



ReSec and Menlo Integration Guide

About this Guide

This guide will walk you through the steps required in order to integrate ReSec's CDR solution into Menlo's safe browsing solution.

Integration Overview

During the integration you will need to perform the following steps:

1. Configure your ReSec system to accept requests from your Menlo instance.
2. Configure Menlo to sanitize downloaded files using the ReSec system.
3. Verify your installation.

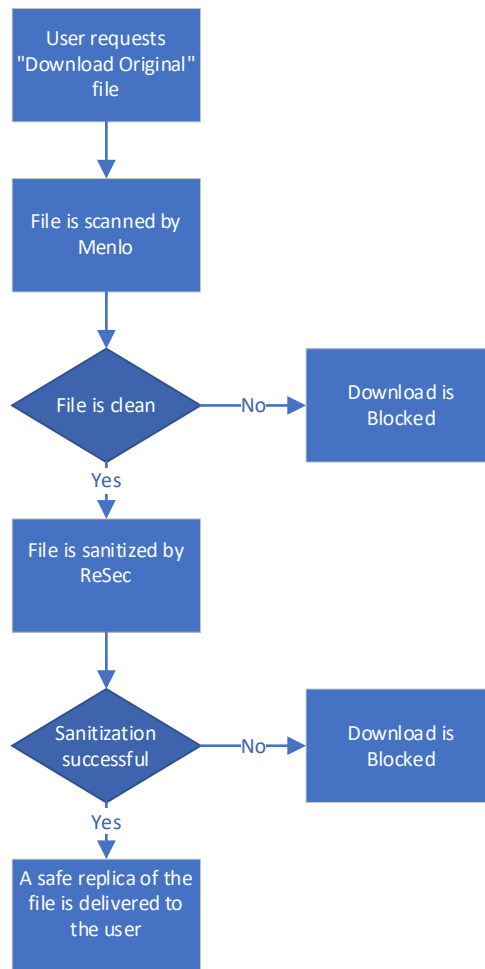
Installation Prerequisites

Before starting, please make sure that your Menlo system and your ReSec system is both up and running.

Setup Procedure

(a) Dataflow / Workflow

When the end-user downloads a file, it will go through the following flow:

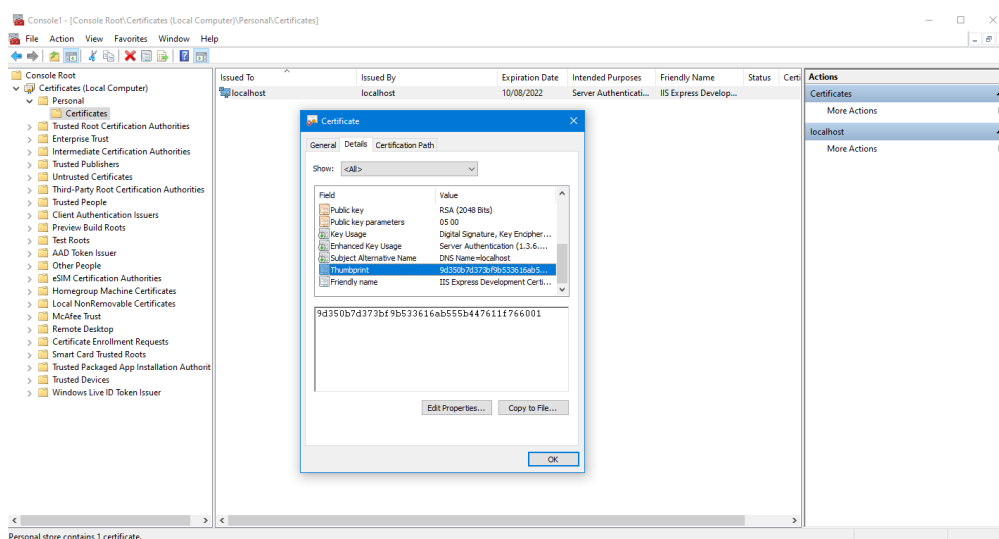


(b) Partner Configuration

Please note that installing or making modifications to ReSec’s server requires assistance from professional system integrators that have been certified by ReSec.

