

Software for the Open Enterprise™

United States - English

 Search[Products & Solutions](#)[Services & Support](#)[Partners & Communities](#)[Download](#)[Login](#)

Configuring FreeRADIUS on Open Enterprise Server for Linux

Novell Cool Solutions: Tip

By [Eric Champagne](#)

Cool Solutions Home

[Resources](#)[Appnotes](#)[Cool Tools](#)[Get Involved](#)[Cool Solutions to Go](#)[Other Cools](#)[Cool Blogs](#)[Cool Solutions Wiki](#)[Open Audio \(podcasts\)](#)Reader Rating  from 13 ratings[Rate This Page](#)[tell a friend](#)[printer friendly](#)[Digg This](#) - [Slashdot This](#)*Posted: 31 Aug 2005*

problem:

After many hours and days trying to configure FreeRADIUS on my OES Linux (SUSE 9 Sp1) with LDAP authentication and a access point Linksys WRT54G ... Here's a step by step documentation for you!

Here is my setup and what you should download before starting the procedure.

solution:

Hardware Needed

1. Server for OES Linux
2. Linksys Router Wireless - WRT54G
3. Workstation XP with Wireless Network Card

Software Needed

1. OES Linux (SuSE 9 SP1) - Installed with eDir + NCP + iManager 2.5
Note: FRESH INSTALLATION
2. FreeRADIUS 1.02
<http://forge.novell.com/modules/xfcontent/downloads.php/edirfreeradius/SLES%209/>
3. Certificates Scripts for Freeradius
http://oriol.joor.net/article_fitxers/1574/certs.tar.gz
4. iManager Plugins for RADIUS
<http://forge.novell.com/modules/xfcontent/downloads.php/edirFreeRADIUS>
5. iManager NMAS Client
<http://support.novell.com/cgi-bin/search/searchtid.cgi?10097107.htm>
Note : Follow this TID to extract the NMASCLIENT.NPM

Step 1 - Install FreeRADIUS

1. Copy the 2 packages for FreeRADIUS on your OES Linux server into /tmp directory.

Book: Novell ZENworks
7 Linux Management
Administrator's
Handbook

SUSE Linux 10.1

2. Go into yast
3. Go Software/Install and remove program - Search for FreeRADIUS package. If there are not installed, install it.
Note: We installed FreeRADIUS with Yast because FreeRADIUS have a couple of dependencies. It's more easy to do it like this if you don't know which package is needed.
4. Return at the command line and install both Freeradium RPM.
rpm -Uvh --force /tmp/freeradius-1.0.2-0.i586.r?pm
rpm -Uvh --force /tmp/freeradius-devel-1.0.2-0.i586.rpm
5. Delete the whole CERTS directory under /etc/raddb/
6. Copy certs.tar.gz under /tmp directory.
7. Unzip the certs.tar.gz - tar -zvf
tar -zxf certs.tar.gz
8. Edit CA.certs like this the follow example:

```
COUNTRY="CA"  
PROVINCE="Quebec"  
CITY="Montreal"  
ORGANIZATION="Complys technologies inc"  
ORG_UNIT="HeadOffice"  
PASSWORD="complys" ; Use a password of your choice
```

```
COMMON_NAME_CLIENT="Rezotik Client SSL"  
EMAIL_CLIENT="i...@complys.dot.com"  
PASSWORD_CLIENT=$PASSWORD
```

```
COMMON_NAME_SERVER="Rezotik Server SSL"  
EMAIL_SERVER="i...@complys.com"  
PASSWORD_SERVER=$PASSWORD
```

```
COMMON_NAME_ROOT="Root certificate"  
EMAIL_ROOT="i...@complys.dot.com"  
PASSWORD_ROOT=$PASSWORD
```

