Juniper Networks | Engineering Simplicity

Juniper Mist Access Assurance Guide

Published
2026-01-27

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

Juniper Mist Access Assurance Guide

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

SUMMARY

Trace the evolution of network access control solutions from the early days of limited corporate use cases to today's wide-ranging requirements for corporate, guest, BYOD, and IoT solutions. Learn how Juniper Mist Access Assurance helps you respond to these challenges through rich features that enhance the user experience while providing you with simplified management and complete visibility.

IN THIS SECTION

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.
- Seemless 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

SUMMARY

Watch videos to get familiar with the architecture behind Juniper Mist Access Assurance. Learn more about microservices and how they Juniper Mist leverages them to provide high availability and scalability.

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.

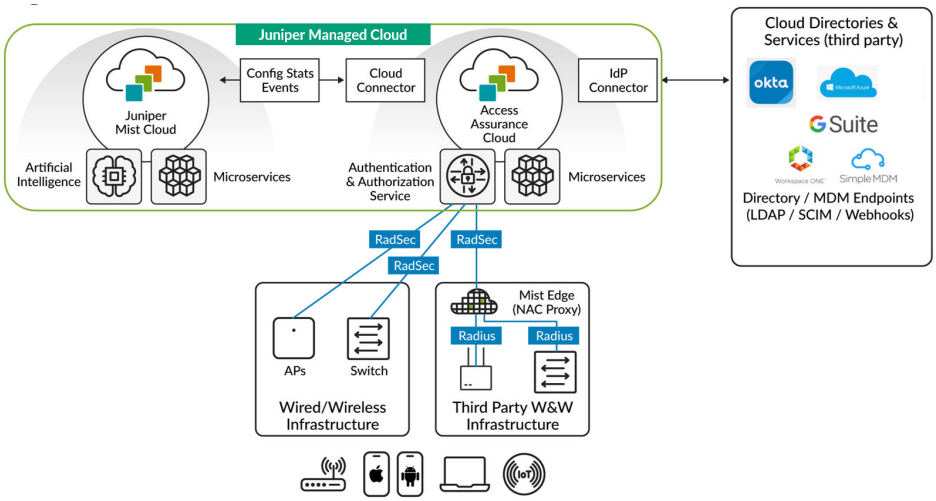
Watch the following video for Mist Access Assurance architecture:

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 5 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

SUMMARY

See how you can deploy Juniper Mist Access Assurance for managed devices, guest devices, IoT devices, and BYOD 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
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 Authentication Methods

SUMMARY

Deploy Juniper Mist Access Assurance with either 802.1X authentication or non-802.1X authentication. Compare the various options to select the best approach for your organization.

IN THIS SECTION

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

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

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

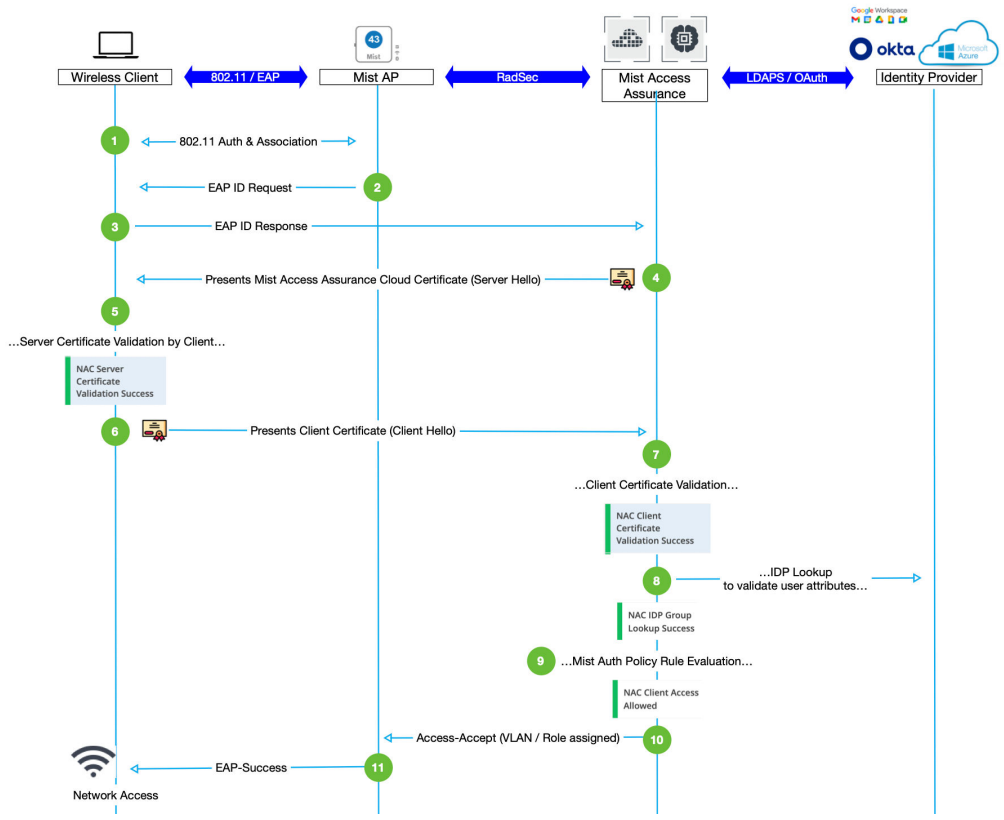
EAP-TLS leverages certificates and cryptography to provide mutual authentication between the client and the server. Both the client and the server must receive a digital certificate signed by a certificate authority (CA) that both the entities trust. This method uses certificates on both the client and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

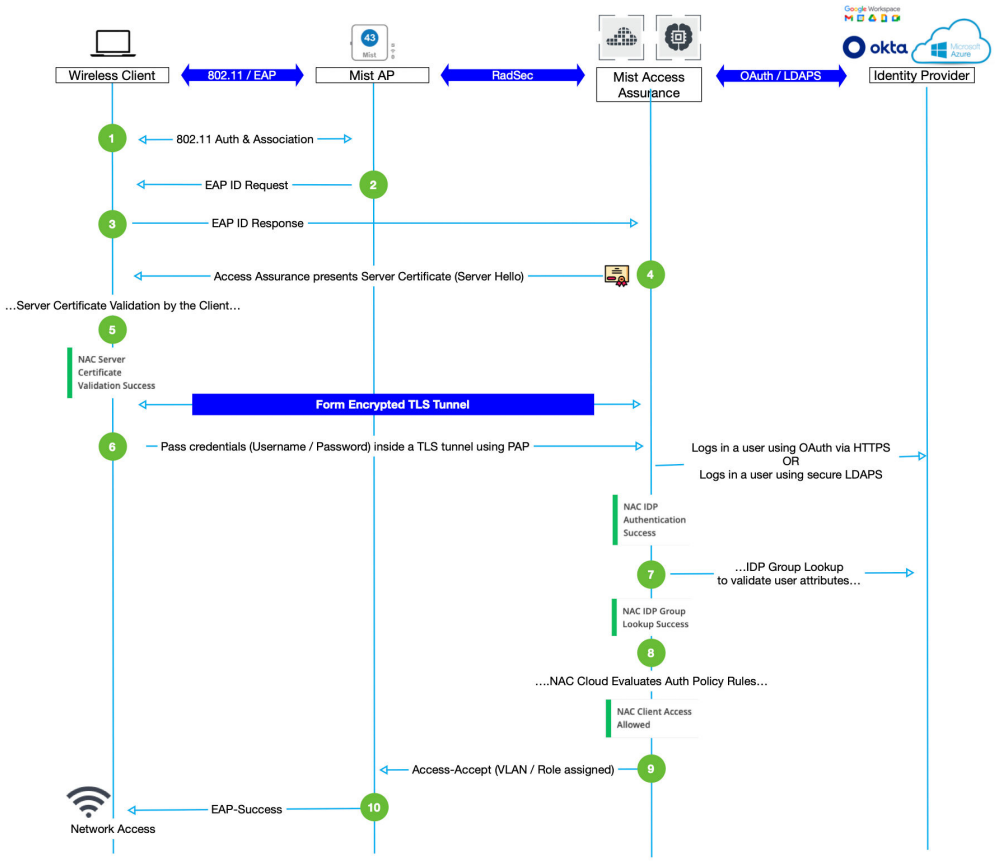
3. The supplicant sends an EAP response to the authentication server (Juniper Mist Access Assurance cloud) through the authenticator.
4. The authentication server responds to the client device with a "Server Hello" message that includes a certificate.
5. The supplicant validates the server certificate. That is, the supplicant verfies 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

SUMMARY

Follow these recommendations to ensure best results when deploying Juniper Mist Access Assurance.

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

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?

Refer to Subscription Types for Juniper Mist - Access Assurance for the latest Access Assurance subscription details.

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 EX4000 series switches running Junos release of 24.4R1-S2.15 and 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

GovClolud

- 52.222.121.10
- 182.30.31.137

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.

For GovCloud, you must allow outbound connections destined to *radsec.nac.us.mist-federal.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.

What are the minimum certificate requirements for using Extensible Authentication Protocol (EAP)?

For EAP certificates, the minimum requirements include using a strong hash algorithm like SHA-256 or better, and a minimum key length of 2048 bits.

RELATED DOCUMENTATION

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

What Do You Want to Do?

Table 3: Top Tasks

If you want to...	Use these resources:
Add Microsoft Entra ID (formerly known as Azure Active Directory) as IdP *Integrate Microsoft Entra ID to validates user attributes before enforcing role-based access policies.*	"Integrate Microsoft Entra ID as an Identity Provider" on page 46
Set up Okta as an identity provider *Configure Okta Workforce Identity Cloud through the Juniper Mist dashboard to authenticate end users attempting to access the network.*	"Integrate Okta as an Identity Provider" on page 40
Add Google Workspace as IdP *Integrate with Google Workspace IdP to leverage secure Lightweight Directory Access Protocol for user/group account provisioning.*	"Integrate Google Workspace as an Identity Provider" on page 29
Configure identity providers *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.*	"Add Identity Providers for Juniper Mist Access Assurance" on page 23

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

Add Identity Providers for Juniper Mist Access Assurance

SUMMARY

Follow these steps to add your identity providers to your organization to enhance authentication and access control. Understand the various options available in the Identity Provider (IdP) settings.

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:

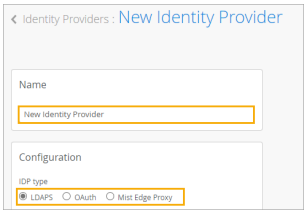
  - "Integrate Microsoft Entra ID as an Identity Provider" on page 46
  - "Integrate Okta as an Identity Provider" on page 40
  - "Integrate Google Workspace as an Identity Provider" on page 29

- 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**



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

   LDAPS

Table 4: Settings for LDAPS IdPs

Parameters	Details
LDAP Type	Select one of the following options from the drop-down menu: • **Azure** • **Okta** • **Custom** Specify the LDAP filter that will identify the type of group, member, or user. This option is available only for LDAP Type **Custom**.
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 **Bind DN**.
Base DN	Enter a whole domain or a specific organization unit (container) in **Search base** 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.

OAuth

For OAuth type of authentication, enter the values as provided in Table 5 on page 26. 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 46 or "Integrate Okta as an Identity Provider" on page 40.

Table 5: Settings for OAuth IdPs

Parameters	Description
OAuth Type	Select one of the following options from the drop-down menu: • Azure • Okta
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.
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.

Table 5: Settings for OAuth IdPs *(Continued)*

Parameters	Description
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 **OAuth Client Credential (CC) Client Id**.

Mist Edge Proxy

Table 6: Settings for Mist Edge Proxy

Parameters	Description
Proxy Hosts	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 **Mist Edge Cluster** field. Mist Edge will listen on the specified addresses for: • Inbound RadSec requests from Mist Access Assurance • RADIUS requests from external RADIUS servers
SSIDs	Enter a comma-separated list of the SSIDs that this IdP will use.
Mist Edge Cluster	Select a cluster from the list. **NOTE**: If you need to add a Mist Edge cluster, select **Mist Edges** from the left menu, and then select **Create Cluster**, and enter the information.

Table 6: Settings for Mist Edge Proxy *(Continued)*

Parameters	Description
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 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: *1abc_university.edu*
RADIUS Authentication Servers	You must specify at least one server. Click **Add Server**, and then enter the IP address, port, and shared secret.
RADIUS Accounting Servers	Click **Add Server**, and then enter the IP address, port, and shared secret.

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

RELATED DOCUMENTATION

- Juniper Mist Access Assurance Use Cases | 6
- Juniper Mist Access Assurance Best Practices | 14
- Juniper Mist Access Assurance Authentication Methods | 8
- Integrate Okta as an Identity Provider | 40
- Integrate Microsoft Entra ID as an Identity Provider | 46

Integrate Google Workspace as an Identity Provider

SUMMARY

Follow these steps to add Mist as a client in your Google Workspace portal, download your certificate, and add your Identity Provider to your Juniper Mist organization.

IN THIS SECTION

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

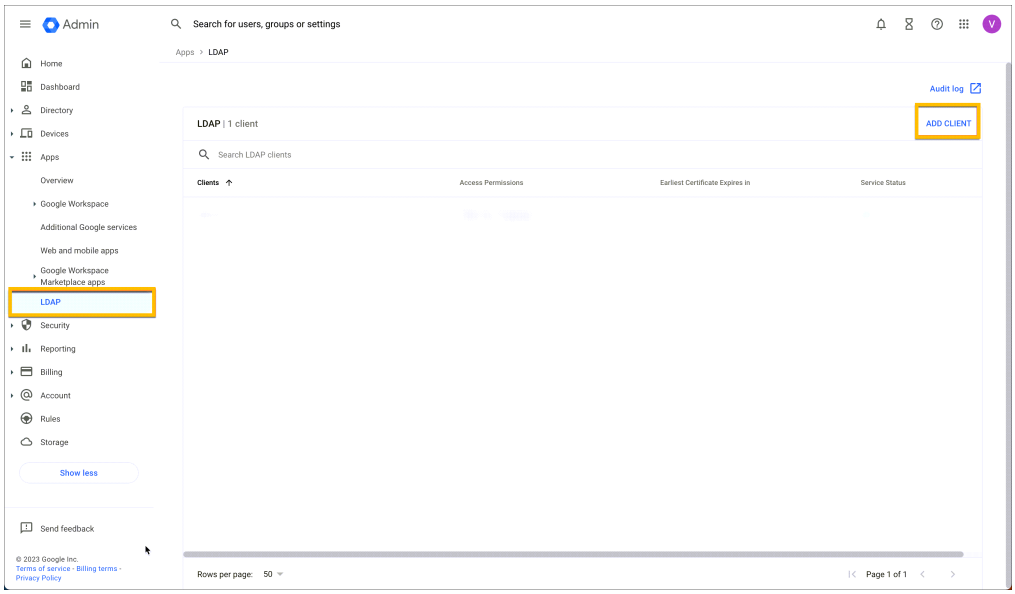
NOTE: Some of the screenshots included in this document are sourced from third-party applications. Be aware that these screenshots may change over time and may not always match the current version of the applications.

Configuration on Google Workspace

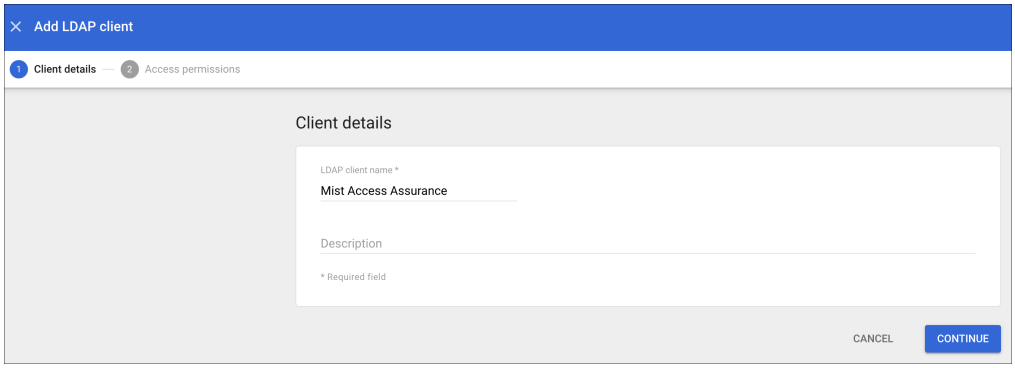
The following procedure shows you how to configure Google Workspace as an identity provider (IdP) with Juniper Mist.

NOTE: The screenshots from third-party applications are correct at the time of publishing. We have no way to know when or if the screenshots will be accurate at any future time. Please refer to the third-party website for guidance about changes to these screens or the workflows involved.

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**.



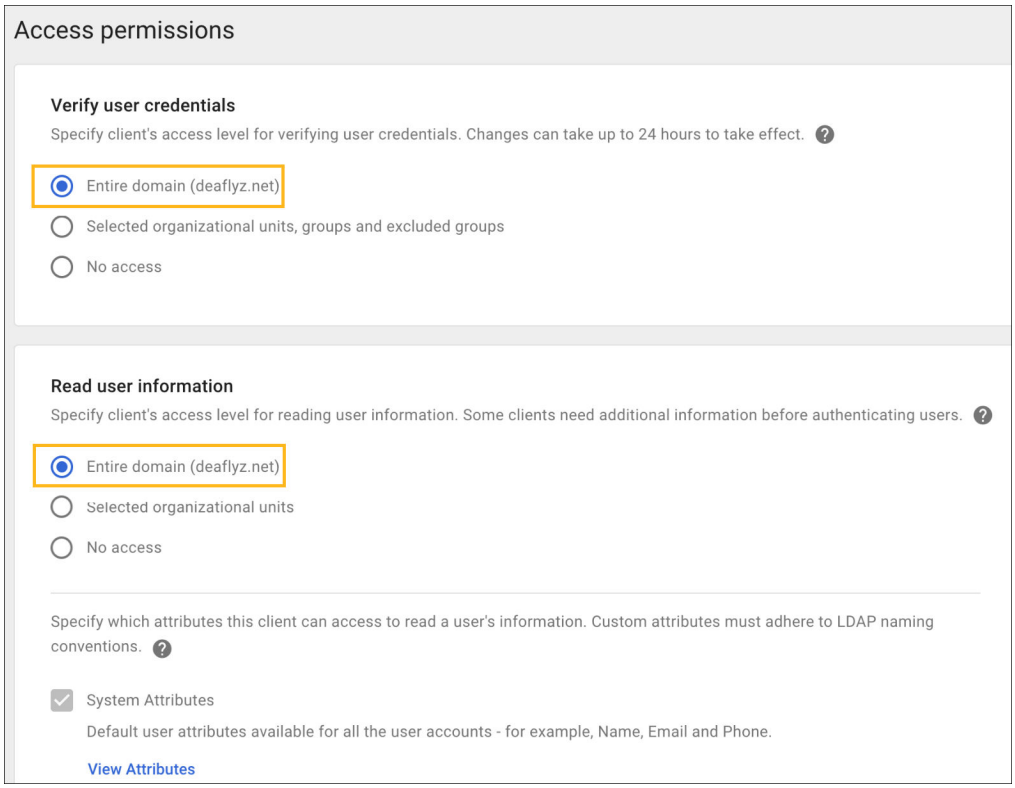
   b. Provide an **LDAP client name** and an optional **Description** and click **Continue**.



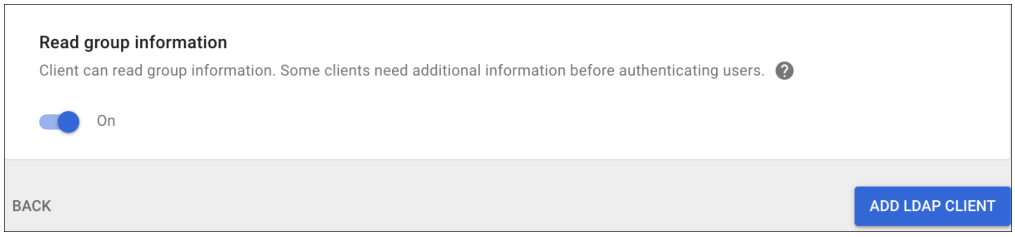
   The **Access permissions** page is displayed after adding the LDAP client.
3. Configure Access Permission for verifying user credentials.
   The following options are available:

- **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.



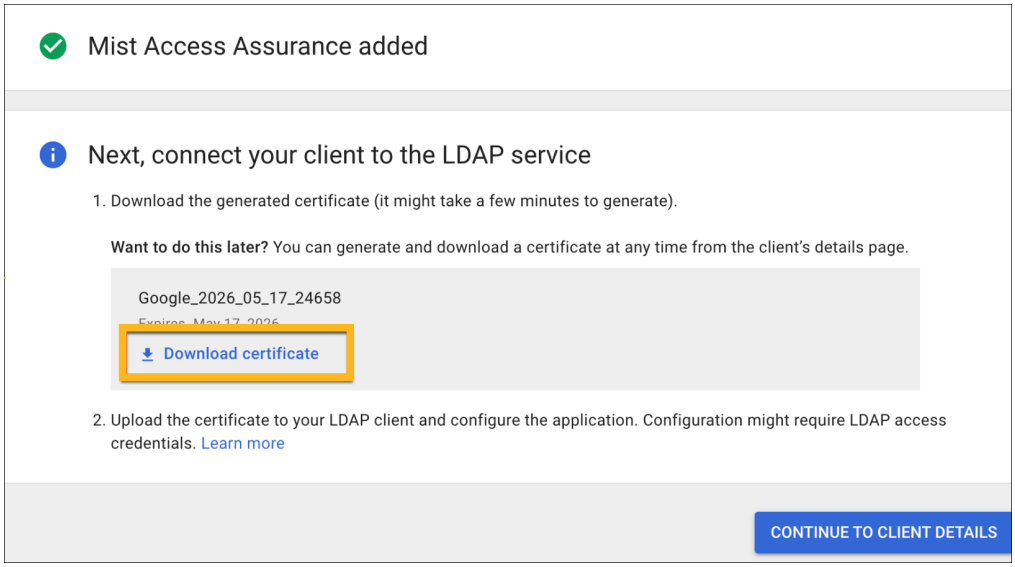
b. Scroll down to **Read group information**. This setting specifies whether the LDAP client can read group details and check a user's group memberships.



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.

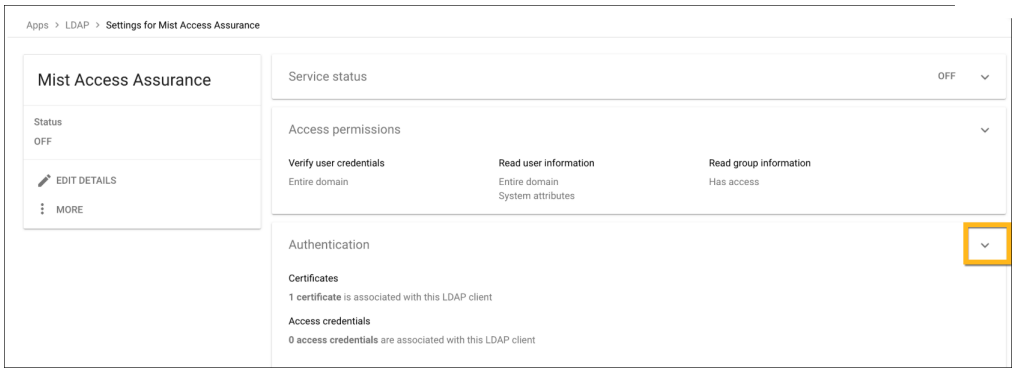
a. Click **Download certificate** and save the downloaded certificate in a secure place. You'll need this certificate when you set up an IdP on the Juniper Mist portal.



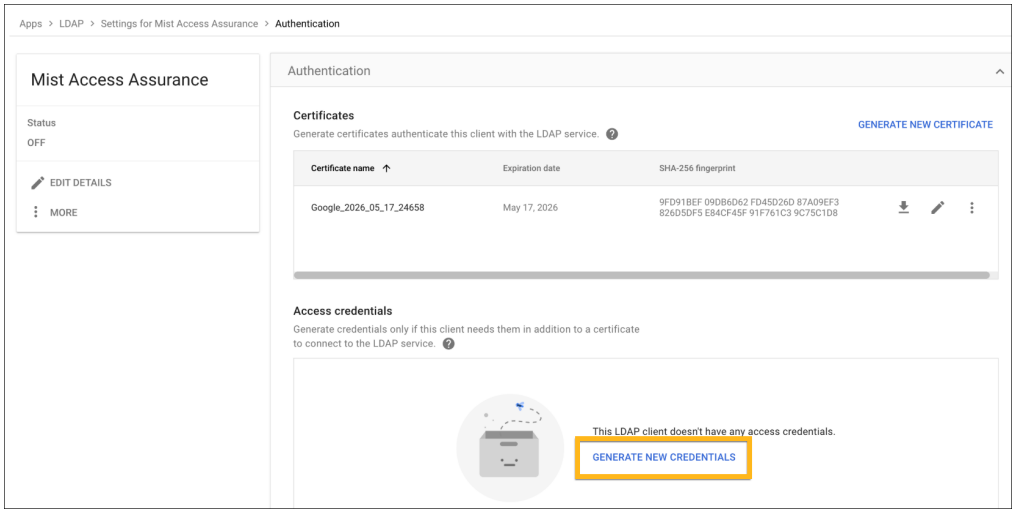
b. Click **Continue to Client Details**.

The Settings for <LDAP client name> page appears.

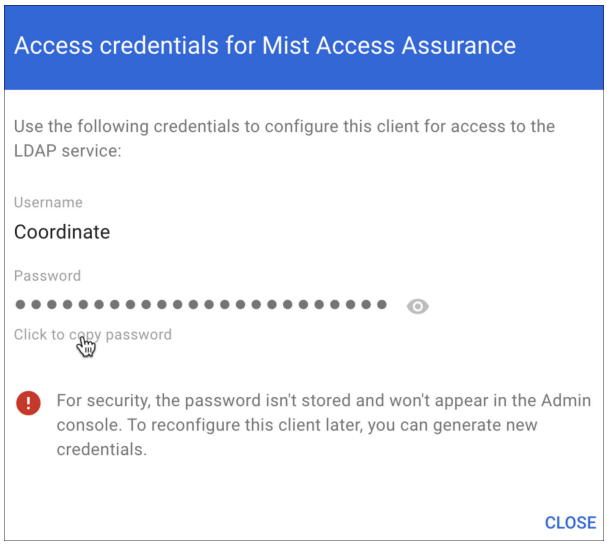
c. Expand the **Authentication** section.



d. Under Access Credentials, click **Generate New Credentials**.



You can view the username and password on the **Access credentials** page.

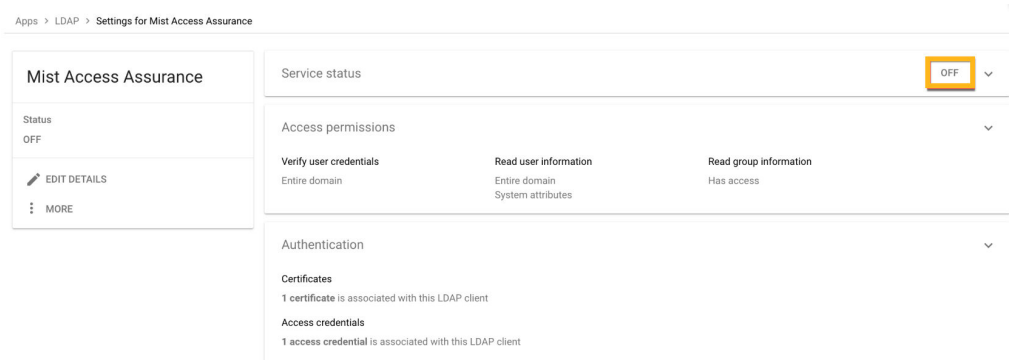


Copy and save the username and password. You need these details for the LDAPS client configuration on the Juniper Mist cloud portal.

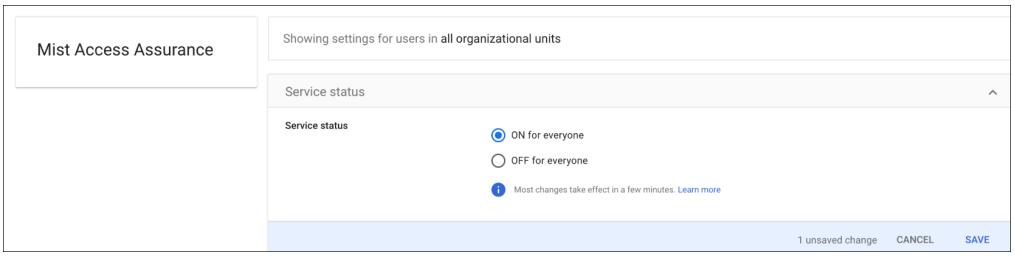
5. Enable the LDAP client service by changing the service status to **On** for the LDAP client. This step enables you to set up a client with the Secure LDAP service.

   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**.



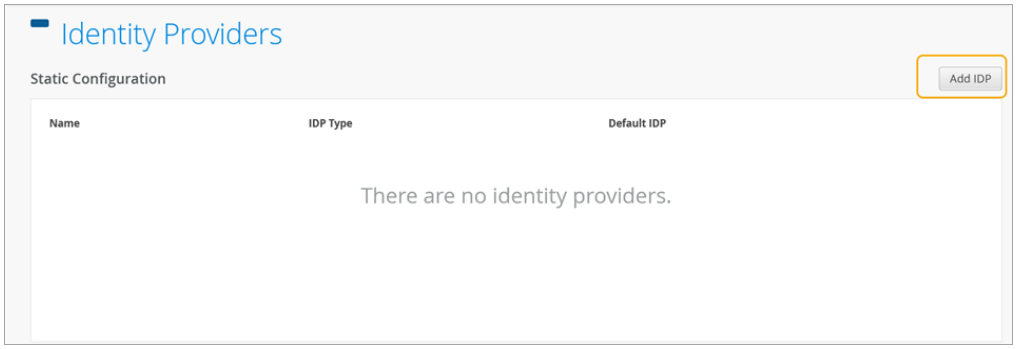
Select **On for everyone** to turn on the service. Allow some time for the changes to apply on the Google side.



Configuration on Juniper Mist Dashboard

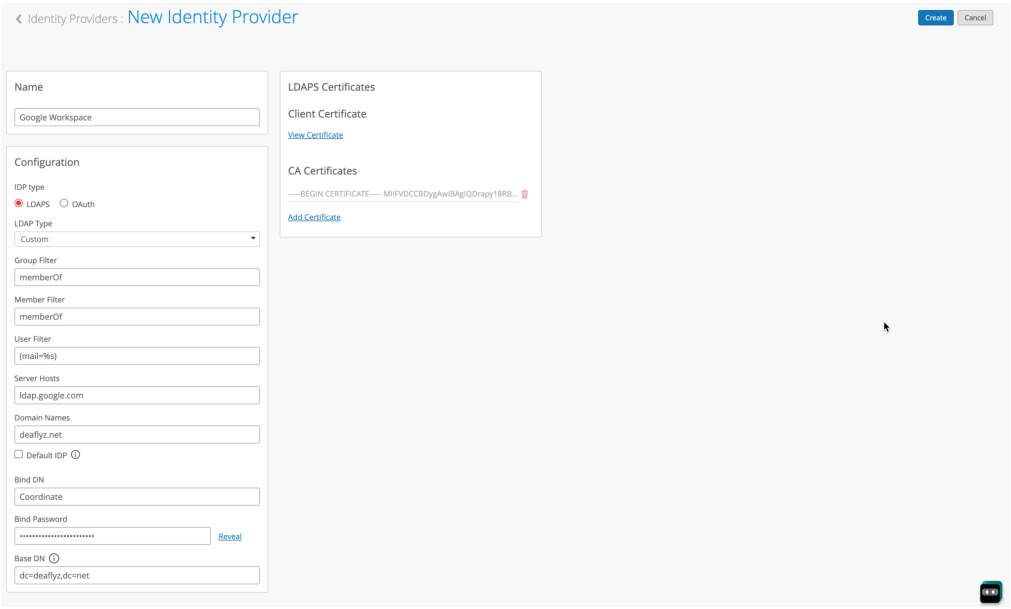
1. From the left menu of the Juniper Mist portal, select **Organization** > **Access** > **Identity Providers**. The Identity Providers page displays any configured identity providers.

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

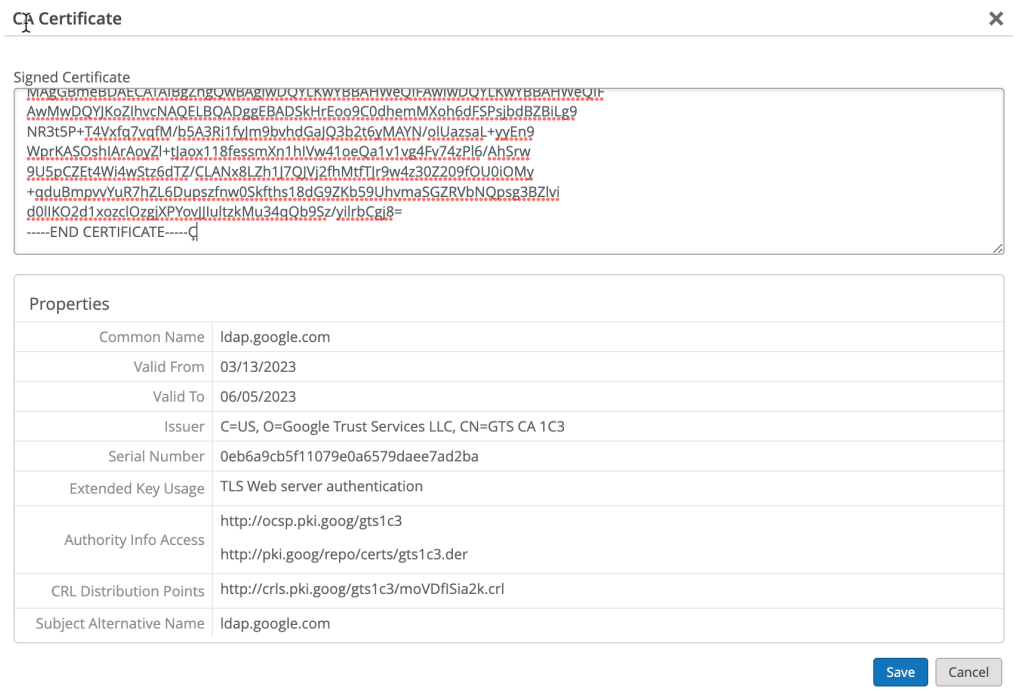


Now configure the LDAPS connector to integrate with the Google Workspace LDAP endpoint.

