Guide for Using RSA SecurID Tokens with CRYPTO-Server
# Table of Contents

**Using RSA SecurID DES Tokens with CRYPTO-Server**................................. 1
  Step 1: Export from the RSA Database ............................................................... 2
  Step 2: Import SecurID Tokens ............................................................................ 4
  Step 3: Recreate ACE Server Agent Hosts on the CRYPTO-Server ..................... 6
      Step 1: Generate a List of Agent Hosts on the RSA ACE Server ..................... 6
      Step 2: Create CRYPTO-Server NAS entries ............................................... 7
      Step 3: Reconfigure NAS devices for RADIUS authentication ....................... 8
  Manage SecurID Token Time Drift ....................................................................... 9
  SecurID Inner Window ..................................................................................... 9
  SecurID Outer Window ..................................................................................... 9
  Set the SecurID Inner/Outer Window .................................................................. 9
  SecurID Token Expiration Report ...................................................................... 10

**Using RSA SecurID AES Tokens with CRYPTO-Server**.............................. 11

**RSA to CRYPTOCard Migration FAQ** ........................................................... 13
License and Warranty Information

CRYPTOCARD Inc and its affiliates retain all ownership rights to the computer program described in this manual and other computer programs offered by the company (hereinafter called CRYPTOCard) and any documentation accompanying those programs. Use of CRYPTOCard software is governed by the license agreement accompanying your original media. CRYPTOCard software source code is a confidential trade secret of CRYPTOCard. You may not attempt to decipher, de-compile, develop, or otherwise reverse engineer CRYPTOCard software, or allow others to do so. Information needed to achieve interoperability with products from other manufacturers may be obtained from CRYPTOCard upon request.

This manual, as well as the software described in it, is furnished under license and may only be used or copied in accordance with the terms of such license. The material in this manual is furnished for information use only, is subject to change without notice, and should not be construed as a commitment by CRYPTOCard. CRYPTOCard assumes no liability for any errors or inaccuracies that may appear in this document.

Except as permitted by such license, no part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means electronic, mechanical, recording or otherwise, without the prior written consent of CRYPTOCard.

CRYPTOCARD reserves the right to make changes in design or to make changes or improvements to these products without incurring the obligation to apply such changes or improvements to products previously manufactured. The foregoing is in lieu of all other warranties expressed or implied by any applicable laws. CRYPTOCard does not assume or authorize, nor has it authorized any person to assume for it, any other obligation or liability in connection with the sale or service of these products. In no event shall CRYPTOCard or any of its agents be responsible for special, incidental, or consequential damages arising from the use of these products or arising from any breach of warranty, breach of contract, negligence, or any other legal theory. Such damages include, but are not limited to, loss of profits or revenue, loss of use of these products or any associated equipment, cost of capital, cost of any substitute equipment, facilities or services, downtime costs, or claims of customers of the Purchaser for such damages.

The Purchaser may have other rights under existing federal, state, or provincial laws in the USA, Canada, or other countries or jurisdictions, and where such laws prohibit any terms of this warranty, they are deemed null and void, but the remainder of the warranty shall remain in effect.

Customer Obligation

Shipping Damage: The Purchaser must examine the goods upon receipt and any visible damage should immediately be reported to the carrier so that a claim can be made. Purchasers should also notify CRYPTOCard of such damage. The customer should verify that the goods operate correctly and report any deficiencies to CRYPTOCard within 30 days of delivery. In all cases, the customer should notify CRYPTOCard prior to returning goods.

Goods returned under the terms of this warranty must be carefully packaged for shipment to avoid physical damage using materials and methods equal to or better than those with which the goods were originally shipped to the Purchaser. Charges for insurance and shipping to the repair facility are the responsibility of the Purchaser. CRYPTOCard will pay return charges for units repaired or replaced under the terms of this warranty.

Copyright

Copyright © 2006, CRYPTOCard Inc All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of CRYPTOCard Inc.

Trademarks

CRYPTOCARD, CRYPTO-Server, CRYPTO-Web, CRYPTO-Kit, CRYPTO-Logon, CRYPTO-VPN, are either registered trademarks or trademarks of CRYPTOCard Inc.

Java is a registered trademark of Sun Microsystems, Inc.; Microsoft Windows and Windows XP/2000/2003/NT are registered trademarks of Microsoft Corporation. SecurID is a registered trademark of RSA Security. All other trademarks, trade names, service marks, service names, product names, and images mentioned and/or used herein belong to their respective owners.

