

Integrations

RadiusAuthentication

V6.1.0

CONTENTS

1	RadiusAuthentication	1
2	Installing RadiusAuthentication	2
2.1	Prerequisite	2
2.2	Installing Radius Authentication	2
2.3	Verifying the Installation	2
3	Configuring the Application	4
3.1	Configuring the Radius Authentication	4
3.2	Configuring Default Settings	5
3.3	Mapping Roles	6
3.4	Importing Roles Map	8
3.5	Importing Dictionary	9
4	Login with RadiusAuthentication	13
4.1	Logging in using RadiusAuthentication in Logpoint	13
5	Manage RadiusAuthentication Users	16
5.1	Managing RadiusAuthentication Users	16
6	Uninstalling Radius Authentication	18
6.1	Uninstalling Radius Authentication	18

RADIUSAUTHENTICATION

The Radius Authentication enables you to log into Logpoint using RADIUS credentials. If your organization uses a RADIUS server, you can export its users along with their respective role-based access control rules in CSV format and import them into Logpoint.

Using the RadiusAuthentication, you can:

1. Log into Logpoint using the RADIUS credentials.
2. Map a particular RADIUS role to a Logpoint user group, thus assigning specific sets of permissions to different RADIUS users.
3. Import a vendor-specific dictionary file to:
 - Map descriptive names to attribute numbers in the RADIUS packet.
 - Define data types for an attribute.
 - Define new attributes.

INSTALLING RADIUSAUTHENTICATION

2.1 Prerequisite

Logpoint v7.5.0

2.2 Installing Radius Authentication

1. Download the .pak file from the [help center](#).
2. Go to *Settings >> System >> Applications*.
3. Click **Import**.
4. **Browse** to the downloaded .pak file.
5. Click **Upload**.

