LOGPOINT

Integrations

RadiusAuthentication

V6.1.2

CONTENTS

CHAPTER

ONE

RADIUSAUTHENTICATION

The Radius Authentication enables you to log into Logpoint using RADIUS credentials, providing centralized user authentication for organizations using a RADIUS server. It supports role-based access control by mapping RADIUS roles to Logpoint user groups, allowing you to assign permission for RADIUS-authenticated users.

RADIUS user access data can be exported in CSV format for external use and later imported into Logpoint as needed. Additionally, vendor-specific dictionary files can be imported to associate descriptive names with attribute numbers in RADIUS packets, define data types for attributes, or add new custom attributes.

CHAPTER

TWO

INSTALLING RADIUSAUTHENTICATION

2.1 Prerequisite

Logpoint v7.7.0 or later

2.2 Installing Radius Authentication

1. Download the .pak file from the Help Center.
2. Go to *Settings >> System Settings* from the navigation bar and click **Applications**.
3. Click **Import**.
4. **Browse** to the downloaded .pak file.
5. Click **Upload**.

After installing Radius Authentication, you can find it in Logpoint login page. To verify:

1. Go to Logpoint login page.
2. Click **Other Authentication Options**.
3. Click **Radius Authentication**.

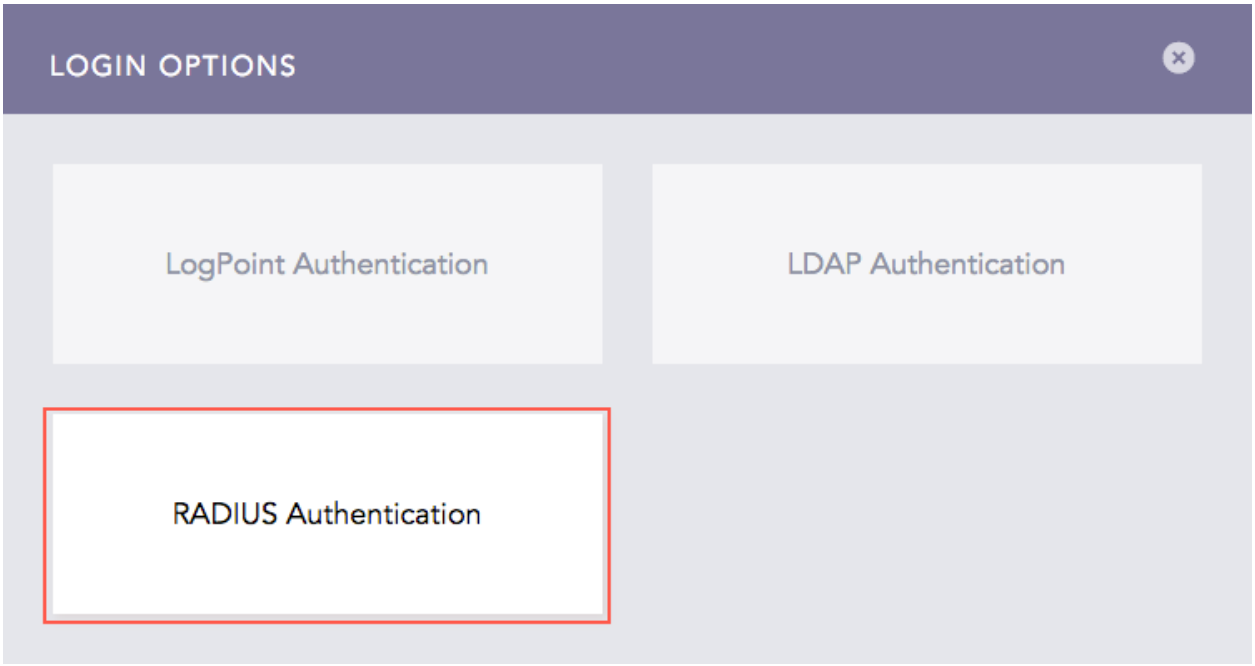

Fig. 1: RADIUS Authentication Login Option

CHAPTER

THREE

UNINSTALLING RADIUS AUTHENTICATION

You must remove the Radius Authentication configuration to delete it.