- **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

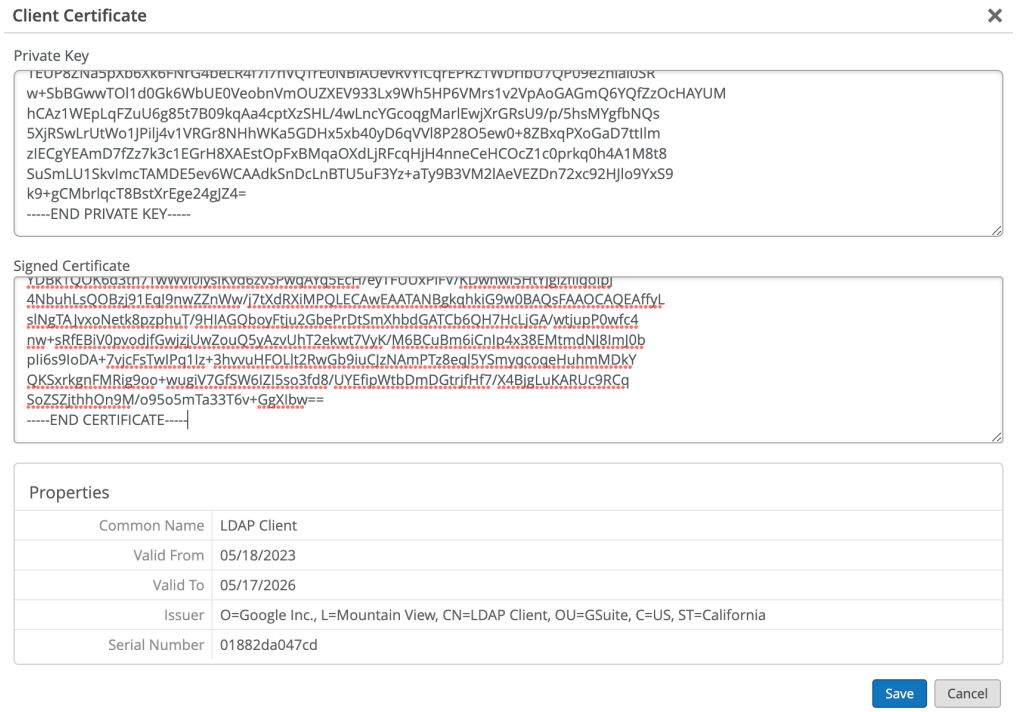



```
-----BEGIN CERTIFICATE-----
MIIFljCCA36gAwIBAgINAgO8U1lrNMcY9QFQZjANBgkqhkiG9w0BAQsFADBHMQsw
CQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExMQzEU
MBIGA1UEAxMLR1RTIFJvb3QgUjEwHhcNMjAwODEzMDAwMDQyWhcNMjcwOTMwMDAw
MDQyWjBGMQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZp
Y2VzIExMQzETMBEGA1UEAxMKR1RTIENBIDFDMzCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAPWI3+dijB43+DdCkH9sh9D7ZYIl/ejLa6T/belaI+KZ9hzp
kgOZE3wJCor6QtZeViSqejOEH9Hpabu5dOxXTGZok3c3VVP+ORBNtzS7XyV3NzsX
lOo85Z3VvMO0Q+sup0fvsEQRY9i0QYXdQTBIkxu/t/bgRQIh4JZCF8/ZK2VWNAcm
BA2o/X3KLu/qSHw3TT8An4Pf73WELnlXXPxXbhqW//yMmqaZviXZf5YsBvcRKgKA
gOtjGDxQSYflispfGStZloEAoPtR28p3CwvJlk/vcEnHXG0g/Zm0tOLKLnf9LdwL
tmsTDIwZKxeWmLnwi/agJ7u2441Rj72ux5uxiZ0CAwEAAaOCAYAwggF8MA4GA1Ud
DwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwEgYDVR0T
AQH/BAgwBgEB/wIBADAdBgNVHQ4EFgQUinR/r4XN7pXNPZzQ4kYU83E1HScwHwYD
VR0jBBgwFoAU5K8rJnEaK0gnhS9SZizv8IkTcT4waAYIKwYBBQUHAQEEXDBaMCYG
CCsGAQUFBzABhhpodHRwOi8vb2NzcC5wa2kuZ29vZy9ndHNyMTAwBggrBgEFBQcw
AoYkaHR0cDovL3BraS5nb29nL3JlcG8vY2VydHMvZ3RzcjEuZGVyMDQGA1UdHwQt
MCswKaAnoCWGI2h0dHA6Ly9jcmwucGtpLmdvb2cvZ3RzcjEvZ3RzcjEuY3JsMFcG
A1UdIARQME4wOAYKKwYBBAHWeQIFAzAqMCgGCCsGAQUFBwIBFhxodHRwczovL3Br
aS5nb29nL3JlcG9zaXRvcnkvMAgGBmeBDAECATAIBgZngQwBAgIwDQYJKoZIhvcN
AQELBQADggIBAIl9rCBcDDy+mqhXlRu0rvqrpXJxtDaV/d9AEQNMwkYUuxQkq/BQ
```

```
cSLbrcRuf8/xam/IgxvYzolfh2yHuKkMo5uhYpSTld9brmYZCwKWnvy15xBpPnrL
RklfRuFBsdeYTWU0AIAaP0+fbH9JAIFTQaSSIYKCGvGjRFsqUBITTcFTNvNCCK9U
+o53UxtkOCcXCb1YyRt8OS1b887U7ZfbFAO/CVMkH8IMBHmYJvJh8VNS/UKMG2Yr
PxWhu//2m+OBmgEGcYk1KCTd4b3rGS3hSMs9WYNRtHTGnXzGsYZbr8w0xNPM1IER
lQCh9BIiAfq0g3GvjLeMcySsN1PCAJA/Ef5c7TaUEDu9Ka7ixzpiO2xj2YC/WXGs
Yye5TBeg2vZzFb8q3o/zpWwygTMD0IZRcZk0upONXbVRWPeyk+gB9lm+cZv9TSjO
z23HFtz30dZGm6fKa+l3D/2gthsjgx0QGtkJAITgRNOidSOzNIb2ILCkXhAd4FJG
AJ2xDx8hcFH1mt0G/FX0Kw4zd8NLQsLxdxP8c4CU6x+7Nz/OAipmsHMdMqUybDKw
juDEI/9bfU1lcKwrmz3O2+BtjjKAvpafkmO8l7tdufThcV4q5O8DIrGKZTqPwJNl
1IXNDw9bg1kWRxYtnCQ6yICmJhSFm/Y3m6xv+cXDBlHz4n/FsRC6UfTd
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFYjCCBEqgAwIBAgIQd70NbNs2+RrqIQ/E8FjTDTANBgkqhkiG9w0BAQsFADBX
MQswCQYDVQQGEwJCRTEZMBcGA1UEChMQR2xvYmFsU2lnbiBudi1zYTEQMA4GA1UE
CxMHUm9vdCBDQTEbMBkGA1UEAxMSR2xvYmFsU2lnbiBSb290IENBMB4XDTIwMDYx
OTAwMDA0MloXDTI4MDEyODAwMDA0MlowRzELMAkGA1UEBhMCVVMxIjAgBgNVBAoT
GUdvb2dsZSBUcnVzdCBTZXJ2aWNlcyBMTEMxFDASBgNVBAMTC0dUUyBSb290IFIx
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAthECix7joXebO9y/lD63
ladAPKH9gvl9MgaCcfb2jH/76Nu8ai6Xl6OMS/kr9rH5zoQdsfnFl97vufKj6bwS
iV6nqlKr+CMny6SxnGPb15l+8Ape62im9MZaRw1NEDPjTrETo8gYbEvs/AmQ351k
KSUjB6G00j0uYODP0gmHu81I8E3CwnqIiru6z1kZ1q+PsAewnjHxgsHA3y6mbWwZ
DrXYfiYaRQM9sHmklCitD38m5agI/pboPGiUU+6DOogrFZYJsuB6jC511pzrp1Zk
j5ZPaK49l8KEj8C8QMALXL32h7M1bKwYUH+E4EzNktMg6TO8UpmvMrUpsyUqtEj5
cuHKZPfmghCN6J3Cioj6OGaK/GP5Afl4/Xtcd/p2h/rs37EOeZVXtL0m79YB0esW
CruOC7XFxYpVq9Os6pFLKcwZpDIlTirxZUTQAs6qzkm06p98g7BAe+dDq6dso499
iYH6TKX/1Y7DzkvgtdizjkXPdsDtQCv9Uw+wp9U7DbGKogPeMa3Md+pvez7W35Ei
Eua++tgy/BBjFFFy3l3WFpO9KWgz7zpm7AeKJt8T11dleCfeXkkUAKIAf5qoIbap
sZWwpbkNFhHax2xIPEDgfg1azVY80ZcFuctL7TlLnMQ/0lUTbiSw1nH69MG6zO0b
9f6BQdgAmD06yK56mDcYBZUCAwEAAaOCATgwggE0MA4GA1UdDwEB/wQEAwIBhjAP
BgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTkrysmcRorSCeFL1JmLO/wiRNxPjAf
BgNVHSMEGDAWgBRge2YaRQ2XyolQL30EzTSo//z9SzBgBggrBgEFBQcBAQRUMFIw
JQYIKwYBBQUHMAGGGWh0dHA6Ly9vY3NwLnBraS5nb29nL2dzcjEwKQYIKwYBBQUH
MAKGHWh0dHA6Ly9wa2kuZ29vZy9nc3IxL2dzcjEuY3J0MDIGA1UdHwQrMCkwJ6Al
oCOGIWh0dHA6Ly9jcmwucGtpLmdvb2cvZ3NyMS9nc3IxLmNybDA7BgNVHSAENDAy
MAgGBmeBDAECATAIBgZngQwBAgIwDQYLKwYBBAHWeQIFAwIwDQYLKwYBBAHWeQIF
AwMwDQYJKoZIhvcNAQELBQADggEBADSkHrEoo9C0dhemMXoh6dFSPsjbdBZBiLg9
NR3t5P+T4Vxfq7vqfM/b5A3Ri1fyJm9bvhdGaJQ3b2t6yMAYN/olUazsaL+yyEn9
WprKASOshIArAoyZl+tJaox118fessmXn1hIVw41oeQa1v1vg4Fv74zPl6/AhSrw
9U5pCZEt4Wi4wStz6dTZ/CLANx8LZh1J7QJVj2fhMtfTJr9w4z30Z209fOU0iOMy
+qduBmpvvYuR7hZL6Dupszfnw0Skfths18dG9ZKb59UhvmaSGZRVbNQpsg3BZlvi
d0lIKO2d1xozclOzgjXPYovJJIultzkMu34qQb9Sz/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



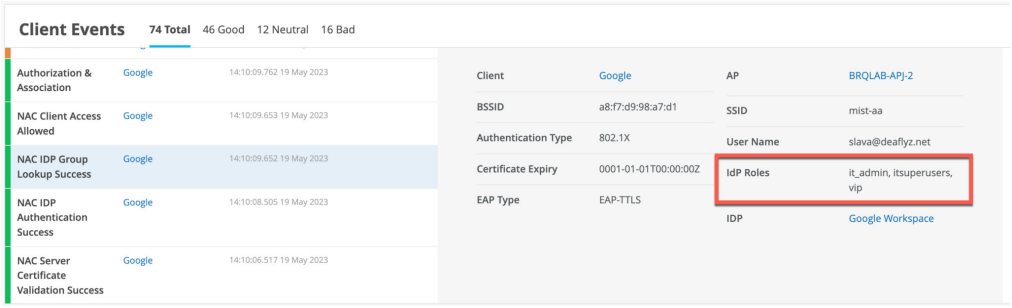
Click **Save**.

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.

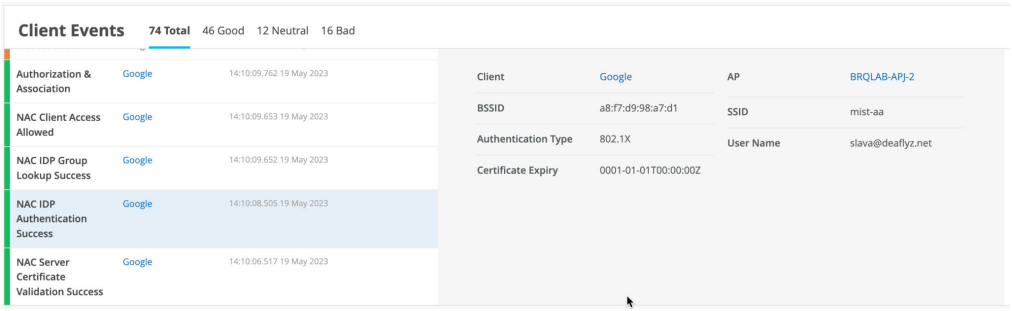
When a user authenticates using EAP-TTS with Google Workspace, you can see the event **NAC IDP Group Lookup Success** that fetches user group membership information.

Figure 8: IDP Group Lookup Success Authentication Event



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



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 135.

SEE ALSO

Add Identity Providers for Juniper Mist Access Assurance | 23

Integrate Microsoft Entra ID as an Identity Provider | 46

Integrate Okta as an Identity Provider | 40

Integrate Okta as an Identity Provider

SUMMARY

Follow these steps to complete pre-requisites, configure your credential apps in Okta, and add your Identity Provider to your Juniper Mist organization.

IN THIS SECTION

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 tenant ID at the top- right corner of the Okta dashboard. 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 tenant ID.

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

OKTA Resource Owner Password Credential App Integration

NOTE: The screenshots from third-party applications are correct at the time of publishing. We have no way to know when or if the screenshots will be accurate at any future time. Please refer to the third-party website for guidance about changes to these screens or the workflows involved.

1. Log in to the Okta administration console and select **Applications > Applications.**
2. Click **Create New App Integration**.

   Under Sign-in method, select **OICD-OpenID Connect** and under Application type, select **Native Application**. The result looks like: <image-needed>

   Click **Next**.
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: .

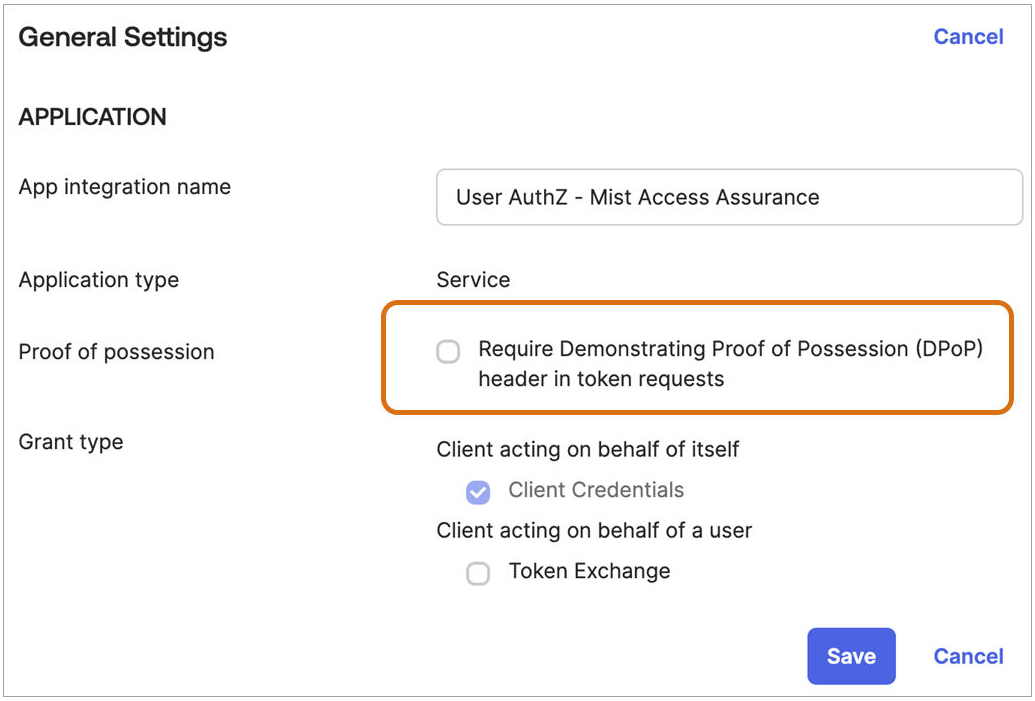
- Client Authentication—Select **Client Secret**

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.self

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

Okta Client Credential App Integration

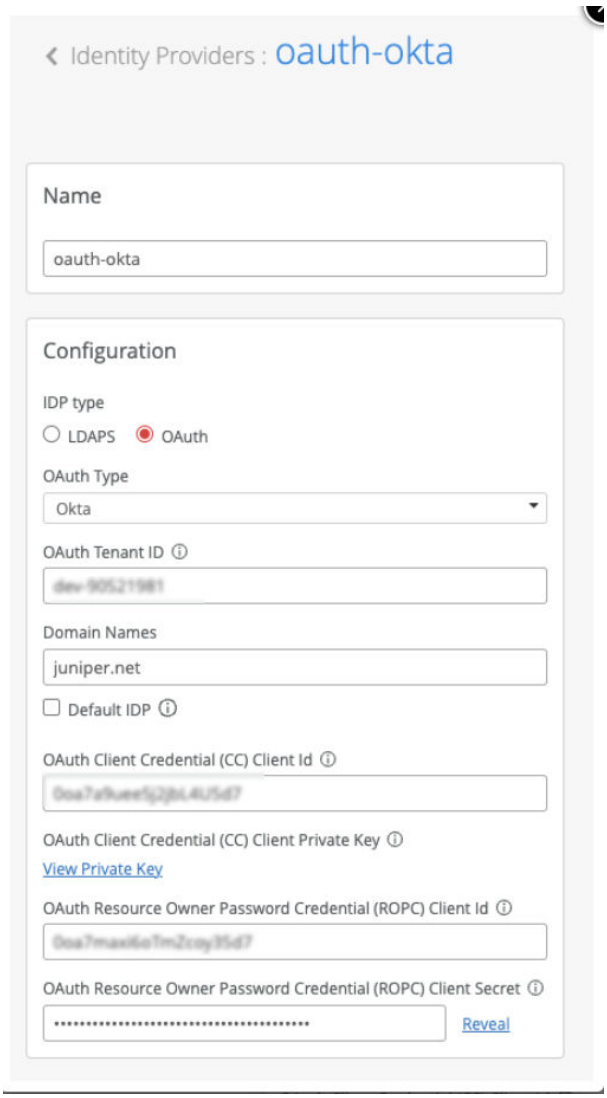
1. Log in to the Okta administration console and select **Applications > Applications.**
2. Click **Create App Integration**.
   The Create a new app integration page opens.
3. Under Sign-in method, select **API Services**.
   The New API Services App Integration page opens.
4. Enter a name for **App 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. Scroll down until you see **General Settings** section. Cick **Edit** and uncheck the **Require Demonstrating Proof of Possession (DPoP) header in token requests**option.



10. Go to the **Okta API Scopes** tab and allow the following read permissions:
    - okta.roles.read
    - okta.users.read
    - okta.groups.read

Configuration on Juniper Mist Dashboard

1. From the left menu of the Juniper Mist portal, select **Organization** > **Access** > **Identity Providers**. The Identity Providers page displays any configured identity providers.
2. Click **Add IDP** to add a new identity provider.
3. On the **New Identity Provider** page, enter the following information:



a. Name—Enter an IdP name.

b. IDP Type—Select an IdP type as **OAuth**.

Table 7: Settings for Identity Provider Type OAuth

Parameters	Description
OAuth Type	Select **Okta**
OAuth Tenant ID	Enter OAuth tenant ID. Use the ID you received during Okta application configuration.

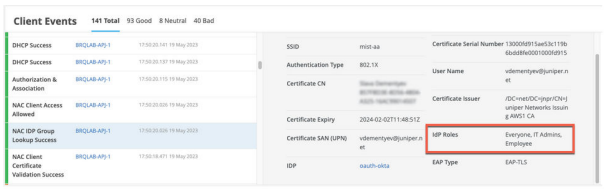
Table 7: Settings for Identity Provider Type OAuth *(Continued)*

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. "Okta Client Credential App Integration" on page 42
OAuth Client Credential (CC) Client Private Key	Enter the private key generated during Okta application configuration. See "Okta Client Credential App Integration" on page 42
OAuth Resource Owner Password Credential (ROPC) Client Id	Enter the secret ID you received and stored during Okta application configuration. See " OKTA Resource Owner Password Credential App Integration" on page 41.
OAuth Resource Owner Password Credential (ROPC) Client Secret	Provide client secret value you received and stored during Okta application configuration. See " OKTA Resource Owner Password Credential App Integration" on page 41

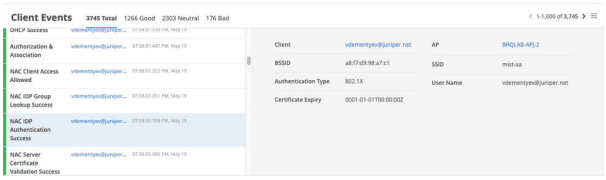
4. Click **Create** to save the changes.

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.



SEE ALSO

- Add Identity Providers for Juniper Mist Access Assurance | 23
- Integrate Microsoft Entra ID as an Identity Provider | 46
- Integrate Google Workspace as an Identity Provider | 29

Integrate Microsoft Entra ID as an Identity Provider

SUMMARY

Follow these steps to understand Entra ID options, add Mist as a new registration in Entra ID, and add your Identity Provider to your Juniper Mist organization.

IN THIS SECTION

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:

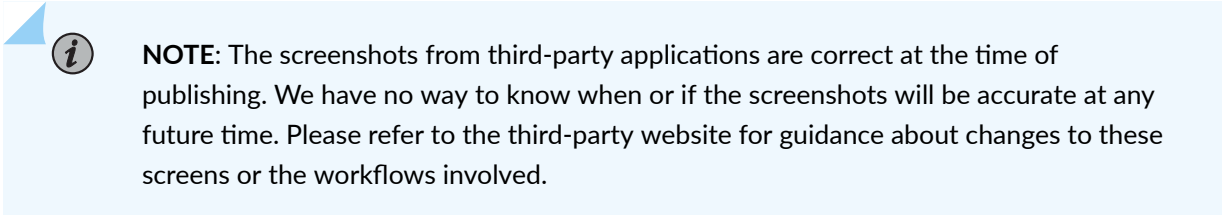
- **User authentication with Extensible Authentication Protocol–Tunneled TLS (EAP-TTLS)**
  - Performs delegated authentication, that is, checks username and password by using OAuth.
  - Retrieves user group membership information to support authentication policies that are based on this user identity.

  - 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.



NOTE: The screenshots from third-party applications are correct at the time of publishing. We have no way to know when or if the screenshots will be accurate at any future time. Please refer to the third-party website for guidance about changes to these screens or the workflows involved.

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.

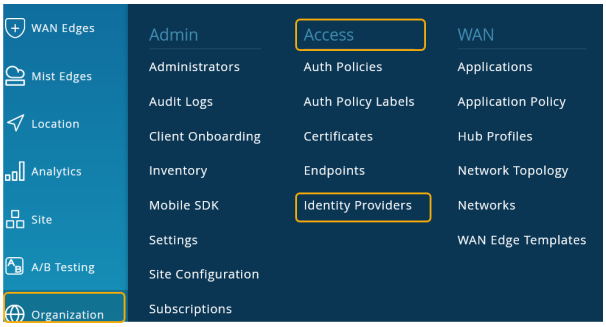
   You will need this information for the **OAuth Client Credentials Client Secret** field on the Juniper Mist portal when you add Azure AD as an IdP.
10. Select **Authentication** in the left-navigation bar and scroll-down to the **Advanced Settings** section. Select **Yes** for **Allow public client flows**.
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.

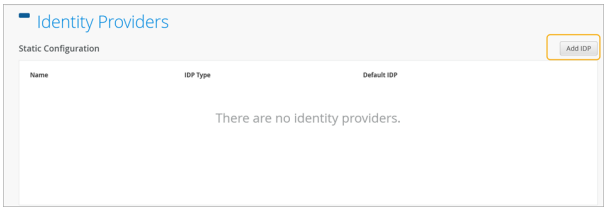
Configuration on Juniper Mist Dashboard

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



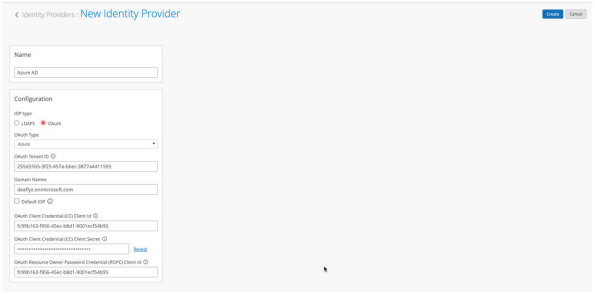
The Identity Providers page displays any configured identity providers.

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



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.

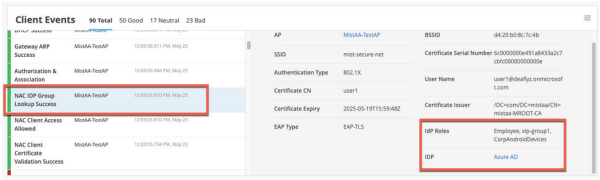
h. **OAuth Client Credential (CC) Client secret**—Enter the application secret that you created earlier on the Azure portal.

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**.

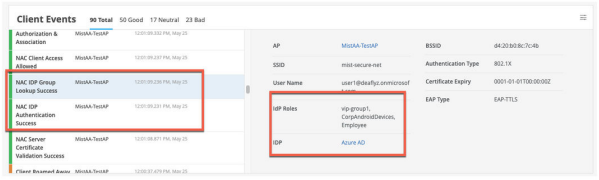
When Juniper Mist Access Assurance authenticates a user by using EAP-TLS with Azure AD, you can see the **NAC IDP Group Lookup Success** event as shown below:

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



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



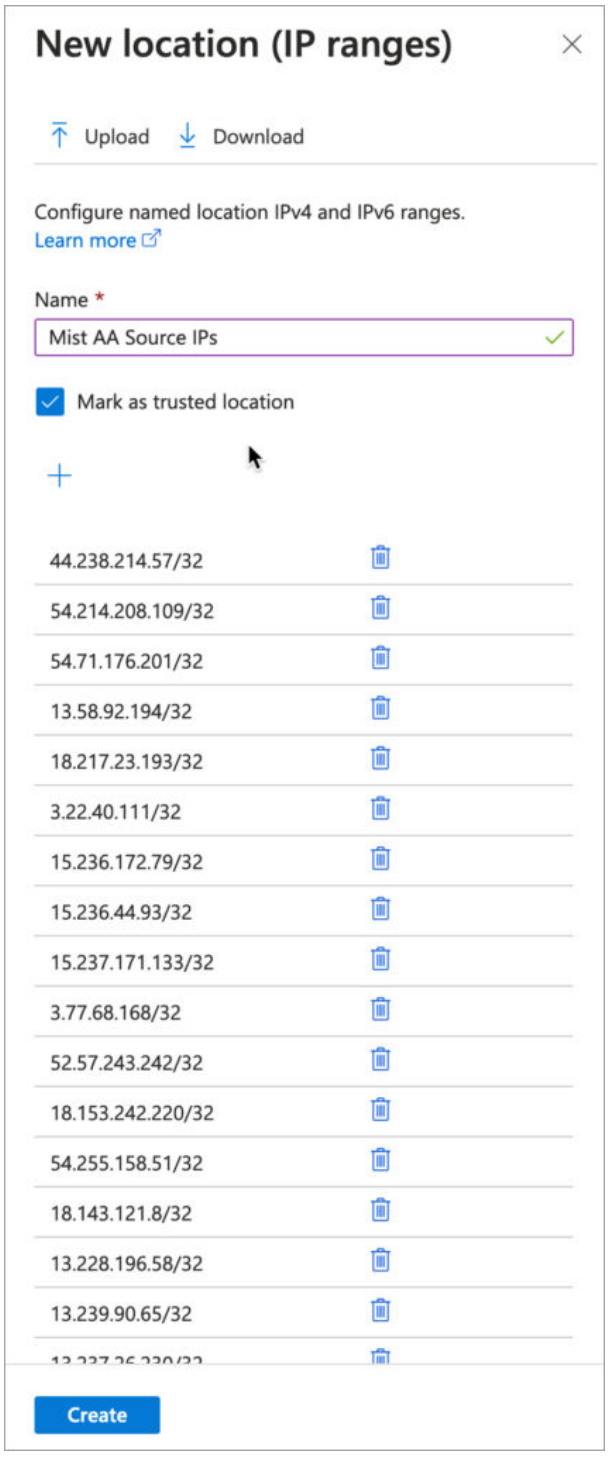
EAP-TTLS Authentication with Azure AD and ROPC

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.

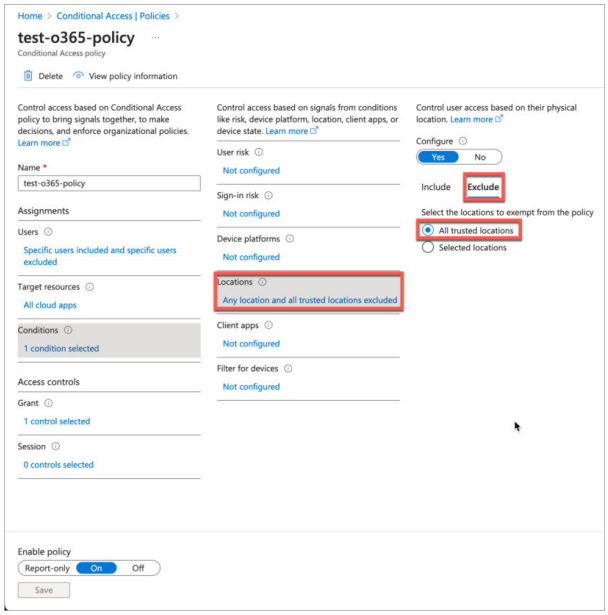
Figure 14: Bypass MFA for Sign in from a Trusted IP Address Range



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



SEE ALSO

Add Identity Providers for Juniper Mist Access Assurance | 23

Integrate Google Workspace as an Identity Provider | 29

Integrate Okta as an Identity Provider | 40

SCIM Integration with Microsoft Entra ID and Okta

SUMMARY

The Mist Access Assurance cloud uses OAuth 2.0 to integrate with Microsoft Entra ID (Azure AD) and Okta for secure user authentication and authorization. System for Cross-domain Identity Management (SCIM) integration enhances the authorization performance by enabling the Access Assurance cloud to maintain a locally synchronized repository of users and groups, reducing latency and dependency on external IdPs. Follow these steps to integrate SCIM with Entra ID or Okta.

IN THIS SECTION

The Mist Access Assurance cloud integrates with external Identity Providers (IdPs) such as Microsoft Entra ID (Azure AD) and Okta using OAuth 2.0. With this integration, Mist Access Assurance manages the:

- Authentication for EAP-TTLS and Admin-Auth
- Authorization (retrieving user group information) for EAP-TLS, EAP-TTLS, and Admin-Auth through OAuth 2.0 connections to the IdPs

As the authentication and authorization operations involve real-time communication with external IdPs, each control-path call can introduce additional latency, affecting the overall response time for authentication and policy evaluation. It also adds a potential bottleneck and failure domain in cases where the IdP service is degraded.

To optimize the authorization process, Juniper Mist Access Assurance supports System for Cross-domain Identity Management (SCIM)-based integration with IdPs. A key benefit of SCIM-based integration is reduced latency during the authorization process.

The Mist Access Assurance cloud utilizes SCIM to maintain a locally synchronized repository of user and group information for each customer organization. This repository enables the policy service to assess user group memberships and enforce authorization rules without requiring real-time lookups to the external IdP.

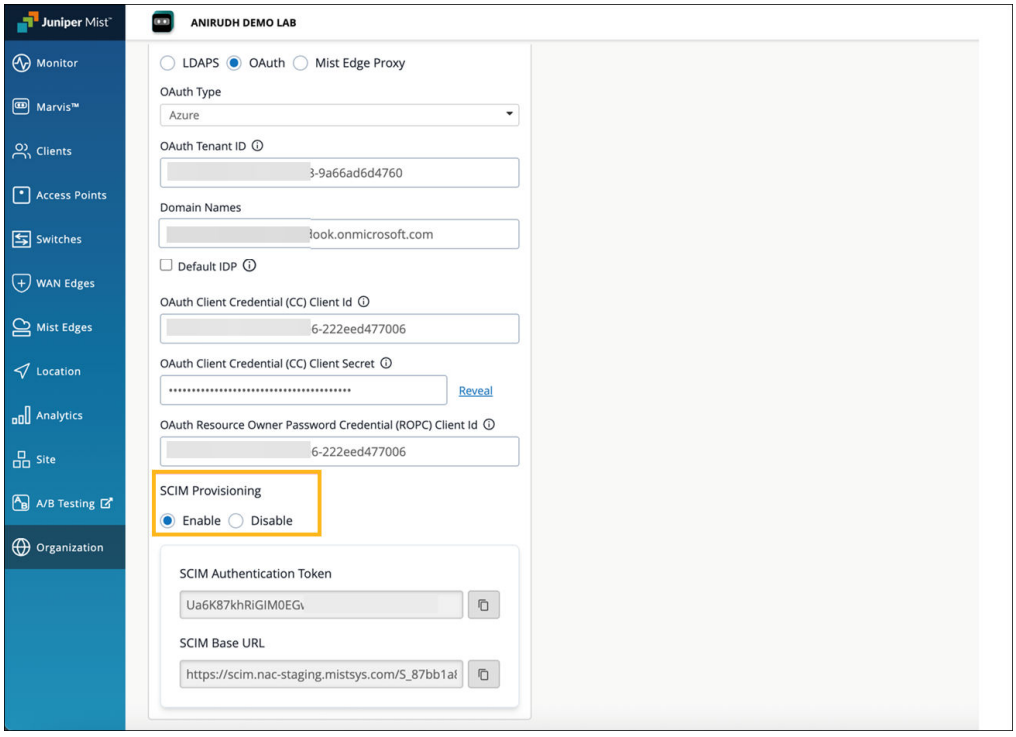
NOTE: If the Mist Access Assurance cloud encounters any error while retrieving group mapping from the SCIM data, it automatically reverts to the existing OAuth-based authorization by connecting to the external IdP.

Disabling SCIM will remove all synchronized user and group data and prevent any further synchronization from the IdP.

Prerequisites

Before you integrate SCIM, ensure to complete the following tasks:

1. Integrate Mist Access Assurance with the Microsoft Entra ID or Okta IdP. See Microsoft Entra ID Integration and Okta Integration for detailed instructions.
2. Ensure that at least one client is onboarded with Mist Access Assurance before proceeding with the SCIM configuration.
3. Enable SCIM provisioning in the IdP configuration. The SCIM Authentication Token and SCIM Base URL are automatically generated when you enable SCIM provisioning. These parameters are required for synchronizing user and group information from the IdP to Mist Access Assurance.

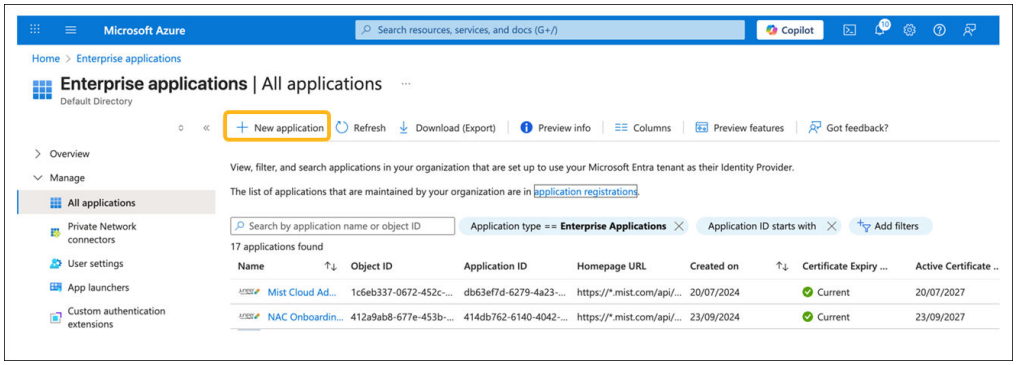


How to Integrate SCIM with Microsoft Entra ID

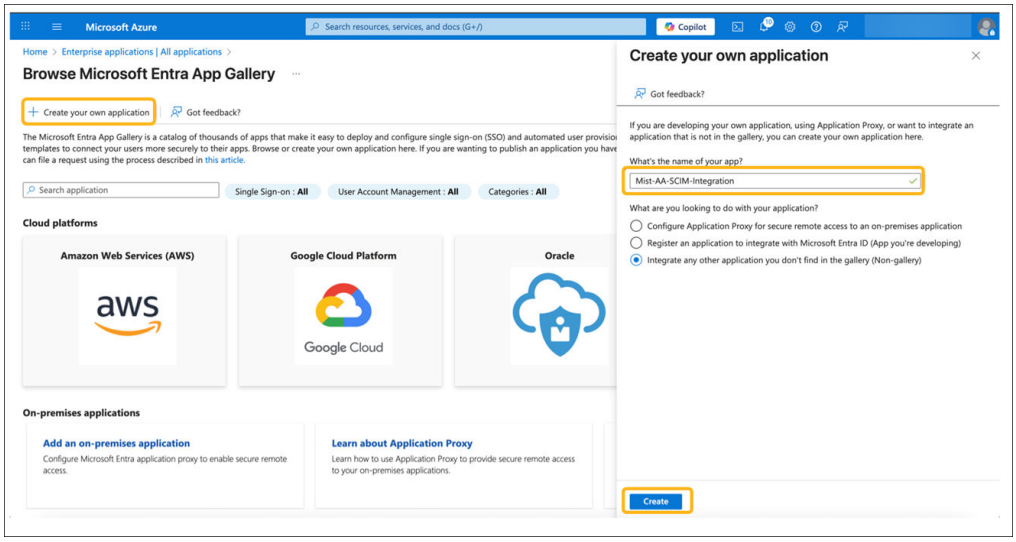
To Integrate SCIM with Microsoft Entra ID:

> **NOTE**: The screenshots from third-party applications are correct at the time of publishing. We have no way to know when or if the screenshots will be accurate at any future time. Please refer to the third-party website for guidance about changes to these screens or the workflows involved.

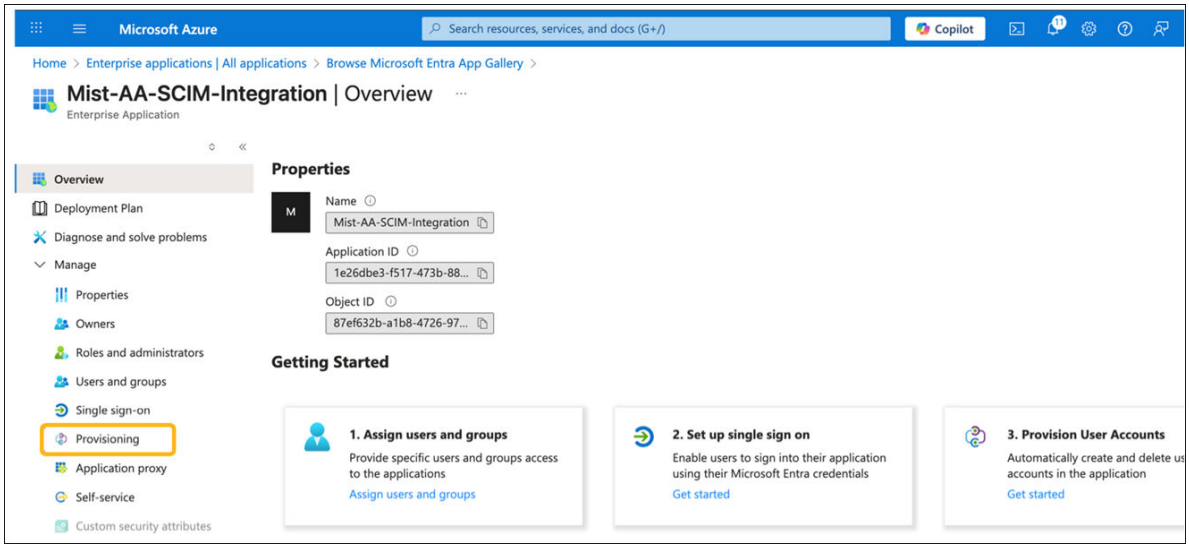
1. Sign in to Microsoft Entra Admin Center, navigate to **Enterprise applications**, and then click **New application**.

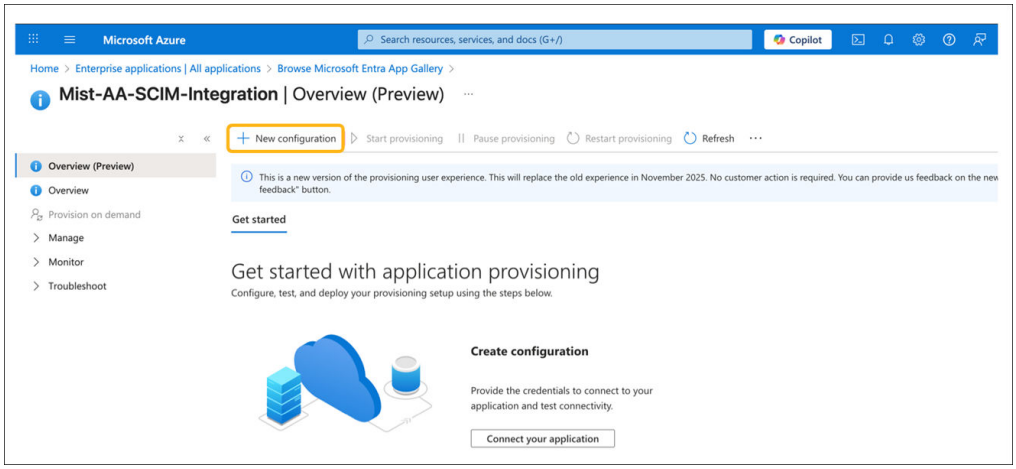


2. Click **Create your own application**. Enter a name for the application and click **Create**.



3. After the application is created, navigate to **Provisioning** under the Manage section and click **New Configuration**.

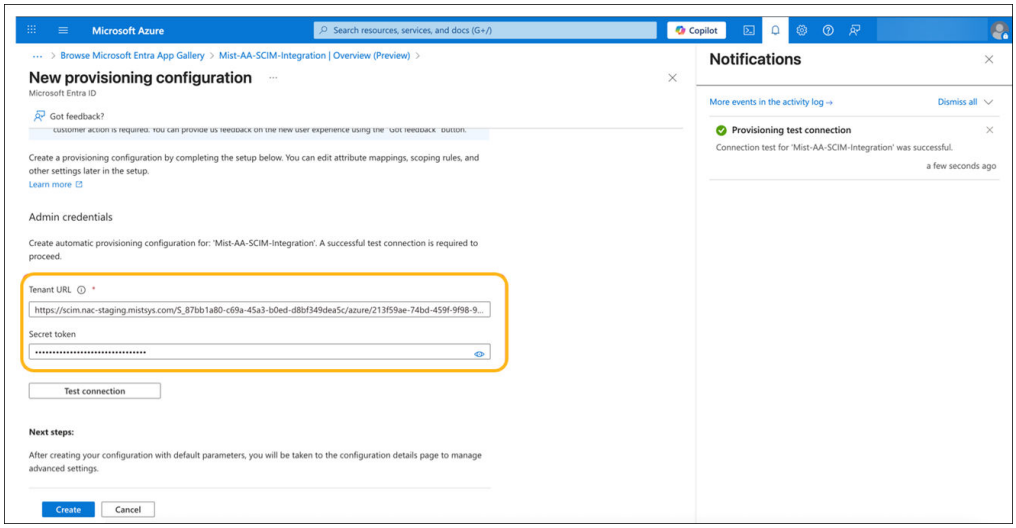




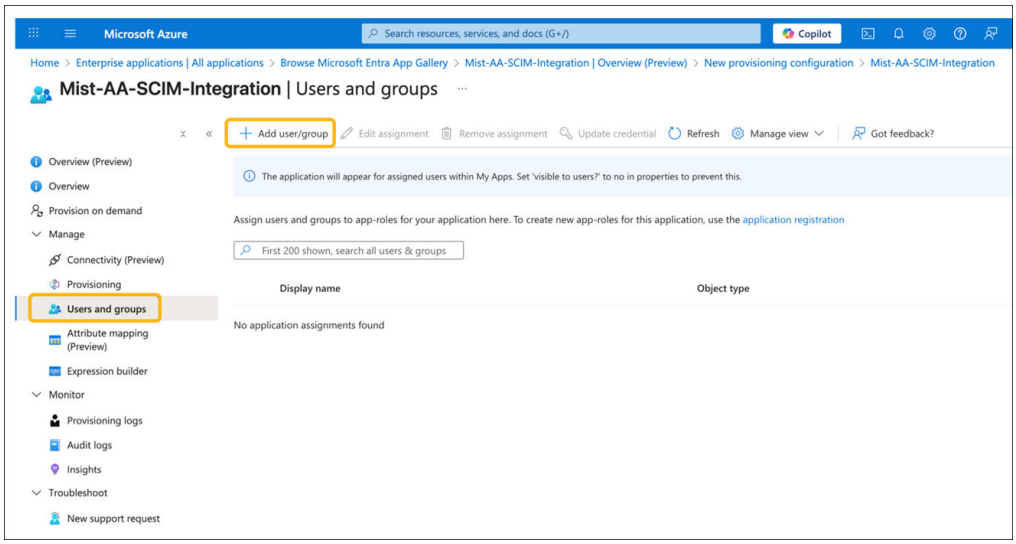
4. Enter the following details from the Mist Access Assurance IdP configuration:

   - **Tenant URL**—SCIM Base URL
   - **Secret Token**—SCIM Authentication Token

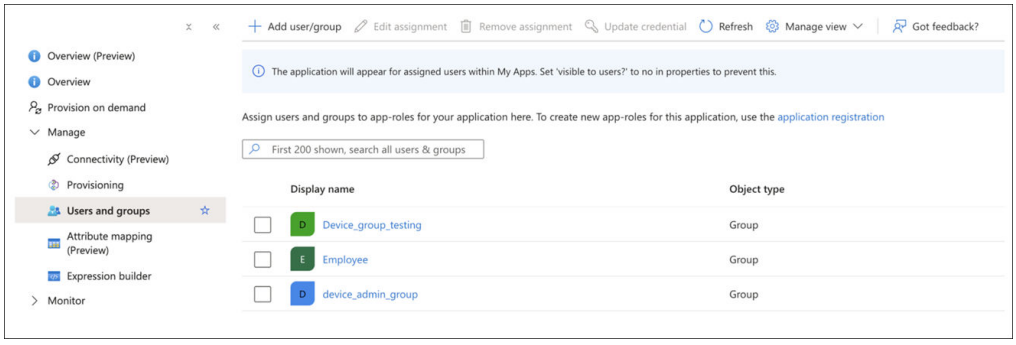
   Click **Test Connection** and verify that the test is successful. Then, click **Create**.



5. Select **Users and groups** under Manage, and click **Add user/group** to assign groups for provisioning.

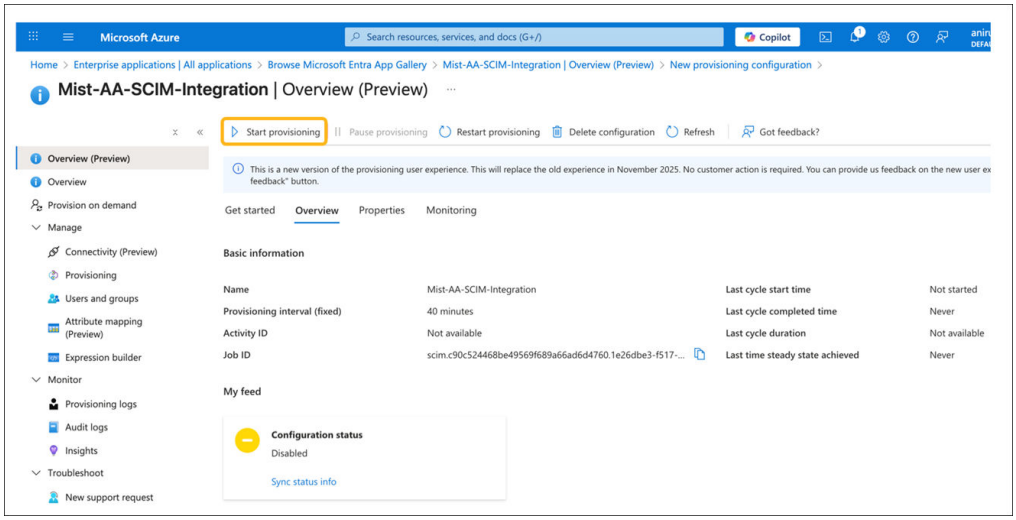


6. Add the groups that need to be provisioned on the Mist Access Assurance cloud.

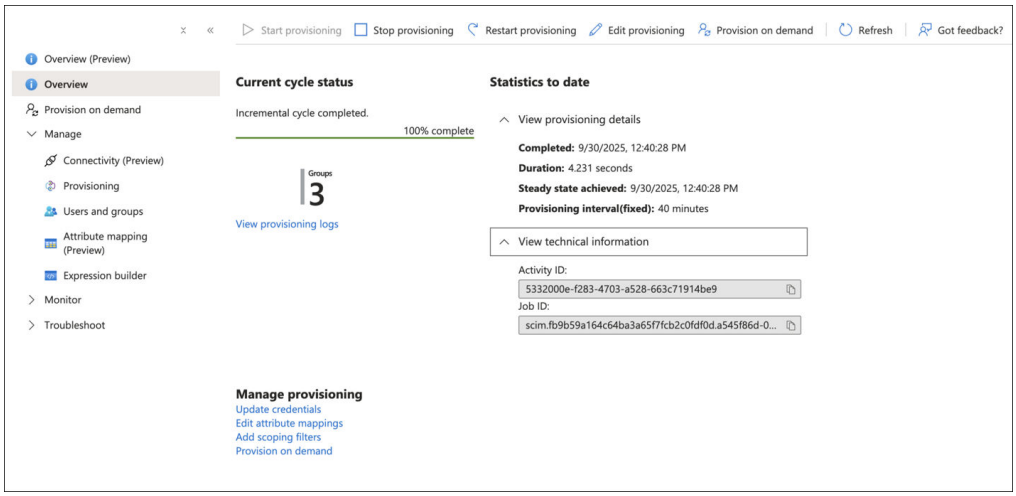


7. Click **Start Provisioning**.

NOTE: The provisioning interval in Microsoft Entra ID is approximately 40 minutes. You must wait for the next sync cycle to verify the provisioning status.



8. Verify that the provisioning status shows as Completed in Entra ID after the 40-minute provisioning interval. The setup for SCIM provisioning with Entra ID is now complete.

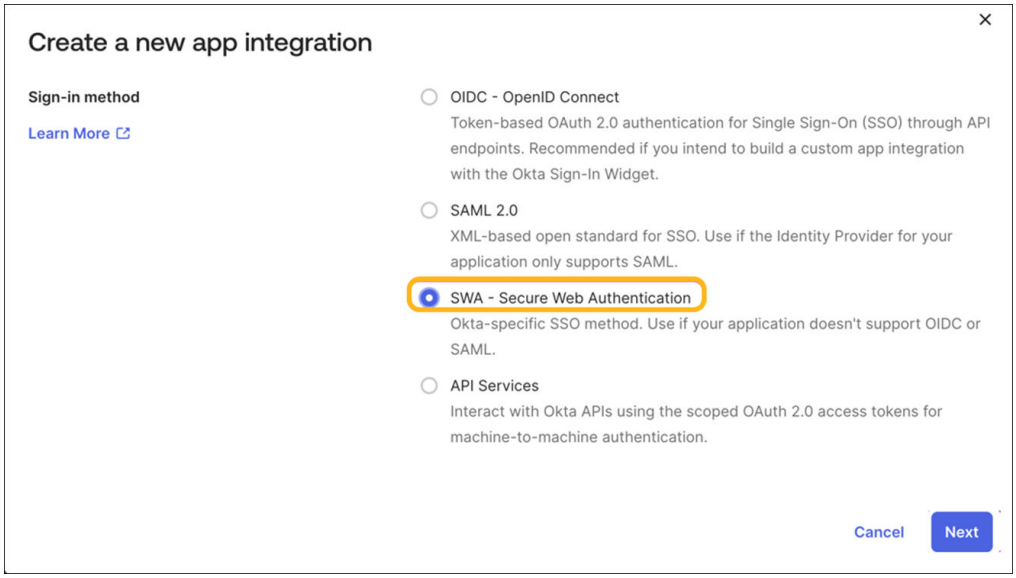


How to Integrate SCIM with Okta

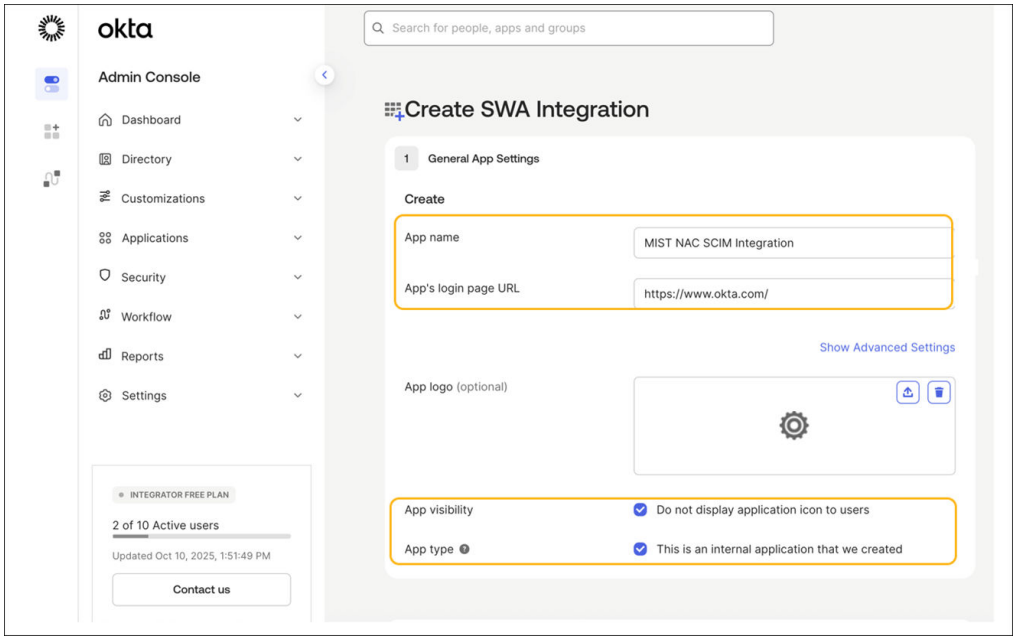
To integrate SCIM with Okta:

NOTE: Some of the screenshots included in this topic are sourced from third-party applications. Be aware that these screenshots might change over time and might not always match the current version of the applications.

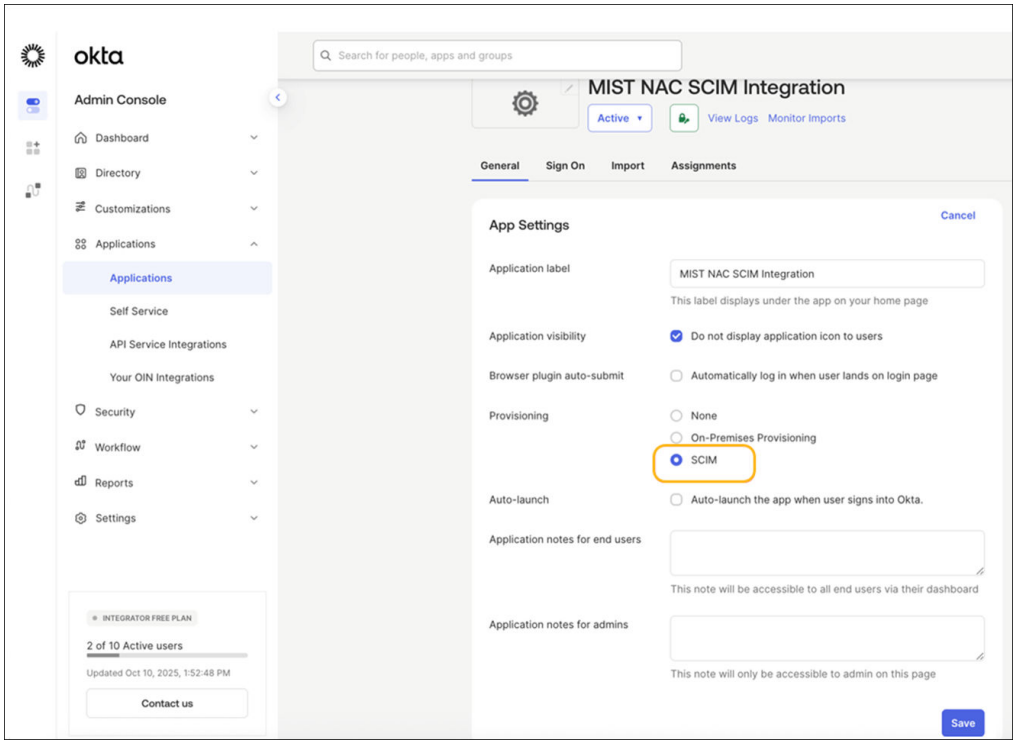
1. Log in to the Okta Admin Console and navigate to **Applications**>**Create App Integration**.
2. Select the Sign-in method as **SWA - Secure Web Authentication** and click **Next**.



3. Enter a name for the application and specify the login page URL for the app. Select the options for App Visibility and App Type, then click **Finish**.



4. Switch to the General tab and click **Edit Settings**. Set the Provisioning Type as **SCIM** and click **Save**.

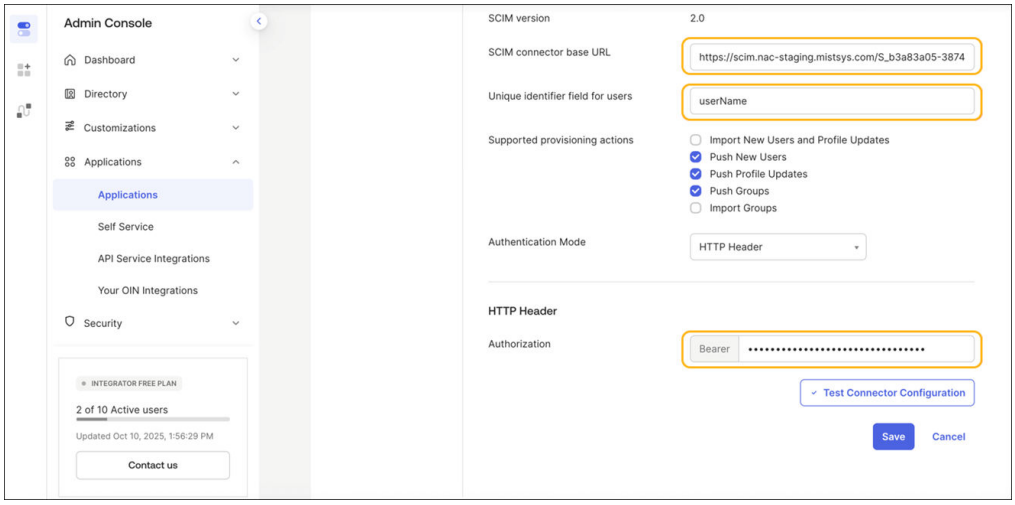


5. In the Provisioning tab:

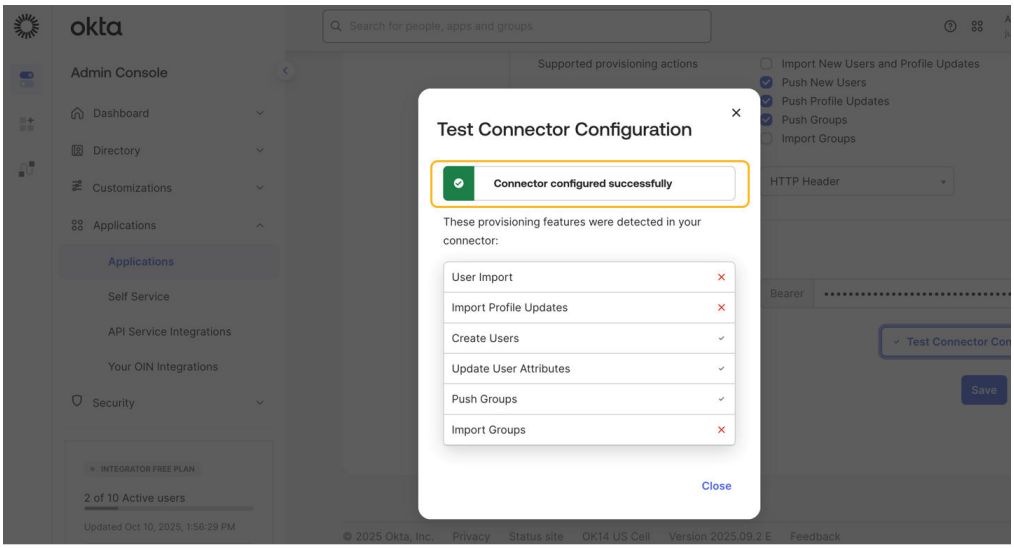
   a. Enter the following details:

   - **SCIM Connector Base URL**—SCIM Base URL from the IdP configuration
   - **Unique Identifier Field for Users**—userName
   - **Authentication Mode**—HTTP header
   - **Authorization**—SCIM Authentication token from the IdP configuration

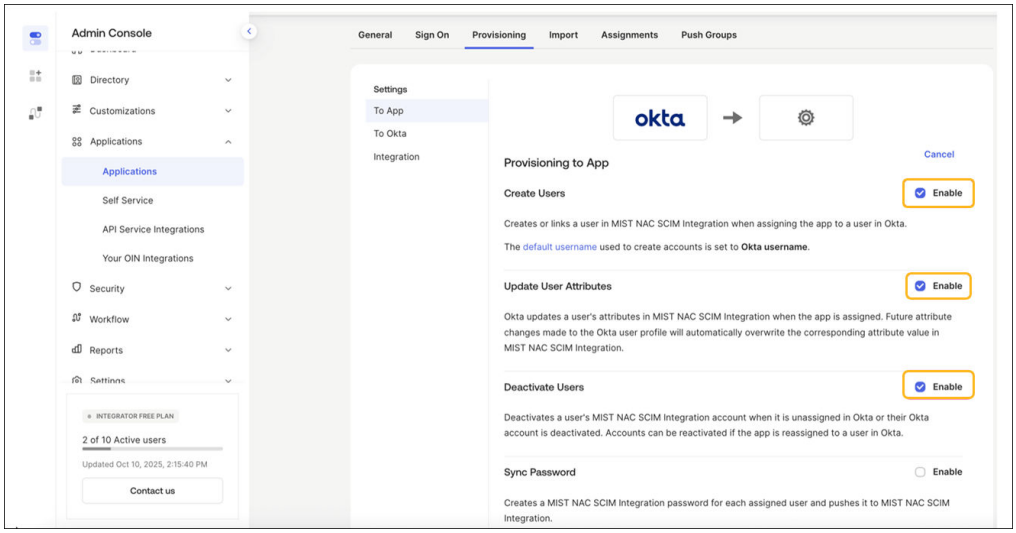
   b. Enable the **Push New Users**, **Push Profile Updates**, and **Push Groups** checkboxes.



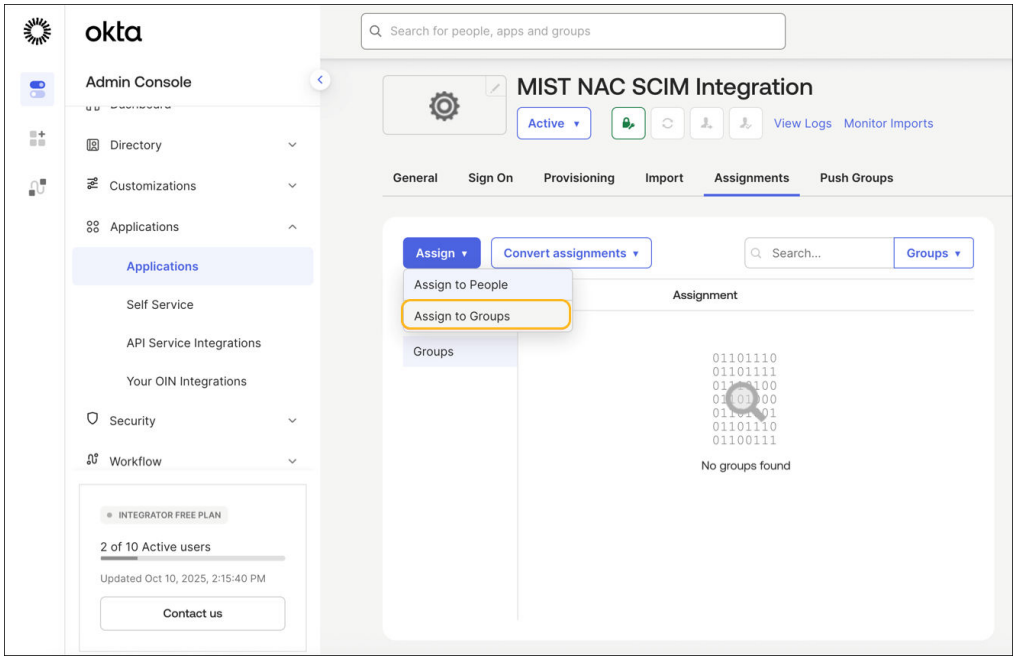
c. Click **Test Connector Configuration**. If you see a success message, click **Save**.

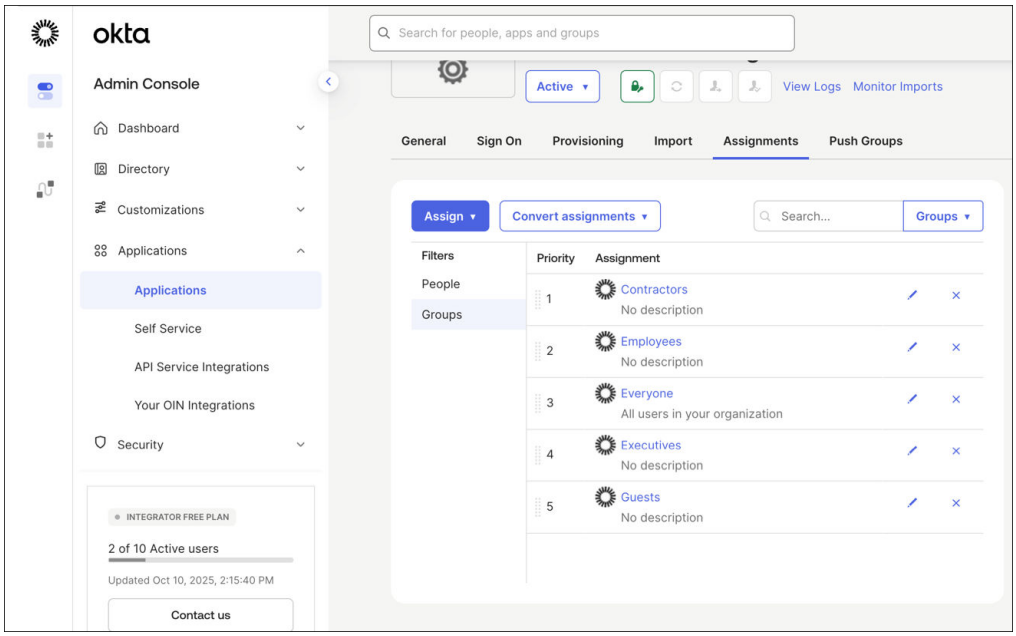


6. In the Provisioning Settings tab, enable the first three provisioning options and click **Save**.
   - Create Users
   - Update User Attributes
   - Deactivate Users

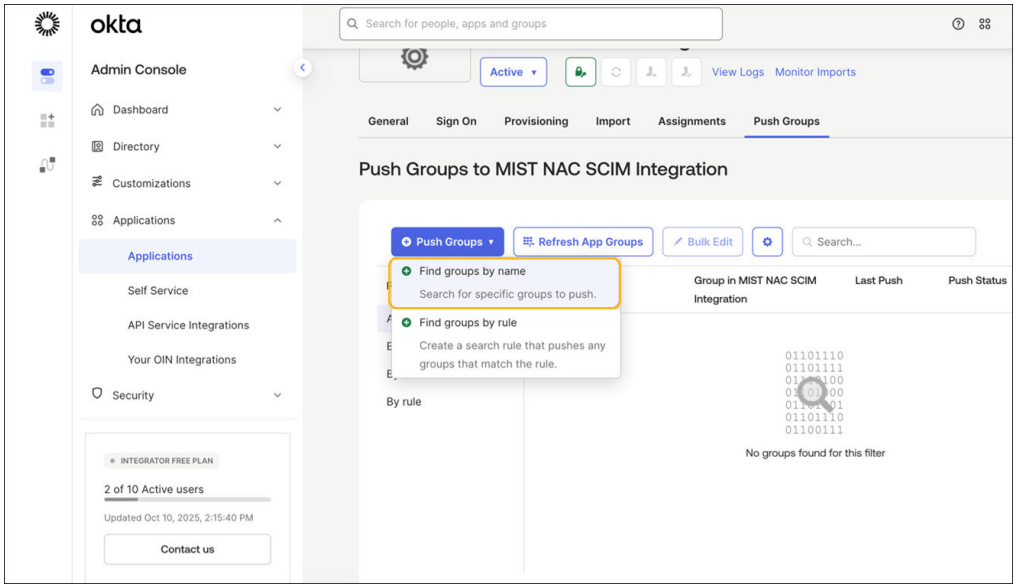


7. Select the Assignments tab and select **Assign**>**Assign to Groups**. Select and assign the groups that need to be provisioned on Mist Access Assurance.

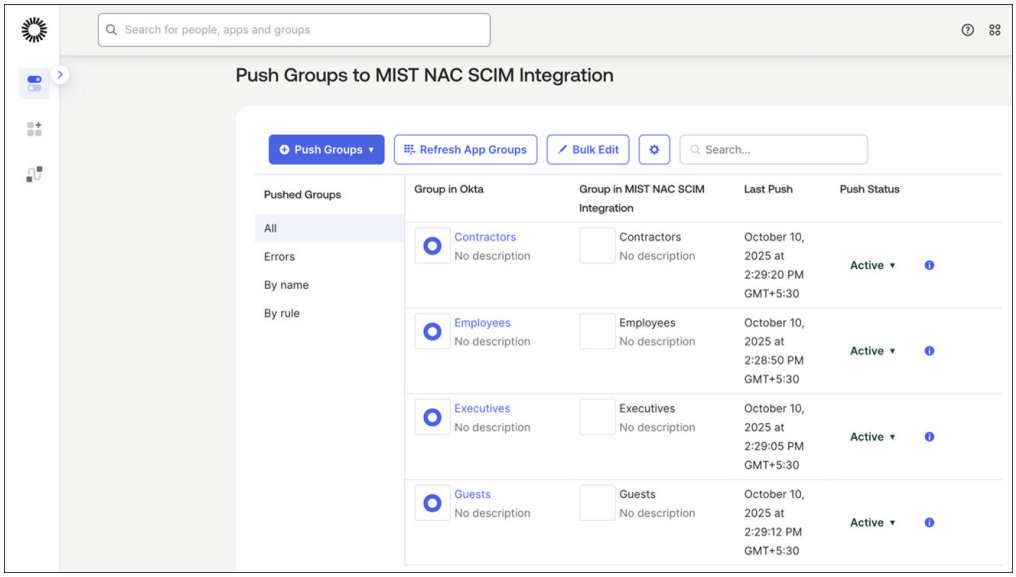




8. Navigate to the Push Groups tab and click **Push Groups** > **Find groups by name**. Push all the required groups for provisioning.



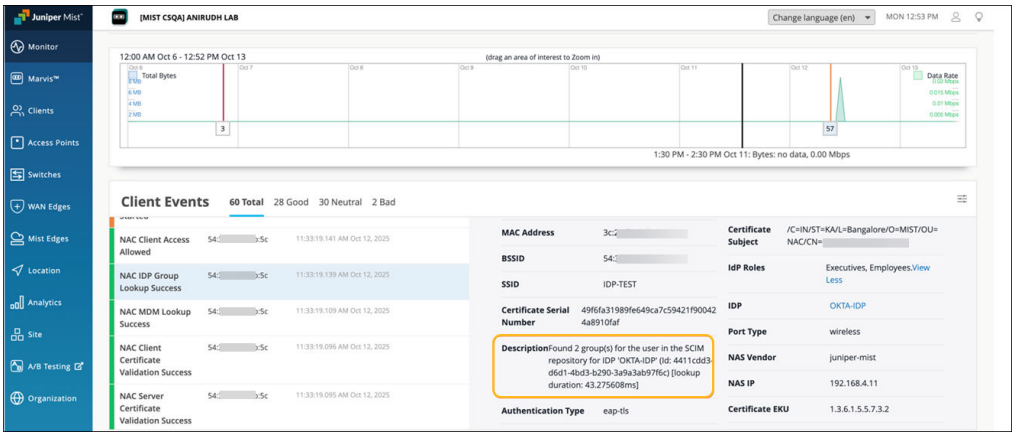
Verify that the **Push Status** shows as Active. The setup for SCIM provisioning with Okta IdP is now complete.



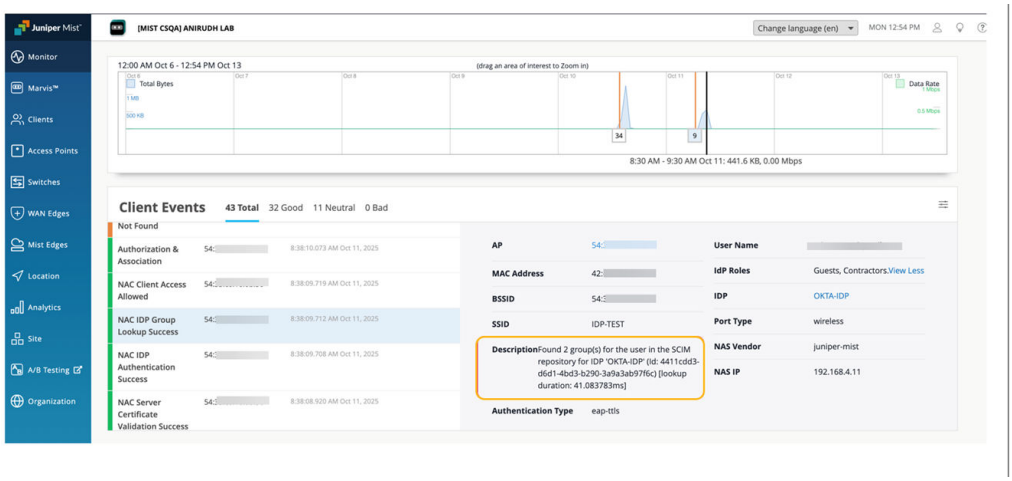
Client Connection and Verification

When a client is connected, you'll see the client events on the Insights page on the Mist portal. In the following examples, clients were connected using both EAP-TLS and EAP-TTLS authentication methods. In both cases, the authorization (that is, user group retrieval and mapping) was performed through the Mist Access Assurance SCIM database. This behavior can be verified in the event description, where the source of group information is shown as the SCIM repository.

Example 1: Client connected using the EAP-TLS authentication



Example 2: Client connected using the EAP-TTLS authentication



JAMF Pro Integration

SUMMARY

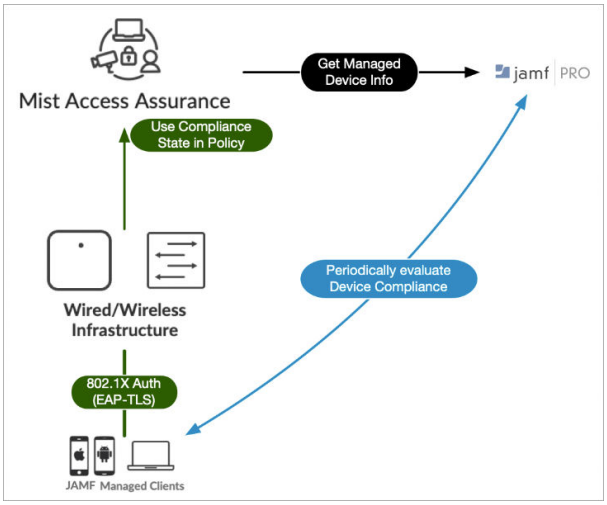
Follow these steps to create your client ID and secret on JAMF Pro, link your JAMF Pro account to your Juniper Mist™ organization, and verify the integration.

IN THIS SECTION

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 16: 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.

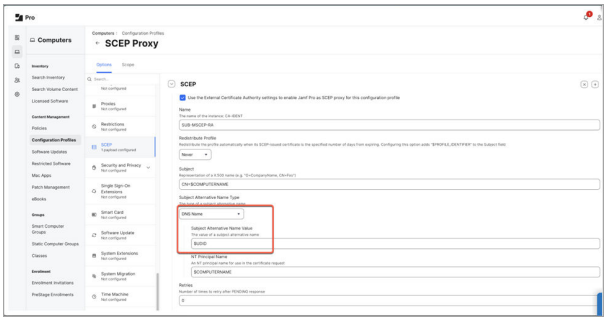
Mist Access Assurance uses the following information during client authentication to match a client with a device record in JAMF:

- **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 17 on page 67 shows location of UDID in configuration profile.

Figure 17: Locating Unique Device ID



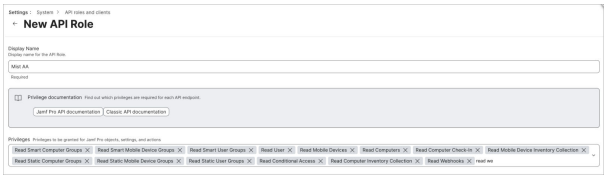
Create Client ID and Secret on the JAMF Pro

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

NOTE: The screenshots from third-party applications are correct at the time of publishing. We have no way to know when or if the screenshots will be accurate at any future time. Please refer to the third-party website for guidance about changes to these screens or the workflows involved.

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 18: 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

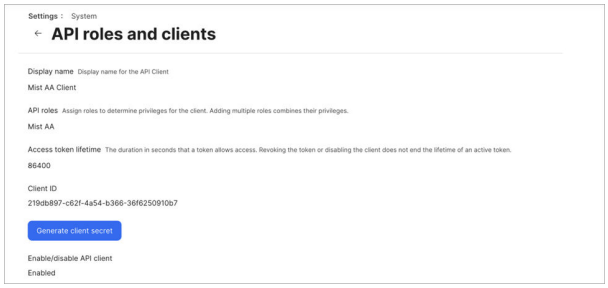
3. Navigate to API Clients tab, and add a new client.

Figure 19: Configure New API Client

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.

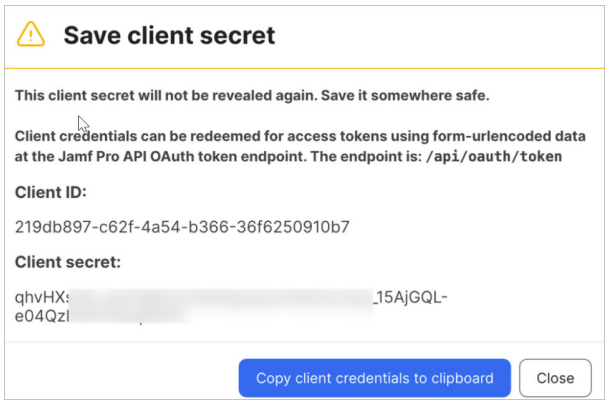
Figure 20: Generate Client Secret



The client secret is generated.

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

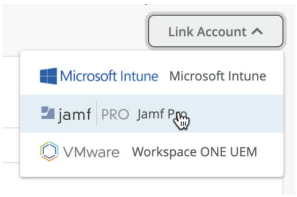
Figure 21: Client Secret Details



Link JAMF Pro Account to Mist Access Assurance

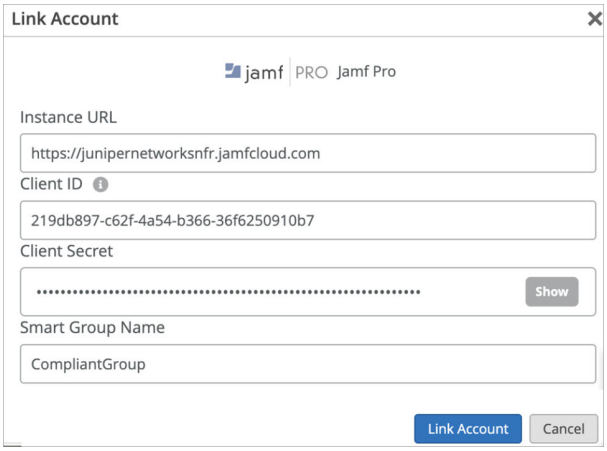
1. Juniper Mist dashboard, navigate to **Organization > Access > Identity Providers**.
2. In the Identity Providers page, scroll down to Linked Account section and click **Link Account** to select **JAMF Pro**.

Figure 22: Linking to JAMF Pro Account



3. In the Link Account pop-up window, enter the details. Figure 23 on page 70 shows a sample of link account details.

Figure 23: Details for Linking JAMF Pro



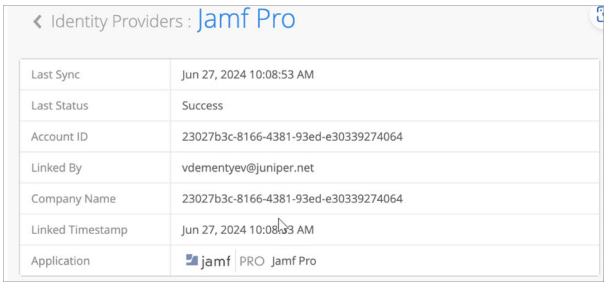
- **Instance URL**—JAMF Pro instance URL. Example: https://<yourjamfurl>.com.
  Remove any trailing / in the Instance URL field.
- **Client ID**—Client ID generated while creating Client ID and Secret on the JAMF Pro dashboard.
- **Client Secret**—Client secret generated while creating Client ID and 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.

> **NOTE**: During JAMF account linking, Access Assurance validates the Smart Group name only against Computer Smart Groups in JAMF Pro. Although JAMF supports Smart Groups for both computers and mobile devices, the Smart Group must exist under Computers to complete the linking. If only mobile devices are managed, create a Computer Smart Group with the same name (a dummy group is sufficient).

After linking is complete, you can see last sync status and time as shown in Figure 24 on page 71.

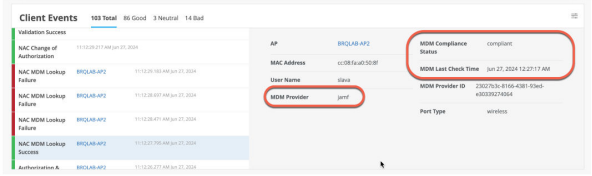
Figure 24: JAMP Pro Sync Status



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 25 on page 71.

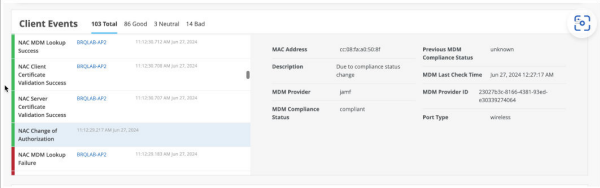
Figure 25: MDM Lookup Details



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 26 on page 72 shows a sample of compliance status change.

Figure 26: MDM Lookup Details- MDM Status Change



SEE ALSO

Add Identity Providers for Juniper Mist Access Assurance | 23

Onboard CA and SCEP Integration for JAMF-Managed Devices

SUMMARY

Onboard CA Configuration in Juniper Mist Access Assurance provides a cloud-native SCEP service that integrates directly with JAMF for automated client certificate distribution. This eliminates the need for an external PKI and simplifies secure Wi-Fi onboarding with EAP-TLS authentication.

IN THIS SECTION

Juniper Mist Access Assurance provides Onboard Certificate Authority (CA) configuration, which delivers a fully managed Simple Certificate Enrollment Protocol (SCEP) infrastructure. When the Onboard CA is enabled, Access Assurance automatically provisions all the elements required for seamless JAMF integration—the Jamf SCEP URL, Jamf Access Token, and Jamf Webhook URL. With only these values, you can integrate JAMF with Juniper Mist Access Assurance without deploying or maintaining any external PKI or on-premises SCEP service. The Onboard CA certificate provided by

Access Assurance is then used to configure a SCEP profile within JAMF, enabling secure client certificate issuance to enrolled devices.

