SafeNet Authentication Service

PCE/SPE Upgrade Guide

gemalto
security to be free

Product Version: SafeNet Authentication Service 3.5.5 PCE/SPE

Document Part Number: 007-012795-005, Rev. A

Release Date: May 2017

Table of Contents

Document PN: 007-012795-005, Rev. A,

Preface

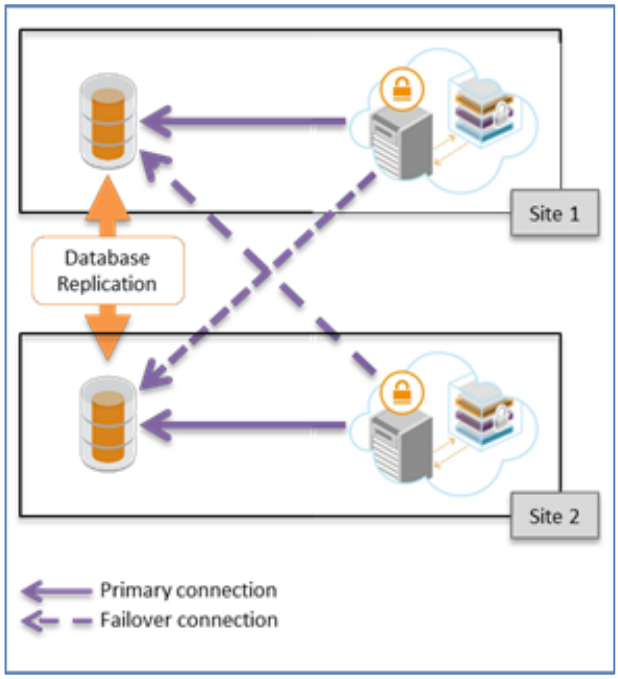
Supported Versions

This document describes how to upgrade from SafeNet Authentication Service (SAS) PCE/SPE versions 3.2, 3.2.1, 3.3.1, 3.3.2, 3.4, 3.5 or 3.5.4 to version 3.5.5.

NOTE: Before upgrading from any previous version to SAS PCE/SPE 3.5.5, please refer the ***System Requirements Guide*** to check if all the required prerequisites are available.

Overview

The SAS solution can be deployed in varying configurations. The instructions included in this document are based on a generic SAS PCE/SPE deployment as depicted in the following diagram, independent of the deployment strategy defined by the customer's specific needs:



NOTE: The adaptation of the generic deployment to the custom requirements of each site (data center) will be determined by your deployment team.

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes SAS users and security officers, 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 the support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	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 login to manage incidents, get latest software upgrades, and access the Gemalto Knowledge Base.	
Documentation	All SAS documentation (Cloud, PCE, SPE, Token and Integration) can be found on the **SafeNet Knowledge Base** Internal. All SAS Agents documentation can be found on the **SafeNet Authentication Service Downloads** page.	

1

SafeNet Authentication Service Components Upgrade

FreeRADIUS

It is recommended that the FreeRADIUS Server and Agent software be upgraded prior to performing any SAS updates. For more information regarding the FreeRADIUS Server and Agent upgrade, refer **FreeRADIUS Upgrade Guide**.

Shibboleth (SAML)

It is recommended that the Shibboleth (SAML) Server and Agent software be upgraded prior to performing any SAS updates. For more information regarding the Shibboleth (SAML) Server and Agent upgrade, refer **Shibboleth Upgrade Guide**.

2

SafeNet Authentication Service Pre-Upgrade Checklist

This section provides a checklist of all the required changes to be made prior to the upgrade of SAS.

SafeNet Authentication Service

This section will guide you through the process of upgrading SAS from versions 3.2, 3.2.1, 3.3.1, 3.3.2, 3.4, 3.5 or 3.5.4 to version 3.5.5. The guide will also cover all the necessary steps to backup and save various installation files and databases for rollback during disaster recovery events.

NOTE: Before upgrading from any previous version to SAS PCE/SPE 3.5.5, please refer the ***System Requirements Guide*** to check if all the required prerequisites are available.

Deployment Diagram/Documentation

An SAS deployment diagram, along with proper documentation, will be needed after upgrading. The diagram should contain a list of all services (Console, Token Validator, BSIDCA, etc.) that each site should be running, as well as which services should be turned off since the upgrade process will turn on all services.

