Deploying and Managing Juniper Mist Access Assurance

Course overview

This two-day, intermediate-level course provides students with the knowledge to configure and monitor Juniper Mist™ Access Assurance. Key topics include the purpose of network access control (NAC); the Juniper Mist Access Assurance cloud architecture; Juniper Mist™ Edge authentication proxy; authentication, authorization, and accounting (AAA) components; 802.1X and Extensible Authentication Protocol (EAP) operations; RADIUS concepts; RADIUS over TLS (RadSec); authorization of 802.1X and non-802.1X devices; identity provider (IdP) integration; Juniper Mist Access Assurance authentication policies and methods; and integration with mobile device management (MDM). The lab includes Juniper Mist Access Assurance, the Juniper Networks® EX4400 Switch, and the Juniper® AP45 High-Performance Access Point.

Course level

Deploying and Managing Juniper Mist Access Assurance is an intermediate-level course.

Audience

The primary audiences for this course include individuals responsible for implementing and monitoring Juniper Mist Access Assurance.

Prerequisites

- General understanding of TCP/IP.
- General understanding of security concepts.
- Completion of the *Introduction to Juniper Mist AI* course, which is recommended but not required.

Related products

Juniper Mist Edge, Juniper Mist Access Assurance, Mist AI

Recommended next course

- *Deploying and Managing Juniper Wireless Networks with Mist AI*

Objectives

- Describe the purpose of and the need for NAC.
- Explain the Juniper Mist Access Assurance cloud architecture.
- Discuss third-party device support with Juniper Mist Edge authentication proxy.
- Describe common use cases with Juniper Mist Access Assurance.
- Discuss Juniper Mist Access Assurance best practices.
- List AAA components.
- Discuss how the RADIUS protocol works.
- Describe RADIUS server attributes.
- Explain the functionality of RadSec.
- Explain 802.1X operations.
- Discuss the Juniper Mist Access Assurance 802.1X certificate and password authentication methods.
- Explain how Juniper Mist Access Assurance can authenticate devices that don’t support 802.1X.
- Describe IdP integration with Juniper Mist Access Assurance.
- Explain how to configure Juniper Mist Access Assurance authentication policies with match labels and action labels.
- Discuss how to configure Juniper Mist Access Assurance authentication methods.
- Explain how to configure Juniper Mist Edge for the Juniper Mist authentication proxy function.
- Describe how to validate Juniper Mist Access Assurance access and authentication.
- Implement Juniper Mist Access Assurance with wired and wireless devices.

- Discuss Juniper Mist Access Assurance integration with MDM providers.

Course contents & objectives

Day 1

Module 01: Understanding Network Access Control

- Describe the components of network access control
- Explain the history of network access control
- Explain Juniper Mist Access Assurance

Module 02: Juniper Mist Access Assurance—Overview

- Explain the cloud architecture
- Explain Juniper Mist-managed devices and requirements
- Describe third-party device support
- Describe the client use cases of Juniper Mist Access Assurance
- Describe the best practices of Juniper Mist Access Assurance

Module 03: RADIUS

- Explain the components of AAA
- Describe how RADIUS works
- Describe RADIUS Change of Authorization

Module 04: X.509 Certificates and PKI

- Describe the purpose and structure of X.509 certificates and PKI

Module 05: 802.1X and EAP Authentication

- Describe 802.1X operations
- Describe EAP operations

Module 06: Identity Providers

- Explain how to use identity providers with Juniper Mist Access Assurance
- Describe Eduroam
- Lab 01: Initial Lab Configuration

Day 2

Module 07: Configuring 802.1X Client Authentication

- Describe authentication policy configuration
- Describe EAP-TLS configuration
- Describe EAP-TTLS configuration
- Lab 02: Configuring 802.1X Client Authentication

Module 08: Non-802.1X Client Authentication

- Explain non-802.1X clients
- Describe MSPK authentication and configuration
- Describe client onboarding using the PSK Portal
- Describe MAB authentication and configuration
- Describe Juniper Mist Access Assurance endpoint management
- Lab 03: Non-802.1X Client Configuration

Module 09: Posture Compliance

- Explain posture compliance
- Describe Microsoft Intune integration
- Describe JAMF Pro integration
- Describe how to verify compliance

Module 10: Integrating Juniper Mist Edge

- Define the features and benefits of Juniper Mist Edge
- Describe Juniper Mist Edge installation
- Explain Juniper Mist Edge as a RADIUS server proxy
- Explain Juniper Mist authentication proxy
- Describe Access Assurance Site Survivability
- Summarize the DHCP relay service
- Review the Juniper Mist Edge management functions

Resources

All-Access Training Pass

On-Demand

Courses

Schedule

Learning Paths

Certification

Key contacts

Americas: networking.training.ams@hpe.com

Europe, Middle East, Africa: networking.training.emea@hpe.com

Asia Pacific & Japan: networking.training.apj@hpe.com

Asset ID

Visit HPE.com

Chat now

© Copyright 2026 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty.
Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Trademark acknowledgments, if needed. All third-party marks are property of their respective owners.

EDU-JUN-JMAA, Revision 26A

HPE.com