2.3 Verifying the Installation

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

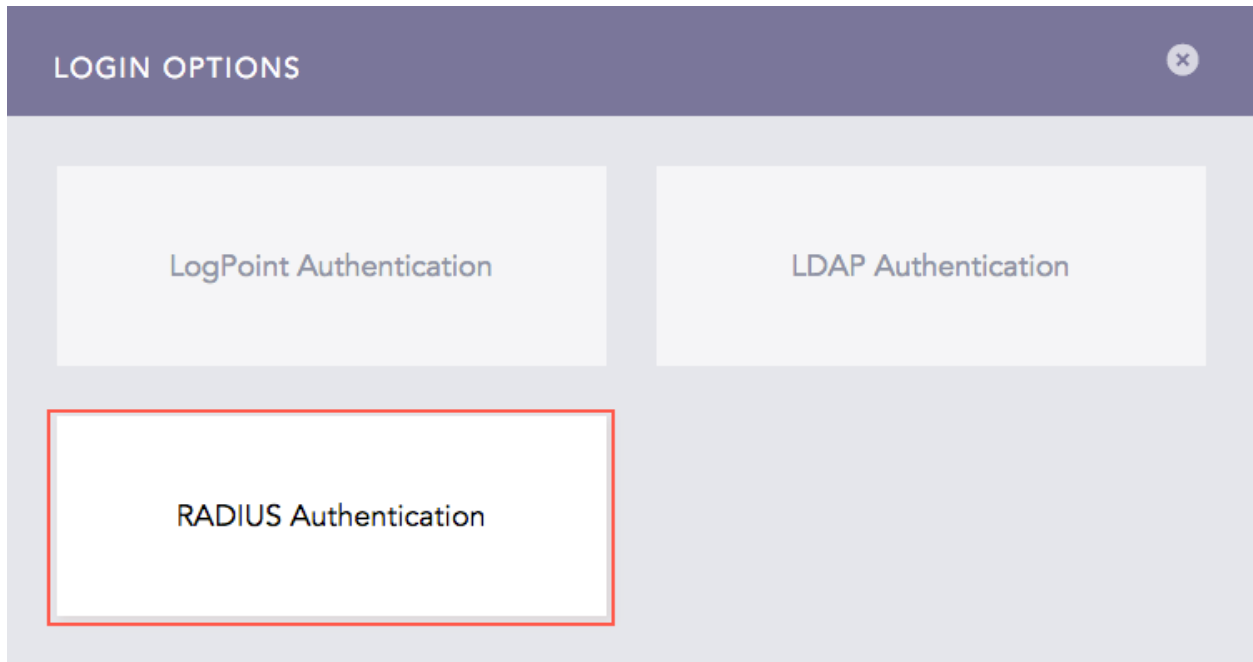


Fig. 1: RADIUS Authentication Login Option

CONFIGURING THE APPLICATION

3.1 Configuring the Radius Authentication

1. Go to *Settings >> System >> Plugins*.
2. Find **Radius Authentication** and click **Manage**.

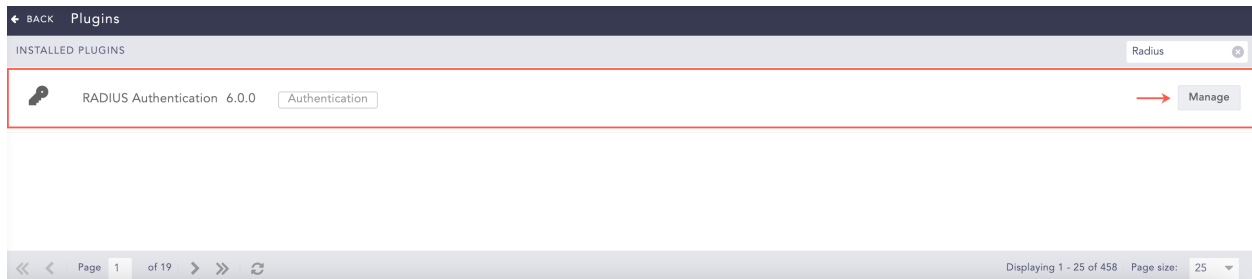
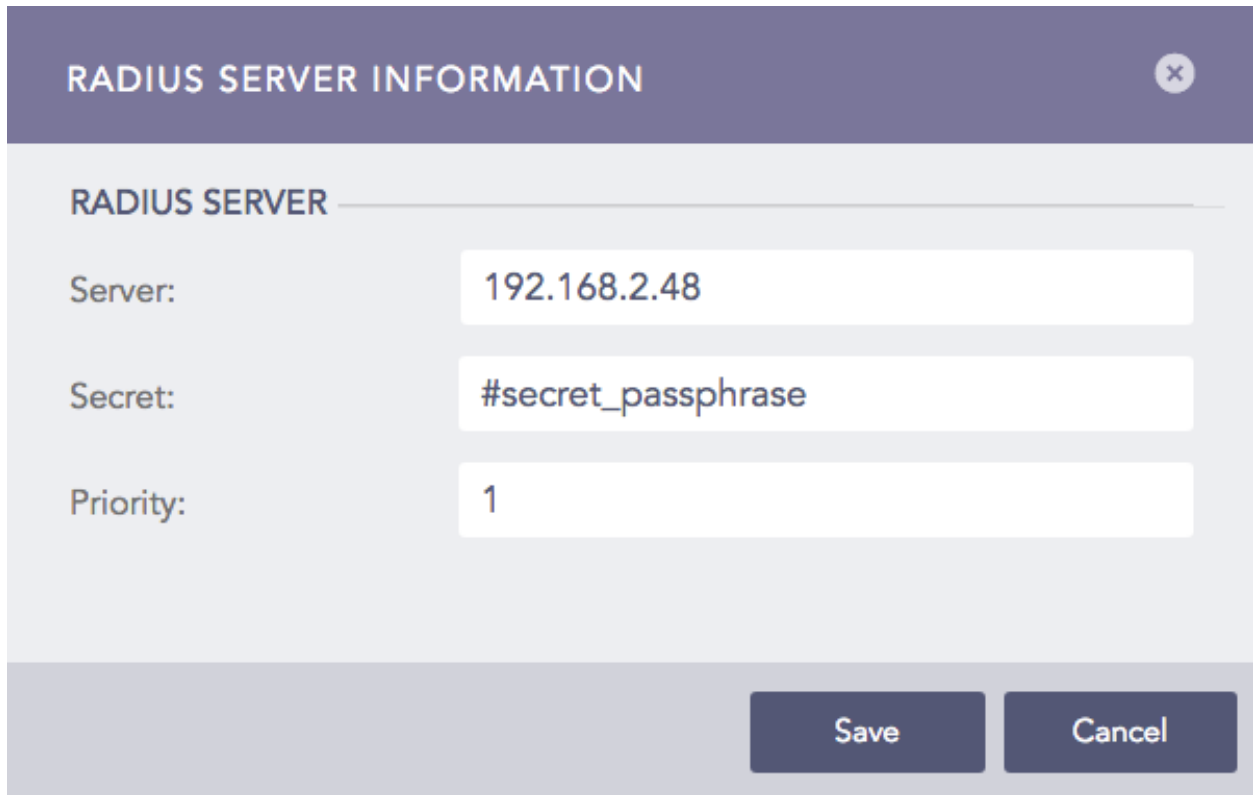


Fig. 1: Manage RADIUS Authentication

3. Click **Add Server**.



The image shows a 'RADIUS SERVER INFORMATION' panel with a dark purple header and a light gray body. The header has a close button (X) in the top right corner. Below the header, the title 'RADIUS SERVER' is followed by a horizontal line. There are three input fields: 'Server:' with the value '192.168.2.48', 'Secret:' with the value '#secret_passphrase', and 'Priority:' with the value '1'. At the bottom right, there are two buttons: 'Save' and 'Cancel'.

