

FreeRadius integration with Novell eDirectory

Date: 28 December 2005
Author: Alexandre Dachine
Version: 1.1

Prerequisites

Necessary hardware

1. Server to host Novell OES Linux
2. Access Point WiFi CISCO AIRONET 1100 series (AIR-AP1121G-A-K9)
3. Windows XP/W2K laptops with WiFi network adapter

Necessary software

1. *Novell OES Linux*
http://download.novell.com/Download?buildid=ppIBUh_8JW0
The following images are necessary:
oes-sp1-linux-1.iso
oes-sp1-linux-2.iso
oes-sp1-linux-3.iso
oes-sp1-linux-5-sles9-2.iso
oes-sp1-linux-6-sles9-3.iso
oes-sp1-linux-7-sles9-4.iso
2. *FreeRadius*
<http://forge.novell.com/modules/xfcontent/downloads.php/edirfreeradius>
Use the SLES9 modules.
3. *RADIUS Plug-in for iManager*
<http://forge.novell.com/modules/xfcontent/downloads.php/edirfreeradius>
4. *Certificate creation scripts for FreeRadius*
http://oriol.joor.net/article_fitxers/1574/certs.tar.gz
5. *iManager v2.5*
6. *Latest Novell client for Windows with NMAS/NICI option*

Useful documentation

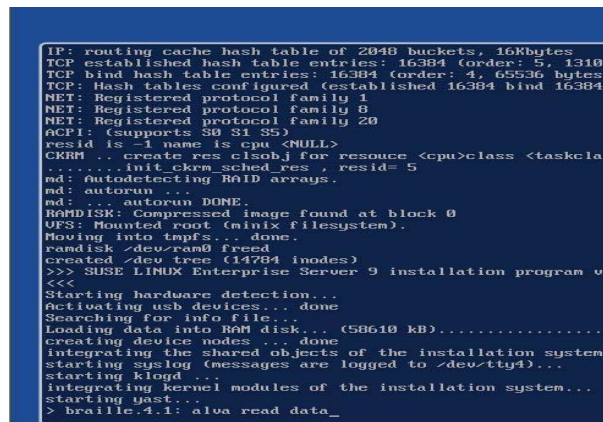
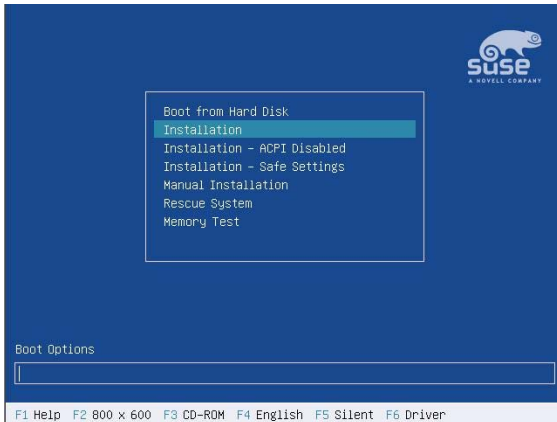
1. http://www.novell.com/documentation/edir_radius/index.html (by Novell)
2. <http://www.novell.com/coolsolutions/tip/15922.html> (by E.Champagne)

Novell OES Linux Server Installation

Important: Before starting, read the following Novell document:
(http://www.novell.com/documentation/oes/pdfdoc/install_linux/install_linux.pdf)

1. Burn CDs from downloaded images.
2. Boot the server with the "*OES-SPI-LINUX-1*" CD.

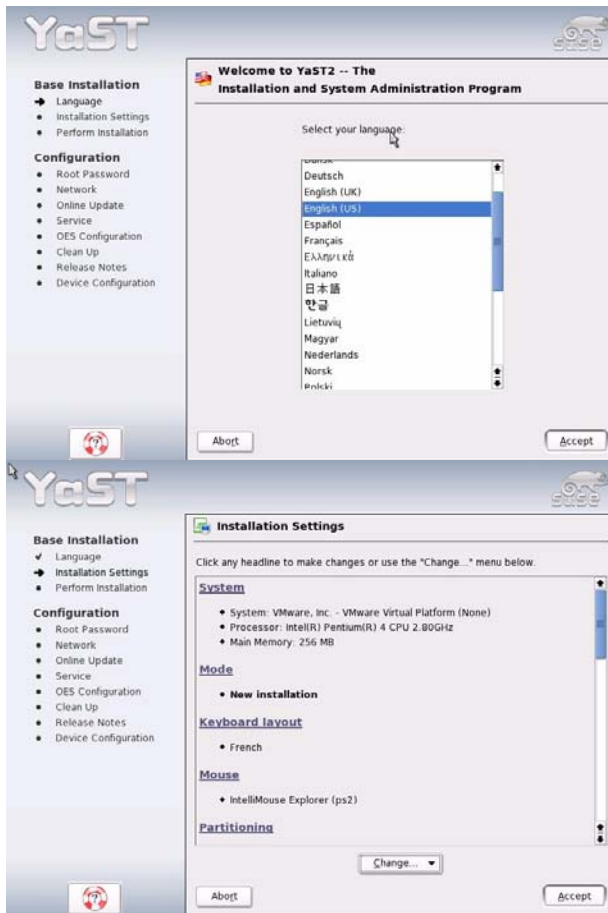
The Installation program starts automatically:



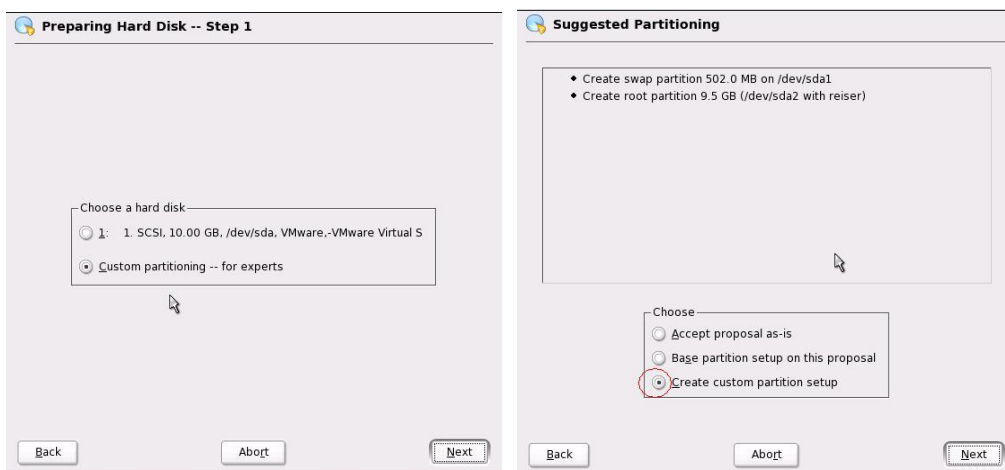
3. Accept the license and continue.



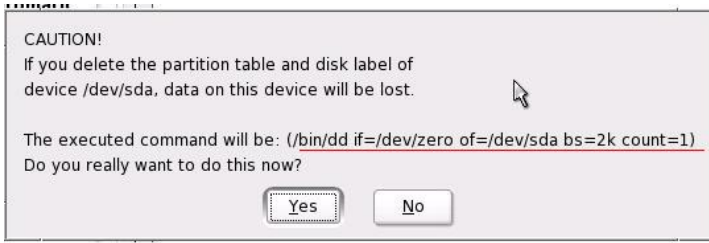
4. Start the setup.



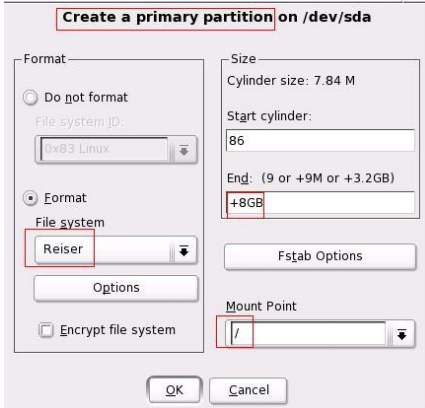
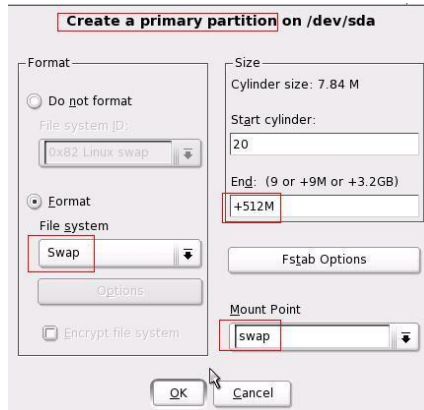
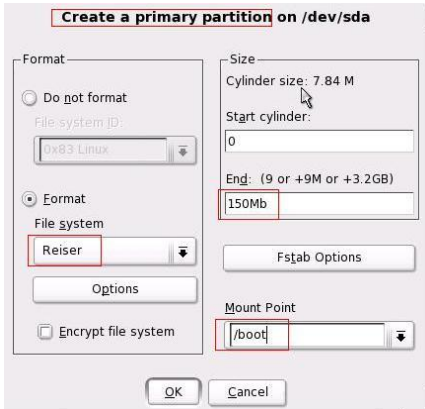
5. Create partitions depending on your needs. Generally, the default configuration proposed by Setup is not sufficient.
 In our case (one physical disk or one logical drive RAID5) the three partitions /, **boot**, and **swap** will be native Linux (outside of the LVM group) and the eventual other ones will be in LVM group. The advantage of LVM partitions is that they can be extended online, without stopping the running system.



