



# SAS Synchronization Agent

## FAQs

### Contents

Description.....	2
Frequently Asked Questions.....	2
Recommended Best Practices.....	6
Advisory Notes.....	6
Product Documentation .....	6
Support Contacts.....	7

## Description

---

This document answers frequently asked questions about the new SafeNet Authentication Service (SAS) Synchronization Agent v3.4, for use with SAS v3.4 or later, and addresses the most common information needs for using the new agent.

The SAS Synchronization Agent allows you to sync users in LDAP or SQL user groups to a SAS user store. 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.

In earlier versions of SAS, up to v3.3.2, a full sync of all user records was performed for each and every sync event. With the new SAS Synchronization Agent, 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.” This also reduces system load, helping to increase the reliability of sync services.

## Frequently Asked Questions

---

### **Q. What are the changes in the new SAS Synchronization Agent compared to v3.3.2?**

- A. The changes include the “differential synchronization” functionality, nested group support, and changes to the Sync History Report.

### **Q. What exactly is “differential synchronization”?**

- A. In previous versions of SAS, a full sync of all user records was performed for each and every sync event. With differential synchronization, only “changed” user records, including additions and deletions, are synchronized since the last successful sync, resulting in less network traffic and reduced sync time. This also reduces system load, helping to increase the reliability of sync 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.

### **Q. What are the benefits of differential synchronization?**

- A. As mentioned previously, only “changed” user records, including additions and deletions, are synchronized since the last successful sync, resulting in less network traffic and reduced sync time. Reduced system load also increases the reliability of sync services. Refer to the next question for additional benefit information.

### **Q: Does differential synchronization allow 20-minute frequency, and does stopping and starting service trigger synchronization again?**

- A: SAS Cloud and SAS PCE/SPE v3.4 and later limit syncing to once every 60 minutes with older versions of the Synchronization Agent that don’t use differential synchronization. The new agent recognizes the Scan Interval setting, and restarting the sync service in the agent initiates scanning and synchronization.

**Q. What changes have been made to the Sync History Report?**

- A. In support of differential synchronization, 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 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.

The screenshot shows the 'LDAP Sync Agent Hosts' interface. At the top, there are buttons for 'Apply', 'Add', 'Change Log', and 'Cancel'. Below these is a summary table for 'View Sync Hosts History up to 100 Rows (1-5000)'. The summary table has columns: Remote Host, Remote IP, First Connect, Last Sync, Sync Recorded, Sync Permission, and actions (Remove, View Sync History). The first row shows TEST41 with Remote IP 10.6.0.239, First Connect 8/17/2014 4:48:20 PM, Last Sync 8/25/2014 3:04:12 PM, Sync Recorded 10082, and Sync Permission Allowed.

Below the summary table is a 'Close' button and a detailed transaction log table. The log table has columns: Transaction ID, Remote Transaction ID, Remote Host, Remote IP, Received Date, Stored Date, Committed Date, Processed Users, Processed Groups, and Removal Time. The log shows multiple transactions for TEST41 with Remote IP 10.6.0.239, all occurring on 8/25/2014, with varying times and processed counts.

**Q. What is nested group support?**

- A. The Synchronization Agent has been enhanced to sync LDAP users within nested groups, where users may be members of a group that is a member of another group.

In the Synchronization Agent, after the **Sync Groups** list has been created, the selected **Groups to Sync** option will determine how these groups and users are filtered, and thus added to SAS.

SAS synchronizes all users in nested groups that are visible in LDAP. SAS is not directly aware of trust relationships in Active Directory. For additional information, refer to the question on page 4 regarding the AD Global Catalog.

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

**Q: What preparation is needed before upgrading the Synchronization Agent?**

- A: 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.

**Q. What is required to use these new features?**

**A.** These new features require SAS Cloud v3.3.3 or later or SAS PCE/SPE v3.4 or later, and SAS Synchronization Agent v3.3.30140 or later. No other configuration changes are required.

Note that this agent version supports only server variants of Windows, as stated in the *SAS Synchronization Agent Configuration Guide*.

**Q: Do I have to upgrade the Synchronization Agent in order to continue using SAS?**

**A:** 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 3.3.3 or later. It is recommended to update the agent in order to enjoy the benefits of differential synchronization. It is also recommended as a best practice to run the latest version of the agent.

