TekRADIUS
Installation & Configuration Guide
Version 5.5
Document Revision 16.5

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 ......................................................................................................... 6
Installation .......................................................................................................................... 7
Configuration ..................................................................................................................... 8
  Settings Tab .................................................................................................................... 8
  Accounting Table ......................................................................................................... 14
  Service Parameters ....................................................................................................... 16
  Alerting ............................................................................................................................ 20
  Clients ............................................................................................................................... 21
  Groups .............................................................................................................................. 23
  Users ................................................................................................................................. 25
Dynamic IP Address Assignment ......................................................................................... 26
Dictionary Editor ................................................................................................................ 27
SQL Query Executioner ..................................................................................................... 28
Reporting ............................................................................................................................ 29
DHCP Server .................................................................................................................... 30
TekRADIUS Manager Menus ............................................................................................. 34
  File Menu ..................................................................................................................... 34
  Service Menu ............................................................................................................... 34
  Help Menu .................................................................................................................... 34
Starting TekRADIUS ......................................................................................................... 35
Monitoring ......................................................................................................................... 36
  Active Sessions ............................................................................................................. 37
  TekRADIUS Log File ................................................................................................. 38
TekRADIUS Specific Attributes (RADIUS Check Items) .................................................. 39
  TekRADIUS-Status ..................................................................................................... 39
  Simultaneous-Use ....................................................................................................... 39
  Simultaneous-Group-Use ............................................................................................ 39
  Expire-Date ................................................................................................................... 39
  User-Credit .................................................................................................................... 40
  Credit-Unit .................................................................................................................... 40
  Authentication-Method ............................................................................................... 40
TLS-Server-Certificate (TLS-Certificate prior to version 4.0) ........................................... 41
TLS-Client-Certificate .................................................................................................... 42
Windows-Domain ............................................................................................................. 42
Directory-Server ............................................................................................................... 42
Active-Directory-Group .................................................................................................. 42
Time-Limit ....................................................................................................................... 43
First-Logon ....................................................................................................................... 43
Login-Time ....................................................................................................................... 43
Generate-MS-MPPE-Keys ................................................................................................. 44
Next-Group ....................................................................................................................... 44
Failure-Reply-Type .......................................................................................................... 44
Tunnel-Tag ....................................................................................................................... 45
Credit-Period .................................................................................................................... 45
Credit-Per-Period ................................................................. 45
External-Executable .............................................................. 46
Credit-Expiry-Action .............................................................. 47
EAP-SIM-Triplet-[1][2][3] ...................................................... 47
HTTP-Access-Level .............................................................. 47
HTTP-User-Name & HTTP-User-Password ................................ 48
Password-Limit ................................................................. 48
Password-Reset ................................................................. 48
Check-MS-DialinPrivilege ..................................................... 48
Lock-MAC-Address ............................................................ 48
Activation-Date ................................................................. 49
Success-Reply-Type ............................................................ 49
OTP-Type ......................................................................... 49
OTP-Length ...................................................................... 49
OTP-Sender ...................................................................... 49
Accounting-Free ............................................................... 49
Data-Volume-Based-Authorization .......................................... 50
Google-Authenticator-Secret .................................................. 50
Google-Authenticator-Issuer .................................................. 51
Quota-Warning-Action ........................................................ 51
Quota-Warning-Threshold .................................................... 51
Concatenated-Password ....................................................... 51
External-Accounting-Action ................................................... 52
Allowed-SSID ................................................................. 52
Data Volume Based Authorization ........................................... 53
Vendor Specific Attribute for Connection Rate Limiting ............... 55
Change of Authorization Support for Disconnecting User Sessions 56
HTTP Interface ................................................................. 57
  Reporting Interface ........................................................ 57
  User Management Interface .............................................. 62
RADIUS Proxy .................................................................... 63
IPv6 Attributes ................................................................... 64
Troubleshooting ................................................................... 65
TekRADIUS Service Messages (TekRADIUS log file) ................. 67
TekRADIUS Command Line Interface - TRCLI.exe .................. 70
Creating and Installing a Self-Signed Certificate for PEAP/EAP-TLS Authentication 74
  Creation of Self Signed Certificate .................................... 74
  Certificate Deployment at Client Side ................................ 75
  Client PEAP Configuration ............................................ 77
  Client EAP-TLS Configuration .................................... 78
SQL Server Configuration .................................................... 80
  Connecting to SQL Express Using TCP/IP ......................... 80
  SQL Express Authentication Configuration ........................ 81
Encoding of Attribute 144 in RFC 4679 (ADSL-Forum Access-Loop-Encapsulation) ......... 82
Failure Codes in Accounting Table DisconnectCause Field when “Save Authentication Failures” Option is Set .................................................. 83
Regular Expression Based Check Attributes ............................ 85
Using Alternative Authentication and Authorization Queries .......... 86
Performance tips ................................................................ 87
Index .............................................................................. 88
Introduction

TekRADIUS is a RADIUS AAA server (Based on RFC 2865 and RFC 2866) and runs under Microsoft Windows (Vista/7/8/10, 2008-2016 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]
- Cisco 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]
- 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.

LEAP, EAP-TLS, EAP-SIM 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.
**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 4.6.1 installed with the latest patches.

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

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 service account for TekRADIUS has read/write access to TekRADIUS application directory and act as part of the operating system (SetbPrivilege) 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. TekRADIUS LT Manager creates database at first run automatically.

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 existing version prior to install a new version. You can keep existing TekRADIUS.ini (Configurations settings), 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 means 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 parameter 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 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.

SQL Connection (Database in LT Edition)

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. 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.

**Password:**

Enter the password of the SQL user.
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.

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 to the attributes received from the access server.

Authentication Query:
If the Use Def. Authorization Query option is unchecked, enter the alternative query. Always use \texttt{AttrType=0} to get check attributes. Query syntax is automatically checked.

By default, to fetch the \texttt{check} attributes from the Users Table, TekRADIUS uses:

\begin{verbatim}
Select Attribute, Val from <users_table> where UserName='%'ietf|1%' and AttrType=0
\end{verbatim}

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 \texttt{AttrType=1} to get success-reply attributes. Query syntax is automatically checked.

By default, to fetch the \texttt{success-reply} attributes from the Users Table, TekRADIUS uses:

\begin{verbatim}
Select Attribute, Val from <users_table> where UserName='% ietf|1%' and AttrType=1
\end{verbatim}
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 password protection method. You can keep passwords in reversible encrypted, hashed or clear text from. Some system integration with 3rd party applications require 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 from to make necessary calculations used in these authentication methods.

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

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.

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 Recording tab.

RegExp Matching:
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.

Enable User Editing for non-Admin Users:
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.

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 password complexity. TekRADIUS Manager will check regular expression as you type. Green background means a valid regular expression entered. Default password policy is

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

- Password must have two uppercase letters.
- Password must have one special case letter.
- Password must have two digits.
- Password must have three lowercase letters.
- Password length must be 8 characters long.

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

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 under the **Database Tables** tab, 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, Accounting.sql and Session.sql for the tables).

![Database Tables Configuration](image)

**Figure 2 - Database Tables Configuration**

**Database 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 to be 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](50) 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),
    [UserName] [nchar](128) NULL,
    [NasIPAddr] [nchar](15) NULL,
    [NasIdentifier] [nchar](255) NULL,
    [NasPort] [nchar](40) 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
) ON [PRIMARY]
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 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 in 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] NOT NULL,
  [SessionID] [nchar](255) NULL,
  [UserName] [nchar](128) NULL,
  [GroupName] [nchar](128) NULL,
  [NasIPAddr] [nchar](15) NULL,
  [NasIdentifier] [nchar](255) NULL,
  [NasPort] [nchar](40) NULL,
  [NasPortType] [nchar](40) NULL,
  [NasPortId] [nchar](255) NULL,
  [ServiceType] [nchar](40) NULL,
  [FramedIPAddr] [nchar](15) NULL,
  [CallingStationID] [nchar](64) NULL,
  [CalledStationID] [nchar](64) NULL,
  [auditsessionid] [nchar](64) NULL
) ON [PRIMARY]
GO
CREATE NONCLUSTERED INDEX [IX_Sessions_1] ON [dbo].[Sessions]
([tracid] ASC)
GO
CREATE NONCLUSTERED INDEX [IX_Sessions_2] ON [dbo].[Sessions]
([TimeStamp] ASC)
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.

> ! The SQL Server service account must have write privilege to selected backup directory.

**Shrink**

To shrink the TekRADIUS database, click **Shrink 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**.

---

**Accounting Table**

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

---

![Figure 3 - Accounting Table Field Selection](image-url)
The left list-box identifies the Accounting Table field; the right list-box identifies the matching RADIUS attribute.

To create additional fields:
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 4 - Adding a dummy attribute for Cisco-AVPair](image-url)
Service Parameters

Enter the following information to configure service specific parameters:

![Figure 5 - Service Parameters Configuration](image)

**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.

**Listen IP 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 a FQDN resolvable to IP address of TekRADIUS machine if it will be used for also HTTPS connections.

**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.

Log files are stored under the `<Application Directory>\Logs directory`.

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.

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.

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.

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.

Def. EAP Method:
You can select default EAP method. Default EAP authentication method is PEAP-EAP-MS-CHAP v2.

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

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.

DHCP Server Enabled:
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.

SSCC (Self Signed Certificate Creation):
Check this option to force TekRADIUS to generate a server certificate dynamically for every PEAP authentication request. If this option is set, it is not necessary to configure a server certificate using the TLS-Server-Certificate attribute.

Server certificate validation must be disabled when this option is enabled.

This option is only available in the commercial edition of TekRADIUS.

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.

HTTP 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.

Accounting Enabled:
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.

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 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.
**Windows Authentication Proxy**

TekRADIUS can act as a proxy for the user accounts defined in the local Windows Domain / Server and Active Directory. 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.

**Windows Auth. Proxy Enabled:**

Check this option to enable the Windows Authentication Proxy feature.

**Type:**

- Windows Domain / Server or Active Directory.

**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 to Active Directory users by settings msRADIUSFramedIPAddress Active Directory attribute.

msNPCallingStationID and msRADIUSFramedIPAddress attribute support requires a commercial license.
Alerting
TekRADIUS can be configured to send e-mail alerts if an error condition occurs for a specified duration.

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.

**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)*.
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 has occurred in 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.

**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**.

**NAS:**

Select and 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 accepts alphanumeric domain names as RADIUS client entries.*

**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:

<table>
<thead>
<tr>
<th>Regular Expression</th>
<th>Input</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>(^.+|)([a-z]+)($)</td>
<td>Domain\user</td>
<td>user</td>
</tr>
<tr>
<td>()([a-z]+)(@[.+]$)</td>
<td>user@Domain</td>
<td>user</td>
</tr>
</tbody>
</table>

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’.

! IMPORTANT! 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 possible to also use other types of utilities that are supported by your access server.
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 it 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.

![Groups Tab](image)

**Figure 8 - 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 attributes 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.

You can create groups with 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 same name of 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.

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 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 9 - Users Tab](image)

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 instruction 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 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.

**Dynamic IP Address Assignment**

Commercial editions of TekRADIUS supports dynamic IP address assignment for the users. You must enable 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 following attributes to the user or group profile to control dynamic IP address assignment parameters;

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

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 as an e-mail attachment to the e-mail address specified in Mail Alerting settings.

![Figure 11 - SQL Query Executioner](image-url)
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.

To select a User or Group, enter the first letters of the User name 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 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 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 of 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 13 - 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 address 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.
The commercial edition of TekRADIUS allows DHCP options to be added to the user profile.
The following RADIUS attributes are translated to DHCP options if they exist in User profiles;

<table>
<thead>
<tr>
<th>RADIUS Attribute</th>
<th>DHCP Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Framed-IP-Address</td>
<td>DHCP-IP-Address</td>
</tr>
<tr>
<td>Framed-IP-Netmask</td>
<td>DHCP-Subnet-Mask</td>
</tr>
<tr>
<td>Framed-Route</td>
<td>DHCP-Classless-Static-Route</td>
</tr>
<tr>
<td>Session-Timeout</td>
<td>DHCP-IP-Address-Lease-Time</td>
</tr>
</tbody>
</table>

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

\[
<\text{Network}>/<\text{Network Bits}> <\text{Default Gateway}>
\]

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 Manager Menus

File Menu

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

Clear Log File. This option clears today's log file.

Normalize MAC addresses. This menu option sets 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 and password pair for an account must be concatenated with a comma as shown below;

Username1,Password1
Username2,Password2

Exit. Closes TekRADIUS Manager.

Service Menu

Start. Starts TekRADIUS background service.

Stop. Stops TekRADIUS background service.

Help Menu

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


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.
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 17 - 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

In order 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. This allows you 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 request attributes must be defined in user or group profiles prior to send 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.
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 a number of 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

In order 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).

In order 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 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 assume 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-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:

![TekOTP](image)

**Figure 19 - 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 the **Configuration / Server Settings** tab 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 **Configuration / Server Settings** tab or as a specific **Directory-Server** attribute in a User or Group profile.

**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 semicolon like Group1;Group2;Group3.

**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.

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)

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. 22:00-01:30 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-MPPE-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 profiles for each NAS-IP-Address value and chain these Groups using the Next-Group attribute.

*It is not possible to use Next-Group attribute with PEAP authentication.*

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 is to send Failure-Reply attributes in an Access-Reject message. Add FailonPasswordFailure=1 parameter under [Server] section of TekRADIUS.ini in order 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.

If this attribute does not exist in a User or Group profile, TekRADIUS assumes a tag value of 1. 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’ 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 be failed.

Enter the full path of the executable as the value of the *External-Executable* attribute. Use double quotes (“ ”) if the path contains space characters. 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.

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

- `External-Executable = C:\Test.bat %ietf|1% %ietf|2%`
- `External-Executable = "C:\Program Files\My App\test.exe" -log %ietf|1% %ietf|2%`
- `External-Executable = "C:\Program\multiotp\multiotp.exe" %ietf|1% %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.

*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:

```plaintext
test|2=password
test|27=3600
test|18=Reply message
```

Sample .bat file content to provide the output above:

```plaintext
@echo off
test\^|2=password
test\^|27=3600
test\^|18=Reply message
```

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

```plaintext
exit /B 0
```
line at the end of the batch file if you like to return positive *(Successful)* response.

**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 bolded 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 attributes in User or Group profiles.

**HTTP-Access-Level**

The *HTTP-Access-Level* attribute is used as a check attribute in User or Group profiles. This attribute specifies 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 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 attribute 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 password age is expired. TekRADIUS will add Password-Reset attribute to the user profile after a successful password change operation.

Password-Limit attribute is 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 change his/her password at first logon.

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 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 Calling-Station-Id attribute as check attribute automatically at user’s first logon attempt. TekRADIUS will check if user tries to logon 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 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 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 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 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 integer type attribute and can exist as check attributes in User or Group profiles.

**OTP-Sender**

You can specify an external program or script to deliver generated generic OTP to remote users. Such applications typically deliver OTPs via e-mail or SMS messages.

**OTP-Sender** attribute is a string 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 similar to *Login-Time* attribute;

\[ \text{[Su|Mo|Tu|We|Th|Fr|Sa|Wk|Hd|Al]<Begin Hour>-<End Hour>} \]

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 a 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 user name in QR code for initialization of Google Authenticator for a user. You can also add an issuer name to be displayed when 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 and 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 Quota-Warning-Threshold attribute to user or group profiles as a check attribute. Its value based on credit amount. If you plan to issue a warning when user consumption reaches to 80% and users’ credit is set to 8000, you should set Quota-Warning-Threshold = 6400.

Quota-Warning-Threshold attribute is 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 part using 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 pattern 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.

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 for the syntax.

*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.
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-MaxGigaWords-Up (*Giga count for each 4 GByte*)
- Nomadix-MaxBytesDown, 32 bit value of number of allowed output octets.
- Nomadix-MaxGigaWords-Down (*Giga count for each 4 GByte*)
- Nomadix-MaxBytes-Total
- Nomadix-MaxGigaWords-Total (*Giga count for each 4 GByte*)

**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-AVP=PAIR=max-input-ocet=<32 bit value of number of allowed input octets>
- Colubris-AVP=PAIR=max-output-ocet=<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>
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 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.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Bytes-in, KBytes-in, MBytes-in</th>
<th>Bytes-out, KBytes-out, MBytes-out</th>
<th>Bytes-sum, KBytes-sum, MBytes-sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mikrotik</td>
<td>Mikrotik-Recv-Limit</td>
<td>Mikrotik-Xmit-Limit</td>
<td>Mikrotik-Total-Limit</td>
</tr>
<tr>
<td>Nomadix</td>
<td>Nomadix-MaxBytesDown</td>
<td>Nomadix-MaxBytesUp</td>
<td>Nomadix-MaxBytes-Total</td>
</tr>
<tr>
<td>ChilliSpot</td>
<td>ChilliSpot-Max-Input-Octets</td>
<td>ChilliSpot-Max-Output-Octets</td>
<td>ChilliSpot-Max-Total-Octets</td>
</tr>
<tr>
<td>Colubris</td>
<td>Colubris-AVPAIR=max-input-octets</td>
<td>Colubris-AVPAIR=max-output-octets</td>
<td>Colubris-AVPAIR=max-output-octets</td>
</tr>
</tbody>
</table>

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 also do 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 attribute 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

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

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

Generic (IETF)

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

Cisco

- Acct-Session-Id
- Framed-IP-Address
- Service-Type = Login

Mikrotik

- Acct-Session-Id
- Framed-IP-Address
- NAS-IP-Address

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 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 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 two access levels to HTTP Interface: User and 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.

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 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;

```html
<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 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 on all users data.

Admin report form must contain 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';
    if (isPlacedUnder) {
        setPosition(divstyle, positionerImgName, true);
    } else {
        setPosition(divstyle, positionerImgName, true);
    }
}

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("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 Avg", "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]));
}
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++)
    sel2.options.add(new Option(OrderByOptions2[i], OrderByOptions2[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>
</select>
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; there are implemented as:

```javascript
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 user name 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>

<form name="PasswordForm" method="post" action="changepass" id="TekRADIUSPasswordForm">
<table align="left" id="TekRADIUSPasswordTable">
<tr>
<td align="right" valign="top">
<strong>Old password:&nbsp</strong>
<input id="oldpassword" name="oldpassword" type="password" value="" />
</td>
</tr>
<tr>
<td align="right" valign="top">
<strong>New password:&nbsp</strong>
<input id="newpassword" name="newpassword" type="password" value="" />
</td>
</tr>
<tr>
<td align="right" valign="top">
<strong>Confirm:&nbsp</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>
</head>
<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 group name.

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 20 - TekRADIUS Proxy Profiles](image)

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 enabled 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 order of remote servers by dragging entries.
IPv6 Attributes

TekRADIUS supports IPv6 attributes specified in RFC 3162, RFC 4818 and RFC 6911. Please use 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. 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 **Application Log** 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 21 - TekRADIUS Counters on Windows Performance Monitor](image-url)
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.

![TekRADIUS Manager Counters Tab](image)

**Figure 22** - 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 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 necessary 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, and 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

- 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_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

A ‘Handshake Failure Alert’ will be also 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.
**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:

```bash
C:\Program Files (x86)\TekRADIUS>trcli

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] "Client IP Address" secret
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 (x86)\TekRADIUS>trcli -u test test123
```

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

**Delete a user:**

```
C:\Program Files (x86)\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:
An example of the use of the Microsoft *MS-Primary-DNS-Server* attribute would be:

C:\Program Files (x86)\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 (x86)\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 (x86)\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 (x86)\TekRADIUS> trcli -m kaplan "ietf|2" check
Attribute 'ietf|2' for the user 'kaplan' has been deleted...

C:\Program Files (x86)\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 (x86)\TekRADIUS> trcli -m kaplan "ietf|0" check
Attribute 'ietf|0' for the user 'kaplan' has been deleted...

C:\Program Files (x86)\TekRADIUS> trcli -a kaplan "ietf|0" newgroup check
Attribute 'ietf|0' for the user 'kaplan' has been added...

**Disable a user without deleting.** Add the attribute *kaplansoft|0* to the user profile with a value of ‘0’;

C:\Program Files (x86)\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 (x86)\TekRADIUS> trcli -c add 102.168.10.10 radius_secret
Client 192.168.10.1 added... Restart TekRADIUS service.
It is necessary to re-start TekRADIUS in order to receive RADIUS packets from the RADIUS clients. 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.

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 (x86)\TekRADIUS>trcli -c delete 102.168.10.10
Client 192.168.10.1 deleted... Restart TekRADIUS service.

List all RADIUS client entries:

C:\Program Files (x86)\TekRADIUS>trcli -c list
127.0.0.1,test,ietf,Enabled
192.168.19.1,deneme,ietf,Disabled
192.168.10.1,test,ietf,Enabled

List active sessions:

C:\Program Files (x86)\TekRADIUS>trcli -l

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>Duration</th>
<th>SessionID</th>
<th>UserName</th>
<th>GroupName</th>
<th>NasIPAddr</th>
<th>NasIdentifier</th>
<th>NasPort</th>
<th>NasPortType</th>
<th>NasPortID</th>
<th>ServiceType</th>
<th>FramedIPAddr</th>
<th>CallingStationID</th>
<th>CalledStationID</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.7.2015 16:55:20</td>
<td>4174</td>
<td>80700006</td>
<td>dwadley</td>
<td>11</td>
<td>192.168.1.43</td>
<td>myport-mstreet, 2154823686</td>
<td>Ethernet, wlan-Hotspot,</td>
<td>10.5.50.4</td>
<td>8C:29:37:B6:06:FF</td>
<td>hotspot1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.7.2015 17:04:45</td>
<td>4165</td>
<td>80700006</td>
<td>kaplan</td>
<td>Blank</td>
<td>192.168.1.43</td>
<td>myport-mstreet, 2154823686</td>
<td>Ethernet, wlan-Hotspot,</td>
<td>10.5.50.4</td>
<td>8C:29:37:B6:06:FF</td>
<td>hotspot1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2 active sessions found.

List active session:

C:\Program Files (x86)\TekRADIUS>trcli -l kaplan

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>Duration</th>
<th>SessionID</th>
<th>UserName</th>
<th>GroupName</th>
<th>NasIPAddr</th>
<th>NasIdentifier</th>
<th>NasPort</th>
<th>NasPortType</th>
<th>NasPortID</th>
<th>ServiceType</th>
<th>FramedIPAddr</th>
<th>CallingStationID</th>
<th>CalledStationID</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.7.2015 17:04:45</td>
<td>4165</td>
<td>80700006</td>
<td>kaplan</td>
<td>Blank</td>
<td>192.168.1.43</td>
<td>myport-mstreet, 2154823686</td>
<td>Ethernet, wlan-Hotspot,</td>
<td>10.5.50.4</td>
<td>8C:29:37:B6:06:FF</td>
<td>hotspot1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1 active session found.

Clear a user’s session:

C:\Program Files (x86)\TekRADIUS>trcli -q kaplan

Send a Packet of Disconnect Request (RFC 3576):

C:\Program Files (x86)\TekRADIUS>trcli -k kaplan pod

Send a Change of Authorization Request (RFC 3576):

C:\Program Files (x86)\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 following format for the attributes:

VendorName|AttributeId=Value
You can concatenate multiple attributes with semicolon. 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:

```
trc -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;

```
trc -k Kaplan coaset
trc -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 user name to send CoA or PoD request to all online users;

```
trc -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 (x86)\TekRADIUS>trcli -k Acct-Session-Id=01aa33d coa "Framed-IP-Address=192.168.1.10"
```

You can use 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)

User passwords are encrypted in Authentication and Group tables in TekRADIUS versions 2.3 and 2.4.

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 in the under Database section before starting TekRADIUS.

The performance counter values can be retrieved with the -p parameter.
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 23 - TekCERT Certificate Parameters](image)

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 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 computer:

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 24 - Select Certificate Store 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 ),
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.

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.
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 different to user’s Windows login 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.

**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.
4. Select the wireless network that requires PEAP authentication,
5. Click Properties.
6. Configure the ‘Association’ parameters, as shown in Figure 35.
7. Select the ‘Authentication’ tab,
8. Select ‘Smart Card or Certificate’ as ‘EAP Type’ from the drop-down list,
9. Click Properties.

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:

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 38 - SQL Server Configuration Manager

Figure 39. - TCP/IP Properties Protocol Selection
Figure 40. - 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 the port number as 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 41. - SQL Express Configuration](image)

1. On the machine with SQL Express installed, open the SQL Server Management Studio Express tool.
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:

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-----------------------------------------------+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Link</td>
<td>Encaps 1</td>
</tr>
<tr>
<td>+-----------------------------------------------+</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Failure Code</th>
<th>Failure Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>1100</td>
<td>Authentication failed</td>
</tr>
<tr>
<td>1101</td>
<td>Windows domain authentication failure</td>
</tr>
<tr>
<td>1102</td>
<td>Windows Active Directory authentication failure</td>
</tr>
<tr>
<td>1103</td>
<td>LDAP authentication failed</td>
</tr>
<tr>
<td>1104</td>
<td>Valid certificate cannot be found</td>
</tr>
<tr>
<td>1105</td>
<td>Invalid authentication method</td>
</tr>
<tr>
<td>1106</td>
<td>External authenticator returned negative response</td>
</tr>
<tr>
<td>1107</td>
<td>Active Directory group does not match</td>
</tr>
<tr>
<td>1108</td>
<td>Missing server certificate</td>
</tr>
<tr>
<td>1109</td>
<td>TLS Certificate cannot be generated</td>
</tr>
<tr>
<td>1110</td>
<td>SIM triplets not configured</td>
</tr>
<tr>
<td>1111</td>
<td>Client certificate cannot be generated</td>
</tr>
<tr>
<td>1112</td>
<td>EAP-SIM Authentication failure</td>
</tr>
<tr>
<td>1113</td>
<td>CHAP authentication failed</td>
</tr>
<tr>
<td>1114</td>
<td>Absent user</td>
</tr>
<tr>
<td>1115</td>
<td>Invalid password</td>
</tr>
<tr>
<td>1116</td>
<td>Password expired</td>
</tr>
<tr>
<td>1117</td>
<td>MS-CHAP-v1 authentication failed</td>
</tr>
<tr>
<td>1118</td>
<td>MS-CHAP-v2 authentication failed</td>
</tr>
<tr>
<td>1119</td>
<td>MS-CHAP-v2 authentication failed (NTLM)</td>
</tr>
<tr>
<td>1120</td>
<td>User-Password required</td>
</tr>
<tr>
<td>1121</td>
<td>User quota exits, accounting is not enabled</td>
</tr>
<tr>
<td>1122</td>
<td>Time limit reached</td>
</tr>
<tr>
<td>1123</td>
<td>Login time restriction</td>
</tr>
<tr>
<td>1124</td>
<td>OTP authentication failed</td>
</tr>
<tr>
<td>1125</td>
<td>PAP authentication failed</td>
</tr>
<tr>
<td>1126</td>
<td>Digest authentication failure</td>
</tr>
<tr>
<td>1127</td>
<td>Local user profile expired</td>
</tr>
<tr>
<td>1128</td>
<td>User profile is not active</td>
</tr>
<tr>
<td>1129</td>
<td>Simultaneous limit reached</td>
</tr>
<tr>
<td>1130</td>
<td>Local user profile disabled</td>
</tr>
<tr>
<td>1131</td>
<td>CHAP authentication failed (OTP)</td>
</tr>
<tr>
<td>1132</td>
<td>CHAP authentication is not supported with Windows/NTLM Authentication Proxy</td>
</tr>
<tr>
<td>1133</td>
<td>Windows authentication is not supported in freeware edition</td>
</tr>
<tr>
<td>1134</td>
<td>OTP authentication is not supported in freeware edition</td>
</tr>
<tr>
<td>1135</td>
<td>User-Name does not match</td>
</tr>
<tr>
<td>1136</td>
<td>RADIUS authentication request does not contain required check attribute</td>
</tr>
<tr>
<td>1137</td>
<td>Check attribute value does not match</td>
</tr>
<tr>
<td>Failure Code</td>
<td>Failure Case</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>1138</td>
<td>Invalid attribute value</td>
</tr>
<tr>
<td>1139</td>
<td>External executable returned negative response</td>
</tr>
<tr>
<td>1140</td>
<td>Windows domain authentication failed since user group is disabled</td>
</tr>
<tr>
<td>1141</td>
<td>LDAP authentication failed since user group is disabled</td>
</tr>
<tr>
<td>1142</td>
<td>User account has no permission to login at the moment</td>
</tr>
<tr>
<td>1143</td>
<td>Insufficient credit</td>
</tr>
<tr>
<td>1144</td>
<td>Simultaneous limit has been set but accounting is not enabled</td>
</tr>
<tr>
<td>1145</td>
<td>User group is disabled</td>
</tr>
</tbody>
</table>
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 have to 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 are 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 must 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 user name and room number as user password. In this case, create the following SQL View:

```sql
Create View AlternativeUsers as Select [Surname] as UserName, 'ietf|1' as Attribute, 0 as AttrType, [Surname] 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:

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

and alternative Authorization query:

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

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 field named tracid and an index for it to Accounting table in order to speed up Accounting functions. Please check if they exist.
- Rebuild indexes after purging old accounting records in Accounting table.
- Disable unused vendor dictionaries in TekRADIUS Manager / Dictionary.
- Lower logging level to Error at settings / service parameters.
Index

Access-Accept Messages ..................................17
Accounting Enabled ........................................18
Accounting Port ............................................18
Accounting Table ..........................................12, 14
Accounting-Checkpoint Message ......................18
Accounting-Interim-Updates message ...............47
Accounting-Off Message ................................18
Accounting-Stop Message ...............................18, 39
Acct-Input-Octets attribute ............................40
Acct-Output-Octets attribute .........................40
Acct-Session-Time attribute .............................40
Active Directory Authentication ......................40
Active Sessions ............................................22, 36
Active-Directory-Group attribute ......................19, 42
Alerting ......................................................20
Application Log ...........................................35, 36, 65
Attribute ....................................................24
Authentication Methods .....................................5
Authentication Required ..................................20
Authentication-Method attribute .....................19, 40, 41, 42, 69
Authz. Query ..............................................9
Backup Database .........................................14
Backup File ................................................14
Change of Authorization ...............................25, 26
Cisco .........................................................55
Cisco-AVPair attribute ..................................15, 27
Clear Log ....................................................65
Client Certificate ..........................................76
Clients ......................................................21
Clients Table ..............................................21
CoA ..........................................................25, 26, 37, 47, 56
Create Database ..........................................12
Create Tables ...............................................12
Credit limit ..................................................37
Credit-Expiry-Action attribute .........................47
Credit-Period attribute ..................................45
Credit-Per-Period attribute .............................26, 45
Credit-Unit attribute .....................................26, 40, 54
Database Maintenance ....................................14
Database Name ..........................................12
Database Tables ...........................................11
DB Session Counter ....................................10
Delete accounting records prior to .................14
Delimiter Character .....................................10
DHCP Server .............................................30
DHCP Server Enabled ....................................17
DHCP-Classless-Static-Route option .............32
DHCP-IP-Address option ................................32
DHCP-IP-Address-Lease-Time option .............32
DHCP-Subnet-Mask option .........................32
Dictionary Editor .........................................26, 27, 28
Directory-Server attribute ............................42
Disconnect ..................................................37
Disconnect Request .....................................25, 26
EAP-SIM .....................................................47
EAP-SIM-Triplet attribute ...............................47
E-mail Alerts ..............................................20
Enabled ......................................................22
Encrypt Passwords .......................................10
Error Duration ............................................20
Expire-Date attribute ....................................39
External-Executable attribute .......................46
Failure Count ............................................17
Failure-Reply-Type attribute .........................44
Fair Usage Policy .........................................47
First-Logon attribute ....................................26, 43, 45
Framed-IP-Address attribute .........................32
Framed-IP-Netmask attribute .........................32
Framed-Route attribute ................................32
FUP .........................................................47
Generate-MS-MPPE-Keys attribute .................44
Google-Authenticator-Issuer .........................51
Google-Authenticator-Secret .........................50
Groups ......................................................23
Groups Table ..............................................13
H3C ........................................................55
HTTP Interface Enabled ................................18
HTTP Port ................................................18
HTTP Reporting Interface ..............................57
HTTP Session Timeout ..................................18
HTTP-Access-Level attribute .......................47, 57
HTTP-User-Name attribute ............................48
HTTP-User-Password attribute .....................48, 49
