Access Point using password “ Cisco123” And Navigate to http://ciscobusiness.cisco/screens/startup.html and Click Start as Show in the below Screenshot.



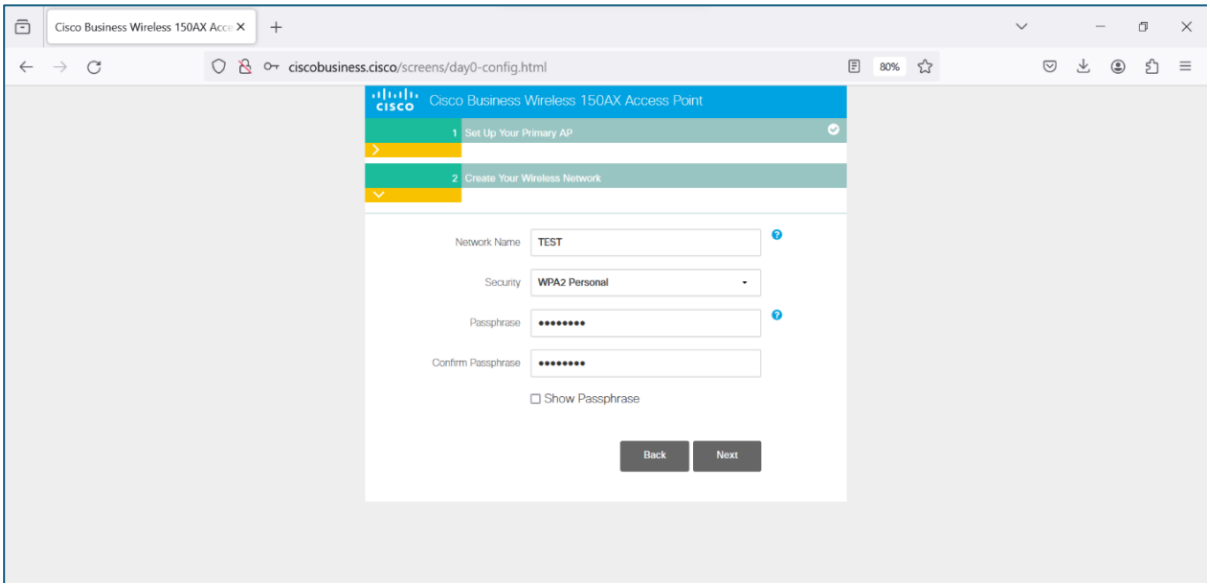
Step 3 : Enter the Desire Credentials for admin account creation and click start



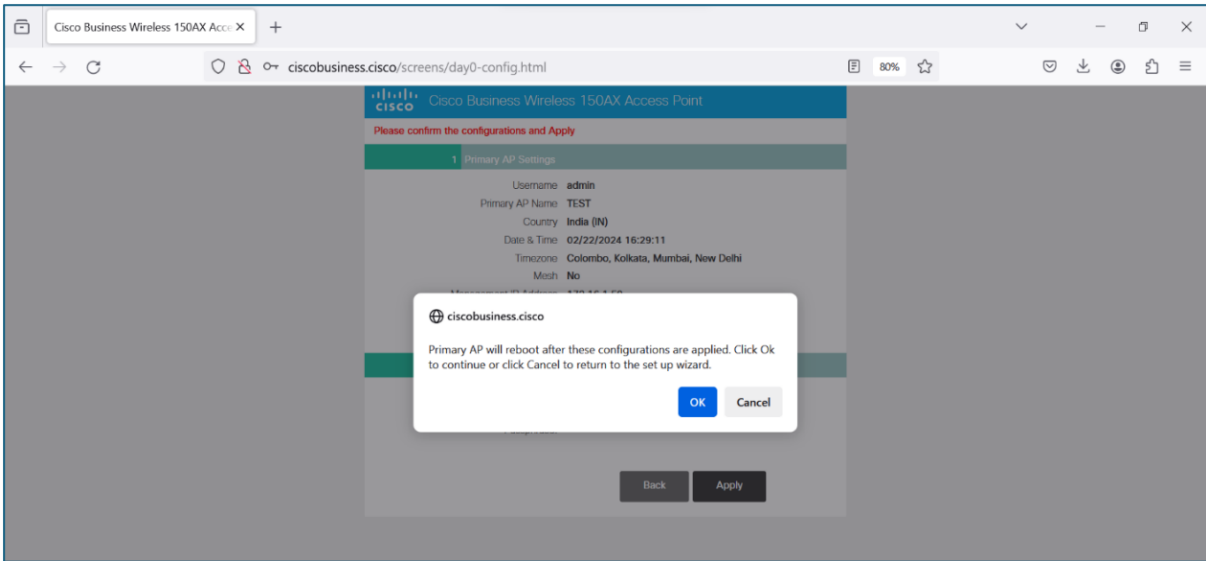
Step 4 : Enter the Desire AP Name and Select Static IP Configuration if required and click Next



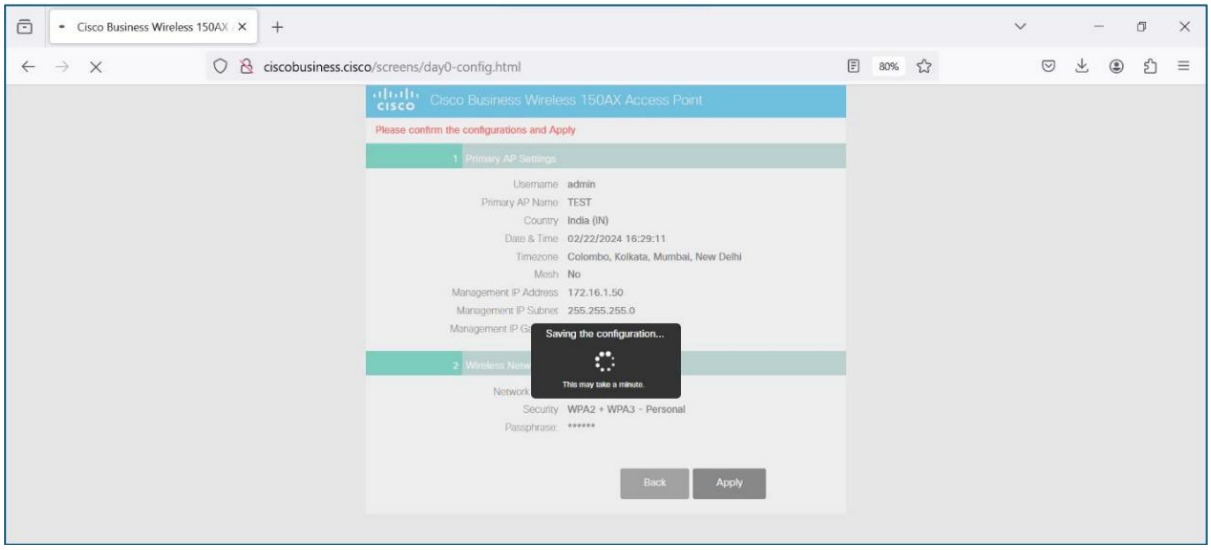
Step 5 : Enter the Desire Network Name and Passphrase and click Next

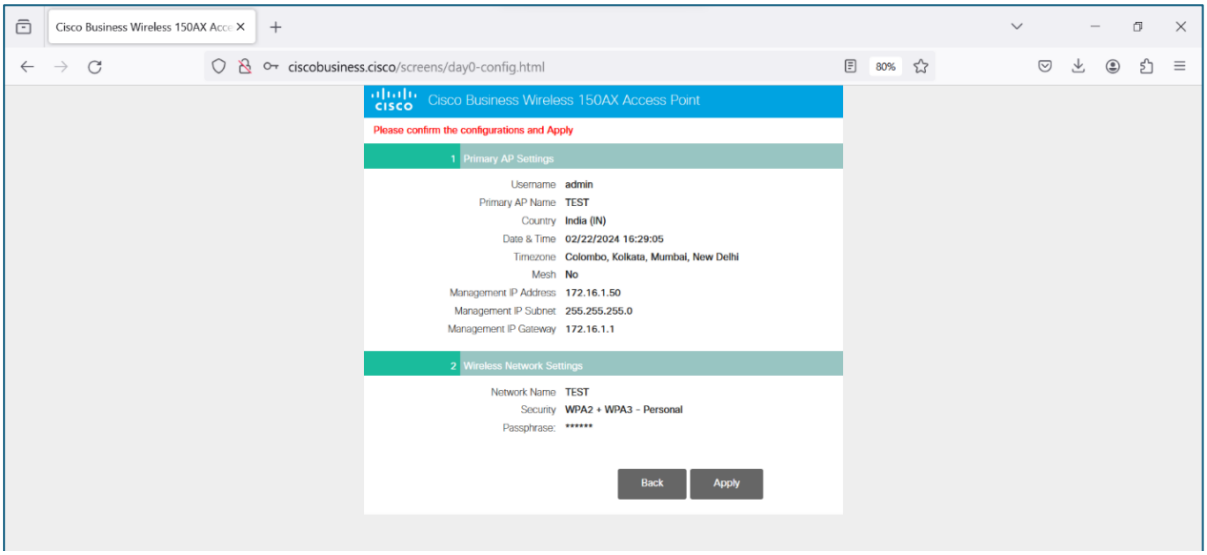


Step 6 : Verify the Configuration done and Click on Apply



Step 7 : A popup will appear on the screen "Primary AP will reboot after these configurations are applied. Click Ok to continue or click Cancel to return to the set-up wizard."





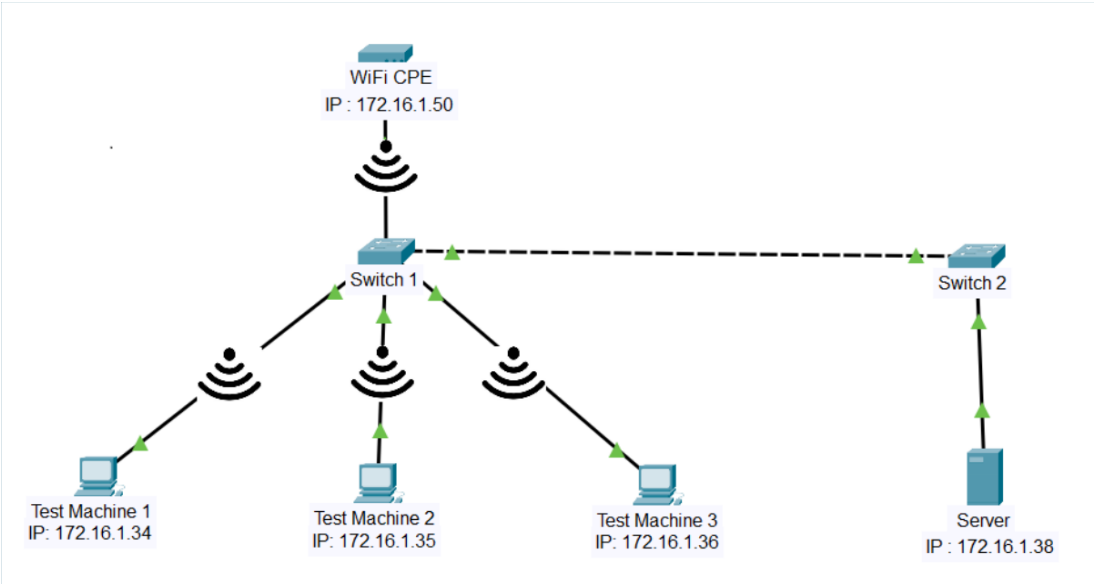
Step 8: Finished Step Now the AP is Ready to Be used.

6. **Preconditions**
   - Network Product documentation which contains information on log file location and procedure to access it.
   - Tester has the necessary privileges to access the log files.
   - Test environment with a Web Browser.

7. **Test Objective**: Verify that all accesses to the webserver are logged with the required information.

8. **Test Plan:**
   8.1 Number of Test Scenarios:
   8.1.1 Check whether the web server is logging the user logging

   8.2 Test Bed Diagram



8.3 Tools Required:- Browser

8.4 Test Execution Steps

- Power up the testbed
- The tester tries to login to the webserver using the correct and incorrect login credentials.
- The tester verifies whether the login attempts were logged correctly with all the required information.

9. **Expected Results for Pass:**

Case 1: All webserver events are logged with all of the required information.

10. **Expected Format of Evidence:** Testing report contains copies of the log file showing the captured information.

11.1 **Test Execution:**

11.1 Test Case Number: 01

11.1.1 **Test Case Name:** TC_WEBSERVER_LOGGING

11.1.2 **Test Case Description:** Verify that all accesses to the webserver are logged with the required information

The web server log shall contain the following information:

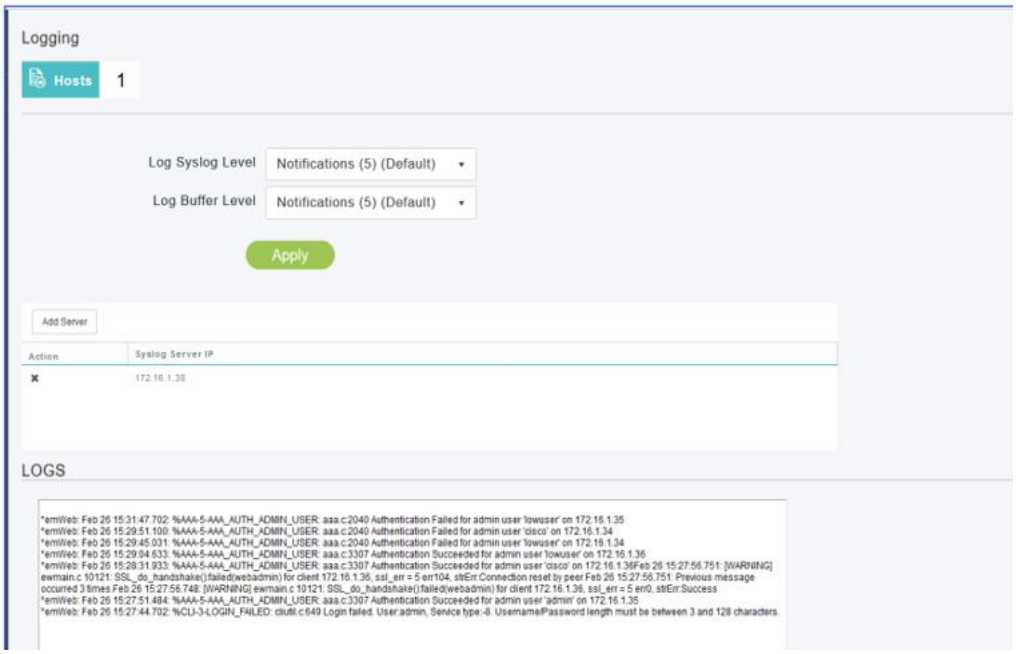
- Access timestamp - Source (IP address)
- Account (if known)
- Attempted login name (if the associated account does not exist)
- Relevant fields in http request. The URL should be included whenever possible.
- Status code of web server response

11.1.3 **Execution Steps:**

Step 1 : Connect to the network with right and wrong credentials.

Step 2: Navigate to advanced > logging and observe the logs.

Step 3: Observed the logs are generating for both Success and Failed login attempts.



11.1.4 **Test Observations:** The CPE has failed to log all the information

12Test Case Result:

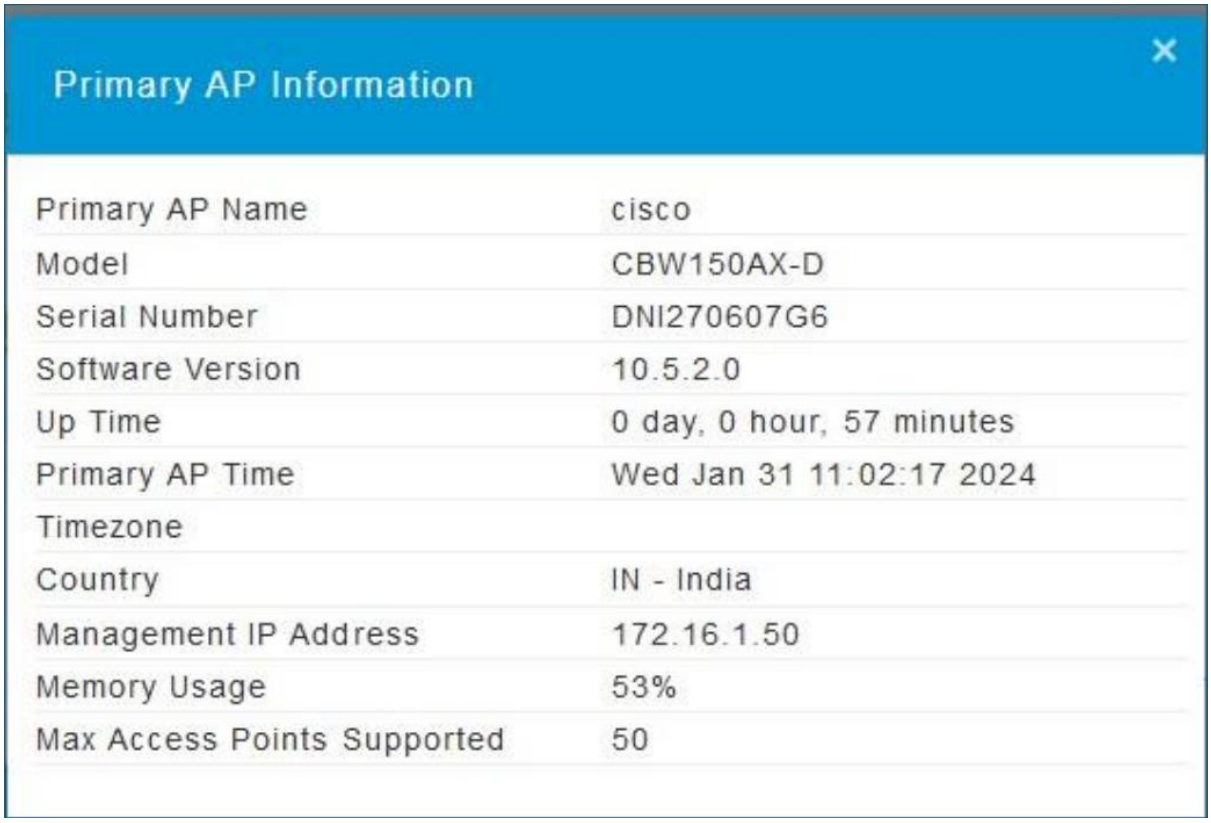
S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_WEBSERVER_LOGGING	FAIL	CPE has failed to log all the information

1.11.3 HTTP User sessions

<DUT Details: > WiFi CPE
<DUT Software Version:> cisco 10.5.2.0
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 11: Web Server
2. **<Security Requirement No & Name >** 1.11.3: HTTP User sessions
3. **<Requirement Description: >**
   - The session ID shall uniquely identify the user and distinguish the session from all
   - other active sessions.
   - The session ID shall be unpredictable.
   - The session ID shall not contain sensitive information in clear text (e.g., account
   - number, social security, etc.).
   - In addition to the Session Idle Time out.
   - Session IDs shall be regenerated for each new session (e.g. each time a user logs in).
   - The session ID shall not be reused or renewed in subsequent sessions.
   - The CPE shall not use persistent cookies to manage sessions but only session cookies.
   - Where session cookies are used the attribute 'Http Only' shall be set to true.
   - Where session cookies are used the 'domain' attribute shall be set to ensure that the cookie can only be sent to the specified domain.
   - Where session cookies are used the 'path' attribute shall be set to ensure that the cookie can only be sent to the specified directory or sub-directory.
   - The CPE shall not accept session identifiers from GET/POST variables.
   - The CPE shall be configured to only accept server generate session ID's.

4. **DUT Confirmation Details**: Screenshot below shows the DUT name (Primary AP Name) , Model number, Serial Number, Software Version.



DUT Configuration Checksum:

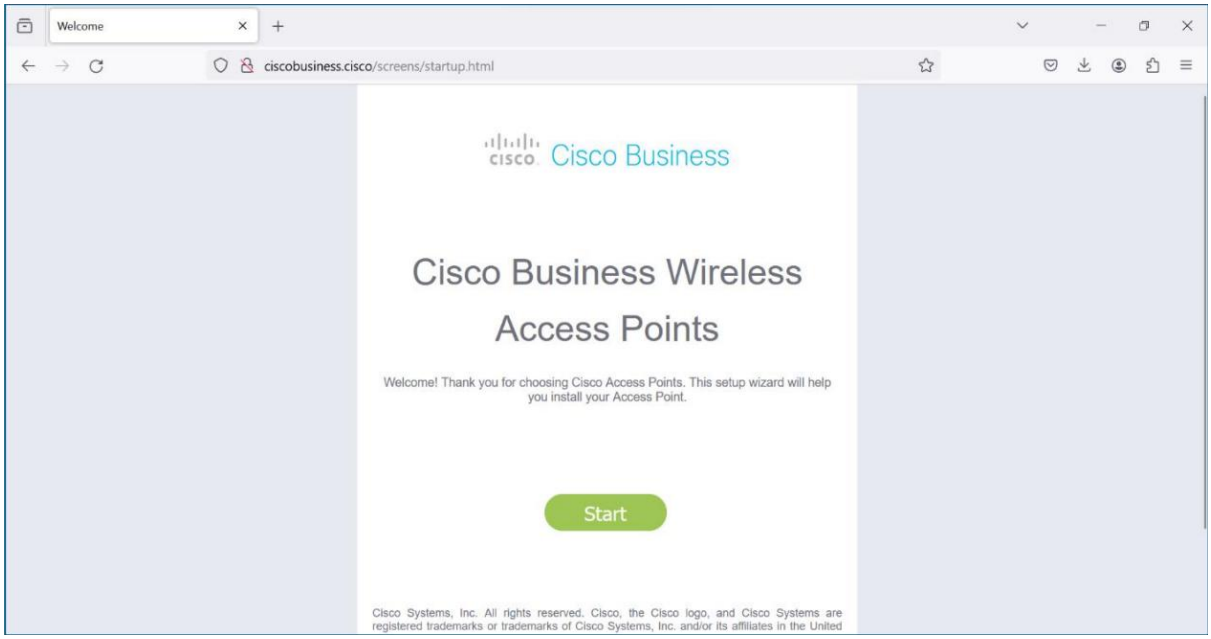
```
PS C:\> certutil -hashfile '.\Configuration files\Configuration 1.txt' SHA256
SHA256 hash of .\Configuration files\Configuration 1.txt:
fab585d185d316ad6c45b1d414d8bf55fa8ef0094173fe9a8a5fa2d3ddc2e43b
CertUtil: -hashfile command completed successfully.
```

5. **DUT Configuration:**

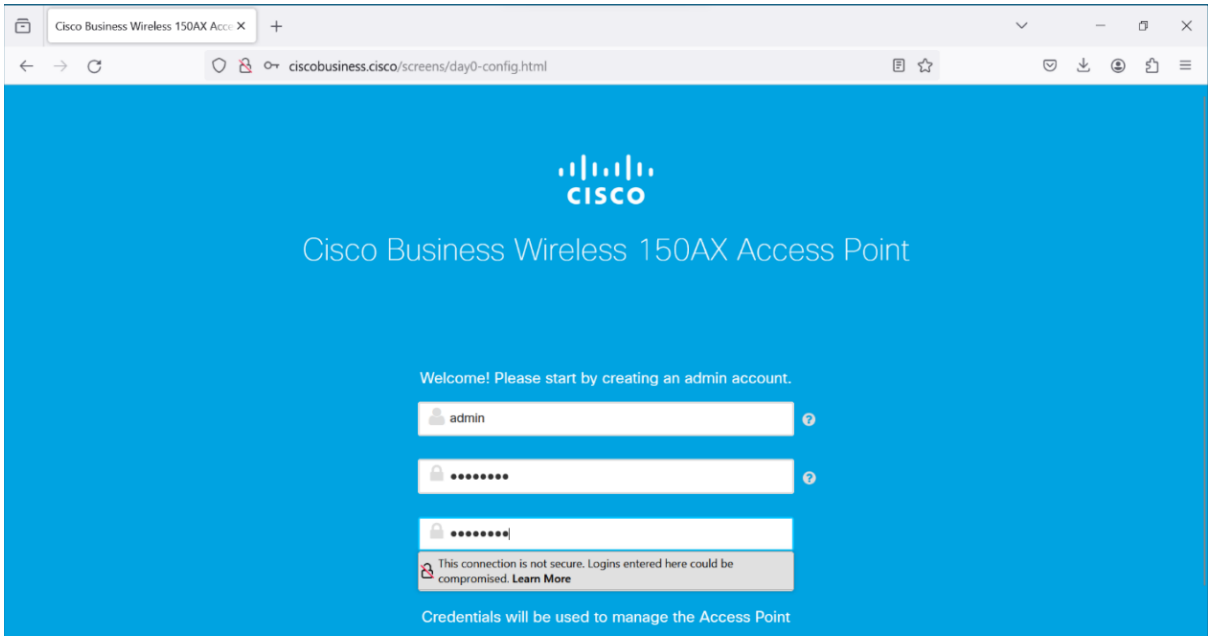
Initial Basic Configuration of CPE

Step 1: Power on the CPE and wait for the CPE to be visible on the Laptop Wi-Fi Scanning “Cisco Business-Setup” or Reset the CPE if not Visible

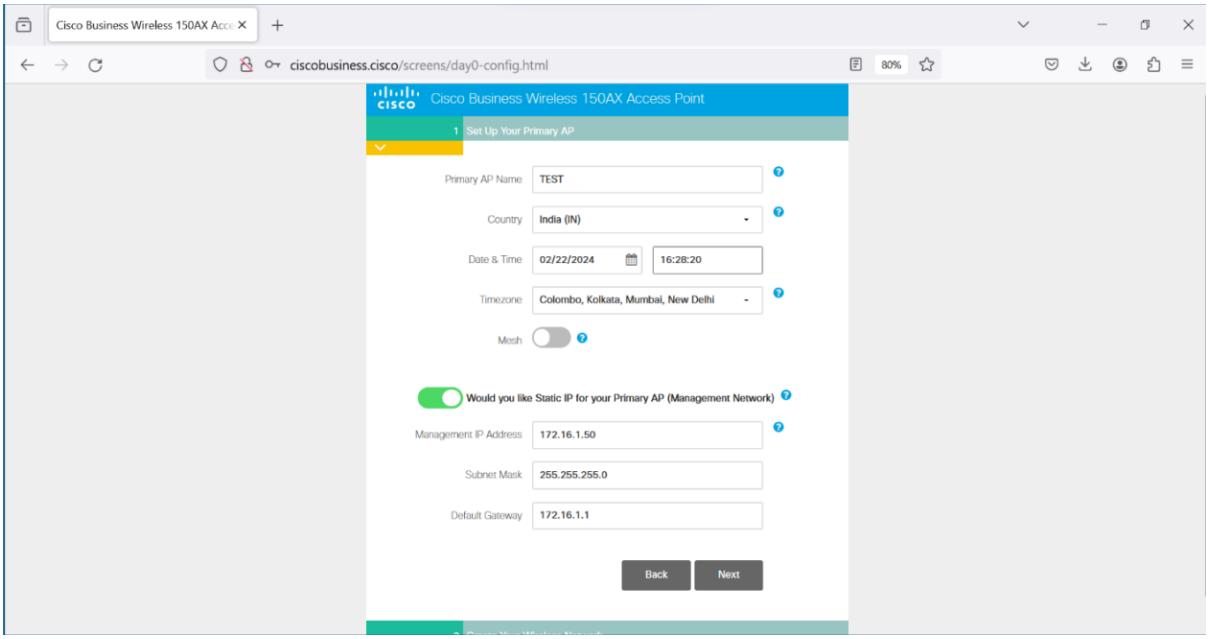
Step 2: Connect To the Wi-Fi Access Point using password “ Cisco123” And Navigate to http://ciscobusiness.cisco/screens/startup.html and Click Start as Show in the below Screenshot.



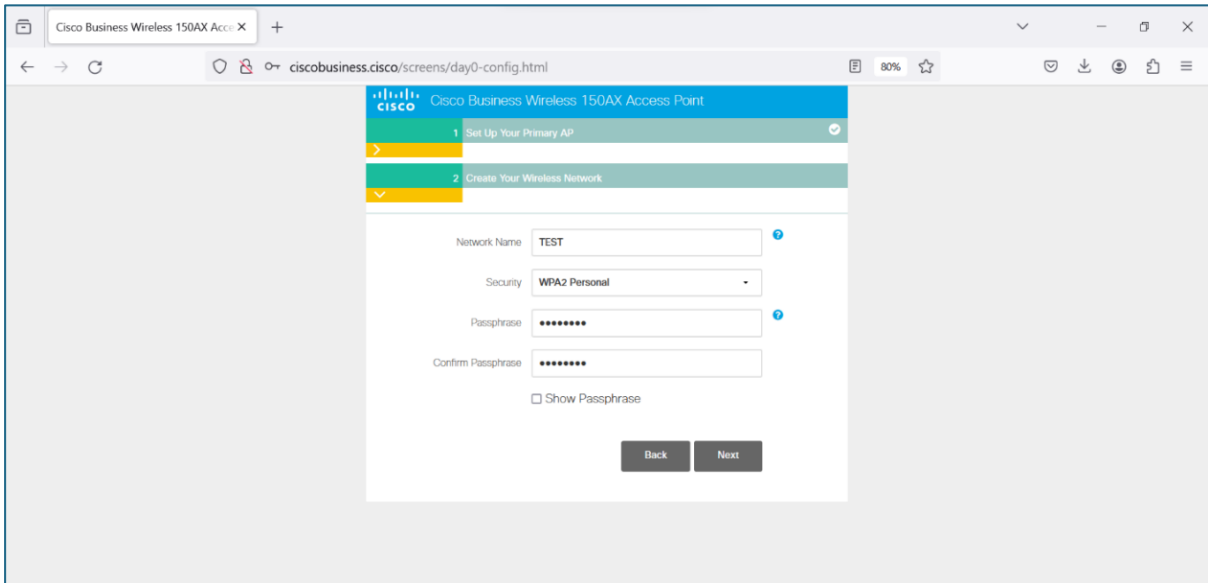
Step 3 : Enter the Desire Credentials for admin account creation and click start



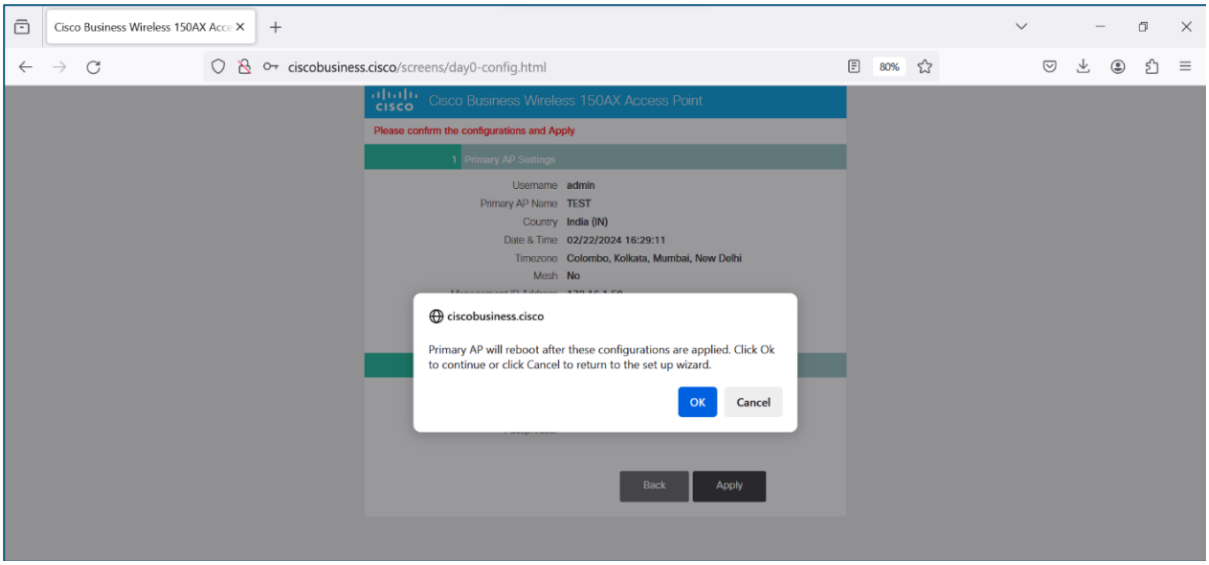
Step 4 : Enter the Desire AP Name and Select Static IP Configuration if required and click Next



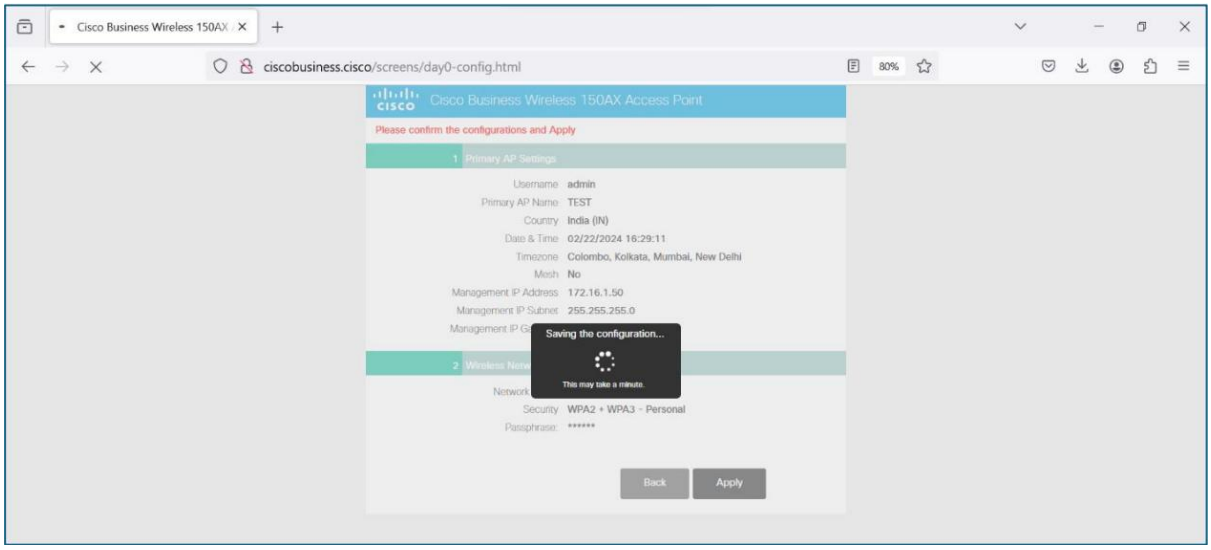
Step 5 : Enter the Desire Network Name and Passphrase and click Next

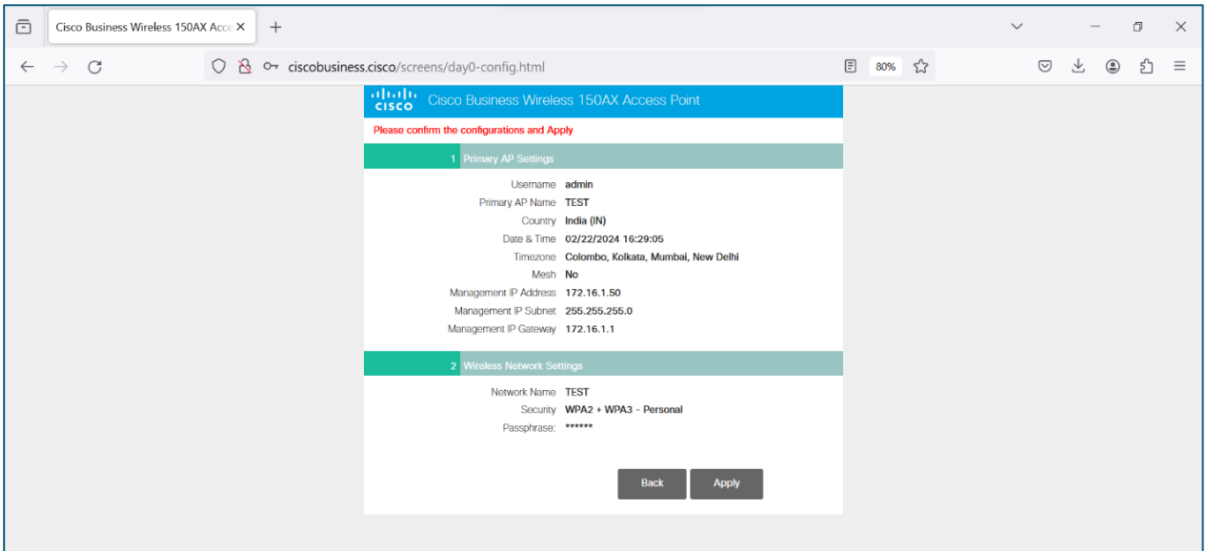


Step 6 : Verify the Configuration done and Click on Apply



Step 7 : A popup will appear on the screen “Primary AP will reboot after these configurations are applied. Click Ok to continue or click Cancel to return to the set-up wizard.”





Step 8: Finished Step Now the AP is Ready to Be used.

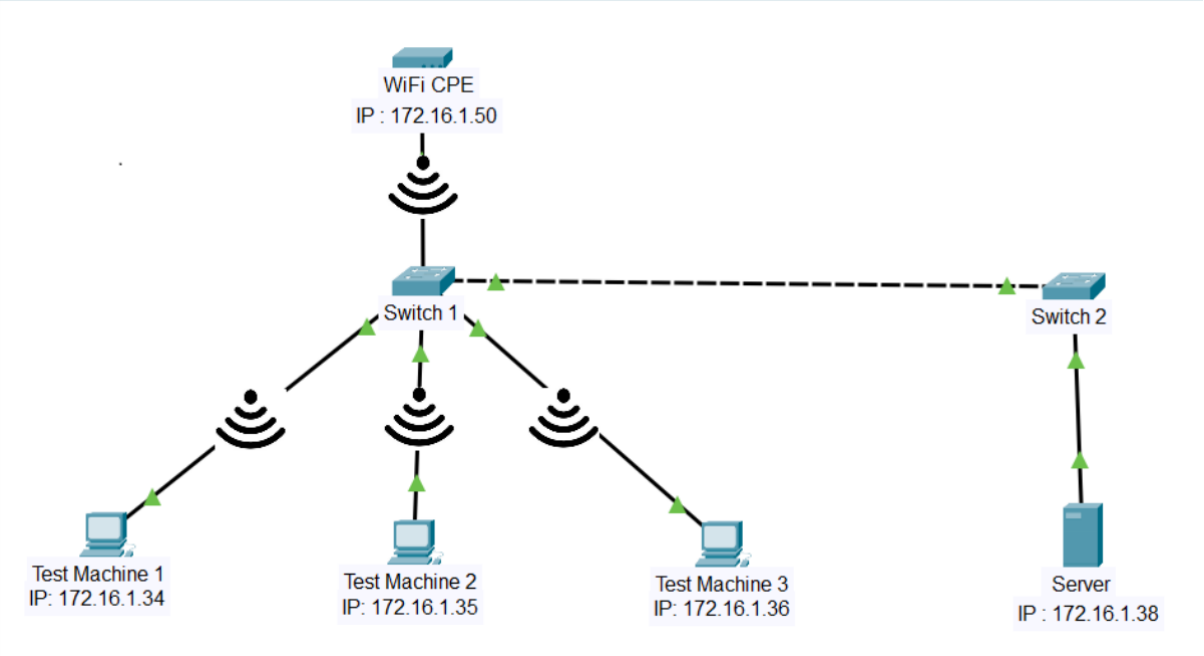
6. **Preconditions**
   - Enable https on DUT
   - The tester has administrative privileges
   - A tester machine is available.
   - Test environment with a Web Browser.
   - The Network Product uses a session ID that is communicated between the client and Network Product to establish and maintain a session.
   - Documentation describing how a session is maintained and where the session ID is stored / and how this is communicated and after how long sessions expire.
   - The documentation should describe the algorithm used to generate the session IDs
7. **Test Objective**: Verify that the above 12 session ID and session cookie requirements have been met.

8. **Test Plan:**

   8.1 Number of Test Scenarios:

   8.1.1 Check whether the user session ID is unique from other active sessions.
   8.1.2 Checking for the session ID vulnerabilities
   8.1.3 Check whether the session ID is disclosing any sensitive information in clear text / regeneration for each new session.
   8.1.4 Check whether the cookie is set to “max-age”, “Http Only”, “domain” attribute, & “path” attribute.
   8.1.5 Check if the CPE is not accepting session identifiers from GET/POST variables.
   8.1.6 Check if the CPE has been configured to only accept server-generated session IDs.
   8.1.7 Check if Session ID's are regenerated for each new session In addition to the Session Idle Timeout

8.2 Test Bed Diagram



8.3 Tools Required

- Browser
- Burp Suite

8.4 Test Execution Steps

– Power up the testbed
– The tester tries to access the Web Server in the browser.
– Access the Cookies and Session IDs and analyse them.
– The tester logs in repeatedly with different user IDs and a number of times with the same user ID in a row and collects the session IDs according to the documentation and the user IDs associated with them. The tester verifies that:
  - a. The session IDs are different between sessions of the same and different users;
  - b. The session IDs seems random based on his/her own experience. The tester may use tests like the bitstream test or the count-the-1s-tests from the diehard test suite. The tester documents how randomness was verified;
  - c. The session IDs are always different between sessions, also when the user ID is the same.

- The tester verifies that when session cookies are used
  - a. neither the "expire" or the "max-age" is set;
  - b. the 'HttpOnly' is set to true;
  - c. the 'domain' attribute is set to the correct domain;
  - d. the 'path' attribute is set to the correct directory or sub-directory.

- The tester verifies that it is impossible to:
    - a. access a session by retrieving the session ID and communicating the session ID through a POST or GET variable.
    - b. generate a session ID on the client by attempting to login with a custom generated session ID.
    - c. keep a session alive for longer than the configured maximum lifetime (by default 8 hours).

9. **Expected Results for Pass:**
    - A list of session IDs and user IDs that are different between sessions even when the tester has logged in with the
    - same user and that are unpredictable as is confirmed by the entropy calculation.
    - A confirmation from the tester that the correct variables are indeed set.
    - A denied access to the tester when attempting the login via GET and POST when using and an expired session.

10. **Expected Format of Evidence:**
    - Session IDs follow the rules 1-3, 5, 6.
    - A session times out after 8 hours or sooner according to the documentation.
    - The correct cookie settings are used.
    - The network product does not accept customly generated session IDs and that session IDs over GET or POST are ignored.

11. **Test Execution:**

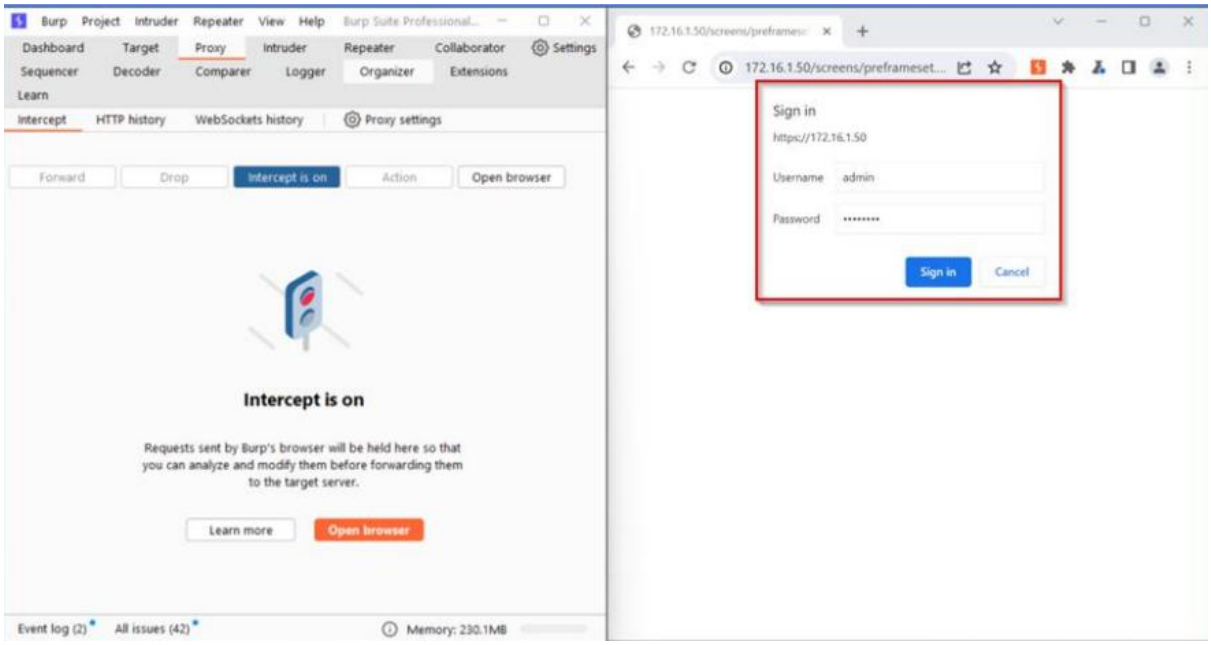
11.1 Test Case Number: 01

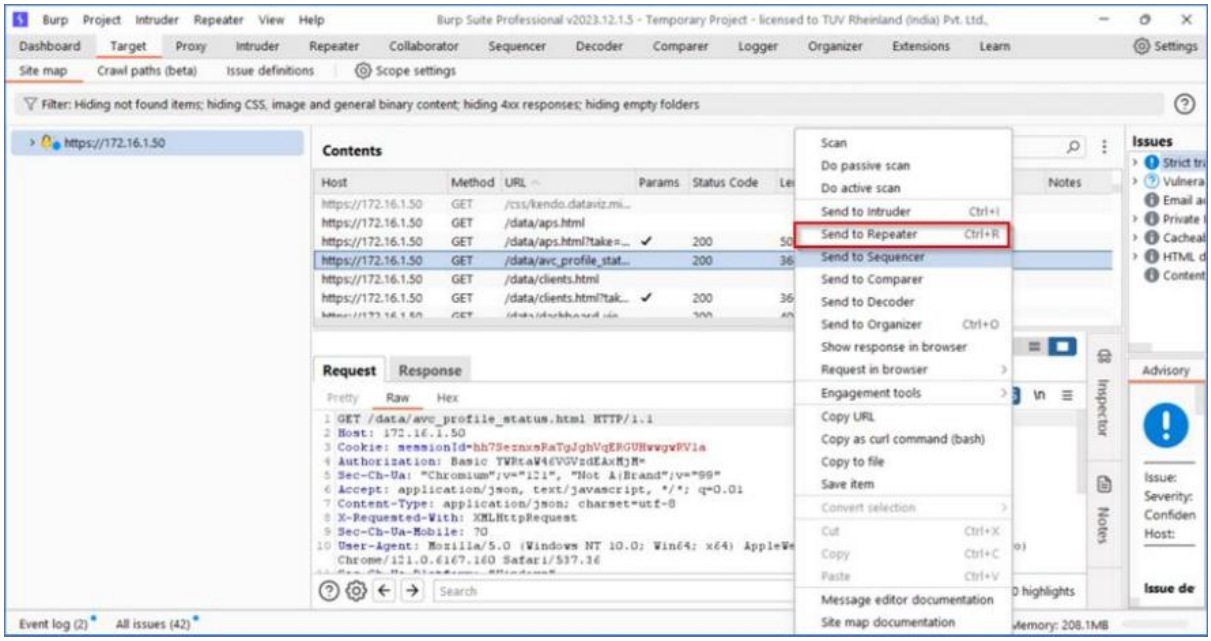
11.1.1 **Test Case Name:** TC_SESSIONID_UNIQUE_TESTS

11.1.2 **Test Case Description:** Verify user session ID is unique from other active sessions.

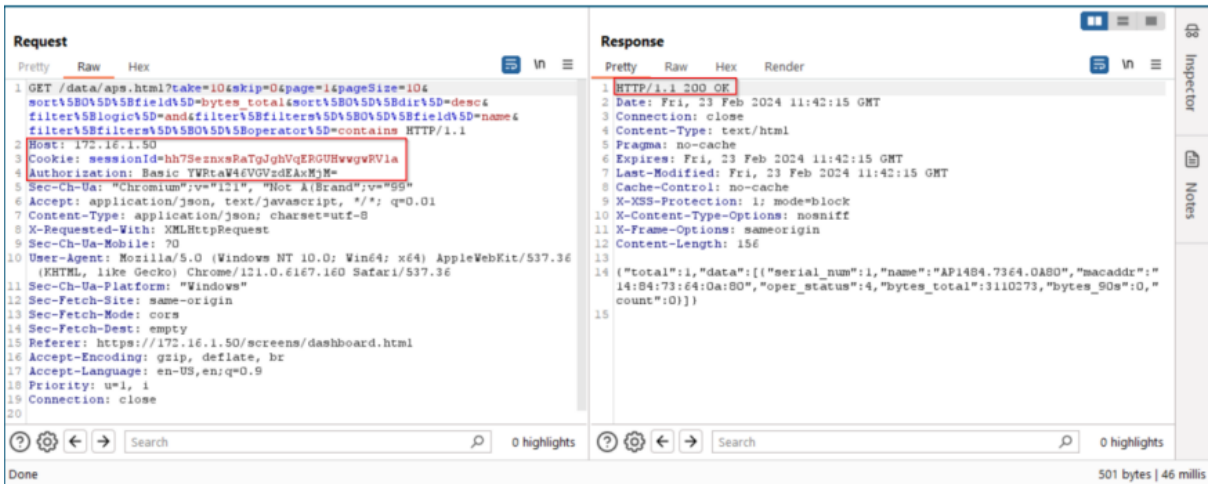
11.1.3 **Execution Steps:**

Step 1 : Open browser and navigate to https://172.16.1.50 and attempt a login then send the request to repeater

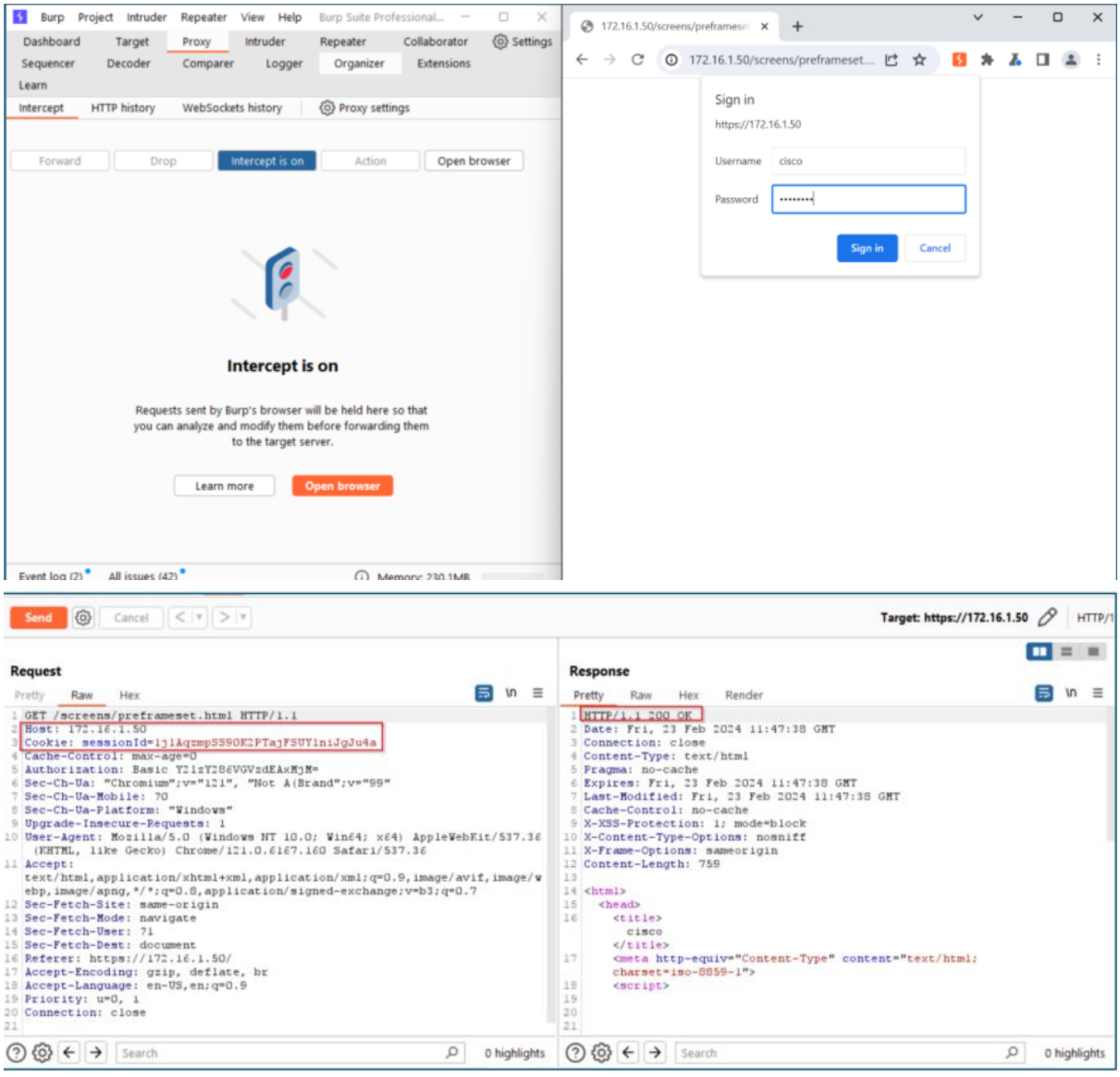




Step 2: Observe the response from server with a unique session id that is created for the user admin



Step 3: Repeat the same steps for user cisco and observe that different session id is created.



11.1.4 **Test Observations:** During the testing process DUT has created unique session ids for two different users

11.2 Test Case Number: 02

11.2.1 **Test Case Name:** TC_SESSIONID_VULNERABILITIES_TESTS

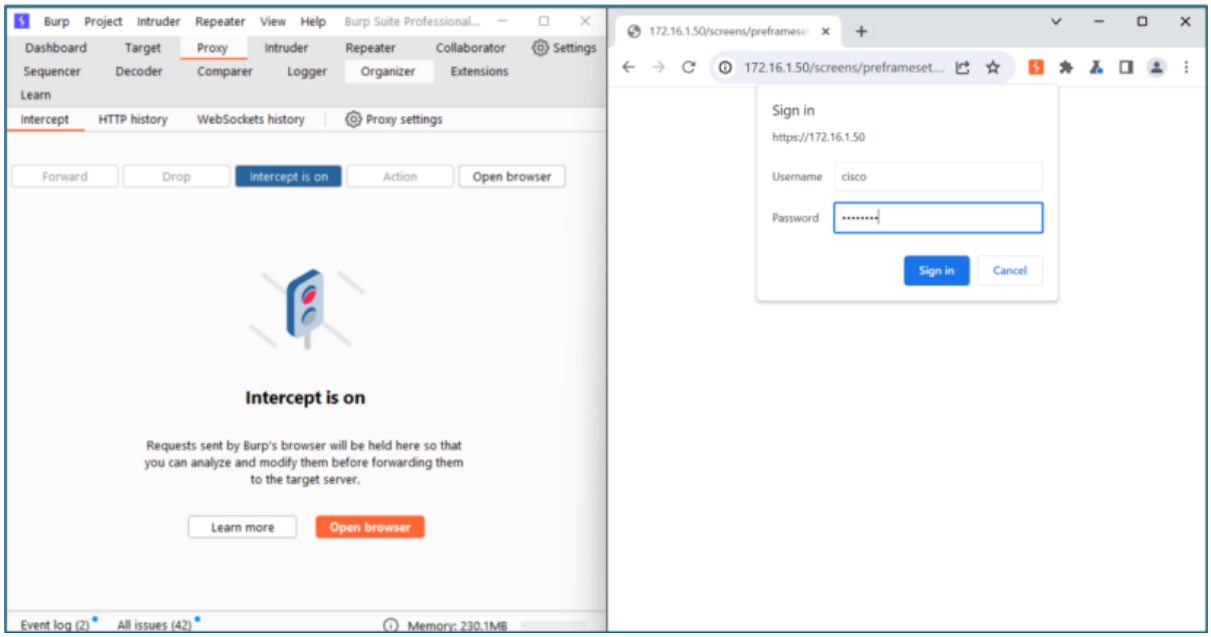
11.2.2 **Test Case Description:**

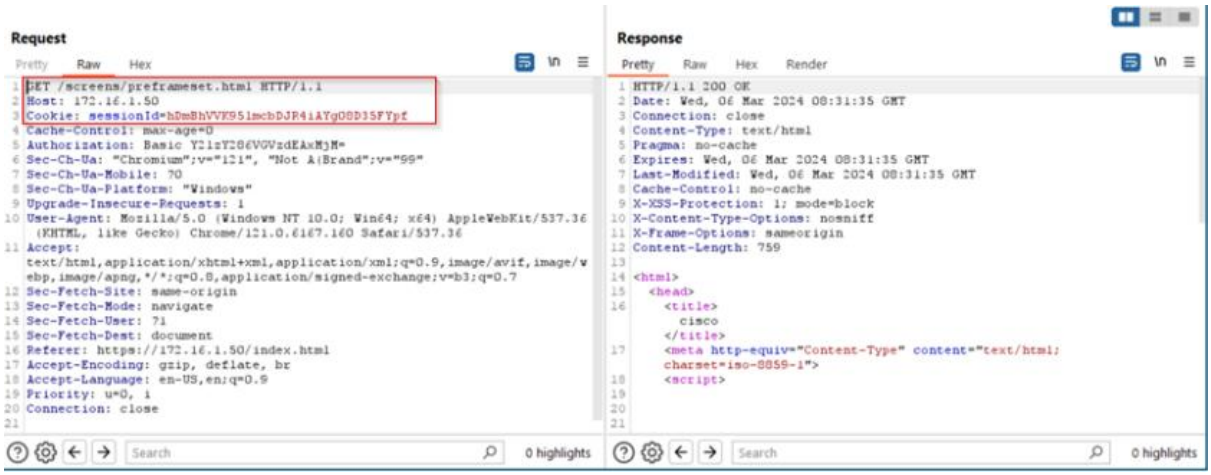
- To check for predictable sessionID
- To check for regeneration of sessionID for each new session,
- To check if subsequent sessions are not reused or renewed,
- To check if CPE is not using persistent cookies to manage sessions but only session cookies.

11.2.3 **Execution Steps:**

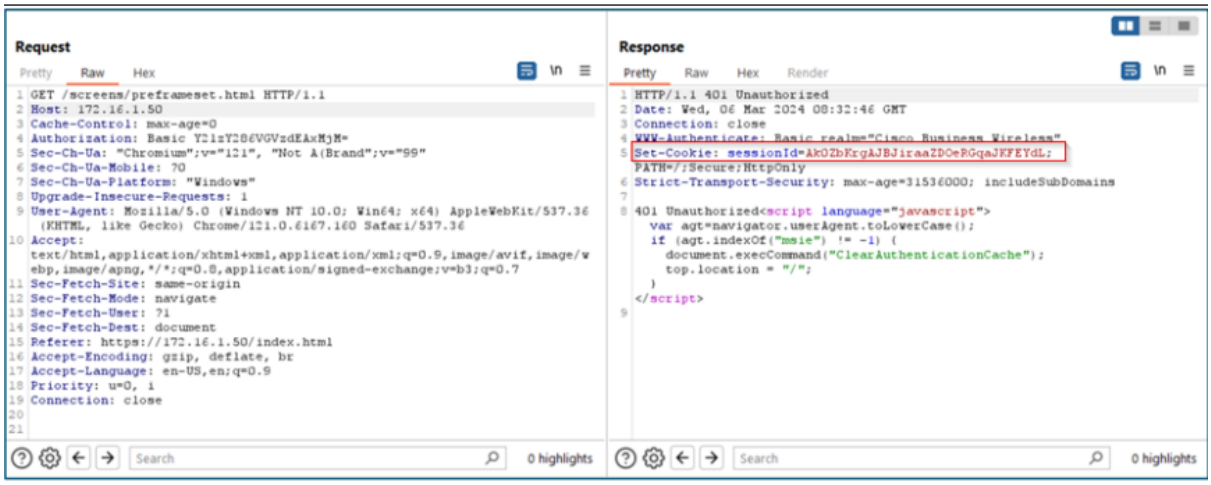
1. **To check for predictable sessionID:**

Step 1: Open the browser and go to https://172.16.1.50 capture the login request and send it to the repeater.

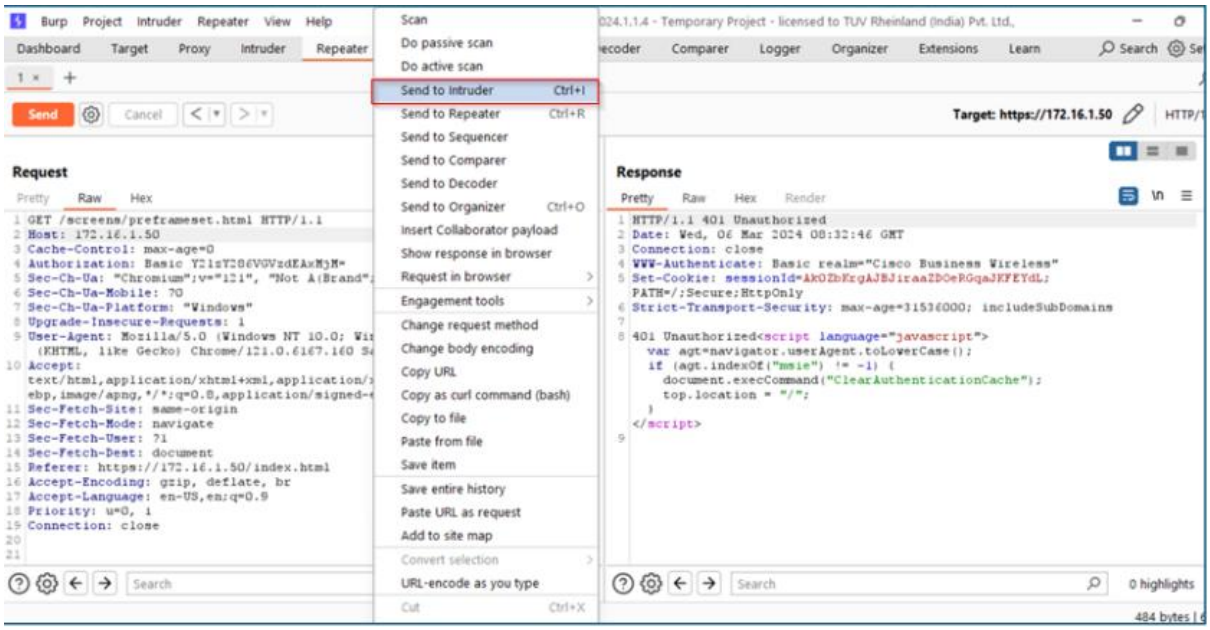




Step 2: Delete the session ID from the request and send and observe that a session id is created in the response.

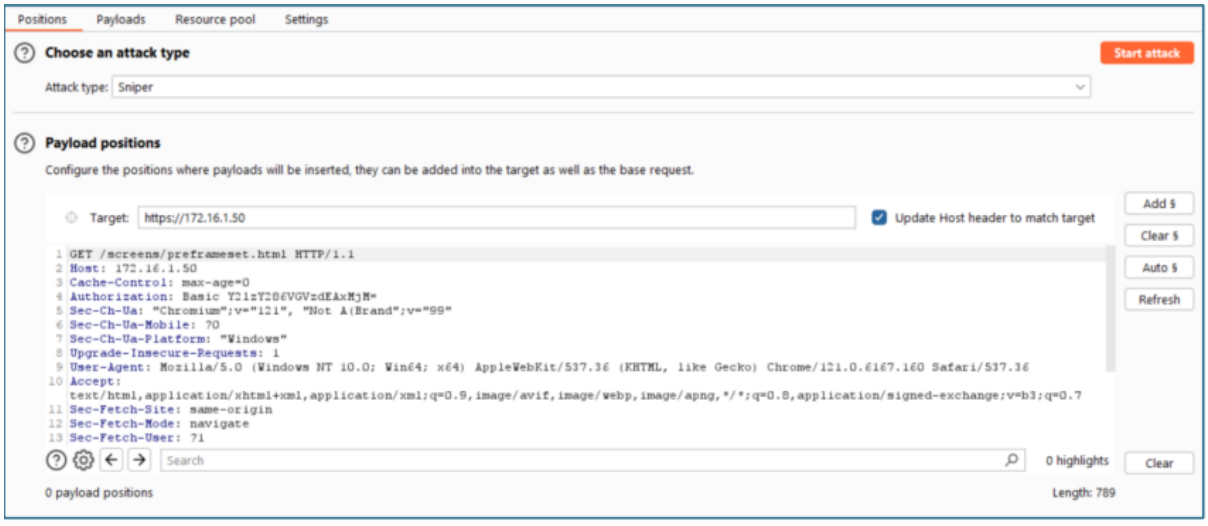


Step 3:Now send the same request to the Intruder.

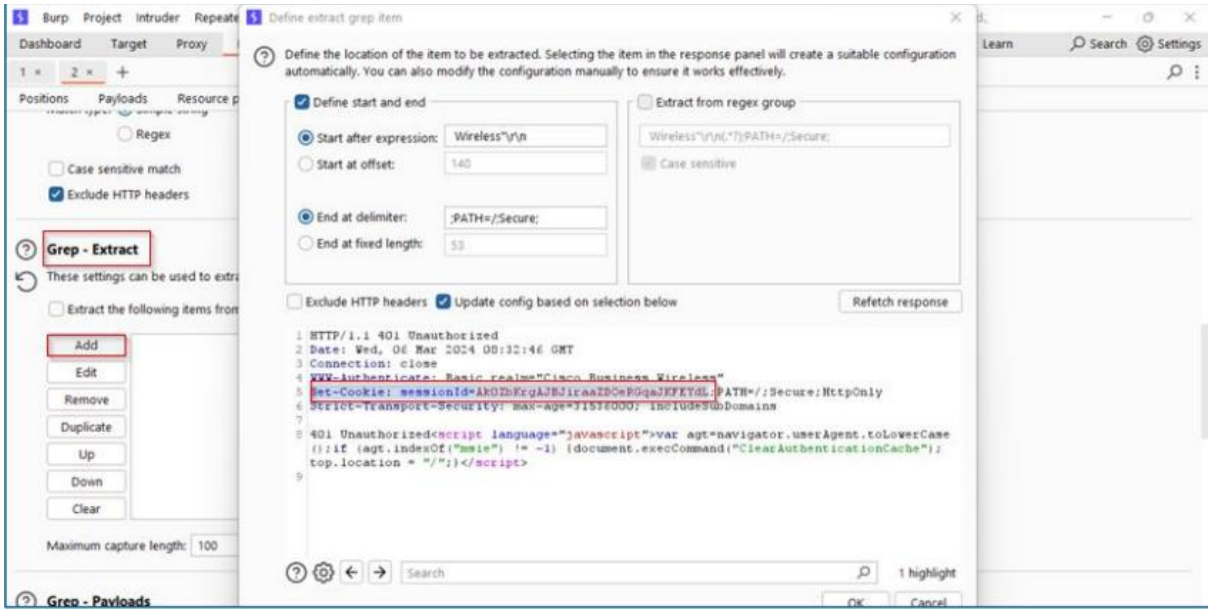


Step 4: In the Intruder, navigate to the payloads tab.

Step 5: Change the payload select Null payloads and make the required changes in settings as given in the screenshots below.

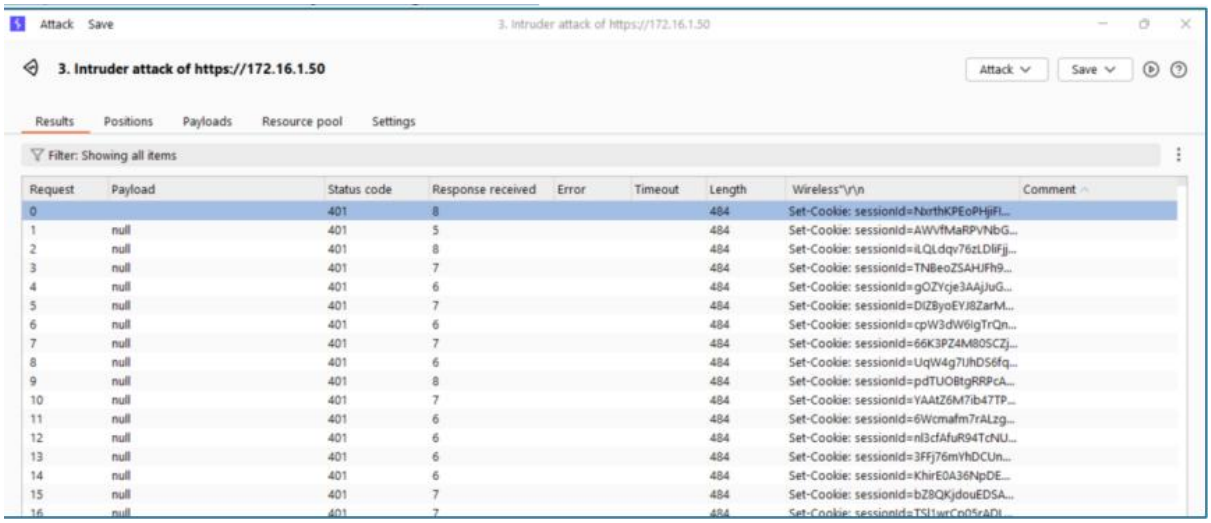


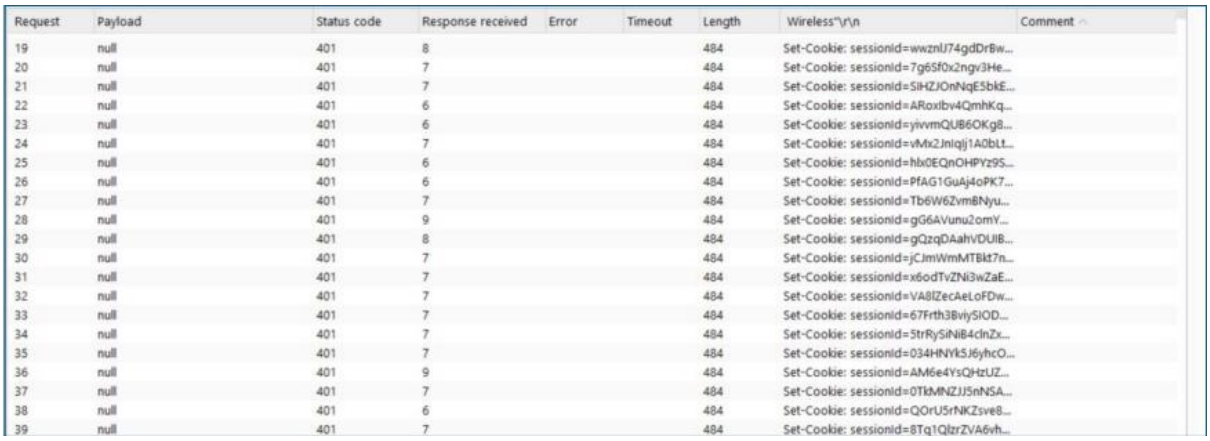
Step 6: Copy the set cookie sessionId.



Step 7: Add it in the grep-extract.

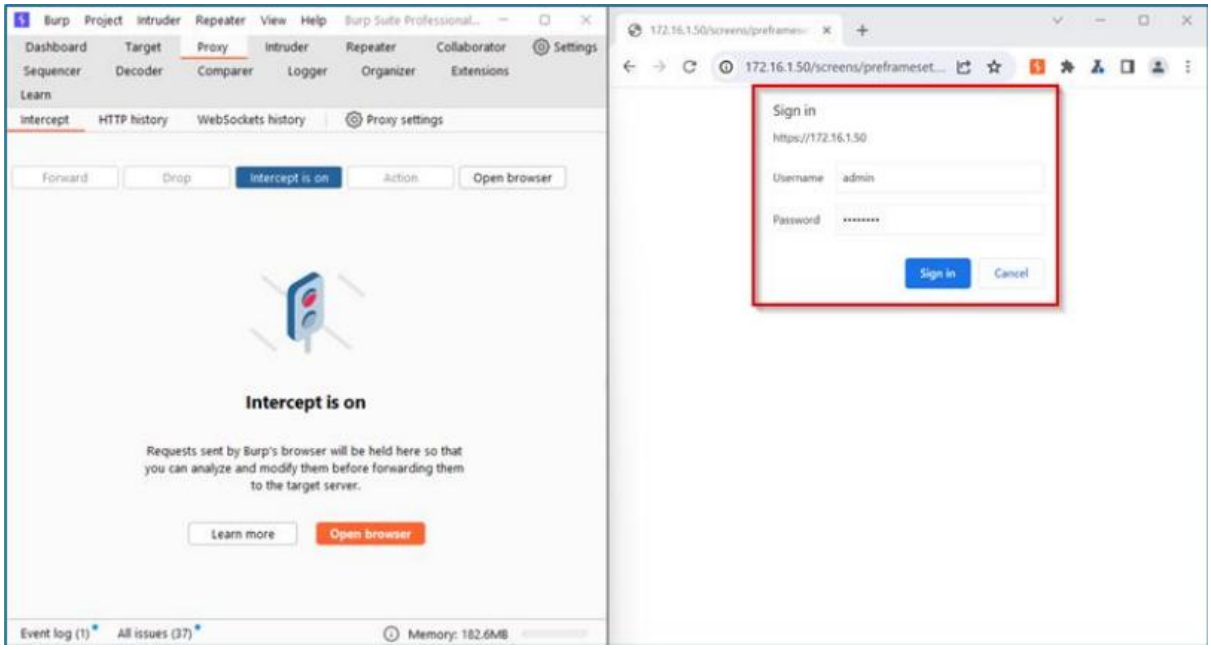
Step 7: Start the attack by clicking on "Start

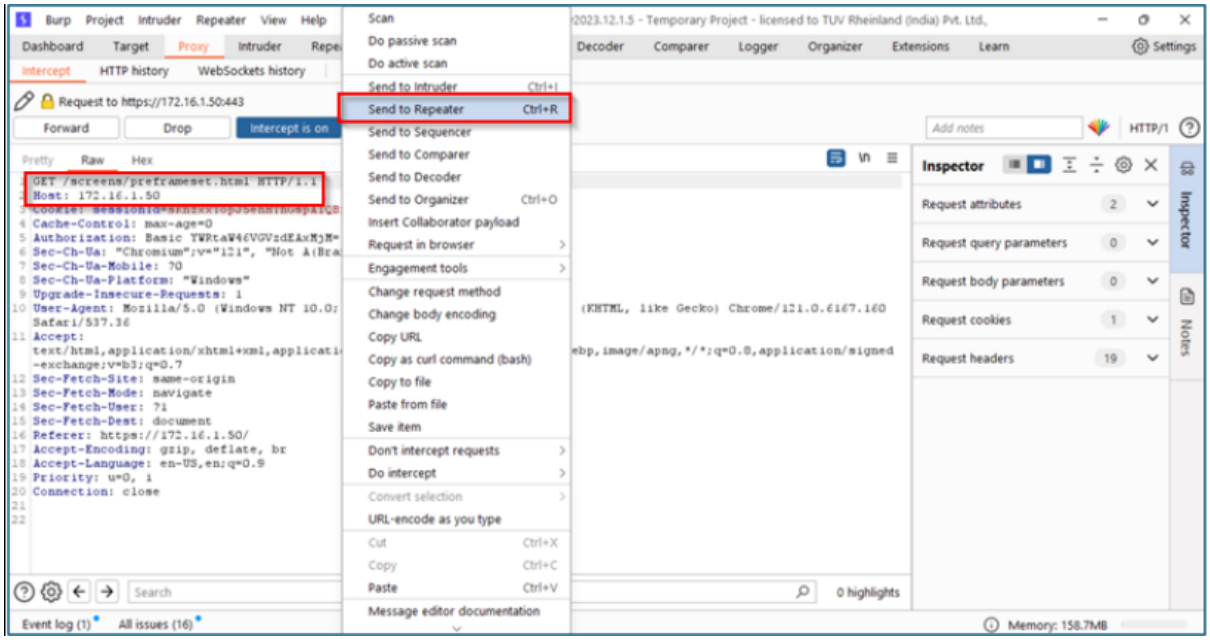


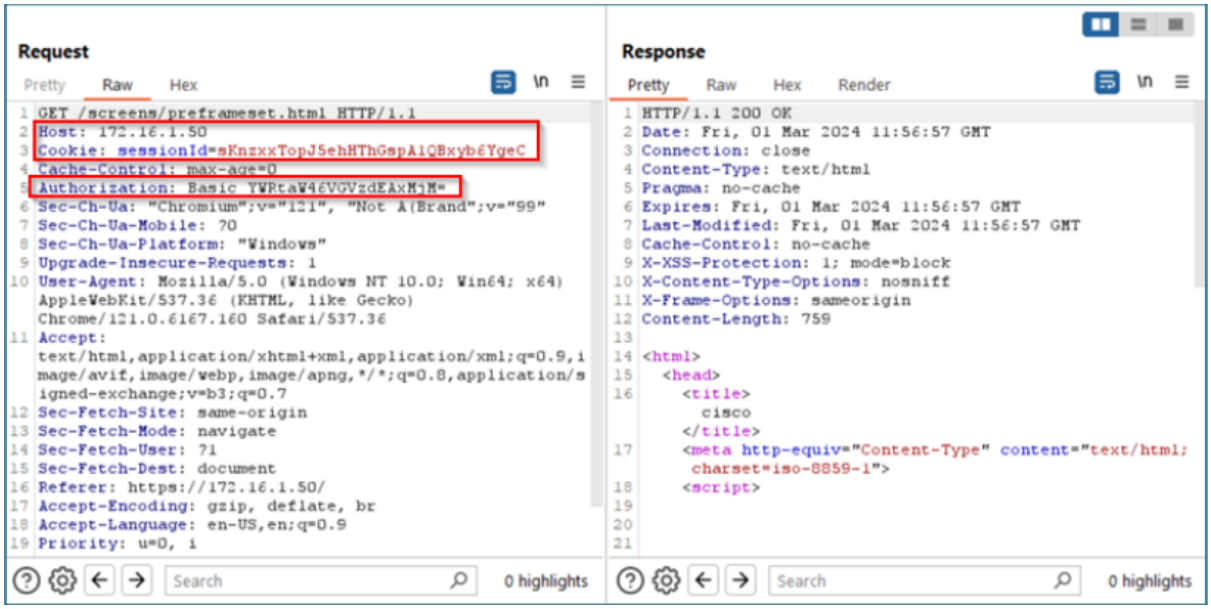


2. To check for regeneration of sessionID for each new session:

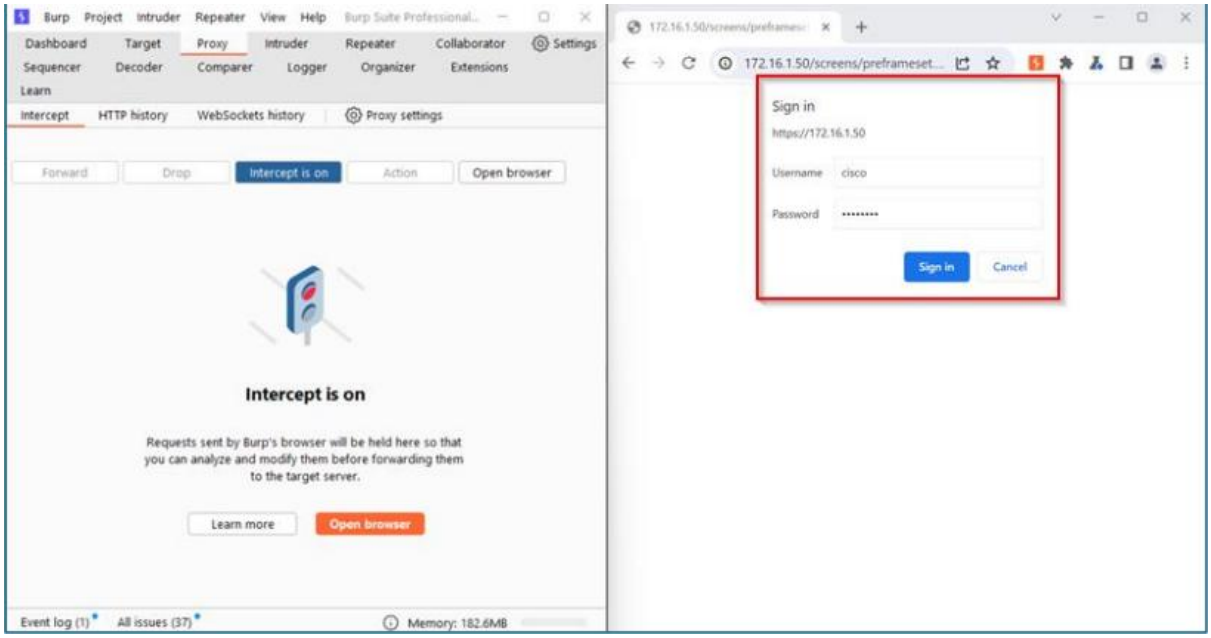
Step 1: Login with admin credentials over GUI intercept the request then send it to repeater and check for the sessionID

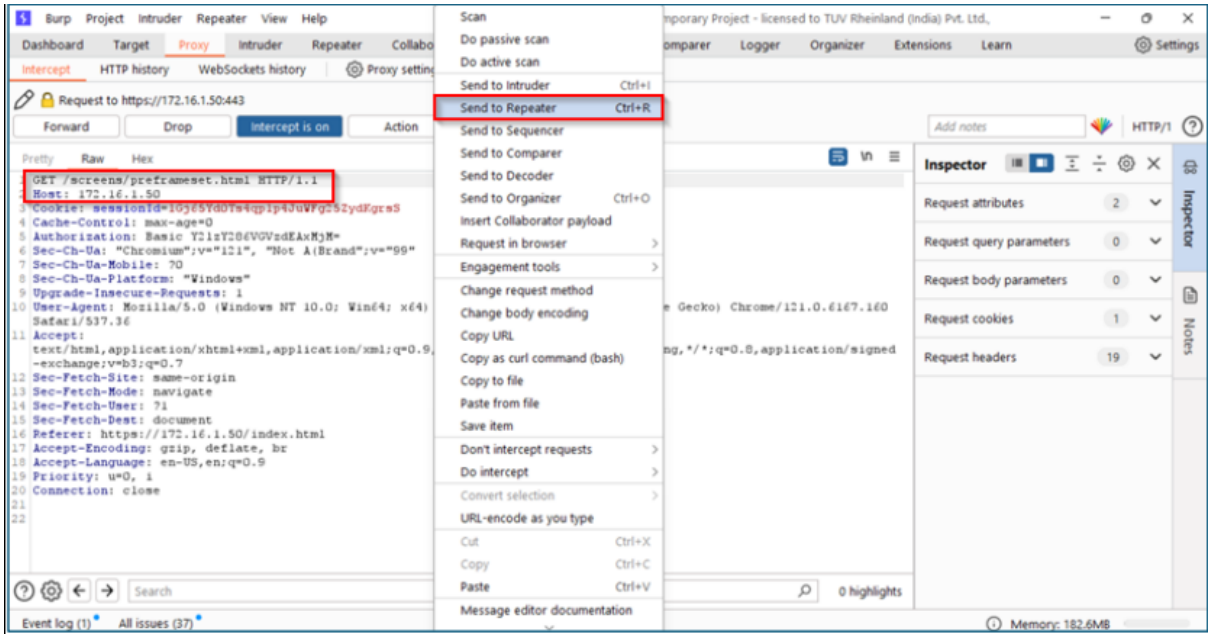


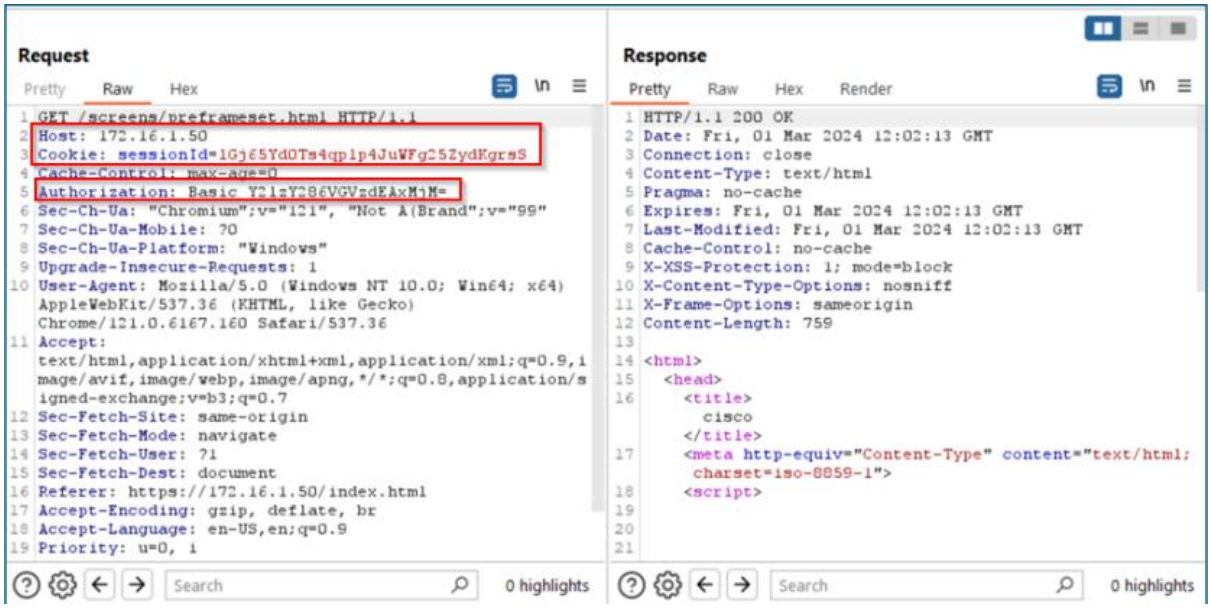




Step 2: Login with cisco credentials over GUI intercept the request then send it to repeater and check for the sessionID.