Installer Backup

Backup existing SAS installer files for disaster recovery purposes.

Download/Copy

Download and unzip the latest **SAS PCE/SPE zip** file, and then copy the new **BlackShield ID Service Provider Edition x64.exe** installer (provided in the .zip file) to all SAS servers.

Cipher Key Export

The SAS **CipherExport** utility is located in the **SAS installation** directory. The default installation path is:

```
<drive>:\Program Files\CRYPTOCard\BlackShield ID\CipherExport
```

To run the CipherExport.exe utility:

1. Open a DOS command prompt in the **CipherExport** directory and enter the following command:

CipherExport.exe export Cipher.bak

This command creates a file called **Cipher.bak** and displays the encryption key in the DOS command prompt.

2. Copy the value of **Export File Key** shown in the DOS prompt and save it to a text file (for example, **ExportFileKey.txt**).
3. Move **Cipher.bak** (created in the **CipherExport** directory) and the **ExportFile.Key.txt** file to a secure location.

> **NOTE**: The CipherExport tool must be run on each SAS server that is in use. Without doing so, you will not be able to perform a restore on the applicable server.

Primary SafeNet Authentication Service Registry Export

1. On the Primary SAS server, open the Windows Registry and locate the following:

   HKEY_LOCAL_MACHINE > SOFTWARE > CRYPTOCARD > BlackShield ID > DAL
2. Right-click on **DAL** and export the Registry key.
3. Save the Registry key file with an appropriate name.
4. Move the Registry key file to a secure location.

License

Locate the latest SAS license file, along with the activation code, and move them to a secure location.

Monitoring Utility

All SAS monitoring utilities should be disabled in the Secondary data center until all components have been upgraded. The Secondary data center should always be upgraded first.

Authentication

Authentication traffic must be routed from the Secondary data center to the Primary data center. There are two ways to achieve this - IP routing or DNS routing.

IP Routing

IP routing is specifically for FreeRADIUS authentication traffic. When FreeRADIUS accepts RADIUS requests, the SAS FreeRADIUS agent will take the incoming authentication and connect to the SAS TokenValidator IP address to validate the user attempting to authenticate, with no DNS lookup required. If this is currently being utilized, go directly to the **FreeRADIUS** section.

DNS Routing

DNS routing is applicable for Token Validator and, optionally, for FreeRADIUS. If DNS routing is utilized for both Token Validator and FreeRADIUS, ensure the following DNS names are configured:

- Public DNS names for token validator(s) (Port 443 TCP)
- Internal DNS names for SAS FreeRADIUS Updater Service (Port 5041 TCP)

FreeRADIUS

FreeRADIUS Agent

1. Browse to the following directory:

   `/usr/local/cryptocard/freeradius`

2. Make a backup copy of the **cryptocardFreeRadiusConfig** file, and name the file `cryptocardFreeRadiusConfig.<DATE>.bak`

   NOTE: **<DATE>** denotes the day when the command is to be executed.

3. Open **the cryptocardFreeRadiusConfig** file with a text editor.
4. Verify that **sections 16** and **24** are set to **Primary TokenValidator IP/Secondary TokenValidator DNS**. If not, change accordingly.
5. If not using SSL, skip to step 6.

   If FreeRADIUS Agent is connecting to Token Validator via SSL, verify the following:

   - **Section 17** and **25** are set to **TCP port 443**. If not, change accordingly.
   - **Section 20** and **28** have a value of **1**. If not, change accordingly.

6. If any changes were made, save the file and restart the **RADIUSD** daemon:

   `/etc/init.d/radiusd restart`

7. Use the **tail** command with the **radiusd.log** to verify that the changes are working correctly:

   `tail –fv /opt/freeradius/freeradius-server-<version>/var/log/radius/radius.log`

FreeRADIUS Updater

1. Browse to the following directory:

   `/usr/local/cryptocard/freeradius_updater/dynamicUpdate/`

2. Make a backup copy of the **sslConfigurationClient.txt** file with the name `sslConfigurationClient.txt.<DATE>.bak`

   NOTE: **<DATE>** denotes the day when the command is to be executed.

