SafeNet Authentication Service
Configuration Guide

SAS Agent for PEAP
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012980-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>30 March, 2015</td>
</tr>
</tbody>
</table>

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

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.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
Contents

Introduction........................................................................................................................................... 4
Third-Party Software Acknowledgement ................................................................................................. 4
Overview................................................................................................................................................ 4
About PEAP ............................................................................................................................................ 4
Sign-On Dataflow .................................................................................................................................. 5
PEAP Checklist ..................................................................................................................................... 6
SAS Agent for PEAP ............................................................................................................................... 6
  Configuring the SAS Agent for PEAP ..................................................................................................... 6
  Install the SAS Agent for PEAP ............................................................................................................ 6
Configuring FreeRADIUS ..................................................................................................................... 9
  Modify the eap.conf File ....................................................................................................................... 11
  Modify the Clients.conf File .................................................................................................................. 11
  Modify the Proxy.conf File ................................................................................................................... 12
Start the FreeRADIUS Service ............................................................................................................. 12
SAS Agent for PEAP Security Recommendations ............................................................................. 13
FreeRADIUS Installation ..................................................................................................................... 14
FreeRADIUS Configuration .................................................................................................................. 15
  Users ................................................................................................................................................... 15
Solution Configuration .......................................................................................................................... 17
  Configuring Certificates ....................................................................................................................... 17
Defining a RADIUS Server ................................................................................................................... 26
Defining PEAP ....................................................................................................................................... 27
Defining the SafeNet FreeRADIUS Agent ............................................................................................. 27
Defining FreeRADIUS in SAS ............................................................................................................... 28
Troubleshooting .................................................................................................................................... 29
  FreeRADIUS Testing .......................................................................................................................... 29
Support Contacts .................................................................................................................................... 31
Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software. Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Overview

This document describes how to use SafeNet Authentication Service (SAS) strong authentication with the Protected Extensible Authentication Protocol (PEAP) using the SafeNet Agent for PEAP.

This document assumes that the communication between a VPN server and mobile devices environment is already configured and working with Protected Extensible Authentication Protocol (PEAP) prior to implementing SAS strong authentication.

About PEAP

The Protected Extensible Authentication Protocol (PEAP) is a common authentication protocol for communication between a VPN server and mobile devices. PEAP encloses the Extensible Authentication Protocol (EAP) within an encrypted and authenticated TLS tunnel.

FreeRADIUS has a built-in feature to locally terminate the Transport Layer Security (TLS) outer tunnel, decrypt the PEAP tunnel, and then extract the inner identity to proxy the MS-CHAPv2 authentication mechanism to another RADIUS server.

PEAP creates two concentric tunnels:

- An encrypted and authenticated TLS outer tunnel
- An inner tunnel that uses an EAP method (such as EAP-MS-CHAPv2) for authentication, and is protected by the TLS outer tunnel
Sign-On Dataflow

The SafeNet Authentication Service (SAS) Agent for PEAP delivers a customized FreeRADIUS version 2.1.10 application running on a Windows platform preconfigured to terminate Phase 1 outer identity and to proxy an MS-CHAPv2 authentication mechanism to another RADIUS server.

A user wants to log on to his organization through a VPN solution using sign-on capabilities embedded in the organization’s SafeNet Authentication Service solution.

1. The VPN client collects the user’s credentials and passes them to the VPN server.
2. The VPN server forwards the request to the FreeRADIUS server (included in the SafeNet Agent for PEAP) through the RADIUS protocol. The FreeRADIUS server is EAP compatible.
3. The SafeNet Agent for PEAP unwraps the EAP and forwards MSCHAPv2 to the SAS FreeRADIUS agent.
4. The SAS FreeRADIUS agent generates an API call to SAS over an https tunnel.
5. SAS evaluates the user’s credentials and returns an “accept” or “reject” response to the FreeRADIUS agent.
6. The FreeRADIUS agent forwards SAS’s response to return an “accept” or “reject” response to the SAS Agent for PEAP.
7. The SAS Agent for PEAP sends a RADIUS Access “accept” or “reject” response to the VPN server.
8. If the OTP value is valid and the user conforms to the remote access policies, the user is authorized and a RADIUS Access “accept” response is returned. If the OTP value is not valid, or the user does not meet the remote access policies, the user is not authorized and a RADIUS Access “reject” response is returned.
PEAP Checklist

Perform the following steps to enable Protected Extensible Authentication Protocol (PEAP) authentication:

- Install and configure the SAS Agent for PEAP
- Configure FreeRADIUS
- Configure certificates
- Define a RADIUS Server
- Define PEAP
- Define a VPN server and client settings

SAS Agent for PEAP

Configuring the SAS Agent for PEAP

The required steps for using the SAS Agent for PEAP are as follows:

- Install the SAS Agent for PEAP
- Convert certificate files using OpenSSL
- Modify the `eap.conf` file
- Modify the `clients.conf` file
- Modify the `proxy.conf` file
- Start the FreeRADIUS service

Install the SAS Agent for PEAP

To install the SAS Agent for PEAP:

1. Run the file `SafenetPEAPPackage-8.0-sp4.msi.msi`
2. On the Welcome window, click Next.
3. On the **Plug-In Selection** window, select **OTP Plug-In for PEAP**, and then click **Install**.

