



# Juniper Mist Access Assurance

Vijendra Singh, Reseller at Juniper Networks

# What is Network Access Control (NAC)?

## Concepts



### Authentication Authorization (AAA)

- 802.1X / MAB
- Identify a User or a Device
- Determine User/Device Role
- Assign VLAN / Policy based on User Identity



### Client Profiling

- Passive Fingerprinting
- Device Type / Manufacturer visibility
- OS version visibility
- Using device fingerprint during AAA



### Posture Compliance

- Determine endpoint health and compliancy (antivirus, firewall, patches/updates etc)
- Agent-based or Agent-less
- Leverage Posture compliance status in AAA



### Zero Trust Network Access

- End-Point agent tunnels user traffic to the Cloud
- Cloud POPs classify end-user traffic and enforce network policies
- Today ZTNA exists outside of traditional NAC as a standalone concept



### Client Onboarding

- App-based on Portal based end-user device provisioning with 802.1X (certificate) or MPSK credentials
- Built-in PKI (cert) infrastructure

# What's Wrong with NAC Solutions Today?

Cisco ISE, Aruba Clearpass, Forescout NAC require professional services or a dedicated NAC IT expert

**Solutions are complex and brittle**

*Impossible to manage without breaking*

**Cumbersome troubleshooting and lack insights**

*No end-to-end visibility*

**Lack agility and scale**

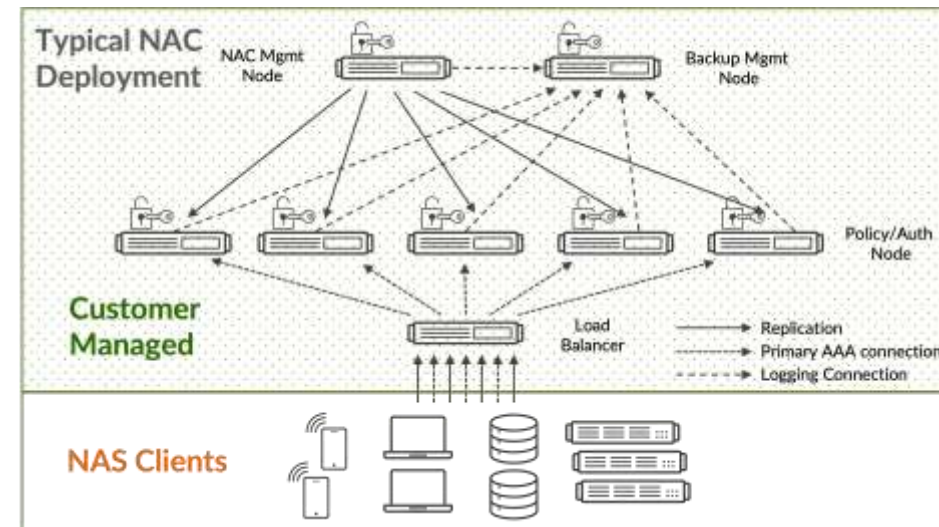
