# PKI Quick Installation Guide

## for PacketFence version 7.4.0

# PKI Quick Installation Guide

by Inverse Inc.

Version 7.4.0 - Jan 2018

# Table of Contents

Chapter 1

# About this Guide

This guide has been created to give a quick start to install the PacketFence PKI in PacketFence 5.2+. This guide does not include advanced troubleshooting of EAP-TLS connections. Refer to the relevant documentation of EAP-TLS, RADIUS and OpenSSL for advanced features.

Chapter 2

# Assumptions

- You have at least one server with PacketFence 5.2 or later.
- The server already has a properly configured switch with 802.1X support.
- The PacketFence RADIUS server is working in your environment.
- A Mail Transport Agent is properly configured on the PacketFence server.
- The PacketFence management IP will be 192.168.1.5.
- The RADIUS shared secret is "useStrongerSecret".

# Installation

## Step 1: Install the PKI

Note

The PacketFence PKI application is available on the PacketFence repository as the package "packetfence-pki". This is available for CentOS 6, CentOS 7 and Debian 7 and Debian 8.

PacketFence PKI can be installed on a standalone machine or on the PacketFence server itself. Communication between the PKI and PacketFence proper will take place over a REST API over port 9393.

### Preparing to install in standalone mode

- Open the ports 9393 and 9292 over TCP to be able to reach the PKI. This has to be done in the firewall (iptables).
- Disable SELinux:

```
# vim /etc/selinux/config
```

Change the line:

```
SELINUX=enforcing
```

to:

```
SELINUX=disabled
```

Reboot for the change to take effect.

### Preparing to install with PacketFence

1. Allow TCP traffic over ports 9393 and 9292 through iptables:

```
# vim /usr/local/pf/conf/iptables.conf
```

Uncomment the following lines.

```
# -A input-management-if --protocol tcp --match tcp --dport 9393 --jump ACCEPT
# -A input-management-if --protocol tcp --match tcp --dport 9292 --jump ACCEPT
```

Restart the iptables service:

```
# bin/pfcmd service iptables restart
```

## Installation

### Debian

In order to use the repository, create a file named `/etc/apt/sources.list.d/packetfence.list`:

```
echo 'deb http://inverse.ca/downloads/PacketFence/debian wheezy wheezy' > /etc/
apt/sources.list.d/packetfence.list
```

Once the repository is defined, you can install packetfence-pki using:

```
# sudo apt-key adv --keyserver keys.gnupg.net --recv-key
 0xFE9E84327B18FF82B0378B6719CDA6A9810273C4
# sudo apt-get update
# sudo apt-get install packetfence-pki
```

### Ubuntu

In order to use the repository, create a file named `/etc/apt/sources.list.d/packetfence.list`:

```
echo 'deb http://inverse.ca/downloads/PacketFence/ubuntu precise precise' > /etc/
apt/sources.list.d/packetfence.list
```

Once the repository is defined, you can install packetfence-pki using:

```
# sudo apt-key adv --keyserver keys.gnupg.net --recv-key
 0xFE9E84327B18FF82B0378B6719CDA6A9810273C4
# sudo apt-get update
# sudo apt-get install packetfence-pki
```

### CentOS/RHEL

Installing on RHEL or CentOS requires the packetfence and packetfence-extra repositories. Install them first and then install the packetfence-pki package itself.

```
# yum localinstall http://inverse.ca/downloads/PacketFence/CentOS6/x86_64/RPMS/
packetfence-release-1-2.centos6.noarch.rpm
# yum install packetfence-pki --enablerepo=packetfence-extra, packetfence
```

# Step 2: Configuring the PKI

## PacketFence-PKI Configuration

Note

The following configuration will allow you to generate certificates for an EAP-TLS configuration, if you want to use the PKI for another purpose you will have to adjust the Key Usage/Extended Key Usage.

## PKI configuration

1. Ensure that the service has started:

```
# service packetfence-pki start
```

2. Log on to the PKI application:

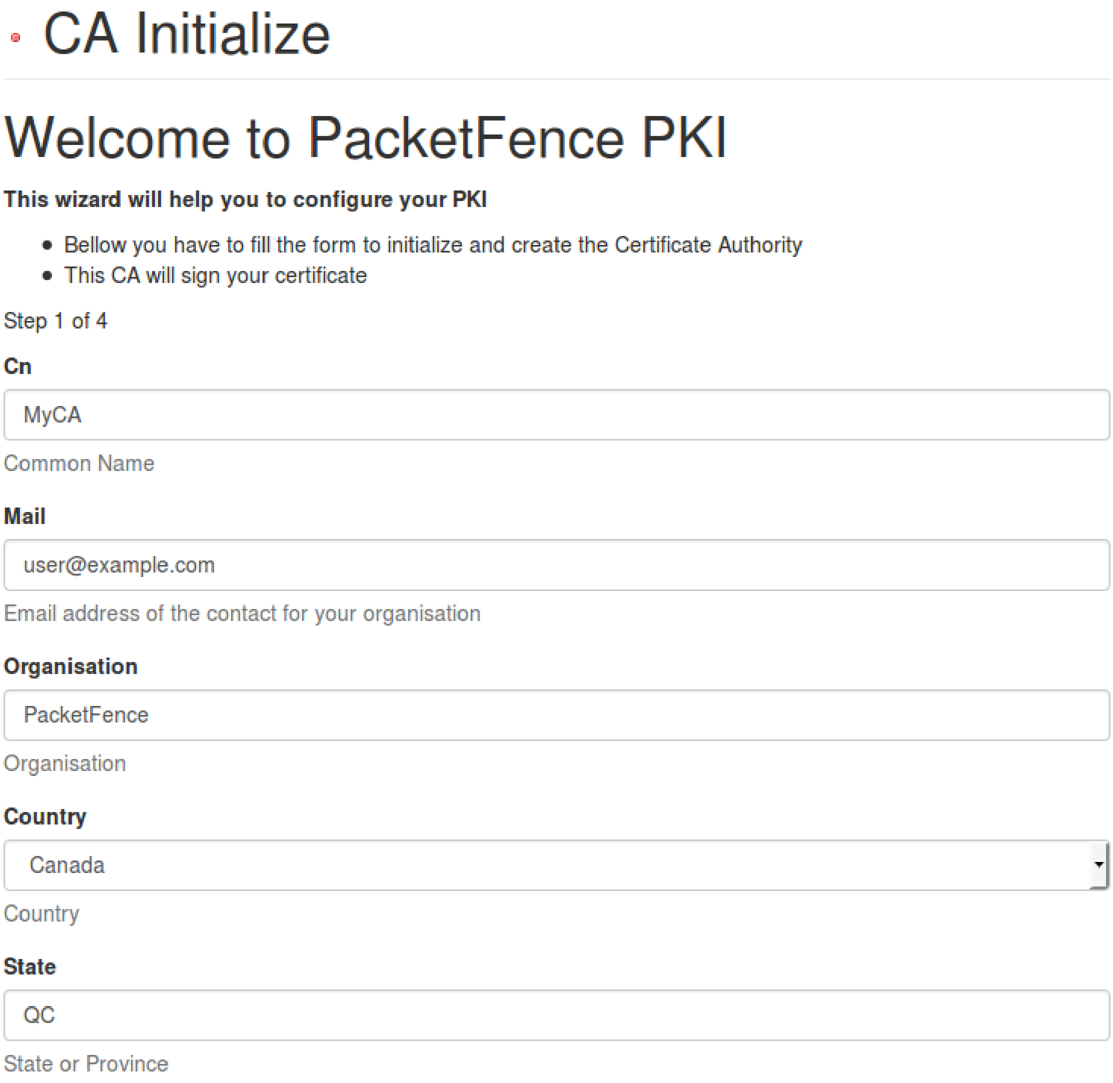
   - URL: https://192.168.1.5:9393
   - Login: admin
   - Default Password: p@ck3tf3nc3

