
# EzIdentity Implementation Guide - PAM Radius

**Document Number**
EZM_IG_PR_00

**Issue Date**
1 July 2016

Version 1.0.0

**Prepared for**
PAM Radius Agent

**Prepared by**
EZMCOM Inc.
4701 PATRICK HENRY DR, SANTA CLARA, CA, 950541863, US.
Tel: +1 510 396 3894
+60 (0)12 570 1114
Email: info@ezmcom.com



## Copyright

### Trademarks

EzIdentity, EzID are either registered trademarks or trademarks of EZMCOM Inc. All other trademarks and registered trademarks are the property of their owners.

### Additional Information, Assistance, or Comments

EZMCOM's technical support specialists can provide assistance when planning and implementing EzIdentity™ in your network. In addition to aiding in the selection of the appropriate authentication products, EZMCOM can suggest deployment procedures that provide a smooth, simple transition from existing access control systems and a satisfying experience for network users. We can also help you leverage your existing network equipment and systems to maximize your return on investment.

EZMCOM works closely with channel partners to offer worldwide Technical Support services. If you purchased this product through an EZMCOM channel partner, please contact your partner directly for support needs.

To contact EZMCOM directly:

International Voice: +60-(0)12-570-1114

North America Voice: +1-510-396-3894

support@ezmcom.com

For information about obtaining a support contract, see our Support Web page at http://www.ezmcom.com.

# Table of Contents

# Document Control

<Remove this section before external release>

## Document Contributor(s)

| Name | Department |
|---|---|
| Ashish Pati | Research & Development |
| Khairi Adammi | Research & Development |
| Ashish Pati | Research & Development |

## Document Reviewer(s)

| Name | Department |
|---|---|
| | |
| | |
| | |
| | |

## Document Approver(s)

| Name | Department | Date Approved |
|---|---|---|
| | | |
| | | |
| | | |

## Document Revision(s)

| Date | Author | Version | Revision Description |
|---|---|---|---|
| | | | |

# 1.0 Introduction

The guide describes the configuration, and usage of PAM module in Linux/Unix/Solaris with EZMCOM EzIdentity™ AS.

## 1.1 Overview

PAM modules can be used in *Nix environments to provide an additional level of security within a given service or application which is PAM aware. This document contains procedures as well as general advice on augmenting current authentication mechanisms with strong two-factor one-time passwords.

## 1.2 Assumption

EzIdentity has been installed and configured and a “Test” user account can be selected in the Assignment Tab.

Local User are created on Linux/ Unix server without password.

## 1.3 Operation

The RADIUS PAM module adds an additional level to authentication for any service or application which is PAM aware. The user would attempt to authenticate to the service or application, and would be prompted for their user name, one-time-password and local-password.

## 1.4 Prerequisites

- Download the RADIUS PAM files from the FreeRadius website: http://freeradius.org/pam_radius_auth/

  Above URL can be change, please refer the correct URL to download the latest package.
- Extract the contents of the tar.gz file to a directory of your choosing and that you have sufficient privileges to read and write to them.
- The Linux/Solaris username and the EzIdentity Token/username must be identical.
- Even though EzIdentity authentication is being used, the EzIdentity user must have an account on the Linux/Solaris system in order for the users to connect without password. When a user logon to a Linux system, the system reads the /etc/passwd file to find the user’s group, default shell and home directory. If this information does not exist, the user will fail to authenticate. This condition does not apply if NIS/NIS+/NFS or LDAP is being used.
- An application must be PAM-aware in order to use a PAM module. The most common PAM configuration files are login, ftp, and sshd. Please consult the application’s documentation to determine if it is PAM-aware.
- Open UDP port 1812,1813, 1645 & 1646 from PAM client to the EzIdentity server.

## 2.0 PAM RADIUS Installation

This section deals primarily with the installation on UNIX of the FreeRADIUS **PAM module**.

| **operating system** | **PAM module location** | **PAM application specific configuration files localtion** |
|---|---|---|
| Linux | /lib/security<br>OR<br>/lib64/security | /etc/pam.d |
| Solaris | /usr/lib/security | /etc/pam.conf |

Please review the Prerequisites section before proceeding in the installation instructions.

Download the following package before proceeding with this guide.

