JUNIPER MIST ACCESS ASSURANCE DATASHEET

Product overview

Juniper Mist Access Assurance is a cloud-based service that ensures zero-trust, identity-based network access and full-stack policy and segmentation assignments with end-to-end user experience visibility. The service delivers a suite of access control functionality with a flexible, yet simple authorization policy framework for onboarding guest, IoT, BYOD, and corporate devices. Client connection is controlled based on user and device identities, regulating access for devices connecting to the network. Access Assurance also provides access control services for devices leveraging 802.1X authentication and MAC Address Bypass for non-802.1X allowlisted, wired IoT devices.

Product Description

Juniper® Mist™ Access Assurance is a microservices-based, cloud network access control (NAC) service that enables enterprises to easily enforce a zero-trust security model. Access Assurance solves many complexity challenges associated with traditional NAC offerings, by removing on-premises server hardware, providing inherent service high-availability, resilience, as well as automatic at-run-time feature updates, security, and vulnerability fixes. Extending Juniper Mist IoT Assurance capabilities, which simplifies on-boarding for headless IoT and BYOD devices, Access Assurance extends support to onboard wired and wireless devices with 802.1X authentication or MAC Authentication Bypass (MAB) methods for non-802.1X devices.

Access Assurance uses hundreds of different vectors to match the identity of the user and the device, such as X.509 certificate attributes, user group memberships, device compliance metrics, as well as location context. These vectors help determine identity-based network admission criteria, such as the network segment or a microsegment a device should connect to and the network policy that should be dynamically applied to a user.

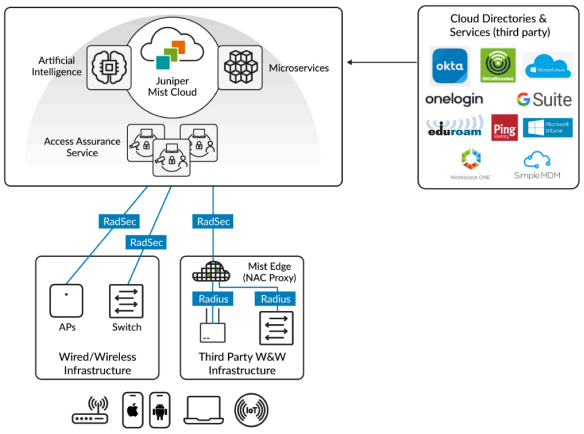

Figure 1: Juniper Mist Access Assurance cloud service greatly simplifies network access control.

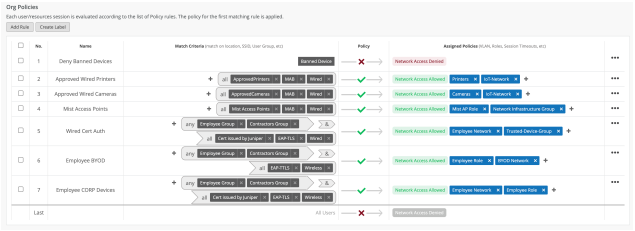

Figure 2: The flexible policy creation interface helps admins assign policies based on business requirements.

Most importantly, Access Assurance provides end-to-end connectivity troubleshooting in a unified view from the client, network infrastructure, and access control perspective, dramatically simplifying Day 2 support. IT admins gain a cohesive view of the end-user experience and can determine whether poor experiences are due to client configuration, network infrastructure, authentication, or a service.

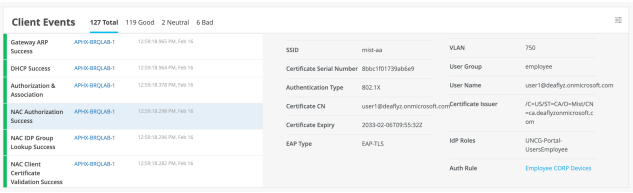

Figure 3: Client SLE tracks network access control events.

Architecture and Key Components

Access Assurance is delivered through Juniper Mist cloud and powered by Mist AI. The microservices architecture ties together high availability, redundancy, and autoscaling for optimal network access across wired, Wi-Fi, and wide area networks. Using geo-awareness, Access Assurance automatically redirects authentication requests from different regions to the nearest Access Assurance instance to provide minimal latency and best end-user experience.

Access Assurance provides an authentication service by integrating external directory services like Google Workspace, Microsoft Azure AD, Okta Identity, and others. It also integrates external Public Key Infrastructure (PKI) and Mobile Device Management (MDM) providers such as Jamf, Microsoft Intune, and others to provide granular user and device identification to enforce identity-based, zero-trust network access control.

