Trend Micro™
Deep Discovery Email Inspector 5.1

Best Practice Guide

Portions of this manual have been reprinted with permission from other Trend Micro documents. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Information in this document is subject to change without notice.

Authors: Daniel Zhai, Lawrence Guan, and Marvin Ma
Editor: Jennifer Miñoza
Release Date: February 17, 2023

Lesson 1: Product Description

1.1. Major Features

Deep Discovery Email Inspector (DDEI) stops sophisticated, targeted attacks and cyber threats by scanning, simulating, and analyzing suspicious links and attachments in email messages before they can threaten your network. Designed to integrate into your existing email network topology, DDEI can act as a Mail Transfer Agent in the mail traffic flow or as an out-of-band appliance silently monitoring your network for cyber threats and unwanted spam messages.

Below is the DDEI release history and a partial list of new features:

- DDEI 2.0 – April 2014, build 1223, advanced detection, sandbox, attachment analysis, embedded URL analysis
- DDEI 2.1 – April 2015, build 1180, supports SPAN/TAP working mode, Syslog integration, email alert enhancement, linked file analysis, web reputation
- DDEI 2.5 – February 2016, DDAN/TMCM/SPS integration, URL rewriting, enhanced syslog integration, DDEI 9100 support
- DDEI 2.6 – March 2017, Deep Discovery Director support, threat intelligence sharing
- DDEI 3.0 - October 2017, License management, Anti-spam, content filtering, predictive machine learning, end-user quarantine
- DDEI 3.1 - June 2018, Central IOC exchange via DDD, new HW model DDEI 7200/9200 based on Dell 14th gen platform, sender authentication, DKIM signing, policy-based message archiving, manual email submission, appliance power-off and restart through the web console
- DDEI 3.2 - October 2018, Central log visibility via DDD 3.5, enhanced Virtual Analyzer, enhanced URL detection, enhanced content filtering, enhanced alert notification
- DDEI 3.5 - April 2019, DLP support, new Virtual Appliance model, DDD 5.0 support, message rerouting, Apex Central 2019 integration, in-line migration support
- DDEI 5.0 - July 2020, SAML for Single Sign-On (SSO), new directory service integration, support handoff action, improved detection, Support NIC Teaming in active/backup mode
- DDEI 5.1 - June 2021, support GW license only, more secure controls on mail traffic, support address rewriting, policy and management enhancement, improved detection. Support extra 10Gb fiber cards.

1.2. License

DDEI 5.1 has two license types:

- Advanced Threat Protection – The Advanced Threat Protection license covers the original DDEI features plus other related enhancements made in this release, such as internal sandboxing, password analyzer, TrendX scanning, and CTP protection etc.
- Gateway Module – The Gateway Module license covers traditional message gateway related features, such as sender filtering, content filtering, anti-spam and EUQ etc.

The administrator can check the license information from the UI web console: **Administration** > **License**. After an in-line update from the previous DDEI version to 5.1, the Advanced Threat Protection license integrates from the previous version, and there will be no Gateway Module license by default.

To use the Gateway Module functions, the administrator needs to provide a Gateway Module license.

The following table contains the detailed function set for each type of license:

Advanced Threat Protection (ATP) Function Set	ATP	GM
Internal Sandbox (include GRID, URL filtering)	Yes	No
Password Analyzer	Yes	No
YARA	Yes	No
Predictive Machine Learning scanning (include Census)	Yes	Yes
Time-of-Click	Yes	Yes
Threat Intelligence Sharing	Yes	Yes
Auxiliary Products/Services	Yes	Yes
Web Service API for Suspicious Objects Sharing	Yes	Yes
Trend Locality Sensitive Hash (TLSH)	Yes	Yes
Macroware detection	Yes	Yes
Anti-spam/Graymail	No	Yes
Email Reputation Service integration	No	Yes
Sender filtering	No	Yes
DKIM signatures	No	Yes
End-User Quarantine	No	Yes
Content filtering	No	Yes
Data Loss Prevention	No	Yes
Email Encryption	No	Yes
ATSE	Yes	Yes
WRS & WIS	Yes	Yes

TABLE 1.2.1.1: Function set for each license type

Advanced Threat Protection (ATP) Function Set	ATP	GM
Business Email Compromise protection	Yes	Yes
Social network attack and phishing protection	Yes	Yes
DDAN integration (Including GRID)	Yes	Yes
Suspicious Objects detection	Yes	Yes
DDD integration	Yes	Yes
All others	Yes	Yes
AU	Yes	Yes

TABLE 1.2.1.1: Function set for each license type

All features in the web console are available regardless of the license type in use. However, the feature would only work when using the appropriate license type. Take note that product configuration backup and restore can be limited depending on the AC type, as can be seen in the following table:

	Restore with only ATP Activated	Restore with only GM Activated	Restore with ATP and GM Activated
Backup with only ATP activated	Allow	Disallow	Disallow
Backup with only GM activated	Disallow	Allow	Disallow
Backup with both ATP and GM activated	Allow	Allow	Allow

TABLE 1.2.1.2: Backup and Restore Options per License Type

Also, upgrading the firmware to version 5.1 automatically converts the AC for versions 5.0 and below to ATP AC.

Lesson 2: Hardware and Performance

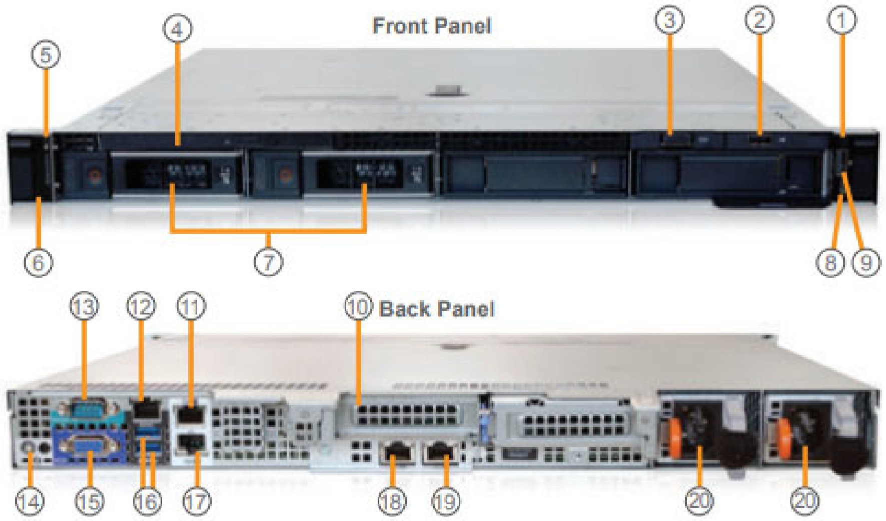
2.1. DDEI Models

Compared to the previous version, DDEI 5.1 also has four hardware types:

- DDEI 7200
- DDEI 9200
- DDEI 7300

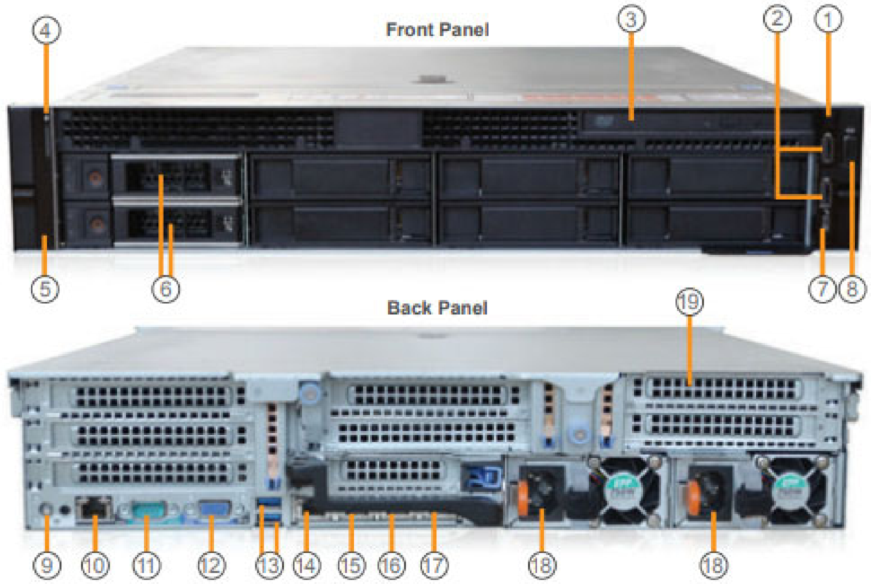
The following are screen shots of different DDEI models showing the front and rear panels.

DDEI 7200



(1) Power-on indicator/button
(2) USB 2.0 connector
(3) Front video connector
(4) Optical drive
(5) System health and ID indicator
(6) Status LED indicators
(7) Hard drives
(8) iDRAC Direct port
(9) USB 2.0 connector
(10) Fiber NIC slot
(11) Management port eth0
(12) iDRAC port
(13) Serial connector
(14) System ID button
(15) Back video connector
(16) USB 3.0 connectors
(17) Data port eth1
(18) Data port eth2
(19) Data port eth3
(20) Power supply connectors

DDEI 9200

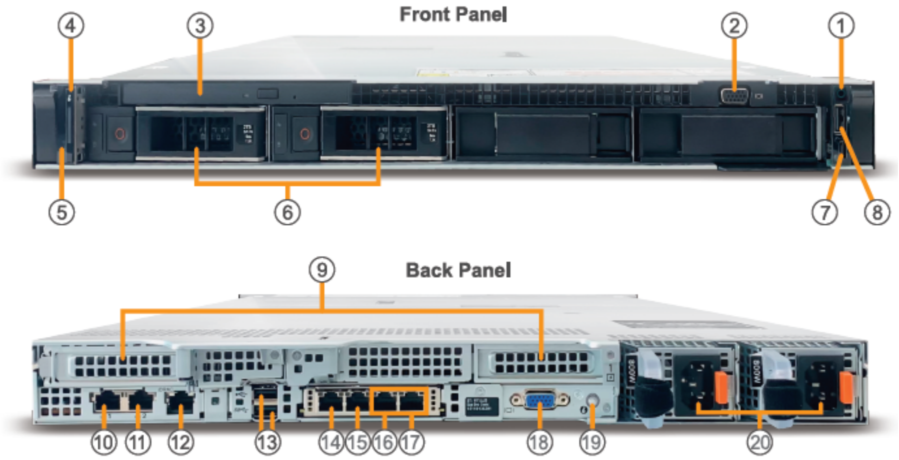


(1) Power-on indicator/button
(2) USB 2.0 connectors
(3) Optical drive
(4) System health and ID indicator
(5) Status LED indicators
(6) Hard drives
(7) iDRAC Direct port

(8) Front video connector
(9) System ID button
(10) iDRAC port
(11) Serial connector
(12) Back video connector
(13) USB 3.0 connectors
(14) Management port eth0

(15) Data port eth1
(16) Data port eth2
(17) Data port eth3
(18) Power supply connectors
(19) Fiber NIC slot

DDEI 7300



(1) Power-on indicator/button
(2) Front video connector
(3) Optical drive
(4) System health and ID indicator
(5) Status LED indicators
(6) Hard drives
(7) iDRAC Direct port

(8) USB 2.0 connector
(9) Expansion card slots
(10) Management port eth0
(11) Data port eth1
(12) iDRAC port
(13) USB 3.0 connectors
(14) Data port eth2

(15) Data port eth3
(16) Data port eth4
(17) Data port eth5
(18) Back video connector
(19) System ID button
(20) Power supply connectors

2.2. Hardware Specifications

The following table lists the hardware specifications for each DDEI model:

TrendMicro Model	DDEI 7100v2	DDEI 7200v1	DDEI 9200v1	DDEI 7300
Dell Model	R430	R440	R740 XL	R450
Memory	2.5 and lower: 64GB (16*4) RDIMM, 1833 MT/s, DDR4	64 GB (4*16GB) RDIMM, 2667 MT/s	128G (8*16GB) RDIMM, 2667 MT/s	64G (4x16GB) RDIMM, 2666 MT/s
	2.5 Sp1 and above: 64GB (16*4), RDIMM, 2133MT/s, DDR4			
iDRAC card	iDRAC7 enterprise	iDRAC9 Enterprise	iDRAC9 Enterprise	iDRAC9 Enterprise
Raid controller	PERC H330 integrated RAID controller	Perc H330	PERC H730P+	PERC H345 PERC H355
RAID setting	RAID 1	RAID 1	RAID 1	RAID 1
HDD	2.5″ SAS (10k RPM), 600 GB	3.5″ SATA (7.2k RPM) 1 TB * 2)	3.5" SATA (7.2K RPM) 4TB * 2	3.5" SATA (7.2 K RPM) 2TB * 2
DVD ROM/CF	DVD ROM, SATA	DVD ROM	DVD ROM	DVD ROM
NIC ports	4 ports on board	4x1 GbE	4x1 GbE	4 x 1GbE
NIC cards	[On-board] 2 x Broadcom 5720 Dual Port 1 GbE LOM	Broadcom 5720 dual port 1 GBe Network LOM	Intel Ethernet I350 QP	Broadcom Gigabit Ethernet BCM5720

TABLE 2.2.1.1: DDEI Hardware Specifications

TrendMicro Model	DDEI 7100v2	DDEI 7200v1	DDEI 9200v1	DDEI 7300
Power supply unit	Dual, hot plug, power supply (1+1) 550w	Redundant power supply 500w	Redundant power supply 750W	Redundant Power Supply 800W
Target throughput	400k emails/day	400k emails/day	800k emails/day	400K Emails /day
Supported DDEI SW version	2.1 or above	3.1 or above	3.1 or above	5.1
Max number of VA instance	30	30	60	30
Max number of VA image type	3	3	3	3
Notes	Motherboard changed to MLK new model since 2.5 SP1	none	none	none

TABLE 2.2.1.1: DDEI Hardware Specifications

2.3. Throughput and Performance

2.3.1. Throughput

The following table lists the throughput of different DDEI models including the maximum number of VA instances and images:

	DDEI 7200/7300	DDEI 9200
Email throughput per day	400k emails	800k emails
Max number of VA instances	30	60
Max number of VA images	3	3

TABLE 2.3.1.1: Throughput per DDEI Model

2.3.2. Performance

High performance is always the key index of messaging security gateway. This performance test was conducted to ensure that the product meets the performance requirement of the users.

The following are enhancements and new features the performance test focused on:

- Enable Gateway Module license only
- Support vmware ESXI 7.0
- Support TLS 1.3 for SMTP transmission
- Support DDD5.3 integration
- Support unknown recipient validation for inbound message
- Support New sandbox image

The table below shows the summary performance result:

Tested Platform	Test Result Conclusion
DDEI 7200 V1 Performance	Compared with DDEI 5.0 with win7 and win10 images, DDEI 7200 V1 Performance has a little downgrade whether DDEI is activated with an ATP license or activated by ATP and GM Licenses. The message throughput satisfies 400K messages per day
DDEI 9200 V1 Performance	Compared with DDEI 5.0 with win7 and win10SP3 images, DDEI 9200 V1 Performance has a little performance upgrade, whether DDEI is activated with an ATP license only or activated by ATP and GM Licenses. The message throughput satisfies 800K messages per day.

TABLE 2.3.1.2: Performance result summary

Tested Platform	Test Result Conclusion
VMWARE Compliance Performance	VMware compliance can support more than 600K/day throughput under 3vCPU, and more than 900K/day throughput under 6vCPU. The performance of VMware compliance on DDEI5.1 have a little downgrade and lower resource cost compared with DDEI5.0 under 3vCPU and 6vCPU. (CPU frequency is based on 2.3GHz and hard disk is based on 7200rpm).
Support TLS 1.3 & DANE for SMTP transmission	TLS1.3 and DANE check have only a little influence on DDEI mail delivery
Gateway license only Performance	Under the Gateway license only scenario, both hardware, and the virtual appliance can satisfy DDEI throughput.
Unknown recipients check Performance	Unknown recipients almost have no performance influence on DDEI5.1
New IMAGE Performance	WIN20_H1 image almost has obvious performance downgrade behavior compared with WIN10RS3 image and WIN19H2 image.
ESXI7.0 virtual appliance Performance	ESXI7.0 have a similar performance to ESXI6.5.

TABLE 2.3.1.2: Performance result summary

Here are the detailed performance test results conducted:

1. DDEI 7200 V1 Performance

- Policy Settings

Licenses	Policy Settings
ATP Only	Default policy
ATP & GM	50 policies with 100 AD users/groups, 2 AD groups in each policy. 40 incoming polices, 10 outgoing polices, and one default Policy. Change SPAM and Content Filter Rules Action as Pass & Tag, No DLP rule enable.

TABLE 2.3.1.3: DDEI 7200 V1 Policy Settings

- Test Result

Version	5.1 (fresh install)	5.0 (fresh install)	5.1 (fresh install)	5.0 (fresh install)
Hardware Model	7200 V1			
Firmware Version	5.1.0	5.0.0	5.1.0	5.0.0
Build Number	5.1.0.1117	5.0.0.1145	5.1.0.1117	5.0.0.1145
U-Sandbox Version	5.7.1123	5.6.1148	5.7.1123	5.6.1148
Sandcastle version	6.0.5106	6.0.4822	6.0.5106	6.0.4822

TABLE 2.3.1.4: DDEI 7200 V1 Test Results

Operation Mode	MTA			
License Type	ATP & GM		ATP	
Image type (Win 7/ Win 10)	12/18			
of Emails:*	2400			
of Spam Emails:*	4482	4530	0	0
of Emails which quarantined:*	192	192	126	126
of Email which delivered:*	23808	23808	23874	23874
of Attachments:*	3618	3618	3600	3600
of Attachments being sanboxed:*	528			
Avg. Latency for emails being sandboxed	0:04:37	0:04:06	0:04:48	0:04:45
Avg. CPU Usage	45.09%	50.86%	49.22%	49.86%
Avg. Mem Usage	62.18%	62.17%	60.89%	61.00%
Avg. Disk IO Usage	5.72$	5.20%	5.10%	4.64%
Total processing time	1:25:47	1:24:35	1:22:45	1:22:44
Total Throughput (msg/day)	402875 (98.6%)	408591 (100%)	417643 (99.98%)	417727 (100%)
Non SPAM throughput (msg/ day)	327638	331469	417643	417727
Total sandboxed samples per day:	8863	8886	9188	9190
cost disk size (KB)	584682	562719	280693	266965

TABLE 2.3.1.4: DDEI 7200 V1 Test Results

2. DDEI 9200 V1 Performance

- Policy Settings

Licenses	Policy Settings
ATP Only	Default policy
ATP & GM	20 policies with 50 AD users/groups, 2 or 3 AD groups in each policy. 16 incoming polices, 4 outgoing polices, and one default Policy. Change SPAM and Content Filter Rules Action as Pass & Tag, No DLP rule enable.

TABLE 2.3.1.5: DDEI 7200 V1 Policy Settings

- Test Result

Version	5.1 (fresh install)	5.0 (fresh install)	5.1 (fresh install)	5.0 (fresh install)
Hardware Model	9200 V1			
Firmware Version	5.1.0	5.0.0	5.1.0	5.0.0

TABLE 2.3.1.6: DDEI 9200 V1 Performance

Build Number	5.1.0.1117	5.0.0.1145	5.1.0.1117	5.0.0.1145
U-Sandbox Version	5.7.1123	5.6.1148	5.7.1123	5.6.1148
Sandcastle version	6.0.5106	6.0.4822	6.0.5106	6.0.4822
Operation Mode	MTA			
License Type	ATP	ATP	ATP & GM	ATP & GM
Image type (Win 7/ Win 10)	24/36			
of Emails:*	8000			
of Spam Emails:*	0	0	15388	15236
of Emails which quarantined:*	420	420	692	692
of Email which delivered:*	79580	79580	79308	79308
of Attachments:*	12000	12000	12048	12048
of Attachments being sanboxed:*	1760			
Avg. Latency for emails being sandboxed	0:04:20	0:04:44	0:04:54	0:03:49
Avg. CPU Usage	55.29%	67.80%	56.90%	72.58%
Avg. Mem Usage	59.13%	57.79%	58.27%	58.88%
Avg. Disk IO Usage	0.49%	0.54%	0.56%	0.61%
Total processing time	2:18:34	2:19:19	2:19:14	2:22:34
Total Throughput (msg/day)	831368 (100.54%)	826893 (100%)	827388 (102.4%)	808043 (100%)
Non SPAM throughput (msg/day)	831368	826893	668239	654151
Total sandboxed samples per day:	18290	18191	18202	17776
cost disk size (KB)	915012	894177	1900948	1878988

TABLE 2.3.1.6: DDEI 9200 V1 Performance

3. VMWARE Compliance Performance

- Policy Settings

Licenses	Policy Settings
ATP & GM	Default policy. Change SPAM and Content Filter Rules Action as Pass & Tag, No DLP rule enable.

