INVISIBLE THREATS & Wi-Fi MISSTEPS

Today's Hottest Security Gaps

Jennifer (JJ) Minella
Security Architect, Viszen Security

Viszen Security

Jennifer (JJ) Minella

AUTHOR | SPEAKER | ADVISOR

PACKET PUSHERS

PACKET PROTECTOR

The Podcast at the Intersection of Networking & Security!

New Episodes Every Tuesday

Meet Jennifer (JJ) Minella

- Co-host of **Packet Protector Podcast** on Packet Pushers network
- 20+ years in **technology**, 15+ years in **security**
- SC Magazine **Top 10 Power Players**
- Member **Forbes** Technology Council
- **CSA Zero Trust Working Group** leadership
- Specialties in **network** and **wireless architecture** and **security**
- **IoT** security, **OT-IT** security including ISA/IEC 62443
- Faculty with I**ANS Research**
- Former **ISC2** International board of directors and chairperson
- Author of ***Wireless Security Architecture*** and ***Low Tech Hacking***
- Award winning **blog** at https://securityuncorked.com
- Founder and principal advisor **Viszen Security** and **CISO Launch**
- Volunteer with RSAC, EWF, BSides, CyberPatriot and others
- **@jjx** on Social Media (Twitter, Bluesky, Mastodon)

2023 OFFICIAL MEMBER Forbes Technology Council

Viszen Security

IANS

Follow Me for More

Follow me on LinkedIn for articles, live events, free resources, and training

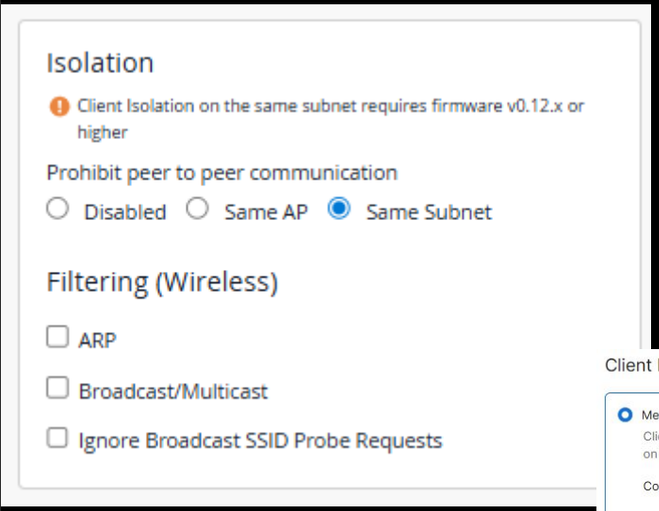
01.

