

Implementing Security Service Edge with Cisco Secure Access (ICSA)

Implementing Security Service Edge with Cisco Secure Access (ICSA)

The 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, highlighting key concepts, configurations, and verification procedures. You will learn about Secure Access Service Edge (SASE) and SSE architecture and the Cisco Secure Access platform, how to configure Secure Private Access (SPA) and Secure Internet Access (SIA) with zero-trust access, threat and content defense, and data loss prevention (DLP), and how to verify enforcement and monitor user experience.

This is a product training and does not map to a Cisco certification or exam. Cisco Secure Access is also covered in Implementing and Operating Cisco Security Core Technologies (SCOR) and Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT) trainings. This training also earns you 17 Continuing Education (CE) credits toward recertification.

How you'll benefit

This class will help you:

- Understand SASE and SSE architecture to design and deploy robust, cloud-native security frameworks across your organization
- Configure SPA and SIA to implement effective zero-trust access controls
- Deploy advanced threat defense and DLP to protect critical enterprise data from modern cyber threats
- Optimize user experience by monitoring traffic and verifying enforcement through integrated Experience Insights tools
- Enhance SOC operations by integrating Cisco Secure Access with platforms like Cisco XDR and Splunk for streamlined visibility
- Earn 17 CE credits toward recertification

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The primary audience for this course is as follows:

- Security Engineers
- Security Administrators
- Network Security Engineers
- Cloud Security Engineers
- Security Architects
- Security Consultants
- Systems Engineers
- Infrastructure Engineers

Course Duration

3 days

Course Price

\$2,895.00 or 29 CLCs

Methods of Delivery

- Instructor Led
- Virtual ILT
- On-Site

- SOC Analysts
- Zero Trust Security Specialists

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

OUTLINE

Module 1: SASE and SSE Architecture

Module 2: Cisco Secure Access Platform and Use Cases

Module 3: Cisco Secure Access Management

Module 4: Initial Configuration Workflow

Module 5: Cisco Secure Access Connectivity Methods

Module 6: User Provisioning and SSO Configuration

Module 7: Common Secure Private Access Configuration

Module 8: Zero Trust Access Configuration

Module 9: VPN-Based Configuration

Module 10: SPA Security Controls Configuration

Module 11: Common Secure Internet Access Configuration

Module 12: Dedicated Secure Internet Access Methods Overview

Module 13: Threat and Content Defense Configuration

Module 14: Data Loss Prevention Configuration

Module 15: Cisco Secure Access Experience Insights

Module 16: Cisco Secure Access Integrations

LAB OUTLINE

Lab 1: Explore Cisco Secure Access Admin Portal

Lab 2: End User Experience

Lab 3: Secure Private Access

Lab 4: Implement Secure Internet Access

Lab 5: Explore Cisco Secure Access Experience Insights