TABLE 2.3.1.7: VMWARE Compliance Performance

- Test Results

Test Result for VMware compliance Test Results without dlp rules under 3vCPU

No.	1	2	3	4	5	6
Email Volume	4msg/sec (disable dlp)	4msg/sec (disable dlp)	8msg/sec (disable dlp)	8msg/sec (disable dlp)	12msg/sec (disable dlp)	12msg/sec (disable dlp)
Total Cores	3vCPU					
Total Mem	10GB					
Avg. CPU Usage	134.26%	34.22%	53.52%	55.73%	70.18%	74.86%
Avg. Mem Usage	33.91%	34.47%	32.05%	33.34%	32.04%	32.74%
Avg. Disk IO Usage	0.40%	2.86%	0.65%	4.00%	0.91%	4.86%
Build Number	5.1.0.1117	5.1.0.1101	5.1.0.1117	5.1.0.1101	5.1.0.1117	5.1.0.1101
License Type	ATP & GM					
# of Emails	2400					
# of Spam Emails	4476	4511	4476	4512	4476	4512
# of Emails which quarantined	192	204	192	204	192	204
# of Email which delivered	23808	23796	23808	23796	23796	23796
# of Attachments	3618					
# of Attachments being sanboxed:*	528					
Avg. Latency for emails being sandboxed (including URL)	0:00:16	0:00:17	0:00:19	0:00:19	0:00:18	0:00:20
Total processing time:	1:43:58	1:41:08	0:54:16	0:52:36	0:37:13	0:36:18
Total Throughputs (msg/day)	332414 (97.3%)	341727 (100%)	636855 (97.7%)	657034 (100%)	928616 (97.6%)	952066 (100%)
Non SPAM throughput (msg/day)	2760418	277496	818081	533511	755467	773077
Total sandboxed samples per day	7331	7535	14469	14932	20911	21447

TABLE 2.3.1.8: VMware compliance Test Results without dlp rules under 3vCPU

Test Result for VMware compliance Test Results without dlp rules under 6vCPU

No.	1	2	3	4	5	6
Email Volume	4msg/sec (disable dlp)	4msg/sec (disable dlp)	8msg/sec (disable dlp)	8msg/sec (disable dlp)	12msg/sec (disable dlp)	12msg/sec (disable dlp)
Total Cores	6vCPU					
Total Mem	16GB					

TABLE 2.3.1.9: VMware compliance Test Results without dlp rules under 6vCPU

Avg. CPU Usage	16.97%	17.35%	26.65%	28.12%	34.47%	39.59%
Avg. Mem Usage	19.60%	22.65%	18.82%	22.12%	18.00%	21.81%
Avg. Disk IO Usage	0.39%	1.56%	0.61%	2.45%	1.20%	4.29%
Build Number	5.1.0.1117	5.1.0.1101	5.1.0.1117	5.1.0.1101	5.1.0.1117	5.1.0.1101
License Type	ATP & GM					
# of Emails	2400					
# of Spam Emails	4476	4512	4476	4512	4476	4526
# of Emails which quarantined	192	203	192	204	192	204
# of Email which delivered	23808	23797	23808	23796	23808	23796
# of Attachments	3618					
# of Attachments being sanboxed:*	528					
Avg. Latency for emails being sandboxed (including URL)	0:00:19	0:00:18	0:00:21	0:00:19	0:00:20	0:00:19
Total processing time:	1:43:57	1:41:07	0:53:53	0:52:38	0:37:19	0:36:25
Total Throughputs (msg/day)	332467 (97.3%)	341783 (100%)	641385 (97.7%)	656618 (100%)	926127 (97.6%)	949016 (100%)
Non SPAM throughput (msg/day)	270462	277528	521767	533173	753404	770047
Total sandboxed samples per day	7314	7519	14110	14445	20374	20878

TABLE 2.3.1.9: VMware compliance Test Results without dlp rules under 6vCPU

4. Support TLS 1.3 & DANE for SMTP transmission test result

Version	5.1 (fresh install)		
Hardware Model	7100 V2		
downstream configuration	No TLS	TLS 1.3	DANE
Build Number	5.1.0.1142		
U-Sandbox Version	5.7.1137		
Sandcastle version	6.0.5112		
Operation Mode	MTA		
License Type	ATP		
Image type (Win 7/ Win 10)	12/18		

TABLE 2.3.1.10: Support TLS 1.3 & DANE for SMTP transmission

of Emails:*	24000		
of Spam Emails:*	0		
of Emails which quarantined:*	126		
of Email which delivered:*	23874		
of Attachments:*	3600		
of Attachments being sanboxed:*	528		
Avg. Latency for emails being sandboxed	0:04:10	0:04:11	0:04:13
Avg. CPU Usage	47.00%	46.59%	47.20%
Avg. Mem Usage	61.40%	60.70%	62.41%
Avg. Disk IO Usage	32.08%	32.17%	32.20%
Total processing time	1:29:57	1:30:13	1:30:18
Total Throughput (msg/day)	384213 (100%)	383077 (99.7%)	382724 (99.61%)
Non SPAM throughput (msg/day)	384213	383077	387224
Total sandboxed samples per day:	8452	8427	8419
cost disk size (KB)	343774	346551	342665

TABLE 2.3.1.10: Support TLS 1.3 & DANE for SMTP transmission

5. Gateway license only performance

- Policy Settings

Hardware platform	DDEI7200V1	VMware appliance
Policy	20 policies with 50 AD users/groups involved, 2 or 3 AD groups in each policy. 16 incoming polices, 4 outgoing polices, and one default Policy, change SPAM and Content Filter Rules Action as Pass & Tag and no DLP rule.	20 policies with 50 AD users/groups involved, 2 or 3 AD groups in each policy. 16 incoming polices, 4 outgoing polices, and one default Policy, change SPAM and Content Filter Rules Action as P ass & Tag, and 4 DLP rules per policy.

TABLE 2.3.1.11: Gateway license policy setting

- Test results

No.	1	2	3	4
Email Volume	16msg/sec (disable dlp)	12msg/sec (disable dlp)	8msg/sec (disable dlp)	4msg/sec (disable dlp)

TABLE 2.3.1.12: Gateway license under DDEI 7200 V1

Hardware Platform	DDEI 7200 V1			
Avg. CPU Usage	16.20%	14.50%	11.93%	8.48%
Avg. Mem Usage	9.90%	9.30%	9.34%	9.65%
Avg. Disk IO Usage	7.49%	7.26%	4.59%	3.61%
Build Number	5.1.0.1153			
License Type	GM			
# of Emails	2400			
# of Spam Emails	4482			
# of Emails which quarantined	180			
# of Email which delivered	23820			
# of Attachments	3612			
# of Attachments being sanboxed:*	528			
Avg. Latency for emails being sandboxed (including URL)	0:00:24	0:00:22	0:00:23	0:00:20
Total processing time:	0:31:26	0:38:25	0:55:13	1:45:18
Total Throughputs (msg/day)	1099469 (100%)	899609 (100%)	625897 (100%)	328205 (100%)
Non SPAM throughput (msg/day)	894143	731607	509011	266912
Total sandboxed samples per day	24188	19791	13769	7220

TABLE 2.3.1.12: Gateway license under DDEI 7200 V1

No.	1	2	3	4
Email Volume	16msg/sec (disable dlp)	12msg/sec (disable dlp)	8msg/sec (disable dlp)	4msg/sec (disable dlp)
Hardware Platform	vmware appliance			
Avg. CPU Usage	23.03%	19.49%	15.44%	10.72%
Avg. Mem Usage	13.25%	13.18%	13.24%	13.28%
Avg. Disk IO Usage	11.55%	9.14%	7.10%	5.03%
Build Number	5.1.0.1153			
License Type	GM			
# of Emails	2400			

TABLE 2.3.1.13: Gateway license under virtual appliance

# of Spam Emails	4482			
# of Emails which quarantined	180			
# of Email which delivered	23820			
# of Attachments	3612			
# of Attachments being sanboxed:*	528			
Avg. Latency for emails being sandboxed (including URL)	0:00:24	0:00:22	0:00:22	0:00:22
Total processing time:	0:31:14	0:38:55	0:55:20	1:45:26
Total Throughputs (msg/day)	1106510 (100%)	888051 (100%)	624578 (100%)	327790 (100%)
Non SPAM throughput (msg/day)	899935	722207	507938	266575
Total sandboxed samples per day	24343	19537	13740	7211

TABLE 2.3.1.13: Gateway license under virtual appliance

6. Unknown recipients check Performance

- Policy Settings

Settings	I	II
Unknown recipients check Performance	Disable	Enabled

- Test Results

Version	5.1 (fresh install)	5.0 (fresh install)
Hardware Model	7100 V1	7100 V1
unknown recipeints configuration	enabled	disabled
Build Number	5.1.0.1153	
U-Sandbox Version	5.7.1137	
Sandcastle version	6.0.5112	
Operation Mode	MTA	
License Type	ATP & GM	
Image type (Win 7/ Win 10)	12/18	
of Emails:*	24000	

TABLE 2.3.1.14: Unknown recipients check Performance

of Spam Emails:*	4482	
of Emails which quarantined:*	192	
of Email which delivered:*	23808	
of Attachments:*	3612	
of Attachments being sanboxed:*	528	
Avg. Latency for emails being sandboxed	0:04:36	0:04:40
Avg. CPU Usage	46.58%	46.56%
Avg. Mem Usage	64.61%	64.37%
Avg. Disk IO Usage	8.68%	7.65%
Total processing time	1:29:13	1:29:21
Total Throughput (msg/day)	387371(100%)	386793 (99.7%)
Non SPAM throughput (msg/day)	315029	314559
Total sandboxed samples per day:	8522	8509

TABLE 2.3.1.14: Unknown recipients check Performance

7. New IMAGE Performance

- Policy Settings

Settings	I	II	III
Image type	WIN10RS3_X64	IN10_20H1	WIN10_19H2

- Test Result

Version	5.1 (fresh install)	5.0 (fresh install)	5.1 (fresh install)
Hardware Model	9200 V1	9200 V1	9200 V1
image type	WIN10_20H1	WIN10_20H1	WIN10_20H1
office version	Office 13_16	Office 13_16	Office 13_16
Image number	60		
Build Number	5.1.0.1161		
U-Sandbox Version	5.7.1137		
Sandcastle version	6.0.5112		
Operation Mode	MTA		
License Type	ATP & GM		

TABLE 2.3.1.15: New IMAGE Performance

of Emails:*	8000		
of Spam Emails:*	15236		
of Emails which quarantined:*	692		
of Email which delivered:*	79308		
of Attachments:*	12048		
of Attachments being sanboxed:*	1760		
Avg. Latency for emails being sandboxed	0:03:05	0:04:13	0:03:08
Avg. CPU Usage	76.49%	74.51%	75.54%
Avg. Mem Usage	62.97%	62.91%	62.79%
Avg. Disk IO Usage	1.58%	0.93%	2.22%
Total processing time	1:38:41	1:17:28	1:31:46
Total Throughput (msg/day)	1167370 (87.79%) (compared with WIN 10 SP3)	1317073 (100%)	1255357 (95.31%) (compared with WIN 10 SP3)
Non SPAM throughput (msg/day)	945030	1066236	1016274
Total sandboxed samples per day:	25437	28975	27617

TABLE 2.3.1.15: New IMAGE Performance

ESXI7.0 virtual appliance Performance

- Policy

Licenses	Policy Settings
ATP & GM	Default policy. Change SPAM and Content Filter Rules Action as Pass & Tag, No DLP rule enable.

- Test Result

No.	1	2	3	4	5	6	7	8
Email Volume	4msg/sec (disable dlp)	4msg/sec (disable dlp)	8msg/sec (disable dlp)	8msg/sec (disable dlp)	12msg/sec (disable dlp)	12msg/sec (disable dlp)	16msg/sec (disable dlp)	16msg/sec (disable dlp)
Total Cores	3vCPU							
Total Mem	10GB							
Avg. CPU Usage	33.44%	33.22%	47.67%	46.60%	58.30%	56.09%	63.35%	62.33%

TABLE 2.3.1.16: virtual appliance(3vCPU) Test Results

Avg. Mem Usage	34.36%	35.44%	33.90%	35.84%	32.71%	35.74%	32.18%	35.37%
Avg. Disk IO Usage	0.34%	1.28%	0.49%	2.78%	0.61%	2.34%	0.76%	2.46%
Build Number	5.1.0.1117							
ESXI Version	7.0	6.0	7.0	6.0	7.0	6.0	7.0	6.0
License Type	ATP & GM							
# of Emails	2400							
# of Spam Emails	4482							
# of Emails which quarantined	192							
# of Email which delivered	23808	23808	23832	23808	23832	23808	23808	23808
# of Attachments	3612							
# of Attachments being sanboxed:*	528							
Avg. Latency for emails being sandboxed (including URL)	0:00:16	0:00:15	0:00:18	0:00:16	0:00:18	0:00:16	0:00:18	0:00:16
Total processing time:	2:01:24	2:01:05	1:11:57	1:11:05	0:54:17	0:54:19	0:45:59	0:45:47
Total Throughputs (msg/day)	284678 (99.74%)	285423 (100%)	480333 (97.7%)	486189 (100%)	636659 (100%)	636268 (97.6%)	751576 (99.93%)	752121 (100%)
Non SPAM throughput (msg/day)	231514	232120	390631	395393	517763	517445	611219	6111663
Total sandboxed samples per day	6262	6279	10567	1096	14836	13997	16594	16606

TABLE 2.3.1.16: virtual appliance(3vCPU) Test Results

No.	1	2	3	4	5	6	7	8
Email Volume	4msg/sec (disable dlp)	4msg/sec (disable dlp)	8msg/sec (disable dlp)	8msg/sec (disable dlp)	12msg/sec (disable dlp)	12msg/sec (disable dlp)	16msg/sec (disable dlp)	16msg/sec (disable dlp)
Total Cores	6vCPU							
Total Mem	16GB							
Avg. CPU Usage	16.93%	17.78%	24.13%	24.08%	29.17%	29.32%	32.41%	32.22%
Avg. Mem Usage	22.37%	26.73%	23.72%	26.88%	22.94%	27.13%	22.28%	27.45%
Avg. Disk IO Usage	0.34%	1.28%	0.48%	1.71%	0.79%	2.57%	2.11%	2.26%
Build Number	5.1.0.1117							
ESXI Version	7.0	6.0	7.0	6.0	7.0	6.0	7.0	6.0

TABLE 2.3.1.17: virtual appliance(6vCPU) Test Results

License Type	ATP & GM							
# of Emails	2400							
# of Spam Emails	4482							
# of Emails which quarantined	192							
# of Email which delivered	23808							
# of Attachments	3612							
# of Attachments being sanboxed:*	528							
Avg. Latency for emails being sandboxed (including URL)	0:00:16	0:00:16	0:00:16	0:00:18	0:00:18	0:00:16	0:00:19	0:00:18
Total processing time:	2:01:37	2:01:22	1:11:32	1:11:01	0:54:33	0:54:13	0:46:09	0:45:53
Total Throughputs (msg/day)	284171 (99.81%)	284717 (100%)	483131 (97.28%)	486646 (100%)	633547 (99.39%)	637442 (100%)	748862 (99.42%)	753214 (100%)
Non SPAM throughput (msg/day)	231102	231546	392906	395765	515232	518400	609062	612551
Total sandboxed samples per day	6336	6263	10810	10706	14097	14023	16367	16463

TABLE 2.3.1.17: virtual appliance(6vCPU) Test Results

Lesson 3: Deployment

DDEI has three deployment modes, MTA, BCC, and SPAN/TAP mode. The following table summarizes the advantages and disadvantages of the DDEI operation modes:

Mode	Advantages	Disadvantages
MTA	• Convenient for configuration • All mails are scanned by DDEI • Can get the accurate mail info • Can interfere with mail routing • Load balancing	• Needs to change mail routing • Might causes a single point issue
BCC	• Does not affect current mail flow • Load balancing	• Mail header info might be incorrect • Does not interfere with mail routing • Recipient notification does not work in BCC mode • BCC capability is required on the existing MTA
SPAN/TAP	• Convenient for deployment • Does not affect current mail flow • Can get accurate mail info	• Cannot scan encrypted traffic • Does not interfere with mail routing • Need to mirror the SMTP traffic

TABLE 3.1.1.1: DDEI Deployment Models Comparisson

The administrator can select the deployment mode based on their requirement.

3.1. MTA Mode

In MTA mode, DDEI works as inline MTA.

The Sender Filtering feature can work when DDEI is in MTA mode and Gateway Module license is activated.

3.1.1. Edge/None Edge Deployment

DDEI Sender Filtering can block senders of spam messages at the IP address of the sender email address level before the policy engine scans the message.

When deploying DDEI as edge, Sender Filtering extracts the sender IP address from SMTP protocol, and the scanner uses the first public IP as the sender IP.

If DDEI serves as an edge MTA in the network, the administrator should specify the edge MTA relay servers:

Administration > **Mail Settings** > **Edge MTA Relay Servers**

In non-edge mode, Sender Filtering (ERS, DHA, Bounce), and the scanner checks the sender IP address before edge MTA. It extracts the sender IP address from the message header (`Received:`) and uses the first Received non-edge IP below the Edge MTA Relay Server as the sender IP.

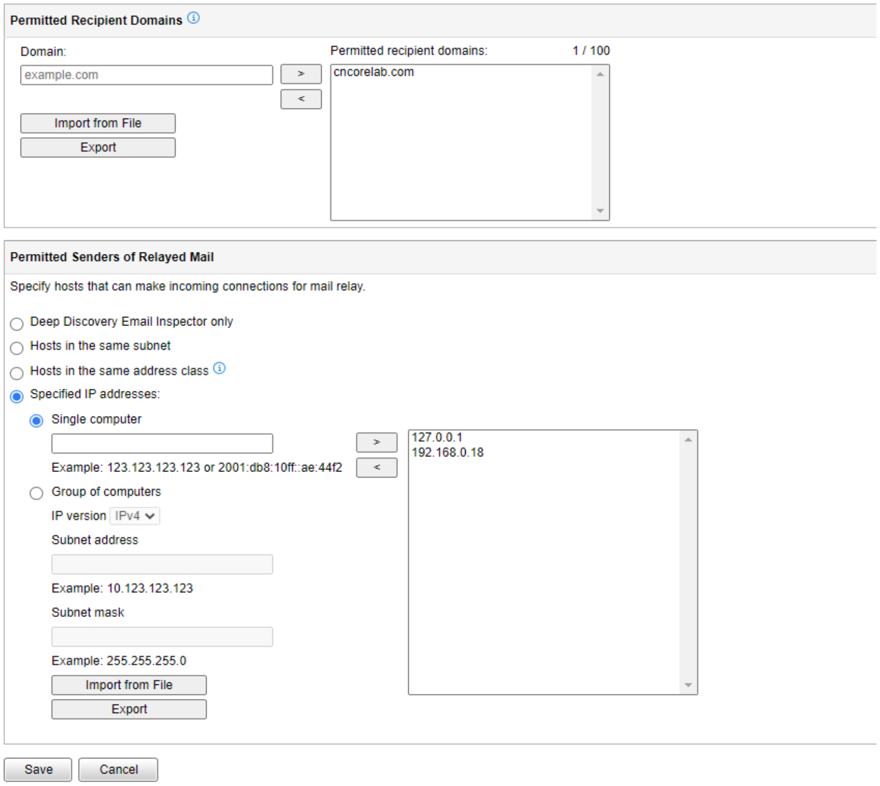
3.1.2. Initial Configuration for MTA Mode

The following are the DDEI default settings:

- IP / Mask: 192.168.252.1 / 255.255.0.0
- Username: `admin`
- Password: `ddei`

For fresh DDEI installation, DDEI is in MTA deployment mode. Use the following steps for the initial MTA Mode configuration:

1. When logging in for the first time, a pop-up window will ask to reset and use a strong password, follow the instructions and reset the log-in password
2. Configure the hostname and network setting. Go to **Administration** > **System Settings** > **Network**, configure the hostname and network setting
3. Activate DDEI: Go to **Administration** > **License**, and enter the Activation Code to activate DDEI
4. Double-check the Operation Mode: Go to **Administration** > **System Settings** > **Operation Mode** and make sure it is on *MTA* mode.
5. Configure the Time setting: Go to **Administration** > **System Settings** > **Time**, set the correct time and time zone
6. Configure the update schedule: Go to **Administration** > **Component Updates** > **Schedule**. The recommended interval setting is 15 minutes
7. Set the Recipient Domains and Permitted Senders. Go to **Administration** > **Mail Settings** > **Limits and Exceptions**, "*Permitted Recipient Domains*" means "Incoming Message Domains", add all internal domains in your network into the list so that DDEI can accept the messages sent to those domains. "*Permitted Senders or Relayed Mail*" means the listed hosts can relay mail to all domains. Typically, the mail server (or outbound MTA) is added to the list to relay the outbound messages from the mail server to DDEI for scanning. Then DDEI relays the outbound messages out after scanning



Permitted Recipient Domains

Domain: example.com

Import from File

Export

Permitted recipient domains: 1 / 100

cncorelab.com

Permitted Senders of Relayed Mail

Specify hosts that can make incoming connections for mail relay.

