

100% Money Back
Guarantee

Vendor: RSA

Exam Code: 050-80-CASECURID01

Exam Name: RSA SecurID Certified Administrator 8.0
Exam

Version: Demo

QUESTION NO: 1

Which of the following can cause the error message "Node Secret Mismatch?" (Choose two)

- A. A user is not activated on the Agent Host.
- B. The Agent is not certified as "Secured by RSA"
- C. The Agent has been uninstalled then re-installed.
- D. The Agent is installed on an unreachable remote network node.
- E. The Node Secret file has been cleared or deleted on the Agent host.

Answer: C,E

Explanation:

QUESTION NO: 2

An RSA Authentication Manager Enterprise license will allow which of the following to be added to a Primary instance?

- A. multiple Replica instances
- B. Risk-Based authentication capability
- C. On-Demand authentication capability
- D. Business Continuity Option (BCO) capability

Answer: A

Explanation:

QUESTION NO: 3

What circumstance would allow an administrator to have read/write access to an RSA Authentication Manager database on a Replica instance?

- A. The Replica is first promoted to a Primary instance.
- B. The Replica instance is in a different domain from the Primary instance.
- C. The database service on the Replica instance is running in Offline mode.
- D. The Replica does not have a network connection to the Primary instance.

Answer: A

Explanation:

QUESTION NO: 4

The term "Silent Collection" refers to gathering information about a user's access and authentication patterns.

- A. True
- B. False

Answer: A

Explanation:

QUESTION NO: 5

Which types of administrative objects are contained within an RSA Authentication Manager Security Domain? (Choose two)

- A. Users
- B. Administrators
- C. Identity Sources
- D. Replica Instances
- E. Security Question Requirements

Answer: A,B

Explanation:

QUESTION NO: 6

If a user has both a Fixed Passcode and an RSA SecurID token assigned,

- A. the Fixed Passcode becomes the user's PIN by default.
- B. either the Fixed Passcode or the token may be used for authentication.
- C. the Fixed Passcode can only be used if the token status is set to 'disabled'.
- D. the user must supply their secret PIN in addition to the Fixed Passcode when authenticating.

Answer: B

Explanation:

QUESTION NO: 7

When adding a new Authentication Agent record to the RSA Authentication Manager database, an attempt is made to resolve the hostname of the Agent Host with its IP Address. If the attempt fails,

- A. the administrator can override the hostname/IP Address by using the Auto-Registration option.
- B. the Agent is added to the database with a 'Pending' status until it is first used for a successful authentication.
- C. a warning is given that the hostname/IP Address cannot be resolved but the database will allow the Agent to be added.
- D. the administrator must correct the address resolution through DNS or editing the /etc/hosts file before the Agent can be added to the database.

Answer: C

Explanation:

QUESTION NO: 8

The Operations Console allows administrators to modify attributes defined in RADIUS dictionary files.

- A. True
- B. False

Answer: A

Explanation:

QUESTION NO: 9

Can multiple Identity Sources be established from the same LDAP directory?

- A. Yes, if the mapped Organizational Units (OUs) do not overlap.
- B. Yes, if duplicate attribute values do not exist in the LDAP directory.
- C. No – only one LDAP directory can be mapped to one Identity Source.
- D. Yes, if no duplicate passwords exist in the LDAP directory (unique password for each user).

Answer: A

Explanation:

QUESTION NO: 10

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

Explanation:

QUESTION NO: 11

A User Group can include which of the following as members?

- A. other User Groups
- B. user Identity Attributes
- C. LDAP Identity Sources
- D. tokens assigned to users

Answer: A

Explanation:

QUESTION NO: 12

Of the following RSA Authentication Manager components, which one is most likely to be located in a network DMZ?

- A. Web Tier
- B. Risk Engine
- C. Replica Server
- D. Authentication Agent

Answer: A

Explanation:

QUESTION NO: 13

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. Populate the database with more than 500 users.
- C. Import more than 500 token records into the database.
- D. Map more than 500 users from an LDAP directory source.

Answer: A

Explanation:

QUESTION NO: 14

An Authentication Manager user can exist in only one Security Domain at any one time.

- A. True
- B. False

Answer: A

Explanation:

QUESTION NO: 15

Within which RSA Authentication Manager menu would you configure the number of incorrect PASSCODES that will invoke Next Tokencode Mode?

- A. Policies
- B. System Setup
- C. Identity Settings
- D. RADIUS Lockout

Answer: A

Explanation:

QUESTION NO: 16

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 Authenticaiton Manager instance clock is set to Universal Coordinated Time.

Answer: A

Explanation:

QUESTION NO: 17

What is the maximum number of active tokens and/or user fixed passcodes that can be assigned to a user at one time?

- A. one
- B. three
- C. seven
- D. unlimited

Answer: B

Explanation:

QUESTION NO: 18

If a user is NOT a member of an Authentication Manager user group, which of the following statements is true?