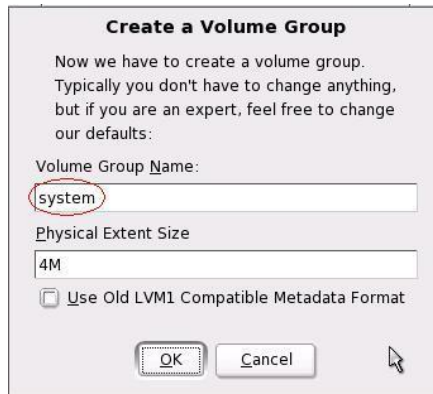
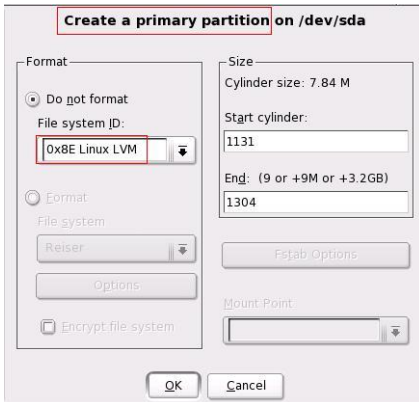
Select 'Expert', then 'Delete partition table and disk label'.

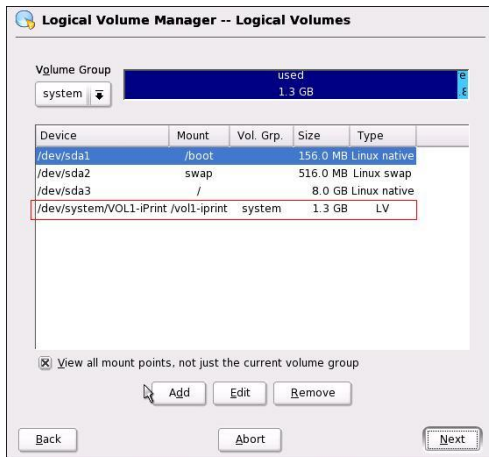
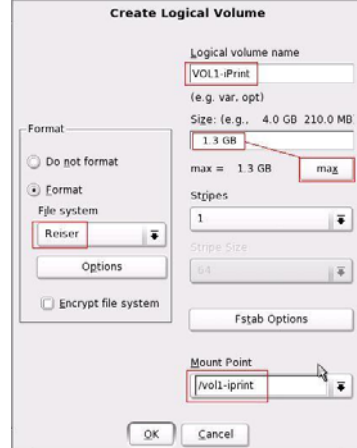
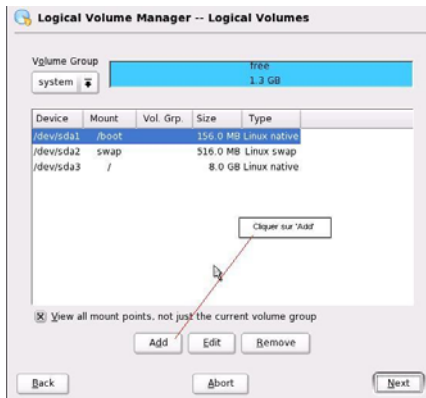
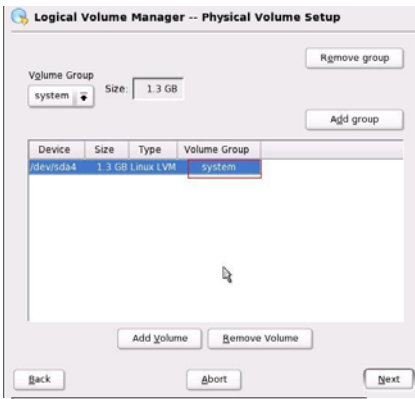
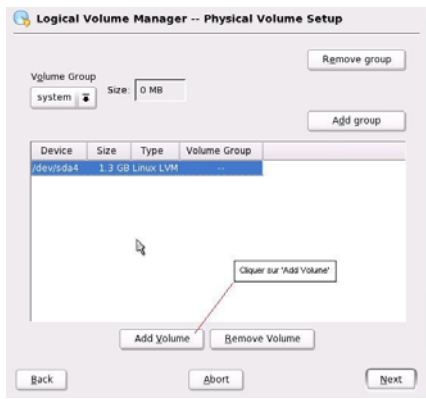


Create partitions /boot, swap, etc.

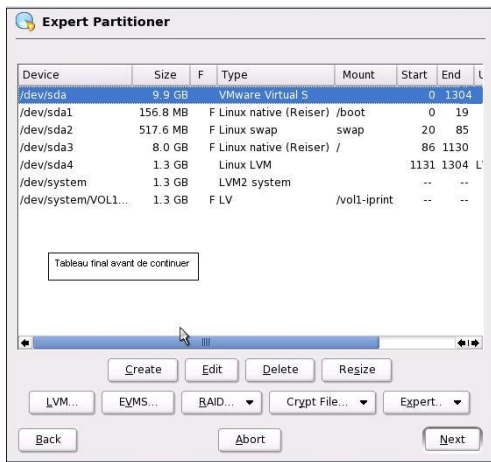


LVM configuration:

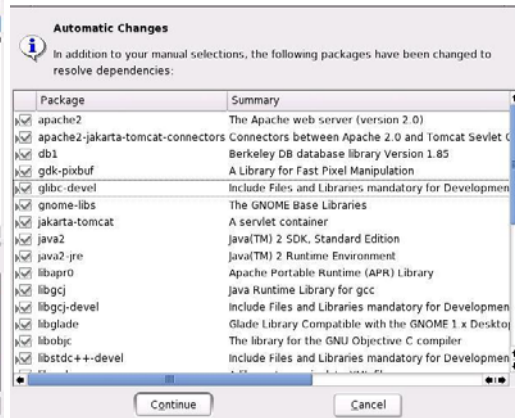
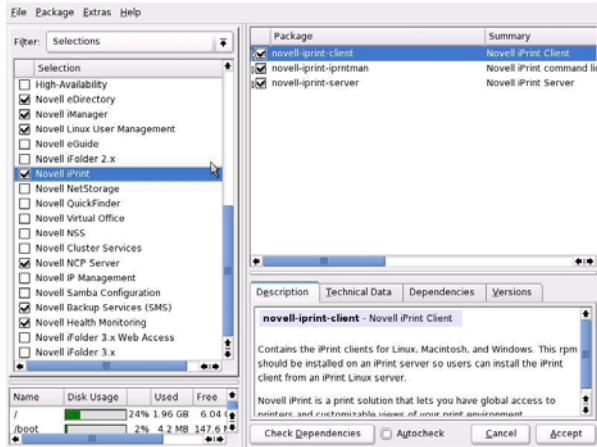
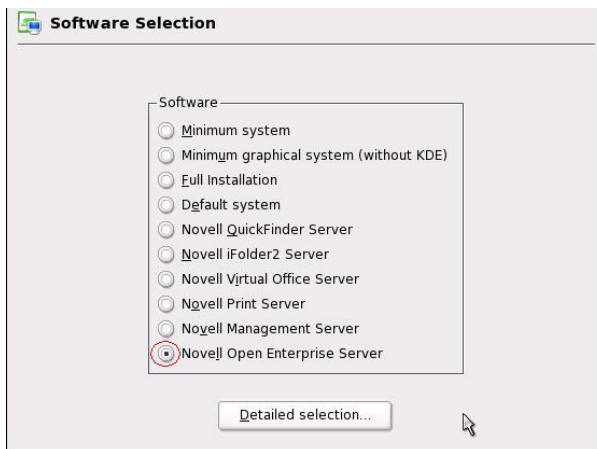


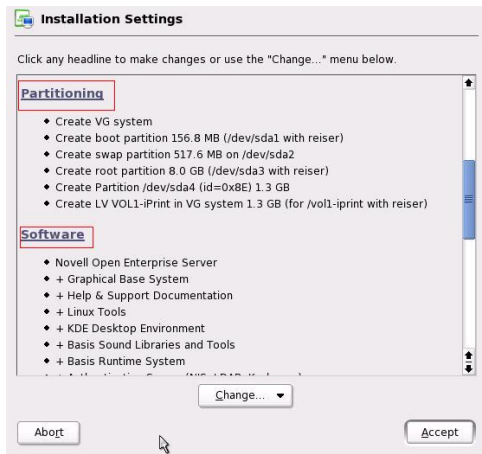


This final table shows partitions before continuing:

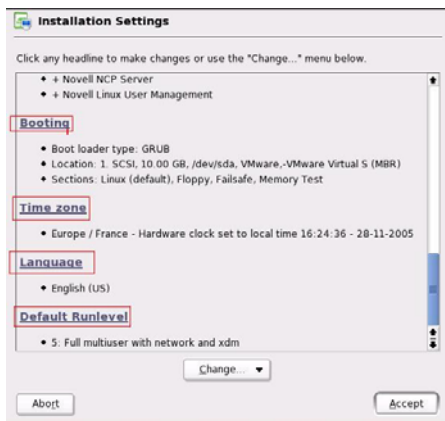


6. Select the installation type 'Novell Open Enterprise Server' and the necessary packages.

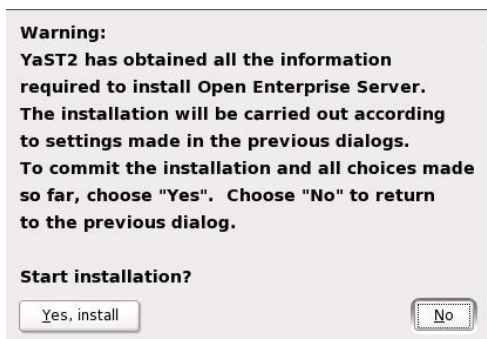




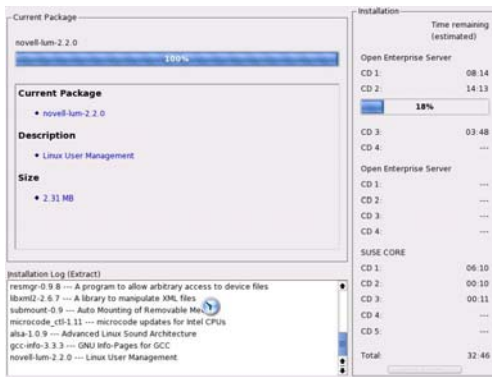
7. Validate other parameters, such as boot type, OS language, time zone and default run-level.



