Bluesocket vWLAN WPA2-Multikey and Rolling-PMK in vWLAN

Configuration Guide

6ABSCG0014-29A

April 2020

To the Holder of this Document

This document is intended for the use of ADTRAN customers only for the purposes of the agreement under which the document is submitted, and no part of it may be used, reproduced, modified or transmitted in any form or means without the prior written permission of ADTRAN.

The contents of this document are current as of the date of publication and are subject to change without notice.

Trademark Information

“ADTRAN” and the ADTRAN logo are registered trademarks of ADTRAN, Inc. Brand names and product names included in this document are trademarks, registered trademarks, or trade names of their respective holders.

Disclaimer of Liability

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products are given “as is”, and any liability arising in connection with such hardware or software products shall be governed by ADTRAN’s standard terms and conditions of sale unless otherwise set forth in a separately negotiated written agreement with ADTRAN that specifically applies to such hardware or software products.

To the fullest extent allowed by applicable law, in no event shall ADTRAN be liable for errors in this document for any damages, including but not limited to special, indirect, incidental or consequential, or any losses, such as but not limited to loss of profit, revenue, business interruption, business opportunity or data, that may arise from the use of this document or the information in it.

Revision History

Rev A	April 2020	Initial release of this guide.

Table of Contents

1. Overview

This configuration guide explains the new Wi-Fi protected access version 2 (WPA2) with Multikey support security feature (WPA2-Multikey) and its configuration in ADTRAN Bluesocket virtual wireless local area network (vWLAN) systems. Included in this guide are a brief overview of the WPA2-Multikey and Rolling-PMK features, their configuration processes, and the methods for testing their configurations.

2. Introduction to WPA2-Multikey and Rolling PMK

With standard Wi-Fi security (Type: WPA2-PSK), the Wi-Fi password must be shared to all wireless users. The challenge is that everyone knows the password and once you know the password you can easily sniff another users traffic. There is no way to assign a unique pre-shared key (PSK) for each user. On the other hand, WPA2-Enterprise security settings are not user friendly and requires the administrator to configure every individual user.

When employed, the WPA2-Multikey feature makes use of a Remote Authentication Dial-In User Service (RADIUS) server for client device authentication, and uses RADIUS attributes to provide secure connection information for each device. As part of the new feature, when using WPA2-Multikey, the access point (AP) performs the RADIUS MAC authentication, rather than vWLAN itself. When devices have completed the registration process, roles, locations, and VLAN settings are determined by the AP, based on the Tunnel-Password and Tunnel-Private-Group-ID attributes contained in the RADIUS ACCEPT messages. These attributes are used to provide the pairwise master key (PMK) and appropriate virtual local area network (VLAN) information for the authenticating client. Once the client has been authenticated, the AP tags all wireless traffic from the device with the VLAN number assigned by the RADIUS server in the Tunnel-Private-Group-ID attribute of the ACCEPT message.

In addition, when the WPA2-Multikey feature is used, the AP tags VLAN frames without performing location discovery, removing the need to add all available locations manually to vWLAN. These locations are populated by the AP when it receives new VLAN information from the RADIUS server and are communicated to vWLAN as an Active or Inactive location. Therefore, client status location information is displayed as a VLAN value (for example, VLAN-325), and location status information includes the CIDR, VLAN ID, and AP.

Rolling-PMK Feature Overview

Rolling-PMK is a unique feature to ADTRAN vWLAN. With the WPA2-MultiKey feature, whenever a client tries to connect to AP, the AP will do a Radius-MAC-Authentication, and in response the Radius server sends the PMK key for that client. When using only the WPA2-Multikey feature, a service provider has to register each client's MAC address and corresponding PMK in their server. This can cause difficulty with end-user experiences because they have to know and share all of their wireless client MAC addresses to the administrator of the vWLAN instance to which they are connecting.

To address this issue, using the Rolling-PMK feature, the RADIUS server can be configured to send multiple PMK keys in the RADIUS Accept message, instead of sending just one PMK in a Radius-Response message. When that occurs, an AP can validate one of the provided keys with a wireless client in a 4-way handshake, thus eliminating the need for the end-user to provide their wireless client information.

WPA2-Multikey and Rolling-PMK Configuration Overview

To configure the WPA2-Multikey and Rolling-PMK features, you will need to complete the tasks described in each of the following sections:

- *Installing Ubuntu 18.04 Live Server AMD64 on page 6*
- *Installing MariaDB on page 7*
- *Installing the FreeRADIUS Server on page 8*
- *Configuring vWLAN for WPA2-Multikey Functionality on page 10*

- *Configuring the FreeRADIUS Server for vWLAN WPA2-Multikey on page 14*
- *Configuring Rolling-PMK for WPA2-Multikey (Optional) on page 18*

3. Hardware and Software Requirements and Limitations

The WPA2-Multikey and Rolling-PMK features are available on all vWLAN instances and Bluesocket access points (BSAPs) running firmware 3.5.0 or later.

The WPA2-Multikey feature is supported natively on the BSAP 2020, 203x, 2135, and 304x Series. This feature is not supported on the BSAP 1900 Series.

Additional Software for WPA2-Multikey and Rolling-PMK Support

In order to implement the WPA2-Multikey and Rolling-PMK features in vWLAN instances, several software systems outside of vWLAN must also be configured. This guide assumes some familiarity with the software packages listed below, although the configuration necessary for use with vWLAN is included in this guide. These additional software systems include the following:

- Ubuntu 18.04 Live Server
- MariaDB
- FreeRADIUS

WPA2-Multikey and Rolling-PMK Configuration Considerations

When implementing the WPA2-Multikey or Rolling-PMK features, keep in mind the following:

- When WPA2-Multikey is configured on vWLAN, APs no longer have standalone capability. Instead, clients cannot be authorized on the AP when the vWLAN server is down.
- When using WPA2-Multikey, client roles cannot be assigned by vWLAN at the AP. Instead, all connected clients are assigned an **Allow All** role which requires firewall and bandwidth limitations to be configured using third-party WAG controllers (such as RGNets).
- When employed, the WPA2-Multikey feature allows each AP to cycle through up to **15** PMK keys when authenticating clients.
- Up to **24** PMKs can be sent simultaneously without affecting client connectivity.

4. Installing Ubuntu 18.04 Live Server AMD64

The first step in the WPA2-Multikey feature configuration for vWLAN is to install Ubuntu 18.04 Live Server with the required software packages. While detailed Ubuntu installation and configuration is outside the scope of this guide, the following information may prove beneficial when completing the installation:

- You can find the Ubuntu 18.04 Live Server AMD64 software for installation online at the following address: http://releases.ubuntu.com/18.04/ubuntu-18.04.3-live-server-amd64.iso.
- Several tutorials are available online for Ubuntu installation.
- When installing Ubuntu, you will need to specify the server name, user name, and associated password.
- You will also need to install an OpenSSH server in order to manage the Ubuntu server.
- You must install any additional packages you want for this server.
- Once the Ubuntu server is installed, reboot the server and execute the following two commands:
  - **`sudo apt-get update`**
  - **`sudo apt-get upgrade`**

5. Installing MariaDB

After you have installed and configured the Ubuntu server, and its configuration is up to date, the next step in configuring vWLAN for WPA2-MultiKey functionality is to install the MariaDB database. To properly install MariaDB using the Ubuntu command line interface, you will first install a MariaDB repository, and then install the database. The MariaDB is used as the database for the FreeRADIUS server, which is required for the WPA2-Multikey feature.

