SafeNet Authentication Service (SAS)

Synchronization Agent Configuration Guide
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.

© 2017 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:** 007-012848-002, Rev. A

**Release Date:** June 2017
## Contents

### Preface

- Purpose of this Guide .......................................................... 4
- Applicability ........................................................................ 4
- Audience ............................................................................. 4
- Support Contacts .................................................................. 5

### 1 Overview

- Environment ......................................................................... 7
- Features ............................................................................. 8

### 2 Installation

- Installing the Synchronization Agent ..................................... 9
- Configuring SafeNet Authentication Service .......................... 9
- Upgrading the Synchronization Agent .................................... 14
  - Upgrading Multiple Redundant Agents .............................. 14
  - Synchronizing UPN for use as a SAML Return Attribute ...... 14

### 3 Configuration

- Configuring the Synchronization Agent for LDAP .................. 15
- Configuring the Synchronization Agent for SQL ................... 20
- Configuring Groups for Synchronization .............................. 25
- Configuring Active Directory Password Synchronization ...... 27
- Granting Agent Permissions in SAS .................................... 28
- Viewing Transaction and Last Sync Details ........................ 29
- Viewing the LDAP Schema .................................................. 30
- Configuring Aliases #3 and #4 ........................................... 31
  - Clone the Schema and Define the Aliases .......................... 31
  - Verify the Changes in SafeNet Authentication Services ...... 32
  - Conflict Resolution ........................................................... 33
- Configuring Other Synchronization Options ........................ 34
- Viewing SAS Server Details ............................................... 36
- Configuring Notification Settings ......................................... 36
- Browsing the User Source .................................................... 40
- Starting and Stopping the Synchronization Agent .................. 42
- Backing Up and Restoring the Synchronization Agent Configuration ...................................................... 42
  - Backing Up the Synchronization Agent Configuration ...... 42
  - Restoring the Synchronization Agent Configuration .......... 42
- Setting the Log Level ........................................................... 43
- Synchronization Agent High Availability Recommendations ........................................................................ 43
Preface

Purpose of this Guide

This document describes how to configure the SafeNet Authentication Service (SAS) Synchronization Agent.

Applicability

This version of the SAS Synchronization Agent Configuration Guide is relevant to SAS Synchronization Agent version 3.5.3 or later.

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—A cloud authentication service of Gemalto.
- **SAS - Service Provider Edition (SAS-SPE)**—The software used to build an authentication service.
- **SAS - Private Cloud Edition (SAS-PCE)**—The on-premises implementation of SAS-SPE.

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes SAS users and security officers, the key manager administrators, and network administrators. It is assumed that the users of this document are proficient with security concepts.

All products manufactured and distributed by Gemalto are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.
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.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Gemalto</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td>Phone</td>
<td>US</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td>Technical Support</td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td>Customer Portal</td>
<td>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.</td>
</tr>
</tbody>
</table>
The SafeNet Authentication Service (SAS) Synchronization Agent has been developed to simplify the task of user creation in SAS. Without the Synchronization Agent, the administrator must manually input user information via the web-based management interface. With the Synchronization Agent configured, LDAP or SQL user groups are monitored for membership changes, and user information updates are automatically made in SAS to reflect these changes.

1. The organization imports its encrypted Synchronization Agent Key File into the SAS Synchronization Agent, configures a connection to its LDAP Directory Server or SQL Server, and selects one or more LDAP or SQL user groups.
2. The SAS Synchronization Agent queries the LDAP Directory Server or SQL Server for all users within the selected groups.
3. Details of the users within the selected groups are transmitted and stored in the agent's user source.
4. When the SAS Synchronization Agent service is started and configured, the agent pushes all user and group information to SAS, which in turn, creates each user and group in the Virtual Server. The Synchronization Agent queries the LDAP Directory Server or SQL Server periodically. The default synchronization period is every 20 minutes. When a change is detected, the user or group is updated in the Virtual Server.
## Environment