*Legacy LDAP and on-prem directories*

**Requires downtime**

*Maintenance, feature updates & security patches*

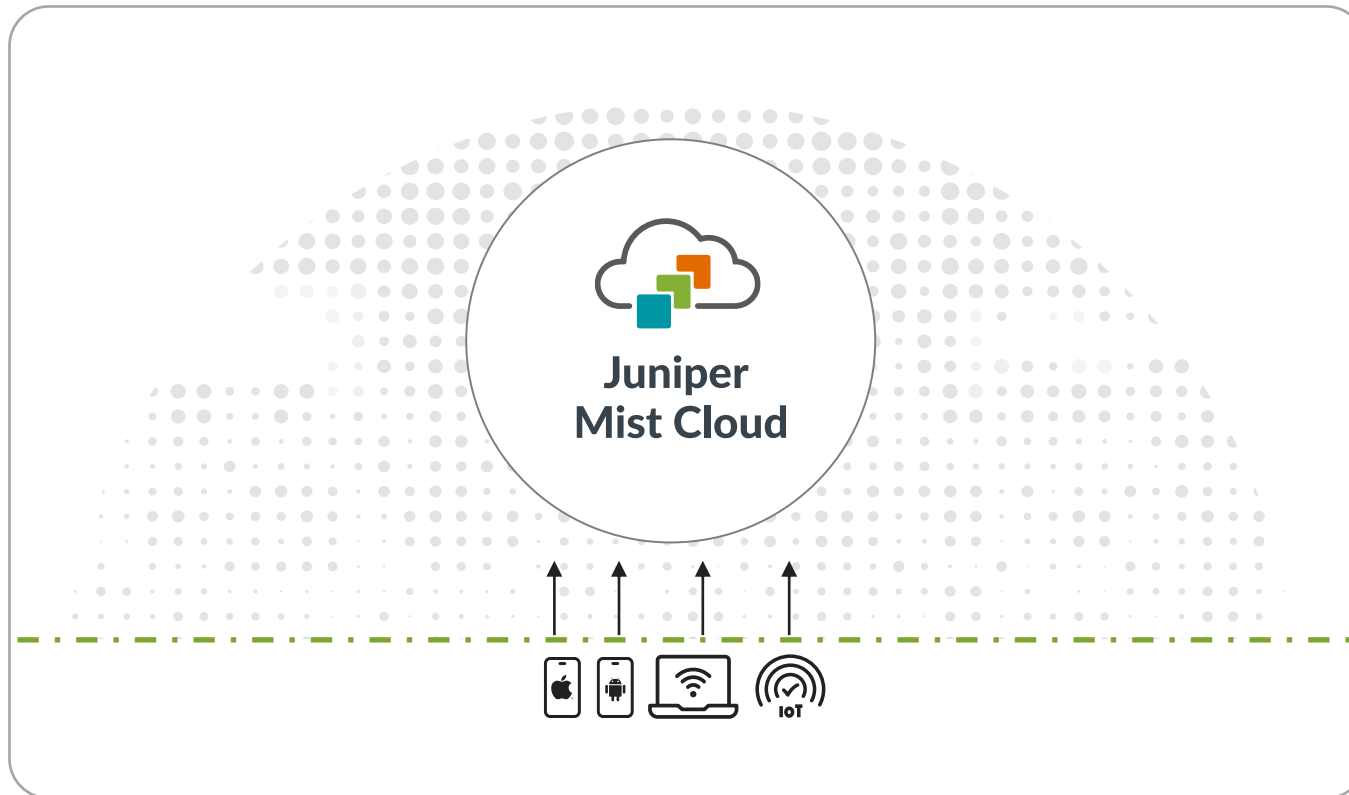
## Current NAC Customer Responsibility

- 1) Design for service redundancy
- 2) Design for high availability
- 3) Design for scale
- 4) Manually scale up or down
- 5) Maintain server hardware / VM servers
- 6) Perform upgrades / security patches



# Juniper Mist Access Assurance

## *Moving to the integrated cloud*



- ✓ **Microservices-based** Cloud NAC service natively integrated into network operations.
- ✓ **IT-friendly Day 0-2 operations** fully integrated into the network, continuously validating end-user experience.
- ✓ **AI-driven** network operations extended to network access control.
- ✓ **Periodic hitless feature updates** security patches and vulnerability fixes without downtime planning.
- ✓ **Geo-awareness, high-availability** Intrinsicly available with the Juniper Mist Cloud.

# High availability, High Reliability & Site Survivability

- All previously known clients (regardless of the auth method) get authenticated and full policy gets applied (VLANs, GBP tags, Roles, etc)
- New clients are authenticated and applied default critical service policy

## Why does it matter?



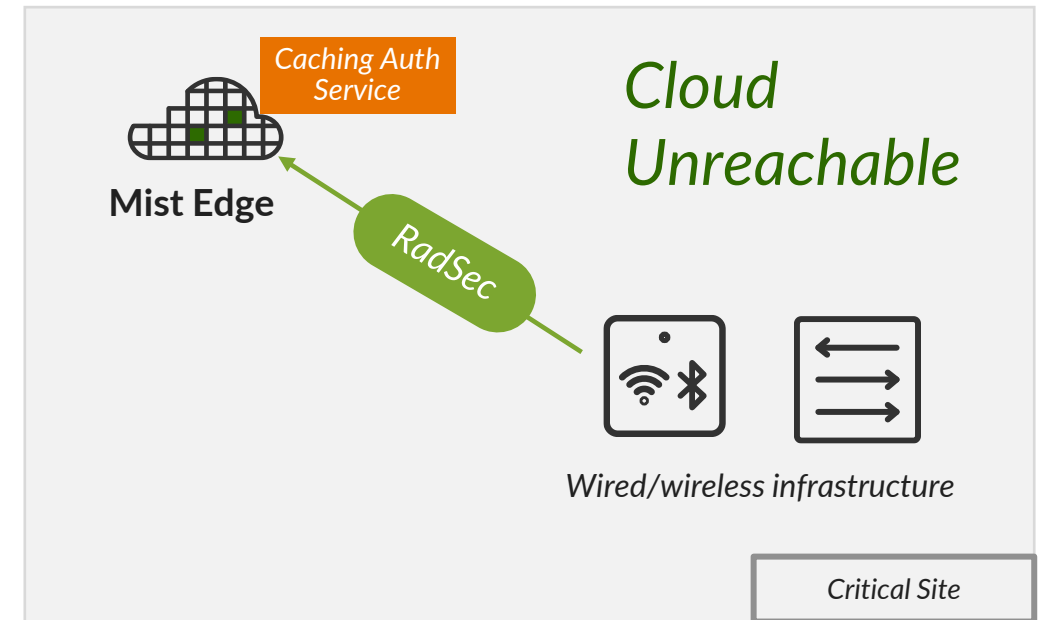
Cloud Microservices are used for the heavy lifting of authentication and authorization services.



