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.

Copyright © 2007-2011 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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 .......................... 5

1 Overview ................................ 7

2 Installing FreeRADIUS .................. 9
   Supported Platforms .................. 9
   Installing FreeRADIUS on SLES ....... 9
   What's Next? ...................... 9

3 Configuring the FreeRADIUS Server on SLES 11 to Integrate with eDirectory ... 11
   Prerequisites for Configuring the FreeRADIUS Server .................... 11
      Configuring eDirectory ............ 11
      Extracting the Self-Signed Certificate of the Certificate Authority . 13
   Modifying the LDAP Module .......... 13
      Example of a Modified LDAP Module ................................ 15
      Example for Creating Multiple Instances of an LDAP Module .......... 16
   Enabling the LDAP Module in the Configuration File ...................... 17
      Authorize Section .................. 17
      Authentication Section ............ 17
      Post-Authentication Section ........ 17

4 Configuring the FreeRADIUS Server on SLES 12 SP3 to Integrate with eDirectory .... 19
   Prerequisites for Configuring the FreeRADIUS Server .................... 19
      Configuring eDirectory ............ 20
      Extracting the Self-Signed Certificate of the Certificate Authority . 21
   Modifying the LDAP Module .......... 21
      Example of a Modified LDAP Module ................................ 23
      Example for Creating Multiple Instances of an LDAP Module .......... 24
   Enabling the LDAP Module in the Configuration File ...................... 25
      Authorize Section .................. 25
      Authentication Section ............ 25
      Post-Authentication Section ........ 25
      Creating a Symbolic Link .......... 26

5 Configuring eDirectory Users for RADIUS Authentication .................. 27
   Prerequisites to Configure eDirectory Users for RADIUS Authentication .... 27
      Configuring iManager Plug-In for RADIUS .......................... 27
      Extending the eDirectory Schema for RADIUS ....................... 28
   Adding RADIUS Attributes to eDirectory Users ...................... 29
      Users .................................. 29
      Profile Objects ....................... 29
   Managing RADIUS Objects ............ 29
      Managing RADIUS Users ............. 30
      Managing RADIUS Profiles ........... 30
6 Novell Technical Support for eDirectory Integrated FreeRADIUS

7 Configuring a FreeRADIUS Server for Token Authentication

8 Security Considerations

9 Troubleshooting

A RADIUS Attribute Definitions

B Radius Authentication Options

C Useful Links
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:

- Chapter 1, “Overview,” on page 7
- Chapter 2, “Installing FreeRADIUS,” on page 9
- Chapter 3, “Configuring the FreeRADIUS Server on SLES 11 to Integrate with eDirectory,” on page 11
- Chapter 5, “Configuring eDirectory Users for RADIUS Authentication,” on page 27
- Chapter 6, “Novell Technical Support for eDirectory Integrated FreeRADIUS,” on page 33
- Chapter 7, “Configuring a FreeRADIUS Server for Token Authentication,” on page 35
- Chapter 8, “Security Considerations,” on page 39
- Chapter 9, “Troubleshooting,” on page 43
- Appendix A, “RADIUS Attribute Definitions,” on page 47
- Appendix B, “Radius Authentication Options,” on page 55
- Appendix C, “Useful Links,” on page 57

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).
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.


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 “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.
Installing FreeRADIUS

- “Supported Platforms” on page 9
- “Installing FreeRADIUS on SLES” on page 9
- “What's Next?” on page 9

Supported Platforms

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

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

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.

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

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

- "Prerequisites for Configuring the FreeRADIUS Server" on page 11
- "Modifying the LDAP Module" on page 13
- "Enabling the LDAP Module in the Configuration File" on page 17

Prerequisites for Configuring the FreeRADIUS Server

Download and install the following:

  After installing eDirectory, you need to use iManager to configure it. Refer to “Configuring eDirectory” on page 11 for more information.
  You also need to extract the self-signed certificate of the certificate authority (CA). For more information, refer to “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 NetIQ Download site (https://www.netiq.com/support/imanager/plugins/).

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.

- "Configuring eDirectory" on page 11
- "Extracting the Self-Signed Certificate of the Certificate Authority" on page 13

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
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.