<table>
<thead>
<tr>
<th>Environment</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Supported Platforms</strong></td>
<td>• Windows Server 2016&lt;br&gt;• Windows Server 2012 R2&lt;br&gt;• Windows Server 2012&lt;br&gt;• Windows Server 2008 R2 SP1 (64-bit)</td>
</tr>
<tr>
<td><strong>Additional Software Components</strong></td>
<td>• Windows .NET 4.6.2&lt;br&gt;Note: Install prior to installing the Sync Agent.&lt;br&gt;• MySQL .NET Connector (required for MySQL)&lt;br&gt;Available at <a href="https://downloads.mysql.com/archives/get/file/mysql-connector-net-6.4.4.msi">https://downloads.mysql.com/archives/get/file/mysql-connector-net-6.4.4.msi</a></td>
</tr>
<tr>
<td><strong>Network Ports</strong></td>
<td>• LDAP: TCP Port 389 - TCP Port 636 (optional)&lt;br&gt;• SAS: TCP Port 8456 (required)&lt;br&gt;• SQL: Appropriate TCP port</td>
</tr>
<tr>
<td><strong>LDAP Directory Server Access or SQL Access</strong></td>
<td>• Read-only</td>
</tr>
<tr>
<td><strong>Active Directory Server Access (for optional domain password synchronization)</strong></td>
<td>• Read-only</td>
</tr>
<tr>
<td><strong>Supported LDAP or SQL User Groups</strong></td>
<td>• Single or multiple LDAP or SQL group(s)</td>
</tr>
<tr>
<td><strong>Supported LDAP Directory Servers</strong></td>
<td>• Active Directory&lt;br&gt;• Novell eDirectory 8.x&lt;br&gt;• Sun One 5.x</td>
</tr>
<tr>
<td><strong>Supported SQL Servers</strong></td>
<td>• MS SQL&lt;br&gt;• MySQL (requires MySQL .NET Connector)&lt;br&gt;See “Additional Software Components” in this table.&lt;br&gt;• Oracle&lt;br&gt;• PostgreSQL</td>
</tr>
</tbody>
</table>
Features

Most organizations maintain information about their users in an SQL database or in an LDAP directory such as Active Directory. The purpose of the Synchronization Agent is to auto-populate SAS with users maintained in one of these user sources.

Key features of the Synchronization Agent include the following:

- Can be used directly with common user repositories
- Can accommodate custom schemas for most LDAP directory and SQL servers
- Does not write to the user source
- Does not require an administrator account to connect to the user source
- Can synchronize multiple user sources, such as multiple LDAP directory servers or multiple SQL servers
- Uses AES encryption between the Synchronization Agent and SafeNet Authentication Service
- Supports SSL between the Synchronization Agent and the LDAP directory server or SQL server
- Supports optional domain password synchronization from Active Directory user sources
Installing the Synchronization Agent

NOTE: If you attempt to install Synchronization Agent v3.5.3 on Windows Server 2012 R2 without .NET 4.6.2, the installer will prompt you to first install .NET 4.6.2 (which, in turn, requires Windows updates: KB2919355 and KB2919442).

NOTE: Synchronization Agent v3.5.3 does NOT support Windows Server 2008 SP2. Customers using Windows Server 2008 SP2 should use Synchronization Agent v3.5.2.

1. On the remote (vendor’s) computer, from an administrator account, run the following installation file:
   - SafeNet Authentication Service Synchronization Agent for SAS Cloud (64-bit)

2. On the Welcome window, click Next.
3. On the License Agreement window, select I accept the terms in the license agreement, and then click Next.

4. On the Customer Information window:
   a. Enter your User Name and Organization.
   b. Select one of the following to determine who can use the application:
      - Anyone who uses this computer (all users)
      - Only for me
   c. Click Next.
5. On the **Destination Folder** window, click the **Change** button to select a new install location, or click **Next** to accept the default location.

![Destination Folder](image)

6. On the **Ready to Install the Program** window, click **Install** to begin installation.

![Ready to Install the Program](image)

When the process has been completed, the **InstallShield Wizard Completed** window opens.
7. Click **Finish** to exit the installation wizard.

**Configuring SafeNet Authentication Service**

**NOTE:** In SAS Cloud, these settings are already configured by the SAS administrators (if needed, the default LDAP Sync Server Settings can be adjusted later). SAS Cloud users should skip to step 7.

1. Open the SAS Management Console.
2. Click **VIRTUAL SERVERS**.
3. Under **Managed Account List**, select the applicable server.
4. Click **COMMS > Communications > LDAP Sync Server Settings**.
   This is where the SAS server is configured to accept synchronized data from LDAP repositories. The host and port settings determine the communication between the LDAP directory server (for example, Active Directory) and the SafeNet Authentication Service.
5. If you are managing your own on-premises SAS server, select **Custom**, and then enter the following information:

| Sync Agent Primary Host | The details entered here are used to set the communication between the LDAP Directory Server (for example, Active Directory) and SAS. |
| Sync Agent Secondary Host | |
| Sync Agent Port (used only if you are using a non-default port; the default port is 8456) |

6. Click **Apply**.

7. On the **COMMS** tab of your Virtual Server, click **Authentication Processing > LDAP Sync Agent Settings**.

8. Click **Download** to download and save the **SASSyncConfigFile.bmc** key file. This file will be required during configuration of the Synchronization Agent.

9. Download and install the **SAS Synchronization Agent** installation package.
   - A link to the agent and other software can be found on the **Snapshot** tab in the **References** module.
   - Installer is available for 64-bit operating systems.

