Est. USA 1981

www.AKCP.com

SP+ Radius User Manual

FreeRADIUS

The world's most popular RADIUS Server

Table of Contents

Introduction

What is RADIUS

Remote Authentication Dial In User Service (**RADIUS**) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service.

This is a feature that we've added to the sensorProbe+ web interface so that the unit can be accessed securely through a Radius Server running on the Local Area Network. It is used to:

A. To authenticate users or devices before granting them access to the units web interface,
B. To authorize those users or devices for access the the units web interface.
C. Accounting is the process of generating log files that record session statistics used for billing, system diagnosis, and usage planning.

Implementation

The sensorProbe+ implements Radius Authentication(RFC 2865) and Accounting(RFC 2866) via the web interface. It means that only log in or log off via the web interface can be authenticated (and logged) with the Radius Server.

As of firmware 5937 it is possible to define specific attributes for each user at the server side to check whether the user has administrator rights or just a simple user (privilege level checking).

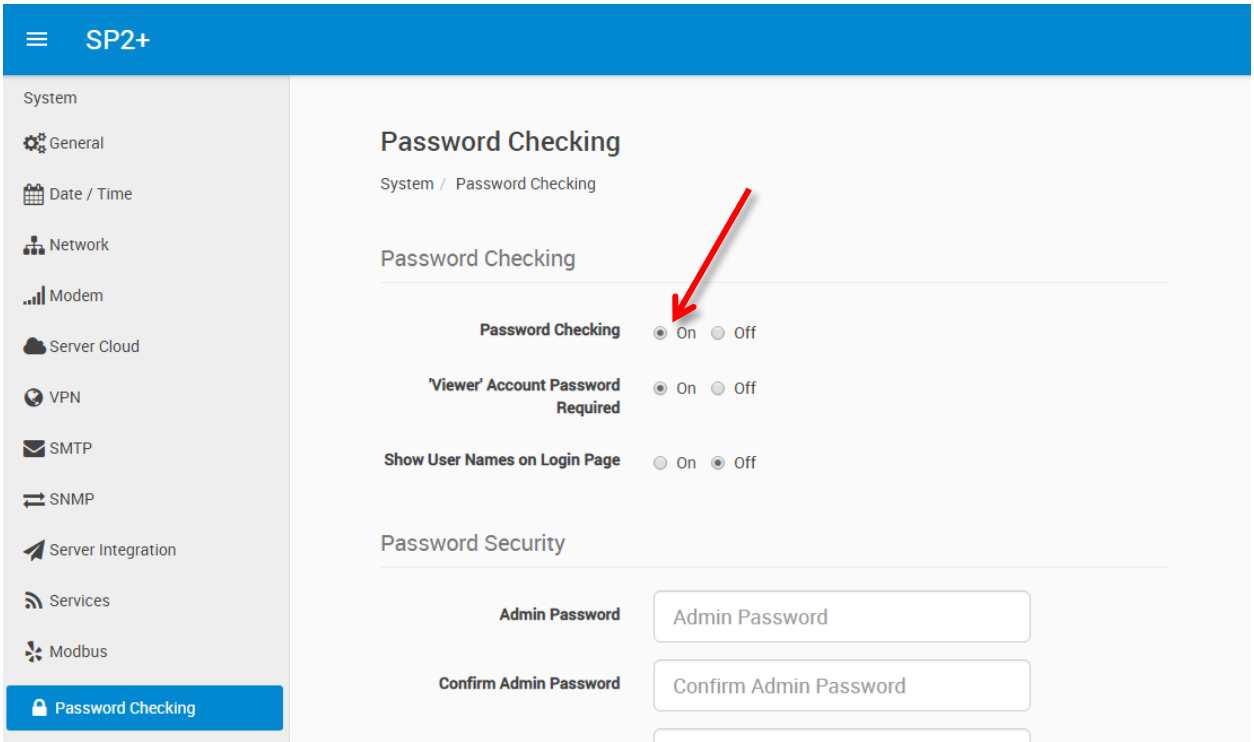
All Radius users which doesn't have the privilege level attributes set, will only have Viewer level (read-only) access to the SP+ web UI (for details, see the section *How it works*).

IPv6 information

In this manual we'll only show the configuration using IPv4 addressing, but the sensorProbe+ also supports Radius with IPv6. The only difference is the IP address format; everything else in the configuration is identical with IPv4.

