WinRADIUS 2.2.6 (32-bit)

Welcome to RADIUS Server for Windows.

Build Options

- OpenSSL 1.0.1j
- OpenLDAP 2.4.40
- Kerberos V (Heimdal 1.6rc2)
- MySQL 5.6.21
- PostgreSQL 9.3.5
- ODBC support (unixODBC 2.3.2)
- Hiredis 0.11.0
- Python 2.7.8
- Perl 5.20.1
- IPv6

Setup

a) Start WinRADIUS Server (Start - Programs - WinRADIUS Server 2.2.6 - Start RADIUS Server (Debug)). *Make sure to stop the scheduled task!*

b) Run tests (in bin\tests folder) (Start - Programs - WinRADIUS Server 2.2.6 - RADIUS Command Prompt)

Useful commands (sanity checks)

a) radiusd.exe -Xv

b) radwho.exe -d ..\etc\raddb

c) run radtestwin.cmd in bin\tests folder

d) run radtest-digest.cmd in bin\tests folder

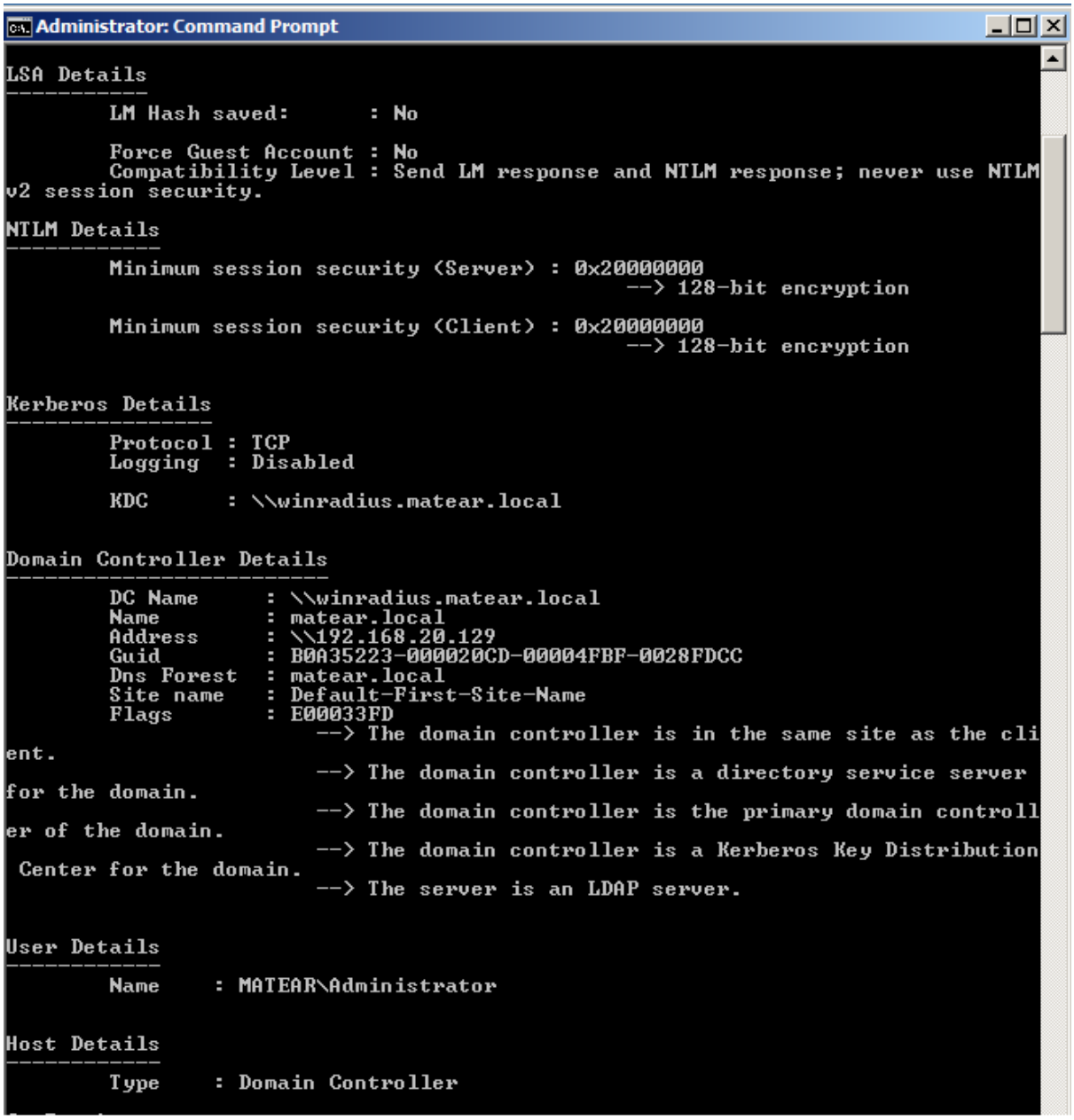
e) run radtest-sim.cmd in bin\tests folder

f) run radeapclient.cmd in bin\tests folder

g) run rad_test_sspi.cmd in bin\tests folder

h) run rad_test_multiotp.cmd in bin\tests folder

bin\sspi_packages_list.exe



multiOTP testing

sbin\multiotp.exe -config log=1 debug=1
sbin\multiotp.exe -config backend-type=files