Installing the MariaDB Repository

The first step in installing the MariaDB is to install and create the MariaDB repository. Follow the steps below to install the repository:

1. In the Ubuntu server's command line, verify that the MariaDB common software properties are installed. If these settings are missing, install them by issuing the following command:

```
$sudo apt-get install software-properties-common
```

2. Next, import the MariaDB GPB key and add the repository key to the system using the **sudo apt-key** command. Enter the command as follows:

```
$sudo apt-key adv --recv-keys --keyserver hkp://keyserver.ubuntu.com:80
  0xF1656F24C74D1D8
```

3. Lastly, add the APT repository by importing the PGP key and adding the repository URL to the Ubuntu 18.04 server using the following commands:

```
$sudo add-apt-repository “deb [arch=amd64, arm64, ppc64el]
  http://mariadb.mirror.liquidtelecom.com/repo/10.4/ubuntu $(lsb_release
  -cs) main”
```

4. The MariaDB repository is now installed and accessible. The next step in the MariaDB installation is to install the MariaDB server.

Installing the MariaDB Server

After installing the MariaDB repository, you can complete the MariaDB installation by installing the MariaDB server. To complete the installation, follow these steps:

1. In the Ubuntu CLI, install Maria DB and the MariaDB server by issuing the following commands:

```
$sudo apt update
$sudo apt -y install mariadb-server mariadb-client
```

2. Once you have issued these commands, you should be prompted to provide MariaDB with a password for the root user. Enter the password when prompted as follows:

```
Username : root
Password : XXXXXXX
```

   If you were not prompted to enter the password, the installation may not be complete and you will need to enter the following command:

```
$sudo mysql_secure_installation
```

   After entering the above command, follow the prompts to complete the installation.

Once the MariaDB repository and server are installed, you can begin to install the FreeRADIUS server.

6. Installing the FreeRADIUS Server

Once you have installed both the Ubuntu 18.04 and MariaDB servers, the next item you will need to install and configure is the FreeRADIUS server. FreeRADIUS is a free, open-source RADIUS protocol server, used in a UNIX environment for Authentication, Authorization, and Accounting (AAA) management. When used in conjunction with vWLAN, it is configured to manage client access when the WPA2-Multikey or Rolling-PMK feature is enabled in the vWLAN network.

To install and configure a FreeRADIUS server for use with vWLAN's WPA2-Multikey feature, follow the instructions detailed in the next sections.

- *Creating a Database for the FreeRADIUS Server on page 8*
- *Installing the FreeRADIUS Server on page 8*
- *Configuring the FreeRADIUS SQL Parameters on page 8*
- *Restarting the FreeRADIUS Service on page 10*

NOTE

Do not begin to install and configure the FreeRADIUS server until you have verified that MariaDB is installed and running correctly.

Creating a Database for the FreeRADIUS Server

The first step in the installation and configuration of the FreeRADIUS server for use with vWLAN is to create a database within MariaDB for the FreeRADIUS server. Once you have verified that MariaDB is installed and running, enter the following commands in the command shell to create the FreeRADIUS server database:

```
$mysql -u root -p
$CREATE DATABASE radius;
$GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY “passwordcreate”;
$FLUSH PRIVILEGES;
$quit
```

Installing the FreeRADIUS Server

Once the database has been created for the FreeRADIUS server, you can install the FreeRADIUS server from the official Ubuntu APT repository to that database.

To install the default version of the FreeRADIUS server, and the FreeRADIUS utilities package, to the previously created FreeRADIUS database, enter the following in the command shell:

```
$sudo apt -y install freeradius freeradius-mysql freerdius-utils
```

Configuring the FreeRADIUS SQL Parameters

The next step in the initial configuration process for the FreeRADIUS server is to specify the SQL parameters for the database. There are several steps necessary to complete the SQL adjustments for the FreeRADIUS server. To begin, you must import the MySQL schema (to define specify how the data will be organized and displayed), and then you must verify that the SQL data tables were created properly. Once the SQL schema is verified, you then create a soft link in the database pointing to the SQL module and additionally define the database connection parameters within the SQL module. Lastly, you must complete a few SQL modifications in the database and restart the FreeRADIUS server.

To configure the FreeRADIUS SQL parameters for use with vWLAN, connect to your command shell and complete the following:

1. First, enter the following command to import the MySQL database schema for the FreeRADIUS server:

   ```
   $sudo su -
   $mysql -u root -p radius <
     /etc/freeradius/3.0/mods-config/sql/main/mysql/schema.sql
   ```

2. Next, verify that the tables for the FreeRADIUS server data have been created using the `use radius;` and `show tables;` commands as shown below:

   ```
   $mysql -u root -p -e “use radius; show tables;”
   Enter password:
   +---------------------+
   | Tables_in_radius |
   +---------------------+
   | nas                  |
   | radacct              |
   | radcheck             |
   | radgroupcheck        |
   | radgroupreply        |
   | radpostauth          |
   | radreply             |
   | radusergroup         |
   ```

3. Once the tables have been verified, create a symbolic link in the FreeRADIUS database for the installed SQL module by entering the following command from the command shell. This command will place the soft link under **/etc/freeradius/3.0/mods-enabled/**.

   ```
   $sudo ln -s
   /etc/freeradius/3.0/mods-available/sql/etc/freeradius/3.0/mods-enabled/
   ```

4. Next, configure the database connection parameters within the SQL module. These parameters should be configured to fit your specific network environment, and should (at a minimum) define the connection information, database table configuration parameters, and processes for managing RADIUS client information.

   Your configuration should resemble the following example:

   > **NOTE**
   >
   > *The following is an example configuration only, to be used for explanatory purposes. You must adjust this configuration to fit your network and environment.*

   ```
   sql {
   driver = "rlm_sql_mysql"
   dialect = "mysql"

   # Connection info:
   server = "localhost"
   port = 3306
   login = "radius"
   password = "password created in step 2"

   # Database table configuration for everything except Oracle
   radius_db = "radius"
   ```

```
}

# Set to ‘yes’ to read radius clients from the database (‘nas’ table)
# Clients will ONLY be read on server startup.
read_clients = yes

# Table to keep radius client info
client_table = "nas"
```

5. The next step in the SQL configuration for the FreeRADIUS server is to make a couple of SQL parameter adjustments to the group right of **etc/freeradius/3.0/mods-enabled/sql** using the following commands:

   ```
   $sudo chgrp -h freerad /etc/freeradius/3.0/mods-available/sql
   $sudo chown -R freerad:freerad /etc/freeradius/3.0/mods-enabled/sql
   ```

6. Once the SQL parameters have been configured, the FreeRADIUS initial configuration is complete and you can restart the FreeRADIUS server.

