SafeNet Synchronization Agent

CUSTOMER RELEASE NOTES

Version: 3.8.6

Issue Date: 12 January 2023

Document Number: 007-013466-011 Rev. C

Contents

Product Description

The SafeNet Synchronization Agent enables you to sync users in LDAP or SQL user groups to a SafeNet Trusted Access (STA) user store. Without the SafeNet Synchronization Agent, the administrator must manually input user information via the web-based management interface. With the SafeNet Synchronization Agent configured, LDAP or SQL user groups are monitored for membership changes and user information updates are automatically made in STA to reflect these changes.

For a list of existing issues as of the latest release, refer to "Known Issues" on page 12.

General Availability Release - 01/12/2023

This general availability release introduces SafeNet Synchronization Agent version 3.8.6 and resolves the issues listed below:

Resolved Issues

Issue	Synopsis
SAS-52749	If password sync is disabled in the Sync Agent, the previously synced password is correctly removed from STA/SAS.
SAS-51256	Updated the default location of logs and name format.
SAS-24871	Placed horizontal scroll bars in the list boxes under the **Status** and **Configuration** tabs for enhanced visibility of large group names.

Service Pack Release - 03/08/2022

This service pack release of SafeNet Synchronization Agent version 3.8.5 introduces the following feature and resolves the issues listed below:

- **Support for Windows Server 2022**

Resolved Issues

Issue	Synopsis
SAS-48511	Enhanced logging for mass deletion prevention.
SAS-47931 SAS-44775	Stability improvements for password synchronization.

Service Pack Release - 07/15/2021

This service pack release of SafeNet Synchronization Agent version 3.8.4 introduces the following features and resolves the issue listed below:

- **Thales Branding**: An updated look and feel for the installation procedure.
- **User Deletion Safeguard**: Allows you to ensure that an anomalously large number of users are not deleted in error. You can block synchronization from proceeding if more than a configurable number of users are queued for deletion.
- **ObjectSid Support**: SafeNet Synchronization Agent will now be able to sync the objectSid from the Active Directory to STA in its string representation . This enables integrations that require this attribute to identify users and validate their permissions.
- **Improved SafeNet Synchronization Agent Logging**: More streamlined logging capabilities.

For more details, please refer to *SafeNet Synchronization Configuration Guide*.

Resolved Issue

Issue	Synopsis
SAS-43103	Groups with users only combined with group nesting synchronizes correctly.

Service Pack Release - 04/17/2020

This service pack release of SafeNet Synchronization Agent version 3.8.3 introduces the following features and resolves the issues listed below:

- **Compatibility with secure default settings enforced by Microsoft:** With this security advisory, Domain Controllers enforce LDAP channel binding and signing. To use these secure default settings, select the Use TLS for LDAP connection setting (and port 636). See Security Advisory - ADV190023.
- **Support for Windows Server 2019 - Desktop Experience (GUI):** Requires .NET 4.8.

> **Duplicate users:** Added the **Consolidate duplicate users** option to the **Other Synchronization Options**.

Issue	Synopsis
SAS-38233	Renaming ATMFD.DLL (Microsoft security bulletin ms15-077) has no impact on SafeNet Synchronization Agent.
SAS-35187	Added debug logging for timeouts that are waiting for a server reply.
SAS-34513	Failover hosts can be configured.
SAS-34251	Removed the info logs for users in multiple groups to reduce the log size.
SAS-30895	Updated the list of additional software components to include the following: • Visual C++ Redistributable Packages for Visual Studio 2013 https://www.microsoft.com/en-ca/download/details.aspx?id=40784 (version 12.0.30501 or later) • Visual C++ Redistributable for Visual Studio 2015 https://www.microsoft.com/en-ca/download/details.aspx?id=48145 (version 14.0.230264 or later)

Service Pack Release - 12/20/2019

This release of SafeNet Synchronization Agent version 3.8.2 introduces support for the FIPS mode within the operating system.