○ Deep Discovery Email Inspector only

○ Hosts in the same subnet

○ Hosts in the same address class

● Specified IP addresses:

● Single computer

Example: 123.123.123.123 or 2001:db8:10ff::ae:44f2

127.0.0.1
192.168.0.18

○ Group of computers

IP version IPv4

Subnet address

Example: 10.123.123.123

Subnet mask

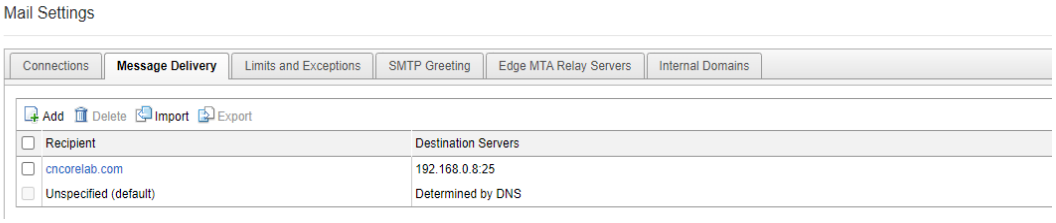
Example: 255.255.255.0

Import from File

Export

Save Cancel

8. Set Message Delivery: Go to **Administration** > **Mail Settings** > **Message Delivery**, set the delivery method for internal domains. Most of the time, select "***Specify servers***" to deliver the incoming mails to the mail server. For multiple destination servers, the lower the priority value, the higher the priority. With the same priority, multiple destination MTA can do load balancing. For outgoing messages from the mail server, DDEI can use DNS to deliver to the Internet directly

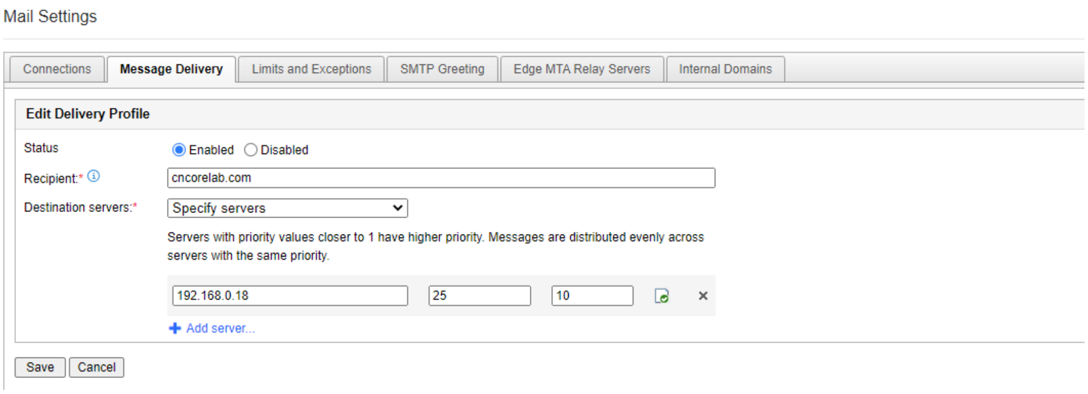


Mail Settings

Connections | **Message Delivery** | Limits and Exceptions | SMTP Greeting | Edge MTA Relay Servers | Internal Domains

Add Delete Import Export

□	Recipient	Destination Servers
□	cncorelab.com	192.168.0.8:25
□	Unspecified (default)	Determined by DNS



Edit Delivery Profile

Status: ● Enabled ○ Disabled

Recipient:* cncorelab.com

Destination servers:* Specify servers

Servers with priority values closer to 1 have higher priority. Messages are distributed evenly across servers with the same priority.

192.168.0.18 | 25 | 10

9. Enable TLS for SMTP connection. Go to **Administration** > **Mail Settings** > **Connections**, then under the ***Transport Layer Security*** section, select any of the following to enable TLS:

- ***Enable incoming TLS*** – This means DDEI is the SMTP server and uses TLS to accept messages. Enable this when using edge deployment
- ***Enable outgoing TLS*** – This means DDEI is the SMTP client and uses TLS to send messages. Enable this option if DDEI needs to scan the outbound mails

10. Set Contacts. This allows DDEI to send alerts and reports to specified contacts. Go to **Administration** > **Accounts / Contacts** > **Contacts**. Type the email addresses of the alert notification and report recipients
11. Verify the DDEI working status:

- Go to **Administration** > **Component Updates**. DDEI should have the latest components.
- Send several test emails (With at least one email containing eicar test virus) from the mail client to DDEI via SMTP. DDEI should be able to process it successfully.
- Go to **Logs** > **Message Tracking**. The message tracking log for those test emails should be displayed.
- Go to **Detections** > **Detected Messages**. The message with the test virus should be displayed.

12. Other configurations:

- Set the Proxy Settings if DDEI has no direct access to the Internet. Go to **Administration** > **System Settings** > **Proxy**. Set the Proxy Server info
- Set the SMTP Notification Server. For MTA Mode, DDEI uses the Internal Postfix Server as the notification server. Keep this setting at default
- Change the default 10 MB maximum message size. This can be adjusted by going to **Administration** > **Mail Settings** > **Limits and Exceptions**. The maximum message size setting is under the *Message Limits* section
- To configure Virtual Analyzer, refer to Integrating with Virtual Analyzer
- To configure the integrated products and services, refer to Integrated Products/Services
- To check the policy settings, refer to Policy Settings. Adjust the policy settings if the default policy settings do not meet the requirement.

3.2. BCC Mode

In BCC mode, the existing MTA should have BCC capability and set to BCC the messages to DDEI. DDEI scans the mails received from MTA. After scanning, DDEI drops those email copies. As the messages were BCC'ed from MTA to DDEI, DDEI cannot get the real recipient address from the envelope, and it displays the mail header address instead in the log query page.

3.2.1. Initial Configuration for BCC Mode

The following are the DDEI default settings:

- IP / Mask: 192.168.252.1 / 255.255.0.0
- Username: `admin`
- Password: `ddei`

For fresh DDEI installation, DDEI is in MTA deployment mode. Use the following steps for the initial BCC Mode configuration:

1. When logging in for the first time, a pop-up window will ask to reset and use a strong password, follow the instructions and reset the log-in password
2. Configure the hostname and network setting. Go to **Administration** > **System Settings** > **Network**, configure the hostname and network setting
3. Activate DDEI: Go to **Administration** > **License**, and enter the Activation Code to activate DDEI
4. Double-check the Operation Mode: Go to **Administration** > **System Settings** > **Operation Mode** and select *BCC* mode. This change requires DDEI to restart
5. Set the SMTP Notification Server. BCC Mode cannot use the internal Postfix server as the notification server. DDEI should use an external SMTP server as the notification server to send email notifications. To do this, go to **Administration** > **System Settings** > **SMTP** and set the External SMTP server
6. Configure the Time setting: Go to **Administration** > **System Settings** > **Time**, set the correct time and time zone
7. Configure the update schedule: Go to **Administration** > **Component Updates** > **Schedule**. The recommended interval setting is 15 minutes
8. Set the ***Permitted Senders*** to allow the MTA to relay messages to DDEI. In BCC mode, add the MTA that will BCC the messages to DDEI into the ***Permitted Senders*** list. It does not need to set the delivery method since DDEI will drop the messages after scanning. Go to ***Administration*** > ***Mail Settings*** > ***Limits and Exceptions***, under ***Permitted Senders or Relayed Mail*** section, add the MTA that will BCC the messages to DDEI into the Specified IP addresses list
9. Set Contacts. This allows DDEI to send alerts and reports to specified contacts. Go to **Administration** > **Accounts / Contacts** > **Contacts**. Type the email addresses of the alert notification and report recipients
10. On the MTA, set to BCC the messages to DDEI. The following Knowledge Base article links on how to configure MTA on several products to BCC the messages to DDEI:

- TrendMicro InterScan Messaging Security Virtual Appliance (IMSVA) https://success.trendmicro.com/solution/1113257
- McAfee Email Gateway (MEG) https://success.trendmicro.com/solution/1113258

- Symantec Messaging Gateway https://success.trendmicro.com/solution/1113259
- Barracuda Email Security Gateway https://success.trendmicro.com/solution/1119972

11. Verify the DDEI working status.

- Go to **Administration** > **Component Updates**. DDEI should have the latest components
- Send several test emails (With at least one email containing eicar test virus) from the mail client to DDEI via SMTP. DDEI should be able to process it successfully
  - If sending from a mail client, add the mail client to DDEI's permitted senders' list
- Go to **Logs** > **Message Tracking**. The message tracking log for those test emails should be displayed
- Go to **Detections** > **Detected Messages**. The message with the test virus should be displayed. As the messages were BCC'ed from MTA to DDEI, DDEI cannot get the real recipient address from the envelope and displays the mail header address instead in the log query page.

12. Other configurations:

- Set the Proxy Settings if DDEI has no direct access to the Internet. Go to **Administration** > **System Settings** > **Proxy**. Set the Proxy Server info
- Set the SMTP Notification Server. For MTA Mode, DDEI uses the Internal Postfix Server as the notification server. Keep this setting at default
- Change the default 10 MB maximum message size. This can be adjusted by going to **Administration** > **Mail Settings** > **Limits and Exceptions**. The maximum message size setting is under the *Message Limits* section
- To configure Virtual Analyzer, refer to Integrating with Virtual Analyzer
- To configure the integrated products and services, refer to Integrated Products/Services
- To check the policy settings, refer to Policy Settings. Adjust the policy settings if the default policy settings do not meet the requirement.

3.3. SPAN/TAP Mode

In SPAN/TAP mode, the existing SMTP routing does not need to be changed. Instead, the administrator should configure a switch or a network tap to send mirrored traffic to DDEI. DDEI receives the mirrored traffic and checks for SMTP traffic that allows it to scan email messages. After scanning, DDEI discards all replicated email messages and does not deliver replicated email messages to recipients.

NOTE:

- In a Port Binding scenario, only eth3 is used for SMTP data traffic checking.
- When the DDEI server has a plug-in NIC card, then the TAP mode port should be the last two NIC ports.

After scanning, DDEI discards all replicated email messages and does not deliver replicated email messages to recipients. To successfully analyze the SMTP traffic, the SMTP traffic in the mirrored traffic must not be encrypted. Disable TLS on the current mail gateway to address this requirement.

3.3.1. Initial Configuration for SPAN/TAP Mode

The following are the DDEI default settings:

- IP / Mask: 192.168.252.1 / 255.255.0.0
- Username: `admin`
- Password: `ddei`

For fresh DDEI installation, DDEI is in MTA deployment mode. Use the following steps for the initial to use SPAN/TAP mode:

1. Disable the SMTP TLS feature between the mail gateway server and the mail server. The SMTP traffic between the mail gateway server and the mail server would be not be encrypted.
2. Configure a switch or a network tap to mirror the traffic which contains the SMTP traffic between the mail gateway server and the mail server, then sends the mirrored traffic to DDEI's eth2 or eth3 port.

```
Core_2960G#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Core_2960G(config)#monitor session 2 source interface gi0/48
Core_2960G(config)#monitor session 2 destination interface gi0/10
Core_2960G(config)#exit
Core_2960G#sh monitor session 2
Session 2
---------
Type : Local Session
Source Ports :
Both : Gi0/48
```

```
Destination Ports : Gi0/10
Encapsulation : Native
Ingress : Disabled
Core_2960G#
```

3. When logging in for the first time, a pop-up window will ask to reset and use a strong password, follow the instructions and reset the log-in password
4. Configure the hostname and network setting. Go to **Administration** > **System Settings** > **Network**, configure the hostname and network setting
5. Activate DDEI: Go to **Administration** > **License**, and enter the Activation Code to activate DDEI
6. Double-check the Operation Mode: Go to **Administration** > **System Settings** > **Operation Mode** and select *SPAN/TAP* mode. This change requires DDEI to restart
7. Set the SMTP Notification Server. SPAN/TAP Mode cannot use the internal Postfix server as the notification server. DDEI should use an external SMTP server as the notification server to send email notifications. To do this, go to **Administration** > **System Settings** > **SMTP** and set the External SMTP server
8. Configure the Time setting: Go to **Administration** > **System Settings** > **Time**, set the correct time and time zone
9. Configure the update schedule: Go to **Administration** > **Component Updates** > **Schedule**. The recommended interval setting is 15 minutes
10. Set Contacts. This allows DDEI to send alerts and reports to specified contacts. Go to **Administration** > **Accounts / Contacts** > **Contacts**. Type the email addresses of the alert notification and report recipients
11. Verify the DDEI working status.

- Go to **Administration** > **Component Updates**. DDEI should have the latest components
- Go to **Logs** > **Message** Tracking. The message tracking log should display the messages in the mirrored traffic.
- Go to **Detections** > **Detected Messages**. It should display detected malware or spam messages (Gateway Module activated)

12. Other configurations:

- Set the Proxy Settings if DDEI has no direct access to the Internet. Go to **Administration** > **System Settings** > **Proxy**. Set the Proxy Server info
- To configure Virtual Analyzer, refer to Integrating with Virtual Analyzer
- To configure the integrated products and services, refer to Integrated Products/Services

- To check the policy settings, refer to Policy Settings. Adjust the policy settings if the default policy settings do not meet the requirement.

Lesson 4: Virtual Analyzer Integration

Virtual Analyzer uses system images to observe sample behavior and characteristics within an isolated and controllable virtual environment then assigns a risk level to the sample. DDEI can either use an internal Virtual Analyzer or external Virtual Analyzer (via DDAN) to analyze the suspicious email message. This helps find the potential threats at an early stage.

NOTE: vDDEI can only use the External Virtual Analyzer to analyze suspicious email messages

4.1. Preparing the Virtual Analyzer Image

To prepare the Virtual Analyzer Image, refer to the "Virtual Analyzer Image Preparation" section on page 258 of the DDEI 5.1 Administration Guide.

TIP: Configure the images similar to the setup that the organization use

Use the Virtual Analyzer Image Preparation Tool to create custom sandbox images to support the DDEI deployment. Refer to the following link on how to use it:

http://docs.trendmicro.com/en-us/enterprise/virtual-analyzer-image-preparation.aspx

4.2. Enabling the Virtual Analyzer

If DDAN (Deep Discovery Analyzer) is present in the environment, DDEI can use it to serve as an external Virtual Analyzer. If there is no DDAN in the environment, use the DDEI internal Virtual Analyzer.

4.2.1. External Virtual Analyzer

Refer to the following steps on how to integrate DDEI with DDAN:

1. Open the DDAN web console.
2. Go to **Help** > **About** and get the API key
3. Open the DDEI web console
4. Go to **Administration** > **Scanning / Analysis** > **External Integration**
5. Set **Source** to *External*, then provide the DDAN server's address and API key
6. Save the configuration.

4.2.2. Internal Virtual Analyzer

Use the following steps on how to use the DDEI Internal Virtual Analyzer:

1. Open the DDEI web console.
2. Go to **Administration** > **Scanning / Analysis** > **External Integration**.
3. Set Source to Internal, then save the configuration.
4. Go to **Administration** > **Scanning / Analysis** > **Overview** > **Images**.
5. Import the images.

- See "Preparing the Virtual Analyzer Image" on page 30 on how to prepare the image
- Use the image information as the image name such as "Win10 EN x64"
- Use either the import tool or HTTP/FTP to import the image.
- Set the instance value to 1 when importing the image and adjust it when the import is complete

6. Wait until the import is successful.

4.3. Updating the File Submission Rules

After enabling the Virtual Analyzer, DDEI 5.1 submits detected non-malicious files to the virtual analyzer for further analysis.

Adjust the file type settings based on the organization’s setup, considering the mail traffic, DDEI performance, and virtual analyzer scanning performance.

To configure the Submission Filters:

1. Open the DDEI web console
2. Go to **Administration** > **Scanning / Analysis** > **Settings** > **Submission Filters**.

NOTE: For the Submission Timeout setting, keep it at the default setting of 20 minutes

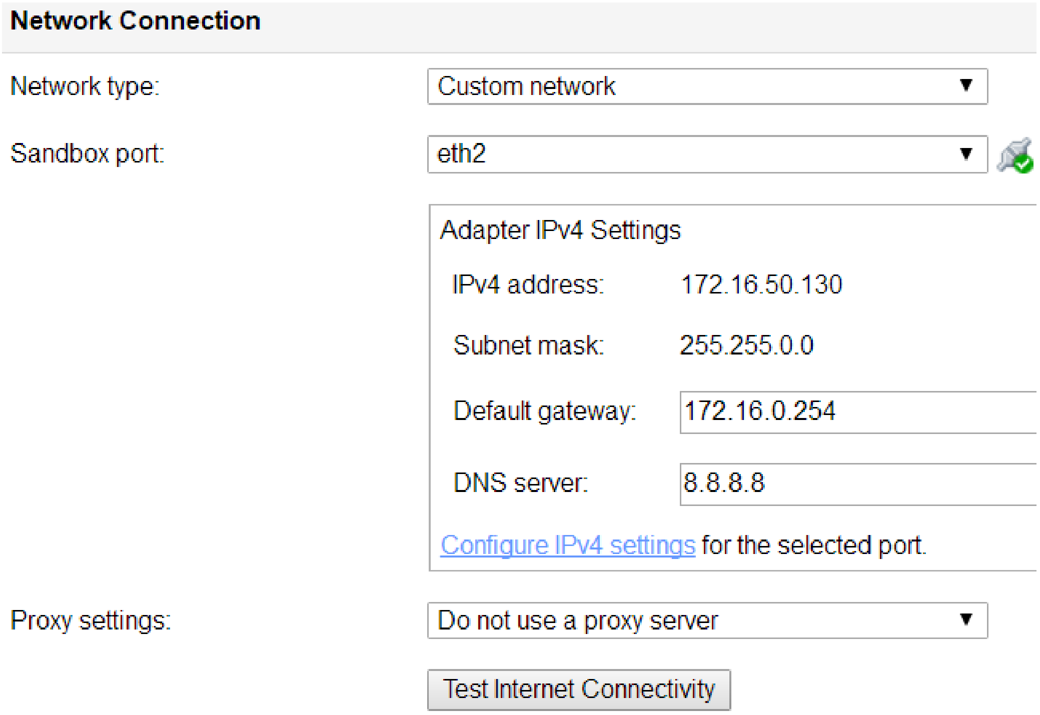
However, the Virtual Analyzer requires more resources if more files are selected. If the Virtual Analyzer cannot handle the submitted files in time, the samples will queue in the Virtual Analyzer queue.

4.4. Internal Virtual Analyzer Network Connection

The internal Virtual Analyzer can obtain more accurate results if it has Internet Access. However, this network should be isolated so that malicious samples do not affect other networks. For security considerations, use a custom network for the Virtual Analyzer to use for Internet access and sample analysis. Use any available network interface (eth1, eth2, eth3) that is not used for the mail network.

Do the following to configure the custom network for the virtual analyzer

1. Determine the network interface (eth1, eth2, or eth3) that will be used for the custom network and connect the isolated network cable to this network interface
2. Open the DDEI web console
3. Go to **Administration** > **System Settings** > **Network**
4. Configure the IPv4 info for the dedicated network interface
5. Go to **Administration** > **Scanning / Analysis** > **Settings** > **Network Connection**
6. Set Network type to Custom network then set the Sandbox port to the dedicated network interface
7. Configure the gateway and DNS server to this dedicated interface and save the settings



Network Connection

Network type: Custom network ▼

Sandbox port: eth2 ▼

Adapter IPv4 Settings

IPv4 address: 172.16.50.130

Subnet mask: 255.255.0.0

Default gateway: 172.16.0.254

DNS server: 8.8.8.8

Configure IPv4 settings for the selected port.

Proxy settings: Do not use a proxy server ▼

Test Internet Connectivity

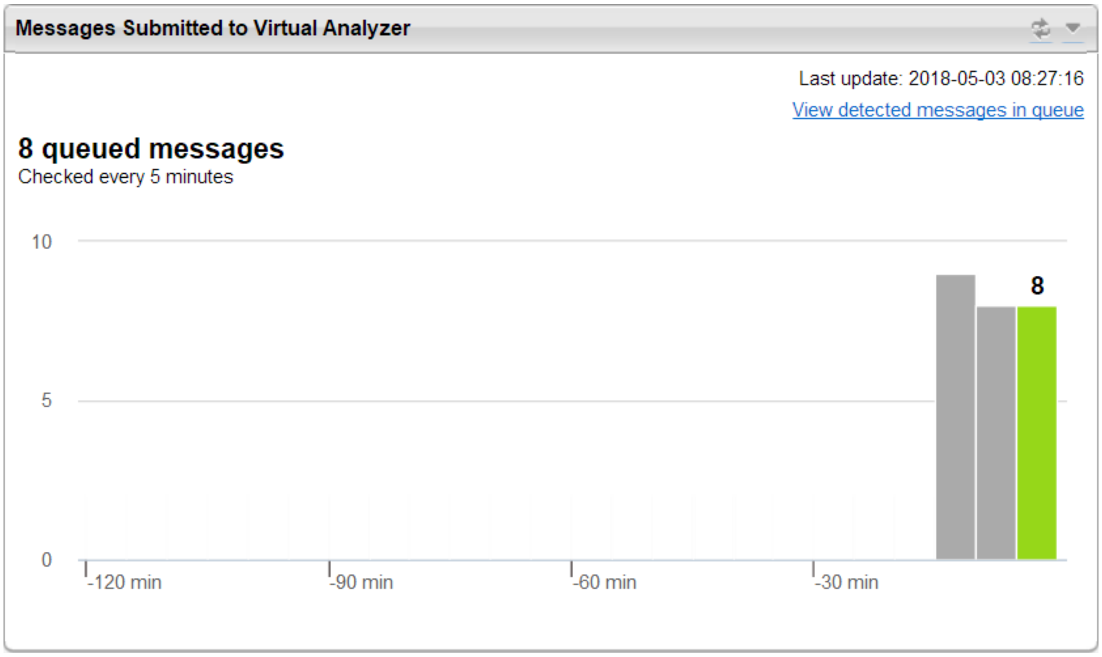
8. Click **Test Internet Connectivity** button to verify the Internet connection.

4.5. Configure Virtual Analyzer Instance Number

In a normal situation, the Virtual Analyzer performs netter if there are more Virtual Analyzer instances. However, this requires more resources and affects the DDEI performance.