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.
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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cacertfile</td>
<td>Specifies the full path of a certificate file in the UNIX file system.</td>
</tr>
</tbody>
</table>

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

Modifying the LDAP Module

You need to modify the following attributes in the ldap module located at:

- **SLES 11:** `/etc/raddb/modules/ldap`
- **SLES 12:** `/etc/raddb/mods-available/ldap`

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Value</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>hostname or IP address</td>
<td>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 eDirectory LDAP server uses SSL Certificate DNS.</td>
</tr>
<tr>
<td>identity</td>
<td>DN of the RADIUS administrator in eDirectory</td>
<td>DN of the RADIUS administrator under which LDAP searches are performed.</td>
</tr>
<tr>
<td>password</td>
<td>password of the RADIUS administrator in eDirectory</td>
<td>The password authenticates the DN of the RADIUS administrator.</td>
</tr>
<tr>
<td>basedn</td>
<td>The DN of the container that stores the RADIUS users and profile objects</td>
<td>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 &quot;Example for Creating Multiple Instances of an LDAP Module&quot; on page 16.</td>
</tr>
<tr>
<td>filter</td>
<td>(cn=%{Stripped-User-Name:-%{User-Name}})</td>
<td>You can use the LDAP search filter to locate the user object by using name supplied by the RADIUS client during authentication.</td>
</tr>
</tbody>
</table>
Configuring the FreeRADIUS Server on SLES 11 to Integrate with eDirectory

### Attributes

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Value</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>start_tls</td>
<td>no</td>
<td>If the value is set to yes, it creates a secure connection on port 389.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>IMPORTANT:</strong> Ensure that the tls_mode attribute is either commented or the tls_mode is set to no and the port is set to 389.</td>
</tr>
<tr>
<td>cacertfile</td>
<td>Full path of the certificate file in the UNIX file system.</td>
<td>A PEM or Base 64 encoded file that contains the CA certificates.</td>
</tr>
<tr>
<td>require_cert</td>
<td>demand</td>
<td>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.</td>
</tr>
<tr>
<td>dictionary_mapping</td>
<td>${raddbdir}/ldap.attrmap</td>
<td>You can use this attribute to map the RADIUS dictionary attributes with LDAP directory attributes.</td>
</tr>
<tr>
<td>password_attribute</td>
<td>nspmPassword</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>IMPORTANT:</strong> Ensure that you have enabled Universal Password for eDirectory. For more information, refer to “Prerequisites for Configuring the FreeRADIUS Server” on page 11.</td>
</tr>
<tr>
<td>edir_account_policy_check</td>
<td>yes</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> 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:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>♦ The existing eDirectory policies on the user accounts can still be applied after integrating with RADIUS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>♦ eDirectory intruder detection is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>IMPORTANT:</strong> If you find the performance of the RADIUS servers unsatisfactory, you can disable the eDirectory account policy check, but there are security risks.</td>
</tr>
</tbody>
</table>
Configuring the FreeRADIUS Server on SLES 11 to Integrate with eDirectory

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 “Enabling the LDAP Module in the Configuration File” on page 17.

Example of a Modified LDAP Module

```plaintext
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"
}
```