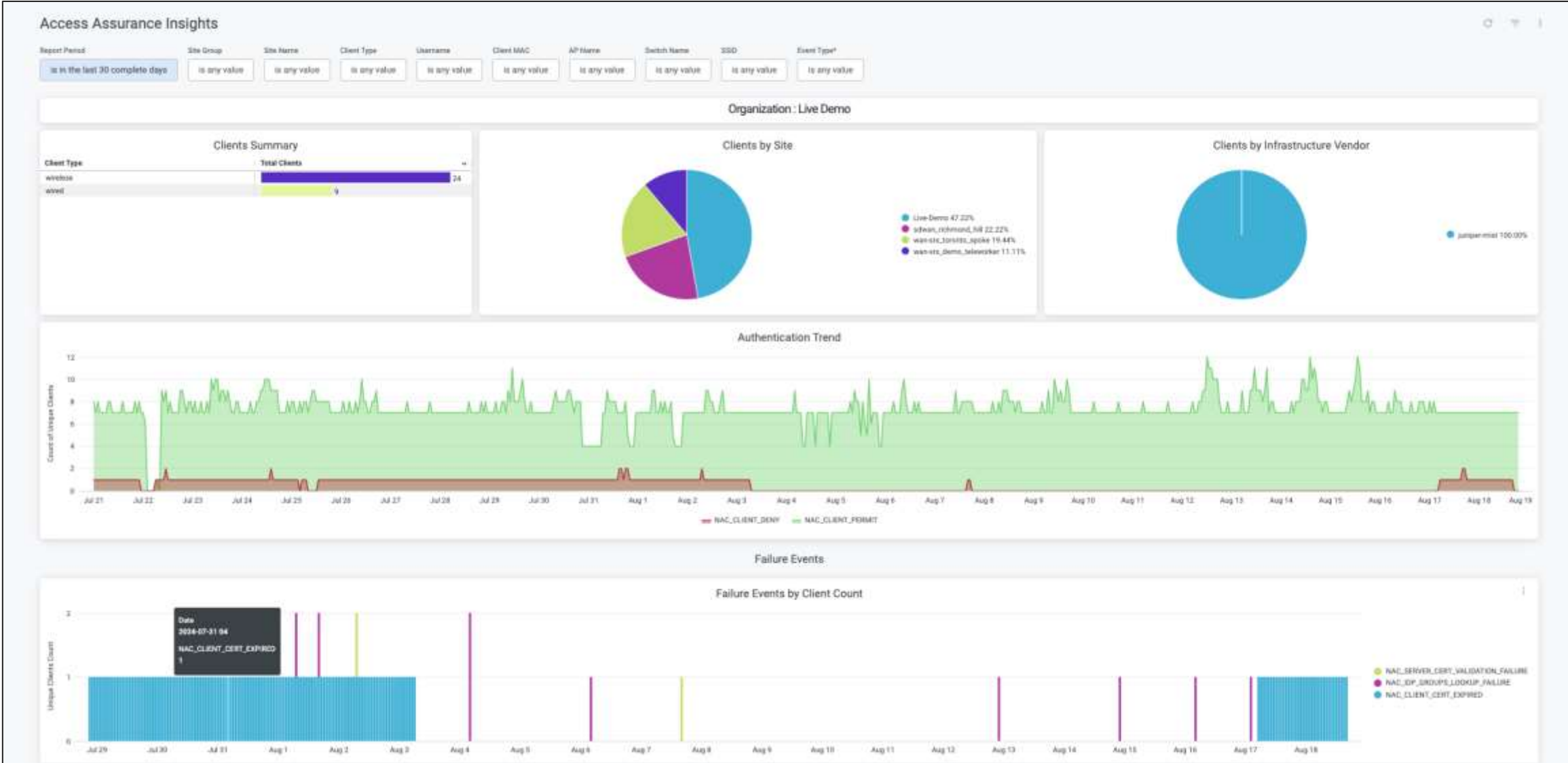
Mist Edge provides a local on-premises point of presence for site survivability functions.