3. Open the **sslConfigurationClient.txt** file with a text editor.

4. In **section 20**, verify that both the IP and DNS are set to **Primary SAS FreeRADIUS Update Service/Secondary SAS FreeRADIUS Update Service**. If not, change accordingly.
5. If changes were made, save the file and restart the FreeRADIUS updater daemon:

   `/etc/init.d/./freerad_updaterservice restart`
6. Check the **freeRadupdateClient-year-month-day.log** file for any errors. The log file is located in:

   `/usr/local/cryptocard/freeradius_updater/log/`
7. Verify that Auth Nodes added in SAS PCE/SPE are loading correctly into **clients.conf**:

   `/opt/freeradius/freeradius-server-<version>/etc/raddb/`

DNS Routing – Changes

If DNS routing is utilized for any or all components, perform the following steps:

Public

1. Make note of the IP address associated with the Secondary Token Validator.
2. Login to your public DNS provider.
3. Change the IP address associated with the Secondary Token Validator DNS to the Primary Token Validator IP address.

Internal

If the FreeRADIUS Updater configuration is not using DNS to connect to the SAS FreeRADIUS Updater Service, skip to the **Stopping Services** section.

1. Make note of the IP address associated with the Secondary FreeRADIUS Updater Service.
2. Login to your internal DNS domain.
3. Change the IP addresses associated with the FreeRADIUS Updater Service DNS to the Primary **FreeRADIUS Updater Service** IP address.

NOTE: Do not route traffic to the public DNS names.

Stopping Services

In the Secondary data center, log on to each SAS server and stop the WWW service. This effectively renders the Secondary data center to only running FreeRADIUS; all traffic has been routed to the Primary data center.

NOTE: These changes must be reverted after the upgrade is complete.

Preparing MS SQL

The following process is divided into two sections:

- **SAS Configuration**: Point all SAS servers in the Primary data center to a Primary MS SQL instance.
- **MS SQL Replication**: Break and remove MS SQL replication.

SAS Configuration

In the Primary SAS data center, verify that each SAS server is pointed to the Primary MS SQL instance for both the Primary and Secondary SQL database configuration (**SAS Console > Database > SQL Database**).

NOTE: Alternatively, if each SAS server in the Primary data center is using DNS to connect to SQL, changing DNS routing can be utilized.

For example:

DB1.acme.com > 192.168.1.2 changes to DB1.acme.com > 192.168.1.10

MS SQL Replication

The following procedure should be performed by a Microsoft DBA or someone with knowledge of Microsoft database replication. All MS SQL nodes must be removed from the peer-to-peer topology. The SAS database (by default, BlackShield) must be removed as a publication. The order of removal should be as follows:

- Remove each MS SQL database instance in the Primary and Secondary data centers
- Remove all Publication(s)
- Remove all Subscription(s)

On the Primary MS SQL instance, create an SAS database backup, and then restore the backup to a new SAS database name. (Use a unique name to indicate that this is before replication break – for example, **SASpreupgrade**).

NOTE: The SAS database backup and restore process to a new SAS database name is for disaster recovery purposes.

Preparing MySQL

In the current SAS PCE installation, if you have set up DBA-managed MySQL database high availability and you want to move to SAS-managed MySQL database high availability then break and remove the existing MySQL replication.

3

SafeNet Authentication Service Upgrade - Primary Data Center

SafeNet Authentication Service Upgrade Procedure

The SAS 3.5.5 introduces a variety of new features and enhancements to its Operators, Account Managers, and end users. (Refer **SAS PCE/SPE 3.5.5 Customer Release Notes** for a list of new features.) Due to the new features, the upgrade may take upwards of 50 minutes (depending on the amount of data in the SAS database). It is recommended that a maintenance window of two hours be allotted to ensure sufficient time is available to upgrade all SAS servers and components.

SafeNet Authentication Service Backups

After completing all procedures under **SafeNet Authentication Service Pre-Upgrade Checklist**, the following items must be backed up and available for disaster recovery:

- Current SAS installers
- Database backup
- Cipher key export (including Primary SAS Registry key export)
- SAS License
- SAS deployment diagram

If this has not been done, revisit and complete all sections in **SafeNet Authentication Service Pre-Upgrade Checklist**.

Monitoring Utility

The SAS Monitoring utility must be disabled in the Primary data center from this point forward until all components are upgraded.

