IMSVA 9.0 with Virtual Analyzer Integration (DDA/DDAN)

Best Practice Guide

Anti-Spyware Anti-Spam Antivirus Anti-Phishing Content & URL Filtering

Table of Contents

Preface

From Virtual Analyzer (DDA/DDAN) integration in IMSVA 8.5, IMSVA 9.0 further enhances its integration features.

This document will guide IMSVA administrators in making IMSVA work with Virtual Analyzer (DDA/DDAN) smoothly, and meet their expectations.

Author

Bryan Xu

Release Date

June 15, 2015

Virtual Analyzer Integration

Virtual Analyzer (DDA/DDAN) server version requirement

IMSVA 9.0 can integrate with following DDA/DDAN versions:

- DDA 3.0
- DDAN 5.0
- DDAN 5.1

Enabling Virtual Analyzer (DDA/DDAN) integration

1. Open the IMSVA web console. Navigate to **Policy** > **Scan Engine**, and select **Enable Advanced Threat Scan Engine** to enable ATSE. (For SNAP & True file type messages, it is not necessary to enable ATSE scanning.)
2. Navigate to **Administration** > **IMSVA Configuration** > **Virtual Analyzer Settings**.
3. Enable **Submit email messages to Virtual Analyzer**, and provide the DDAN server information. Below is an example:

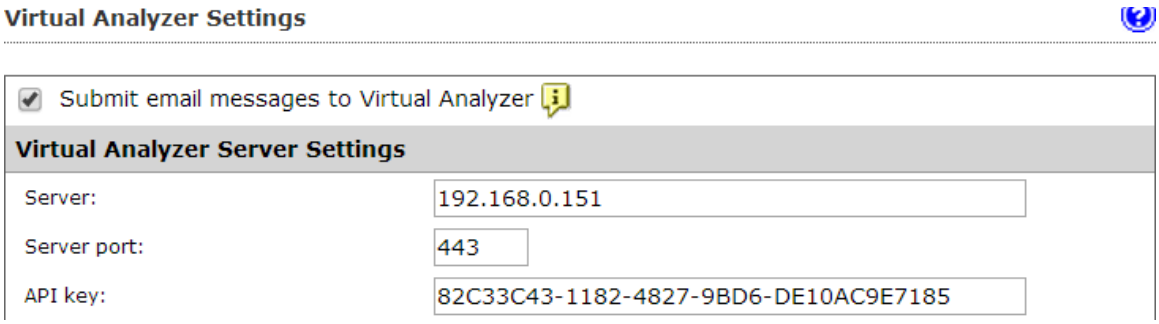

Figure 1

   - Administrators can get the API key from the DDAN web console under **Help** > **About** info.
4. For Security Level Settings, choose **Low** (default) for a more conservative security level. Selecting **High** will provide a more aggressive security level.

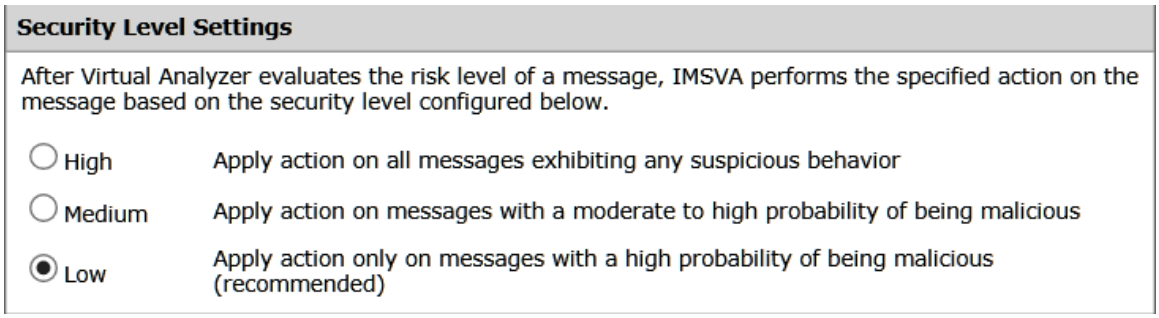

Figure 2

Submission of messages to the Virtual Analyzer

IMSVA will submit messages to the Virtual Analyzer (DDA/DDAN) when enabled. This task is performed in any of following scenarios:

- When ATSE detects messages containing possible virus, IMSVA will submit these messages to the Virtual Analyzer for double confirmation.
  If DDAN's analysis result shows "No risk", IMSVA will dismiss ATSE's detection and pass the mail to the next rule.

