



IMSVA 9.1 with Virtual Analyzer Integration (DDAN)

Best Practice Guide



Anti-Spyware



Anti-Spam



Antivirus



Anti-Phishing



Content & URL
Filtering



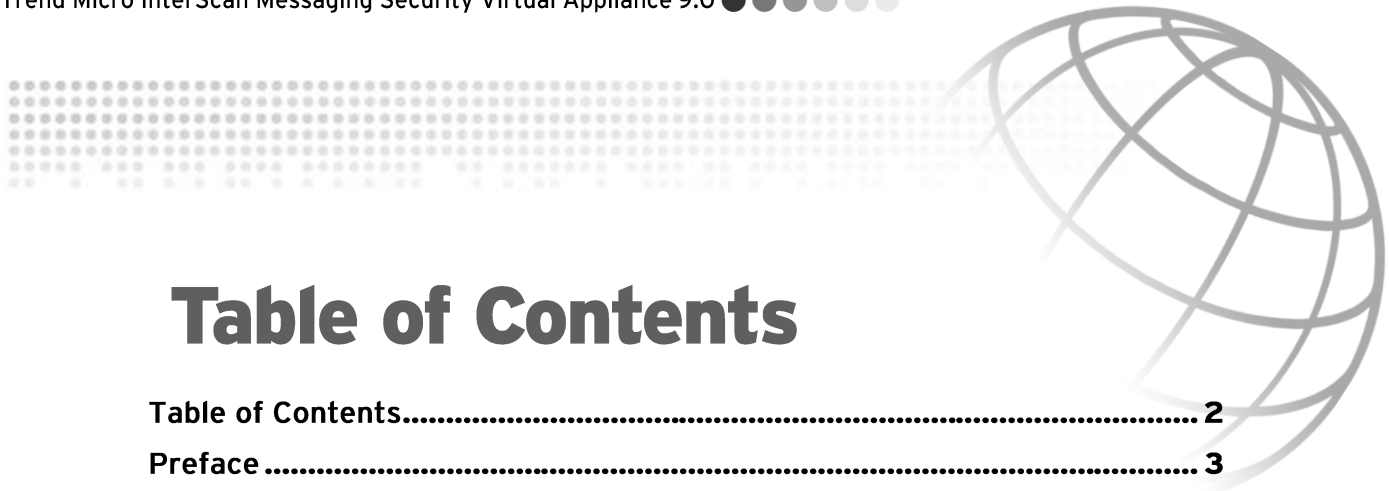


Table of Contents

- Table of Contents..... 2**
- Preface 3**
- Author 3**
- Release Date 3**
- Virtual Analyzer Integration..... 4**
 - Virtual Analyzer (DDAN) server version requirement 4
 - Enabling Virtual Analyzer (DDAN) integration 4
 - Submission of messages to the Virtual Analyzer 5
 - Virtual Analyzer Queue..... 9
 - Virtual Analyzer scanning exceptions10
 - Virtual Analyzer related logs.....10
 - Virtual Analyzer Cache Mechanism12
- Connected Threat Defense (CTD)..... 13**
 - Action Mapping13
 - Configure Smart Protection Server (Optional).....14
 - Register IMSVA to TMCM14
 - Configure TMCM15
 - Messages deteted by Suspicious Object (SO).....16
- DDAN-Related Rule Samples 17**
 - Enabling Social Engineering Attack Protection (SNAP) Scanning17
 - Submitting all executable files to theVirtual Analyzer for analysis.....18
 - Submitting all *.js files and *.vbs files to theVirtual Analyzer for analysis.....21
- Troubleshooting24**
 - Issue: All the messages submitted to the Virtual Analyzer are quarantined.24
- FAQ 25**

Preface

From Virtual Analyzer (DDAN) integration in IMSVA 8.5, IMSVA 9.0 and IMSVA 9.1 further enhances its integration features.

This document will guide IMSVA 9.1 Administrators in making IMSVA 9.1 work smoothly with Virtual Analyzer (DDAN), and meet their expectations.