When configuring the instance number, use the following widgets to monitor the DDEI and Virtual Analyzer performance and adjust as necessary:

- The Message Queue dashboard on **Dashboard** > **Overview** displays how many email messages are in the DDEI queue
- The Hardware Status dashboard on **Dashboard** > **System Status** shows the current resource usage
- The Messages Submitted to Virtual Analyzer dashboard on **Dashboard** > **Virtual Analyzer** shows how many email messages are in the Virtual Analyzer queue.



Messages Submitted to Virtual Analyzer

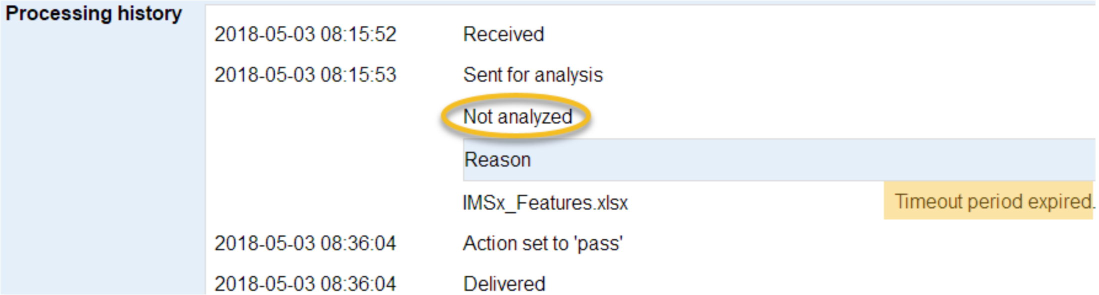
Last update: 2018-05-03 08:27:16

View detected messages in queue

8 queued messages

Checked every 5 minutes

Try to increase the number of instances if there are many email messages queued in the virtual analyzer and if the message tracking logs show some messages can not be analyzed on time.



Processing history	2018-05-03 08:15:52	Received	
	2018-05-03 08:15:53	Sent for analysis	
		Not analyzed	
		Reason	
		IMSx_Features.xlsx	Timeout period expired.
	2018-05-03 08:36:04	Action set to 'pass'	
	2018-05-03 08:36:04	Delivered	

Lesson 5: Integration with Products and Services

DDEI 5.1 can integrate with some third party applications

5.1.1. Apex Central

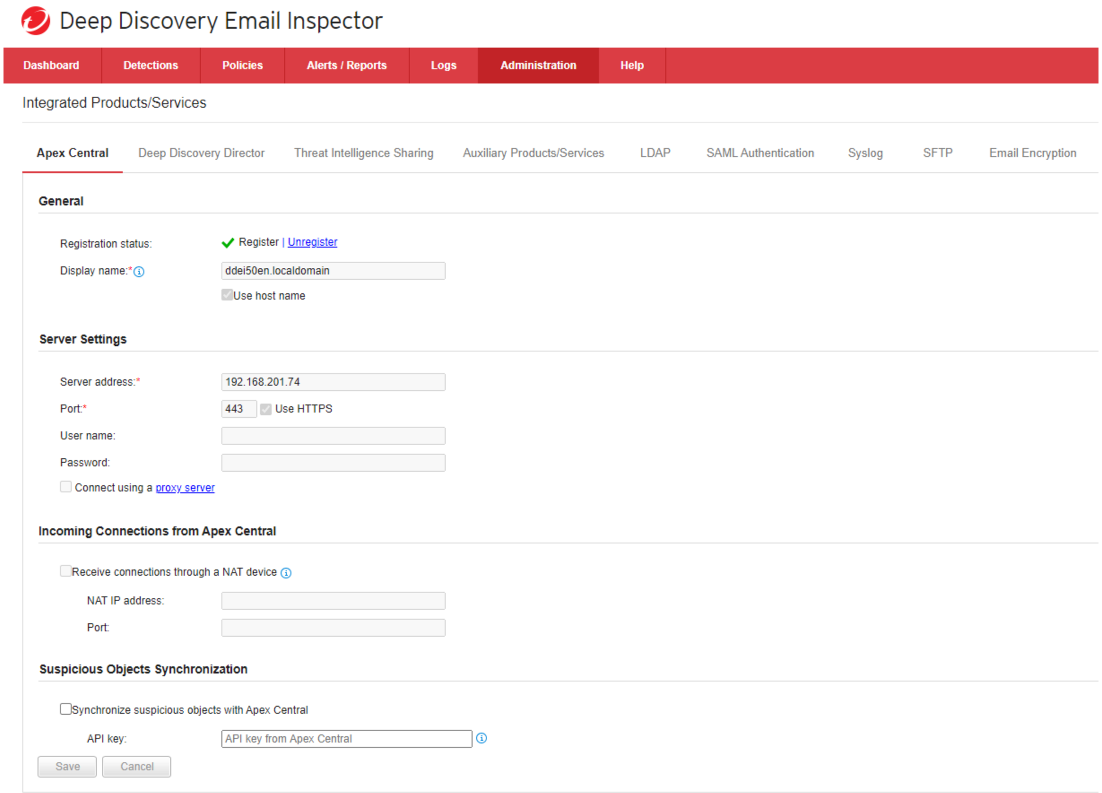
Register DDEI to Apex Central if Apex Central is present in the environment:

1. Open the DDEI web console
2. Go to **Administration** > **Administration** > **Integrated Products/Services** > **Apex Central** and register DDEI to Apex Central

NOTE:

If using the Connected Threat Defense (CTD) solution, provide the Apex Central API key on this page. See "Register to Apex Central" on page 84 for more detailed information.

If DDEI is behind NAT devices, Apex Central cannot directly connect to DDEI. Configure the *Incoming Connections from Apex Central* for the NAT IP address and ports mapped on the NAT devices.



General

Registration status: ✓ Register | Unregister

Display name:* ddei50en.localdomain

☑ Use host name

Server Settings

Server address:* 192.168.201.74

Port:* 443 ☑ Use HTTPS

User name:

Password:

□ Connect using a proxy server

Incoming Connections from Apex Central

□ Receive connections through a NAT device

NAT IP address:

Port:

Suspicious Objects Synchronization

□ Synchronize suspicious objects with Apex Central

API key: API key from Apex Central

5.1.2. Deep Discovery Director

Use Deep Discovery Director (DDD) to manage multiple DDEI servers. Use it to deploy DDEI update, upgrade, and Virtual Analyzer images. Use it also to replicate configuration and to aggregate the logs.

1. Open the DDEI web console
2. Go to **Administration** > **Integrated Products/Services** > **Deep Discovery Director** then register DDEI to DDD.

5.1.3. Threat Intelligence Sharing

DDEI can share threat intelligence data (such as suspicious URLs) with other products or services (Such as a Blue Coat ProxySG device) through HTTP or HTTPS web service.

Consider enabling this feature if such third-party products exist in the environment.

5.1.4. Auxiliary Products/Services

To help provide effective detection and blocking at the perimeter, DDEI can distribute Virtual Analyzer suspicious objects list to auxiliary products and services. To do this:

1. Open the DDEI web console
2. Go to **Administration** > **Integrated Products/Services** > **Auxiliary Products/Services** and configure the required services

Refer to the "Auxiliary Products/Services" section on page 119 of the DDEI Administration Guide for more detailed information

5.1.5. LDAP

DDEI integrates with an LDAP server for user-group definition and administrator privileges. DDEI supports the following types of directory servers:

- Microsoft Active Directory on Windows Server 2016 and 2019
- Microsoft AD Global Catalog on Windows Server 2016 and 2019
- Lotus Domino V9 and V10
- OpenLDAP

On a configured AD LDAP, the following features can be activated:

- Policies can use Active Directory user or group as Senders/Recipients address
- Use Active Directory user to logon to the DDEI admin console
- End-User Quarantine authentication
- DHA protection under sender filtering
- Bounce attack protection under sender filtering

NOTE: Since DDEI only supports a secure LDAP connection, the AD administrator needs to enable LDAPS on the LDAP server. Microsoft enhanced the LDAP in early 2020, after that, please choose SSL as the access protocol rather than StartTLS.

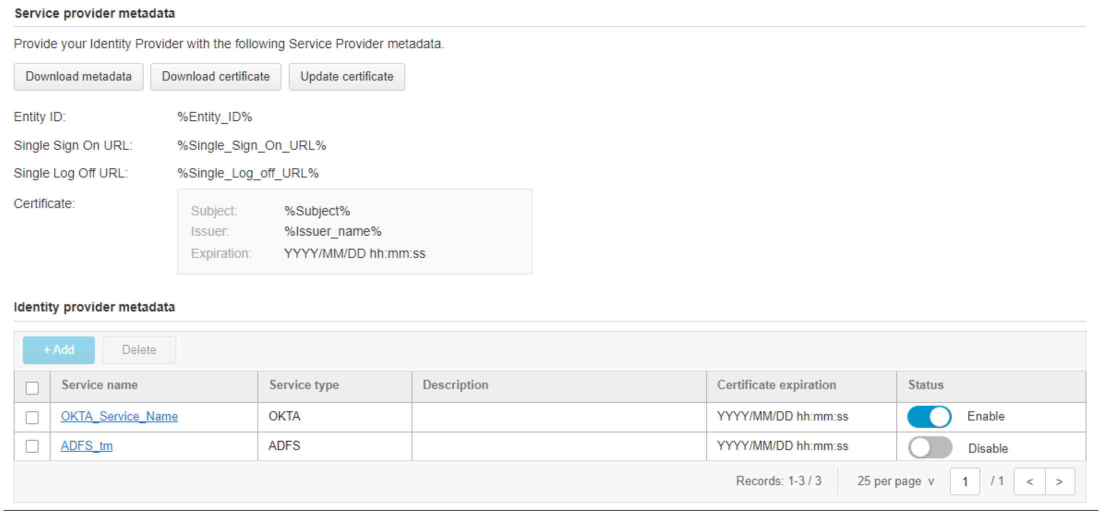
5.1.6. SAML Authentication

Security Assertion Markup Language (SAML) is an open authentication standard that allows for the secure exchange of user identity information from one party to another. SAML supports single sign-on (SSO), a technology that allows for single user login to work across multiple applications and services. When using SAML settings in DDEI, users signing in to the organization portal can seamlessly sign in to DDEI without an existing DDEI account.

In SAML single sign-on, a trust relationship is established between the identity provider (IdP) and the service provider (SP) by using SAML metadata files. The identity provider contains the user identity information stored on a directory server. In this case, the service provider (which is DDEI) uses the user identity information from the identity provider for user authentication and authorization.

DDEI supports the following identity providers for single sign-on:

- Microsoft Active Directory Federation Services (AD FS) 4.0 or 5.0
- Okta



Service provider metadata

Provide your Identity Provider with the following Service Provider metadata.

Entity ID: %Entity_ID%

Single Sign On URL: %Single_Sign_On_URL%

Single Log Off URL: %Single_Log_off_URL%

Certificate:

Subject: %Subject%
Issuer: %Issuer_name%
Expiration: YYYY/MM/DD hh:mm:ss

Identity provider metadata

□	Service name	Service type	Description	Certificate expiration	Status
□	OKTA_Service_Name	OKTA		YYYY/MM/DD hh:mm:ss	● Enable
□	ADFS_tm	ADFS		YYYY/MM/DD hh:mm:ss	○ Disable

Records: 1-3 / 3 25 per page ∨ 1 / 1 < >

Although DDEI supports these identity providers, only one can be used. For more detailed information and configuration, refer to the "SAML Integration" section on page 149 of the DDEI Administration Guide

5.1.7. Syslog

DDEI supports CEF, LEEF, and Trend Micro Event Format (TMEF) Syslog format.

- When using HP ArcSight, use CEF
- When using IBM Security QRadar use LEEF
- For other types of Syslog servers, TMEF log format can be used.

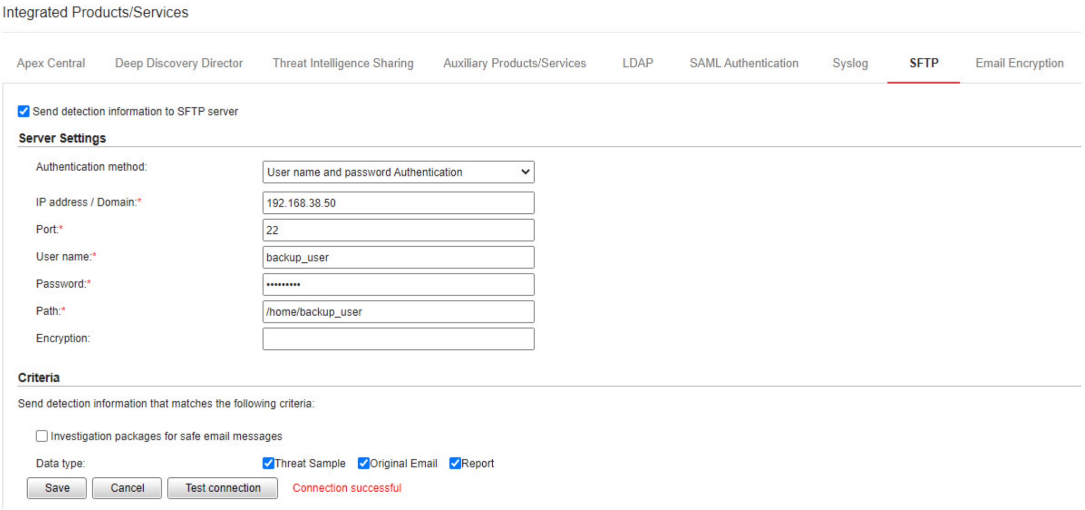
To configure the Syslog server:

1. Login to the DDEI web console
2. Go to **Administration** > **Integrated Products/Services** > **Log Settings**

5.1.8. SFTP

DDEI can be configured to send Virtual Analyzer detection information to a secure FTP (SFTP) server:

1. Login to the DDEI web console
2. Go to **Administration** > **Integrated Products/Services** > **SFTP** to enable Send detection information to SFTP server feature
3. Click the ***Test connection*** button to make a connection test, especially in a production environment.



☑ Send detection information to SFTP server

Server Settings

Authentication method:	User name and password Authentication
IP address / Domain:*	192.168.38.50
Port:*	22
User name:*	backup_user
Password:*	••••••••
Path:*	/home/backup_user
Encryption:	

Criteria

Send detection information that matches the following criteria:

☐ Investigation packages for safe email messages

Data type: ☑ Threat Sample ☑ Original Email ☑ Report

Connection successful

5.1.9. Email Encryption

To use email encryption, DDEI must be registered to sender domain first:

- Register and submit domains one by one or no more than ten at a time.
- When the domain is approved, Trend Micro sends a key file to the specified email address Import it to DDEI to complete the registration
- Up to 300 domains can be registered to the Trend Micro Email Encryption Server
- The feature is only available on Gateway Module license. All UI options are disabled if the license is invalid or expired
- When registering a domain for the first time, provide an email address to receive domain ownership verification key files. This email address can be updated only after a domain is successfully registered

Configure a default sender address for message signing. DDEI uses the default sender address when encrypting a message from a sender domain that is not in the Domain list. DDEI signs these messages with the default sender address.

1. Login to the DDEI Web console
2. Go to **Administration** > **Integrated Products / Services** > **Email Encryption**
3. Under ***Default Email Identify for Message Signing***, type the default sender address
4. Click **Save**.

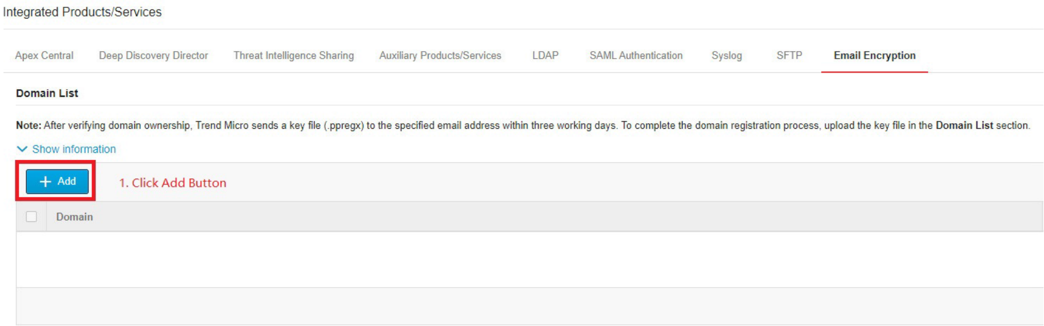
When using DDD to manage DDEI:

- Registration information will come from DDD
- Email Encryption page of DDEI will become read-only

When unregistering from DDD, all registration information in DDEI will be automatically deleted and email encryption will return to the unregistered state.

Registration

1. Go to **Administration** > **Integrated Products / Services** > **Email Encryption** then click **Add**

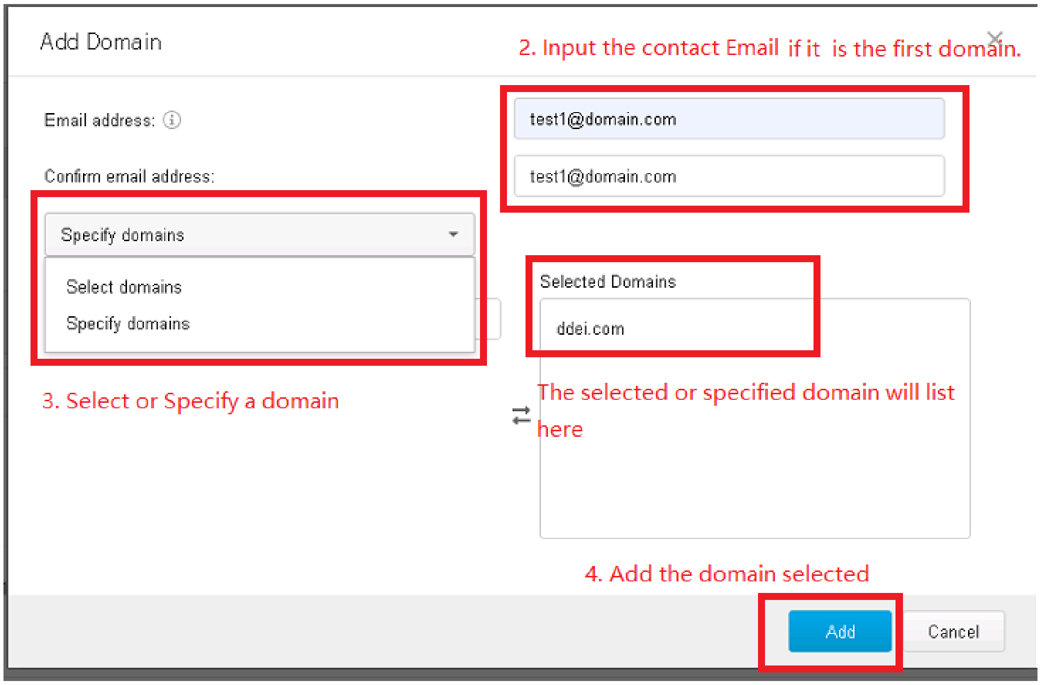


Note: After verifying domain ownership, Trend Micro sends a key file (.ppregx) to the specified email address within three working days. To complete the domain registration process, upload the key file in the **Domain List** section.

