Cisco Secure Access Control System v5.x (ACS)

Modality: Virtual Classroom

Duration: 3 Days

CLC: 27 Units

About This Course:

This course, Cisco Secure Access Control System will begin as a simple prologue and understudies will be trained on how access to different segments of the framework can be controlled while keeping up security as the course advances. The accompanying significant ideas will be included in the course:

Authorization: Placing limitations or restrictions on the functions that users are permitted to perform inside the system or network.

Authentication: Identification of the gadgets in the system or network to control the access of the user.

Accounting: Tracking the activity of user for improved security

Additionally, understudies will be acquainted with various conventions for security and authentication including Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+), the Extensible Authentication Protocol (EAP), and IEEE 802.1X.

Furthermore, with hands-on practice and theoretical explanations for the execution of protocols for improved security, understudies of the course of Cisco Secure Access Control System will also be acquainted with designs and processes that can be utilized for focused outcomes. For additional inside and out information and practice, hands-on labs are incorporated as a feature of the educational plan of the course permits understudies to design Cisco Secure Access Control System and Cisco network devices without problems. Also, the course fills in as material of preparation for various Cisco Certification Trainings.

Cisco Certified Network Administrators gain a normal of $84,000 annually.

Course Outline:

After the completion, understudies of this course of Cisco Secure Access Control System will be able to:

- Weigh of different Access Control System solutions pros and cons including ACS Express, Cisco Secure ACS – 1121, ACS on VMware, and Cisco Service ACCS – 1120.
- Define and efficiently configure authentication and security protocols including EAP, IEEE 802.1X, TACACS+, and RADIUS.
- Explain the job of different Cisco Secure Access Control System segments.
- Install Secure ACS of Cisco utilizing a setup script

- Define Cisco Secure ACS licensing
- Comprehend and define the difference between values, value types, and attributes.
- Comprehend the importance of user authorization, authentication, and accounting, and explain how identity stores work.
- Adequately design character score lines
- Comprehend the essentials of the Protocol of Lightweight Direct Access and leverage the protocol for the powerful setup of outside identity stores.
- Execute TACACS+ to perform different capacities on Cisco Secure ACS.
- Comprehend the various parts of Cisco Secure ACS to troubleshoot and monitor issues.
- Utilize a local certificate authority (CA) for the troubleshooting and configuration of computerized certificates that Cisco Secure ACS self-signs
- Troubleshoot and Configure EAP and IEEE 802.1X inside the environments of Cisco Secure ACS.

Audience:

This course has been planned for:

- Architects, engineers, network administrators, and security professionals who are maintaining security within the network and responsible for user authentication.
- Partners of the channels of Cisco who are liable for the maintenance, implementation, and selling of various solutions identified with the Cisco Secure Access Control System
- Engineers of Sales of Cisco Secure Access Control Systems

Prerequisites:

- The certification of CCNA or comprehension and experience with the concepts included in the training of Cisco certification.
- Hands-on experience and operational knowledge with the MS Windows operating system
- Having information and involvement with the certification training of Implementing Cisco IOS Network Security Cisco is a plus.

Suggested prerequisite courses:

- MS-MCSA-Windows10 MCSA: Windows 10 Boot Camp.
- Cisco Certified Network Associate (CCNA) -- Routing and Switching Training Boot Camp v3.0 (CS-CCNA)
- Implementing Cisco IOS Network Security v3.0 (IINS).

Course Outline:

Module 1: Identity Management Solution Overview
Lesson 1A: Reviewing Identity Management
Lesson 1B: Understanding Borderless Security
Module 2: Product Overview and Initial Configuration
Lesson 2A: Reviewing RADIUS and TACACS+
Lesson 2B: Reviewing Cisco Secure ACS v5.2

Lesson 2C: Installing Cisco Secure ACS v5.2
Lesson 2D: Understanding Cisco Secure ACS Attributes and Dictionaries
Lesson 2E: Adding Network Devices to Cisco Secure ACS
Lesson 2F: Configuring Identity Stores and Identity Sequence

Module 3: Advanced Cisco Secure ACS Configuration and Device Management

Lesson 3A: Configuring LDAP with External Identity Store
Lesson 3B: Configuring Active Directory with External Identity Store
Lesson 3C: Configuring Authentication, Authorization, and Accounting with TACACS+
Lesson 3D: Understanding Cisco Secure ACS and Certification Authority
Lesson 3E: Monitoring, Reporting, and Troubleshooting

Module 4: IEEE 802.1X with Cisco Secure ACS v5.2

Lesson 4A: Introducing IEEE 802.1X
Lesson 4B: Reviewing IEEE 802.1X Policy Elements (RADIUS)
Lesson 4C: Configuring IEEE 802.1X and Windows XP, Vista, and 7
Lesson 4D: Configuring IEEE 802.1X with Cisco Secure Services Client (SSC)
Lesson 4E: Using IEEE 802.1X Port-Based Authentication
Lesson 4F: Troubleshooting IEEE 802.1X

Module 5: System Operations

Lesson 5A: Configuring Distributed Deployment
Lesson 5B: Configuring Cisco Secure ACS System Administration Features

Return to Top