C2C - CISCO DOD COMPLY-TO-CONNECT V1.1

Course Code: 860002

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.

This training also earns you 32 Continuing Education (CE) credits toward recertification.

What You'll Learn

At the end of the 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 purporse 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

Who Needs to Attend

This training is a Department of Defense mandate, ensuring compliance with cybersecurity protocols and procedures. The target audience includes individuals seeking the knowledge and skills involved in deploying, operating, and verifying Cisco DoD C2C network architecture, such as:

- 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

These skills can be found in the following Cisco course:

C2C - CISCO DOD COMPLY-TO-CONNECT V1.1

Course Code: 860002

VIRTUAL CLASSROOM LIVE	$4,995 USD	5 Day

Virtual Classroom Live Outline

Section 1: C2C Fundamentals

- Comply to Connect Overview
- From C2C to ZTA
- Steps to Implement C2C

Section 2: Cisco Identity-Based Networking Services

- Cisco IBNS Overview
- AAA Role in Cisco IBNS
- Compare Cisco IBNS and Cisco ISE Solutions
- Explore Cisco IBNS Architecture Components

Section 3: Introducing Cisco ISE Architecture

- Cisco ISE as a Network Access Policy Engine
- Cisco ISE Use Cases
- Cisco ISE Functions

Section 4: Introducing Cisco ISE Deployment

- Cisco ISE Deployment Models
- Cisco ISE Licensing and Network Requirements
- Cisco ISE Context Visibility Features
- New Features in Cisco ISE 3.X

Section 5: Introducing Cisco ISE Policy Enforcement Components

- 802.1X for Wired and Wireless Access
- MAC Authentication Bypass for Wired and Wireless Access
- Identity Management
- Active Directory Identity Source
- Additional Identity Sources
- Certificate Services

Section 6: Introducing Cisco ISE Policy Configuration

- Cisco ISE Policy

- Cisco ISE Authentication Rules
- Cisco ISE Authorization Rules

Section 7: PKI and Advanced Supplicants

- Public Key Infrastructure (PKI)
- TEAP in Comply to Connect (C2C)
- Secure Client ISE features and Configuration for C2C

Section 8: Introducing the Cisco ISE Profiler

- Web Access with Cisco ISE
- ISE Profiler
- Cisco ISE Probes
- Profiling Policy
- Custom Attributes in Profile

Section 9: Introducing Cisco ISE Endpoint Compliance Services

- Endpoint Compliance Services Overview

Section 10: Configuring Client Posture Services and Compliance

- Client Posture Services and Provisioning Configuration

Section 11: Introducing Profiling Best Practices and Reporting

- Profiling Best Practices

Section 12: C2C Use Cases

- Cisco CX ISE Reporting Tool
- ISE Reporting
- ISE Hardening
- Profiling Best Practices for C2C

Section 13: C2C Third-Party Integrations-Tenable

- Tenable Use Case
- Tenable Overview and Capabilities
- Tenable Integration Prerequisites
- Tenable Integration Configuration
- Policy Design
- Policy Enforcement
- Enforcement Verification

Section 14: C2C Third-Party Integrations-MECM

- MECM Use Case
- MECM Overview and Capabilities
- MECM Integration Prerequisites
- MECM Integration Configuration
- Policy Design
- Policy Enforcement
- Enforcement Verification

Section 15: C2C Third-Party Integrations-Trellix

- Trellix Use Case

- Trellix Overview and Capabilities
- Trellix Integration Prerequisites
- Trellix Integration Configuration
- Policy Enforcement
- Enforcement Verification

Section 16: Troubleshooting Cisco ISE Policy and Third-Party NAD

- Cisco ISE Third-Party Network Access Device Support
- Troubleshooting Cisco ISE Policy Configuration

Section 17: Exploring Cisco TrustSec

- Cisco TrustSec Overview
- Cisco TrustSec Enhancements
- Cisco TrustSec Configuration

Section 18: Working with Network Access Devices

- Reviewing AAA
- Cisco ISE TACACS+ Device Administration
- Configuring TACACS+ Device Administration
- TACACS+ Device Administration Guidelines and Best Practices

Virtual Classroom Live Labs

- 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 ISE to Tenable Integration Simulation
- Lab 16: Cisco ISE to MECM Integration Simulation
- Lab 17: Cisco ISE to Trellix Integration Simulation
- Lab 18: Cisco TrustSec
- Lab 19: TACACS+ Basic Device Administration
- Lab 20: TACACS+ Command Authorization