In order to allow ReSec to receive files from Menlo, please follow the following steps:

1. Make sure there is a valid SSL certificate on ReSec’s machine and bind it to the ReSec’s WebAPI port (8443).
 - a. Obtain a server certificate from any trusted certificate authority (E.G [Thawte](#), [Verisign](#), and [Let's Encrypt](#)).
 - b. Find the certificate’s hash / thumbprint:
 - Open *MMC* and add the *Certificates* snap-in



- Find the newly added certificate and double-click it
 - Navigate to the *Details* tab
 - Copy the value of the *Thumbprint* field
- c. Open a CMD windows as admin and execute the following command:

```
netsh http add sslcert ipport=0.0.0.0:8443 certhash={certificate's thumbprint}
appid={26f1c54d-740b-480d-aff1-8fcacbbcbace}
```

For example:

The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The text in the window reads:

```

Microsoft Windows [Version 10.0.18363.778]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netsh http add sslcert ipport=0.0.0.0:8443 certhash=9d350b7d373bf9b533616ab555b447611f766001appid={26f1c54d-740b-480d-aff1-8fcacbbcbace}
  
```

- Ask the system integrator to generate a WebAPI key and assign it to the web API (in the RezoneWebApi.exe.config file)

```

</ReZoneWebApi.Properties.Settings>
</userSettings>
<applicationSettings>
  <ReZoneWebApi.Properties.Settings>
    <setting name="AutoStartTimeout" serializeAs="String">
      <value>100</value>
    </setting>
    <setting name="AutoStart" serializeAs="String">
      <value>False</value>
    </setting>
    <setting name="WebApiPort" serializeAs="String">
      <value>8000</value>
    </setting>
    <setting name="WebApiSecuredPort" serializeAs="String">
      <value>8443</value>
    </setting>
    <setting name="AuthorizationToken" serializeAs="String">
      <value>[REDACTED] </value>
    </setting>
  </ReZoneWebApi.Properties.Settings>
  
```

(c) MSIP Configuration

1. Enable Menlo File REST API Server Integration:

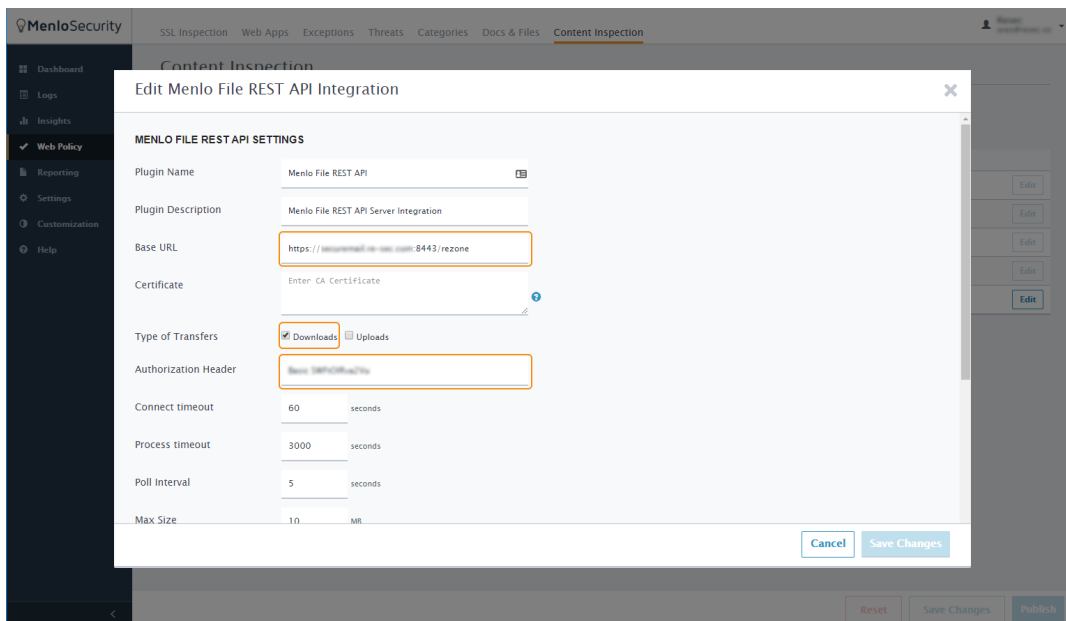
- Navigate to the *Web Policy* -> *Content Inspection* section
- Check the *Enabled* checkbox
- Press the *Edit* button

The screenshot displays the MenloSecurity interface for configuring Content Inspection. The left sidebar shows the navigation menu with 'Web Policy' selected. The main content area is titled 'Content Inspection' and features a search bar and a table of services. The 'Menlo File REST API' service is highlighted, showing it is enabled and has an 'Edit' button next to it.

