Administering and Positioning Cisco Umbrella Operations

Duration: 3 Days **Course Code: ADMUMB** **Version: 2.X** **Delivery Method: Company Event**

Overview:

Cisco Umbrella is a cloud-delivered security platform that provides the first line of defense against threats on the Internet. This course focuses on understanding, administering, and positioning Cisco Umbrella, along with its integration into modern security architectures. Students with a basic understanding of Cisco products and IT solutions will gain the ability to describe Cisco Umbrella, understand Secure Internet Gateway (SIG) capabilities, ransomware protection, and threat intelligence. In addition, the course introduces Cisco Secure Access (ZTA, VPN), providing insight into modern Zero Trust and cloud security solutions. Sign up with EnterOne to get access to this Cisco online training course today.
Updated 09/08/2026

Target Audience:

The primary audience for this course is as follows:

- Channel Partner
- System Engineers
- System Administrators
- Architects
- Security Professionals

Objectives:

- Upon completing this course, the learner will be able to meet these overall objectives:
- Describe and position Cisco Umbrella
- Discuss Secure Internet Gateway and Ransomware Protection
- Learn about DNS & IP layer enforcement & Intelligent Proxy
- Describe Command and control callback blocking
- Discuss Threat Intelligence
- Compare Umbrella Packages
- Understand how to use Cisco Umbrella Virtual Appliance
- Explain the ease of Integrating Cisco Umbrella into Active Directory
- Discuss Umbrella Reporting
- Understand Utilize Multi-Organization Tools
- Understand Zero Trust Access (ZTA) concepts using Cisco Secure Access
- Understand VPN-based access policies within Cisco Secure Access
- Understand security validation and reporting in Cisco Secure Access

Prerequisites:

The knowledge and skills that the learner should have before attending this course are as follows:

- Basic understanding of Cisco products and solutions

Testing and Certification

- *N\A*

Follow-on-Courses:

- *None recommended*

Content:

Course Outlines

Module 1. Describe Cisco Umbrella

- What Is Umbrella
- Enforcement
- Umbrella Investigate
- DNS Overview
- Why DNS?
- Intelligence and Statistical Models
- Co-occurrence Model
- Spike Rank Model
- Predictive IP Space Monitoring
- Connecting to Umbrella

Module 2. Umbrella Deployment Options

- On-Premises Deployment Options
- DHCP Server
- DNS Server Forwarders
- Recursive DNS
- Configuring DNS Forwarders

Module 3. Configure Policy Components: Part 1

- Destination Lists
- Content Categories
- Application Settings
- Tenant Controls
- Security Settings

Module 4. Configure Policy Components: Part 2

- Block Page Appearance
- Integrations
- Selective Decryption Lists
- Bypass Users
- Bypass Codes

Module 5. Umbrella Policies: DNS, Firewall, and Web

- Umbrella Policy Types
- DNS Policy
- SSL Decryption
- Identities
- Security Categories
- Content Access
- Application Control
- Destination Lists
- File Analysis
- Block Page
- Bypass Users and Bypass Codes
- Policy Summary
- Web Policy
- PAC File and SAML
- HTTPS Inspection
- File Type Control
- Firewall Policy
- Firewall Rule
- IPsec Parameters
- Network Tunnel Requirements

Lab 1. Deploying Cisco Umbrella

Log in to the Umbrella dashboard, forward DNS to the Umbrella resolvers, and confirm that forwarding is active.

Lab 2. Configuring Umbrella Policy Components

Build destination lists, content categories, content security, application settings, and a block page.

Lab 3. Configuring Umbrella DNS Policy (Instructor demo)

Create and test a DNS policy, use the Policy Tester, and review the resulting activity.

Lab 4. SIG Integration

Configure a Web policy, deploy the root CA certificate and PAC file, and verify proxy enforcement and reporting.

Lab 5. Cloud Firewall Integration

Establish an SD-WAN tunnel to Umbrella, configure cloud-firewall rules, and validate the policy.

Lab 6. Active Directory Integration Using Virtual Appliance (Instructor demo)

Deploy virtual appliances, enable redirection, install the AD script and connector, and validate the integration.

Lab 7. Umbrella User Account and Roles Management

Configure user roles and accounts, then validate the resulting access.

Lab 8. Umbrella Reporting

Review the core and additional reports and configure scheduled reports.

Lab 11. Umbrella Integration with Catalyst Center (Instructor demo)

Integrate Umbrella with Catalyst Center, modify the DNS default policy, provision a network device, and validate secure connectivity.

