

Implementing Security Service Edge with Cisco Secure Access

Duration: 3 Days Course Code: ICSA Version: 1.0

Overview:

Implementing Security Service Edge with Cisco Secure Access (ICSA) training explores how to deploy, configure, and operate a Security Service Edge (SSE) solution using the Cisco Secure Access platform. The course highlights key concepts, configurations, and verification procedures. Participants will learn about Secure Access Service Edge (SASE) and SSE architecture, the Cisco Secure Access platform, and how to configure Secure Private Access (SPA) and Secure Internet Access (SIA) with zero-trust access. The training also covers threat and content defense, data loss prevention (DLP), and methods for verifying enforcement and monitoring user experience. This is a product training course and does not map directly to a Cisco certification or exam. Cisco Secure Access topics are also covered in the **Implementing and Operating Cisco Security Core Technologies (SCOR)** and **Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT)** training courses. Completing this training earns **17 Continuing Education (CE) credits** toward recertification. *Updated 22/09/2026*

Target Audience:

This class is intended for the following participants:

- Security Engineers
- Security Administrators
- Network Security Engineers
- Cloud Security Engineers
- Security Architects
- Security Consultants
- Systems Engineers
- Infrastructure Engineers
- SOC Analysts
- Zero Trust Security Specialists

Objectives:

- Describe the SASE frameworks, the SSE cloud-based security services it includes, and the SD-WAN concepts and Cisco SD-WAN edge device on-box security capabilities that complete the SASE architecture.
- Describe the Cisco Secure Access platform architecture and primary use cases.
- Describe the Cisco Secure Access management options and the Admin Portal.
- Describe the building blocks of the Cisco Secure Access initial configuration workflow.
- Describe the user-side traffic acquisition methods and private-application backhaul methods available in Cisco Secure Access.
- Additional Course Objectives
- Configure Cisco Secure Access user provisioning and SAML-based SSO authentication.
- Configure the common Cisco Secure Access components required for Secure Private Access, including app-side connectivity, private resource definition, and access policy.
- Configure Zero Trust Access in Cisco Secure Access using client-based and browser-based methods.
- Configure VPNaaS and Branch IPsec in Cisco Secure Access for Secure Private Access.
- Configure Endpoint Posture, Security, and IPS Profiles in Cisco Secure Access for Secure Private Access.
- Configure the common Cisco Secure Access components required for Secure Internet Access.
- Describe the access methods dedicated to Secure Internet Access in Cisco Secure Access.
- Configure threat and content defense capabilities in Cisco Secure Access for Secure Internet Access.
- Configure Data Loss Prevention (DLP) in Cisco Secure Access.
- Verify Cisco Secure Access user experience using Experience Insights.
- Integrate Cisco Secure Access with Cisco XDR and Splunk Enterprise to enhance SOC operations.

Prerequisites:

Recommended Prerequisites

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- 2+ years of experience in network security or security administration
- Basic understanding of enterprise routing and switching
- Basic understanding of WAN networking concepts
- Basic understanding of VPN technologies (IPsec, SSL/TLS)
- Basic understanding of DNS, HTTP/HTTPS, and web security concepts
- Basic understanding of Zero Trust principles
- Familiarity with cloud-based security services

Relevant Cisco Learning Offerings

These skills can be found in the following Cisco Learning Offerings:

- SCOR - Implementing and Operating Cisco Security Core Technologies
- CCNA - Implementing and Administering Cisco Solutions
- SDWFND - Cisco Catalyst SD-WAN Operation and Deployment
- ENSDWI - Implementing Cisco Catalyst SD-WAN Solutions

Testing and Certification

- None

Follow-on-Courses:

- None recommended

Content:

Course Outline

- SASE and SSE Architecture
- Cisco Secure Access Platform and Use Cases
- Cisco Secure Access Management
- Initial Configuration Workflow
- Cisco Secure Access Connectivity Methods
- User Provisioning and SSO Configuration
- Common Secure Private Access Configuration
- Zero Trust Access Configuration
- VPN-Based Configuration
- SPA Security Controls Configuration
- Common Secure Internet Access Configuration
- Dedicated Secure Internet Access Methods Overview
- Threat and Content Defense Configuration
- Data Loss Prevention Configuration
- Cisco Secure Access Experience Insights
- Cisco Secure Access Integrations

Lab Outline

- Explore Cisco Secure Access Admin Portal
- End User Experience
- Secure Private Access
- Implement Secure Internet Access
- Explore Cisco Secure Access Experience Insights

Further Information:

For More information, or to book your course, please call us on Head Office Tel.: +974 40316639

training@globalknowledge.qa

www.globalknowledge.com/en-qa/

Global Knowledge, Qatar Financial Center, Burj Doha, Level 21, P.O.Box 27110, West Bay, Doha, Qatar