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Settings
Sequencer Decoder Comparer Logger Organizer Extensions
Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Intercept is on
Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.
Learn more
Open browser
Event log (1) All issues (37) Memory: 182.6MB
172.16.1.50/screens/preframeset...
Sign in
https://172.16.1.50
Username cisco
Password
Sign in
Cancel

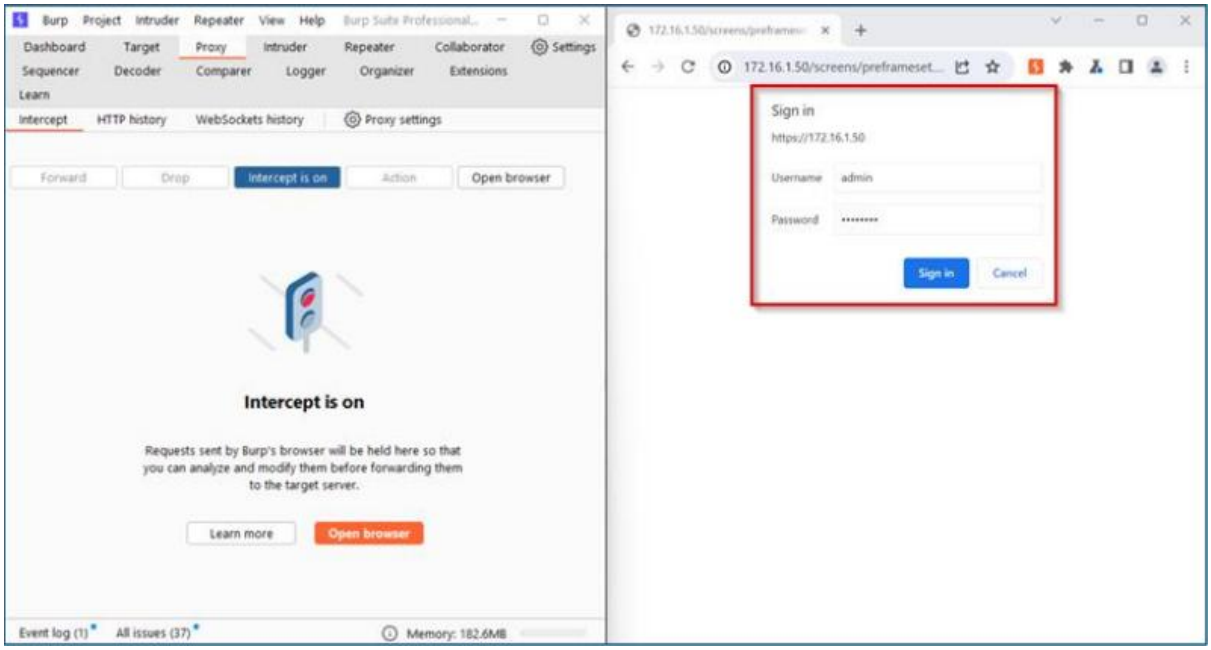

Request to https://172.16.1.50:443
Forward Drop Intercept is on Action
GET /screens/preframeset.html HTTP/1.1
Host: 172.16.1.50
Scan
Do passive scan
Do active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Insert Collaborator payload
Request in browser
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command (bash)
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 1
Request headers 19
Event log (1) All issues (37) Memory: 182.6MB

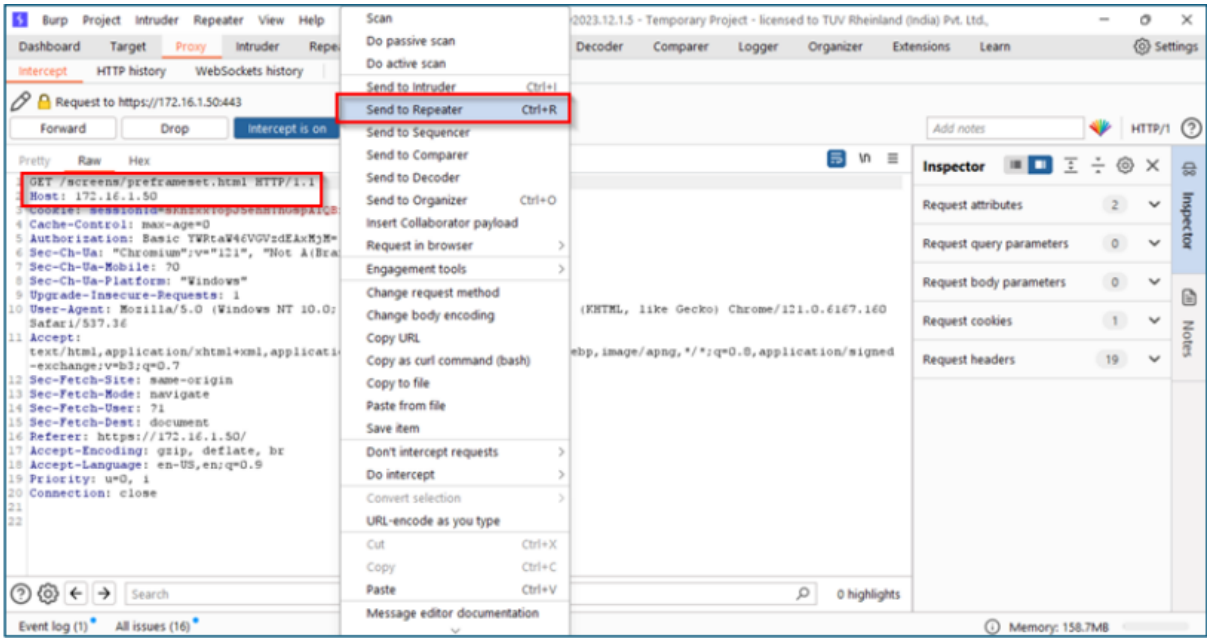


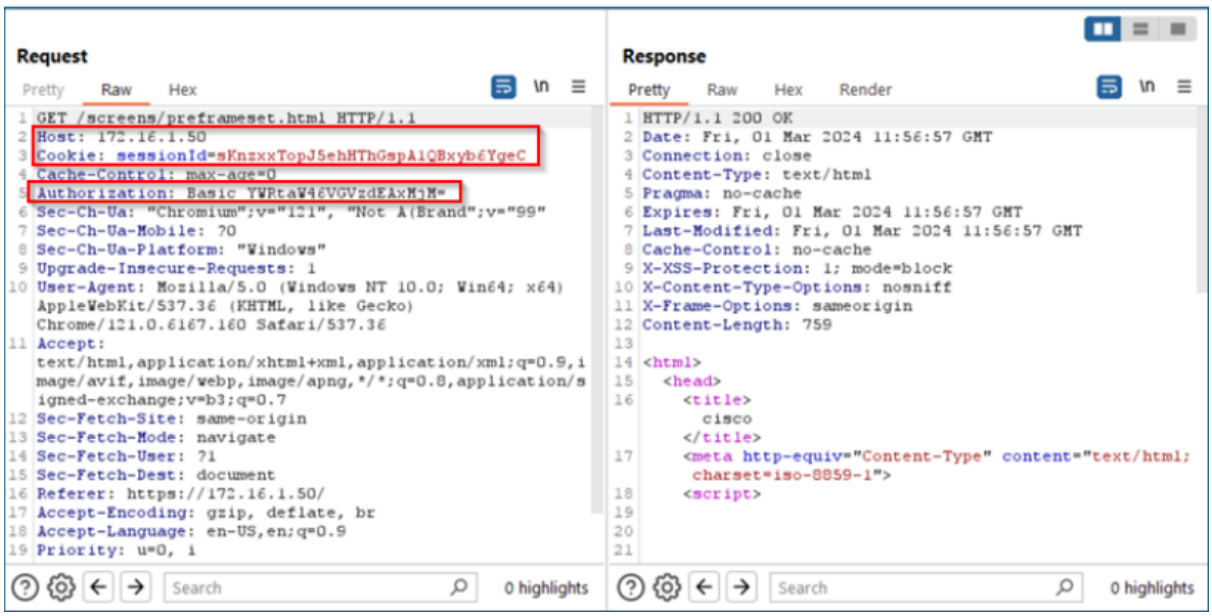
Step 3: Observe if the session ID's are regenerated for each new session.

3. To check if subsequent sessions are not reused or renewed:

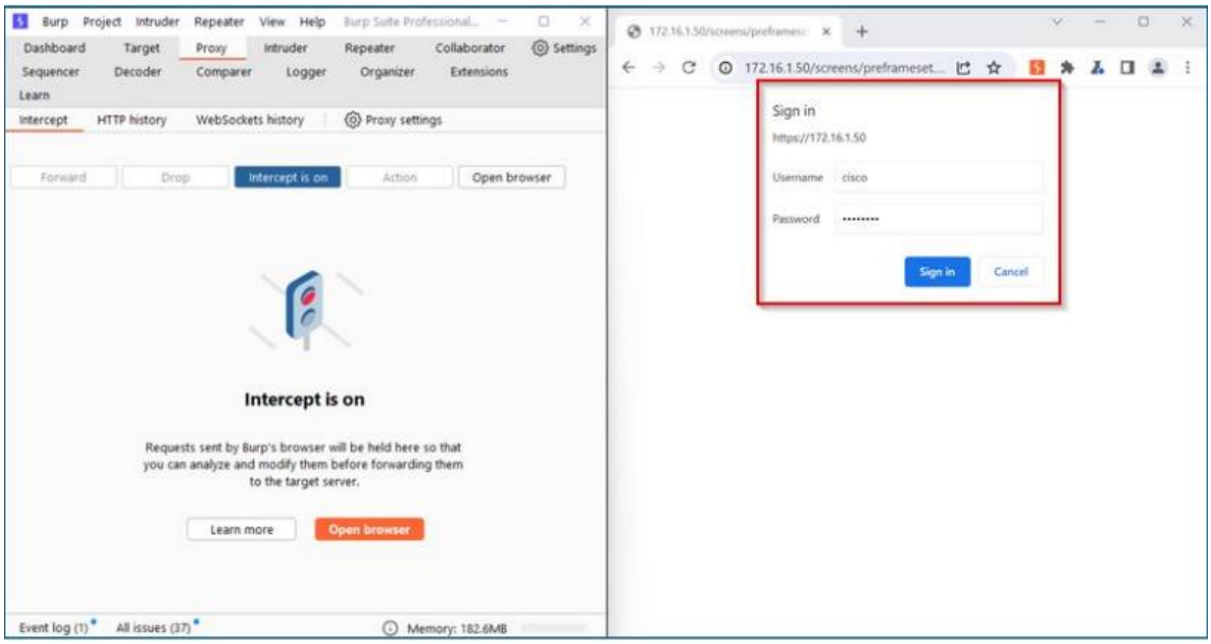
Step 1: Login with admin credentials over GUI intercept the request then send it to repeater and check for the sessionID.

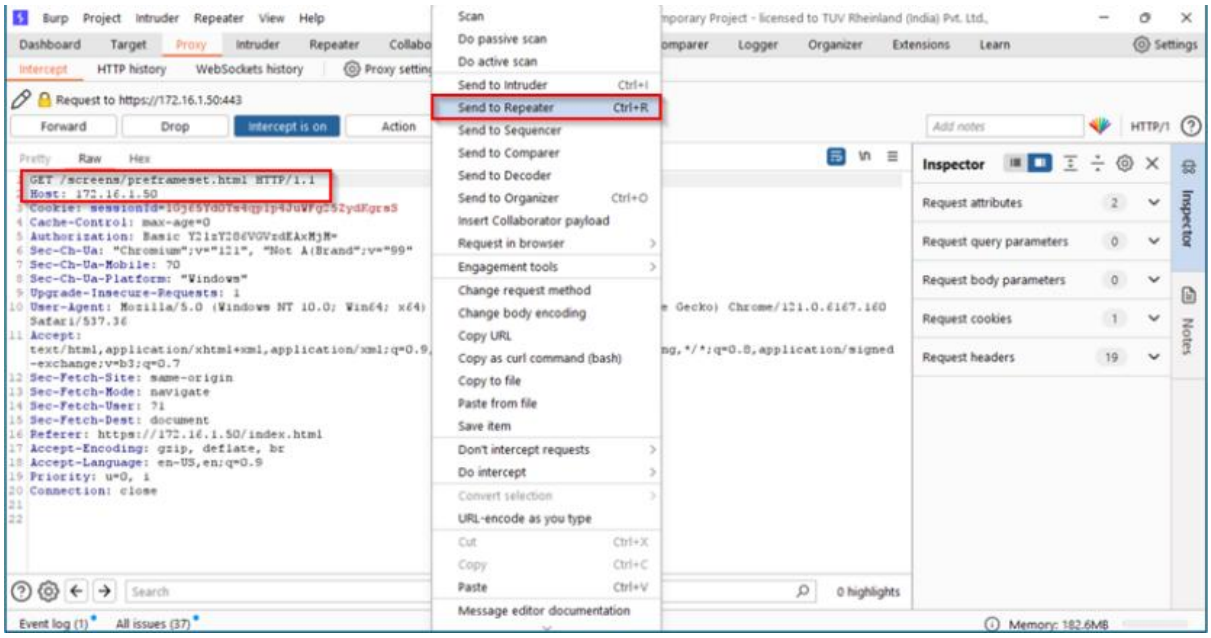


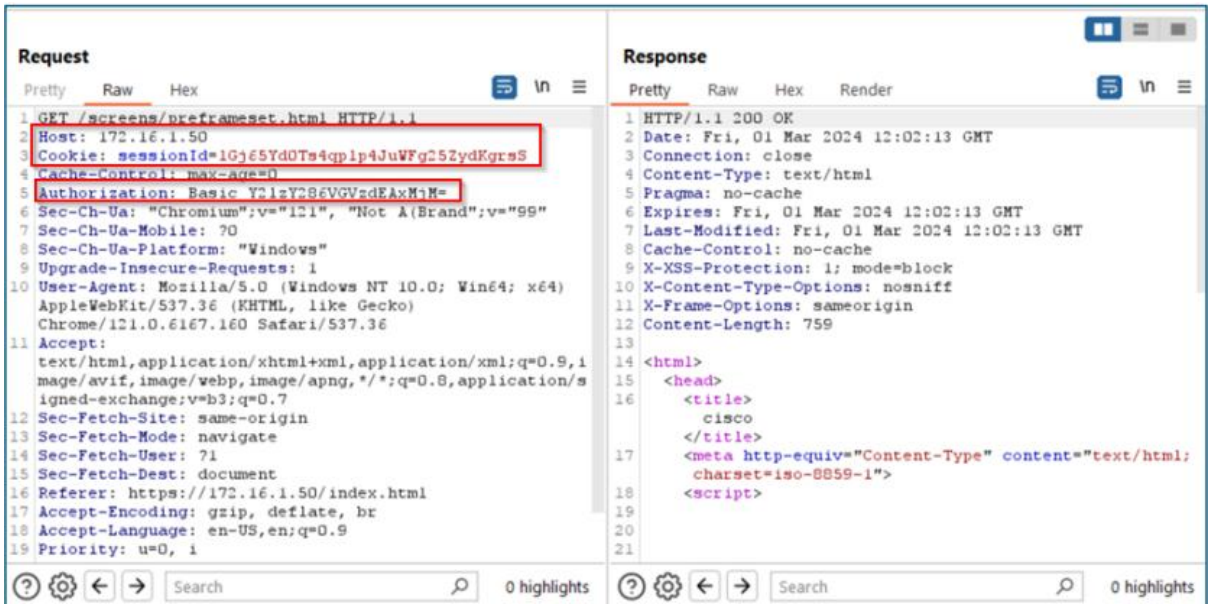




Step 2: Login with cisco credentials over GUI intercept the request then send it to repeater and check for the sessionID.


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Settings
Sequencer Decoder Comparer Logger Organizer Extensions
Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Intercept is on
Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.
Learn more
Open browser
Event log (1) All issues (37) Memory: 182.6MB
172.16.1.50/screens/preframeset...
Sign in
https://172.16.1.50
Username cisco
Password
Sign in
Cancel

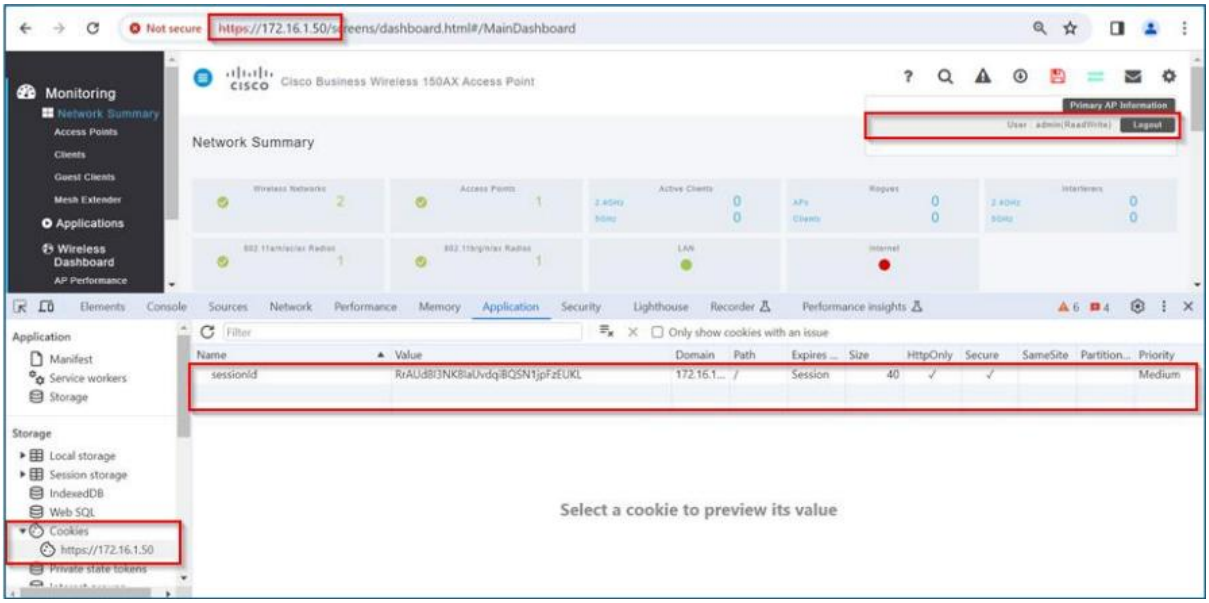

Request to https://172.16.1.50:443
Forward Drop Intercept is on Action
Pretty Raw Hex
GET /screens/preframeset.html HTTP/1.1
Host: 172.16.1.50
Scan
Do passive scan
Do active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Insert Collaborator payload
Request in browser
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command (bash)
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 1
Request headers 19
Notes
Event log (1) All issues (37) Memory: 182.6MB

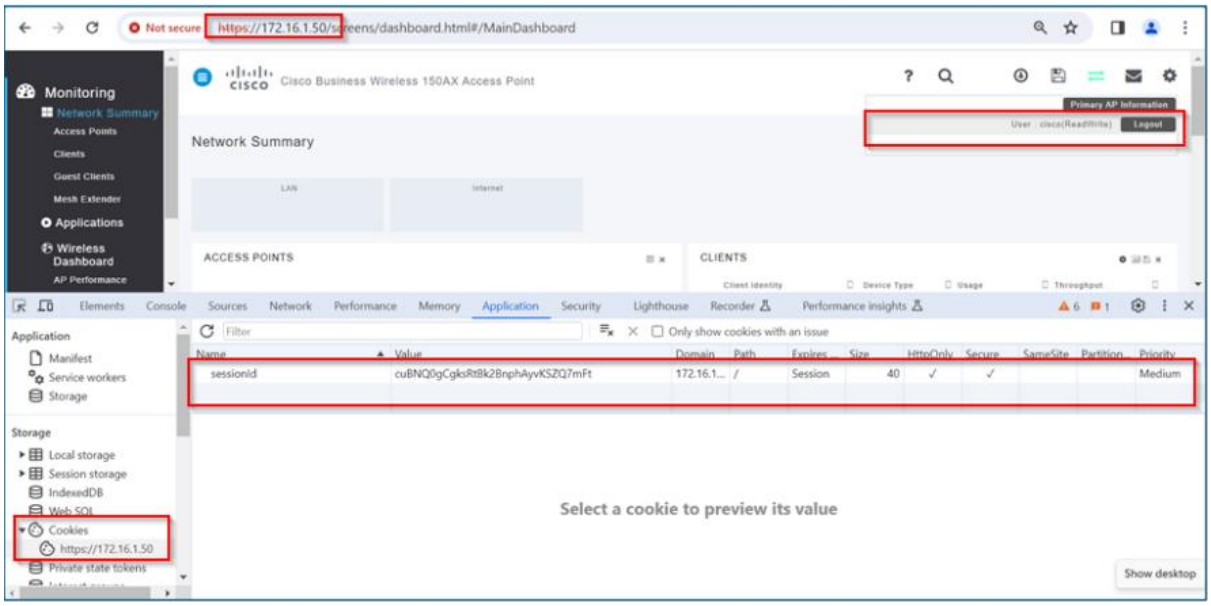


Step 3: Observe if the sessionID's are not reused or renewed

4. To check if CPE is not using persistent cookies to manage sessions but only session cookies

Step 1: Login over GUI with two different credentials and observe if the CPE is not using persistent cookies to manage sessions but only session cookies.





11.2.4 **Test Observations:**

- the session id is unpredictable.
- t was observed that the session ID's are regenerated for each new session
- it was observed that the session ID's are not reused or renewed
- it was observed that the CPE is not using persistent cookies to manage sessions but only session cookies

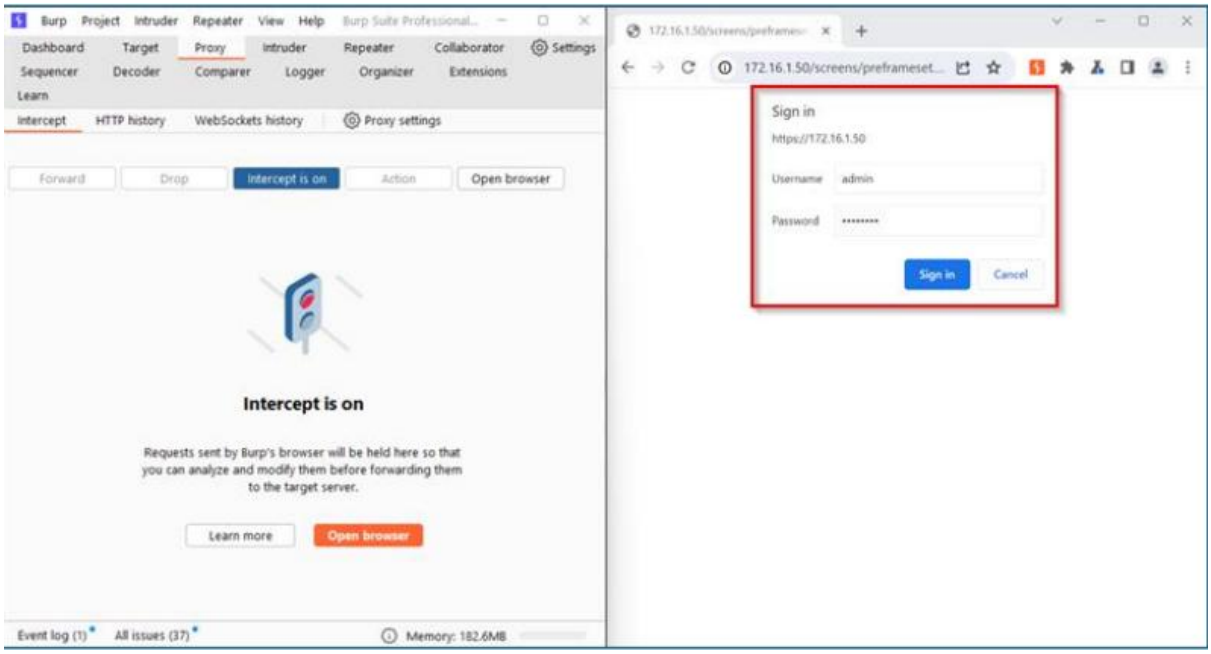
11.3 Test Case Number: 03

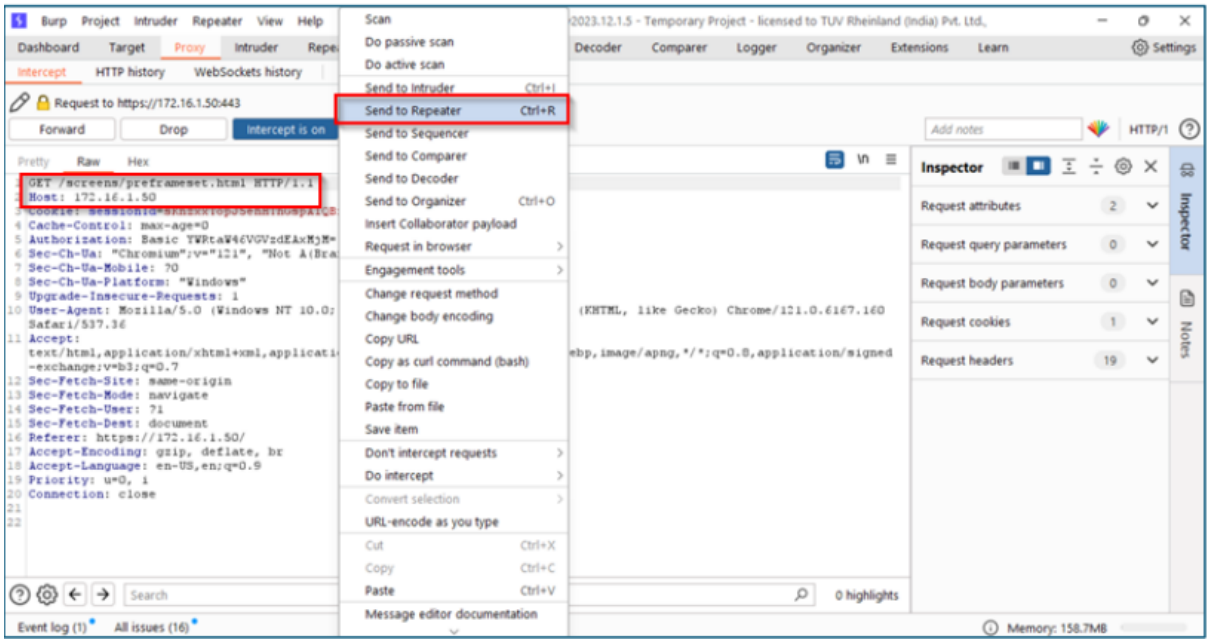
11.3.1 **Test Case Name:** TC_SESSIONID_ SENSITIVE_INFORMATION_TESTS

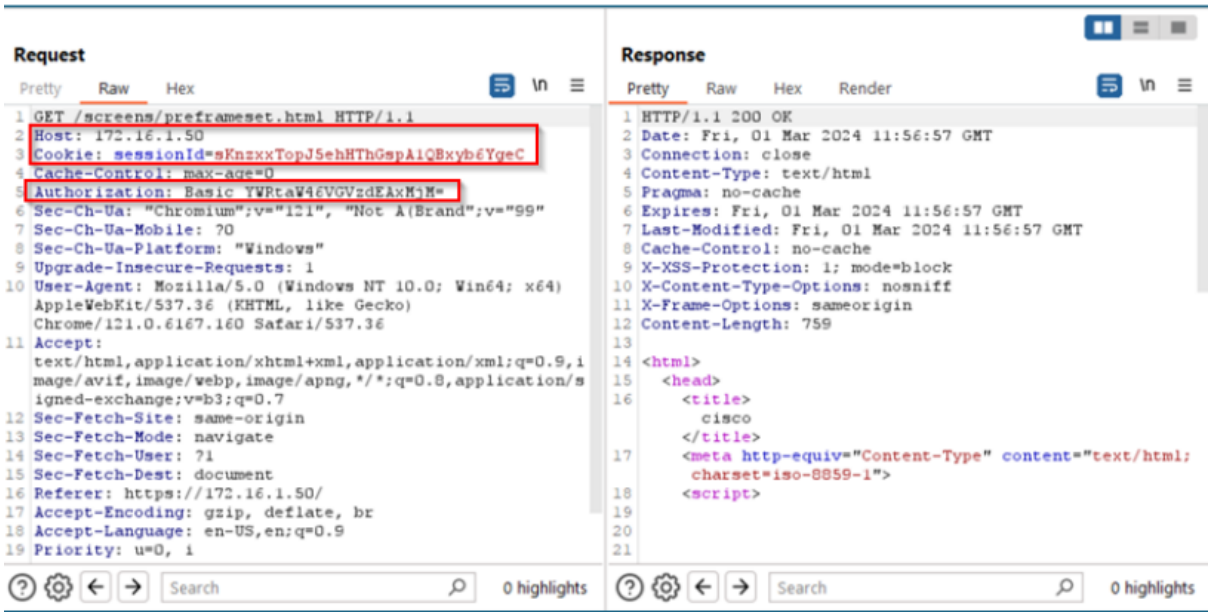
11.3.2 **Test Case Description:** Verify that the session ID is disclosing any sensitive information in clear text / regeneration for each new session.

11.3.3 **Execution Steps:**

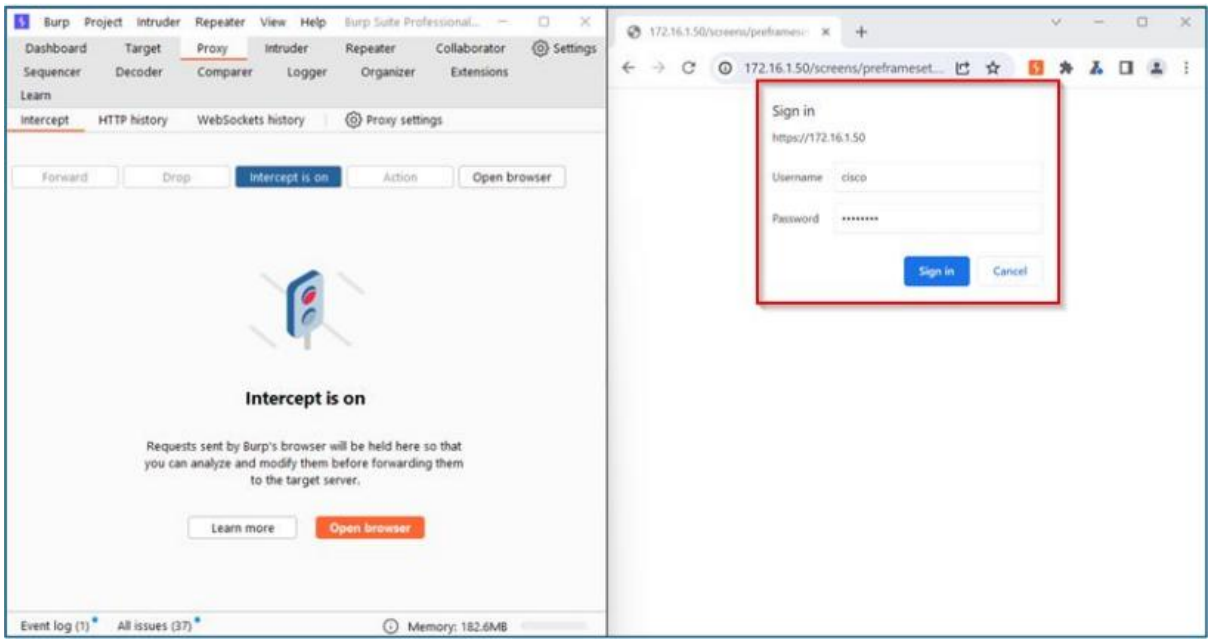
Step 1: Login with admin credentials over GUI, intercept the request then send it to repeater and check for the sessionI D.

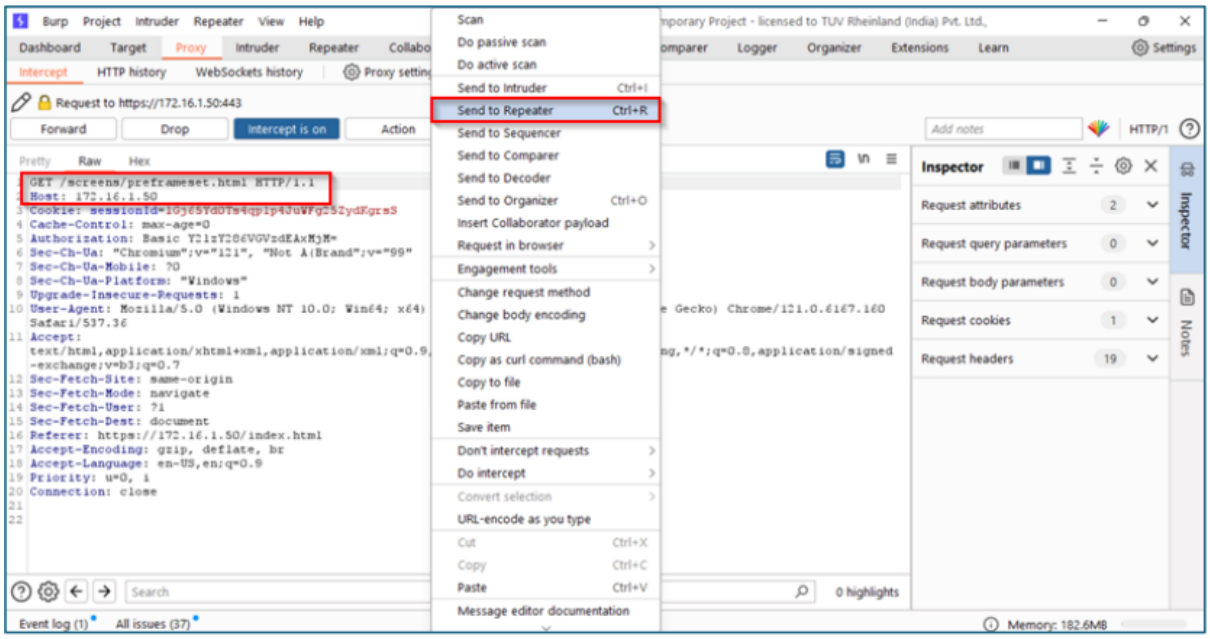

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Settings
Sequencer Decoder Comparer Logger Organizer Extensions
Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Intercept is on
Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.
Learn more Open browser
Event log (1) All issues (37) Memory: 182.6MB
172.16.1.50/screens/preframeset...
Sign in
https://172.16.1.50
Username admin
Password
Sign in Cancel

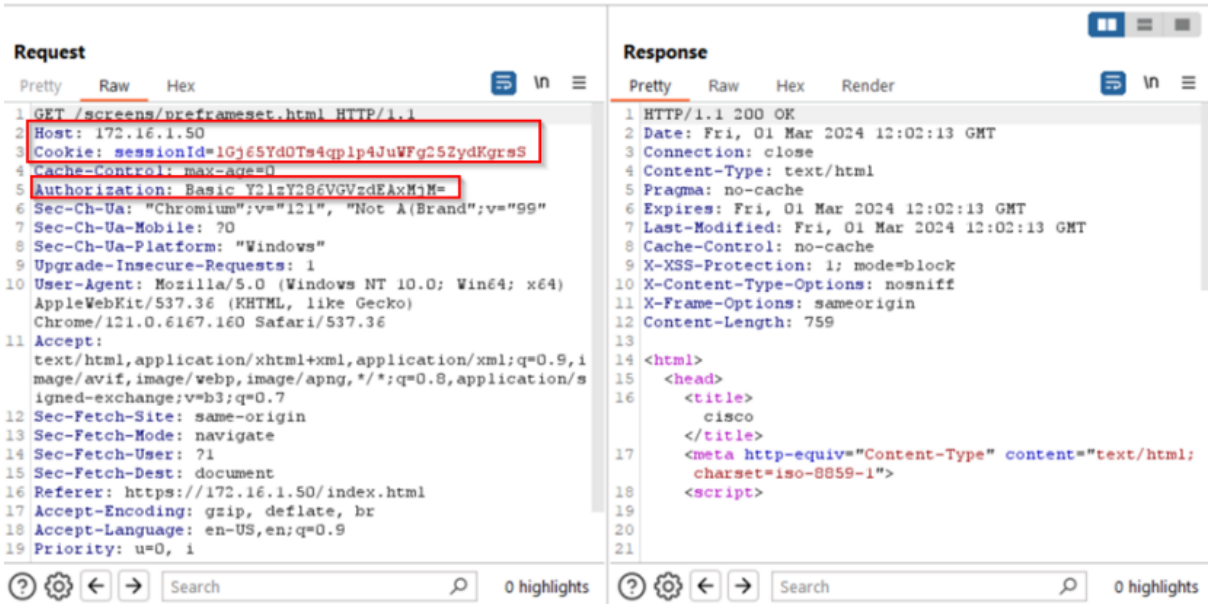

Request to https://172.16.1.50:443
Forward Drop Intercept is on
Pretty Raw Hex
GET /screens/preframeset.html HTTP/1.1
Host: 172.16.1.50
Scan
Do passive scan
Do active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Insert Collaborator payload
Request in browser
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command (bash)
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Event log (1) All issues (16) Memory: 158.7MB



Step 2: Login with cisco credentials over GUI intercept the request then send it to repeater and check for the sessionID.







11.3.4 **Test Observations:** During the testing process it has been observed that session ID's is not disclosing any sensitive information in clear text / regeneration for each new session.

11.4 Test Case Number: 04

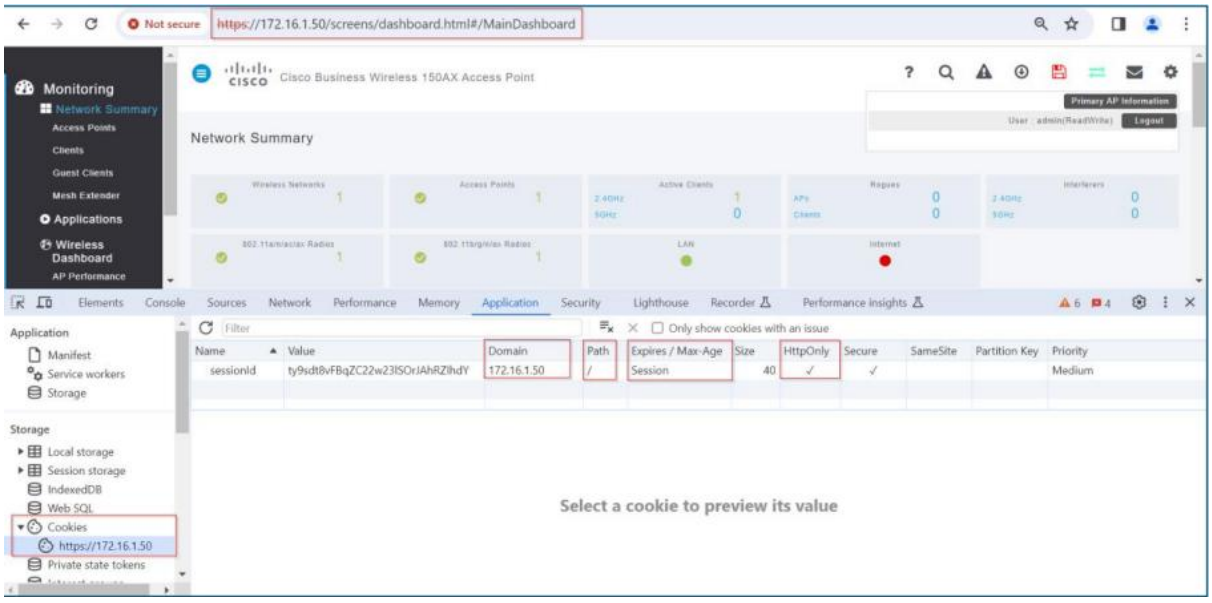
11.4.1 **Test Case Name:** TC_SESSIONID_COOKIE_ATTRIBUTE

11.4.2 **Test Case Description:** Verify that the cookie is set to "max-age", "HttpOnly", "domain" attribute, & "path" attribute.

11.4.3 **Execution Steps:**

Step 1: Open browser and navigate to https://172.16.1.40 and login with valid credentials.

Step 2: Press "f12" and navigate to cookie tab and observe that the cookie is properly set with "max-age", "HTTP Only", "domain" attribute, & "path" attribute.



11.4.4 **Test Observations:** During the testing process it has been observed that DUT is properly set the cookie with “max-age”, “HTTP Only”, “domain” attribute, & “path” attribute.

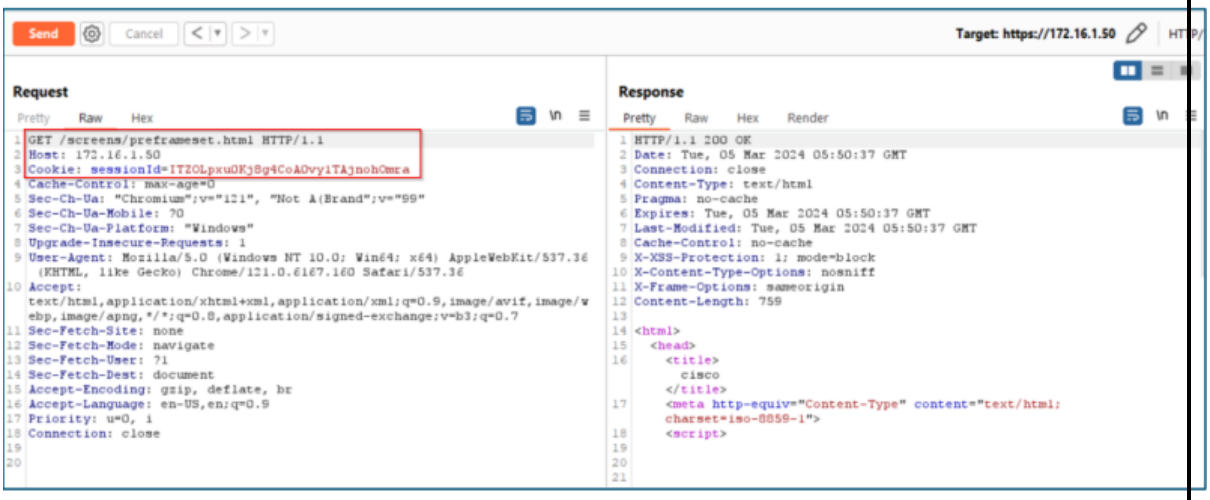
11.5 Test Case Number: 05

11.5.1 **Test Case Name:** TC_SESSIONID_ FROM_GET_POST

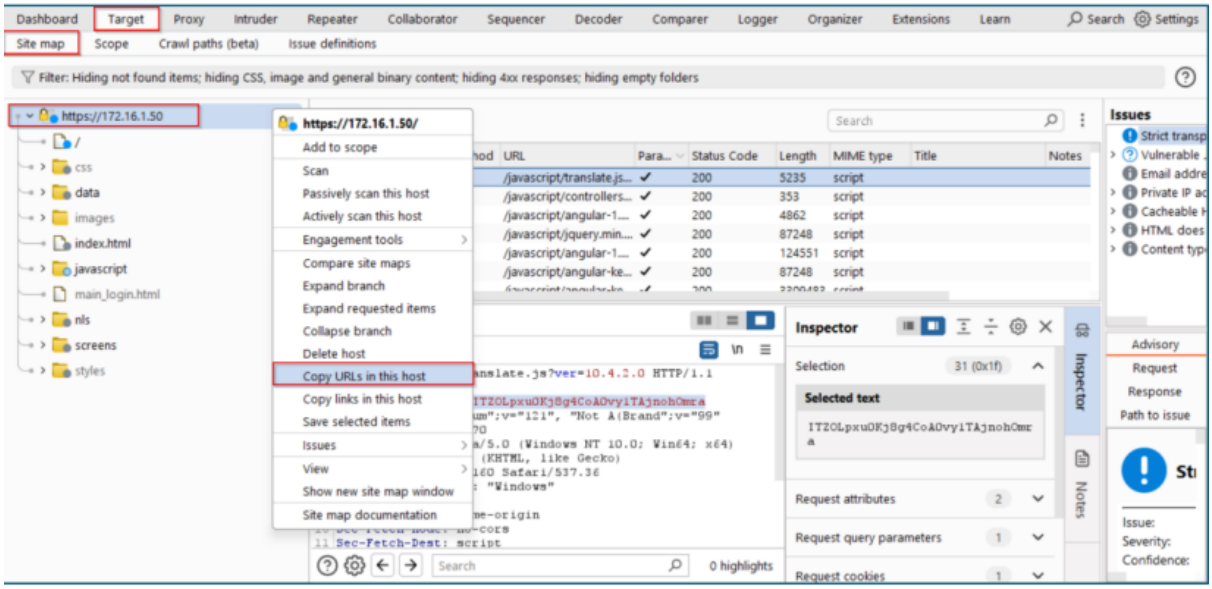
11.5.2 **Test Case Description:** Verify that the CPE is not accepting session identifiers from GET/POST variables.

11.5.3 **Execution Steps:**

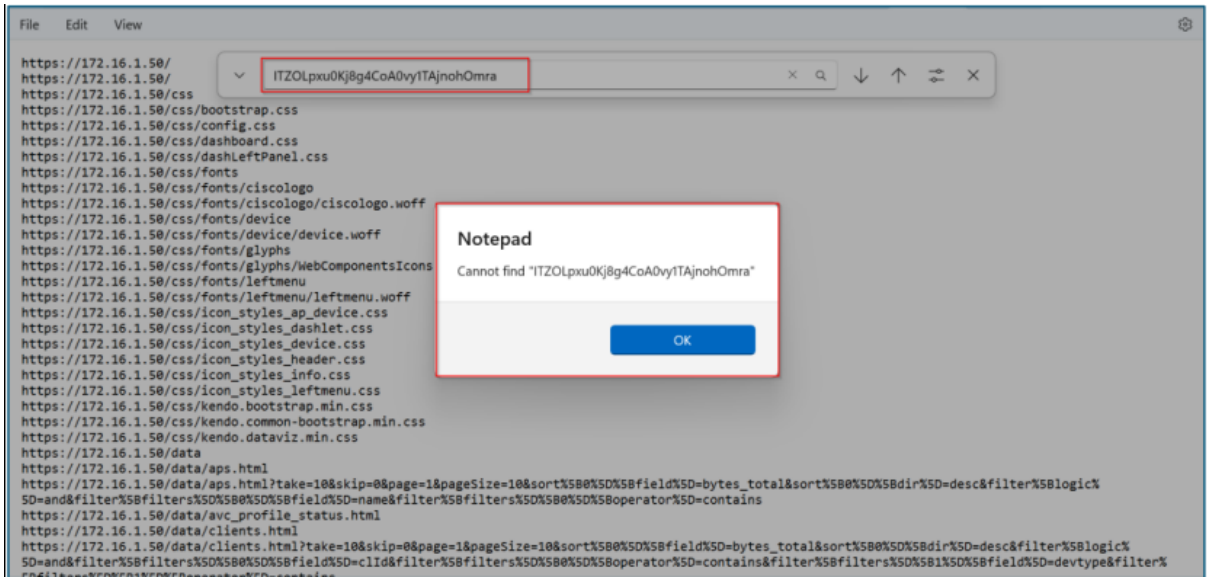
Step 1: Login over GUI and intercept the request and send it to repeater



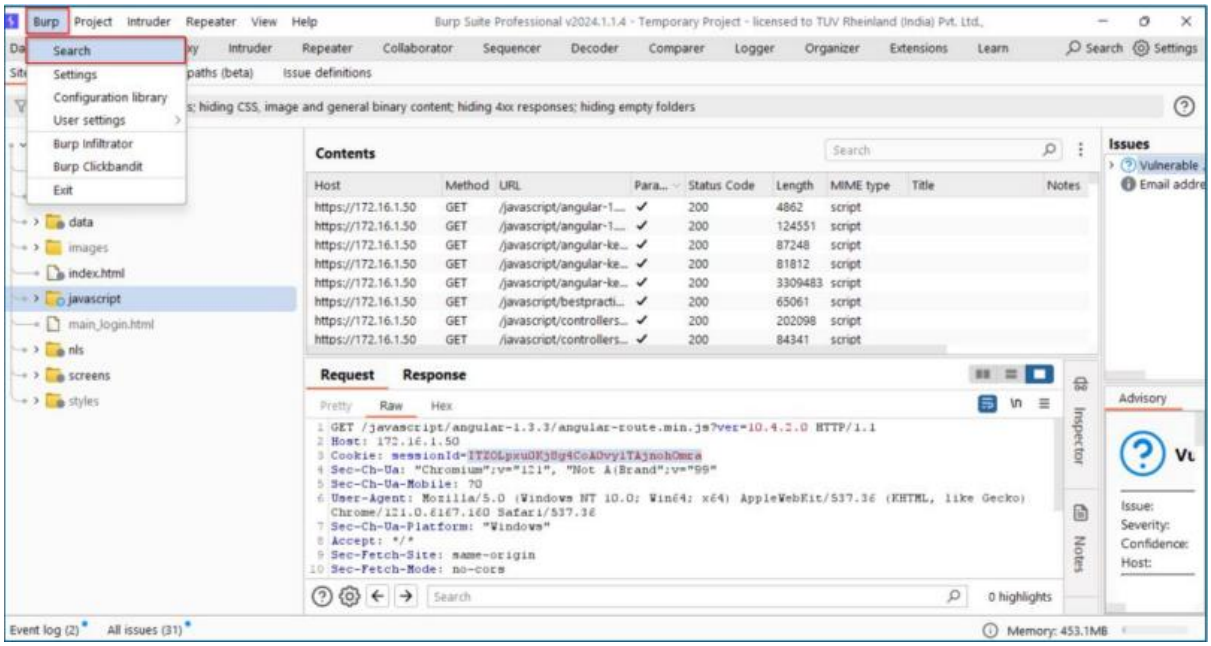
Step 2: Navigate to Target > Site map > https://172.16.1.50 > copy URL’s in this host



Step 3: Paste the URL's in a notepad and check for the session ID variables i.e. "ITZOLpxu0Kj8g4CoA0vy1TajnohOmra"

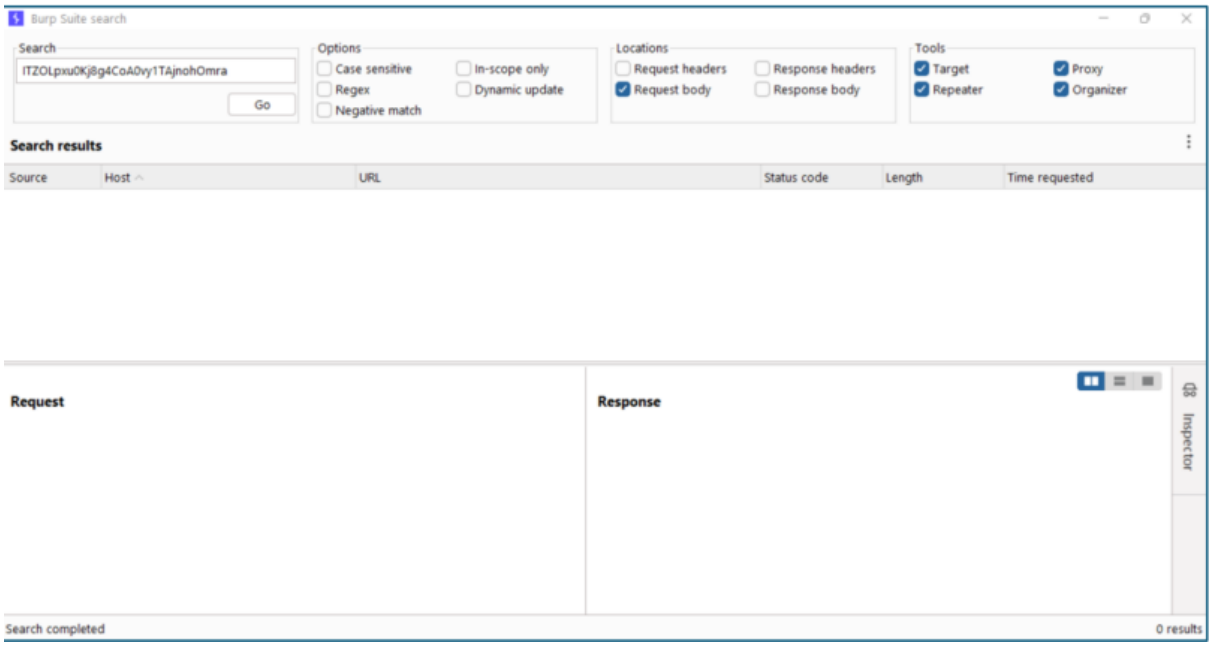


Step 5: To check if the CPE is not accepting session identifiers from POST variables navigate to burp > search and paste the session id.



step 6: Paste the session ID in search and select only request body as it only shows the POST content then click on go.

Step 7: Observe if any session Ids are generated that are getting accepted from the POST variable.



11.5.4 **Test Observations:** During the testing process it has been observed that the CPE is not accepting session identifiers from GET/POST variables.

11.6 Test Case Number: 06

11.6.1 **Test Case Name:** TC_ SERVER_GENERATED_SESSIONID_TESTS

11.6.2 **Test Case Description:** Verify that the CPE has been configured to only accept server-generated session IDs.

11.6.3 **Execution Steps:**

Step 1: Log in to the CPE's root level access.
Step 2: Check session management settings for server-generated session ID option.
Step 3: Initiate a session and verify the session ID originates from the server.
Step 4: Try accessing services with a non-server-generated session ID to ensure denial.
Step 5: Navigate pages or refresh application to confirm session ID consistency

11.6.4 **Test Observations:** OEM dependent

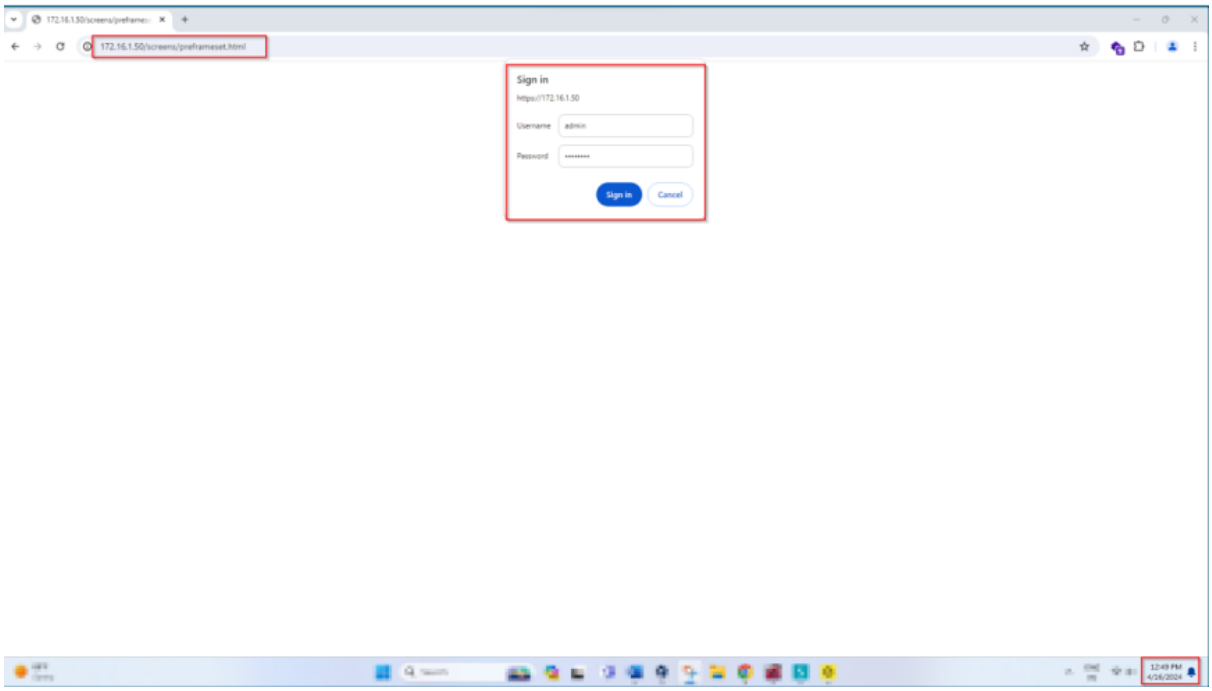
11.7 Test Case Number: 07

11.7.1 **Test Case Name:** TC_ SESSION_IDLE_TIMEOUT

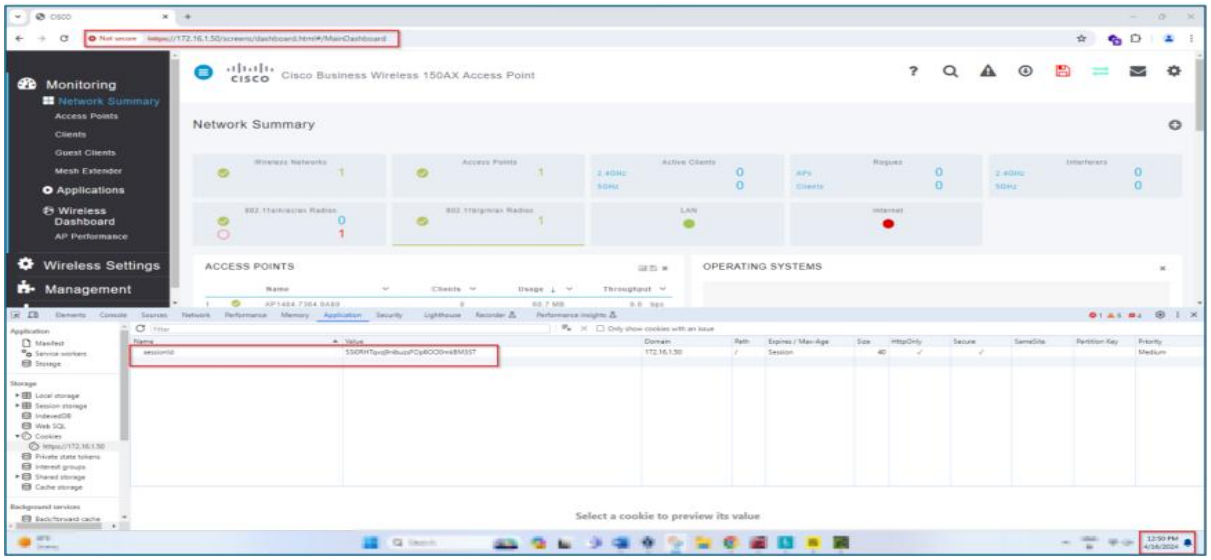
11.7.2 **Test Case Description:** Verify that the DUT regenerates session IDs for each new session and adheres to the defined session idle timeout period.

11.7.3 **Execution Steps:**

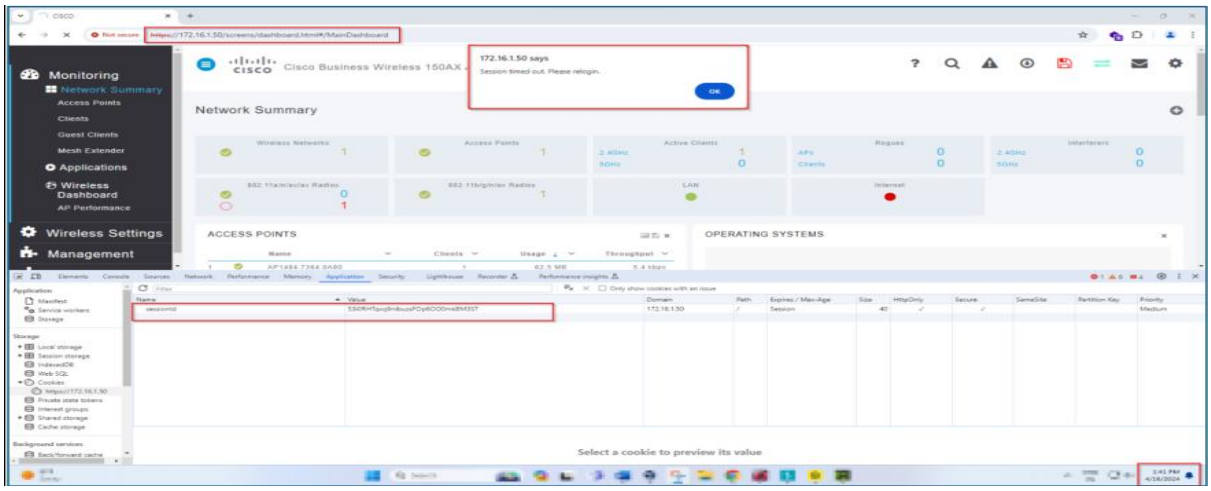
Step 1: Navigate to https://172.16.1.50 and provide the credentials to login.



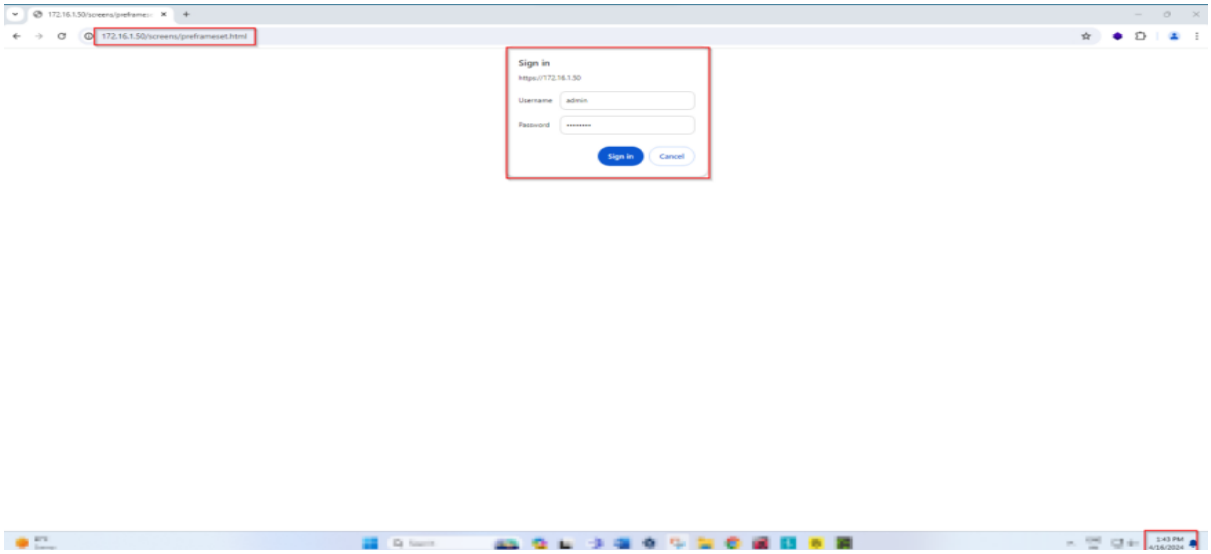
Step 2: Press “F12“ to observe the session ID generated and also note the time.



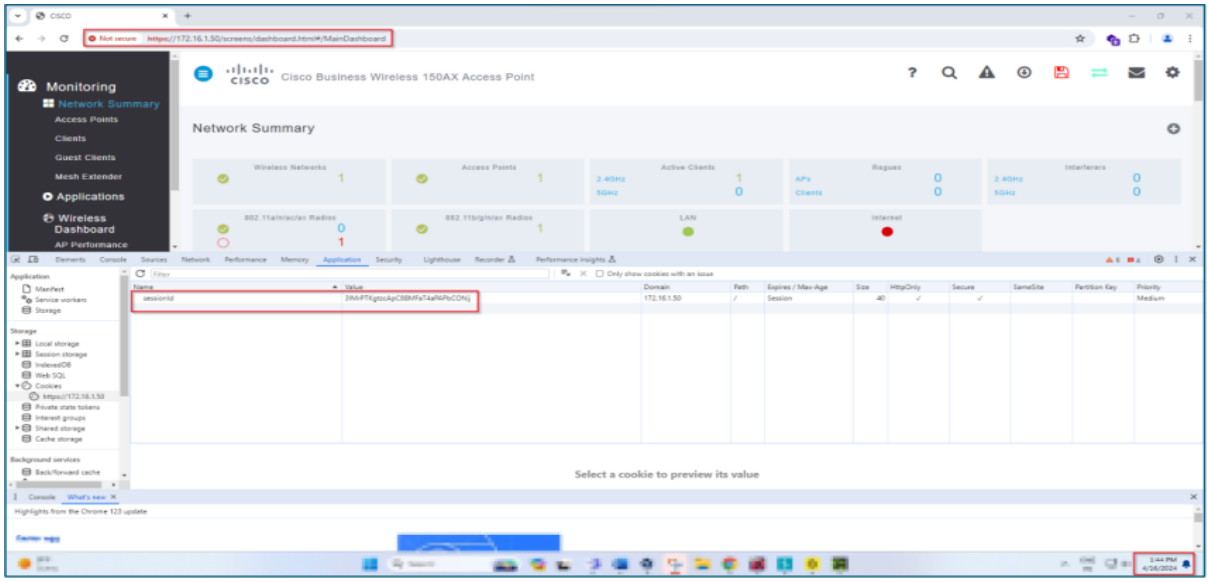
Step 3: Observe that the session gets terminated after being idle. Also observe the session ID during this time



Step 4: Navigate to https://172.16.1.50 and provide the same credentials as above to login.



Step 5: Press “F12“ to observe the session ID generated and also note the time.



11.7.4 **Test Observations:** During the testing process it has been observed that the session ID gets changed for the same user after keeping the session idle and then relogging with the same credentials

12. **<u>Test Case Result:</u>**

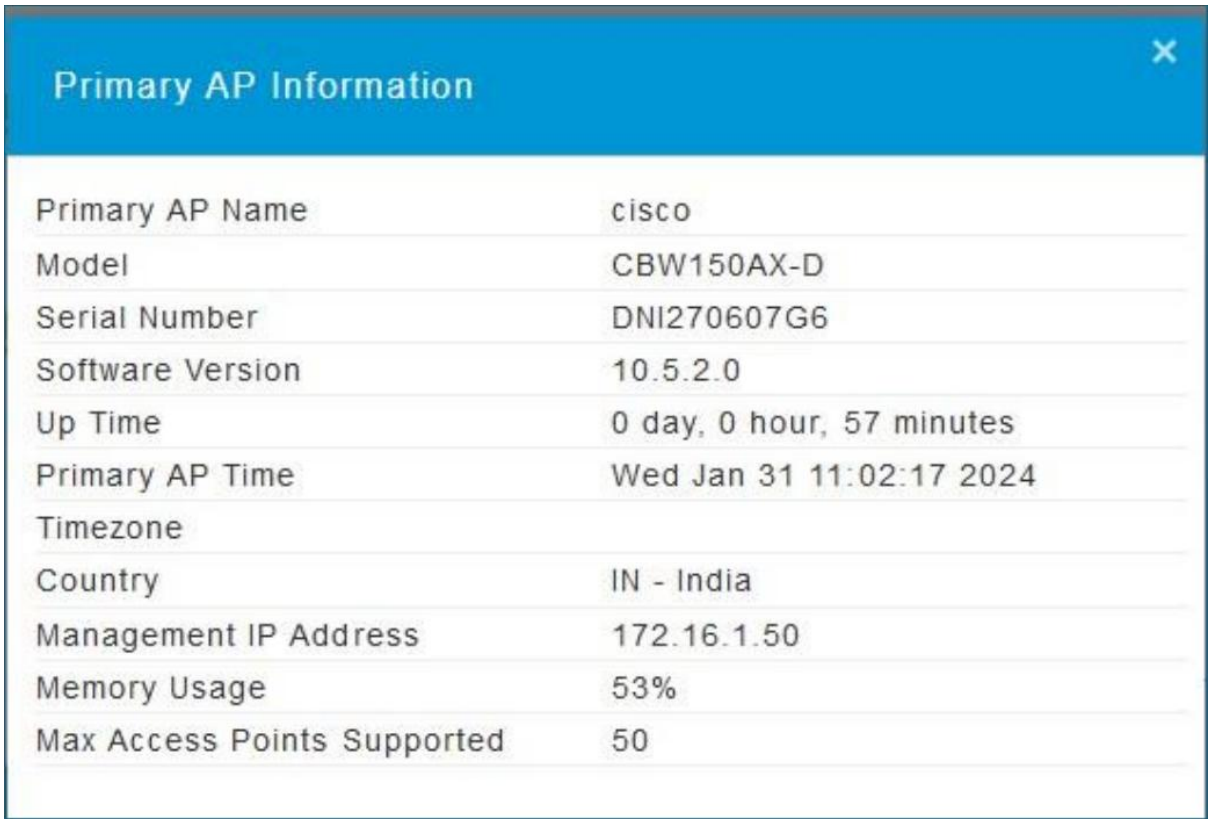
S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_SESSIONID_UNIQUE_TESTS	PASS	all the criteria have been met
2	TC_SESSIONID_VULNERABILITIES_TESTS	PASS	
3	TC_SESSIONID_ SENSITIVE_INFORMATION_TESTS	PASS	
4	TC_SESSIONID_COOKIE_ATTRIBUTE	PASS	
5	TC_SESSIONID_ FROM_GET_POST	PASS	
6	TC_ SERVER_GENERATED_SESSIONID_TESTS	OEM Dependent	
7	TC_ SESSION_IDLE_TIMEOUT	PASS	

1.11.4: HTTP input validation

<DUT Details: > WiFi CPE
<DUT Software Version:> cisco 10.5.2.0
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 11: Web Server
2. **<Security Requirement No & Name >** 1.11.4: HTTP input validation
3. **<Requirement Description: >** The CPE shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks. The CPE shall validate, filter, escape, and encode user-controllable input before it is placed in output that is used as a web page that is served to other users.
4. **DUT Confirmation Details**:

Screenshot below shows the DUT name (Primary AP Name) , Model number, Serial Number, Software Version.



DUT Configuration Checksum:

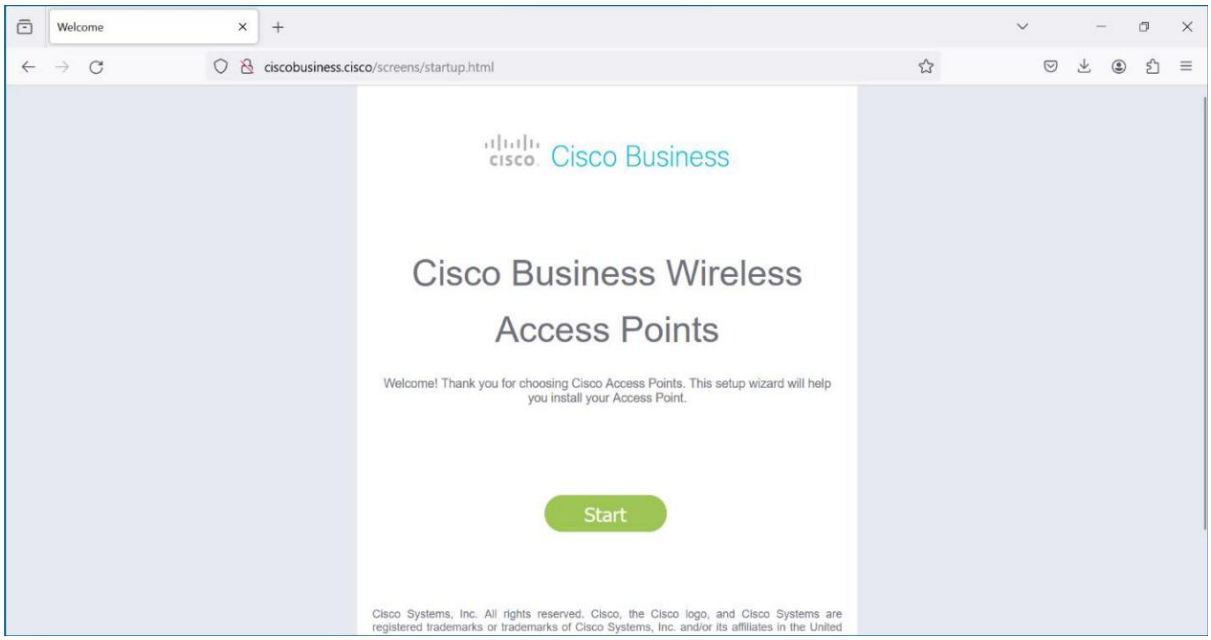
```
PS C:\> certutil -hashfile '.\Configuration files\Configuration 1.txt' SHA256
SHA256 hash of .\Configuration files\Configuration 1.txt:
fab585d185d316ad6c45b1d414d8bf55fa8ef0094173fe9a8a5fa2d3ddc2e43b
CertUtil: -hashfile command completed successfully.
```

5. **DUT Configuration:**

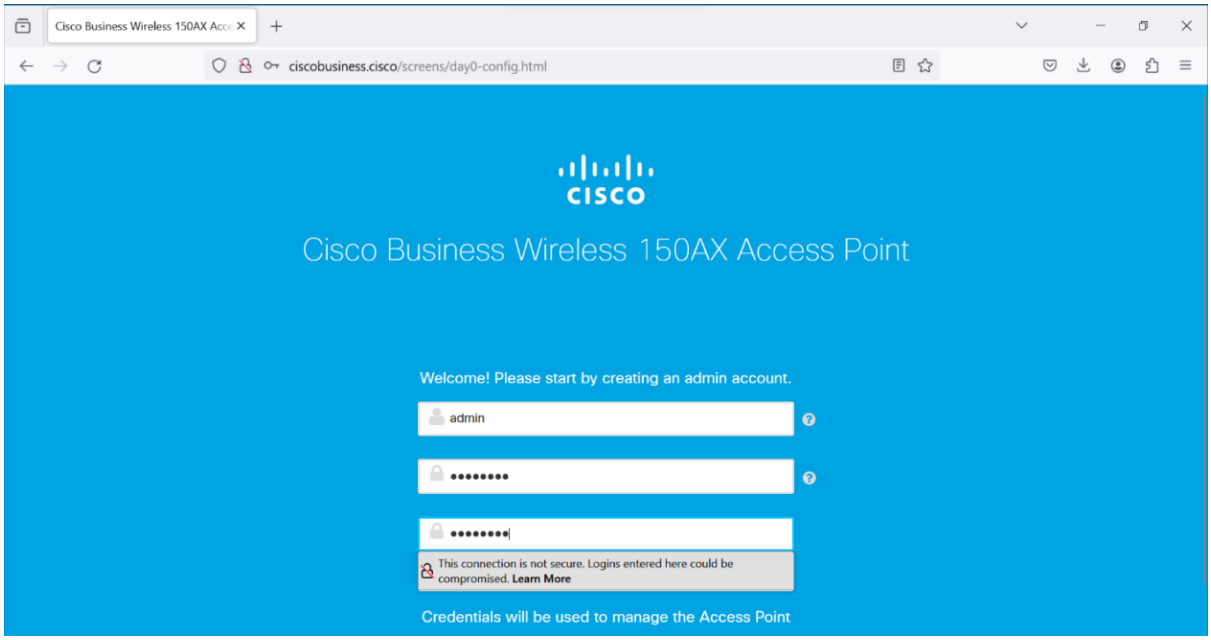
Initial Basic Configuration of CPE

Step 1: Power on the CPE and wait for the CPE to be visible on the Laptop Wi-Fi Scanning "Cisco Business-Setup" or Reset the CPE if not Visible

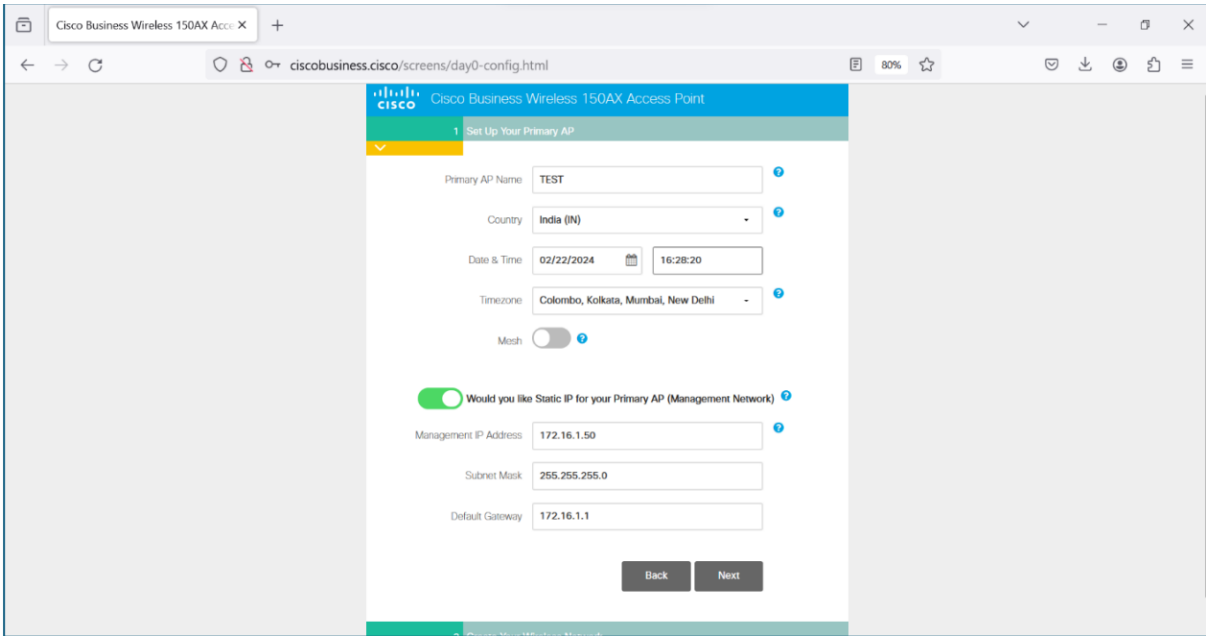
Step 2: Connect To the Wi-Fi Access Point using password " Cisco123" And Navigate to http://ciscobusiness.cisco/screens/startup.html and Click Start as Show in the below Screenshot.