Service Pack Release - 10/24/2019

This service pack release of SafeNet Synchronization Agent version 3.8.2 resolves the issue listed below:

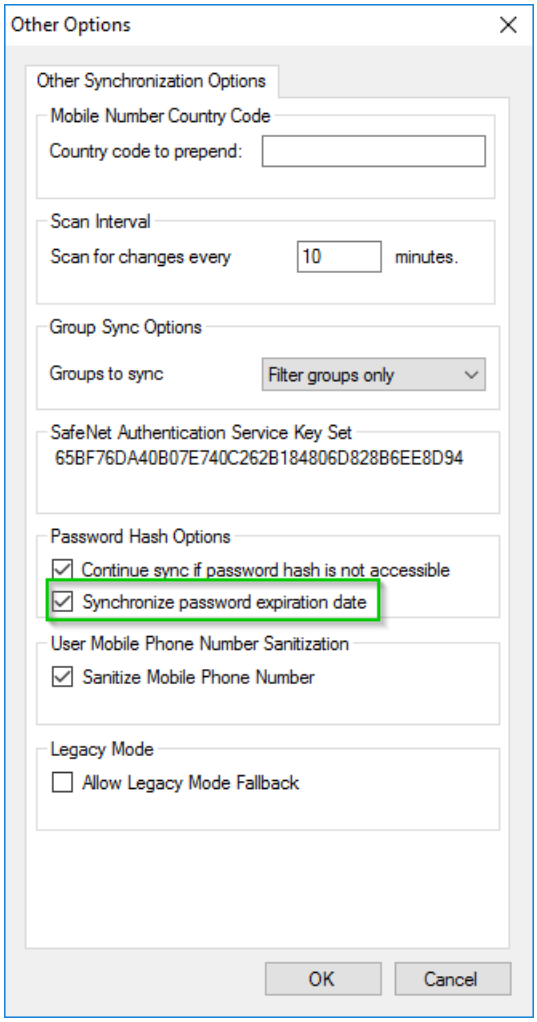
Resolved Issue

Issue	Synopsis
SAS-33863	Users IDs that are shorter than 16 bytes long and contain a '0' byte, such as 0x000003E8, are successfully synchronized to STA from SQL database.

Service Pack Release – 05/07/2019

This service pack release of SafeNet Synchronization Agent version 3.8.1 introduces the following feature and resolves the issues listed below:

> **Synchronize password expiration date check box:** The password expiry synchronization feature is now optional and can be turned off in the **Other Synchronization Options** section on the **Configuration** tab. It is selected by default.



Resolved Issues

Issue	Synopsis
SAS-28762	The correct password expiry dates are synchronized in a global catalog environment.
SAS-10782	You can successfully configure the SafeNet Synchronization Agent with eDirectory.

Service Pack Release – 03/25/2019

This service pack release of SafeNet Synchronization Agent version 3.8.0 introduces the following feature:

> **Legacy mode** is disabled by default. Fallback to legacy mode can be enabled to provide backward compatibility if you are using a new Sync Agent against an old STA server.

Resolved Issue

Issue	Synopsis
SAS-27399	Added information about configuring the SafeNet Synchronization Agent for PostgreSQL to the *Synchronization Agent Configuration Guide*, such as the database name must be in lowercase, and mixed-case SQL attributes or field names must be declared with double-quotes.

Service Pack Release – 11/06/2018

This service pack release of SafeNet Synchronization Agent version 3.7.0 resolves the issues listed below and introduces the following features:

- Ability to select whether or not leading zeros in mobile phone numbers are processed; see SafeNet Synchronization Agent, **Configuration > Other Synchronization Options > Configure > User Mobile Phone Number Sanitization**.
- Support for the display of password expiry information on the STA consoles.
- Reimplementation of the password synchronization library.
- Synchronization of users from Azure AD into STA as described in SafeNet Synchronization Agent Configuration Guide, version 3.7.0, revision A, “Appendix A: Synchronize Azure AD Users”.

> **NOTE** It is not possible to synchronize Azure AD **passwords** into STA using the SafeNet Synchronization Agent.

Resolved Issues

Issue	Synopsis
SAS-23617	SafeNet Synchronization Agent logs the following error message if the user ID exceeds 16 characters: “Error syncing user with id <userId>. Cannot sync a user with id longer than 16 bytes.” Where <userId> is the user ID provided by the client.
SAS-21920	Synchronize AD password hashes with STA. **CAUTION!** If you are using password synchronization, validate this release of SafeNet Synchronization Agent in a test environment before upgrading.
SAS-17220	When password synchronization is enabled, memory usage does not increase.

Service Pack Release – 09/04/2018

This service pack for SafeNet Synchronization Agent version 3.6.0 resolves the issues listed below, as well as providing:

- **Continue sync if password hash is not accessible:** This feature enables the SafeNet Synchronization Agent to skip individual user passwords that cannot be acquired and thereby continue to synchronize the passwords that can be acquired.