**Q: I am running Synchronization Agent v3.3.3. Should I upgrade to v3.4?**

**A:** Yes. Synchronization Agent v3.4 is a maintenance release to v3.3.3 that fixes several defects, and is recommended for all customers. It is generally recommended as a best practice to run the latest version of the agent.

**Q. What is the upgrade procedure for the new Synchronization Agent?**

**A.** Launch the installer to upgrade the agent. It is not necessary to stop the service or uninstall the agent.

**Q: How do I upgrade multiple redundant agents?**

**A:** 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 start, upgrade another agent and start, until all agents have been upgraded.

**Q. What if I have a mixed environment of different versions of the Synchronization Agent configured against the same LDAP server and the same authentication virtual server?**

**A.** This is not supported. Mixing newer agents that use differential synchronization with older agents that don't negates the benefits of differential synchronization. All older agent versions should be upgraded to the latest version, as described in previous answer.

**Q: Can the Synchronization Agent sync multiple domains to SAS using Active Directory Global Catalog?**

**A:** Yes. Although the Synchronization Agent does not directly support Active Directory, it can be configured to sync with a Global Catalog for LDAP searches. To enable this functionality in the Synchronization Agent, you must set the **Port** field on the **User Source Configuration** window to **3268**, which is the port to which Global Catalog queries are directed.

In addition to the above configuration changes, note the following additional steps that may need to be performed:

- The selected **Synch Groups** must be set as “universal” groups.
- In SAS, under **Authentication Processing > LDAP Sync Agent Settings**, it is recommended to enable the **Use Delayed Sync Removal** option.
- In the Synchronization Agent, under **User Source Configuration**, select the option **Manually edit searched containers**, and then add the containers from the sub-domains.
- In order for the Synchronization Agent to scan and sync Global Catalog groups to SAS, you must bind to **DC=<root>,DC=<domain>** to search over all sub-domains. Then, you will need to do one of the following:
  - In the Synchronization Agent, under **User Source Configuration**, select the option **Manually edit searched containers**, and then add the containers from the sub-domains.
  - If the above procedure does not produce the intended results (all domain groups are not displayed), enter a NULL value (" ") for **Manually edit searched Containers** to instruct the Agent to search the entire Active Directory tree.

The Microsoft TechNet article entitled *Global Catalog and LDAP Searches* provides additional information and can be found at the following link:

<http://technet.microsoft.com/en-us/library/cc978012.aspx>

**Q: How can I test differential synchronization before placing it into use?**

**A:** Testing should normally not be necessary since differential synchronization does not change scanning or what is synchronized. Testing the new agent version is possible with a separate virtual subscriber that can be created under Service Provider accounts. It is not possible to use the new and old agent versions together in the same virtual subscriber.

**Q: Can I revert back to not using differential synchronization?**

**A:** Differential synchronization does not introduce new functionality and results in the same user data in SAS. In case of unforeseen issues, it is possible to revert to the last agent version (3.03.20178) that does not use differential synchronization.

Stop all agents, except one. Launch the installer for version 3.03.20178 to upgrade this agent (which can still be running), and start the service. Continue upgrading additional agents.

For information on backup and restore procedures, refer to the *SAS Synchronization Agent Configuration Guide*.

**Q: Can the new Synchronization Agent version be used with earlier versions of SAS PCE/SPE?**

**A:** No. Synchronization Agent v3.4 (or later) is only supported with SAS v3.4 or later. The Synchronization Agent v3.03.20178 continues to be provided and supported for SAS v3.3.2, as well as earlier versions of SAS that are still under full support.

### Q: What is the upgrade path for SAS PCE/SPE?

A: The SAS server should be upgraded first to v3.4. Existing Synchronization Agents will continue to work but the scan interval is limited now 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.

## Recommended Best Practices

---

- Deployment of a single SAS Synchronization Agent ensures reliable synchronization and is recommended for most organizations. Deployment of two agents is recommended to meet redundancy or resiliency requirements. Each agent must be identically configured except that they may point to different LDAP servers (of the same directory), which is recommended for better resiliency towards LDAP.
- It is recommended to run the latest version of the agent.

## Advisory Notes

---

### 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

A single Virtual Server can synchronize only to a single User Store. 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.

## Product Documentation

---

The following documentation supports the SAS Synchronization Agent:

- SAS Synchronization Agent Customer Release Notes
- SAS Synchronization Agent Configuration Guide

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

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

## 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	<a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a> 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.	