Setting up Radius on the sensorProbe+

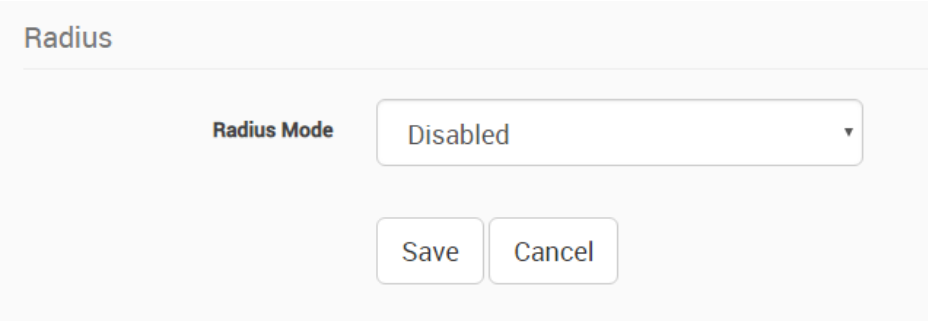
1. Enable the Radius Server authentication



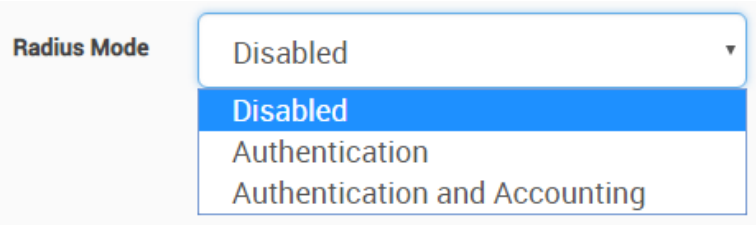
First log in to the sensorProbe+ as an Administrator (Admin user).

Then navigate to the **Settings page >> Password Checking** and turn it on as shown in the screen shot above. Depending on your setup, you may have password checking enabled already.

Scroll down on the page for the **Radius settings**:

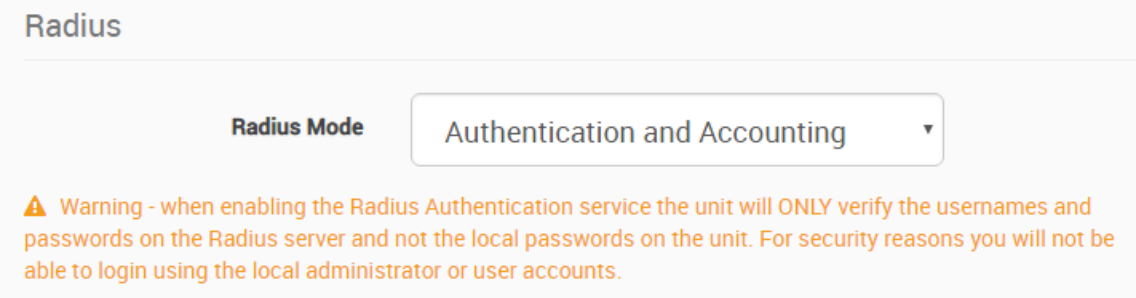


By default Radius is disabled.



Enable the Radius password checking on the sensorProbe+ by choosing the Radius Mode:

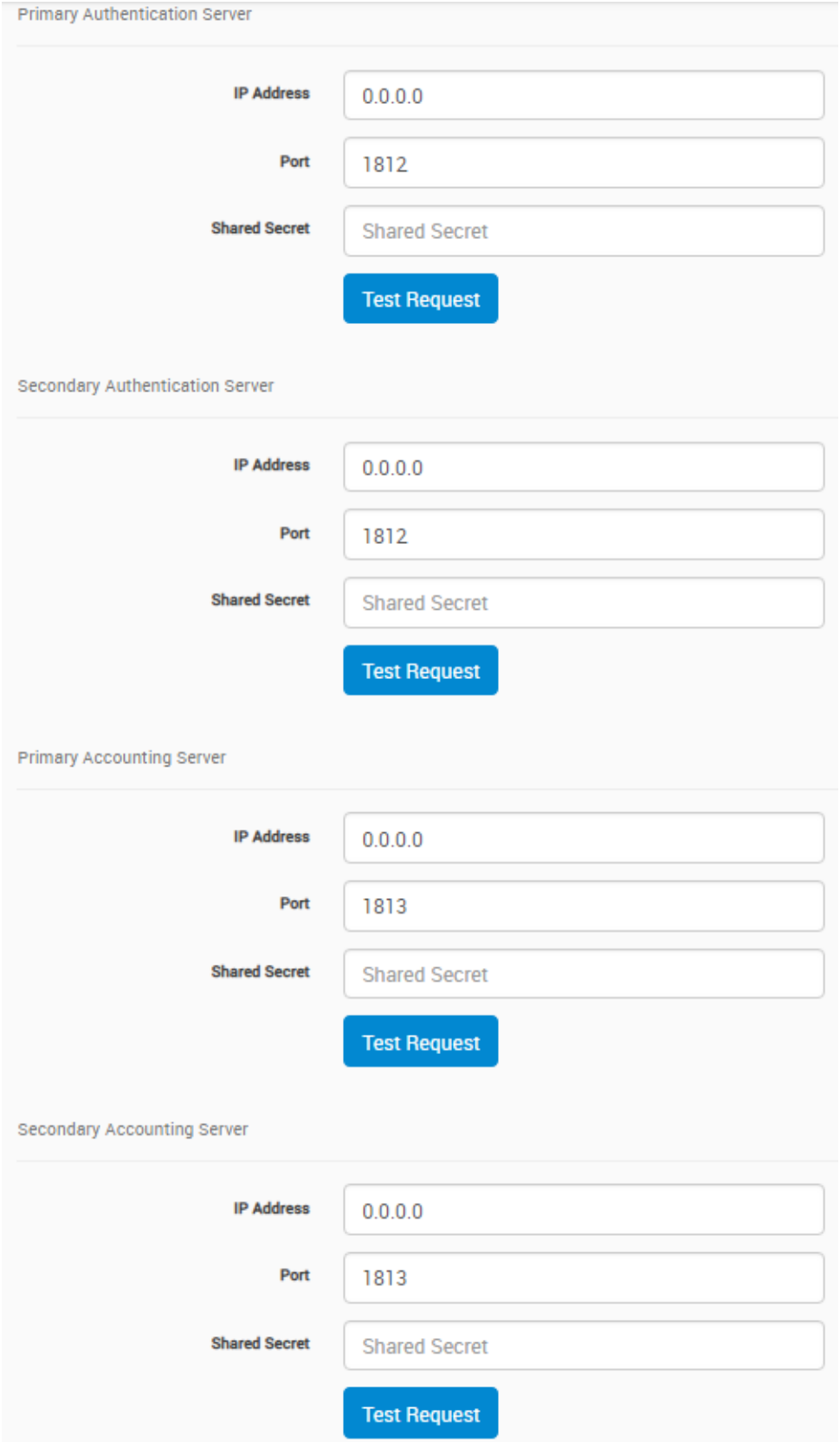
- **Authentication:** usernames and passwords will be ONLY checked with Radius server
- **Authentication and Accounting:** as above but also log the access data on the server



The most important parameters for the configuration are:

1. IP Address of the Radius server
2. Shared Secret
3. Port (if it's different than the default 1812 and 1813)

Before saving your settings, make sure that you test them (see below).

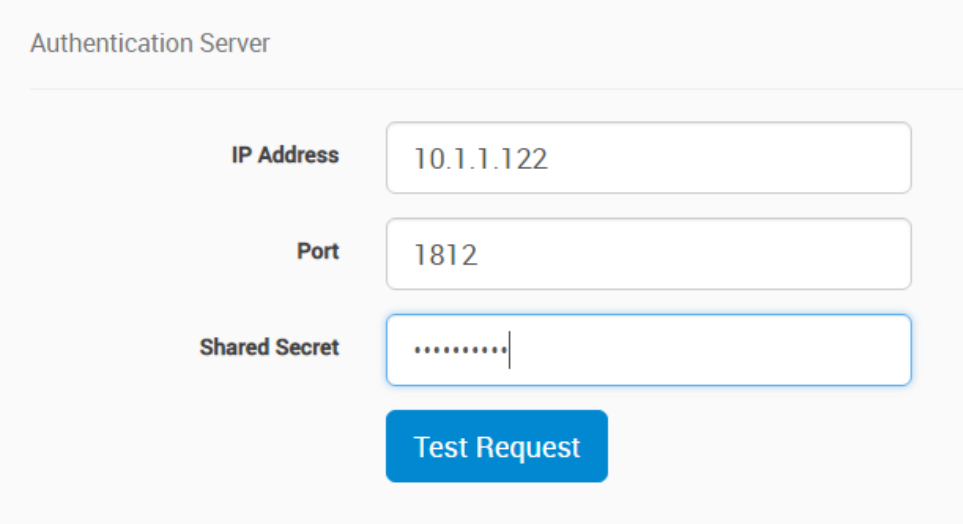


You can also specify secondary servers for redundancy (both for Authentication and Accounting), but if you only have one server just use the **Primary server's options** and leave the Secondary settings at default.