After you login there are few steps to follow to have the PKI working for an EAP-TLS configuration with PacketFence. You will need to configure the following items:

- A Certification Authority (CA)
- Profiles for each purpose, e.g. server/client auth are 2 different profiles
- The REST API authentication and authorization
- A RADIUS server certificate
- A PKI Provider (optional)
- A Provisioner (optional)

Follow the four step wizard to create your certification authority, your client and server profile and your REST API configuration.

## Certification Authority



CA Initialize

Welcome to PacketFence PKI

**This wizard will help you to configure your PKI**

- Bellow you have to fill the form to initialize and create the Certificate Authority
- This CA will sign your certificate

Step 1 of 4

**Cn**

MyCA

Common Name

**Mail**

user@example.com

Email address of the contact for your organisation

**Organisation**

PacketFence

Organisation

**Country**

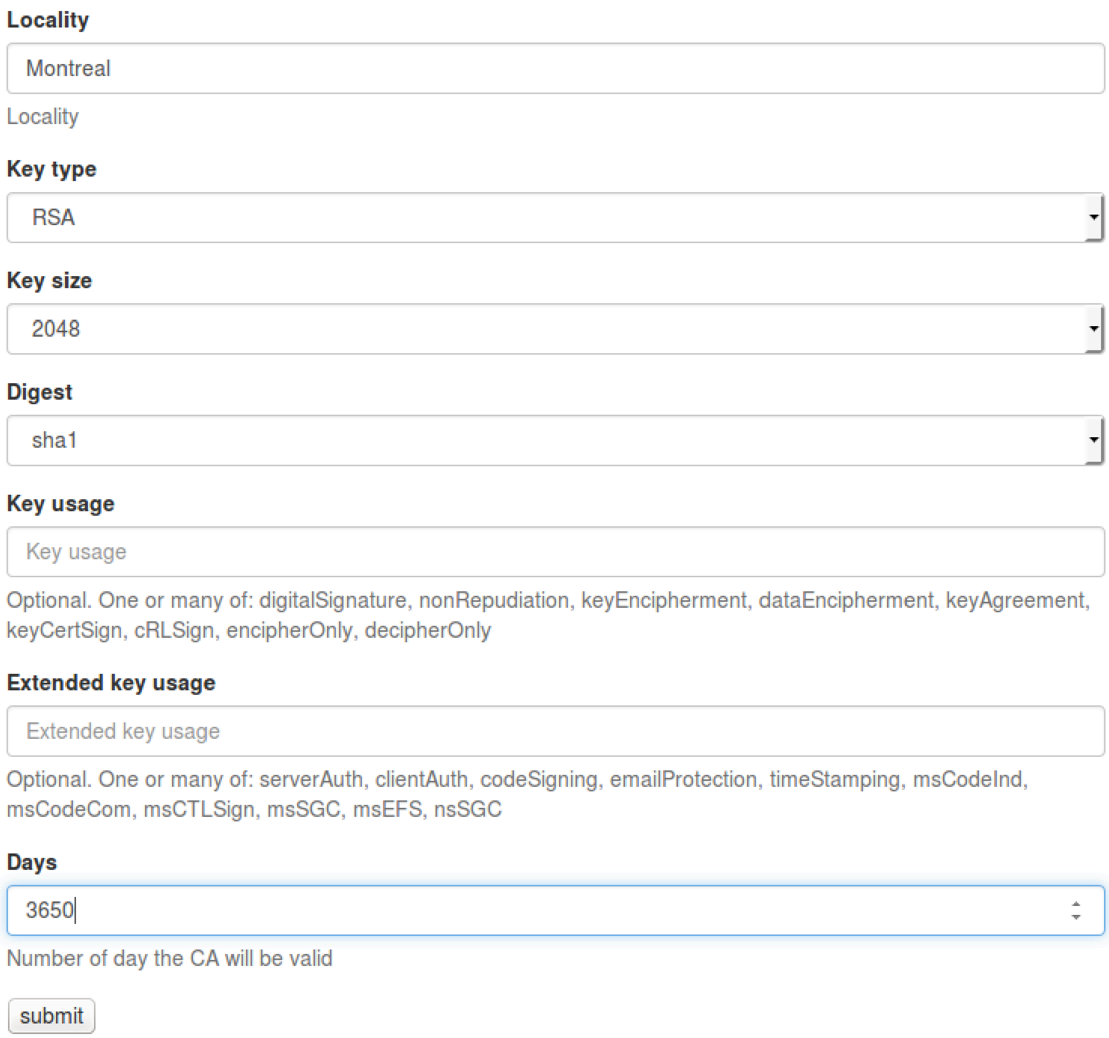
Canada

Country

**State**

QC

State or Province



**Locality**

Montreal

Locality

**Key type**

RSA

**Key size**

2048

**Digest**

sha1

**Key usage**

Key usage

Optional. One or many of: digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly, decipherOnly

**Extended key usage**

Extended key usage

Optional. One or many of: serverAuth, clientAuth, codeSigning, emailProtection, timeStamping, msCodeInd, msCodeCom, msCTLSign, msSGC, msEFS, nsSGC

**Days**

3650

Number of day the CA will be valid

Fill out the following fields that will be used to generate the certification authority.

