GreenRADIUS Web API Guide

MAY 2020

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.

INTRODUCTION

GreenRADIUS provides state-of-the-art two-factor authentication (2FA) while allowing easy integration with your existing enterprise directory service. In many cases, organizations want a way to add 2FA to a custom website and similar. The GreenRADIUS Web API provides exactly this, an easy to use Web API for applications to integrate with GreenRADIUS over HTTPS, Rest API.

PURPOSE

This document describes the GRAS Web API interface for interfacing to GRAS/GreenRADIUS for system integrators, application developers, and anyone else interested in integrating GreenRADIUS with their systems.

WORKING OF THE WEB API

GreenRADIUS carries out two-factor authentication by validating the username and password, and the OTP/Response from a token associated with the user as described in this section. The following token types are currently supported:

- YubiKey OTP
- OATH-HOTP and OATH-TOTP (such as YubiKey in OATH-HOTP mode, Google Authenticator and other Authenticator apps)
- Green Rocket 2FA mobile app (which uses push notifications)
- FIDO U2F
- FIDO2 WebAuthN (coming soon)
- Temporary Token (please refer to the GreenRADIUS admin guide for details)

The Web API returns “OK” if the user credentials and the token are both successfully authenticated/validated. Otherwise, an error message is returned. The returning of the error details in the response is configurable. It is controlled by a configuration entry "**grasapi_show_error_details**" present in the **sys_settings** table in the **ykrop2** database. The default state is “**true**”, i.e. error details are returned. To disable the returning of error details, set the value of the **‘grasapi_show_error_details’** setting to “**false**”. The response format is described in the RESPONSE FORMAT as listed in the sections below.

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

WEB API FOR 2FA USING OTP OR GREEN ROCKET 2FA MOBILE APP

REQUEST FORMAT

https://<<IP address or host name of GreenRADIUS>>/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 WHEN **grasapi_show_error_details** is set to false

t=2020-12-16T14:14:32Z0763
status=OK

Parameter	Type	Description
T	String	Response time
Status	String	The status of authentication request: **OK** = Authentication successful **AUTHENTICATION_ERROR** = Authentication unsuccessful. (invalid username and/or password and/or OTP or the user account is locked and authentication requests cannot be processed, but masking the actual error details. Please refer to the Lockout Mechanism in the Web API section below.)
Class	String	The class (or the configured return attribute) for returning user's group membership information

RESPONSE FORMAT WHEN **grasapi_show_error_details** is set to true

t=2020-05-15T09: 09: 57Z0407
status=ACCOUNT_LOCKEDOUT
code=503
message=Service Unavailable

Parameter	Type	Description
T	String	Response time
Status	String	The status of authentication request: **OK** = Authentication successful **REPLAYED_OTP** = OTP has already been used **INVALID_OTP** = The OTP/Temporary Token is invalid **AUTHENTICATION_ERROR** = Authentication unsuccessful. (invalid username and/or password and/or OTP) **ACCOUNT_LOCKEDOUT** =User account is locked and authentication request cannot be processed. Please refer to the **Lockout Mechanism in the Web API** section below. **MISSING_PARAMETER** - When username or password is missing
code	String	Code corresponding to the error **503: Service Unavailable**
message	String	The message describing the error
Class	String	The class (or the configured return attribute) for returning user's group membership information

Note: The "code" and "message" parameters are returned only in case of "ACCOUNT_LOCKEDOUT" status.

USERNAME AND PASSWORD VALIDATION

- Determines if OTP is appended to username or password and accordingly extracts the values of the username and password 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	• Checks if the token is blocked • Validates OTP with configured validation server(s) (YubiCloud or internal validation server in GreenRADIUS) • Checks if the token is assigned to the user ○ If not, and if the auto-provisioning feature is enabled in GreenRADIUS, the token is automatically assigned to the user if the authentication is successful (including username and password validation) • If OTP validation is successful, the system switches to 2FA mode for the user if single factor or Temporary Token is enabled prior to authentication

Temporary Token	• Checks if the max use of the Temporary Token has been reached • Checks if the Temporary Token is expired (time expiration) • Validates Temporary Token
OATH-HOTP and OATH-TOTP	• 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 and FIDO2 WebAuthN	• Checks if the token is assigned to the user • Validates the token

WEB API FOR 2FA USING FIDO2 YUBIKEY (COMING SOON)

GreenRADIUS 2FA using FIDO2 tokens involves the use of the following API twice during processing of one authentication request.

