Implementing Security Service Edge with Cisco Secure Access (ICSA)

Description

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 training 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

© 2026 Cisco and/or its affiliates. All rights reserved.

Who should enroll

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

Technology areas

- Security

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
- 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 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

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)

© 2026 Cisco and/or its affiliates. All rights reserved.

- Basic understanding of DNS, HTTP/HTTPS, and web security concepts
- Basic understanding of Zero Trust principles
- Familiarity with cloud-based security services

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

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

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

© 2026 Cisco and/or its affiliates. All rights reserved.

Links

- Cisco U. Learning Path
- Cisco Learning Locator

© 2026 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R) 7/24