

RSA Ready Implementation Guide for RSA | ECAT

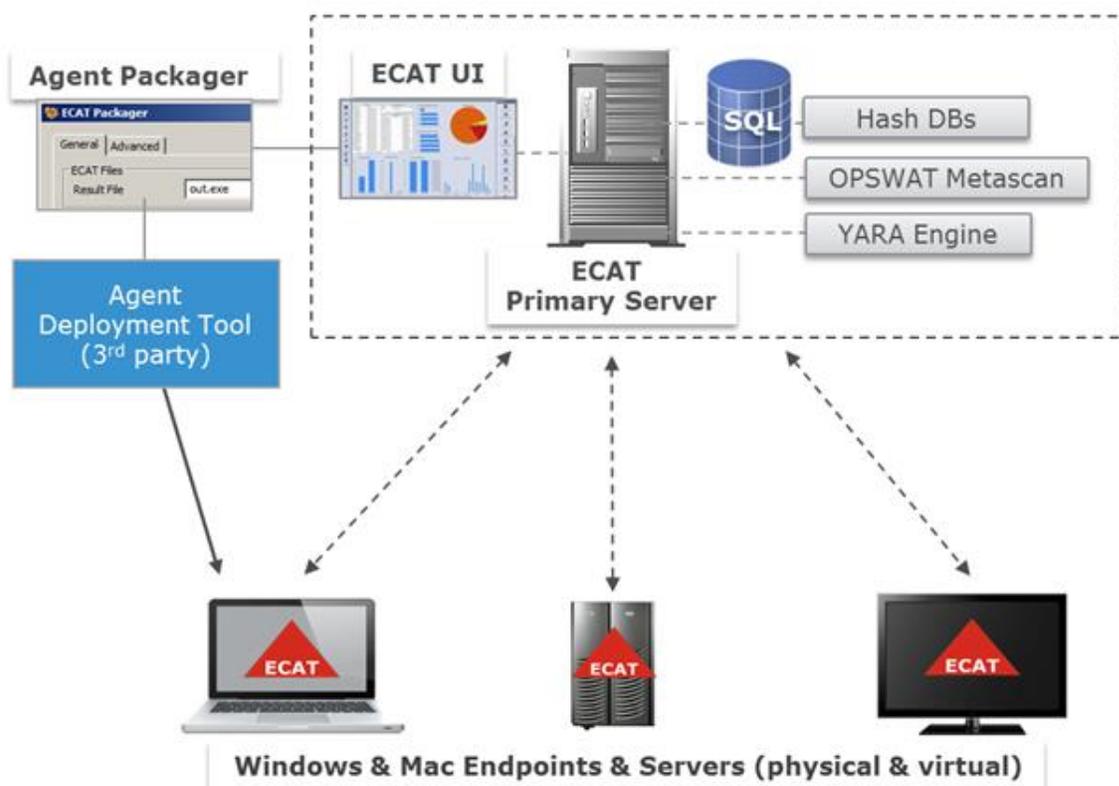
OPSWAT Metascan 3.10

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.

RSA ECAT Supported Features	
OPSWAT Metascan 3.10	
Analyze Module	Yes
Display Verdict in Module Properties	Yes



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.

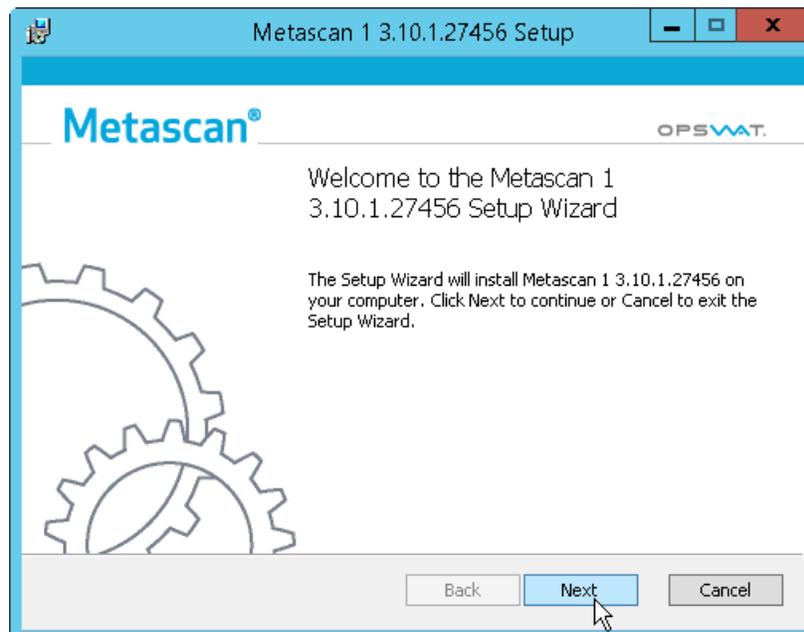
All RSA ECAT components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