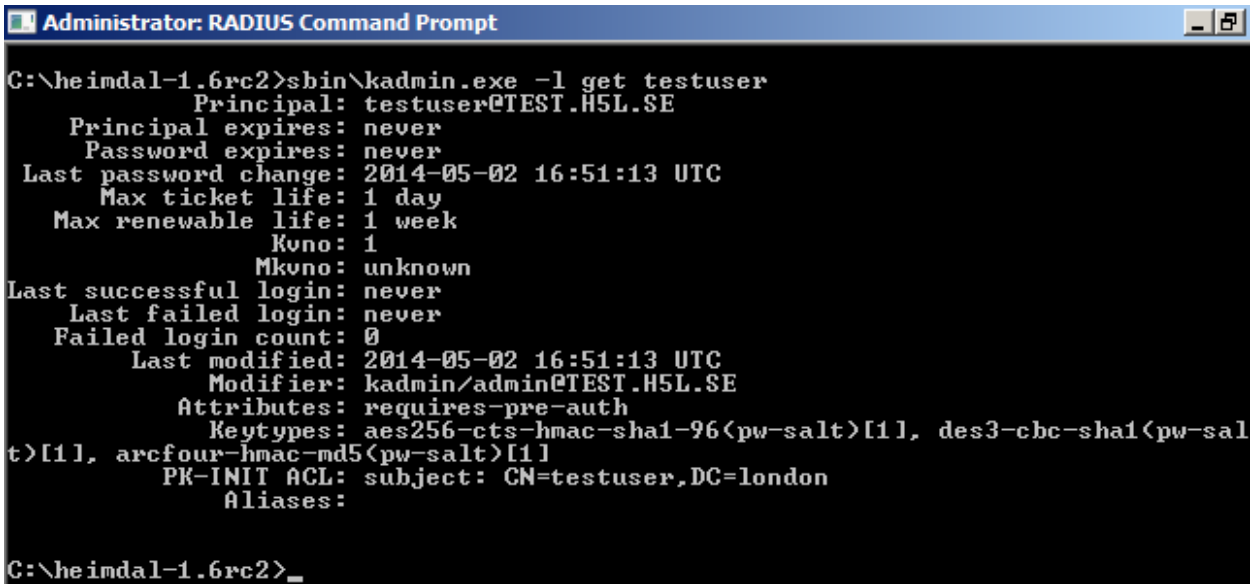
sbin\multiotp.exe -log -delete test_user2
sbin\multiotp.exe -log -create -prefix-pin test_user2 HOTP 31323334353637383930313233343536373839 30 ThisIsAnOtherBigAlphaNumericPrefixPin 6 0

sbin\multiotp.exe -keep-local -log test_user2 ThisIsAnOtherBigAlphaNumericPrefixPin755224

Modules Set Up

rlm_krb5

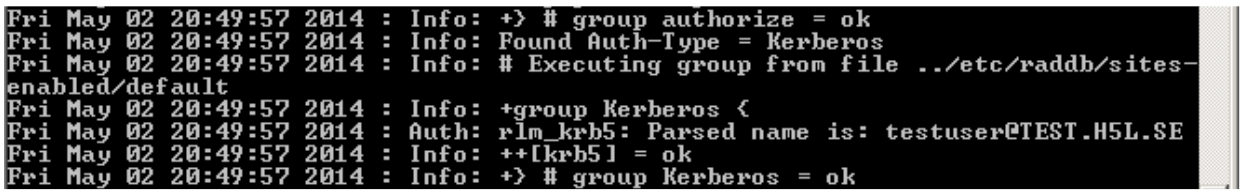
- ✓ Install and set up Heimdal Kerberos (Server)
- ✓ Obtain a valid kerberos ticket for a particular user (a.k.a. kinit <user name>)



- ✓ Add/Adjust some values in: modules/krb5, users, and sites-enabled/default

```
krb5 {
        keytab = C:/heimdal-1.6rc2/etc/krb5.keytab
        service_principal = host/london@TEST.H5L.SE
}


Auth-Type Kerberos {
         krb5
}
```

- ✓ Send a RADIUS auth packet containing the username and password to validate against Kerberos Server (e.g. radclient utility)