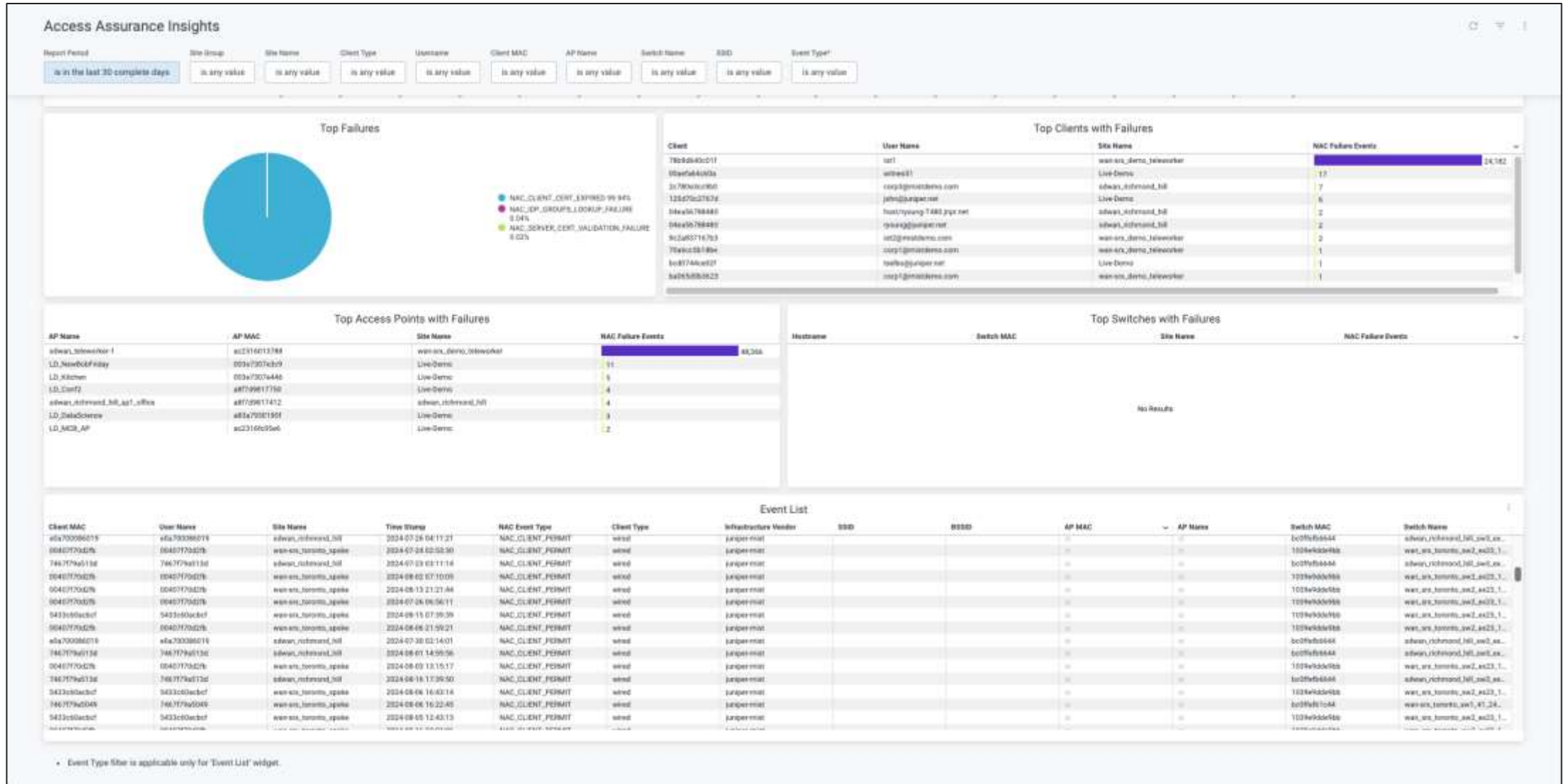
Lean operations on the Mist Edge side.



# Access Assurance Insights in Premium Analytics



# Access Assurance Insights in Premium Analytics





# Education Use Cases for IoT Assurance



# Challenges of Today's IoT/BYOD Solutions

## Lack of Central Management

*Difficult to monitor and manage thousand devices*

## Limited Visibility

*Limited visibility of user activities*

## Weak Password Policy

*Use of easily guessable or shared passwords makes devices vulnerable to attacks*

## No Automation for Access Codes Generation

*Manual generation of access codes need huge IT resources*

**3019 Pre-Shared Keys**

SSID	Role	Expiring Keys	Client Count
config-w2	appliances	Within 1 Month	vdementyev@juniper.net
misticast	fullnetaccess	Within 1 Week	1tot-devices
watchme	guests	Within 1 Day	
localpskstat			