Publication History

<table>
<thead>
<tr>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 21, 2006</td>
<td>Initial release</td>
</tr>
</tbody>
</table>
Additional Information, Assistance, or Comments
CRYPTOCard’s technical support specialists can provide assistance when planning and implementing CRYPTOCard in your network. In addition to aiding in the selection of the appropriate authentication products, CRYPTOCard can suggest deployment procedures that provide a smooth, simple transition from existing access control systems and a satisfying experience for network users. We can also help you leverage your existing network equipment and systems to maximize your return on investment. This complimentary support service is available from your first evaluation system download.
CRYPTOCard works closely with channel partners to offer worldwide Technical Support services. If you purchased this product through a CRYPTOCard channel partner, please contact your reseller directly for support needs.
To contact CRYPTOCard directly:
   International Voice: +1-613-599-2441
   North America Toll Free: 1-800-307-7042
   support@cryptocard.com

Related Documentation
Refer to the Support & Downloads section of the CRYPTOCard website for additional documentation and interoperability guides:
Using RSA SecurID DES Tokens with CRYPTO-Server

CRYPTO-Server supports SecurID DES tokens. You need to import the token information into CRYPTO-Server so that it can recognize them. The import process consists of 3 steps:

- Step 1: Export from the RSA database
- Step 2: Import to the CRYPTOCard database
- Step 3: Recreate ACE Server Agent Hosts on the CRYPTO-Server

If you are using AES tokens refer to Using RSA SecurID AES Tokens with CRYPTO-Server on page 11.
Step 1: Export from the RSA Database

The first step involves exporting the token and user information from the RSA database. The CRYPTO-Server export wizard walks you through this process.

To export from the RSA database

1. On the ACE server, select Token|Export Tokens to export the list of tokens. The Export Tokens dialog window is displayed.
2. In the Export Token dialog window select the appropriate option:
   - Select the radio button that best describes the range of tokens to be exported
   - In the Seed Size drop down menu, select 64-Bit.
   - Select the option Export data in token .ASC format.
   - Click OK and select a file name and location for the file. This exports the user list to a file.

![Export Tokens Dialog](image-url)
3. On the ACE server, select User|List Users to export the list of users. The List Users window is displayed.

4. In the List Users window, select the appropriate option:
   - In the List to section, select File.
   - In the Report Type section, select the Standard Report.
   - In the List section, select All users.
   - Click OK and select a file name and location for the resulting file. The user file is exported in that location.
Step 2: Import SecurID Tokens

The second step involves importing the SecurID information into CRYPTO-Server. During the import process, CRYPTO-Server assigns SecurID tokens to users as follows:

- LDAP (AD/Open Directory/OpenLDAP) integrated with CRYPTO-Server: Tokens are assigned when the SecurID default login name matches the LDAP user logon name. If no match is found, the token is imported but not assigned to the user.
- CRYPTO-Server internal user database: Tokens are assigned using the SecurID default login name. If the name does not exist in the directory, it is created during import and the token is assigned.

The user PIN is not imported. CRYPTO-Server accepts the PIN provided with the SecurID passcode on the first logon attempt and the normal PIN management procedures apply.

Note: Be sure that you enter the PIN correctly. CRYPTO-Server will accept the PIN as it is entered, regardless of whether it is correct.

To import SecurID tokens

1. Click on the Import SecurID icon on the CRYPTO-Console toolbar. The Import SecurID Wizard is displayed. The Wizard will import your token records and users into CRYPTO-Server. Click on Next to continue.
2. Click on the Add file button to locate and add the .asc export file you want to import. Click Next to continue.

Note: Skip import RSA tokens and proceed to import RSA users is the option that provides a method to import users from an existing ACE server that do not have tokens or for whom tokens are not being imported. This option is not valid for CRYPTO-Server implementations with LDAP.
3. Locate and add the .rpt user export file to be imported by clicking the Browse button. Click Next to continue.

![Import Screen](image)

**Note:** For systems using LDAP integrated with CRYPTO-Server click Cancel. Tokens will be imported and matched to existing LDAP users.

After the import process is complete, all users and tokens are displayed in CRYPTO-Console. You can view all tokens through the Search tab, and assigned tokens can be found in the Token List for each user. If errors or exceptions occurred during the import, they are reported in the file: Warninglog<yymmddhhmmss>.log, where <yymmddhhmmss> is the file timestamp. The location of the file is:

- Windows C:\Program Files\CRYPTOCard\CRYPTO-Console
- Mac: Applications/CRYPTO-Console
- Linus: /usr/local/cryptocard/CRYPTO-Console
Step 3: Recreate ACE Server Agent Hosts on the CRYPTO-Server

Recreating the RSA agent host on the CRYPTO-Server involves 3 steps:

- Step 1: Generate a list of all agent hosts or clients configured on the RSA ACE server.
- Step 2: Add the RSA agent host/client entries to the RADIUS Protocol or CAP Protocol NAS list on the CRYPTO-Server.
- Step 3: Reconfigure hardware-based RSA agent systems to use the RADIUS authentication protocol.