1. Go to *Settings >> System Settings* from the navigation bar and click **Plugins**.
2. Find **Radius Authentication** and click **Manage**.
3. Click the **Delete** (🗑) icon from **Actions** and click **Yes**.

To uninstall Radius Authentication:

1. Go to *Settings >> System Settings* from the navigation bar and click **Applications**.
2. Click the **Uninstall** (🗑) icon from **Actions** and click **Uninstall**.

CHAPTER

FOUR

CONFIGURING RADIUS AUTHENTICATION

You can configure radius authentication to add servers to log into Logpoint using Radius authentication. You can also select Logpoint user group as the default role and map the roles to define access permission.

1. Go to *Settings >> System Settings* from the navigation bar and click **Plugins**.
2. Find **Radius Authentication** and click **Manage**.
3. Click **ADD SERVER**.
4. Enter the IP Address of the RADIUS **Server**.
5. Enter the **Secret** passphrase of the RADIUS server.
6. Set the **Priority**, 1 being the highest.

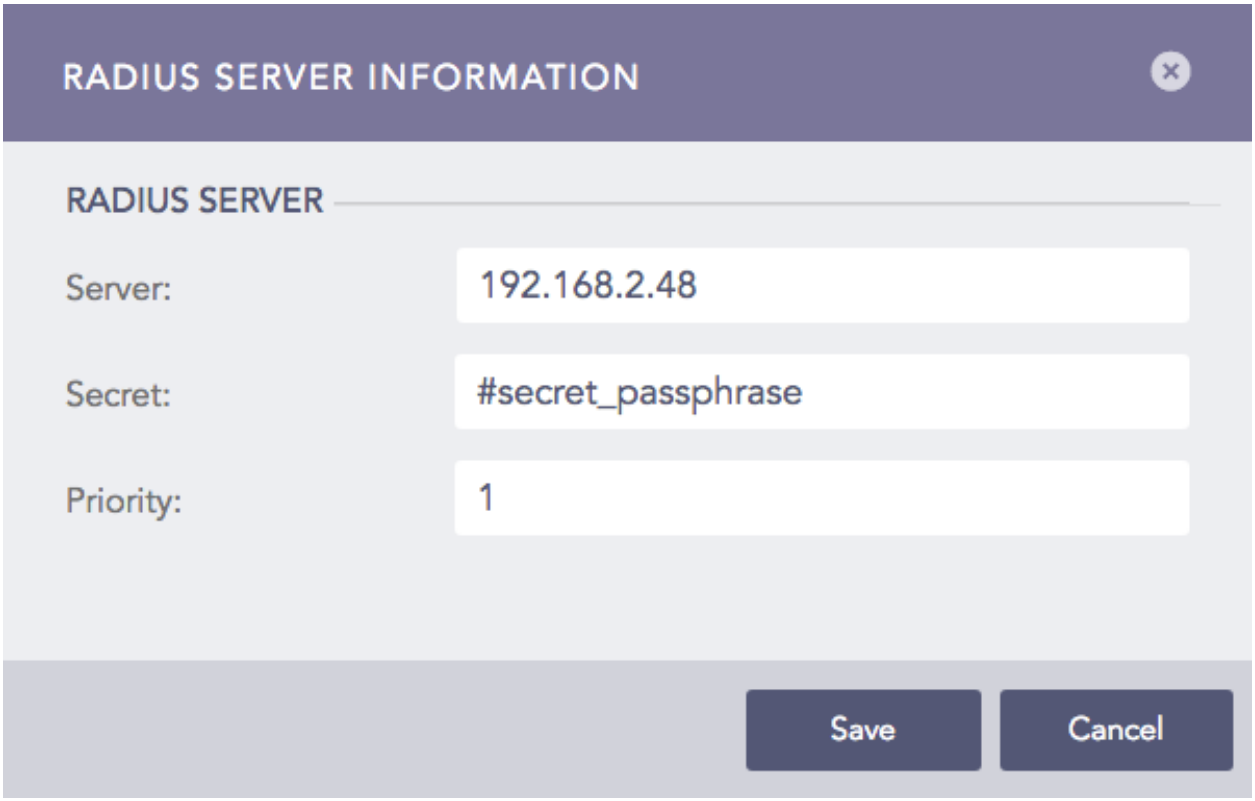

Fig. 1: RADIUS Server Information

7. Click **Save**.
8. In **DEFAULT SETTINGS**, Select a Logpoint user group as the **Default Role**.
9. Enter the **Role Attribute**.

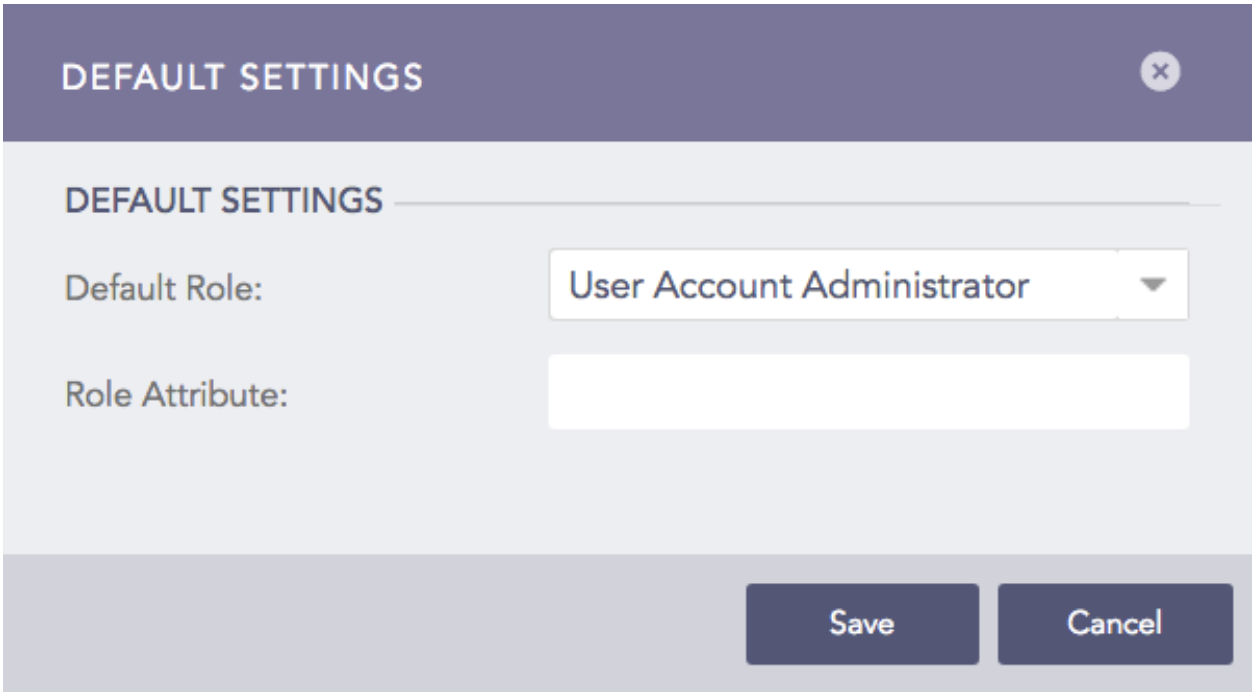

Fig. 2: Default Settings

10. Click **Save**.

4.1 Mapping Roles

You can map roles of the radius server to a Logpoint user group to define access permission in Logpoint.

1. Go to *Settings >> System Settings* from the navigation bar and click **Plugins**.
2. Find **Radius Authentication** and click **Manage**.
3. Click **ROLES MAPPING**.

