+1 (219) 764-3800

6210 Central Ave, Portage IN

sales@ctclc.com

www.ctclc.com

CISCO
Partner

Platinum Learning

WHERE GREAT TRAINING HAPPENS EVERYDAY!

Administering and Troubleshooting Cisco Secure Access (SECACC)

Administering and Troubleshooting Cisco Secure Access (SECACC)

This course provides a comprehensive technical understanding of Cisco Secure Access within the Cisco Security Cloud and SASE architecture. Designed for network and security engineers, it covers Zero Trust fundamentals, Secure Service Edge (SSE), and cloud security design principles. Students learn how to deploy and manage Cisco Security Cloud Control (SCC), onboard Secure Access, configure subscriptions, and validate service readiness. The curriculum includes identity integration with Okta, DUO, and Active Directory, deployment of virtual appliances, DNS Defense configuration, and Umbrella migration strategies. Learners explore integrations with Catalyst SD-WAN, Meraki SD-WAN, Cisco Secure Firewall, and ISR platforms, including Secure Internet Access (SIA) and Secure Private Access (SPA) workflows. Advanced topics include policy design, endpoint posture enforcement, ZTNA configuration, AI-driven security controls, Data Loss Prevention (DLP), Digital Experience Insights, ThousandEyes integration, monitoring, troubleshooting, APIs, and Terraform automation.

Upon completion, students can design, deploy, integrate, secure, and automate Cisco Secure Access in enterprise SASE environments.

How You Will Benefit

This course provides practical knowledge and implementation-level understanding of FMC, Cisco Secure Firewall, and Cisco Secure Access integration within modern hybrid security architectures. Rather than focusing only on theory, the training emphasizes real-world deployment models used in enterprise and government environments.

Who Should Attend

This course is designed for technical professionals responsible for designing, deploying, managing, or troubleshooting Cisco security solutions in hybrid environments.

• Network Administrators
• Enterprise Network Engineers
• Network Architects
• Network Security Engineers responsible for NGFW deployment and policy management.
• Security Architects designing SASE/SSE and zero trust architecture.
• SOC Analysts who need cross-platform visibility between firewall and cloud security platforms.
• Systems Engineers and Pre-Sales Engineers supporting hybrid Secure Access deployments.
• IT Operations teams managing IPsec tunnels, routing policies, and segmentation.

Course Duration
5 days
Course Price
$4,495.00 or TBD CLCs
Methods ofDelivery
• Instructor Led
• Virtual ILT
• On-Site

Outline

Module 0: Course Introduction
- Module Topics
- General Administration
- Introductions
- Webex Meeting Center Basics
- Lab Access for CTCLC Lab
- Cisco Secure Access Unified Architecture
- Cisco Secure Access
- Cisco Secure Access Capabilities
- Cisco Secure Access Remote Access
- Cisco Secure Access ZTNA
- Catalyst SD-WAN + Cisco Secure Access Integration
- Cisco Security Innovations
- Digital Experience Insights Problem Identification
- Module Summary

Module 1: Introduction to Cisco Cloud Security & SASE/SSE
- Module Topics
- Lesson 1: Cloud Security Basics
- Lesson 2: Security Design Principles
- Lesson 3: Security Product Overview
- Lesson 4: Zero Trust Fundamentals
- Lesson 5: SASE Fundamentals
- Module Summary

Module 2: Cisco Security Cloud Control
- Module Topics
- Lesson 1: Security Cloud Control Overview
- Lesson 2: Security Cloud Control Products
- Lesson 3: Secure Cloud Control Organizations
- Lesson 4: Secure Cloud Control Interface
- Lesson 5: Secure Cloud Control MultiOrg / MSP
- Lesson 6: Secure Coud Control Subscription
- Lesson 7: Secure Cloud Control User Management
- Lesson 8: Unified User Experience
- Lesson 9: Unified Secure SD-WAN Experience
- Lesson 10: SCC Integrations with SD-WAN
- Module Summary

Module 3: Cisco Secure Access Overview
- Module Topics
- Lesson 1: Secure Access Overview
- Lesson 2: Secure Access Use Cases
- Lesson 3: Secure Access Protocols
- Lesson 4: Secure Access Authentication Overview
- Lesson 5: Network Connectivity Overview

- Lesson 6: Client Connectivity
- Lesson 7: Data Controls and Protection
- Module Summary

Module 4: Onboarding Cisco Secure Access
- Module Topics
- Lesson 1: Secure Access Initial Configuration
- Lesson 2: Secure Access Subscription
- Lesson 3: Getting Started Workflow
- Lesson 4: Secure Access Service Status
- Lesson 5: Secure Access Configuration Range Limits
- Lesson 6: Network Requirements for Secure Access
- Module Summary

