Cisco DoD Comply-to-Connect (CPLL-C2C)

Duration: 180 Days

The Cisco DoD Comply-to-Connect (C2C) Learning Path teaches you how to implement and deploy a Department of Defense (DoD) Comply-to-Connect network architecture using Cisco Identity Services Engine (ISE). This Learning Path 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.

Skills You'll Learn:

- Gain foundational knowledge of 802.1X, MAC authentication bypass (MAB), and extensible authentication protocol (EAP) configuration for both wired and wireless devices
- Gain foundational knowledge of ISE architecture and deployment
- Enforce and configure ISE policy and integrate with supplicants, PKI, and TrustSec
- Understand how ISE profiler works to identify endpoints and configure for network authorization
- Learn about Cisco endpoint compliance with posture assessment with supplicants and third-party network access device (NAD) products
- Explore Cisco ISE monitoring and C2C compliance reporting
- Discover C2C use cases and AAA/terminal access controller access-control system (TACACS+)

Learning Path Objectives:

1. C2C Fundamentals and 802.1X: Gain foundation knowledge of 802.1X, MAB, and EAP and discover how Cisco ISE secures devices on the network including non-supplicant devices.
2. ISE Architecture and Deployment: Learn about the components necessary to implement and deploy ISE infrastructure, including their functionality and requirements.
3. Cisco ISE Policy Enforcement: Discover the fundamentals of ISE policy components and configuration, integration with PKI and supplicants, and Trustsec architecture.
4. ISE Profiler: Learn how endpoints connect to the network and how to regulate their access to assign network authorization and meet compliance policies through best practices and reporting.

5. Cisco ISE Endpoint Compliance: Understand the need to enforce posture and the difference between agent-based and third-party agents through services and provisioning configuration.
6. C2C Use Cases: Examine specific customer C2C use cases and scenarios, including network access devices utilizing AAA and TACACS+.