ReSec and Menlo Integration Guide

Tel: +972-73-7373796
info@ReSec.co
www.ReSec.co
2 Hatochen St, North Ind. Zone
Caesarea 3088900 P.O.Box 3137, Israel

RESEC®

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.

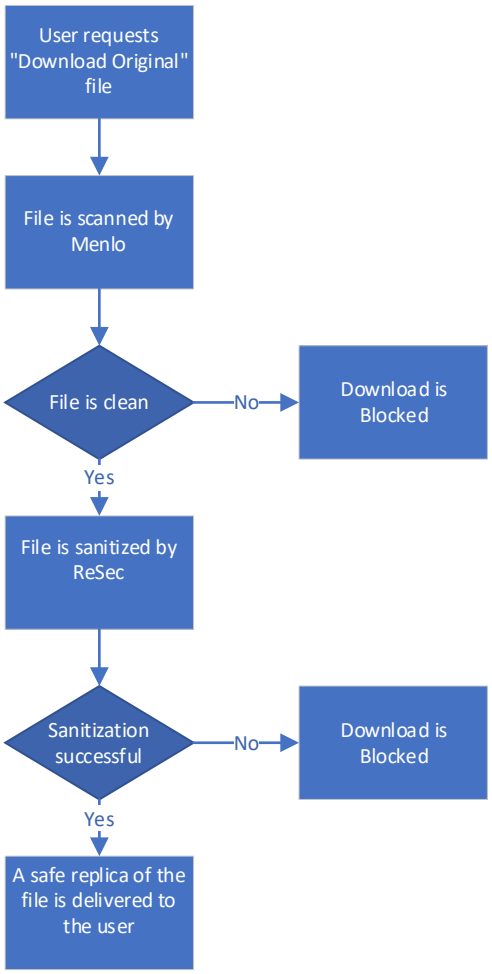
Installation Prerequisites

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:

