



## JUNIPER ACCESS CONTROL

### Junos Pulse Access Control (JPAC)

#### Course Overview

This three-day course provides detailed coverage of the configuration of the Junos Pulse Access Control Service (JPACS) offered by Juniper Networks. Students will work with the solution elements—the JPACS, the SRX Series Services Gateways firewall enforcer, Junos Pulse, and the Odyssey Access Client (OAC)—to configure secured access to network resources. Key topics include JPACS deployment, basic implementation, and element configuration. Students will have the opportunity to apply their knowledge in several hands-on labs.

#### Objectives

After successfully completing this course, you should be able to:

- Introduction to JPACS
- Typical deployment scenarios
- Terminology
- JPACS configuration elements
- Roles
  - Authentication realms
  - Authentication servers
  - Resource policies
  - Sign-in policies
- Firewall enforcer configuration elements
  - Infranet policies
- Junos Pulse configuration elements
  - Connections
  - Location Awareness
  - Host Checker Integration
- Odyssey Access Client configuration elements
  - Host Checker Integration
  - Host Enforcer
- Troubleshooting

#### Target Audience

The intended audience for this course includes network engineers, support personnel, reseller support, and individuals responsible for implementing the Junos Pulse Access Control Service.

#### Course Level

Intermediate

#### Prerequisites

This course assumes that students have:

- know the TCP/IP protocol suite, including addressing and routing.
- have Ethernet experience, including addressing, basic switching operations and VLANs.
- have knowledge of basic security and access management concepts, including 802.1x and RADIUS.

It is recommended (but not required) that students attend the following courses:

- IJOS
- JSEC
- or have equivalent experience with Junos devices and SRX Series firewalls



**Chapter 1: Course Introduction**

**Chapter 2: Junos Pulse Access Control Service**

- Need for Access Control
- JPACS Components
- JPACS Component Interaction
- Sample JPACS Deployments

**Chapter 3: Initial Configuration**

- JPACS Initial Configuration: Console
- JPACS Initial Configuration: Admin UI
- Firewall Enforcer Initial Configuration
- Verification and Troubleshooting
- Lab 1: Initial Configuration

**Chapter 4: The Access Management Framework**

- Access Management Framework Elements

**Chapter 5: Roles**

- Configuring User Roles
- Role Mapping
- Configure Sign-in Policies
- Lab 2: Roles

**Chapter 6: Client Access Methods**

- Client Access Methods
- Configure Agent Access
- Configure Agentless Access
- Lab 3: Configure Client Access Methods

**Chapter 7: Firewall Enforcement**

- Resource Policy Overview
- Firewall Enforcement Overview
- Configure Firewall Enforcement
- Captive Portal
- Lab 4: Firewall Enforcement

**Chapter 8: Layer 2 Enforcement**

- 802.1X Operations
- RADIUS Elements
- MAC Authentication

**Chapter 9: Configuring Layer 2 Enforcement**

- Configure an 802.1X Authenticator
- Configure 802.1X Support on the JPACS
- Configure MAC Authentication
- Lab 5: Policy Configuration Using 802.1X

**Chapter 10: Endpoint Defence**

- What Is Host Checker?
- Host Checker Configuration
- Enhanced Endpoint Security (EES) Configuration
- Enforcing Policies
- Lab 6: Endpoint Security

**Chapter 11: Authentication Options**

- Authentication Process Review
- Configuring Authentication Servers
- Configuring Authentication Realms
- Lab 7: Authentication Options

**Chapter 12: Management and Troubleshooting**

- Logging
- System Monitoring
- Troubleshooting Component Communications
- Troubleshooting User Interactions
- Configuration File Management
- Working with JTAC
- Lab 8: Logging and Troubleshooting

**Chapter 13: High Availability**

- Describe High Availability
- JPAC Service Clustering
- Firewall Options
- Lab 9: JPAC Service Clustering

**Chapter 14: Integration**

- IF-MAP Federation
- NSM Integration
- STRM Integration
- IDP Integration

**Appendix A: Junos Pulse Gateway Chassis Management**

- CMC Benefits
- Configure CMC

**Appendix B: ScreenOS Enforcer Configuration**

- ScreenOS Policies
- Configure Firewall Enforcement
- Verify Operations

**Cost AUD \$2,299 inc. GST**

For Available Dates & T&Cs see: [www.crystalecho.com](http://www.crystalecho.com)