Module 5: Secure Access Virtual Appliances
- Module Topics
- Lesson 1: Virtual Appliance
- Lesson 2: Deploying Virtual Appliances
- Lesson 3: Managing DNS Forwarders
- Module Summary

Module 6: DNS Defense
- Module Topics
- Lesson 1: DNS Defense Overview
- Lesson 2: Cisco DNS Cloud Security Service
- Lesson 3: DNS Enforcement
- Lesson 4: Cisco DNS Defense Threat Intelligence
- Lesson 5: Cisco DNS Defense Deployment
- Lesson 6: Cisco DNS Defense Deployment Integrations
- Lesson 7: DNS Defense Reporting and Retention
- Lesson 8: Configure DNS Defense in Secure Access
- Lesson 9: Umbrella Migration to Secure Access
- Module Summary

Module 7: Manage User/Group & Endpoint Devices
- Module Topics
- Lesson 1: Secure Access User Provisioning
- Lesson 2: Manual Provisioning
- Lesson 3: Directory Integration with Entra
- Lesson 4: SSO Authentication with Entra ID
- Lesson 5: Directory Integration with Okta
- Lesson 6: SSO Authentication with Okta
- Lesson 7: IDP Integration with DUO Auth Proxy
- Lesson 8: SSO Integration with DUO Auth Proxy
- Lesson 9: DUO SCIM Integration with Secure Access
- Lesson 10: DUO SAML Integration for Proxy and ZTA
- Lesson 11: Troubleshooting Identity Providers (IDP)
- Lesson 12: Active Directory Integration

- Lesson 13: Generate API Keys for AD Integration
- Lesson 14: Configure AD Integration
- Module Summary

Module 8: Network Connections Overview
- Module Topics
- Lesson 1: Network Connection Overview
- Lesson 2: Resource Connector Groups Overview
- Lesson 3: Deploying Resource Connector Groups
- Lesson 4: Network Tunnel Group Overview
- Lesson 5: Deploying Network Tunnel Groups
- Lesson 6: Network Tunnel Configuration
- Lesson 7: Network Tunnel Routing
- Module Summary

Module 9: Cisco Secure Access Integrations
- Module Topics
- Lesson 1: Cisco Secure Access Integrations Overview
- Lesson 2: Integration of Identity Services Engine (ISE)
- Lesson 3: Cisco Identity Intelligence
- Lesson 4: Splunk Security Integration
- Lesson 5: Cisco XDR Integration
- Lesson 6: Google Chrome
- Module Summary

Module 10: Catalyst SD-WAN / SSE Integration
- Module Topics
- Lesson 1: Catalyst SD-WAN Fundamentals
- Lesson 2: Catalyst SD-WAN SCC Integration
- Lesson 3: Catalyst SD-WAN / SSE Integration Overview
- Lesson 4: Catalyst SD-WAN / SSE Configuration
- Lesson 5: Catalyst SD-WAN / SSE Policy Groups Integration
- Lesson 6: Catalyst SD-WAN / SSE SIA Workflow
- Lesson 7: Catalyst SD-WAN / SSE SPA Workflow
- Lesson 8: Catalyst SD-WAN / SSE Monitoring
- Lesson 9: Catalyst SD-WAN / SSE Troubleshooting
- Module Summary

Module 11: Meraki SD-WAN / Integration
- Module Topics
- Lesson 1: Meraki MX
- Lesson 2: Meraki SD-WAN Overview
- Lesson 3: Meraki SD-WAN for Performance
- Lesson 4: Meraki SD-WAN Auto-VPN
- Lesson 5: Meraki SD-WAN / SSE Integration
- Lesson 6: Meraki Secure Access Configuration
- Lesson 7: Meraki Secure Access Integration
- Lesson 8: Manually Create Tunnels with Meraki MX

- Module Summary

Module 12: Secure Firewall / SSE Integration
- Module Topics
- Lesson 1: Secure Firewall Overview
- Lesson 2: Secure Firewall Integration
- Lesson 3: Manually Configuration Tunnels
- Lesson 4: Troubleshooting
- Module Summary

Module 13: Cisco ISR / SSE Integration
- Module Topics
- Lesson 1: Cisco ISR / SSE Integration Overview
- Lesson 2: Router CLI Troubleshooting
- Module Summary