Author

Bryan Xu

Release Date

February 14, 2017

Virtual Analyzer Integration

Virtual Analyzer (DDAN) server version requirement

IMSVa 9.1 can integrate with the following DDAN versions:

- DDAN 5.0
- DDAN 5.1
- DDAN 5.5

Enabling Virtual Analyzer (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 & “Name or extension” messages, it is not necessary to enable ATSE scanning.)
2. Navigate to **Policy > Virtual Analyzer**. The **Virtual Analyzer Settings** tab appears by default.
3. For Security Level Settings, choose Low (default) for a more conservative security level. Selecting High will provide a more aggressive security level.
4. For Timing Settings, it is suggested to keep it to the default value, 1800.

This setting defines the maximum waiting time for the analysis result. If IMSVA cannot get the analysis result from Virtual Analyzer (DDAN) in the maximum waiting time, it will trigger Virtual Analyzer scanning exceptions.

Virtual Analyzer Settings		Server Management
<input checked="" type="checkbox"/> Submit email messages to Virtual Analyzer ⓘ		
Security Level Settings		
After Virtual Analyzer evaluates the risk level of a message, IMSVA performs the specified action on the message based on the security level configured below.		
<input type="radio"/> High	Apply action on all messages exhibiting any suspicious behavior	
<input type="radio"/> Medium	Apply action on messages with a moderate to high probability of being malicious	
<input checked="" type="radio"/> Low	Apply action only on messages with a high probability of being malicious (recommended)	
Timing Settings		
Maximum time allowed for analysis:	<input type="text" value="1800"/>	seconds (Value range: 300-1800)

Figure 1

5. Go to **Server Management** tab, and set the DDAN server info.

Server Management > Add Server

Virtual Analyzer Server

☒ Enable

Server: 192.168.0.151
Example: server.us.trendnet.org or 10.1.1.1

Port: 443

API key: 82C33C43-1182-4827-9BD6-DE10AC9E7185

Preference: ⓘ 10

Save

Cancel

Figure 2

- Administrators can get the API key from the DDAN web console under **Help > About** info.
 - IMSVA 9.1 supports multiple DDAN servers, and **Preference** represents each server’s priority.
6. An Administrator can set the multiple DDAN servers here. The lower the **Preference**, the higher the priority.

Virtual Analyzer Settings

Server Management

Server List

+ Add

🗑 Delete

<input type="checkbox"/>	Server	Port	API Key	Preference	Enable
<input type="checkbox"/>	192.168.0.155	443	91E140D4-2C57-4239-AE55-B26213A63CED	10	<input checked="" type="checkbox"/>
<input type="checkbox"/>	192.168.0.151	443	82C33C43-1182-4827-9BD6-DE10AC9E7185	10	<input checked="" type="checkbox"/>

Figure 3

Submission of messages to the Virtual Analyzer

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

Policy List > Rule Summary > Scanning Conditions

Take rule action when: any condition matched (OR) ▼

Save

Cancel

C&C Email

☐

C&C email settings

Phishing/Social Engineering Attack/Spam

☒

Phishing email

☐

Social Engineering Attack Protection ⓘ

☒

Spam detection settings

Figure 4

Scanning process flow:

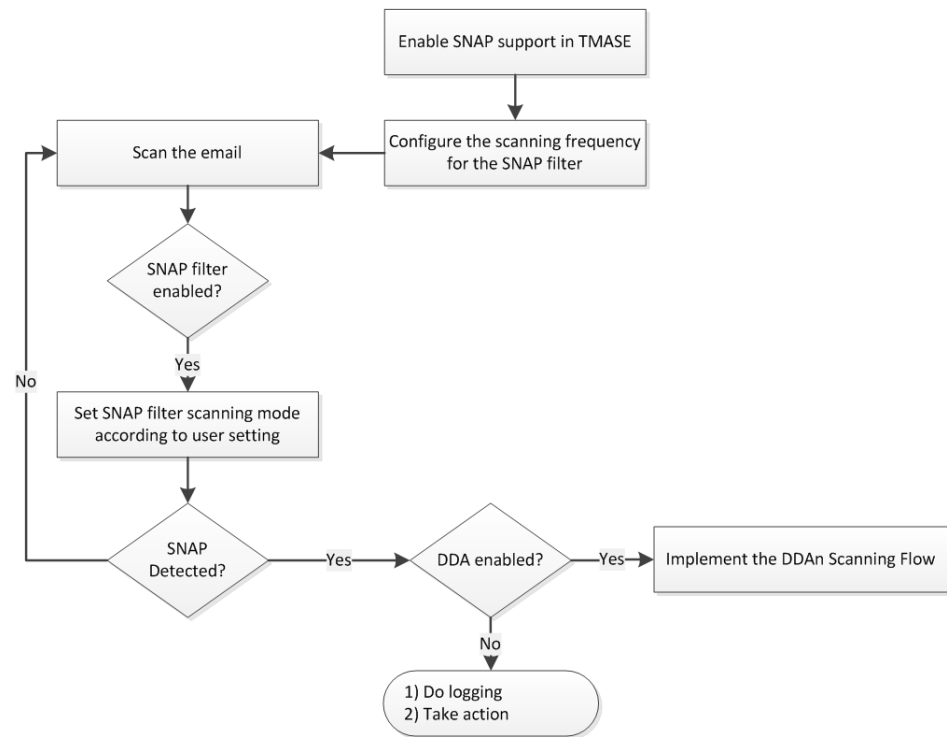


Figure 5

- 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. Such would be creating a rule to submit executable files, documents and compressed files to Virtual Analyzer for analyzing.

True File Type Selection

Select:

Selected attachment types

☒ Executable

☒ Document

☐ Image

☐ Media

☒ Compressed files

☐ Microsoft Windows shortcuts

Virtual Analyzer Scanning

☒ Submit files to Virtual Analyzer

Figure 6

- If the Administrator set to submit any name or extension attachments to DDAN, IMSVA will submit the related messages to the Virtual Analyzer for analyzing. Such would be creating a separate rule to submit *.js files to Virtual Analyzer for analyzing.

The image shows two configuration panels from a web interface. The top panel, titled 'Name or Extension Settings', contains a 'Select:' dropdown menu with 'Selected attachment names' selected. Below this are three checkboxes: 'File extensions to scan (recommended)' (unchecked), 'File extensions to consider scanning (more commonly exchanged)' (unchecked), and 'Attachments named' (checked). To the right of the checked checkbox is an 'Import' button. Below these options is a text input field with the text '*.js' inside, which is circled in green. A note above the field reads 'Use the full filename (not the extension) and separate each entry'. The bottom panel, titled 'Virtual Analyzer Scanning', has a yellow background and contains a checked checkbox labeled 'Submit files to Virtual Analyzer' with an information icon to its right.

Figure 7

Note: If it is preferred to submit both **True File Type** messages and **Name or Extension** messages to Virtual Analyzer for analyzing, it is suggested to create separate rules to address this - one rule for True File Type messages and another rule for Name or Extension messages.

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:

Mail Areas & Queues Management

Quarantine

Archive

Postpone

MTA

Virtual Analyzer

Criteria

Search:

All Products

Dates:

01/06/2017

16

39

to

01/06/2017

17

39

mm/dd/yyyy

hh

mm

mm/dd/yyyy

hh

mm

Sender:

Recipient(s):

Subject:

Display Log

☐ All 6 record(s)

Release

1-6 of 6

Page 1

Result as of 2017年1月6日 17:39:39

<input type="checkbox"/>	Timestamp	Sender	Recipient	Subject	Submission	Query Time	Attempts	Expiration
<input type="checkbox"/>	2017年1月6日 17:07:58	bryan_xu@qq.com	bryan_xu@cncorelab.com	Sample: TROJ_CRYPTWALL.XXTXL	2017年1月6日 17:09:17	2017年1月6日 17:39:33	12	2017年1月6日 17:39:17
<input type="checkbox"/>	2017年1月6日 17:07:58	bryan_xu@qq.com	bryan_xu@cncorelab.com	Sample: TROJ_CRYPTWALL.XXTXP	2017年1月6日 17:09:18	2017年1月6日 17:38:36	12	2017年1月6日 17:39:18
<input type="checkbox"/>	2017年1月6日 17:07:57	bryan_xu@qq.com	bryan_xu@cncorelab.com	Sample: TROJ_CRYPTWALL.YYY	2017年1月6日 17:09:10	2017年1月6日 17:38:46	12	2017年1月6日 17:39:10
<input type="checkbox"/>	2017年1月6日 17:07:57	bryan_xu@qq.com	bryan_xu@cncorelab.com	Sample: TROJ_CRYPTWALL.BTM	2017年1月6日 17:09:11	2017年1月6日 17:39:17	12	2017年1月6日 17:39:11
<input type="checkbox"/>	2017年1月6日 17:07:57	bryan_xu@qq.com	bryan_xu@cncorelab.com	Sample: TROJ_CRYPTWALL.CC	2017年1月6日 17:09:12	2017年1月6日 17:38:56	12	2017年1月6日 17:39:12
<input type="checkbox"/>	2017年1月6日 17:07:57	bryan_xu@qq.com	bryan_xu@cncorelab.com	Sample: TROJ_CRYPTWALL.MG	2017年1月6日 17:09:13	2017年1月6日 17:39:07	12	2017年1月6日 17:39:13

