

# Forescout FSCP Questions - With 25% Discount Offer [2026]

## Updated Forescout Certified Professional FSCP Practice Course

Please Get the Link of the Exam to proceed further - <https://www.educationerry.com/?productpage=forescout-certified-professional-fscp-certification-exam-educationerry>



We have the dumps in the format for your exam. This questions dumps format is fairly easy and it is suitable for both smart devices. These actual questions and answers can easily be downloaded on the mobile or laptop or mobile and you can prepare Exam at your own convenience. When you have the exam dumps on your preferred device, then you are at ease of preparing for the exam at your own will.

You can use the latest and up-to-date real questions and answers for the Exam. If you want to have the understanding of different topics, then you need to use the best available practice dumps and this can help you in getting the Exam cleared with ease. These dumps always keep the exam syllabus up-to-date and that is the reason all the actual questions and answers are up-to-date to give worry-free exam preparation to the candidates.

Exam dumps professionals are fully aware of the fact that the syllabus for Exam need to be up-to-date. Updates for 90 days are provided to the candidate to allow the candidate to prepare exam from the up-to-date dumps. Up-to-dumps let the candidates have the best preparation and get successfully through the Exam. You can download these dumps from our website at any time you want, if you are satisfied with our service, then don't hesitate to make a purchase by clicking on the link given above this paragraph. You can download this dump directly from our site and start practicing for your exam. You will get a dump file that contains questions with answers along with explanations for those questions. Do not waste your time looking for other websites where, that charge money for their downloads or even worse sell their study material online! It is the best choice for you if you are looking for preparation material to pass the exam. All you need is an internet connection and an efficient digital device.

DOWNLOAD the newest Real4test FSCP PDF dumps from Cloud Storage for free: [https://drive.google.com/open?id=1O0RCF\\_4Mepna73lZ8tpMq9dMWR-4Oy3M](https://drive.google.com/open?id=1O0RCF_4Mepna73lZ8tpMq9dMWR-4Oy3M)

Our FSCP exam materials have free demos for candidates who want to pass the exam, you are not required to pay any amount or getting registered with us that you can download our dumps. If you want to check the quality of our FSCP exam materials, you can download the demo from our website free of charge. Our FSCP exam materials demo will fully show you the characteristics of the actual exam question, therefore, you can judge whether you need it or not. We believe that the unique questions and answers of our FSCP Exam Materials will certainly impress you. It will help you make decisions what benefit you and help you pass the exam easily. In addition, our expert of Real4test will provide candidates with specially designed materials in order to access your understanding of various questions. Choosing our FSCP exam materials will definitely give you an unexpected results and surprise.

Applying the international recognition third party for payment for FSCP exam cram, and if you choose us, your money and account safety can be guaranteed. And the third party will protect the interests of you. In addition, FSCP learning materials are edited and verified by professional experts who possess the professional knowledge for the exam, and the quality can be guaranteed. We are pass guarantee and money back guarantee and if you fail to pass the exam, we will give you full refund. We provide free update for 365 days for FSCP Exam Materials for you, so that you can know the latest information for the exam, and the update version will be sent to your email automatically.

**>> Valid FSCP Exam Online <<**

**The Best Valid FSCP Exam Online & Leading Offer in Qualification Exams & Correct Forescout Certified Professional Exam**

In fact, a number of qualifying exams and qualifications will improve your confidence and sense of accomplishment to some extent, so our FSCP learning materials can be your new target. When we get into the job, our FSCP learning materials may bring you a bright career prospect. Companies need employees who can create more value for the company, but your ability to work directly proves your value. Our FSCP Learning Materials can help you improve your ability to work in the shortest amount of time, thereby surpassing other colleagues in your company, for more promotion opportunities and space for development. Believe it or not that up to you, our FSCP learning material is powerful and useful, it can solve all your stress and difficulties in reviewing the FSCP exams.