Disabling Traffic

On the Primary data center, the following traffic must be disabled (internal or external) once the maintenance window commences:

- HTTP (80)
- HTTPS (443)
- RADIUS (1812)
- LDAP Sync (8456)

SafeNet Authentication Service 3.2/3.2.1/3.3.1 to 3.3.2 Upgrade

Direct upgrade from SAS 3.2.x to SAS 3.5.4 is not supported. The administrators have to upgrade using the following path:

1. SAS 3.2.x to SAS 3.3.2
2. SAS 3.3.2 (and later) to SAS 3.5.4

Prerequisites

SAS

Ensure that
- Backup of cipher keys from all SAS Servers is taken
- Backup of most recent SAS licensing is taken
- Backup of current and new version of SAS installers is taken
- Snapshot of SAS Systems (if VM), before upgrade is taken

Database

- Break the database replication (if deployed, any).
- All SAS Servers are pointed towards Primary MSSQL Instance
- SAS DB backup is taken

Supported Specifications & Servers

PostgreSQL 9.x
MS SQL 2008 and MS SQL 2012
MySQL 5.6

Upgrade Process

1. Backup the Cipher Export and Export File Key from all SAS Servers and copy them to a safe location.
2. Backup the SAS DB from MSSQL and copy to a safe location.
3. Delete all Publication and Subscription on all MSSQL instances.
4. Drop/Delete databases on all MSSQL instances, EXCEPT FOR PRIMARY MSSQL.
5. Upgrade Primary SAS server to a newer version of SAS by running the setup file.
6. Upgrade all other SAS Servers to a new version of SAS.
7. Stop IIS, and BlackShield services on all SAS Servers
8. Make a backup of SAS DB from Primary MSSQL instance and move it to a safe location
9. Import updated SAS DB into all other MSSQL instances

   NOTE: All MSSQL instances will now have identical DB's at this time
10. Rebuild replication between all MSSQL instances

11. Start IIS and BlackShield services on all SAS Servers

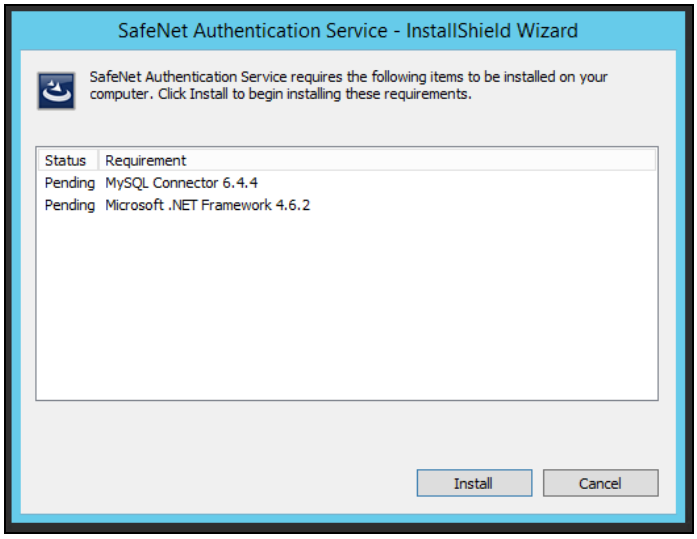
SAS Server Upgrade

1. Double-click SAS Service Provider Edition.exe.
2. Follow the on-screen instructions.
3. Click **Yes** to continue with the upgrade.

SafeNet Authentication Service 3.3.2 (and later) to 3.5.5 Upgrade

NOTE: Upgrading from SAS 3.3.2 to SAS 3.4 (and later versions) will require LDAP User Source to be reconfigured with **use local database** option selected, prior to the upgrade (if it was not selected already).

NOTE: If you are using MySQL as the SAS database, upgrading from SAS 3.3.2 to SAS 3.5.5 will require MySQL Connector 6.4.4. After running the **BlackShield ID Service Provider Edition.exe** (as listed below, in the steps), the SAS InstallShield Wizard displays a prompt to install MySQL Connector 6.4.4 (if required). After successful installation of MySQL Connector, the process will install .NET Framework 4.6.2.



Perform the following steps on the Primary SAS server:

1. Run **BlackShield ID Service Provider Edition.exe**. Change the install path to where the existing SAS installation file is located. Select **Custom** during the installation wizard, and disable Salesforce and PostgreSQL.
2. Start the installation.
3. Once the DBUpgrader DOS prompt is displayed, navigate to Windows Services and stop ALL BlackShield services.