- A. The user can not be restricted to certain login times.
- B. The user can not be forced to adhere to password polices.
- C. The user can not take advantage of Risk-Based authentication.
- D. The user can not log on to an unrestricted Authentication Agent.

Answer: A

Explanation:

QUESTION NO: 19

What are three steps an administrator can use for reporting past user transactions stored in the RSA Authentication Manager audit database? (Choose three)

- A. Run a report job.
- B. Edit a report template.
- C. View a report job output.
- D. View the Audit Monitor utility.
- E. Use the 'view-audit-log' command line utility.
- F. Export the audit database to a spreadsheet format.

Answer: A,B,C

Explanation:

QUESTION NO: 20

Token expiration dates;

- A. Appear on the token display thirty days prior to expiration.
- B. Are programmed into a token record at the time of manufacture.
- C. Vary according to the date set by the administrator when assigning the token.
- D. Depend on the clock in the Authentication Agent to determine if the token is active.

Answer: B

Explanation:

QUESTION NO: 21

Which statements concerning RSA SecurID time-synchronous authentication are true? (Choose two)

- A. On-demand codes have a 5-minute synchronization window.
- B. Token expiration dates are based on the date of the token's first use.
- C. Calculation of a tokencode involves the use of Universal Coordinated Time.
- D. An administrator can configure the tokencode change interval on an RSA SecurID token.
- E. Tokencode calculations are performed by both the RSA Authentication Manager instance and RSA SecurID tokens.

Answer: C,E

Explanation:

QUESTION NO: 22

The Authentication Activity Monitor is helpful in which of the following cases?

- A. Monitoring a user's network path to the Web Tier server
- B. Locating RSA SecurID tokens that are near their expiration date
- C. Defining parameters for the Self-Service Troubleshooting Policy
- D. Troubleshooting authentication attempts while in direct contact with the user

Answer: D

Explanation:

QUESTION NO: 23

Which of the following services is NOT an option to users through the Self-Service Console?

- A. Changing a password or PIN
- B. Creating an individual PIN policy
- C. Requesting a replacement token
- D. Resynchronizing an RSA SecurID token

Answer: B

Explanation:

QUESTION NO: 24

For RSA Authentication Manager administration, "Administrative Role" is a combination of.
(Choose two)

- A. scope
- B. domain
- C. group list
- D. permissions
- E. RADIUS profile

Answer: A,D

Explanation:

QUESTION NO: 25

What can cause the error message "Cannot Communicate with RSA Authentication Manager" to be displayed on the RSA Authentication Agent when the Agent is used for the first time?

- A. The Agent is open only to locally known users.
- B. The Primary Instance cannot resolve the Agent's name.
- C. The Agent contains two conflicting Network Interface Cards.
- D. The Agent has the wrong name and IP address for the Primary Instance.

Answer: D

Explanation:

QUESTION NO: 26

If the access time range allowed for a group is specified as 8 AM to 6 PM each weekday, which statement about a group member's login is true?

- A. All group members will be logged out automatically at 6 PM.
- B. A user will be prompted to renew their login each day after 8 AM.
- C. A user's individual access times override a group's access time range.
- D. Once logged in during the allowed time period, a user can remain logged in indefinitely.

Answer: D

Explanation:

QUESTION NO: 27

Which RSA SecurID authentication method can use alphabetic characters as part of the user's PASSCODE?

- A. Key Fob
- B. PINPad
- C. On-demand authentication
- D. Software Token in PINPad mode

Answer: A

Explanation:

QUESTION NO: 28

The “Quick Search” function that allows access to a user’s account, token and recent activity is a feature of

- A. The User Dashboard.
- B. The Self-Service Console.
- C. On-Demand Authentication.
- D. The Windows MMC Snap-In.

Answer: A

Explanation:

QUESTION NO: 29

If a user forgets his/her PIN and still has possession of his/her token, an Administrator should verify the identity of the user and then

- A. Clear the user’s old PIN.
- B. Disable the user’s token.
- C. Assign a new token to the user.
- D. Assign a temporary Fixed Passcode.

Answer: A

Explanation:

QUESTION NO: 30

A user is trying to authenticate to establish a VPN connection but receives an “Access Denied” message. The most recent authentication log entry for the user shows the message: “PIN Rejected”. What should the next action be?

- A. Clear the user’s PIN.
- B. Resynchronize the user’s token.
- C. Clear the VPN Agent’s Node Secret.
- D. Instruct the user to log in using only a tokencode.

Answer: D

Explanation:

To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Trying our product !

- ★ **100%** Guaranteed Success
- ★ **100%** Money Back Guarantee
- ★ **365 Days** Free Update
- ★ **Instant Download** After Purchase
- ★ **24x7** Customer Support
- ★ Average **99.9%** Success Rate
- ★ More than **69,000** Satisfied Customers Worldwide
- ★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 One Year Free Update <p>Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 Money Back Guarantee <p>To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 Security & Privacy <p>We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

[Guarantee & Policy](#) | [Privacy & Policy](#) | [Terms & Conditions](#)

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © 2004-2015, All Rights Reserved.