



JUNIPER ACCESS CONTROL

Juniper Networks Certified Internet Associate (JNCIA-AC)

CUAC - Configuring Unified Access Control (3 days)



Configuring Unified Access Control (CUAC)

Course Overview

This three-day course discusses the configuration of the Unified Access Control solution offered by Juniper Networks. Students will work with the solution elements—the Infranet Controller, the Infranet Enforcer, and the Infranet Agent—to configure secured access to network resources. Key topics include Unified Access Control 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 deploy the Infranet Controller and Infranet Enforcer to support common environments. Specific topics include:

- Introduction to Unified Access Control
- Typical deployment scenarios
- Terminology
- Infranet Controller configuration elements
- Roles
- Authentication realms
- Authentication servers
- Resource policies
- Sign-in policies
- Overlay Enforcer configuration elements
 - Infranet policies
- Odyssey Access client configuration elements
- Host Checker
- Host Enforcer
- Troubleshooting

Target Audience

The intended audience for this course includes network engineers, support personnel, reseller support, and anyone responsible for implementing the Unified Access Control products.

Prerequisites

Completion of Configuring Juniper Networks Firewall/IPSec VPN Products (CJFV) or equivalent experience with ScreenOS firewalls is required. The course also assumes that students understand internetworking basics, basic security concepts, network administration, application support, and basic remote access concepts.

Chapter 1: Course Introduction

Chapter 2: The UAC Solution

- Need for Unified Access Control
- UAC Components
- UAC Component Interaction
- Sample UAC Deployments

Chapter 3: Initial Configuration

- Infranet Controller Initial Configuration: Console
- Infranet Controller Initial Configuration: Admin UI
- Overlay Enforcer Initial Configuration
- Verification and Troubleshooting
- Lab 1: Initial Configuration

Chapter 4: The Access Management Framework

- Access Management Framework Elements

Chapter 5: Overlay Enforcement

- Layer 3 Secure Access Options
- Policy Type



crystalecho.com

Chapter 6: Configuring Overlay Enforcement

- Overlay Enforcement Configuration
- Verifying Operations
- Lab 2, Parts 1 and 2: Overlay Enforcement
- Configuring Additional Features
- Lab 2, Part 3: Guest Access and Additional Features

Chapter 7: Endpoint Security

- What Is Host Checker?
- Host Checker Configuration
- Remediation Options
- Lab 3: Endpoint Security

Chapter 8: Layer 2 Enforcement

- 802.1X Operations
- RADIUS Elements
- MAC Authentication

Chapter 9: Configuring Layer 2 Enforcement

- Configuring an 802.1X Authenticator
- Configuring 802.1X Support on the IC
- Configuring MAC Authentication
- Lab 4: Policy Configuration Using 802.1X

Chapter 10: Management and Troubleshooting

- Logging
- Monitoring
- Troubleshooting Component Communications
- Troubleshooting User Interactions
- Configuration File Management
- Lab 5: Logging and Troubleshooting

Chapter 11: Authentication Options

- The Authentication Process
- Configuring Authentication Servers
- Configuring Authentication Realms
- Lab 6: Authentication Options

Chapter 12: Integration

- IC Clustering
- NSM Integration
- STRM Integration
- IDP Integration
- Firewall Options
- NAP Interoperability

Cost AUD \$2,299 inc. GST

For Available Dates & Terms and Conditions see:
www.crystalecho.com

JUNIPER
NETWORKS
EDUCATION SERVICES
AUTHORIZED PARTNER