Display: 15 per page

Figure 1

Virtual Analyzer scanning exceptions

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

System Status	Exception	Actions
Cloud Pre-Filter	Security settings violations	Quarantine and Notify
▼ Policy		
Policy List	Malformed messages ⓘ	Quarantine and Notify
Scanning Exceptions	Encryption exception ⓘ	Quarantine and Notify
Policy Objects	Virtual Analyzer scanning exceptions ⓘ	Quarantine and Notify

Figure 2

Virtual Analyzer related logs

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

Log Query

Criteria

Type: **Policy events** **Advanced persistent threat**

Dates: 01/06/2017 16:00:00 mm/dd/yyyy hh:mm

Sender:

Recipient(s):

Rule:

Use semi-colons to separate multiple search criteria. Type any keyword to specify an exact match with "username".

Display Log

Policy Events

Print current page Export to CSV

Results per page: 15 1-5 of 5

Timestamp	Action	Name	Type	Advanced Threat Type	Subject	Message ID
2017年1月6日 17:21:47	Attachment deleted; Subject tagged	N/A	N/A	Analyzed advanced threat	DDAN Name Extension: JS Sample 3	20170106090755.2A14D12C05D@imsva91.bryan.com
2017年1月6日 17:21:47	Attachment deleted; Subject tagged	N/A	N/A	Analyzed advanced threat	DDAN Name Extension: JS Sample 5	20170106090756.05A8B12C051@imsva91.bryan.com
2017年1月6日 17:21:47	Attachment deleted; Subject tagged	N/A	N/A	Analyzed advanced threat	DDAN Name Extension: JS Sample 10	20170106090754.275D012C059@imsva91.bryan.com
2017年1月6日 17:15:47	Attachment deleted; Subject tagged	N/A	N/A	Analyzed advanced threat	DDAN Name Extension: JS Sample 2	20170106090754.8B3D612C05B@imsva91.bryan.com
2017年1月6日 17:15:47	Attachment deleted; Subject tagged	N/A	N/A	Analyzed advanced threat	DDAN Name Extension: JS Sample 1	20170106090753.7F8FA12C051@imsva91.bryan.com

Figure 3

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”.

Virtual Analyzer Cache Mechanism

IMSVA 9.1 will cache the virtual analysis result for a significant time. IMSVA will check the virtual analysis cache first before submitting the message to DDAN for analyzing. If there is a cache result, IMSVA will use this cache result directly instead of submitting the file to DDAN.

The cache contains files' SHA1 info and result. That means when multiple messages with the same attachment enter IMSVA, if the attachment's cache result exists, IMSVA will just use the cache result directly and there is no need to submit the mail to DDAN.

The cache would be cleaned everytime DTAS agent restarts; while IMSVA will also automatically restart DTAS agent service every day at around 23:00. This means IMSVA will keep the virtual analysis cache result with the maximum time less than one day.

Administrators can also manually restart DTAS agent (S99DTASAGENT restart) to clean the cache.

Connected Threat Defense (CTD)

IMSVA 9.1 supports Connected Threat Defense (CTD) solution. Administrators can configure IMSVA to subscribe to the Suspicious Object (SO) lists from the Control Manager server. Using the Control Manager console, you can create customized actions for objects detected by the suspicious object lists to provide custom defense against threats in Trend Micro products.