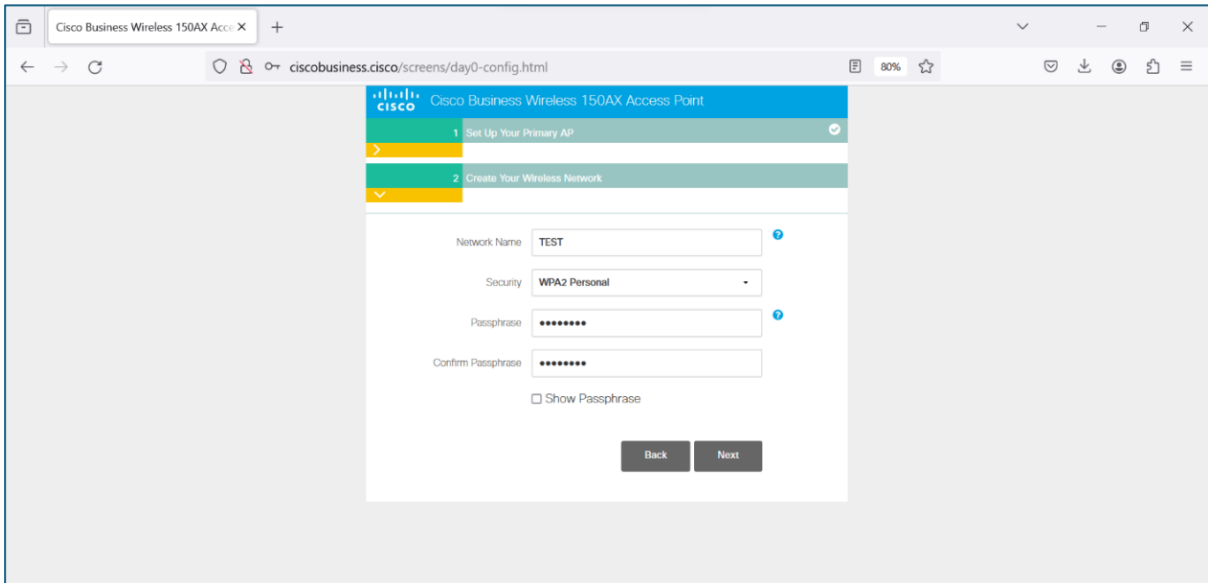
Step 3 : Enter the Desire Credentials for admin account creation and click start



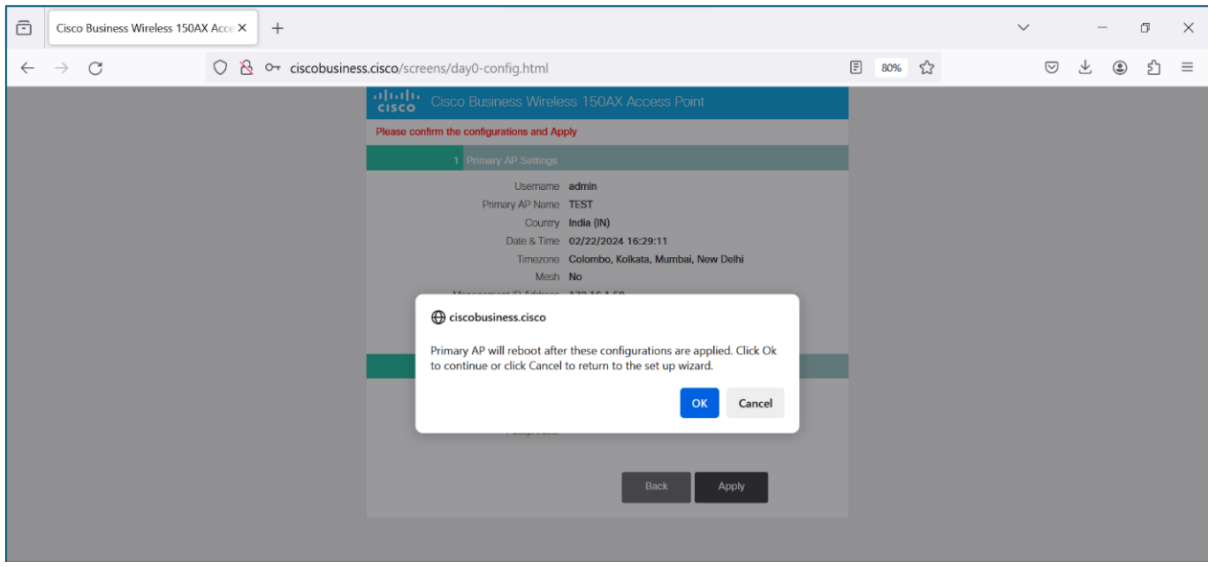
Step 4 : Enter the Desire AP Name and Select Static IP Configuration if required and click Next



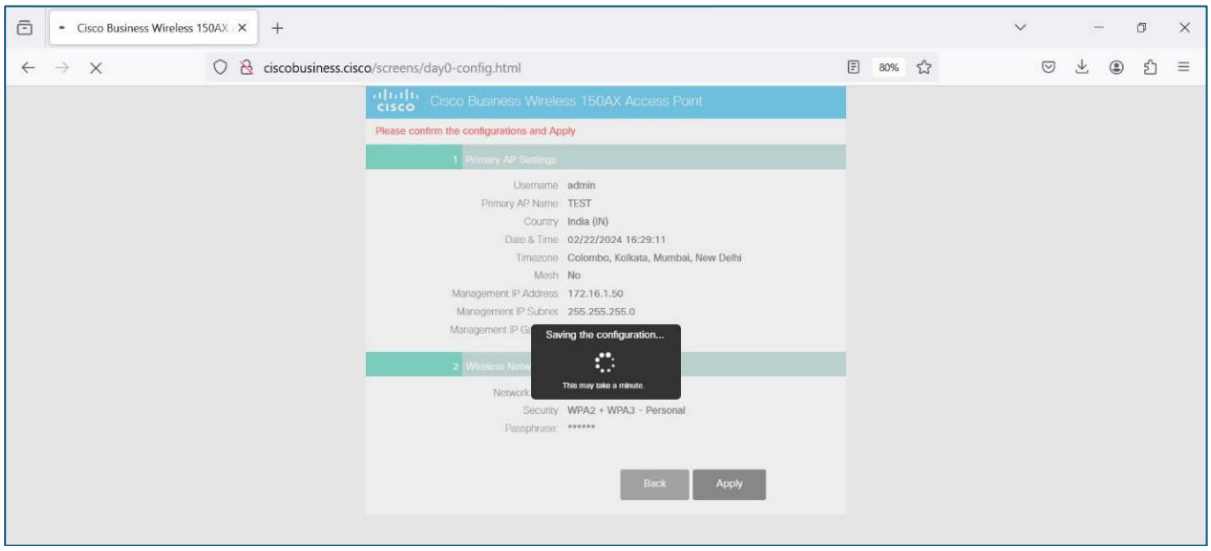
Step 5 : Enter the Desire Network Name and Passphrase and click Next

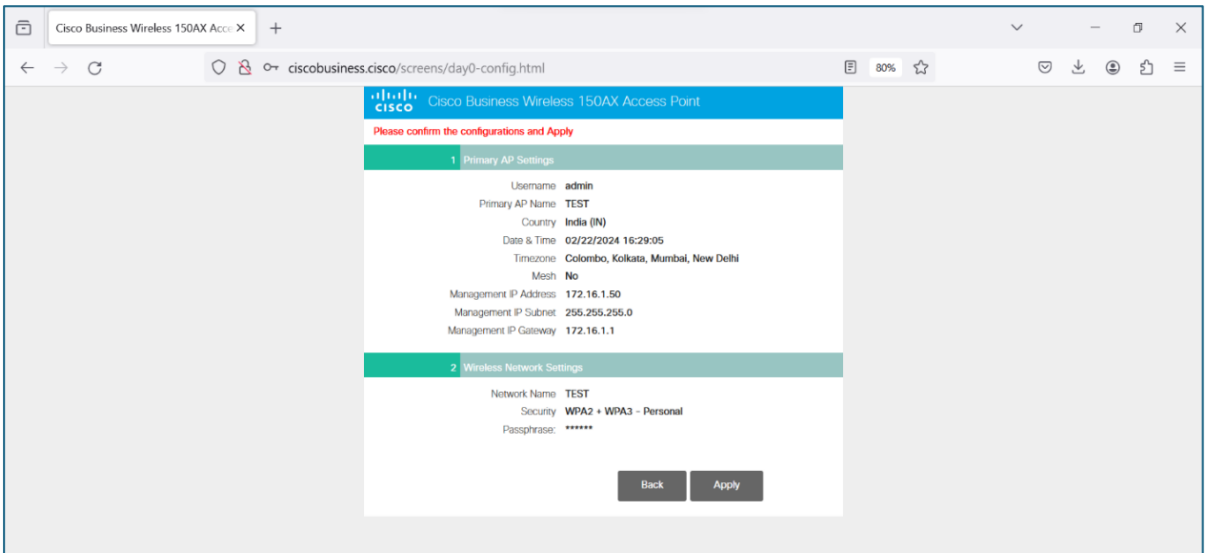


Step 6 : Verify the Configuration done and Click on Apply



Step 7 : A popup will appear on the screen “Primary AP will reboot after these configurations are applied. Click Ok to continue or click Cancel to return to the set-up wizard.”





Step 8: Finished Step Now the AP is Ready to Be used.

6. **Preconditions**
   - Enable https on DUT
   - The Vendor must provide a Certificate stating that the Web Application is tested and free from command injection or cross-site scripting attacks.
   - Network Product documentation which contains information on log file location and procedure to access it.
   - Tester has the necessary privileges to access the log files.
   - HTTPS access to DUT.
   - The tester should have a list of payloads to perform this attack.
   - Test environment with a Web Browser.
   - Knowledge about XSS and Command Injection attacks.
7. **Test Objective**: The DUT shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks

8. **Test Plan:**

8.1 Number of Test Scenarios:

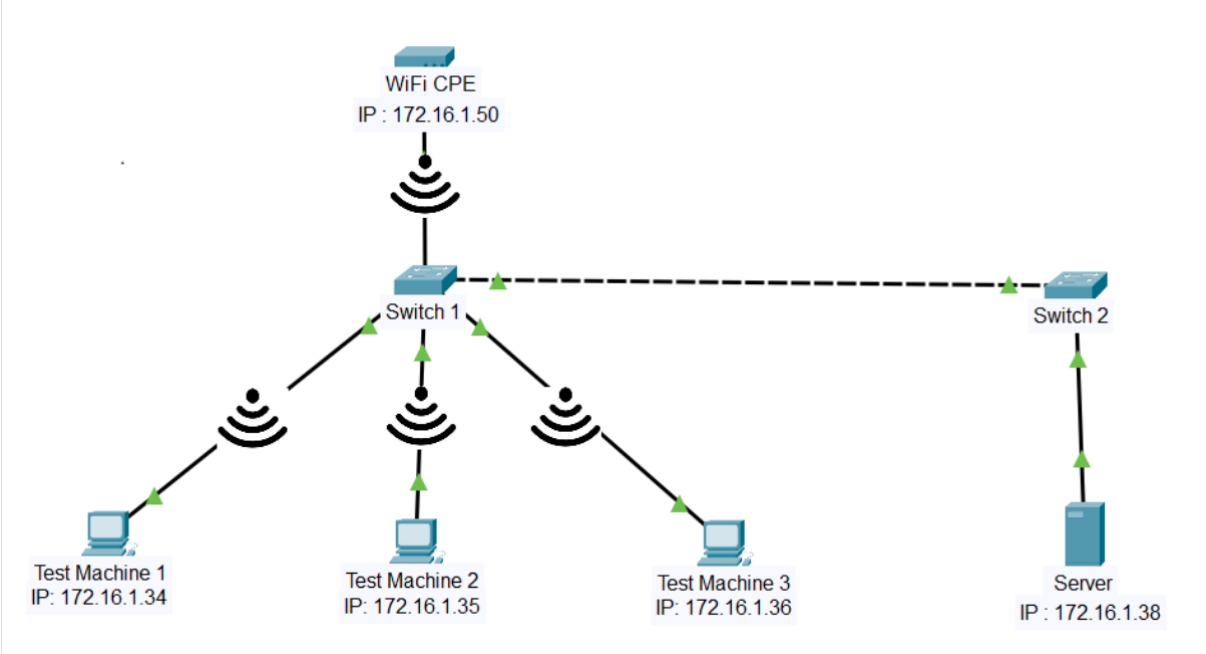
8.1.1. Test Scenarios for XSS attack

- Manual check via Cheat Sheet
- Automated check via tool

8.1.2. Test Scenarios for Command Injection attack

- Manual check via Cheat Sheet
- Automated check via tool

8.2 Test Bed Diagram



8.3 Tools Required

- Default DUT configuration tool for Web Server as per vendor. It can be command line, GUI or any other interface as specified in vendor documentation.
- Browser
- Burp Suite Professional v2023.9.3
- XSStrike (https://github.com/s0md3v/XSStrike)
- Commix (https://github.com/commixproject/commix)

8.4 Test Execution Steps

- Power up the testbed
- The tester manually tries to find the inputs/ entry points in the Web Application (such as search bar, username & password field, URL, etc.)
- Perform manual test on inputs/ entry points for XSS and Command Injection vulnerability based on cheat sheets.

– The tester using automated tools like Burp suite, XSStrike and Commix to find XSS and Command Injection vulnerability.

9. **Expected Results for Pass:** The Web Application must be free from XSS and Command Injection vulnerability.

10. **Expected Format of Evidence:** Testing report contains copies of the log file showing the captured information.

11. **Test Execution:**

11.1 Test Case Number: 01

11.1.1 **Test Case Name:** TC_XSS_TESTING

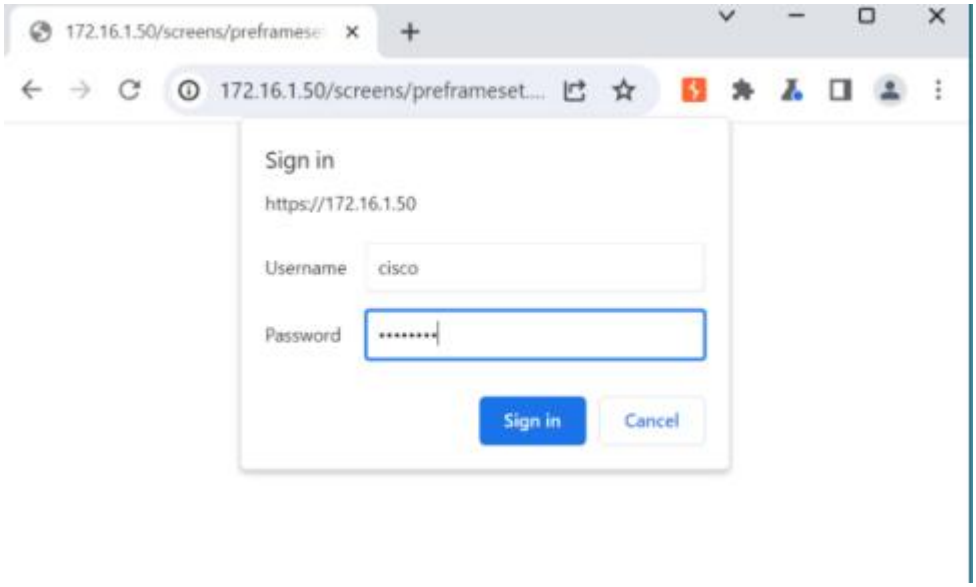
11.1.2 **Test Case Description:** Verify that all the input in the WEB Application is free from XSS attack.

- Manual approach
- Automated approach

11.1.3 **Execution Steps:**

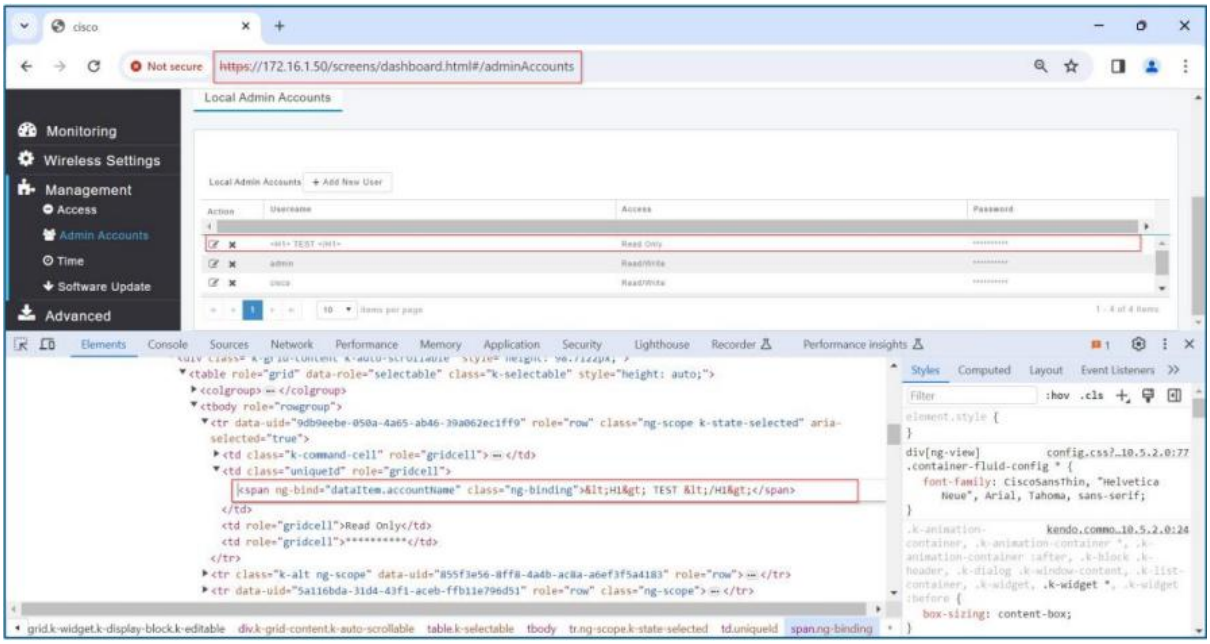
Step 1 : The tester shall open any Web Browser (Mozilla Firefox, Google Chrome) and go to the web address/IP of the DUT.

- URL: http://<IP address of DUT>



Step2: Find all the input in the WEB Application/Page

Step 3: Login to the account and navigate to management -> admin account -> Add new user.



Step 4:

1. Manual Approach

- Use the below cheat sheet for XSS and try it in the input and observe the behaviour.

- (https://gist.githubusercontent.com/kurobeats/9a613c9ab68914312cbb415134795b45/raw/c24dd91dd91c324ae5c28b124aa4d379dbcb8e59/xss_vectors.txt)

```
%253Cscript%253Ealert('XSS')%253C%252Fscript%253E
<IMG SRC=x onload="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onafterprint="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onbeforeprint="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onbeforeunload="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onerror="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onhashchange="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onload="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmessage="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ononline="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onoffline="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onpagehide="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onpageshow="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onpopstate="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onresize="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onstorage="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onunload="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onblur="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onchange="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x oncontextmenu="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x oninput="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x oninvalid="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onreset="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onsearch="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onselect="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onsubmit="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onkeydown="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onkeypress="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onkeyup="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onclick="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondblclick="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmousedown="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmousemove="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmouseout="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmouseover="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmouseup="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmousewheel="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onwheel="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondrag="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondragend="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondragenter="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondragleave="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondragover="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondragstart="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondrop="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onscroll="alert(String.fromCharCode(88,83,83))">
```

Note: Use any Proxy tool (Burp suite) to bypass the client-side validation and test server-side input validation and intruder to inject the above payload

1. Automated Approach.
    - Command used: ***xsstrike –crawl –u <URL of WEB Application>***

```
┌─[ashwini@ashwini-newslab]─[~/XSStrike]
└──╼ $ python3 xsstrike.py --crawl -u http://172.18.0.8/

        XSStrike v3.1.5

[~] Crawling the target
 !] Progress: 1/1

┌─[ashwini@ashwini-newslab]─[~/XSStrike]
└──╼ $
```

(Here we can see the tool has not detected any vulnerable object)

```
┌─[ashwini@ashwini-newslab]─[~/XSStrike]
└──╼ $ python3 xsstrike.py --crawl -u http://172.18.0.8/

        XSStrike v3.1.5

[~] Crawling the target
[+] Potentially vulnerable objects found at http://172.18.0.8/
------------------------------------------------------------
6   output.innerHTML = input.value;
------------------------------------------------------------
 !] Progress: 1/1
```

(**Here we can see the tool has detected a vulnerable object this must be manually checked and if found vulnerable the test case will fail**)

11.1.4 **Test Observations:** It should be ensured that any input on the WEB Application should not be vulnerable to XSS attacks.

11.2 **Test Case Number:** 02

11.2.1 **Test Case Name:** TC_CI_TESTING

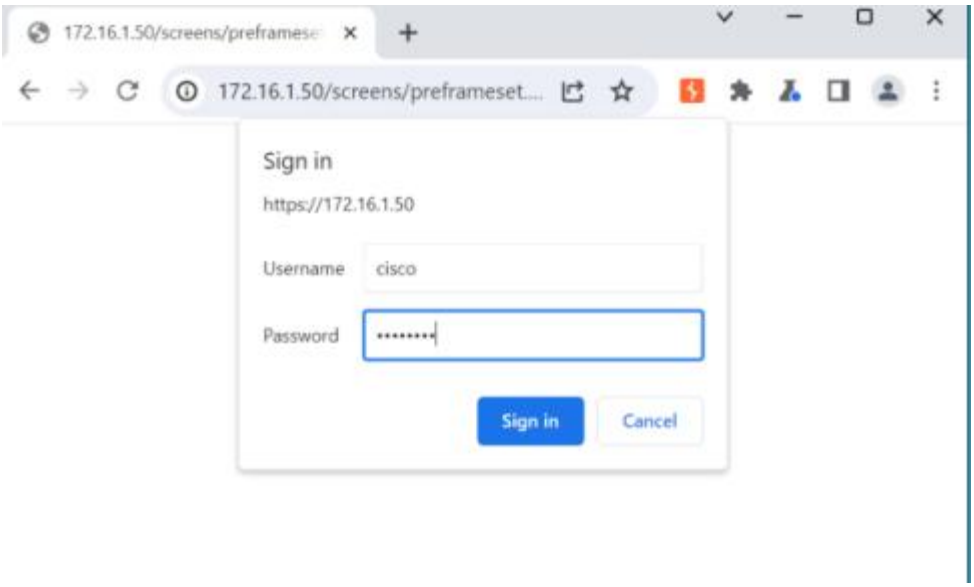
11.2.2 **Test Case Description:** Verify that all the input in the WEB Application is free from Command Injection attack.

- Manual approach
- Automated approach

11.2.3 **Execution Steps:**

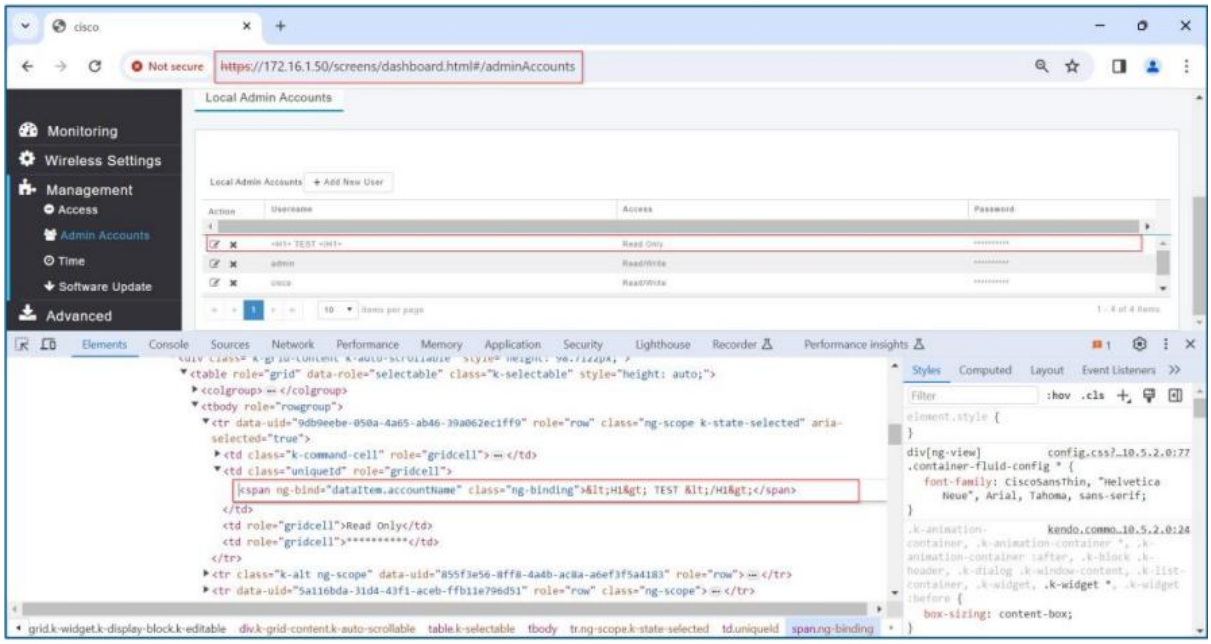
Step 1 : The tester shall open any Web Browser (Mozilla Firefox, Google Chrome) and go to the web address/IP of the DUT.

- URL: http://<IP address of DUT>



Step2: Find all the input in the WEB Application/Page

Step 3: Login to the account and navigate to management -> admin account -> Add new user.



Step 4:

1. Manual Approach

- Use the below cheat sheet for Command Injection and try it in the input and observe the behaviour.
- (https://hackersonlineclub.com/command-injection-cheatsheet/)

```
&lt;!--#exec%20cmd=&quot;/bin/cat%20/etc/passwd&quot;--&gt;
&lt;!--#exec%20cmd=&quot;/bin/cat%20/etc/shadow&quot;--&gt;
&lt;!--#exec%20cmd=&quot;/usr/bin/id;--&gt;
&lt;!--#exec%20cmd=&quot;/usr/bin/id;--&gt;
/index.html|id|
;id;
;id
;netstat -a;
;id;
|id
|/usr/bin/id
|id|
|/usr/bin/id|
||/usr/bin/id|
|id;
||/usr/bin/id;
;id|
;|/usr/bin/id|
\n/bin/ls -al\n
\n/usr/bin/id\n
\nid\n
\n/usr/bin/id;
\nid;
\n/usr/bin/id|
\nid|
;/usr/bin/id\n
;id\n
|usr/bin/id\n
|nid\n
```

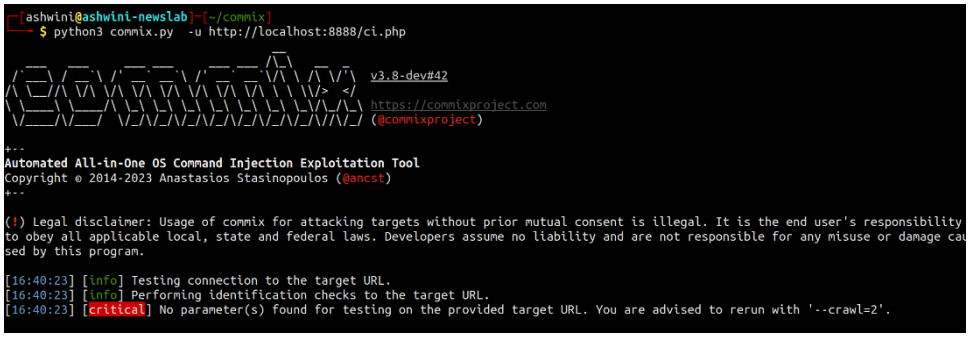
Note: Use any Proxy tool (Burp suite) to bypass the client-side validation and test server-side input validation and intruder to inject the above payload

(A snapshot of few Command Injection payloads)

a. Use any Proxy tool (Burp suite) to bypass the client-side validation and test server-side input validation

- Automated Approach.

- Command used: ***<Read the utility documentation to get information about the usage>***



(Here we can see the tool has not detected any vulnerable object)

(**Here we can see the tool has detected a vulnerable object this must be manually checked and if found vulnerable the test case will fail**)

11.2.4 **Test Observations:** It should be ensured that any input on the WEB Application should not be vulnerable to Command Injection attacks.

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_XSS_TESTING	PASS	all the criteria have been met
2	TC_CI_TESTING	PASS	

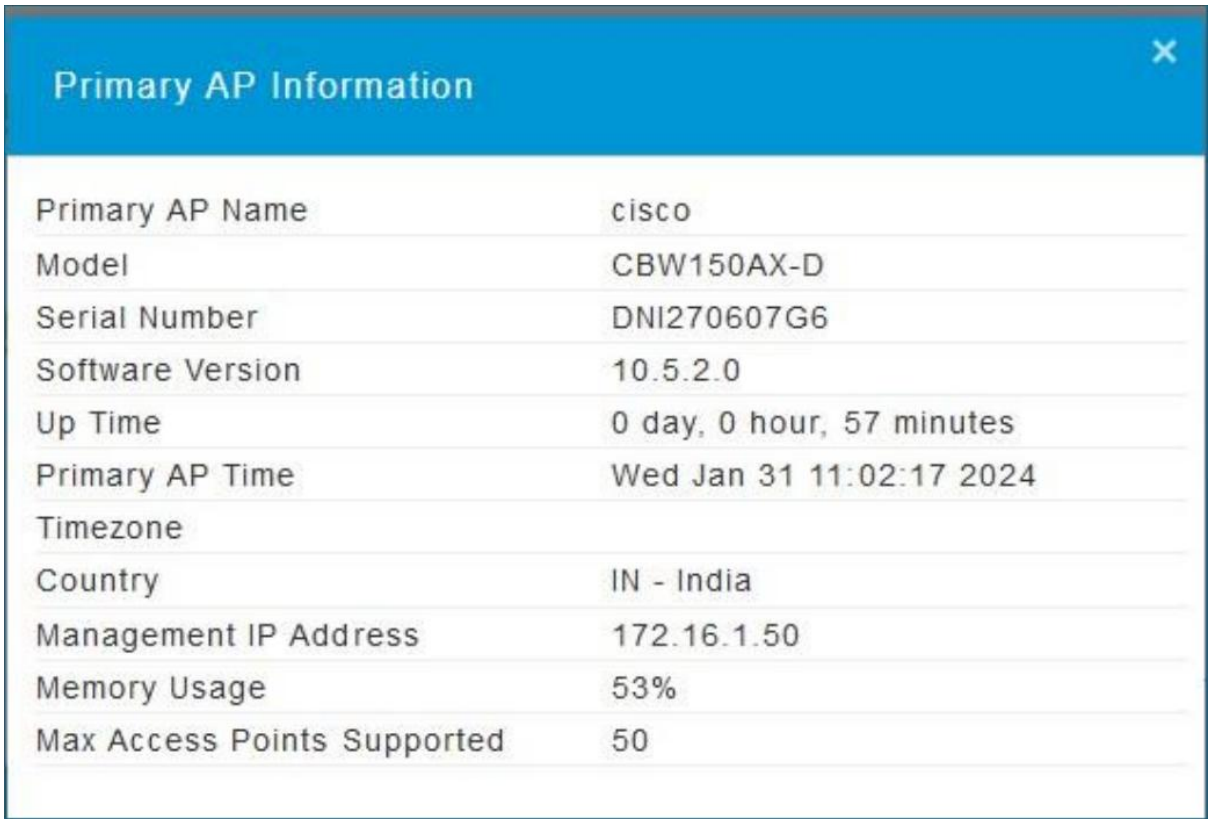
1.11.5: No unused HTTP methods

<DUT Details: > WiFi CPE
<DUT Software Version:> cisco 10.5.2.0
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 11: Web Server
2. **<Security Requirement No & Name >** 1.11.5 No unused HTTP methods
3. **<Requirement Description: >** HTTP methods that are not required shall be deactivated. Standard requests to web servers only use GET, HEAD, and POST. If other methods are required, they shall not introduce security leaks such as TRACK or TRACE.

4. **DUT Confirmation Details**:

Screenshot below shows the DUT name (Primary AP Name), Model number, Serial Number, Software Version.



DUT Configuration Checksum:

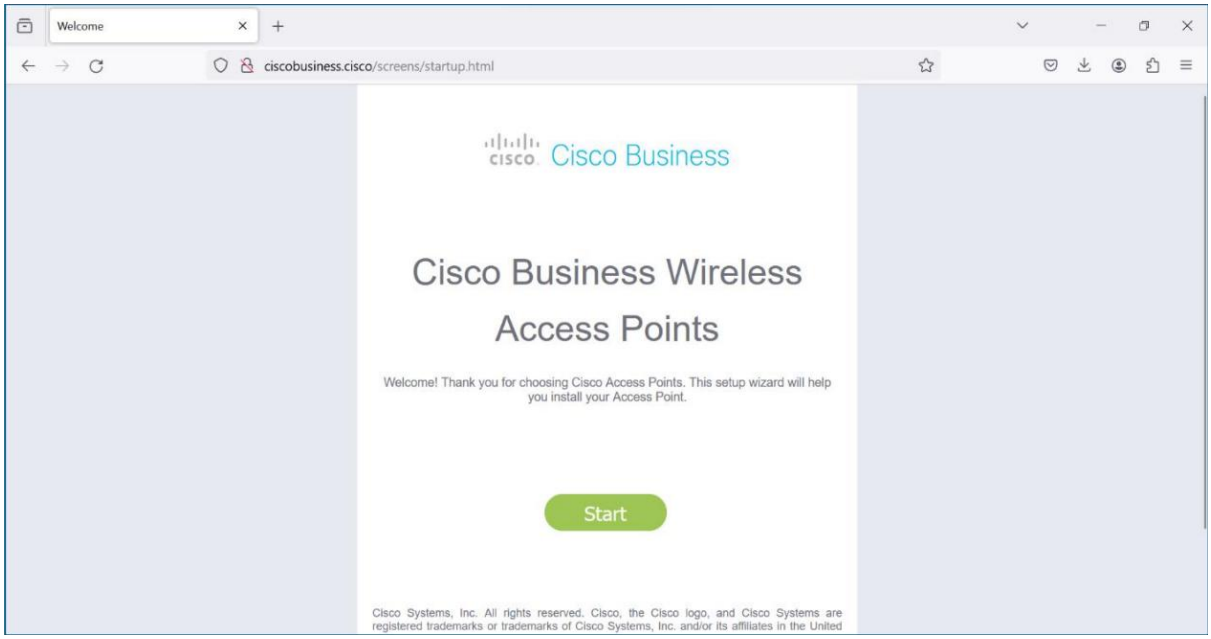
```
PS C:\> certutil -hashfile '.\Configuration files\Configuration 1.txt' SHA256
SHA256 hash of .\Configuration files\Configuration 1.txt:
fab585d185d316ad6c45b1d414d8bf55fa8ef0094173fe9a8a5fa2d3ddc2e43b
CertUtil: -hashfile command completed successfully.
```

5. **DUT Configuration:**

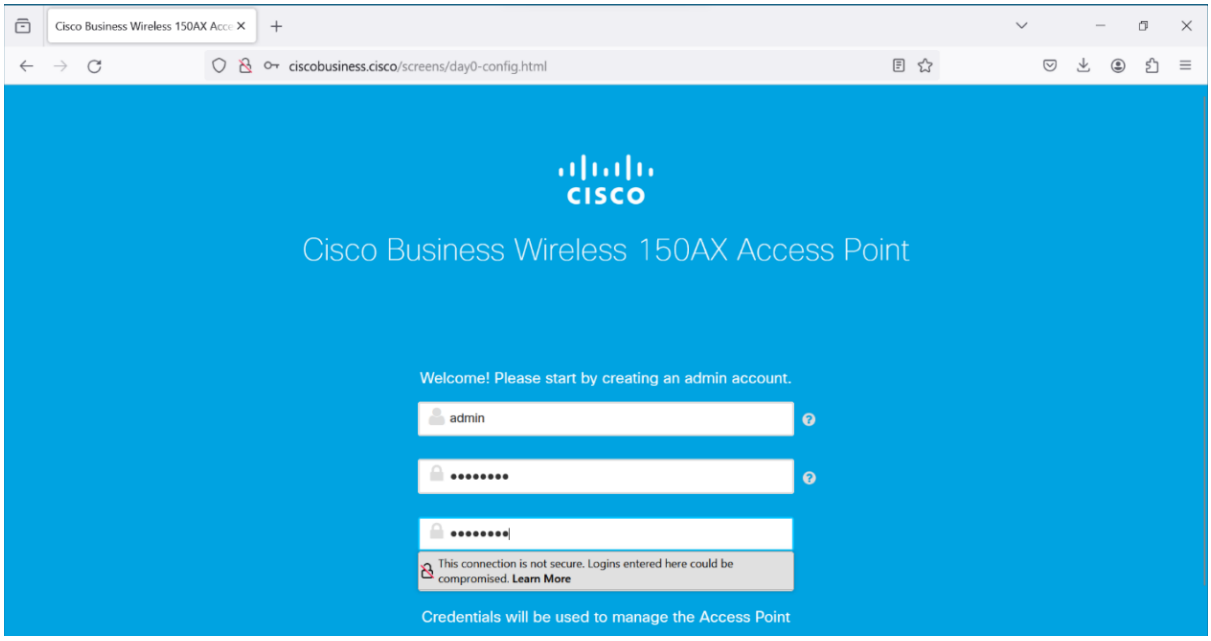
Initial Basic Configuration of CPE

Step 1: Power on the CPE and wait for the CPE to be visible on the Laptop Wi-Fi Scanning "Cisco Business-Setup" or Reset the CPE if not Visible

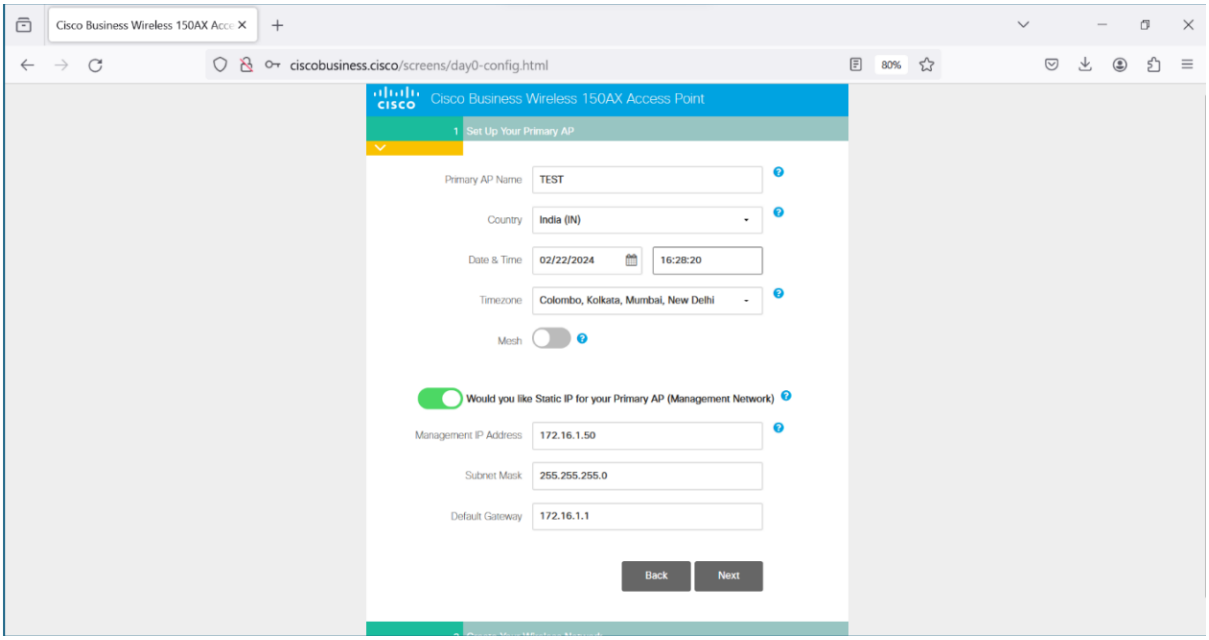
Step 2: Connect To the Wi-Fi Access Point using password " Cisco123" And Navigate to http://ciscobusiness.cisco/screens/startup.html and Click Start as Show in the below Screenshot.



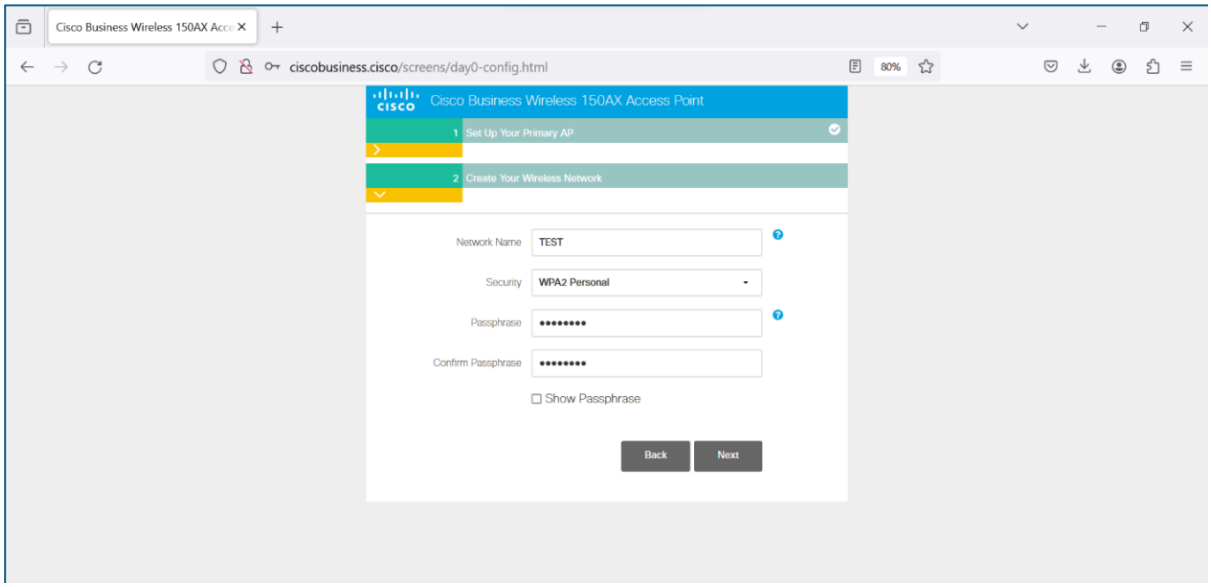
Step 3 : Enter the Desire Credentials for admin account creation and click start



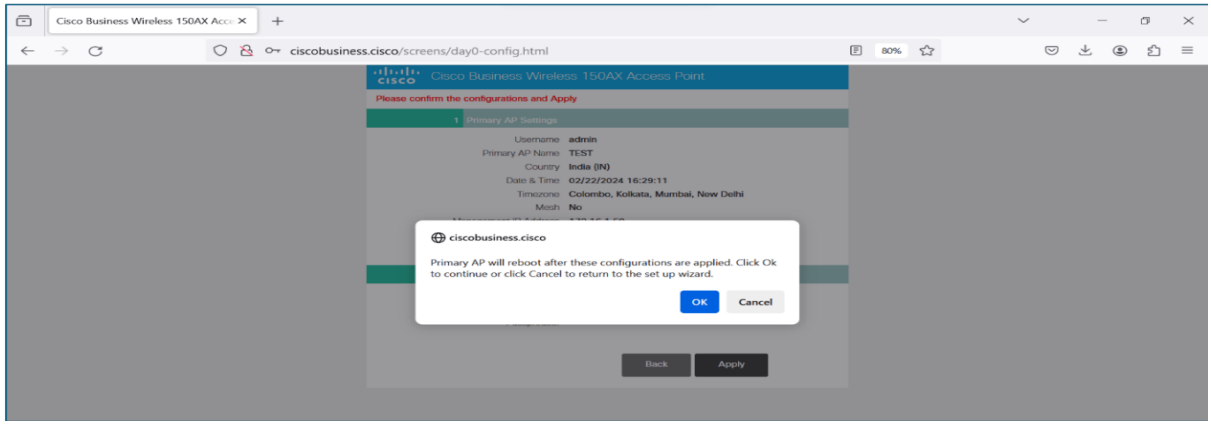
Step 4 : Enter the Desire AP Name and Select Static IP Configuration if required and click Next



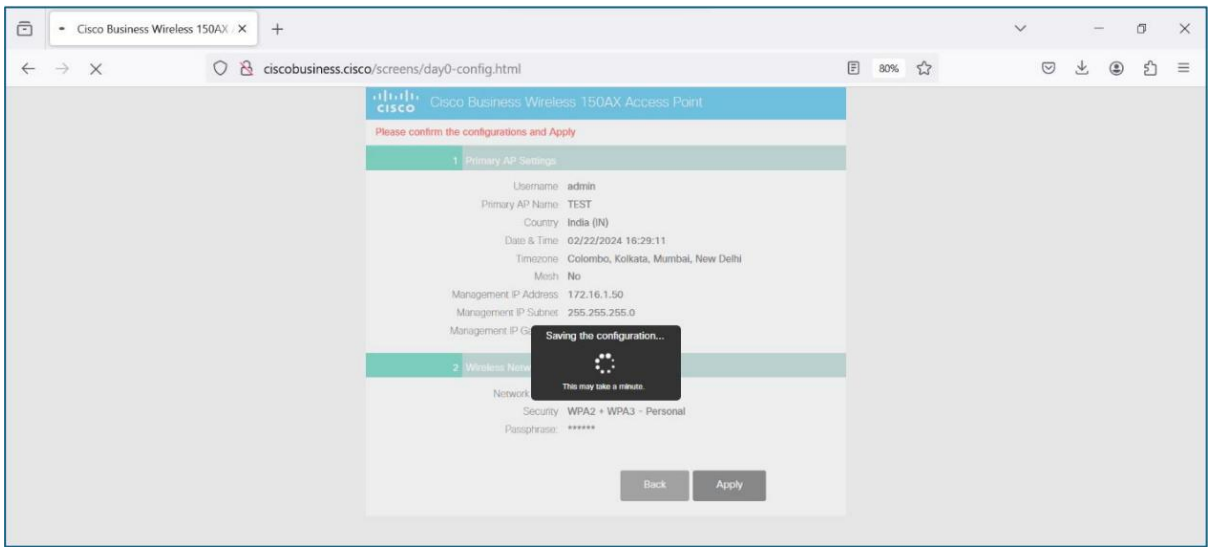
Step 5 : Enter the Desire Network Name and Passphrase and click Next

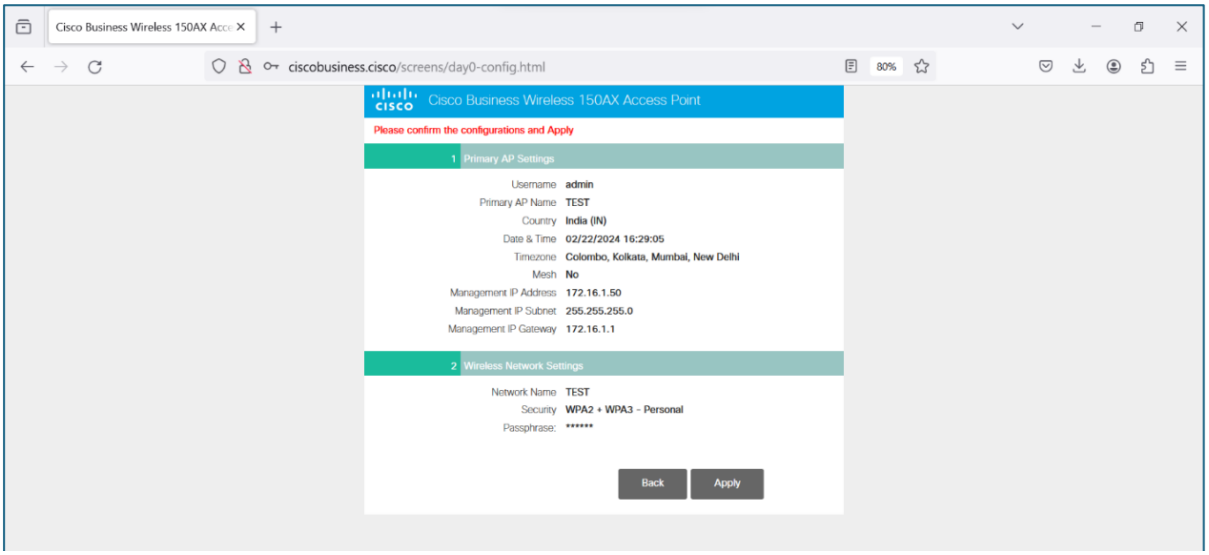


Step 6 : Verify the Configuration done and Click on Apply



Step 7 : A popup will appear on the screen “Primary AP will reboot after these configurations are applied. Click Ok to continue or click Cancel to return to the set-up wizard.”



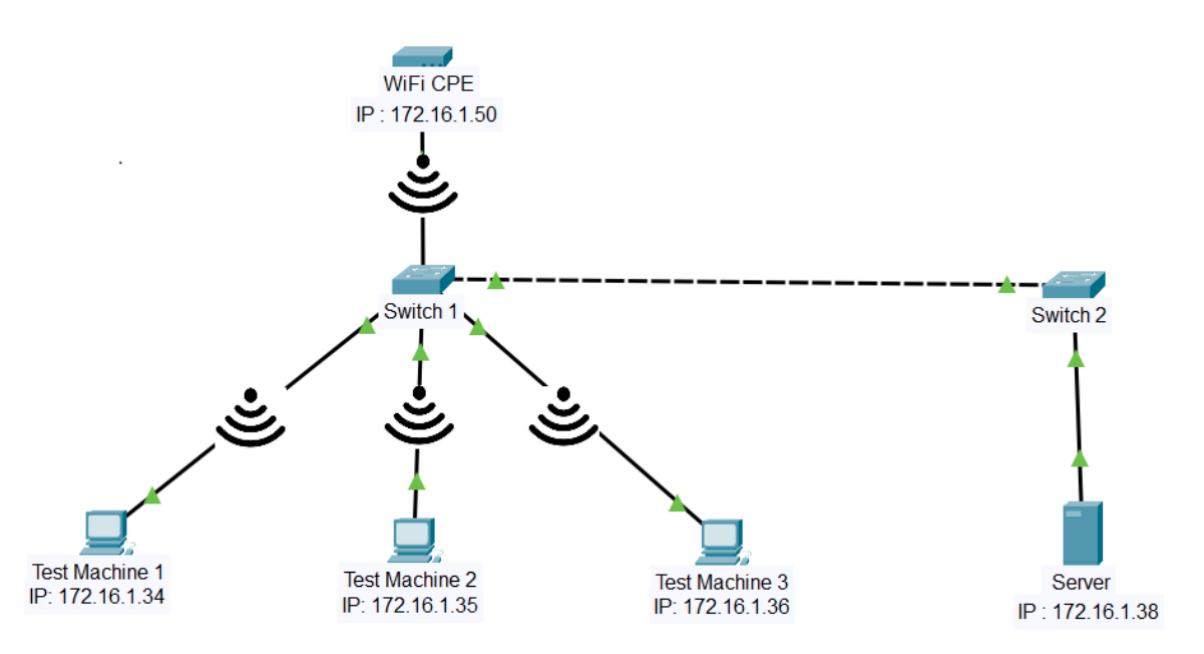


Step 8: Finished Step Now the AP is Ready to Be used.

6. **Preconditions**
   - Enable https in DUT.
   - The tester has needed administrative privileges.
   - A tester machine is available.
   - Test environment with a provision to access the DUT.
   - Vendor list of Enabled and necessary methods in the DUT Web-Server.
   - Tester must have Burp Suite installed in his testing machine

7. **Test Objective**: Check whether the DUT supports other methods apart from GET, HEAD, POST

8. **Test Plan:**
   - 8.1 Number of Test Scenarios:
     - 8.1.1 Check whether the DUT supports other methods apart from GET, HEAD, POST
   - 8.2 Test Bed Diagram



8.3 Tools Required

- Browser
- Burp suite

8.4 Test Execution Steps

- Open browser and navigate to https://wificpe-ip.
- Intercept the request using burpsuite proxy and send it to repeater.
- Change the Request Methods.
- Replace all HTTP Methods one by one and observe the response.

9. **Expected Results for Pass:**

Case 1: System settings and configurations have been found adequately set, in all Web components of the system, to ensure that unneeded HTTP methods are deactivated.

10. **Expected Format of Evidence:** Testing report contains copies of the log file showing the captured information.
11. **Test Execution:**

11.1 Test Case Number: 01

11.1.1 **Test Case Name:** TC_NO_UNUSED_HTTP_METHODS

11.1.2 **Test Case Description:** Verify that the Web server has deactivated all HTTP methods that are not required.

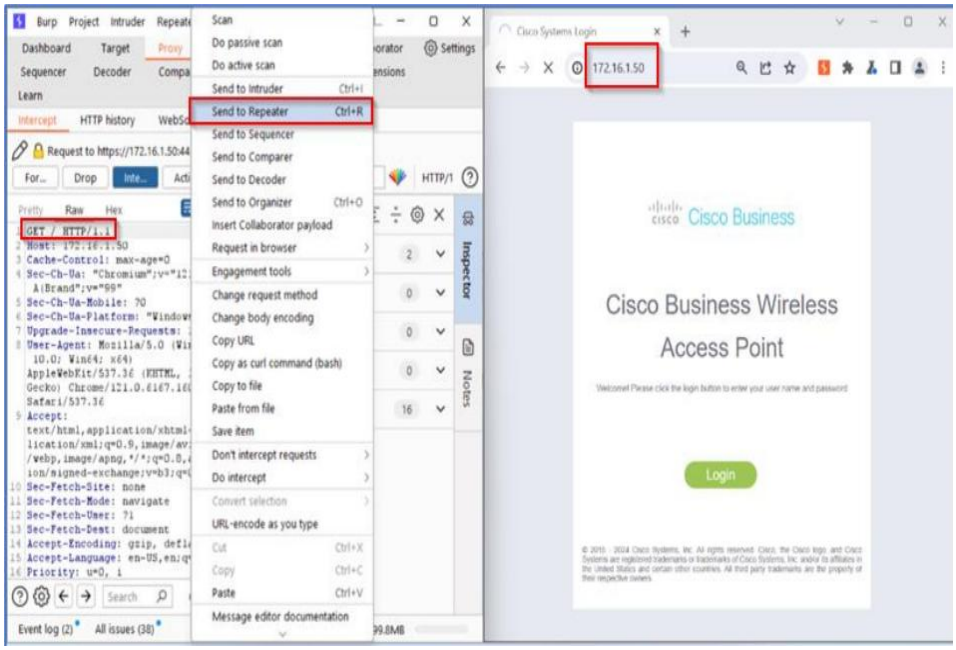
11.1.3 **Execution Steps:**

Step 1 : Open browser and navigate to https://172.16.1.50

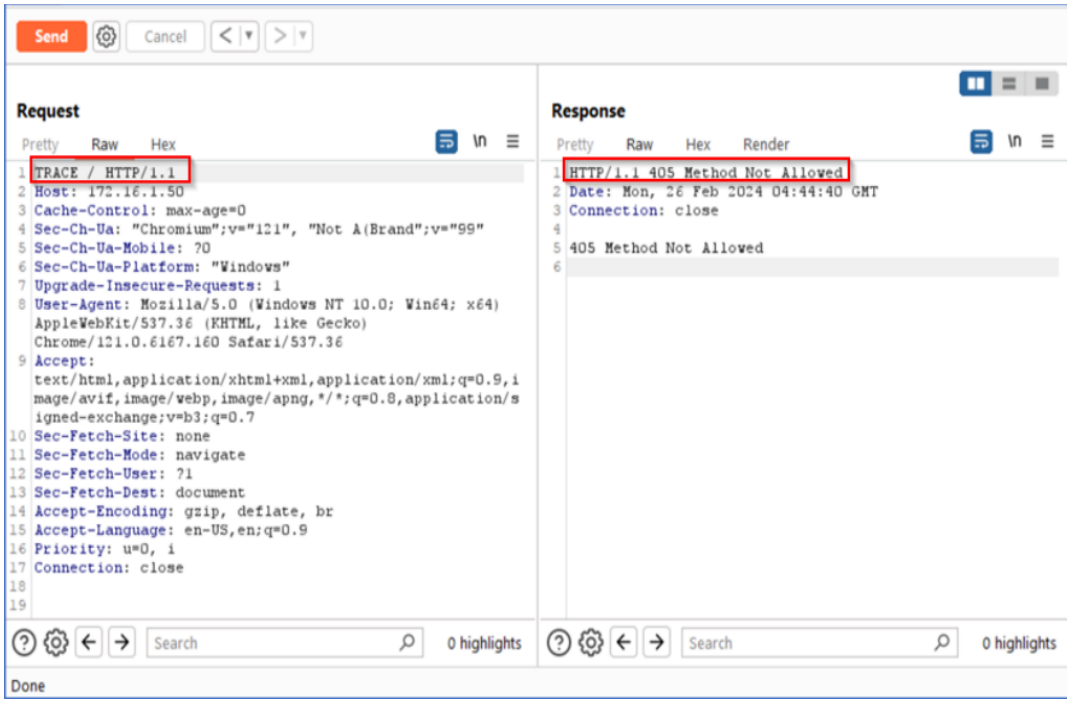
Step 2: Intercept the request using burp suite proxy and send it to repeater.

Step 3: Change the Request Methods.

GET:

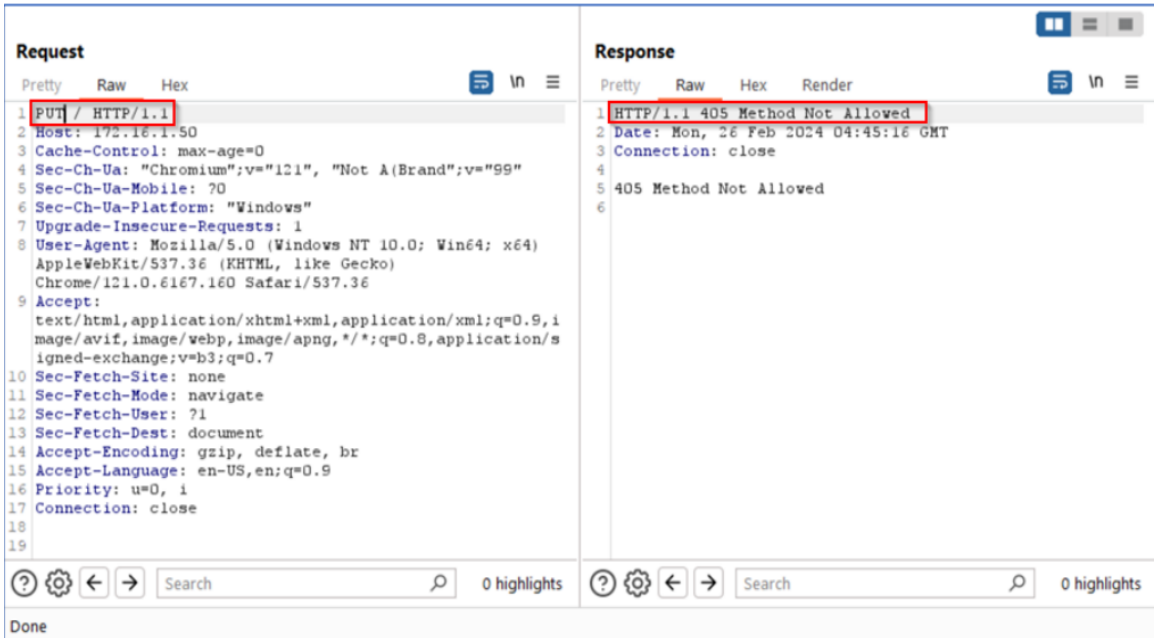


Step 4: Replace all HTTP Methods one by one and observe the response. Step 5: Check for TRACE Method

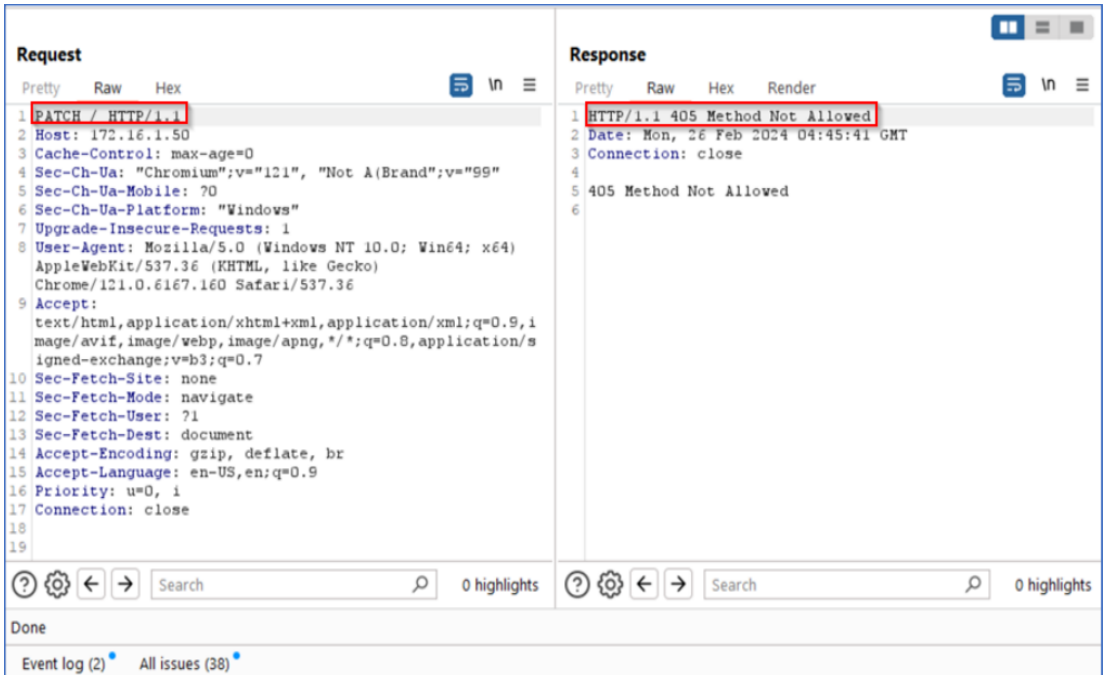


Step 6: Check for TRACK Method

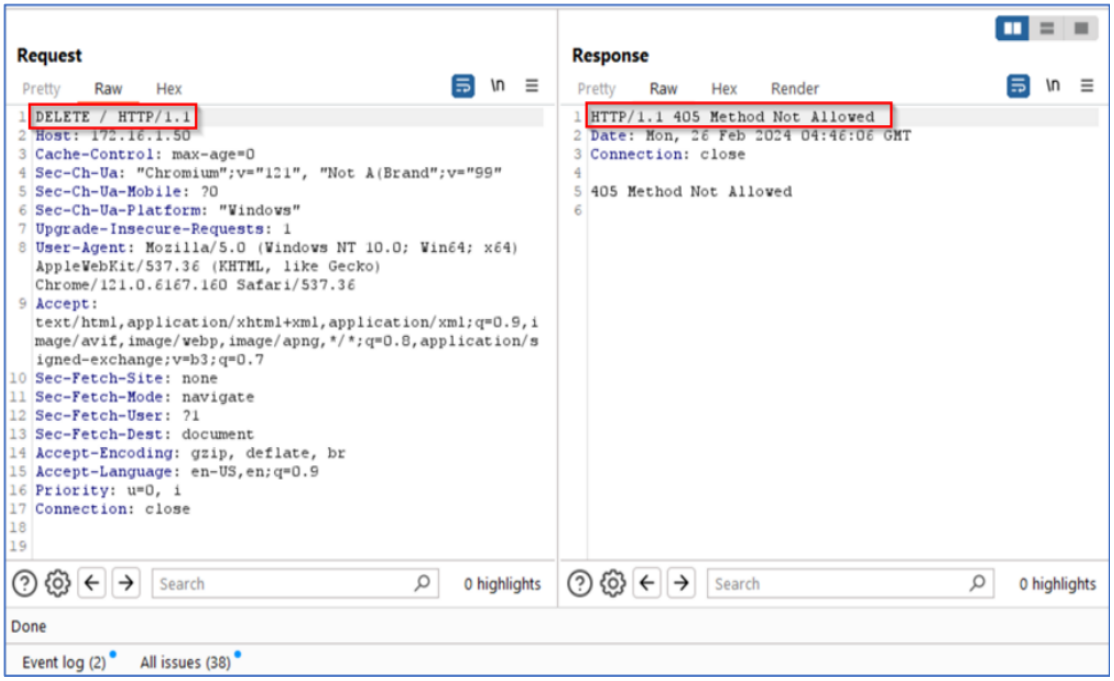
Step 7: Check for PUT Method



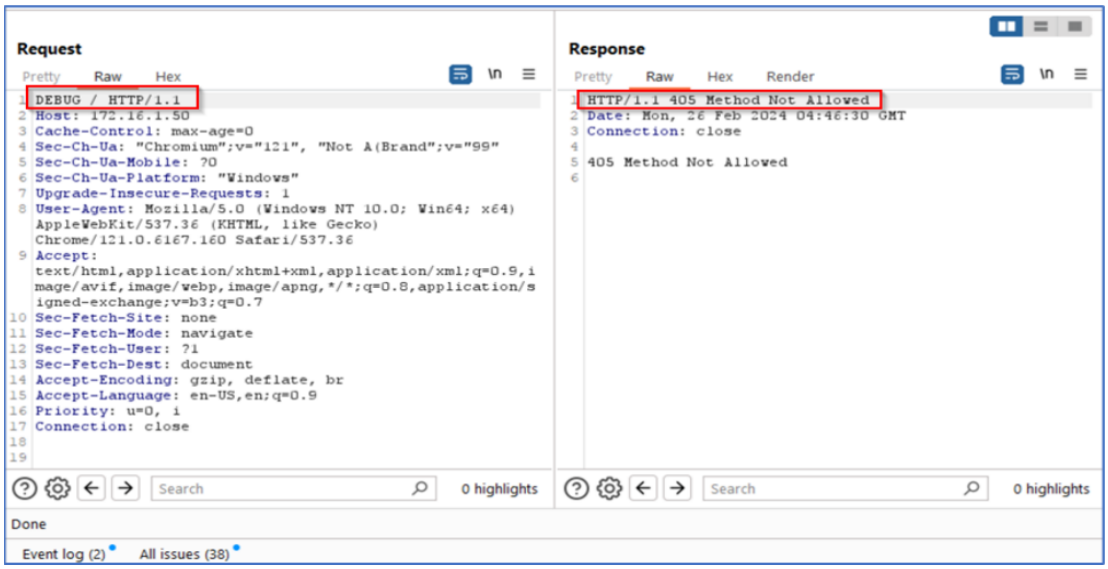
Step 8: Check for PATCH Method



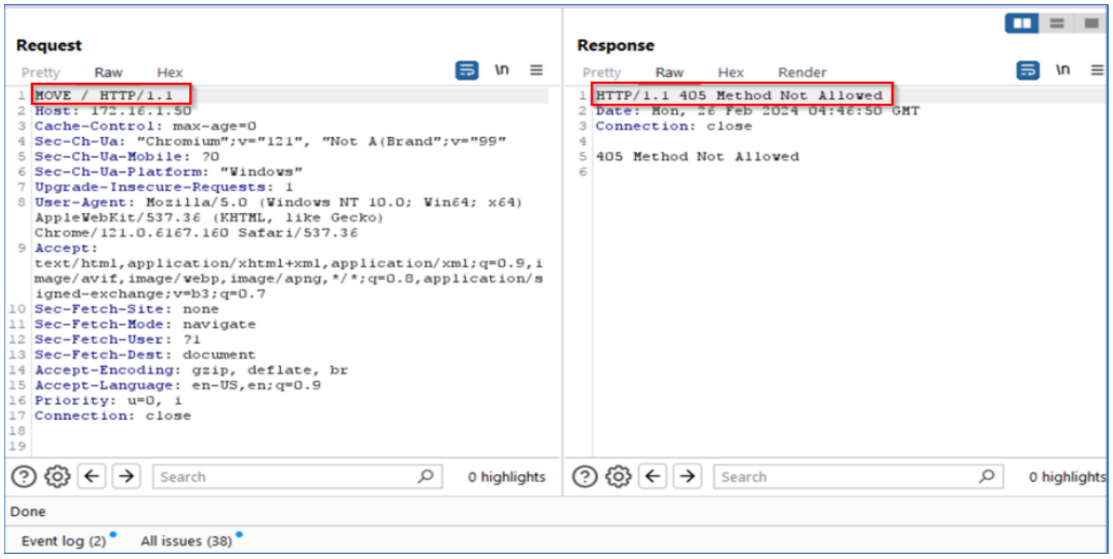
Step 9: Check for DELETE Method



Step 10: Check for DEBUG Method



Step 11: Check for MOVE Method



Step 12: same step follow for other http method also

11.1.4 **Test Observations:** The test confirmed that the web server is correctly configured to deactivate HTTP methods that are not required. Only the standard GET, HEAD, and POST methods are enabled, in line with the requirement. No other methods that could potentially introduce security leaks, such as TRACK or TRACE, are enabled. This ensures that the web server maintains a high level of security

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_UNUSED_HTTP_METHODS	PASS	all the criteria have been met

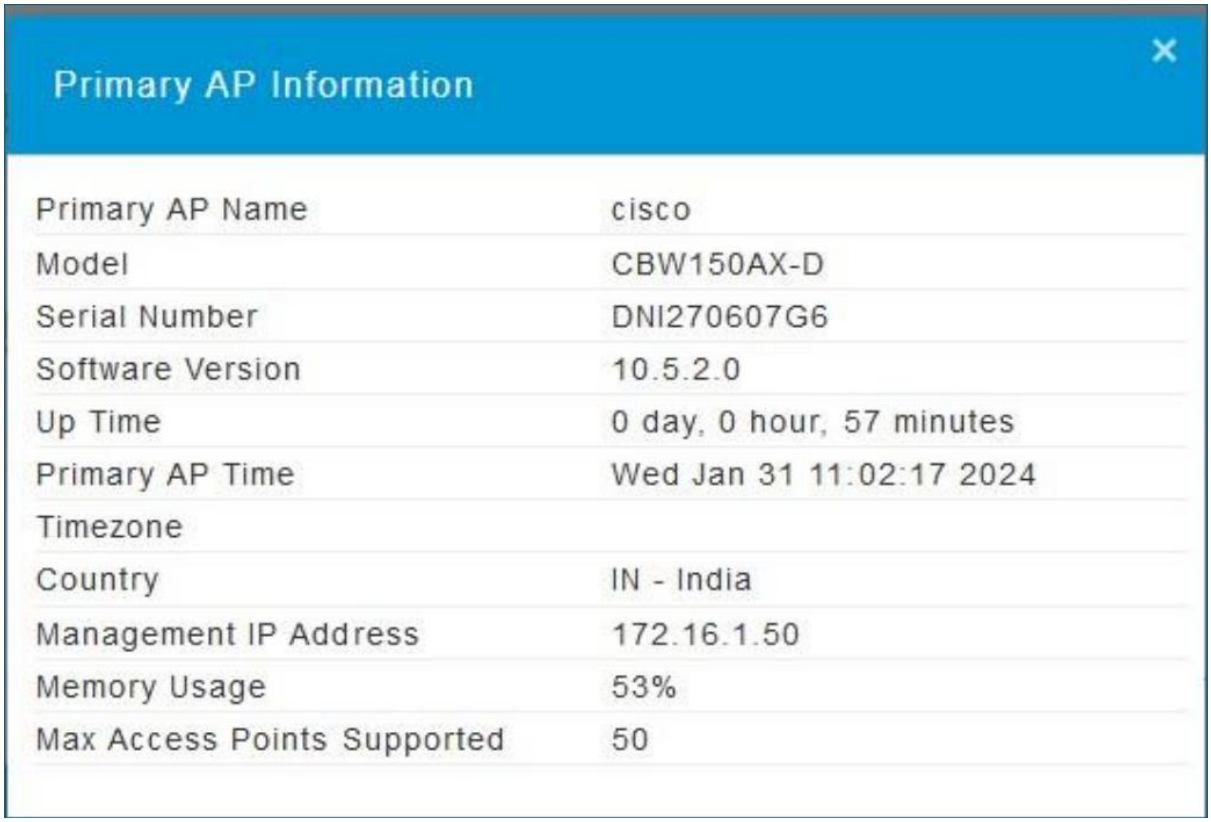
1.11.6: No unused add-ons

<DUT Details: > WiFi CPE
<DUT Software Version:> cisco 10.5.2.0
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 11: Web Server
2. **<Security Requirement No & Name >** 1.11.6: No unused add-ons
3. **<Requirement Description: >** All optional add-ons and components of the web server shall be deactivated if they are not required. In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required.

4. **DUT Confirmation Details**:

Screenshot below shows the DUT name (Primary AP Name) , Model number, Serial Number, Software Version.



