TekRADIUS

Installation & Configuration Guide
Version 5.8

Document Revision 21.6

https://www.kaplansoft.com/

TekRADIUS is built by Yasin KAPLAN

TekRADIUS Manual is edited by David VANT

Read 'Readme.rtf' for last-minute changes and updates, which can be found in the application directory.

Table of Contents

Table of Contents 3
Introduction 5
System Requirements 7
Installation 8
Configuration 9
Settings Tab 9
Accounting Table 14
Parameters / Service 15
Parameters / Authentication 18
Parameters / Accounting 22
Parameters / DHCP Server 23
Parameters / Cipher Suites 24
Parameters / Mail Alerting 25
Parameters / HTTP Interface 26
Clients 27
Groups 29
Users 31
Dynamic IP Address Assignment 33
Dictionary Editor 34
SQL Query Executioner 35
Reporting 36
DHCP Server 37
TekRADIUS Manager Menus 40
File Menu 40
Service Menu 41
Help Menu 41
Starting TekRADIUS 42
User Group Determination via Policy Matching 43
Monitoring 44
Active Sessions 45
TekRADIUS Log File 47
TekRADIUS Specific Attributes (RADIUS Check Items) 48
TekRADIUS-Status 48
Simultaneous-Use 48
Simultaneous-Group-Use 48
Expire-Date 48
User-Credit 49
Credit-Unit 49
Authentication-Method 49
TLS-Server-Certificate (TLS-Certificate prior to version 4.0) 50
TLS-Client-Certificate 51
Windows-Domain 51
Directory-Server 51
Active-Directory-Group 52
Time-Limit 52
First-Logon 52
Login-Time 52
Generate-MS-MPPE-Keys 53
Next-Group 53
Failure-Reply-Type 54
Tunnel-Tag 54
Credit-Period 54
Credit-Per-Period 54
External-Executable 55
Credit-Expiry-Action 56
EAP-SIM-Triplet-[1|2|3] 57
EAP-SIM-OP 57
EAP-SIM-OPc 57
EAP-SIM-Key 58
EAP-SIM-SQN 58

HTTP-Access-Level 58
HTTP-User-Name & HTTP-User-Password 58
Password-Limit 58
Password-Reset 59
Check-MS-DialinPrivilege 59
Lock-MAC-Address 59
Activation-Date 59
Success-Reply-Type 59
OTP-Type 60
OTP-Length 60
OTP-Sender 60
OTP-Timeout 60
Accounting-Free 60
Data-Volume-Based-Authorization 61
Google-Authenticator-Secret 61
Google-Authenticator-Issuer 61
Quota-Warning-Action 62
Quota-Warning-Threshold 62
Concatenated-Password 62
External-Accounting-Action 62
Allowed-SSID 63
DHCP-Server 63
Description 63
Client-Label 63
Email-Address 63
TLS-Allowed-CA 64
Simultaneous-Limit-Action 64
NAS-Vendor 64
Request-Certificate 64
X509-Revocation-Mode 64
TekRADIUS-Logging 65
Lock-IMEI 65
Data Volume Based Authorization 66
Vendor Specific Attribute for Connection Rate Limiting 68
Change of Authorization Support for Disconnecting User Sessions 69
HTTP Interface 70
Reporting Interface 70
User Management Interface 75
RADIUS Proxy 76
IPv6 Attributes 77
Troubleshooting 78
TekRADIUS Service Messages (TekRADIUS log file) 80
Third Party Application Integration 84
TekRADIUS Command Line Interface - TRCLI.exe 85
Creating and Installing a Self-Signed Certificate for PEAP/EAP-TLS Authentication 90
Creation of Self Signed Certificate 90
Certificate Deployment at Client Side 91
Client PEAP Configuration 93
Client EAP-TLS Configuration 94
SQL Server Configuration 96
Connecting to SQL Express Using TCP/IP 96
SQL Express Authentication Configuration 97
Encoding of Attribute 144 in RFC 4679 (ADSL-Forum Access-Loop-Encapsulation) 98
Failure Codes in Accounting Table DisconnectCause Field when “Save Authentication Failures” Option is Set 99
Regular Expression Based Check Attributes 101
Using Alternative Authentication and Authorization Queries 102
Performance tips 103
Creating ODBC Connection Profiles for TekRADIUS OD 104
Creating an ODBC DSN for SQLite 104
Creating an ODBC DSN for MySQL 104
Creating an ODBC DSN for MariaDB 105
Creating an ODBC DSN for PostgreSQL 107
Creating an ODBC DSN for Oracle Database 108
Index 109

Introduction

TekRADIUS is a RADIUS AAA server *(Based on RFC 2865 and RFC 2866)* and runs under Microsoft Windows *(Vista/7/8/10, 2008-2022 Server)* operating systems. Visit https://www.kaplansoft.com/TekRADIUS regularly for updates.

The following authentication methods are supported by TekRADIUS:

- PAP [RFC 2865]
- CHAP [RFC 2865]
- MS-CHAP v1 [RFC 2548, RFC 2759]
- MS-CHAP v2 [RFC 2548, RFC 2759]
- LEAP
- EAP-MD5 [RFC 2284, RFC 2869]
- EAP-MS-CHAP v2 [draft-kamath-pppext-eap-mschapv2-02.txt]
- EAP-TLS [RFC 2716]
- EAP-TTLS [RFC 5281]
- EAP-SIM [RFC 4186]
- EAP-AKA [RFC 4187]
- PEAPv0-EAP-MS-CHAP v2 [draft-kamath-pppext-peapv0-00.txt] *(As implemented in Windows XP SP1)*
- Digest [draft-sterman-aaa-sip-00.txt] *(SIP Authentication)*
- OTP *(One Time Password)* authentication based on RFC 2289 and Google Authenticator.

TekRADIUS also supports RFC 2868 *(RADIUS Attributes for Tunnel Protocol Support)* and RFC 3079 (Deriving Keys for use with Microsoft Point-to-Point Encryption *(MPPE))*. PPTP/L2TP connections may be authenticated and authorized using TekRADIUS. TekRADIUS also supports TCP *(RFC 6613)* and TLS *(RFC 6614-RadSec)* transports. TekRADIUS can proxy RADIUS requests to other RADIUS servers.

TekRADIUS supports TLS 1.0, TLS 1.1, TLS 1.2 and TLS 1.3. EAP-TLS with TLS 1.3 is also supported *(RFC 9190)*.

! *LEAP, EAP-TLS, EAP-SIM, EAP-AKA and EAP-TTLS are only supported in the commercial edition of TekRADIUS. You can use only PAP, CHAP, MS-CHAP, MS-CHAP-v2, EAP-MD5 and EAP-MS-CHAP-v2 as inner authentication methods with EAP-TTLS. Inner authentication methods supported in PEAP are EAP-MD5 and EAP-MS-CHAP-v2. CHAP authentication can be used just for local user profiles.*

TekRADIUS has a built-in DHCP server that can assign IP addresses to wireless clients based on the usernames entered for PEAP/EAP authentication and not just based on MAC addresses. The DHCP server function is available in both the free and commercial editions of TekRADIUS.

! *IP address assignment based on username is only supported in the commercial edition of TekRADIUS.*

TekRADIUS can send Packet of Disconnect *(PoD)* or execute a user defined session kill command when a user's credit is fully consumed *(SP Edition only)*.

! *The execution of a user defined session kill command when a user's credit is fully consumed is only supported in the SP Edition of TekRADIUS.*

TekRADIUS supports the following signature algorithms:

RSASSA-PKCS1-v1_5 algorithms

- rsa_pkcs1_sha1 (0x0201)
- rsa_pkcs1_sha256 (0x0401)
- rsa_pkcs1_sha384 (0x0501)
- rsa_pkcs1_sha512 (0x0601)

ECDSA algorithms

- ecdsa_secp256r1_sha256 (0x0403)
- ecdsa_secp384r1_sha384 (0x0503)
- ecdsa_secp521r1_sha512 (0x0603)

RSASSA-PSS algorithms with public key OID rsaEncryption

- rsa_pss_rsae_sha256 (0x0804)
- rsa_pss_rsae_sha384 (0x0805)
- rsa_pss_rsae_sha512 (0x0806)

Supported Elliptic Curve Groups *(ECDHE)*

- secp256r1 (0x0017)
- secp384r1 (0x0018)
- secp521r1 (0x0019)
- x25519 (0x001D)

System Requirements

A Pentium class CPU with 2 GB of RAM is ideal for most configurations; however, it is necessary to have Microsoft .NET Framework 4.8 installed with the latest patches.

TekRADIUS standard edition supports only Microsoft SQL Server; TekRADIUS LT supports both Microsoft SQL Server and SQLite.

The TekRADIUS SQL edition requires Microsoft SQL Server. Any version of Microsoft SQL server, including Express editions, may be used. The disk space required and SQL edition necessary depends on the application. Please see section entitled 'SQL Server Configuration' for instructions on how to configure the SQL Server for use with TekRADIUS.

Although an "sa" equivalent SQL user is needed to create the initial database and tables, a less privileged SQL user may be used for regular operations.

Please make sure that the service account for TekRADIUS has read/write access to TekRADIUS application directory and act as part of the operating system *(SeTcbPrivilege)* privilege if you run TekRADIUS service application under an account other than Local System Account.

TekRADIUS LT does not require an additional database server. TekRADIUS LT uses its own built-in SQLite database. The TekRADIUS LT Manager creates database at first run automatically.

TekRADIUS OD supports SQLite, MySQL, MariaDB and PostgreSQL databases through ODBC. ODBC connection profiles must be created in ODBC Data Source Administrator *(64-bit)* / System DSN. TekRADIUS automatically creates necessary tables, indexes and views in the database. Th database user must have enough privilege to create tables, indexes and views in the database. Allow multiple queries in ODBC profiles for MySQL and MariaDB databases.

An SC/PC compatible smart card reader is required for importing SIM triplets from a SIM card.

Installation

Unzip **TekRADIUS.zip** or **TekRADIUSLT.zip** and launch **Setup.exe** that comes with the distribution. Follow the instructions of the setup wizard. The setup will install TekRADIUS Manager *(TRManager.exe)* and the TekRADIUS Service *(TekRADIUS.exe)* and add a shortcut for TekRADIUS Manager to the desktop and the start menu. TekRADIUS service can be started or stopped through TekRADIUS Manager / Service menu. You do not have to keep TekRADIUS Manager running if TekRADIUS service is running.

Please uninstall the existing version prior to installing a new version. You can keep existing TekRADIUS.ini *(Settings file)*, TekRADIUS.db *(Dictionary file)* and TekRADIUS.db3 *(TekRADIUS LT SQLite database)* files.

Configuration

Run TekRADIUS Manager with Administrative privileges from the desktop shortcut or selecting TekRADIUS Manager from **Start > Programs > TekRADIUS > TekRADIUS Manager**.

! *Administrative privileges mean either logged in as Administrator or as a user that is a member of the built-in 'Administrator' group.*

NOTE: It is not possible to access settings without administrative privileges. Running TekRADIUS Manager from an ordinary user account causes TekRADIUS Manager to run in 'Operator' mode, which only provides for:

- Changing existing user profiles,
- Monitoring active sessions,
- Generating usage reports. *(Please see the related section on generating usage reports.)*

Initialization parameters should be configured before running the TekRADIUS Service. It is necessary to save the changes and restart the TekRADIUS service after making any configuration changes.

Settings Tab

Click the **Settings** tab to start configuration.

Database *(SQL Edition Only)*

The SQL Connection must be configured first. Enter the following information:

SQL Server

Enter the IP address or the FQDN of the server running the SQL server or select a detected SQL server from the drop-down list.

If the SQL server is installed on the same server as TekRADIUS, 'Localhost' *(without quotes)* may be used to identify the SQL Server. If the default instance of an SQL server is used, use '**.**' *(period mark)* to denote the default instance. The TekRADIUS Manager will add a service dependency if a local SQL server is selected. This will be removed when a remote SQL server is selected.

Timeout

Enter the connection timeout *(in seconds)* for the SQL Server. The default value is 30 seconds.

Username

Enter the SQL username to be used to connect to the SQL server.

The SQL server must be configured to support at least username/password-based authentication. The authentication mode may be changed using SQL Server Management Studio *(right click the registered SQL Server instance, select Properties and then Security)*. For SQL Server 2000, consult http://support.microsoft.com/kb/285097. Refer to the section titled 'SQL Server Configuration' to configure an SQL Server to use with TekRADIUS.

TekRADIUS will use Windows authentication and logged-in user's credentials to connect to the SQL server if you leave username and password blank. You need to set a Windows user account for the TekRADIUS service application if you prefer Windows authentication in

place of SQL authentication. Go to Administrative Tools / Services / TekRADIUS service, right click and select properties to specify a user account manually in Log On tab;

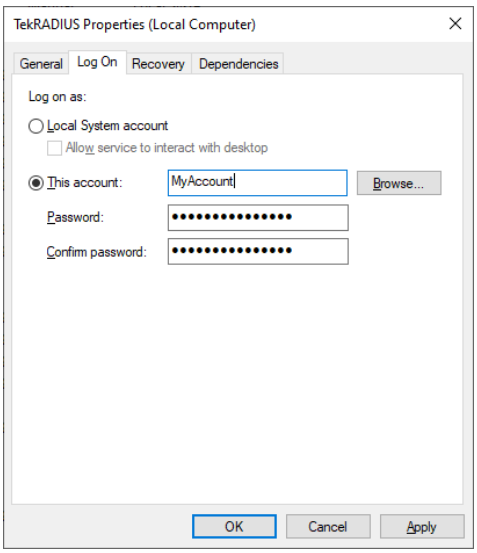


Figure 0 – Manually configurating a service account

Windows *(or Active Directory)* account must have "Act as part of the operating system" privilege.

Password

Enter the password of the SQL user.

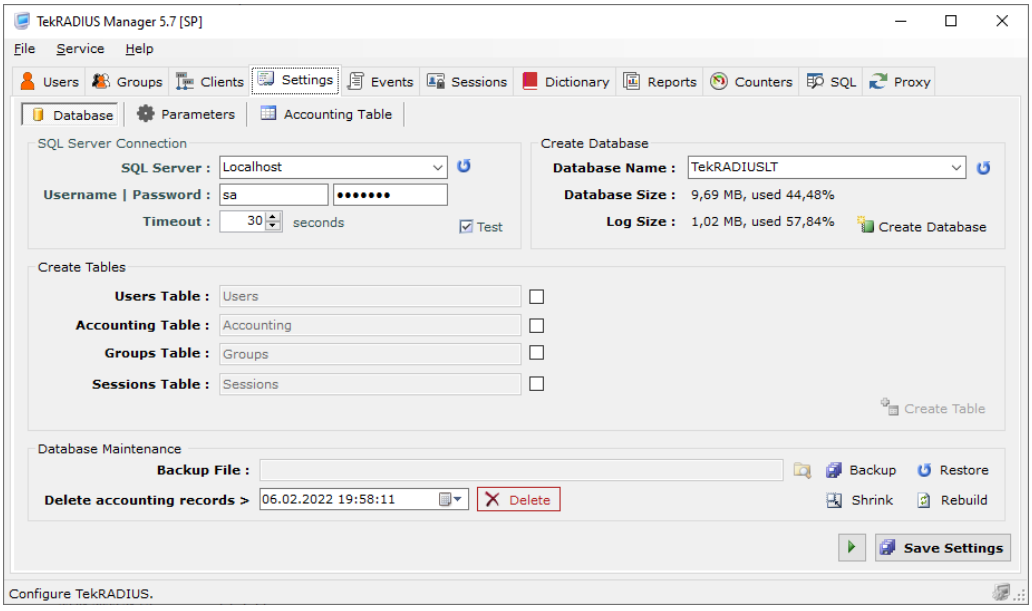


Figure 1 - **Database** Connection Settings

To test the settings before saving, click **Test Connection**. "*Connection Successful but database does not exist*" or "*Connection Successful but there was missing table(s)*" responses indicate that the configuration is valid.

The database and all associated database tables may be either created from within TekRADIUS Manager or manually using SQL scripts. The SQL scripts for the manual creation of the

TekRADIUS database and tables can be found in the TekRADIUS installation directory (*TekRADIUS.sql* for the database, and *Users.sql, Groups.sql, Acconting.sql* and *Session.sql* for the tables).

Create Tables

If TekRADIUS Manager can access the SQL Server, it is now possible to create the necessary database and tables. If TekRADIUS finds any previously created tables, it automatically unchecks entries for those tables.

Create Database / Database Name:

Enter the database name. The default name is 'TekRADIUS'. Click **Create Database** to create the database. The following SQL clause is executed automatically to create the database:

```
CREATE DATABASE [TekRADIUS]
GO
```

If the database is created successfully, the message *"Database created and connection settings are updated…"* will be displayed.

Create Tables / Users Table:

The Users Table contains the user definitions and the check and reply RADIUS attributes for the users. Uncheck the checkbox if the Users Table is not created.

The following SQL clause is automatically executed to create the Users Table:

```
USE [TekRADIUS]
GO

CREATE TABLE [dbo].[Users](
      [UserName] [nchar](64) NOT NULL,
      [Attribute] [nchar](16) NULL,
      [AttrType] [int] NULL,
      [Val] [nchar](64) NULL
) ON [PRIMARY]
GO

CREATE NONCLUSTERED INDEX [IX_Users] ON [dbo].[Users]
([UserName] ASC)
GO
```

Create Tables / Accounting Table:

The Accounting Table stores RADIUS accounting messages. Uncheck the checkbox if the Accounting Table is not to be created.

The following SQL clause is executed to create the Accounting Table *(Indexes are vital for high performance!):*

```
USE [TekRADIUS]
GO

CREATE TABLE [dbo].[Accounting](
      [tracid] [nchar](32) NOT NULL,
      [SessionID] [nchar](255) NOT NULL,
      [StatusType] [nchar](30) NULL,
      [InputOcts] [bigint] NULL CONSTRAINT [DF_Accounting_InputOcts]  DEFAULT ((0)),
      [OutOcts] [bigint] NULL CONSTRAINT [DF_Accounting_OutOcts]  DEFAULT ((0)),
      [InputGigaWord] [bigint] NULL CONSTRAINT DF_Accounting_InputGigaWord DEFAULT (0),
      [OutputGigaWord] [bigint] NULL CONSTRAINT DF_Accounting_OutputGigaWord DEFAULT (0),
      [OutOcts] [bigint] NULL CONSTRAINT [DF_Accounting_OutOcts]  DEFAULT ((0)),
      [UserName] [nchar](128) NULL,
      [NasIPAddr] [nchar](15) NULL,
      [NasIdentifier] [nchar](255) NULL,
      [NasPort] [nchar](40) NULL,
      [NasPortId] [nchar](255) NULL,
```

```
	[NasPortType] [nchar](40) NULL,
	[ServiceType] [nchar](40) NULL,
	[FramedIPAddr] [nchar](15) NULL,
	[CallingStationId] [nchar](128) NULL,
	[CalledStationId] [nchar](128) NULL,
	[AcctSessTime] [int] NULL,
	[DisconnectCause] [nchar] (128),
	[TimeStamp] [datetime] NOT NULL,
	[Amount] [int] NULL)
GO

CREATE NONCLUSTERED INDEX [IX_Accounting_1] ON [dbo].[Accounting]
(
	[tracid] ASC
)
GO
CREATE NONCLUSTERED INDEX [IX_Accounting_2] ON [dbo].[Accounting]
(
	[TimeStamp] ASC
)
GO
CREATE NONCLUSTERED INDEX [IX_Accounting_3] ON [dbo].[Accounting]
(
	[StatusType] ASC
)
GO
CREATE NONCLUSTERED INDEX [IX_Accounting_4] ON [dbo].[Accounting]
(
	[UserName] ASC
)
GO
CREATE NONCLUSTERED INDEX [IX_Accounting_5] ON [dbo].[Accounting]
(
	[SessionID] ASC
)
GO
CREATE NONCLUSTERED INDEX [IX_Accounting_6] ON [dbo].[Accounting]
(
	[NASIPAddr] ASC
)
GO
```

InputOcts and OutOcts fields stores Acct-Input-Octets and Acct-Output-Octets attributes respectively in RADIUS Accounting packets. Acct-Input-Gigawords and Acct-Output-Gigawords attributes are used to report how many times maximum integer value is exceeded in RADIUS accounting packets for a user session. TekRADIUS updates Acct-Input-Gigawords and Acct-Output-Gigawords attribute values if corresponding gigaword values are greater than zero. Stored values in the accounting table are kept in 64 bit columns so stored values reflect updated usage values with gigaword counts. Gigaword values are stored just for informational purposes. You can alter column sizes to use disc space more efficiently.

Create Tables / Groups Table:

The Groups Table contains common check and reply RADIUS attributes for the users. Uncheck the checkbox if the Groups Table is not to be created.

The following SQL clause is executed to create the Groups Table:

```
USE [TekRADIUS]
GO

CREATE TABLE [dbo].[Groups]
(
	[GroupID] [nchar](64) NULL,
	[Attribute] [nchar](64) NULL,
	[AttrType] [int] NULL,
	[Val] [nchar](128) NULL
) ON [PRIMARY]
GO

CREATE NONCLUSTERED INDEX [IX_Groups] ON [dbo].[Groups]
([GroupID] ASC)
GO
```

Create Tables / Sessions Table

TekRADIUS stores active sessions on the Sessions Table. When a RADIUS accounting start message is received, a record for that session will be added to the Sessions Table. TekRADIUS will remove that record as soon as it receives a RADIUS accounting stop message for that session. TekRADIUS clears the Sessions table every time the service starts. The sessions displayed in the **Active Sessions** tab are derived from the Sessions Table. Uncheck the checkbox if the Sessions table is not to be created.

The following SQL clause is executed to create the Sessions table:

```
   USE [TekRADIUS]
   GO

CREATE TABLE [dbo].[Sessions](
  [tracid] [nchar](32) NOT NULL,
  [TimeStamp] [datetime] NULL,
  [SessionID] [nchar](255) NULL,
  [UserName] [nchar](128) NULL,
  [GroupName] [nchar](128) NULL,
  [NasIPAddr] [nchar](40) NULL,
  [NasIdentifier] [nchar](255) NULL,
  [NasPort] [nchar](40) NULL,
  [NasPortType] [nchar](40) NULL,
  [NasPortId] [nchar](255) NULL,
  [ServiceType] [nchar](40) NULL,
  [FramedIPAddr] [nchar](40) NULL,
  [CallingStationID] [nchar](128) NULL,
  [CalledStationID] [nchar](128) NULL,
  [auditsessionid] [nchar](64) NULL,
  [OUserName] [nchar](128) NULL,
  [LastActivity] [datetime] NULL,
  [CallOrigin] [nchar](16) NULL,
  [Active] [int] NULL,
  [InterimUpdatePeriod] [int] NULL,
PRIMARY KEY CLUSTERED
(
  [tracid] ASC
)
) ON [PRIMARY]
GO

ALTER TABLE [dbo].[Sessions] ADD  CONSTRAINT [DF_Sessions_Active]  DEFAULT ((1)) FOR [Active]
GO

ALTER TABLE [dbo].[Sessions] ADD  CONSTRAINT [DF_Sessions_InterimUpdatePeriod]  DEFAULT ((0))
FOR [InterimUpdatePeriod]
GO
```

Click **Create Tables** to create the selected tables. If the tables are created successfully, the message *"Table(s) created and connection settings are updated..."* will be displayed. The `AttrType` field is set to "0" for RADIUS check attributes, "1" for success-reply attributes and "2" for failure-reply attributes in the Users and Groups tables.

Database Maintenance

The TekRADIUS Database may be shrunk and old accounting records deleted to save space, and a backup may be taken of the database for disaster recovery purposes.

Backup / Restore

Enter the filename for the database backup and click **Backup**. You can restore backup data later by clicking **Restore** button. Backup and Restore functions are accessible through File / Database menu.

! *The created backup file is in TekRADIUS proprietary format.*

Shrink

To shrink the TekRADIUS database, click **Shrink Database**. You can invoke VACUUM[1] statement at the SQL tab of TekRADIUS Manager to shrink the local SQLite database. You can run

```
VACUUM main INTO 'Full path for the backup database'
```

to make a backup of an existing database.

Rebuild

Click **Rebuild** to re-create indexes in Accounting and Sessions table. You should do this when you upgrade from a version prior to 5.4.

Delete

Enter a date and time prior to which all accounting records should be deleted and click **Delete**. You can run the following statement to delete accounting data older than one month in TekRADIUS LT;

```
DELETE from Accounting where strftime('%m', 'now', 'localtime') - strftime('%m', [TimeStamp]) > 1
```

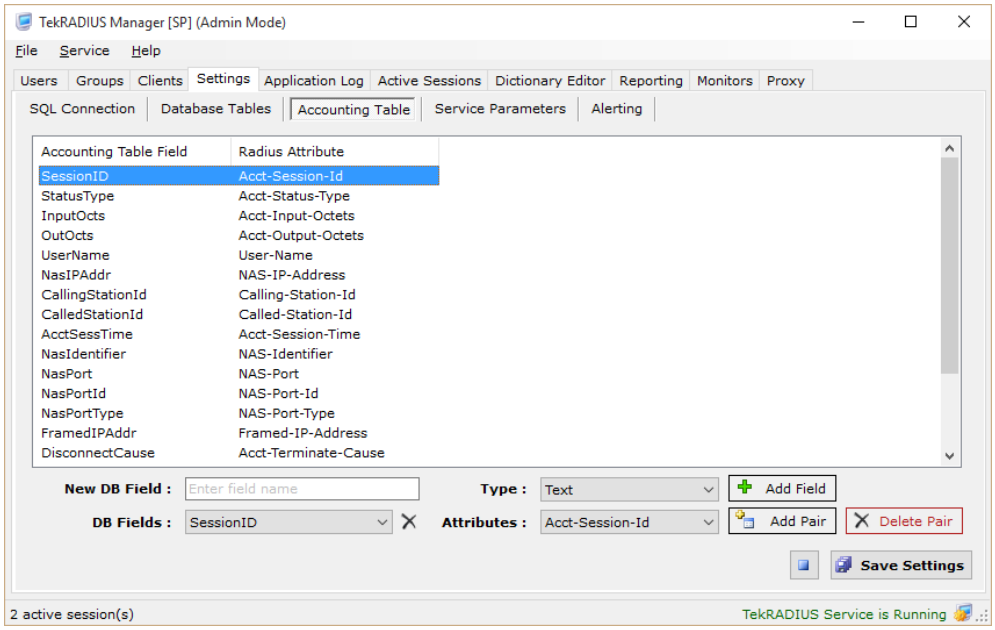


Figure 2 - Accounting Table Field Selection

Accounting Table

It is possible to define in which field of the accounting table will store which RADIUS accounting attributes that are received in RADIUS Accounting messages. Additional accounting fields may be created and assigned to a RADIUS attribute. Existing field/attribute pairs may also be deleted.

The left list-box identifies the Accounting Table field; the right list-box identifies the matching RADIUS attribute.

To create additional fields:

[1] Please see https://sqlite.org/lang_vacuum.html for more details.

1. Type a unique field name into the 'New DB Field' box,
2. Select type of the RADIUS attribute to be stored in this field from the 'Type' drop-down list,
3. Click **Add Field**.

To define Field/Attribute pairs:

1. Select the required field from the 'DB Fields' drop-down list and the corresponding RADIUS attribute from the 'Attributes' drop-down list,
2. Click **Add Pair**.

To delete Field/Attributes:

1. Select the required pair in the main display,
2. Click **Delete Pair**.

Special consideration is required for the *Cisco-AVPair* attribute as it is necessary to manually enter the Cisco-AVPair key to the Radius Attribute. For example, if the Cisco access server sends *Cisco-AVPair="connect-progress=LAN Set Up"*, it would be necessary to add *"connect-progress"* as the RADIUS Attribute;

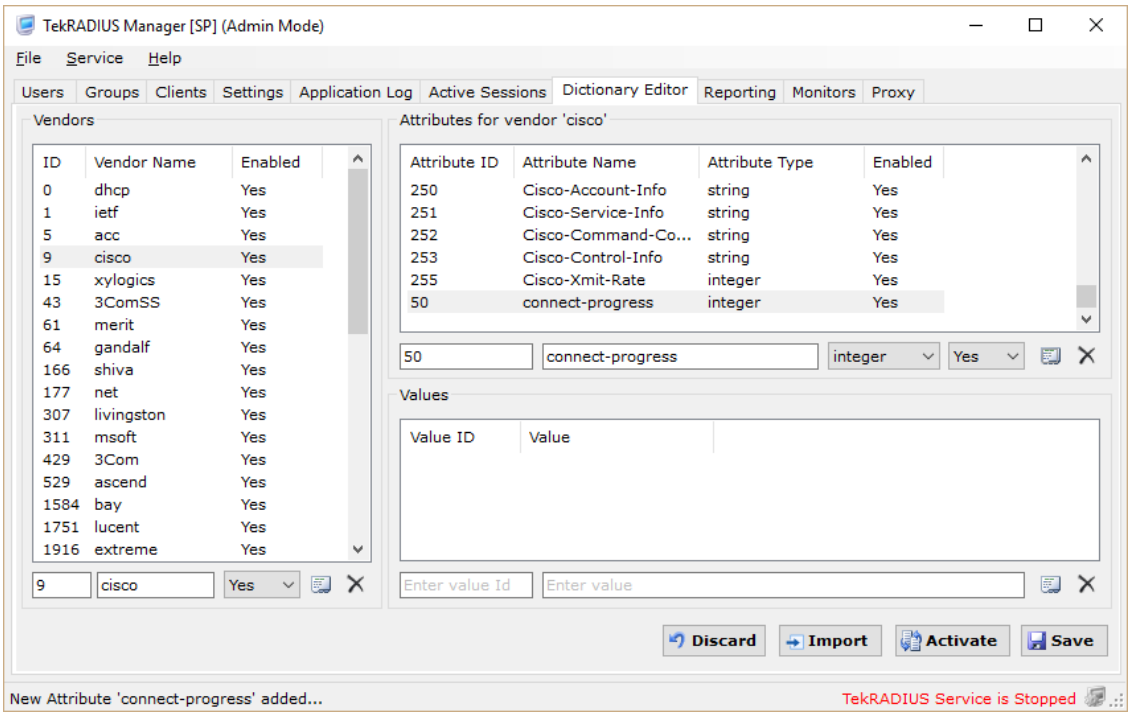


Figure 3. - Adding a dummy attribute for Cisco-AVPair

Parameters / Service

Enter the following information to configure service specific parameters:

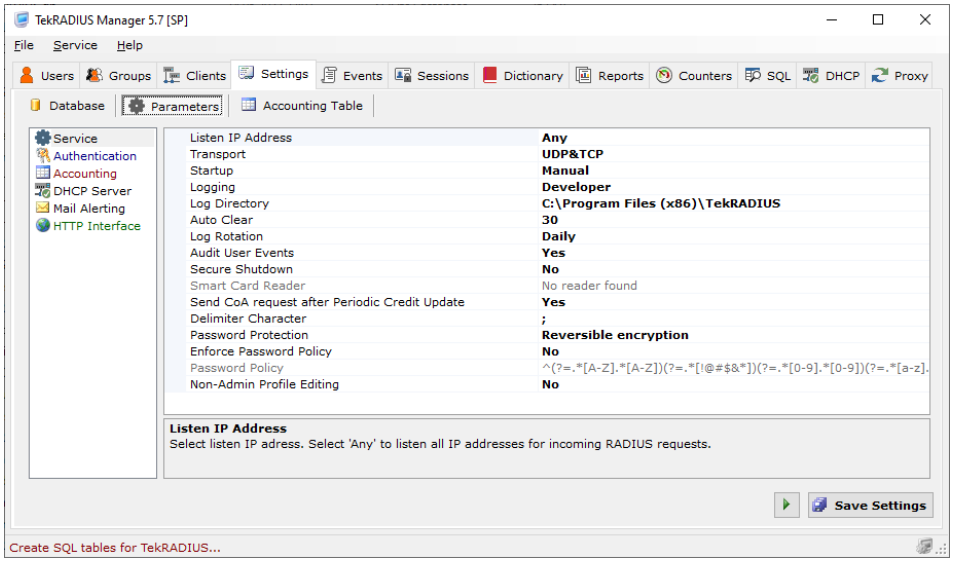


Figure 5 - Service Parameters Configuration

Listen IP Address

From the drop-down list, select an IP address for TekRADIUS to listen for incoming messages. The list contains all IP addresses associated with all enabled network interfaces.

If an IP address, used by TekRADIUS, is removed from the Windows Network configuration, TekRADIUS will automatically select the first available IPv4 address in the network settings at startup.

Transport

From the drop-down list, select transport. TekRADIUS enables both UDP and TCP transports.

Startup

Select the startup mode of the TekRADIUS Windows service. The default startup mode is 'Manual'. Click **Save Settings** to make the selected mode active.

Logging

Select the logging level of the TekRADIUS service. Select either:

- 'None' for no logging,
- 'Errors' to log errors,
- 'Sessions' to log session information and errors,
- 'Debug' to provide more details on errors and gives packet decodes for authentication exchanges.
- "Developer" for special diagnostic output.

Log Directory

Log files are stored under the **<Application Directory>\Logs directory** by default.

Auto Clear

TekRADIUS can delete log files older than specified days. Set 0 to disable this feature.

Log Rotation

TekRADIUS rotates log files daily by default or you can choose hourly if your system generates large log files.

Audit User Events

TekRADIUS logs user, group, client and configuration changes under Windows Event Log / Application and Services Log / TekRADIUS Audit when this option is enabled. This requires a commercial license.

Secure Shutdown *(SP Edition only)*

Check this option to force TekRADIUS to terminate for any active sessions when it is shutdown. Termination is performed by sending a PoD packet by default. Termination is performed with a Kill command if a Kill command is defined for a NAS.

Smart Card Reader

Select Smart Card Reader to read SIM triplets from a SIM card for EAP-SIM authentication.

Delimiter Character

Specify the delimiter character to be used when entering multiple string-type, reply attributes in user or group profiles. The default value is a semi-colon "**;**".

Password Protection

This option enables you to choose a password protection method. You can keep passwords in reversible encrypted, hashed or clear text from. Some system integration with 3rd party applications requires you to set Clear text option.

You cannot use OTP or Google Authenticator when you use SHA Hashing to protect password values in TekRADIUS database. You also cannot use CHAP or MS-CHAP based authentication methods with local user profiles in TekRADIUS since TekRADIUS needs to access to user password in clear text form to make necessary calculations used in these authentication methods.

User passwords cannot be changed when passwords are kept in hashed form in the TekRADIUS database using MS-CHAP password changing methods.

Enforce Password Policy

Check this box to enforce password policy specified for the user profiles. You can specify a regular expression-based password policy to check passwords for complexity.

Password entered for User-Password and HTTP-User-Password attributes through either TekRADIUS Manager, TRCLI.exe or HTTP interface of TekRADIUS are checked against policy specified in "Password Policy" options below. TekRADIUS will also check passwords entered in password changing operations *(Changing aged passwords through MS-CHAP-v2 e.g.)*.

Password Policy

You can enter a regular expression to check the complex password. The TekRADIUS Manager will check regular expressions as you type. Green background means a valid regular expression entered. Default password policy is

```
^(?=.*[A-Z].*[A-Z])(?=.*[!@#$&*])(?=.*[0-9].*[0-9])(?=.*[a-z].*[a-z].*[a-z]).{8}$
```

`(?=.*[A-Z].*[A-Z])`	Password must have two uppercase letters.
`(?=.*[!@#$&*])`	Password must have one special case letter.
`(?=.*[0-9].*[0-9])`	Password must have two digits.
`(?=.*[a-z].*[a-z].*[a-z])`	Password must have three lowercase letters.
`.{8}`	Password length must be 8 characters long.

You can alter this regular expression to specify complex password policies.

Non-Admin User Editing

TekRADIUS disables user editing functions *(Adding, removing, changing user profiles)*, when you run TekRADIUS manager with a Windows user who is not in Administrators group. You can enable user editing functions for non-Admin users by checking this option. This feature is available only in commercial editions.

DHCP Server *(Available with a commercial license)*

You can specify a global DHCP server IP address in service parameters which will be used to forward DHCP requests to acquire IP addresses to be returned in Framed-IP-Address attribute in authorization responses. You can specify individual DHCP server IP address per user or per group by adding DHCP-Server attribute to user or group profiles.