- CN: Subject of the certification authority
- Mail: Email address of the admin or any other mail that suit your situation
- OU: Organization Unit
- Organization: Name of your company
- Country: Country (select in the list)
- State: state code (i.e. NY, CA, QC, etc...)
- Locality: City where is the organization
- Key type, size and digest: we recommend to use the following RSA, 2048, sha1
- Key Usage and Extended Key Usage are not necessary for the certification authority
- Days: Number of validity days, i.e. 10y = 3650

### Caution

Remember that after the expiration date of your certification authority, every certificate generated by it will be invalidated. We recommend at least 10 years for the CA.

# Profile

# RADIUS server authentication Profile

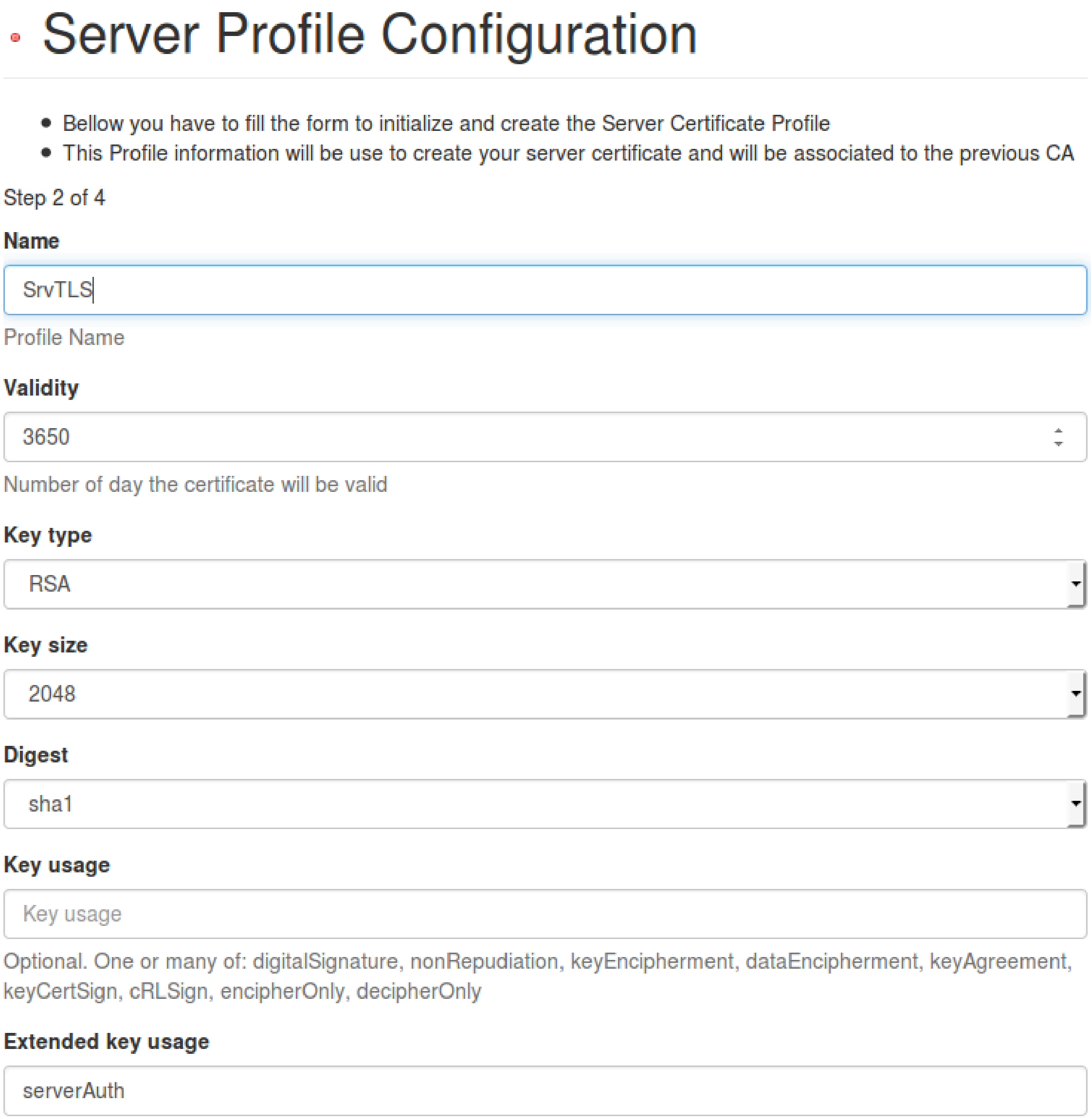
This profile will be used to generate the RADIUS server certificate and key. The server certificate is used by the RADIUS server to authenticate its end of the connection to the client.

Fill out the following fields that will be used to generate the certificate profile to use for generating server certificates.

- Name: A name by which to identify this profile
- CA: The certification authority you created earlier
- Validity: Number of validity days, i.e. 2y = 730
- Key type, size and digest: we recommend using the following: RSA, 2048, sha1
- Key Usage: Optional
- Extended Key Usage: "serverAuth"
- The P12 mail setup is mandatory for the server authentication profile. This is required to send the certificate and password by email using the **send certificate** button.
    - If your mail alerts are already working with PacketFence you should use the following:
        - P12 smtp server: 127.0.0.1
        - Tick P12 mail password

The following fields should be configured according to your preferences and will fill out the email sent when exporting the certificate:

- From: The email address of the CA manager
- Subject: A descriptive line indicating that this is the certificate required to authenticate
- Header: Text that will appear in all emails sent with the certificate
- Footer: Optional, e.g. "This email has been generated automatically, please do not reply."