5. In **Radius Role**, enter the role of the user in the radius server.

5. Select a **Logpoint User Group** to assign to the Radius role.
6. Click **Add**. A table lists the mapped RADIUS roles and LogPoint user groups. You can edit or delete the added role mappings from the table.

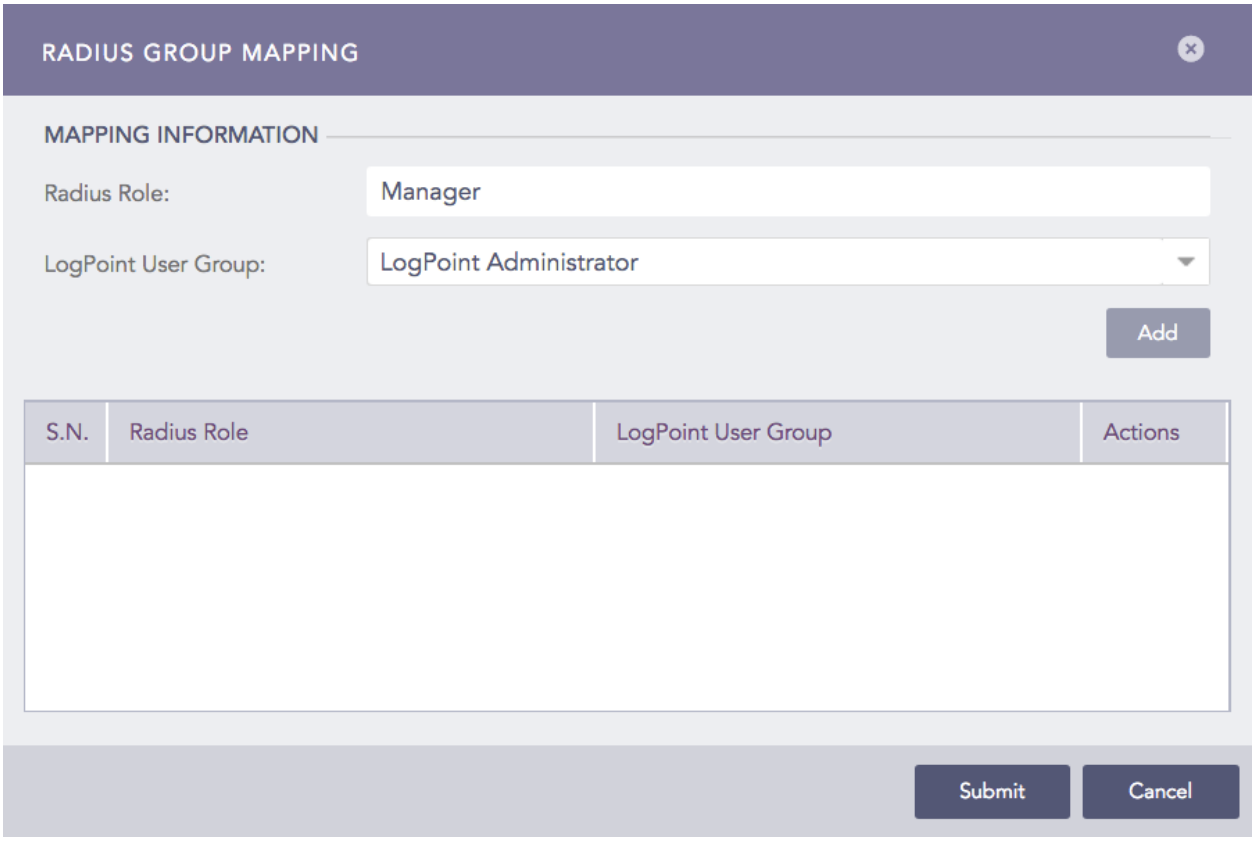

Fig. 3: RADIUS Group Mapping

7. Click **Submit**.

4.2 Importing Roles Map

A **roles map** file contains the mapping of RADIUS users with their respective RADIUS roles in a Comma Separated Value (CSV) file. To assign multiple roles to a user, separate the roles by a colon (:) in the roles map file.

