SAS FreeRADIUS Updater

Configuration Guide

SafeNet
THE DATA PROTECTION COMPANY

Document Information

Product Version	SAS FreeRADIUS Updater 1.04
Document Part Number	007-012472-001, Revision E
Release Date	February 2015

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

Installing and Configuring FreeRADIUS Updater

FreeRADIUS is a common open source RADIUS server. It is customizable and free for download from the Internet.

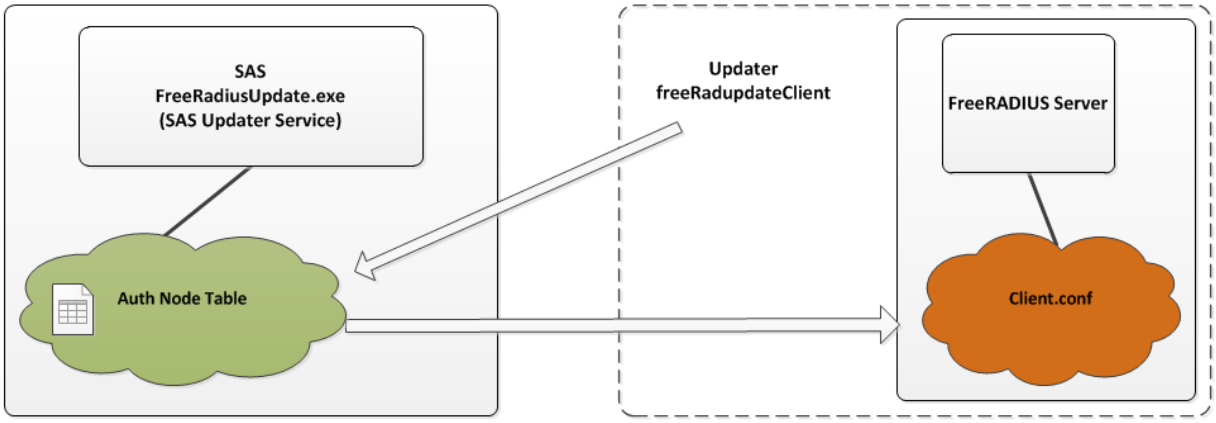
The FreeRADIUS Server software is applied by installing the following patch:

/usr/local/cryptocard/freeradius_updater/freeradius-server-2.2.0p1.patch

When receiving Linux real-time signal 39, the software is able to read the following:

/opt/freeradius/freeradius-server-2.2.0/etc/raddb/clients.conf

The in-memory **clients.conf** file is updated when receiving authentication requests.



NOTE: FreeRADIUS Server may be used to customize rlm modules, such as Cryptocard FreeRADIUS Agent software.

Installing FreeRADIUS Updater on Linux

Installing FreeRADIUS Updater on Linux requires accessing RPM.

cryptocard-freeradius-updater-1.04.0017-27622.x86_64.rpm

cryptocard-freeradius-updater-1.04.0017-27622.i686.rpm

The above process installs the following:

- **FreeRADIUS Server** – /opt/freeradius/freeradius-server-2.2.0
- **FreeRADIUS Updater Agent** - /usr/local/cryptocard/freeradius_updater

Upgrading FreeRADIUS Updater on Linux

To upgrade FreeRADIUS Updater, do one of the following:

- Install FreeRADIUS Updater from the RPM package; the installed version will be updated.
- Uninstall the previous version and install the new version.

Configuring FreeRADIUS Updater

To configure the FreeRADIUS Agent:

