

Wi-Fi Security

Conversation Starter..

Phil Keeley

SE – Juniper Mist

2021 Magic Quadrant



Gartner Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure, Mike Toussaint, Christian Canales, Tim Zimmerman, 16 November 2021.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the US and internationally and is used with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Juniper Networks.

JUNIPER
driven by Mist AI

Primary Security Options

802.1x EAP

Best Option – but can be complex to deploy

Pre Shared Key

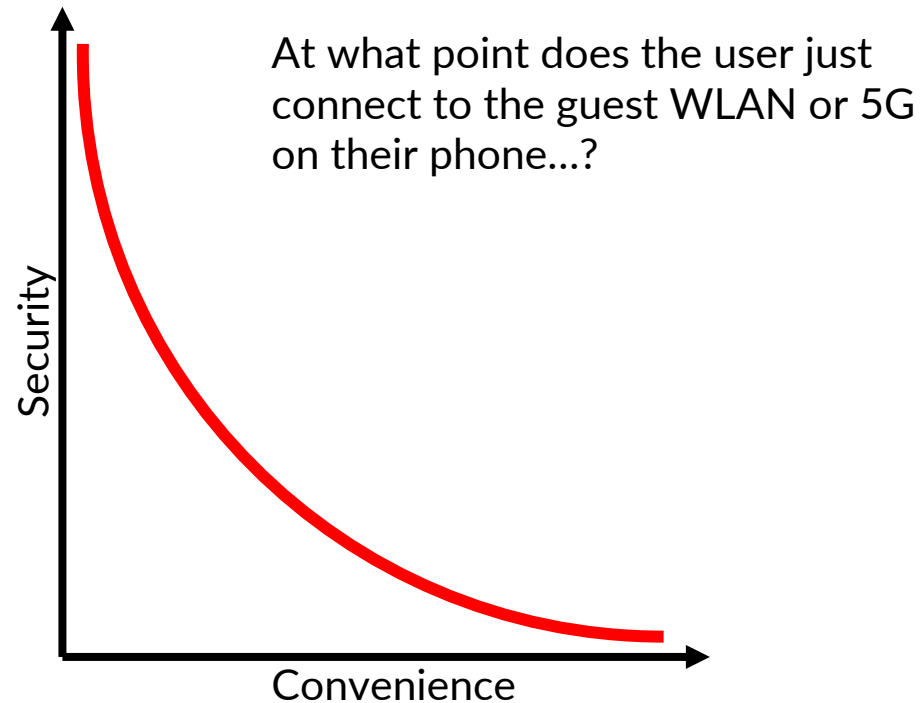
Issues – Privacy – Key Management Etc

Open / Captive Portal

Traditional Guest Access – Mac Issues, HTTPS, CNA

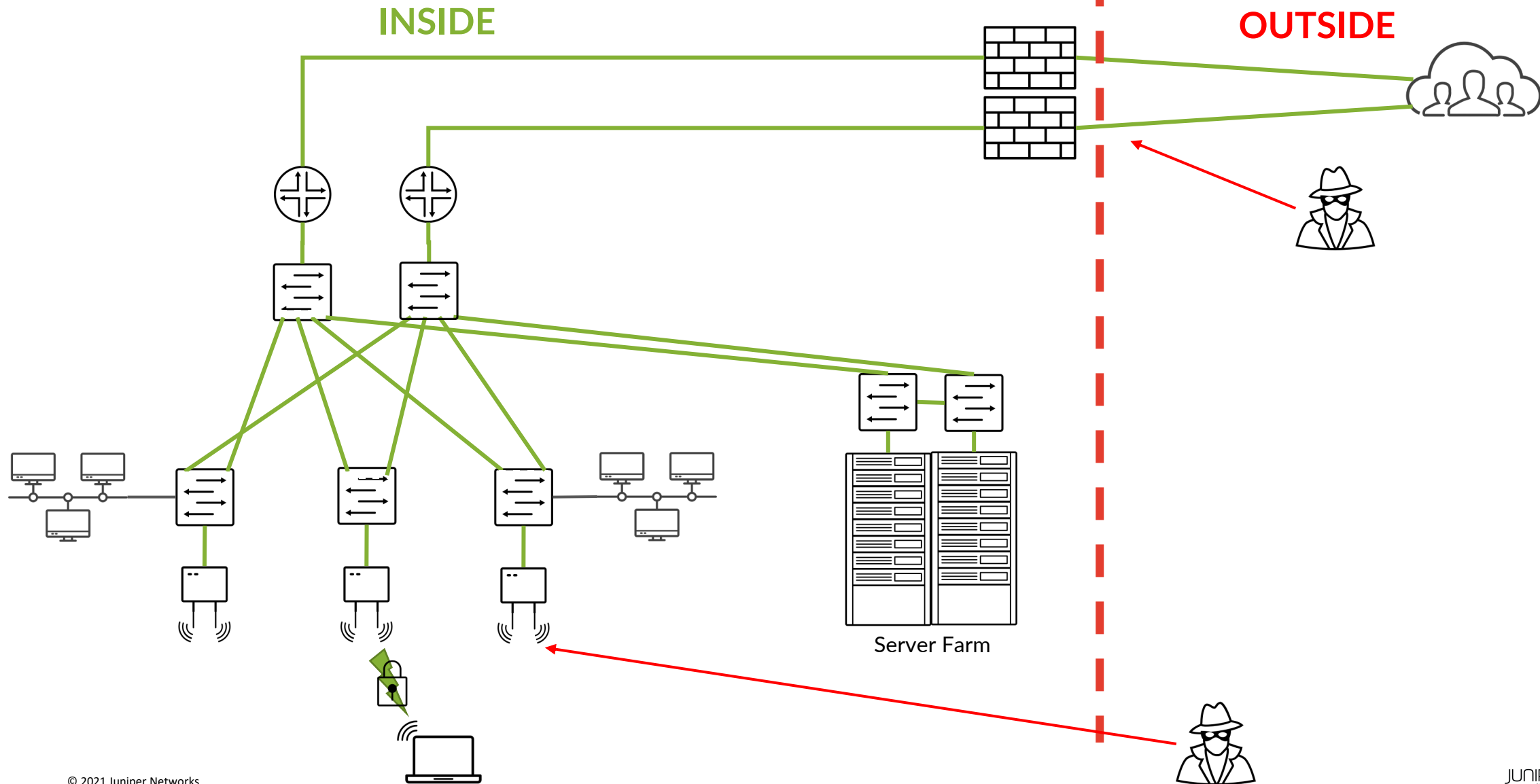
Security Considerations

Security is a large part of the user experience – ensuring the right solution is a challenge!