> **NOTE**: The BlackShield services cannot run while DBUpgrader is performing its upgrade. This is to prevent any new queued data from being added to the database while DBUpgrader is running. The upgrade may take up to 30 minutes.

4. After installation is complete, browse to the following directory and verify that no errors appear in the SQL upgrade logs:

   `\Program Files\CRYPTOCard\BlackShield ID\Log`

5. Restart the SAS server.
6. Once the server is running, login to the SAS server and wait for six (6) minutes.
7. Click **Event Viewer > Application** and verify that there are no BlackShield errors.
8. Check the BlackShield log file to ensure that there are no errors. The log is located in:

   `\Program Files\CRYPTOCard\BlackShield ID\Log`

9. If no errors appear, disable the components that are not utilized on this SAS server.

If there is more than one SAS server in the Primary data center, perform the steps above for each SAS server, omitting steps 3 and 6.

After each SAS server is upgraded:

- Test each server for the components it is servicing (for example, Console, BSIDCA, etc.).
- Disable any services (Windows or Web) that the SAS servers are NOT servicing.
- Verify that any other changes made prior to the upgrade are still configured as desired.

Recreating MS SQL Peer-to-Peer Replication

The following should be performed by a Microsoft DBA or someone with knowledge of Microsoft database replication.

Once the SAS servers are upgraded in the Primary data center, replication must be re-established. However, replication should not start until archived and queued LDAP sync transactions have been processed. Once data has been processed, replication can be re-established.

For more information, learn how to **Configure Peer-to-Peer Transactional Replication (SQL Server Management Studio)**.

> **NOTE**: Peer-to-peer replication must be re-established before upgrading SAS in the Secondary data center.

SafeNet Authentication Service Post-Upgrade Changes – Primary Data Center

After SAS is upgraded, additional post-SAS-upgrade checks must be performed prior to the SAS upgrades in the Secondary data center.

MS SQL Database Configuration

In the Primary SAS data center, check each SAS server (if applicable) and re-point to its respective Primary and Secondary SQL database (**SAS Console > Database > SQL Database**).

NOTE: If DNS/IP changes were used to route both the MS SQL DNS name to a Primary SQL instance, revert the DNS/IP mapping to its pre-upgrade setting

For example:

DB1.acme.com > 192.168.1.2 changes to DB1.acme.com > 192.168.1.10

MySQL Database Configuration

After upgrading to SAS PCE/SPE 3.5.5, if you want to set up SAS-managed MySQL database high availability, perform the following steps:

1. Take backup of the existing MySQL database.
2. Using the MySQL database backup, create slave MySQL databases.
3. Set up master and slave databases, and then configure database settings in SAS.
   For details, refer **Installation Guide**.

Enable Traffic

Traffic can now be re-enabled (internal or external) to allow customers to start authenticating, synchronizing, and administering users in SAS. However, re-enabling traffic must be controlled to prevent excessive load.

RADIUS/HTTP(S)

RADIUS and HTTP(s) traffic should be the first types of traffic to be re-enabled.

1. Login to the FreeRADIUS Server and use the tail command with the **radius.log** file:

   `tail –fv /opt/freeradius/freeradius-server-<version>/var/log/radiusd/radiusd.log`

2. Re-enable RADIUS traffic and verify that authentication is succeeding.
3. Re-enable HTTP(S) traffic and then browse to the public SAS Console URL. Login to SAS and verify that Token Validator authentication is succeeding. If authentication is succeeding, continue to LDAP Sync.

LDAP Sync

Re-enable LDAP sync traffic and verify that LDAP sync traffic is committing correctly.

Monitoring Utility

If an SAS Monitoring utility is used to monitor any SAS components in the Primary data center, re-enable it when the SAS upgrade has completed.

4

SafeNet Authentication Service Upgrade - Secondary Data Center

Once SAS has been upgraded in the Primary data center, replication has been rebuilt, and traffic has been re-enabled, SAS upgrades must be performed in the Secondary data center.