8. Now Setup is ready to copy files.



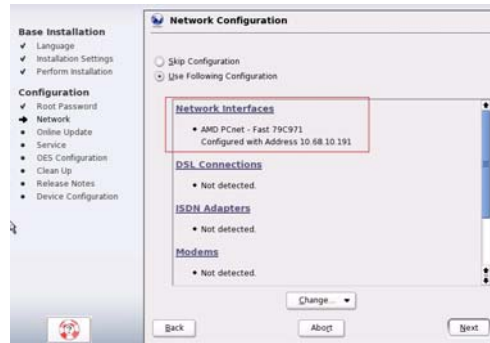
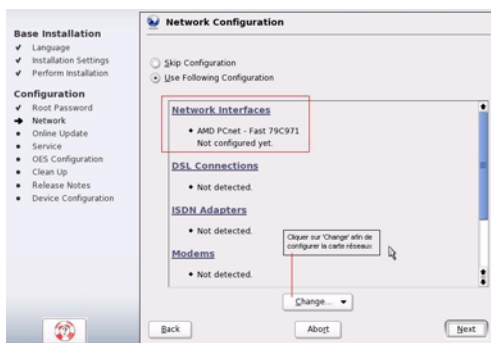
The copy starts and takes between 20 and 60 min., depending on server performances and amount of selected packages. After that the server restarts automatically.



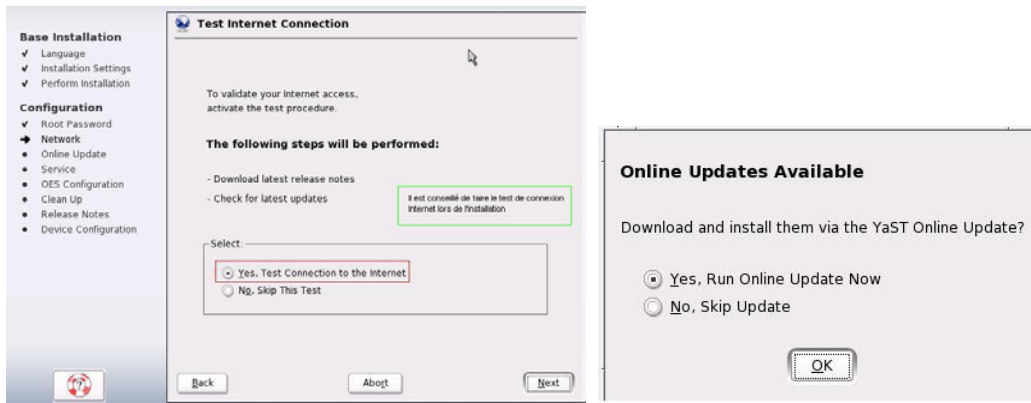
- After reboot the setup goes on. You are asked to give the root password. If the password is longer than 8 characters, click 'Expert', then 'Blowfish'; if not, the password will be truncated.



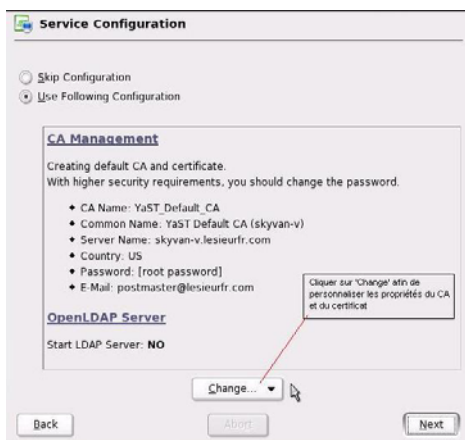
- Select and configure the NIC(s).



- Test the Internet connection during the setup.



12. Customize the properties of the CA and the common certificate. Personally, I would name the common certificate the same as the server, such as *srv1.domain.org*



The next step is eDirectory configuration. You have two options:

- (A) Join an existing tree
- (B) Create a new tree

13. In case (A) you must make sure that the tree is healthy and ready to accept a new Linux server, and the schema has been extended. See <http://www.novell.com/documentation/oes/pdfdoc/coexist-mig/coexist-mig.pdf> and http://www.novell.com/documentation/oes/pdfdoc/install_linux/install_linux.pdf. The following screenshots show how to create new tree.

eDirectory Configuration - New or Existing Tree

New or Existing Tree

New Tree

Existing Tree

Tree Name

SKY-V

Back Abort Next

eDirectory Configuration - New Tree Information

EDN admin name with context (i.e. cn=admin.o=novell)

cn=admin.o=asn

Admin Password

Verify Admin Password

Back Abort Next

eDirectory Configuration - New Server Configuration

Enter Server Context

o=asn

Directory Information Base (DIB) Location

/var/nds/dib

Enter LDAP Port

389

Enter Secure LDAP Port

636

Enter iMonitor Port

8028

Enter Secure iMonitor Port

8030

Back Abort Next

eDirectory Configuration - NTP & SLP

Network Time Protocol (NTP) Server

Un des serveurs locaux

10.68.10.168

Do not configure SLP

Use multicast to access SLP

Configure SLP to use an existing Directory Agent

SLP sera configuré plus tard, si nécessaire

Service Location Protocol Directory Agent Address

Service Location Protocol Scopes

DEFAULT

Back Abort Next

Perform eDirectory Configuration

- ✓ Save configuration information for YaST2
- ✓ Perform time synchronization
- ✓ Configure and start the Service Location Protocol
- ✓ Copy the NICI Foundation Key file
- ✓ Establish eDirectory on all static IP addresses

Configuring and starting eDirectory

This will take a while.....

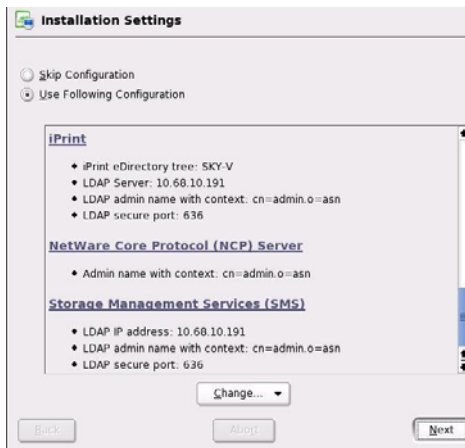
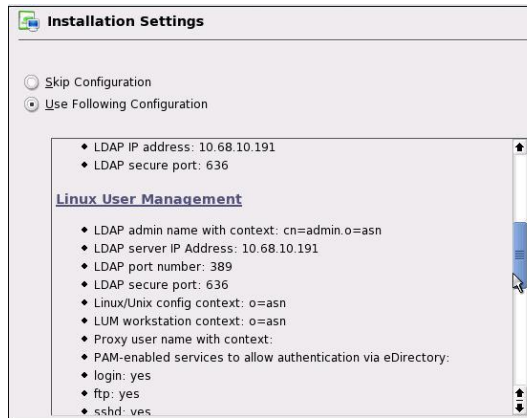
- Wait for eDirectory to respond to LDAP requests
- Fetch the eDirectory tree root certificate
- Perform OES schema extension
- Configure the default NMAS login method

Configure and start eDirectory using "ndsconfig"

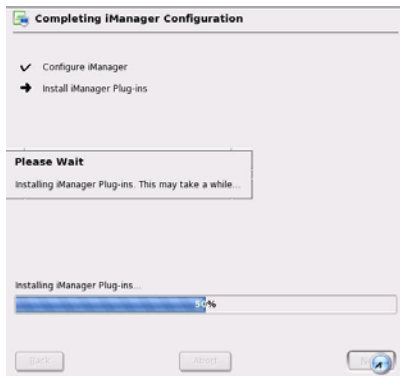
54%

Back Abort Next

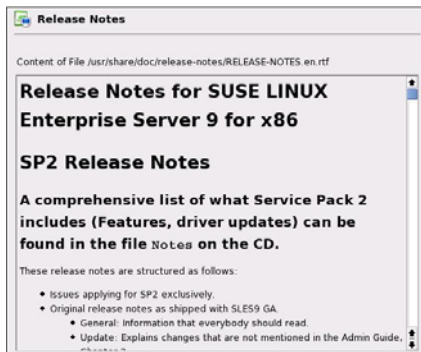
14. After eDirectory configuration has finished, the setup shows a summary table indicating the configuration of Novell products selected during previous steps (for example, iManager, SMS, LDAP, etc.).



15. The configuration of selected products is now finalized.



16. Release notes are displayed.



17. Check the video configuration (monitor, resolution, graphical adapter, etc.) and modify if necessary.
18. Finally, the last screen says the setup is finished. Click OK and reboot.

Applying Patches on Novell OES Linux server

There are two possibilities: **rug** or **RedCarpet**. Officially Novell doesn't support Red Carpet in this version of OES (see http://www.novell.com/documentation/oes/pdfdoc/install_linux/install_linux.pdf).