Lab 12. Umbrella-Splunk Integration

Install Splunk, install the add-on, and configure the data inputs.

Appendix/Bonus Lab. Explore the Cisco Security Cloud Control Portal

Explore the Cisco Security Cloud Control (SCC) dashboard.

Bonus Labs

Lab 13. Active Directory User Integration with Cisco Secure Access (Instructor demo)

Remove the Umbrella integration, log in to Cisco Secure Access, install the AD script and connector, and validate the integration.

Lab 14. Configure AD FS for SAML (Instructor demo)

Configure AD FS as a SAML identity provider and verify the integration.

Lab 15. Cisco Secure Client with Zero Trust Access

Create Zero Trust posture profiles and a private resource, then configure and test browser- based and client-based access.

Lab 16. Cisco Secure Client with Virtual Private Networks (VPNs)

Configure a VPN profile and posture, define resources and access rules, and test the VPN connection.

- Network Tunnel Configuration
- Policy Tester

Module 6. Integrating Umbrella with Active Directory

- Integration Benefits
- Umbrella Virtual Appliances (VAs)
- Virtual Appliance Requirements
- Firewall and ACL Requirements
- Virtual Appliance with an HTTP/HTTPS Proxy
- Virtual Appliance Deployment
- Configure the Virtual Appliance
- Active Directory Integration
- Active Directory Prerequisites
- Umbrella AD Components
- Connect Active Directory to Umbrella

Module 7. Umbrella Roaming Security: Roaming Client

- Why Roaming?
- Cisco Secure Client
- Migration from the Umbrella Roaming Client
- Prerequisites and Supported Operating Systems
- Deployment Methods
- Manual and Standard Installation
- Security Profile Installation (OrgInfo.json)
- Configuring Secure Client Options
- Behavior Behind a Virtual Appliance
- Internal Domains

Module 8. Umbrella Roaming Security: AnyConnect Roaming Security

- AnyConnect Roaming Security Overview
- Supported Operating Systems and Network Access
- json Profile
- Deployment Through the Cisco ASA
- Configure the Umbrella Profile
- Configure and Apply the Group Policy
- Roaming Computer Settings
- IP-Layer Enforcement

Module 9. Cisco Umbrella DNS Mobile Security

- Cisco Security Connector
- Apple iOS Devices: Requirements and Installation
- Android OS Devices: Prerequisites
- Download the Umbrella Android Configuration
- Push the Umbrella Certificate to Devices
- Anonymizing Mobile Devices

Module 10. User Account Management

- Manage Accounts
- Manage User Roles
- Custom User Roles

Module 11. Umbrella Reporting

Lab 9. Leveraging Umbrella Investigate

Investigate a domain and a SHA-256 file hash.

Lab 10. Cisco XDR Integration Walk-Through Demo

Log in to Cisco XDR and integrate Umbrella with the platform.

Lab 17. Configure and Test Security

Create security profiles, enable IPS on an access policy, and validate enforcement.

Lab 18. Cisco Secure Access Reporting

- Built-in Reports
- Report Retention
- Overview Page
- Report Scheduling
- Security Activity Report
- Activity Search Report
- Admin Audit Log

Module 12. Umbrella Investigate

- Domain Summary View
- Umbrella Risk Score
- Timeline Section
- DNS Resolution Table
- WHOIS Record Data
- GeoIP Section
- Investigate Sample View
- Security Features
- IP Addresses Section
- Subdomains Section
- Co-occurrences

Module 13. Umbrella Multi-Organization

- Multi-Org Console
- Centralized Reports
- Centralized Settings
- Org Management
- Admins and Delegated Admins

Module 14. Integrating Umbrella with Cisco XDR

- Unified Detection and Response
- Value of the Integration
- Core Telemetry Sources
- Integration Architecture
- Operational Efficiency
- Incident Response Workflow
- Configuration Workflow

Module 15. Integrating Umbrella with Cisco Splunk

- Why Integrate Umbrella with Splunk
- Pre-Configuration Checklist
- Integration Architecture
- Cisco Cloud Security Umbrella Add-On for Splunk
- Configure the Add-On Inputs

Labs Outlines

Labs are designed to assure learners a whole practical experience, through the following practical activities:

Lab 0. Accessing the Lab Devices

Get familiar with the pod topology, IP addressing, and credentials, and verify

connectivity between the Windows devices.

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK