SafeNet Authentication Service

FreeRADIUS Upgrade Guide

Document Information

Document Part Number	007-012796-001, Rev. B
Release Date	October 2014

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

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.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Introduction

Upgrading SAS FreeRADIUS consists of two parts:

- FreeRADIUS Updater (Server/Auth Node Updater) upgrade
- FreeRADIUS Agent upgrade

Any location that contains the word **<version>** denotes the version of FreeRADIUS that is being installed.

Prerequisites

The following prerequisites are required prior to upgrading the SAS FreeRADIUS Agent and FreeRADIUS Updater:

- cryptocard-freeradius-updater rpm package (FreeRADIUS Server <version>)
- cryptocard-freeradius-agent rpm package
- libtool-ltdl must be installed (x64 if on 64bit Linux)

FreeRADIUS Updater

FreeRADIUS Updater handles all incoming RADIUS authentication for SAS. It also contains a feature where SAS can synchronize Auth Nodes to FreeRADIUS. This reduces the administrative overhead involved with manually adding an Auth Node and RADIUS client entry in SAS and FreeRADIUS respectively.

Prerequisites

The following prerequisites are required prior to upgrading SAS FreeRADIUS Updater:

- cryptocard-freeradius-updater rpm package (FreeRADIUS Server <version>)
- libtool-ltdl must be installed (x64 if on 64-bit Linux)

Upgrading FreeRADIUS Updater

The following steps must be performed on all FreeRADIUS servers deployed with SAS:

1. Log on to the SAS FreeRADIUS server, and then switch to root.
2. Stop the FreeRADIUS daemon (**radiusd**) and updater (**freerad_updaterservice**):

   /etc/init.d/radiusd stop

   /etc/init.d/freerad_updaterservice stop
3. Uninstall the **cryptocard-freeradius-updater RPM** package.

   Verify the packages that are installed:

   rpm –qa | grep cryptocard*

4. Uninstall the **cryptocard-freeradius-updater RPM** package:

   rpm -e <cryptocard-freeradius-updater version listed above>

5. Rename the residual directories:

   mv /usr/local/cryptocard/freeradius_updater /usr/local/cryptocard/freeradius_updater.<SAS version>

   mv /opt/freeradius /opt/freeradius.<SAS version>

6. Change to the directory where the new **FreeRADIUS Updater RPM** is located, and then type the following command:

   rpm -ivh cryptocard-freeradius-updater*.rpm

7. Change to the directory **/opt/freeradius/freeradius-server-<version>/sbin**, and then type the following command:

   ./radiusd –Xx

NOTE: This step is required to configure FreeRADIUS for the first time. If **radiusd** fails start, perform the following steps:

a. Change to the **/etc/ld.so.conf.d** directory, and then type the following command:

   vi freeradius-server-2.2.0-x86_64.conf

b. Add the following line:

   /opt/freeradius/freeradius-server-2.2.0/lib64/

c. Save the file.

d. Repeat step 7. If startup fails, stop the daemon (hold down **Ctrl+C**) and then run it again.

8. Hold down **Ctrl+C** to stop the **FreeRADIUS server** that is running in **debug** mode.

9. Use the following command to copy **rc.radiusd** (the FreeRADIUS startup script) to the **/etc/init.d** directory (if prompted, overwrite the existing file):

   cp /opt/freeradius/freeradius-server-<version>/sbin/rc.radiusd /etc/init.d/radiusd

10. Modify the **radiusd** daemon:

    a. Change to the **/etc/init.d** directory

    b. Open the **radiusd** daemon with a text editor.

    c. Add the following lines below the line **#!/bin/sh**:

       # chkconfig: 2345 88 10

       # Description: Start/Stop the RADIUS Server daemon

    d. Save the daemon.

11. Use the following command to add **radiusd** to the runlevels:

    chkconfig --add radiusd

12. Modify the **radiusd.conf** file as follows:

    a. Change to the following directory: **/opt/freeradius/freeradius-server-<version>/etc/raddb**

    b. Open the **radiusd.conf** file with a text editor.

c. In the **log** section, make the following changes:

- destination = files (line 376)
- auth = yes (line 443)
- auth_badpass = yes (line 451)
- auth_goodpass = no (line 452)

d. Save the file.