Service Name	Description	Enabled	Action
File Hash Check	Multi-Engine Hash Check for Virus	<input type="checkbox"/>	Edit
Full File Scan	Anti-Virus Scan	<input type="checkbox"/>	Edit
SandBox Inspection	Cloud-Based SandBox Inspection	<input type="checkbox"/>	Edit
WildFire Analysis	WildFire Malware Analysis	<input type="checkbox"/>	Edit
Menlo File REST API	Menlo File REST API Server Integration	<input checked="" type="checkbox"/>	Edit

2. Configure Menlo File REST API Settings:

- Fill the *Base URL* according to the URL obtained from the ReSec server. E.G
`https://MyReSecServer.com:8443/Rezone`
- *Type of Transfer* should be set to *Downloads*
- *Authorization Header* should be set according to the value that was provided by ReSec's system integrator.



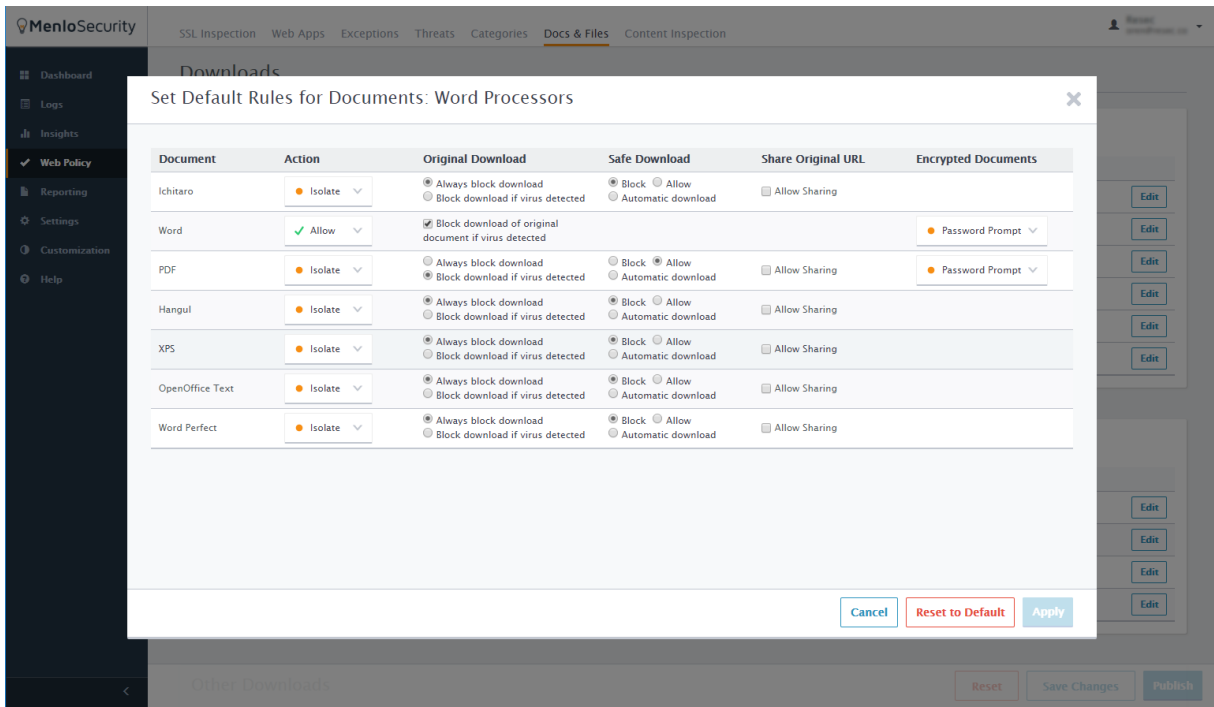
3. Navigate to *Web Policy* -> *Docs & Files* -> *Downloads* -> *Document Rules* and press *Edit*

The screenshot displays the MenloSecurity web interface. The top navigation bar includes 'SSL Inspection', 'Web Apps', 'Exceptions', 'Threats', 'Categories', 'Docs & Files', and 'Content Inspection'. The left sidebar shows a menu with 'Web Policy' selected. The main content area is titled 'Downloads' and contains two sections: 'Document Rules' and 'File Rules'. The 'Document Rules' section has a 'Set Default Rules' button and a table with columns 'Document', 'Action', and 'Rules'. The 'File Rules' section also has a 'Set Default Rules' button and a table with columns 'File Type', 'Action (Isolated / Non-Isolated)', and 'Rules'. At the bottom right, there are 'Reset', 'Save Changes', and 'Publish' buttons. The URL at the bottom is 'https://admin.menlosecurity.com/#/policy/contents'.

