



Vendor: RSA Security

Exam Code: 050-v71-CASECURID02

Exam Name: RSA SecurID Certified Administrator 7.1

Exam

Version: DEMO

1. An RSA SecurID tokencode is unique for each successful authentication because

- A. a token periodically calculates a new code
- B. the user continuously changes their secret PIN
- C. the Node Secret is updated after each authentication
- D. the Server's clock is set to Universal Coordinated Time (UTC)

Answer: A

2. RSA SecurID tokens are initially supplied with matching token records. After tokens are assigned, deployed and used by end-users, what information might be overwritten if the original token records are re-imported into the RSA Authentication Manager database? (Choose two)

- A. user assignment
- B. tokencode values
- C. Authentication Agent usage
- D. token time offset information
- E. system PIN parameter settings

Answer: A,D

3. A user reports a problem while trying to authenticate. The administrator checks recent activities and sees that the last message associated with this user is "New Pin Cancelled." What is the most likely cause?

- A. The user is not in New PIN mode.
- B. The user is not in the server database.
- C. The user did not complete the New PIN operation successfully.
- D. The user is not authorized to authenticate through this Authentication Agent.

Answer: C

4. When assigning a user a Temporary Fixed Tokencode to replace a lost token, what is the default value for the expiration period of that Tokencode?

- A. 24 hours
- B. 5 days
- C. 14 days
- D. 30 days

Answer: C

5. A user is trying to authenticate from their workstation to the RSA Authentication Manager but receives an "Access Denied" message. The Server's log is showing the following error message: "Node secret mismatch". What is a likely cause?

- A. The sdconf.rec is missing from the Agent machine.
- B. The user is not allowed to authenticate on that Agent.
- C. The Agent has not been added into the Server database.
- D. The secret key used to encrypt Agent communication has been deleted.

Answer: D

6.Operation between Windows, Linux and UNIX platforms is supported by RSA Authentication Manager for which types of communications? (Choose two)

- A. Agent to Server
- B. Database Replication
- C. Primary to Replica Server
- D. Trusted Realm authentication
- E. Database server to Server Node

Answer: A,D

7.Three consecutive log entries for one user contain the message "Authentication Method Failed", what administrative action would NOT be appropriate?

- A. resynchronize the token
- B. set the user's PIN to Next Tokencode
- C. assign a temporary Fixed Passcode for troubleshooting
- D. check the system time of the RSA Authentication Manager host

Answer: B

8.An RSA Authentication Manager administrator would edit an Identity Attribute parameter

- A. to ignore users with duplicate user names.
- B. to store additional user information in a user record.
- C. to specify an LDAP Bind DN and Bind DN password.
- D. when the LDAP server is not in the same domain as the RSA Authentication Manager server.

Answer: B

9.If the RSA Authentication Manager places a token into Next Tokencode Mode, and the user waits for three minutes (three tokencode increments) to enter his/her next tokencode, what will be the expected result?

- A. The Server will not accept the value because it is not sequential.
- B. The authentication will be successful even though the input was delayed.
- C. The Server will ask for a third tokencode, so that it has two sequential codes.
- D. The Server will assume that the token has been stolen, and disable the token.

Answer: A

10.If a group has been defined with access times of 9 AM to 5 PM, Monday through Friday. When can a member of that group log in?

- A. at any time but must renew their login at 9 AM each day
- B. during the specified time frame, but must log out by 5 PM
- C. during that time frame and can remain logged in indefinitely
- D. during that time frame but is automatically logged out at 5 PM

Answer: C

11.When creating and running RSA Authentication Manager version 7.1 reports, the administrator has the option of (Choose two)

- A. allowing the report to run with the scope of the administrator who is running the report.
- B. defining report criteria by writing an SQL query to extract data directly from the database.
- C. customizing a report template by adding and removing columns and applying data filters.
- D. creating and running reports from a Replica database server if the Primary server is down.
- E. previewing the report output before the report is run to make sure the desired data is included.

Answer: A,C

12. Authenticators should NOT be shared by multiple users because of

- A. license concerns.
- B. hostname conflicts.
- C. database restrictions.
- D. repudiation concerns.

Answer: D

13. If multiple users request On-demand Tokencodes but are not receiving them, you would want to confirm that

- A. the users are not in New PIN mode.
- B. SMS or SMTP services are configured correctly.
- C. the tokens assigned to the users have not expired.
- D. the tokens assigned to the users have been resynchronized.

Answer: B

14. The RSA Authentication Manager has settings where (by default) three incorrect PASSCODES will invoke Next Tokencode Mode. Where is this configuration setting located?

- A. Within the Setup menu.
- B. Within the Identity menu.
- C. Within the Policies menu.
- D. Within the RADIUS menu.

Answer: C

15. You are assisting a user who is working offline on a Microsoft Windows Authentication Agent. If you provide this user with an Offline Emergency Passcode, you must tell the user

- A. to use the code in place of the RSA SecurID token passcode without using a PIN.
- B. to use the code in place of the RSA SecurID tokencode but continue to use the existing PIN.
- C. to use the code in place of the RSA SecurID tokencode but you will also issue a temporary replacement PIN.

D. to first enter their Windows password and, when prompted for the Emergency Access Code, enter the code that you provide.

Answer: A

16. A feature of the RADIUS protocol is

- A. the ability to track a user's login and logout time (RADIUS accounting).
- B. the computer time setting can be checked remotely (remote time service).
- C. a user's default login name becomes their password (RADIUS login synchronization).
- D. the user Profile and Attribute Value Pair matches their tokencode (RADIUS token matching).

Answer: A

17. RSA Authentication audit log records

- A. can be archived using a scheduled job.
- B. are only accessible by the Super Admin administrator.
- C. are always deleted from the database when they are archived.
- D. can be digitally signed by the administrator for archival storage protection.

Answer: A

18. An RSA Authentication Manager is licensed for 500 users. The license must be upgraded if you want to

- A. assign more than 500 tokens to individual users.
- B. import more than 500 token records into the database.
- C. import more than 500 users from an LDAP directory source.
- D. allow cross-realm authentication for more than 500 remote users.

Answer: A

19. If a Super Admin administrator can view a certain set of user records in the Authentication Manager database but a Help Desk administrator can not,

- A. the Help Desk administrator should be assigned a Super Admin role.
- B. the Super Admin administrator's privileges should be set to 'delegatable'.
- C. the Help Desk administrator scope may not allow viewing of these users.
- D. this would be considered a normal difference between these two types of administrators.

Answer: C

20. How many RSA Authentication Manager servers can be in a single Instance (maximum) under an Enterprise license?

- A. 1 database server and a single Server Node
- B. 1 Primary server and up to 3 Replica servers
- C. 1 database server and up to 4 Server Nodes
- D. 1 Primary server and up to 15 Replica servers

Answer: C