By leveraging the Access Assurance SCEP infrastructure, you can automate the distribution of client certificates to JAMF-managed endpoints, binding them to Wi-Fi profiles for EAP-TLS authentication. This feature ensures that every device connecting to the network is authenticated through strong, certificate-based trust while fully managed from the Juniper Mist Access Assurance cloud.

NOTE: When a device is marked as inactive or deleted in JAMF, you must revoke the client certificate manually through the Juniper Mist portal.

To enable JAMF to leverage Juniper Mist Access Assurance as its SCEP infrastructure for client certificate distribution, follow these steps:

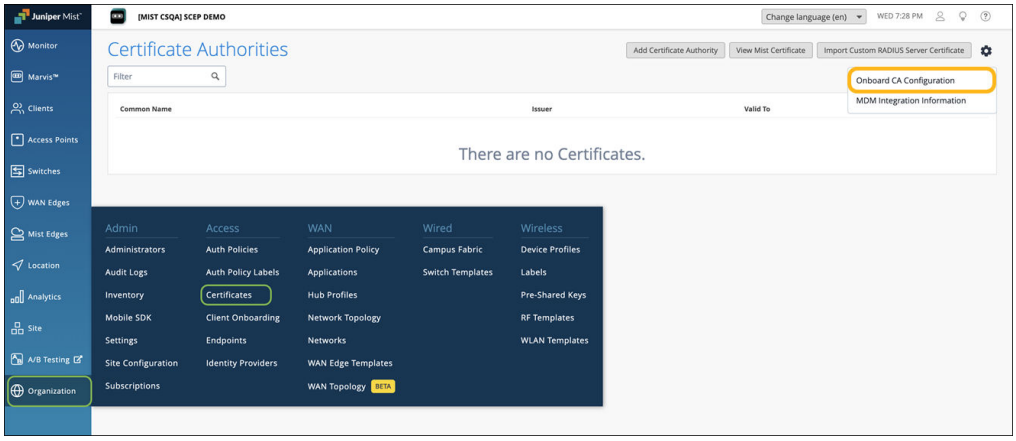
Enable Onboard CA Configuration

To enable the Onboard CA configuration:

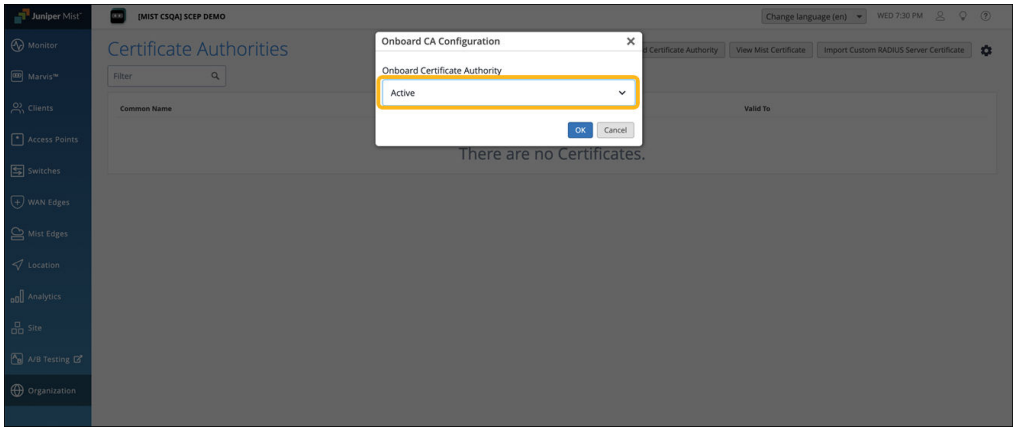
1. From the left menu of the Juniper Mist portal, select **Organization** > **Access** > **Certificates**.

   The Certificate Authorities page appears.

2. Click the settings icon on the upper-right corner of the page and select **Onboard CA Configuration**.



3. Select **Active** and click **OK**.

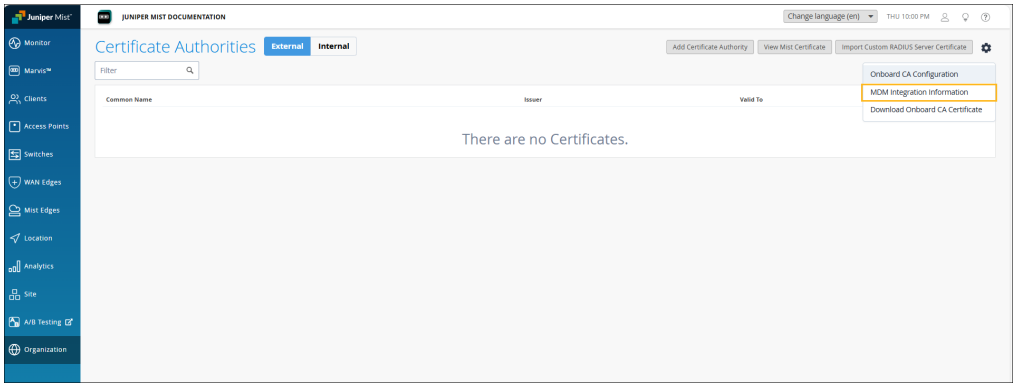


The onboard Certificate Authority service is enabled, and the respective SCEP endpoints are generated for each MDM.

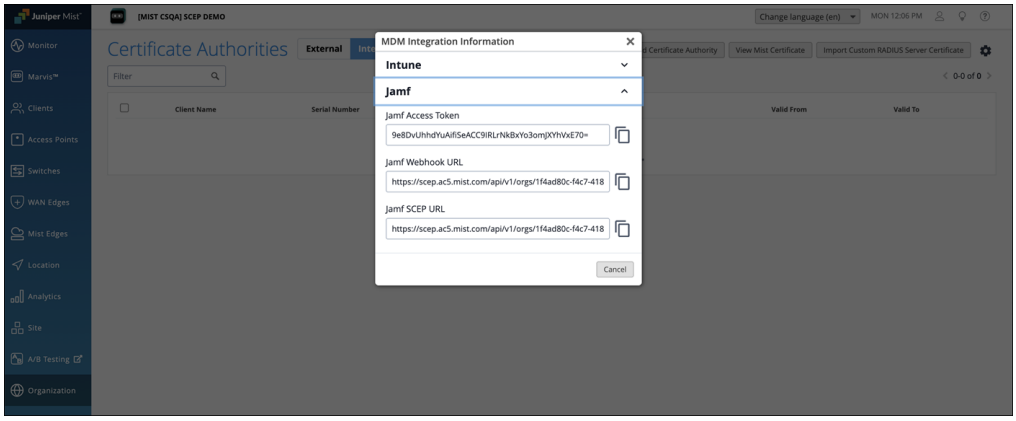
When the Onboard CA configuration is activated, you'll see the following tabs displayed:

- External—Displays the details of the external CAs.
- Internal— Displays the details of client certificates issued by the built-in CA through the NAC portal or MDM.

4. Click the settings icon on the upper-right corner of the page again and select **MDM Integration Information**.



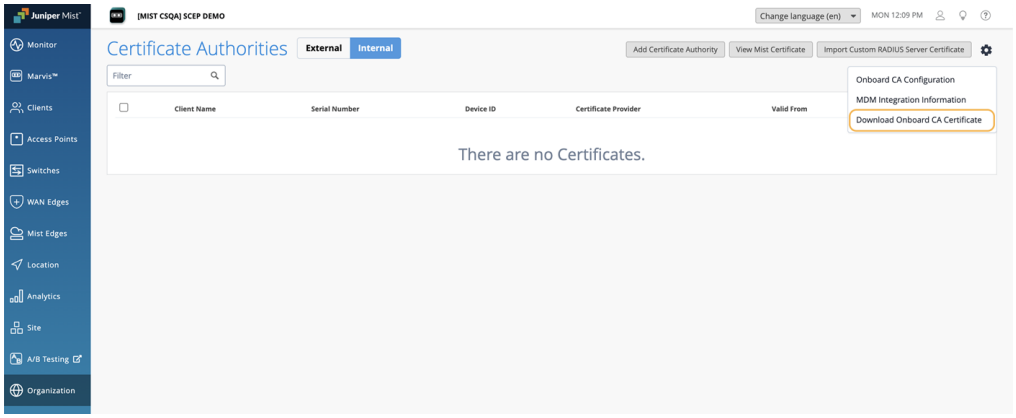
5. Copy the JAMF Access Token, JAMF Webhook URL, and JAMF SCEP URL. You'll need to use this URL in the JAMF SCEP profile.



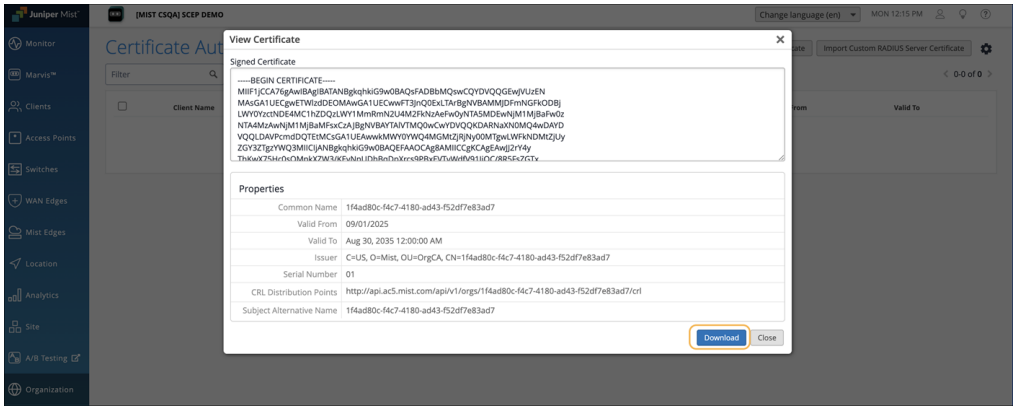
Download the Mist Org CA and Onboard CA Certificates

The Mist Org CA certificate is required to configure JAMF managed clients to trust the RADIUS server certificate of the Mist Access Assurance service. The onboard CA certificate is needed to configure the SCEP profile on JAMF.

1. Click the settings icon on the upper-right corner of the Certificates page and select **Download Onboard CA Certificate** to download the certificate issued by the built-in Mist Org CA.



2. Navigate to **Organization**>**Access**>**Certificates**. Click **View Mist Certificate** and click **Download**.



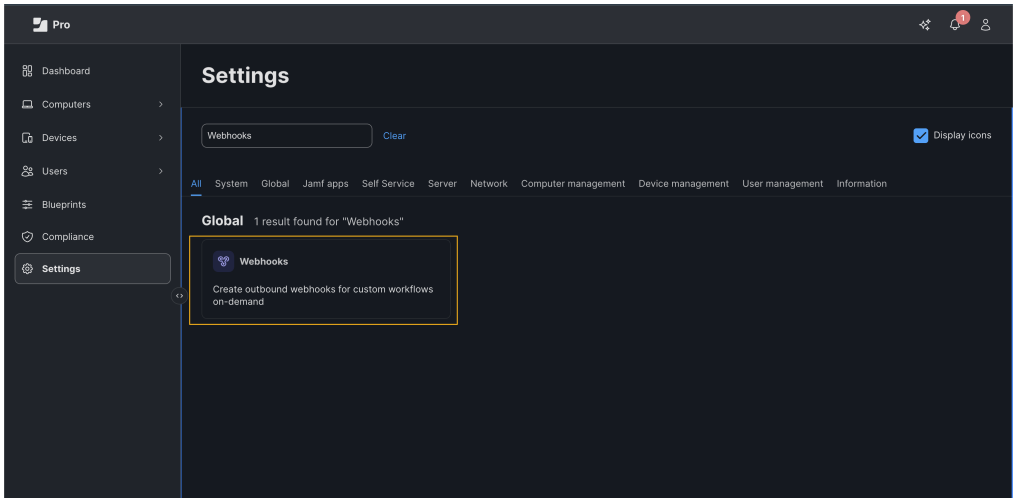
NOTE: If you are using a Custom RADIUS Server Certificate, the Mist Org CA certificate is not required. You'll need to have the Root CA certificate of the Custom RADIUS Server Certificate issuer.

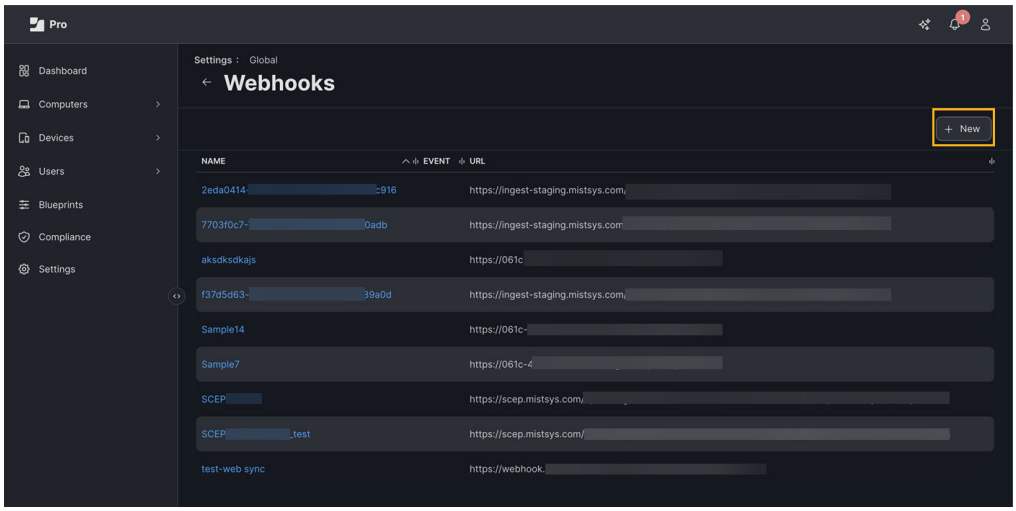
Configure a JAMF Webhook

You'll need to configure a JAMF webhook to receive dynamically generated SCEP challenges for each certificate enrollment request.

NOTE: The screenshots from third-party applications are correct at the time of publishing. We have no way to know when or if the screenshots will be accurate at any future time. Please refer to the third-party website for guidance about changes to these screens or the workflows involved.

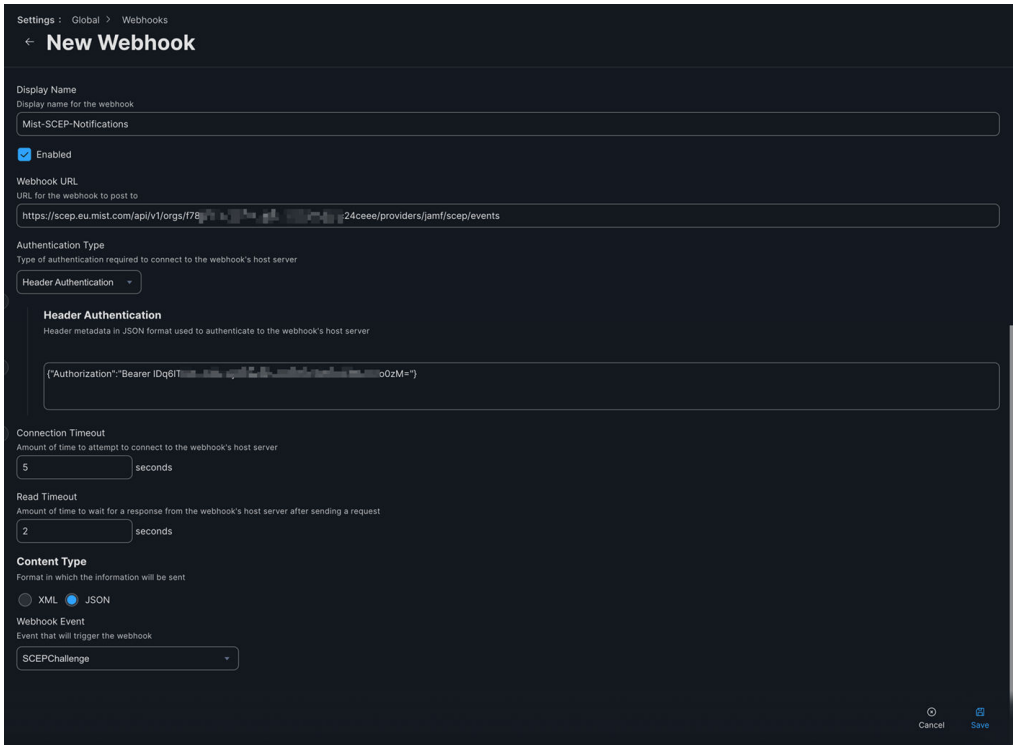
1. In the JAMF Pro dashboard, navigate to **Settings**>**Webhooks**, and click **New**.





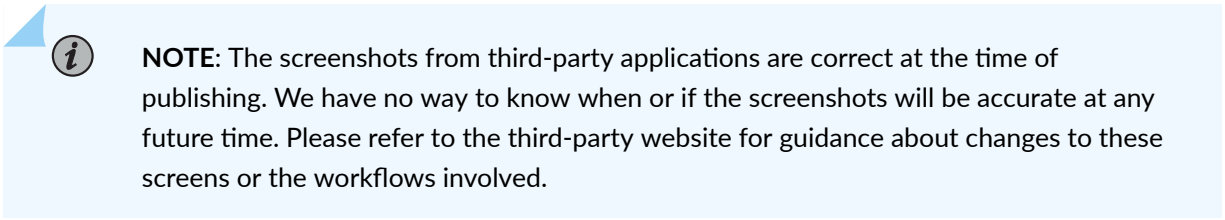
2. In the New Webhook page, enter the following information and click **Save**:

   - Display Name—Name for the webhook
   - Webhook URL.—Jamf Webhook URL that you copied earlier.
   - Authentication Type—Header Authentication
   - Header metadata—{"Authorization":"Bearer <Jamf Access Token"}
   - Connection Timeout—5 seconds
   - Read Timeout—2 seconds
   - Content Type—JSON
   - Webhook Event—SCEP Challenge



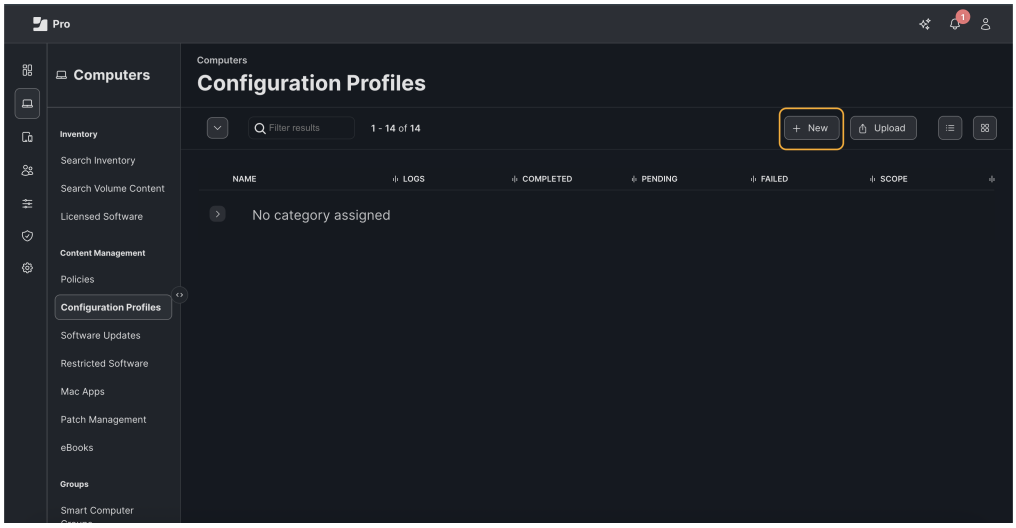
Create a Configuration Profile

We've used the macOS device as an example, but the steps are the same for iOS devices.



NOTE: The screenshots from third-party applications are correct at the time of publishing. We have no way to know when or if the screenshots will be accurate at any future time. Please refer to the third-party website for guidance about changes to these screens or the workflows involved.

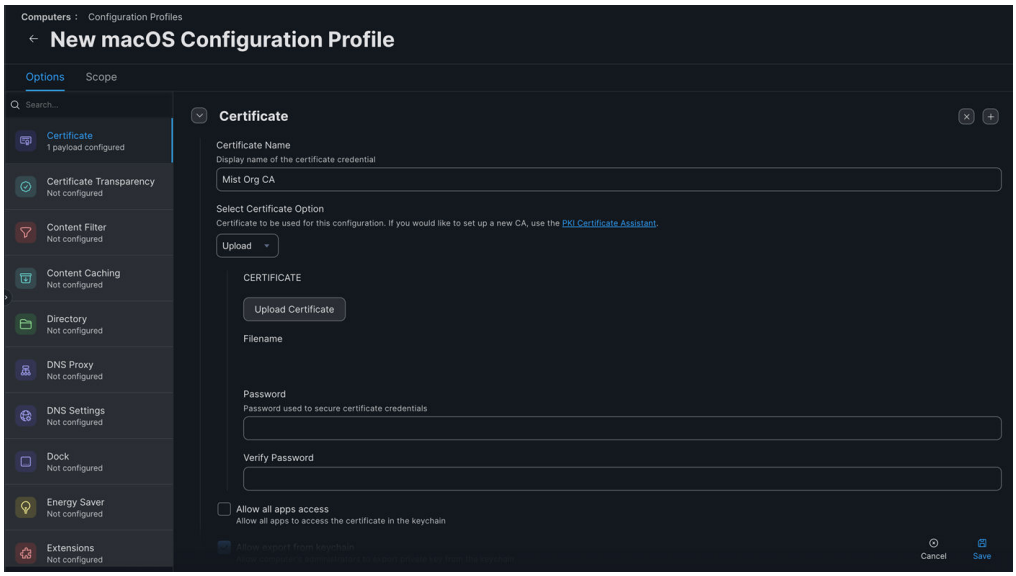
1. In the JAMF Pro dashboard, navigate to **Computers** >**Configuration Profiles** , and click **New**.



2. Select the **Certificate** tab, enter the following information and click **Save**:

   - Certificate Name
   - Click **Upload Certificate** and upload the Mist Org CA certificate that you downloaded earlier.

     If you are using a Custom RADIUS Server Certificate, the Mist Org CA certificate is not required. You'll need to have the Root CA certificate of the Custom RADIUS Server Certificate issuer.



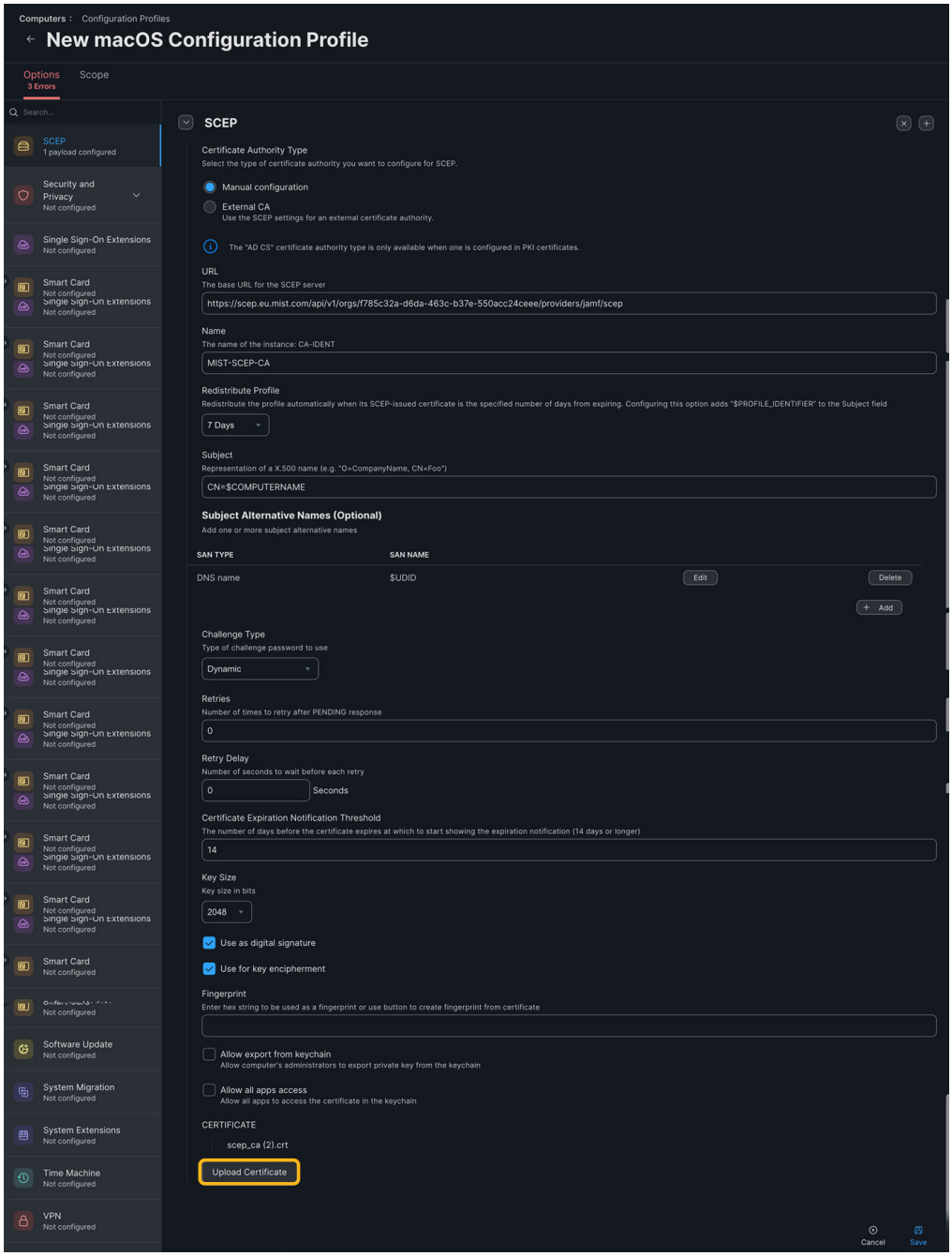
3. Select the **SCEP** tab, enter the following information and click **Save**:

   - URL—Jamf SCEP URL
   - Name—MIST-SCEP-CA

- Redistribute Profile—number of days before the certificate expiration date to push the profile again
- Subject—CN=$COMPUTERNAME
- SAN Type—add the DNS Name with value $UDID

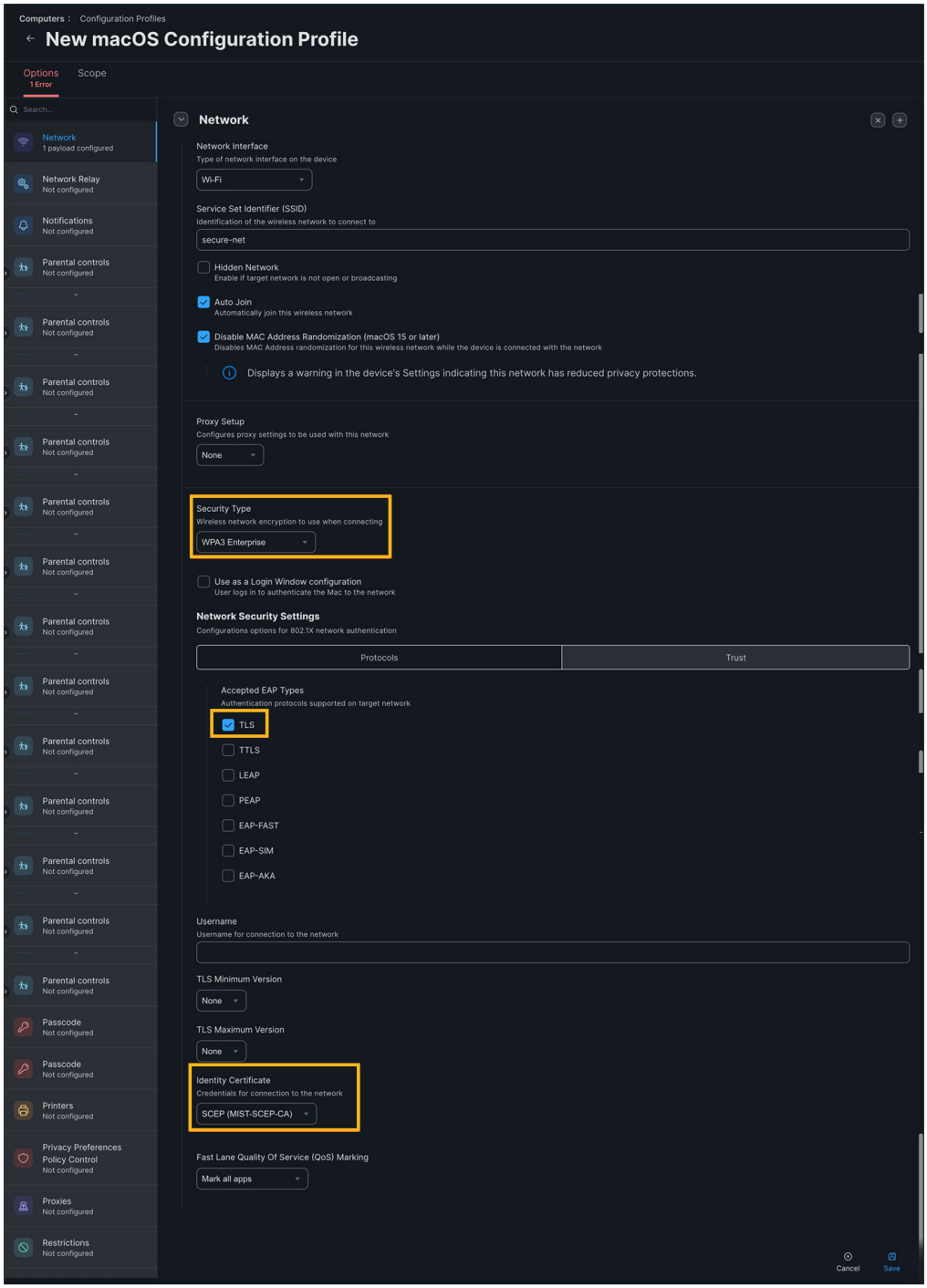
> **NOTE**: Including the Device ID in the SAN:DNS field is mandatory because NAC uses this value for device identification and compliance checks.

- Challenge Type—Dynamic
- Retries—3
- Retry Delay—5
- Certificate Expiration Notification Threshold—number of days before the certificate expiration date to display the certificate expiration notification
- Key Size—2048
- Select the **Use as digital signature** checkbox
- Select the **Use for key encipherment** checkbox
- Do not select the **Allow Export from keychain** checkbox
- Certificate—Upload the Mist Onboard CA certificate that you downloaded in the earlier step.

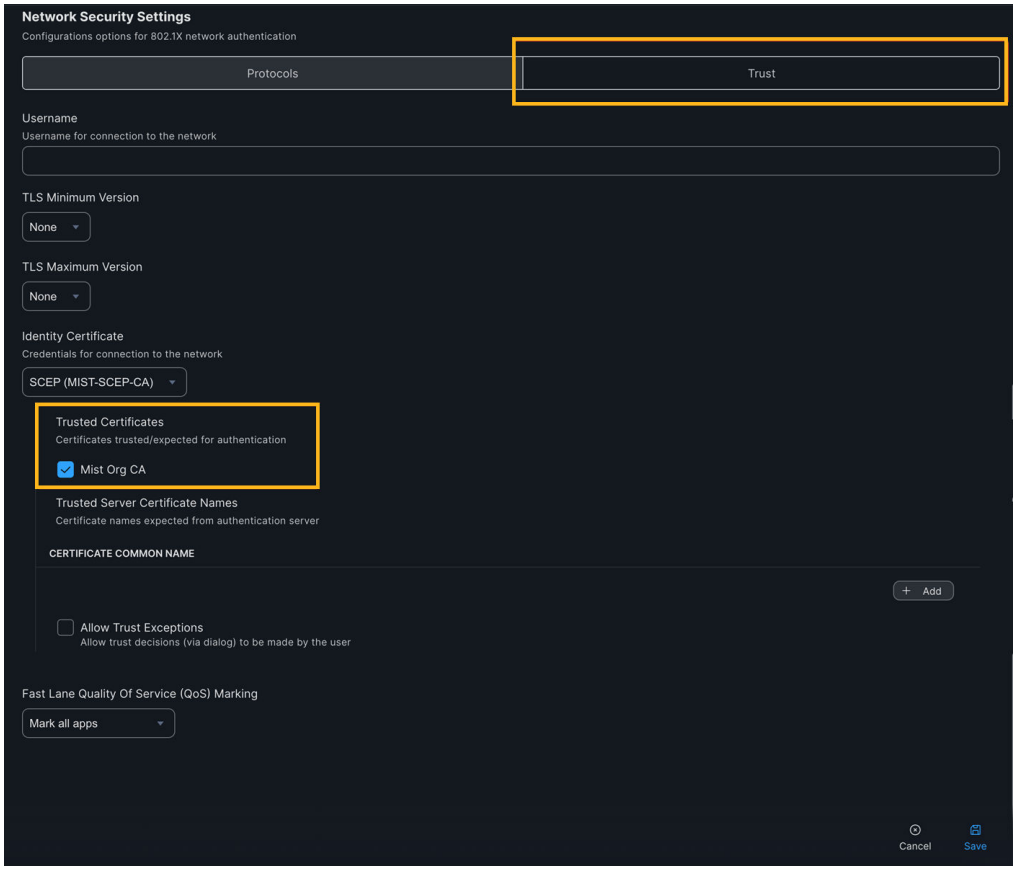


4. Select the **Network** tab, click **Configure** to enable the Wi-Fi profile. Enter the following information and click **Save**:

   - SSID—Your SSID name
   - Security Type—WPA2 or WPA3 Enterprise depending on your WLAN configuration
   - Accepted EAP Types—TLS
   - Identity Certificate—SCEP (MIST-SCEP-CA)



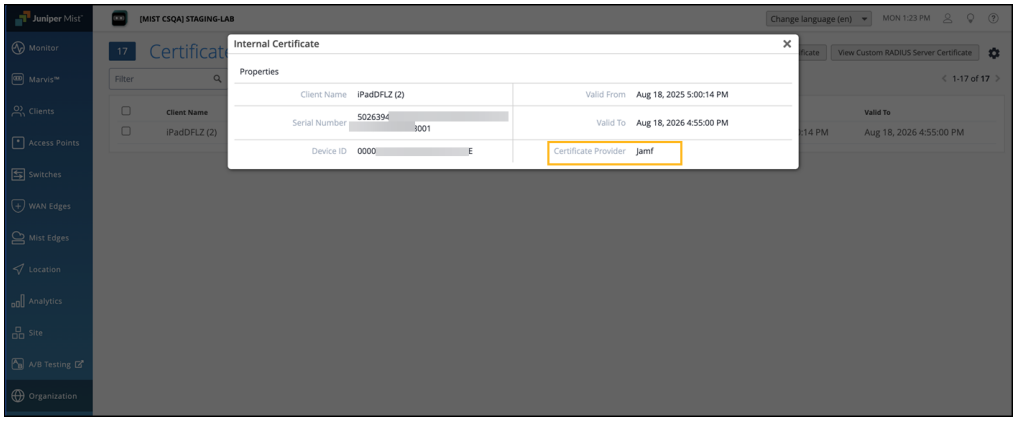
Ensure to select the **Trust** tab and check the Mist Org CA certificate for Server Certificate validation:



5. Select the **Scope** tab and assign the profile to your devices.

   When the profile is pushed to the client, you'll see a new certificate issued to your macOS device under **Keychain Access** >**My Certificates**.

   Switch to the Juniper Mist portal and confirm that the client certificate is issued under **Certificates**>**Internal**.



Integrate with Microsoft Intune

SUMMARY

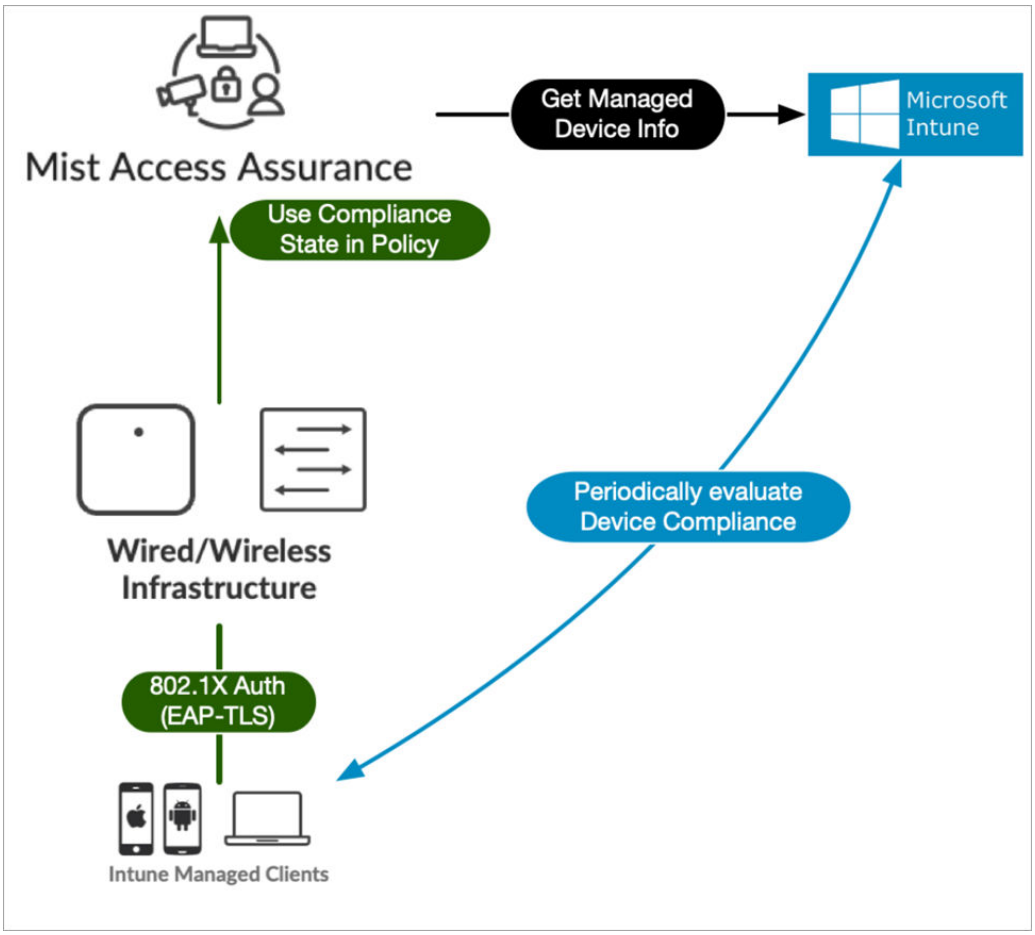
Follow these steps to understand Intune integrations, link your Intune account to your Juniper Mist organization, create policy rules, and view client events.

IN THIS SECTION

Overview

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.

Figure 27: Microsoft Intune Integration for Getting Compliance State of the Device



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).

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.

NOTE: Some of the screenshots included in this document are sourced from third-party applications. Be aware that these screenshots may change over time and may not always match the current version of the applications.

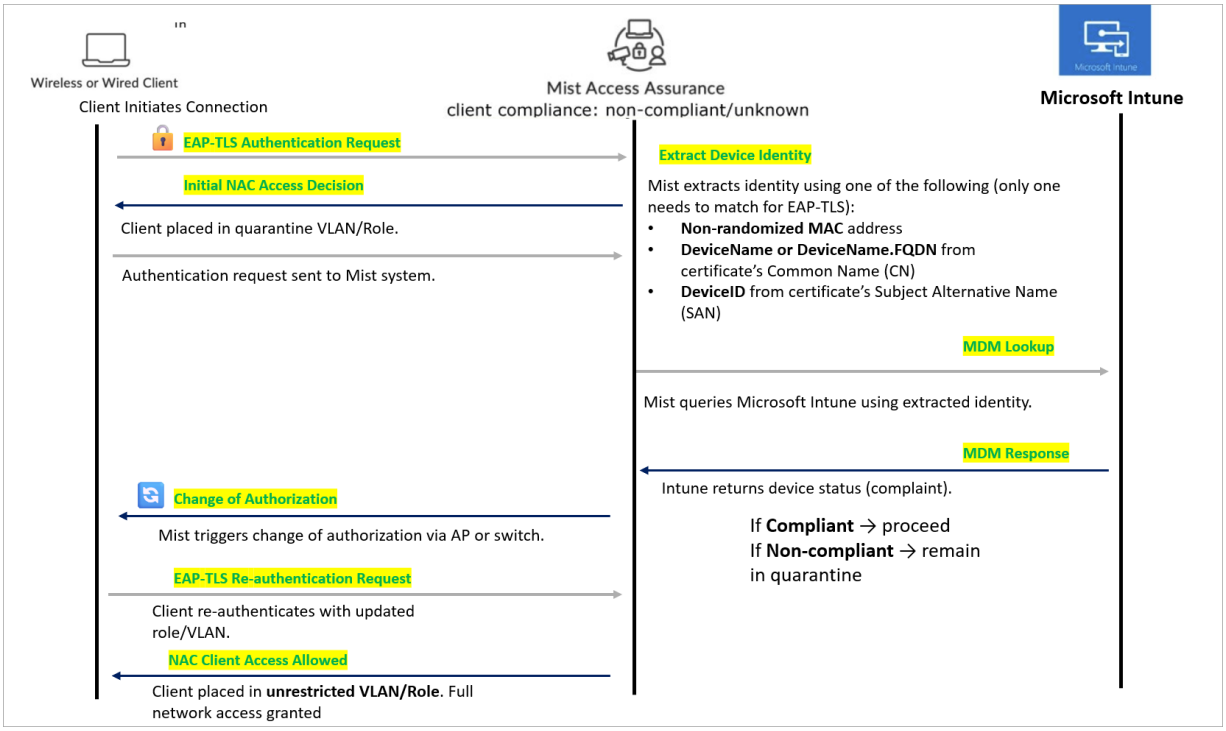
How it Works

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 if 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 Figure 28 on page 86.

Figure 28: Authentication and Authorization for Microsoft Intune



Client onboarding sequence includes:

1. EAP-TLS Authentication—Client initiates a connection (wired or wireless) and authentication request is sent to the Mist system.
2. Initial NAC Access Decision—Client is placed in a quarantine VLAN/Role. Restricted access is provided until device compliance is verified.
3. Device Identity Extraction—Mist uses the following information during client authentication to match a client with a device record in Microsoft Intune (in order of lookup):
   - Non-randomized MAC address
   - DeviceName or DeviceName.FQDN from the certificate's Common Name (CN) field
   - DeviceID from the certificate's Subject Alternative Name (SAN) as a DNS entry

   For EAP-TLS authentication, a match is successful if any one of these identifiers is found.

   For EAP-TTLS authentication, Mist Access Assurance uses only the non-randomized MAC address to match with Intune device records.
4. MDM Lookup—Mist queries Microsoft Intune using the extracted identity.Retrieve the device's compliance status.
5. MDM Response- Intune returns the device status.
   - If the client device is found compliant, access is provided.
   - If the client device is non-compliant, it remains in quarantine.
6. Change of Authorization (CoA)—Mist triggers CoA via the AP or switch. Client session is refreshed with updated access rights.
7. EAP-TLS Re-Authentication—Client re-authenticates with the updated VLAN/Role.
8. Final NAC Access Decision—Client is placed in an unrestricted VLAN/Role. Full network access is granted.

NOTE: The device lookup process via Microsoft Intune can time depending on system load and response intervals. To ensure a seamless onboarding experience, we recommend configuring an authentication policy that permits initial access for the client device.

Configure the policy in accordance with your organization's security standards and access control policies to establish appropriate safeguards during the initial connection.

Once the MDM lookup succeeds and the device record is added to the Dynamic Device Database (DDB), the Mist MDM service automatically sends a Change of Authorization (CoA) message to the associated AP or switch. This prompts the client to reconnect.

Upon reconnection, the client is evaluated against the MDM Authentication policy, which determines access based on the device's compliance status—either Compliant or Non-compliant.

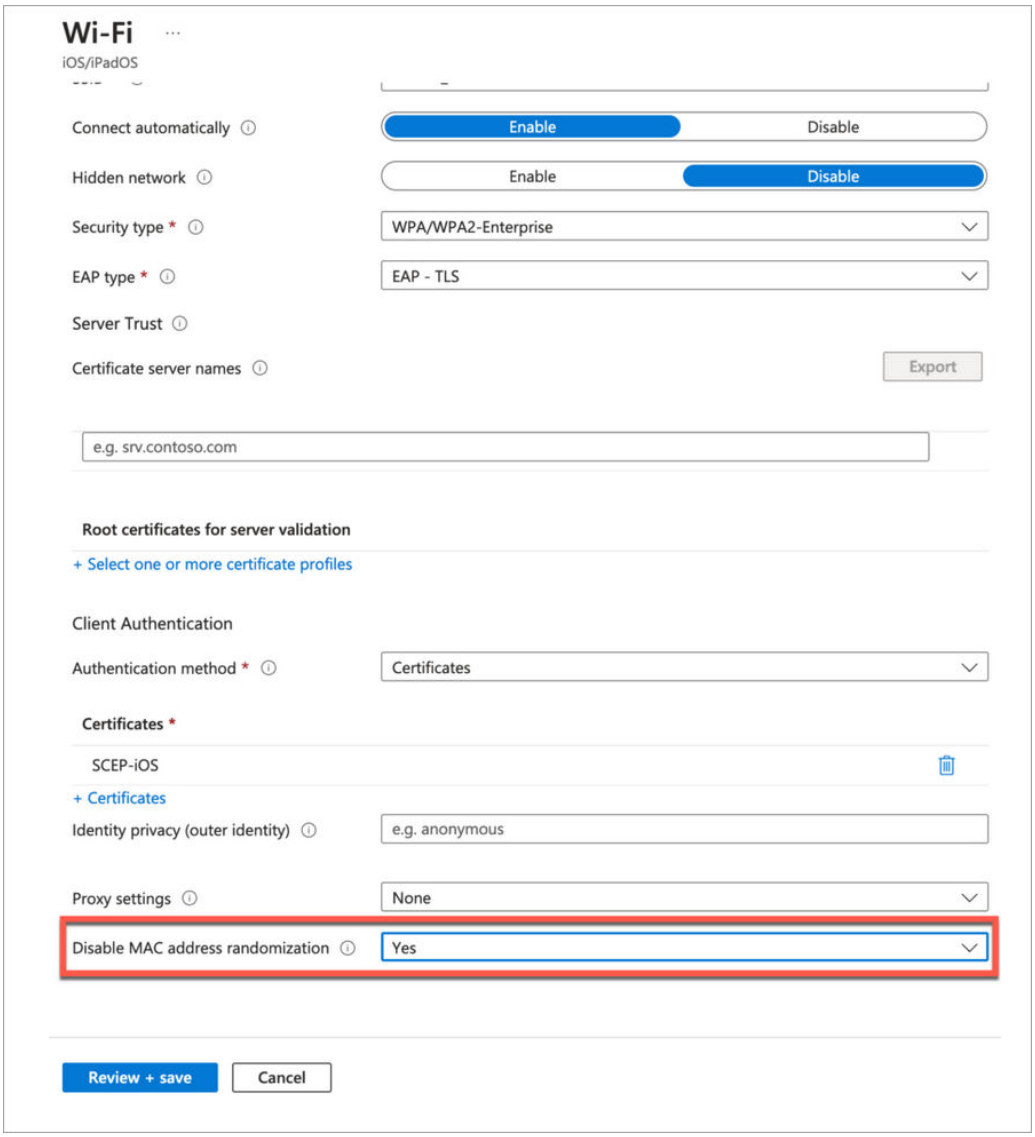
Following sections provide more details about the identifiers.

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.

NOTE: The screenshots from third-party applications are correct at the time of publishing. We have no way to know when or if the screenshots will be accurate at any future time. Please refer to the third-party website for guidance about changes to these screens or the workflows involved.

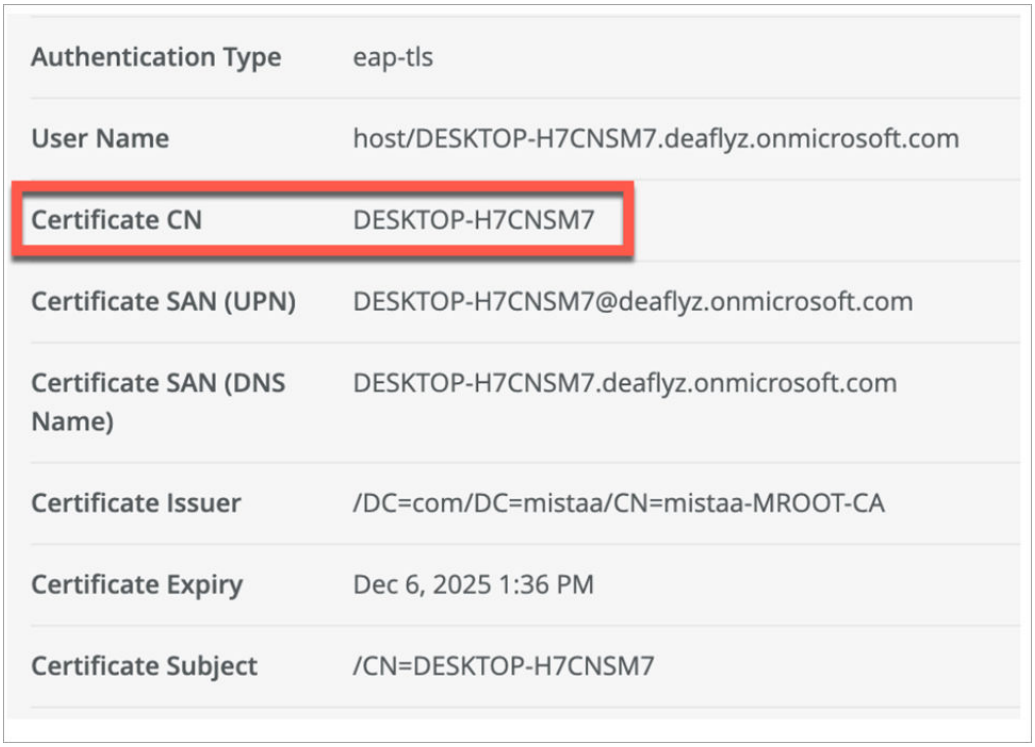
Figure 29: Disable MAC Address Randomization



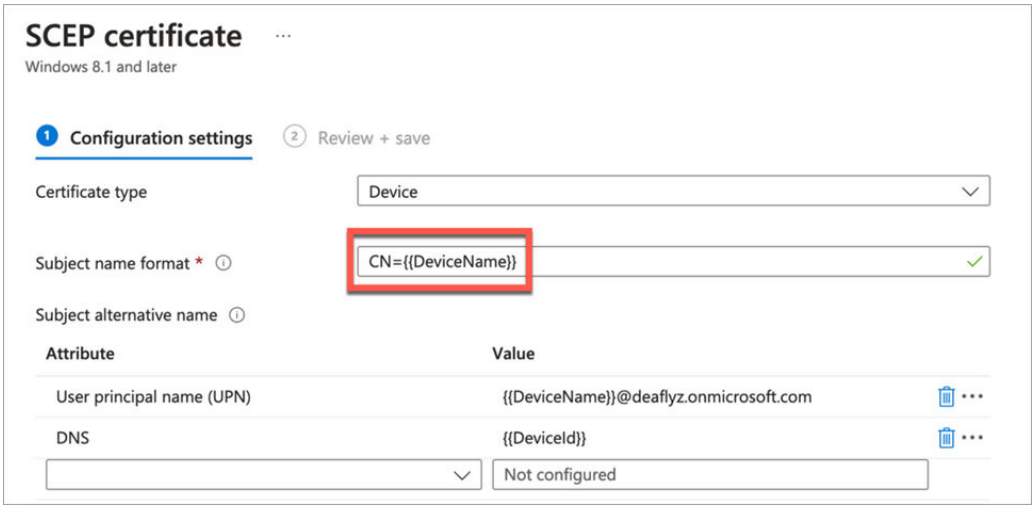
DeviceName or DeviceName.FQDN

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

Figure 30: Certificate CN Details

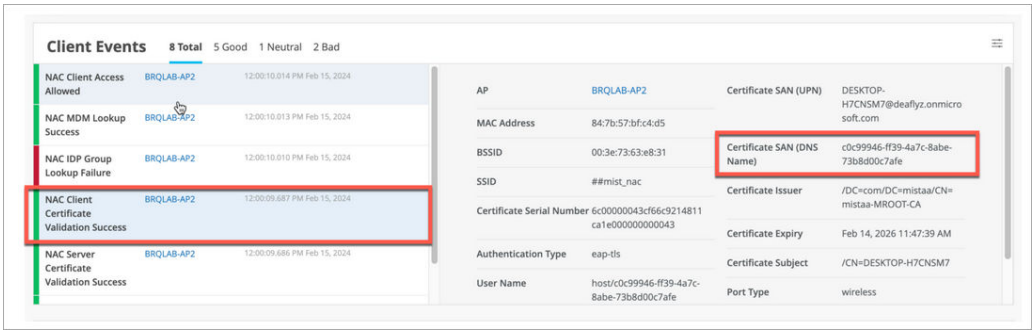


In Intune SCEP profile, use the variables to create this certificate.

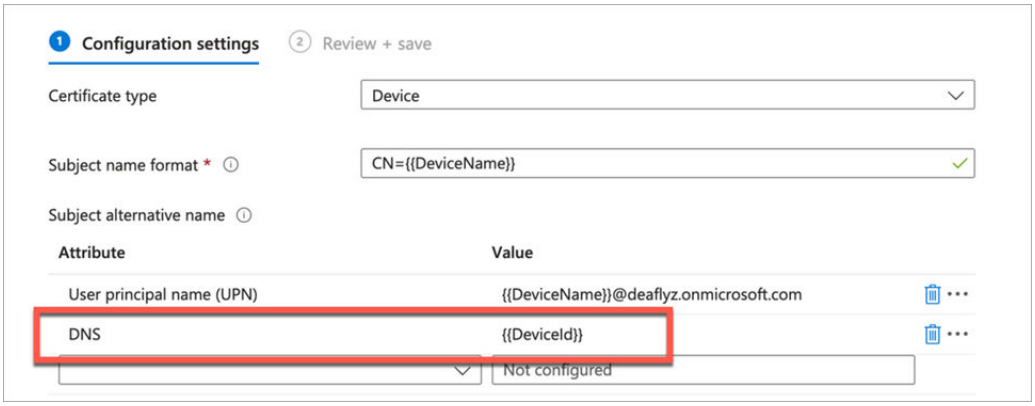


DeviceID in Certificate's SAN:DNS

Intune Device ID encoded in SAN:DNS certificate attribute in Juniper Mist portal client events as shown in the following illustration.



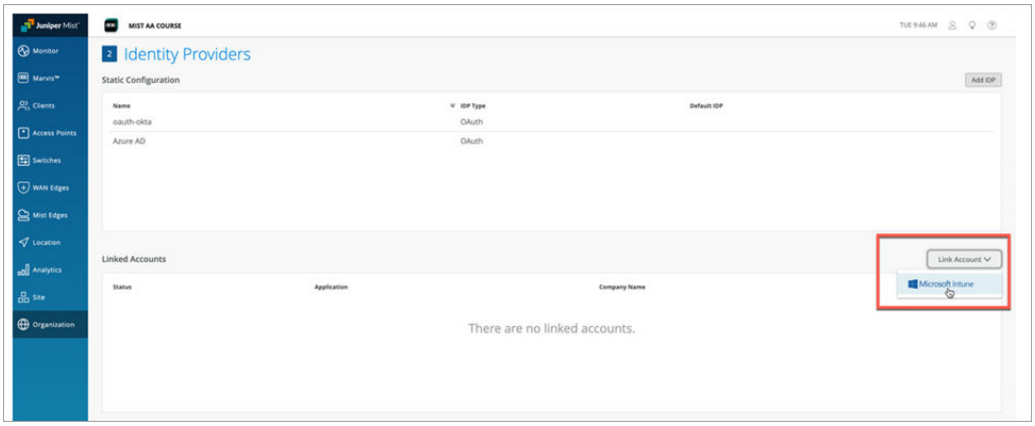
In Intune SCEP profile, use the variable to encode Intune Device ID in the SAN:DNS certificate field.



Adding Intune to the Mist Portal

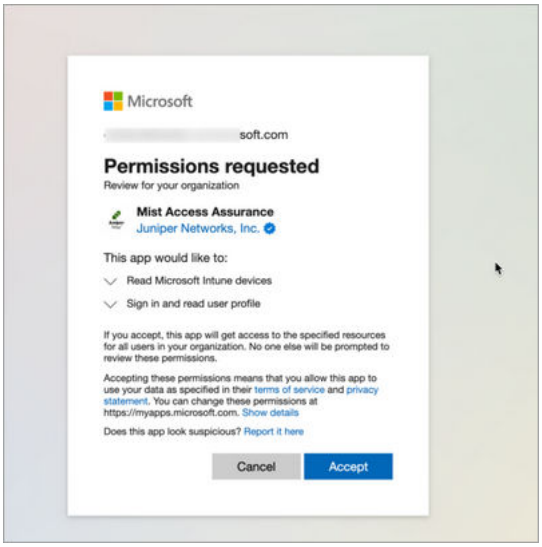
To add Microsoft Intune to the Mist Access Assurance portal:

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.



4. 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.

Figure 31: Permissions for Intune Integration



After linking the Intune account, connected Intune account status is displayed on the Identity Providers page.

Figure 32: Linked Intune Account Status

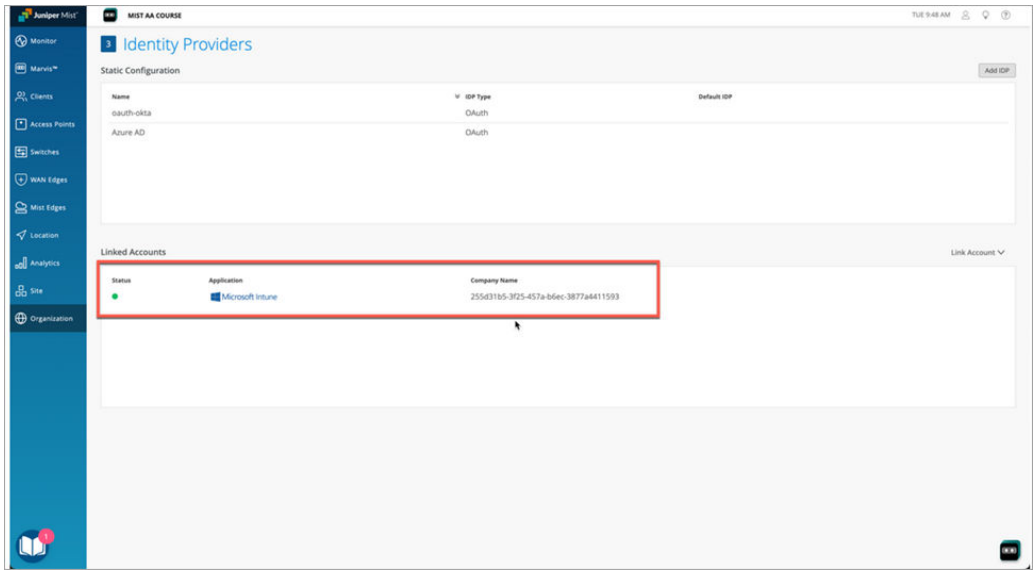
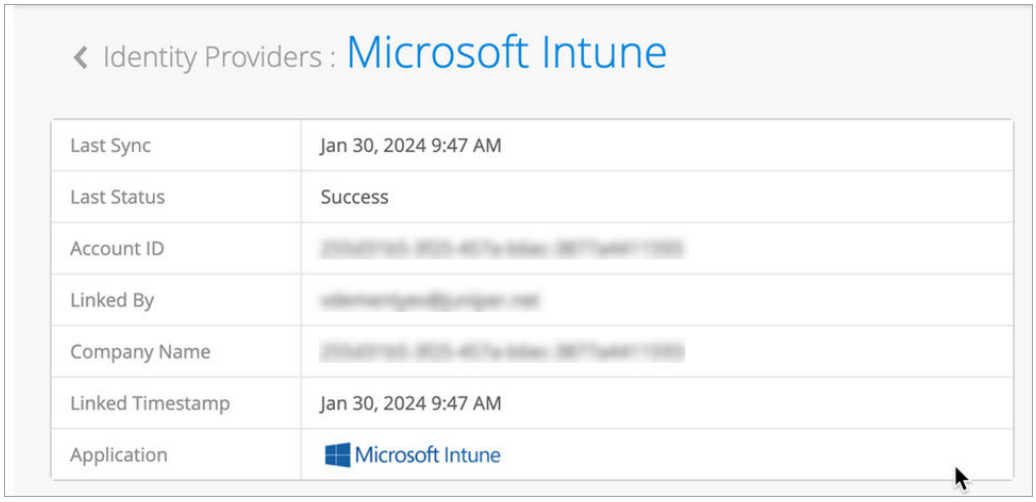


Figure 33: Linked Intune Account Details



5. (Optional) After linking the Intune account, you can see the Intune account status on the Identity Providers page: **Organization | Access > Identity Providers**.

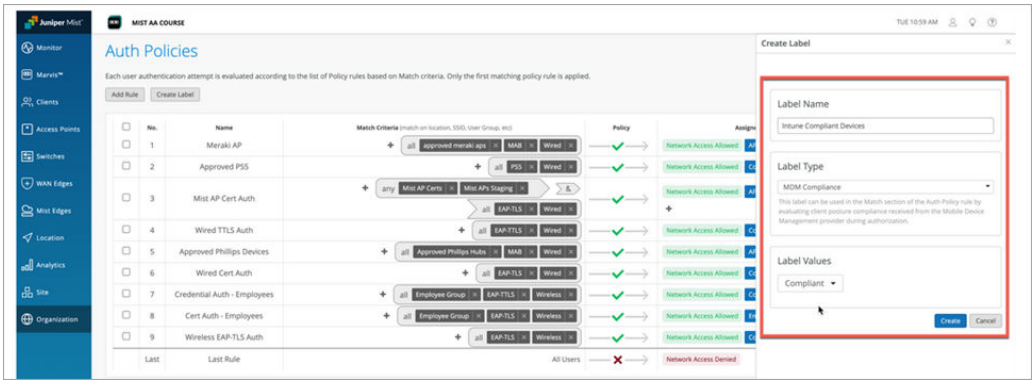
Creating Policy Rules

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.

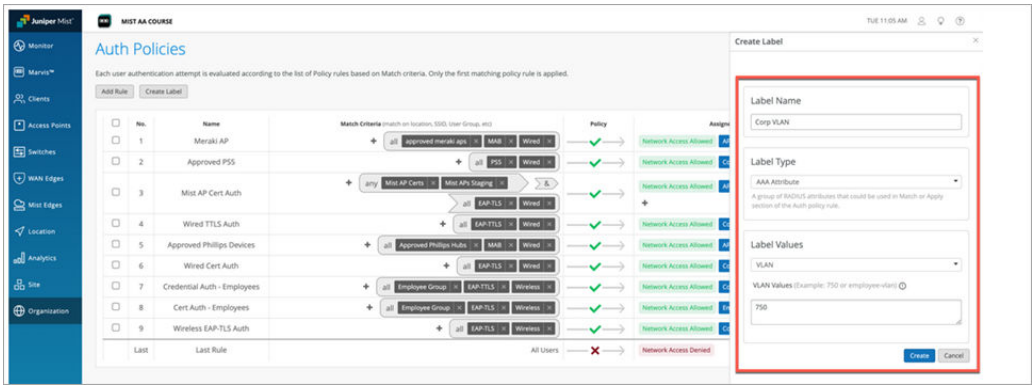
Create compliance and quarantine labels:

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

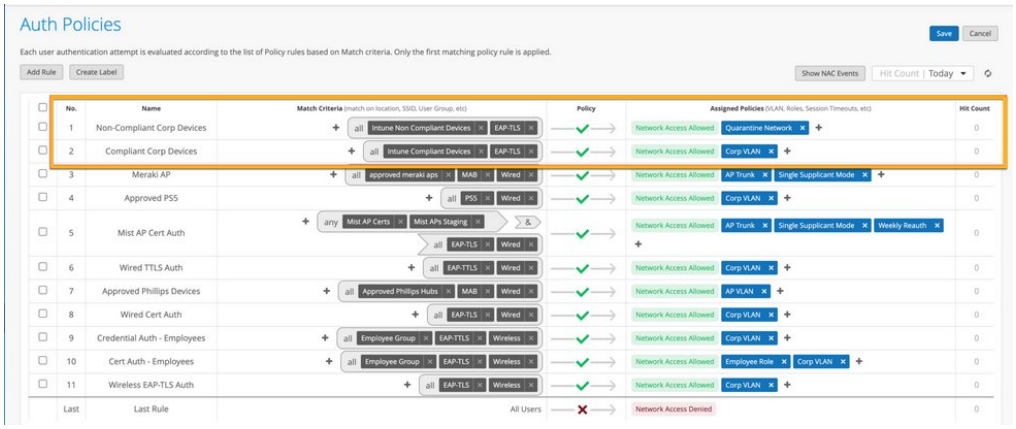
   - **Label Name**: Quarantine, **Label Type**: AAA, **Label Value**: VLAN, *1*
   - **Label Name**: Corp VLAN, **Label Type**: AAA, **Label Value**: VLAN, *750*



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**.

Figure 34: Compliance Rules Based on Intune

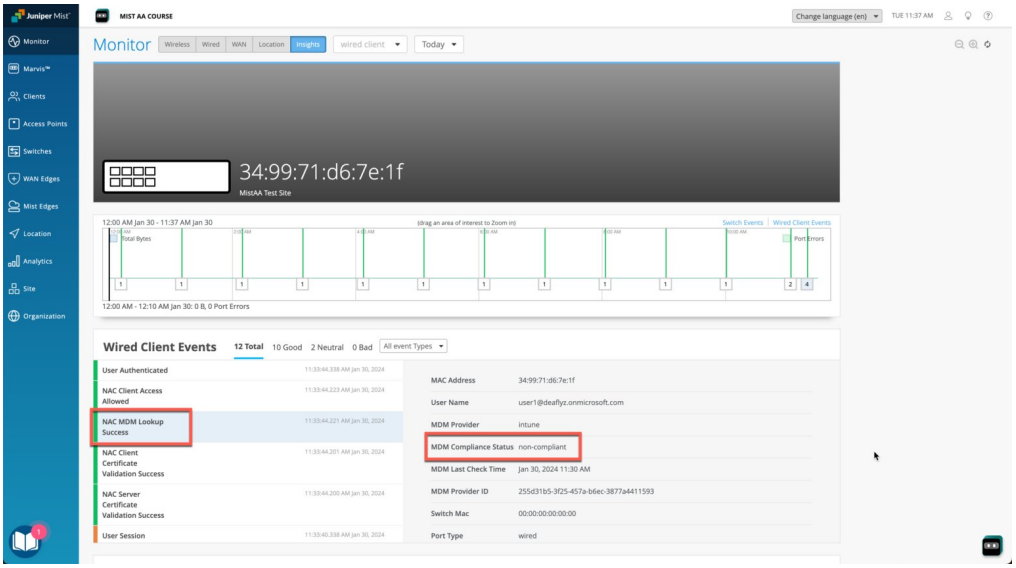


5. Repeat these steps to create the quarantine rule.
6. When finished, click **Save**.

Viewing Client Events

As shown in the following illustration, 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.

Figure 35: Monitor Intune-based Access Assurance Policy Events in the Mist Portal



RELATED DOCUMENTATION

Juniper Mist Access Assurance Authentication Methods | 8

Integrate Microsoft Entra ID as an Identity Provider | 46

Onboard CA and SCEP Integration for Microsoft Intune-Managed Devices

SUMMARY

Onboard CA Configuration in Juniper Mist Access Assurance provides a cloud-native SCEP service that integrates directly with Intune for automated client certificate distribution. This eliminates the need for an external PKI and simplifies secure Wi-Fi onboarding with EAP-TLS authentication.

IN THIS SECTION

Juniper Mist Access Assurance provides Onboard Certificate Authority (CA) Configuration, which delivers a fully managed Simple Certificate Enrollment Protocol (SCEP) infrastructure. When the Onboard CA is enabled, Access Assurance automatically provisions the Intune SCEP URL. With this URL, users can integrate Intune with Mist Access Assurance without deploying or maintaining any external PKI or on-premises SCEP service. The Onboard CA Certificate provided by Access Assurance is then used to configure a SCEP profile within Intune, enabling secure client certificate issuance to enrolled devices.

By leveraging the Access Assurance SCEP infrastructure, you can automate the distribution of client certificates to Intune-managed endpoints, binding them to Wi-Fi profiles for EAP-TLS authentication. This feature ensures that every device connecting to the network is authenticated through strong, certificate-based trust while fully managed from the Juniper Mist Access Assurance cloud.

NOTE: When a device is marked as inactive or deleted in Intune, you must revoke the client certificate manually through the Juniper Mist portal.

To enable Intune to leverage Juniper Mist Access Assurance as its SCEP infrastructure for client certificate distribution, follow these steps:

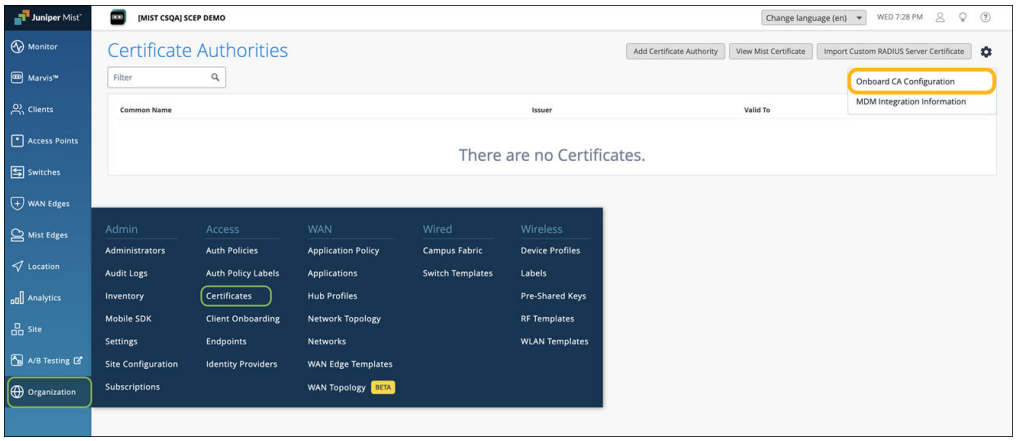
Enable Onboard CA Configuration

To enable the Onboard CA configuration:

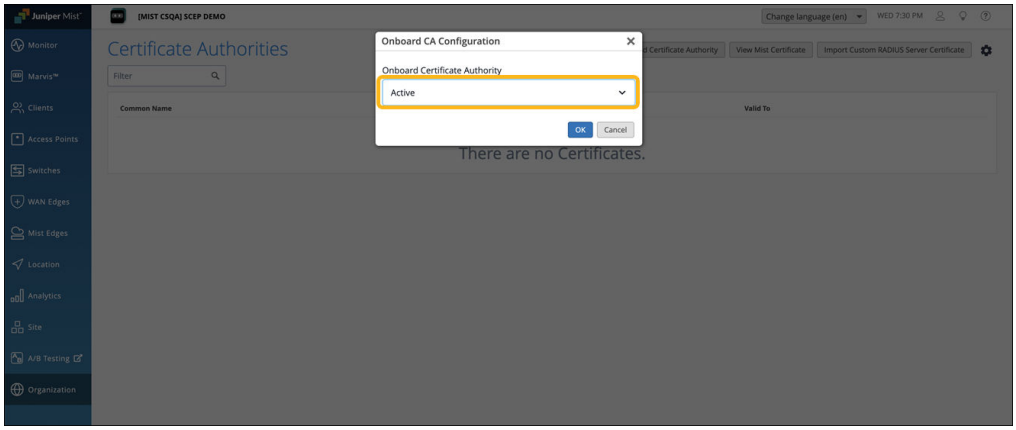
1. From the left menu of the Juniper Mist portal, select **Organization** > **Access** > **Certificates**.

   The Certificate Authorities page appears.

2. Click the settings icon on the upper-right corner of the page and select **Onboard CA Configuration**.



3. Select **Active** and click **OK**.

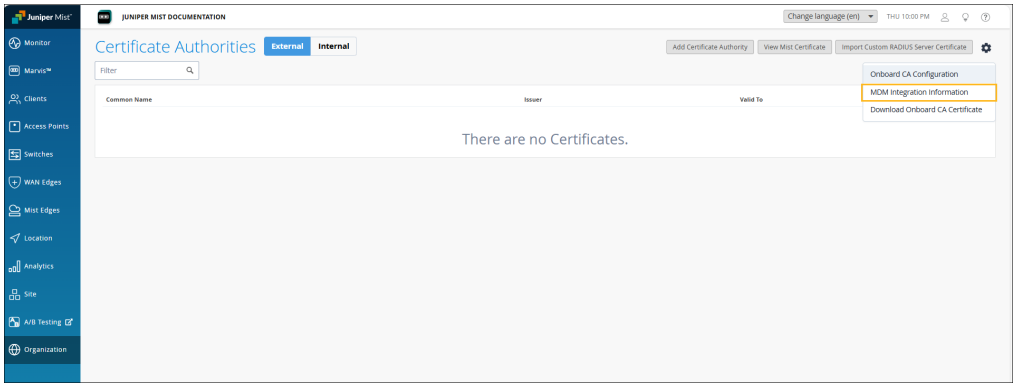


   The onboard Certificate Authority service is enabled, and the respective SCEP endpoints are generated for each MDM.

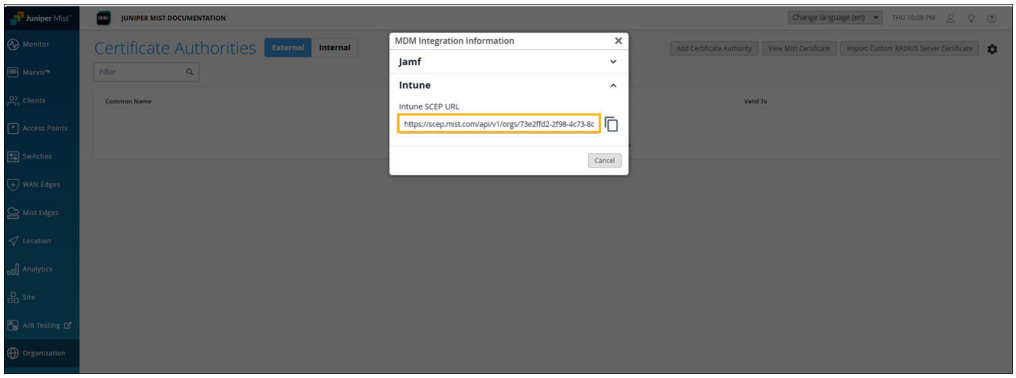
   When the Onboard CA configuration is activated, you'll see the following tabs displayed:

   - External—Displays the details of the external CAs.
   - Internal— Displays the details of client certificates issued by the built-in CA through the NAC portal or MDM.

4. Click the settings icon on the upper-right corner of the page again and select **MDM Integration Information**.



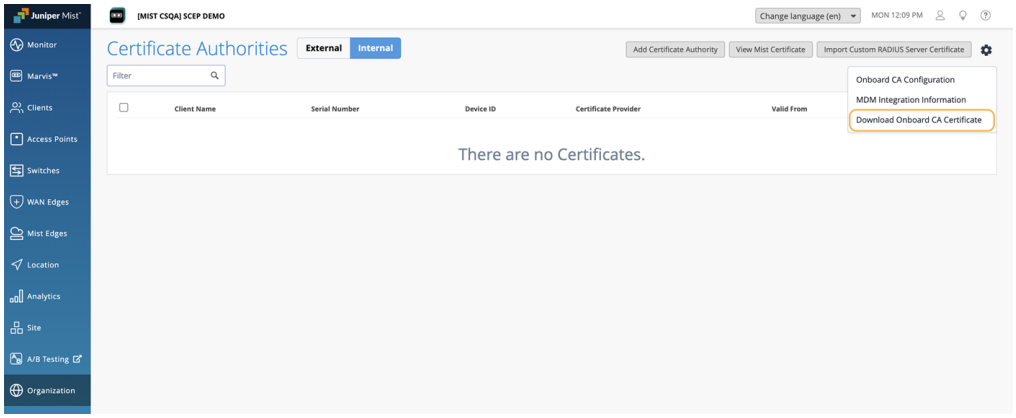
5. Copy the Intune SCEP URL listed for Intune. You'll need to use this URL in the Intune SCEP profile.



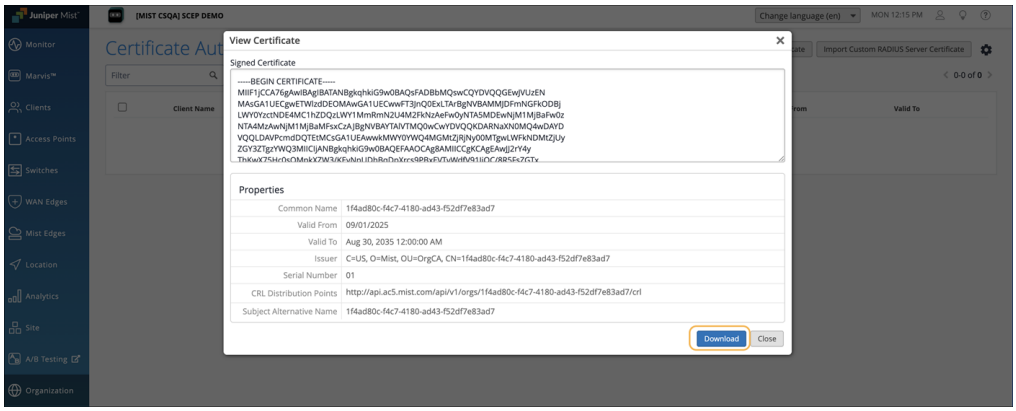
Download the Mist Org CA and Onboard CA Certificates

The Mist Org CA certificate is required to configure Intune managed clients to trust the RADIUS server certificate of the Mist Access Assurance service. The onboard CA certificate is needed to configure the SCEP profile on Intune.

1. Click the settings icon on the upper-right corner of the Certificates page and select **Download Onboard CA Certificate** to download the certificate issued by the built-in Mist Org CA.



2. Navigate to **Organization**>**Access**>**Certificates**. Click **View Mist Certificate** and click **Download**.



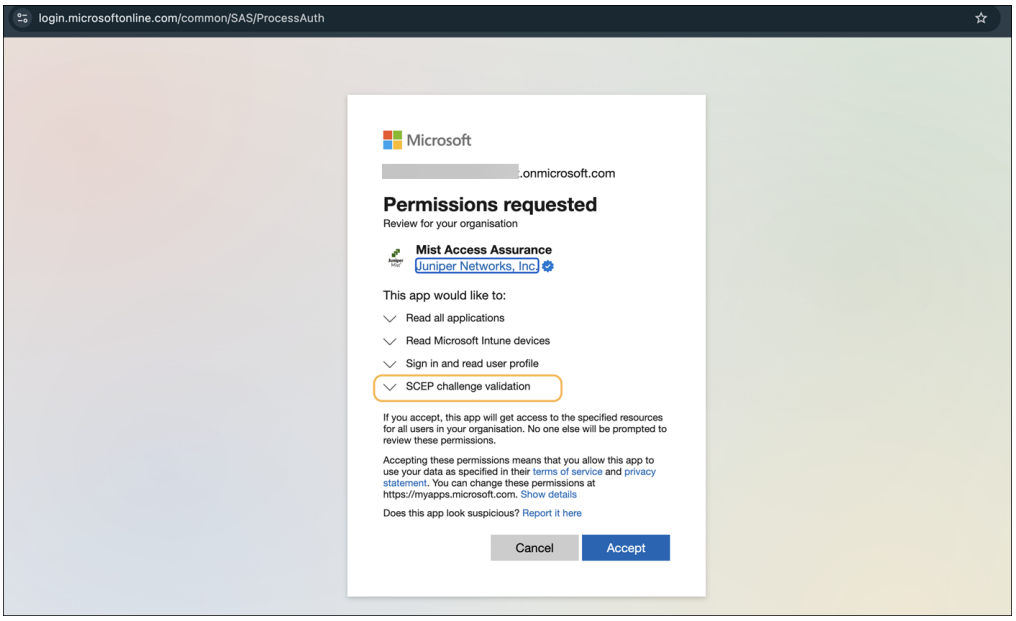
NOTE: If you are using a Custom RADIUS Server Certificate, the Mist Org CA certificate is not required. You'll need to have the Root CA certificate of the Custom RADIUS Server Certificate issuer.

Link Intune to the Mist Portal

Link your Intune account with Juniper Mist. See Adding Intune to the Mist Portal.

NOTE: The screenshots from third-party applications are correct at the time of publishing. We have no way to know when or if the screenshots will be accurate at any future time. Please refer to the third-party website for guidance about changes to these screens or the workflows involved.

NOTE: If your Intune account is already linked to the organization, you must relink the MDM account. This ensures that Mist Access Assurance receives the updated set of permissions required for Onboard CA operations.



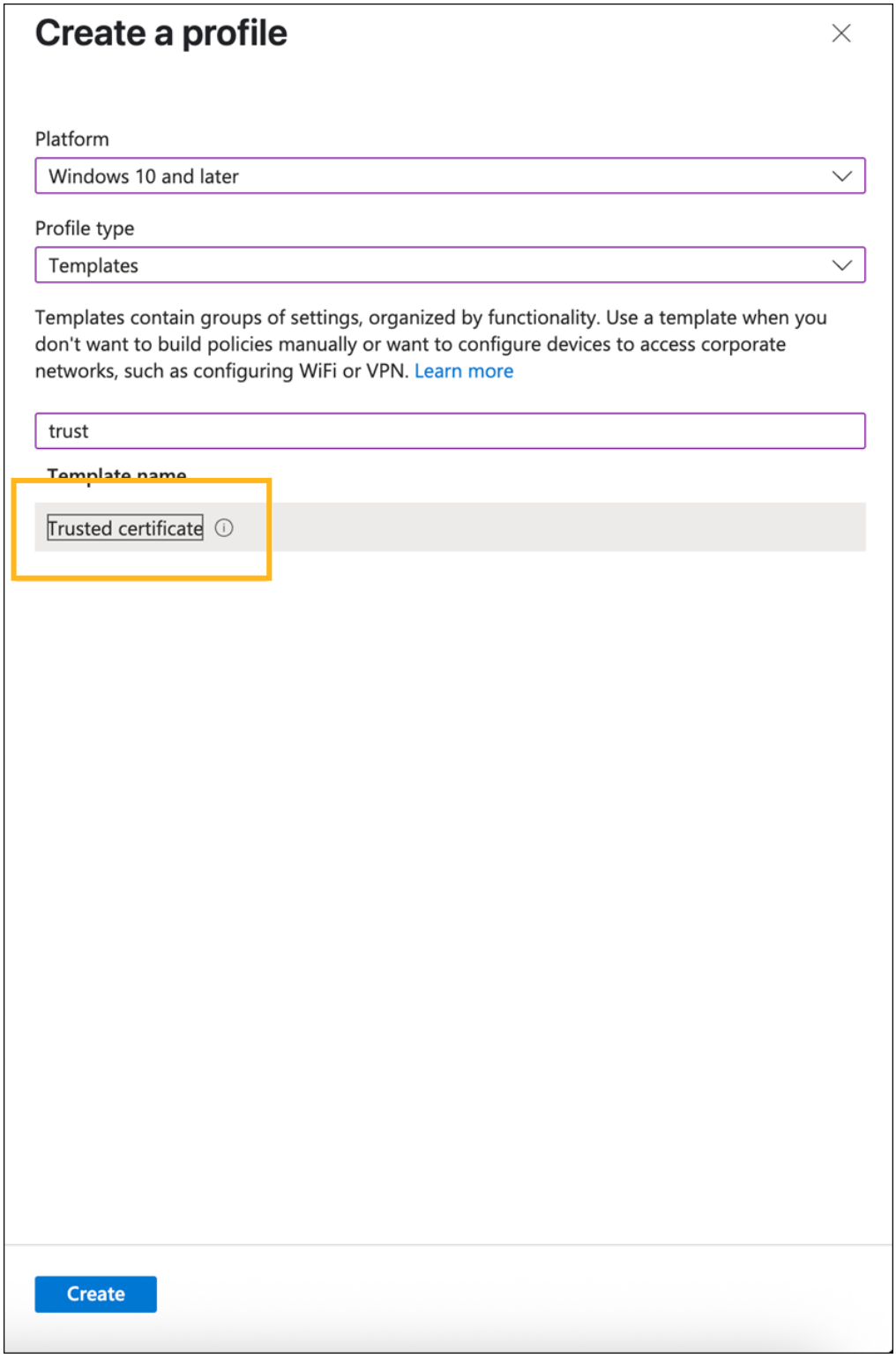
Create Configuration Profiles

Create OS-specific configuration profiles in Intune.

Create Trusted Certificate Profile

For each OS type that you plan to enroll, create two Trusted Certificate Profiles—one for the Mist CA certificate and one for the Mist SCEP CA certificate.

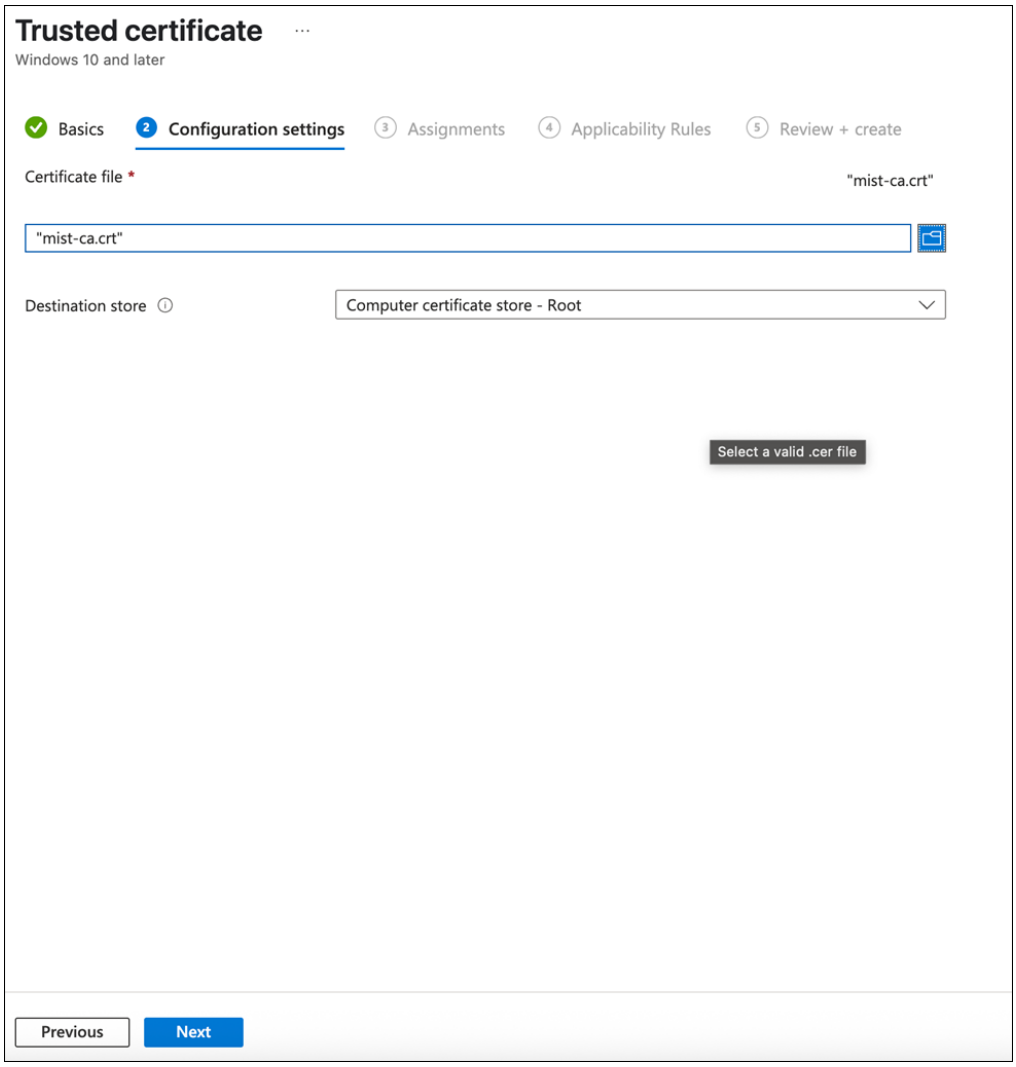
1. Navigate to **Devices**>**Configuration**, and click **Create**>**New Policy**.
2. Select a platform. We've used Windows 10 and later in this example.
3. Select **Templates** as the Profile Type.
4. Select **trust** from the template list and click **Create**.



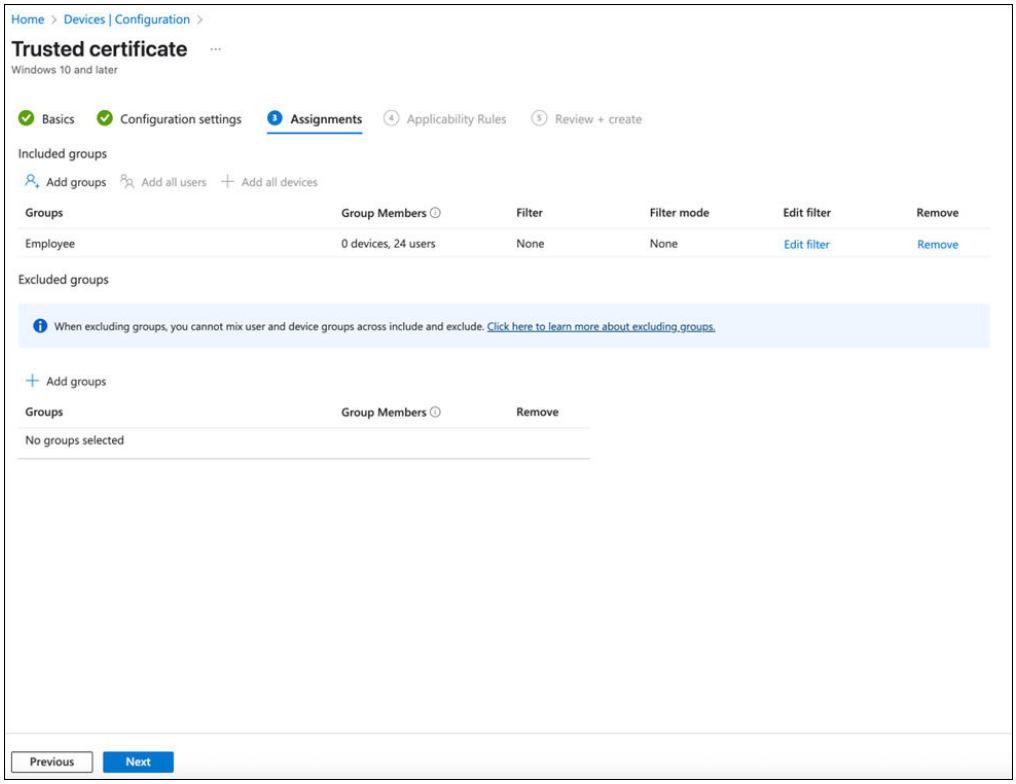
5. Provide a name for the Mist Org CA trusted certificate and click **Next**.

6. Upload the Mist Org CA certificate that you downloaded earlier.

If you are using a Custom RADIUS Server Certificate, the Mist Org CA certificate is not required. You'll need to have the Root CA certificate of the Custom RADIUS Server Certificate issuer.

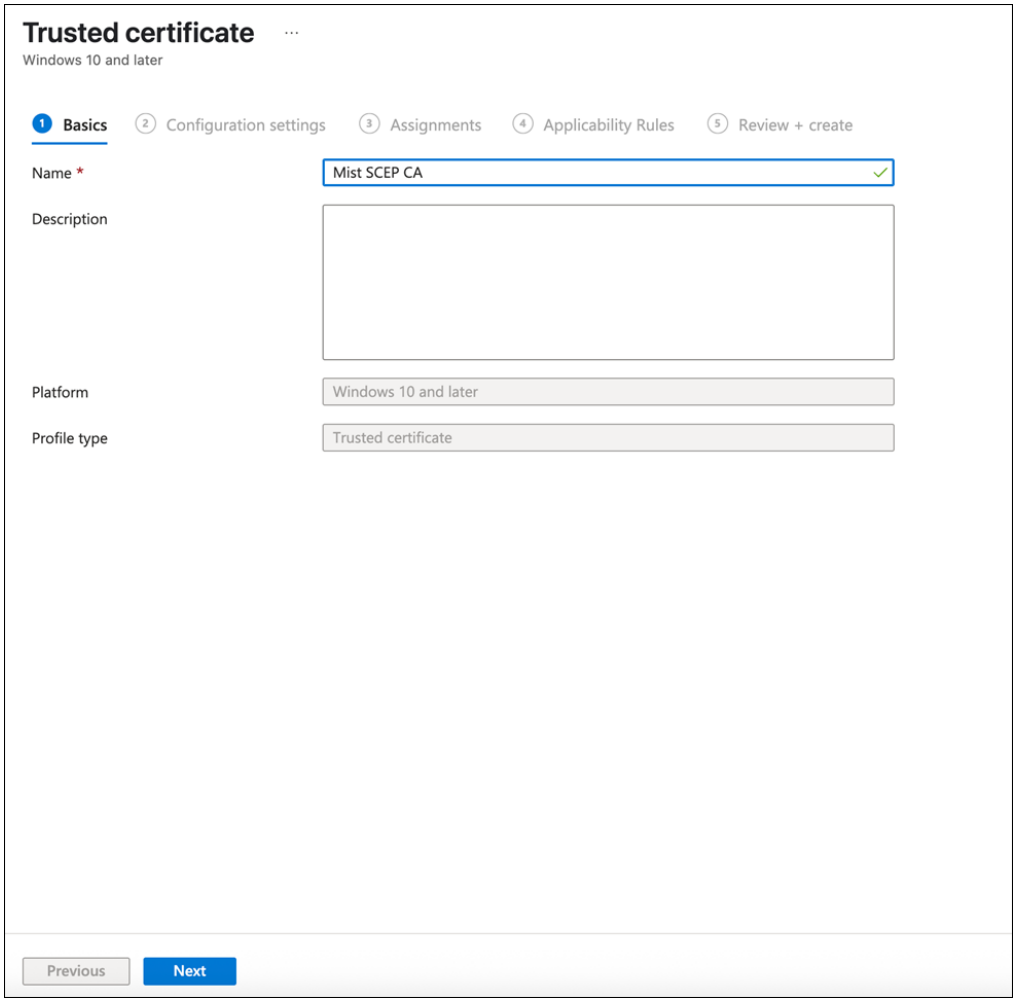


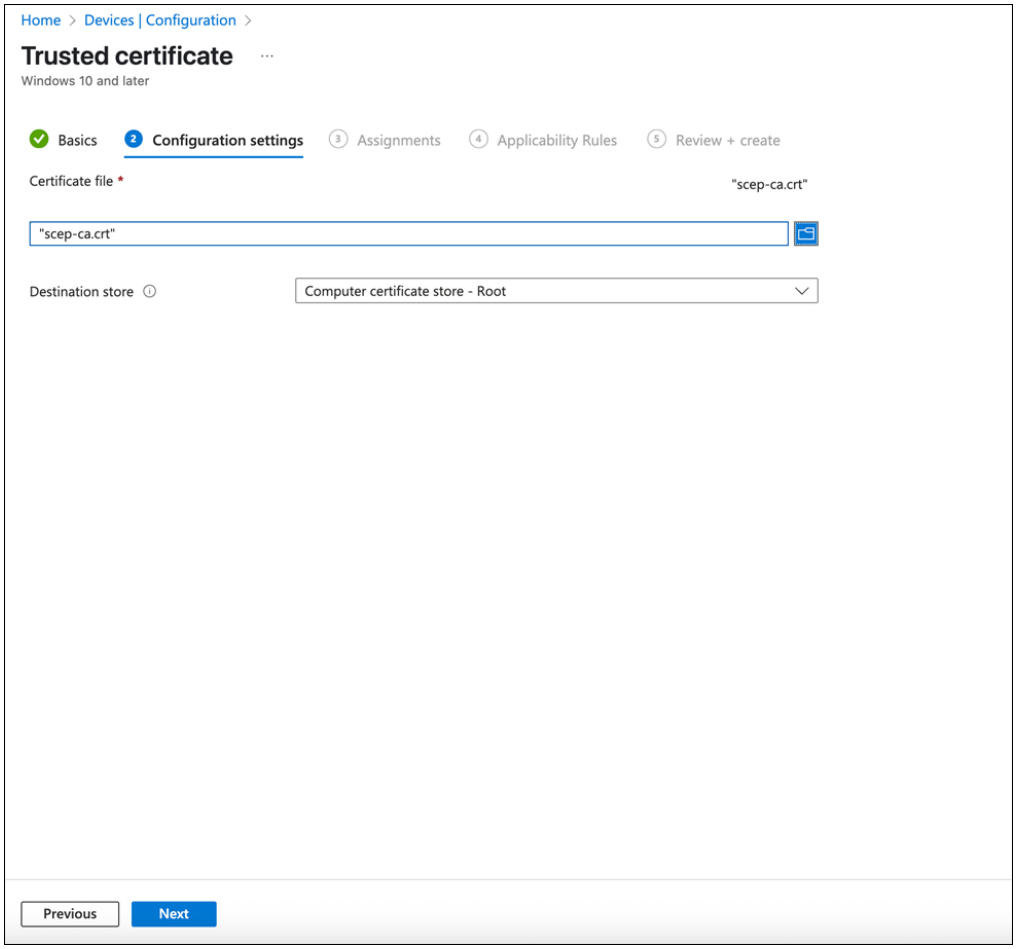
7. Assign this profile to specific user group or all devices:



8. Click **Next** and then click **Create**.

9. Repeat steps 1 through 8 for the Mist Onboard CA certificate.

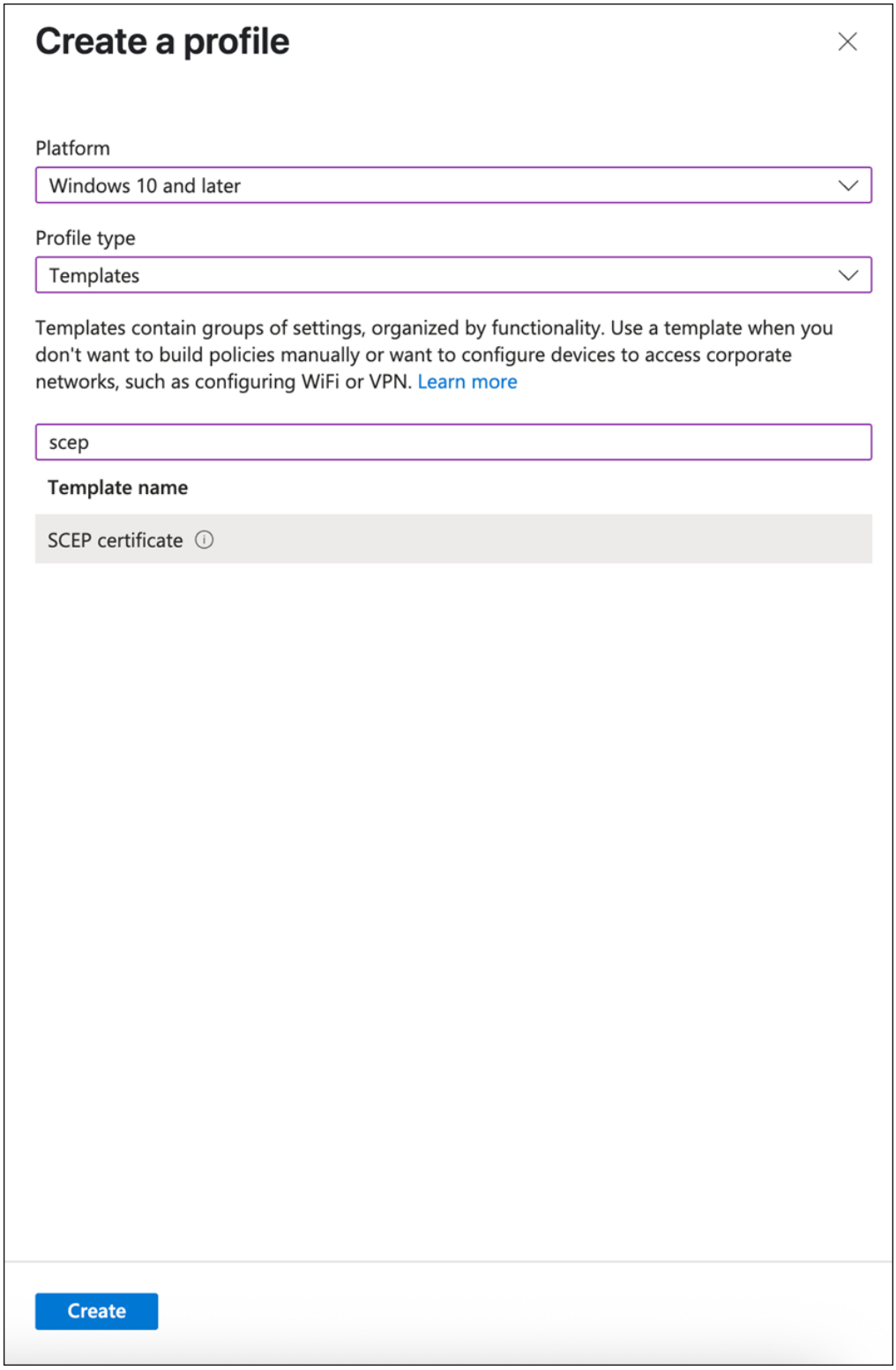

Trusted certificate
Windows 10 and later
1 Basics
2 Configuration settings
3 Assignments
4 Applicability Rules
5 Review + create
Name *
Mist SCEP CA
Description
Platform
Windows 10 and later
Profile type
Trusted certificate
Previous
Next



Create a SCEP Certificate Profile

The SCEP certificate profile instructs the client to obtain a client certificate from the Mist SCEP Service. In this example we use the User Certificate type, but you can follow the same steps for a device certificate.

1. Navigate to **Devices**>**Configuration**, and click **Create**>**New Policy**.
2. Select a platform. We've used Windows 10 and later in this example.
3. Select **Templates** as the Profile Type.
4. Select the **SCEP** from the template list and click **Create**.



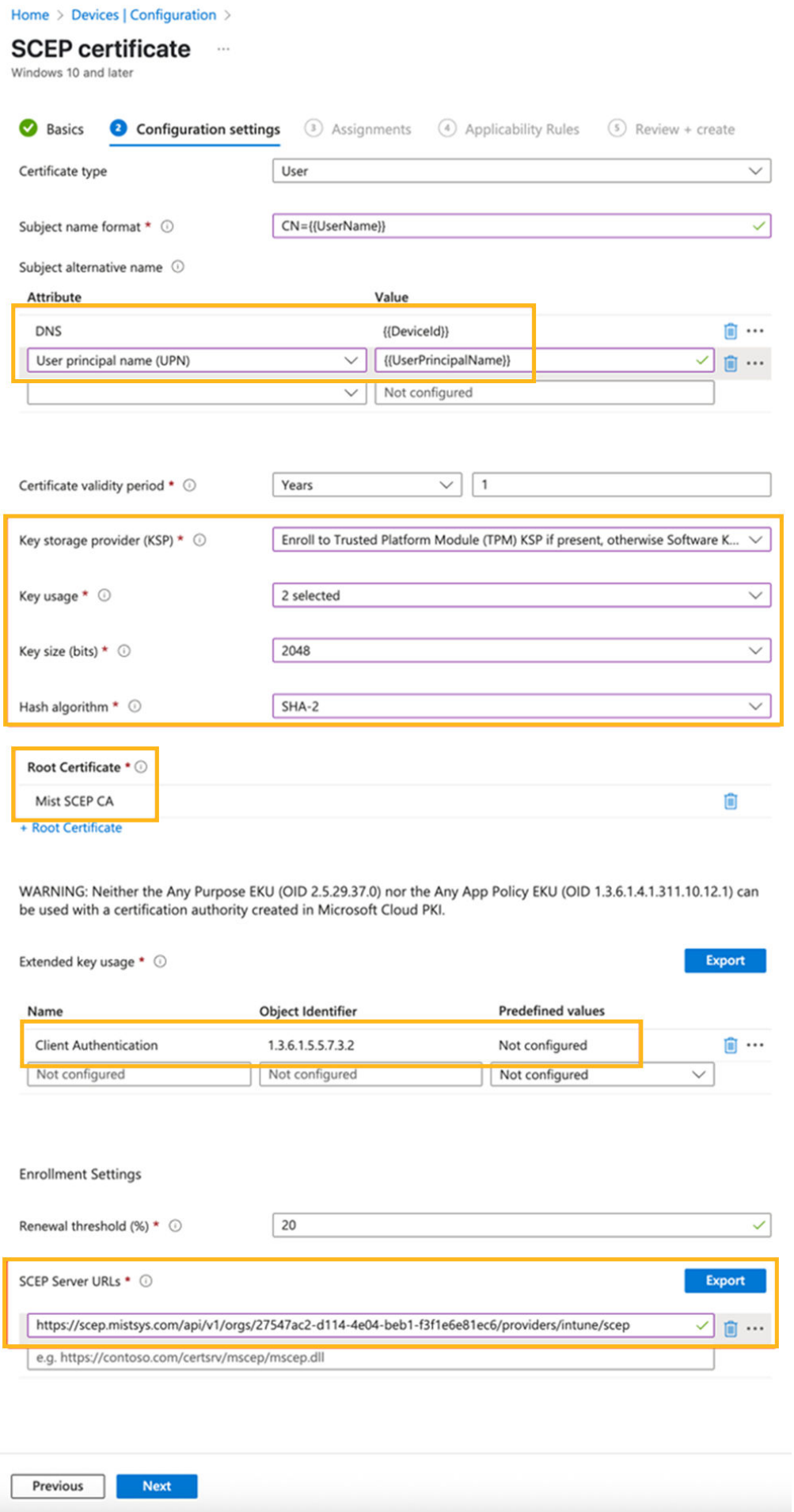
5. Provide a name for the certificate and click **Next**.

6. Enter the configuration settings as shown in the following example. Add the SCEP URL in the **SCEP Server URLs** field.

   Provide the optimal format of the certificate so that the extra information about the user or device can be encoded for NAC to use in policy evaluation. In this example, the Intune Device ID is encoded in the SAN:DNS field, which enables periodic checks for device compliance. The full user principal name is encoded in the SAN:UPN field, which enables group membership lookup against the Entra ID.

   The client will be instructed to trust the Mist SCEP CA Certificate.

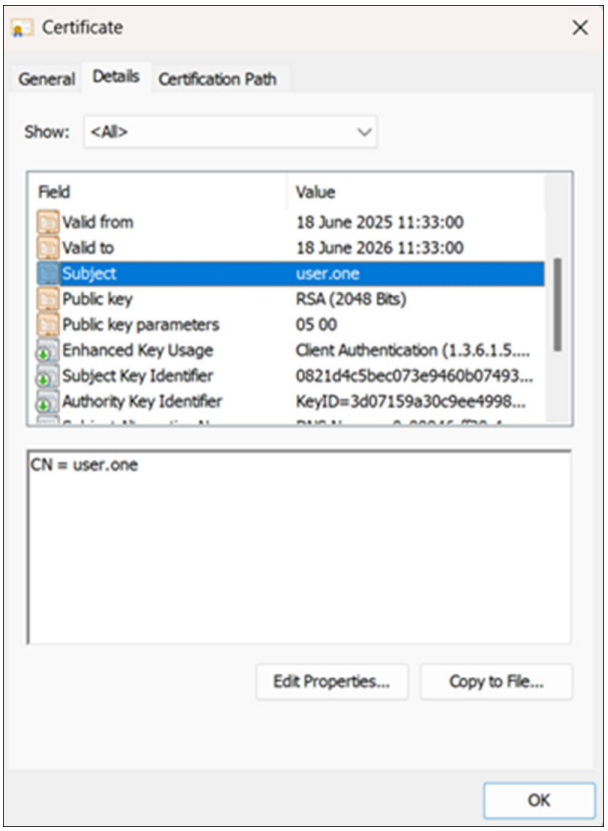
   NOTE:
   Including the Device ID in the SAN:DNS field is mandatory because NAC uses this value for device identification and compliance checks.


Home > Devices | Configuration >
SCEP certificate
Windows 10 and later
Basics
2 Configuration settings
3 Assignments
4 Applicability Rules
5 Review + create
Certificate type
User
Subject name format *
CN={{UserName}}
Subject alternative name
Attribute
Value
DNS
{{DeviceId}}
User principal name (UPN)
{{UserPrincipalName}}
Not configured
Certificate validity period *
Years
1
Key storage provider (KSP) *
Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software K...
Key usage *
2 selected
Key size (bits) *
2048
Hash algorithm *
SHA-2
Root Certificate *
Mist SCEP CA
+ Root Certificate
WARNING: Neither the Any Purpose EKU (OID 2.5.29.37.0) nor the Any App Policy EKU (OID 1.3.6.1.4.1.311.10.12.1) can be used with a certification authority created in Microsoft Cloud PKI.
Extended key usage *
Export
Name
Object Identifier
Predefined values
Client Authentication
1.3.6.1.5.5.7.3.2
Not configured
Not configured
Not configured
Not configured
Enrollment Settings
Renewal threshold (%) *
20
SCEP Server URLs *
Export
https://scep.mistsys.com/api/v1/orgs/27547ac2-d114-4e04-beb1-f3f1e6e81ec6/providers/intune/scep
e.g. https://contoso.com/certsrv/mscep/mscep.dll
Previous
Next

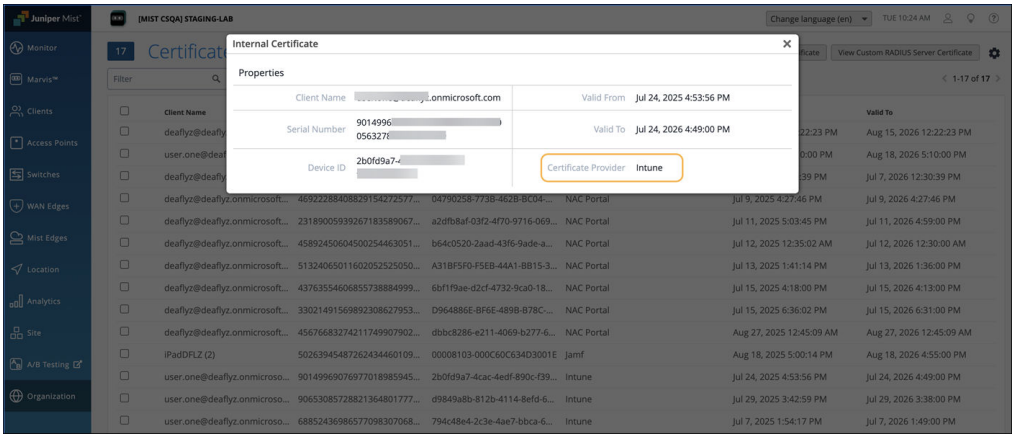
7. Assign this profile to specific user group or all devices.

8. Click **Next** and then click **Create**.

After the profile is pushed to the Windows client, you'll see a new client certificate issued under Personal User Certificate storage:

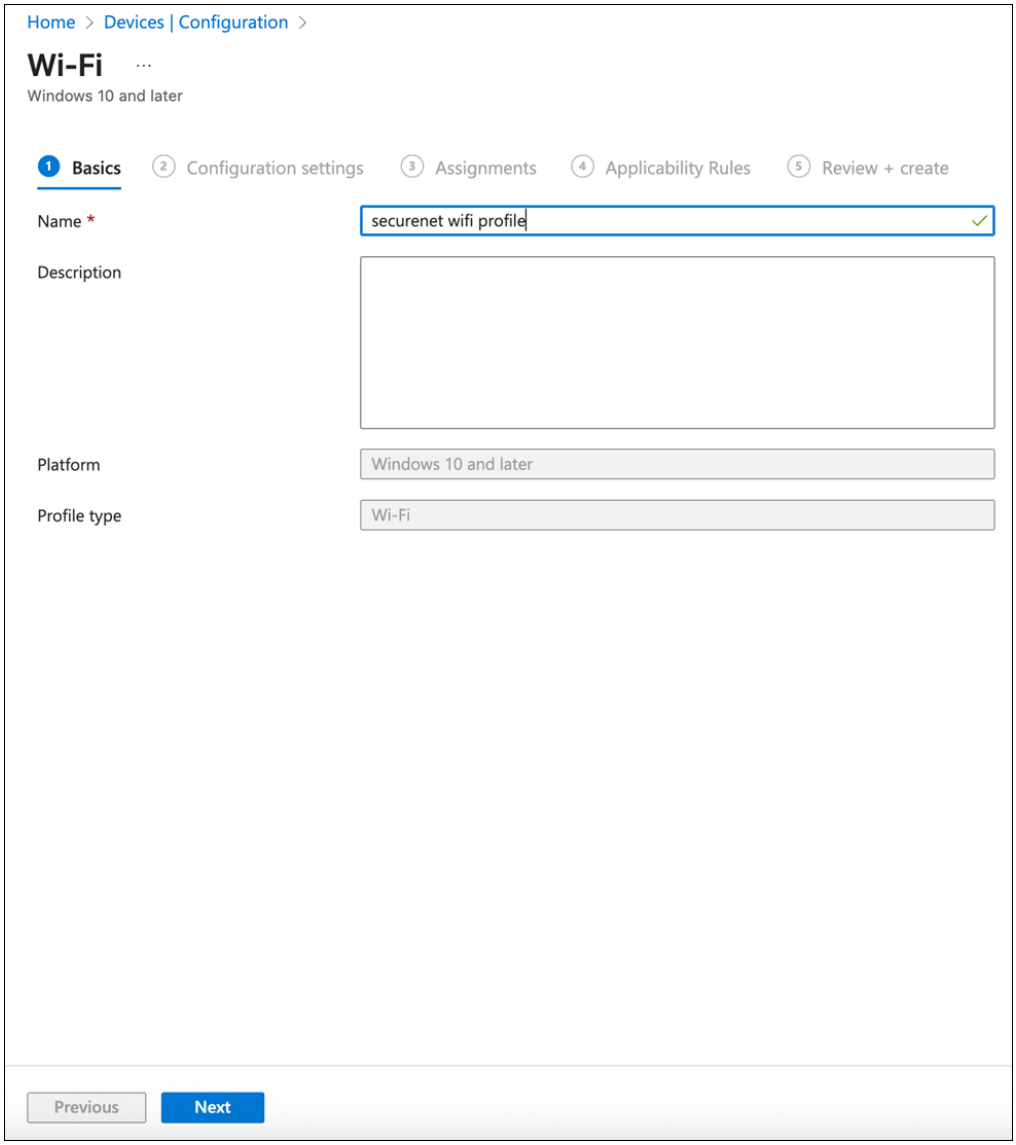


Switch to the Juniper Mist portal and confirm that the client certificate is issued under **Certificates**>**Internal**.



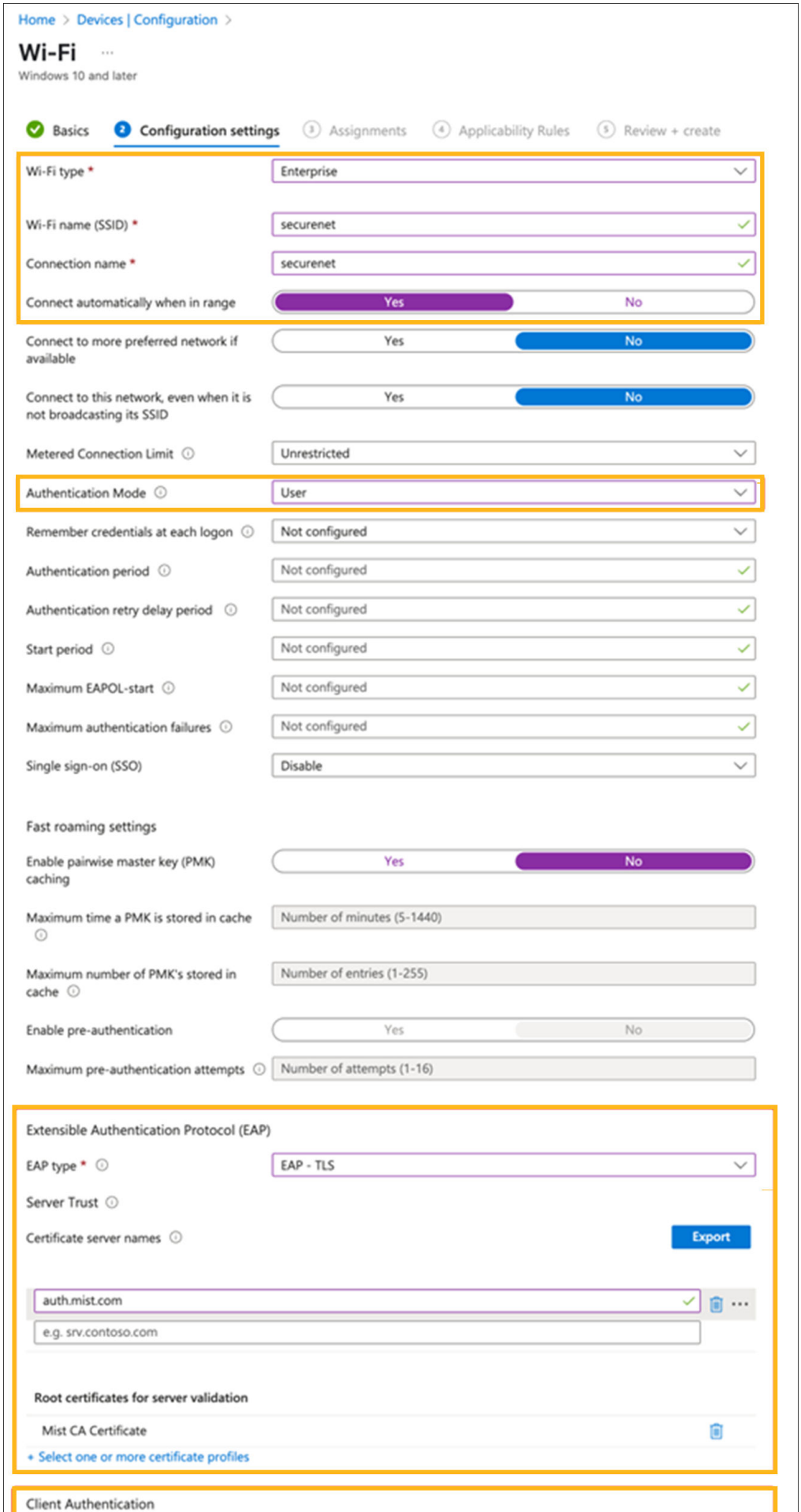
Create a Wi-Fi Profile

1. Navigate to **Devices**>**Configuration**, and click **Create**>**New Policy**.
2. Select a platform. We've used Windows 10 and later in this example.
3. Select **Templates** as the Profile Type.
4. Select **Wi-Fi** from the template list.
5. Provide a name for the certificate and click **Next**.



6. Enter the configuration settings as shown in the following example.
   - Select **Enterprise** as the security type.

- Provide your SSID name.
- Set the correct authentication mode (user and computer, user, or computer) based on the type of SCEP certificate you are providing to the clients.
- Add the Mist CA certificate as the Root Certificate for server (RADIUS) validation.
- Add the SCEP Profile as the Client certificate for client authentication.


Home > Devices | Configuration >
Wi-Fi
Windows 10 and later
Basics
Configuration settings
Assignments
Applicability Rules
Review + create
Wi-Fi type *
Enterprise
Wi-Fi name (SSID) *
securenet
Connection name *
securenet
Connect automatically when in range
Yes
No
Connect to more preferred network if available
Yes
No
Connect to this network, even when it is not broadcasting its SSID
Yes
No
Metered Connection Limit
Unrestricted
Authentication Mode
User
Remember credentials at each logon
Not configured
Authentication period
Not configured
Authentication retry delay period
Not configured
Start period
Not configured
Maximum EAPOL-start
Not configured
Maximum authentication failures
Not configured
Single sign-on (SSO)
Disable
Fast roaming settings
Enable pairwise master key (PMK) caching
Yes
No
Maximum time a PMK is stored in cache
Number of minutes (5-1440)
Maximum number of PMK's stored in cache
Number of entries (1-255)
Enable pre-authentication
Yes
No
Maximum pre-authentication attempts
Number of attempts (1-16)
Extensible Authentication Protocol (EAP)
EAP type *
EAP - TLS