- If the administrator enables the Social Engineering Attack Protection (SNAP) feature, and this feature detects messages, IMSVA will submit these messages to the Virtual Analyzer for double verification.

Figure 3

Scanning process flow:

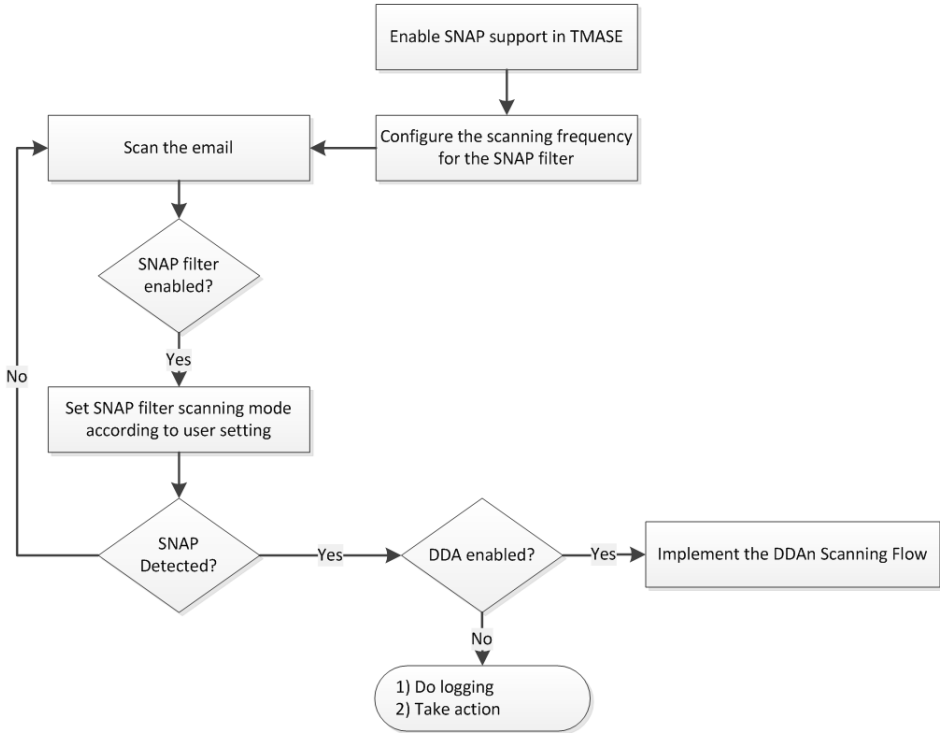

Figure 4

- If the administrator set to submit any true file type attachments to DDAN, IMSVA will submit the related messages to the Virtual Analyzer for analyzing.

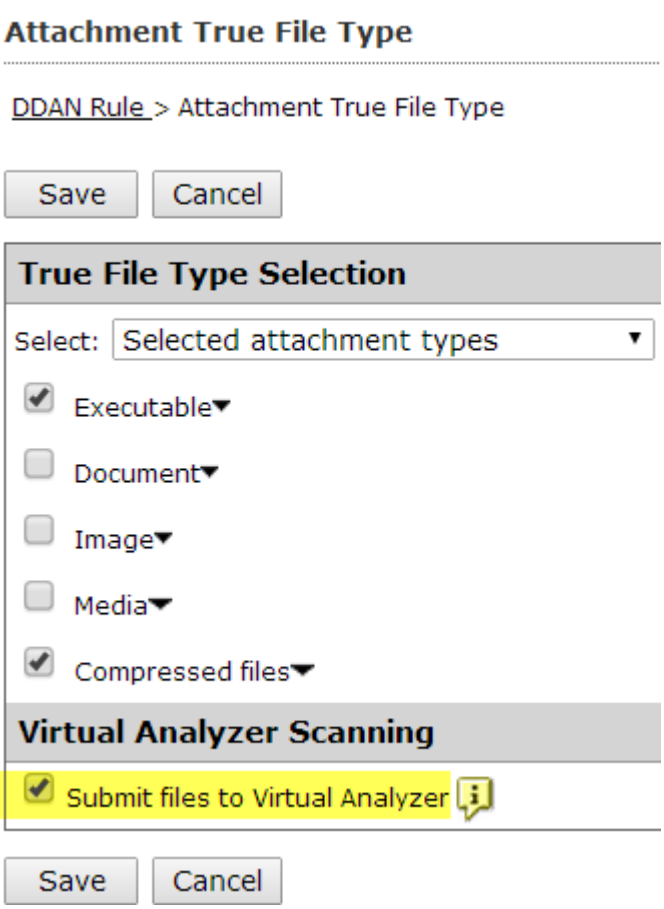
Attachment True File Type
DDAN Rule > Attachment True File Type
Save
Cancel
True File Type Selection
Select:
Selected attachment types
Executable
Document
Image
Media
Compressed files
Virtual Analyzer Scanning
Submit files to Virtual Analyzer
Save
Cancel