Restarting the FreeRADIUS Service

Once the FreeRADIUS server and it’s database have been created and installed, and the SQL parameters have been configured, you can restart the FreeRADIUS service to apply the configuration changes. To restart the service, enter the following command:

```
$sudo systemmyco restart freeradius.service
```

Once the FreeRADIUS server has been installed, configured, and rebooted, you can begin to configure vWLAN for the WPA2-Multikey feature.

7. Configuring vWLAN for WPA2-Multikey Functionality

After configuring the FreeRADIUS server, the next step is to configure vWLAN for the WPA2-Multikey feature operation. Before beginning the vWLAN configuration, ensure that the following prerequisites have been met:

- vWLAN is running firmware 3.5.0 or higher
- The FreeRADIUS server is installed and accessible by vWLAN
- An AP is connected to the switchport that allows access to the virtual LANs used
- You have administrator access to the vWLAN instance and GUI

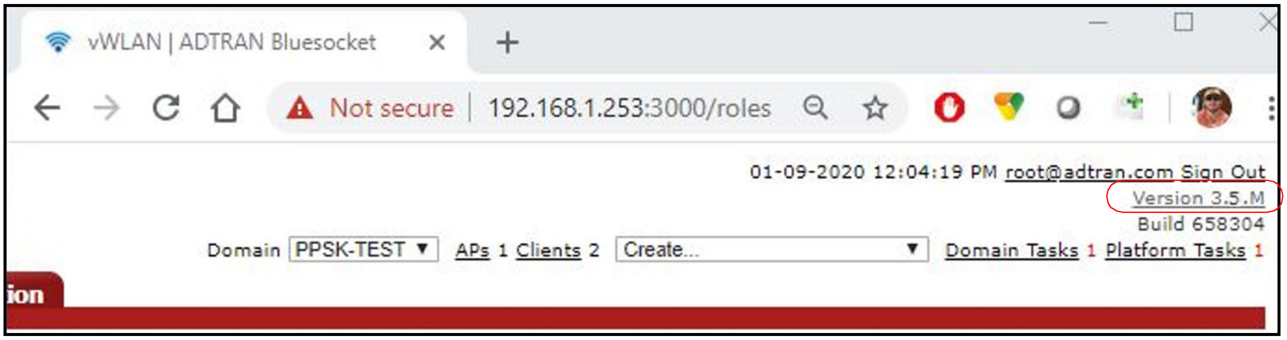
Once the prerequisites have been met, you can begin to configure vWLAN for WPA2-Multikey functionality. The vWLAN configuration process includes completing the following tasks:

- *Verifying the vWLAN Firmware Version on page 10*
- *Configuring External Authentication Servers on page 11*
- *Creating an SSID for WPA2-Multikey on page 12*
- *Applying the SSID to an AP Template on page 12*
- *Applying the AP Template to the APs on page 13*
- *Applying the Configuration to the APs on page 14*

Verifying the vWLAN Firmware Version

Before beginning to configure vWLAN for use with the WPA2-Multikey feature, you must ensure that the firmware version you are running supports the feature. You must be running firmware 3.5.0 or later for the WPA2-Multikey feature to be available.

To verify the vWLAN firmware version, connect to the vWLAN GUI and look in the top right corner of the main GUI dashboard. The vWLAN firmware version is displayed directly beneath the vWLAN instance login information, as shown below:



01-09-2020 12:04:19 PM root@adtran.com Sign Out
Version 3.5.M
Build 658304
Domain PPSK-TEST ▼ APs 1 Clients 2 Create... ▼ Domain Tasks 1 Platform Tasks 1

Configuring External Authentication Servers

Once you have verified that you are running a version of vWLAN that supports the WPA2-Multikey feature, you can begin to configure the external authentication servers in the vWLAN instance. The configuration of these servers rests on configuring a RADIUS server within the vWLAN instance that will be used for the WPA2-Multikey authentication. This step is basically associating vWLAN with the FreeRADIUS server configured earlier in the process, and consists of configuring a RADIUS and accounting server within vWLAN.

Configuring the WPA2-Multikey RADIUS Server

To begin configuring an external authentication server for the WPA2-Multikey feature, first connect to the vWLAN GUI and navigate to the **Configuration** tab. Next, select **External Authentication** > **Servers**, and then select **Create Server**. In the **Create Server** menu, enter the following parameters:

- **Server Type**: Select **RadiusMultiKeyAuthServer** from the drop-down menu.
- **Name**: Input a name of your choice in the field.
- **Accounting Server**: Leave this field blank.
- **IP Address**: Enter the IP address of the previously created FreeRADIUS server.
- **Port**: Should be **1812** by default.
- **RADIUS COA**: Make sure this check box is selected.
- **RADIUS COA Port**: Should be **3799** by default.
- **Shared Secret/Password**: Enter a password in the appropriate field.

NOTE

Be sure to keep a copy of this password. You will need it later in the configuration.

Once you have entered the parameters outlined above, select **Create Authentication Server** to create the server vWLAN will use for authentication with the WPA2-Multikey feature.

Configuring the WPA2-Multikey Accounting Server

After you have created the RADIUS server to be used with the WPA2-Multikey feature, you can begin configuring the accounting server. To begin configuring the accounting server for the WPA2-Multikey feature, first connect to the vWLAN GUI and navigate to the **Configuration** tab. Next, select **External Authentication**

> **Accounting**, and then select **Create Accounting Server**. In the **Create Accounting Server** menu, enter the following parameters:

- **Name**: Input a name of your choice in the field.
- **Enabled**: Make sure this check box is selected.
- **IP Address**: Enter the IP address of the previously created FreeRADIUS server.
- **Port**: Should be **1813** by default.
- **Shared Secret/Password**: Enter a password in the appropriate field.

NOTE

Be sure to keep a copy of this password. You will need it later in the configuration.

Once you have entered the parameters outlined above, select **Create Accounting Server** to create the server vWLAN will use for accounting with the WPA2-Multikey feature.

Creating an SSID for WPA2-Multikey

After you have configured the external authentication and accounting servers for use with the WPA2-Multikey feature, you must create an SSID to be used exclusively for WPA2-Multikey client connections. This SSID will allow clients to use private pre-shared keys (PPSK) for communication with the RADIUS server.