1. Click Add Button

2. Provide information

- Email address and Confirm email address section are hidden if a domain is already registered
- The email address will receive domain ownership verification key files from Trend Micro
- Domains can be selected from internal domains



2. Input the contact Email if it is the first domain.

Email address: test1@domain.com

Confirm email address: test1@domain.com

Specify domains

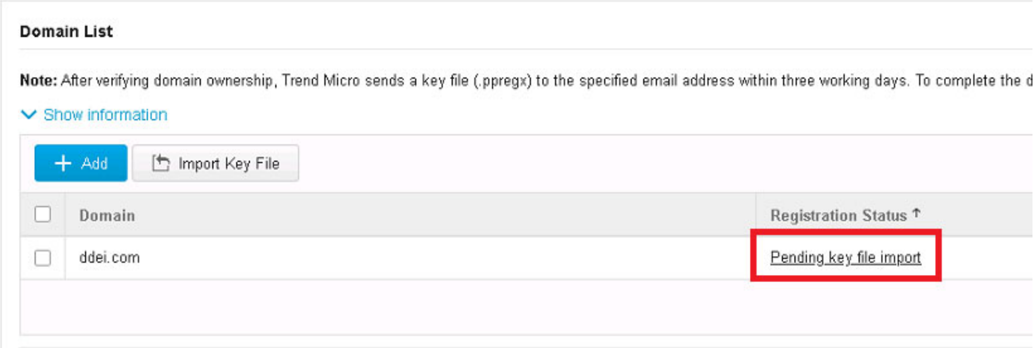
ddei.com

3. Select or Specify a domain

The selected or specified domain will list here

4. Add the domain selected

3. After adding a domain, the status will be Pending key file import



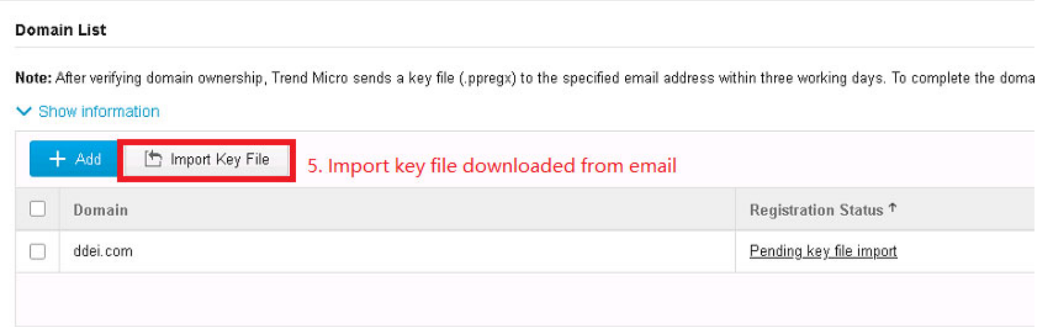
Domain List

Note: After verifying domain ownership, Trend Micro sends a key file (.ppregx) to the specified email address within three working days. To complete the d

☐	Domain	Registration Status ↑
☐	ddei.com	Pending key file import

4. Import key file

- A dialog box will pop up after clicking on Import Key File
- Import Key File button is hidden if no domain is added or all domains have finished registration



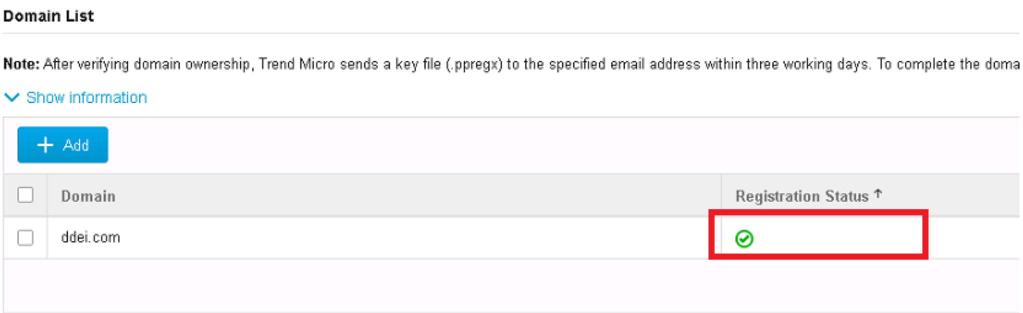
Domain List

Note: After verifying domain ownership, Trend Micro sends a key file (.ppregx) to the specified email address within three working days. To complete the doma

5. Import key file downloaded from email

☐	Domain	Registration Status ↑
☐	ddei.com	Pending key file import

5. Status will change to Completed after importing the key file



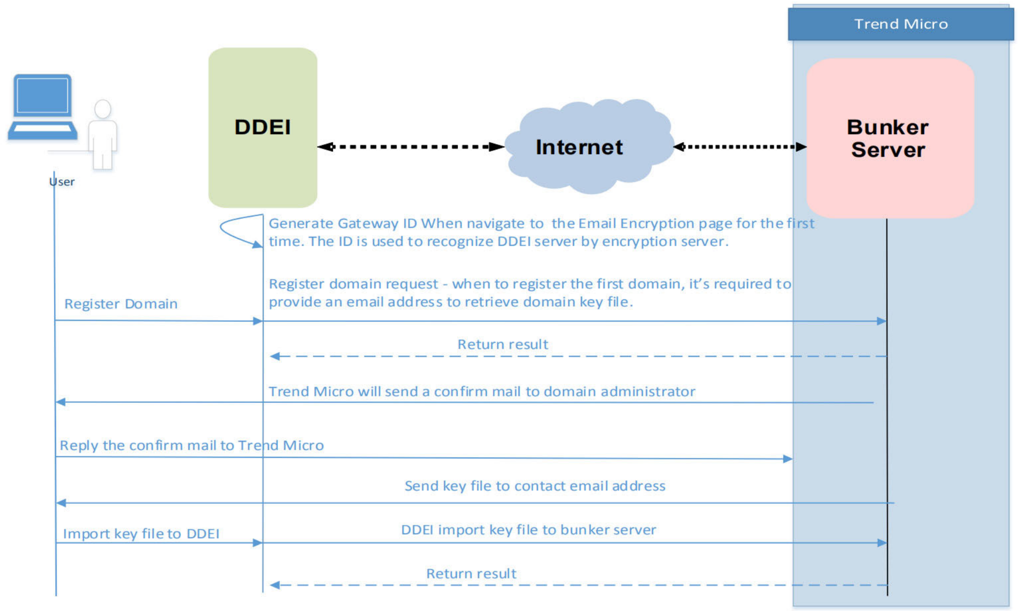
Domain List

Note: After verifying domain ownership, Trend Micro sends a key file (.ppregx) to the specified email address within three working days. To complete the doma

☐	Domain	Registration Status ↑
☐	ddei.com	✓

Registration flow (Without DDD)

Registration flow (Without DDD)

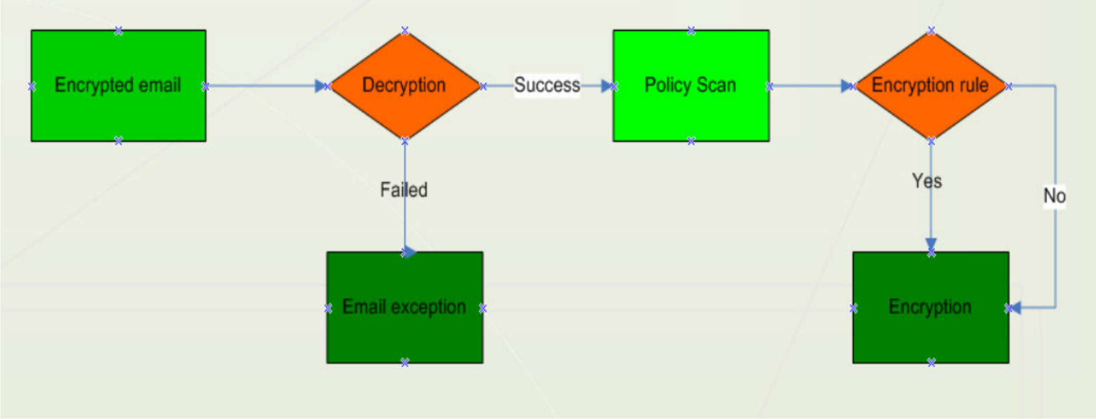

Trend Micro
User
DDEI
Internet
Bunker Server
Generate Gateway ID When navigate to the Email Encryption page for the first time. The ID is used to recognize DDEI server by encryption server.
Register Domain
Register domain request - when to register the first domain, it's required to provide an email address to retrieve domain key file.
Return result
Trend Micro will send a confirm mail to domain administrator
Reply the confirm mail to Trend Micro
Send key file to contact email address
Import key file to DDEI
DDEI import key file to bunker server
Return result

EMAIL ENCRYPTION ACTION

Email encryption action has the following flow:

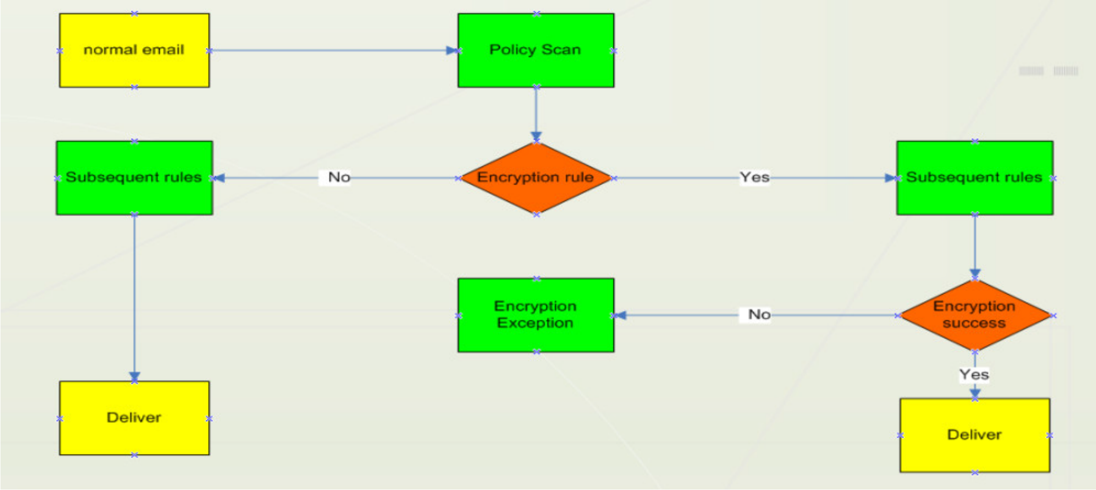
1. Allow to specify the email encryption action in either inbound/outbound content filtering rule or DLP rule
2. The encryption action is a non-terminal action; subsequent rules continuously scan the messages even if the message has matched rules with encrypt action
3. DDEI applies email encryption only during delivery (Before DKIM signing, if in use)
4. Encryption is only available in MTA, while decryption supports all operation modes
5. Encryption only takes effect once, even if the message matches more than one rule that contain the encrypt action.
6. Encryption only takes effect when DDEI is registered to Bunker with at least one domain registered. If not configured, Pass and Tag action will apply for rules with encrypt rule

ENCRYPTED EMAIL PROCESS



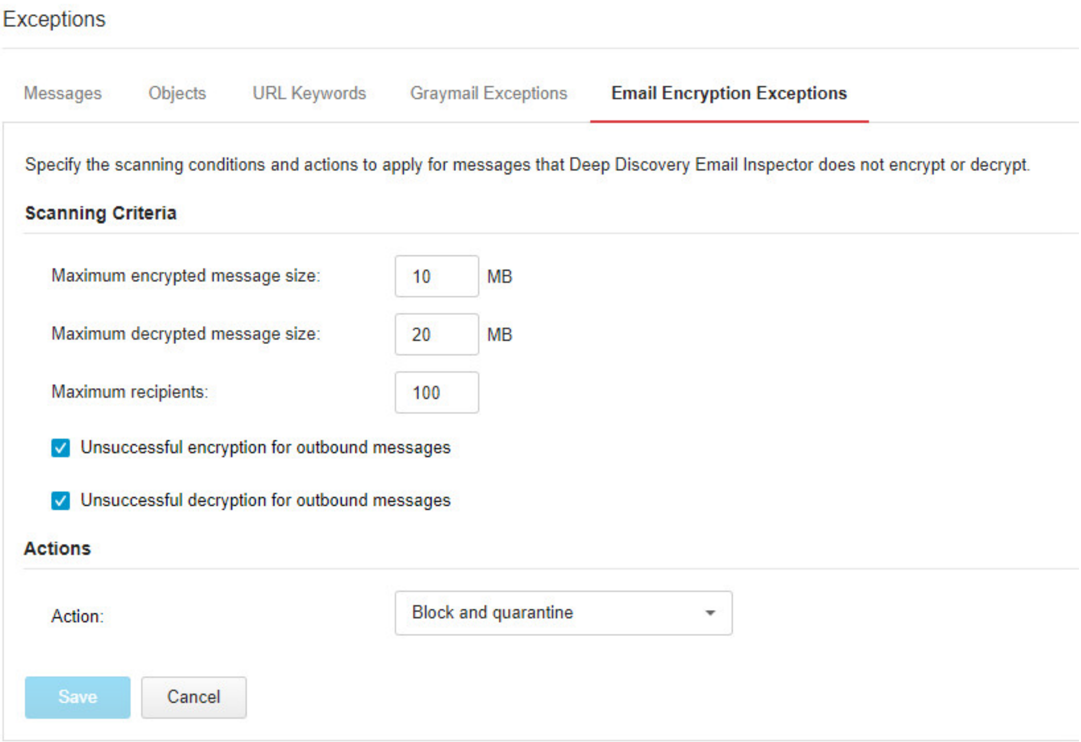
- When DDEI receives encrypted emails, it will try to decrypt the message first.
- Before DDEI sends the original encrypted emails, it encrypts the email regardless if an encryption rule is matched or not.
- DDEI does not trigger exception if the encrypted message does not match an encryption action rule.

NORMAL EMAIL PROCESS



- When DDEI receives encrypted emails, it will try to decrypt the message first.
- Before DDEI sends the original encrypted emails, it encrypts the email regardless if it matches an encryption rule or not.
- DDEI does not trigger an exception if the encrypted message does not match an encryption action rule.

To configure email encryption exception action, go to **Policies** > **Exceptions** > **Email Encryption** Exceptions



Specify the scanning conditions and actions to apply for messages that Deep Discovery Email Inspector does not encrypt or decrypt.

Scanning Criteria

Maximum encrypted message size: 10 MB

Maximum decrypted message size: 20 MB

Maximum recipients: 100

☑ Unsuccessful encryption for outbound messages

☑ Unsuccessful decryption for outbound messages

Actions

Action: Block and quarantine

Securely storing the cache and store key list in the IBE server

- After DDEI registers at least one domain to Bunker, DDEI retrieves the global public key and gateway key and store them in DB.
- When encrypting and decrypting emails, DDEI retrieves the private key for every email address and then store them
- DDEI schedule an update for the global public key, private key, and clean expired key every month from Bunker through a scheduled task.

Lesson 6: Product Configuration

6.1. Initial Configuration

During initial deployment, use the recommendations in the "Deployment" chapter on page 25. It includes recommendations for:

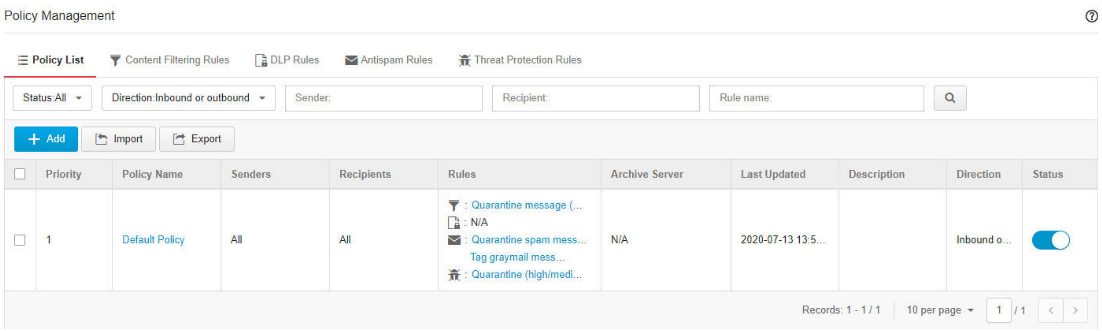
- MTA Mode
- BCC Mode
- SPAN/TAP Mode

After the initial configuration, refer to the "Virtual Analyzer Integration" chapter on page 34 to configure the virtual analyzer as it is a vital part of DDEI. After that, refer to "Integration with Products and Services" chapter on page 40 to integrate DDEI with other products and services.

Also, use custom policies if the default DDEI policies does not meet the company requirements.

6.2. Policy Settings

DDEI 5.1 contains a default policy that checks the messages sent from All to All.



□	Priority	Policy Name	Senders	Recipients	Rules	Archive Server	Last Updated	Description	Direction	Status
□	1	Default Policy	All	All	: Quarantine message (... : N/A : Quarantine spam mess... Tag graymail mess... : Quarantine (high/medi...	N/A	2020-07-13 13:5...		Inbound o...	●

Records: 1 - 1 / 1 10 per page 1 / 1

It is suggested to create a different set of policy for incoming and outgoing emails.

6.2.1. Policy Management Guidelines

When configuring policies, consider the following rules:

- Create ***Content Filtering Rules***, ***DLP rules***, ***Antispam Rules***, and ***Threat Protection Rules*** first, then create the policy
- The Content Filtering Rules, DLP rules, and Antispam Rules need the Gateway Module license; otherwise, those three parts will not work
- A policy **must include** and **only can consist** of one *Threat Protection Rule*
- Content Filtering Rules, DLP Rules, and Antispam Rules are an option in a policy. A policy may include none, one, or multiple content filtering rules, DLP rules, and antispam rules
- One message can only be checked by, at most, one policy
- If a message with multiple recipients matches different policies, DDEI will split the message into multiple messages for the number of affected recipients
- ***Delete message***, ***Block and quarantine***, and ***Deliver direct*** actions are terminal actions in a policy rule. When applying one terminal action, the DDEI scanning daemon would not continue to process the remaining rules and parts in the policy's rule set.
- The last policy should be All to All so that DDEI checks all messages.

6.2.2. Understanding Multiple Policy Matching

This section explains which policy the coming messages will use for scanning.

Unlike other Trend Micro products (Such as Interscan Messaging Security, Interscan Messaging Security Suite, or Hosted Email Security or Email Security) when it comes to multiple policies, DDEI uses a logic that is similar to firewall rules:

1. DDEI checks the from/to addresses (envelope addresses) information of new incoming message

2. If the message in the from/to addresses matches the first policy's Senders/Recipients setting, DDEI will use the first policy to check this message and take the final action based on this policy's scanning result. If the message cannot trigger any of this policy's scanning rules, the final action is to deliver. This message will not go through to the next policy.
3. The message will go through to the next policy until it reaches a policy that matches the sender/recipient setting and takes action based on the policy's scanning result.
4. If the message does not match with all the policies' Senders/Recipients setting, DDEI will deliver the email
5. If the message contains multiple recipients and only a part of the recipients can match one policy's Senders/Recipients setting, DDEI will split this message into two messages. The matching policy will check one message, and the other message will keep checking if it will match the remaining policies.

NOTE: Only one email can be checked by, at most, one policy

Here are some examples of policy match

ing:

Policy Priority	Policy Name	Senders	Recipients
1	`Special_Recipients`	ALL	• ceo@cncorelab.com • cfo@cncorelab.com • cio@cncorelab.com
2	`Special_Senders`	• ceo@cncorelab.com • marketing@cncorelab.com • *@partner.com	ALL
3	`Sales_Team`	ALL	• Sales1@cncorelab.com • Sales2@cncorelab.com
4	`To_Partner`	*@cncorelab.com	*@partner.com
5	`Incoming`	ALL	• *@cncorelab.com • *@cncorelab.net
6	`Outgoing`	*@cncorelab.com	ALL
7	`Default policy`	ALL	ALL

TABLE 6.2.1.1: Policy Matching Samples

Examples	Senders	Recipients	Matched Policy
1	cfo@partner.com	ceo@cncorelab.com	Policy 1: `Special_Recipients`
2	cio@partner.com	• bryan_xu@cncorelab.com • cio@cncorelab.com • Sales1@cncorelab.com	• Policy 1: `Special_Recipients` • Policy 2: `Special_Senders`
3	ceo@cncorelab.com	cfo@partner.com	Policy 2: `Special_Senders`
4	cfo@cncorelab.com	cfo@partner.com	Policy 4: `To_Partner`
5	bryan_xu@msn.com	Sales1@cncorelab.com	Policy 3: `Sales_Team`
6	bryan_xu@msn.com	• ceo@cncorelab.com • Sales1@cncorelab.com • bryan_xu@cncorelab.com	• Policy 1: `Special_Recipients` • Policy 3: `Sales_Team` • Policy 5: `Incoming`

TABLE 6.2.1.2: Policy Matching Results

In examples 2 and 6, it contains multiple recipients that fit different policies. DDEI will split the original mail into multiple mails for it to match other policies.

Best Practices on Priorities for Policy Usage

- It's known that one message can only be checked by, at most, one policy. Therefore, the smaller range of matched conditions, the higher the priority of the policy.
- Set select senders/recipients with a high priority policy. Set a lower priority for more common roles
- The last policy should be All to All so that DDEI could check all messages.

6.2.3. Understanding Policy Rules

A policy in DDEI is composed of four parts:

- Content Filtering Rules
- DLP Rules
- Antispam Rules
- Threat Protection Rules

The Content Filtering Rules, DLP Rules, and Antispam Rules sections may contain multiple rules, and the priority of those rules are changeable.

The Threat Protection section can only have one rule and also must contain only one rule.

Rule Actions

DDEI has the following action types:

Parts	Actions (Red color actions are Terminal Actions)
Content Filtering Rules	• Delete message • Block and quarantine • Encrypt message • Strip all attachments • Sanitize file • Pass and tag • Deliver directly • Change recipient
DLP Rules	• Delete message • Block and quarantine • Encrypt message • Strip all attachments • Pass and tag • Deliver directly • Change recipient
Antispam Rules	• Delete message • Block and quarantine • Pass and tag • Deliver directly • Change recipient
Threat Protection Rules	• Delete message • Block and quarantine • Strip attachments, redirect links to blocking page, and tag • Strip attachments, redirect links to warning page, and tag • Pass and tag • Change recipient

TABLE 6.2.1.3: Policy Rule Action Types

Terminal Actions cause the scanning daemon not to continue to process the remaining rules and parts in the policy's rule set.

Strip attachments can work for those attachments that trigger the scanning criteria.

Redirect links can work for the links which WRS detects as risk URLs.

Scanning Order

To streamline the scanning order and avoid confusion, this section treats split email as a separate message.

1. The scanning order of the policy has four parts. This is the fixed order and cannot be changed:

- Content Filtering Rules
- DLP Rules
- Antispam Rules
- Threat Protection Rules

2. The scanning order for multiple rules for each part are as follows:

If the part contains multiple rules, each rule checks the email one by one from the higher priority rule to the lower priority rule. The rule priority is changeable.

SCANNING RESULT AND FINAL ACTION

1. If the email triggered one rule, DDEI takes action as defined in that rule
2. If the action is not a terminal action, the scanning daemon will process the remaining parts/ rules
3. If the email triggers one rule with a terminal action (delete or quarantine), DDEI will take the terminal action immediately and not continue to process the remaining parts/rules. In this situation:

   Final action = Previously triggered rules' non-terminal action + Terminal action

4. If the last triggered rule has no terminal action, in this situation:

   Final action = All of the triggered rules' actions + Deliver.