Field	Value
Server:	192.168.2.48
Secret:	#secret_passphrase
Priority:	1

Fig. 2: RADIUS Server Information Panel

4. Enter the RADIUS **Server** IP Address.
5. Enter the **Secret** passphrase of the RADIUS server.
6. Set the **Priority** of the RADIUS server in the application, 1 being the highest priority.
7. Click **Save**.

3.2 Configuring Default Settings

1. Click **Default Settings**.

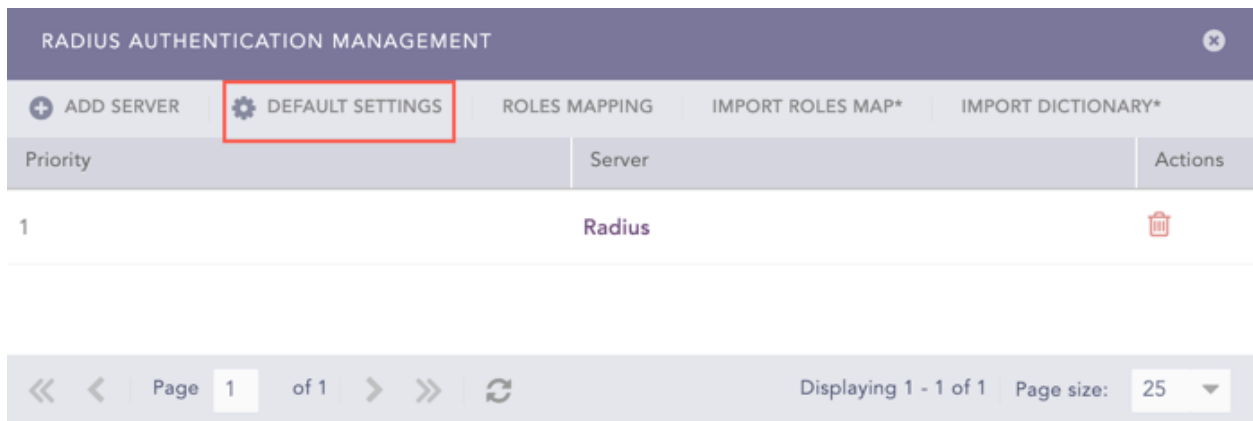


Fig. 3: Radius Authentication Management Panel

2. Select a LogPoint user group as the **Default Role**.

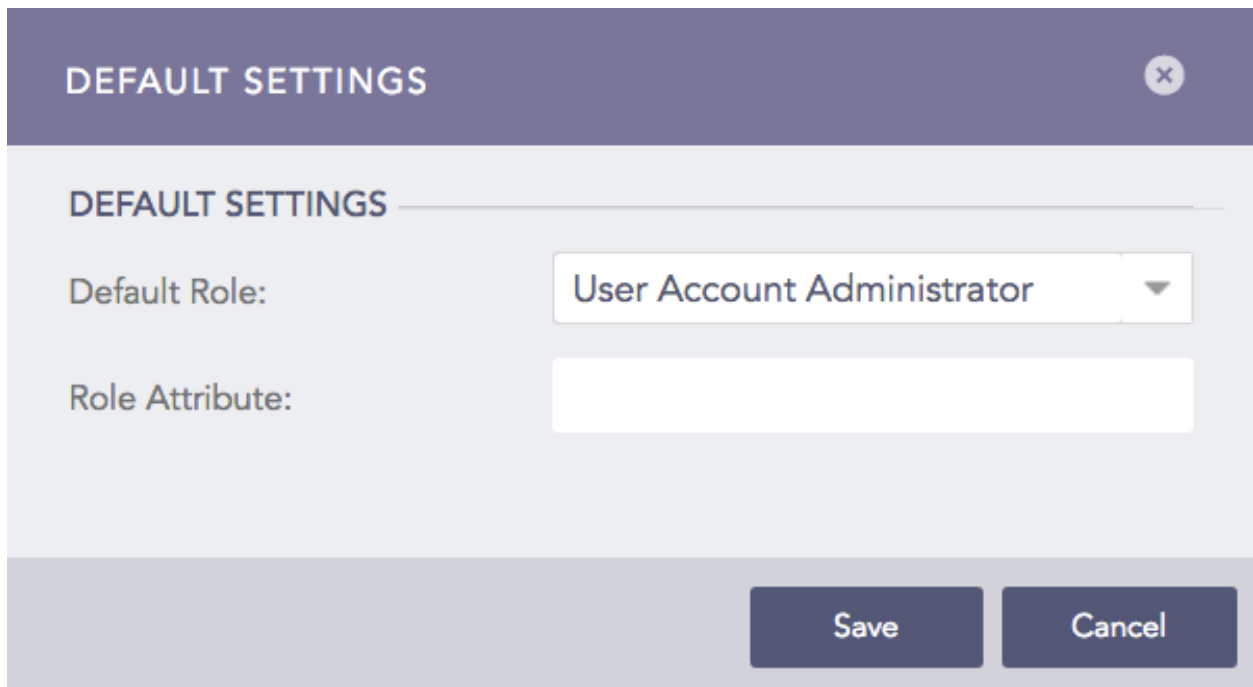


Fig. 4: Default Settings Panel

3. Click **Save**.

3.3 Mapping Roles

You can map a Radius role to a LogPoint user group to define access permission on LogPoint.

Follow these steps to map an Radius role to a LogPoint user group:

1. Click **Roles Mapping**.
2. Enter a **Radius Role**.
3. Select a **LogPoint User Group** to assign to the Radius role mentioned above.

RADIUS GROUP MAPPING

MAPPING INFORMATION

Radius Role:

Manager

LogPoint User Group:

LogPoint Administrator

Add

S.N.	Radius Role	LogPoint User Group	Actions
------	-------------	---------------------	---------

Submit

Cancel

Fig. 5: RADIUS Group Mapping

3. 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.

RADIUS GROUP MAPPING

MAPPING INFORMATION

Radius Role:

LogPoint User Group:

Add

S.N.	Radius Role	LogPoint User Group	Actions
1	Manager	LogPoint Administrator	^ v

Submit

Cancel

Fig. 6: Added RADIUS Group Mapping

- Click **Submit**.

3.4 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.

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

Fig. 7: Roles Map File (CSV)

Note: To assign multiple roles to a user, separate the roles by a colon (:) in the roles map file.

Follow these steps to import a roles map file:

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

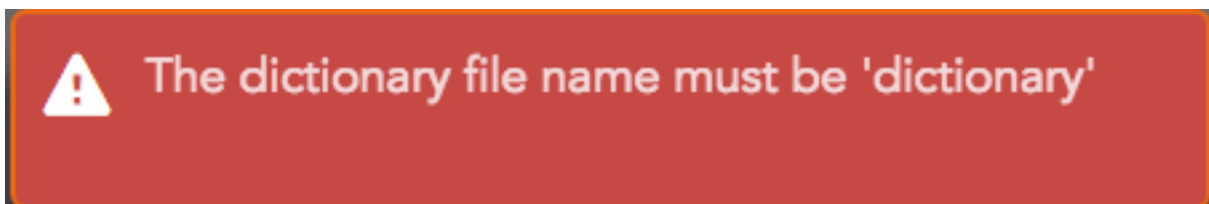
3.5 Importing Dictionary

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.

The Radius Authentication application includes a dictionary file by default. However, you can also import a vendor-specific dictionary file.

Follow these steps to import a dictionary in the Radius Authentication application:

1. Set the name of the dictionary file as **dictionary**. Otherwise, the application prompts the following error:



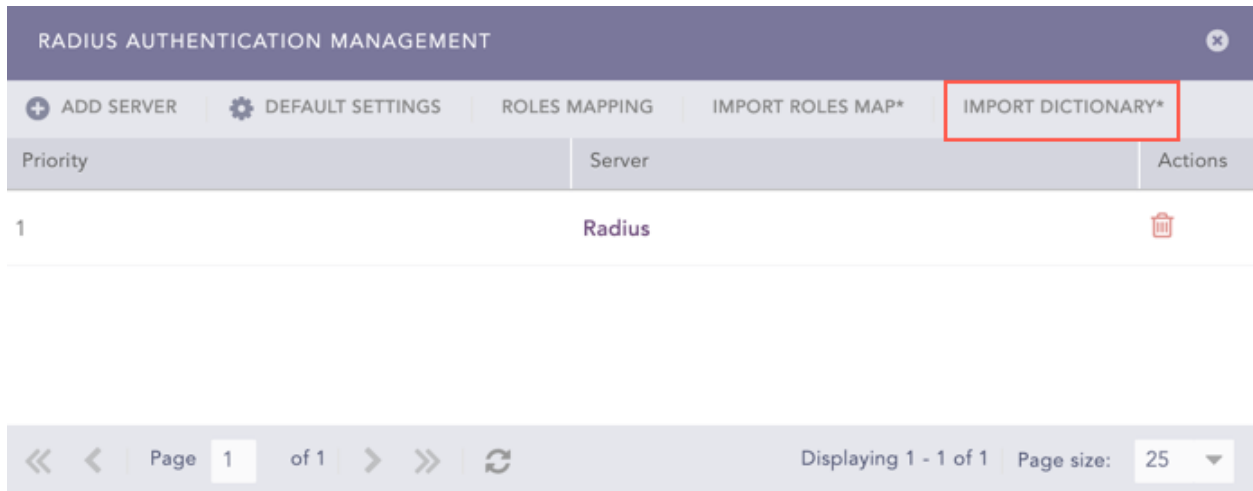


Fig. 8: Importing Dictionary

2. Click **Import Dictionary**.
3. **Browse** and open the dictionary file.
4. Click **Submit**.

You can find the default dictionary of the Radius Authentication application at the following location:

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

The default dictionary file consists of the following part:

```
#
# 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:
```

(continues on next page)

(continued from previous page)

```

#
# 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
#$INCLUDE dictionary.tunnel
#$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

```

(continues on next page)

(continued from previous page)

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

LOGIN WITH RADIUSAUTHENTICATION

4.1 Logging in using RadiusAuthentication in Logpoint

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

To log in with RADIUS Authentication:

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

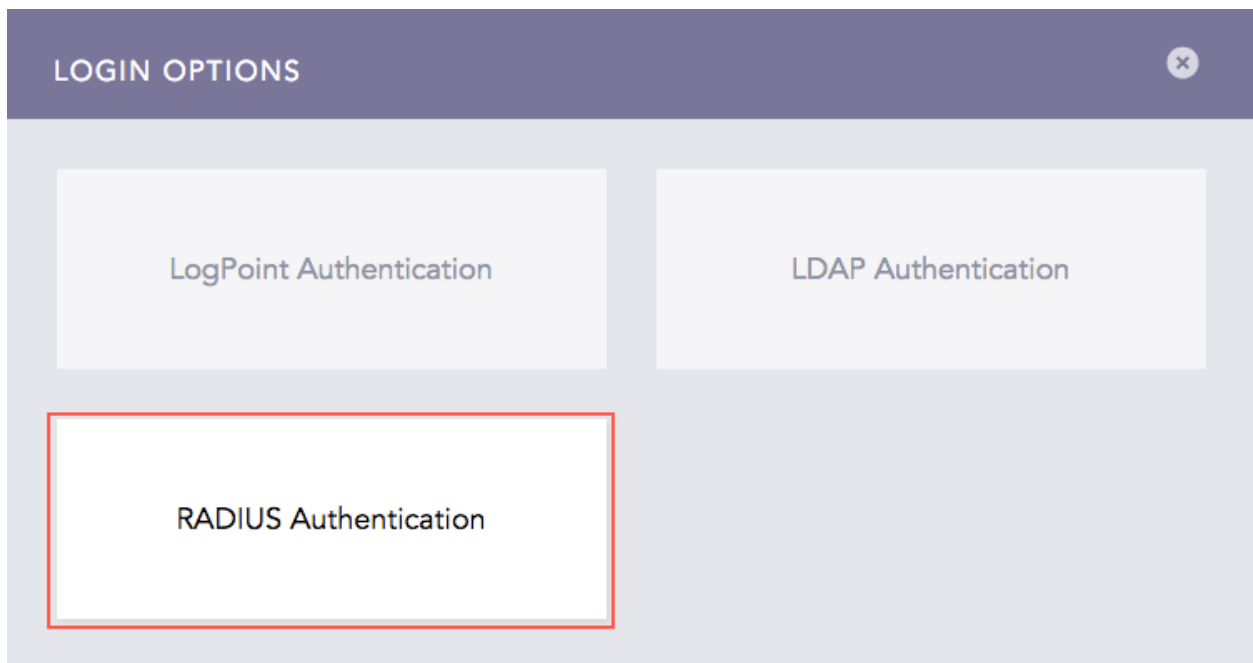


Fig. 1: Login Options

4. Enter your RADIUS **Username** and **Password**.

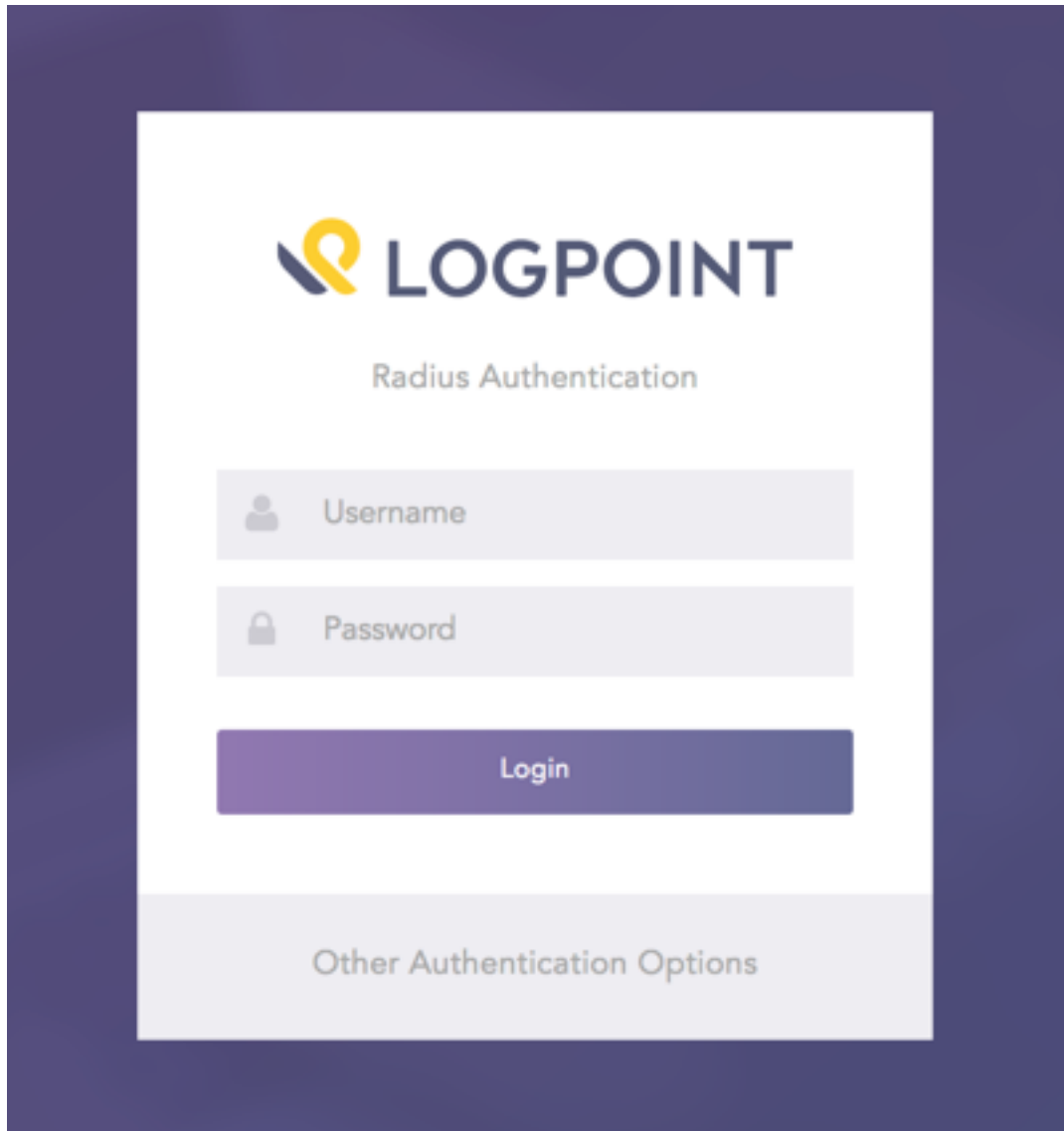
The image shows a login page for Logpoint's Radius Authentication. It features a dark purple background with a white rectangular form in the center. At the top of the form is the Logpoint logo, which consists of a stylized yellow and blue icon followed by the word "LOGPOINT" in blue. Below the logo is the text "Radius Authentication" in a smaller, grey font. There are two input fields: the first is labeled "Username" with a grey user icon to its left, and the second is labeled "Password" with a grey lock icon to its left. Below these fields is a solid purple "Login" button. At the bottom of the form is a light grey rectangular area with the text "Other Authentication Options" in a grey font.

