

# Juniper Mist Access Assurance Guide

Published  
2025-02-20

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

*Juniper Mist Access Assurance Guide*

Copyright © 2025 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

## YEAR 2000 NOTICE

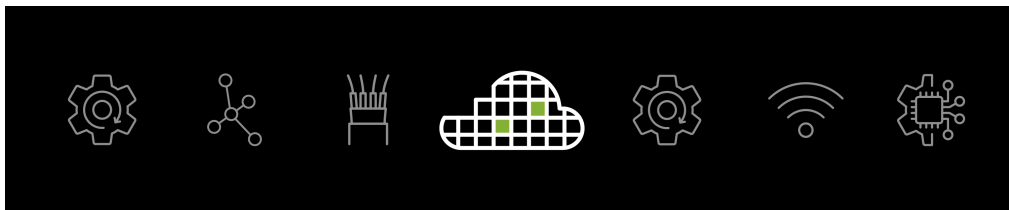
Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

## END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

## About This Guide

The Juniper Mist™ Access Assurance service provides secure network access control (NAC) for your wired and wireless networks. Use this guide to configure and manage access control based on user and device identities.



# 1

CHAPTER

## Overview

---

### IN THIS CHAPTER

- [Juniper Mist Access Assurance Overview | 2](#)
  - [Juniper Mist NAC Architecture | 4](#)
  - [Juniper Mist Access Assurance Use Cases | 6](#)
  - [Juniper Mist Access Assurance Authentication Methods | 8](#)
  - [Juniper Mist Access Assurance Best Practices | 14](#)
  - [Mist Access Assurance—Frequently Asked Questions | 16](#)
-



# Juniper Mist Access Assurance Overview

## IN THIS SECTION

- [Features | 2](#)
- [Benefits | 3](#)

Juniper Mist Access Assurance is an advanced, cloud-based network access control (NAC) service that secures your wireless and wired network by providing identity-based network access to devices and users. With this service, you can control who and what can access your network. You can set up simple rules to allow or deny access to different types of devices, such as guests, corporate devices, and devices generating IoT and BYOD traffic. The service checks the user and device identities before letting them connect to the network. The service uses 802.1X authentication for 802.1-enabled devices and MAC Authentication Bypass (MAB) verification for non-802.1X devices.

Watch the following video for a quick overview on how NAC has changed over time and what it looks like today:



**Video:** [Evolution of Existing NAC Solutions](#)

Watch the following video to understand how Juniper Mist Access Assurance delivers NAC based on modern cloud services built with Mist AI:



**Video:** [Juniper Mist Access Assurance: Cloud-Based Network Access Control](#)

## Features

- Microservices architecture that ensures high availability and scalability to support large deployments at a global level.
- Geo-affinity for automatic connections to access points and switches to the nearest authentication service port
- X.509 certificate management that maintains network trustworthiness with efficient digital certificate handling

- 802.1X and non-802.1X authentication to ensure versatile network security
- Network policy and microsegmentation facilitate targeted traffic control and threat containment.
- Integration with external directory services such as Google Workspace, Microsoft Entra ID (previously known as Microsoft Azure Active Directory), and Okta Identity
- Third-party support for compatibility with non-Juniper network infrastructure
- Marvis Virtual Network Assistant for AI-powered network insights, diagnostics, and troubleshooting

## Benefits

- User experience visibility—Visibility to user experience—Manage network operations—for example, monitor end-to-end user connections and troubleshoot network issues—from a single dashboard.
- Single pane of glass for management and operations—Efficiently perform your day-to-day access assurance tasks on the Juniper Mist portal, which provides full-stack management capability in one dashboard for end-to-end visibility to operations.
- Seamless onboarding—Easily onboard wired and wireless devices by using 802.1X or MAB validation methods.
- Simplified management—With our geographically distributed cloud authentication service, you can remove dependency on standalone authentication, authorization, and accounting (AAA) servers. This service automates updates to latest software patches without service downtime.
- Unified policy—Easily create authentication policies for both wired and wireless clients, replacing traditional complex AAA configurations.

## RELATED DOCUMENTATION

---

[Juniper Mist NAC Architecture | 4](#)

---

[Juniper Mist Access Assurance Use Cases | 6](#)

---

[Juniper Mist Access Assurance Best Practices | 14](#)

---

[Juniper Mist Access Assurance Authentication Methods | 8](#)

---

[Mist Access Assurance—Frequently Asked Questions | 16](#)

# Juniper Mist NAC Architecture

Juniper Mist Access Assurance leverages a microservices architecture. This architecture prioritizes uptime, redundancy, and automatic scaling, enabling an optimized network connection across wired, wireless, and wide area networks.

Watch the following video for Mist Access Assurance architecture:

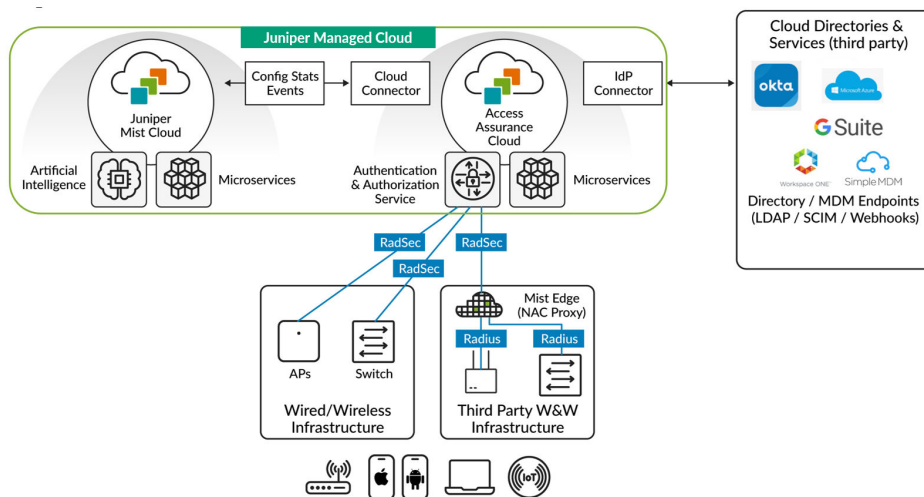


**Video:** [Mist Access Assurance Architecture 1](#)

Juniper Mist Access Assurance enhances its authentication service by incorporating external directory services such as Google Workspace, Microsoft Entra ID, Okta Identity and mobile device management (MDM) providers, such as Jamf and Microsoft Intune. This integration helps in accurately identifying users and devices, and enhances security measures by granting network access to only verified, trusted identities.

Figure 1 on page 4 shows the framework of Mist Access Assurance network access control (NAC).

**Figure 1: Juniper Mist Access Assurance Architecture**



The Juniper Mist authentication service, decoupled from the Juniper Mist cloud, acts as a standalone cloud service. The authentication and authorization service is distributed globally across various points of presence for enhanced performance and reliability.

This Juniper Mist authentication service uses a microservices approach. That is, a dedicated group or pool of microservices manages the functions of each of the service components, such as policy enforcement or user device authentication. Similarly, individual microservices manage each of the

additional tasks, such as session management, endpoint database maintenance, and connectivity to the Juniper Mist cloud.

Devices managed by the Juniper Mist cloud, such as Juniper® Series of High-Performance Access Points or Juniper Networks® EX Series Switches, send authentication requests to the Juniper Mist Authentication Service. These requests are automatically encrypted using RADIUS over TLS (RadSec) and sent through a secure Transport Layer Security (TLS) tunnel to the Authentication Service.

The Mist Authentication Service processes these requests and then connects to external directory services (Google Workspace, Microsoft Azure AD, Okta Identity, and others) and PKI and MDM providers (Jamf, Microsoft Intune, and others). The purpose of this connection is to further authenticate and provide context about the devices and users trying to connect the network.

In addition to the authentication tasks, the Juniper Mist Authentication Service relays back key metadata, session information, and analytics to the Juniper Mist cloud. This data sharing offers users end-to-end visibility and centralized management.

We use a Juniper Mist Edge platform as an authentication proxy to integrate a third-party network infrastructure with Juniper Mist Access Assurance. The third-party infrastructure interacts with the Juniper Mist Edge platform through RADIUS. The Juniper Mist Edge platform, in turn, uses RadSec to secure the communication and then proceeds with authentication.

This cloud-native microservices architecture enhances authentication and authorization services and supports regular feature updates and necessary security patches with minimal network downtime.

Watch the following video for Mist Access Assurance high-availability architecture:



**Video:** [Mist Access Assurance Architecture 2](#)

---

Watch the following video for Mist Access Assurance workflow:



**Video:** [Introduction to Mist Access Assurance](#)

---

Watch the following video for information about scaling Mist Access Assurance architecture:



**Video:** [Scaling NAC in Production](#)

---

Watch the following video for an overview of micro-services based architecture:



**Video:** [What Should NAC Look Like](#)

---

## RELATED DOCUMENTATION

[Juniper Mist Access Assurance Overview | 2](#)

[Juniper Mist Access Assurance Use Cases | 6](#)

[Juniper Mist Access Assurance Best Practices | 14](#)

[Juniper Mist Access Assurance Authentication Methods | 8](#)

[Mist Access Assurance—Frequently Asked Questions | 16](#)

# Juniper Mist Access Assurance Use Cases

Juniper Mist Access Assurance supports several uses cases including:

**Table 1: Access Assurance Use Cases**

Use Cases	Examples	Types of Access	Access Management Features
Managed devices	Corporate-owned user devices such as mobile devices, PCs, laptops, wireless access points and other devices.	Corporate network and public Internet	Access management through policy enforcement on devices and users of corporate networks
Guest devices	Visitors such as vendors, partners, customers, and sponsored guest devices	Public Internet and limited intranet	Self-registration through captive portal and sponsor-controlled access  Limited access to a selected area of the network to ensure appropriate network segmentation and to restrict network access to internal resources

**Table 1: Access Assurance Use Cases (Continued)**

Use Cases	Examples	Types of Access	Access Management Features
Unattended devices (Internet of Things (IoT))	IoT and Machine-to-Machine (M2M) devices deployed in corporate environments	Very limited intranet access	Access policy based on discovered or profiled device category  Network segmentation and restriction of network access to internal resources
BYOD	Employees who use their own devices such as smartphones, tablets, or laptops or use company devices from remote locations	Job-related company resources and the public Internet	Self-provisioning portal for the end user to get personal preshared key (PSK) through single sign-on (SSO)

**RELATED DOCUMENTATION**


---

[Juniper Mist Access Assurance Overview | 2](#)


---

[Juniper Mist NAC Architecture | 4](#)


---

[Juniper Mist Access Assurance Best Practices | 14](#)


---

[Juniper Mist Access Assurance Authentication Methods | 8](#)


---

[Mist Access Assurance—Frequently Asked Questions | 16](#)

# Juniper Mist Access Assurance Authentication Methods

## IN THIS SECTION

- [Certificate-Based Authentication and Credential-Based Authentication | 8](#)
- [802.1X Authentication Methods | 9](#)

IEEE 802.1X is a standard for port-based network access control. It provides a mechanism for authenticating devices that connect to a LAN or WLAN through a switch or access point. Juniper Mist Access Assurance supports both 802.1X authentication and non-802.1X authentication, that is MAC Authentication Bypass (MAB), for uniform access control across wired and wireless networks.

We support the following methods for secure access with 802.1X:

- Extensible Authentication Protocol–Transport Layer Security (EAP-TLS) (digital certificate-based)
- EAP-TTLS/PAP (Tunneled Transport Layer Security) (credential-based)

We support the following non-802.1X authentication methods:

- MAC Authentication Bypass (MAB)
- Multi Pre-Shared Key (MPSK)

## Certificate-Based Authentication and Credential-Based Authentication

### IN THIS SECTION

- [Certificate-Based Authentication | 9](#)
- [Password-Based Authentication | 9](#)

802.1X authentication method supports credential-based (user name and password) and certificate-based authentication.

## Certificate-Based Authentication

- Certificate-based authentication enables mutual authentication between server and client devices and implements cryptography to provide secure network access.
- Digital certificates use a public key infrastructure (PKI) that requires a private-public key pair.
- An identity provider (IdP) is optional in certificate-based authentication. You can use an IdP to check user or device information such as account state and group information.
- Certificates are stored in secured storage.
- Certificate-based authentication requires client device provisioning, for which you typically use mobile device management (MDM).

Juniper Mist Access Assurance can integrate with any existing PKI and cloud-based IdPs such as Microsoft Azure AD, Okta, or Google Workspace to ensure certificate-based authentication is implemented in all applicable use cases.

## Password-Based Authentication

- Password-based authentication requires an IdP for authentication. As most IdPs enforce multi-factor authentication (MFA), password-based authentication becomes impractical in 802.1X environments, particularly in wireless networks.
- The risk of person-in-the-middle attacks is significant, as 802.1X does not manage MFA well, especially on a wireless network.

We recommend password-based authentication only for scenarios where a PKI deployment is not immediately feasible or during transitions to certificate-based authentication. Avoid password-based 802.1X authentication in networks that support BYOD because of potential MITM attack vectors.

## 802.1X Authentication Methods

### IN THIS SECTION

- EAP-TLS | 10



The 802.1X protocol is an IEEE standard for port-based network access control (NAC) on both wired and wireless access points. The primary function of 802.1X is to define authentication controls for any user or device that attempts to access a LAN or WLAN protecting Ethernet LANs from unauthorized user access. Additionally, 802.1X blocks all traffic to and from a supplicant (client) at the interface until the supplicant presents its credentials and the authentication server (a RADIUS server) validates them.

The basic 802.1X authentication mechanism consists of three components:

- Supplicant—Client devices with authentication software. The client device seeks access to the network. This device could be a desktop or laptop computer, a tablet, a phone, and so on.
- Authenticator—The initial gateway, typically a switch or an access point (AP) that intercepts the supplicant's access request.
- Authentication Server—Compares the supplicant's ID with the credentials stored in a database. If the credentials and the supplicant ID match, the supplicant gets to access the network.

Let's understand how Juniper Mist Access Assurance uses each of the 802.1X authentication methods. See "[Juniper Mist Access Assurance Use Cases](#)" on page 6.

## EAP-TLS

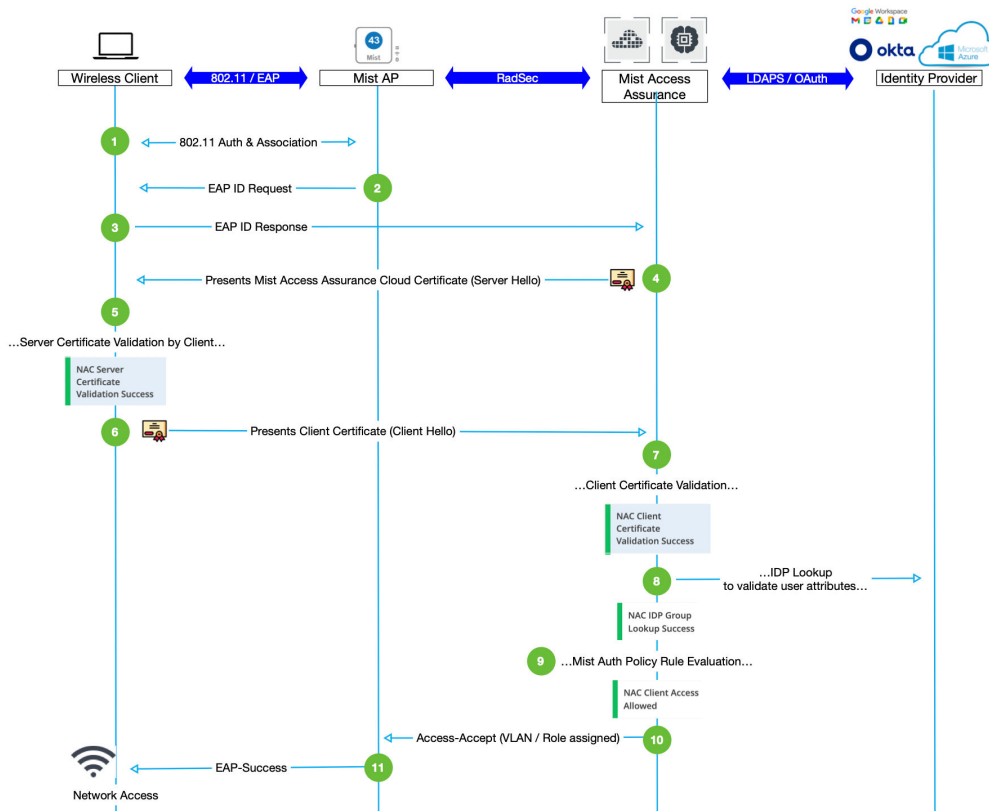
EAP-TLS leverages certificates and cryptography to provide mutual authentication between the client and the server. Both the client and the server must receive a digital certificate signed by a certificate authority (CA) that both the entities trust. This method uses certificates on both the client and server sides for authentication. For this authentication, the client and the server must trust each other's certificate.

### Features

- Uses TLS to provide secure identity transaction
- An open IETF standard that is universally supported
- Uses X.509 certificates for authentication

Figure 1 shows the EAP-TLS authentication sequence.

Figure 2: 802.1X EAP-TLS Authentication Sequence (Certificate-Based Method)



The 802.1X standard specifies EAP as the encryption format for data transmission between a supplicant and an authenticator.

This method performs a four-way handshake with the following steps:

1. Either the authenticator (for example an AP) initiates a session request or the supplicant (a wireless client device) sends a session initiation request to the authenticator.
2. The authenticator sends an EAP request to the supplicant asking for the supplicant's identity.
3. The supplicant sends an EAP response to the authentication server (Juniper Mist Access Assurance cloud) through the authenticator.
4. The authentication server responds to the client device with a "Server Hello" message that includes a certificate.
5. The supplicant validates the server certificate. That is, the supplicant verifies whether the server certificate is signed by a trusted CA.
6. The supplicant sends a "Client Hello" message through the authenticator to present the client certificate to the Juniper Mist Access Assurance service

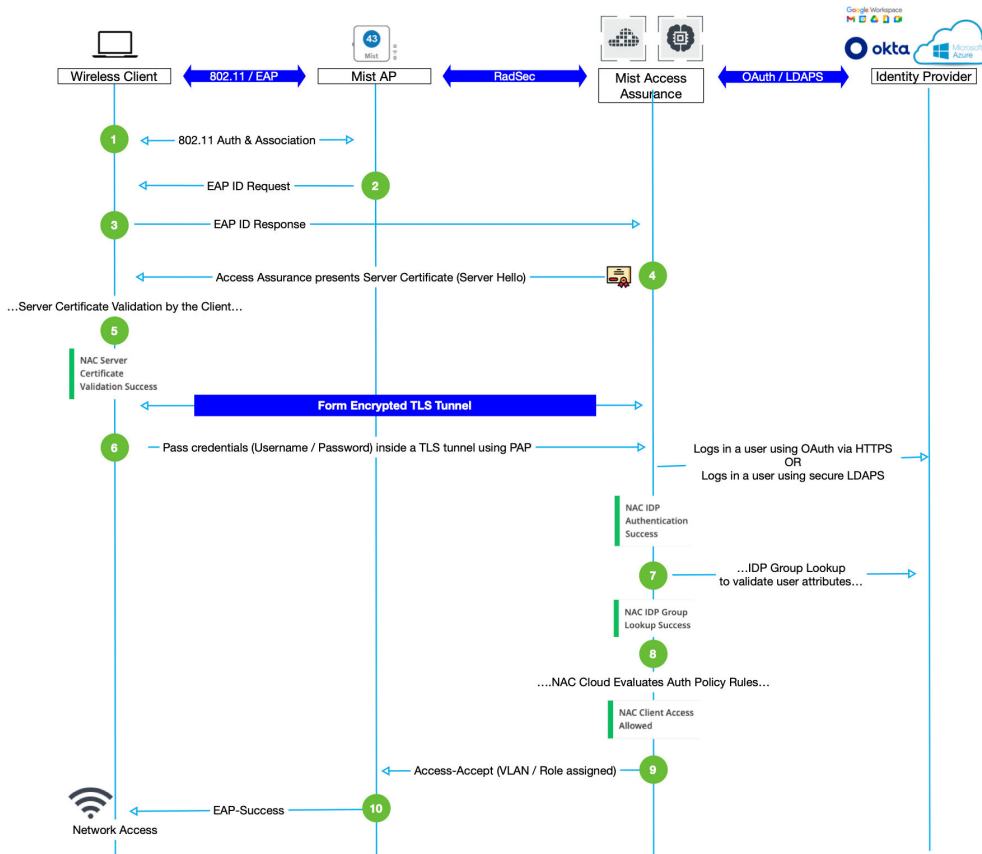
7. Juniper Mist Access Assurance validates that the client certificate is signed by a trusted CA.
8. Juniper Mist Access Assurance looks up the configured identity provider (IdP) sources and connects to an IdP to verify the user's name and some basic attributes.
9. Juniper Mist Access Assurance performs policy lookup and applies role and permission-based access to the client device.
10. Juniper Mist Access Assurance sends information about the VLAN and the assigned role to the authenticator so that it can assign the supplicant to the right network.
11. The authenticator sends an EAP-success message and provides access to the supplicant.

### **Extensible Authentication Protocol–Tunneled TLS (EAP-TTLS/PAP)**

EAP-TTLS-PAP uses user credentials, such as username and password on the client side and server certificate on the server side to perform authentication. When a client device establishes a secure TLS tunnel with authentication server, it passes credentials using PAP protocol inside an encrypted tunnel.

Figure 2 shows the EAP-TTLS/PAP authentication sequence.

Figure 3: 802.1X EAP-TTLS/PAP Authentication Sequence (Credential-Based Method)



EAP-TTLS/PAP authentication involves the following steps:

1. Either the authenticator (for example an AP) initiates a session request or the supplicant (a wireless client device) sends a session initiation request to the authenticator.
2. The authenticator sends an EAP request asking for identification information to the supplicant.
3. A supplicant sends an EAP response to the authentication server (example: Juniper Mist Access Assurance cloud).
4. The authentication server responds to the client device with a "Server Hello" message that includes a certificate. The server sends the message through the authenticator.
5. The supplicant validates the server certificate. That is, the supplicant verifies whether the server certificate is signed by a trusted CA. This validation sets up an encrypted TLS tunnel.
6. The supplicant sends account credentials, such as user name and password, through a TLS tunnel to the server. The supplicant encrypts the information with Lightweight Directory Access Protocol over SSL (LDAPS) or OAuth (HTTPS).

7. Juniper Mist Access Assurance performs a lookup against its configured identity provider sources to find the user's name along with some basic attributes.
8. Juniper Mist Access Assurance performs policy lookup and applies role and permission-based access to the client device.
9. Juniper Mist Access Assurance sends information about the VLAN and the assigned role to the authenticator so that it can assign the supplicant to the right network.
10. The authenticator sends an EAP-success message and provides access to the supplicant.

#### SEE ALSO

---

[Juniper Mist Access Assurance Overview | 2](#)

---

[Juniper Mist NAC Architecture | 4](#)

---

[Juniper Mist Access Assurance Use Cases | 6](#)

---

[Juniper Mist Access Assurance Best Practices | 14](#)

---

[Mist Access Assurance—Frequently Asked Questions | 16](#)

## Juniper Mist Access Assurance Best Practices

Here's a list of some network access control (NAC) best practices, which you can implement with Juniper Mist Access Assurance:

- **Use 802.1X framework:** A standard for NAC and is supported across most client devices. As a best practice, we recommend that you onboard corporate devices that support 802.1X authentication. Note: You can also perform MAC-less onboarding of non-802.1X devices that connect through IoT or BYOD.
- **Use credential-based authentication with identity provider:** Users connect to the network by using their username and password. An identity provider (IdP) must verify the credentials and the user account.
- **Use Certificate-based authentication:** This method uses the digital certificates installed on client devices for authentication. These certificates can be assigned either to a device or to a user profile.
- **Move to cloud-based IdPs:** Cloud-based identity providers such as Microsoft Azure Active Directory, Okta, Ping Identity, or Google Workspace are becoming more common and offer various advantages.

- Use of Public Key Infrastructure (PKI): Use public key infrastructure (PKI): Use PKI to create, store, distribute, and revoke digital certificates.
- Provision devices: Configure Juniper Mist Access Assurance to provision devices at scale. Typically, you use mobile device management (MDM) platforms in enterprise environments for device provisioning.
- Use an automated NAC solution: An automated NAC solution can provide visibility, control, and automated response for every device connected to a . This solution also provides secure network access by enforcing policies across all devices and users.
- Use multi-factor authentication: Provide an additional layer of security by using more than one form of authentication for network access
- Perform network segmentation: Network segmentation can help prevent the spread of malware and limit the impact of security breaches.
- Implement a guest access policy: Provide different types of access to different users based on the requirements. A guest access policy can help control access to the network by visitors and contractors.

Watch the following video for access control best practices:



Video: [Mist Access Assurance Best Practices](#)



**NOTE:** The choice between credential-based and certificate-based authentication depends on your specific requirements and the level of security needed. Note that certificate-based authentication is currently considered the most secure method.

## RELATED DOCUMENTATION

[Juniper Mist NAC Architecture](#) | 4

[Juniper Mist Access Assurance Use Cases](#) | 6

[Juniper Mist Access Assurance Authentication Methods](#) | 8

[Mist Access Assurance—Frequently Asked Questions](#) | 16

# Mist Access Assurance—Frequently Asked Questions

## What is Mist Access Assurance?

Juniper Mist Access Assurance is a cloud service that provides secure, identity-based network access control (NAC). The cloud service offers a comprehensive policy framework to allow or deny network access to various devices such as guests, corporate devices, and devices generating IoT and BYOD traffic. User and device identity determine whether a client receives access. Juniper Mist Access Assurance supports 802.1X authentication and MAC address bypass for non-802.1X wired IoT devices in the allowlist.

## How do you order Mist Access Assurance subscriptions?

We provide the Juniper Mist Access Assurance service as a subscription based on the average concurrently active client devices seen over a 7-day period.

**Table 2: Mist Access Assurance Subscriptions Package**

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

For information about license numbering and license pools, see [Licensing Information](#).

Your subscription to IoT Assurance also grants you access to Juniper Mist Access Assurance.

Contact your Juniper account team or partner to obtain a license. For more information, visit: <https://www.juniper.net/us/en/how-to-buy/form.html>.

Refer to [Juniper Mist Access Assurance Datasheet](#) for details.

## We have a Juniper Mist wired and wireless infrastructure. Do we need to purchase any additional hardware to enable Access Assurance?

You don't need any additional hardware to install and maintain Juniper Mist Access Assurance.

Juniper Mist Access Assurance supports:

- Juniper Networks EX Series switches with
  - Junos OS Release 20.4R3-S7 or later
  - Junos OS Release 22.3R3 or later
  - Junos OS Release 22.4R2 or later
  - Junos OS Release 23.1R1 or later
- Juniper® Series of High-Performance Access Points with firmware version 0.6.x or above.

### **What are Juniper Mist Access Assurance – Source IP Addresses?**

Juniper Mist Access Assurance is geographically distributed cloud authentication service. In some cases users require to create allow list using for Access Assurance source IP addresses to communicate with external Identity Providers.

Juniper Networks recommends to leverage Layer 7 based verification instead of IP-based firewall rules. For example, to validate client certificates for LDAPS communication or validate OAuth client id/secrets.

#### **US West**

- 44.238.214.57
- 54.214.208.109
- 54.71.176.201

#### **US East**

- 13.58.92.194
- 18.217.23.193
- 3.22.40.111

#### **EU Paris**

- 15.236.172.79
- 15.236.44.93
- 15.237.171.133

#### **EU Frankfurt**

- 3.77.68.168



- 52.57.243.242
- 18.153.242.220

#### **APAC Sydney**

- 54.255.158.51
- 18.143.121.8
- 13.228.196.58

#### **APAC Singapore**

- 13.239.90.65
- 13.237.26.230
- 54.252.79.22

### **Do I need to add any firewall rules to configure my access points and switches to use Mist Access Assurance?**

Yes, on your firewall you must allow outbound connections destined to *radsec.nac.mist.com* over TCP Port 2083.

### **Why is the Access Assurance option missing in the Juniper Mist UI?**

Juniper Mist Access Assurance has limited availability. Contact your Juniper Mist representative if you want to use this feature or need any additional details about the feature

### **What happens if I lose connectivity to the Juniper Mist cloud?**

The Juniper Mist Access Assurance service has a microservices architecture, which makes the service very resilient. In the rare event of persistent loss of connectivity to the Juniper Mist cloud, all authenticated and authorized client devices will maintain their functionality and roam seamlessly.

### **Which authentication methods do you support with Mist Access Assurance?**

Juniper Mist Access Assurance supports the following authentication methods:

- 802.1X
  - Extensible Authentication Protocol (EAP)–Transport Layer Security (TLS)/Protected Extensible Authentication Protocol (PEAP)–Transport Layer Security (TLS)–Certificate-based authentication.

In addition to certificate validation, you can optionally use an identity provider for additional authorization context.

- Extensible Authentication Protocol–Tunneled TLS (EAP-TTLS)—Credential-based authentication. Require Identity Provider such as Azure AD, Okta, and Google Workspace.
- **Non-802.1X**
  - MAC Authentication Bypass (MAB)—You can use MAB for devices that don't support 802.1X authentication methods, such as wired IoT devices.

See "[Juniper Mist Access Assurance Authentication Methods](#)" on page 8 for details.

### **Do we experience any latency when we use Juniper Mist Access Assurance?**

Juniper Mist Access Assurance has a microservices architecture with geo-affinity features. The service can connect to the nearest service, reducing delay and making it as fast as systems located on your premises. We suggest that you use the cloud service on a trial basis to experience an improvement in your user experience.

### **Have you made any changes to PSK-based IoT onboarding?**

Preshared Key (PSK)-based IoT device onboarding continues to work the same way as before. Refer to [Multi PSK – Mist IoT Assurance](#) for details.

## **RELATED DOCUMENTATION**

---

[Juniper Mist NAC Architecture | 4](#)

---

[Juniper Mist Access Assurance Use Cases | 6](#)

---

[Juniper Mist Access Assurance Best Practices | 14](#)

---

[Juniper Mist Access Assurance Authentication Methods | 8](#)

# 2

CHAPTER

## Identity Provider Integration

---

### SUMMARY

Use the information in this chapter to integrate with various Identity Providers (IdPs) to enhance authentication and access control in Juniper Mist portal.