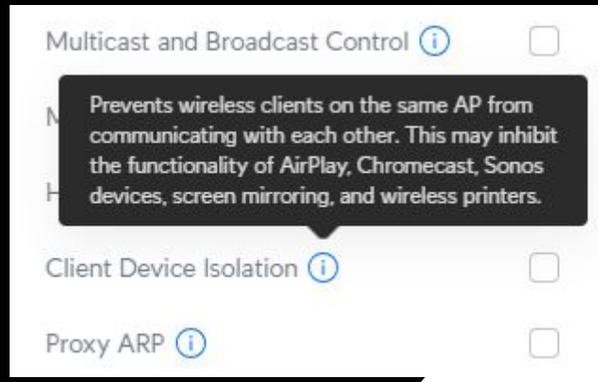
INVISIBLE SSID MISCONFIGURATIONS

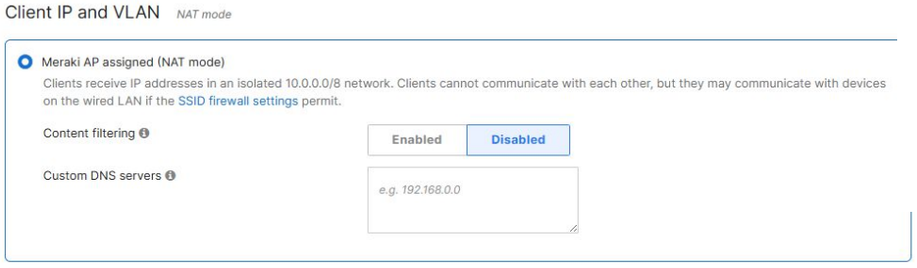
MISSING PEER ISOLATION

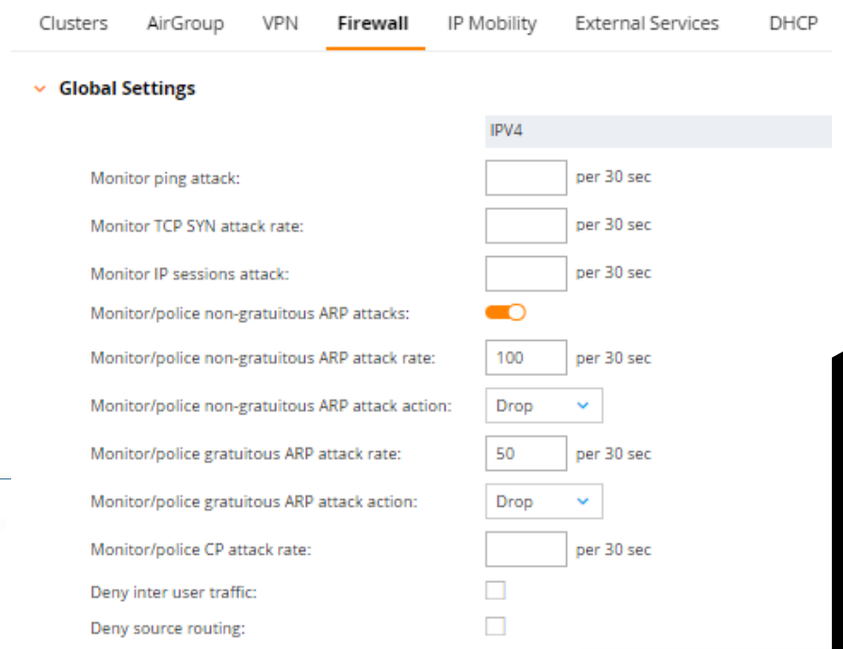
That little check box that keeps Wi-Fi endpoints from being able to talk directly to other Wi-Fi endpoints.

