

IDENTITY SERVICES ENGINE (ISE) ADMINISTERING ADVANCED

Course Code: 860060

This 5-day advanced training course dives deep into Cisco Identity Services Engine (ISE) with a focus on profiling, posturing, and policy creation, along with in-depth troubleshooting techniques. Participants will learn how to leverage Cisco ISE to enhance network security, endpoint compliance, and policy enforcement through a structured approach. The course includes extensive hands-on labs, real-world case studies, and advanced troubleshooting methods to ensure participants gain the expertise needed to design, deploy, and maintain a secure Cisco ISE environment.

What You'll Learn

At the conclusion of this course, you should have an understanding of:

- Advanced Profiling in Cisco ISE
- Advanced Posturing in Cisco ISE
- Policy Creation and Enforcement in Cisco ISE
- Advanced Integrations and Automation
- In-Depth Troubleshooting, AI/ML Analytics, and Best Practices

Who Needs to Attend

- Network Security Engineers
- Network Security Architects
- ISE Administrators
- Senior Security Operations Center (SOC) personnel responsible for Incidence Response
- Cisco Integrators and Partners

Prerequisites

To fully benefit from this course, you 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

Recommended Cisco offerings that may help you meet these prerequisites:

- Cisco CCNP Security Certification training
- Implementing and Configuring Cisco Identity Services Engine (ISE) v4.0 or v4.1

IDENTITY SERVICES ENGINE (ISE) ADMINISTERING ADVANCED

Course Code: 860060

CLASSROOM LIVE

\$4,295 USD

5 Day

Classroom Live Outline

MODULE 1: Advanced Profiling in Cisco ISE

- Lesson 1: Introduction to Profiling
 - ☒ Overview of Cisco ISE Profiling Services
 - ☒ Importance of Profiling in Network Access Control
 - ☒ Profiling Policies and Attribute Collection
- Lesson 2: Profiling Techniques and Configuration
 - ☒ Passive vs. Active Profiling Methods
 - ☒ Device Sensor Capabilities and Probes (RADIUS, DHCP, HTTP, SNMP, NetFlow)
 - ☒ Endpoint Classification and Profiling Policy Creation
- Lesson 3: Profiling Enhancements and Best Practices
 - ☒ Creating Custom Profiling Policies
 - ☒ Tuning Profiling Accuracy and Efficiency
 - ☒ Integrating Cisco ISE with Network Infrastructure for Optimal Profiling
- Lesson 4: Troubleshooting Profiling Issues
 - ☒ Debugging Profiling Policies
 - ☒ Analyzing Live Logs and Reports
 - ☒ Resolving Misclassification and Incorrect Device Profiling

MODULE 2: Advanced Posturing in Cisco ISE

- Lesson 1: Introduction to Posture Assessment
 - ☒ Role of Posturing in Endpoint Security
 - ☒ Understanding Cisco ISE Posture Policies
 - ☒ NAC Agent vs. Secure Client Posture Module
- Lesson 2: Posture Configuration and Deployment
 - ☒ Configuring Posture Conditions and Remediation Actions
 - ☒ Deploying Posture Assessment in a Wired and Wireless Network

- ☒ Endpoint Compliance and Remediation Techniques
- Lesson 3: Posturing for BYOD and Corporate Devices
 - ☒ Implementing Posture Policies for BYOD and Corporate-Owned Devices
 - ☒ Integrating Cisco ISE with MDM for Posture Compliance
 - ☒ Automating Quarantine and Remediation Workflows
- Lesson 4: Troubleshooting Posturing Issues
 - ☒ Common Posturing Failures and Debugging Techniques
 - ☒ Monitoring Posture Logs and Reports
 - ☒ Resolving Agent Installation, Communication, and Policy Mismatch Issues

MODULE 3: Policy Creation and Enforcement in Cisco ISE

- Lesson 1: Overview of Policy Creation in Cisco ISE
 - ☒ Cisco ISE Policy Framework
 - ☒ Authentication vs. Authorization Policies
 - ☒ Creating Hierarchical Policy Structures
- Lesson 2: Advanced Policy Configuration
 - ☒ Configuring Policy Sets and Conditions
 - ☒ Attribute-Based Access Control (ABAC) Implementation
 - ☒ Dynamic Authorization with Change of Authorization (CoA)
- Lesson 3: Adaptive Network Access Policies
 - ☒ Implementing Context-Aware Policies
 - ☒ Role-Based and Device-Based Policy Enforcement
 - ☒ Integrating Cisco ISE with External Identity Sources (LDAP, AD, SAML)
- Lesson 4: Policy Troubleshooting and Optimization
 - ☒ Using Live Logs and Policy Simulation for Debugging
 - ☒ Analyzing Authentication and Authorization Failures
 - ☒ Optimizing Policy Efficiency and Reducing Latency

