SafeNet Authentication Service

Migration Guide

CRYPTO-Server v6.4 to SAS

Document Information

Software Version	SAS 3.3.2
Document Part Number	007-012397-002, Rev. B
Release Date	September 2014

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

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	• 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

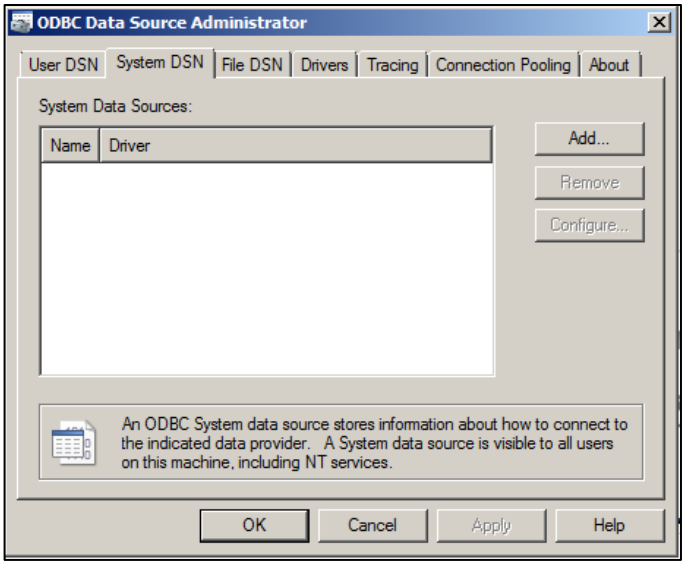
On the CRYPTO-Server computer, a **grant statement** must be added to allow a connection from SAS. Add one of the following statements to the MySQL Server used by CRYPTO-Server v6.4.x:

- 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 ODBC Driver on SAS

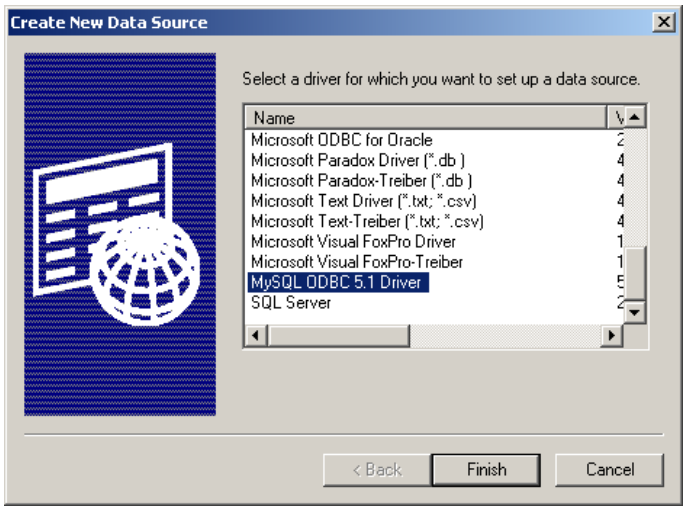
The ODBC driver on the SAS computer must be configured to connect to the CRYPTO-Server v6.x database.

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.)

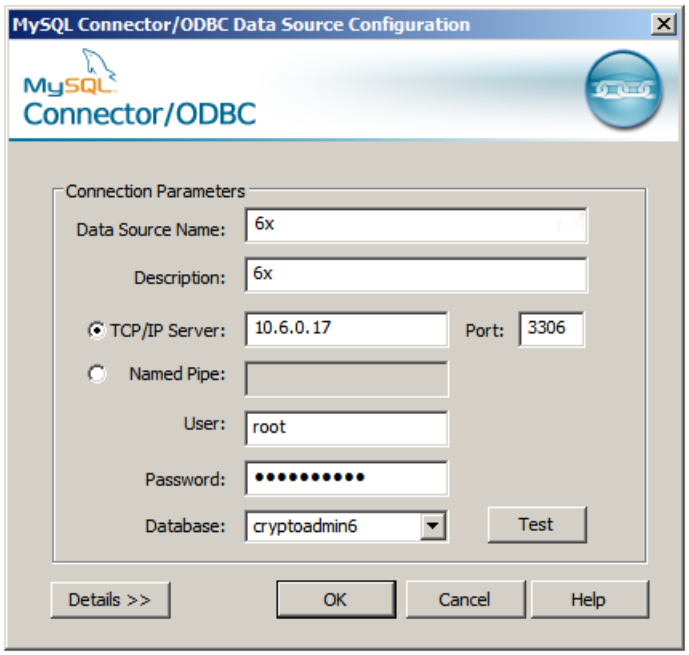
5. On the **System DSN** window, click **Add**.
6. On the **Create New Data Source** window, select **MySQL ODBC 5.1 Driver**, and then click **Finish**.



(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.

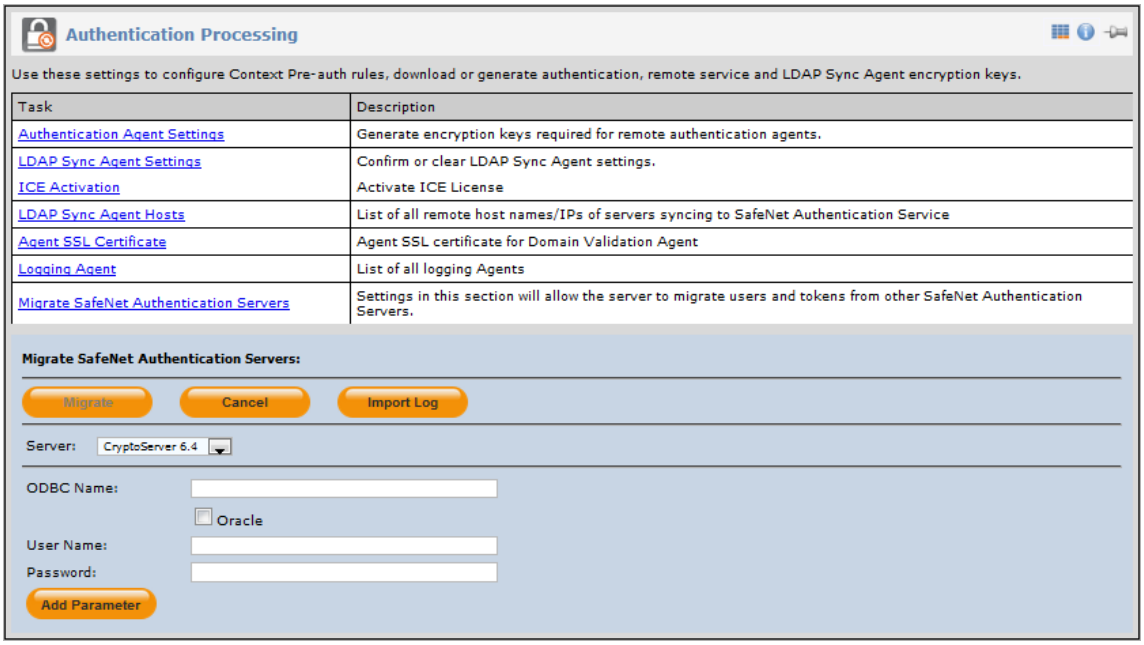


(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)

8. Click **OK**.

Step 3: Run Migration from the SAS Management Console

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



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 SafeNet Customer Support. SafeNet 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 SafeNet 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	SafeNet, Inc. 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 SafeNet Knowledge Base.	