It's a CHECKBOX
Why so hard? ¯_(ツ)_/¯





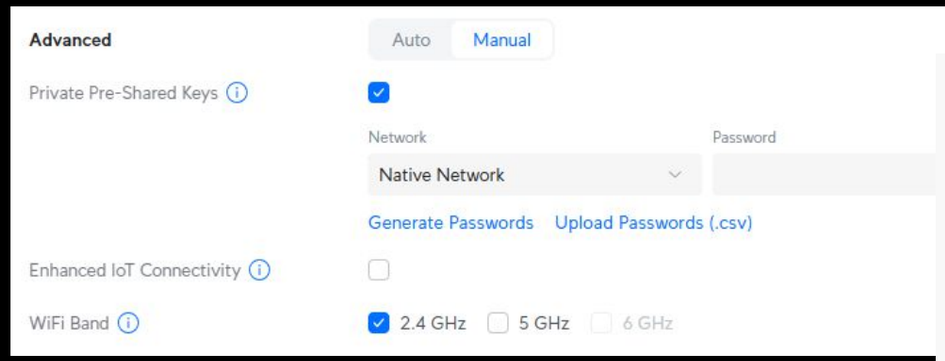


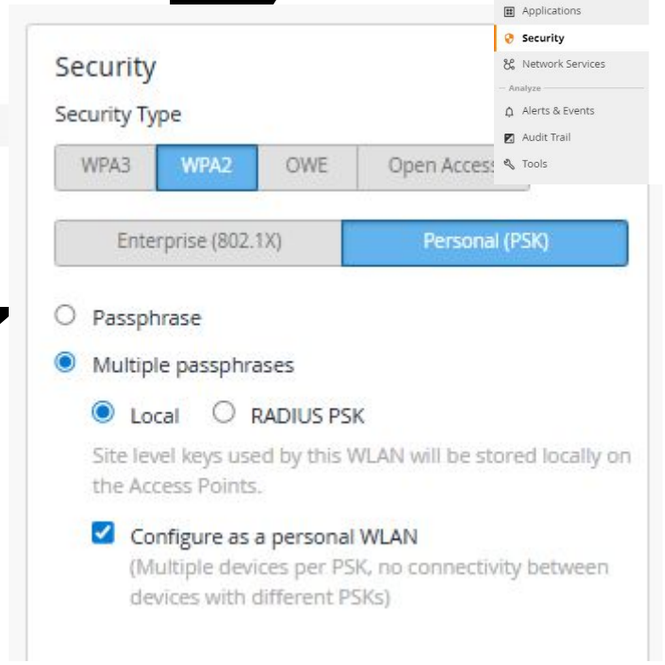


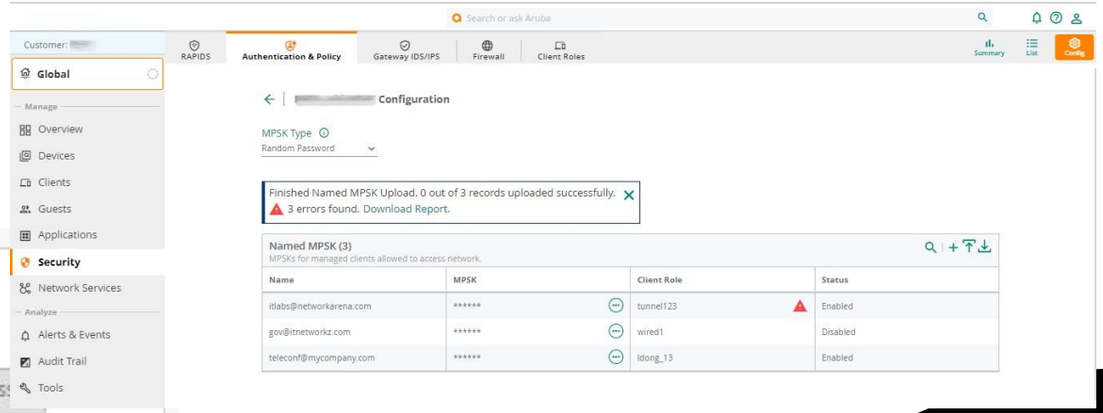
Viszen Security

MPSK W/O SEGMENTATION

MPSK-PPSK-UPSK-IPSK - does not natively/default to segmenting same-key traffic on all platforms.







Viszen Security

M.I.A. WIRED SEGMENTATION

82% of networks have multiple SSIDs tied to the same wired VLAN with incorrect filtering/ACL.

Viszen Security

Attacks

Missing segmentation can lead to several attacks

Malware Spread

Unfettered lateral movement supports propagation of ransomware and other malware through an infrastructure.

Enumeration & Discovery

Helps the adversary identify targets, credentials, roles, trust relationships, and pathways for lateral movement.

Endpoint Exposure

Aside from ransomware, overly permissive networks including those allowing direct communication and zero conf protocols expose endpoints to numerous vulnerabilities.

02.

INVISIBLE RADIUS FAILS

SHARED SECRET, SHARED SHAME

RADIUS: Now with 100% of Your Root Password

Unless RadSec is implemented, RADIUS shared secrets are sent in the cleartext everywhere. A large number of admins have configured shared secrets to match high level root admin passwords.

BAD EAPS!

Legacy and deprecated EAP types

at times configured for other services, sometime accidentally or unwittingly

Overly permissive EAP list

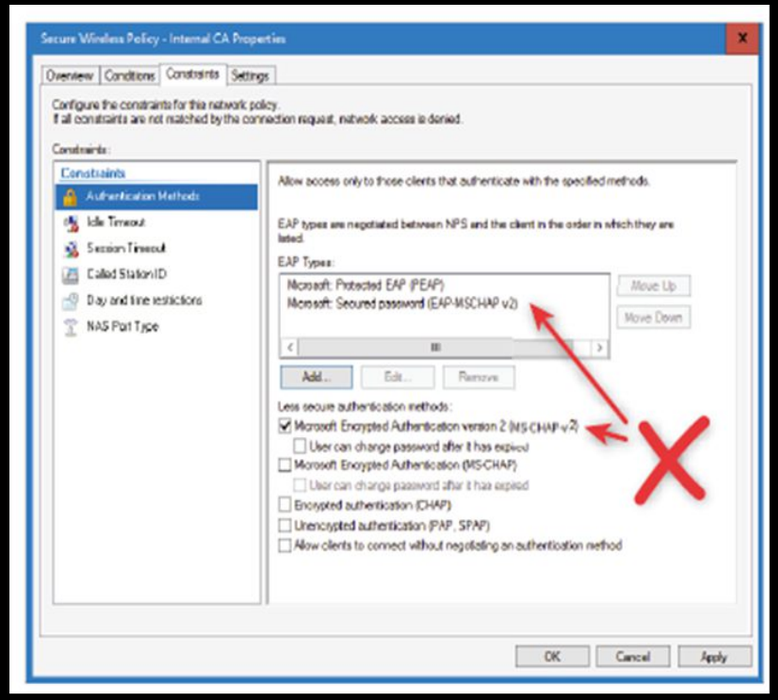
because we clicked all the boxes, it finally worked, we don't know why, and now we're not touching it!