Figure 5

Virtual Analyzer Queue

Administrators can query the "Virtual Analyzer" queue (IMSVA UI > Mail Areas & Queues > Query > Virtual Analyzer) for the queued mails waiting for DDAN's analysis result:

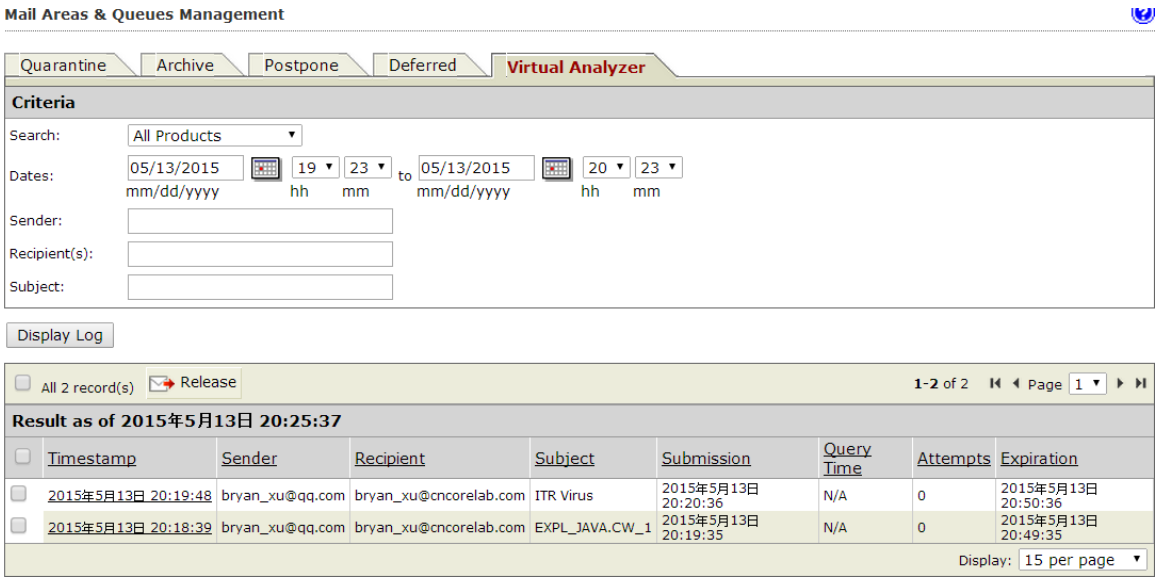

Figure 6

Virtual Analyzer scanning exceptions

If IMSVA cannot get any results from the Virtual Analyzer (DDA/DDAN) in the maximum waiting time, an exception will occur.

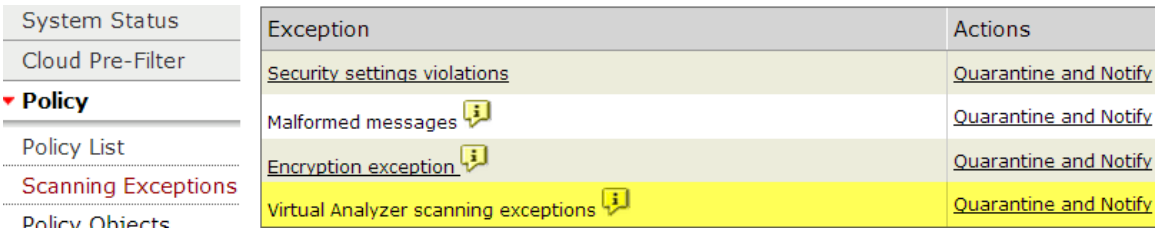

Figure 7

Virtual Analyzer related logs

Administrators can query the email logs which are detected by DDAN from UI > Logs > Query.

