# RSA Ready Implementation Guide for RSA Contract RSA Ready Implementation Guide for

# **OPSWAT Metascan 3.10**

Peter Waranowski, RSA Partner Engineering Last Modified: 03/09/2016





# **Solution Summary**

RSA ECAT integrates with OPSWAT Metascan via Metascan's REST API service. This integration allows ECAT administrators to analyze modules with multiple anti-malware engines from a context menu within the ECAT UI. The results of the analysis can be viewed on the OPSWAT Verdict in the properties of a selected module. The time of the last analysis performed on the module will be shown in the Analysis Time field, also found in the properties of the module.





# **Partner Product Configuration**

## Before You Begin

This section provides instructions for configuring OPSWAT Metascan with RSA ECAT. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All RSA ECAT components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

## **OPSWAT Metascan Configuration**

#### Install OPSWAT Metascan

Metascan can be installed on the same machine where ECAT ConsoleServer is running, or on another

server on the LAN. It is recommended, however, to install it on the same machine, if possible.

1. Obtain the Metascan installation executable from:

https://portal.opswat.com/user/register

- 2. Double-click the .exe file to run the installation wizard.
- 3. Click Next.





- 4. The End-User License Agreement dialog is displayed. Read the agreement fully, and check I accept the terms in the License Agreement if you agree.
- 5. Click **Next**.Change the settings here if you wish, or leave it at the default settings and click **Next**.

岁 Metascan 1 3.10.1.	Metascan 1 3.10.1.27456 Setup 📃 💻 🗙									
Custom Setup Select the way you want features to be installed	OPSVAT.									
Click the icons in the tree below to change the way features will be installed.										
RAM Drive Metascan Client	Main components of Metascan 1									
Metadefender Email Age Engines ICAP Server Documentation	This feature requires 714MB on your hard drive. It has 5 of 6 subfeatures selected. The subfeatures require 333MB on your									
Location: C:\Program Files (x86)\OPSWAT\Metascan 1\ Browse										
Reset Disk Usage	Back Next Cancel									

6. Click **Install**. Wait until the Completed the Metascan... dialog is displayed.





7. Click **Finish**.



8. Set the Metascan, Metascan Helper, Metascan Quarantine and Metascan REST services to Automatic startup type. Start the services if they are not already started.

#### **Configure ECAT ConsoleServer**

ECAT ConsoleServer can integrate with Metascan installed either locally or on a remote system. If Metascan is running on a remote system, ensure that the REST API service is installed and running on that system.

#### To integrate with Metascan installed locally:

Edit the ConsoleServer config file to add the following line:

```
<add key="AntiVirusConfiguration" value="(local)" />
```

Important: Do not forget to start the service. ConsoleServer will not start if it is configured to work with Metascan locally, but Metascan itself is not started.

#### To integrate with Metascan installed remotely:

Edit the ConsoleServer config file to add the following line:

<add key="AntiVirusConfiguration" value="http://{hostname}:8008" />



# **RSA ECAT Configuration**

### RSA ECAT UI Screens

Scan with context menu:

🕅 RSA ECAT											
Configure Tool:	s View Abou	ut									
Main Menu 🛛 🕮	🌔 Dashboa	ard 🛃	뒤 Modules 🗙	😨 Download	Files 🗗	deploy.jar	🗥 Instant	:IOCs 🕹 Machines	💻 VM2181		
<b>^</b>	Windows	Mac OS X									
	Drag a colum										
	File Name		IIOC Score 🔻	Risk Score	Machine C	Signature	Size In Bytes	Description	Hash Look	Compile Ti	First Seen
	eicar.com	E at	100 - 100 - 100	1.0.1	1 1	Not Signed	68 bytes		Unknown		2/8/2016 3:
Dashboard	svchost.exe	Eul	t Blacklist-writeli	Modula	0 1	Valid: Micr	26.5 kB	Host Process for Windows Se	Unknown	7/13/2009 7	2/8/2016 10.
	lsass.exe	Sau	e Local Conv	Module	0 1	Valid: Micr	30.5 kB	Local Security Authority Proce	. Unknown	9/15/2015 1	2/8/2016 10.
	EcatServiceDr	rvi Sca	an with OPSWAT		0 1	Signed: [Ce	188.4 kB		Unknown	12/17/2015	2/8/2016 10.
Machines	spoolsv.exe	An	alyze Module	L.S.	0 1	Valid: Micr	546.0 kB	Spooler SubSystem App	Unknown	2/11/2012 1	2/8/2016 10.
	MsMpEng.ex	<sup>ce</sup> Ma	lware Analysis	-	0 1	Valid: Micr	21.6 kB	Antimalware Service Executable	Unknown	9/13/2012 1	2/8/2016 10.
C'	spsys.sys	Sea	arch with Google	•	0 1	Valid: Micr	416.5 kB	security processor	Unknown	5/11/2009 1	2/8/2016 10.
Modules	tintsvr.exe	Sea	arch with VirusTot	alSearch 🕨	0 1	Valid: Micr	80.0 kB	Teinet	Unknown	7/13/20098	2/8/2016 10.
m	dumpfve.sys	Op	en in a Separate V	iew	0 1	Valid: Micr	53.8 kB	Bitlocker Drive Encryption Cr	Unknown	7/13/2009 7	2/8/2016 10.
Ŭ	mcupdate_G	en Vie	w Certificate		0 1	Valid: Micr	481.9 kB	Intel Microcode Update Library	Unknown	5/9/2015 2:	2/8/2016 10.
IP List	EcatService.e:	xe Co	ру	Ctrl+C	0 1	Valid: RSA	1.21 MB		Unknown	12/17/2015	2/8/2016 10.
ii tist	ntoskrnl.exe		5		0 1	Valid: Micr	5.31 MB	NT Kernel & System	Unknown	9/28/2015 9	2/8/2016 10.

Verdict in Module Properties

🕅 RSA ECAT								- B >
Configure Tool	s View About							Ju -
Main Menu 🛛 🕸	🌔 Dashboard 🛛 🗗 ।	Modules 🗙 🔇 Downlo	ad Files	🗗 deploy.jar	🗥 Instant	:10Cs 🕹 M	achines 💻 VM2181	
Windows Mac OSX								
	Drag a column header here	to group by that column			Properties 😐 🖉			
	File Name	IIOC Score 🔻 Risk Score	Machine	C Signature	Size In Bytes	Description	Summary	All
	eicar.com	129	1 1	Not Signed	68 bytes		File.Status	· · · · ·
Dashboard							Blacklist Category	•
	svchost.exe	13	0 1	Valid: Micr	26.5 KB	Host Process for	Blocking Status	Unknown
	Isass.exe	12	0 1	Valid: Micr	30.5 kB	Local Security Au	Downloaded	True
	EcstSanriceDriver11009 cur	<b>1</b> 0	0 1	Signed: ICe	199 / kB		liOC Level 1	1
- T	conserviceonverniceositys	0	0 1	Signed, (ce.	. 100.4 kB		IIOC Level 2	1
Machines	spoolsv.exe	- 10	0 1	Valid: Micr	546.0 kB	Spooler SubSyste	IIOC Score	129
	MsMpEng.exe	9	0 1	Valid: Micr	21.6 kB	Antimalware Sen	Risk Score	1
ل ف							Status	Neutral
	spsys.sys	8	0 1	Valid: Micr	416.5 kB	security processo	Reputation	
Modules	tintsvr.exe	8	0 1	Valid: Micr	80.0 kB	Teinet	Analysis Time	2/8/2016 3:21:18 PM
	dumphia our	<b>e</b>	0 1	Valid: Micr	53.9 kB	Bitlocker Drive Fr	AV Definition Hash	13099381200000000
[min]	adinprocisiya	• •	0 1	edito, Micha	55.0 KD	Didocker Drive Er	AV Description	Found Infected on 2/8/2016 by: ClamAV s
	mcupdate_GenuineIntel.dll	8	0 1	Valid: Micr	481.9 kB	Intel Microcode I	AV First Threat	Eicar-Test-Signature
-	EcatSeptice.exe	6	0 1	Valid: RSA	1.21 MB		AV Scan Result	Infected
IP List							AV Version	1
	ntoskml.exe	5	0 1	Valid: Micr	5.31 MB	NT Kernel & Syste	Cert. Bias Status	Undefined
	vpnagent.exe	<u> </u>	0 1	Valid: Cisco.	595.4 kB	VPN Agent Servio	Company Name Count	33
							File Name Courte	