



RSA SecurID Certified Administrator Certification Examination Study Guide

Introduction

The RSA SecurID Certified Administrator (CA) examination is based on the critical job functions that an individual would typically be expected to perform with competence when managing an RSA SecurID system and an RSA Authentication Manager deployment.

An RSA SecurID Administrator is a person who works in a Help Desk, Call Center, Support, or Security Administrator role within an organization using RSA SecurID products.

An analysis of the major job functions expected of an RSA SecurID CA determined that there are three major areas of job role responsibility:

- General knowledge about RSA SecurID technology and the RSA Authentication Manager product
- Aptitude and familiarity with managing the RSA Authentication Manager database and common configurations – including RSA Authentication Agent configurations
- Supporting RSA SecurID users through troubleshooting specific access issues; performing routine system maintenance to assure user availability

Candidate Background and Experience

A Certified Administrator candidate should have a minimum of two years of professional experience in one or more of the following technical areas and understand how these technologies relate to and integrate with the RSA SecurID product. Elements of the CA exam touch upon each of these areas.

- Internet and Networking technologies
 - *DNS, TCP*
- Operating systems and user administration
 - *UNIX or Linux, Windows and Active Directory*
- Web Servers and Browsers
- LDAP Directory Servers

Examination Domains

The RSA SecurID Certified Administrator examination is comprised of three major Domains (subject areas). Each Domain is represented by a series of questions designed to evaluate competence and knowledge of elements relating to that domain. The following table describes the proportion of the examination that relates to each domain:

| Domain | % of Examination |
|--|-------------------------|
| 1.0: RSA SecurID Product Knowledge | 36 % |
| 2.0: Database Management & Configuration | 37 % |
| 3.0: Troubleshooting & Maintenance | 27 % |
| TOTAL | 100 % |

Domain 1.0: RSA SecurID Product Knowledge

The Certified Administrator must have a fundamental knowledge of RSA SecurID theory of operation, component architecture, and operation of various authenticators (token types). The CA is expected to be able to work with end users, educate them in the use of RSA SecurID authenticators for system logon, and have a working knowledge of how various components (Agents and Servers) work together to form a protective security perimeter.

Content Areas

- RSA Documentation
 - *Finding and accessing documentation resources*
- RSA Authentication Manager Operations
 - *Time synchronous authentication*
 - *New PIN, Next tokencode, and Disabled authenticator states*
 - *Contribution of authentication to overall system security*
 - *User, Group, Security Domain, Identity Source and Realm structures*
 - *Agent-to-Server communications and communication services and ports*
- Architecture
 - *Server availability and Replication*
 - *Authentication Agent configurations*
- Authenticators
 - *Types available in the RSA SecurID product family*
 - *Application and operation of each type*

Domain 1.0 Sample Items

The Clear PIN button on the Token menu for token serial number 10159732 is grayed out (inactive). The assigned user tells you that they have created a PIN of 4598. The tokencode displayed on the token is 559296. What should this user enter at a PASSCODE prompt?

- 4598
- 559296
- 4598559296
- 459810159732

'B' is the correct choice because, even though the user believes they have set a PIN, the Token menu indicates no PIN has been established (the Clear PIN button is active only when a PIN is set).

A small group of users in a field office want to share a single token for remote access. Why would you advise against this approach?

- A single Agent cannot be installed on a remote access server
- All the users would need to be present whenever the token is used
- It would be too difficult for all of the users to decide on a single PIN
- Access logs cannot tell with certainty exactly which user is logged in

'D' is the correct choice. 'A' and 'B' are not valid statements; 'C' may be true but this question highlights the significance that a token issued to a single user offers a level of assurance of identity and non-repudiation.

On-Demand tokencodes are characterized by

- a periodic tokencode change calculated with a time component
- a tokencode chosen by the user that replaces their PASSCODE
- a passcode that is used without a PIN if the user forgets their PIN
- a tokencode sent to a user by text message or via email when requested by a user

'D' is the correct choice. 'A' is not correct – it describes a typical time-based or time-synchronous token; 'B' describes a non-existent option; 'C' describes a function of an emergency access passcode ("Temporary Fixed Passcode").

Domain 2.0: Database Management and Configuration

The Certified Administrator must have a fundamental knowledge of database functions, administrative tasks, and administrative access for database management and configuration.