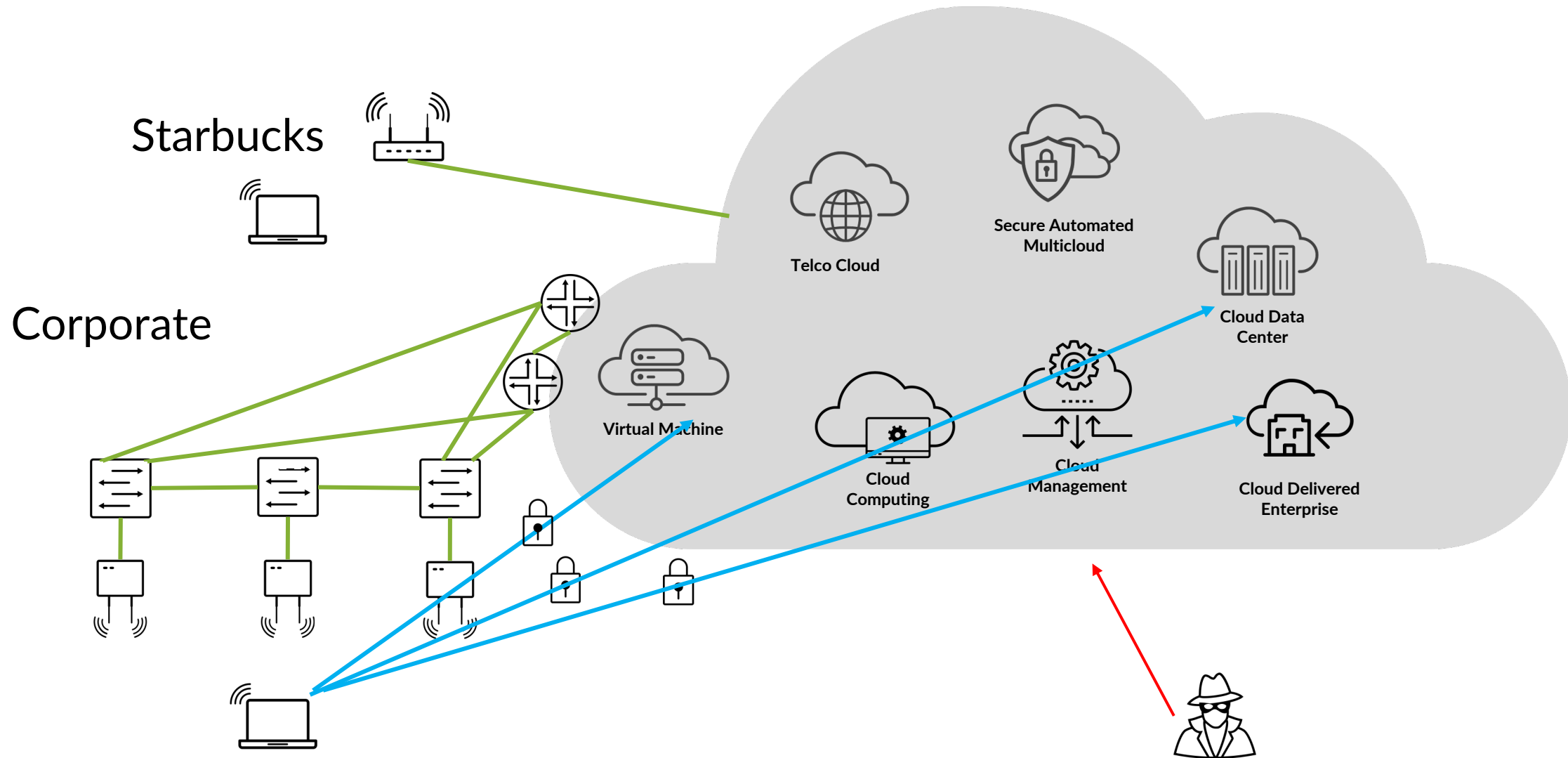


Video Credit: <https://10guards.com/en/>
Original Link: <https://www.youtube.com/watch?v=84gvEKJiJzc>

Networks are changing...



2025 Corporate Network - Glorified Hotspot..?



MPSK / PPSK / DPSK – Many versions!

- Addressing the main issues with the traditional PSK
 - Single key – gets shared – no audit trail
 - Single key – almost impossible to manage rotation
 - Single key – all users are the same per SSID
 - SSID proliferation for client differentiation
- Multiple Pre Shared Key
 - Key per user / application / type of device
 - Multiple VLAN support
 - Key rotation made simpler
 - Single SSID – unlimited types of user

Visitor Guest Management – Seamless & Secure

Sponsored Guest Access

The screenshot shows the 'Guest Portal Options' configuration window. The 'Authorization' tab is selected. Under 'Authorization Options', the 'Sponsored Guest Access' checkbox is checked and highlighted with a purple box. Below it, the 'Allowed email domains' field contains 'email.com'. In the 'Authorization Settings' section, the 'Sponsor email request will remain valid for' field is set to '60 Minutes' and is also highlighted with a purple box. Other options include 'Passphrase', 'Authentication code via Email', 'Authentication code via Text Message', and various social sign-in options (Google, Facebook, Amazon, Microsoft, Azure). The 'Devices remain authorized for' field is set to '8 Hours'. At the bottom, there are 'Preview Guest Portal', 'OK', and 'Cancel' buttons.

Integrated - Personal PreShared Key



- ✓ Provision a unique, temporary code for each visitor
- ✓ Share credentials via email and or text message with visitors
- ✓ No more insecure guest network policies, with one password for all

IOT – Real Customer Example

- Large distributed retailer – 18,000 sites
- 10 IOT VLANs defined
- Different PSK per device type per VLAN per site
- Around 200,000 keys in the system – only valid on relevant site
- Managed automatically through API – from Service Now & Netbox
- Each PSK has a policy attached to only allow specific service
- Key value is very low in real terms

