SafeNet Authentication Service (SAS)

Migration Guide

SafeWord/SAMx

gemalto
security to be free

Document Part Number: 007-012524-001, Rev. F

Release Date: June 2016

Contents

Introduction

Applicability

The information in this document applies to the following:

- **SafeNet Authentication Service (SAS)**—A cloud authentication service of SafeNet, Inc.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—The software used to build a SafeNet authentication service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A term used to describe the implementation of SAS-SPE on-premises.

Purpose of this Guide

This guide describes migrating to SafeNet Authentication Service (SAS SPE and PCE Editions) from SafeNet Authentication Manager Express (SAMx), SafeWord 2008, SafeWord PremierAccess (for Solaris), and SafeWord RemoteAccess. It describes all of the processes required to do the following:

Run the Migration Compatibility Analysis Tool and generate the report you will use to determine whether migration is right for your organization.

- Understand and implement the recommendations for successful migration.
- Acquire a trial SafeNet Authentication Service account, and then configure, test, and validate it.
- Complete the transition to SafeNet Authentication Service.

Users are encouraged to read this guide in the order in which information is presented as successive sections often rely on information and concepts presented in prior sections.

Audience

This guide is intended for SAS Service Provider Administrators responsible for how managed authentication services are delivered to accounts, and for configuring the service to reflect the Service Provider's internal business processes, Service Level Agreements, and management hierarchy.

Terminology

The following terms are important to understanding the information presented in this guide:

- **Virtual Server**—This term refers to an individual account's virtual authentication server.
- **Subscriber**—When presented in lowercase ("subscriber"), the term applies to all accounts that you create and manage. When presented in proper case, the term ("Subscriber") refers to accounts that are not Service Providers.
- **Root Service Provider**—This term refers to the root organization that has installed and "owns" SAS, SAS-SPE, or SAS-PCE. Every other organization is either a Virtual Service Provider or Subscriber. A Root Service Provider has its own virtual server, and is able to create and manage Virtual Service Provider and Subscriber accounts it creates on SAS, SAS-SPE, or SAS-PCE.
- **Service Provider**—A Service Provider has its own virtual server, and is able to create and manage Virtual Service Provider and Subscriber accounts it creates on SAS, SAS-SPE, or SAS-PCE.
- **Virtual Service Providers**—A Virtual Service Provider has its own virtual server, and is able to create and manage Virtual Service Provider and Subscriber accounts it creates on SAS, SAS-SPE or SAS-PCE. Virtual Service Providers are Service Provider accounts which have a Service Provider as a parent.

Additional Reading

This guide is supplemented by a range of integration, branding, and subscriber guides. These include:

- Service Provider Quick Start Guide
- Operator Guide for Subscribers
- LDAP Synchronization Agent Guide
- Branding and Customization Guide
- Service Provider Billing and Reporting Reference Guide
- Using SafeNet Authentication Service to protect:
    - Network access through VPNs, Citrix, Terminal Server, and other similar remote access methods
    - Logon to Windows and Linux machines and networks
    - Microsoft web applications, such as OWA, SharePoint, and Remote Web Workplace
- Cloud applications, such as Salesforce.com, Google Apps, etc.
- Custom web applications

- Best Practices for migration users and companies to your service, including transparent, interruption-free migration:
    - From an in-house strong authentication solution
    - From static passwords
    - For mixed environments supporting B2B, B2C, and other combinations of users and organizations
    - Using and importing third-party authenticators
    - Extending services to complex organizations with:
        - Regional cost centers
        - Distributed management
        - Complex networks, including multiple LDAP directories and user sources

Understanding SafeNet Authentication Service (SAS, SPE, PCE)

SafeNet Authentication Service (SAS) is the cloud authentication service provided by SafeNet. SafeNet Authentication Service – Service Provider Edition (SAS-SPE) is the software used to build a SafeNet Authentication Service. SafeNet Authentication Service – Private Cloud Edition (SAS-PCE) is the term used to describe the implementation of SAS-SPE on-premises.