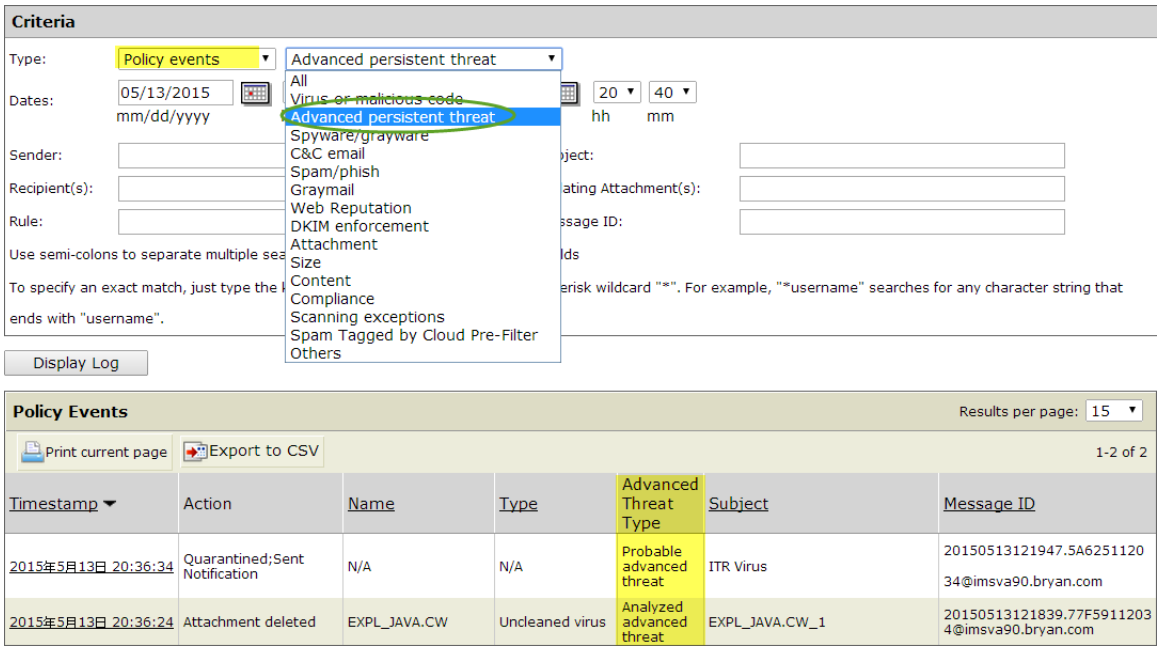

Figure 8

If DDAN analyzes a mail failure, or IMSVA result queries from DDAN fail until expiration, Virtual Analyzer scanning exceptions will be triggered and the Advanced Threat Type will display “Probable advanced threat”.

DDAN-Related Rule Samples

Enabling Social Engineering Attack Protection (SNAP) Scanning

SNAP is a new feature available in IMSVA 9.0. This scanning feature is disabled by default and administrators may choose to enable it.

With SNAP enabled, administrators can either create a new rule only for these SNAP features, or modify current spam rules.