### IN THIS CHAPTER

- Integrate Okta as an Identity Provider | **22**
  - Integrate Google Workspace as an Identity Provider | **27**
  - Integrate Microsoft Entra ID as an Identity Provider | **33**
  - Integrate with Microsoft Intune | **40**
  - JAMF Pro Integration | **45**
  - Use Case: Mist Edge Proxy for Eduroam | **51**
  - Add Identity Providers for Juniper Mist Access Assurance | **56**
-

# What Do You Want to Do?

Table 3: Top Tasks

If you want to...	Use these resources:
<p><b>Add Microsoft Entra ID (formerly known as Azure Active Directory) as IdP</b>  <i>Integrate Microsoft Entra ID to validate user attributes before enforcing role-based access policies.</i></p>	<p><a href="#">"Integrate Microsoft Entra ID as an Identity Provider" on page 33</a></p>
<p><b>Set up Okta as an identity provider</b>  <i>Configure Okta Workforce Identity Cloud through the Juniper Mist dashboard to authenticate end users attempting to access the network.</i></p>	<p><a href="#">"Integrate Okta as an Identity Provider" on page 22</a></p>
<p><b>Add Google Workspace as IdP</b>  <i>Integrate with Google Workspace IdP to leverage secure Lightweight Directory Access Protocol for user/group account provisioning.</i></p>	<p><a href="#">"Integrate Google Workspace as an Identity Provider" on page 27</a></p>
<p><b>Configure identity providers</b>  <i>Integrate Juniper Mist cloud with an external identity provider and enable your organization to use a SAML identity provider or you can configure an LDAP server connection.</i></p>	<p><a href="#">"Add Identity Providers for Juniper Mist Access Assurance" on page 56</a></p>

## RELATED DOCUMENTATION

[Juniper Mist NAC Architecture | 4](#)

[Juniper Mist Access Assurance Use Cases | 6](#)

[Juniper Mist Access Assurance Best Practices | 14](#)

[Juniper Mist Access Assurance Authentication Methods | 8](#)

[Mist Access Assurance—Frequently Asked Questions | 16](#)

# Integrate Okta as an Identity Provider

## IN THIS SECTION

- [OKTA Resource Owner Password Credential App Integration | 23](#)
- [Okta Client Credential App Integration | 24](#)
- [Configuration on Juniper Mist Dashboard | 24](#)

You can use Okta Workforce Identity Cloud through the Juniper Mist dashboard to authenticate end users attempting to access the network. Juniper Mist Access Assurance uses Okta as an identity provider (IdP) to perform various authentication tasks.:

- For credential-based (EAP-TTLS) authentication, Okta:
  - Performs delegated authentication, that is, checks username and password by using OAuth.
  - Retrieves user group membership information to support authentication policies based on this user identity.
  - Gets the status—active or suspended—of an user account
- For certificate-based (EAP-TLS or EAP-TTLS ) authorization, Okta:
  - Retrieves user group membership information to support authentication policies based on this user identity
  - Gets the status—active or suspended—of an user account

## Prerequisites

- Create a subscription for Okta and get your tenant ID. During subscription creation, you specify a tenant that is used to create a URL to access the Okta dashboard. You can find your ID at the top-right corner of the Okta dashboard. Note that the tenant ID must not include okta.com.



**NOTE:** Your Okta login URL has the following format:

`https://{your-okta-account-id}-admin.okta.com/admin/getting-started`

Replace {your-okta-account-id} with your Okta account ID.

- You must have super user permission on the Juniper Mist portal.

## OKTA Resource Owner Password Credential App Integration

1. Log in to the Okta administration console and select **Applications > Applications**.
2. Click **Create App Integration**.  
The Create a new app integration page opens.
3. Under Sign-in method, select **OIDC-OpenID Connect** and under Application Type, select **Native Application**.
4. On the New Native App Integration page, select:
  - **App integration name**—Enter a name that you resonate with.
  - **Grant Type**—Select **Resource Owner Password**.
  - **Controlled Access**—Select **Allow everyone in your organization to access**. In this example, we are granting everyone access to the application.
5. Click **Save**.  
After the system is saved as a new app integration, the application reloads with the General tab selected.
6. On the General tab, click **Edit** and select following options:
  - Client Authentication—Select **Client Secret**
  - Proof Key for Code Exchange—Select **Require PKCE as Additional Verification**
7. Click **Save** to continue.  
Okta generates the client ID and the client secret after this step.  
Note the client ID and client secret. You'll need this information later.
8. Go to the **Okta API Scopes** tab and select the following check boxes to grant read permissions:
  - okta.roles.read
  - okta.users.read
  - okta.users.read

Now, go to the Juniper Mist cloud portal and start integrating Okta as an IdP.

## Okta Client Credential App Integration

1. Log in to the Okta administration console and select **Applications > Applications**.
2. Click **Create App Integration**.  
The Create a new app integration page opens.
3. Under Sign-in method, select **API Services**.  
The New API Services App Integration page opens.
4. Enter a name for **App integration name** and then click **Save**.
5. Go to the General tab in the new app integration page and click **Edit**.
6. Click **Edit** and select the client authentication method as **Public key / Private key** and then click **Add Key** in the **PUBLIC KEYS** section.
7. Select the file format as **PEM** in the Private Key section, then copy the private key and save it in a safe place.  
In a safe place, save the private key file that Okta generates.  
You will not be able to retrieve this private key again.  
  
Click **Done**.
8. Click **Save** to store and activate the key.  
  
You can notice that the status of the key is now Active. Copy the Client ID and secret displayed on the screen,
9. Go to the **Okta API Scopes** tab and allow the following read permissions:
  - okta.roles.read
  - okta.users.read
  - okta.users.read

## Configuration on Juniper Mist Dashboard

1. On the Juniper Mist portal, click **Organization** and select **Identity Providers** under **Access**.  
The Identity Providers page opens displaying a list of configured identity providers (if any).
2. Click **Add IDP** to add a new identity provider.
3. On the **New Identity Provider** page, enter the following information:

< Identity Providers : **oauth-okta**

**Name**

oauth-okta

**Configuration**

IDP type

LDAPS  OAuth

OAuth Type

Okta

OAuth Tenant ID ⓘ

dev-90521981

Domain Names

juniper.net

Default IDP ⓘ

OAuth Client Credential (CC) Client Id ⓘ

0aa7af8uef1q29u4u75d7

OAuth Client Credential (CC) Client Private Key ⓘ

[View Private Key](#)

OAuth Resource Owner Password Credential (ROPC) Client Id ⓘ

0aa7max6a7m2cay35d7

OAuth Resource Owner Password Credential (ROPC) Client Secret ⓘ

..... [Reveal](#)

- a. Name—Enter an IdP name.
- b. IDP Type—Select an IdP type as **OAuth**.

**Table 4: Settings for Identity Provider Type OAuth**

Parameters	Description
OAuth Type	Select <b>Okta</b>
OAuth Tenant ID	Enter OAuth tenant ID. Use the ID you received during Okta application configuration.



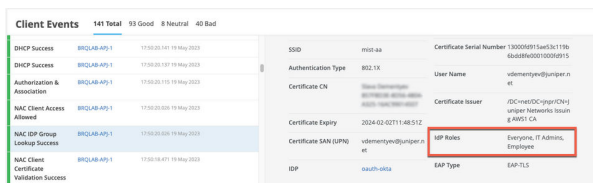
**Table 4: Settings for Identity Provider Type OAuth (Continued)**

Parameters	Description
Domain Names	Enter your Okta users domain name. Example: abc.com
Default IDP	Set the selected identity provider as default if user domain name is not specified.
OAuth Client Credential (CC) Client Id	Use the ID you received during Okta application configuration.  <a href="#">"Okta Client Credential App Integration" on page 24</a>
OAuth Client Credential (CC) Client Private Key	Enter the private key generated during Okta application configuration. See <a href="#">"Okta Client Credential App Integration" on page 24</a>
OAuth Resource Owner Password Credential (ROPC) Client Id	Enter the secret ID you received and stored during Okta application configuration.  See <a href="#">" OKTA Resource Owner Password Credential App Integration" on page 23.</a>
OAuth Resource Owner Password Credential (ROPC) Client Secret	Provide client secret value you received and stored during Okta application configuration.  See <a href="#">" OKTA Resource Owner Password Credential App Integration" on page 23</a>

4. Click **Create** to save the changes.

In Juniper Mist portal, go to **Monitoring > Insights > Client Events**.

When a user authenticates using EAP-TLS with Okta, you can see the event called **NAC IDP Group Lookup Success** as shown below:



In case of EAP-TTLS authentication, you can see the **NAC IDP Authentication Success** event. This event indicates that Azure AD has validated user credentials. You can also see the **NAC IDP Group Lookup Success** event that fetches user group memberships.

The screenshot displays a 'Client Events' window with a table of events. The 'NAC IDP Authentication Success' event is highlighted, showing details for a client with the user name 'valentyn@juniper.net'. The 'NAC IDP Group Lookup Success' event is also visible, indicating successful group membership retrieval.

Client	Client	AP	SSID	SSID	User Name
valentyn@juniper.net	valentyn@juniper.net	BHQAB-872	u877d958a7c1	mist-ss	valentyn@juniper.net
Authentication Type	802.1X				
Certificate Expiry	0001-01-01T00:00:00Z				

## SEE ALSO

[Add Identity Providers for Juniper Mist Access Assurance | 56](#)

[Integrate Microsoft Entra ID as an Identity Provider | 33](#)

[Integrate Google Workspace as an Identity Provider | 27](#)

# Integrate Google Workspace as an Identity Provider

## IN THIS SECTION

- [Configuration on Google Workspace | 28](#)
- [Configuration on Juniper Mist Dashboard | 29](#)
- [About EAP-TTLS and Azure AD using ROPC | 32](#)

Juniper Mist Access Assurance allows you to integrate with Google Workspace as Identity Provider (IdP) to leverage secure Lightweight Directory Access Protocol over SSL (LDAPS) connector for the following use cases:

- For certificate-based (EAP-TLS or EAP-TTLS) authorization:
  - Retrieves user group membership information to support authentication policies based on this user identity
  - Gets the status—active or suspended—of an user account
- EAP-TTLS with PAP

- Checks the username and password for authentication with Google's Identity Provider

## Configuration on Google Workspace

The following procedure shows you how to configure Google Workspace as an identity provider (IdP) with Juniper Mist.

1. Log in to your [Google Workspace](#) portal by using your Google administrator credentials.  
The Google Admin dashboard appears.
2. Create an LDAP client.
  - a. From the Google Admin console, on the left-navigation bar, go to **Apps > LDAP** and click **Add Client**.
  - b. Provide an **LDAP client name** and an optional **Description** and click **Continue**.  
The **Access permissions** page is displayed after adding the LDAP client.
3. Configure Access Permission for verifying user credentials.  
The following options are available:
  - **Verify user credentials**—Allows user credential authentication using EAP-TTLS/PAP. This setting specifies which organizational groups the LDAP client can access to verify the user's credentials.
  - **Read user Information**—Allows you to read basic user information. This setting specifies which organizational units and groups the LDAP client can access to retrieve additional user information.
  - a. Select **Entire domain** for both the options if no specific organization is required.
  - b. Scroll down to **Read group information**. This setting specifies whether the LDAP client can read group details and check a user's group memberships.  
After you finish configuring access permissions and added LDAP client, the certificate is generated automatically on the same page.
4. Download the generated LDAPS client certificate.
  - a. Click **Download certificate** and save the downloaded certificate in a secure place. You'll need this certificate when you set up an IdP on the Juniper Mist portal.
  - b. Click **Continue to Client Details**.  
The Settings for <LDAP client name> page appears.
  - c. Expand the **Authentication** section.
  - d. Under Access Credentials, click **Generate New Credentials**.  
You can view the username and password on the **Access credentials** page.

Copy and save the username and password. You need these details for the LDAPS client configuration on the Juniper Mist cloud portal.

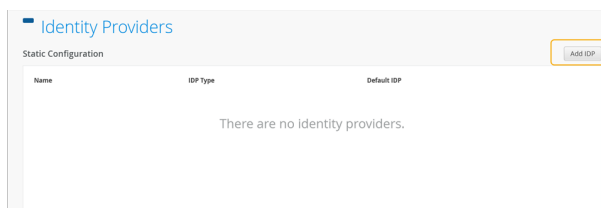
5. Enable the LDAP client service by changing the service status to **On** for the LDAP client. This step enables you to set up a client with the Secure LDAP service.
  - a. From the Google Admin console, go to **Apps > LDAP**. Select your client and click **Service Status**. The service status, displayed at the top right of the page, is initially set as **OFF**.

Select **On for everyone** to turn on the service. Allow some time for the changes to apply on the Google side.

## Configuration on Juniper Mist Dashboard

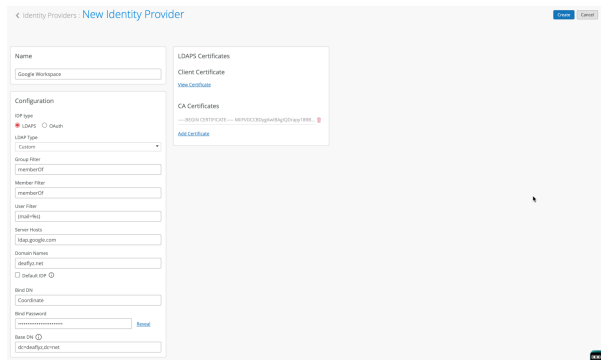
1. On the Juniper Mist portal, from the left menu select **Organization > Access > Identity Providers**. The Identity Providers page appears, displaying a list of configured IdPs (if any)

Figure 4: Identity Providers Page



2. Click **Add IDP** to add a new IdP.
3. On the **New Identity Provider** page, enter the required information to integrate with Google Workspace.

Figure 5: Update Identity Provider Details

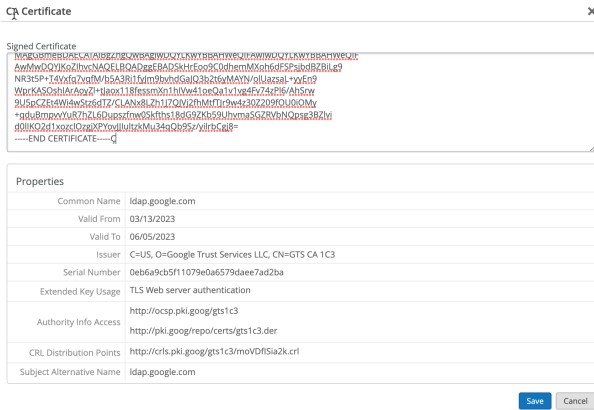


Now configure the LDAPS connector to integrate with the Google Workspace LDAP endpoint.

- **Name**—Enter an IdP name. (In this example, enter **Google Workspace**.)
- **IDP Type**—Select **LDAPS**.
- **LDAP Type**—Select **Custom**.
- **Group Filter**—Select **memberOf**. This option is required to obtain group memberships from *Group attribute*.
- **Member Filter**—Select **memberOf**.
- **User Filter**—Enter **(mail=%s)**.
- **Server Hosts**—Enter **ldap.google.com**.
- **Domain Names**—Enter your Google Workspace domain name. For example: **abc.com**.
- **Bind DN**—Use the username provided by Google in the previous step.
- **Bind Password**—Enter the password for the above username.
- **Base DN**—Configure your base dn matching your Google Workspace domain. For example, if your domain is abc.com, then your base DN is **dc=abc,dc=com**.

4. In the CA Certificates section, click **Add Certificate** and paste the following two certificates:

Figure 6: Add CA Certificate



```

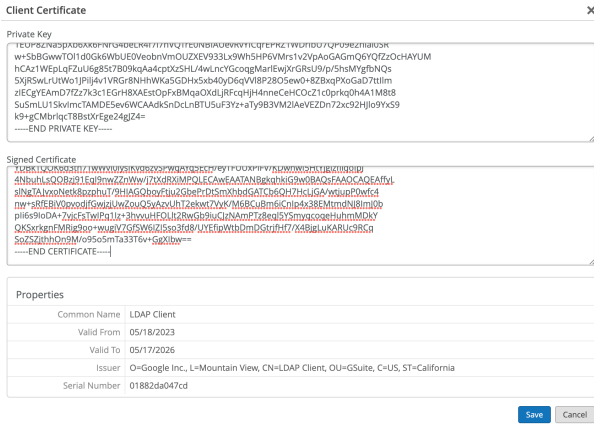
-----BEGIN CERTIFICATE-----
MIIFljCCA36gAwIBAgINAgO8U11rNMcY9QFQZjANBgkqhkiG9w0BAQsFADBHMQsw
CQYDVQQGEwJVZUeIMCAGA1UEChMZMR29vZ2x1IFRydXN0IFNlcnZpY2VzIEExMQZEU
MBIGA1UEAxMLR1RTIFJvb3QgUjJEWWhcNMjAwODEzMDAwMDQyWWhcNMjcwOTMwMDAw

```

```
tdufThcV4q508DIrGKZTqPwJNl
1IXNDw9bg1kWRxYtnCQ6yICmJhSFm/Y3m6xv+cXDB1Hz4n/FsRC6UfTd
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFjYCCBEqAwIBAgIQd70NbNs2+RrQIQ/E8FjTDTANBgkqhkiG9w0BAQsFADBX
+qduBmpvvYuR7hZL6Dupszfnw0Skfths18dG9ZKb59UhvmaSGZRVbNQpsg3BZ1vi
d0lIK02d1xozc10zgjXPYovJJIu1tzkMu34qQb9Sz/yilrbCgj8=
-----END CERTIFICATE-----
```

5. Under **Client Certificate**, add a client certificate you downloaded from Google. Place the file ending with **.key** under Private Key, and the file ending with **.crt** under Signed Certificate as shown in the following sample:

**Figure 7: Add Client Certificate**



Click **Save**.

On the Juniper Mist portal, go to **Monitoring > Insights > Client Events**.

When a user authenticates using EAP-TTLS , you can see the **NAC IDP Authentication Success** and **NAC IDP Group Lookup Success** events that fetch user group membership information.

When a user authenticates using EAP-TTS with Google Workspace, you can see the event **NAC IDP Group Lookup Success** that fetches user group membership information.

**Figure 8: IDP Group Lookup Success Authentication Event**

Client Events		74 Total	46 Good	12 Neutral	16 Bad
Authorization & Association	Google	14/10/2023 10:50:30			
NAC Client Access Allowed	Google	14/10/2023 10:50:30			
NAC IDP Group Lookup Success	Google	14/10/2023 10:50:30			
NAC IDP Authentication Success	Google	14/10/2023 10:50:30			
NAC Server Certificate Validation Success	Google	14/10/2023 10:50:30			

Client	Google	AP	BRQLAB-473-2
BSSID	a8f7d998a7d51	SSID	m501-aa
Authentication Type	802.1X	User Name	slava@deflyx.net
Certificate Expiry	0001-01-01T00:00:00Z	IDP Roles	admin, GroupAdmin, vip
EAP Type	EAP-TTLS	IDP	Google Workspace

In case of EAP-TTLS authentication, you can see the **NAC IDP Authentication Success** event. This event indicates that Google Workspace has validated user credentials.

**Figure 9: IDP Authentication Success Event**

Client Events		74 Total	46 Good	12 Neutral	16 Bad
Authorization & Association	Google	14/10/2023 10:50:30			
NAC Client Access Allowed	Google	14/10/2023 10:50:30			
NAC IDP Group Lookup Success	Google	14/10/2023 10:50:30			
NAC IDP Authentication Success	Google	14/10/2023 10:50:30			
NAC Server Certificate Validation Success	Google	14/10/2023 10:50:30			

Client	Google	AP	BRQLAB-473-2
BSSID	a8f7d998a7d51	SSID	m501-aa
Authentication Type	802.1X	User Name	slava@deflyx.net
Certificate Expiry	0001-01-01T00:00:00Z		

You may leverage IDP Roles from Google Workspace in your Auth policy rules to perform network segmentation based on user roles.

## About EAP-TTLS and Azure AD using ROPC

Extensible Authentication Protocol–Tunneled TLS (EAP-TTLS) leverages LDAPS OAuth flow with Azure AD to perform user authentication. This implies the use of legacy authentication, which involves the use of a username and password without MFA. There are several factors to consider when employing this method:

- Configure client devices with the correct Wi-Fi profile, either from GPO or MDM. Providing only username and password at the login prompt does not work for some operating systems.
- Users must use Google Email ID (username@domain) username format for entering the username.
- Configure clients to trust server certificate. See "[Use Digital Certificates](#)" on page 64.

### SEE ALSO

[Add Identity Providers for Juniper Mist Access Assurance](#) | 56

[Integrate Microsoft Entra ID as an Identity Provider](#) | 33

[Integrate Okta as an Identity Provider](#) | 22

# Integrate Microsoft Entra ID as an Identity Provider

## IN THIS SECTION

- [Configuration in Entra ID Portal | 34](#)
- [Configuration on Juniper Mist Dashboard | 35](#)
- [EAP-TTLS Authentication with Azure AD and ROPC | 37](#)

Microsoft Azure Active Directory (Azure AD), now known as Microsoft Entra ID, is an identity and access management solution. With Juniper Mist Access Assurance, you can integrate an authentication service into Entra ID by using OAuth to perform:

- **User authentication with Extensible Authentication Protocol–Tunneled TLS (EAP-TTLS)**
  - Performs delegated authentication, that is, checks username and password by using OAuth.
  - Retrieves user group membership information to support authentication policies that are based on this user identity.
  - Gets the status—active or suspended—of an user account.
- **User Authorization with Extensible Authentication Protocol–Transport Layer Security (EAP-TLS) and EAP-TTLS**
  - Retrieves user group membership information to support authentication policies that are based on this user identity.
  - Gets the status—active or suspended—of an user account
- **EAP-TTLS with Password Authentication Protocol (PAP)**
  - Performs delegated authentication, that is, checks username and password by using OAuth or Resource Owner Password Credentials (ROPC).
  - Retrieves user group membership information to support authentication policies that are based on this user identity.
  - Gets the status—active or suspended—of an user account



## Configuration in Entra ID Portal

To integrate Entra ID with Juniper Mist Access Assurance, you need the Client ID, Client Secret, and Tenant ID, which are values that the Entra ID portal generates.

1. Use your credentials to sign in to the [Azure portal](#) and navigate to your AD.
2. In Microsoft Entra admin center, from the left-navigation bar, select **App registrations**.
3. Click **New Registration**.
4. On the New Registration page, enter the required information in the following fields. Note that the following list displays sample user input and sample settings.
  - **Name**—Mist AA IDP connector
  - **Supported Account Type**—Select **Accounts in this organizational directory only (Default Directory only - Single tenant)**.
5. Click **Register** to continue.  
The registered application page appears displaying information about the newly created connector.
6. Note down the following details:
  - **Application (Client) ID**—You'll need to enter this information in the **OAuth Client Credential (CC) Client ID** and **Resource Owner Password Credential Client ID** fields on the Juniper Mist cloud portal.
  - **Directory (Tenant) ID**—You'll need this information for the **OAuth Tenant ID** field on the Juniper Mist portal.

You will need to set up an identity provider (IdP) connector on the Juniper Mist portal:

7. Click **Add a certificate or secret** on the same page.
8. In the Clients and secrets page, click **New client secret**.  
The Add a client secret window appears.
9. Enter the required information in the following fields and click **Add**.
  - **Description**—Provide description for the client secret.
  - **Expires**—Select expiry period for the secret.

The system generates **Value** and **Secret ID**.

Copy and save the information in the **Value** field in a safe location. Note that you'll see this field only once. That is, right after the secret ID is created.

You will need this information for the **OAuth Client Credentials Client Secret** field on the Juniper Mist portal when you add Azure AD as an IdP.

10. Select **Authentication** in the left-navigation bar and scroll-down to the **Advanced Settings** section. Select **Yes** for **Allow public client flows**.

11. Select **API permissions** in the left-navigation bar.

Under **Microsoft Graph**, add the following permissions:

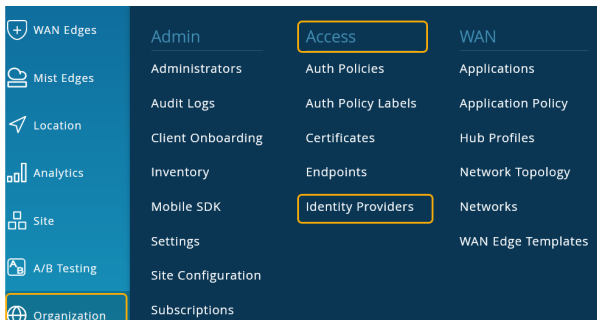
- **User.Read—Delegated**
- **User.Read.All—Application**
- **Group.Read.All—Application**
- **Device.Read.All—Application**

Click Grant admin consent.

You must give your application the required access permissions to use Microsoft Graph API to fetch information about users.

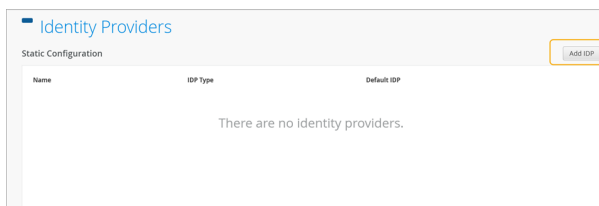
## Configuration on Juniper Mist Dashboard

1. On the Juniper Mist portal, from the left menu, select **Organization > Access > Identity Providers**.



The Identity Providers page appears, displaying a list of configured IdPs (if any).

**Figure 10: Identity Providers Page**



2. Click **Add IDP** to add a new IdP.

3. On the **New Identity Provider** page, enter the required information as shown below.

**Figure 11: Add Azure AD as Identity Provider**

The screenshot shows the 'New Identity Provider' configuration page in the Juniper Mist portal. The page is titled 'Identity Providers: New Identity Provider' and has 'Done' and 'Cancel' buttons in the top right. The configuration fields are as follows:

- Name:** Azure AD
- Configuration:**
  - OAuth:  OAuth
  - OAuth Type: Azure
  - OAuth Tenant ID: 00000000-0000-0000-0000-000000000000
  - Domain Names: juniper.com
- Default IDP:**  Default IDP
- OAuth Client Credential (CC) Client id:** 00000000-0000-0000-0000-000000000000
- OAuth Client Credential (CC) Client secret:** [Redacted]
- OAuth Resource Owner Password Credential (ROPC) Client id:** 00000000-0000-0000-0000-000000000000

- a. **Name**—Enter an IdP name (For this example: Azure AD).
- b. **IDP Type**—Select **OAuth**.
- c. **OAuth Type**—Select **Azure** from the drop-down list.
- d. **OAuth Tenant ID**—Enter the directory (tenant) ID that you copied from the Azure AD application.
- e. **Domain Names**—Enter the domain name, that is, the user's username (For example: username@domain.com). The domain name field examines incoming authentication requests, identifying the respective username and associated domain. A connector uses the domain name that you set up to identify the Azure tenant the connector needs to communicate with.
- f. **Default IDP**—Check this option to get machine group memberships.
- g. **OAuth Client Credential (CC) Client id**—Enter the application (client) ID of the registered application in Microsoft Entra admin center.
- h. **OAuth Client Credential (CC) Client secret**—Enter the application secret that you created earlier on the Azure portal.
- i. **OAuth Resource Owner Password Credential (ROPC) Client id**—Enter the application (client) ID of the registered Azure AD application.

On the Juniper Mist portal, go to **Monitoring > Insights > Client Events**.

When Juniper Mist Access Assurance authenticates a user by using EAP-TLS with Azure AD, you can see the **NAC IDP Group Lookup Success** event as shown below:

Figure 12: Success Message for EAP-TLS Authentication by IDP

Client Events	90 Total	50 Good	17 Neutral	23 Bad
Gateway ARP Success	MiscAA:TestAP	1/23/2020 10:11 PM	MiscAA:TestAP	
Authentication & Association	MiscAA:TestAP	1/23/2020 10:16 PM	MiscAA:TestAP	
NAC IDP Group Lookup Success	MiscAA:TestAP	1/23/2020 10:17 PM	MiscAA:TestAP	
NAC Client Access Allowed	MiscAA:TestAP	1/23/2020 10:17 PM	MiscAA:TestAP	
NAC IDP Authentication Success	MiscAA:TestAP	1/23/2020 10:17 PM	MiscAA:TestAP	
NAC Server Certificate Validation Success	MiscAA:TestAP	1/23/2020 10:17 PM	MiscAA:TestAP	

AP	MiscAA:TestAP	BSSID	442030B87C4b
SSID	Misc-secure-net	Certificate Serial Number	6500000049F1a8453a27c5f0000000000e
Authentication Type	802.1X	User Name	user1@idp.ty.comcrossof.com
Certificate CN	user1	Certificate Issuer	JOC-Contoso-PrivateCA-MiscAA:MS007-CA
Certificate Expiry	2025-05-19T13:59:48Z	EAP Type	EAP-TLS
EAP Type	EAP-TLS	IDP Roles	Employee, HigGroup1, CorporateDevices
		IDP	Azure AD

For EAP-TTLS authentication, you see the NAC IDP Authentication Success event. This event indicates that Azure AD has validated the user credentials. For this authentication, you also see the NAC IDP Group Lookup Success event that fetches user group memberships.

Figure 13: Success Message for EAP-TTLS Authentication by IDP

Client Events	90 Total	50 Good	17 Neutral	23 Bad
Authentication & Association	MiscAA:TestAP	1/23/2020 10:11 PM	MiscAA:TestAP	
NAC Client Access Allowed	MiscAA:TestAP	1/23/2020 10:16 PM	MiscAA:TestAP	
NAC IDP Group Lookup Success	MiscAA:TestAP	1/23/2020 10:17 PM	MiscAA:TestAP	
NAC IDP Authentication Success	MiscAA:TestAP	1/23/2020 10:17 PM	MiscAA:TestAP	
NAC Server Certificate Validation Success	MiscAA:TestAP	1/23/2020 10:17 PM	MiscAA:TestAP	
Flower Treatment Success	MiscAA:TestAP	1/23/2020 10:17 PM	MiscAA:TestAP	

AP	MiscAA:TestAP	BSSID	442030B87C4b
SSID	Misc-secure-net	Authentication Type	802.1X
User Name	user1@idp.ty.comcrossof.com	Certificate Expiry	0001-01-01T00:00:00Z
EAP Type	EAP-TLS	IDP Roles	HigGroup1, CorporateDevices, Employee
		IDP	Azure AD

## EAP-TTLS Authentication with Azure AD and ROPC

EAP-TTLS leverages Resource Owner Password Credentials (ROPC) OAuth flow with Azure AD to authenticate users and retrieve user group information. You must consider several factors when you use a legacy authentication such as ROPC flow, which verifies only user name and password and skips multi-factor authentication (MFA).

- You must configure the client devices with the correct wireless profile, either by using mobile device management (MDM) or a Group Policy Object (GPO). If you provide only user name and password at the login prompt, legacy authentication fails to work for some operating systems.
- The username that a user enters must be in the User Principal Name (UPN) format (username@domain).
- You must configure clients to trust the server certificate.
- Users must log in at least once to the Azure portal before attempting access using ROPC authentication. This step is important to test user accounts.
- The Azure portal must store user passwords either in full cloud accounts, or in a local AD where password synchronization is enabled with Azure AD Connect. Federated Authentication users are not supported.