1. On the Linux server, enter the following to go to the FreeRADIUS Updater folder:

   cd /usr/local/cryptocard/freeradius_updater

2. Enter the following to view the contents of the FreeRADIUS Updater folder:

   [root@localhost freeradius_updater]# **ls -l**
   total 6432
   -rw-r--r-- 1 root root 9668 Nov 11 23:03 CRYPTOCard-license.txt
   drwxr-xr-x 2 root root 4096 Feb 18 11:54 dynamicUpdate
   -rw-r--r-- 1 root root 114005 Nov 11 23:03 freeradius-server-2.2.0p1.patch
   -rw-r--r-- 1 root root 3768017 Nov 11 23:08 freeradius-server-2.2.0.tar.bz2
   -rwxr-xr-x 1 root root 45064 Nov 11 23:07 freeRadupdateClient
   -rwxr-xr-x 1 root root 2253 Nov 11 23:03 freerad_updaterPostInstall.sh
   -rw-r--r-- 1 root root 1019 Nov 11 23:03 freerad_updaterPreUninstall.sh
   -rwxr-xr-x 1 root root 5432 Nov 11 23:03 freerad_updaterservice
   lrwxrwxrwx 1 root root 18 Feb 18 11:41 libcrypto.so -> libcrypto.so.1.0.0
   -rwxr-xr-x 1 root root 2115077 Nov 11 23:07 libcrypto.so.1.0.0
   lrwxrwxrwx 1 root root 15 Feb 18 11:41 libssl.so -> libssl.so.1.0.0
   -rwxr-xr-x 1 root root 471501 Nov 11 23:08 libssl.so.1.0.0
   drwxr-xr-x 2 root root 4096 Feb 25 18:16 log
   drwxr-xr-x 2 root root 4096 Feb 18 11:41 Open Source Licenses
   drwxr-xr-x 2 root root 4096 Feb 18 11:41 secretKeys

- The updater file **freeRadupdateClient** (located in the Updater folder) communicates with the **freeRadupdateServer.exe** file (located on the SAS Server using an authenticated SSL tunnel on TCP/IP). The **freeRadupdateClient** file is managed by the **/etc/init.d/freerad_updaterservice** shell script, which performs management tasks such as system-boot time, start, and stop.
- The Updater checks the server every 300 seconds (the default setting) for updates, which can be changed by modifying the value in the Updater configuration file (Section 19).

3. To configure the **freeRadupdateClient** file, edit the following file:

   /usr/local/cryptocard/freeradius_updater/dynamicUpdate/sslConfigurationClient.txt

   The **freeRadupdateClient** file has a total of 21 sections, of which only the following may be modified:

   - Section 6 – Log level
   - Section 20 – Number of Servers (SAS addresses)

   NOTE: A restart is required after configuring the sslConfigurationClient.txt file.

   To restart the service run the following: **/etc/init.d/freerad_updaterservice restart**

Modifying sslConfigurationClient.txt

Modify the file **sslConfigurationClient.txt** to set the frequency for contacting SAS to pull down Auth Nodes.

> **NOTE:** If there is both a primary and a secondary FreeRADIUS Updater installation, perform the following instructions on both.

To modify the FreeRADIUS Updater sslConfigurationClient.txt file:

1. Go to: **/usr/local/cryptocard/freeradius_updater/dynamicUpdate/**, and open the file **sslConfigurationClient.txt** with an editor.
2. Go the following sections and change the following values:
   - **Section 4**: Ensure that the value is **Cipher unused**
   - **Section 6**: Change **value** from **1 (Error)** to **4 (Debug)**.
   - **Section 9**: Ensure that the value is **TLS Version**. **Values are: 1.1, 1.2, match server**
   - **Section 19**: Change **value** from **300** to **60**.
   - On the primary FreeRADIUS server, in **section 20**, change the following:

Default Value	Modified Value
2	2
127.0.0.1	**IP of Primary SAS Server**
5041	5041
5	5
500	500
127.0.0.1	**IP of Secondary SAS Server**
5041	5041
5	5
500	500

   - On the secondary FreeRADIUS server, in **section 20**, change the following:

Default Value	Modified Value
2	2
127.0.0.1	**IP of Secondary SAS Server**
5041	5041
5	5
500	500
127.0.0.1	**IP of Primary SAS Server**
5041	5041
5	5
500	500

3. Save the file and exit the editor.
4. Run the following command to restart the *freerad_updaterservice* daemon:

   /etc/init.d/freerad_updaterservice restart

Configuring SAS

Increasing the Number of Authentication Nodes

The maximum number of Auth Nodes can be increased by selecting **On Boarding > Manage: Account Name > Services**.

> **NOTE:** Defining this parameter determines the maximum number of IPs that can be put into the Auth Nodes table.