1. Open a Terminal session with root account and type the following commands:

```
rug set-prefs cache-directory /patches/oes/10-nov-2005 #optional  
rpm -qa |grep pubkey
```

```
skyvan-u:/media/cdrom # rpm -qa | grep pubkey  
gpg-pubkey-0dfb3188-41ed929b  
gpg-pubkey-9c800aca-40d8063e  
gpg-pubkey-15c17deb-3f9e80c9  
gpg-pubkey-3d25d3d9-36e12d04  
skyvan-u:/media/cdrom # █
```

rug sl

```
skyvan-u:/media/cdrom # rug sl  
# | Service URI | Name  
-----  
1 | https://update.novell.com/data | Novell_Update_Server  
skyvan-u:/media/cdrom # █
```

```
rug act -s 1 activation-code-received-from-Novell email-address #activation OES
```

rug sub oes

```
skyvan-u:/media/cdrom # rug act -s 1 2B8AF458ECD900 sancxo@rin.r  
System successfully activated  
Refreshing channel data  
Refresh complete  
skyvan-u:/media/cdrom # rug sub oes  
Subscribed to channel 'oes'  
skyvan-u:/media/cdrom # █
```

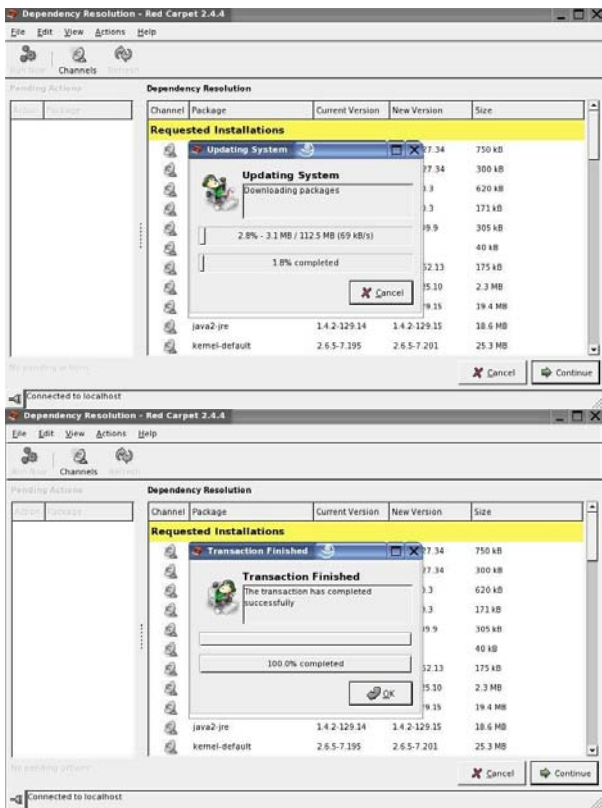
rug pl #lists all available patches

rug pin oes:* #installation of patches, time-consuming!

The download and successful installation are confirmed by following messages:

Download complete
Transaction finished

If patches were applied with Red Carpet, you will see following messages:



2. Reboot the server.

FreeRadius Server Installation

1. Copy the packages *freeradius-1.0.2-0.i586.rpm*, *freeradius-devel-1.0.2-0.i586.rpm*, *certs.tar.gz* and *radius_npm.tar.gz* into a temporary folder (for example, /tmp/freeradius/sources).

2. Launch YAST and install the following packages:

cyrus-sasl-devel	openssl	postgresql-libs
heimdal-devel	openssl-devel	python
heimdal-lib	postgresql-devel	python-devel
mysql-devel	openldap2-client	db-devel
mysql-shared	openldap-devel	

3. Install FreeRadius, from the Terminal console:

4. rpm -Uhv freeradius-1.0.2-0.i586.rpm
rpm -Uhv freeradius-devel-1.0.2-0.i586.rpm

```
SRV&SNO2:/tmp/freeradius/sources #  
SRV&SNO2:/tmp/freeradius/sources # rpm -Uhv freeradius-1.0.2-0.i586.rpm  
Preparing... ##### [100%]  
 1:freeradius ##### [100%]  
SRV&SNO2:/tmp/freeradius/sources # rpm -Uhv freeradius-devel-1.0.2-0.i586.rpm  
Preparing... ##### [100%]  
 1:freeradius-devel ##### [100%]  
SRV&SNO2:/tmp/freeradius/sources # █
```

FreeRadius Server Configuration+

1. Uncompress the package *radius_npm.tar.gz*
`tar -zxf radius_npm.tar.gz`

Copy *radius.npm* to `/var/opt/novell/iManager/nps/packages/` so iManager can find it.
`cp /tmp/freeradius/sources/radius.npm /var/opt/novell/iManager/nps/packages/`

2. Install the FreeRadius and NMAS plug-ins in iManager.

- Launch iManager.
- Go to Configure iManager, then Module Installation, then Available Novell Plug-in Modules.
- Select Novell Radius Plugin (2.5.20050406) and NMAS plugin for eDirectory (2.5.0.20050224).
- Click Install.
- Re-launch Tomcat and Apache.

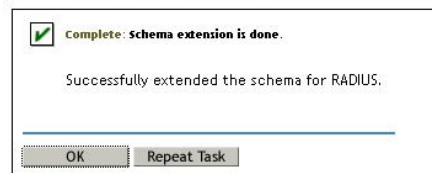
`rcnovell-tomcat4 restart`
`rcapache2 restart`

- If needed, reboot the server

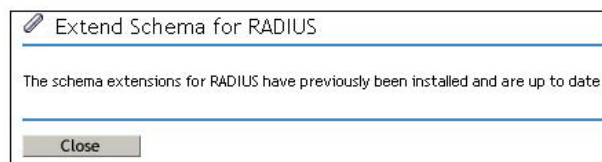
3. Extend the eDirectory schema.

The Novell documentation describes three possible scenarios. In our case it's number 3 (rather simple):

- Launch iManager.
- Choose RADIUS, 'Extend Schema for Radius'.



If the schema is already extended, a message will confirm that.



4. Generate and customize the FreeRadius client & server certificates.

`mv /etc/raddb/certs /etc/raddb/certs.org`
`tar -zxf /tmp/freeradius/sources/certs.tar.gz`

One of files generated is *root.der*. You will need to install it on your laptops.

- Open **CA.certs** and modify it as follows:

```
# Edit the following variables for your organization.
#
COUNTRY="FR"
PROVINCE="IdF"
CITY="PARIS"
ORGANIZATION="Your-Company"
ORG_UNIT="HeadOffice"
PASSWORD="XXXXX"

COMMON_NAME_CLIENT="LESIEUR FreeRadius"
EMAIL_CLIENT="v-info@rin2.fr"
PASSWORD_CLIENT=$PASSWORD

COMMON_NAME_SERVER="LESIEUR Server FreeRadius"
EMAIL_SERVER="v-info@rin2.fr"
PASSWORD_SERVER=$PASSWORD

COMMON_NAME_ROOT="LESIEUR SRVASN02"
EMAIL_ROOT="v-info@rin2.fr"
PASSWORD_ROOT=$PASSWORD

#
# lifetime, in days, of the certs
#
#LIFETIME=760
# modified by A.Dachine, Dec 7, 2005
LIFETIME=3650
```

- Modify also the line number 85, as follows
echo "newreq.pem" | ./CA.pl -newca || exit 2

- (optional) Modify also the line number 68 of the file /etc/ssl/openssl.cnf, as follows
default_days = 3650 #10 years

- Go to the folder where the script **certs.sh** is stored (/tmp/freeradius/sources) and run it, as follows:

./certs.sh

- Copy the entire folder /tmp/freeradius/sources/certs to /etc/raddb/certs.

cp -r /tmp/freeradius/sources/certs /etc/raddb/

- Extract the eDirectory auto-signed certificate.

- Launch iManager and login to eDirectory.
- Go to 'eDirectory administration', then 'Modify Object'
- Select the CA object and go to its properties. This object is unique in eDirectory and is found in the SECURITY container. In our production eDirectory, the server holding CA role is NOT the FreeRadius server - this is *not* a problem.
- Click the Certificates tab, then choose Self-Signed.
- Click Export and choose NO for private key.
- Save the file in B64 format, named as **/etc/raddb/certs/rootder.b64**



Do you want to export the private key with the certificate?

Yes

No

Select an output format.

File in binary DER format

File in Base64 format

The certificate has been exported using the following parameters:

Parameter	Value
Export private key	No
File format	Base64 encoded

[Save the exported certificate to a file.](#)

7. Modify the file /etc/raddb/radiusd.conf as follows:

```
max_requests = 7680
#server's IP
bind_address = 100.68.100.152
port = 1812
hostname_lookups = no
log_stripped_names = yes
log_auth = yes

# MODULE CONFIGURATION
modules {
    pap {
        encryption_scheme = crypt
    }

    chap {
        authtype = CHAP
    }
    pam {
        pam_auth = radiusd
    }

    # Extensible Authentication Protocol
$INCLUDE ${confdir}/eap.conf

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

    # Lightweight Directory Access Protocol (LDAP)
    ldap {
        server = "srv02.zoo.com"
        identity = "cn=adm-radius,ou=site2,o=zoo"
        password = YYYYYY
        basedn = "o=zoo"
        filter = "(uid=%{Stripped-User-Name}:-%{User-Name})"
        base_filter = "(objectclass=radiusprofile)"
        start_tls = yes
        tls_cacertfile = /etc/raddb/certs/rootder.b64
        tls_cacertdir = /etc/raddb/certs/
        tls_require_cert = "demand"
        access_attr = "dialupAccess"
        dictionary_mapping = ${raddbdir}/ldap.attrmap

        ldap_connections_number = 10
        password_attribute = nspmPassword
        edir_account_policy_check=yes
    }
}
```

```

        timeout = 4
        timelimit = 3
        net_timeout = 1
    }
authorize {
    #
    preprocess
    auth_log
    chap
    mschap
    suffix
    eap
    # Read the 'users' file
    files
    ldap
}
# Authentication.
authenticate {
    Auth-Type PAP {
        pap
    }
    Auth-Type CHAP {
        chap
    }
    Auth-Type MS-CHAP {
        mschap
    }

    unix

    Auth-Type LDAP {
        ldap
    }

    eap
}
# Post-Authentication
post-auth {
    reply_log
    ldap
    Post-Auth-Type REJECT {
        ldap
    }
}
}