Wi-Fi User Authentication

- 802.1X usual route to secure connection
 - Positives:
 - VLAN derivation
 - Role based access
 - Firewall based on role
 - Negatives
 - Radius server infrastructure required
 - Complex to configure and maintain (client and IT)
 - Limited options in cloud first deployments
- Multiple Pre Shared Key
 - Positives:
 - Same VLAN, Role based access and firewall rules
 - Simple setup from corporate and end user perspective
 - Traceable key sharing and device control
 - Negatives
 - Not as secure as 802.1X

Edit Pre-Shared Key

Key Name
Guest_001_PSK

SSID
Guest-PSK

VLAN
101
(1 - 4094)

Passphrase
..... Reveal
Characters: 8 Generate Random

Expiration Date
Duration

Expire in: 6 Months

Usage
Multiple users

Max Usage
(Please contact Mist for firmware)
 Unlimited devices Set number of devices
3

Role
(Please contact Mist for firmware)
GuestUser

Save Cancel

MPSK as a corporate connection – Customer concept

- Device connects with well known PSK – which allows access to registration site
- User authenticates and generates a unique key / policy pair auto installed on laptop
- Device re-connects with new PSK
- Periodically – background task on laptop creates a new PSK
 - Laptop uses Mist API to push new PSK into MIST cloud
 - Laptop connects using the new PSK to validate it works
 - Laptop then deletes it's old PSK in the Mist API
 - Self rotating keys!
- Keys don't have to be Password1234 – they can contain any ASCII character
- API automation removes the need to have human readable keys

API is Key!

Get Update Delete Org Psk

DELETE OPTIONS GET

GET /api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/psks/12139591-3e45-4701-81bc-56824acabfca

HTTP 200 OK
Allow: DELETE, GET, OPTIONS, PUT
Content-Type: application/json
Vary: Accept




```
{
  "usage": "multi",
  "id": "12139591-3e45-4701-81bc-56824acabfca",
  "name": "_Member",
  "for_site": false,
  "last_used": null,
  "site_id": "00000000-0000-0000-0000-000000000000",
  "org_id": "9777c1a0-6ef6-11e6-8bbf-02e208b2d34f",
  "created_time": 1635448574,
  "modified_time": 1635448574,
  "ssid": "Live-Demo-MPSK",
  "passphrase": "tQnL+M=h",
  "role": "",
  "expire_time": 1666898123
}
```

Media type: application/json

Content: {
 "passphrase": "my_new_key"
}

PUT

But a great GUI helps.


LIVE DEMO WED, 02:14 AM   

16 Pre-Shared Keys Reveal Passphrases Import Export Add Key

SSID	Role	Expiring Keys
Live-Demo-MPSK	4 sales	Within 1 Month 0
MPSK-Personal-WLAN	4 terminal	Within 1 Week 0
Live_demo_do_not_remove	2	Within 1 Day 0
Abhi-FS-radius_test	2	
null	2	

Filter

< 1-16 of 16 >

<input type="checkbox"/> Key Name	 MAC	Created Time	Modify Time	Passphrase	Expiration	Max Usage	Usage	SSID
<input type="checkbox"/> Envoy visitor #107333836		Oct 5, 2021 08:31:14 PM	Oct 5, 2021 08:31:14 PM	*****		Unlimited	Multiple users	Live_demo_do_not_ren
<input type="checkbox"/> Envoy visitor #108109416		Oct 13, 2021 06:47:50 PM	Oct 13, 2021 06:47:50 PM	*****		Unlimited	Multiple users	Live_demo_do_not_ren
<input type="checkbox"/> gap-test		Jul 23, 2021 09:12:47 PM	Jul 23, 2021 09:12:47 PM	*****		2 Max	Multiple users	Live-Demo-MPSK
<input type="checkbox"/> Mike-10		Feb 12, 2020 09:30:44 PM	Oct 21, 2021 12:14:18 PM	*****		Unlimited	Multiple users	Live-Demo-MPSK
<input type="checkbox"/> MPSK-Key1		Aug 5, 2021 02:33:25 AM	Aug 5, 2021 02:33:25 AM	*****		Unlimited	Multiple users	MPSK-Personal-WLAN

