

050-80-CASECURID01^{Q&As}

RSA SecurID Certified Administrator 8.0 Exam

Pass RSA 050-80-CASECURID01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/050-80-casecurid01.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by RSA Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

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.

Correct Answer: D

QUESTION 2

In the case where a Microsoft Windows Authentication Agent is configured for Offline Authentication, if a user requests an Emergency Access Tokencode from the Help Desk, what must the user remember?

- A. their secret PIN
- B. their token's serial number
- C. their token's last tokencode
- D. their computer's Node Secret value

Correct Answer: A

QUESTION 3

Settings for the Lockout Policy affect which of the following?

- A. User attempts to log in to the Self-service console
- B. Administrator login to the RSA Operations Console
- C. User authentication attempts using an RSA SecurID token
- D. User login to a Windows environment with Windows Password Integration

Correct Answer: C

QUESTION 4

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

Correct Answer: A

QUESTION 5

A user has an RSA SecurID Key Fob. The Key Fob Change Interval is 60 seconds and has been used successfully in the past. If the RSA Authentication Manager is now out of synch with the token by 2 minutes, what will happen when the user tries to authenticate?

- A. Authentication Manager will automatically adjust the token offset value and authenticate the user.
- B. Authentication Manager will reject the PASSCODE and the user will receive an "Access Denied" message.
- C. Authentication Manager will post a "Token Requires Resync" message in the log and deny access to the user.
- D. Authentication Manager will request the user for next tokencode, adjust the user's token offset value, and authenticate the user.

Correct Answer: D

[050-80-CASECURID01
VCE Dumps](#)

[050-80-CASECURID01
Practice Test](#)

[050-80-CASECURID01
Study Guide](#)