10. Prepare the following information, as it will be required for the Synchronization Agent configuration:
   - The IP address/host name and port number of your LDAP directory server or SQL server.
   - An account name and password that can be used by the Synchronization Agent to connect to the LDAP directory server or SQL server. The account password should be set to **never expire** to ensure that the Synchronization Agent is always able to connect to LDAP or SQL. The user account does not need write permissions because the Synchronization Agent only reads from the directory.
   - For LDAP environments, TCP Port 389 or 636 must be open between the Synchronization Agent and the LDAP directory server.
   - TCP Port 8456 must be open between the Synchronization Agent and SAS.
   - To use domain password synchronization, the computer running the Synchronization Agent must be part of that Active Directory domain. In addition, the computer must have the following Active Directory permissions:
     - Replication Directory Changes
     - Replication Directory Changes All
   - For configuration details, go to: [https://support.microsoft.com/en-us/kb/303972](https://support.microsoft.com/en-us/kb/303972).

11. Configure the SAS Synchronization Agent by following the instructions in the next chapter.
Upgrading the Synchronization Agent

NOTE: If you attempt to install Synchronization Agent v3.5.3 on Windows Server 2012 R2 without .NET 4.6.2, the installer will prompt you to first install .NET 4.6.2 (which, in turn, requires Windows updates: KB2919355 and KB2919442).

NOTE: Synchronization Agent v3.5.3 does NOT support Windows Server 2008 SP2. Customers using Windows Server 2008 SP2 should use Synchronization Agent v3.5.2.

To upgrade the Synchronization Agent, launch the provided installer file. It is not necessary to stop the service or uninstall the agent.

If the Synchronization Agent installer file detects a MySQL configuration without a .NET Connector, a warning is displayed, as shown in the accompanying figure.

Upgrading Multiple Redundant Agents

SAS supports syncing a Virtual Server through multiple agents that are configured with the same groups and attribute mappings. All agents must be upgraded at the same time. To upgrade, stop all agents except one. Upgrade this agent (which can still be running) and then start it, upgrade another agent and then start it, until all agents have been upgraded.

Synchronizing UPN for use as a SAML Return Attribute

The UPN (User Principal Name) attribute, shown in the accompanying figure, can be synchronized from Active Directory with Synchronization Agent version 3.5.1 (or later). This attribute can then be used as a return attribute for SAML authentication in SAS Cloud v3.5.1 (or later).

After the Synchronization Agent is upgraded to version 3.5.1 (or later) and the default AD schema is used, the UPN automatically synchronizes for all users on the first sync after the upgrade. The amount of time for this first synchronization to complete can be noticeable, depending on the number of users.

If you are using a custom Active Directory schema, and you want to synchronize the UPN attribute from Active Directory, you will need to manually add this attribute in the Synchronization Agent. (The custom schema configuration should match UPN mapping in the default Active Directory schema.)

Refer to “SAML Service Providers Module” in the Service Provider Administrator Guide for details about how to add an attribute in the SAS Management Console.
3 – Configuration

Configuring the Synchronization Agent for LDAP

An appropriate pre-configured LDAP schema has been provided for each of the supported LDAP Directory Servers. These default schemas cannot be changed but new schemas can be created if necessary. However, it is recommended that the default schemas be used if possible.

**NOTE:** For SQL environments, see “Configuring the Synchronization Agent for SQL” on page 20.

1. From an administrator account, launch the SAS Synchronization Agent by clicking Start > SafeNet > Agents > SAS Sync Agent. If necessary, right-click SAS Sync Agent and select Run as administrator.
3. Browse to the location of the SASSyncConfigFile.bmc key file saved in step 8 of page 13, and load the file. The Virtual Server Name field displays the name of your Virtual Server.
5. On the **User Source Type** window, select **LDAP**, and then click **Next**.

6. On the **LDAP Configuration** window, enter the following information, and then click **Next**:

<table>
<thead>
<tr>
<th><strong>Host name or IP</strong></th>
<th>Enter the host name or IP address of the LDAP directory server (i.e., the Active Directory, eDirectory, or Sun One Directory host name or IP address).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port</strong></td>
<td>Enter the port number of the LDAP directory server. Usually, TCP port 389 is used. If required, the Active Directory Global Catalog (TCP port 3268) may be used.</td>
</tr>
</tbody>
</table>
| **Use TLS for LDAP connection** | Select this option if you have a certificate installed on the server. If selected, change the **Port** value to 636.  
**Note:** Password synchronization is always encrypted, regardless of this setting (meaning, this setting only applies to other attributes). |
| **Number of Failover hosts** | Select the number of failover LDAP directory servers that are available for the Synchronization Agent to connect to in the event that the primary server is inaccessible. |
| **Connection Timeout (secs)** | Enter a specific timeout value when accessing LDAP. The default value is 60 seconds. An invalid value will display a message at the bottom of the window. |
**NOTE:** All servers must have access to the same Base DN.

