



THE
DATA
PROTECTION
COMPANY

SAS Synchronization Agent

CUSTOMER RELEASE NOTES

Version: 3.4.170.28367
Document Part Number: 007-012682-002, Rev. B
Issue Date: 6 March 2015

Contents

Product Description	2
Release Description	2
New Features and Enhancements	2
Advisory Notes	4
Resolved and Known Issues	5
Compatibility and Upgrade Information	5
Product Documentation	6
Support Contacts	7

Product Description

The SafeNet Authentication Service (SAS) Synchronization Agent allows you to sync users in LDAP or SQL user groups to a SAS user store. Without the SAS Synchronization Agent, the administrator must manually input user information via the web-based management interface. With the SAS 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.

Release Description

The SAS Synchronization Agent, version 3.4.170.28367, includes several new features and enhancements, and resolves several defects.

New Features and Enhancements

New Features

Differential Synchronization

In previous versions of SAS, a full sync of all user records was performed for each and every sync event. With this version, the SAS Synchronization Agent has been enhanced so that only changed user records, including additions and deletions, are synchronized, resulting in less network traffic and reduced sync time. This is referred to as “differential synchronization.” Reduced system load also increases the reliability of synchronization services.

User records are sent in “batches” to the SAS user store. With differential synchronization, the initial sync may take longer to complete as it builds up its local information store, but subsequent syncs typically complete much faster.

Differential syncing occurs in parallel with scanning the user store. This means that new users can typically start using authentication before all users are synchronized. If the agent cannot connect to the server, the sync is retried with the next user store scan. Differential synchronization also re-enables scan intervals less than 60 minutes down to a minimum of 20 minutes, and instant synchronization by stopping and starting the agent.

Sync History Report

In support of differential synchronization, the **Sync History Report** (available through the SAS Management Console) has been updated. The **User’s Total** column heading has been changed to **Processed Users** and the **Group’s Total** column heading has been changed to **Processed Groups**.

The **Processed Groups** column displays the number of changed groups that were processed during the sync batch. The **Processed Users** column displays only the number of users in this batch sent to be synced since the last successful sync. Each batch contains up to 40 users or groups.

The **Sync History Report** is viewed in the SAS Management Console by clicking **COMMS > Authentication Processing > LDAP Sync Agent Hosts**. Click the **View Sync History** link. User changes appear in the report incrementally as they occur.

Sync Host Notification Alert

A new alert option called **Sync Host Notification** can now be enabled for SAS operators. When enabled, an alert will be sent via email or SMS indicating that permissions should be edited to allow the SAS server to accept syncs from the Synchronization Agent. This option is configured under **Virtual Servers > Policy > Role Management > Alert Management** and is enabled by default when creating a new Virtual Server. The alert is only sent when a newly added agent attempts to synchronize for the first time.

Enhancements

Support for Syncing LDAP Users from Nested Groups

The SAS Synchronization Agent has been enhanced to allow syncing of LDAP users from nested groups, where users may be members of a group that is a member of another group. The sync behavior for groups is determined by the **Group Sync Options** setting on the **Other Configuration Options** tab in the Synchronization Agent.

After the **Synch Groups** list has been created, the option selected below will determine how these groups and users are filtered, and thus added to SAS.

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

- **Groups with users only**—Groups contained in the **Synch Groups** list will be synchronized, and nested groups will be automatically included if their parent group is synced. For users, their “direct” group membership is maintained. For example, Group A contains Group B as a nested group, and User1 is a user in Group B. When Group A is synchronized, User1’s membership in Group B (the direct group) is maintained. Group A has no relationship to User1 other than being the parent of Group B.
- **Filter groups only**—Only the groups contained in the **Synch Groups** list will be synchronized. Nested groups must be explicitly added to the list to be included in the sync. This option is the default setting.
- **None**—Only the users will be synced from the groups contained in the **Synch Groups** list. Group designations will not be synced and thus group memberships will not be maintained. Users will be synced to a single, inclusive SAS users list.



NOTE: In SAS, the **Assignment** tab will display group membership attributes for a user’s parent group(s); in the example above, Group A. However, auto-provisioning rules trigger only on “direct” group membership, which means that nested groups require their own auto-provisioning rules.



NOTE: SAS syncs all nested groups that are visible in LDAP. SAS is not aware of trust relationships in Active Directory.

Before updating the Synchronization Agent, it is recommended to verify that, if the **Groups with users only** option is enabled under **Group Sync Options**, that LDAP groups configured for syncing do not contain nested groups with users you do not intend to sync.

After upgrading, all users of nested groups will be synced automatically if the **Groups with users only** option is enabled. Nested groups that were configured separately for syncing can be removed since this becomes redundant.

Additional information can be found in the *SafeNet Authentication Service Synchronization Agent Configuration Guide*.

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

The new features and enhancements are implemented with SAS v3.3.3 and later, and SAS Synchronization Agent build 3.3.30211.27765 and later. No other configuration changes are required. Note that this agent version supports only server variants of Windows. All supported Windows operating systems are listed under “Operating Systems” on page 5.

Earlier versions of the Synchronization Agent will continue to work with SAS, but the new and all future versions will use differential synchronization with SAS v3.3.3 and later. It is recommended to update the agent in order to realize the benefits of differential synchronization. It is also recommended, as a best practice, to run the latest version of the agent.

Previous versions of the Synchronization Agent will be disabled at a future date.

Minimal DN Scope for LDAP Scanning

It is advised to limit LDAP scanning to Distinguished Names (DN) that encompass all sync groups but is not unnecessarily larger than that. This ensures optimal synchronization performance, particularly with Active Directory. With an overly broad scanning scope for very large Active Directories, LDAP scanning may not always report all users to the Synchronization Agent, which can lead to users being marked in SAS for delayed removal, and then deleted after 24 hours. It is recommended to keep the **Delayed Sync Removal** feature enabled in the 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.

Resolved and Known Issues

Resolved Issues

Issue	Synopsis
SAS-5997	Synchronization is no longer halted if a sync group is not found in the user source (ActiveDirectory/LDAP).
SAS-5931	Active Directory user accounts that have expired and been reactivated are now processed correctly by the Synchronization Agent.
SAS-5905	To improve performance, changed user records are now processed in smaller batches, with each batch containing up to 40 users or groups.
SAS-5815	Group memberships are now processed correctly to ensure proper synchronization between LDAP and SAS.
SAS-5543	Changes to Email Templates are now saved correctly.
SAS-5006 ¹	Synchronized groups are now fully removed from SAS when deleted.

Compatibility and Upgrade Information

Interoperability

SafeNet Authentication Service

- SafeNet Authentication Service v3.3.3 and later

Operating Systems

- Windows Server 2012 R2 (64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2008 SP2 (64-bit)
- Windows Server 2008 R2 (64-bit)

Supported Directories

LDAP

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

¹ This issue was resolved in v3.3.3 of the Synchronization Agent.

SQL

- MS SQL
- MySQL
- 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

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, upgrade another agent and then start, until all agents have been upgraded.

Upgrading SAS PCE/SPE

The SAS server should be upgraded first to v3.4. Existing Synchronization Agents 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 v3.4 in order to obtain the benefits of differential synchronization and regain a scan interval of every 20 minutes. Restarting the sync service in the agent initiates scanning and synchronization.

Product Documentation

The following additional documentation is associated with this release:

- SafeNet Authentication Service Synchronization Agent Configuration Guide

All documents can be found at the following link on the SafeNet website:

<http://www2.safenet-inc.com/sas/implementation-guides.html>

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

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