ODBC DSN *(OD Edition Only)*

Select ODBC connection profile to connect to the database. Database must be created, and an ODBC DNS must be configured first. TekRADIUS will automatically create necessary tables, indexes and views. Please see "Creating ODBC Connection Profiles for TekRADIUS OD" for how to create ODBC DSNs.

Policy Matching.

Please see User Group Determination via Policy Matching section.

Dynamic Peer Discovery.

Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI) based on RFC 7585 *(Requires SP license)*.

Proxy RADIUS Server Polling Period.

TekRADIUS can poll remote RADIUS servers specified in proxy profiles by sending RADIUS Status-Server *(RFC 5997)* requests. TekRADIUS will mark the server offline after three consecutive requests go unanswered. Set a value greater than 0 to enable polling.

Parameters / Authentication

RADIUS Authentication Port

Enter the UDP RADIUS authentication port between 1 and 65535. If no value is entered, the default port of 1812 will be used.

If the selected port is used by another program, TekRADIUS will disable the RADIUS Authentication thread and add the following event entry to the Windows Event Log: *"Unable to initialize TekRADIUS Authentication thread"*.

TLS Port

TekRADIUS uses TCP port 2083 for TLS transport by default. Enter the TCP port between 1 and 65535 for TLS transport.

Server Certificate

Select a certificate for Server Authentication for TLS transport. TekRADIUS lists valid certificates in Windows Certificate Store / Local Machine. This certificate will also be used by default for PEAP sessions if you do not set a TLS-Server-Certificate in user or group profiles. The same certificate is used for HTTPS connections to TekRADIUS HTTP interface. The certificate must be generated for an FQDN resolvable to IP address of the TekRADIUS machine if it will be used for also HTTPS connections.

TekRADIUS will automatically switch the most current certificate after the selected certificate is expired if you create and add a new certificate with the same subject name in Windows Certificate Store / Local Machine / personal folder.

Trusted CAs

TekRADIUS performs mutual authentication for TLS transport *(RadSec)* by default. You can specify allowed Certificate Authorities for client certificates. Specified CAs will be also checked in EAP-TLS negotiations. All valid CAs *(The ones in Windows Certificate Store / Local Machine / Trusted Root Certification Authorities folder)* are trusted by default.

Enable TLS 1.3

Enable TLS 1.3 for EAP-TLS PEAP and EAP-TTLS. TekRADIUS supports TLS 1.0, TLS 1.1 and TLS 1.2 by default.

Include Certificate Chain of Trust

TekRADIUS adds all certificates up to the root CA certificate in certificates section of TLS handshake when this option is enabled. TekRADIUS will add only server certificate when it's disabled.

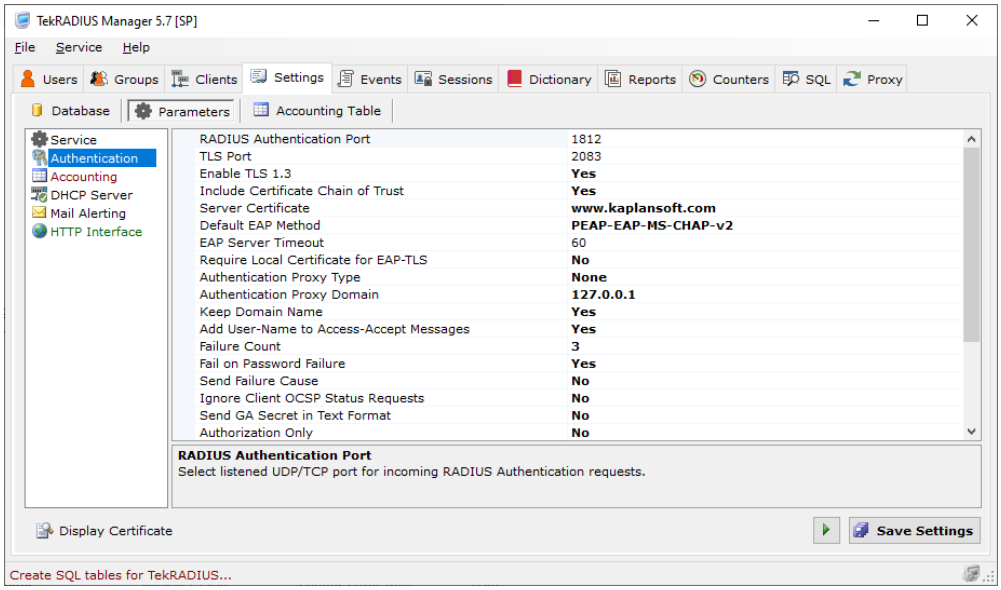


Figure 6 - Service Parameters - Authentication

Authentication Proxy Type

TekRADIUS can act as a proxy for the user accounts that cannot be found in TekRADIUS database. Non-existent user accounts can be authenticated against Windows Domain / Server and Active Directory user accounts. If this feature is enabled and TekRADIUS cannot find a valid entry in the Users Table, the username/password will be checked against user specified domain or Windows server.

If the username/password is valid in the domain or server, Success-Reply attributes are fetched from the Default user Group. If specific RADIUS check and reply attributes are required for specific users, for example, to limit the number of simultaneous sessions using the Simultaneous-Use attribute or to check an AD group with the Active-Directory-Group attribute, create a User profile without the User-Password attribute and add the Authentication-Method attribute as a check item with the value 'Windows' or 'Active Directory' depending on domain type.

TekRADIUS does not check user dial-in privilege by default. You can enable it by adding Check-MS-DialinPrivilege = True as a check attribute to Default user group, proxy Windows user profile or TekRADIUS local group profile created for user's primary user group in Active Directory.

Select proxy method to be used. Select “None” to disable this feature.

Authentication Proxy Domain

Enter the Domain name of the Windows or Active Directory or specify Windows server name.

You can validate user Ethernet MAC address received in RADIUS authentication requests against msNPCallingStationID value in Active Directory for Active Directory users. You can assign static IP addresses and IP routes to Active Directory users by settings msRADIUSFramedIPAddress and msRADIUSFramedRoute Active Directory attributes respectively.

msNPCallingStationID, msRADIUSFramedIPAddress and msRADIUSFramedRoute attribute support requires a commercial license.

By default, TekRADIUS runs as the Local System account. This is generally regarded as the best practice for Windows services. The Local System account should have access to query the AD *(read-only access)* in most default domain environments. Some further configurations may be required if the server is not a member of the domain *(maybe in another domain)* or the AD environment has been locked down from defaults. The solution is to elevate the privileges used to run the TekRADIUS service. This is done under

Control Panel → Admin Tools → Services

Select the TekRADIUS service, then the Logon tab. Change the service account to an account that has both Local Administrator rights and at least read access to the AD.

Keep Domain Name:

Check this option to prevent TekRADIUS from automatically removing characters before a ‘\’ character in a *User-Name* attribute received in access and accounting requests. The default action is for TekRADIUS to remove all characters before a ‘\’ character.

Default EAP Method

You can select the default EAP method. The default EAP authentication method is PEAP-EAP-MS-CHAP v2.

EAP Server Timeout

Indicates how many seconds TekRADIUS waits for a RADIUS response from the client. TekRADIUS aborts EAP sessions and clear cached data for the session when this timer expires.

Enable TLS Session Resumption

Enables RFC 5077 *(Stateless)* based TLS session resumption. This also enables PEAP fast reconnect.

Session Ticket Encryption Key Lifetime

Specify lifetime duration for the encryption key to encrypt issued session tickets in hours.

Require Local Certificate for EAP-TLS

TekRADIUS accept all client submitted valid certificates for client authentication in EAP authentication sessions. Clients can be authenticated only when the client certificates match the ones specified in the user profiles when this option is enabled.

Add User-Name to Access-Accept Messages

Check this option to force TekRADIUS to automatically add the *User-Name* attribute to RADIUS *Access-Accept* replies.

Failure Count

TekRADIUS can disable a user profile after a number of unsuccessful login attempts. Set the Failure Count to the number of allowed unsuccessful login attempts before the User profile is disabled. Entering 0 disables this feature.

If Mail Alerting is enabled, notification will be sent when a user profile is automatically disabled.

Send Failure Cause

Check this option to force TekRADIUS to add the failure cause to *Access-Reject* replies using the IETF *Reply-Message (18)*. You can localize messages to be sent. TekRADIUS keeps failure messages under Dictionary Editor / Vendors (ietf) / Attribute (Acct-Terminate-Cause). Please also see "Failure Codes in Accounting Table DisconnectCause Field when Save Authentication Failures Option Set" section.

Use Default Authentication Query

Uncheck this box to specify an alternative query to select the authentication attributes from the Users Table to be checked against the attributes received from the access server.

Authentication Query

If the *Use Def. Authorization Query* option is unchecked, enter the alternative query. Always use ***AttrType=0*** to get check attributes. Query syntax is automatically checked.

By default, to fetch the ***check*** attributes from the Users Table, TekRADIUS uses:

```
Select Attribute, Val from <users_table> where UserName='%ietf|1%' and AttrType=0
```

Please see Using Alternative Authentication and Authorization Queries section for more details.

Use Default Authorization Query

Uncheck this box to specify an alternative query to select the authorization parameters from the Users Table to be returned to the access server.

Authorization Query

If the *Use Def. Authorization Query* option is unchecked, enter the alternative query. Always use ***AttrType=1*** to get success-reply attributes. Query syntax is automatically checked.

By default, to fetch the ***success-reply*** attributes from the Users Table, TekRADIUS uses:

```
Select Attribute, Val from <users_table> where UserName='% ietf|1%' and AttrType=1
```

Use Regular Expression Match

Check this box to match string type attributes in incoming RADIUS Access-Requests with the check attributes defined in user or group profiles using regular expressions. This feature is available only in commercial editions.

Cache User/Group Attributes.

TekRADIUS can cache configured check / reply attributes for user and group profiles as the authentication requests are received. TekRADIUS will not perform database queries when cached attributes found for an incoming RADIUS authentication request. This can significantly reduce the load on the database. This feature is enabled by default. TekRADIUS will automatically clear cached entries when the related user or group profile is altered through TekRADIUS Manager, TekRADIUS HTTP interface or TRCLI. You can also clear the whole attribute cache through the TekRADIUS Manager / Service / Clear Cached Attributes menu. You should disable attribute caching if you add / modify user or group profiles by accessing the database directly.

Parameters / Accounting

Enable RADIUS Accounting

Check this box to enable the collection and processing of accounting packets from RADIUS clients.

When an *Accounting-Checkpoint* message is received for a previously unknown session, this checkpoint message is assumed to be an accounting session start *(an entry will also be added in the Sessions Table)*.

When an *Accounting-Stop* message is received for an already stopped session and the previously received *Accounting-Stop* of the session has no *Acct-Session-Time* attribute *(Acct-Session-Time=NULL),* the session's stored stop record is updated by the newly received one.

When an *Accounting-Off* message is received from a RADIUS client, all active sessions with that RADIUS client will be stopped with *Acct-Session-Time=NULL* and the session entries will be cleared in the Sessions Table.

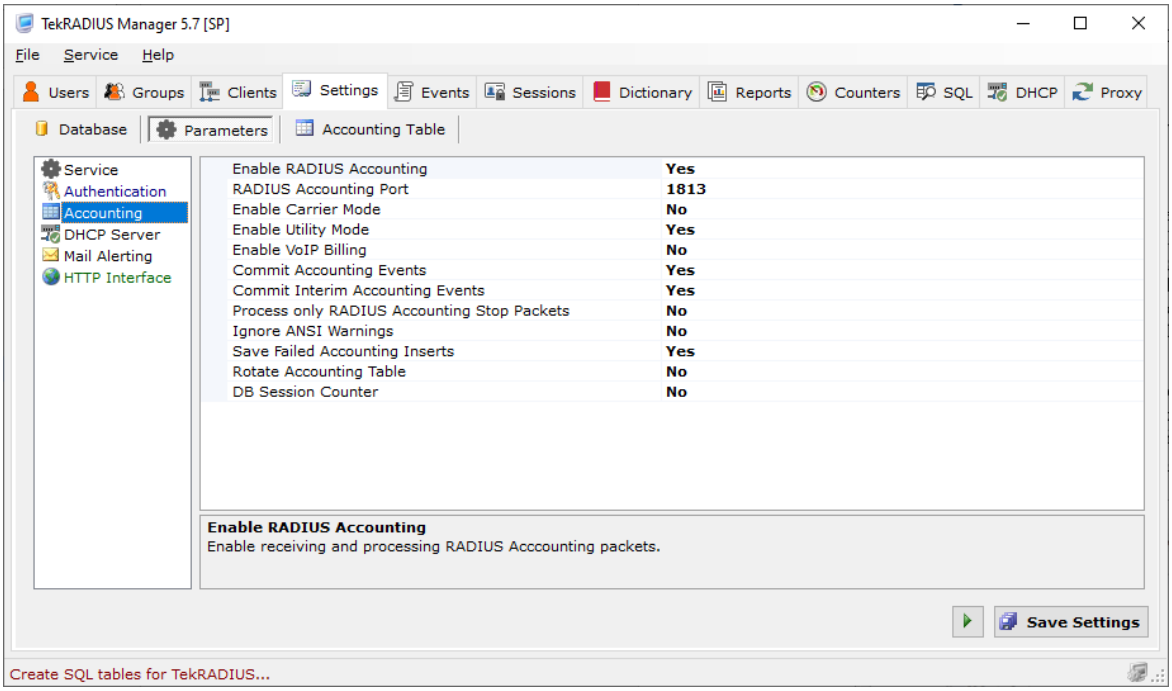


Figure 7. - Service Parameters – Accounting

RADIUS Accounting Port

Enter the UDP RADIUS accounting port between 1- 65535; if no value is entered, the default port of 1813 will be used.

If the port number entered is the same as that used by authentication, accounting will be disabled. If the selected port is used by another program, TekRADIUS will disable the RADIUS Accounting thread and add the following event entry to Windows Event Log: *"Unable to initialize TekRADIUS Accounting thread"*.

If TekRADIUS cannot initialize either the Authentication or Accounting threads, execution of the startup sequence is halted and adds the following event entry to Windows Event Log: *"Could not start any of TekRADIUS threads; exiting..."*

VOIP Billing Enabled

Please see TekRADIUS Rate Editor Manual for details.

Ignore ANSI Warnings

Large attribute values in accounting packets may cause truncation errors. Check this option to force SQL Server to ignore these truncation errors.

Save Failed Accounting Inserts

Check this option to save failed accounting table updates into a daily rotated file which can be found under Log sub directory under TekRADIUS application directory.

Save Authentication Failures *(SP Edition only)*

Check this option to save failed authentication attempts into accounting table. Failure records inserted with StatusType field set to Failure. You can query and list these records through Reports tab.

Commit Interim Accounting Event

You need to keep individual accounting updates *(Checkpoint packets)* for the active sessions for high resolution usage reporting. TekRADIUS converts received accounting updates to stop packets and updates the last accounting stop record with the received accounting checkpoint to stop packets to keep disk usage minimal. You may not see correct usage when you execute reports for long duration sessions with short reporting periods. Set this option to see high resolution reports if you have long duration accounting sessions.

Rotate Accounting Table

You can have a monthly rotated accounting table. TekRADIUS creates accounting tables for each month when this option is enabled. TekRADIUS adds "_YYYYMM" *(Accounting table for May will be Accounting_202205 e.g.)* suffix for monthly created tables. TekRADIUS clones the original accounting table with its existing indexes and constraints while creating a monthly table. Please note that reporting will be performed on the active table when monthly rotation is enabled. Records in the previous tables will be discarded while reporting queries are executed. You can query older accounting tables through the SQL tab.

DB Session Counter:

Check this option to use multiple instances of TekRADIUS with the same database. By default, TekRADIUS stores simultaneous session counters in memory; however, enabling this option forces the session counters to be stored in the database. You must enable this option if you have a secondary TekRADIUS server for backup purposes.

Parameters / DHCP Server

Enable DHCP Server

Check this option to enable the TekRADIUS built-in DHCP server. The DHCP server automatically assigns IP addresses to all wired or wireless devices from pools of IP Addresses defined Pools in the **DHCP** tab.

A unique feature of the TekRADIUS DHCP server is that it allows IP addresses to be assigned to wireless clients based on the usernames entered in PEAP/EAP authentication and not solely on the client MAC addresses.

! *The IP address assignment based usernames is available only in commercial editions of TekRADIUS.*

Enable DHCP Lease History

Check this option to enable TekRADIUS to keep records of assigned IP addresses.

Parameters / Cipher Suites

You can specify allowed cipher suites in the TLS sessions established for EAP authentication. You must enable at least one cipher suite for TLS <= 1.2 and you must enable TLS_AES_128_GCM_SHA256 or TLS_AES_128_GCM_SHA384 for TLS 1.3

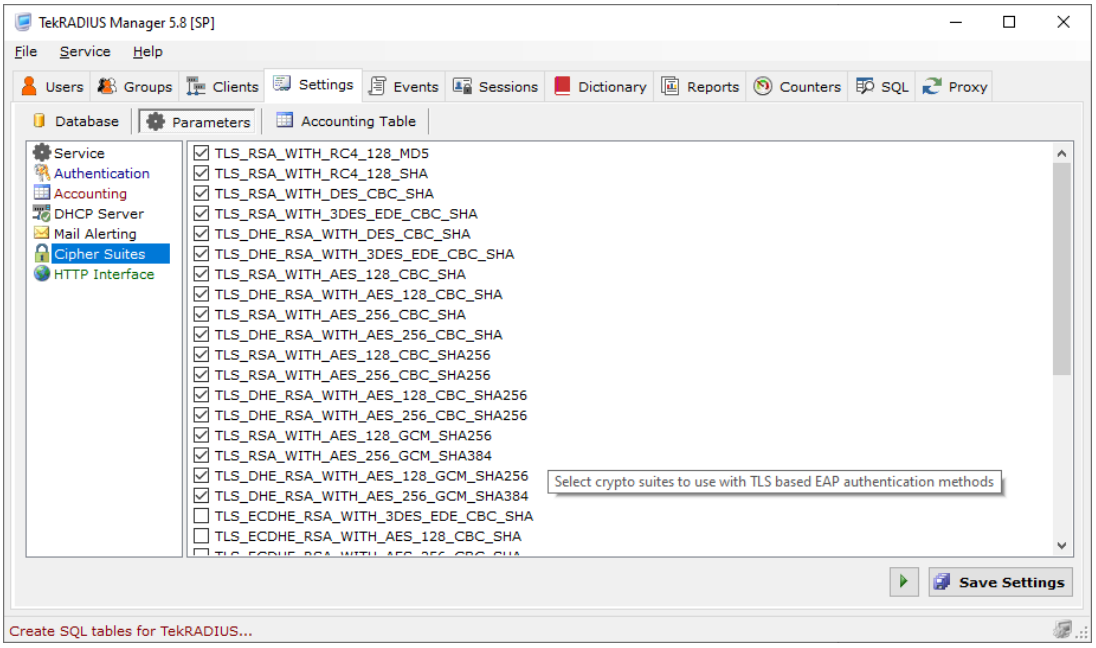


Figure 8. - Service Parameters – Accounting

Parameters / Mail Alerting

TekRADIUS can be configured to send e-mail alerts if an error condition occurs for a specified duration.[2]

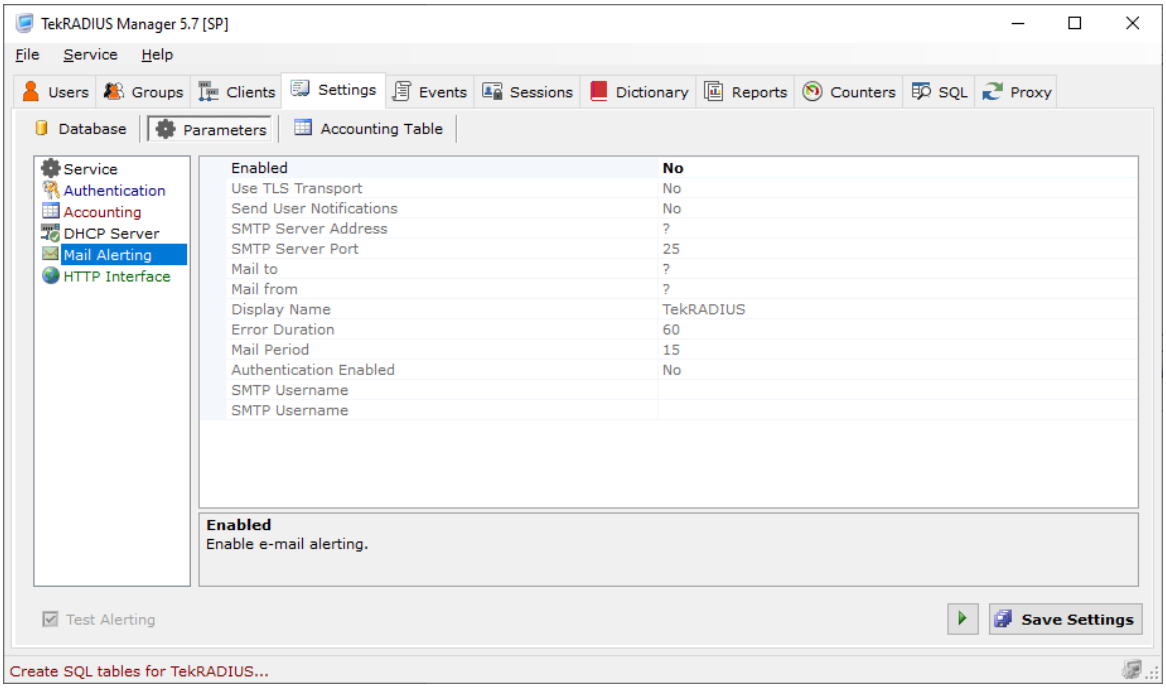


Figure 9 - Alerting Configuration

Enter the following information to configure alerting:

Mail Alerting Enabled

Check this option to enable the Mail Alerting feature.

SMTP Server

Enter the IP address or FQDN of the SMTP server.

Mail To

Enter the e-mail address to which alerts are to be sent.

Mail From

Enter the e-mail address that will be shown as the sender email address.

Authentication Required

Check this option if the SMTP server requires user authentication.

SMTP Username

If 'Authentication Required' has been checked, enter the SMTP username.

Password

If 'Authentication Required' has been checked, enter the password of the SMTP user.

[2] Please set SMTP port as 587, go to https://myaccount.google.com/lesssecureapps and set Allow less secure apps: ON if you prefer to use a Gmail account.

Error Duration

Enter the minimum error duration *(in seconds)* before sending an e-mail alert *(Default: 60 seconds)*.

Mail Period

Enter the minimum duration *(in minutes)* before sending the next e-mail alert *(Default: 15 minutes)*.

Send User Notifications

TekRADIUS notify users via email when followed event occur:

- Low user credit (2000)
- When user consumes all configured credit (2001)
- Account lockout due to incorrect password entry (2002)
- When user's password is changed (2003)
- When password is needed to be changed in 7 days *(When password aging is enabled for the user)* (2004)
- When password is needed to be changed in 24 hours *(When password aging is enabled for the user)* (2005)

Notification email is sent to the email address added to the user profile with Email-Address *(Check)* attribute. This option requires Enterprise license.

You can customize sent messages by edition relevant values in TekRADIUS Dictionary. Local vendor "ietf" and attribute "Acct-Terminate-Cause" and edit values 2000-2005

Click **Test Alerting** to test the E-Mail Alerting configuration. If the configuration is valid, a test message will be sent by TekRADIUS to the 'Mail To' email address.

TekRADIUS will send notifications via e-mail when system errors *(Such as database connection failures)*, startup and shutdown events occur for a specified duration. TekRADIUS sends also a warning message when a user account is locked due to number of failed authentications attempts if **Settings / Service Parameters / Failure Count** value is set to a value greater than zero.

Parameters / HTTP Interface

HTTP Interface Enabled, Port

Check this option to enable the TekRADIUS HTTP interface. Refer to the 'HTTP Reporting Interface' section of this manual for more details.

Use TLS Transport

You can secure HTTP connections using TLS transport. Server Certificate set in Authentication parameters will be used for as server certificate.

Mutual TLS Authentication

TekRADIUS requires clients to submit a valid certificate for client authentication in the TLS negotiation when it's enabled.

Trusted CAs

You can specify allowed Certificate Authorities for client certificates when mutual authentication is enabled. All valid CAs *(The ones in Windows Certificate Store / Local Machine / Trusted Root Certification Authorities folder)* are trusted by default.

Session Timeout

If the HTTP Interface is enabled, select the timeout before a user session expires. Once an HTTP session has expired, the user will need to re-logon to gain HTTP access.

Enable REST API

Allows you to access HTTP REST API to perform various user/group/client management operations. Please see HTTP REST API reference document at TekRADIUS support site.[3]

Clients

RADIUS clients are defined in the **Clients** tab. RADIUS client data is stored the 'Clients Table' in the TekRADIUS.db file, under the installation directory. When RADIUS client information is added, edited or deleted, the changes will be immediately written to the 'Clients Table'.

To add a new RADIUS client, enter the following settings and click **Add/Update** *(+)*; to alter settings of an existing RADIUS client, select the client from the table and make the required changes to the following settings and click **Add/Update**. Similarly, to delete an existing RADIUS client entry, select the required client from the table and click the **Delete** *(X)* button.

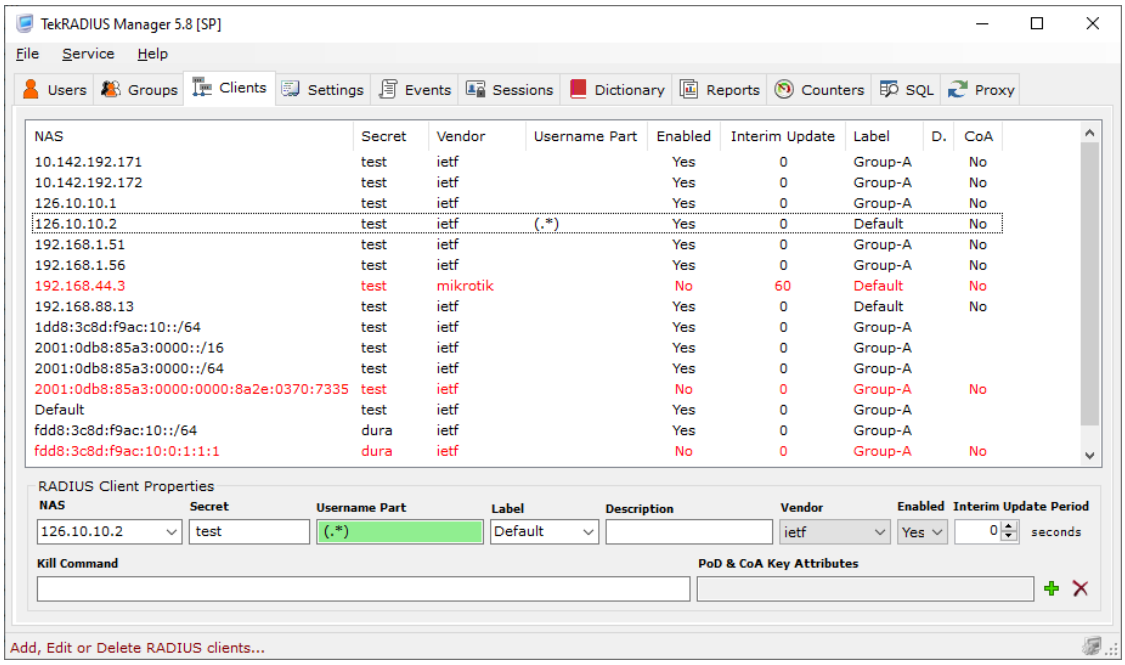


Figure 10 - RADIUS Clients

NAS

Select an existing NAS or enter the IP address of a new RADIUS client. You can also specify a subnet like 192.168.1.0/24. The SP edition of TekRADIUS can accept FQDN names, which are automatically queried every 60 seconds for IP address changes, enabling this feature to be used with dynamic DNS services.

! *Only the SP edition of TekRADIUS can accept alphanumeric domain names as RADIUS client entries.*

[3] https://www.kaplansoft.com/TekRADIUS/Docs/RESTAPI.pdf

Secret

Enter the shared secret for the RADIUS client. The secret cannot be left blank.

Username Part

Enter a regular expression to specify username portion for a received username in User-Name attribute from this RADIUS client. Start always with (^) and end with ($). TekRADIUS will take seconds group of regular expression as username. Matching is performed in case insensitive. Left blank if you do not use this option. Samples;

Regular Expression	Input	Result
`(^.+\\)([a-z]+)($)`	`Domain\user`	`user`
`(^)([a-z]+)(@.+$)`	`user@Domain`	`user`

Label

You can set a group label for client entries. You can specify assigned group label as a check attribute by adding Client-Label attribute as a check attribute to user or group profiles. This will enable you to restrict user authentication attempts from a specific group of NAS devices. *TekRADIUS will set Client-Label attribute in user and group profiles to default client group when a client group is deleted.*

Vendor

Select the vendor of the RADIUS client. If the vendor is not known, or is not listed, select 'ietf' as the Vendor.

Enabled

To temporarily disable a RADIUS client, select 'No' from the drop-down list. The default value is 'Yes'.

Interim Update Period

If the RADIUS client supports sending Interim Accounting Messages, the 'Interim Update Period' may be set to force TekRADIUS to clear any associated active sessions and simultaneous session entries if an update is not received in the period specified. The minimum allowed value for interim update period is 60 seconds.

Setting interim update period to 0 disables interim update period checking for the selected RADIUS client. The default setting is '0'.

IP Pool Group

You can specify an IP pool group name for each client when DHCP server is enabled. IP address assignments are made from specified IP pool group for the requests coming from the client.

! *A default RADIUS client entry may be created in version 2.5 onwards to enable TekRADIUS to accept a RADIUS request from unlisted RADIUS clients with the correct shared key.*

A 'Kill' command can be defined to drop user sessions through the **Active Sessions** tab if the host supports a command line utility to send an appropriate signal to disconnect a particular user session.

The following variables can be used as parameters with the "Kill" command;

```
$NASIPAddress
$SessID
$UserName
$NasPort
$NasPortId
$Calling-Station-Id
```

Some NAS devices support SNMP MIBs that can be used to disconnect users. In this case it is possible to use the command line 'SNMP set' utility to disconnect users. Please consult your NAS documentation to find out whether the NAS supports this function and which MIB to use.

This is an example to clear TTY sessions on a Cisco device:

```
c:\util\snmpset $NASIPAddress public .1.3.6.1.4.1.9.2.9.10.0 integer $NasPort
```

It is also possible to use other types of utilities that are supported by your access server.

TekRADIUS checks if the added client supports RADIS CoA automatically and this is indicated in the CoA column of clients list.

Groups

Groups are defined in the **Groups** tab. Group profiles are used for common RADIUS attributes associated with a group of users. The Default user Group is added automatically when the database tables are created. The Default user Group cannot be deleted as is required by TekRADIUS for proper operation.

If RegExp Matching is enabled in **Settings / SQL Connection**, Regular Expressions may be specified to match patterns in Check type attributes

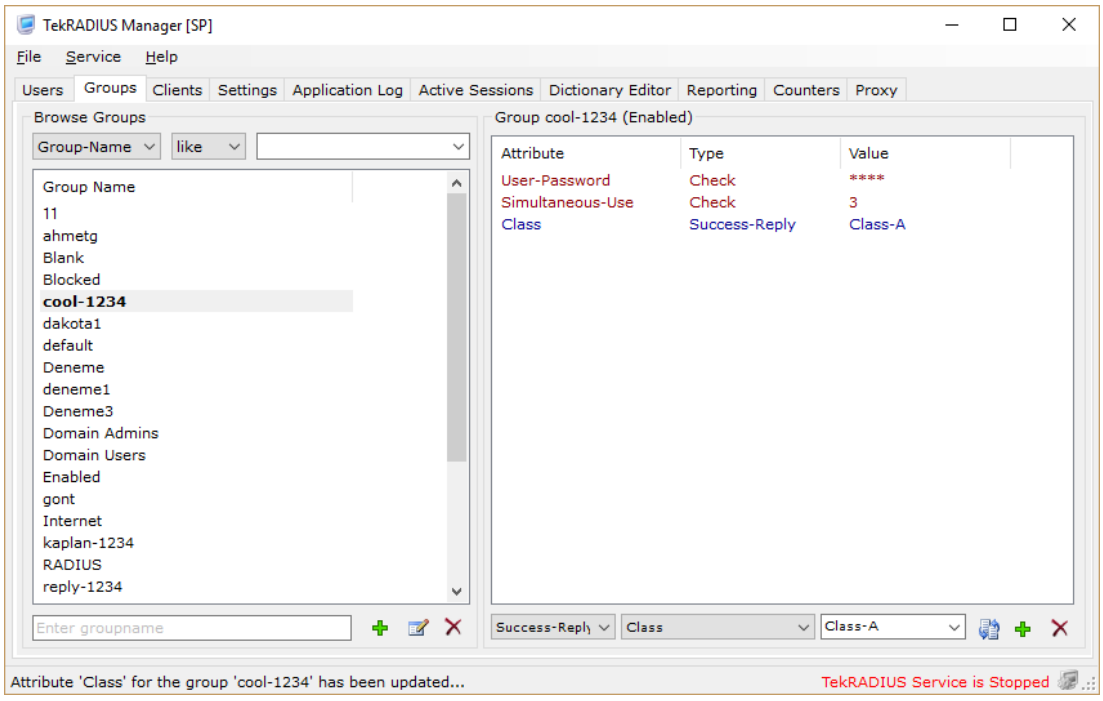


Figure 11 - Groups Tab

New Group profiles are defined and attributes assigned in the **Groups** tab. Existing Groups may be modified or deleted; and the entire Groups Table may be searched to locate any existing Group.

To add a new Group:

1. Enter a non-blank group name in the 'Group:' text box *(Bottom left),*
2. Click the **Add** icon.

To modify an existing Group's name or its attributes:

1. Select the existing Group,
2. Makes any changes to its name or its attributes (see below),
3. Click the **Modify** icon.

To delete an existing Group:

1. Select the required Group,
2. Click the **Delete** icon.

! *The Default Group can neither be modified nor deleted.*

! *If a group is deleted, the Users associated with that group are moved automatically to the Default group.*

To search for a particular group:

1. Enter the first letters of the group name in the Browse Groups window *(if the search box is left blank, all groups will be retrieved)*,
2. Click the **Search** icon.

Matching group names will be listed in the group list box. It is also possible to search for a specific attribute and its value in the group profiles.

"Check" and "reply" attributes may be added or deleted for a user Group.

To add an attribute to a Group:

1. Select the required attribute from the entry fields,
2. Click the **Add/Update** icon.

To delete an existing attribute from a Group:

1. Select the Group and attribute,
2. Click the **Delete** icon.

Attribute:

1. Select the attribute type (*Check* or *Reply*) from the first dropdown list,
2. Select the attribute name from the second dropdown list,
3. Select the attribute value from the third dropdown list or manually type in the value as appropriate.

To restrict access to unauthenticated users, add *Failure-Reply* attributes to the user or group profiles. TekRADIUS will reply with an *Access-Accept* message containing the *Failure-Reply* attributes if that User or Group profile has *Failure-Reply* attributes defined when the authentication fails; if the User or Group profile does not have any *Failure-Reply* attributes, TekRADIUS will reply with an *Access-Reject* message.

! *This feature is not available for PEAP authentication, VPN authentication or when the authentication failure is caused by an invalid authentication method.*

! *Use this feature with extreme care. If the Default user group has Failure-Reply attributes, all failed authentication attempts will be replied with Access-Reject messages containing the Failure-Reply attributes. When a user is authorized with Failure-Reply, TekRADIUS will NOT check the Simultaneous-Use, Simultaneous-Group-Use, Expire-Date, Login-Time, TekRADIUS-Status nor Quota parameters.*

! *To send Failure-Reply attributes in an Access-Accept message, add the Failure-Reply-Type attribute as a check attribute to the user or group profile with value of 'Accept'.*

Check items will be listed in dark red, *success-reply* items will be listed in dark blue and *failure-reply* items will be listed in turquoise.

