



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

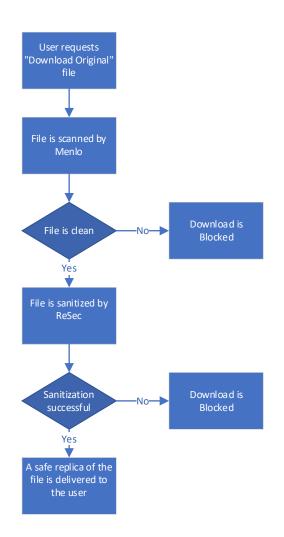
Before starting, please make sure that your Menlo system and your ReSec system is both up and running.



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 <u>Thawte</u>, <u>Verisign</u>, and <u>Let's</u> <u>Encrypt</u>).
 - b. Find the certificate's hash / thumbprint:
 - Open MMC and add the Certificates snap-in

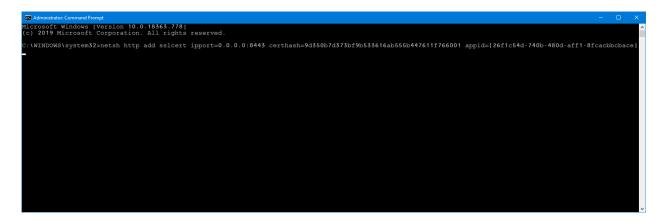
Console Root	Issued To	Issued By	Evni	ation Date	Intended Purposes	Friendly Name	Status	Certi	Actions	
 Q Certificates (Local Computer) 	localhost	localhost		3/2022	Server Authenticati	IIS Express Develop	010103	cere	Certificates	
 Personal Certificates 									More Actions	-
Certificates Trusted Root Certification Authorities		6 Certificate			×					
> 🧰 Enterprise Trust		General Details Certification Pat	-						localhost	•
> intermediate Certification Authorities		General octors cerunication Pat							More Actions	,
Comparison of the second		Show: <all></all>	\sim							
> Third-Party Root Certification Authorities		Field	Value	^						
> 📫 Trusted People		Public key	RSA (2048 Bits)							
> Client Authentication Issuers > Preview Build Roots		Public key parameters	05 00							
> Test Roots		Key Usage	Digital Signature, Key E							
> 🔛 AAD Token Issuer		Enhanced Key Usage Subject Alternative Name	Server Authentication (DNS Name=localhost	1.3.6						
> 🧰 Other People		Thumbprint	9d350b7d373bf9b5336	16ab5						
> I eSIM Certification Authorities > I Homegroup Machine Certificates		Friendly name	IIS Express Developme	nt Certi						
> Local NonRemovable Certificates										
> 🧾 McAfee Trust		9d350b7d373bf9b53361	6ab555b447611f76	6001						
> Remote Desktop Certificate Enrollment Requests										
Smart Card Trusted Roots										
> Trusted Packaged App Installation Authorit										
> Trusted Devices										
> 📔 Windows Live ID Token Issuer										
		E	dit Properties Co	by to File						
				ОК						
		L								
									1	

- 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>
<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>

<value> </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

⊘Menlo Security	SSL Inspection Web Apps Exceptions Threat	s Categories Docs & Files Content Inspection		L Brack -
Dashboard	Content Inspection			
🗈 Logs	Search All States V	Clear		
✓ Web Policy				
Reporting	Service Name	Description Multi-Engine Hash Check for Virus	Enabled	
Settings	Full File Scan	Anti-Virus Scan		
Customization	SandBox Inspection	Cloud-Based SandBox Inspection		
⊖ Help	WildFire Analysis	WildFire Malware Analysis		
	Menlo File REST API	Menlo File REST API Server Integration		Edit
<			Reset Save Char	nges Publish



- 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.

Menlo Security	y SSL Inspection Web Ap	ps Exceptions Threats Categories Docs & Files Content Inspection	L familian -
Dashboard Logs	Content Inspe Edit Menlo File RES		
ılı Insights ✔ Web Policy	MENLO FILE RESTAPI SET	INGS	Î
Reporting	Plugin Name	Menio File REST API	Edit
Customization	Plugin Description	Menlo File REST API Server Integration	Edit
⊖ Help	Base URL	https:// 8443/rezone	Edit
	Certificate	Enter CA Certificate	Edit
	Type of Transfers	Cownloads 🗐 Uploads	
	Authorization Header	Been (MPCH w/Ve	
	Connect timeout	60 seconds	
	Process timeout	3000 seconds	
	Poll Interval	5 seconds	
	Max Size	10 MR Cancel Save Changes	
		Lunci and Simple	
<			