![Plug-In Selection Window](image)

4. On the **Welcome** window, click **Next**.

![Welcome Window](image)
5. On the **License Agreement** window, select **I accept the license agreement**, and then click **Next**.

6. On the **Destination Folder** window, accept the default folder or use the **Browse** button to select a different folder. When ready, click **Next** to continue.
7. The installation process begins. When the **Completing SafeNet OTP Plug-in Package 8.2 Setup Wizard** window is displayed, click **Finish**.

![Completing SafeNet OTP Plug-in Package 8.2 Setup Wizard](image)

**Configuring FreeRADIUS**

The **SAS Agent for PEAP 8.2** installs FreeRADIUS version 2.1.10, preconfigured to handle EAP termination. PEAP requires a server-side certificate to identify the FreeRADIUS server during EAP negotiation.

---

**NOTE:** Information regarding configuring certificates can be found on page 17.

---

FreeRADIUS requires the issuing Root CA certificate. These certificate files should be in **.pem** format and can be placed in the following location:

```
C:\ProgramFiles (x86)\SafeNet\Authentication\SafeNetPEAPpackage\FreeRADIUS\etc\raddb\certs
```

The **SAS Agent for PEAP 8.2** installation delivers the necessary OpenSSL tools to convert your MS CA Root certificate, as well as your FreeRADIUS certificate issued by the same MS CA, into **.pem** format.

1. Before running the OpenSSL commands to convert the files, place both certificate files in the OpenSSL folder:

```
C:\Program Files (x86)\SafeNet\Authentication\SafeNetPEAPpackage\OpenSSL
```

---

**NOTE:** Windows uses the **.pfx** extension by default. Rename the FreeRADIUS certificate file with a **.p12** extension.
2. Launch `openssl.exe` using `cmd` and then browse to:

```bash
C:\Program Files (x86)\SafeNet\Authentication\SafeNetPEAPpackage
```

Disregard the warning message shown below.

```bash
C:\Program Files (x86)\SafeNet\Authentication\SafeNetPEAPpackage\OpenSSL>openssl
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
OpenSSL> pkcs12 -in freeradius.p12 -out freeradius.pem -passin pass:12345678 -passout pass:12345678
MAC verified OK
OpenSSL>
```

**Convert Root CA Certificate to .pem**

**Usage:** `x509 -inform der -in certificate.cer -out certificate.pem`

**Example:** `x509 -inform der -in myca.cer -out myca.pem`

**Convert FreeRADIUS Certificate to .pem**

**Usage:** `pkcs12 -in <.p12 file> -out <.pem file> -passin pass:<.p12 password> -passout pass:<.pem password>`

**Example:** `pkcs12 -in freeradius.p12 -out freeradius.pem -passin pass:1111 -passout pass:1111`

`passin-pfx password`

`passout-pem new password`
Modify the eap.conf File

The file **eap.conf** contains all relevant certificate information required for FreeRADIUS to establish a successful EAP session.

The default path for **eap.conf** is:

C:\Program Files (x86)\SafeNet\Authentication\SafeNetPEAPpackage\FreeRADIUS\etc\raddb\n
In the file, modify lines 155-158 for your FreeRADIUS and RootCA certificates that were prepared using OpenSSL commands.

Modify the Clients.conf File

The file **Clients.conf** contains information regarding RADIUS Clients. The default path to the **Clients.conf** file is:

C:\Program Files (x86)\SafeNet\Authentication\SafeNetPEAPpackage\FreeRADIUS\etc\raddb\n
In the file, specify the SAS server that has FreeRADIUS configured.
Modify the Proxy.conf File