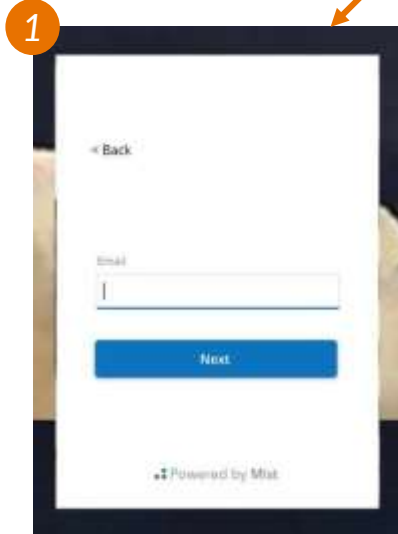
Key Name	A- Created Time	Modify Time	Passphrase	Expiration	Max Usage	SSID	VLAN ID	Role	Actions
1tot-devices	Dec 17, 2020 06:02:46 PM	May 10, 2022 05:27:00 PM	*****	May 1, 2023 10:32:33 AM	8 Max	watchme	710	appliances	
1tot-devices-old	May 6, 2022 09:12:13 PM	May 10, 2022 05:26:53 PM	*****	May 31, 2022 10:32:33 AM	8 Max	watchme	710	appliances	
cdoudkey0c7000	Feb 2, 2022 07:44:43 PM	Feb 2, 2022 07:44:43 PM	*****		Unlimited	config-w2	1		
cdoudkey0c7001	Feb 2, 2022 09:05:12 PM	Feb 2, 2022 09:05:12 PM	*****		Unlimited	config-w2	1		
cdoudkey0c7002	Nov 2, 2021 11:00:32 AM	Nov 2, 2021 11:00:32 AM	*****		Unlimited	config-w2	1		
cdoudkey0c7003	Nov 2, 2021 11:00:32 AM	Nov 2, 2021 11:00:32 AM	*****		Unlimited	config-w2	1		
cdoudkey0c7004	Nov 2, 2021 11:00:32 AM	Nov 2, 2021 11:00:32 AM	*****		Unlimited	config-w2	1		
cdoudkey0c7005	Nov 2, 2021 11:00:32 AM	Nov 2, 2021 11:00:32 AM	*****		Unlimited	config-w2	1		
cdoudkey0c7006	Nov 2, 2021 11:00:32 AM	Nov 2, 2021 11:00:32 AM	*****		Unlimited	config-w2	1		
cdoudkey0c7007	Nov 2, 2021 11:00:32 AM	Nov 2, 2021 11:00:32 AM	*****		Unlimited	config-w2	1		
cdoudkey0c7008	Nov 2, 2021 11:00:32 AM	Nov 2, 2021 11:00:32 AM	*****		Unlimited	config-w2	1		

# Juniper's IoT Assurance Solution

User authenticates using Corp credentials via SSO



PSK gets automatically generated using SSO  
Email as PSK Name:



User navigates to SPP URL, i.e. [getmyspk.company.com](https://getmyspk.company.com)



## Feature:

- Self Provisioning MPSK Portal for BYOD

## Function:

- Self-Provisioning Portal for the end users to get Personal PSK via Single Sign-On

## Outcome:

- Complete BYOD package with seamless end user onboarding (no certificates, no 3<sup>rd</sup> party apps, zero complexity)
- Native Integration into any User Directory using SAML
  - Corporate Email = PSK Name
- Flexible Onboarding Workflows based on desired use-case (Employees vs Contractors vs Sponsored Guests vs Event visitors)

# Demo 1 – IoT Assurance

The screenshot displays the Mist STAGING-LAB interface. The left sidebar contains navigation options: Monitor, Marvis™, Clients, Access Points, Switches, WAN Edges, CBRS, Location, Analytics, Site, and Organization. The main content area is titled "Client Onboarding" and features a table with 5 PSK Portal(s). A blue button labeled "Add PSK Portal" is located in the top right corner of the table area. The table columns are PSK PORTAL NAME, SSID, AUTHORIZATION, URL, and DATE CREATED. The table contains five rows of data, each with a checkbox in the first column.

<input type="checkbox"/>	PSK PORTAL NAME	SSID	AUTHORIZATION	URL	DATE CREATED
<input type="checkbox"/>	test-byod	ppsk-cloud	SSO	https://pskportal.mistsys.com/#!byod/812e31fb-53ef-4264-8b9e-8b152eddbab7	Mar 15, 2022 08:47:10 PM
<input type="checkbox"/>	psk-admin1	ppsk-cloud	SSO	https://pskportal.mistsys.com/#!admin/39ab0fee-137c-4d34-84b4-6600796a16a2	Mar 15, 2022 10:21:11 AM
<input type="checkbox"/>	PhaniTest	ppsk-cloud	SSO	https://pskportal.mistsys.com/#!byod/4d0805db-b017-42d5-a5cd-9350a076ef72	Apr 26, 2022 06:57:16 AM
<input type="checkbox"/>	NWS50-BYOD	_ResNet	SSO	https://pskportal.mistsys.com/#!byod/170fb3d5-de10-4cb6-b6ec-b5adb7f5f906	May 24, 2022 10:51:04 AM
<input type="checkbox"/>	get-wifi-byod1	ppsk-cloud	SSO	https://pskportal.mistsys.com/#!byod/e20f87c4-6ba2-4430-a26a-fb270f065c4f	Mar 15, 2022 09:54:36 AM

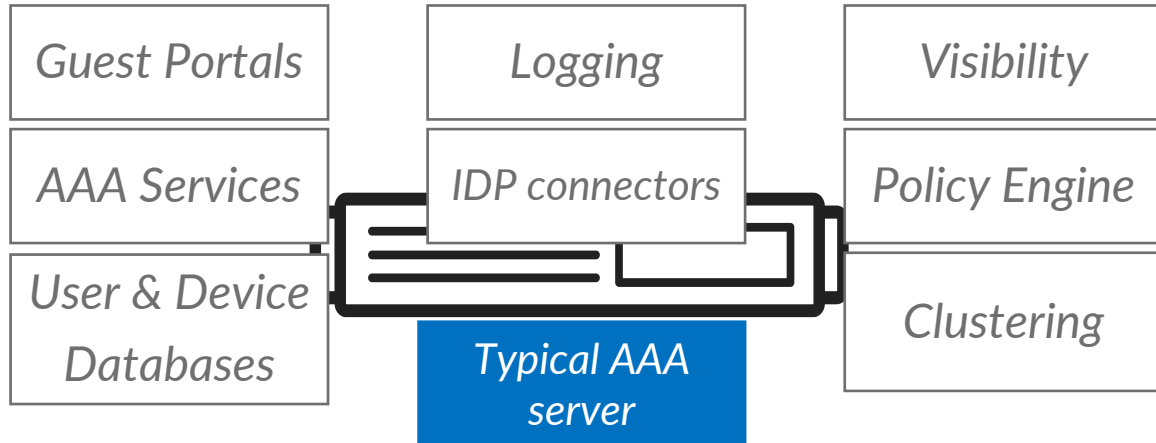


# Education Use Cases for NAC Assurance

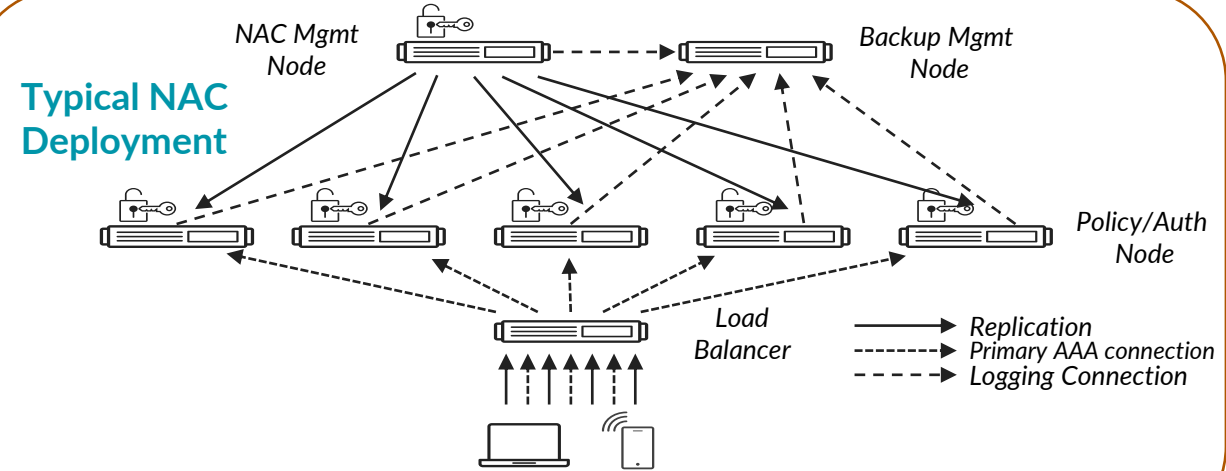
# Challenges of Today's NAC

## Functional & Architectural Complexity

### NAC: Logical Functions



### NAC: Physical Architecture



Solutions are complex, brittle, lack scale



Cumbersome troubleshooting and lacking insights



Requires downtime planning

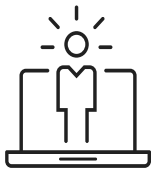
# Juniper Mist Access Assurance Solution



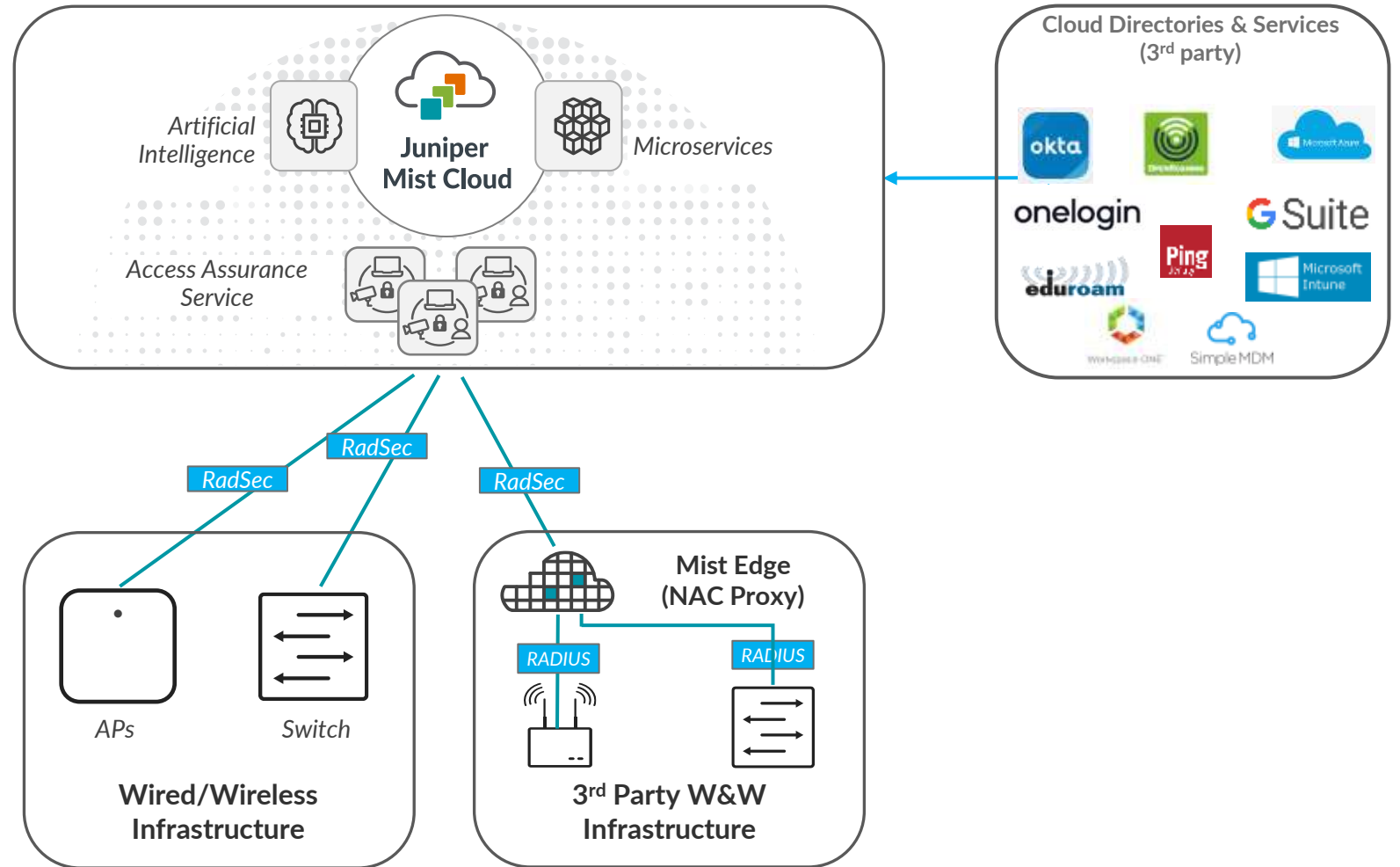
Micro-Services based Cloud NAC Offering



Industry-first AI powered operations



IT-friendly day 0-2 operations



# Mist Access Assurance = Cloud NAC Service

## *IT-friendly yet flexible Auth Policy configuration*

Name	Type	Values
VLAN with Web Filtering	AAA Attribute	VLAN: 720
VP-USERS	Directory Attribute	Group: vip-users
vip role	AAA Attribute	Role: vip-cert
Unrestricted VLAN	AAA Attribute	VLAN: 750
Slava's cert	Certificate Attribute	Common Name (CN): slava
Printers	Client List	Client MAC: 00aa0c*
Mistifi LAB Users	AAA Attribute	Realm: @lab.mistifi.com
Machine Authentication	AAA Attribute	User Name: host!*
IoT Tunnel VLAN	AAA Attribute	VLAN: 710
Employees in Azure AD	Directory Attribute	Group: Employee

### Policy

Org Policies

Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied.

No.	Name	Match Criteria (match on location, SSID, User Group, etc)	Policy	Assignments (VLANs, etc)
<input type="checkbox"/>	1	Wireless Cert Auth + Cert Issued by LAB CA × EAP-TLS × Wireless ×	→ ✓	Network Access Allowed Unrestricted VLAN × Employee Role × +
<input type="checkbox"/>	2	TTLS auth against... + Employees in Azure AD × EAP-TTLS ×	→ ✓	Network Access Allowed VLAN with Web Filtering × +
<input type="checkbox"/>	3	Wired Cert Auth + Cert Issued by LAB CA × EAP-TLS × Wired ×	→ ✓	Network Access Allowed Unrestricted VLAN × +
<input type="checkbox"/>	4	Printer MAB + AuthorizedPrinters × MAB × Wired ×	→ ✓	Network Access Allowed IoT Wired VLAN × +
<input type="checkbox"/>	5	JNPR Cert + EAP-TLS × Wireless ×	→ ✓	Network Access Allowed Unrestricted VLAN × +
	Last	All Users	→ ✗	Network Access Denied

*Note: A tooltip for 'AAA Attribute' shows 'VLAN: 750'.*

# Demo 2 – NAC Assurance

## Client State Machine Extended to NAC

STAGING-LAB MON, 05:45 PM

Monitor Wireless Wired WAN insights client: slava@lab.mistifi.com 12:00 am, Sep 2 — 12:00 am, Sep 3

b6-ac-fc-ae-d6-8f BRQLAB

12:00 AM Sep 2 - 12:00 AM Sep 3 (drag an area of interest to Zoom In)