To begin configuring the SSID for WPA2-Multikey, first connect to the vWLAN GUI and navigate to the **Configuration** tab. Next, select **Wireless** > **SSIDs**. In the **SSID** menu, select **Create SSID** and enter the following parameters:

- **Name/ESSID**: Enter the name for the SSID in this field.
- **Broadcast SSID**: Make sure this check box is selected.
- **Authentication**: Select **WPA2-PSK** from the drop-down menu.
- **Cipher**: Select **AES-CCM** from the drop-down menu.
- **Multi Key**: Make sure this check box is selected.
- **RADIUS Multi Key Authentication Server**: Select the RADIUS server you created in the previous step from the drop-down menu (refer to *Configuring External Authentication Servers on page 11*).

Once you have entered the parameters outlined above, select **Create SSID** to create the SSID clients will use for connecting to vWLAN using the WPA2-Multikey feature.

Applying the SSID to an AP Template

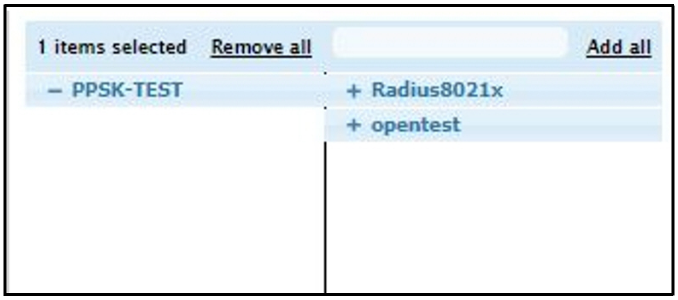
Once you have created the SSID to use with the WPA2-Multikey feature, you must apply that SSID to an AP template. The AP template should be one that any APs supporting Multikey connections will use.

NOTE

The following instructions are basic instructions for adding an SSID to a new AP template, or updating an existing template with the SSID. For more details about AP templates and their configuration, refer to the Bluesocket vWLAN Administrator's Guide, available online at https://supportcommunity.adtran.com.

To begin applying the SSID to an AP template, connect to the vWLAN GUI and navigate to the **Configuration** tab. Next, select **Wireless** > **AP Templates**. If you are updating an AP template with the newly created SSID, select the appropriate template from the list, and then select **Edit** at the bottom of the menu. If you are creating a new AP template, select **Create AP Template** from the bottom of the menu.

In the AP template configuration, add the SSID to the template and then select either **Create AP Template** or **Update AP Template**.



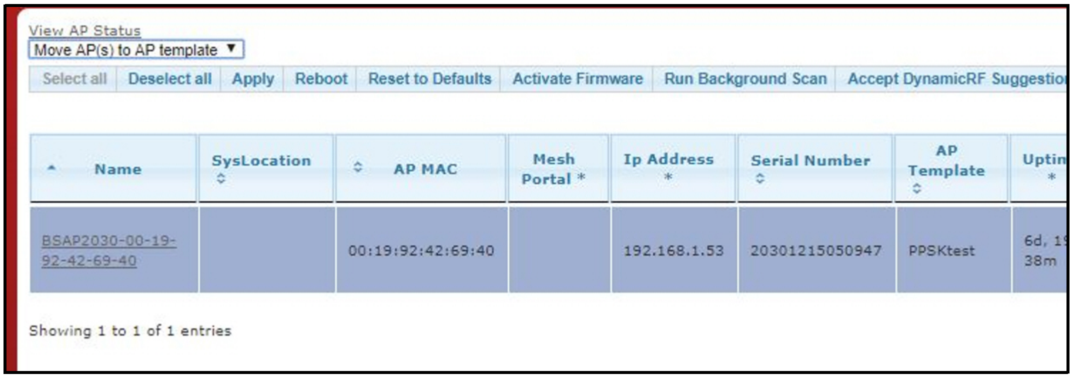
Once you have applied the WPA2-Multikey SSID to the appropriate AP template, you can then apply the AP template to the appropriate APs.

Applying the AP Template to the APs

Once you have created an AP template with the WPA2-Multikey parameters, you must apply that template to the appropriate APs.

To begin applying the AP template to the APs, connect to the vWLAN GUI and navigate to the **Configuration** tab. Next, select **Wireless** > **Access Points** and follow these steps:

1. In the **Access Points** menu, select the APs from the list to which you will be applying the template.
2. Once you have selected the APs from the list, select **Move AP(s) to AP Template** from the top left corner of the menu.
3. When prompted, select the AP template to which you just applied the WPA2-Multikey SSID from the list (refer to *Applying the SSID to an AP Template on page 12*).



Name	SysLocation	AP MAC	Mesh Portal *	Ip Address *	Serial Number	AP Template	Uptin *
BSAP2030-00-19-92-42-69-40		00:19:92:42:69:40		192.168.1.53	20301215050947	PPSKtest	6d, 1 38m

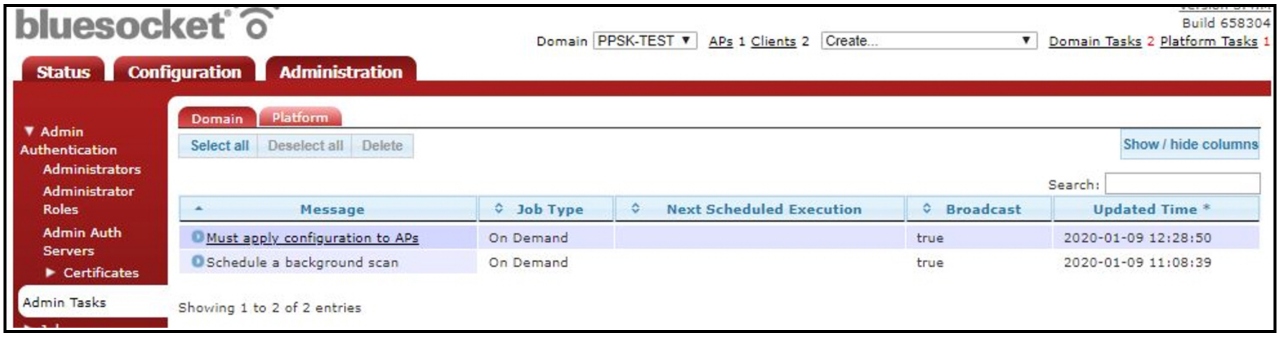
Showing 1 to 1 of 1 entries

After applying the AP template to the appropriate APs, you must manually push the template changes to the AP by initiating a domain task, as described in the next section.

Applying the Configuration to the APs

Once the AP template has been created and applied to the appropriate APs, you must manually push the configuration changes to the APs using a domain task.

To initiate this task, connect to the vWLAN GUI and select **Domain Task** from the top right of the vWLAN GUI. You will then be presented a list of the available domain tasks. From that list, select the blue dot next to the **Must apply configuration to APs** task to begin the task execution.



Message	Job Type	Next Scheduled Execution	Broadcast	Updated Time
Must apply configuration to APs	On Demand		true	2020-01-09 12:28:50
Schedule a background scan	On Demand		true	2020-01-09 11:08:39

Showing 1 to 2 of 2 entries

When the task is completed, a message is generated to indicate the successful execution of the task. Once you receive this message, the vWLAN configuration for the WPA2-Multikey feature is complete, and you can begin configuring the FreeRADIUS server specifics for the vWLAN WPA2-Multikey feature.

