Sasa Software Gate Scanner® REST API Integration

May 2020

Changes, Errors and Omissions Expected

REST API Documentation

Documentation provided in “Gate Scanner Rest API Version Documentation.pdf”

Focal points:

Oren Dvoskin, Marketing, orend@sasa-software.com
Michael Baras, Sales Engineer, michaelb@sasa-software.com

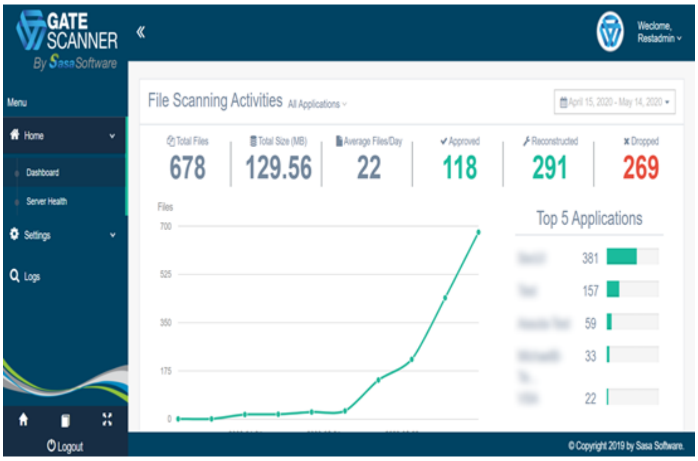
Test Environment

Address for the service: https://api.sasa-software.com/scanner.svc
API Key To Connect: 85ccff8f-68a4-4dfb-81a8-d41109e8fa45
Monitoring environment: https://api.sasa-software.com:8881/
Username: Menlo-User **Password:** Menlo@SasaAPI1!
Please provide us the Public IP addresses which will access the service.

Profile IDs:
We pre-configured several profile IDs for Scan/CDR security policies.
Each profile performs a different action.
2: Multi AV + Multi True Type. No Reconstruction
35: Multi AV + Next Gen AV (Sentinel One). No Reconstruction.
43: Multi AV + Multi True Type + Next Gen AV (Sentinel One) + Single Pass (Soft) Reconstruction.
32: Single pass (Soft) reconstruction. No Detection.
21: Multi pass (Hard) reconstruction. No Detection.

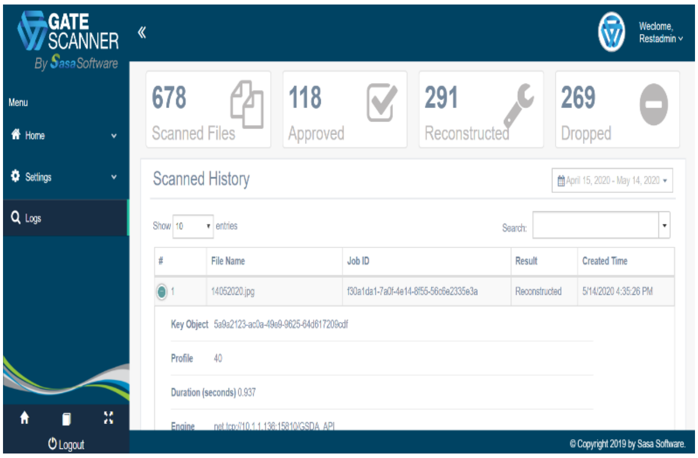
GateScanner REST API admin

Navigate to https://api.sasa-software.com:8881/admin/login.html
Enter username/pass: (Menlo-User/Menlo@SasaAPI1!)
Dashboard shows an overview of the scanning activities.
Server health shows connection status.
Settings: change password.
Logs shows detailed results for every file.



Total Files	Total Size (MB)	Average Files/Day	Approved	Reconstructed	Dropped
678	129.56	22	118	291	269

Top 5 Applications: 381, 157, 59, 33, 22



678 Scanned Files | 118 Approved | 291 Reconstructed | 269 Dropped

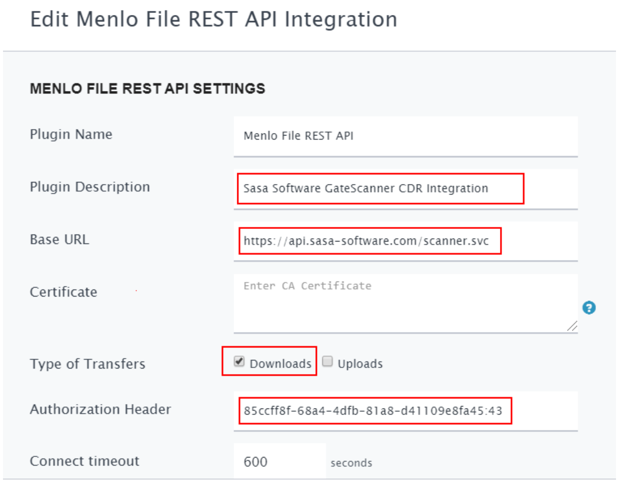
#	File Name	Job ID	Result	Created Time
1	14052020.jpg	f30a1da1-7a0f-4e14-8f55-56c6e2335e3a	Reconstructed	5/14/2020 4:35:26 PM

