Administration Guide

Integrating Novell eDirectory with FreeRADIUS 1.1

January 02, 2011

Novell

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. For more information on exporting Novell software, see the Novell International Trade Services Web page (http://www.novell.com/info/exports/). Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see Novell Documentation (http://www.novell.com/documentation/).

Novell Trademarks

For a list of Novell trademarks, see Trademarks (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This guide describes how to integrate Novell eDirectory with FreeRADIUS and configure eDirectory users for RADIUS authentication. This guide is intended for eDirectory or RADIUS administrators and is divided into the following sections:

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation to enter your comments.

Documentation Updates

For the most recent version of the *Integrating Novell eDirectory with FreeRADIUS Administration Guide*, see the Novell Documentation site (http://www.novell.com/documentation/edir_radius/index.html).

Additional Documentation

For documentation on getting started with the integration of eDirectory with FreeRADIUS, see the *Integrating Novell eDirectory with FreeRADIUS Quick Start Guide* on the Novell Documentation site (http://www.novell.com/documentation/edir_radius/index.html).

1 Overview

You can integrate Novell eDirectory 8.8 or later with FreeRADIUS on SUSE Linux Enterprise Server (SLES) 10 and SLES 11 to allow wireless authentication for eDirectory users.

If you are new to FreeRADIUS, refer to the FreeRADIUS Web site (http://www.freeradius.org) for more information.

For more information on eDirectory, refer to the *Novell eDirectory 8.8 Administration Guide* (http://www.novell.com/documentation/edir88/index.html).

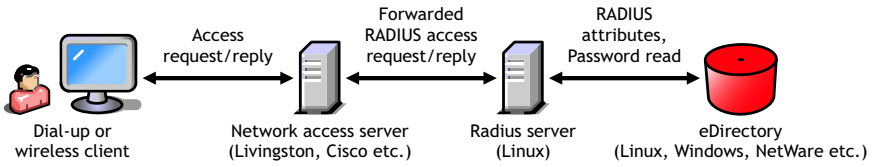
By integrating eDirectory with FreeRADIUS, you can do the following:

- Use Universal Password for RADIUS authentication

  Universal Password provides single login and authentication for eDirectory users. Users do not need a separate password for RADIUS and eDirectory authentication.
- Enforce eDirectory account policies for users

  The existing eDirectory policies on the user accounts can still be applied even after integrating with RADIUS. Also, you can make use of the intruder lockout facility of eDirectory by logging the failed logins into eDirectory.

Figure 1-1 *Wireless Authentication to eDirectory Integrated with FreeRADIUS*



FreeRADIUS and eDirectory can be on two different machines. For example, you can have an eDirectory LDAP server with NMAS running on NetWare, but run FreeRADIUS on Linux without eDirectory on it. Token-based authentication is not supported on NetWare.

eDirectory users can use any of the following protocols for RADIUS authentication:

- CHAP
- EAP-MSCHAP v1 and v2
- EAP-TLS
- LEAP
- MS-CHAP v1 and v2
- PEAP

For a complete list of protocols and information about them, refer to "FreeRADIUS Features" (http://www.freeradius.org/features.html) and to the IETF Web site (http://ietf.org/rfc).

IMPORTANT: We recommend that you use SHA-1 or SHA-2 algorithms and not MD5 authentication protocols for better security.

To integrate eDirectory with FreeRADIUS, you need to complete the following tasks:

- Install and configure FreeRADIUS server. For more information, see Chapter 2, "Installing FreeRADIUS," on page 9.
- Enable RADIUS authentication for eDirectory users by using the iManager plug-in for RADIUS to configure them. For more information, see Section 5.1.1, "Configuring iManager Plug-In for RADIUS," on page 27
- Install Novell Radius LDAP Extensions for token-based authentication. For more information, see Step 3 on page 36.

2 Installing FreeRADIUS

2.1 Supported Platforms

The eDirectory integration with FreeRADIUS is supported on the following Linux platforms:

- SUSE Linux Enterprise Server (SLES) 10
- SLES 11

2.2 Installing FreeRADIUS on SLES

1. Log in as the `root` user.
2. Install the FreeRADIUS package from the OS installation media.

   For example, on a SLES 10 computer, click *YaST* > *Software* > *Software Management* > *Package Search*.

   Enter `freeradius` in the search query and select the package for installation.

2.3 What's Next?

After installing FreeRADIUS, you need to configure the FreeRADIUS server and eDirectory users. For more information, refer to:

- Chapter 3, “Configuring the FreeRADIUS Server on SLES 10 to Integrate with eDirectory,” on page 11
- Chapter 4, “Configuring the FreeRADIUS Server on SLES 11 to Integrate with eDirectory,” on page 19
- Chapter 5, “Configuring eDirectory Users for RADIUS Authentication,” on page 27

3 Configuring the FreeRADIUS Server on SLES 10 to Integrate with eDirectory

This chapter helps you configure the FreeRADIUS server to integrate with Novell eDirectory and discusses the following information:

3.1 Prerequisites for Configuring the FreeRADIUS Server

Download and install the following:

- ❒ Install FreeRADIUS on SLES 10. For installation instructions, refer to Chapter 2, "Installing FreeRADIUS," on page 9.
- ❒ Install Novell eDirectory 8.8 or later: For installation instructions, refer to the *NetIQ eDirectory 8.8 Installation Guide* (https://www.netiq.com/documentation/edir88/).

  After installing eDirectory, you need to use iManager to configure it. Refer to Section 3.1.1, "Configuring eDirectory," on page 12 for more information.

  You also need to extract the self-signed certificate of the certificate authority (CA). For more information, refer to Section 3.1.2, "Extracting the Self-Signed Certificate of the Certificate Authority," on page 13.
- ❒ Install Novell iManager 2.7.*x* or later: For installation instructions, refer to the *iManager 2.7 Installation Guide* (https://www.netiq.com/documentation/imanager/).
- ❒ Install the Radius iManager plug-in. You can download the plug-in from the Novell Download site (http://download.novell.com/SummaryFree.jsp?buildid=QL_myGHU0V4~).

Security considerations:

- ❒ Ensure that you meet the security considerations discussed in Chapter 8, "Security Considerations," on page 39.

The following prerequisite tasks explain how to configure eDirectory so that you can log in to the system as a system administrator.

3.1.1 Configuring eDirectory

You need to use iManager to perform the following configuration tasks for eDirectory:

- "Enabling Universal Password for eDirectory Users" on page 12
- "Creating the RADIUS Administrator Object" on page 12
- "Granting Administration Rights for the RADIUS Administrator" on page 12
- "Granting Rights to RADIUS Administrator to Retrieve the Password" on page 12

Enabling Universal Password for eDirectory Users

Ensure that you enable Universal Password for the users in eDirectory. After enabling it, you need to set the Universal Password either manually or by logging in.

For more information, refer to *Deploying Universal Password* in the *Password Management 3.3.x Guide* (https://www.netiq.com/documentation/edir88/pwm_administration88/data/bookinfo.html).

Creating the RADIUS Administrator Object

For information on creating a RADIUS Administrator object in eDirectory, refer to "Managing User Accounts" in the *NetIQ eDirectory Administration Guide* (https://www.netiq.com/documentation/edir88/).

You need to provide the DN of the RADIUS Administrator object while modifying the attributes in the LDAP module.

Granting Administration Rights for the RADIUS Administrator

Grant the RADIUS administrator the write right for the ACL attribute of the user object whose Universal Password needs to be read. This gives the RADIUS administrator administrative rights to that user object.

The eDirectory administrator can also be the RADIUS administrator. For more information on eDirectory rights, refer to the *NetIQ eDirectory Administration Guide* (https://www.netiq.com/documentation/edir88/).