DUT Configuration Checksum:

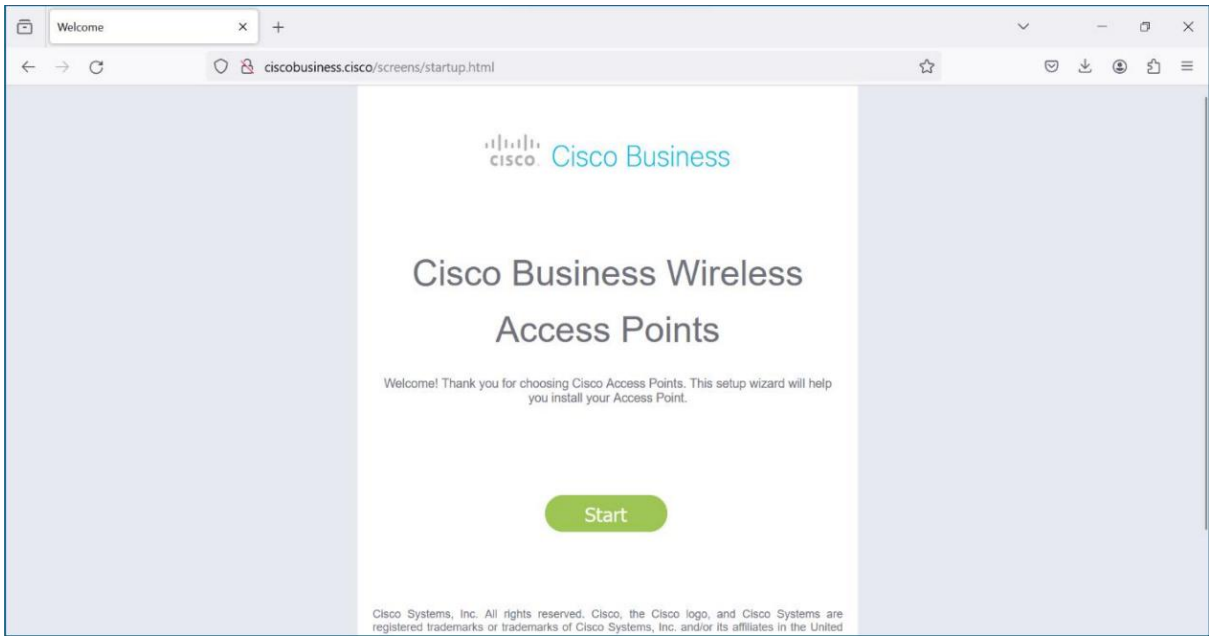
```
PS C:\> certutil -hashfile '.\Configuration files\Configuration 1.txt' SHA256
SHA256 hash of .\Configuration files\Configuration 1.txt:
fab585d185d316ad6c45b1d414d8bf55fa8ef0094173fe9a8a5fa2d3ddc2e43b
CertUtil: -hashfile command completed successfully.
```

5. **DUT Configuration:**

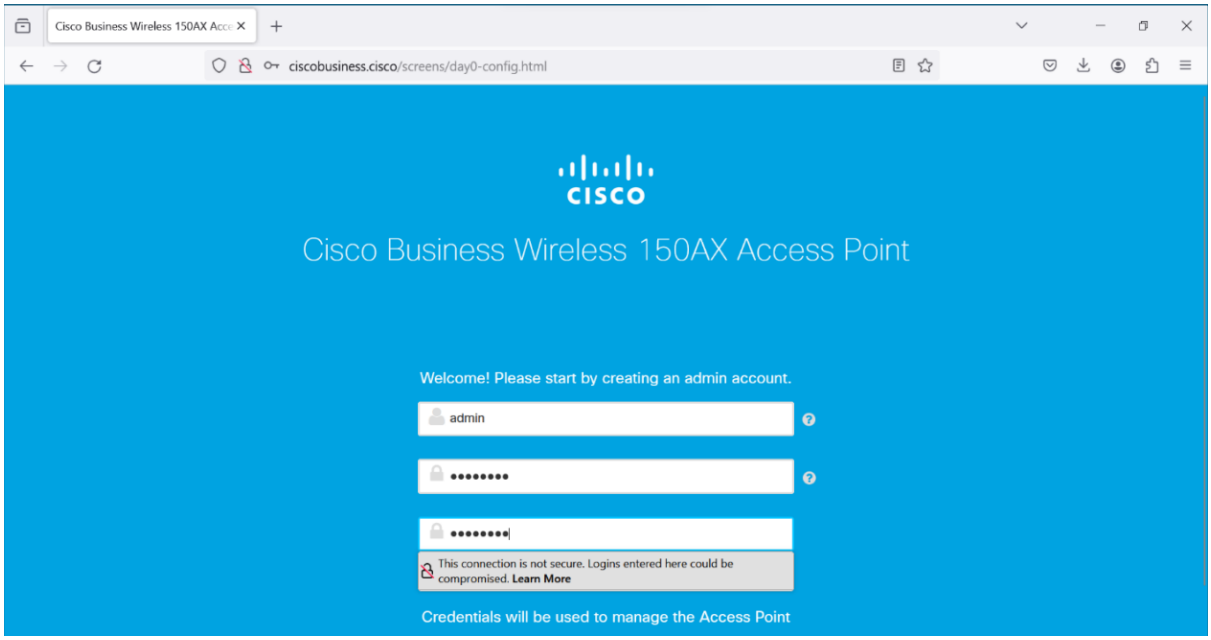
Initial Basic Configuration of CPE

Step 1: Power on the CPE and wait for the CPE to be visible on the Laptop Wi-Fi Scanning "Cisco Business-Setup" or Reset the CPE if not Visible

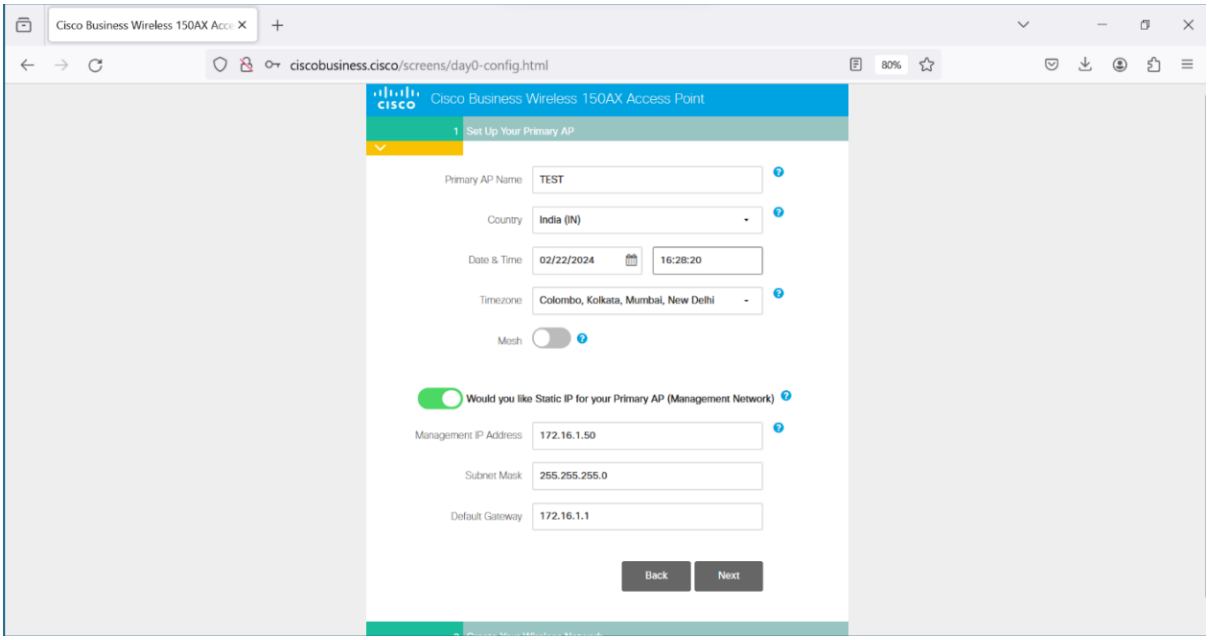
Step 2: Connect To the Wi-Fi Access Point using password " Cisco123" And Navigate to http://ciscobusiness.cisco/screens/startup.html and Click Start as Show in the below Screenshot.



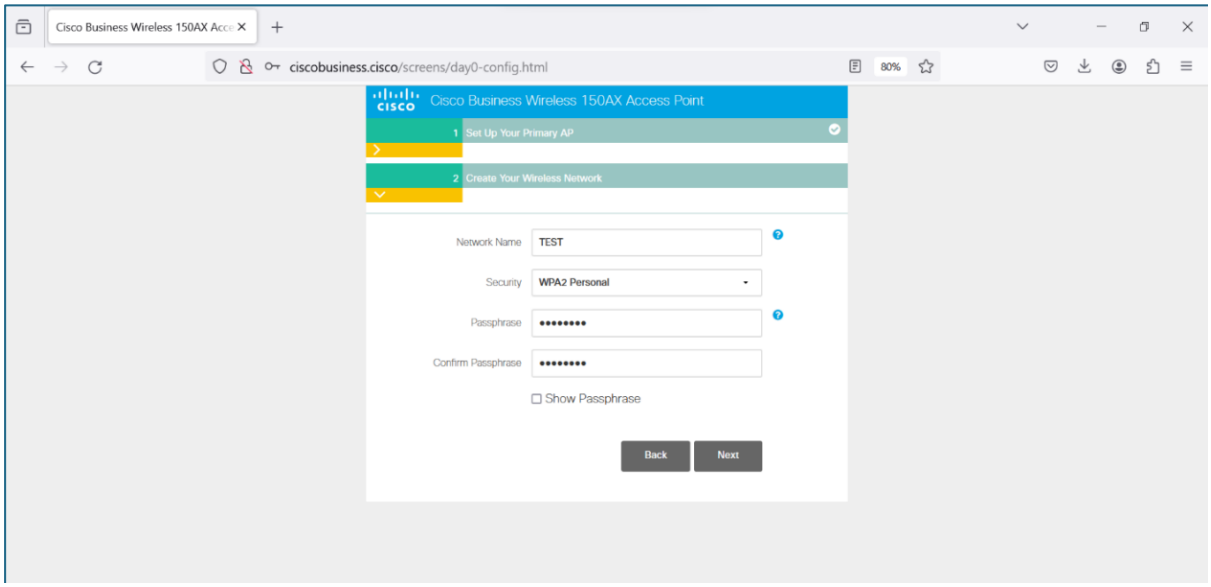
Step 3 : Enter the Desire Credentials for admin account creation and click start



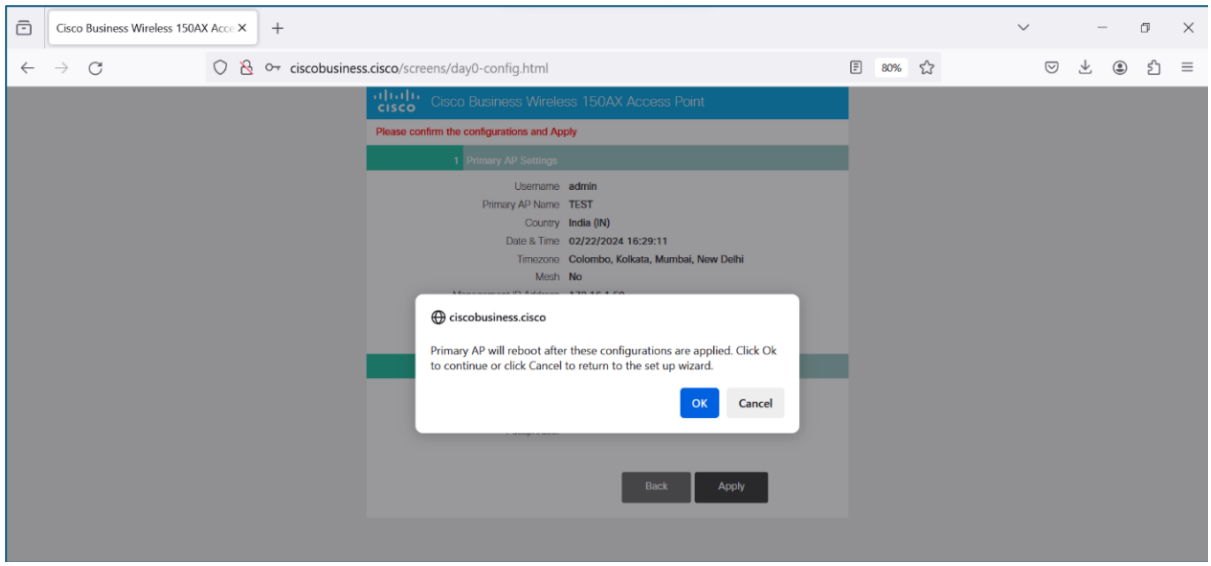
Step 4 : Enter the Desire AP Name and Select Static IP Configuration if required and click Next



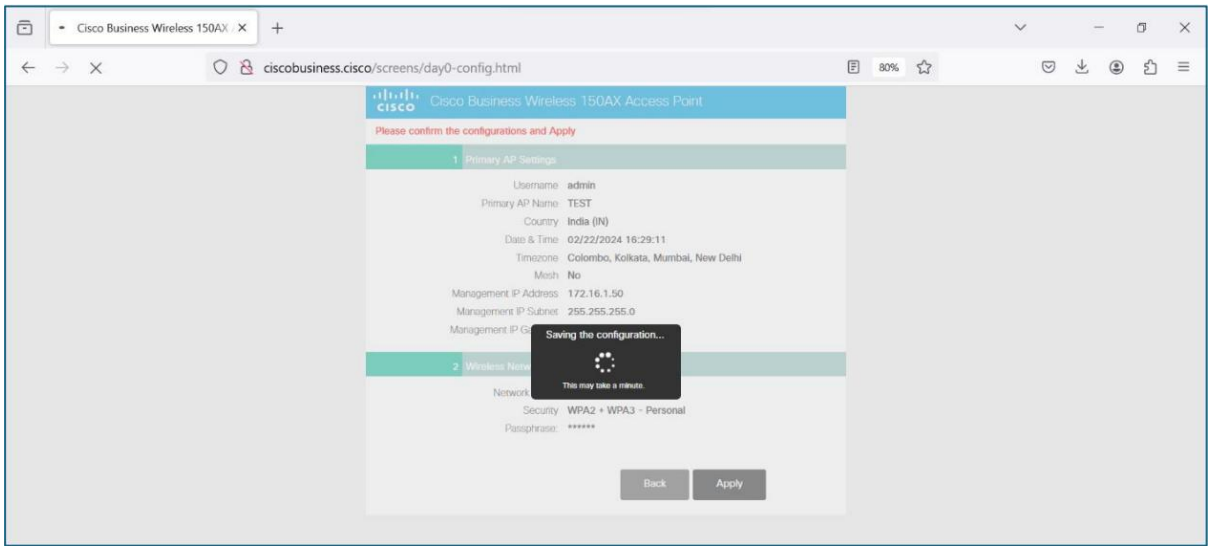
Step 5 : Enter the Desire Network Name and Passphrase and click Next

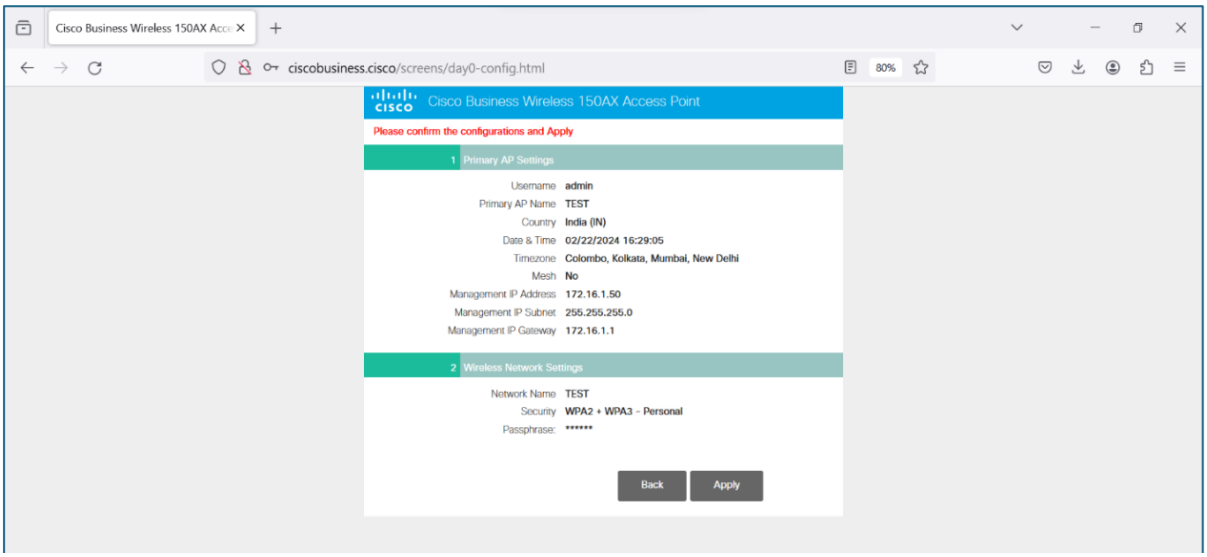


Step 6 : Verify the Configuration done and Click on Apply



Step 7 : A popup will appear on the screen “Primary AP will reboot after these configurations are applied. Click Ok to continue or click Cancel to return to the set-up wizard.”





Step 8: Finished Step Now the AP is Ready to Be used.

6. **Preconditions**
   - Enable https on DUT
   - The vendor has supplied a list of add-ons or scripting tools for Web server components needed for system operation, and that therefore need to be exempted from the test investigation.
   - The tester has administrative privileges.
   - A tester machine is available.
7. **Test Objective**: To verify that the Web server has deactivated unneeded add-ons and unneeded scripting components.

8. **Test Plan:**

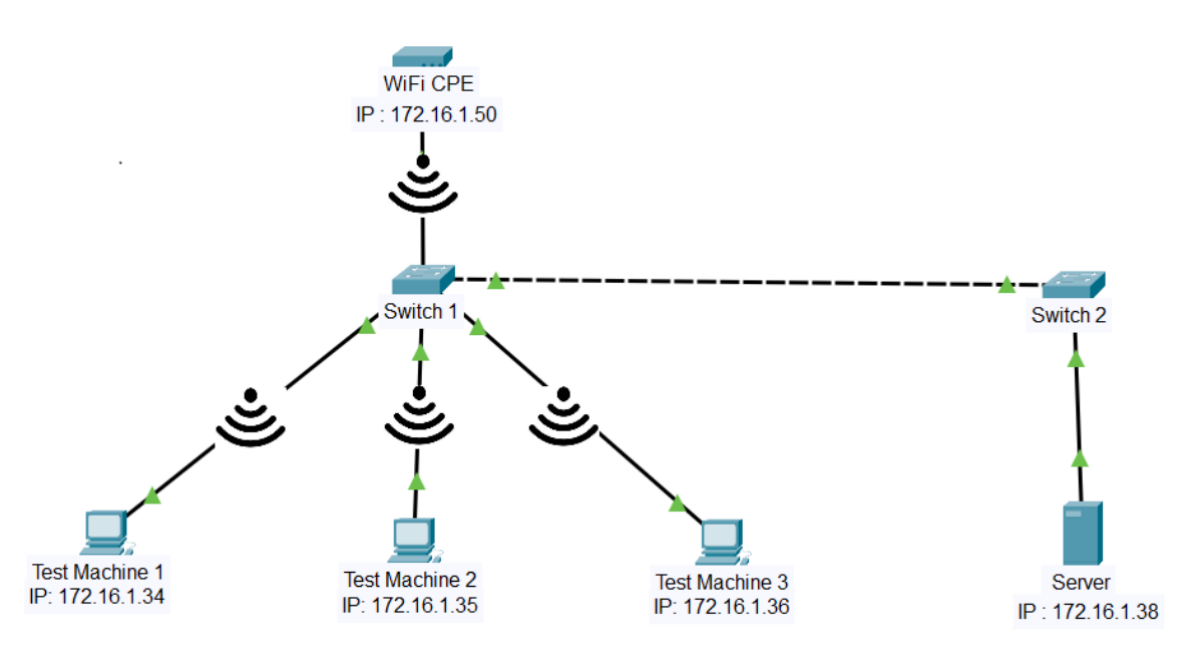
8.1 Number of Test Scenarios:

8.1.1 Check if the web server has WebDAV activated

8.1.2 Check that the DUT is restricting execution of system commands with SSI (server side includes) Injection

8.1.3 Check if any CGI directories are accessible for file uploads.

8.2 Test Bed Diagram



8.3 Tools Required

- Cadaver
- Browser
- Dirsearch
- nikto

8.4 Test Execution Steps

- Power up the testbed
- Check that the web server is only running and listening on known ports (e.g., tcp port 80 and/or 443). Check that
- CGI or other scripting components, Server Side Includes (SSI), and WebDAV are deactivated if they are not required.
- The tester verifies that nothing else has been installed than the web server.
- The tester verifies that relevant system settings and configurations are correct to ensure fulfilment of the requirement.
- The tester scans the Webserver using a suitable tool (e.g., Nikto) and verifies the tool report for availability of any default content.

9. **Expected Results for Pass:** System settings and configurations have been found adequately set, in all Web components of the system, to ensure that all unneeded add-ons or script components are deactivated.

10. **Expected Format of Evidence:** Testing report contains copies of the log file showing the captured information.

11. **Test Execution:**

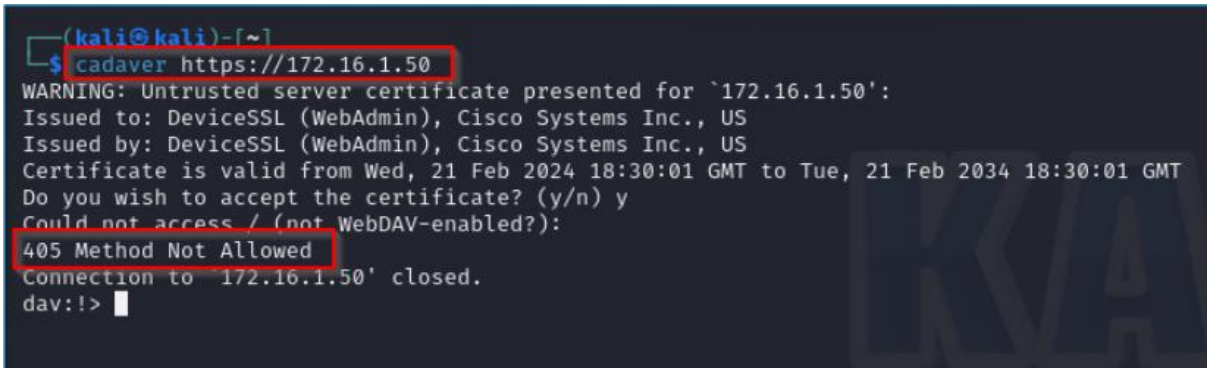
11.1 Test Case Number: 01

11.1.1 **Test Case Name:** TC_ WEBDAV_TESTING

11.1.2 **Test Case Description:** Verify that web server has WebDAV activated

11.1.3 **Execution Steps:**

Step 1 : Open kali linux and run the command cadver https://172.16.1.50 and follow the instructions.



Step 2: Observe that WebDAV is not activated in the DUT.

Step 3: Check if there are any other directories accessable for WebDav to be enabled by running the command “dirsearch -u https://172.16.1.40 -w /home/kali/Downloads/cgi-files.txt“.

Note: The 'cgi-files.txt' file contains the relevant payload based on the understanding of the Device Under Test (DUT) filesystem.

11.1.4 **Test Observations:** DUT has no directories to access so the WebDAV is deactivated.

11.2 Test Case Number: 02

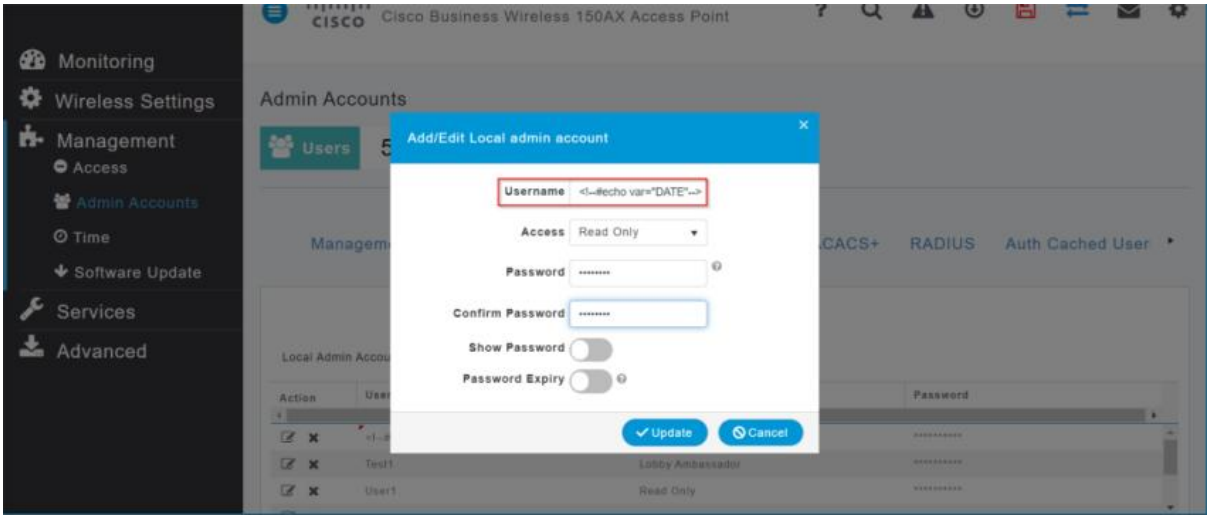
11.2.1 **Test Case Name:** TC_ SSI_TESTING

11.2.2 **Test Case Description:** Verify that web server has SSI activated

11.2.3 **Execution Steps:**

Step 1: Open browser, navigate to https://172.16.1.50 and login

Step 2: Navigate to Administrator panel then Add profile then in the profile name put the payload “←#echo var="DATE"-->”



Step 3: Click f12 and click on “Apply to Device” and observe the network traffic.

Step 4: Observe that the request has been proceeded by DUT. Step 5: Verifying whether the DUT have SSI, CGI & WebDAV active using Nikto tool.

Step 5: Verifying whether the DUT have SSI, CGI & WebDAV active using Nikto tool.

11.2.4 **Test Observations:** It should be ensured that SSI is deactivated if not required

11.3 Test Case Number: 03

11.3.1 **Test Case Name:** TC_ CGI_TESTING

11.3.2 **Test Case Description:** Verify that web server has CGI activated

11.3.3 **Execution Steps:**

Step 1 : Open kali linux and run the command dirsearch -u https://172.16.1.50 -w /home/kali/Downloads/cgifiles.txt.


(kali㉿kali)-[~/Downloads]
$ dirsearch -u https://172.16.1.50 -w /home/kali/Downloads/cgi-files.txt
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
from pkg_resources import DistributionNotFound, VersionConflict
v0.4.3
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 90
Output File: /home/kali/Downloads/reports/https_172.16.1.50/_24-02-23_04-24-48.txt
Target: https://172.16.1.50/
[04:24:48] Starting:
Task Completed

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat cgi-files.txt
/cgi-bin/14all-1.1.cgi
/cgi-bin/14all.cgi
/cgi-bin/a1disp3.cgi
/cgi-bin/a1stats/a1disp3.cgi
/cgi-bin/a1stats/a1disp4.cgi
/cgi-bin/admin.cgi
/cgi-bin/adsl.cgi
/cgi-bin/auktion.cgi
/cgi-bin/bbs/read.cgi
/cgi-bin/bhrss.py
/cgi-bin/calendar/calendar.pl
/cgi-bin/cgi
/cgi-bin/CGIProxy.fcgi
/cgi-bin/commerce.cgi
/cgi-bin/cookie.cgi
/cgi-bin/cvename.cgi
/cgi-bin/dcforum.cgi
/cgi-bin/ddns
/cgi-bin/dial
/cgi-bin/directorypro.cgi
/cgi-bin/disorder
/cgi-bin/e-cms/vis/vis.pl
/cgi-bin/emsgb/easymsgb.pl
/cgi-bin/emu/html/emumail.cgi
/cgi-bin/emumail.cgi
/cgi-bin/emumail/emumail.cgi
/cgi-bin/ezshopper/search.cgi
/cgi-bin/FileSeek.cgi
/cgi-bin/FileSeek2.cgi
/cgi-bin/firmwarecfg
/cgi-bin/firmwareupgrade
/cgi-bin/generate.cgi
/cgi-bin/gH.cgi
/cgi-bin/hsx.cgi
/cgi-bin/im_trbbs.cgi
/cgi-bin/ImageFolio/admin/admin.cgi
/cgi-bin/img.pl
/cgi-bin/Intruders.cfg
/cgi-bin/jammail.pl
/cgi-bin/kaiseki.cgi
/cgi-bin/kerbynet
/cgi-bin/loader
/cgi-bin/loadpage.cgi
/cgi-bin/luci
/cgi-bin/magiccard.cgi
/cgi-bin/mail/emumail.cgi
```

Step 2: Observe that there is no CGI directory available.
Step 3: Word list to brute force for CGI bin directory

11.3.4 **Test Observations:** It should be ensured that CGI is deactivated if not required

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_ WEBDAV_TESTING	PASS	all the criteria have been met
2	TC_ SSI_TESTING	PASS	
3	TC_ CGI_TESTING	PASS	

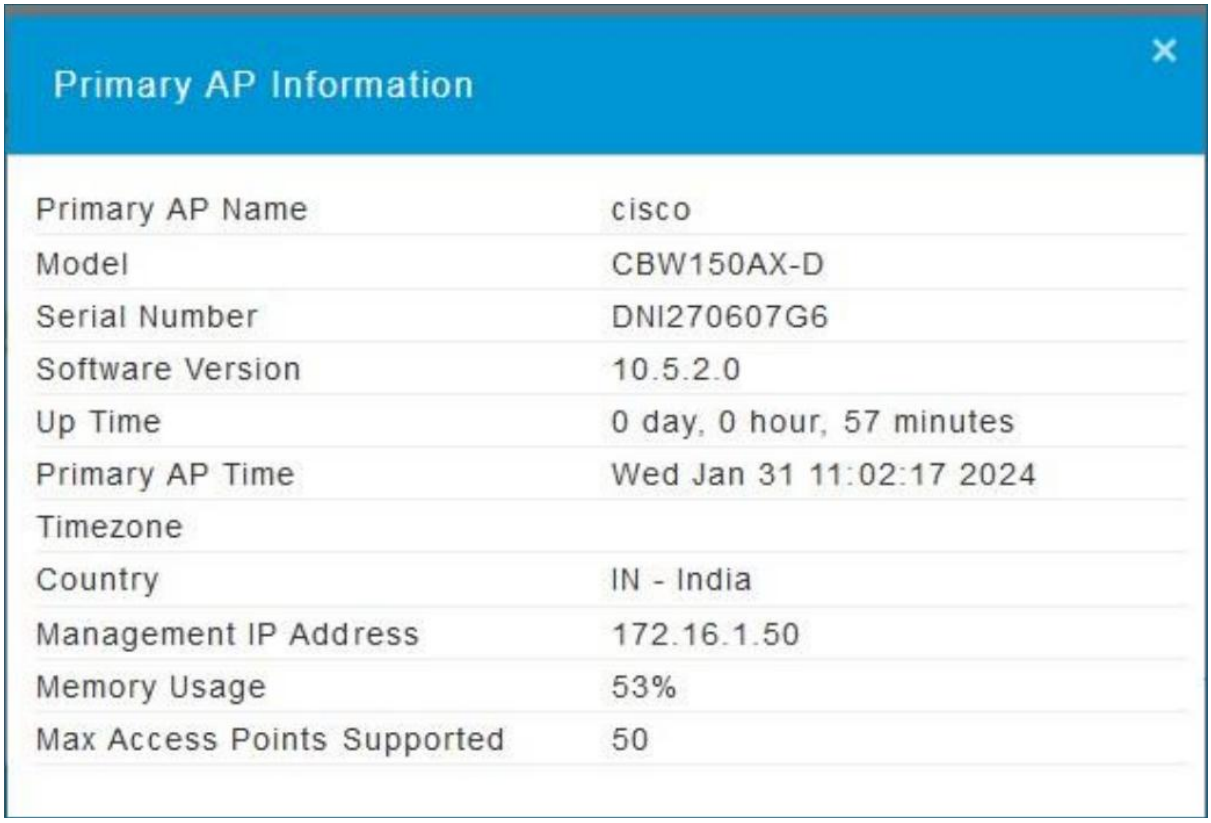
1.11.7: No compiler, interpreter, or shell via CGI or other server- side scripting

<DUT Details: > WiFi CPE
<DUT Software Version:> cisco 10.5.2.0
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 11: Web Server
2. **<Security Requirement No & Name >** 1.11.7: No compiler, interpreter, or shell via CGI or other server- side scripting
3. **<Requirement Description: >** If CGI (Common Gateway Interface) or other scripting technology is used, the CGI directory- or other corresponding scripting directory - shall not include compilers or interpreters (e.g., PERL interpreter, PHP interpreter/compiler, Tcl interpreter/compiler or operating system shells).

4. **DUT Confirmation Details**:

Screenshot below shows the DUT name (Primary AP Name) , Model number, Serial Number, Software Version.



DUT Configuration Checksum:

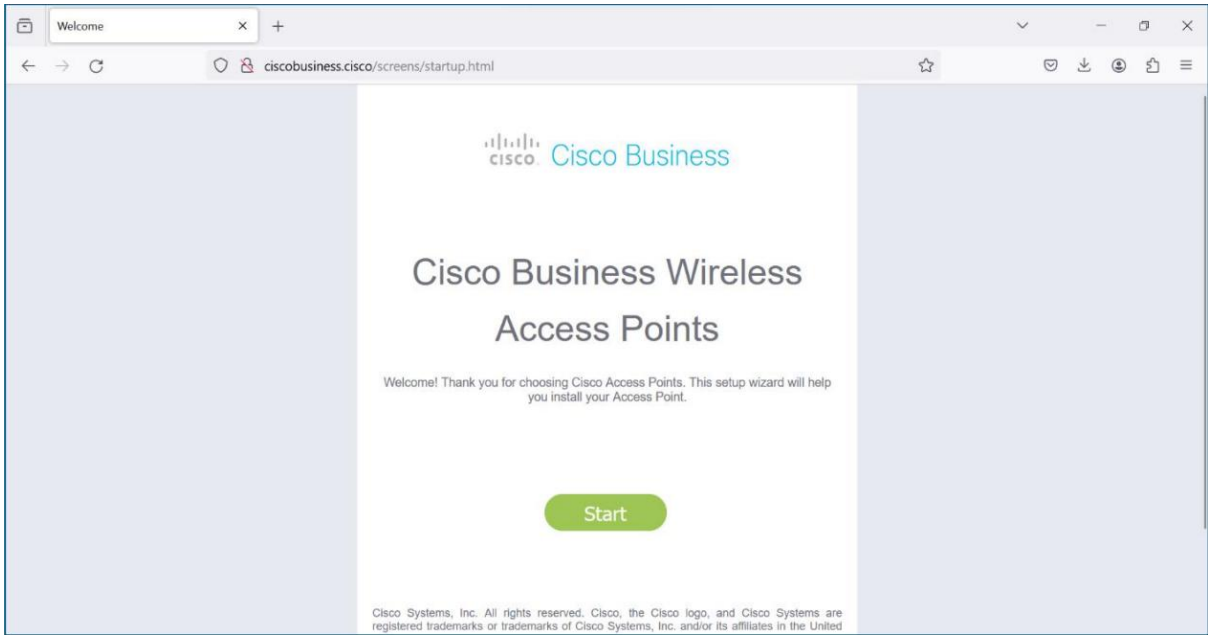
```
PS C:\> certutil -hashfile '.\Configuration files\Configuration 1.txt' SHA256
SHA256 hash of .\Configuration files\Configuration 1.txt:
fab585d185d316ad6c45b1d414d8bf55fa8ef0094173fe9a8a5fa2d3ddc2e43b
CertUtil: -hashfile command completed successfully.
```

5. **DUT Configuration:**

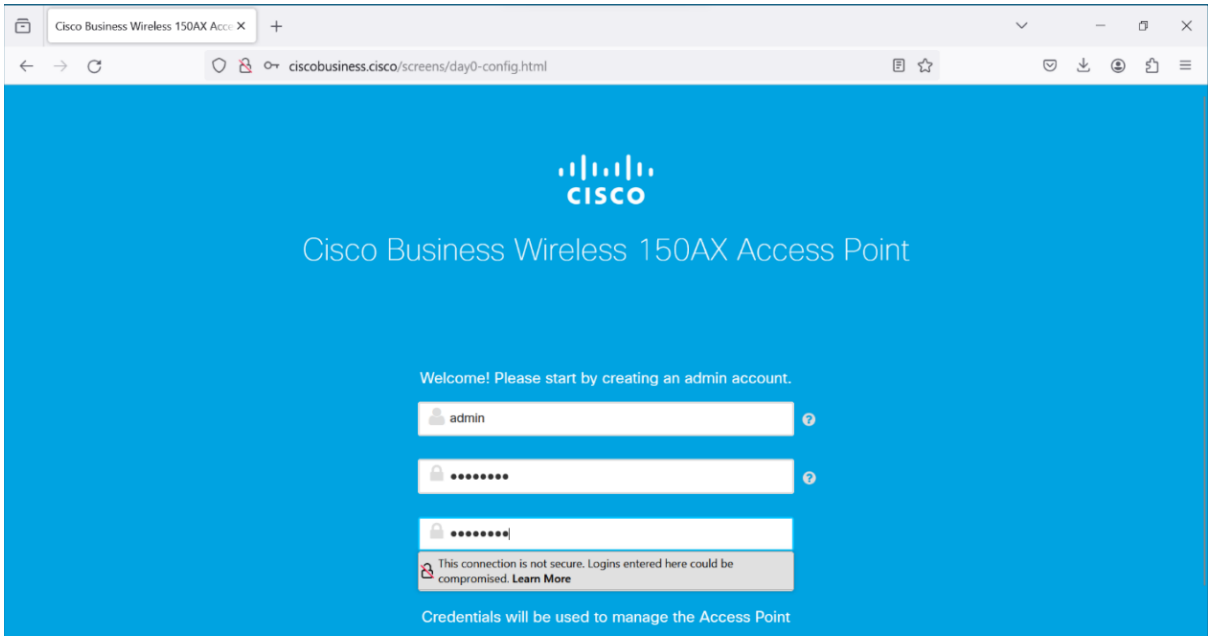
Initial Basic Configuration of CPE

Step 1: Power on the CPE and wait for the CPE to be visible on the Laptop Wi-Fi Scanning “Cisco Business-Setup” or Reset the CPE if not Visible

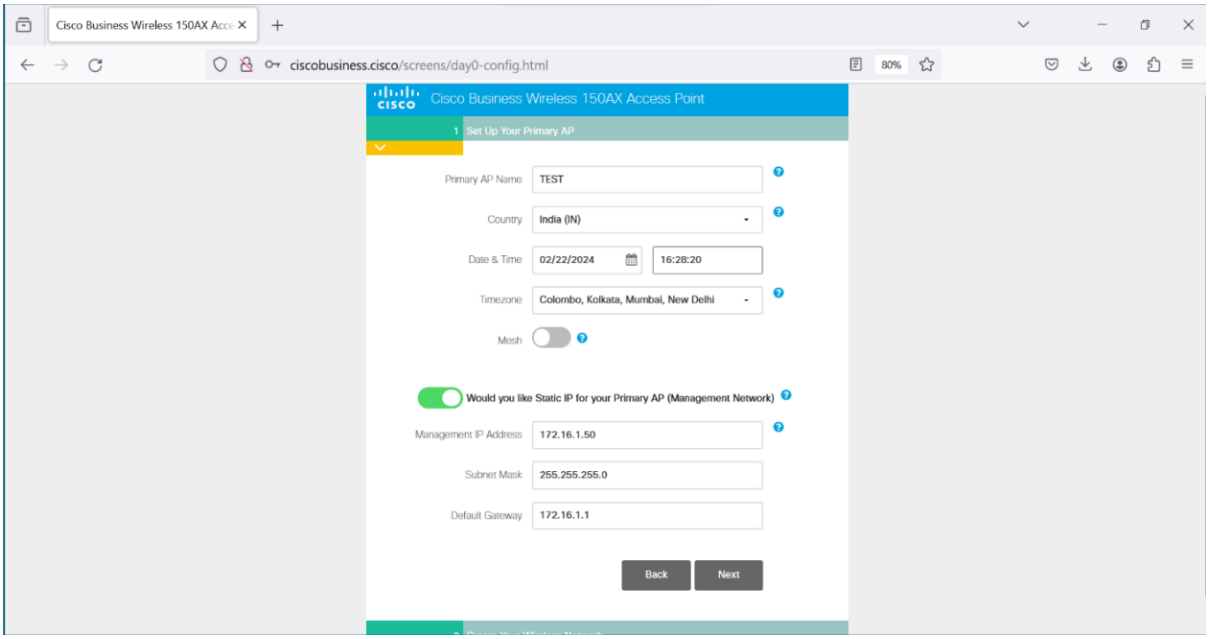
Step 2: Connect To the Wi-Fi Access Point using password " Cisco123" And Navigate to http://ciscobusiness.cisco/screens/startup.html and Click Start as Show in the below Screenshot.



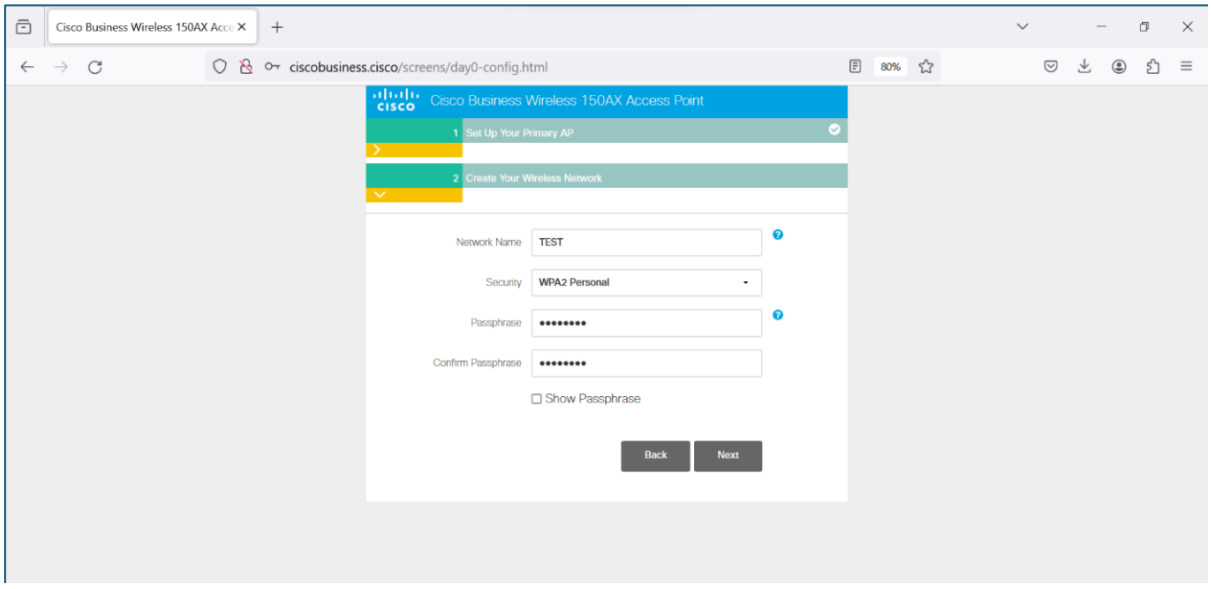
Step 3 : Enter the Desire Credentials for admin account creation and click start



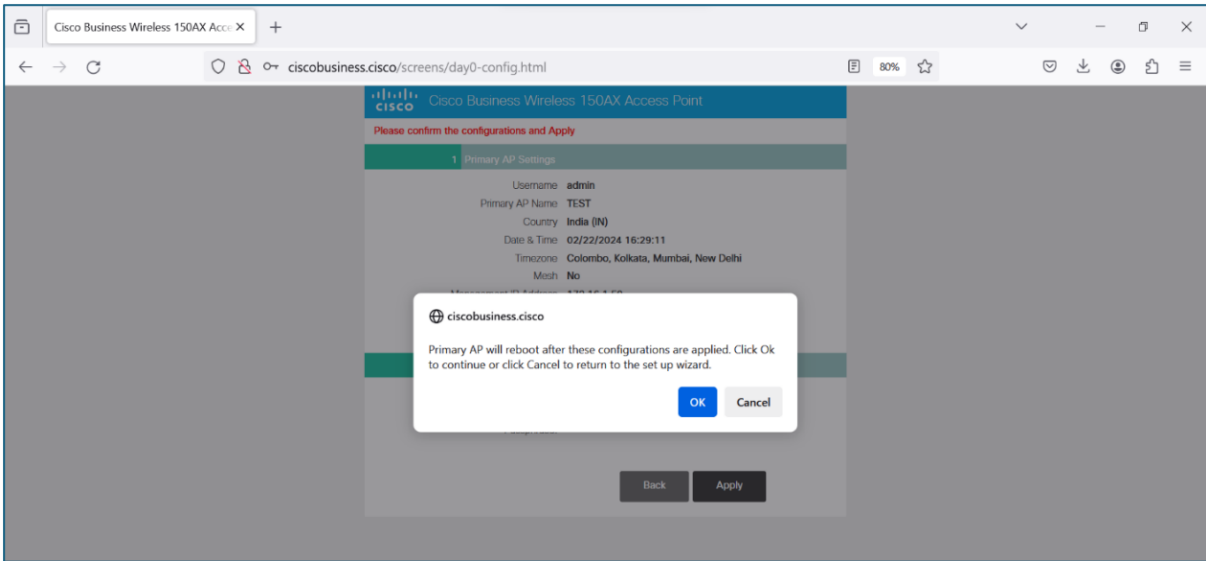
Step 4 : Enter the Desire AP Name and Select Static IP Configuration if required and click Next



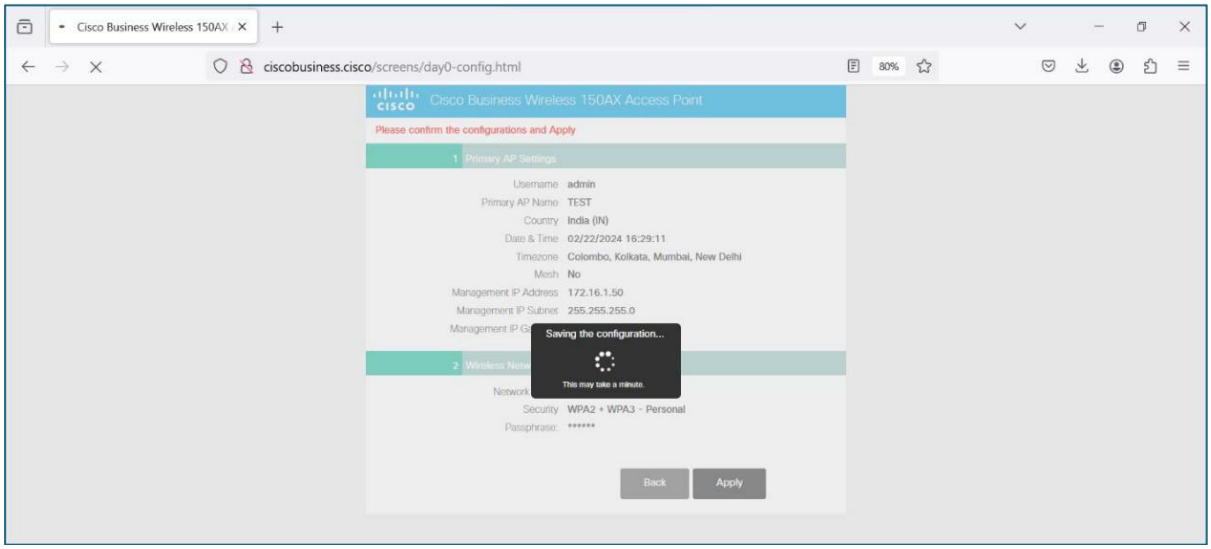
Step 5 : Enter the Desire Network Name and Passphrase and click Next

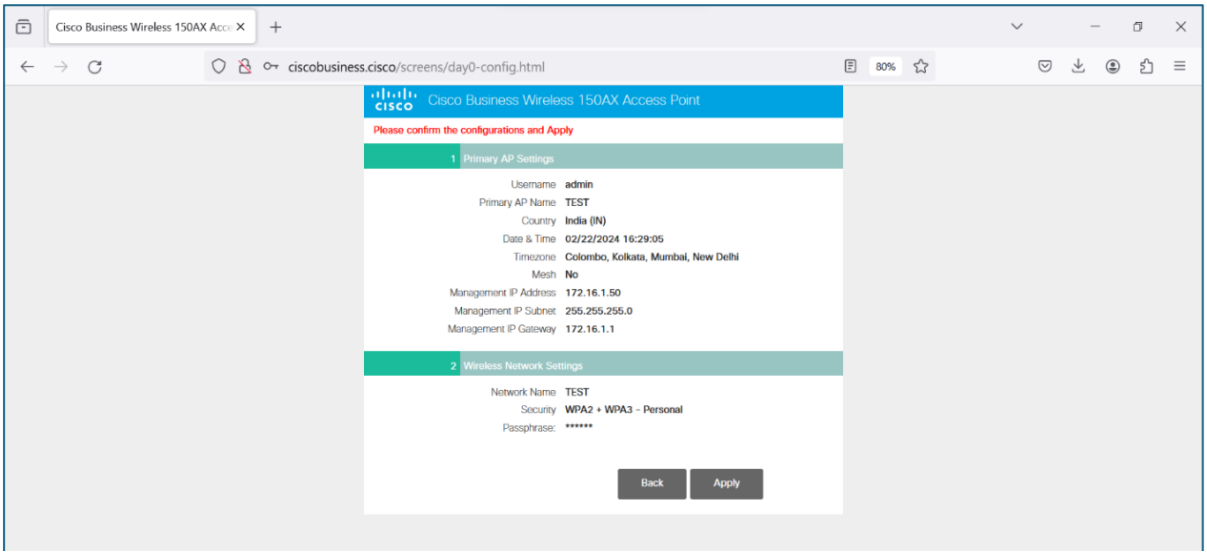


Step 6 : Verify the Configuration done and Click on Apply



Step 7 : A popup will appear on the screen “Primary AP will reboot after these configurations are applied. Click Ok to continue or click Cancel to return to the set-up wizard.”





Step 8: Finished Step Now the AP is Ready to Be used.

6. **Preconditions**
   - Enable https on DUT
   - The tester has administrative privileges.
   - A tester machine is available.
7. **Test Objective**: To verify that there are no compilers, interpreters, or shell accessible via CGI or other scripting components.

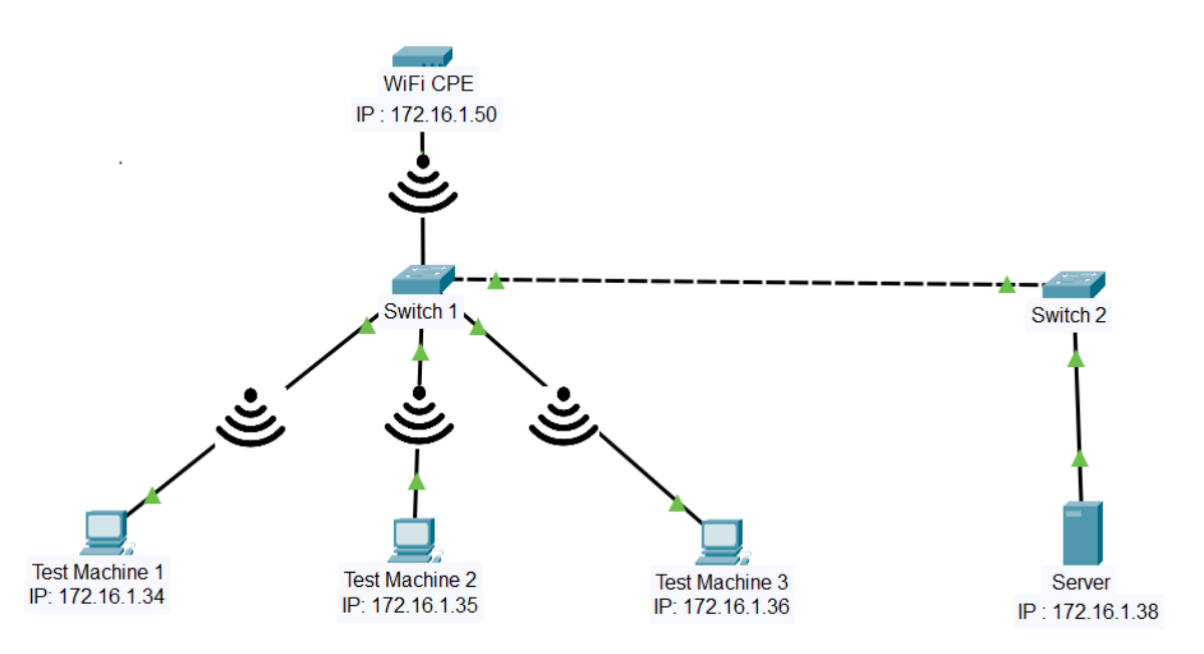
8. **Test Plan:**

8.1 Number of Test Scenarios:

8.1.1. Test Scenario for CGI and scripting directory

- This test scenario is regarding CGI, scripting directory and check for compiler/interpreter or shell in CGI

8.2 Test Bed Diagram



8.3 Tools Required

- Cadaver
- Browser
- Dirsearch
- Nikto

8.4 Test Execution Steps

- Power up the testbed
- The tester tries to access the Shell of Web Server.
- Consult the web server configuration to identify all directories used for CGI or other scripting components.
- In case the DUT is using other than CGI they must give the information about different technology used and further tests should be performed on that technology. (This document only deals with CGI Scripts)
- The tester manually checks that there are no compilers or interpreters (e.g., PERL® interpreter, PHP interpreter/compiler, Tcl interpreter/compiler or operating system shells) in the directory/directories used for CGI or for other scripting tools (including PERL®, PHP, and others).
- The tester will run some web scanning tools like Nikto, to get the detailed information and verify that there are no compilers or interpreters (e.g., PERL® interpreter, PHP interpreter/compiler, Tcl interpreter/compiler or operating system shells) in the directory/directories used for CGI or for other scripting tools (including PERL®, PHP, and others).

9. **Expected Results for Pass:**

- There are no compilers, interpreters or shells in directories accessible via CGI or other scripting components.

10. **Expected Format of Evidence:** Testing report contains copies of the log file showing the captured information.

11. **Test Execution:**

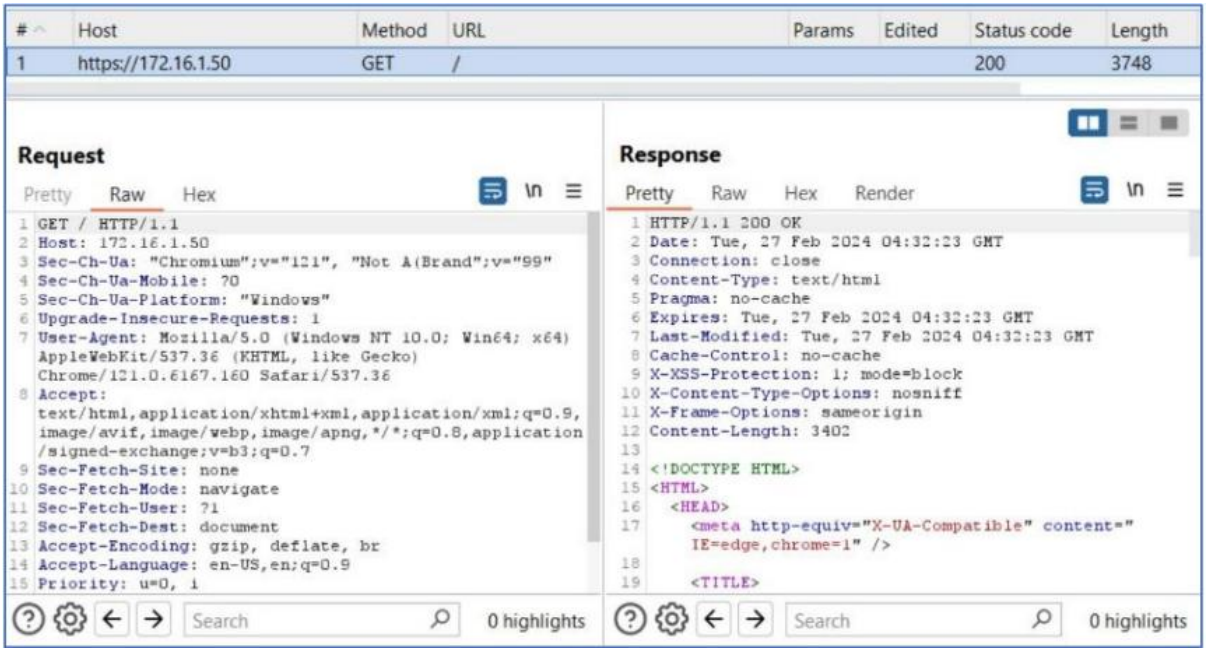
11.1 Test Case Number: 01

11.1.1 **Test Case Name:** TC_NO_COMPILER_FOR_CGI_SCRIPTING

11.1.2 **Test Case Description:** There are no compilers, interpreters, or shells in directories accessible via CGI or other scripting components.

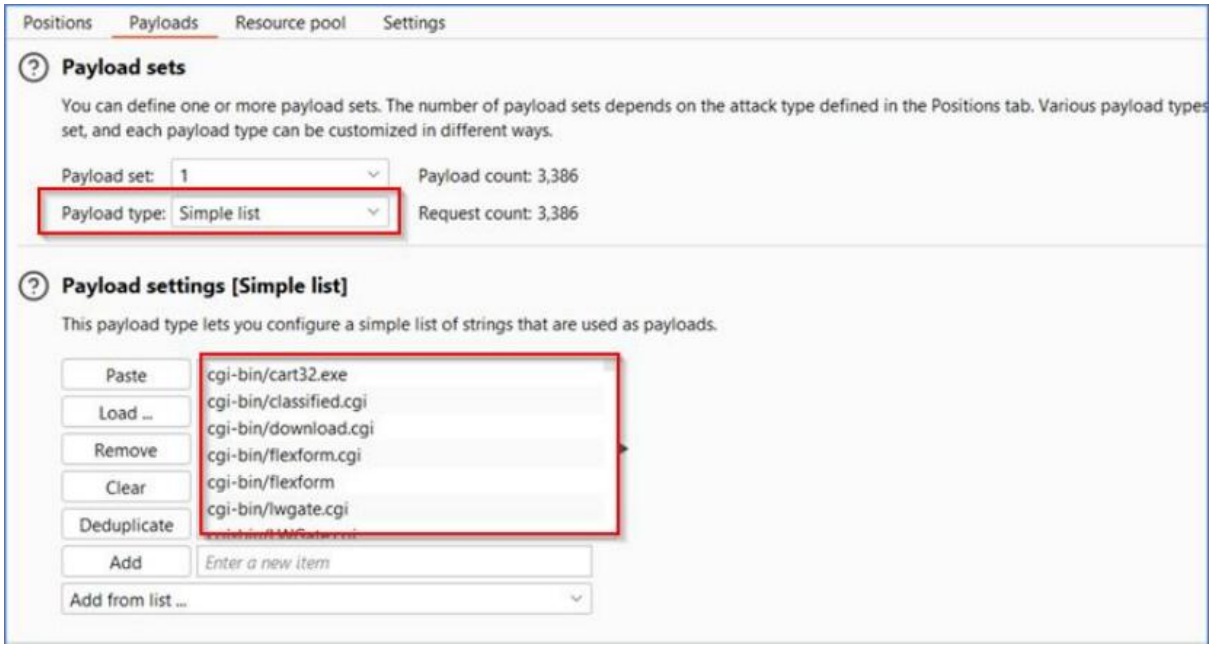
11.1.3 **Execution Steps:**

Step 1: Open browser and intercept the login page.

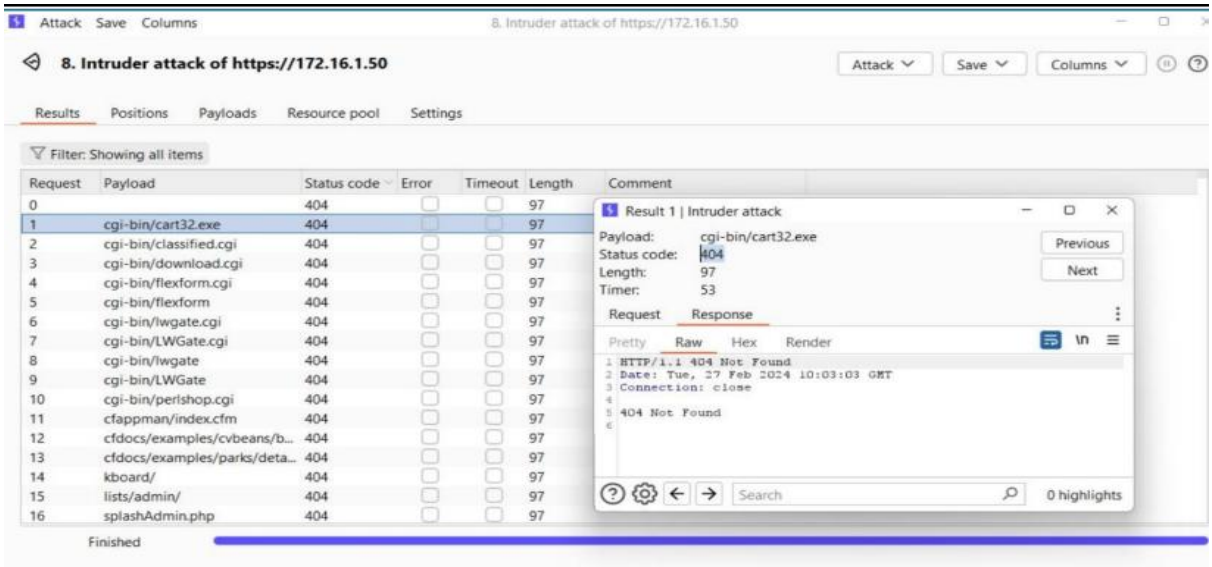


Step 2: Send the request to the intruder and add position to the payload

Step 3: Add cgi directories/ scripting directories in the payload tab.



Step 4: Start the attack and observed that no cgi directory or scripting directory is available by default.



Step4: If we discover a CGI directory or scripting directory, we should verify that the directory does not contain any compilers or interpreters.

11.1.4 **Test Observations:** observe that there are no CGI or scripting directories available

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_COMPILER_FOR_CGI_SCRIPTING	PASS	all the criteria have been met

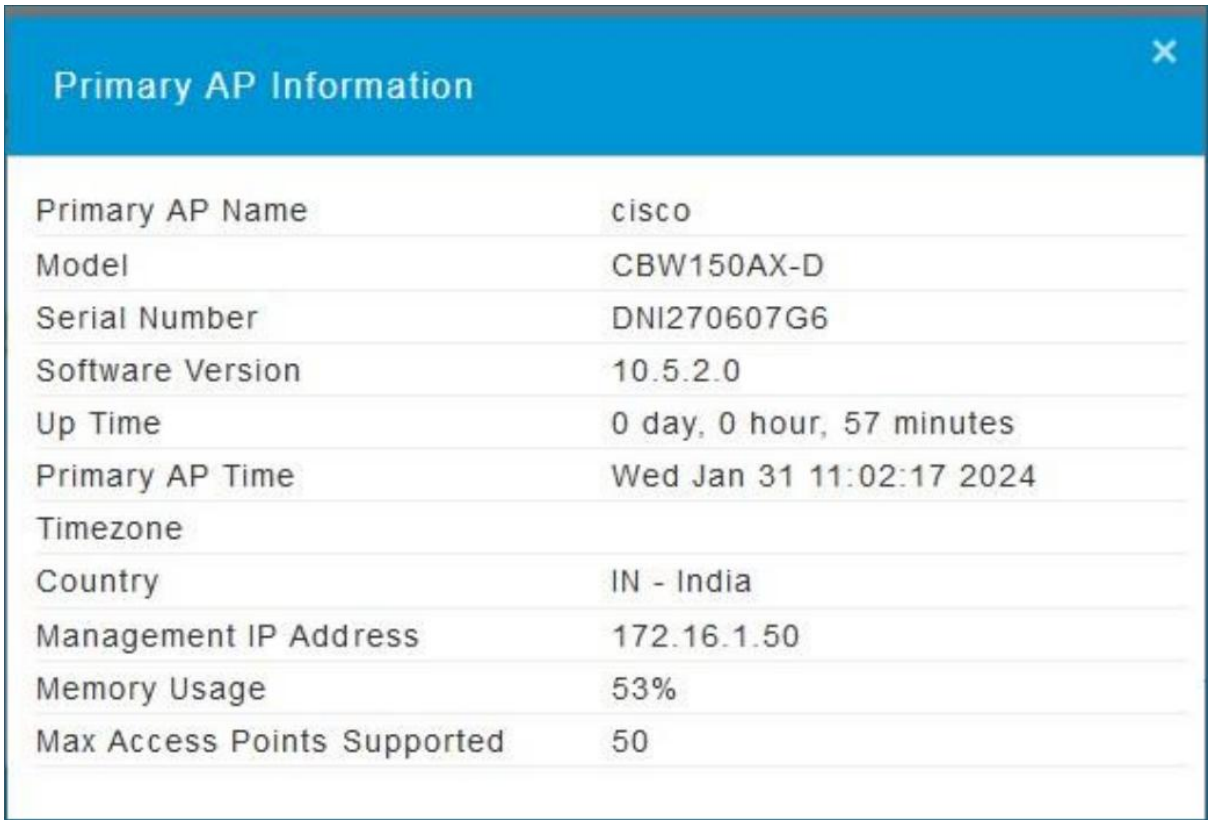
1.11.8: No CGI or other Scripting for uploads

<DUT Details: > WiFi CPE
<DUT Software Version:> cisco 10.5.2.0
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 11: Web Server
2. **<Security Requirement No & Name >** 1.11.8: No CGI or other Scripting for uploads
3. **<Requirement Description: >** If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads.

4. **DUT Confirmation Details**:

Screenshot below shows the DUT name (Primary AP Name) , Model number, Serial Number, Software Version.



DUT Configuration Checksum:

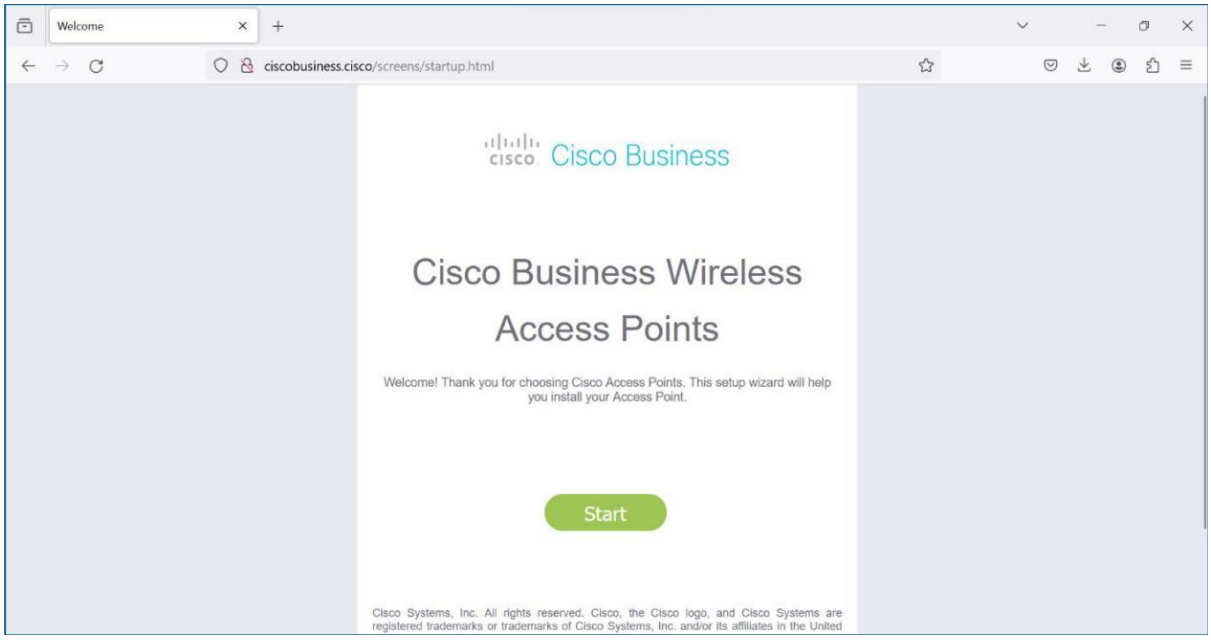
```
PS C:\> certutil -hashfile '.\Configuration files\Configuration 1.txt' SHA256
SHA256 hash of .\Configuration files\Configuration 1.txt:
fab585d185d316ad6c45b1d414d8bf55fa8ef0094173fe9a8a5fa2d3ddc2e43b
CertUtil: -hashfile command completed successfully.
```

5. **DUT Configuration:**

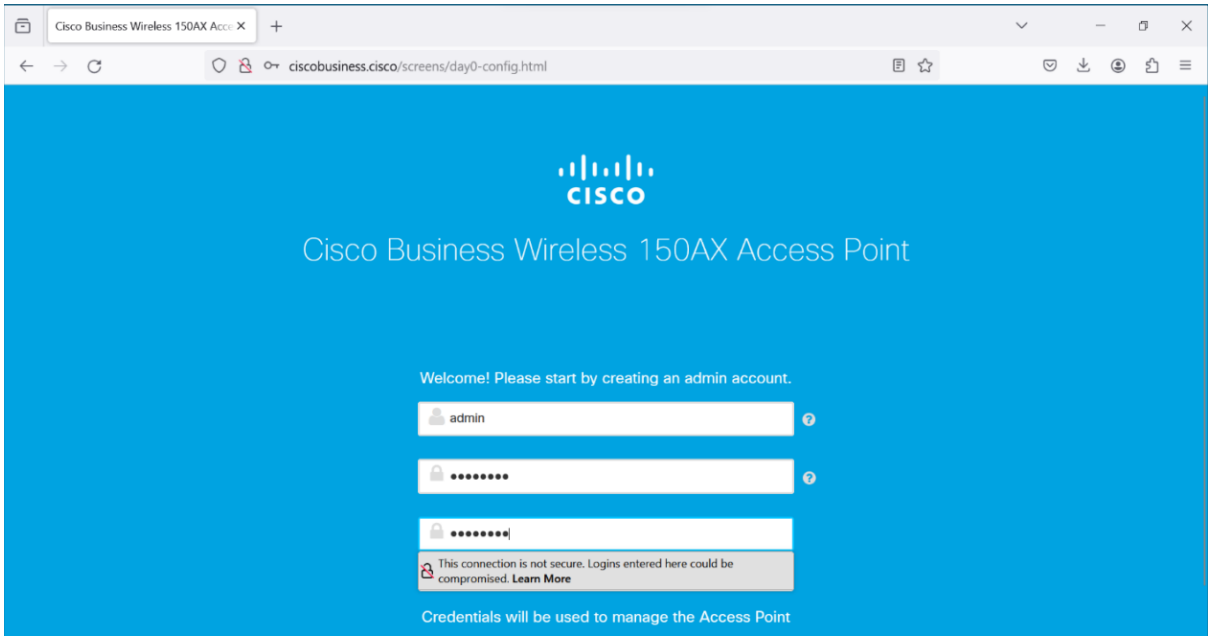
Initial Basic Configuration of CPE

Step 1: Power on the CPE and wait for the CPE to be visible on the Laptop Wi-Fi Scanning "Cisco Business-Setup" or Reset the CPE if not Visible

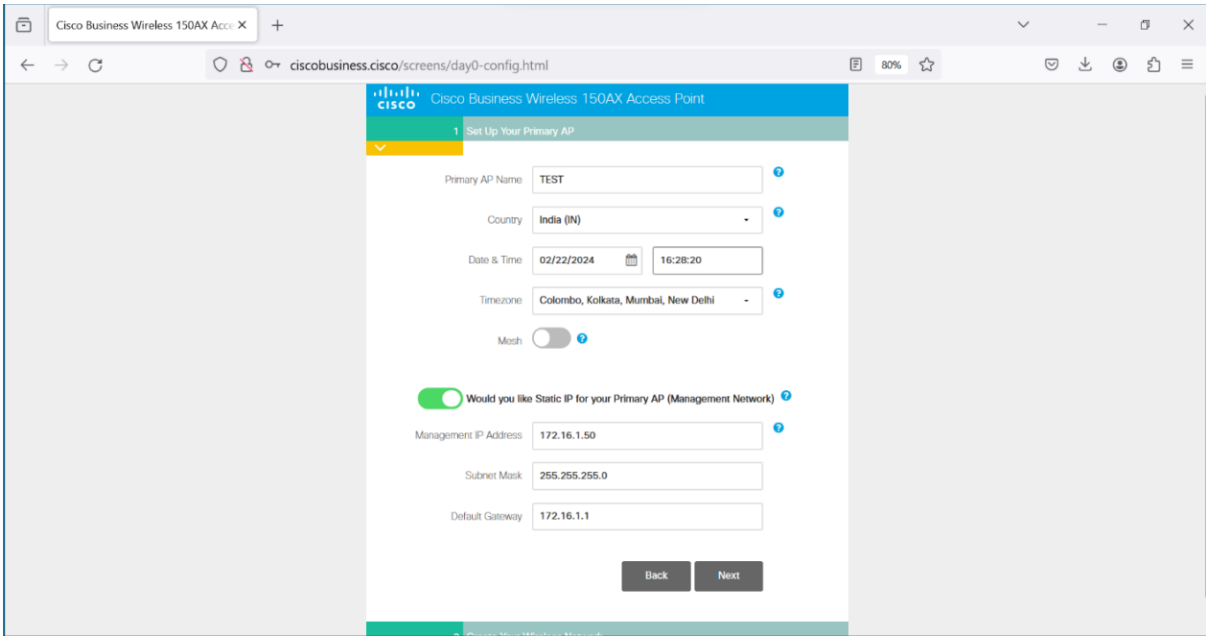
Step 2: Connect To the Wi-Fi Access Point using password " Cisco123" And Navigate to http://ciscobusiness.cisco/screens/startup.html and Click Start as Show in the below Screenshot.



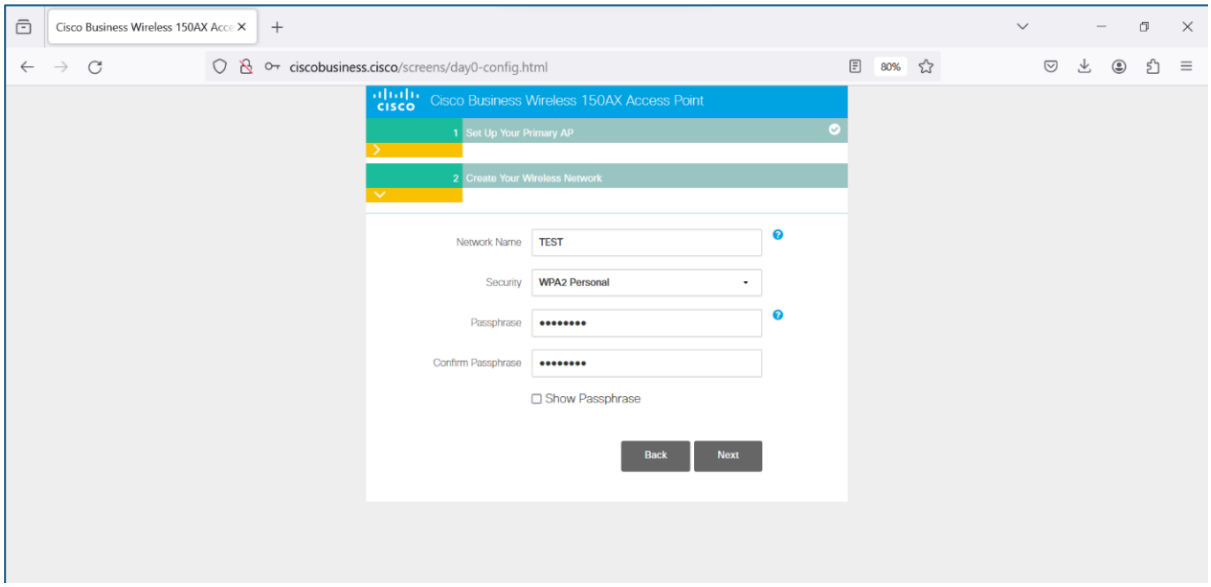
Step 3 : Enter the Desire Credentials for admin account creation and click start



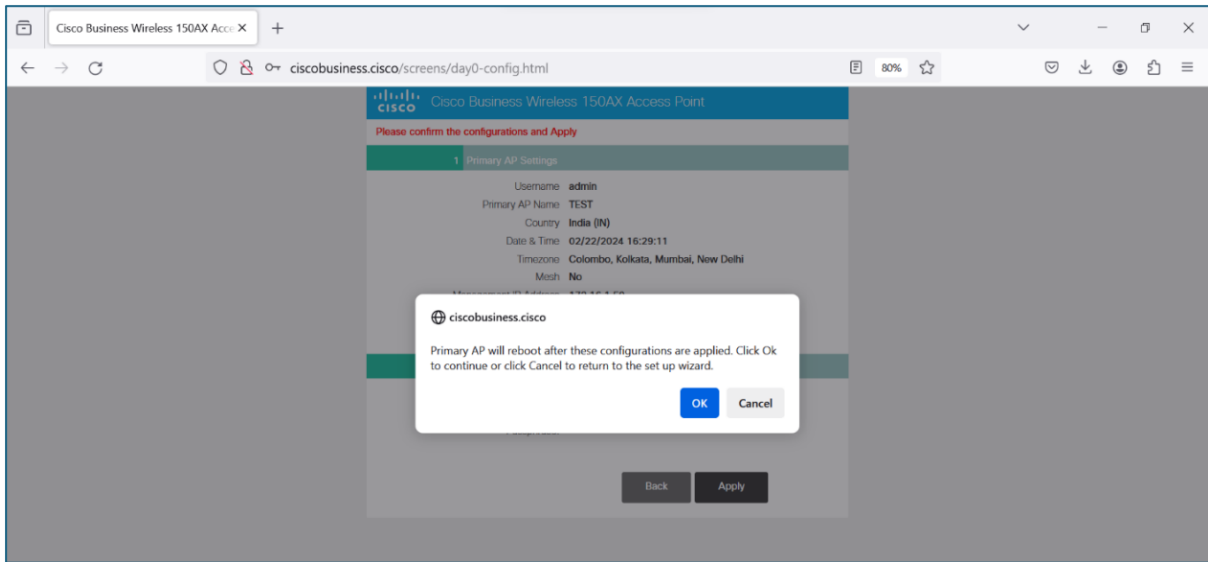
Step 4 : Enter the Desire AP Name and Select Static IP Configuration if required and click Next



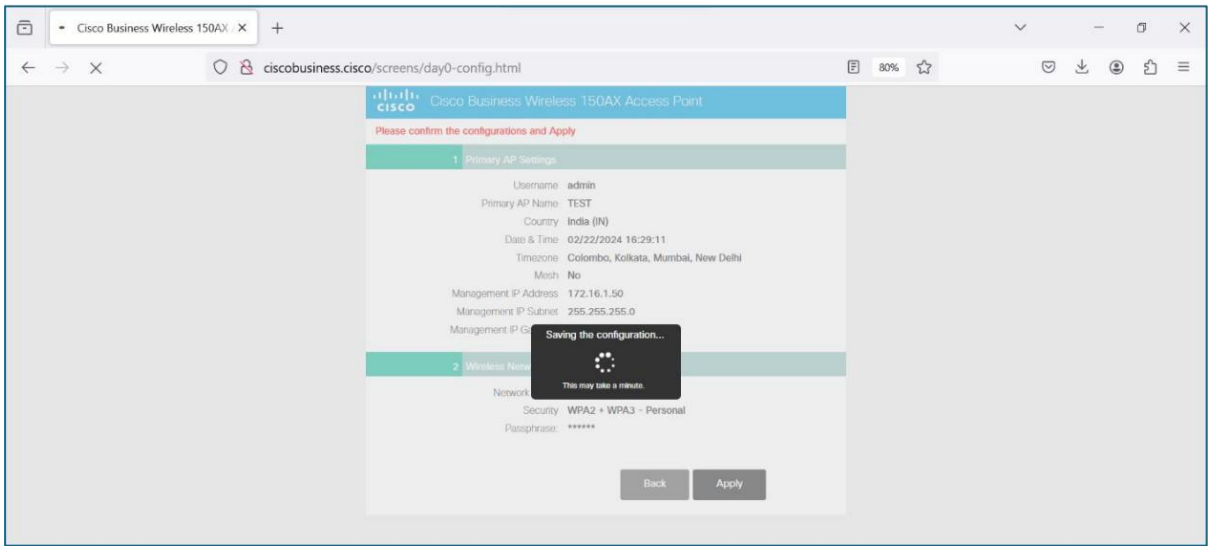
Step 5 : Enter the Desire Network Name and Passphrase and click Next

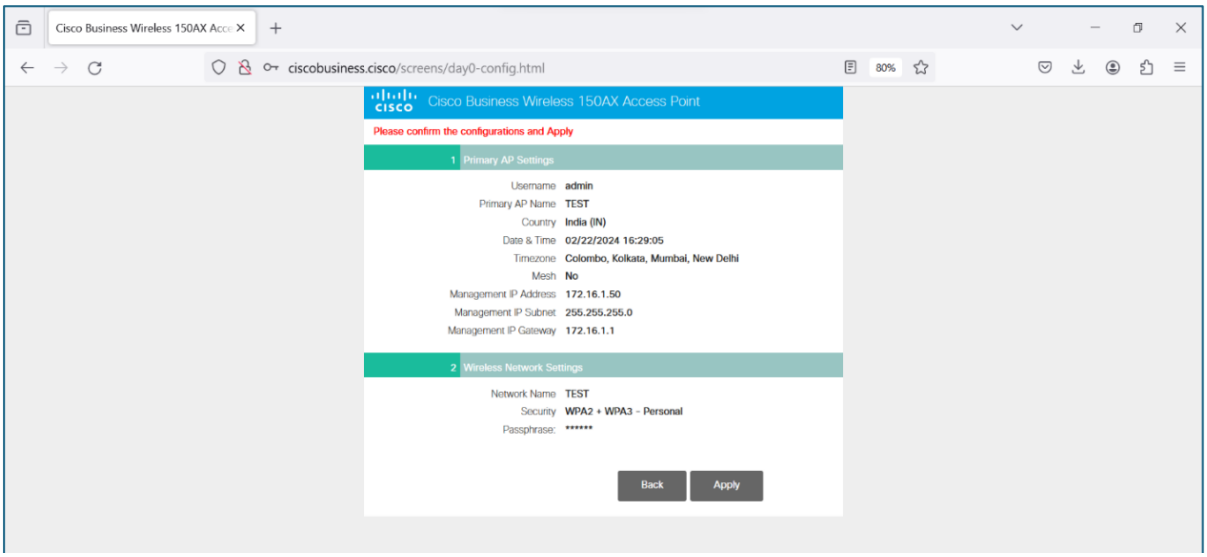


Step 6 : Verify the Configuration done and Click on Apply



Step 7 : A popup will appear on the screen “Primary AP will reboot after these configurations are applied. Click Ok to continue or click Cancel to return to the set-up wizard.”





Step 8: Finished Step Now the AP is Ready to Be used.

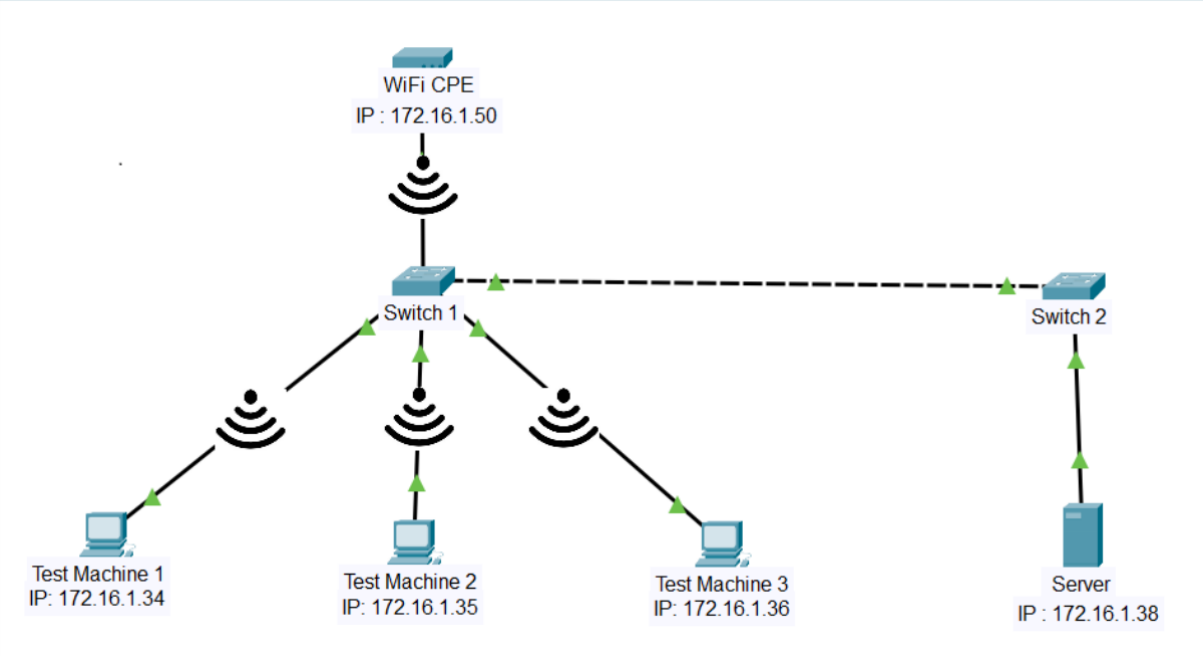
6. **Preconditions**
   - The tester has administrative privileges
   - A tester machine is available.
   - Test environment with a Terminal.
   - Test Environment with a Browser
   - If the web server is configured with CGI/Scripting on, this test applies
   - The tester checks the vendor documentation for the “upload directory”

7. **Test Objective**: To test whether the upload directory is equal to the CGI/Scripting directory.

8. **Test Plan:**
   8.1 Number of Test Scenarios:
   8.1.1. Test Scenario for CGI/scripting and Upload Directory

- This test scenario is regarding CGI/scripting and Upload Directory

8.2 Test Bed Diagram



8.3 Tools Required

- Dirsearch (cgi Wordlist)
- Default DUT configuration tool for Web Server as per vendor. It can be command line, GUI or any other interface as specified in vendor documentation.

8.4 Test Execution Steps

- Power up the testbed
- The tester tries to access the Shell of Web Server.
- Consult the web server configuration to identify all directories used for CGI or other scripting components.
- In case the DUT is using other than CGI they must give the information about different technology used and further tests should be performed on that technology. (This document only deals with CGI Scripts)
- Consult the vendor documentation to identify all directories used for upload.
- The tester manually checks that the CGI and upload directory are not different and verify it in the DUT.
- The tester will run some web scanning tools like Nikto, to get the detailed information and verify that the CGI and upload directory are different.

9. **Expected Results for Pass:**

- The configured upload directory is different from the CGI/Scripting directory.
- Additional evidence might be provided that shows that the web server has no write rights for the CGI/Scripting directory.

10. **Expected Format of Evidence:** A part of the configuration file / screenshot of the configuration showing that the web server is properly configured.

11. **Test Execution:**

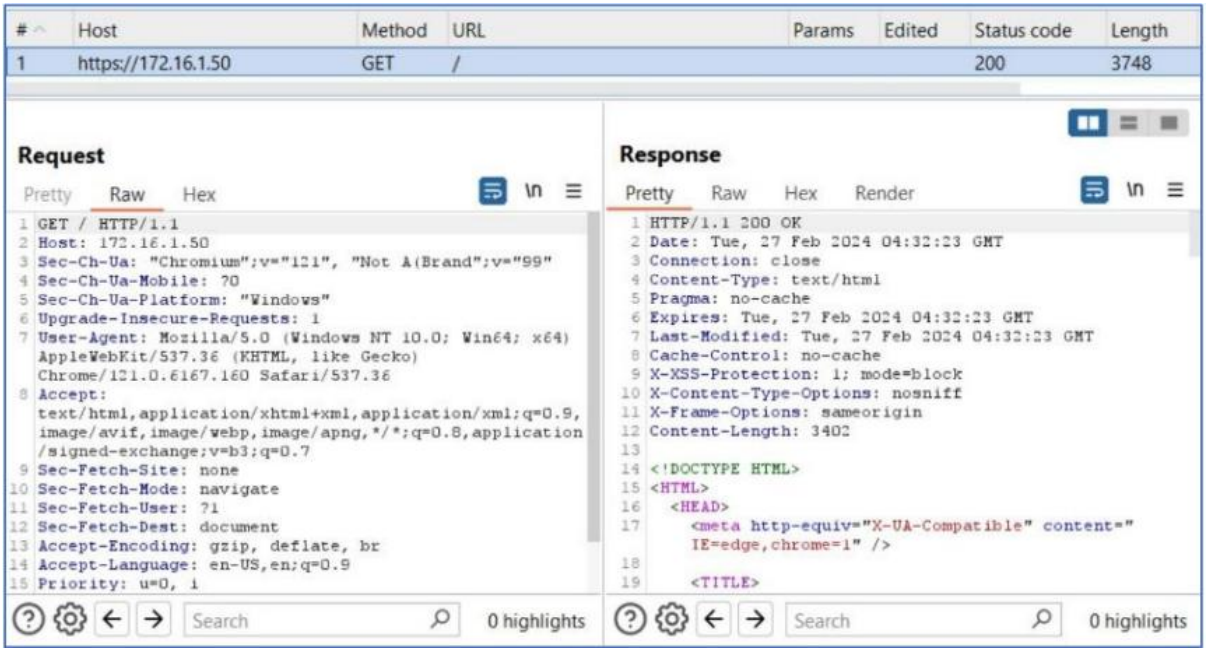
11.1 Test Case Number: 01

11.1.1 **Test Case Name:** TC_NO_CGI_OR_SCRIPTING_FOR_UPLOADS

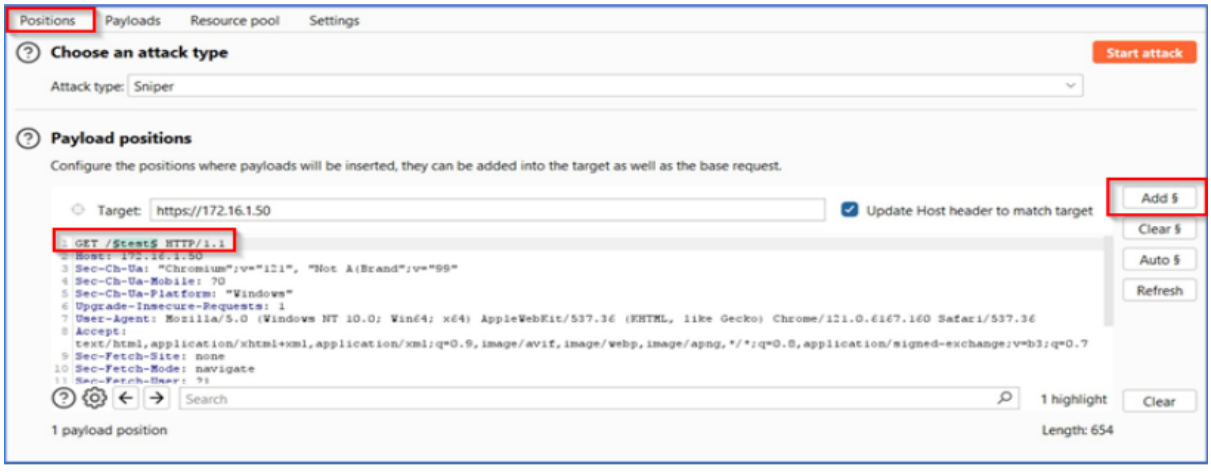
11.1.2 **Test Case Description:** To test whether the upload directory is equal to the CGI/Scripting directory.

11.1.3 **Execution Steps:**

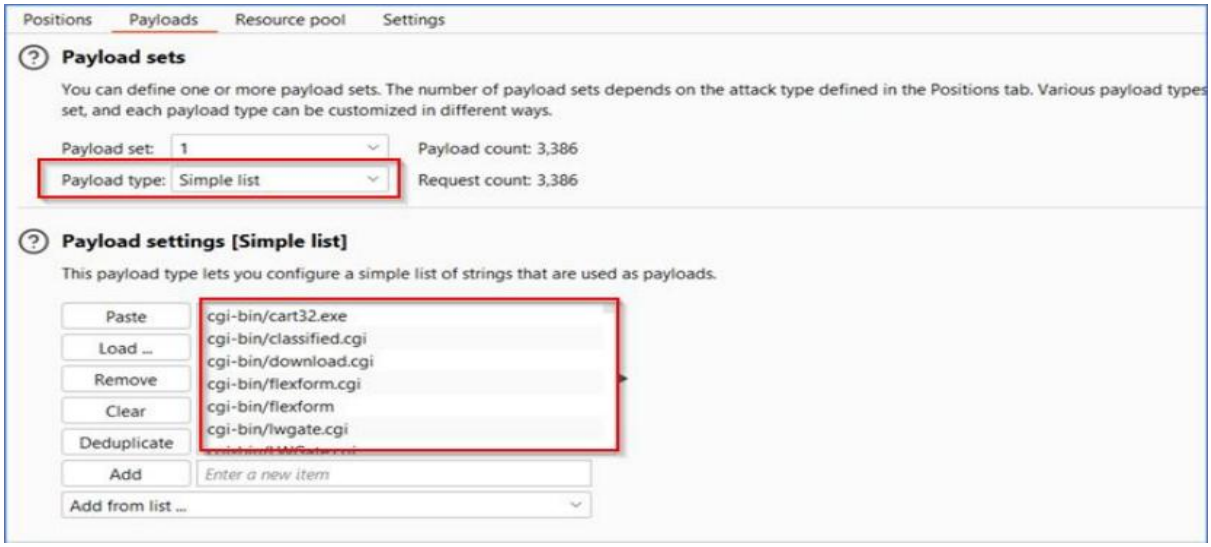
Step 1: Open browser and intercept the login page.



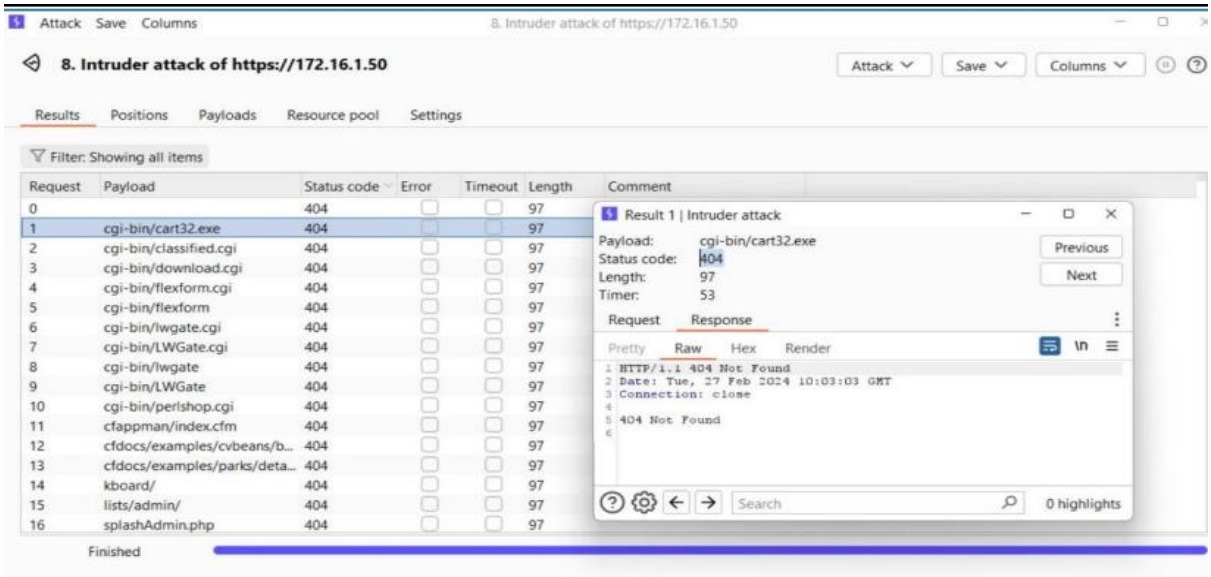
Step 2: Send the request to the intruder and add position to the payload



Step 3: Add cgi directories/ scripting directories in the payload tab.



Step 4: Start the attack and observed that no cgi directory or scripting directory is available by default.



Step4: If we discover a CGI directory or scripting directory, we should verify that the directory does not have wright right.

Note: To verify that the directory does not have write permissions, we may require support from the OEM.

Step 5: I should be ensured that CGI/scripting directory and upload directory are different. Additionally, check does not have write permissions.

11.1.4 **Test Observations:** observed that no CGI or scripting directories are being used.

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_CGI_OR_SCRIPTING_FOR_UPLOADS	Not decided	Need OEM support

1.11.9: No execution of system Commands with SSI

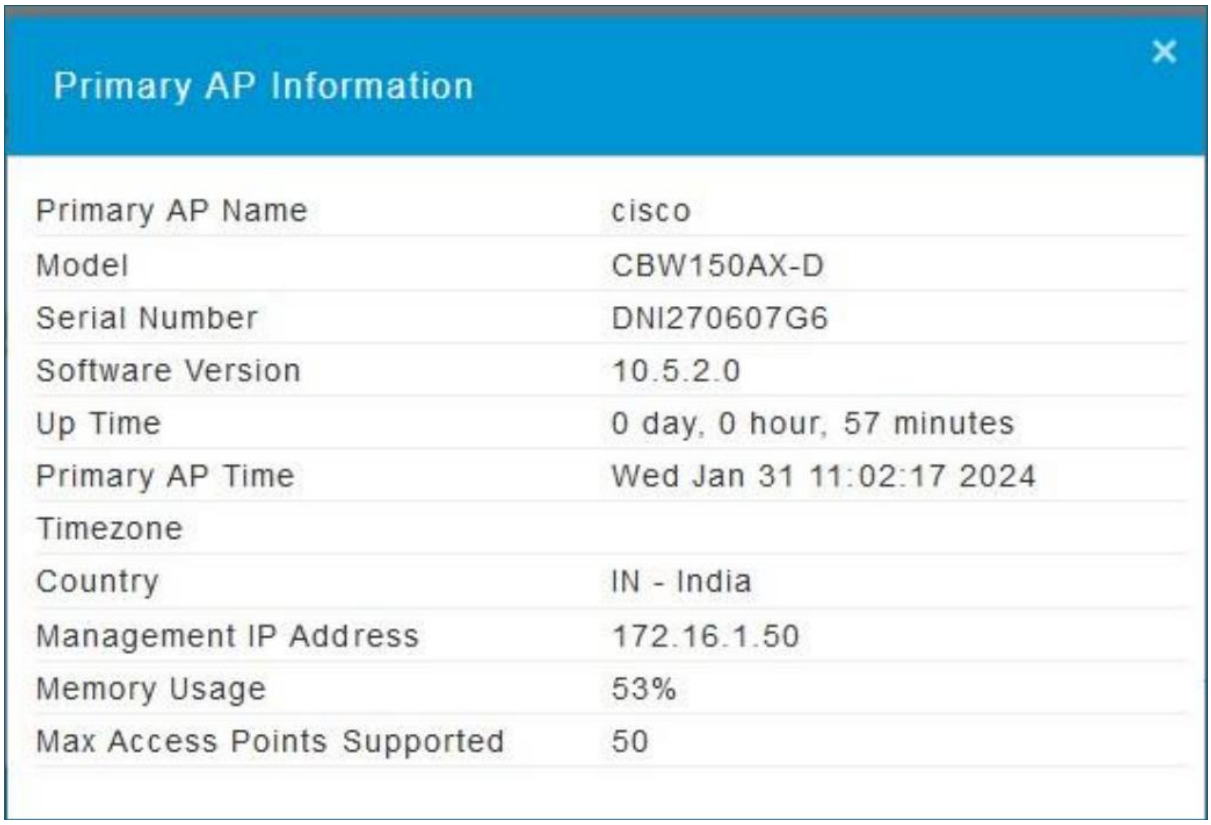
<DUT Details: > WiFi CPE
<DUT Software Version:> cisco 10.5.2.0
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 11: Web Server
2. **<Security Requirement No & Name >** 1.11.9: No execution of system Commands with SSI
3. **<Requirement Description: >** If Server Side Includes (SSI) is active, the execution of system commands shall be

deactivated.

4. **DUT Confirmation Details**:

Screenshot below shows the DUT name (Primary AP Name) , Model number, Serial Number, Software Version.



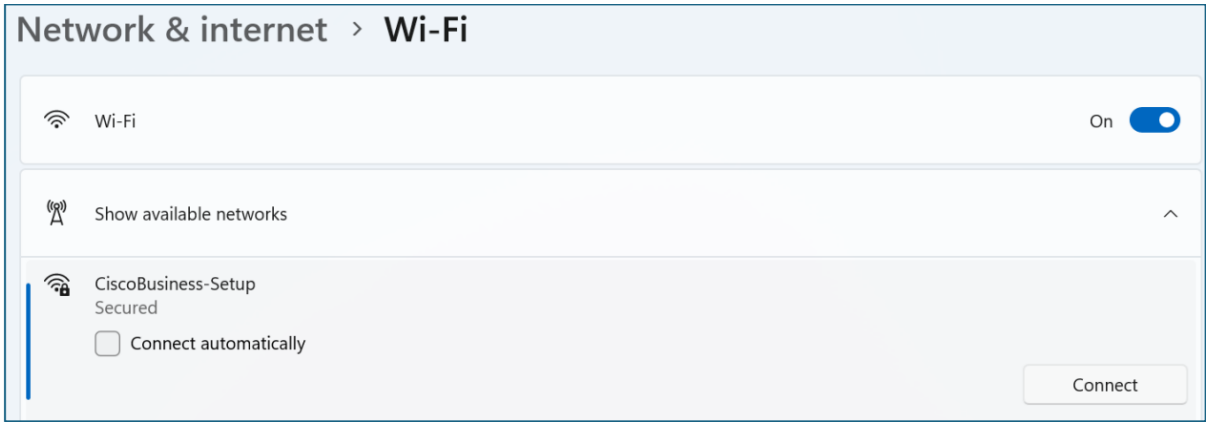
DUT Configuration Checksum:

