Implementing and Configuring Cisco Identity Services Engine v1.1 (300-715)

Exam Description: Implementing and Configuring Cisco Identity Services Engine v1.1 (SISE 300-715) is a 90-minute exam associated with the CCNP Security Certification. This exam tests a candidate's knowledge of Cisco Identity Services Engine (ISE), including architecture and deployment, policy enforcement, Web Auth and guest services, profiler, BYOD, endpoint compliance, and network access device administration. The course, Implementing and Configuring Cisco Identity Services Engine, helps candidates to prepare for this exam.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

10% **1.0** **Architecture and Deployment**

- 1.1 Configure personas
- 1.2 Describe deployment options
- 1.3 Describe hardware and virtual machine performance specifications
- 1.4 Describe zero-touch provisioning

25% **2.0** **Policy Enforcement**

- 2.1 Configure native AD and LDAP
- 2.2 Describe identity store options
  - 2.2.a LDAP
  - 2.2.b AD
  - 2.2.c PKI
  - 2.2.d Multifactor authentication
  - 2.2.e Local
  - 2.2.f SAML IDP
  - 2.2.g Rest ID
- 2.3 Configure wireless network access using 802.1X
- 2.4 Configure wired network access using 802.1X and IBNS 2.0
  - 2.4.a Monitor mode
  - 2.4.b Low impact
  - 2.4.c Closed mode
- 2.5 Implement MAB
- 2.6 Configure Cisco TrustSec
- 2.7 Configure policies including authentication and authorization profiles

15% 3.0 Web Auth and Guest Services

- 3.1 Configure web authentication
- 3.2 Configure guest access services
- 3.3 Configure sponsor and guest portals

15% 4.0 Profiler

- 4.1 Implement profiler services
- 4.2 Implement probes
- 4.3 Implement CoA
- 4.4 Configure endpoint identity management

15% 5.0 BYOD

- 5.1 Describe Cisco BYOD functionality
  - 5.1.a Use cases and requirements
  - 5.1.b Solution components
  - 5.1.c BYOD flow
- 5.2 Configure BYOD device on-boarding using internal CA with Cisco switches and Cisco wireless LAN controllers
- 5.3 Configure certificates for BYOD
- 5.4 Configure block list/allow list

10% 6.0 Endpoint Compliance

- 6.1 Describe endpoint compliance, posture services, and client provisioning
- 6.2 Configure posture conditions and policy, and client provisioning
- 6.3 Configure the compliance module
- 6.4 Configure posture agents and operational modes
- 6.5 Describe supplicant, supplicant options, authenticator, and server

10% 7.0 Network Access Device Administration

- 7.1 Compare AAA protocols
- 7.2 Configure TACACS+ device administration and command authorization

2023 Cisco Systems, Inc. This document is Cisco Public.