Resolved Issues

Issue	Synopsis
SAS-22768	MySQL Connector download works correctly.
SAS-24470	Debug logs correctly exclude exception messages if notification emails are not configured.

Service Pack Release – 04/18/2018

This service pack advises customers about potential difficulties with the installation process as described by SAS-22768:

Summary: When attempting to install Sync Agent 3.5.5 for MySQL, if you click on the connector link and then install connector version 6.9.9, the installation process fails.

Workaround: Manually download and install MySql.Data.dll version 6.10.6.

Service Pack Release – 04/13/2018

This service pack introduces Synchronization Agent version 3.5.5 and resolves the issues listed below.

Resolved Issues

Issue	Synopsis
SAS-21919	Password synchronization is supported in AD domains that have the Recycle Bin option enabled.
SAS-19467	Passwords synchronize correctly against the AD Global Catalog in multi-domain environments.

Service Pack Release – 09/27/2017

This service pack resolves the issue listed below, as well as providing:

- Enhanced password synchronization in multi-domain environments
- Improved debug logging for password synchronization scenarios
- Configurable log locations
- A notification template in case of user repository scan errors

Resolved Issue

Issue	Synopsis
SAS-17164	AD password synchronization succeeds in multi-domain or subdomain environments.

Service Pack Release – 06/29/2017

This service pack resolves the issue listed below.

Resolved Issue

Issue	Synopsis
SAS-16794	SafeNet Synchronization Agent correctly queries Oracle-based user repositories.

Service Pack Release – 06/16/2017

This service pack introduces Synchronization Agent version 3.5.3 and includes: support for Windows Server 2016; update to .NET 4.6.2; unbundling of MySQL Connector; and additional issue resolutions.

> **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** This release does NOT support Windows Server 2008 SP2. Customers using Windows Server 2008 SP2 should NOT implement this service pack.

Resolved Issues

Issue	Synopsis
SAS-16648 / SAS-10385	Sensitive information such as user names is only logged with logging set to debug level.
SAS-13871	The Synchronization Agent installer correctly prompts for prerequisite service packs.
SAS-10465	The Synchronization Agent correctly synchronizes with idle Active Directories.

Service Pack Release – 01/13/2017

This service pack introduces Synchronization Agent version 3.5.2 with Gemalto branding, in addition to resolving the issues listed below.

Resolved Issues

Issue	Synopsis
SAS-11557	The Synchronization Agent now correctly accounts for users in nested groups.
SAS-11402	The Synchronization Agent console updates the Synchronization Details when the operator switches their view to a different Virtual Server.
SAS-10466	The Synchronization Agent now presents directory changes to STA in the following order to prevent User ID conflicts: 1) Deletions, 2) Updates, 3) Additions.
SAS-8971	The Synchronization Agent now correctly performs bit operations on a Boolean attribute in the "Disabled Bit" field used by eDirectory.

General Availability Release – 07/29/2016

The SafeNet Synchronization Agent, version 3.5.1, features are now available.

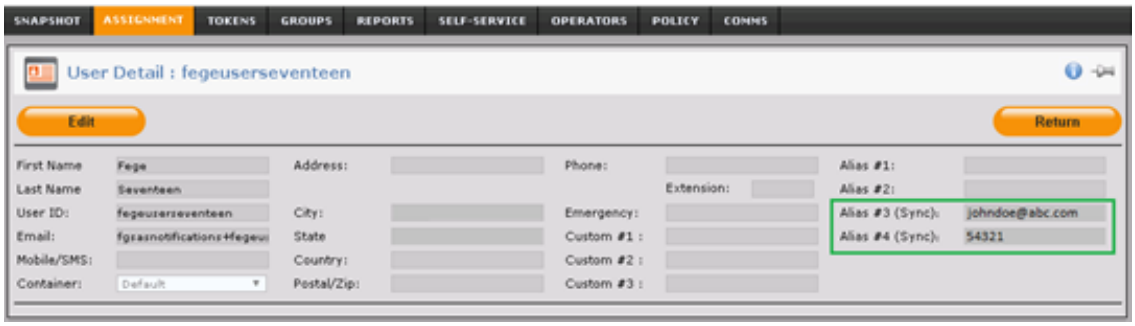
Synchronized Aliases

You can now configure Alias #3 and Alias #4 to be synchronized from the LDAP by creating a customized LDAP schema. Whereas Alias #1 and Alias #2 can be configured on the STA console by the operator only, the new Alias #3 and Alias #4 are synchronized from the LDAP source.