Granting Rights to RADIUS Administrator to Retrieve the Password

By default, the administrator does not have the right to read the Universal Password. The eDirectory administrator needs to modify the password policy to enable the RADIUS Administrator to read the Universal Password.

Use the following procedure to grant rights to the RADIUS administrator in order to retrieve the Universal Password:

1. In iManager, click the *Roles and Tasks* button . 
2. Click *Passwords* > *Password Policies* and select the password policy being used.
3. Click *Universal Password* > *Configuration Options*.
4. Select *Allow admin to retrieve passwords* from the Universal Password Retrieval section.
5. Click *Apply*, then click *OK*.

3.1.2 Extracting the Self-Signed Certificate of the Certificate Authority

Extract the self-signed certificate of the certificate authority in Base 64 format. For information on extracting the certificate, refer to the *NetIQ Certificate Server Administration Guide* (https://www.netiq.com/documentation/edir88/crtadmin88/data/bookinfo.html).

You need to provide the extracted path and the certificate filename while modifying the attributes in the `LDAP module` of the `radiusd.conf` configuration file.

Parameter	Description
tls_cacertfile	Specifies the full path of a certificate file in the UNIX file system.

NOTE: The RADIUS server administrator must ensure that the (UNIX) user with RADIUS server rights also has rights to read the certificate files

3.2 Modifying the LDAP Module

You need to modify the following attributes in the ldap module in the `/etc/raddb/radiusd.conf` file:

Attributes	Value	Remarks
server	hostname or IP address	You can use either the hostname or the IP address of the LDAP server based on the SSL Certificate DNS or SSL CertificateIP. Ensure that the server name you use here matches the server name in the DN attribute of the eDirectory LDAP server certificate. By default, the eDirecttory LDAP server uses SSL CertificateDNS.
port	636	LDAP server port
identity	DN of the RADIUS administrator in eDirectory	DN of the RADIUS administrator under which LDAP searches are performed.
password	password of the RADIUS administrator in eDirectory	The pasword authenticates the DN of the RADIUS administrator.
basedn	The DN of the container that stores the RADIUS users and profile objects	The RADIUS server looks for objects in the subtree under this basedn. If you want multiple search bases, you can create multiple LDAP modules. For an example, refer to Section 3.2.2, “Example for Creating Multiple Instances of an LDAP Module,” on page 16.
filter	(cn=%{Stripped-User-Name:-%{User-Name}})	You can use the LDAP search filter to locate the user object by using name supplied by the RADIUS client during authentication.
start_tls	no	If the value is set to `yes`, it creates a secure connection on port 389. **IMPORTANT:** Ensure that the tls_mode attribute is either commented or that tls_mode is set to `no` and the port is set to 389.

Attributes	Value	Remarks
tls_mode	yes	Creates a secure connection on port 636. **IMPORTANT:** Enure that the start_tls attribute is either commented or that start_tls is set to `no` and the port is set to 636.
tls_cacertfile	Path of the certificate file in the UNIX file system	A PEM or Base 64 encoded file that contains the CA certificates.
tls_require_cert	demand	By setting the value of this attribute to `demand`, you configure FreeRADIUS to verify the certificate. The authentication fails if a certificate does not verify.
dictionary_mapping	${raddbdir}/ldap.attrmap	You can use this attribute to map the RADIUS dictionary attributes with LDAP directory attributes.
password_attribute	nspmPassword	By setting the value of this attribute to nspmPassword, you configure FreeRADIUS to enable users to use their Universal Passwords for RADIUS authentication. The nspmPassword string is not case sensitive. For example, you can use either nspmPassword or nspmpassword. **IMPORTANT:** Ensure that you have enabled Universal Password for eDirectory. For more information, refer to Section 3.1, “Prerequisites for Configuring the FreeRADIUS Server,” on page 11.
edir_account_policy_check	yes	An eDirectory account policy check is enabled by default. By setting the value of this attribute to `no`, you disable the eDirectory account policy check and intruder detection in eDirectory. **NOTE:** If a user has grace logins, they are used up when the user authenticates through RADIUS. This might lock the user's account without warning. The advantages of an eDirectory account policy check are: ◆ The existing eDirectory policies on the user accounts can still be applied after integrating with RADIUS. ◆ eDirectory intruder detection is enabled. **IMPORTANT:** If you find the performance of the RADIUS servers unsatisfactory, you can disable the eDirectory account policy check, but there are security risks.
access_attr	dialupAccess	By setting the value of this attribute to dialupAccess, you configure FreeRADIUS to allow or deny access to an user. This attribute should be present and set to either `true` or `false` for each user. If you do not want to use this attribute to control access to the user, you need to comment out access_attr = dialupAccess. For the steps to specify this attribute for the user, see “Modifying RADIUS Users” on page 30.

For more detailed explanation of the attributes, refer to the `/usr/share/doc/packages/freeradius/rlm_ldap` file.

After modifying the LDAP module, you need to enable the module and specify `ldap` in the `post-authenticiation` section of the `radiusd.conf` file. For more information, refer to Section 3.3, "Enabling the LDAP Module in the Configuration File," on page 16.

3.2.1 Example of a Modified LDAP Module

```
ldap
{
    server = "eDir.test.com"
    port = 636
    identity = "cn=admin,o=org"
    password = secret
    basedn = "o=org"
    filter = "(cn=%{Stripped-User-Name:-%{User-Name}})"
    base_filter = "(objectclass=radiusprofile)"
    # set this to 'yes' to use TLS encrypted connections
    # to the LDAP database by using the StartTLS extended
    # operation.
    # The StartTLS operation is supposed to be used with normal
    # ldap connections instead of using ldaps (port 636) connections
    start_tls = no
    tls_mode = yes
    tls_cacertfile  = /etc/raddb/certs/cacert.b64
    # tls_cacertdir    = /path/to/ca/dir/
    # tls_certfile    = /path/to/radius.crt
    # tls_keyfile    = /path/to/radius.key
    # tls_randfile    = /path/to/rnd
    tls_require_cert  = "demand"
    # default_profile = "cn=radprofile,ou=dialup,o=My Org,c=UA"
    # profile_attribute = "radiusProfileDn"
    access_attr = "dialupAccess"
    # Mapping of RADIUS dictionary attributes to LDAP
    # directory attributes.
    dictionary_mapping = ${raddbdir}/ldap.attrmap
    ldap_connections_number = 5
    #
    # NOTICE: The password_header directive is NOT case insensitive
    #
    # password_header = "{clear}"
    #
    #  The server can usually figure this out on its own, and pull
    #  the correct User-Password or NT-Password from the database.
    #
    #  Note that NT-Passwords MUST be stored as a 32-digit hex
    #  string, and MUST start off with "0x", such as:
    #
    #  0x000102030405060708090a0b0c0d0e0f
    #
    #  Without the leading "0x", NT-Passwords will not work.
    #  This goes for NT-Passwords stored in SQL, too.
    #
    password_attribute = nspmPassword
    # groupname_attribute = cn
    # groupmembership_filter = "(|(&(objectClass=GroupOfNames)(member=%{Ldap-
UserDn}))(&(objectClass=GroupOfUniqueNames)(uniquemember=%{Ldap-UserDn})))"
    # groupmembership_attribute = radiusGroupName
    timeout = 4
    timelimit = 3
    net_timeout = 1
    # compare_check_items = yes
    # do_xlat = yes
    # access_attr_used_for_allow = yes
    edir_account_policy_check = yes
    }
```

3.2.2 Example for Creating Multiple Instances of an LDAP Module

If you want multiple search bases, you can create multiple LDAP modules by using the following syntax in the `module` section of the `radiusd.conf` file.

```
modules
{
        ...........
        ...........

        ldap ldap1
        {
         attribute = value
         attribute = value
         ..............
         ..............
        }

        ldap ldap2
        {
         attribute = value
         attribute = value
         ..............
         ..............
        }
        ldap ldap3
        {
         attribute = value
         attribute = value
         ..............
         ..............
        }
}
```

You can use the configured modules in the `authorize`, `authenticate`, and `post-authenticate` sections by specifying the module name and instance name. For example:

```
authorize
{
        .....
        .....
        ldap ldap1
        ldap ldap2
        .....
        .....
}
```

3.3 Enabling the LDAP Module in the Configuration File

3.3.1 Authorize Section

To enable the `ldap` module, uncomment it in the `authorize` section of the `/etc/raddb/radiusd.conf` file. To disable it, comment it. In addition, if all RADIUS users are not present in the local system (`/etc/passwd` file), comment the `files` module as follows:

```
authorize
     {
          ...
         # files
          ...
         #
         # The ldap module will set Auth-Type to LDAP if it has not
         # already been set.
         ldap
         ...
    }
```

For information on setting up LDAP with FreeRADIUS, refer to the `/usr/share/doc/packages/freeradius/ldap_howto.txt` and `/usr/share/doc/packages/freeradius/rlm_ldap` files.

