IBM

Exam C2150-202

IBM Security Access Manager for Mobile V8.0 Implementation

Version: 6.0

[Total Questions: 70]

Question No : 1

Which two features require a product license key? (Choose two.)

A. Access Manager for Web
B. Access Manager for Mobile
C. Access Manager Session Cache
D. Access Manager for Load Balancing
E. Access Manager Risk-based Authentication

Answer: A,B

Reference:http://www-
01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/6/897/ENUS214-
036/index.html&lang=en&request_locale=en

Question No : 2

You are tasked with designing a solution that meets the following requirements:

1. Allow authenticated users to access web resources for transaction amounts less than $1.000

2. Require additional authentication for transaction amounts greater than or equal to $1.000

Which features of ISAM for Mobile will help meet the above requirements when designing the plan to deploy ISAM for Mobile?

A. Custom attributes,Policy,OTP
B. Predefined attributes,Policy,OTP
C. Custom attributes,Policy,Device registration
D. Predefined attributes,Policy,Device registration

Answer: A

Question No : 3

As the administrator for ISAM for Mobile, you are tasked with setting up risk based policies

that allow access to resources outside of normal hours after additional authentication. The landing pages for the resources are on different servers that are in different domains. You add info.js to the landing pages for each resource.

Which mechanism should be used to ensure the risk based policies are evaluated correctly for each resource?

A. Cross Site Scripting
B. Cross Script Java Sharing
C. Cross Site Request Forgery
D. Cross Origin Resource Sharing

Answer: C

Question No : 4

A security analyst has developed and successfully tested an adjusted Trusteer Policy Information Point (PIP) in the Development environment.

The next step is to deploy this new Trusteer PIP in the Acceptance environment so the proper testing can be executed.

How is this new Trusteer PIP deployed?

A. Log into the Environment Dashboard. Select the Trusteer PIP in the Development area and use the Propagate option to deploy in on the Acceptance environment.
B. Select on your Development environment in the "Secure Mobile Settings / Policy / Information Points" screen the Trusteer PIP,choose the Export option, move the file to the Acceptance environment and use the Import option on the equivalent screen.
C. Select on your Development environment in the "Secure Mobile Settings / Policy / Information Points" screen the Trusteer PIP,choose the Download option, move the file to the Acceptance environment and use the Upload option on the equivalent screen.
D. Select the Trusteer PI P in the "Secure Mobile Settings / Policy / Information Points" screen on the Development environment, use the Promote option to enable it to be received by another environment. Next login to the Acceptance environment and use the Receive option.

Answer: D

Question No : 5

Which two attributes may be automatically set during device registration? (Choose two.)

A. stepUp
B. deviceId
C. isRegistered
D. userConsent
E. authenticationLevel

Answer: D,E

Reference:http://www-
01.ibm.com/support/knowledgecenter/SSELE6_8.0.0.4/com.ibm.isam.doc_8.0.0.4/admin/c
pt/consent_based_device_registration.html(Content-based devise registration 3rd Para)

Question No : 6

Which member of the IBM Security Access Manager product family acts as a Policy
Enforcement Point(PEP)?

A. IBM Tivoli Federated Identity Manager
B. IBM Security Access Manager for Web
C. IBM Security Access Manager for Mobile
D. IBM Security Access Manager of Enterprise Single Sign-on

Answer: B,C

Reference:http://www-01.ibm.com/common/ssi/cgi-
bin/ssialias?infotype=an&subtype=ca&appname=gpateam&supplier=872&letternum=ENUS
AP14-0399

Question No : 7

Which rule must a policy include to require an unauthenticated user to consent to register a
device?

A. The userConsent attribute is set to true and that permits access with Obligation Register Device.

B. The registeredDeviceCount is missing or set to zero and that permits access with Obligation Register Device.

C. The userConsent attribute is not present and that will permit access with Authentication Consent Register Device.

D. The riskScore attribute is below a configured threshold and that will permit access with ObligationRegister Device.

Answer: D

Reference:http://www.ibm.com/developerworks/library/se-accessmanager/

Question No : 8

Which three types of application logs are available? (Choose three.)

A. Fsck
B. Mga
C. Cluster
D. System
E. Performance
F. Management_ui

Answer: B,C,F

Reference:http://www-01.ibm.com/support/docview.wss?uid=swg27042973&aid=14(Chapter 6 Viewing application log files)

Question No : 9

Which two types of risk profiles are supported? (Choose two.)

A. Custom risk profiles
B. Obligated risk profiles
C. Pre-defined risk profiles

D. Content-based risk profiles
E. Consent-based risk profiles

Answer: B,C

Reference:http://www-01.ibm.com/support/docview.wss?uid=swg27042973&aid=8(Chapter 2 Risk Management overview)

Question No : 10

How many DMZ network segments can the appliance support?

A. 2
B. 4
C. 6
D. 8

Answer: A

Reference:http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=an&subtype=ca&appname=gpateam&supplier=897&letternum=ENUS 212-438

Question No : 11

Which two valid predefined obligations are provided to use in policy authoring? (Choose two.)

A. One-time password
B. Consent select device
C. Consent register device
D. Consent unregister device
E. POTP one-time password

Answer: A,C