Manage Key Utilisation

Active Clients Registered Clients

10 Registered Clients ?

< 1-10 of 10 >

User	MAC	Site	Last Seen	Manufact
Dell-PK	1a:97:16:d4:c1:26	Philip Keeley	01:58:54 AM, Nov 17	Unknow
amazon-eb979f062	1c:4d:66:a2:73:58	Philip Keeley	02:08:06 AM, Nov 17	Amazori
ClairesiPhone2	1e:b7:c1:9a:1c:68	Philip Keeley	01:25:39 AM, Nov 17	Apple
amazon-741cfc879	20:a1:71:06:4b:c1	Philip Keeley	02:03:27 AM, Nov 17	Amazori
pkeeley-mbp	38:f9:d3:96:39:31	Philip Keeley	01:46:03 AM, Nov 17	Apple
OnePlus-8-Pro	4c:4f:ee:de:57:47	Philip Keeley	02:48:39 AM, Nov 16	OnePlu
Apple-TV	70:73:cb:c8:a9:1d	Philip Keeley	02:00:17 AM, Nov 17	Apple
LAPTOP-DE2MO9P6	80:91:33:85:2f:33	Philip Keeley	01:54:13 AM, Nov 17	AzureV
Philips-MBP	98:01:a7:ad:51:f1	Philip Keeley	04:20:39 AM, Nov 16	Apple
localhost	a8:10:87:b3:31:9c	Philip Keeley	10:28:15 AM, Nov 16	Texas I

Active Clients Registered Clients

6 Active Clients ?

< 1-6 of 6 >

User	MAC	Site	Last Seen	Manufact
Dell-PK	1a:97:16:d4:c1:26	Philip Keeley	01:58:54 AM, Nov 17	Unknow
amazon-eb979f062	1c:4d:66:a2:73:58	Philip Keeley	02:08:06 AM, Nov 17	Amazori
ClairesiPhone2	1e:b7:c1:9a:1c:68	Philip Keeley	01:25:39 AM, Nov 17	Apple
amazon-741cfc879	20:a1:71:06:4b:c1	Philip Keeley	02:03:27 AM, Nov 17	Amazori
pkeeley-mbp	38:f9:d3:96:39:31	Philip Keeley	01:46:03 AM, Nov 17	Apple
Apple-TV	70:73:cb:c8:a9:1d	Philip Keeley	02:00:17 AM, Nov 17	Apple

So is a single SSID possible?

6 Pre-Shared Keys

Reveal Passphrases

Import

Export

Add Key



SSID	Role	Expiring Keys
Single-WLAN	CorpUser	Within 1 Month
	GuestUsers	Within 1 Week
	meetpad	Within 1 Day
	printer	

Filter

< 1-6 of 6 >

<input type="checkbox"/>	Key Name	MAC	Created Time	Modify Time	Passphrase	Expiration	Max Usage	Usage	SSID	VLAN ID	Role	Actions
<input type="checkbox"/>	Corp_User_001		Nov 17, 2021 02:43:16 AM	Nov 17, 2021 02:43:16 AM	*****		Unlimited	Multiple users	Single-WLAN	201	CorpUser	
<input type="checkbox"/>	Corp_User_002		Nov 17, 2021 02:34:25 AM	Nov 17, 2021 02:43:25 AM	*****		Unlimited	Multiple users	Single-WLAN	201	CorpUser	
<input type="checkbox"/>	Guest_001		Nov 17, 2021 02:33:39 AM	Nov 17, 2021 02:33:39 AM	*****	Nov 22, 2021 02:33:03 AM	2 Max	Multiple users	Single-WLAN	101	GuestUsers	
<input type="checkbox"/>	Guest_002		Nov 17, 2021 02:33:19 AM	Nov 17, 2021 02:33:49 AM	*****	Nov 22, 2021 02:33:03 AM	2 Max	Multiple users	Single-WLAN	101	GuestUsers	
<input type="checkbox"/>	IOT_Meeting_Room_Pad		Nov 17, 2021 02:45:40 AM	Nov 17, 2021 02:45:40 AM	*****	Jan 1, 2023 07:30:00 AM	10 Max	Multiple users	Single-WLAN	302	meetpad	
<input type="checkbox"/>	IOT_Printer		Nov 17, 2021 02:44:20 AM	Nov 17, 2021 02:44:20 AM	*****		5 Max	Multiple users	Single-WLAN	301	printer	

Thank you

JUNIPER 
driven by Mist AI