SafeNet Authentication Service Upgrades

Perform the following steps on the Secondary SAS server:

1. Run **BlackShield ID Service Provider Edition.exe**. Change the install path to where the existing SAS installation file is located. Select **Custom** during the installation wizard, and disable **Salesforce** and **PostgreSQL**.
2. Start the installation.
3. After installation is complete, browse to the following directory and verify that no errors appear in the SQL upgrade logs:

   `\Program Files\CRYPTOCard\BlackShield ID\Log`
4. Restart the SAS server.
5. Click **Event Viewer > Application** to verify that there are no BlackShield errors.
6. Check the BlackShield log file to ensure that there are no errors. The log is located in:

   `\Program Files\CRYPTOCard\BlackShield ID\Log`
7. If no errors appear, disable the components that are not utilized on this SAS Server.

If there is more than one SAS server in the Secondary data center, perform the steps above for each server.

After each SAS server upgrade, test all services components specific to each SAS server site. Disable any services (Windows or web) that the SAS servers are NOT servicing.

Verify that any other changes made prior to the upgrade are still configured as desired.

Authentication Redirect – Secondary Data Center

Once the SAS servers have been upgraded in the Secondary data center, authentication (RADIUS/Token Validator) must now be re-directed to the Secondary data center.

Token Validator

In the **Public** section, you were instructed to change the DNS routing of the Secondary Token Validator to route to the Primary Token Validator IP address. This change must be reverted to the original setting. To do so, login to your public DNS provider and change the IP address associated with the Secondary Token Validator DNS back to the Secondary Token Validator IP.

FreeRADIUS Agent

If the FreeRADIUS Agent is configured with DNS, navigate to the **DNS Routing** section below.
If configured with IP, visit **IP Routing** section on page 22.

DNS Routing

If the FreeRADIUS agent is utilizing DNS, perform the following steps:

1. Browse to the following directory:

   `/usr/local/cryptocard/freeradius`
2. Open the c**ryptocardFreeRadiusConfig** file with a text editor.
3. In **section 16**, change the DNS to the DNS setting prior to SAS upgrade.
4. If the **FreeRADIUS Agent** is not using SSL, skip this step and proceed to step 5.

   If **FreeRADIUS Agent** is connecting to the **TokenValidator via SSL**, verify the following:

   - **Section 17** is set to TCP port **443**. If not, change accordingly.
   - **Section 20** has a value of **1**. If not, change accordingly.
5. In **section 24**, change the DNS to the DNS setting prior to SAS upgrade.
6. If the **FreeRADIUS Agent** is not using SSL, skip this step and proceed to step 7. If the **FreeRADIUS Agent** is connecting to the TokenValidator via SSL, verify the following:

   - **Section 25** is set to TCP port **443**. If not, change accordingly.
   - **Section 28** has a value of **1**. If not, change accordingly.
7. If any changes were made, save the file and restart the **RADIUSD** daemon using the following command:

   `/etc/init.d/radiusd restart`
8. Use the **tail** command with the **radiusd.log** file to verify the changes are working correctly:

   `tail –fv /opt/freeradius/freeradius-server-<version>/var/log/radiusd/radiusd.log`

IP Routing

If the FreeRADIUS agent is utilizing IP, perform the following steps:

1. Browse to the following directory:

   `/usr/local/cryptocard/freeradius`
2. Open the **cryptocardFreeRadiusConfig** file with a text editor.
3. In **section 16**, change the IP to the IP setting prior to SAS upgrade.

4. If the **FreeRADIUS Agent** is not using SSL, skip this step and proceed to step 5. If **FreeRADIUS Agent** is connecting to the TokenValidator via SSL, verify the following:
   - **Section 17** is set to TCP port **443**. If not, change accordingly.
   - Section **20** has a value of **1**. If not, change accordingly.
5. In **section 24**, change the IP to the IP setting prior to SAS upgrade.
6. If the **FreeRADIUS Agent** is not using SSL, skip this step and proceed to step 7. If the FreeRADIUS agent is connecting to TokenValidator via SSL, verify the following:

   Section 25 is set to TCP port **443**. If not, change accordingly.

   Section 28 has a value of **1.** If not, change accordingly.
7. If any changes were made, save the file and restart the **RADIUSD** daemon:

   `/etc/init.d/radiusd restart`
8. Use the **tail** command with the **radiusd.log** to verify the changes are working correctly:

   `tail –fv /opt/freeradius/freeradius-server-<version>/var/log/radiusd/radiusd.log`

FreeRADIUS Updater

If FreeRADIUS Updater is configured with DNS, continue with the **Internal DNS** section below, followed by “DNS Routing”. If configured with IP, visit **IP Routing**.