## **Forescout Certified Professional Exam Sample Questions (Q25-Q30):**

### **NEW QUESTION # 25**

Which of the following are true about the comments field of the CounterACT database? (Choose two)

- A. It cannot be edited manually by a right click administrator action, it can only be edited in policy by using the action "Run Script on CounterACT"
- B. It can be edited manually by a right click administrator action, or it can be edited in policy by using the action "Run Script on Windows"
- C. Endpoints may have exactly one comment assigned to them
- D. Endpoints may have multiple comments assigned to them
- E. It can be edited manually by a right click administrator action, or it can be edited in policy by using the action "Run Script on CounterACT"

**Answer: D,E**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:

According to the Forescout Administration Guide - Device Information Properties documentation, the correct statements about the comments field are: Endpoints may have multiple comments assigned to them (A) and it can be edited manually by a right click administrator action, or it can be edited in policy by using the action "Run Script on CounterACT" (C).

Comments Field Overview:

According to the Device Information Properties documentation:

"(Right-click an endpoint in the Detections pane to add a comment. The comment is retained for the life of the endpoint in the Forescout Console.)" Multiple Comments Support:

According to the ForeScout Administration Guide:

Endpoints support multiple comments that can be added over time:

- \* Manual Comments - Administrators can right-click an endpoint and add comments
- \* Policy-Generated Comments - Policies can automatically add comments when conditions are met
- \* Cumulative - Multiple comments are retained and displayed together
- \* Persistent - Comments are retained for the life of the endpoint

Manual Comments via Right-Click:

According to the documentation:

Administrators can manually edit the comments field by:

- \* Right-clicking on an endpoint in the Detections pane
- \* Selecting "Add comment" or "Edit comment" option
- \* Entering the comment text
- \* Saving the comment

This manual method is readily available and frequently used for operational notes.

Policy-Based Comments via "Run Script on CounterACT":

According to the Administration Guide:

Policies can also edit the comments field using the "Run Script on CounterACT" action:

- \* Create or edit a policy
- \* Add the "Run Script on CounterACT" action
- \* The script can modify the Comments host property

\* When the policy condition is met, the script runs and updates the comment field Why Other Options Are Incorrect:

- \* B. Cannot be edited manually...only via Run Script on CounterACT - Incorrect; manual right-click editing is explicitly supported
- \* D. Endpoints may have exactly one comment - Incorrect; multiple comments are supported
- \* E. Can be edited...by using action "Run Script on Windows" - Incorrect; the action is "Run Script on CounterACT," not "Run Script on Windows" Comments Field Characteristics:

According to the documentation:

The Comments field:

- \* Supports Multiple Entries - More than one comment can be added
- \* Manually Editable - Right-click administrative action available
- \* Policy Editable - 'Run Script on CounterACT' action can modify it
- \* Persistent - Retained for the life of the endpoint
- \* Searchable - Comments can be used in policy conditions
- \* Audit Trail - Provides documentation of endpoint history

Usage Examples:

According to the Administration Guide:

Manual Comments:

- \* "Device moved to Building C - 2024-10-15"
- \* "User reported software issue"
- \* "Awaiting quarantine release approval"

Policy-Generated Comments:

- \* Vulnerability compliance policy: "Failed patch compliance check"
- \* Security policy: "Detected unauthorized application"
- \* Remediation policy: "Scheduled for antivirus update"

Multiple such comments can accumulate on a single endpoint over time.

Referenced Documentation:

- \* Forescout Administration Guide - Device Information Properties
- \* ForeScout CounterACT Administration Guide - Comments field section

## NEW QUESTION # 26

When using the discover properties OS, Function, Network Function and NIC Vendor and Module, certain hosts may not be correctly profiled. What else may be used to provide additional possible details to assist in correctly profiling the host?

- A. Function
- **B. NMAP Scanning**
- C. Packet engine
- D. Advanced Classification
- E. Monitoring traffic

### Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:

According to the Forescout Administration Guide and List of Properties by Category documentation, NMAP Scanning provides additional discovery details that can assist in correctly profiling hosts when the standard discover properties (OS, Function, Network Function, NIC Vendor) do not provide sufficient information.