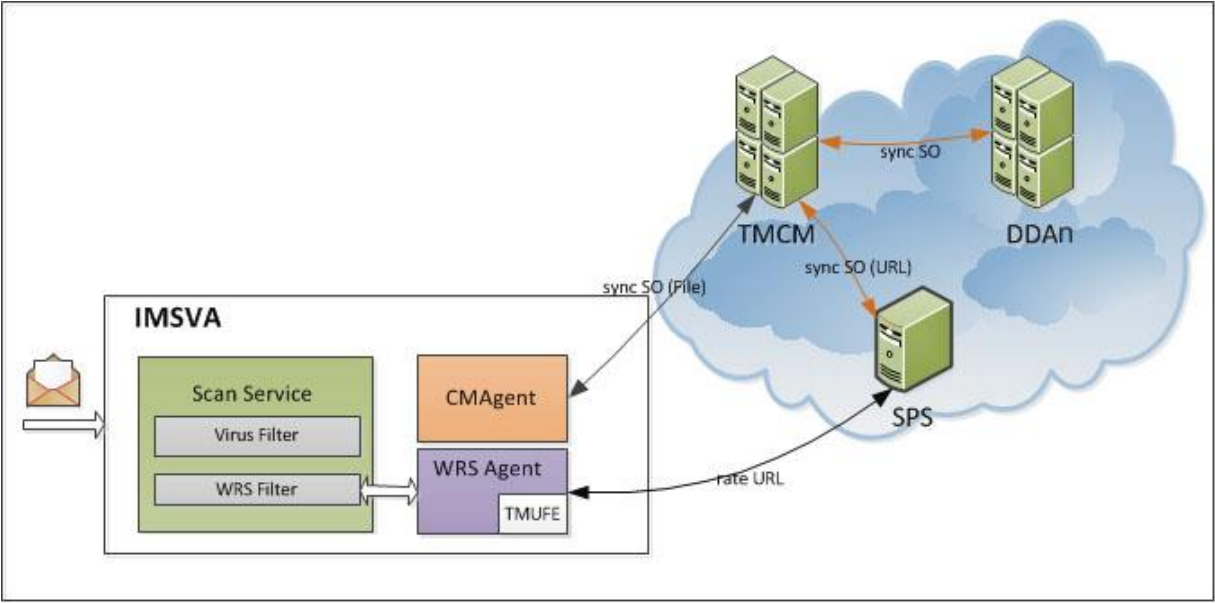


Figure 9

- File checking: IMSVA can sync Suspicious Object (SO) file list information from the Control Manager server and use the SO to do file checking.
- URL checking: This is optional. In order to address this feature, IMSVA needs to use Smart Protection Server (Local SPS server) to do Web Reputation Services (WRS) checking.

Action Mapping

TMC can configure the Suspicious Object (SO) with Log, Block or Quarantine action, and IMSVA will map the action as mentioned in following table:

	Action on TMC	Mapped Action on IMSVA
SO - Files	N/A or Log	Pass & Log

	Block or Quarantine	Quarantine & Log
SO - URLs	N/A or Log	Pass & Log
	Block	Quarantine & Log

