

## JNCIA-AC Exam Objectives (Exam: JN0-140)

This list is intended to provide a general view of the skill set required to successfully complete the specified certification exam. Topics listed are subject to change.

- UAC Overview
- Access Management Framework
- Endpoint Defense

### UAC Overview

- List the key elements of the UAC solution
- Describe the functionality of UAC solution elements
- Describe the problems addressed by the UAC solution
- List UAC deployment options
- Perform initial configuration with the console and GUI
- Configure initial connectivity between the IC and the Overlay Enforcer
- Verify UAC connectivity

### Access Management Framework

- General Access Management
- Discuss Dynamic policy evaluation
- User Roles
- Configure user roles, UI and Session settings
- List the types of restrictions available at the role level
- Configure agent access for a role
- Resource Policies
- Configure Source IP enforcement policy
- Configure IPSec enforcement policy
- Describe the relationship between the access method and resource policy
- Describe Host Enforcer policy
- Authentication Servers
- Configure Radius servers settings
- Configure connectivity for AD/NT authentication
- Configure connectivity for LDAP authentication
- Authentication Realms
- Identify the settings configured in a realm
- Identify server combinations that are used for authentication and directory.

- Describe role mapping order and the effects of stop rules
- Configure user name and groups based role mapping
- Configure LDAP attribute role mapping
- Discuss pre and post authentication policies
- Sign-in Policies
- Describe Sign-in Policy options and Restrictions
- Describe how to enable and disable a Sign-in policy
- Discuss preconfiguring the Odyssey Access Client
- 802.1x
- Configure the Infranet Controller as a Radius Server
- Configure Location Group policies
- Configure Radius client policies
- Configure Radius attribute policies
- Describe how to use the Infranet Enforcer as a Radius Client
- Discuss deployment options used with 802.1x

## **Endpoint Defense**

- Identify the functionality of host checker
- Create Host Checker policies
- Implement Host Checker at the realm and role level
- Describe and manage integrated scan components (ESAP updates)