7. On the **Select LDAP Schema** window, select the **LDAP Schema** from the list, and then click **Next**.

8. On the **LDAP Credentials** window, enter the following information, and then click **Next**:

| **User DN** | Enter the User DN created for the Synchronization Agent connection to the LDAP directory server. The User DN contains the user name (and location of the user within LDAP) that is used by the Synchronization Agent to connect to the LDAP directory server. For AD environments, specifying the UPN is sufficient; for example, ldapreadonly@my.domain. |
|**Base DN** | Select the highest level in the directory in which the Synchronization Agent is to begin its search for users.  
*For example:* In the sample shown, the Base DN is DC=number, DC=sys.  
Define the User DN as `<username>@number.sys`  
For non-Active Directory schemas, this value may be more complicated.  
*For example:* `uid=<username>, ou=Administrators, dc=aecl, dc=crypto, dc=prod` |
| **Append Base DN to User DN** | Select this option to add the Base DN to the information defined in User DN.  
*For example:* If the User DN is `uid=<username>` and the Base DN is `dc=aecl, dc=crypto, dc=prod`, the following would be submitted to the LDAP directory server when connecting:  
`uid=<username>, dc=aecl, dc=crypto, dc=prod` |
| **Password** | Enter the password created for the Synchronization Agent connection to the LDAP directory server. |
9. For **Active Directory** LDAP schemas, the following window is displayed. Select the **Enable password synchronization** check box to allow users to use their Active Directory password (domain password) to also access resources protected by SAS.

Click **Next**, and then skip to step 12.

For more details, please refer to "Configuring Active Directory Password Synchronization" on page 27.

10. For **non-Active Directory** LDAP schemas, the agent starts to search for all containers that have users, starting from the Base DN. To exclude or add containers, select **Override the list of containers found**, and then click **Next**.
11. The **Override Container List** window is displayed. You can add or remove the containers to be searched for users, and then click **Next** to continue.

![Override Container List Window]

12. On the **Configuration Complete** window, click **Finish**.

13. Select the **Status** tab.
   a. Under **Synchronization Details**, click **Details** to view the LDAP connection details.
   b. Click **OK** to close this window.

![User Source Connection Details Window]

**NOTE:** Password information is not displayed.

The Synchronization Agent is now configured for LDAP.

Repeat these steps for each Virtual Server that you wish to add.

The next step is to configure the LDAP group memberships that are used to determine which users are synchronized. See “Configuring Groups for Synchronization” on page 25.
Configuring the Synchronization Agent for SQL

For SQL environments, prepare the SQL schema before configuring the connection details.

**NOTE:** For LDAP environments, refer to “Configuring the Synchronization Agent for LDAP” on page 15.

1. From an administrator account, launch the Synchronization Agent by clicking **Start > SafeNet > Agents > SAS Sync Agent**. If necessary, right-click **SAS Sync Agent** and select **Run as administrator**.

   ![Start Menu](image)

   The SafeNet Authentication Service Sync Agent window displays, as shown in step 4 on page 15.

2. Under **SafeNet Authentication Server Virtual Server**, beside the **Virtual Server Name** field, click **Add**.

3. Browse to the location of the **SASSyncConfigFile.bmc** key file saved in step 8 on page 13, and load the file.
The **Virtual Server Name** field displays the name of your Virtual Server.

4. To configure an SQL schema for your SQL server environment, click the **Configuration** tab.
   a. Under **SQL Schema Configuration**, click **Configure**. The **SQL Schema Management** window is displayed, showing the first of five statements in the sample user source schema.
   b. To add a new schema, enter a name in the **Mapping Schema Name** field and then click **Add**.

The number of each SQL statement is displayed at the bottom left of each window:

1. Single User
2. User List
3. Groups
4. User's Groups
5. Group's Membership

NOTE: The Synchronization Agent uses null padding for binary values. On MySQL, use the BINARY data type instead of VARBINARY for your SQL queries.

c. In each statement's window, do the following:
   - Following the word SELECT in the SQL Statement box, replace each default field name with the corresponding field name used in your SQL environment. Ensure that all of the fields in the edited statement are listed in the same order as in the default statement.
   - Under Filter Columns, replace each default field name with the corresponding field name used in your SQL environment.

d. Click Apply to save your changes.

e. Click Next or Previous to move through the statements.

f. When the field names in all five SQL statements comply with the field names used in your SQL environment, click OK to save the configured SQL schema.

5. Click the Configuration tab.

a. Under User Source Configuration, click Configure.

b. On the User Source Type window, select SQL, and then click Next.
c. In the **Provider** field, select the appropriate database provider from the list, and then click **Next**.

![Select your database provider](image)

- **For PostgreSQL**: Enter the configuration settings required to connect to your PostgreSQL database.
- **For MySQL**: Enter the configuration settings required to connect to your MySQL database.
- **For MS SQL**: Enter the configuration settings required to connect to your MS SQL database.
- **For Oracle**: Enter the configuration settings required to connect to your Oracle database.

Depending on your SQL settings, you may be prompted to enter one or more failover hosts or servers for the agent to connect to in the event that the primary SQL server is inaccessible.
If you selected MySQL and the .NET Connector is not present, the system will prompt you to install it.

6. On the **Database Found** window, click **Next**.

7. On the **Custom SQL Mapping** window, select the SQL schema whose statements were defined previously (see step 4 on page 21) and then click **Next**.