```
PS C:\> certutil -hashfile '.\Configuration files\Configuration 1.txt' SHA256
SHA256 hash of .\Configuration files\Configuration 1.txt:
fab585d185d316ad6c45b1d414d8bf55fa8ef0094173fe9a8a5fa2d3ddc2e43b
CertUtil: -hashfile command completed successfully.
```

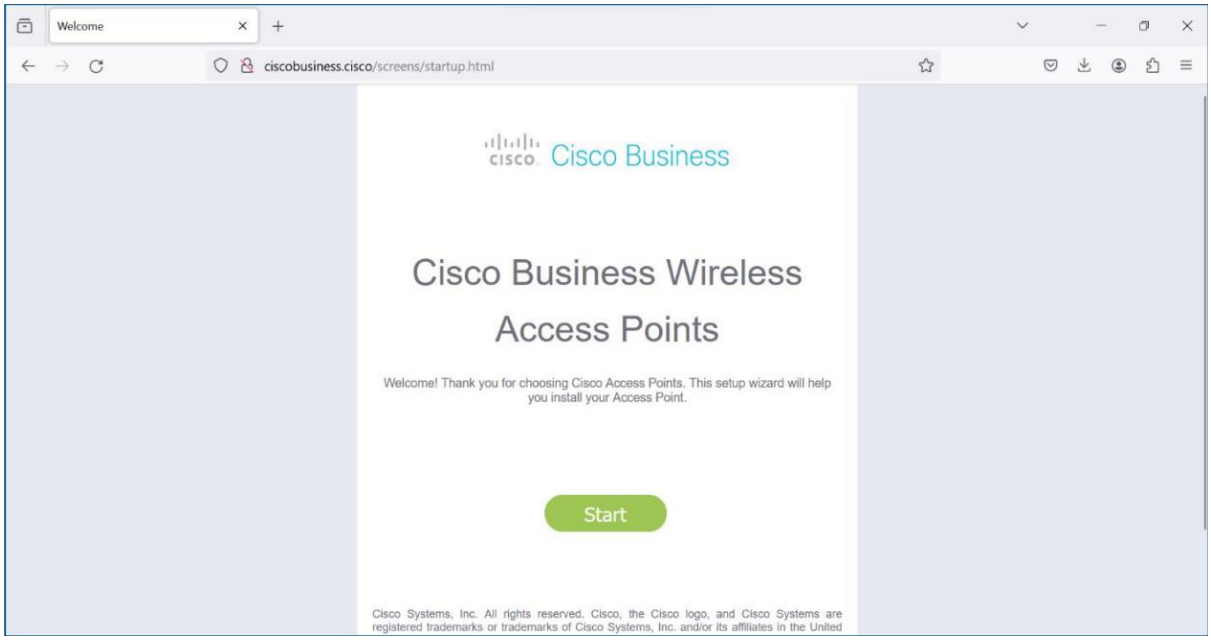
5. **DUT Configuration:**

Initial Basic Configuration of CPE

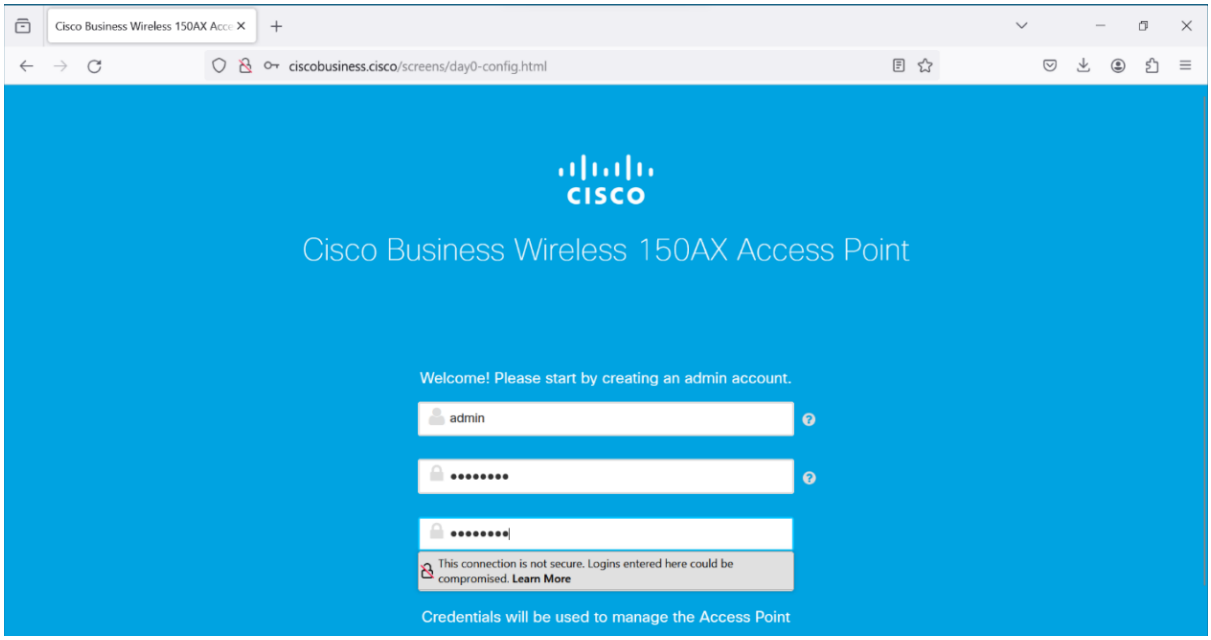
Step 1: Power on the CPE and wait for the CPE to be visible on the Laptop Wi-Fi Scanning "Cisco Business-Setup" or Reset the CPE if not Visible



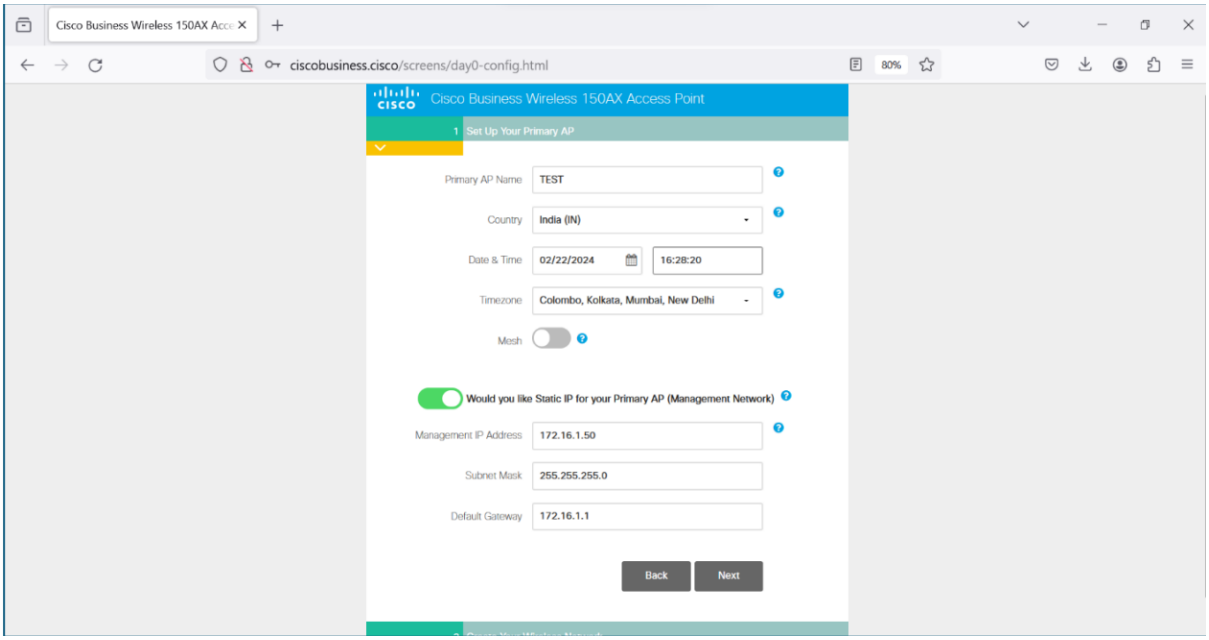
Step 2: Connect To the Wi-Fi Access Point using password " Cisco123" And Navigate to http://ciscobusiness.cisco/screens/startup.html and Click Start as Show in the below Screenshot.



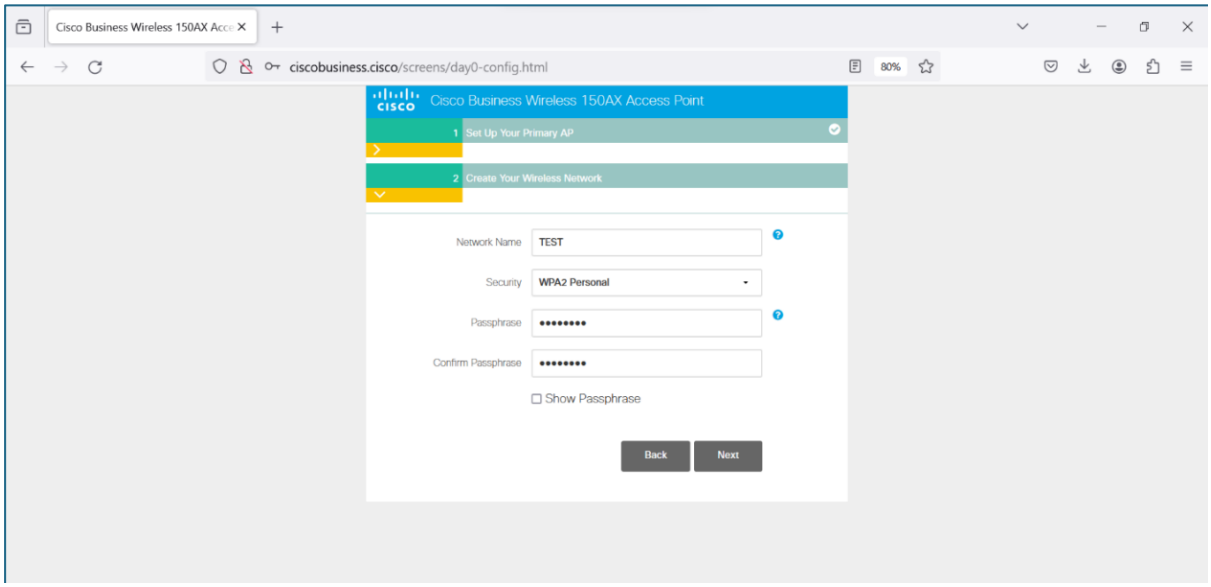
Step 3 : Enter the Desire Credentials for admin account creation and click start



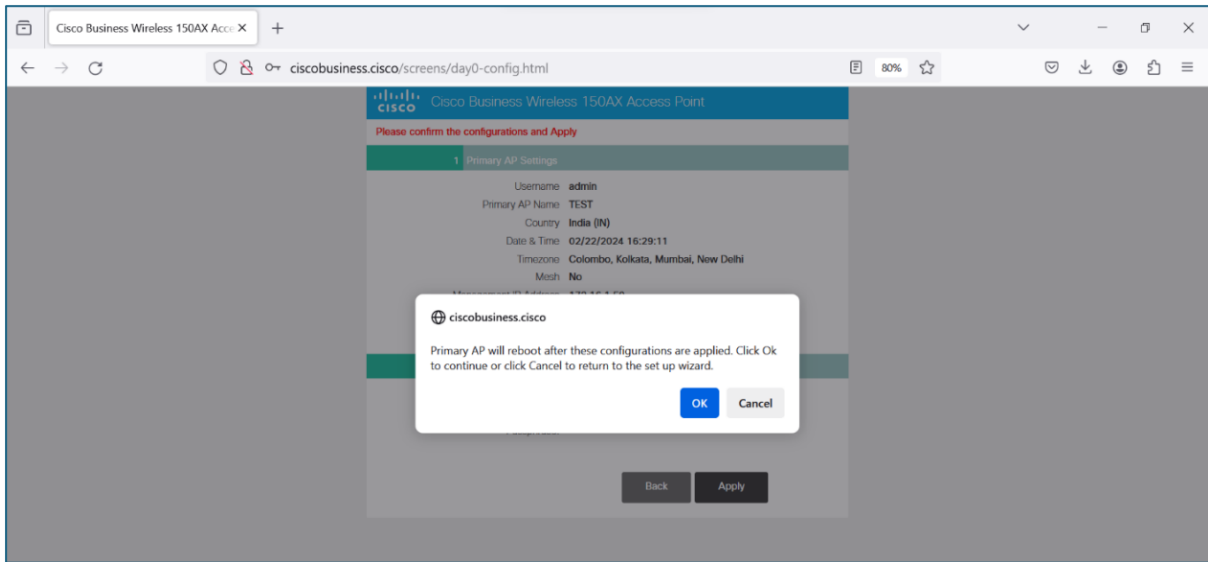
Step 4 : Enter the Desire AP Name and Select Static IP Configuration if required and click Next



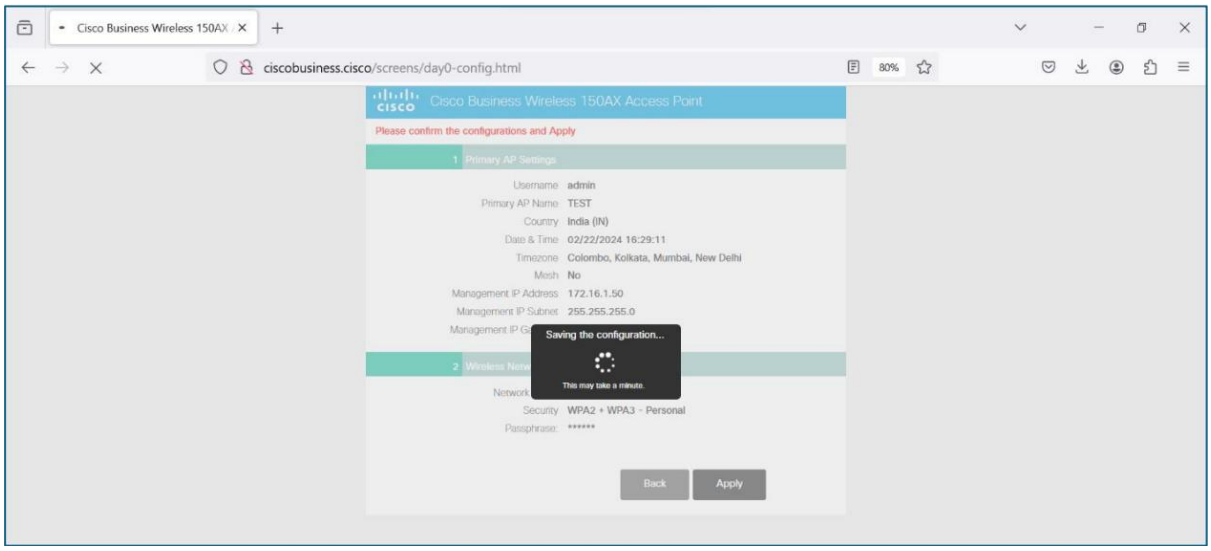
Step 5 : Enter the Desire Network Name and Passphrase and click Next

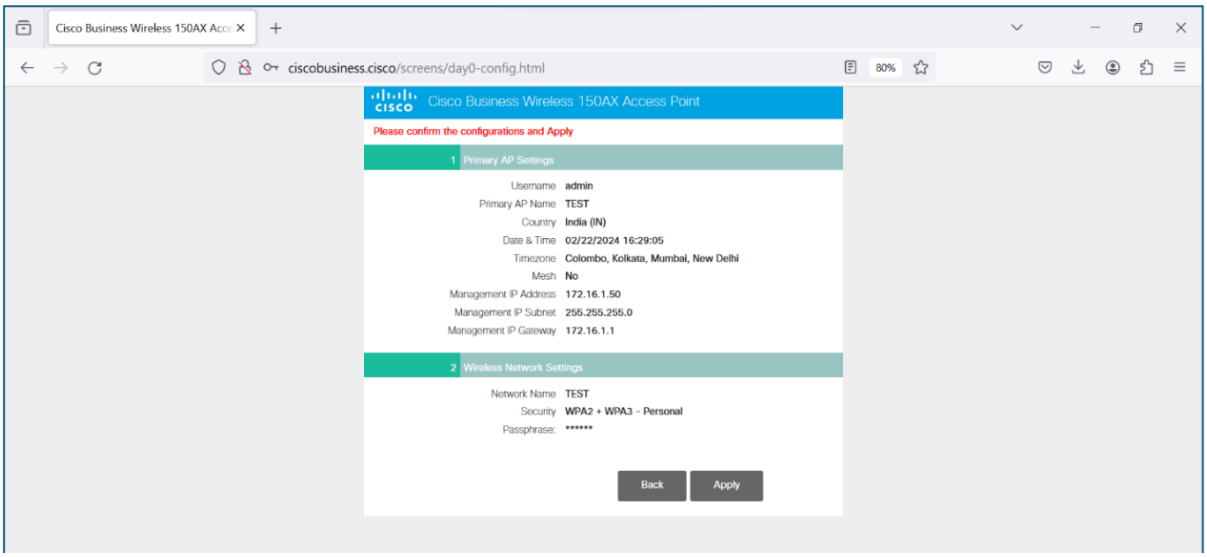


Step 6 : Verify the Configuration done and Click on Apply



Step 7 : A popup will appear on the screen “Primary AP will reboot after these configurations are applied. Click Ok to continue or click Cancel to return to the set-up wizard.”





Step 8: Finished Step Now the AP is Ready to Be used.

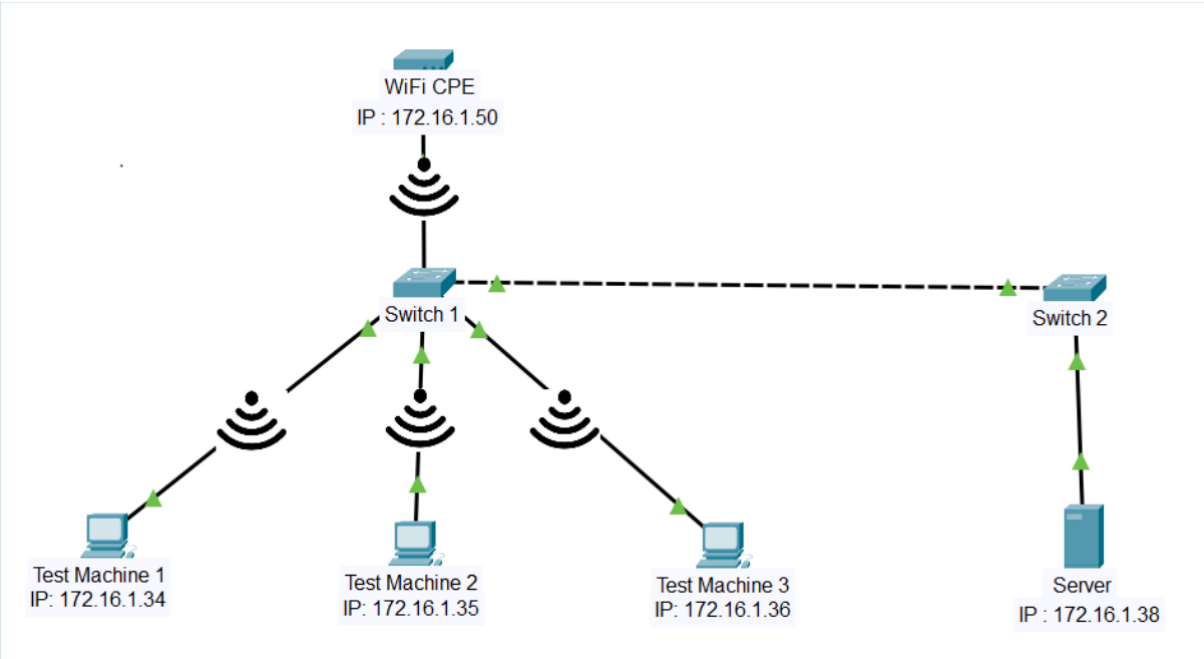
6. **Preconditions**
   - The tester has administrative privileges.
   - If the web server is configured with SSI active, this test applies.
   - A tester machine is available.
   - Test environment with a Terminal.
7. **Test Objective**: To test whether it is possible to use the exec directive and if so, whether it can be used for system commands.

8. **Test Plan:**

   8.1 Number of Test Scenarios:

   8.1.1. Test Scenario for SSI - This test scenario is regarding SSI.

   8.2 Test Bed Diagram



8.3 Tools Required

- Dirsearch (cgi Wordlist)
- Default DUT configuration tool for Web Server as per vendor. It can be command line, GUI or any other interface as specified in vendor documentation.

8.4 Test Execution Steps

- Power up the testbed
- The tester tries to access the Shell of Web Server.
- The tester checks whether execution of system commands is disabled in the web server configuration.
- The tester actually attempts to use the exec directive in an SSI file with and without system commands.
- Some web scanning tools like Nikto should be used to scan the webserver for the SSI exec.

9. **Expected Results for Pass:**
   - The execution of system commands via SSIs exec directive is disabled in the web server configuration.
   - It is impossible to execute system commands via SSIs exec directives.

10. **Expected Format of Evidence:** A part of the configuration file / screenshot of the configuration showing that the web server is properly configured.

11. **Test Execution:**

11.1 Test Case Number: 01

11.1.1 **Test Case Name:** TC_NO_EXECUTION_OF_SYSTEM_COMMANDS

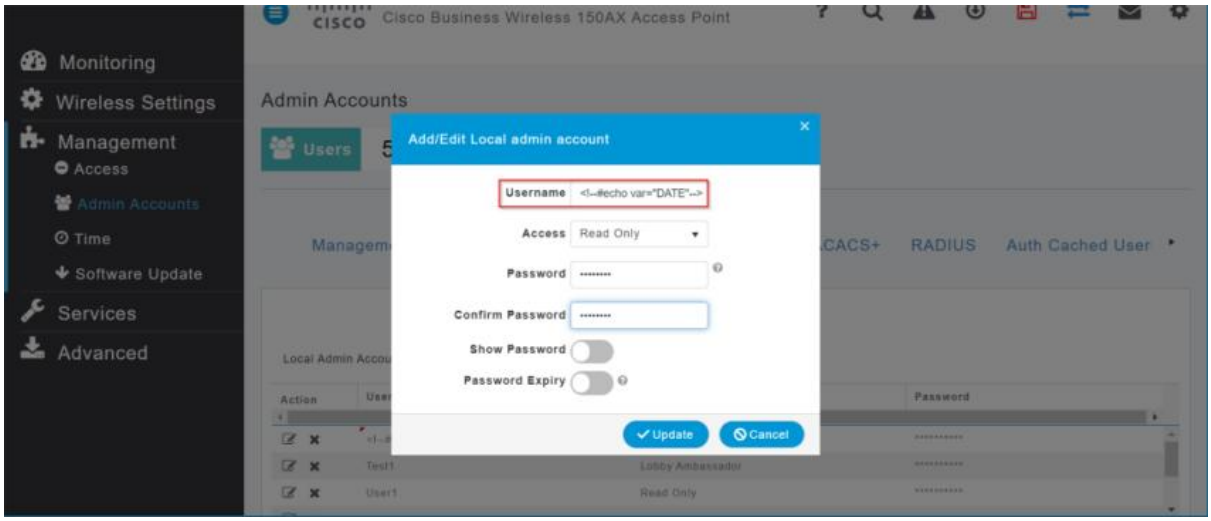
11.1.2 **Test Case Description:** To test whether DUT is restricting execution of system

commands with SSI (server side includes)

11.1.3 **Execution Steps:**

Step 1: Open browser, navigate to https://172.16.1.50 and login

Step 2: Navigate to Administrator panel then Add profile then in the profile name put the payload "←#echo var="DATE"-->"



Step 3: Click f12 and click on "Apply to Device" and observe the network traffic.

Step 4: Observe that the request has been proceeded by DUT.

Step 5: Verifying whether the DUT have SSI active using Nikto tool.

11.1.4 **Test Observations:** Observed that SSI is not active

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_CGI_OR_SCRIPTING_FOR_UPLOADS	Pass	

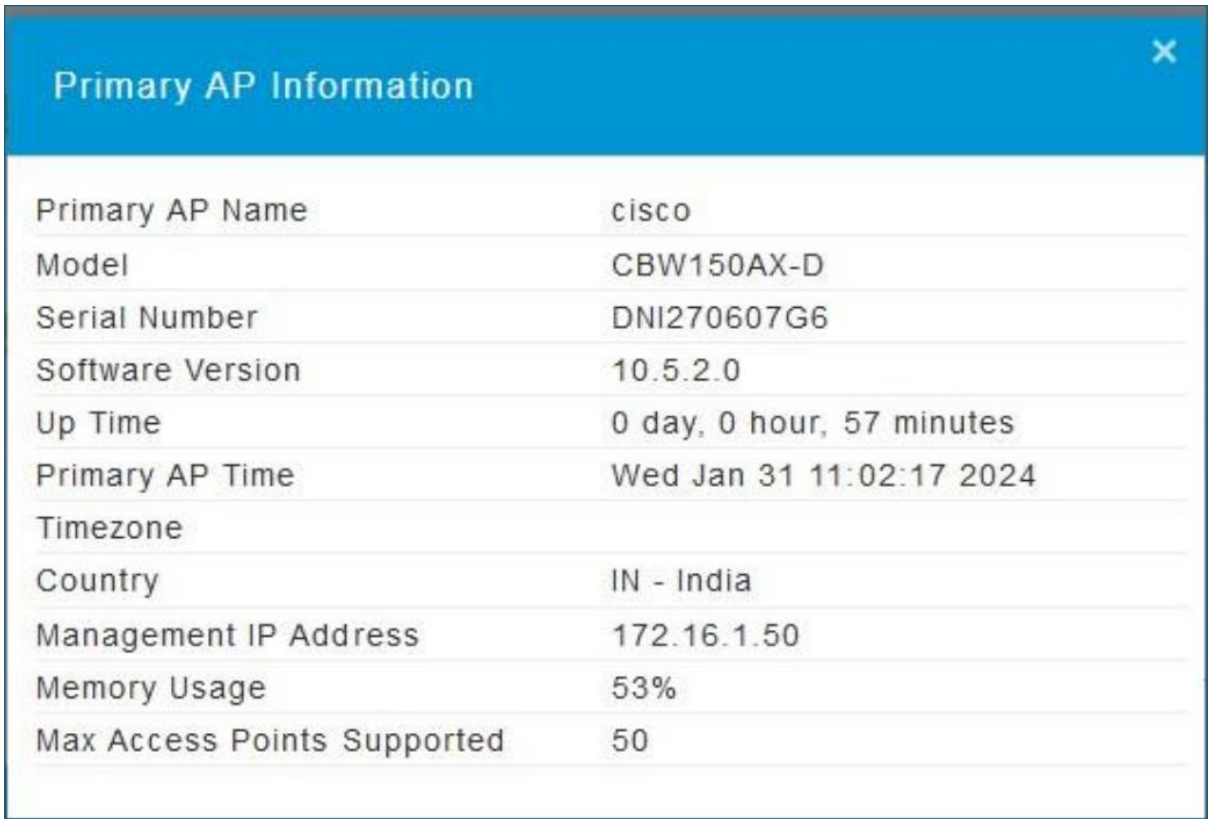
1.11.10: No Default Content

<DUT Details: > WiFi CPE
<DUT Software Version:> cisco 10.5.2.0
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 11: Web Server
2. **<Security Requirement No & Name >** 1.11.10: No Default Content
3. **<Requirement Description: >** Default content (examples, help files, documentation, aliases) that is provided with the standard installation of the web server shall be removed.

4. **DUT Confirmation Details**:

Screenshot below shows the DUT name (Primary AP Name) , Model number, Serial Number, Software Version.



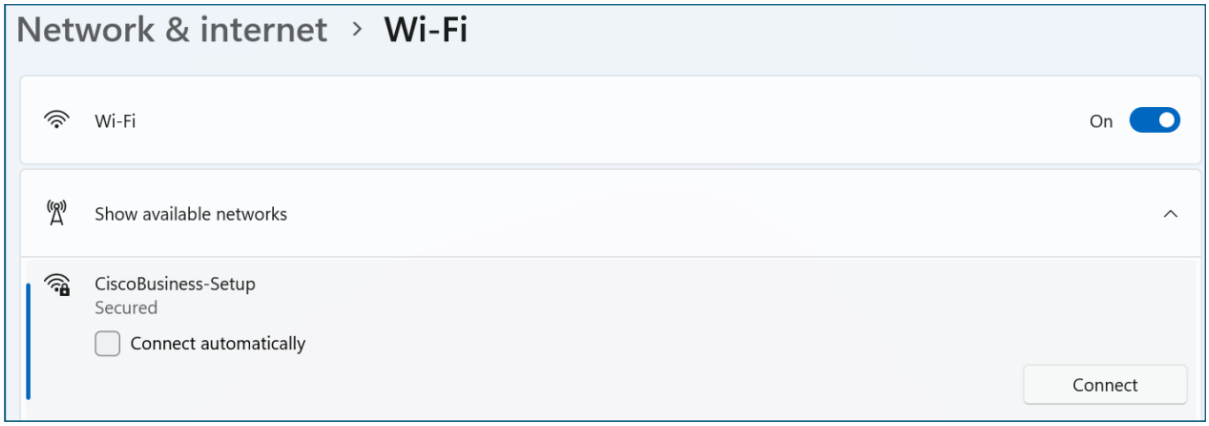
DUT Configuration Checksum:

```
PS C:\> certutil -hashfile '.\Configuration files\Configuration 1.txt' SHA256
SHA256 hash of .\Configuration files\Configuration 1.txt:
fab585d185d316ad6c45b1d414d8bf55fa8ef0094173fe9a8a5fa2d3ddc2e43b
CertUtil: -hashfile command completed successfully.
```

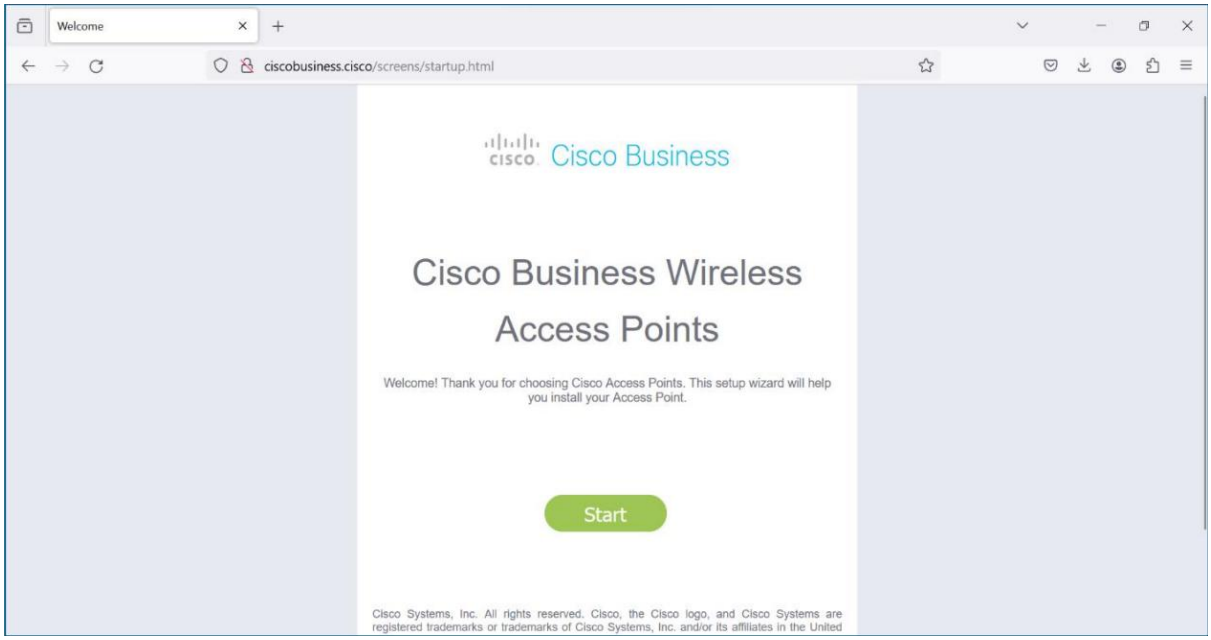
5. **DUT Configuration:**

Initial Basic Configuration of CPE

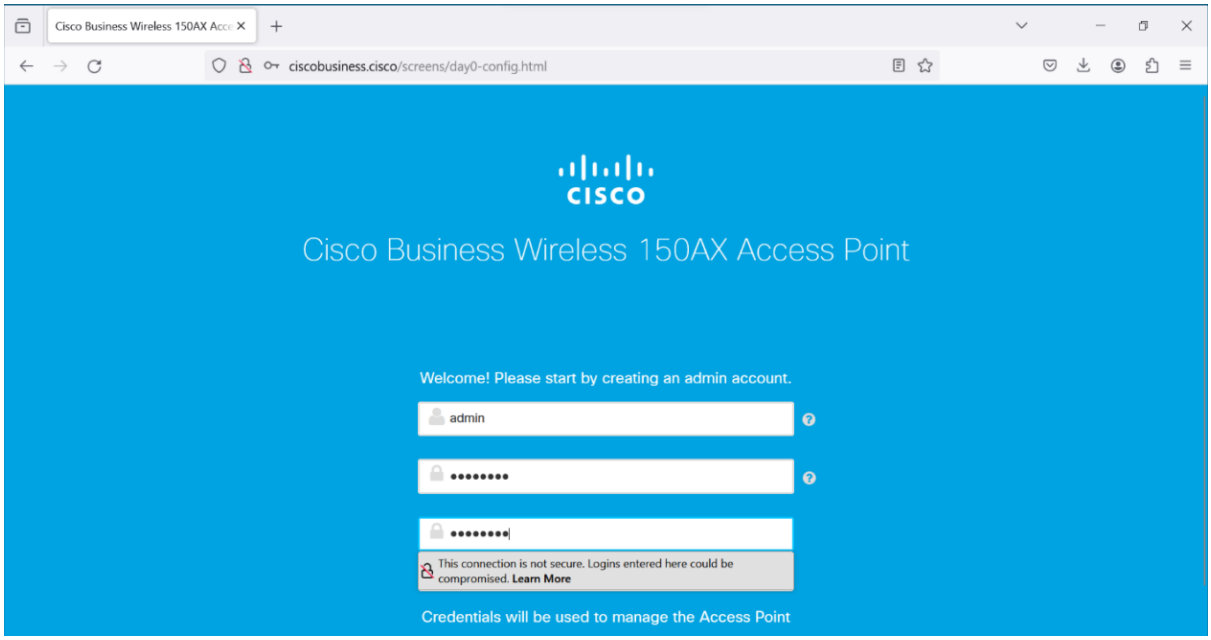
Step 1: Power on the CPE and wait for the CPE to be visible on the Laptop Wi-Fi Scanning "Cisco Business-Setup" or Reset the CPE if not Visible



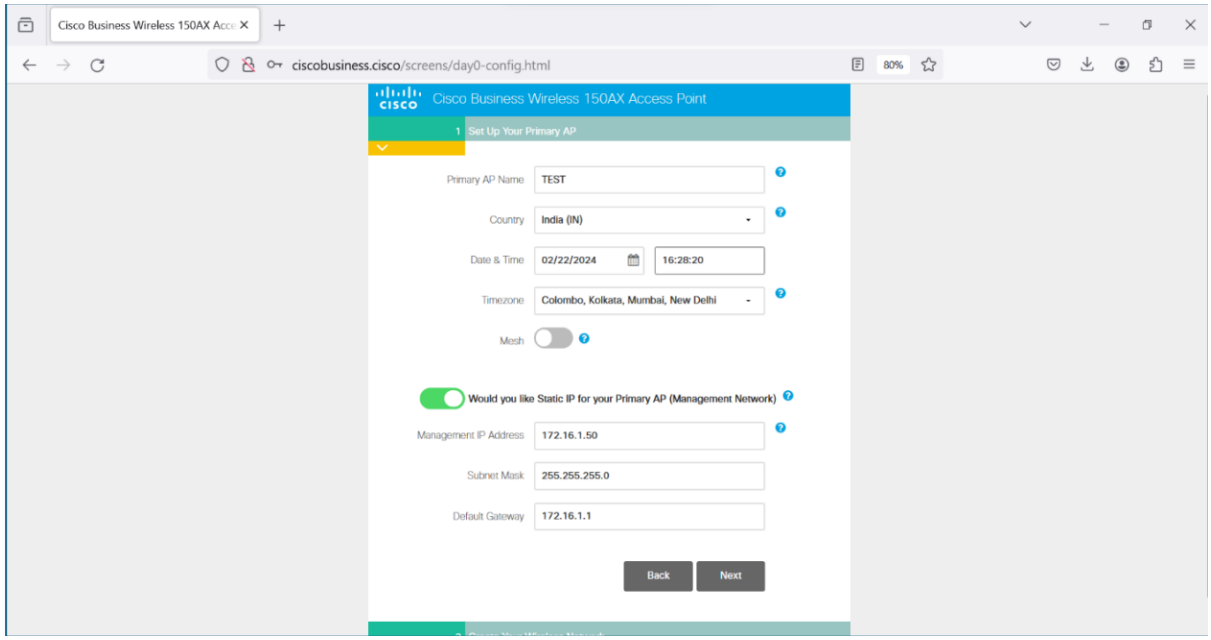
Step 2: Connect To the Wi-Fi Access Point using password " Cisco123" And Navigate to http://ciscobusiness.cisco/screens/startup.html and Click Start as Show in the below Screenshot.



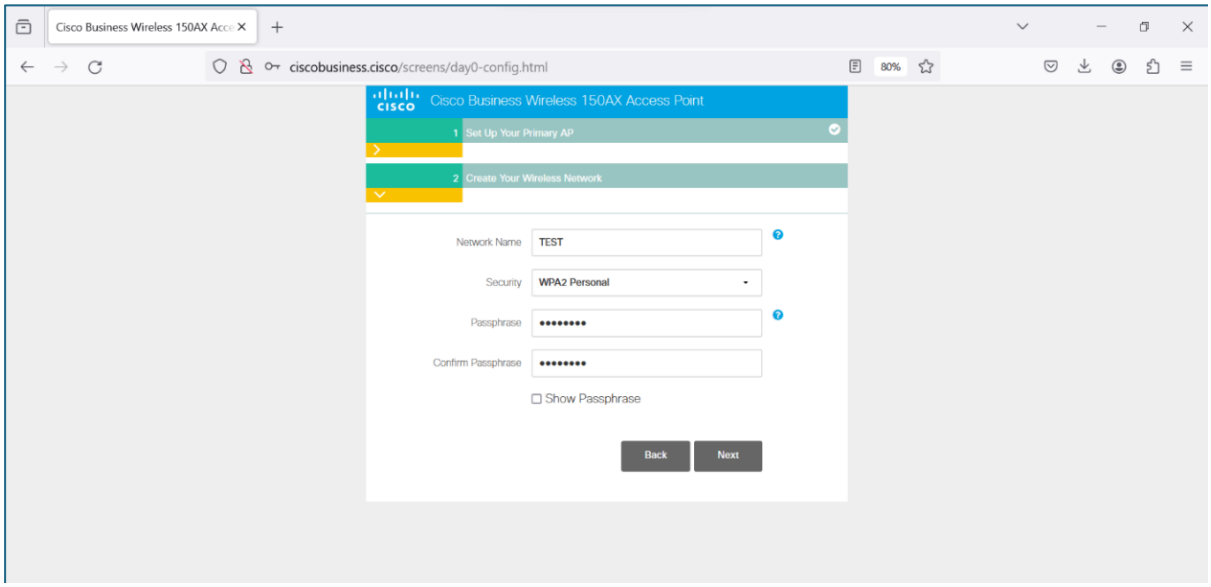
Step 3 : Enter the Desire Credentials for admin account creation and click start



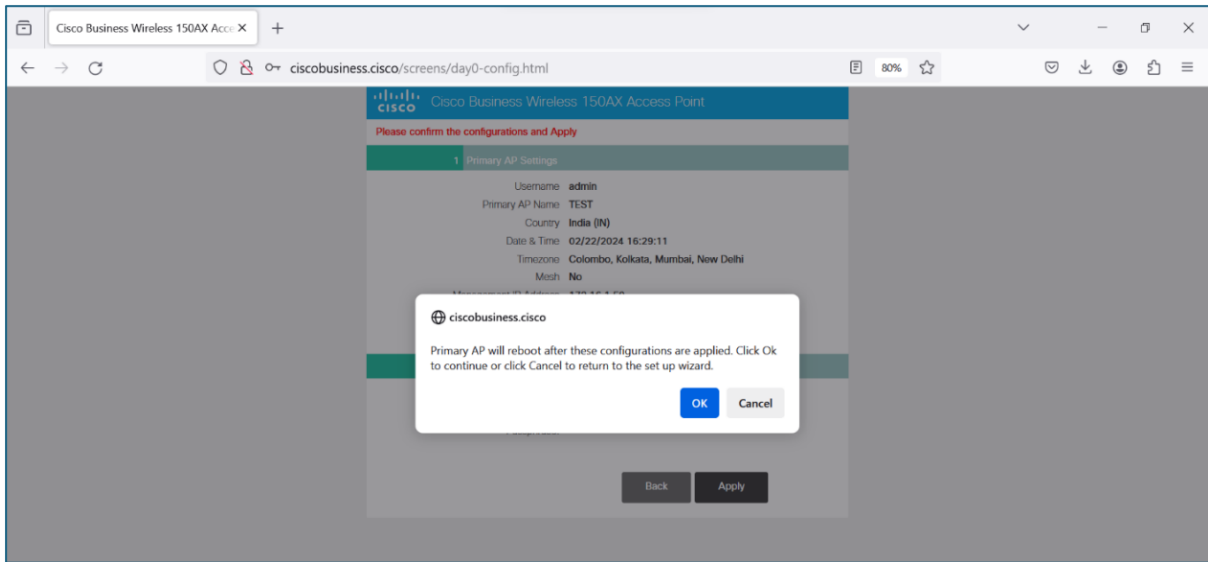
Step 4 : Enter the Desire AP Name and Select Static IP Configuration if required and click Next



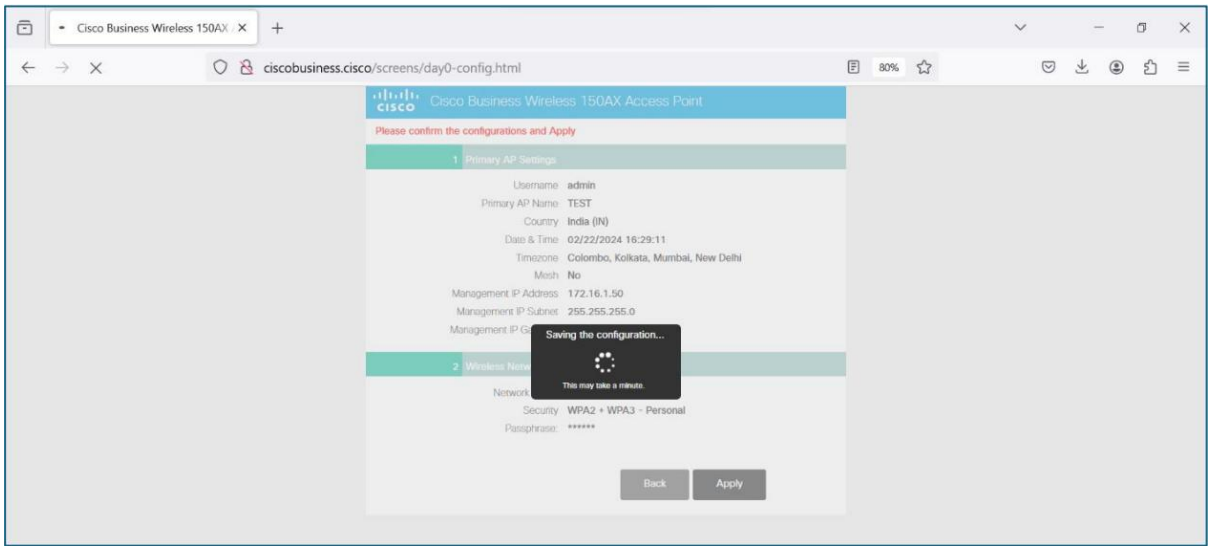
Step 5 : Enter the Desire Network Name and Passphrase and click Next

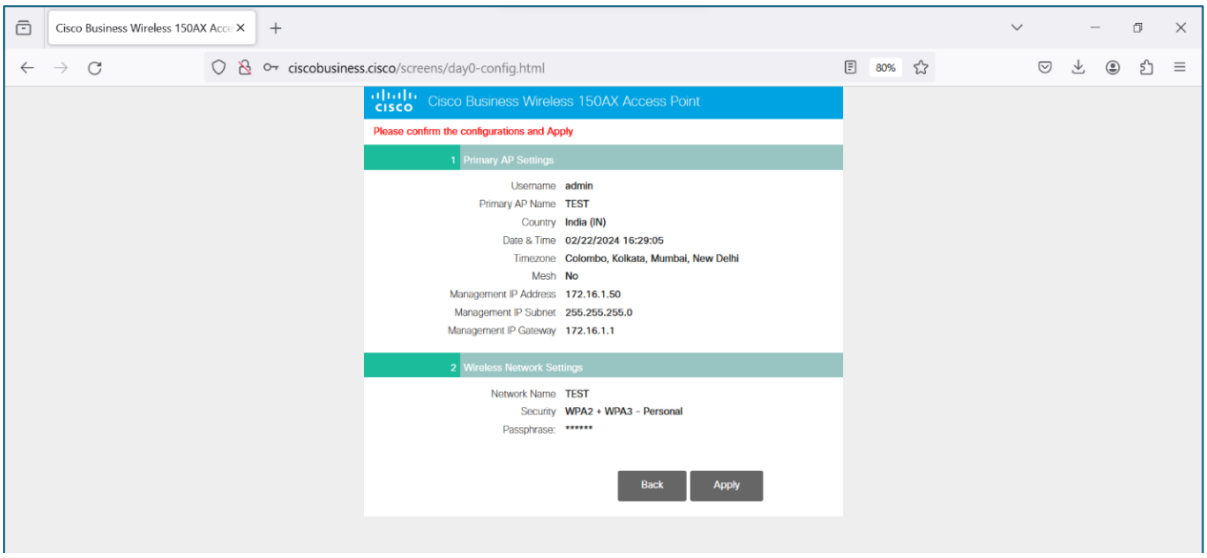


Step 6 : Verify the Configuration done and Click on Apply



Step 7 : A popup will appear on the screen “Primary AP will reboot after these configurations are applied. Click Ok to continue or click Cancel to return to the set-up wizard.”

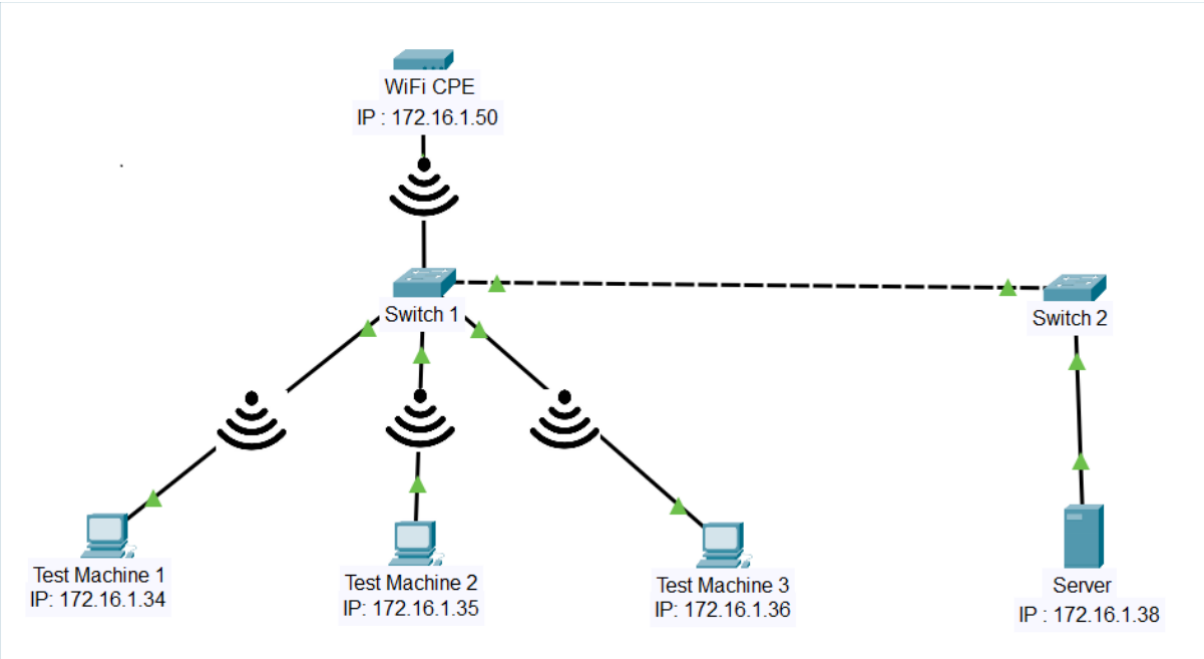




Step 8: Finished Step Now the AP is Ready to Be used.

6. **Preconditions**
   - Enable https on DUT
   - Tester must have Dir search installed on the testing machine
7. **Test Objective**: To verify that there is no default content on the web server, that is not needed for web server operation, since such default content can be useful for an attacker.

8. **Test Plan:**
   8.1 Number of Test Scenarios:
      8.1.1 Check whether the webserver has any default content
      8.1.2 Test Bed Diagram



8.2 Tools Required

- Browser
- Dirsearch

8.3 Test Execution Steps

- Open the Linux machine (Test Machine)
- Type the command dirsearch –u wificpe-ip -w /pwd/directorylist.txt
- Observe the existing default directory with the status of 200
- Check whether the existing directory on the GUI interface is accessible
- Observe that the page is redirected to the login page

9. **Expected Results for Pass:** No default content (examples, help files, documentation, aliases, un-needed directories or manuals) has been found to remain on any Web server component.

10. **Expected Format of Evidence:** Log files and screen shots of test executions.

11. **Test Execution:**

11.1 Test Case Number: 01

11.1.1 **Test Case Name:** TC_NO_DEFAULT_CONTENT

11.1.2 **Test Case Description:** To verify that there is no default content on the web server, that is not needed for web server operation, since such default content can be useful for an attacker

11.1.3 **Execution Steps:**

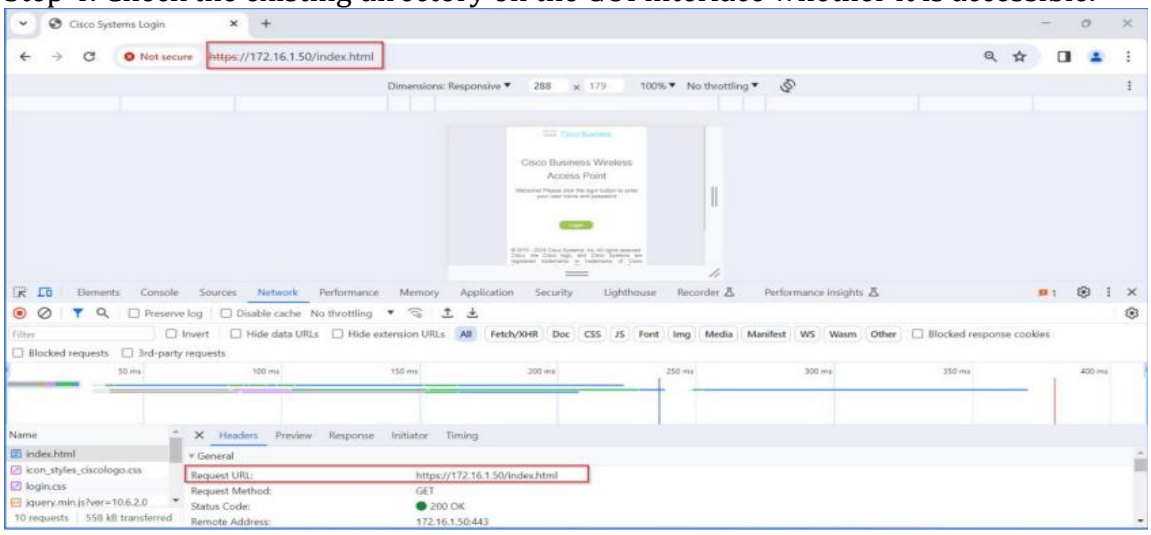
Step 1 : Open the Linux machine.

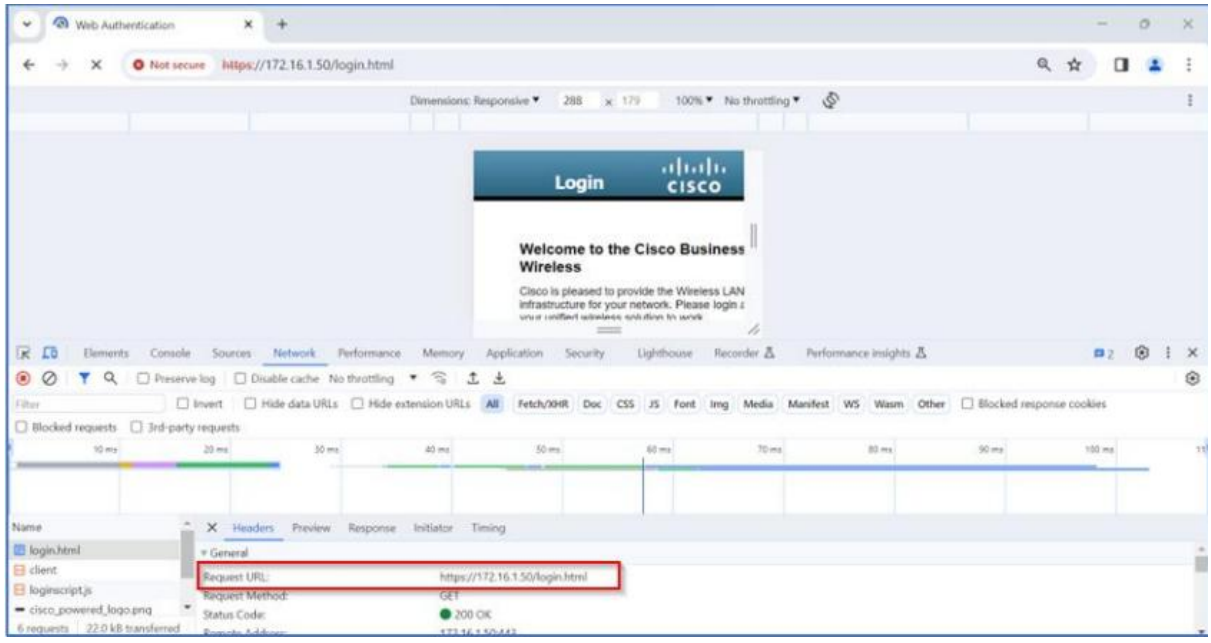
Step 2: Type the command “dirsearch –u 172.16.1.50 -w /home/kali/directorylist.txt“

Step 3: Observe the existing default directory with the status of 200

```
┌──(kali㉿kali)-[~]
└─$ dirsearch -u https://172.16.1.50 -w /home/kali/directorylist.txt
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API.
 See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 10337

Output File: /home/kali/reports/https_172.16.1.50/_24-02-23_04-02-19.txt

Target: https://172.16.1.50/

[04:02:19] Starting:
[04:14:29] 301 -   94B  - /images  →  https:///images/index.html
[04:16:15] 200 -    8KB - /login.html
[04:21:22] 301 -   95B  - /screens  →  https:///screens/index.html

Task Completed
```

Step 4: Check the existing directory on the GUI interface whether it is accessible.





Step 5: Observe that the page is redirected to the login page

11.1.4 **Test Observations:** During the testing process it was observed that the DUT does not have any default content like help files, documentation, aliases etc available to the user.

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_DEFAULT_CONTENT	PASS	all the criteria have been met

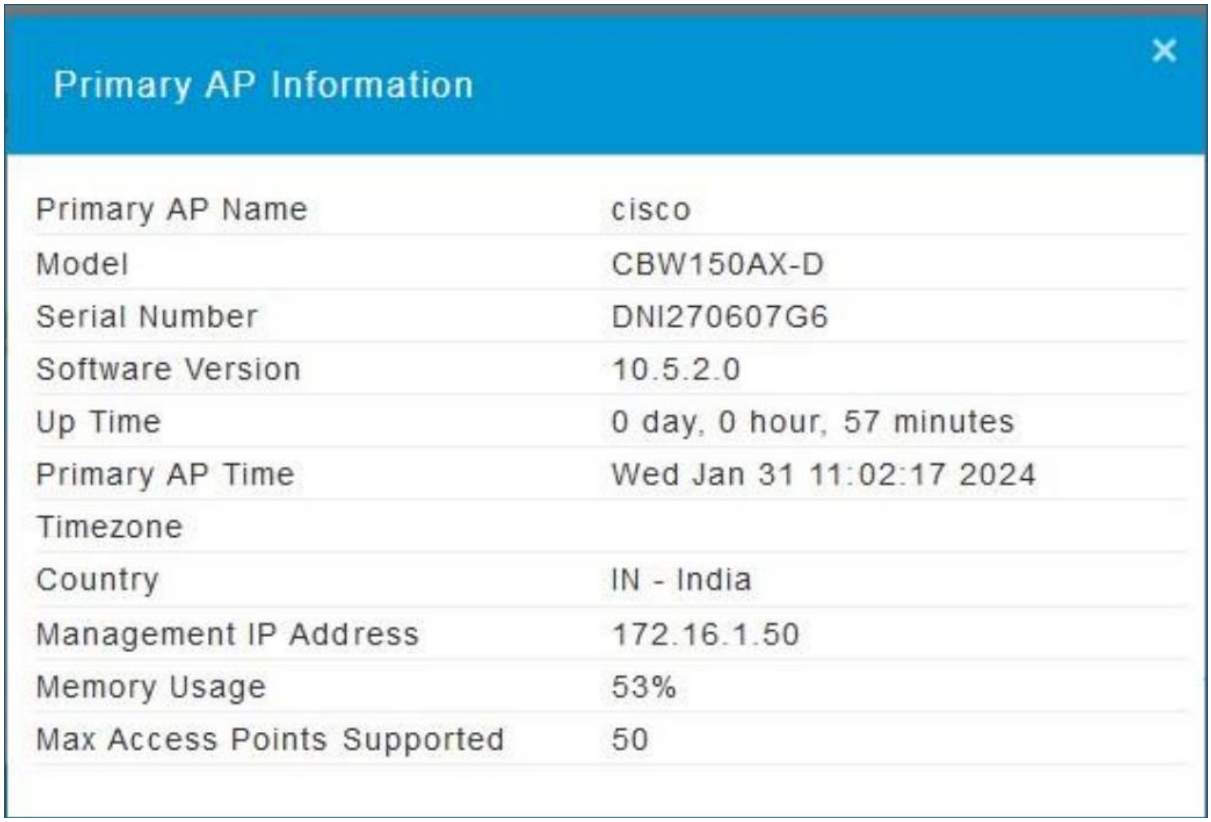
1.11.11: No Directory Listing

<DUT Details: > WiFi CPE
<DUT Software Version:> cisco 10.5.2.0
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 11: Web Server
2. **<Security Requirement No & Name >** 1.11.11: No Directory Listing
3. **<Requirement Description: >** Directory listings (indexing) / Directory browsing shall be deactivated.

4. **DUT Confirmation Details**:

Screenshot below shows the DUT name (Primary AP Name) , Model number, Serial Number, Software Version.



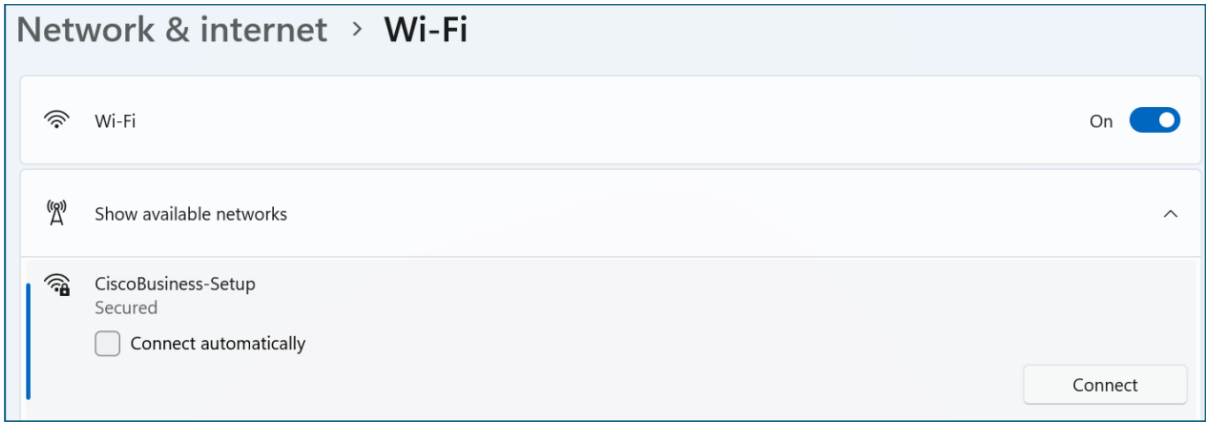
DUT Configuration Checksum:

```
PS C:\> certutil -hashfile '.\Configuration files\Configuration 1.txt' SHA256
SHA256 hash of .\Configuration files\Configuration 1.txt:
fab585d185d316ad6c45b1d414d8bf55fa8ef0094173fe9a8a5fa2d3ddc2e43b
CertUtil: -hashfile command completed successfully.
```

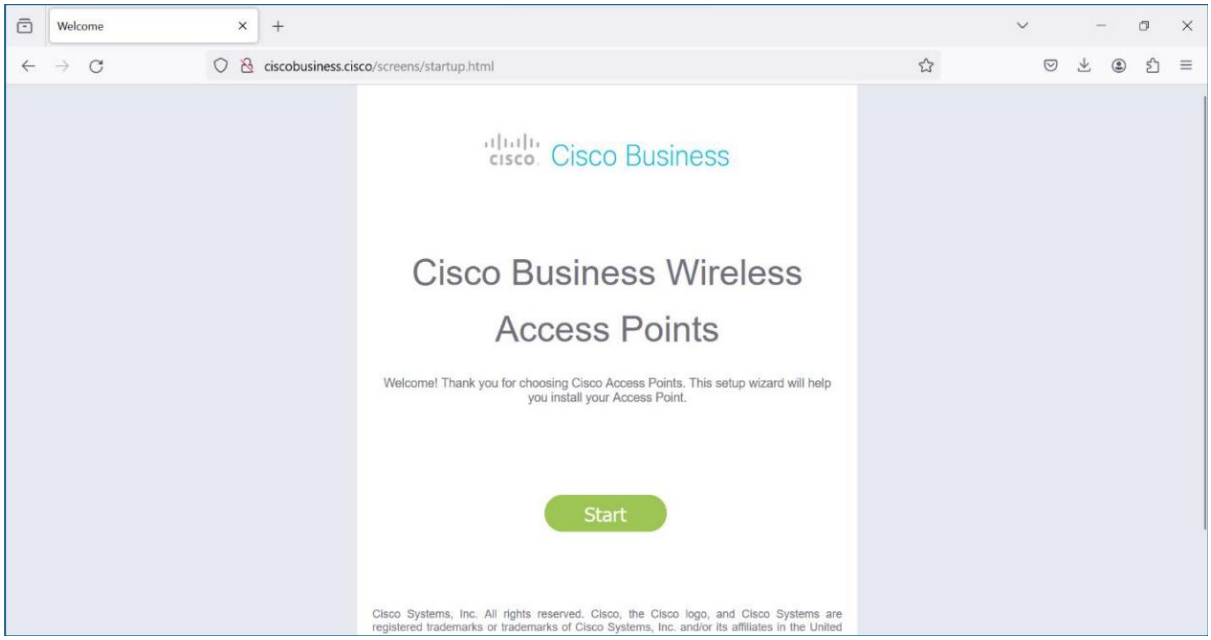
5. **DUT Configuration:**

Initial Basic Configuration of CPE

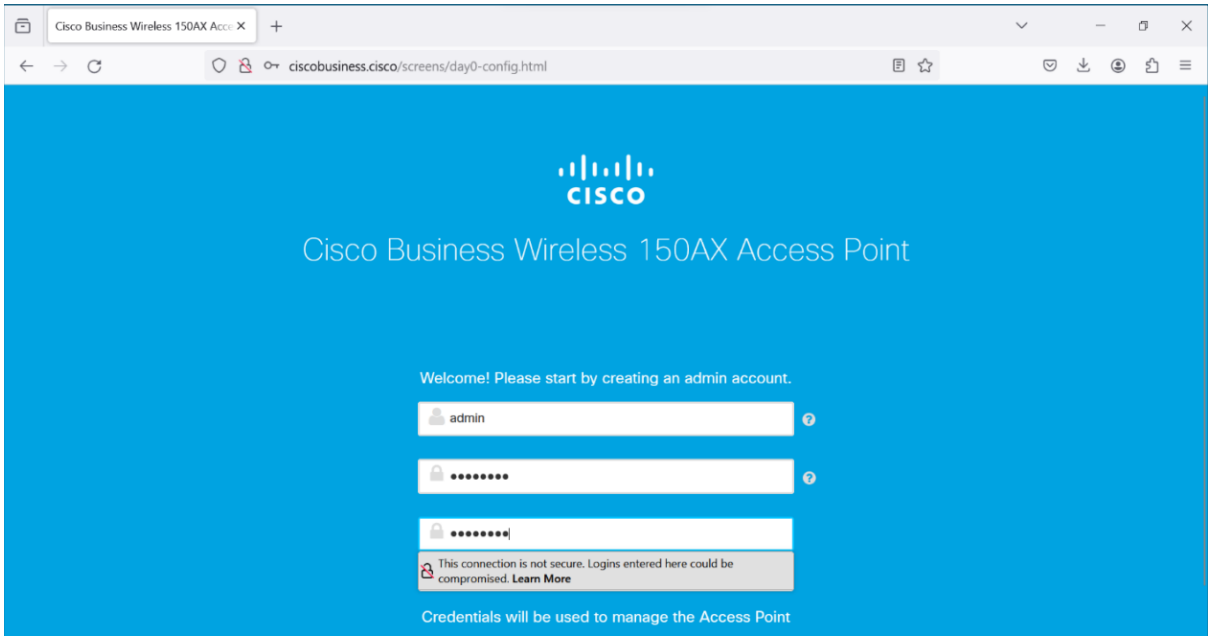
Step 1: Power on the CPE and wait for the CPE to be visible on the Laptop Wi-Fi Scanning "Cisco Business-Setup" or Reset the CPE if not Visible



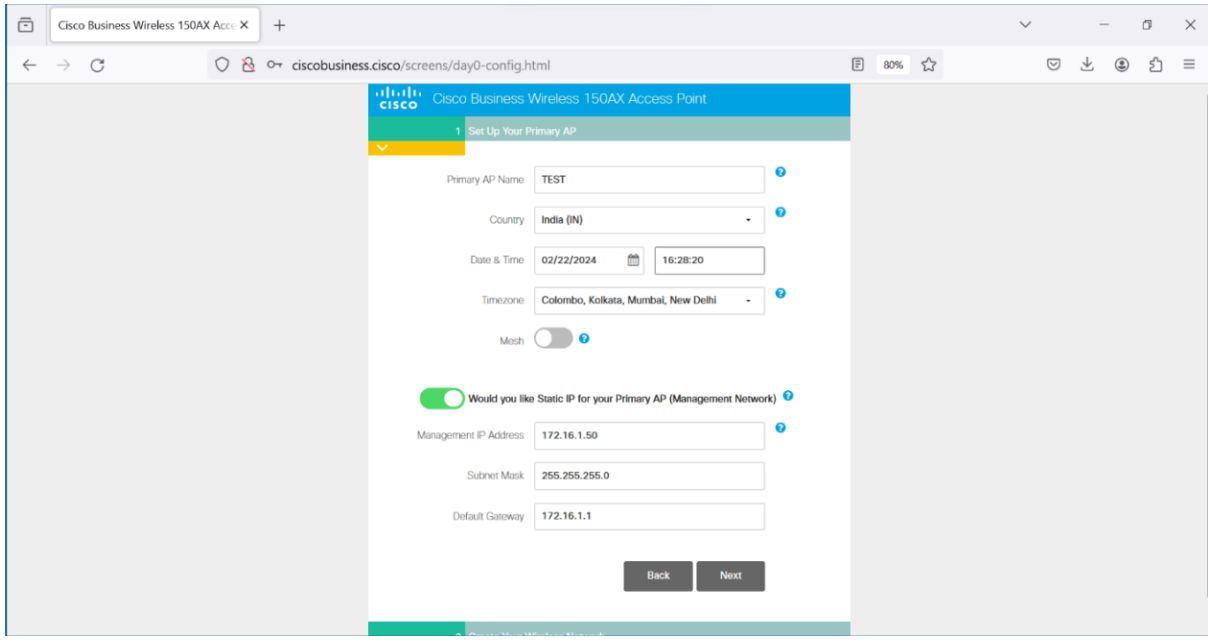
Step 2: Connect To the Wi-Fi Access Point using password " Cisco123" And Navigate to http://ciscobusiness.cisco/screens/startup.html and Click Start as Show in the below Screenshot.



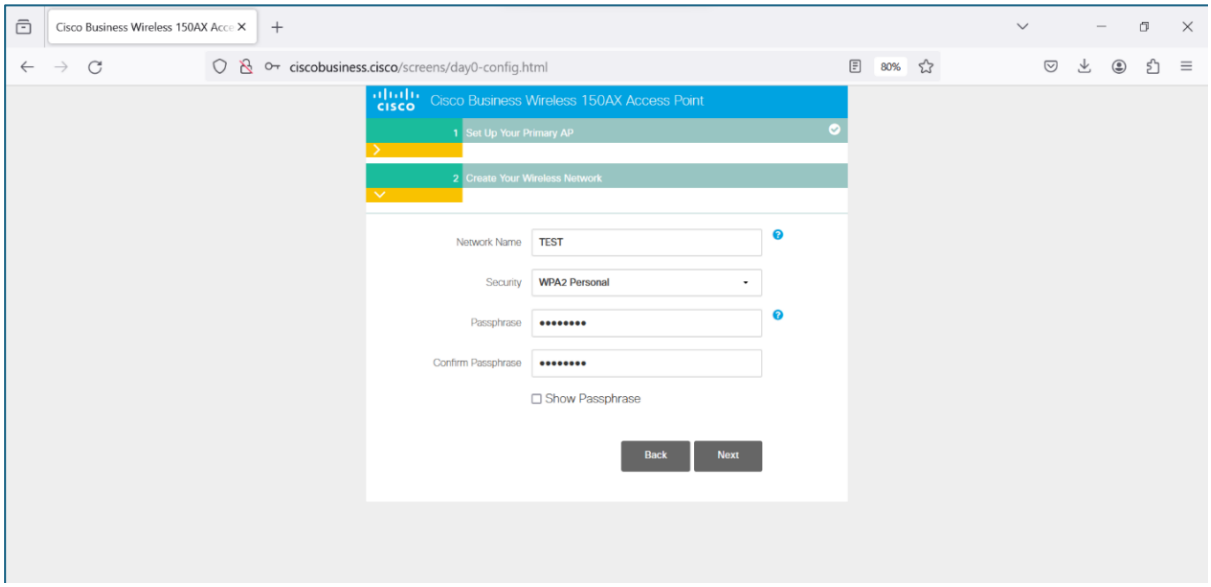
Step 3 : Enter the Desire Credentials for admin account creation and click start



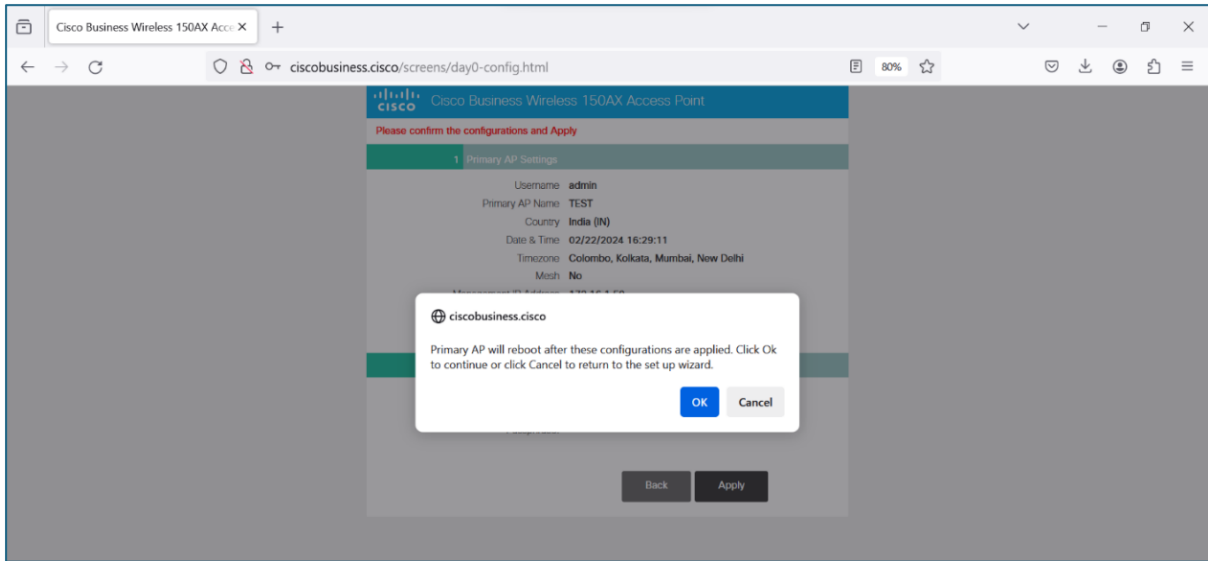
Step 4 : Enter the Desire AP Name and Select Static IP Configuration if required and click Next



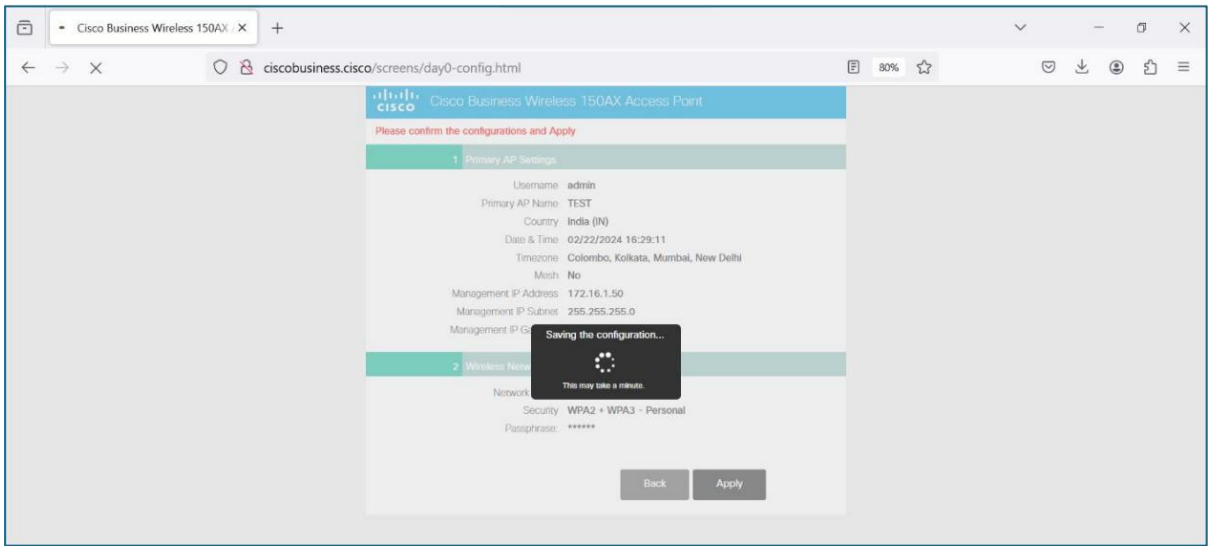
Step 5 : Enter the Desire Network Name and Passphrase and click Next

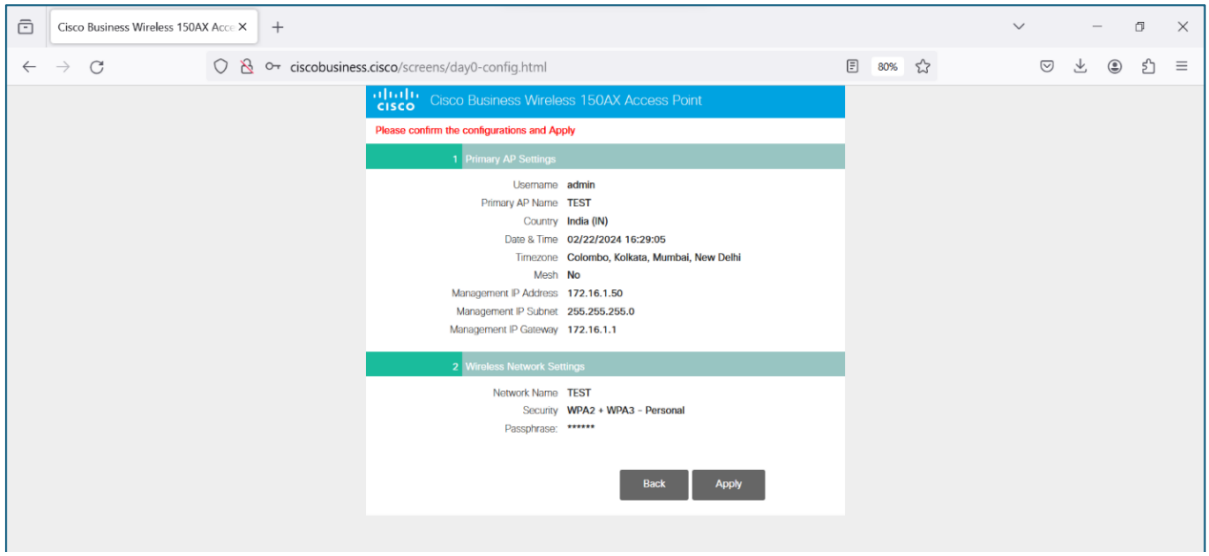


Step 6 : Verify the Configuration done and Click on Apply



Step 7 : A popup will appear on the screen “Primary AP will reboot after these configurations are applied. Click Ok to continue or click Cancel to return to the set-up wizard.”

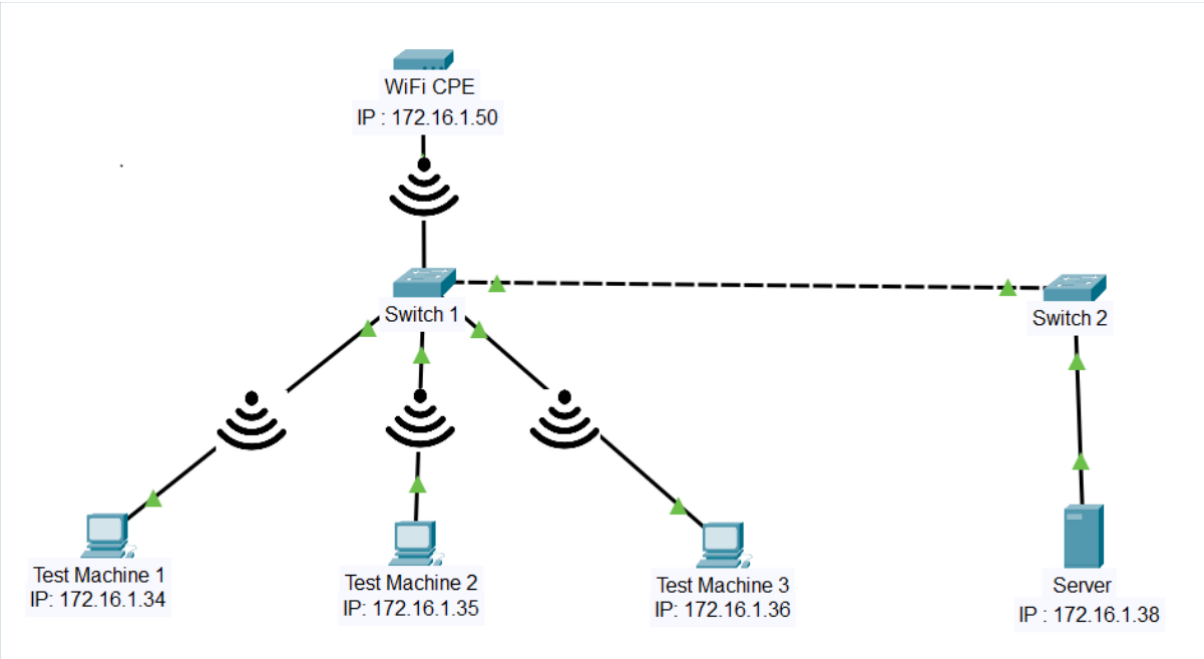




Step 8: Finished Step Now the AP is Ready to Be used.

6. **Preconditions**
   - Enable https on DUT
   - Tester must have Dir search installed on the testing machine
7. **Test Objective**: To verify that Directory listings / Directory browsing has been deactivated in all Web server components.

8. **Test Plan:**
   8.1 Number of Test Scenarios:
   8.1.1 Check if webserver has any directory listing
   8.2 Test Bed Diagram



8.3 Tools Required

- Browser
- Dirsearch

8.4 Test Execution Steps

- Open the Linux machine (Test Machine)
- Type the command dirsearch –u wificpe-ip -w /pwd/directorylist.txt
- Observe the existing default directory with the status of 200
- Check whether the existing directory on the GUI interface is accessible
- Observe that the page is listing the file and directory

9. **Expected Results for Pass:** Evidence that Directory listing / Directory browsing has been deactivated in all Web server components.

10. **Expected Format of Evidence:**

- Log files and screen shots of test executions.

11. **Test Execution:**

11.1 Test Case Number: 01

11.1.1 **Test Case Name:** TC_NO_DIRECTORY_LISTINGS

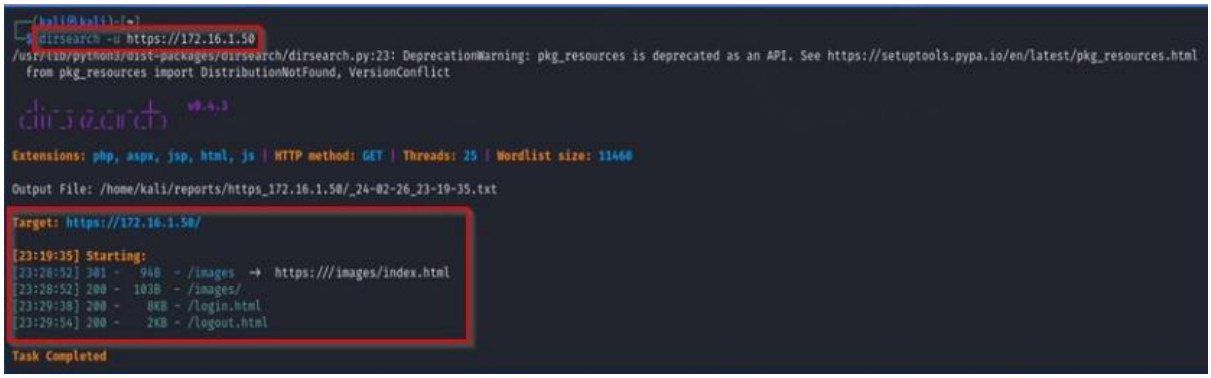
11.1.2 **Test Case Description:** To verify that Directory listings / Directory browsing has been deactivated in all Web server components.

11.1.3 **Execution Steps:**

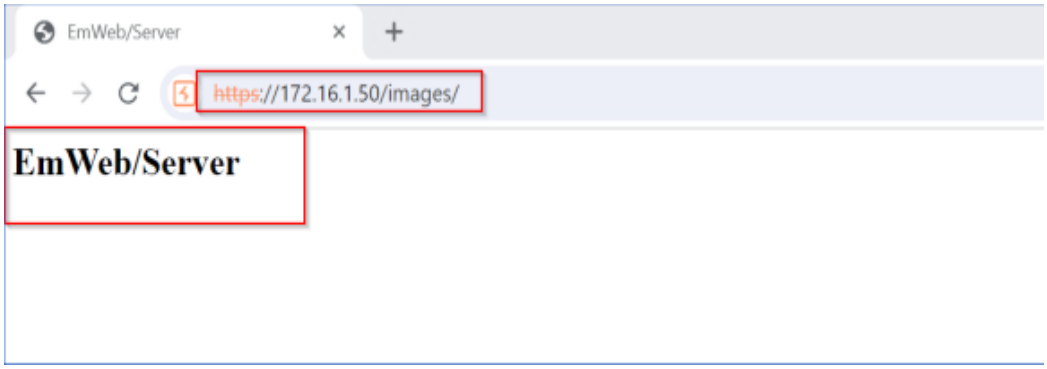
Step 1 : Open the Linux machine.

Step 2: run the command dirsearch -u https://172.16.1.50

Step 3: Observe the existing directory with the status of 200



Step 4: Now try to access the directory



Step 5: Observe that the webserver is not listing any directories

11.1.4 **Test Observations:** During the testing process it has been observed that the DUT has not listed any directories

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_DIRECTORY_LISTINGS	PASS	all the criteria have been met

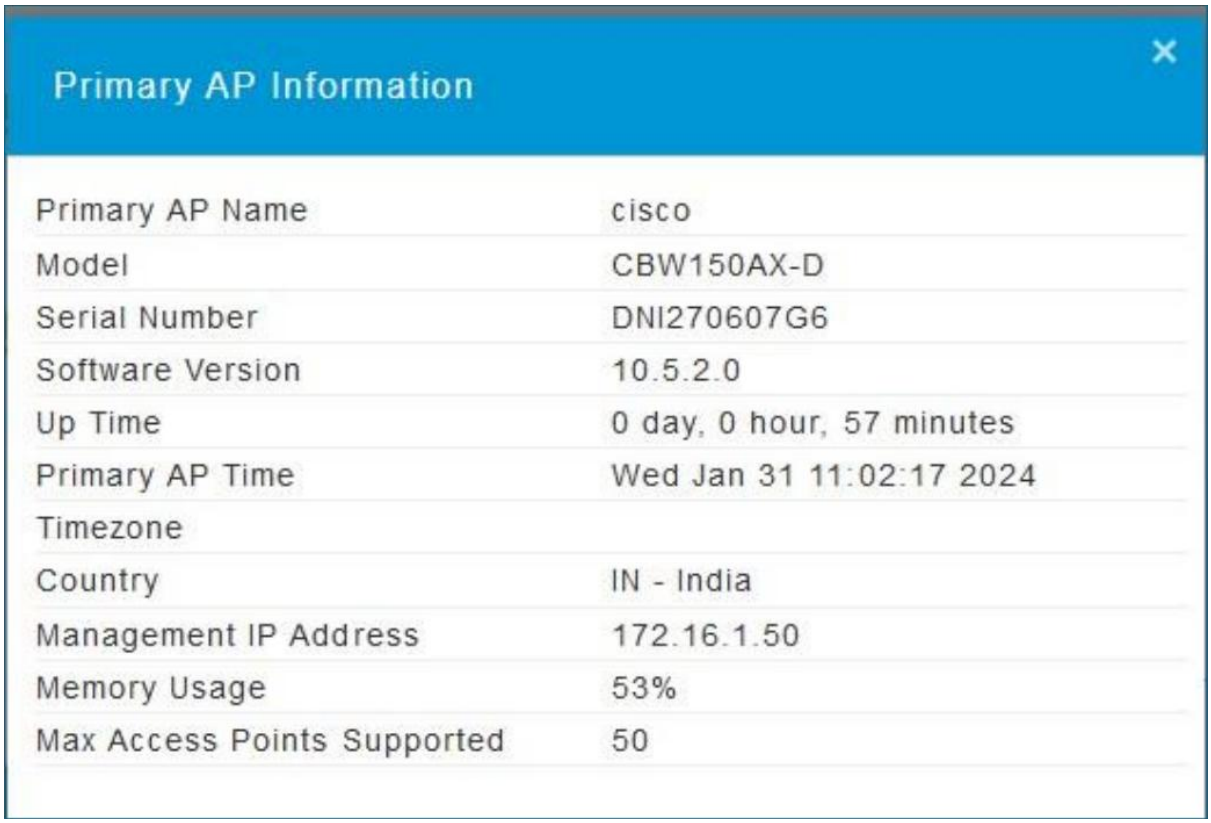
1.11.12: Information in HTTP Headers

<DUT Details: > WiFi CPE
<DUT Software Version:> cisco 10.5.2.0
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 11: Web Server
2. **<Security Requirement No & Name >** 1.11.12: Information in HTTP Headers
3. **<Requirement Description: >** The HTTP header shall not include information on the version of the web server
   and the modules/add-ons used

4. **DUT Confirmation Details**:

Screenshot below shows the DUT name (Primary AP Name) , Model number, Serial Number, Software Version.



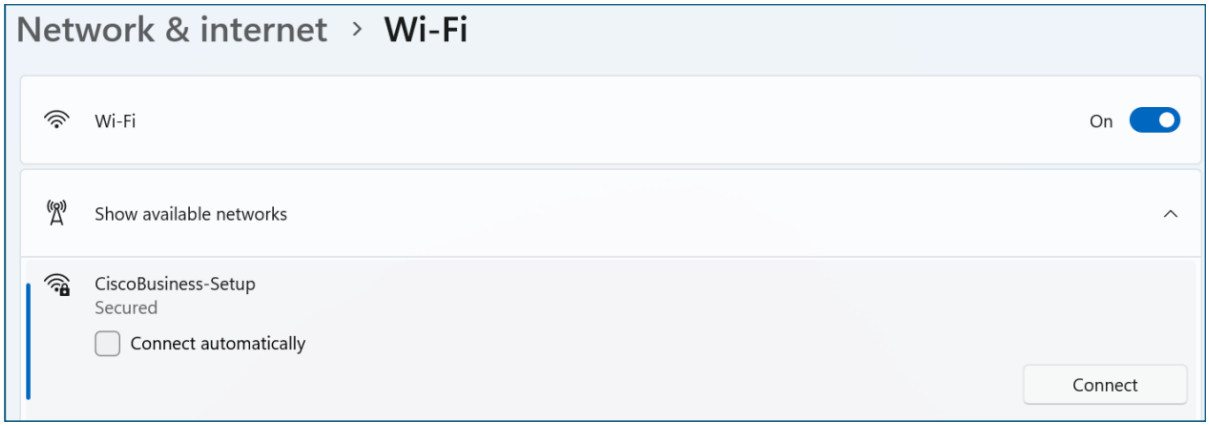
DUT Configuration Checksum:

```
PS C:\> certutil -hashfile '.\Configuration files\Configuration 1.txt' SHA256
SHA256 hash of .\Configuration files\Configuration 1.txt:
fab585d185d316ad6c45b1d414d8bf55fa8ef0094173fe9a8a5fa2d3ddc2e43b
CertUtil: -hashfile command completed successfully.
```

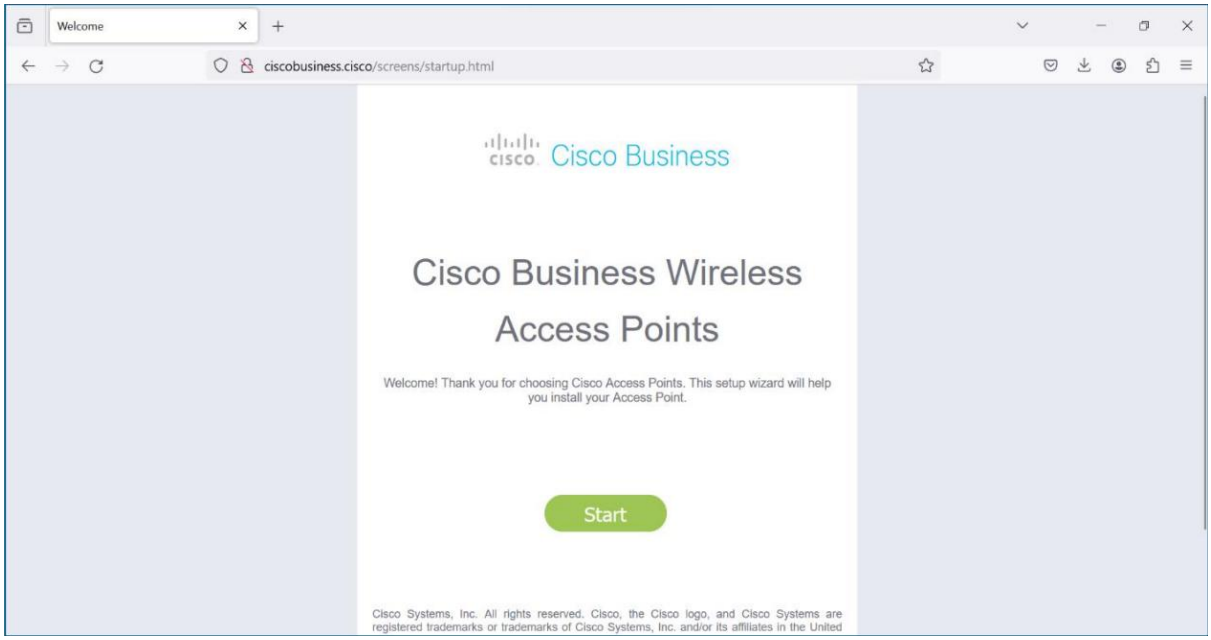
5. **DUT Configuration:**

Initial Basic Configuration of CPE

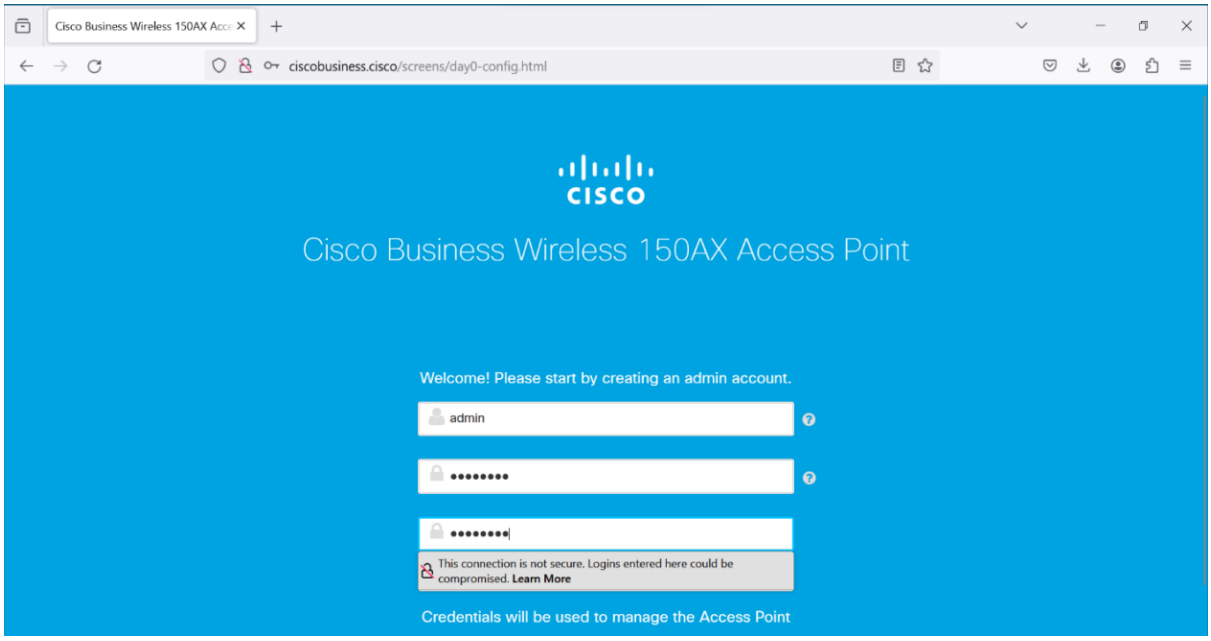
Step 1: Power on the CPE and wait for the CPE to be visible on the Laptop Wi-Fi Scanning "Cisco Business-Setup" or Reset the CPE if not Visible



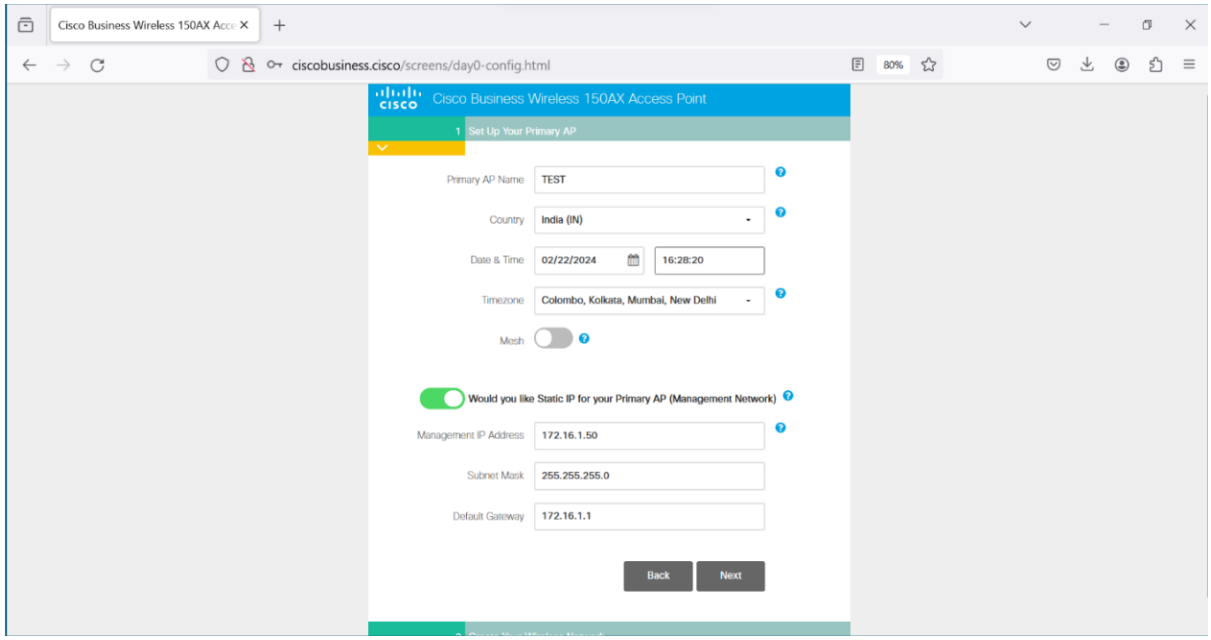
Step 2: Connect To the Wi-Fi Access Point using password " Cisco123" And Navigate to http://ciscobusiness.cisco/screens/startup.html and Click Start as Show in the below Screenshot.



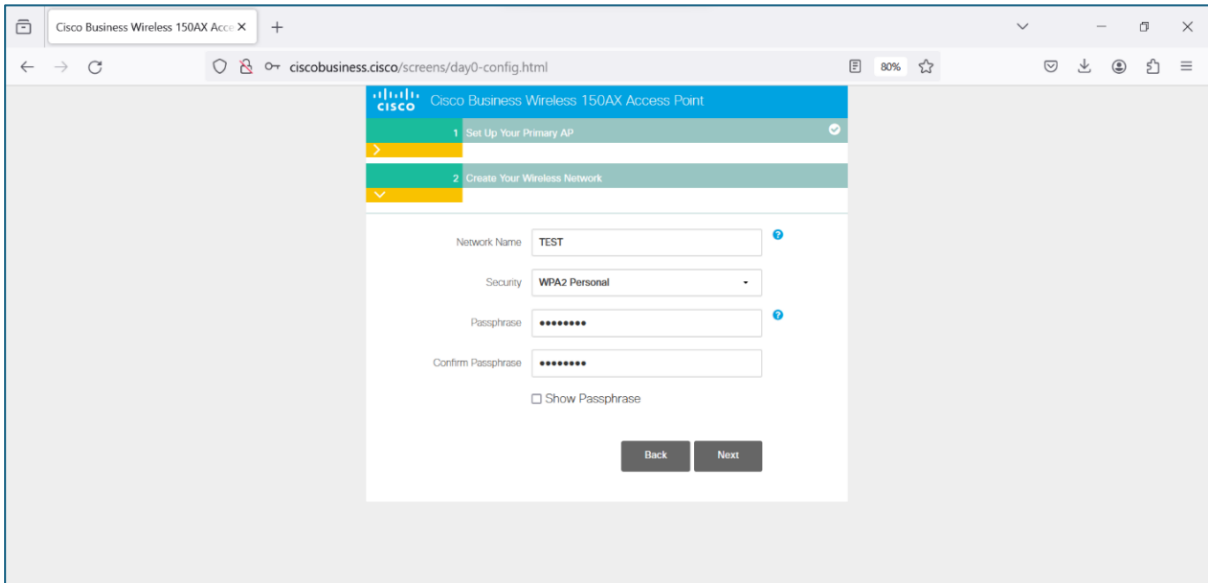
Step 3 : Enter the Desire Credentials for admin account creation and click start



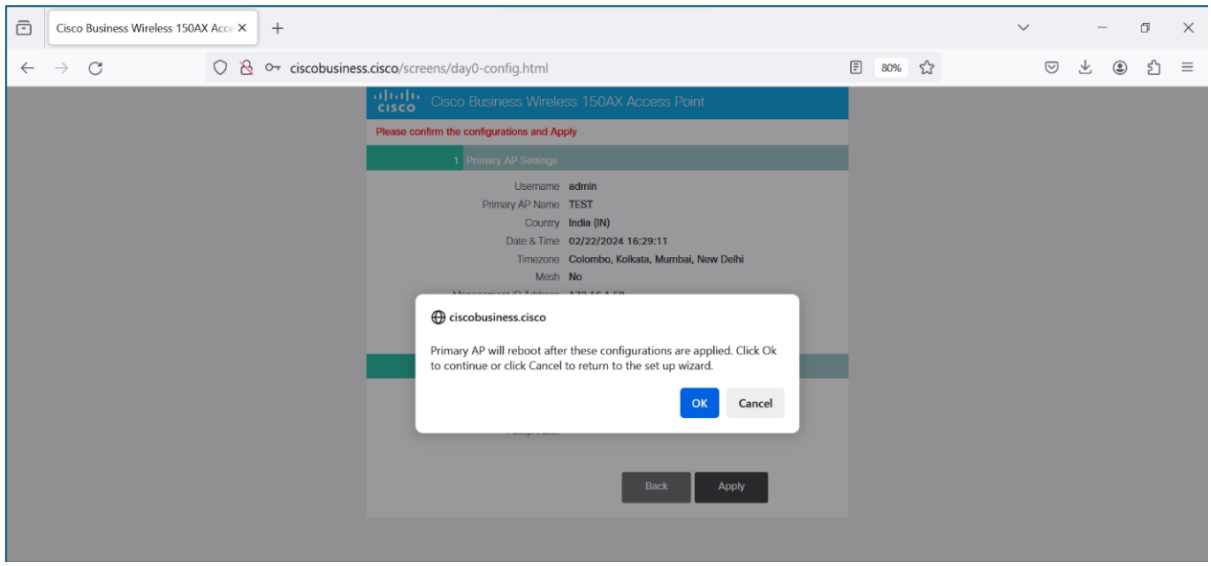
Step 4 : Enter the Desire AP Name and Select Static IP Configuration if required and click Next



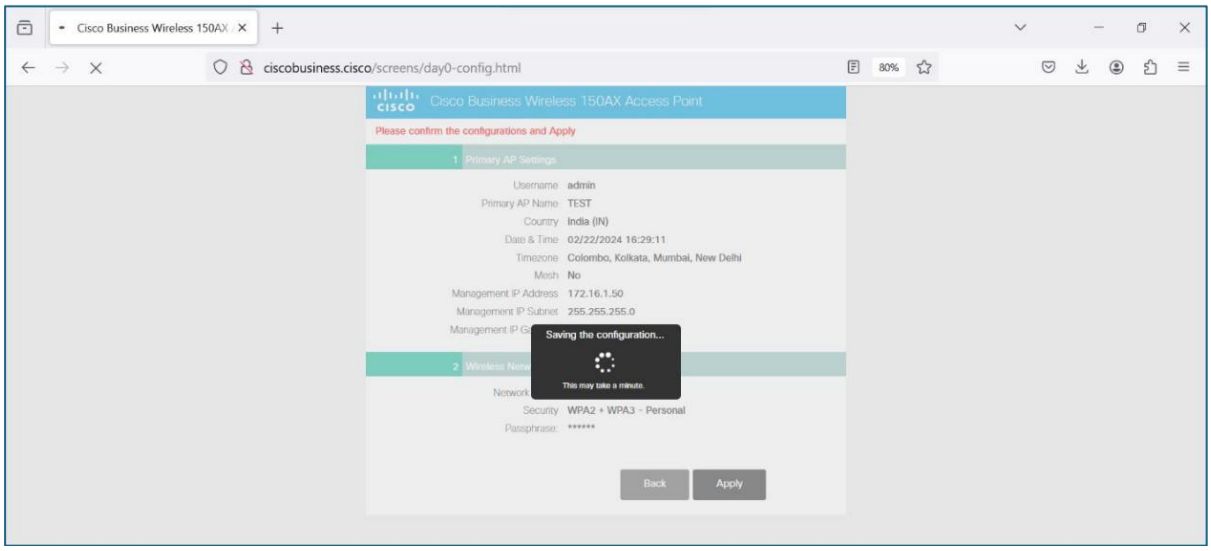
Step 5 : Enter the Desire Network Name and Passphrase and click Next

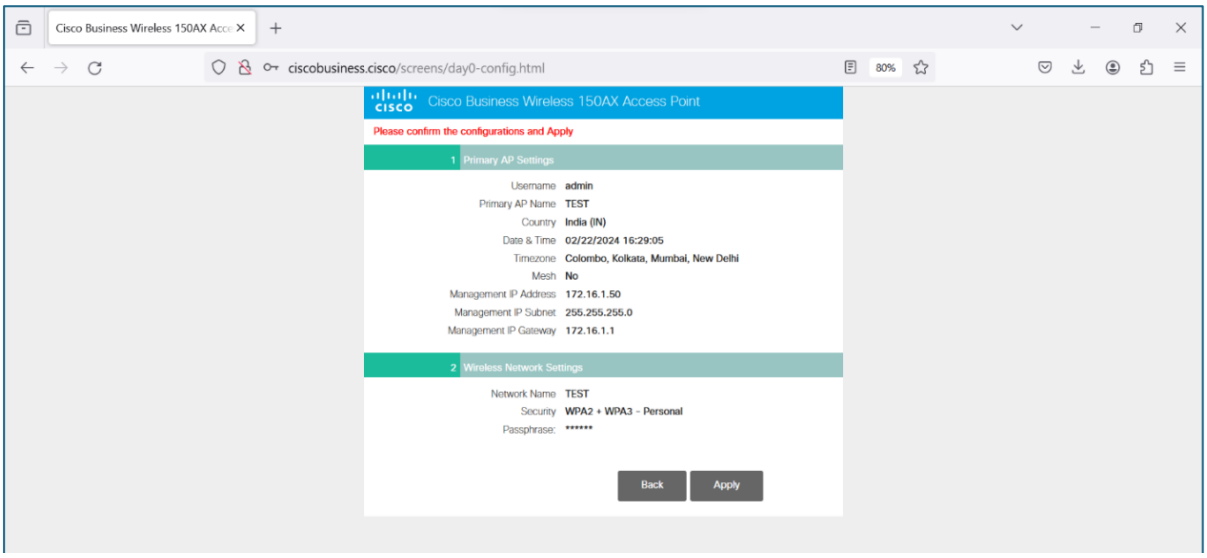


Step 6 : Verify the Configuration done and Click on Apply



Step 7 : A popup will appear on the screen “Primary AP will reboot after these configurations are applied. Click Ok to continue or click Cancel to return to the set-up wizard.”





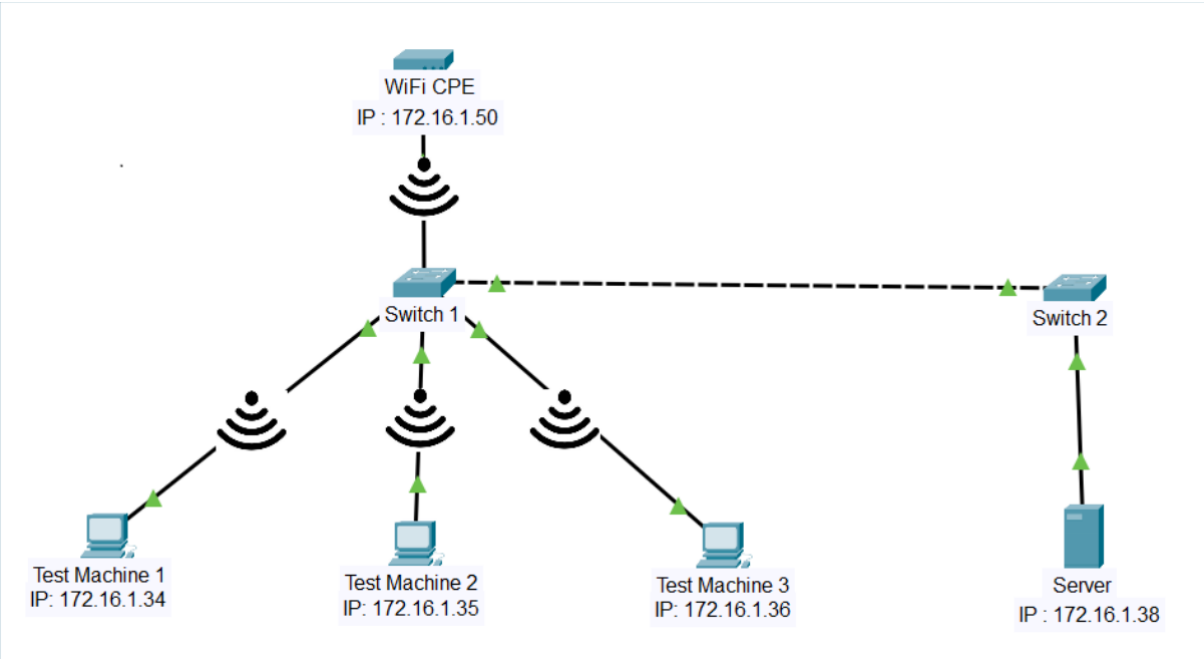
Step 8: Finished Step Now the AP is Ready to Be used.

6. **Preconditions** Tester should have Burp suite installed in the test machine.
7. **Test Objective**: To verify that HTTP headers do not include information on the version of the web server and the modules/add-ons used.
8. **Test Plan:**

8.1 Number of Test Scenarios:

8.1.1 Check if any server information is disclosing in response headers

8.2 Test Bed Diagram



8.3 Tools Required

- Browser
- Burp suite

8.4 Test Execution Steps

- Open browser and navigate to https://wificpe-ip.
- Intercept the request using burpsuite proxy and observe the response.
- Additionally the tester will run some web scanning tools like Nikto, to get the detailed information and verify that the HTTP headers do not include information on the version of the web server.

9. **Expected Results for Pass:** Evidence that HTTP headers do not include information on the version of the web server and the modules/addons used

10. **Expected Format of Evidence:** Log files and screen shots of test executions.

11. **Test Execution:**

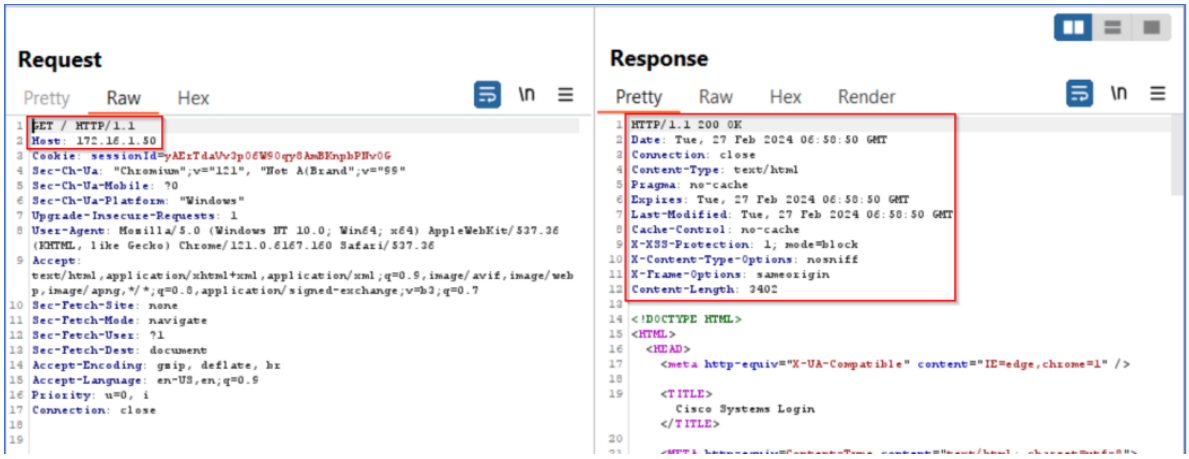
11.1 Test Case Number: 01

11.1.1 **Test Case Name:** TC_NO_WEB_SERVER_HEADER_INFORMATION

11.1.2 **Test Case Description:** To verify that HTTP headers do not include information on the version of the web server and the modules/add-ons used.

11.1.3 **Execution Steps:**

Step 1 : Open the browser and navigate to http://172.16.1.40 and intercept the traffic and observe the response.



11.1.4 **Test Observations:** During the testing process it was observed that the HTTP header has not disclosed information of the version of the web server and the modules/add-ons used.

12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_UNUSED_HTTP_METHODS	PASS	all the criteria have been met

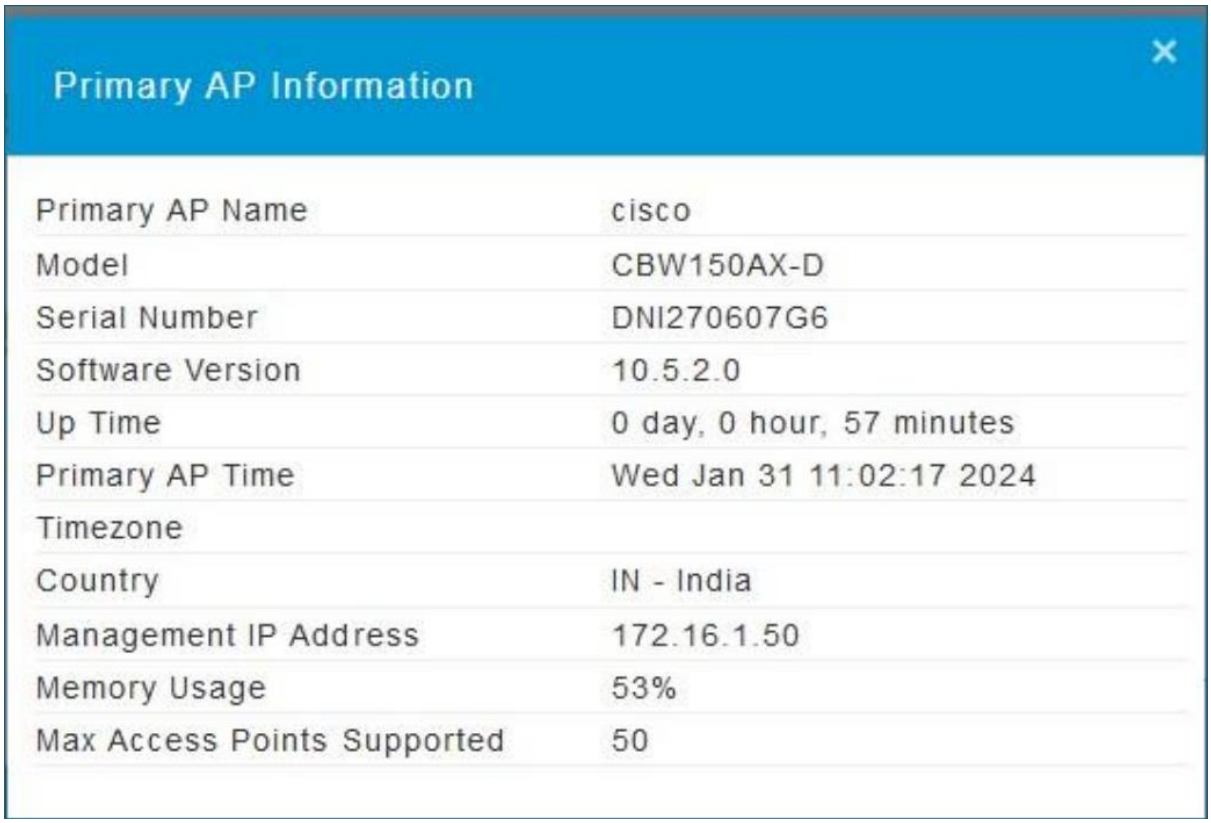
1.11.13: Information in Error Page

<DUT Details: > WiFi CPE
<DUT Software Version:> cisco 10.5.2.0
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 11: Web Server
2. **<Security Requirement No & Name >**1.11.13: Information in Error Page
3. **<Requirement Description: >** User-defined error pages shall not include version information about the web server and the modules/add-ons used. Error messages shall not include internal information such as internal server names, error codes, etc. Default error pages of the web server shall be replaced by error pages defined by the vendor.

4. **DUT <u>Confirmation Details</u>**:

Screenshot below shows the DUT name (Primary AP Name) , Model number, Serial Number, Software Version.



DUT Configuration Checksum:

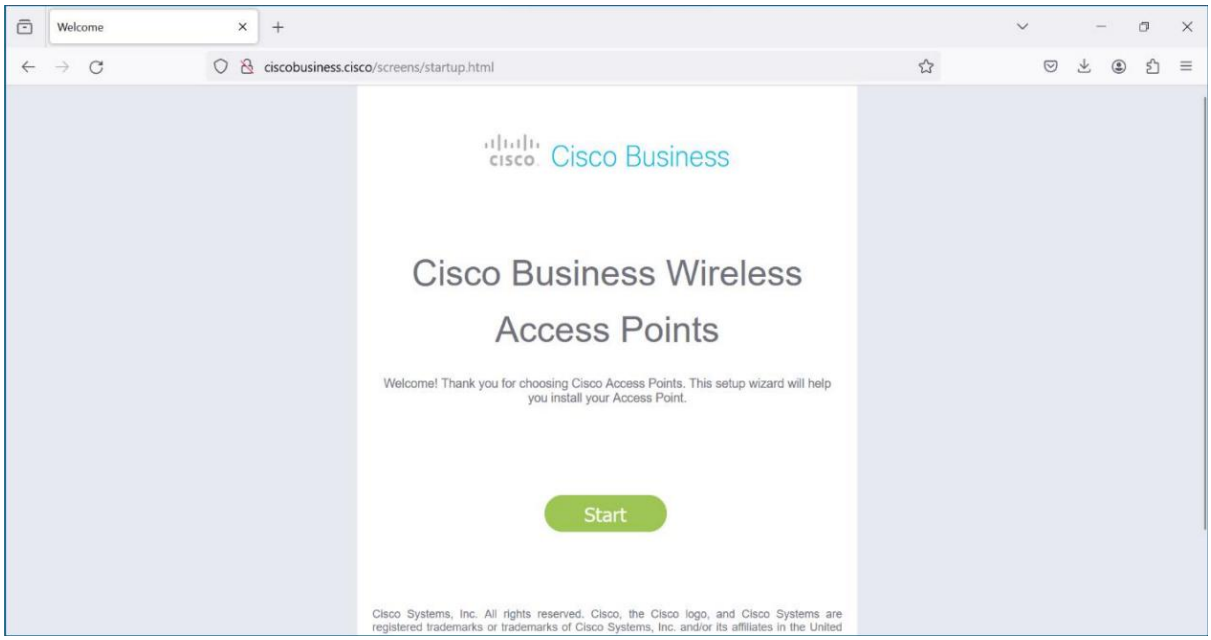
```
PS C:\> certutil -hashfile '.\Configuration files\Configuration 1.txt' SHA256
SHA256 hash of .\Configuration files\Configuration 1.txt:
fab585d185d316ad6c45b1d414d8bf55fa8ef0094173fe9a8a5fa2d3ddc2e43b
CertUtil: -hashfile command completed successfully.
```

5. **DUT Configuration:**

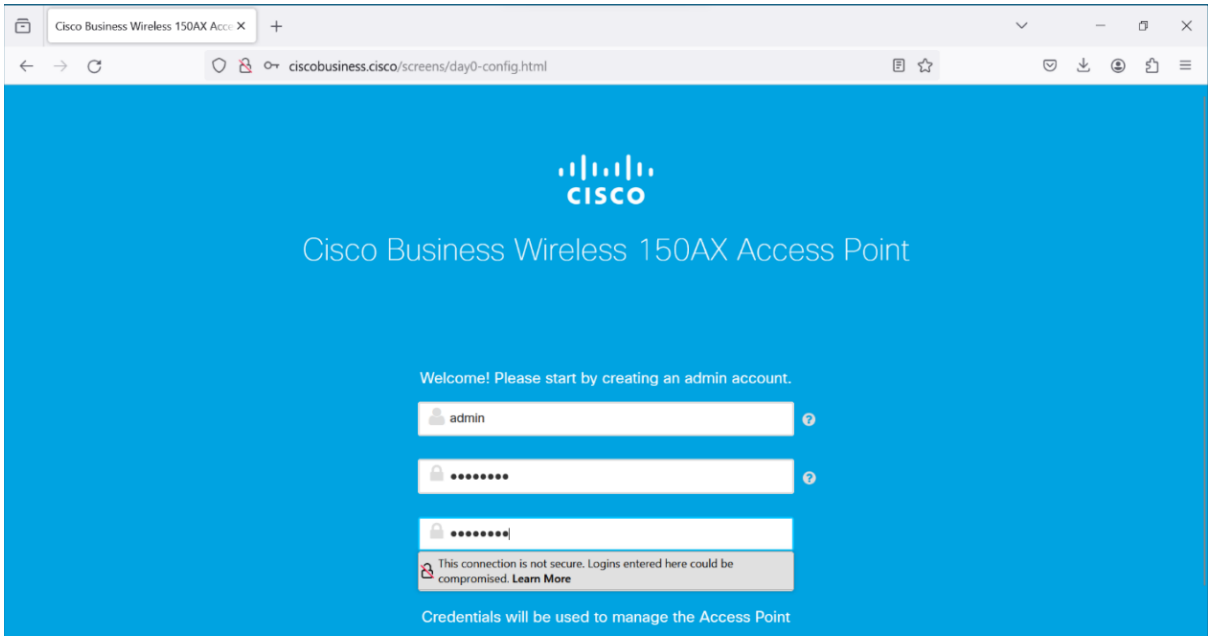
Initial Basic Configuration of CPE

Step 1: Power on the CPE and wait for the CPE to be visible on the Laptop Wi-Fi Scanning "Cisco Business-Setup" or Reset the CPE if not Visible

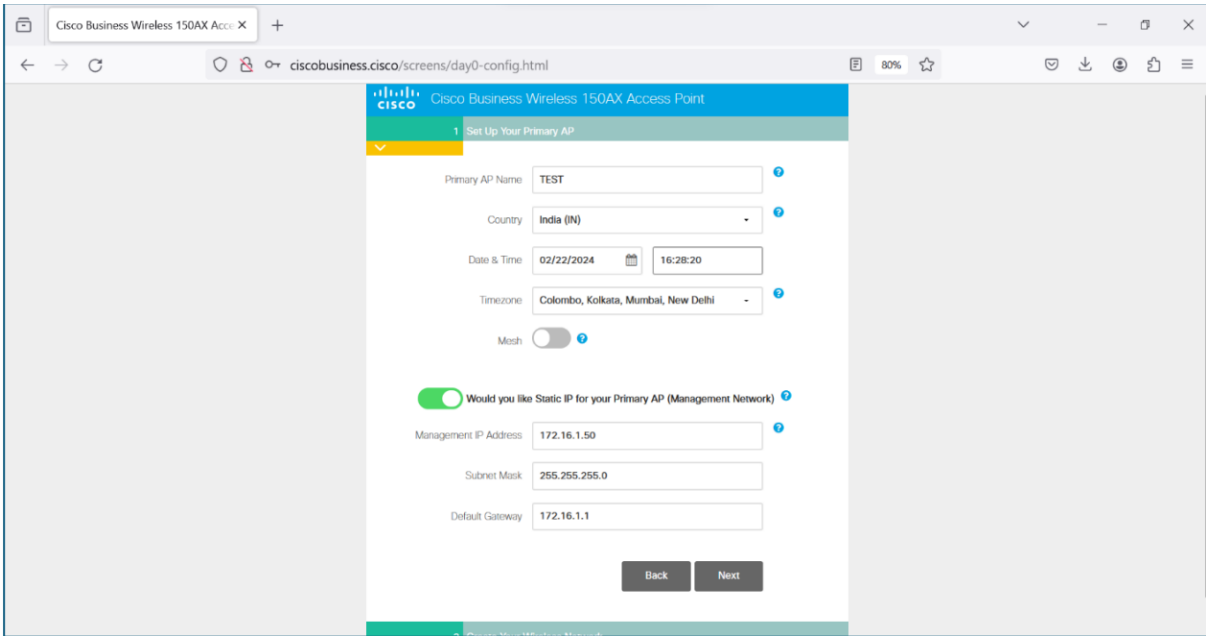
Step 2: Connect To the Wi-Fi Access Point using password " Cisco123" And Navigate to http://ciscobusiness.cisco/screens/startup.html and Click Start as Show in the below Screenshot.



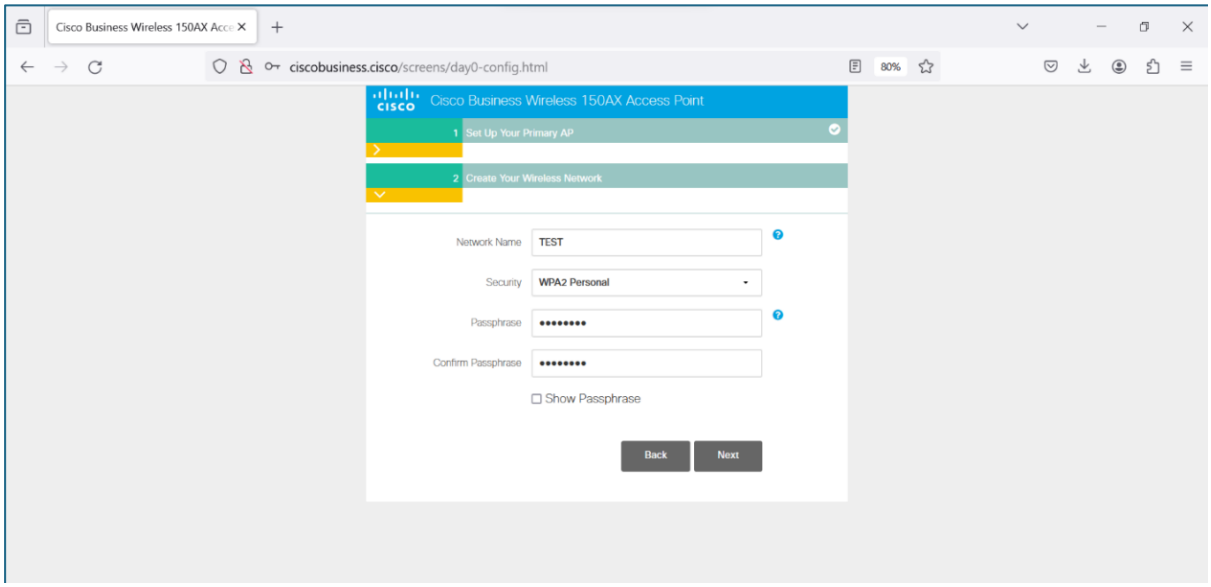
Step 3 : Enter the Desire Credentials for admin account creation and click start



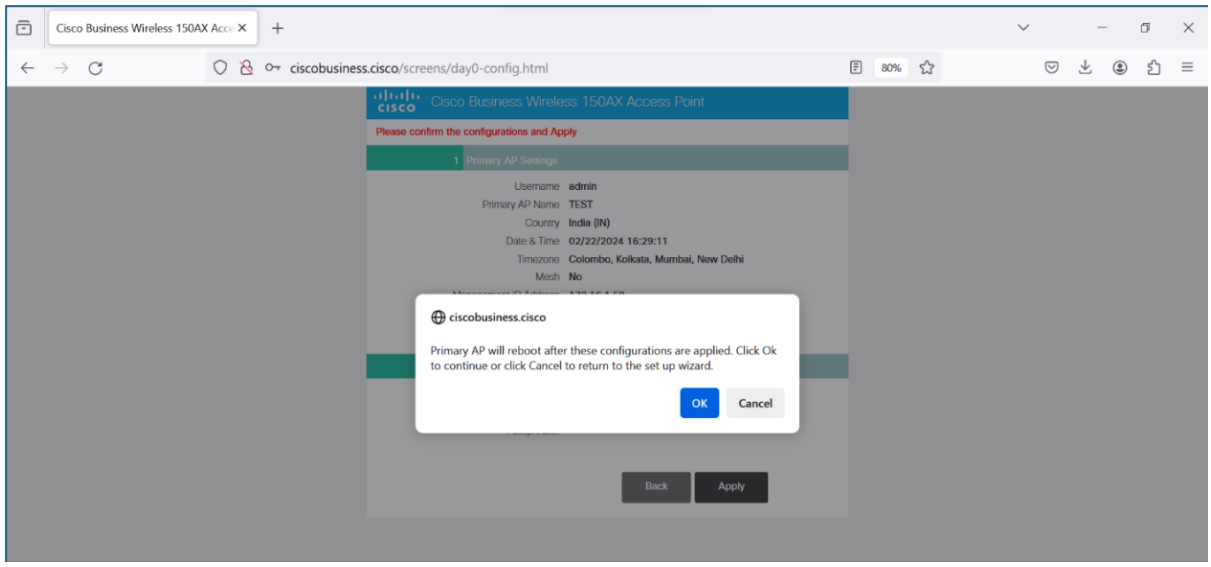
Step 4 : Enter the Desire AP Name and Select Static IP Configuration if required and click Next



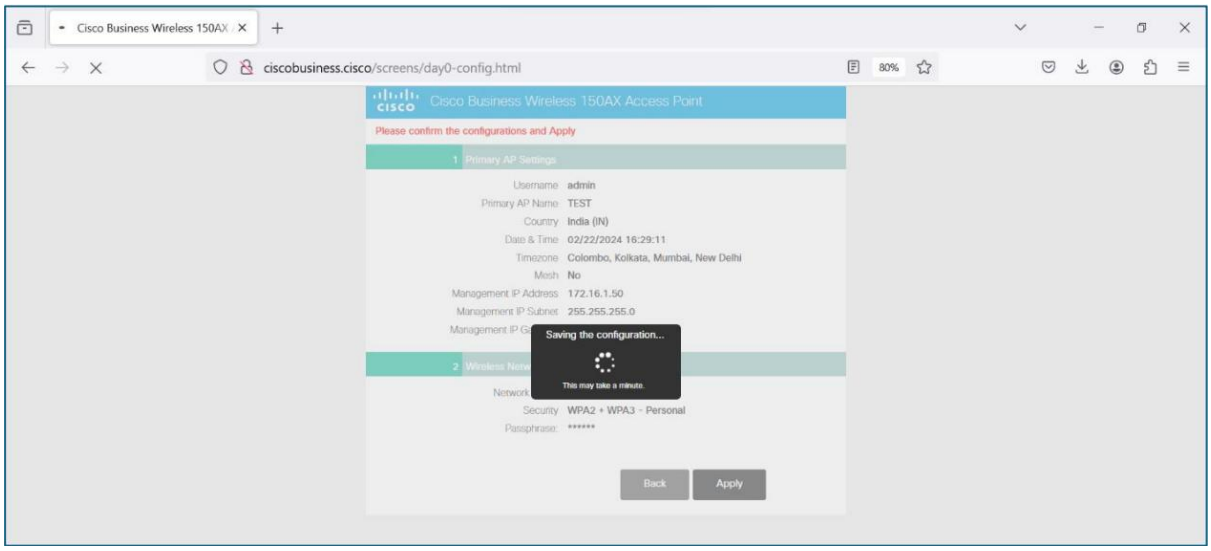
Step 5 : Enter the Desire Network Name and Passphrase and click Next

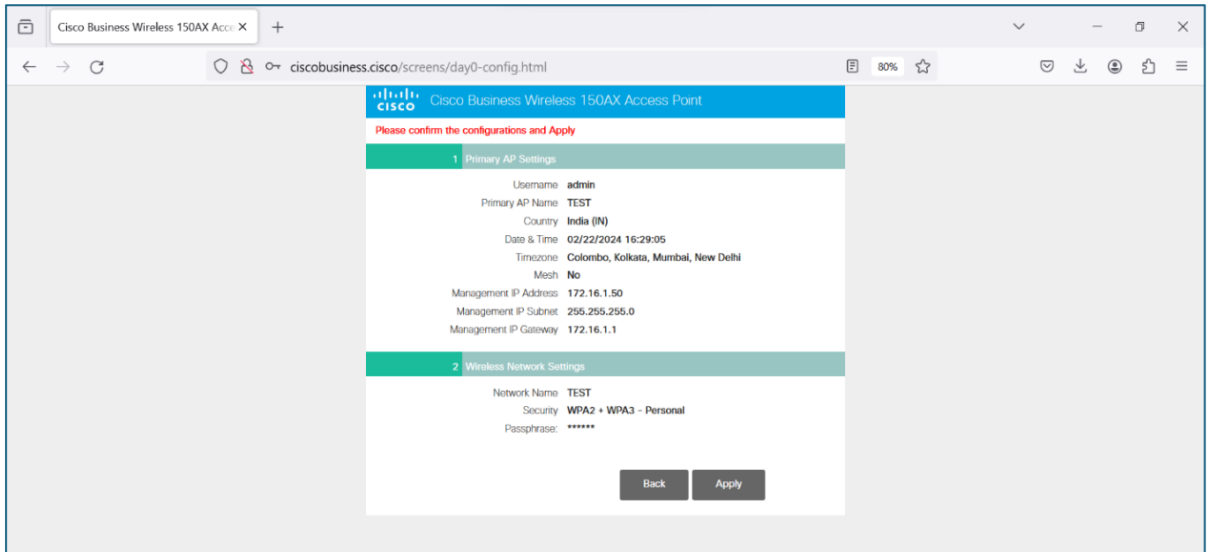


Step 6 : Verify the Configuration done and Click on Apply



Step 7 : A popup will appear on the screen “Primary AP will reboot after these configurations are applied. Click Ok to continue or click Cancel to return to the set-up wizard.”





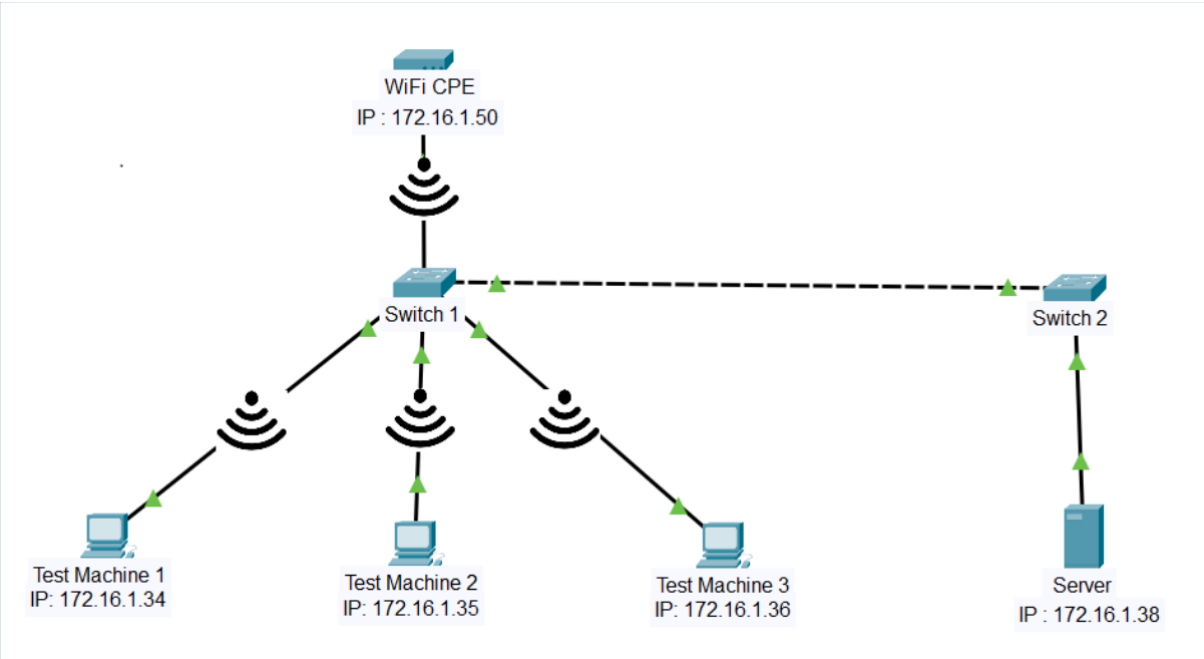
Step 8: Finished Step Now the AP is Ready to Be used.

6. **Preconditions** Tester should have Burp suite installed in the test machine.
7. **Test Objective**: To verify that error pages and error messages do not include information about the web server.
8. **Test Plan:**

8.1 Number of Test Scenarios:

8.1.1 Check if the web server is disclosing any sensitive information when a error message is triggered.

8.2 Test Bed Diagram



8.3 Tools Required

- Browser
- Burp suite

8.4 Test Execution Steps

- Open browser and navigate to https://wificpe-ip.
- Intercept the request using burpsuite proxy
- Remove the session id and then click send.
- Observe that the error message is triggered.
- Intercept the request and try to generate error page/error message at least 5 times

9. **Expected Results for Pass:** Evidence that generated error pages and error messages do not include information about the web server.
10. **Expected Format of Evidence:** Log files and screen shots of test executions.
11. **Test Execution:**

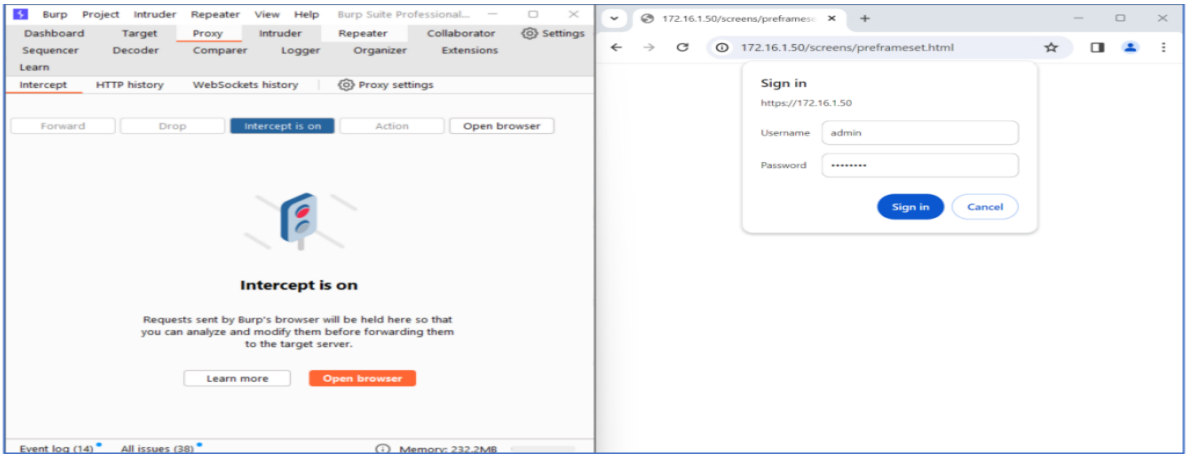
11.1 Test Case Number: 01

11.1.1 **Test Case Name:** TC_NO_WEB_SERVER_ERROR_PAGES_INFORMATION

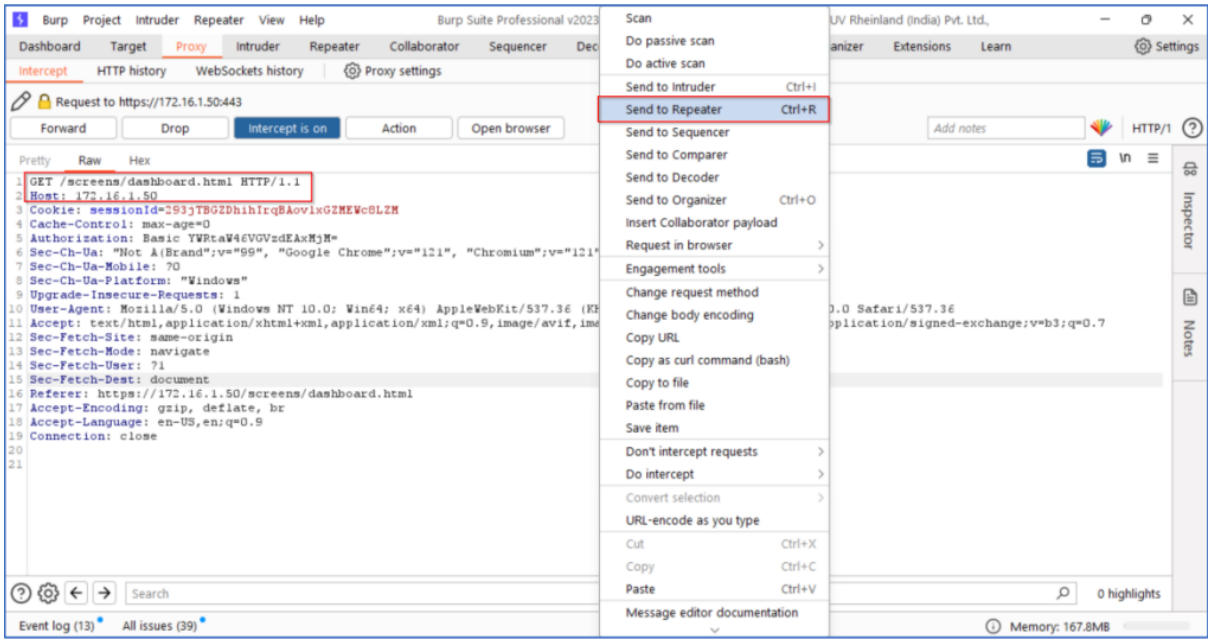
11.1.2 **Test Case Description:** To verify that error pages and error messages do not include information about the web server.

11.1.3 **Execution Steps:**

Step 1 : Open the browser and navigate to http://172.16.1.50 and intercept the traffic and observe the response.

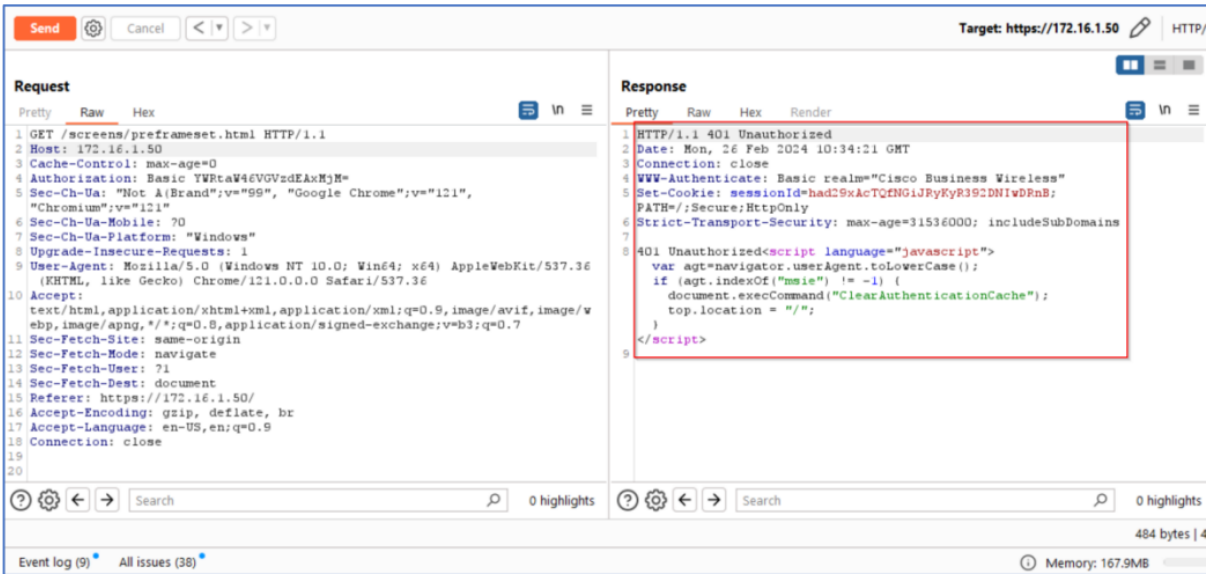


Step2 : send request to repeater

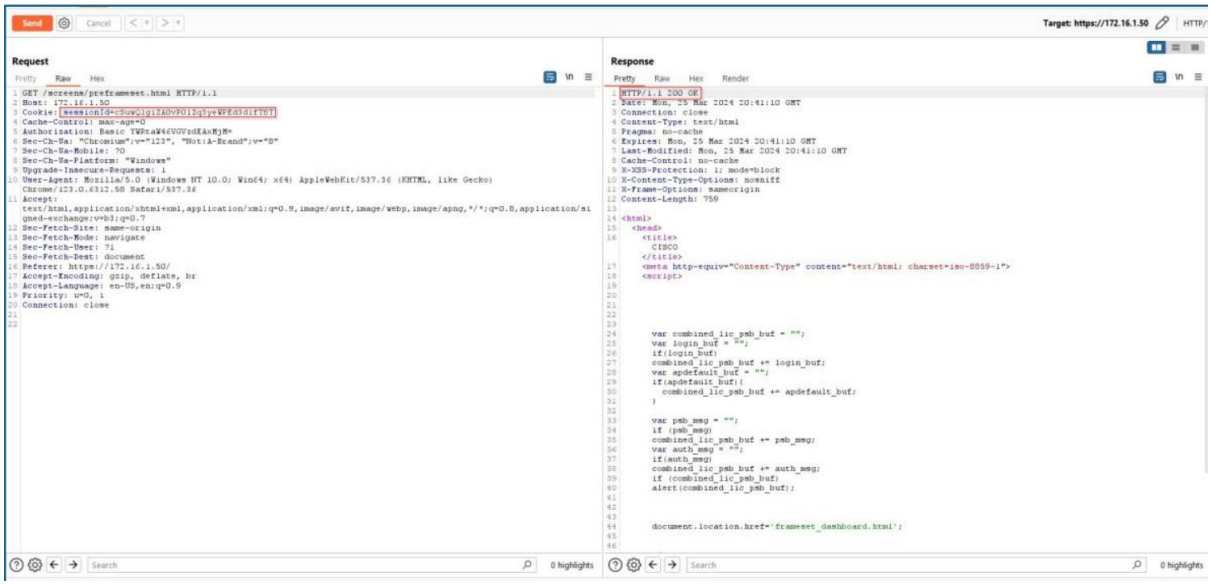


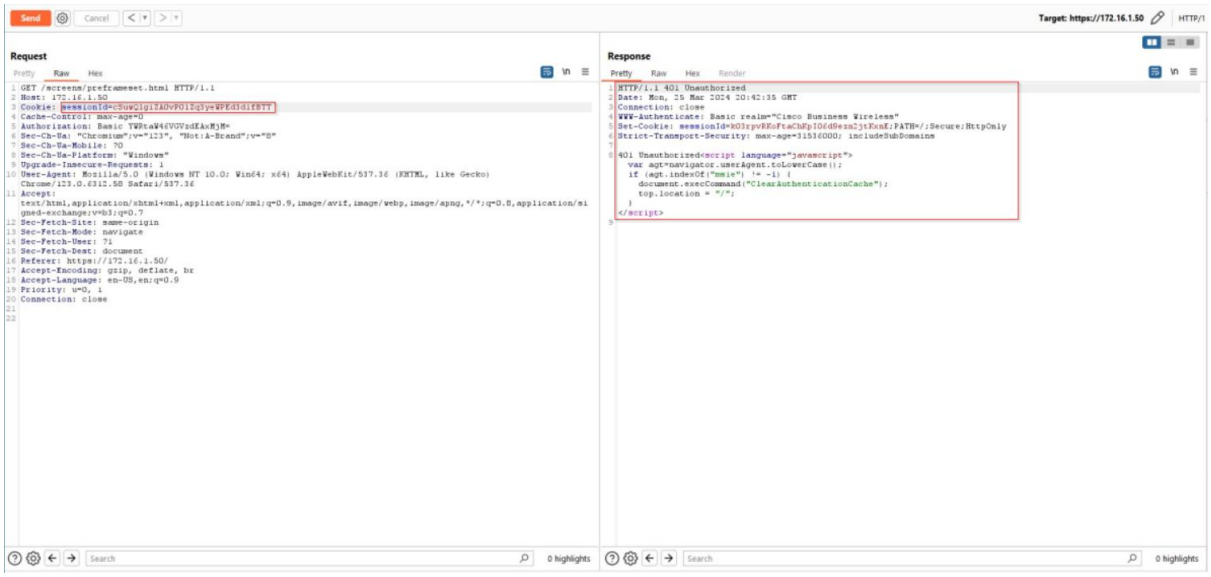
Step 3: Remove the session id and then click send.

Step 4: Observe that the error message is triggered

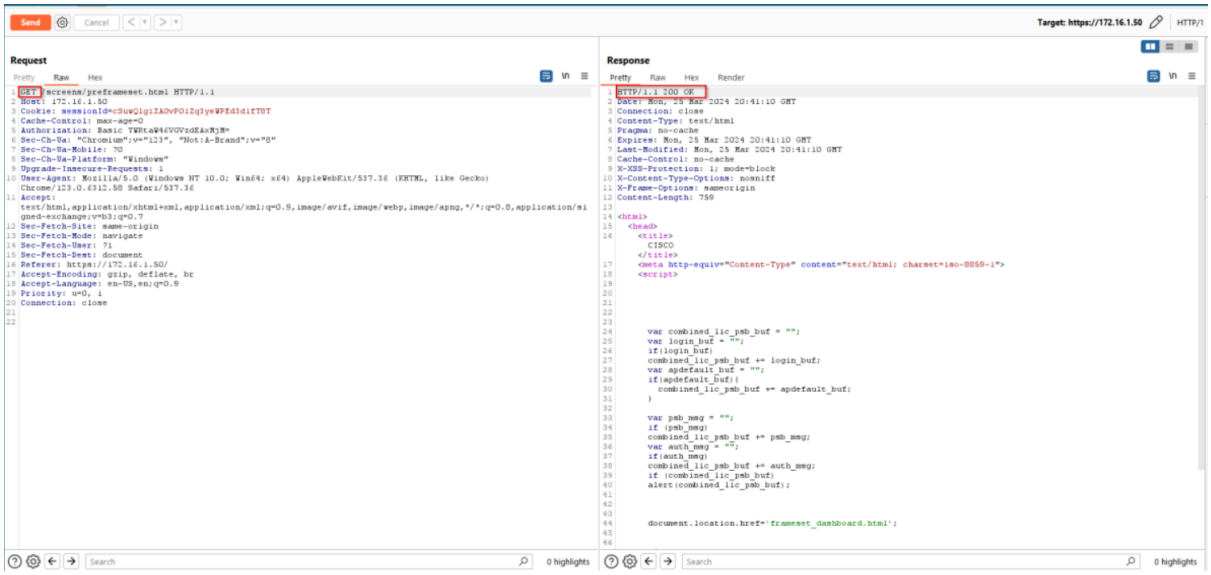


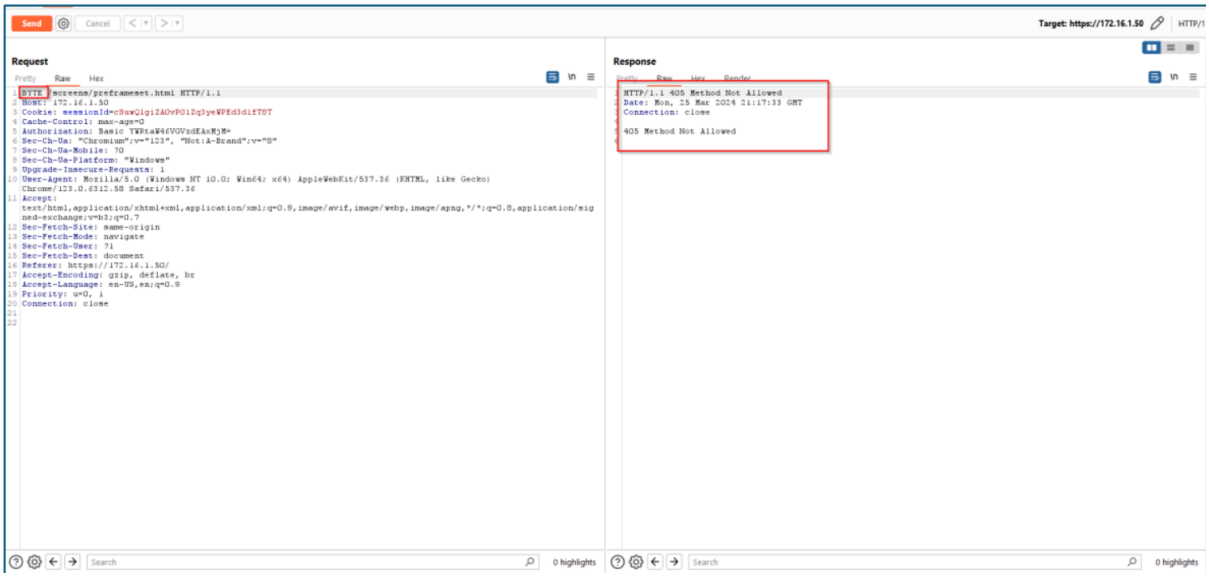
Step 5: Changed the session id and then click send and observer the error message is triggered.



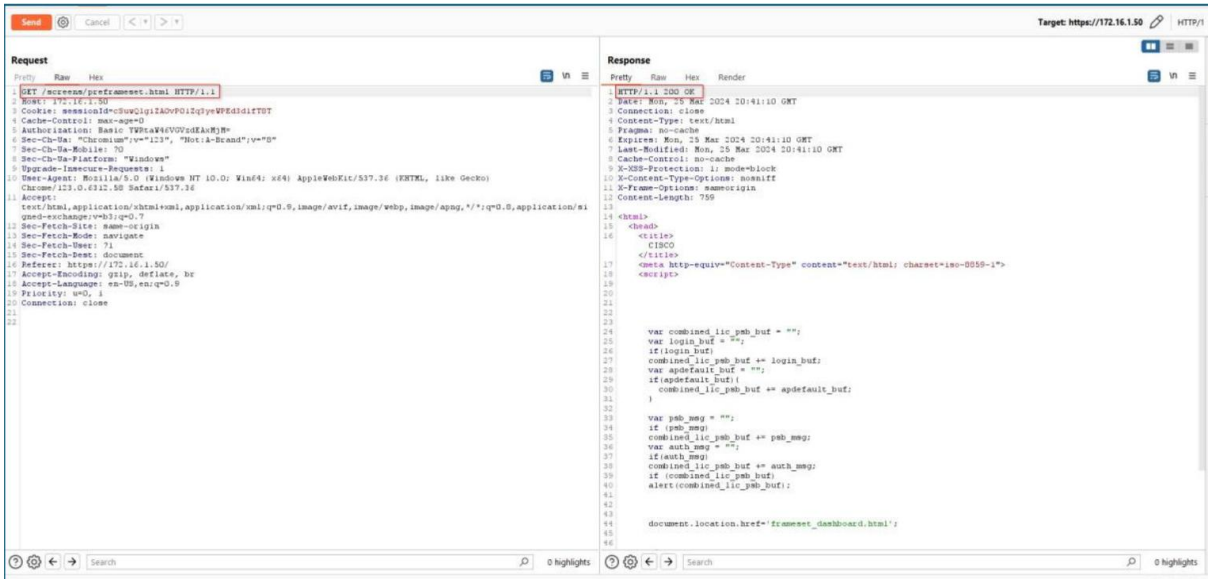


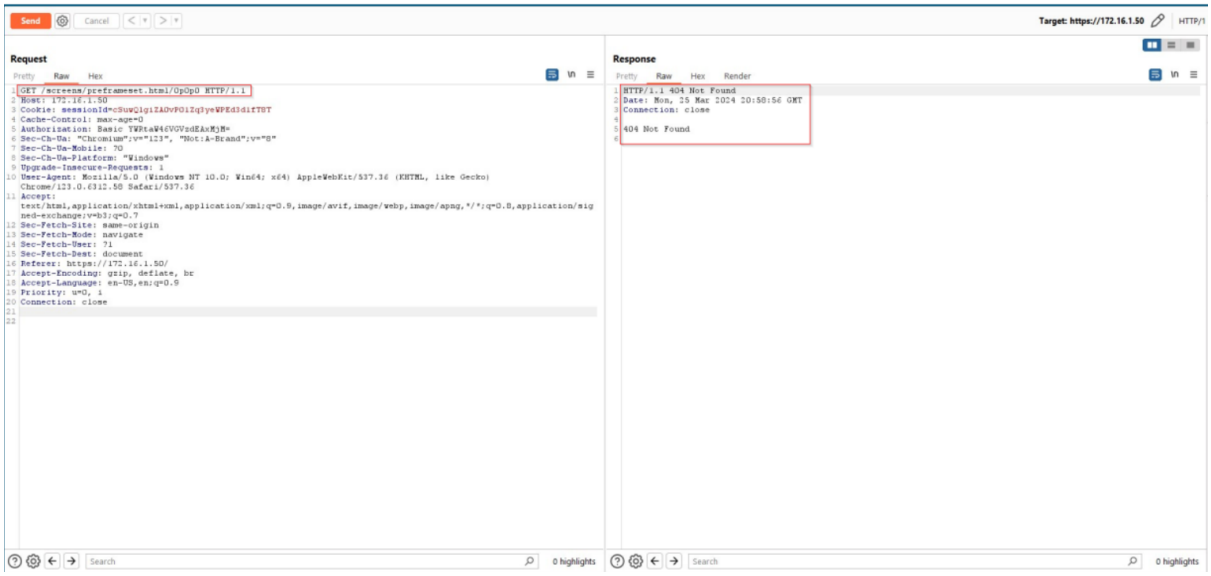
Step 6: Changed the HTTP method and then click send and observer the error message is triggered.



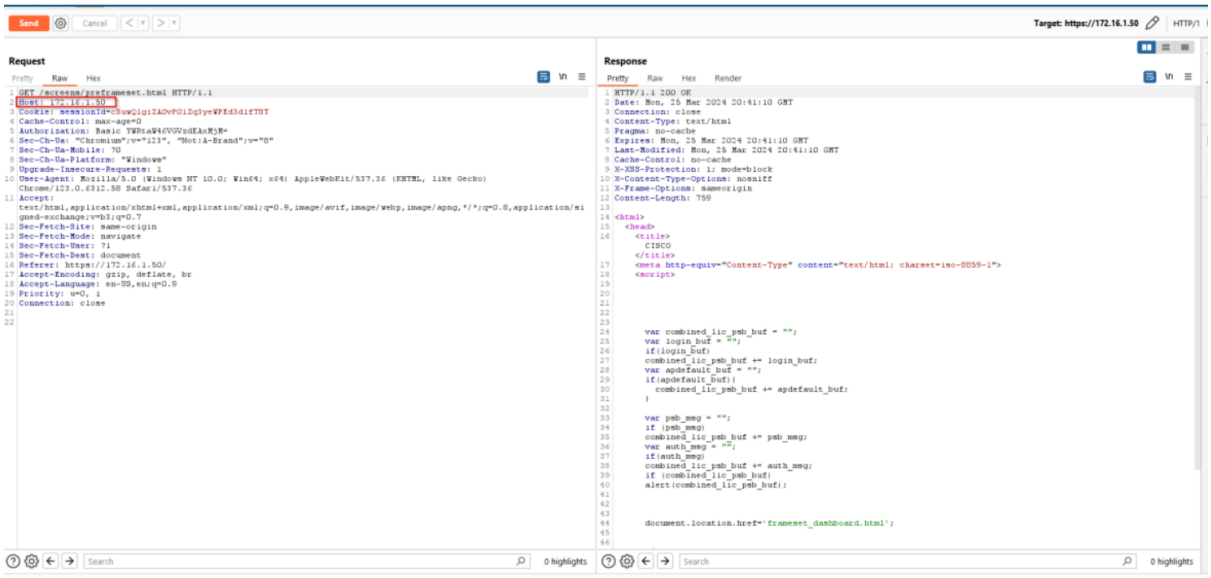


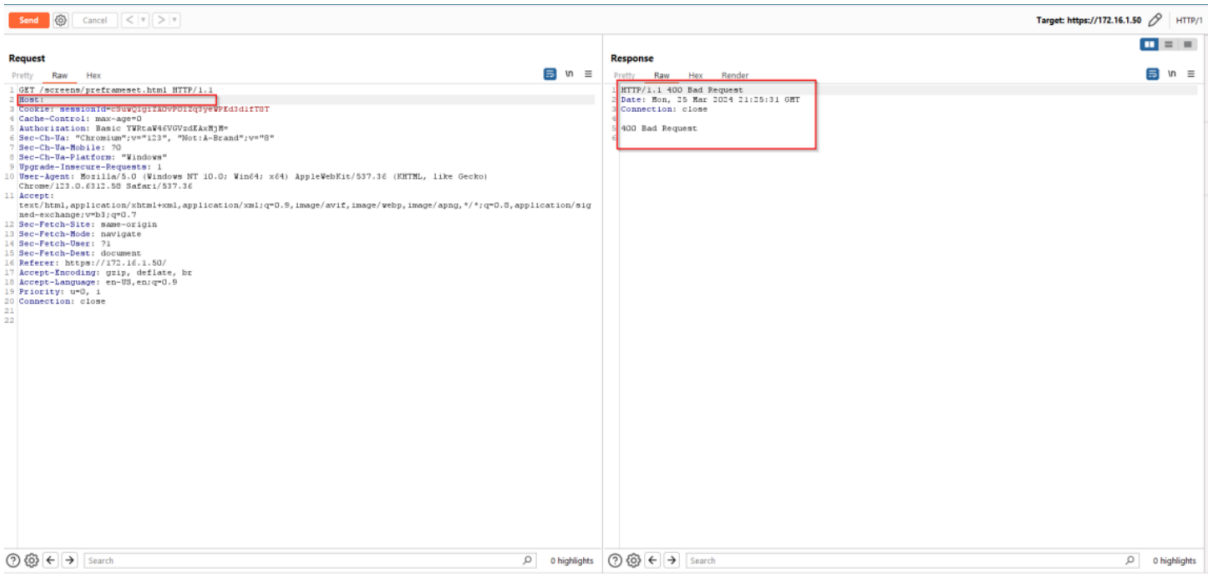
Step 7: Changed the file path and then click send and observer the error message is triggered.





Step 8: Removed the HOST IP and then click send and observer the error message is triggered.





11.1.4 **Test Observations:** During the testing process it was observed that User-defined error page has not included version information about the web server and the modules/add-ons used. Error messages does not include internal information such as internal server names, error codes, etc

12. **Test Case Result:**

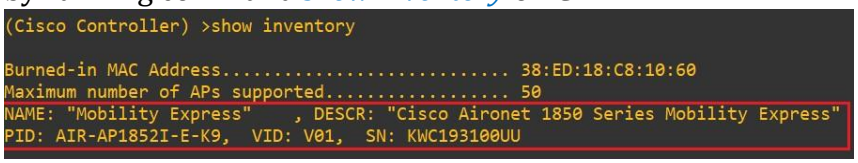
S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_WEB_SERVER_ERROR_PAGES_INFORMATION	PASS	all the criteria have been met

Section 1.12: Other Security Requirement

1.12.1: Remote Diagnostic Procedure - Verification

<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 12 Other Security Requirement
2. **<Security Requirement No & Name >** 1.12.1 Remote Diagnostic Procedure - Verification
3. **<Requirement Description: >** If the CPE is providing Remote access for troubleshooting purposes/alarm maintenance, then it should be allowed only for authorized users and all activities performed by the remote user is to be logged with parameters like User id, time stamp, interface type, event level (e.g., CRITICAL, MAJOR, MINOR), result type (e.g., SUCCESS, FAILURE).
4. **DUT Confirmation Details**:
   - This section involves information about DUT like software/firmware version, Hardware version model.
   - DUT Cisco WLC contains default boot image with version 8.10.183.0. The model is AIRAP1852I-E-K9. The inventory shows model serial no. & model description.
   - Verification of DUT Cisco wireless LAN controller's HW product series information by running command *show inventory* on CLI.



   - Verification of DUT Cisco WLC's high-level system SW information by running command *show sysinfo* on CLI.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.10.183.0
OUI File Last Update Time........................ N/A

System Name...................................... Aironet-Controller
System Location..................................
System Contact...................................
System ObjectID.................................. 1.3.6.1.4.1.9.1.2250
IP Address....................................... 10.208.38.2
Last Reset....................................... 1: reload command

System Up Time................................... 0 days 3 hrs 33 mins 5 secs
System Timezone Location......................... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
System Stats Realtime Interval................... 5
System Stats Normal Interval..................... 180

Configured Country............................... IN  - India

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled

--More-- or (q)uit
```