Server Trust
Certificate server names
Export
auth.mist.com
e.g. srv.contoso.com
Root certificates for server validation
Mist CA Certificate
+ Select one or more certificate profiles
Client Authentication

Initiate a device sync from Intune so that the devices can obtain the latest profile updates. The client devices can automatically obtain the digital certificates.

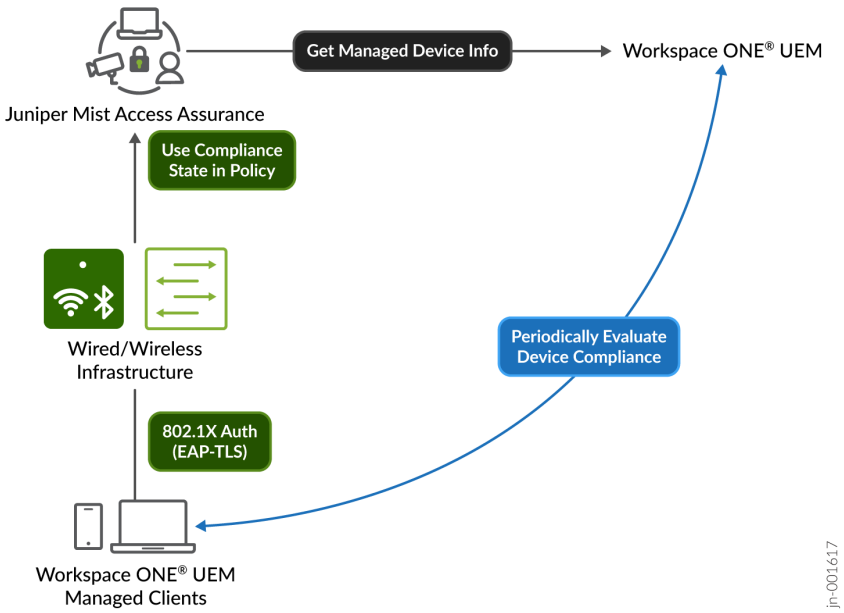
Workspace ONE UEM Integration

SUMMARY

Follow these steps to link a Workspace ONE account to a Juniper Mist organization, and understand how Mist Access Assurance leverages the enrolled device compliance status for policy rule creation.

IN THIS SECTION

Juniper Mist Access Assurance supports native integration with Workspace ONE® UEM, enabling comprehensive evaluation of endpoint compliance across devices such as laptops and mobile phones. Using predefined policies, Workspace ONE assesses device compliance based on security parameters such as antivirus presence, firewall status, and OS patch levels. Juniper Mist Access Assurance retrieves the latest device compliance status from Workspace ONE and applies it to authentication policies to enforce access control decisions.



Device Compliance Status Data Retrieval from Workspace ONE

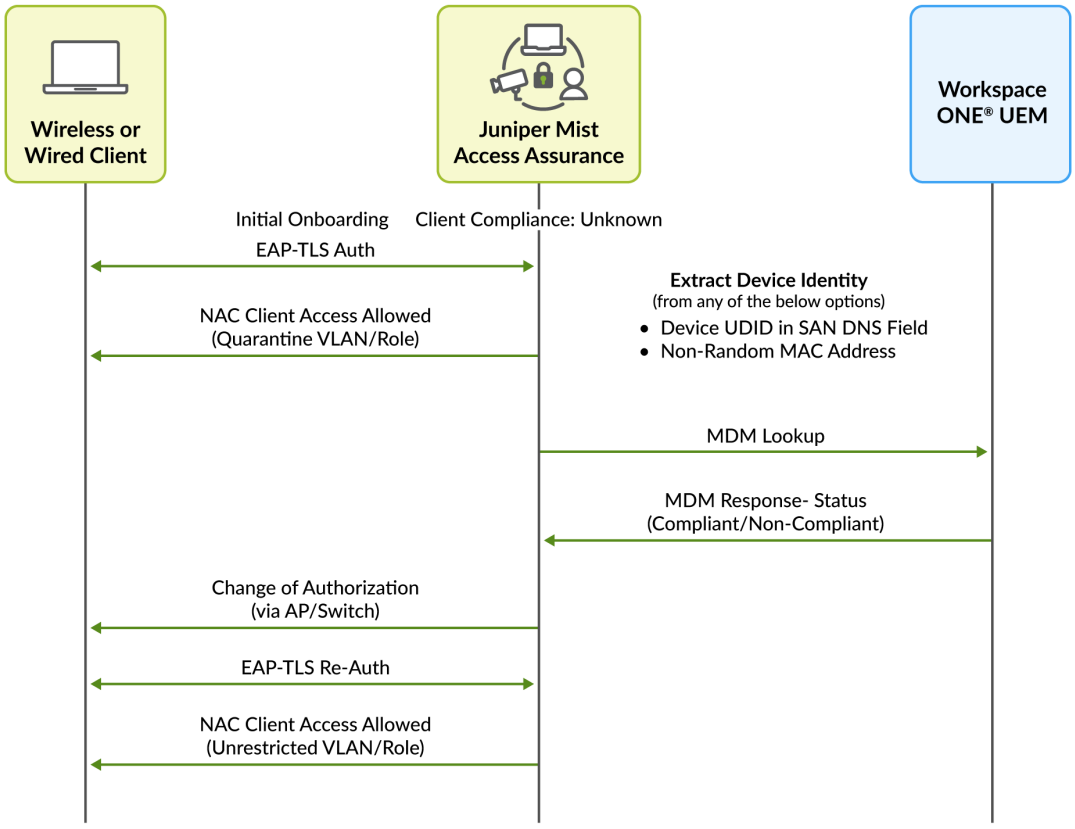
Juniper Mist Access Assurance uses an API-based polling mechanism to query Workspace ONE every two hours for each managed client that has been authenticated. The compliance status information is cached for quick retrieval.

To prevent any additional delays, the compliance information is retrieved after the authentication process is complete. After the initial onboarding of a device is complete, its compliance status is refreshed every 2 hours.

If a device's compliance state changes, Juniper Mist Access Assurance automatically triggers a Change of Authorization (CoA) to re-evaluate the policy and enforce the appropriate access control measures. This automatic triggering of CoA ensures that compliance changes are promptly addressed, maintaining security and policy adherence without requiring manual intervention.

Figure 36 on page 116 illustrates how Juniper Mist Access Assurance retrieves Workspace ONE-managed device compliance data for authentication.

Figure 36: Authentication and Authorization Process for Workspace ONE

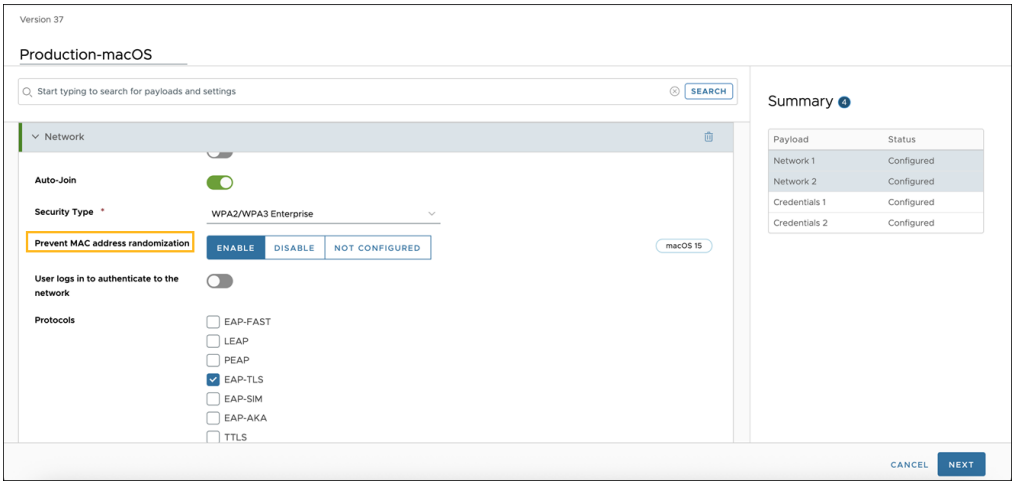


NOTE: To support the CoA functionality, APs must run firmware version 0.14 or later

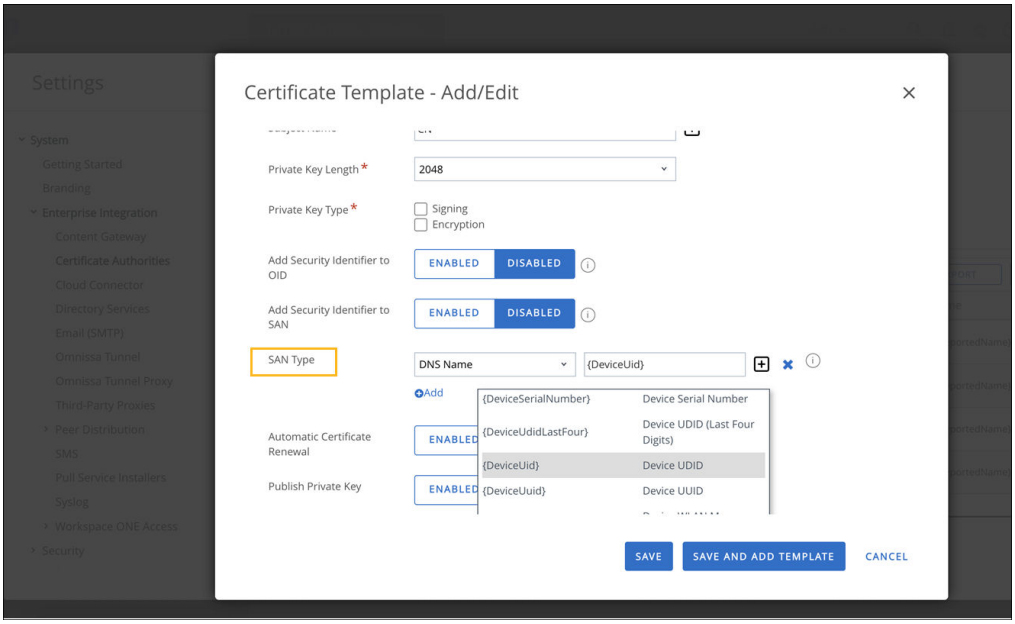
Juniper Mist Access Assurance uses the following information during client authentication to match a client with a device record in Workspace ONE:

NOTE: Some of the screenshots included in this topic are sourced from third-party applications. Be aware that these screenshots might change over time and might not always match the current version of the applications.

- **Non-randomized MAC address**—For authentication using EAP-TTLS or EAP-TLS, the MAC address of the client device is matched against a managed device record in Workspace ONE. To ensure accurate MAC-based device matching, you must disable MAC address randomization in the Wi-Fi configuration profiles on client devices.



- **Workspace ONE UDID encoded in SAN:DNS certificate attribute**—In Workspace ONE Certificate templates, use the **{DeviceUid}** variable to encode the Device UDID in the SAN:DNS certificate field.

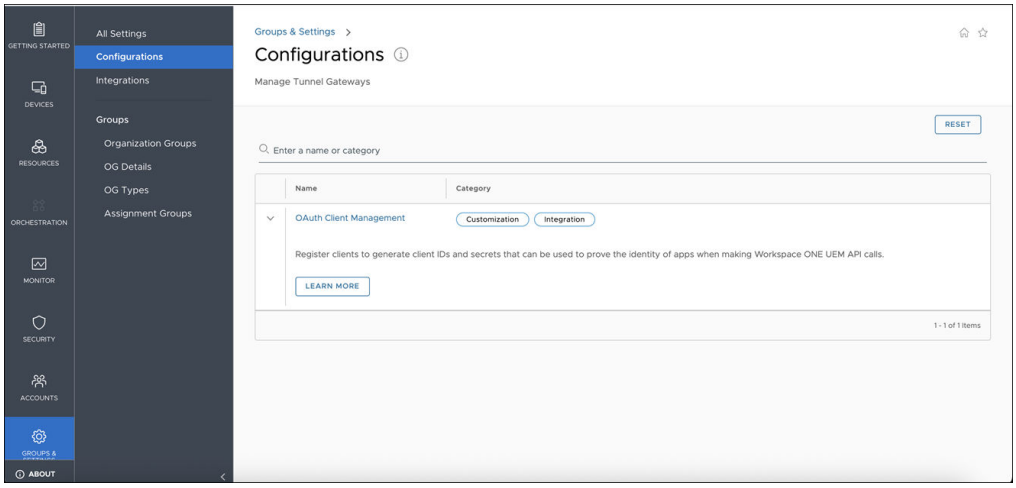


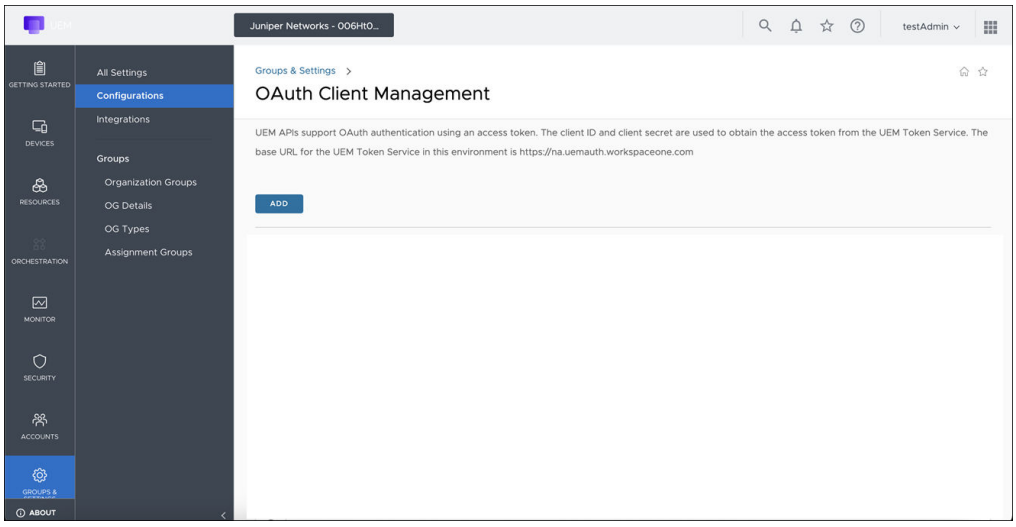
Configure Client ID and Client Secret in Workspace ONE

To integrate Workspace ONE with Juniper Mist Access Assurance, you'll need to set up a Workspace ONE API Client ID and Client Secret.

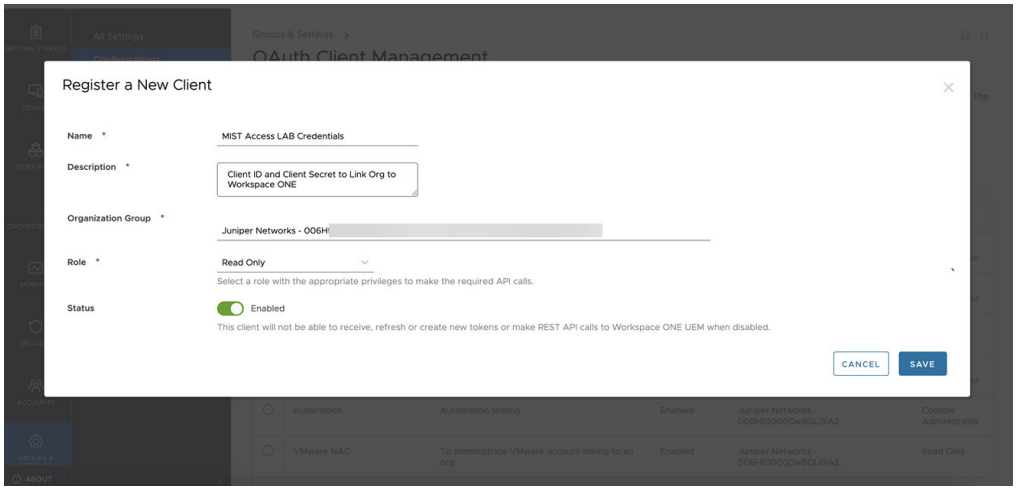
NOTE: The screenshots from third-party applications are correct at the time of publishing. We have no way to know when or if the screenshots will be accurate at any future time. Please refer to the third-party website for guidance about changes to these screens or the workflows involved.

1. In the Workspace ONE portal, navigate to **Groups & Settings**> **Configurations**>**OAuth Client Management**, then click **Add**.

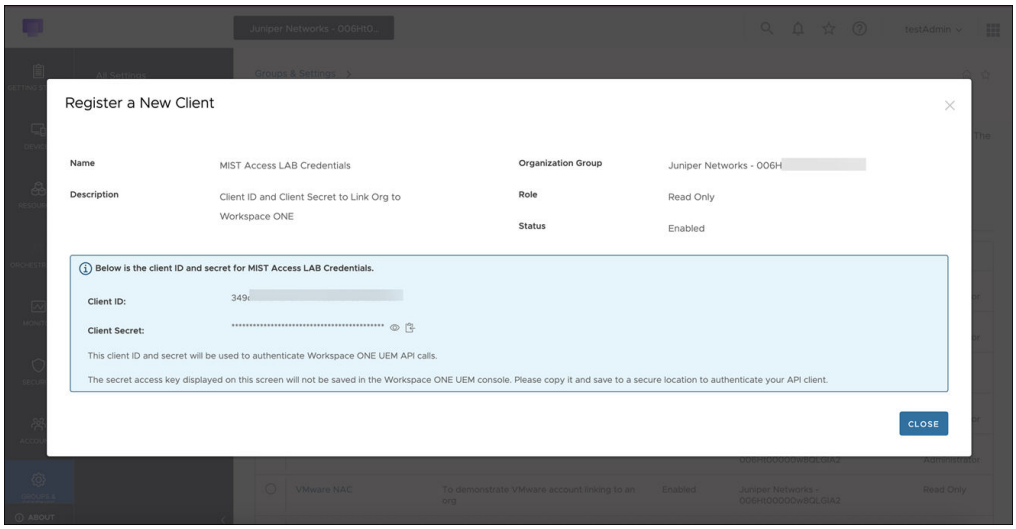




2. Enter the required details to create a Client ID. Ensure that the role is set to **Read Only** and the status is **Enabled**, as shown in the following example. Click **Save**.



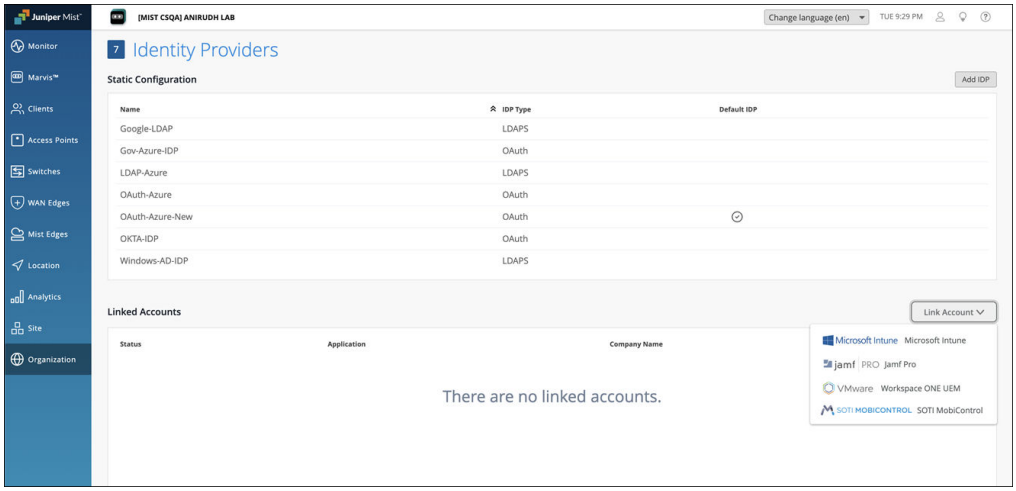
3. Copy the generated Client ID and Client Secret. These credentials are required to link your Mist organization with Workspace ONE.



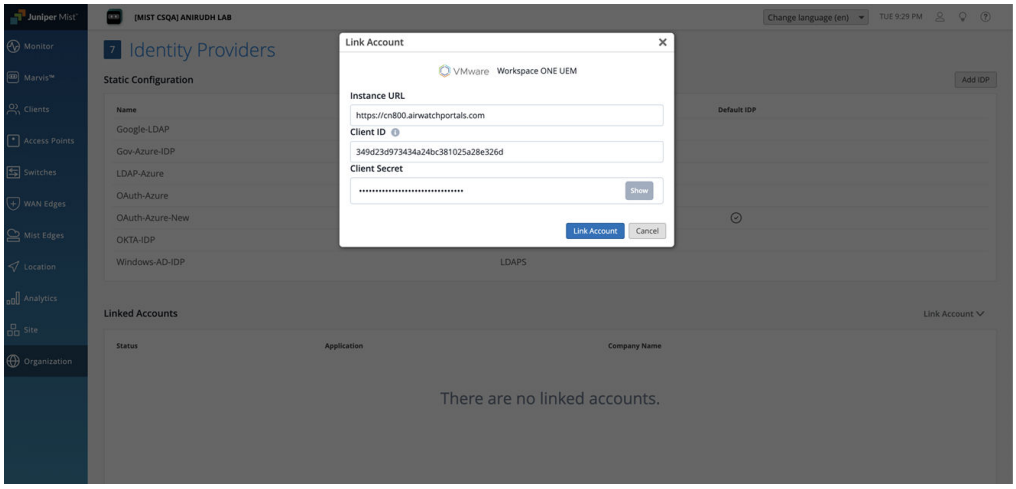
Link Workspace ONE to the Mist Portal

To link Workspace ONE with the Mist Portal:

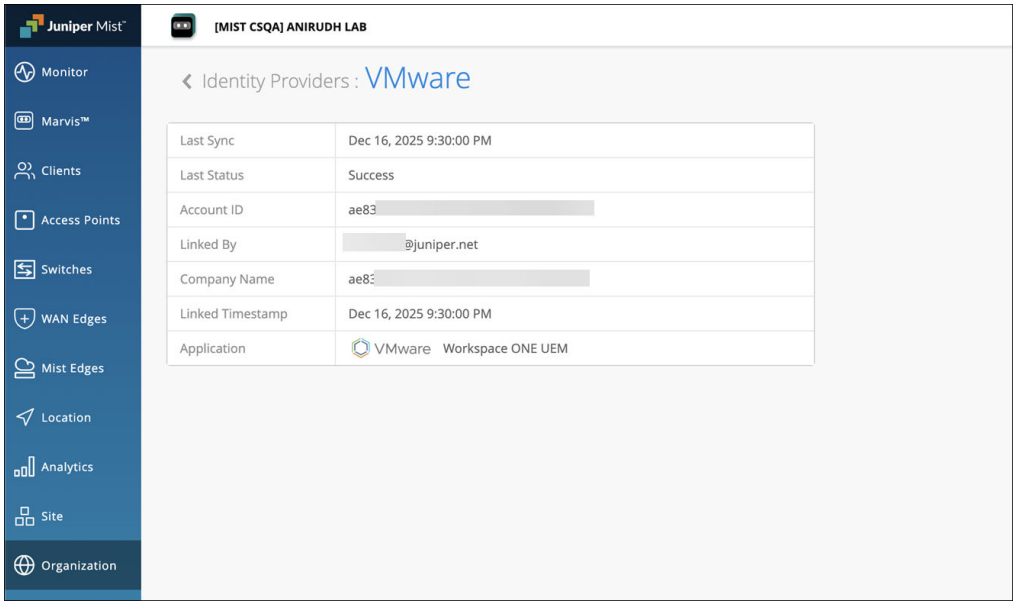
1. From the left menu of the Juniper Mist portal, select **Organization**> **Access**>**Identity Providers**.
2. In the Linked Accounts section, click **Link Account**.
3. Select **VMware Workspace ONE UEM**.



4. In the Link Account page, provide the Instance URL (for example, https://ABC.awmdm.com OR https://ABC.airwatchportals.com), Client ID and Client Secret. Then, click **Link Account**.



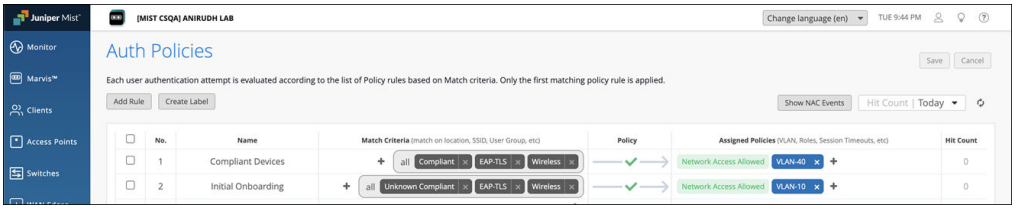
After you link the Workspace ONE account, you can see the account status on the Identity Providers page. You can click the account to view the details of the last sync.



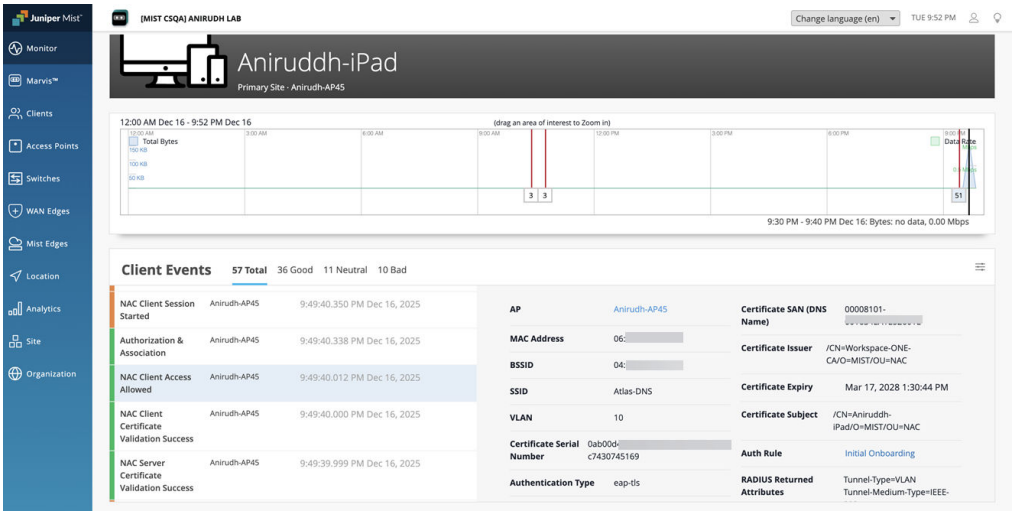
Verify Client Connection and Device Lookup Status

The initial MDM lookup for a new client occurs after the device has been authenticated for the first time. To facilitate this lookup, you'll need to create an auth rule that allows first-time device connections and assigns the devices to a quarantine VLAN.

NOTE: Do not include the **Compliant** or **Non-Compliant** MDM compliance labels in the match conditions for this rule. You can optionally use the **Unknown Compliant** label as a match criterion. Ensure this rule is placed at a lower priority than your standard access policies.

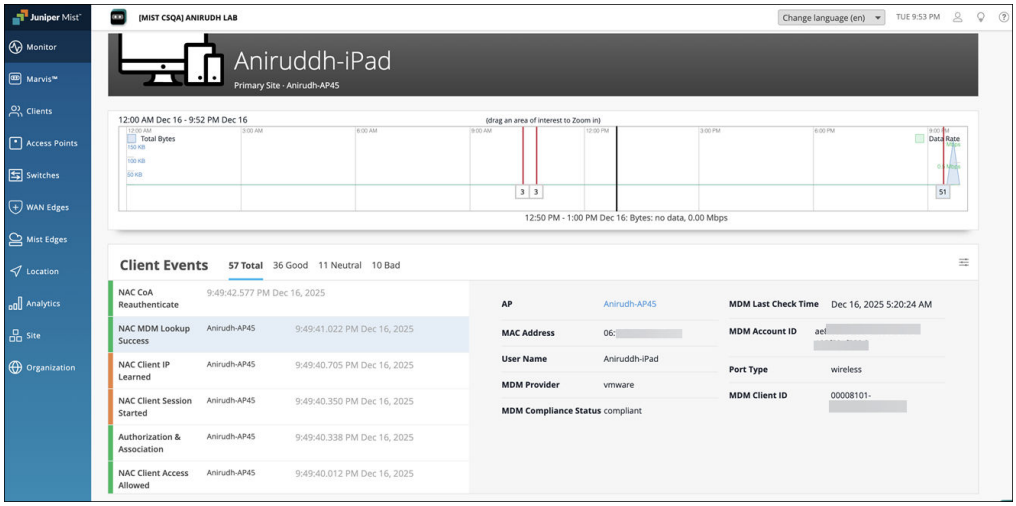


When the client is connected, you'll see the NAC Client Access Allowed event on the Insights page.

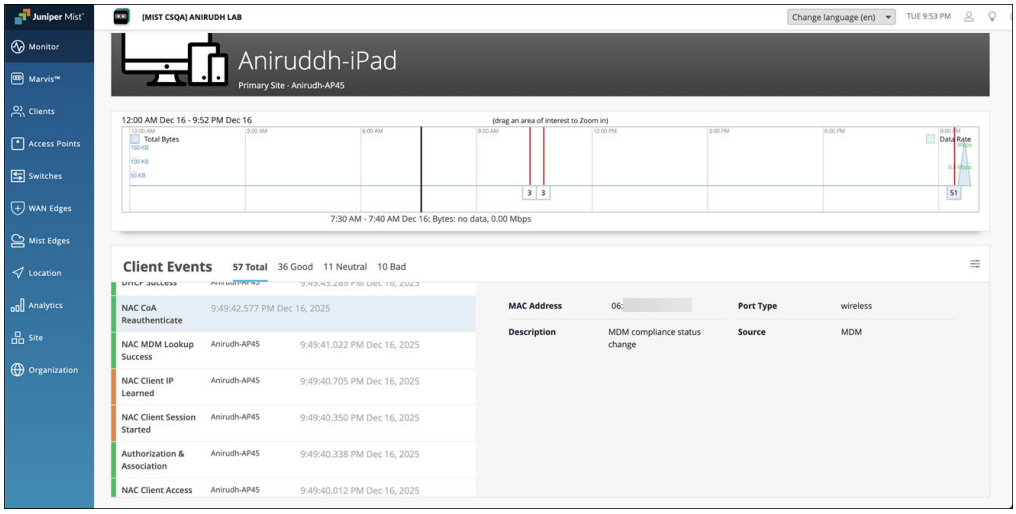


After the client connects, Juniper Mist Access Assurance:

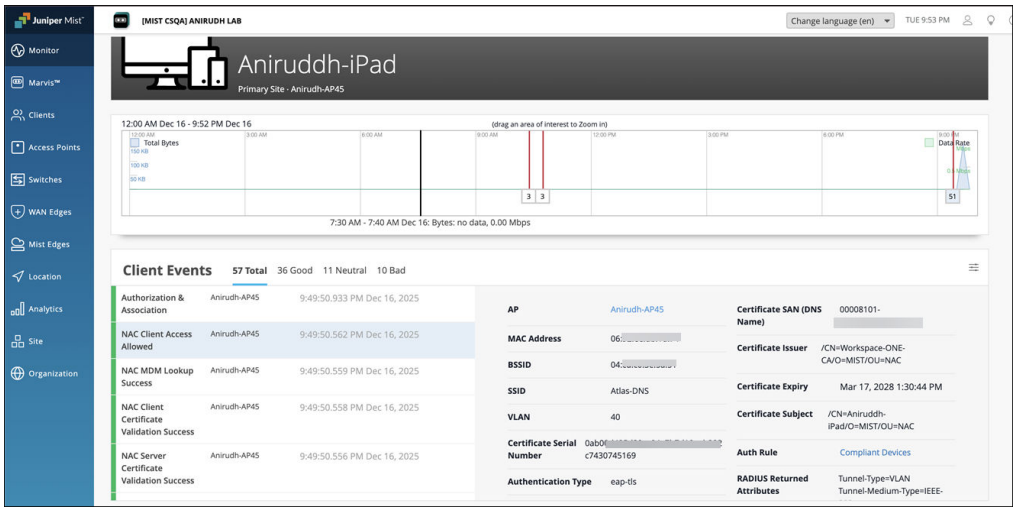
1. Retrieves the device's compliance status from Workspace ONE.



2. Triggers a Change of Authorization (CoA) to reauthenticate the client.



3. On re-authentication, the client is matched against the appropriate policy based on its updated compliance status.



For all subsequent authentications, Juniper Mist Access Assurance uses the cached MDM data, which is automatically refreshed every two hours to capture any compliance changes.

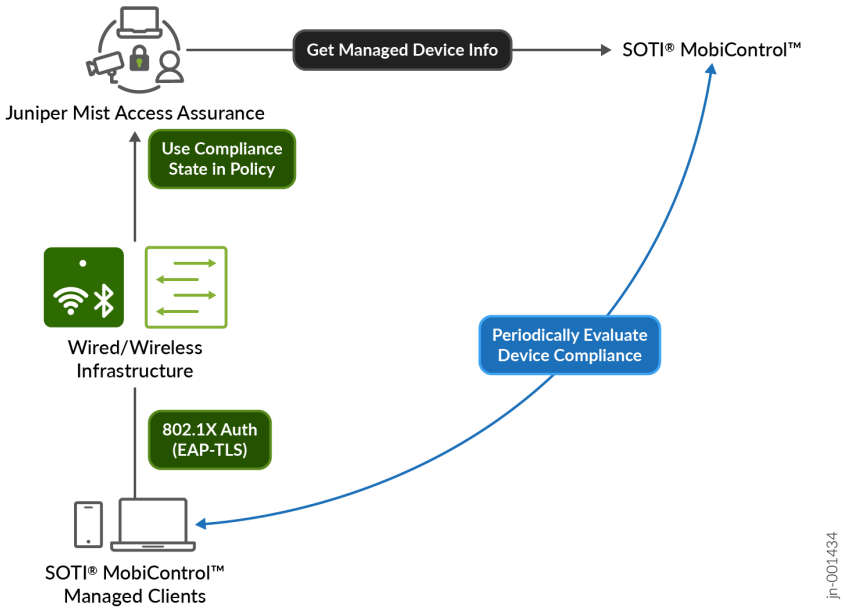
SOTI MobiControl Integration

SUMMARY

Follow these steps to understand SOTI MobiControl integrations, link your SOTI MobiControl account to your Juniper Mist organization, create policy rules, and view client events.

IN THIS SECTION

Juniper Mist Access Assurance supports native integration with SOTI MobiControl, enabling comprehensive evaluation of endpoint compliance across devices such as laptops and mobile phones. Using predefined policies, SOTI MobiControl assesses device compliance based on security parameters such as antivirus presence, firewall status, and OS patch levels. Juniper Mist Access Assurance retrieves the latest device compliance status from SOTI MobiControl and applies it to authentication policies to enforce access control decisions.



Compliance Data Retrieval from SOTI MobiControl

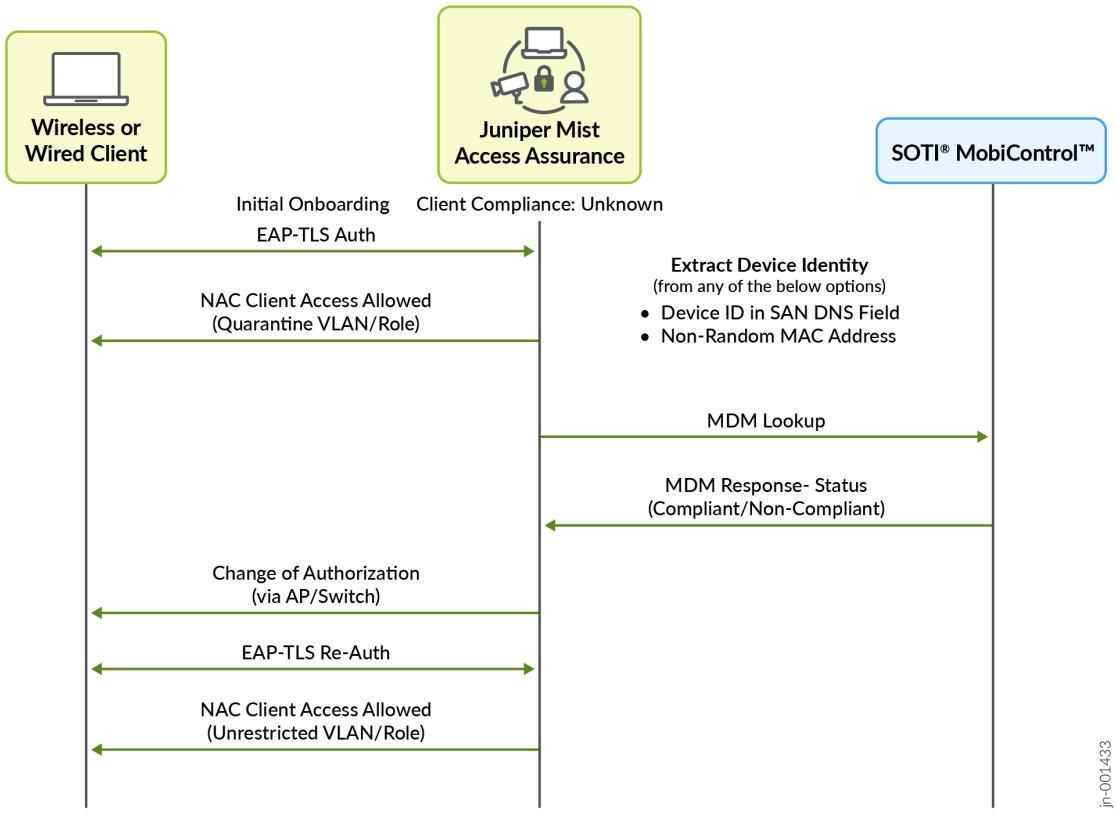
Juniper Mist Access Assurance uses an API-based polling mechanism to query SOTI MobiControl every two hours for each managed client that has been authenticated. The compliance status information is cached for quick retrieval.

To prevent any additional delays, the compliance information is retrieved after the authentication process is complete. After the initial onboarding of a device is complete, its compliance status is refreshed every 2 hours.

If a device's compliance state changes, Juniper Mist Access Assurance automatically triggers a Change of Authorization (CoA) to re-evaluate the policy and enforce the appropriate access control measures. This automatic triggering of CoA ensures that compliance changes are promptly addressed, maintaining security and policy adherence without requiring manual intervention.

Figure 37 on page 126 illustrates how Juniper Mist Access Assurance retrieves SOTI MobiControl-managed device compliance data for authentication.

Figure 37: Authentication and Authorization Process for SOTI MobiControl

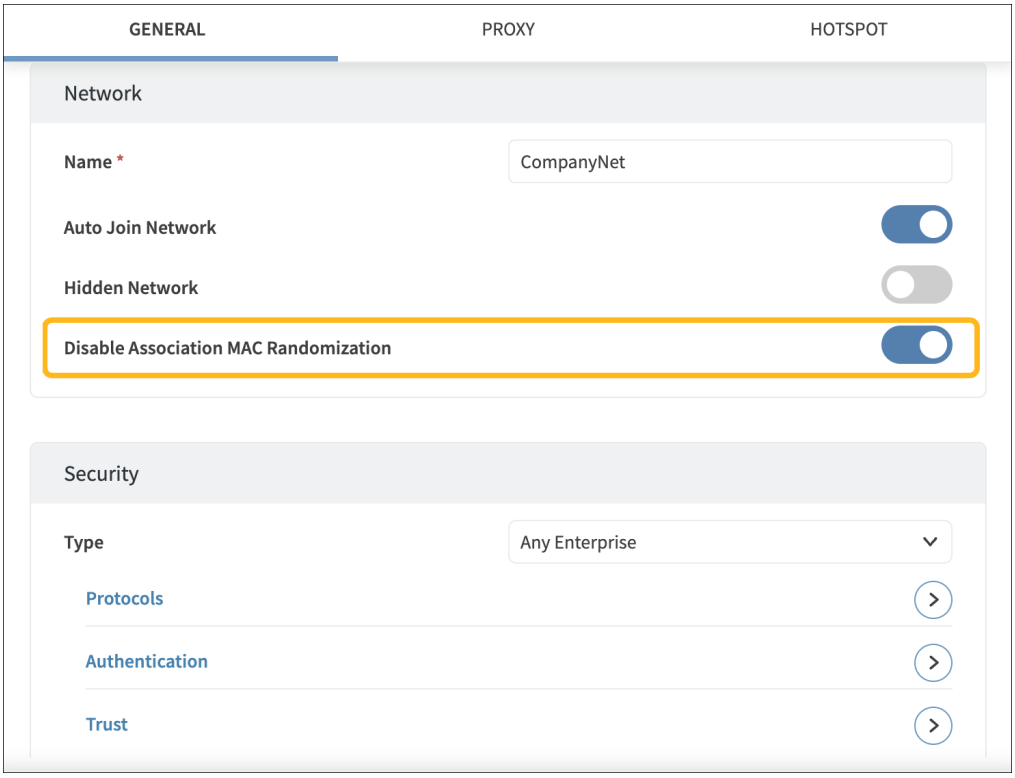


NOTE: To support the CoA functionality, APs must run firmware version 0.14 or later

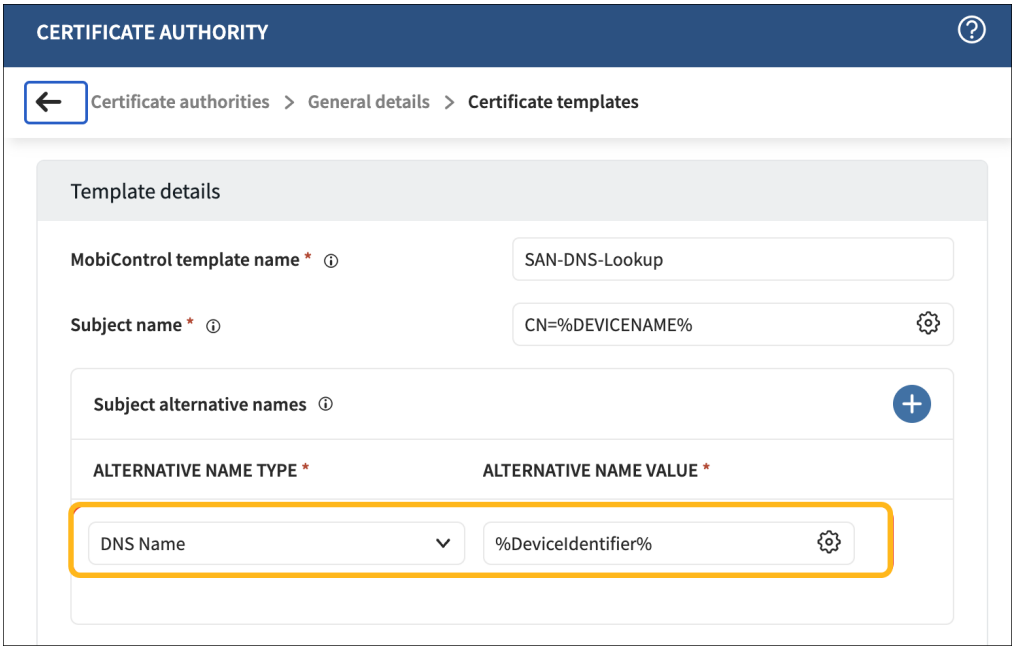
Juniper Mist Access Assurance uses the following information during client authentication to match a client with a device record in SOTI MobiControl:

NOTE: Some of the screenshots included in this topic are sourced from third-party applications. Be aware that these screenshots might change over time and might not always match the current version of the applications.

- **Non-randomized MAC address**—For authentication using EAP-TTLS or EAP-TLS, the MAC address of the client device is matched against a managed device record in SOTI MobiControl. To ensure accurate MAC-based device matching, you must disable MAC address randomization in the Wi-Fi configuration profiles on client devices. At the time of this writing, SOTI MobiControl supports disabling MAC address randomization in Wi-Fi configuration profiles for only iOS and Android devices.



- **SOTI MobiControl Device ID encoded in SAN:DNS certificate attribute**—In SOTI MobiControl Certificate templates, use the **%DeviceIdentifier%** variable to encode the Device ID in the SAN:DNS certificate field.

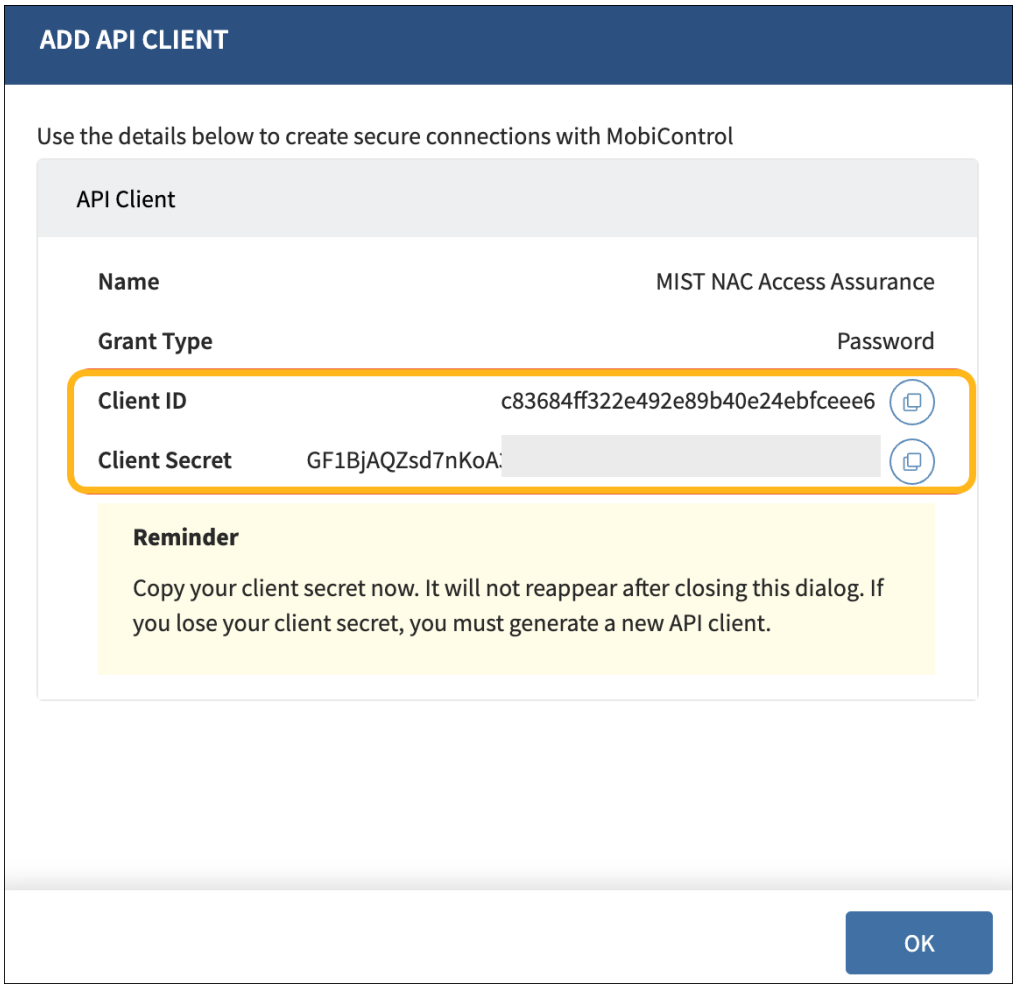


Configure SOTI MobiControl

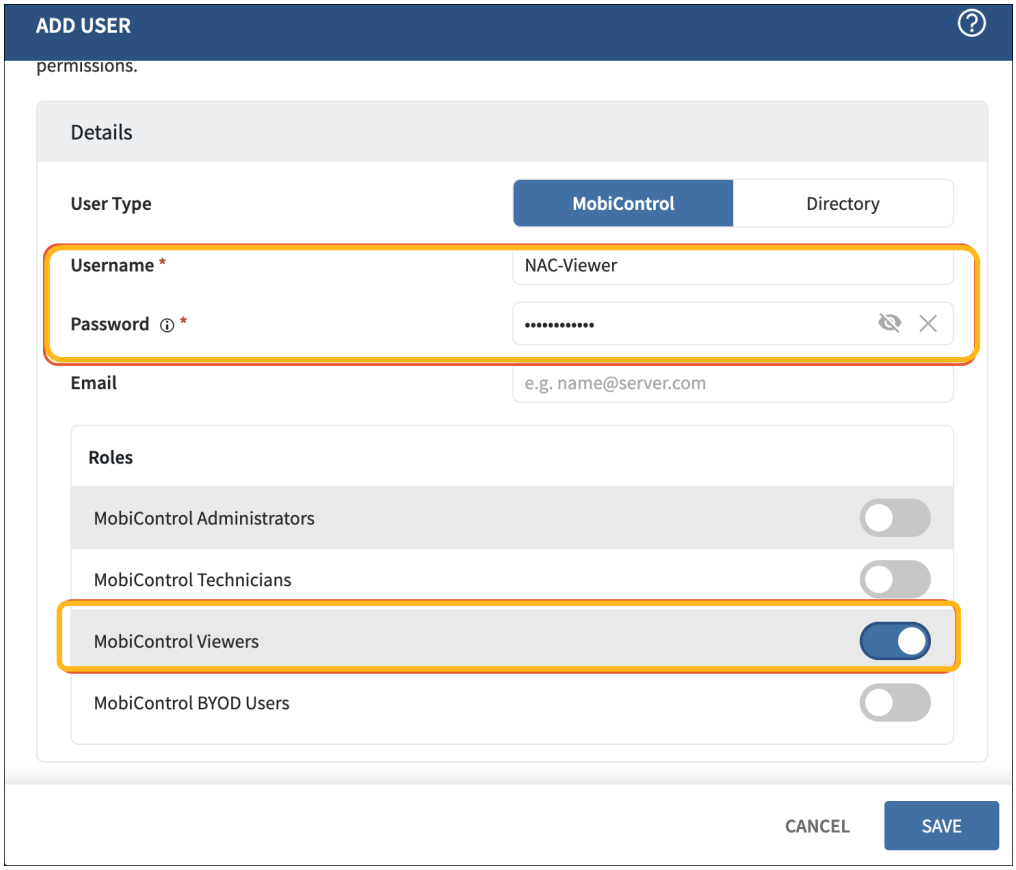
To integrate SOTI MobiControl with Juniper Mist, you'll need to set up a SOTI MobiControl API client ID.

> **NOTE**: The screenshots from third-party applications are correct at the time of publishing. We have no way to know when or if the screenshots will be accurate at any future time. Please refer to the third-party website for guidance about changes to these screens or the workflows involved.

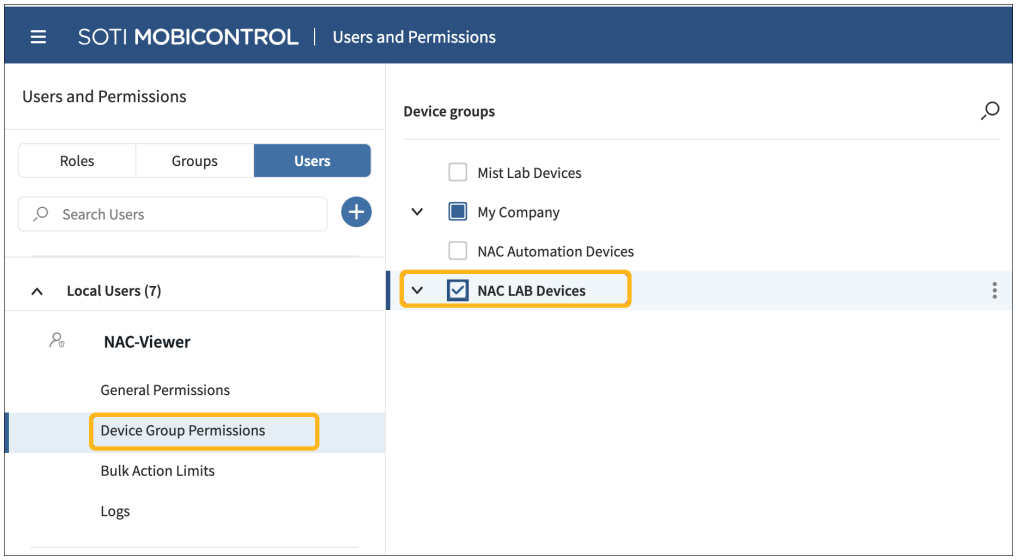
1. In SOTI MobiControl, navigate to **Global Settings**>**Services API Client**. Click **+** to generate a new Client ID and Client Secret. Copy these values.



2. Create user credentials with view-only access for the MobiControl WebConsole. Navigate to **Users and Permissions** > **Users** and click **+** to add a user.



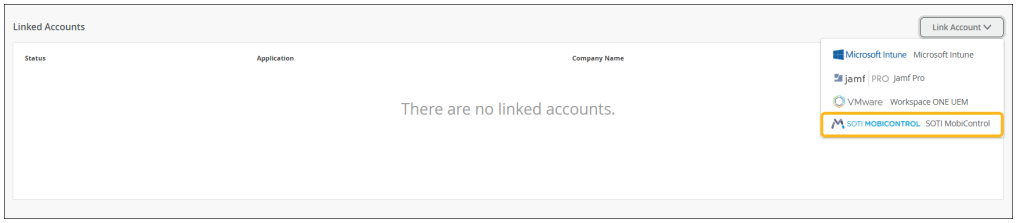
3. Ensure that the user has access to the device group where the devices will be enrolled.



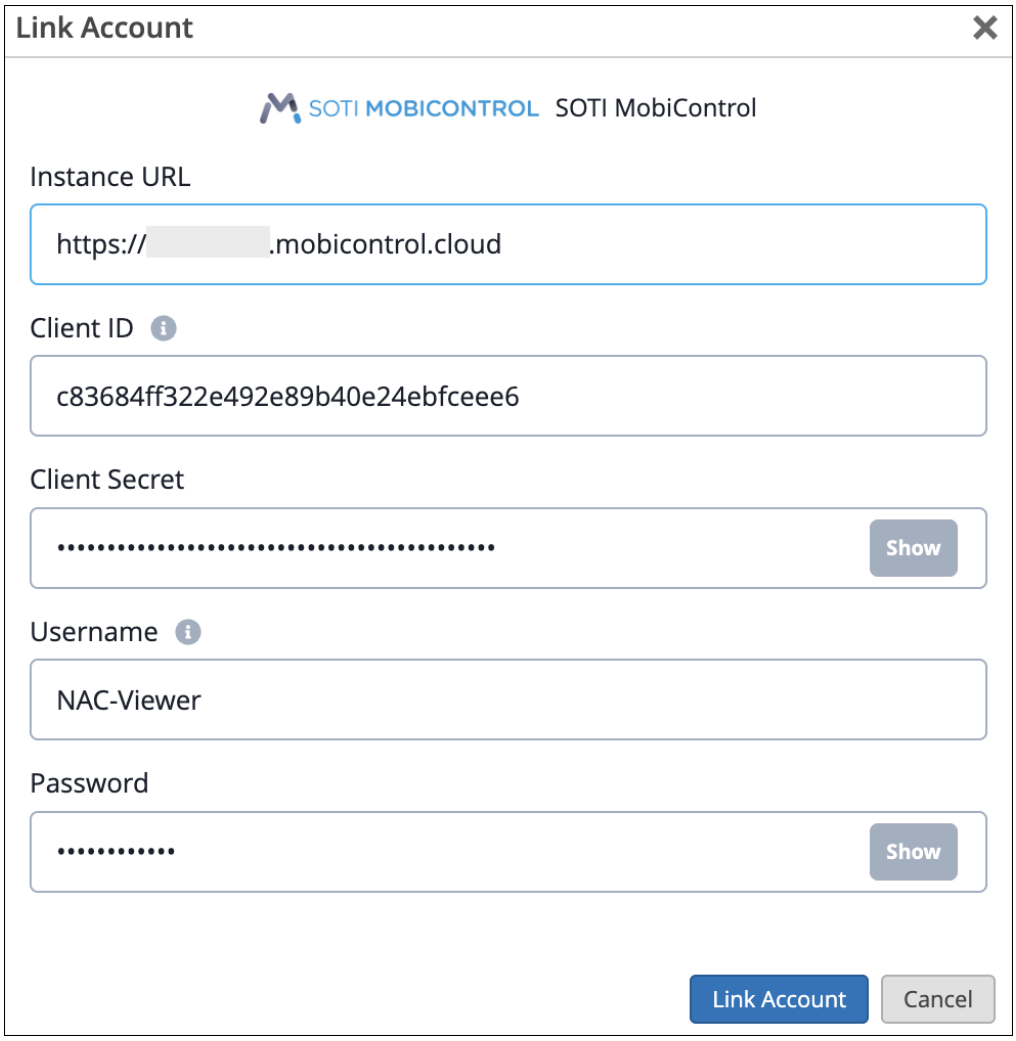
Add SOTI MobiControl to the Juniper Mist Portal

To add SOTI MobiControl to the Juniper Mist 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**.

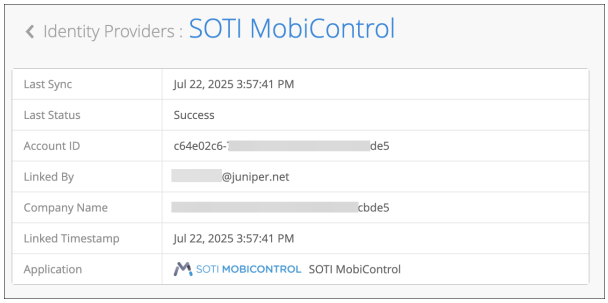


3. Select **SOTI MobiControl**.
4. In the Link Account page, provide the Client ID, Client Secret, Username, Password and SOTI MobiControl Instance URL (for example, https://ABC.mobicontrol.cloud).



After linking the SOTI MobiControl account, you can see the SOTI MobiControl account status on the Identity Providers page.

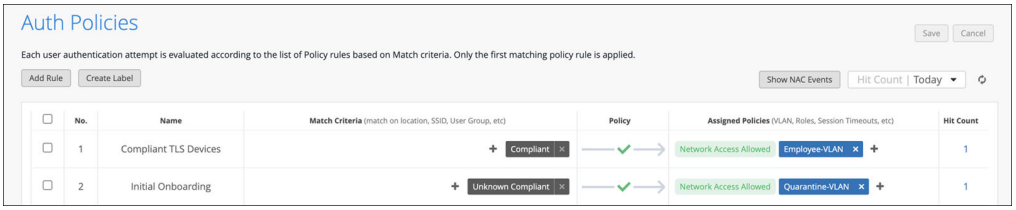
You can click the account to view the details of the last sync.



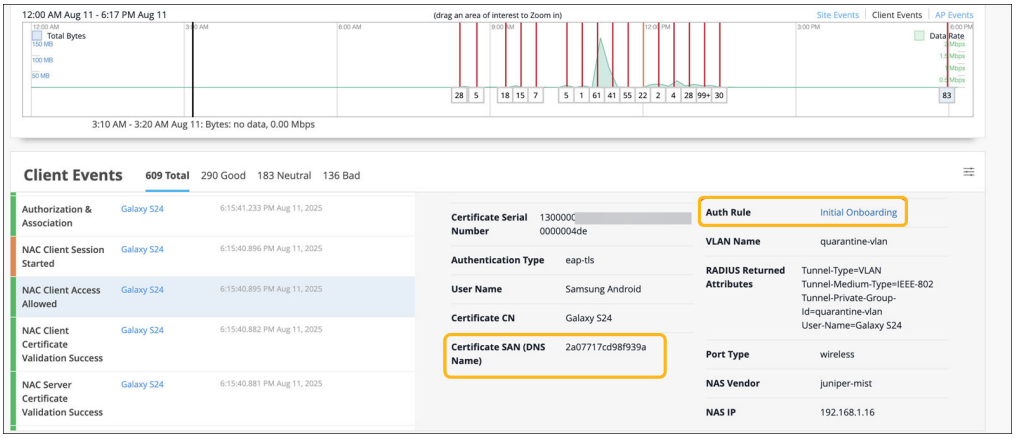
Verify SOTI MobiControl

The initial MDM lookup for a new client occurs after the device has been authenticated for the first time. To facilitate this lookup, you'll need to create an auth rule that allows first-time device connections and assigns the devices to a quarantine VLAN.

NOTE: Do not include the **Compliant** or **Non-Compliant** MDM compliance labels in the match conditions for this rule. You can optionally use the **Unknown Compliant** label as a match criterion. Ensure this rule is placed at a lower priority than your standard access policies.

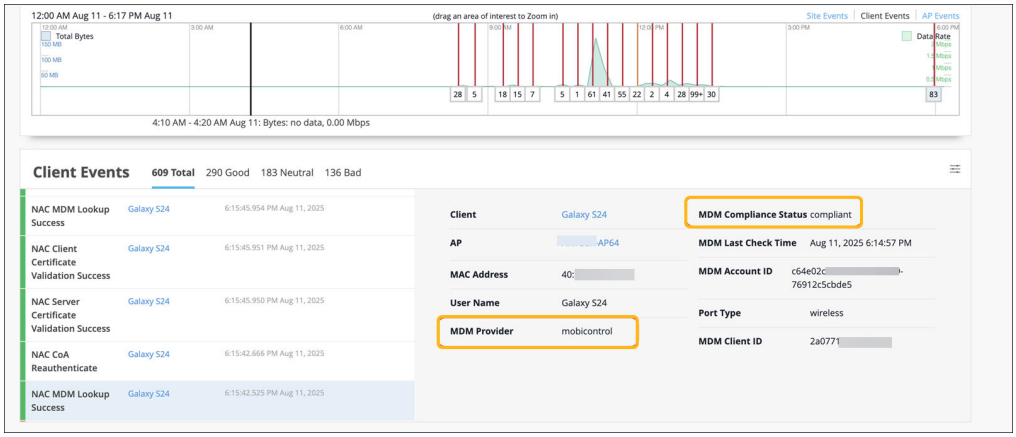


When the client is connected, you'll see the NAC Client Access Allowed event in the Insights page.

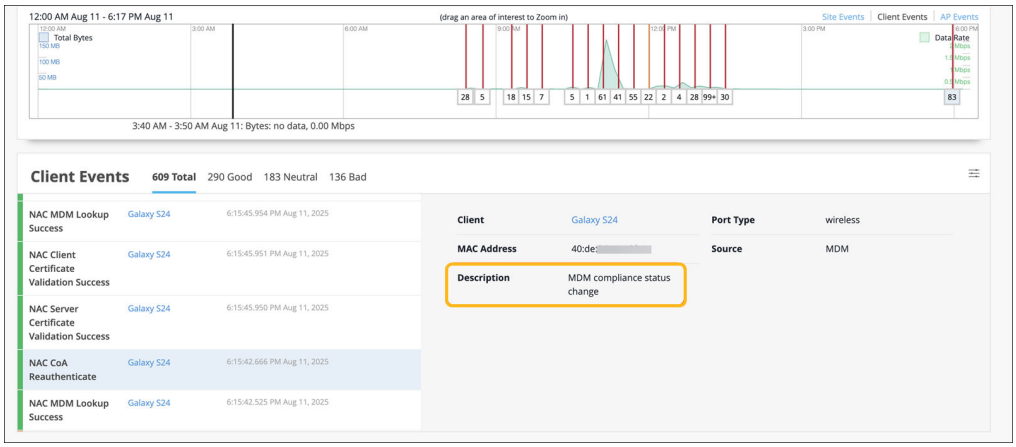


After the client connects, Juniper Mist Access Assurance:

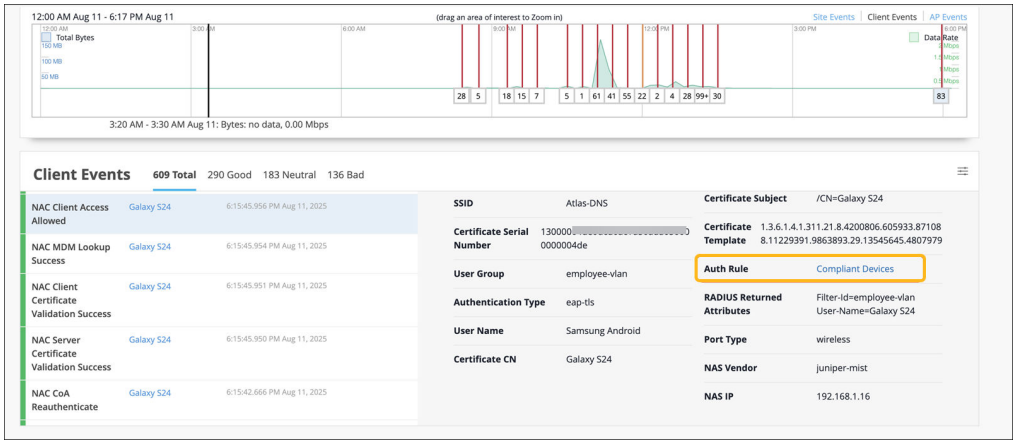
1. Retrieves the device's compliance status from SOTI MobiControl



2. Triggers a Change of Authorization (CoA) to reauthenticate the client



3. On re-authentication, the client is matched against the appropriate policy based on its updated compliance status.



For all subsequent authentications, Juniper Mist Access Assurance uses the cached MDM data, which is automatically refreshed every two hours to capture any compliance changes.

CHAPTER 3

Access Assurance Settings

IN THIS CHAPTER

Use Digital Certificates

SUMMARY

Follow these steps to generate and use certificates for the RADIUS server that is integrated with Juniper Mist Access Assurance for each organization.

IN THIS SECTION

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 identity 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.

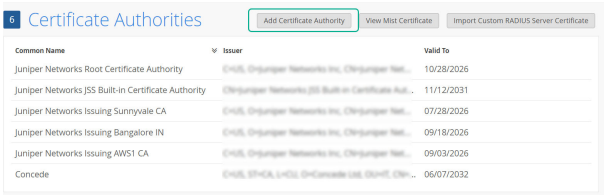
You can obtain the certificate from an external CA. The CA can be a well-known, public CA or an enterprise CA.

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

Video: Certificate Creation for Lab-Testing Use

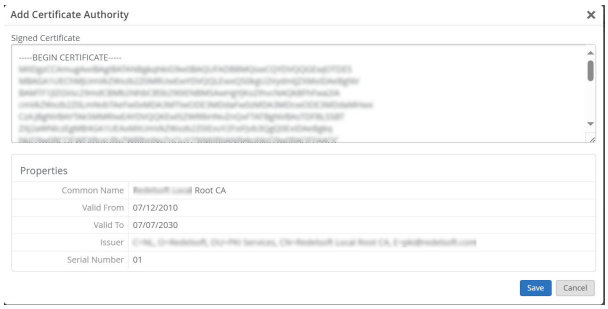
To add a CA certificate:

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**.



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

Figure 38: 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 39 on page 137.

Figure 39: Server Certificate Issued by Mist Access Assurance

Subject

RDN	Value
Common Name (CN)	auth.mist.com
Organizational Unit (OU)	
Organization (O)	Mist
Country (C)	US

Properties

Property	Value
Issuer	CN = ,OU = OrgCA,O = Mist,C = US
Subject	CN = auth.mist.com,OU = ,O = Mist,C = US
Valid From	1 Dec 2022, midnight
Valid To	1 Aug 2023, midnight
Serial Number	
CA Cert	No
Key Size	4096 bits
Fingerprint (SHA-1)	
Fingerprint (MD5)	
SANS	auth.mist.com

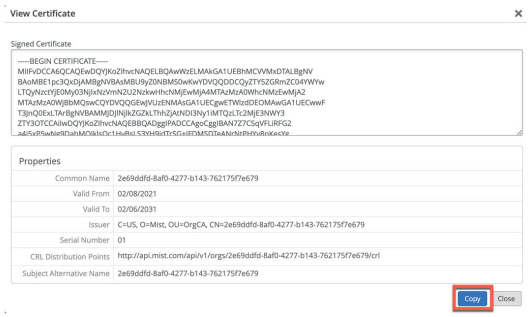
On the client side, you must configure client devices to trust the Mist CA certificate and optionally validate server certificate name as **auth.mist.com**.

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 40: View and Copy Mist Certificate



3. Store the content of the certificate on your local machine and add the extension **.crt** or **.cer** in the file name. For example: **mymistorgca.crt**.
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.

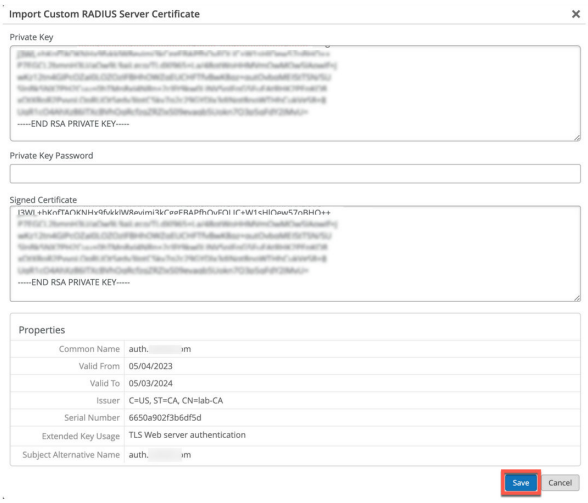
To upload your certificate to the Juniper Mist portal:

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 41: Import Custom RADIUS Server Certificate

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

Figure 42: Enter Custom Server Certificate Details



- **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 | **164**

Juniper Mist Access Assurance Use Cases | **6**

Juniper Mist Access Assurance Authentication Methods | **8**

Configure Authentication Policy | **141**

Configure Authentication Policy Labels | **144**

Configure Authentication Policy

SUMMARY

Create authentication policies to control which users can access which resources on your network.

IN THIS SECTION

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 144 for details.

Create Authentication Policy

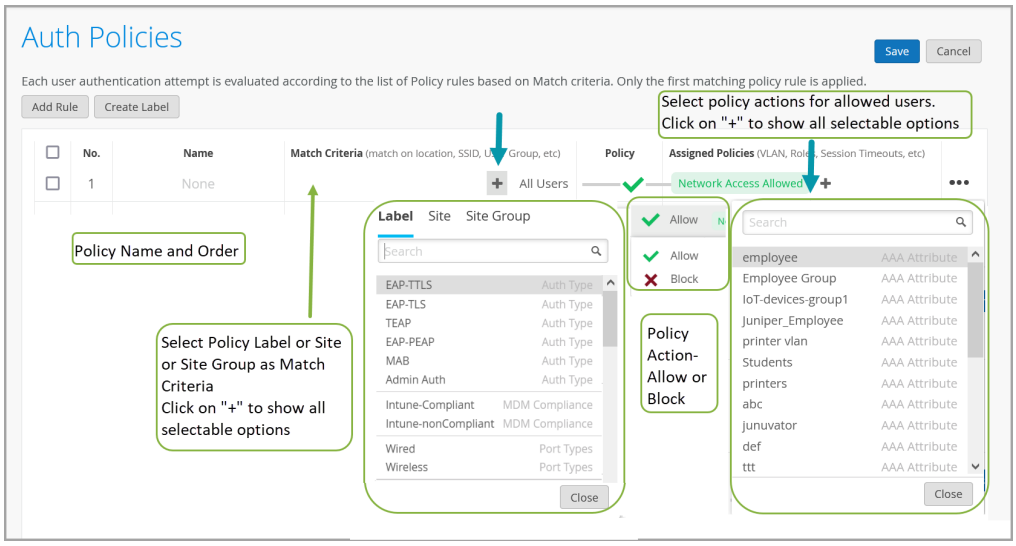
To create an authentication policy:

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 43: 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 *number*. 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: • Allow • Block
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 | **144**

NAC Events | **295**

Juniper Mist Access Assurance Use Cases | **6**

Juniper Mist Access Assurance Authentication Methods | **8**

Configure Certificate-Based (EAP-TLS) Authentication | **164**

Configure Credentials-Based (EAP-TTLS) Authentication | **194**

Configure Authentication Policy Labels

SUMMARY

Add labels to identify the users and resources that you want to refer to in your authentication policies, to control access to your network.

IN THIS SECTION

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 146 to select the label type.

Table 9: Parameters for New Label

Label Type	Details	Role in Authentication Policy Rule
AAA Attribute	A group of user attributes that works as the match criteria and helps determine the policy action that specifies permission. Options: • Role: Assigned user role. This can be used in applying role-based policies. • VLAN: VLAN ID or named VLANs. This can be used to assign VLAN to a client. • Realm: A domain used in authentication, often to specify where user credentials are valid. • User Name: unique identifier assigned to an individual or device. This can be used match the User Name RADIUS attribute of the authenticating device. • GBP Tag: Group Policy Tag) used to assign specific groups of users or devices to different types of network traffic management. • Session Timeout: Sets the maximum time allowed before user sessions are reset, from 3600 to 604800 seconds. • Custom Vendor Specific Attribute: Custom attributes that can be configured to be returned in the Access-Accept	Match criteria and policy permit action

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

Label Type	Details	Role in Authentication Policy Rule
	message.These attributes are tailored to specific vendors and can include roles or permissions. Examples: • Cisco: Cisco-AVPair, Cisco-NAS-Port, Cisco-Fax-Account-ID-Origin. • Juniper: Juniper-local-user-name. • Palo Alto Networks: PaloAlto-Admin-Role, PaloAlto-Admin-Access-Domain. • You can find vendor-specific attributes (VSAs) for different vendors in their respective documentation or configuration guides. • Custom Standard RADIUS Attribute (these are standard IETF RADIUS attributes such as *Idle-Timeout=600* or *Termination-Action=RADIUS-Request*, and can be modified with additional attributes. • Dynamic Wired Port Configuration (these are VLAN names that Access Assurance returns for the RADIUS attribute *Egress-VLAN-Name* in Access-Accept message, and are especially useful with dynamic port configurations, for example to automatically use trunk ports for AP	

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

Label Type	Details	Role in Authentication Policy Rule
	connections or to differentiate between tagged and untagged VLANs). • Returned User Name: Identifier of the user such as username, email that gets into the system once the user has successfully authenticated. Options: • Automatic • Certificate CN • Certificate SAN:UPN • Certificate SAN:Email • Certificate SAN:DNS • Configured Port VLAN ID: VLAN ID that a device is assigned to on a particular port after successful authentication. • NAS IP Address: The IP address of the network access server (the gateway device) where the authentication request is being made.	

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

Label Type	Details	Role in Authentication Policy Rule
Certificate Attribute	A group of user or device certificate fields used during authentication. Options: • Common Name (CN) • Subject • Serial Number • Issuer • Subject Alternative Name (SAN)	Match criteria
Client List	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* For devices that don't support 802.1X, you can use **Client Lists** to allow approved devices access the network.	Match criteria
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

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

Label Type	Details	Role in Authentication Policy Rule
MDM Compliance	Used in the Match section of the policy rule by evaluating client posture compliance received from the Mobile Device Management provider during authorization. • Compliant • Non-Compliant • Unknown	Match criteria
Client Label	Used to match a label or list of labels assigned to a MAC address in the NAC Endpoints Database. Enter text. Example: building3, floor2, printer.	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 | **141**

Juniper Mist Access Assurance Use Cases | **6**

Juniper Mist Access Assurance Authentication Methods | **8**

Configure Certificate-Based (EAP-TLS) Authentication | **164**

Configure Credentials-Based (EAP-TTLS) Authentication | **194**

WPA3 Radius PSK Support in Juniper Mist Access Assurance

SUMMARY

Follow these steps to configure a WPA3-Personal SSID with Multiple Passphrases (Multi-PSK) in Juniper Mist Access Assurance using MAC-based device registration for secure, role-based client connectivity.

IN THIS SECTION

Introduction

Juniper Mist Access Assurance supports WPA3 Multiple Passphrases (Multi-PSK), allowing you to deploy a single WPA3-Personal SSID with multiple passphrases through MAC-based device registration. This capability simplifies wireless network management by enabling different device types to securely connect to the same SSID while using unique passphrases for each group.

In WPA2 Multi-PSK deployments, multiple passphrases can be assigned to a single SSID, and any device providing a valid passphrase can authenticate successfully. However, WPA3 uses the Simultaneous Authentication of Equals (SAE) protocol, which enforces a mutual key exchange between the client and the network. As a result, for WPA3 Multi-PSK to function correctly, the client's MAC address or MAC OUI must be pre-associated with the corresponding passphrase to ensure a proper key match during authentication.

Requirements

To enable and use WPA3 Multiple Passphrases (Multi-PSK) in Juniper Mist Access Assurance, ensure the following prerequisites are met:

- AP Firmware: Version 0.14.x or later
- Subscription: Access Assurance Standard (or higher)

NOTE:

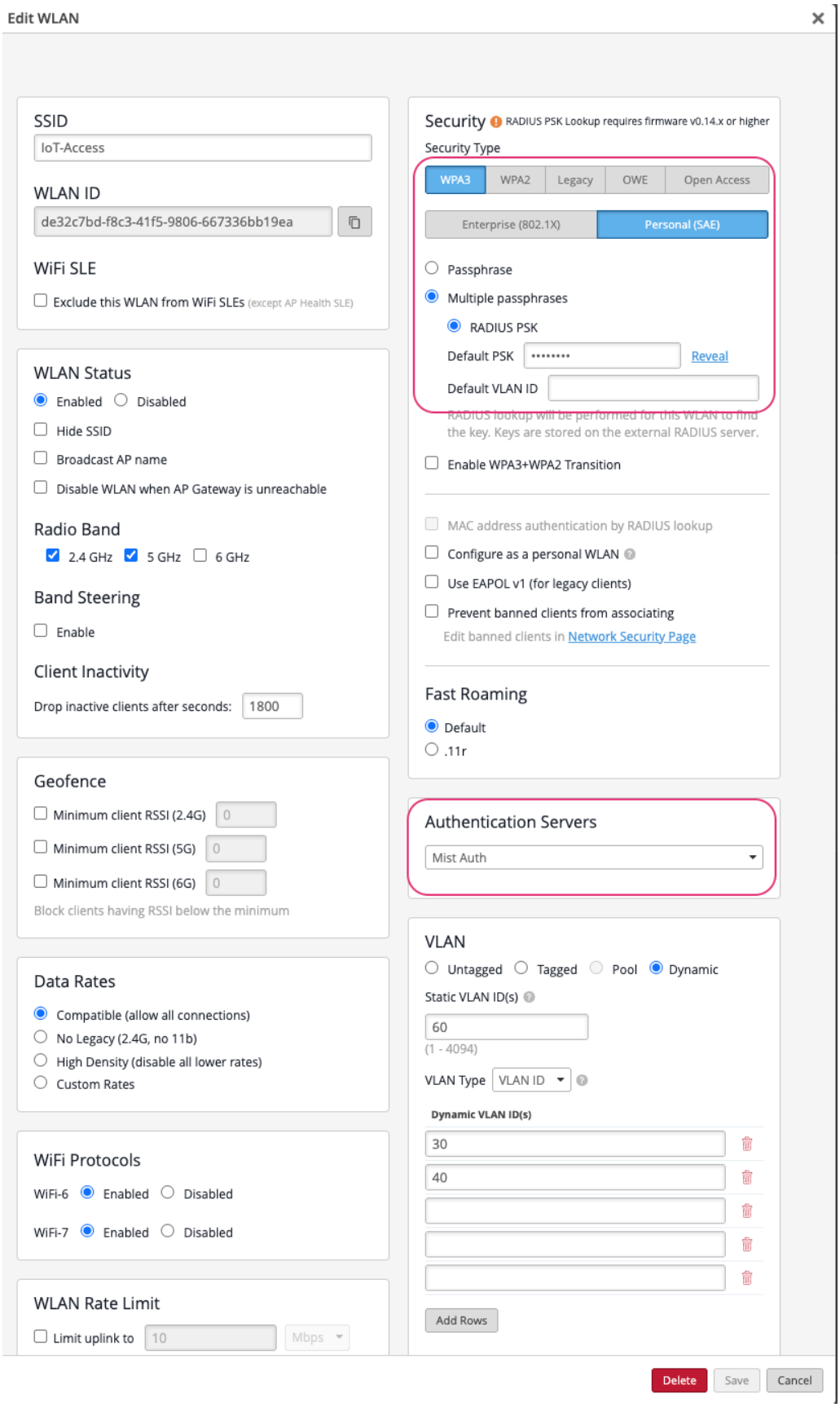
1. WPA3 Multi-PSK is supported at the organization level only. Both the WLAN and pre-shared keys (PSKs) must be configured at the organization level.
2. Client onboarding is not currently supported with WPA3 Multi-PSK. Therefore, all PSK entries must be manually created and associated with the corresponding MAC address or MAC OUI.

WLAN Configuration

Follow the steps below to configure a WPA3-Personal (SAE) WLAN with Multiple passphrases in Juniper Mist portal.

1. Navigate to **Organization** > **Wireless** > **WLAN Templates** and click **Add WLAN**.
2. Choose **WPA3** and **Personal (SAE)** as the security mode.
3. Enable **Multiple Passphrases** and **RADIUS PSK**.
4. Enter the **Default PSK** and **Default VLAN ID**:
   - The default PSK is used by clients whose MAC addresses are not registered.
   - If no VLAN is specified, unregistered clients are automatically assigned to VLAN 999 by default.
5. Scroll down to the **Authentication Servers** section and select **Mist Auth** as the authentication server.
6. In the VLAN section, enable **Dynamic VLANs** and include all VLAN IDs that will be used for the WPA3 passphrases.
7. Click **Save** to apply the configuration.

Figure 44: WLAN Configuration

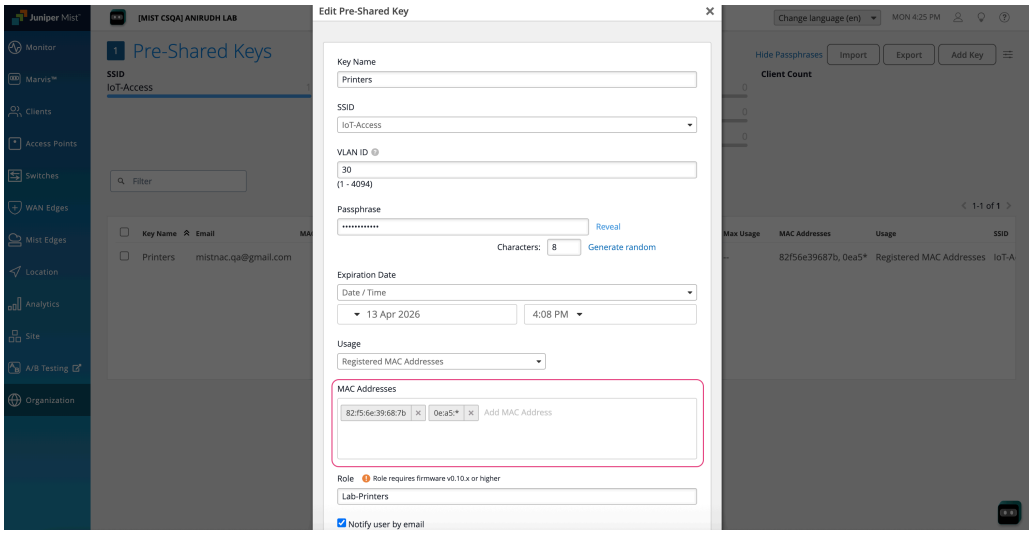


Pre-Shared Key Configuration

After configuring the WLAN, follow these steps to create and register WPA3 RADIUS PSK entries in Juniper Mist portal.

1. Navigate to **Organization** > **Wireless** > **Pre-Shared Keys**.
2. Click on **Add Key**.
3. Select SSID from the list that is configured with WPA3 RADIUS PSK. Provide all the required information, such as **Key Name**, **SSID**, **VLAN ID**, **Passphrase**, **Expiration date**, **Role**, and **Usage** as **Registered MAC Addresses**. Enter the MAC Address(es) or MAC OUIs. One or more MAC addresses or OUIs can be associated with this passphrase .
4. Click **Save**.

Figure 45: Pre-Shared Key Configuration