Key Object 5a9a2123-ac0a-49e9-9625-64d617209cdf
Profile 40
Duration (seconds) 0.937
Engine net.tcp://10.1.1.136:15810/GSDA_API

Menlo Security Admin definitions

Login to the Menlo Security admin:
https://admin.menlosecurity.com/
Navigate to Content Inspection settings.
Configure the Menlo File REST API Integration to connect with GateScanner CDR: Web Policy -> Content Inspection -> Edit "Menlo File REST API Integration"

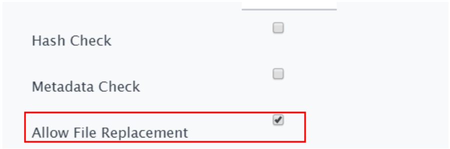
Base URL: https://api.sasa-software.com/scanner.svc
Plugin description: Sasa Software GateScanner CDR
Type of Transfers: downloads (we also support uploads)
Authorization Header: <GateScanner API Key>:<Profile ID>
e.g. 85ccff8f-68a4-4dfb-81a8-d41109e8fa45:43
Allow File Replacement: Yes



Edit Menlo File REST API Integration

MENLO FILE REST API SETTINGS

Plugin Name: Menlo File REST API
Plugin Description: Sasa Software GateScanner CDR Integration
Base URL: https://api.sasa-software.com/scanner.svc
Certificate: Enter CA Certificate
Type of Transfers: ☑ Downloads □ Uploads
Authorization Header: 85ccff8f-68a4-4dfb-81a8-d41109e8fa45:43
Connect timeout: 600 seconds

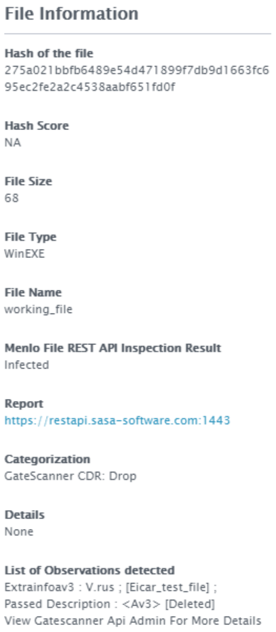


Hash Check □
Metadata Check □
Allow File Replacement ☑

File Security logs

Navigate logs and search for "File Request", scroll down to "File Information"
Malicious/blocked files will contain scanning results
Reconstructed files will contain information on the disarm operation.

Blocked file



File Information

Hash of the file
275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

Hash Score
NA

File Size
68

File Type
WinEXE

File Name
working_file

Menlo File REST API Inspection Result
Infected

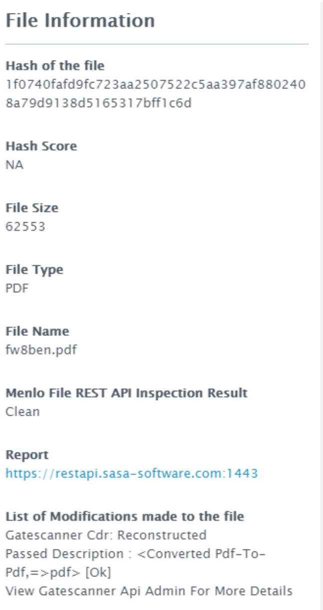
Report
https://restapi.sasa-software.com:1443

Categorization
GateScanner CDR: Drop

Details
None

List of Observations detected
Extrainfoav3 : V.rus ; [Eicar_test_file] ;
Passed Description : <Av3> [Deleted]
View Gatescanner Api Admin For More Details

Reconstructed (disarmed) file



File Information

Hash of the file
1f0740fafd9fc723aa2507522c5aa397af8802408a79d9138d5165317bff1c6d

Hash Score
NA

File Size
62553

File Type
PDF

File Name
fw8ben.pdf

Menlo File REST API Inspection Result
Clean

Report
https://restapi.sasa-software.com:1443

List of Modifications made to the file
Gatescanner Cdr: Reconstructed
Passed Description : <Converted Pdf-To-Pdf,=>pdf> [Ok]
View Gatescanner Api Admin For More Details