8. Configuring the FreeRADIUS Server for vWLAN WPA2-Multikey

Once vWLAN has been configured to communicate with the established FreeRADIUS server, and the APs have been configured to support WPA2-Multikey client connections, you can begin to configure the FreeRADIUS server specifically for your vWLAN and AP instances on which you've configured the WPA2-Multikey feature. The configuration of the FreeRADIUS server for vWLAN WPA2-Multikey connections relies on completing the following tasks:

- *Registering IP Addresses of AP and vWLAN Instances as RADIUS Clients on page 14*
- *Creating a MAC User in the FreeRADIUS Server on page 16*
- *Adding VLAN and PMK Parameters for the Wireless Client on page 16*
- *Restarting the FreeRADIUS Server on page 17*
- *Testing the WPA2-Multikey Feature Configuration on page 17*

Before beginning the FreeRADIUS server configuration for vWLAN WPA2-Multikey, ensure that the following prerequisites have been met:

- Ubuntu is installed with MariaDB and FreeRADIUS (refer to *Installing Ubuntu 18.04 Live Server AMD64*, *Installing MariaDB*, or *Installing the FreeRADIUS Server*).
- vWLAN External Authentication Servers have been created (refer to *Configuring External Authentication Servers on page 11*).
- You have command line (SSH) access to the Ubuntu Server.

Registering IP Addresses of AP and vWLAN Instances as RADIUS Clients

The first step in configuring the FreeRADIUS server for use with the vWLAN WPA2-Multikey feature is to register any APs and vWLAN instances that will be used with the WPA2-Multikey feature with the FreeRADIUS server. This is accomplished by providing the IP addresses of any APs and vWLAN instances as clients within the FreeRADIUS server configuration.

To register the APs and vWLAN IP addresses with the FreeRADIUS server as clients, follow these steps:

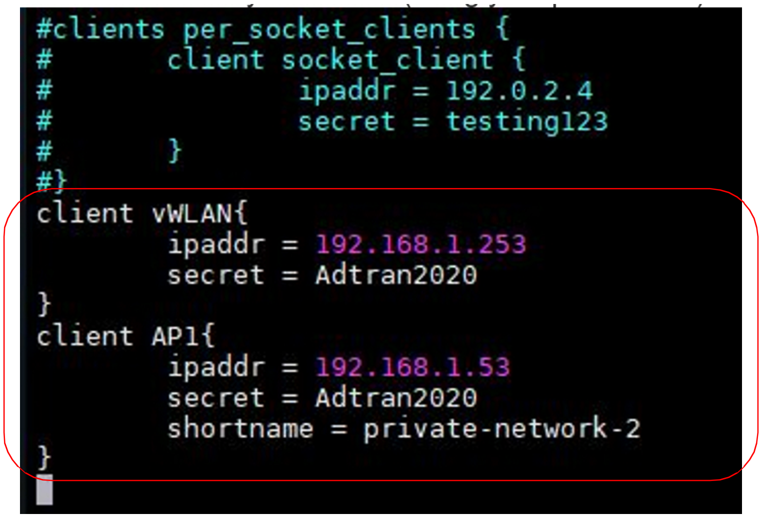
1. From the Ubuntu command line interface, open the FreeRADIUS clients file using the following command:

```
$sudo nano /etc/freeradius/3.0/clients.conf
```

2. Next, you will have to add an entry for every AP and vWLAN instance within the RADIUS client file. To do this you will enter the following items for each AP/vWLAN instance using the client entry configuration commands:

- IP address of the vWLAN instance (for testing connectivity to the RADIUS server)
- IP address of the AP (for client validation to the RADIUS server)
- Authentication credentials for each AP/vWLAN instances (specified when you created the external authentication servers in vWLAN; refer to *Configuring External Authentication Servers on page 11*).

To enter these parameters, enter the client commands as shown in the example below:



```
#clients per_socket_clients {
#       client socket_client {
#               ipaddr = 192.0.2.4
#               secret = testing123
#       }
#}
client vWLAN{
        ipaddr = 192.168.1.253
        secret = Adtran2020
}
client AP1{
        ipaddr = 192.168.1.53
        secret = Adtran2020
        shortname = private-network-2
}
```

NOTE

These are sample client entry configurations. Be sure to use the parameters necessary for your network and to ensure the same spacings as shown in the example above.

In this example configuration, we have entered the following parameters:

- The IP address of the vWLAN server (to test connectivity to the RADIUS server): **192.168.1.253**
- The IP address of an AP (for client validation to the RADIUS server): **192.168.1.53**
- The password used to connect with this RADIUS server (for both vWLAN and the AP): **Adtran2020**

NOTE

This is the password/shared secret configured for the external authentication servers in vWLAN (refer to Configuring External Authentication Servers on page 11).

- The optionally configured shortname parameter: **private-network-2**

Repeat these client entries for each AP that will be used for the WPA2-Multikey feature. After each AP has been added as a RADIUS client, you can move to the next step of FreeRADIUS server configuration, in which you create a MAC user in the FreeRADIUS server.

Creating a MAC User in the FreeRADIUS Server

After creating client entries for each AP and vWLAN instance that will be using the WPA2-Multikey feature, you can begin configuring the MAC users in the RADIUS server. The MAC address for each wireless client must be added to the FreeRADIUS SQL database.

To create a MAC user in the FreeRADIUS SQL database, connect to the command line and follow these steps:

1. Enter the following command to access the FreeRADIUS SQL database:

```
$sudo mysql -u root -p radius
```

2. Enter the wireless client MAC address using the command as shown below from the **mysql>** prompt. In the following example, the MAC address being added is **5C:99:60:D9:05:48**. When you enter a MAC address into the SQL database, you must remove the colon character (**:**) from the MAC address, so the MAC address would be entered as follows: **5c9960d90548**.

```
mysql>insert into radcheck (username, attibute, op, value) values
  (‘5c9960d90548’, ‘Cleartext-Password’, ‘:=’, ‘5c9960d0548’);
```

3. Next, verify that the MAC address entry was added to the database using the command shown below:

```
mysql>select * from radcheck;
+---+------------+-------------------+----+----------+
| ud | username | attribute        | op | value      |
+---+------------+-------------------+----+----------+
| 1 | 5c9960d90548 | Cleartext-Password | ;= | 5c9960d90548
```

Once the MAC address entry has been verified in the FreeRADIUS SQL database, the MAC user creation process is complete.