Server Profile Configuration

- Bellow you have to fill the form to initialize and create the Server Certificate Profile
- This Profile information will be use to create your server certificate and will be associated to the previous CA

Step 2 of 4

**Name**

SrvTLS

Profile Name

**Validity**

3650

Number of day the certificate will be valid

**Key type**

RSA

**Key size**

2048

**Digest**

sha1

**Key usage**

Key usage

Optional. One or many of: digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly, decipherOnly

**Extended key usage**

serverAuth

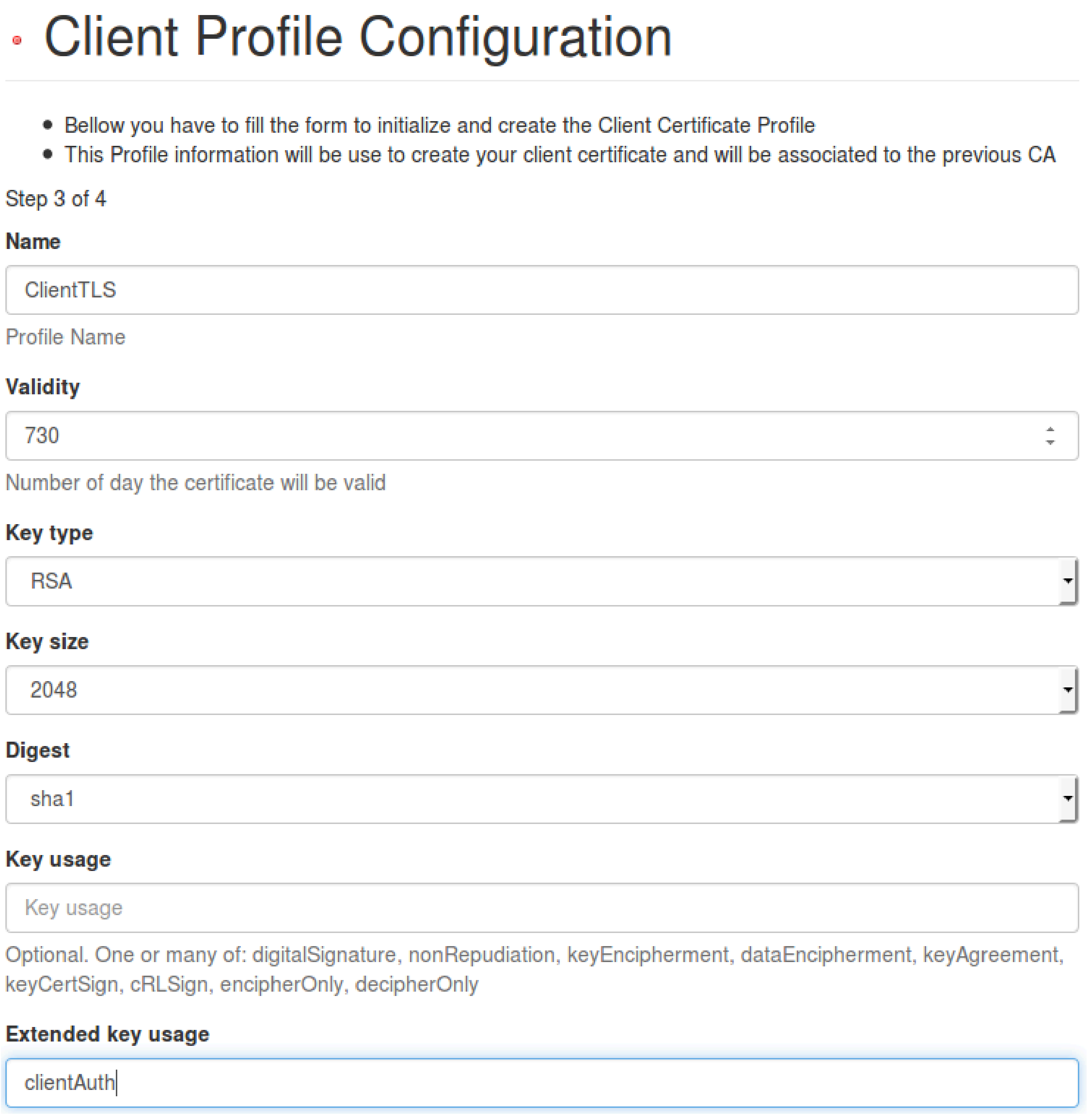
After the creation of your certificate you need to sign it, press the button *Sign* in the list of certificate.

### Caution

We recommend using a long validity for your RADIUS server certificate to avoid it expiring too frequently (i.e. two to five years).

## Client Authentication Profile

This profile will be used to generate the RADIUS client certificate and key. The client certificate is used by the 802.1X supplicant to authenticate its end of the connection to the server.



# Client Profile Configuration

- Bellow you have to fill the form to initialize and create the Client Certificate Profile
- This Profile information will be use to create your client certificate and will be associated to the previous CA

Step 3 of 4

**Name**

ClientTLS

Profile Name

**Validity**

730

Number of day the certificate will be valid

**Key type**

RSA

**Key size**

2048

**Digest**

sha1

**Key usage**

Key usage

Optional. One or many of: digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly, decipherOnly

**Extended key usage**

clientAuth

# Creating a profile:

Fill out the following fields that will be used to generate the certificate profile to use for generating user certificates.

- Name: A name by which to identify this profile
- CA: The certification authority you created earlier
- Validity: Number of validity days, i.e. 2y = 730
- Key type, size and digest: we recommend using the following: RSA, 2048, sha1
- Key Usage: Optional
- Extended Key Usage: "clientAuth"