3.3.2 Authentication Section

Uncomment the following under `authenticate` section of the `/etc/raddb/radius.conf` file.

```
Auth-Type LDAP
         {
            ldap
          }
```

3.3.3 Post-Authentication Section

You need to add `ldap` in the `post-authentication` section of the `/etc/raddb/radiusd.conf` file as shown below:

```
post-auth
    {
         #  Get an address from the IP Pool.
         ldap
         #       main_pool
         #
         #  If you want to have a log of authentication replies,
         #  un-comment the following line, and the 'detail reply_log'
         #  section, above.
         #       reply_log
         #
         #  After authenticating the user, do another SQL qeury.
         #
         #  See "Authentication Logging Queries" in sql.conf
         #  sql
         #
         #  Access-Reject packets are sent through the REJECT sub-section
         #  of the post-auth section.
         #
       Post-Auth-Type REJECT
           {
              ldap
            }
     }
```

4 Configuring the FreeRADIUS Server on SLES 11 to Integrate with eDirectory

This section helps you configure the FreeRADIUS server to integrate with Novell eDirectory:

4.1 Prerequisites for Configuring the FreeRADIUS Server

Download and install the following:

- ❒ Install FreeRADIUS on SLES 11. For installation instructions, refer to Chapter 2, “Installing FreeRADIUS,” on page 9.
- ❒ Install Novell eDirectory 8.8 or later: For installation instructions, refer to the *NetIQ eDirectory 8.8 Installation Guide* (https://www.netiq.com/documentation/edir88/).

  After installing eDirectory, you need to use iManager to configure it. Refer to Section 4.1.1, “Configuring eDirectory,” on page 20 for more information.

  You also need to extract the self-signed certificate of the certificate authority (CA). For more information, refer to Section 4.1.2, “Extracting the Self-Signed Certificate of the Certificate Authority,” on page 21.
- ❒ Install Novell iManager 2.7.*x* or later: For installation instructions, refer to the *iManager 2.7 Installation Guide* (https://www.netiq.com/documentation/imanager/).
- ❒ Install the Radius iManager plug-in. You can download the plug-in from the Novell Download site (http://download.novell.com/SummaryFree.jsp?buildid=QL_myGHU0V4~).

Security considerations:

- ❒ Ensure that you meet the security considerations as discussed in Chapter 8, “Security Considerations,” on page 39.

The following prerequisite tasks explain how to configure eDirectory so that you can log in to the system as a system administrator.

4.1.1 Configuring eDirectory

You need to use iManager to perform the following configuration tasks for eDirectory:

- "Enabling Universal Password for eDirectory Users" on page 20
- "Creating the RADIUS Administrator Object" on page 20
- "Granting Administration Rights for the RADIUS Administrator" on page 20
- "Granting Rights to RADIUS Administrator to Retrieve Password" on page 20

Enabling Universal Password for eDirectory Users

Ensure that you enable Universal Password for the users in eDirectory. After enabling, you need to set the Universal Password either manually or by logging in.

For more information, refer to *Deploying Universal Password* in the *Password Management 3.3.x Guide* (https://www.netiq.com/documentation/edir88/pwm_administration88/data/bookinfo.html).

Creating the RADIUS Administrator Object

An Administrator object is a User object.

For information on creating a RADIUS Administrator object in eDirectory, refer to the Managing User Accounts section in the *NetIQ eDirectory Administration Guide* (https://www.netiq.com/documentation/edir88/).

You need to provide the DN of the RADIUS Administrator object while modifying the attributes in the LDAP module.

Granting Administration Rights for the RADIUS Administrator

Grant the RADIUS administrator the write right for the ACL attribute of the user object whose Universal Password needs to be read. This gives the RADIUS administrator administrative rights to that user object.

The eDirectory administrator can also be the RADIUS administrator. For more information on eDirectory rights, refer to the *NetIQ eDirectory Administration Guide* (https://www.netiq.com/documentation/edir88/).

Granting Rights to RADIUS Administrator to Retrieve Password

By default, the administrator does not have the right to read the Universal Password. The eDirectory administrator needs to modify the password policy to enable the RADIUS Administrator to read The Universal Password.

Use the following procedure to grant rights to the RADIUS administrator in order to retrieve the Universal Password:

1. In iManager, click the *Roles and Tasks* button  .
2. Click *Passwords* > *Password Policies* and select the password policy being used.
3. Click *Universal Password* > *Configuration Options*.
4. Select *Allow admin to retrieve passwords* from the `Universal Password Retrieval` section.
5. Click *Apply*, then click *OK*.

4.1.2 Extracting the Self-Signed Certificate of the Certificate Authority

Extract the self-signed certificate of the certificate authority in Base 64 format. For information on extracting the certificate, refer to the *NetIQ Certificate Server Administration Guide* (https://www.netiq.com/documentation/edir88/crtadmin88/data/bookinfo.html).

You need to provide the extracted path and the certificate filename while modifying the attributes in the LDAP module of the `radiusd.conf` configuration file.

Parameter	Description
cacertfile	Specifies the full path of a certificate file in the UNIX file system.

NOTE: The RADIUS server administrator must ensure that the (UNIX) user with RADIUS server rights also has rights to read the certificate files.

4.2 Modifying the LDAP Module

You need to modify the following attributes in the ldap module in the `/etc/raddb/modules/ldap` file:

Attributes	Value	Remarks
server	hostname or IP address	You can use either the hostname or the hostname or IP address of the LDAP server based on the SSL CertificateDNS or SSL CertificateIP. Ensure that the server name you use here matches with the server name in the DN attribute of the eDirectory LDAP server certificate. By default, the eDirecttory LDAP server uses SSL Certificate DNS.
identity	DN of the RADIUS administrator in eDirectory	DN of the RADIUS administrator under which LDAP searches are performed.
password	*password of the RADIUS administrator in eDirectory*	The pasword authenticates the DN of the RADIUS administrator.
basedn	The DN of the container that stores the RADIUS users and profile objects	The RADIUS server looks for objects in the subtree under this basedn. If you want multiple search bases, you can create multiple LDAP modules. For an example, refer to Section 3.2.2, “Example for Creating Multiple Instances of an LDAP Module,” on page 16.
filter	(cn=%{Stripped-User-Name:-%{User-Name}})	You can use the LDAP search filter to locate the user object by using name supplied by the RADIUS client during authentication.
start_tls	no	If the value is set to `yes`, it creates a secure connection on port 389. **IMPORTANT:** Ensure that the tls_mode attribute is either commented or the tls_mode is set to `no` and the port is set to 389.

