Cisco DoD Comply-to-Connect v1.0 (C2C-GOV)

Cisco DoD Comply-to-Connect v1.0 (C2C-GOV)

The Cisco DoD Comply-to-Connect (C2C) training teaches you how to implement and deploy a Department of Defense (DoD) Comply-to-Connect network architecture using Cisco Identity Services Engine (ISE). This training covers implementation of 802.1X for both wired and wireless devices and how Cisco ISE uses that information to apply policy control and enforcement. Additionally, other topics like supplicants, non-supplicants, ISE profiler, authentication, authorization, and accounting (AAA) and public key infrastructure (PKI) support, reporting and troubleshooting are covered. Finally, C2C specific use case scenarios are covered.

How you'll 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 towards recertification

Why Attend with Current Technologies CLC

- Our Instructors are in 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

Course Duration

5 days

Course Price

$4,595.00 or 50 CLCs

Methods of Delivery

- Instructor Led
- Virtual ILT
- On-Site

Who Should Attend

The primary audience for this course is as follows:

- 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

OUTLINE

Module 1: C2C Fundamentals

Module 2: Cisco Identity-Based Networking Services

Module 3: 802.1X EAP Authentication

Module 4: Configure Devices for 802.1X Operation

Module 5: Configure Access for Non-Supplicant Devices

Module 6: Introducing Cisco ISE Architecture

Module 7: Introducing Cisco ISE Deployment

Module 8: Introducing Cisco ISE Policy Enforcement Components

Module 9: Introducing Cisco ISE Policy Configuration

Module 10: PKI and Advanced Supplicants

Module 11: Troubleshooting Cisco ISE Policy and Third-Party NAD Support

Module 12: Exploring Cisco TrustSec

Module 13: Introducing the Cisco ISE Profiler

Module 14: Introducing Profiling Best Practices and Reporting

Module 15: Introducing Cisco ISE Endpoint Compliance Services

Module 16: Configuring Client Posture Services and Compliance

Module 17: Working with Network Access Devices

Module 18: C2C Use Cases

LAB OUTLINE

- Lab 1: Configure and Test 802.1X Operations
- Lab 2: Configure Initial Cisco ISE Configuration and System Certificate Usage
- Lab 3: Integrate Cisco ISE with Active Directory
- Lab 4: Configure Cisco ISE Policy for MAB
- Lab 5: Configure Cisco ISE Policy for 802.1X
- Lab 6: TEAP on Windows

- Lab 7: Configure Cisco TrustSec
- Lab 8: Configure Profiling
- Lab 9: Customize the Cisco ISE Profiling Configuration
- Lab 10: Create Cisco ISE Profiling Reports
- Lab 11: Configure Cisco ISE Compliance Services
- Lab 12: Configure Client Provisioning
- Lab 13: Configure Posture Policies
- Lab 14: Test and Monitor Compliance-Based Access
- Lab 15: Configure Cisco ISE for Basic Device Administration
- Lab 16: Configure Cisco ISE Command Authorization
- Lab 17: DISA Reports
- Lab 18: Certificate-Based Authentication for Cisco ISE Administration