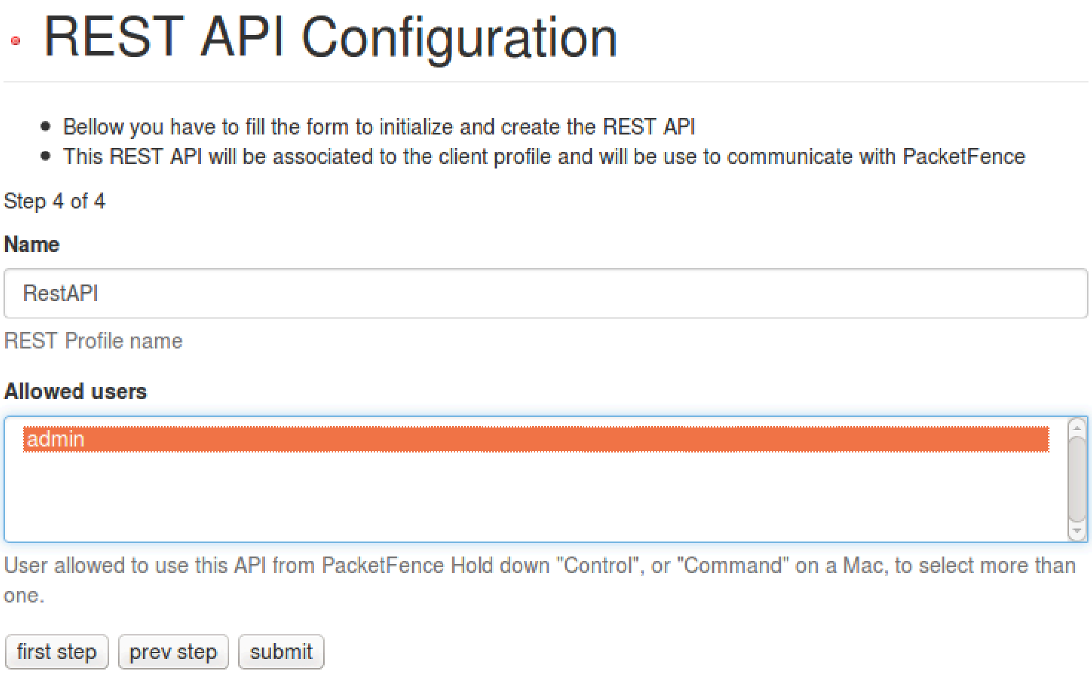
Information about Key Usage and Extended Key Usage is available from RFC5280, parts 4.2.1.3 and 4.2.1.12.

- The P12 mail setup is mandatory for the server authentication profile. This is required to send the certificate and password by email using the **send certificate** button.
  - If your mail alerts are already working with PacketFence you should use the following:
    - P12 smtp server: 127.0.0.1
    - Check "P12 mail password"

The following fields should be configured according to your preferences and will fill out the email sent to the user for which the certificate has been created:

- From: The email address of the CA manager
- Subject: A descriptive line indicating that this is the certificate required to authenticate
- Header: Text that will appear in all emails sent with the certificates
- Footer: Optional, e.g. "This email has been generated automatically, please do not reply."

## REST API Configuration



REST API Configuration

- Bellow you have to fill the form to initialize and create the REST API
- This REST API will be associated to the client profile and will be use to communicate with PacketFence

Step 4 of 4

**Name**

RestAPI

REST Profile name

**Allowed users**

admin

User allowed to use this API from PacketFence Hold down "Control", or "Command" on a Mac, to select more than one.

The fields shown above are required to allow use of the REST API over which PacketFence and the PKI exchange authentication information. A username and password are mandatory.

## User creation

Additional users for specific tasks may be created under Configuration → Users → Create .

All fields are mandatory.

Users can be associated with the REST API configuration.

## Password change

Caution: Please be sure to change the default password to the PKI.

Passwords can be changed in the "Users" tab by editing the user.

# Step 3: Configuring PacketFence

## Certificate storage on PacketFence

It is recommended to create a separate directory to separate EAP-TLS certificates from server certificates:

```
# mkdir /usr/local/pf/conf/ssl/tls_certs/
```

RADIUS EAP-TLS authentication requires three files, the CA certificate, the server certificate and the private key.

The CA certificate generated by the PacketFence PKI will be placed in /usr/local/packetfence-pki/ca/. Copy the CA certificate (and not it's private key) to the directory created above and make sure it is readable by the "pf" user.

In the case where the PKI was installed on the same server as PacketFence, this will mean for example:

```
# cp /usr/local/packetfence-pki/ca/YourCA.pem /usr/local/pf/conf/ssl/tls_certs/
# chown pf:pf /usr/local/pf/conf/ssl/tls_certs/*
```

Since the server certificate is stored in the PKI database, you will have to sign and export it to the PacketFence server.

On the PKI web interface, under Certificates click on the "sign" icon for the certificate for your RADIUS server. This will automatically sign the certificate with your CA. Use the *Send certificate* or *Download certificate* to export it. The certificate will be exported in p12 format which combines both the certificate and its key. The password to decrypt the file will be send by email.

Copy the p12 formatted file to the tls_cert directory on the PacketFence server. E.g.

```
# scp /path/to/your/downloads/YourCert.* root@192.168.1.5:/usr/local/pf/conf/ssl/
tls_certs/
```

Then, convert the p12 file to the pem format using the openssl tool:

```
# openssl pkcs12 -in YourCert.p12 -nocerts -out /usr/local/pf/conf/ssl/tls_certs/
YourCert.key -nodes
# openssl pkcs12 -in YourCert.p12 -out /usr/local/pf/conf/ssl/tls_certs/
YourCert.pem -clcerts -nokeys
```

Ensure that the files are readable by "pf":

```
# chown pf:pf /usr/local/pf/conf/ssl/tls_certs/*
```

## RADIUS EAP-TLS and packetfence-pki

Using the PKI generated certificates requires editing the radius EAP configuration file.

Edit the /usr/local/pf/conf/radiusd/eap.conf file and replace the following lines with references to your new certificates in the *tls* configuration block:

```
private_key_file = [% install_dir %]/conf/ssl/server.key
certificate_file = [% install_dir %]/conf/ssl/server.pem
```

E.g.

```
private_key_file = [% install_dir %]/conf/ssl/tls_certs/YourCert.key
certificate_file = [% install_dir %]/conf/ssl/tls_certs/YourCert.pem
ca_file = [% install_dir %]/conf/ssl/tls_certs/YourCA.pem
```

Certificate revocation checks also have to be configured using OCSP in the same block.

