FIREFLY

CISCO PARTNER Platinum Learning

Cisco SecureAccess Administering and Troubleshooting • SECACC

DURATION: 5 DAYS | **PRICE:** USD 4495 | **CLCs:** 45 | **CE:** 40

COURSE CODE: SECACC | **FORMAT:** Lecture & Lab

COURSE DESCRIPTION

This course delivers a comprehensive framework for understanding, deploying,managing, and troubleshooting Cisco Secure Access in modern hybridenvironments. Students begin with an introduction to cloud security principlesand foundational models such as Secure Access Service Edge (SASE) and ZeroTrust Access, before progressing into detailed coverage of Cisco Secure Accessarchitecture, core features, licensing options, and integrations with CiscoSD-WAN, Secure Firewall, and Meraki. Buildingon that foundation, learners will work through the full Secure Access lifecycle- from initial onboarding and configuration to user and identity management,DNS forwarder set up, network connectivity, and the creation of internet andprivate access policies. The course places strong emphasis on endpointsecurity, VPN services, data loss prevention (DLP), malware protection, and thedeployment and use of Cisco Secure Client across multiple platforms andoperating systems. Advanced topics include monitoring andlogging, troubleshooting methodologies, scalability planning, and leveragingThousandEyes for digital experience monitoring and network performanceinsights. Students will also explore Cisco Secure Access APIs to supportautomation, integration, and operational efficiency within their environments.

To get the most out of the Cisco SecureAccess Admin and Troubleshooting course, attendees should have a workingknowledge of the following prerequisites.

COURSE PREREQUISITES

- Networking Fundamentals
- Understanding of TCP/IP, DNS, HTTP/S, and general networking protocols
- Familiarity with routing and switching concepts (static routes, VLANs, BGP basics)
- Experience with IPsec VPN concepts and tunnel configuration
- Knowledge of firewall operations and basic security policy management
- Security Concepts

Cisco SecureAccess Administering and Troubleshooting • SECACC

• General understanding of cybersecurity principles and terminology
• Awareness of Zero Trust, SASE, and SSE frameworks (conceptual level)
• Familiarity with identity and access management (IAM) and authentication protocols such as SAML, RADIUS, or LDAP
• Basic understanding of threat detection and incident response workflows
• Cisco-Specific Experience
• Hands-on experience with Cisco networking or security products is beneficial
• Familiarity with Cisco Firepower, Umbrella, Duo, or Meraki is an advantage
• Cisco CCNA or CCNP Security certification (or equivalent knowledge) is recommended
For Help Desk Personnel Specifically
• Experience working with ticketing systems and handling Tier 1/Tier 2 escalations
• Basic understanding of VPN clients and remote access troubleshooting
• Familiarity with user authentication issues and endpoint connectivity

WHO SHOULD ATTEND

• This course is intended forIT and security professionals involved in the design, implementation,administration, or troubleshooting of Cisco security solutions across hybridenvironments.

• NetworkAdministrators - Manageand maintain network infrastructure with a focus on secure connectivity andpolicy enforcement.

• EnterpriseNetwork Engineers -Build and support large-scale network environments requiring integratedsecurity controls.

• NetworkArchitects - Designresilient, secure network frameworks aligned with organizational and compliancerequirements.

• Network Security Engineers -Oversee next-generation firewall (NGFW) deployments and the development ofcomprehensive security policies.

• SecurityArchitects - Developand guide SASE/SSE and zero trust strategies across distributed enterpriseenvironments.

• SOCAnalysts - Requireunified visibility across firewall and cloud security platforms to supporteffective threat detection and response.

• SystemsEngineers & Pre-Sales Engineers- Provide technical guidance and support for hybrid Secure Access solutiondeployments.

• ITOperations Teams -Administer IPsec tunnels, routing policies, and network segmentation withincomplex hybrid infrastructures.

• HelpDesk Support Personnel- Handle Tier 1 and Tier 2 escalations related to secure access issues, VPNconnectivity, and user authentication problems, and benefit from foundationalknowledge of Cisco security platforms to resolve incidents more efficiently.

Cisco SecureAccess Administering and Troubleshooting • SECACC

Instructor Led Training

To view the schedule and secure your site

SIGN UP HERE