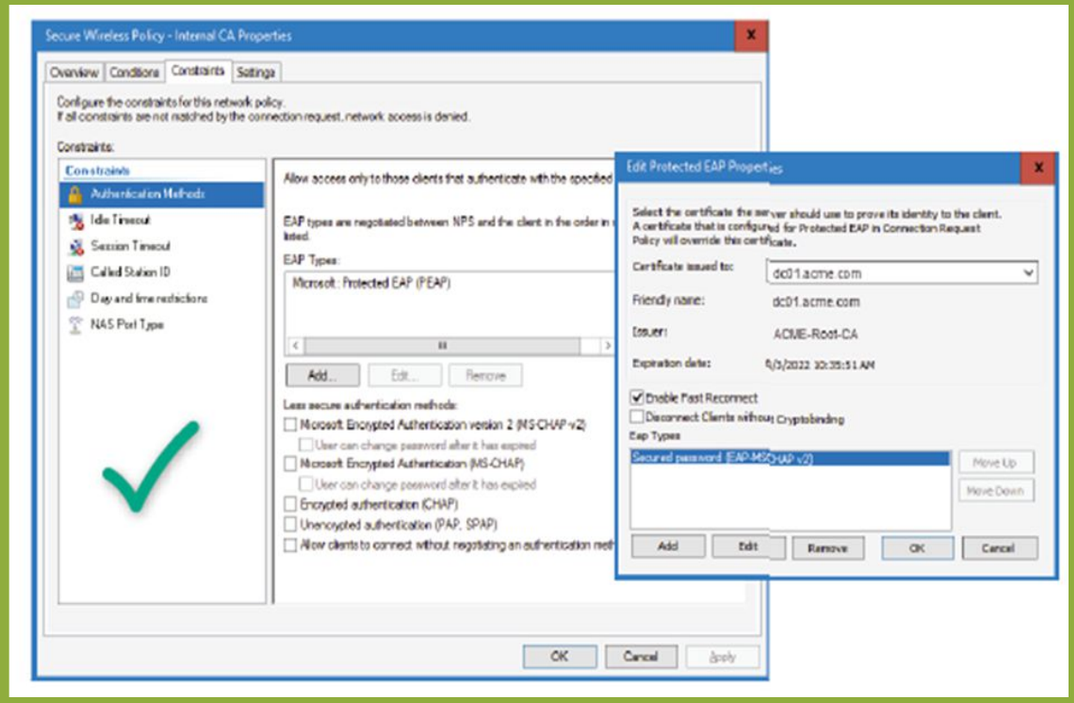
NAKED EAP

802.1X Gone Commando AKA
Your Creds are Showing...

Common misunderstanding about inner auth and secured outer tunnels for EAP often means insecure inner methods are allowed without their hard outer shell. Especially common (and risky) in PEAP/MSCHAPv2 use cases.