Fig. 2: Radius Login Page

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."

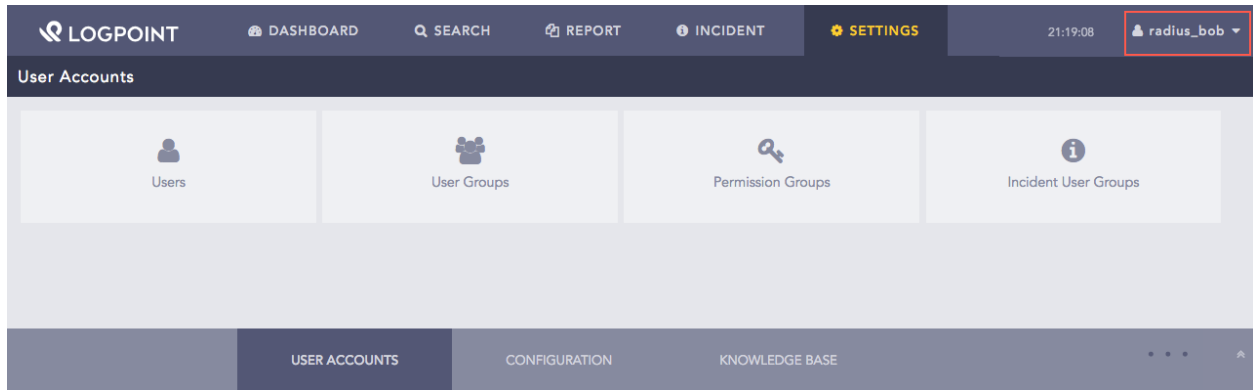


Fig. 3: User Logged In with Radius Authentication

MANAGE RADIUSAUTHENTICATION USERS

5.1 Managing RadiusAuthentication Users

Logpoint users with sufficient privilege can manage RADIUS users.

To manage RADIUS users:

1. Go to *Settings >> System >> User Accounts*.
2. Click **Users**.
3. In the **Plugin Users** drop-down, click **RADIUS Authentication**.