9. Go on line 85 into CA.certs and modify the line with the follow one:
echo "newreq.pem" | ./CA.pl -newca || exit 2
10. Copy the whole directory /tmp/certs into /etc/raddb
11. Extract the seft signed certificate with the following step
 - o Open ConsoleOne
 - o Highlight the Security Container
 - o Go on properties of CERTIFICATE AUTHORITY OBJECT then go on the Certificate Tab under Self Signed Certificate
 - o Click on Export - Say NO on export Private Key.
 - o Save your file with B64 format with the following name under /etc/raddb/certs/rootder.b64
12. Modify the file /etc/raddb/radiusd.conf

```
# ... Change under MODULE SECTION ... #
modules {
    pap {
        encryption_scheme = crypt
    }

    chap {
        authtype = CHAP
    }

    pam {
        pam_auth = radiusd
    }

    unix {
        cache = no
        cache_reload = 600
        radwtmp = ${logdir}/radwtmp
    }

$INCLUDE ${confdir}/eap.conf

    mschap {
        authtype = MS-CHAP
        use_mppe = yes
        require_encryption = yes
        require_strong = yes
        authtype = MS-CHAP
    }

    ldap {
        server = "localhost"
        identity = "cn=admin,o=complys"
        password = password # !!! Use your own admin password here !!!
        basedn = "o=complys"
        filter = "(uid=${Stripped-User-Name:-%{?User-Name}})"
        base_filter = "(objectclass=radiusprofile)"
        start_tls = yes
        tls_cacertfile = /etc/raddb/certs/rootder.b64
        access_attr = "dialupAccess"
        ldap_connections_number = 5
        password_attribute = nspmPassword
        edir_account_policy_check=yes
        timeout = 4
        timelimit = 3
        net_timeout = 1

    }

# ... CHANGE UNDER AUTHORIZE SECTION ... #

authorize {
    preprocess
    chap
```

13. Modify the file /etc/raddb/eap.conf

```
eap {
    default_eap_type = peap
    timer_expire     = 60
    ignore_unknown_eap_types = no
    md5 {
    }
    leap {
    }
    tls {
        private_key_password = complys
        private_key_file     = /etc/raddb/certs/cert-srv.pem
        certificate_file     = /etc/raddb/certs/cert-srv.pem
        CA_file              = /etc/raddb/certs/demoCA/cacert?.pem
        dh_file               = /etc/raddb/certs/dh
        random_file          = /etc/raddb/certs/random
        fragment_size       = 1024
        include_length      = yes
    }
    ttls {
        default_eap_type = md5
        copy_request_to_tunnel = yes
        use_tunneled_reply = yes
    }
    peap {
        default_eap_type = mschapv2
    }
    mschapv2 {
    }
}
```

14. Modify the file /etc/raddb/clients.conf

```
client 192.168.1.0/24 {
    secret = rezotik
    shortname = newton
}
```

Note: My subnet is 192.168.1.0/24 ... Change it for your subnet. "secret" attribute is the secret password to know to be able to connect on the Radius Server.

15. Modify the file /etc/raddb/users

!!! EMPTY THE WHOLE FILE !!! We don't need it because you will use authentication LDAP

16. Start FreeRADIUS at the command line : radiusd -X -A

Note: You should see "READY TO PROCESS REQUESTS" if your configuration is good. Otherwise double checked your files.

Note: You should test your radius connection with NTRadPing Utility before continuing.

Step 2 - Install RADIUS Plugin and NMAS Client Plugin into iManager

1. Install RADIUS.NPM and NMASSCLIENT.NPM into iManager **Note:** I will not describe all the step ... I'll assume that you are a Novell Administrator and you should know how to use iManager and add a plugin into it.
2. Install both LDIF included with the NPG files for RADIUS.
Note: The most easiest way to had it without problem is ConsoleOne under Tools/NDS Import/Export
3. Open iManager - Go under RADIUS
4. Click on Extend Schema for RADIUS - Say Yes to Extend the schema.

Step 3 - Create a Universal Password Policy

1. Open iManager - Go under PASSWORD
2. Click on Password Policy
3. Add a NEW POLICY - Give the policy name - Exemple : Universal Password Policy
4. Disable Advanced Password Rules
5. Click on VIEW OPTIONS
6. Enable everything except : Remove the NDS password when setting Universal Password.
7. Next - Next -
8. DON'T ASSIGN ANY USERS OR CONTAINER NOW!

