

Day 1: Introduction to Forescout and Network Security

- 1.1. Course Overview 1.1.1. Welcome and Course Objectives 1.1.2. About Forescout
- 1.2. Network Security Fundamentals 1.2.1. The Importance of Network Security 1.2.2. Common Network Security Threats
- 1.3. Forescout Platform Introduction 1.3.1. Forescout Components and Architecture 1.3.2. Installation and Setup

Day 2: Forescout Deployment and Configuration

- 2.1. Forescout Deployment Options 2.1.1. On-Premises vs. Cloud Deployment 2.1.2. Hardware and Software Requirements
- 2.2. Initial Configuration 2.2.1. System Settings 2.2.2. Licensing and Registration
- 2.3. Device Discovery and Classification 2.3.1. Scanning and Discovery Techniques 2.3.2. Device Classification and Profiling

Day 3: Policy Creation and Enforcement

- 3.1. Policy Fundamentals 3.1.1. Understanding Policy Rules 3.1.2. Policy Best Practices
- 3.2. Policy Creation 3.2.1. Creating Access Control Policies 3.2.2. Custom Policy Rules
- 3.3. Enforcement and Remediation 3.3.1. Implementing Policy Enforcement 3.3.2. Remediation Strategies

Day 4: Monitoring and Troubleshooting

- 4.1. Real-time Monitoring 4.1.1. Live Dashboard 4.1.2. Alerts and Notifications
- 4.2. Reporting and Analysis 4.2.1. Generating Reports 4.2.2. Analyzing Network Activity
- 4.3. Troubleshooting Forescout 4.3.1. Common Issues and Solutions 4.3.2. Troubleshooting Best Practices
- 4.4. Certification Exam Preparation 4.4.1. Exam Overview 4.4.2. Practice Questions and Review