For example:

```
ocsp {
    enable = yes
    override_cert_url = yes
    url = "http://192.168.1.5:9292/pki/ocsp/"
}
```

Restart radiusd to regenerate the new configuration files and enable EAP-TLS using your CA signed certificates:

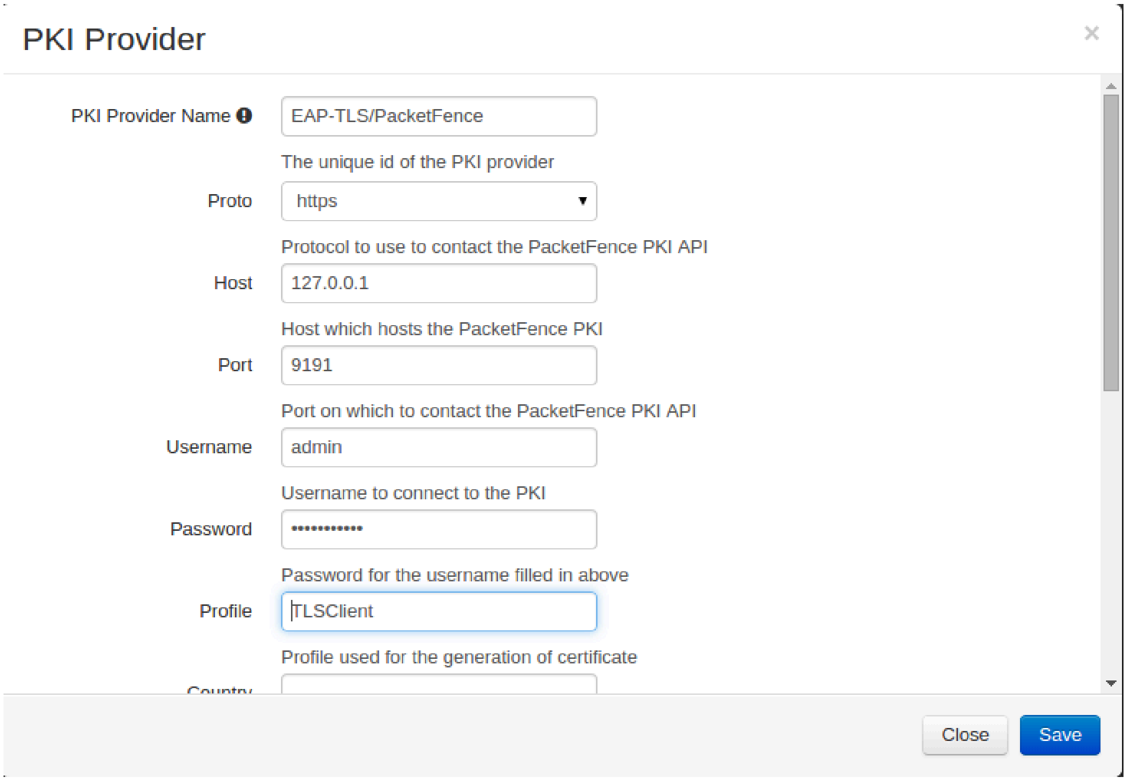
```
# /usr/local/pf/bin/pfcmd service radiusd restart
```

## PacketFence provider configuration

Using the PKI requires configuring the PKI providers section in the PacketFence GUI under Configuration > Users. The provider configuration defines how PacketFence connects to the PKI REST API and which profile will be used.

Add a new PKI provider and select PacketFence PKI.

Fill out the form for a PKI provider according to the PKI configuration profile you created earlier. Pay attention to the username and password which have to match an authorized user in the PKI configuration.



## PKI Provider

PKI Provider Name: EAP-TLS/PacketFence

The unique id of the PKI provider

Proto: https

Protocol to use to contact the PacketFence PKI API

Host: 127.0.0.1

Host which hosts the PacketFence PKI

Port: 9191

Port on which to contact the PacketFence PKI API

Username: admin

Username to connect to the PKI

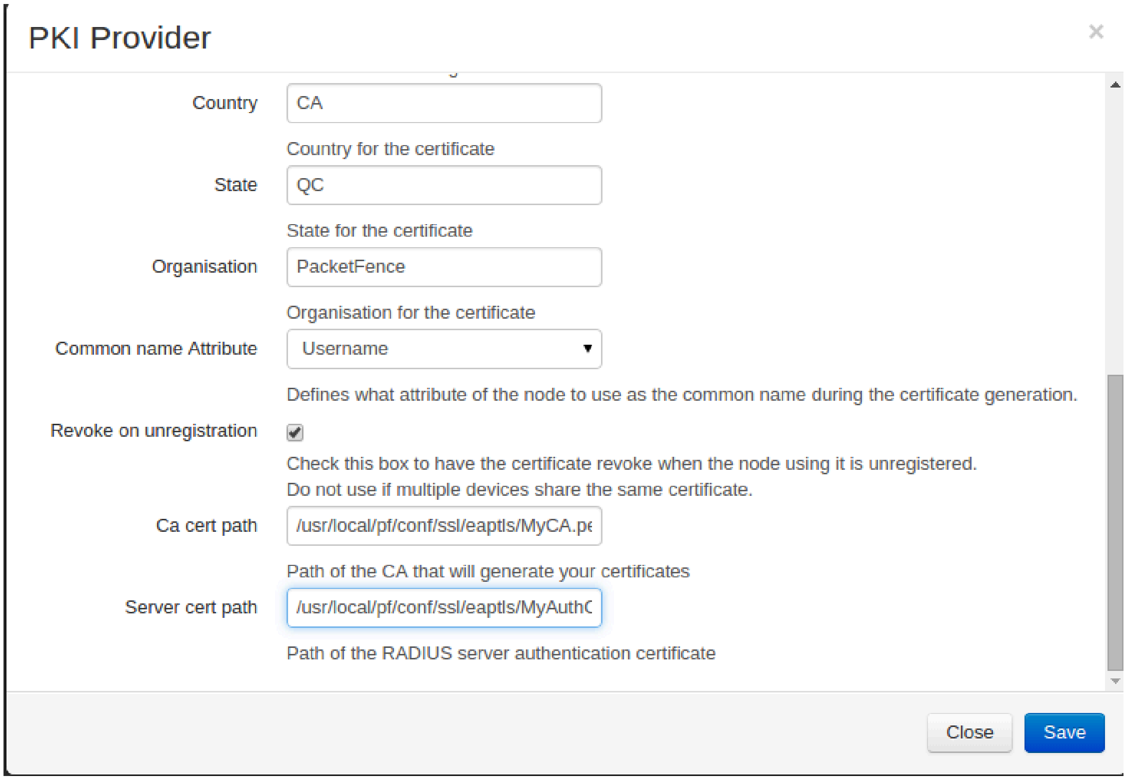
Password: •••••••••••

Password for the username filled in above

Profile: TLSClient

Profile used for the generation of certificate

Country



## PKI Provider

Country: CA

Country for the certificate

State: QC

State for the certificate

Organisation: PacketFence

Organisation for the certificate

Common name Attribute: Username

Defines what attribute of the node to use as the common name during the certificate generation.