Internal DNS

In the section **Internal**, you were instructed to change the DNS routing of the FreeRADIUS Updater Service DNS to route to the Primary FreeRADIUS Updater Service IP. This change needs to be reverted to the original setting. Login to your internal DNS domain and revert the IPs associated with the FreeRADIUS Updater Service DNS to the original settings.

DNS Routing

If FreeRADIUS Updater is utilizing DNS in the FreeRADIUS agent, perform the following steps:

1. Browse to the following directory:

   `/usr/local/cryptocard/freeradius_updater/dynamicUpdate/`
2. Open the **sslConfigurationClient.txt** file with a text editor.
3. In **section 20**, change the two DNS settings to the DNS names prior to SAS upgrade.
4. Once changes are made, save the file and restart the **FreeRADIUS Updater** daemon:

   `/etc/init.d/./freerad_updaterservice restart`
5. Check the **freeRadupdateClient-year-month-day.log** file for any errors. The log file is located in:

   `/usr/local/cryptocard/freeradius_updater/log/`
6. Verify that Auth Nodes added in SAS PCE/SPE are loading correctly in **clients.conf**:

   `/opt/freeradius/freeradius-server-<version>/etc/raddb/`

IP Routing

If FreeRADIUS Updater is utilizing IP in the FreeRADIUS agent, perform the following steps:

1. Browse to the following directory:
   `/usr/local/cryptocard/freeradius_updater/dynamicUpdate/`
2. Open the **sslConfigurationClient.txt** file with a text editor.
3. In section 20, change the two IPs to the IP settings prior to SAS upgrade.
4. Once these changes are made, save the file and restart the FreeRADIUS updater daemon:
   `/etc/init.d/./freerad_updaterservice restart`
5. Check the **freeRadupdateClient-year-month-day.log** file for any errors. The log file is located in:
   `/usr/local/cryptocard/freeradius_updater/log/`
6. Verify that the Auth Nodes added in SAS PCE/SPE are loading correctly in the **clients.conf** file:
   `/opt/freeradius/freeradius-server-<version>/etc/raddb/`

5
SafeNet Authentication Service Post-Upgrade Checklist

After SAS is upgraded in both the Primary and Secondary data centers, it is recommended to verify the SAS configuration from both the Primary and Secondary SAS Consoles (SYSTEM level). It is also recommended to perform a final round of testing for authentication(s) that SAS is processing.

Configuration Verification

1. Connect to both the Primary and Secondary SAS servers hosting the SAS Console.
2. Open a browser and browse to the SAS Console (using an internal IP address; for example, https://localhost/console).
3. Login with local/domain admin credentials to the SYSTEM Level.
4. Click **SYSTEM > Setup**. Verify that the configuration is unchanged for the following:
   - Permit LDAP
   - FreeRADIUS Synchronization
5. Click **SYSTEM > Communications**. Verify that the configuration is unchanged for the following:
   - SMS Settings
   - E-mail Settings
   - Operator E-mail Validation URL
   - Shibboleth Agent Settings

Authentication Testing

- **Console Login** – Login to an SAS virtual server account and verify that each tab (On-Boarding, Virtual Servers, Snapshot, Reports, etc.) is displaying information properly.
- **RADIUS** – Verify that RADIUS authentication can be performed against a virtual server and that customers are authenticating against both the Primary and Secondary data centers.
- **Shibboleth** – Verify that SAML authentication can be performed against a virtual server, and ensure authentication is functioning properly.
- **TokenValidator** – Verify that Token Validator authentication can be performed against a virtual server, and that customers are authenticating against both the Primary and Secondary data centers.

Document PN: 007-012795-005, Rev. A,

Windows Registry Changes (Optional)

If any SAS Windows Registry settings were changed prior to the upgrade, verify that these changes are still in place by going to the following Windows Registry location. This check needs to be performed on each SAS server.

HKEY_LOCAL_MACHINE\SOFTWARE\CRYPTOCard\BlackShield ID

6
Additional Considerations

SafeNet Authentication Service Table Management

Due to the large volume of the data accumulated over time in the **SourceUserslog** table, it is recommended that the table is truncated, or undergo table rotation, to improve SAS performance.