- Verification of DUT Cisco WLC's system information on Web access.

5. **DUT Configuration**:

   Login to DUT with username 'admin' (with read-write privilege) and create a new user 'Test' with read-only privilege.

```
root@APMUMCSAE002D:/etc# ssh Admin@10.208.38.2


(Cisco Controller)
User: Admin
Password:********
Welcome to the Cisco Mobility Express command line interface.
Only commands which are listed in the command reference guide for this release are supported.
http://www.cisco.com/c/en/us/support/wireless/mobility-express/products-command-reference-list.html
```

Screenshot shows login with 'admin' user to DUT.

```
(Cisco Controller) >config mgmtuser add Test Test@123 read-only
```

Screenshot shows creating a new user with read-only permissions.

```
(Cisco Controller) >show mgmtuser

User Name                Permissions    Description           Password Strength   Telnet Capable   Password Type
-----------------------  -----------  --------------------  -----------------  --------------  ------------
Admin                    read-write                                Strong          Yes             Type-0
Test                     read-only                                 Strong          Yes             Type-0
```

Screenshot shows the user is created in user database.

show interface summary (to check the status of physical interfaces)

```
(Cisco Controller) >show interface summary

 Number of Interfaces..... 2

Interface Name                   Port Vlan Id  IP Address      Type    Ap Mgr Guest
-------------------------------- ---- -------- --------------- ------- ------ -----
management                       1    untagged 10.208.38.2     Static  Yes    N/A
virtual                          N/A  N/A      192.0.2.1       Static  No     N/A
```

Screenshot shows the available interface available in the DUT

show sysinfo (it shows different parameters like, software version info, serial no, conf register, etc)

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.10.183.0
OUI File Last Update Time........................ N/A

System Name...................................... Aironet-Controller
System Location.................................
System Contact..................................
System ObjectID.................................. 1.3.6.1.4.1.9.1.2250
IP Address....................................... 10.208.38.2
Last Reset....................................... 1: reload command

System Up Time................................... 1 days 20 hrs 59 mins 59 secs
System Timezone Location......................... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
System Stats Realtime Interval................... 5
System Stats Normal Interval..................... 180

Configured Country............................... AL  - Albania
```

Screenshot shows the DUT info like 1) manufacturer 2) DUT version 3) model etc.

6. **Preconditions:**
   - OEM need to provide the documentation to identify authorized/unauthorized users for remote login
   - Vendor should provide documentation to verify parameters present in audit logs.
7. **Test Objective:** To verify that DUT have remote login feature with only for authorized users
8. **Test Plan:**
   - Validating the remote access of DUT by authorized persons only
   - Validating the activity performed by the remote user have logged properly in the DUT

8.1 **Number of Test Scenarios:**

8.1.1 Network product is providing Remote access

8.1.2 Remote access for trouble shooting purpose should only be allowed to authorized users.

8.2 **Test Setup Diagram**

Testing Terminal
Test Terminal OS: Linux Ubuntu 22.04.3
IP Address: 10.208.38.11
Putty V 0.76
OpenSSH_8.9p1

DUT
Cisco AP Aironet 1850
IP Address: 10.208.38.2

8.3 **Tools Used:**

- DUT terminal(Console)

8.4 **Test Execution Steps:** Below are the execution steps,

Case 1: Network product is providing Remote access.

1) Attempt to login to DUT via SSH with admin user (read-write privilege).
2) Verify the remote login is successful via audit logs.

Case 2: Remote access for trouble shooting purpose should only be allowed to authorized users.

NOTE: DUT has 3 privilege levels. Lobby-admin being the lowest and read-write being the highest,

- Read-write: Users with read-write privilege can execute all the show, config, and exec commands.
- Read only: Users with read only privilege can execute only the show commands.
- Lobby-Admin: Users who can create only guest user accounts. While creating a guest user, a lobby ambassador can create and delete a guest user.

A. Authorized user (read-only) can login remotely and perform trouble shooting/maintenance actions.
B. Login to DUT with username 'admin' (with read-write privilege) and create a new user 'Test' with read-only privilege.
   Login with the username 'user1'.
   Now for trouble shooting purpose execute below commands & check their output.
   - Show logging (to view audit logs for all the critical activities like (changing passwords, rebooting device etc.), login messages, config changes, physical interface related changes, Crypto parameter changes etc.).
   - Show Interface summary (to check the status of physical interfaces)
   - Show sysinfo (it shows different parameters like, software version info, serial no, conf register etc.)
C. Verify that for each action performed in step a.3) above, the DUT generated audit records capturing the following details:
   - User ID of the user that issued the command.
   - Time Stamp
   - Interface type
D. Event level (Critical, major, minor etc.)
   - Result type (success, failure)
   - Authorized user (Read-write) can login remotely and perform trouble shooting/maintenance actions.

- Login to DUT with username Admin (Read-write privilege).
- Now for trouble shooting purpose execute below commands & check their output.

i. Show logging (to view audit logs for all the critical activities like (changing passwords, rebooting device etc.), login messages, config changes, physical interface related changes, Crypto parameter changes etc.).
ii. Show Interface summary (to check the status of physical interfaces)
iii. Show sysinfo (it shows different parameters like, software version info, serial no, conf register etc.)
iv. config mightier add Test Test@123 read-only (To create new user)

E. Verify that for each action performed in step a.3) above, the DUT generated audit records capturing the following details:

i. User ID of the user that issued the command.
ii. Time Stamp
iii. Interface type
iv. Event level (Critical, major, minor etc.)
v. Result type (success, failure)

F. Unauthorized user(Lobby-admin) can login remotely.

i. Login to DUT with username Admin (Read-Write Privilege) and create a new user 'test_lobby' with privilege lobby-admin.
ii. Attempt to Login with the unprivileged user 'test_lobby'.

9. **Expected Result for Pass:** Authorized users only able to login remotely to the DUT at the same time the details of performed operations by a user will be logged.
10. **Expected Format of Evidence:** Screenshot of DUT terminal(Console)
11. **Test Execution:**

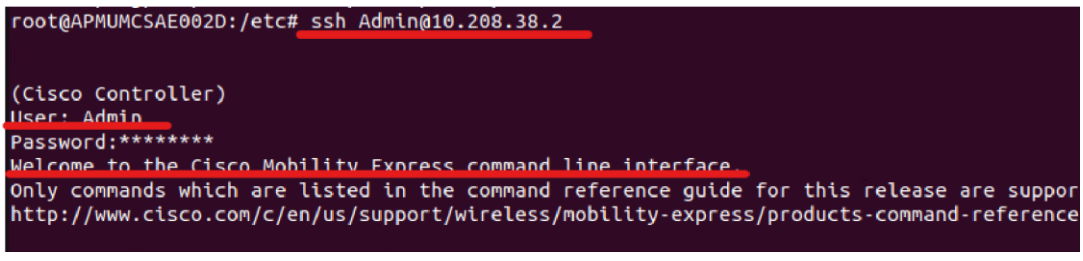
11.1 **Test Case Number:** 01

11.1.1 **Test Case Name:** TC_NO_REMOTE_ACCESS

11.1.2 **Test Case Description:** Verifying the DUT have remote access

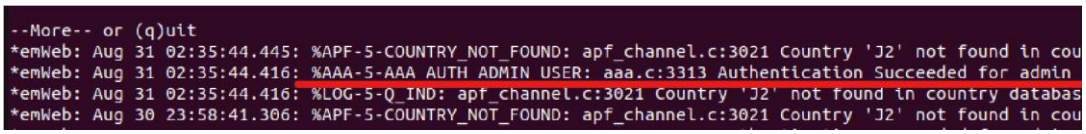
11.1.3 **Execution Steps:** Below are the execution steps with evidence:

1) Attempt to login to DUT via SSH with username 'admin' (read-write privilege).



Screenshot showing login with 'admin' user remotely via SSH.

2) Verify the remote login is successful via audit logs.



Screenshot showing successful login of 'admin' user via audit logs.

11.1.4 **Test Observations:** It is observed that the DUT provides remote access to users via SSH. The admin user is logged in successfully remotely and can access audit logs for reference.

11.2 **Test Case Number:** 02

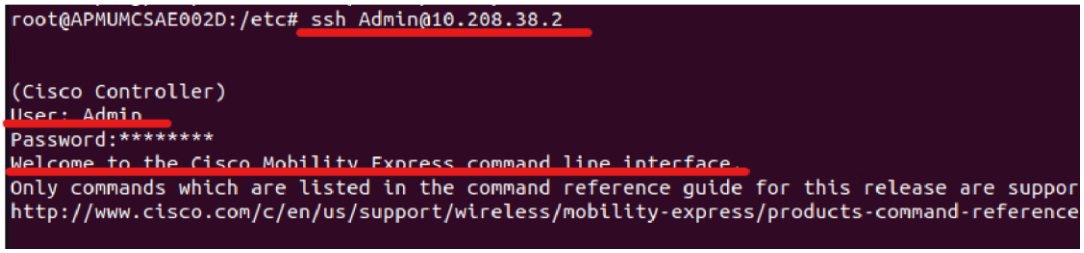
11.2.1 **Test Case Name:** TC_NO_REMOTE_ACCESS_WITH_AUTHORIZATION & LOG

11.2.2 **Test Case Description:** Verifying the DUT providing remote access to authorized persons only and all logs related to user performed.

11.2.3 **Execution Steps:**

1) Authorized user (read-only) can login remotely and perform trouble shooting/maintenance actions. a)

i. Login to DUT with username 'admin' (with read-write privilege) and create a new user 'Test' with read-only privilege.

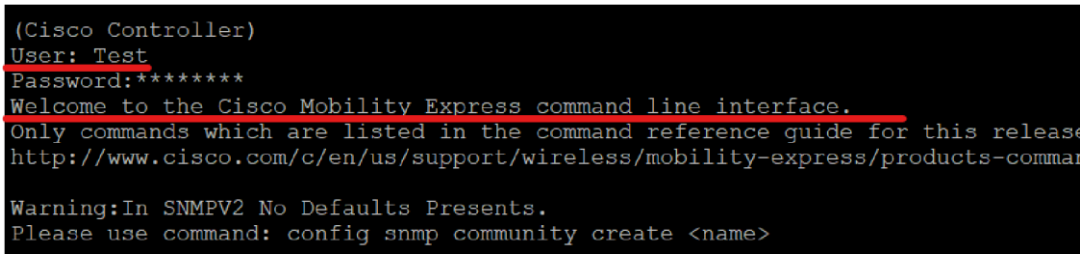


Screenshot showing login with 'admin' user remotely via SSH.

Screenshot shows creating a new user with read-only permissions.

Screenshot shows the user is created in user database.

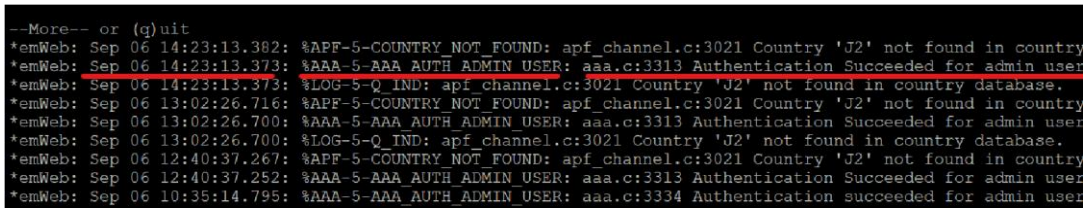
i. Login with the username 'user1'.



Screenshot showing successful login of newly created user 'test' with read-only privileges.

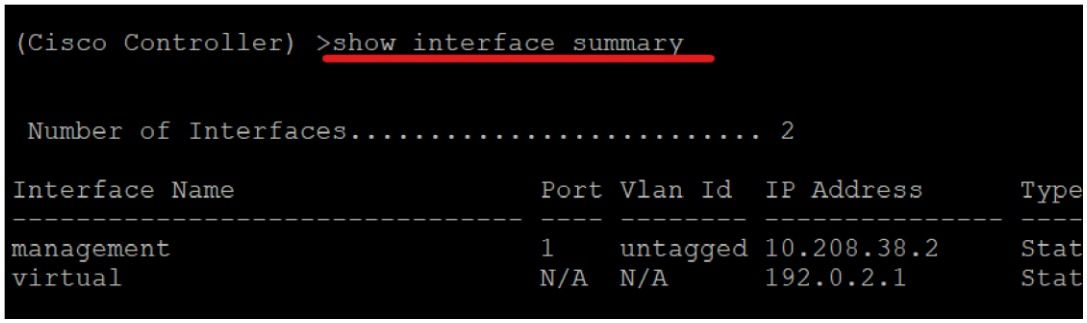
ii. Now for trouble shooting purpose execute below commands & check their output.

iii. Show logging (to view audit logs for all the critical activities like (changing passwords, rebooting device etc), login messages, config changes, physical interface related changes, Crypto parameter changes etc).



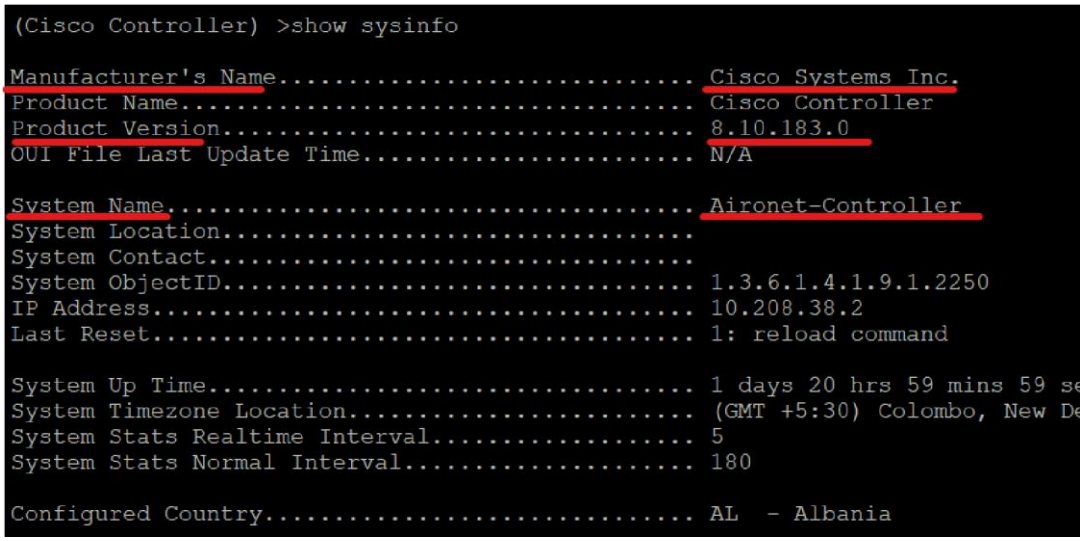
Screenshot showing the audit logs of successful login of 'Test' user.

iv. Show Interface summary (to check the status of physical interfaces)



Screenshot showing the physical interfaces available on DUT.

v. Show sysinfo (it shows different parameters like, software version info, serial no, conf register etc.)



Screenshot showing system info like 1) Manufacturer 2) Model 3) Product version etc.

Verify that for each action performed in step a.3) above, the DUT generated audit records capturing the following details:

- User ID of the user that issued the command.
- Time Stamp
- Interface type iv. Event level (Critical, major, minor etc.)
- Result type (success, failure)

It is found out that for user Test no action performed above is logged in log message. The Log messages only show login events.

Below are the details captured in log messages for login of user.

1) Timestamp format: Date and time of the message or event.

2) Facility: It denotes the source or the cause of the system message.

3) Severity: Single-digit code from 0 to 7 that is the severity of the message

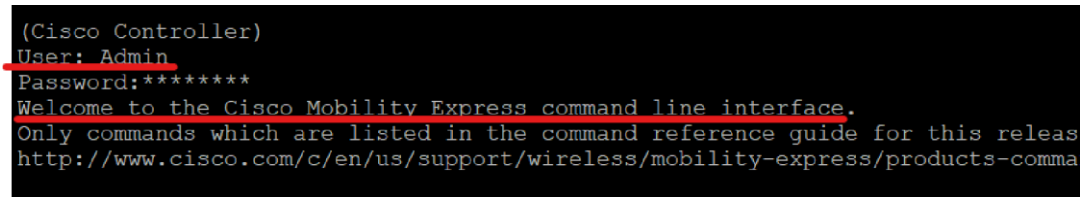
4) Mnemonic: Text string that uniquely describes the message

5) Description: Text string containing detailed information about the event being reported.

Note: The above list details are not like the details required in requirement description.

2) Authorized user (Read-write) can login remotely and perform trouble shooting/maintenance actions. a)

i. Login to DUT with username Admin (Read-write privilege).



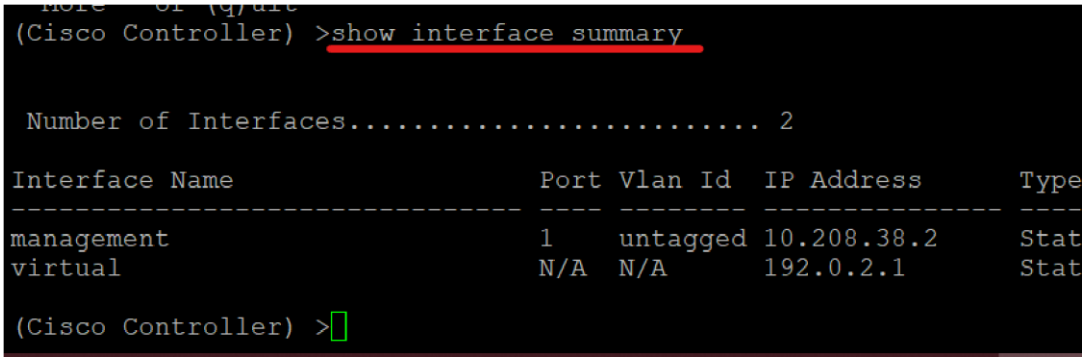
Screenshot showing the successful login of the 'admin' user.

ii. Now for trouble shooting purpose execute below commands & check their output

iii. 'Show logging' (to view audit logs for all the critical activities like changing passwords, rebooting device etc), login messages, config changes, physical interface related changes, Crypto parameter changes

Screenshot showing the 'show logging' output for successful login of 'admin' user.

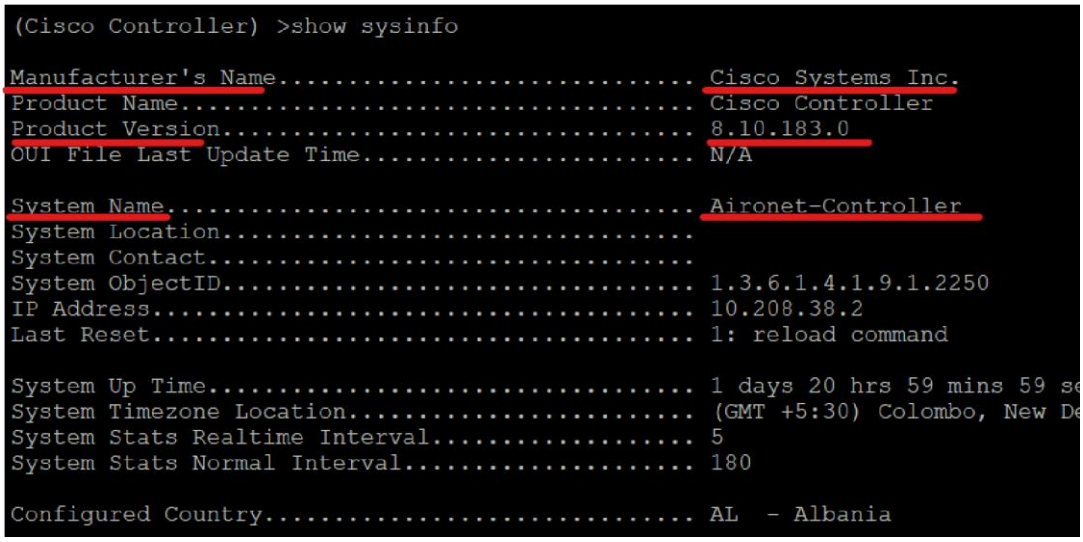
Interface summary' (to check the status of physical interfaces)



(it shows different parameters like, software version info,

Manufacturer 2) Product version 3) Model etc. Show

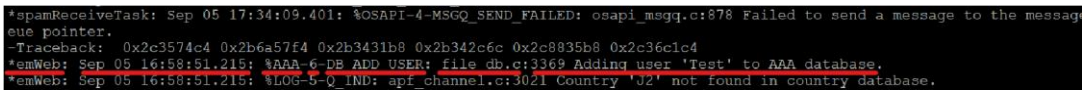
Screenshot shows available interfaces on DUT.



'Show sysinfo' serial no, conf register etc.)

Screenshot shows the system info like 1)

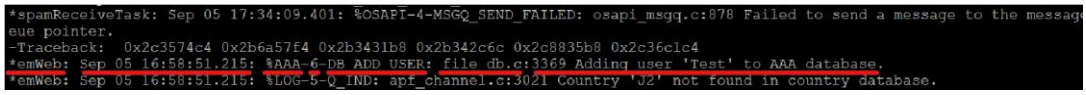
config mightier add Test Test@123 read-only' (To create new user)



Screenshot shows the user 'Test' created with read-only privileges and successfully login to DUT.

Verify that for each action performed in step a.3) above, the DUT generated audit records capturing the following details:

- User ID of the user that issued the command.
- Time Stamp
- Interface type iv. Event level (Critical, major, minor etc.)
- Result type (success, failure)



It has been found out that only the last command to create new user can generate the audit log, above all events are not able to generate any audit logs, The Audit logs that generated contains below details.

1) Timestamp format: Date and time of the message or event.

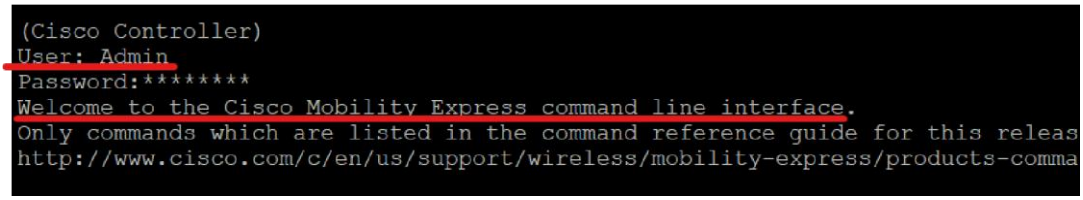
2) Facility: It denotes the source or the cause of the system message.

3) Severity: Single-digit code from 0 to 7 that is the severity of the message

4) Mnemonic: Text string that uniquely describes the message

5) Description: Text string containing detailed information about the event being reported.

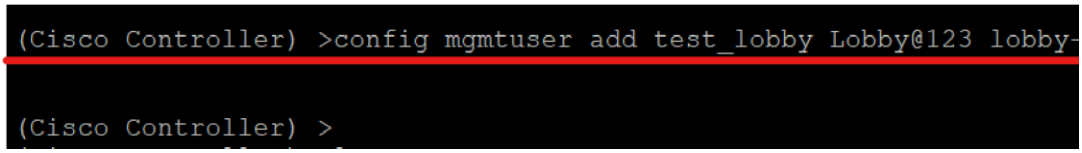
Note: The above list details are not like the details required in requirement description.



3) Unauthorized user (Lobby-admin) can login remotely. a)

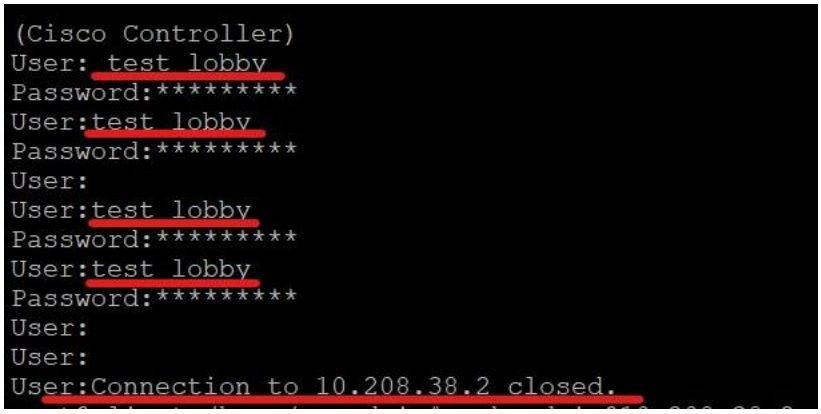
i. Login to DUT with username Admin (Read-Write Privilege) and create a new user 'test_lobby' with privilege lobby-admin.

Screenshot shows successful login to DUT with 'admin' user.

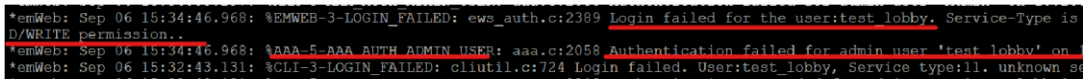


Screenshot shows command to create the new user 'test_lobby' with lobby-admin privileges.

ii. Attempt to Login with the unprivileged user 'test_lobby'.



Screenshot shows user 'test_lobby' can't login cause of no read or write privileges.



Screenshot shows the audit logs for login denied for 'test_lobby' user. elow are the execution steps with evidence:

11.2.4 **Test Observations:**

- It is observed that the authorized users with read-only privilege can login remotely and perform trouble shooting activities like show audit logs, show interface status, show system info, but DUT cannot generate audit logs for the activities performed by read-only users.
- It is observed that the authorized users with read-write privilege (Admin users) can login remotely and perform trouble shooting activities like show audit logs, show interface status, show system info, create new users but DUT cannot generate audit logs for the activities performed by read-write users. Users with read-write privilege are admin users.
- The DUT only generates audit logs for successful login.
- It is observed that for unauthorized users with lobby-admin privileges DUT does not allow remote login, The unauthorized users can't login remotely and hence the unauthorized users with Lobby-admin privileges cannot perform any trouble shotting activities.

12. Test Case Result:

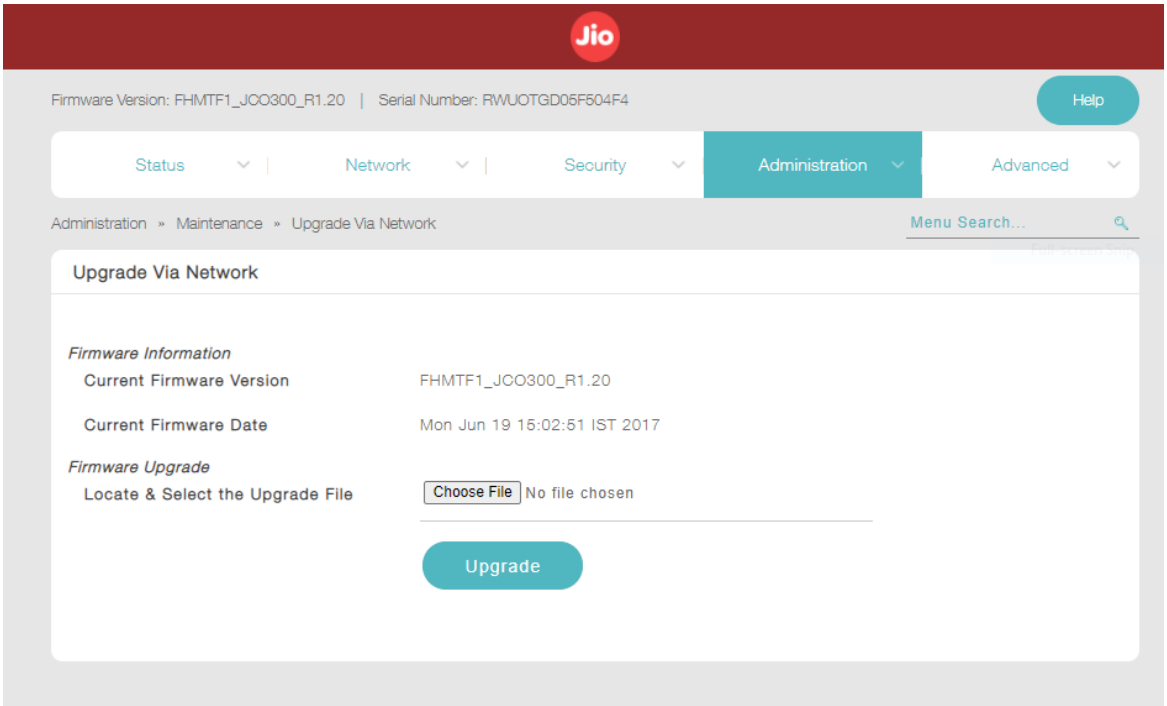
S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_REMOTE_ACCESS	PASS	
2	TC_NO_REMOTE_ACCESS_WITH_AUTHORIZATION & LOG	FAIL	

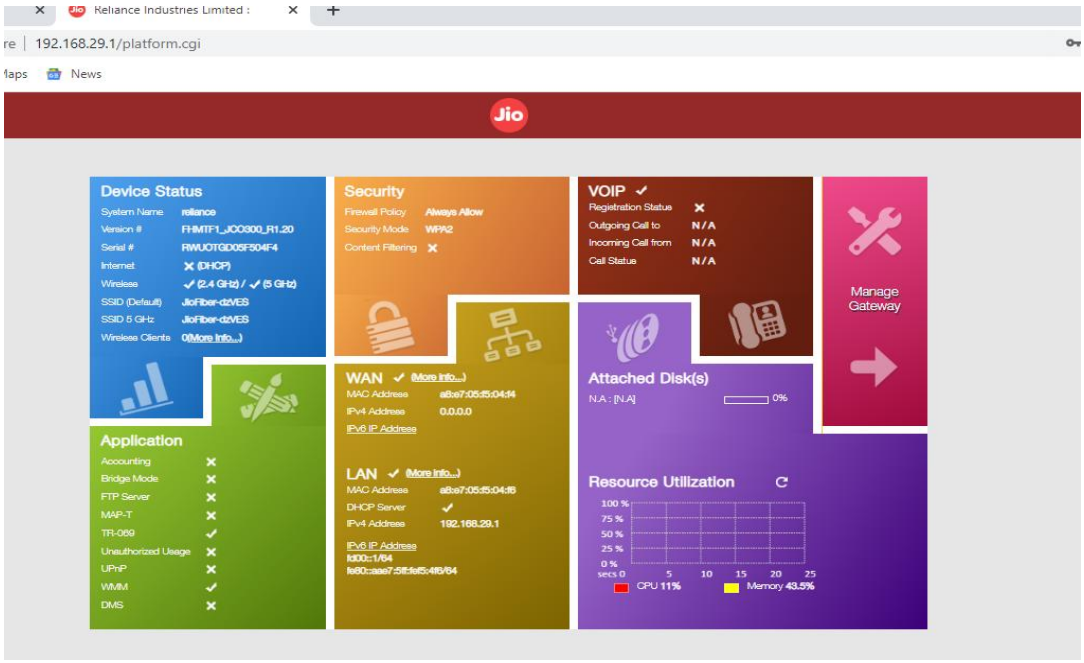
1.12.2 No Password Recovery

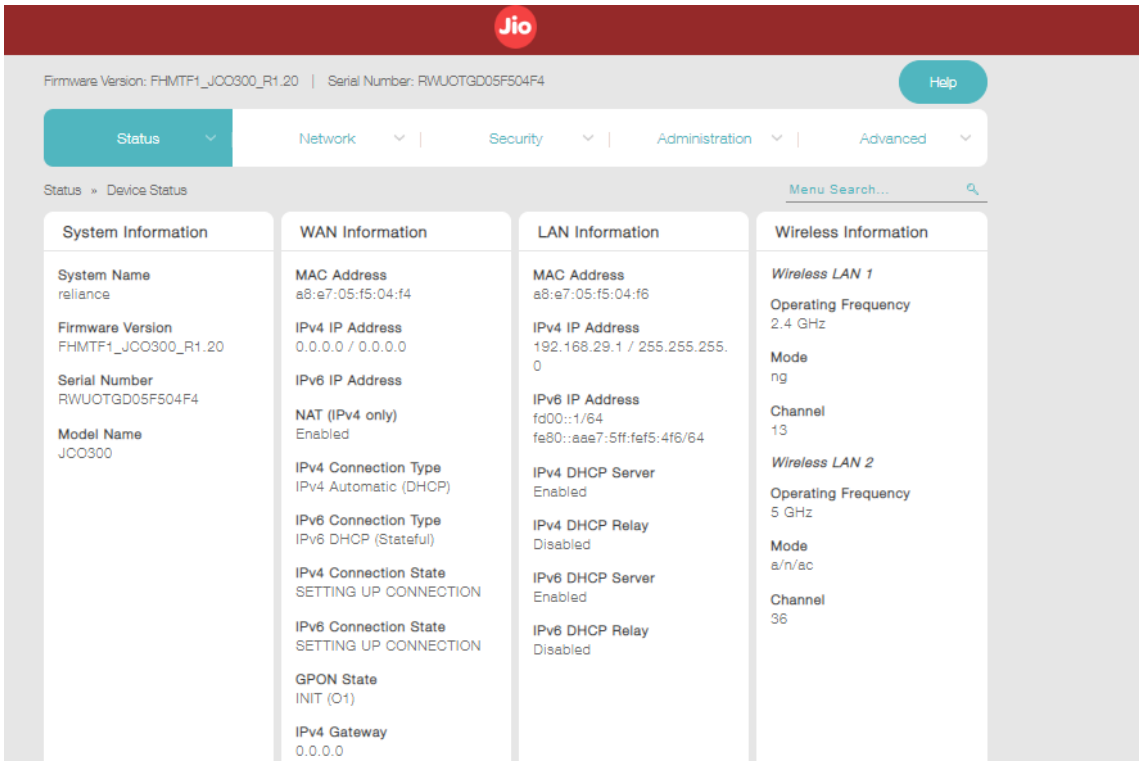
<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 1.12 Other Security Requirement
2. **<Security Requirement No & Name >** 1.12.2 No Password Recovery
3. **<Requirement Description: >** Network devices have a function that resets the current system password. In the event of system password reset, the entire configuration of the CPE shall be irretrievably deleted. No provision should exist for password recovery.
4. **DUT Confirmation Details**:
   - Use the command line/GUI interface to get details of the machine on which test is conducted.
   - Use GUI to get Application No/Version No & hardware Info

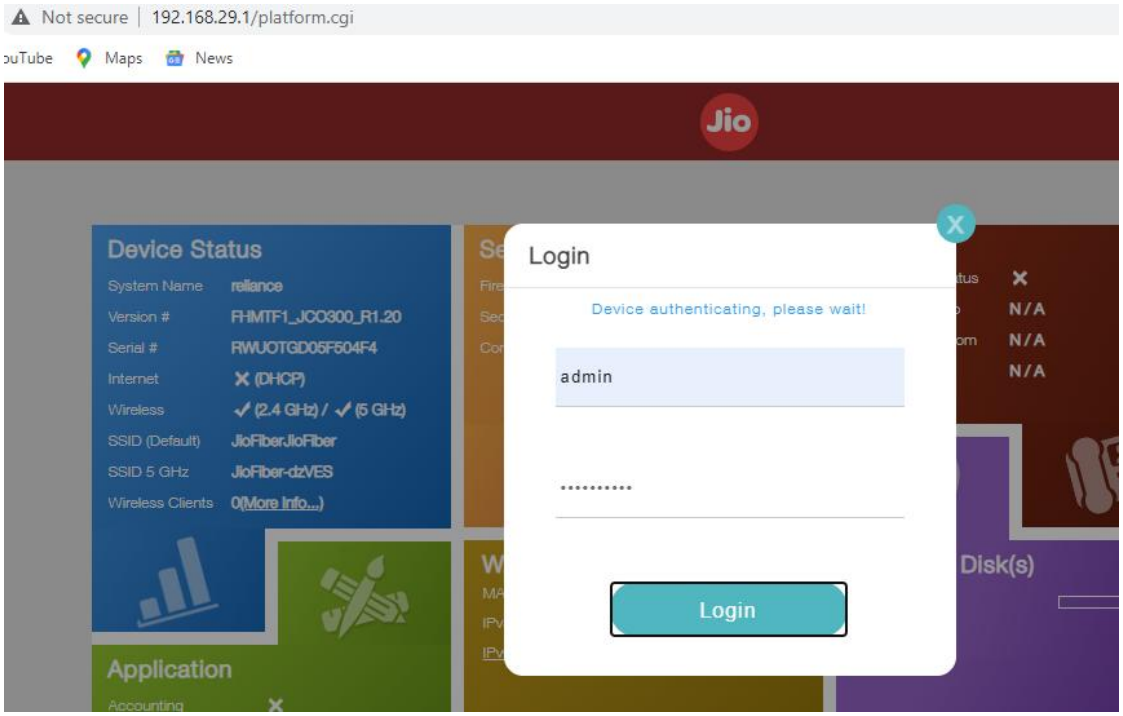
The below screenshot shows the firmware version of the DUT







5. **DUT Configuration**:
    - The Tester opens GUI(https) of DUT(192.168.29.1) in tester machine (192.168.29.118).



- The Tester attempts to login DUT using “admin” account.

6. **Preconditions:** OEM need to provide documentation regarding how to reset the system credentials in the DUT by using password reset/factory reset

7. **Test Objective:** To verify that it is possible to reset the system credentials in the DUT using password reset/factory reset

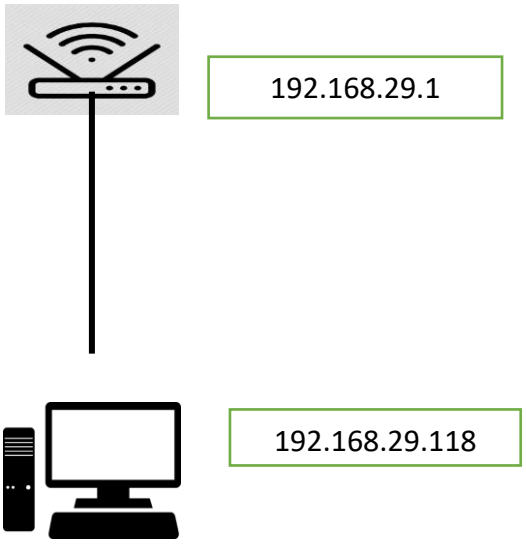
8. **Test Plan:**
   - The tester list the list of system accounts available in the DUT
   - Reset the password of system account in the DUT
   - Factory reset the DUT

   8.1 **Number of Test Scenarios:**

   8.1.1 Reset the system accounts in the DUT

   8.1.2 Factory reset the DUT

8.2 **Test Setup Diagram**



8.3 **Tools Used:** Web browser(client)

8.4 **Test Execution Steps:** The tester must verify for the compliance to the pre-requisites:

- Reset the current system password in the DUT
- Perform factory reset in the DUT

9. **Expected Result for Pass:** System password recovery should not be possible in the DUT.
10. **Expected Format of Evidence:** Screenshot of DUT webpage
11. **Test Execution:**

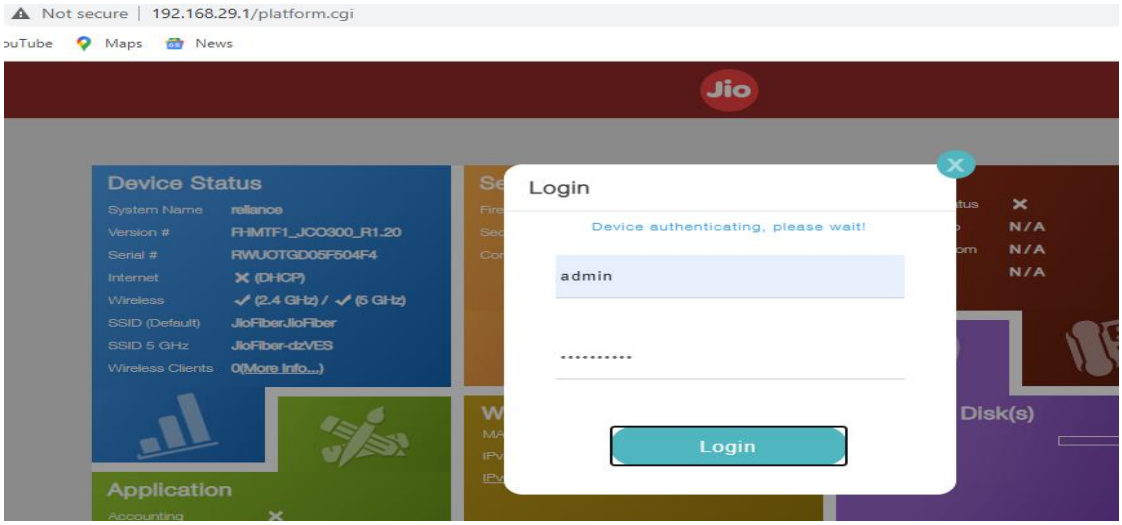
11.1 **Test Case Number:** 01

11.1.1 **Test Case Name:** TC_NO_CURRENT_SYSTEM_PW_RESET

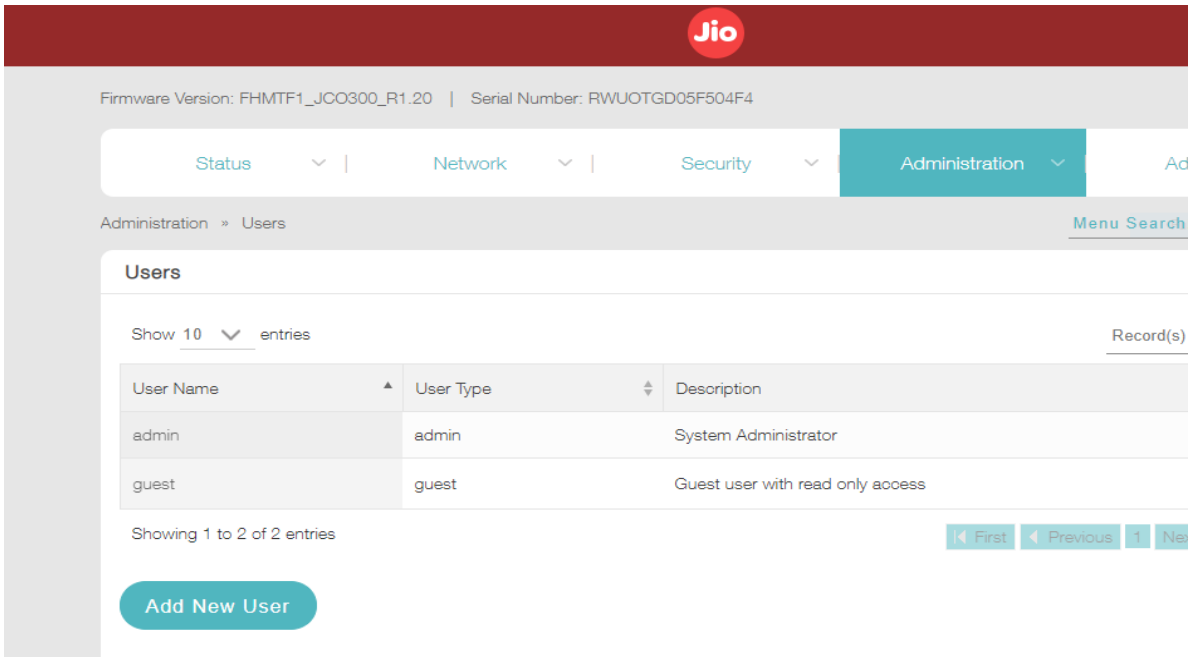
11.1.2 **Test Case Description:** Ensuring that DUT have system password reset option

11.1.3 **Execution Steps:**

1. Login to the DUT with admin credentials



2. Check the list of available users in the DUT



3. Reset the system password for accounts “admin” and “guest”

11.1.4 **Test Observations:** DUT have the capability to do the system password reset

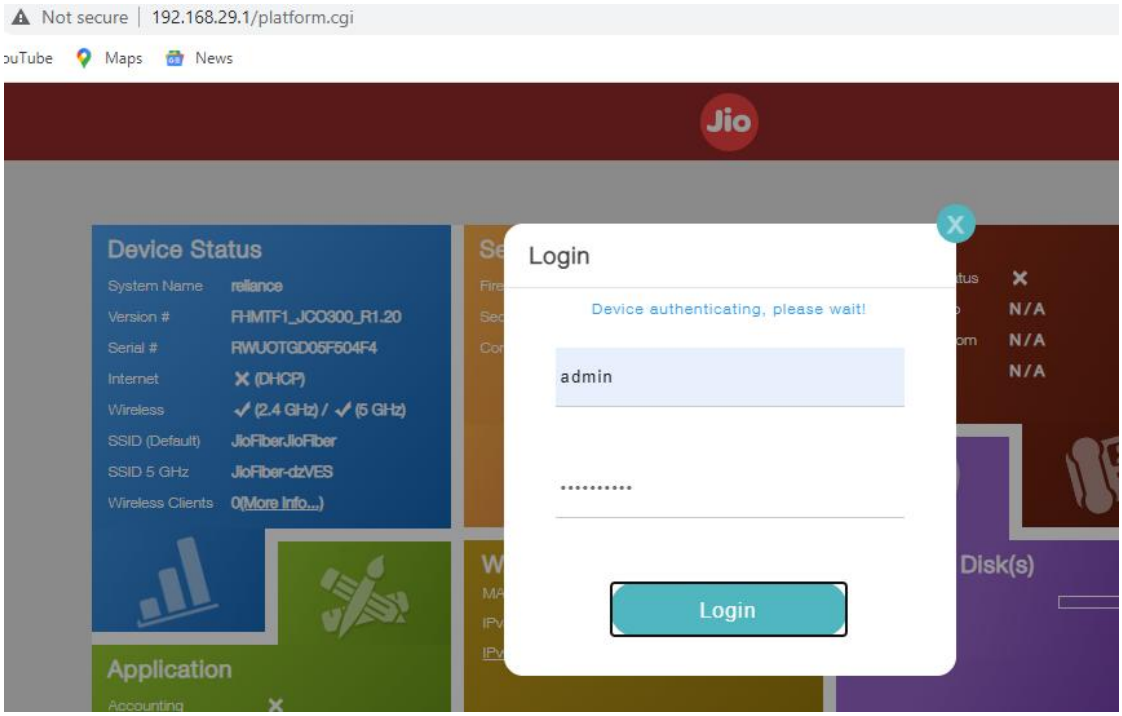
11.2 **Test Case Number:** 02

11.2.1 **Test Case Name:** TC_NO_FACTORY_RESET

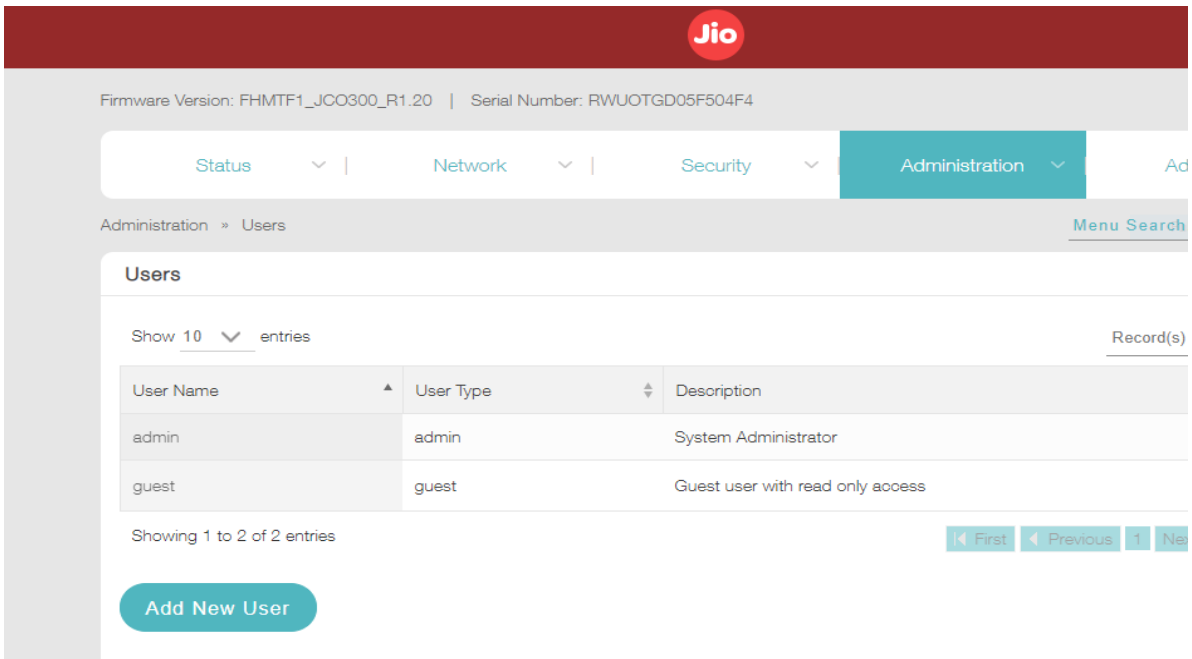
11.2.2 **Test Case Description:** Ensuring that entire configuration of DUT(including system credential) recovery is not possible after performing factory reset

11.2.3 **Execution Steps:**

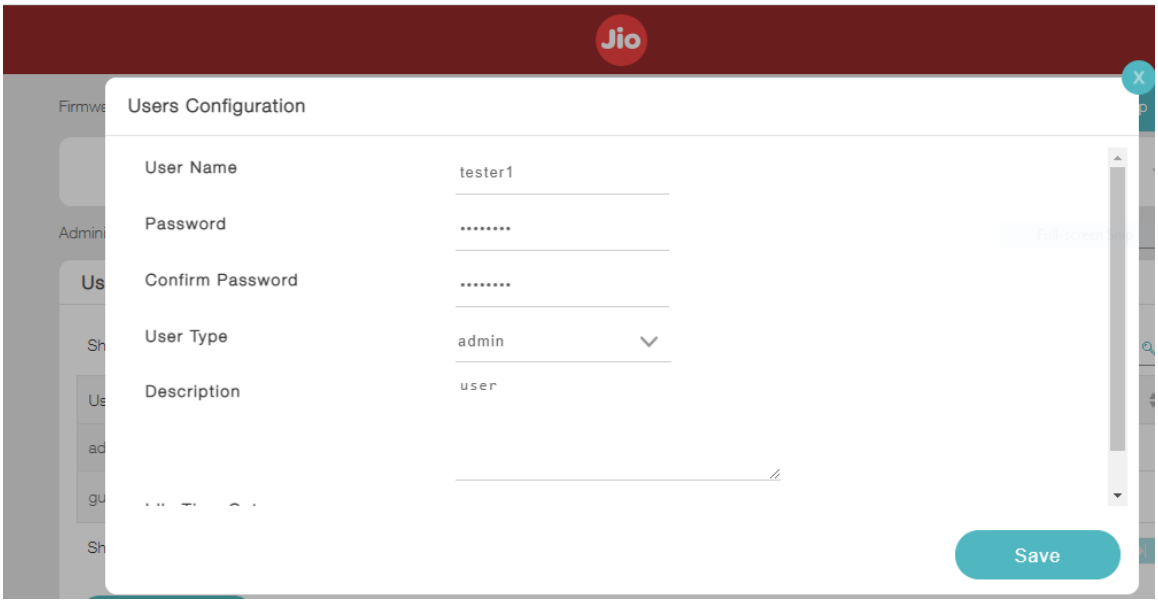
1. Login to the DUT with admin credentials



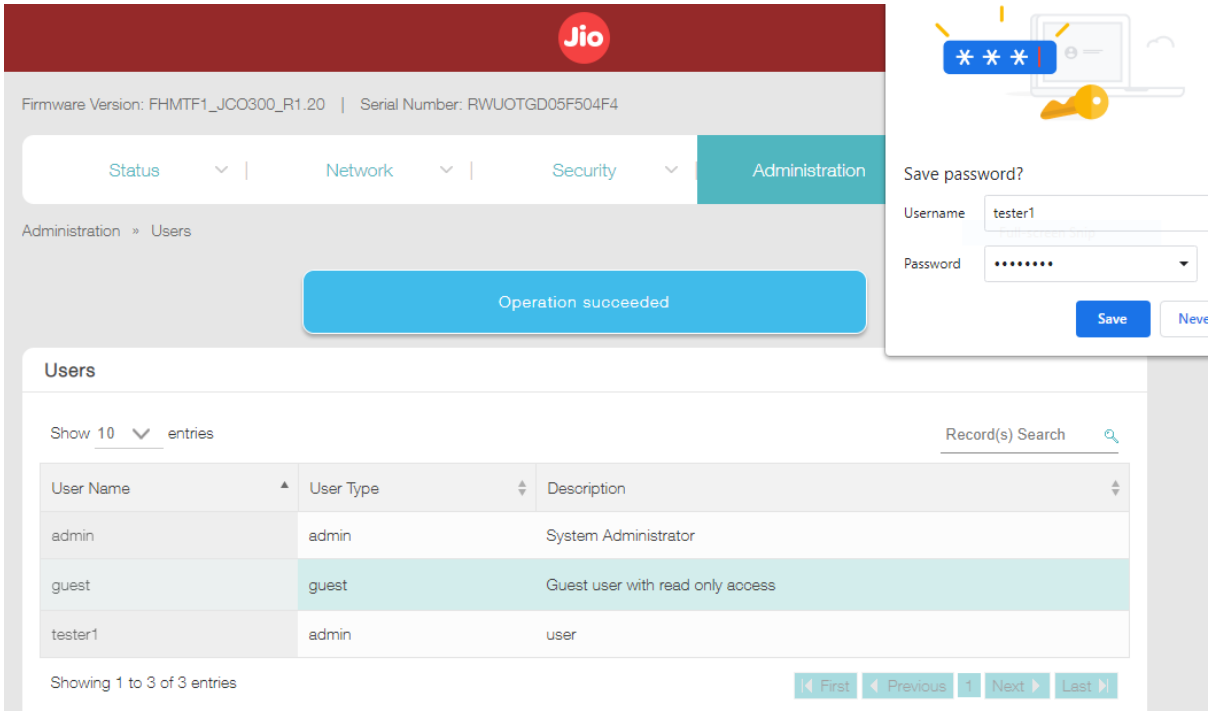
2. Check the list of available users in the DUT



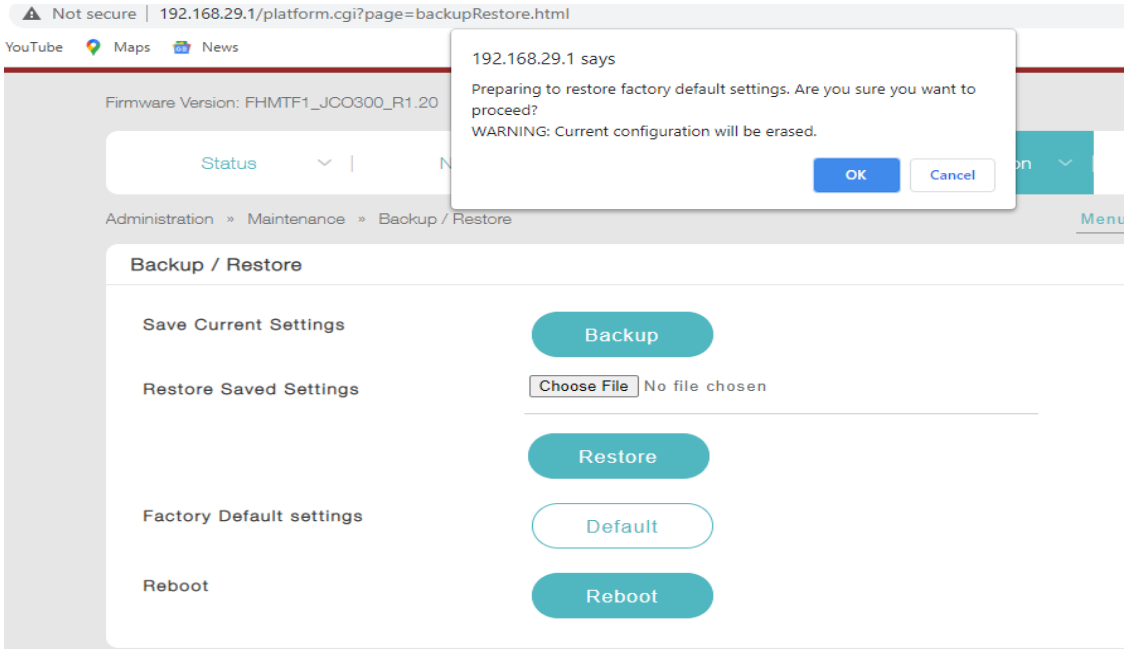
3. Create new system account in the DUT with the name of “tester1”



4. Again check the list of users available in the DUT

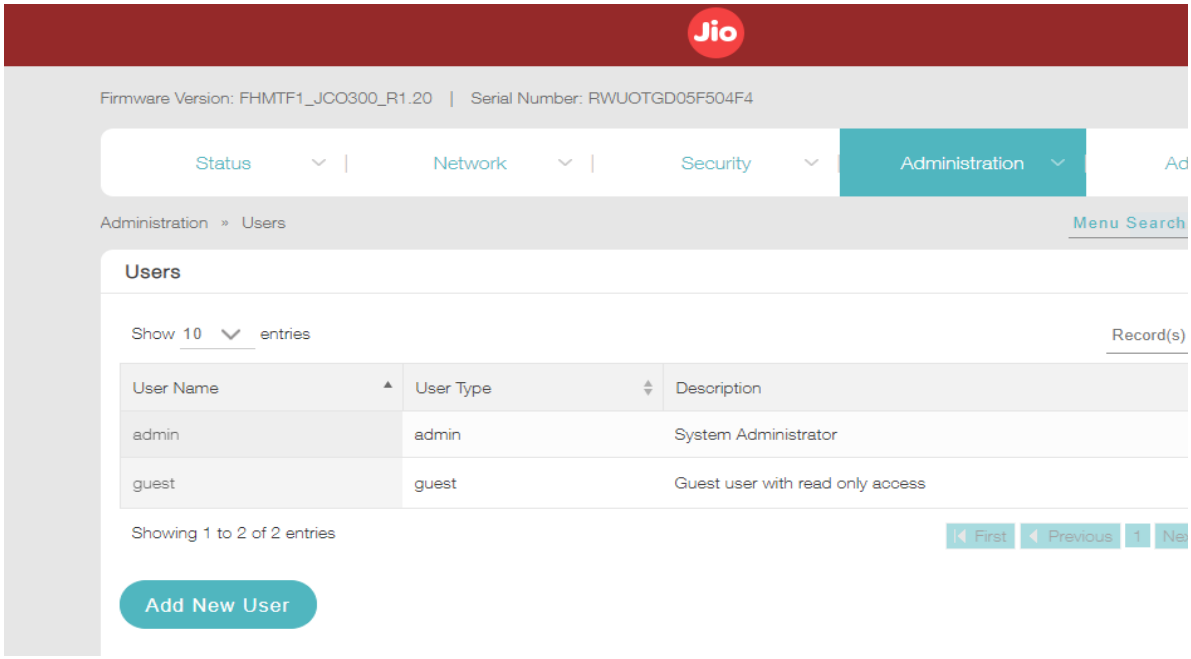


5. Perform factory reset on the DUT



6. Login the DUT with default credentials(Username - admin & Password – Jiocentrum)

7. Check the previously created user account “tester1” is there or not in the DUT



11.2.4 **Test Observations:** The previously created account is not there after performing factory reset. So, Password recovery is not possible. The previously configured information also deleted.

12. **<u>Test Case Result:</u>**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_CURRENT_SYSTEM_PW_RESET	PASS	
2	TC_NO_FACTORY_RESET	PASS	

1.12.3 Software Integrity Check - Installation

<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 12 Other Security Requirement
2. **<Security Requirement No & Name >** 1.12.3 Software Integrity Check - Installation
3. **<Requirement Description: >** CPE should validate the software package integrity before the installation / upgrade. Tampered software shall not be executed or installed if integrity check fails.
4. **DUT Confirmation Details**:
   - This section involves information about DUT like software/firmware version, Hardware version model.
   - DUT Cisco WLC contains default boot image with version 8.10.183.0. The model is AIRAP1852I-E-K9. The inventory shows model serial no. & model description.
     Verification of DUT Cisco wireless LAN controller's HW product series information by running command *show inventory* on CLI.