NAKED EAP

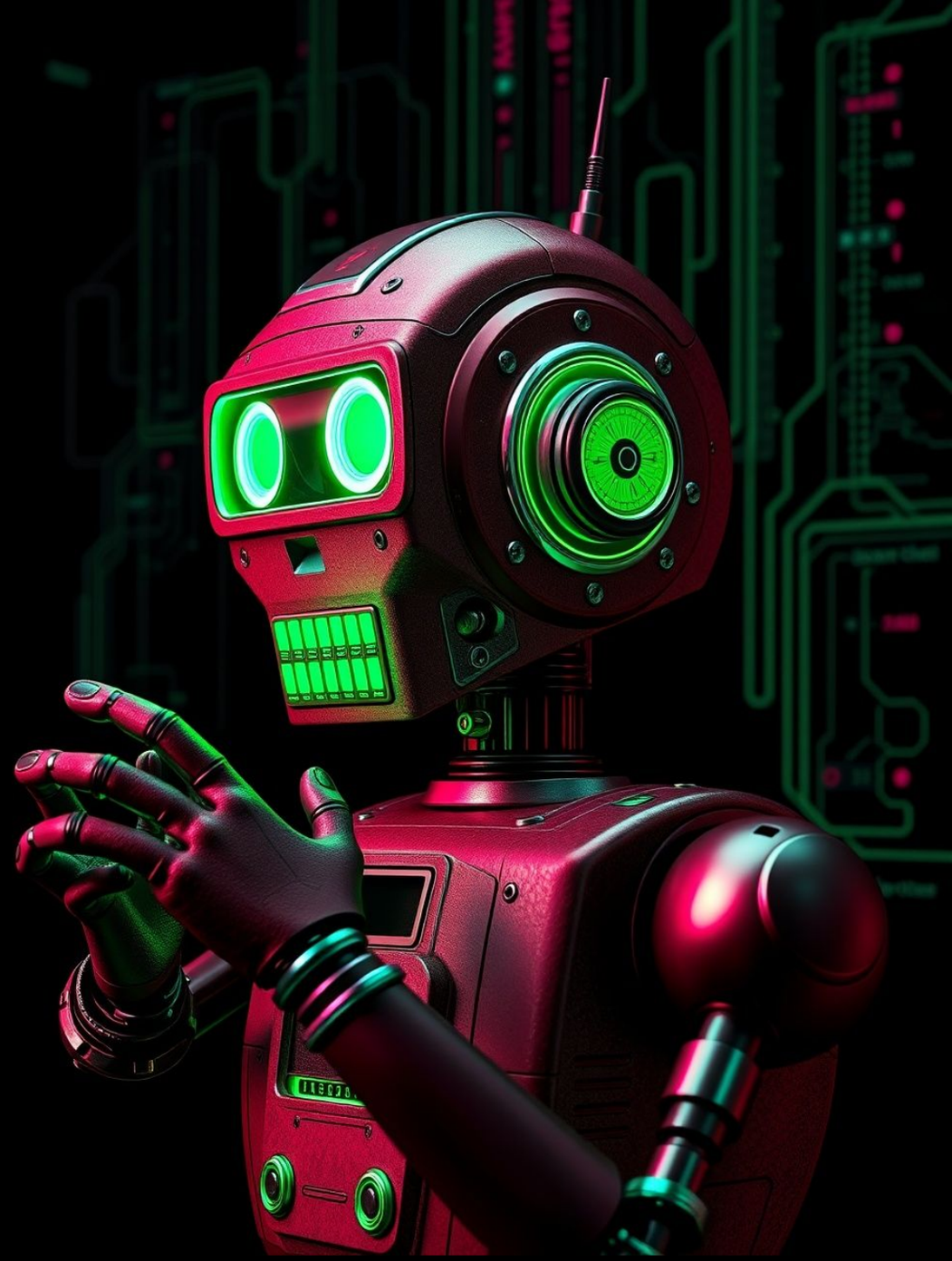

Secure Wireless Policy - Internal CA Properties
Overview
Conditions
Constraints
Settings
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Authentication Methods
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Allow access only to those clients that authenticate with the specified methods.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Microsoft: Protected EAP (PEAP)
Microsoft: Secured password (EAP-MSCHAP v2)
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method
OK
Cancel
Apply


Secure Wireless Policy - Internal CA Properties
Overview
Conditions
Constraints
Settings
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Authentication Methods
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
EAP Types:
Microsoft: Protected EAP (PEAP)
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP v2)
Microsoft Encrypted Authentication (MS-CHAP)
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
OK
Cancel
Apply
Edit Protected EAP Properties
Select the certificate the server should use to prove its identity to the client.
A certificate that is configured for Protected EAP in Connection Request
Policy will override this certificate.
Certificate issued to:
dc01.acme.com
Friendly name:
dc01.acme.com
Issuer:
ACME-Root-CA
Expiration date:
Enable Fast Reconnect
Disconnect Clients without Cryptobinding
Eap Types
Secured password (EAP-MSCHAP v2)
Move Up
Move Down
Add
Edit
Remove
OK
Cancel

LACK OF LOGIC

AND, OR, IF, THEN are our friends

RADIUS policies are often missing even basic binary Boolean logic, missing out on the most basic security controls such as ensuring the thing connecting is BOTH a known user AND a known device.



but...
the WORST
RADIUS SIN
of ALL

NOT VALIDATING the FREAKIN' SERVER CERTIFICATE

Attacks

Bad RADIUS-ing can lead to countless attacks and a false sense of security

Nearest Neighbor Attack

Pivoting through neighbor organizations using 802.1X/EAP with username/password creds scaped from the dark web is the latest hotness.

Adversary-in-the-Middle

On-path, evil twin, and a host of adversary-in-the-middle attacks are easy when server cert validation is bypassed.

Rogue Endpoints

Unknown and unauthorized endpoints on a presumably secured internal 802.1X network are extremely dangerous for myriad reasons.

03.

INVISIBLE VENDOR FAILS

DISCLAIMER

no shade, just facts...