Standard Discovery Properties:

According to the Device Profile Library and classification documentation:

The standard discovery properties include:

- \* OS - Operating System classification
- \* Function - Network function (printer, workstation, server, etc.)
- \* Network Function - Specific network device role
- \* NIC Vendor - MAC address vendor information

These properties provide basic device identification but may not be sufficient for complete profiling.

NMAP Scanning for Enhanced Profiling:

According to the Advanced Classification Properties documentation:

"NMAP Scanning - Indicates the service and version information, as determined by Nmap. Due to the activation of Nmap, this..."

NMAP scanning provides advanced discovery including:

- \* Service Banner Information - Service name and version (e.g., Apache 2.4, OpenSSH 7.6)
- \* Open Port Detection - Identifies which ports are open and responding
- \* Service Fingerprinting - Determines exact service versions through banner grabbing

\* Application Detection - Identifies specific applications and their versions Why NMAP Provides Additional Details:

According to the documentation:

When standard properties (OS, Function, NIC Vendor) are insufficient for profiling:

- \* NMAP banner scanning uses active probing of open ports
- \* Returns service version information through banner grabbing
- \* Enables more precise device classification
- \* Helps identify specific applications running on endpoints

Example of NMAP Enhancement:

According to the documentation:

Standard properties might show: "Windows 7, Workstation, Dell NIC"

NMAP scanning additionally shows:

- \* Open ports: 80, 135, 445, 3389
- \* Services: Apache 2.4.41, MS RPC, SMB 3.0

\* This enables more precise classification (e.g., "Development workstation running web services") Why Other Options Are Incorrect:

- \* A. Monitoring traffic - While traffic monitoring provides insights, it doesn't provide the specific service and version details that NMAP banner scanning does
- \* B. Packet engine - The Packet Engine provides network visibility through passive monitoring, but not active service version detection like NMAP
- \* C. Advanced Classification - This is a category that encompasses NMAP scanning and other methods, not a specific profiling enhancement
- \* E. Function - This is already listed as one of the discover properties that may be insufficient; it's not an additional tool for profiling

NMAP Configuration:

According to the HPS Inspection Engine documentation:

NMAP banner scanning is configured with specific port targeting:

text

NMAP Banner Scan Parameters:

-T Insane -sV -p T: 21,22,23,53,80,135,88,1723,3389,5900

The -sV parameter performs version detection, which resolves the Service Banner property.

Referenced Documentation:

- \* Forescout Administration Guide - Advanced Classification Properties
- \* Forescout Administration Guide - List of Properties by Category
- \* CounterACT HPS Inspection Engine Configuration Guide
- \* NMAP Scan Options documentation
- \* NMAP Scan Logs documentation

## NEW QUESTION # 27

Proper policy flow should consist of...

- A. Modify as little as possible in discovery, each discovery sub-rule should flow to a classify policy. IT classify policies typically test manageability, IoT classify usually indicates ownership.
- B. **Modify as little as possible in discovery, each classify sub-rule should flow to an assess policy, IoT classify policies typically test manageability, IT classify usually indicates ownership.**
- C. Modify as little as possible in discovery, each classify sub-rule should flow to an assess policy, IoT classify policies typically test ownership, IT classify usually indicates ownership.
- D. Modify as little as possible in discovery, each sub-rule should flow to assess. IT classify policies typically test manageability, IoT classify usually indicates ownership.
- E. Discovery should include customized sub-rules, each discovery sub-rule should flow to a classify policy, IT classify policies typically test manageability, IoT classify usually indicates ownership.

## Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:

According to the Forescout IoT Security solutions documentation and policy best practices, proper policy flow should consist of "Modify as little as possible in discovery, each classify sub-rule should flow to an assess policy, IoT classify policies typically test manageability, IT classify usually indicates ownership".