```
(Cisco Controller) >show inventory

Burned-in MAC Address.............................. 38:ED:18:C8:10:60
Maximum number of APs supported..................... 50
NAME: "Mobility Express"    , DESCR: "Cisco Aironet 1850 Series Mobility Express"
PID: AIR-AP1852I-E-K9,  VID: V01,  SN: KWC193100UU
```

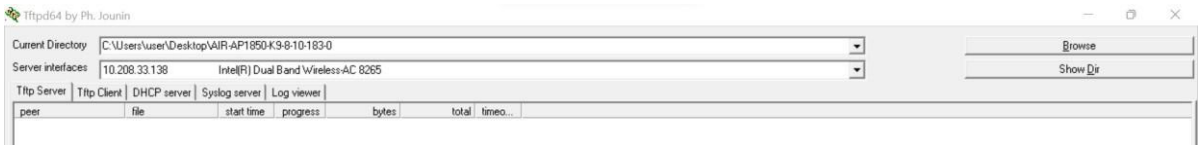
     Verification of DUT Cisco WLC's high-level system SW information by running command *show sysinfo* on CLI.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name................................ Cisco Systems Inc.
Product Name....................................... Cisco Controller
Product Version.................................... 8.10.183.0
OUI File Last Update Time.......................... N/A

System Name........................................ Aironet-Controller
System Location.....................................
System Contact......................................
System ObjectID.................................... 1.3.6.1.4.1.9.1.2250
IP Address......................................... 10.208.38.2
Last Reset......................................... 1: reload command

System Up Time..................................... 0 days 3 hrs 33 mins 5 secs
System Timezone Location........................... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
System Stats Realtime Interval..................... 5
System Stats Normal Interval....................... 180

Configured Country................................. IN  - India

State of 802.11b Network........................... Enabled
State of 802.11a Network........................... Enabled

--More-- or (q)uit
```

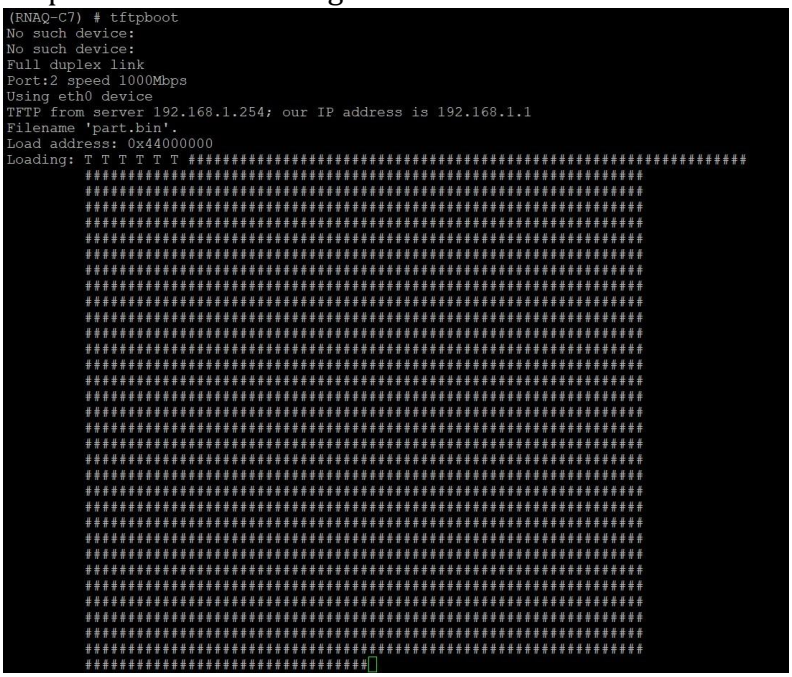
     Verification of DUT Cisco WLC's system information on Web access.

5. **DUT Configuration**:

1) Copy the updated software image from windows terminal to DUT with the help of TFTP.



Screenshot showing the file transfer via TFTP from test terminal to DUT, the file transfer includes updated software image.



Screenshot showing the updated software image being copied from test terminal to DUT via TFTP.

2) Run Hexeditor of terminal machine and change certificate values in the boot image.

```
-rw-rw-r--  1 mumadmin mumadmin  63250484 Jun 19 11:57 part.bin
root@APMUMCSAE002D:/home/mumadmin# hexedit part.bin
```

Screenshot showing the software image 'part.bin' is tampered using hexeditor.
Screenshot continues,

```
BE EF CA FE  01 00 02 01  01 02 00 04  00 00 01 74  ..S .....=...................t
73 74 65 6D  73 3B 4F 55  3D 4C 50 3B  4F 3D 43 69  ..Y..$CN=NescoSystems;OU=LP;O=Ci
36 41 35 36  36 06 00 24  43 4E 3D 4E  65 73 63 6F  scoSystems...6396A566..$CN=Nesco
43 69 73 63  6F 53 79 73  74 65 6D 73  07 00 01 00  Systems;OU=AP;O=CiscoSystems....
EC 13 66 70  9E BC B7 63  E2 9C D9 C2  FE 3B AB C2  ..................fp...c.....;..
DD 50 5C 08  4F 34 4E F5  5F 61 D3 5F  A5 76 64 1F  ...J..!.)...5.g..P\.O4N._a._.vd.
39 E9 CA 55  C5 23 6A 15  59 6B 40 89  04 72 55 31  _...K.%+.OP%.{rO9..U.#j.Yk@..rU1
DC 08 CD 0B  A2 F8 7B 39  95 50 AB 4D  FC 44 72 A3  .V...c6MI..qI.j?......{9.P.M.Dr.
43 59 C6 6D  00 C6 94 38  CA BA 5F DB  A6 91 75 34  ...XC6L.[L'.h;(?CY.m...8.._...u4
35 45 88 92  5C 6B 72 80  4D F4 E7 EC  A3 AC 1E 4E  .......J.Z....=p5E..\kr.M.......N
A6 62 D2 55  11 1C 3E 55  52 6E 42 53  63 87 E9 39  ..@#..K..6a.%.^..b.U..>URnBSc..9
A9 14 0B 8C  B1 02 9C 5C  99 A1 F7 5C  D8 11 1B 38  .v.U|..0E...7+.........\...\...8
00 01 41 EB                                         1..%.B...eR...t...A.
```

Screenshot showing the values changed in certificate of the software image thus tampering the image.

6. **Preconditions:**
   - Vendors should provide updated software package/image for upgradation.
   - Vendors should provide tampered software to perform validation check.
   - Vendor should provide the documentation related software integrity check

7. **Test Objective:** To verify that DUT validate the software package integrity before the installation / upgrade stage or not

8. **Test Plan:** Installation/upgrade of software in the DUT

   8.1 **Number of Test Scenarios:**

   8.1.1 8.1.1 DUT should validate the software package integrity before the installation/upgrade

   8.1.2 Tampered software shall not be executed or installed if integrity check fails.

   8.2 **Test Setup Diagram**

Testing Terminal
Test Terminal OS: Linux Ubuntu 22.04.3
IP Address: 10.208.38.11
Putty V 0.76
OpenSSH_8.9p1

DUT
Cisco AP Aironet 1850
IP Address: 10.208.38.2

   8.3 **Tools Used:**

   - DUT terminal(Console), Hex Editor,TFTP for file transfer

   8.4 **Test Execution Steps:** Below are the execution steps,

CASE 1: DUT should validate the software package integrity before the installation/upgrade.

- Login to DUT with Admin user and verify current version of the DUT firmware.
- Copy the updated software image from windows terminal to DUT with the help of TFTP.
- Verify that integrity check is executed before the updated software image is loaded. Verify that updated software image is loaded after successful integration check.

CASE 2: Tampered software shall not be executed or installed if integrity check fails.

- copy the boot image (part.bin) from DUT to terminal for tampering.
- Run Hex editor of terminal machine and change certificate values in the boot image.
- After editing save the edited image and copy the tampered boot image over TFTP. Verify that the DUT check the integrity of the software image downloaded from TFTP server before installation. Device failed to load the tampered image giving error message as Image signing verification failed.

9. **Expected Result for Pass:**
    - DUT validating the software image by verifying their integrity
10. **Expected Format of Evidence:** Screenshot of DUT terminal(Console), Configuration of Hex editor and configuration of TFTP server
11. **Test Execution:**

11.1 **Test Case Number:** 01

11.1.1 **Test Case Name:** TC_NO_SOFTWARE_INTEGRITY_VERIFICATION

11.1.2 **Test Case Description:** Validating the DUT software installation based on integrity

11.1.3 **Execution Steps:**

Below are the execution steps with evidence:

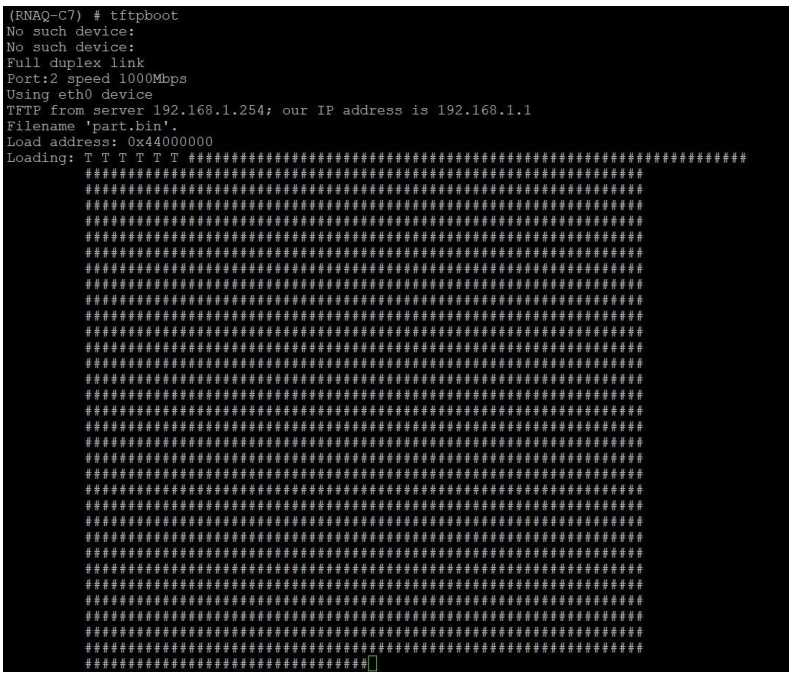
- Login to DUT with Admin user and verify current version of the DUT firmware.

```
(Cisco Controller) >show run-config

Press Enter to continue...

System Inventory
NAME: "Mobility Express"     , DESCR: "Cisco Aironet 1850 Series Mobility Expr
PID: AIR-AP1852I-E-K9,  VID: V01,  SN: KWC193100UU

Burned-in MAC Address.............................. 38:ED:18:C8:10:60
Maximum number of APs supported.................... 50
Press Enter to continue or <ctrl-z> to abort


System Information
Manufacturer's Name................................ Cisco Systems Inc.
Product Name....................................... Cisco Controller
Product Version.................................... 8.10.151.0
OUI File Last Update Time.......................... N/A

System Name........................................ Cisco1852i
System Location.....................................
System Contact......................................
System ObjectID.................................... 1.3.6.1.4.1.9.1.2250
IP Address......................................... 10.208.38.2
Last Reset......................................... 1: reload command
```

Screenshot showing the current version of the software and model of DUT.

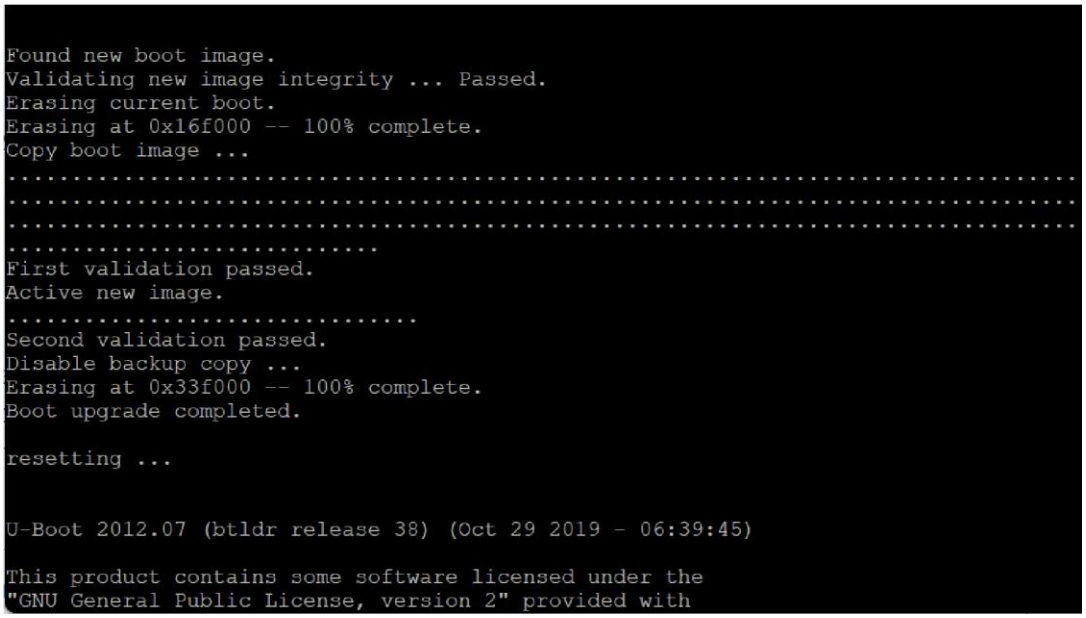
- Copy the updated software image from windows terminal to DUT with the help of TFTP.

Screenshot showing the file transfer via TFTP from test terminal to DUT, the file transfer includes updated software image.



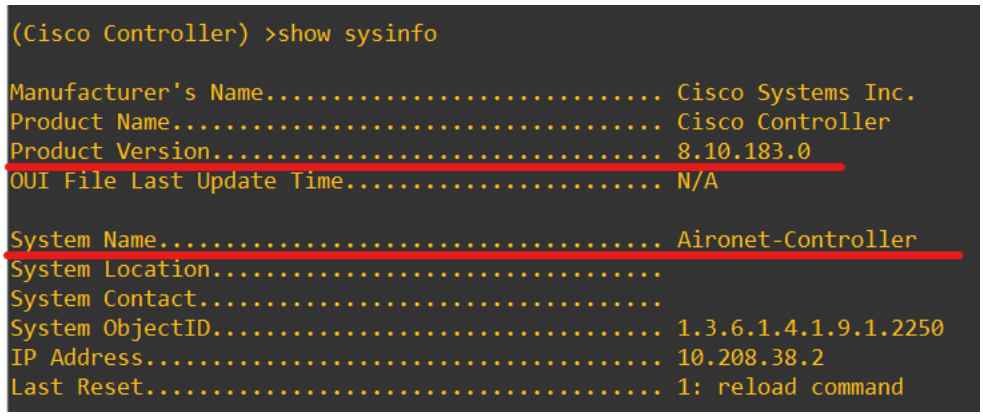
Screenshot showing the updated software image being copied from test terminal to DUT via TFTP.

- Verify that integrity check is executed before the updated software image is loaded.



Screenshot showing the DUT validating the integrity of the updated software image after it was transferred from test terminal to DUT. After a successful software integrity check DUT initiates the installation of new updated software image.

Verify that updated software image is loaded after successful integration check.



Screenshot showing that DUT got updated to new updated software image.

11.1.4 **Test Observations:** It is observed that the DUT validates the software package integrity before the installation/upgrade. The DUT verifies the updates software image once it was transferred from test terminal to DUT, the software image integrity validated before installation takes place after image is copied from test terminal to DUT.

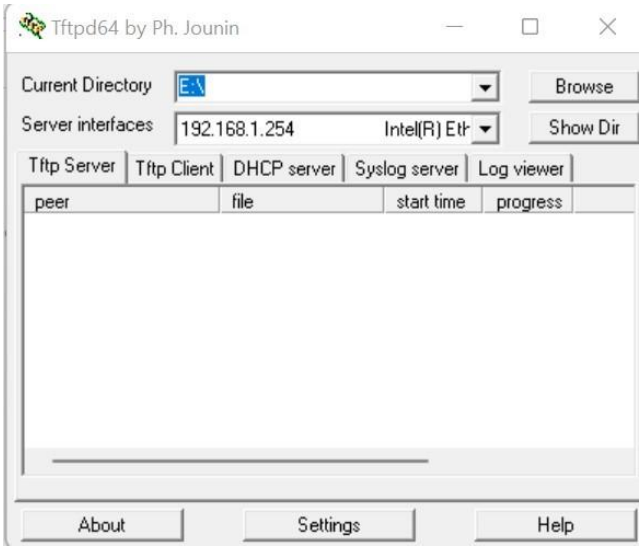
11.2 **Test Case Number:** 02

11.2.1 **Test Case Name:** TC_NO_TAMPERED_SOFTWARE_INTEGRITY_VERIFICATION

11.2.2 **Test Case Description:** Verifying the DUT not installing the tampered image

11.2.3 **Execution Steps:**

1) Copy the boot image (part.bin) from DUT to terminal for tampering.



Screenshot showing copying of image from DUT to test terminal with the help of TFTPd application installed on test terminal.

2) Run Hexeditor of terminal machine and change certificate values in the boot image.

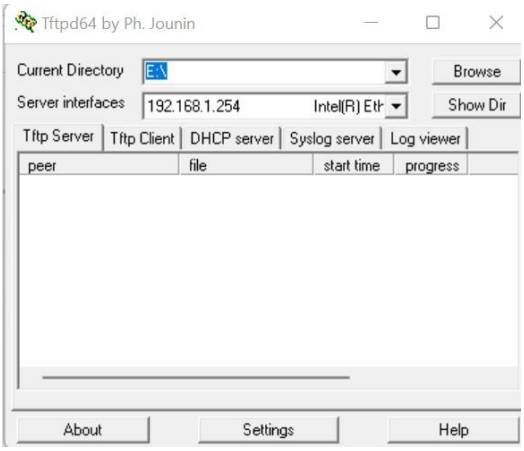
```
-rw-rw-r--  1 mumadmin mumadmin  63250484 Jun 19 11:57 part.bin
root@APMUMCSAE002D:/home/mumadmin# hexedit part.bin
```

Screenshot showing the software image 'part.bin' is tampered using hexeditor.

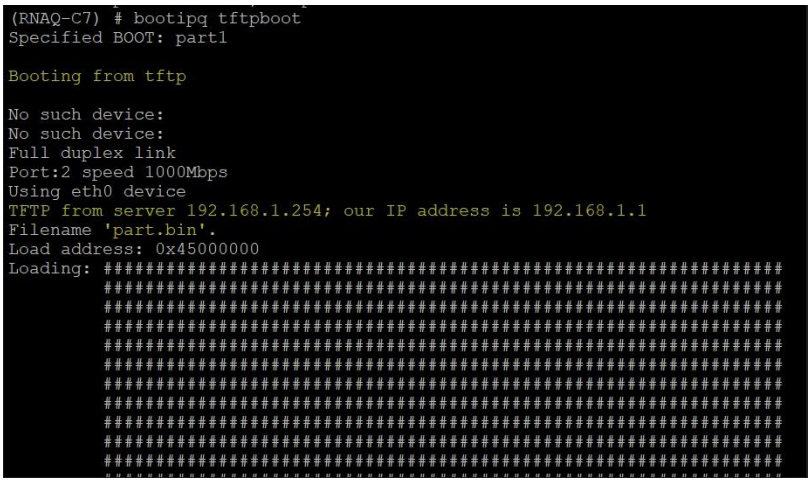
```
BE EF CA FE  01 00 02 01  01 02 00 04  00 00 01 74  ..S .....=.....t
73 74 65 6D  73 3B 4F 55  3D 4C 50 3B  4F 3D 43 69  ..Y..$CN=NescoSystems;OU=LP;O=Ci
36 41 35 36  36 06 00 24  43 4E 3D 4E  65 73 63 6F  scoSystems...6396A566..$CN=Nesco
43 69 73 63  6F 53 79 73  74 65 6D 73  07 00 01 00  Systems;OU=AP;O=CiscoSystems....
EC 13 66 70  9E BC B7 63  E2 9C D9 C2  FE 3B AB C2  .................fp...c.....;..
DD 50 5C 08  4F 34 4E F5  5F 61 D3 5F  A5 76 64 1F  ...J..!.)...5.g..P\.O4N._a._.vd.
39 E9 CA 55  C5 23 6A 15  59 6B 40 89  04 72 55 31  _...K.%+.OP%.{rO9..U.#j.Yk@..rU1
DC 08 CD 0B  A2 F8 7B 39  95 50 AB 4D  FC 44 72 A3  .V...c6MI..qI.j?......{9.P.M.Dr.
43 59 C6 6D  00 C6 94 38  CA BA 5F DB  A6 91 75 34  ...XC6L.[L'.h;(?CY.m...8.._...u4
35 45 88 92  5C 6B 72 80  4D F4 E7 EC  A3 AC 1E 4E  .......J.Z....=p5E..\kr.M.....N
A6 62 D2 55  11 1C 3E 55  52 6E 42 53  63 87 E9 39  ..@#..K..6a.%.^..b.U..>URnBSc..9
A9 14 0B 8C  B1 02 9C 5C  99 A1 F7 5C  D8 11 1B 38  .v.U|..0E...7+.....\...\...8
00 01 41 EB                                         1..%.B...eR...t...A.
```

Screenshot showing the values changed in certificate of the software image thus tampering the image.

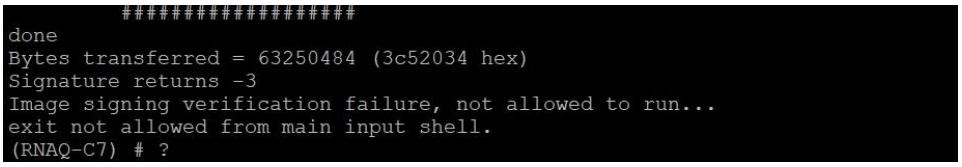
3) After editing save the edited image and copy the tampered boot image over TFTP.



Screenshot showing the image being transferred after modification/tampering.



Screenshot showing the status of the tampered image copying from test terminal to DUT via TFTPD.



4) Verify that the DUT check the integrity of the software image downloaded from TFTP server before installation. Device failed to load the tampered image giving error message as Image signing verification failed.

Screenshot showing integrity check is completed and failed after file is copied, The DUT validate the integrity of the copied image after file is transferred via TFTP and integrity check failed cause of image certificate was tampered and integrity was changed.

11.2.4 **Test Observations:** It is observed that the DUT does not allow to install the tampered image before validation check is successful, DUT validates the tampered software image before installation and when integrity check failed DUT gives an error message 'Image signing verification failed'.

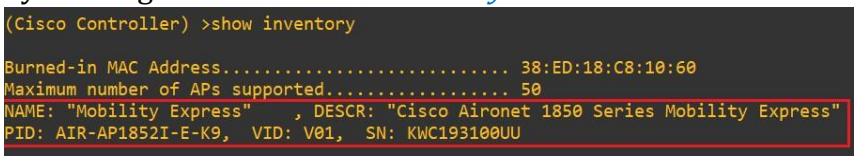
12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_SOFTWARE_INTEGRITY_VERIFICATION	PASS	
2	TC_NO_TAMPERED_SOFTWARE_INTEGRITY_VERIFICATION	PASS	

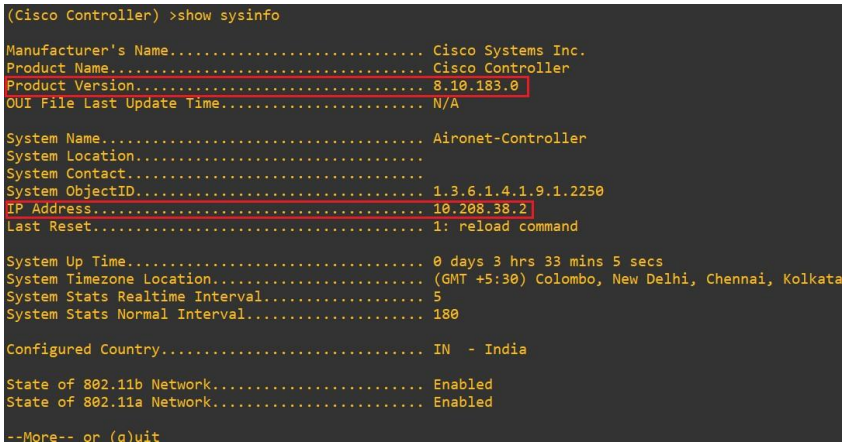
1.12.4 Software Integrity Check - Boot

<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 12 Other Security Requirement
2. **<Security Requirement No & Name >** 1.12.4 Software Integrity Check - Boot
3. **<Requirement Description: >** The CPE shall verify the integrity of a software component at the time of boot / re-boot typically by comparing the result of a measurement (typically a cryptographic hash / CRC) of the component to the expected reference value.
4. **DUT Confirmation Details**:
   - This section involves information about DUT like software/firmware version, Hardware version model.
   - DUT Cisco WLC contains default boot image with version 8.10.183.0. The model is AIRAP1852I-E-K9. The inventory shows model serial no. & model description.
   - Verification of DUT Cisco wireless LAN controller's HW product series information by running command *show inventory* on CLI.

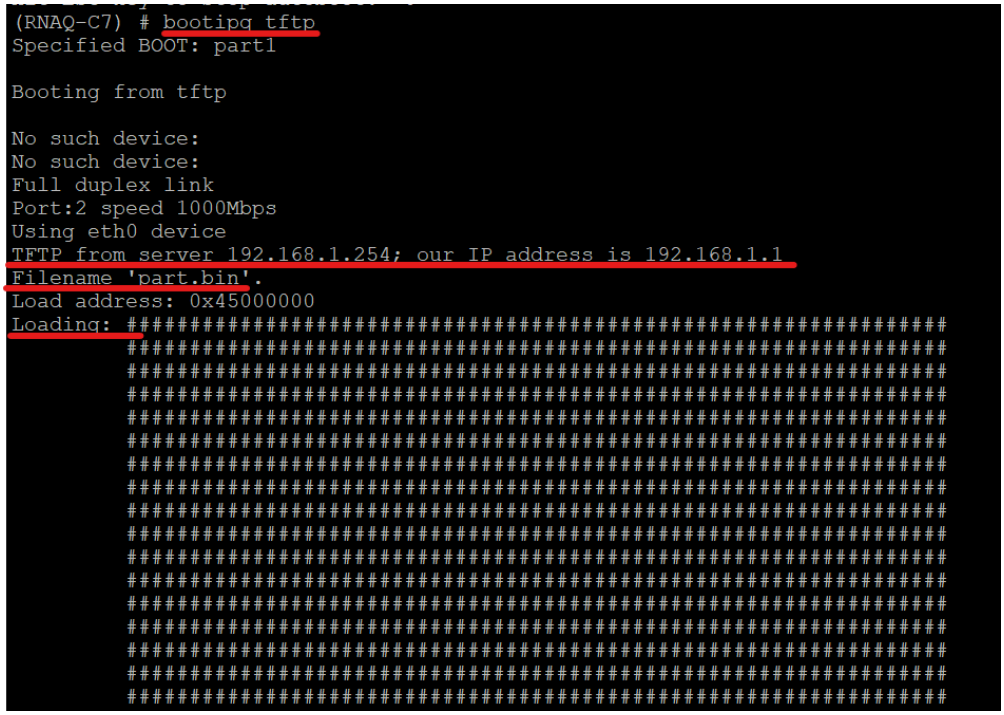


   - Verification of DUT Cisco WLC's high-level system SW information by running command *show sysinfo* on CLI.



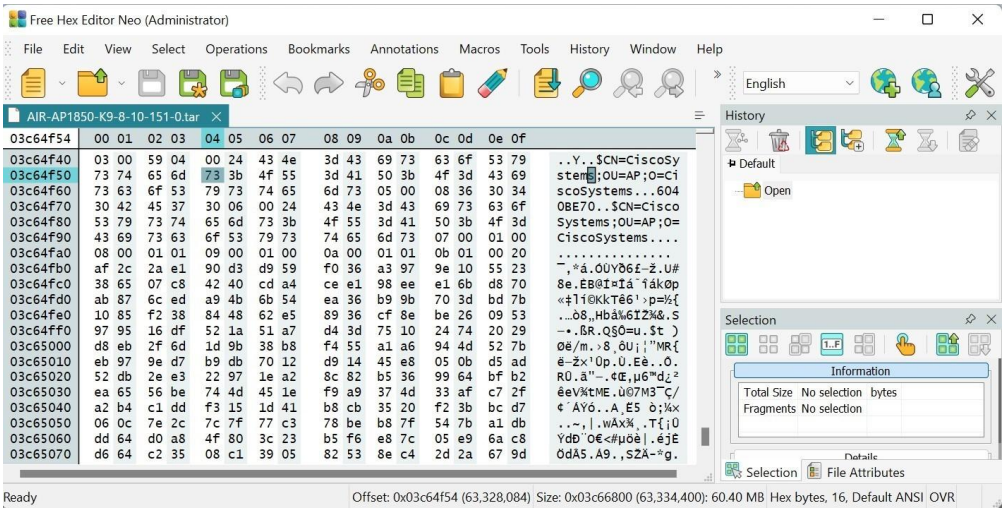
   - Verification of DUT Cisco WLC's system information on Web access.

5. **DUT Configuration**:
   After editing save the edited image and boot the DUT from tampered image stored on TFTP server.



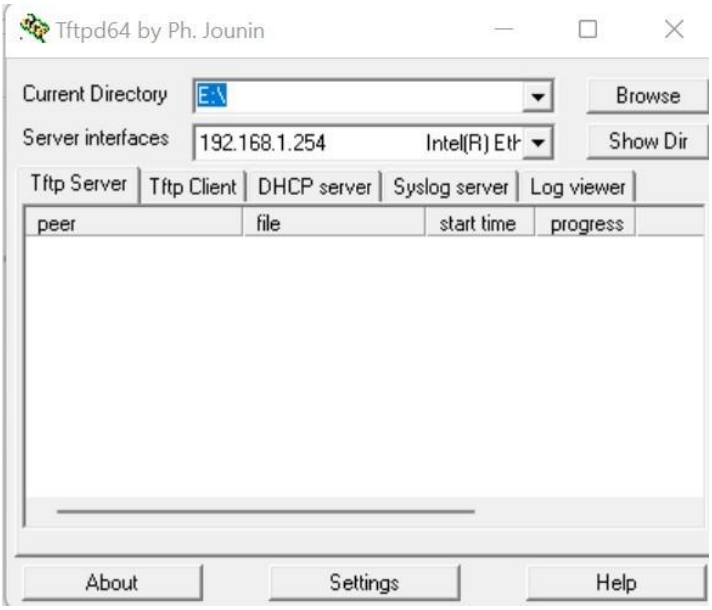
Screenshot showing the tftp server used to download the modified software image on DUT for loading.

Run Hexeditor of terminal machine and change values in the boot image.



Screenshot show hexeditor used to change the bit from the software image and the bit. before modification.

Verify the boot image file in DUT (image software) and copy the boot image from DUT to terminal for tampering via TFTP.



Screenshot showing the TFTP server downloading the software image file from DUT to remote terminal for modification with hexeditor.

6. **Preconditions:**

- Vendors should provide the documentation to provide information on integrity algorithms used while booting.
- Vendor should provide.
    - Valid image for boot.
    - Invalid/corrupt image for boot.

7. **Test Objective:** To validate that DUT verifying the integrity of a software image at the time of boot

8. **Test Plan:** Rebooting the DUT and verifying the integrity of a software image at boot time of DUT

8.1 **Number of Test Scenarios:**

8.1.1 Rebooting the DUT

8.2 **Test Setup Diagram**

Testing Terminal
Test Terminal OS: Linux Ubuntu 22.04.3
IP Address: 10.208.38.11
Putty V 0.76
OpenSSH_8.9p1

DUT
Cisco AP Aironet 1850
IP Address: 10.208.38.2

8.3 **Tools Used:**

- DUT terminal(Console), Hex editor, TFTP server

8.4 **Test Execution Steps:**

Below are the execution steps,

Case 1: Booting the DUT

- Power on the CPE and login using proper credentials.
- Verify different commands available to DUT and then restart the CPE.
- Observe the boot process for self-test.
- Verify that software integrity is checked as part of the booting process.

9. **Expected Result for Pass:** At the boot time, The DUT should verify the integrity of a software image

10. **Expected Format of Evidence:** Screenshot of DUT terminal (Console), Hex editor, and TFTP server

11. **Test Execution:**

11.1 **Test Case Number:** 01

11.1.1 **Test Case Name:** TC_NO_SW_INTEGRITY_VERIFICATION_BOOT

11.1.2 **Test Case Description:** Verifying the DUT have mechanism for verifying the integrity of software image at boot time

11.1.3 **Execution Steps:**

Below are the execution steps with evidence:

- Power on the CPE and login using proper credentials.

```
(Cisco Controller)
User: Admin
Password:*********
Welcome to the Cisco Mobility Express command line interface.
Only commands which are listed in the command reference guide for this release are su
http://www.cisco.com/c/en/us/support/wireless/mobility-express/products-command-refer

Warning:In SNMPV2 No Defaults Presents.
Please use command: config snmp community create <name>
```

Screenshot showing login with default admin user.

- Verify different commands available to DUT for Admin user and then restart the CPE.

```
(Cisco Controller) >?

apciscoshell    Go to AP Console
clear           Clear selected configuration elements.
config          Configure switch options and settings.
cping           Send capwap echo packets to a specified mobility peer IP address.
debug           Manages system debug options.
eping           Send Ethernet-over-IP echo packets to a specified mobility peer IP address.
grep            Print lines matching a pattern.
help            Help
linktest        Perform a link test to a specified MAC address.
logout          Exit this session. Any unsaved changes are lost.
ping            Send ICMP echo packets to a specified IP address.
reset           Reboot (hard reload) options.
restart         Restart (soft reload) the switch.
save            Save switch configurations.
show            Display switch options and settings.
test            Test trigger commands
transfer        Transfer a file to or from the switch.

(Cisco Controller) >res?
reset           restart
(Cisco Controller) >restart ?

(Cisco Controller) >restart

The system has unsaved changes.
Would you like to save them now? (y/N) y


Configuration Saved!         Stopping DHCPv6 client...
```

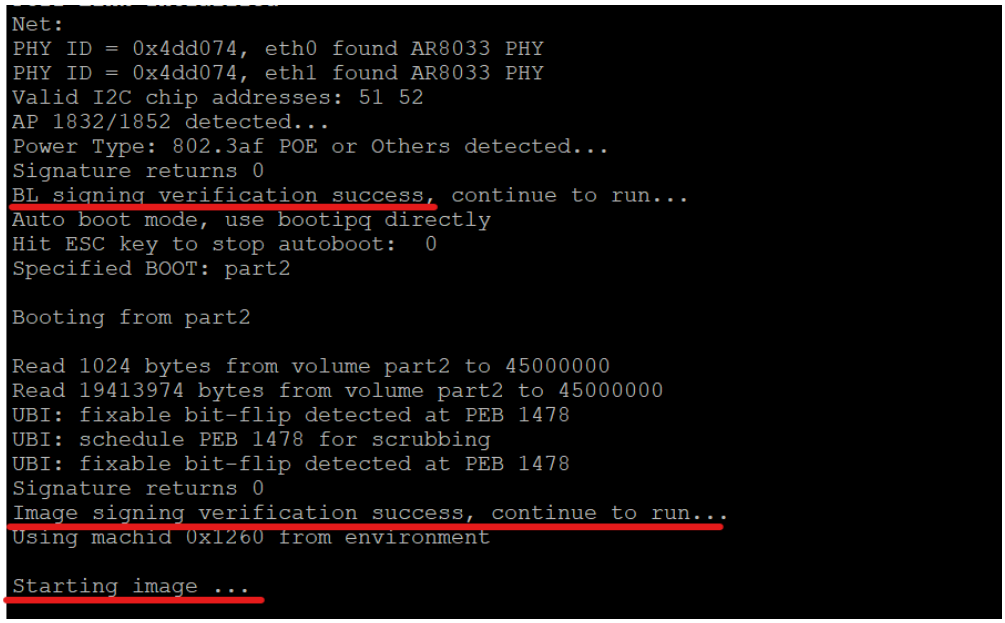
Screenshot showing the commands allocated to admin user and “restart” command from the list, which executed on next line.

```
Configuration Saved!         Stopping DHCPv6 client...
[  OK  ] Stopped target Timers.
         Stopping Cisco rtd service...

SIGHUP handler received signal 1
 si_signo: 1, si_errno: 0, si_code: 128, si_addr: 0x0
         Stopping Cisco brain service...
         Stopping Cisco led service...
         Stopping System Monitor service...
[  OK  ] Stopped Cisco klogd.
[  OK  ] Stopped Cisco printkd.
[  OK  ] Stopped System Monitor service.
[  OK  ] Stopped NSS Firmware Monitor daemon.
[  OK  ] Stopped NTP_PROC daemon.
[  OK  ] Stopped Cisco led service.
[  OK  ] Stopped AP Trace daemon.
[  OK  ] Stopped Hostapd process.
[  OK  ] Stopped OpenSSH server daemon.
[  OK  ] Stopped Cisco rtd service.
[  OK  ] Stopped Fast CGI daemon.
[  OK  ] Stopped Cisco brain service.
[  OK  ] Stopped capwapd.
[  OK  ] Stopped Clean Air daemon.
[  OK  ] Stopped DNSmasq.
[  OK  ] Stopped Serial Getty on ttyS0.
[  OK  ] Stopped DHCPv6 client.
[  OK  ] Stopped gRPC server daemon.
[  OK  ] Removed slice system-serial\x2dgetty.slice.
[  OK  ] Stopped WCPD process.
[  OK  ] Stopped target Basic System.
[  OK  ] Stopped target Paths.
[  OK  ] Stopped target Sockets.
```

- Observe the boot process for self-tests.

Screenshot showing different processes are stopped with acknowledge message as OK, It shows the processes are stopped without any error.

- Verify that software integrity is checked as part of the booting process.



Screenshot showing the message verification of image signature is successful and image is started to load.

11.1.4 **Test Observations:** It is observed that when DUT is allowed to boot with correct/non-tampered image the DUT verifies the signing of the boot image, and upon successful verification DUT allows the image to load.

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_SW_INTEGRITY_VERIFICATION_BOOT	PASS	

1.12.5 Unused Physical Interfaces Disabling

<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 12 Other Security Requirement
2. **<Security Requirement No & Name >** 1.12.5 Unused Physical Interfaces Disabling
3. **<Requirement Description: >** The CPE shall support the mechanism to verify all the physically accessible interfaces. Physically accessible Interfaces (including LAN ports) which are not under use shall be disabled by configuration so that they remain inactive even in the event of a reboot.
4. **DUT Confirmation Details**:
   - This section involves information about DUT like software/firmware version, Hardware version model.
   - DUT Cisco WLC contains default boot image with version 8.10.183.0. The model is AIRAP1852I-E-K9. The inventory shows model serial no. & model description.
   - Verification of DUT Cisco wireless LAN controller's HW product series information by running command *show inventory* on CLI.

```
(Cisco Controller) >show inventory

Burned-in MAC Address.............................. 38:ED:18:C8:10:60
Maximum number of APs supported.................... 50
NAME: "Mobility Express"    , DESCR: "Cisco Aironet 1850 Series Mobility Express"
PID: AIR-AP1852I-E-K9,  VID: V01,  SN: KWC193100UU
```

   - Verification of DUT Cisco WLC's high-level system SW information by running command *show sysinfo* on CLI.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name................................ Cisco Systems Inc.
Product Name....................................... Cisco Controller
Product Version.................................... 8.10.183.0
OUI File Last Update Time.......................... N/A

System Name........................................ Aironet-Controller
System Location.....................................
System Contact......................................
System ObjectID.................................... 1.3.6.1.4.1.9.1.2250
IP Address......................................... 10.208.38.2
Last Reset......................................... 1: reload command

System Up Time..................................... 0 days 3 hrs 33 mins 5 secs
System Timezone Location........................... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
System Stats Realtime Interval..................... 5
System Stats Normal Interval....................... 180

Configured Country................................. IN  - India

State of 802.11b Network........................... Enabled
State of 802.11a Network........................... Enabled

--More-- or (q)uit
```

   - Verification of DUT Cisco WLC's system information on Web access.

5. **DUT Configuration**: Command to shut the AUX port execute command.
   'config ap lag-mode support disable'

```
(Cisco Controller) >config ap lag-mode support disable

Warning! All APs with LAG enabled will be rebooted.
And non lag APs will have DTLS connection teared down causing
 them to disjoin and rejoin again.
 Are you sure you want to continue? (y/n) y
```

Screenshot showing the command to disable the link aggregation mode which is used by AUX port it is same as disabling the physical AUX port.

Verify the status of the AUX port with the command 'show ap lag-mode'.

```
(Cisco Controller) >show ap lag-mode

LAG-Mode Support ............................... Disabled
```

Screenshot showing the AUX port is disabled.

reboot the device with 'restart' command.

```
(Cisco Controller) >restart

The system has unsaved changes.
Would you like to save them now? (y/N) y


Configuration Saved!
```

Screenshot showing the restart command executed and DUT has initiated restart.

6. **Preconditions:**
   - Review the documentation provided by vendor to verify the mechanism for identifying all the physical interfaces present on DUT.
   - After identifying the physical interfaces available on DUT, review the document and verify the configuration to disable them permanently.
7. **Test Objective:** To verify that DUT have capability to disable the unused physical interface and it's status still disable after rebooting of DUT also

8. **Test Plan:**
    - Verify the list of physical interfaces available in the DUT
    - Disable the unused physical interfaces in the DUT
    - Reboot the DUT and verify the disabled interfaces still in disable state

8.1 **Number of Test Scenarios:**

8.1.1 Disable the unused interface in the DUT and verify status of disable interface after rebooting of DUT

8.2 **Test Setup Diagram**

Testing Terminal
Test Terminal OS: Linux Ubuntu 22.04.3
IP Address: 10.208.38.11
Putty V 0.76
OpenSSH_8.9p1

DUT
Cisco AP Aironet 1850
IP Address: 10.208.38.2

8.3 **Tools Used:**

- DUT terminal(Console)

8.4 **Test Execution Steps:**

Below are the execution steps,

- Login with 'admin' user and run command 'show interface summary' to check the management physical interface and its status.
- Run command. 'Show ap lag-mode' to check the status of AUX port.
- Once interface list is displayed, evaluator found out that AUX port is an unused port, and it cannot be used as it poses threat of spanning tree loop. So, to shut the AUX port execute command.
- Verify the status of the AUX port with command 'show ap lag-mode'.
- Now reboot the device with 'reload' command.
- Once reload is complete login to DUT with admin user (mumuser with privilege 15)
- Verify the status of the disabled interface (It should remain disabled after reboot).

9. **Expected Result for Pass:** Disabled interface should be disable state even after rebooting of DUT
10. **Expected Format of Evidence:** Screenshot of DUT terminal(Console)
11. **Test Execution:**

11.1 **Test Case Number:** 01

11.1.1 **Test Case Name:** TC_NO_DISABLE_PHY_INTERFACES

11.1.2 **Test Case Description:** Verifying the DUT physical interfaces, disable the unused interfaces and reboot the DUT for any changing happen in DUT interface status.

11.1.3 **Execution Steps:**

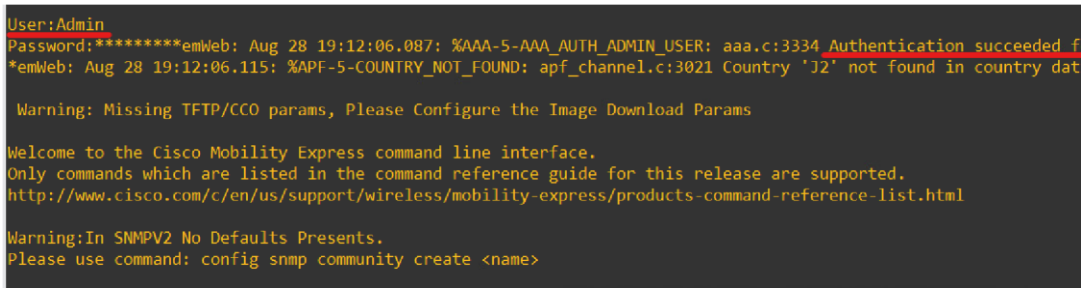
Below are the execution steps with evidence:

- To be completed after vendor provides documentation –

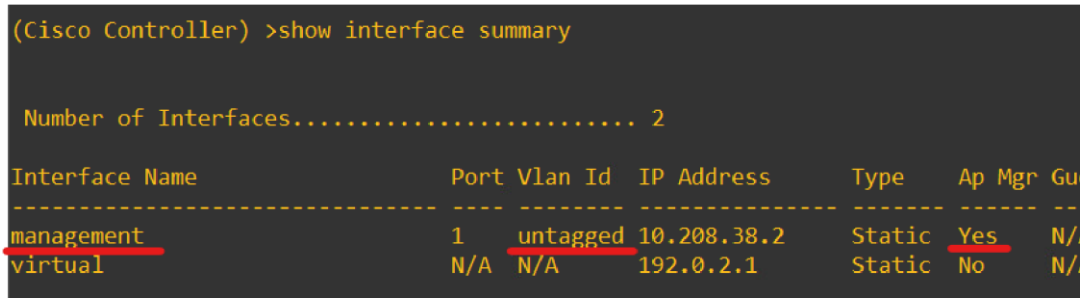
i. The evaluator has identified that there are 2 physical interfaces available on DUT.

- POE/ management port: The POE port or the management port is used to provide power to DUT, this port cannot be disabled, as this port is only power supply available for DUT.
- AUX port: it is designed to perform port Link Aggregation (LAG). The AUX port will be disabled by default.
- The AUX port is not manageable and is simply bridged back to the controller. Avoid connecting another AP to this port or devices such as switches/hubs or the same switch or uplink as the PoE port because it can create spanning tree loop issues. Case 2: DUT shall support the mechanism to identify all the physical interface and to disable them.

ii. Login with 'admin' user and run command 'show interface summary' to check the management physical interface and its status.



Screenshot showing the user admin logged in successfully.



Screenshot showing 1st physical interface management interface with is the POE interface as well.

iii. Run command. 'show ap lag-mode' to check the status of AUX port.

Screenshot showing the link aggregation mode is by default disabled this is used by AUX port which is 2nd physical port and this port is only used for lag-mode.

iv. Once interface list is displayed, evaluator found out that AUX port is an unused port, and it cannot be used as it poses threat of spanning tree loop. So, to shut the AUX port execute command.

```
(Cisco Controller) >config ap lag-mode support disable

Warning! All APs with LAG enabled will be rebooted.
And non lag APs will have DTLS connection teared down causing
 them to disjoin and rejoin again.
 Are you sure you want to continue? (y/n) y
```

Screenshot showing the command to disable the link aggregation mode which is used by AUX port it is same as disabling the physical AUX port.

v. Verify the status of the AUX port with command 'show ap lag-mode'.

```
(Cisco Controller) >show ap lag-mode

LAG-Mode Support ..............................  Disabled
```

Screenshot showing the AUX port is disabled.

vi. Now reboot the device with 'restart' command.

```
(Cisco Controller) >restart

The system has unsaved changes.
Would you like to save them now? (y/N) y


Configuration Saved!
```

Screenshot showing the restart command executed and DUT has initiated restart.

vii. Once reload is complete login to DUT with 'admin' user.

```
User:  Admin
Password:********
 Warning: Missing TFTP/CCO params, Please Configure the Image Download Params

Welcome to the Cisco Mobility Express command line interface.
Only commands which are listed in the command reference guide for this release a
http://www.cisco.com/c/en/us/support/wireless/mobility-express/products-command-
```

Screenshot showing the login successful with user admin

viii. Verify the status of disabled interface. (It should remain disabled after reboot)

```
(Cisco Controller) >show ap lag-mode

LAG-Mode Support ..............................  Disabled

(Cisco Controller) >
```

Screenshot showing the AUX port remained disabled after reboot.

11.1.4 **Test Observations:** It is observed that the unused AUX port is by disabled by default, also it can be disabled manually with command. The unused physical aux port is not manageable directly, but it can be managed indirectly with lag mode commands, The AUX port remain disabled after reboot as well.

12. Test Case Result:

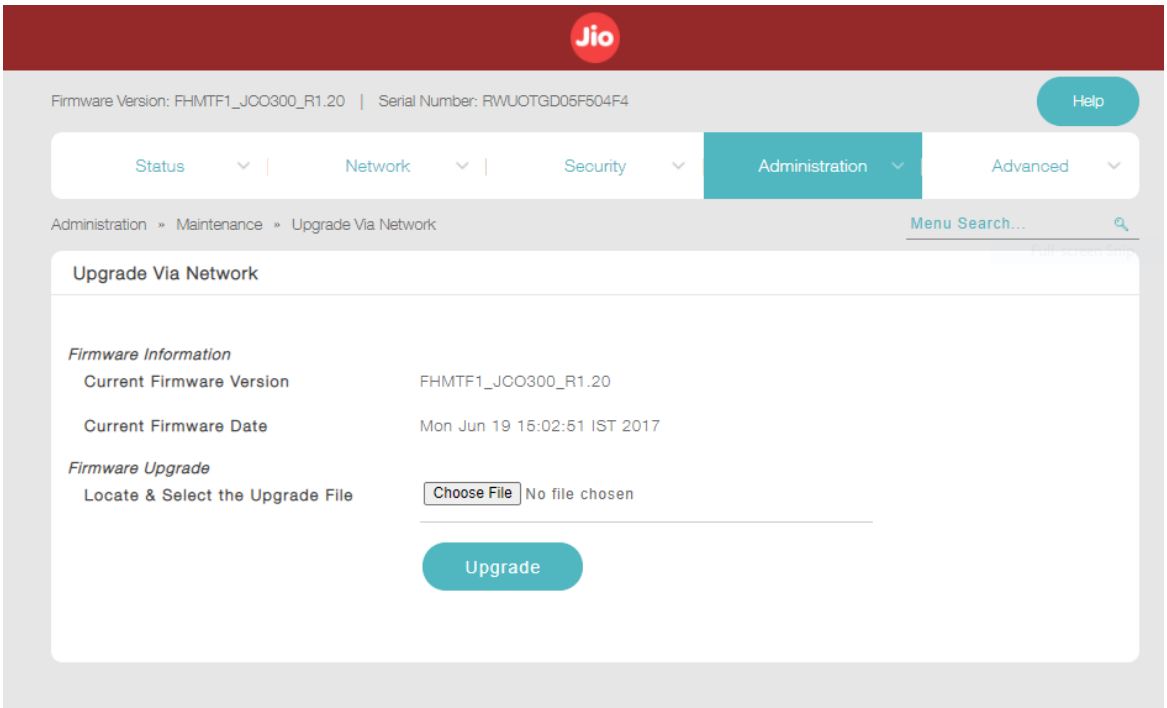
S. No	**TEST CASE NAME**	**PASS/FAIL**	**Remarks**
1	TC_NO_DISABLE_PHY_INTERFACES	PASS	

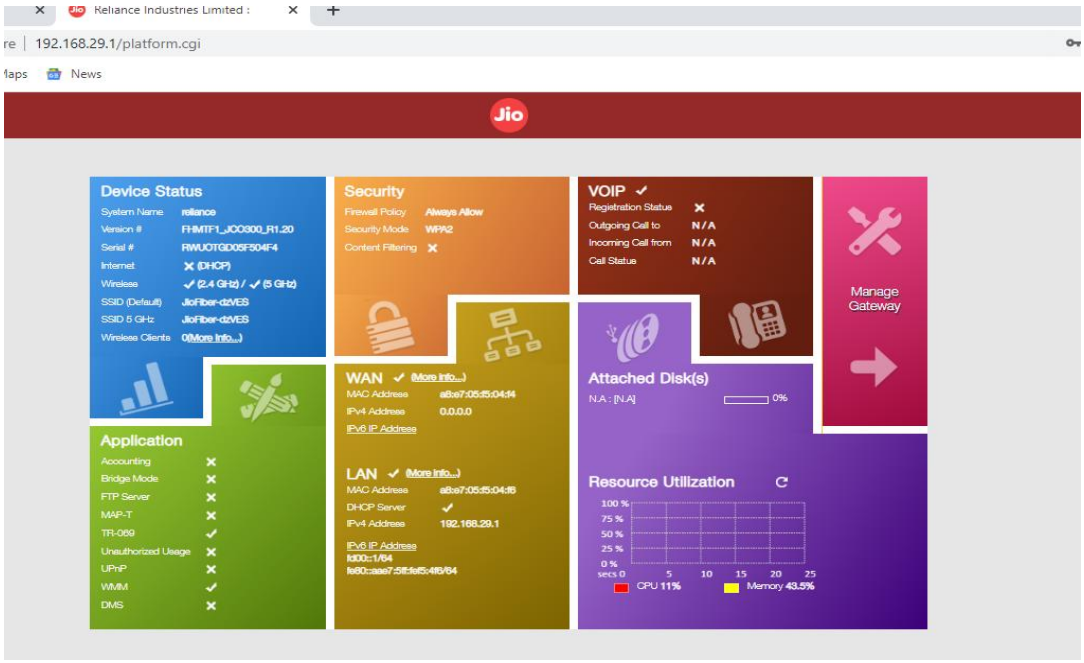
1.12.6: No Default Profile

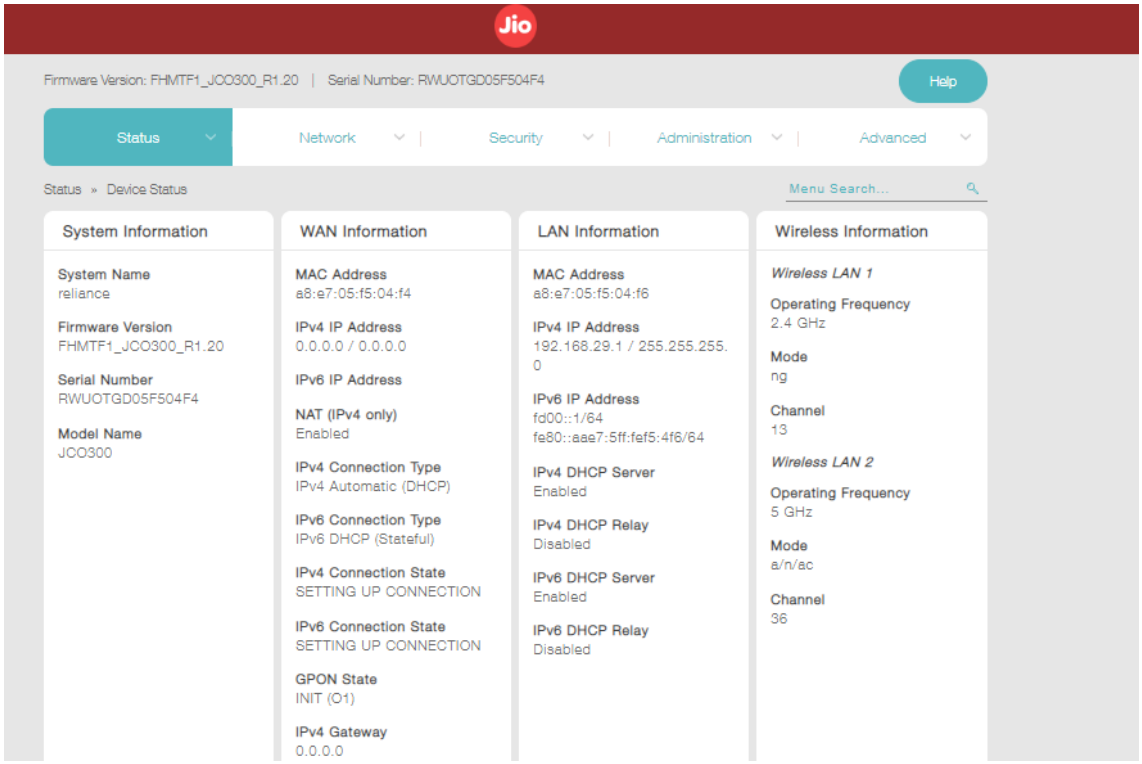
<DUT Details: > WiFi CPE
<DUT Software Version:> Jio FHMTF1_JCO300_R1.20
<Digest Hash of OS> Hash of DUT OS is required
<Digest Hash of Configuration> Hash of DUT configuration is required
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs
<ITSAR Version No:> 1.0.1
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 1.12 Other Security Requirement
2. **<Security Requirement No & Name >** 1.12.6 No Default Profile
3. **<Requirement Description: >** Predefined or default user accounts shall be deleted or disabled. Default accounts such as guest, master are generally preconfigured with known or nil authentication attribute and therefore such standard users shall be deleted or disabled.
4. **DUT Confirmation Details**:
    - Use the command line/GUI interface to get details of the machine on which test is conducted.
    - Use GUI to get Application No/Version No & hardware Info

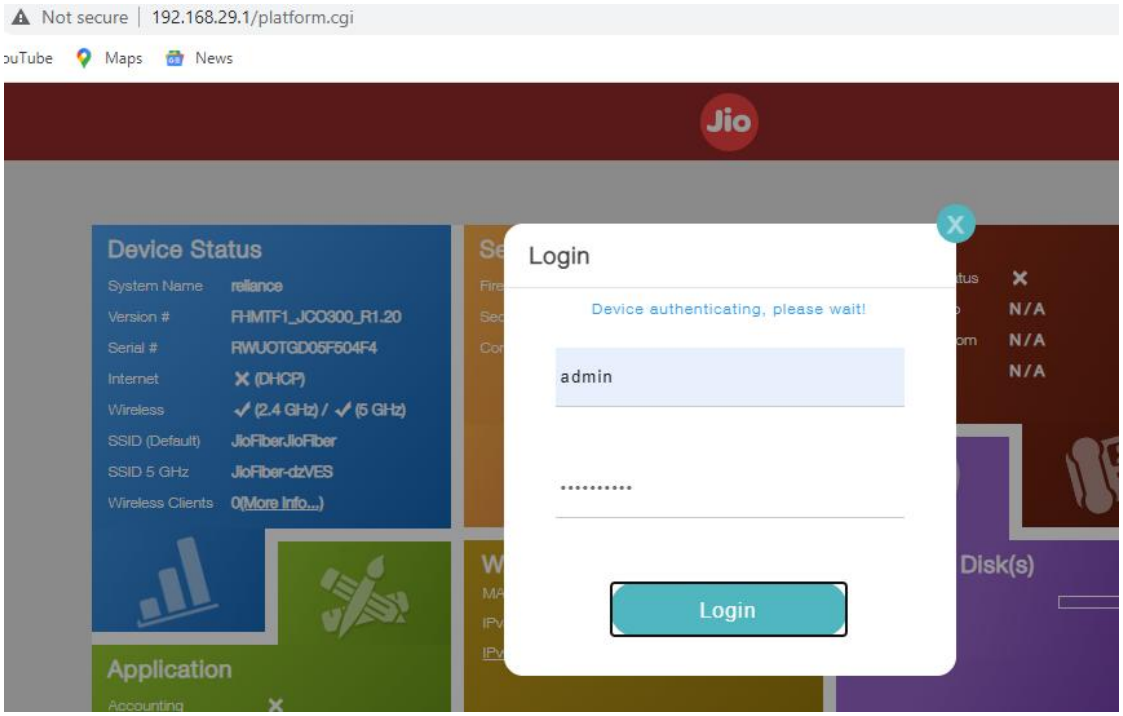
The below screenshot shows the firmware version of the DUT







5. **DUT Configuration**:
   - The Tester opens GUI(https) of DUT(192.168.29.1) in tester machine (192.168.29.118).



- The Tester attempts to login DUT using “admin” account.

6. **Preconditions:** OEM need to provide documentation regarding how to delete/disable/modify the default user accounts in the DUT

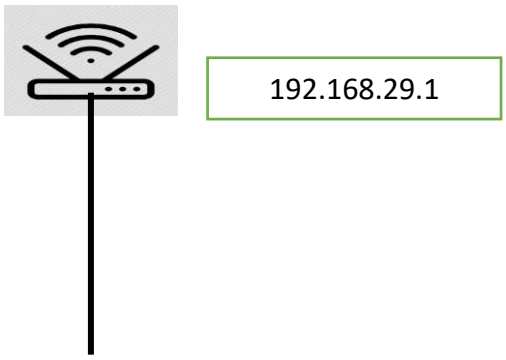
7. **Test Objective:** To verify that it is possible to delete/disable/modify the default user accounts in the DUT

8. **Test Plan:**
   - The tester shall identify what all user accounts available in the DUT
   - Delete the default user account in the DUT

   8.1 **Number of Test Scenarios:**

   8.1.1 Delete the Default user accounts in the DUT

   8.2 **Test Setup Diagram**



192.168.29.118

8.3 **Tools Used:**

- Web browser(client)

8.4 **Test Execution Steps:**

- The tester must verify for the compliance to the pre-requisites:
- Perform factory reset on the DUT
- Create new user with admin privileges
- Delete/disable the predefined or default accounts on the DUT

9. **Expected Result for Pass:** Predefined or Default user accounts possible to delete/disable in the DUT.

10. **Expected Format of Evidence:** Screenshot of DUT webpage

11. **Test Execution:**

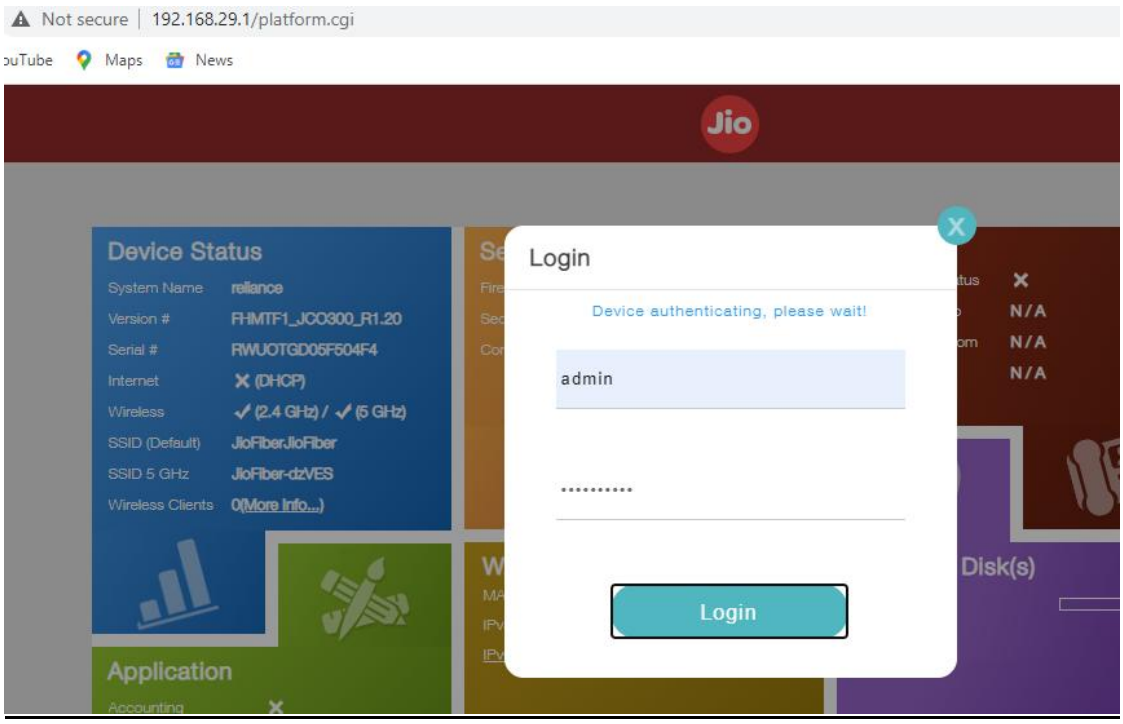
11.1 **Test Case Number:** 01

11.1.1 **Test Case Name:** TC_NO_DEFAULT_ACCOUNT_DELETE

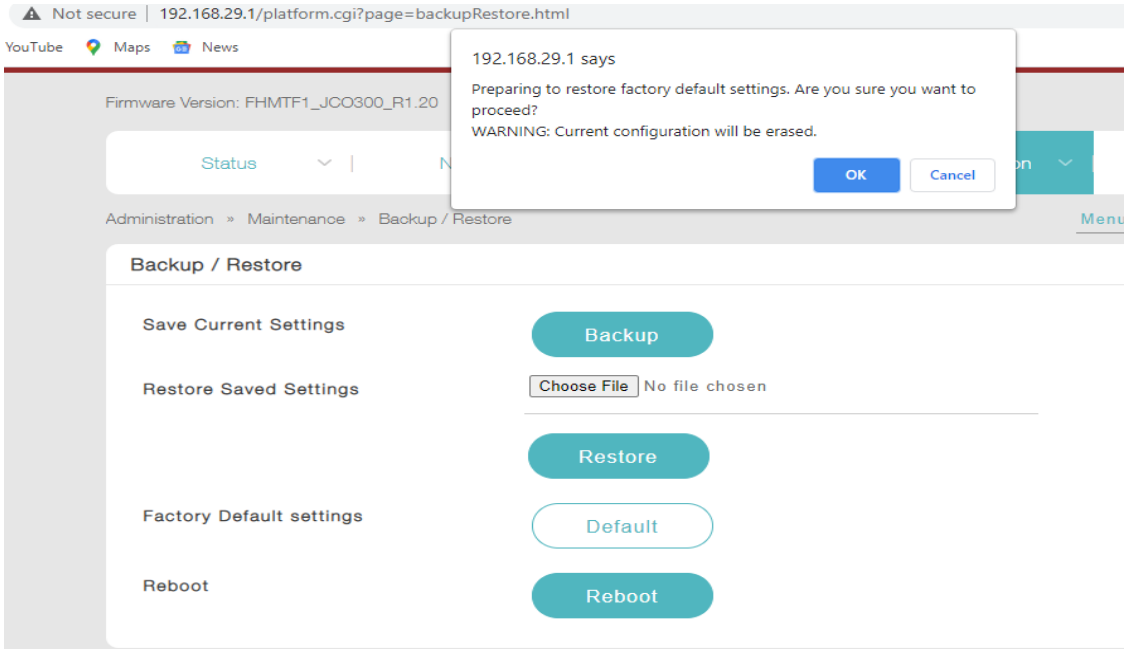
11.1.2 **Test Case Description:** Ensuring that predefined or default user accounts are possible to delete/disable in the DUT

11.1.3 **Execution Steps:**

1. Login to the DUT with admin credentials



2. Perform factory reset on the DUT

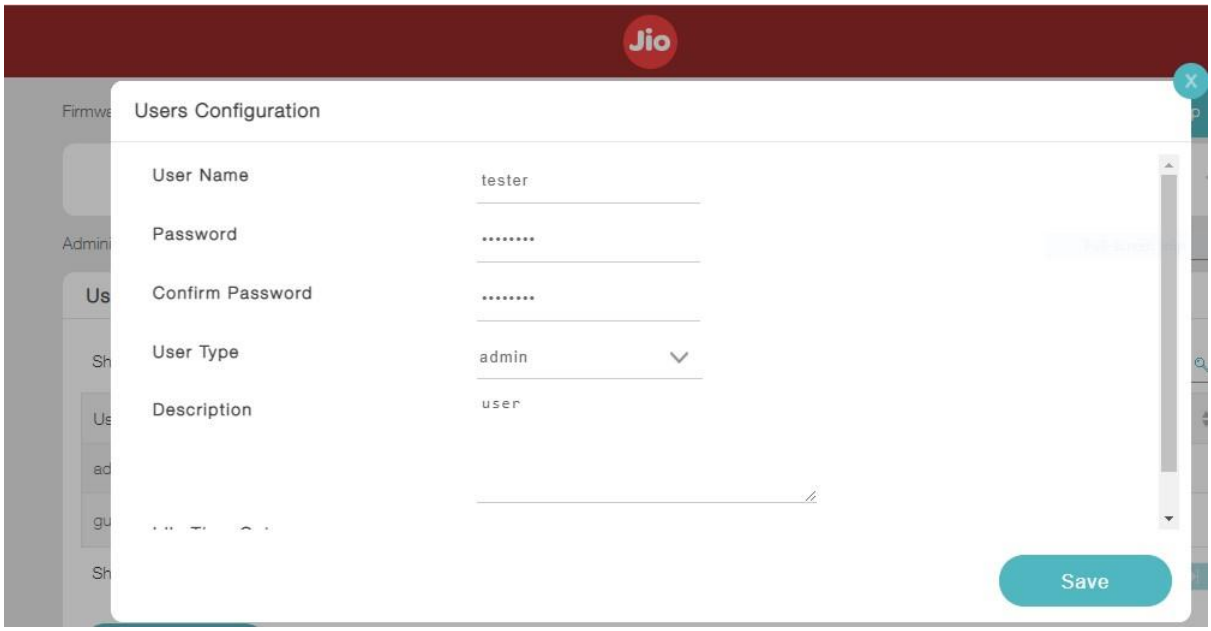


3. Login the DUT with default credentials(Username - admin & Password – Jiocentrum)

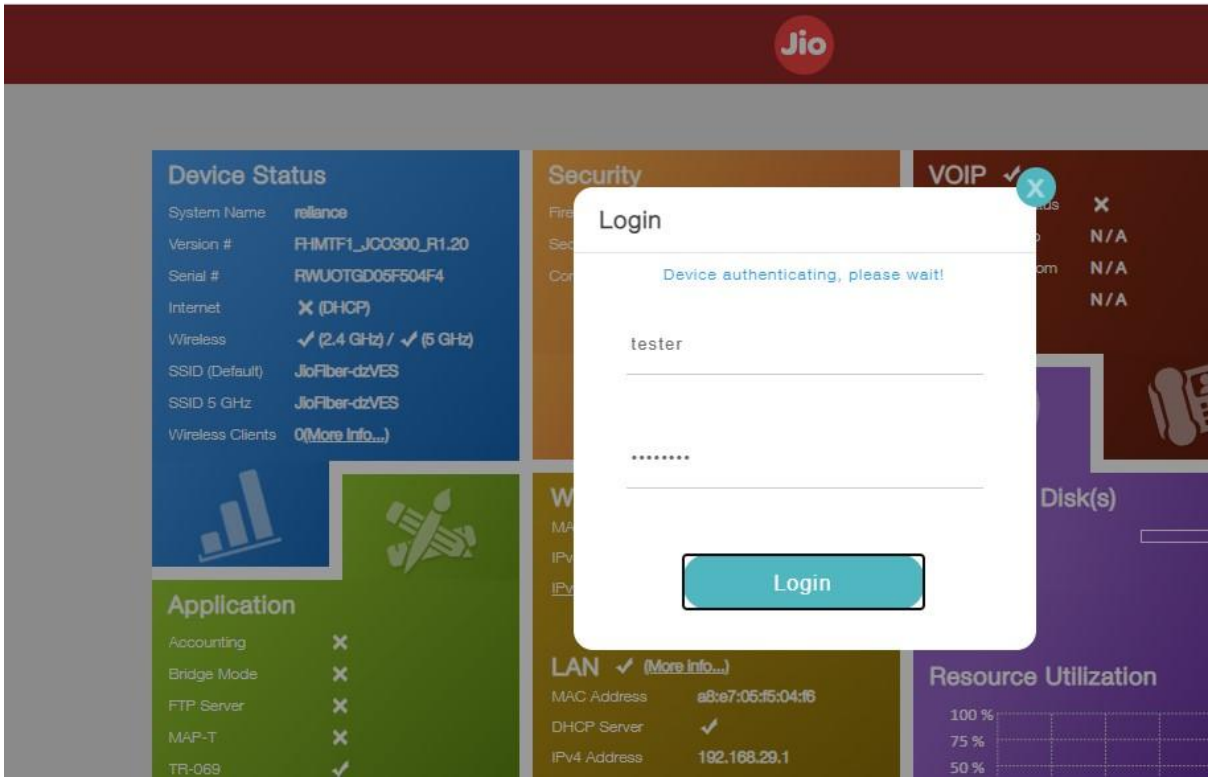
4. After 1st login, The DUT asking to change credentials for admin and guest user accounts.

5. After relogin the DUT with updated credentials(Username – admin, Password – Test@123)

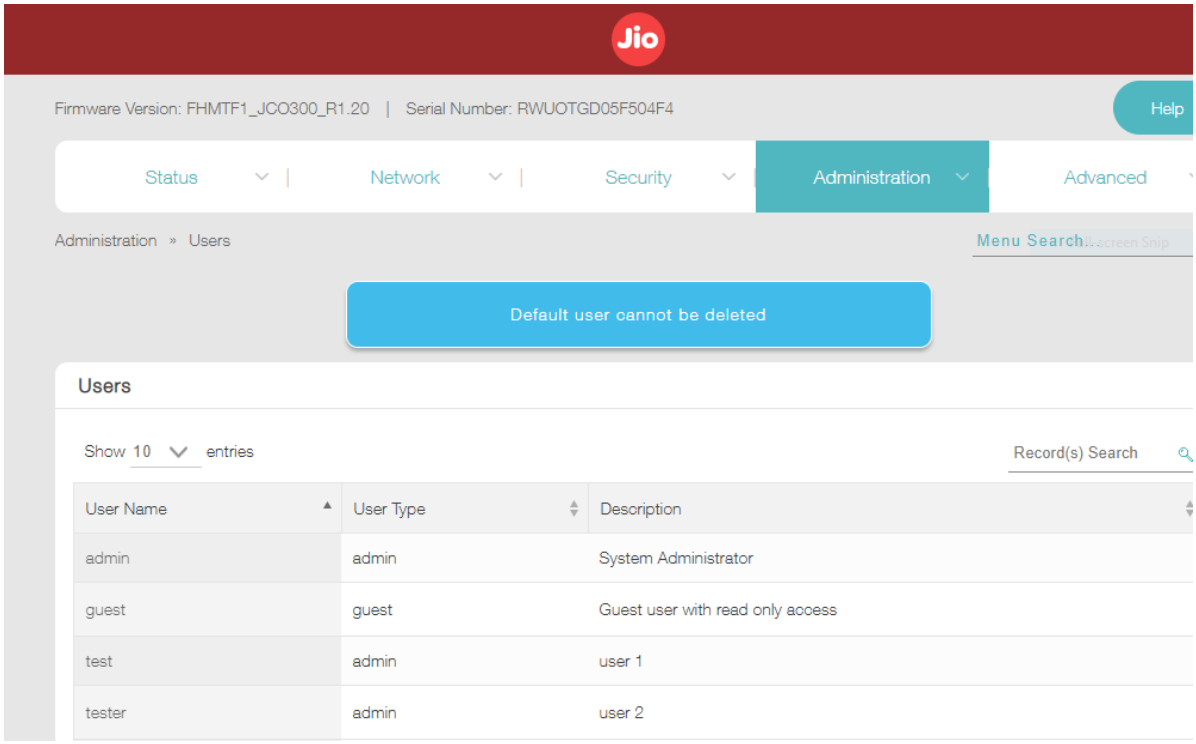
6. Create the new user in the name of “tester” with admin role privileges.



7. Logout the admin account and login with the tester account credentials(Username – tester, Password – Test@1234)



8. Try to delete/disable the default account such as “admin”



11.1.4 **Test Observations:** The predefined or default accounts in the DUT not possible to delete

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_DEFAULT_ACCOUNT_DELETE	FAIL	