These examples are equal-opportunity offenders — every vendor has had their turn breaking the rules. No vendors were harmed during the creation of this presentation.

Securing WPA3-Personal Networks

WPA3™ Specification v3.4

4 STA AKM Selection Preference Order

When a WPA3 STA needs to choose between multiple AKMs advertised on a BSS, the STA shall select the first AKM in preference order from the applicable list in the subclauses below. No preference order is defined for AKMs that are not specified in this section.

NOTE: This preference order applies when the STA selects between the set of AKMs that are both advertised on a given BSS and enabled in the STA's Network Profile. It does not imply any requirements on the AKMs enabled in the STA's Network Profile and does not imply any preference regarding the STA's selection between multiple BSSs.

4.1 Personal modes

1. FT Authentication over SAE using group-dependent hash 00-0F-AC:25
2. SAE Authentication using group-dependent hash 00-0F-AC:24
3. FT Authentication over SAE 00-0F-AC:9
4. SAE Authentication 00-0F-AC:8
5. FT Authentication over PSK 00-0F-AC:4
6. PSK using SHA-256 00-0F-AC:6
7. PSK 00-0F-AC:2

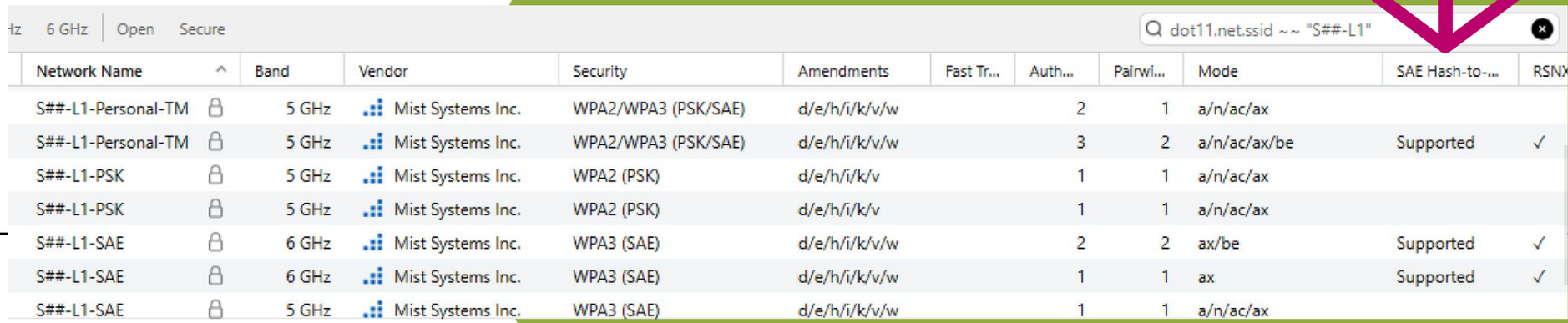
Dragonblood: Don't call it a comeback, it never left!

Mist only uses AKM:24 on 6GHZ * Wi-Fi 6

Viszen Security

Dragonblood: Don't call it a comeback, it never left!