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

Dashboard	Downloads			
Logs				
Insights	Document Rules Set Default Rules			
Web Policy	Document *	Action	Rules	
Reporting	Engineering Applications	Isolate	Default	Edit
Settings	Other Documents	Isolate	Default	Edit
Customization	Presentation Tools	Detailed	Custom	Edit
Help	Productivity	Isolate	Default	Edit
	Spreadsheets	Isolate	Default	Edit
	Word Processors	Detailed	Custom	Edit
	File Rules Set Default Rules			
	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

Set Default	Rules for Docum	ents: Word Processors				×
Set Default	Rules for Docum	ents. word Frocessors				<u> </u>
Document	Action	Original Download	Safe Download	Share Original URL	Encrypted Documents	
Ichitaro	● Isolate 🗸	Always block download Block download if virus detected	 Block Allow Automatic download 	Allow Sharing		
Word	🗸 Allow 🗸	Block download of original document if virus detected			● Password Prompt ∨	
PDF	● Isolate 🗸	 Always block download Block download if virus detected 	 Block Allow Automatic download 	Allow Sharing	● Password Prompt ∨	
Hangul	● Isolate 🗸	 Always block download Block download if virus detected 	 Block Allow Automatic download 	Allow Sharing		
XPS	🗧 İsolate 🗸 🗸	Always block download Block download if virus detected	 Block Allow Automatic download 	Allow Sharing		
OpenOffice Text	● Isolate 🗸	Always block download Block download if virus detected	 Block Allow Automatic download 	Allow Sharing		
Word Perfect	😑 Isolate 🗸 🗸	 Always block download Block download if virus detected 	 Block Allow Automatic download 	Allow Sharing		
				Cance	Reset to Default Ap	ply

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*.

MenloSecurity	Web Logs	Audit Logs										±	85 17-11-10
Dashboard	Show logs for	All Logs Web Logs	Application Logs								i 🗅 Source IP		
Logs											89.138.151.	130	
Insights											Access Mod Prepend	1	
Web Policy	All groups	○ Last week ∨	Luser ID O Do	main	🧳 Catego	ny Y	A Threat Type	ė			Response Co	ode	
Reporting	All Risk Levels	✓ All Requests ✓	O All Prot ∨ O Us	er Agent⁄	 All Actio 		Filter Clear	7			200		
Settings								_			iframe False		
Customization	Date *	User ID	URL	Cat	Threat Ty	Use	Request	1	Action		Protocol		
Help	May-19-2020 01:50:39 PM	oren@resec.co	https://doc-08-04-docs.googleu	Web Ho		Chrome	. File Request	LOW	Allow	Ø	https Region		
	May-19-2020 01:50:06 PM	oren@resec.co	https://doc-08-04-docs.googleu	Web Ho		Chrome	File Request	LOW	Isolate	Ø	eu-central-1	a	
	May-19-2020 01:49:31 PM	oren@resec.co	https://drive.google.com/drive/fo	. Persona		Chrome.	. Page Request	LOW	Isolate	œ	Rule Matche document_W		
	May-19-2020 01:48:59 PM	oren@resec.co	https://doc-14-04-docs.googleu	Web Ho		Chrome.	File Request	LOW	Allow	œ	File Info	mation	
	May-19-2020 01:48:37 PM	oren@resec.co	https://doc-14-04-docs.googleu	Web Ho		Chrome.	. File Request	LOW	Isolate	ß		580fad585deec60d870	d562f31e04
	May-19-2020 01:45:59 PM	oren@resec.co	https://doc-14-04-docs.googleu	Web Ho		Chrome.	. File Request	LOW	Allow	Ø	186fb65005 Hash Score	:4caa85d3415735	
	May-19-2020 01:45:35 PM	oren@resec.co	https://docs.google.com/nonceSi	Persona		Chrome.	Page Request	LOW	Isolate	Ø	NA		
	May-19-2020 01:45:35 PM	oren@resec.co	https://doc-14-04-docs.googleu	Web Ho		Chrome.	Page Request	LOW	Isolate	Ø	File Size 18316		
	May-19-2020 01:45:27 PM	oren@resec.co	https://drive.google.com/drive/fo	. Persona		Chrome	Page Request	LOW	Isolate	8	File Type Word		
	May-19-2020 01:43:19 PM	oren@resec.co	https://doc-14-04-docs.googleu	Web Ho		Chrome.	. File Request	LOW	Allow	R	File Name Word%20with	%20VBS.docm	
	May-19-2020 01:43:12 PM	oren@resec.co	https://doc-14-04-docs.googleu	Web Ho		Chrome.	. File Request	LOW	Isolate	Ø	Menio File R	EST API Inspection Res	ult
	May-19-2020 01:42:29 PM	oren@resec.co	https://drive.google.com/drive/fo	. Persona		Chrome.	. Page Request	LOW	Isolate	8	Ciedii		_
<	May-19-2020									-		Edit Policy	