Revoke on unregistration: ☑

Check this box to have the certificate revoke when the node using it is unregistered.
Do not use if multiple devices share the same certificate.

Ca cert path: /usr/local/pf/conf/ssl/eaptls/MyCA.pe

Path of the CA that will generate your certificates

Server cert path: /usr/local/pf/conf/ssl/eaptls/MyAuthC

Path of the RADIUS server authentication certificate

The "server certificate path" and "CA cert path" both need to be absolute (e.g. /usr/local/pf/conf/ssl/tls_certs/MyCA.pem is an absolute path).

The "Common name attribute" field defines how the certificate will be generated and what type of "ownership" will associate the certificate to the connection. If you select *MAC address*, a certificate will be generated for the device itself using the MAC address as the identifier. If you select *Username*, a certificate will be generated for the user using his login name on the authentication backend (e.g. Active-Directory).

This means that revoking the certificate for a username based certificate will block all the devices that this user registered. If you generate the certificates using the MAC address, revoking a certificate will block only that device.

## Provisioners configuration

Provisioners allow devices to automatically configure themselves to connect to the proper SSID (if applicable), use the proper authentication method (e.g. EAP-TLS) and trust the CA certificate and any certificate signed by it.

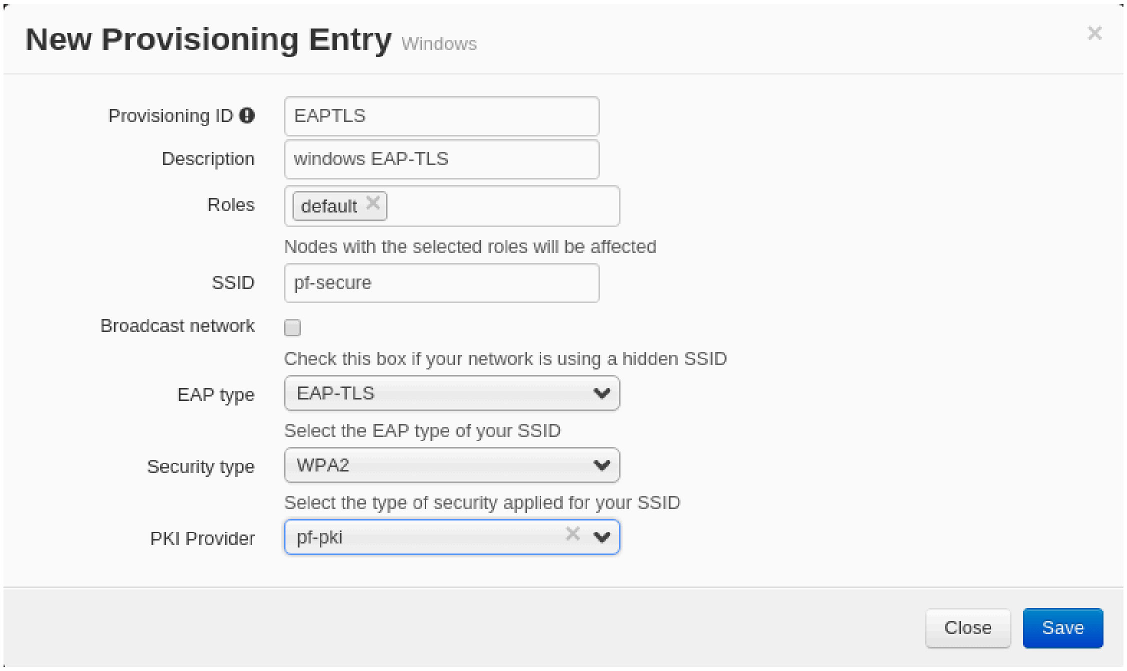
Provisioners are configured in the PacketFence administration GUI under Configuration > Users > Provisioners.

Add a new provisioner for each of the classes of devices to be supported amongst Android, Apple Devices and Windows. Fill out the form, choosing a different Provisioning Id per provisioner.

The fields affect the provisioning behavior in the following fashion:

- Roles: The "Roles" field defines which devices will be affected by the provisioning item. If empty all devices for this class will be affected.
- SSID: The "SSID" field defines which SSID will be configured on the device using the authentication profile.
- EAP-Type: The EAP type defines the authentication method supported and should be set to EAP-TLS to integrate with the PacketFence PKI.
- Security type: The security type should be set to WPA2 to integrate with the PacketFence PKI.
- PKI Provider: This should match the provider you configured earlier in the section on providers.

The following is an example on how to configure an EAP-TLS connection for Windows/Android/OS X/iOS