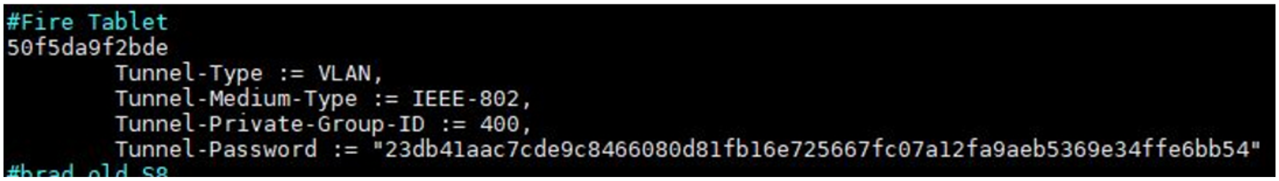
Adding VLAN and PMK Parameters for the Wireless Client

Once the wireless client MAC address entry has been created in the FreeRADIUS server, you can the configure the server for the VLAN and PMK parameters that will be used by authenticating clients.

To begin adding the VLAN and PMK parameters to the FreeRADIUS server configuration, connect to the command line and open the **#sudo nano /etc/freeradius/3.0/users** file, using the command shown below:

```
joe@freeradius3:/etc/freeradius/3.0$ sudo nano users
```

Once the file has opened, append the following to the end of the file:



```
#Fire Tablet
50f5da9f2bde
        Tunnel-Type := VLAN,
        Tunnel-Medium-Type := IEEE-802,
        Tunnel-Private-Group-ID := 400,
        Tunnel-Password := "23db41aac7cde9c8466080d81fb16e725667fc07a12fa9aeb5369e34ffe6bb54"
#brad old S8
```

NOTE

Add the entry exactly as it appears above, maintaining the same indention rules.

With this addendum to the file, you are specifying the following:

- The MAC address of the wireless client (**5c9960d90548**)
- The actual VLAN that needs to be assigned to the MAC address (**Tunnel-Private-Group-ID ;= 400**)
- The PMK value generated from http://jorisvr.nl/wpapsk.html (**Tunnel-Password** value)

> **NOTE**
>
> *The password input on the PMK generator is the password to connect to the WPA2-Multikey SSID for each wireless client. That password can be the same for multiple MAC addresses.*

Once you have appended the VLAN and PMK information to the users file, you can restart the FreeRADIUS server.

Restarting the FreeRADIUS Server

After you have registered the necessary vWLAN and AP instances, MAC addresses, and VLAN and PMK parameters with the FreeRADIUS server, you can restart the server to apply the configuration changes.

To restart the FreeRADIUS server you will be stopping all processes on any existing servers and restarting the FreeRADIUS server in debug mode. This process is necessary to apply any configuration changes.

To stop all processes on any existing servers, enter the **killall** command as follows:

```
joe@freeradius3:~$ sudo killall freeradius
```

Then, restart the server using the following command:

```
joe@freeradius3:~$ sudo freeradius -XXX
```

When the server comes back up, you can verify that it is listening for requests to be sent when the following messages appear:

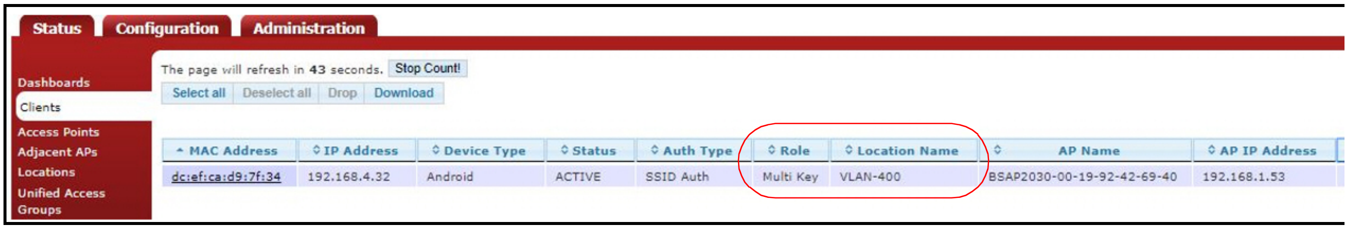
```
Thu Jan 2 13:09:43 2020 : Debug: Listening on proxy address :: port 47277
Thu Jan 2 13:09:43 2020 : Info: Ready to process requests
```

Once the FreeRADIUS server is ready, all configuration for the WPA2-Multikey feature is complete and you can now test that everything works appropriately.

Testing the WPA2-Multikey Feature Configuration

After you have configured vWLAN and your FreeRADIUS server for the WPA2-Multikey feature, you can perform a test connection to verify that everything is functioning correctly. To perform a test connection, follow these steps:

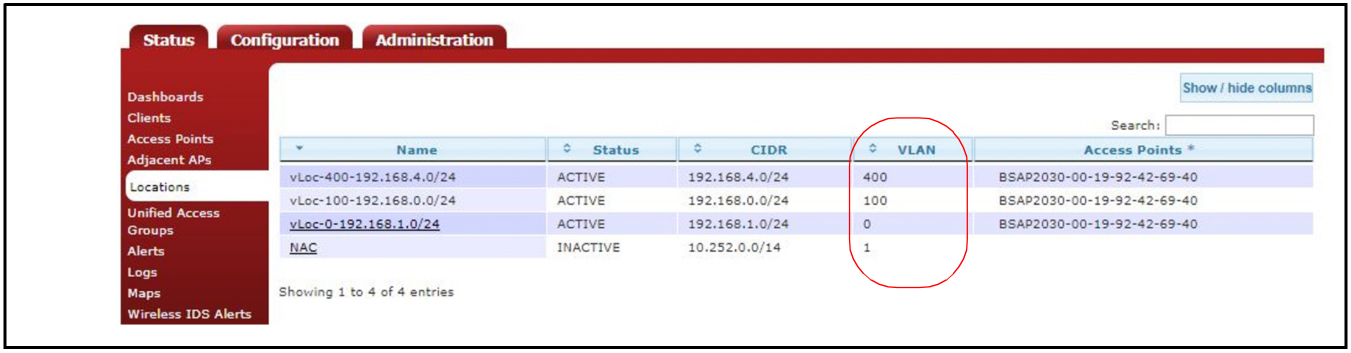
1. Connect a wireless client to the WPA2-Multikey SSID that you created in vWLAN.
2. Verify the wireless connectivity in vWLAN by connection to the GUI and navigating to the **Status** tab and selecting **Clients**. In the **Clients** menu you can verify that your client appears and is connected into the correct role (**Multi Key**) and location (**VLAN 400**).



The page will refresh in 43 seconds.