13. Modify the **sslConfigurationClient.txt** file:

a. Change to the following directory:

/usr/local/cryptocard/freeradius_updater/dynamicUpdate

b. Open the **sslConfigurationClient.txt** file, and verify/change the following:

- **Section 6** – Change the value to **4 (DEBUG)**
- **Section 17** – Verify the path as: **/opt/freeradius/freeradius-server-<version>/etc/raddb/clients.conf**
- **Section 20** – Change the **127.0.0.1** IP address to the following:
  - Primary SAS FreeRADIUS Updater Service IP/DNS
  - Secondary SAS FreeRADIUS Updater Service IP/DNS

NOTE: This step must be performed on all SAS FreeRADIUS servers. If there are FreeRADIUS servers in each data center, the configuration should point to its own SAS FreeRADIUS Updater Service as the primary.

c. Save the file.

14. Restart the FreeRADIUS daemon (**radiusd**) and updater (**freerad_updaterservice**):

/etc/init.d/freerad_updaterservice restart

/etc/init.d/radiusd restart

15. Verify that there are no errors in the following log files:

- **/opt/freeradius/freeradius-server-<version>/var/log/radius/radius.log**
- **/usr/local/cryptocard/freeradius_updater/log/freeRadupdateClient-date.log**

16. In SAS, add an Auth Node to a Virtual Server.
17. Restart the **freerad_updaterservice** daemon, or wait five minutes, for the Auth Node to become active.
18. Stop the FreeRADIUS daemon:

/etc/init.d/radiusd stop

FreeRADIUS Agent Upgrade

Prerequisites

The following prerequisite is required prior to upgrading the SAS FreeRADIUS Agent:

- cryptocard-freeradius-agent rpm package

Upgrading FreeRADIUS Agent

Perform the steps below on all FreeRADIUS servers deployed with SAS:

1. Log on to the SAS FreeRADIUS server, and then switch to root
2. Uninstall the **cryptocard-freeradius-agent RPM** packages:
   a. Use the following command to verify the packages that are installed:

      rpm –qa | grep cryptocard*

   b. Run the following command to uninstall the **cryptocard-freeradius-agent RPM** package:

      rpm -e <cryptocard-freeradius-agent version listed above>

   c. Rename the residual directories:

      mv /usr/local/cryptocard/freeradius /usr/local/cryptocard/freeradius.<SAS version>
3. Install the new FreeRADIUS Agent RPM:
   a. Go to the directory where the new **FreeRADIUS Agent RPM** is located and type the following command:

      rpm –ivh cryptocard-freeradius-agent-*.rpm

   b. Change to the following directory:

      /usr/local/cryptocard/freeradius

   c. Extract the files rlm_challAvecAuth-versions.tar and rlm_mschap-versions.tar:

      for i in *.tar; do tar -xvf $i; done

   d. Change to the following directory:

      /usr/local/cryptocard/freeradius/rlm_challAvecAuth-versions

   e. Copy **rlm_challAvecAuth-<version>.so** to the following directory:

      cp rlm_challAvecAuth-<version>.so /opt/freeradius/freeradius-server-<version>/lib64/
4. Once the **rlm_challAvecAuth-<version>.so** file has been copied to **/opt/freeradius/freeradius-server-<version>/lib64/**, the owner and group membership permissions need to be set. The permissions must be similar to other files in the directory.

   For example:

   -rwxr-xr-x 1 root root rlm_challAvecAuth-2.2.0.so

5. Change to the following directory:

   /opt/freeradius/freeradius-server-<version>/lib64/

   Type the following commands:

   rm rlm_challAvecAuth.so

   ln -sv /opt/freeradius/freeradius-server-<version>/lib64/rlm_challAvecAuth-<version>.so /opt/freeradius/freeradius-server-<version>/lib64/rlm_challAvecAuth.so

6. Change to the following directory and open the file **dictionary.freeradius.internal** with a text editor:

   /opt/freeradius/freeradius-server-<version>/share/freeradius

7. Verify that the **Auth-Type** definition for **challAvecAuth** exists. If it does not exist, add the following line below the line **VALUE Auth-Type MSCHAP-V2 1034:**

   VALUE Auth-Type challAvecAuth 1035

8. Run the following command to copy the **challAvecAuth** file from **/usr/local/cryptocard/freeradius/** to **/opt/freeradius/freeradius-server-<version>/etc/raddb/modules/**:

   cp /usr/local/cryptocard/freeradius/challAvecAuth /opt/freeradius/freeradius-server-<version>/etc/raddb /modules/

9. Modify the **default** file:

   a. Go to the following location:

      /opt/freeradius/freeradius-server-<version>/etc/raddb/sites-enabled/

   b. Open the **default** file with a text editor. Locate **auth_log** in the **authorize** section and add the following line below **auth_log**:

      challAvecAuth

      Example:

      ```
      #  If you want to have a log of authentication requests,
      #  un-comment the following line, and the 'detail auth_log'
      #  section, above.
#       auth_log
      challAvecAuth
      ```

c. In the **default** file, in the **authenticate** section, and add the following line below **pam**:

Auth-Type challAvecAuth {

challAvecAuth

}

Example:

```
# Pluggable Authentication Modules.
# pam
Auth-Type challAvecAuth {
        challAvecAuth
}
```

d. Save the file.