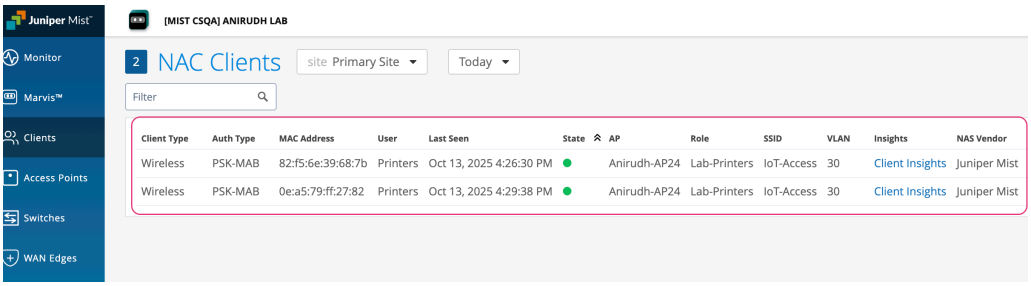
Once configured, devices with matching MAC addresses or OUIs can authenticate using the associated passphrase. Devices whose MAC addresses are not registered can authenticate with the default PSK specified in the WLAN configuration.

Client Connection and Verification

Clients with registered MAC addresses or OUIs connect using their assigned WPA3 Multi-PSK passphrase and the corresponding VLAN.

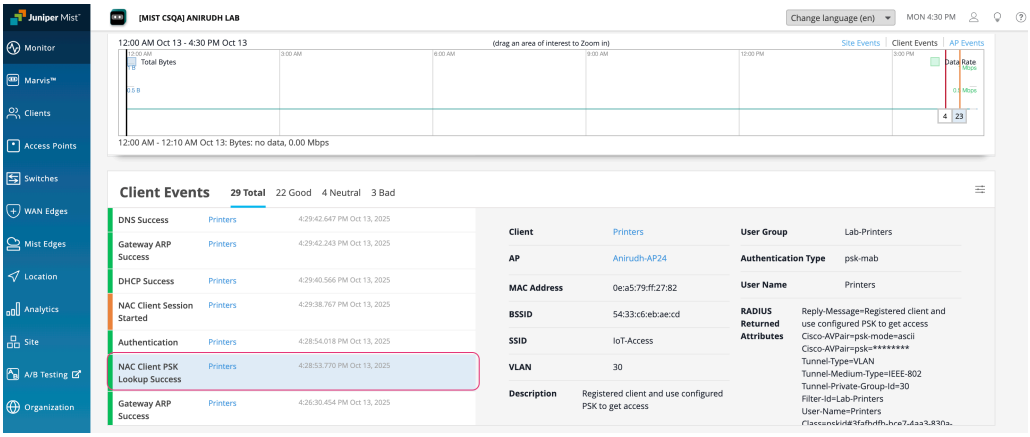
To verify the connection, navigate to **Clients** > **NAC Clients**. The Key Name from the PSK configuration will be displayed as the **User**.

Figure 46: View NAC Clients



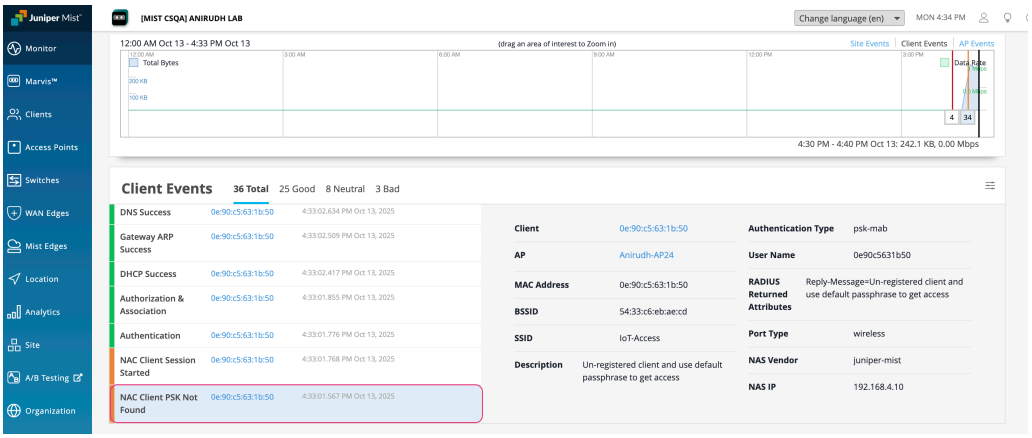
From this view, you can click on **Client Insights** to review detailed connection events and confirm the key lookup process during authentication.

Figure 47: View NAC Client Events—Registered Clients



Clients with unregistered MAC addresses will connect using the default PSK and be placed in the default VLAN.

Figure 48: View NAC Client Events—Unregistered Clients



RELATED DOCUMENTATION

- Juniper Mist Access Assurance Use Cases | 6
- Juniper Mist Access Assurance Best Practices | 14
- Juniper Mist Access Assurance Authentication Methods | 8
- *Subscription Types for Juniper Mist*

Site Survivability

SUMMARY

Use Access Assurance Site Survivability (NAC Edge) to ensure that users and devices can authenticate locally even when the site's WAN link to the Mist Access Assurance cloud is down.

IN THIS SECTION

Site Survivability Overview

IN THIS SECTION

Mist Access Assurance is a cloud-based solution that ensures high availability for authentication services. However, there are situations where sites need to continue authenticating users and devices even if their WAN links are down. Access Assurance Site Survivability (NAC Edge) addresses this requirement by providing on-site continuity, ensuring that users and devices can continue to securely connect to the network.

In Site Survivability mode, a lightweight Access Assurance service (NAC Edge service) runs on the on-premises Mist Edge appliance(s). This service processes RADIUS over TLS (RadSec) requests by using a secure local cache of previously authenticated clients. Mist access points (APs) and switches establish a secondary RadSec tunnel to the local Mist Edge, while third-party clients connect to the same Mist Edge acting as a RADIUS server. If the WAN connection is disrupted, the proxy service automatically fails over to the NAC Edge service running on the local Mist Edge, ensuring continuous authentication services. When the WAN connection is restored, authentication traffic seamlessly transitions back to the cloud-based Access Assurance.

How Site Survivability Works

Here's a high-level overview of how Site Survivability works:

- **Normal Operation (WAN link is up):**
  - APs, switches, and Mist Edges establish a RadSec tunnel to the cloud Network Access Control (NAC).
  - The cloud NAC processes the client authentication requests through this RadSec tunnel.
  - The site-level Mist Edge's NAC Edge service synchronizes a local cache of recently authenticated clients and configured server certificates from the cloud at regular intervals (every 30 minutes). Note that the NAC Edge RADIUS service serves client authentication requests only when the Access Assurance cloud is unreachable from the Mist Edge.
- **Outage (WAN link is down):**

  - When connectivity to the cloud NAC is lost, network devices automatically switch over to the NAC Edge, which is configured as the backup RadSec server.
  - The NAC Edge validates client certificates (for EAP-TLS) using your trusted Organization Certificate Authority (CA), checks the local cache for the client, and provides the cached authorization attributes, such as VLAN information.
  - Clients not found in the cache are assigned to a customer-defined default VLAN.
- **Recovery (WAN link is restored):**
  - Devices switch back to the cloud NAC based on their built-in failback behavior.
  - Mist Edge re-establishes primary RadSec sessions.
  - Client authentication requests are processed by the cloud NAC.

What's Supported in Site Survivability Mode

- **Authentication methods (when the WAN link is down):**

  802.1X EAP-TLS and MAC Authentication Bypass (MAB) using cached entries
- **Authorization:**
  - The system returns cached attributes for recognized clients, such as VLAN and RADIUS AVPs.
  - For unknown MAB clients, customer configured default VLAN is used in case of cache misses.
  - For 802.1X clients that have successfully passed EAP-TLS validation but are not recognized, the default VLAN is used in case of cache misses.
- **Cache behavior:**
  - Configurable Time-To-Live (TTL) ranging from 1 to 30 days, with a default setting of 7 days
  - Persistent cache even across Edge device restarts
  - Automatic cleanup of client entries once the TTL expires

What's Not Supported in Site Survivability Mode

When the WAN link is down, NAC Edge relies solely on the local cached information and cannot connect to external systems. This means

- EAP-TTLS and Device-Auth authentication are not supported. For example, password-based authentication is not supported.

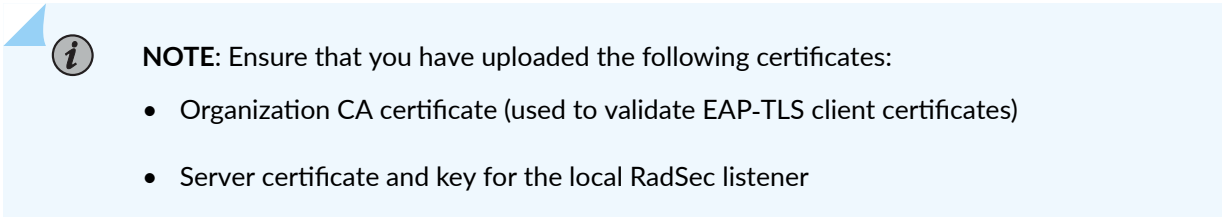
- External Identity Providers (IdPs) are unavailable, so no cloud directory or IdP lookups occur.
- MDM provider-based policies cannot be enforced.
- Real-time cloud policy evaluations are not possible.
- New devices without cache entries cannot obtain dynamic policies and are assigned the default VLAN you have configured.

Configure Site Survivability Settings

Site Survivability is enabled at the site level. The following requirements must be met for implementing Mist Access Assurance Site Survivability:

- A Mist Access Assurance Site Survivability subscription (S-CLIENT-SS-1/3/5) is necessary.
- At least one Mist Edge should be assigned to the site.
- Endpoints (laptops, mobiles and IoT devices) should be authenticated and authorized into your corporate network.

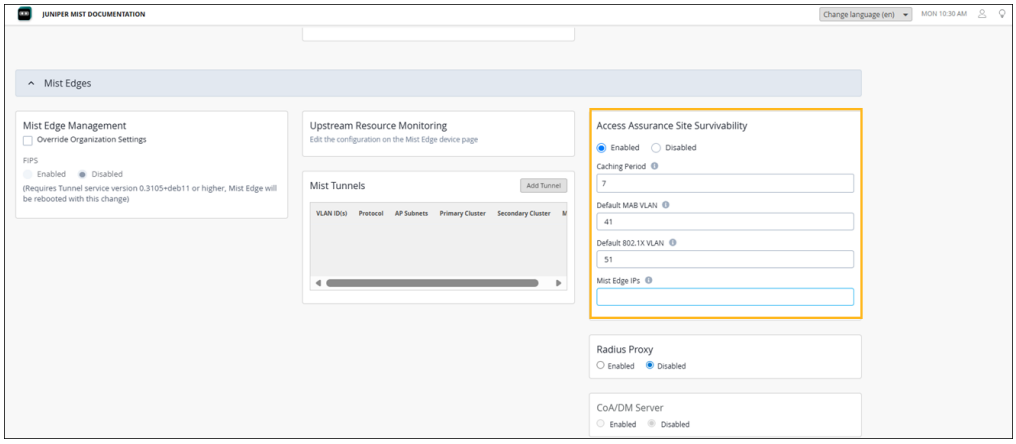
To configure Access Assurance Site Survivability:



NOTE: Ensure that you have uploaded the following certificates:

- Organization CA certificate (used to validate EAP-TLS client certificates)
- Server certificate and key for the local RadSec listener

1. Click **Organization** > **Site Configuration** to go to the list of sites.
2. Click the site in which you want to configure Access Assurance site survivability.
   The site page is displayed.
3. Scroll down to **Access Assurance Site Survivability** tile.
4. Select the **Enabled** check box on the Access Assurance Site Survivability tile.



5. Configure the settings as described below:
   - Caching Period—Enter the number of days (1 to 30) for which a cache of each NAC client should be maintained. The default is 7 days.
   - Default MAB VLAN—Enter the VLAN ID or VLAN Name of the VLAN for unknown MAB clients.
   - Default 802.1X VLAN—Enter the VLAN ID or name of the VLAN for unknown 802.1X clients that pass EAP-TLS authentication.
   - Mist Edge IPs—Enter the OOBM IP address(es) of the Mist Edge(s) acting in the site survivability mode.
6. Save the site configuration by clicking **Save** on the upper right of the page.

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

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:
Understand your use case *Understand different use cases supported by Juniper Mist Access Assurance.*	• "Use Case" on page 6 • "Authentication Methods" on page 8
Enable Mist Authentication *Use WLAN templates for wireless devices and use switch templates for wired clients.*	"Configure Certificate-Based (EAP-TLS) Authentication" on page 164
Configure certificates *Manage trusted certificate authorities and Mist access assurance server certificate configuration.*	"Use Digital Certificates" on page 135
Configure identity providers *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.*	"Add Identity Providers for Juniper Mist Access Assurance" on page 23
Create policies *Configure an authentication policy to authenticate end users or devices.*	• "Configure Authentication Policy Labels" on page 144 • "Configure Authentication Policy" on page 141

Table 10: Top Tasks *(Continued)*

If you want to...	Use these resources:
View connected clients and troubleshoot any issues *Validate connected client devices and get further details on user access and authentication in Juniper Mist portal.*	"Validate Access and Authentication" on page 300

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

SUMMARY

Follow the appropriate procedures and video demos below to configure certificate-based EAP-TLS authentication for your wireless or wired network.

IN THIS SECTION

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.

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 135
  - "Configure Authentication Policy Labels" on page 144
  - "Configure Authentication Policy" on page 141

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. 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).

> **NOTE**: The **Access** menu is available only if you have an Access Assurance subscription.

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 135.

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 141.

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 135 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 141.

      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.

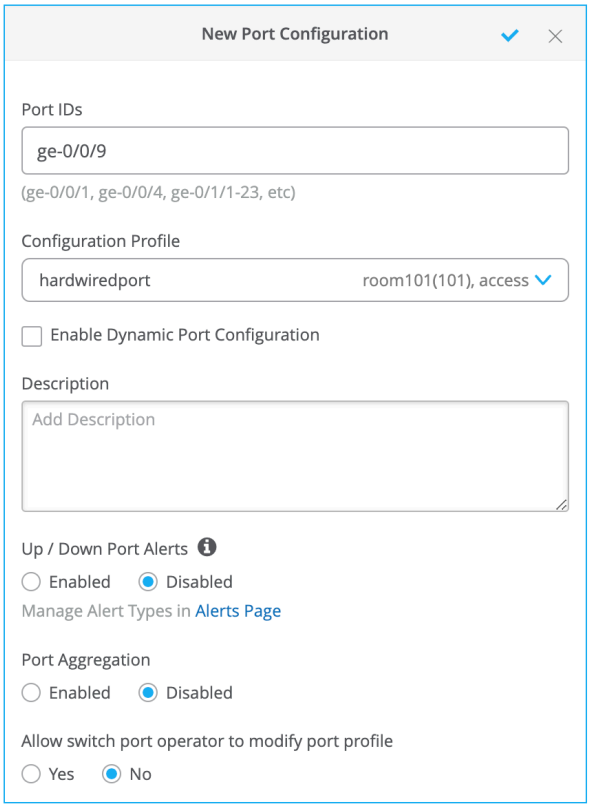
   c. Scroll down to the Port Profile section and select:

      - 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 49: Assign Port Profile to Port Ranges on a Switch



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:

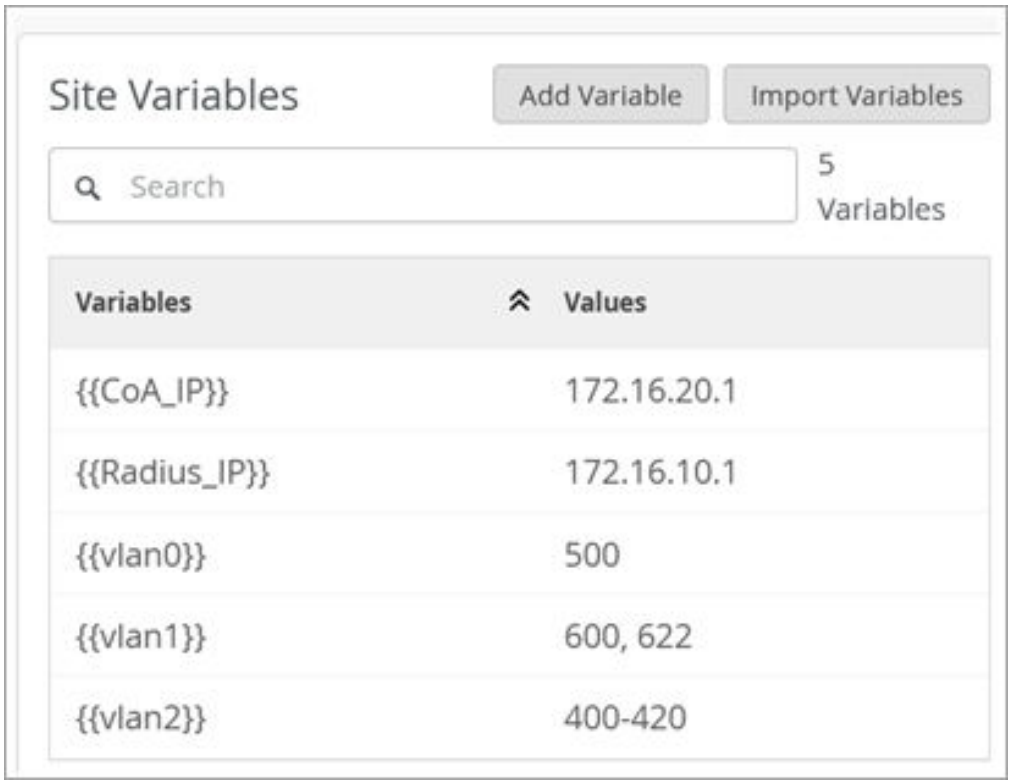
Video: https://mist.wistia.com/embed/iframe/zs88vs3piv

Example: Configure Authentication Policy using Site Variables

You can use site variables in authentication policy to assign the VLANs specific to the sites. This flexibility can be particularly useful when creating and managing authentication policies across various locations. By leveraging site variables, you can streamline the process of configuring authentication policies and ensure consistency across different sites.

1. Create site variables.
   a. In the Juniper Mist cloud portal, click **Organization > Admin > Site Configuration**.
   b. Select the site for which you want to configure site variables.
   c. Scrolls down to the **Site Variables** pane and click the **Add Variable** button.
   d. In the pop-up screen that appears, type a name for the variable and specify the value it represents.

Figure 50: Create Site Variables



The following table shows a list of variables used in this example.

Table 11: Site Variables Samples

Site	Variable	Value
Site-1	{{vlan0}}	100
	{{vlan1}}	200,222
	{{vlan2}}	20-30
	{{Radius_IP}}	172.16.20.1
	{{CoA_IP}}	172.16.10.1
Site-2	{{vlan0}}	500
	{{vlan1}}	600,622

Table 11: Site Variables Samples *(Continued)*

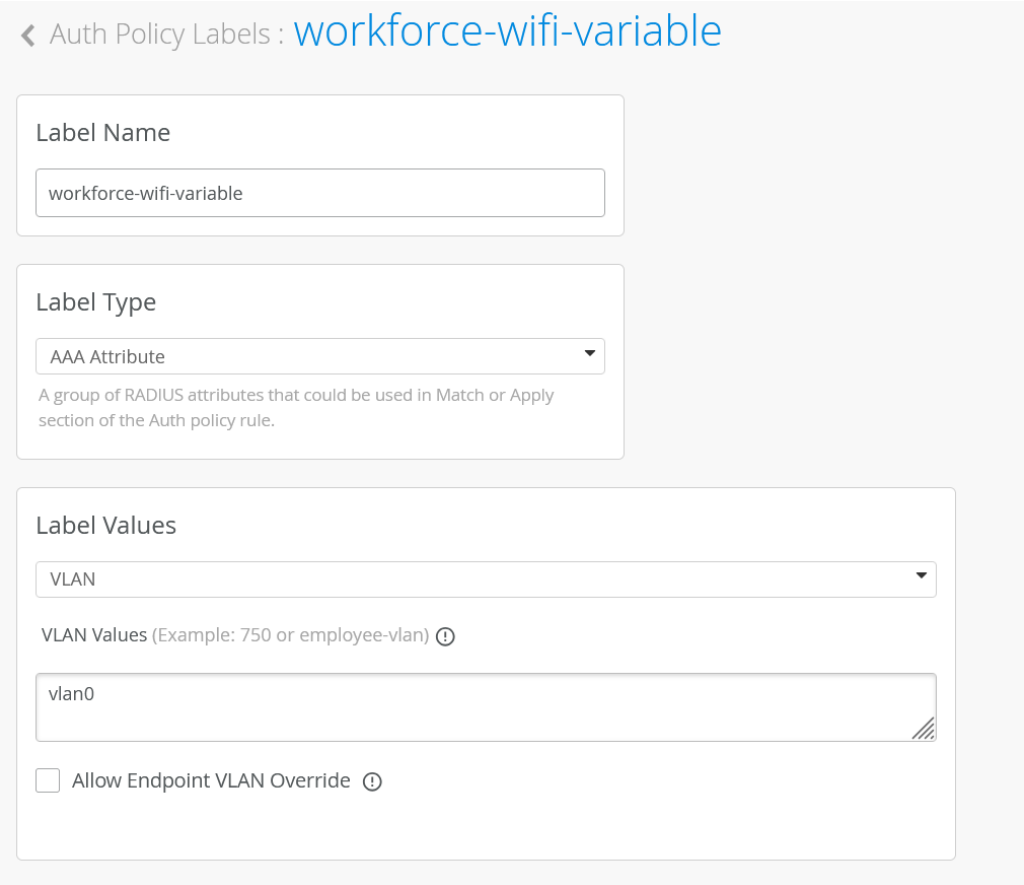
Site	Variable	Value
	{{vlan2}}	400-420
	{{Radius_IP}}	172.16.40.1
	{{CoA_IP}}	172.16.30.1

e. Click Save.

2. Create an Authentication Policy label.

a. From the left menu of the Juniper Mist portal, select **Organization** > **Access** > **Auth Policy Labels**.

Figure 51: Create a Label



- Label Name—Enter the label name (example: workforce-wifi-variable).

- Label Type—Select the type as **AAA Attributes**.
- Label Values—Enter client label. For this example, enter label value as vlan0. This is the site variables you created in previous procedure.

b. Click **Create**.

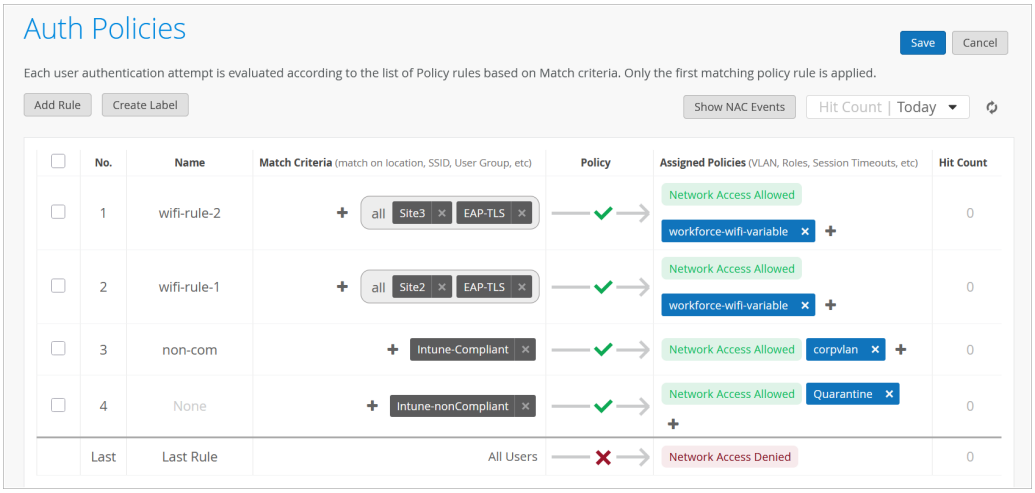
3. Create Authentication Policy.

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

b. In Authentication Policy page, add a new policy:

i. Click **Add Rule** to create a rule. In this rule, use the label you created in the previous step.

Figure 52: Create Auth Policy



ii. **Name**—Enter a name for the policy.

iii. **Match Criteria**—Select the match criteria such as site and authentication type such as EAP-TLS.

iv. **Policy**—Select Allowed.

v. **Policy action**—Select **Network Access Allowed**.

vi. **Assigned Policies**—Select the labels created in previous procedure under AAA attribute.

4. 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.

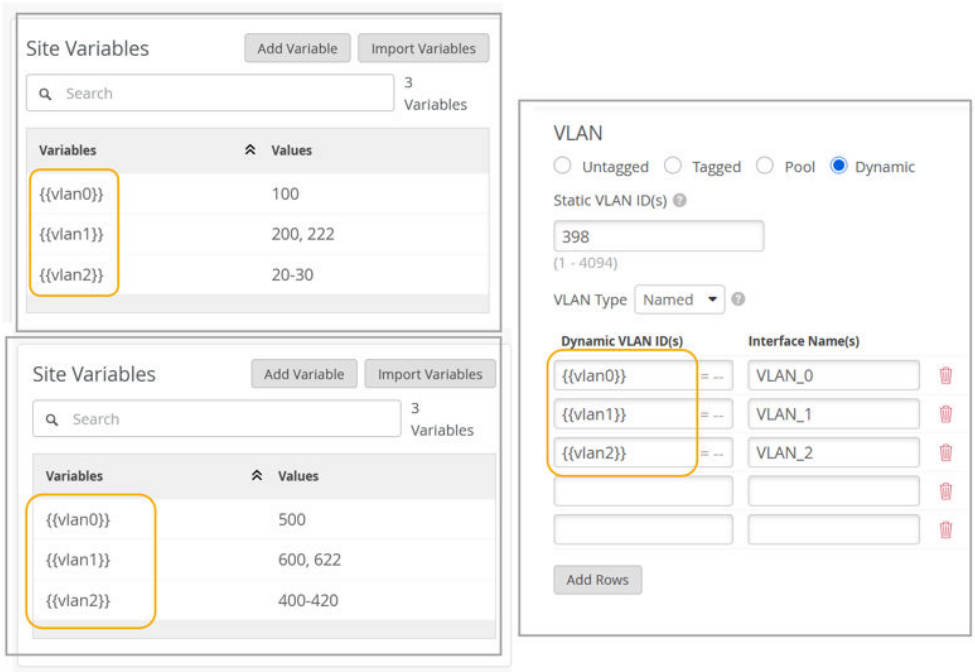
b. On the WLAN Templates page, click **Add WLAN**.

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—Select Dynamic. In the VLAN Type, select Named and enter the site variable created for VLAN.

Figure 53: Configure VLANs in WLAN Template



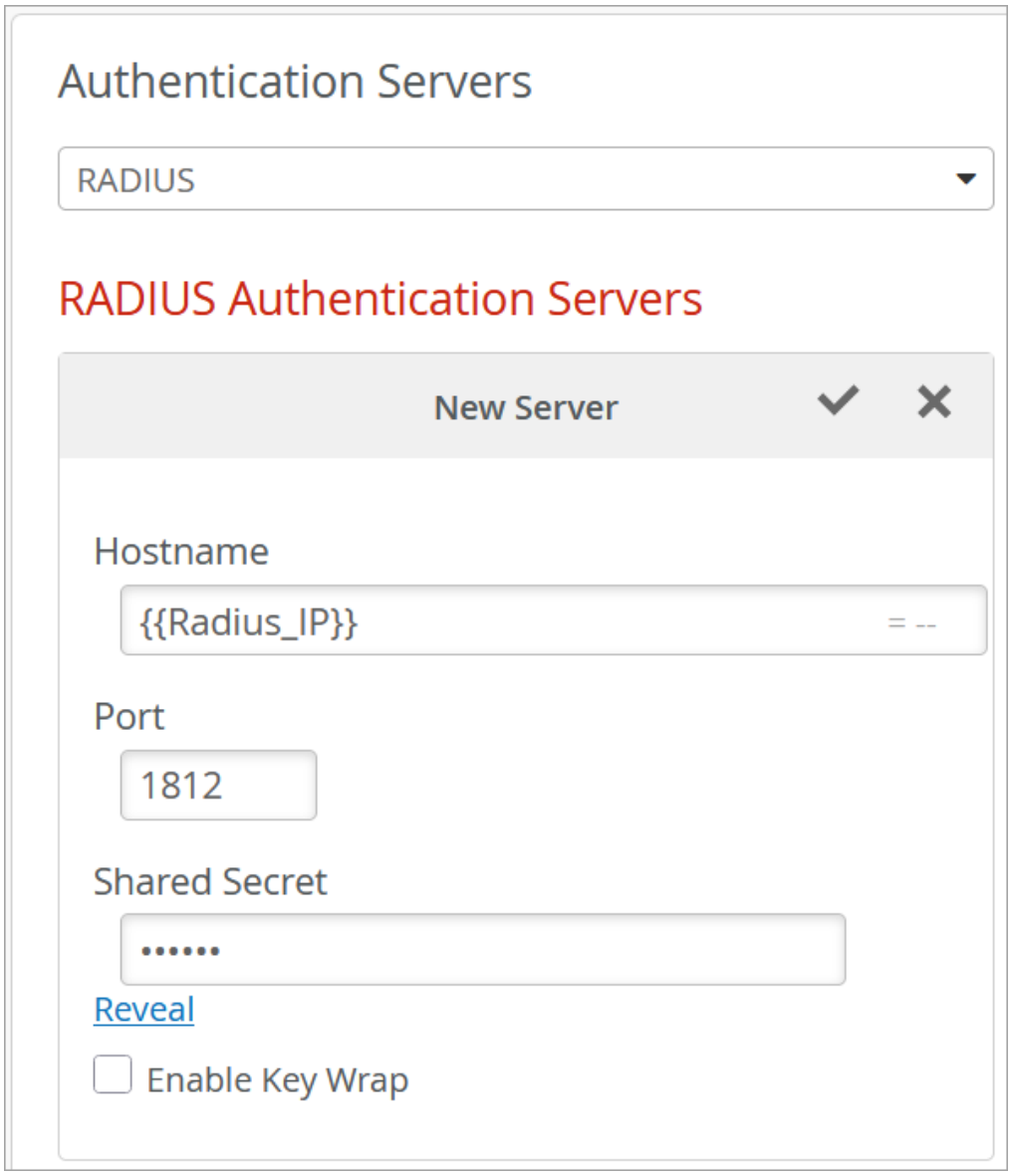
Now the SSID configuration is complete.

e. Click **Create**.

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

a. If you are using RADIUS authentication server, In the WLAN template page, go to **Authentication Server** section and select RADIUS from the drop-down box.

Figure 54: Configure RADIUS Authentication Server



Enter the following details:

i. **Hostname**— The IP address or FQDN of your RADIUS server. Enter the variable you created here.

ii. **Port**— Typically, the default RADIUS port is 1812 for authentication and 1813 for accounting, but this might vary based on your server configuration.

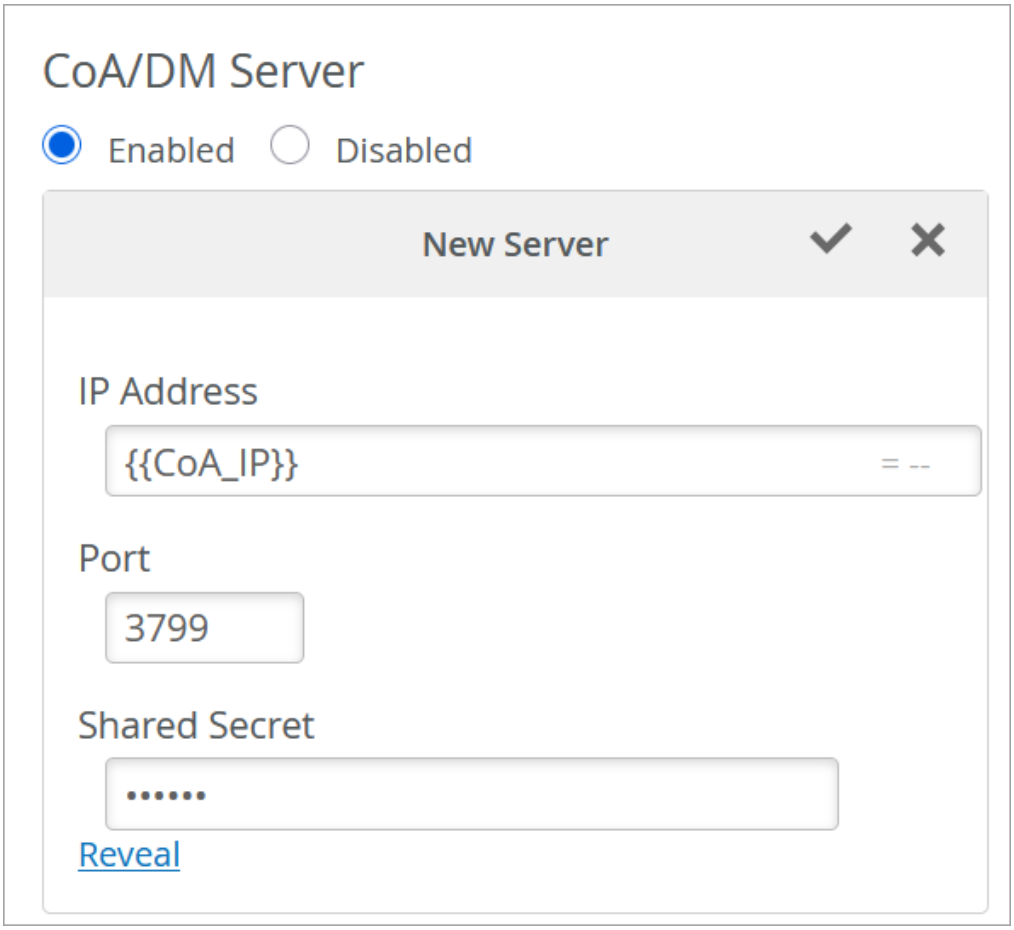
iii. **Shared Secret**— The shared secret used to authenticate the Mist APs with your RADIUS server.

iv. (Optional) **Enable Key Wrap**— If your RADIUS server supports key wrapping, enable this feature and enter the necessary key details.

a. You can also enable Change of Authorization (CoA) or Disconnect Message (DM) servers in as part of the WLAN creation process.

Scroll down to the **CoA/DM Server** section and check the **Enabled** box.

Figure 55: Configure CoA/DM Server



Enter the following details:

i. **Hostname**—The IP address of your CoA/DM server. Enter the variable you created here.

ii. **Port**— Retain the default port is 3799

iii. **Shared Secret**— The shared secret used to authenticate the Mist APs with your server.

5. Save your configuration

Once the configuration is complete, the authentication policy uses the site variables to assign the wireless VLAN for Site 1 and Site 2. When the policy is applied, for Site 1, value 100 is assigned VLAN 0. Similarly for Site 2, value 500 is assigned VLAN 1. In the same way, for Site 1, Radius server with IP address 172.16.20.1 and CoA server with IP address 172.16.10.1 will be used and for Site 2, Radius server with IP address 172.16.30.1 and CoA server with IP address 172.16.40.1 are used.

SEE ALSO

Configure Authentication Policy | **141**

Configure Authentication Policy Labels | **144**

Use Digital Certificates | **135**

Configure Certificate-Based (EAP-TLS) Authentication with Azure IdP Integration | **183**

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

SUMMARY

Follow these steps to configure a wired device to authenticate devices based on their MAC addresses.

IN THIS SECTION

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 165
- 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

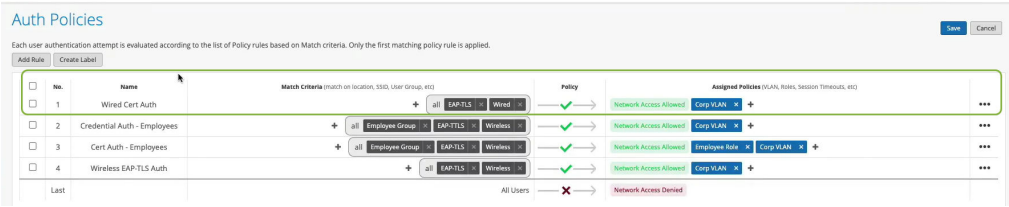
Video: Wired Authentication Validation

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 141.

Figure 56: 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**.

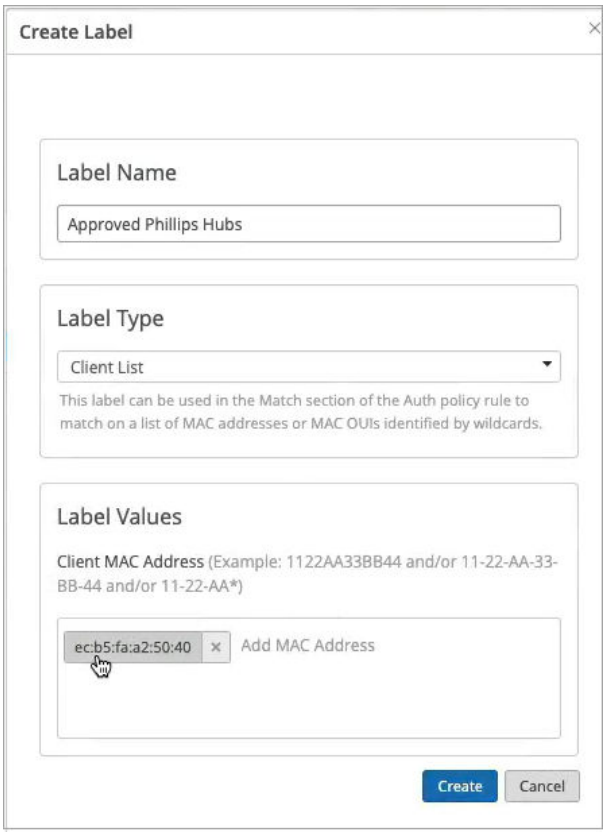
iii. Policy—Select **Allowed**

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 57: Label for Non-Dot1x device



Enter the following information in the respective fields:

i. Label Name—Enter the label name (example: Approved Phillips Hubs)

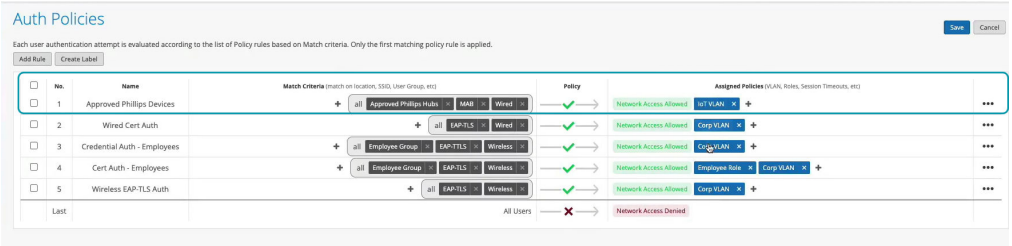
ii. Label Type—Select the type Client List

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 58: 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.

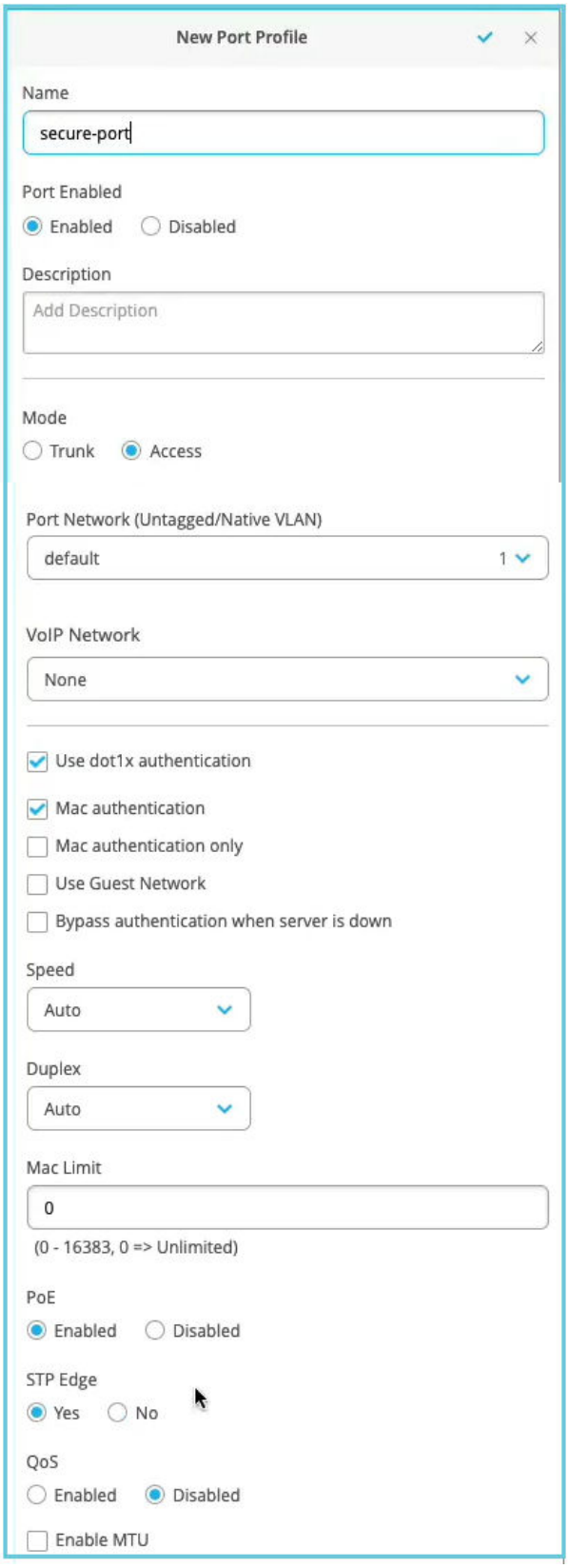
   a. From the left menu of the Juniper Mist portal, select **Organization > Wired > Switch Templates**.

   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 59: Port Profile Options



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.

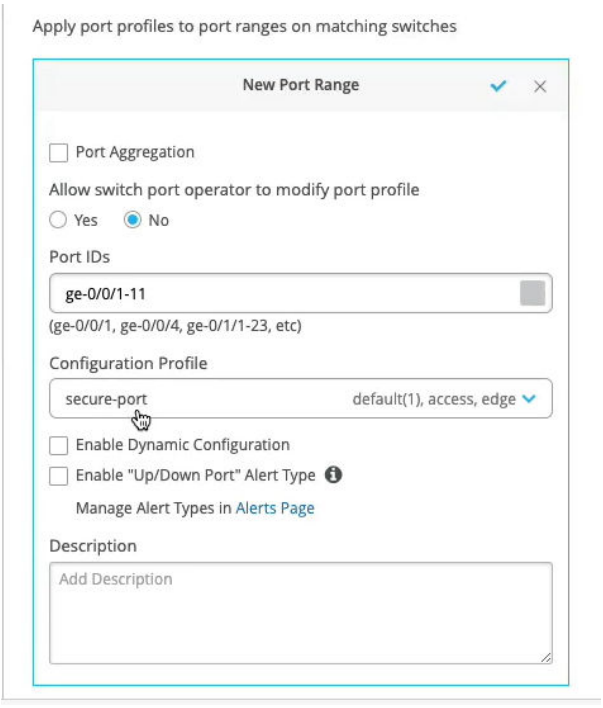
iv. STP Edge—Select **Yes**to configure the port as a Spanning Tree Protocol (STP) edge port. This setting ensures that the port is treated as an edge port.

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 60: Assign Port Profile to Port Ranges on a Switch



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 | **141**

Configure Authentication Policy Labels | **144**

Use Digital Certificates | **135**

Configure Certificate-Based (EAP-TLS) Authentication with Azure IdP Integration | **183**

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

SUMMARY

Follow these steps to register your Juniper Mist™ organization in Microsoft Entra ID, add your Identity Provider in Juniper Mist, and create authentication policies for your user groups.

IN THIS SECTION

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 164 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.

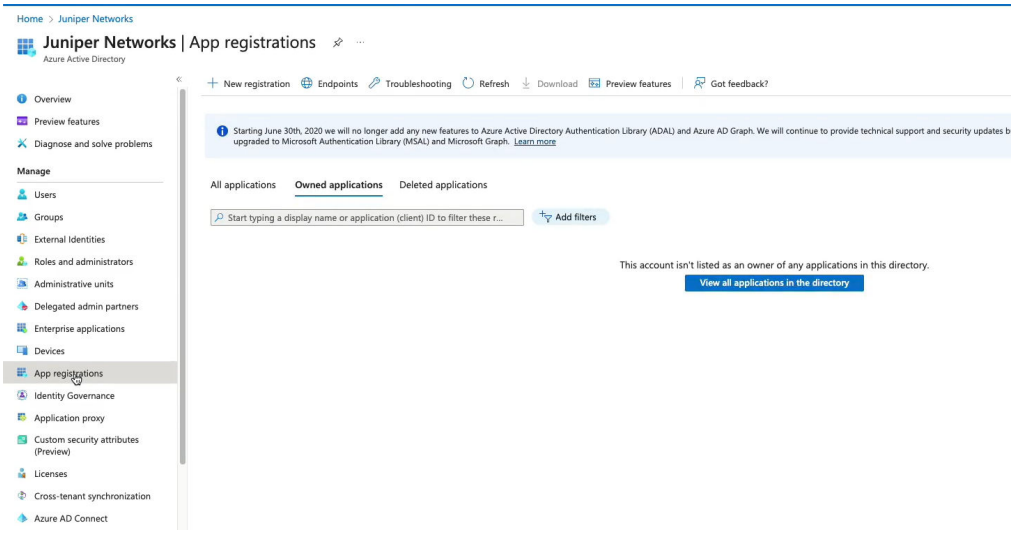
To create authentication using Okta as an IdP, watch the following video:

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 61: 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.

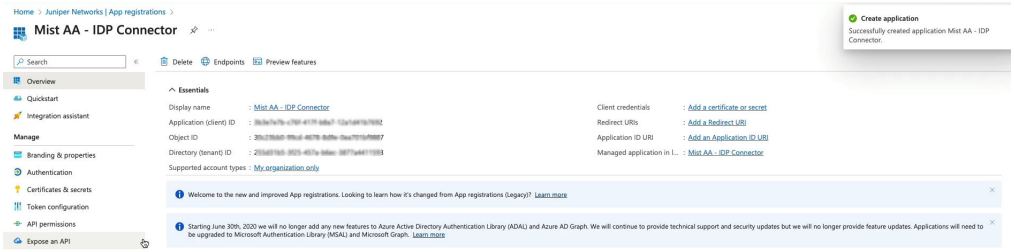
If you want to register a new application on the Azure portal, click the **New registration** tab.

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 62 on page 186.

Figure 62: New Application Details



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

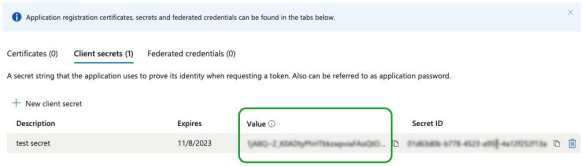
- Application (Client) ID—You'll need to enter this information in the **OAuth Client Credential (CC) Client ID** and **Resource Owner Password Credential Client ID** fields.
- Directory (Tenant) ID—You need this information for the **OAuth Tenant ID** field.

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 63 on page 186.

Figure 63: 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**.

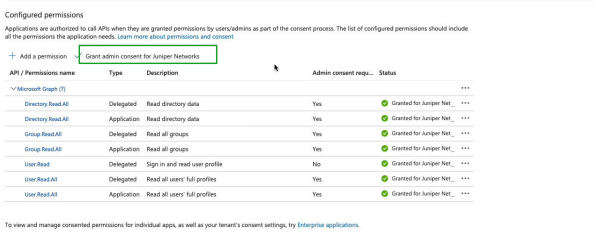
   You must give your application the required access permissions to use Microsoft Graph API to fetch information about users.

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 64 on page 187.

Figure 64: API Permissions for Application



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.

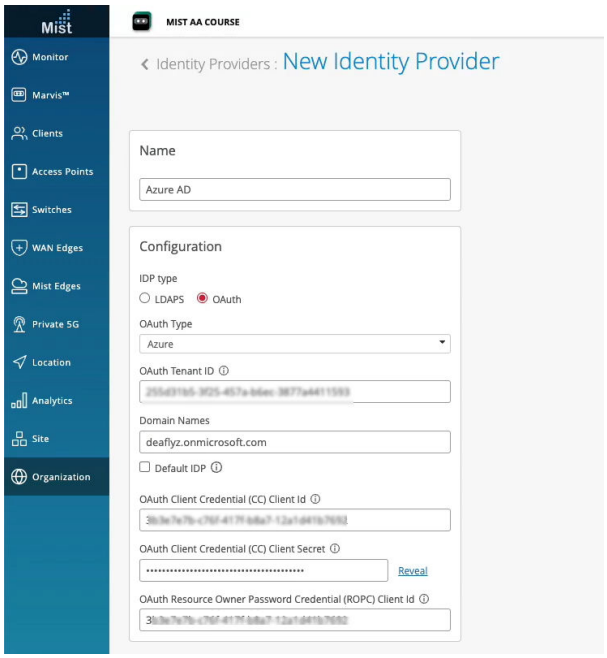
3. On the Juniper Mist portal, add Azure AD as an identity provider.

   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 65 on page 188.

Figure 65: Add Azure AD as Identity Provider



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.

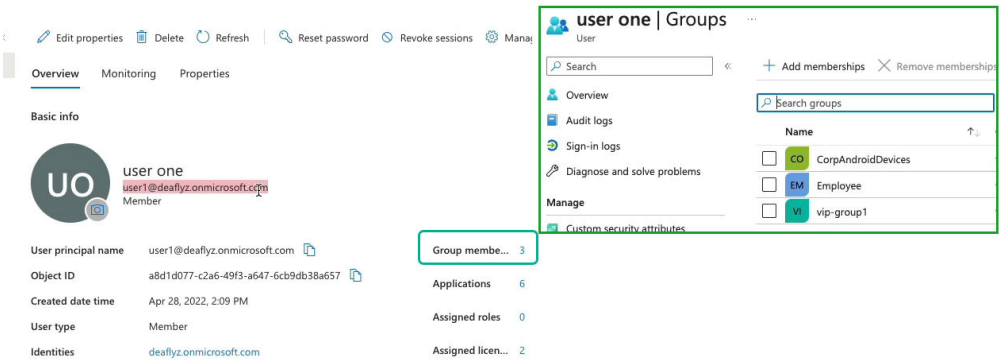
vii. **OAuth Client Credential (CC) Client secret**—Azure AD application secret. Azure AD application secret. Enter the value component of the client secret that the Azure portal generated for the IdP connector.

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.

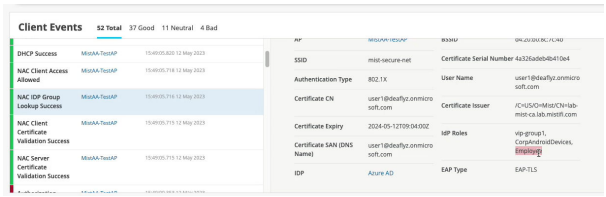
Figure 67 on page 189 and Figure 66 on page 189 show an user's details in Azure AD and the Juniper Mist portal.

Figure 66: 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 67: User Details on Juniper Mist Portal



In the example shown in Figure 67 on page 189, the user belongs to the group, **Employee**.

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

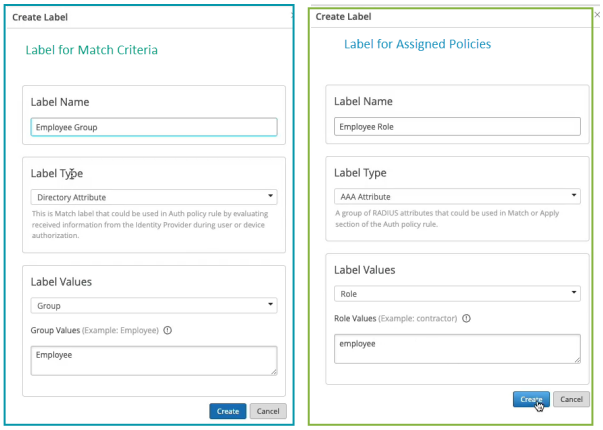
Create Authentication Policy Based on Group Details

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.

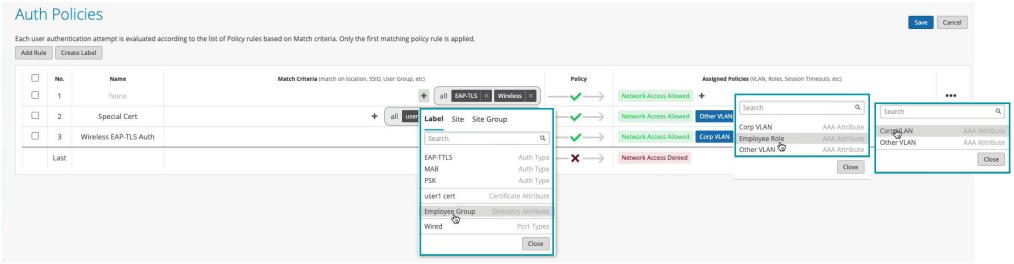
Figure 68: Labels for Authentication Policies



- 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 69: 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.

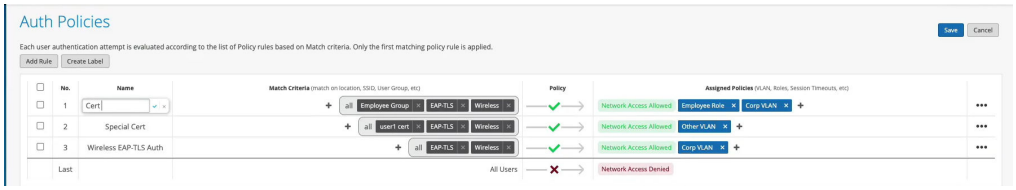
c. In the Policy column, click the check mark icon (✓), and then select the action you want to enforce, Allow or Block, on the resources you will identify next.

d. Click the (+) in the Assigned Policies column and selectthe 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 70 on page 191 shows the completed authentication policy.

Figure 70: 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.

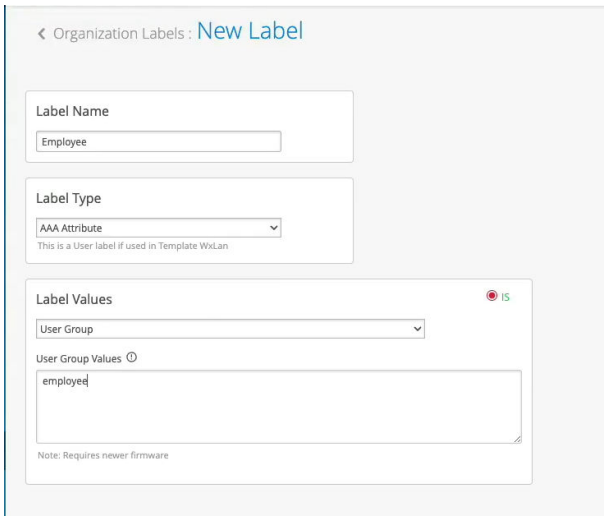
   b. Enter a **Label Name** so that you'll recognize the label when creating your policy.

   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 71: Create New Label



d. Click **Create** at the top right corner of the Organization Labels screen.

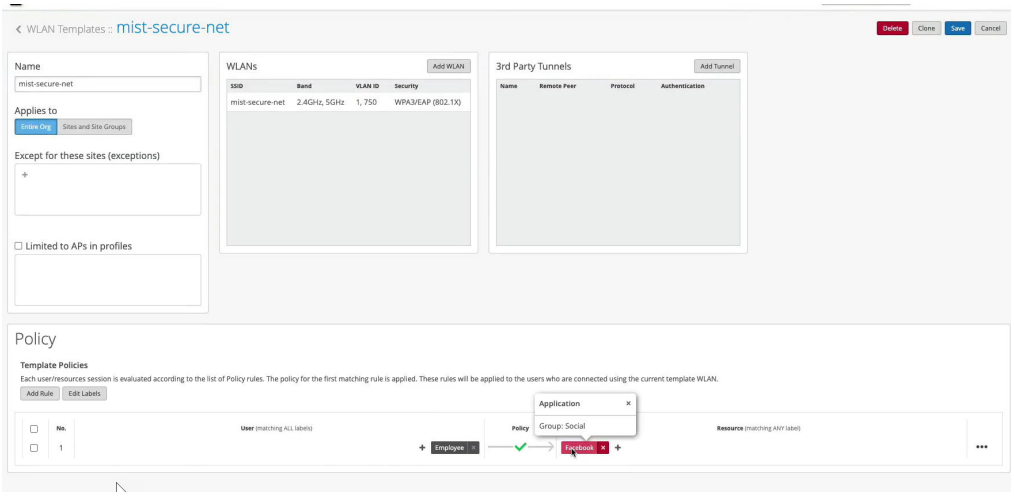
e. Repeat the above steps to add other labels as needed for other user groups.

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.



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 | 141

Configure Authentication Policy Labels | 144

Use Digital Certificates | 135

Configure Certificate-Based (EAP-TLS) Authentication | 164

Configure MAC-Based Authentication and MAC Authentication Bypass (MAB) | 177

Add Identity Providers for Juniper Mist Access Assurance | 23

Configure Credentials-Based (EAP-TTLS) Authentication

SUMMARY

To secure your network with credentials-based authentication, follow these steps to import your certificate, create authentication policies, and update the port profiles to use EAP-TTLS (802.1X) authentication.

IN THIS SECTION

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 23.
- 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 135 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 141.

      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.

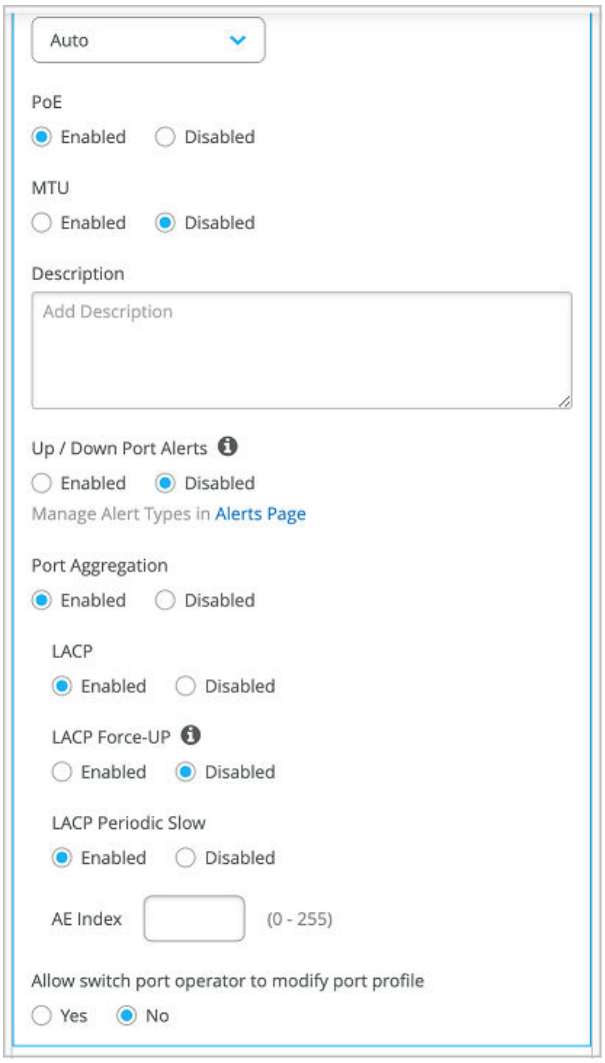
   c. Scroll down to the Port Profile section and configure the following settings:

      - 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 72: Assign Port Profile to Port Ranges on a Switch



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 144.

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 | 141

Configure Authentication Policy Labels | 144

Configure Certificate-Based (EAP-TLS) Authentication | 164

Configure Certificate-Based (EAP-TLS) Authentication with Azure IdP Integration | 183

Configure MAC-Based Authentication and MAC Authentication Bypass (MAB) | 177

Configure Client Device for EAP-TTLS Authentication | 197

Add Identity Providers for Juniper Mist Access Assurance | 23

Configure Client Device for EAP-TTLS Authentication

SUMMARY

To secure your network through EAP-TTLS authentication, follow these configuration steps on the client device.

IN THIS SECTION

Juniper Mist Access Assurance supports **EAP-TTLS authentication only with PAP** as the inner method. By default, most client devices such as Apple iOS/macOS and Windows attempt to use PEAP-MSCHAPv2 or EAP-TTLS/MSCHAPv2 when a user enters credentials at the SSID login prompt. These methods rely on password hashing (such as MSCHAPv2) and are not supported with modern cloud-based Identity Providers (IdPs). To enable successful onboarding, client devices must be explicitly configured to use **EAP-TTLS with PAP**. In production deployments, this configuration is typically

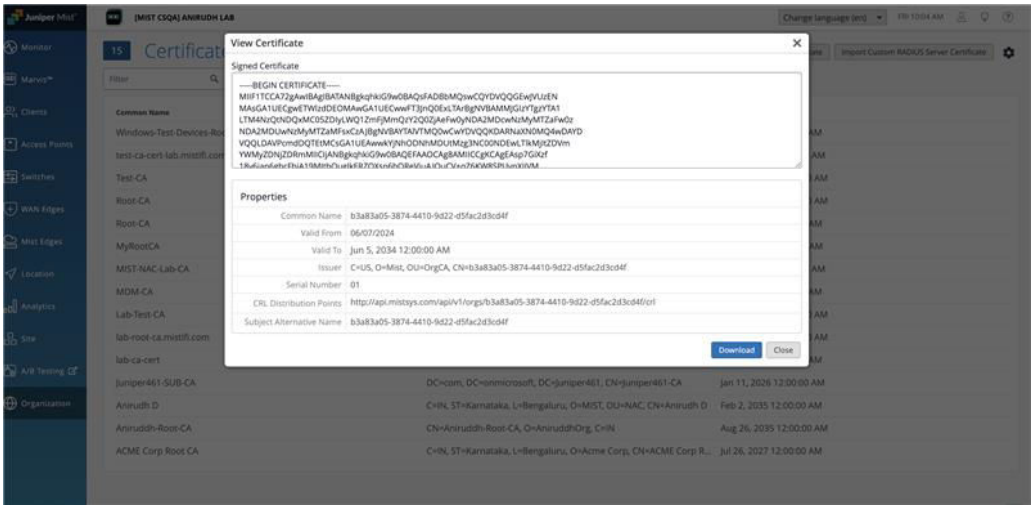
enforced through Mobile Device Management (MDM) solutions. For validation or lab testing, however, the method can also be manually configured on the device by following the steps below

Prerequisites

1. **Download the Juniper Mist Org CA certificate**:
   Client devices must trust the Mist Access Assurance server. The Mist Org CA certificate must be included in the wireless profile you configure.

   a. On the Juniper Mist portal, go to **Organization > Access > Certificates.**. In the Certificate Authorities page, click **View Mist Certificate** to display the certificate details.

   Figure 73: Download Juniper Mist CA Certificate

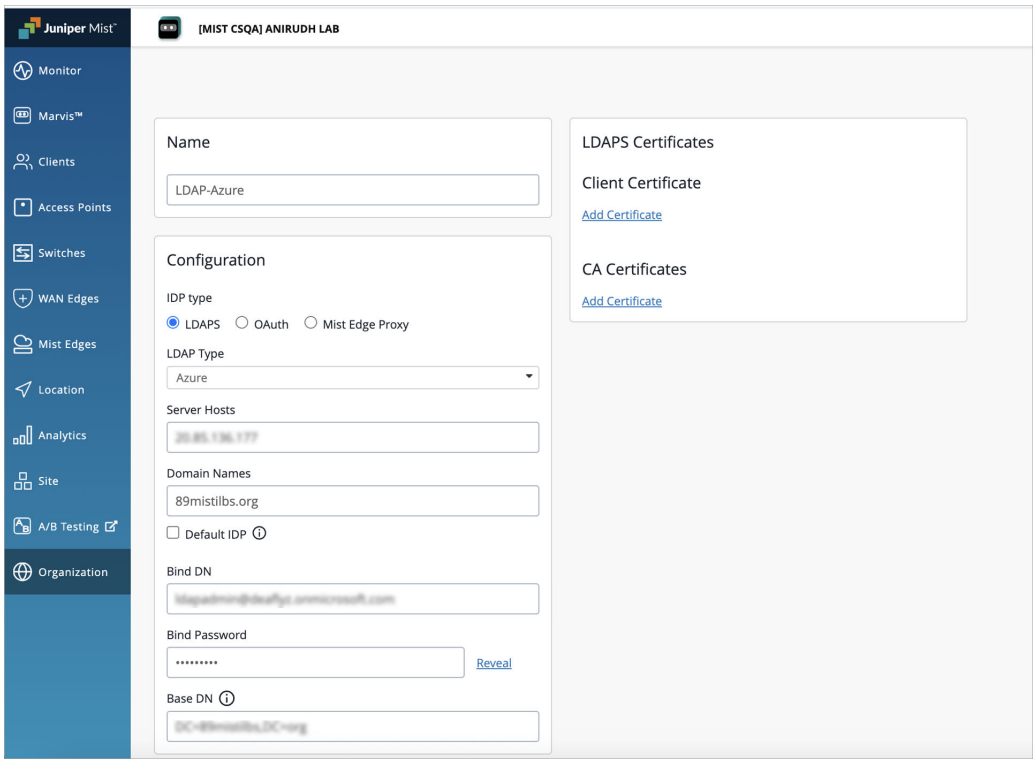


   b. Click **Download Certificate** to download the certificate on your client device.