5. If there are no rules triggered:

   Final action = Deliver

DELIVER DIRECTLY ACTION

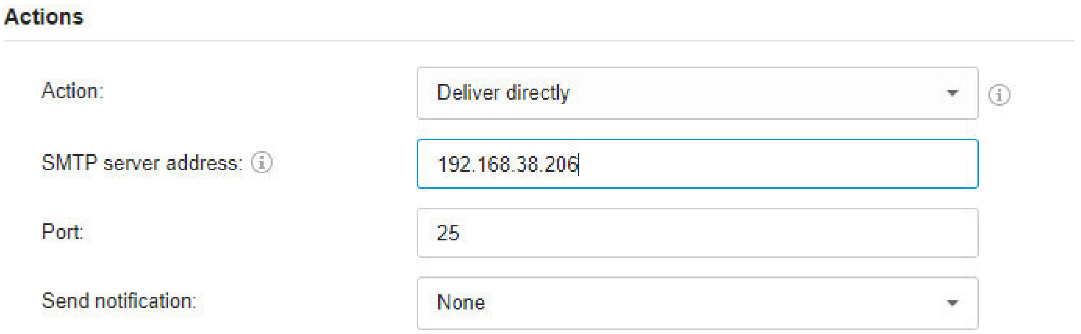
In DDEI 5.1, rule based hand-off action is introduced for ***Deliver directly*** action:

- "Deliver directly" option is available with or without specifying an SMTP server information during new policy rule creation

  – If SMTP server is configured, the matched message will be delivered to the particular SMTP server. Otherwise, it will be delivered to the original server as specified in the ***Mail Delivery*** settings.

- With terminal action, the message is delivered directly without further scanning by other rules

- This action is applicable for all types of policy rules.
- The action result can be viewed on detection or tracking log pages.



Actions

Action: Deliver directly

SMTP server address: 192.168.38.206

Port: 25

Send notification: None

6.2.4. Understanding Policy Objects

ADDRESS GROUPS

An address group is a collection of user email addresses in the organization. Instead of creating policies to apply policy rules to each address individually, administrator can create an address group to apply policy rules to several email addresses at the same time.

NOTIFICATIONS

Administrator can define the notifications based on the requirements and the notification can be used in any of the rules. Tokens are supported in the notification mail to provide more detailed information.

REPLACEMENT FILE

DDEI uses a replacement file to replace stripped attachments in detected messages to notify the recipient that the email message was processed and the suspicious or malicious attachment is removed.

STAMP

A message stamp is inserted in an email message to notify a recipient that DDEI has processed the message.

REDIRECT PAGES

Administrator can customize the content of the redirect page. If the action contain "***redirect links***", DDEI will use the setting on this page.

1. The Threat Protection Rules contain two types of redirect action:

- Redirect to blocking page
- Redirect to warning page

2. If WRS detects the URL as risky, and the Threat Protection Rule contain "***redirect links to blocking page***", DDEI will use the blocking page setting under **Policies** > **Policy Objects** > **Redirect Pages**. In this situation, the redirect page could be either "Use external redirect page" or built-in blocking page
3. If WRS detects the URL as a risky URL and the Threat Protection Rule contains "***redirect links to warning page***", DDEI will use the built-in warning page setting under **Policies** > **Policy Objects** > **Redirect Pages**.

ARCHIVE SERVERS

Configure archive servers to store email messages that match a policy. When using this option for a policy, DDEI automatically sends a copy of matched messages to the specified archive server.

DATA IDENTIFIERS

Digital assets are files and data that an organization must protect against unauthorized transmission.

Define digital assets using the following data identifiers:

- Expressions: Data that has a certain structure.
- File attributes: File properties such as file type and file size.
- Keyword lists: A list of special words or phrases.

DLP TEMPLATES

A Data Loss Prevention (DLP) template combines DLP data identifiers and logical operators (And, Or, Except) to form condition statements. Only files or data that satisfy a certain condition statement will be subject to a DLP policy.

For example, a file must be a Microsoft Word file (file attribute) AND must contain certain legal terms (keywords) AND must contain ID numbers (expressions) for it to be subject to the "Employment Contracts" policy. This policy allows Human Resources personnel to send the file to recipients within a domain. Sending the same file to recipients outside the domain is blocked.

Create templates after configuring data identifiers.

Create Sample Policies

DDEI contains a default policy that checks the messages sent from All to All. It is suggested to create a different policy for incoming and outgoing emails.

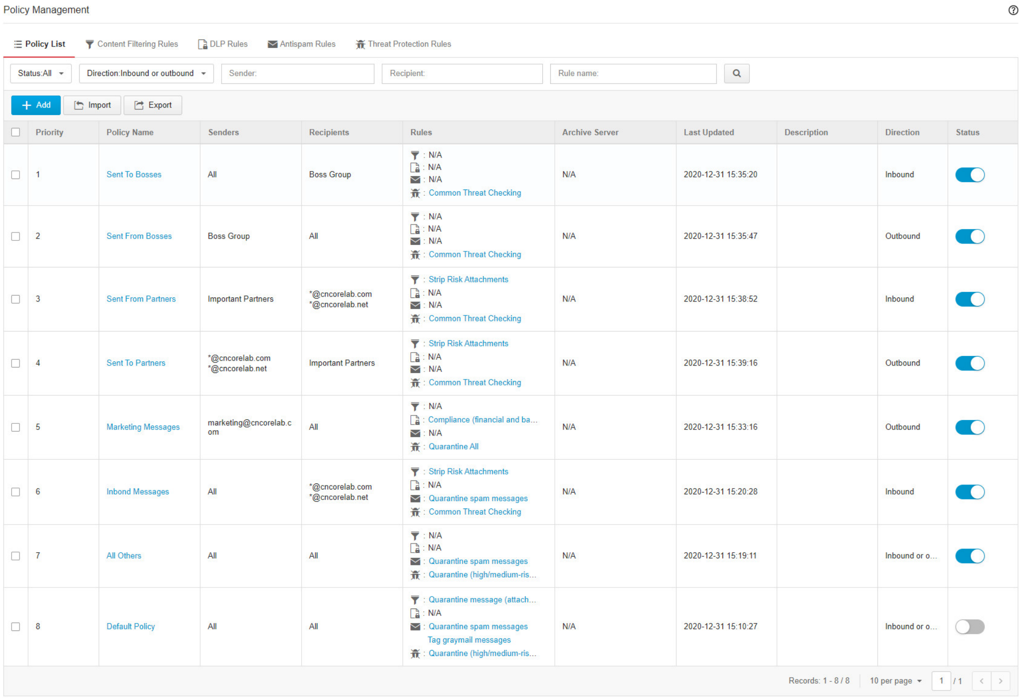
SCENARIO

- Internal domain: cncorelab.com, cncorelab.net

- Important partners: partner1.com, partner2.com

REQUIREMENTS

- Common threat checking action:
  - High Risk: Quarantine messages
  - Medium Risk: Strip suspicious attachments, redirect links to blocking page, and tag subject
  - Low Risk: Strip suspicious attachments, redirect links to a warning page, and tag the subject.
- Messages from Bosses or sent to Bosses: Only do threat checking and do not do content filtering and antispam checking
- Messages sent from important partners or sent to important partners: Do not do antispam checking
- Messages sent from marketing@cncorelab.com: Do DLP checking and threat checking, quarantine email contains a threat
- All other inbound messages: Do content filtering, antispam, and threat checking
- All other mails: Do antispam checking and threat checking.

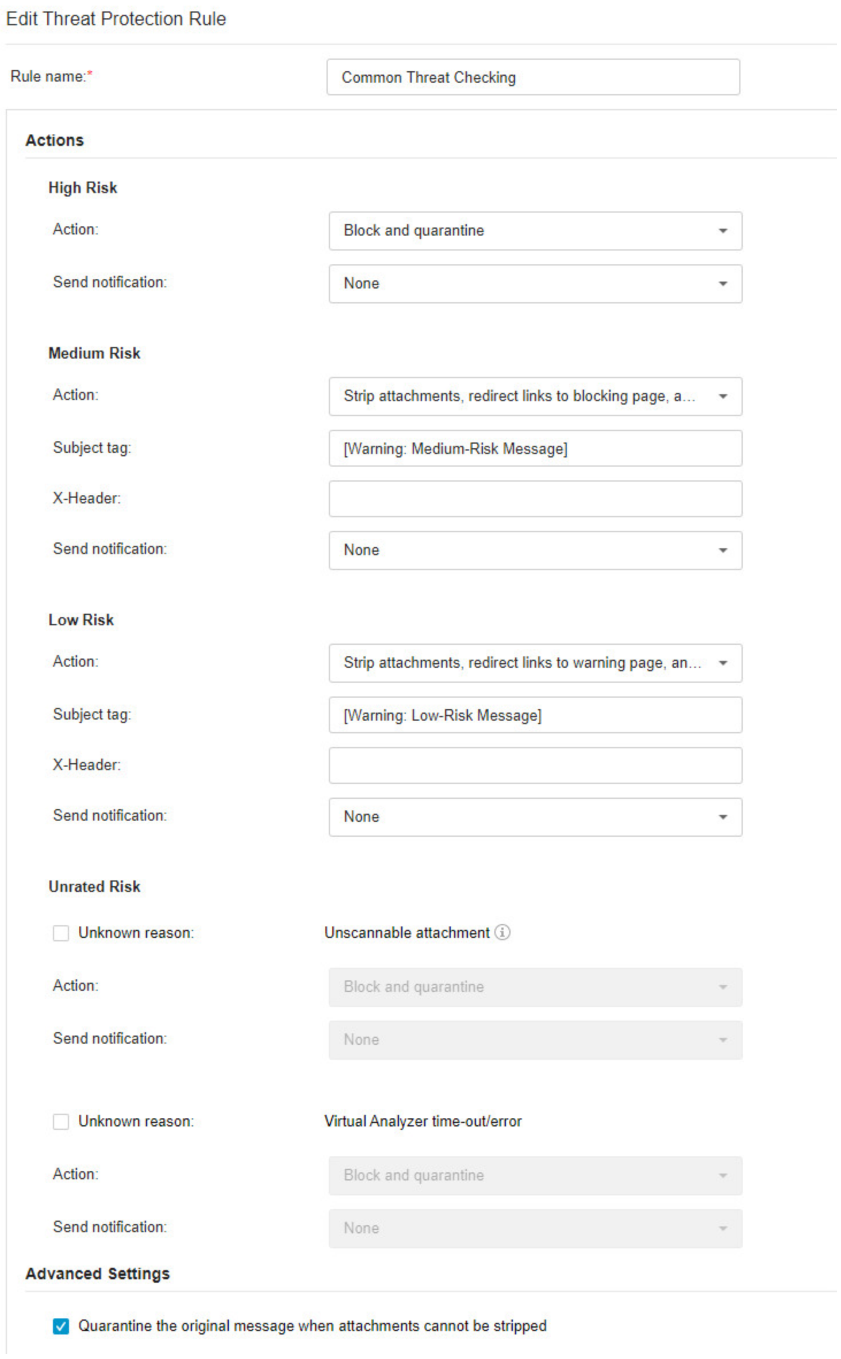


Policy Management

□	Priority	Policy Name	Senders	Recipients	Rules	Archive Server	Last Updated	Description	Direction	Status
□	1	Sent To Bosses	All	Boss Group	: N/A : N/A : N/A : Common Threat Checking	N/A	2020-12-31 15:35:20		Inbound	●
□	2	Sent From Bosses	Boss Group	All	: N/A : N/A : N/A : Common Threat Checking	N/A	2020-12-31 15:35:47		Outbound	●
□	3	Sent From Partners	Important Partners	*@cncorelab.com *@cncorelab.net	: Strip Risk Attachments : N/A : N/A : Common Threat Checking	N/A	2020-12-31 15:38:52		Inbound	●
□	4	Sent To Partners	*@cncorelab.com *@cncorelab.net	Important Partners	: Strip Risk Attachments : N/A : N/A : Common Threat Checking	N/A	2020-12-31 15:39:16		Outbound	●
□	5	Marketing Messages	marketing@cncorelab.com	All	: N/A : Compliance (financial and ba... : N/A : Quarantine All	N/A	2020-12-31 15:33:16		Outbound	●
□	6	Inbond Messages	All	*@cncorelab.com *@cncorelab.net	: Strip Risk Attachments : N/A : Quarantine spam messages : Common Threat Checking	N/A	2020-12-31 15:20:28		Inbound	●
□	7	All Others	All	All	: N/A : N/A : Quarantine spam messages : Quarantine (high/medium-ris...	N/A	2020-12-31 15:19:11		Inbound or o...	●
□	8	Default Policy	All	All	: Quarantine message (attach... : N/A : Quarantine spam messages Tag graymail messages : Quarantine (high/medium-ris...	N/A	2020-12-31 15:10:27		Inbound or o...	○

MAJOR STEPS IN CREATING POLICIES AND RULES

1. Create the common threat checking rule
   a. Login to DDEI Web console
   b. Go to **Policies** > **Policy Management** > **Threat Protection Rules**
   c. Refer to the following screenshot to add a threat protection rule



Edit Threat Protection Rule

Rule name:* Common Threat Checking

Actions

High Risk

Action: Block and quarantine

Send notification: None

Medium Risk

Action: Strip attachments, redirect links to blocking page, a...

Subject tag: [Warning: Medium-Risk Message]

X-Header:

Send notification: None

Low Risk

Action: Strip attachments, redirect links to warning page, an...

Subject tag: [Warning: Low-Risk Message]

X-Header:

Send notification: None

Unrated Risk

□ Unknown reason: Unscannable attachment ⓘ

Action: Block and quarantine

Send notification: None

□ Unknown reason: Virtual Analyzer time-out/error

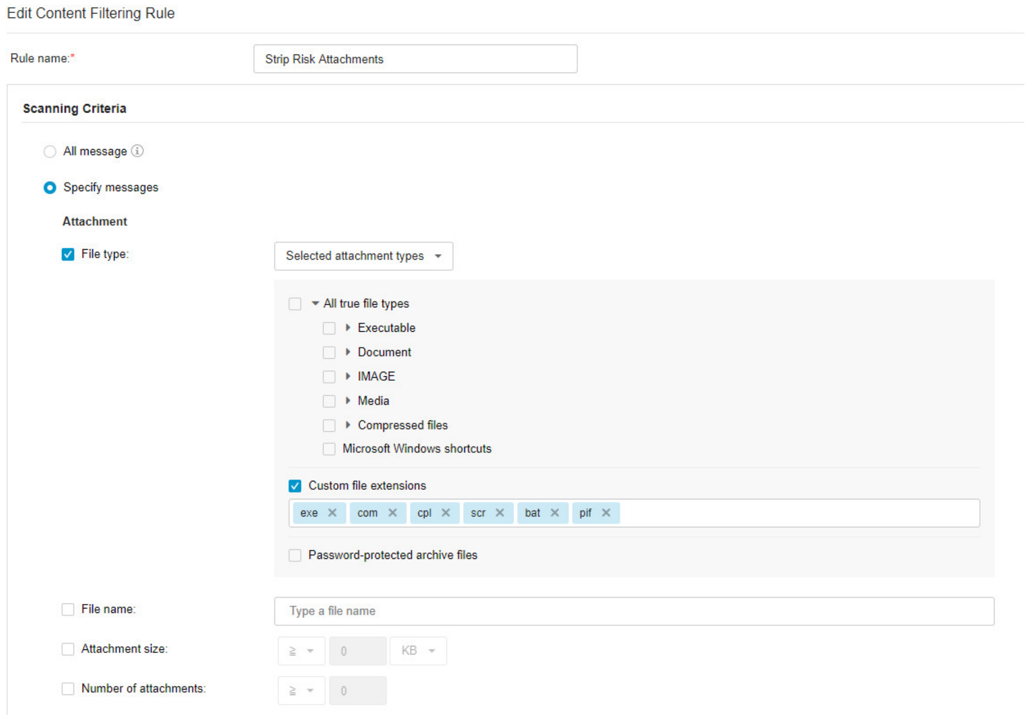
Action: Block and quarantine

Send notification: None

Advanced Settings

☑ Quarantine the original message when attachments cannot be stripped

2. Create another Threat Protection Rule to quarantine all messages and name it "*Quarantine all*"
3. Create a content filtering rule to strip attachments (Such as exe, com, bat, pif, scr, cpl)
   a. Go to **Policies** > **Policy Management** > **Content Filtering Rules**
   b. Refer to the following screenshot to add a content filtering rule



Edit Content Filtering Rule

Rule name:* Strip Risk Attachments

Scanning Criteria

○ All message

● Specify messages

Attachment

☑ File type: Selected attachment types

- □ All true file types
  - □ Executable
  - □ Document
  - □ IMAGE
  - □ Media
  - □ Compressed files
  - □ Microsoft Windows shortcuts
- ☑ Custom file extensions: exe ✕ com ✕ cpl ✕ scr ✕ bat ✕ pif ✕
- □ Password-protected archive files

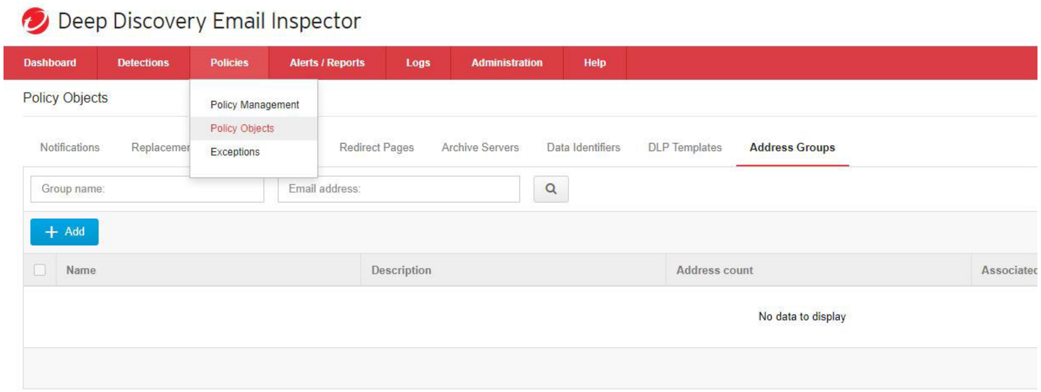
□ File name: Type a file name

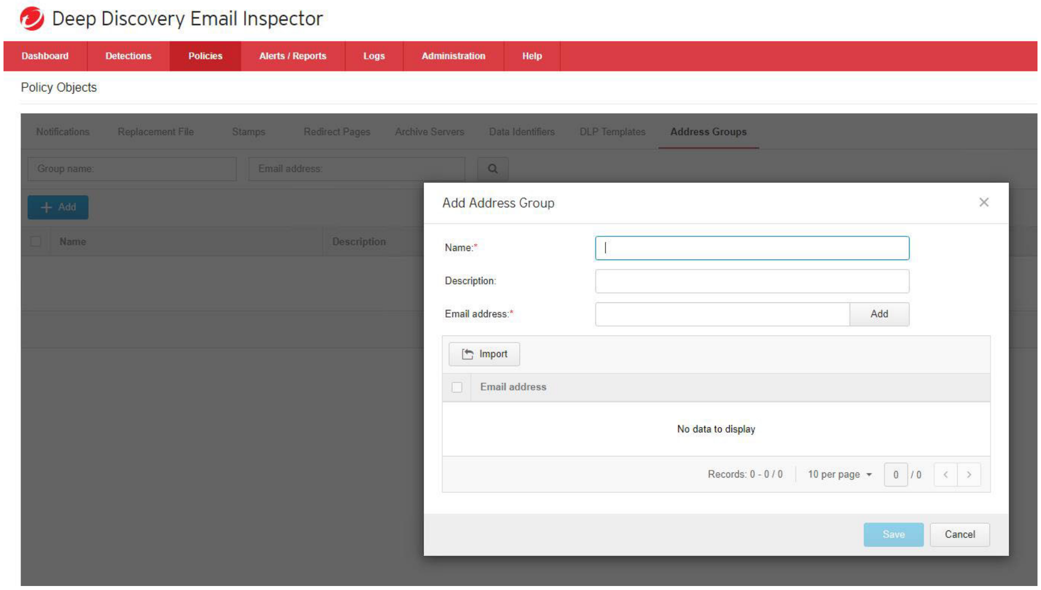
□ Attachment size: ≥ 0 KB

□ Number of attachments: ≥ 0

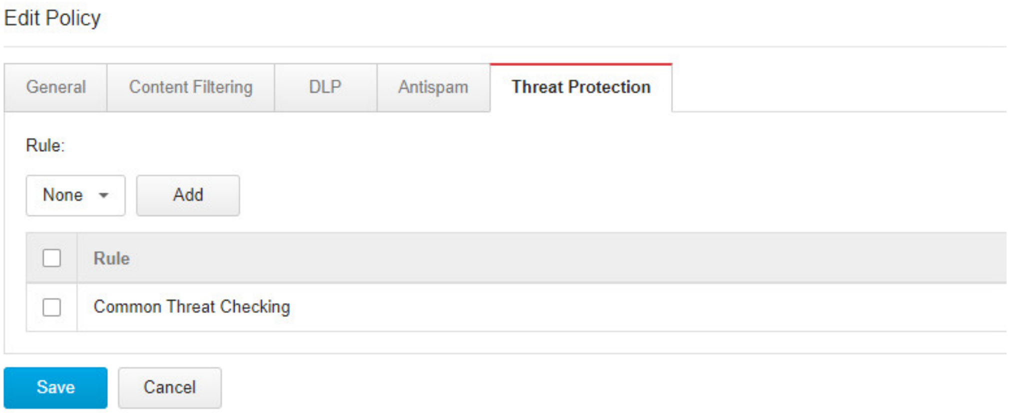
4. Create a policy to filter the messages sent to bosses.