MODULE 4: Advanced Integrations and Automation

- Lesson 1: Cisco ISE Integration with Third-Party Solutions
 - ☒ Integrating Cisco ISE with Cisco Secure Network Analytics (Stealthwatch)
 - ☒ Connecting Cisco ISE with SIEM and Threat Intelligence Platforms
 - ☒ API-Based Automation for Identity and Policy Management
- Lesson 2: Automating Cisco ISE Operations
 - ☒ Automating Network Access Control with pxGrid and Cisco Catalyst Center
 - ☒ Dynamic Policy Adjustments Based on Threat Intelligence
 - ☒ Implementing REST API for ISE Management and Reporting
- Lesson 3: Security Group Tags (SGT) and TrustSec Integration
 - ☒ Overview of Security Group Tags (SGT) and TrustSec Framework
 - ☒ Implementing SGT for Role-Based Access Control (RBAC)
 - ☒ Policy Enforcement Using SGT-Based Access Controls
 - ☒ Troubleshooting SGT Deployment Issues
- Lesson 4: ISE with Firepower Integration
 - ☒ Overview of Cisco ISE and Firepower Integration
 - ☒ Configuring Firepower and ISE Integration

- ☒ Threat Detection and Dynamic Policy Enforcement
- ☒ Troubleshooting ISE and Firepower Integration
- Lesson 5: ISE Use Cases
 - ☒ Reviewing Complex ISE Deployments and Best Practices
 - ☒ Lessons Learned from Large-Scale ISE Implementations

MODULE 5: In-Depth Troubleshooting, AI/ML Analytics, and Best Practices

- Lesson 1: Advanced Troubleshooting Techniques
 - ☒ Debugging Authentication and Authorization Issues
 - ☒ Analyzing Logs with TACACS+, RADIUS, and Syslog
 - ☒ Using the Cisco ISE CLI and Debug Commands
- Lesson 2: Common Issues and Resolutions
 - ☒ Addressing Profiling and Posture Failures
 - ☒ Troubleshooting CoA and Policy Mismatches
 - ☒ Resolving Endpoint and Device Registration Issues
- Lesson 3: AI/ML Analytics in Cisco ISE
 - ☒ Behavior-Based Anomaly Detection – Identifies suspicious network activity based on deviations from normal user and device behavior.
 - ☒ Automated Threat Response – Enhances security by dynamically adjusting access policies based on AI-driven risk assessments.
 - ☒ Enhanced Endpoint Profiling – Improves device classification accuracy using ML-based pattern recognition.
 - ☒ Predictive Security Insights – Uses historical and real-time data to anticipate potential security threats before they materialize.
- Lesson 4: Multi-Factor Classification in Cisco ISE
 - ☒ Context-Aware Authentication – Considers multiple attributes, such as device posture, location, and user role, before granting access.
 - ☒ Risk-Based Access Control – Assigns risk scores to endpoints based on behavioral analytics, compliance status, and security posture.
 - ☒ Dynamic Policy Adjustments – Adapts authentication and authorization policies in real-time based on the risk assessment of the requesting entity.
 - ☒ Integration with AI/ML Analytics – Uses AI-driven insights to refine classification accuracy and enhance security decision-making.
- Lesson 5: Performance Optimization and Scaling Cisco ISE
 - ☒ High-Availability and Redundancy Considerations
 - ☒ Scaling Cisco ISE in Large Enterprise Networks
 - ☒ Best Practices for Policy Optimization and Log Retention

Classroom Live Labs

- Lab 0: Lab Access
- Lab 1: Cisco ISE GUI Familiarization and Initial Configuration
- Lab 2: WLC Integration and Policy Set Configuration
- Lab 3: Identity Source and Wireless Policy
- Lab 4: Wired Switch Integration and Policy Setup
- Lab 5: Create Policies for Domain Computers