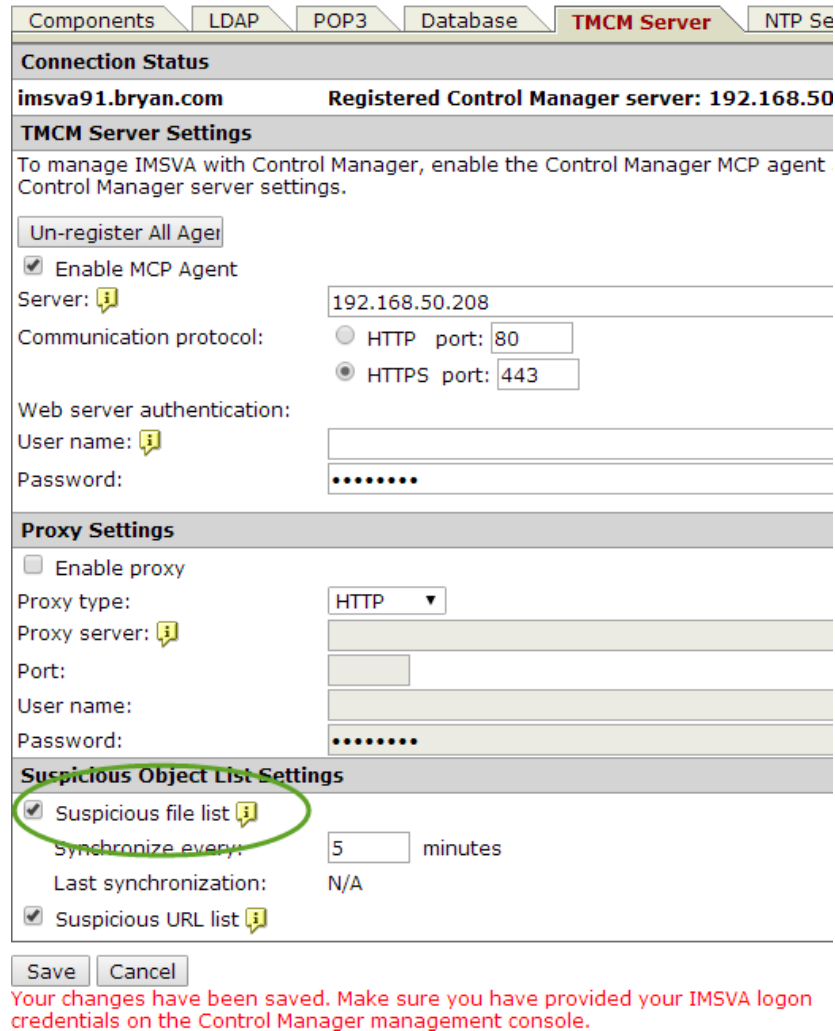
Configure Smart Protection Server (Optional)

After registering Smart Protection Server (Local SPS Server) to the TMCM server, it will be able to sync Suspicious URL info from TMCM.

If IMSVA enables Suspicious URL list feature (by selecting **Smart Protection Server** on the **Web Reputation Services** tab under **Policy > Smart Protection**), IMSVA will be able to detect suspicious URL.

Register IMSVA to TMCM

1. Open IMSVA web console, and navigate to **Administration > IMSVA Configuration > Connections**.
2. Click **TMCM Server** tab.
3. Configure the TMCM server info.
4. Select **Suspicious file list** under Suspicious Object List Settings section.
5. (Optional) For IMSVA to detect suspicious URL, an Administrator can select **Suspicious URL list** under Suspicious Object List Settings section. (In order to enable this feature, IMSVA needs to use Smart Protection Server (Local SPS server) to do Web Reputation Services (WRS) checking.)



Components | LDAP | POP3 | Database | **TCMC Server** | NTP Se

Connection Status

imsva91.bryan.com Registered Control Manager server: 192.168.50

TCMC Server Settings

To manage IMSVA with Control Manager, enable the Control Manager MCP agent. Control Manager server settings.

Un-register All Agent

☒ Enable MCP Agent

Server: ⓘ 192.168.50.208

Communication protocol: ☐ HTTP port: 80 ☒ HTTPS port: 443

Web server authentication:

User name: ⓘ

Password:

Proxy Settings

☐ Enable proxy

Proxy type: HTTP

Proxy server: ⓘ

Port:

User name:

Password:

Suspicious Object List Settings

☒ Suspicious file list ⓘ

Synchronize every: 5 minutes

Last synchronization: N/A

☒ Suspicious URL list ⓘ

Save Cancel

Your changes have been saved. Make sure you have provided your IMSVA logon credentials on the Control Manager management console.

Figure 10

Configure TCMC

After registering IMSVA to TCMC, in order to make IMSVA can synchronize suspicious file list from TCMC, Administrators will also have to provide IMSVA logon credentials on the TCMC console.

1. Open TCMC web console, navigate to **Administration > Managed Servers**.
2. Next to **Server Type**, select **InterScan Messaging Security Virtual Appliance**.
3. Find your IMSVA server and click the **Edit** icon in the Actions column.
4. The Edit Server screen appears, under **Authentication**, provide your IMSVA log in credentials.