Content Areas

- Database Functions
 - *User management*
 - *Token management*
 - *Authentication Agent management*
 - *Group management*
 - *Security Domain management*
- Token/User assignments and token expiration/replacement
- Administrative tasks and granularity (permissions, scope and delegation)
- Trusted Realm authentication
- RSA Credential Manager operations

Domain 2.0 Sample Items

By default, how many bad authentication attempts will result in a user becoming locked out?

- 1
- 3
- 7
- 10

'C' is the correct choice.

Where is the value (above) configured?

- Token Policy menu screen
- Lockout Policy menu screen
- Authentication Agent menu screen
- Token Attribute Definition menu screen

'B' is the correct choice – Lockout policy sets the number of failed attempts for a given time period.

In what ways is a user allowed to authenticate through an Authentication Agent? (CHOOSE TWO)

- Adding both the user and Agent to a Security Domain
- Setting the Agent configuration to be “open to all users”
- Adding a user to a Group then activating the Group on the Agent
- Adding a user to a Group then adding the Group and Agent to a Realm
- Configuring the system settings to allow Authentication Agent “Auto-Registration”

'B' and 'C' are correct choices. 'A' is incorrect because this will not automatically enable the user on an Agent (unless the Agent is 'open to all users'); 'D' is incorrect because adding a Group and Agent to a Realm will not automatically activate the user on the Agent; 'E' is not valid because the 'Auto-Registration' function is not associated with user activations – it is designed to allow automatic registration of Agents in the database.

True or False: When configuring external LDAP Identity Sources, it is important not to map to overlapping Organizational Units (OUs).

- True
- False

This is true. Overlapping OUs may result in duplicate user identities drawn from an LDAP source and create Authentication Manager database conflicts.

Domain 3.0: Troubleshooting and Maintenance

The Certified Administrator must be able to troubleshoot specific end user issues relating to system logon, access, and use of the RSA SecurID tokens. The CA must also be able to carry out maintenance tasks relating to token records, token replacements, database backup and archiving, and report/audit management.

Content Areas

- Troubleshooting
 - *Interpretation of Error and Log messages at the Server, Agent, and Operating System levels*
- Token Issues
 - *New PIN mode*
 - *Next Tokencode mode*
 - *Re-synchronization*
- Report Management
- Primary and Replica server maintenance
- Database
 - *Archival Storage*
 - *Backups*
- Support for Offline users related to the RSA SecurID for Microsoft Windows Agent

Domain 3.0 Sample Items

If you receive an email message from an end user stating that the user has forgotten their PIN, it would be most appropriate to first

- select Disable Token from the Manage User screen
- verify the identity of the individual making the request
- check the Clear PIN checkbox in the Manage Token menu
- set the token to New PIN Mode from the Manage Token menu

'B' is the correct choice because before any other action is taken, the user's identity should be confirmed. It might be possible for an attacker to find or steal a token then, by setting a new PIN, the attacker could use the token as if they were a legitimate user.

If you view a message of "Unable to resolve principal by login ID and/or alias" in an Authentication Report or the Authentication Activity Monitor, this would indicate that

- The token assigned to the user is likely locked out or disabled.
- The user has not registered their token through the Credential Manager self-service console.
- The Node Secret at the Agent may have been corrupted and needs to be re-sent by the server.
- The username entered at the authentication prompt does not match any record in the database.

'D' is the correct choice. The "Unable to resolve..." message indicates that the entered userID does not exist in the Auth. Manager database. (the user may have mis-typed this information at the authentication prompt) 'A' is not correct because a locked user account or disabled token will result in a "Principal locked out" or "Token disabled" message, respectively. 'B' is irrelevant to the stated question. 'C' is not correct because a Node Secret issue will result in a "Node Secret Mismatch" message.

If an Identity Source is created and linked to Realm A why would these users not be listed in Realm B?

- All users must be part of the same Security Domain.
- An Identity Source can be associated with only one Realm.
- The tokens assigned to the users are likely locked out or disabled
- The administrator viewing users must have View permission in both Realms.

'B' is the correct choice – an Identity Source may only be linked with one Realm. Choices 'A', 'C', and 'D' are irrelevant to the stated question.