Attributes	Value	Remarks
cacertfile	Full path of the certificate file in the UNIX file system.	A PEM or Base 64 encoded file that contains the CA certificates.
require_cert	demand	By setting the value of this attribute to `demand`, you configure FreeRADIUS to verify the certificate. The authentication fails if a certificate does not verify.
dictionary_mapping	${raddbdir}/ldap.attrmap	You can use this attribute to map the RADIUS dictionary attributes with LDAP directory attributes.
password_attribute	nspmPassword	By setting the value of this attribute to nspmPassword, you configure FreeRADIUS to enable users to use their Universal Passwords for RADIUS authentication. The nspmPassword string is not case sensitive. For example, you can use either nspmPassword or nspmpassword. **IMPORTANT:** Ensure that you have enabled Universal Password for eDirectory. For more information, refer to Section 4.1, “Prerequisites for Configuring the FreeRADIUS Server,” on page 19.
edir_account_policy_check	yes	An eDirectory account policy check is enabled by default. By setting the value of this attribute to `no`, you disable the eDirectory account policy check and intruder detection in eDirectory. **NOTE:** If a user has grace logins, they are used up when the user authenticates through RADIUS. This might lock the user's account without warning. The advantages of an eDirectory account policy check are: ◆ The existing eDirectory policies on the user accounts can still be applied after integrating with RADIUS. ◆ eDirectory intruder detection is enabled. **IMPORTANT:** If you find the performance of the RADIUS servers unsatisfactory, you can disable the eDirectory account policy check, but there are security risks.
access_attr	dialupAccess	By setting the value of this attribute to dialupAccess, you configure FreeRADIUS to allow or deny access to an user. This attribute should be present and set to either `true` or `false` for each user. If you do not want to use this attribute to control access to the user, you need to comment out access_attr = dialupAccess. For steps to specify this attribute to the user, see “Modifying RADIUS Users” on page 30.

For more detailed explanation of the above attributes, refer to the `/usr/share/doc/packages/freeradius-server-doc/rlm_ldap` file.

After modifying the LDAP module, you need to enable the module and specify `ldap` in the `post-authentication` section of the `/etc/raddb/sites-available/default` file. For more information, refer to Section 4.3, "Enabling the LDAP Module in the Configuration File," on page 24.

4.2.1 Example of a Modified LDAP Module

```
 ldap
      {
         server = "eDir.test.com"
         identity = "cn=admin,o=org"
         password = secret
         basedn = "o=org"
         filter = "(cn=%{Stripped-User-Name:-%{User-Name}})"
         #base_filter = "(objectclass=radiusprofile)"
         ldap_connections_number = 5
         timeout = 4
         timelimit = 3
         net_timeout = 1
         tls
         {
         # Set this to 'yes' to use TLS encrypted connections
         # to the LDAP database by using the StartTLS extended operation.
          # The StartTLS operation is supposed to be used with normal ldap
         # connections instead of using ldaps connections
         start_tls = yes
         cacertfile = /path/to/cacert.pem
         # cacertdir = /path/to/ca/dir/
         # certfile = /path/to/radius.crt
         # keyfile  = /path/to/radius.key
         # randfile = /path/to/rnd
         require_cert = "demand"
        }
        # default_profile = "cn=radprofile,ou=dialup,o=My Org,c=UA"
        # profile_attribute = "radiusProfileDn"
        #access_attr = "dialupAccess"
        dictionary_mapping = ${confdir}/ldap.attrmap
        # password_attribute = userPassword
        edir_account_policy_check = no
        #  Group membership checking.  Disabled by default.
        # groupname_attribute = cn
        # groupmembership_filter =
"(|(&(objectClass=GroupOfNames)(member=%{LdapUserDn}))(&(objectClass=GroupOfUnique
Names)(uniquemember=%{Ldap-UserDn})))"
        # groupmembership_attribute = radiusGroupName
        # compare_check_items = yes
        # do_xlat = yes
        # access_attr_used_for_allow = yes
    }
```

4.2.2 Example for Creating Multiple Instances of an LDAP Module

If you want multiple search bases, you can create multiple LDAP modules by using the following syntax in the module section of the `etc/raddb/modules/ldap.conf` file.

```
modules
      {
       ...........
       ...........

       ldap ldap1
       {
        attribute = value
        attribute = value
        ..............
        ..............
       }
       ldap ldap2
       {
        attribute = value
        attribute = value
        ..............
        ..............
       }
       ldap ldap3
       {
        attribute = value
        attribute = value
        ..............
        ..............
       }
   }
```

You can use the configured modules in the authorize, authenticate, and post-authenticate sections by specifying the module name and instance name. For example:

```
authorize
    {
       .....
       .....
       ldap ldap1
       ldap ldap2
       .....
       .....
   }
```

4.3 Enabling the LDAP Module in the Configuration File

4.3.1 Authorize Section

To enable the `ldap` module, uncomment it in the `authorize` section of the `/etc/raddb/sitesavailable/default` file. To disable it, comment it.

```
authorize
    {
          ...
          ...
        #
        # The ldap module will set Auth-Type to LDAP if it has not
        # already been set.
        ldap
        ...
    }
```

For information on setting up LDAP with FreeRADIUS, refer to the `/usr/share/doc/packages/freeradius/ldap_howto.txt` and `/usr/share/doc/packages/freeradius/rlm_ldap` files.

4.3.2 Authentication Section

Uncomment the following under `authenticate` section of the `/etc/raddb/sites-available/default` file.

```
Auth-Type LDAP
  {
    ldap
  }
```

4.3.3 Post-Authentication Section

You need to add `ldap` in the `post-authenticate` section of the `/etc/raddb/sites-available/default` file as shown below:

```
post-auth
   {

    ldap
        Post-Auth-Type REJECT
            {
              ldap
            }
   }
```

5 Configuring eDirectory Users for RADIUS Authentication

Through the iManager plug-in for RADIUS, you can configure Novell eDirectory users to authenticate through FreeRADIUS. You can convert the existing eDirectory users to RADIUS users by adding the RADIUS attributes. If you want to add new FreeRADIUS users, you need to first add a corresponding eDirectory user and then add RADIUS attributes to the user objects.

5.1 Prerequisites to Configure eDirectory Users for RADIUS Authentication

- ❒ Download and install the Novell iManager plug-in for RADIUS from the Novell Download site (http://download.novell.com/SummaryFree.jsp?buildid=QL_myGHU0V4~).

  Ensure that you configure the iManager plug-in with an SSL/TLS connection to eDirectory for RADIUS to work with iManager plug-in. For more information, refer to the "Secure LDAP Certificates" in the *iManager 2.7.x Administration Guide* (http://www.novell.com/documentation/imanager27/imanager_admin_273/data/bx8g5g8.html).

- ❒ Extend the eDirectory schema to add the FreeRADIUS schema. For more information, refer to Section 5.1.2, "Extending the eDirectory Schema for RADIUS," on page 28.

5.1.1 Configuring iManager Plug-In for RADIUS

You need to configure the iManager plug-in with an SSL/TLS connection to eDirectory for RADIUS to work with the iManager plug-in. You can have the RADIUS iManager plug-in and iManager on same machine or on two different machines.

- If you configure RADIUS iManager plug-in and iManager on same machine, then iManager is configured for SSL/TLS connection to eDirectory by default.
- If you want to configure the RADIUS iManager plug-in and iManager on different machines, you need to manually configure the iManager for SSL/TLS connection to eDirectory. For more information, refer to the *iManager 2.7 Administration Guide* (http://www.novell.com/documentation/imanager27/imanager_admin_274/?page=/documentation/imanager27/imanager_admin_274/data/bx8g5g8.html).

5.1.2 Extending the eDirectory Schema for RADIUS

There are three possible scenarios for extending the eDirectory schema for RADIUS.