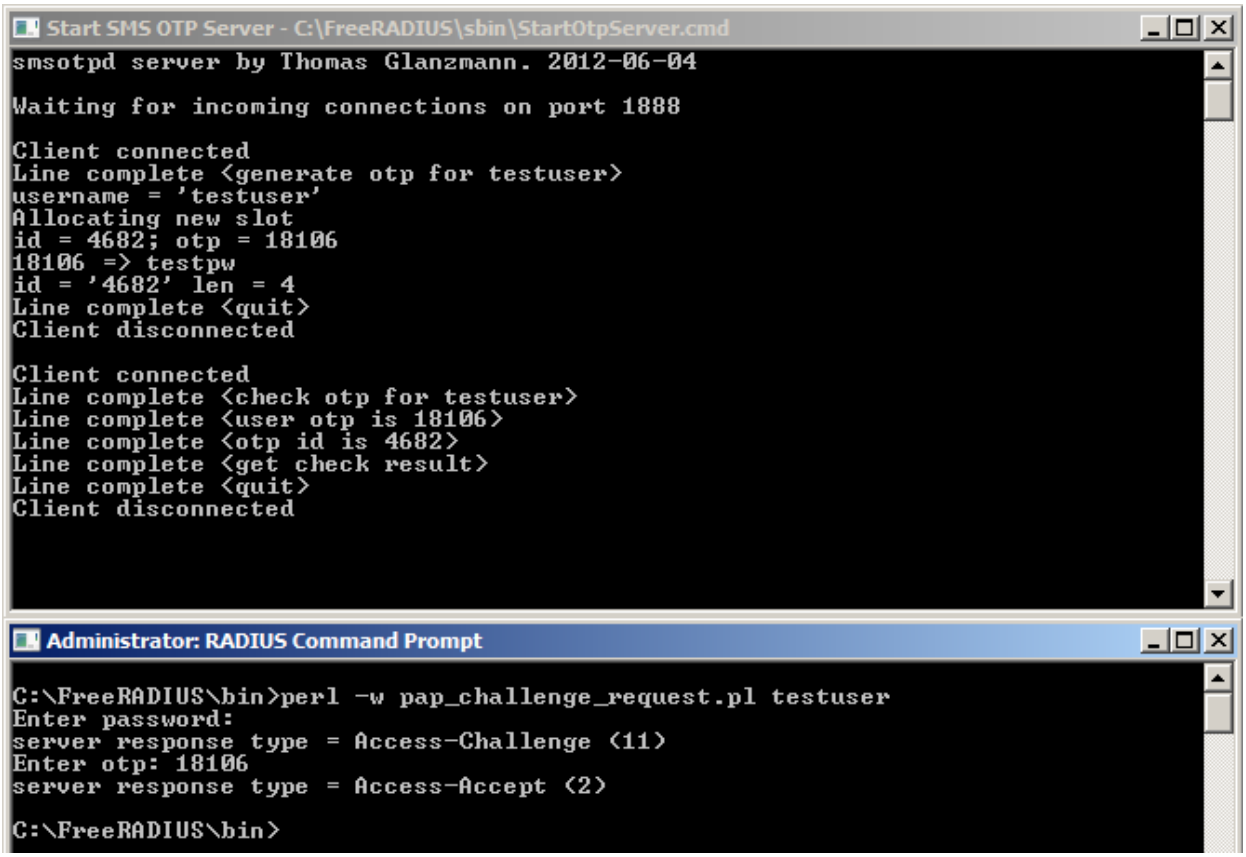
rlm_smsotp

- ✓ Start SMS OTP server (Start – All Programs - WinRADIUS Server 2.2.6 – Start SMS OTP server)

- ✓ Add/Adjust some values in: sites-enabled/default and users files

```
authenticate {
        …
        …
        Auth-Type smsotp {
            pap
            smsotp
        }

        Auth-Type smsotp-reply {
            smsotp
        }
       …
       …

}

authorize {
       …
       …
       smsotp
       …
       …
}

DEFAULT Auth-Type := smsotp
```

- ✓ Issue a RADIUS auth packet containing the username and password to validate against the SMS OTP Server (e.g. pap_challenge_request.pl utility found in the 'bin' folder)


Start SMS OTP Server - C:\FreeRADIUS\sbin\StartOtpServer.cmd
smsotpd server by Thomas Glanzmann. 2012-06-04
Waiting for incoming connections on port 1888
Client connected
Line complete <generate otp for testuser>
username = 'testuser'
Allocating new slot
id = 4682; otp = 18106
18106 => testpw
id = '4682' len = 4
Line complete <quit>
Client disconnected
Client connected
Line complete <check otp for testuser>
Line complete <user otp is 18106>
Line complete <otp id is 4682>
Line complete <get check result>
Line complete <quit>
Client disconnected
Administrator: RADIUS Command Prompt
C:\FreeRADIUS\bin>perl -w pap_challenge_request.pl testuser
Enter password:
server response type = Access-Challenge (11)
Enter otp: 18106
server response type = Access-Accept (2)
C:\FreeRADIUS\bin>