Scroll down the screen to enter the Secondary server options, or leave them at default settings.

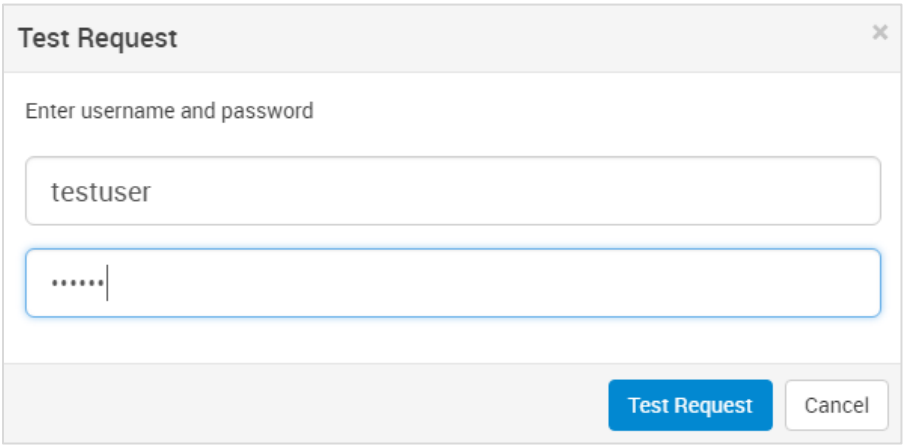
See below in this manual for information about the algorithm used for the failover.

2. Set up the connection in the sensorProbe+ Web UI

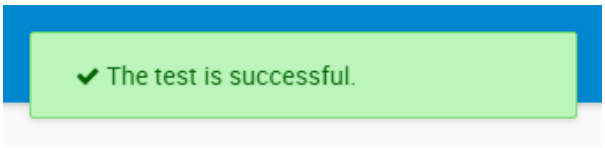


Specify the parameters for the **Radius Primary Authentication Server**.

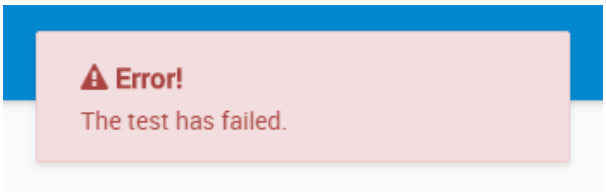
Now you need to enter the IP address of the server machine, the port and the shared secret, then click on the "*Test Request*" button which will bring up the dialog box as shown in the screen shot below:



Enter the Username and Password of a valid Radius user and click the "*Send Testing Request*" button.