- "Extending the Schema if a Mapping Already Exists between RADIUS:Profile and rADIUSProfile" on page 28
- "Extending the Schema if a Mapping Does Not Exist between RADIUS:Profile and rADIUSProfile" on page 28
- "Extending the Schema if a Mapping Already Exists between RADIUS:Profile and Another Attribute" on page 29

Extending the Schema if a Mapping Already Exists between RADIUS:Profile and rADIUSProfile

1. In iManager, click the *Roles and Tasks* button  .
2. Click *LDAP* > *LDAP Options*.
3. Select *View LDAP Groups* and click the group corresponding to the LDAP server you want to use.
4. Select *Class Map*.
5. Select the *RADIUS:Profile* to *rADIUSProfile mapping*.
6. Click *Edit*.
7. Change the primary LDAP class name to anything other than rADIUSProfile, such as novellradiusprofile.
8. Click *Apply*.
9. Refresh the LDAP server.
10. Click *RADIUS* > *Extend schema for RADIUS*.
11. Click *OK*.

Extending the Schema if a Mapping Does Not Exist between RADIUS:Profile and rADIUSProfile

1. In iManager, click the *Roles and Tasks* button  .
2. Click *LDAP* > *LDAP Options*:
3. Select *View LDAP Groups* and click the group corresponding to the LDAP server you want to use.
4. Select *Class Map*.
5. Click *Add mapping* button.
6. In the eDirectory class drop-down list, select *RADIUS:Profile*.
7. Change the primary LDAP class name to anything other than rADIUSProfile, such as novellradiusprofile.
8. Click *OK*.
9. Refresh the LDAP server.
10. Click *RADIUS* > *Extend schema for RADIUS*.
11. Click *OK*.

Extending the Schema if a Mapping Already Exists between RADIUS:Profile and Another Attribute

To extend the schema if a mapping already exists between RADIUS:Profile and any name other than rADIUSProfile:

1. In iManager, click the *Roles and Tasks* button  .
2. Click *RADIUS* > *Extend schema for RADIUS*.
3. Click *OK*.

5.2 Adding RADIUS Attributes to eDirectory Users

You can add the RADIUS attributes to the following:

- Section 5.2.1, "Users," on page 29
- Section 5.2.2, "Profile Objects," on page 29

You can also add the RADIUS attributes when you are modifying users or the eDirectory objects.

5.2.1 Users

1. Create RADIUS users through Radius iManager plug-in.

   For more information, see "Creating RADIUS Users" on page 30.
2. Launch iManager, select *Directory Administration* > *Modify Object*, then select RADIUS users for which you want to add attributes.
3. Click *General* > *Other*.
4. Select the attributes for the RADIUS users.
5. Specify a value for each selected attribute, then click *OK*.

5.2.2 Profile Objects

You can create Profile objects in eDirectory to store a set of RADIUS attributes. Profile objects help in associating a User object collectively with the RADIUS attributes. For example, assume that you want to assign a set of RADIUS attributes, such as Auth-Type, NAS-IP-Address, and Framed-IPX-Network to users Jack, Tom, and Jane. You can create a Profile object called PR1 containing these RADIUS attributes and then assign PR1 to all three users. For more information, see Section 5.3.2, "Managing RADIUS Profiles," on page 30.

5.3 Managing RADIUS Objects

You can manage RADIUS objects by using the iManager plug-in for RADIUS. Ensure that you meet all the Prerequisites to Configure eDirectory Users for RADIUS Authentication before proceeding.

- Section 5.3.1, "Managing RADIUS Users," on page 30
- Section 5.3.2, "Managing RADIUS Profiles," on page 30

5.3.1 Managing RADIUS Users

You can create, modify, and delete RADIUS users.

- "Creating RADIUS Users" on page 30
- "Modifying RADIUS Users" on page 30
- "Deleting RADIUS Users" on page 30

Creating RADIUS Users

1. In iManager, click the *Roles and Tasks* button  .
2. Click *RADIUS* > *Create RADIUS User*.
3. Specify the User object you want to create either by typing the object name or by using the object selector.
4. (Optional) Specify the Profile object you want to associate with the user by typing its name or by using the object selector.
5. Click *OK*.

Modifying RADIUS Users

1. In iManager, click the *Roles and Tasks* button  .
2. Click *RADIUS* > *Modify RADIUS User*.
3. Specify the User object you want to modify either by typing the object name or by using the object selector.
4. (Optional) Specify or modify the RADIUS attributes for the User object.
5. Click *OK*.

Deleting RADIUS Users

1. In iManager, click the *Roles and Tasks* button  .
2. Click *RADIUS* > *Delete RADIUS User*.
3. Specify the User object you want to delete either by typing the object name or by using the object selector.
4. Click *OK*.

5.3.2 Managing RADIUS Profiles

You can create, modify, and delete RADIUS profiles.

- "Creating RADIUS Profiles" on page 31
- "Modifying RADIUS Profiles" on page 31
- "Deleting RADIUS Profiles" on page 31

Creating RADIUS Profiles

1. In iManager, click the *Roles and Tasks* button  .
2. Click *RADIUS* > *Create RADIUS Profile*.
3. Specify the context for the Profile object you want to create either by typing the object name or by using the object selector.
4. Click *OK*.

Modifying RADIUS Profiles

1. In iManager, click the *Roles and Tasks* button  .
2. Click *RADIUS* > *Modify RADIUS Profile*.
3. Specify the RADIUS Profile object you want to modify either by typing the object name or by using the object selector.
4. (Optional) Specify or modify the RADIUS attributes for the Profile object.
5. Click *OK*.

Deleting RADIUS Profiles

1. In iManager, click the *Roles and Tasks* button  .
2. Click *RADIUS* > *Delete RADIUS Profile*.
3. Specify the RADIUS Profile object you want to delete either by typing the object name or by using the object selector.
4. Click *OK*.

6 Novell Technical Support for eDirectory Integrated FreeRADIUS

You can report bugs and request assistancethrough Bugzilla. Novell Technical Support (NTS) can assist customers only if the customers use the RPMs shipped with SUSE Linux Enterprise Server (SLES) 10 and above.

Before you report a FreeRadius bug, check (https://bugs.freeradius.org/bugzilla/index.cgi) to find out if the bug you intend to file has already been filed by someone else.

To file a new bug:

1. Create a new account at the FreeRADIUS Web site (https://bugs.freeradius.org/bugzilla/createaccount.cgi).

   A password is sent to you from this site.
2. Log in with the password.
3. Click *New* to file new bugs after a successful login.

   You need to give information such as version, component, OS, and severity. The maintainer or the component owner is notified after you save your changes.

For information on writing bugs, refer to the bug writing guidelines (http://www.freedos.org/bugs/bugzilla/bugwritinghelp.html).

7 Configuring a FreeRADIUS Server for Token Authentication

This section describes how to configure a RADIUS server for token authentication:

7.1 Prerequisites for Token Authentication

Install or configure the following:

- ❒ Install FreeRADIUS 1.1.7 or later. On SUSE Linux Enterprise Server (SLES) 10 or later, install `freeradius-1.1.0-19.9.x.rpm`. On SLES 11 or later, install `freeradius-server-2.1.1-7.10.13.rpm`.

  For installation instructions, refer to Chapter 2, “Installing FreeRADIUS,” on page 9.
- ❒ Install Novell eDirectory 8.8 SP2 or later on Linux.
- ❒ Configure the RADIUS server to integrate with eDirectory, depending on your platform. For instructions, refer to “Configuring the FreeRADIUS Server on SLES 10 to Integrate with eDirectory” on page 11 or Chapter 4, “Configuring the FreeRADIUS Server on SLES 11 to Integrate with eDirectory,” on page 19.
- ❒ Install token authentication method in eDirectory.

  For installation instructions, refer to the vendor documentation (http://www.vasco.com/solutions/partners/novell.aspx).