```

8. Modify the file /etc/raddb/clients.conf as follows:

```

client 100.68.100.0/23 {
    secret      = XXXXX
    shortname   = Site-ASN-Servers
}
#
client 100.68.160.0/24 {
    secret      = XXXXX
    shortname   = Access-Points-WiFi_DATA
    nastype     = other
    ### nastype = cisco
}

```

9. Modify the file /etc/raddb/eap.conf as follows :

```

eap {
default_eap_type = peap
timer_expire    = 60
ignore_unknown_eap_types = no
cisco_accounting_username_bug = no

    md5 {
    }
    leap {
    }

    gtc {
        challenge = "XXXXXX"
        auth_type = PAP
    }
    tls {
#       private_key_password = whatever
        private_key_password = XXXXXX
        private_key_file = /etc/raddb/certs/cert-srv.pem
        certificate_file = /etc/raddb/certs/cert-srv.pem
        # Trusted Root CA list
        CA_file = /etc/raddb/certs/demoCA/cacert.pem
        dh_file = ${raddbdir}/certs/dh
        random_file = ${raddbdir}/certs/random
        fragment_size = 1024
        include_length = yes

        #       check_crl = yes
#       check_cert_cn = %{User-Name}
    }
    ttls {
        default_eap_type = md5
        copy_request_to_tunnel = yes
        use_tunneled_reply = yes
    }

    peap {
        default_eap_type = mschapv2
    }
    mschapv2 {
    }
}
}

```

10. Modify the file /etc/raddb/users.

The goal of modification is to just empty the file, because LDAP directory will be used instead.
If you do not want to empty it, find the following line

DEFAULT Auth-Type = System

and replace it with **DEFAULT Auth-Type = LDAP**

11. Activate the UP (Universal Password) for eDirectory users who are going to use FreeRadius.

- Launch iManager
- Go to 'Passwords', Password policies, New
- Give a name to the policy and configure it.
 - ** ' Remove the NDS Password when setting Universal Password ' : No
 - ** ' Synchronize NDS Password when setting Universal Password ' : Yes
 - ** ' Synchronize Simple Password when setting Universal Password ' : Yes

- ** ' Allow user agent to retrieve password' : Yes
- ** ' Allow admin agent to retrieve passwords' : Yes
- ** ' Synchronize distribution password when setting Universal Password' : Yes
- ** ' Verify whether existing passwords comply with the password policy (verification occurs on login)' : Yes

Password Policy Wizard

Step 1 of 8: Name and describe the Password Policy

Create a policy name and description of the policy that you are creating.

Policy Name:
 (ex. Engineering)

Description:

Password Change Message:

Create a new Password Policy based on the default settings (Click Next to see summary)

Password Policy Wizard

Step 2 of 8: Select the Universal Password options

Universal Password lets you simplify the integration and management of different password and authentication Policy, you can increase security by setting rules for how users create their passwords.

Would you like to enable Universal Password?

No (skip to Step 4)

Yes (skip to Step 4)

Enable the Advanced Password Rules (go to Step 3)

Hide Options

Universal Password Synchronization

Remove the NDS password when setting Universal Password

Synchronize NDS password when setting Universal Password

Synchronize Simple Password when setting Universal Password

Universal Password Retrieval

Allow user agent to retrieve password

Allow admin to retrieve passwords

Synchronize Distribution Password when setting Universal Password

Authentication

Verify whether existing passwords comply with the password policy (verification occurs on login)

Password Policy Wizard

Step 4 of 8: Enable the Forgotten Password feature

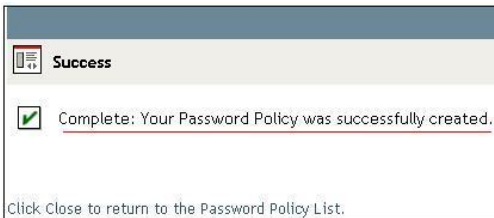
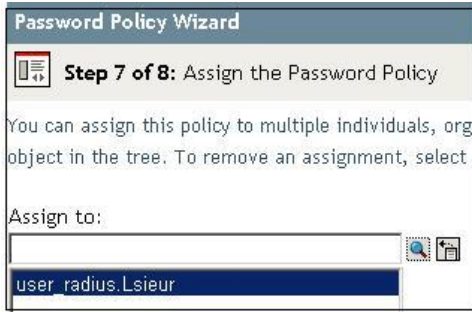
This feature lets you set up self-service options for users who remember a password.

Would you like to enable the Forgotten Password feature?

Yes

No (skip to Step 7)

- Associate the policy with FreeRadius users (user by user, or with OU).



12. Create a user like *adm_radius*, with a password. This account will be used to do LDAP searches. Do not deactivate it!

13. Make sure the user *adm_radius* has the following rights for each FreeRadius user:

- ** Compare/Read/Write for ACL attribute
- ** Compare/Read for all attributes rights
- ** Browse for Entry rights



14. Give the user *adm_radius* retrieval rights for Universal Password (if this wasn't done yet).

- Launch iManager
- Go to Passwords, Password Policies
- Select or create a policy, then edit it
- Go to Universal Password, Configuration Options
- Select 'Allow admin to retrieve passwords' in 'Universal Password Retrieval'

15. Declare an eDirectory user as a FreeRadius user.

- Create a new eDirectory user (or choose an existing one) with a password.
- Launch iManager and go to the RADIUS category.
- Click Create Radius User and select the user just created, then click OK.
- Click Modify Radius User, select the user just created, and click the 'Other Items' tab.
- Find the 'Dial Up Access' attribute and set it to ON, then click OK.
- Make sure the user is associated with the policy created in step 11 (Passwords, Passwords Policies).
- If necessary, manually type the UP.
- In iManager, go to Set Universal Password and check to see that the NDS has not expired.

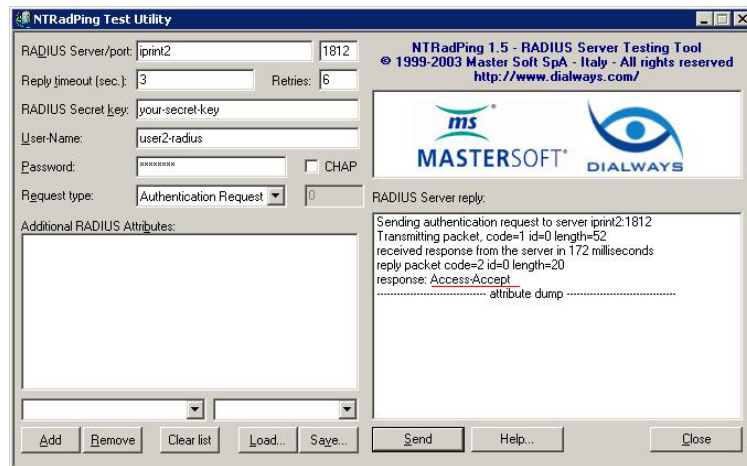
16. Make absolutely sure that eDirectory object of each FreeRadius user contains the '**UniqueID**' attribute. It must contain the login name of the user. If the attribute doesn't exist, add it. Otherwise, LDAP searches, which are the part of authorization / authentication FreeRadius process, will fail.

17. Start the RADIUS service:

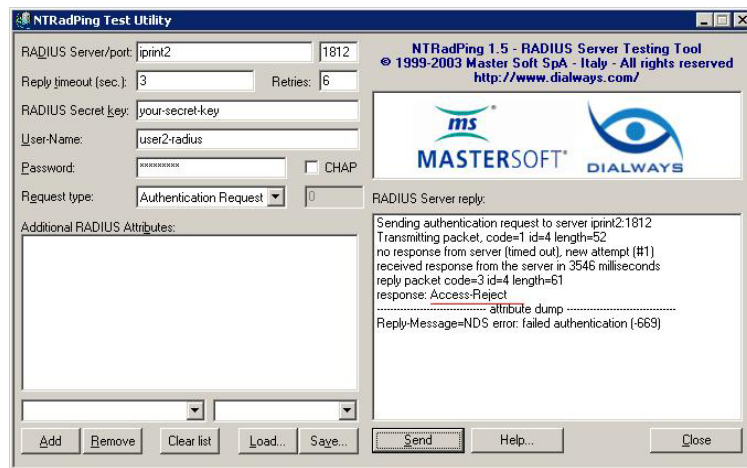
rcradiusd start

18. Before configuring the laptops, test FreeRadius with:

*** *NTRadPing*, from a workstation



Good result --->



Bad result --->

*** **radtest** command, locally on server

Good result:

```
radtest user2-radius password iprint2:1812 1812 secret-passphrase
Sending Access-Request of id 218 to 10.68.10.152:1812
  User-Name = "user2-radius"
  User-Password = "password"
  NAS-IP-Address = iprint2
  NAS-Port = 1812
rad_recv: Access-Accept packet from host 10.68.10.152:1812, id=218, length=20
```

Bad result:

```
radtest user2-radius password iprint2:1812 1812 secret-passphrase
Sending Access-Request of id 218 to 10.68.10.152:1812
  User-Name = "user2-radius"
  User-Password = "password"
  NAS-IP-Address = iprint2
  NAS-Port = 1812
rad_recv: Access-Reject packet from host 10.68.10.152:1812, id=218, length=20
```