Aug 24 - 28, 2026 | 9:00 AM - 5:00 PM EDT

Nov 30 - Dec 4, 2026 | 9:00 AM - 5:00 PM EST

Jan 11 - 15, 2027 | 8:30 AM - 4:30 PM EST

Mar 8 - 12, 2027 | 8:30 AM - 4:30 PM EST

C2C - CISCO DOD COMPLY-TO-CONNECT V1.1

Course Code: 860002

ON-DEMAND	$900 USD

On-Demand Outline

Section 1: C2C Fundamentals

- Comply to Connect Overview
- From C2C to ZTA
- Steps to Implement C2C

Section 2: Cisco Identity-Based Networking Services

- Cisco IBNS Overview
- AAA Role in Cisco IBNS
- Compare Cisco IBNS and Cisco ISE Solutions
- Explore Cisco IBNS Architecture Components

Section 3: Introducing Cisco ISE Architecture

- Cisco ISE as a Network Access Policy Engine
- Cisco ISE Use Cases
- Cisco ISE Functions

Section 4: Introducing Cisco ISE Deployment

- Cisco ISE Deployment Models
- Cisco ISE Licensing and Network Requirements
- Cisco ISE Context Visibility Features
- New Features in Cisco ISE 3.X

Section 5: Introducing Cisco ISE Policy Enforcement Components

- 802.1X for Wired and Wireless Access
- MAC Authentication Bypass for Wired and Wireless Access
- Identity Management
- Active Directory Identity Source
- Additional Identity Sources
- Certificate Services

Section 6: Introducing Cisco ISE Policy Configuration

- Cisco ISE Policy

- Cisco ISE Authentication Rules
- Cisco ISE Authorization Rules

Section 7: PKI and Advanced Supplicants

- Public Key Infrastructure (PKI)
- TEAP in Comply to Connect (C2C)
- Secure Client ISE features and Configuration for C2C

Section 8: Introducing the Cisco ISE Profiler

- Web Access with Cisco ISE
- ISE Profiler
- Cisco ISE Probes
- Profiling Policy
- Custom Attributes in Profile

Section 9: Introducing Cisco ISE Endpoint Compliance Services

- Endpoint Compliance Services Overview

Section 10: Configuring Client Posture Services and Compliance

- Client Posture Services and Provisioning Configuration

Section 11: Introducing Profiling Best Practices and Reporting

- Profiling Best Practices

Section 12: C2C Use Cases

- Cisco CX ISE Reporting Tool
- ISE Reporting
- ISE Hardening
- Profiling Best Practices for C2C

Section 13: C2C Third-Party Integrations-Tenable

- Tenable Use Case
- Tenable Overview and Capabilities
- Tenable Integration Prerequisites
- Tenable Integration Configuration
- Policy Design
- Policy Enforcement
- Enforcement Verification

Section 14: C2C Third-Party Integrations-MECM

- MECM Use Case
- MECM Overview and Capabilities
- MECM Integration Prerequisites
- MECM Integration Configuration
- Policy Design
- Policy Enforcement
- Enforcement Verification

Section 15: C2C Third-Party Integrations-Trellix

- Trellix Use Case

- Trellix Overview and Capabilities
- Trellix Integration Prerequisites
- Trellix Integration Configuration
- Policy Enforcement
- Enforcement Verification

Section 16: Troubleshooting Cisco ISE Policy and Third-Party NAD

- Cisco ISE Third-Party Network Access Device Support
- Troubleshooting Cisco ISE Policy Configuration

Section 17: Exploring Cisco TrustSec

- Cisco TrustSec Overview
- Cisco TrustSec Enhancements
- Cisco TrustSec Configuration

Section 18: Working with Network Access Devices

- Reviewing AAA
- Cisco ISE TACACS+ Device Administration
- Configuring TACACS+ Device Administration
- TACACS+ Device Administration Guidelines and Best Practices

On-Demand Labs

- 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 ISE to Tenable Integration Simulation
- Lab 16: Cisco ISE to MECM Integration Simulation
- Lab 17: Cisco ISE to Trellix Integration Simulation
- Lab 18: Cisco TrustSec
- Lab 19: TACACS+ Basic Device Administration
- Lab 20: TACACS+ Command Authorization

C2C - CISCO DOD COMPLY-TO-CONNECT V1.1

Course Code: 860002

PRIVATE GROUP TRAINING	5 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 5/18/2026 6:55:54 AM