

SafeNet Authentication Service (SAS)

Migration Guide

CRYPTO-Server v6.4 to SAS

All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Part Number: 007-012397-002, Rev. F

Release Date: June 2016

Contents

Introduction	4
Third-Party Software Acknowledgement.....	4
Applicability	4
Migration Prerequisites and Limitations.....	4
Migration Process	5
Step 1: Enable Connection of the SAS Computer to the CRYPTO-Server Database.....	5
Step 2: Configure the ODB Driver on SAS.....	6
Step 3: Run Migration from the SAS Management Console.....	8
Support Contacts	9

Introduction

Third-Party Software Acknowledgement

Material from third-party software is used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Applicability

The information in this document applies to the following:

Supported CRYPTO-Server Version	6.4.x
Supported Database Servers	MySQL
Supported Operating Systems	Windows 2008 R2
Supported Architecture	64-bit
Network Port	<ul style="list-style-type: none">• TCP Port 1433 (MS SQL)• TCP Port 3306 (MySQL)

Migration Prerequisites and Limitations

Users, operators, tokens, and groups can be migrated from a CRYPTO-Server v6.4.x to the SafeNet Authentication Service (SAS) server.

- The migration tool must be run on a SAS server already configured with an active database (**SYSTEM** tab). A subscriber or service provider account must exist.
- The following must be installed on a separate server:
 - SAS Server v3.3 or higher
 - MS SQL 2008
 - ODBC driver, available from the following link: <http://dev.mysql.com/downloads/connector/odbc/5.1.html>
- Verify that the license installed on SAS supports an equal or greater number of tokens as the CRYPTO-Server v6.4.x licenses to ensure that all tokens are imported and activated for all users. If the number of tokens supported by the SAS SPE license is smaller, the import and activation will not take place for any user, operator, token, or group.
- The migration feature requires that an existing ODBC data source be configured on the SAS SPE server to connect to the corresponding CRYPTO-Server v6.4.x database (that is, a MySQL ODBC data source configured on the SAS SPE server to connect to a MySQL database on the 6.4.x CRYPTO-Server).
- The migration function will not import RADIUS attributes and clients. These must be manually created in the Microsoft RADIUS server (IAS/NPS) or FreeRADIUS server.

- CAP Protocol-enabled agents are not supported in SAS (CRYPTO-Logon, CRYPTO-Web, and certain Citrix Web Interface agents). They must be updated to SAS agents.
- CRYPTO-Server version v6.4.x software tokens are imported and marked as Legacy tokens (v6.4.x Legacy token) in the database. Users with CRYPTOCARD v6.4.x Software Tools installed can authenticate against CRYPTO-Server v6.4.x without changing their client-side software. This does not include CRYPTO-Server agents such as CRYPTO-Logon.
- CRYPTO-Server v6.4.x software tokens cannot be reissued. The client-side CRYPTOCARD Software Tools must be upgraded to the SAS Software Tools, and an MP software token must be issued to the user.
- If a duplicate serial number is detected during migration, the migration utility will change the serial number and then assign the token to the user. The change in the serial number does not affect a migrated user's ability to authenticate against SAS.
- If the SAS server is configured to use LDAP, tokens are assigned and activated when the migration utility finds a match between the CRYPTOCARD server token name and the LDAP user logon name. If a match is not found, the token is imported but placed into inventory.
- Static password-enabled users in CRYPTO-Server v6.4.x will not be migrated to SAS SPE.
- KT-1 tokens with serial number 3120xxxxx or earlier, and RB-1 tokens with serial number 2020xxxxx or earlier, will be migrated into SAS SPE but it might not be possible to reinitialize these tokens. These older tokens might need to be replaced with more recent models due to firmware compatibility issues.
- SAS does not support **Verify Signature** for tokens that are initialized with token option **Mark-1**. If **Verify Signature** is used, tokens should be re-initialized to **Mark-2** with CryptoServer 6.4 prior to migration to SAS or replaced with new tokens.
- Serial initializers are not supported in SAS SPE. Serial token initializers must be upgraded to USB token initializers.

Migration Process

The migration process consists of the following steps:

- Step 1: Enable Connection of the SAS Computer to the CRYPTO-Server Database – see below
- Step 2: Configure the ODBC Driver on SAS – see page 6
- Step 3: Run Migration from the SAS Management Console – see page 8

Step 1: Enable Connection of the SAS Computer to the CRYPTO-Server Database

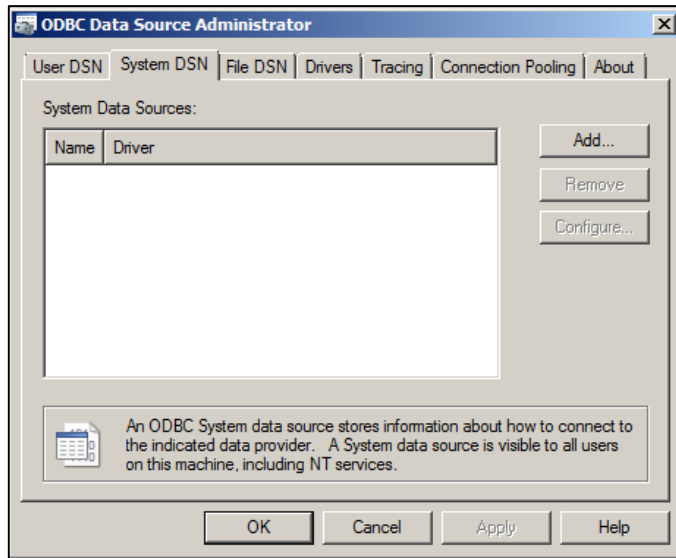
On the CRYPTO-Server computer, a **grant** statement must be added to allow a connection from SAS. Add one of the following statements to the MySQL Server used by CRYPTO-Server v6.4.x:

- Grant all privileges on *.* to root@'IP_Address_of_SAS_Server' identified by 'password'
- Grant all privileges on *.* to root@'Hostname_of_SAS_Server' identified by 'password'
- Flush privileges

Step 2: Configure the ODB Driver on SAS

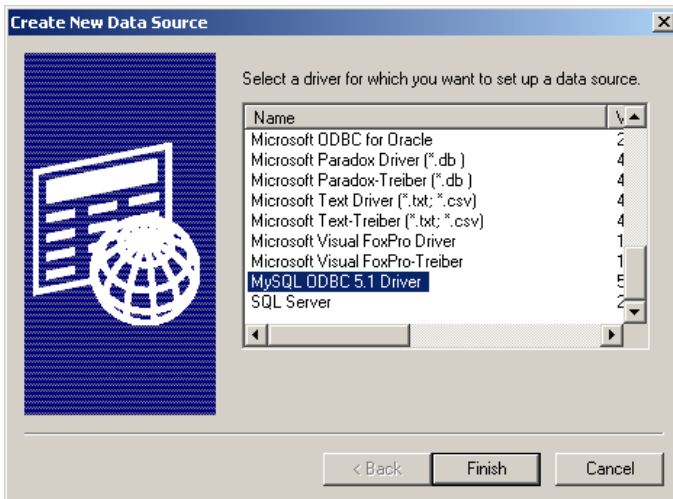
The ODBC driver on the SAS computer must be configured to connect to the CRYPTO-Server v6.x database.

1. Install the MySQL ODBC driver.
2. Select **Start > Programs > Administrative Tools**.
3. Right-click on **Database Sources (ODBC)** and select **Run as administrator**.
4. On the **ODBC Data Source Administrator** window, click the **System DSN** tab.



(The screen image above is from Microsoft™ software. Trademarks are the property of their respective owners.)

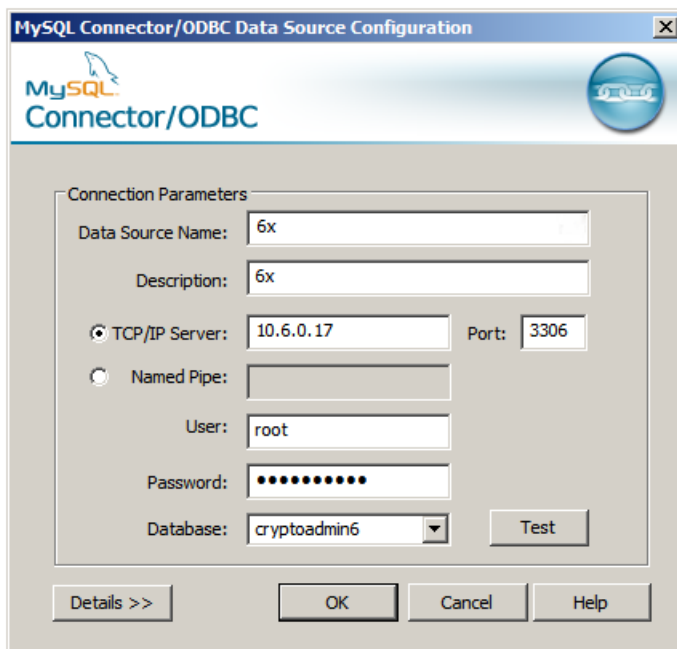
5. On the **System DSN** page, click **Add**.
6. On the **Create New Data Source** window, select **MySQL ODBC 5.1 Driver**, and then click **Finish**.



(The screen image above is from Microsoft™ software. Trademarks are the property of their respective owners.)

7. On the **MySQL Connector/ODBC Data Source Configuration** window, complete the fields as follows:

Data Source Name	Enter a name for the CRYPTO-Server.
Description	Enter a description of the CRYPTO-Server.
TCP/IP Server	Select this option and type the TCP/IP server address.
Port	Enter the TCP/IP server port number.
Named Pipe	Do not select this option.
User	Enter the MySQL user name.
Password	Enter the MySQL password.
Database	Enter the CRYTO-Server database.



(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)

8. Click **OK**.

Step 3: Run Migration from the SAS Management Console

1. Log in to the SAS Management Console.
2. Select **VIRTUAL SERVERS > COMMS > Authentication Processing**.

Authentication Processing

Use these settings to configure Context Pre-auth rules, download or generate authentication, remote service and LDAP Sync Agent encryption keys.

Task	Description
Authentication Agent Settings	Generate encryption keys required for remote authentication agents.
LDAP Sync Agent Settings	Confirm or clear LDAP Sync Agent settings.
ICE Activation	Activate ICE License
LDAP Sync Agent Hosts	List of all remote host names/IPs of servers syncing to SafeNet Authentication Service
Agent SSL Certificate	Agent SSL certificate for Domain Validation Agent
Logging Agent	List of all logging Agents
Migrate SafeNet Authentication Servers	Settings in this section will allow the server to migrate users and tokens from other SafeNet Authentication Servers.

Migrate SafeNet Authentication Servers:

Migrate Cancel Import Log

Server: CryptoServer 6.4

ODBC Name:

Oracle

User Name:

Password:

Add Parameter

3. Click **Migrate SafeNet Authentication Servers**.
4. In the **Server** list, select **CryptoServer 6.4**.
5. Complete the following fields:

ODBC Name	Enter the ODBC name.
User Name	Enter the user name.
Password	Enter the password.

6. Click **Migrate**. When the migration process is finished, a list of imported tokens will be displayed.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	