If an attempt is made to add a previously defined attribute, the previously defined attribute will be updated with the parameters of the new one.

Hexadecimal strings should be entered with the 0x prefix *(for example, enter 0x54656B524144495553 for the string 'TekRADIUS')*.

Multiple "check" and "reply" attributes may be added to a user profile by separating the values with the delimiter character *(Default is semicolon ";")* can be set at Settings / DB Connection. Multiple value entries are supported only for string and IP address type attributes for RADIUS authentication. It is also possible to have multiple entries for IP address type DHCP reply attributes.

TekRADIUS will convert delimiter character into NULL character *(0x00)* while sending RADIUS replies when multiple rules specified for NAS-Filter-Rule *(RFC 4849)* attribute.

You can specify individual tags for the attributes which require tags such as tunnel attributes or ERX-Service-Activate. You can add numerical tag prefix to the value like 2:123.

You can create groups with the same name in Active Directory when you enable Windows or Active Directory Authentication proxies in Settings / Service Parameters. This will enable you to have check and reply attributes for a specific Active Directory group. TekRADIUS looks for a local group profile with the same name as the AD user's primary group name when an authentication request is received for an AD user. TekRADIUS falls back to default local user group if such a local group profile cannot be found. You can set user's primary group using Active Directory User & Group Manager application *(ADGUM.exe)* comes with TekRADIUS installation.

Informational type attributes may be added to User or Group profiles. Additional 'vendors' may be added to the TekRADIUS dictionary to store User or Group specific data, such as addresses and phone numbers. Informational type attributes, displayed in dark green, are not used while authenticating or authorizing users.

You can synchronize group attribute changes with the active sessions of users of the group by sending a Change of Authorization *(CoA)* request if your access servers support it *(SP edition only)*. CoA button  will be enabled automatically when you edit reply attributes. TekRADIUS will not add attributes that already exist in user profiles while sending a CoA request.

TekRADIUS will also ask you if you would you like to disconnect active sessions of users of the group when you delete a group profile *(SP edition only)*. TekRADIUS will send a Disconnect Request to your access servers to disconnect active sessions of users of the deleted group.

! *User attributes override Group attributes!*

Users

In the **Users** tab, new Users may be defined, added to existing Groups and attributes assigned; existing Users may be modified or deleted; and the entire Users Table may be searched to locate any existing Users.

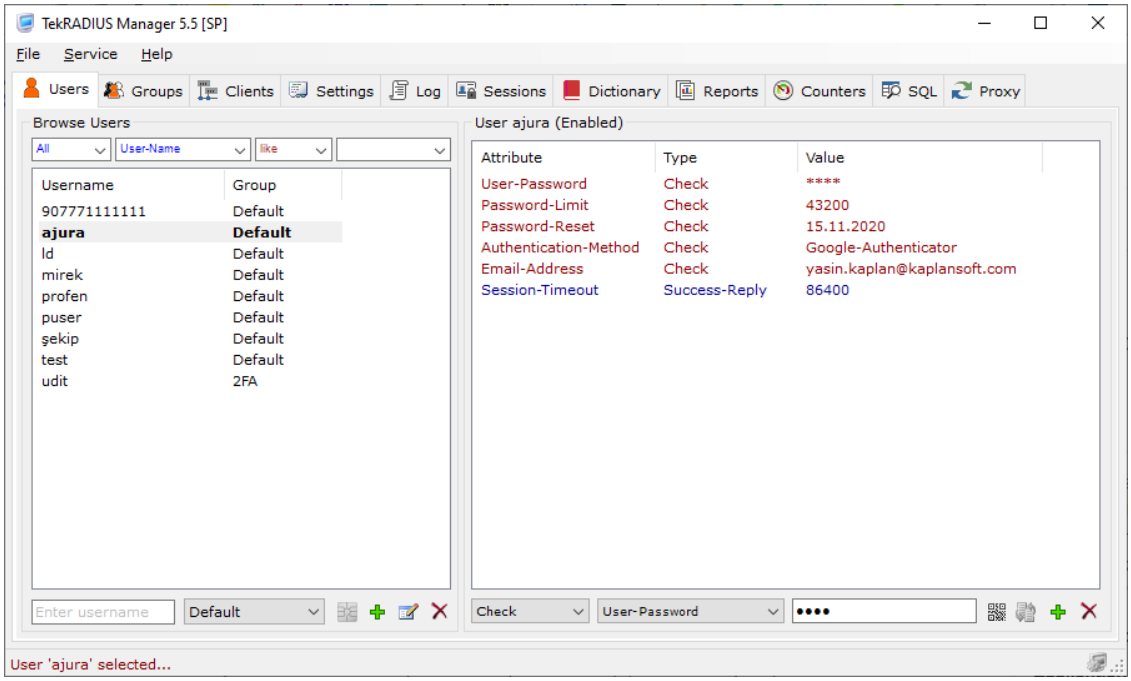


Figure 12 - Users Tab

To add a new User:

1. Enter a username in the user text field (*bottom left*),
2. Select the user Group,
3. Click the **Add** icon.

Follow the instructions in the 'Groups' section above for instructions on how to search for, modify or delete Users.

The *User-Password* attribute is stored encrypted in the Users and Groups tables.

A default User profile may be defined and will be used when an incoming RADIUS authentication request does not match any of the existing User profiles. If Windows Authentication Proxy *(WAP)* or Active Directory Proxy *(ADP)* is enabled, TekRADIUS will try to authenticate the user against WAP and then ADP, and finally, if a 'Default' User profile exists, it will be checked against the 'Default' User profile. *Simultaneous-Use* and *First-Logon* attributes have no function in the 'Default' User profile. The username 'Default' is reserved for the default User profile.

Attributes defined in User profiles have precedence over those defined in Group profiles. If the same attributes are defined in both a User and associated Group profile, the attribute in the User profile will be preferred. Only one instance of an attribute in check or reply attributes can be used.

Click the Import SIM Triplets button to import SIM triplets from the SIM card inserted in the smart card reader. The use of a smart card reader can be selected through **Settings / Service Parameters**.

You can synchronize user attribute changes with the active sessions of the user by sending a Change of Authorization *(CoA)* request if your access servers support it *(SP edition only)*. CoA button will be enabled automatically when you edit reply attributes.

TekRADIUS will also ask you if you would you like to disconnect active sessions of the user when you delete a user profile *(SP edition only)*. TekRADIUS will send a Disconnect Request to your access servers to disconnect active sessions of the delete user.

You can send Google Authenticator key to the user's email address if it is added using Email-Address *(Check)* attribute by clicking button. This option is available with SP license. You must set SMTP server parameters in Settings / Alerting to send email messages. You can also use TRCLI.exe to send Google Authenticator key to user's email address.

Dynamic IP Address Assignment

Commercial editions of TekRADIUS support dynamic IP address assignments for the users. You must enable a built-in DHCP server and create at least one IP pool. You need to add Framed-IP-Address = Select-by-TekRADIUS as a reply attribute to user or group profiles. You can add the following attributes to the user or group profile to control dynamic IP address assignment parameters;

- **Session-Timeout.** TekRADIUS allocates IP addresses for the user for 24 hours. You can increase or decrease lease time by adding Session-Timeout as a reply attribute to the user or group profile.

- **DHCP-IP-Pool.** TekRADIUS allocates IP addresses from the **Default** IP address pool by default. You can specify an alternative IP pool by adding the DHCP-IP-Pool attribute as a DHCP reply attribute to the user or group profile.

SP license enables you to acquire an IP address from a DHCP server when you set Framed-IP-Address = Acquire-Using-DHCP. You can specify a DHCP server by adding DHCP-Server attribute to the user or group profile.

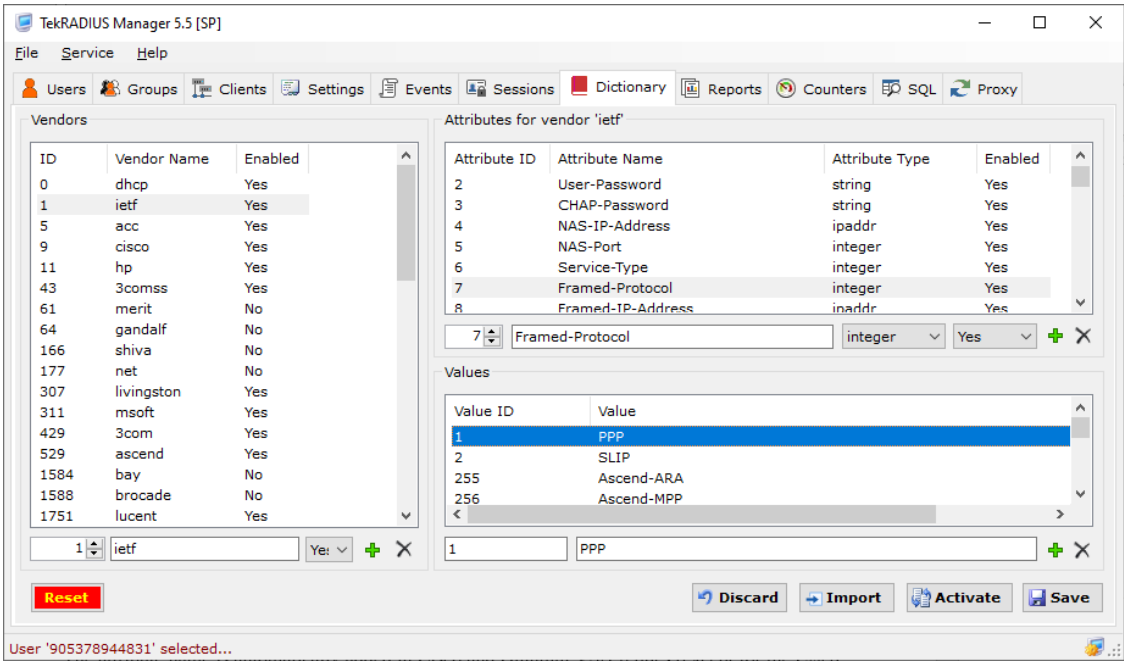


Figure 13 - Dictionary Editor

TekRADIUS expects a RADIUS accounting start packet with a Framed-IP-Address attribute set for the assigned IP address. TekRADIUS checks the DHCP IP binding table every 15 seconds and clears static binding entries if there is not an associated active session for the assigned IP address.

Dictionary Editor

RADIUS dictionary entries can be edited using the **Dictionary Editor** tab. RADIUS dictionary entries *(Vendors, Attributes and Values)* and client definitions are stored in TekRADIUS.db, which can be found in the application directory.

The Dictionary consists of Vendors, Attributes and Values tables. If a valid entry for a vendor could not be found because a vendor or an attribute has been deleted or disabled, VSAs from that vendor are ignored when authenticating the user. Also, reply attributes configured for a vendor are not sent to the NAS if there is no entry for that vendor in the TekRADIUS.db/Vendors table.

The attribute name is automatically added in Cisco and Quintum VSA replies (except for the *Cisco-AVPair* attribute). For example, the *Quintum-h323-preferred-lang* reply attribute will be sent as *Quintum-h323-preferred-lang = H323-preferred-lang=TR*.

Attributes in received RADIUS packets that are not in the dictionary are ignored. If there are duplicate attributes in request packets, only the first attribute is processed, except for Cisco and Quintum AVPs *(Cisco & Quintum VSA 1)*. To optimize performance, disable unnecessary vendors.

Text based dictionary files may be imported by clicking the import button. An example of a text-based dictionary file is shown below;

```
VENDOR          Netscreen                       3224

BEGIN-VENDOR    Netscreen

ATTRIBUTE       NS-Admin-Privilege                              1       integer
ATTRIBUTE       NS-VSYS-Name                                    2       string
ATTRIBUTE       NS-User-Group                                   3       string
ATTRIBUTE       NS-Primary-DNS                                  4       ipaddr
```

```
ATTRIBUTE       NS-Secondary-DNS                        5       ipaddr
ATTRIBUTE       NS-Primary-WINS                         6       ipaddr
ATTRIBUTE       NS-Secondary-WINS                       7       ipaddr

ATTRIBUTE       NS-NSM-User-Domain-Name                 220     string
ATTRIBUTE       NS-NSM-User-Role-Mapping                221     string

VALUE   NS-Admin-Privilege          Root-Admin              1
VALUE   NS-Admin-Privilege          All-VSYS-Root-Admin     2
VALUE   NS-Admin-Privilege          VSYS-Admin              3
VALUE   NS-Admin-Privilege          Read-Only-Admin         4
VALUE   NS-Admin-Privilege          Read-Only-VSYS-Admin    5

END-VENDOR      Netscreen
```

You can drag and drop dictionary files to Dictionary tab to import vendor dictionaries. You can revert your dictionary to factory default by clicking the Reset button. You can also click the reset button to have the most updated RADIUS dictionary that comes with the new version of TekRADIUS. Every new release of TekRADIUS may have RADIUS dictionary updates. TekRADIUS will preserve existing RADIUS dictionary file If you install TekRADIUS on to an existing installation. You can update the existing dictionary file by clicking the Reset button at left bottom of the Dictionary tab of TekRADIUS Manager.

SQL Query Executioner

You can execute SQL queries directly on TekRADIUS database through SQL tab. You can save query results in CSV format, print or send them as an e-mail attachment to the e-mail address specified in Mail Alerting settings.

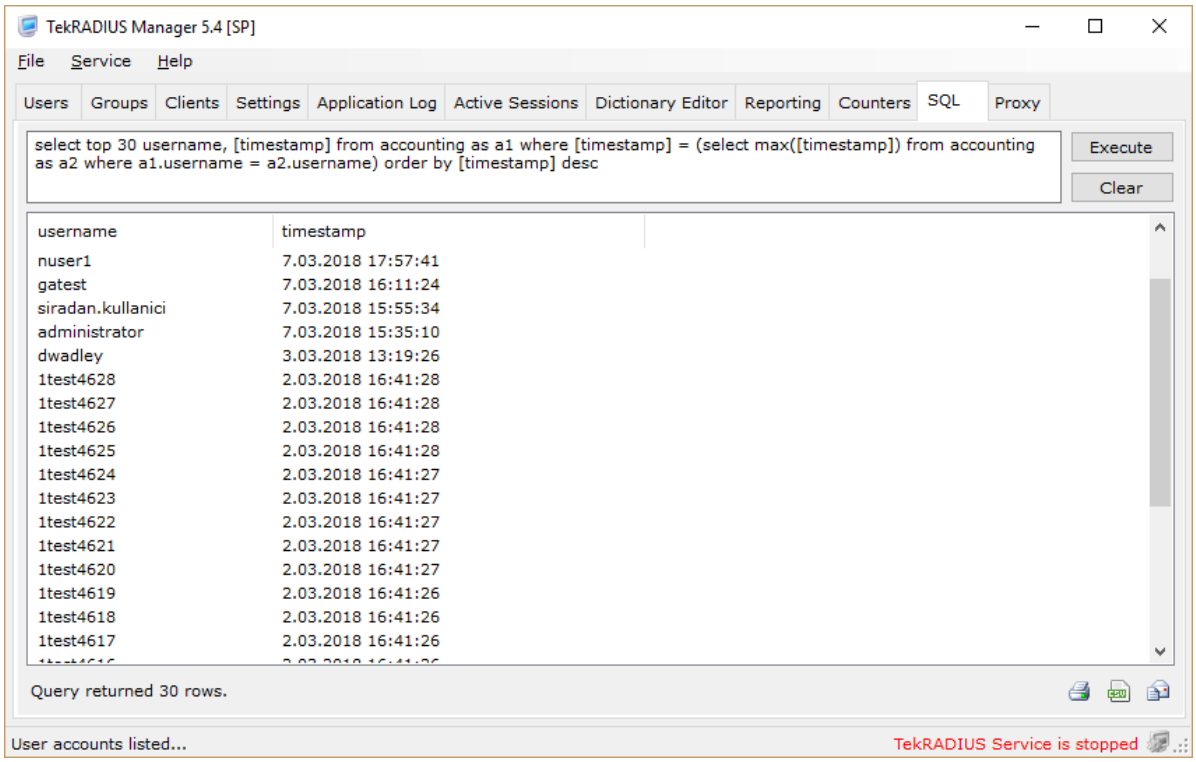


Figure 14 - SQL Query Executioner

You can run queries by clicking Execute button or typing F5, F9 or CTLR + Enter.

Reporting

TekRADIUS provides a simple interface for browsing RADIUS Accounting records stored in the accounting table and accessed via the **Reporting** tab. Reports can be generated for a selected User, or all users in a Group, for a specified interval of dates.

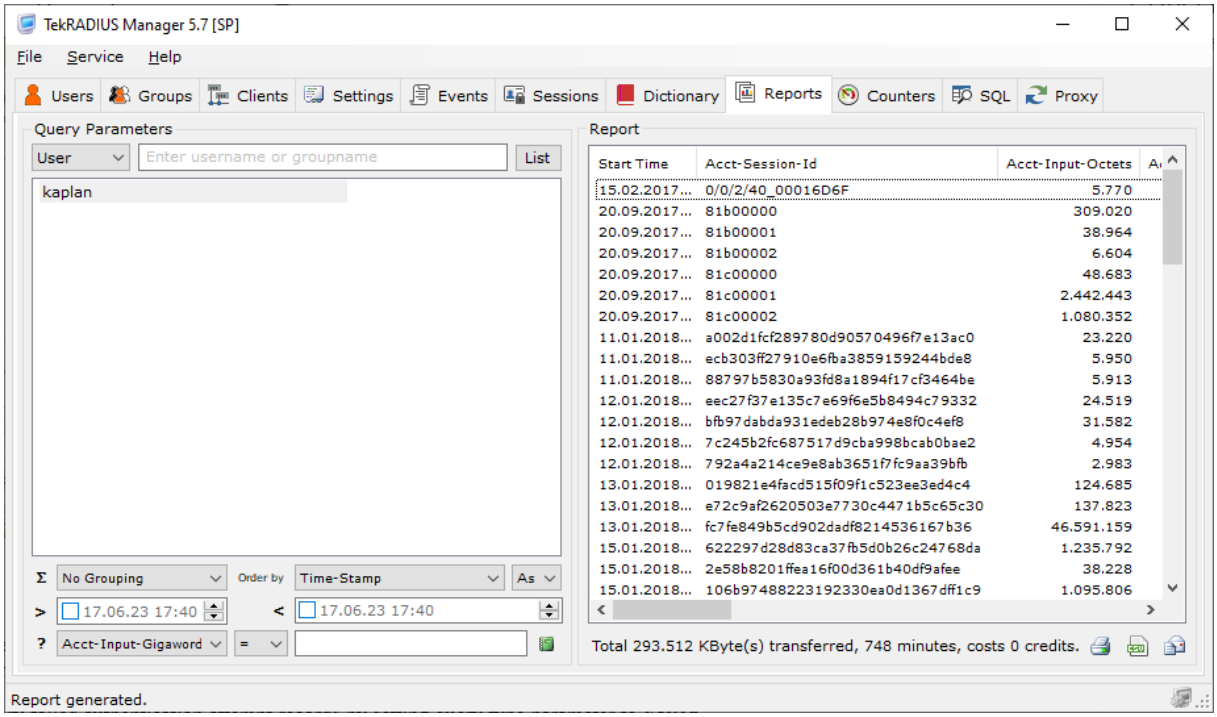


Figure 15 - Reporting Tab

To select a User or Group, enter the first letters of the Username or Group name and click the **List** button. If the Query parameter box is left blank, all users in the TekRADIUS database will be listed if 'User' has been selected; and all groups will be listed if 'Group' has been selected.

You can also query failed authentication attempt records by setting query type parameter to **Failed**. You will get a user list with failed authentication attempts recorded in the accounting table when you click list button. Please make sure that you have enabled **Save Authentication Failures** option at Settings / SQL Connection tab for this feature *(SP Edition only)*.

Dates when accounting events occurred may be optionally selected. If no dates are specified, all session entries will be listed for the selected User(s). Click the **Report** icon to list the accounting entries. The results may be printed or saved as a CSV file.

TekRADIUS generates a user list from the the accounting table. You may not see all users listed when you select "All Users" since some users may not have accounting events in the accounting table.

DHCP Server

TekRADIUS has a built-in DHCP server to assign IP addresses to the wired or wireless devices on the network, and accessed via the **DHCP** tab. Within this tab, it is possible to define DHCP pools and monitor IP address usage and active DHCP assignments.

! *The **DHCP** tab is only available if the DHCP server has been enabled in the **Settings / Service Parameters** tab.*

Commercial editions of TekRADIUS provide a unique feature; the assignment of static IP addresses to wired/wireless clients with DHCP. Most Ethernet switches and WiFi Access Points do not support the assignment of a static IP address to clients based on their usernames, although they may support Ethernet MAC address-based reservation; however, TekRADIUS DHCP server can assign a static IP address to the user based on the username.

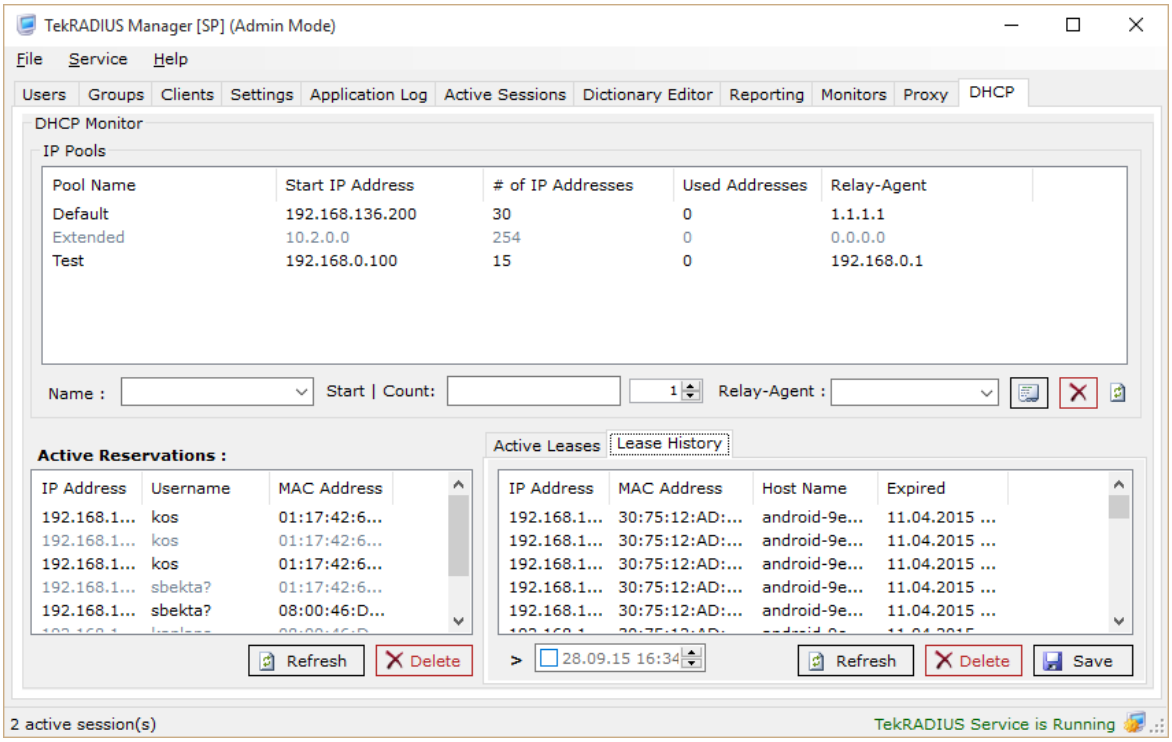


Figure 16 - DHCP Tab

It is necessary to define at least one DHCP pool named 'Default'. TekRADIUS will assign IP addresses from this pool if an individual DHCP profile is not found for the incoming DHCP request.

Individual profiles for users can be defined based on MAC addresses. IP addresses can be assigned from a DHCP IP Pool by adding DHCP-IP-Pool option or specifying a specific IP address by adding *Framed-IP-Address* as a *Success-Reply* attribute to DHCP profile.

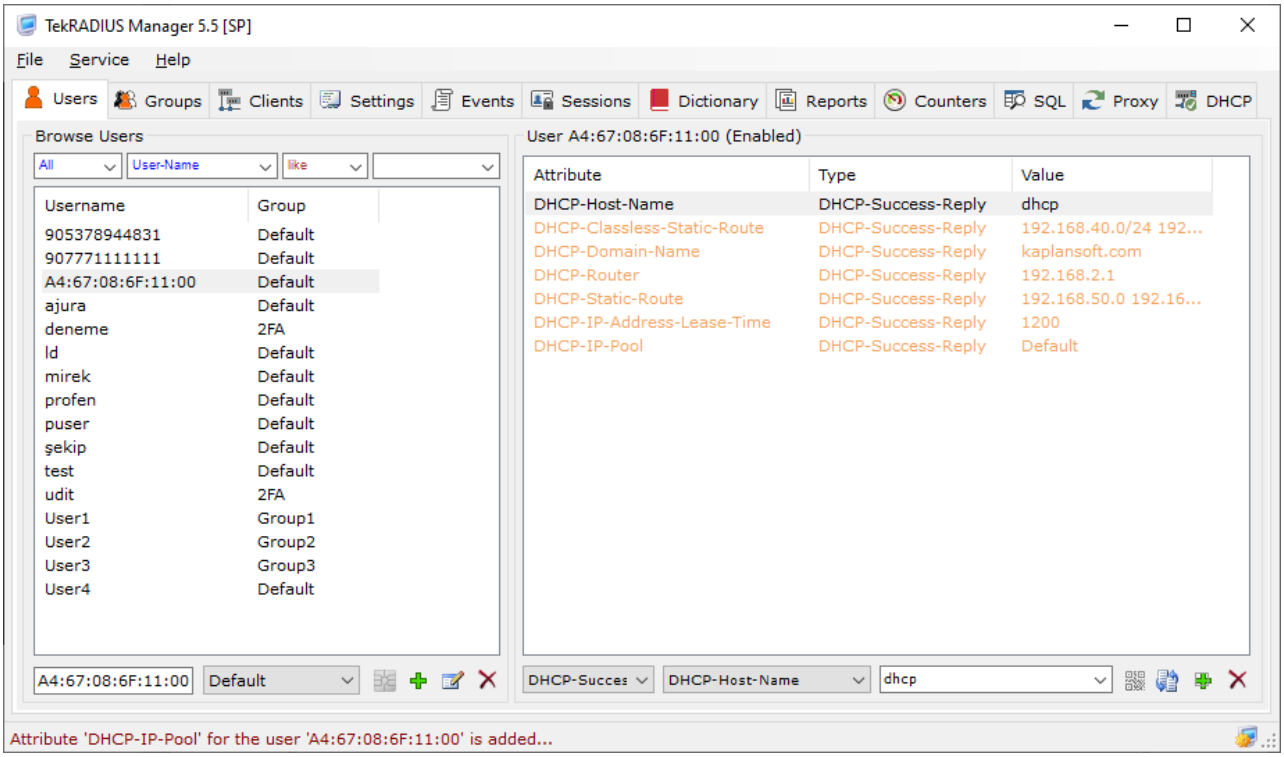


Figure 17 - DHCP Profile based on MAC Address

The commercial edition of TekRADIUS allows DHCP options to be added to the user profile.

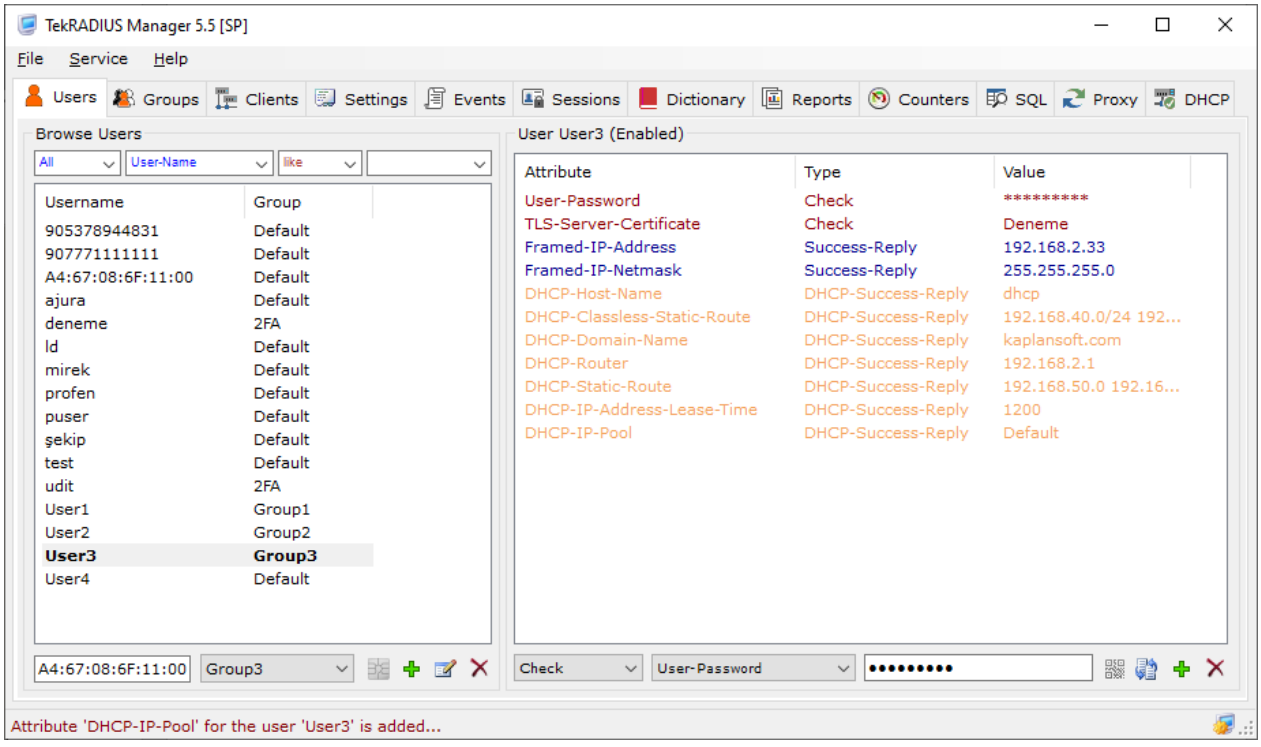


Figure 18 - User Profile with DHCP Options

The following RADIUS attributes are translated to DHCP options if they exist in User profiles;

RADIUS Attribute	DHCP Option
Framed-IP-Address	*DHCP-IP-Address*
Framed-IP-Netmask	*DHCP-Subnet-Mask*
Framed-Route	*DHCP-Classless-Static-Route*
Session-Timeout	*DHCP-IP-Address-Lease-Time*

DHCP-Classless-Static-Route value must be entered in the following CIDR format:

```
<Network>/<Network Bits> <Default Gateway>
```

Example:

```
192.168.0.0/24 192.168.0.1
```

If a DHCP IP pool of IP addresses is exhausted and Mail Alerting is enabled, TekRADIUS will send an e-mail notification.

A DHCP profile can be disabled by adding the *TekRADIUS-Status = Disabled (Check)* attribute.

A Relay-Agent IP address can be specified in order to distinguish the source network of the DHCP request and assign an IP address accordingly. This is especially useful when multiple VLANs exist within an Ethernet network. You can enter NAS-Identifier as Relay-Agent if Relay-Agent is also a RADIUS client and its IP address is variable. TekRADIUS will match IP Pool against NAS-Identifier in the Access-Request to reserve an IP address for the DHCP request from authenticated user.

Assigned IP addresses can be viewed in the Active Leases section. If static IP addresses are assigned to EAP authenticated users through DHCP, it is also possible to monitor the IP address reservations in the Active Reservations section.

TekRADIUS may choose different IP pools based on their available IP address count and some DHCP attributes must be specified based on the selected IP pool such as DHCP-Router and DHCP-Subnet-Mask. You can specify pool based attributes by creating a user profile with the same name as the IP pool name in the Users tab.

TekRADIUS Manager Menus

File Menu

Open Log File. This menu option opens daily rotated TekRADIUS log file which includes diagnostic output for RADIUS authentication and accounting event.

Clear Log File. This option clears the active log file.

Database

Backup. You can backup Users, Groups and Client tables. The backup file format is TekRADIUS proprietary. You can restore created backup file in other editions of TekRADIUS *(MS SQL, SQLite and ODBC)*.

Restore. This function enables you to restore previously created backup file.

Normalize MAC addresses. This menu option sets the format of all MAC addresses in TekRADIUS database to `11:22:33:AA:BB:CC` format.

Import user accounts. You can import user accounts in a text file by choosing this menu option. Every line of the text file must contain a single user account and every username, password and group name triplet *(or just a username and password pair)* for an account must be concatenated with a comma *(or the list separator in locale settings)* as shown below:

```
Username1,Password1,Group1
Username2,Password2,Group2
:
Usernamen,Passwordn,Groupn
```

Specified groups must be created manually prior to start an import process. TekRADIUS will import user accounts into the selected group in the Groups tab of TekRADIUS Manager if the specified groups are not found or group is not specified.

You can also use double quotes as text qualifiers:

```
"Username1","Password1","Group1"
```

Group name is optional, and its existence must be specified when asked. You can also add extra attributes for the imported user profiles. Use Attribute=Val format when specifying the extra attributes. You can add multiple attributes as shown below:

```
"Username1","Password1","Group1","Calling-Station-
Id=10:56:34:AA:11:01|Check";"Framed-Protocol=1|Success-Reply"
```

You can also specify attribute type by concatenating value with the attribute type using pipe (“|”) character. Possible values:

- Check
- Success-Reply
- Failure-Reply

- Informational
- DHCP-Success-Reply
- DHCP-Failure-Reply
- CoA-Set
- CoA-Reset

Extra attributes will be added as Check attributes if the attribute type is not specified.

Leave the password blank field if the user profile has not a password:

```
"Username1","","Group1"
```

You can use the same import file format while importing through the HTTP interface of TekRADIUS.

Export user accounts. You can export user accounts as csv files. You can optionally add group names for exported user accounts.

Import Certificate. Imports an X.509 certificate to the Windows Certificate Store / Local Machine / Personal store for server authentication.

Exit. Close TekRADIUS Manager.

Service Menu

Start. Starts TekRADIUS background service.

Stop. Stops TekRADIUS background service.

Rebuild Counters. Resets and rebuilds performance counters.

Clear Cached AD Data. Clears cached user membership information for AD users.

Clear Cached Attributes. Clears cached user / group check and reply attributes.

Display Index Fragmentation. Display index status in the database. The result will be displayed in the SQL tab.

Help Menu

About. Displays TekRADIUS version, registration information and system id.

Help. Opens TekRADIUS Installation & Configuration Manual file.

Import License. Imports and activates license *(Registration.key)* file

Starting TekRADIUS

Start or stop TekRADIUS from within the **Settings** tab by clicking the **Run** or **Stop** icon to the left of the **Save Settings** button at the bottom right of the screen.

If the service starts successfully, the "*TekRADIUS Service is Running*" message will be displayed at the bottom right message section of TekRADIUS Manager. If the TekRADIUS service is already running when any changes are made to the configuration, TekRADIUS will prompt for confirmation to restart the TekRADIUS service to make the changes active.