New Provisioning Entry Windows

Provisioning ID: EAPTLS

Description: windows EAP-TLS

Roles: default

Nodes with the selected roles will be affected

SSID: pf-secure

Broadcast network: □

Check this box if your network is using a hidden SSID

EAP type: EAP-TLS

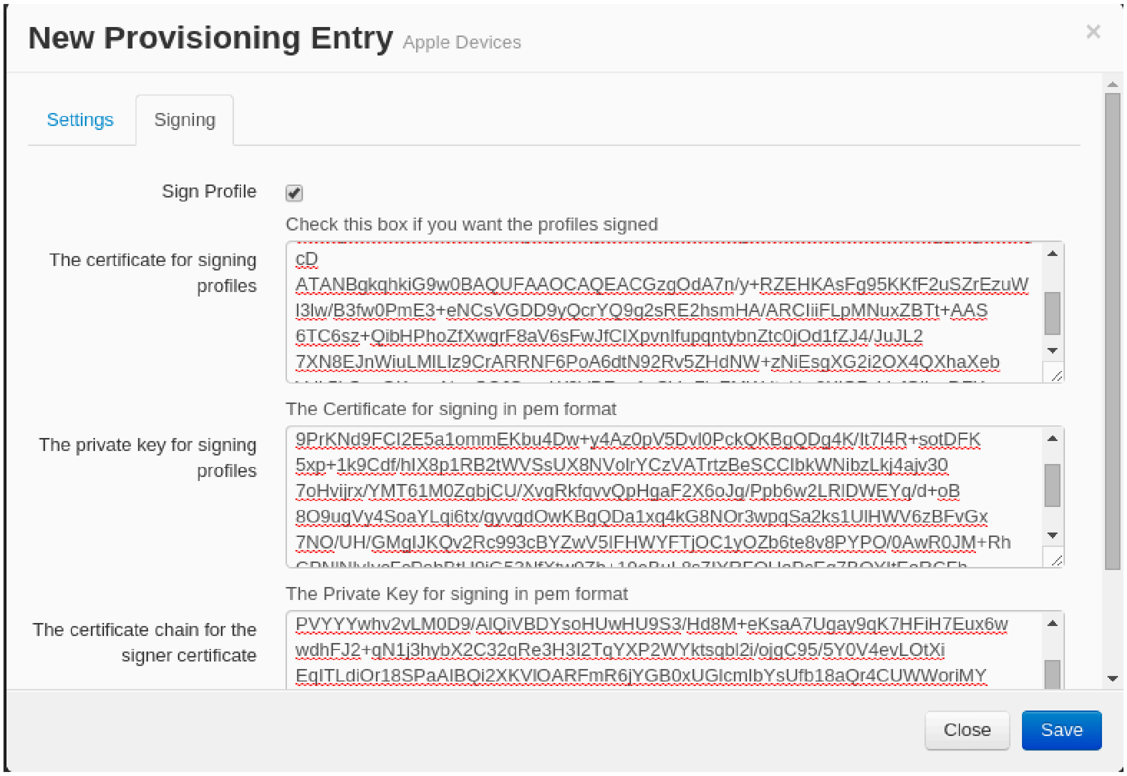
Select the EAP type of your SSID

Security type: WPA2

Select the type of security applied for your SSID

PKI Provider: pf-pki

OS X/iOS require signing the provisioning profile with a Certification Authority already trusted by the device such as e.g. VeriSign. Configuring this has to be done in the *Signing* tab in the "Apple devices".



New Provisioning Entry Apple Devices

Sign Profile: ☑

Check this box if you want the profiles signed

The certificate for signing profiles:

cD
ATANBgkqhkiG9w0BAQUFAAOCAQEACGzgOdA7n/y+RZEHKAsFg95KKfF2uSZrEzuW
l3lw/B3fw0PmE3+eNCsVGDD9yQcrYQ9g2sRE2hsmHA/ARCIiiFLpMNuxZBTt+AAS
6TC6sz+QibHPhoZfXwgrF8aV6sFwJfCIXpvnIfupqntybnZtc0jOd1fZJ4/JuJL2
7XN8EJnWiuLMlLIz9CrARRNF6PoA6dtN92Rv5ZHdNW+zNiEsgXG2i2OX4QXhaXeb

The Certificate for signing in pem format

The private key for signing profiles:

9PrKNd9FCI2E5a1ommEKbu4Dw+y4Az0pV5Dvl0PckQKBgQDg4K/It7l4R+sotDFK
5xp+1k9Cdf/hIX8p1RB2tWVSsUX8NVolrYCzVATrtzBeSCClbkWNibzLkj4ajv30
7oHvijrx/YMT61M0ZgbjCU/XvgRkfqvvQpHgaF2X6oJg/Ppb6w2LRIDWEYq/d+oB
8O9ugVy4SoaYLqi6tx/gyvgdOwKBgQDa1xq4kG8NOr3wpqSa2ks1UlHWV6zBFvGx
7NO/UH/GMgIJKQv2Rc993cBYZwV5IFHWYFTjOC1yOZb6te8v8PYPO/0AwR0JM+Rh

The Private Key for signing in pem format

The certificate chain for the signer certificate:

PVYYYwhv2vLM0D9/AIQiVBDYsoHUwHU9S3/Hd8M+eKsaA7Ugay9qK7HFiH7Eux6w
wdhFJ2+qN1j3hybX2C32qRe3H3I2TqYXP2WYktsqbl2i/ojgC95/5Y0V4evLOtXi
EqITLdiOr18SPaAIBQi2XKVIOARFmR6jYGB0xUGlcmIbYsUfb18aQr4CUWWoriMY

Fill out the fields with the contents of the Base64 encoded certificates. To extract this information from a pem formatted certificate, copy the file content included between the begin and end tag, not including the delimiters themselves. For instance if the file content is:

```
----- BEGIN CERT -----
1234567890asdfghjkl
zxcvbnmqwertyuiop78
----- END CERT -----
```

Copy everything between the BEGIN and END lines, but not the lines themselves. Repeat this operation for the certificate key and intermediate certificate if any.

## Connection Profiles Configuration

Provisioners have to be enabled on the Connection Profiles configuration in the PacketFence GUI.

Under Configuration > Main > Connection Profiles, select each of the provisioners created above which should be active for the profile. If no connection profile is defined, configure the "default" profile to use the provisioners created.

### Note

If you use two different connection profiles for the open and secure networks, make sure you configure the provisioners on both profiles.

## Passthroughs required for Android

Android devices require passthroughs to be created to allow them to fetch the configuration application from the Play Store.

Add the following to the "Fencing" section of the Configuration tab in the PacketFence GUI.

```
passthrough=enabled
passthroughs=*.ggpht.com,*.googleusercontent.com,android.clients.google.com,
  *.googleapis.com,*.android.clients.google.com,*.gvt1.com
```

## Revocation process

Certificates can be checked for revocation at authentication time using either OCSP to interrogate the PKI for every RADIUS authentication or using the certificate revocation lists (CRL).

OSCP is scalable, its main downside would be that one request per certificate authentication is sent to the PKI to verify if the certificate is still valid and that adds additional latency to authentication. Additionally, RADIUS authentication then becomes dependent on an external service which could be unreachable although that can be mitigated in the FreeRADIUS configuration.

Using a CRL implies that each time the CRL is updated, every services that uses this CRL has to download it again. For security reason we recommend a short delay on CRL expiration (to avoid using revoked certificate on the network).

By default a CRL list will be created when you revoke a certificate. The file will be under /usr/local/packetfence-pki/ca/YourProfileName.crl. Note that one CRL by profile will be created.