

Current Technologies

Computer Learning Centers



Cisco DoD Comply-to- Connect (C2C)

**WHERE GREAT TRAINING
HAPPENS EVERYDAY!**



Cisco DoD Comply-to-Connect (C2C)

Course Duration

5 Days

Course Price

\$4595.00

50 CLCs

Methods of Delivery

In-Person ILT

Virtual ILT

Onsite ILT

About this Class

In this Cisco DoD Comply-to-Connect (C2C) comprehensive, hands-on course has an exploration of Cisco C2C (Cisco-to-Cisco) security integrations and Cisco Identity Services Engine, focusing on identity-driven access control, endpoint visibility, compliance enforcement, and ecosystem integrations. It is designed for network and security professionals who need to implement and operate advanced identity-based security solutions across complex enterprise environments. The course progresses from foundational concepts into advanced design, integration, and operational troubleshooting.

Students begin by examining Cisco Identity-Based Networking Services and Cisco ISE architecture and deployment models, establishing a strong foundation in how authentication, authorization, and accounting are enforced across wired and wireless networks. The curriculum then advances into policy configuration, PKI and certificate-based authentication, endpoint profiling, and posture compliance, emphasizing how identity, device context, and security posture drive dynamic access decisions.

The course also explores real-world C2C use cases and third-party integrations with platforms such as Tenable, MECM, and Trellix, demonstrating how external security and endpoint intelligence enhances policy enforcement. Cisco TrustSec and TACACS+ device administration modules extend identity-based control into segmentation and infrastructure access management. Extensive hands-on labs reinforce each topic, preparing students to deploy, integrate, and troubleshoot enterprise-grade Cisco ISE and C2C solutions with confidence.

Cisco DoD Comply-to-Connect (C2C)

How you will benefit

This class will help you:

- Learn how to operate, manage, configure, and troubleshoot the Cisco C2C solution
- Gain an understanding of how the Cisco ISE security components relate to the C2C architecture
- Earn 32 CE credits toward recertification

Why Attend with Current Technologies CLC

- Our Instructors are the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The job roles best suited to the material in this course are:

- Network Security Engineers
- Network Administrators
- Security Administrators

Prerequisites

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- Familiarity with 802.1X
- Familiarity with Microsoft Windows Operating Systems
- Familiarity with Cisco IOS CLI for wired and wireless network devices
- Familiarity with Cisco Identity Service Engine

Cisco DoD Comply-to-Connect (C2C)

Objectives

After taking this course, you should be able to:

- Define DoD C2C, including its steps and alignment with ISE features/functions and Zero Trust
- Describe Cisco Identity-Based Networking Services
- Describe the Cisco Identity Services Engine
- Explain Cisco ISE deployment
- Describe Cisco ISE policy enforcement components
- Describe Cisco ISE policy configuration
- Explain PKI fundamentals, technology, components, roles, and software supplicants
- Describe the Cisco ISE profiler service
- Configure endpoint compliance
- Configure client posture services
- Describe profiling best practices and reporting
- Describe the four main use cases within C2C
- Explain the purpose and the configuration of integrating Cisco ISE with Tenable
- Describe the purpose and benefits of integrating Cisco ISE with MECM
- Describe the purpose and benefits of integrating Cisco ISE with Trellix
- Troubleshoot Cisco ISE policy and third-party NAD support
- Describe Cisco ISE TrustSec configurations
- Configure Cisco ISE device administration

Cisco DoD Comply-to-Connect (C2C)

Course Outline

Module 1: C2C Fundamentals

Module 2: Cisco Identity-Based Networking Services

Module 3: Introducing Cisco ISE Architecture

Module 4: Introducing Cisco ISE Deployment

Module 5: Introducing Cisco ISE Policy Enforcement Components

Module 6: Introducing Cisco ISE Policy Configuration

Module 7: PKI and Advanced Supplicants

Module 8: Introducing the Cisco ISE Profiler

Module 9: Introducing Cisco ISE Endpoint Compliance Services

Module 10: Configuring Client Posture Services and Compliance

Module 11: Introducing Profiling Best Practices and Reporting

Module 12: C2C Use Cases

Module 13: C2C Third-Party Integrations—Tenable

Module 14: C2C Third-Party Integrations—MECM

Module 15: C2C Third-Party Integrations—Trellix

Module 16: Troubleshooting Cisco ISE Policy and Third-Party NAD Support

Module 17: Exploring Cisco TrustSec

Module 18: Working with Network Access Devices

Cisco DoD Comply-to-Connect (C2C)

Lab Outline

- Lab 1: Initial Configuration and Certificate Usage
- Lab 2: Integrate Cisco ISE with Active Directory
- Lab 3: AAA Policy for MAB
- Lab 4: AAA Policy for 802.1X
- Lab 5: TEAP on Windows
- Lab 6: Cisco ISE Profiling Configuration
- Lab 7: Profiling Customization
- Lab 8: Cisco ISE Compliance Services
- Lab 9: Client Provisioning
- Lab 10: Posture Policies
- Lab 11: Compliance-Based Access
- Lab 12: Profiling Reports
- Lab 13: DISA Reports
- Lab 14: Certificate-Based Authentication for Cisco ISE Administration
- Lab 15: Cisco TrustSec
- Lab 16: TACACS+ Basic Device Administration
- Lab 17: TACACS+ Command Authorization