- You must disable MFA for users who select ROPC authentication. One way to achieve MFA bypass for EAP-TTLS is to mark [Mist Access Assurance Source IP addresses](#) as trusted locations using following procedure:
  1. In the Microsoft Entra portal, go to **Protection > Conditional Access > Named locations** and select **New location**.
  2. In the New location (IP ranges), enter the details.

Figure 14: Bypass MFA for Sign in from a Trusted IP Address Range

## New location (IP ranges) ✕

[↑ Upload](#) [↓ Download](#)

Configure named location IPv4 and IPv6 ranges.  
[Learn more](#)

Name <sup>\*</sup>

 ✓

Mark as trusted location

[+](#)

44.238.214.57/32	<a href="#">✕</a>
54.214.208.109/32	<a href="#">✕</a>
54.71.176.201/32	<a href="#">✕</a>
13.58.92.194/32	<a href="#">✕</a>
18.217.23.193/32	<a href="#">✕</a>
3.22.40.111/32	<a href="#">✕</a>
15.236.172.79/32	<a href="#">✕</a>
15.236.44.93/32	<a href="#">✕</a>
15.237.171.133/32	<a href="#">✕</a>
3.77.68.168/32	<a href="#">✕</a>
52.57.243.242/32	<a href="#">✕</a>
18.153.242.220/32	<a href="#">✕</a>
54.255.158.51/32	<a href="#">✕</a>
18.143.121.8/32	<a href="#">✕</a>
13.228.196.58/32	<a href="#">✕</a>
13.239.90.65/32	<a href="#">✕</a>
13.227.26.220/32	<a href="#">✕</a>

[Create](#)

3. Enter a name for the location.
4. Select **Mark as trusted location**.

5. Enter the IP range for Juniper Mist Access Assurance IP addresses.
6. Click **Create**.
7. In the Conditional Access MFA policy, refer the trusted IP sources as exclusion criteria.

**Figure 15: Exclude Named Location from Access Policy**

The screenshot shows the configuration page for a Conditional Access policy named 'test-o365-policy'. The policy is currently disabled. The configuration is as follows:

- Name:** test-o365-policy
- Assignments:**
  - Users:** Specific users included and specific users excluded
  - Target resources:** All cloud apps
  - Conditions:** 1 condition selected
  - Access controls:** 1 control selected
  - Session:** 0 controls selected
- Control access based on signals from conditions:**
  - User risk:** Not configured
  - Sign-in risk:** Not configured
  - Device platforms:** Not configured
  - Locations:** Any location and all trusted locations excluded
  - Client apps:** Not configured
  - Filter for devices:** Not configured
- Control user access based on their physical location:**
  - Configure:** Yes (selected), No
  - Include/Exclude:** Exclude (selected), Include
  - Select the locations to exempt from the policy:** All trusted locations (selected), Selected locations

At the bottom, the 'Enable policy' toggle is set to 'Off' (Report-only). A 'Save' button is visible at the bottom left.

## SEE ALSO

[Add Identity Providers for Juniper Mist Access Assurance | 56](#)

[Integrate Google Workspace as an Identity Provider | 27](#)

[Integrate Okta as an Identity Provider | 22](#)

# Integrate with Microsoft Intune

## IN THIS SECTION

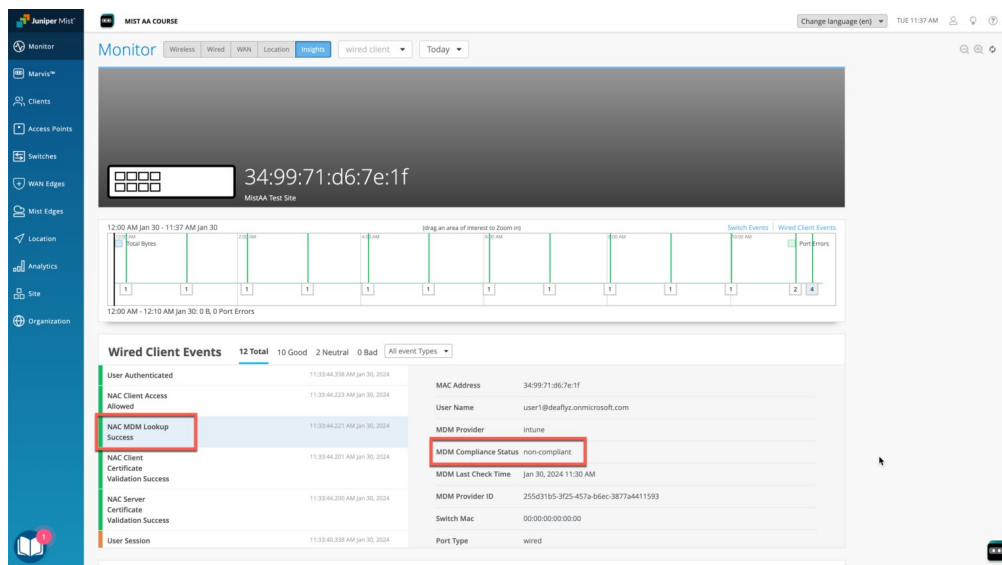
[Adding Intune to the Mist Portal | 42](#)

- Creating Policy Rules | 42
- Viewing Client Events | 43
- How it Works | 44

Microsoft Intune Endpoint Management uses Device Compliance Policies to check for the presence of an antivirus software, account for firewall rules, check clients for the latest security patches, and so on. Juniper Mist™ Access Assurance can leverage the compliance state of Intune-managed device for additional posture assessment according to the Auth Policies you create.

You can integrate Access Assurance with the Intune for use in the Mist portal. For example, you can use the integration to create a client authorization policy in Mist that segregates non-compliant clients to a quarantine VLAN while letting compliant ones access the corporate network. To do so, you need to be running firmware version 0.14 or later on the Juniper Mist APs, and have an administrator account on Microsoft Entra ID (this is to grant read privileges to Mist Access Assurance to get the Intune device data).

**Figure 16: Monitor Intune-based Access Assurance Policy Events in the Mist Portal**



As wireless clients log on and are authorized on a Juniper Mist AP, the cloud-based Mist Access Assurance service learns the client's security compliance status from Intune. It then uses that information in an authentication policy to connect the client to a selected VLAN based on the results. In the figure above, which shows the Insights tab on the Monitor portal page, Intune has classified one of the clients as non-compliant.



## Adding Intune to the Mist Portal

To add Microsoft Intune to the Mist Access Assurance portal:

1. From the left menu of the Juniper Mist portal, select **Organization | Access > Identity Providers**
2. In the Linked Accounts section, click **Link Account**.
3. Select Microsoft Intune. You will be redirected to Microsoft Entra ID / Intune for the Single Sign On (SSO) login, and then prompted to grant permission for the Mist Access Assurance portal to read Microsoft Intune device data.
4. (Optional) After linking the Intune account, you can see the Intune account status on the Identity Providers page: **Organization | Access > Identity Providers**.

## Creating Policy Rules

With the Intune account linked to Mist, you can leverage managed the device compliance status in your Mist Auth Policies. For example, you can put non-compliant clients into a quarantine VLAN, while allowing compliant devices to connect to the corporate VLAN. You do this by creating a pair of labels for compliance and non-compliance, and another pair for corp and quarantine VLANs. Then you use these labels in a pair of Auth Policy rules to automatically govern network access.

Create compliance and quarantine labels:

1. From the left menu of the Juniper Mist portal, select **Organization > Access > Auth Policies**.
2. Click the **Create Label** button and give the label a name, for example, **Intune-Compliant**.
3. Under **Label Type**, choose **MDM Compliance**.
4. Under **Label Values**, select **Compliant**.
5. Click the **Create** button.
6. Repeat these steps to create the remaining labels, as shown here:
  - **Label Name:** Intune-Non-Compliant, **Label Type:** MDM Compliance, **Label Value:** Non Compliant
  - **Label Name:** Quarantine, **Label Type:** AAA, **Label Value:** VLAN, *1*
  - **Label Name:** Corp VLAN, **Label Type:** AAA, **Label Value:** VLAN, *750*

Figure 17: Compliance Rules Based on Intune

No.	Name	Match Criteria (match on location, SSID, User Group, etc)	Policy	Assigned Policies (VLAN, Rules, Session Timeout, etc)	Hit Count
1	Non-Compliant Corp Devices	+ all Intune Non-Compliant Devices EAP-TLS	→	Network Access Allowed Quarantine Network	0
2	Compliant Corp Devices	+ all Intune Compliant Devices EAP-TLS	→	Network Access Allowed Corp VLAN	0
3	Meraki AP	+ all approved meraki aps MAB Wired	→	Network Access Allowed AP Trunk Single Supplicant Mode	0
4	Approved PSS	+ all PSS Wired	→	Network Access Allowed Corp VLAN	0
5	Mist AP Cert Auth	any Mist AP Certs Mist APs Staging & all EAP-TLS Wired	→	Network Access Allowed AP Trunk Single Supplicant Mode Weekly Reauth	0
6	Wired TTLS Auth	+ all EAP-TTLS Wired	→	Network Access Allowed Corp VLAN	0
7	Approved Phillips Devices	+ all Approved Phillips Hubs MAB Wired	→	Network Access Allowed AP VLAN	0
8	Wired Cert Auth	+ all EAP-TLS Wired	→	Network Access Allowed Corp VLAN	0
9	Credential Auth - Employees	+ all Employee Group EAP-TTLS Wireless	→	Network Access Allowed Corp VLAN	0
10	Cert Auth - Employees	+ all Employee Group EAP-TTLS Wireless	→	Network Access Allowed Employee Role Corp VLAN	0
11	Wireless EAP-TLS Auth	+ all EAP-TLS Wireless	→	Network Access Allowed Corp VLAN	0
Last	Last Rule		All Users →	Network Access Denied	0

Create Auth Policy Rules:

1. Click the **Add Rule** button and give the rule a name, for example, **Corp Compliant**.
2. In the **Match Criteria** column, click the + icon and then select **Intune-Compliant** from the list that appears.
3. In the **Policy** column, select **Allow**.
4. In the Assigned Policies column, click the + icon and then select **Corp VLAN**.
5. Repeat these steps to create the quarantine rule.
6. When finished, click **Save**.

## Viewing Client Events

As shown in Figure 1, in the Client Events section on the Insights tab of the Monitor portal page, the values show for some parameters depend on how you have configured Microsoft.

- **Non-randomized MAC address**—If you want to show non-randomized MAC addresses under **Client Events**, you need to disable MAC randomization in the Intune Wi-Fi settings. This display supports both EAP-TTLS and EAP-TLS authentication, and uses the client MAC address from Intune.
- **DeviceName** or **DeviceName.FQDN**—Under **Client Events**, the name shown for *Certificate CN* comes from the Intune SCEP certificate configuration (it's the Subject name format field). The **Client Events** name shown for *Certificate SAN (DNS Name)* comes from the Intune SCEP profile variable used to encode the Intune Device ID in the SAN:DNS certificate field.

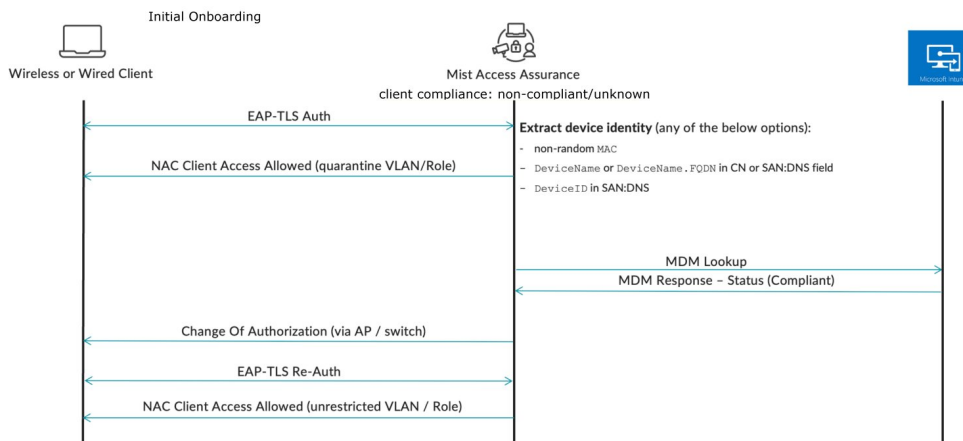
## How it Works

The Access Assurance API polls Microsoft Intune every two hours for a list of authenticated Intune-managed clients, and makes any necessary updates. The default polling interval for Microsoft Intune to its managed devices is every eight hours. Mist Access Assurance caches the retrieved compliance state data to optimize retrieval times.

Whenever a device is found to be out of compliance, Mist Access Assurance issues a Change Of Authorization command and re-runs the policy. The policy then triggers the required corrective actions, as needed, to bring the device back in to compliance.

The communication flow between the two services is shown in the following illustration.

**Figure 18: Authentication and Authorization for Microsoft Intune**



## RELATED DOCUMENTATION

[Juniper Mist Access Assurance Authentication Methods | 8](#)

[Integrate Microsoft Entra ID as an Identity Provider | 33](#)

# JAMF Pro Integration

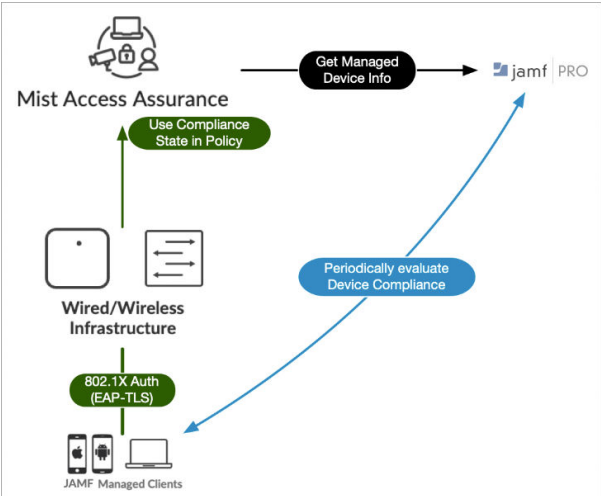
**IN THIS SECTION**

- JAMF Device Data Retrieval | 46
- Create Client ID and Secret on the JAMF Pro | 47
- Link JAMF Pro Account to Mist Access Assurance | 49
- Verification | 50

Mist Access Assurance allows you to integrate natively into JAMF Pro Endpoint Management platform for checking managed endpoint compliance state.

JAMF evaluates JAMF managed devices (MacBook, iPad, iPhone and other iOS devices) for compliance. Evaluation is done using Smart Computer Groups for MACbooks and Smart Device Groups for iPads and iOS devices for presence of antivirus, firewall status, software version, and so on. Mist Access Assurance obtains the compliance state of the devices and leverages that state in authentication policy rules to perform posture assessment.

**Figure 19: JAMF Evaluation of Managed Devices**



## JAMF Device Data Retrieval

Mist Access Assurance retrieves JAMF managed device data in the following manner:

- Access Assurance uses API-based polling mechanism toward JAMF every two hours for every managed client that has been previously authenticated. Compliance states information is cached for fast retrieval.
- Information retrieval is performed out-of-band, that is, after the authentication process to avoid any additional delays. After initial device onboarding, information is updated every two hours.
- In case device compliance status changes, then Mist Access Assurance automatically trigger a Change Of Authorization to re-run the policy and apply respective action.
- Juniper Mist access points (APs), which connect JAMF managed devices to the wireless network, must have firmware version 0.14 or higher.

Mist Access Assurance uses the following information during client authentication to match a client with a device record in JAMF:

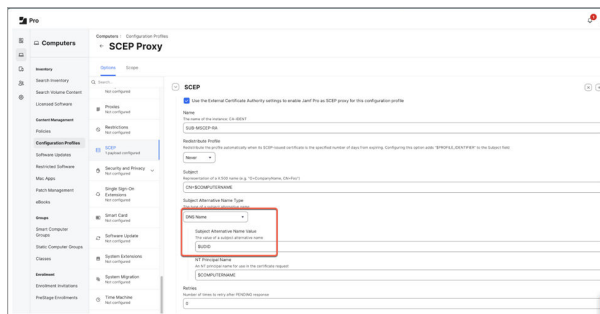
- **Non-randomized MAC address**—This method can be used with EAP-TTLS or EAP-TLS authentication. Client MAC device is matched with a device MAC present in JAMF. For wireless profile, make sure MAC randomization or rotation is disabled.



**NOTE:** iOS devices do not have native Ethernet NIC, so this method is only useful with iOS devices that are connected through wireless.

- **JAMF Device UDID** encoded in SAN:DNS certificate attribute. [Figure 20 on page 46](#) shows location of UDID in configuration profile.

Figure 20: Locating Unique Device ID

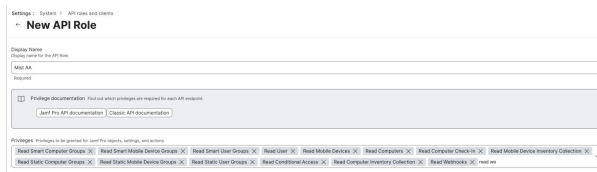


## Create Client ID and Secret on the JAMF Pro

For integration with JAMF Pro, you need client ID and secret.

1. In the JAMF Pro dashboard navigate to **Settings > API roles and clients**.
2. Create a role for Mist Access Assurance connector and assign the permissions.

**Figure 21: Configuring API Roles and Clients**



Assign the following read-only permissions:

- Read Computer Check-In
  - Read Mobile Devices
  - Read Computers
  - Read Mobile Device Inventory Collection
  - Read Static User Groups
  - Read Static Computer Groups
  - Read Mobile Device Self Service
  - Read Conditional Access
  - Read Smart Computer Groups
  - Read Computer Inventory Collection
  - Read Smart Mobile Device Groups
  - Read Smart User Groups
  - Read User
  - Read Webhooks
3. Navigate to API Clients tab, and add a new client.

**Figure 22: Configure New API Client**

Settings : System

**New API Client**

Display Name: Mist AA Client

API roles: Mist AA

Access token lifetime: 86400

Generate client secret

Enable/disable API client: Enabled

Select the API role created in the previous step and set access token refresh time (example 24 hrs). Then click **Enable/disable API Client** to toggle it to **Enable API Client**.

4. Save the details and click Generate client secret on the next page.

**Figure 23: Generate Client Secret**

Settings : System

**API roles and clients**

Display name: Mist AA Client

API roles: Mist AA

Access token lifetime: 86400

Client ID: 219db897-c62f-4a54-b366-36f6250910b7

Generate client secret

Enable/disable API client: Enabled

The client secret is generated.

5. Copy both Client ID and Secret and save it in safe place to retrieve later.

**Figure 24: Client Secret Details**

**Save client secret**

This client secret will not be revealed again. Save it somewhere safe.

Client credentials can be redeemed for access tokens using form-urlencoded data at the Jamf Pro API OAuth token endpoint. The endpoint is: /api/oauth/token

**Client ID:**  
219db897-c62f-4a54-b366-36f6250910b7

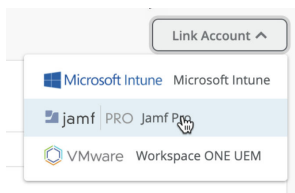
**Client secret:**  
qhvHX: [redacted] .15AjGQL-e04Qzl

Copy client credentials to clipboard Close

## Link JAMF Pro Account to Mist Access Assurance

1. Juniper Mist dashboard, navigate to **Organization > Access > Identity Providers**.
2. In the Identity Providers page, scroll down to Linked Account section and click **Link Account** to select **JAMF Pro**.

Figure 25: Linking to JAMF Pro Account



3. In the Link Account pop-up window, enter the details. [Figure 26 on page 49](#) shows a sample of link account details.

Figure 26: Details for Linking JAMF Pro

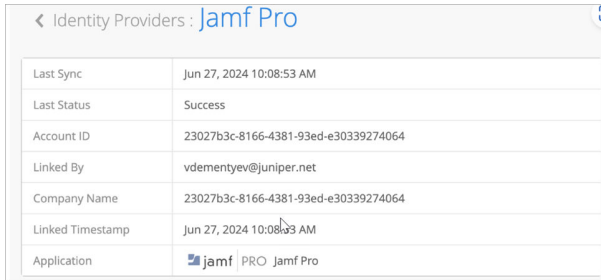
- **Instance URL**—JAMF Pro instance URL. Example: `https://<yourjamfurl>.com`. Remove any trailing `/` in the Instance URL field.
- **Client ID**—Client ID generated while creating Client ID and Secret on the JAMF Pro dashboard.
- **Client Secret**—Client secret generated while creating Client ID and Secret on the JAMF Pro dashboard.
- **Smart Group Name**—Smart group name to match against. JAMF Pro allows you to create groups for managed computers, mobile devices, or users. Smart Groups (both computer and mobile device smart groups) offer dynamic rule based matching, which allows you to set policies such as



running software, OS versions of your managed devices. In case a client is found in JAMF and is part of selected Smart Group then it is considered as MDM compliant.

After linking is complete, you can see last sync status and time as shown in [Figure 27 on page 50](#).

**Figure 27: JAMP Pro Sync Status**

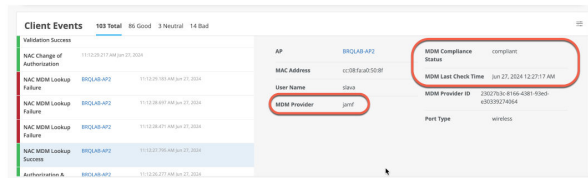


Identity Providers : Jamf Pro	
Last Sync	Jun 27, 2024 10:08:53 AM
Last Status	Success
Account ID	23027b3c-8166-4381-93ed-e30339274064
Linked By	vdementyev@juniper.net
Company Name	23027b3c-8166-4381-93ed-e30339274064
Linked Timestamp	Jun 27, 2024 10:08:53 AM
Application	jamf   PRO Jamf Pro

## Verification

On the Juniper Mist portal, navigate to Monitoring > Insights > Client Events to see the information. Under Client Insights, you can see MDM lookups are performed for iOS managed devices as shown in [Figure 28 on page 50](#).

**Figure 28: MDM Lookup Details**



Client Events		163 Total	85 Good	3 Neutral	14 Bad
Installation Success					
NAC Change of Authentication	11/12/2024 10:08:53 AM				
NAC MDM Lookup	11/12/2024 10:08:53 AM	Success			
NAC MDM Lookup	11/12/2024 10:08:53 AM	Failure			
NAC MDM Lookup	11/12/2024 10:08:53 AM	Failure			
NAC MDM Lookup	11/12/2024 10:08:53 AM	Failure			
NAC MDM Lookup Success	11/12/2024 10:08:53 AM				
Authentication A	11/12/2024 10:08:53 AM				

AP	BRQJAS-AP2
MAC Address	e128f5a02558f
User Name	sdm
MDM Provider	jamf
MDM Compliance Status	compliant
MDM Last Check Time	Jun 27, 2024 12:21:17 AM
MDM Provider ID	23027b3c-8166-4381-93ed-e30339274064
Port Type	wireless

Note that during initial MDM lookup for a new client, lookup is performed post initial authentication. After MDM state changes, Mist Access Assurance initiates CoA to re-authenticate the client and apply the correct policy. Upon subsequent authentications, NAC uses MDM cache which is updated periodically to reflect any changes for every 2 hours. [Figure 29 on page 51](#) shows a sample of compliance status change.

Figure 29: MDM Lookup Details- MDM Status Change

Client Events			MD Total	85 Good	3 Neutral	14 Bad
NAC MDM Lookup Success	88QJAB-AP2	11/12/2024 10:00 AM (Jun 27, 2024)				
NAC Client Certificate Validation Success	88QJAB-AP2	11/12/2024 10:00 AM (Jun 27, 2024)				
NAC Server Certificate Validation Success	88QJAB-AP2	11/12/2024 10:00 AM (Jun 27, 2024)				
NAC Change of Authorization	11/12/2024 10:00 AM (Jun 27, 2024)					
NAC MDM Lookup Failure	88QJAB-AP2	11/12/2024 10:00 AM (Jun 27, 2024)				

MAC Address	e1287a-95503bf	Previous MDM Compliance Status	unknown
Description	Due to compliance status change	MDM Last Check Time	Jun 27, 2024 12:27:17 AM
MDM Provider	junif	MDM Provider ID	20237626-8166-4381-93ac-693032764684
MDM Compliance Status	compliant	Port Type	wireless

## SEE ALSO

[Add Identity Providers for Juniper Mist Access Assurance](#) | 56

# Use Case: Mist Edge Proxy for Eduroam

## SUMMARY

This eduroam use case illustrates how to use Mist Edge as an IdP Proxy.

## IN THIS SECTION

- [Overview](#) | 51
- [Firewall Requirements](#) | 53
- [Configure Juniper Mist](#) | 54
- [Configure Eduroam](#) | 55
- [Verification](#) | 55

## Overview

This use case shows how you can integrate Juniper Mist Access Assurance with eduroam NROs (National Roaming Operators) using Mist Edge acting as a RADIUS proxy. Mist Edge acts as a gateway to eduroam RADIUS servers with a static public IP or NAT IP assigned such that it can be registered as a RADIUS client in the eduroam admin portal.

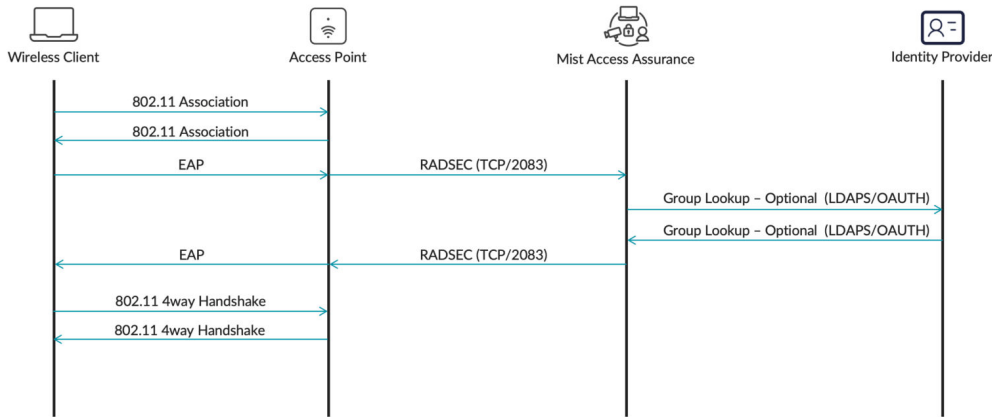
Mist Edge Proxy is used in particular with eduroam SP and IdP authentication flows; it does not affect home users authentication.

The following call flows illustrate three types of users in eduroam networks and how each type authenticates via Mist Access Assurance and Mist Edge proxy: home users on campus, external visitors on campus (SP), and home roaming users (IdP).

### Home Users

Home users are clients that are connecting to the eduroam SSID on their own university campus. For example, a user with an *@university1.edu* account is currently at University 1. This user is on their "home" realm. This is the typical scenario for most authentications happening daily at this university.

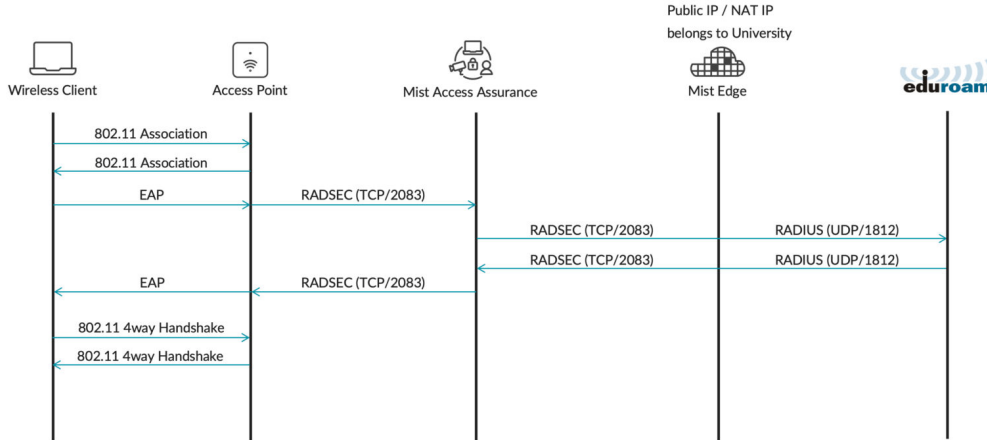
This scenario does not require Mist Edge proxy. The user authenticates directly with Mist Access Assurance.



### External Visitors

External visitors are clients who are visiting a university campus from another institution. For example, a user with an *@university2.edu* account is currently visiting University 1. This user is identified by a realm that is not the "home" realm.

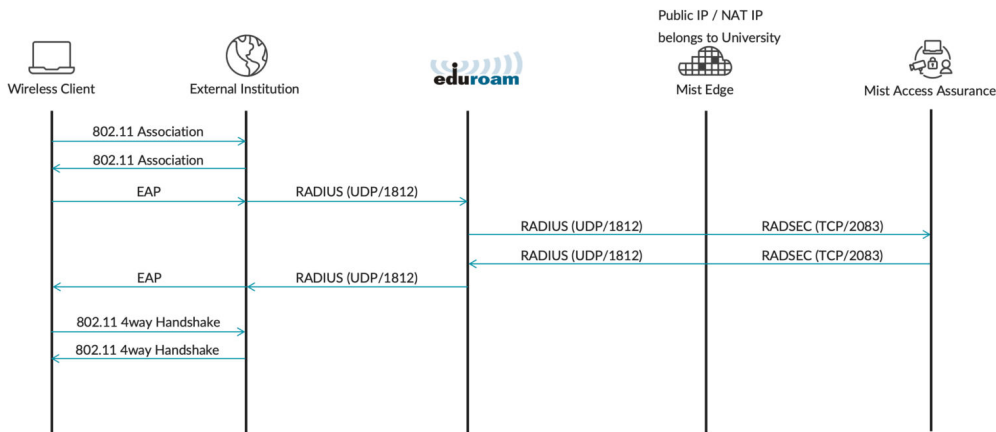
This scenario requires Mist Edge Proxy IDP to forward authentication requests to university2.edu via eduroam RADIUS servers. External visitors authenticate via a Mist Edge proxy, where Mist Edge the proxies authentication requests towards the eduroam national RADIUS servers.



### Home Roaming Users

Home roaming users are clients who are visiting a different institution and would like to authenticate to an eduroam SSID by using their home university credentials.

In this example, a user with an *@university1.edu* account is visiting University 2. The authentication requests are coming from university2.edu via eduroam RADIUS servers towards university1.edu. RADIUS Access-Requests from eduroam national RADIUS servers are received by the Mist Edge Proxy and then forwarded to the Mist Access Assurance service for authentication.



### Firewall Requirements

Mist Edge uses Out Of Band Management interface (OOBM) for all its proxy functionalities. It is possible to either assign a public IP address to the OOBM interface or place it behind NAT firewall.