The aliases can be used by the user as an alternative to their User ID when authenticating.

The synchronization of Alias #3 and Alias #4 is configured through the SAS Synchronization Agent web-based management interface. For additional details about the Synchronization Agent, please refer to the *SafeNet Synchronization Agent Configuration Guide*.

The screen shot below shows how the new aliases appear in the STA console as part of the user details.



Active Directory Password Synchronization and Authentication

This enhancement is applicable to STA and currently supported SAS PCE versions. In the case of SAS PCE, passwords can also be validated through a direct LDAP connection.

The Synchronization Agent can now be used to synchronize the Active Directory Password of users from the LDAP into SAS.

Operators can then allow 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 STA database.

> **NOTE** Currently, STA does not synchronize the password expiry state. The AD password is handled as a cached credential, where the credential will remain valid until it is updated by the user through the domain controller.

There are two requirements for Active Directory password synchronization:

> The computer running the Synchronization Agent must be part of that Active Directory domain.

> The computer must have the following Active Directory permissions:

- Replication Directory Changes
- Replication Directory Changes All

Refer to "Synchronization Agent and STA Configuration " below for configuration details.

For details about configuring authentication with Active Directory Password on STA, refer to “Managing a Token” and “Configure Pre-Authentication Rules” in the *STA Service Provider Administrator Guide*.

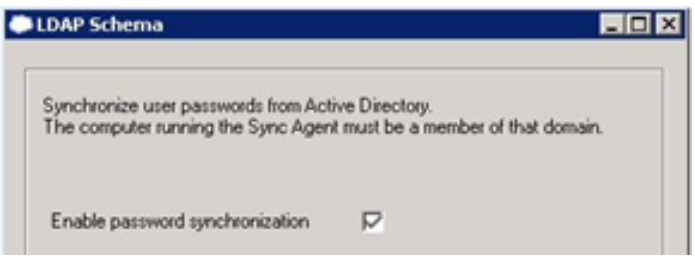
Synchronization Agent and STA Configuration

Configure the Synchronization Agent to Enable Active Directory Synchronization

This step is required to synchronize Active Directory passwords into STA.

1. In the Synchronization Agent, on the **LDAP Schema** window, select the **Enable password synchronization** option.

   For additional details about the Synchronization Agent, please refer to the *SafeNet Synchronization Agent Configuration Guide*.

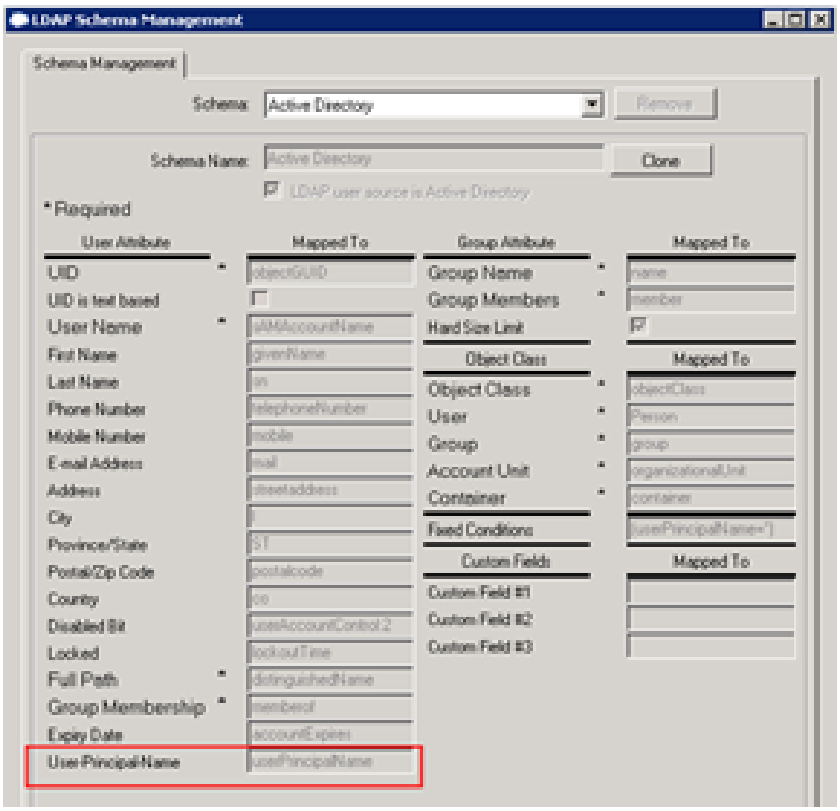


> **NOTE** To disable the use of AD passwords, simply clear the **Enable password synchronization** check box. After successful synchronization, the AD passwords are removed from STA, and they can no longer be used for authentication into STA—the passwords will still appear as assigned, but they can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