User	RADIUS Role
admin	admin:operator
bob	admin
john	normal
chris	Manager
mark	Manager

Fig. 4: Roles Map File (CSV)

CSV files must be created without a header row. If a header is included, it will be processed as a valid RADIUS role entry.

To import a roles map file:

1. Click **Import Roles Map**.
2. **Browse** the roles map file (CSV).
3. Click **Submit**.

4.3 Importing Dictionary

The RADIUS dictionary file maps the attribute numbers in the RADIUS packet to a descriptive name. Using the dictionary, you can define data types for different attributes or define new attributes of the RADIUS packets.

Radius Authentication includes a dictionary file by default but you can also import a vendor-specific dictionary file.

To import a dictionary in the Radius Authentication:

1. Go to *Settings >> System Settings* from the navigation bar and click **Plugins**.
2. Find **Radius Authentication** and click **Manage**.
3. Click **IMPORT DICTIONARY**.
4. **Browse** and open the dictionary file. The name of the dictionary file must be **dictionary**.
5. Click **Submit**.

You can find the default dictionary of the Radius Authentication at:

/opt/immune/installed/webserver/pluggables/modules/Authentication/apps/
↪RadiusAuthentication/utils/dictionary

The default dictionary file consists of:

```
#
# Version $Id: dictionary,v 1.1.1.1 2002/10/11 12:25:39 wichert Exp $
#
#  This file contains dictionary translations for parsing
#  requests and generating responses.  All transactions are
#  composed of Attribute/Value Pairs.  The value of each attribute
#  is specified as one of 4 data types.  Valid data types are:
#
#  string  - 0-253 octets
#  ipaddr  - 4 octets in network byte order
#  integer - 32 bit value in big endian order (high byte first)
#  date    - 32 bit value in big endian order - seconds since
#                               00:00:00 GMT,  Jan.  1,  1970
#
#  FreeRADIUS includes extended data types which are not defined
#  in RFC 2865 or RFC 2866.  These data types are:
#
#  abinary - Ascend's binary filter format.
#  octets  - raw octets, printed and input as hex strings.
#            e.g.: 0x123456789abcdef
#
#
#  Enumerated values are stored in the user file with dictionary
#  VALUE translations for easy administration.
#
#  Example:
#
#  ATTRIBUTE       VALUE
#  --------------  -----
#  Framed-Protocol = PPP
#  7               = 1     (integer encoding)
#


#
#  Include compatibility dictionary for older users file. Move this
#  directive to the end of the file if you want to see the old names
#  in the logfiles too.
#
#$INCLUDE dictionary.shasta
#$INCLUDE dictionary.shiva
#$INCLUDE dictionary.tunnel
```

(continues on next page)

(continued from previous page)

```
#$INCLUDE dictionary.usr
#$INCLUDE dictionary.versanet
#$INCLUDE dictionary.erx
#$INCLUDE dictionary.freeradius
#$INCLUDE dictionary.alcatel

#
#       Following are the proper new names. Use these.
#
ATTRIBUTE       User-Name               1       string
ATTRIBUTE       User-Password           2       string
ATTRIBUTE       CHAP-Password           3       octets
ATTRIBUTE       NAS-IP-Address          4       ipaddr
ATTRIBUTE       NAS-Port                5       integer
ATTRIBUTE       Service-Type            6       integer
ATTRIBUTE       Framed-Protocol         7       integer
ATTRIBUTE       Framed-IP-Address       8       ipaddr
ATTRIBUTE       Framed-IP-Netmask       9       ipaddr
ATTRIBUTE       Framed-Routing          10      integer
ATTRIBUTE       Filter-Id               11      string
ATTRIBUTE       Framed-MTU              12      integer
ATTRIBUTE       Framed-Compression      13      integer
ATTRIBUTE       Login-IP-Host           14      ipaddr
ATTRIBUTE       Login-Service           15      integer
ATTRIBUTE       Login-TCP-Port          16      integer
ATTRIBUTE       Reply-Message           18      string
ATTRIBUTE       Callback-Number         19      string
ATTRIBUTE       Callback-Id             20      string
ATTRIBUTE       Framed-Route            22      string
ATTRIBUTE       Framed-IPX-Network      23      ipaddr
ATTRIBUTE       State                   24      octets
ATTRIBUTE       Class                   25      octets
ATTRIBUTE       Vendor-Specific         26      octets
ATTRIBUTE       Session-Timeout         27      integer
ATTRIBUTE       Idle-Timeout            28      integer
ATTRIBUTE       Termination-Action      29      integer
```