Huawei ....................................................55
IETF Reply-Message (18) ..............................17
Ignore ANSI Warnings ....................................9
Interim Update Period ..................................22
Issue-Kill-Command .....................................47
Keep Domain Name .....................................17
Kill .........................................................22, 37
Listen IP Address ........................................16
Listen IP Port .............................................16
Log file .....................................................35
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging</td>
<td>17</td>
</tr>
<tr>
<td>Login-Time attribute</td>
<td>43, 49</td>
</tr>
<tr>
<td>Mail Alerting Enabled</td>
<td>20</td>
</tr>
<tr>
<td>Mail From</td>
<td>20</td>
</tr>
<tr>
<td>Mail Period</td>
<td>20</td>
</tr>
<tr>
<td>Mail To</td>
<td>20</td>
</tr>
<tr>
<td>Mikrotik</td>
<td>55</td>
</tr>
<tr>
<td>Monitoring</td>
<td>36</td>
</tr>
<tr>
<td>MS-CHAP</td>
<td>46</td>
</tr>
<tr>
<td>msNPCallingStationID</td>
<td>19</td>
</tr>
<tr>
<td>msRADIUSFramedIPAddress</td>
<td>19</td>
</tr>
<tr>
<td>NAS</td>
<td>21</td>
</tr>
<tr>
<td>New DB Field</td>
<td>15</td>
</tr>
<tr>
<td>Next-Group attribute</td>
<td>44</td>
</tr>
<tr>
<td>One-Time Password Authentication</td>
<td>41</td>
</tr>
<tr>
<td>OTP</td>
<td>49</td>
</tr>
<tr>
<td>Packet of Disconnect</td>
<td>37</td>
</tr>
<tr>
<td>Password</td>
<td>8, 20</td>
</tr>
<tr>
<td>PEAP Inner Auth. Method</td>
<td>17</td>
</tr>
<tr>
<td>PoD</td>
<td>37, 47, 56</td>
</tr>
<tr>
<td>Refresh Log</td>
<td>65</td>
</tr>
<tr>
<td>RegExp Matching</td>
<td>10, 11, 23</td>
</tr>
<tr>
<td>Reporting</td>
<td>29</td>
</tr>
<tr>
<td>RFC 3756</td>
<td>56</td>
</tr>
<tr>
<td>Secret</td>
<td>21, 22</td>
</tr>
<tr>
<td>Secure Shutdown</td>
<td>17</td>
</tr>
<tr>
<td>Send Failure Reply</td>
<td>17</td>
</tr>
<tr>
<td>Send-POD</td>
<td>47</td>
</tr>
<tr>
<td>Server Certificate</td>
<td>75</td>
</tr>
<tr>
<td>Service Parameters</td>
<td>16</td>
</tr>
<tr>
<td>Sessions Table</td>
<td>13</td>
</tr>
<tr>
<td>Session-Timeout attribute</td>
<td>32, 39</td>
</tr>
<tr>
<td>Session-Timeout parameter</td>
<td>53</td>
</tr>
<tr>
<td>Shrink Database</td>
<td>14</td>
</tr>
<tr>
<td>Simultaneous-Use attribute</td>
<td>19, 26, 39</td>
</tr>
<tr>
<td>Smart Card Reader</td>
<td>17</td>
</tr>
<tr>
<td>SMS</td>
<td>49</td>
</tr>
<tr>
<td>SMTP Server</td>
<td>20</td>
</tr>
<tr>
<td>SMTP Username</td>
<td>20</td>
</tr>
<tr>
<td>SQL Connection</td>
<td>8</td>
</tr>
<tr>
<td>SQL Server</td>
<td>8</td>
</tr>
<tr>
<td>SCC (Self Signed Certificate Creation)</td>
<td>18</td>
</tr>
<tr>
<td>Starting TekRADIUS</td>
<td>35</td>
</tr>
<tr>
<td>Startup</td>
<td>17</td>
</tr>
<tr>
<td>TekCERT</td>
<td>74</td>
</tr>
<tr>
<td>TekRADIUS Command Line Interface</td>
<td>70</td>
</tr>
<tr>
<td>TekRADIUS log file</td>
<td>37, 38</td>
</tr>
<tr>
<td>TekRADIUS specific attributes</td>
<td>39</td>
</tr>
<tr>
<td>TekRADIUS-Status attribute</td>
<td>32, 39</td>
</tr>
<tr>
<td>Test Alerting</td>
<td>21</td>
</tr>
<tr>
<td>Time-Limit attribute</td>
<td>43</td>
</tr>
<tr>
<td>Timeout</td>
<td>8</td>
</tr>
<tr>
<td>TLS-Certificate attribute</td>
<td>69</td>
</tr>
<tr>
<td>TLS-Client-Certificate attribute</td>
<td>42</td>
</tr>
<tr>
<td>TLS-Server-Certificate attribute</td>
<td>18, 40, 41</td>
</tr>
<tr>
<td>TRCLI</td>
<td>47</td>
</tr>
<tr>
<td>TRCLL.exe</td>
<td>70</td>
</tr>
<tr>
<td>Tunnel-Assignment-ID attribute</td>
<td>45</td>
</tr>
<tr>
<td>Tunnel-Client-Auth-ID attribute</td>
<td>45</td>
</tr>
<tr>
<td>Tunnel-Client-Endpoint attribute</td>
<td>45</td>
</tr>
<tr>
<td>Tunnel-Medium-Type attribute</td>
<td>45</td>
</tr>
<tr>
<td>Tunnel-Passwd attribute</td>
<td>45</td>
</tr>
<tr>
<td>Tunnel-Preference attribute</td>
<td>45</td>
</tr>
<tr>
<td>Tunnel-Private-Group-ID attribute</td>
<td>45</td>
</tr>
<tr>
<td>Tunnel-Server-Auth-ID attribute</td>
<td>45</td>
</tr>
<tr>
<td>Tunnel-Server-Endpoint attribute</td>
<td>45</td>
</tr>
<tr>
<td>Tunnel-Tag attribute</td>
<td>45</td>
</tr>
<tr>
<td>Tunnel-Type attribute</td>
<td>45</td>
</tr>
<tr>
<td>Use Def. Authorization Query</td>
<td>9</td>
</tr>
<tr>
<td>Use Defa ult Authorization Query</td>
<td>9</td>
</tr>
<tr>
<td>User credit</td>
<td>37</td>
</tr>
<tr>
<td>User-Credit attribute</td>
<td>40, 45, 54</td>
</tr>
<tr>
<td>Username</td>
<td>8</td>
</tr>
<tr>
<td>User-Name attribute</td>
<td>17</td>
</tr>
<tr>
<td>User-Password attribute</td>
<td>26, 57</td>
</tr>
<tr>
<td>User-Quota attribute</td>
<td>40</td>
</tr>
<tr>
<td>Users</td>
<td>25</td>
</tr>
<tr>
<td>Users Table</td>
<td>12</td>
</tr>
<tr>
<td>Vendor</td>
<td>22</td>
</tr>
<tr>
<td>VOIP Billing Enabled</td>
<td>18</td>
</tr>
<tr>
<td>VPN</td>
<td>46</td>
</tr>
<tr>
<td>Windows Auth. Proxy Enabled</td>
<td>19</td>
</tr>
<tr>
<td>Windows Authentication Proxy</td>
<td>19</td>
</tr>
<tr>
<td>Windows Domain</td>
<td>19</td>
</tr>
<tr>
<td>Windows-Domain attribute</td>
<td>42</td>
</tr>
<tr>
<td>ZTE</td>
<td>55</td>
</tr>
</tbody>
</table>