For steps to specify this attribute to the user, see “Modifying RADIUS Users” on page 30.
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.

```plaintext
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
    ....
    ....
}

Enabling the LDAP Module in the Configuration File

- "Authorize Section" on page 17
- "Authentication Section" on page 17
- "Post-Authentication Section" on page 17

Authorize Section

To enable the ldap module, uncomment it in the authorize section of the /etc/raddb/sites-available/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.

Authentication Section

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

Auth-Type LDAP
{
    ldap
}

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
    }
}
Configuring the FreeRADIUS Server on SLES 12 SP3 to Integrate with eDirectory

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

- “Prerequisites for Configuring the FreeRADIUS Server” on page 19
- “Modifying the LDAP Module” on page 21
- “Enabling the LDAP Module in the Configuration File” on page 25

Prerequisites for Configuring the FreeRADIUS Server

Download and install the following:

  After installing eDirectory, you need to use iManager to configure it. Refer to “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 “Extracting the Self-Signed Certificate of the Certificate Authority” on page 21.
- Install Novell iManager 3.1 or later: For installation instructions, refer to the iManager 3.1 Installation Guide (https://www.netiq.com/documentation/imanager-31/imanager_install/data/bookinfo.html).
- Install the Radius iManager plug-in. You can download the plug-in from the NetIQ Download site (https://www.netiq.com/support/imanager/plugins/).

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.

- “Configuring eDirectory” on page 20
- “Extracting the Self-Signed Certificate of the Certificate Authority” on page 21
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 Guide (https://www.netiq.comdocumentation/edirectory-91/edir_admin/data/b1j5uu69.html).

Creating the RADIUS Administrator Object

An Administrator object is a User object.


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/edirectory-91/).

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 option.
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.
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/edirectory-91/edir_admin/data/b1j4t6zc.html).

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cacertfile</td>
<td>Specifies the full path of a certificate file in the UNIX file system.</td>
</tr>
</tbody>
</table>

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

Modifying the LDAP Module

You need to modify the following attributes in the ldap module located at:

- **SLES 12:** /etc/raddb/mods-available/ldap

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Value</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>hostname or IP address</td>
<td>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 eDirectory LDAP server uses SSL Certificate DNS.</td>
</tr>
<tr>
<td>identity</td>
<td>DN of the RADIUS administrator in eDirectory</td>
<td>DN of the RADIUS administrator under which LDAP searches are performed.</td>
</tr>
<tr>
<td>password</td>
<td>password of the RADIUS administrator in eDirectory</td>
<td>The password authenticates the DN of the RADIUS administrator.</td>
</tr>
<tr>
<td>basedn</td>
<td>The DN of the container that stores the RADIUS users and profile objects</td>
<td>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 “Example for Creating Multiple Instances of an LDAP Module” on page 24.</td>
</tr>
<tr>
<td>filter</td>
<td>(cn=%{Stripped-User-Name:-%{User-Name}})</td>
<td>You can use the LDAP search filter to locate the user object by using name supplied by the RADIUS client during authentication.</td>
</tr>
</tbody>
</table>
### Attributes

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Value</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>start_tls</td>
<td>no</td>
<td>If the value is set to <strong>yes</strong>, it creates a secure connection on port 389.</td>
</tr>
<tr>
<td>cacertfile</td>
<td>Full path of the certificate file in the UNIX file system.</td>
<td>A PEM or Base 64 encoded file that contains the CA certificates.</td>
</tr>
<tr>
<td>require_cert</td>
<td>demand</td>
<td>By setting the value of this attribute to <strong>demand</strong>, you configure FreeRADIUS to verify the certificate. The authentication fails if a certificate does not verify.</td>
</tr>
<tr>
<td>dictionary_mapping</td>
<td>${raddbdir}/ldap.attrmap</td>
<td>You can use this attribute to map the RADIUS dictionary attributes with LDAP directory attributes.</td>
</tr>
<tr>
<td>password_attribute</td>
<td>nspmPassword</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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. |
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 “Enabling the LDAP Module in the Configuration File” on page 25.

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"
```

For steps to specify this attribute to the user, see “Modifying RADIUS Users” on page 30.
#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=GroupOfUniqueNames)(uniqueメンバー=%{Ldap-UserDn}))"
# groupmembership_attribute = radiusGroupName
# compare_check_items = yes
# do_xlat = yes
# access_attr_used_for_allow = yes

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/mods-available/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
    ....
    ....
}

Enabling the LDAP Module in the Configuration File

- “Authorize Section” on page 25
- “Authentication Section” on page 25
- “Post-Authentication Section” on page 25
- “Creating a Symbolic Link” on page 26

Authorize Section

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

```plaintext
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.

Authentication Section

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

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

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
        }

}

Creating a Symbolic Link

You need to create a Symbolic link for ldap module inside /etc/raddb/mods-enabled/ as shown below::

    ln -s source_file myfile
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.

- “Prerequisites to Configure eDirectory Users for RADIUS Authentication” on page 27
- “Adding RADIUS Attributes to eDirectory Users” on page 29
- “Managing RADIUS Objects” on page 29

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 “Extending the eDirectory Schema for RADIUS” on page 28.

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).
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.

Adding RADIUS Attributes to eDirectory Users

You can add the RADIUS attributes to the following:

- “Users” on page 29
- “Profile Objects” on page 29

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

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.

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 “Managing RADIUS Profiles” on page 30.

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.

- “Managing RADIUS Users” on page 30
- “Managing RADIUS Profiles” on page 30
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.

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.
You can report bugs and request assistance through 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](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](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).
Configuring a FreeRADIUS Server for Token Authentication

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

- “Prerequisites for Token Authentication” on page 35
- “Configuring Token Authentication for FreeRADIUS on SLES” on page 35

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.
  

- 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 Chapter 3, “Configuring the FreeRADIUS Server on SLES 11 to Integrate with eDirectory,” on page 11.

- 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.

Configuring Token Authentication for FreeRADIUS on SLES

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

1. Uncomment the following lines in the authenticate section:

```plaintext
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.

```plaintext
dict {
    ...
    password_attribute = 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:


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

```bash
# 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 -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:
Supported Extension: 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 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.
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:

- “Protecting the RADIUS Server” on page 39
- “Risks of Enabling PAP” on page 40
- “Protecting the Configuration Files” on page 40
- “Defining Roles and Granting Rights to Administrators” on page 40
- “Risks of Enabling Universal Password” on page 41
- “Risks of Disabling eDirectory Account Policy Checking” on page 41

### 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.
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.

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
   ```

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.
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.

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

- **“Error Codes” on page 43**

**Error Codes**

- “-603 fffffda5 NO SUCH ATTRIBUTE” on page 43
- “-1659 fffff985 E ACCESS NOT ALLOWED” on page 44
- “-1697 Oxffffff9f NMAS_E_INVALID_SPM_REQUEST” on page 45
- “SSL Error” on page 45

### -603 fffffda5 NO SUCH ATTRIBUTE

- “Source” on page 43
- “Explanation” on page 43
- “Possible Cause” on page 44
- “Action” on page 44
- “Possible Cause” on page 44
- “Action” on page 44
- “Possible Cause” on page 44
- “Action” on page 44

**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.

---

**-1659 fffff985 E ACCESS NOT ALLOWED**

- “Source” on page 44
- “Explanation” on page 45
- “Possible Cause” on page 45
- “Action” on page 45

**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.

**-1697 Oxffffff95f NMAS_E_INVALID_SPM_REQUEST**
- “Source” on page 45
- “Explanation” on page 45
- “Possible Cause” on page 45
- “Action” on page 45

**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.

**SSL Error**
- “Explanation” on page 45
- “Action” on page 45

**Explanation**
User may see the SSL Error while extending the Radius schema.

**Action**
Import the self-signed CA certificates into the Java keystore.
## RADIUS Attribute Definitions

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

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>radiusArapFeatures</td>
<td>The password information that the NAS should send to the user in an ARAP feature flags packet.</td>
<td></td>
</tr>
<tr>
<td>radiusArapSecurity</td>
<td>An ARAP security module to be used in an access-challenge packet.</td>
<td></td>
</tr>
<tr>
<td>radiusArapZoneAccess</td>
<td>Usage of the ARAP zone list for the user.</td>
<td>1=Only allow access to the default zone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2=Use the zone filter inclusively</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4=Use the zone filter exclusively</td>
</tr>
<tr>
<td>radiusCallbackId</td>
<td>The name of a place to be called or interpreted by the NAS.</td>
<td></td>
</tr>
<tr>
<td>radiusCallbackNumber</td>
<td>The dialing string to be used for callback.</td>
<td></td>
</tr>
<tr>
<td>radiusCalledStationId</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>radiusCallingStationId</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>radiusClass</td>
<td>Multivalued attribute sent by the RADIUS server to the client to be forwarded to the RADIUS accounting server.</td>
<td></td>
</tr>
<tr>
<td>radiusFilterId</td>
<td>The name of the filter list for the user.</td>
<td></td>
</tr>
<tr>
<td>radiusFramedAppleTalkLink</td>
<td>The AppleTalk network number that should be used for the serial link to the user, which is another AppleTalk router.</td>
<td></td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Description</td>
<td>Values</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>radiusFramedAppleTalkNetwork</td>
<td>The AppleTalk Network number that the NAS should probe to allocate an AppleTalk node for the user.</td>
<td></td>
</tr>
<tr>
<td>radiusFramedAppleTalkZone</td>
<td>The AppleTalk Default Zone to be used for this user.</td>
<td></td>
</tr>
<tr>
<td>radiusFramedCompression</td>
<td>The compression protocol to be used for the link.</td>
<td>0=None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1=VJ TCP/IP header compression [10]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2=IPX header compression</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3=Stac-LZS compression</td>
</tr>
<tr>
<td>radiusFramedIPAddress</td>
<td>The address to be configured for the user.</td>
<td>IP address</td>