Synchronize UPN for use as a SAML Return Attribute

The UPN (User Principal Name) attribute can now be synchronized from Active Directory with the Synchronization Agent. This attribute can then be used as a return attribute for SAML authentication in STA.

After the Synchronization Agent is upgraded to version 3.5.1 and the default AD schema is used, the UPN will automatically synchronize 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.

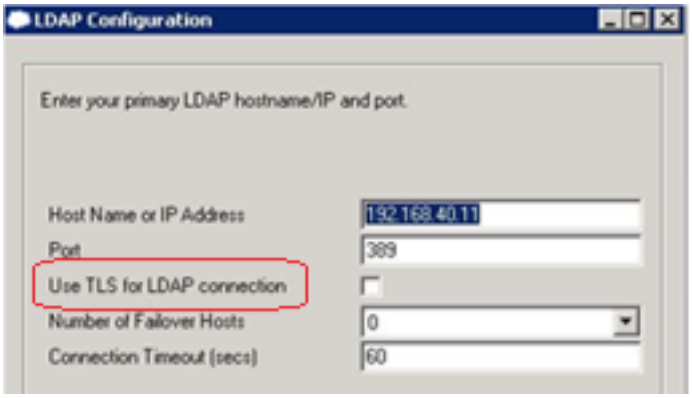


If you are using a custom Active Directory schema, and you want to synchronize the UPN attribute from Active Directory, you will need to manually add this attribute in the Synchronization Agent. (Custom schema configuration should match UPN mapping in the default Active Directory schema.)

Then, refer to “SAML Service Providers Module” in the *Service Provider Administrator Guide* for details on how to add an attribute in the STA Token Management console.

LDAP Configuration—Use SSL Option Renamed

The **Use SSL** option has been renamed to **Use TLS for LDAP connection** in the **LDAP Configuration** window.



Advisory Notes

Recommended Best Practices

- When deploying the Synchronization Agent, a single agent ensures reliable synchronization and is recommended for most organizations. Two agents are recommended to meet redundancy or resiliency requirements.
- It is recommended to run the latest version of the Synchronization Agent.

System Requirements

Note that only server variants of Windows are supported with Synchronization Agent version v3.4 and later. All supported Windows operating systems are listed under "Operating Systems " on page 13.

The STA server should be upgraded first to v3.4. Existing Synchronization Agents (up to v3.3.2) will continue to work, but the scan interval will be limited to once every 60 minutes (instead of every 20 minutes), even if the agent is manually stopped and restarted.

It is recommended to upgrade the Synchronization Agent to v3.5.1 in order to obtain the benefits of differential synchronization and regain a scan interval of every 20 minutes. Restarting the synchronization service in the agent initiates scanning and synchronization.

Minimal DN Scope for LDAP Scanning

To ensure optimal synchronization performance, it is advised to limit LDAP scanning to Distinguished Names (DN) that encompass all sync groups. With an overly broad scanning scope for very large LDAP Directories, LDAP scanning may not always report all users to the Synchronization Agent, which can lead to users being marked in STA for delayed removal, and then deleted after 24 hours.

Note that the Synchronization Agent will not allow modifications to be made to the DN scope for Active Directory if the default settings are used. Search containers cannot be specified if the **LDAP user source is Active Directory** check box is selected. This option allows the Synchronization Agent to determine if the custom schema is for an Active Directory (AD) implementation of LDAP. If this option is enabled, the agent will always target all LDAP queries against the Base DN and use Active Directory optimized search queries.

In addition, it is recommended to keep the **Use Delayed Sync Removal** feature enabled in the STA Token Management console under **COMMS > Authentication Processing > LDAP Sync Agent Settings**.

Synchronizing Users and Groups with Multiple LDAP or SQL User Stores

Only a single user store can be synchronized to a Virtual Server. Note that this is currently not enforced. It is strongly advised to verify that all agents are configured for exactly the same groups and attributes; otherwise, synchronization conflicts and inconsistencies can arise. Differing synchronization configurations for the same Virtual Server are not supported.