The following ports and destinations must be allowed:

- **Inbound** (towards Mist Edge OOBM interface)

- RADIUS Auth & Acct (1812 / 1813 UDP) – you could limit source IPs to eduroam national RADIUS servers
- RadSec (2083 TCP) – you could limit source IPs based on the [following document](#).
- **Outbound** (from Mist Edge OOBM interface):
  - RADIUS Auth & Acct (1812 / 1813 UDP)
  - RadSec (2083 TCP) towards radsec.nac.mist.com
  - HTTPS (443 TCP) towards ep-terminator.<mist\_cloud\_env>.mist.com (more on correct endpoint for your cloud environment in [this document](#)).



#### NOTE:

- Mist Access Assurance only supports EAP-TLS, TEAP or EAP-TTLS methods for home users and home roaming users.
- For external visitors any EAP method is supported, including PEAP-MSCHAPv2. EAP method support is determined by an external institution RADIUS servers.
- Dedicated Mist Edge(s) are a must for the IDP proxy functionality.
- For proxy service redundancy multiple Mist Edges can be used as part of the same Mist Edge cluster.

## Configure Juniper Mist

Complete these steps in the Juniper Mist Portal.

1. On the Mist Edges page, claim or register a Mist Edge and create a Mist Edge cluster.

You can do these tasks by selecting **Mist Edges** from the left menu of the Juniper Mist portal. Then use the buttons to **Claim Mist Edge**, **Create Mist Edge**, and **Create Cluster**.

2. On the Identity Providers page, add a Mist Edge Proxy Identity Provider.

For help, see "[Add Identity Providers for Juniper Mist Access Assurance](#)" on page 56.

3. On the Auth Policies page, configure rules for your eduroam SSID.

The following example shows a basic scenario. Both home and external users are on eduroam network. External users are placed into a Guest VLAN, while home and home roaming users are placed into a primary university VLAN.

Each user authentication attempt is evaluated according to the list of Policy rules based on Match criteria. Only the first matching policy rule is applied.

No.	Name	Match Criteria (match on location, SSID, User Group, etc)	Policy	Assigned Policies (VLAN, Roles, Session Timeout, etc)	Hit Count
1	Eduroam Home and Home Roaming Users	+ all + eduroam SSID + Home Users	✓	Network Access Allowed Unrestricted VLAN	0
2	Eduroam External Visitors	+ eduroam SSID	✓	Network Access Allowed Guest VLAN	1

## Configure Eduroam

In the Eduroam admin console, add your Mist Edges. Depending on the eduroam NRO, the admin console might look different, but the overall integration points will remain the same.

### Eduroam Hotspot RADIUS Servers

eduroam Dashboard

eduroam Hotspot RADIUS Servers

Friendly Name	IP Address	Secret		
Mist Edge 1	203.0.113.1	*****	Edit	Delete
Mist Edge 2	203.0.113.2	*****	Edit	Delete

Previous Next

### eduroam IdP Realms

eduroam Dashboard

IdP Realms

IdP Realm: example.edu

Name: example.edu  
Load Balance Type: hashbalance  
Handle: [Test Realm] [Edit]

RADIUS Servers

Friendly Name	IP Address	Secret	Auth Port	Acct Port	Order		
Mist Edge 1	203.0.113.1	*****	1812	1813	1	Edit	Delete
Mist Edge 2	203.0.113.2	*****	1812	1813	2	Edit	Delete

## Verification

To verify the configuration, check the events on the Client Insights page or under NAC Events on the Auth Policies page.



**NOTE:** For external users only, a NAC Client Access Allowed or Denied event will be generated without any other NAC events, due to the fact that authentication is handled by an external RADIUS server (eduroam).

Client Events		244 Total	92 Good	103 Neutral	49 Bad
DNS Success	stava@mistaa.com	12-01-14-01 PM 1/16/2024			
DHCP Success	stava@mistaa.com	12-01-14-05 PM 1/16/2024			
Gateway ARP Success	stava@mistaa.com	12-01-14-57 PM 1/16/2024			
Authentication & Association	stava@mistaa.com	12-01-14-24 PM 1/16/2024			
MAC Client Access Allowed	stava@mistaa.com	12-01-14-28 PM 1/16/2024			
MAC Client Access Denied	stava@mistaa.com	12-01-14-27 PM 1/16/2024			
Client	Anonymous	12-01-14-01 PM 1/16/2024			

Client	stava@mistaa.com	Authentication Type	eap-pap
AP	BQQLAB-AP2	User Name	stava@mistaa.com
MAC Address	0a:1b:23:6d:16:90	Auth Rule	Education External Visitors
BSSID	00:3c:79:63:e4:52	RADIUS Returned Attributes	Tunnel-Type=VLAN Tunnel-Medium-Type=IEEE-802 802 Tunnel-Private-Group-Id=300
SSID	MS-Unity-Net	Port Type	wireless
VLAN	300	NAC Header	juniper-mlnx

## SEE ALSO

[Add Identity Providers for Juniper Mist Access Assurance | 56](#)

[Configure Authentication Policy | 69](#)

# Add Identity Providers for Juniper Mist Access Assurance

Juniper Mist™ Access Assurance integrates with various Identity Providers (IdPs) to enhance authentication and access control. Identity providers serve as authentication source (in case of EAP-TTLS) and authorization source (by obtaining user group memberships, account state etc) for EAP-TLS or EAP-TTLS.

Here are the supported IdPs:

- Microsoft Entra ID (formerly known as Azure Active Directory)
- Okta Workforce Identity
- Google Workspace
- Juniper Mist Edge Proxy

Juniper Mist Access Assurance uses identity providers (IdPs) to:

- Get additional identity context such as user group memberships and account state of clients. This information is available in certificate-based authentication methods such as Extensible Authentication Protocol–Transport Layer Security (EAP-TLS) and Extensible Authentication Protocol–Tunneled TLS (EAP-TTLS).
- Authenticate clients by validating credentials. EAP-TTLS supports credential-based authentication.

Remember that configuring IdPs is optional for EAP-TLS certificate-based authentication, but it is mandatory for credential-based authentication (EAP-TTLS). If you're setting up an IdP, ensure you have the necessary details, such as client ID and client secret, from the identity provider.

Juniper Mist Access Assurance uses the following protocols to integrate into any IdP to look up users and get device state information:

- Secure Lightweight Directory Access Protocol (LDAP)
- OAuth 2.0

Configuring IdPs is optional for EAP-TLS certificate-based authentication and mandatory for credential-based authentication (EAP-TTLS).

### Prerequisites

- If you're using Azure, Okta, or similar IdPs, register with the IdP. You can obtain the client ID and client secret details from the IdP after registration.

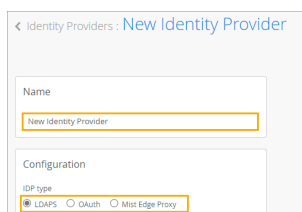
For help, see:

- ["Integrate Microsoft Entra ID as an Identity Provider" on page 33](#)
- ["Integrate Okta as an Identity Provider" on page 22](#)
- ["Integrate Google Workspace as an Identity Provider" on page 27](#)
- If you're using Mist Edge Proxy as IdP, claim or register a Mist Edge and create Mist Edge cluster.

You can do these tasks by selecting **Mist Edges** from the left menu of the Juniper Mist portal. Then use the buttons to **Claim Mist Edge**, **Create Mist Edge**, and **Create Cluster**.

To add identity providers for Juniper Mist Access Assurance:

1. From the left menu of the Juniper Mist portal, select **Organization > Access > Identity Providers**.
2. Click **Add IDP** near the top-right corner of the Identity Providers page.
3. On the New Identity Provider page, enter a **Name** and select the **IDP type**:
  - **LDAPS**
  - **OAuth**
  - **Mist Edge Proxy**



The screenshot shows the 'New Identity Provider' configuration page. It has a breadcrumb trail: '< Identity Providers > New Identity Provider'. There are two main sections: 'Name' and 'Configuration'. The 'Name' section has a text input field containing 'New Identity Provider'. The 'Configuration' section has an 'IDP type' label and three radio button options: 'LDAPS' (which is selected), 'OAuth', and 'Mist Edge Proxy'.

4. Refer to the tables below to enter the information required for the selected type.

### LDAPS



Table 5: Settings for LDAPS IdPs

Parameters	Details
LDAP Type	Select one of the following options from the drop-down menu: <ul style="list-style-type: none"> <li>• <b>Azure</b></li> <li>• <b>Okta</b></li> <li>• <b>Custom</b></li> </ul>
Server Hosts	Enter the name or the IP address of the LDAP server you're going to use for authentication.
Domain Names	Enter the fully qualified domain name (FQDN) of the LDAP server.
Default IDP	Set the selected identity provider as default IdP. The system performs lookup in this IdP if the entered user domain name is unknown or not found.
Bind DN	Specify the user whom you've allowed to search the base domain name. Example: cn=admin, dc=abc, dc=com.
Bind Password	Enter the password of the user who is mentioned in the <b>Bind DN</b> .
Base DN	Enter a whole domain or a specific organization unit (container) in <b>Search base</b> to specify where users and groups are found in the LDAP tree, for example: OU=NetworkAdmins,DC=your,DC=domain,DC=com.
LDAPS Certificates	Add the Certificate Authority-generated certificate and the client certificate.

Table 5: Settings for LDAPS IdPs (Continued)

Parameters	Details
<ul style="list-style-type: none"> <li>Group Filter</li> <li>Member Filter</li> <li>User Filter</li> </ul>	Specify the LDAP filter that will identify the type of group, member, or user. This option is available only for LDAP Type <b>Custom</b> .

## OAuth

For OAuth type of authentication, enter the values as provided in [Table 6 on page 59](#). Some of the fields you enter here requires values you'll receive when you configure Azure or Okta Application. See "[Integrate Microsoft Entra ID as an Identity Provider](#)" on page 33 or "[Integrate Okta as an Identity Provider](#)" on page 22.

Table 6: Settings for OAuth IdPs

Parameters	Description
OAuth Type	Select one of the following options from the drop-down menu: <ul style="list-style-type: none"> <li>Azure</li> <li>Okta</li> </ul>
OAuth Tenant ID	Enter OAuth tenant ID. Use the ID you received during Azure or Okta application configuration.
Domain Names	Enter a fully qualified domain name.
Default IDP	Set the selected identity provider as default if user domain name is not specified.
OAuth Client Credential (CC) Client Id	The application ID of your client application. Use the ID you received during Azure or Okta application configuration.

**Table 6: Settings for OAuth IdPs (Continued)**

Parameters	Description
OAuth Client Credential (CC) Client Private Key	(For Okta) Enter the private key generated during Okta application configuration.
OAuth Resource Owner Password Credential (ROPC) Client Id	(For Okta) Enter the client secret ID. Use the secret ID you received during Okta application configuration.
OAuth Resource Owner Password Credential (ROPC) Client Secret	(For Okta) Provide client secret value. Use the secret value you received during Okta application configuration.
OAuth Client Credential (CC) Client Id	(For Azure) Enter the client ID generated during Azure application configuration.
OAuth Client Credential (CC) Client Secret	(For Azure) Enter the client secret value generated during Azure application configuration.
OAuth Resource Owner Password Credential (ROPC) Client Id	(For Azure) same as <b>OAuth Client Credential (CC) Client Id</b> .

### Mist Edge Proxy

**Table 7: Settings for Mist Edge Proxy**

Parameters	Description
Proxy Hosts	<p>Enter a comma-separated list of the public IP or NAT IP addresses of the Mist Edges that are acting as proxies. All these addresses must be part of the cluster that you identify in the <b>Mist Edge Cluster</b> field.</p> <p>Mist Edge will listen on the specified addresses for:</p> <ul style="list-style-type: none"> <li>• Inbound RadSec requests from Mist Access Assurance</li> <li>• RADIUS requests from external RADIUS servers</li> </ul>

Table 7: Settings for Mist Edge Proxy (Continued)

Parameters	Description
SSIDs	Enter a comma-separated list of the SSIDs that this IdP will use.
Mist Edge Cluster	Select a cluster from the list. <b>NOTE:</b> If you need to add a Mist Edge cluster, select <b>Mist Edges</b> from the left menu, and then select <b>Create Cluster</b> , and enter the information.
Exclude Realms	Use this option if you want to avoid proxying certain users. This is required only when EAP-TLS is used for users without any external IdP added as authorization source.  Enter the domain names/realms that you want to exclude; all other valid user realms will be proxied.
Operator Name	If you specify an operator name, it will be included in access requests that are forwarded to the external RADIUS server. For example, some eduroam NROs require the operator name attribute.  This attribute must start with 1, followed by an FQDN.  Example: <i>1abc_university.edu</i>
RADIUS Authentication Servers	You must specify at least one server. Click <b>Add Server</b> , and then enter the IP address, port, and shared secret.
RADIUS Accounting Servers	Click <b>Add Server</b> , and then enter the IP address, port, and shared secret.

- To save the changes, click **Create** at the top-right corner of the New Identity Provider page.

## RELATED DOCUMENTATION

Juniper Mist Access Assurance Best Practices | 14

---

Juniper Mist Access Assurance Authentication Methods | 8

---

Integrate Okta as an Identity Provider | 22

---

Integrate Microsoft Entra ID as an Identity Provider | 33

# 3

CHAPTER

## Access Assurance Settings

---

### IN THIS CHAPTER

- [Use Digital Certificates | 64](#)
  - [Configure Authentication Policy | 69](#)
  - [Configure Authentication Policy Labels | 72](#)
  - [Juniper Mist Access Assurance Endpoints | 76](#)
-

# Use Digital Certificates

## IN THIS SECTION

- [Use Certificate Authority \(CA\) Certificate | 65](#)
- [Use Default Server Certificate by Juniper Mist Access Assurance | 66](#)
- [Use Custom Server Certificates | 67](#)

When using EAP authentication, both the client and server must verify each other's identity. The client must trust the server it is communicating with, and the server must authenticate the client. The server certificate is the first step in this mutual authentication process, and the client must validate or trust it before proceeding with the communication.

If we take a look at any EAP transaction (say EAP-TLS or EAP-TTLS), regardless if it is wireless or wired authentication, the first step is for the server to identify itself by sending a "Server Hello" message to the client device.

When a client device receives a server certificate, it looks at the list of trusted Certificate Authorities (CAs) in the Wi-Fi or LAN profile and check if the server certificate is signed by one of the trusted CAs. Optionally, if configured, checks if the server name matches the list of trusted server names in the client configuration.

We recommend not bypassing validation step and trust server certificate. This is a high security risk and can open MITM (Man in the middle) attacks.

You can use one of the following methods to generate and use certificates for the RADIUS server that is integrated with Juniper Mist Access Assurance for each organization.

- **CA Certificate**—Juniper Mist requires specific CA certificates to establish trust with your client devices. These certificates, issued by trusted Certificate Authorities (CAs), enable Juniper Mist Access Assurance to grant network access to client devices. The validation of client devices by Juniper Mist is based upon the presentation of certificates by the devices, which must be signed by the same CA.
- **Default Juniper Mist Access Assurance Certificate**—Mist organization maintains its unique, private Mist Certificate Authority (CA) responsible for issuing the Access Assurance server certificate. In the absence of specific configurations, clients will receive a default certificate authenticated by their respective Mist Org CA. This certificate corresponds to the domain "auth.mist.com".

- Custom Server Certificate—Custom server certificate is favored when you prefer not to modify the current client configuration, and you want clients to trust server certificates issued by the same Certificate Authority (CA) that provided the client certificates. You must enter the Private Key and the Signed Certificate that you obtained from your RADIUS server.

Read following procedures to understand how to use the above certificates.

## Use Certificate Authority (CA) Certificate

For Extensible Authentication Protocol–Transport Layer Security (EAP-TLS) certificate-based authentication to work, you must add the trusted CA certificate on the Juniper Mist portal.

This step enables the Juniper Mist Access Authentication to trust client certificates signed by your added CAs.

You can obtain the certificate from an external CA. The CA can be a well-known, public CA or an enterprise CA.

Watch the following video to learn how to generate a certificate for testing or lab use:



**Video:** [Certificate Creation for Lab-Testing Use](#)

To add a CA certificate:

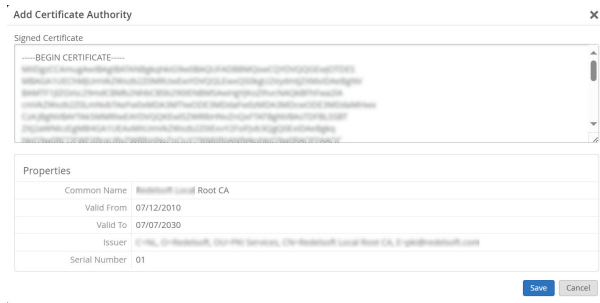
1. From the left menu of the Juniper Mist portal, select **Organization > Access > Certificates**. The Certificate Authorities page appears displaying a list of certificates.
2. Click **Add Certificate Authority**.

Common Name	Issuer	Valid To
Juniper Networks Root Certificate Authority	E=CN, O=Juniper Networks Inc., C=Juniper Net...	10/28/2026
Juniper Networks JSS Built-in Certificate Authority	O=Juniper Networks JSS Built-in Certificate Auth...	11/12/2031
Juniper Networks Issuing Sunnyvale CA	E=CN, O=Juniper Networks Inc., C=Juniper Net...	07/28/2026
Juniper Networks Issuing Bangalore IN	E=CN, O=Juniper Networks Inc., C=Juniper Net...	09/18/2026
Juniper Networks Issuing AWS1 CA	E=CN, O=Juniper Networks Inc., C=Juniper Net...	09/03/2026
Concede	E=CN, O=CA, U=CN, O=Concede Ltd, OU=CN...	06/07/2032

3. Paste your CA certificate in the Signed Certificate field.



**Figure 30: Add Certificate Authority**



The text must include the `--BEGIN CERTIFICATE--` and `--END CERTIFICATE--` lines.

The system parses and decodes the imported CA certificate and displays the certificate properties under the **Properties** pane. We recommend that you add your Root CA, as well as all your intermediate CAs or issuing certificates.

## Use Default Server Certificate by Juniper Mist Access Assurance

Juniper Mist cloud acts as a private certificate authority (CA) for each organization added on the Juniper Mist cloud. Juniper Mist issues a server certificate. If no certificates are configured, the Juniper Mist portal presents a default server certificate signed by Juniper Mist CA to the client devices.

Certificate will be issued for the name `auth.mist.com` and displays the information similar to what you see in [Figure 31 on page 66](#).

**Figure 31: Server Certificate Issued by Mist Access Assurance**

Subject	
RDN	Value
Common Name (CN)	auth.mist.com
Organizational Unit (OU)	277076a2c-022a-4a2a-8a2a-777076a2c022a
Organization (O)	Mist
Country (C)	US

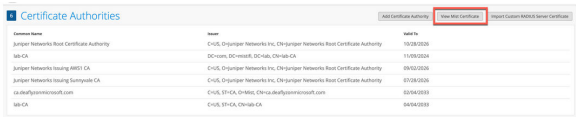
  

Properties	
Property	Value
Issuer	CN = 277076a2c-022a-4a2a-8a2a-777076a2c022a, OU = OrgCA,O = Mist,C = US
Subject	CN = auth.mist.com, OU = 277076a2c-022a-4a2a-8a2a-777076a2c022a, O = Mist,C = US
Valid From	1 Dec 2022, midnight
Valid To	1 Aug 2023, midnight
Serial Number	50 000000 00 000000 00 000000 00 000000 00 000000 00 000000 00 000000 00 000000
CA Cert	No
Key Size	4096 bits
Fingerprint (SHA-1)	80 00
Fingerprint (MD5)	00 00
SANS	auth.mist.com

On the client side, you must configure client devices to trust the Mist CA certificate and optionally validate server certificate name as **auth.mist.com**.

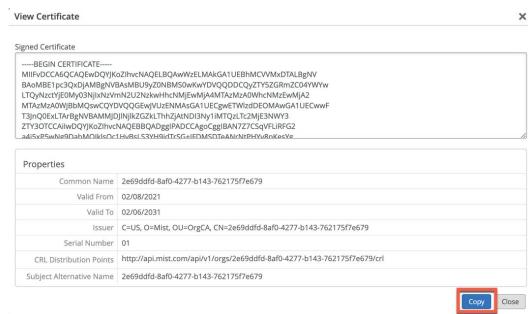
To download the Juniper Mist server certificate:

1. From the left menu of Juniper Mist portal, select **Organization > Access > Certificates**. The Certificate Authorities page appears displaying a list of certificates.
2. Click **View Mist Certificate**.



The screen displays the **Signed Certificate** details. Copy the certificate content from the **Signed Certificate** field.

Figure 32: View and Copy Mist Certificate



3. Store the content of the certificate on your local machine and add the extension **.cert** or **.cer** in the file name. For example: **mymistorgca.cert**.
4. Import the certificate file to all your client devices as a trusted root certificate.  
Once you configure a client device to trust the Juniper Mist CA certificate, you can use the certificate until the certificate is valid.

## Use Custom Server Certificates

You may already have a PKI and want to keep the existing configuration undisturbed. In such a scenario, you must upload the public certificate of your root CA and the public/private key pair of the RADIUS server on the Juniper Mist portal.

Ensure that your client devices also use the same certificates so that the RADIUS server validates each client's (supplicant's) certificate. Perform this task if you want to keep the current setup of your clients unchanged, and you want the clients to trust the server certificate that's issued by the same CA that issued their certificates.

To upload your certificate to the Juniper Mist portal:

1. From the left menu of Juniper Mist portal, select **Organization > Access > Certificates**.  
The page appears displaying a list of certificates.
2. Click **Import Custom Radius Certificate** to open the certificate page.

**Figure 33: Import Custom RADIUS Server Certificate**

Common Name	Name	Expiration
lab-CA	lab-CA	05/04/2023
Juniper Networks Root Certificate Authority	Juniper Networks Root Certificate Authority	10/28/2025
Juniper Networks Issuing Certificate CA	Juniper Networks Issuing Certificate CA	07/28/2025
Juniper Networks Issuing MDT CA	Juniper Networks Issuing MDT CA	07/28/2025
lab@juniper.com	lab@juniper.com	03/04/2023
missoua@MDT-CA	missoua@MDT-CA	05/03/2024

3. On the **Import Custom RADIUS Server Certificate** page, enter your CA certificate details:

**Figure 34: Enter Custom Server Certificate Details**

Import Custom RADIUS Server Certificate

Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA...
-----END RSA PRIVATE KEY-----
```

Private Key Password

Signed Certificate