Step 1: Generate a List of Agent Hosts on the RSA ACE Server

An RSA Agent host report must be generated so agent hosts/clients can be created on the CRYPTO-Server.

To generate the list of agent hosts on the RSA ACE Server

1. On the RSA ACE server, select Agent Host|List Agent Hosts. The List Agent Host window is displayed.
2. In the List Agent Host window select the appropriate option:
   - In the List to section, select the File radio button.
   - In the List section Select All agent hosts.
   - Click OK to generate the list.
Step 2: Create CRYPTO-Server NAS entries

To create CRYPTO-Server NAS entries

1. Open the CRYPTO-Console and connect to the CRYPTO-Server.
2. Select Server|Server configuration. The New Key-Value window is displayed.
3. For hardware-based RSA agents, right/control-click on the RADIUSProtocol Entity and select New Key-Value. The New Key-value window is displayed.

![New Key-value window](image)

4. In the Key field enter Key: NAS.x. Where x is a number for the server (e.g. NAS.3).
5. In the Value field enter <First IP>, <Last IP>, <Hostname>, <Shared Secret>, <Perform Reverse Lookup?>, <Authentication Protocols>. To specify a single IP address, use the same address for both <First IP> and <Last IP>.
6. Restart the CRYPTO-Protocol daemon (ccptcld)/service.
Step 3: Reconfigure NAS devices for RADIUS authentication

All hardware-based RSA agent systems must be reconfigured to use the RADIUS authentication protocol. In this section, we have used the CISCO VPN Concentrator as an example.

To reconfigure NAS devices for RADIUS authentication

1. Log on to the CISCO VPN Concentrator administrative tool.
2. Create an Authentication Server at the Configuration, Servers, Authentication or Configuration, User Management, and Groups level. A RADIUS configuration entry requires the following information:

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server type</td>
<td>Specifies the protocol to be used.</td>
</tr>
<tr>
<td>Authentication Server</td>
<td>Specifies the location of the CRYPTO-Server RADIUS Server, i.e. CRYPTO-Protocol Server.</td>
</tr>
<tr>
<td>Server Port</td>
<td>Specifies the RADIUS Port. The default is 1812.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Specifies the amount of time in seconds the VPN server will wait for the request.</td>
</tr>
<tr>
<td>Retries</td>
<td>Specifies the number of times the VPN server will try to contact the CRYPTO-Server RADIUS Server, i.e. CRYPTO-Protocol Server.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>testing123</td>
</tr>
</tbody>
</table>

3. Assign the authentication method to users or groups once the entry has been added.
Manage SecurID Token Time Drift

Time drifts in SecurID tokens can cause a failed login. CRYPTO-Server provides two settings for managing time drifts: the SecurID inner window and outer window setting.

SecurID Inner Window

The inner window setting determines the number of minutes, before and after the current time, during which a password will be considered valid. For example, if the value of this setting is 3, CRYPTO-Server will authenticate a user provided the password falls in the range of ±3 minutes of the current time.

SecurID Outer Window

This setting determines the number of minutes before and after the SecurID Inner Window during which a user may resynchronize their token during logon. If the password provided by the user falls inside this window, the user will be required to provide the next password in sequence before access will be granted.

Set the SecurID Inner/Outer Window

**To set the SecurID inner/outer window**

1. From the CRYPTO-Console menu bar, select Server|System Configuration and modify as follows.

<table>
<thead>
<tr>
<th>Entity</th>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token</td>
<td>SecurIDInnerWindow</td>
<td>An integer between 1-1440 minutes. The default is 10.</td>
</tr>
<tr>
<td>Token</td>
<td>SecurIDOuterWindow</td>
<td>An integer between 1-1440 minutes. The default is 30.</td>
</tr>
</tbody>
</table>

2. Click Apply to confirm to set the values.
SecurID Token Expiration Report

CRYPTO-Server generates an RSA token expiration validation report that is emailed to the System Administrator and lists all tokens due to expire in the following 30 days. CRYPTOCard recommends generating a token expiration report from the RSA ACE server when you migrate the tokens to CRYPTO-Server.