MAC Address	IP Address	Device Type	Status	Auth Type	Role	Location Name	AP Name	AP IP Address
dc:ef:ca:d9:7f:34	192.168.4.32	Android	ACTIVE	SSID Auth	Multi Key	VLAN-400	BSAP2030-00-19-92-42-69-40	192.168.1.53

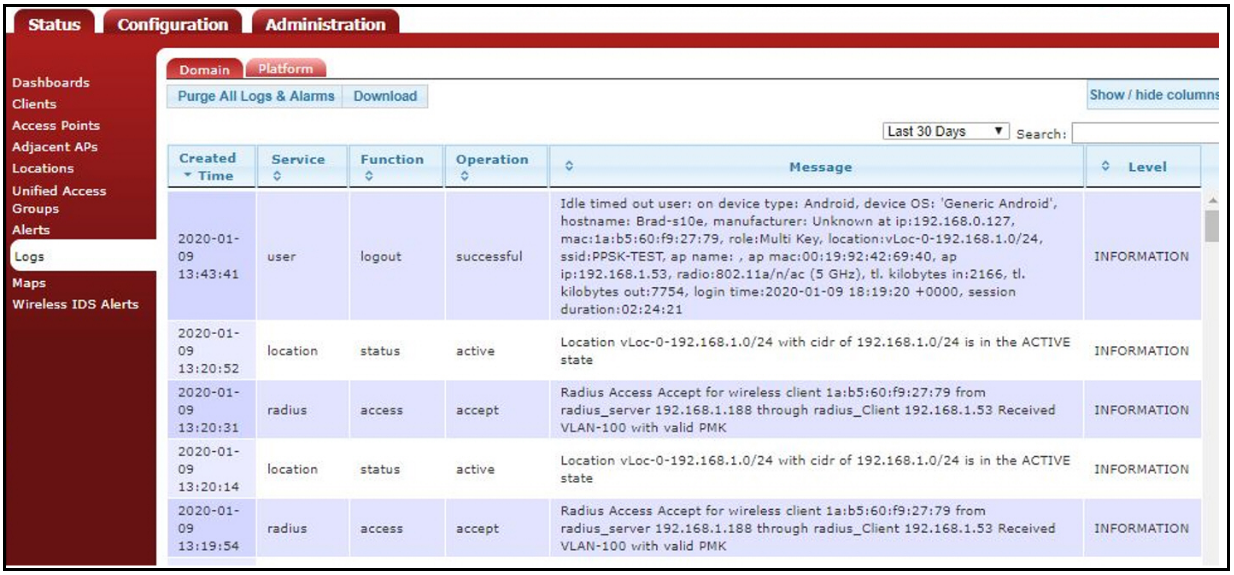
3. Next, verify that the location information automatically assigned to the AP and the client (i.e., the VLAN assignment) are correct by navigating to the **Status** tab and selecting **Locations**. In the **Locations** menu you can verify the VLAN assigned to the AP and client, as well as that all other information is correct for your network.



Name	Status	CIDR	VLAN	Access Points
vLoc-400-192.168.4.0/24	ACTIVE	192.168.4.0/24	400	BSAP2030-00-19-92-42-69-40
vLoc-100-192.168.0.0/24	ACTIVE	192.168.0.0/24	100	BSAP2030-00-19-92-42-69-40
vLoc-0-192.168.1.0/24	ACTIVE	192.168.1.0/24	0	BSAP2030-00-19-92-42-69-40
NAC	INACTIVE	10.252.0.0/14	1	

Showing 1 to 4 of 4 entries

4. After verifying the client connections and location information, view the vWLAN logs for RADIUS communication to double-check for any reported issues. In the vWLAN GUI, navigate to the **Status** tab and select **Logs** to view the vWLAN logs.



Created Time	Service	Function	Operation	Message	Level
2020-01-09 13:43:41	user	logout	successful	Idle timed out user: on device type: Android, device OS: 'Generic Android', hostname: Brad-s10e, manufacturer: Unknown at ip:192.168.0.127, mac:1a:b5:60:f9:27:79, role:Multi Key, location:vLoc-0-192.168.1.0/24, ssid:PPSK-TEST, ap name: , ap mac:00:19:92:42:69:40, ap ip:192.168.1.53, radio:802.11a/n/ac (5 GHz), tl. kilobytes in:2166, tl. kilobytes out:7754, login time:2020-01-09 18:19:20 +0000, session duration:02:24:21	INFORMATION
2020-01-09 13:20:52	location	status	active	Location vLoc-0-192.168.1.0/24 with cidr of 192.168.1.0/24 is in the ACTIVE state	INFORMATION
2020-01-09 13:20:31	radius	access	accept	Radius Access Accept for wireless client 1a:b5:60:f9:27:79 from radius_server 192.168.1.188 through radius_Client 192.168.1.53 Received VLAN-100 with valid PMK	INFORMATION
2020-01-09 13:20:14	location	status	active	Location vLoc-0-192.168.1.0/24 with cidr of 192.168.1.0/24 is in the ACTIVE state	INFORMATION
2020-01-09 13:19:54	radius	access	accept	Radius Access Accept for wireless client 1a:b5:60:f9:27:79 from radius_server 192.168.1.188 through radius_Client 192.168.1.53 Received VLAN-100 with valid PMK	INFORMATION

Once you have verified that the connections are functional, you have completed the WPA2-Multikey feature configuration. You can now optionally choose to configure the Rolling-PMK feature.

9. Configuring Rolling-PMK for WPA2-Multikey (Optional)

Rolling-PMK is a unique feature to ADTRAN vWLAN. With the WPA2-MultiKey feature, whenever a client tries to connect to AP, the AP will do a Radius-MAC-Authentication, and in response the Radius server sends the PMK key for that client. When using only the WPA2-Multikey feature, a service provider has to register each client's MAC address and corresponding PMK in their server. This can cause difficulty with end-user experiences because they have to know and share all of their wireless client MAC addresses to the administrator of the vWLAN instance to which they are connecting.

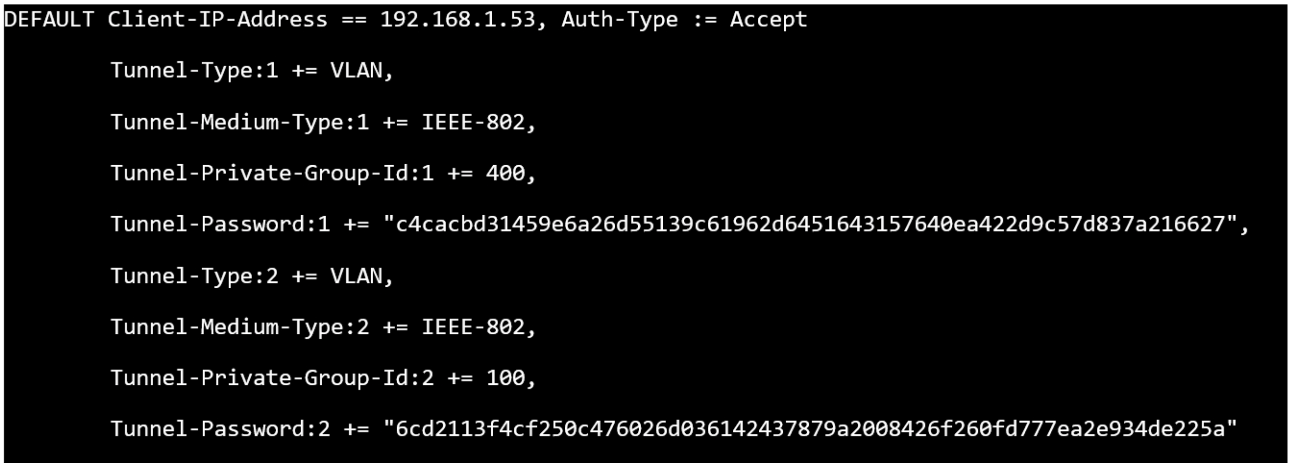
To address this issue, using the Rolling-PMK feature, the RADIUS server can be configured to send multiple PMK keys in the RADIUS Accept message, instead of sending just one PMK in a Radius-Response message. When that occurs, an AP can validate one of the provided keys with a wireless client in a 4-way handshake, thus eliminating the need for the end-user to provide their wireless client information.