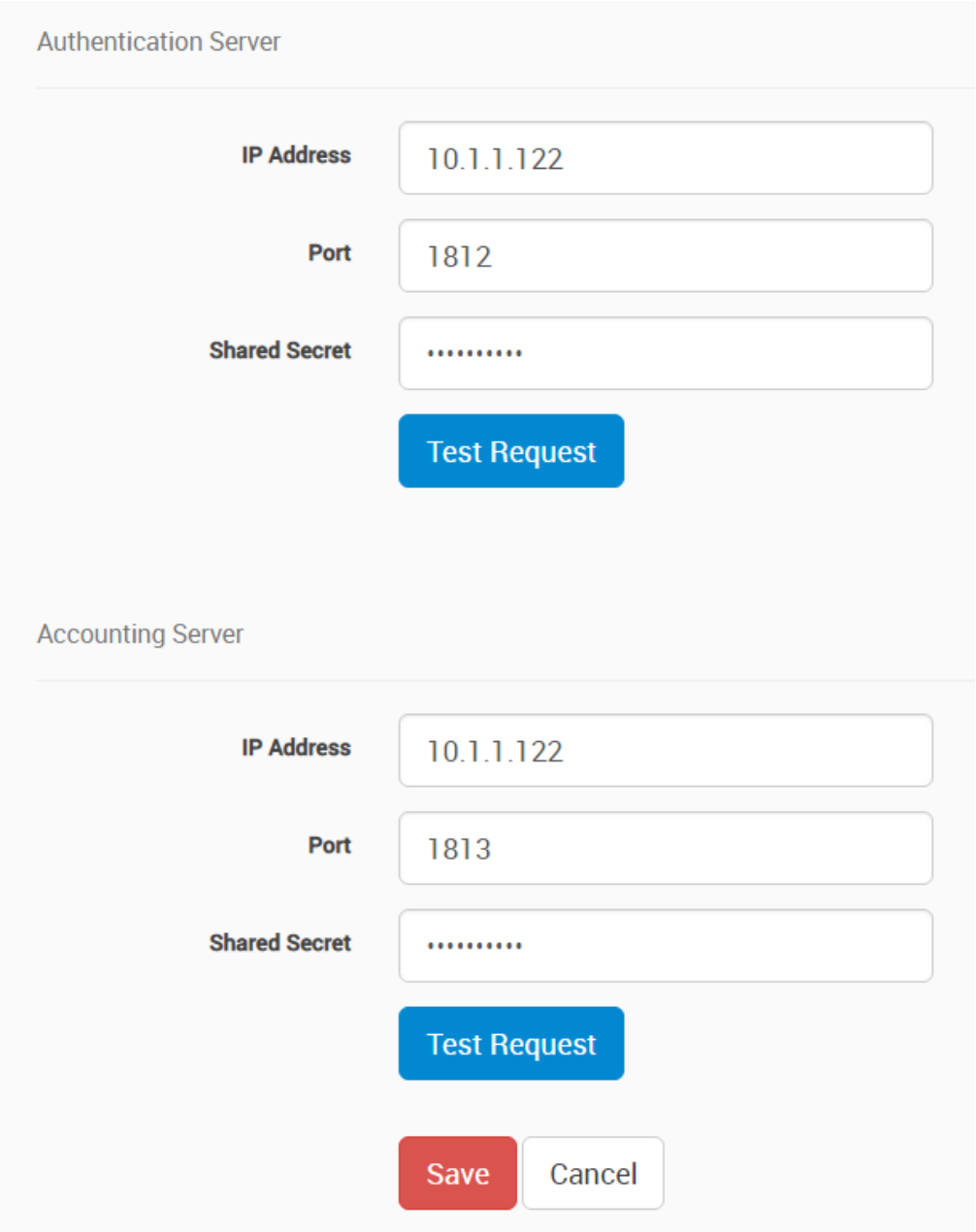


If the Radius server is running, the settings and the login details are correct, you will receive the "Successful" notification as shown in the screen shot above.



If you get an error popup, check that the server settings are correctly set up in the configuration for the Authentication server, and that the user name and password is correct.
Verify that the network subnet is allowed in the Radius configuration (ACL).
Also, check for any firewall or network routing problem that might prevent successful communication with the Radius server.

Note: The Radius user names are case-sensitive!

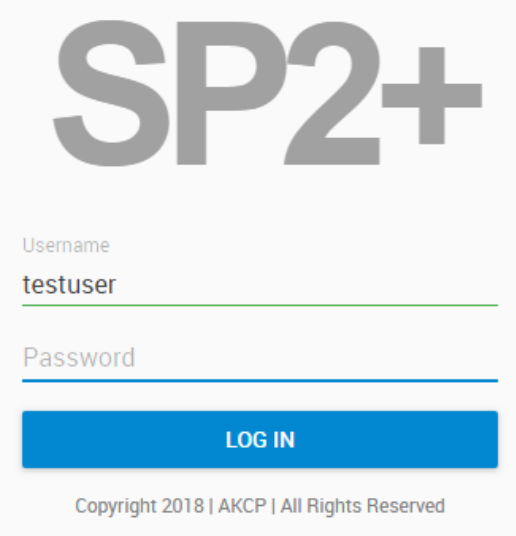


Press the **Save** button to save the settings if the test was successful.

Simply repeat the same steps to connect to an **Accounting server**.
Accounting is optional and you don't need to specify it if you select only Authentication mode.

Note: It is recommended to confirm the server settings with a test, since you won't be able to log in again if your settings are wrong.

