# Course Description



Aruba Advanced ClearPass Configuration

This advanced course uses a real-world case study on which participants will learn how to design, deploy and troubleshoot several aspects of the ClearPass security product. This 5-day training is focused on active student participation, design exercises, introduction of new features and hands-on labs.

The lectures introduce different customer requirements and explain the fundamentals under the technologies required to fulfill them, while the lab guide displays the entire process from planning all the way up to implementation, testing and troubleshooting if required. Through this process the candidates will acquire skill sets that prepare them to face any challenging scenario.

# Ideal candidate for this course

Typical candidates for this training include:

* Network Security Experts
* Individuals who implement network access control solutions.
* Network managers with Aruba access device experience (wired & wireless).
* Network administrators who already own a ClearPass solution and are looking to deploy advanced features.

# Suggested Prerequisites

* Any current Aruba ClearPass certification.
* Aruba ClearPass Configuration course

# Topics

* Network Requirements
  + ClearPass Goals
  + Network Topology
  + List of available resources
  + Scenario Analysis
  + Authentication requirements
  + Multiple user account databases
  + User Account attributes
  + High Level Design
* PDI and Digital Certificates
  + Certificate Types
  + PKI
  + Certificate Trust
  + Certificate File Formats
  + ClearPass as CA



* + Certificate Use cases:
    - EAP
    - HTTPS
    - Service-based certificates
    - Onboarding
    - Clustering
    - RadSec
    - NAD Captive Portal
  + Installing Certificates
  + Enrollment over Secure Transport
* Cluster Design
  + ClearPass Server Placement
  + Determine the layout of the Cluster
  + High-Availability Schema
  + Design High-Availability
  + VIP Failover
  + VIP Mapping
  + Insight Primary and Secondary
* Network Integration
  + Authentication Sources
    - Local User Repository
    - Endpoint Repository
    - Admin User Repository
    - Guest User Repository
    - Guest Device Repository
    - Onboard Device Repository
    - Active Directory
    - SQL Server
  + Define External Servers
    - Unified Endpoint Management
    - Email Server
  + Endpoint Profiling
    - IF-MAP
    - Active Scans (SNMP)
    - DHCP
    - HTTPS
  + Network Devices
    - RadSec
    - Dynamic Authorization
    - Logging of RADIUS Accounting
    - Device-groups
    - Location Attributes
  + Policy Simulation
* Corporate Access Design
  + Define the Requirements
  + High-level design
  + Services Design
  + Plan TIPs Roles
  + User Authentication
  + Machine Authentication
  + Tunneled EAP, EAP-TLS and Protected EAP
  + One versus Multiple Services
  + Plan Enforcement
  + Device-groups based Enforcement
  + Service Implementation
  + OnGuard Design and implementation
    - Quarantine users
    - Remediation
  + Onboard Design and implementation
    - User and device authorization
  + Informational Pages
  + Authorization validation
  + Troubleshooting Enforcement
  + Downloadable Roles



* Guest Access Design
  + Guest Network Design
  + Captive Portal Flow
  + Design Tasks
  + Define Web Pages
  + Guest Services Design
  + Guest Services
  + Guest Access Controls
  + Configure Network Access Devices
  + Guest Account Creation
  + Guest Self-Registration
  + Guest Sponsor Approval
  + Self-Registration AD Drop-Down List
  + Requirements for Guest Enforcement
* Multi-Pre Shared Key
  + Define the Requirements
  + High-level design
  + Device authorization
  + Service Design and implementation
* Wired Access
  + AAA configuration
  + 802.1X and MAC auth
  + Using client profiling for authorization
  + Using conflict attribute for authorization
  + User Roles configuration in ArubaOS-S
  + User Roles configuration in ArubaOS-CX
  + Web Redirection
  + Multi-Service Ports
  + Downloadable User Roles Enforcement Profiles
  + Downloadable User Roles Configuration and Validation
* Administrative Access
  + TACACs+ based NAD administration
  + TACACs+ command Authorization
  + Policy Manager Administrators
  + Guest and Onboard Operators
  + Register devices for MPSK
  + Insight Operators
  + Insight Reports and Alerts

# Course Objectives:

After you successfully complete this course, expect to be able to:

* Design a ClearPass cluster
* Design a High availability solution with Virtual IP address following the best practices
* Describe Public Key Infrastructure and certificate format types
* Plan the certificates used by ClearPass
* Explain how Enrollment over Secure Transport can automate the certificate generation process
* Leverage RADIUS services to handle corporate wireless connections
* Deploy WEBAUTH services to handle health checks
* Describe the proposed RADIUS services that handles guest wireless connections
* Explain general guest considerations
* Design guest RADIUS services
* Describe the proposed Onboard services
* Describe the MPSK feature
* Leverage these features in your deployment
* Plan a successful wired access deployment
* Provide administrative access control to ClearPass modules and NADs
* Generate custom reports and alerts