> **NOTE**: If you are using a custom server certificate, use the **Root CA** of the server certificate instead of the Mist Org CA.

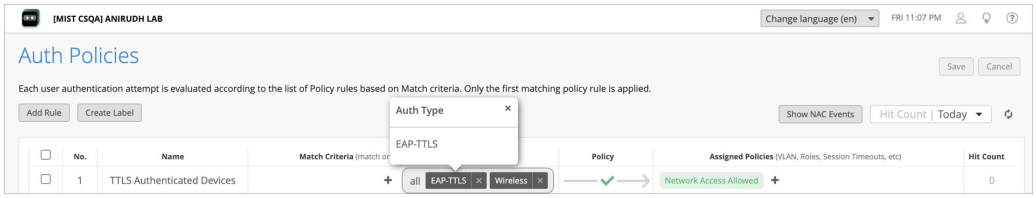
2. **Configure the Identity Provider (IdP)**: In Juniper Mist dashboard, navigate to **Organization > Access > Identity Providers > Add IDP** and configure the required IdP details. For details, see "Add Identity Providers for Juniper Mist Access Assurance" on page 23.

Figure 74: Configure the Identity Provider



3. **Create an Auth Policy Rule**: Under **Organization> Access> Auth Policies**, define an appropriate Auth Policy Rule that allows EAP-TTLS client devices to connect to the network. For details, see "Configure Authentication Policy" on page 141.

Figure 75: Create an Auth Policy



Configure Apple Device for EAP-TTLS Authentication

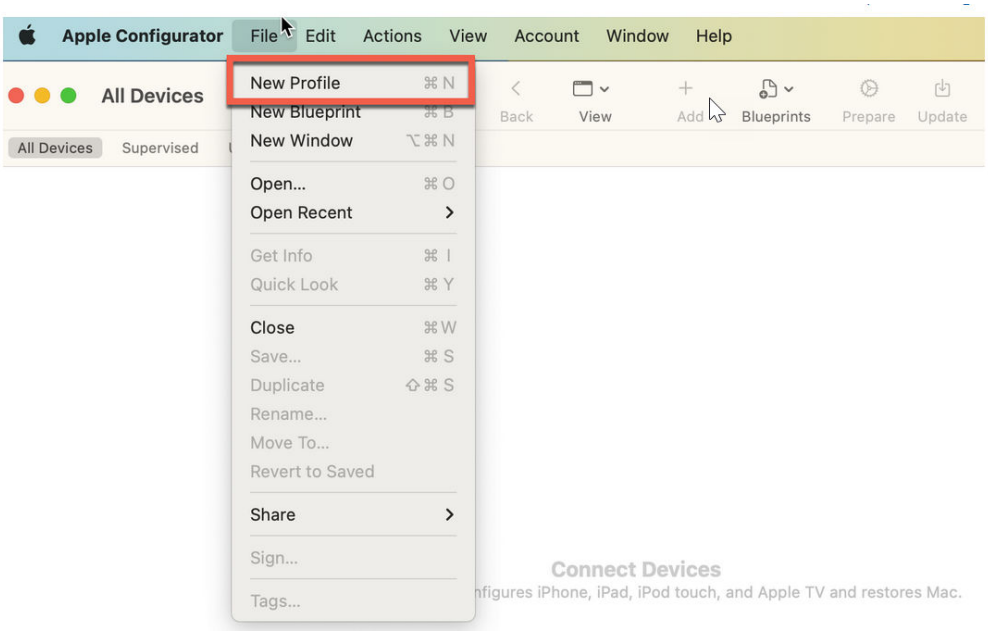
We've described the configuration using Apple macOS device.

For this task, create an EAP-TTLS network profile using a free Apple Configurator tool.

Create a profile on your Apple client device:

1. On your macOS client, open your Apple Configurator tool, and click **File > New Profile**

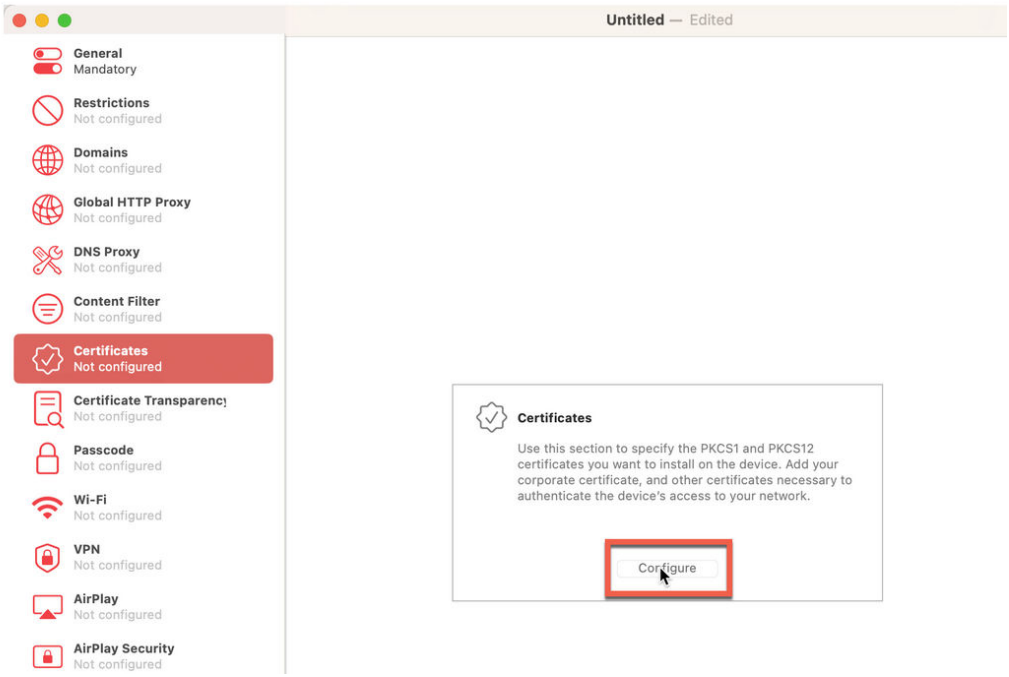
Figure 76: Wi-Fi Profile Configuration for Apple Client



A new configuration profile document opens.

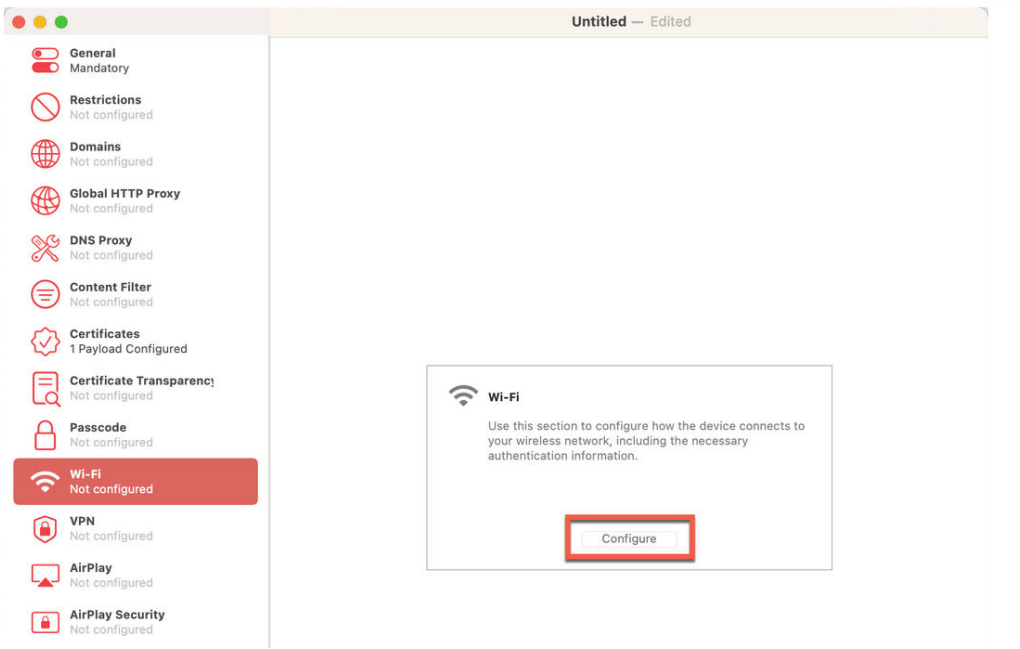
2. On the left-navigation bar of the Apple Configurator page, click **Certificates > Configure**. Select and upload your Mist Certificate you downloaded (as mentioned in "Prerequisites" on page 198). For the client devices to trust the Juniper Mist Access Assurance Server, you must include it in the wireless profile.

Figure 77: Upload Juniper Mist CA Certificate in Wi-Fi Profile Configuration



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

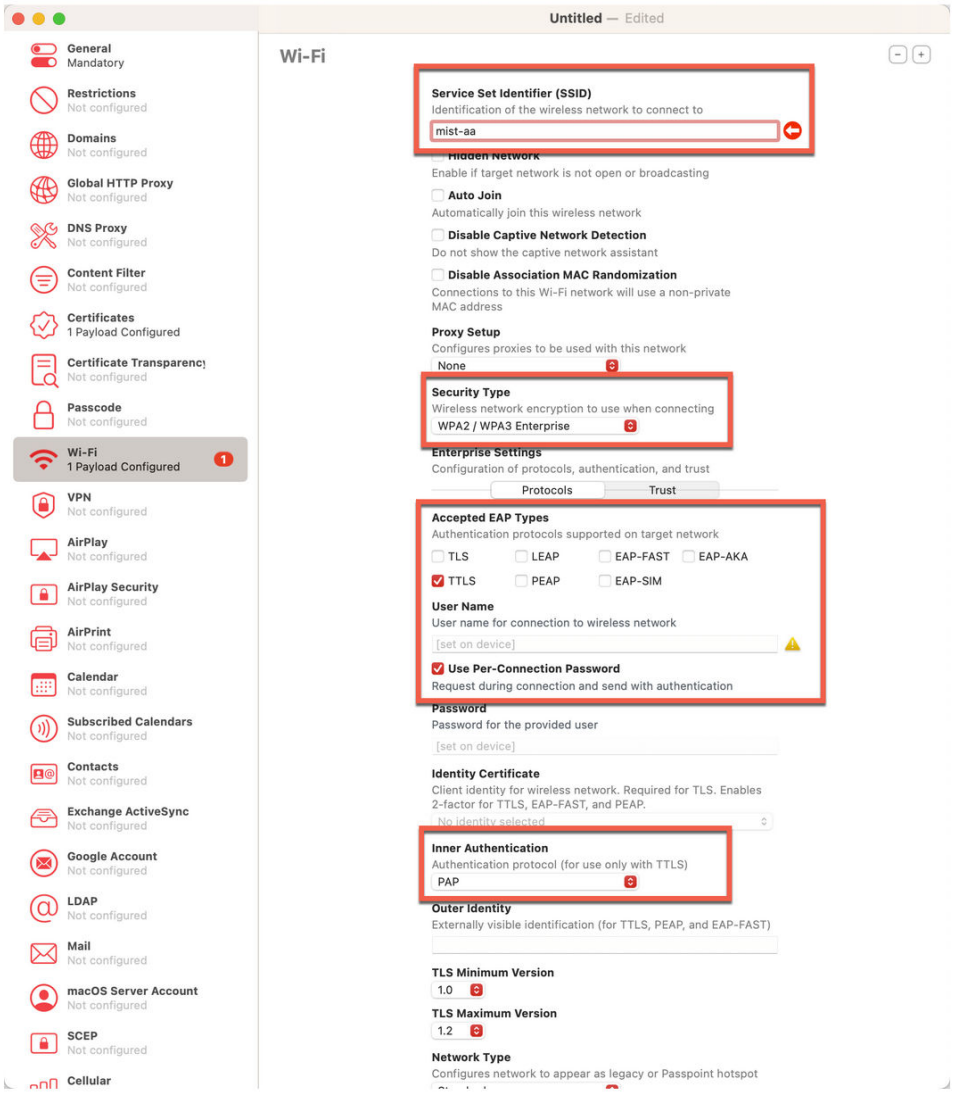
Figure 78: Wi-Fi Profile Configuration



Enter the following options for the Wi-Fi settings:

- **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**

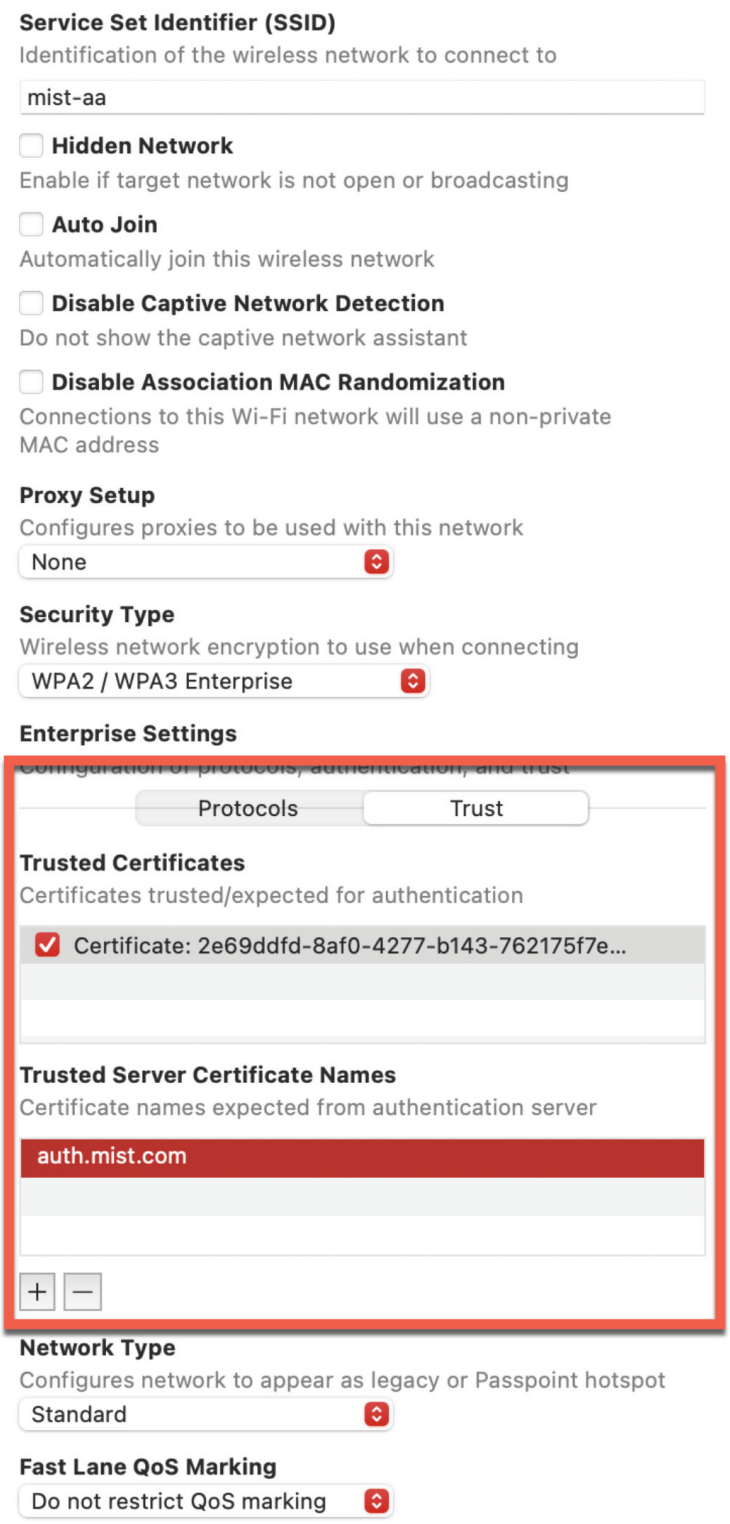
Figure 79: Wi-Fi Profile Configuration Settings



4. On the same page, under **Enterprise Settings** next to **Protocols**, click **Trust**. The page displays a list of uploaded certificates.

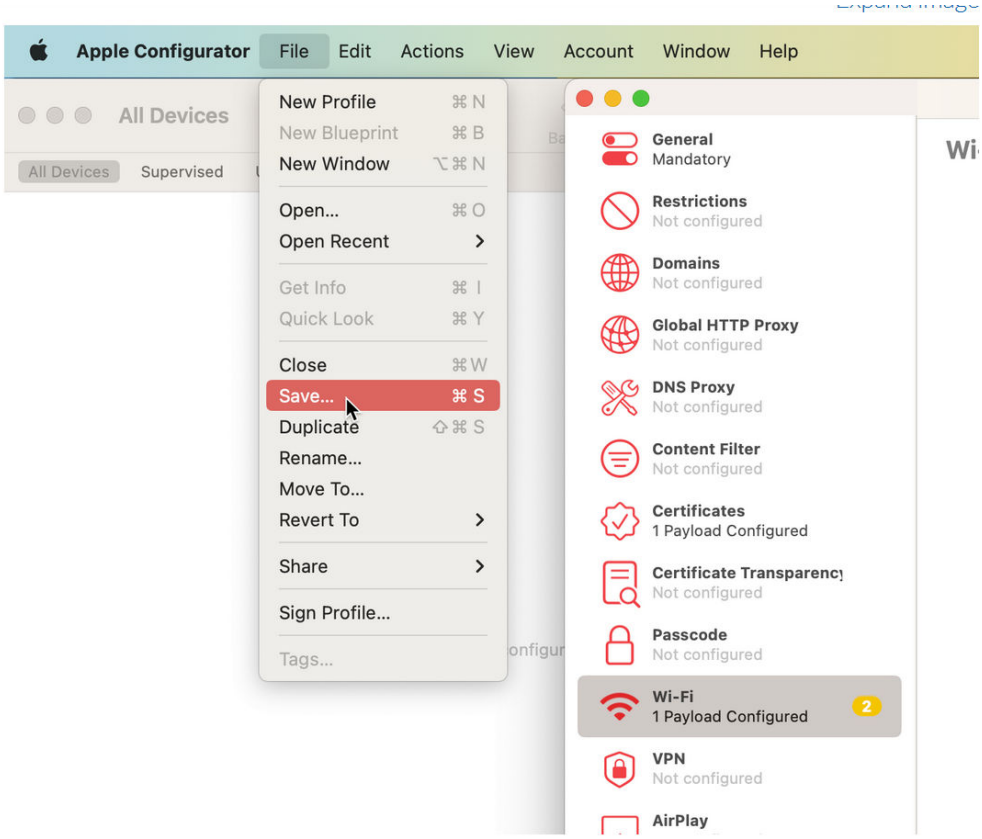
Select the Juniper Mist CA certificate and enter **auth.mist.com** under **Trusted Server Certificate Name**. This step enables the client device to trust the Juniper Mist Access Assurance Server.

Figure 80: Trust Juniper Mist CA Certificate in Wi-Fi Profile



5. Save the profile configuration.

Figure 81: Save Wi-Fi Profile Configuration



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

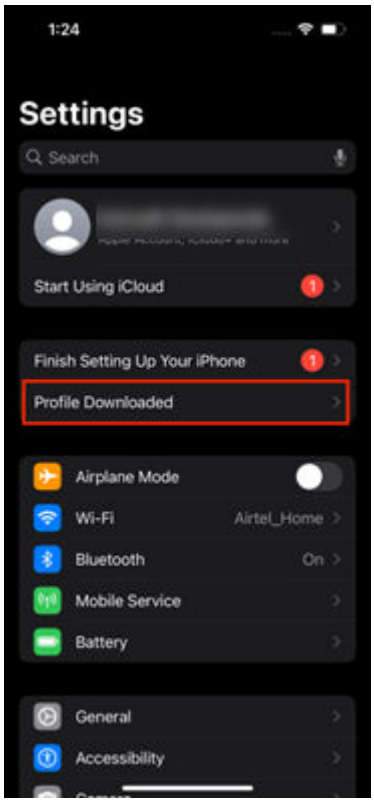
Now you can install the profile on to your macOS device and connect to SSID through EAP-TTLS.

For iOS and iPadOS

To test EAP-TTLS on an iPhone or iPad, you can export the configured Wi-Fi profiles from your macOS device and share them via AirDrop. Once received, install these profiles on the iOS device to connect using EAP-TTLS with PAP authentication.

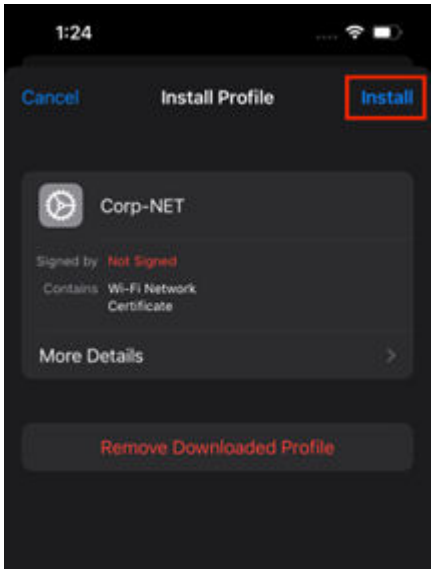
1. On your iOS device, open the Settings app and tap **Profile Downloaded**.

Figure 82: Locate Profile



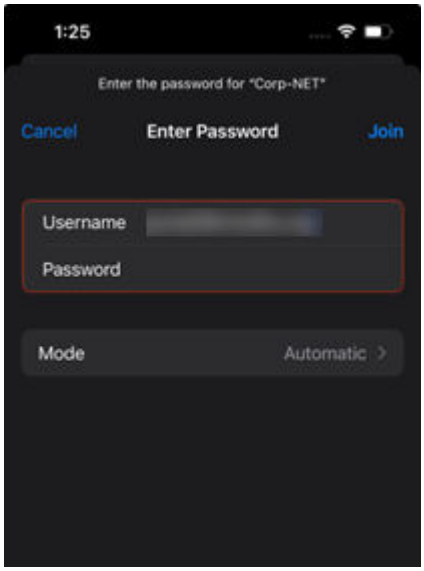
2. Tap **Install** in the upper-right corner of the screen.

Figure 83: Install Profile



3. Follow the on-screen instructions to complete the installation process.
4. Enter username and password and click **Join** connect wireless network.

Figure 84: Connect Wireless Network

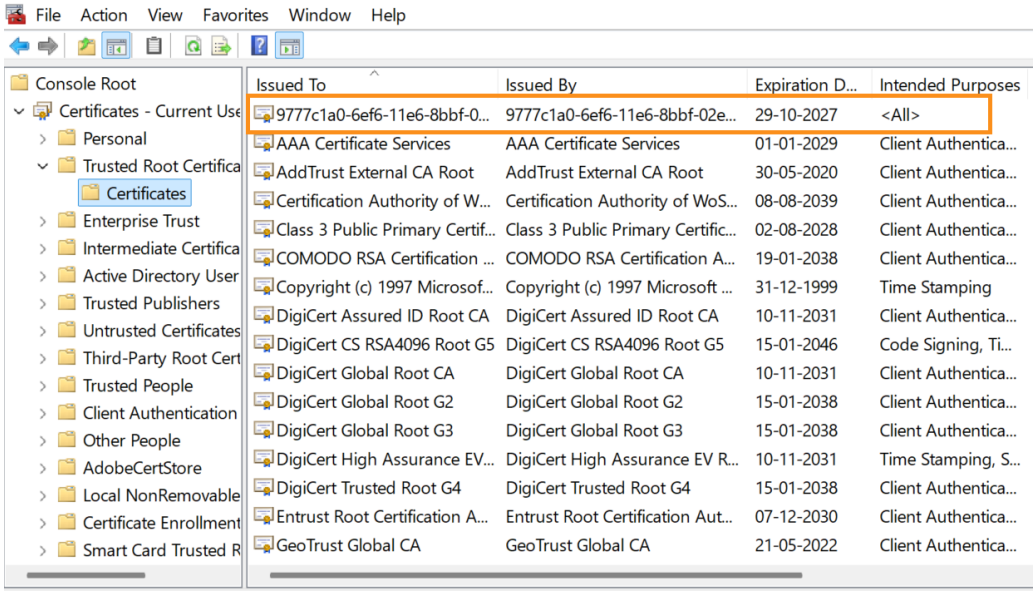


Configure Windows Device for EAP-TTLS Authentication

Use the following steps to configure a Windows device for EAP-TTLS authentication.

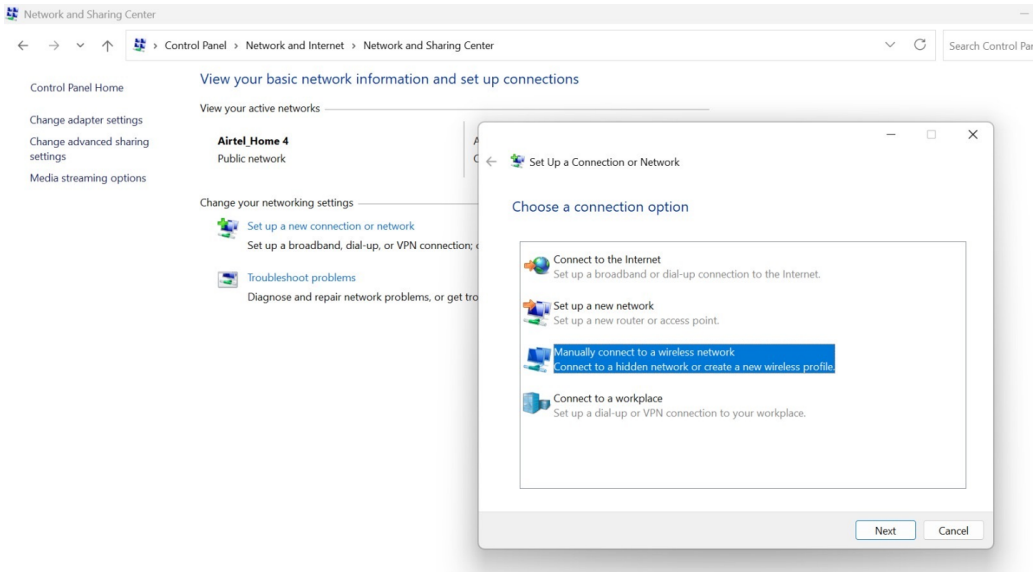
1. Download the Juniper Mist Org CA certificate (as mentioned in "Prerequisites" on page 198) and import the Mist Org CA Certificate on to your Windows device under **Manage Computer Certificates > Trusted Root Certification Authorities**.

Figure 85: Trusted Root Certificates on Windows Device



2. On your Windows device, go to **Control Panel > Network and Sharing Center > Set up a new connection or network** and select **Manually connect to a wireless network** and Click **Next**.

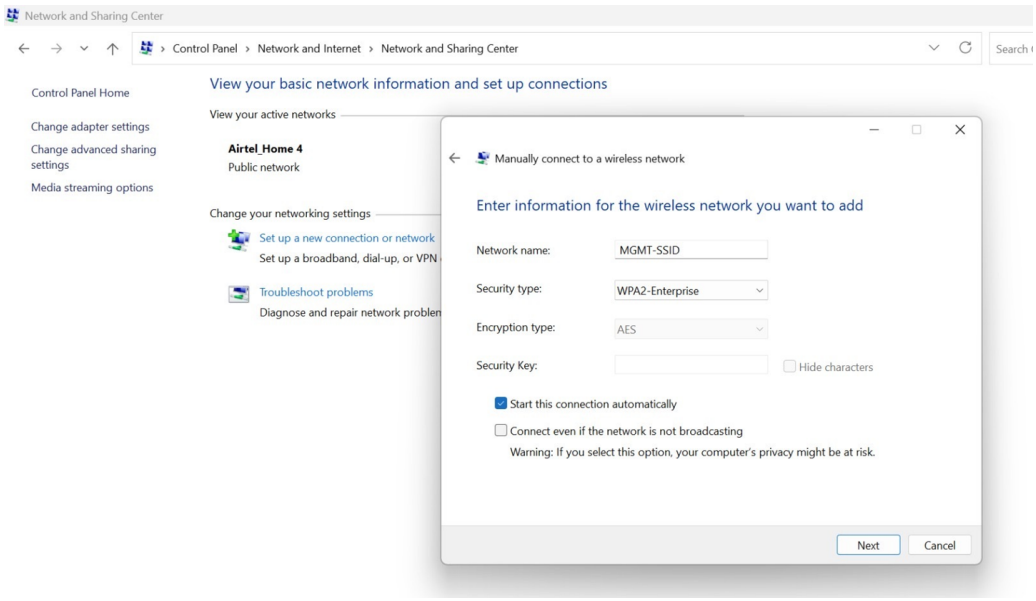
Figure 86: Setup New Connection



3. In the **Enter information for the wireless network you want to add**, provide the following details:
   - **Network name**— Provide an SSID name.

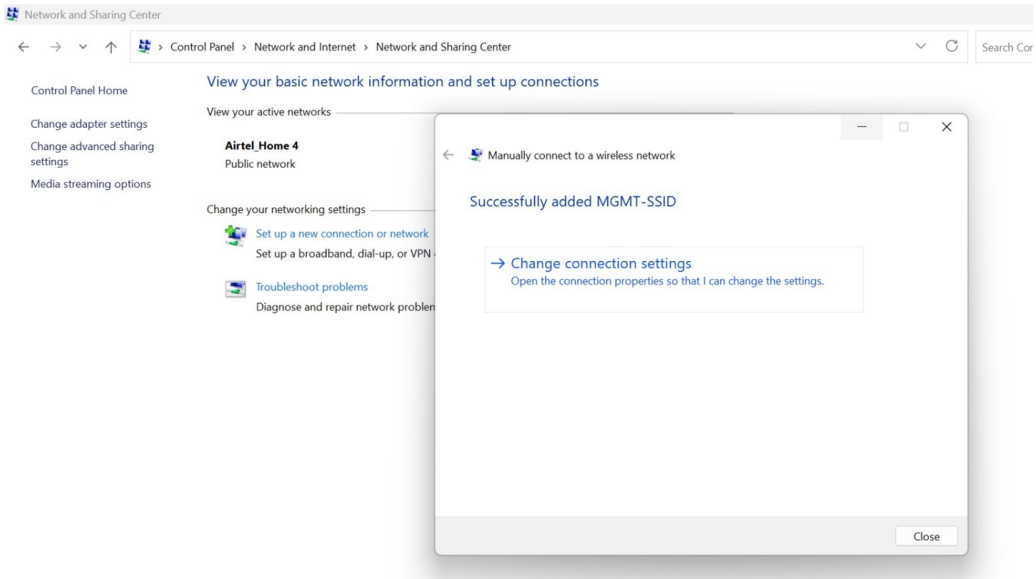
- **Security type**—Select the WPA2-Enterprise or WPA3-Enterprise option.

Figure 87: Enter Information for Wireless Network



When you click **Next**, a confirmation message appears stating that your SSID has been successfully added.

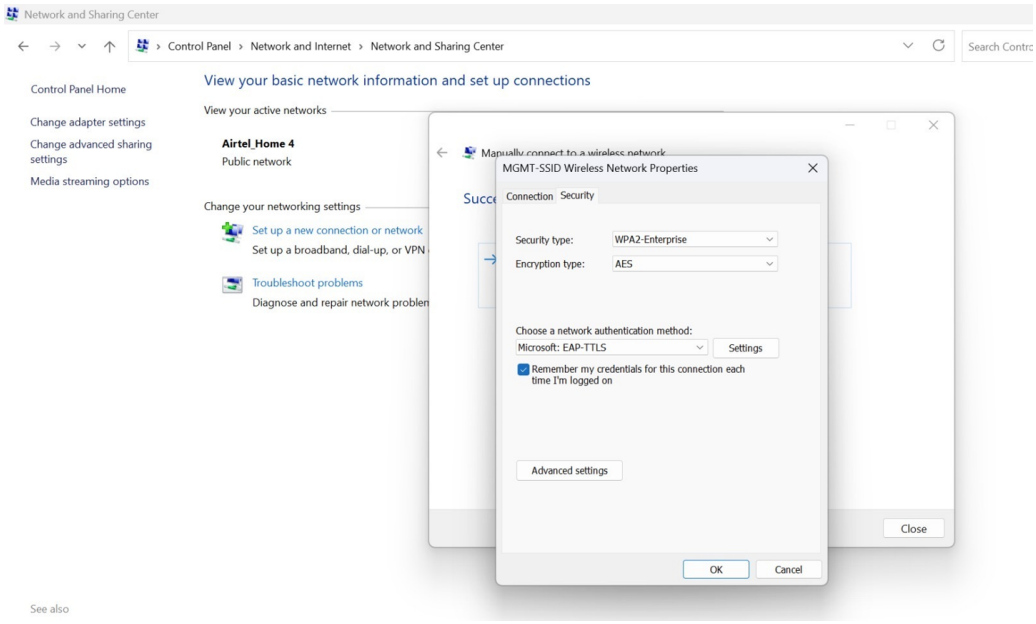
Figure 88: Configure Wireless Network: Connection Settings



Click **Change connection settings**.

4. Go to the Security tab, and under **Choose a network authentication method**, select **Microsoft: EAP-TTLS** and click Settings.

Figure 89: Configure Wireless Network Properties

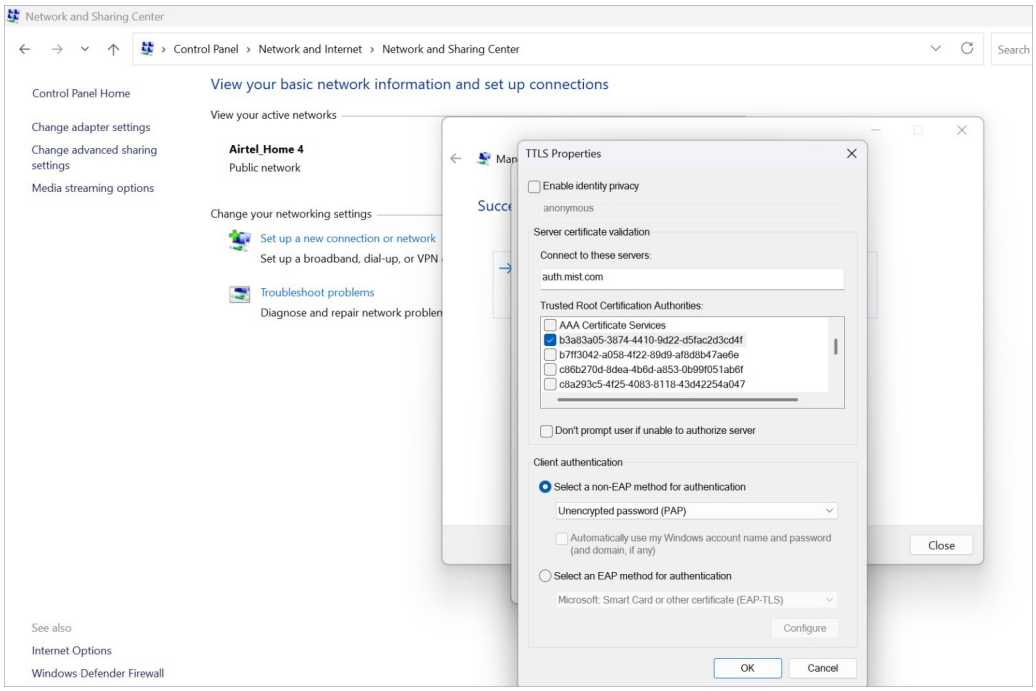


5. In the **TTLS Properties** window, perform following actions:

   - Disable the **Enable Identity Privacy** option.
   - For the **Connect to these servers**, enter `auth.mist.com`
   - Under **Trusted Root Certification Authorities**, select the **Mist Org CA** certificate or Root CA of your custom RADIUS server certificate.
   - For **Select a non-EAP method for authentication**, select **Unencrypted password (PAP)**

   .

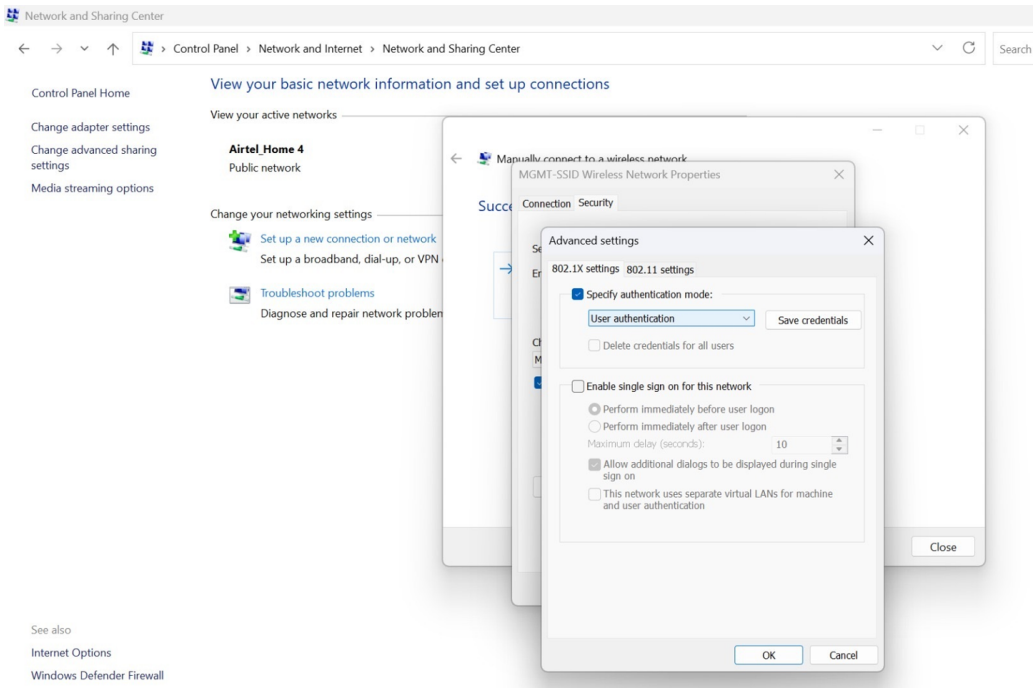
Figure 90: Configure Wireless Network: TTLS Properties



Click **OK**.

6. Back in the Security tab, click **Advanced settings**.
   - Check **Specify authentication mode** and select **User Authentication** option.
   - Click **OK**, then **Close** to complete your configuration.

Figure 91: Configure Wireless Network: Advance Settings

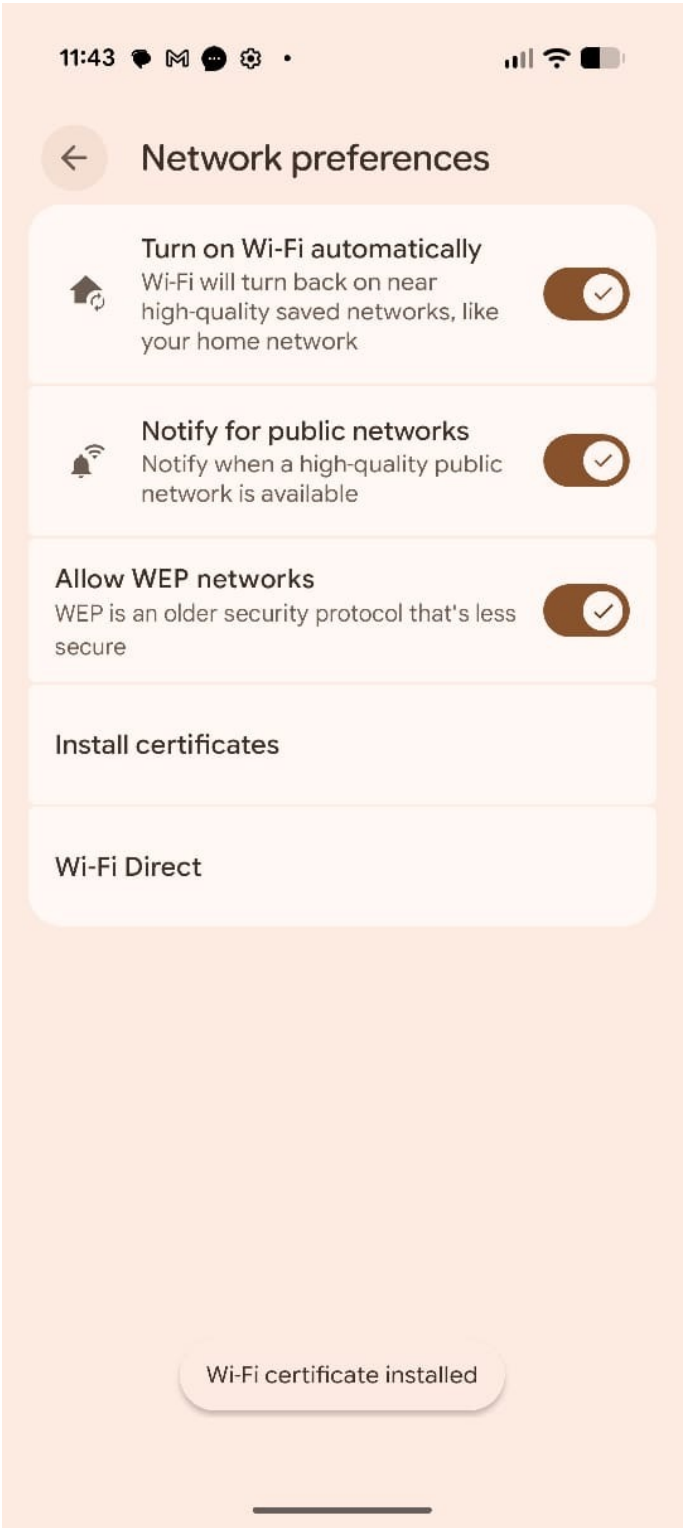


Configure Android Device for EAP-TTLS Authentication

Use the following steps to configure an Android device for EAP-TTLS authentication. Navigation steps may vary slightly depending on the device model; the example provided here is based on a Google Pixel 9.

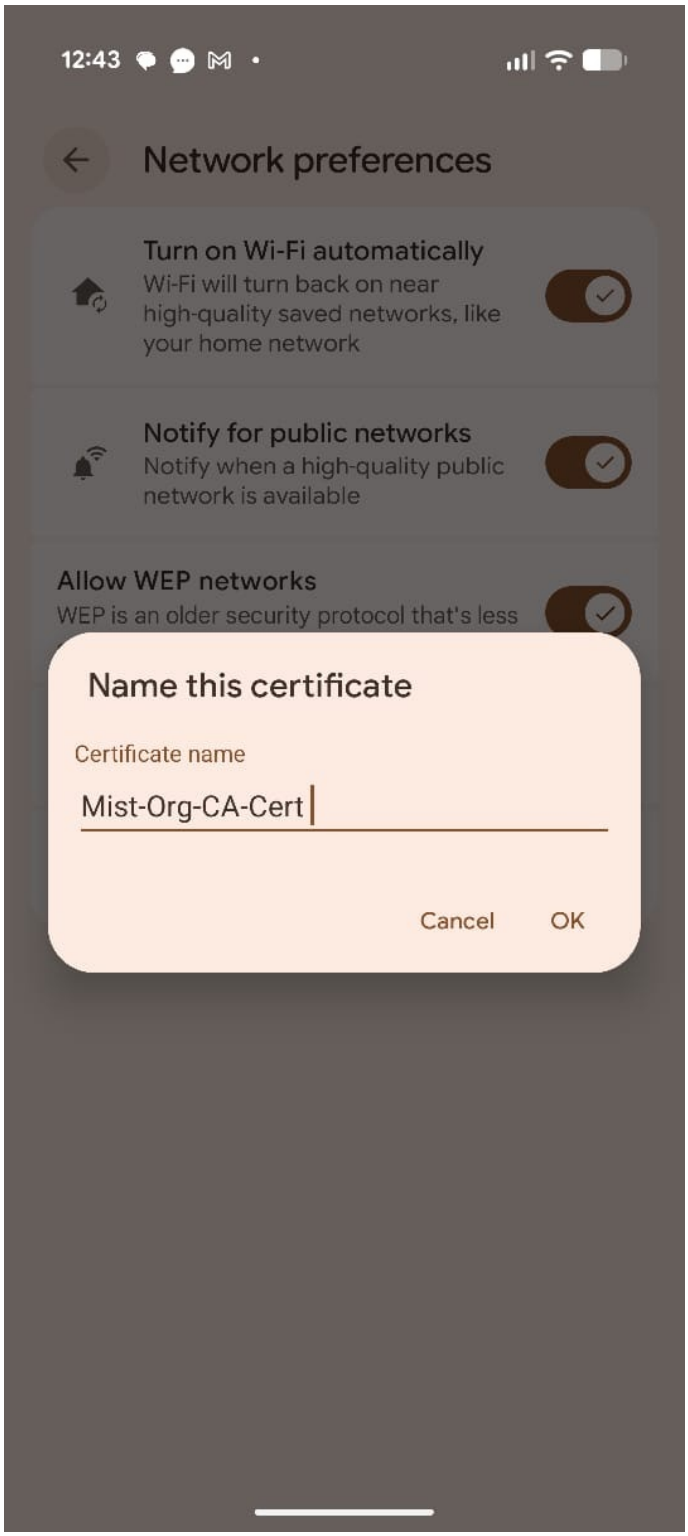
1. Download the Mist Org CA Cert and saved to your device's storage.
2. Open the **Settings** app on your Android device and navigate to **Settings > Network and Internet> Internet > Network Preferences**. Click **Install Certificates**.

Figure 92: Install Certificate



3. From the internal storage upload the Mist Org CA certificate and enter the name of the certificate. If you are using a custom RADIUS server certificate, choose the Root CA corresponding to that server instead of the Mist Org CA.

Figure 93: Enter Certificate Name



4. Once the CA certificate is downloaded and installed, click on the SSID and configure the connection as follows:

   - **EAP Method**: TTLS
   - **Phase 2 Authentication**: PAP
   - **CA Certificate:** Select the **Org CA Certificate**
   - **Domain**: Enter `auth.mist.com`.
   - **Credentials**: Enter the **Username** and **Password**.

Figure 94: Configure Wireless Network

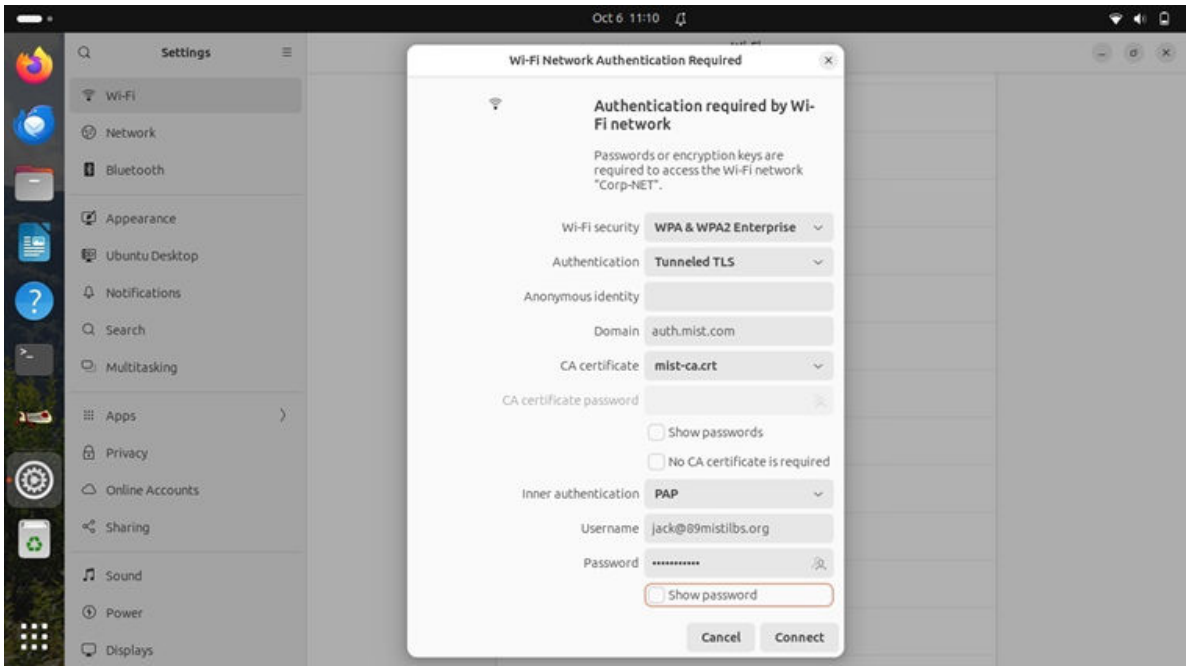
Click **Connect** to complete the configuration.

Configure Linux Device for EAP-TTLS Authentication

Use the following steps to configure EAP-TTLS authentication on a Linux (Ubuntu) device:

1. Open the network settings and click on the SSID to be connected.

Figure 95: Wireless Network Configuration

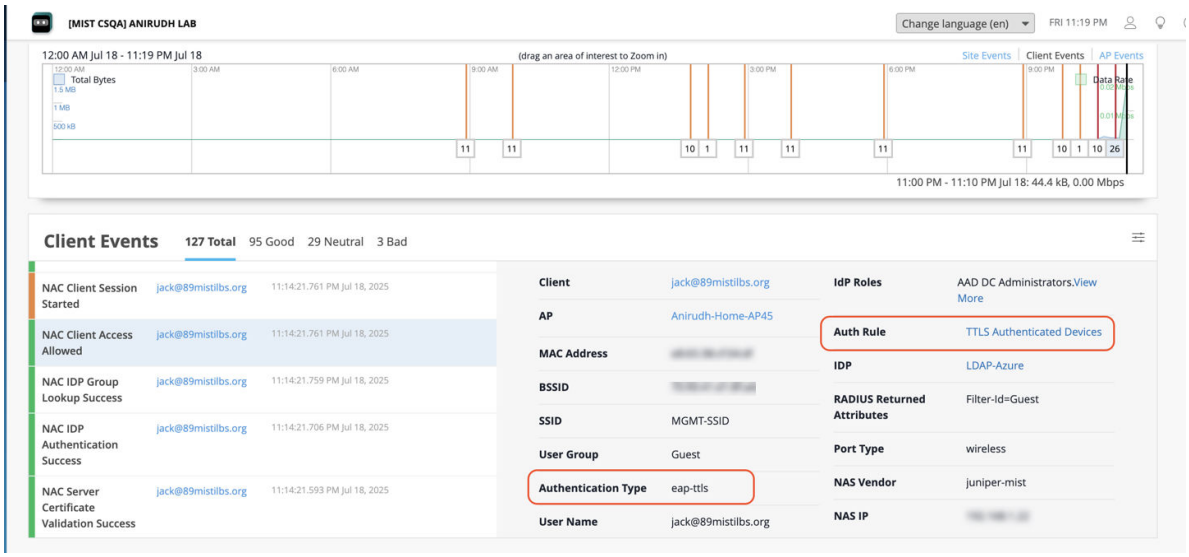


2. Under **Wi-Fi Security**, choose **WPA & WPA2 Enterprise**.
3. For **Authentication**, select **Tunneled TLS (EAP-TTLS)**.
4. Set the **Domain** field to: **auth.mist.com**
5. For the **CA certificate**, select the Mist Org CA certificate that was previously downloaded. If you are using a custom RADIUS server certificate, choose the Root CA corresponding to that server instead of the Mist Org CA.
6. Set **Inner authentication** (or Phase 2 Authentication) to **PAP**.
7. Enter the **Username** and **Password** provided for authentication.
8. Click **Connect** to complete the configuration.

Client Connection and Verification

1. Connect your client device to the network with the username and password.
2. In the Juniper Mist portal, navigate to **Monitor > Service Levels > Insights**. Under the Client Events section, view NAC client authentication events.

Figure 96: NAC Client Authentication Events



RELATED DOCUMENTATION

Configure Authentication Policy | 141

Configure Authentication Policy Labels | 144

Use Digital Certificates | 135

Configure Certificate-Based (EAP-TLS) Authentication | 164

Configure Certificate-Based (EAP-TLS) Authentication with Azure IdP Integration | 183

Configure EAP-TEAP Authentication for a Windows Device

SUMMARY

To secure your network, follow these steps to configure a client device for EAP-TEAP (Tunneled Extensible Authentication Protocol) authentication.

Tunneled Extensible Authentication Protocol (TEAP) 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)

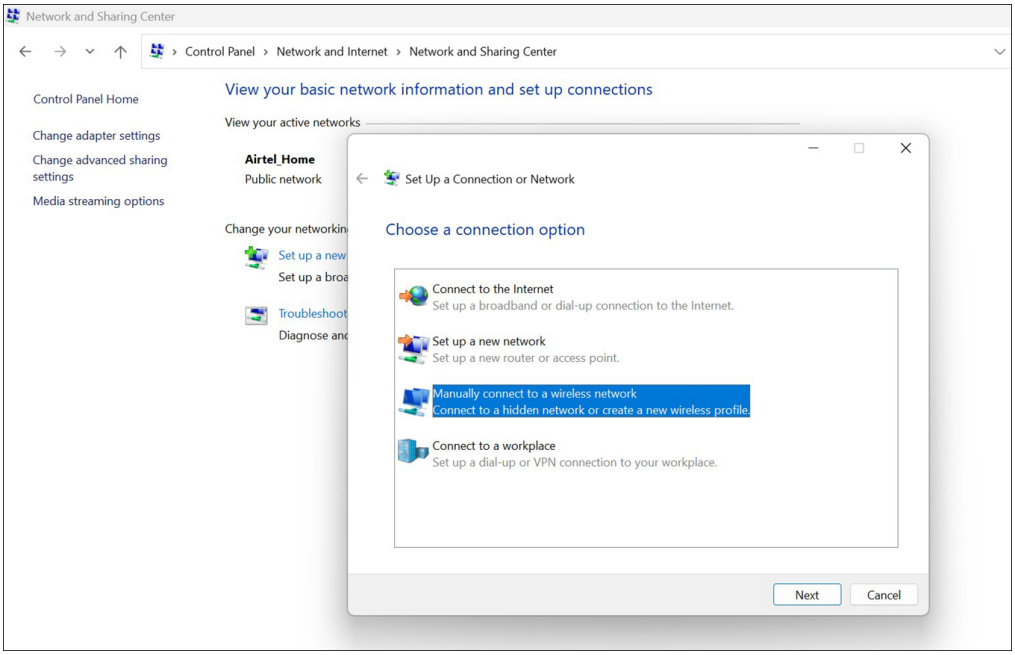
NOTE: Juniper Mist Access Assurance supports EAP-TEAP, requiring mandatory machine and user authentication, with EAP-TLS as the authentication method for both.

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.

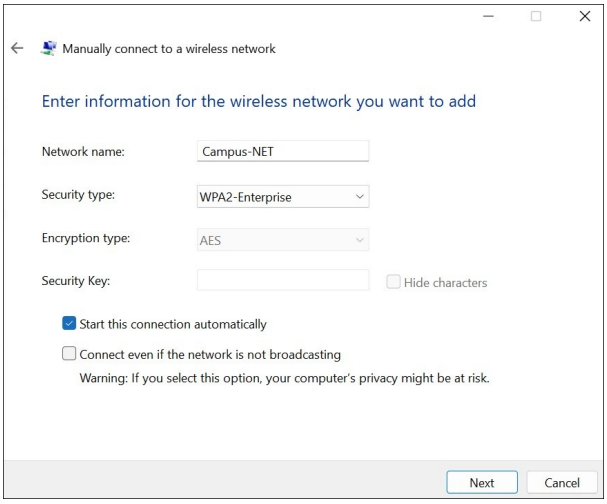
To configure EAP-TEAP on a Windows device:

1. On your Windows device, navigate to **Control Panel** > **Network and Internet** > **Network and Sharing Center**. Then, click **Set up a new connection or network**.
2. Select **Manually connect to a wireless network** and click **Next**.

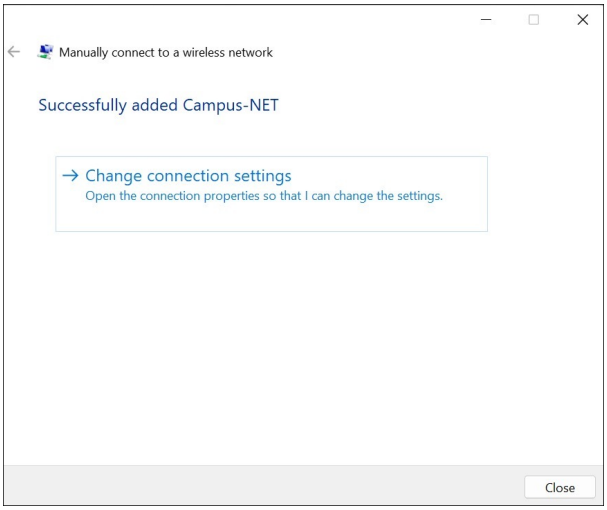


3. Enter the following details for the wireless network and click **Next**:

   - **Network name**—Provide an SSID name.
   - **Security type**—Select the **WPA2-Enterprise** or **WPA3-Enterprise** option.

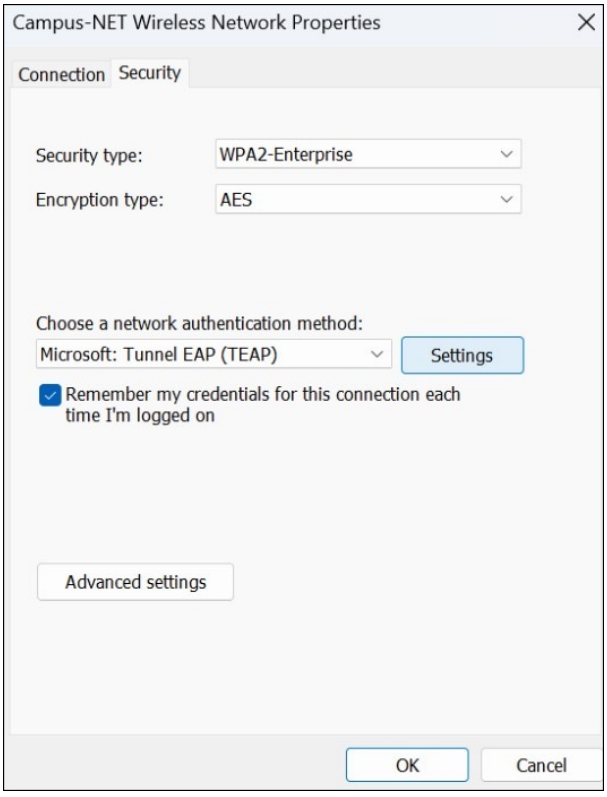


4. Click **Change connection settings**.



The Wireless Network Properties dialog box appears.

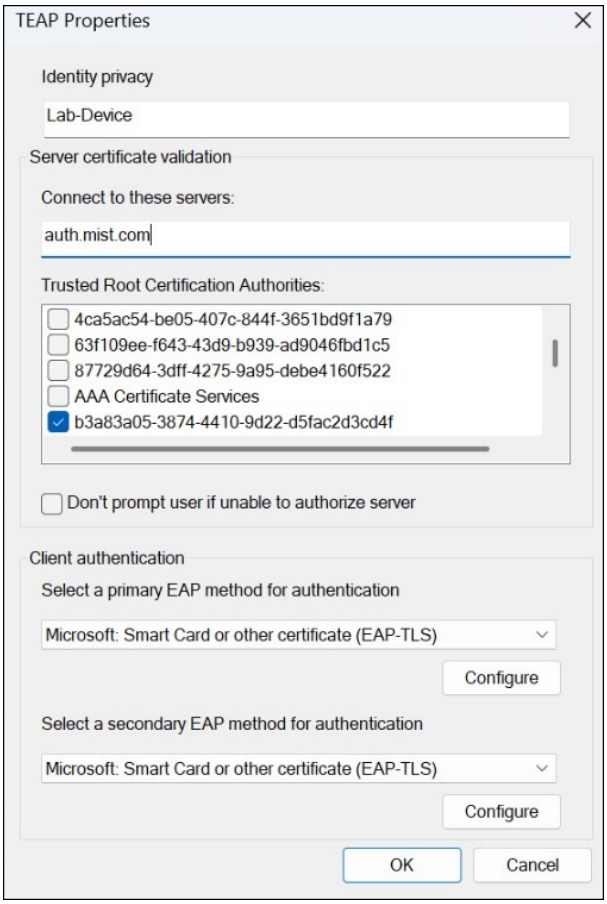
5. Select the **Security** tab and select TEAP under **Choose a network authentication method**. Then, click **Settings**.



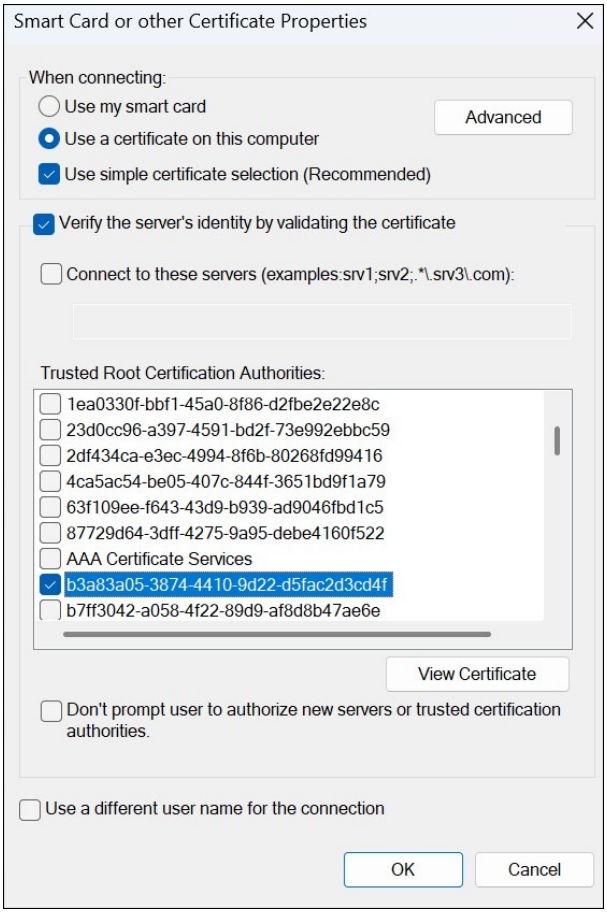
6. Select the following options in the TEAP Properties dialog box:

   - **Identity privacy**—The Identity is set to anonymous by default, but you can override it to the desired identity if necessary.

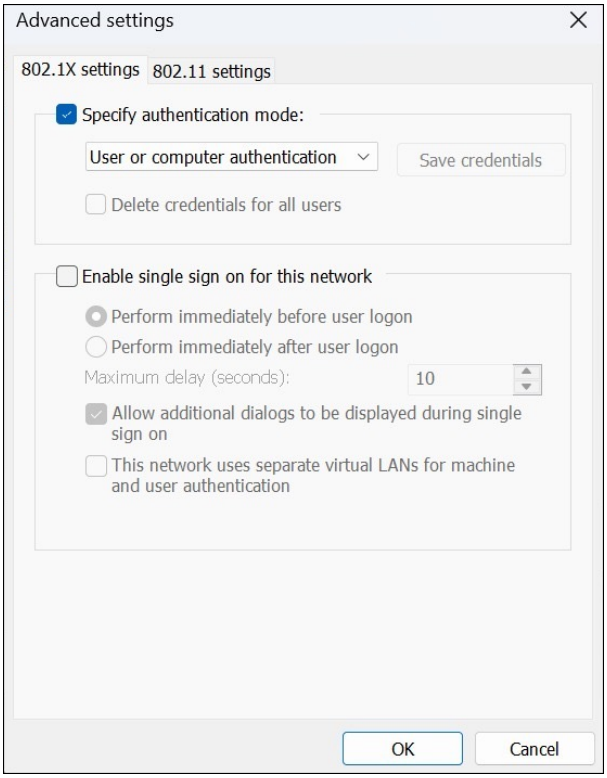
- **Connect to these servers**—Enter **auth.mist.com** if you're using the default Mist Access Assurance server certificate. If you're using a custom RADIUS server certificate, provide the certificate SAN:DNS name.
- **Trusted Root Certification Authorities**—Select the Mist Org CA certificate (or your custom RADIUS server certificate).
- **Authentication Method**—Select **Microsoft: Smart Card or other certificate (EAP-TLS)** as the Primary and Secondary EAP methods for authentication.



7. Click **Configure** for both the primary and secondary EAP methods. In the Smart Card or other certificate Properties dialog box that appears for each:
   - Ensure that the **Use simple certificate selection (Recommended)** option is selected.
   - Select the trusted root Certificate Authority (CA) that enables the client to trust the Mist Access Assurance server certificate. Ensure that you select the same CA for both the primary and secondary EAP methods
   - Click **OK**.

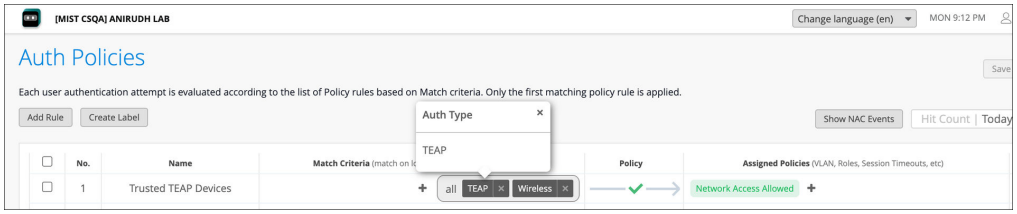


8. In the Security tab of the Wireless Network Properties dialog box, click **Advanced settings**.
9. In the Advanced settings dialog box:
   a. Select the **Specify authentication mode** check box and choose **User or Computer authentication**.
   b. Click **OK** and then click **Close**.



10. Verify the configuration:

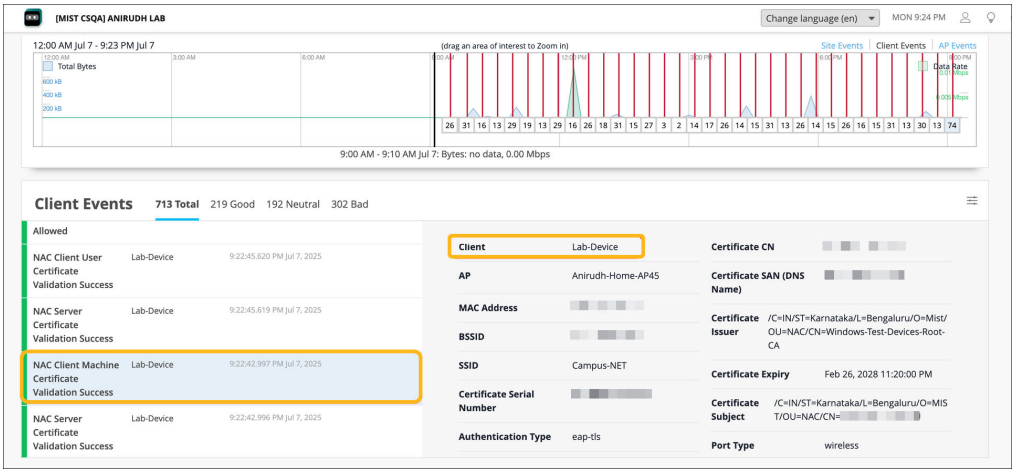
    a. In the Juniper Mist portal, create an authentication policy. Add a rule to allow the TEAP Auth Type.

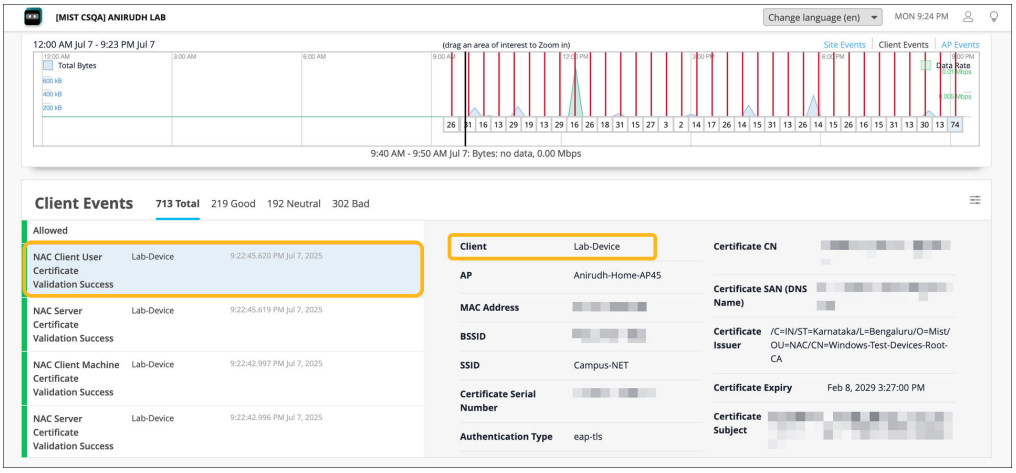


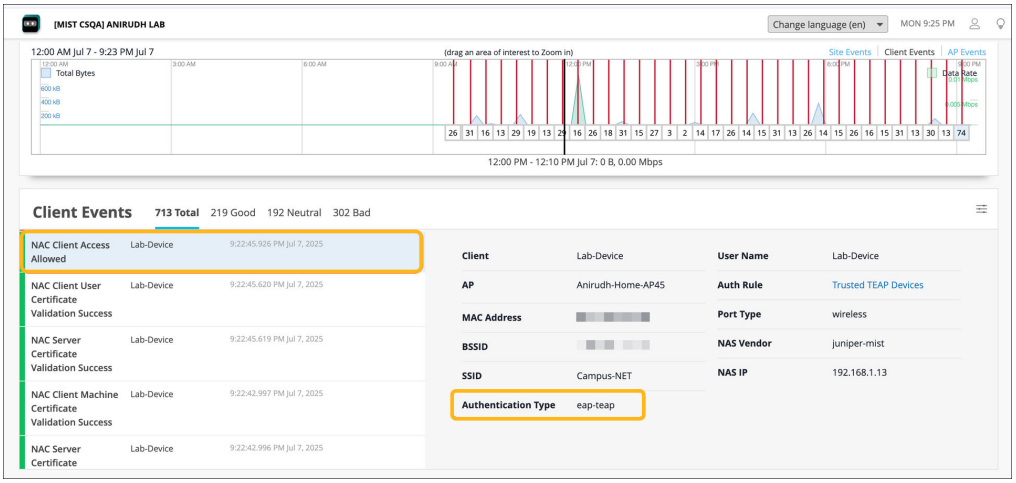
    b. Add the CA certificate to enable Juniper Mist Access Assurance to trust client certificates issued by your added CAs. To add the certificate, navigate to the **Organization** > **Access** > **Certificates**> **Add Certificate Authority** page. For detailed steps about adding a CA certificate, see "Use Certificate Authority (CA) Certificate" on page 136.

    c. Connect the client device to the network.

    d. Navigate to the **Monitor** > **Service Levels** > **Insights** page and go to the Client Events section. Verify the NAC Client authentication events.







RELATED DOCUMENTATION

Configure Authentication Policy | 141

Configure PEAP-EAP-TLS Authentication for a Windows Device

SUMMARY

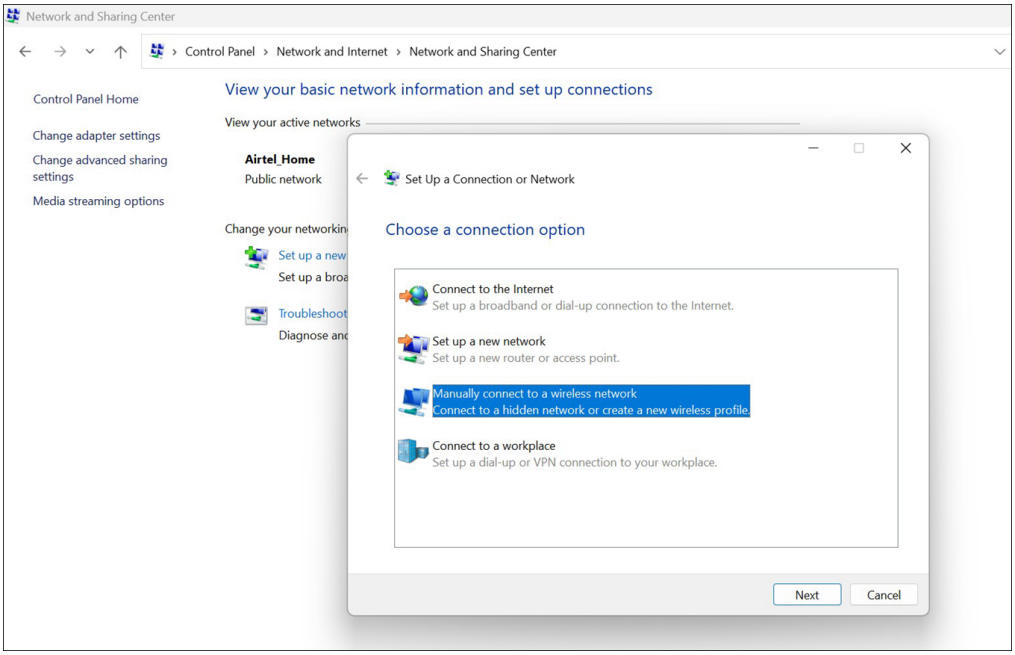
Follow these steps to configure a Windows client device for Protected Extensible Authentication Protocol (PEAP) authentication with EAP-TLS as the inner authentication method.

The Protected Extensible Authentication Protocol (PEAP) uses a tunneled EAP method for the authentication process. PEAP uses Transport Layer Security (TLS) to establish a secure, encrypted tunnel between a client and an authentication server. It encapsulates the EAP authentication process within this tunnel, thus enabling secure exchange of authentication data between the client and server.

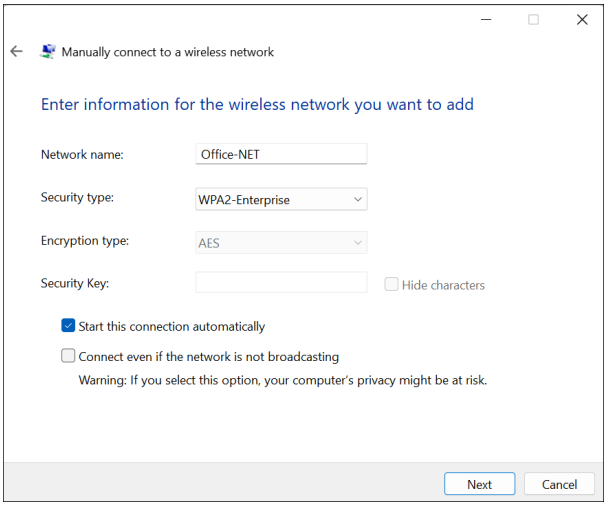
NOTE: Juniper Mist Access Assurance supports PEAP with EAP-TLS authentication only; PEAP with EAP-MSCHAP v2 is not supported.

PEAP-EAP-TLS uses EAP-TLS as the inner authentication method within the secure tunnel. EAP-TLS requires both client and server certificates for mutual authentication. To configure PEAP-EAP-TLS on a Windows device:

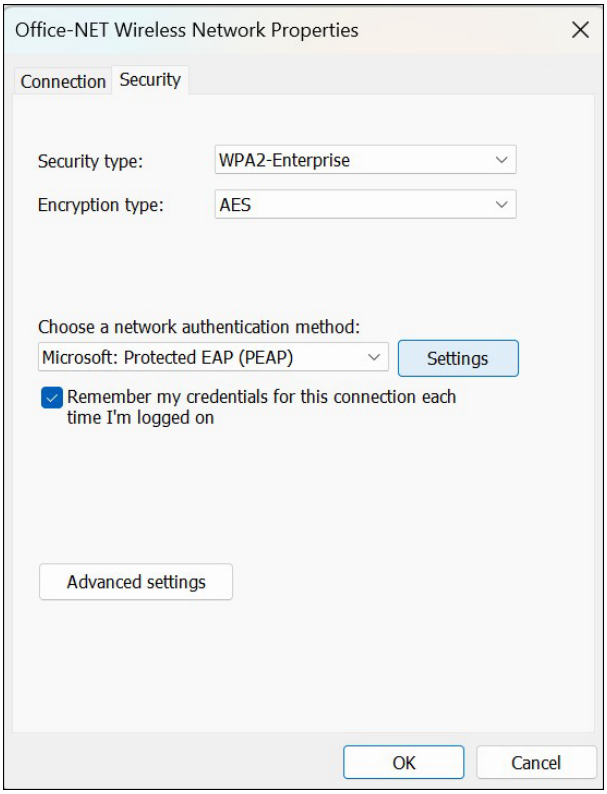
1. On your Windows device, navigate to **Control Panel** > **Network and Internet** > **Network and Sharing Center**. Then, click **Set up a new connection or network**.
2. Select **Manually connect to a wireless network** and click **Next**.



3. Enter the following details for the wireless network and click **Next**:
   - **Network name**—Provide an SSID name.
   - **Security type**—Select the **WPA2-Enterprise** or **WPA3-Enterprise** option.



4. Click **Change connection settings**.
   The Wireless Network Properties dialog box appears.
5. Select the **Security** tab and click **Settings** under **Choose a network authentication method**.

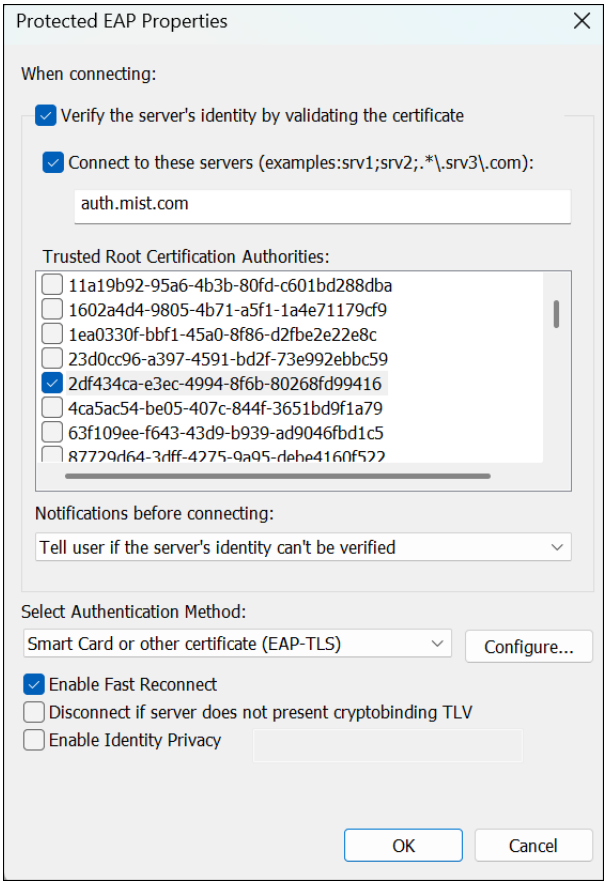


6. Select the following options in the Protected EAP Properties dialog box:

   - **Connect to these servers**—Enter **auth.mist.com** if you're using the default Mist Access Assurance server certificate. If you're using a custom RADIUS server certificate, provide the certificate SAN:DNS name.

   - **Trusted Root Certification Authorities**—Select the Mist Org CA certificate (or your custom RADIUS server certificate).

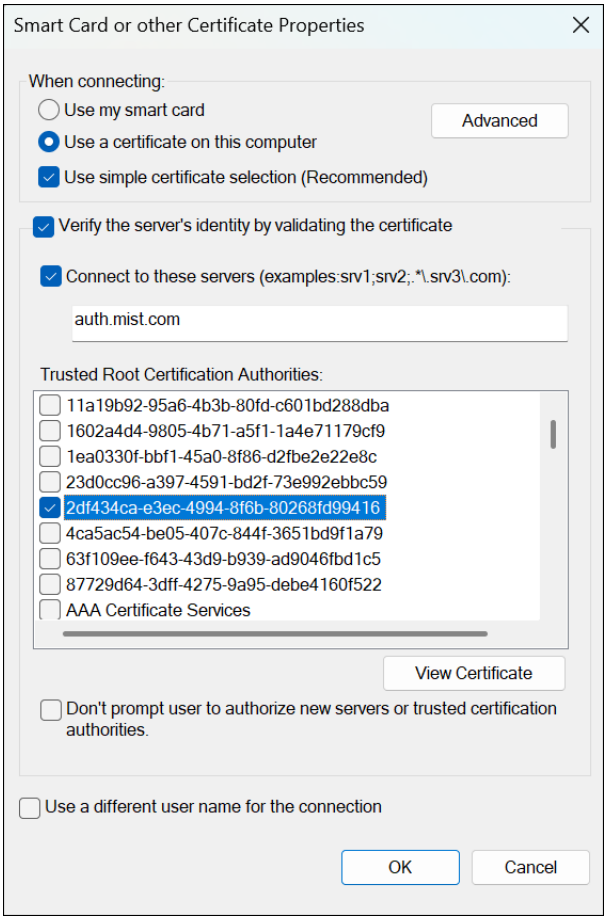
   - **Authentication Method**—Select **Smart Card or other certificate (EAP-TLS)**



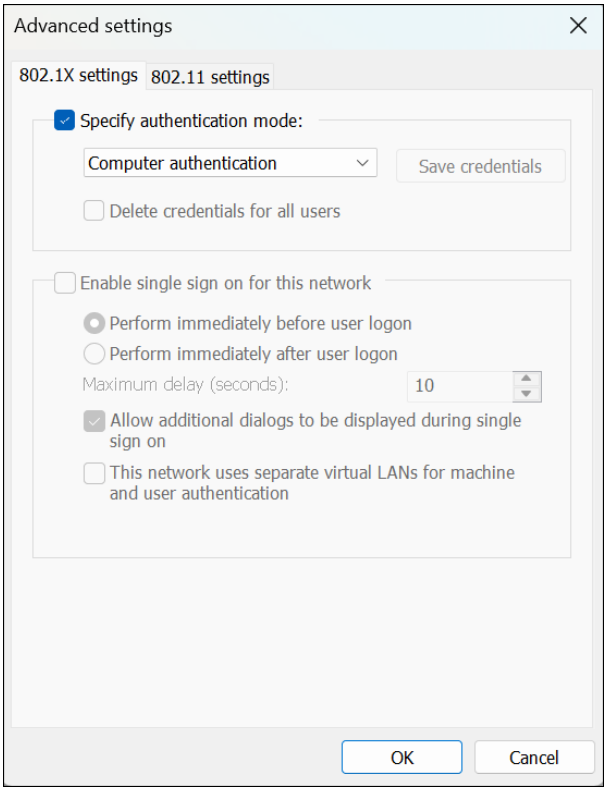
Click **Configure**.

The Smart Card or other certificate Properties dialog box appears.

7. Verify that the server is listed as **auth.mist.com**. Select the Mist Org CA certificate and click **OK**.

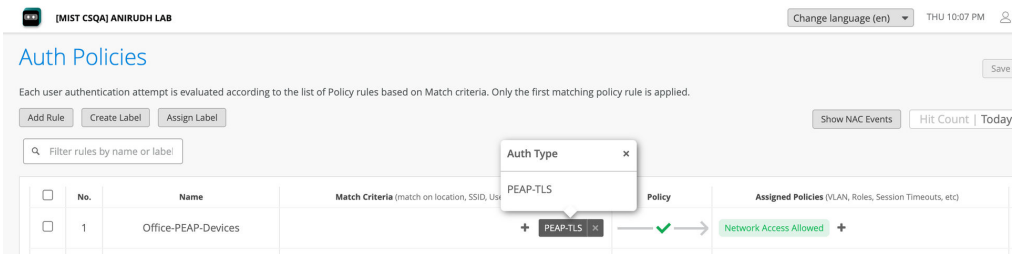


8. In the Security tab of the Wireless Network Properties dialog box, click **Advanced settings**.
9. In the Advanced settings dialog box:
   a. Select the **Specify authentication mode** check box and choose the appropriate authentication mode.
   b. Click **OK** and then click **Close**.



10. Verify the configuration:

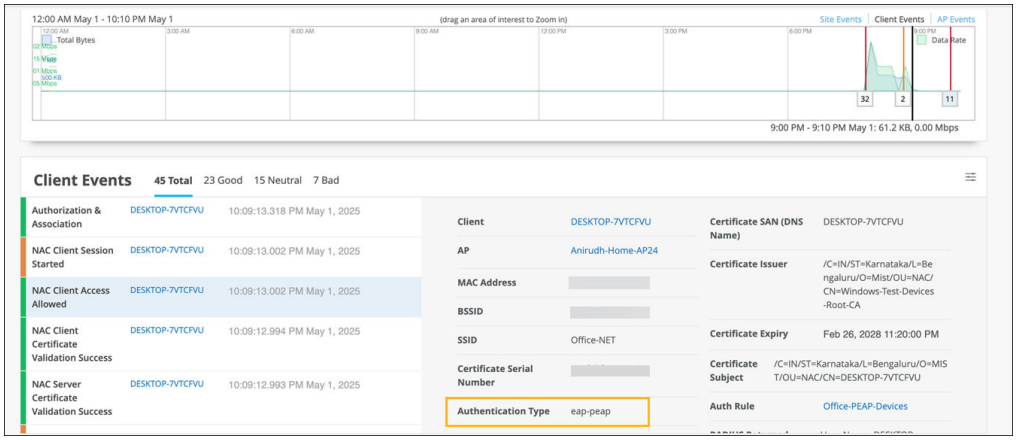
    a. In the Juniper Mist portal, create an authentication policy. Add a rule to allow the PEAP-TLS Auth Type.



    b. Add the CA certificate to enable Juniper Mist Access Assurance to trust client certificates issued by your added CAs. To add the certificate, navigate to the **Organization** > **Access** > **Certificates**> **Add Certificate Authority** page. For detailed steps about adding a CA certificate, see "Use Certificate Authority (CA) Certificate" on page 136.

    c. Connect the client to the network.

    d. Navigate to the **Monitor** > **Service Levels** > **Insights** page and go to the Client Events section. Verify the NAC Client authentication events.



Self-provisioning for IoT and Personal Devices

SUMMARY

Automate client onboarding at scale, for personal devices and IoT, with secure self provisioning.

IN THIS SECTION

Wireless users in environments like dormitories can securely self-provision their personal devices such as Xboxes, Apple TV, and Roku. Likewise, unattended IoT devices can securely and automatically join a specified VLAN, or network segment. We call this the Personal Network Experience. And because it eliminates the need for client MAC address registration and IT intervention, it is an ideal solution for providing Wi-Fi access at scale.

Self provisioning with the Personal Network Experience works by connecting a SAML-compliant identity provider (IDP), for example, Microsoft Entra ID, to the Mist Active Assurance portal. Users log on to the WLAN, where they are redirected to the single-sign-on service for authentication and authorization. Mist assigns authenticated users a personal preshared key (PSK) that is specific to both the individual user and/or the SSID. Using personal PSKs also enables micro-segmentation, which means you can have users connect to a specific VLAN according to their role or profile. The same is true for IoT devices; they can be automatically connected to a specific VLAN, a best practice for protecting against IoT take-over attacks.

In the Mist console, you can configure both the complexity of the required passphrase, and the frequency of key rotation.

Figure 97: Self-Provisioning Logon Screen

During self-provisioning, laptop users can generate a unique passphrase, then copy and paste it into the portal when prompted. Or, if working from a mobile device, they can have the passphrase emailed to them. Generated passphrases expire after 24 hours.

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.

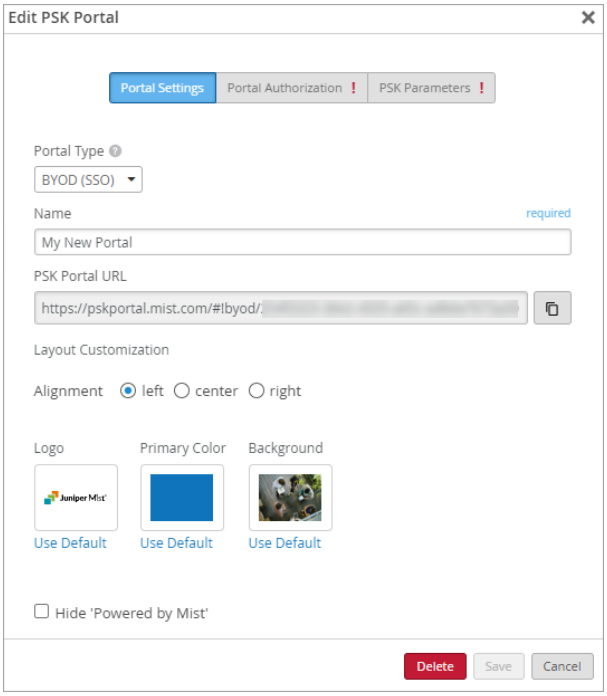
  Copy the following information from your SAML 2.0 app integration, and save it so that you can use it to set up your PSK portal in Juniper Mist.

  - Signing Algorithm
  - Issuer ID (this key may vary, for example, in Okta, this value is called *Identity Provider Issuer* and in Azure, it's called *Azure AD Identifier*.
  - SSO URL (this key may vary, for example, in Okta, this value is called *Identity Provider Single Sign-On URL* and 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.

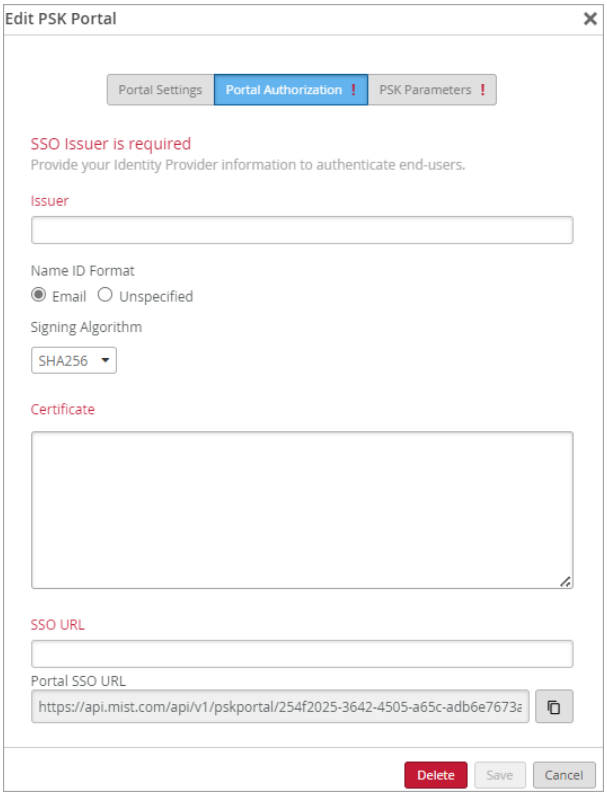
Configure Self-Provisioning

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.

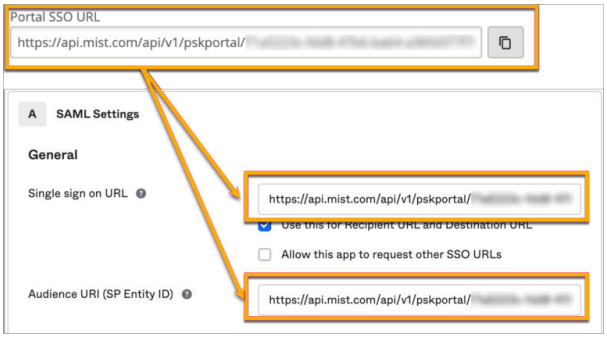
   c. Enter the copied value into the appropriate field to identify your Juniper Mist PSK portal to your IdP. For help, see your IdP documentation.

   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.

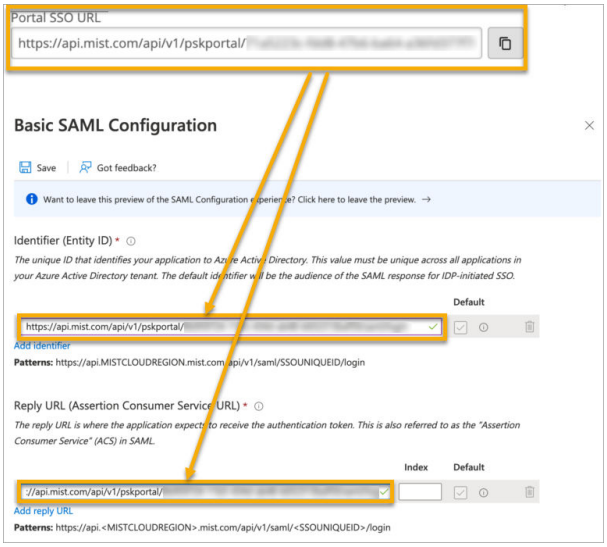
   Okta Example

   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.



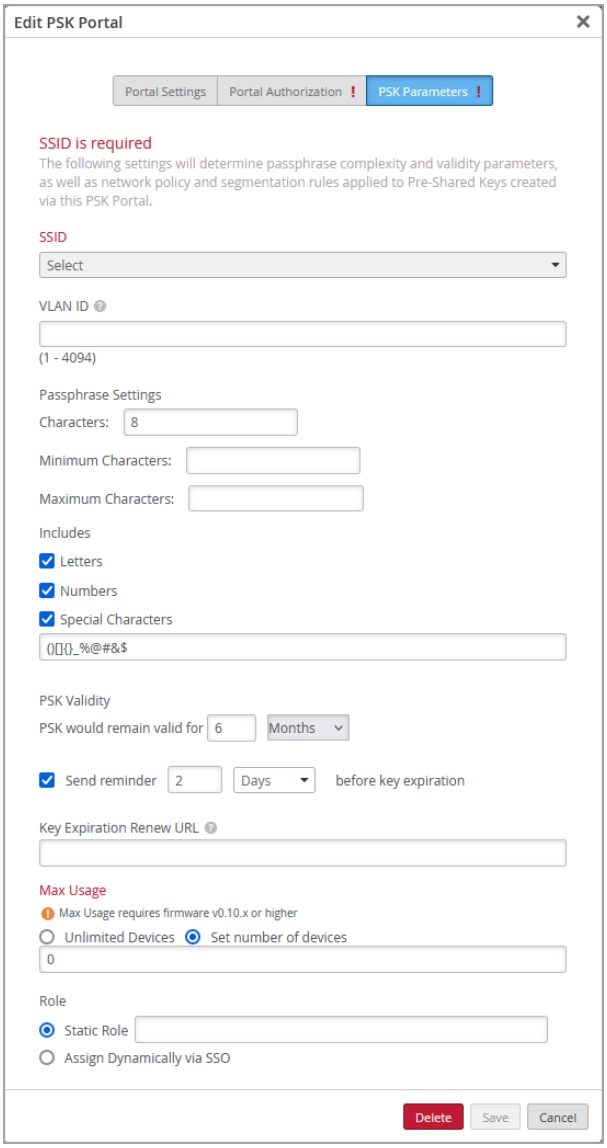
8. Return to the Juniper Mist portal.
9. On the **PSK Parameters** tab of the Edit PSK Portal window:
   - Select the **SSID** (required).

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

   - Adjust the optional settings as needed.

Table 12: Optional Settings

Option	Description
VLAN ID	Specify a ID if you want to assign this portal's users to a particular VLAN. The ID must exist in the VLAN list for the WLAN.
Passphrase Settings	Enter settings to enforce your policies for password complexity.
PSK Validity	You can set the key expiration period and 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 an single sign-on URL (for example, using your corporate identity provider URL through Okta or Microsoft Azure).
Max Usage	Enter the maximum number of devices that can connect to your portal.
Role	If you want to limit access to certain types of user accounts, specify the roles that are allowed to use the portal. These needs to be roles that you've set up for your IdP user accounts.



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.

Client Onboarding Through a NAC Portal Using the Marvis Client App

SUMMARY

Onboard your device to the Juniper Mist Access Assurance network securely by using Wi-Fi client certificates provisioned by the NAC onboarding portal through the Marvis Client app.

IN THIS SECTION

Onboarding a device through a Network Access Control (NAC) portal enables provisioning of Wi-Fi client certificates through the Marvis client app. The onboarding process uses the Onboard Mist Certificate Authority, which enables issuing of EAP-TLS client certificates to devices. These certificates are used by clients to authenticate to the Juniper Mist Access Assurance network using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).

The Marvis client app can be pre-installed on devices or downloaded directly from the NAC Onboarding Portal. The end user needs to authenticate to the NAC Onboarding Portal using their SSO credentials (Azure AD, Okta).

On successful authentication, the NAC portal (integrated with the enterprise IdP) provisions a device-bound X.509 client certificate and delivers a preconfigured Wi-Fi network profile, which should be installed within the Marvis Client app. Once the profile is installed, the app enables the device to seamlessly connect to the designated secure SSID using EAP-TLS.

This onboarding process eliminates manual PKI distribution and SSID configuration, while enforcing enterprise network access policies for unmanaged devices in a BYOD environment.

Benefits of Client Onboarding Through a NAC Portal

Onboarding a client through a NAC portal using the Marvis client app ensures secure, seamless, and password-less access to your organization's Wi-Fi network. Traditional Wi-Fi connections using usernames and passwords are vulnerable to misuse, leaks, and manual errors. The NAC onboarding

portal eliminates these risks by using certificate-based authentication issued only after validating your identity through your organization's Single Sign-On (SSO) system.

In addition to ease of use, onboarding provides enterprise-grade security for BYOD (Bring Your Own Device), guests, and contractors, eliminating the need for IT intervention for every connection.

Onboarding a device to a NAC portal using the Marvis client app provides the following benefits:

- A unique digital certificate tied to your identity and device.
- Automatic installation of a secure Wi-Fi profile, requiring no manual setup.
- Access governed by zero trust network policies defined in the Juniper Mist cloud.

You can onboard Android, Windows, macOS, and iOS devices. Onboarding is supported on devices running:

- Windows—Release 10 or 11
- macOS—Sonoma (version 14) and later releases
- Android—Android 12+
- iOS—16 and later release

Before You Begin

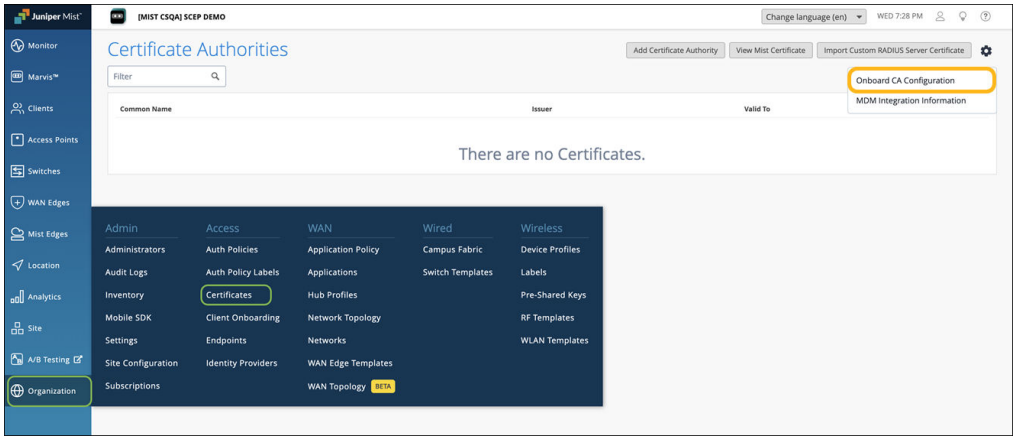
Before proceeding to onboard a device, ensure to

- Obtain and activate a Juniper Mist™ Access Assurance subscription. For information about subscription management, see the Juniper Mist Management Guide.
- Enable onboarding:

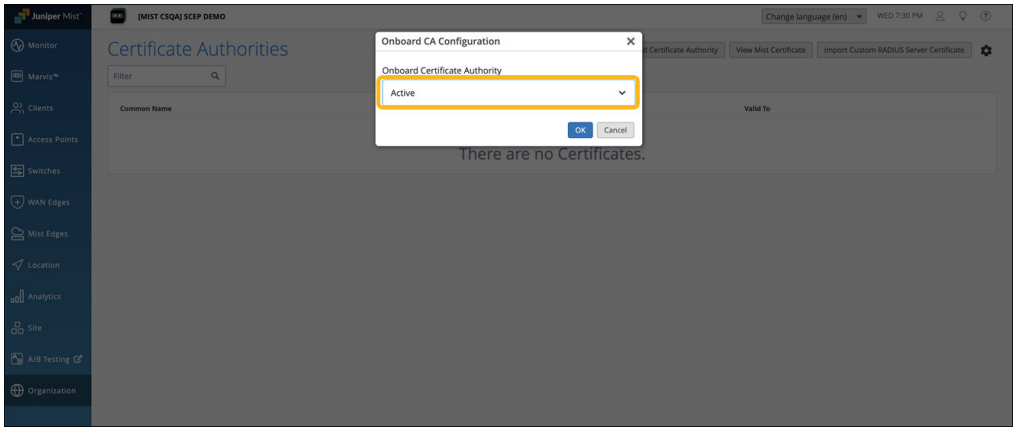
  1. From the left menu of the Juniper Mist portal, select **Organization** >**Access**>**Certificates**.

     The Certificate Authorities page appears.

  2. Click the settings icon on the upper-right corner of the page and select **Onboard CA Configuration**.

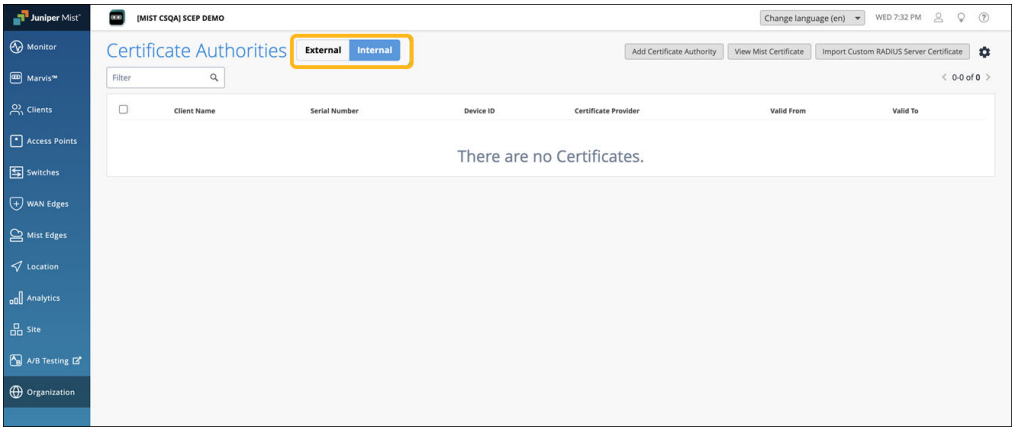


3. In the Onboard CA Configuration dialog box, select **Active** and click **OK** to enable the built-in CA to issue the client certificates.