Step 4 - Configure your linksys Router Wireless WRT54G

1. Go into the administration web page of your router.
2. Under Wireless Security - Choose

Security Mode: WPA RADIUS

WPA Algorithms: TKIP

RADIUS Server Address: 192.168.1.30 <----- IP Address of my OES Linux server

RADIUS Port: 1812

Shared Key: complys <----- Secret password of radius server

Key Renewal Timeout: 3600 seconds

Step 5 - Configure your Wireless card under Windows XP

1. Under Network Connection - Go on properties of your Wireless Card
2. Click on Wireless Network
3. Enable : Use Windows to configure my wireless networks settings.
4. Click on ADD under PREFERED NETWORKS SECTION.
5. Enter the SSID of your Wireless Router.
6. Click on AUTHENTICATION TAB
7. Choose in the DROP DOWN LIST for EAP Type : Protected EAP (PEAP)
8. Click on PROPERTIES just under the drop down list.
9. Disable VALIDATE SERVER CERTIFICATE
10. Select Secured password (EAP-MSCHAP v2) for Authentication Method.
11. Click on Configure ...
12. Disable AUTOMATICALLY USE MY WINDOWS LOGON NAME AND PASSWORD
13. Click OK - Click OK
14. Click on CONNECTION Tab
15. Disable CONNECT WHEN THIS IS IN RANGE
16. Click OK.

Note: You should have a connection with your SSIDNAME(On Demand)

Step 6 - Create a USERS and RADIUS USERS under eDirectory

1. Create a user in by ConsoleOne or via iManager

2. Give him username and a password
3. Open iManager - Go under RADIUS
4. Click on CREATE RADIUS USERS
5. Choose the user that you just created
6. Click on MODIFY RADIUS USERS
7. Click on OTHERS ITEMS Tab
8. Add ON to the dialupAccess Attribute.
9. Apply changes

Step 7 - Try your connection with Windows XP wireless card

1. Go under VIEW AVAILABLE WIRELESS NETWORK
2. Click SSIDNAME(ON DEMAND) access point.
3. Enter the credential of the user that you just created
4. THAT'S IT !!!!

Step 8 - Troubleshoot USERS login

1. First Problem - Error FAILED AUTHENTICATE -669 under the FreeRADIUS Console.
Note: A great tools to troubleshoot if your user is ready to work with Radius is UNIVERSAL PASSWORD DIAG UTILITY.

<http://support.novell.com/cgi-bin/search/searchtid.cgi?/2970885.htm>

Note: The NMAS Client plugins for iManager (See STEP 2) should be installed to synchronize UP (Universal Password) with NDS password, etc ...

A good user should return this:

Object DN: cn=radmin,o=complys
EMail: [NONE]
Password Status: Enabled, Set
Simple Password Status: Set
Password Policy DN: cn=Universal Password Policy,cn=Password Policies,cn=Security

a bad user should return this:

Object DN: cn=radius2,o=complys
EMail: [NONE]
Password Status: Enabled, Set, UP != NDS
Simple Password Status: Set, Simple != NDS
Password Policy DN: cn=Universal Password Policy,cn=Password Policies,cn=Security

Hope this will help you. Comments are welcome!


Eric Champagne, CNE, CCNA

Reader Comments


- You rock for figuring this out. I had this on my to-do list, and now my task will be much simpler. Scott Flowers
- Been working with this for awhile. This doc has helped, but the certificate info is not very informative. It is

- however the only thing you can find on Novell's site for setting this up. So thank you for your help.
- Wow ! Wonderful. We need more doc like this one. Very easy to follow the step by step is well done. Bravo ! Bravo ! Craig Johnson
 - This process is inundated with way too much information about certificates (in regard to the title about configuring FreeRADIUS). Perhaps a doc title change?
 - WOW ! Very nice docs. We need more documents like this one. I follow the steps and it works. Craig Johnson
 - Great document! However, I'm having trouble with the certs as well. You say to delete the certs directory, and then unzip the certs.tar.gz zip file. Four files come out of this, and the document asks for many more .pem files that are now gone since I deleted the CERTS folder under /etc/raddb. Any help would be appreciated.
 - Thanks a lot, Eric! The only problem, the oriol.joor.net site is not reachable, can't download certs.tar.gz Sancxo

Like what you see?

Sign up for our weekly newsletter. 


Want to contribute?

It could earn you a nano!
Learn more. 

Like Wikis?

Join the Cool Solutions
Wiki. 

**Interested?**

Request a sales
call 

Novell Cool Solutions (corporate web communities) are produced by WebWise Solutions. www.webwiseone.com