To configure the Rolling-PMK feature, connect to the command line for the FreeRADIUS server and follow these steps:

1. To begin the Rolling-PMK configuration, you will need to edit the user file on the FreeRADIUS server using the following command:

```
$sudo nano /etc/freeradius/3.0/users
```

2. Specify an array of PMKs to send from the RADIUS server by entering the following configuration:



```
DEFAULT Client-IP-Address == 192.168.1.53, Auth-Type := Accept

        Tunnel-Type:1 += VLAN,

        Tunnel-Medium-Type:1 += IEEE-802,

        Tunnel-Private-Group-Id:1 += 400,

        Tunnel-Password:1 += "c4cacbd31459e6a26d55139c61962d6451643157640ea422d9c57d837a216627",

        Tunnel-Type:2 += VLAN,

        Tunnel-Medium-Type:2 += IEEE-802,

        Tunnel-Private-Group-Id:2 += 100,

        Tunnel-Password:2 += "6cd2113f4cf250c476026d036142437879a2008426f260fd777ea2e934de225a"
```

NOTE

Maintain the same indention rules as displayed above when configuring the PMK parameters.

When these parameters are added to the FreeRADIUS user file's configuration, you are specifying the following:

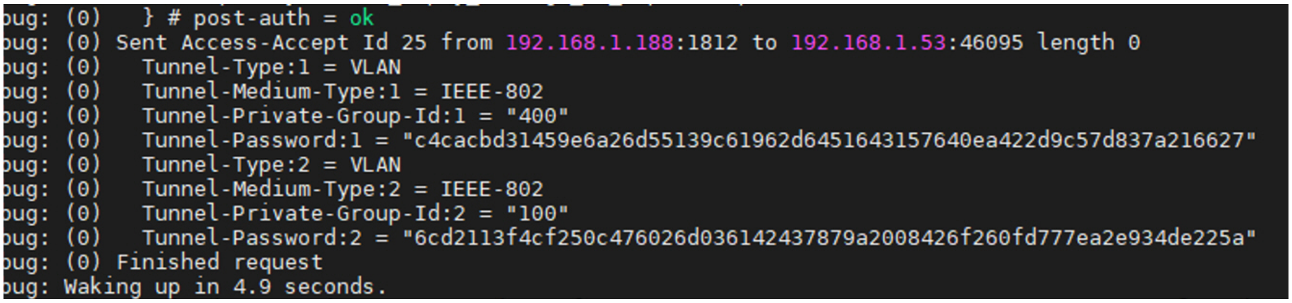
- The actual VLAN that needs to be assigned to connecting clients (Tunnel-Private-Group-Id)
- The PMK value generated from http://jorisvr.nl/wpapsk.html (**Tunnel-Password** value).

3. Once the PMK information has been added to the FreeRADIUS server, you must restart the server to apply the changes. Follow the steps outlined in *Restarting the FreeRADIUS Service on page 10* to restart the FreeRADIUS server. Once you receive the messages that the server is ready to process requests, the FreeRADIUS server configuration for Rolling-PMK is complete and you can test the feature functionality.

Testing the Rolling-PMK Feature

To test the Rolling-PMK feature functionality, connect a wireless client to the WPA2-Multikey SSID and view the responses on the FreeRADIUS server. The wireless client you are connecting should be one that is not built into the database or user file on the RADIUS server, and you should use one of the passwords in your configured array (not the HEX string/PMK parameter, but the actual password). Once you attempt to connect the client, you should see an array of responses sent to the AP and your client should connect.

Responses should appear as follows:



```
bug: (0)   } # post-auth = ok
bug: (0) Sent Access-Accept Id 25 from 192.168.1.188:1812 to 192.168.1.53:46095 length 0
bug: (0)   Tunnel-Type:1 = VLAN
bug: (0)   Tunnel-Medium-Type:1 = IEEE-802
bug: (0)   Tunnel-Private-Group-Id:1 = "400"
bug: (0)   Tunnel-Password:1 = "c4cacbd31459e6a26d55139c61962d6451643157640ea422d9c57d837a216627"
bug: (0)   Tunnel-Type:2 = VLAN
bug: (0)   Tunnel-Medium-Type:2 = IEEE-802
bug: (0)   Tunnel-Private-Group-Id:2 = "100"
bug: (0)   Tunnel-Password:2 = "6cd2113f4cf250c476026d036142437879a2008426f260fd777ea2e934de225a"
bug: (0) Finished request
bug: Waking up in 4.9 seconds.
```

Once the connection is verified, the Rolling-PMK feature has been successfully configured.

10. Additional Resources

There are several additional tools and resources that can be used to help manage FreeRADIUS servers and associated databases. *Table 1* below provides information about these resources so that you can find access to tools that might further help you configure and manage the WPA2-Multikey and Rolling-PMK features for vWLAN.

NOTE

ADTRAN does not accept any responsibility for your use of the tools described below. The information provided below is for reference use only.

Table 1. Additional Resources for Managing FreeRADIUS and Databases

Resource	Purpose	For More Information Visit:
Apache Web Server	Open-source implementation of an HTTP server.	https://httpd.apache.org/
PHP	Open-source scripting language.	https://www.php.net/
phpMyAdmin	GUI-based management tool for managing databases.	https://www.phpmyadmin.net/
Daloradius	Provides a Web administration interface for FreeRADIUS.	https://sourceforge.net/p/daloradius/wiki/Home/
Ubuntu	Open-source Linux base server.	http://releases.ubuntu.com

11. Warranty and Contact Information

Warranty and contact information for all ADTRAN products can be obtained using the information in the following sections.

Warranty

Warranty information can be found online by visiting www.adtran.com/warranty.

Contact Information

To contact ADTRAN, choose one of the following methods:

Department	Contact Information	
Customer Care	From within the U.S.: From outside the U.S.:	(888) 4ADTRAN ((888)-423-8726)+ +1 (256) 963-8716
Technical Support	Support Community Product Support:	www.supportforums.adtran.com www.adtran.com/support
Training	Email: ADTRAN University:	training@adtran.com www.adtran.com/training
Sales	For pricing and availability:	1 (800) 827-0807