REQUEST FORMAT

https://<<IP address or host name of GreenRADIUS>>/gras-api/v1/authentication/authenticate-fido2?Authentication-Request-ID=NULL&user=<<username>>&password=<<password>>&Application-Session-ID=<<application specified string>>

Parameter	Type	Required	Description
Authentication-Request-ID	String	Optional	For starting a new authentication session, this parameter may not be specified or specified as NULL For all subsequent calls to the API within the same logical authentication session, the calling application shall provide the Authentication-Request-ID returned by the API during the first API call at the start of the new authentication session
User	String	Yes	The username
Password	String	Optional	The password is mandatory at the start for a new authentication request and may not be specified for subsequent calls to the API

Application-Session-ID	String	Optional	The calling application may specify its own session ID which will be logged by GreenRADIUS and returned in the API response
Signed-Response	String	Optional	This parameter is optional and may not be specified for the first call to the API when a new authentication session is started After the first call to the API has returned a FIDO2 challenge and the application has processed the challenge to get a response signed by a FIDO2 YubiKey, the application makes subsequent call to the API and provides the Signed-Response to GreenRADIUS for validation.

RESPONSE FORMAT

t=2020-12-16T14:14:32Z0763
status=OK
Authentication-Request-ID= E665BB2C9CC47ED238EC73D1306E0AFE
Application-Session-ID= 0DB6FD264068AA45FB8171AC53C45122
Challenge={json encoded FIDO2 challenge}

Parameter	Type	Description
t	String	Response time
status	String	The status of authentication request: **OK** = Authentication successful **CHALLENGE-ISSUED** = FIDO2 challenge **AUTHENTICATION_ERROR** = Authentication unsuccessful. (invalid username and/or password and/or OTP) **MISSING_PARAMETER** - When username or password is missing
Authentication-Request-ID	String	For a new authentication session, GreenRADIUS will generate a unique Authentication-Request-ID and return it to the calling application
Application-Session-ID	String	The Application-Session-ID parameter provided by the caller will be returned for use by caller
Challenge	String	Json encoded FIDO2 challenge (if applicable)

USERNAME AND PASSWORD VALIDATION

- For the first call to the API (i.e. when the Authentication-Request-ID is not provided or is NULL), GreenRADIUS validates the username and password

- If the authentication fails, it returns "AUTHENTICATION_ERROR" status
- On successful validation, if a FIDO2 token is assigned to the specified user, GreenRADIUS will generate a challenge and return it in the response

FIDO2 VALIDATION

Token Type	Validation
FIDO U2F and FIDO2 WebAuthN	• Checks if the token is assigned to the user • Validates the token

NOTE

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

LOCKOUT MECHANISM IN WEB API

An attacker could attempt to determine the user password by brute-forcing the user password against the Web API. To deal with this, the lockout mechanism has been introduced in the Web API.
When the lockout mechanism is enabled and when the consecutive failed attempts from a user exceed a certain limit, the rate limiting kicks in and the user account is locked-out for a specified amount of time. Any further attempts for that user are ignored during the lockout period.

DISABLING THE LOCKOUT MECHANISM

The lockout mechanism is **disabled** by default. Setting the value of the **'maximum_allowed_failed_attempts'** setting in **sys_settings** table in the **ykrop2** database to **0** disables the lockout mechanism. The default value of this setting is **0**.

ENABLING THE LOCKOUT MECHANISM

To **enable** the lockout mechanism, set the value of the **'maximum_allowed_failed_attempts'** setting in the **sys_settings** table in **ykrop2** database to any positive integer. This value defines the number of consecutive failed attempts allowed by a user.

The duration for which a user account will remain locked (in seconds) is defined by the setting **'authentication_lockout_duration'** in **sys_settings** table in **ykrop2** database. The default value is **600 seconds**.

Setting	Permitted values	Default value
maximum_allowed_failed_attempts	Any positive integer	0
authentication_lockout_duration (in seconds)	Any positive integer	600

ABBREVIATIONS

- API – Application Programming Interface
- VA – Virtual Appliance
- OATH – Open Authentication
- OTP – One-Time Password
- HOTP – Event based OTP - RFC 4226
- TOTP – Time based OTP – RFC 6238
- HMAC OTP – used in YubiKey OTP (proprietary format)
- AD – Active Directory
- LDAP – Lightweight Directory Access Protocol