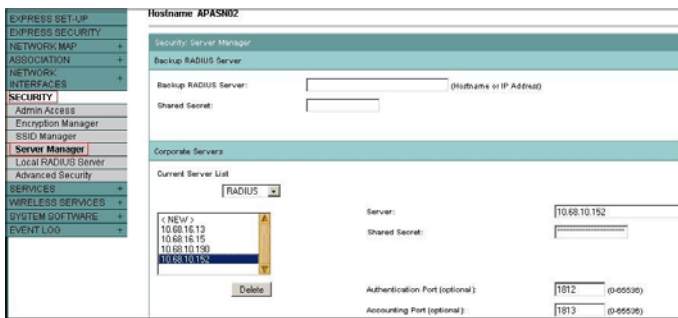

*** Testing the UP and NDS passwords synchronization with UP Diag Tool could be useful, too. We did not need it. (<http://support.novell.com/cgi-bin/search/searchtid.cgi?/2970885.htm>)

Access Points Configuration

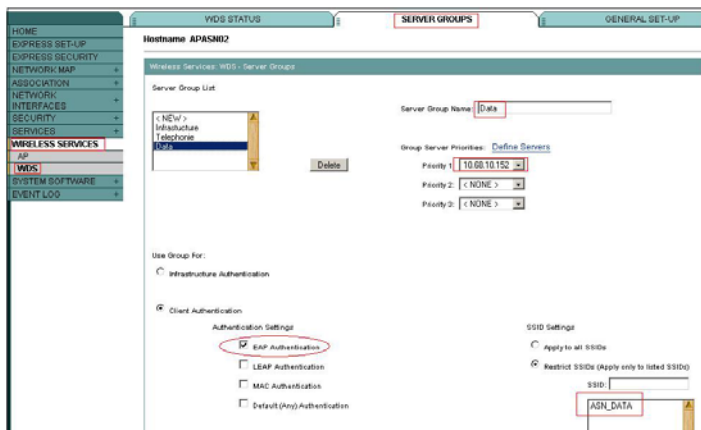
Model: CISCO AIRONET 1100 series (AIR-AP1121G-A-K9)

Note: Your configuration may be different.

1. Log in to the HTTP interface of the AP (Access point). We have two.
2. Go to Security/Server Manager/ and add the following information to the 'Current Server List RADIUS' list:
 - IP address of FreeRadius server
 - Secret phrase
 - Port numbers (1812 and 1813, by default)Click Apply.



3. Go to Wireless Services/WDS, 'Server Groups' tab, select the server group list 'Data' and:
 - Put the IP address of FreeRadius server in the 'Priority 1' field
 - make sure that 'Client Authentication' = 'EAP Authentication'
 - make sure that 'Restrict SSID' = 'ASN_DATA'
4. Click Apply.



The WiFi APs now redirect the authentication requests of laptops to the FreeRadius server.

Laptop Configuration

Context:

We want to have as few authentications as possible (our laptops open two sessions: local and Novell). The goal here is to catch the login/password pair of the local Windows session and forward it to FreeRadius, which, in turn, will check it against eDirectory. If the login/password is validated by eDirectory, the user is assigned an IP address and allowed to use network services. Otherwise, IP address is not assigned and the user can access nothing on the LAN.

So, if FreeRadius is configured correctly, a user opens local Windows session, is validated by LDAP (eDirectory), and then opens a second session to the Novell network.

Models used:

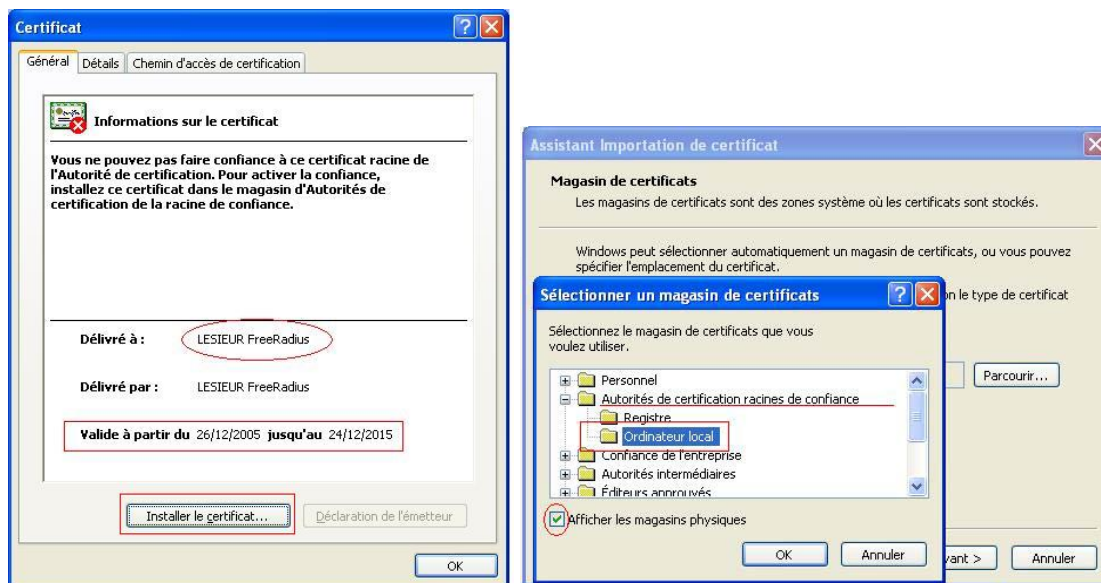
Dell Latitude D610 (Intel PRO 2200BG), Dell Latitude D600 (TrueMobile 1300 MiniPCI) and Dell Latitude D600 (Intel PRO 2100 3A)

Common steps for all models:

*** Do not use the Windows WiFi client, because it functions poorly. Use the proprietary WiFi client/tool instead.

*** Update the WiFi driver and configuration tool.

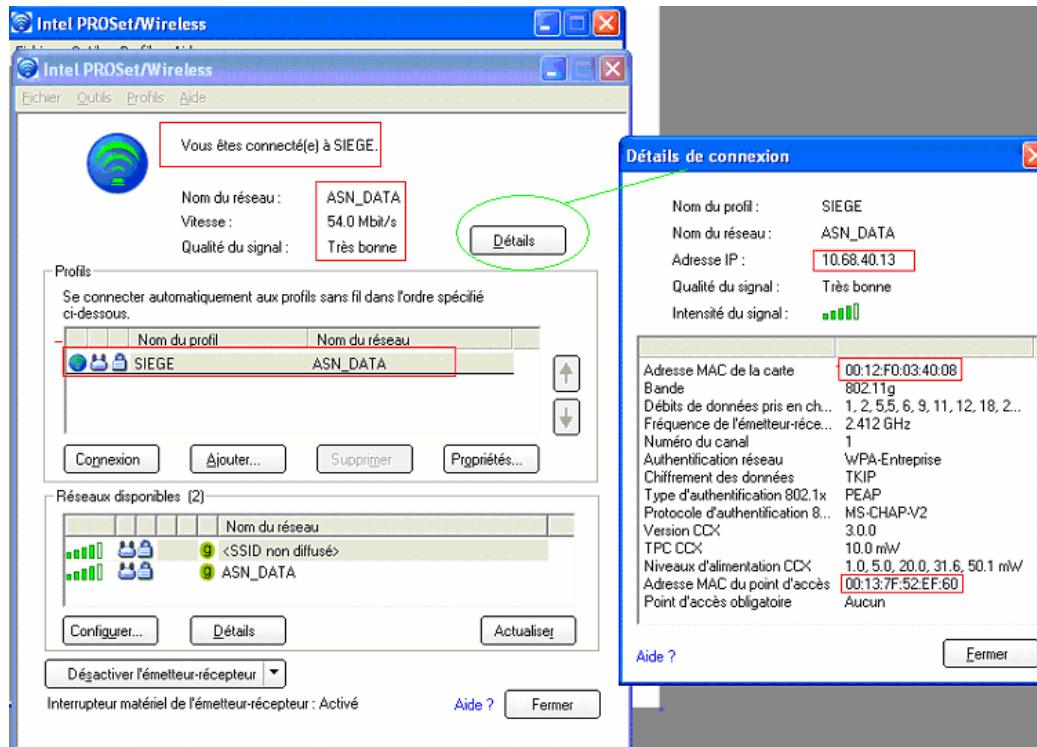
*** Install the *root.der* certificate in the 'Trusted root certification authorities' category. During WiFi connection profile configuration do not forget to select this security certificate.



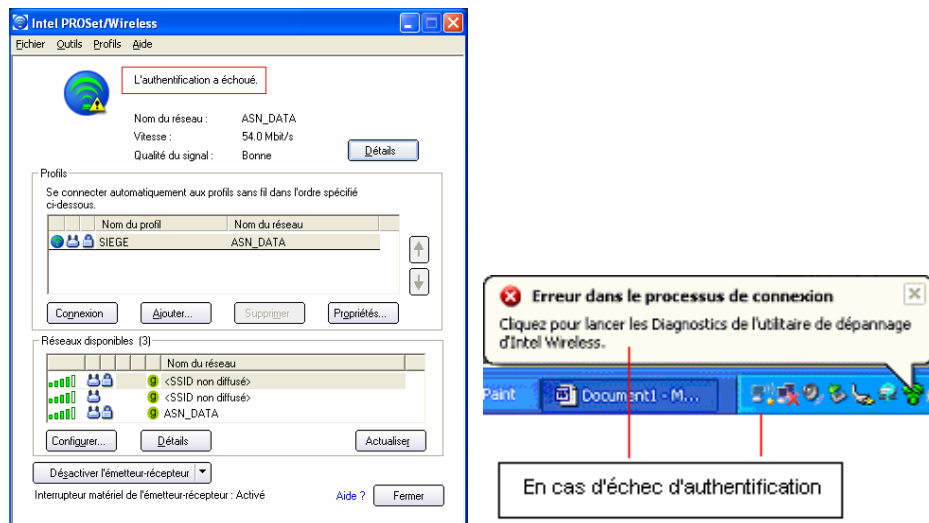
Dell Latitude D610 (Intel PRO 2200BG)

For a driver update go to <http://support.euro.dell.com/support/downloads/> and find the *R107434.exe* file.