OPSWAT Metascan Configuration

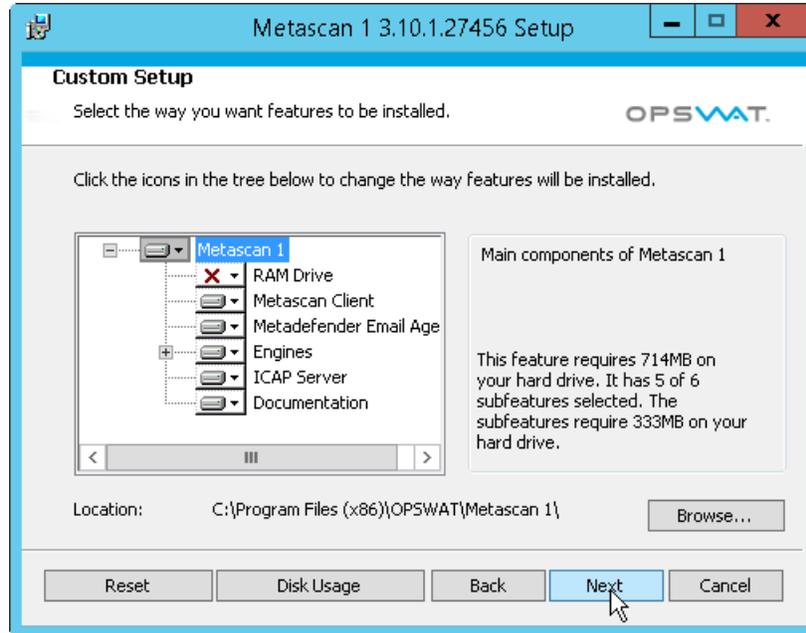
Install OPSWAT Metascan

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.

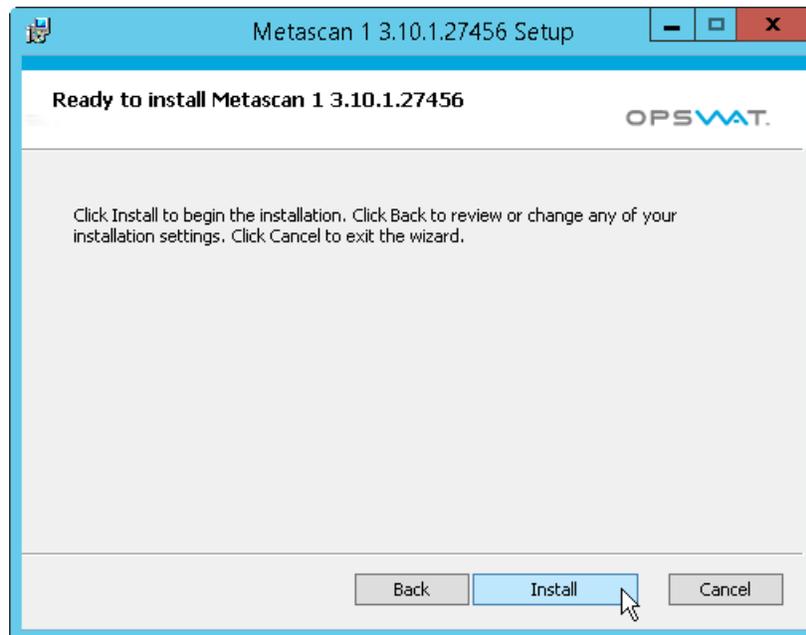
1. Obtain the Metascan installation executable from:
<https://portal.opswat.com/user/register>
2. Double-click the .exe file to run the installation wizard.
3. Click **Next**.