- Lab 6: Create Policies for Employee
- Lab 7: Create Policies for Contractor
- Lab 8: Create Authorization Profile for Wireless Users
- Lab 9: DHCP Profiling
- Lab 10: Active Directory Profiling
- Lab 11: Block Unknown OUI Clients
- Lab 12: Block Anomalous Clients
- Lab 13: Configure Posture Compliance Services on Cisco ISE
- Lab 14: Configure Client Provisioning Portal
- Lab 15: Configure Posture Elements and Posture Policy
- Lab 16: Posture Authorization Profiles and Policy Sets
- Lab 17: Posture Compliance Configuration and Testing
- Lab 18: ISE MDM Posture
- Lab 19: ISE and FTD
- Lab 20: Adaptive Network Control Policy
- Lab 21: ISE and SNA integration
- Lab 22: ANC Global Exception Policy
- Lab 23: Test Adaptive Network Control
- Lab 24: ISE App on Splunk Enterprise
- Lab 25: ISE syslog configuration for Splunk
- Lab 26: Syslog Data on Splunk
- Lab 27: ISE Automation using APIs

IDENTITY SERVICES ENGINE (ISE) ADMINISTERING ADVANCED

Course Code: 860060

VIRTUAL CLASSROOM LIVE

\$4,295 USD

5 Day

Virtual Classroom Live Outline

MODULE 1: Advanced Profiling in Cisco ISE

- Lesson 1: Introduction to Profiling
 - ☒ Overview of Cisco ISE Profiling Services
 - ☒ Importance of Profiling in Network Access Control
 - ☒ Profiling Policies and Attribute Collection
- Lesson 2: Profiling Techniques and Configuration
 - ☒ Passive vs. Active Profiling Methods
 - ☒ Device Sensor Capabilities and Probes (RADIUS, DHCP, HTTP, SNMP, NetFlow)
 - ☒ Endpoint Classification and Profiling Policy Creation
- Lesson 3: Profiling Enhancements and Best Practices
 - ☒ Creating Custom Profiling Policies
 - ☒ Tuning Profiling Accuracy and Efficiency
 - ☒ Integrating Cisco ISE with Network Infrastructure for Optimal Profiling
- Lesson 4: Troubleshooting Profiling Issues
 - ☒ Debugging Profiling Policies
 - ☒ Analyzing Live Logs and Reports
 - ☒ Resolving Misclassification and Incorrect Device Profiling

MODULE 2: Advanced Posturing in Cisco ISE

- Lesson 1: Introduction to Posture Assessment
 - ☒ Role of Posturing in Endpoint Security
 - ☒ Understanding Cisco ISE Posture Policies
 - ☒ NAC Agent vs. Secure Client Posture Module
- Lesson 2: Posture Configuration and Deployment
 - ☒ Configuring Posture Conditions and Remediation Actions
 - ☒ Deploying Posture Assessment in a Wired and Wireless Network

- ☒ Endpoint Compliance and Remediation Techniques
- Lesson 3: Posturing for BYOD and Corporate Devices
 - ☒ Implementing Posture Policies for BYOD and Corporate-Owned Devices
 - ☒ Integrating Cisco ISE with MDM for Posture Compliance
 - ☒ Automating Quarantine and Remediation Workflows
- Lesson 4: Troubleshooting Posturing Issues
 - ☒ Common Posturing Failures and Debugging Techniques
 - ☒ Monitoring Posture Logs and Reports
 - ☒ Resolving Agent Installation, Communication, and Policy Mismatch Issues

MODULE 3: Policy Creation and Enforcement in Cisco ISE

- Lesson 1: Overview of Policy Creation in Cisco ISE
 - ☒ Cisco ISE Policy Framework
 - ☒ Authentication vs. Authorization Policies
 - ☒ Creating Hierarchical Policy Structures
- Lesson 2: Advanced Policy Configuration
 - ☒ Configuring Policy Sets and Conditions
 - ☒ Attribute-Based Access Control (ABAC) Implementation
 - ☒ Dynamic Authorization with Change of Authorization (CoA)
- Lesson 3: Adaptive Network Access Policies
 - ☒ Implementing Context-Aware Policies
 - ☒ Role-Based and Device-Based Policy Enforcement
 - ☒ Integrating Cisco ISE with External Identity Sources (LDAP, AD, SAML)
- Lesson 4: Policy Troubleshooting and Optimization
 - ☒ Using Live Logs and Policy Simulation for Debugging
 - ☒ Analyzing Authentication and Authorization Failures
 - ☒ Optimizing Policy Efficiency and Reducing Latency