8. On the **Configuration Complete** window, click **Finish** to save your changes.

9. Click the **Status** tab.
   a. Under **Synchronization Details**, click **Details** to see the SQL connection information.

   ![Database Found Window](image)

   ![Custom SQL Mapping Window](image)

   ![Configuration Complete Window](image)

   ![User Source Connection Details Window](image)

   **NOTE:** Password information is not displayed.

The SAS Synchronization Agent is now configured for SQL.

The next step is to configure the SQL group memberships that are used to determine which users are synchronized. See “Configuring Groups for Synchronization” on page 25.
Configuring Groups for Synchronization

The Sync Groups box lists all LDAP or SQL user groups configured for synchronization with SAS.

To view the users in the groups selected for synchronization, and ensure that the groups were configured correctly, see “Browsing the User Source” on page 40.

For LDAP, the Synchronization Agent will sync LDAP users within nested groups, where users may be members of a group that is a member of another group. Group Sync Options allow retention of group membership attributes for users (see “Configuring Other Synchronization Options” for more information).

SAS synchronizes users and groups that are visible in LDAP. SAS is not aware of trust relationships in Active Directory.

1. On the SAS Sync Agent Configuration tab, under Groups for Synchronization, click Configure.

2. On the Groups for Synchronization window, do the following:
   a. To search for an available group, enter the first letters of the required group’s name in the Available Groups field. (The results will not display until the Search button is used.)
   b. Click Search. When available groups are found, the results will be displayed in a window on the left.
   c. Use the arrow buttons to add or remove highlighted Available Groups to and from the Sync Groups list.
   d. When finished, click OK.
NOTE: Synchronization will take place only if the Sync Groups list contains at least one group. Keep in mind that groups will be synchronized even if they contain no users.

In the rare event that you wish to remove all users from SAS and, in essence, start from scratch, you can change your Synchronization Agent configuration to include one new empty group, remove the other groups, and then synchronize. SAS will be updated with just the one empty group. You can now reconfigure the Synchronization Agent to include the groups you would like, and on the next sync, SAS will be updated with those groups.

3. On the Warning message, click Yes to confirm your changes to the list of synchronized groups.

The groups selected for synchronization are displayed in the Status tab’s Sync Groups list.
Configuring Active Directory Password Synchronization

This functionality requires Synchronization Agent version 3.5.1 (or later) and SAS Cloud version 3.5.1 (or later). Prior to SAS v3.5.1, LDAP password validation and authentication was only available with SAS-PCE/SPE, with a direct LDAP connection. In SAS Cloud v3.5.1 (or later), AD password synchronization and authentication is available through the use of the same LDAP filtering attribute, located in the SAS Management Console, in COMMS > Authentication Processing > Pre-authentication Rules. Pre-authentication rules with AD can be used in SAS Cloud only when AD password synchronization is enabled. Refer to the Service Provider Administrator Guide for details.

Users can authenticate into SAS using their existing Active Directory (AD) password (their domain password), without the requirement of a token or other password to be provisioned. Operators manage this functionality by synchronizing the users’ AD passwords into SAS, which allows users to temporarily authenticate with their AD password until a token is activated by the user.

NOTE: Active Directory passwords are double-hashed and encrypted in all stages of transmission and storage between Active Directory, the Synchronization Agent, and in the SAS database.

NOTE: MSCHAPv2 authentication protocol is not supported for LDAP/AD passwords.

To use Active Directory passwords as assigned passwords or in pre-authentication rules, on the LDAP Schema window, select the Enable password synchronization option.

NOTE: To disable the use of AD passwords, simply de-select the Enable password synchronization check box. After successful synchronization, the AD passwords are removed from SAS, and they can no longer be used for
authentication into SAS—the passwords will still appear as assigned, but they can no longer be used for authentication.

NOTE: In SAS Cloud, the Accept LDAP/AD Password in ASSIGNMENT > Tokens > Assign must be selected for the user. Refer to the Service Provider Administrator Guide for details. This option will not be displayed in the SAS Management Console until the Enable password synchronization feature is enabled in the Synchronization Agent, and passwords are synced over to SAS.

Granting Agent Permissions in SAS

1. From the COMMS tab of your virtual server, click Authentication Processing > LDAP Sync Agent Hosts. The new Sync Agent Host is listed.

2. To enable sync permission for this host, click Change Permission.

3. Under Change Sync Agent Host Permission, select Allow, and then click Apply.

The Sync Agent Host is now shown as having sync permission.
Viewing Transaction and Last Sync Details

In the Synchronization Agent, click the Status tab.

Under Sync Details, the following information displays:

- **Last Sync Time**—The last synchronization attempt by the agent.
- **Last Scan Duration**—The amount of time required to scan all groups to retrieve user information.
- **Users in Cache**—The number of users held in the cache.
- **Users in Source**—The number of users in the source database.

