

## Administering and Positioning Cisco Umbrella Operations

**Duration: 3 Days**    **Course Code: ADMUMB**    **Version: 2.1**    **Delivery Method: Company Event**

### Overview:

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the Internet. Being able to understand and position how Cisco Umbrella works and what are the features is the key focus of this 3-day Cisco online IT class.

Students who enter the course with a basic understanding of Cisco products and IT solutions will be able to describe the Cisco Umbrella, understand Secure Internet Gateway and Ransomware Protection, discuss Threat Intelligence, and use Cisco Roaming Client.

**The course qualifies for 18 Cisco Continuing Education Credits (CE).**

### Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

### Target Audience:

The primary audience for this course is as follows:

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

### Objectives:

- |  |  |
|--|--|
| ■ <b>After completing this course you should be able to:</b> | ■ Understand Roaming Security  |
| ■ How to describe and position Cisco Umbrella                | ■ Basic understanding of Cisco Roaming Client                          |
| ■ Discuss Secure Internet Gateway and Ransomware Protection  | ■ Understand how to use Cisco Umbrella Virtual Appliance               |
| ■ Learn about DNS & IP layer enforcement & Intelligent Proxy | ■ Explain the ease of Integrating Cisco Umbrella into Active Directory |
| ■ Describe Command and control callback blocking             | ■ Discuss Umbrella Reporting   |
| ■ Discuss Threat Intelligence                                | ■ Understand Utilize Multi-Organization Tools                          |
| ■ Compare Umbrella Packages                                  |  |

### Prerequisites:

**Attendees should meet the following prerequisites:**

- Basic understanding of Cisco products and solutions

## Content:

### Module 1: Describe Cisco Umbrella

- What is Umbrella
- Enforcement
- DNS Overview
- Why DNS?
- Co-occurrence Model
- Spike Rank Model
- Predictive IP Space Monitoring
- Connecting to Umbrella

### Module 2: Umbrella Deployment Options

- DHCP Server
- DNS Server Forwarders
- Recursive DNS
- 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 Policies
- Umbrella Policies – DNS
- SSL Decryption
- Identities
- Security Categories
- Content Access
- Control Applications
- Destination Lists
- File Analysis
- Block Page
- Bypass Users and Bypass Codes
- Policy Summary
- Umbrella Policies: Web
- PAC File and SAML
- HTTPS Inspection
- File Analysis
- File Type Control
- Umbrella Policies: Firewall
- Firewall Rule
- IPSec Parameters
- Network Tunnel Requirements
- Network Tunnel Configuration
- Policy Tester

### Module 11: Umbrella Reporting

- Umbrella Built-in Reports
- 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
- Subdomain Section
- Co-occurrences Features

### Module 13: Umbrella Multi-Organization

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

### Module 14: Integrating Umbrella within Cisco SecureX

- Cisco SecureX Ribbon
- Create Cisco SecureX Account
- Add an Integration Module
- Cisco SecureX Dashboard

### Lab Outline:

#### Discovery Lab 0: Accessing the Lab Devices

- Task 1: Understanding your Lab Environment
- Task 2: Lab IP Addressing, Usernames and Passwords
- Task 3: Testing Connectivity between Windows Devices

#### Discovery Lab 1: Deploying Cisco Umbrella

- Task 1: Log in to the Umbrella Dashboard
- Task 2: Configure your DNS Server Forwarder to Umbrella DNS Servers
- Task 3: Confirm you are Forwarding to Umbrella DNS Servers

#### Discovery Lab 2: Configuring Umbrella Policy Components

### Discovery Lab 5: Cloud Firewall Integration

- Task 1: Pre-Cloud Firewall Configuration Test
- Task 2: SD-WAN and Umbrella Tunnel Integration
- Task 3: Configure Cloud-Firewall Rules
- Task 4: Validate Cloud-Firewall Policy

### Discovery Lab 6: Active Directory Integration using the Virtual Appliance

- Task 1: Deploy Umbrella Virtual Appliances
- Task 2: Enable VA Redirect to Umbrella
- Task 3: Installing the Active Directory Script and Connector
- Task 4: Validate Umbrella Active Directory Integration

### Discovery Lab 7: Deploying Umbrella Roaming Client

- Task 1: Deploy Umbrella Roaming Client
- Task 2: Validate and Review Roaming Client Web Usage Activities

### Discovery Lab 8: Deploying AnyConnect Roaming Security

- Task 1: Configuring the ASA to Deploy AnyConnect Roaming Security Module
- Task 2: Create and Test Umbrella Roaming Security Policy
- Task 3: Review Umbrella Roaming Client Web Usage and Activities

### Discovery Lab 9: Umbrella User Account and Roles Management

- Task 1: Configuring Umbrella User Roles
- Task 2: Configuring Umbrella User Accounts
- Task 3: Validating Umbrella User Roles and Accounts

### Discovery Lab 10: Umbrella Reporting

- Task 1: Reviewing Umbrella Core Reports
- Task 2: Reviewing Umbrella Additional Reports
- Task 3: Configuring Umbrella Scheduled Reports

### Discovery Lab 11: Leveraging Umbrella Investigate

- Task 1: Investigating a Domain
- Task 2: Investigating a SHA-256 File Hash

### Discovery Lab 12: SecureX Integration Walk Through Demo

## Module 6: Integrating Umbrella with Active Directory

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

## Module 7: Umbrella Roaming Security-Roaming Client

- Umbrella Roaming Security-Roaming Client
- Prerequisites
- Downloading the Umbrella Roaming Client
- Umbrella Status
- Identity Support
- Prerequisites for Active Directory Integration

## Module 8: Umbrella Roaming Security-AnyConnect Roaming Security

- Supported Operating Systems
- Deployment Steps

## Module 9: Cisco Umbrella DNS Mobile Security

- Apple iOS Devices
- Requirements
- Installation
- Android OS Devices
- Prerequisites
- Download the Umbrella Android Configuration
- Push the Umbrella Certificate to Devices

## Module 10: User Account Management

- Manage Accounts
- Manage User Roles

- Task 1: Configuring Destination Lists
- Task 2: Configuring Content Categories
- Task 3: Configuring Content Security
- Task 4: Configuring Application Settings
- Task 5: Configuring Block Page Appearance

## Discovery Lab 3: Configuring Umbrella DNS Policy

- Task 1: Configure Umbrella DNS Policy
- Task 2: Test Your Umbrella DNS Policy
- Task 3: Umbrella Policy Tester
- Task 4: Review Umbrella Activities

## Discovery Lab 4: SIG Integration

- Task 1: Configure Umbrella Web Policy
- Task 2: Deploy Umbrella Root CA Certificate and PAC file
- Task 3: Verify Umbrella Web Policy
- Task 4: Review Umbrella Proxy Reporting

- Task 1: Creating your Cisco SecureX Login
- Task 2: Integrating Umbrella within Cisco SecureX

## Further Information:

For More information, or to book your course, please call us on 0800/84.009

[info@globalknowledge.be](mailto:info@globalknowledge.be)

[www.globalknowledge.com/en-be/](http://www.globalknowledge.com/en-be/)