Administrator: Start RADIUS Server - StartServer.cmd
Fri May 02 21:27:48 2014 : Info: +group smsotp {
Fri May 02 21:27:48 2014 : Debug: rlm_smsotp: Generate OTP
Fri May 02 21:27:48 2014 : Auth: rlm_smsotp: Uniq id is 4682
Fri May 02 21:27:48 2014 : Debug: rlm_smsotp: Sending Access-Challenge.
Fri May 02 21:27:48 2014 : Info: ++[smsotp] = handled
Fri May 02 21:27:48 2014 : Info: +} # group smsotp = handled
Sending Access-Challenge of id 241 to 127.0.0.1 port 57653
Reply-Message = "Enter Mobile PIN:"
State = 0x34363832
Fri May 02 21:27:48 2014 : Info: Finished request 0.
Fri May 02 21:27:48 2014 : Debug: Going to the next request
Fri May 02 21:27:48 2014 : Debug: Waking up in 5.0 seconds.
Fri May 02 21:27:53 2014 : Info: Cleaning up request 0 ID 241 with timestamp +9
Fri May 02 21:27:53 2014 : Info: Ready to process requests.
rad_recv: Access-Request packet from host 127.0.0.1 port 57653, id=242, length=7
3
Reply-Message = "Enter Mobile PIN:"
State = 0x34363832
User-Name = "testuser"
User-Password = "18106"
Fri May 02 21:27:56 2014 : Info: # Executing section authorize from file ../etc/
raddb/sites-enabled/default
Fri May 02 21:27:56 2014 : Info: +group authorize {
Fri May 02 21:27:56 2014 : Info: ++[preprocess] = ok
Fri May 02 21:27:56 2014 : Info: ++[chap] = noop
Fri May 02 21:27:56 2014 : Info: ++[mschap] = noop
Fri May 02 21:27:56 2014 : Info: ++[digest] = noop
Fri May 02 21:27:56 2014 : Info: ++[wimax] = ok
Fri May 02 21:27:56 2014 : Info: [suffix] No '@' in User-Name = "testuser", look
ing up realm NULL
Fri May 02 21:27:56 2014 : Info: [suffix] No such realm "NULL"
Fri May 02 21:27:56 2014 : Info: ++[suffix] = noop
Fri May 02 21:27:56 2014 : Debug: rlm_sim_files: insufficient number of challeng
es for imsi testuser: 0
Fri May 02 21:27:56 2014 : Info: ++[sim_files] = notfound
Fri May 02 21:27:56 2014 : Info: [eap] No EAP-Message, not doing EAP
Fri May 02 21:27:56 2014 : Info: ++[eap] = noop
Fri May 02 21:27:56 2014 : Info: [files] users: Matched entry DEFAULT at line 51
Fri May 02 21:27:56 2014 : Info: ++[files] = ok
Fri May 02 21:27:56 2014 : Debug: rlm_smsotp: Found reply to access challenge (A
UTZ), Adding Auth-Type 'smsotp-reply'
Fri May 02 21:27:56 2014 : Info: ++[smsotp] = ok
Fri May 02 21:27:56 2014 : Info: ++[expiration] = noop
Fri May 02 21:27:56 2014 : Info: ++[logintime] = noop
Fri May 02 21:27:56 2014 : Info: [pap] WARNING! No "known good" password found f
or the user. Authentication may fail because of this.
Fri May 02 21:27:56 2014 : Info: ++[pap] = noop
Fri May 02 21:27:56 2014 : Info: +} # group authorize = ok
Fri May 02 21:27:56 2014 : Info: Found Auth-Type = smsotp-reply
Fri May 02 21:27:56 2014 : Info: # Executing group from file ../etc/raddb/sites-
enabled/default
Fri May 02 21:27:56 2014 : Info: +group smsotp-reply {
Fri May 02 21:27:56 2014 : Debug: rlm_smsotp: Found reply to access challenge
Fri May 02 21:27:56 2014 : Auth: rlm_smsotp: SocketReply is OK
Fri May 02 21:27:56 2014 : Info: ++[smsotp] = ok
Fri May 02 21:27:56 2014 : Info: +} # group smsotp-reply = ok

rlm_eap2

users file:

```
mgw        Auth-Type := eap2, Cleartext-Password := "tttt"
```

eap-fast.conf

```
network={
        ssid="test"
        key_mgmt=WPA-EAP
        eap=FAST
        anonymous_identity="mgw"
        identity="mgw"
        password="tttt"
        phase1="fast_provisioning=1"
        phase2="auth=MSCHAPV2"
        pac_file="freeradius.eap-fast-pac"
}
```