When the Onboard CA Configuration is activated, you'll see the following tabs displayed:

- External—Displays the details of the external CAs.
- Internal— Displays the details of client certificates issued by the built-in CA through the NAC portal or MDM.



- Ensure that you have an IdP account with app integration capability. Your IdP can be any provider that supports SAML 2.0 integrations. Examples include Azure, Google, and Okta.

In this topic, we show you how to create a NAC portal and integrate it with Microsoft Azure and Okta.

How to Set Up a NAC Portal and Integrate It with Microsoft Azure

IN THIS SECTION

Setting up a NAC onboarding portal and integrating it with Azure involves the following steps:

Create a NAC Portal and Integrate It with Azure

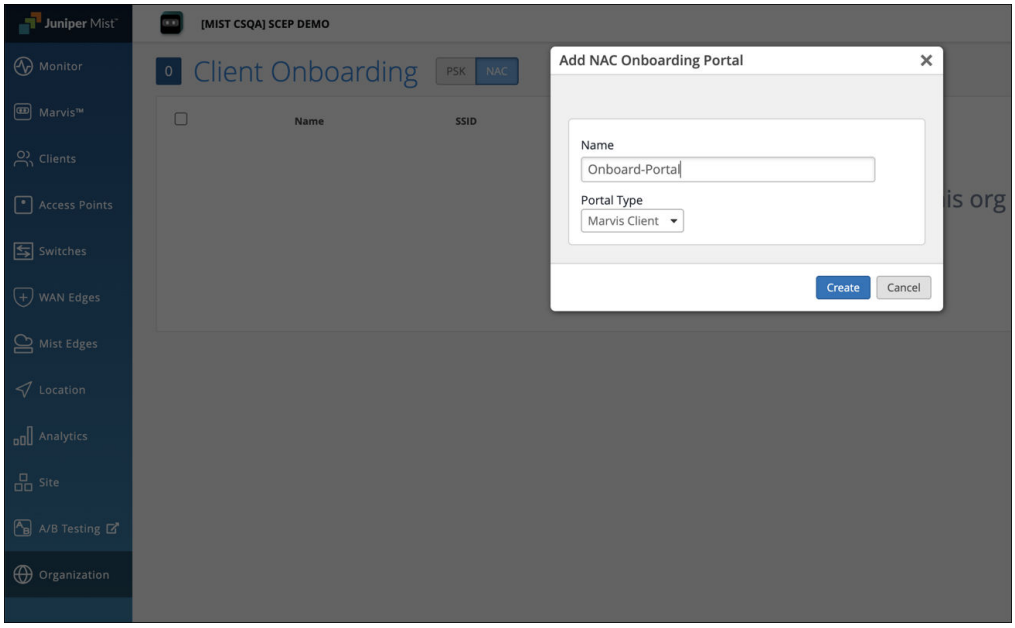
Ensure that the onboard CA configuration is enabled on the Certificates page. See "Before you Begin" on page 241.

1. Create a NAC portal. When you create the portal, a NAC portal URL will be generated for users to access using SSO.

   a. From the left menu of the Juniper Mist portal, select **Organization**>**Client Onboarding**, and select the **NAC** tab.

   b. Click **Add NAC Onboarding Portal** at the top-right corner of the Client Onboarding page.

   c. In the Add NAC Onboarding Portal page, provide a name and click **Create**.

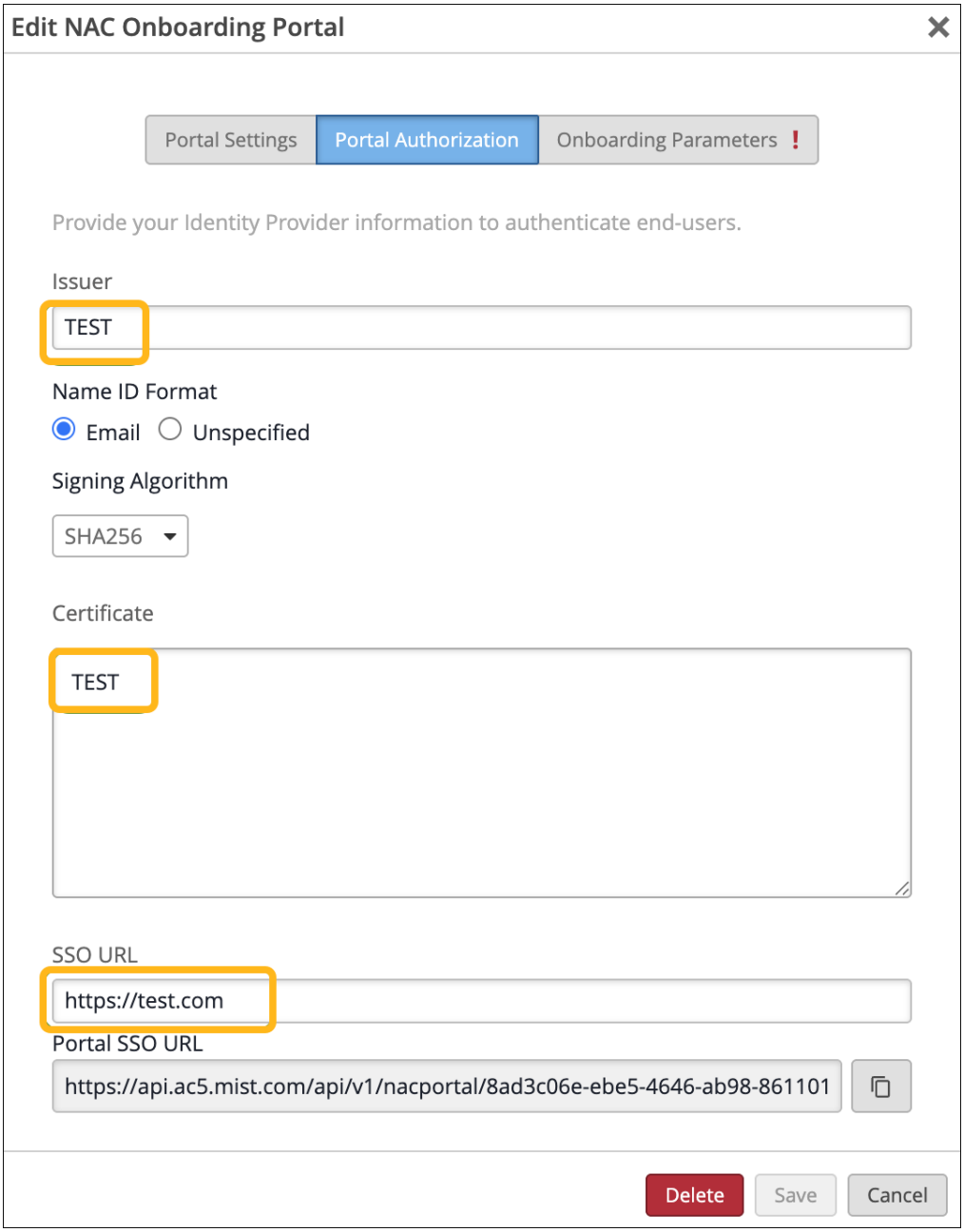


The Edit NAC Onboarding portal page displays.

d. Select the **Portal Authorization** tab:

   i. Enter placeholder values for **Issuer**, **Certificate**, and **SSO URL**. These values will later be replaced with actual values from the IdP.

   ii. Copy the **SSO Portal URL** to use later.

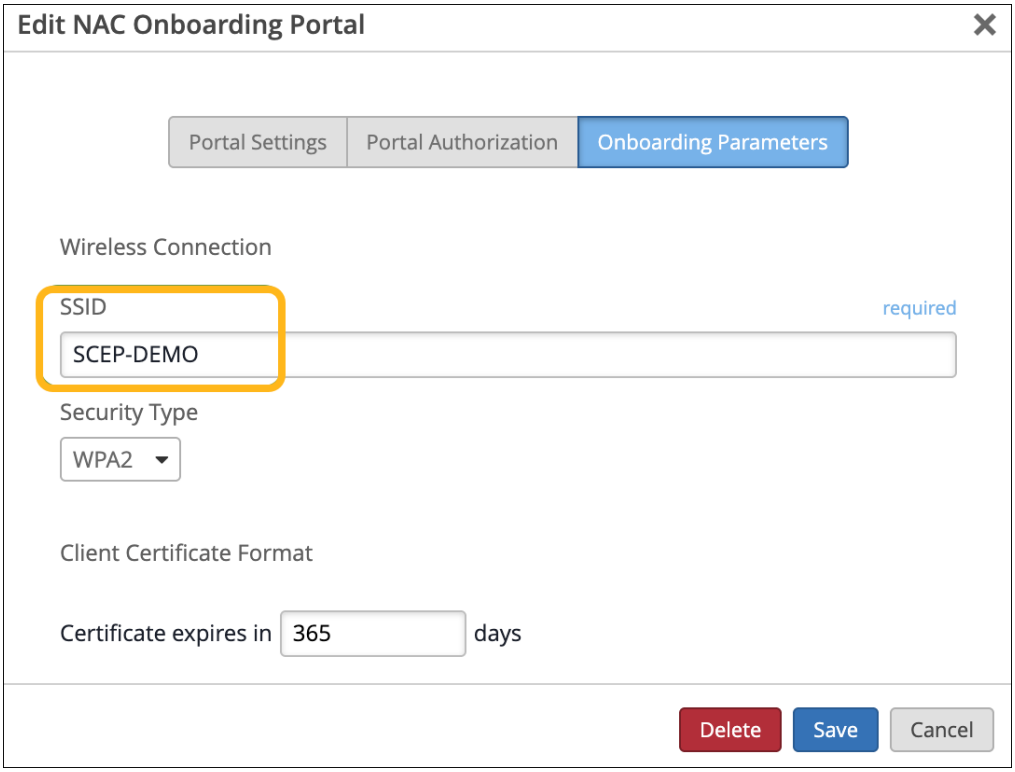


e. Select the **Onboarding Parameters** tab and configure the following:

   i. Enter the SSID name to be provisioned.

   ii. Select the Security Type as WPA2 or WPA3 Enterprise.

   iii. Set the number of days after which the client certificate will expire. The value can range from 1-1825 days (up to 5 years).

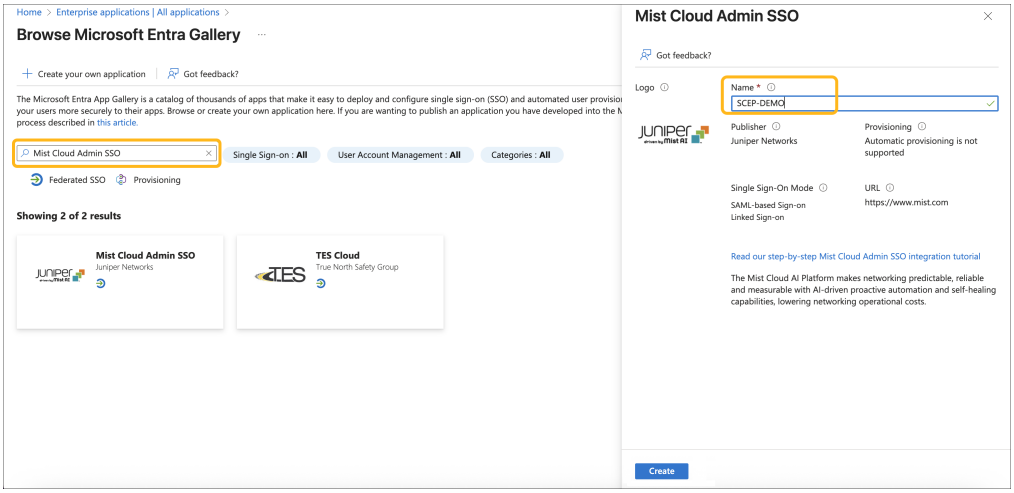


2. Configure SSO and integrate the NAC portal with Microsoft Azure:

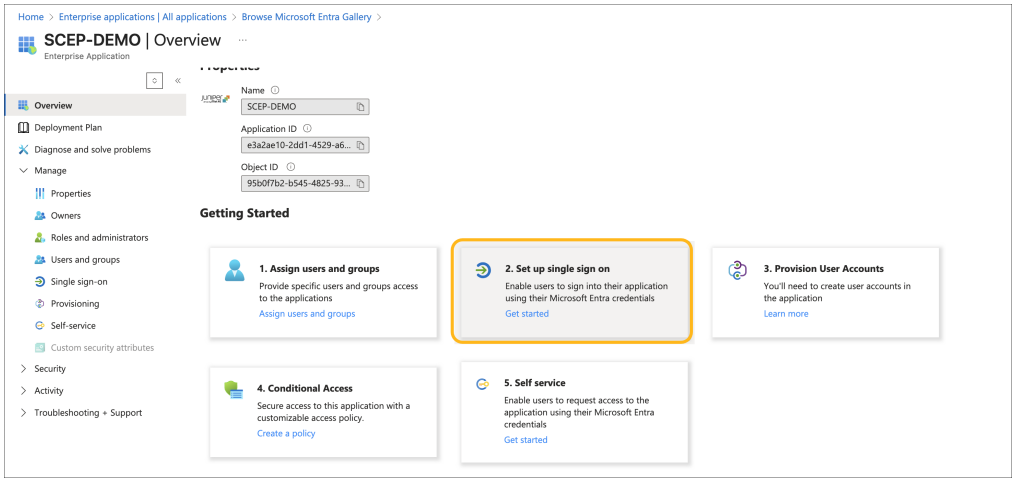
   a. Log into the Azure portal. Navigate to **Enterprise Applications** and click **New Application**.

   b. In the Browse Microsoft Entra Gallery section, type **Mist Cloud Admin SSO** in the search box.

   c. Select **Mist Cloud Admin SSO** from the results panel. Provide a name for the application and click **Create**.

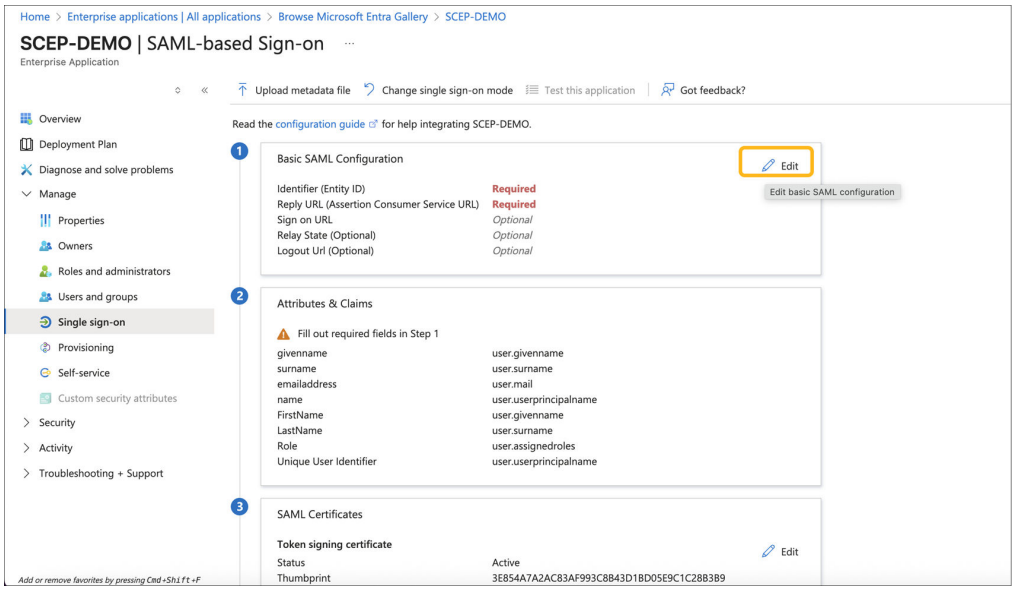


   d. Open the application and click **Set up Single Sign-On**.

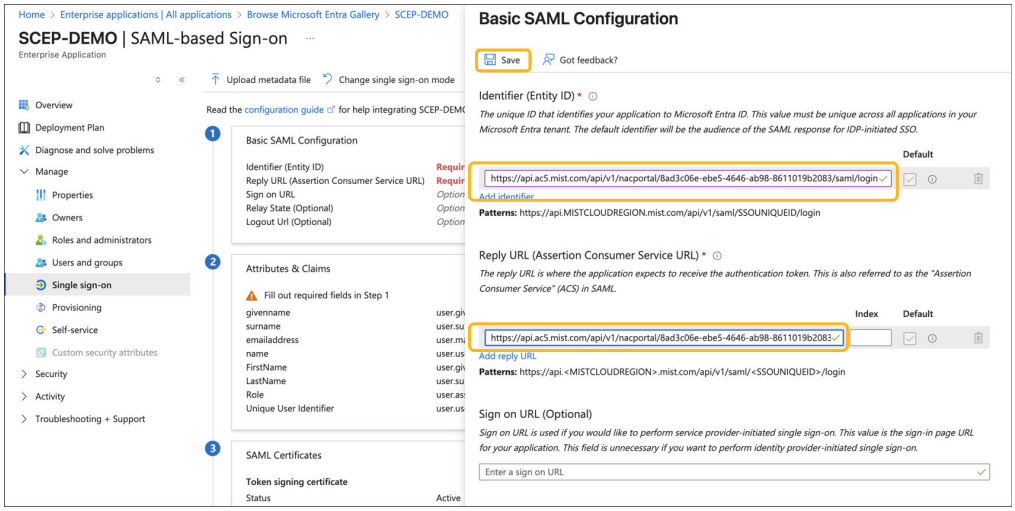


e. Select **SAML** as the SSO method.

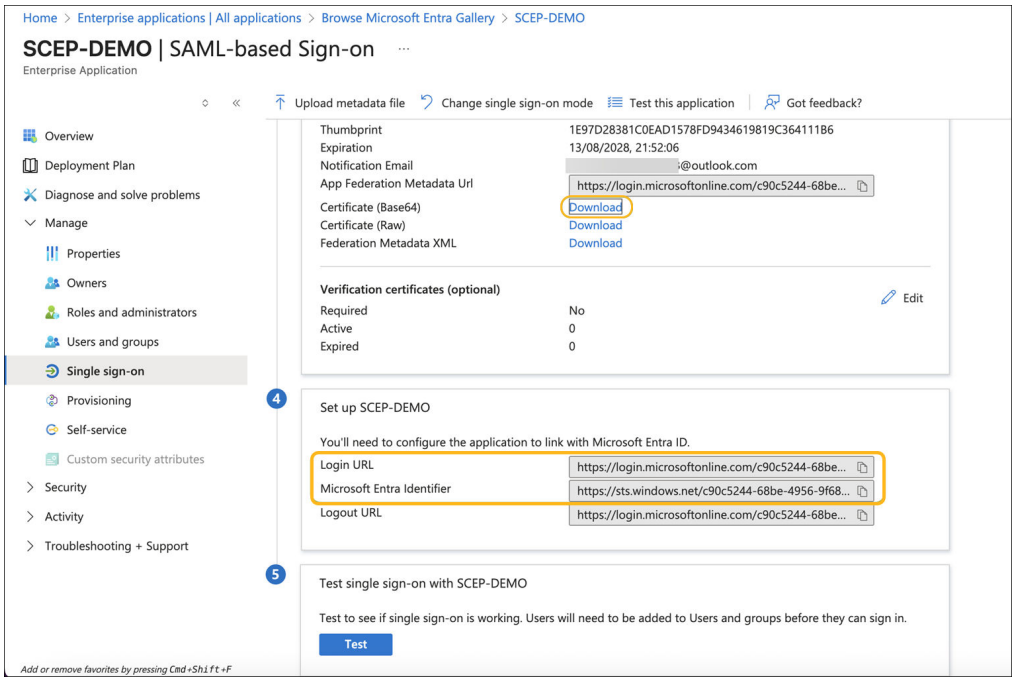
f. Click **Edit Basic SAML Configuration**.



g. In the SAML configuration page, set the Identifier and Reply URL to the Portal SSO URL copied earlier from the NAC Onboarding Portal. Click **Save**.

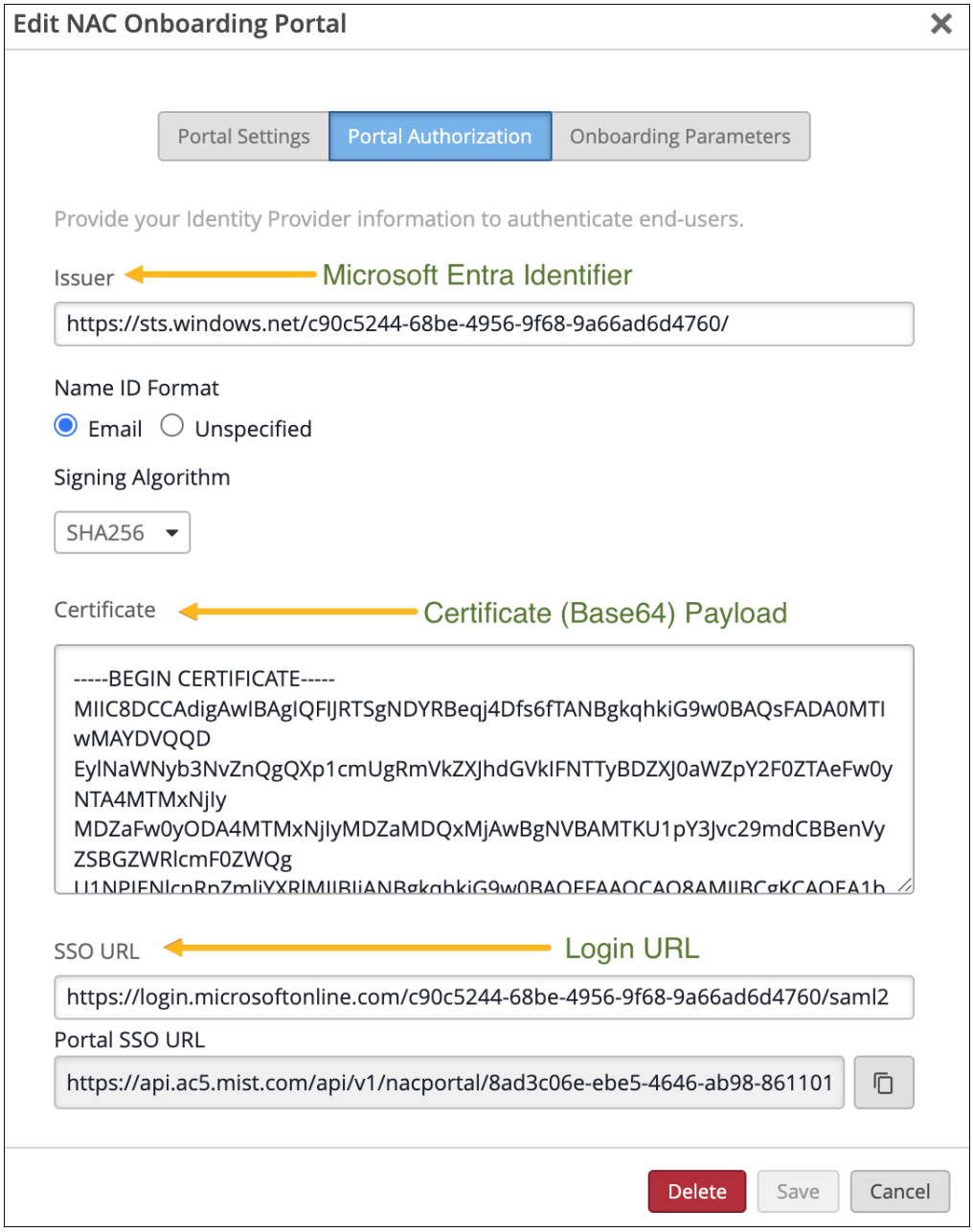


h. Download the Certificate (Base64) and copy the Login URL and Microsoft Entra Identifier.

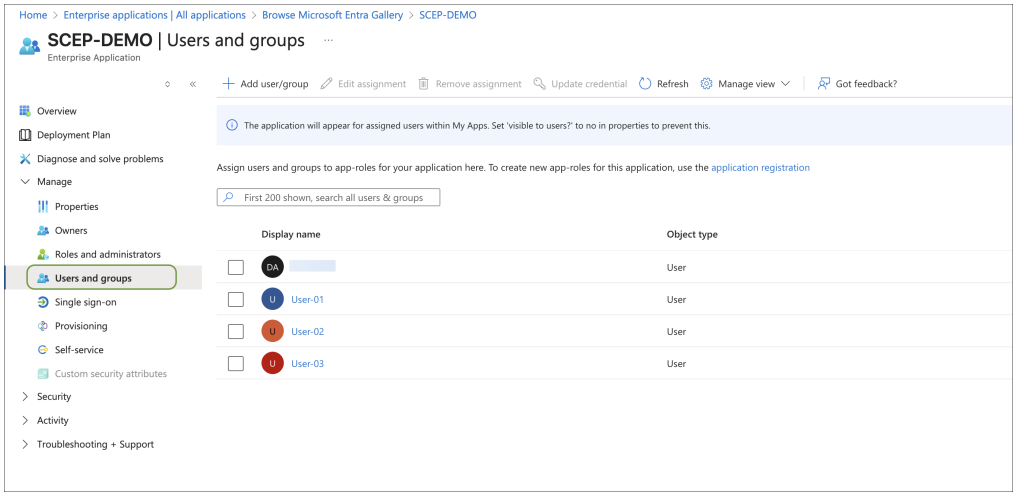


i. In the Juniper Mist portal, go to the Portal Authorization tab for your NAC Onboarding Portal:

- Replace Issuer with the Microsoft Entra Identifier.
- Replace Certificate with the payload from the downloaded Base64 certificate.
- Replace SSO URL with the Login URL.



3. Assign users and groups to the Azure application to enable them to access the portal.

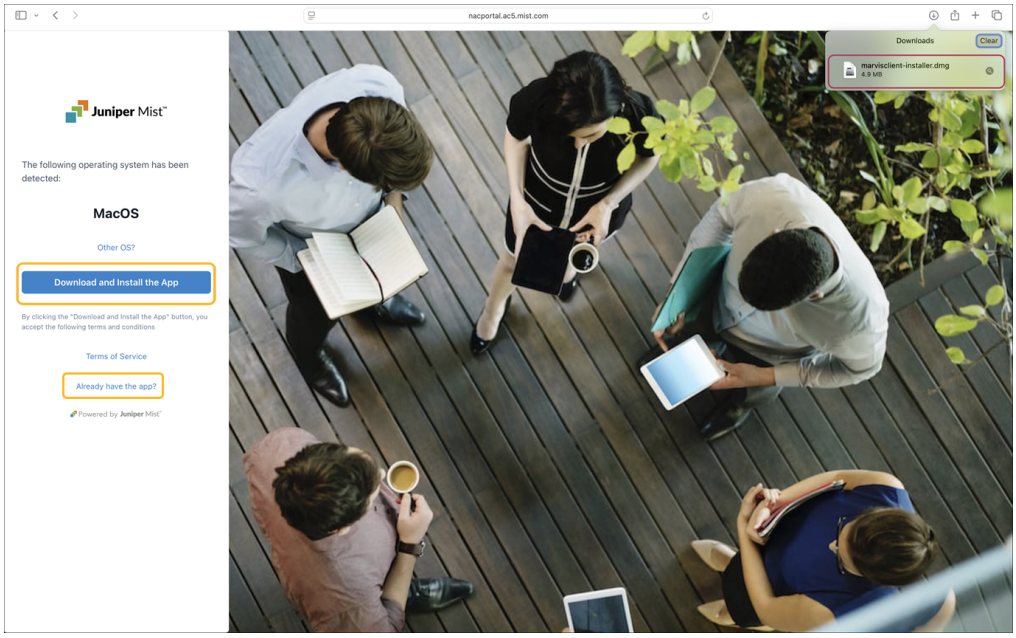


Download the Marvis Client App and Wi-Fi Profile

After you configure the NAC portal and integrate it with Azure, users can log in to the NAC portal using Azure SSO and install the Wi-Fi profile through the Marvis client app. We've used a macOS device as an example here.

1. On a macOS device, access the NAC Portal using the URL listed under the **Portal Settings** tab of the NAC Onboarding Portal and sign in using your Azure SSO credentials.

   After a successful authentication, the following page displays.



2. Click **Download and Install App** to install the Marvis client app.

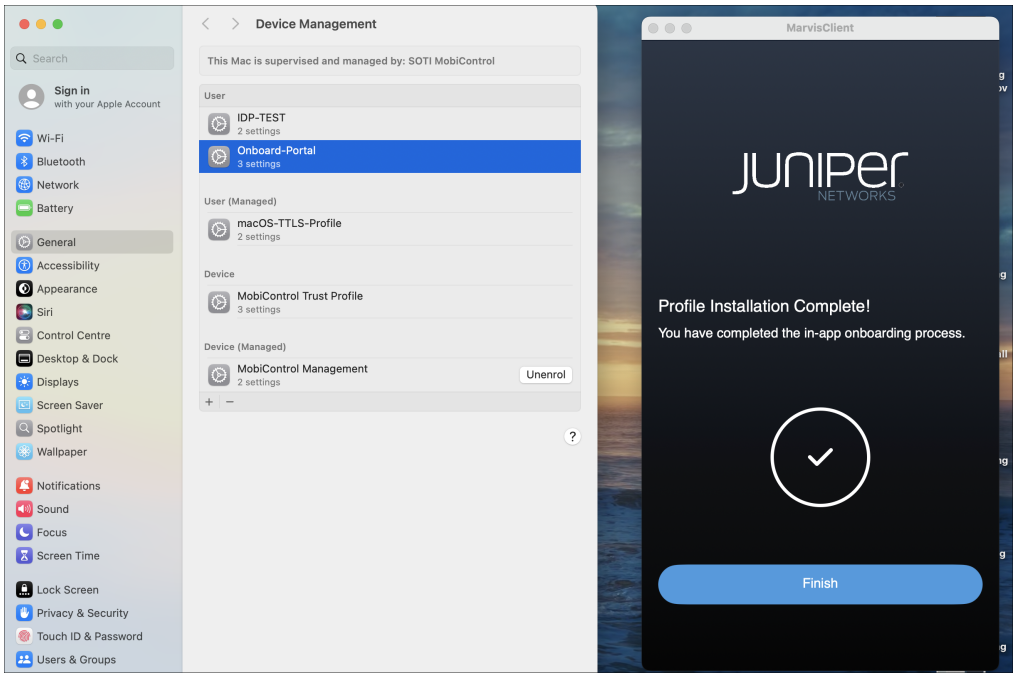
If your device is running Windows or macOS, the app is downloaded automatically and you can install the app once the download process is complete.

For Android and iOS, you will be redirected to the Google or Apple Play Store to download the app.

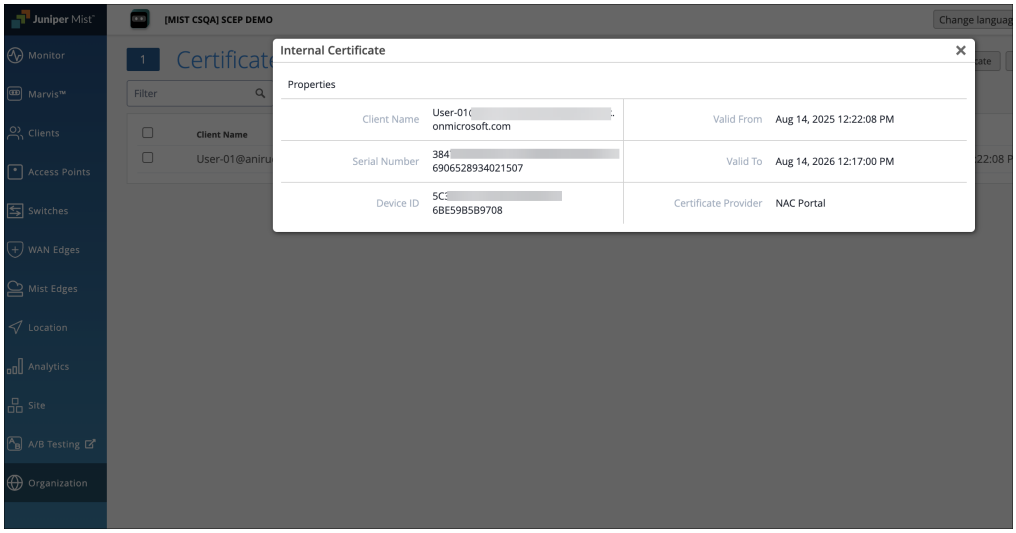
3. After you install the Marvis client app (or if you have installed the app already), switch to the NAC portal page and click **Already have the app?** to install the profile.

   You will be redirected to the Marvis client app to install the Wi-Fi profile.

4. Click **Install**, and then navigate to **Settings**>**General** > **Device Management** on your device and complete the profile installation.



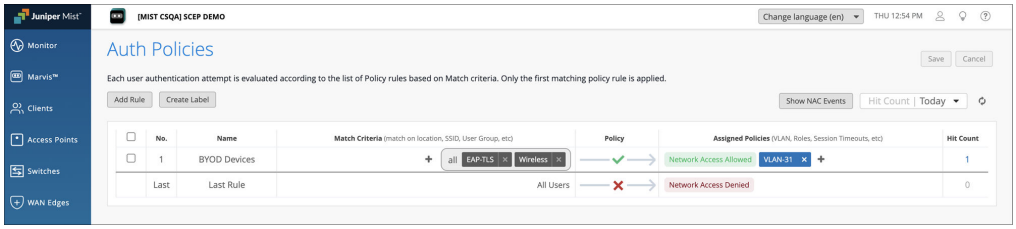
5. On the Juniper Mist portal, open the Certificates page and verify the client-issued certificate details under the Internal section.



Verify Client Connectivity to the Network

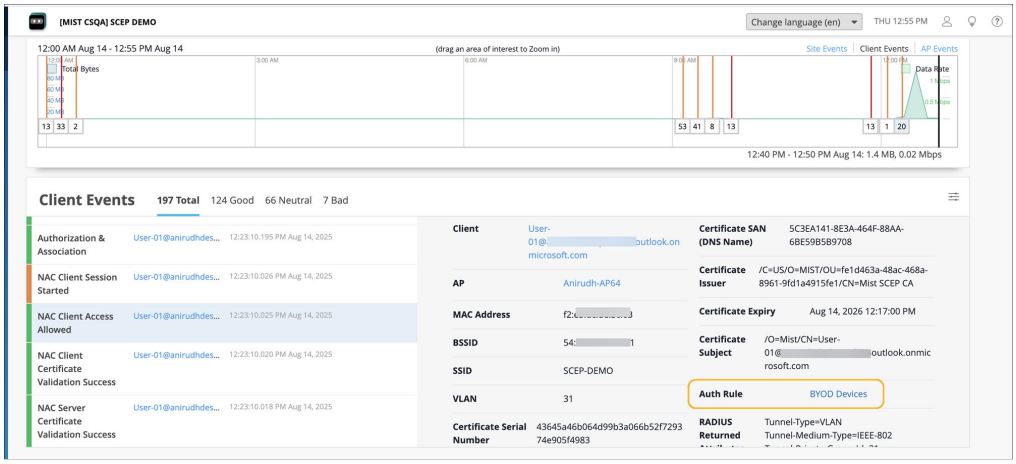
Verify that the device connects to the Access Assurance network through the client certificate provisioned through the Marvis client app.

1. From the left menu of the Juniper Mist portal, select **Organization**> **Access**>**Auth Policies** and configure the required authentication policy rules for the device.



2. Connect the device to the network and confirm successful authentication.

3. Navigate to the **Monitor**>**Service Levels**>**Insights** page and go to the Client Events section. Verify the NAC Client authentication events.



How to Set Up a NAC Portal and Integrate It with Okta

IN THIS SECTION

Setting up a NAC onboarding portal and integrating it with Okta involves the following steps:

Create a NAC Portal and Integrate It with Okta

Ensure that the onboard CA configuration is enabled on the Certificates page. See "Before you Begin" on page 241.

1. Create a NAC portal. When you create the portal, a NAC portal URL will be generated for users to access using SSO.

   a. From the left menu of the Juniper Mist portal, select **Organization**>**Client Onboarding**, and select the **NAC** tab.

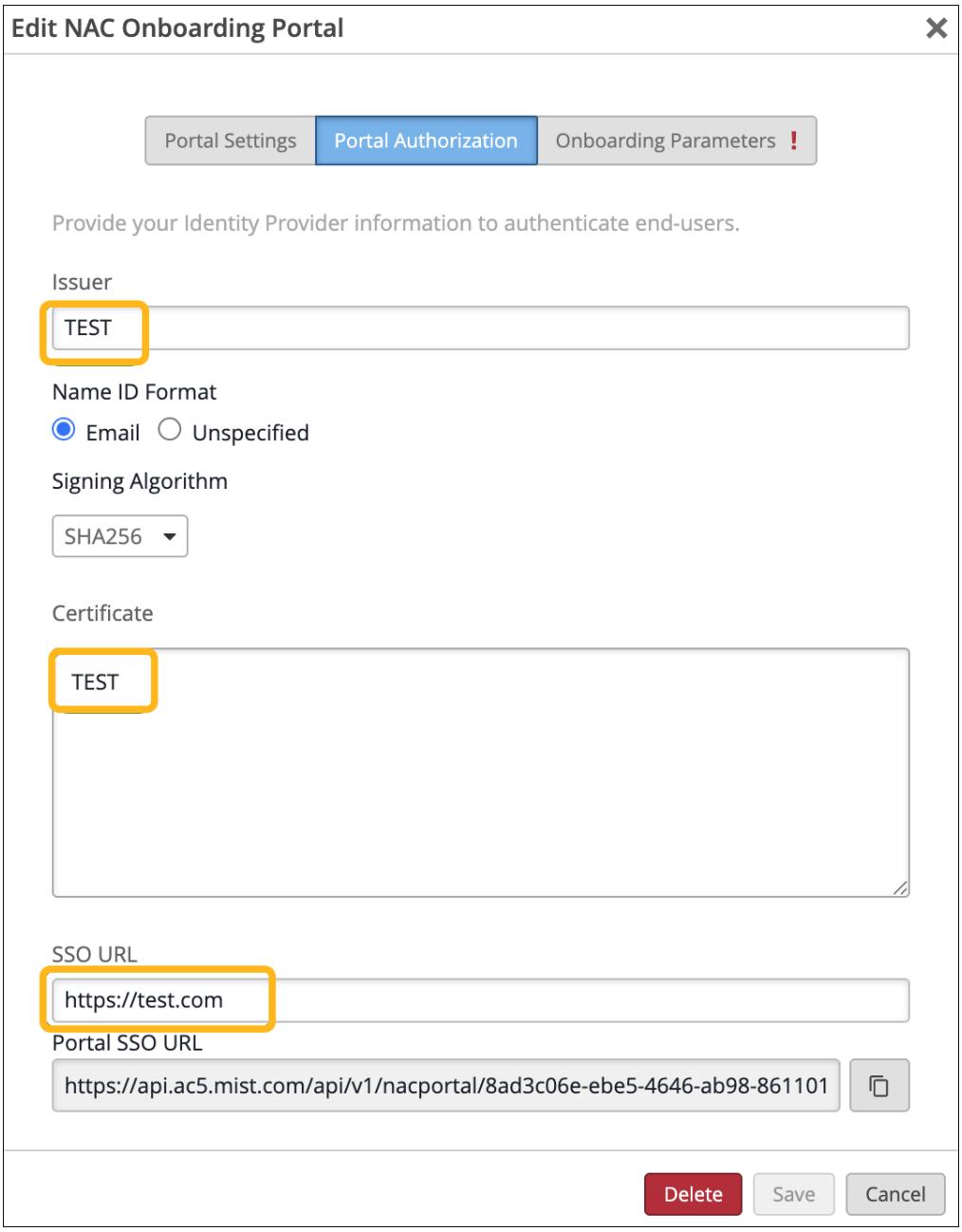
   b. Click **Add NAC Onboarding Portal** at the top-right corner of the Client Onboarding page.

   c. In the Add NAC Onboarding Portal page, provide a name and click **Create**.

d. Select the **Portal Authorization** tab:

   i. Enter placeholder values for **Issuer**, **Certificate**, and **SSO URL**. These values will later be replaced with actual values from the IdP.

   ii. Copy the **SSO Portal URL** to use later.

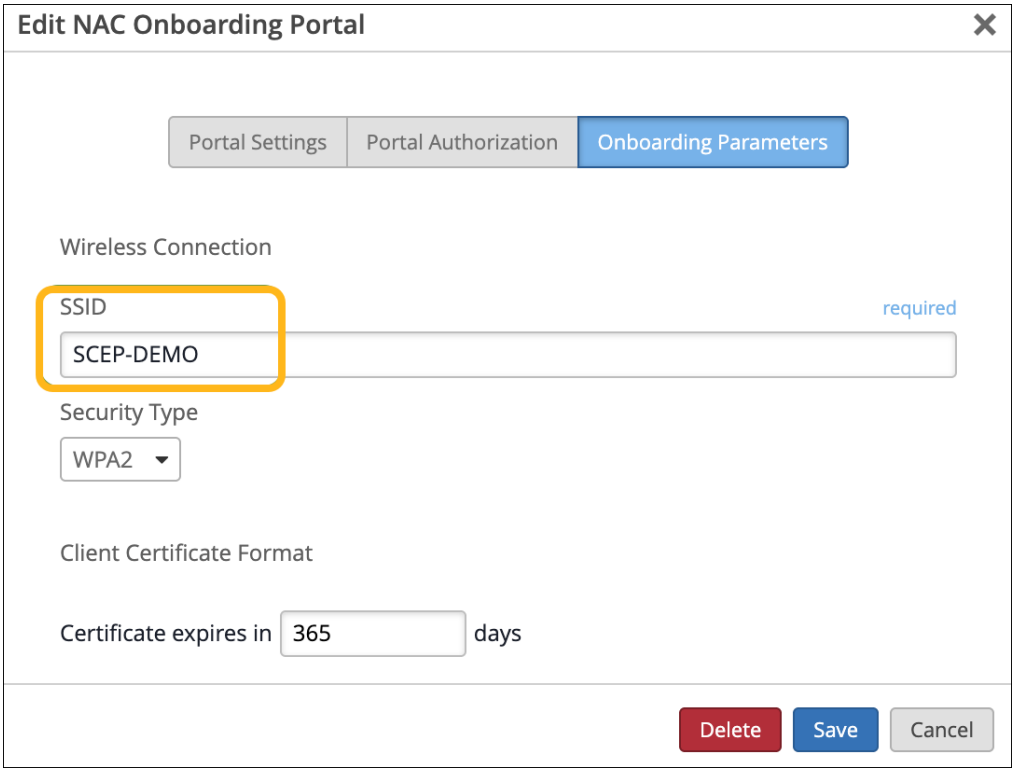


e. Select the **Onboarding Parameters** tab and configure the following:

   i. Enter the SSID name to be provisioned.

ii. Select the Security Type as WPA2 or WPA3 Enterprise.

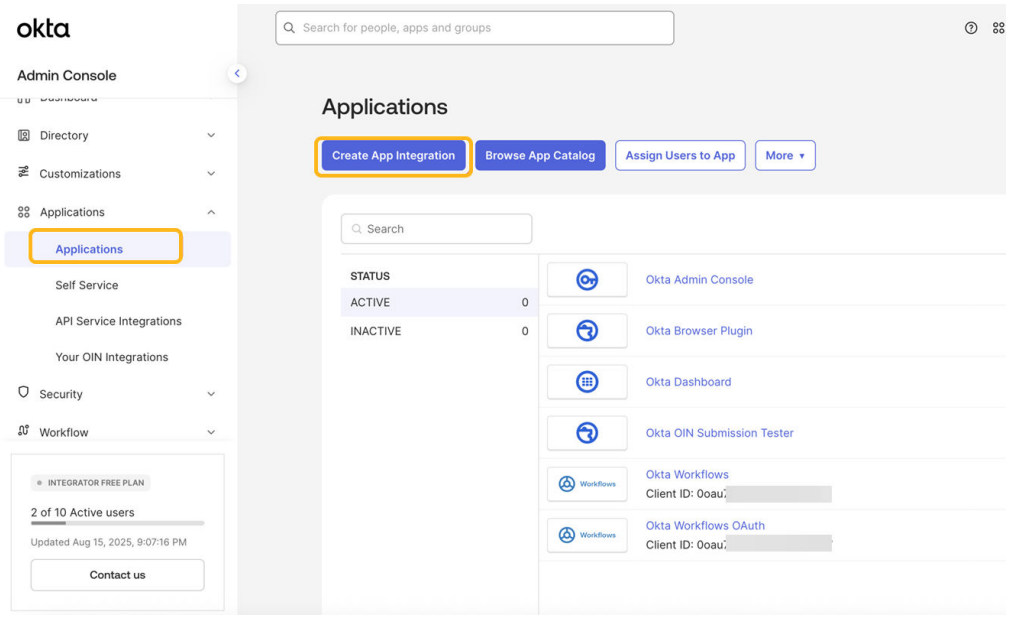
iii. Set the number of days after which the client certificate will expire. The value can range from 1-1825 days (up to 5 years).



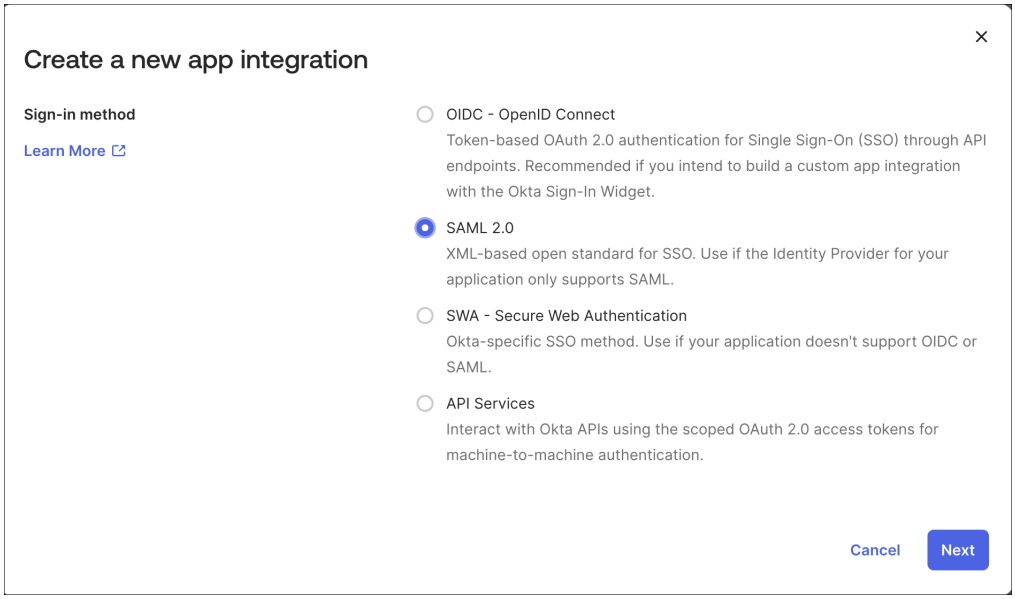
2. Configure SSO and integrate the NAC portal with Okta:

   a. Log in to the Okta administration console and navigate to the Applications page.

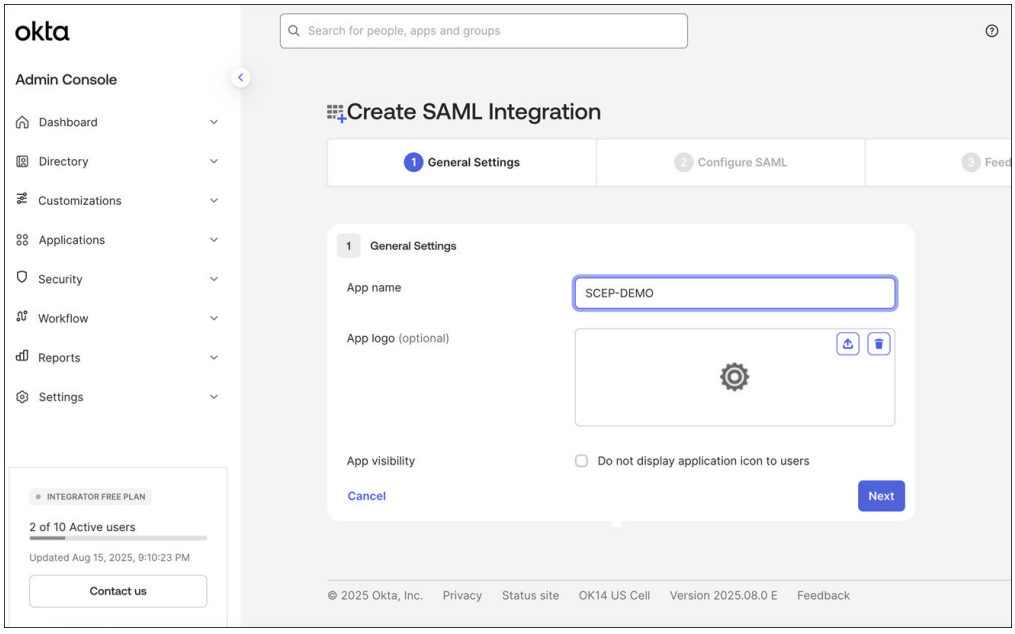
   b. Click **Create App Integration**.



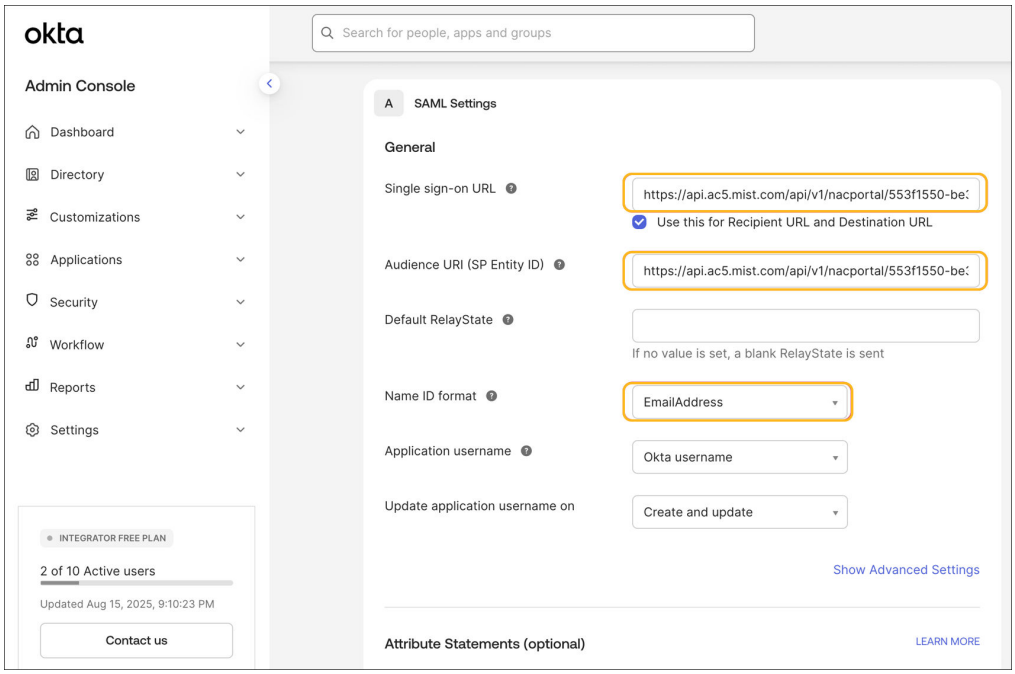
c. Select **SAML 2.0** as the Sign-in method and click **Next**.



d. Enter an app name and click **Next**.

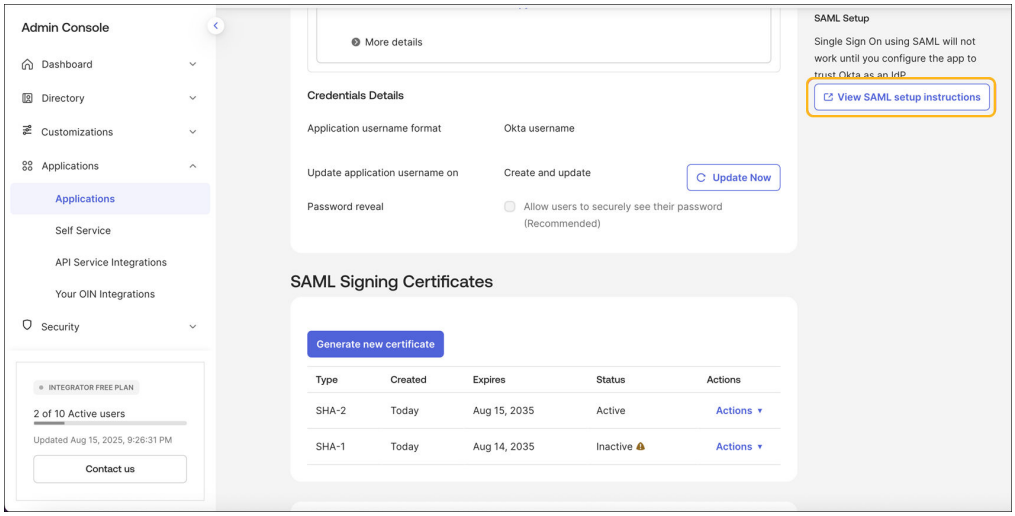


e. Paste the Portal SSO URL that you copied earlier to the **Single Sign On URL** and **Audience URL** fields under SAML Settings. Set the Name ID format to EmailAddress, click **Next**, and then click **Finish**.

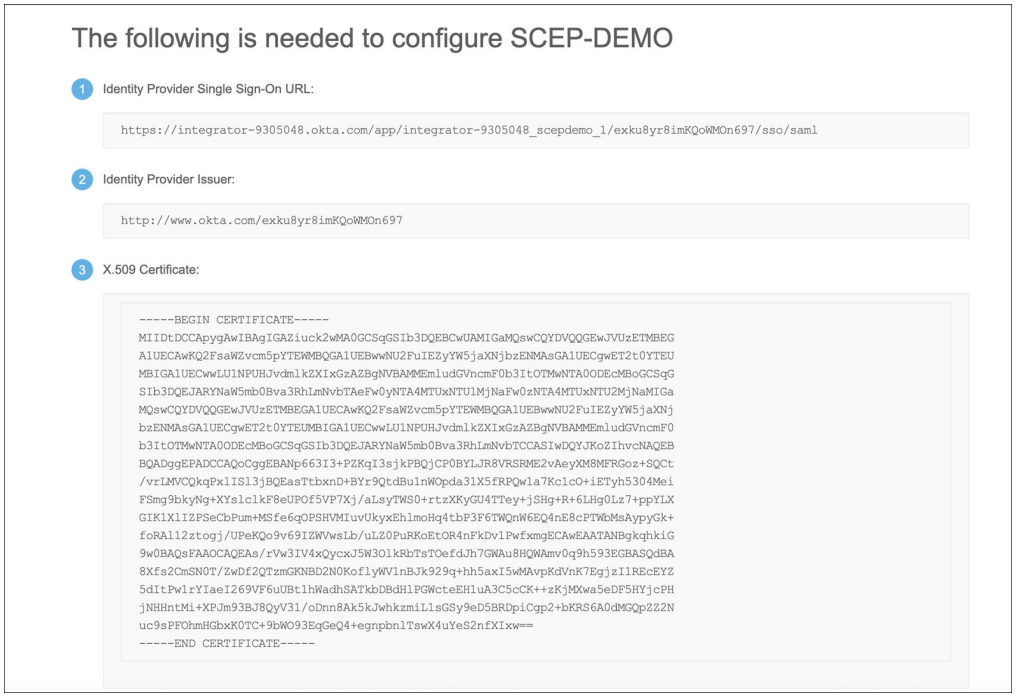


You will be redirected to the app in edit mode.

f. Scroll down and click **View SAML setup instructions**.



g. Copy the Identity Provider Single Sign-On URL, Identity Provider Issuer, and X.509 Certificate.

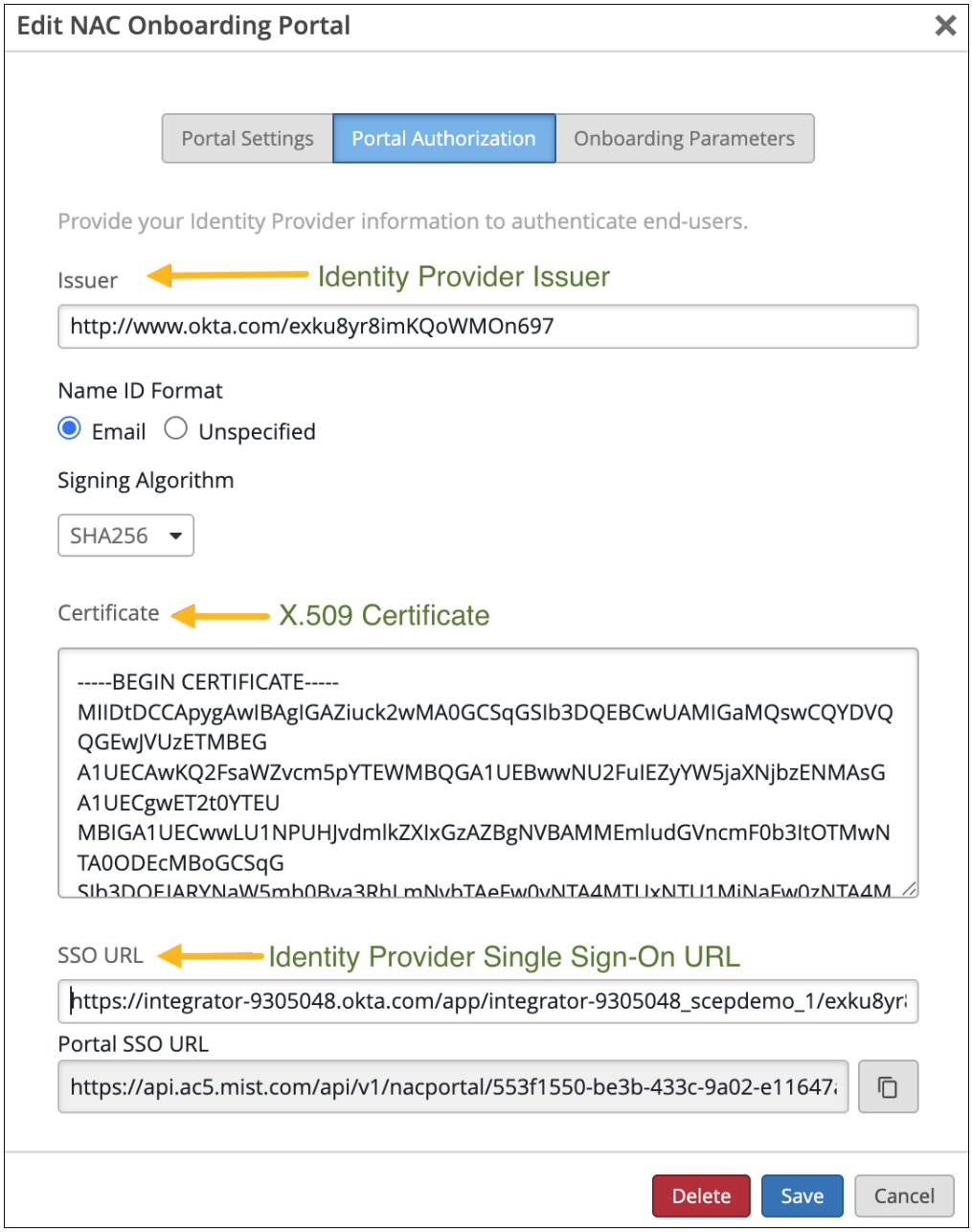


h. Switch to the Juniper Mist portal and go to the **Portal Authorization Settings** tab of the Edit NAC Onboarding Portal page. Paste the information that you copied in the previous step in the following fields:

Issuer—Identity Provider Issuer

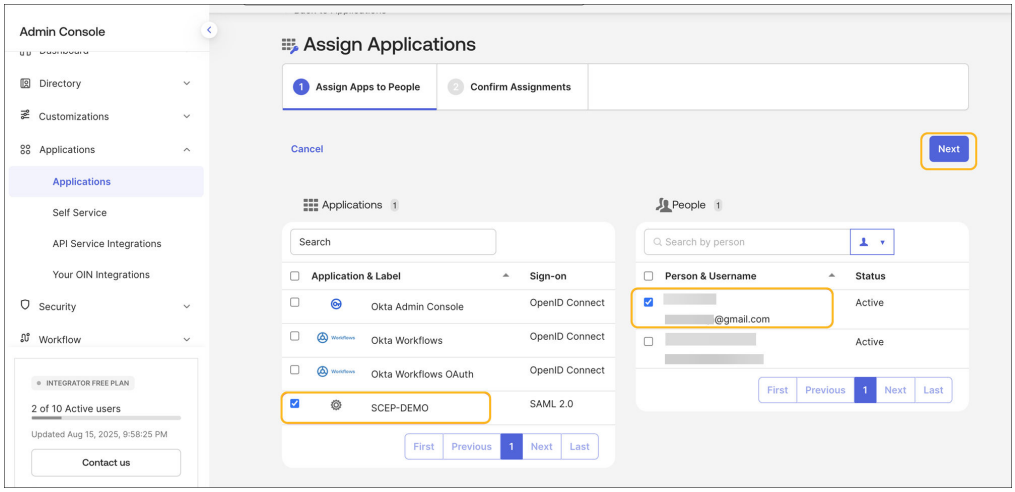
SSO URL—Identity Provider Single Sign-On URL

Certificate—X.509 Certificate



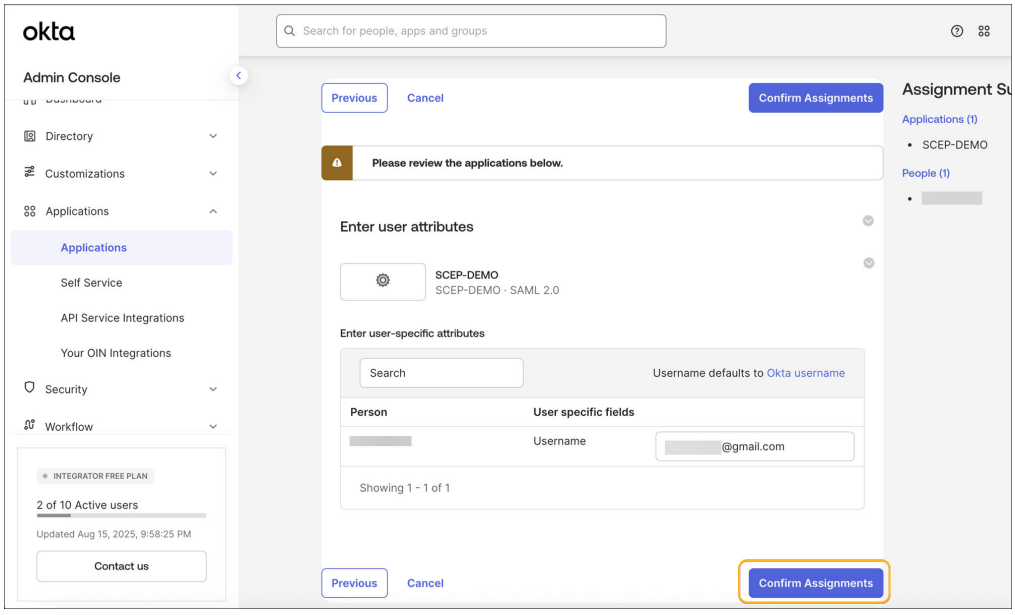
Click **Save**.

i. Go to **Applications**>**Assign Users to App** and assign users.



j. Select the user and the application, then click **Next**.

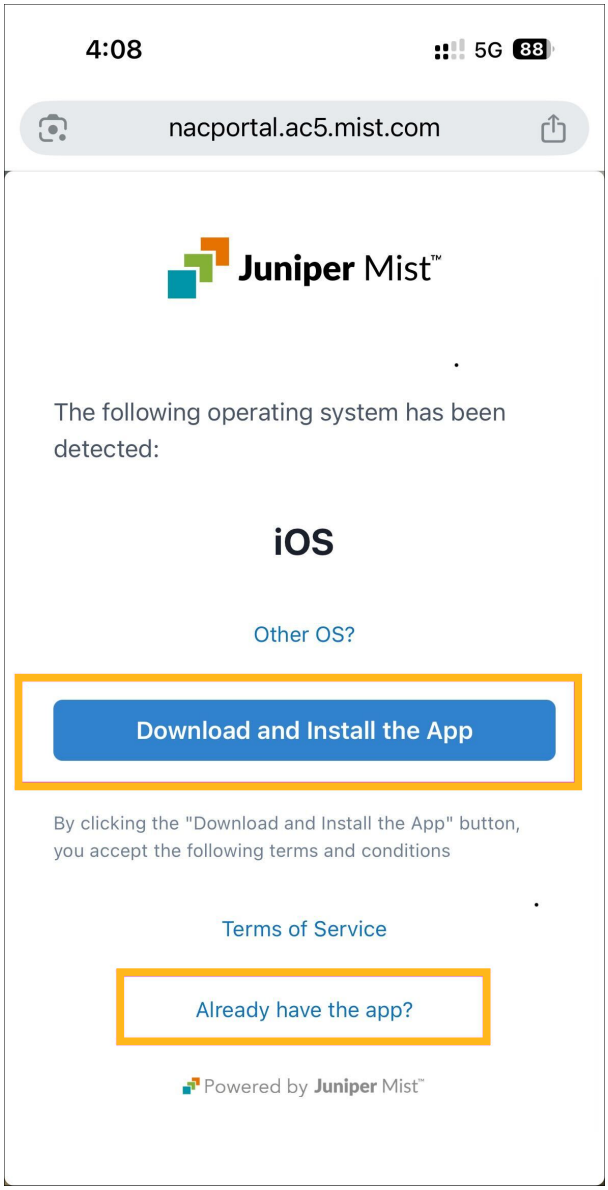
k. Click **Confirm Assignments**.



Download the Marvis Client App and Wi-Fi Profile

After you configure the NAC portal and integrate it with Okta, users can log in to the NAC portal using Okta SSO and install the Wi-Fi profile through the Marvis client app. We've used an iOS device as an example here.

1. On your iOS device, access the NAC Portal URL listed under the **Portal Settings** tab of the Edit NAC Onboarding Portal page and sign in using your Okta SSO credentials.



2. Click **Download and Install App** to install the Marvis client app.

   If your device is running Windows or macOS, the app is downloaded automatically and you can install the app once the download process is complete.

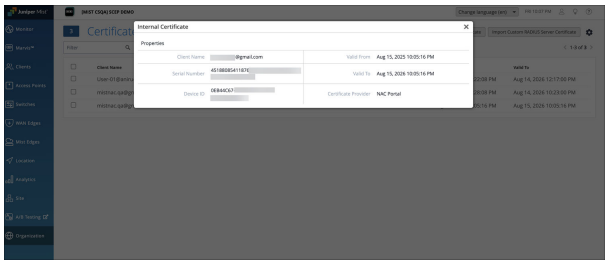
   For Android and iOS, you will be redirected to the Google or Apple Play Store to download the app.

3. After you install the Marvis client app (or if you have installed the app already), switch to the NAC portal page and click **Already have the app?** to install the profile.

   You will be redirected to the Marvis client app to install the Wi-Fi profile.

4. Click **Install**.

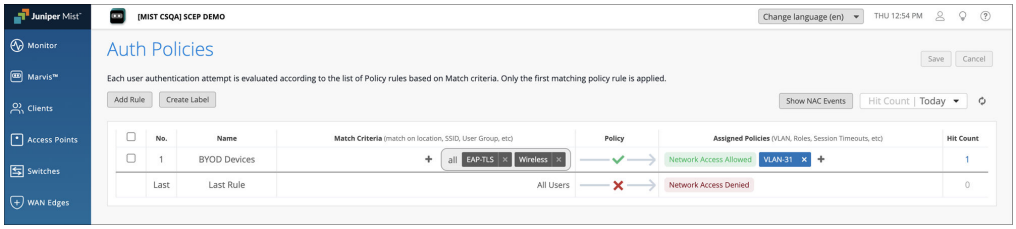
5. On the Juniper Mist portal, open the Certificates page and verify the client-issued certificate details under the Internal section.



Verify Client Connectivity to the Network

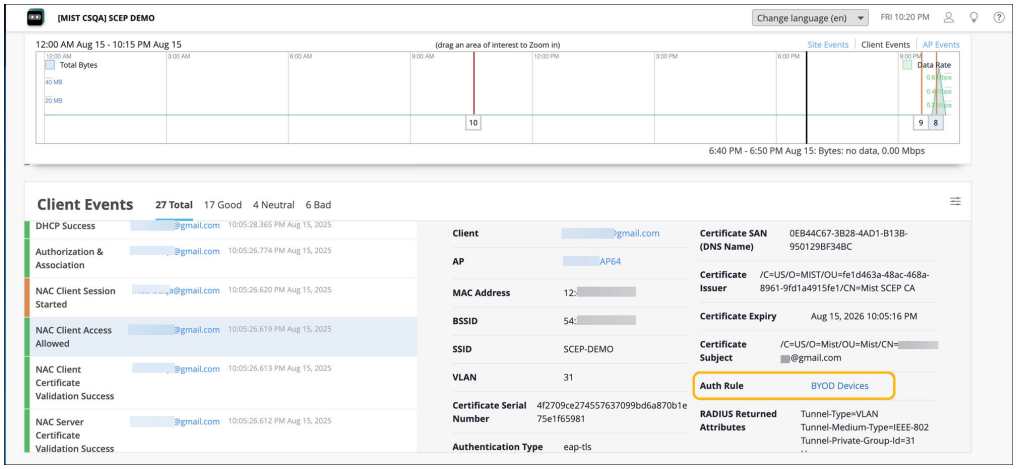
Verify that the device connects to the Access Assurance network through the client certificate provisioned through the Marvis client app.

1. From the left menu of the Juniper Mist portal, select **Organization**> **Access**>**Auth Policies** and configure the required authentication policy rules for the device.



2. Connect the device to the network and confirm successful authentication.

3. Navigate to the **Monitor**>**Service Levels**>**Insights** page and go to the Client Events section. Verify the NAC Client authentication events.



Mist Access Assurance Endpoints

SUMMARY

Follow these steps to register endpoints, assign attributes and labels, and use them in auth policy rules for controlled network access.

IN THIS SECTION

Network Access Control (NAC) Endpoints page provides you with a database of all endpoints identified by their MAC addresses. Here, you can assign each endpoint with various attributes, such as Name, VLAN, Role, Client Label, and Description. After creating an endpoint, you can reference its Client Label directly in the match criteria of auth policy rules for MAB-based authentication. By utilizing client labels in auth policy rules, you can dynamically assign policy actions such as VLAN assignments, roles, and more.

In the following example, an endpoint is registered, assigned a client label and name, and the label is used in the auth policy match criteria to override the username returned in the RADIUS Access-Accept.

Register Endpoints

Use the following steps to set up endpoints for NAC:

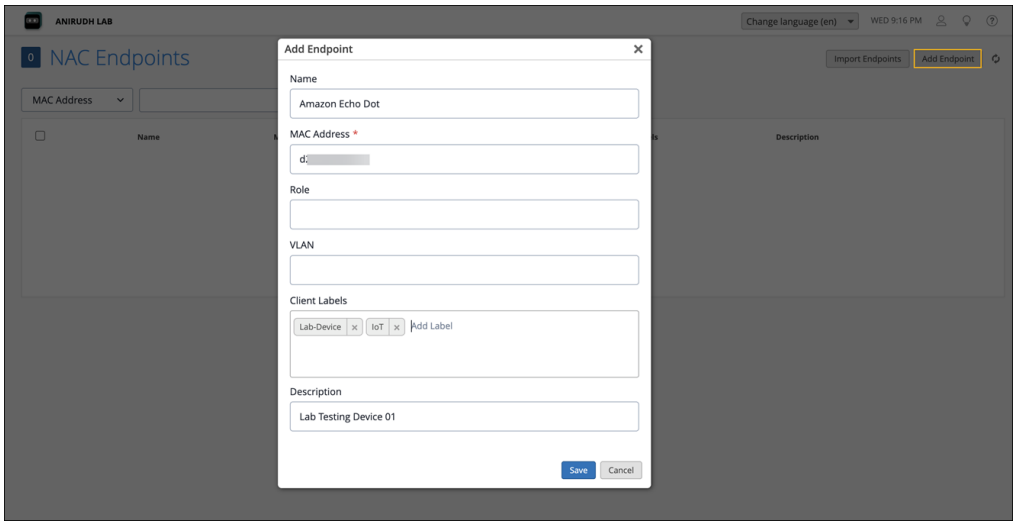
1. From the left menu of the Juniper Mist portal, select **Organization** > **Access** > **Endpoints**. Click **Add Endpoint**.

   You can also import endpoints by uploading a CSV file. See "Import Endpoints" on page 264.

2. In the Add Endpoint page, enter the following details and click **Save**:

   - **Name** (Optional)—Name of the endpoint. You can use this value to override the User-Name attribute in RADIUS Access Accept during authentication on a per-endpoint basis for better visibility.
   - **MAC Address** (Required)—The unique MAC address of the endpoint.
   - **Role** (Optional)—A role that can be associated with the endpoint. Specify a value only if it is necessary to override role assignment during authentication on a per-endpoint basis.

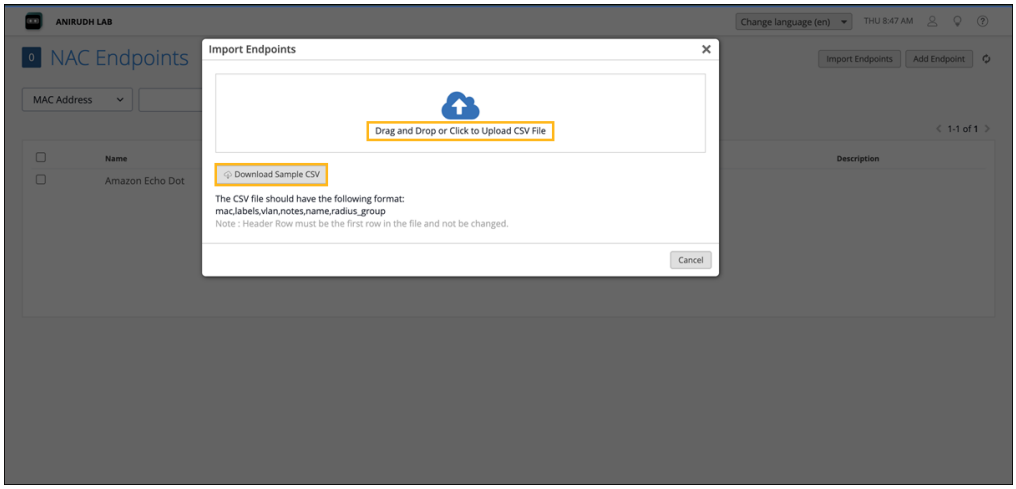
- **VLAN** (Optional)—VLAN ID between 1 to 4094 or VLAN name that can be assigned to an endpoint. Specify a value only if it is necessary to override VLAN assignment during authentication on a per-endpoint basis.
- **Client Labels** (Optional)—One or more labels (tags) applied to the endpoint. These labels can be used in the match criteria of auth policy rules.
- **Description** (Optional)—Additional information that helps identify or provide context for the endpoint.



Import Endpoints

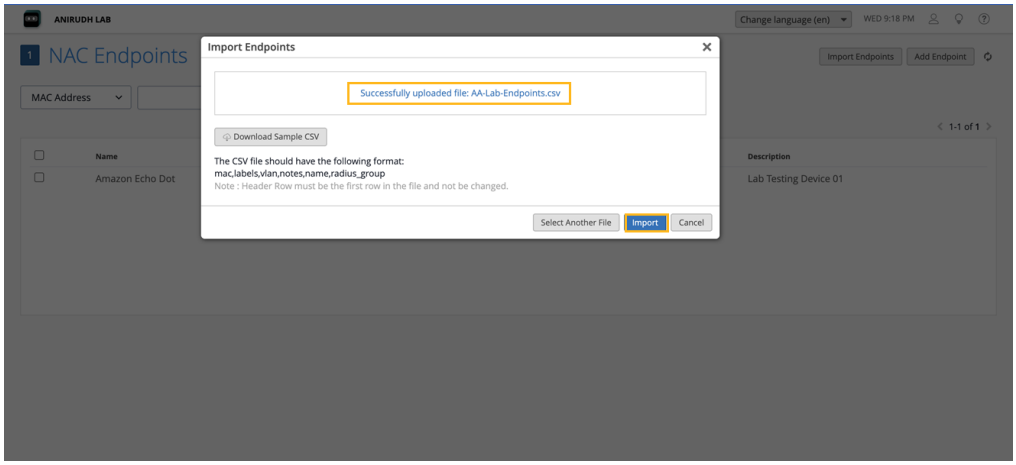
To import endpoints:

1. Click **Import Endpoints** on the upper-right corner of the NAC Endpoint page.



2. Upload the CSV file to the portal using the **Drag and Drop** or **Click to Upload CSV File** option. You can click **Download Sample CSV** to download a sample CSV file with correct headers and format.

3. Click **Import**.



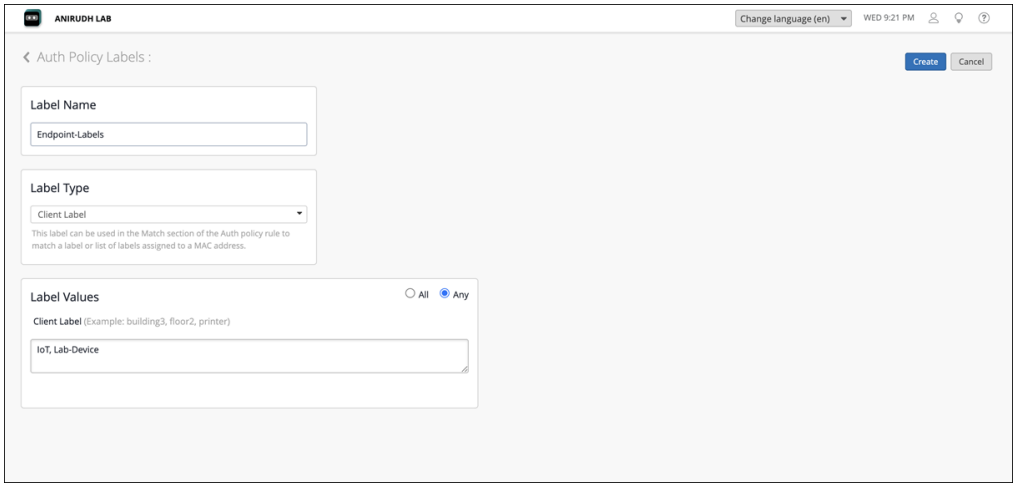
Configure Auth Policy Labels

In the previous step, you have registered an endpoint. Now, you can use Client Label in the match criteria of the auth policy rules.

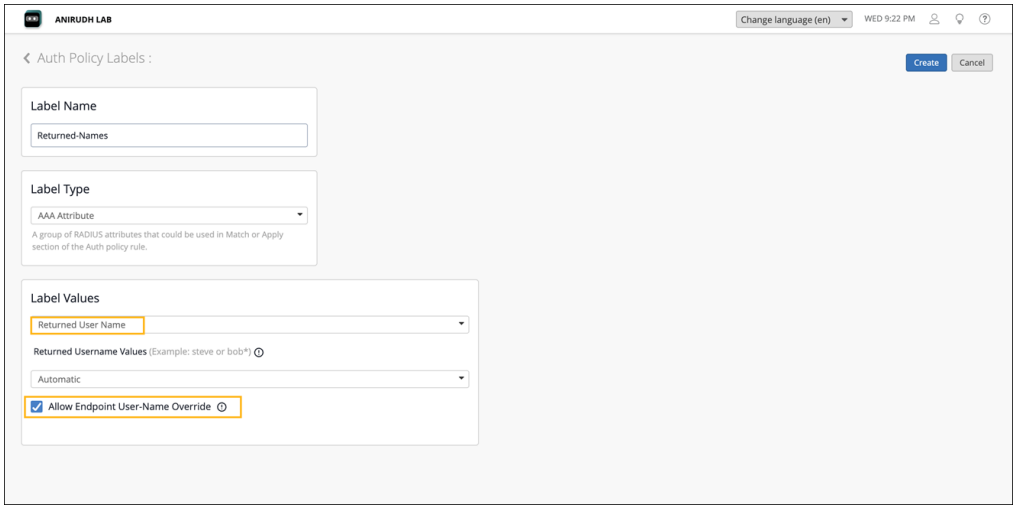
1. From the left menu of the Juniper Mist portal, select **Organization** > **Access** > **Auth Policy Labels**.

2. On the Auth Policy Labels page, click **Add Label** and enter the details.

   - Label Name—Enter the label name.
   - Label Type—Select the type as **Client Label**.
   - Label Values—Enter the labels that you assigned when adding a new NAC endpoint.
   - Click **Create**.

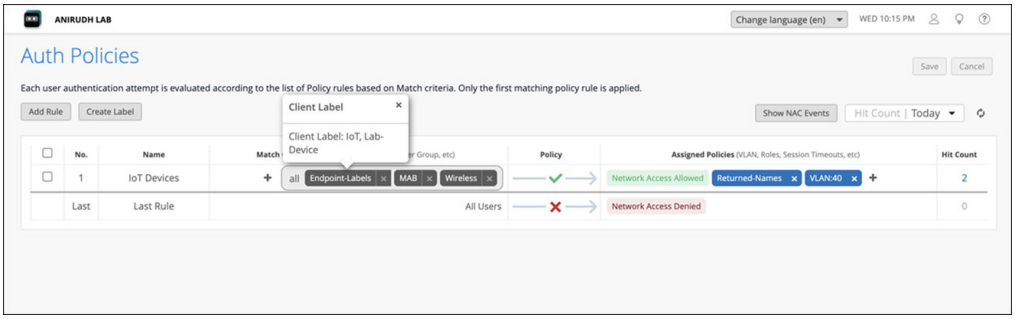


3. Create a Label with the Label Value **Returned User Name** and enable **Allow Endpoint User-Name Override** to override the User-Name returned in the RADIUS Access-Accept with the Endpoint Name.



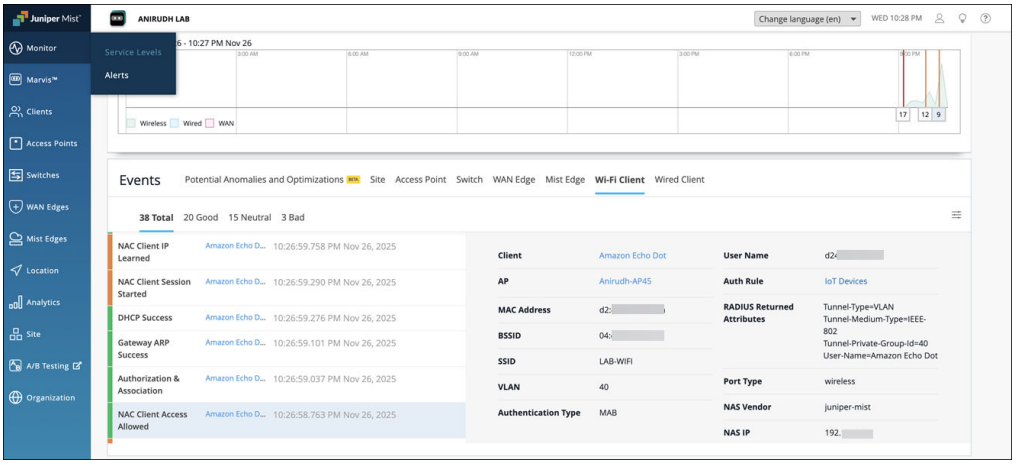
Configure Auth Policy Rules

Navigate to **Organization**>**Access**>**Auth Policies**. Click **Add Rule** and assign the Client Label in the match criteria of the auth policy rule. In the assigned policies section, add the Returned User Name labels. Also add VLAN, Role labels as needed.

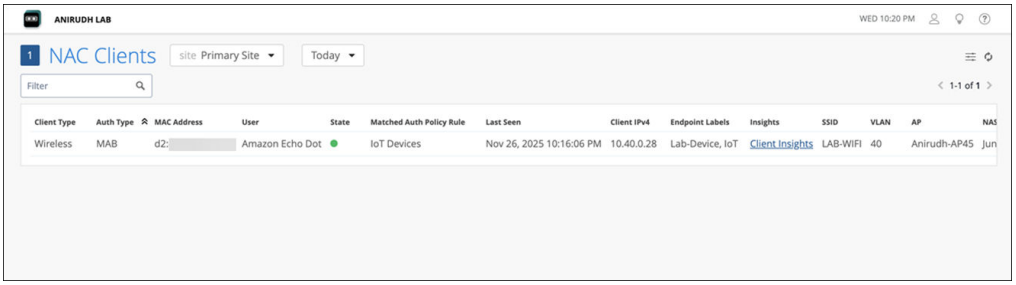


Client Connection and Verification

Navigate to **Monitor**>**Service Levels**>**Events**>**Wi-Fi Client** to review client connectivity and confirm assigned attributes in the NAC Events.



You can also use the NAC Clients page to view the client connectivity status along with the assigned User-Name, VLAN and Role.



RELATED DOCUMENTATION

Install Juniper Mist Edge VM for Juniper Mist Authentication Proxy

SUMMARY

Follow these steps to install a Juniper Mist™ Edge virtual machine (VM) for the Juniper Mist Authentication Proxy functionality.

IN THIS SECTION

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

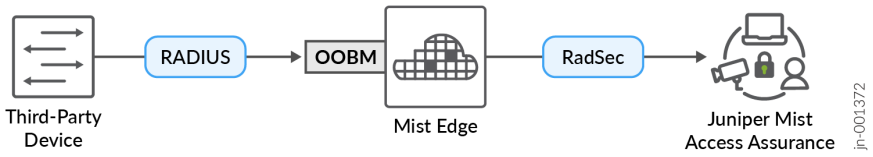
Juniper Mist Edge virtual machine (VM) requires out-of-band management (OOBM) interface to act as Juniper Mist Auth Proxy.

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 98: Juniper Mist Edge as Auth Proxy—Flow of Connections

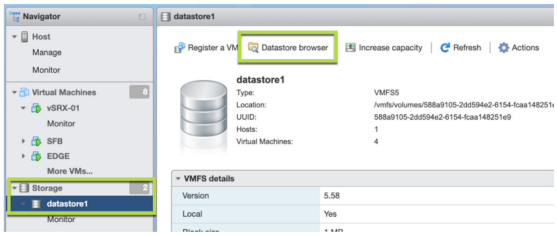


Install Juniper Mist Edge VM

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.

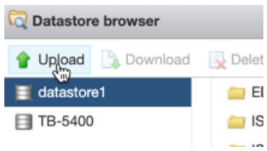
c. Click **Datastore browser** and select the datastore to which you will upload the file.

Figure 99: Select Datastore to Upload File



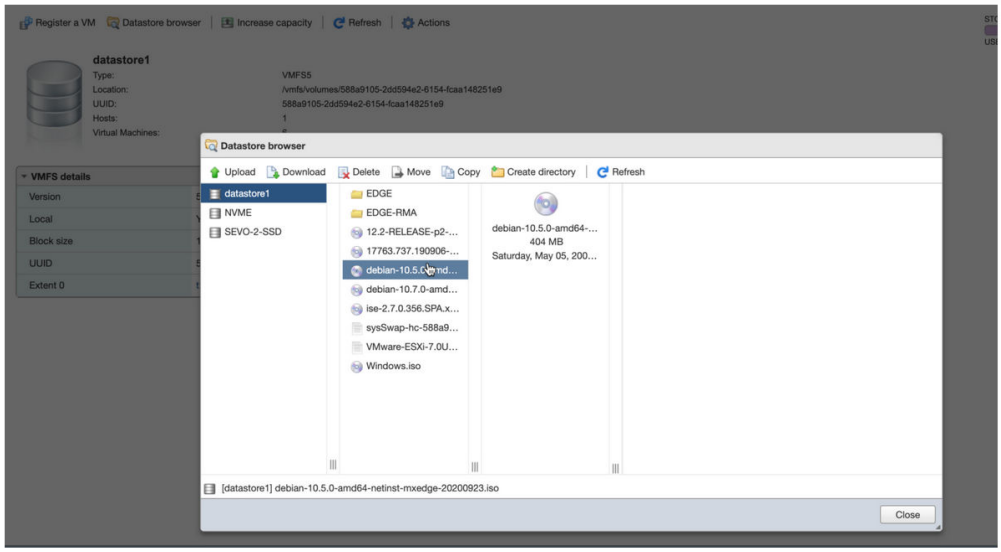
d. Click **Upload** and then select the ISO file that you have downloaded in the previous step.

Figure 100: Upload ISO File



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

Figure 101: Refresh Datastore Browser

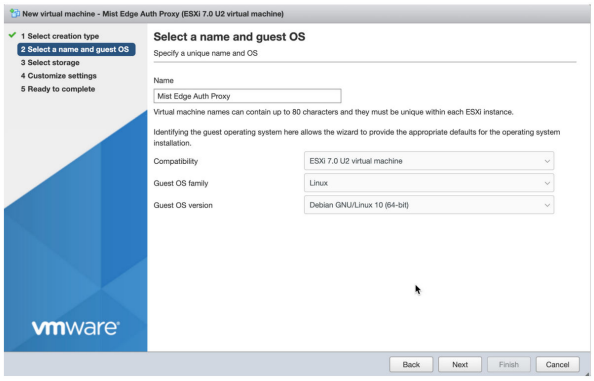


3. Create a VM with the following configuration.

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.

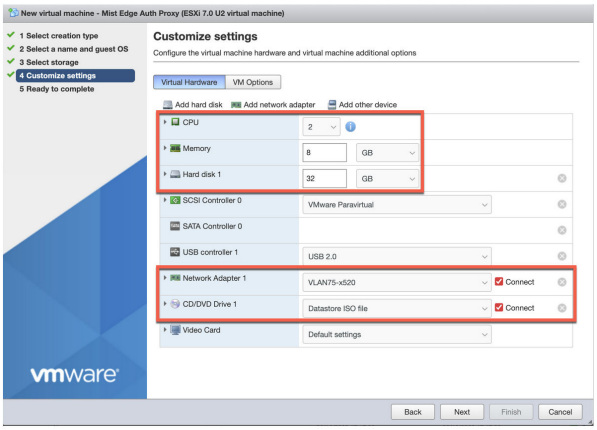
Figure 102: Enter Details of Juniper Mist Edge VM



- **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 103: Customize Settings for VM



See Virtual Mist Edge for detailed instructions.

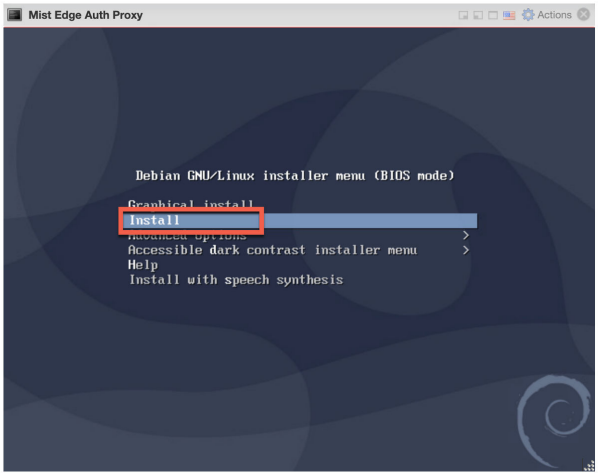
d. Click Finish after you complete the setup.

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 104: Install Juniper Mist Edge VM



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

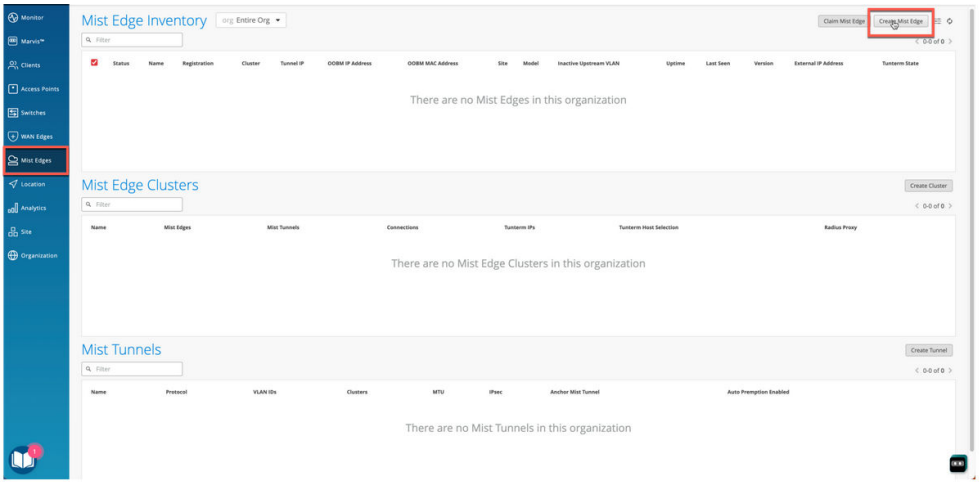
On the installation page, you can see the progress of the installation for some time (30 seconds to a minute) and a request to wait.

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

Create a Juniper Mist Edge VM on the Juniper Mist Portal

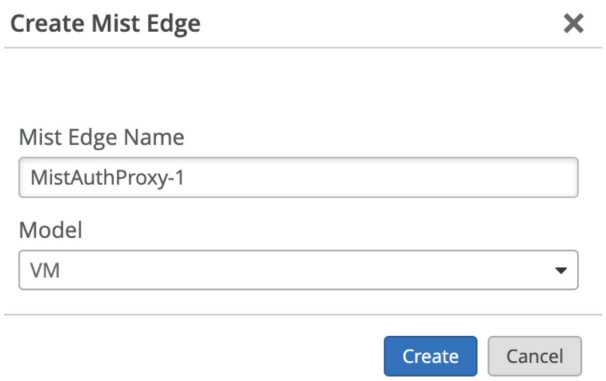
1. From the left menu of the Juniper Mist portal, select **Mist Edges**. Then on the top right of the page, click **Create Mist Edge**.

Figure 105: Create Juniper Mist Edge VM



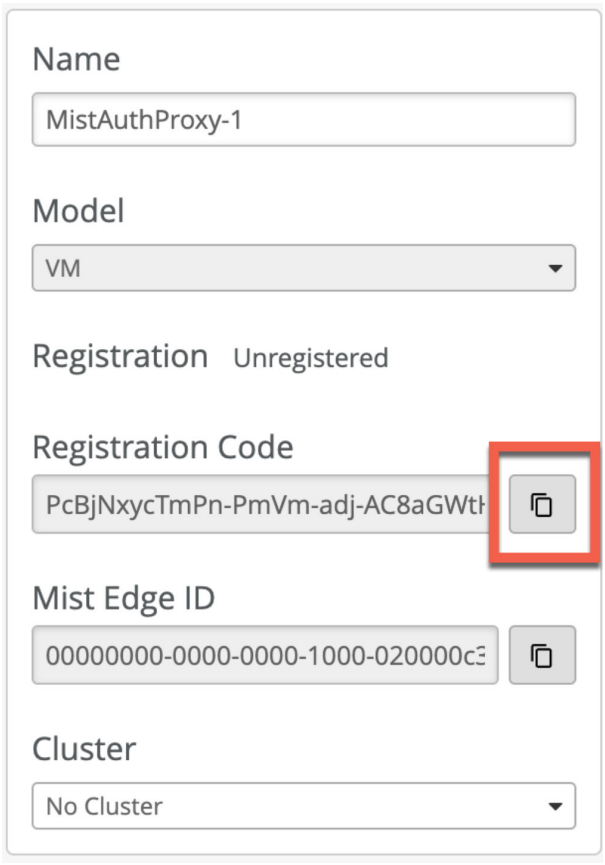
2. On the Create Mist Edge page, enter a name for the Juniper Mist Edge device and select **VM** as the model.

Figure 106: Enter Details for Juniper Mist Edge VM



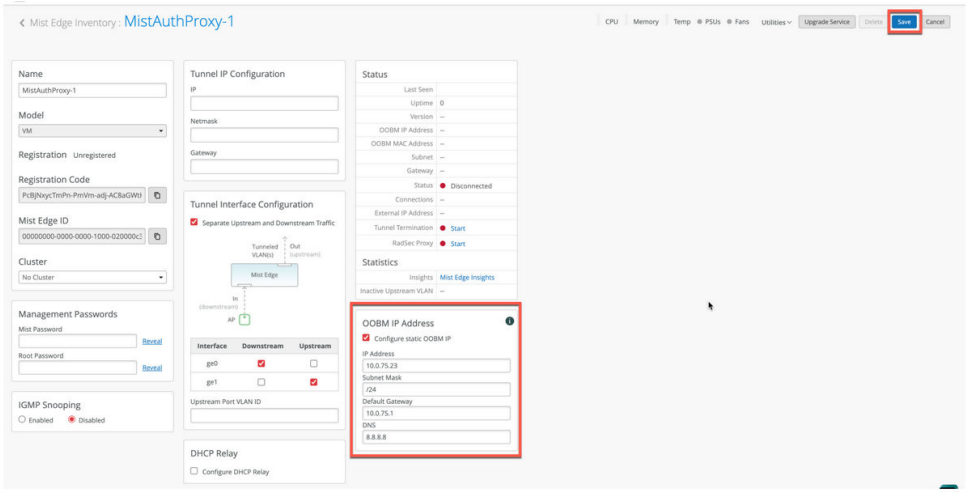
3. Copy the registration code and save the information.

Figure 107: Copy Registration Code



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.

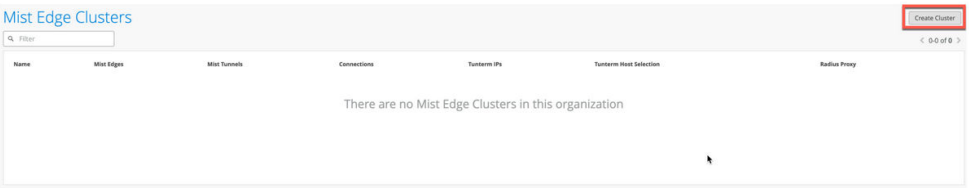
Figure 108: Juniper Mist Edge VM Out-of-Band Management IP Address



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

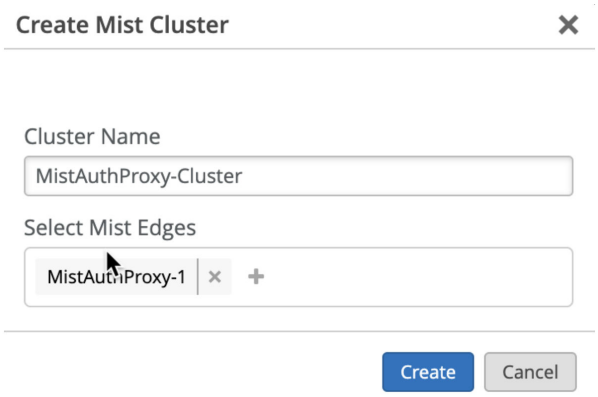
4. On the Mist Edge Inventory page, scroll down to the Mist Edge Clusters pane and click **Create Cluster**.

Figure 109: 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 110: Select Mist Edge VM for Cluster



6. Click **Create** to continue.
7. Provision your Juniper Mist Edge VM.

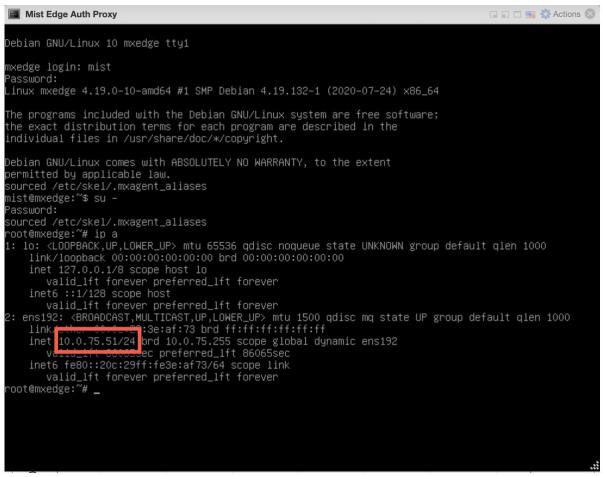
   After you configure the Juniper Mist Edge on the Juniper Mist portal, connect to the console interface.

   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 111: Provision Juniper Mist Edge VM



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 112: Juniper Mist Edge VM in Mist Edge Inventory

SEE ALSO

- Use Digital Certificates | **135**
- Configure Certificate-Based (EAP-TLS) Authentication | **164**
- Configure Certificate-Based (EAP-TLS) Authentication with Azure IdP Integration | **183**
- Configure MAC-Based Authentication and MAC Authentication Bypass (MAB) | **177**
- Add Identity Providers for Juniper Mist Access Assurance | **23**

Juniper Mist Authentication Proxy: Third-Party Device Support

SUMMARY

Follow these steps to use Juniper Mist Authentication Proxy to support end-client and management-user authentication into third-party devices such as Cisco IOS devices.

IN THIS SECTION

Overview

IN THIS SECTION

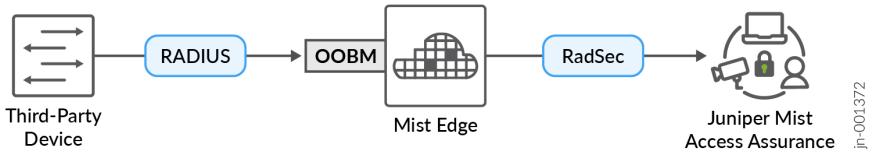
Juniper Mist™ Access Assurance supports end-client and management-user authentication into third-party devices by leveraging a Mist Auth Proxy application running on a Mist Edge platform.

Mist Edge is managed by the Mist Cloud and servers as a “gateway” for any non-Mist managed device that needs to:

- Perform authentication of end-clients connecting to it (for example, a third-party switch, wireless LAN controller, or access point (AP)
- Authentication management-users (for example, admin login to a firewall or switch CLI management interface)

To set this up, you'll add your third-party devices as RADIUS clients at the Mist Edge Cluster. The cluster wraps all authentication traffic into a secured RadSec tunnel and sends it to the Mist Access Assurance cloud.

Figure 113: Juniper Mist Edge as Auth Proxy—Flow of Connections



Design Considerations

- Mist Edge can serve as authentication proxy from multiple sites; it is not required to have an edge per site.
- For redundancy purposes, we recommend to install at least a few Mist Edges in different data centers or points of presense (PoP).

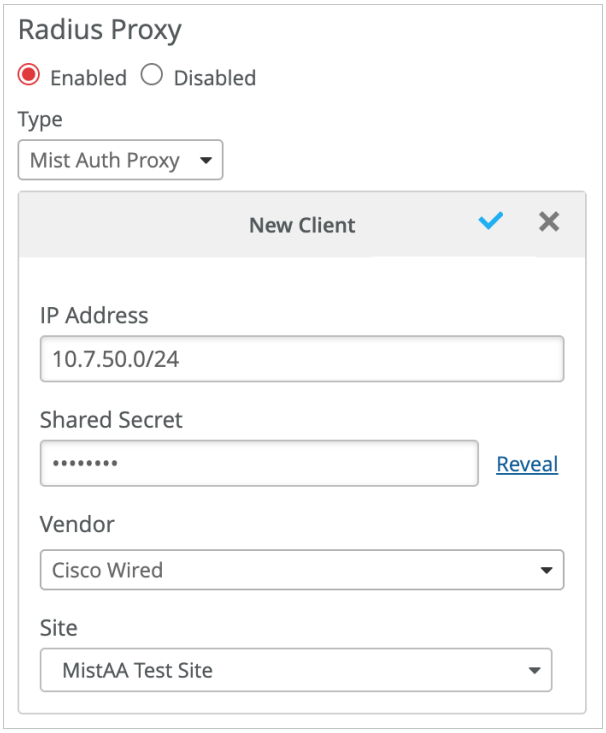
- Mist Auth Proxy functionality is supported on all Mist Edge platforms. We recommend that you use a dedicated Mist Edge appliance (or VM) for Mist Auth Proxy and avoid combining Mist Auth Proxy with Tunterm or OCProxy functionality.
- If you are using Mist Edge VM, note that you need only a single network interface and need **ME-VM-OC-PROXY** to unlock the Mist Auth proxy functionality.

About RADIUS Attributes

- Based on the configured vendor, Mist Access Assurance automatically sends correct RADIUS Attributes in access-accept response to assign VLANs, roles (firewall filters) and session timeouts.
- Leverage custom vendor-specific RADIUS attribute labels to send specific attribute back in case of any special use cases.

Add a Third-Party Vendor and Configure an Authentication Policy

1. **Mist Edge Cluster Configuration:** Add your third-party vendor as a RADIUS client in your cluster configuration:
   a. From the left menu of the Juniper Mist portal, select **Mist Edges**.
   b. Under **Mist Edge Clusters**, click an existing cluster or create a new cluster.
   c. On the cluster page, under **Radius Proxy**, click **Enabled**.
   d. Set type as **Mist Auth Proxy**.
   e. Click **Add Client**.
   f. Enter the information for the new client:
      - IP Address
      - Shared Secret
      - Vendor
      - Site (optional)



g. Click the checkmark at the top of the New Client section to save your settings.

h. Click **Save** at the top-right corner of the Mist Edge Clusters page.

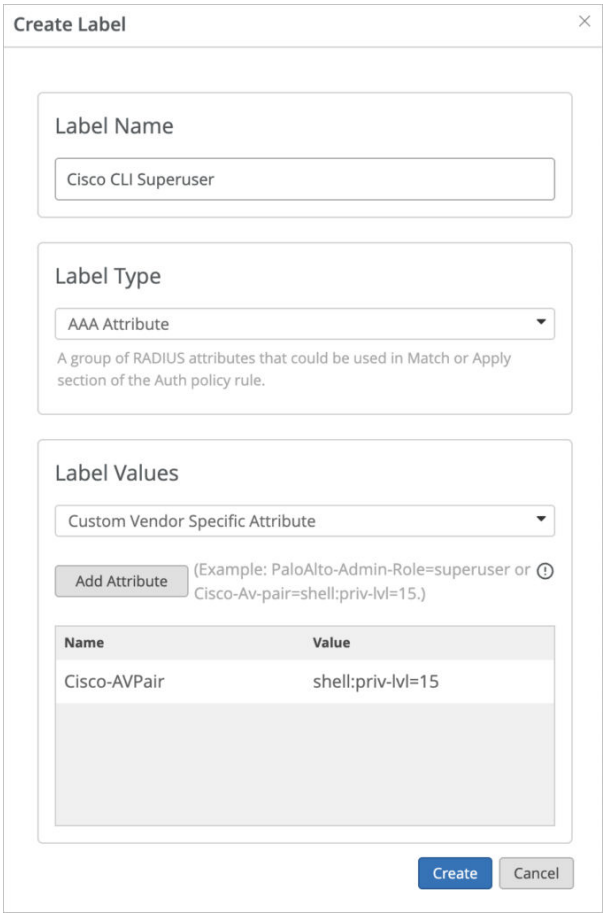
2. **Resource Label:** Add a label to identify your third-party vendor device as a resource that you can use later in your auth policies.

   a. From the left menu, select **Organization** > **Access** > **Auth Policies**.

   b. At the top of the Auth Policies page, click **Create Label**.

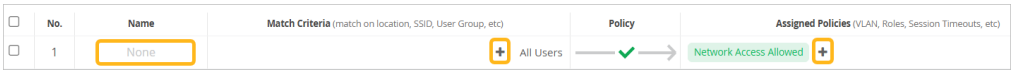
   c. Enter the following information:

   - Label Name—Enter a descriptive label so that you'll recognize this third-party vendor device when you're using this label in your auth policies.
   - Label Type—Select **AAA Attribute**.
   - Label Values—Select **Custom Vendor Specific Attribute**.
   - Click **Add Attribute**, enter a **Name** and a **Value**, and then click **Create**.



3. **Auth Policy:** Add a rule to identify the users who get authenticated by your third-party device.
   a. At the top of the Auth Policy page, click **Add Rule**.

      The new rule appears at the top of the rules, numbered. 1.

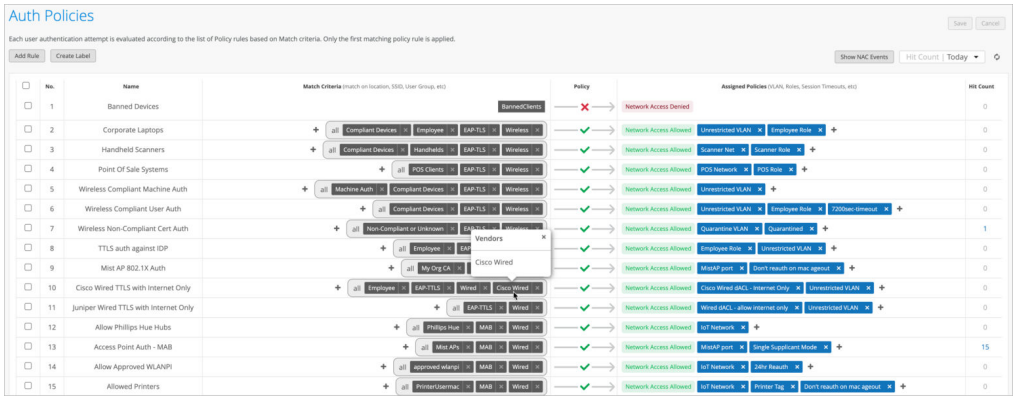


   b. Enter the information for this policy:
      - Name—Enter a descriptive name to identify the purpose of this policy.
      - Match Criteria—Click +, and then select the users or user groups that are authenticated by this vendor device.
      - Policy—Leave the green checkmark in place because you want to allow these users to access the resource.
      - Assigned Policies—Click +, and then select the label that you created for your third-party vendor device.

   c. Click **Save** at the top-right corner of the Auth Policies page.

4. Add rules for additional vendors as needed.

   This example shows numerous rules for different purposes. You can hover over any resource or user label to see more information.



Configure your third-party vendor device to use Mist Edge as the RADIUS server.

Configuring Your Third-Party Vendor Device

Point your third-party vendor devices towards Mist Edge OOBM IP address as the RADIUS server.

If you're deploying multiple Mist Edges, add each Mist Edge as RADIUS server in failover or load-balance mode, depending on your third-party device support.

Example: Cisco IOS Device Configuration