Under Transaction Details, the following information displays:

- **ID**—The ID number of the current transaction record.
- **Status**—The status of the transaction.
- **Scan Started**—The start date and time of an LDAP Directory Server or SQL Server scan.
- **Scan Ended**—The end date and time of an LDAP Directory Server or SQL Server scan.
- **Sent to SAS**—The date and time the transaction was delivered to SAS.
- **Refresh**—Refreshes the display.
- **Second auto refresh**—How often a refresh is performed (seconds).
- **Save As**—Saves all transaction details to a file.
- **Clear**—Permanently deletes all transaction details from the display.
Viewing the LDAP Schema

In an LDAP directory server environment, you can view the LDAP schema settings.

**NOTE:** This is not relevant for SQL environments.

1. In the Synchronization Agent, click the **Configuration** tab.
2. Under **LDAP Schema Configuration**, click **Configure**.

   The **LDAP Schema Management** window is displayed with the mapping schema information.

   ![LDAP Schema Management Window](image)

   The **LDAP user source is Active Directory** check box allows the Synchronization Agent to determine if the custom schema is for an Active Directory (AD) implementation of LDAP. For these implementations only, the agent will not attempt to automatically determine the search scope by traversing the entire AD directory tree, but rather will always target all LDAP queries against the Base DN. This option is automatically enabled for the default Active Directory schema.

3. Click **Cancel** to close the window.

   **NOTE:** A pre-configured LDAP schema has been provided for each of the supported LDAP Directory Servers. The default LDAP schema is in a read-only state, with all editing capabilities disabled. It is recommended that the default schemas be used if possible. However, to allow for customized schemas, you can use the **Clone** button to create an identical copy of the currently selected schema, and make changes to the cloned schema. Note that a customized schema is not applied until the agent is reconfigured with the new schema.
Configuring Aliases #3 and #4

You can configure Alias #3 and Alias #4 to be synchronized from the LDAP by creating a customized LDAP schema.

NOTE: Alias #1 and Alias #2 can be configured on the SAS console by the operator only. Alias #3 and Alias #4 can be synchronized from the LDAP source only.

NOTE: You cannot change the default schema. But, you can modify a cloned schema.

Clone the Schema and Define the Aliases

1. Click **Start > All Programs > SafeNet > Agents > LDAP Sync Manager**. The SafeNet Authentication Service Sync Agent window displays.
2. Click the **Configuration** tab.
3. Click **Configure** in the LDAP Schema Configuration section. The LDAP Schema Management window displays.
4. Click **Clone** and type a schema name in the field provided.
5. Type the values for Alias #3 and Alias #4 in the fields provided.

NOTE: The values must exactly match those in the corresponding LDAP source. In addition, each user name and alias must be unique within a SAS Account. SAS will resolve conflicts according to rules described in the Conflict Resolution section.

6. Click **Apply** and then **OK** to save your changes.

7. Click the **Status** tab.

8. Click **Details** in the Synchronization Details section. The User Source Connection Details window displays.

9. Verify that the **Mapping** name exactly matches the **Schema Name** used in step 4.

10. Click **OK** to close the User Source Connection Details window.

11. Click **Stop** and then **Start** in the Service Status section. This sequence forces the LDAP Sync Agent to synchronize with the SAS server.

 Verify the Changes in SafeNet Authentication Services

From the SAS console:

1. Click **VIRTUAL SERVERS > ASSIGNMENT**.

2. Search for the User with Alias #3 and/or Alias #4.

3. Verify that the synchronized aliases (Alias #3 and/or Alias #4) display in the User Detail module.
Conflict Resolution

Alias #3 and Alias #4 may not be unique in the LDAP source. However, the SAS LDAP synchronization process must be completed even when conflicts exist. The Conflict Resolution tables that follow indicate how SAS resolves such conflicts during provisioning and synchronization.

Conflicts During Provisioning

<table>
<thead>
<tr>
<th>New user being added with conflicting …</th>
<th>Synced “User ID”</th>
<th>Local “User ID”</th>
<th>Synced Aliases</th>
<th>Local Alias</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local User</td>
<td>New local user not added (UI message displayed)</td>
<td>New local user not added (UI message displayed)</td>
<td>New local user not added (UI message displayed)</td>
<td>New local user not added (UI message displayed)</td>
</tr>
<tr>
<td>Local Alias</td>
<td>New local user not added (UI message displayed)</td>
<td>New local user not added (UI message displayed)</td>
<td>New local user not added (UI message displayed)</td>
<td>New local user not added (UI message displayed)</td>
</tr>
</tbody>
</table>

Conflicts During Synchronization

<table>
<thead>
<tr>
<th>New user being added with conflicting …</th>
<th>Synced “User ID”</th>
<th>Local “User ID”</th>
<th>Synced Aliases</th>
<th>Local Alias</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synced User</td>
<td>New synced user not added</td>
<td>New synced user is added, overwrites local user</td>
<td>New synced user is added, deletes previously synced alias</td>
<td>New synced user is added, deletes local alias</td>
</tr>
<tr>
<td>Synced Alias</td>
<td>New synced user IS added without the alias</td>
<td>New synced user IS added without the alias</td>
<td>New synced user IS added without the alias</td>
<td>New synced user IS added, deletes local alias</td>
</tr>
</tbody>
</table>

**NOTE:** In case of a conflicting alias, if you want to free-up the alias from one user so that it can be synced to another user, you must change the alias value instead of deleting it – changing the alias value will allow SAS to trigger a process to attempt to re-resolve the conflict (simple alias deletion will not).
Configuring Other Synchronization Options

1. In the Synchronization Agent, click the **Configuration** tab.
2. Under **Other Synchronization Options**, click **Configure**.