The file **Proxy.conf** contains information on the RADIUS servers that the RADIUS requests are being proxied to. The default path for **Proxy.conf** is:

```
C:\Program Files (x86)\SafeNet\Authentication\SafenetPEAPpackage\FreeRADIUS\etc\raddb\n```

In the file, modify lines 670-674 (realm DEFAULT) and use the same secret that was used in the **Clients.conf** file.

![Proxy.conf file screenshot](image)

**Start the FreeRADIUS Service**

Once all FreeRADIUS configuration has been performed as described in the previous sections, start the FreeRADIUS service from the **Services** snap-in.

![Services snap-in screenshot](image)
SAS Agent for PEAP Security Recommendations

OS Hardening

Security of the RADIUS service absolutely depends on having a secured operating system as a foundation. SafeNet recommends hardening the operating system using your organization’s system administration requirements.

Ownership of raddb

The RADIUS client.conf file contains cleartext shared secrets to authenticate client systems and devices, and therefore must have minimal ownership and access. The /etc/raddb directory (or the equivalent directory containing FreeRADIUS configuration files) must be owned by a domain admin, as well as all files contained in the directory.

To enhance security, it is possible to use SafeNet ProtectDrive for encrypting files on your system.

Permissions for raddb

Allowing write access to the RADIUS DB directory would allow deletion and replacement of the configuration files, which would undermine the entire security of the server configuration. The /etc/raddb directory, and the configuration files in the directory, must be set to read-only access for all users except the domain admin.

Strong Shared Secrets

The security of RADIUS depends heavily on the strength of the shared secret. The shared secret string for each client must be at least 22 characters, but not more than 31 characters. The secret must not use dictionary words, or guessable patterns or variations of words. It should include a variety of special, numeric, and alphabetic characters.

Restricted Network Access

Restricting network access with IP filtering to just those systems or networks that require access reduces the risk of the most common attacks. Restrict network access using host-based IP filtering to the minimum number of networks or systems requiring access.

NOTE:

Refer to the SAS FreeRADIUS Agent Configuration Guide for more information on the FreeRADIUS Agent:
http://bel1web002:9876/Files/35e0f930d3a447bfa27ff701cf8d6bab
FreeRADIUS Installation

1. Use the following commands to start the FreeRADIUS installation:

```
cd /usr/ports/net/freeradius2
make install
```

Accept the default settings unless otherwise instructed.
FreeRADIUS Configuration

Users

1. Run the following command to edit the users file:
   
   cd /usr/local/etc/
   
   su <enter your password>
   
   cd raddb
   
   nano users

2. Add the following to the top of the file:
   
   NULL Proxy-To-Realm := LOCAL
   
   DEFAULT FreeRADIUS-Proxied-To => 127.0.0.1, Proxy-To-Realm := Safeword

3. When prompted, press Ctrl+X and select Yes to save.

4. Do the following to edit the proxy.conf file:
   
   a. Run the command: – nano proxy.conf
   
   b. Page down to the end of the file and paste in the following:
      
      realm LOCAL {
       
      type = radius
       
      authhost = LOCAL
accthost = LOCAL
}

realm Safeword {

type = radius

authhost = 172.16.0.15:1812
accthost = 172.16.0.15:1813
secret = 1234
}

NOTE: You will need to change the authhost, accthost, and secret to match your installation of SAS. Simply use the arrow keys and replace the text in nano. Important! Do not change anything in the LOCAL realm.

c. When prompted, press Ctrl+X and select Yes to save the file.

5. Do the following to edit the clients.conf file:

   a. Run the command: – nano clients.conf

   b. Page down to the end of the file and press the right mouse button to paste in the following:


```
client 172.16.0.5 {

    secret = testing123
    shortname = nms1
}
```

   NOTE: You will need to change the secret to anything you want. You must also change the shortname to the name of your VPN server.

c. When prompted, press Ctrl+X and select Yes to save the file.

6. Do the following to edit the eap.conf file:

   a. Run the command: – nano eap.conf

   b. In the eap section, locate this line:


```
default_eap_type = md5
```

   Change the value to peap.

   c. In the PEAP section, locate this line:


```
proxy_tunneled_request_as_eap = yes
```

   Change the value to no.
d. When prompted, press Ctrl+X and select Yes to save the file.

Solution Configuration

PEAP adds a TLS layer on top of EAP and uses TLS to authenticate the server to the client. To achieve this, the FreeRADIUS server is required to have a server certificate. In this guide, as an example, a Microsoft CA is used, but any other CA can be designated to provide a server certificate.

Configuring Certificates

Configure a Certificate Template from the CA for FreeRADIUS

1. Open the CA snap-in.
2. In the left pane, right-click Certificate Templates and select Manage.
3. In the certificates list, right-click the **Web Server** template and select **Duplicate Template**.

![Certificate Templates Console]

**NOTE:** You can choose any other certificate template that has a Server Authentication EKU.

4. Select **Windows Server 2003 Enterprise** and then click **OK**.

![Certificate Templates Console - Duplicate Template]
5. On the **Properties of New Template** window, enter a name in the **Template display name** field, and then click **Request Handling**.

6. Select the option **Allow private key to be exported**. Click **Apply**, and then click **OK**.
Enable the Certificate Template

1. Open the CA snap-in.

2. In the left pane, right-click **Certificate Templates** and select **New > Enable Certificate template**.

3. On the **Enable Certificate Templates** window, select your certificate template and then click **OK**.
Enroll a Certificate from the CA for FreeRADIUS

To access the certificate enrollment site page:

1. Open a web browser and go to http://<localhost>/certsr, where <localhost> is the name of your company’s CA server.

2. Select Request a Certificate.


4. On the Advanced Certificate Request window, fill in the form with your identity certificate information and then click Submit.

5. When the Certificate Installed window is displayed, you can close the browser.
Exporting the FreeRADIUS Certificate to a pfx (P.12) File

To export the FreeRADIUS Certificate to a pfx (P.12) file:

1. Double-click the identity certificate.
2. On the Details tab, select Copy to File.

- On the Welcome window, click Next.
3. On the Export Private Key window, select Yes, and then click Next.

4. On the Export File Format window, click Next to accept the default .PFX setting.
5. On the **Password** window, enter a password and then confirm it. Click **Next** to continue.

   ![Password window](image)

   **NOTE:** Remember this password as it will be needed later when converting the .pfx file to .pem in OpenSSL configurations.

6. On the **File to Export** window, browse to the location where you wish to save the resulting certificate and enter a path and name for the pfx. Click **Next** to continue.

   ![File to Export window](image)
7. On the **Completing the Certificate Export Wizard** window, click **Finish**.
Defining a RADIUS Server

NOTE: In this section, NetMotion Mobility XE is used as an example of a VPN server.

Define the following entries for each RADIUS server:

- IP Address
- Port
- NAS ID
- Shared Secret

In the RADIUS Server Entry logon window, enter your logon credentials, and then click OK.

(The screen image above is from NetMotion® Wireless software. Trademarks are the property of their respective owners.)
Defining PEAP

To define a RADIUS-EAP (PEAP and EAP-TLS) authentication scheme:

1. Log in to the NetMotion Mobility XE Server console.

Defining the SafeNet FreeRADIUS Agent

The SafeNet FreeRADIUS Agent is a strong authentication agent that allows RADIUS clients to communicate with SAS via the RADIUS protocol.

This agent uses an encrypted key file to communicate with the authentication server. This ensures that all authentication attempts made against the server are from valid, recognized agents.

A key file must be loaded and registered with SafeNet ID agents, and a matching key must be registered with the server.

To set up this configuration, the main steps are:

- Load the specific encrypted key file to communicate with the SafeNet ID server.
- Configure FreeRADIUS to use the agent.

SAS FreeRADIUS Agent integrates a FreeRADIUS server with the SAS authentication server. SAS developers have written an rlm plug-in for the FreeRADIUS server that has defined a reprogrammable, publishable interface. This plug-in is free and is released as a GPL program, similar to FreeRADIUS.
SAS developers have also added their proprietary suite of protocols, which handle authentication with the SAS authentication server.

The following is an example of the `radiusd debug` command, resulting in successful authentication:

```
NOTE: Refer to the SAS FreeRADIUS Agent Configuration Guide for more information on the FreeRADIUS Agent:
```

**Defining FreeRADIUS in SAS**

To allow authentication requests to the SafeNet SAS server, an authentication node must be created for the FreeRADIUS server on which the SafeNet FreeRADIUS agent is installed.

1. In your SAS console, select `Virtual Server > COMMS > Auth Nodes`.
2. Click `Add` and then enter at least the following:
   - A descriptive name
   - The IP address of the FreeRADIUS server
   - The FreeRADIUS shared secret (this must be identical in both SAS and on the FreeRADIUS server)
The following is an example of **Auth Nodes** settings:

![Auth Nodes settings](image)

### Troubleshooting

#### FreeRADIUS Testing

In order to test the FreeRADIUS server, start the server in debug mode. This does two things:

- Starting the server in debug mode executes a script that will create the test certificates that contain the attributes. The server certificate must have special OID’s or else the process will fail.
- Allows you to test the configuration.

Enter `radius -X` at the bash prompt. If all goes well, the last line will read as follows:

*Ready to process requests.*
If this result is not displayed, go back and check your work; you most likely entered something incorrectly.

The following is an example of the **radiusd debug** command, resulting in successful authentication:
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.

Table 1: Support Contacts

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td>Phone</td>
<td>United States</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td>Technical Support</td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td>Customer Portal</td>
<td>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.</td>
</tr>
</tbody>
</table>