Use eapol_test utility to test EAP-FAST

```
Fri May 02 21:50:16 2014 : Info: Found Auth-Type = eap2
Fri May 02 21:50:16 2014 : Info: # Executing group from file ../etc/raddb/sites-
enabled/default
Fri May 02 21:50:16 2014 : Info: +group authenticate {
Fri May 02 21:50:16 2014 : Info: [eap2] Request found, released from the list
CTRL-EVENT-EAP-SUCCESS 00:00:00:00:00:00
Fri May 02 21:50:16 2014 : Debug: ==> Success
Fri May 02 21:50:16 2014 : Info: [eap2] Freeing handler
Fri May 02 21:50:16 2014 : Info: ++[eap2] = ok
Fri May 02 21:50:16 2014 : Info: +} # group authenticate = ok
Fri May 02 21:50:16 2014 : Info: # Executing section post-auth from file ../etc/
raddb/sites-enabled/default
Fri May 02 21:50:16 2014 : Info: +group post-auth {
*** post_auth ***
(('User-Name', '"mgw"'), ('NAS-IP-Address', '127.0.0.1'), ('Calling-Station-Id',
 '"02-00-00-00-00-01"'), ('NAS-IPv6-Address', '0:0:0:0:0:0:0:1'), ('Framed-MTU',
 '1400'), ('NAS-Port-Type', 'Wireless-802.11'), ('Connect-Info', '"CONNECT 11Mbp
s 802.11b"'), ('EAP-Message', '0x0207006b2b0117030100600012f34165998d05299c5aa0c
a4329fdda2e07415626f225a0c1dc4642a3125f629f44fe68510062ed9326e08c6cf0f521ad42864
7aa67ae9bc2656d6b10965171b554ab5b401eca817803eb0f90131298276ac41f3313aa2c182be31
4a6a05e'), ('State', '0x972ab39fa5b8e65e33784a2c074ed74f'), ('Message-Authentica
tor', '0xd6cdaf59088f07755c3fad85fdd1bb45'), ('EAP-Type', 'EAP-FAST'))
Fri May 02 21:50:16 2014 : Info: ++[python] = ok
Fri May 02 21:50:16 2014 : Info: ++[exec] = noop
Fri May 02 21:50:16 2014 : Info: +} # group post-auth = ok
Sending Access-Accept of id 7 to 127.0.0.1 port 51736
        MS-MPPE-Recv-Key = 0xf2ae23fd20be65fd461bf4ccd4082deb7157ec28e629e626828
d4cd80ffbd323
        MS-MPPE-Send-Key = 0x9378c7b979af12fa44de1de31e5b12c2b9ebc5934acaf309c3d
d54cc27ecc609
        EAP-Message = 0x03070004
        User-Name = "mgw"
        Message-Authenticator = 0x00000000000000000000000000000000
Fri May 02 21:50:16 2014 : Info: Finished request 32.
```


RADIUS packet matching with station
MS-MPPE-Send-Key (sign) - hexdump(len=32): 93 78 c7 b9 79 af 12 fa 44 de 1d e3 1
e 5b 12 c2 b9 eb c5 93 4a ca f3 09 c3 dd 54 cc 27 ec c6 09
MS-MPPE-Recv-Key (crypt) - hexdump(len=32): f2 ae 23 fd 20 be 65 fd 46 1b f4 cc
d4 08 2d eb 71 57 ec 28 e6 29 e6 26 82 8d 4c d8 0f fb d3 23
decapsulated EAP packet (code=3 id=7 len=4) from RADIUS server: EAP Success
EAPOL: Received EAP-Packet frame
EAPOL: SUPP_BE entering state REQUEST
EAPOL: getSuppRsp
EAP: EAP entering state RECEIVED
EAP: Received EAP-Success
EAP: Status notification: completion (param=success)
EAP: EAP entering state SUCCESS
CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully
EAPOL: IEEE 802.1X for plaintext connection; no EAPOL-Key frames required
WPA: EAPOL processing complete
EAPOL: SUPP_PAE entering state AUTHENTICATED
EAPOL: SUPP_BE entering state RECEIVE
EAPOL: SUPP_BE entering state SUCCESS
EAPOL: SUPP_BE entering state IDLE
eapol_sm_cb: result=1
EAPOL: Successfully fetched key (len=32)
PMK from EAPOL - hexdump(len=32): f2 ae 23 fd 20 be 65 fd 46 1b f4 cc d4 08 2d e
b 71 57 ec 28 e6 29 e6 26 82 8d 4c d8 0f fb d3 23
EAP: deinitialize previously used EAP method (43, FAST) at EAP deinit
ENGINE: engine deinit
MPPE keys OK: 0 mismatch: 0
SUCCESS

rlm_ldap

- ✓ Install and set up OpenLDAP Server (For instance, add a testing user, certificates, etc)
- ✓ Edit sites-enabled/default file:

```
authorize {
    …
    …

    ldap
    …
    …
}

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

Edit modules/ldap file and adjust some values accordingly (e.g. server name, base dn, etc)

```
Fri May 02 23:36:26 2014 : Info: Found Auth-Type = LDAP
Fri May 02 23:36:26 2014 : Info: # Executing group from file ../etc/raddb/sites-
enabled/default
Fri May 02 23:36:26 2014 : Info: +group LDAP {
Fri May 02 23:36:26 2014 : Info: [ldap] login attempt by "testuser" with passwor
d "testpw"
Fri May 02 23:36:26 2014 : Info: [ldap] user DN: uid=testuser,ou=People,dc=examp
le,dc=com
Fri May 02 23:36:26 2014 : Debug:   [ldap] (re)connect to localhost:389, authent
ication 1
Fri May 02 23:36:26 2014 : Debug:   [ldap] setting TLS CACert File to ../etc/rad
db/certs/ldap/RootCA.pem
Fri May 02 23:36:26 2014 : Debug:   [ldap] setting TLS CACert Directory to ../et
c/raddb/certs/ldap
Fri May 02 23:36:26 2014 : Debug:   [ldap] setting TLS Cert File to ../etc/raddb
/certs/ldap/Server.pem
Fri May 02 23:36:26 2014 : Debug:   [ldap] setting TLS Key File to ../etc/raddb/
certs/ldap/Server.key
Fri May 02 23:36:26 2014 : Debug:   [ldap] setting TLS Rand File to ../etc/raddb
/certs/ldap/random
Fri May 02 23:36:26 2014 : Debug:   [ldap] bind as uid=testuser,ou=People,dc=exa
mple,dc=com/testpw to localhost:389
Fri May 02 23:36:26 2014 : Debug:   [ldap] waiting for bind result ...
Fri May 02 23:36:26 2014 : Debug:   [ldap] Bind was successful
Fri May 02 23:36:26 2014 : Info: [ldap] user testuser authenticated succesfully
Fri May 02 23:36:26 2014 : Info: ++[ldap] = ok
Fri May 02 23:36:26 2014 : Info: +} # group LDAP = ok
Fri May 02 23:36:26 2014 : Info: # Executing section post-auth from file ../etc/
raddb/sites-enabled/default
Fri May 02 23:36:26 2014 : Info: +group post-auth {
*** post_auth ***
(('User-Name', '"testuser"'), ('User-Password', '"testpw"'), ('NAS-IP-Address',
'127.0.0.1'), ('NAS-Port', '1812'))
Fri May 02 23:36:26 2014 : Info: ++[python] = ok
Fri May 02 23:36:26 2014 : Info: ++[exec] = noop
Fri May 02 23:36:26 2014 : Info: +} # group post-auth = ok
Sending Access-Accept of id 164 to 127.0.0.1 port 49221
```

rlm_sql (MS SQL, MySQL, PostgreSQL & ODBC)

MS SQL

- ✓ Make sure that MS SQL server service is up and running and it can be accessed. FreeTDS and unixODBC utilities can be used to test connection to MS SQL servers.
- ✓ Create 'radius' database
- ✓ Execute all SQL scripts under the *etc/raddb/sql/mssql* folder
- ✓ Edit etc/raddb/sql.conf file:

```
sql {
        #
        #   Set the database to one of:
        #
        #           mysql, mssql, oracle, postgresql
        #
        database = "unixodbc"

        driver = "rlm_sql_${database}"

        server = "MSSQLTestServer"
        login = "testsqluser"
        password = "xxxx"
…
…
}
```

- ✓ Edit etc/raddb/sites-enabled/default file:

```
authorize {
    …
    ...
    sql
    …
    …
}

accounting {
    …
    …
    sql
    …
    …
}
```

Test commands

bin\odbcinst.exe -q -s ; bin\odbcinst.exe -q -d

bin\odbcinst.exe -j


Administrator: Start RADIUS Server - StartServer.cmd
ello, testuser
Sat May 03 02:06:51 2014 : Info: ++[files] = ok
Sat May 03 02:06:51 2014 : Info: [sql] expand: %{User-Name} -> testuser
Sat May 03 02:06:51 2014 : Info: [sql] sql_set_user escaped user --> 'testuser'
Sat May 03 02:06:51 2014 : Debug: rlm_sql (sql): Reserving sql socket id: 31
Sat May 03 02:06:51 2014 : Info: [sql] expand: SELECT id,UserName,Attribute,Val
ue,op FROM radcheck WHERE Username = '%{SQL-User-Name}' ORDER BY id -> SELECT id
,UserName,Attribute,Value,op FROM radcheck WHERE Username = 'testuser' ORDER BY
id
Sat May 03 02:06:51 2014 : Info: [sql] User found in radcheck table
Sat May 03 02:06:51 2014 : Info: [sql] expand: SELECT id,UserName,Attribute,Val
ue,op FROM radreply WHERE Username = '%{SQL-User-Name}' ORDER BY id -> SELECT id
,UserName,Attribute,Value,op FROM radreply WHERE Username = 'testuser' ORDER BY
id
Sat May 03 02:06:51 2014 : Info: [sql] expand: SELECT groupname   FROM
radusergroup   WHERE username = '%{SQL-User-Name}' -> SELECT groupname
        FROM radusergroup   WHERE username = 'testuser'
Sat May 03 02:06:51 2014 : Info: [sql] expand: SELECT radgroupcheck.id,radgroup
check.GroupName,radgroupcheck.Attribute,radgroupcheck.Value,radgroupcheck.op FR
OM radgroupcheck,radusergroup WHERE radusergroup.Username = '%{SQL-User-Name}' A
ND radusergroup.GroupName = radgroupcheck.GroupName ORDER BY radgroupcheck.id ->
 SELECT radgroupcheck.id,radgroupcheck.GroupName,radgroupcheck.Attribute,radgrou
pcheck.Value,radgroupcheck.op FROM radgroupcheck,radusergroup WHERE radusergrou
p.Username = 'testuser' AND radusergroup.GroupName = radgroupcheck.GroupName ORD
ER BY radgroupcheck.id
Sat May 03 02:06:51 2014 : Info: [sql] User found in group static
Sat May 03 02:06:51 2014 : Info: [sql] expand: SELECT radgroupreply.id,radgroup
reply.GroupName,radgroupreply.Attribute,radgroupreply.Value,radgroupreply.op FR
OM radgroupreply,radusergroup WHERE radusergroup.Username = '%{SQL-User-Name}' A
ND radusergroup.GroupName = radgroupreply.GroupName ORDER BY radgroupreply.id ->
 SELECT radgroupreply.id,radgroupreply.GroupName,radgroupreply.Attribute,radgrou
preply.Value,radgroupreply.op FROM radgroupreply,radusergroup WHERE radusergrou
p.Username = 'testuser' AND radusergroup.GroupName = radgroupreply.GroupName ORD
ER BY radgroupreply.id
Sat May 03 02:06:51 2014 : Debug: rlm_sql (sql): Released sql socket id: 31
Sat May 03 02:06:51 2014 : Info: ++[sql] = ok
Sat May 03 02:06:51 2014 : Info: ++[expiration] = noop
Sat May 03 02:06:51 2014 : Info: ++[logintime] = noop
Sat May 03 02:06:51 2014 : Info: [pap] WARNING: Auth-Type already set. Not sett
ing to PAP
Sat May 03 02:06:51 2014 : Info: ++[pap] = noop
Sat May 03 02:06:51 2014 : Info: +} # group authorize = ok
Sat May 03 02:06:51 2014 : Info: Found Auth-Type = Local
Sat May 03 02:06:51 2014 : Info: WARNING: Please update your configuration, and
remove 'Auth-Type = Local'
Sat May 03 02:06:51 2014 : Info: WARNING: Use the PAP or CHAP modules instead.
Sat May 03 02:06:51 2014 : Info: User-Password in the request is correct.
Sat May 03 02:06:51 2014 : Info: # Executing section post-auth from file ../etc/
raddb/sites-enabled/default
Sat May 03 02:06:51 2014 : Info: +group post-auth {
*** post_auth ***
(('User-Name', '"testuser"'), ('User-Password', '"testpw"'), ('NAS-IP-Address',
'127.0.0.1'), ('NAS-Port', '1812'))
Sat May 03 02:06:51 2014 : Info: ++[python] = ok
Sat May 03 02:06:51 2014 : Info: ++[exec] = noop
Sat May 03 02:06:51 2014 : Info: +} # group post-auth = ok
Sending Access-Accept of id 251 to 127.0.0.1 port 63393
        Reply-Message = "Hello, testuser"
        Framed-IP-Address := 127.0.0.1
        Framed-Protocol := PPP
        Service-Type := Framed-User
        Framed-Compression := Van-Jacobson-TCP-IP
Sat May 03 02:06:51 2014 : Info: Finished request 0.
Sat May 03 02:06:51 2014 : Debug: Going to the next request
Sat May 03 02:06:51 2014 : Debug: Waking up in 4.9 seconds.
Sat May 03 02:06:56 2014 : Info: Cleaning up request 0 ID 251 with timestamp +3
Sat May 03 02:06:56 2014 : Info: Ready to process requests.

rlm_sspi (Experimental module!)

users file:

```
# SSPI test users
Administrator      Auth-Type := sspi
Guest              Auth-Type := sspi
```

sites-enables/default

```
authorize {
…
…
sspi
…
…
}

authenticate {
…
…
Auth-Type sspi {
        sspi
    }
…
…

}
```

Sending an access request …

rad_test_sspi.cmd

```
Thu May 08 01:42:22 2014 : Info: Found Auth-Type = sspi
Thu May 08 01:42:22 2014 : Info: # Executing group from file ../etc/raddb/sites-
enabled/default
Thu May 08 01:42:22 2014 : Info: +group sspi {
Thu May 08 01:42:22 2014 : Info: rlm_sspi: Using default server mechanism: Negot
iate
Thu May 08 01:42:22 2014 : Info: rlm_sspi: Using default client mechanism: NTLM

Thu May 08 01:42:22 2014 : Info: rlm_sspi: Validating user ... UpdatusUser
Thu May 08 01:42:22 2014 : Auth: rlm_sspi: Impersonated User Name: LONDON\Updatu
sUser
Thu May 08 01:42:22 2014 : Auth: rlm_sspi: User's Primary Group Name: LONDON\Non
e (S-1-5-21-2202974141-873423652-2567894797-513)
Thu May 08 01:42:22 2014 : Info: ++[sspi] = ok
Thu May 08 01:42:22 2014 : Info: +} # group sspi = ok
Thu May 08 01:42:22 2014 : Info: # Executing section post-auth from file ../etc/
raddb/sites-enabled/default
Thu May 08 01:42:22 2014 : Info: +group post-auth {
```

```
Sending Access-Request of id 253 to 127.0.0.1 port 1812
        User-Name = "UpdatusUser"
        User-Password = "WandA2014"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 1812
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=253, length=83
        Reply-Message = "SEC_E_OK: The operation completed successfully. (0x0000
0000)"

          Total approved auths:  1
            Total denied auths:  0
               Total lost auths:  0
```

Using an invalid password …

```
Thu May 08 01:47:20 2014 : Info: +> # group authorize = ok
Thu May 08 01:47:20 2014 : Info: Found Auth-Type = sspi
Thu May 08 01:47:20 2014 : Info: # Executing group from file ../etc/raddb/sites-
enabled/default
Thu May 08 01:47:20 2014 : Info: +group sspi {
Thu May 08 01:47:20 2014 : Info: rlm_sspi: Using default server mechanism: Negot
iate
Thu May 08 01:47:20 2014 : Info: rlm_sspi: Using default client mechanism: NTLM