Features and Benefits

Client Experience-First

Access Assurance provides a unified view of the client connectivity experience and can easily identify a problem and perform root cause analysis. All client events including connection and authentication successes and failures are captured by Juniper Mist cloud. With this data, Juniper Mist cloud helps simplify day-to-day operations by easily identifying if an end-user connectivity issue is caused by a client configuration mistake, network infrastructure and service problems, or authentication policy configuration issues. The Juniper Mist service level expectations (SLEs) for wired and wireless clients are enhanced to include network access events, such as authentication events, certificate validations, and more.

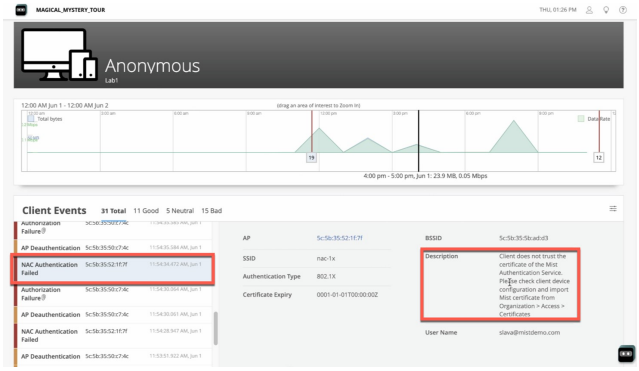

Figure 4: Client SLE failures provide descriptions for known issues.

Single Pane of Glass for Management and Operations

Access Assurance is tightly integrated with Juniper Mist cloud providing full-stack management and day-to-day operations for Wi-Fi Assurance, Wired Assurance, SD-WAN Assurance, and Access Assurance in one dashboard for end-to-end visibility. The Marvis™ AI engine leverages data from multiple sources for anomaly detection to provide actionable metrics. Through the dashboard, users can:

- create and apply access policies that ensure only authorized devices and users are allowed network access
- assign users and devices to the correct network segment
- prevent users and devices from accessing restricted resources
- add and modify certificates and certificate authorities
- configure identity providers
- monitor client activity across the organization

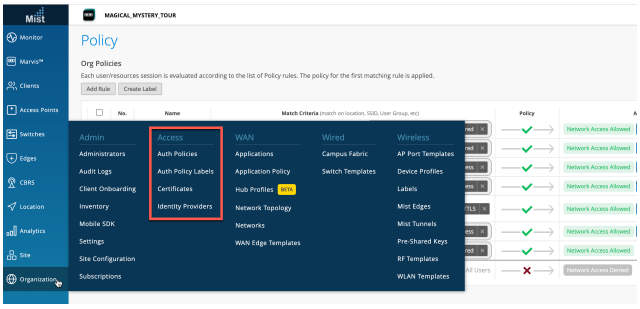

Figure 5: A friendly user interface highlights Access controls.

Granular User and Device Identity

Access Assurance is capable of granular identity fingerprinting based on X.509 certificate attributes. It also uses intrusion, detection, and prevention (IDP) information like group membership, user account state, MDM compliance state, client lists, and user location for fingerprinting. The resulting user and device fingerprint provides an identity vector for accurate policy assignment within the zero-trust principles.

Figure 6: Identity fingerprinting is possible through multiple methods.

Network Policy Enforcement and Microsegmentation

Based on user and device identity, Access Assurance can instruct the network to assign a user to a specific network segment (VLAN or a group-based policy tag), as well as enforce network policy by assigning a user role. Such roles can be leveraged in the Juniper Mist WxLAN policy framework or switch policies.

Figure 7: Enforced policies for VLANs, group-based policies, and user roles are easily visible.

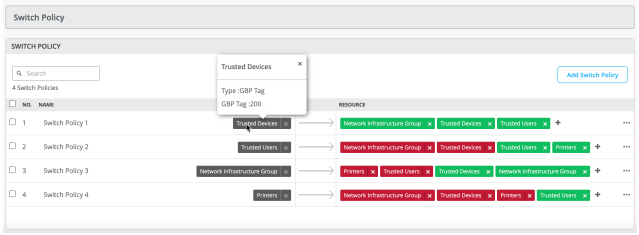

Figure 8: Recognizing policies with group-based tags is quick and fast.

Built-in High Availability and Geo-Affinity

With Access Assurance, organizations gain reliable and low-latency network access control of their networks in single and multisite deployments. Juniper has deployed cloud instances of its network access control cloud service in multiple regional locations. In multisite deployments, authentication traffic coming from the network infrastructure is automatically directed to the nearest Access Assurance instance. Latency is minimized and users enjoy an exceptional wireless experience. This automated process is fully transparent to users and requires no involvement from the IT team. Organizations are assured reliable, redundant network access for client devices regardless of the state of the nearest regional instance.

