



# Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT)

## What you'll learn in this course

The Designing and Implementing Secure Cloud Access for Users and Endpoints training teaches you the skills for designing and implementing cloud security architecture, user and device security, network and cloud security, cloud application and data security, cloud visibility and assurance, and responding to cloud threats.

This training prepares you for the 300-740 SCAZT v1.0 exam. If passed, you earn the Cisco Certified Specialist – Security Secure Cloud Access certification and satisfy the concentration exam requirement for the Cisco Certified Network Professional (CCNP) Security certification.

## Course duration

- Instructor-led training: 5 days in the classroom with hands-on lab practice
- Virtual instructor-led training: 5 days of web-based classes with hands-on lab practice
- E-learning: Equivalent of 5 days of video instruction with hands-on lab practice

## Who should attend

- Network Engineers
- Network Security Engineers
- Network Architects
- Sales/Presales Engineers

## How to enroll

To enroll in the SCAZT course or explore our larger catalog of courses on Cisco Digital Learning, contact us at <training@fastlane-mea.com>

## Technology areas

- Networking

## Course details

### Outline

- Demonstrate a comprehensive understanding of common cloud attack tactics and mitigation strategies
- Industry Security Frameworks
- Cisco Security Reference Architecture Fundamentals
- Cisco Security Reference Architecture Common Use Cases
- Cisco SAFE Architecture
- Certificate-Based User and Device Authentication
- Cisco Duo Multifactor Authentication for Application Protection
- Cisco Duo with AnyConnect VPN for Remote Access
- Introducing Cisco ISE Endpoint Compliance Services
- SSO using SAML or OpenID Connect
- Deploying On-Premises Threat Prevention
- Examining Content Filtering
- Exploring Cisco Umbrella SIG
- Reverse Proxy
- Securing Cloud Application with Cisco Umbrella SIG
- Exploring Cisco SD-WAN ThousandEyes
- Optimizing SaaS Applications
- Security Policies for Remote Access VPN
- Cisco Secure Access
- Cisco Secure Firewall
- Web Application Firewall
- Cisco Secure Workload Deployments, Agents, and Connectors
- Cisco Secure Workload Structure and Policy
- Cloud Security Attacks and Mitigations
- Multicloud Security Policies
- Cloud Visibility and Assurance
- Cisco Secure Network Analytics and Cisco Secure Analytics and Logging
- Cisco XDR
- Cisco Attack Surface Management
- Cloud Applications and Data Access Verifications
- Automation of Cloud Policy
- Response to Cloud Threats
- Automation of Cloud Threat Detection and Response

### Prerequisites

The knowledge and skills you are expected to have before attending this training are:

- Basic understanding of enterprise routing
- Basic understanding of WAN networking
- Basic understanding of Cisco SD-WAN
- Basic understanding of Public Cloud services
- These skills can be found in the following Cisco Learning Offerings:
- Implementing and Administering Cisco Solutions 1.0
- Implementing Cisco SD-WAN Solutions 2.0
- Cisco SD-WAN Operation and Deployment 1.0