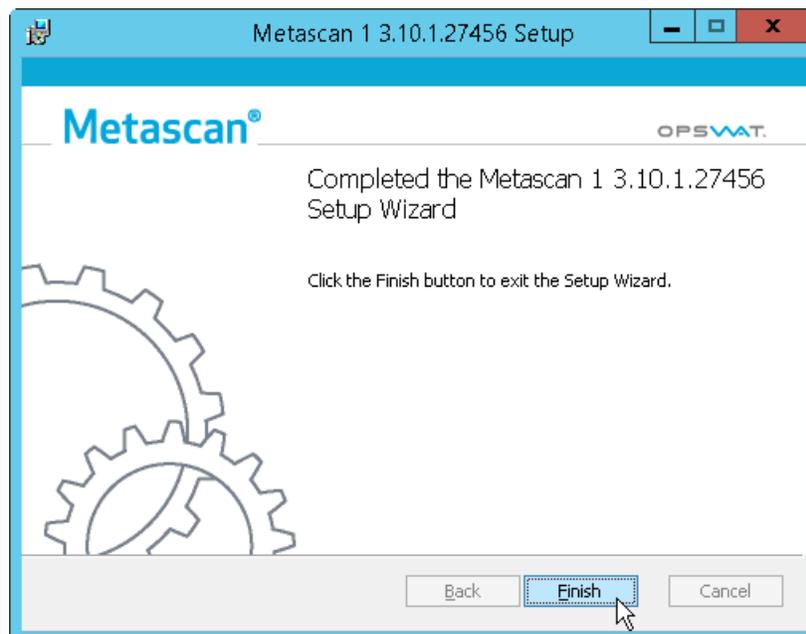
4. The End-User License Agreement dialog is displayed. Read the agreement fully, and check I **accept the terms in the License Agreement** if you agree.
5. Click **Next**. Change the settings here if you wish, or leave it at the default settings and click **Next**.



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:

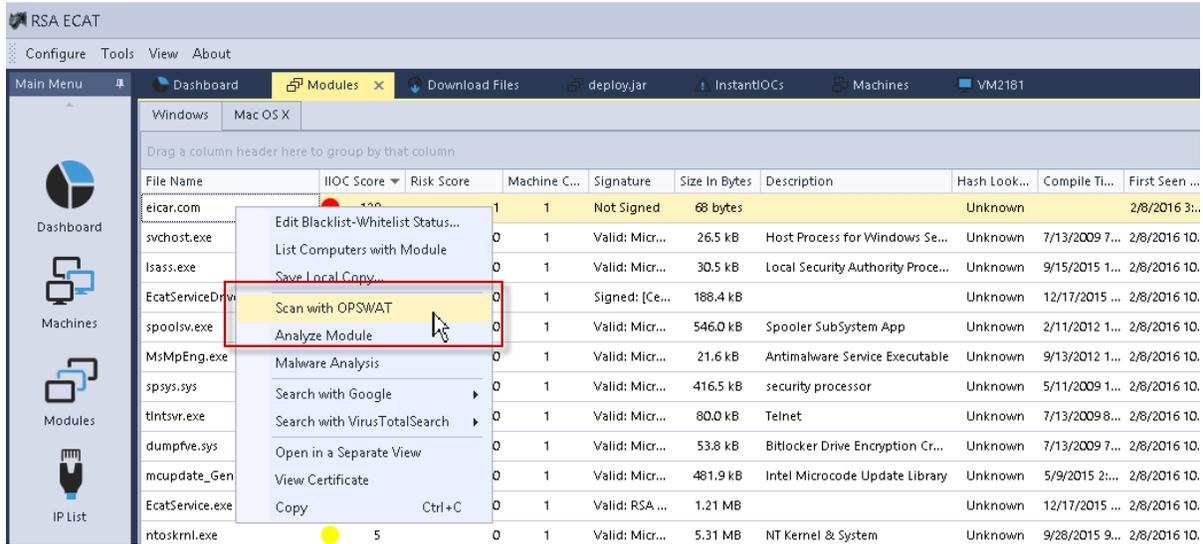
Edit the ConsoleServer config file to add the following line:

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

RSA ECAT Configuration

RSA ECAT UI Screens

Scan with context menu:



Verdict in Module Properties