Automatic Feature and Security Updates

The Juniper Mist microservices-based cloud architecture keeps Access Assurance optimized with the most advanced technologies. New features, security patches, and updates are automatically added to Access Assurance on a bi-weekly basis without interruptions or service downtime. This capability dramatically simplifies and improves service operations for network IT administrators, eliminating lengthy software upgrades and service downtime. Juniper can easily deploy new features and functions to its cloud-based services, bringing advancements to market more rapidly and continuously improving your client-to-cloud experience.

Extending Juniper Mist IoT Assurance with Access Assurance

Access Assurance is coupled with Juniper Mist IoT Assurance to build out controls for onboarding and management of corporate devices with 802.1X authentication well as MAC-less onboarding of non-802.1X IoT and BYOD devices. IoT Assurance simplifies IT operations and secures connections for headless IoT and BYOD devices via a Multiple Pre-Shared Key (MPSK) mechanism. It incorporates a full suite of access control functionality leveraging MPSK or Private Pre-Shared Key (PPSK) as a new type of identity and policy vector.

IoT Assurance also provides PSK Portal creation enabling BYOD onboarding workflows by automating PSK generation based on user identity, leveraging Security Assertion Markup Language (SAML) for an SSO experience. It enables seamless client device onboarding via mobile QR code or by typing a personalized passphrase without installing any client software.

Marvis Virtual Network Assistant

Marvis Virtual Network Assistant uses Mist AI to help IT teams interact and engage with their networks. The Marvis AI engine binds together Access Assurance with other Juniper Mist cloud-based services, such as Wired Assurance, Wi-Fi Assurance, and WAN Assurance, helping the operations team move closer to achieving The Self-Driving Network™ with simplified troubleshooting and performance analysis.

Using features powered by Mist AI, helpdesk staff and network administrators can simply ask a question in natural language and get actionable insights using Marvis Conversational Interface that help them identify and solve network issues. Marvis brings proactive anomaly detection into the SLE dashboard. With Marvis Actions, staff gain proactive, actionable insights to identify network access issues across the full stack, providing recommendations for user connectivity issues. This provides our customers easy root cause analysis across the full network stack and authentication services.

API-Driven Architecture

Access Assurance service is 100% based on public Representational State Transfer (REST) APIs that allow easy integration with external security information and event management (SIEM) or IT service management systems or other platforms for both configuration and policy assignment. These APIs provide the capability to invoke actions based on user or external events, as well as for using the cloud-native Webhook framework. Overall, the Juniper Mist platform is 100% programmable, using open APIs, for full automation and seamless integration with complementary Juniper access, wired, wireless, WAN, security, user engagement, and asset location solutions.

Specifications

Feature	Description
X.509 certificate management	External PKI support Automatic CRL/OSCP certificate revocation check
External identity provider integration	The following protocols are supported to integrate into any identity provider to do user lookup and get device state information: • Secure Lightweight Directory Access Protocol (LDAP) • OAuth2 • RADIUS over TLS (RadSec) client
802.1X Authentication Methods	The following EAP methods are supported for secured 802.1X access: • Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) • Protected Extensible Authentication Protocol PEAP TLS Tunnel • Extensible Authentication Protocol (TEAP) (TLS/TLS) Extensible Authentication Protocol-Tunneled TLS (EAP-TTLS (PAP)
Non-802.1X authentication methods	MAC Authentication Bypass (MAB) Multi Pre-Shared Key (MPSK)
Network policy and microsegmentation	Assign VLANs, role and group-based policy tags dynamically based on the user identity
Third-party network infrastructure support	Supported via Mist Edge Auth Proxy application, third-party vendor devices can communicate over standard RADIUS to the Mist Edge Auth Proxy
Juniper Mist IoT Assurance (Included with Access Assurance subscription)	IoT and BYOD client-device onboarding • Create, rotate, auto-expire PSKs and MPSKs • Dynamic traffic engineering • Key-based WxLAN policy • Personal WLAN creation and management • Active device usage tracking per PSK • Automated key provisioning and rotation

Ordering Information

The Access Assurance service is provided as a subscription, based on the average concurrently active client devices seen over a 7-day period.

SKU	Description
S-CLIENT-S-1	Standard Access Assurance subscription for 1 client for 1 year
S-CLIENT-S-3	Standard Access Assurance subscription for 1 client for 3 years
S-CLIENT-S-5	Standard Access Assurance subscription for 1 client for 5 years

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions, and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable, and secure networks to move at the speed of business.

Corporate and Sales Headquarters

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

Phone: 888.JUNIPER (888.586.4737)

or +1.408.745.2000

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240 1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

Phone: +31.207.125.700

Juniper Networks | Driven by Experience™