Modify a current spam rule to enable SNAP:

1. Navigate to IMSVA UI > Policy > Policy List.
2. Click **Default spam rule**.
3. Edit the scanning conditions, and select **Social Engineering Attack Protection**:

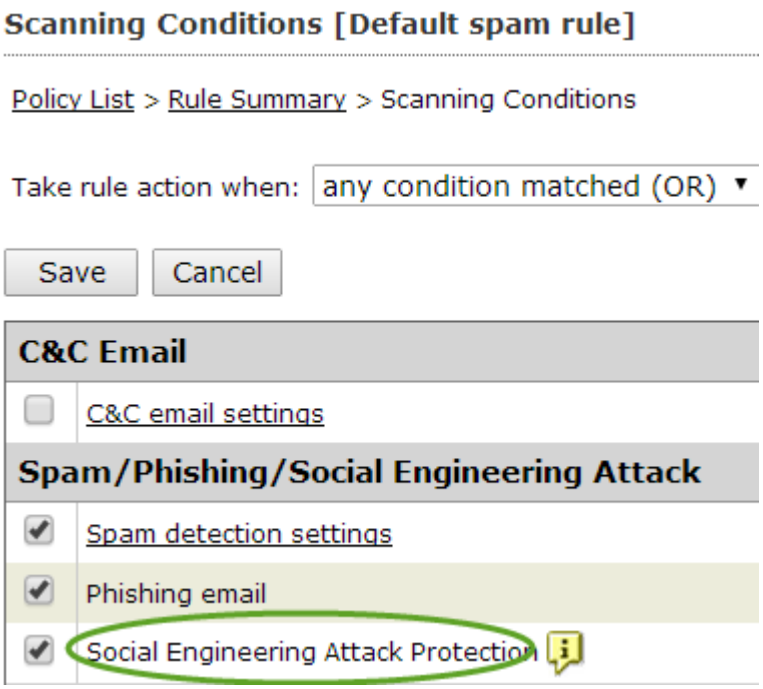

Figure 9

4. Save the changes.

SNAP may still be enabled even without an integrated Virtual Analyzer (DDA/DDAN):

- Without Virtual Analyzer integrated, SNAP will work in conservative mode.
- With Virtual Analyzer integrated, SNAP will work in aggressive mode.

Submitting all executable files to theVirtual Analyzer for analysis

Rule requirement:

Upon submission of messages containing executable attachments to the Virtual Analyzer:

- If the analysis result is high risk, IMSVA will delete the entire message and send a notification to the administrator.
- If the analysis result is no risk, IMSVA will not intercept the messages in this rule.

Steps to create this rule:

1. Navigate to Policy > Policy Notifications, and create a new notification named "DDAN Notification" with the following additional information:

   Recipient: Administrator's mail address.
   Subject: DDAN detected high risk messages
   Message body:
   Sender: %SENDER%
   Recipient: %RCPTS%
   Subject: %SUBJECT%

   DDAN detected %FILENAME% in this mail as high risk and deleted the whole mail.

2. Go to Policy > Policy List, and add a new rule for all messages.

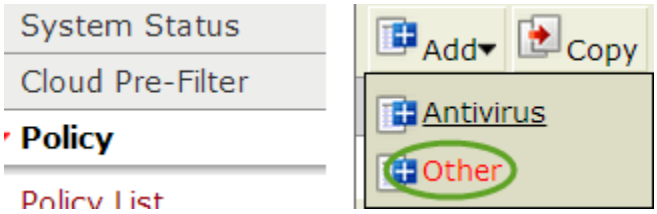

Figure 10

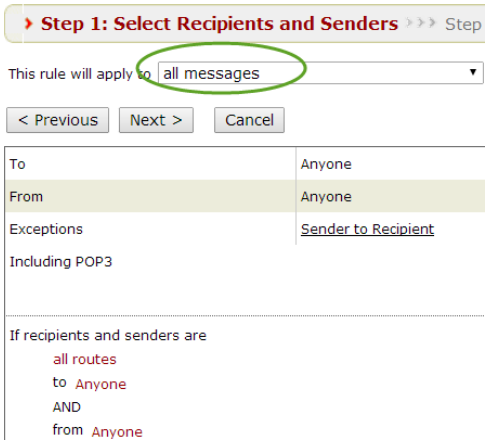

Figure 11

3. For Scanning Conditions, select **Attachment** > **True file type**, then check both **Executable** and **Submit files to Virtual Analyzer** options. Click **Save**.