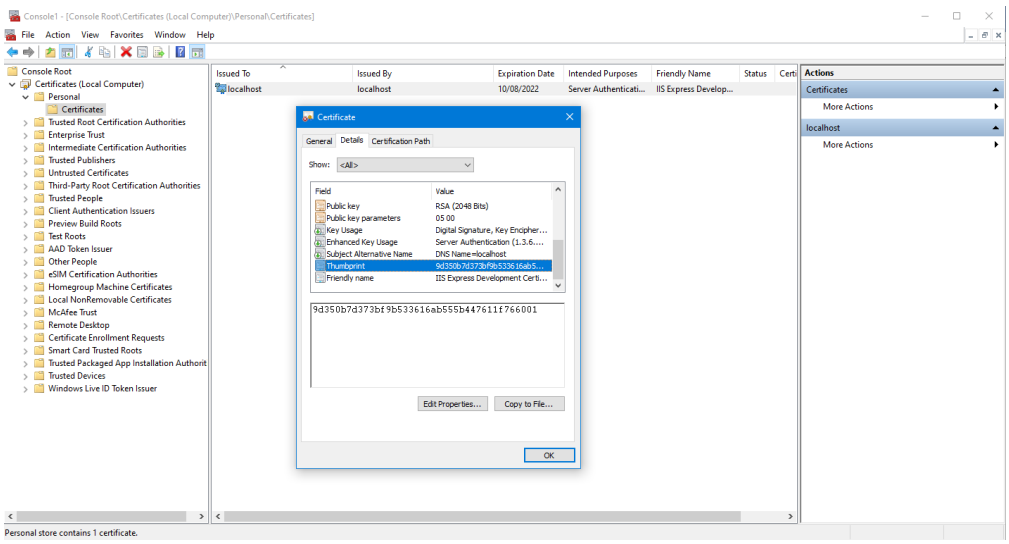


(b) Partner Configuration

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

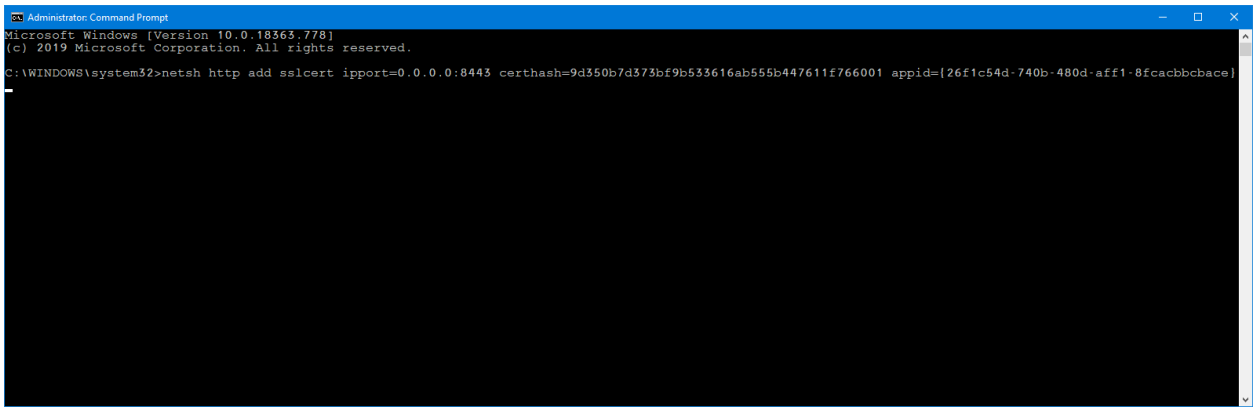


      - Find the newly added certificate and double-click it
      - Navigate to the *Details* tab
      - Copy the value of the *Thumbprint* field

   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:

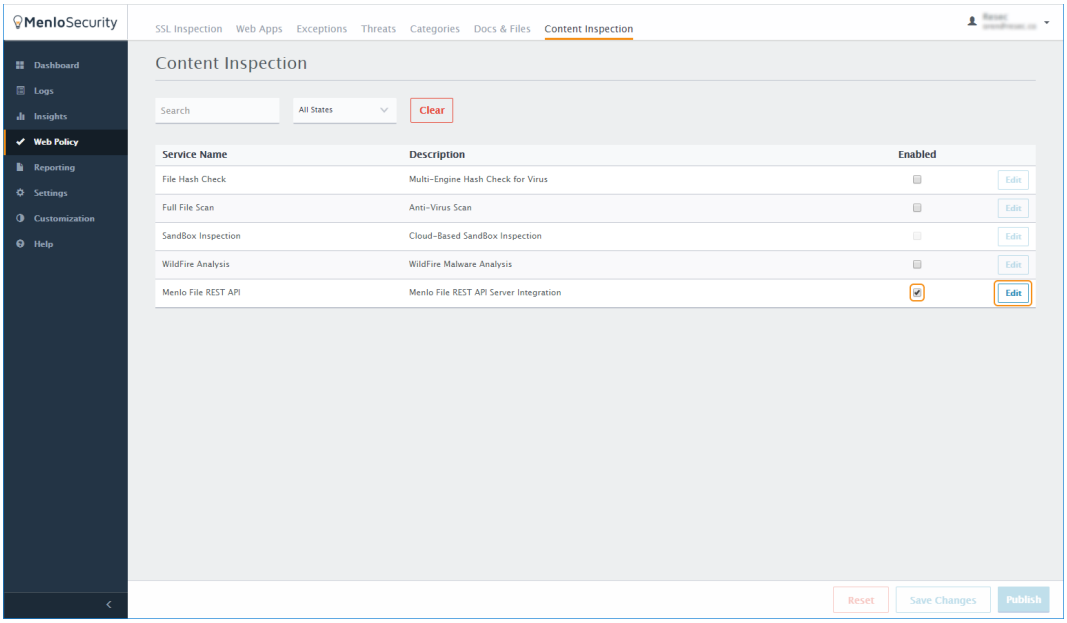


2. Ask the system integrator to generate a WebAPI key and assign it to the web API (in the RezoneWebApi.exe.config file)

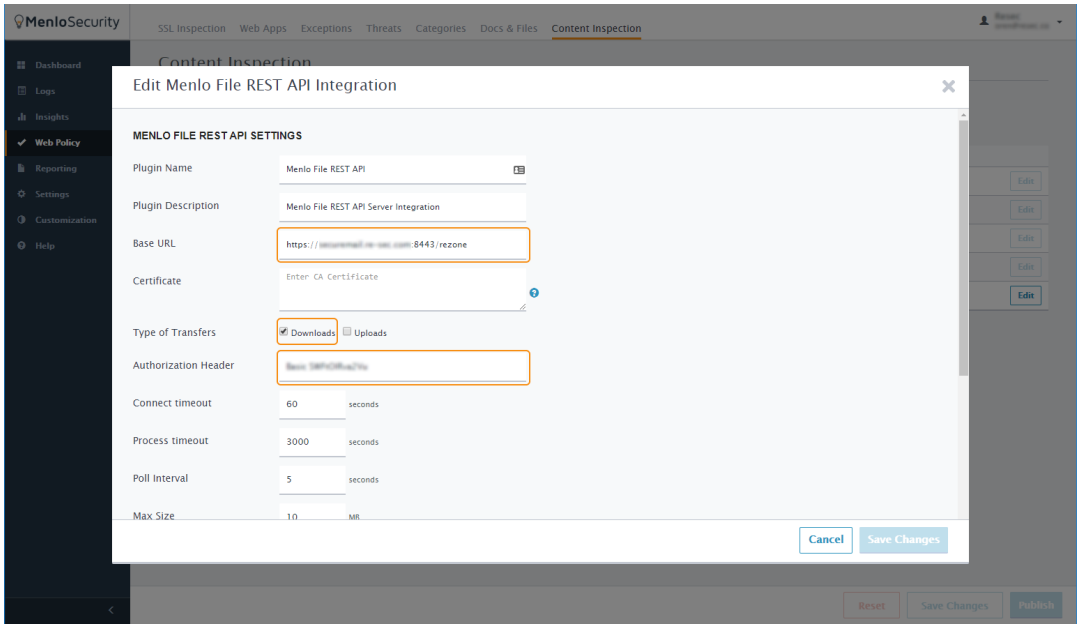
```
</ReZoneWebApi.Properties.Settings>
  </userSettings>
  <applicationSettings>
    <ReZoneWebApi.Properties.Settings>
      <setting name="AutoStartTimeout" serializeAs="String">
        <value>100</value>
      </setting>
      <setting name="AutoStart" serializeAs="String">
        <value>False</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

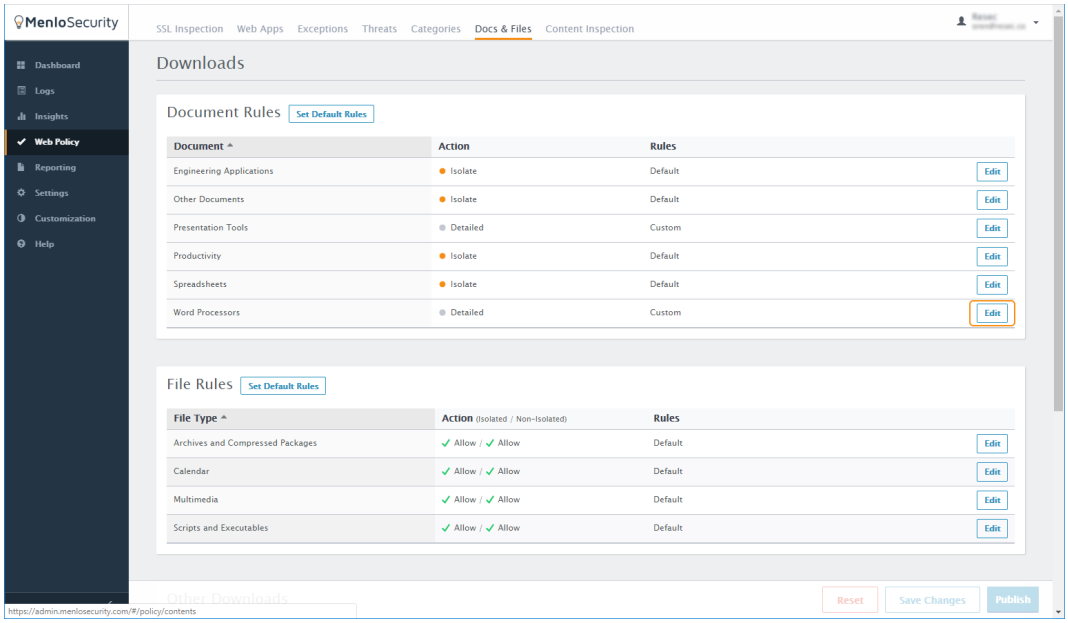
1. Enable *Menlo File REST API Server Integration*:
   - Navigate to the *Web Policy -> Content Inspection* section