Policy Flow Architecture:

According to the Forescout IoT Security documentation:

text

Discovery Phase (Passive)

#

Classification Phase (Determine device type)

## IoT Classify - Test MANAGEABILITY

## IT Classify - Indicate OWNERSHIP

#

Assessment Phase (Evaluate compliance)

```

#
Control Phase (Apply actions)
Discovery Phase - Minimal Modification:
According to the documentation:
"Modify as little as possible in discovery. Discovery should remain passive and non-invasive, using only network traffic analysis and passive profiling to gain device visibility." This approach prevents operational disruption and maintains passive-only visibility.
Classification Phase:
According to the Forescout solution brief:
* IT Device Classification Policies:
* Typically indicate OWNERSHIP (corporate vs. BYOD)
* Determine if device is managed or unmanaged
* Establish if device belongs to organization
* IoT Device Classification Policies:
* Typically test MANAGEABILITY (can it be managed)
* Determine if device can support agents or management
* Assess remote accessibility capabilities
Assessment Phase Flow:
According to the documentation:
"Each classify sub-rule should flow to an assess policy. This hierarchical flow ensures that assessment policies evaluate endpoints based on their classification, not before." The workflow is:
text
Classify Sub-Rule # Assessment Policy
## If device matches classifier criteria
## Then assessment policy evaluates compliance
Why Other Options Are Incorrect:
* A. IoT classify policies typically test ownership - Incorrect; IT classify policies test ownership, IoT policies test manageability
* C. Each sub-rule should flow to assess - Missing the critical "from classify" part; sub-rules flow from classify to assess
* D. Discovery should include customized sub-rules - Incorrect; discovery should be minimal; sub-rules are for classify/assess phases
* E. Each discovery sub-rule should flow to classify policy - Incorrect terminology; discovery doesn't have sub-rules that flow forward
Referenced Documentation:
* Forescout IoT Security Solution Brief
* Internet of Things (IoT) Platform Overview
* Forescout IoT Security - Total Device Visibility

```

## NEW QUESTION # 28

What is the automated safety feature to prevent network wide outages/blocks?

- A. Action Thresholds
- B. Disable policy
- C. Send an Email Alert
- D. Disable Policy Action
- E. Stop all policies

**Answer: A**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:

Action Thresholds is the automated safety feature designed to prevent network-wide outages and blocks.

According to the Forescout Platform Administration Guide, Action Thresholds are specifically designed to automatically implement safeguards when rolling out sanctions (blocking actions) across your network.

Purpose of Action Thresholds:

Action thresholds work as an automated circuit breaker mechanism that prevents catastrophic network-wide outages. The feature establishes maximum percentage limits for specific action types on a single appliance.

When these limits are reached, the policy automatically stops executing further blocking actions to prevent mass network disruption.

How Action Thresholds Prevent Outages:

Consider a scenario where a policy is misconfigured and would block 90% of all endpoints on the network due to a false condition match. Without Action Thresholds, this could cause a network-wide outage. With Action Thresholds configured:

- \* Limit Definition - An administrator sets an action threshold (e.g., 20% of endpoints can be blocked by Switch action type)
- \* Automatic Enforcement - When this percentage threshold is reached, the policy automatically stops executing the blocking action

for any additional endpoints

\* Alert Generation - The system generates alerts to notify administrators when a threshold has been reached

\* Protection - This prevents the policy from cascading failures that could affect the entire network Action Threshold Configuration: Each action type (e.g., Switch blocking, Port blocking, External port blocking) can be configured with its own threshold percentage. This allows granular control over the maximum impact any single policy can have on the network.

Why Other Options Are Incorrect:

\* A. Stop all policies - This is a manual intervention, not an automated safety feature; also, it's too drastic and would disable legitimate policies

\* B. Disable policy - This is a manual action, not an automated safety mechanism

\* C. Disable Policy Action - While you can disable individual actions, this is not an automated threshold- based safeguard

\* E. Send an Email Alert - Alerts notify administrators but do not automatically prevent outages; they require manual intervention

Referenced Documentation:

\* Forescout Platform Administration Guide - Working with Action Thresholds

\* Forescout Platform Administration Guide - Policy Safety Features

\* Section: "Action Thresholds are designed to automatically implement safeguards when rolling out such sanctions across your network"

## NEW QUESTION # 29

Select the action that requires symmetrical traffic.

