GREENRADIUSVIRTUAL APPLIANCE

WEB API GUIDE

GREENRADIUS VA VERSION: 2.0.0.0

OCTOBER 4, 2015

DISCLAIMER

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Green Rocket Security Inc. shall have no liability for any error or damages of any kind resulting from the use of this document. The Green Rocket Security Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

1900 Camden Ave San Jose, California 95124 +1-888-793-3247 www.greenrocketsecurity.com

INTRODUCTION

GreenRADIUS virtual appliance (VA) can be used for two-factor authentication using existing enterprise directory. It provides an API for applications to integrate with GreenRADIUS server over HTTP (referred as the Web API).

This document describes the Web API interface of the GreenRADIUS VA (version 2.0.0.0 or later) for system integrators, application developers and anyone else interested in integrating the GreenRADIUS two factor authentication into their systems.

WORKING OF THE WEB API

GreenRADIUS Virtual Appliance carries out two factor authentication by first validating the username and password and then the OTP (appended to either to the username or the password) as described in this section. Following Token types are currently supported for OTP:

- Standard YubiKey (44 char OTP)
- OATH-HOTP (OATH-TOTP support coming soon)
- FIDO-U2F (version 1.0)
- Temporary Token (please refer GreenRADIUS admin guide for details)

The Web API returns 'OK' if the user credentials and the OTP, both are successfully authenticated. Otherwise status reflecting the type of error is returned as described in the RESPONSE format given below.

THE WEB API - HTTP 'POST' REQUEST PARAMETERS AND THE RESPONSE FORMAT

REQUEST FORMAT

https://<<host name of GRVA>>/wsapi/ropverify.php?user=<<username>>&password=<<password+OTP>>

Parameter	Type	Required	Description
User or User+OTP	String	Yes	The username with or without OTP appended
Password or Password+OTP	String	Yes	The password with or without OTP appended

RESPONSE FORMAT

t=2015-10-01T14:14:32Z0763
status=OK

Parameter	Type	Description
t	String	Response time
Status	String	The status of authentication request: **OK** – Authentication successful **REPLAYED_OTP** – Already used OTP **INVALID_OTP** - The OTP/Temporary Token is invalid **AUTHENTICATION_ERROR** - Authentication unsuccessful.

		(invalid username and/or password and/or OTP) **MISSING_PARAMETER** - When username or password is missing
Class	String	The class or User Group Membership information

USERNAME AND PASSWORD VALIDATION

- Determines if OTP is appended to username or password and accordingly extracts the values of the username and password to pass on to OpenLDAP/AD for authentication
- If authentication fails, returns 'AUTHENTICATION_ERROR' status

OTP VALIDATION

Depending upon the token type an OTP is validated as follows:

Token Type	Validation
Yubikey	• Check if the token is expired or blocked • Validates OTP with configured validation server • Checks if the token is assigned to the user ○ If not, and if Auto-provisioning is enabled on the GreenRADIUS VA, the Token is assigned to the user (if the username and password are valid)
Temporary Token	• Checks if the max use of temp Token is reached • Checks if the temp token is expired (time expiration) • Validates OTP (if OTP is successful; the system switches to OTP mode for user)
OATH-HOTP	• Checks if the token is expired • Checks if the token is assigned to the user • Checks if the token is blocked • Validates OTP
FIDO-U2F	• Checks if the token is expired • Checks if the token is assigned to the user • Validates OTP

NOTE

The Web API supports only the POST request type. When it receives any other request type, it responds with "ERROR Invalid Request".

ABBREVIATIONS

- API – Application Programming Interface
- VA – Virtual Appliance
- OATH –Open authentication
- OTP – One time password
- HOTP – HMAC OTP
- AD – Active Directory

- LDAP – Light Weight Directory Access Protocol

REFERENCES

- GreenRADIUS Virtual Appliance Configuration and Administration Guide