PassQueen
a.k.a dumpsqueen.com

RSA SecurID Certified Administrator 8.0 Exam

RSA 050-80-CASECURID01

Version Demo

Total Demo Questions: 9

Total Premium Questions: 98

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, RSA Authentication Manager Overview	6
Topic 2, RSA Authentication Manager Installation and Configuration	7
Topic 3, RSA Authentication Manager Administration	40
Topic 4, RSA Authentication Manager Authentication	35
Topic 5, RSA Authentication Manager Maintenance and Troubleshooting	10
Total	98

QUESTION NO: 1

When using the “Resynchronize Token” function, after an administrator enters two consecutive tokencodes, the token clock time is displayed.

A. False

B. True

ANSWER: B

Explanation:

True is correct. The Resynchronize Token process is designed to correct the time offset between a time-based SecurID token and RSA Authentication Manager. The administrator obtains and enters two tokencodes generated consecutively by the assigned token. Authentication Manager uses the sequence and the expected token-code interval to calculate the token’s clock setting and resynchronize it with the system. After the two tokencodes are processed, the resynchronization workflow displays the token clock time, allowing the administrator to review the calculated token time as part of confirming the operation. This visibility is useful when investigating authentication failures caused by clock drift, an incorrect time setting, or a token that has not been used for an extended period. The task applies to time-based SecurID tokens because their generated tokencodes depend on both the token seed and the current token clock. RSA Authentication Manager administrative documentation covers token management and resynchronization procedures, while RSA’s documentation portal provides the product documentation resources for SecurID environments. See the RSA Authentication Manager 8.0 Administrator’s Guide and the RSA documentation portal.

QUESTION NO: 2

The term "Secured by RSA” is most closely associated with

A. An RSA token device.

B. Asecure directory server.

C. An Authentication Agent device.

D. AManaged Security Provider company.

ANSWER: C

Explanation:

An Authentication Agent device. is correct. In RSA SecurID terminology, an authentication agent is the software component installed on, or integrated with, a protected resource such as a server, VPN, web application, or network-access device. The agent communicates with RSA Authentication Manager to request and validate authentication, then permits or denies access according to the authentication result and applicable policy. A resource protected in this way is commonly described as an authentication agent device, and “Secured by RSA” identifies the association between that protected device and RSA authentication technology. The wording therefore concerns the protected endpoint or application where the agent is operating, rather than the authenticator a user possesses or an organization delivering security services. This distinction is important for administration: the device must be configured as an authentication agent in Authentication Manager, assigned the appropriate agent record and configuration information, and connected to the relevant authentication policies. RSA’s documentation describes authentication agents as the components that protect resources and interact with Authentication Manager during authentication processing. See the RSA Authentication Manager 8.0 Administrator’s Guide and the RSA SecurID documentation portal.

QUESTION NO: 3

During a token resynchronization process for a time-based RSA SecurID token, which statements are true? (Choose two)

A. The user provides consecutive tokencodes.

B. Authentication Manager updates the token time offset when the codes validate.

C. Authentication Manager assigns a new token seed.

D. The user's PIN is automatically cleared.

E. The token expiration date is extended.

ANSWER: A B

Explanation:

The user provides consecutive tokencodes and **Authentication Manager updates the token time offset when the codes validate** are correct. Resynchronization is used when the token clock has drifted beyond the normal validation window. Authentication Manager evaluates the sequence of codes to determine the token's offset relative to the server time and records the corrected offset.

Resynchronization does not assign a new token seed, reset the user's PIN, or change the token's factory expiration date. See the RSA documentation portal for SecurID token troubleshooting and administration procedures.

QUESTION NO: 4

Which types of events can RSA Authentication Manager audit and reporting functions help administrators investigate? (Choose two)

A. Authentication events

B. Administrative events

C. The contents of token seeds

D. All network packets traversing the organization

E. A user's local browser history

ANSWER: A B

Explanation:

Authentication events and **administrative events** are correct. Authentication Manager records information about authentication processing, such as successful and failed requests, and it also records administrative actions performed in the deployment. Administrators can use audit data and reports to support troubleshooting, review, and compliance activities.

Authentication Manager audit reporting does not capture the contents of a user's token seed or operate as a packet-capture utility for all network traffic. See the RSA documentation portal for audit and reporting documentation.

QUESTION NO: 5

What action will allow an Authentication Agent to register automatically with RSA Authentication Manager?

A. Edit the Authentication Agent Access Policy to allow auto-registration

B. Enable "Allow authentication agent auto-registration" in the Agent record

C. Select the option to “Allow Auto Registration” during installation of the Agent

D. Add “Auto-Registration=ALLOW" as a parameter value in the sdconf.rec file

ANSWER: B

Explanation:

Enable "Allow authentication agent auto-registration" in the Agent record is correct because RSA Authentication Manager controls whether an individual Authentication Agent is permitted to create or update its registration automatically through the agent record's auto-registration setting. When this setting is enabled, the agent can contact Authentication Manager and complete its registration without an administrator manually registering the agent through the Security Console first. This supports controlled deployment of agents while retaining an explicit server-side authorization decision for each agent record.