```
!
aaa group server radius Mist-Access-Assurance
server name MistEdge
deadtime 2
!
aaa authentication login default group Mist-Access-Assurance
aaa authorization exec default group Mist-Access-Assurance
!
!
!
radius server MistEdge
address ipv4 <mist edge OOBM IP Address> auth-port 1812 acct-port 1813
key <shared secret>
!
```

NOTE: When verifying a login, always add the domain name for the user, such as user123@company.net@10.148.2.21

Checking Login Records

As part of your verification process for your new auth policy, you can check the status of all login attempts on the NAC Clients page and the NAC Events page.

Figure 114: NAC Clients Page

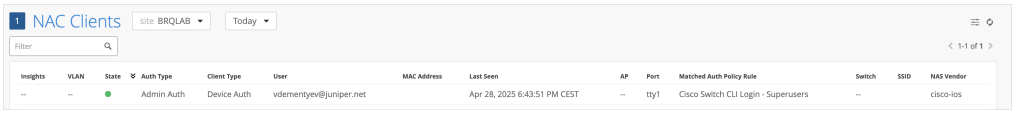
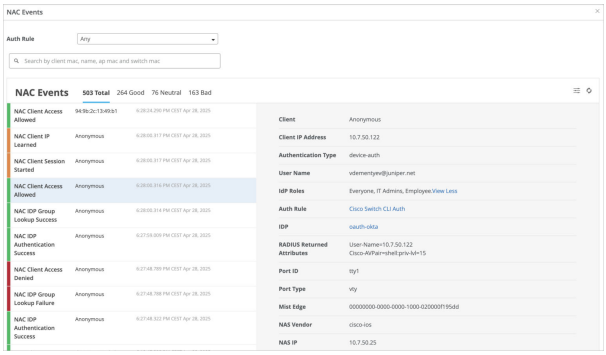


Figure 115: NAC Events



Use Case: Mist Edge Proxy for Eduroam

SUMMARY

As you plan your Juniper Mist™ and eduroam deployment, read through this use case to see how you can integrate Juniper Mist Access Assurance with eduroam by using Mist Edge as an IdP Proxy.

IN THIS SECTION

Overview

IN THIS SECTION

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.

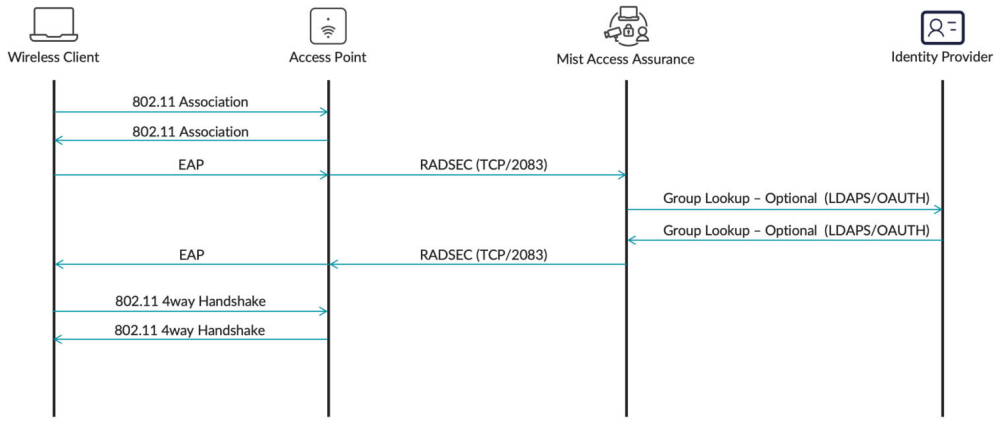
Mist Edge Proxy is used in particular with eduroam SP and IdP authentication flows; it does not affect home users authentication.

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.

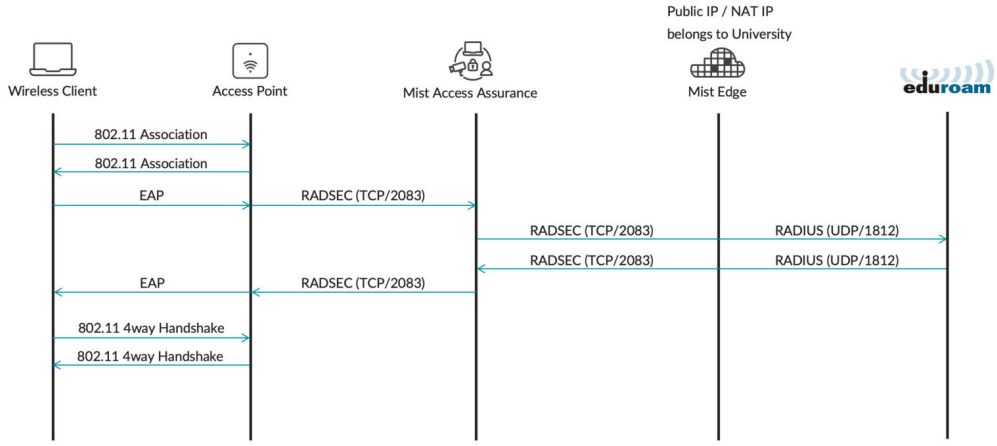
This scenario does not require Mist Edge proxy. The user authenticates directly with Mist Access Assurance.



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.

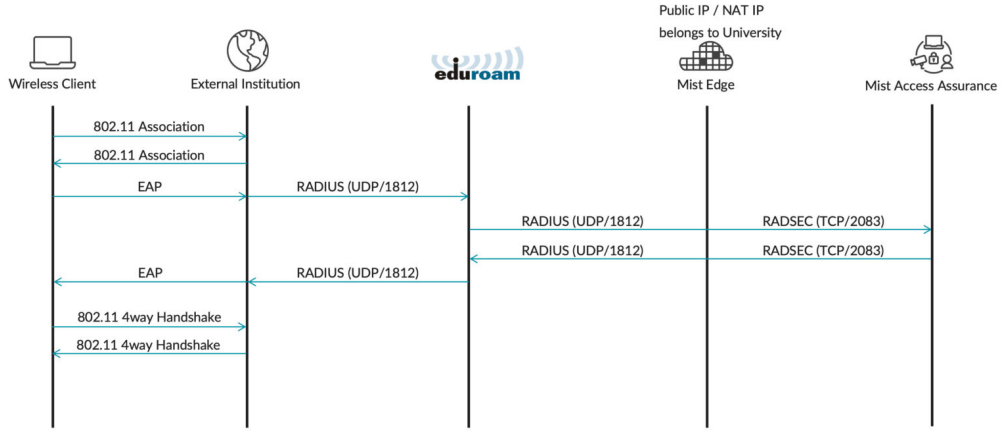
This scenario requires Mist Edge Proxy IDP to forward authentication requests to university2.edu via eduroam RADIUS servers. External visitors authenticate via a Mist Edge proxy, where Mist Edge the proxies authentication requests towards the eduroam national RADIUS servers.



Home Roaming Users

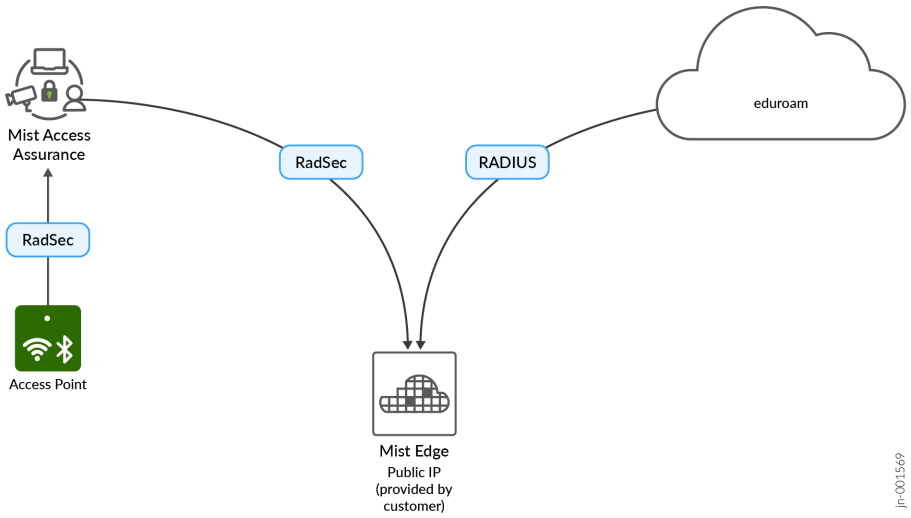
Home roaming users are clients who are visiting a different institution and would like to authenticate to an eduroam SSID by using their home university credentials.

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. You need to ensure that traffic can flow to and from the Mist Edge OOBM interface.



Allow the following ports and destinations:

- **Inbound** (towards Mist Edge OOBM interface)
  - RADIUS Auth & Acct (1812 / 1813 UDP). You can limit source IPs to eduroam national RADIUS servers.
  - RadSec (2083 TCP). You can 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. Onboard your Mist Edge devices and create a Mist Edge cluster.

   Tips:

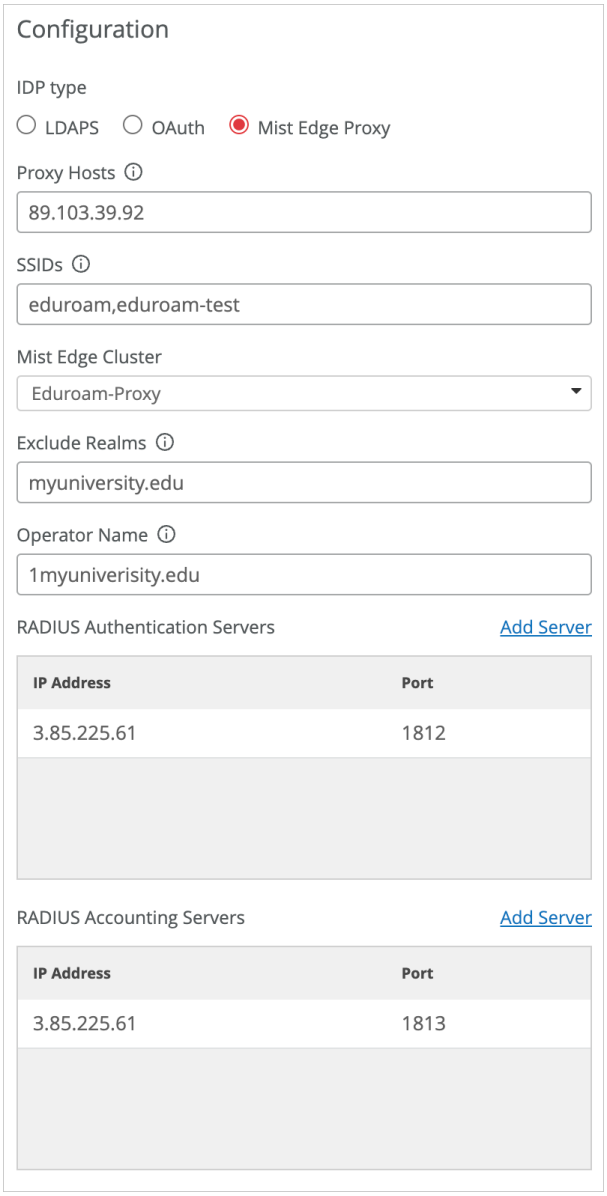
   - To add a device—From the left menu, select **Mist Edges**. Click **Claim Mist Edge** for a previously onboarded device or click **Create Mist Edge** for a new device.
   - To add a Mist Edge cluster—From the left menu, select **Mist Edges**. On the Mist Edges page, click **Create Cluster**. Enter a name, and select the edge devices to include.

2. Add a Mist Edge Proxy IDP.

   Tips:

   - To add an Identity Provider using Mist Edge Proxy—From the left menu, select **Organization** > **Access** > **Identity Providers**. In the Static Configuration section of the page, click **Add IDP**. Select **Mist Edge Proxy** as the IDP type. Complete the fields in the Configuration section. Refer to the on-screen tips for help.
   - To specify Proxy Hosts—Enter the public IPv4 addresses that Mist Edge will listen on for RadSec and RADIUS requests. All of these devices must belong to the specified Mist cluster.
   - To exclude domains/realms from this proxy—Enter the domains/realms, separated by commas. For example, in most cases you'll use local authentication for your own users, so you'd exclude the domain for your university, such as myuniversity.edu.
   - To specify the RADIUS Operator-Name attribute in requests—Enter the attribute in this format: 1<fqdn> such as 1myuniversity.com.

   Example



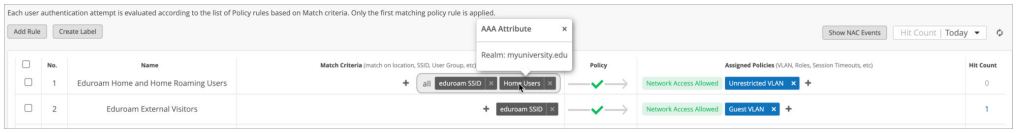
For more information, see "Add Identity Providers for Juniper Mist Access Assurance" on page 23.

3. Configure access rules for your users and visitors.

   Tips:

   - To add a policy—From the left menu, select **Organization** > **Access** > **Auth Policies**.Click **Add Rule**. Enter a name, match criteria, action (allow or block), and policies.
   - For detailed instructions—See "Configure Authentication Policy" on page 141.

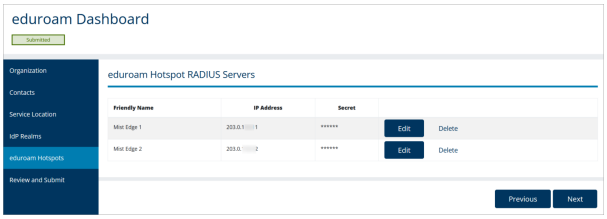
   The following example shows a rules applying to all three types of users. The first rule places home and home roaming users into the primary university VLAN. The second rule places external visitors into a guest VLAN.



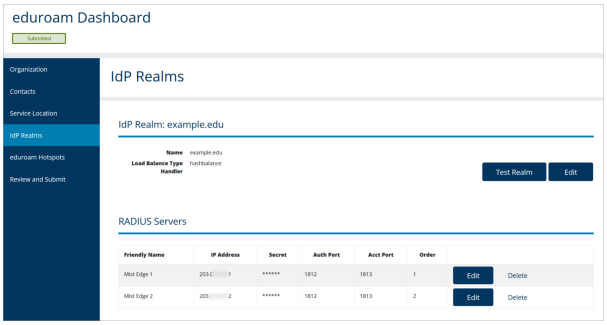
Configure eduroam

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



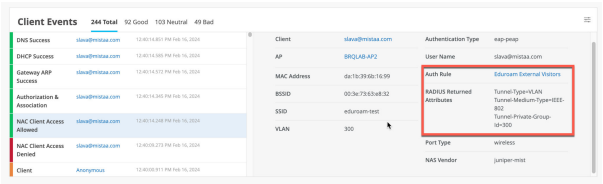
Eduroam IdP Realms



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).



Troubleshooting Tip: If you're not seeing the expected results, review the firewall configuration. Make sure that you've opened all the required ports and destinations.

5

CHAPTER

Monitoring

IN THIS CHAPTER

Juniper Mist Access Assurance NAC Clients

SUMMARY

Get visibility into the user experience for your wireless and wired client devices by using the NAC Clients page.

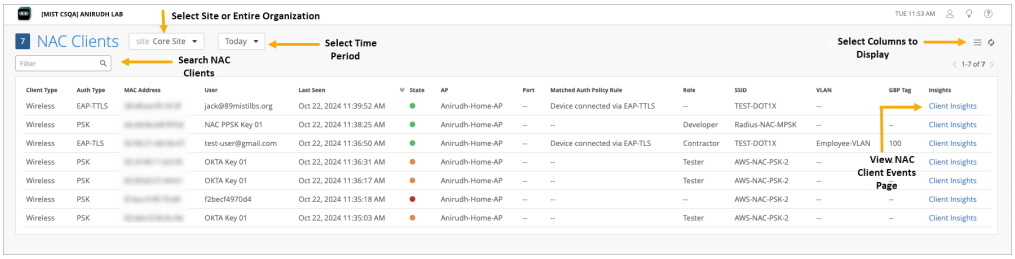
The client data includes information about the present and past connections with details such as client type, users, auth type, MAC addresses and so on.

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.

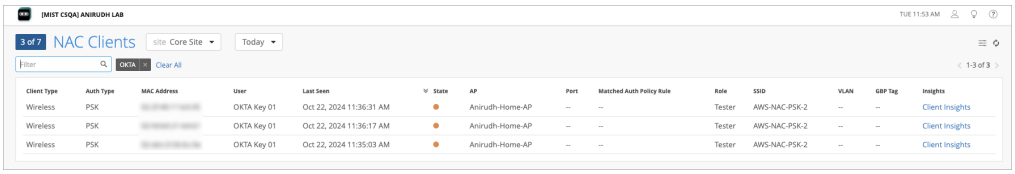
Figure 116: NAC Clients Page



- 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 117: Using Filter to Search Clients



- 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

Monitor the effectiveness of your access policies by using the NAC Events page.

IN THIS SECTION

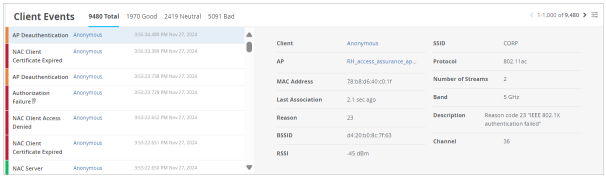
Finding the NAC Event Information

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

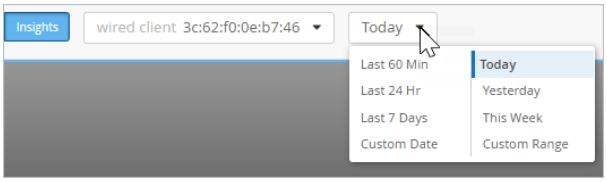
View NAC Events on the Insights Page

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.



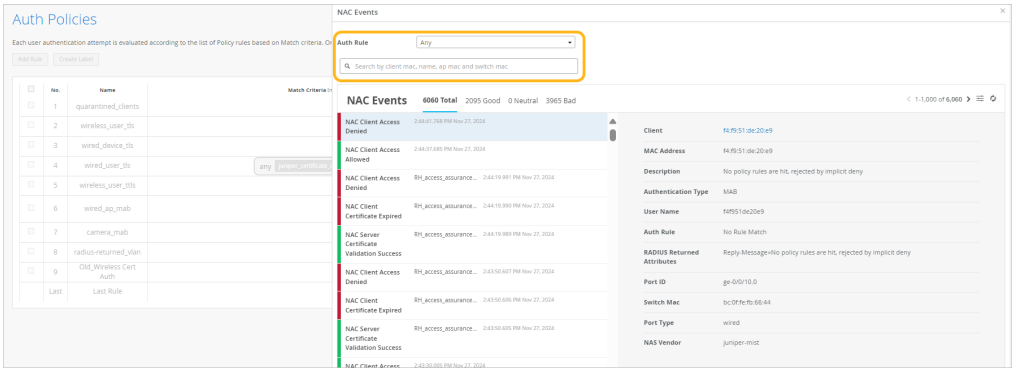
One advantage of this view is that you can use **Today** menu at the top of the Insights page to select the time frame that you want to view.



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.



View Options

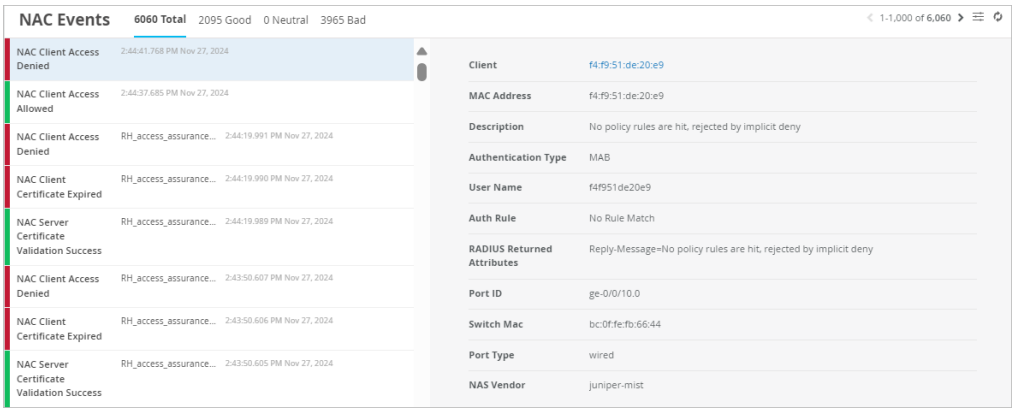
On both the Insights page and the NAC Events pop-up page, you can use various UI features to view information about NAC events.

- 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 298.
- 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.

- 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 13: NAC Event Types

Positive NAC Events	Neutral NAC Events	Negative NAC Events
• NAC Client Access Allowed • NAC Client Certificate Validation Success • NAC Machine Certificate Validation Success • NAC User Certificate Validation Success • NAC CoA Disconnect • NAC CoA Reauthenticate • NAC IDP Authentication Success • NAC IDP Group Lookup Success • NAC IDP User Lookup Success • NAC MDM Lookup Success • NAC Server Certificate Validation Success	NAC MDM Device Not Found	• NAC Client Access Denied • NAC Client Cert Revoked • NAC Client Certificate Expired • NAC Client Certificate Validation Failure • NAC Machine Certificate Expired • NAC Machine Certificate Revoked • NAC Machine Certificate Validation Failure • NAC User Certificate Expired • NAC User Certificate Revoked • NAC User Certificate Validation Failure • NAC IDP Admin Config Failure • NAC IDP Admin Config Failure • NAC IDP Authentication Failure • NAC IDP Group Lookup Failure • NAC IDP Lookup Failure • NAC IDP Unknown • NAC IDP Unreachable • NAC IDP User Disabled • NAC IDP User Lookup Failure

Table 13: NAC Event Types *(Continued)*

Positive NAC Events	Neutral NAC Events	Negative NAC Events
		• NAC MDM Lookup Failure • NAC Server Certificate Validation Failure

Validate Access and Authentication

SUMMARY

To ensure positive user experiences and quickly resolve authentication issues, check on connected and failed client devices, identify issues, and get guidance from Marvis about root causes and recommended actions.

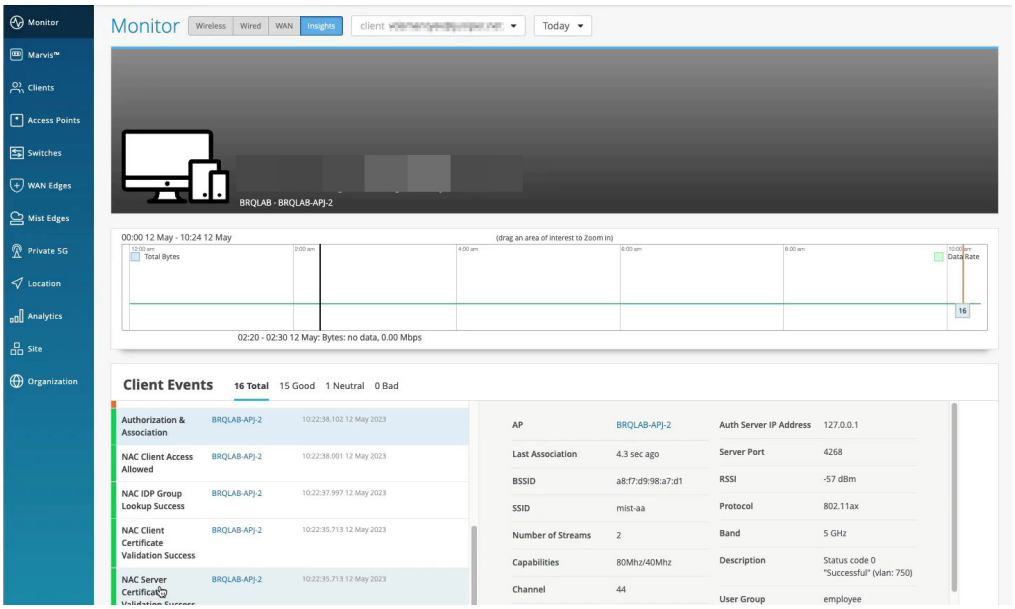
IN THIS SECTION

Check Connected Client Devices

1. On Juniper Mist portal, select **Clients > WiFi Clients** or **Clients > Wired Clients** to open the clients page.

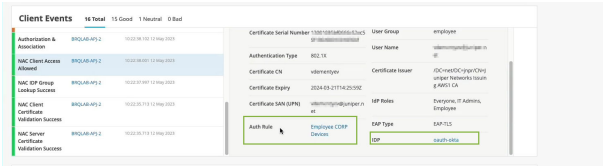
   This page lists all the clients connected to your site. It provides the details such as name, IPv4 address, MAC address, Type, and so on. You can also see the link to **Client Insights**. Click this link to go to **Monitor > Insights page** where you view get additional details.
2. Go to the Insights 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 118: View Mist Insights Page



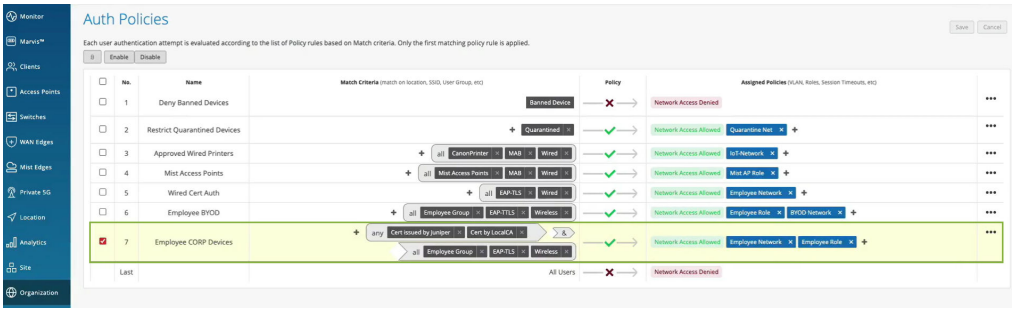
3. In the Client Events block, you can view a list of all events recorded by Mist PACE for the selected site during the selected time frame.

Figure 119: 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.

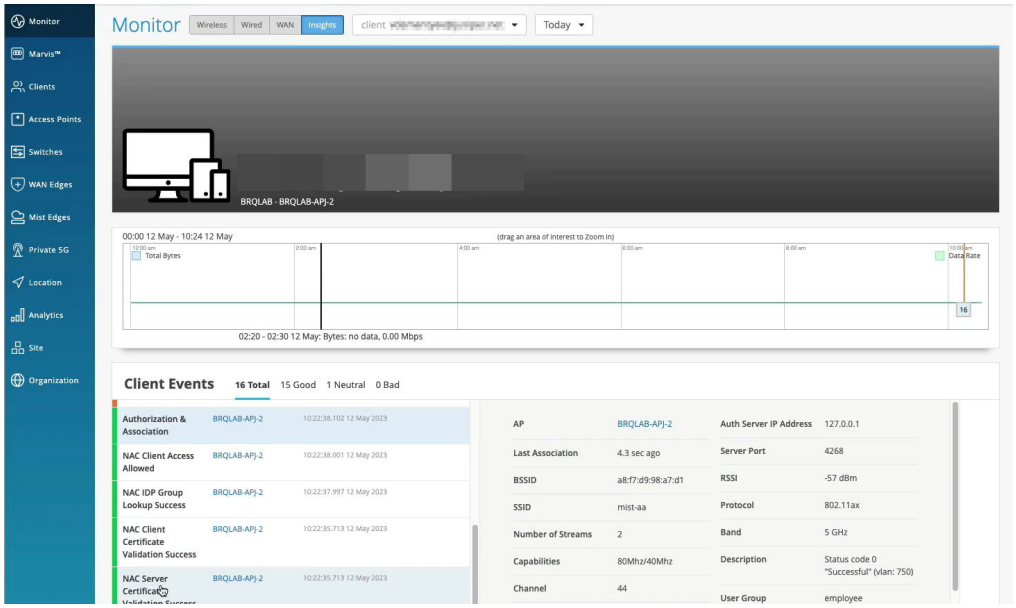
Watch the following video on validating access and authentication configuration:

Video: How to Validate

Check Failed Client Devices

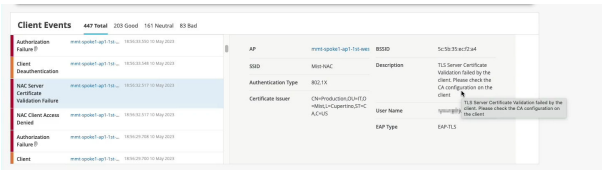
1. On Juniper Mist portal, select **Monitor > Service Levels** from the left menu of the Juniper Mist portal. Then click the **Insights** button at the top of the Monitor page.

Figure 120: 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 121: 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:

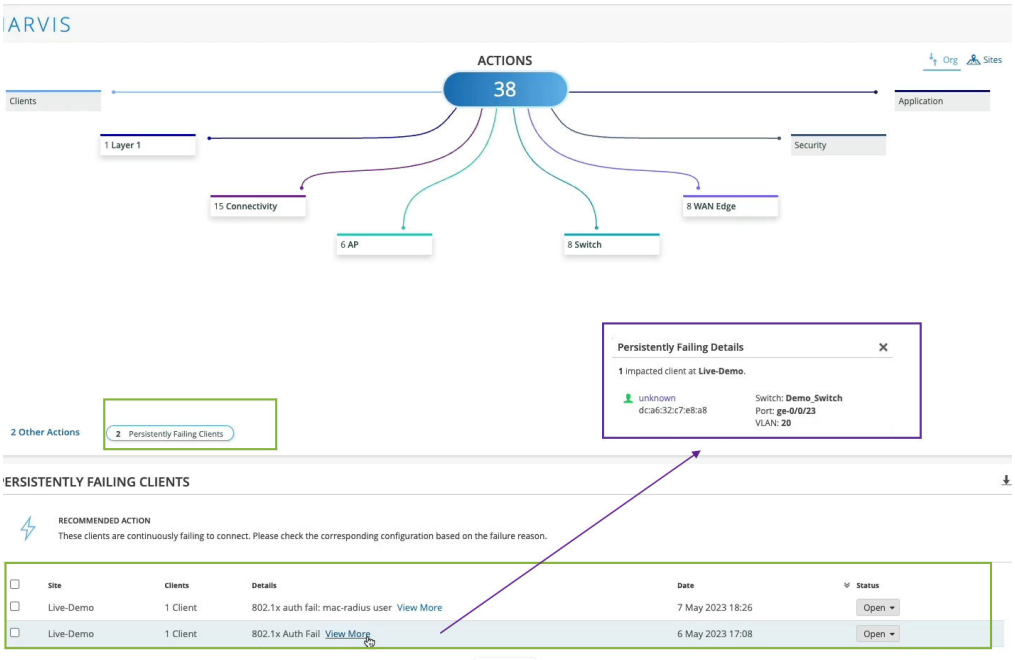
Video: Mist Access Assurance - Troubleshoot Client

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.

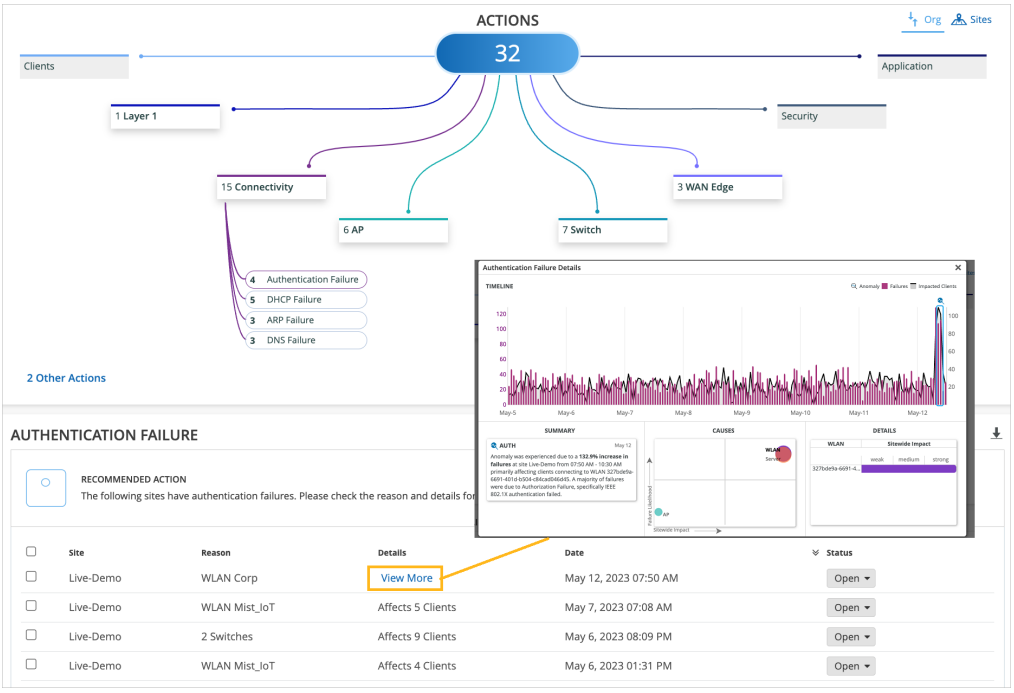
Click **View More** to get the details of the failing client. You can use this information to identify the location of users who are experiencing connectivity issues by pinpointing the specific switch, port, and VLAN they are connected to.

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.

2. 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 122: 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 | **295**

Configure Authentication Policy | **141**

Configure Certificate-Based (EAP-TLS) Authentication | **164**

Configure Certificate-Based (EAP-TLS) Authentication with Azure IdP Integration | **183**