</tr>
<tr>
<td>radiusFramedIPNetmask</td>
<td>The IP netmask to be configured for the user.</td>
<td>IP address</td>
</tr>
<tr>
<td>radiusFramedIPXNetwork</td>
<td>The PX network number to be configured for the user.</td>
<td></td>
</tr>
<tr>
<td>radiusFramedMTU</td>
<td>The maximum transmission unit to be configured for the user.</td>
<td></td>
</tr>
<tr>
<td>radiusFramedProtocol</td>
<td>The framing to be used for framed access.</td>
<td>1=PPP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2=SLIP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3=AppleTalk Remote Access Protocol (ARAP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4=Gandalf proprietary SingleLink/MultiLink protocol</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5=Xylogics proprietary IPX/SLIP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6=X.75 Synchronous</td>
</tr>
<tr>
<td>radiusFramedRoute</td>
<td>Multivalued attribute for routing information to be configured for the user on the NAS.</td>
<td></td>
</tr>
<tr>
<td>radiusFramedRouting</td>
<td>The routing method for the user, when the user is a router to a network.</td>
<td>0=None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1=Send routing packets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2=Listen for routing packets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3=Send and Listen</td>
</tr>
<tr>
<td>radiusIdleTimeout</td>
<td>Sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt.</td>
<td></td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Description</td>
<td>Values</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>radiusLoginIPHost</td>
<td>Indicates the system to use for connecting to the user.</td>
<td></td>
</tr>
<tr>
<td>radiusLoginLATGroup</td>
<td>Describes the LAT group codes that the user is authorized to use.</td>
<td></td>
</tr>
<tr>
<td>radiusLoginLATNode</td>
<td>The node to use for automatically connecting the user through LAT.</td>
<td></td>
</tr>
<tr>
<td>radiusLoginLATPort</td>
<td>The port to use for connecting the user through LAT.</td>
<td></td>
</tr>
<tr>
<td>radiusLoginLATService</td>
<td>The system to use to connect the user through LAT.</td>
<td></td>
</tr>
<tr>
<td>radiusLoginService</td>
<td>The service to use to connect the user to the login host.</td>
<td>0=Telnet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1=Rlogin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2=TCP Clear</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3=PortMaster (proprietary)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4=LAT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5= X25-PAD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6= X25-T3POS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8=TCP Clear Quiet (suppresses any NAS-generated connect string)</td>
</tr>
<tr>
<td>radiusLoginTCPPort</td>
<td>The TCP port with which the user is to be connected.</td>
<td>An integer (i ) (0 &lt; i &lt; 65536).</td>
</tr>
<tr>
<td>radiusPasswordRetry</td>
<td>The number of authentication attempts a user is allowed to attempt before being disconnected.</td>
<td>Integer.</td>
</tr>
<tr>
<td>radiusPortLimit</td>
<td>The maximum number of ports to be provided to the user by the NAS.</td>
<td>Integer.</td>
</tr>
<tr>
<td>radiusPrompt</td>
<td>Indicates whether the NAS should echo the user’s response (to a challenge) as it is entered.</td>
<td>0=No Echo</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1=Echo</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Description</td>
<td>Values</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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 |
<p>| radiusTunnelAssignmentId       | Multivalued attribute that is used to indicate to the tunnel initiator the particular tunnel to which a session is to be assigned. |                                                                      |</p>
<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
</table>
| 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 |
<p>| 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. |                                                                      |</p>
<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius Tunnel Type</td>
<td>Multivalued attribute that indicates the tunneling protocols to be used</td>
<td>1 Point-to-Point Tunneling Protocol (PPTP) [1]</td>
</tr>
<tr>
<td></td>
<td>for a tunnel initiator or the tunneling protocol in use for a tunnel</td>
<td>2 Layer Two Forwarding (L2F) [2]</td>
</tr>
<tr>
<td></td>
<td>terminator.</td>