Document	Action	Rules	
Engineering Applications	Isolate	Default	Edit
Other Documents	Isolate	Default	Edit
Presentation Tools	Detailed	Custom	Edit
Productivity	Isolate	Default	Edit
Spreadsheets	Isolate	Default	Edit
Word Processors	Detailed	Custom	Edit

File Type	Action (Isolated / Non-Isolated)	Rules	
Archives and Compressed Packages	Allow / Allow	Default	Edit
Calendar	Allow / Allow	Default	Edit
Multimedia	Allow / Allow	Default	Edit
Scripts and Executables	Allow / Allow	Default	Edit

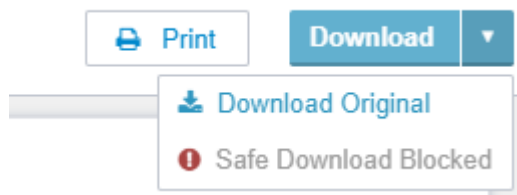
4. Edit the rules for every file that you want to pass through ReSec



There are two options for passing the file through ReSec:

- (1) Allow – this automatically passes the downloaded file through the ReSec sanitization process before downloading the file.
- (2) Isolate – this option creates a flat (PDF) preview of the file before letting the user download the file.

In both cases, when the user selects the *Download Original* option, they will receive a sanitized version of the document after it was processed by ReSec.



(d) Verifying the Results

To verify the results please follow the installation steps and download a file.

Navigate to *Logs* and find your file. When you double click it to view the details, you should see that the *Menlo File REST API Inspection Result* contains the value *Clean*.

The screenshot displays the MenloSecurity Web Logs interface. The main area shows a table of logs with columns for Date, User ID, URL, Category, Threat Type, User Agent, Request, and Action. A detailed view of a log entry is shown on the right, highlighting the 'Menlo File REST API Inspection Result' as 'Clean'.

Date	User ID	URL	Cat...	Threat Ty...	Use...	Request...	I	Action
May-19-2020 01:50:39 PM	oren@resec.co	https://doc-08-04-docs.googleu...	Web Ho...		Chrome...	File Request...	LOW	Allow
May-19-2020 01:50:06 PM	oren@resec.co	https://doc-08-04-docs.googleu...	Web Ho...		Chrome...	File Request...	LOW	Isolate
May-19-2020 01:49:31 PM	oren@resec.co	https://drive.google.com/drive/fo...	Persona...		Chrome...	Page Request...	LOW	Isolate
May-19-2020 01:48:59 PM	oren@resec.co	https://doc-14-04-docs.googleu...	Web Ho...		Chrome...	File Request...	LOW	Allow
May-19-2020 01:48:37 PM	oren@resec.co	https://doc-14-04-docs.googleu...	Web Ho...		Chrome...	File Request...	LOW	Isolate
May-19-2020 01:45:59 PM	oren@resec.co	https://doc-14-04-docs.googleu...	Web Ho...		Chrome...	File Request...	LOW	Allow
May-19-2020 01:45:35 PM	oren@resec.co	https://docs.google.com/nonceSi...	Persona...		Chrome...	Page Request...	LOW	Isolate
May-19-2020 01:45:35 PM	oren@resec.co	https://doc-14-04-docs.googleu...	Web Ho...		Chrome...	Page Request...	LOW	Isolate
May-19-2020 01:45:27 PM	oren@resec.co	https://drive.google.com/drive/fo...	Persona...		Chrome...	Page Request...	LOW	Isolate
May-19-2020 01:43:19 PM	oren@resec.co	https://doc-14-04-docs.googleu...	Web Ho...		Chrome...	File Request...	LOW	Allow
May-19-2020 01:43:12 PM	oren@resec.co	https://doc-14-04-docs.googleu...	Web Ho...		Chrome...	File Request...	LOW	Isolate
May-19-2020 01:42:29 PM	oren@resec.co	https://drive.google.com/drive/fo...	Persona...		Chrome...	Page Request...	LOW	Isolate
May-19-2020	oren@resec.co	https://doc-14-04-docs.googleu...	Web Ho...		Chrome...	File Request...	LOW	Isolate

File Information

- Source IP: 89.138.151.130
- Access Mode: Request
- Response Code: 200
- iframe: False
- Protocol: https
- Region: eu-central-1a
- Rule Matched: document_Word
- Hash of the file: 472a806859507a585deec0d870d562f31e041866b65005c4ca885d3415735
- Hash Score: NA
- File Size: 18316
- File Type: Word
- File Name: Word%20with%20VBS.docm
- Menlo File REST API Inspection Result: Clean**