REST API Test Application

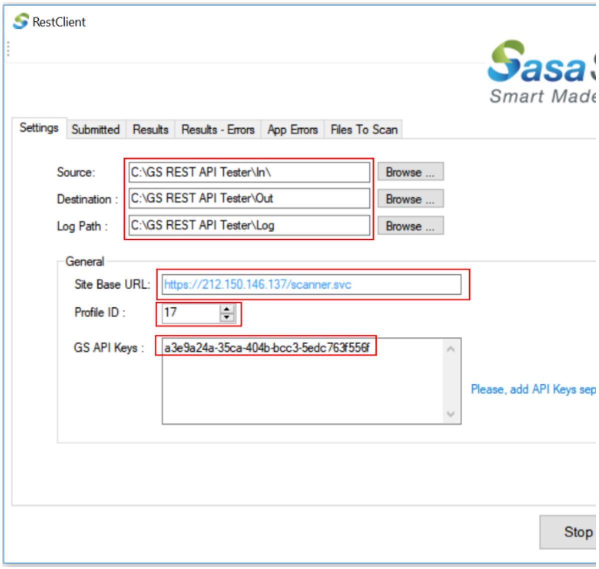
A simple test application is provided to ensure the REST API connection is working.

Send us your IP address to open a firewall port.

- **Install:**
  Download application via secure link.
  Extract “GSRestTester.zip”
  Create directories for: source, destination, log files
  Run “APIClientHttp.exe”

- **Configure:**
  Directories, service URL, profile, API key.
  Save configuration.

- **Profile ID:**
  Select desired scanning profile as described above.



Source: C:\GS REST API Tester\In\
Destination : C:\GS REST API Tester\Out
Log Path : C:\GS REST API Tester\Log

General
Site Base URL: https://212.150.146.137/scanner.svc
Profile ID : 17
GS API Keys : a3e9a24a-35ca-404b-bcc3-5edc763f556f

Please, add API Keys sep

Place desired original files in “source” directory.
Run application and iterate as needed.
All files in the source directory are scanned sequentially (one at a time).
Progress can be viewed in the different tabs (submitted, results, etc).
Upon completion, a “scan ended” popup will appear.
Resulting files will be placed in uniquely identified directories.
Files converted to a different format might have multiple suffixes (e.g. .doc.docx)
A single log file is created.

Supported file types

The general concept

Deep threat scans: Can be performed for any file type that can be processed by commercial AVs. & NGAV.
Content disarm: Can be performed for productivity documents (MS-Office, PDF, Emails, Media files), and files that can be restructured, including custom/proprietary files (e.g. DICOM). Every file type has unique operations for disarm/restructuring, including multiple target/intermediate file types.

Supported file types

Every file-type supports multiple options and intermediate formats defined by a scanning policy.
Full list of supported file-type and options is available in the Gate Scanner® manual and management application.

		Deep Threat Scans		Content Disarm		
File Type	**File policy check**	**Multi True Type Scan**	**Multi AV scans**	**Active Content Neutralization**	**File Restructuring**	**Comments**
Text based	✓	✓	✓	✓	✓	Available as: “soft” (same format), “hard” (to an intermediate format, editable file), “view only” (to an intermediate format, non- editable, to a PDF containing an image)
MS-Office	✓	✓	✓	✓	✓	
PDF	✓	**+ Digital Signature Verification** (as an option)	✓	✓	✓	
Media files	✓	✓	✓	✓	✓	
Archives Deep scans	✓	✓	✓	✓	✓	Performed according to embedded file type.
Password Protected files	✓	✓	✓	✓	✓	Supports archives, MS-Office, PDF (as an option)
Emails (.eml)	✓	✓	✓	✓	✓	Emails deconstructed according to RFC2822
Medical Imaging Files (DICOM)	✓	✓	✓	**DICOM conformance specific restructuring**		Full deconstruction of DICOM: metadata and pixel data.
Custom files (e.g. AutoCAD files)	✓	✓	✓	**As supported by the file type**		Custom files can be defined and added to GS CDR upon request (requires implementation)
Executable/Binary files (.exe, .dll, .bin, etc)	✓	✓	✓	-		-
Other files types	✓	✓	✓	-		-
External Scans	External scanning solutions (e.g. Sandboxes) can be optionally integrated for supported files					

– Sasa Software Confidential –
Changes, Errors and Omissions Expected