How to check if you are connected:



In case of authentication failure you will see following messages and information:



(In case of authentication failure)

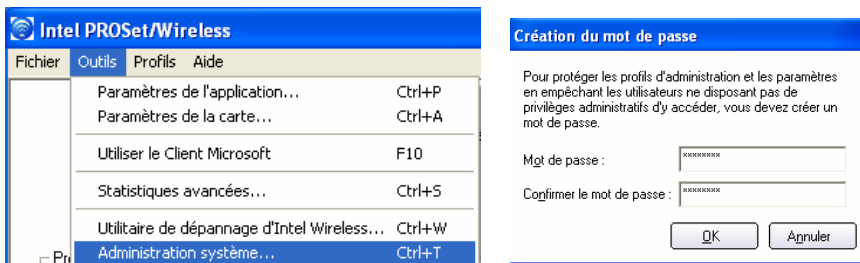


la carte WiFi cherche le réseau

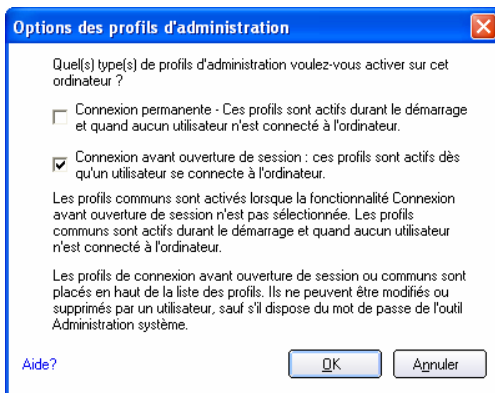
(The WiFi card seeking the network ...)

Configuring the Intel PROSet/Wireless tool

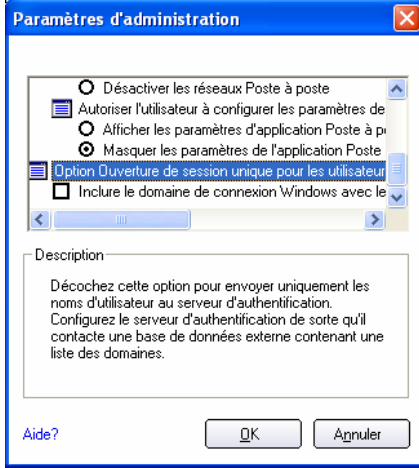
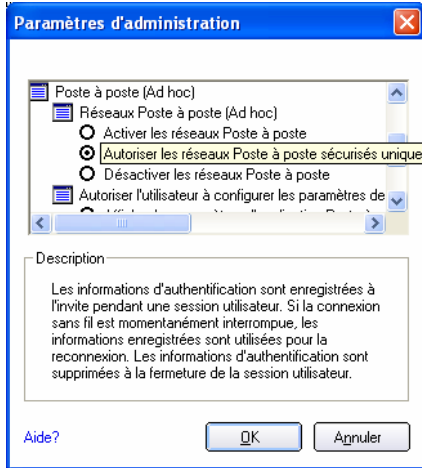
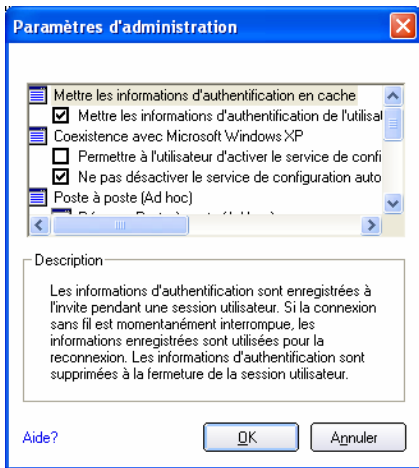
1. Go to Tools / System Administration and provide a password.



2. Click Options and select “Connection before session opening”).

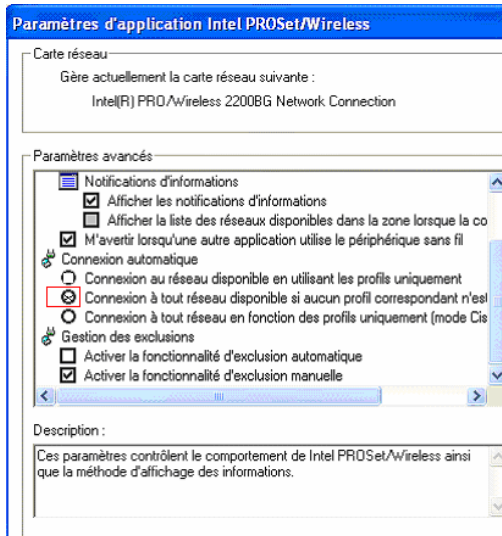
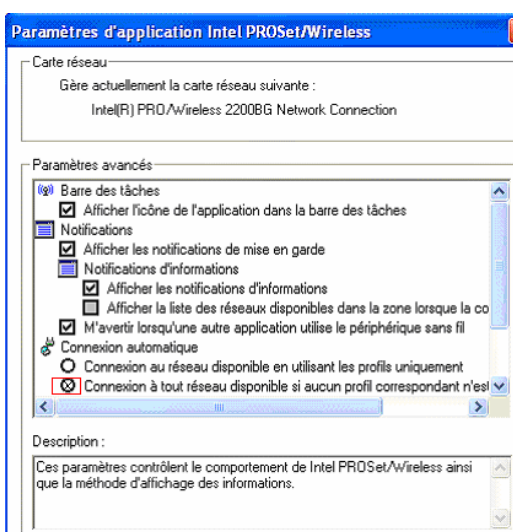


3. Click Parameters and select the options shown below.



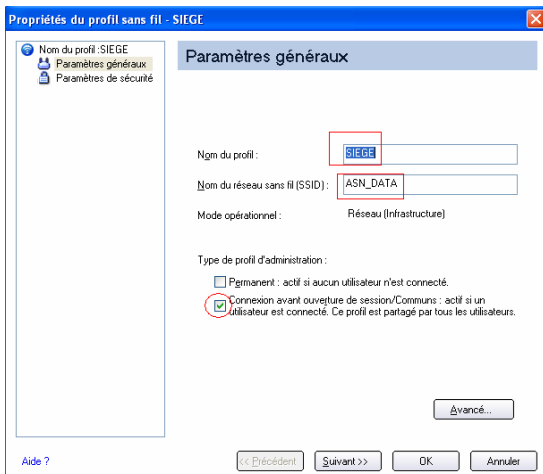
4. Go to Tools / Application Parameters.



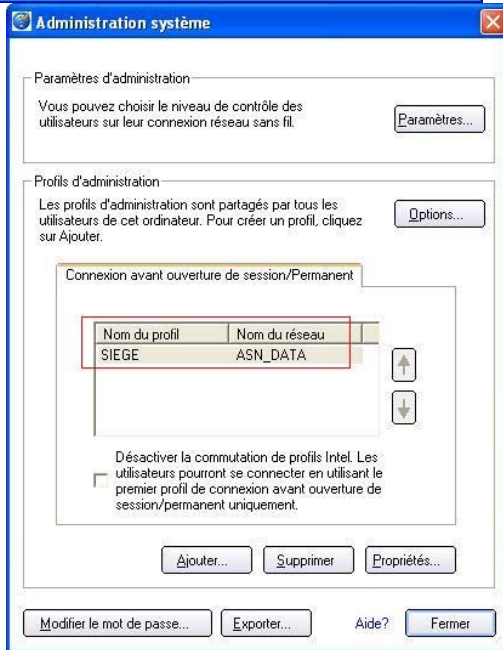
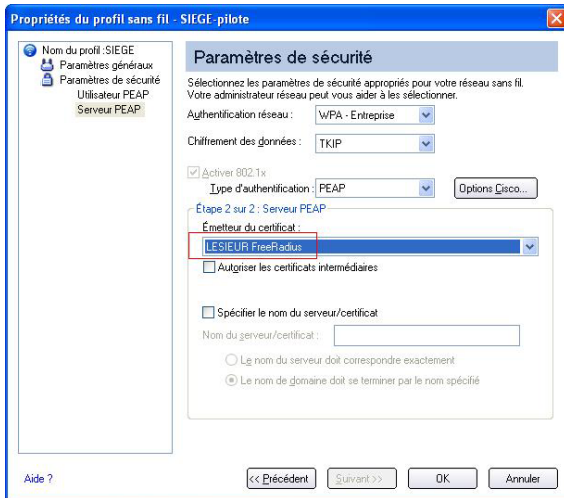
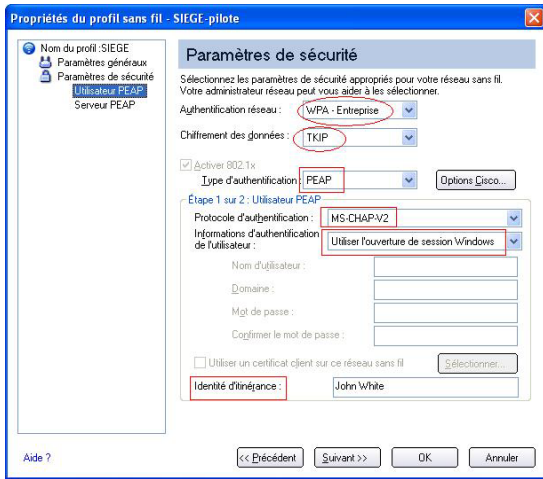


Connection profile “SIEGE” configuration

1. Go to Tools / System Administration, provide the password, and click the Add tab.



Fill in the last field (*Identité d'itinérance*) with user's last/first names, even if it's optional. This will help very much during debugging, if any. Do not use French accents!