This guide provides end-to-end migration instructions for transferring from your organization's current SafeWord authentication solution to SafeNet Authentication Service. The guide includes overview migration information, instructions for using the SafeNet Cloud Migration Compatibility Analysis Tool to help determine if migration is right for your organization, instructions for using the Migration Utility to back up your existing data before migration, step-by-step procedures for a migrating with minimal interruption in service, and post-migration test and validation information.

You can migrate to SafeNet Authentication Service from any of the following SafeNet products:

- SafeNet Authentication Management Express (SAMx)
- SafeWord 2008
- SafeWord PremierAccess (for Solaris)
- SafeWord RemoteAccess

Sample migrations can be found later in this section.

SafeNet provides a Cloud Migration Compatibility Analysis Tool and a Migration Utility to use before migrating to SafeNet Authentication Service.

- The **Cloud Migration Compatibility Analysis Tool** gathers information about users and data that will not migrate to SafeNet Authentication Service. It provides a detailed report about potential migration issues, along with recommendations for resolving those issues before migration.
- The **Migration Utility** is used to automatically gather all the data required for migrating to SAS. This data is stored in your installation directory.

Understanding the Migration Process

The following is a summary of the migration process:

- Run the Migration Compatibility Analysis Tool to generate an analysis report of what will and what will not migrate to SafeNet Authentication Service.
- Review the SafeNet Authentication Service Migration Analysis Report and the recommendations for resolving components and data that are not migration compatible.
- Create a list of alternatives for migrating existing authentication services to SafeNet Authentication Service.
- Gather the data that is required for migration using the Migration Utility.
- Acquire a SafeNet Authentication Service trial account.
- Configure the SafeNet Authentication Service account, including operator roles, agents, auth nodes, token templates, groups, and containers (if necessary).
- Validate your import.
- Test authentication with the trial SafeNet Authentication Service account.
- Complete the transition to a live SafeNet Authentication Service production account.

Preparing for Migration

This section describes the best methods for preparing to migrate to SafeNet Authentication Services. It includes the following:

- Running the Cloud Migration Compatibility Analysis Tool
- Reviewing the analysis report
- Resolving migration incompatibilities
- Using the Migration Utility

Running the Cloud Migration Compatibility Analysis Tool

The Migration Compatibility Analysis Tool runs tests against your current installation, searching and reporting database and agent incompatibilities. The Cloud Migration Analysis Tool does not modify your current installation; it simply reads the existing log files and database to create the report about your current installation. The tool may be run multiple times.

This tool should be run on the latest general availability releases of SafeWord 2008, SAM Express, SafeWord PremierAccess, and SafeWord RemoteAccess. Upgrade to the latest general availability release before continuing.

If the tool is being used on a Solaris machine, you must untar it into a directory named **CloudMigrationTool** immediately under the SafeWord home directory. If the tool is being used on a Windows machine, you may unzip the tool into any directory. The following are examples of “home” directories:

- c:\Program Files (x86)\Aladdin\SafeWord
- c:\Program Files\SafeNet\SAMx
- /opt/SecureComputing/PremierAccess

To run the Cloud Migration Analysis Tool:

1. Open a command line shell and change to the **CloudMigrationTool** directory.
2. Run the batch file or shell script named **run**. The tool will output an HTML-formatted report file into the same directory.
3. The tool does not require command line arguments. The optional arguments are as follows:
    - To analyze archived log files going back for more than one month, use the **-am** command line argument, specifying the number of months to analyze. For example: **run -am 3**
    - To generate verbose output, use the **-v** command line argument. For example: **run -am 3 -v**
4. Locate the report file. It can be found in the **CloudMigrationTool** directory. The utility will prompt you to display the report. Click **Yes** to open the report automatically.