MODULE 4: Advanced Integrations and Automation

- Lesson 1: Cisco ISE Integration with Third-Party Solutions
 - ☒ Integrating Cisco ISE with Cisco Secure Network Analytics (Stealthwatch)
 - ☒ Connecting Cisco ISE with SIEM and Threat Intelligence Platforms
 - ☒ API-Based Automation for Identity and Policy Management
- Lesson 2: Automating Cisco ISE Operations
 - ☒ Automating Network Access Control with pxGrid and Cisco Catalyst Center
 - ☒ Dynamic Policy Adjustments Based on Threat Intelligence
 - ☒ Implementing REST API for ISE Management and Reporting
- Lesson 3: Security Group Tags (SGT) and TrustSec Integration
 - ☒ Overview of Security Group Tags (SGT) and TrustSec Framework
 - ☒ Implementing SGT for Role-Based Access Control (RBAC)
 - ☒ Policy Enforcement Using SGT-Based Access Controls
 - ☒ Troubleshooting SGT Deployment Issues
- Lesson 4: ISE with Firepower Integration
 - ☒ Overview of Cisco ISE and Firepower Integration
 - ☒ Configuring Firepower and ISE Integration

- ☒ Threat Detection and Dynamic Policy Enforcement
- ☒ Troubleshooting ISE and Firepower Integration
- Lesson 5: ISE Use Cases
 - ☒ Reviewing Complex ISE Deployments and Best Practices
 - ☒ Lessons Learned from Large-Scale ISE Implementations

MODULE 5: In-Depth Troubleshooting, AI/ML Analytics, and Best Practices

- Lesson 1: Advanced Troubleshooting Techniques
 - ☒ Debugging Authentication and Authorization Issues
 - ☒ Analyzing Logs with TACACS+, RADIUS, and Syslog
 - ☒ Using the Cisco ISE CLI and Debug Commands
- Lesson 2: Common Issues and Resolutions
 - ☒ Addressing Profiling and Posture Failures
 - ☒ Troubleshooting CoA and Policy Mismatches
 - ☒ Resolving Endpoint and Device Registration Issues
- Lesson 3: AI/ML Analytics in Cisco ISE
 - ☒ Behavior-Based Anomaly Detection – Identifies suspicious network activity based on deviations from normal user and device behavior.
 - ☒ Automated Threat Response – Enhances security by dynamically adjusting access policies based on AI-driven risk assessments.
 - ☒ Enhanced Endpoint Profiling – Improves device classification accuracy using ML-based pattern recognition.
 - ☒ Predictive Security Insights – Uses historical and real-time data to anticipate potential security threats before they materialize.
- Lesson 4: Multi-Factor Classification in Cisco ISE
 - ☒ Context-Aware Authentication – Considers multiple attributes, such as device posture, location, and user role, before granting access.
 - ☒ Risk-Based Access Control – Assigns risk scores to endpoints based on behavioral analytics, compliance status, and security posture.
 - ☒ Dynamic Policy Adjustments – Adapts authentication and authorization policies in real-time based on the risk assessment of the requesting entity.
 - ☒ Integration with AI/ML Analytics – Uses AI-driven insights to refine classification accuracy and enhance security decision-making.
- Lesson 5: Performance Optimization and Scaling Cisco ISE
 - ☒ High-Availability and Redundancy Considerations
 - ☒ Scaling Cisco ISE in Large Enterprise Networks
 - ☒ Best Practices for Policy Optimization and Log Retention

Virtual Classroom Live Labs

- Lab 0: Lab Access
- Lab 1: Cisco ISE GUI Familiarization and Initial Configuration
- Lab 2: WLC Integration and Policy Set Configuration
- Lab 3: Identity Source and Wireless Policy
- Lab 4: Wired Switch Integration and Policy Setup
- Lab 5: Create Policies for Domain Computers

- Lab 6: Create Policies for Employee
- Lab 7: Create Policies for Contractor
- Lab 8: Create Authorization Profile for Wireless Users
- Lab 9: DHCP Profiling
- Lab 10: Active Directory Profiling
- Lab 11: Block Unknown OUI Clients
- Lab 12: Block Anomalous Clients
- Lab 13: Configure Posture Compliance Services on Cisco ISE
- Lab 14: Configure Client Provisioning Portal
- Lab 15: Configure Posture Elements and Posture Policy
- Lab 16: Posture Authorization Profiles and Policy Sets
- Lab 17: Posture Compliance Configuration and Testing
- Lab 18: ISE MDM Posture
- Lab 19: ISE and FTD
- Lab 20: Adaptive Network Control Policy
- Lab 21: ISE and SNA integration
- Lab 22: ANC Global Exception Policy
- Lab 23: Test Adaptive Network Control
- Lab 24: ISE App on Splunk Enterprise
- Lab 25: ISE syslog configuration for Splunk
- Lab 26: Syslog Data on Splunk
- Lab 27: ISE Automation using APIs

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

Date created: 12/19/2025 6:30:28 PM

Copyright © 2025 Global Knowledge Training LLC. All Rights Reserved.