<td>3 Layer Two Tunneling Protocol (L2TP) [3]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 Ascend Tunnel Management Protocol (ATMP) [4]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 Virtual Tunneling Protocol (VTP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 IP Authentication Header in the Tunnel-mode (AH) [5]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7 IP-in-IP Encapsulation (IP-IP) [6]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8 Minimal IP-in-IP Encapsulation (MIN-IP-IP) [7]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9 IP Encapsulating Security Payload in the Tunnel-mode (ESP) [8]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10 Generic Route Encapsulation (GRE) [9]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 Bay Dial Virtual Services (DVS)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12 IP-in-IP Tunneling [10]</td>
</tr>
<tr>
<td>radiusVSA</td>
<td>Multivalued RADIUS vendor-specific attributes.</td>
<td></td>
</tr>
<tr>
<td>radiusTunnelClientEndpoint</td>
<td>Multivalued attribute that has the address of the initiator end of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>tunnel.</td>
<td></td>
</tr>
<tr>
<td>radiusAuthType</td>
<td>Authentication types such as MS-ChAP or NS-MTA-MD5.</td>
<td></td>
</tr>
<tr>
<td>radiusClientIPAddress</td>
<td>The client through which the user requests must be sent.</td>
<td>IP address</td>
</tr>
<tr>
<td>radiusGroupName</td>
<td>Multivalued attribute that lists the groups the user belongs to.</td>
<td></td>
</tr>
<tr>
<td>radiusHint</td>
<td>Provides a hint for the user.</td>
<td></td>
</tr>
<tr>
<td>radiusHuntgroupName</td>
<td>Multivalued attribute of Huntgroup for the user.</td>
<td></td>
</tr>
<tr>
<td>radiusProfileDn</td>
<td>The DN of radiusProfile object for this user.</td>
<td></td>
</tr>
<tr>
<td>radiusProxyToRealm</td>
<td>The FreeRADIUS (non-protocol) attribute used to forward RADIUS requests.</td>
<td></td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Description</td>
<td>Values</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>radiusReplicateToRealm</td>
<td>A deprecated FreeRADIUS attribute.</td>
<td></td>
</tr>
<tr>
<td>radiusRealm</td>
<td>A FreeRADIUS (non-protocol) attribute.</td>
<td></td>
</tr>
<tr>
<td>radiusSimultaneousUse</td>
<td>Limits the number of times one user account can log in.</td>
<td></td>
</tr>
<tr>
<td>radiusLoginTime</td>
<td>A FreeRADIUS (non-protocol) attribute used to define the time span during which a user can log in to the system.</td>
<td></td>
</tr>
<tr>
<td>radiusUserCategory</td>
<td>A FreeRADIUS (non-protocol) attribute. Refers to the definition of a group to which the user belongs.</td>
<td></td>
</tr>
<tr>
<td>radiusStripUserName</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dialupAccess</td>
<td>Used for access control.</td>
<td></td>
</tr>
<tr>
<td>radiusExpiration</td>
<td>The expiration date of the RADIUS account.</td>
<td></td>
</tr>
<tr>
<td>radiusCheckItem</td>
<td>Multivalued attribute which stores the generic radius check-items.</td>
<td></td>
</tr>
<tr>
<td>radiusReplyItem</td>
<td>Multivalued attribute that stores generic radius reply items.</td>
<td></td>
</tr>
</tbody>
</table>
Radius Authentication Options

You can use different authentication protocols through the RADIUS server.

<table>
<thead>
<tr>
<th>Authentication Protocol</th>
<th>radiusAuthType</th>
<th>eDir-Auth-Option</th>
<th>password_attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAP</td>
<td>LDAP</td>
<td>Leave as blank</td>
<td>Leave as blank</td>
</tr>
<tr>
<td>CHAP</td>
<td>CHAP</td>
<td>Leave as blank</td>
<td>nsmp password</td>
</tr>
<tr>
<td>Token-based Authentication (OTP)</td>
<td>LDAP</td>
<td>digipass (for VASCO digipass method)</td>
<td>Leave as blank</td>
</tr>
</tbody>
</table>

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 “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 “Configuring Token Authentication for FreeRADIUS on SLES” on page 35.
- CHAP authentication requires Universal Password. Enable the `password_attribute` and set it to `nsmpassword`. 
Radius Authentication Options
Useful Links

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

<table>
<thead>
<tr>
<th>Description</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information on configuring FreeRADIUS in a wireless environment by using Xsupplicant as the Supplicant and using FreeRADIUS as the back-end authentication server.</td>
<td>802.1 X Port-Based Authentication HOW TO (<a href="http://www.tldp.org/HOWTO/8021X-HOWTO/">http://www.tldp.org/HOWTO/8021X-HOWTO/</a>)</td>
</tr>
</tbody>
</table>
| 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) |
Comments on “An Initial Security Analysis of the IEEE 802.1X Standard” (http://www.funk.com/radius/Solns/umdresp_wp.asp)  
IEEE 802.1X For Wireless LANs (http://www.ieee802.org/1/files/public/docs2000/ieee_plenary.PDF)  
802.1X Still Evolving as a Standard (http://www.mtghouse.com/8021X.pdf) |