CHAPTER

FIVE

LOGIN WITH RADIUSAUTHENTICATION

After configuring Radius Authentication, you can log into Logpoint using the RADIUS credentials.

1. Go to the Logpoint login page.
2. Click **Other Authentication Options**.
3. Select **RADIUS Authentication**.

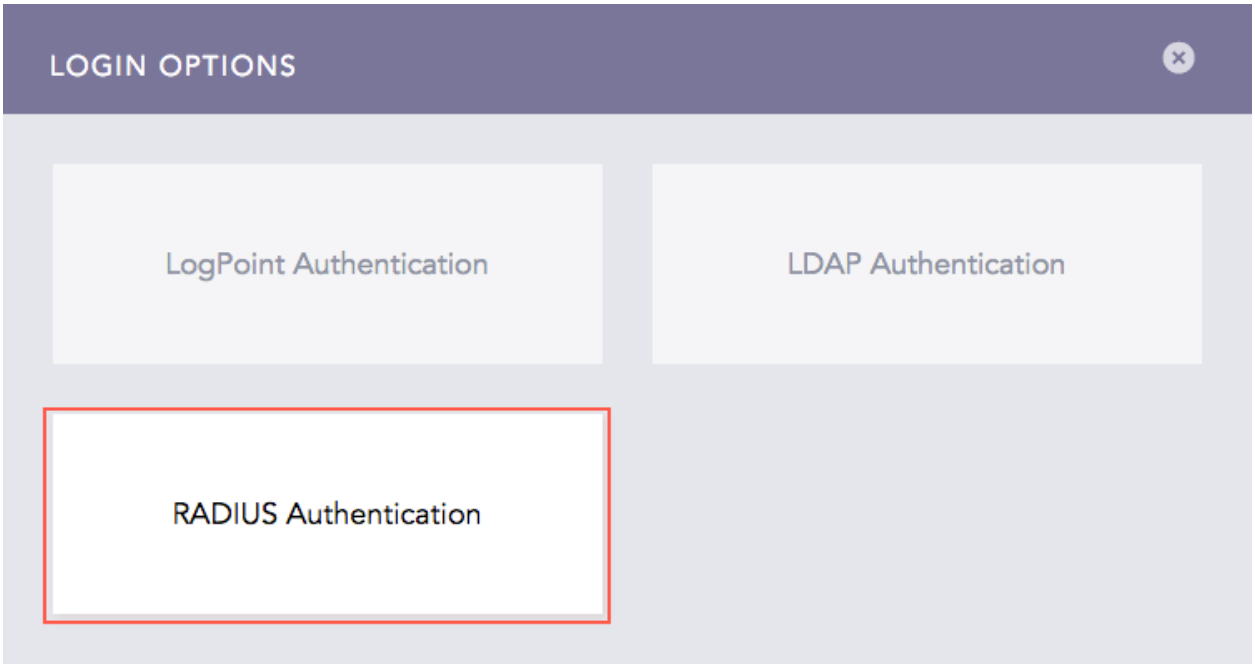

Fig. 1: Login Options

4. Enter your RADIUS **Username** and **Password**.
5. Click **Login**.

If you have configured Duo Security in your Logpoint, verify with the Duo's two-factor authentication. Go to Duo Security Guide for more information.

Once you log in with the RADIUS credentials, the system adds "radius_" as a prefix to your username. For example, if you log in as "bob" with the RADIUS Authentication option, Logpoint updates your username as "radius_bob."