Examination Preparation

Product Training

Although RSA SecurID product training is not a strict requirement in preparation for the RSA SecurID Certified Administrator Certification Examination, it is highly recommended. Analysis of test results indicates that a majority of candidates who attend training prior to testing are more likely to successfully pass the exam on their first attempt.

RSA Security offers the following courses that relate to the RSA SecurID product and material covered on the CA exam:

- RSA SecurID Administration
 - *This course covers the fundamental concepts and operating principles of RSA SecurID technology; end-user organization and administration; system functions; end-user support. This course material most closely relates to the Certified Administrator certification.*
- RSA SecurID Installation and Configuration
 - *Assumes prerequisite experience of RSA SecurID Administration. This course covers installation and configuration of RSA SecurID system components; deployment planning; strategies for system redundancy and load-balancing. Although the material in this course more closely supports the Certified Systems Engineer certification, candidates for Certified Administrator may be interested in the more technical subject matter of this course for future use or career advancement.*

For full and detailed descriptions of RSA Security course offerings, visit: www.rsa.com (use the [Services > Training and Certification](#) links).

Product Experience

Many of the areas addressed by the CA exam will be familiar to the candidate who has worked with the RSA SecurID product through administrative operations involving RSA Authentication Manager, Authentication Agents, and other system components.

For example: Knowing what menu options appear in the Authentication Manager Security Console speaks to the candidate's overall product awareness; knowing what error and log messages are likely when authenticating through various Agents and under varying conditions speaks to the candidate's ability to assist with and troubleshoot end user problems.

The CA exam content areas cover a wide range of RSA SecurID product functions because a Certified Administrator may be called upon to assist with deployments, work closely with and educate end users, and maintain the day-to-day operation of RSA Authentication Manager across a variety of scenarios.

Study and Preparation Materials

As is common with other industry certification exams, RSA SecurID CA examination questions were constructed, reviewed, edited, and refined by groups of subject matter experts. A requirement of each test item is that it be referenced to a definitive source – document, publication, product menu selection, etc. Therefore, a finite set of preparation materials can be recommended for study and exam preparation. Although not all of the materials listed below are available in the public domain, the list does constitute a body of knowledge from which examination test items have been drawn.

- RSA Security Training Materials (Available only as part of an RSA Security training program)
 - *RSA SecurID Administration course Student Guide*
 - *RSA SecurID Installation and Configuration course Student Guide*
- RSA SecurID product documentation (Available with the product software)
 - *RSA Authentication Manager Administrator's Guide*
 - *RSA Authentication Manager Installation Guide*
 - *RSA Authentication Manager Planning Guide*
 - *RSA Authentication Agent Installation and Administration Guides*
- RSA Authentication Manager Help Menus and Help Screens (These Help functions are only available as part of installed and operating RSA Authentication Manager software.)

Examination Details

Testing Centers, Locations, and Registration

The RSA SecurID Certified Administrator examination is administered by the Pearson VUE organization – an internationally known examination provider. Examination centers are located worldwide. Visit the Pearson VUE web site (www.vue.com) and use the [Test Center Locator](#) to find a testing facility convenient to you.

You may also use the Pearson VUE site to create a personal login account and register for an exam. The RSA SecurID Certified Administrator exam code is 050-v71-CASECURID02.

Exam Questions

The RSA SecurID CA exam consists of 70 questions to be completed in 90 minutes. The exam consists of multiple-choice, multiple-response, or true/false type questions. The exam is computer-based and closed book – you may not utilize any printed material, personal computers, calculators, cell phones, etc. during the test.

The minimum passing score is 65%. Test results are calculated automatically at the conclusion of the test and testing center personnel can usually provide you with an authorized copy of your results before you leave the testing center.

Exam Costs

The fee for taking the exam is US\$ 150.00.

Language Availability

The RSA SecurID Certified Administrator exam is available in English.

What to expect at the Testing Center

You must present two forms of identification; one of which is a photo ID.

You will be required to electronically accept the terms of an RSA Certified Security Professional Certification Non-Disclosure and Program Agreement before beginning the examination.

Re-taking the Exam

There is no limit on the number of times that you can re-take the certification exam. However, to maintain integrity and confidentiality of the test items, 60 days is the required elapsed time before retaking the test a third time. Please note that you must pay the full exam fee each time that you retake the test.