SafeNet Authentication Service Logging Service

In SAS, data stored in the database is displayed within the user interface. SAS provides the ability to pull data in near real-time (Authentication and Operator Activity) from SAS to an SAS Remote Logging Agent. The agent can then push the data to display in several formats (Event Viewer, syslog, SIEM (ArcSight), or log file).

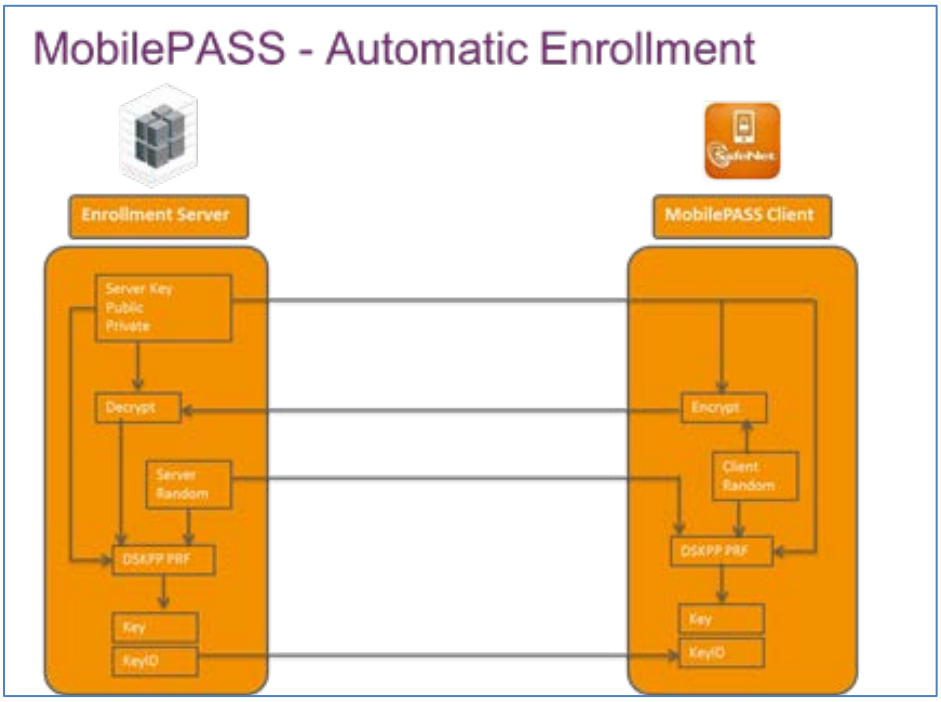
The logging service in SAS must be configured in a way similar to the SAS Synchronization Agent. For more information, refer **SAS Remote Logging Agent Documentation**.

Once SAS has been configured, it is recommended that DNS record(s) be created that are mapped back to SAS.

MobilePASS

SAS supports Gemalto's MobilePASS software token, as well as the next-generation MobilePASS+. MobilePASS and MobilePASS+ provide one-step installation, along with highly secure standards-based activation.

This token uses a provisioning method called Dynamic Symmetric Key Provisioning Protocol (DSKPP).



(Image based on principal data flow for DSKPP key generation using a public server key – RFC 6063.)

Key Facts – MobilePASS and MobilePASS+ Enrollment

- Enrollment occurs via SSL.
- In order to enroll, the server sends the username for the user and the enrollment password encoded in a URL or an activation code via an email.
- The enrollment URL and the enrollment password are per-user passwords stored encrypted in a user's personalization data attributes.
- It can also be configured with an expiration date/time.
- It never crosses the wire in clear text; it is hashed with other protocol data, including random data sent to the server protected with public key cryptography.
- The resulting hash is only valid for that session and cannot be used by an attacker in another session.
- Once enrolled, the password is deleted from the SAS back end, allowing no other enrollments to re-use it.

> **NOTE**: Password communication and delivery to the customer can be implemented in a secure fashion using out-of-band channels (for example, SMS, e-mail, etc.) to registered users only.

Due to the requirement for SSL as part of this enrollment process, the server that handles enrollment must have an SSL certificate installed, and it must be trusted by all systems with which you intend to enroll tokens. With this in mind, it is recommended that you use a certificate from a known public Certification Authority (CA) that is trusted by all devices without the need for any device customization. This will simplify the end-user experience and allow enrollment on platforms such as Windows, which, at an OS level, will perform validation on the certificate.