

Updated on 29/11/2023

Sign up

FSAA training (ForeScout Advanced Administrator)

4 days (28 hours)

Presentation

Have you attended our FCSA (ForeScout Certified Administrator) training course, or would you like to prepare for ForeScout certification? If you want to master ForeScout's advanced features, this course is for you.

This Forescout Advanced Administrator training course will deepen your technical, theoretical and fundamental knowledge of the ForeScout platform. During the course, you'll explore various use cases, best practices and problem scenarios.

Led by an experienced instructor, our course covers practical ForeScout CounterACT configuration and maintenance skills.

Participants will learn how to design security policies using all our available tools. You'll organize resources in a network environment, and watch CounterACT monitor and protect a corporate network.

Our training offers you an excellent way of maximizing your team's efficiency by improving employee skills and competence.

This advanced training course will introduce you to the latest version of the tool, [ForeScout 8.2](#).

Objectives

- Developing advanced skills with CounterACT
- Gain a better understanding of how to configure, deploy and maintain CounterACT
- How to configure HPS
- Threat reporting
- Creating advanced diagnostics

Target audience

- System and network administrator.

Prerequisites

- Have completed our [FSCA training](#)

Our FSAA (ForeScout Advanced Administrator) training program

Introduction

- A brief introduction to ForeScout's vision and concepts of network access control
- Terms and architecture
 - plug-in
 - segment
 - channel
 - organizational unit
 - general network vocabulary

Installing CounterACT

- Installing and configuring CounterACT
- Installing Web certificates on CounterACT
- SSL (Secure Sockets Layer) certificate
- Licensing - Key points
- The modules
- Endpoint identity tracking
- Time parameters
- Console presentation
 - The main features
 - Navigation overview

Plugins

- Plugin optimization
 - HPS Plugin overview
 - UD Plugin
 - Plugin Switch
- Remote inspection for corporate hosts
- SecureConnector

- Windows update options
- User directory
- Supported server types
- Switches

Policy features

- Overview of the entire model policy flow
- Advanced policy conditions
- Advanced policy: Tools and actions
- Policy best practices
- Policy features
- Examples of personalized policies

Notifications

- CounterACT integrated notifications
- HTTP notification
- Page customization
 - Customization tool
 - Advanced customization
 - Administrator's e-mail address
- HTTP redirect page
- HTML Head tag elements
- Using data tags

SIEM/Syslog

- SIEM/Syslog overview
- Syslog
- About SIEM
-

McAfee ePolicy Orchestrator

- Introducing ePO
 - Introduction to McAfee ePO
 - CounterACT extension
 - ePO plugin
 - Example of an ePO strategy

Microsoft System Center

- Configuration Manager (SCCM)
- About the Microsoft plugin
- SMS/SCCM Plugin

- SCCM plugin
- Installation overview
 - SCCM server details
 - Default server
 - Assign devices
 - Advanced SCCM options
 - Testing the SCCM plugin
 - SCCM - Available properties

VPN plugin

- Typical steps after installation
- VPN plugin
- VPN CounterACT
- Plugin hub
- Supported VPN devices
- Supported blocking methods
- VPN integration
- RADIUS Credentials - Example
- Plugin activation
- Cisco example
- VPN - Basic troubleshooting
- Demonstration with instructor

Wireless plug-in

- Overview
- Supported suppliers
- Access points and controllers
- Writing commands
- Wireless data points
- Sample policy

802.1X

- Architectural requirements
- 802.1X Foundation
- Implementing CounterACT
- 802.1X policy
- Supplicant 802.1X
- Remediation - Example
 - Best practice certificates
 - Troubleshooting 802.1X

Advanced troubleshooting

- Basic troubleshooting
- Diary review

- fstool debug
- Logs and troubleshooting
 - HPS Newspapers
 - Policy action log
 - Systematic troubleshooting in CounterACT
- Process example
- Guest login
- Troubleshooting process
- System event logs
- General use test
- Hardware testing
- Plugin testing
- System event logs
- Network troubleshooting
- Technical support plugin
- Epoch Time
- CounterACT CLI

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.