FreeRADIUS client download URL: http://freeradius.org/pam_radius_auth/

### 2.1 PAM Radius Client Installation

Dependency packages **gcc & pam-devel**

**Below Steps to configure the PAM RADIUS on Client machine:**

Login as root. Extract the package to a temporary location then browse to this temporary location.

**Step 1**: Extract the client pam_radius-x.x.x.tar.gz in /tmp

```
tar –xvzf pam_radius-x.x.0.tar.gz
```

**Step 2**: change direct to the newly extracted directory

```
cd /tmp/pam_radius-x.x.x
```

**Step 3**: run configure.

```
./configure
```

**Step 4**: run to make to compile the files.

```
make
```

**Step 5**: new file pam_radius_auth.so will be created.

Copy pam_radius_auth.so file to /lib/security/ directory if it is 32bit OS

```
cp pam_radius_auth.so /lib/security/pam_radius_auth.so
```

Copy pam_radius_auth.so to /lib64/security/ directory if it is 64bit OS

```
cp pam_radius_auth.so /lib64/security/pam_radius_auth.so
```

## 2.2 Configuration file for RADIUS Server

When the FreeRADIUS PAM module is used it searches for a file called server in the **/etc/raddb** directory. This file contains the location of the RADIUS servers, the shared secret, and the order in which each RADIUS server will be checked. A generic server configuration file called pam_radius_auth.conf can be found in the FreeRADIUS module source directory which you extracted to a temporary location.

This file must be renamed and placed into the **/etc/raddb** directory. Verify that "**/etc/raddb**" directory exists. If it does not type:

```
mkdir /etc/raddb
```

Now, copy the generic server configuration file over to the **/etc/raddb** directory by going into the freeRADIUS PAM module source directory and typing:

```
cp pam_radius_auth.conf  /etc/raddb/server
```

Below is an example of the default server configuration file. Blank lines or lines beginning with # are considered as comments or simply ignored.

```
vi /etc/raddb/server
```

```
# pam_radius_auth configuration file.  Save as: /etc/raddb/server
# server[:port]          shared_secret          timeout (s)
#127.0.0.1:1812          localsecretkey          1
EzIdentity-RADIUS        secret                 60

# See the INSTALL file for pam.conf hints
```

**Server[:port]:-** This is the EzIdentity Radius server Domain name or IP address followed by :port which can be 1812 or 1645 depending upon the EzIdentity server configuration.

**Share_secret:-** This is the EzIdentity Radius server secret key, please request EZMCOM's support engineer for the shared secret.

**Timeout (s):-** The timeout field controls the time the module waits before deciding if the server has failed to respond. This setting is optional. If multiple RADIUS Server lines exist, they are tried in order. If the server fails to respond, it is skipped and the next server is used. A RADIUS port must be specified with the ip address in the server file.

Secure the RADIUS server configuration file. That can be done by below commands:

```
chown root /etc/raddb
chmod 700 /etc/raddb
chmod 700 /etc/raddb/server
```

## 3.0 Configuring per Application

The last step in setting up the FreeRADIUS PAM module is to configure the PAM-aware application. All the applications listed in the /etc/pam.d directory or the pam.conf files are PAM-aware. EzIdentity only offers support for the PAM-aware application listed in the Linux and Solaris PAM configuration examples section listed below. In theory, the EzIdentity module will work for most applications in the pam.d directory.

---

**NOTE:** Please take backup of Original file before changing anything in the configuration to use Radius authentication.

---

### 3.1 SSHD (OpenSSH)

For security reasons and compatibility with the FreeRADIUS PAM module you must have at least SSH2 version 2.4 for F-Secure or SSH2 version 2.9 for OpenSSH.

**Note:** EzIdentity will only provide support for versions of OpenSSH/OpenSSL included with RedHat or any updates provided by RedHat.

Please replace /etc/pam.d/sshd with below content to enables EzIdentity Radius authentication.