The system will then log you out of the web interface and connect to the Radius server for password checking.



Now you can log into the web interface using **only** the Radius usernames and passwords. However, the built-in local Admin user will always be available to use.
Also, the unit falls back to local authentication mode if a Radius server is unreachable.

All Radius users which doesn't have the privilege level attributes set, will only have Viewer level (read-only) access to the SP+ web UI (for details, see the section *How it works*).

Important Note: If you happen to get logged out of the unit while setting up the Radius server or do not want to use the Radius server to log in, you can press the reset button on the unit for 8 seconds. This disables all password checking functions. Wait about 10 seconds then you should be able to open the web UI without any passwords.

How it works

Important note: The following only applies to newer SP+ firmware 5937 and later

Authorization and Privilege Level checking

It is possible to define specific attributes for each user at the server side to check whether the user has administrator rights or just a simple user (privilege level checking).
All Radius users which doesn't have the privilege level attributes set, will only have Viewer level (read-only) access to the SP+ web UI.
Note that Radius permissions can only use the default permission levels (Admin/User/Viewer), you cannot customize them as you can with local users.

The privilege level checking is done using a custom dictionary to check the **AKCP-User-Role** attribute, with numbers as follows:

0-15 - *Viewer*
16-31 - *User*
32 and above - *Admin*

In order for this to work, the Radius server's configuration needs to have the **AKCP-User-Role** custom vendor attribute defined in the "dictionary" file. You can copy-paste the following to add this new attribute to the dictionary file:

```
VENDOR            AKCP        3854
BEGIN-VENDOR      AKCP

#
# AKCP Attributes
#
ATTRIBUTE   AKCP-User-Role    1     integer

END-VENDOR  AKCP
```

Once the AKCP-User-Role attribute is defined in the Radius "dictionary" file and the Radius service is restarted, then it should be available to use.

Then in the "users" file this new attribute must be set for each user. See some examples below.

IMPORTANT: Make sure to use TAB (or double TAB) character after a newline to add the AKCP-User-Role attribute per user. Space, comma etc. will not work!

```
testuser Cleartext-Password := "testpw"
      AKCP-User-Role := 16
# 16 = User level

testadmin Cleartext-Password := "admin1"
      AKCP-User-Role := 32
# 32 = Admin level

tst Cleartext-Password := "tst"
      AKCP-User-Role := 0
# 0 = Viewer level
```

If you are using a different authentication database to store Radius users (ex. SQL, LDAP etc.) then adapt the configuration accordingly to define the attribute per user.

Even if the unit has been added to AKCPro Server (APS), only Radius authentication works and the Access Control users cannot be used to log in to the unit's Web UI.

When Radius mode is enabled, the existing local accounts (User, Viewer and other accounts) are not used unless there is a communication issue with the Radius server, in which case the units will fall back to the local password authentication.

However, the built-in local Admin user will always be available to use. You should not have "admin" or "Admin" user in your Radius configuration, as it will be ignored and the local Admin account is used instead.

Note: We recommend that you avoid using the same username in both the unit's local user database and on the Radius server, as this could lead to incorrect permissions being applied for the user.

Authentication

The following attributes are being sent with an Authentication package:

User-Name
This Attribute indicates the name of the user to be authenticated.

User-Password
This Attribute indicates the password of the user to be authenticated.

NAS-IP-Address
This Attribute indicates the identifying IP Address of the NAS which is requesting the authentication of the user. AKCP's NAS-IP-Address is the SP+ unit's IP Address.

Service-Type
This Attribute indicates the type of service the user has requested, or the type of service to be provided.

Possible value: 1 Login-User

AKCP-User-Role
This Attribute defines the privilege level of the user to be authenticated.
If this attribute is not defined, then the user's privilege level will be Viewer only.

Possible values:
0-15 - *Viewer*
16-31 - *User*
32 and above - *Admin*

Note: The sensorProbe+ does not interpret any attributes of an Access-Accept or Access-Reject package.

Example authentication package

```
Access-Request
    User-Name(1):          testadmin
    User-Password(2):      Encrypted
    NAS-IP-Address(4):     10.1.1.155
    Service-Type(6):       Login-User(1)
    Login-IP-Host(14):     10.1.1.41
    AKCP-User-Role = 32
```

Accounting

The following attributes are being sent with the Accounting package:

Acct-Status-Type

This attribute has three values:

1: Start
2: Stop
3: Interim-Update

A package with Acct-Status-Type *Start* will be sent when a user session begins (When the user logs in via web interface).