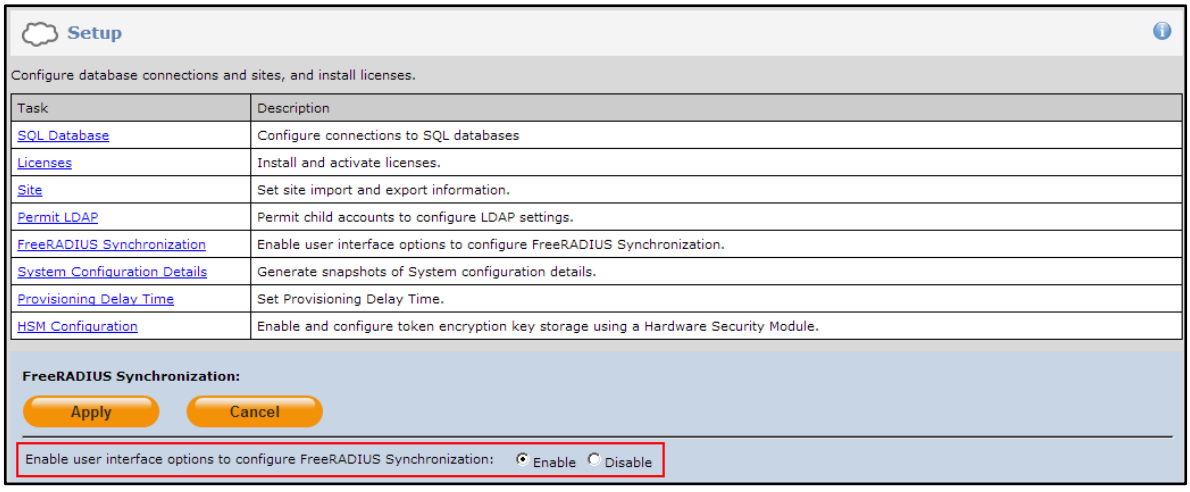
Enabling Synchronization

FreeRADIUS synchronization must be enabled for the Updater functionality to be configured and to work properly.

> **NOTE:** Ensure that you log on as an administrator when enabling synchronization.

To enable synchronization:

1. Click **System > Setup**.
2. Click **FreeRADIUS Synchronization**.



3. For the **Enable user interface options to configure FreeRADIUS Synchronization** option, select **Enable**.
4. Click **Apply**.

Modifying sslConfigurationServer.txt

Modify **sslConfigurationServer.txt** to allow the FreeRADIUS Updater Agent to connect and ask for Auth Node updates.

> **NOTE:**
>
> If there is both a primary and secondary FreeRADIUS Updater installation, perform the following instructions on both.

To modify the FreeRADIUS Updater sslConfigurationServer.txt file:

1. On the SAS server, go to **\<BlackShield installation path>\freeradconfig\bin\DynamicUpdateConfig**, and open **sslConfigurationServer.txt** with an editor.
2. Change the following values:
   - **Section 6**: Change value from **1 (Error)** to **4 (Debug)**.
   - **On the primary SAS server, section 7:** Change value from **127.0.0.1** to the IP of the primary SAS server.
   - **On the secondary SAS server, section 7:** Change value from **127.0.0.1** to the IP of the secondary SAS server.
   - **On the primary SAS Server, section 21:** Change the following:

Default Value	Modified Value
2	2
127.0.0.1	**IP of Primary SAS Server**
0	0
80	80
/freeradconfig/getFreeRadConfiguration.asmx	/freeradconfig/getFreeRadConfiguration.asmx
\secretKeys\RemoteSite.bsidkey	\secretKeys\RemoteSite.bsidkey
10	10
400	400
127.0.0.1	**IP of Secondary SAS Server**
0	0
80	80
/freeradconfig/getFreeRadConfiguration.asmx	/freeradconfig/getFreeRadConfiguration.asmx
\secretKeys\RemoteSite.bsidkey	\secretKeys\RemoteSite.bsidkey
10	10
400	400

- On the secondary SAS Server, section 21, change the following:

Default Value	Modified Value
2	2
127.0.0.1	**IP of Secondary SAS Server**
0	0
80	80
/freeradconfig/getFreeRadConfiguration.asmx	/freeradconfig/getFreeRadConfiguration.asmx
\secretKeys\RemoteSite.bsidkey	\secretKeys\RemoteSite.bsidkey
10	10
400	400
127.0.0.1	**IP of Primary SAS Server**
0	0
80	80
/freeradconfig/getFreeRadConfiguration.asmx	/freeradconfig/getFreeRadConfiguration.asmx
\secretKeys\RemoteSite.bsidkey	\secretKeys\RemoteSite.bsidkey
10	10
400	400

3. Save and close the file.
4. Ensure that this is done on both the Primary and the Secondary SAS servers.
5. Restart the **BlackShield ID FreeRADIUS Service** in Windows Services.