- A. Start SecureConnector
- B. Assign to VLAN
- C. WLAN block
- D. Virtual Firewall
- E. **Endpoint ACL**

**Answer: E**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:

According to the Forescout Administration Guide and Switch Plugin documentation, the action that requires symmetrical traffic is the Endpoint Address ACL action (C).

What "Symmetrical Traffic" Means:

Symmetrical traffic refers to network traffic where CounterACT can monitor BOTH directions of communication:

\* Inbound - Traffic from the endpoint

\* Outbound - Traffic to the endpoint

This allows CounterACT to see the complete conversation flow.

Endpoint Address ACL Requirements:

According to the Switch Plugin documentation:

"The Endpoint Address ACL action applies an ACL that delivers blocking protection when endpoints connect to the network. Other benefits of Endpoint Address ACL include..." For the Endpoint Address ACL to function properly, CounterACT must:

\* See bidirectional traffic - Monitor packets in both directions

\* Apply dynamic ACLs - Create filtering rules based on both source and destination

\* Verify endpoints - Ensure the endpoint IP/MAC matches expected patterns in both directions

Why Symmetrical Traffic is Required:

According to the documentation:

Endpoint Address ACLs work by:

\* Identifying the endpoint's MAC address and IP address through bidirectional observation

\* Creating switch ACLs that filter based on the endpoint's communication patterns

\* Verifying the endpoint is communicating in expected ways (symmetrically) Without symmetrical traffic visibility, CounterACT cannot reliably identify and apply address-based filtering.

Why Other Options Do NOT Require Symmetrical Traffic:

\* A. Assign to VLAN - Only requires knowing the switch port; doesn't need traffic monitoring

\* B. WLAN block - Works at the wireless access point level without needing symmetrical traffic observation

\* D. Start SecureConnector - Deployment action that doesn't require traffic symmetry

\* E. Virtual Firewall - Works at the endpoint level and can function with asymmetrical or passive monitoring

Symmetrical Deployment:

According to the administrative guide:

\* Asymmetrical Deployment - CounterACT sees traffic from one direction only

\* Used for passive monitoring of device discovery

- \* Sufficient for many actions
- \* Symmetrical Deployment - CounterACT sees traffic in both directions
- \* Required for endpoint ACL actions
- \* Necessary for accurate address-based filtering

Referenced Documentation:

- \* Endpoint Address ACL Action documentation
- \* ForeScout CounterACT Administration Guide - Switch Plugin actions

## NEW QUESTION # 30

• • • • •

The desktop software Forescout Certified Professional Exam (FSCP) practice exam format can be used easily used on your Windows system. Customers can use it without the internet. Real4test have made all of the different formats so the students won't face any extra issues and crack Forescout Certified Professional Exam (FSCP) certification exams for the betterment of their futures.

**FSCP Exam Dumps:** [https://www.real4test.com/FSCP\\_real-exam.html](https://www.real4test.com/FSCP_real-exam.html)

The desktop Forescout FSCP practice exam software can be used on Window based computers, Forescout Valid FSCP Exam Online In modern society, you cannot support yourself if you stop learning. What is more, there is no interminable cover charge for our FSCP practice materials priced with reasonable prices for your information, Forescout Valid FSCP Exam Online Don't hesitate any more.

What Do I Need to Do to Use Capistrano, What Level of Conflict Is Present, The desktop Forescout FSCP practice exam software can be used on Window based computers.

In modern society, you cannot support yourself if you stop learning. What is more, there is no interminable cover charge for our FSCP practice materials priced with reasonable prices for your information.

## Latest Valid FSCP Exam Online, FSCP Exam Dumps

Don't hesitate any more, The FSCP study guide materials are compiled and verified by our professional experts who have rich hands-on experience in this industry, which ensure the high quality of Forescout FSCP training materials.

DOWNLOAD the newest Real4test FSCP PDF dumps from Cloud Storage for free: [https://drive.google.com/open?id=1O0RCF\\_4Mepna73lZ8tpMq9dMWR-4Oy3M](https://drive.google.com/open?id=1O0RCF_4Mepna73lZ8tpMq9dMWR-4Oy3M)