Known Issues

This table provides a list of known issues as of the latest release.

Issue	Synopsis
SAS-47195	**Summary:** SafeNet Synchronization Agent spams event viewer when creating auto indexes. **Workaround:** None
SAS-29238	**Summary:** When synchronizing users with aliases that are members of a nested group, alias3 and alias4 are not synchronized. **Workaround:** None
SAS-22689	**Summary:** An Active Directory group that comprises child users only, cannot be synced unless those child users include users from the root domain. **Workaround:** None
SAS-21946	**Summary:** If a group includes a nested group and the Agent is set to sync Filter groups only, the fail-safe that cancels a sync when a group appears empty does not function correctly. **Workaround:** None
SAS-16215	**Summary:** Sync Client does not update Users in cache and User in source for SQL user repositories. **Workaround:** None
SAS-15924	**Summary:** Sync Agent does not connect to MySQL data source when the latest MySQL Connector is installed. **Workaround:** Download and install MySQL .NET Connector 6.10.7.
SAS-59919	**Summary:** Configuration for changing log location for sync agent is not working. **Workaround:** Update log path from **Registry Editor > Software > CRYPTOCard > BlackShield ID > LogDir**.

Compatibility and Upgrade Information

Interoperability

SafeNet Authentication Service

> SafeNet Authentication Service v3.4 and later

Operating Systems

- Windows Server 2022
- Windows Server 2019 (Desktop Experience option)
- Windows Server 2016
- Windows Server 2012 R2

> **NOTE** If you attempt to install SafeNet 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 requires Windows updates: KB2919355 and KB2919442). Links for these software components are provided in this table.

- Windows Server 2012
- Windows Server 2008 R2 SP1 (64-bit)

Additional Software Components

- Microsoft .NET Framework 4.6.2 (Offline Installer) for Windows Server 2012 R2 https://www.microsoft.com/en-us/download/details.aspx?id=53344
  Install prior to installing the Sync Agent

> **NOTE** Install prior to installing the Synchronization Agent on Windows Server 2012 R2. The installer will try to resolve all dependencies automatically on other supported operating systems.

- Windows Server 2012 R2 Update (KB2919355) https://www.microsoft.com/en-ca/download/details.aspx?id=42334
- Windows Server 2012 R2 Update (KB2919442) https://www.microsoft.com/en-ca/download/details.aspx?id=42153
- Visual C++ Redistributable Packages for Visual Studio 2013 https://www.microsoft.com/en-ca/download/details.aspx?id=40784
- Visual C++ Redistributable for Visual Studio 2015 https://www.microsoft.com/en-ca/download/details.aspx?id=48145
- MySQL .NET Connector (required for MySQL)
  https://dev.mysql.com//Downloads/Connector-Net/mysql-connector-net-6.10.7.msi

Supported Directories

LDAP

- Active Directory
- Novell eDirectory 8.x
- SunOne 5.x

SQL

- MS SQL

- MySQL (requires MySQL .NET Connector) See "Additional Software Components" on the previous page.
- Oracle
- PostgreSQL

Upgrade Instructions

Upgrading the Synchronization Agent
To upgrade the Synchronization Agent, run the installer program. It is not necessary to stop the service or uninstall the existing agent.

Upgrading Multiple Redundant Agents
STA 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, upgrade another agent and then start, until all agents have been upgraded.

Upgrading SAS PCE/SPE to v3.4
The SAS server should be upgraded first to v3.4. Existing Synchronization Agents (up to v3.3.2) will continue to work, but the scan interval will be limited to once every 60 minutes (instead of every 20 minutes), even if the agent is manually stopped and restarted.

It is recommended to upgrade the Synchronization Agent to v3.5.1 in order to obtain the benefits of differential synchronization and regain a scan interval of every 20 minutes. Restarting the synchronization service in the agent initiates scanning and synchronization.

> **NOTE** SAS PCE/SPE v3.4 does not use the new synchronized attributes introduced with Synchronization Agent v3.5.1.

Product Documentation

The following additional documentation is associated with this release:

- *SafeNet Synchronization Agent Configuration Guide*

See Customer Support Portal for documentation associated with this product. 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.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales 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 Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone

The support portal also lists telephone numbers for voice contact (Contact Us).