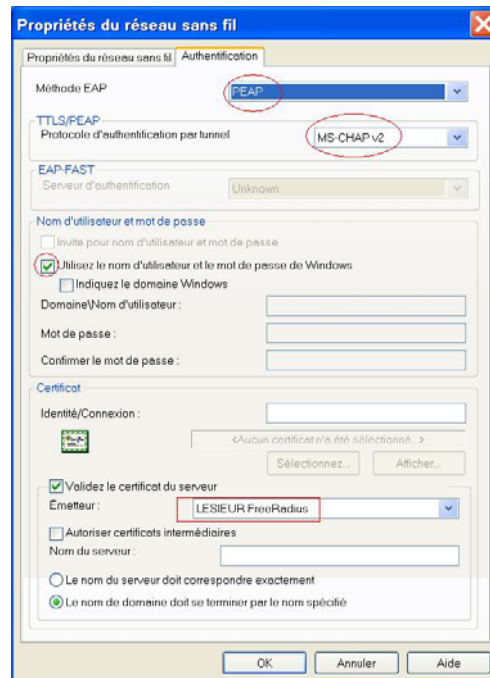
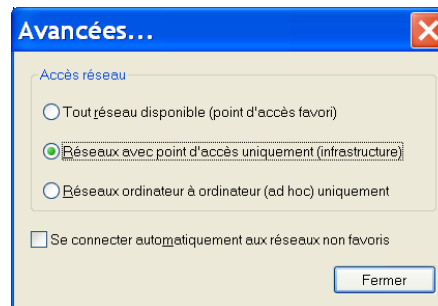


Dell Latitude D600 (TrueMobile 1300 MiniPCI)

For a driver update go to <http://support.euro.dell.com/support/downloads/> and find the *R94825.exe* file.

Configuring the WIFI ASN_DATA Connection

1. Launch the WiFi card tool. Click Advanced, then Properties.



How to check if you are connected ...

1. Move the mouse over the WiFi card icon. If you are connected, authentication state and IP address are displayed.

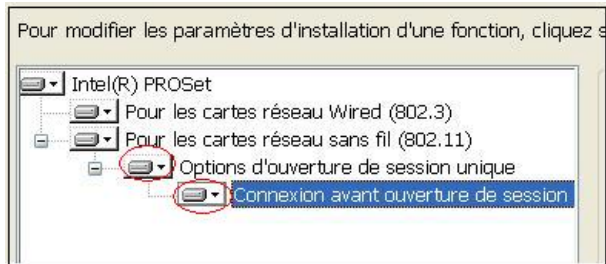


If the IP is 0.0.0.0, you are not connected.

Dell Latitude D600 (Intel PRO 2100 3A)

For a driver update go to <http://support.dell.com/support/downloads/> and look for the *R105328.exe* file.


During installation do not forget to select two options: Options for unique session opening - and Connection before session opening.



Configuring the WIFI ASN_DATA connection

Général Sécurité Avancé Mot de passe

Paramètres généraux

 Ngm du profil :

Nom du réseau (SSID) :

Mode opérationnel :

Infrastructure - Connexion à un point d'accès

Ad hoc - Connexion directe à d'autres ordinateurs

Paramètres de réseau avancés

Activer Cisco Compatible Extensions

Général Sécurité Avancé Mot de passe

Paramètres de sécurité

 Authentification réseau :

Chiffrement des données :

Paramètres de clé de chiffrement

Définir la clé manuelle

Index de clé :

Niveau de chiffrement :

Utiliser des caractères ASCII (5 caractères requis)

Utiliser les clés hexadécimales (10 chiffres hexadécimaux requis)

Clé :

Paramètres 802.1x

802.1x activé

Type d'authentification :

Paramètres PEAP

Identité d'itinérance

Identité du serveur

Émetteur du certificat :

Autoriser les certificats intermédiaires

Nom du serveur/certificat :

Le nom du serveur doit correspondre exactement.

Le nom de domaine doit se terminer par le nom spécifié

Authentification en tunnel

Protocole d'authentification :

Informations d'authentification de l'utilisateur

Demander les informations d'authentification à la connexion

Utiliser l'ouverture de session Windows

Enregistrer les informations d'authentification de l'utilisateur

Certificat client

Utiliser le certificat client

Général Sécurité Avancé Mot de passe

Extensions Cisco compatibles

Activer la prise en charge de la gestion radioélectrique

Point d'accès obligatoire

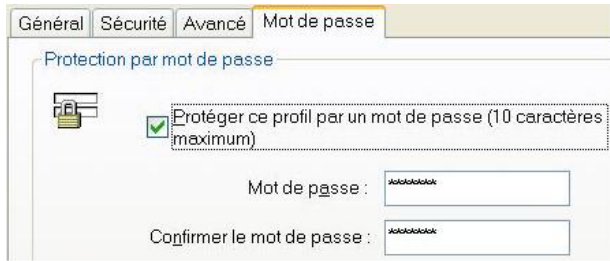
Utiliser l'adresse MAC du point d'accès obligatoire :

Importation automatique

Activer l'importation automatique

Gestion avancée des profils

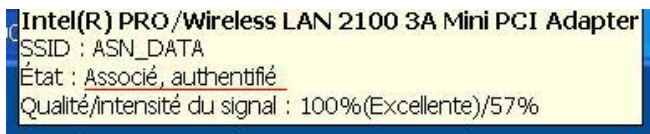
Ce profil peut être utilisé par tous les utilisateurs (Profil commun)



How to check if you are connected ...

Method 1

Move the mouse over the WiFi card icon. The SSID and connection state are displayed.

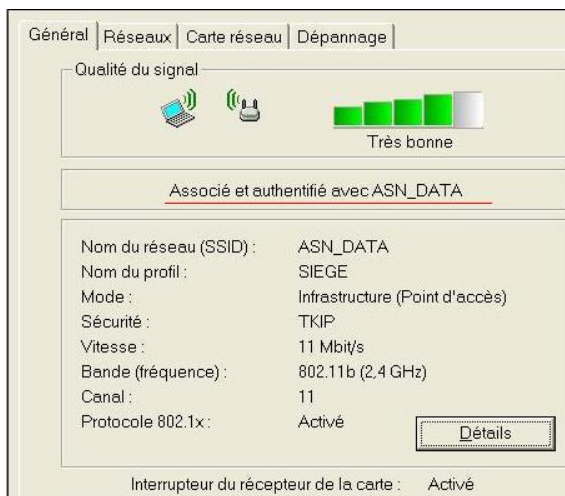


Method 2

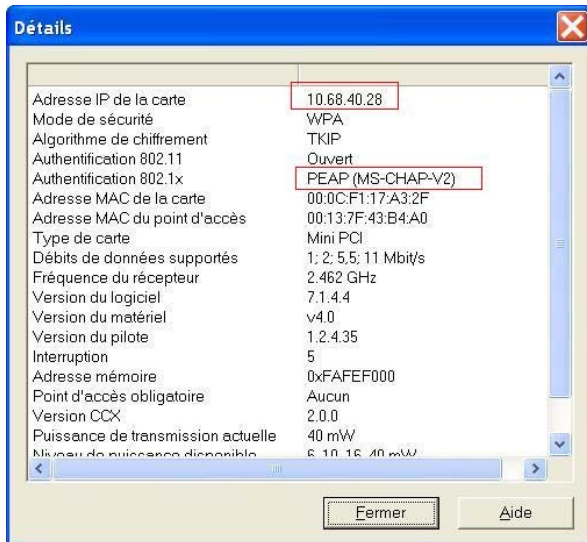
Double-click the WiFi card icon.



Click the General tab.



and then click Details:



How to check if a user connects without going to the laptop:

1. Open a session to the FreeRadius server (Putty or local).
2. Run this command:

```
grep -ir user-name /var/log/radius/radact/access-point-IP-address/reply-details-XXXXYYYY
```

where XXXXYZZ is the date of the file. You should see a list of user's names. Normally, these are successfully connected users! If no user connected, 'Reply' files are not created.

3. Now run this command:

```
grep -ir "login ok" /var/log/radius/radius.log
```

Each line with "Login OK" means a successful connection.

Known problems (laptops)

1. Symptom:

WiFi connection seems to be established, but no network application works.

Cause:

IP address of WiFi card is 0.0.0.0

Solution:

Go to WiFi connection properties (My Network Places) and check if the TCP/IP protocol is associated with the card.

2. Symptom:

Everything seems to be configured correctly, but the user still can't connect.

Cause:

Most probably there is something wrong with Universal/NDS Password.

Solution:

On the FreeRadius server, stop the RADIUS service (**rcradiusd stop**) and re-launch it in debug mode (**radiusd -X -A**)

Find the exact error. Then:

-- Make sure you followed step 16 of the FreeRadius Server Configuration section of this document, especially the last point (NDS password expiration). Normally, when you change NDS password, UP is

synchronized.

-- If not, change the NDS password once again from a workstation that has the Novell Client installed with the NMAS/NICI option, or from iManager/C1/NWAdmin32.

-- After that, normally, the WiFi connection should be established. It was for us. Don't forget to stop the debug mode of the RADIUS service (press Ctrl-C) and re-launch it normally (**rcradiusd start**).