To create the expiration report

1. On the RSA ACE server, select Token|List Tokens. The List Tokens window is displayed.
2. In the List Tokens window select the appropriate option:
   - In the List to section, select File.
   - In the List section select A range of tokens by expiration.
   - Click OK.
3. Select the token expiration day range and click OK.
Using RSA SecurID AES Tokens with CRYPTO-Server

You cannot import AES tokens to the CRYPTO-Server database. Instead you need to configure the CRYPTO-Server to proxy the authentication requests from the AES based RSA tokens to the RSA ACE server.

To configure CRYPTO-Server to proxy the authentication requests

1. From CRYPTO-Console select the Server|System Configuration. The Configuration window is displayed.
2. In the Entity section of the Configuration window, right click on RadiusProtocol. From the popup menu, select New key-value. The New Key-value window is displayed.
3. In the Key field enter the following: SECURID.Proxy.0
4. In the Value field, enter the server information in the following format:
   SECURID,IpAddress_of_ACE_Server,ACE_server_Radius_Authentication_port,ACE_server_Radius_Accounting_port,shared_secret
   For example if the RSA server IP address is 192.168.10.1 and it uses the port 1645 for Radius authentication and 1646 for Radius accounting, the value would is:
   SECURID,192.168.10.1,1645,1646,shared secret
Ensure that the IP address of the RSA server does not already fall within any other NAS.x keys defined for the RadiusProtocol entity on our server or there will be an error in the RadiusProtocol.dbg log about overlapping entries.

5. In the New Key-value window, click on OK to save your information.
6. Restart the CRYPTO-Protocol service, and check the RadiusProtocol.dbg log to ensure there are no errors.

**Note:** When an RSA user tries to authenticate via CRYPTO-Server and the user is not found in our database, CRYPTO-Server will then try to proxy the request to the ACE server.
RSA to CRYPTOCard Migration FAQ

Does CRYPTOCard support RSA New PIN Mode?
Yes. Select the user’s token and the Usage tab. You can put a checkmark in Force Change PIN on next use.

How do you schedule an LDAP (AD/OpenLDAP/Open Directory) user import?
Unlike the RSA ACE server, the CRYPTO-Server does not schedule LDAP user imports. The CRYPTO-Server connects directly to LDAP and displays the users within the CRYPTO-Console. Tokens can then be assigned to each user. User Administration is performed via the Microsoft AD Users and Computers MMC Snap In, Workgroup Manager or the native LDAP management tool.

Does CRYPTO-Server support multiple Operator authenticator methods?
No. All CRYPTO-Server Operators must use a CRYPTOCard token.

Can I specify a minimum and maximum PIN length?
Yes. This can be set within the token properties under the PIN tab. The minimum PIN length can be set to 3, the maximum to 8.

How do I reset an out-of-sync RSA token?
Normally, an out-of-sync RSA token is due to server or client time and date issues. Check the date and time values on the server and the client. By default, the SecurIDInnerWindow value is 10 and the SecurIDOuterWindow value is 30. These settings can be modified to a maximum value of 1440.

How do I add a host agent/client?
CRYPTOCard refers to RSA host agents/clients as NAS clients. A NAS client can be added to the CRYPTO-Server by placing a NAS entry into the appropriate Protocol section of the Server configuration window.
Can I assign my CRYPTOCard/RSA users a static password?
Yes. A static password can be assigned to a user, but only if their token is deassigned or deactivated. This is useful if a token is lost or damaged.

Can I configure User Access Times on the CRYPTO-Server?
Yes. This is possible through the configuration of Access Control Lists (ACLs).

Can a CRYPTOCard user be assigned multiple tokens?
Yes. Note that challenge-response mode is not supported in this case.

Is the CRYPTO-Server RADIUS server RFC-compliant?
Yes. The CRYPTO-Server RADIUS server is RFC-compliant.

Can my RSA/CRYPTOCard users be assigned Administrative roles?
Yes. A user can be designated as an Operator of the CRYPTO-Server. You can customize operator permissions for each user or use a global template.

How do I generate a token expiration report on the CRYPTO-Server?
CRYPTOCard tokens do not expire but RSA tokens do expire. An email notification is sent to the CRYPTO-Server administrator if an RSA token or set of tokens is due to expire within 30 days. The settings for this feature can be changed through the CRYPTO-Console.

Does CRYPTO-Server support realms and sites?
Yes. Refer to the Administrator Guide for more information.

Does CRYPTO-Server support profiles?
Yes. Authorization properties can be set at the Group and User level. To set an authorization property, right/control-click on the object and select Set Authorization Properties.

Does CRYPTO-Server perform logging?
Yes. The CRYPTO-Server uses Log4j as its logging service. For more information, see http://logging.apache.org/log4j/docs/.