1. Select *Vasco Method for NMAS* to download `VASCO_NMAS_Method_3.4_iMan27.zip` or later.
2. Extract the zip and follow the instructions documented in the `VASCO NMAS Method Release Notes.pdf` file.

7.2 Configuring Token Authentication for FreeRADIUS on SLES

Ensure that you meet all the requirements mentioned in Section 7.1, “Prerequisites for Token Authentication,” on page 35 before proceeding.

1. Uncomment the following lines in the `authenticate` section:

```
authenticate {
                ...
                ...
                Auth-Type LDAP {

                                  ldap
                               }
                ...
```

The above configuration section is present in the following configuration files:

- **SLES 10**: /etc/raddb/radiusd.conf file
- **SLES 11**: /etc/raddb/sites-available/default

2 Comment or delete the line "password_attribute = nspmPassword" in the ldap section.

```
ldap {
          ...
         password_atribute = nspmPassword
         ...
                  }
      ...
```

The above configuration section is present in the following configuration files:

- **SLES 10**: /etc/raddb/radiusd.conf
- **SLES 11**: /etc/raddb/modules/ldap

3 Install the RADIUS LDAP Extension RPM:

3a Download the `novell-radius-ldap-extension-1.1.0-3.zip` file from the eDirectory integration with FreeRADIUS (http://download.novell.com/Download?buildid=NqQA7-rn_ak~) Web page.

3b Install the `novell-radius-ldap-extensions-1.1.x.rpm`. For example,

```
#rpm -ivh novell-radius-ldap-extensions-1.1.0-2.rpm
```

4 Add the RADIUS LDAP extension information:

4a Edit the `radauth_ldapxtn.ldif` file and enter the appropriate LDAP Server DN. For example, you can use the following command to get the LDAP Server DN by appropriately modifying the hostname, port, and trusted root certificate:

```
/opt/novell/eDirectory/bin/ldapsearch -h ldap-server-1.acme.org -p 636 -e /
root/TrustedRootCert.der -s base -L | grep dsaName | cut -c 10- | sed -e "s/
cn=/dn: cn=LDAP Server - /"
```

4b Modify the LDAP Server DN to add the RADIUS LDAP Extension information by appropriately modifying the hostname, port, trusted root certificate, and adminDN:

```
/opt/novell/eDirectory/bin/ldapmodify -h ldap-server-1.acme.org a-p 636 -D
cn=admin,o=org -W -e /root/TrustedRootCert.der -f radauth_ldapxtn.ldif
```

IMPORTANT: For deleting the RADIUS LDAP extension information, replace `add: extensionInfo` with `delete: extensionInfo` in the `radauth_ldapxtn.ldif` file and run the above `ldapmodify` command.

4c Restart LDAP Server by running the following commands in sequence:

```
/opt/novell/eDirectory/sbin/nldap -u

/opt/novell/eDirectory/sbin/nldap -l
```

4d Execute the following command to check that the module is loaded:

```
/opt/novell/eDirectory/bin/ldapsearch -h ldap-server-1.acme.org -p 636 -e /
root/TrustedRootCert.der -b "" -s base supportedExtension | grep 510.100
```

If the module is loaded correctly, you see the following reply:

```
supportedExtension: 2.16.840.1.113719.1.510.100.1
```

If the module is not loaded correctly, restart eDirectory and verify that the module is correctly loaded.

5 Set the default login sequence.

From eDirectory: Use iManager to set the default login sequence for a user in eDirectory.

5a In Novell iManager, click the *Roles and Tasks* tab.

5b Click *Users* > *Modify Users*.

You can select a single object or multiple objects, or perform a simple or advanced selection of the User to be modified.

5c To modify a single object, click *Select a single object*, specify the *Username* or use the *Object Selector* icon to select it, then click *OK*.

5d Click *NMAS Login Sequences*.

5e Select the token authentication method in the default login sequence.

5f Click *OK*.

This sets the token method as the default for the selected user.

From RADIUS Server: Delete all default authentication entries in the `/etc/raddb/users` configuration file and add the token method as default sequence.

For example:

```
DEFAULT eDir-Auth-Option := "digipass"
             Fall-Through = 1
```

The `digipass` method is selected as the default token method to authenticate all the users in the eDirectory.

IMPORTANT: The default token method set in the RADIUS server takes precedence over the eDirectory method for authenticating users.

NOTE: There is a a known issue with FreeRADIUS server on SLES 11 when it is configured for token authentication. To work around this issue, comment the `files` parameter in the `authorize` section of the `/etc/raddb/sites-enabled/inner-tunnel` file or delete the file.

---

8 Security Considerations

Integration of Novell eDirectory with FreeRADIUS requires that passwords be read in clear text. This means that deploying a RADIUS server affects the security of eDirectory and user passwords. Ensure that the following security considerations are met before integrating eDirectory with FreeRADIUS:

8.1 Protecting the RADIUS Server

In order to support several RADIUS protocols, the RADIUS server must have access to users eDirectory passwords.

Therefore, you need to take the following precautions:

- Ensure that you protect the RADIUS server from any attack or subversion. Have a strong eDirectory password for the RADIUS server.
- Always protect the RADIUS server with local and network-edge firewalls, so that it is not directly accessible to the Internet.
- Avoid the exploitation of the vulnerabilities in the software running on the host with root privileges by restricting host login.
- Apply the latest security patches to the networked services running on the host and strictly control access to these services by using a good firewall configuration.
- Regularly monitor and review the log files for any evidence of attack. You need to enable the logging of critical information such as username and passwords in case of authentication or password failures.

  To enable logging of usernames, authentication failures, and passwords, set the value of the following parameters to *yes* in the `/etc/raddb/radiusd.conf` file:

  - `log_stripped_names=yes`

    Logs the User-Name attribute as it was found in the request.

  - `log_auth=yes`

    Logs authentication requests to the log file.

  - `log_auth_badpass=yes`

`log_auth_goodpass=yes`

Log passwords with the authentication requests. Enabling log_auth_badpass logs a password when it is rejected and enabling log_auth_goodpass logs a password when the password is correct

NOTE: Protect the log file by using file system rights. For more information, refer to Section 8.3, "Protecting the Configuration Files," on page 40.

8.2 Risks of Enabling PAP

RADIUS supports protocols that are generally recognized to be unsafe to use in a security-sensitive area, such as PAP.

Be aware of the serious security risks that PAP can present to your user and the systems to which they connect. We strongly recommend that you disable PAP.

8.3 Protecting the Configuration Files

Because the `radiusd.conf`, `proxy.conf`, and `clients.conf` configuration files contain passwords in plain text, they must not be readable by anyone other than the FreeRADIUS administrator (`root`).

You need to protect the following configuration files in `/usr/local/etc/raddb/`:

- clients
- clients.conf
- naspasswd
- proxy.conf
- radiusd.conf
- realms
- snmp.conf
- users

You need to give read/write rights to the above files to `root` users only.

1. Log in as `root`.
2. Execute the following command for each of the files listed above:

```
chmod go-rwx filename
```

8.4 Defining Roles and Granting Rights to Administrators

There are three major roles in eDirectory that you need to clearly define:

- **eDirectory administrator:** Needs complete access rights to the tree.
- **RADIUS administrator:** Needs access only to the RADIUS container and users.

  The eDirectory administrator can grant the RADIUS administrator rights to read the Universal Password of all users under container C by granting the administrator inheritable write rights to the ACL attribute of C.

After eDirectory is integrated with FreeRADIUS, the RADIUS administrator needs to be given rights to read the login details of the RADIUS users.

- **RADIUS and eDirectory users:** Need access rights as defined by the eDirectory administrator to all of their own attributes. Access to RADIUS attributes is not required.