```
-----BEGIN CERTIFICATE-----
MIIDBTCCAeICAwIBAgIQA...
-----END CERTIFICATE-----
```

Properties

Common Name	auth. .im
Valid From	05/04/2023
Valid To	05/03/2024
Issuer	C=US, ST=CA, CN=lab-CA
Serial Number	6650a9023b6d5d
Extended Key Usage	TLS Web server authentication
Subject Alternative Name	auth. .im

Save Cancel

- **Private Key**—Copy and paste the private key information. The text must include the BEGIN RSA PRIVATE KEY and END RSA PRIVATE KEY lines.
  - **Private Key Password**—Enter the passphrase of the private key (if available).
  - **Signed Certificate**—Copy and paste the certificate as text. Ensure that you include all the intermediate CAs and the Root CA certificate. The text must include the --BEGIN CERTIFICATE-- and --END CERTIFICATE-- lines.
4. Click **Save**.
  5. Set up your client devices to trust the root certificate authority (CA) that signed your server certificate.

With this step, you ensure that when you update or change your server certificate (which is usually done every year or after a few years), the client devices will trust the new server certificate because they trust the parent CA that signed it.

**Guidelines for using custom server certificates:**

- Do not use a wildcard certificate, for example: *\*.abc.com* for 802.1X authentication.
- You can use a certificate that contains a common name (CN) or a subject alternative name (SAN) for 802.1X authentication..
- We recommend the following x509 extension attributes. The majority of the client device operating systems support these extensions.
  - Use certificate version 3 or v3 (not legacy v1)
  - If the server name is being used as a validation criterion on the client side, then the certificate should include the SAN extension with the DNS name of the server.
  - Include Extended Key Usage as a TLS web server authentication criterion (required for most Android devices).

Now you can move forward with the certificate-based authentication process.

**SEE ALSO**

---

[Configure Certificate-Based \(EAP-TLS \) Authentication | 83](#)

---

[Juniper Mist Access Assurance Use Cases | 6](#)

---

[Juniper Mist Access Assurance Authentication Methods | 8](#)

---

[Configure Authentication Policy | 69](#)

---

[Configure Authentication Policy Labels | 72](#)

## Configure Authentication Policy

**IN THIS SECTION**

- [Create Authentication Policy | 70](#)

You must configure Juniper Mist Access Assurance with an authentication policy to authenticate end users or devices that attempt to access the network or applications.

The policy consists of a set of rules that devices and users must fulfill to get access to the network and use the network resources. Juniper Mist Access Assurance evaluates the authentication requests based on the specified policy conditions. If a user or device satisfies the conditions, Juniper Mist Access Assurance applies actions that either allow or deny access to the user or the device. These actions also apply attributes (VLAN, role) to the allowed users.

Juniper Mist Access Assurance uses "labels" as the policy matching criteria and also as a policy action for allowed users. You can create labels on the Authentication Policy Labels page or on the Authentication Policy page. See "[Configure Authentication Policy Labels](#)" on page 72 for details.

## Create Authentication Policy

To create an authentication policy:

1. On the Juniper Mist portal, from the left menu, select **Organization > Access > Auth Policies**.

A list of existing rules, if any, appears.

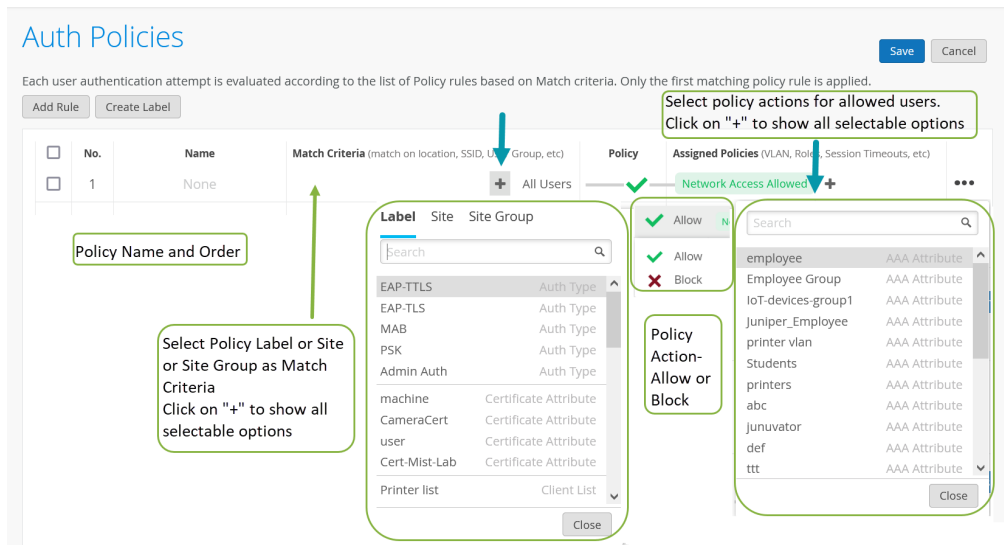


**NOTE:** The Hit Count column on the Auth Policies page displays the number of NAC events for each rule. You can filter the hit count information for the last 60 minutes, last 24 hours, last 7 days, yesterday, today, this week, or for a custom date or range.

2. On the Auth Policies page, click **Add Rule** to add a new rule.  
The system inserts a new row allowing you to add a new policy.
3. Click the field in the Name column and enter a policy name. Then click the blue check mark to apply your changes.

The following figure shows the options that you use to configure an authentication policy.

Figure 35: Authentication Policy Configuration Options



Select Policy Label, Site, or Site Groups as the the match criteria. Click Add (+) to see the available options.

Select **Allow** or **Block** to specify the policy action.

Specify the assigned policy for the allowed users. Click Add (+) to see the available options.

The following table explains the options that you use to configure an authentication policy.

Table 8: Authentication Policy Options

Field	Description
No.	Abbreviation for <i>number</i> . The authentication policy number. This entry indicates the position of the authentication policy.
Name	You can use up to 32 characters including alphanumeric characters and special characters underscore and dash.
Match Criteria	Match criteria for the policy. You can select labels, sites, or site groups from the available list. Click the + icon to display the list. If you have created policy labels, the Juniper Mist portal displays the detail in the drop-down menu.

Table 8: Authentication Policy Options (*Continued*)

Field	Description
Policy	Policy actions. Select one of these policy actions: <ul style="list-style-type: none"> <li>• Allow</li> <li>• Block</li> </ul>
Assigned Policy	Apply policy actions for the allowed users. With policy actions, you can assign additional attributes such as roles or VLANs to the allowed users. If you have created policy labels, the Juniper Mist portal displays the labels when you click the + icon.

4. Click **Save** to save your changes for the policy.

#### SEE ALSO

[Configure Authentication Policy Labels | 72](#)

[NAC Events | 138](#)

[Juniper Mist Access Assurance Use Cases | 6](#)

[Juniper Mist Access Assurance Authentication Methods | 8](#)

[Configure Certificate-Based \(EAP-TLS \) Authentication | 83](#)

[Configure Credentials-Based \(EAP-TTLS\) Authentication | 106](#)

## Configure Authentication Policy Labels

#### IN THIS SECTION

- [Create Labels | 73](#)

A network access control policy is a set of rules and guidelines for providing secure access to the devices that attempt to connect to a network. A policy consists of certain criteria that devices and users must fulfill to get access to the network and use network resources.

You can configure Juniper Mist Access Assurance with an authentication policy to enable Juniper Mist-managed devices to connect the clients to the network or applications.

Juniper Mist leverages "Labels" as policy matching criteria and the uses labels apply the relevant policy actions that specify permission. That is, when you create authentication policies, you can use the labels as:

- **Match criteria:** A set of match criteria that must be satisfied to apply the policy rule.
- **Policy permit action:** A set of actions to apply in case of a match—such as applying additional attributes (VLAN, role, and group-based policy tag).

## Create Labels

You can create labels on the following pages:

- Authentication Policies
- Authentication Policy Labels

To create labels in the Authentication Policy Labels page:

1. On the Juniper Mist portal, from the left menu, select **Organization > Access > Auth Policy Labels**.  
A list of existing labels, if any, appears.
2. On the Auth Policy Labels, click **Add Labels** and enter the following details:
  - **Label Name**—Enter a unique name for the label. You can use up to 32 characters including alphanumeric characters and one or more of the special characters.
  - **Label Type**—Specify the label type. See the information in [Table 9 on page 74](#) to select the label type.



Table 9: Parameters for New Label

Label Type	Details	Role in Authentication Policy Rule
AAA Attribute	<p>A group of user attributes that works as the match criteria and helps determine the policy action that specifies permission.</p> <p>Options:</p> <ul style="list-style-type: none"> <li>• Role</li> <li>• VLAN</li> <li>• Realm</li> <li>• User Name</li> <li>• GBP Tag</li> <li>• Session Timeout (sets the maximum time allowed before user sessions are reset, from 3600 to 604800 seconds).</li> <li>• Custom Vendor Specific Attribute (these are returned in the Access-Accept message, for example, <i>Sec-Admin-Role=superuser</i>, and can be modified with additional attributes).</li> <li>• Custom Standard RADIUS Attribute (these are standard IETF RADIUS attributes such as <i>Idle-Timeout=600</i> or <i>Termination-Action=RADIUS-Request</i>, and can be modified with additional attributes).</li> <li>• Dynamic Wired Port Configuration (these are VLAN names that Access Assurance returns for the RADIUS</li> </ul>	Match criteria and policy permit action

Table 9: Parameters for New Label (*Continued*)

Label Type	Details	Role in Authentication Policy Rule
	<p>attribute <i>Egress-VLAN-Name</i> in Access-Accept message, and are especially useful with dynamic port configurations, for example to automatically use trunk ports for AP connections or to differentiate between tagged and untagged VLANs).</p>	
Certificate Attribute	<p>A group of user or device certificate fields used during authentication.</p> <p>Options:</p> <ul style="list-style-type: none"> <li>• Common Name (CN)</li> <li>• Subject</li> <li>• Serial Number</li> <li>• Issuer</li> <li>• Subject Alternative Name (SAN)</li> </ul>	Match criteria
Client List	<p>A list of MAC addresses or MAC Organizationally Unique Identifiers (OUIs) identified by wildcard values. Examples: 1122AA33BB44 or 11-22-AA-33-BB-44 or 11-22-AA*</p> <p>For devices that don't support 802.1X, you can use <b>Client Lists</b> to allow approved devices access the network.</p>	Match criteria

Table 9: Parameters for New Label (*Continued*)

Label Type	Details	Role in Authentication Policy Rule
SSID	SSID name used during user or device authentication, based on the incoming called station identifier attribute. You can combine multiple SSIDs in one label using comma-separated values.	Match criteria
Directory Attribute	User group membership. The identity provider (IdP) provides user group information during user or device authorization.	Match criteria

3. Click **Create** to save your settings for the new label.

The labels you create in this task become available for you to select as match condition or policy permit action when you create authentication policies.

#### SEE ALSO

[Configure Authentication Policy | 69](#)

[Juniper Mist Access Assurance Use Cases | 6](#)

[Juniper Mist Access Assurance Authentication Methods | 8](#)

[Configure Certificate-Based \(EAP-TLS\) Authentication | 83](#)

[Configure Credentials-Based \(EAP-TTLS\) Authentication | 106](#)

## Juniper Mist Access Assurance Endpoints

#### IN THIS SECTION

- [Adding Endpoints | 77](#)
- [Example of Using NAC Endpoint Label in Auth Policy | 78](#)

Network access control (NAC) Endpoints page provides you with database of endpoints identified by their MAC addresses. Here, you can assign each endpoint with various attributes, such as name, VLAN, role and client label. Once an endpoint is labeled, you can leverage the label name in your authentication policy page as match criteria.

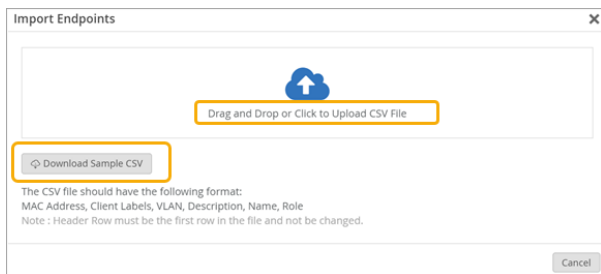
You can add or import a new endpoint to the database manually or by uploading a CSV file. Having a database of endpoints MAC addresses simplifies the access control using MAC authentication as now you can easily add new clients, assign respective labels, view, and edit existing clients by leveraging search functionality.

## Adding Endpoints

Use the following steps to set up endpoints for NAC:

1. To access NAC Endpoints page, from the left menu of the Juniper Mist portal, select **Organization > Access > Endpoints**.
2. A list of existing endpoints, if any, appears. You can search the endpoint by MAC address or by label.
3. You can Import an endpoint using a CSV file or add an endpoint.
  - a. Click the **Import** button in the upper right corner.

**Figure 36: Import NAC Endpoints**



In the Import Endpoint window, click **Download Sample CSV** button to download a sample CSV file with correct headers and format. Upload your CSV file to the portal using the **Drag and Drop or Click to Upload CSV File** option.

- b. Click the **Add Endpoint** button to add new endpoint.

**Figure 37: Create a NAC Endpoint**

The screenshot shows a web form titled "Add Endpoint". The fields are as follows:

- Name:** Camera1-Floor1
- MAC Address:** 112233441122
- Role:** (empty)
- VLAN:** (empty)
- Client Labels:** Camera, floor, Hold Label
- Description:** I

Buttons: Save, Cancel

In the Add Endpoint page, enter the following details:

- **Name**—(Optional) Name of the endpoint. You can also name the endpoint after authentication for better visibility. Naming is also done by sending configured name in User-Name attribute in RADIUS Access Accept.
- **MAC Address**—MAC Address of the endpoint.
- **Role**—(Optional) Role to an endpoint which can be leveraged in Auth Policy rule to override a role on a per-endpoint basis.
- **VLAN**—(Optional) VLAN ID between 1 to 4094 or VLAN name to an endpoint, which can be used to override VLAN assignment on a per-endpoint basis.
- **Client Labels**—(Optional) List of labels or tags assigned to an endpoint, which can be leveraged in Auth Policies as a match criteria. For example, cameras, printers, IoT-devices, quarantined-clients, floor, and so on.
- **Description:** (Optional) Description of the endpoint that you can relate with.

4. Click **Save**.

The system adds the endpoint you created to the database. Now you can use the label in creating an authentication policy.

## Example of Using NAC Endpoint Label in Auth Policy

In the previous step, you have created an endpoint with labels cameras and floor 1. Now, you can use the labels in auth policy.

1. From the left menu of the Juniper Mist portal, select **Organization > Access > Auth Policies**.

2. On the Auth Policies page, select **Create Label** and enter the details.

**Figure 38: Create a NAC Endpoint**

- Label Name—Enter the label name (example: Cameras in floor 1)
  - Label Type—Select the type as **Client Label**.
  - Label Values—Enter client label. For this example, enter label values as cameras, floor 1. These are the labels you assigned when adding a new NAC endpoint.
3. Create an authentication policy.
    - a. Click **Add Rule** to create a rule. In this rule, use the label you created in the previous step.

**Figure 39: Create Auth Policy**

ID	Name	Match Criteria	Policy	Assigned Policies
19	TMO Cable Modem	Label-modem, MAB, Wired	Network Access Allowed	TMO Uplink
20	Switch CLI Auth	Client Label, MAB, Wired	Network Access Allowed	Cisco CLI - Supervisor, Juniper Mgmt Superser, Palo Employee Group
21	Juniper Switch CLI Auth	Client Label, MAB, Wired	Network Access Allowed	Juniper Mgmt Superser
22	Admin Login	Client Label: cameras, floor1, Palo Alto	Network Access Allowed	Palo Employee Group
23	Cameras in Floor1	Cameras in Floor1, MAB, Wired	Network Access Allowed	Camera-VLAN-Floor1

- b. **Name**—Enter a name for the policy.
- c. **Match Criteria**—Select the client label (cameras, floor 1), MAB (MAC Authentication Bypass), and Wired.
- d. **Policy**—Select Allowed.
- e. **Policy action**—Select **Network Access Allowed**.
- f. **Assigned Policies**—Select the required policy.

## RELATED DOCUMENTATION

[Juniper Mist NAC Architecture | 4](#)

---

[Juniper Mist Access Assurance Use Cases | 6](#)

---

[Juniper Mist Access Assurance Best Practices | 14](#)

---

[Juniper Mist Access Assurance Authentication Methods | 8](#)

---

[Mist Access Assurance—Frequently Asked Questions | 16](#)

# 4

CHAPTER

## Access Assurance Configuration

---

### SUMMARY

Use the information in this topic to get started with configuring Juniper Mist Access Assurance in Juniper Mist Cloud portal. This configuration facilitates identity-based network access for both devices and users.

### IN THIS CHAPTER

- Configure Certificate-Based (EAP-TLS ) Authentication | **83**
  - Configure MAC-Based Authentication and MAC Authentication Bypass (MAB) | **89**
  - Configure Certificate-Based (EAP-TLS ) Authentication with Azure IdP Integration | **95**
  - Configure Credentials-Based (EAP-TTLS) Authentication | **106**
  - Configure Client Device for EAP-TTLS Authentication | **109**
  - TEAP Configuration for Windows Client | **114**
  - Install Juniper Mist Edge VM for Juniper Mist Authentication Proxy | **118**
  - Enable Client Onboarding with a BYOD PSK Portal | **128**
-



# Configuration Overview



Video: [Simple EAP-TLS Authentication Configuration](#)

## What Do You Want to Do?

Table 10: Top Tasks

If you want to...	Use these resources:
<p><b>Understand your use case</b>  <i>Understand different use cases supported by Juniper Mist Access Assurance.</i></p>	<ul style="list-style-type: none"> <li>• <a href="#">"Use Case" on page 6</a></li> <li>• <a href="#">"Authentication Methods" on page 8</a></li> </ul>
<p><b>Enable Mist Authentication</b>  <i>Use WLAN templates for wireless devices and use switch templates for wired clients.</i></p>	<p><a href="#">"Configure Certificate-Based (EAP-TLS ) Authentication" on page 83</a></p>
<p>Configure certificates  <i>Manage trusted certificate authorities and Mist access assurance server certificate configuration.</i></p>	<p><a href="#">"Use Digital Certificates" on page 64</a></p>
<p><b>Configure identity providers</b>  <i>Integrate Juniper Mist cloud with an external identity provider and enable your organization to use a SAML identity provider or you can configure an LDAP server connection.</i></p>	<p><a href="#">"Add Identity Providers for Juniper Mist Access Assurance" on page 56</a></p>
<p><b>Create policies</b>  <i>Configure an authentication policy to authenticate end users or devices.</i></p>	<ul style="list-style-type: none"> <li>• <a href="#">"Configure Authentication Policy Labels" on page 72</a></li> <li>• <a href="#">"Configure Authentication Policy" on page 69</a></li> </ul>

Table 10: Top Tasks (Continued)

If you want to...	Use these resources:
<p><b>View connected clients and troubleshoot any issues</b></p> <p><i>Validate connected client devices and get further details on user access and authentication in Juniper Mist portal.</i></p>	<p><a href="#">"Validate Access and Authentication" on page 143</a></p>

## RELATED DOCUMENTATION

[Juniper Mist NAC Architecture | 4](#)

[Juniper Mist Access Assurance Use Cases | 6](#)

[Juniper Mist Access Assurance Best Practices | 14](#)

[Juniper Mist Access Assurance Authentication Methods | 8](#)

[Mist Access Assurance—Frequently Asked Questions | 16](#)

# Configure Certificate-Based (EAP-TLS ) Authentication

## IN THIS SECTION

- [Configure Certificate-Based \(EAP-TLS\) Authentication for Wireless Network | 84](#)
- [Configure Certificate-Based \(EAP-TLS\) Authentication for Wired Network | 86](#)

When you set up a wireless or wired connection, an important step is to configure secure network access. With Juniper Mist Access Assurance, you can set up an authentication method using 802.1X.

Extensible Authentication Protocol–Transport Layer Security (EAP-TLS), one of the protocols that support 802.1X authentication, verifies both client and server certificates at each point of the

communication path. This authentication method uses trusted digital certificates to validate users and provide seamless network access.

In the following tasks, you configure certificate-based EAP-TLS authentication on the Juniper Mist cloud portal. With this configuration, you can provide access to all clients that present trusted certificates in a wireless or wired network.

## Prerequisites

- You must obtain digital certificates, that is source X.509 certificates, from certificate authorities (CAs), which are trusted third parties, or generate the certificates internally.
- You must configure the client device as a supplicant that a RADIUS server can authenticate using 802.1X. You typically configure clients by using mobile device management (MDM) or group policies in production deployments.
- Your network must have Juniper® Series of High-Performance Access Points to perform wireless client authentication.
- Configure the public or private enterprise TLS-server certificate that the cloud RADIUS server will use.
- Get familiar with the following procedures:
  - ["Use Digital Certificates" on page 64](#)
  - ["Configure Authentication Policy Labels" on page 72](#)
  - ["Configure Authentication Policy" on page 69](#)

## Configure Certificate-Based (EAP-TLS) Authentication for Wireless Network

To set up certificate-based authentication in a wireless network using the Juniper Mist portal:

1. Import a trusted root certificate authority (CA). Juniper Mist uses the CA-generated certificate as a server certificate.
  - a. On Juniper Mist portal, click From the left menu of the Juniper Mist portal, select **Organization > Access > Certificates**. The Certificates page displays the list of already added certificates (if any). The Certificates page appears displaying the list of already added certificates (if any).

- b. Click **Add Certificate Authority** to import your certificate. If you've configured your public key infrastructure (PKI), import your root and intermediate CAs. See ["Use Digital Certificates" on page 64](#).

Once you import a CA, an authenticating server trusts any client certificate issued by this CA.

Similarly, a client device validates a server certificate by verifying whether it is signed by a trusted CA that you've added.

## 2. Create authentication policies.

Without any authentication policies, the servers reject all attempts by clients to connect to the network. To allow connections from valid clients, you need to add appropriate rules to set up the authentication policies.

- a. From the left menu of the Juniper Mist portal, select **Organization > Access > Auth Policies** to create a new rule to provide access to clients with valid certificates. .

See ["Configure Authentication Policy" on page 69](#).

- b. Define an authentication policy with the following details. Select the required option for each field from the respective drop-down lists. The following list shows sample inputs.

- i. Name—Enter a name for the policy.
- ii. Match Criteria—Select **EAP-TLS**.
- iii. Policy—Select **Allowed**.
- iv. Assigned Policies—Select **Network Access Allowed**.

## 3. Configure the SSID.

Wireless LANs (WLANs) are modular elements and each WLAN contains the configuration for a given service set identifier (SSID).

- a. From the left menu of the Juniper Mist portal, select **Organization > Wireless > WLAN Templates**.

On the WLAN Templates page, either click an existing template to open its configuration page or click **Create Template** in the upper-right corner of the page to create a template.

- b. On the WLAN Templates page, click Add WLAN.

- c. Give the SSID a name. Typically, this name is the same as the WLAN name.

- d. Select an option for each of the following fields:

- Security Type— Select **Enterprise (802.1X)**. Additionally select either **WPA2** or **WPA3**.
- Authentication Server—**MIST auth**.
- VLAN—Specify the type of VLAN the AP will use in the switch connection.

Now the SSID configuration is complete.

e. Click **Create**.

4. On the WLAN Templates page, under **Applies To**, select either **Entire Org** or **Site/Site Groups**.

The following videos show how to configure certificate-based (EAP-TLS) authentication for wireless networks.



Video: [Simple EAP-TLS Authentication Configuration](#)



Video: [Access Assurance Demo Contrasting Against 2 Other Solutions](#)

Now your network is ready to securely authenticate clients by using EAP-TLS. The Juniper Mist cloud verifies the client certificates and grants access and authorization based on the authentication policy configuration.

You can view the associated clients on the Juniper Mist portal in:

- Select **Clients > Wired Clients** to see client details
- Select **Monitor > Service Levels > Insights** to view client events.

## Configure Certificate-Based (EAP-TLS) Authentication for Wired Network

To set up certificate-based authentication for a wired network by using the Juniper Mist portal:

1. Import a trusted root certificate authority (CA). Juniper Mist uses the CA-generated certificate as a server certificate. See "[Use Digital Certificates](#)" on page 64 for details.
2. Create authentication policies.
  - a. From the left menu of the Juniper Mist portal, select **Organization > Access > Auth Policies**.  
Create a new rule to allow access to clients with valid certificates. See "[Configure Authentication Policy](#)" on page 69.  
Define an authentication policy with the following details. Select the required option for each field from the respective drop-down lists.
    - i. Name—Enter a name for the policy.
    - ii. Match Criteria—Select **EAP-TLS**.
    - iii. Policy—Select **Allowed**.
    - iv. Assigned Policies—Select **Network Access Allowed**.
3. Configure the switch.

- a. From the left menu of the Juniper Mist portal, select **Organization > Wired > Switch Templates**.  
On the Switch Templates page, either click an existing template to open its configuration page or click **Create Template** in the upper-right corner of the page to create a template.
- b. In the Authentication Servers section, select **Mist Auth** as the authentication server.
- c. Scroll down to the Port Profile section and select:
  - In the Mode field, select **Access**.
  - Enable the Use dot1x authentication option.
- d. Assign the port profile to each port of the switch where the connected wired clients require network access.  
In the Select Switches Configuration section on the Port Configuration tab, click **Add Port Range** to associate a port profile with a port.

**Figure 40: Assign Port Profile to Port Ranges on a Switch**

The screenshot shows a 'New Port Configuration' dialog box with the following fields and options:

- Port IDs:** A text input field containing 'ge-0/0/9'. Below it, a hint text reads '(ge-0/0/1, ge-0/0/4, ge-0/1/1-23, etc)'. There is a checkmark icon in the top right of the dialog.
- Configuration Profile:** A dropdown menu showing 'hardwiredport' and a secondary dropdown showing 'room101(101), access' with a downward arrow.
- Enable Dynamic Port Configuration:** An unchecked checkbox.
- Description:** A large text area with the placeholder text 'Add Description'.
- Up / Down Port Alerts:** A section with an information icon. It has two radio buttons: 'Enabled' (unchecked) and 'Disabled' (checked). Below it is a link: 'Manage Alert Types in Alerts Page'.
- Port Aggregation:** Two radio buttons: 'Enabled' (unchecked) and 'Disabled' (checked).
- Allow switch port operator to modify port profile:** Two radio buttons: 'Yes' (unchecked) and 'No' (checked).

- e. Click **Save**.

For procedure on leveraging certificate attributes to create an authentication policy, watch the following video:



**Video:** [EAP-TLS Leveraging Certificate Attributes to Create Auth Policies](#)

Now your network can use EAP-TLS to securely authenticate clients. The Juniper Mist cloud verifies the client certificates and grants access and authorization based on the authentication policy configuration.

You can view the associated clients on the Juniper Mist portal.

- Select **Clients > Wired Clients** to see client details
- Select **Monitor > Service Levels > Insights** to view client events.

Watch the following video to learn how to configure a Windows client device for EAP-TLS authentication for test or lab usage:



**Video:** [Manual Network Configuration for Lab Use - EAP-TLS for Windows](#)

Watch the following video to learn how to configure an Android client device for EAP-TLS authentication for test or lab usage:



**Video:** <https://mist.wistia.com/embed/iframe/zs88vs3piv>

## SEE ALSO

[Configure Authentication Policy | 69](#)

[Configure Authentication Policy Labels | 72](#)

[Use Digital Certificates | 64](#)

[Configure Certificate-Based \(EAP-TLS \) Authentication with Azure IdP Integration | 95](#)

# Configure MAC-Based Authentication and MAC Authentication Bypass (MAB)

## IN THIS SECTION

- [Configure MAC-Based Authentication for Wired Device | 89](#)

MAC authentication is used to authenticate devices based on their physical MAC addresses. You can use MAC authentication along with certificate-based or credential-based authentication as an additional layer of security.

Juniper Mist Access Assurance supports MAC Authentication Bypass (MAB) for uniform access control across wired and wireless networks. This topic provides an example for configuring MAB for a wired device.

The example shows you how to create MAC authentication for a wired device in addition to certificate-based EAP-TLS authentication. The task also includes the steps to create an authentication policy for a wired-side device that does not support dot 1x (such as a Phillips hub).

## Prerequisites

- You must have already configured certificate-based authentication. See "[Configure Certificate-Based \(EAP-TLS\) Authentication for Wireless Network](#)" on page 84
- A Juniper Networks EX Series Switch.

## Configure MAC-Based Authentication for Wired Device

Learn how to configure and validate MAC-based authentication for wired devices by watching the following videos:



Video: [Wired Authentication Using Mist Access Assurance](#)



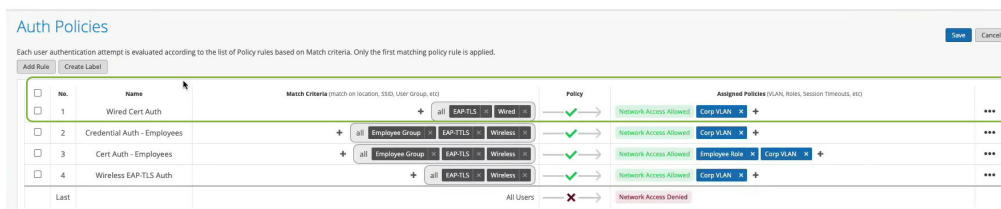


### Video: [Wired Authentication Validation](#)

Use the following steps to set up MAC-based authentication in a network using the Juniper Mist portal:

1. Create authentication policies.
  - a. From the left menu of the Juniper Mist portal, select **Organization > Access > Auth Policies**. Create a new rule to provide access to clients with valid certificates. See "[Configure Authentication Policy](#)" on page 69.

**Figure 41: Create Auth Policy for Wired Client**



Define an authentication policy with the following details:

- i. Name—Enter the name for the policy (ex: Wired Cert Auth)
  - ii. Match Criteria—Select **EAP-TLS** and **Wired**.
  - iii. Policy—Select **Allowed**
  - iv. Policy action—**Network Access Allowed**
  - v. Assigned VLAN—Corp VLAN
2. To provide authentication for a non-dot1.x device on the LAN side, create a new policy label.
    - a. On the Auth Policies page, select **Create Label** and enter the details.

Figure 42: Label for Non-Dot1x device

The screenshot shows a 'Create Label' dialog box with the following fields and content:

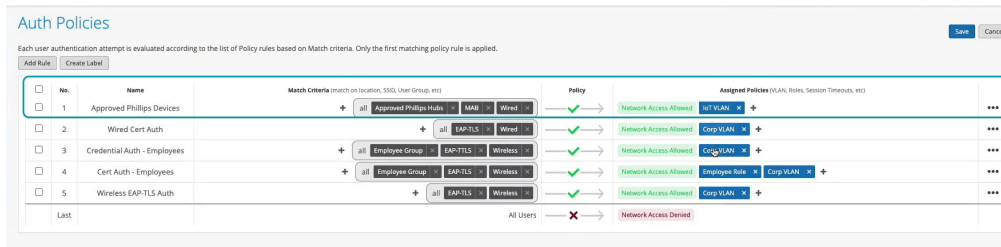
- Label Name:** A text input field containing 'Approved Phillips Hubs'.
- Label Type:** A dropdown menu set to 'Client List'. Below it is a note: 'This label can be used in the Match section of the Auth policy rule to match on a list of MAC addresses or MAC OUIs identified by wildcards.'
- Label Values:** A section titled 'Label Values' with a sub-header 'Client MAC Address (Example: 1122AA33BB44 and/or 11-22-AA-33-BB-44 and/or 11-22-AA\*)'. It contains a list of MAC addresses with one entry 'ecb5:fa:a2:50:40' and an 'Add MAC Address' button.
- Buttons:** 'Create' and 'Cancel' buttons at the bottom right.

Enter the following information in the respective fields:

- i. Label Name—Enter the label name (example: Approved Phillips Hubs)
  - ii. Label Type—Select the type Client List
  - iii. Label Values—Enter MAC address of the device
3. Create a new authentication policy.
    - a. Click **Add Rule** to create a new rule.
 

In this rule, use the label you created in the previous step for non-dot1x device. In this rule, use the label you created in the previous step for a non-dot1x device.

**Figure 43: Authentication Policy for Non-Dot1X devices**



Enter the following information in the respective fields:

- i. Name—Enter **Name**. Example: Approved Phillips Devices.
- ii. Match Criteria—Select **Approved Phillips Hubs**, **MAB (MAC Authentication Bypass)**, and **Wired**.
- iii. Policy—Select **Allowed**.
- iv. Policy action—Select **Network Access Allowed**.
- v. Assigned Policies—Select **IoT VLAN**.

Now you have created a policy to authenticate non-dot1X device.

4. Configure the switch to perform the authentication.
  - a. From the left menu of the Juniper Mist portal, select **Organization > Wired > Switch Templates**.
  - b. On the Switch Templates page, either click an existing template to open its configuration page or click **Create Template** in the upper-right corner of the page to create a template.
  - c. In the Authentication Servers section, select **Mist Auth** as the authentication server.
  - d. Scroll down to the Port Profile section and enter the details.

Figure 44: Port Profile Options

New Port Profile ✓ ✕

Name

Port Enabled  
 Enabled  Disabled

Description

---

Mode  
 Trunk  Access

Port Network (Untagged/Native VLAN)  
 1 ▾

VoIP Network  
 ▾

---

Use dot1x authentication  
 Mac authentication  
 Mac authentication only  
 Use Guest Network  
 Bypass authentication when server is down

Speed  
 ▾

Duplex  
 ▾

Mac Limit  
  
(0 - 16383, 0 => Unlimited)

PoE  
 Enabled  Disabled

STP Edge  
 Yes  No

QoS  
 Enabled  Disabled

Enable MTU

Enter the required information or select the required options in the following fields:

- i. Name—Enter a name (for example: **secure-port**).
- ii. Mode—Select **Access**.
- iii. Enable the **Use dot1x authentication** and **Use MAC authentication** options. If the client device supports 802.1X, the switch port performs 802.1X authentication. If the client device does not support 802.1X, the switch port performs MAC authentication.
- iv. STP Edge—Select **Yes** to configure the port as a Spanning Tree Protocol (STP) edge port. This setting ensures that the port is treated as an edge port.

This example uses the default values for the remaining fields.

- e. Assign a port profile to each port of the switch where the connected wired clients require network access.

In the Select Switches Configuration section, on the Port Config tab, click **Add Port Range** to associate a port profile with a port.

**Figure 45: Assign Port Profile to Port Ranges on a Switch**

Apply port profiles to port ranges on matching switches

New Port Range ✓ ✕

Port Aggregation

Allow switch port operator to modify port profile

Yes  No

Port IDs

ge-0/0/1-11

(ge-0/0/1, ge-0/0/4, ge-0/1/1-23, etc)

Configuration Profile

secure-port default(1), access, edge ▾

Enable Dynamic Configuration

Enable "Up/Down Port" Alert Type ⓘ

[Manage Alert Types in Alerts Page](#)

Description

Add Description

Enter a port ID and select the configuration profile that you created in the previous step.

- f. Click **Save**.

Now your network is ready to securely authenticate clients. The Juniper Mist cloud verifies the client certificates and grants access and authorization based on the authentication policy configuration.

You can view the associated clients on the Juniper Mist portal.

- Select **Clients > Wired Clients** to see client details
- Select **Monitor > Service Levels > Insights** to view client events.

#### SEE ALSO

[Configure Authentication Policy | 69](#)

[Configure Authentication Policy Labels | 72](#)

[Use Digital Certificates | 64](#)

[Configure Certificate-Based \(EAP-TLS \) Authentication with Azure IdP Integration | 95](#)

## Configure Certificate-Based (EAP-TLS ) Authentication with Azure IdP Integration

#### IN THIS SECTION

- [Configure Certificate-Based \(EAP-TLS\) Authentication for Wireless Network | 97](#)
- [Create Authentication Policy Based on Group Details | 101](#)
- [Create an Authentication Policy in a WLAN Template | 103](#)