   - Check the *Enabled* checkbox
   - Press the *Edit* button



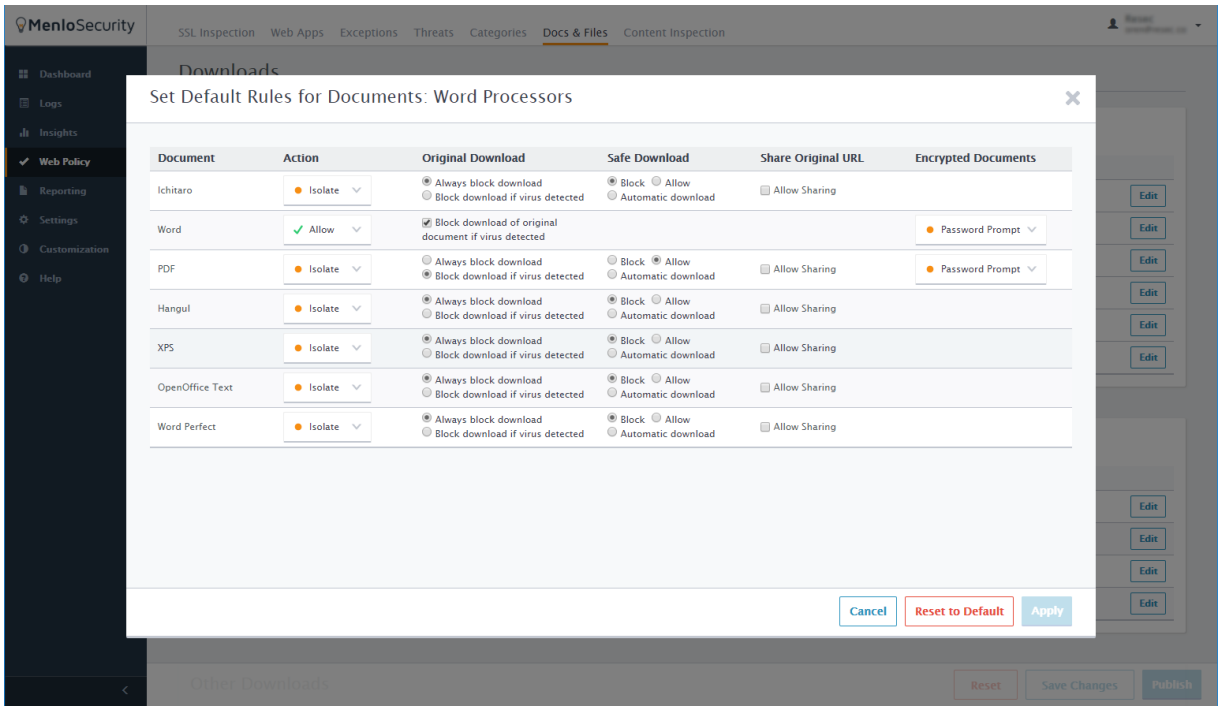
2. Configure *Menlo File REST API Settings*:
   - Fill the *Base URL* according to the URL obtained from the ReSec server. E.G https://MyReSecServer.com:8443/Rezone
   - *Type of Transfer* should be set to *Downloads*
   - *Authorization Header* should be set according to the value that was provided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



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



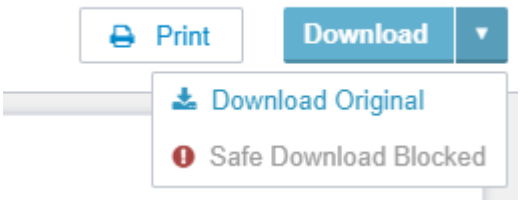
4. Edit the rules for every file that you want to pass through ReSec



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*.