   a. Go to **Policies** > **Policy Objects**
   b. Click **Address Groups**
   c. On the ***Add*** to configure a new Address group named "***Boss Group***", and the boss's email address into this group





d. Use the newly created address group as the policy recipients address
e. On the ***Threat Protection*** page, add the Common Threat Checking rule created in step 1 and then save the rule



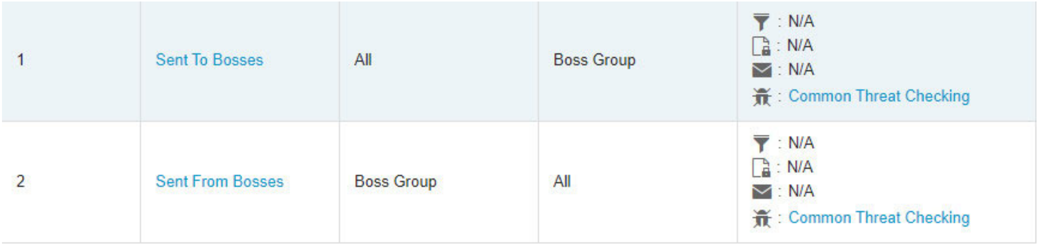
Edit Policy

Rule:

□	Rule
□	Common Threat Checking

5. Create a policy to filter the messages sent from the bosses

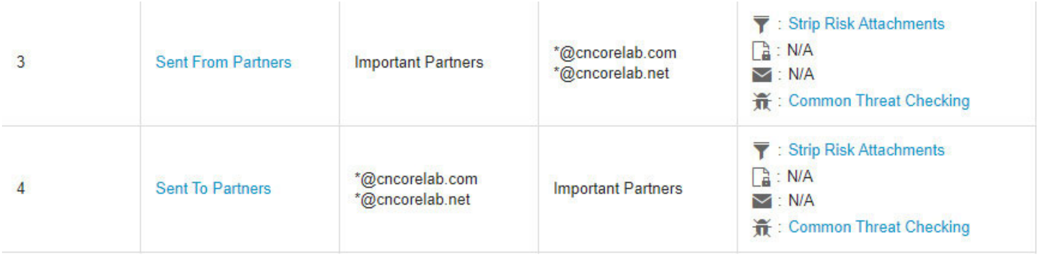
    a. Status: `enabled`
    b. Policy name: ***Sent from Bosses***
    c. Priority: 2
    d. Sent from Boss Group to All
    e. The newly created policies should appear as the following:



1	Sent To Bosses	All	Boss Group	▼ : N/A 🗎 : N/A ✉ : N/A 🐞 : Common Threat Checking
2	Sent From Bosses	Boss Group	All	▼ : N/A 🗎 : N/A ✉ : N/A 🐞 : Common Threat Checking

6. Create Policies for important partners:

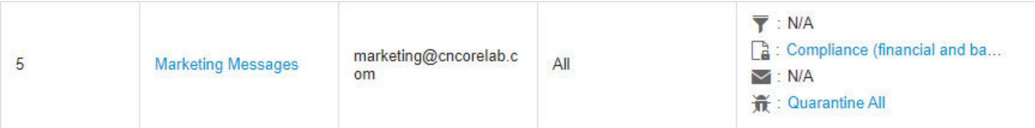
    a. Create a new address group and name it as "***Important_Partners***"
    b. On the ***Content Filtering*** page, add the ***Strip Risk Attachment*** rule created in step 3
    c. Priority: Two policies with 3 and 4 priority
    d. Policies for partners are as follows:



3	Sent From Partners	Important Partners	*@cncorelab.com *@cncorelab.net	▼ : Strip Risk Attachments 🗎 : N/A ✉ : N/A 🐞 : Common Threat Checking
4	Sent To Partners	*@cncorelab.com *@cncorelab.net	Important Partners	▼ : Strip Risk Attachments 🗎 : N/A ✉ : N/A 🐞 : Common Threat Checking

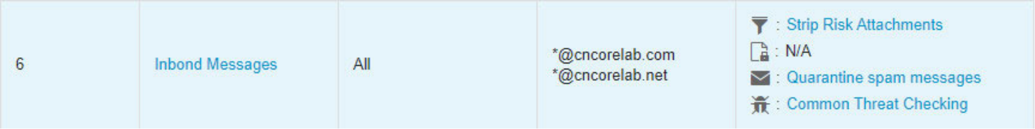
7. Create the following policies

- "***Marketing Messages***" for marketing messages with the DLP rule and threat protection rule. Set the priority to 5.



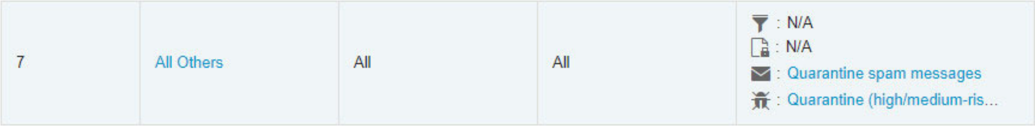
5	Marketing Messages	marketing@cncorelab.com	All	▼ : N/A 🗎 : Compliance (financial and ba... ✉ : N/A 🐞 : Quarantine All

- "*Inbound Messages*" for all other inbound emails. Set the priority to 6



6	Inbond Messages	All	*@cncorelab.com *@cncorelab.net	▼ : Strip Risk Attachments 🗎 : N/A ✉ : Quarantine spam messages 🐞 : Common Threat Checking

- "*All Other*" for other messages. Set the priority to 7



7	All Others	All	All	▼ : N/A 🗎 : N/A ✉ : Quarantine spam messages 🐞 : Quarantine (high/medium-ris...

Add other policies as required such as graymail checking rule into the Antispam Rules part.

Understanding Policy Exceptions

Policy exceptions reduce threat-related false positives. Configure exceptions to classify certain email messages as safe. Specify the safe senders, recipients, and X-header content, add files, URLs, IP addresses and domains, add URL keywords, or specify senders to bypass graymail scanning. Specify whether need to encrypt or decrypt messages. Safe email messages are discarded (BCC and SPAN/TAP mode) or delivered to the recipient (MTA mode) without further investigation.

Take note of the following:

- **Policies** > **Exceptions** > **Messages** apply to all types of rule, which include content filtering rules, antispam rules and threat protection rules.
- **Policies** > **Exceptions** > **Objects** apply only to threat protection rules.
- Policy exceptions does not affect Sender Filtering
- If DDEI is registered to Apex Central, DDEI synchronizes Suspicious Object exceptions from Apex Central every 10 minutes. Synchronized Suspicious Objects exceptions are listed under **Policies** > **Exceptions** > **Objects** including the source info of Apex Central
- **Policies** > **Exceptions** > **Messages**, supports wildcard (*)
- **Policies** > **Exceptions** > **Objects**, **URL** objects supports wildcard (*)

For some one-click URL, if accessed by DDEI, the administrator can add them into the **Policies** > **Exceptions** > **URL** Keywords list, so that DDEI will not access those URLs.

As an example, if the administrator trusts all mails from bryan_xu@msn.com and does not want DDEI to scan and take actions on all mails from this sender, the administrator can add bryan_xu@msn.com into the **Policies** > **Exceptions** > **Messages** > **Senders** list.

Another example would be false detection for a normal application file, in this case, add the file SHA1 value to into **Policies** > **Exceptions** > **Objects** exceptions list.

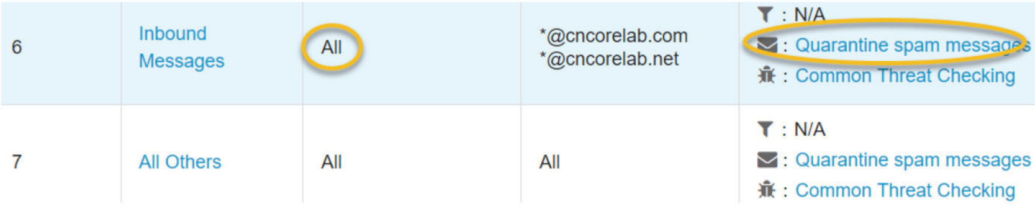
DDEI5.1 supports Email Encryption Exceptions on **Policies** > **Exceptions** > **Email Encryption Exceptions**. Specify the scanning conditions and actions to apply to messages that DDEI does not encrypt or decrypt.

Additional Sample Policies

The sender exception settings under **Policies** > **Exceptions** > **Messages** apply to all types of rules, including content filtering rules, antispam rules, and threat protection rules. However, exception settings cannot be used to skip a rule such as antispam checking because doing so also skips content filter and threat protection checking. Do the following instead of directly setting the approved senders for antispam rule:

1. Create a new policy without the antispam rule in this policy. Other rules are the same as the existing policy, which contains antispam rule.
2. Set the senders' addresses in the approved senders list.
3. Set the newly created policy with a higher priority than the antispam rule enabled policy.

For example, Policy 6 of "Inbound Messages" has quarantined many spam emails, and the administrator wants to set the approved senders for spam rule checking.



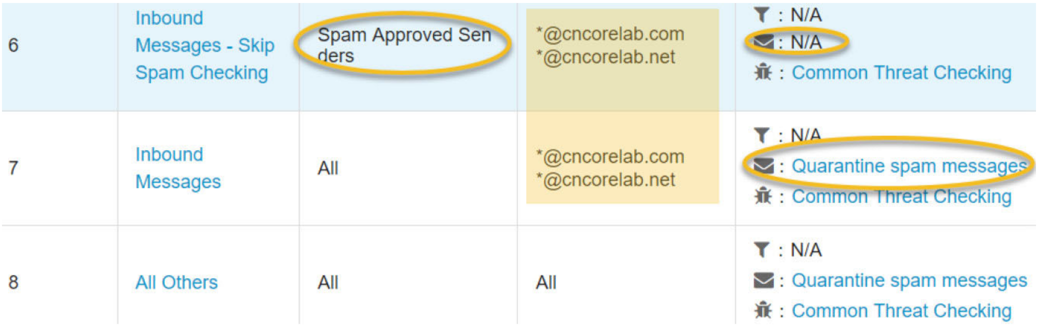
6	Inbound Messages	All	*@cncorelab.com *@cncorelab.net	▼ : N/A ✉ : Quarantine spam messages 🐞 : Common Threat Checking
7	All Others	All	All	▼ : N/A ✉ : Quarantine spam messages 🐞 : Common Threat Checking

The administrator can address this with the following steps.

1. Add a new policy.

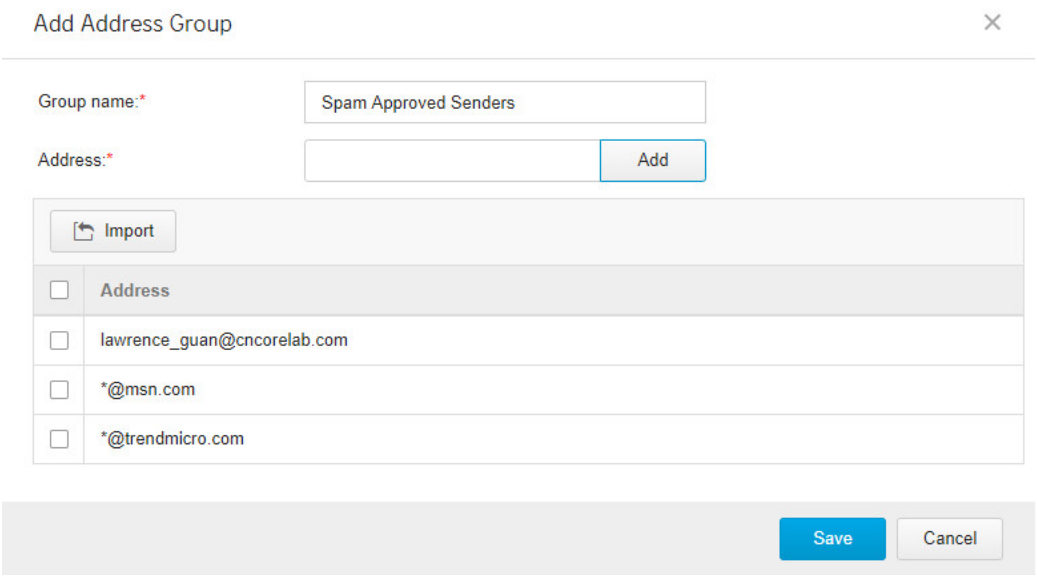
- Status: `Enabled`
- Policy name: ***Inbound Messages - Skip Spam Checking***
- Priority: 6
  - The current policies with a priority lower than 6 (including 6) will have a lower priority than the newly created policy.
- Senders: From address group, Spam Approved Senders.
- Others: The same as the original policy, 6 of "***Inbound Messages***", except for the spam rule. There is no spam rule of "***Quarantine spam messages***" in this newly created policy.

2. The newly created policies will show as follows.



6	Inbound Messages - Skip Spam Checking	Spam Approved Senders	*@cncorelab.com *@cncorelab.net	▼ : N/A ✉ : N/A 🐞 : Common Threat Checking
7	Inbound Messages	All	*@cncorelab.com *@cncorelab.net	▼ : N/A ✉ : Quarantine spam messages 🐞 : Common Threat Checking
8	All Others	All	All	▼ : N/A ✉ : Quarantine spam messages 🐞 : Common Threat Checking

3. Add the email address of the senders that should skip the anti-spam checking into the ***Spam Approved Senders*** address group



Add Address Group ✕

Group name:* Spam Approved Senders

Address:* [Add]

[Import]

□	Address
□	lawrence_guan@cncorelab.com
□	*@msn.com
□	*@trendmicro.com

[Save] [Cancel]

Senders/Recipients Exceptions

Instead of setting the Senders/Recipients exceptions directly into the Policy settings, create a separate policy with a priority higher than the dedicated policy and then add the Senders/ Recipients addresses to the exception list.

The sample policies such as ***Sent to Bosses***, and ***Sent from Bosses*** as defined in "Create Sample Policies" on page 52 are example policies of Senders/Recipients exceptions.

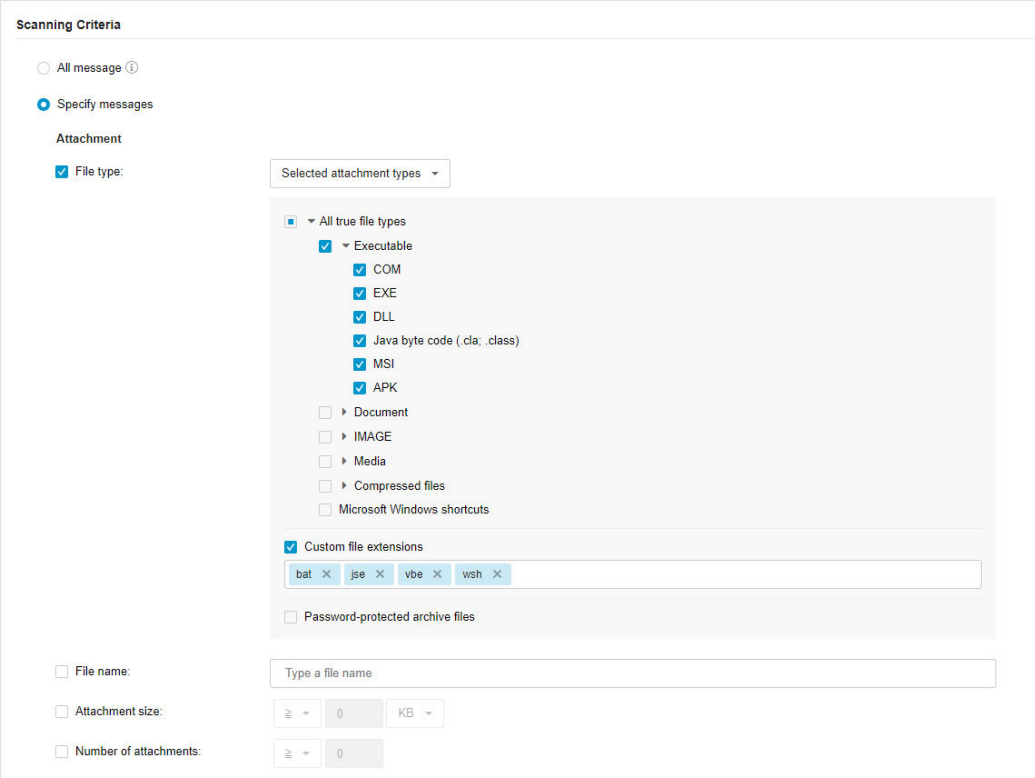
Multiple Content Filtering Conditions Checking

Each content filtering rule can check for different criteria such as file type, file name, attachment size, keywords. If a rule contains more than one scanning criteria, such as if it includes file type checking and keywords, then all of those scanning criteria needs to be triggered.

When creating a policy that should trigger ANY of the content criteria, use multiple content filtering rules. Each rule should contain one scanning criteria and add all of the created content filtering rules into the policy.

Take note of the following examples where it only needs to match one of the criteria to trigger the rule:

- Custom file type:



Scanning Criteria

○ All message ⓘ

● Specify messages

Attachment

☑ File type: Selected attachment types ▾

- ■ ▾ All true file types
  - ☑ ▾ Executable
    - ☑ COM
    - ☑ EXE
    - ☑ DLL
    - ☑ Java byte code (.cla; .class)
    - ☑ MSI
    - ☑ APK
  - □ ▸ Document
  - □ ▸ IMAGE
  - □ ▸ Media
  - □ ▸ Compressed files
  - □ Microsoft Windows shortcuts

☑ Custom file extensions: bat ✕ jse ✕ vbe ✕ wsh ✕

□ Password-protected archive files

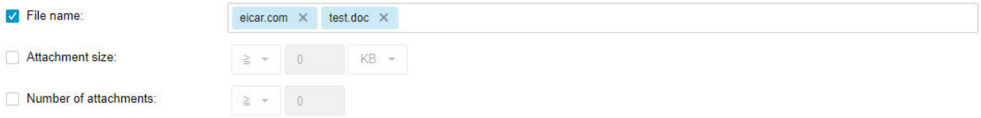
□ File name: Type a file name

□ Attachment size: ≧ ▾ 0 KB ▾

□ Number of attachments: ≧ ▾ 0

This filter means that the email will match the custom file extensions criteria if it contains any one type of attachment such as `test.exe` and `test.bat`

- Attachment file name



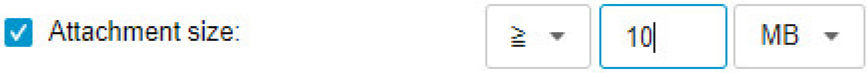
☑ File name: eicar.com ✕ test.doc ✕

□ Attachment size: ≧ ▾ 0 KB ▾

□ Number of attachments: ≧ ▾ 0

This filter means that the email will match the File name criteria if it `eicar.com` or `test.doc` file attachment

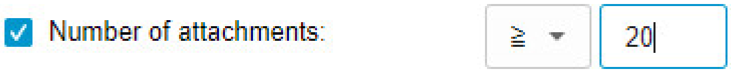
- Attachment size



☑ Attachment size: ≧ ▾ 10 MB ▾

This filter means that the email will match the attachment size criteria if the attachment is equal or greater than 10 MB.

- Number of attachments

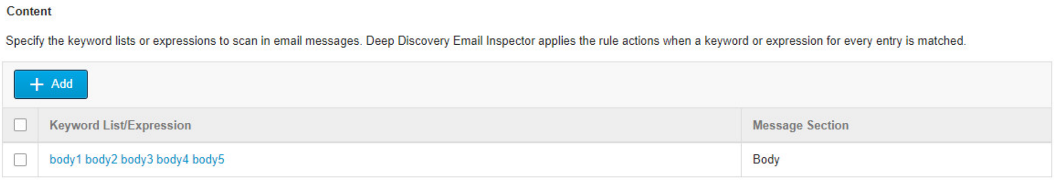


☑ Number of attachments: ≧ 20

This means that the email will match the number of attachments criteria if it contains 20 or more attachments.

- Keywords:

In the example, the email will match the "body1 body2 body3 body4 body5" criteria if the message body contains any of the keywords in the list.

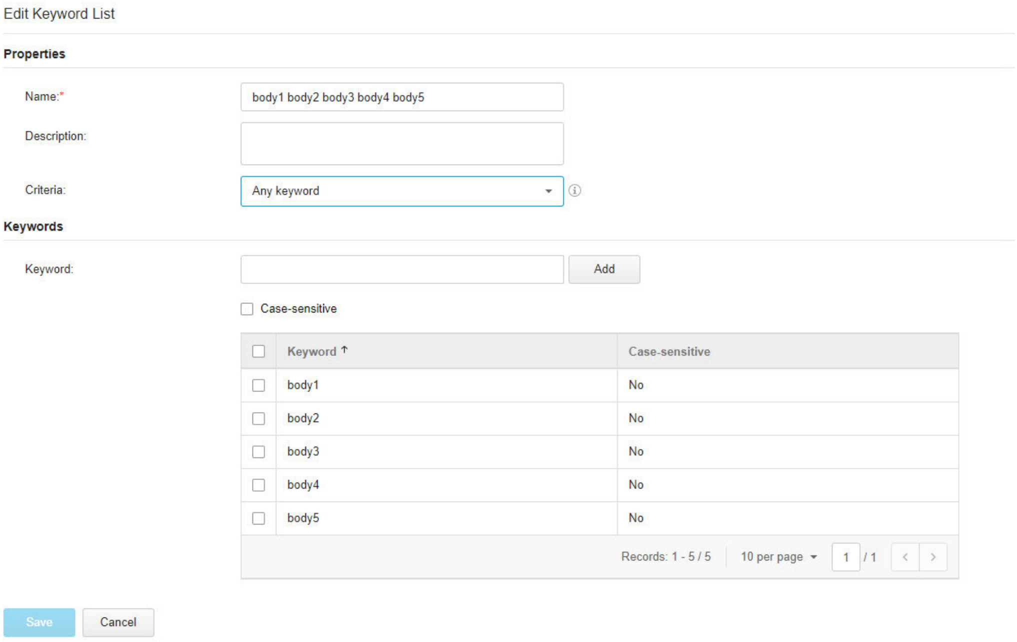


Content

Specify the keyword lists or expressions to scan in email messages. Deep Discovery Email Inspector applies the rule actions when a keyword or expression for every entry is matched.