We can extend the Extensible Authentication Protocol–Transport Layer Security (EAP-TLS) authentication process through the integration of an external identity provider (IdP). With this integration, an IdP validates an EAP-TLS authentication exchange and ensures that only trusted users have network access. By introducing an additional verification through IdP integration with EAP-TLS authentication, you can enhance the robustness of network access control (NAC).

In Juniper Mist™, you can integrate Microsoft Azure Active Directory (AD), now known as Microsoft Entra ID, as identity provider using OAuth. This integration allows you to leverage Azure AD as an identity provider in combination with Mist Access Assurance and perform:

- Authenticate users via EAP-TTLS by doing delegated authentication checking username and password via OAuth.
- Obtain user group memberships to leverage them in authentication policies.
- Obtain user account state information (active / suspended).
- Authorize users via EAP-TLS or EAP-TTLS.

Azure AD returns the following details that you can use to fine-tune your authentication policies in Juniper Mist Access Assurance:

- Group memberships: Information about the groups to which an user belongs provides insights about user roles and permissions.
- Account validation: Account status is essential to ensure that Juniper Mist Access Assurance grants network access only to valid active users.
- Additional user context: Gathering additional information about users allows us to better understand the user's profile. When you configure identity provider lookup, the system sends an API request to the configured identity provider to fetch additional context for the authenticated user.

## Overview

This task shows you how to look up the Azure AD for the common name (CN) associated with a specific domain name when you evaluate a certificate. The results from Azure AD look up fetch additional information about the user which you'll use to define the authentication policy. This task is applicable for a wireless network.

As a prerequisite for this task, you must configure EAP-TLS authentication. See ["Configure Certificate-Based \(EAP-TLS\) Authentication" on page 83](#) for details.

In this example, you'll:

1. Create a new application on the Azure portal to use Azure AD as an IdP.
2. Integrate Azure AD as an IdP and grant API permissions in Microsoft Graph for the registered application.
3. Retrieve details about users logged in to the Juniper Mist portal.
4. Further refine the authentication policy with the additional details that the IdP fetches about users who are logged in.

To create authentication using Okta as an IdP, watch the following video:

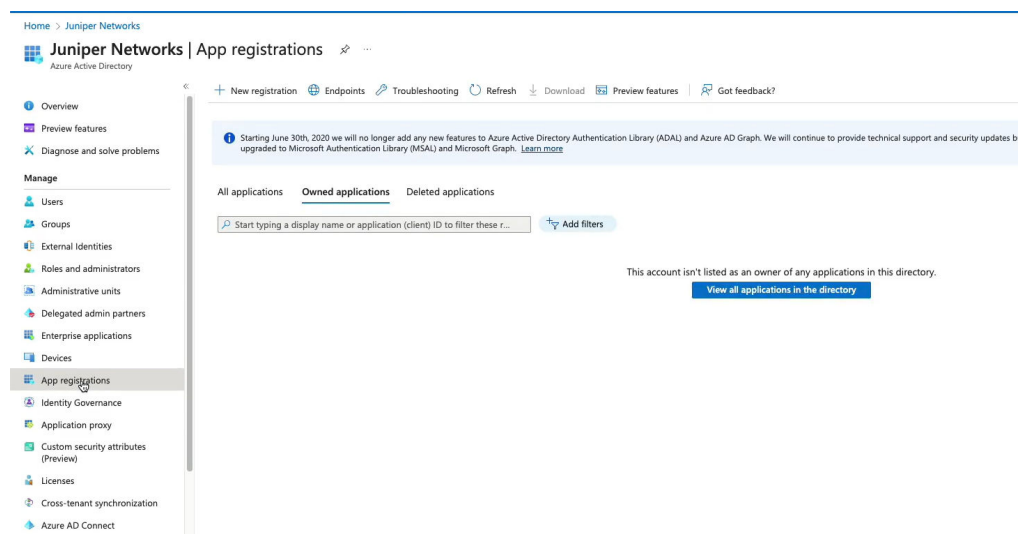


Video: [Access Assurance Demo Contrasting Against 2 Other Solutions](#)

## Configure Certificate-Based (EAP-TLS) Authentication for Wireless Network

1. On the Microsoft Azure portal, set up an IdP connector on Azure AD.
  - a. Use your credentials to sign in to the [Azure portal](#) and navigate to your Azure AD.
  - b. From the left-navigation bar, select **App registrations**.

Figure 46: New Application Registration



If you have already registered your application, go to the **Owned Applications** tab. Click the application name to see details such as client ID, tenant ID, and client secret.

If you want to register a new application on the Azure portal, click the **New registration** tab.

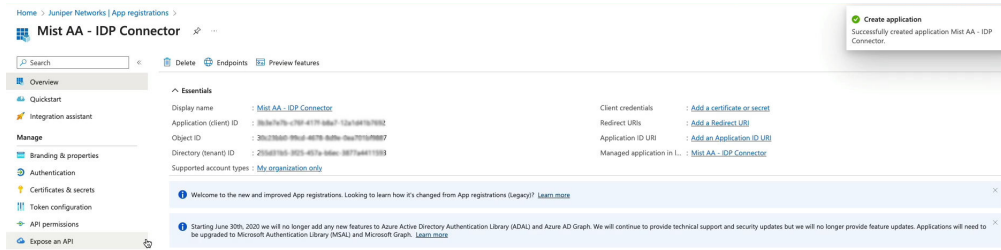
In the New Registration page, enter the required information in the following fields. Note that the Name field in the following list shows sample user input.

- **Name**—Enter **Mist AA IDP connector**
  - **Supported Account Type**—Select **Accounts in this organization directory only**.
- c. Click **Register** to continue.
 

A page appears displaying information about the newly created connector as shown in [Figure 47](#) on [page 98](#).



Figure 47: New Application Details



d. Note down the following details, which you will need to set up an IdP connector on the Juniper Mist portal:

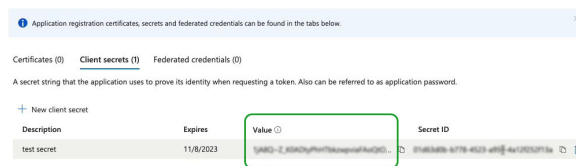
- Application (Client) ID—You'll need to enter this information in the **OAuth Client Credential (CC) Client ID** and **Resource Owner Password Credential Client ID** fields.
- Directory (Tenant) ID—You need this information for the **OAuth Tenant ID** field.

e. On the left-navigation bar, select **Certificates and Secrets > New Client Secret**. Enter the following details and click **Add**.

- Name
- Expiry time

The system generates **Value** and **Secret ID** as shown in [Figure 48 on page 98](#).

Figure 48: Client Secret Details



Note down the information in the Value field. You need this information for the **OAuth Client Credentials Client Secret** field in the Juniper Mist portal while adding Azure AD as an IdP.

2. Grant delegate permissions and application permissions to the Azure AD application. With these permissions, the application can read users, groups, and directory information.

a. On the Azure portal page for the registered application, in the left-navigation bar, select **API permissions > Add a permission**.

You must give your application the required access permissions to use Microsoft Graph API to fetch information about users.

b. On the Add a permission page, under Microsoft Graph, add the following permissions on the **Delegated Permissions** and **Application Permissions** tabs.

- • Directory.Read.All
- Group.Read.All
- User.Read
- User.Read.All

Click **grant admin consent for your AD** as shown in [Figure 49 on page 99](#).

**Figure 49: API Permissions for Application**

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission **Grant admin consent for Juniper Networks**

API / Permission name	Type	Description	Admin consent req...	Status
Microsoft Graph (7)				...
Directory.Read.All	Delegated	Read directory data	Yes	Granted for Juniper Net...
Directory.Read.All	Application	Read directory data	Yes	Granted for Juniper Net...
Group.Read.All	Delegated	Read all groups	Yes	Granted for Juniper Net...
Group.Read.All	Application	Read all groups	Yes	Granted for Juniper Net...
User.Read	Delegated	Sign in and read user profile	No	Granted for Juniper Net...
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Juniper Net...
User.Read.All	Application	Read all users' full profiles	Yes	Granted for Juniper Net...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Application permissions are required for the application to operate in your Azure AD. Delegated permissions are essential when your connector uses username and password for authentication.

3. On the Juniper Mist portal, add Azure AD as an identity provider.
  - a. On the Juniper Mist portal, from the left menu select **Organization > Access > Identity Providers**. The Identity Providers page appears displaying a list of configured IdPs (if any).
  - b. Click **Add IDP** to add a new IdP.
  - c. On the **New Identity Provider** page, enter the required information as shown in [Figure 50 on page 100](#).

Figure 50: Add Azure AD as Identity Provider

The screenshot shows the Mist web interface for configuring a new identity provider. The sidebar on the left contains navigation icons for Monitor, Marvis, Clients, Access Points, Switches, WAN Edges, Mist Edges, Private 5G, Location, Analytics, Site, and Organization. The main content area is titled "Identity Providers: New Identity Provider" and contains the following fields and options:

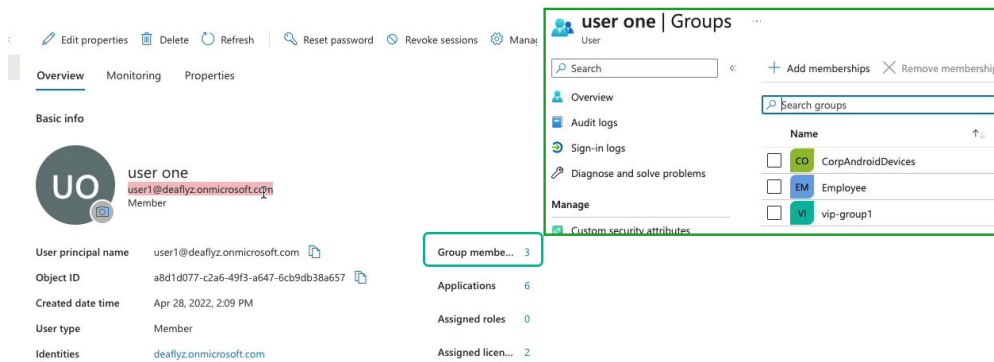
- Name:** A text input field containing "Azure AD".
- Configuration:**
  - IDP type:** Radio buttons for "LDAPs" and "OAuth", with "OAuth" selected.
  - OAuth Type:** A dropdown menu set to "Azure".
  - OAuth Tenant ID:** A text input field containing "2f5a271b5-3025-467a-bd6e-3877a6411593".
  - Domain Names:** A text input field containing "deaflyz.onmicrosoft.com".
  - Default IDP:** An unchecked checkbox.
  - OAuth Client Credential (CC) Client id:** A text input field containing "3b13e7e7b-c76f-417f-bd6e-12a7d81b7692".
  - OAuth Client Credential (CC) Client Secret:** A masked text input field with a "Reveal" link.
  - OAuth Resource Owner Password Credential (ROPC) Client id:** A text input field containing "3b13e7e7b-c76f-417f-bd6e-12a7d81b7692".

- i. **Name**—Enter an IdP name (In this example, use Azure AD)
- ii. **IDP Type**—Select **OAuth**.
- iii. **OAuth type**—Select **Azure** from the drop-down list.
- iv. **OAuth Tenant ID**—Enter the Azure AD tenant ID.
- v. **Domain Names**—Enter the domain name, that is, the user's username (for example: username@domain.com). The domain name field examines incoming authentication requests, identifying the respective username and associated domain. After setting up the domain name for a connector, the connector can identify the Azure tenant it needs to communicate with.
- vi. **OAuth Client Credential (CC) Client id**—Enter the client ID of the registered Azure AD application.
- vii. **OAuth Client Credential (CC) Client secret**—Azure AD application secret. Azure AD application secret. Enter the value component of the client secret that the Azure portal generated for the IdP connector.
- viii. **OAuth Resource Owner Password Credential (ROPC) Client id**— Enter the Azure AD application ID. This ID is the same as the OAuth client credential client ID.

When you authenticate a user by using EAP-TLS, Juniper Mist matches the username to the specified domain name. Juniper Mist sends an API request to the corresponding Azure AD tenant to fetch the details for that user.

Figure 52 on page 101 and Figure 51 on page 101 show a user's details in Azure AD and the Juniper Mist portal.

Figure 51: User Details on the Azure AD



On the Juniper Mist portal, you can view the group membership information returned by Azure AD. On the Juniper Mist portal, navigate to **Monitoring > Insights > Client Events** to see the information.

Figure 52: User Details on Juniper Mist Portal

Client Events	52 Total	37 Good	11 Neutral	4 Bad
DHCP Success	M5AA7u5uP	15:00:05:00:12:May 2023		
NAC Client Access Allowed	M5AA7u5uP	15:00:05:17:12:May 2023		
NAC IDP Group Setup Success	M5AA7u5uP	15:00:05:17:12:May 2023		
NAC Client Certificate Validation Success	M5AA7u5uP	15:00:05:17:12:May 2023		
NAC Server Certificate Validation Success	M5AA7u5uP	15:00:05:17:12:May 2023		

SSID	m5p-secure-net	Certificate Serial Number	4a23a5de4b410e4
Authentication Type	802.1X	User Name	user1@deaflyz.onmicro soft.com
Certificate CN	user1@deaflyz.onmicro soft.com	Certificate Issuer	AC1C5D-M5AA7CN1ab m5p.ca.lab.mistsoft.com
Certificate Expiry	2024-05-12T09:04:00Z	IP Roles	vip-group1, CorpAndroidDevices, Employee
Certificate SAN (DNS Name)	user1@deaflyz.onmicro soft.com	IDP	Azure AD
IDP	Azure AD	EAP Type	EAP-TLS

In the example shown in Figure 52 on page 101, the user belongs to the group, **Employee**.

You can create an authentication policy based on the group details.

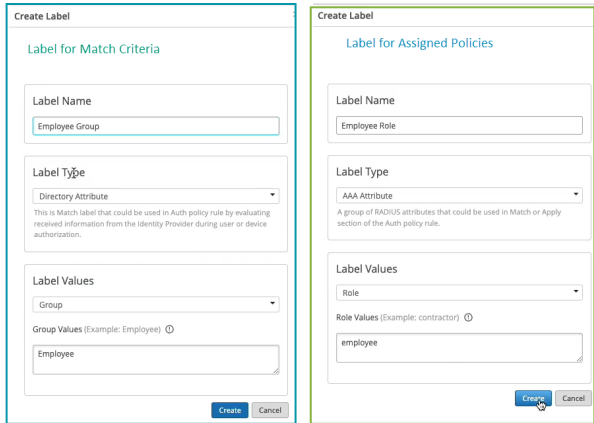
## Create Authentication Policy Based on Group Details

You can create an authentication policy using the label with directory attribute based on the user group membership retrieved by the IDP.

To create an authentication policy:

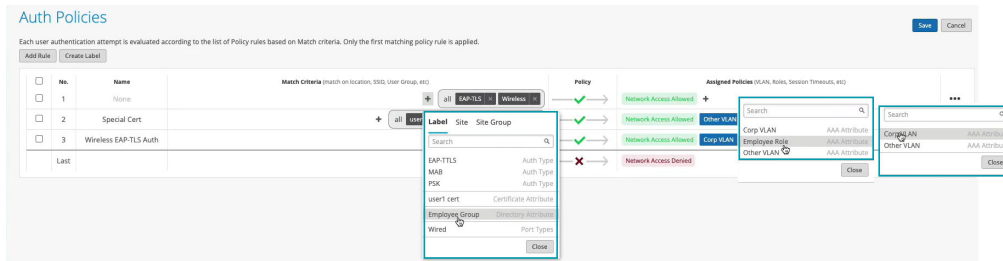
1. On the Juniper Mist portal, from the left menu, select **Organization > Access > Auth Policy**.
2. On the Auth Policy page, click **Create Labels** and enter the details.

**Figure 53: Labels for Authentication Policies**



- Create a label **Employee Group** with label type as **Directory Attribute** based on the user group membership retrieved by the IdP. Select label value as **Group** and group value as **Employee**. Use this label as policy match criteria.
  - Create a label **Employee Role** with label type as **AAA Attribute**. Select label value as **Role** and role value as **Employee**. Use this label to assign policies.
3. Create authentication policy by clicking **Add Rule**. The system inserts a new row allowing you to add a new policy.

**Figure 54: Create Labels for Authentication Policy**



- a. Enter policy name.
- b. Click the add icon (+) in the Match Criteria column and select a user label from the list that appears. Select the label (Employee Group) you created based on directory attributes.

- c. In the Policy column, click the check mark icon (✓), and then select the action you want to enforce, Allow or Block, on the resources you will identify next.
  - d. Click the (+) in the Assigned Policies column and select the label (Employee Role) you created based on AAA attribute for assigned policies. Since the user is part of the employee group, you can assign the employee role and move them to the corporate VLAN.
4. Click **Save**.

Figure 55 on page 103 shows the completed authentication policy.

**Figure 55: Authentication Policy**



## Create an Authentication Policy in a WLAN Template

When you add an authentication policy in your WLAN template, it applies to all WLANs that use this template. First, you'll create the labels that you need to reference in the policy. Then you'll edit the template to add the policy.

1. Create labels for your users so that you can use these labels in your WxLAN policy.
  - a. From the left menu, select **Organization > Wireless > Labels**.  
Only organization-level labels are available for WLAN policies.
  - b. Enter a **Label Name** so that you'll recognize the label when creating your policy.
  - c. Select the appropriate **Label Type** and **Label Values** for the users that you want to identify.  
Label Types for users include AAA Attribute, Access Point, WiFi Client, and WLAN. Values vary by the selected type.

In the following example, the AAA Attribute type is selected, and the Label Value is User Group. By creating labels that correspond to your system user groups, you can create different policies for different groups of users.

**Figure 56: Create New Label**

Organization Labels : **New Label**

Label Name  
Employee

Label Type  
AAA Attribute  
This is a User Label if used in Template WxLan

Label Values IS  
User Group  
User Group Values ⓘ  
employee  
Note: Requires newer firmware

- d. Click **Create** at the top right corner of the Organization Labels screen.
  - e. Repeat the above steps to add other labels as needed for other user groups.
2. Go to **Organization > Wireless > WLAN Templates**.  
The WLAN Template page appears, displaying the list of existing WLAN templates.
  3. Click the template that you want to add the policy to.
  4. In the **Policy** section of the template, click **Add Rule**.
  5. Select the users, the policy, and the resources that the rule applies to:
    - In the **User** section, click the add icon (+). Then select one of the user labels that you created earlier.
    - In the **Policy** section, click the check mark icon (✓). Then select the action you want to enforce: **Allow** or **Block**.
    - In the **Resources** column, click the add icon (+). Then select one of the resource labels that you created earlier.

The screenshot shows the Mist WLAN Template configuration page for 'mist-secure-net'. The 'Name' field is filled with 'mist-secure-net'. Under 'Applies to', there is a 'Choose Org' button and a 'Site and Site Groups' dropdown. The 'Except for these sites (exceptions)' field is empty. The 'Limited to APs in profiles' checkbox is unchecked. The 'WLANs' table has one entry: 'mist-secure-net' with Band '2.4GHz, 5GHz', VLAN ID '1, 750', and Security 'WPA3/EAP (802.1X)'. The '3rd Party Tunnels' table is empty. The 'Policy' section is expanded, showing 'Template Policies' with a description: 'Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied. These rules will be applied to the users who are connected using the current template WLAN.' Below this is a table with columns 'No.' and 'Policy'. One rule is listed: '1' with 'User (matching ALL labels)'. To the right of the rule is a flow diagram: 'User (matching ALL labels)' -> 'Policy: Employees' -> 'Resource: Resource (matching ANY labels)'. A dropdown menu is open over the 'Employees' policy, showing 'Application' and 'Group: Social'.

6. When finished creating and ordering policies, click **Save** at the top of the screen.

The following video shows how to configure authentication policy in WLAN Template when using certificate-based (EAP-TLS) authentication integrated with Azure AD.



**Video:** [EAP-TLS with Azure - Validation & WxLAN Integration](#)

## SEE ALSO

[Configure Authentication Policy | 69](#)

[Configure Authentication Policy Labels | 72](#)

[Use Digital Certificates | 64](#)

[Configure Certificate-Based \(EAP-TLS\) Authentication | 83](#)

[Configure MAC-Based Authentication and MAC Authentication Bypass \(MAB\) | 89](#)

[Add Identity Providers for Juniper Mist Access Assurance | 56](#)



# Configure Credentials-Based (EAP-TTLS) Authentication

## IN THIS SECTION

- [Configure Credential-Based \(EAP-TTLS \) Authentication for Wired Network | 107](#)

Extensible Authentication Protocol–Tunneled TLS (EAP-TTLS) use username and password on the client side and server certificate on the server side to provide secure access.

The following tasks show you how to configure EAP-TTLS for wired clients. These authentication methods validate the username and password by using the credentials stored in the identity providers (IdPs).

## Prerequisites

- You must integrate and configure an identity provider (IdP) with the Juniper Mist portal. See ["Add Identity Providers for Juniper Mist Access Assurance" on page 56](#).
- You must configure the client device as a supplicant. For this configuration, you must add the root-certificate authority (CA) certificate of the enterprise public key infrastructure (PKI) and enter the username and password in the IdP.
- You need a Juniper Access Point to perform wireless client authentication (wireless client-specific task).
- You must configure the public or private enterprise TLS-server certificate that the cloud RADIUS server will use.

Watch the following video to learn how to configure credential-based (EAP-TTLS ) authentication with Azure IdP Integration:



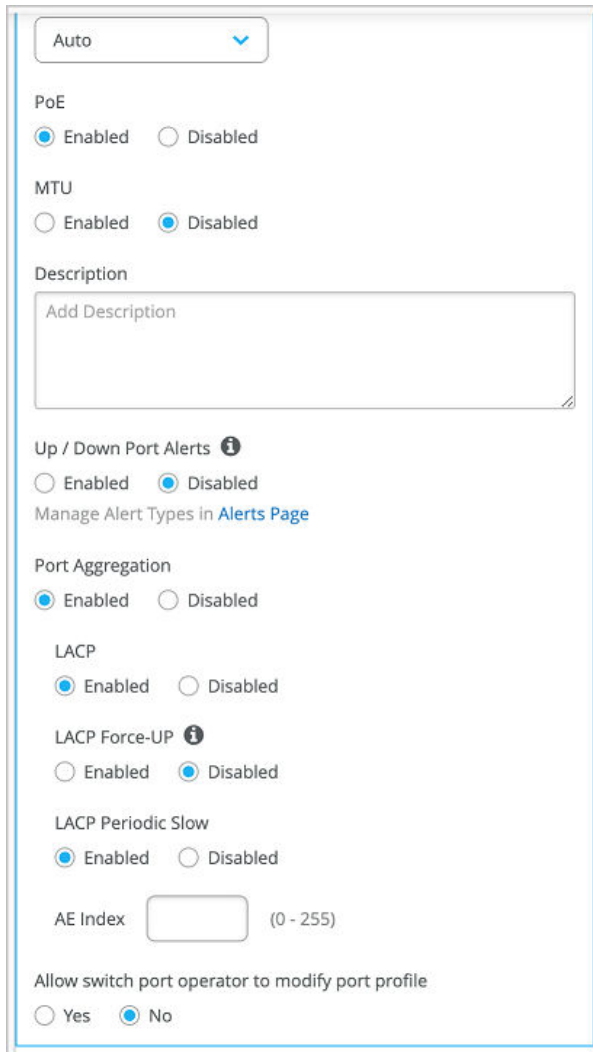
Video: [EAP-TTLS with Azure Configuration - Credential-Based Auth](#)

## Configure Credential-Based (EAP-TTLS ) Authentication for Wired Network

To set up certificate-based authentication for a wired network using the Juniper Mist portal:

1. Import a trusted root certificate authority (CA). Juniper Mist uses the certificate authority (CA)-generated certificate as a server certificate. See ["Use Digital Certificates" on page 64](#) for details.
2. Create authentication policies.
  - a. From the left menu of the Juniper Mist portal, select **Organization > Access > Auth Policies**.  
Create a new rule to allow access to clients with valid certificates. See ["Configure Authentication Policy" on page 69](#).  
Define an authentication policy with the following details. Select the required option for each field from the respective drop-down lists.
    - i. Name—Enter a name for the policy. (ex: TLS-Clients)
    - ii. Match Criteria—Select **EAP-TTLS**.
    - iii. Policy—Select **Allowed**
    - iv. Assigned Policies—Select **Network Access Allowed**.
3. Configure the switch.
  - a. From the left menu of the Juniper Mist portal, select **Organization > Wired > Switch Templates**.  
On the Switch Templates page, either click an existing template to open its configuration page, or click **Create Template** in the upper-right corner of the page to create a template.
  - b. In the Authentication Servers section, select **Mist Auth** as the authentication server.
  - c. Scroll down to the Port Profile section and configure the following settings:
    - Mode—Access
    - Enable the Use dot1x authentication option.
  - d. Assign the port profile to each port of the switch where the connected wired clients require network access.  
On the **Port Config** tab, in the **Select Switches Configuration** section, , click Add Port Range to associate a port profile with a port.

**Figure 57: Assign Port Profile to Port Ranges on a Switch**



Auto

PoE  
 Enabled  Disabled

MTU  
 Enabled  Disabled

Description  
 Add Description

Up / Down Port Alerts ⓘ  
 Enabled  Disabled  
 Manage Alert Types in [Alerts Page](#)

Port Aggregation  
 Enabled  Disabled

LACP  
 Enabled  Disabled

LACP Force-UP ⓘ  
 Enabled  Disabled

LACP Periodic Slow  
 Enabled  Disabled

AE Index  (0 - 255)

Allow switch port operator to modify port profile  
 Yes  No

e. Click **Save**.

Now your network can use EAP-TTLS to securely authenticate clients.

The Auth Policy allows clients with a valid username and password to access the network.

The Juniper Mist cloud verifies the username and password against the credentials stored in the public credential provider and grants access and authorization based on the "[Label Configuration](#)" on page 72.

You can view the associated clients on the Juniper Mist portal.

- Select **Clients > Wired Clients** to see client details
- Select **Monitor > Service Levels > Insights** to view client events.

## SEE ALSO

[Configure Authentication Policy | 69](#)

[Configure Authentication Policy Labels | 72](#)

[Configure Certificate-Based \(EAP-TLS \) Authentication | 83](#)

[Configure Certificate-Based \(EAP-TLS \) Authentication with Azure IdP Integration | 95](#)

[Configure MAC-Based Authentication and MAC Authentication Bypass \(MAB\) | 89](#)

[Configure Client Device for EAP-TTLS Authentication | 109](#)

[Add Identity Providers for Juniper Mist Access Assurance | 56](#)

# Configure Client Device for EAP-TTLS Authentication

This topic provides details on how to configure a client device for Extensible Authentication Protocol-Tunneled TLS (EAP-TTLS) authentication. The procedure uses an Apple client device as an example.

When using Juniper Mist Access Assurance, you need additional configuration when using EAP-TTLS/PAP (credentials-based) authentication for Apple devices. For this task, you must create a profile using a free [Apple Configurator tool](#).



**NOTE:** Providing username and password at the login prompt by clicking on the SSID does not work for Apple devices. Apple devices use PEAP-MSCHAPv2 or EAP-TTLS/MSCHAPv2 authentication methods, which use password hashing algorithm that is not supported by any cloud-based Identity Provider.

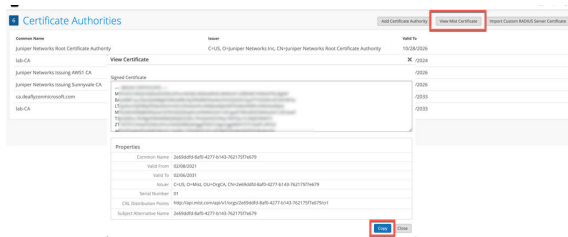
To create a Wi-Fi profile:

1. Download the Juniper Mist server certificate.

In order for the client devices to trust the Mist Access Assurance server certificates, the Mist Certificate must be included in the Wi-Fi profile.

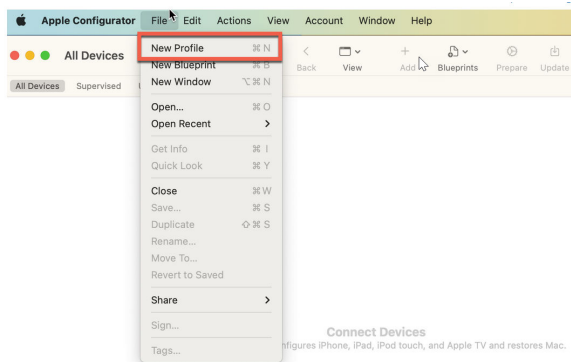
- a. On the Juniper Mist portal, go to **Organization > Access > Certificates**.  
The Certificate Authorities page appears.

**Figure 58: View and Save Mist Server Certificate**



- b. Click **View Mist Certificate** and copy the certificate details.  
 Save the certificate locally as a file with the **.crt** extension. For example: **mist-cert.crt**.  
 If you are using your own custom server certificate, download your Certificate Authority (CA) certificate for this step instead of downloading a Juniper Mist Certificate.
2. Create a new profile on your Apple client device.
- a. On your Mac computer, open your Apple Configurator tool, and click **File > New Profile**.

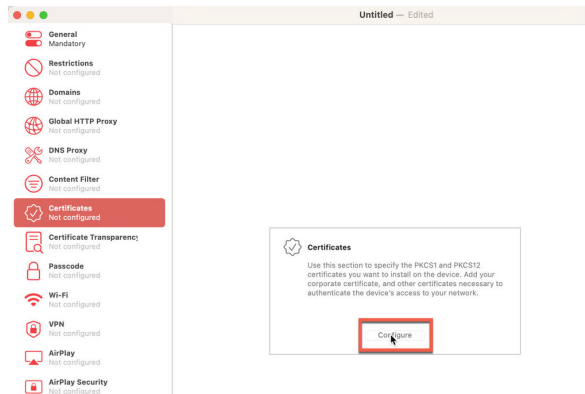
**Figure 59: Wi-Fi Profile Configuration for Apple Client**



A new configuration profile document opens.

- b. On the left-navigation bar of the Apple Configurator tool, click **Certificates > Configure**.

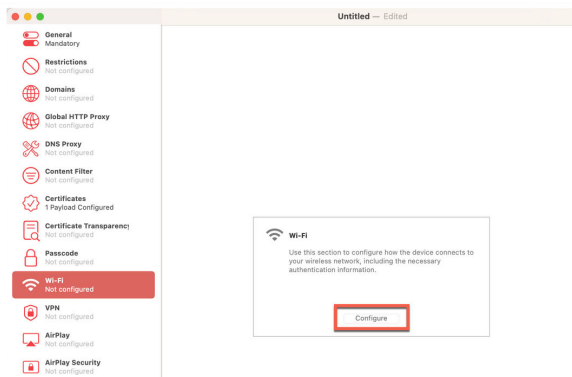
**Figure 60: Upload Juniper Mist Server Certificate in Wi-Fi Profile Configuration for Apple Client**



Select and upload your Mist Certificate you downloaded in the previous procedure.

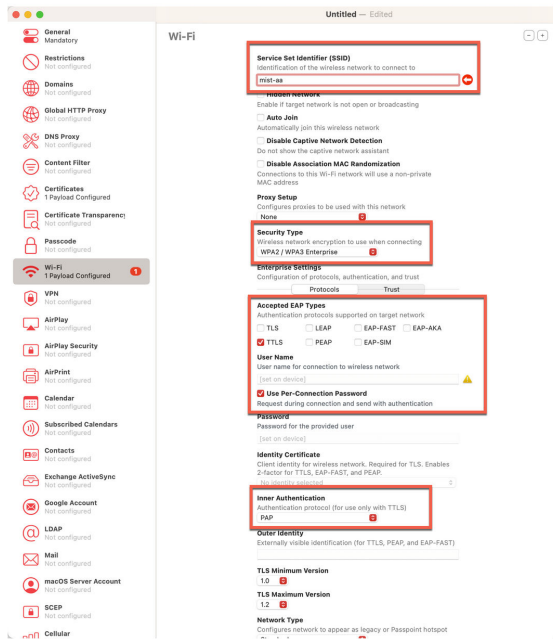
- c. From the left-navigation bar of the Apple Configurator tool, select **Wi-Fi** and click **Configure**.

**Figure 61: Wi-Fi Profile Configuration for Apple Client**



Enter the following options for the Wi-Fi settings:

Figure 62: Settings in Wi-Fi Profile Configuration for Apple Client



- SSID—Your network's SSID. Ensure that you enter the correct SSID including capital letters.
  - Security Type—WPA2/WPA 3 Enterprise
  - Accepted EAP Types—TTLs and select Per-connection Password.
  - Inner Authentication—PAP
- d. On the same page, under **Enterprise Settings**, click **Trust**. The page displays a list of uploaded certificates.

Figure 63: Trust Juniper Mist Server Certificate in Wi-Fi Profile Configuration for Apple Client

**Service Set Identifier (SSID)**  
 Identification of the wireless network to connect to

**Hidden Network**  
 Enable if target network is not open or broadcasting

**Auto Join**  
 Automatically join this wireless network

**Disable Captive Network Detection**  
 Do not show the captive network assistant

**Disable Association MAC Randomization**  
 Connections to this Wi-Fi network will use a non-private MAC address

**Proxy Setup**  
 Configures proxies to be used with this network

**Security Type**  
 Wireless network encryption to use when connecting

**Enterprise Settings**  
 Configuration of protocols, authentication, and trust

Protocols Trust

**Trusted Certificates**  
 Certificates trusted/expected for authentication

Certificate: 2e69ddfd-8af0-4277-b143-762175f7e...

**Trusted Server Certificate Names**  
 Certificate names expected from authentication server

auth.mist.com

+ -

**Network Type**  
 Configures network to appear as legacy or Passpoint hotspot

**Fast Lane QoS Marking**

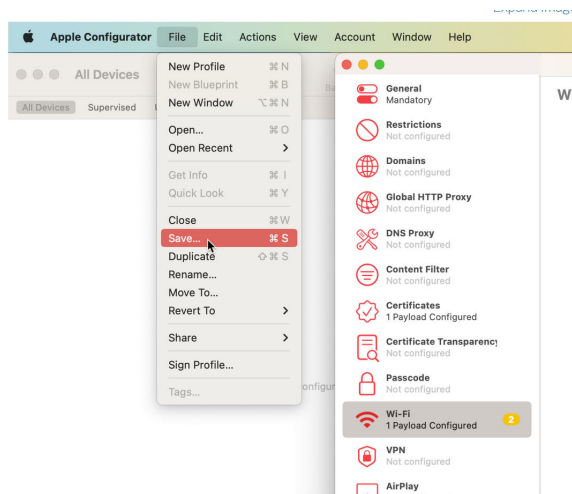
Select the Juniper Mist certificate. This step enables the client devices to trust the Juniper Mist server certificate.

Now you can distribute it to your Apple clients.

- e. Save your configuration.



Figure 64: Save Wi-Fi Profile Configuration



To Sign the profile, you need an Apple trusted certificate. This step is required for production use.

Now you can distribute the certificate to your Apple clients.

Watch the following video to learn how to create a network profile for EAP-TLS for testing or lab use:



**Video:** [Manual Network Profile Configuration for Lab Use - EAP-TLS for MacOS-iOS-iPadOS](#)

## RELATED DOCUMENTATION

[Configure Authentication Policy | 69](#)

[Configure Authentication Policy Labels | 72](#)

[Use Digital Certificates | 64](#)

[Configure Certificate-Based \(EAP-TLS\) Authentication | 83](#)

[Configure Certificate-Based \(EAP-TLS\) Authentication with Azure IdP Integration | 95](#)

## TEAP Configuration for Windows Client

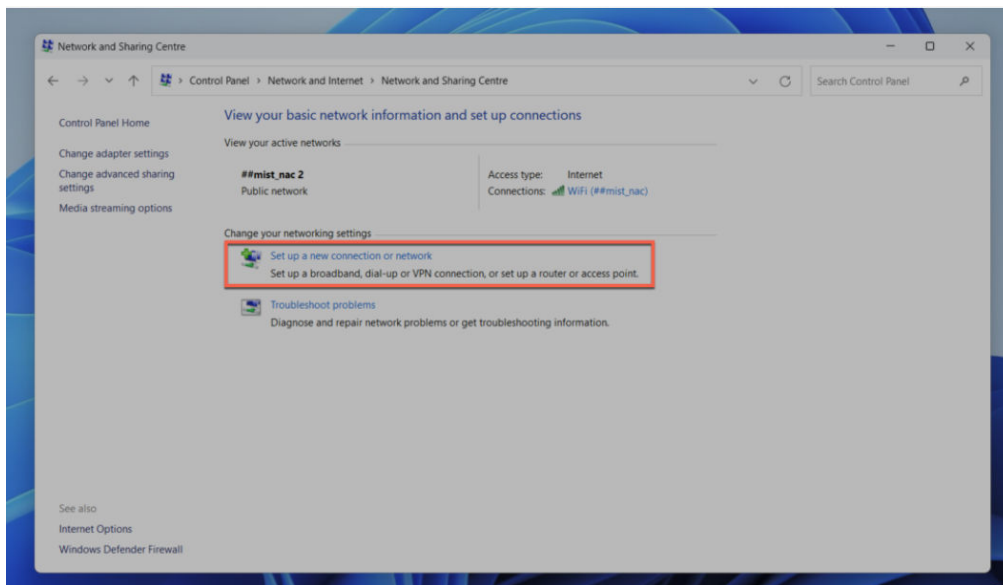
TEAP (Tunneled Extensible Authentication Protocol) is a tunnel-based EAP method that enables secure communication between a peer and a server by using the Transport Layer Security (TLS) protocol to establish a mutually authenticated tunnel. Within the tunnel, TLV objects are used to convey authentication-related data between the EAP peer and the EAP server. ([RFC 7170 - Tunnel Extensible Authentication Protocol](#))

Currently TEAP support is available for Windows 10 Version and above.

As of now, you can configure wireless and wired profile with TEAP manually or through scripts, which can be distributed using MDM or GPO. Current MDM solutions do not provide out-of-the box support for TEAP configuration.

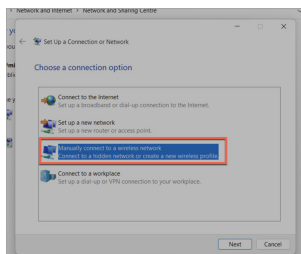
1. Navigate to **Control Panel > Network and Sharing Centre** and click **Set up a new connection or network**.

**Figure 65: TEAP Configuration - Set up New Connection**



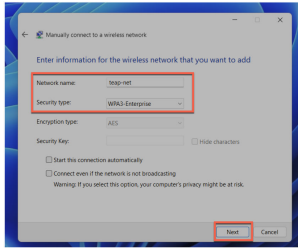
2. Select the **Manually connect to a wireless network** option.

**Figure 66: TEAP Configuration - Select Manually Connect Option**



3. Enter the details for the wireless network.

**Figure 67: TEAP Configuration - Enter Wireless Network Details**

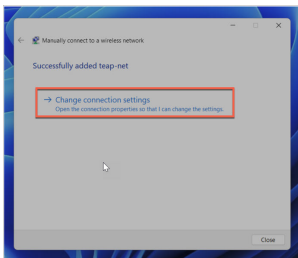


- **Network Name**—Provide an SSID name.
- **Security Type**—Select the WPA3-Enterprise option.

Click Next.

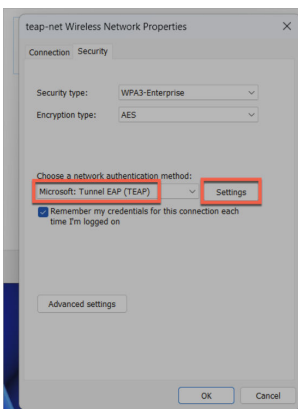
4. Click **Change connection settings**.

**Figure 68: TEAP Configuration - Change Settings for Network**



5. In the Wireless Network Properties, enter the details.

**Figure 69: TEAP Configuration - Choose Authentication Method**

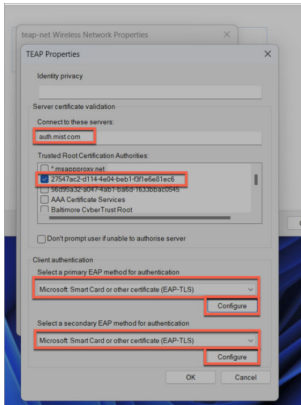


- **Choose a network authentication method**—Select Microsoft:Tunnel EAP (TEAP).

Click **Settings**.

- In the TEAP Properties window, select the options.

**Figure 70: TEAP Configuration - Select TEAP Properties**

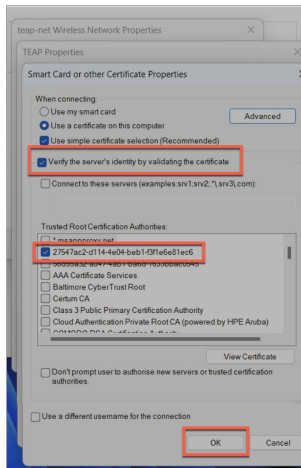


- **Connect to these servers**—Enter auth.mist.com.
- **Trusted Root Certification Authorities**—Select trusted Root CA for the client to validate Mist Access Assurance server certificate (or your custom RADIUS server certificate)
- **Select a primary EAP methods for authentication**—Microsoft Smart Card or other certificate (EAP-TLS)
- **Select a secondary EAP methods for authentication**—Microsoft Smart Card or other certificate (EAP-TLS)

Click **Configure** for each of the EAP-TLS options.

- For each option, ensure **Use simple certificate selection (Recommended)** is selected and check the same Root CA to enable the client to trust Mist Access Assurance server certificate.

Figure 71: TEAP Configuration - Choose Root CA



Click **OK**.

## RELATED DOCUMENTATION

[Configure Authentication Policy | 69](#)

[Configure Authentication Policy Labels | 72](#)

[Use Digital Certificates | 64](#)

[Configure Certificate-Based \(EAP-TLS \) Authentication | 83](#)

[Configure Certificate-Based \(EAP-TLS \) Authentication with Azure IdP Integration | 95](#)

# Install Juniper Mist Edge VM for Juniper Mist Authentication Proxy

## IN THIS SECTION

- [Juniper Mist Edge VM as Juniper Mist Auth Proxy | 119](#)
- [Install Juniper Mist Edge VM | 120](#)
- [Create a Juniper Mist Edge VM on the Juniper Mist Portal | 123](#)

Read this topic to learn how to install a Juniper Mist™ Edge virtual machine (VM) for the Juniper Mist Authentication Proxy functionality.

## System Requirements

Minimum hardware requirements for a Juniper Mist Edge VM to support the Juniper Mist Auth Proxy functionality:

- Hypervisor: VMware ESXi (Versions – 6.7.0 and 7.0)
- CPU: 2 vCPUs
- RAM: 16-GB RAM
- Hard Disk: 32 GB, thick provisioned
- Network Interface Card (NIC): Single virtual NIC



**NOTE:** You need to provide unrestricted access to debian and mistsys repo in the environments where you create the Mist Edge VM for initial bring up. Also, ensure that the Firewall has Port-80 and Port-443 open.

## Juniper Mist Edge VM as Juniper Mist Auth Proxy

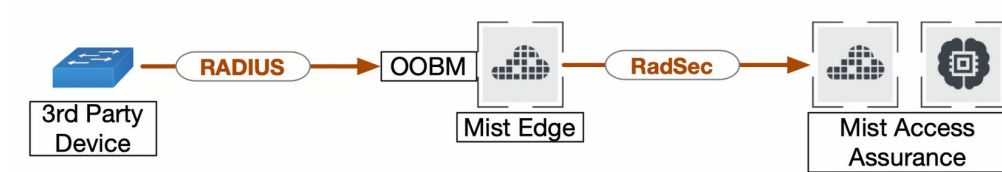
Juniper Mist Edge virtual machine (VM) requires out-of-band management (OOBM) interface to act as Juniper Mist Auth Proxy.

You can specify a port on which the client contacts the RADIUS server. By default, the client uses port 1812 (as specified in RFC 2865). You can also specify an accounting port to send accounting packets. The default port is 1813 (as specified in RFC 2866).

You must configure TCP port 2083 to allow outbound connections destined to radsec.nac.mist.com.

Additionally, you must provide Juniper Mist Edge VM access to the EP terminator service [ep-terminator.mistsys.net (TCP 443)] on the Juniper Mist cloud. See [Firewall Configuration: Juniper Mist Ports and IP Addresses](#).

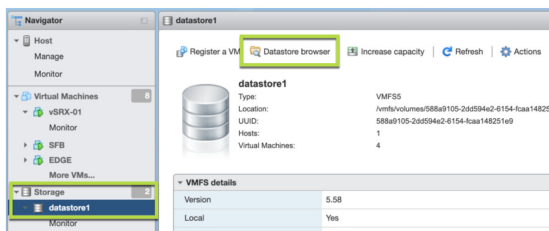
Figure 72: Juniper Mist Edge as Auth Proxy—Flow of Connections



## Install Juniper Mist Edge VM

1. Download installation image from Juniper Mist portal. See [Create a Juniper Mist Edge VM Using the VMWare ESXi Portal](#).
2. In the VMware ESXi Portal, upload the ISO to the VMware storage.
  - a. On the vSphere Web client, select your virtual machine (VM) from the left navigation bar.
  - b. Select the datastore under **Storage** from the inventory.
  - c. Click **Datastore browser** and select the datastore to which you will upload the file.

Figure 73: Select Datastore to Upload File



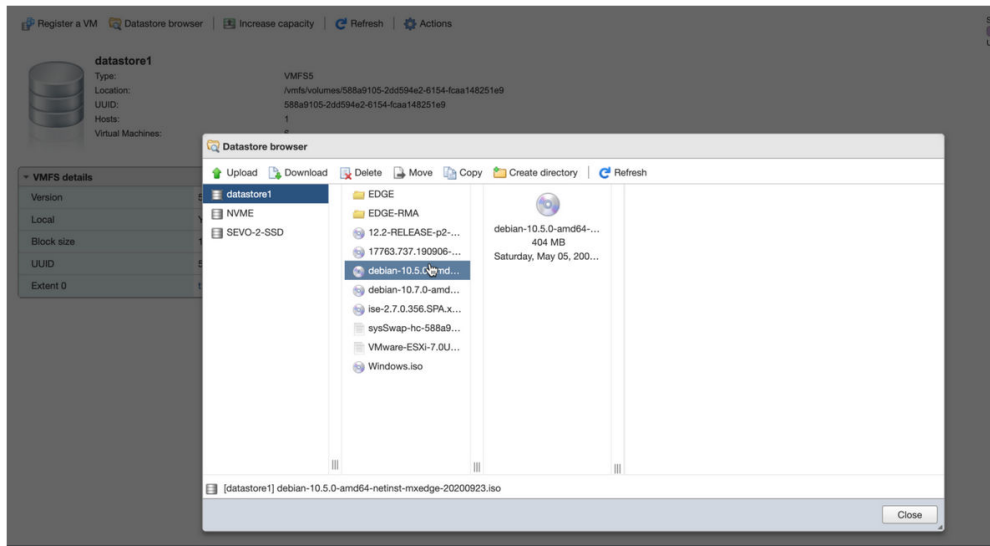
- d. Click **Upload** and then select the ISO file that you have downloaded in the previous step.

Figure 74: Upload ISO File



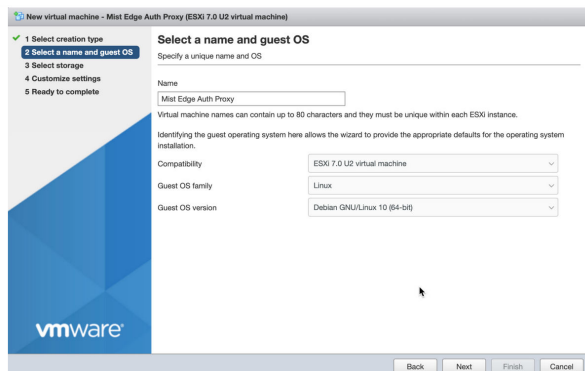
- e. Refresh the Datastore browser to see the uploaded file in the list.

Figure 75: Refresh Datastore Browser



3. Create a VM with the following configuration.
  - a. On the Select a create type page, select **Create a new virtual machine**.
  - b. On the Select a name and guest OS page, enter the required details.

Figure 76: Enter Details of Juniper Mist Edge VM

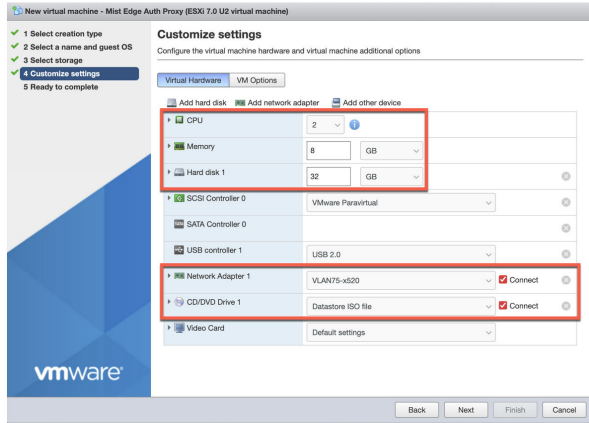


- **Name**—Enter a name for the VM.
- **Compatibility**—Select the ESXi version running on the vSphere. For example: ESXi 7.0 U2 virtual machine.
- **Guest OS family**—Select the guest operating system family. For example: Linux.
- **Guest OS version**—Select a guest operating system version. for example: Debian GNU/Linux 10 [64-bit].



- c. On the Customize settings page, make the required changes.

**Figure 77: Customize Settings for VM**



See [Virtual Mist Edge](#) for detailed instructions.

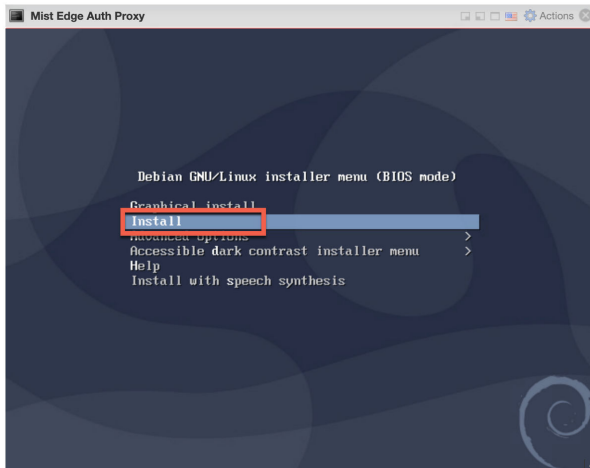
- d. Click Finish after you complete the setup.

Power on the VM when it is created.

4. When the Juniper Mist Edge VM powers on, install the VM.

On the Juniper Mist Edge VM install page, select **Install** and press **Enter**. The default selection is **Graphical install**.

**Figure 78: Install Juniper Mist Edge VM**



After the installation, the system displays the 'mxedge login:'.

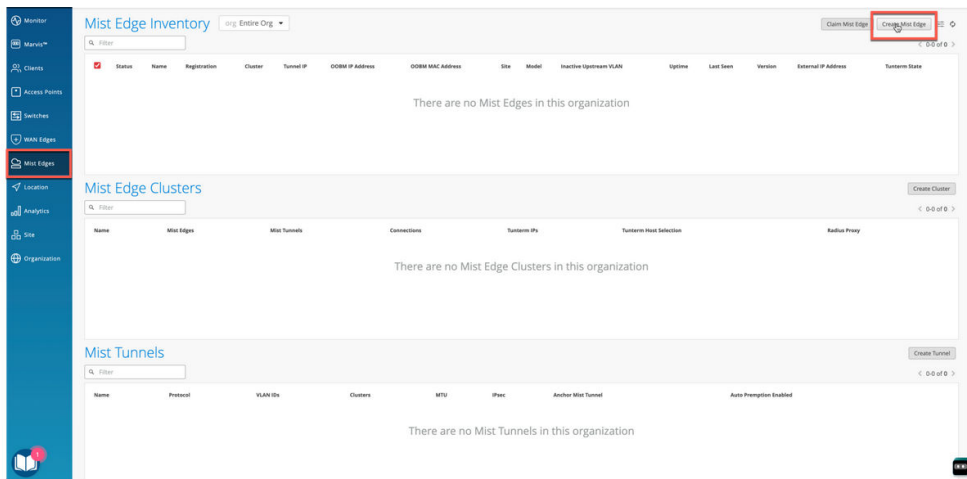
On the installation page, you can see the progress of the installation for some time (30 seconds to a minute) and a request to wait.

After you select **Install**, the installation proceeds automatically without any user intervention.

## Create a Juniper Mist Edge VM on the Juniper Mist Portal

1. From the left menu of the Juniper Mist portal, select **Mist Edges**. Then on the top right of the page, click **Create Mist Edge**.

Figure 79: Create Juniper Mist Edge VM



2. On the Create Mist Edge page, enter a name for the Juniper Mist Edge device and select **VM** as the model.

**Figure 80: Enter Details for Juniper Mist Edge VM**

Create Mist Edge ✕

---

Mist Edge Name

Model

---

3. Copy the registration code and save the information.

**Figure 81: Copy Registration Code**

Name

Model

Registration Unregistered

Registration Code

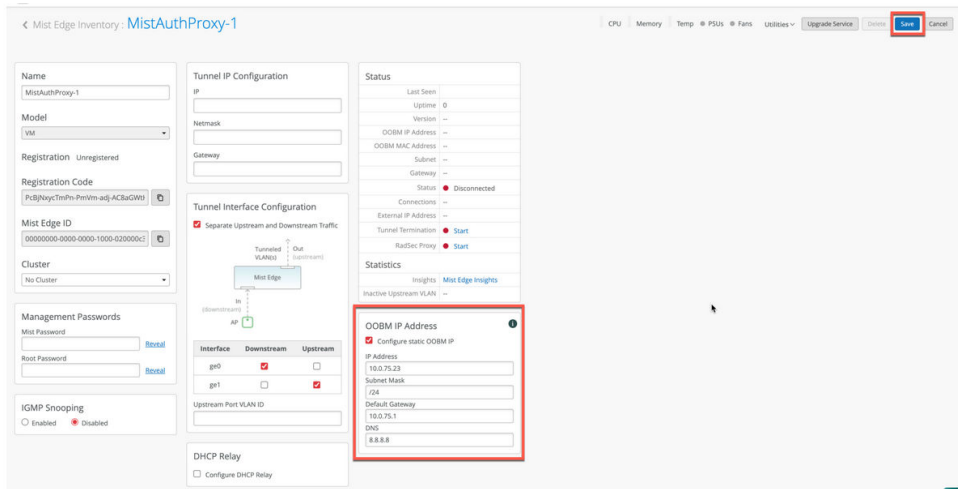
Mist Edge ID

Cluster

Note that by default Dynamic Host Configuration Protocol (DHCP) provides the out-of-band management (OOBM) IP address. On the Juniper Mist portal, you can see the assigned static OOBM

IP address as shown in the following figure. We recommend that you use a static out-of-band management IP address for the Juniper Mist authentication proxy use case.

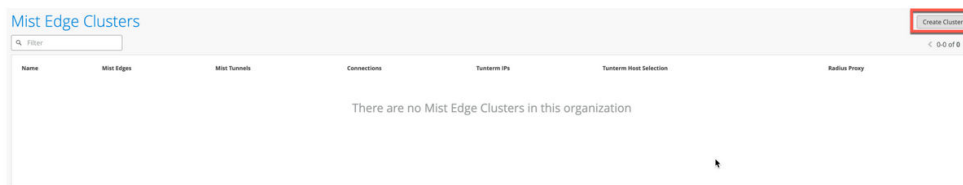
**Figure 82: Juniper Mist Edge VM Out-of-Band Management IP Address**



For the Juniper Mist authentication proxy use case, you do not need to configure the tunnel interface IP.

4. On the Mist Edge Inventory page, scroll down to the Mist Edge Clusters pane and click **Create Cluster**.

**Figure 83: Create Juniper Mist Edge Cluster**



5. On the Create Mist Cluster page, enter the cluster name and select your deployed Juniper Mist Edge VM.

**Figure 84: Select Mist Edge VM for Cluster**

Create Mist Cluster ✕

Cluster Name  
MistAuthProxy-Cluster

Select Mist Edges  
MistAuthProxy-1 ✕ +

Create Cancel

6. Click **Create** to continue.

7. Provision your Juniper Mist Edge VM.

After you configure the Juniper Mist Edge on the Juniper Mist portal, connect to the console interface.

a. When your Juniper Mist Edge VM boots up for the first time, log in to the VM using the following credentials:

- **Username:** mist
- **Password:** Mist@1234
- **Root (su -) password:** mist

b. Get the current management IP address from DHCP by issuing the `ip a` command. In the command output, you can see that the OOBM interface is `ens192`.

Figure 85: Provision Juniper Mist Edge VM

