

## NAME

config.radius - Radius configuration file

## SYNOPSIS

```
RADIUS_CLIENT client-ip-address shared-secret
RADIUS_AUTH domain-name auth-type [auth-type-arguments]
RADIUS_USER_ACCOUNT username [password]
RADIUS_USER_CHECK_NUMBER username phone-number
RADIUS_USER_CHECK_ATTRIBUTE username radius-attribute-spec
RADIUS_USER_RETURN_ATTRIBUTE username radius-attribute-spec
```

## DESCRIPTION

The radius configuration file `config.radius` specifies:

- Clients or network access services (NAS) that may use the radius server for authentication.
- Authentication types based on a domain extension.
- Radius native user accounts.

The radius configuration file is line oriented. A commentary line starts with hash mark at the beginning of a new line. Empty lines are ignored.

RADIUS\_CLIENT lines define radius clients that are allowed to connect to the radius server on the firewall to perform authentication. RADIUS\_CLIENT requires two arguments: the *client-ip-address* and *shared-secret* to be used between the client and the server (firewall). Note that *client-ip-address* is not necessarily the address of the system initiating the radius authentication request. Multi-hop radius proxying allows for relaying of radius requests through multiple radius servers. Only the radius clients that directly contact the firewall need a RADIUS\_CLIENT line.

RADIUS\_AUTH lines specify the authentication type to be used for authentication requests for usernames with domain extension. E.g. of the form *username@domain-name*. This so-called Realm based authentication applies when the authentication type `Realm` is set. Currently only `TX-Auth` and `RADIUS` can be used for *auth-type*.

`TX-Auth` indicates that the authentication database (see `authsrv(8)`) on the firewall should be used. Only the *username* part of the account name is presented to the authentication server. This also implies that all users in the authentication database can be authenticated in case of a `DEFAULT` Realm authentication (see `EXAMPLES`). This form of authentication also implies that only PAP authentication requests are possible since by design the authentication database stores all passwords in encrypted form.

The `RADIUS` authentication type defines a proxy relay; requests will be forwarded to the IP address specified in *auth-type-arguments*. Please note that radius proxying will only work in conjunction with radius servers that support multi-hop proxying.

RADIUS\_USER\_ACCOUNT lines define native radius accounts (*usernames*) and their *passwords*. The *password* is optional. If it is omitted the firewall authentication service will be used with the aforementioned restrictions regarding PAP authentication. By specifying a *password* for *username* both PAP and CHAP can be used. This is recommended for Global Roaming use. A special case is the *username* DEFAULT which is used as a place holder for defining fallback authentication (e.g. for forwarding all requests to RADIUS or TX-Auth based authentication).

Optionally a user account can be augmented with a telephone number check. This requires a RADIUS\_USER\_CHECK\_NUMBER line which specifies the *phone-number* of the given *username*. Please note that leading zeroes are usually not provided by the Telcos.

Generic radius check and return attributes for one or more specific radius user accounts can be specified. This feature should be used with care. This is because no sanity checking on the parameters is possible. To specify a check on or the return of a radius attribute use the RADIUS\_USER\_CHECK\_ATTRIBUTE and RADIUS\_USER\_RETURN\_ATTRIBUTE lines respectively. The *username* parameter defines the user account the attribute check or return applies to. The *radius-attribute-spec* parameter contains the attribute specification. It consists of an attribute name followed by an equal sign (=) followed by a double quoted (") string defining the attribute value. Valid attributes and their values are vendor specific and should therefore be looked up in the documentation of the radius client.

## EXAMPLES

Allow the radius client with IP address 172.16.2.6 to contact the radius server on the firewall for authentication requests. The shared secret is *secret*:

```
RADIUS_CLIENT 172.16.2.6 secret
```

Specify a user account for the user *daffy@acme.nl* with password *duck*:

```
RADIUS_USER_ACCOUNT daffy@acme.nl duck
```

Specify a user account for the user *bugs@acme.nl* with password *bunny* and request a telephone number check. The number is *5551234*:

```
RADIUS_USER_ACCOUNT bugs@acme.nl bunny
RADIUS_USER_CHECK_NUMBER bugs@acme.nl 5551234
```

Specify a fallback proxy relay to the radius server with IP address 192.168.1.33 for users in the domain *acme.nl*:

```
RADIUS_AUTH acme.nl RADIUS 192.168.1.33
RADIUS_USER_ACCOUNT DEFAULT Realm
```

**FILES**

`/usr/local/config/config.radius`

Location of the radius configuration file on the firewall.

**SEE ALSO**

`radius(7)`, `authsrv(8)`.

**BUGS**

Please report bugs to `fwsupport@tunix.nl`.

**AUTHOR**

Copyright 1999-2003 TUNIX Internet Security & Opleidingen

**VERSION**

Version \$Revision: 1.5 \$ \$Date: 2003/05/16 13:41:55 \$ (\$Name: RADIUS\_01 \$)