Vendors are still using AKM:8 instead of AKM:24



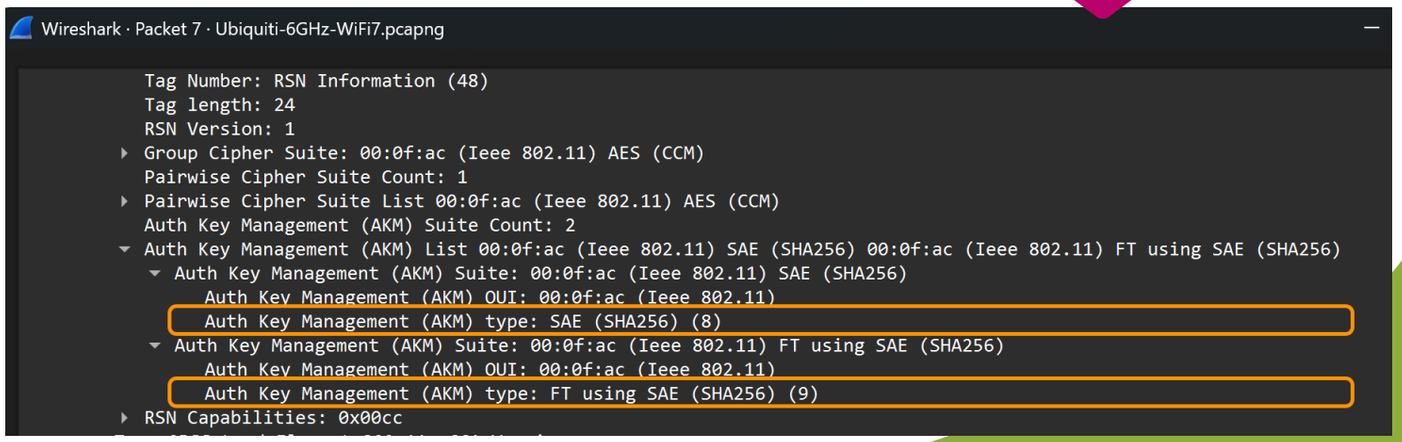
Network Name	Band	Vendor	Security	Amendments	Fast Tr...	Auth...	Pairwi...	Mode	SAE Hash-to-...	RSNX
S##-L1-Personal-TM	5 GHz	Mist Systems Inc.	WPA2/WPA3 (PSK/SAE)	d/e/h/i/k/v/w		2	1	a/n/ac/ax		
S##-L1-Personal-TM	5 GHz	Mist Systems Inc.	WPA2/WPA3 (PSK/SAE)	d/e/h/i/k/v/w		3	2	a/n/ac/ax/be	Supported	✓
S##-L1-PSK	5 GHz	Mist Systems Inc.	WPA2 (PSK)	d/e/h/i/k/v		1	1	a/n/ac/ax		
S##-L1-PSK	5 GHz	Mist Systems Inc.	WPA2 (PSK)	d/e/h/i/k/v		1	1	a/n/ac/ax		
S##-L1-SAE	6 GHz	Mist Systems Inc.	WPA3 (SAE)	d/e/h/i/k/v/w		2	2	ax/be	Supported	✓
S##-L1-SAE	6 GHz	Mist Systems Inc.	WPA3 (SAE)	d/e/h/i/k/v/w		1	1	ax	Supported	✓
S##-L1-SAE	5 GHz	Mist Systems Inc.	WPA3 (SAE)	d/e/h/i/k/v/w		1	1	a/n/ac/ax		

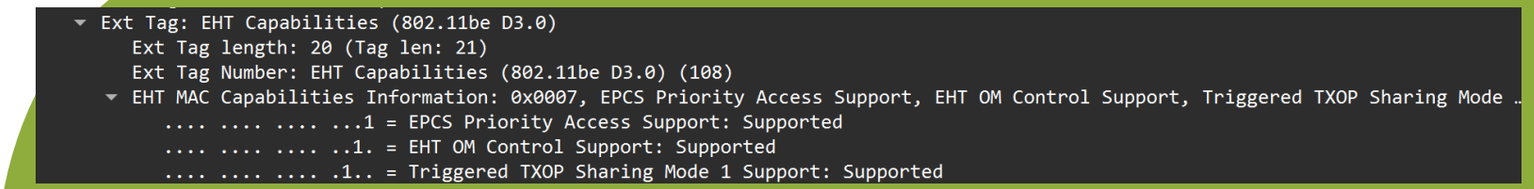
Mist only uses AKM:24 on 6GHZ * Wi-Fi 6

Viszen Security

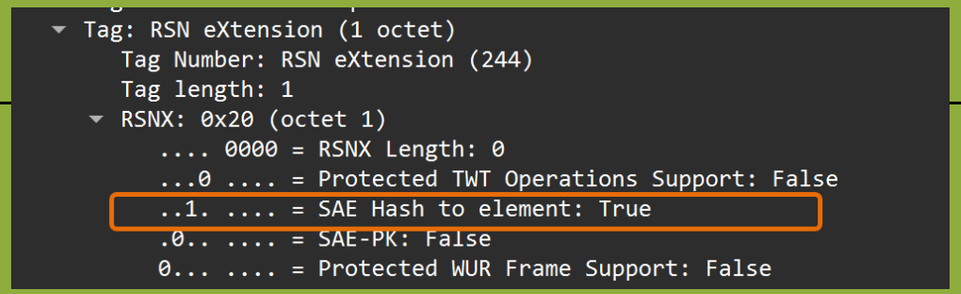
Dragonblood: Don't call it a comeback, it never left!

Vendors are still using AKM:8 instead of AKM:24





Ubiquiti Wi-Fi 7 on 6GHz, no AKM:24 in sight



However, they do have H2E enabled

Viszen Security

Dragonblood: Don't call it a comeback, it never left!