8.5 Risks of Enabling Universal Password

The risks of enabling Universal Password are documented in Security Considerations (http://www.novell.com/documentation/nmas33/admin/data/bc0mf7f.html) section of the *NMAS Administration Guide*. For information on deploying Universal Password, see Enable Universal Password (http://www.novell.com/documentation/password_management33/pwm_administration/data/allr1ls.html) section in the *Password Management 3.3.x Guide*.

8.6 Risks of Disabling eDirectory Account Policy Checking

With eDirectory integration, the RADIUS server can read the Universal Password from eDirectory. Therefore, if the account of the user is disabled or closed in eDirectory, the RADIUS server can still read the Universal Password and authorize the user. Also, the intruder detection facility of eDirectory is bypassed.

To avoid these risks, it is recommended that you enable the eDirectory account policy check so that the authorization fails if either the RADIUS server or the eDirectory server does not authorize the user.

Figure 8-1 *eDirectory Account Policy Check Disabled*

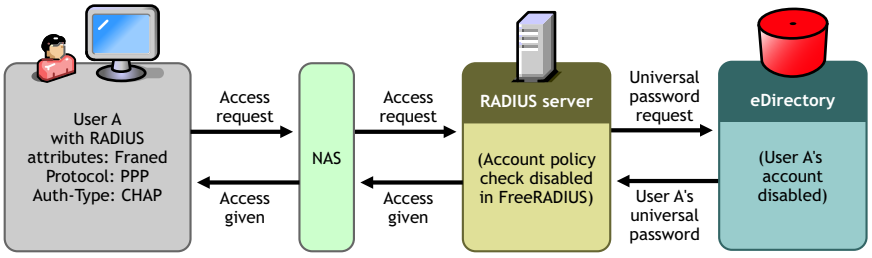
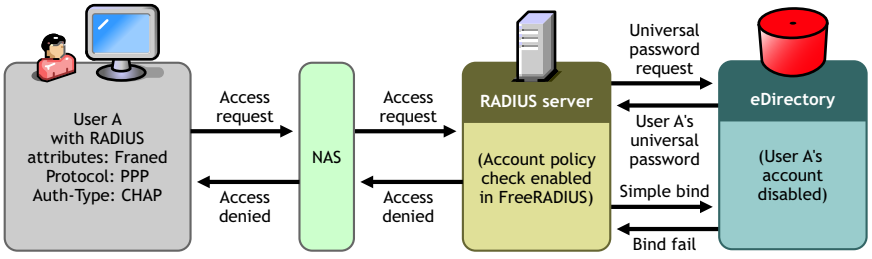


Figure 8-2 *eDirectory Account Policy Check Enabled*



9 Troubleshooting

This section provides information on error codes and solutions for common problems you might encounter while using Novell eDirectory integrated with FreeRADIUS.

9.1 Error Codes

9.1.1 -603 fffffda5 NO SUCH ATTRIBUTE

Source

eDirectory.

Explanation

The requested attribute could not be found. In eDirectory or NDS. If an attribute does not contain a value, then the attribute does not exist for the specific object.

The request might be one of the following:

- Read an eDirectory or NDS schema attribute definition
- Remove an eDirectory or NDS schema attribute definition
- Update an eDirectory or NDS schema attribute definition

IMPORTANT: Applying solutions mentioned in this topic could make the problem worse if the actual cause of the problem is not known. Before following a course of action, ensure that you understand the cause of the error and the consequences for the actions suggested.

Possible Cause

The definition for the specified schema attribute does not exist on the server replying to the request.

Action

Look at the type of object the error is occurring on.

If the object is a simple object, such as a single user that is not a critical user, delete and re-create the problem object.

If it is the source server that is missing the attribute, then use DSREPAIR to perform a Receive All Updates from the Master to This Replica operation on the source server.

IMPORTANT: The Receive All Updates from the Master to This Replica operation in DSREPAIR removes the replica and then places the replica back on the server. This operation cannot be performed on the server that holds the master replica. If this operation needs to be performed on the server holding the master replica, use DSREPAIR to reassign the master replica to another replica ring before starting this operation.

Possible Cause

The specified object does not have the specified attribute.

Action

Perform a Send All Objects to Every Replica in the Ring operation from DSREPAIR.

IMPORTANT: When a Send All Objects to Every Replica in the Ring operation is performed on large partitions or partitions with numerous replicas, it can result in considerable traffic on the network.

Possible Cause

The requester does not have sufficient rights to the attributes for the specified object.

Action

If it is appropriate, assign necessary rights to the requester.

9.1.2 -1659 fffff985 E ACCESS NOT ALLOWED

Source

Novell Modular Authentication Services (NMAS).

Explanation

You do not have sufficient rights to read the Universal Passwords of the users.

Possible Cause

The *Allow admin to retrieve passwords* option is not enabled in the password policy.

Action

Enable the *Allow admin to retrieve passwords* option in the password policy.

9.1.3 -1697 Oxfffff95f NMAS_E_INVALID_SPM_REQUEST

Source

Novell Modular Authentication Services (NMAS).

Explanation

The requested password operation is invalid.

Possible Cause

Universal Password is not enabled for the container in which the object exists.

Action

Enable Universal Password for the container containing the objects.

A RADIUS Attribute Definitions

This section describes the RADIUS attributes and possible values of an attributes in the base schema.

Attribute Name	Description	Values
radiusArapFeatures	The password information that the NAS should send to the user in an ARAP feature flags packet.	
radiusArapSecurity	An ARAP security module to be used in an access-challenge packet.	
radiusArapZoneAccess	Usage of the ARAP zone list for the user.	1=Only allow access to the default zone 2=Use the zone filter inclusively 4=Use the zone filter exclusively
radiusCallbackId	The name of a place to be called or interpreted by the NAS.	
radiusCallbackNumber	The dialing string to be used for callback.	
radiusCalledStationId	Allows the NAS to use the Access-Request packet to send the phone number that the user called, using Dialed Number Identification (DNIS) or similar technology.	
radiusCallingStationId	Allows the NAS to use the access-request packet to send the phone number that the call came from, using Automatic Number Identification (ANI) or similar technology.	
radiusClass	Multivalued attribute sent by the RADIUS server to the client to be forwarded to the RADIUS accounting server.	
radiusFilterId	The name of the filter list for the user.	
radiusFramedAppleTalkLink	The AppleTalk network number that should be used for the serial link to the user, which is another AppleTalk router.	

Attribute Name	Description	Values
radiusFramedAppleTalkNetwork	The AppleTalk Network number that the NAS should probe to allocate an AppleTalk node for the user.	
radiusFramedAppleTalkZone	The AppleTalk Default Zone to be used for this user.	
radiusFramedCompression	The compression protocol to be used for the link.	0=None 1=VJ TCP/IP header compression [10] 2=IPX header compression 3=Stac-LZS compression
radiusFramedIPAddress	The address to be configured for the user.	IP address
radiusFramedIPNetmask	The IP netmask to be configured for the user.	IP address
radiusFramedIPXNetwork	The PX network number to be configured for the user.	
radiusFramedMTU	The maximum transmission unit to be configured for the user.	
radiusFramedProtocol	The framing to be used for framed access.	1=PPP 2=SLIP 3=AppleTalk Remote Access Protocol (ARAP) 4=Gandalf proprietary SingleLink/MultiLink protocol 5=Xylogics proprietary IPX/SLIP 6=X.75 Synchronous
radiusFramedRoute	Multivalued attribute for routing information to be configured for the user on the NAS.	
radiusFramedRouting	The routing method for the user, when the user is a router to a network.	0=None 1=Send routing packets 2=Listen for routing packets 3=Send and Listen
radiusIdleTimeout	Sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt.	