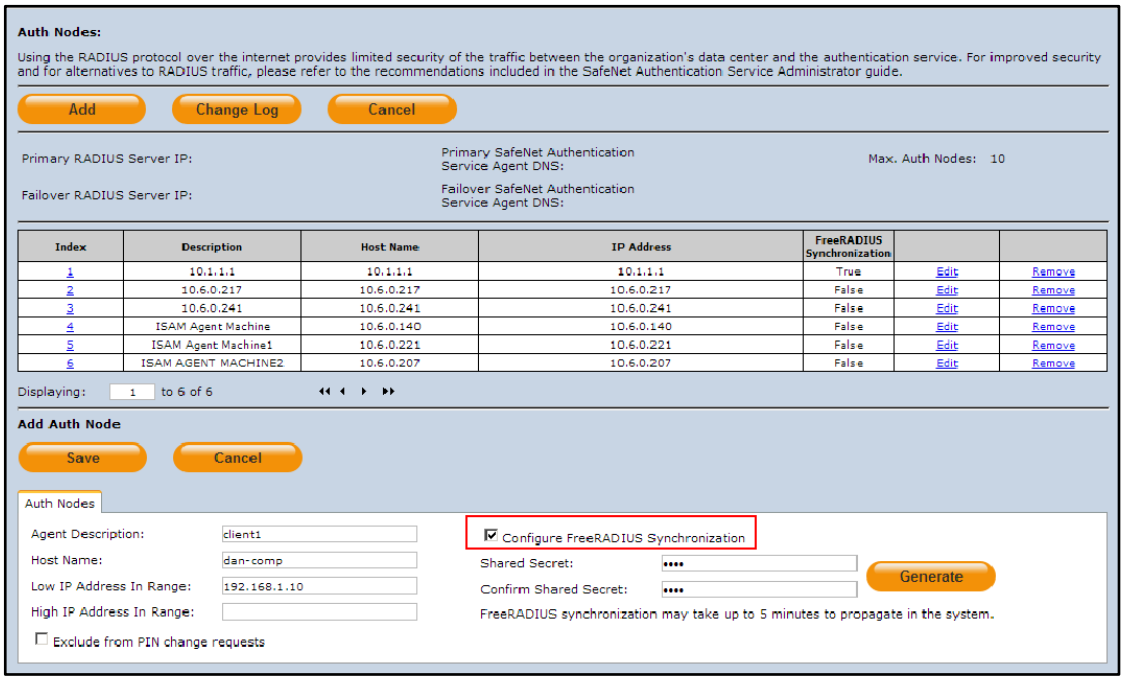
Adding Auth Nodes

Auth Nodes can be added, deleted, or edited using Virtual Servers.

To add auth nodes:

1. Click **VIRTUAL SERVERS**.
2. Select the account from the **Managed Account List**.
3. Click **COMMS > Auth Nodes > Auth Nodes**.

NOTE: Verify that the **Configure FreeRADIUS Synchronization** check box is selected. This ensures that the FreeRADIUS Updater will sync this Auth Node record.



4. Click **Add**.
5. Create Auth Nodes for both the Primary and Secondary FreeRADIUS Agents.

Accessing BlackShield ID FreeRADIUS Service

The FreeRADIUS Service accesses the **http://127.0.0.1/freeradconfig/getFreeRadConfiguration.asmx** web service, which is accessible only from the local machine and always runs on the SAS server.

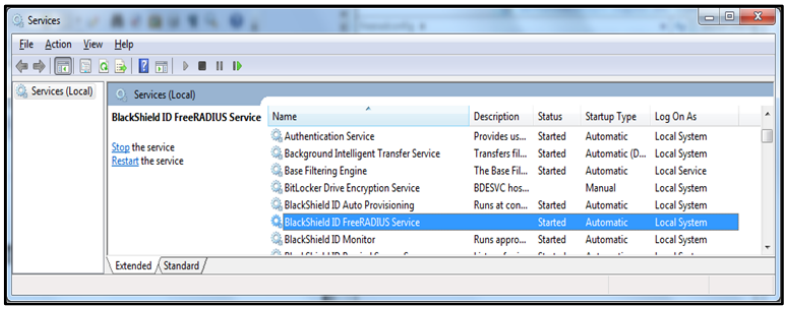
All files relevant to the FreeRADIUS Service are located in:

C:\Program Files\CRYPTOCard\BlackShield ID\freeradconfig

> **NOTE:** A restart is required after configuring the FreeRADIUS Service.

To access the Windows Service:

1. Open **Windows Task Manager**.
2. Select **Services > Services**.



3. Click **BlackShield ID FreeRADIUS Service** and then click **Restart the service**.

Verifying Synchronization

To ensure that the Updater is working correctly:

1. Check the log files for sync success messages:

   /usr/local/cryptocard/freeradius_updater/log/freeRadupdateClient - <date>.log

2. Check the **client.conf** file and ensure that your SAS Auth Node records are added to the end of the file.

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.	