

# RADIUS Integration for Lastline Enterprise and Analyst On-Premise

January 17, 2024

## 1 Introduction

This guide describes the integration of the RADIUS Protocol so that it can be used by the Lastline Enterprise or Analyst On-Premise.

The purpose of using the RADIUS Protocol is to allow an alternative source of authentication. This is useful in enterprise solutions where all authentication is centralized to one location. Configuring the Lastline Manager/Analyst On-Premise to use the RADIUS Protocol will allow users to use the aforementioned centralized authentication service.

This means that users can login to Lastline Manager/Analyst On-Premise using existing credentials on their centralized auth server on their network.

In the following sections, this guide will describe how to configure and successfully use the RADIUS Protocol.

## 2 Overview of the RADIUS Integration

### 2.1 Scope

- Only used for authentication.
- Account must already exist on the Lastline Manager/Analyst On-Premise
- Only RADIUS PAP authentication type.
- Only freeradius dictionary tested and supported. Other dictionaries may be configured. See 4.2 for custom dictionary configuration or contact Lastline support at [support@lastline.com](mailto:support@lastline.com)

### 2.2 Glossary

This section briefly defined a few terms that will be used in the documentation.

#### 2.2.1 FreeRADIUS

An open source, high performance, RADIUS suite that supports all common authentication protocols.

#### 2.2.2 RADIUS Dictionary

Dictionary file that contains a list of RADIUS attributes and values. These attributes and values are then used to map between descriptive names and on-the-wire-data. The names have no meaning outside of the RADIUS server itself, and are never exchanged between server and clients. The dictionary is specific to each RADIUS server.

#### 2.2.3 Network Access Server (NAS)

A Nas is a single point of access to a remote resource. In this integration, the Lastline Manager/Analyst On-Premise is the NAS.

## 2.3 Architecture

When using the RADIUS Integration a Lastline Manager/Analyst On-Premise can be configured to send RADIUS Authentication requests to a configured RADIUS server. The user has the option to choose whether he or she wants to authenticate using the default Lastline Manager/Analyst On-Premise authentication or through the RADIUS Server.

The current implementation of RADIUS authentication uses PAP authentication by containing a shared secret between the NAS and the RADIUS server. The protocol "hides" the password using the following [implementation](#).

Upon a successful authentication response from the RADIUS Server, the Lastline Manager/Analyst On-Premise will authenticate the user to the portal. The authentication will only work if the account already exists on the portal and the mapping is correct (see: 3.3).

After the RADIUS authentication is performed and is valid, the user will be logged into the Lastline Manager/Analyst On-Premise.

## 3 Requirements

### 3.1 Required Version

The Lastline Enterprise must be version 7.3 or above.

### 3.2 RADIUS Server

Currently, freeRADIUS is fully supported and tested on version 2.1.12. The freeRADIUS dictionary will work with some other RADIUS servers, including Windows Server 2016 Network Policy Server, and other RADIUS servers may work by configuring custom dictionaries (see: 4.2). The RADIUS server must also permit users to perform PAP authentication. Please contact support at [support@lastline.com](mailto:support@lastline.com) if there is a compatibility issue with the RADIUS server; additional RADIUS servers can be supported in future versions.

### 3.3 RADIUS Attribute Mapping

In order for the Lastline Manager/Analyst On-Premise to authenticate the user based on the response from the RADIUS, one of the following two conditions must be met:

#### **"User-Name" attribute in response**

If the "User-Name" attribute is present in the response of the authentication, this value will be used to authenticate to the Lastline Manager/Analyst On-Premise. For example, let's assume "DOMAIN\jdoe" is the username of the original auth request, the response from the RADIUS server must be mapped to the correct username on the Lastline Manager/Analyst On-Premise, such as "jdoe@DOMAIN.com".

#### **No "User-Name" in response**

If there is no "User-Name" in the response of the authentication, then the username of the request will be used. For example, if a valid auth response is returned for "jdoe@DOMAIN.com", then this user will be used to authenticate to the Lastline Manager/Analyst On-Premise.

### 3.4 RADIUS Dictionary

A valid dictionary must be presented to the RADIUS client. If the "server\_type" parameter for the configuration is "freeradius" (the default), then the dictionary of freeRADIUS version 2.1.12 will be used. The freeRADIUS dictionary is known to be compatible with Windows Server 2016 Network Policy Server.

## 4 Configuration

### 4.1 Configuring Lastline Manager/Analyst On-Premise

To configure a RADIUS server to be used for authentication, please refer to the [Lastline RADIUS API docs](#). In particular, the "/papi/radius/configure" method is used for RADIUS configuration.

### 4.2 Configuring Custom Dictionaries

If a different type of RADIUS server is used (not freeRADIUS-compatible), or the default dictionary provided with the installation does not work, it is possible to provide a custom dictionary. This custom dictionary must be placed in the following path: "/var/lib/pyrad/dicts/other/dictionary" and the "server\_type" for configuration MUST be set to "other".

### 4.3 Configuration Example

The following dictionary is an example of a valid RADIUS configuration:

```
{
  "appliance_uuid": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
  "enabled": true,
  "server_type": "freeradius",
  "server": "freeradius.mydomain.com",
  "auth_port": 1812,
  "secret": "mysupersharedradiussecret",
  "nas_identifier": "LLManager"
}
```

This can be performed with a curl command, like the following:

```
curl -d "appliance_uuid=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF" \
  -d "enabled=true" \
  -d "server_type=freeradius" \
  -d "server=freeradius.mydomain.com" \
  -d "auth_port=1812" \
  -d "secret=mysupersharedradiussecret" \
  -d "nas_identifier=LLManager" \
  "https://<FQDN>/papi/radius/configure?api_key=YOURAPIKEY&api_token=YOURAPITOKEN"
```

### 4.4 Successful Configuration

After a successful POST to the configuration API, the Lastline Manager/Analyst On-Premise will perform a new configuration task on itself that may take a few minutes. After this is completed, a new login page will be displayed and will look like the figure below:

### Log in to the Lastline Portal

Username

Password

RADIUS Sign On


[Forgot your password?](#)


RADIUS Login page

Notice this figure includes a new check box labeled as "RADIUS Sign On". If this checkbox is selected, the user will authenticate through the configured RADIUS server. If the user does not have this checkbox selected, then the authentication will be performed through the Lastline Manager/Analyst On-Premise user portal instead.

If this login page is not displayed, then there was either an error in the configuration or the configuration process is still pending. To view this information, please visit the appliance action logs page, located in the "Appliances->Logs->Action Logs" section of the user portal. Additional documentation on this page can be found [here](#).

A successful configuration log will look like the first row in the following table :

Appliance: My Manager1 

Quick search   

Start time	Last status update	Type	Status
2014-12-10 23:51:22	2014-12-10 23:52:01	CONFIGURE	Success
2014-12-10 04:02:11	2014-12-10 04:03:17	CONFIGURE	Pending

Successful configuration log after configuring RADIUS