Automatic registration is an Authentication Manager configuration capability, not simply an installer choice or a local configuration-file directive. The administrator enables the appropriate auto-registration permission in the Authentication Agent configuration maintained by Authentication Manager, then ensures the agent has the required connection and trust configuration to communicate with the deployment. RSA's Authentication Manager documentation describes administration of Authentication Agents and their registration behavior in the Security Console. See the RSA Authentication Manager 8.0 documentation and RSA's Authentication Agent documentation.

QUESTION NO: 6

An organization configures RSA Authentication Manager to process authentication requests from a VPN concentrator by using RADIUS. Which object identifies the VPN concentrator to Authentication Manager?

A. A RADIUS client record

B. An Authentication Agent record

C. A user group

D. An identity source

ANSWER: A

Explanation:

A RADIUS client record is correct. In RSA Authentication Manager, a RADIUS client record represents the network-access device or application that sends RADIUS Access-Request messages to the Authentication Manager RADIUS server. The record identifies the client and contains settings used to validate and process its requests.

The RADIUS client is distinct from an Authentication Agent record. Authentication Agent records apply to RSA Authentication Agents, whereas RADIUS client records are used for devices that communicate through the RADIUS protocol. See the RSA documentation portal for RADIUS administration guidance.

QUESTION NO: 7

Which actions are appropriate when several users report that requested On-Demand Tokencodes are not being delivered? (Choose two)

A. Verify connectivity to the configured SMTP server or SMS gateway.

B. Verify users' registered delivery addresses or phone numbers.

C. Clear each affected user's SecurID PIN.

D. Resynchronize all assigned hardware tokens.

E. Change the token expiration date.

ANSWER: A B

Explanation:

When multiple users are affected, the shared delivery configuration should be investigated. Administrators should verify that the configured SMTP server or SMS gateway is reachable and accepts messages from Authentication Manager. They

should also review the affected users' registered email addresses or telephone numbers to confirm that valid delivery destinations are configured.

Clearing a SecurID PIN or resynchronizing a hardware token does not correct a shared email or SMS delivery failure. See the RSA documentation portal for on-demand authentication and delivery-service troubleshooting guidance.

QUESTION NO: 8

A user password policy can be used to define

A. Which character strings cannot be used for passwords.

B. The number of password attempts before a user is locked out.

C. Which RSA SecurID token types can be used with or without PINs.

D. If Windows Password Integration is used with Authentication Manager.

ANSWER: A

Explanation:

“Which character strings cannot be used for passwords.” is correct because an RSA SecurID Authentication Manager user password policy controls requirements and restrictions for passwords that users set and manage within Authentication Manager. Among these controls, an administrator can configure disallowed or prohibited character strings so that passwords containing predictable, organization-specific, or otherwise unsuitable text are rejected. This helps prevent users from selecting passwords containing easily guessed terms such as company names, product names, common words, or other strings that the organization chooses to block.

Using restricted strings is a practical complement to ordinary password-complexity requirements. Complexity rules may require a minimum length and a mixture of character categories, but they do not necessarily prevent a password from including a known sensitive or predictable word. By defining strings that cannot appear in a password, the password policy enforces a more targeted standard whenever a user creates or changes an Authentication Manager password. RSA documents password-policy administration as part of Authentication Manager’s identity and credential-management configuration. See the RSA Authentication Manager 8.0 Administrator’s Guide and the RSA Authentication Manager 8.0 documentation.

QUESTION NO: 9

What are two elements are involved in Risk-Based Authentication? (Choose two)

A. a user’s device profile

B. a user’s Security Level

C. the length of a user’s PIN

D. the behavior pattern of a user

E. the strength of a user’s Passcode

ANSWER: A D

Explanation:

Risk-Based Authentication evaluates contextual information about an access attempt to calculate whether the attempt resembles the user’s normal activity and whether additional authentication should be required. A user’s device profile is a core input because RSA SecurID can recognize device-related characteristics and compare the current device context with previously observed devices. This helps distinguish a familiar access pattern from one that may warrant a step-up challenge.

The behavior pattern of a user is also a core input. Behavioral and contextual signals, such as typical usage patterns and other characteristics of the authentication attempt, allow the risk engine to assess whether the request is consistent with the legitimate user's established profile. The resulting risk evaluation supports adaptive authentication: lower-risk requests may proceed normally, while elevated-risk requests can require stronger verification. RSA describes this approach as using risk and contextual intelligence to make authentication decisions, rather than relying solely on a static credential. See the RSA SecurID product overview and RSA's security resources for information on adaptive, risk-based access protection.