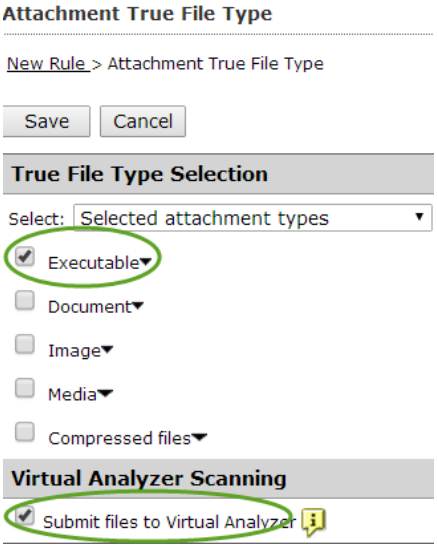

Figure 12

4. For Action, select both **Delete entire message** and **Send policy notifications**. Choose the notification name, "DDAN Notification", created earlier.
5. Save the rule.

Troubleshooting

Issue: All the messages submitted to the Virtual Analyzer are quarantined.

The root cause would probably be that IMSVA could not get any response from the Virtual Analyzer in the maximum waiting time, and then triggered the Virtual Analyzer scanning exceptions.
The IMSVA DTAS Agent default query delay time is 900 seconds, which means that IMSVA will try to query the Virtual Analyzer's analysis result after 15 minutes from the time the message was submitted. If the maximum time set to a value less than 900 seconds, the mail would trigger a scanning exception.

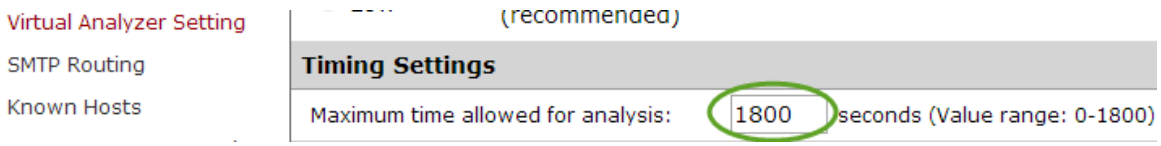

Figure 13

Suggestions:
Do not set the maximum time to a value lower than 1200 seconds. It is recommended to assign a default value of 1800 seconds.

Asynchronization Mode

By default, IMSVA 9.0 works with Virtual Analyzer within synchronization mode, as previously described.

IMSVA 9.0 build 1513 and later supports asynchronization mode which administrators may enable.
In asynchronization mode, there are two scenarios:

- Messages are marked as suspicious by the ATSE or SNAP engine.
  a) IMSVA 9.0 will take the rule action immediately without waiting for the evaluation result from the Virtual Analyzer.
  b) IMSVA 9.0 will still send a copy of the email sample to the Virtual Analyzer for further analysis and will add the information to the corresponding policy event log once it receives the results.

- Messages with true file types are sent to the Virtual Analyzer for analysis.
  a) IMSVA 9.0 will bypass the true file types filter rule directly without waiting for the evaluation result from the Virtual Analyzer.
  b) IMSVA 9.0 will still send a copy of the email sample to the Virtual Analyzer for further analysis and will add the information to the corresponding policy event log once it receives the results.

For asynchronization mode, IMSVA will perform real-time submission to DDAN, but will also implement the virus rule action and bypass true file type action at the same time. It will then update the logs based on the DDAN result.
Administrators may contact Trend Micro Technical Support for information on enabling IMSVA to support Virtual Analyzer integration mode (Hot Fix Build 1513).

FAQ

Question:

Can IMSVA 9.0 with DDAN integrated detect macro threats?

Answer:

Yes, IMSVA 9.0 with ATSE 9.826.1078 or later, supports macro threat detection. Please refer to KB 1110914 for more detailed information.

Question:

How do ATSE and DDAN handle compressed file?

Answer:

Similar to normal files, ATSE and DDAN can uncompress the file and check the files in it.

Question:

If IMSVA encounters timeout issues and cannot get the analysis result from DDAN, what will happen?

Answer:

When failing to query the analysis result from DDAN, IMSVA will retry before maximum waiting time. If it still fails, Virtual Analyzer scanning exceptions will be triggered. The default action for the mail is "Quarantine and Notify".

Question:

As mentioned, IMSVA DTAS Agent default query delay time is 900 seconds. Can an administrator decrease the delay time?

Answer:

Yes, administrators can add parameter query_delay into imss.ini under [dda] section. The value 300 (5 minutes) may be set, as an example. S99DTASAGENT will have to be restarted to apply the changes.