**Mobile Number Country Code**

The **Country code to prepend** field is used as follows:

- If the Cell Number’s leading digits are **00**, the agent will remove the leading **00**, regardless of the content of the **Country code to prepend** field.
  
  For example: **0041-77889991111** becomes **4177889991111**

- If the Cell Number’s leading digit is **0**, the agent will remove the **0** and prepend the country code to it if **Country code to prepend** contains a numeric value.
  
  For example: When using **31** as the prepend country code, **0778-89991111** becomes **3177889991111**

- If the Cell Number’s leading digit is between **1** and **9**, the agent will prepend the country code to it if **Country code to prepend** contains a numeric value.
  
  For example: When using **31** as the prepend country code, **778-89991111** becomes **3177889991111**

**NOTE:** The Synchronization Agent automatically removes all non-numeric characters, except for the + symbol, from the data in the schema’s Cell Number mapping.

**Scan Interval**

The **Scan Interval** determines how frequently the Synchronization Agent scans the LDAP directory server or SQL server for changes. The default interval is 20 minutes.
**Group Sync Options**

The **Group Sync Options** setting determines how groups are synchronized to SAS, and which group memberships users have in SAS. This setting does not affect which users are synchronized. With all options, all users in Sync Groups and any nested groups therein are synchronized.

In the **Groups to sync** field, select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>This sync option will not send any groups to SAS. Group designations will not be synchronized, and thus group memberships will not be maintained. Users from Sync Groups or any nested groups therein are synced to a single, inclusive SAS users list.</td>
</tr>
<tr>
<td>Filter groups only</td>
<td>This sync option will send only filter groups to SAS. Groups that contain users from any Sync Groups or any filtered groups therein are synchronized. The group memberships for all users are retained.</td>
</tr>
</tbody>
</table>
| Nested filter groups only | This sync option sends direct filter groups and all their nested groups to SAS.  
  - If User1 is a member of Group B which is nested in filter Group A, then Groups A and B will be synced to SAS.  
  - If User1 is also a member of Group C, which is not a filter group or nested into a filter group, then Group C will not be synced. |
| Groups with users only | This sync option builds a list of groups out of each user’s group membership. All groups that are found are sent to SAS. This can include direct filter groups and all their nested groups, as well as groups that are not nested below the configured filter groups. Groups that contain users from any Sync Groups or any nested groups therein are synchronized. The group memberships for all users are retained. |

**NOTE:** The Synchronization Agent will report an error on each scan if a previously synced group is detected as empty. This is logged by the Synchronization Agent. Synchronization resumes when the group appears populated again, or is removed from the Sync Groups list in the Synchronization Agent configuration. To delete a populated synchronization group and its users in SAS, the group must be removed from the Sync Groups list. Nested groups, which are not explicitly configured in Sync Groups, are synchronized also when empty.

**SafeNet Authentication Service Key Set**

The value displayed in the **SafeNet Authentication Service Key Set** field must be identical to the **Key Set** value displayed on your virtual server **Key Set** field under **COMMS > Authentication Processing > LDAP Sync Agent Settings**. See the screen image in step 7 of “Installing the Synchronization Agent” on page 9.
Viewing SAS Server Details

1. In the Synchronization Agent, click the **Configuration** tab.
2. Under **SafeNet Authentication Service Synchronization Server**, click **Details**.
   
   The **Server Details** window is displayed, showing the primary and secondary SAS server IP addresses and ports.

   ![Server Details Window]

   3. Click **OK** to close the window.

Configuring Notification Settings

The Synchronization Agent can be configured to send email alerts if it is unable to connect to SAS, or to the LDAP directory server or SQL server. An email alert can also be sent if an expected group is not found, or if synchronization fails. The text can be customized for each alert.

**NOTE:** Email alerts may be configured only if the service status is stopped.

1. In the Synchronization Agent, click the **Notification** tab.

2. Under **SMTP Configuration**, click **Configure**.
3. The **SMTP Configuration** window is displayed. These settings define the mail server (SMTP) used by the SAS server to send out notifications to the operator/administrator who manages the Virtual Server, and provides LDAP sync process notifications (for example, failed or succeeded).