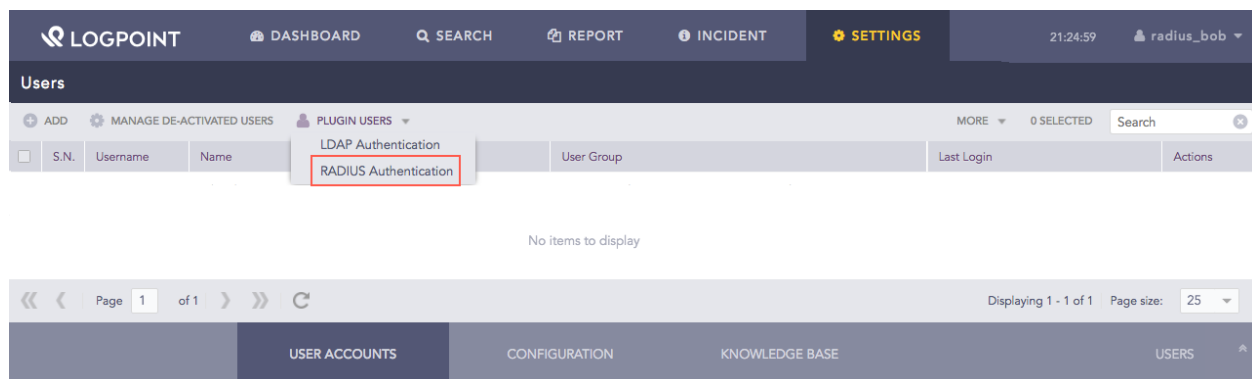


Fig. 1: Plugin Users

4. Click the **De-Activate User** icon in **Actions** to deactivate a user.

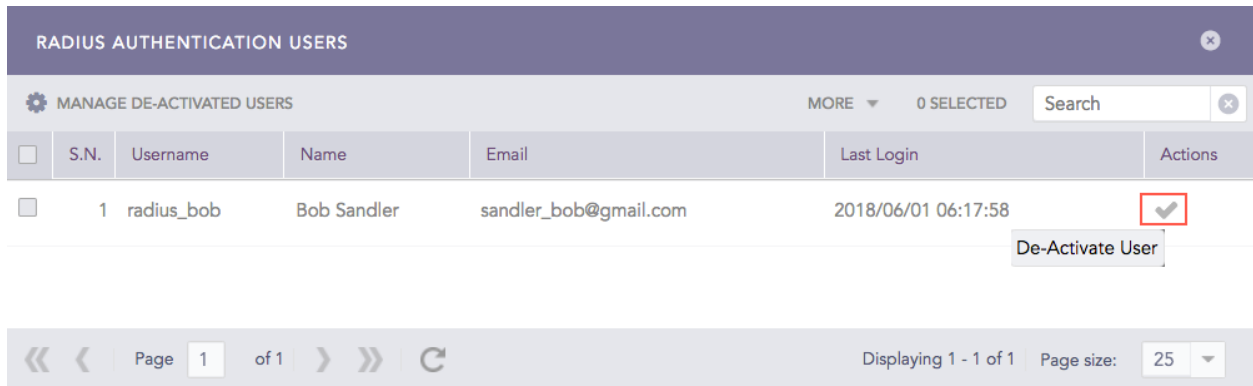


Fig. 2: De-Activate RADIUS Users

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

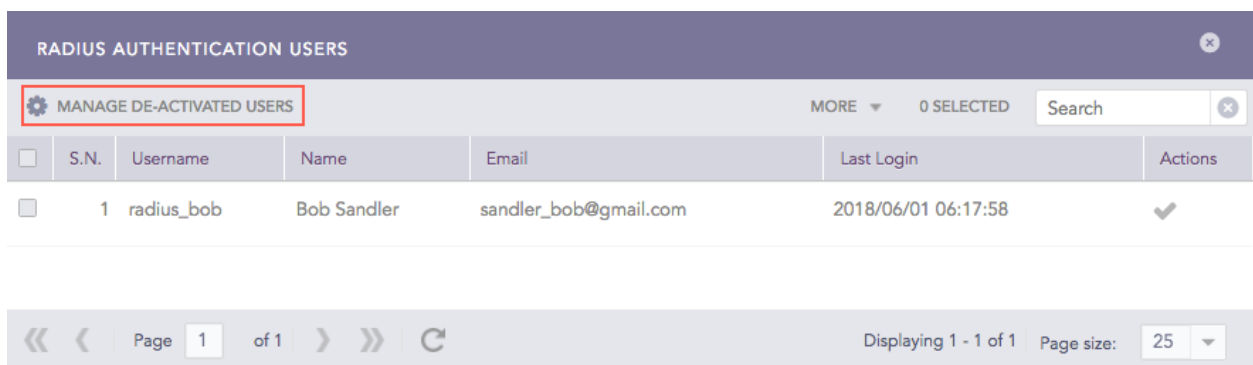


Fig. 3: Manage De-Activated RADIUS Users

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

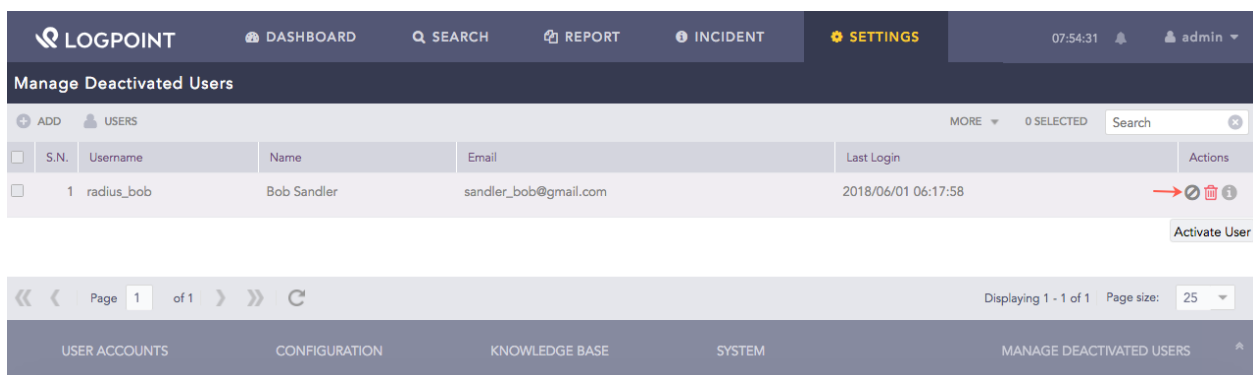


Fig. 4: Activate the De-Activated RADIUS Users

UNINSTALLING RADIUS AUTHENTICATION

6.1 Uninstalling Radius Authentication

You must remove the Radius Authentication configuration to delete it.

1. Go to *Settings >> System >> Applications*.
2. Click the **Uninstall** (🗑️) icon from the **Actions** column.