Thu May 08 01:47:20 2014 : Info: rlm_sspi: Validating user ... UpdatusUser
Thu May 08 01:47:20 2014 : Auth: rlm_sspi: ERROR_LOGON_FAILURE: Logon failure: u
nknown user name or bad password. (0x0000052E)
Thu May 08 01:47:20 2014 : Info: ++[sspi] = reject
Thu May 08 01:47:20 2014 : Info: +> # group sspi = reject
Thu May 08 01:47:20 2014 : Info: Failed to authenticate the user.
Thu May 08 01:47:20 2014 : Info: Using Post-Auth-Type REJECT
```

```
Sending Access-Request of id 47 to 127.0.0.1 port 1812
        User-Name = "UpdatusUser"
        User-Password = "WandA2013"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 1812
rad_recv: Access-Reject packet from host 127.0.0.1 port 1812, id=47, length=80
        Reply-Message = "SEC_E_LOGON_DENIED: The logon attempt failed (0x8009030
C)"

           Total approved auths:  0
             Total denied auths:  1
              Total lost auths:  0
```

Using a disabled account …

```
Thu May 08 01:51:01 2014 : Info: +> # group authorize = ok
Thu May 08 01:51:01 2014 : Info: Found Auth-Type = sspi
Thu May 08 01:51:01 2014 : Info: # Executing group from file ../etc/raddb/sites-
enabled/default
Thu May 08 01:51:01 2014 : Info: +group sspi {
Thu May 08 01:51:01 2014 : Info: rlm_sspi: Using default server mechanism: Negot
iate
Thu May 08 01:51:01 2014 : Info: rlm_sspi: Using default client mechanism: NTLM

Thu May 08 01:51:01 2014 : Info: rlm_sspi: Validating user ... Guest
Thu May 08 01:51:01 2014 : Auth: rlm_sspi: ERROR_ACCOUNT_DISABLED: Logon failure
: account currently disabled. (0x00000533)
Thu May 08 01:51:01 2014 : Info: ++[sspi] = reject
Thu May 08 01:51:01 2014 : Info: +> # group sspi = reject
Thu May 08 01:51:01 2014 : Info: Failed to authenticate the user.
Thu May 08 01:51:01 2014 : Info: Using Post-Auth-Type REJECT
```

rlm_perl

Just uncomment *perl* from sites-enables/default post-auth section

Note: Make sure Perl has been installed and check the PERL5LIB environment variable.

```
Thu May 08 19:39:16 2014 : Debug: rlm_perl: Added pair User-Password = testpw
Thu May 08 19:39:16 2014 : Debug: rlm_perl: Added pair NAS-Port = 1812
Thu May 08 19:39:16 2014 : Debug: rlm_perl: Added pair NAS-IP-Address = 127.0.0.
1
Thu May 08 19:39:16 2014 : Debug: rlm_perl: Added pair User-Name = testuser
Thu May 08 19:39:16 2014 : Debug: rlm_perl: Added pair Message-Authenticator = 0
x08a567edf516ded47c6c5f439f4265f8
Thu May 08 19:39:16 2014 : Debug: rlm_perl: Added pair Reply-Message = Hello, te
stuser
Thu May 08 19:39:16 2014 : Debug: rlm_perl: Added pair Auth-Type = PAP
Thu May 08 19:39:16 2014 : Debug: rlm_perl: Added pair Cleartext-Password = test
pw
Thu May 08 19:39:16 2014 : Info: ++[perl] = ok
```

rlm_python

Just uncomment *python* from sites-enables/default post-auth section

Note: Make sure Python 2.7 has been installed and check the PYTHONHOME environment variable.

```
*** post_auth ***
(('User-Name', '"testuser"'), ('User-Password', '"testpw"'), ('NAS-IP-Address',
'127.0.0.1'), ('NAS-Port', '1812'), ('Message-Authenticator', '0x08a567edf516ded
47c6c5f439f4265f8'))
Thu May 08 19:39:16 2014 : Info: ++[python] = ok
```

Notes:

- IPv6 is enabled by default. If your system doesn't support it, please update the relevant sections in radiusd.conf file
- MySQL Authentication: create database 'radius' and run scripts in \etc\raddb\sql\mysql. More information in: http://wiki.freeradius.org/guide/SQL-HOWTO
- Uncomment all 'sql' references in radiusd.conf file. MySQL Server should be up and running before starting radius server
- LDAP Authentication: update etc\raddb\modules\ldap file (e.g. basedn, etc)
- OpenLDAP for Windows can be downloaded from SourceForge: http://sourceforge.net/projects/openldapwindows/
- Heimdal for Windows can be downloaded from SourceForge: http://sourceforge.net/projects/heimdal-win/
- Hostapd/WPA Supplicant for Windows can be downloaded from SourceForge: http://sourceforge.net/projects/hostapd/
- Redis Server for Windows can be downloaded from SourceForge: http://sourceforge.net/projects/redis/
- multiOTP can be downloaded from here: http://www.multiotp.net/
  Thanks to *Andre Liechti*, for the support and contribution

Source Code

The source code is available at:

- FreeRADIUS Project, http://freeradius.org/
- WinRADIUS Project, http://winradius.eu/

* Please, report any issues/feedback/etc to the following email address: support@winradius.eu