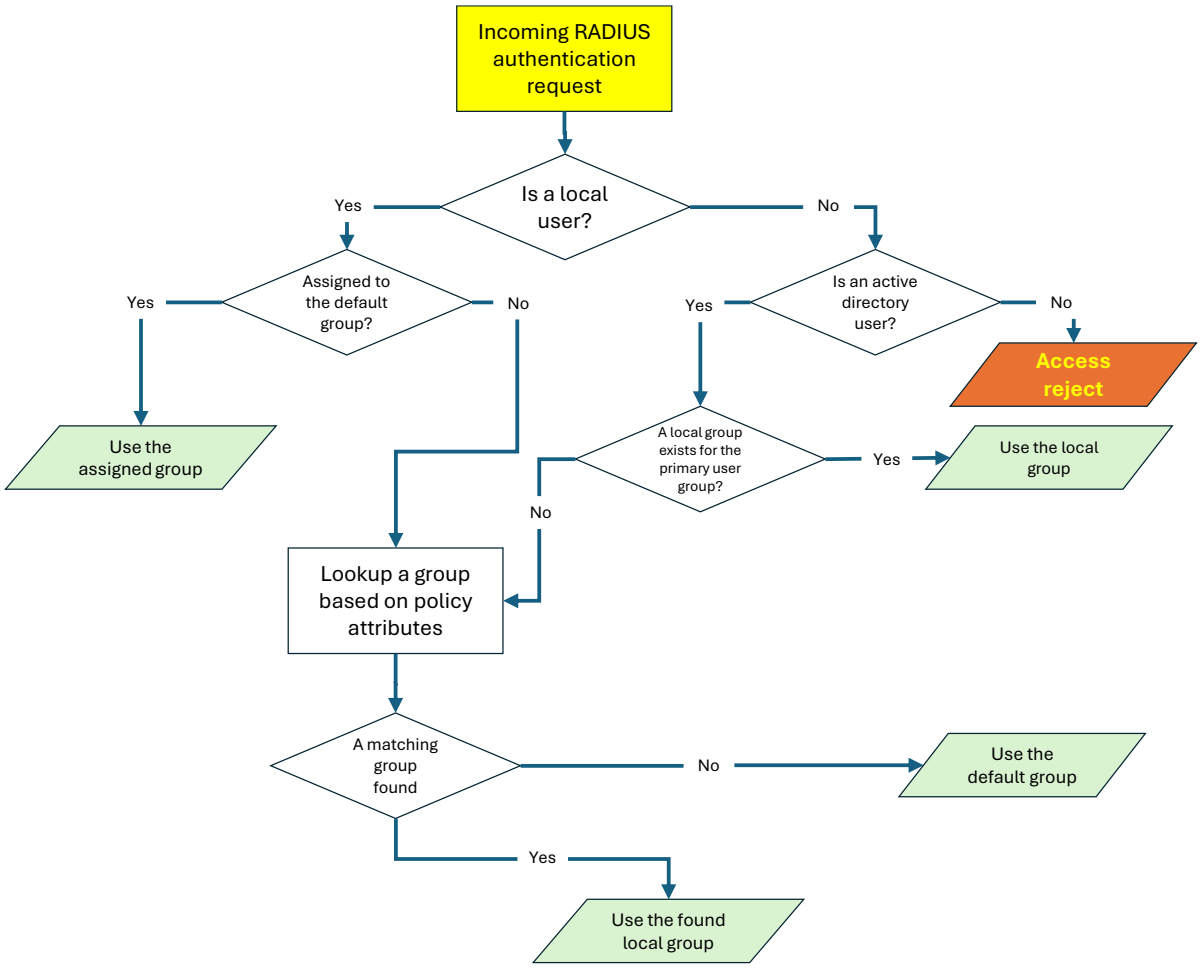
If the TekRADIUS service cannot start, examine the Application Log tab and the TekRADIUS log file, located under **<Application Directory>\Logs**, ensuring that you have enabled logging in **Settings / Service Parameters** tab.

User Group Determination via Policy Matching

Every user profile in TekRADIUS is associated with a group profile. Group profiles enable you to group common check / reply attributes for a group of users. TekRADIUS allows you to authenticate with a different set of group attributes chained with Next-Group attribute in the primary group. Policy matching allows you to specify an alternative primary user group for an incoming authentication request when user is assigned to the default user group in TekRADIUS. Policy matching is also used to determine local user group for AD/Windows user accounts when there is not a corresponding local user group for the user's primary AD group. Matching based on policy attributes added as check attributes to the group profiles:

- Client-Label
- NAS-IP-Address
- NAS-Identifier
- Service-Type
- Framed-Protocol
- Called-Station-Id
- NAS-Port-Type
- Authentication-Method

Group membership determination is performed as shown in the diagram below



Monitoring

Application Log entries added by TekRADIUS may be viewed in the **Application Log** tab. If the 'Enable Auto Refresh' option is checked, the list will be automatically refreshed; otherwise, the log can be manually refreshed by clicking the **Refresh Log** button. All log entries can be deleted by clicking the **Clear Log** button. It is necessary to have administrative privileges to read from, and write to, the event log in Microsoft Vista.

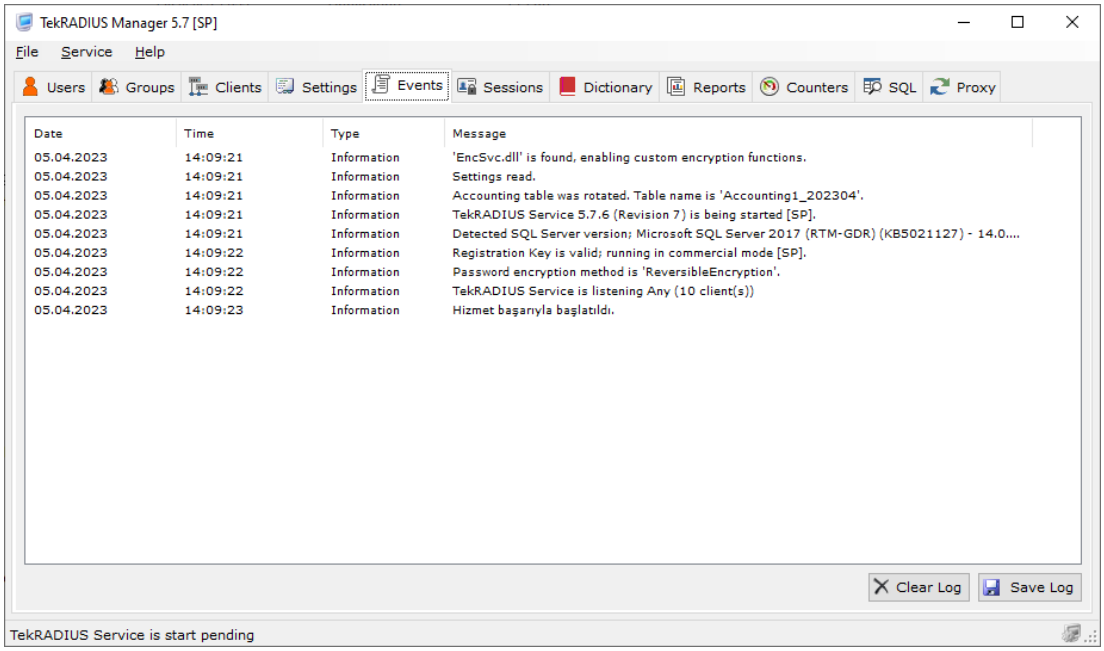
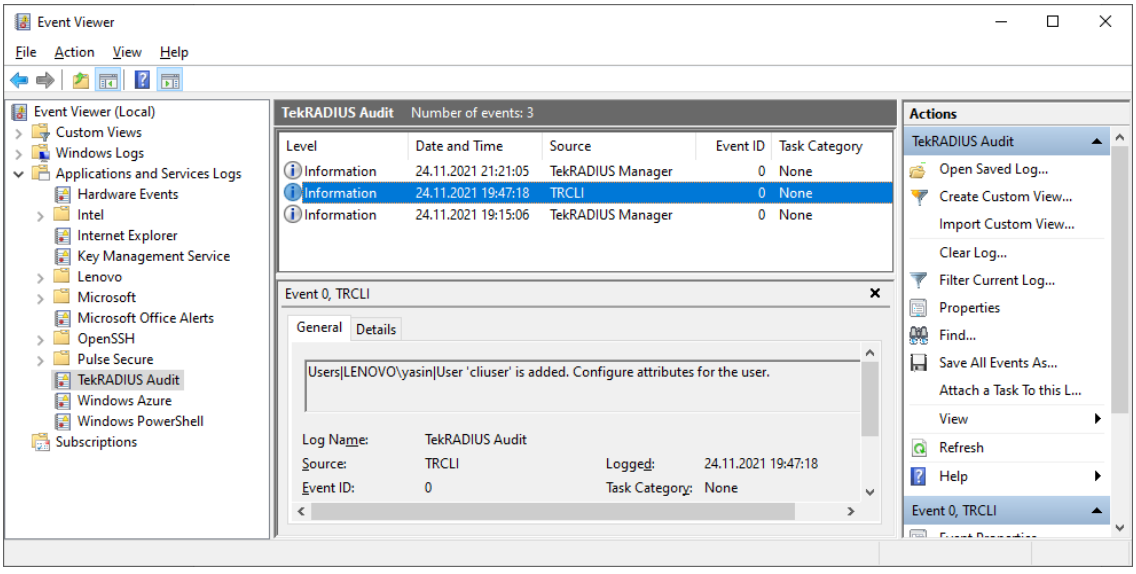


Figure 19 - Application Log Tab

Active sessions can be monitored from the **Active Sessions** tab; this list is not refreshed automatically. To refresh the list, click the **Refresh** button or set a refresh period in seconds. There are additional hidden information columns that can be revealed by checking the 'Show Detail' option in context menu accessible when you right click on active session list.

! *TekRADIUS automatically clears all entries in the Sessions table when the TekRADIUS service is restarted.*



Active Sessions

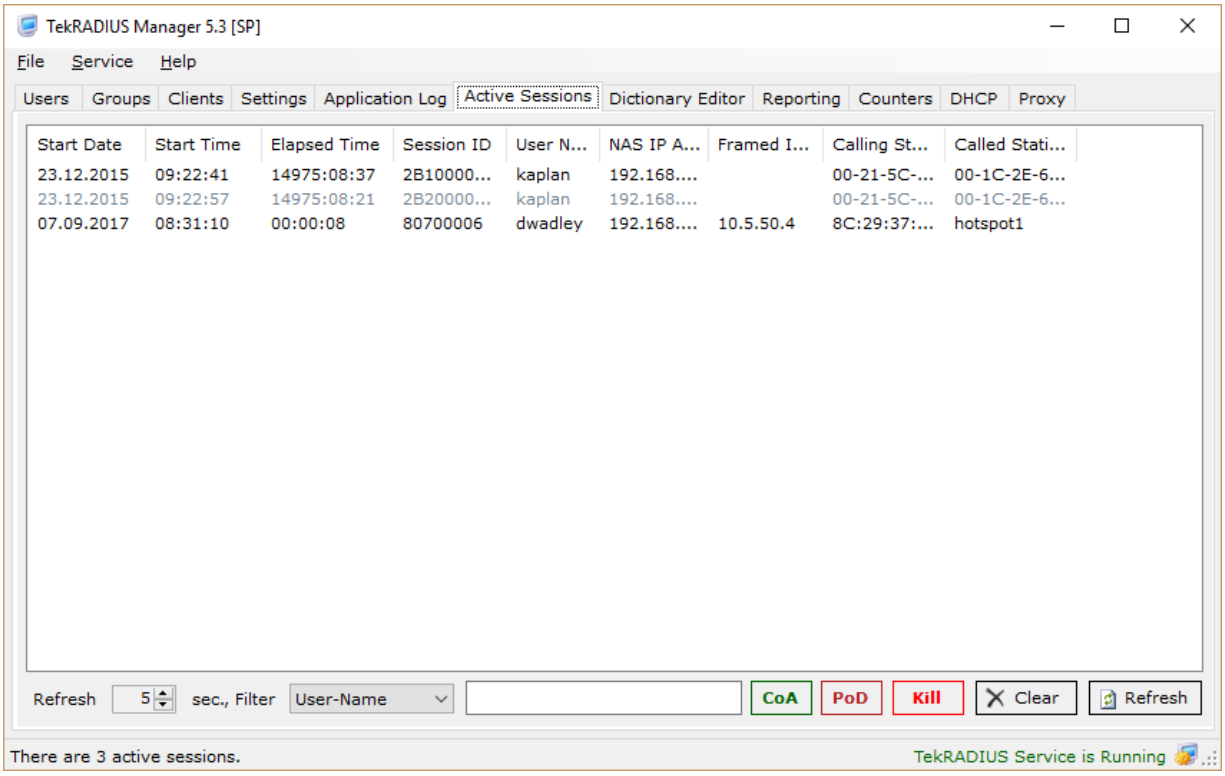


Figure 20 - Active Sessions Tab

To view active sessions, the RADIUS clients must send RADIUS accounting Start/Stop packets to TekRADIUS. Most RADIUS clients support Stop-Only mode; if the clients are configured to send only RADIUS Accounting-Stop packets, it is not possible to view the active sessions.

Clear, Kill, PoD and CoA functions can be executed for selected active sessions. The Clear function inserts an artificial stop record for the selected session and clears the entry in the Sessions table, it does not disconnect the user session nor decrement the simultaneous session counter *(TekRADIUS Server must be restarted to reset the simultaneous session counters).*

If a user has a time-based credit limit, clearing the user session will also update the user credit. If a data volume-based credit has been defined or a session is a VoIP call, use the Kill or PoD functions. Click **Kill** to execute the user function defined in the **Client** tab. Click **PoD** to send a RADIUS *Disconnect-Message (or Packet of Disconnect, PoD)* to the remote client.

You can send two types of CoA requests for selected active sessions; CoA set and CoA reset. These requests allow you to change status and active sessions without disconnecting it. You can lower or upper user connection rate by sending set and reset requests respectively. CoA set and reset attributes must be defined in user or group profiles prior to sending CoA requests.

NOTE: it is necessary to configure the client to accept PoD or CoA messages from TekRADIUS. CoA option is available only in SP Edition.

An alternating color scheme (**Black**/Gray) is used to increase readability in the sessions list.

TekRADIUS includes following attributes in PoD / CoA requests in order the NAS distinguish a particular user session;

Default

- User-Name
- Acct-Session-Id
- Acct-Multi-Session-Id (If exists)
- Calling-Station-Id
- Called-Station-Id
- Framed-IP-Address
- NAS-Port

Cisco

- User-Name
- Calling-Station-Id
- Framed-IP-Address

Mikrotik

- User-Name
- Framed-IP-Address
- NAS-Port
- NAS-Port-Type
- Calling-Station-Id

Xirrus

- Calling-Station-Id

Aruba

- User-Name
- NAS-IP-Address
- Framed-IP-Address
- Calling-Station-Id

Meraki

- Event-Timestamp

Ericsson

- User-Name

You can specify a custom PoD action through Kill Command of RADIUS client entry using TRCLI.exe;

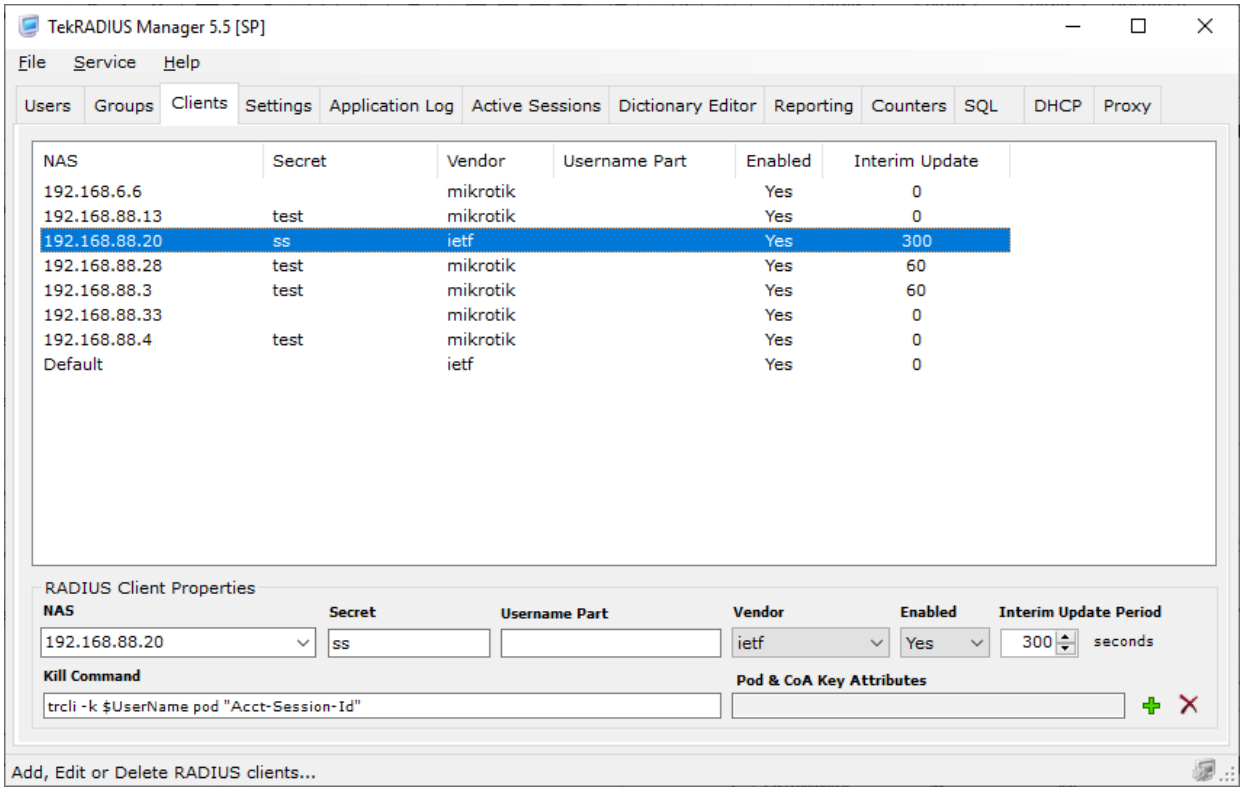


Figure 21. - Custom PoD action

TekRADIUS will send PoD requests to 192.168.88.20 by adding User-Name and Acct-Session-Id attributes to the request to in the example above.

You can alternatively specify which attributes will be used as key attributes while sending CoA and PoD requests by setting **PoD & CoA Key Attributes** parameter for a client entry. Click PoD & CoA Key Attributes parameter and choose attributes to added CoA and PoD requests;

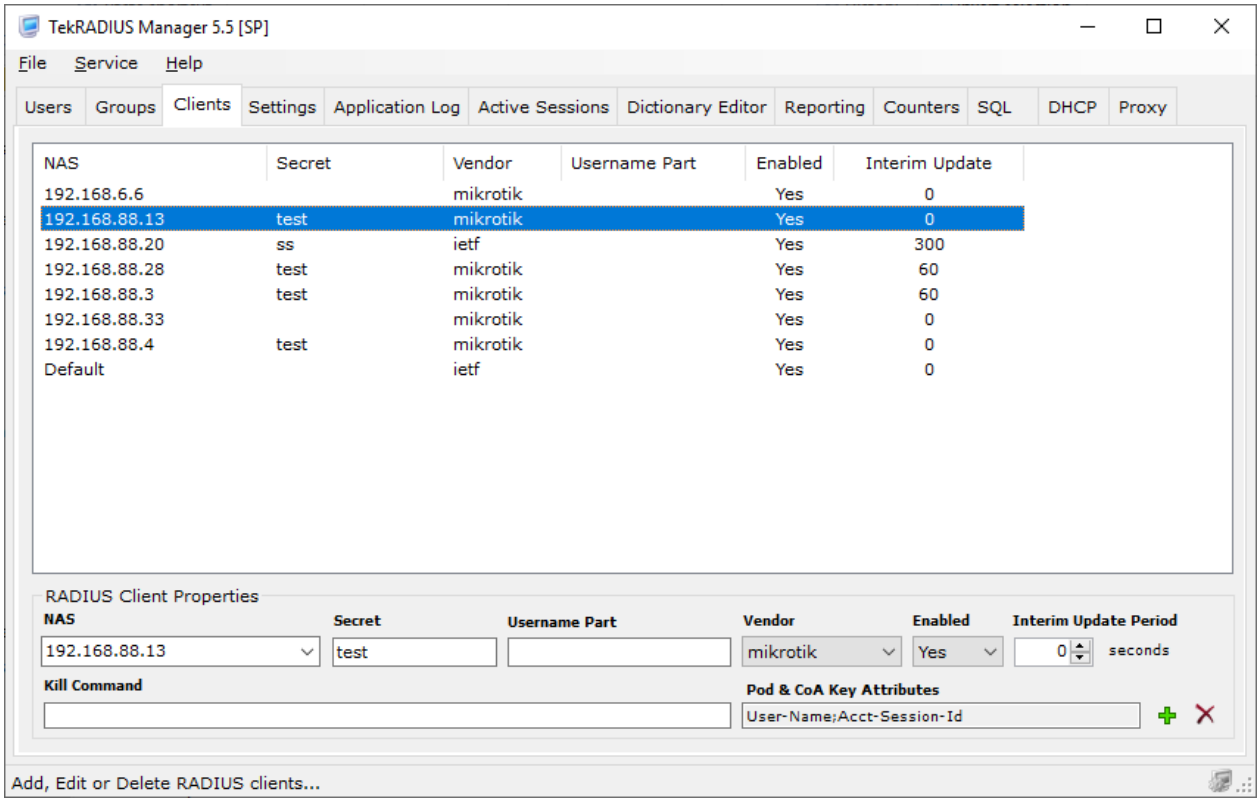


Figure 22. - Attribute selection for PoD and CoA requests

TekRADIUS Log File

Session details and errors that have occurred are logged in the TekRADIUS log file. The Log files are located under the **<Application Directory>\Logs** directory. The logging detail level can be specified from the **Settings / Service Parameters** tab. The TekRADIUS log file is rotated daily. It is also possible to open the current log file from the 'File' menu of TekRADIUS Manager.

TekRADIUS Specific Attributes (RADIUS Check Items)

TekRADIUS provides several special attributes; their names and functions are described below. These attributes can be added to User or Group profiles only as check attributes. These attributes are listed under vendor KaplanSoft in the dictionary editor.

TekRADIUS-Status

TekRADIUS will reject authentication requests if the *TekRADIUS-Status* attribute is set to '*Disabled*' in User or Group profiles. If this attribute does not exist in the User or Group profile, TekRADIUS will assume that the User or Group is enabled. **NOTE:** A user attempting authentication will receive *failure-reply* if the User profile has *Failure-Reply* attributes when the user profile was disabled.

Simultaneous-Use

To use the *Simultaneous-Use* attribute, Accounting must be enabled on TekRADIUS, otherwise users with the *Simultaneous-Use* attribute set will receive an *Access-Reject*. This feature will not function if the RADIUS client sends only RADIUS *Accounting-Stop* packets *(most RADIUS clients only support accounting stop-only mode).* You must disable credentials caching in your access servers for proper use of Simultaneous-Use attribute.

In order to set a simultaneous session limit for a user, add the *Simultaneous-Use* attribute as a Check attribute in the User profile. If this attribute is added to a Group profile, the number of total sessions for a group can be limited. TekRADIUS first checks if a Group's limit, specified with Simultaneous-Group-Use attribute in the user's group profile, has been reached and then checks the individual User's limit.

Simultaneous-Group-Use

In order to use the *Simultaneous-Group-Use* attribute, Accounting must be enabled on TekRADIUS, otherwise users with the *Simultaneous-Group-Use* attribute set will receive an *Access-Reject*. This feature will not function if the RADIUS client sends only RADIUS *Accounting-Stop* packets *(most RADIUS clients only support accounting stop-only mode).*

To set a simultaneous session limit for a group, add the *Simultaneous-Group-Use* attribute as a Check attribute in the Group profile. TekRADIUS first checks if a Group's limit has been reached and then checks the individual User's limit.

Expire-Date

An *Expire-Date* parameter can be specified in User or Group profiles to disallow logins after the specified date for a User or Group of users. Add the *Expire-Date* as a check item in a User or Group profiles. When *Expire-Date* is added as a check item to the User profile, TekRADIUS will automatically add the *Session-Timeout* attribute, with remaining time in seconds, as a reply-item to an authorization response. You can use date format based on your locale settings. You need to use T character in place of space between date and time when you add this attribute using TRCLI *(12.03.2013T23:30 e.g.)*. TekRADIUS keeps date values as an integer value representing seconds since July, 1st 1970 in the database.

User-Credit

A usage quota may be specified for a user in units specified in the *Credit-Unit* parameter. The *User-Credit* attribute can be added as a check item in the User or Group profiles. TekRADIUS will automatically add *User-Credit* attribute to the user profile if *User-Credit* attribute exists in Group profile in first authentication attempt for the user profile and TekRADIUS will also create a local proxy user profile if user exists in Active Directory not in the local database.

In order to use the *User-Credit* attribute, Accounting must be enabled on TekRADIUS, otherwise users with the *User-Quota* attribute set will receive an *Access-Reject*. If the *Credit-Unit* is not specified, TekRADIUS assumes the default units of seconds.

TekRADIUS updates the value in the *User-Credit* attribute when an *Accounting-Stop* or *Checkpoint* message is received for the user-session. TekRADIUS uses the *Acct-Session-Time*, *Acct-Input-Octets* and *Acct-Output-Octets* attributes in the *Accounting-Stop* or *Checkpoint* messages to update the *User-Credit* value.

If the *Acct-Session-Time* attribute is not present in the *Accounting-Stop* or *Checkpoint* messages, TekRADIUS will use the value of [Accounting Stop Time] - [Accounting Start Time] in place of *Acct-Session-Time* if *Credit-Unit* attribute is time based.

Credit-Unit

The unit of accounting data can be set using the *Credit-Unit* attribute. If this attribute is added to a User or Group profile and its value set to 'Seconds', TekRADIUS will undertake accounting based on seconds. If the *Credit-Unit* attribute value is set to Bytes, Kbytes or Mbytes, TekRADIUS will undertake accounting based on data usage *(Acct-Input-Octets, Acct-Output-Octets* or sum of *Acct-Input-Octets* and *Acct-Output-Octets)*, and not the *Acct-Session-Time*.

If this attribute does not exist in either the User or Group profile, the default unit of 'Seconds' will be used. This attribute also specifies the unit of the values used in the *User-Credit* attribute.

Authentication-Method

The *Authentication-Method* attribute may be used as a RADIUS check item within TekRADIUS. For example, if a user is only granted login using PAP, then that user cannot login using the CHAP protocol.

In order to authenticate users with PEAP or EAP-TLS, it is necessary to add the *TLS-Server-Certificate* attribute to the User or Group profile.

It is not possible to use the Windows Authentication Proxy feature with CHAP or EAP-MD5 authentication methods as TekRADIUS is unable to retrieve a user's clear text password.

! *Windows Authentication with MS-CHAP-v1, MS-CHAP-v2 EAP-MS-CHAP v2 and PEAPv0-EAP-MS-CHAP-v2 are supported only in the commercial edition.*

TekRADIUS supports PAP, CHAP, MS-CHAP-v1, MS-CHAP-v2, EAP-MD5, EAP-MS-CHAP v2 and PEAPv0-EAP-MS-CHAP-v2 *(as implemented in Windows XP SP1)*, Digest *(draft-sterman-aaa-sip-00.txt)* authentication methods.

Active Directory Authentication

There are two options for authenticating users against Active Directory;

1. Activate AD Proxy (or *Windows Auth. Proxy* on a domain-connected server) in **Settings / Service Parameters**. A local User profile is not necessary in this case.
2. With a local User or Group profile, add *Authentication-Method = Active-Directory* and *Directory-Server = <AD Domain>*. If TekRADIUS is installed on a domain-member server, add *Authentication-Method = Windows*.

One-Time Password Authentication

Commercial editions of TekRADIUS Supports OTP *(One Time Password)* authentication-based RFC 2289. To use OTP authentication, the *Authentication-Method* attribute needs to be added to User or Group profiles with one of following values: *OTP-MD4*, *OTP-MD5* or *OTP-SHA1*. The initial value of User-Password must be calculated using an OTP password generator. A suitable OTP password generator is TekOTP (http://www.tekotp.com/). See below for an example of TekOTP OTP generation:

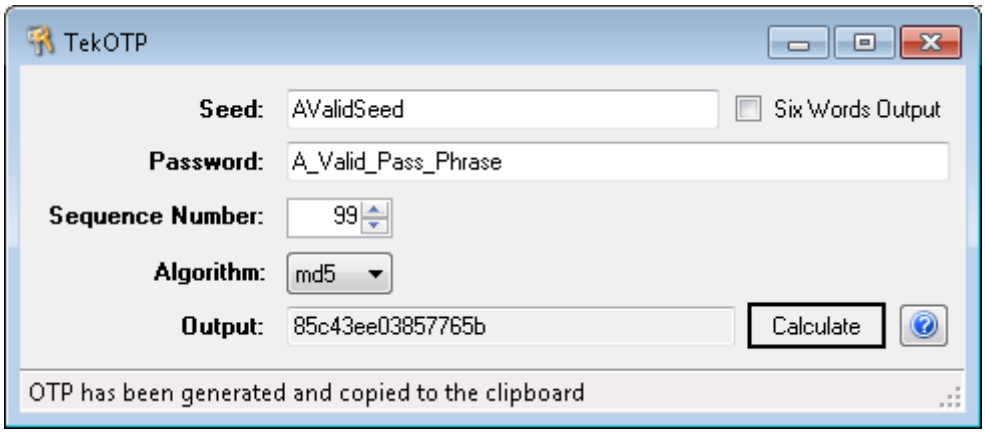


Figure 23. - TekOTP

Note: The initial password must be generated by unchecking the 'Six Words Output' option. The initial value must be entered as User-Password in user profiles as a check attribute. Another OTP must be generated after increasing **Sequence Number** bye one for the first authentication attempt for the client. Client must enter the six words form of OTP when implementing CHAP or MS-CHAP-v1/v2.

TLS-Server-Certificate (TLS-Certificate prior to version 4.0)

The *TLS-Server-Certificate* holds the server certificate name that has been configured for PEAP or EAP-TLS sessions. When TekRADIUS receives a PEAP or EAP-TLS authentication request, the User profile is first searched for a *TLS-Server-Certificate* attribute, if it is not found then the Group profile is searched. If TekRADIUS cannot find the *TLS-Server-Certificate* in the User or Group profiles, then PEAP or EAP-TLS authentication requests will be rejected.

Server Certificates must be installed with their private keys in the Windows Certificate Store. Please make sure that you have set Private Key Exportable option while importing a 3rd party certificate to Windows Certificate store / Local Machine. See the section 'Creating and Installing a Self-Signed Certificate for PEAP/EAP-TLS Authentication' in this manual for information about installing certificates. TekRADIUS distinguishes certificates using the CN property of the Subject field of the certificates.

TLS-Client-Certificate

The *TLS-Client-Certificate* holds the client certificate name that has been configured for EAP-TLS sessions. When TekRADIUS receives an EAP-TLS authentication request, the received certificate in the authentication request is first checked against the *TLS-Client-Certificate* attribute in the User profile; if the User profile does not contain a *TLS-Client-Certificate* attribute, the received certificate is then checked against the *TLS-Client-Certificate* attribute in the Group profile.

In order to verify a certificate that has been specifically assigned to a user, a copy of the client certificate must exist in the Local Windows Certificate Store in the server on which TekRADIUS is installed. If TekRADIUS cannot find the user certificate in the local certificate store, TekRADIUS performs a X.509 chain validation only.

Client Certificates must be installed also in the Windows Certificate Store if self-signed certificates are used. Please make sure that you have set Private Key Exportable option while importing a 3rd party certificate to Windows Certificate store / Local Machine. See the section 'Creating and Installing a Self-Signed Certificate for PEAP/EAP-TLS Authentication' in this manual for information about installing certificates. TekRADIUS distinguishes certificates using the CN property of the Subject field of the certificates.

Windows-Domain

To authenticate a user against a Windows Domain, add the *Authentication-Method* check-attribute with a value of *Windows* to either a User profile, Group profile or the Default Group profile. The domain that holds a user account can either be set globally in **Settings / Service Parameters / Authentication / Authentication Proxy Domain** or as a specific *Windows-Domain* attribute in a User or Group profile.

The local domain can be specified within the **Settings / Server Settings** tab by entering a '.' *(period mark)* as the parameter value. Enter the domain name or domain server IP address without the '\\' *(double back slash)*.

Windows-Domain is a string type attribute and only exists as a check attribute in User or Group profiles.

Directory-Server

To authenticate a user against Active Directory, add the *Authentication-Method* check-attribute with a value of *Active-Directory* to either a User profile, Group profile or the Default Group profile. The Active Directory that holds a user account can either be set globally in the **Settings / Service Parameters / Authentication / Authentication Proxy Domain** or as a specific *Directory-Server* attribute in a User or Group profile.

To authenticate against an LDAP Directory server, add the *Authentication-Method* check-attribute with a value of *LDAP* to either a User profile, Group profile or the Default Group profile. Set Directory-Server value to an LDAP URL. Example;

```
ldap://example.com:389/uid=%uid%,dc=example,dc=com
```

TekRADIUS will populate the `%uid%` variable with the received username in the authentication request. You can omit LDAP standard port 389 or 636 for LDAPS URLs. Base authentication method must be PAP for LDAP authentication.

Directory-Server is a string type attribute and only exists as a check attribute in User or Group profiles.

Active-Directory-Group

If Active Directory authentication has been implemented, a user's Active Directory group membership can be validated by adding the *Active-Directory-Group* attribute as a check attribute to the User or Group profile. You can concatenate multiple groups with semicolons like Group1;Group2;Group3. You may need to add domain user accounts used to run TekRADIUS service and TekRADIUS Manager to Windows Authorization Access (WAA) group to fetch Active Directory user groups in your Active Directory Domain.[1]

Active-Directory-Group is a string type attribute and can exist as a check attribute only in User or Group profiles.

Time-Limit

If the *Time-Limit* check-attribute is added to a User or Group profile, TekRADIUS will check if the specified duration *(Minutes)* has elapsed since the first logon, specified using the *First-Logon* attribute. If the *First-Logon* attribute is not found, TekRADIUS assumes that the current login attempt is the first login attempt and then adds the *First-Login* attribute to the User profile as a check attribute with the current date and time as its value. Add *Time-Limit = 43200* (Check) for one month period to user or group profile.

Time-Limit is an integer type attribute and can exist as a check attribute in user or group profiles.

! *If the allowed total session time is set using the* Session-Timeout *attribute and the remaining time for the allowed time span for the user is less than* Session-Timeout *value, TekRADIUS will set the* Session-Timeout *value to the remaining time for the allowed period.*

First-Logon

The *First-Logon* attribute is automatically added to user profiles at the first login attempt by TekRADIUS if the User or Group profile has a *Time-Limit* attribute. This attribute can be manually updated using TekRADIUS Manager or trcli.exe.

First-Logon is a string type attribute and can exist as a check attribute only in user profiles.

Login-Time

The allowed login days and hours can be limited for a user by adding *Login-Time* as a check attribute to the User or Group profile. When this attribute is added to a User or Group profile, the default action will be to reject the access request if the authentication request is not received within the defined time period. The syntax of the *Login-Time* attribute is:

```
[Su|Mo|Tu|We|Th|Fr|Sa|Wk|Hd|Al]<Begin Hour>-<End Hour>
```

Where:

Wk : Weekdays *(Working days based on your locale settings)*
Hd : Weekend *(Weekend days based on your local settings)*
Al : All days of the week *(All seven days of a week)*

[1] https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/apps-apis-require-access

Hours must be in 24-hour format (e.g., 22:55). Several periods may be defined by concatenating the periods with commas ‘,’. Every period is processed individually; ‘Tu11:00-12:00, Tu12:00-14:00’ is not interpreted as ‘Tu:11:00-14:00’. Longer periods are preferred over shorter periods when overlapping periods are defined. If ‘Tu12:00-14:00, Al13:00-17:00’ have been defined, TekRADIUS will prefer ‘Al13:00-17:00’ on Tuesdays at 13:30.

Examples:

1. **Wk09:00-18:00, Hd12:00-16:00** will allow logins from 09:00 to 18:00 during weekdays and from 12:00 to 16:00 at weekends.
2. **Mo10:00-23:50, We10:00-23:50, Hd11:00-17:00** will allow logins from 10:00 to 23:50 on Monday and Wednesday, and from 11:00 to 17:00 at weekends.
3. **Al09:00-18:00, Fr08:00-19:00** will allow logins from 09:00 to 18:00 for all days except Friday; login attempts are allowed from 08:00 to 19:00 on Fridays.

Login-Time is a string type attribute and can exist only as a check attribute in User or Group profiles.

Upper and lower time can span across day boundaries. Al22:00-01:30 is valid, for instance.

Generate-MS-MPPE-Keys

TekRADIUS automatically generates 128 bits Encryption Keys for authenticated L2TP and PPTP sessions when the incoming RADIUS *Access-Request* has the *Tunnel-Type (64)* attribute with the value set to *PPTP* or *L2TP*. This behavior can be changed by adding the *Generate-MS-MPPE-Keys* attribute to a User or Group profile as a check attribute.