CHAPTER

SIX

MANAGE RADIUSAUTHENTICATION USERS

Logpoint users with high privilege can manage RADIUS users.

1. Go to *Settings >> System Settings* and click **User Accounts**.
2. Click **Users**.
3. In the **Plugin Users**, click **RADIUS Authentication**.
4. Click the **De-Activate User** icon in **Actions** to deactivate a user.

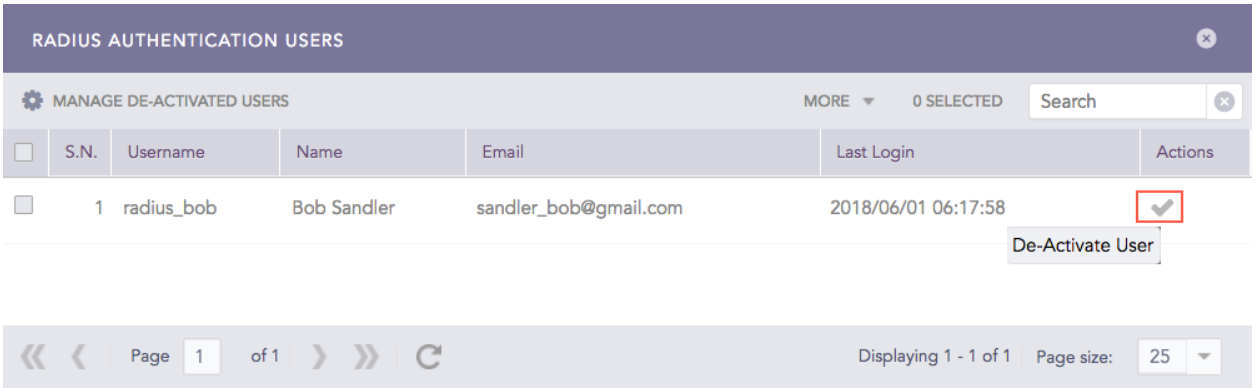

Fig. 1: De-Activate RADIUS Users

5. Click **Yes**.
6. Enter your credentials and click **Ok**.
7. Click **Manage De-Activated Users**.

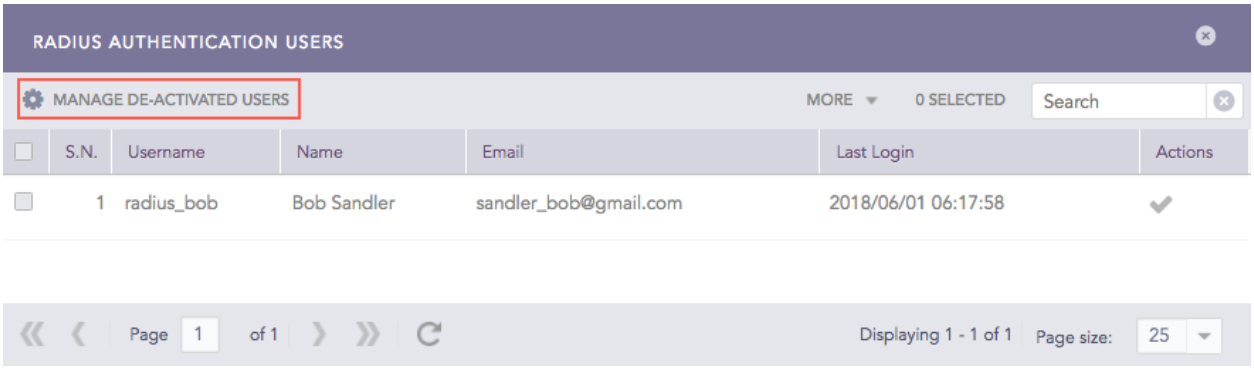

Fig. 2: Manage De-Activated RADIUS Users

8. Click the **Activate** icon or the **Delete** icon to activate or delete the de-activated user respectively.