```

Mist Edge Auth Proxy
Debian GNU/Linux 10 mxedge tty1
mxedge login: mist
Password:
Linux mxedge 4.19.0-10-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
sourced /etc/skel/.mxagent_aliases
mist@mxedge:~$ su -
Password:
sourced /etc/skel/.mxagent_aliases
root@mxedge:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 3e:af:78:bd:f1:ff:ff:ff:ff:ff:ff
    inet 10.0.75.51/24
        brd 10.0.75.255 scope global dynamic ens192
            tc preferred_lft 86065sec
    inet6 fe80::20c:29ff:fe3e:af73/64 scope link
        valid_lft forever preferred_lft forever
root@mxedge:~#

```

Now, you can initiate an SSH session and connect to the Juniper Mist Edge VM with the username mist. Example:

```
ssh mist@<OOBM-IP>, password is Mist@1234
```

Switch to root:

Issue the su - command and use **mist** as the password.

#### 8. Initiate SSH from the Juniper Mist Edge VM and perform bootstrap.

To perform a bootstrap on the Juniper Mist Edge VM and onboard the device to the Juniper Mist portal, use the following CLI commands:

```

mist@mxedge:~$ su -
Password: abc1
root@mxedge:~# apt-get update
root@mxedge:~# mxagent register --registration-code <paste registration code from step 3>

```

When the process completes, the CLI displays the following message:

```
registration finished successfully. (regfile at /var/lib/mxagent/mxagent.reg
```

After successful registration, the Juniper Mist Edge VM automatically reboots and downloads the configuration from the Juniper Mist Cloud portal.

After the reboot, you can see the updated status of the Juniper Mist Edge VM on the Juniper Mist portal. The Status field on the Mist Edge Inventory page displays **Connected** and a corresponding orange icon.

**Figure 86: Juniper Mist Edge VM in Mist Edge Inventory**

The screenshot shows the 'Mist Edge Inventory' page with a search filter and a table of devices. The table has columns for Status, Name, Registration, Cluster, Tunnel IP, OOBM IP Address, OOBM MAC Address, Site, Model, Inactive Upstream VLAN, Uptime, Last Seen, Version, External IP Address, and Tunnel State. A single entry is visible with the status 'Connected' and a registration state of 'Registered'.

Status	Name	Registration	Cluster	Tunnel IP	OOBM IP Address	OOBM MAC Address	Site	Model	Inactive Upstream VLAN	Uptime	Last Seen	Version	External IP Address	Tunnel State
Connected	MistAuthProxy-1	Registered	MistAuthProxy-Cluster	--	10.0.75.23	00:0c:29:3c:a7:73	Unassigned	VM	--	29m	06:01:06 PM, Jun 16	--	--	Not Installed

## SEE ALSO

[Use Digital Certificates | 64](#)

[Configure Certificate-Based \(EAP-TLS \) Authentication | 83](#)

[Configure Certificate-Based \(EAP-TLS \) Authentication with Azure IdP Integration | 95](#)

[Configure MAC-Based Authentication and MAC Authentication Bypass \(MAB\) | 89](#)

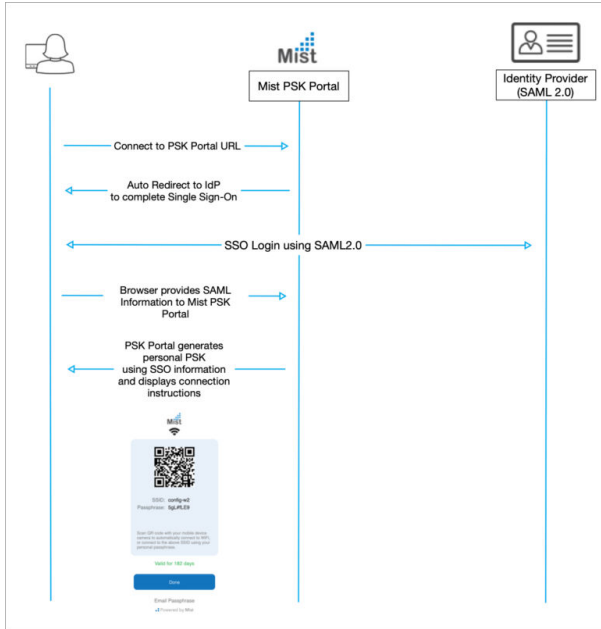
[Add Identity Providers for Juniper Mist Access Assurance | 56](#)

# Enable Client Onboarding with a BYOD PSK Portal

## SUMMARY

Set up a client onboarding workflow for a Bring Your Own Device (BYOD) Preshared Key (PSK) Portal. These portals allow users to self-provision PSKs.

When everything is set up, the “workflow” for the BYOD PSK Portal will look like this:



Users will see something similar to the following example, but with the changes that you make to customize the appearance and the text.



## Before You Begin

- Obtain and activate a Juniper Mist™ Access Assurance subscription. For information about subscription management, see the [Juniper Mist Management Guide](#).
- In your Juniper Mist organization, configure at least one organization-level WLAN with Multi-PSK enabled (either local or cloud PSK options are fine). For help with WLAN configuration, see the [Juniper Mist Wireless Assurance Configuration Guide](#).
- In your IdP admin console, configure a SAML 2.0 app integration. Your PSK portal will integrate with this application to enable Single Sign-On (SSO) access to your portal users. You can use a wide variety of IdPs (such as Okta and Microsoft Azure), as long as they support SAML 2.0. For help setting up a SAML 2.0 app integration, see your IdP documentation.



Copy the following information from your SAML 2.0 app integration, and save it so that you can use it to set up your PSK portal in Juniper Mist.

- Signing Algorithm
- Issuer ID



**NOTE:** Your IdP admin console might show a different name for the Issuer ID. For example:

- In Okta, this value is called Identity Provider Issuer.
- In Azure, it's called Azure AD Identifier.

- SSO URL



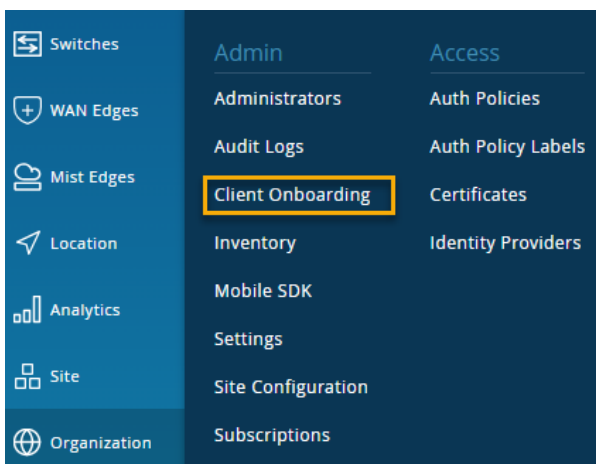
**NOTE:** Your IdP admin console might show a different name for the SSO URL. For example:

- In Okta, this value is called Identity Provider Single Sign-On URL.
- In Azure, it's called Login URL.

- Certificate—Copy the full text of the certificate, from the *BEGIN CERTIFICATE* line through the *END CERTIFICATE* line.

To set up client onboarding with a BYOD PSK Portal:

1. From the left menu of the Juniper Mist portal, select **Organization > Access > Client Onboarding**.



2. Click **Add PSK Portal** at the top-right corner of the Client Onboarding page.



3. In the Add PSK Portal pop-up window, enter a **Name**, select **BYOD (SSO)** as the portal type, and then click **Create**.

4. On the **Portal Settings** tab of the Edit PSK Portal window:
  - Keep the default layout options, or make changes to customize the sign-in screen.
  - Copy the **PSK Portal URL** so that you can provide it to your users.

5. On the **Portal Authorization** tab of the Edit PSK Portal window:
  - Enter the **Issuer**, **Signing Algorithm**, **SSO URL**, and **Certificate** that you copied from your app integration in your IdP admin console.

- Select a **Name ID Format**. Most people use the e-mail address for the name ID. If you use a different identifier for your IdP user accounts, select **Unspecified**.

6. Copy the **Portal SSO URL**.
7. Open a separate browser window, and complete these steps to finalize your SAML 2.0 app integration:
  - a. Navigate to your IdP admin console.
  - b. Go to the settings for your SAML 2.0 app integration.
  - c. Enter the copied value into the appropriate field to identify your Juniper Mist PSK portal to your IdP. For help, see your IdP documentation.
  - d. Save the changes.

Your IdP might have different names for the field where you need to paste the Portal SSO URL. Consider the following examples, and see your IdP documentation for help.

### Okta Example

In this example, the **Portal SSO URL** from Juniper Mist is copied into the appropriate fields in the Okta Admin Console.

### Microsoft Azure Example

In this example, the **Portal SSO URL** from Juniper Mist is copied into the appropriate fields in the Azure Admin Console.

8. Return to the Juniper Mist portal.
9. On the **PSK Parameters** tab of the Edit PSK Portal window:
  - Select the **SSID** (required).



**NOTE:** The list includes only SSIDs for organization-level WLANs that have Multi-PSK enabled.

- Adjust the optional settings as needed. For example:
  - Specify a **VLAN ID** if you want the users of this portal to be assigned to a particular VLAN. To use this option, you must enter a VLAN that is included in the VLAN list for the WLAN.
  - Set the **Passphrase Settings** to enforce your policies for password complexity.

- Adjust the **PSK Validity** options to set the expiration period and to send reminders before key expiration.

If you enable the option to send reminders, Juniper Mist sends users an email when their PSK is about to expire.

The email includes either the default reauthentication URL or your **Key Expiration Renew URL** (if you enter one). This is typically a single sign-on URL (for example, using your corporate identity provider URL through Okta or Microsoft Azure).

- Under **Max Usage**, you can limit the number of devices that can connect to your portal.
- Under **Role**, you can specify a role to limit access to certain types of user accounts (using the roles that you set up for your IdP user accounts).

Edit PSK Portal ✕

Portal Settings
Portal Authorization !
PSK Parameters ↓

**SSID is required**

The following settings will determine passphrase complexity and validity parameters, as well as network policy and segmentation rules applied to Pre-Shared Keys created via this PSK Portal.

**SSID**

Select

**VLAN ID** ⓘ

(1 - 4094)

**Passphrase Settings**

Characters:

Minimum Characters:

Maximum Characters:

**Includes**

Letters

Numbers

Special Characters

[]\`\_!@#&.\$

**PSK Validity**

PSK would remain valid for  Months ↓

Send reminder  Days ↓ before key expiration

**Key Expiration Renew URL** ⓘ

**Max Usage**

ⓘ Max Usage requires firmware v0.10.x or higher

Unlimited Devices  Set number of devices

0

**Role**

Static Role

Assign Dynamically via SSO

Delete
Save
Cancel

10. Click **Save** at the bottom of the Edit PSK Portal window.



**NOTE:** The button is unavailable until you enter the required settings on the various tabs. The required settings are labeled in red type.

11. Verify that your portal works as expected by going to the **PSK Portal URL** that you copied from the Portal Settings tab of the Edit PSK window.
12. Provide your users with the **PSK Portal URL** so that they can connect to your portal.



**TIP:** Create a CNAME in your DNS to create a more user friendly URL that is associated with your domain.

Users can follow the on-screen text to onboard their devices.

# 5

CHAPTER

## Monitoring

---

### IN THIS CHAPTER

- [Juniper Mist Access Assurance NAC Clients | 137](#)
  - [NAC Events | 138](#)
  - [Validate Access and Authentication | 143](#)
-

# Juniper Mist Access Assurance NAC Clients

Juniper Mist provides visibility into wireless and wired client devices authenticated to your network through NAC Clients page. The client data includes information about the present and past connections with details such as client type, users, auth type, MAC addresses and so on.

1. Access NAC Clients page from the left menu of the Juniper Mist portal by selecting **Clients > NAC Clients**.

The NAC clients page lists all clients authenticated to your network.

2. Use options on the NAC Clients page to filter and view specific information.

Figure 87: NAC Clients Page

The screenshot shows the Juniper Mist NAC Clients page. At the top, there are navigation elements: 'Select Site or Entire Organization' (set to 'Core Site'), 'Select Time Period' (set to 'Today'), and 'Search NAC Clients'. A search bar is present. Below the navigation is a table with columns: Client Type, Auth Type, MAC Address, User, Last Seen, State, AP, Part, Matched Auth Policy Rule, Role, SSID, VLAN, GBP Tag, and Insights. The table contains several rows of client data. A 'View NAC Client Events Page' button is visible on the right side of the table.

Client Type	Auth Type	MAC Address	User	Last Seen	State	AP	Part	Matched Auth Policy Rule	Role	SSID	VLAN	GBP Tag	Insights
Wireless	EAP-TTLS	[REDACTED]	jack@9m50l8s.org	Oct 22, 2024 11:39:52 AM	●	Anirudh-Home-AP	--	Device connected via EAP-TTLS	--	TEST-DOT1X	--	--	Client Insights
Wireless	PSK	[REDACTED]	NAC PPSK Key 01	Oct 22, 2024 11:38:25 AM	●	Anirudh-Home-AP	--	--	Developer	Radius-NAC-MPSK	--	--	Client Insights
Wireless	EAP-TLS	[REDACTED]	test-user@gmail.com	Oct 22, 2024 11:36:50 AM	●	Anirudh-Home-AP	--	Device connected via EAP-TLS	Contractor	TEST-DOT1X	Employee-VLAN	130	Client Insights
Wireless	PSK	[REDACTED]	OKTA Key 01	Oct 22, 2024 11:36:31 AM	●	Anirudh-Home-AP	--	--	Tester	AWS-NAC-PSK-2	--	--	Client Insights
Wireless	PSK	[REDACTED]	OKTA Key 01	Oct 22, 2024 11:36:17 AM	●	Anirudh-Home-AP	--	--	Tester	AWS-NAC-PSK-2	--	--	Client Insights
Wireless	PSK	[REDACTED]	f2bec4970d4	Oct 22, 2024 11:35:18 AM	●	Anirudh-Home-AP	--	--	Tester	AWS-NAC-PSK-2	--	--	Client Insights
Wireless	PSK	[REDACTED]	OKTA Key 01	Oct 22, 2024 11:35:03 AM	●	Anirudh-Home-AP	--	--	Tester	AWS-NAC-PSK-2	--	--	Client Insights

- Filter by site name or view the details for entire organization.
- Click period and select one of the defined reporting periods. Alternatively, select a range of days from the calendar to customize the reporting period. By default, the dashboard shows data for the present day (Today).
- Search the client by client type, auth type, user, and matched auth policy rule.

The following illustration shows the filtering done using the **User** option.

Figure 88: Using Filter to Search Clients

The screenshot shows the Juniper Mist NAC Clients page with a search filter applied to the 'User' column. The search bar contains 'OKTA' and 'Clear All'. The table displays three rows of client data, all filtered by the 'OKTA' user.

Client Type	Auth Type	MAC Address	User	Last Seen	State	AP	Part	Matched Auth Policy Rule	Role	SSID	VLAN	GBP Tag	Insights
Wireless	PSK	[REDACTED]	OKTA Key 01	Oct 22, 2024 11:36:31 AM	●	Anirudh-Home-AP	--	--	Tester	AWS-NAC-PSK-2	--	--	Client Insights
Wireless	PSK	[REDACTED]	OKTA Key 01	Oct 22, 2024 11:36:17 AM	●	Anirudh-Home-AP	--	--	Tester	AWS-NAC-PSK-2	--	--	Client Insights
Wireless	PSK	[REDACTED]	OKTA Key 01	Oct 22, 2024 11:35:03 AM	●	Anirudh-Home-AP	--	--	Tester	AWS-NAC-PSK-2	--	--	Client Insights



- By default, the list displays columns such as client type, auth type, MAC address, user and so on. You can use the table options on the top-right corner of the page to display or hide specific columns in the NAC clients list table.
- Use previous and next arrows are located in the top right corner of the list to navigate between the different pages in the list view if the client count is greater than 1000.

3. Click **Client Insights** link under **Insights** column.

The link directs you to **Insights** page where you can view additional details about the NAC clients such as a list of all events recorded by Mist for the client.

## RELATED DOCUMENTATION

[Juniper Mist NAC Architecture | 4](#)

[Juniper Mist Access Assurance Use Cases | 6](#)

[Juniper Mist Access Assurance Best Practices | 14](#)

[Juniper Mist Access Assurance Authentication Methods | 8](#)

[Mist Access Assurance—Frequently Asked Questions | 16](#)

# NAC Events

## SUMMARY

View good, neutral, and bad outcomes of access policies.

## IN THIS SECTION

- [Finding the NAC Event Information | 138](#)
- [View Options | 140](#)
- [NAC Event Types | 141](#)

## Finding the NAC Event Information

You can take two paths to find the NAC Event information.

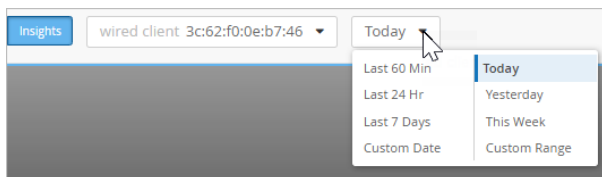
## View NAC Events on the Insights Page

From the left menu, select **Monitor** > **Service Levels**, and then click **Insights**.

NAC events are included in the **Client Events** section. NAC events are listed along with other event types, as shown in this example.

Client Events		Client	
AP Deauthentication	Anonymous	Client	Anonymous
NAC Client Certificate Expired	Anonymous	SSID	CDRP
AP Deauthentication	Anonymous	AP	RH_access_assurance_01
Authorization Failure	Anonymous	Protocol	802.11ac
NAC Client Access Denied	Anonymous	MAC Address	78:08:05:05:01:17
NAC Client Certificate Expired	Anonymous	Number of Screens	2
NAC Server	Anonymous	Last Association	2.1 sec ago
		Reason	23
		Description	Reason code 23: IEEE 802.1X authentication failed
		Reason	04:20:05:7f:63
		Channel	36
		Reason	45 dBm

One advantage of this view is that you can use **Today** menu at the top of the Insights page to select the time frame that you want to view.



## View NAC Events on the Auth Policies Page

From the left menu, select **Organization** > **Access** > **Auth Policies**, and then click the **Show NAC Events** button in the top-right corner of the page. The NAC Events page pops up on the right half of the screen.

One advantage of this view is that you can use the **Auth Rule** menu to show the NAC events for a particular rule in your auth policy. If needed, you can use the search box to narrow down the list to a particular client or device.

Auth Policies

Each user authentication attempt is evaluated according to the list of Policy rules based on Match criteria.

Auth Rule: Any

Search by client mac, name, ip, mac and switch map

NAC Events		Client	
NAC Client Access Denied	2:44:41:188 PM Nov 21, 2024	Client	14:95:51:de:20:e9
NAC Client Access Denied	2:44:37:481 PM Nov 21, 2024	MAC Address	14:95:51:de:20:e9
NAC Client Access Denied	RH_access_assurance... 2:44:19:001 PM Nov 21, 2024	Description	No policy rules are hit, rejected by implicit deny
NAC Client Certificate Expired	RH_access_assurance... 2:44:19:000 PM Nov 21, 2024	Authentication Type	MAB
NAC Server Certificate Validation Success	RH_access_assurance... 2:44:19:000 PM Nov 21, 2024	User Name	149510a20e9
NAC Client Access Denied	RH_access_assurance... 2:43:50:007 PM Nov 21, 2024	Auth Rule	No Rule Match
NAC Client Access Denied	RH_access_assurance... 2:43:50:006 PM Nov 21, 2024	RADIUS Returned Attributes	Reply-Message=No policy rules are hit, rejected by implicit deny
NAC Server Certificate Validation Success	RH_access_assurance... 2:43:50:005 PM Nov 21, 2024	Port ID	ge-0/0/10.0
NAC Client Access Denied	RH_access_assurance... 2:43:50:005 PM Nov 21, 2024	Switch Mac	bc:0f:0c:0c:66:44
NAC Server Certificate Validation Success	RH_access_assurance... 2:43:50:005 PM Nov 21, 2024	Port Type	wired
NAC Client Access Denied	RH_access_assurance... 2:43:50:005 PM Nov 21, 2024	NAS Vendor	juniper-mst

## View Options

On both the Insights page and the NAC Events pop-up page, you can use various UI features to view information about NAC events.

- Use the tabs above the event list to show all, good, neutral, or bad events.
- To select the event types to include, click the **Event Filter** button at the top-right corner of the event list.



For a full list of the available events, see "[NAC Event Types](#)" on page 141.

- To see the latest available data, click the **Refresh** button at the top-right corner of the events list.



- Click an event to see a summary on the right side of the page.

NAC Events		6060 Total	2095 Good	0 Neutral	3965 Bad	< 1-1,000 of 6,060 > ☰
NAC Client Access Denied	2:44:41.768 PM Nov 27, 2024					
NAC Client Access Allowed	2:44:37.685 PM Nov 27, 2024					
NAC Client Access Denied	RH_access_assurance... 2:44:19.991 PM Nov 27, 2024					
NAC Client Certificate Expired	RH_access_assurance... 2:44:19.990 PM Nov 27, 2024					
NAC Server Certificate Validation Success	RH_access_assurance... 2:44:19.989 PM Nov 27, 2024					
NAC Client Access Denied	RH_access_assurance... 2:43:50.607 PM Nov 27, 2024					
NAC Client Certificate Expired	RH_access_assurance... 2:43:50.606 PM Nov 27, 2024					
NAC Server Certificate Validation Success	RH_access_assurance... 2:43:50.605 PM Nov 27, 2024					

<b>Client</b>	f4:f9:51:de:20:e9
<b>MAC Address</b>	f4:f9:51:de:20:e9
<b>Description</b>	No policy rules are hit, rejected by implicit deny
<b>Authentication Type</b>	MAB
<b>User Name</b>	f4f951de20e9
<b>Auth Rule</b>	No Rule Match
<b>RADIUS Returned Attributes</b>	Reply-Message=No policy rules are hit, rejected by implicit deny
<b>Port ID</b>	ge-0/0/10.0
<b>Switch Mac</b>	bc:0f:fe:fb:66:44
<b>Port Type</b>	wired
<b>NAS Vendor</b>	juniper-mist

- In the summary, click a hyperlink to view more information.
  - The **Client** link goes to the Insights page. There, you'll see additional client and event information.
  - The **Auth Policy** link highlights the policy on the Auth Policies page.



**TIP:** If you're using the pop-up NAC Events page, the Auth Policies are partly hidden behind the pop-up window. You might prefer to open this link in a new tab.

## NAC Event Types

To select the event types to include, click the Event Filter button at the top-right corner of the NAC Events section.



In the Event Filter pop-up window, select or clear the check boxes to show or hide the events. Click **OK** to save your settings.

**Table 11: NAC Event Types**

Positive NAC Events	Neutral NAC Events	Negative NAC Events
<ul style="list-style-type: none"> <li>• NAC Client Access Allowed</li> <li>• NAC Client Certificate Validation Success</li> <li>• NAC Machine Certificate Validation Success</li> <li>• NAC User Certificate Validation Success</li> <li>• NAC CoA Disconnect</li> <li>• NAC CoA Reauthenticate</li> <li>• NAC IDP Authentication Success</li> <li>• NAC IDP Group Lookup Success</li> <li>• NAC IDP User Lookup Success</li> <li>• NAC MDM Lookup Success</li> <li>• NAC Server Certificate Validation Success</li> </ul>	<ul style="list-style-type: none"> <li>NAC MDM Device Not Found</li> </ul>	<ul style="list-style-type: none"> <li>• NAC Client Access Denied</li> <li>• NAC Client Cert Revoked</li> <li>• NAC Client Certificate Expired</li> <li>• NAC Client Certificate Validation Failure</li> <li>• NAC Machine Certificate Expired</li> <li>• NAC Machine Certificate Revoked</li> <li>• NAC Machine Certificate Validation Failure</li> <li>• NAC User Certificate Expired</li> <li>• NAC User Certificate Revoked</li> <li>• NAC User Certificate Validation Failure</li> <li>• NAC IDP Admin Config Failure</li> <li>• NAC IDP Admin Config Failure</li> <li>• NAC IDP Authentication Failure</li> <li>• NAC IDP Group Lookup Failure</li> <li>• NAC IDP Lookup Failure</li> <li>• NAC IDP Unknown</li> <li>• NAC IDP Unreachable</li> <li>• NAC IDP User Disabled</li> <li>• NAC IDP User Lookup Failure</li> </ul>

Table 11: NAC Event Types (Continued)

Positive NAC Events	Neutral NAC Events	Negative NAC Events
		<ul style="list-style-type: none"> <li>• NAC MDM Lookup Failure</li> <li>• NAC Server Certificate Validation Failure</li> </ul>

## Validate Access and Authentication

### IN THIS SECTION

- [Check Connected Client Devices | 143](#)
- [Check Failed Client Devices | 145](#)
- [Marvis Actions to Identify Authentication Issues | 146](#)

Read this topic to learn how to validate user access and authentication in Juniper Mist portal.

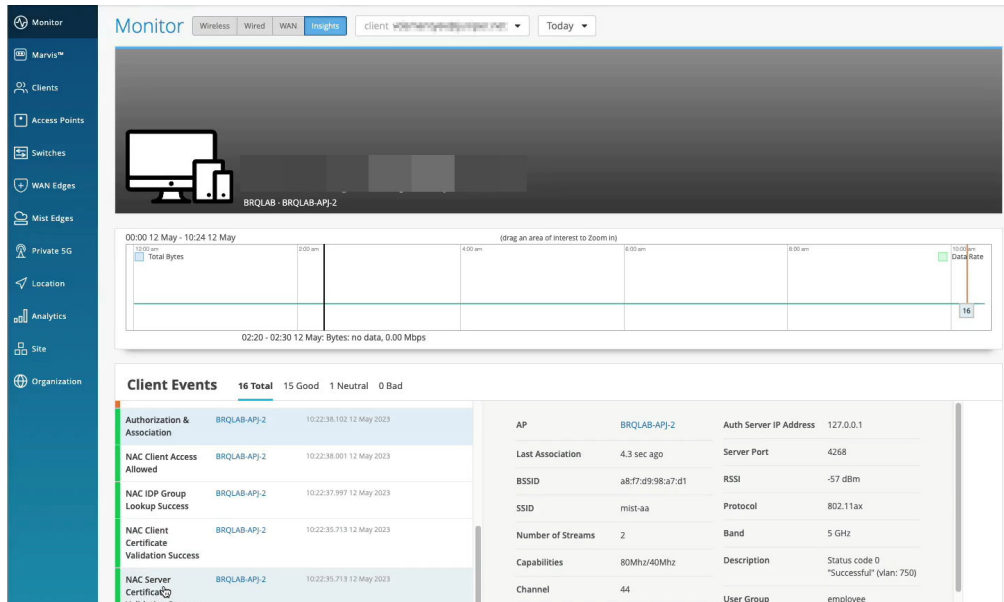
### Check Connected Client Devices

1. On Juniper Mist portal, select **Clients > WiFi Clients** or **Clients > Wired Clients** to open the clients page.

This page lists all the clients connected to your site. It provides the details such as name, IPv4 address, MAC address, Type, and so on. You can also see the link to **Client Insights**. Click this link to go to **Monitor > Insights page** where you view get additional details.

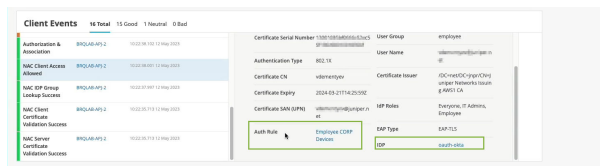
2. Go to the Insights dashboard directly, select **Monitor > Service Levels** from the left menu of the Juniper Mist portal. Then click the **Insights** button at the top of the Monitor page.

Figure 89: View Mist Insights Page



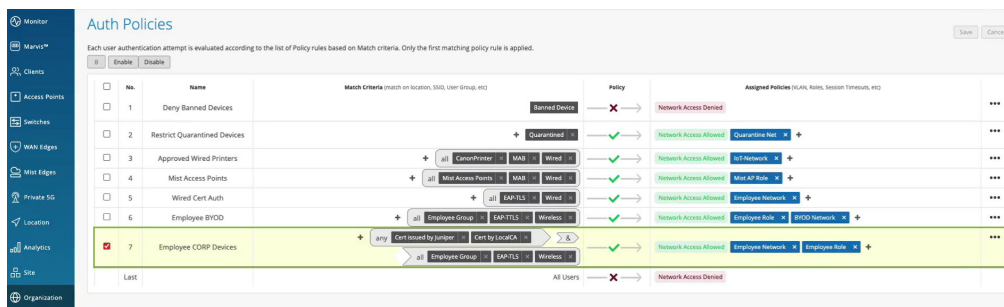
3. In the Client Events block, you can view a list of all events recorded by Mist PACE for the selected site during the selected time frame.

Figure 90: View Client Events



These events apply only to wireless clients such as cell phones and laptop computers. When you select an event from the list, Mist shows a summary of the event to the right of the list. You can see the details such as Certificate details, authentication type, VLAN, Auth Rule, and Identity provider (IdP).

4. Click on the **Auth Rule** to open the rule in Auth Policies page.



The portal highlights the policy that was applied to the client device. You can view the details such as match criteria, policy rule, and policy action.

Watch the following video on validating access and authentication configuration:

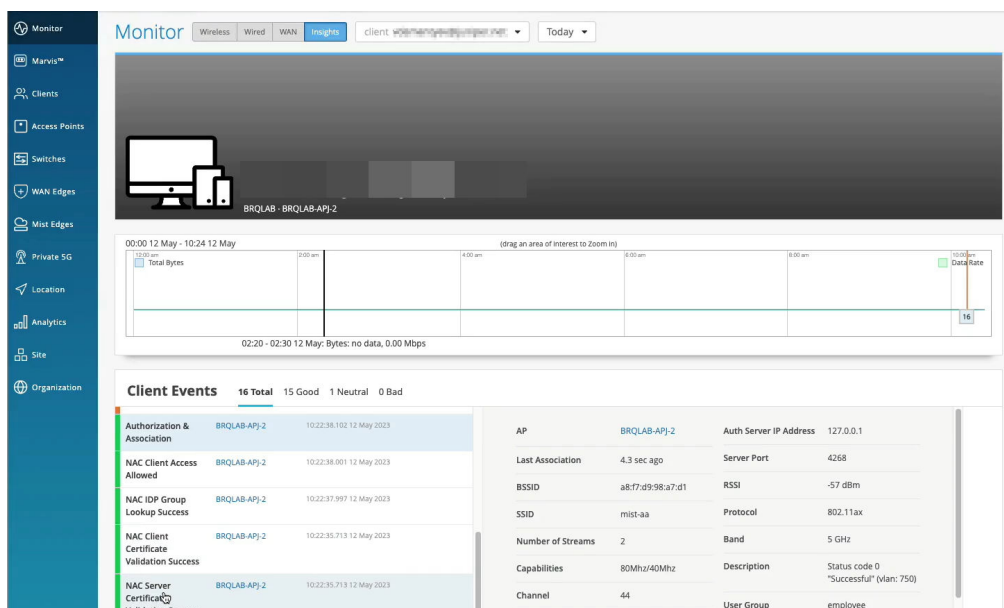


Video: [How to Validate](#)

## Check Failed Client Devices

1. On Juniper Mist portal, select **Monitor** > **Service Levels** from the left menu of the Juniper Mist portal. Then click the **Insights** button at the top of the Monitor page.

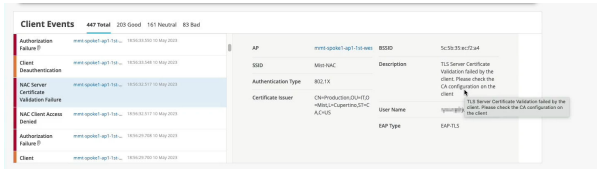
Figure 91: View Mist Insights Page



2. In the Client Events block, you can view a list of all events recorded by Mist PACE for the selected site during the selected time frame.



Figure 92: View Client Events



When you select an event from the list, Mist shows a summary of the event to the right of the list. You can scroll up and down on the summary to get all the details. In case of a failed access, you can check the **Description** field to understand the reason for failure.

Watch the following video on validating access and authentication configuration:



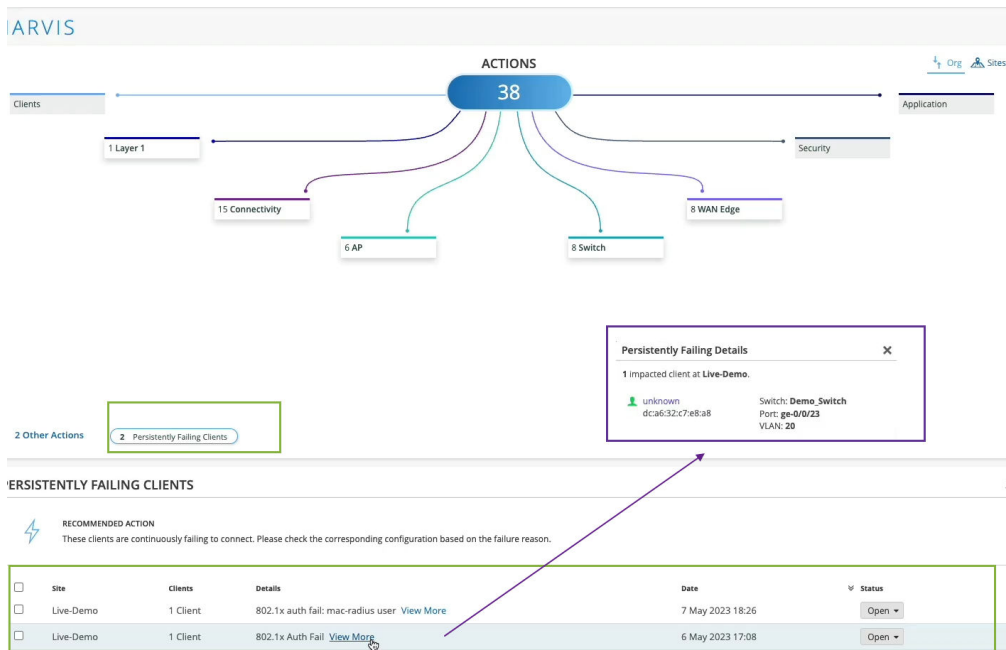
Video: [Mist Access Assurance - Troubleshoot Client](#)

## Marvis Actions to Identify Authentication Issues

Marvis Actions is a one-stop information center that provides visibility into ongoing site-wide network issues that affect user experience in an organization.

The type of subscription you have for your organization determines the Marvis Actions usage. See [Marvis Actions for Wired, WAN, and Wireless Assurance](#) for details.

1. On Juniper Mist portal, select **Marvis™** from the left menu of the Juniper Mist portal.



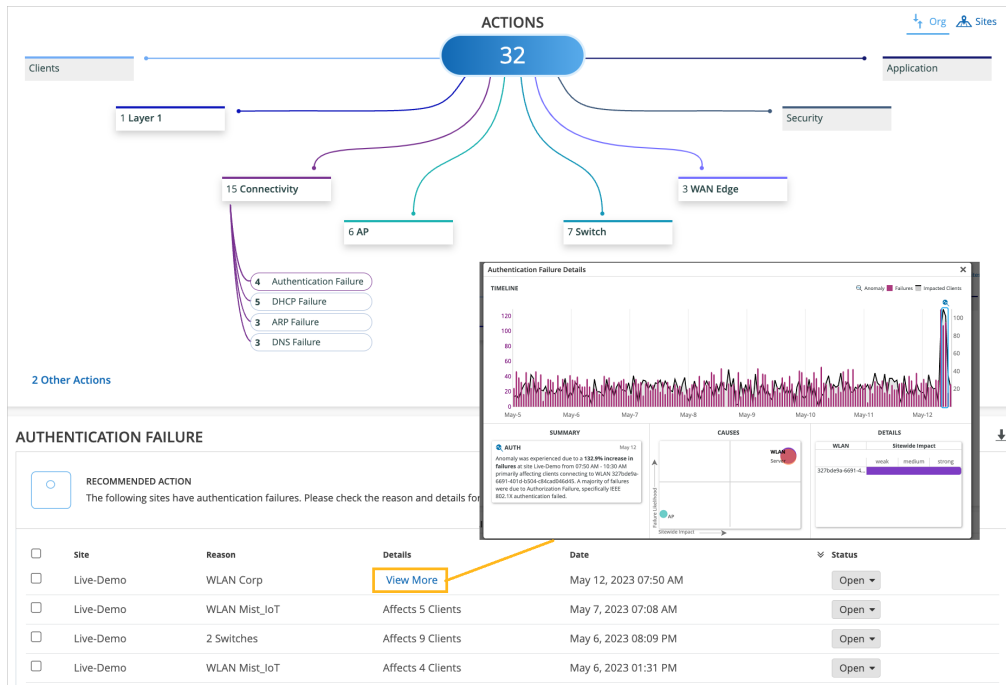
The Persistently Failing Clients action highlights wired or wireless clients that continuously fail to connect due to a client-specific issue; that is, the scope of failure isn't the access point (AP), switch, wireless LAN (WLAN), or server. The failure can be due to authentication failures from entering the wrong preshared key (PSK) or failures caused by incorrect 802.1x configuration. Marvis displays the list of clients experiencing a failure and the WLANs they are trying to connect to.

Click **View More** to get the details of the failing client. You can use this information to identify the location of users who are experiencing connectivity issues by pinpointing the specific switch, port, and VLAN they are connected to.

**NOTE:** Note:  
 After you fix this issue, the Persistently Failing Clients action automatically resolves within an hour. As this action is considered low priority, Marvis does not list the Persistently Failing Clients action in the Latest Updates section or on the Sites tab.

- In the MARVIS page, you'll notice that the page displays the information under different categories. Marvis indicates the number of issues detected for a category. For example, in the following screenshot, you'll notice that Marvis lists 15 issues for the Connectivity category.

Figure 93: Connectivity Failures in Marvis Actions Page



Click **View More** to get the details of the failing client. The Authentication Failure Details page showing the summary of the issue, cause, and details. The screenshot shows an example of how Marvis Actions reports an 802.1x authentication failure.

If the issue is not related to authentication or authorization, look at the layer above and investigate if there is an actual network service-related issue. For instance, your gateway may not be responding, or you may have run out of IP addresses.

Watch the following video on Marvis actions on validating access and authentication configuration:



Video: [Troubleshoot Client Marvis CI](#)

## SEE ALSO

[NAC Events | 138](#)

[Configure Authentication Policy | 69](#)

[Configure Certificate-Based \(EAP-TLS \) Authentication | 83](#)

[Configure Certificate-Based \(EAP-TLS \) Authentication with Azure IdP Integration | 95](#)