Edit Server

Server Information

Server:
https://192.168.50.91:8445
For example: http(s)://<server_name>-port_number

Display name:
imsva91.bryan.com_IMSVA

Product:
InterScan Messaging Security Virtual Appliance 9.1

Authentication

User name:
admin

Password:

Connection

☐ Use a proxy server for the connection

Save

Cancel

5. Click **Save**.

Messages deteted by Suspicious Object (SO)

IMSVA 9.1 contains following two hidden rules for suspicious object detection:

- TCMC_Suspicious file detection
- TCMC_Suspicious URL detection

These rules are executed after virus rules and have higher priority than other rules.

Scenario 1: A known virus was defined in both pattern file and SO list. IMSVA will use pattern file to detect it as a real virus.

Scenario 2: An unknow malicious file (not included in pattern file) was defined in SO list. IMSVA will detected it as “Suscipious Object” with the rule name “TCMC_Suspicious file detection”:

Policy Events		
<div><div>Print current page</div><div>Export to CSV</div></div>		
Timestamp ▼	Action	Rule
2016年10月20日 12:30:17	Quarantined	TCMC_Suspicious file detection
2016年10月20日 12:30:13	Quarantined	TCMC_Suspicious file detection
2016年10月20日 12:30:07	Quarantined	TCMC_Suspicious file detection

Log Query Details

Timestamp:	2016 年 10 月 20 日 12:30:17
Sender:	test@test.com
Recipient:	bryan_xu@cncorelab.com
Subject:	Sample File 2
Original size (KB):	159.7
Violating attachments:	Sample_Virus2.rar/ D44F.exe_name
Violation reason:	Suspicious Objects
True file type:	N/A
Rule:	TBCM_Suspicious file detection
Action:	Quarantined
Message ID:	20161020043014.8EB9A12C051@imsva91.bryan.com
Internal ID:	48FB8A0D-3F44-6105-B29E-4AF84843866F
Scanner:	imsva91.bryan.com

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 4

4. Save the changes.

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

- Without Virtual Analyzer integrated, SNAP will work in conservative mode.
- With Virtual Analyzer integrated, SNAP will work in aggressive mode, and IMSVA will submit these detected messages to the Virtual Analyzer for double verification.

Submitting all executable files to the Virtual 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, low risk or medium risk, IMSVA will not intercept the messages in this rule.

Steps to create this rule:

1. Open the IMSVA web console.
2. Go to **Policy > Virtual Analyzer > Virtual Analyzer Settings**.
3. Make sure that Security Level Settings is set to **Low**.
4. Go to **Policy > Policy Notifications**, and create a new notification named “VA High Risk Mail Notification” with the following additional information:

Recipient: Administrator’s mail address.

Subject: Virtual Analyzer 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.