**NOTE**: Backup original file

```
#%PAM-1.0
auth        sufficient    /lib64/security/pam_radius_auth.so client_id=2 prompt=Password
auth        requisite     /lib64/security/pam_unix.so use_first_pass
password    required    /lib64/security/pam_unix.so
session     required    /lib64/security/pam_unix.so
account     required    /lib64/security/pam_access.so
session     required    /lib64/security/pam_console.so
```

---

**NOTE:** The client_id is NAS-Identifier and must be passed according to the deployment.
client_id=<DOMAIN_ID>|<OS_NAME>|<DEVICE_TYPE>
For Example: client_id=2|Linux|PAM

---

Please change the following configuration in sshd_config file, which is located under the etc/ssh/ directory.

| | |
|---|---|
| PasswordAuthentication | yes |
| PermitEmptyPasswords | no |
| ChallengeResponseAuthentication | yes |
| UsePrivilegeSeparation | no |
| UsePAM | yes |

### 3.2 Login

The LOGIN PAM file affect local console login sessions. Please replace /etc/pam.d/login with below content to enables EzIdentity Radius authentication.

**NOTE**: Backup original file.

```
#%PAM-1.0
auth          sufficient      /lib64/security/pam_radius_auth.so client_id=2 prompt=Password
auth          required        /lib64/security/pam_unix.so use_first_pass
account       required    /lib64/security/pam_permit.so
account       required    /lib64/security/pam_unix.so
password      required    /lib64/security/pam_unix.so
session       required    /lib64/security/pam_unix.so
session       required        /lib64/security/pam_loginuid.so
```

**NOTE:** The client_id is NAS-Identifier and must be passed according to the deployment.
client_id=<DOMAIN_ID>|<OS_NAME>|<DEVICE_TYPE>
For Example: client_id=2|Linux|PAM

### 3.3 KDE/GMD/XDM (Graphical Desktop Logon)

EzIdentity authentication can be enabled for users who logon to KDE or Gnome. In theory, any Desktop manager is supported, as they will most likely use XDM, GDM, or KDE as their logon manager. The following changes to either the XDM, GDM or KDE PAM configuration file enables EzIdentity authentication.

Please replace /etc/pam.d/gdm-password with below content to enables EzIdentity Radius authentication. Some of the distribution use /etc/pam.d/gdm for the GUI, please verify accordingly.
**NOTE**: Backup original file.

```
#%PAM-1.0
auth        sufficient      /lib64/security/pam_radius_auth.so client_id=2 prompt=Password
auth         requisite     /lib64/security/pam_unix.so use_first_pass
account     required     /lib64/security/pam_access.so
account     required     /lib64/security/pam_unix.so
password     required     /lib64/security/pam_unix.so
session     required     /lib64/security/pam_unix.so
```

**NOTE:** The client_id is NAS-Identifier and must be passed according to the deployment.
client_id=<DOMAIN_ID>|<OS_NAME>|<DEVICE_TYPE>
For Example: client_id=2|Linux|PAM

### 3.4 SU

The SU PAM file affect local SU sessions. Please replace /etc/pam.d/su-l with below content to enables EzIdentity Radius authentication.

**NOTE**: Backup original file.

```
#%PAM-1.0
auth     sufficient    pam_rootok.so
auth     sufficient    /lib64/security/pam_radius_auth.so client_id=2 prompt=Password
auth     requisite     /lib64/security/pam_unix.so use_first_pass
accountrequired      /lib64/security/pam_access.so
accountrequired      /lib64/security/pam_unix.so
password   required      /lib64/security/pam_unix.so
sessionrequired      /lib64/security/pam_unix.so
```

**NOTE:** The client_id is NAS-Identifier and must be passed according to the deployment.
client_id=<DOMAIN_ID>|<OS_NAME>|<DEVICE_TYPE>
For Example: client_id=2|Linux|PAM

## 4.0 Reference

http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Managing_Smart_Cards/PAM_Configuration_Files.html

http://freeradius.org/pam_radius_auth/USAGE

## 5.0 Feedback

EZMCOM welcomes your comments and suggestions about this manual and other documentation included with this product. Your input is an important part of the information used for future revisions. If you find errors or have general suggestions for improvement, please indicate the document, chapter, section, and page number. Please send your comments and suggestions to:

**support.global@ezmcom.com**



**USA** +1 510.396.3894
**Asia Pacific** +60 (1) 2.570.1114
**Email** support@ezmcom.com
**Web** www.ezmcom.com