A package with Acct-Status-Type *Stop* will be sent when a user session ends (When the user logs off via web interface or because of idle timeout).

A package with Acct-Status-Type *Interim-Update* will be sent when a user accesses the SP+ web interface in a session.

Acct-Session-Id

The *Acct-Session-Id* is a unique Accounting ID to make it easier to match the start and stop records in a log file.
AKCP's Acct-Session-Id is a string that consists of:
u<user's IP>n<SP+ IP>r<Radius's IP>_<Random ID>

Acct-Authentic

This attribute is included in an Accounting-Request with Acct-Status-Type set to *Start* to indicate how the user was authenticated.

Possible value: 1 RADIUS.

Acct-Terminate-Cause

This attribute is included in an Accounting-Request with Acct-Status-Type set to *Stop* to indicate how the session was terminated.

Possible values are:
1: User Request - User requested the termination of service via pressing the logoff button.
4: Idle-Timeout - The idle timer expired for the user.

Note: The sensorProbe+ does not interpret any attributes of an Accounting-Response package.

Example accounting package

```
Accounting-Start
    User-Name(1):               testadmin
    Acct-Status-Type(40):        Start(1)
    Acct-Session-Id(44):        u10.1.1.41n10.1.1.155r10.1.1.41_4d6b2ddcd33da5.55190932
    Acct-Authentic(45):         RADIUS(1)

Accounting-Stop
    User-Name(1):               testadmin
    Acct-Status-Type(40):        Stop(2)
    Acct-Session-Id(44):        u10.1.1.41n10.1.1.155r10.1.1.41_4d6b2ddcd33da5.55190932
    Acct-Terminate-Cause(49):    User-Request(1)

Accounting-Interim-Update
    User-Name(1):               testadmin
    Acct-Status-Type(40):        Interim-Update(3)
    Acct-Session-Id(44):        u10.1.1.41n10.1.1.155r10.1.1.41_4d6b2ddcd33da5.55190932
```

Primary, Secondary Server and the Fail-over algorithm

In the sensorProbe+, users can setup Primary and Secondary Radius Servers for both Authentication and Accounting.

For Access-Request, Accounting-Start and Accounting-Stop packages, the sensorProbe+ will try to send these packages to the primary server first. If the primary server has failed then the unit will try with the secondary server (if the user enables it in the configuration). This procedure will repeat every time when the sensorProbe+ tries to send these packages.

For Accounting-Interim-Update package, the sensorProbe+ will try to send this package to the primary server first. If the primary server has failed then the unit will try with the secondary server (if the user enables it in the configuration).
For the next Accounting-Interim-Update request, the sensorProbe+ will use simplified Back off algorithm (E(c) = ((2^c) - 1) / 2) and use the number of failures as c to calculate the amount of time in minutes from the last attempt to wait before the unit will try to send Accounting-Interim-Update request to the primary server again.

For example, if the primary server has failed and the secondary server succeeds, then the next request will be sent to the secondary server without trying the primary server. After the amount of time (calculated by the simplified Back off algorithm), the sensorProbe+ will try to send the package to the primary server again.
If the primary server accepts the request, then the number of failures will be set to 0, otherwise the sensorProbe+ will increase the number of failures by 1 and calculate the amount of time to wait before trying to send a request to the primary server again.

Troubleshooting

In order to verify that the Radius configuration is set correctly with the attributes, you can monitor the login progress via the browser console as follows:

Open the WebUI login screen
Press F12 -> Go to Network tab
After you've logged in, check for the "role" parameter.
It should match the attribute you've set for the user. If it's not, then verify the server's configuration as the attribute is sent by the server.

You can also monitor the login from the Radius server side, if you start the service with the debug logging parameter (radiusd -X).

Example log from a Radius server assigning the attribute 19 for the user when logging in from the unit:
(1) Sent Access-Accept Id 25 from 192.168.1.24:1812 to 192.168.1.152:60443 length 0
(1) AKCP-User-Role = 19
(1) Finished request

Also try to refresh the browser web cache with CTRL-F5, if you've recently upgraded the firmware.

Please contact support@akcp.com if you have any further technical questions or problems.

Thanks for Choosing AKCP!