Understanding the Cloud Migration Analysis Tool Report

When you run the analysis tool, a report is created about your existing installation. This report identifies those components that will not migrate, along with recommended SAS equivalents where available. The following tests are run by the Cloud Migration Analysis Tool:

- **Archived Logs Test**—Identifies agents that may be in use and lists them with recommendations for migration to equivalent SAS agents.
- **Access Control List (ACL) Test**—Identifies existing login access control lists and web access control lists. No modified ACLs are migrated. If you did not modify the default login ACL or the default web ACL, ignore the ACL test warning. Otherwise, login ACLs and web ACLs will not migrate. If you are using web ACLs, you will need to use the corresponding SAS feature.
- **Fixed Password Conflict Test**—Identifies users who are assigned a fixed password along with other authenticators. Users who are assigned a fixed password and other authenticators will only have the fixed password or another authenticator; they will not have both.
- **Nested Administrator Groups Test**—Identifies any nested admin groups. SAS does not support nested groups, so nested admin groups will be migrated over but flattened. Flattening will preserve element information and membership in the group, but will remove parent-child relationships. This flattened group will be renamed by aggregating the group's existing name with that of all the ancestors.
- **Personalization Data Attributes Assigned to Roles Test**—Identifies any personalization data (PD) attributes that are assigned to roles. PD attributes assigned to roles will not migrate.
- **Users with More Than Two Aliases Test**—Identifies any users assigned more than two aliases. Only the first two aliases will migrate to SAS.
- **Users Assigned More Than Three PD Attributes Test**—Identifies any users assigned more than three PD attributes. Only the first three PD attributes assigned to users will be migrated to SAS.
- **Users Assigned Reserved PD Attributes Test**—Identifies any users assigned any PD attributes that are reserved by SAM Express (SafeWord). No PD attributes that are reserved by SAM Express (SafeWord) will migrate to SAS.
- **Privileged Users Test**—Identifies any users assigned administrator, local administrator, or help desk privileges. None of these privileges will migrate to SAS.

- Authenticators Assigned to More than One User Test—Identifies any authenticators assigned to more than one user. Authenticators can only be assigned to one user in SAS.
- Group Mismatch Test—Identifies any users assigned an authenticator belonging to a different group. A user and their assigned authenticator must belong to the same group in SAS.

What Is Migrated

The following items are automatically migrated to SAS:

- Users
- Authenticators
- Groups

What Is Not Migrated

The following items are not automatically migrated to SAS. You will need set up and configure these items manually in SAS. Recommended alternatives, where available, are listed below:

- SafeWord agents. Equivalent SAS agents are available for use. (See the Migration Compatibility Analysis Tool Report for details.)
- Login and web access control lists in the existing environments. ACLs are not migration-compatible. Only unmodified default Login ACLs and unmodified default Web ACLs will migrate successfully.
- Users assigned a fixed password and another authenticator. Only one will be accepted, not both.
- Nested administration groups. These will be migrated, but flattened, preserving element information and membership in the group, but removing parent-child relationships.
- Personalization data attributes assigned to roles.
- Users with more than two aliases. Only the first two aliases will migrate.
- Users with more than three personalization data attributes assigned. Only the first three attributes will migrate to SAS. You may wish to remove the additional attributes before migration.
- Reserved personalization data attributes assigned to a user. You may wish to remove reserved attributes before migration.
- Privileged Users. Privileges assigned to users do not migrate. You may wish to remove the privileges before migration.
- Authenticators assigned to more than one user. Authenticators can only be assigned to one user in SAS. You may optionally remove the authenticator from all but one user before migration.

Token Compatibility

The following SafeWord tokens are compatible with SafeNet Authentication Service:

- Fixed passwords
- Legacy tokens:
  - Silver 2000
  - Gold 3000
  - Platinum tokens
- eTokenPASS
  - Time synchronous
  - Event synchronous
- NG OTP
- Alpine Tokens
  - Time synchronous
  - Event synchronous
- SafeWord GOLD
- SafeNet eToken 3300
- SafeNet MobilePASS
  - Event synchronous
  - Time synchronous

Agent Compatibility

The table below provides the suggested SAS agents to use as replacements for the SAMx SafeNet agents that were used pre-migration:

SAMx SafeNet Agent	SAS Agent
SAMx IAS NPS Agent	SAS IAS NPS Agent
Citrix Agent for Web Interface	SAS Agent for Citrix Web Interface (Version 4.6 only. Later versions of Citrix Web Interface should use the SAS FreeRADIUS Agent.)
Citrix Access Gateway Agent	SAS FreeRADIUS Agent
SAMx Outlook Web Access Agent	SAS Agent for Exchange
SAMx SafeNet RADIUS Server	SAS FreeRADIUS Agent
SAMx Domain Login Agent	SAS Microsoft Windows Logon Agent

Universal Web Agent Web Login Server	SAS IIS Agent (Only supported on Windows operating systems)
SAMx Cloud Portal Agent	SAS Shibboleth Agent

Sample Migration Report Summary

The table below is a summary of the results from a sample Cloud Migration Analysis Tool test. It includes the tests that were run, the SafeWord components found that are not migration compatible, and SafeNet Authentication Service recommendations for resolving the compatibility issues. You may wish to set up a similar table based on your test results.

Test	SafeWord Component	SAS Recommendation
Archived Logs	SAMx RADIUS Server	Use the SAS FreeRADIUS Agent
Archived Logs	SAM Express SafeNet RADIUS Server	Use the SAS FreeRADIUS Agent
Archived Logs	SAM Express OWA Agent	Use the SAS Agent for Exchange
Archived Logs	Domain Login Agent	Use the SAS Microsoft Windows Login Agent
Access Control List	Login and Web ACLs	Unmodified default Login ACLs and default Web ACL will migrate successfully.
Fixed Password Conflicts	Users assigned a fixed password and another authenticator	Only one, either the fixed password or the other assigned authenticator will migrate. Assigned authenticators take priority over fixed passwords during migration.
Nested Administration Groups	Administrative groups within groups	Nested administration groups are flattened and then migrated. The flattened group is renamed by aggregating the group's existing name with that of all of its ancestor's names. You may optionally flatten nested groups pre-migration in SafeWord. Groups in the internal database can be flattened via the Admin Console.
Personalization Data (PD) Attributes Assigned to Roles	Roles assigned personalization data attributes	Move the attributes assigned to roles to the users.
Users with more than Two Aliases	Users with more than two aliases	Only the first two aliases will migrate to SafeNet Authentication Service. You may remove the extra aliases before migration, if desired.
Users Assigned more than Three Personalization Data Attributes	Users assigned more than three personalization data attributes	Only the first three personalization data attributes assigned to a user will migrate to SafeNet Authentication Service. You may optionally remove the extra attributes before migration.

Users Assigned Reserved PD Attributes	Users assigned reserved personalization data attributes	No reserved personalization data attributes will migrate to SafeNet Authentication Service. You may optionally remove these attributes before migration.
Privileged Users	Users assigned Administrator, Local Administrator, or Help Desk privileges	Privileges assigned to users will not migrate to SafeNet Authentication Service.
Authenticators Assigned to More than One User	Authenticators assigned to more than one user	SafeNet Authentication Service only allows an authenticator to be assigned to one user. You may remove the authenticator from all but one user before migration, if desired.
Group Mismatch	Users assigned an authenticator belonging to a different group.	In SafeNet Authentication Service, a user and their assigned authenticator must belong to the same group. Migration will automatically move the authenticator into the user's group.

Additional Migration Issues and Resolutions

The following are additional issues you may encounter in migration and suggested resolutions:

- **Authentication Broker**: If you are currently using the Authentication Broker with your SafeWord product to migrate users from another product into SafeWord, users who have not been migrated to SafeWord will not be migrated to SafeNet Authentication Service. You should complete the migration of users with the Authentication Broker before migrating to SafeNet Authentication Service.
- **IAS/NPS Agent**: This agent allows you to specify users in Active Directory for inclusion in or exclusion from SafeWord authentication. SafeNet Authentication Service does not support this feature.
- **Non-migration-compatible data**: Data that is not migration compatible will not be retrievable after migration to SafeNet Authentication Service. We recommend backing up this data before migration in case you need to refer to it later.
- **Fixed Passwords**: By default, user passwords in SafeWord are case insensitive and are stored in upper case. For authentication to succeed following migration to SafeNet Authentication Service, the passwords must be entered in all upper case or be reset. If the SafeWord user passwords are set as case-sensitive, they will continue to operate correctly following migration.

Backing up the Database with the Migration Utility

The Migration Utility is used to back up your existing database before migration. The utility must be run on the machine where the SafeWord core servers are installed.

In SafeWord 2008 and SAM Express, the Migration Utility is run by selecting the **Gather data for migration to SAS** option from the **Start** menu. In SafeWord PremierAccess and SafeWord Remote, the utility is run by copying and then extracting the **.tar** or **.zip** file to the directory level where the Servers and Lib files are located. You may request the file by contacting SafeNet Technical Support.

The Migration Utility creates three files in Active Directory environments and two in SafeWord environments:

- In Active Directory environments, it generates an **.ldif** backup file, a **.csv** (comma-separated value) file, and a **signers.cfg** file.
- On SafeWord databases, it creates an **.ldif** file and a **signers.cfg** file.

The **.ldif** file is the database file, the **signers.cfg** file contains the encryption keys, and the **.csv** file lists users who have tokens assigned to them. After running the Migration Utility, the files can be found in your installation directory in the folder named **GetMigrationData**.

To back up your database:

1. Run the Migration Utility.
   - **(On SafeWord 2008 and SAM Express)**: Click **Start > Programs > SafeNet > SAM Express > Gather data for migration to SaS**. A command prompt appears requesting an encryption key. If you wish to encrypt your data, skip to step 2. If you will not encrypt your data, click **Enter**, and then enter your login credentials.
   - **(On SafeWord PremierAccess and SafeWord RemoteAccess)**: Browse to the location where you untarred or unzipped the utility files. Run the script using the **GetMigrationData.sh** or **GetMigrationData.bat** command.
2. If you are encrypting data for migration, on the command line that displays, do the following:
   a. Type an 8-16 character encryption key, and then click **Enter**.

      It is important that you remember this encryption key, as you will be using it again when you import your data into your SAS account.

   b. Type your user name.

   c. Type your fixed password.

   When the backup is complete, a “Success” message appears. The backup files are located in your installation directory in a folder named **GetMigrationData**.
3. Press any key to continue.

Migrating to SafeNet Authentication Service

Once you have run the Migration Analysis Tool, reviewed its report and determined how to resolve issues with components of your existing system that are not migration compatible, acquired a trial SafeNet Authentication Service account, and backed up your existing database, you are ready to migrate to SafeNet Authentication Service. This section contains the relevant information for the following:

- Understanding the logic and attributes of migration
- Acquiring a SafeNet Authentication Service account
- Resolving incompatible component issues
- Configuring the SafeNet Authentication Service trial account
- Migrating data to SafeNet Authentication Service
- Validating the export to SAS and import from SafeWord
- Testing the new environment
- Troubleshooting
- Completing the switch to SafeNet Authentication Service
- Purchasing professional services

SafeWord Migration Logic Summary

The following is a summary of the logic and attributes that SafeNet Authentication Service uses to process a decrypted SafeWord LDIF file and optional supplementary user CSV file. The process results in the common data structure that is used for migration.

Base Logic

1. The user selects the **LDIF** file and the organization to which they wish to migrate. Optionally, they may also specify a supplementary **CSV** (comma-separated value) file with user information.
2. The **LDIF** file is scanned for domain names and for any signs that the file may not have been decrypted.
    - If the file has not been decrypted, migration fails.
    - Domain names are stored by type for later use.
3. The domain name list is parsed for data.
4. The extra user file gets parsed if it was specified.
5. **SccUsers** gets parsed.
6. When complete, the result is a common data structure, which is used for migration.

Acquiring a Trial SafeNet Authentication Service Account

SafeNet offers four different implementations of SafeNet Authentication Service:

- **Enterprise Cloud Service**—Fully automated strong authentication-as-a-service. No infrastructure required.
- **Service Provider Cloud Service**—True multi-tier, multi-tenant, cloud-based, two-factor authentication service for service providers to offer to their customers.
- **Private Cloud Edition (PCE)**—On-premises system providing secure and fully automated strong authentication solution for the enterprise.
- **Service Provider Edition (SPE)**—Fully automated, multi-tier, and multi-tenant strong authentication-as-a-service solution for service providers who require the service to be offered from their own location.

When you have determined which service solution and which product solution is right for your organization, request a free 30-day trial account by completing the request form, which is available here:

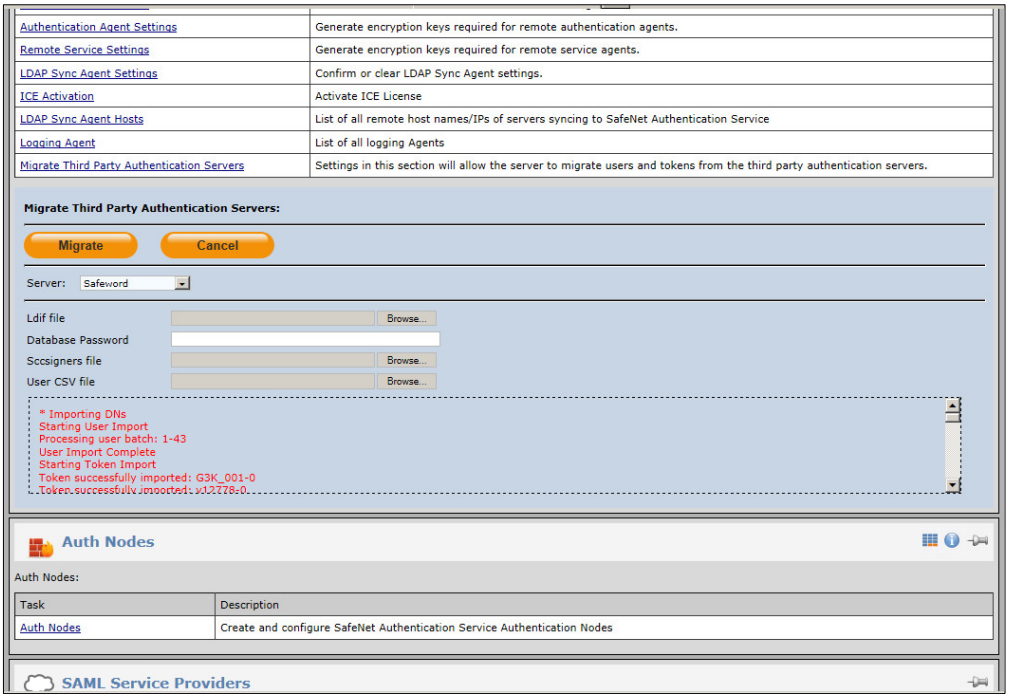
http://www2.safenet-inc.com/sas/free-trial.html

When you receive your trial account, configure it, including operator roles, agents, auth nodes, token templates, groups, and containers (if necessary). Refer to the SafeNet Authentication Service documentation for setup and configuration details.

Migrating to SafeNet Authentication Service

SafeNet recommends implementing a phased migration to SAS. This means that rather than moving all of your users, agents, and data over immediately, you will be using a “piloting method” to create and test a mock migration prior to making the actual migration. You will be migrating agents, and then users and tokens. Using the SafeNet Authentication Broker as an aid in the phased migration process will allow you to easily make the transition.

1. In the **Authentication Processing** pane, click the **Migrate Third Party Authentication Servers** option.

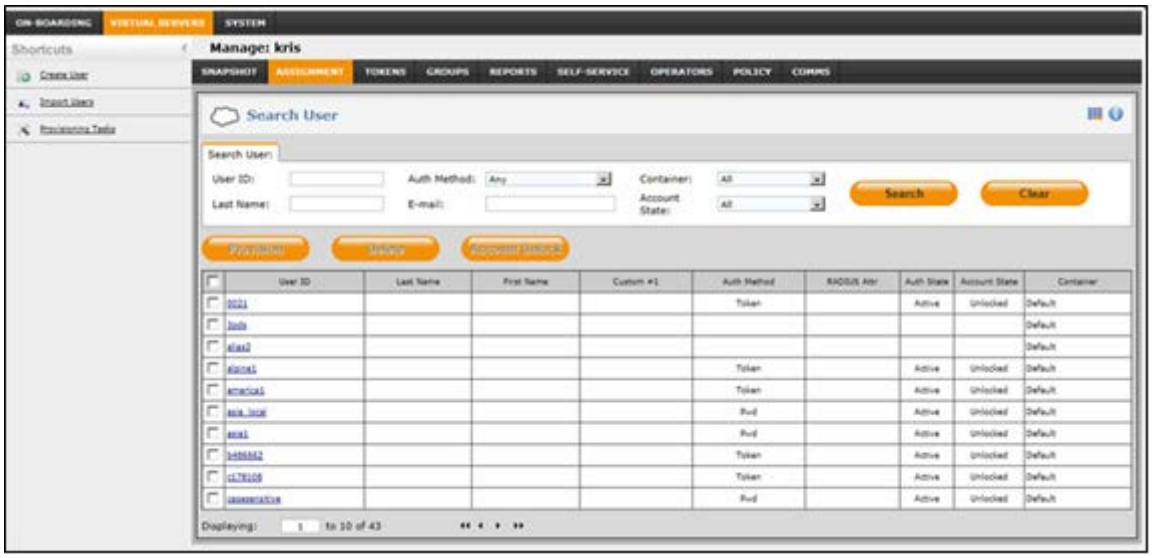


2. From the **Server** list, select **SafeWord**, and then do the following:
   - At the **Ldif file** field, click **Browse**, and then locate the **.ldif** file that was automatically generated using the Migration Utility.
   - If your backup file is encrypted with a password, enter that password in the **Database Password** field; otherwise, skip to the next step.
   - At the **Sccsigners file** field, click **Browse**, and then locate the **signers.cfg** file.
   - At the **User CSV file** field, click **Browse**, and then and locate the **.csv** file (if necessary).
   - Click **Migrate**. You are returned to the **COMMS** tab.
3. Scroll down to the **Authentication Processing** section. Your migration results appear in red text.

Validating your Migration

To validate your migration, confirm that the users migrated successfully:

1. Click the **VIRTUAL SERVERS** tab.
2. Click the **ASSIGNMENT** tab.
3. Click **Search**.
4. Confirm that your existing users and their authenticators were migrated successfully.



5. Select the **TOKENS** tab and click **Search**. Confirm that your existing authenticators were migrated successfully.

Setting Up SafeNet Authentication Service Agents

Since SafeWord agents do not migrate to SafeNet Authentication Service, before testing authentication, you must set up equivalent agents in SafeNet Authentication Service to perform the functions that were previously performed by your SafeWord agents. Refer back to the Migration Analysis Report to determine which agents you will need to install and set up in SafeNet Authentication Service. For agent setup and configuration information, refer to the SafeNet Authentication Service documentation.

Testing Authentication in SafeNet Authentication Service

To confirm that SafeNet Authentication Service authentication is functioning as expected, do the following:

- Select the desired users with assigned authenticators that you wish to test.
- Request that the users attempt to authenticate as they normally would, but to point to the server where the trial SafeNet Authentication Service account is installed instead of the server where SafeWord is installed.
- Confirm that these users are able to authenticate successfully.

Troubleshooting

If users are unable to authenticate successfully, do the following:

- Confirm your migration data to ensure users and their authenticators were migrated into SafeNet Authentication Service correctly.
- Request that users resynchronize their authenticators by attempting to authenticate twice using valid passcodes.
- Confirm that the SafeNet Authentication Service agents you are using for authentication are configured properly. Refer to the SafeNet Authentication Service documentation.
- If users are still unable to authenticate successfully, contact SafeNet Authentication Service Technical Support.

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.	