Module 14: End User Connectivity
- Module Topics
- Lesson 1: Zero Trust Network Access (ZTNA) Overview
- Lesson 2: Universal ZTNA
- Lesson 3: End User Connectivity
- Lesson 4: Zero Trust Access Configuration
- Lesson 5: Secure Access VPN Profiles
- Lesson 6: Secure Access Internet Security
- Lesson 7: Secure Client Overview
- Lesson 8: Secure Access Zero Trust Clients
- Lesson 9: Secure Client Modules
- Lesson 10: Security Architecture
- Lesson 11: iOS Native Zero Trust Access
- Lesson 12: Secure Client Configuration and Deployment
- Lesson 13: Cloud Deployment Management
- Lesson 14: Secure Client Remote Access
- Lesson 15: Secure Client ThousandEyes Agent
- Lesson 16: Secure Client Posture Agent
- Lesson 17: Network Visibility Module
- Lesson 18: Client Connectivity
- Module Summary

Module 15: Managing Secure Access Resources & Security
- Module Topics
- Lesson 1: Secure Access Sources and Destinations
- Lesson 2: Secure Access Internet and SaaS Resources
- Lesson 3: Secure Access Private Resources
- Lesson 4: Secure Access Private Resource Groups
- Lesson 5: Secure Access Application Portal
- Lesson 6: Authentication, Authorization and Accounting (AAA)
- Lesson 7: DNS Services
- Lesson 8: Enablement Schedule

- Module Summary

Module 16: Profiles and Settings
- Module Topics
- Lesson 1: Secure Access Zero Trust Endpoint Posture Profiles
- Lesson 2: Secure Access VPN Posture Profiles
- Lesson 3: Secure Access IPS Profiles
- Lesson 4: Secure Access Security Profiles
- Lesson 5: Secure Access App Risk Profiles
- Lesson 6: Secure Access Threat Categories
- Lesson 7: Secure Access Notification Pages
- Lesson 8: Secure Access Do Not Decrypt Lists
- Lesson 9: Secure Access Certificates
- Module Summary

Module 17: Cisco Secure Access AI / DLP
- Module Topics
- Lesson 1: Secure Access AI Overview
- Lesson 2: AI Assistant Monitoring and Troubleshooting
- Lesson 3: Secure Access Self-Healing
- Lesson 4: Cisco Secure Access AI Access
- Lesson 5: Secure Access Data Classification
- Lesson 6: AI Guardrails
- Lesson 7: Configuring AI Guardrails
- Lesson 8: Data Loss Prevention (DLP)
- Lesson 9: AI Supply Chain Blocking
- Module Summary

Module 18: Configuring Access Policies & Access Rules
- Module Topics
- Lesson 1: Application Workflows
- Lesson 2: Access Policy Overview
- Lesson 3: Secure Access Policy Rule Defaults
- Lesson 4: Secure Access Global Policy Settings
- Lesson 5: Secure Access Policy Rules
- Lesson 6: Creating Secure Access Private Access Rules
- Lesson 7: Creating Secure Access Internet Access Rules
- Lesson 8: Associating Identity with Internet Traffic Policies
- Module Summary

Module 19: Digital Experience Insights
- Module Topics
- Lesson 1: Digital Experience Insights
- Lesson 2: Enable ThousandEyes Integration
- Lesson 3: Experience Insights Dashboard
- Lesson 4: AI Insights
- Lesson 5: Remote Worker Use-Case
- Lesson 6: Secure Access Enterprise Agents Insights

- Lesson 7: Secure Access SAAS Insights
- Lesson 8: Proactive Monitoring
- Lesson 9: Experience Scanner
- Lesson 10: Agent Deployment
- Module Summary

Module 20: Secure Access Monitoring & Troubleshooting
- Module Topics
- Lesson 1: Secure Access Service Status
- Lesson 2: Secure Access Monitoring
- Lesson 3: Secure Access Alerting Framework
- Lesson 4: Monitor - Management
- Lesson 5: Secure Access Reporting
- Lesson 6: Client Troubleshooting
- Lesson 7: ZTNA Client Troubleshooting
- Lesson 8: Clientless ZTNA Certificate Troubleshooting
- Lesson 9: Private Resource Access Troubleshooting
- Module Summary

Module 21: Secure Access API's and Infrastructure as Code (IAC)
- Module Topics
- Lesson 1: Configuration Evolution
- Lesson 2: Cisco Secure Access API Overview
- Lesson 3: API Use Case in Cisco Secure Access
- Lesson 4: Ansible
- Lesson 5: Create an API Keys
- Lesson 6: Secure Access API Authentication
- Lesson 7: Secure Access Postman Library
- Lesson 8: Infrastructure as Code
- Lesson 9: Cisco Secure Access Terraform
- Module Summary