<table>
<thead>
<tr>
<th><strong>From e-mail address</strong></th>
<th>Enter the email address from which notifications are sent.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hostname/IP Address</strong></td>
<td>Enter the IP address or host name of the SMTP server (mail server) used for sending out notifications.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Enter the port used by the specific mail server to send and receive emails.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>If credentials are required to log on to the SMTP server, enter the username and password of the account from which the notifications are sent.</td>
</tr>
</tbody>
</table>

4. Click **OK** to close the window.

5. Under **E-mail Test**, in the **Enter e-mail Address** field, enter a recipient email address, and then click **Test** to test the SMTP configuration.

6. To customize the email alerts that are sent, under **E-mail Message Templates**, click **Customize**.
7. On the **Email Templates** window, enter the following information, and then click **OK**:

<table>
<thead>
<tr>
<th>Message</th>
<th>Select the message type:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• LDAP Connection Issues</td>
</tr>
<tr>
<td></td>
<td>• User Source Server Connection Issues</td>
</tr>
<tr>
<td></td>
<td>• Sync Server Connection Issues</td>
</tr>
<tr>
<td></td>
<td>• Missing Group</td>
</tr>
<tr>
<td></td>
<td>• Active Directory Replication Issues</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subject</th>
<th>Modify the <strong>Subject</strong> and <strong>Body</strong> content as required.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Body</td>
<td></td>
</tr>
</tbody>
</table>

8. Under **Event Recipient Lists**, click **Add** to add an email address to which alerts are sent.
9. On the **Mailing List** window, enter the following information:

<table>
<thead>
<tr>
<th>List Name</th>
<th>Enter a name for the email list.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recipient E-mail</strong></td>
<td>For each address to be added to the <strong>Recipient Email List</strong>, enter a valid email address into the <strong>Recipient Email</strong> field, and then click <strong>Add</strong>.</td>
</tr>
<tr>
<td><strong>Recipient Email List</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Events</strong></td>
<td>Select the appropriate events for which the recipient will receive an alert:</td>
</tr>
<tr>
<td></td>
<td>• Sync Server Connection Issues</td>
</tr>
<tr>
<td></td>
<td>• User Source Connection Issues</td>
</tr>
<tr>
<td></td>
<td>• Missing Group</td>
</tr>
</tbody>
</table>

10. Click **OK** to close the window. The **List Name** displays in the **Event Recipient Lists** box.
Browsing the User Source

When a connection has been established between the Synchronization Agent and the organization’s LDAP directory server or SQL server, the Synchronization Agent queries the server for all users within the user groups that were selected for synchronization. The user information is transmitted and stored in the Synchronization Agent’s user source.

The following may be viewed in the Synchronization Agent’s user source:

- The list of groups selected for synchronization
- The details of the users stored in the user source (if available):
  - User name
  - First name
  - Last name
  - Email
  - Phone number
  - Cell number
  - List of LDAP or SQL user groups in which the user is a member

**To browse the user source:**

1. In the Synchronization Agent, click the **Browse User Source** tab.
2. Click the **Users** tab and then click **Search**. A list of the first 500 users is displayed.
3. To search the entire user source for a specific user, enter the first few letters of the required user name in the **User Name** box, and then click **Search**.
4. In the **User Name** list, select the required user. The details of the selected user are displayed in the **Details** box.

5. To view a list of groups, click the **Groups** tab, and then click **Search**. A list of the first 500 groups is displayed.

![Screenshot of the SafeNet Authentication Service interface](image)

6. To search the entire user source for a specific group, enter the first letters of the required group’s name in the **Group Name** box and then click **Search**.

7. In the **Group Name** list, click the required group. The names of the users included in the selected group are displayed in the **Details** area.
Starting and Stopping the Synchronization Agent

1. In the Synchronization Agent, click the **Status** tab.
2. Under **Service Status**, click **Start** or **Stop**.

![Service Status](image)

Backing Up and Restoring the Synchronization Agent Configuration

You can back up the Synchronization Agent configurations of all your virtual servers, as well as restore any backed-up configuration.

**Backing Up the Synchronization Agent Configuration**

1. In the **SAS Sync Agent** menu, click **File > Backup All Configurations**.

![SAS Sync Agent](image)

2. Select the location and name of the backup file.

**Restoring the Synchronization Agent Configuration**

1. In the SAS Sync Agent menu, click **File > Restore Configurations**.
2. Select the location and name of the appropriate backup file.
   - If multiple virtual servers have been configured, a box is displayed listing all of them.
3. Select the virtual server(s) to be restored.
3 – Configuration

Setting the Log Level

1. In the SAS Sync Agent menu, click **File > Log Level**.
2. Adjust the log level for more or less logging. The default log level is **Info**.

![Safenet Authentication Service Sync Agent](image)

Synchronization Agent High Availability Recommendations

A high availability configuration with multiple synchronization agents ensures there is no single point of failure. Configuration should include:

- Identically configured sync agents with the same group configuration and schema.
- The content of the LDAP server(s) the sync agents are pointed to is identical.

**NOTE:** If agent configurations are not synchronized or the content of the LDAP directory servers differs, the synchronization agents will work against each other, as all agents are active. Active/Passive configuration is not available.