CISCO IDENTITY SERVICE ENGINE DEPLOYMENT WORKSHOP

Version 4.2

Blue River Education GmbH, Schoßbachstrasse 20c, 9400 Wolfsberg, Austria
Company Register FN 429823, VAT ID ATU69349314

https://br-experts.eu/
office@blueriveredu.com

1 Course Overview

This 5-day workshop teaches students to deploy and use Cisco Identity Services Engine (ISE), an identity and access control policy platform that simplifies the delivery of consistent, highly secure access control across wired, wireless, and VPN connections. Through hands-on practice via lab exercises and in-depth coverage of architecture, components, and personas, students will gain an in-depth understanding of Cisco ISE.

Please note that this workshop is based on real-world use cases and deployment experiences that also will be discussed during the workshop. We will point out real-life deployments whenever discussing topics or performing practical exercises.

Use cases include but are not limited to services such as policy enforcement, profiling services, web authentication, guest access services, Bring Your Own Device (BYOD), endpoint services, and Terminal Access Controller Access Control Server (TACACS+) device administration.

2 Who Should Attend

- Network Security Engineers
- Network Security Architects
- ISE Administrators
- Cisco Integrators and Partners

3 Prerequisites

To fully benefit from this course, attendees should have the following knowledge:

- Familiarity with the Cisco IOS Software Command-Line Interface (CLI) for wired and wireless devices
- Familiarity with Cisco AnyConnect Secure Mobility Client
- Familiarity with Microsoft Windows operating systems
- Familiarity with 802.1X

4 Why Attend a Blue River Experts Course

Our courses are not delivered by instructors but by consulting system engineers who have vast experience regarding real life design, deployment, and troubleshooting of actual customer installations. Besides delivering courses, our engineers usually design and deploy large enterprise solutions or perform real world POVs (proof of value) and POCs (proof of concept) for large customers. We are often requested and contracted by product vendors to help customers make buying decisions based on their particular use case. This allows us to discuss real world use cases, designs, and operational situations with our students.

If you would like to get educated by experts who will explain to you the whole life cycle from day 0 to day 2 as they have comprehensive knowledge from having written numerous business requirements documents, customer requirements documents, high level design and detailed design documents and having deployed and troubleshooted many customer installations then you should choose to attend one of our courses.

5 Course Objectives

After completing this course, students will be able to:

- Understand the architecture and services of Cisco ISE
- Deploy ISE with different personas and topologies
- Configure and launch secure access for
  - Employee devices
  - Guest devices with different requirements
  - Employee provided devices (BYOD)
- Deploy and troubleshoot wireless endpoints

6 Course Details

6.1 Understanding Cisco ISE Architecture and Features

- 802.1x, EAP and RADIUS fundamentals with packet capture
- Cisco ISE Architecture
- Cisco ISE Services / Features and Personas

6.2 Cisco ISE Licensing

- License Types
- License vs Feature Segregation
- License Consumption Details

6.3 Cisco ISE Configuration Menu(s)

- Cisco ISE Role Based Access Control
- Cisco ISE Menus Overview

6.4 Topologies and their Deployment

- Understanding the requirements of various topologies
- Small, medium and large deployments
- Using logs for troubleshooting deployments

6.5 Providing Secure Access to Employees

- Policy sets and typical use cases.
- Authentication Services and Authentication Stores (Active Directory, LDAP, etc.)
- Authentication Types and configuring their stores
- Configuring Authentication Policies based on various parameters like store, authentication type, protocol, NAD type, NAD, user, medium, location, deployment
- Configuring Authorization Policies – local / global exception policies and authorization policies
- Deploying Dot1x with ACLs and giving different access to different type of users
- Understanding live logs, live sessions, and reports for above use cases
- Troubleshooting

6.6 Identifying Devices and Granting Access (Profiling)

- What is Profiling and why do we need it
- Introducing the Cisco ISE Profiler
- Different probes and how to configure them to identify the profile of a device
- Understanding and configuring profiling components
- Configuring and verifying policies for profiled devices
- Profiling best practices and reporting

