

# SISAS (IMPLEMENTING CISCO SECURE ACCESS SOLUTIONS)

## Objetivo

Implementing Cisco Secure Access Solutions (SISAS) versão 1.0 é um treinamento que faz parte da grade de certificação CCNP Security. Este curso visa preparar os engenheiros em segurança de rede com os conhecimentos e as habilidades que eles precisam para projetar e implantar e fornecer suporte em solução de segurança no controle de acesso a rede utilizando o protocolo 802.1x em conjunto com as funcionalidades do Cisco ISE (Identity Services Engine). Será abordado pelo curso desde a preparação e configuração dos switches para utilização do protocolo 802.1x até a integração com o Cisco ISE. São apresentados às recomendações da Cisco, para a configuração do Cisco ISE nas atividades de autenticação, autorização e controle do acesso à rede através da verificação das conformidades requeridas, tais como equipamentos utilizados, o sistema operacional em uso, as atualizações requeridas, software antivírus dentre outros requerimentos que são suportados pelo sistema. Após a conclusão deste curso, o aluno será capaz de atender aos seguintes objetivos gerais: Compreender arquitetura do protocolo 802.1X, implantação e operação em produtos Cisco em rede cabeada (switches); Compreender a função do produto Cisco ISE, a sua arquitetura, funcionalidades e capacidades; Compreender as combinações mais comuns da arquitetura EAP (Extensible Authentication Protocols) nos processos de autenticação; Integrar uma Infraestrutura de chave pública (PKI) com ISE; Compreender como disponibilizar as bases usuárias no ISE, desde a interna até a integração com base externa, como por exemplo, o AD Microsoft, para os processos em autenticação; Compreender e disponibilizar a processo MAB na fase de autenticação (MAC Authentication Bypass); Como configurar as Políticas do ISE na fase de Autorização do acesso a rede; Compreender as características da arquitetura Cisco "TrustSec"; Implantar o controle de acesso dos visitantes (Perfil Guest), e disponibilizar a delegação de acesso via usuários patrocinadores (Perfil Sponsor); Implantar o processo para verificação da Postura (Conformidades) para liberação de acesso a rede; Implantar o processo para identificação de ativos utilizados no acesso a redes (Serviço Profiling); Entender o processo para controle de acesso à rede "BYOD" utilizando o ISE; Fornecer suporte para solucionar os problemas mais comuns do ISE.

## Público Alvo

O público principal deste curso são os responsáveis em projetar, implantar e prestar suporte em segurança em soluções para controle de acesso a rede cabeada (switches camada 2 e 3), utilizando o protocolo 802.1x com o Cisco ISE. Esse curso faz parte dos cursos preparatórios para a certificação CCNP Security.

## Pré-Requisitos

Para aproveitar ao máximo este curso, é recomendável que o aluno possua as seguintes habilidades e conhecimentos: Ter participado no curso ICND 1, ou possuir conhecimentos equivalentes abrangidos pelo curso; Ter participado no curso IINS, ou possuir conhecimentos básicos em segurança abrangidos pelo curso; Conhecimento do sistema operacional Microsoft Windows.

## Carga Horária

40 horas (5 dias).

## Conteúdo Programático

Threat Mitigation through Identity Services  
Identity Services  
Secure Access Solution Portfolio  
Access Control in Cisco SAFE  
Authentication, Authorization and Accounting (AAA)  
Change of Authorization Process (CoA)  
Identity Sources  
Protocol RADIUS  
Protocol TACACS+

802.1X and EAP  
IEEE 802.1X Overview  
802.1X Message Flow  
802.1X Authorization  
802.1X VLAN Assignment  
802.1X Downloadable ACLs  
802.1X Host Modes  
802.1X Phased Deployment  
802.1X Monitor Mode  
802.1X Low Impact Mode  
802.1X Closed Mode  
802.1X Deployment Mode Comparison  
802.1X Phased Deployment Guidelines  
Change of Authorization  
MAC Authentication Bypass (MAB)  
Extensible Authentication Protocol (EAP) Tunnel and Non-Tunnel EAP  
Traditional User and Machine Authentication  
EAP Chaining Operation  
EAP Chaining: Corporate Asset and User  
EAP Chaining: Corporate Asset, User Logged Off  
EAP Chaining: Personal Asset with NAM  
EAP Chaining: Personal 3rd Party Asset  
Cisco AnyConnect 3.x Supplicant

Identity System Quick Start  
Access the Cisco ISE  
The Cisco ISE GUI  
Local User Database  
Network Access Devices in Cisco ISE  
Cisco ISE Default Authentication Policy

- Switch Configuration Procedure
- Configure Global AAA Parameters
- Configure RADIUS Peering
- Configure Switch for 802.1X Monitor Mode
- Windows Native Supplicant
- Verify Authentication on ISE
- Verify Authentication on Switch

- Cisco Identity Services Engine (ISE) Fundamentals
- Cisco ISE Overview
- Cisco ISE Operational Components
- Cisco ISE as Policy Platform
- Cisco ISE High-Level Flow
- Cisco ISE Personas
- Cisco ISE Deployment Examples

- Cisco ISE with PKI
- Server Authentication in EAP
- TLS-Protected Communication
- X.509v3 Certificates
- Use of Server Certificate
- First Validation: Verify Server Certificate
- Second Validation: Verify Server Signature
- PKI Enrollment Procedure
- Verify PKI Enrollment

- Cisco ISE Authentication
- Policy Elements in Cisco ISE
- Cisco ISE Authentication Policy Example
- Cisco ISE Rule-Based Authentication
- Authentication Conditions Tune Rule-Based Authentication (Situational)
- Define Simple Conditions (Optional)
- Create or Tune Compound Conditions (Optional)
- Define Allowed Protocols (Optional)
- Tune or Create Authentication Rules (Optional)
- Tune Default Authentication Rule (Optional)
- Cisco Network Access Manager
- Networks and Network Groups in Cisco NAM
- Network Settings in Cisco NAM

- Configuring Cisco ISE for External Authentication
- External Authentication
- Active Directory
- Authentication Methods with Active Directory
- AD-Derived Group Membership
- Active Directory Integration Methods
- Active Directory Integration Procedure
- Configure AD Domain and Store

- Test AD Connection
- Join Active Directory
- Select Groups from Directory
- Cisco ISE Identity Source Sequence
- Configure Identity Source Sequence
- Apply Identity Source Sequence
- Verify External Authentication

- Advanced Access Control
- Certificate-based User Authentication
- EAP-TLS Bidirectional Authentication
- Verification of Client Certificates
- Implementation Procedure for EAP-TLS in Cisco ISE Deployment
- Select CA Certificate for EAP Verification
- Deploy Certificates on Clients
- Configure 802.1X Supplicant to Use EAP-TLS
- Configure Supplicant to Use Certificates
- Configure Certificate Authentication Profile
- Apply Certificate Authentication Profile to Identity Source Sequence
- Verify EAP-TLS Operation

- Authorization
- Cisco Cloud Web Security Traffic Redirection Overview
- Authorization in Cisco ISE
- Authorization Policy Element Overview
- Downloadable ACLs
- Authorization Profiles Authorization Policy
- Building Compound Conditions
- Authorization Policy Configuration
- Verify Authentication and Authorization

- Security Group Access (SGA) and MACsec Implementation
- Cisco Switch Configuration
- Cisco ISE Authentication
- Cisco ISE Internal Databases
- Cisco ISE Rule-Based Authentication
- Configure Cisco ISE Rule-Based Authentication
- External Authentication
- Active Directory Integration Procedure
- Cisco ISE Identity Source Sequence
- Configure Cisco ISE Identity Source Sequence
- Cisco ISE Authorization Policy Overview
- Cisco ISE Authorization Policy Elements
- Authorization Policy Configuration
- Verify Authentication and Authorization

- Web Authentication and Guest Access
- WebAuth process

WebAuth operation  
Configure WebAuth  
Verify WebAuth

Guest Access Services  
WebAuth and guest access  
Guest access applications  
Portal placement  
Configuration scopes  
Configuration procedures

Endpoint Access Control Enhancements  
Posture  
NAC Agents  
Client provisioning  
Posture conditions, requirements, remediation actions, and policy  
Configure posture  
Verify posture

Profiler  
Profiler service Probes  
Profiling without Probes  
Profiling policies  
Configure profiling  
Verify profiling

BYOD  
BYOD feature  
Single and dual SSID design  
Dual SSID flow  
Authorization in dual SSID design  
BYOD process

Troubleshooting Network Access Control  
Troubleshooting procedure and tools  
Failure Reason Editor  
Connectivity tests  
General Diagnostic Tools  
Evaluate Configuration Validator  
Posture Troubleshooting  
Troubleshooting 802.1X Authentication  
Troubleshoot 802.1x on a Switch  
Troubleshoot RADIUS Peering  
Troubleshoot Peering with the User Database  
Troubleshoot Server-Side Certificate Issues

Troubleshoot Client-Side Certificate Issues  
Troubleshoot Disallowed Authentication Protocol  
Troubleshoot Machine Authentication  
Troubleshooting MAB  
Troubleshoot Missing Endpoint MAC Address  
Troubleshooting Central Web Authentication  
Troubleshoot Mismatch of ACL Name  
Troubleshooting Posture and Profiling

#### Roteiro de Laboratórios

Lab 1-1: Bootstrap Identity System  
Lab 2-1: Enroll Cisco ISE in PKI  
Lab 2-2: Implement MAB and Internal ISE Authentication  
Lab 2-3: Implement External Authentication  
Lab 3-1: Implementing EAP-TLS with Identity Services Engine (ISE)  
Lab 3-2: Implementing Authorization  
Lab 4-1: Configuring Cisco ASA Access Policy  
Lab 4-2: Implement Guest Access  
Lab 5-1: Implement Posture  
Lab 5-2: Profiler