Total bytes

3:00 am - 4:00 am, Sep 2: Bytes: no data, 0.00 Mbps

Client Events 29 Total 14 Good 15 Neutral 0 Bad

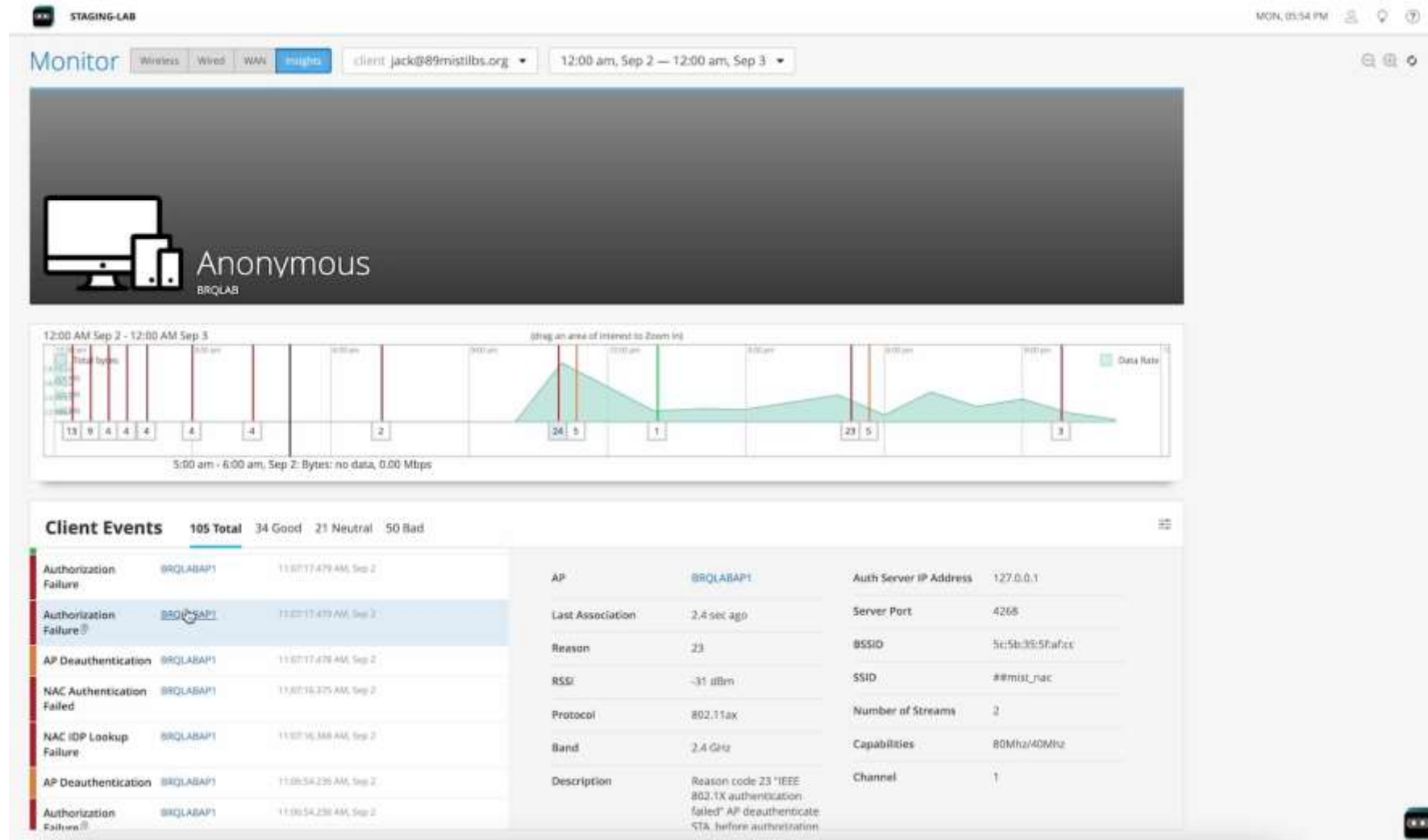
Event	AP	Time
Success		
Authorization & Reassociation	BRQLABAP2	11:04:26.603 PM, Sep 2
NAC Authorization Success	BRQLABAP2	11:04:26.801 PM, Sep 2
NAC Server Certificate Validation Success	BRQLABAP2	11:04:26.998 PM, Sep 2
NAC Client Certificate Validation Success	BRQLABAP2	11:04:28.098 PM, Sep 2
DNS Success	BRQLABAP1	11:04:03.674 PM, Sep 2
Gateway ARP	BRQLABAP1	11:04:03.398 PM, Sep 2

AP	BRQLABAP2	BSSID	5c:5b:35:5f:b0:69
SSID	##mist_nac	Certificate Serial Number	580000024a206196258220ab2700000000024a
Authentication Type	802.1X	User Name	slava@lab.mistifi.com
Certificate CN	slava	Certificate Issuer	/DC=com/DC=mistifi/DC=lab/CN=lab-CA
Certificate Expiry	2023-01-07T11:36:24Z	Certificate SAN (Email)	slava@lab.mistifi.com
Certificate SAN (JPN)	slava@lab.mistifi.com	EAP Type	EAP-TLS



# Demo 2 – NAC Assurance

## Client State Machine Extended to NAC – Failure case





# Thank you

---

JUNIPER  
NETWORKS

Driven by  
Experience™