6.7 Providing Access to Guest Users and their Devices

- Understanding guest access through central web authentication (CWA)
- Understanding guest types and their typical use cases
- Understanding different portals such as guest, sponsor, mydevices, certificate provisioning, client provisioning, posturing
- Deploying self-registered guest users
- Deploying sponsored guest users
- Deploying hot-spot guest users
- Troubleshooting guest activity

6.8 Providing Access to Employee-Owned Devices (BYOD)

- Overview of BYOD (Bring Your Own Device), why BYOD
- Different types of BYOD and their security
- Dual SSID BYOD flow
- Single SSID BYOD flow
- Configuring ISE for BYOD use cases
- Managing devices on-boarded by an employee through my-devices portal
- Validate live logs, live sessions, reports, license details for BYOD on-boarded users
- Troubleshooting ISE for BYOD use cases

6.9 Client Posture Services and Compliance

- Posturing devices overview
- Posturing conditions and their remediation.
- Posturing policies, requirements and conditions
- Configuring and deploying posture policies
- Validating live logs, live sessions, reports, and license details for postured devices

6.10 Device Administration

- Overview of TACACS
- How to configure TACACS on various Network Access Devices (switch, wireless LAN controller, etc.)
- How to configure TACACS on ISE
- How to give different privileges for different ISE users through TACACS

6.11 Describe Cisco ISE TrustSec

- Define Cisco TrustSec
- Configure ISE TrustSec

7 LAB Exercises

7.1 Installing and Configuring Cisco ISE

- Completing the Setup Wizard

7.2 Understanding Cisco ISE CLI Configuration & Services

- How to access the Cisco ISE Command Line Interface
- Exploring the services running on Cisco ISE
- Exploring CLI configuration such as IP address, netmask, default gateway, domain name, etc.
- Verifying and validating the configuration

7.3 Accessing Cisco ISE GUI and understanding Menus / Services

- Accessing the Cisco ISE GUI
- Exploring default dashboards
- Creating your own dashboard
- How to create endpoints manually
- Configuring a network access device (NAD)
- Exploring other important menus items
- Exploring system information
- Changing your password
- Logging out of the system

7.4 Certificate Enrolment

- Importing Third Party Root CA Certificates
- Generating a Certificate Signing Request (CSR) for an Admin Certificate
- Signing a CSR
- Binding signed certificates to ISE services
- ISE Admin Certificate verification
- Modifying a signed certificate, adding different services

7.5 Configuring Policies, Policy Sets, Rules, Conditions

- Configuring Network Device Groups
- Configuring Network Access Devices (NAD)
- Associating NADs with Network Device Groups (NDG)
- Configure policies based on medium, location, and POD number

7.6 Configuring Active Directory

- Configuring Active Directory, retrieving groups and attributes

7.7 Configuring Authentication Sequence

- Configure an existing or new authentication sequence

7.8 Giving Secure Access to your Enterprise Domain Users based on Active Director Groups

- Assigning different privileges to Active Directory users based on their groups
- Authorize enterprise users who belong to another group and assign special privileges
- Azure AD integration

7.9 Configuring Guest Access

- Configuring sponsored guest users
- Configuring self-registered guest users
- Configuring a hotspot and provide Internet access to hotspot users
- Azure AD SAML integration (Overview)

7.10 Profiling a device using device sensors

- Profiling devices using built-in device sensors of a wireless LAN controller (WLC)

7.11 Configuring Dual SSID BYOD and onboarding your own Windows Machine

- Configuring BYOD

7.12 Configuring TACACS for Login Management

- Using TACACS to allow access to a wireless LAN controller and assigning privileges

7.13 Configuring Posture

- Configuring posture policy, validating posture of a device and give corresponding access
- Configuring agentless posture

7.14 Configuring Cisco ISE TrustSec

- Configuring Cisco ISE TrustSec