Training overview

Cisco DoD Comply-to-Connect (C2C)

Description

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.

You'll also learn how to integrate Splunk analytics and reporting into the C2C solution, which provides comprehensive training on endpoint compliance, telemetry verification, and automated reporting workflows to meet DoD mandates. Finally, C2C specific use case scenarios are covered. This training also earns you 32 Continuing Education (CE) credits toward recertification.

How you'll benefit

Thistraining 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
- Leverage Splunk's advanced analytics and reporting capabilities to ensure endpoint compliance, streamline reporting workflows, and meet DoD C2C mandates
- Earn 32 CE credits toward recertification

Who should enroll

This trainingis aDepartment 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

Technology areas

- Security

Objectives

- DefineDoD 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

Prerequisites

Thereareno 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 Learning Offering:

- Implementing and Configuring Cisco Identity Services Engine (SISE)

Outline

- C2C Fundamentals
- Cisco Identity-Based Networking Services
- Introducing Cisco ISE Architecture
- Introducing Cisco ISE Deployment
- Introducing Cisco ISE Policy Enforcement Components
- Introducing Cisco ISE Policy Configuration
- PKI and Advanced Supplicants
- Introducing the Cisco ISE Profiler

- Introducing Cisco ISE Endpoint Compliance Services
- Configuring Client Posture Services and Compliance
- Introducing Profiling Best Practices and Reporting
- C2C Use Cases
- C2C Splunk Dashboards & Reporting
- C2C Third-Party Integrations—Tenable
- C2C Third-Party Integrations—MECM
- C2C Third-Party Integrations—Trellix
- Troubleshooting Cisco ISE Policy and Third-Party NAD Support
- Exploring Cisco TrustSec
- Working with Network Access Devices

Lab Outline

- Initial Configuration and Certificate Usage
- Integrate Cisco ISE with Active Directory
- AAA Policy for MAB
- AAA Policy for 802.1X
- TEAP on Windows
- Cisco ISE Profiling Configuration
- Profiling Customization
- Cisco ISE Compliance Services
- Client Provisioning
- Posture Policies
- Compliance-Based Access
- Profiling Reports
- Certificate-Based Authentication for Cisco ISE Administration
- C2C Capstone Discovery
- Cisco ISE to Tenable Integration Simulation
- Cisco ISE to MECM Integration Simulation
- Cisco ISE to Trellix Integration Simulation
- Cisco TrustSec
- TACACS+ Basic Device Administration
- TACACS+ Command Authorization