Vendors are still using AKM:8 instead of AKM:24

All vendors Wi-Fi 7 on 6GHz, by default are advertising AKM:8... no AKM:24 in sight

PMF integrity probably still works... ?
¯_(ツ)_/¯

PMF group mgmt. suite advertisements missing

Expected.... at the end of RSNE

Information Element	Details
.... .1..	MFP Required: Yes
.... 1...	MFP Capable: Yes
....0	Joint Multi-band RSNA: Not supported
.... ..0.	PeerKey Enabled: No
.... .0..	Reserved
.... 0...	Reserved
...0	BIP Compact Encapsulation: Not supported
..0.	Extended Key ID for Individually Addressed Frames: Not supported
.0..	OCVC: Not supported
0...	Reserved
PMKID Count:	0
Group Management Cipher Suite OUI:	00-0F-AC (IEEE 802.11)
Group Management Cipher Suite Type:	BIP-CMAC-128 (6)

UBNT7 | 6 GHz | Ubiquiti Networks... | WPA3 (SAE) | d/e/h/i/k/r/v/w | OTA | 2 | 1 | ax/be

Network Details | Spectrum 2.4 / 5 GHz | Spectrum 6 GHz | Advanced Details

Information Element	Details
Version:	1
Group Cipher Suite OUI:	00-0F-AC (IEEE 802.11)
Group Cipher Suite Type:	CCMP-128 (4)
Pairwise Cipher Suite Count:	1
Pairwise Cipher Suite List	
Auth Key Management Suite Count:	2
Auth Key Management Suite List	
RSN Capabilities:	0x00cc
5 bytes BSS Load	*Station Count: 0, Channel Utilization: 2%*

Missing...

Viszen Security

MPSK... PPSK.. UPSK... IPSK.. DPSK... no workie on WPA3 securely and easily

Proprietary Not-Secure MPSK on WPA3

Creating a Network That Uses a Dynamic Pre-Shared Key

Last Updated **Oct 08, 2025** | 8 minutes read | # **RUCKUS One** # **Product Guides** # **Install and Upgrade**

- WPA2 (Recommended) is strong Wi-Fi security that is widely available on all mobile devices manufactured after 2006. WPA2 should be selected unless you have a specific reason to choose otherwise.
- WPA security can be configured if you have older devices that do not support WPA2. These devices were likely manufactured before 2006. RUCKUS recommends that you upgrade or replace the older devices. 6 GHz radios are supported with WPA3 only.
- WPA2/WPA3 mixed mode supports the high-end WPA3, which is the highest level of Wi-Fi security available and WPA2 which is still common and still provides good security. The WPA2/WPA3 mixed mode only will apply to the 'supported' AP models. This Network will not be applied to the Non-Supported AP models. Note that the combination of Dynamic Pre-Shared Key (DPSK) technology with WPA3 encryption results in a DPSK3.

Note:

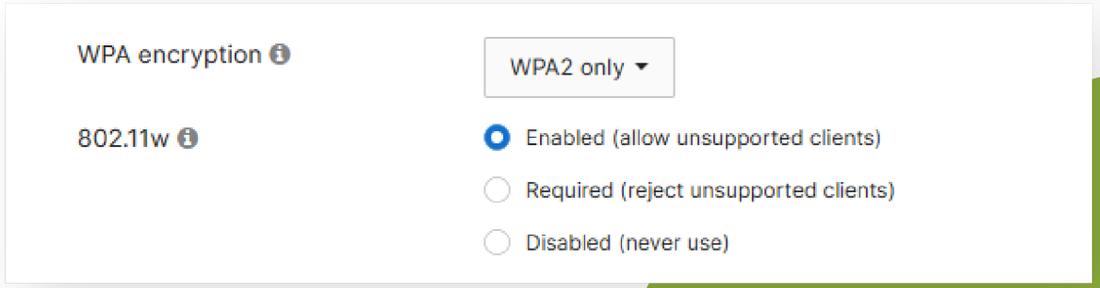
- Wi-Fi-6E clients must connect on 2.4 GHz/ 5 GHz to bind the passphrase first and then connect to service DPSK network on 6 GHz radio.
- In general, mobile devices manufactured after 2006 support WPA2 and devices manufactured after 2019 support WPA3.

Ruckus telling everyone WPA2 is secure... and then instructing towards a downgrade to pre-connect to bind the DPSK before moving to 6GHz.

Viszen Security

WPA2 with PMF Required...

Myriad Configs for Shooting Oneself in the Foot



Meraki UI allows WPA2 only with PMF required... supported but definitely not ideal

Viszen Security

THANK YOU!

QUESTIONS
COMMENTS
DISCUSSION