If this attribute exists in a User or Group profile and its value is set to ‘*NOT-Generate*’, TekRADIUS will not generate encryption keys. If its value is set to ‘*VPN-Generate-128*’ or ‘*VPN-Generate-40*’ *(For 40 bits encryption keys)*, TekRADIUS will generate encryption keys if user is authenticated via Microsoft authentication methods regardless of whether the *Tunnel-Type* attribute was present or not in the *Access-Request*.

TekRADIUS also automatically generates WPA encryption keys and sends them in a final *Access-Accept* packet after a successful PEAP authentication session for a wireless connection. Some access points do not report the port type as wireless, so in some cases it is necessary to force TekRADIUS to generate the encryption keys; to achieve this, add the *Generate-MS-MPEE-Keys* attribute as a check attribute to a User or Group profile with its value set to *WPA-Generate*.

The *Generate-MS-MPPE-Keys* attribute is an integer type attribute and can exist only as a check attribute in user profiles.

Next-Group

This attribute is used to chain Group profiles. The *Next-Group* attribute can be used only in Group profiles as a check attribute. Authentication of an incoming access-request will first be attempted with the User attributes and then the primary Group of which the user is a member. If this fails, TekRADIUS will then try to authenticate with the User attributes and the next Group’s attributes. **NOTE:** Attributes in User profiles overrides those used in Group profiles; do not use attributes in User profiles that are used in chained Group profiles.

For example, to authenticate a session based on a specific *NAS-IP-Address* contained within a pool of NAS devices, each with a different NAS-IP-Address, create a Group profile for each *NAS-IP-Address* value and chain these Groups using the *Next-Group* attribute.

The *Next-Group* attribute is a string type attribute and can exist only as a check attribute in Group profiles.

Failure-Reply-Type

The *Failure-Reply-Type* attribute is used as a check attribute in User or Group profiles to alter the behavior of TekRADIUS when *Failure-Reply* attributes exist in a User or Group profile; the value of *Failure-Reply-Type* can either be set to *Accept* or *Reject*. When it is set to *Accept*, *Failure-Reply* attributes are sent in an *Access-Accept*; if it is set to *Reject*, *Failure-Reply* attributes are sent in an *Access-Reject* message.

The default behavior of TekRADIUS if this attribute does not exist in a User or Group profile and *Failure-Reply* attributes are configured to be send *Failure-Reply* attributes in an *Access-Reject* message. Add FailonPasswordFailure=1 parameter under [Server] section of TekRADIUS.ini to send Failure-Reply attributes in an Access-Reject message when user entered password is not valid.

Failure-Reply-Type is an integer type attribute and can exist only as a check attribute in user or group profiles.

Tunnel-Tag

The Tunnel-Tag attribute is used as a check attribute in User or Group profiles. This attribute sets the tag values of tunnel attributes (*Tunnel-Type*, *Tunnel-Medium-Type*, *Tunnel-Client-Endpoint*, *Tunnel-Server-Endpoint*, *Tunnel-Password*, *Tunnel-Private-Group-ID*, *Tunnel-Assignment-ID*, *Tunnel-Preference*, *Tunnel-Client-Auth-ID* and *Tunnel-Server-Auth-ID*) that is sent in RADIUS replies. You can also specify individual tags for tagged attributes.

If this attribute does not exist in a User or Group profile, TekRADIUS assumes a tag value of 0 *(Except Tunnel-Private-Group-Id attribute. You must add Tunnel-Tag = 0 as a check attribute to the user or group profile otherwise TekRADIUS will not add tag field to the Tunnel-Private-Group-Id attribute value).* This attribute can have a value between 0-15 inclusive.

Tunnel-Tag is an integer type attribute and can exist only as a check attribute in user or group profiles.

Credit-Period

The *Credit-Period* attribute is used as a check attribute to User or Group profiles. This attribute specifies a time-duration for user credit. For example, it is possible to assign users daily, weekly or monthly time credits by adding the *Credit-Period* attribute to User or Group profiles. This attribute must be used in conjunction with the *Credit-Per-Period* and *User-Credit* attributes.

Credit-Period is an integer type attribute and can exist only as a check attribute in user or group profiles.

Credit-Per-Period

The *Credit-Per-Period* attribute is used as a check attribute in User or Group profiles and is used to set a credit-limit for the period specified by the *Credit-Period* attribute.

If neither a User nor Group profile has a *Credit-Period* attribute, the default period will be '*Daily'*. This attribute must be used in conjunction with the *User-Credit* attribute.

If this attribute is added to a User or Group profile, the *First-Logon* attribute will be automatically added to the User profile after user's first successful logon. Period end and start times are calculated based on *First-Logon* date/time. TekRADIUS will set the value of the *User-Credit* attribute to the value defined in the *Credit-Per-Period* attribute after every *Credit-Period* expiry.

Sample User profile:

User has 2 hours credit per day;

```
User-Credit = 7200 (Check)
Credit-Unit = Seconds (Check)
Credit-Period = Daily (Check)
Credit-Per-Period = 7200 (Check)
```

Credit-Per-Period is an integer type attribute and can exist only as a check attribute in User or Group profiles.

TekRADIUS will send CoA requests to NAS devices for the active users with Credit-Period and Credit-Per-Period attributes to update authorized amount of credit while updating user credits *(SP edition only)*.

External-Executable

The *External-Executable* attribute is used as a check attribute in User or Group profiles to check the result from an external executable. A return code '0' *(or HTTP return code 200)* is assumed as success and return codes other than '0' are assumed as failure. If the execution fails for any reason, it will be assumed as a failure and authentication will fail.

Enter the full path of the executable as the value of the *External-Executable* attribute. Use double quotes (" ") if the path contains space characters if the executable is not an HTTP URL nor sendmail command. Constant or variable parameters may be specified for the executable. Use *%<RADIUS attribute>%* to use received RADIUS attributes in *Access-Request* messages. You can also use `%auxstr%` variable. Please see Concatenated-Password attribute to see how to set `%auxstr%` value. TekRADIUS can get user e-mail addresses and mobile phone numbers from Active Directory. You can use `%mail%` and `%mobile%` variables to use user e-mail address and mobile phone number as parameters for the executable. You can get seen IP address of a RADIUS client using `%ciaddr%` variable which can be different than reported in NAS-IP-Address attribute.

These are typical valid examples that can be used in user or group profiles;

```
External-Executable = C:\Test.bat %ietf|1% %ietf|2% %mobile%
External-Executable = "C:\Program Files\My App\test.exe" -log %ietf|1% %ietf|2%
External-Executable = http://kaplansoft.com/test.php?username=%ietf|1%&pass=%ietf|2%
External-Executable = https://kaplansoft.com/test.php?username=%ietf|1%&pass=%ietf|2%
External-Executable = "C:\Progra~1\multiotp\multiotp.exe" %ietf|1% %ietf|2%
External-Executable = sendmail %mail% %ietf|40%
External-Executable = sql:Select count(*) from Sessions where UserName ='%ietf|1%'
External-Executable = [udp|tcp|tls]://kaplansoft.com:600/username=%ietf|1%,pass=%ietf|2%
```

User-Name (Standard RADIUS attribute #1) and *User-Password* (Standard RADIUS attribute #2) are used in the examples above. Refer to the RADIUS dictionary for the other attributes.

You must enable Mail Alerting at Settings / Alerting in order to user sendmail internal command.

External-Executable is a string type attribute and can exist only as a check attribute in User or Group profiles.

TekRADIUS also accepts reply attributes from the console output of an external executable. This is especially useful when an external authenticator is used for MS-CHAP authentication methods and it is necessary to have encryption keys generated for VPN sessions.

! *TekRADIUS requires a clear text password to generate VPN encryption keys.*

The example below will return *User-Password*, *Session-Timeout* and *Reply-Message* attributes:

```
ietf|2=password
ietf|27=3600
ietf|18=Reply message
```

Sample .bat file content to provide the output above;

```
@echo off
ietf^|2=password
ietf^|27=3600
ietf^|18=Reply message
```

NOTE: Every line must be terminated with CRLF and you should add

```
exit /B 0
```

line at the end of the batch file if you would like to return a positive *(Successful)* response.

When a mail message is sent sendmail action result is assumed to be successful.

If your SQL query does not return any rows TekRADIUS assumes the action result is failure. If a query returns one row and one character action result is determined by the returned value. It must be a numeric character and it must be other than "0" *(without quotes)* for a successful execution. The action result is assumed to be successful if the query returns more than one row.

If an HTTP server returns one character action result is determined by the returned value. It must be a numeric character and it must be other than "0" *(without quotes)* for a successful execution. Action result is assumed to be successful if the server returns more than one character.

Credit-Expiry-Action

When a user's credit is fully consumed, TekRADIUS can send Packet of Disconnect *(PoD),* Change of Authorization *(CoA),* or execute user-defined session kill command *(SP Edition only)*. This feature can be enabled on a user or group basis by adding *Credit-Expiry-Action* as a check attribute to a User or Group profile respectively; either the '*Send-POD*', '*Send-CoA*' or '*Issue-Kill-Command*' action can be selected.

You can configure attributes for CoA requests by adding these attributes as CoA-Set type attributes in user or group profiles. You can change connection speed without disconnecting user session by sending a CoA request. This allows you to apply "Fair Usage Policy *(FUP)*" to user sessions. You can send CoA-Reset request by manually either through TekRADIUS Manager Active Sessions tab or through command line utility TRCLI to restore authorization status of user sessions. TekRADIUS also sends CoA-Reset attributes after periodic credit update specified with Credit-Period if CoA-Reset attributes exist in user or group profiles.

The access server must be configured to send *Accounting-Interim-Updates* (Checkpoint) messages so that TekRADIUS can monitor credit usage. If the '*Issue-Kill-Command*' action is selected, the kill command must be defined in the **Clients** tab.

Credit-Expiry-Action is an integer type attribute and can exist only as a check attribute in User or Group profiles.

EAP-SIM-Triplet-[1|2|3]

TekRADIUS stores SIM triplets in *EAP-SIM-Triplet* attributes for EAP-SIM authentication in the following format:

```
0x<Hexadecimal encoded 16 Byte RAND string><Hexadecimal encoded 4 Bytes SRES string><Hexadecimal encoded 8 Bytes Kc string>
```

Example:

```
0xF926A7CDE05A44A8B749204E6F8DBB51F51440E587F4A6CD5A02B07A
```

The bold section denotes the SRES portion.

These attributes are automatically inserted to a user profile when the **Import SIM triplets** button in **Users** tab is clicked. It is also possible to manually enter these attributes into a user profile.

EAP-SIM-Triplet attributes are string type attributes and can exist only as a check attribute in User or Group profiles.

EAP-SIM-OP

You can set the 128-bit Operator Variant Algorithm Configuration value for a user profile by adding EAP-SIM-OP as a check attribute to a user profile for EAP-SIM and EAP-AKA authentication methods. Use the following format

```
0x<Hexadecimal encoded 16 Bytes string>
```

Example:

```
0xAABBCC11226677889900AABBCCDDEEFF
```

EAP-SIM-OP attribute is a string type attribute and can exist only as a check attribute in User or Group profiles.

EAP-SIM-OPc

You can set the 128-bit value derived from OP and K for a user profile by adding EAP-SIM-OPc as a check attribute to a user profile. Use the following format.

```
0x<Hexadecimal encoded 16 Bytes string>
```

Example:

```
0xAABBCC11226677889900AABBCCDDEEFF
```

The *EAP-SIM-OPc* attribute is a string type attributes and can exist only as a check attribute in User or Group profiles.

EAP-SIM-Key

You can set the 128-bit subscriber key for a user profile by adding EAP-SIM-Key as a check attribute to a user profile. Use the following format

```
0x<Hexadecimal encoded 16 Bytes string>
```

Example:

```
0xAABBCC11226677889900AABBCCDDEEFF
```

EAP-SIM-Key attribute is a string type attribute and can exist only as a check attribute in User or Group profiles.

EAP-SIM-SQN

TekRADIUS automatically sets EAP-SIM-SQN attribute value for each successful EAP-AKA authentication attempt for a user profile. You do not need to add or edit this value. This value can be recovered by TekRADIUS based on AUTS response from the client.

EAP-SIM-SQN attribute is a string type attribute and can exist only as a check attribute in profiles.

HTTP-Access-Level

The *HTTP-Access-Level* attribute is used as a check attribute in User or Group profiles. This attribute specifies the user's access level to the TekRADIUS HTTP interface.

By default, all users have access to the TekRADIUS HTTP interface with user-level privilege, enabling them to view their own usage statistics. Admin rights can be granted to a User or Group profile by adding *HTTP-Access-Level = Admin* as a check attribute. Admin users can generate reports for all User and Group profiles. *HTTP-Access-Level = Operator* has a restricted level of user / group management *(Cannot add new users or groups, cannot change passwords)*. TekRADIUS will display user level form without usage reporting functions when you set *HTTP-Access-Level = Compact.* You need to have user-report.compact.html file with user-report.html if you use a custom user form.

HTTP-Access-Level is an integer type attribute and can exist as a check attribute in User or Group profiles.

HTTP-User-Name & HTTP-User-Password

If a user profile does not have a *User-Password* configured, *HTTP-User-Name* and *HTTP-User-Password* attributes can be added as check attributes to the user profile to enable access to the HTTP reporting interface. The *HTTP-User-Password* attribute must be added to the user profile if the *HTTP-User-Name* attribute is used.

HTTP-User-Name and *HTTP-User-Password* attributes are string type attributes and can exist as check attributes only in User profiles.

Password-Limit

You can apply password aging by adding Password-Limit attribute as a check attribute to user or group profiles. Password-Limit is specified by in minutes. TekRADIUS can request a new password if you implement MS-CHAP authentication methods in your RADIUS clients when the

password age is expired. TekRADIUS will add Password-Reset attribute to the user profile after a successful password change operation.

Password-Limit attribute is an integer type attribute and can exist as check attributes in User or Group profiles.

Password-Reset

TekRADIUS uses Password-Reset attribute to track password change periods with Password-Limit attribute. This attribute will be added/updated automatically after a successful password change operation. You can add Password-Reset set to a past date *(01.01.1970, e.g.)* with Password-Limit attribute as check attributes to a user profile manually to force the user to change his/her password at first logon.

Not all authentication methods provide a method to change user password. You need to deploy MS-CHAP based authentication methods to allow users to change their passwords.

Password-Reset attribute is string type attribute and can exist as check attributes only in User profiles.

Check-MS-DialinPrivilege

TekRADIUS does not check user dial-in privilege by default. You can enable it by adding Check-MS-DialinPrivilege = True as a check attribute to Default user group, proxy Windows user profile or TekRADIUS local group profile created for user's primary user group in Active Directory.

Check-MS-DialinPrivilege attribute is an integer type attribute and can exist as check attributes in User or Group profiles.

Lock-MAC-Address

You can restrict user logon from a specific computer, or an access device specified with its MAC address. TekRADIUS will add a Calling-Station-Id attribute as a check attribute automatically at the user's first logon attempt. TekRADIUS will check if user tries to log on from the same station successive logon attempts. You need to add Lock-MAC-Address = Yes as a check attribute to user or group profiles for this function.

Lock-MAC-Address attribute is an integer type attribute and can exist as check attributes in User or Group profiles.

Activation-Date

You can specify an activation date for user and group profiles by adding Activation-Date attribute as a check attribute. Authentication requests will be allowed after the specified date.

Activation-Date attribute is a date type attribute and can exist as check attributes in User or Group profiles.

Success-Reply-Type

TekRADIUS returns Access-Accept response to successful RADIUS authentication requests by default. You can alter this behavior to response back with Access-Challenge to successful RADIUS authentication requests. This is useful if you would like to return additional authentication tokens to RADIUS clients *(Please see OTP attributes below)*.

Success-Reply-Type attribute is an integer type attribute and can exist as check attributes in User or Group profiles.

OTP-Type

TekRADIUS can generate generic numeric or alphanumeric One-Time-Password, OTP strings. Generated OTP values are kept in %otp% variable and returned to RADIUS clients in Reply-Message attribute in Access-Accept or Access-Challenge responses. OTPs can be passed as a parameter to an executable specified in OTP-Sender through %otp% variable.

OTP-Type attribute is an integer type attribute and can exist as check attributes in User or Group profiles.

OTP-Length

You must have OTP-Length attribute in user or group profiles for generic OTP generation. This specifies character length for the OTP.

OTP-Length attribute is an integer type attribute and can exist as check attributes in User or Group profiles.

OTP-Sender

You can specify an external program, HTTP(S) URL or script to deliver generated generic OTP to remote users. Such applications typically deliver OTPs via e-mail or SMS messages. Please see External-Executable attribute for the syntax.

OTP-Sender attribute is a string type attribute and can exist as check attributes in User or Group profiles.

OTP-Timeout

Generated OTPs are good for 30 seconds. You can increase or decrease this timeout value in seconds by adding OTP-Time attribute to user or group profiles.

OTP-Timeout attribute is an integer type attribute and can exist as check attributes in User or Group profiles.

Accounting-Free

You can specify day and time periods for free usage for users. The allowed login days and hours can be limited for a user by adding *Accounting-Free* as a check attribute to the User or Group profile. When this attribute is added to a User or Group profile, TekRADIUS will not update user credit if the accounting request *(Interim update or Stop)* is received within the defined time period. The syntax of the *Accounting-Free* attribute is like *Login-Time* attribute;

```
[Su|Mo|Tu|We|Th|Fr|Sa|Wk|Hd|Al]<Begin Hour>-<End Hour>
```

Where:

Wk : Weekdays *(Working days based on your locale settings)*

Hd : Weekend *(Weekend days based on your local settings)*

Al : All days of the week *(All seven days of a week)*

Hours must be in 24-hour format (e.g., 22:55). Several periods may be defined by concatenating the periods with commas ‘,’. Every period is processed individually; ‘Tu11:00-12:00, Tu12:00-14:00’ is not interpreted as ‘Tu:11:00-14:00’. Longer periods are preferred over shorter periods when overlapping periods are defined. If ‘Tu12:00-14:00, Al13:00-17:00’ have been defined, TekRADIUS will prefer ‘Al13:00-17:00’ on Tuesdays at 13:30.

Examples:

- **Wk09:00-18:00, Hd12:00-16:00** will allow free usage from 09:00 to 18:00 during weekdays and from 12:00 to 16:00 at weekends.
- **Mo10:00-23:50, We10:00-23:50, Hd11:00-17:00** will allow free usage from 10:00 to 23:50 on Monday and Wednesday, and from 11:00 to 17:00 at weekends.
- **Al09:00-18:00, Fr08:00-19:00** will allow free usage from 09:00 to 18:00 for all days except Friday; free usage is allowed from 08:00 to 19:00 on Fridays.

Accounting-Free is a string type attribute and can exist only as a check attribute in User or Group profiles. This attribute is supported with SP license.

Upper and lower time can span across day boundaries. Al22:00-01:30 is valid, for instance.

Data-Volume-Based-Authorization

TekRADIUS adds vendor specific attributes to authorization reply if user credit type is data volume based depending on vendor. Please see Data Volume Based Authorization for more information. You can disable this behavior by adding Data-Volume-Based-Authorization = Disabled as a check attribute to user or group profiles.

Data-Volume-Based-Authorization attribute is an integer type attribute and can exist as check attributes in User or Group profiles.

Google-Authenticator-Secret

This attribute keeps encrypted secret for Google-Authenticator and is not visible in user profiles.

Google-Authenticator-Secret attribute is a string type attribute and can exist as a check attribute in User profiles.

Google-Authenticator-Issuer

TekRADIUS encodes only username in QR code for initialization of Google Authenticator for a user. You can also add an issuer name to be displayed when the user reads QR code. Add ~ character in front of issuer name if you prefer only issuer name to be displayed for the OTP in the mobile Authenticator application.

Google-Authenticator-Issuer attribute is a string type attribute and can exist as check attributes in User or Group profiles.

Quota-Warning-Action

You can execute an action to send a notification to user when user's credit consumption reaches to a certain level. This can be an SMS or e-mail message. You can invoke an external executable to send such a notification message. Please see External-Executable attribute for the syntax.

External-Executable is a string type attribute and can exist only as a check attribute in User or Group profiles.

Quota-Warning-Threshold

You need to specify a threshold value if you plan to issue a warning when user consumption reaches a certain level. This can be done by adding a Quota-Warning-Threshold attribute to user or group profiles as a check attribute. Its value is based on credit amount. If you plan to issue a warning when user consumption reaches 80% and users' credit is set to 8000, you should set Quota-Warning-Threshold = 6400.

Quota-Warning-Threshold attribute is an integer type attribute and can exist as check attributes in User or Group profiles.

Concatenated-Password

Concatenated-Password attribute allows you to specify a regular expression pattern to split received User-Password in an authentication request. TekRADIUS will update User-Password to value captured with regular expression capture group named **password**. You can get other parts using a capture group named **auxstr**. TekRADIUS will use updated User-Password in primary authentication method specified for the user. You can pass "auxstr" value in `%auxstr%` variable as a parameter to an executable specified with External-Executable. This is useful when you need to implement two factor authentication with an access server which does not support RADIUS challenges. This attribute requires a commercial license. Here is a sample.

```
Concatenated-Password = (?<auxstr>[^,]+),(?<password>.+)
```

Regular expression patterns must contain **password** and **auxstr** named capture groups. This regular expression splits received passwords concatenated with a comma in User-Password attribute and sets User-Password to second part of the original User-Password value. Captured first part value assigned to `%auxstr%` variable.

Please note that you can use this feature only when PAP authentication method is deployed.

Concatenated-Password is a string type attribute and can exist only as a check attribute in User or Group profiles.

External-Accounting-Action

This attribute enables you to perform RADIUS accounting externally. You can specify an external executable which you can pass received attributes in RADIUS accounting requests as command line parameter. This attribute is available with SP license. Please see External-Executable attribute for the syntax.

You can use External-Accounting-Action if you plan to process incoming accounting packets using a stored procedure. Add "sql:" prefix (Without quotation marks) to your SQL statement and specify as External-Accounting-Action. Example;

```
sql:exec dbo.CommitAccounting '%ietf|40%', '%ietf|1%', '%ietf|4%', '%ietf|44%'
```

External-Accounting-Action is a string type attribute and can exist only as a check attribute in User or Group profiles.

Allowed-SSID

Allowed-SSID attribute allows you to specify which wireless networks are allowed for user login. You can specify more than one network by concatenating them using commas.

Allowed-SSID is a string type attribute and can exist only as a check attribute in User or Group profiles.

DHCP-Server

You can specify a DHCP server to acquire an IP address for the user when Framed-IP-Address = Acquire-Using-DHCP in user or group profile. TekRADIUS will request an IP address directly by issuing a DHCP request to broadcast address if this attribute does not exist in user or group profile.

DHCP-Server is an IP address type attribute and can exist only as a check attribute in User or Group profiles.

Description

The Description attribute allows you to add descriptive information to a user or group profile. It has no use in RADIUS AAA operations.

Description is a string type attribute and can exist only as a informational attribute in User or Group profiles.

Client-Label

You can set a group label for client entries specified in TekRADIUS Manager / Clients tab. You can specify the assigned group label as a check attribute by adding Client-Label attribute as a check attribute to user or group profiles. This will enable you to restrict user authentication attempts from a specific group of NAS devices.

Client-Label is a string type attribute and can exist only as a check attribute in User or Group profiles.

Email-Address

You can add an email address to user profile using Email-Address attribute. TekRADIUS uses this email address to send user notification when "Send User Notifications" option is enabled in Settings / Alerting. Email-Address is also required to send Google Authenticator key manually embedded in an email.

Email-Address is a string type attribute and can exist as a check or informational attribute in only User profiles.

TLS-Allowed-CA

TekRADIUS accepts EAP-TLS authentication requests if the client submits a valid certificate if Req. Local Cet. For EAP-TLS option is not set. You can limit this behavior by specifying allowed Certificate Authorities as client certificate signers. You can select multiple certificate authorities.

TLS-Allowed-CA is a string type attribute and can exist only as a check attribute in User or Group profiles.

Simultaneous-Limit-Action

You can instruct TekRADIUS what action will be performed when an authentication request is received with simultaneous session count is limited *(Either with Simultaneous-Use or Simultaneous-Group-Use)* Default action to reject authentication request when the session limit is reached. But you can instruct TekRADIUS to disconnect the oldest user session by adding Simultaneous-Limit-Action = Disconnect-Oldest as a check attribute.

Simultaneous-Limit-Action is an integer type attribute and can exist only as a check attribute in User or Group profiles.

NAS-Vendor

You can limit a user to login from a NAS device belonging to a particular vendor by adding NAS-Vendor attribute to user or group profiles.

NAS-Vendor is an integer type attribute and can exist only as a check attribute in User or Group profiles.

Request-Certificate

You can add Request-Certificate attribute to user or group profile to accomplish mutual server-client authentication while establishing PEAP and EAP-TTLS outer tunnels.

Request-Certificate is an integer type attribute and can exist only as a check attribute in User or Group profiles.

X509-Revocation-Mode

X509-Revocation-Mode attribute enables you to control the behavior of TekRADIUS while checking client certificate revocation status in EAP-TLS authentication. Possible values;

- **NoCheck**. No revocation check is performed on the certificate.
- **Online**. A revocation check is made using an online certificate revocation list (CRL).
- **Offline**. A revocation check is made using a cached certificate revocation list (CRL).

X509-Revocation-Mode is an integer type attribute and can exist only as a check attribute in User or Group profiles.

TekRADIUS-Logging

You can add Request-Certificate attribute to user or group profile to set a individual logging level user or group level. This allows you to have detailed logging for users or groups If you keep log level low to save disc space.

TekRADIUS-Logging is an integer type attribute and can exist only as a check attribute in User or Group profiles.

Lock-IMEI

You can restrict access from a specific modem/mobile device, or an access device specified with its IMEI. TekRADIUS will add the 3GPP-IMEISV attribute as a check attribute automatically at the user's first logon attempt. TekRADIUS will check if users try to log on from the same device successive logon attempts. You need to add Lock-IMEI = Yes as a check attribute to user or group profiles for this function.

Lock- IMEI attribute is an integer type attribute and can exist as check attributes in User or Group profiles.

Data Volume Based Authorization

The RADIUS protocol provides a standard way to instruct access servers or Network Access Servers *(NAS)* to limit the maximum session time for an authorized user by the *Session-Timeout* parameter. Unfortunately, the RADIUS protocol does not provide a standard way to instruct the NAS to restrict the session based on a maximum amount of data that can be uploaded or downloaded; however, some vendors provide Vendor Specific Attributes *(VSA)* for this purpose:

Mikrotik

- Mikrotik-Recv-Limit, 32-bit value of number of allowed input-octets.
- Mikrotik-Recv-Limit-Gigawords *(Giga count for each 4 GByte)*
- Mikrotik-Xmit-Limit, 32-bit value of number of allowed output octets.
- Mikrotik-Xmit-Limit-Gigawords *(Giga count for each 4 GByte)*
- Mikrotik-Total-Limit, 32-bit value of number of allowed total octets.
- Mikrotik-Total-Limit-Gigawords *(Giga count for each 4 GByte)*

Nomadix

- Nomadix-MaxBytesUp, 32-bit value of number of allowed input octets.
- Nomadix-MaxBytesDown, 32-bit value of number of allowed output octets.

Chillispot

- ChilliSpot-Max-Input-Octets, 32-bit value of number of allowed input octets.
- ChilliSpot-Max-Input-Gigawords *(Giga count for each 4 GByte)*
- ChilliSpot-Max-Output-Octets, 32-bit value of number of allowed output octets.
- ChilliSpot-Max-Output-Gigawords *(Giga count for each 4 GByte)*
- ChilliSpot-Max-Total-Octets, 32-bit value of number of allowed total octets.
- ChilliSpot-Max-Total-Gigawords *(Giga count for each 4 GByte)*

Colubris

- Colubris-AVPAIR=max-input-octets=<32-bit value of number of allowed input octets>
- Colubris-AVPAIR=max-output-octets=<32-bit value of number of allowed output octets>

Ericsson *(Former Redback)*

- Session-Traffic-Limit=in:<Inbound traffic allowed in KBytes>.
- Session-Traffic-Limit=out:<Outbound traffic allowed in KBytes>.
- Session-Traffic-Limit=aggregate:<Aggregate traffic allowed in KBytes>

Juniper *(Former ERX/Unisphere)*

- ERX-Service-Volume=< Aggregate traffic allowed in Bytes>
- ERX-Service-Volume-Gigawords *(Giga count for each 4 GByte)*

TekRADIUS uses the *User-Credit* attribute to store user quotas, which can be set using the *Credit-Unit* attribute. The *Credit-Unit* attribute can have the following values:

- Seconds
- Minutes
- Bytes-in
- KBytes-in
- MBytes-in
- Bytes-out
- KBytes-out
- MBytes-out
- Bytes-sum
- KBytes-sum
- MBytes-sum

If the *User-Credit* attribute exists in a user profile and is set to a value other than *Seconds* or *Minutes*, TekRADIUS SP will add following attributes to the *Success-Reply* message depending on the vendor of the NAS. You can disable this behavior by adding Data-Volume-Based-Authorization = Disabled as a check attribute to user or group profiles.

	Bytes-in, KBytes-in, MBytes-in	Bytes-out, KBytes-out, MBytes-out	Bytes-sum, KBytes-sum, MBytes-sum
Mikrotik	Mikrotik-Recv-Limit	Mikrotik-Xmit-Limit	Mikrotik-Total-Limit
Nomadix	Nomadix-MaxBytesDown	Nomadix-MaxBytesUp	Nomadix-MaxBytes-Total
Chillispot	ChilliSpot-Max-Input-Octets	ChilliSpot-Max-Output-Octets	ChilliSpot-Max-Total-Octets
Colubris	Colubris-AVPAIR=max-input-octets	Colubris-AVPAIR=max-output-octets	Colubris-AVPAIR=max-output-octets
Ericsson	Session-Traffic-Limit= in:<Traffic in KB>	Session-Traffic-Limit= out:<Traffic in KB>	Session-Traffic-Limit= aggregate:<Traffic in KB>
Jun,ğer	N/A	N/A	ERX-Service-Volume=< Aggregate traffic allowed in Bytes>

The values of these attributes are set to the value of *User-Credit* specified in the User profile. TekRADIUS will update the *User-Credit* value as RADIUS *Accounting-stop* or *Checkpoint (Interim-Update)* messages are received. This feature is available in SP edition only.

Vendor Specific Attribute for Connection Rate Limiting

The RADIUS protocol does not provide a standard way to limit user connection rates which could be useful to apply fair usage policies. Some vendors provide Vendor Specific Attributes *(VSA)* for connection rate limiting. Here is a list of vendor specific attributes to limit user connection rate for 1 Mbps download and 128 Kbps upload;

Mikrotik

- Mikrotik-Rate-Limit, 128k/1024k *(or 128k/1M)*

H3C

- H3C-Input-Average-Rate = 131072
- H3C-Input-Peak-Rate = 131072
- H3C-Output-Average-Rate = 1048576
- H3C-Output-Peak-Rate = 1048576

Huawei

- Huawei-Input-Average-Rate = 131072
- Huawei-Input-Peak-Rate = 131072
- Huawei-Output-Average-Rate = 1048576
- Huawei-Output-Peak-Rate = 1048576

ZTE

- ZTE-Rate-Ctrl-Scr-Up = 131072
- ZTE-Rate-Ctrl-Scr-Down = 1048576

Cisco *(ISG)*

- Cisco-AVPair = ip:sub-policy-Out=Out_Policy,ip:sub-policy-In=In_Policy

Juniper *(ERX/Unisphere)*

- ERX-Max-Data-Rate-Up = 131072
- ERX-Max-Data-Rate-Dn = 1048576

You need to have a policy map defined in the ISG for specified policies;

```
policy-map Out_Policy
class class-default
shape average 1024000
policy-map In_Policy
class class-default
police 128000
```

Cisco *(PPP)*

- Cisco-AVPair=lcp:interface-config#1=rate-limit input 128000 128000 128000 conform-action transmit exceed-action drop,lcp:interface-config#1=rate-limit output 1024000 1024000 1024000 conform-action transmit exceed-action drop

Change of Authorization Support for Disconnecting User Sessions

You can disconnect user sessions by sending a Disconnect Message as described in RFC 5176 *(RFC 3756)*. Disconnect Message, DM *(a.k.a Packet of Disconnect or PoD)*, is a special form Change of Authorization packet but its special purpose is to disconnect a user session.

You can disconnect user sessions through the Active Sessions tab. You can select sessions to be disconnected and click "Disconnect" button. TekRADIUS will send a PoD packet to NAS. Attributes in a PoD packet are selected based on vendor specified for the NAS in Clients tab. Here is a list of attributes sent in PoD packets based on vendors;

Generic

- User-Name
- Acct-Session-Id
- Acct-Multi-Session-Id (If exists)
- Calling-Station-Id
- Called-Station-Id
- Framed-IP-Address
- NAS-Port
- NAS-IP-Address
- Cisco-AVPair = audit-session-id

Cisco

- User-Name
- Calling-Station-Id
- Framed-IP-Address
- *Service-Type*

Mikrotik

- User-Name
- Framed-IP-Address
- NAS-Port
- NAS-Port-Type
- Calling-Station-Id

Xirrus

- Calling-Station-Id

Aruba

- User-Name
- NAS-IP-Address
- Framed-IP-Address
- Calling-Station-Id

Meraki

- Event-Timestamp

Ericsson

- User-Name

Juniper (ERX/Unisphere)

- User-Name
- Acct-Session-Id

Attributes received in Accounting-Start packets will be added to PoD packets *(Only exception is Service-Type attribute in Cisco PoDs)*. Try IETF, if you experience problems when you select Cisco as then vendor.

TekRADIUS SP edition can send a PoD or CoA packet when the user consumes all credit specified in the user profile. This can be set by adding Credit-Expiry-Action = Send-PoD or Credit-Expiry-Action = Send-CoA respectively as a check attribute to user or group profile. RADIUS interim accounting must be enabled in the NAS device in order for this feature works. You must also configure CoA-Set attributes in user or group profile for Send-CoA option.

HTTP Interface

TekRADIUS SP comes with an HTTP interface for basic user management and reporting tasks. To access the HTTP interface the built-in HTTP server must be enabled in **Settings / Service Parameters**. The HTTP Interface can be accessed by typing **http://<Listen IP Address>:<HTTP Port>**. The HTTP port can be changed in **Settings / Service Parameters**.

There are four access levels to HTTP Interface: User, Compact, Operator, Admin levels. All users have User Level access to the HTTP Interface. Users should enter their usernames and passwords specified in the *User-Password* attribute in their profiles. For Admin access it is necessary to add *HTTP-Access-Level = Admin* as a check attribute to User or Group profiles. Please see HTTP-Access-Level attribute.

TekRADIUS has five built-in html pages/forms for the HTTP Interface. New, custom forms may be designed, using predefined form fields and variables.

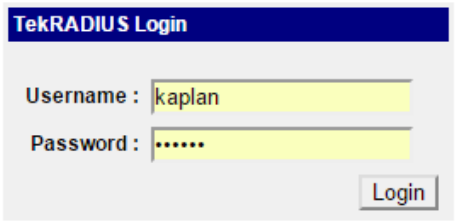
To override the built-in forms, create the following files and put them into the TekRADIUS application directory.

login.html

This html form contains the username and password entry fields.

Login form must contain following form and fields;

```
<form name="LoginForm" method="post" action="login" id="TekRADIUSLoginForm">
 <input name="Username" type="Text" id="Username">
 <input name="Password" type="Password" id="Password">
 <input type="submit" name="Login" value="Login" id="Login">
</form>
```



error.html

This form displays error messages generated by the built-in HTTP server.

Error form must contain following predefined variable;

`%error%` *(Error message generated by built-in HTTP server)*

Reporting Interface

Reporting interface is functionally equivalent to the reporting interface available in the TekRADIUS Manager GUI.

admin-report.html

This form provides access to Admin HTTP Interfaces. Admin users can query all user's data.

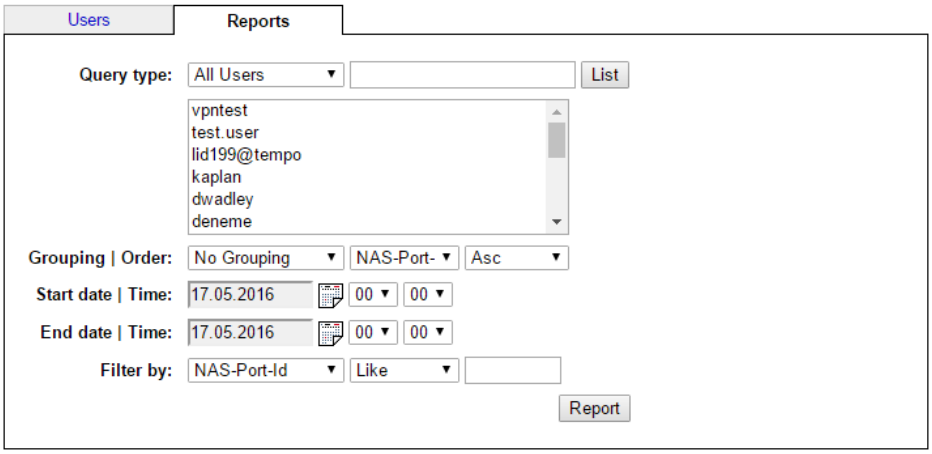
Admin report form must contain the following form, fields and Javascripts. The `Initialize()` function must be invoked in `<body onload="Initialize();">`.

```
<script language="javascript" type="text/javascript">
```

```
    function Initialize() {
    var chk = '%grouping%';
    var z;
    var MyElement = document.getElementById('QueryType');

    if (chk!='') {
     for (z = 0; z < MyElement.options.length; z++)
     {if (MyElement.options[z].value == '%querytype%') {MyElement.options[z].selected = true;}}

     MyElement = document.getElementById('Grouping');

     for (z = 0; z < MyElement.options.length; z++)
     {if (MyElement.options[z].value == '%grouping%') {MyElement.options[z].selected = true;}}

     MyElement = document.getElementById('OrderDirection');

     for (z = 0; z < MyElement.options.length; z++)
     {if (MyElement.options[z].value == '%orderdirection%') {MyElement.options[z].selected = true;}}

     MyElement = document.getElementById('StartHour');

     for (z = 0; z < MyElement.options.length; z++)
     {if (MyElement.options[z].value == '%starthour%') {MyElement.options[z].selected = true;}}

     MyElement = document.getElementById('EndHour');

     for (z = 0; z < MyElement.options.length; z++)
     {if (MyElement.options[z].value == '%endhour%') {MyElement.options[z].selected = true;}}

     MyElement = document.getElementById('StartMinute');

     for (z = 0; z < MyElement.options.length; z++)
     {if (MyElement.options[z].value == '%startminute%') {MyElement.options[z].selected = true;}}

     MyElement = document.getElementById('EndMinute');

     for (z = 0; z < MyElement.options.length; z++)
     {if (MyElement.options[z].value == '%endminute%') {MyElement.options[z].selected = true;}}

     MyElement = document.getElementById('FilterCondition');

     for (z = 0; z < MyElement.options.length; z++)
     {if (MyElement.options[z].value == '%filtercondition%') {MyElement.options[z].selected = true;}}
    }
    Grouping_onclick();
    }

        function fixPosition(divname) {
            divstyle = getDivStyle(divname);
            positionerImgName = divname + 'Pos';
            isPlacedUnder = false;
            if (isPlacedUnder) {
                setPosition(divstyle, positionerImgName, true);
            } else {
                setPosition(divstyle, positionerImgName)
            }
        }

        function toggleDatePicker(eltName, formElt) {
            var x = formElt.indexOf('.');
            var formName = formElt.substring(0, x);
            var formEltName = formElt.substring(x + 1);
            newCalendar(eltName, document.forms[formName].elements[formEltName]);
            toggleVisible(eltName);
        }

        function fixPositions() {
            fixPosition('daysOfMonth');
            fixPosition('daysOfMonth2');
        }

        function Cancel() {
            hideElement("daysOfMonth");
        }

        hideElement('daysOfMonth');
        hideElement('daysOfMonth2');

        function Grouping_onclick() {
            var OrderByOptions1 = new Array(%OrderByOptions1%);
            var OrderByOptions2 = new Array("Time Usage", "Data In", "Data Out", "Data Sum");
            var FilterByOptions1 = new Array(%FilterByOptions1%);
            var FilterByOptions2 = new Array("Sum Data In", "Sum Data Out", "Sum Data Agg", "Sum
Duration", "Over Usage");
            var sel1 = document.getElementById("OrderBy");
            var sel2 = document.getElementById("FilterBy");
            var z;

            sel1.innerHTML = "";
            sel2.innerHTML = "";

            if (document.getElementById("Grouping").value == "No Grouping") {

            document.getElementById('StartHour').style.visibility='visible';
```

```
            document.getElementById('EndHour').style.visibility='visible';
            document.getElementById('StartMinute').style.visibility='visible';
            document.getElementById('EndMinute').style.visibility='visible';

            for (i=0; i<OrderByOptions1.length; i++)
                {sel1.options.add(new Option(OrderByOptions1[i], OrderByOptions1[i]));}
            for (i=0; i<FilterByOptions1.length; i++)
                {sel2.options.add(new Option(FilterByOptions1[i], FilterByOptions1[i]));}
            } else {

            document.getElementById('StartHour').value = '00';
            document.getElementById('EndHour').value = '00';
            document.getElementById('StartMinute').value = '00';
            document.getElementById('EndMinute').value = '00';
            document.getElementById('StartHour').style.visibility='hidden';
            document.getElementById('EndHour').style.visibility='hidden';
            document.getElementById('StartMinute').style.visibility='hidden';
            document.getElementById('EndMinute').style.visibility='hidden';

            for (i=0; i<OrderByOptions2.length; i++)
                {sel1.options.add(new Option(OrderByOptions2[i], OrderByOptions2[i]));}
            for (i=0; i<FilterByOptions2.length; i++)
                {sel2.options.add(new Option(FilterByOptions2[i], FilterByOptions2[i]));}
            }

                 for (z = 0; z < sel1.options.length; z++)
                 {if (sel1.options[z].value == '%orderby%') {sel1.options[z].selected = true;}}

                 for (z = 0; z < sel2.options.length; z++)
                 {if (sel2.options[z].value == '%filterby%') {sel2.options[z].selected = true;}}
        }

    function QueryType_onchange() {
     document.ReportForm.submit();
    }

</script>

    <form name="ReportForm" method="post" action="report" id="TekRADIUSReportForm">
    <select id="QueryType" name="QueryType">
     <option selected="selected">All Users</option>
     <option>User</option>
     <option>Group</option>
    </select>
    <input id="QueryName" name="QueryName" type="text" value="%queryname%" />
    <select id="SelectedUser" name="SelectedUser" size="6">
     %selecteduser%
    </select>
    <select id="Grouping" name="Grouping" onchange="Grouping_onclick()">
     <option>No Grouping</option>
     <option>Day</option>
     <option>Week</option>
     <option>Month</option>
     <option>All records</option>
    </select>
    <select id="OrderBy" name="OrderBy">
     %orderbyops%
    </select>
    <select id="OrderDirection" name="OrderDirection">
     <option>Asc</option>
     <option>Desc</option>
    </select>
    <input id="StartDate" name="StartDate" size="10" value="%startdate%">
    <select id="StartHour" name="StartHour">
     <option>00</option>
     :
     <option>23</option>
    </select>
    <select id="StartMinute" name="StartMinute">
     <option>00</option>
     :
     <option>59</option>
    </select>
    <input id="EndDate" name="EndDate" size="10" value="%enddate%">
    <select id="EndHour" name="EndHour">
     <option>00</option>
     :
     <option>23</option>
     </select>
     <select id="EndMinute" name="EndMinute">
      <option>00</option>
     :
     <option>59</option>
    </select>
    <select id="FilterBy" name="FilterBy">
     %filterbyops%
    </select>
    <select id="FilterCondition" name="FilterCondition">
     <option>Like</option>
     <option>Equal</option>
```

```
 <option>Not equal</option>
 <option>Greater</option>
 <option>Less than</option>
</select>
<input id="FilterValue" name="FilterValue" type="text" value="%filtervalue%" />
<input id="Report" name="Report" type="submit" value="Report" />
</form>
```

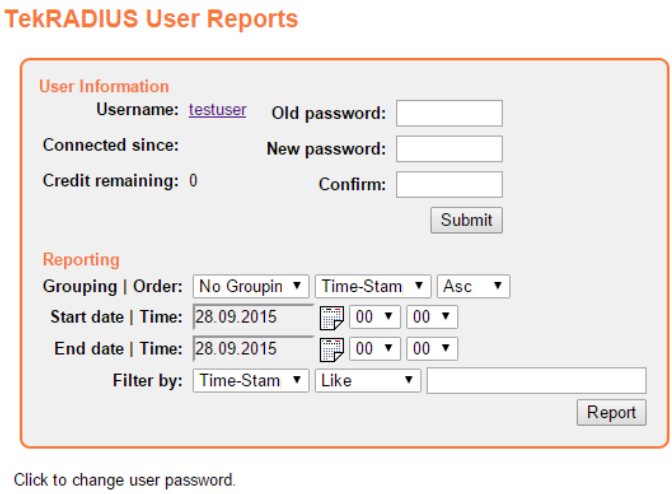


user-report.html

This form provides access to the User HTTP Interface. Regular users can query only their usage data.

The User form contains the same variables, form controls and Javascripts as the Admin report form, except the `<select id="QueryType" name="QueryType">` form field and the `Initialize()` function; these are implemented as:

```
function Initialize() {
  var chk = '%grouping%';
  var MyElement, z;

  if (chk!='') {
   MyElement = document.getElementById('Grouping');

   for (z = 0; z < MyElement.options.length; z++)
   {if (MyElement.options[z].value == '%grouping%') {MyElement.options[z].selected = true;}}

   MyElement = document.getElementById('OrderDirection');

   for (z = 0; z < MyElement.options.length; z++)
   {if (MyElement.options[z].value == '%orderdirection%') {MyElement.options[z].selected = true;}}

   MyElement = document.getElementById('StartHour');

   for (z = 0; z < MyElement.options.length; z++)
   {if (MyElement.options[z].value == '%starthour%') {MyElement.options[z].selected = true;}}

   MyElement = document.getElementById('EndHour');

   for (z = 0; z < MyElement.options.length; z++)
   {if (MyElement.options[z].value == '%endhour%') {MyElement.options[z].selected = true;}}

   MyElement = document.getElementById('StartMinute');

   for (z = 0; z < MyElement.options.length; z++)
   {if (MyElement.options[z].value == '%startminute%') {MyElement.options[z].selected = true;}}

   MyElement = document.getElementById('EndMinute');

   for (z = 0; z < MyElement.options.length; z++)
   {if (MyElement.options[z].value == '%endminute%') {MyElement.options[z].selected = true;}}

   MyElement = document.getElementById('FilterCondition');

   for (z = 0; z < MyElement.options.length; z++)
   {if (MyElement.options[z].value == '%filtercondition%') {MyElement.options[z].selected = true;}}
  }

  Grouping_onclick();
 }
```



The username can be utilized by adding the `%username%` variable, the connection time by adding the `%connected%` variable, and the remaining user credit by adding the `%remained%` variable in the user report form.

The default report forms do not have log out function; TekRADIUS HTTP server clears user sessions after the HTTP Session timeout expires, specified in **Settings / Service Parameters**.

A log out button may be added by including the following form object to ReportForm:

```
<input id="Logout" name="Logout" type="submit" value="Logout" />
```

To hide the report summary *(Total 0 session(s) found, 0 KByte(s) transferred, 0 minutes),* the following form object can be added:

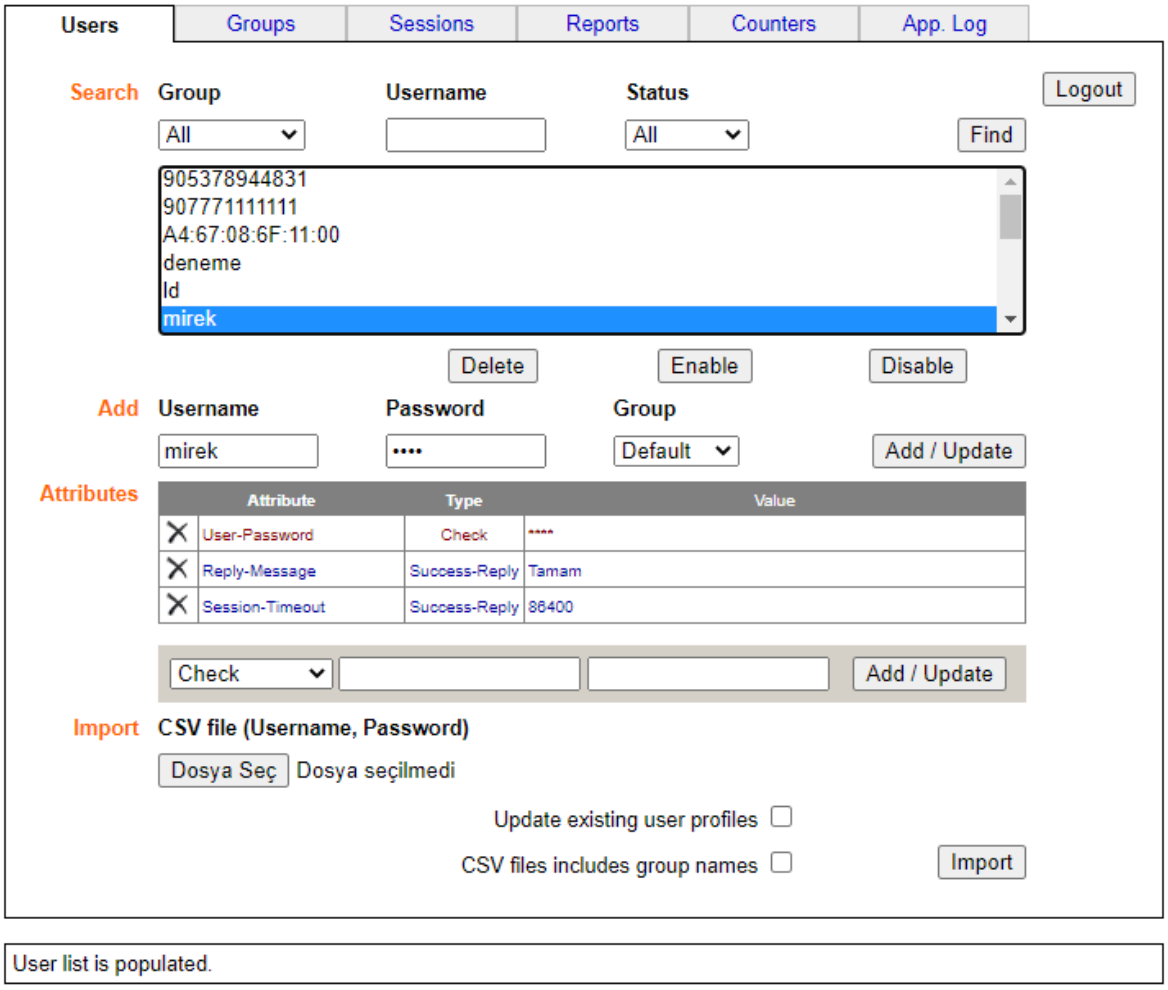
```
<input type="hidden" id="HideSummary" name="HideSummary" value="True">
```

You can have a password change only user-report.html or combine with reporting features listed above;

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<head>
    <title>Change User Password</title>
</head>
<body>
    <form name="PasswordForm" method="post" action="changepass" id="TekRADIUSPasswordForm">
    <table align="left" id="TekRADIUSPasswordTable">
        <tr>
            <td align="right" valign="top">
                <strong>Old password: </strong>
                <input id="oldpassword" name="oldpassword" type="password" value="" />
            </td>
        </tr>
        <tr>
            <td align="right" valign="top">
                <strong>New password: </strong>
                <input id="newpassword" name="newpassword" type="password" value="" />
            </td>
        </tr>
        <tr>
            <td align="right" valign="top">
                <strong>Confirm: </strong>
                <input id="confirmpassword" name="confirmpassword" type="password" value="" />
            </td>
        </tr>
        <tr>
            <td align="right" valign="top">
                <input id="ChangePass" name="ChangePass" type="submit" value="Submit" />
            </td>
        </tr>
    </table>
    </form>
</body>
</html>
```

User Management Interface

HTTP based user management interface allows you create user profiles assigned to existing user groups. You can enable, disable, delete, change membership and update passwords for existing user profiles. You can also import user accounts in CSV files. Username and Password pairs must be delimited with comma "," *(without quotes)* and each user entry must be kept in a separate line terminated with Carriage Return + Line Feed. You can also optionally add a group name.



You can also configure attributes for the user profiles. Refer to TekRADIUS dictionary for the attributes can be configured for the user and group profiles.

Sample html forms can be downloaded from the TekRADIUS support site.

RADIUS Proxy

TekRADIUS can proxy incoming RADIUS requests to other RADIUS servers. RADIUS proxying is supported in SP editions of TekRADIUS. You need to have RADIUS proxy profiles and each profile has remote server entries. You can create RADIUS proxy profiles at Proxy tab at Proxy tab of TekRADIUS Manager.

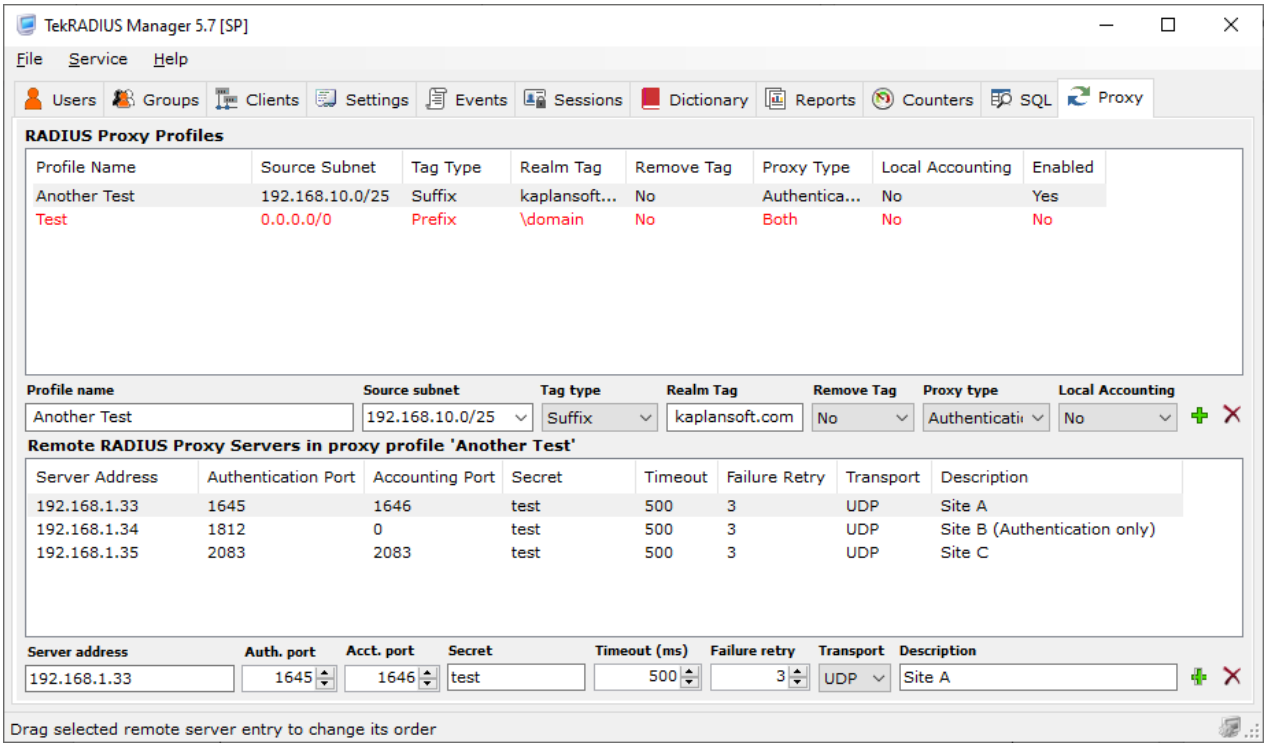


Figure 24. - TekRADIUS Proxy Profiles

Proxy profile matching is performed with source IP subnet of RADIUS clients and realm tags found in User-Name attributes found in RADIUS requests. You can perform Authentication or Accounting only proxying. You can also locally process proxied RADIUS accounting requests. A newly created RADIUS profile is disabled by default. You can enable it by double clicking RADIUS profile entry.

You need to have at least one remote server entry for a RADIUS proxy profile. You can change the order of remote servers by dragging entries. If you set RADIUS authentication port = 0 and RADIUS accounting port a value other than 0, specified RADIUS server will be used just for accounting vice versa. You cannot set both ports to zero for a RADIUS Proxy server entry.

IPv6 Attributes

TekRADIUS supports IPv6 attributes specified in RFC 3162, RFC 4818 and RFC 6911. Please use the following syntax rules when entering these attributes to user and group profiles.

IPv6 Address

An IPv6 address consists of 128 bits and is presented in eight 16-bit blocks. Each 16-bit block is converted to a four-digit hexadecimal number. Blocks are separated by colons.

Example: `2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A`

A contiguous sequence of 16-bit blocks set to 0 can be replaced with double colon (::). Zero compression can only be applied once in an IP address. To determine how many blocks have been omitted, you just have to count the remaining blocks and subtract this number from 8.

`FE80:0:0:0:2AA:FF:FE9A:4CA2` can be zero compressed to `FE80::2AA:FF:FE9A:4CA2`.

IPv6 Prefix

IPv6 prefixes are used to specify IPv6 subnets, routes, and address ranges. The syntax of IPv6 prefixes in address/prefix-length format. It is similar to the Classless Inter-Domain Routing *(CIDR)* notation for IPv4 *(for instance, 192.168.0.0/16 represents a Class B subnet)*. Subnet masks are no longer used in IPv6.

Example: `21DA:D3:0:2F3B::/64` represents a subnet of 264 addresses, where the first 64 bits are fixed and the last 64 bits are variable.

IPv6 Interface Id

The last 64 bits of an IPv6 address are the interface identifier that is unique to the 64-bit prefix of the IPv6 address. You need to enter Framed-Interface-Id attribute in aaaa:bbbb:cccc:ddddd format. Each block concatenated with semicolons represents a 16 bits hexadecimal number.

Example: `10:1:1:1`

Troubleshooting

Error messages can be viewed on the TekRADIUS Manager Status bar or in the log file for the TekRADIUS service. Logging is enabled in the **Settings /Service Parameters** tab.

There are five levels of logging: None, Errors, Sessions, Debug and Developer. If Errors is selected, TekRADIUS logs just error messages. If Sessions is selected, both Session *(Authentication and Accounting)* and Error messages will be logged. Debug logs session and error messages along with additional transaction information. The developer logs all the information contained in the Debug setting plus packet decodes of the RADIUS messages received. The TekRADIUS Service must be restarted if the logging level setting is changed.

Log files are located in the **<Application Directory>\Logs** directory. Use logging only when needed as it has a negative impact on performance.

Startup errors and warnings are logged in the Application Log of the Windows Event Viewer. TekRADIUS related Application Log entries can be viewed in the **Event** tab of TekRADIUS Manager. The events listed in the Application Log tab are not refreshed automatically unless 'Enable Auto Refresh' is checked. The list can be refreshed manually by clicking the **Refresh Log** button. The **Clear Log** button clears logging messages but use it with care; it also clears all Application Log entries in Windows Event Viewer.

TekRADIUS counters may be monitored using Windows Performance Monitor *(Perfmon.exe)*.

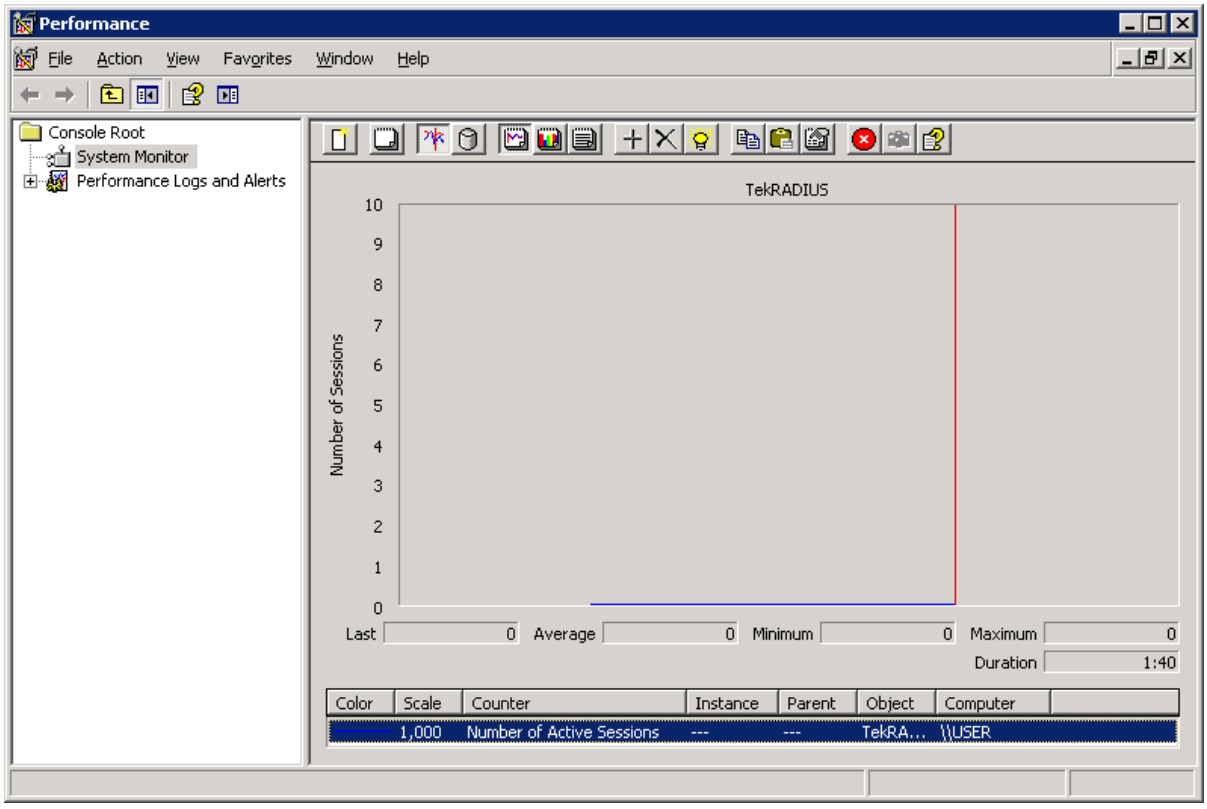


Figure 25. - TekRADIUS Counters on Windows Performance Monitor

TekRADIUS provides numerous counters:

- Number of Active Sessions
- RADIUS accounting requests received
- RADIUS authentication requests received
- RADIUS accounting errors
- RADIUS authentication errors
- RADIUS unauthorized accounting requests received
- RADIUS unauthorized authentication requests received
- RADIUS successful authentication requests received
- RADIUS failed authentication requests received
- RADIUS accounting requests receive rate
- RADIUS authentication requests receive rate
- RADIUS accounting errors rate
- RADIUS authentication errors rate
- RADIUS accounting-start requests received
- RADIUS accounting-stop requests received
- RADIUS accounting-start requests processed
- RADIUS accounting-stop requests processed

These counters can also be monitored through TekRADIUS Manager within the **Counters** tab.

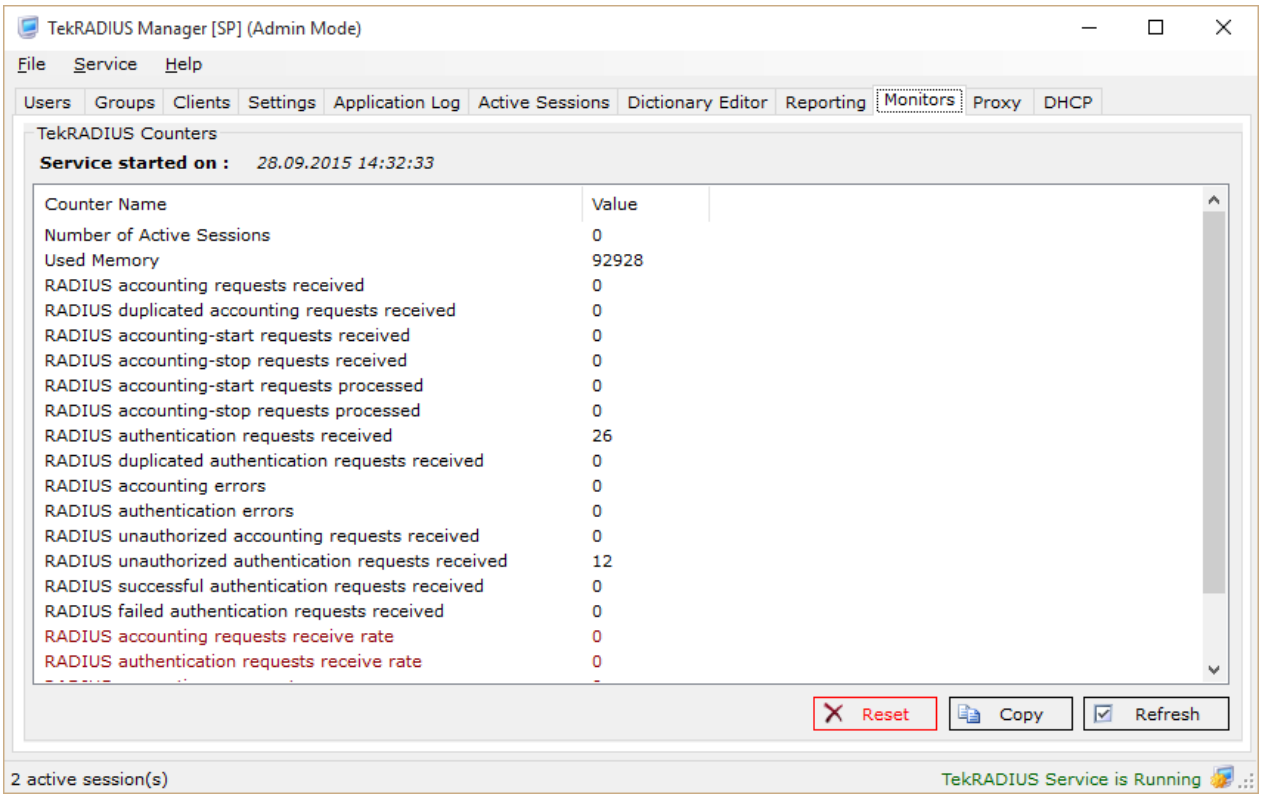


Figure 26. - TekRADIUS Manager Counters Tab

TekRADIUS Service Messages (TekRADIUS log file)

TekRADIUS Service is being started.

This message provides notification that the TekRADIUS service is being started.

Settings could not be loaded. Please reconfigure.

The settings file (*TekRADIUS.ini'* in the application directory) cannot be found or is corrupted. Examine the file for corruption or reconfigure TekRADIUS.

Create missing tables on SQL Server, exiting.

TekRADIUS needs, at a minimum, the Users and Groups tables to be created in the TekRADIUS database. If TekRADIUS cannot find one of these tables, startup will terminate.

Accounting or Sessions table missing, disabling Accounting...

TekRADIUS Accounting implementation needs both the Accounting and Sessions tables to be created in the TekRADIUS database. If TekRADIUS cannot find one of these tables, accounting will be disabled.

No client defined, check 'Clients' table in TekRADIUS.db.

TekRADIUS's RADIUS protocol implementation requires that client IP addresses and their corresponding secret keys are listed in the 'Clients' table in the TekRADIUS.db file, located in the application directory. This file is automatically generated by TekRADIUS Manager when the RADIUS clients are defined. TekRADIUS cannot authenticate an incoming request without the Client's secret keys; if this file cannot be found or read at startup, TekRADIUS terminates startup.

TekRADIUS Service is being stopped.

This message provides notification that the TekRADIUS service is being stopped.

No vendor defined, check 'Vendors' table.

TekRADIUS reads the vendor ID's from the 'Vendors' table in the TekRADIUS.db. If a valid entry for a vendor could not be found in the 'Vendors' table, those VSAs associated with that vendor are ignored when authenticating the user, and reply attributes configured for the vendor are not sent to the NAS. Similarly, unknown vendor attributes in RADIUS Accounting messages are simply ignored. If a VSA is configured for a particular user and the vendor ID is removed from the 'Vendors' table, TekRADIUS Manager will automatically delete the VSA associated with that vendor from the Users profile when that user is selected.

No Attributes defined, check 'Attributes' table in TekRADIUS.db.
No value defined, check 'Values' table in TekRADIUS.db.

TekRADIUS cannot be run without reading the 'Dictionary' tables at startup from the TekRADIUS.db file, located in the application directory.

Could not connect to SQL Server.

This is a general error message indicating that the SQL server cannot be reached. If this happens at startup, TekRADIUS continues the startup process but it is necessarily need to check what has going wrong; please see the SQL Server Configuration section of this manual. The most common causes include not enabling TCP/IP transport of the SQL server or selecting Mixed Mode Authentication.

Unable to initialize TekRADIUS Authentication thread.

Check if there is another application using the same UDP port as the TekRADIUS Authentication thread *(Default is 1812)*.

Unable to initialize TekRADIUS Accounting thread.

Check if there is another application using the same UDP port as the TekRADIUS Accounting thread *(Default is 1813)*.

Invalid Accounting data insert configuration, using default

It is possible to configure which attributes, contained in the incoming RADIUS Accounting messages, are inserted into the 'Accounting' table. If a mistake has been made in the manual configuration of accounting messages within the 'TekRADIUS.ini' file, TekRADIUS will ignore the erroneous configuration and use the default query string:

```
INSERT INTO Accounting (SessionID, StatusType, UserName, NASIPAddr)
```

TekRADIUS Service is listening on: x.x.x.x

This message provides notification that the TekRADIUS service has successfully started.

Stopping active sessions

If Accounting is enabled and active user sessions are found, TekRADIUS automatically inserts artificial RADIUS Accounting stop records for the active user sessions *while you stop the TekRADIUS service gracefully*. These stop records can be distinguished from others as they are set *AcctSessionTime=NULL*.

All active sessions stopped

After successfully inserting all the artificial stop records for active user sessions, TekRADIUS provides this notification.

Authorization successful for user x

If TekRADIUS has been configured to run in Authorization Only mode, TekRADIUS notifies every successful user Authorization with this message.

Authorization failed for user x

If TekRADIUS is configured to run in 'Authorization Only' mode, there must be at least one *Success-Reply* attribute configured for the users to be authorized, otherwise users will receive *Access-Reject*.

Authentication failed for user x. Simultaneous limit has been set but accounting is not enabled...

In order to use the *Simultaneous-Use* attribute, Accounting must be enabled on TekRADIUS, otherwise users with the *Simultaneous-Use* attribute set will receive *Access-Reject*.

Authentication failed for user x

Either the user password, or one of check items configured in the User profile or user's Group profile, does not match the received attributes in the RADIUS *Access-Request* message. Check also to ensure that a valid RADIUS secret key for the RADIUS Authentication client has been configured.

No such user: x

TekRADIUS cannot find a valid user profile for the incoming RADIUS *Authentication-Request* packet.

Unsupported Cipher Suite, TLS Session has been aborted, sending Handshake Failure.

TekRADIUS TLS implementation supports following cipher suites.

- TLS_RSA_WITH_ARC4_128_MD5
- TLS_RSA_WITH_ARC4_128_SHA1
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256 *(TLS 1.3)*
- TLS_AES_256_GCM_SHA384 *(TLS 1.3)*

A ‘Handshake Failure Alert’ will also be sent.

TLS Session has failed. Sending TLS Alert.

TekRADIUS cannot verify the client TLS Finished message.

PEAP Authentication failed. A valid certificate could not be found for user x

A valid certificate cannot be found when authenticating the user using PEAP. Verify that the user has a *TLS-Certificate* attribute in the User or Group profile and that the certificate is stored in the Windows Certificate Store.

Authentication failed for user 'x'. Unsupported EAP authentication method.

A RADIUS client requested an authentication method that is not configured for the user. Check that the value of the *Authentication-Method* attribute configured for the user matches the authentication method selected.

Invalid Auth. packet received from: x.x.x.x

Either an incoming RADIUS Authentication message from a RADIUS client, not listed in 'Clients' table, has been received, or the specified size of RADIUS packet did not match the actual size, or a duplicate packet has been received.

Debug Message (Radius Authentication)

Debug messages occur with socket and SQL connection errors. Take the necessary actions according to the message.

Acct. packet with invalid secret received from: x.x.x.x

Either a RADIUS Accounting packet from a RADIUS client that is not listed in the 'Clients' table has been received or the RADIUS secret key configured for the x.x.x.x is invalid.

Debug Message (Radius Accounting)

Debug messages will be received for socket and SQL connection errors. Take the necessary actions according to the message.

Third Party Application Integration

TekRADIUS uses open databases to store user, group and client data. RADIUS accounting records are also stored in the database. You can integrate your existing applications by accessing the database directly. But you must consider the following;

- TekRADIUS keeps passwords in a proprietary reversible encryption method. You must disable encryption or you must use your own custom encryption module. Create a .NET .dll named EncSvc.dll which exports Encrypt and Decrypt functions. Each function must have two parameters a key value which will be used for symmetric encryption/decryption and a value to be encrypted or decrypted. EncSvc.dll must be placed TekRADIUS application directory and must be signed with a valid code signing certificate.

- Set following parameters as shown below

    - Settings / Parameters / Authentication / Failure Count = 0

    - Settings / Parameters / Authentication / Cache User/Group Attributes = No

You can also consider using command line interface TRCLI application for the integration. Please see the next section for the usage.

TekRADIUS provides also a HTTP REST based API. Please see latest API reference document in TekRADIUS web site.

You do not have to disable encryption if you prefer integration via TRCLI or the API. You can also use Failure Count and User/Group attribute caching if you prefer TRCLI and API methods for the integration.

TekRADIUS Command Line Interface - TRCLI.exe

TekRADIUS also has a command line utility, TRCLI.exe (located in the TekRADIUS application directory), which can be used for batch user processing and web-based applications to add, delete or modify users in the TekRADIUS database.

When executed, TRCLI looks for TekRADIUS.ini *(located in the TekRADIUS application directory),* which stores database connection information. If TRCLI is to be run from another directory, add the TekRADIUS installation directory to the Environment variable %PATH%.

When a new user is added, the user will be added to the 'Default' user Group. The user's Group can be changed using the attribute '*ietf|0*'.

Below is an example output of TRCLI when executed without any parameters:

```
C:\Program Files\TekRADIUS>trcli

TekRADIUS CLI - © 2008-2015 KaplanSoft, All rights reserved (Admin).

 Add User            :
  TRCLI -u user password group
 Add Group           :
  TRCLI -g group
 Delete User/Group   :
  TRCLI -[d|dg] [user/group]
 Add Attribute       :
  TRCLI -[a|ag] [user/group] "attribute" "value" [check|sreply|freply|inf|coaset|coareset]
 Delete Attribute    :
  TRCLI -[m|mg] [user/group] "attribute" [check|sreply|freply|inf|coaset|coareset]
 Retrieve Attributes :
  TRCLI -[r|rg] [user/group]
 Service Operations  :
  TRCLI -s [start|stop|query]
 Client  Operations  :
  TRCLI -c [add|delete|list] -a "Client IP Address" -s "secret"
 Send Google Auth.Key:
  TRCLI -ga user [email address]
 Help                :
  TRCLI -h

 Service & Client Operations require administrative privileges.
```

Use case examples:

Add a user: A username and password must be supplied.

```
C:\Program Files\TekRADIUS>trcli -u test test123

User 'test' has been added. Configure attributes for the user.
```

Delete a user:

```
C:\Program Files\TekRADIUS>trcli -d test

User 'test' deleted...
```

Add an attribute to an existing profile user *(Attributes can only be added to existing users).*

NOTE: TekRADIUS uses a special notation for storing attributes in User profiles.

For example, IETF Service-Type (7) attribute with value ARAP (3) is added, as shown below:

```
C:\Program Files\TekRADIUS>trcli -a kaplan "ietf|7" 3 check
Attribute 'ietf|7' for the user 'kaplan' has been added...
```

An example of the use of the Microsoft *MS-Primary-DNS-Server* attribute would be:

```
C:\Program Files\TekRADIUS> trcli -a kaplan "msoft|28" 192.168.10.1
```

Refer to the TekRADIUS Dictionary Editor Please for the notion of vendors and attributes.

Delete an attribute from a user profile

```
C:\Program Files\TekRADIUS>trcli -m kaplan "ietf|7" check
Attribute 'ietf|7' for the user 'kaplan' has been deleted...
```

Retrieve attributes configured for a user

```
C:\Program Files\TekRADIUS>trcli -r kaplan
ietf|0,sss,Check
ietf|1,kaplan,Check
ietf|2,deneme,Check
ietf|6,2,Check
ietf|8,255.255.255.254,SReply
```

All attributes, including check and reply attributes, are listed in 'Attribute, Value, Attribute_Type' format. TRCLI will list all user profiles if you do not specify a username.

Change password of a user profile: Remove and then re-add the check attribute *ietf|2* with a new password value.

```
C:\Program Files\TekRADIUS>trcli -m kaplan "ietf|2" check
Attribute 'ietf|2' for the user 'kaplan' has been deleted...

C:\Program Files\TekRADIUS>trcli -a kaplan "ietf|2" 5678 check
Attribute 'ietf|2' for the user 'kaplan' has been added...
```

Change group of a user profile: Remove and then re-add the check attribute *ietf|0* with a new group id.

```
C:\Program Files\TekRADIUS>trcli -m kaplan "ietf|0" check
Attribute 'ietf|0' for the user 'kaplan' has been deleted...

C:\Program Files\TekRADIUS>trcli -a kaplan "ietf|0" newgroup check
Attribute 'ietf|0' for the user 'kaplan' has been added...
```

Disable a user profile. Add the attribute *kaplansoft|0* to the user profile with a value of '0';

```
C:\Program Files\TekRADIUS>trcli -a kaplan "kaplansoft|0" 0 check
Attribute kaplansoft|0' for the user 'kaplan' has been added...
```

To enable the user, set the value of "kaplansoft|0" attribute to "1".

Add a RADIUS client (NAS, Access Point…) entry. The IP address of NAS device and the secret key must be specified.

```
C:\Program Files\TekRADIUS>trcli -c add -a "102.168.10.10" -s "radius_secret"
Client entry 192.168.10.1 added (Enabled).
```

Client options can be specified through the command line

```
-a "Client IP Address"
-s "Secret"
-v "Vendor"
-r "Regular Expression for Username"
-e Enabled, "Yes" or "No"
-k "Kill Command"
-i "Interim Update Period (Seconds)"
-g "Client Group"
-d "Description"
```

By default, the RADIUS client's vendor type is set to '*ietf*' and is enabled. The vendor type and status can be changed through TekRADIUS Manager.

Update a RADIUS client (NAS, Access Point…) entry. To update a RADIUS client, specify the parameter to be updated.

```
C:\Program Files\TekRADIUS>trcli -c update 102.168.10.10 -s "test"
Client entry 192.168.10.1 is updated (Enabled).
```

Delete a RADIUS client (NAS, Access Point…) entry. To delete a RADIUS client, it is only necessary to specify just the IP address of NAS device.

```
C:\Program Files\TekRADIUS>trcli -c delete 102.168.10.10
Client entry 192.168.10.1 is deleted.
```

List all RADIUS client entries

```
C:\Program Files\TekRADIUS>trcli -c list

126.10.10.1,fatsa1,ietf,Enabled,Default,""
126.10.10.2,fatsa2,ietf,Enabled,Default,""
192.168.44.3,deneme,mikrotik,Disabled,Default,"Komut satirindan..."
```

List active sessions

```
C:\Program Files\TekRADIUS>trcli -l

TimeStamp, Duration, SessionID, UserName, GroupName, NasIPAddr, NasIdentifier,
NasPort, NasPortType, NasPortID, ServiceType, FramedIPAddr, CallingStationID,
CalledStationID

4.7.2015 16:55:20, 4174, 80700006, dwadley, 11, 192.168.1.43, myport-mstreet,
2154823686, Ethernet, wlan-Hotspot, , 10.5.50.4, 8C:29:37:B6:06:FF, hotspot1

4.7.2015 17:04:45, 4165, 80700006, kaplan, Blank, 192.168.1.43, myport-mstreet,
215482368, Ethernet, wlan-Hotspot, , 10.5.50.4, 8C:29:37:B6:06:FF, hotspot1

2 active sessions found.
```

List active sessions for a user

```
C:\Program Files\TekRADIUS>trcli -l kaplan

TimeStamp, Duration, SessionID, UserName, GroupName, NasIPAddr, NasIdentifier, NasPort,
NasPortType, NasPortID, ServiceType, FramedIPAddr, CallingStationID, CalledStationID

4.7.2015 17:04:45, 4165, 80700006, kaplan, Blank, 192.168.1.43, myport-mstreet,
215482368, Ethernet, wlan-Hotspot, , 10.5.50.4, 8C:29:37:B6:06:FF, hotspot1

1 active session found.
```

Clear a user's session:

```
C:\Program Files\TekRADIUS>trcli -q Kaplan
```

Send a Packet of Disconnect Request *(RFC 3576)*:

```
C:\Program Files\TekRADIUS>trcli -k Kaplan pod
```

Send a Change of Authorization Request *(RFC 3576)*:

```
C:\Program Files\TekRADIUS>trcli -k Kaplan coa "ietf|44=01aa33d;ietf|8=192.168.1.10"
```

You can specify your own set of attributes in Packet of Disconnect and Change of Authorization requests. Please surround attributes in double quotes and use the following format for the attributes;

```
VendorName|AttributeId=Value
```

You can concatenate multiple attributes with semicolons. You can see vendor names and attribute Ids in TekRADIUS Dictionary. TekRADIUS will use value from RADIUS accounting start packet if you omit value for the attribute. For example;

```
trcli -k Kaplan coa "Acct-Session-Id;Framed-IP-Address =192.168.1.10"
```

You can also send CoA-Set or CoA-Reset attributes if these attributes are configured in user or group profile;

```
trcli -k Kaplan coaset
trcli -k Kaplan coareset
```

TekRADIUS will get Acct-Session-Id value for active session entry for user Kaplan from received RADIUS Accounting start packet since its value is omitted. You can use "all" as username to send CoA or PoD request to all online users;

```
trcli -k all coaset "Acct-Session-Id;Framed-IP-Address=192.168.1.10"
```

You can specify attributes other than User-Name to match active session to send PoD or CoA requests. Following example uses Session-Id to match an active session and sends a CoA request;

```
C:\Program Files\TekRADIUS>trcli -k Acct-Session-Id=01aa33d coa "Framed-IP-
Address=192.168.1.10"
```

You can use the following attributes to match active sessions;

```
Group-Name (ietf|0) [TekRADIUS Group name]
User-Name (ietf|1)
NAS-IP-Address (ietf|4)
NAS-Port (ietf|5)
Service-Type (ietf|6)
Framed-IP-Address (ietf|8)
Called-Station-Id (ietf|30)
Calling-Station-Id (ietf|31)
NAS-Identifier (ietf|32)
Acct-Session-Id (ietf|44)
NAS-Port-Type (ietf|61)
NAS-Port-Id (ietf|87)
```

! *The encryption of passwords in the Authentication and Group tables is optional in version 2.5. When upgrading from versions 2.3 or 2.4, start TekRADIUS Manager with default values. If it is necessary to upgrade from a version prior to version 2.3, manually edit TekRADIUS.ini, located in the application directory, and set* EncryptPasswords=0 *the under* ***Database*** *section before starting TekRADIUS.*

The performance counter values can be retrieved with the -p parameter.

You can set or reset Google Authenticator secret and send it to specify user e-mail address;

```
C:\Program Files\TekRADIUS>trcli -ga Kaplan -ea user@kaplansoft.com
```

-ea parameter is optional. If the user is a local user, TekRADIUS can send Google Authenticator secret to the e-mail address specified with Email-Address attribute in the user profile. TekRADIUS will obtain an e-mail address from the Active Directory for the user, if the user is an Active Directory user. Mail Alerting must be configured and TekRADIUS service must be in running state for this function to work.

Create a backup archive

```
C:\Program Files\TekRADIUS>trcli -bu "C:\Archive\mybackup.bak"

'EncSvc.dll' is found, enabling custom encryption functions.

Backup Users (14832)... 100%

Backup Groups (288)... 100%

Backup Clients (14)... 100%

Creating backup file...

Backup file is created at 'C:\Archive\mybackup.bak'
```

The SQL edition of TRCLI (TRCLI.exe) allows you to backup from a remote SQL server. This is useful when you synchronize your local database with a remote database manually.

```
trcli -bu "Archive file" <remote SQL server address> <Database> <username> <password>
```

Restore from a backup archive

```
C:\Program Files\TekRADIUS>trcli -rs "C:\Archive\mybackup.bak" -o

'EncSvc.dll' is found, enabling custom encryption functions.

Backup is created on '22.06.2023 17:52:37' at 'MyPC' by 'MyPC\myuser' (MS SQL).
Existing records will be overwritten. Continue? [y/n] y

Restore Groups...100%

Restore Users... 100%

Restore Clients... 100%

Restore operation is completed.
```

-o parameter is optional. TRCLI will overwrite existing records if specified. You can suppress confirmation by adding -p command line option.

Creating and Installing a Self-Signed Certificate for PEAP/EAP-TLS Authentication

A server-side X.509 digital certificate is required for PEAP/EAP-TLS authentication. This certificate can be issued from an organization's internal Certificate Authority or it can be purchased from a third-party Certificate Authority, such as VeriSign, however, this may be costly for test environments.

Creation of Self Signed Certificate

TekCERT is a standalone executable program that can be used to generate self-signed certificates for test environments. TekCERT may be downloaded from the TekRADIUS Support site and requires Microsoft .NET Framework 4.0. When TekCERT is run, the following form enables the creation of a certificate:

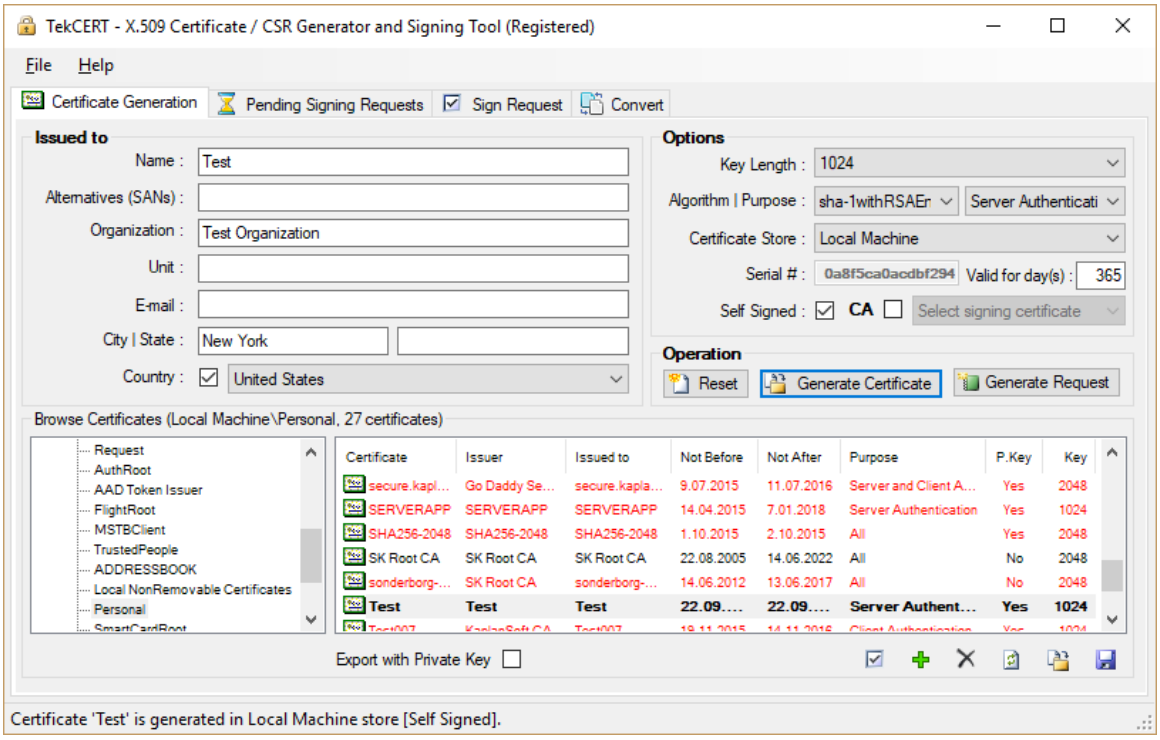


Figure 27. - TekCERT Certificate Parameters

Click the **Generate Certificate** button to create the certificate after completing all the necessary fields. At a minimum, a valid 'Name' must be entered for the certificate.

After creating the certificate for client deployment, the public key in the .cer *(DER encoded X.509)* format may be exported. Select the generated certificate at **Browse Certificates** section and click the **Export** button.

Client certificates can also be created using TekCERT. Select 'Client Certificate' as the Purpose in the certificate parameters. Client certificates with their associated private keys may be exported for client deployment in .pfx format.

Certificate Deployment at Client Side

It is not necessary to deploy a root certificate on clients if the server's certificate is not to be verified by the clients. If client verification of the server certificate is required, the root certificate must be exported and deployed on the clients.

Server Certificate

To install the server certificate onto a client compute:

1. Copy the file that contains the server certificate to the client computer,
2. Locate the certificate file on the client computer,
3. Right click on the certificate then select **Install Certificate**,
4. Click **Next** on the 'Certificate Import Wizard' dialog,
5. Select 'Place all certificates in the following store',
6. Click **Browse**,
7. Check 'Show physical stores',
8. Select 'Trusted Root Certification Authorities/Local Computer',
9. Click **OK** to close the 'Select Certificate Store' dialog,
10. Click **Next** after selecting the certificate store on the 'Certificate Import Wizard' dialog,
11. Click **Finish** to complete the manual deployment of the server root certificate.

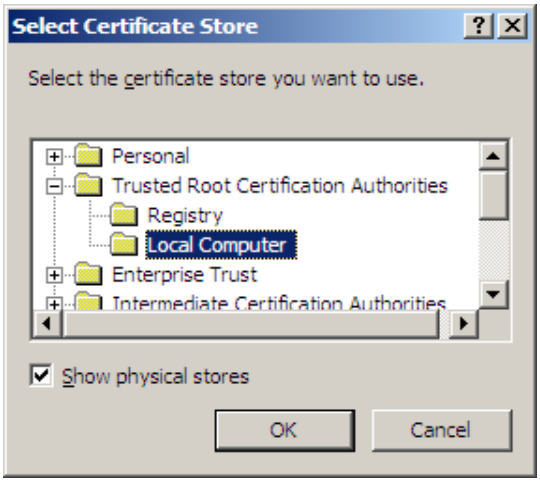


Figure 28. - Select Certificate Store Dialog

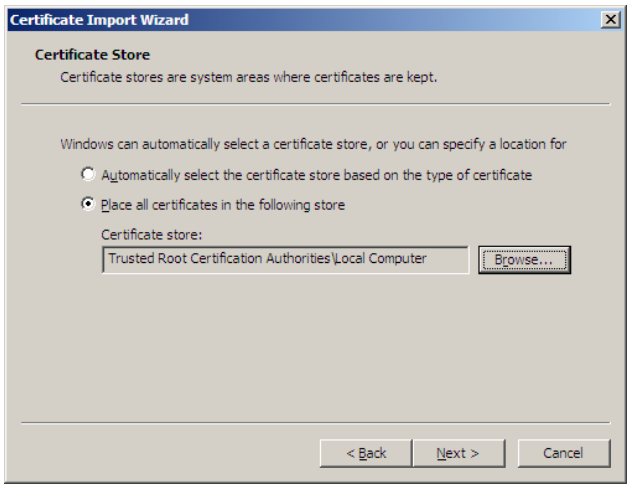


Figure 29. - Certificate Import Wizard Dialog

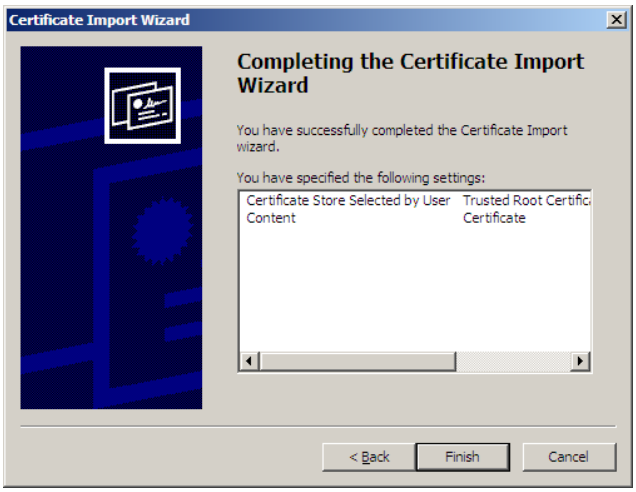


Figure 30. - Certificate Import Wizard Dialog

Client Certificate

To import a client certificate:

1. Copy the file containing the client certificate to the client computer,
2. Locate the certificate file on the client computer,
3. Double click on the certificate file,
4. Click **Next** *(see Figure)*,

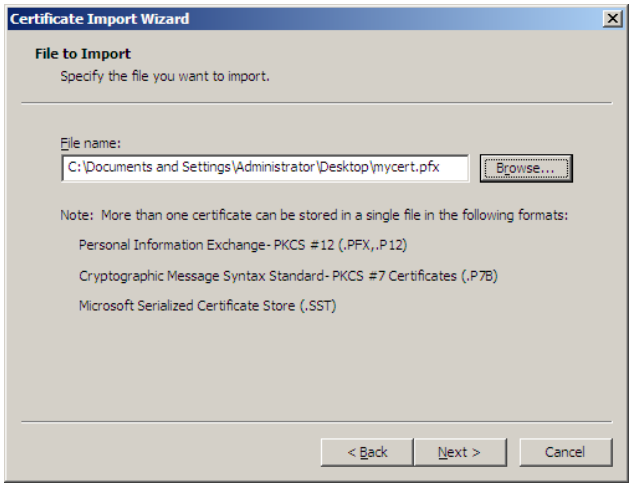


Figure 31. - Certificate Import Wizard Dialog

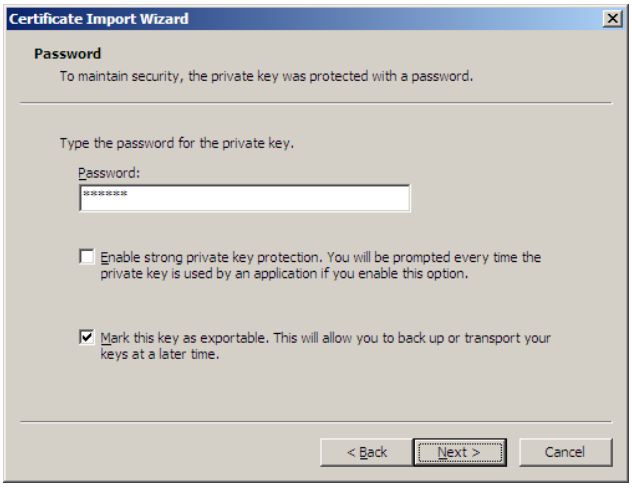


Figure 32. - Certificate Import Wizard Dialog

5. Enter the private key password,
6. Select 'Mark this key as exportable…',
7. Click **Next**,
8. Select 'Automatically select the certificate store based on the type of certificate',
9. Click **Next**,
10. Click **Finish** at the last dialog.

Client PEAP Configuration

Although there are commercially and freely available PEAP supported 802.1X supplicant alternatives for Windows, Windows editions have a built-in supplicant.

In order to configure PEAP *(PEAPv0-EAP-MS-CHAP v2)* Authentication for a Wireless Network Connection:

1. Open 'Network Connections' *(Start/Settings/Network Connections)*,
2. Right click on the chosen wireless connection,
3. Select **Properties**. The detected wireless networks will be shown in the 'Preferred networks' window on the 'Wireless Networks' tab.

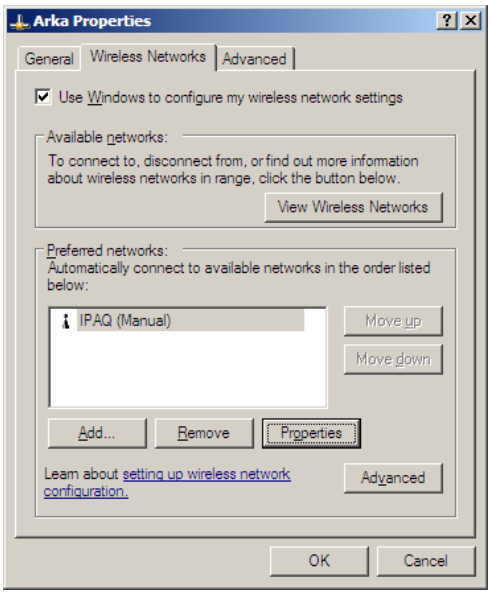


Figure 33. - Wireless Networks Connection/Wireless Networks Tab

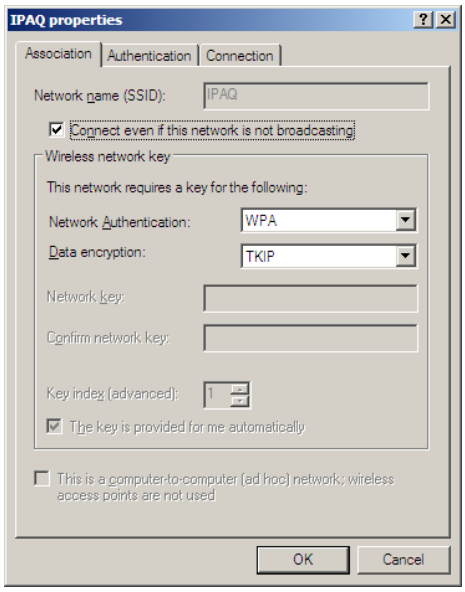


Figure 34. - Association Parameters

4. Select the wireless network that requires PEAP authentication,
5. Click **Properties**,
6. Configure "Association" parameters as shown in Figure ,
7. Select the 'Authentication' tab,
8. Select 'Protected EAP (PEAP)' as 'EAP Type' from the drop-down list,
9. Click **Properties**.

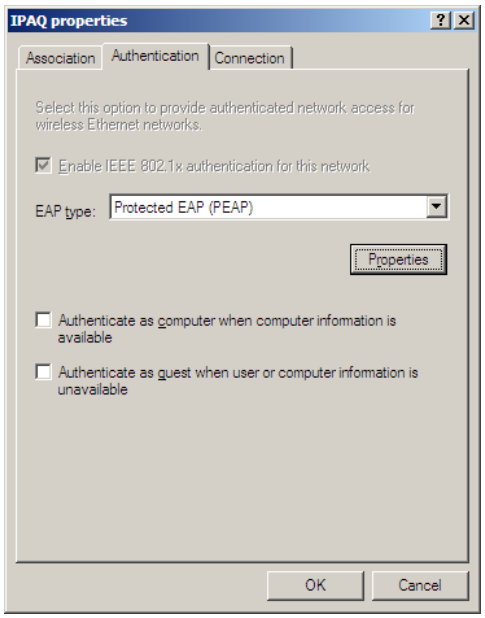


Figure 35. - EAP Type Selection

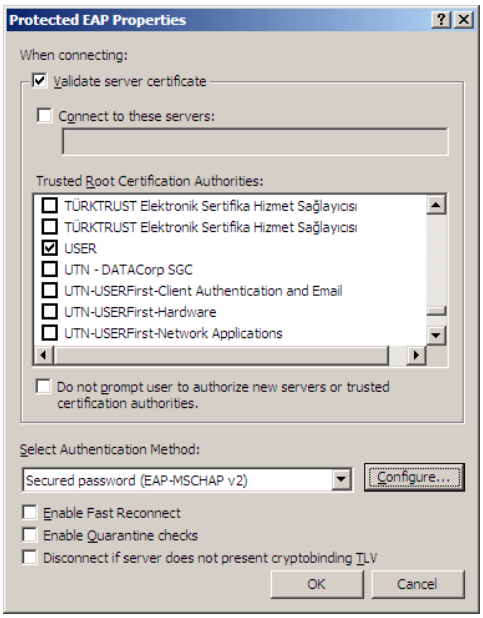


Figure 36. - Protected EAP Properties Settings

10. Optionally check 'Validate server certificate', and select the server root certificate installed previously in the 'Trusted Root Certification Authorities' list,
11. Set the other options as shown in Figure .

If it is necessary to authenticate a user with a username/password pair that is different to user's Windows logon username/password:

12. Click the **Configure** button on the 'Protected EAP Properties' dialog,
13. Uncheck 'Automatically use my Windows logon name and password' on the 'EAP MSCHAPv2 Properties' dialog,
14. Click **OK**.

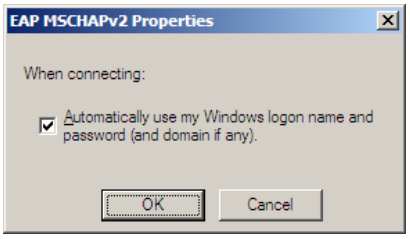


Figure 37. - EAP MSCHAPv2 Properties Dialog

Client EAP-TLS Configuration

To configure EAP-TLS Authentication for a Wireless Network Connection:

1. Open Network Connections *(Start/Settings/Network Connections)*,
2. Right click on the chosen wireless connection,
3. Select **Properties**. The detected wireless networks will be shown in the 'Preferred networks' window on the 'Wireless Networks' tab.

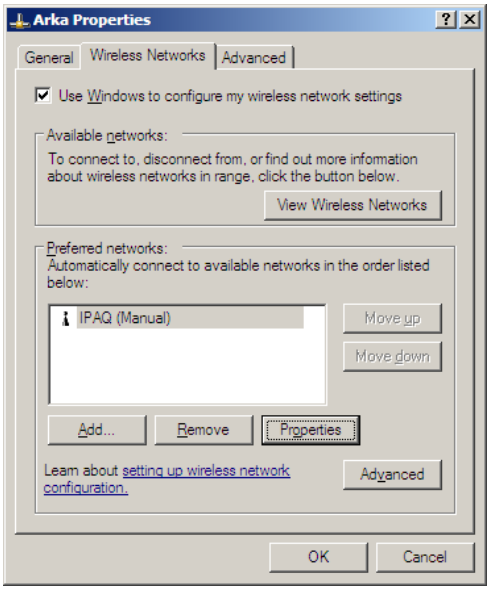


Figure 38. - Wireless Networks Connection/Wireless Networks Tab

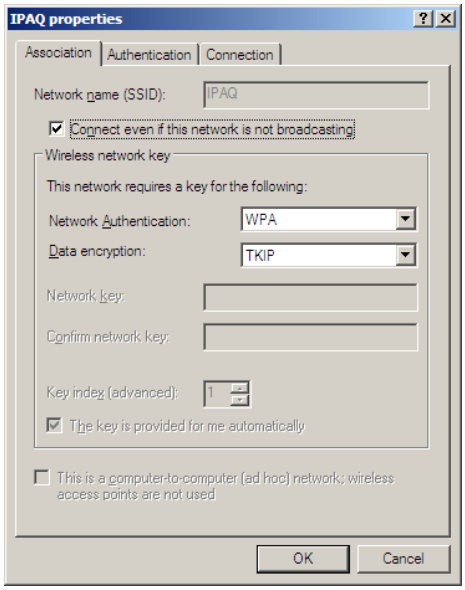


Figure 39. - Association Parameters

4. Select the wireless network that requires PEAP authentication,
5. Click **Properties**,
6. Configure the 'Association' parameters, as shown in Figure .
7. Select the 'Authentication' tab,
8. Select 'Smart Card or Certificate' as 'EAP Type' from the drop-down list,
9. Click **Properties**,

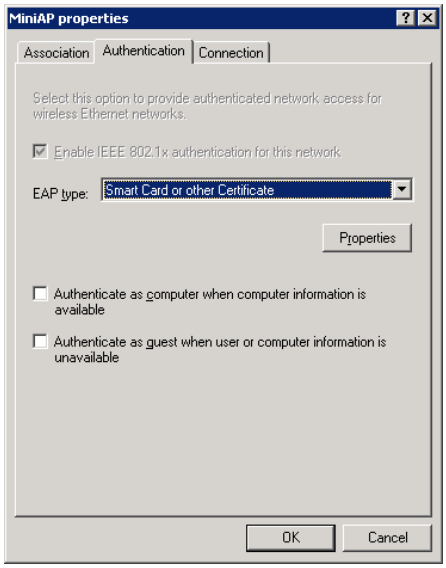


Figure 40. - EAP Type Selection

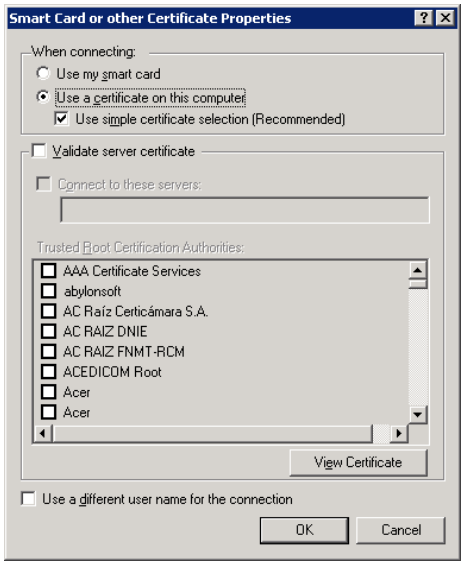


Figure 41. - Protected EAP Properties Settings

10. Optionally check 'Validate server certificate' and select the server root certificate installed previously in the 'Trusted Root Certification Authorities' list.
11. Set the other options as shown in Figure 6.

SQL Server Configuration

Connecting to SQL Express Using TCP/IP

By default, SQL Express does not accept any connections from another computer. This means it is not possible to remotely connect to it with SQL Management Studio, an ODBC connection, etc.

To allow TCP/IP connections, follow these steps:

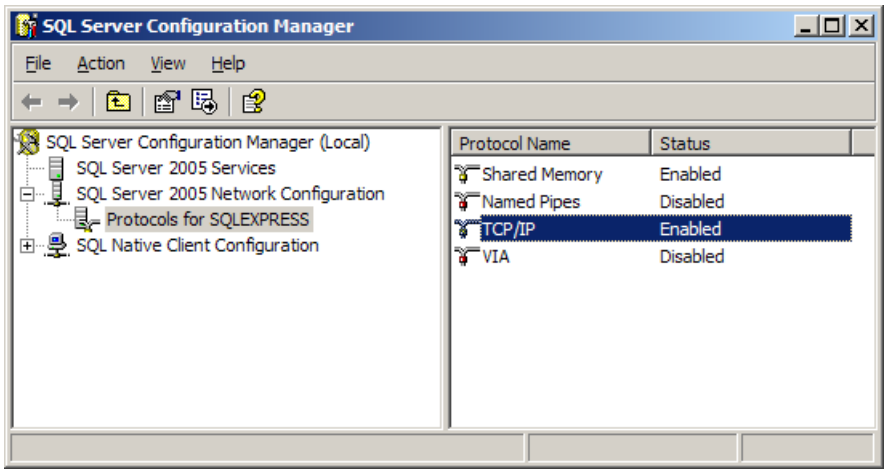


Figure 42. - SQL Server Configuration Manager

1. Launch the SQL Server Configuration Manager from **Programs>Microsoft SQL Server 2005>Configuration Tools**
2. Click on the 'Protocols for SQLEXPRESS' node under 'SQL Server 2005 Network Configuration'.
3. Double click 'TCP/IP'

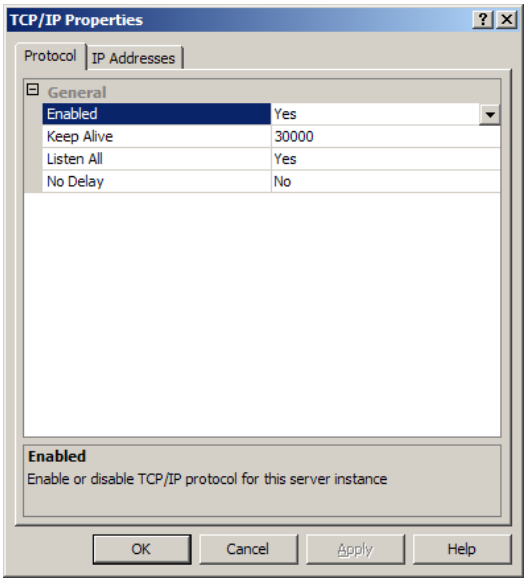


Figure 43. - TCP/IP Properties Protocol Selection

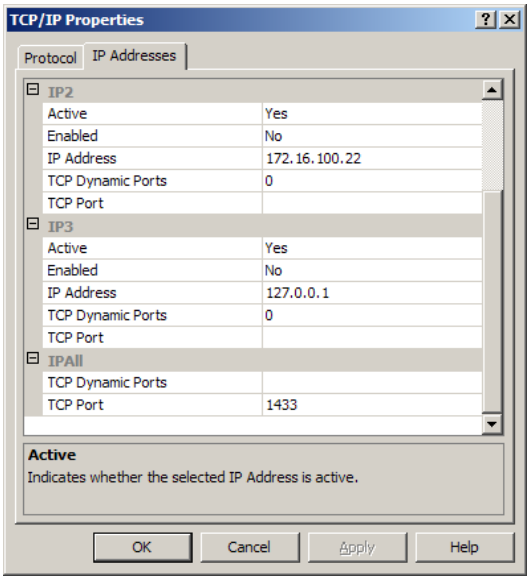


Figure 44. - TCP/IP Properties IP Address Selection

4. Select 'Yes' next to 'Enabled' and click the [OK] button to save the changes.
5. On the IP Addresses tab, under the IP All node, clear the 'TCP Dynamic Ports' field. Also, enter port number 1433 to listen on in the 'TCP Port' field.
6. Restart the Microsoft SQL Server Express service using either the standard service control panel or the SQL Express tools.

SQL Express Authentication Configuration

TekRADIUS requires SQL Server authentication to be enabled on the instance of SQL Express. To do this:

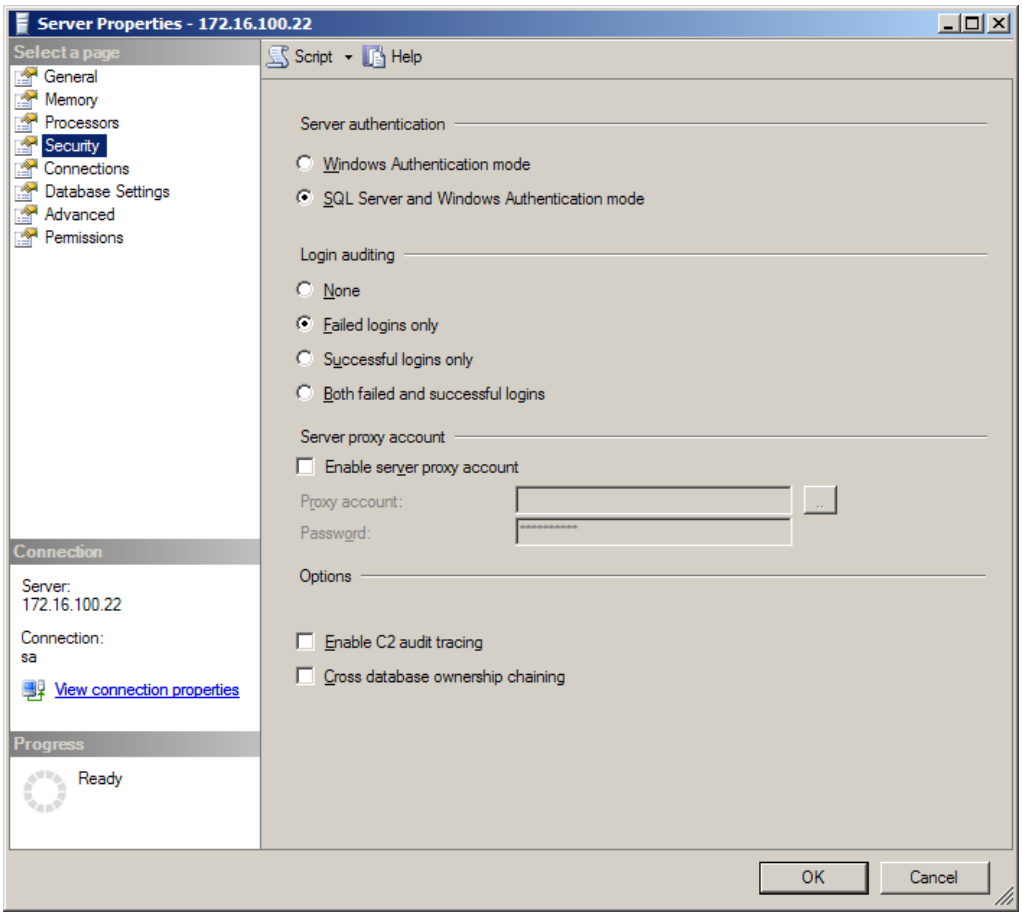


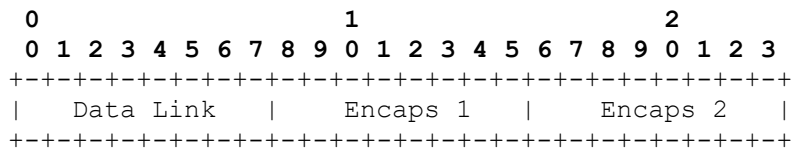
Figure 45. - SQL Express Configuration

1. On the machine with SQL Express installed, the SQL Server Management Studio Express tool opens.
2. Right-click the instance of SQL Express to configure it and select 'Properties'.
3. Select the 'Security' section on the left.
4. Change the Server Authentication to SQL Server and Windows Authentication mode *(Select 'Mixed Mode' in other Microsoft SQL Server Editions)*.
5. Restart the Microsoft SQL Server Express service using either the standard service control panel or the SQL Express tools.

Encoding of Attribute 144 in RFC 4679 (ADSL-Forum Access-Loop-Encapsulation)

This Attribute describes the encapsulation(s) used by the subscriber on the DSL access loop. It MAY be present in both *Access-Request* and *Accounting-Request* packets.

This field is a string, 3 bytes in length, logically divided into three 1-byte sub-fields as shown in the following diagram:




```
Octet[0] - 0x01 AAL5
Octet[0] - 0x02 Ethernet

Octet[1] - 0x00 Not Available
Octet[1] - 0x01 Untagged Ethernet
Octet[1] - 0x02 Single-Tagged Ethernet

Octet[2] - 0x00 Not available
Octet[2] - 0x01 PPPoA LLC
Octet[2] - 0x02 PPPoA Null
Octet[2] - 0x03 IPoA LLC
Octet[2] - 0x04 IPoA NULL
Octet[2] - 0x05 Ethernet over AAL5 LLC with FCS
Octet[2] - 0x06 Ethernet over AAL5 LLC without FCS
Octet[2] - 0x07 Ethernet over AAL5 Null with FCS
Octet[2] - 0x08 Ethernet over AAL5 Null without FCS
```

Failure Codes in Accounting Table DisconnectCause Field when "Save Authentication Failures" Option is Set

TekRADIUS inserts a failure code to Accounting Table DisconnectCause Field when Save Authentication Failures Option Set. Here are current values and corresponding failure cases;

Failure Code	Failure Case
1100	Authentication failed
1101	Windows domain authentication failure
1102	Windows Active Directory authentication failure
1103	LDAP authentication failed
1104	Valid certificate cannot be found
1105	Invalid authentication method
1106	External authenticator returned negative response
1107	Active Directory group does not match
1108	Missing server certificate
1109	TLS Certificate cannot be generated
1110	SIM triplets not configured
1111	Client certificate validation failure
1112	EAP-SIM Authentication failure
1113	CHAP authentication failed
1114	Absent user
1115	Invalid password
1116	Password expired
1117	MS-CHAP-v1 authentication failed
1118	MS-CHAP-v2 authentication failed
1119	MS-CHAP-v2 authentication failed (NTLM)
1120	User-Password required
1121	User quota exits, accounting is not enabled
1122	Time limit reached
1123	Login time restriction
1124	OTP authentication failed
1125	PAP authentication failed
1126	Digest authentication failure
1127	Local user profile expired
1128	User profile is not active
1129	Simultaneous limit reached
1130	Local user profile disabled
1131	CHAP authentication failed (OTP)
1132	CHAP authentication is not supported with Windows/NTLM Authentication Proxy
1133	Windows authentication is not supported in freeware edition
1134	OTP authentication is not supported in freeware edition
1135	User-Name does not match
1136	RADIUS authentication request does not contain required check attribute
1137	Check attribute value does not match

Failure Code	Failure Case
1138	Invalid attribute value
1139	External executable returned negative response
1140	Windows domain authentication failed since user group is disabled
1141	LDAP authentication failed since user group is disabled
1142	User account has no permission to login at the moment
1143	Insufficient credit
1144	Simultaneous limit has been set but accounting is not enabled
1145	User group is disabled
1147	User is not connected from allowed SSIDs or SSID information cannot be obtained

Regular Expression Based Check Attributes

Most common use for this option is to limit wireless user access from specific SSIDs. Some of access points reports connected SSID in Called-Station-Id attribute;

```
Called-Station-Id = 02-AB-00-19-F3-4E:ABC-Guest

Called-Station-Id = CC-AB-00-19-FA-4E:ABC-Company
```

If you wish to limit user access to a Guest network, regardless of access point connected, enable RegExp based matching and add

```
Called-Station-Id = :ABC-Guest
```

as a check attribute to user or group profiles.

Using Alternative Authentication and Authorization Queries

You can uncheck **Use Default Authentication Query** and **Use Default Authorization Query** options and define your own query sentences. If you are going to verify the password, you must uncheck the **Encrypt Passwords** option.

The outputs of these queries should return fields that contain Attribute and Val fields. Typically, Authentication Query should return at least the following records for the user named test;

```
ietf|0,Default
ietf|1,test
```

For the password;

```
ietf|2,password
```

Attribute option in the first field is organized as vendor_id|attribute_id. See the Dictionary tab for possible options. The query you will use for authorization should again produce a similar output. For example, to return for the value of session timeout as 3600 seconds.

```
ietf|27,3600
```

If you use an alternative query sentence that begins with "Select", the Where clause in the query should contain AttrType = 0 for Authentication and AttrType = 1 for Authorization.

Let's assume that you have a custom table having following fields;

```
[RoomNumber],[BirtDate],[DocumentType],[Id],[CheckInDate],[CheckOutDate],[Name],
[Surname],[Nationality]
```

And you would like to use Surname as username and room number as user password. In this case, create the following SQL View;

```
Create View AlternativeUsers as Select [Surname] as UserName, 'ietf|1' as
Attribute, 0 as AttrType, [Surname] as Val Union Select [Surname] as UserName,
'ietf|2' as Attribute, 0 as AttrType, [RoomNumber] as Val Union Select [Surname]
as UserName, 'ietf|0' as Attribute, 0 as AttrType, 'Default' as Val) Union
Select [Surname] as UserName, 'ietf|27' as Attribute, 1 as AttrType, 3600' as
Val)
```

As an alternative Authentication query;

```
Select Attribute, Val from AlternativeUsers where UserName='%ietf|1%' and
AttrType=0
```

and alternative Authorization query;

```
Select Attribute, Val from AlternativeUsers where UserName='%ietf|1%' and
AttrType=1
```

Your query must start with `select * from dbo.MyFunctionName` if you use SQL functions which return a table values.

You must uncheck the **Encrypt Passwords** option.

Performance tips

Here are some tips for increasing TekRADIUS performance:

- Increase memory as much as you can if the SQL server is running on the same machine.
- Latest versions add a filed named tracid and an index for it to Accounting table to speed up accounting functions. Please check if they exist.
- Rebuild indexes after purging old accounting records in the accounting table.
- Disable unused vendor dictionaries in TekRADIUS Manager / Dictionary.
- Lower logging level to Error at settings / service parameters.
- Disable RADIUS accounting if it's not needed.

Creating ODBC Connection Profiles for TekRADIUS OD

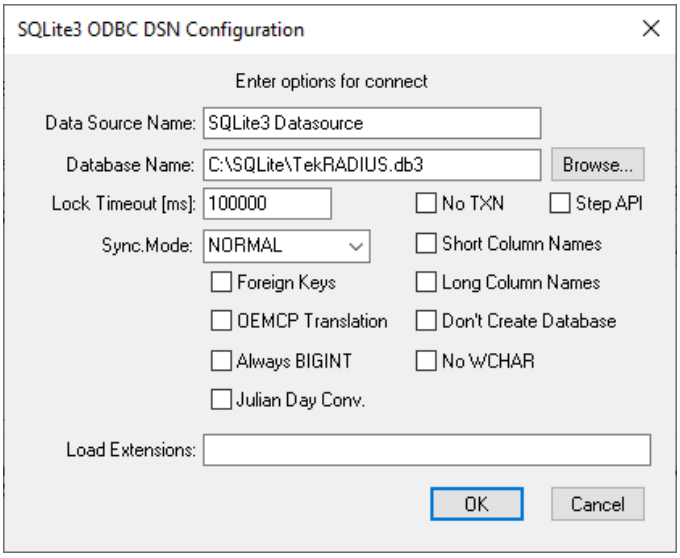
TekRADIUS OD supports SQLite, MySQL, MariaDB, PostgreSQL and Oracle databases through ODBC. You need to download install ODBC drivers for these databases, create an empty database and an ODBC DSN prior to configuring TekRADIUS OD. DSNs must be created in ODBC Data Source Administrator (64-bit) System DSN.

TekRADIUS LT supports SQLite directly. We recommend you use TekRADIUS LT if you plan to use an SQLite database.

Creating an ODBC DSN for SQLite

You can obtain 64-bit SQLite ODBC driver from http://www.ch-werner.de/sqliteodbc/

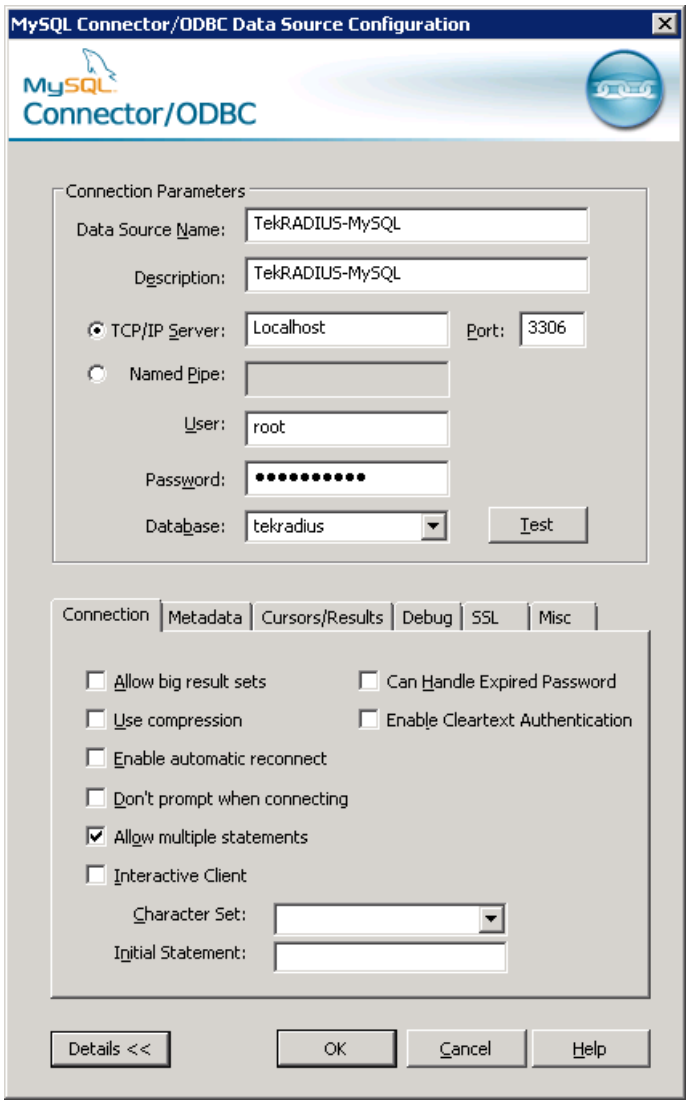
Here are typical parameters;



ODBC driver does not create database file. Database files must be created prior to create the DSN. TekRADIUS OD will automatically cerate necessary tables, indexes and views.

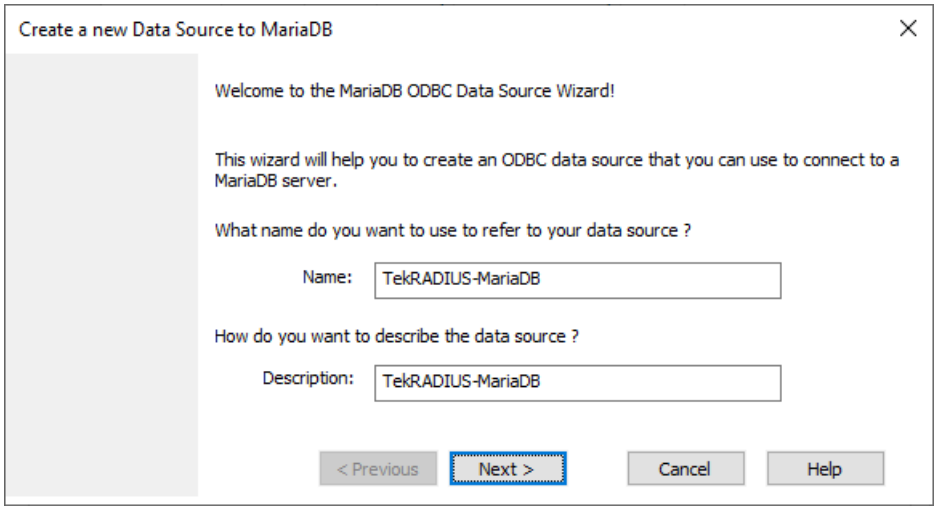
Creating an ODBC DSN for MySQL

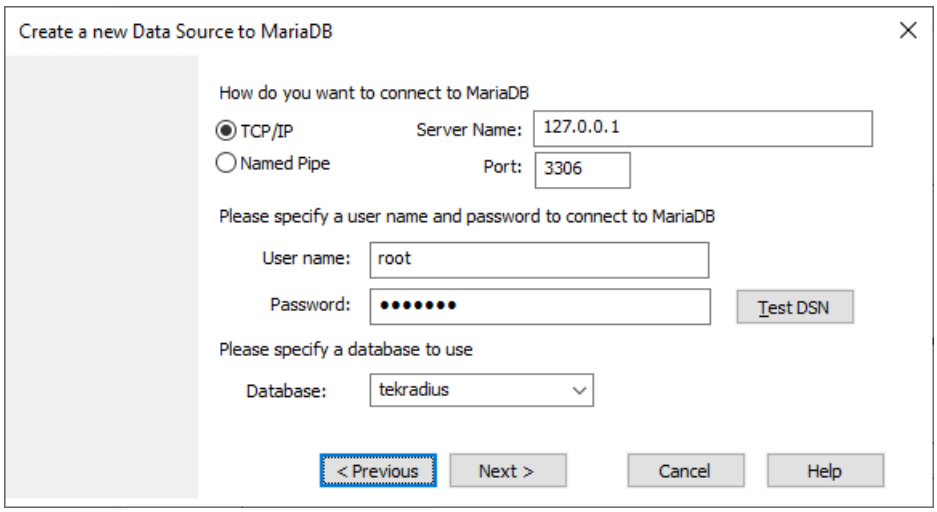
You can download the latest MySQL ODBC driver from https://dev.mysql.com/downloads/connector/odbc/ You need to create the database prior to configure the DSN.

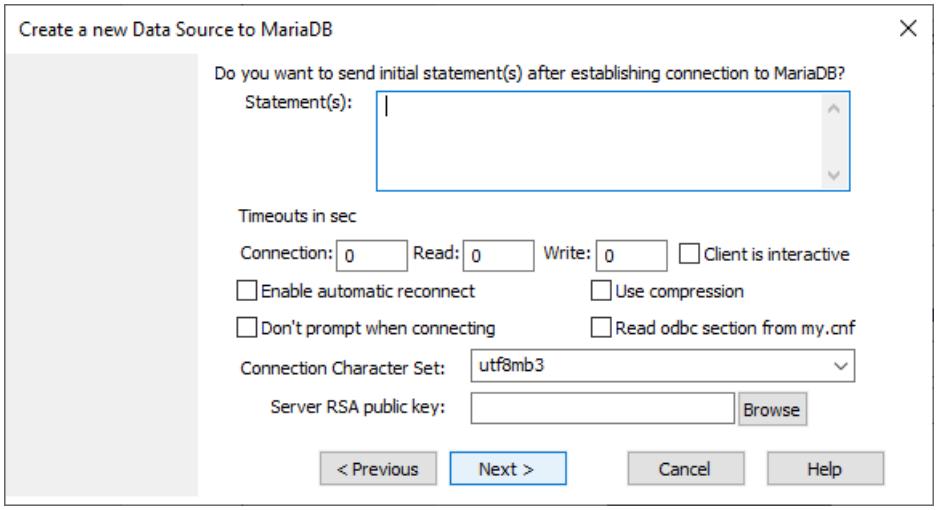


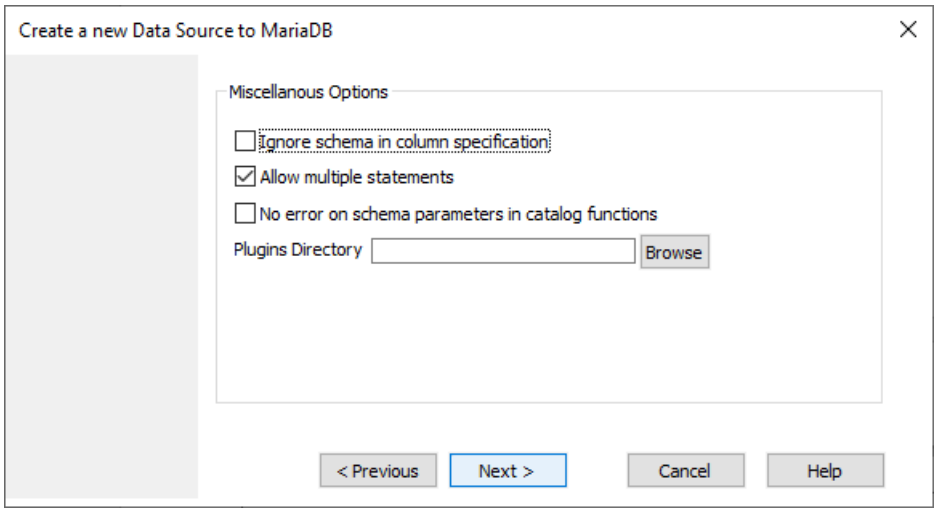
Creating an ODBC DSN for MariaDB

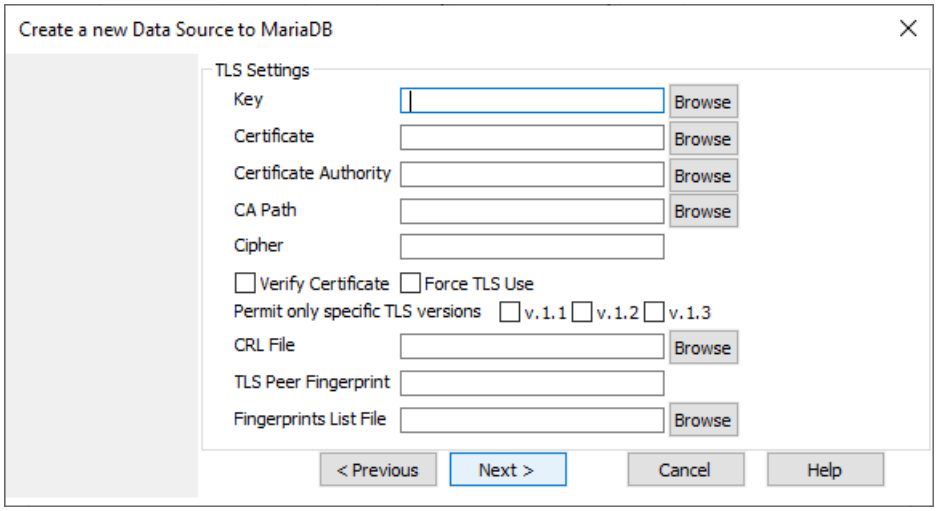
You can download the latest ODBC driver for MariaDB from https://mariadb.com/downloads/connectors/connectors-data-access/odbc-connector MariaDB ODBC driver has a wizard to configure the DSN. You need to create the database prior to configuring the DSN.

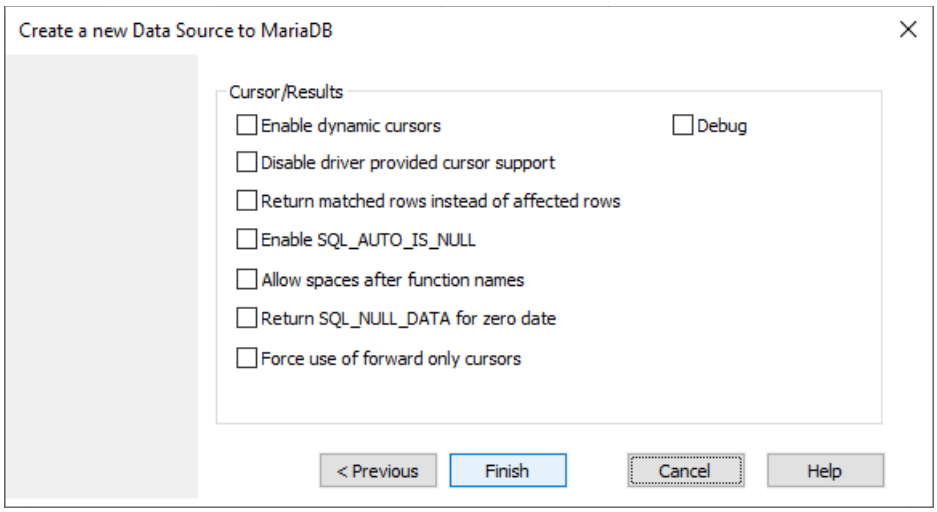






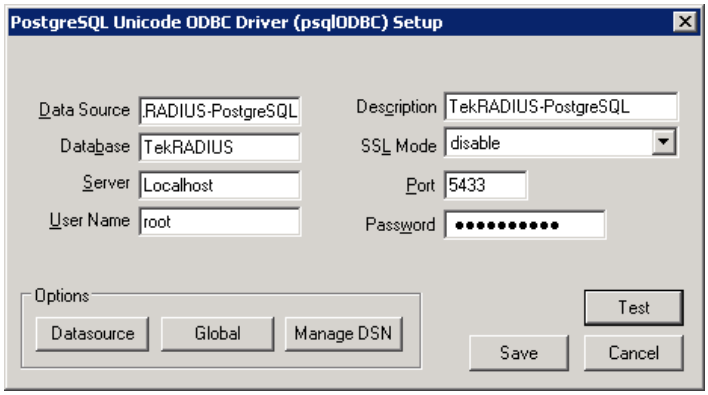






Creating an ODBC DSN for PostgreSQL

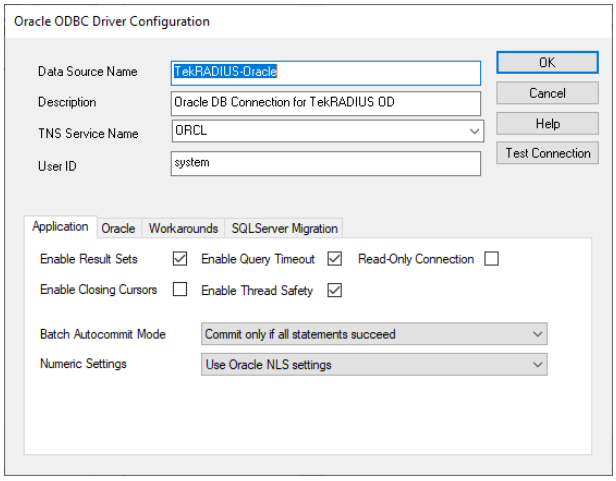
You can download the latest ODBC driver for PostgreSQL from https://www.postgresql.org/ftp/odbc/versions/msi/ You need to create the database prior to configuring the DSN.



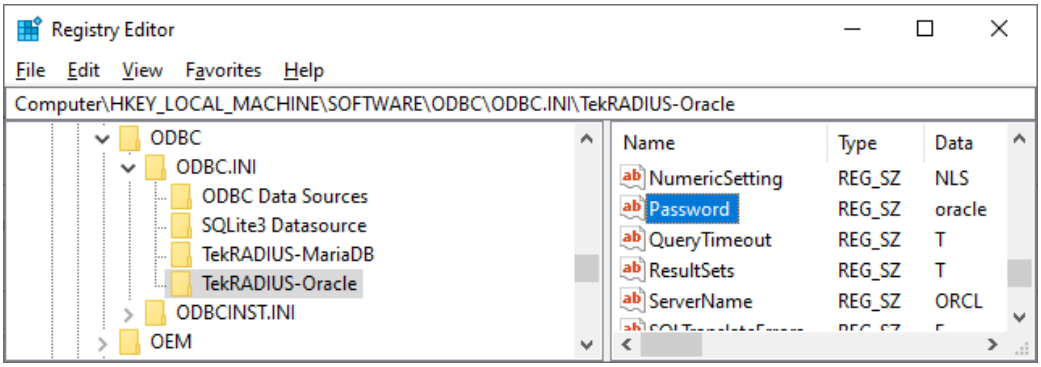
Creating an ODBC DSN for Oracle Database

Please see https://www.oracle.com/tr/database/technologies/releasenote-odbc-ic.html for installing Oracle ODBC driver. You need to create the database prior to configuring the DSN.

ODBC profile for an Oracle database has not an option to save password for the database.



You can specify the password manually by setting Password parameter of the ODBC profile in Windows Registry;



Your database must have an entry in your local tnsnames.ora file under Instant Client network/admin folder *(C:\instantclient_21_3\network\admin e.g.)*.

Index

Access-Accept Messages 20
Accounting Port 22
Accounting Table 11, 14
Accounting-Checkpoint Message 22
Accounting-Interim-Updates message 57
Accounting-Off Message 22
Accounting-Stop Message 22, 48
Acct-Input-Octets attribute 49
Acct-Output-Octets attribute 49
Acct-Session-Time attribute 49
Active Directory Authentication 49
Active Sessions 28, 44
Active-Directory-Group attribute 19, 52
ADGUM 31
Application Log 42, 44, 78
Attribute 30
Authentication Methods 5
Authentication Required 25
Authentication-Method attribute 19, 49, 50, 51, 83
Authz. Query 21
Backup Database 13
Backup File 13
Change of Authorization 31, 32
Cisco 68
Cisco-AVPair attribute 15, 34
Clear Log 78
Client Certificate 92
Clients 27
Clients Table 27
CoA 31, 32, 45, 56, 69
Create Database 11
Create Tables 11
Credit limit 45
Credit-Expiry-Action attribute 56
Credit-Period attribute 54
Credit-Per-Period attribute 32, 54
Credit-Unit attribute 32, 49, 66
Database Maintenance 13
Database Name 11
Database Tables 11
DB Session Counter 23
Delete accounting records prior to 14
Delimiter Character 17
DHCP Server 37
DHCP-Classless-Static-Route option 39
DHCP-IP-Address option 39
DHCP-IP-Address-Lease-Time option 39
DHCP-Subnet-Mask option 39
Dictionary Editor 33, 34, 35
Directory-Server 51
Directory-Server attribute 51
Disconnect 45
Disconnect Request 31, 33
DSN 7, 18, 104, 105, 107, 108
EAP-AKA 5, 57, 58
EAP-SIM 57
EAP-SIM-Triplet attribute 57
ECDHE 6, 82
E-mail Alerts 25
Enabled 28
Encrypt Passwords 17
Error Duration 26
Expire-Date attribute 48
External-Executable attribute 55
Failure Count 20
Failure-Reply-Type attribute 54
Fair Usage Policy 56
First-Logon attribute 32, 52, 55
Framed-IP-Address attribute 39
Framed-IP-Netmask attribute 39
Framed-Route attribute 39
FUP 56
Generate-MS-MPPE-Keys attribute 53
Google-Authenticator-Issuer 61
Google-Authenticator-Secret 61
Groups 29
Groups Table 12
H3C 68
HTTP Interface Enabled 26
HTTP Port 26
HTTP Reporting Interface 70
HTTP Session Timeout 27
HTTP-Access-Level attribute 58, 70
HTTP-User-Name attribute 58
HTTP-User-Password attribute 58, 59
Huawei 68
IETF Reply-Message (18) 21
Ignore ANSI Warnings 23
IMEI 65
Interim Update Period 28
Issue-Kill-Command 56
Keep Domain Name 20
Kill 28, 45
LDAP 51, 99, 100
Listen IP Address 16, 18

Listen IP Port 18
Log file 42
Logging 16
Login-Time attribute 52, 60
Mail Alerting Enabled 25
Mail From 25
Mail Period 26
Mail To 25
MariaDB 2, 7, 104, 105
Mikrotik 68
Monitoring 44
MS-CHAP 56
msNPCallingStationID 20
msRADIUSFramedIPAddress 20
msRADIUSFramedRoute 20
MySQL 2, 7, 104
NAS 27
NAS-Filter-Rule 31
New DB Field 15
Next-Group attribute 53
ODBC 7, 18, 96, 104, 105, 107, 108
One-Time Password Authentication 50
Oracle 2, 104, 108
OTP 60
Packet of Disconnect 45
PAP 5, 49, 51, 99
Password 10, 25
PEAP Inner Auth. Method 20
PoD 45, 56, 69
PostgreSQL 2, 7, 104, 107, 108
RadSec 5, 19
Refresh Log 78
RegExp Matching 17, 21, 29
Reporting 36
RFC 3756 69
RFC 4849 31
secp256r1 6
secp384r1 6
secp521r1 6
Secret 28
Secure Shutdown 17
Send Failure Reply 21
Send-POD 56
Server Certificate 91
Service Parameters 15, 18, 22, 23, 24, 25, 26
Sessions Table 13
Session-Timeout attribute 39, 48
Session-Timeout parameter 66
Shrink Database 14
Simultaneous-Use attribute 19, 32, 48
Smart Card Reader 17
SMS 60
SMTP Server 25
SMTP Username 25
SQL Connection 9
SQL Server 9
SQLite 7, 8, 104
Starting TekRADIUS 42, 43
Startup 16
TekCERT 90
TekRADIUS Command Line Interface 85
TekRADIUS log file 45, 47
TekRADIUS specific attributes 48
TekRADIUS-Status attribute 39, 48
Test Alerting 26
Time-Limit attribute 52
Timeout 9
TLS-Certificate attribute 83
TLS-Client-Certificate attribute 51
TLS-Server-Certificate attribute 49, 50
TRCLI 56
TRCLI.exe 84, 85
Tunnel-Assignment-ID attribute 54
Tunnel-Client-Auth-ID attribute 54
Tunnel-Client-Endpoint attribute 54
Tunnel-Medium-Type attribute 54
Tunnel-Password attribute 54
Tunnel-Preference attribute 54
Tunnel-Private-Group-ID attribute 54
Tunnel-Server-Auth-ID attribute 54
Tunnel-Server-Endpoint attribute 54
Tunnel-Tag attribute 54
Tunnel-Type attribute 54
Use Def. Authorization Query 21
Use Default Authorization Query 21
User credit 45
User-Credit attribute 49, 54, 55, 66
Username 9
User-Name attribute 20
User-Password attribute 32, 70
User-Quota attribute 49
Users 31
Users Table 11
Vendor 28
VOIP Billing Enabled 22
VPN 56
Windows Auth. Proxy Enabled 19
Windows Domain 20
Windows-Domain attribute 51
x25519 6
ZTE 68