

Course Outline

Administering & Positioning Cisco Umbrella Operations Course ADMUMB: 3 days Instructor Led

All Cisco courses are delivered by a Cisco Authorized Platinum Learning Partner

About this course

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 its 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 Umbrella deployment options and policy components, as well as the integration of Umbrella with Active Directory. We will discuss the importance and deployment of Umbrella Roaming Security to cover your mobile workforce with Roaming Client and AnyConnect Roaming Security. We will also take a close look at Umbrella Investigate, which provides rich threat intelligence and adds the security context needed to uncover and predict threats. We will conclude with integrating Umbrella within Cisco SecureX platform which strengthens your security across network, endpoint, cloud and applications.

Audience profile

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

At course completion

After completing this course, students will be able to:

- How to describe and position Cisco Umbrella
- Discuss Secure Internet Gateway and Ransomware Protection
- Learn about DNS & IP layer enforcement & Intelligent Proxy
- Discuss Threat Intelligence
- On Premise Deployment Options
- Understand Umbrella Policies and Components
- Explain the ease of Integrating Cisco Umbrella into Active Directory
- Understand how to use Cisco Umbrella Virtual Appliance
- Understand Roaming Security, Cisco Roaming Client, and AnyConnect Roaming Security
- Cisco Umbrella Investigate security features
- Understand Utilize Multi-Organization Tools
- Integrating Umbrella within Cisco SecureX Platform

Course Outline

Module 1: Describe Cisco Umbrella

- Enforcement

Course Outline

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

Module 2: Umbrella Deployment Options

- On Premise 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

- Configure Umbrella Policies
- Umbrella Policies – DNS
 - Umbrella DNS Policy: SSL Decryption
 - Umbrella DNS Policy: Identities
 - Umbrella DNS Policy: Security Categories
 - Umbrella DNS Policy: Content Access
 - Umbrella DNS Policy: Control Applications
 - Umbrella DNS Policy: Destination Lists
 - Umbrella DNS Policy: File Analysis

Course Outline

- Umbrella DNS Policy: Block Page
- Umbrella DNS Policy: Bypass Users and Bypass Codes
- Umbrella DNS Policy: Policy Summary
- Umbrella Policies: Web
 - Umbrella Web Policy: PAC File and SAML
 - Umbrella Web Policy: HTTPS Inspection
 - Umbrella Web Policy: File Analysis
 - Umbrella Web Policy: File Type Control
- Umbrella Policies: Firewall
 - Umbrella Firewall Policy: Firewall Rule
 - Umbrella Firewall Policy: IPSec Parameters
 - Umbrella Firewall Policy: Network Tunnel Requirements
 - Umbrella Firewall Policy: Network Tunnel Configuration
- Configuring Umbrella Policy: Policy Tester

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
- Umbrella AD Components
- Connect Active Directory to Umbrella

Module 7: Umbrella Roaming Security-Roaming Client

- Umbrella Roaming Client Benefits
- 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

Course Outline

- Deployment Steps

Module 9: Cisco Umbrella DNS Mobile Security

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

Module 10: User Account Management

- Manage Accounts
- Manage User Roles

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
- DNS Resolution
- WHOIS Record Data
- GeoIP
- Investigate Sample View
- Security Features
- IP Addresses
- Subdomains
- Co-occurrences

Module 13: Umbrella Multi-Organization

- Multi-org console

Course Outline

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

Module 14: Integrating Umbrella within Cisco SecureX

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

Lab Outline:

- Accessing the Lab Devices
- Deploying Cisco Umbrella
- Configuring Umbrella Policy Components
- Configuring Umbrella DNS Policy
- SIG Integration
- Cloud Firewall Integration
- Active Directory Integration using the Virtual Appliance
- Deploying Umbrella Roaming Client
- Deploying AnyConnect Roaming Security
- Umbrella User Account and Roles Management
- Umbrella Reporting
- Leveraging Umbrella Investigate