Attribute Name	Description	Values
radiusLoginIPHost	Indicates the system to use for connecting to the user.	
radiusLoginLATGroup	Describes the LAT group codes that the user is authorized to use.	
radiusLoginLATNode	The node to use for automatically connecting the user through LAT.	
radiusLoginLATPort	The port to use for connecting the user through LAT.	
radiusLoginLATService	The system to use to connect the user through LAT.	
radiusLoginService	The service to use to connect the user to the login host.	0=Telnet 1=Rlogin 2=TCP Clear 3=PortMaster (proprietary) 4=LAT 5= X25-PAD 6= X25-T3POS 8=TCP Clear Quiet (suppresses any NAS-generated connect string)
radiusLoginTCPPort	The TCP port with which the user is to be connected.	An integer *i (0 < i < 65536).*
radiusPasswordRetry	The number of authentication attempts a user is allowed to attempt before being disconnected.	Integer.
radiusPortLimit	The maximum number of ports to be provided to the user by the NAS.	Integer.
radiusPrompt	Indicates whether the NAS should echo the user's response (to a challenge) as it is entered.	0=No Echo 1=Echo

Attribute Name	Description	Values
radiusServiceType	The type of service the user has requested or the type of service to be provided.	1=Login 2=Framed 3=Callback Login 4=Callback Framed 5=Outbound 6=Administrative 7=NAS Prompt 8=Authenticate Only 9=Callback NAS Prompt 10=Call Check 11=Callback Administrative
radiusSessionTimeout	The maximum number of seconds of service to be provided to the user before termination of the session or prompt.	Integer.
radiusTerminationAction	Indicates the kind of action the NAS should take when the specified service is completed.	0=Default 1=RADIUS-Request
radiusTunnelAssignmentId	Multivalued attribute that is used to indicate to the tunnel initiator the particular tunnel to which a session is to be assigned.	

Attribute Name	Description	Values
radiusTunnelMediumType	Multilevel attribute used to indicate which transport medium to use when creating a tunnel for protocols (such as L2TP) that can operate over multiple transports.	1 IPv4 (IP version 4) 2 IPv6 (IP version 6) 3 NSAP 4 HDLC (8-bit multidrop) 5 BBN 1822 6 802 (includes all 802 media plus Ethernet canonical format) 7 E.163 (POTS) 8 E.164 (SMDS, Frame Relay, ATM) 9 F.69 (Telex) 10 X.121 (X.25, Frame Relay) 11 IPX 12 Platelike 13 Decant IV 14 Banyan Vines 15 E.164 with NSAP format subduers
radius Tunnel Password	The password to be used to authenticate to a remote server.	
radius Tunnel Preference	Multilevel attribute that should be included in each set to indicate the relative preference assigned to each tunnel, when more than one set of tunneling attributes is returned by the RADIUS server to the tunnel initiator.	
radius Tunnel Private Group Id	Multilevel attribute that indicates the group ID for a particular tunneled session.	
radius Tunnel Server Endpoint	Multilevel attribute that indicates the address of the server end of the tunnel.	

Attribute Name	Description	Values
radius Tunnel Type	Multivalued attribute that indicates the tunneling protocols to be used for a tunnel initiator or the tunneling protocol in use for a tunnel terminator.	1 Point-to-Point Tunneling Protocol (PPTP) [1] 2 Layer Two Forwarding (L2F) [2] 3 Layer Two Tunneling Protocol (L2TP) [3] 4 Ascend Tunnel Management Protocol (ATMP) [4] 5 Virtual Tunneling Protocol (VTP) 6 IP Authentication Header in the Tunnel-mode (AH) [5] 7 IP-in-IP Encapsulation (IP-IP) [6] 8 Minimal IP-in-IP Encapsulation (MIN-IP-IP) [7] 9 IP Encapsulating Security Payload in the Tunnel-mode (ESP) [8] 10 Generic Route Encapsulation (GRE) [9] 11 Bay Dial Virtual Services (DVS) 12 IP-in-IP Tunneling [10]
radiusVSA	Multivalued RADIUS vendor-specific attributes.	
radiusTunnelClientEndpoint	Multivalued attribute that has the address of the initiator end of the tunnel.	
radiusAuthType	Authentication types such as MS-CHAP or NS-MTA-MD5.	
radiusClientIPAddress	The client through which the user requests must be sent.	IP address
radiusGroupName	Multivalued attribute that lists the groups the user belongs to.	
radiusHint	Provides a hint for the user.	
radiusHuntgroupName	Multivalued attribute of Huntgroup for the user.	
radiusProfileDn	The DN of radiusProfile object for this user.	
radiusProxyToRealm	The FreeRADIUS (non-protocol) attribute used to forward RADIUS requests.	

Attribute Name	Description	Values
radiusReplicateToRealm	A deprecated FreeRADIUS attribute.	
radiusRealm	A FreeRADIUS (non-protocol) attribute.	
radiusSimultaneousUse	Limits the number of times one user account can log in.	
radiusLoginTime	A FreeRADIUS (non-protocol) attribute used to define the time span during which a user can log in to the system.	
radiusUserCategory	A FreeRADIUS (non-protocol) attribute. Refers to the definition of a group to which the user belongs.	
radiusStripUserName		
dialupAccess	Used for access control.	
radiusExpiration	The expiration date of the RADIUS account.	
radiusCheckItem	Multivalued attribute which stores the generic radius check-items.	
radiusReplyItem	Multivalued attribute that stores generic radius reply items.	

B Radius Authentication Options

You can use different authentication protocols through the RADIUS server.

Authentication Protocol	*radiusAuthType*	*eDir-Auth-Option*	*password_attribute*
PAP	LDAP	Leave as blank	Leave as blank
CHAP	CHAP	Leave as blank	nspm password
Token-based Authentication (OTP)	LDAP	digipass (for VASCO digipass method)	Leave as blank

Ensure that you use the following settings for these authentication protocols:

- For PAP, CHAP, and OTP, ensure that you specify an appropriate value for the `radiusAuthType` attribute for each authentication protocol as indicated in the table.
- On SUSE Linux Enterprise Server (SLES) 10, add the default authentication entry in the `/etc/raddb/users` configuration file. For more information, see Section 7.2, “Configuring Token Authentication for FreeRADIUS on SLES,” on page 35.
- On SLES 11, select `digipass` as default login sequence for token-based authentication. For more information, see Section 7.2, “Configuring Token Authentication for FreeRADIUS on SLES,” on page 35
- CHAP authentication requires Universal Password. Enable the `password_attribute` and set it to `nspmpassword`.

C Useful Links

This section provides some useful links to additional information about wireless authentication support in FreeRADIUS:

Description	Links
Information on configuring FreeRADIUS in a wireless environment by using Xsupplicant as the Supplicant and using FreeRADIUS as the back-end authentication server.	802.1 *X* Port-Based Authentication HOW TO (http://www.tldp.org/HOWTO/8021X-HOWTO/)
Information on configuring FreeRADIUS to a Windows XP client with EAP/TLS.	◆ HOW TO: EAP/TLS Setup for FreeRADIUS and Windows XP Supplicant (http://www.freeradius.org/doc/EAPTLS.pdf) ◆ FreeRADIUS/WinXP Authentication Setup (http://text.dslreports.com/forum/remark,9286052~mode=flat)
Information on security in wireless networks.	802.11, 802.1*x*, and Wireless Security (http://www.sans.org/rr/whitepapers/wireless/171.php) IS IEEE 802.1*X* Ready for General Deployment? (http://www.sans.org/rr/whitepapers/casestudies/709.php) Comments on “An Initial Security Analysis of the IEEE 802.1*X* Standard” (http://www.funk.com/radius/Solns/umdresp_wp.asp) IEEE 802.1*X* For Wireless LANs (http://www.ieee802.org/1/files/public/docs2000/ieee_plenary.PDF) 802.1*X* Still Evolving as a Standard (http://www.mtghouse.com/8021X.pdf)