10. Modify the **mschap** file:

a. Change to the following directory:

/opt/freeradius/freeradius-server-<version>/lib64/

b. Back up the existing **rlm_mschap-2.2.0.so** by running the following command:

mv rlm_mschap-2.2.0.so rlm_mschap-2.2.0.so.orig

c. Change to the following directory:

/usr/local/cryptocard/freeradius/rlm_mschap-versions

d. Copy the **rlm_mschap-<version>.so** file to the **/opt/freeradius/freeradius-server-<version>/lib64/** directory:

cp rlm_mschap-<version>.so /opt/freeradius/freeradius-server-<version>/lib64

e. Once the **rlm_mschap-<version>.so** has been copied, the owner and group membership permissions need to be set on **rlm_mschap-<version>.so**. The permissions must be similar to other files in the directory:

For example:

-rw-r----- 1 root root rlm_mschap-2.2.0.so

f. Change to the following directory and open the **mschap** file with a text editor:

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

g. Locate and verify that the settings below are not commented and that the values are set to **yes**. Add the values to the file if they do not exist:

- use_mppe = yes
- require_encryption = yes

h. In the **mschap** file, locate and verify that the settings below are not commented and that the values are set to **yes**. Add the values to the file if they do not exist:

- external_module = yes
- mschap_success_pack_limit_len = yes

Example:

```
#
use_mppe = yes

# if mppe is enabled require_encryption makes
# encryption moderate
#
require_encryption = yes
external_module = yes
mschap_success_pack_len = yes
```

i. Save the file.

11. Create a symbolic link from **libchallAvecAuthImplement.so** to **/usr/local/cryptocard/freeradius/lib/librlm_mschap_external.so.1** using the following command:

    ln -sv /usr/local/cryptocard/freeradius/lib/libchallAvecAuthImplement.so /usr/local/cryptocard/freeradius/lib/librlm_mschap_external.so.1

12. Modify the **cryptocardFreeRadiusConfig** file:

    a. Change to the following directory:

    /usr/local/cryptocard/freeradius/

    b. Open the **cryptocardFreeRadiusConfig** file with a text editor, and change the following:

    - **Section 7** - Change to **1**
    - **Section 9** - Change to **2**
    - **Section 16** – Change IP address to the following:
        - Primary FreeRADIUS(s)
            - Primary TokenValidator IP/DNS
        - Secondary FreeRADIUS(s)
            - Secondary TokenValidator IP/DNS

    If SAS TokenValidator requires an SSL connection, continue below. If it is not using SSL, continue to the next step.

    - **Section 17** – Change to **443**
    - **Section 20** – Change to **1**
    - **Section 24** – Change IP address to the following:
        - Primary FreeRADIUS(s)
            - Secondary TokenValidator IP/DNS
        - Secondary FreeRADIUS(s)
            - Primary TokenValidator IP/DNS

    If SAS TokenValidator requires an SSL connection, please continue below. If it is not using SSL, continue to the next step.

    - **Section 25** – Change to **443**
    - **Section 28** – Change to **1**

    c. Save the file.

13. Restart the **radiusd** daemon:
    a. Run the following command:

       /etc/init.d/radiusd restart

    b. Verify that the **radiusd** daemon has launched properly in one of the following log files:
       - opt/freeradius/freeradius-server-<version>/etc/var/log/radiusd/radius.log
       - /var/log/messages
14. Delete the directories **rlm_challAvecAuth-versions** and **rlm_mschap-versions** using the following commands:

    rm –fR /usr/local/cryptocard/freeradius/rlm_challAvecAuth-versions

    rm –fR /usr/local/cryptocard/freeradius/rlm_mschap-versions
15. Confirm a successful update by performing the following tasks:
    - Verify a successful RADIUS authentication attempt against the added SAS Auth Node.
    - Verify a successful PIN change via RADIUS.

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.	