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

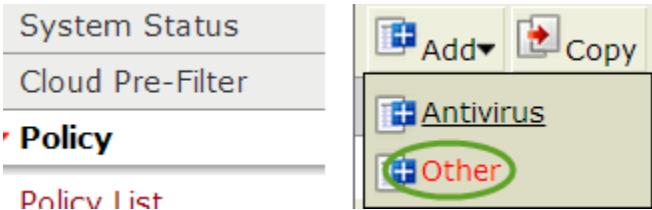


Figure 5

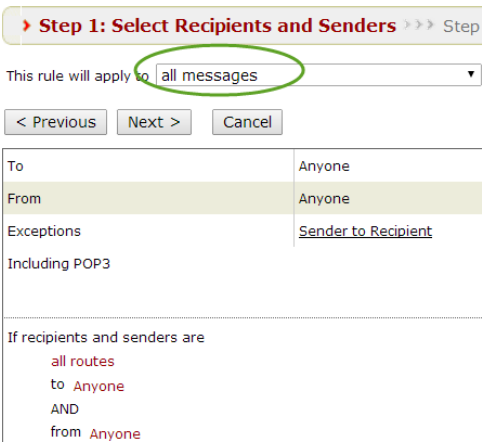


Figure 6

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

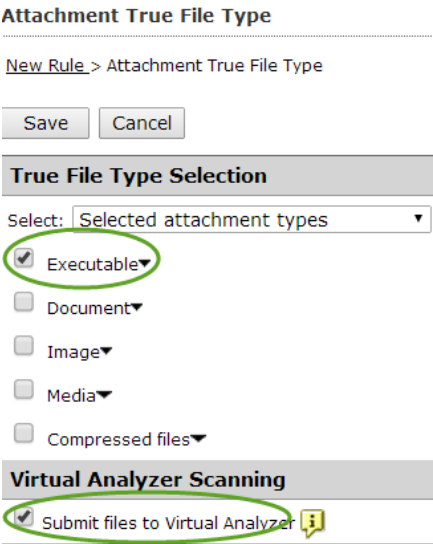


Figure 7

7. For Action, select both **Delete entire message** and **Send policy notifications**. Choose the notification name, " Virtual Analyzer Notification", created earlier.
8. Save the rule.

Submitting all *.js files and *.vbs files to the Virtual Analyzer for analysis

Note: If you prefer to submit both **True File Type** messages and **Name or Extension** messages to the Virtual Analyzer for analysis, it is suggest to create seperate rules to address this.

Rule requirement:

Upon submission of messages containing script attachments (*.js or *.vbs) to the Virtual Analyzer:

- If the analysis result contains risk, IMSVA will quarantine the 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. Open the IMSVA web console.
2. Go to **Policy > Virtual Analyzer > Virtual Analyzer Settings**.
3. Make sure that Security Level Settings is set to High.
4. Go to **Policy > Policy Notifications**, and create a new notification named “VA Risk Mail Notification” with the following additional information:

Recipient: Administrator’s mail address.

Subject: Virtual Analyzer detected risk messages

Message body:

Sender: %SENDER%

Recipient: %RCPTS%

Subject: %SUBJECT%

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

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

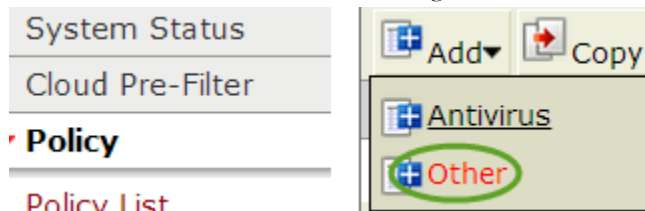


Figure 8

Step 1: Select Recipients and Senders >>> Step

This rule will apply to all messages

< Previous Next > Cancel

To	Anyone
From	Anyone
Exceptions	Sender to Recipient
Including POP3	

If recipients and senders are

all routes
to Anyone
AND
from Anyone

Figure 9

6. For Scanning Conditions, select **Attachment > Name or extension**, then input the name extension as “*.js;*.vbs” and check Submit files to Virtual Analyzer. Click **Save**.

Name or Extension Settings

Select: Selected attachment names

☐ File extensions to scan (recommended)▼

☐ File extensions to consider scanning (more commonly

☒ Attachments named Import

Use the full filename (not the extension) and separa

.js;.vbs

Virtual Analyzer Scanning

☒ Submit files to Virtual Analyzer

Save Cancel

Figure 10

7. For Action, select both **Quarantine to** and **Send policy notifications**. Choose the notification name, "VA Risk Mail Notification ", created earlier.
8. Save the rule.

Troubleshooting

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

The root cause would probably be that DDAn is very busy and IMSVA could not get any response from the Virtual Analyzer in the maximum waiting time, thus triggering the Virtual Analyzer scanning exceptions. The IMSVA 9.1 DTAS Agent default query delay time is 60 seconds, which means that IMSVA will try to query the Virtual Analyzer's analysis result after 1 minute from the time the message was submitted. If there are no results, IMSVA will retry every minute until the maximum timing settings or maximum retry times (20 times). The mail would then trigger a virtual analyzer scanning exception.

Timing Settings	
Maximum time allowed for analysis:	1800 seconds (Value range: 300-1800)

Figure 11

Suggestions:

- Set the maximum time larger than 900 seconds.
- If DDAN is always busy, try to reduce the files that are sent for analyzing.

FAQ

Question:

Can IMSVA 9.1 with DDAN integrated detect macro threats?

Answer:

Yes, IMSVA 9.1 supports macro threat detection. Please refer to [KB 1110914](#) for more detailed information.

Question:

How do ATSE and DDAN handle compressed files?

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”.