□	Keyword List/Expression	Message Section
□	body1 body2 body3 body4 body5	Body

To create this filter, define the keyword list first in **Policy Objects** > **Data Identifiers** > **Keywords List**:



Edit Keyword List

Properties

Name:* body1 body2 body3 body4 body5

Description:

Criteria: Any keyword

Keywords

Keyword:

□ Case-sensitive

□	Keyword ↑	Case-sensitive
□	body1	No
□	body2	No
□	body3	No
□	body4	No
□	body5	No

Records: 1 - 5 / 5 10 per page 1 / 1

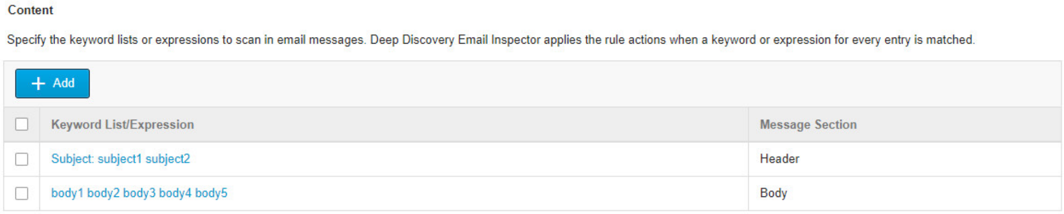
To do content checking with multiple criteria such as in the following examples:

```
(Mail subject contains subject1 or subject 2) AND (Mail body
contains body1 or body2 or body3 or body4)
```

- OR -

```
 (Mail subject contains subject1 or subject 2) OR (Mail body
contains body1 or body2 or body3 or body4 or body5)
```

Create a separate content rule to address these conditions. One rule with the keywords ***subject1*** or ***subject2*** and another content rule for the keywords ***body1***, ***body2***, ***body3***, ***body4***, ***body5***.



Content

Specify the keyword lists or expressions to scan in email messages. Deep Discovery Email Inspector applies the rule actions when a keyword or expression for every entry is matched.

□	Keyword List/Expression	Message Section
□	Subject: subject1 subject2	Header
□	body1 body2 body3 body4 body5	Body

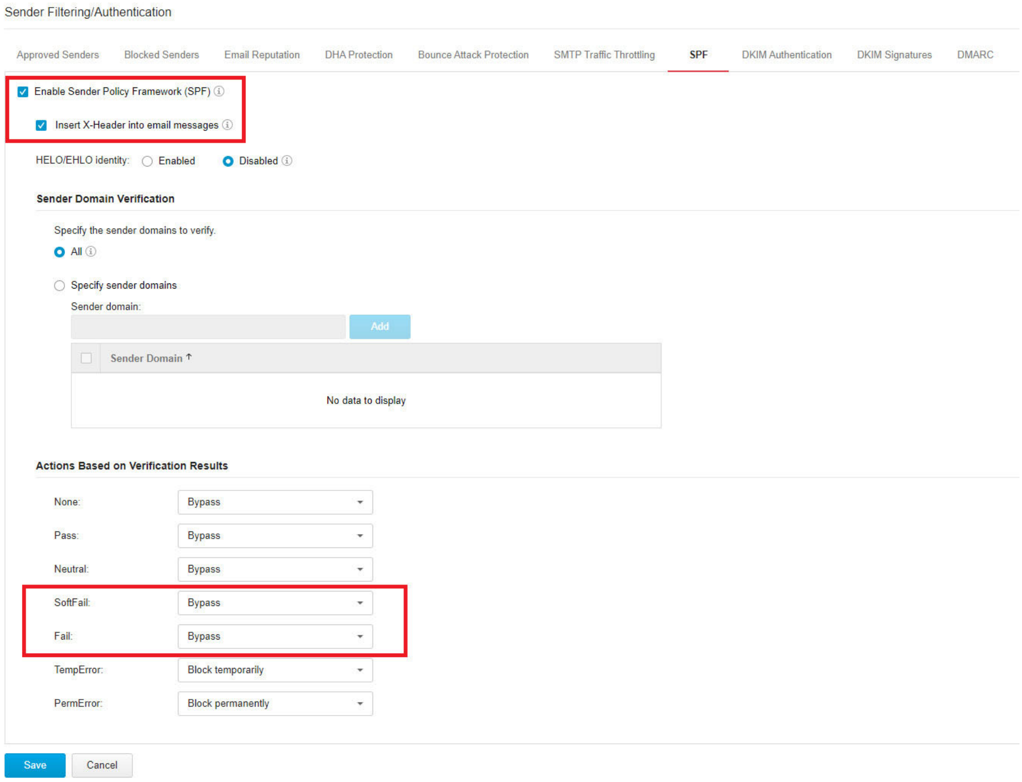
- Sender authentication results

To use Sender Authentication Results as criteria in the Content Filtering Rule, configure SPF/DKIM/DMARC actions to bypass Sender Filtering/Authentication and insert the x-header into the message. See “Sender Filtering Settings” on page 68 for more details.

Since there is no option to quarantine messages in Sender Filtering/Authentication, use the Content Filter rule to do the quarantine action.

The following is an example of setting SPF in Sender Authentication Results for Content Filter rule.

  - Enable SPF and set options for actions for Fail and Softfail



Sender Filtering/Authentication

Approved Senders | Blocked Senders | Email Reputation | DHA Protection | Bounce Attack Protection | SMTP Traffic Throttling | SPF | DKIM Authentication | DKIM Signatures | DMARC

☑ Enable Sender Policy Framework (SPF)

☑ Insert X-Header into email messages

HELO/EHLO identity: ○ Enabled ● Disabled

Sender Domain Verification

Specify the sender domains to verify.

● All

○ Specify sender domains

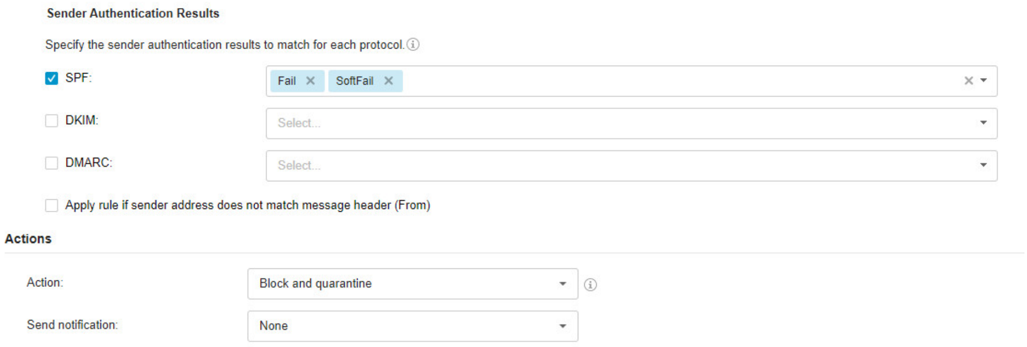
Sender domain:

□	Sender Domain ↑
	No data to display

Actions Based on Verification Results

None:	Bypass
Pass:	Bypass
Neutral:	Bypass
SoftFail:	Bypass
Fail:	Bypass
TempError:	Block temporarily
PermError:	Block permanently

- Create a Content Filtering rule, that will be triggered if the SPF check is Fail or Softfail



Sender Authentication Results

Specify the sender authentication results to match for each protocol.

☑ SPF:	Fail ✕ SoftFail ✕
□ DKIM:	Select...
□ DMARC:	Select...

□ Apply rule if sender address does not match message header (From)

Actions

Action:	Block and quarantine
Send notification:	None

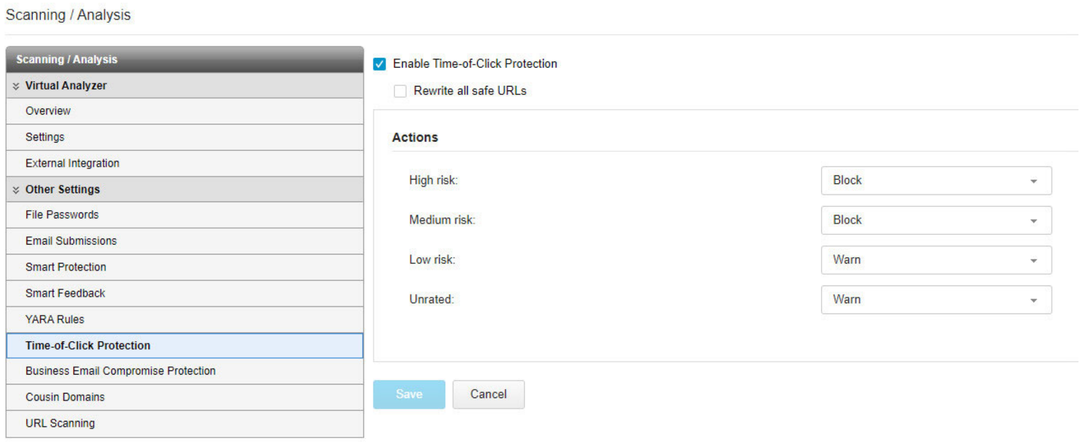
6.3. Time-Of-Click Protection

Use Time-of-Click for protection against malicious URLs in email messages. When this feature is enabled, DDEI rewrites suspicious URLs in email messages for further analysis. Trend Micro Smart Protection Network (SPN) analyzes a rewritten URL every time the URL is clicked and applies specified actions based on the URLs' risk levels.

To enable this option:

1. Login to the DDEI Web console
2. Go to **Administration** > **Scanning / Analysis** > **Other Settings** > **Time-of-Click Protection**

Optionally enable "***Rewrite all safe URLs***" to also rewrite URLs that Web Reputation Services (WRS) consider safe in email messages for further analysis.



☑ Enable Time-of-Click Protection

□ Rewrite all safe URLs

Actions

High risk:	Block
Medium risk:	Block
Low risk:	Warn
Unrated:	Warn

The risk level pertains to the Virtual Analyzer analysis result and is based on WRS scores:

WRS Score	Risk Level	Description
81~100	Safe	No known or potential threats
66~68 except 71	Minimal Risk	Associated with spam or has a history of being compromised
51~65	Medium Risk	Possibly a phishing page or a potential source of malware or spyware
0~50	High Risk	Verified to be phishing page or a source of malware or spyware
*71	Unrated	Unrated or Unknown

TABLE 6.3.1.1: WRS Scores and Risk Level Equivalent

NOTE: DDEI 5.1 Time-Of-Click protection does not rewrite the URLs that have keywords that match any of those defined in **Policies** > **Exception** > **URL Keywords**

6.4. Transport Layer Security (TLS)

In MTA mode, enabling TLS encrypts the SMTP traffic. DDEI supports TLS v1.0, v1.1 and v1.2 and will always try to use the higher TLS version to communicate when sending or receiving MTA. To enable this option:

1. Login to the DDEI Web console
2. Go to **Administration** > **Mail Settings** > **Connections**

If the administrator wants to replace the default TLS certificate with their own certificate, refer to the following steps:

1. Prepare the certificate file in PEM format and put all types of certificates into one PEM file using the following structure:

```
-----BEGIN RSA PRIVATE KEY-----
Private key base64 code lines
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
Server Certificate base64 code lines
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate Certificate base64 code lines
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root Certificate base64 code lines
-----END CERTIFICATE-----
```

2. 2.In the DDEI Web console, go to **Administration** > **Mail Settings** > **Connections** and upload the following with your own certificate file that was prepared in the previous step:

- CA certificate
- Private key
- SMTP server certification

3. Save the changes.
4. Send incoming test emails to make sure that TLS works as expected. If DDEI can be accessed via the Internet, use the www.checktls.com website to do testing.

6.5. Sender Filtering Settings

Sender Filtering features work when DDEI is on MTA mode and the Gateway Module license is activated. In DDEI 5.1, Sender Filtering checks for the following:

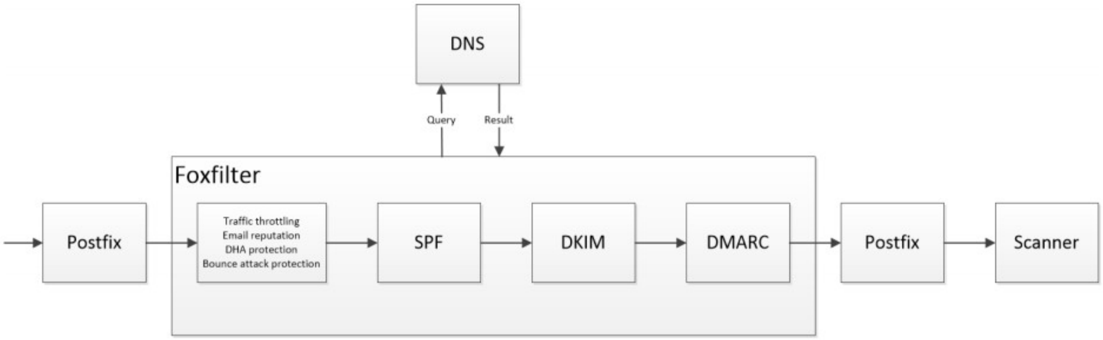
- Email Reputation Services (ERS)
- DHA Protection
- Bounce Attack Protection
- SMTP Traffic Throttling
- SPF
- DKIM
- DMARC

NOTE:

Refer to the "Sender Filtering Settings" and "Sender authentication results" section on DDEI 5.1 Administrator Guide for more information for a sample setting about Sender Authentication in Content Filtering rule.

6.5.1. Enable Sender Filtering

The following is the scan order for DDEI 5.1 Sender Filtering:



With the Gateway Module license activated, evaluate if the Sender Filtering features should be enabled or not depending on the requirements.

Below are the major settings for Sender Filtering features:

1. If DDEI is deployed as a non-edge, go to **Administration** > **Mail Settings** > **Edge MTA Relay Servers** and specify the edge MTA servers that relay the external messages to DDEI.

2. To enable Email Reputation (ERS) checking without a portal account, sign up for an ERS portal account:

- Go to https://ers.trendmicro.com
- Click Sign in to sign up for an ERS portal account by providing a Gateway Module license (Activation Code).

3. Configure the settings for Email Reputation, DHA Protection, Bounce Attack Protection, Traffic Throttling, SMTP, SPF, DKIM/DMARC as necessary.

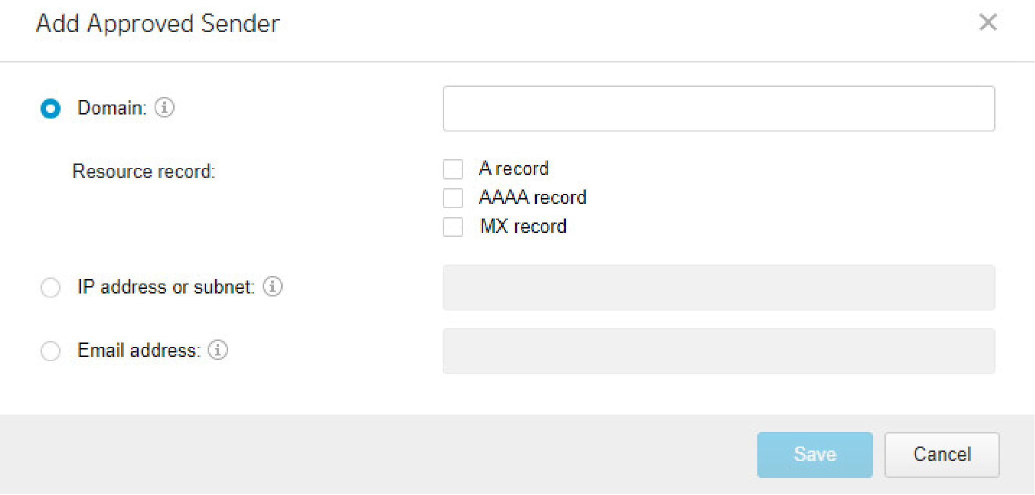
6.5.2. Maintain Sender Filtering

DDEI blocks any IP address or sender email address that trigger the sender filtering rules.

Approved Senders

The Approved Senders is a list of trusted senders that bypass sender filtering and sender authentication in DDEI. Configure this setting by going to **Administration** > **Sender Filtering/ Authentication** > **Approved Senders**.

- In the Approved Senders, the Domain type resolves the domain into IP addresses based on the selected options, and the changes only take effect on those with resolved IP addresses.
- For the IP address list (Including resolved domain IP and added IP), it affects all entries in the Sender Filtering section
- For the email address list, it only takes effect on SMTP Traffic Throttling



Add Approved Sender

● Domain:

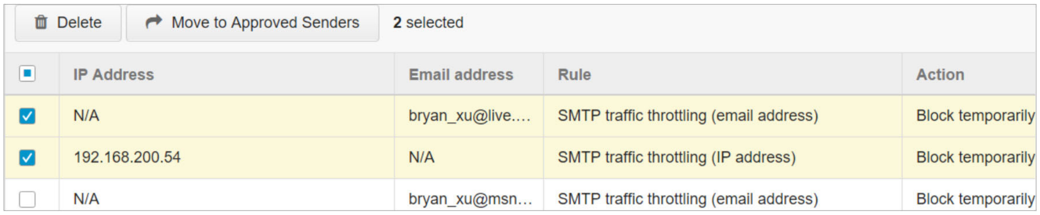
Resource record: □ A record □ AAAA record □ MX record

○ IP address or subnet:

○ Email address:

Blocked Senders

The Blocked Senders is a list of senders that DDEI blocks permanently or temporarily. Configure this setting by going to **Administration** > **Sender Filtering/Authentication** > **Blocked Senders**. The block list contains the blocked IP or email address, block reason, and action. For false positive detections, move the entry to the Approved Senders.



■	IP Address	Email address	Rule	Action
☑	N/A	bryan_xu@live....	SMTP traffic throttling (email address)	Block temporarily
☑	192.168.200.54	N/A	SMTP traffic throttling (IP address)	Block temporarily
☐	N/A	bryan_xu@msn...	SMTP traffic throttling (email address)	Block temporarily

6.5.3. SPF, DKIM, and DMARC Identification

DDEI supports the following sender authentication standards to effectively detect and fight against techniques used in email phishing and spoofing:

- Sender Policy Framework (SPF)
- DomainKeys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting & Conformance (DMARC)

SPF

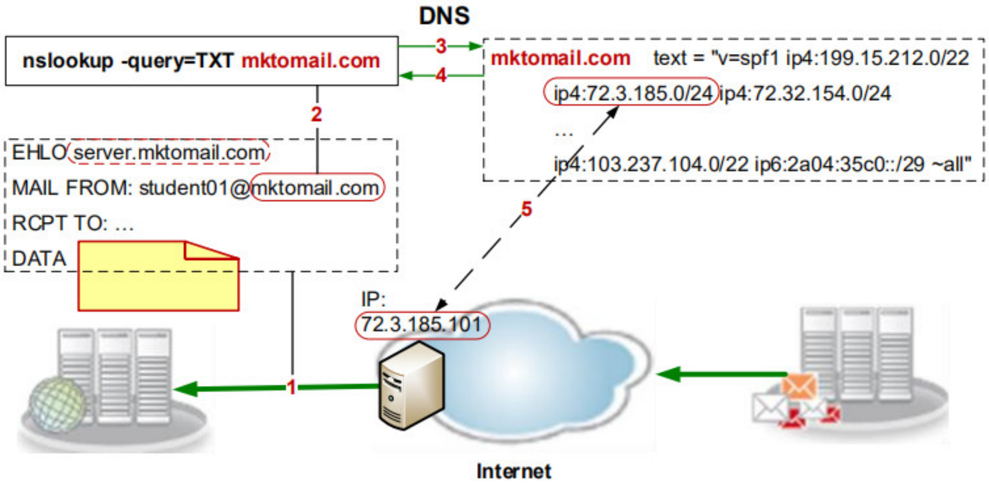
Sender Policy Framework (SPF) is an email validation protocol designed to detect and block email spoofing by providing a mechanism to allow receiving mail exchangers to verify that incoming mail from a domain comes from an IP Address authorized by that domain's administrators.

The list of authorized sending hosts and IP addresses for a domain is published in the DNS in a specially formatted TXT record.

DDEI uses the domain of "Envelope From" address or HELO/EHLO to query the SPF DNS record and confirm that the sending IP address is allowed to do that based on the DNS record.

1. 1. The SMTP Client establishes a connection to the SMTP Server and submits the EHLO and MAIL FROM commands.
2. The mail server extracts the domain name from the MAIL FROM command. It can also use the domain name provided in the EHLO command.
3. The mail server queries the DNS record of type TXT for this domain.
4. The DNS server responds with the TXT record for the specified domain that includes the instructions on handling the mail client's IP address.
5. The mail server checks if the mail client's source IP address matches the instructions and implements the configured action.

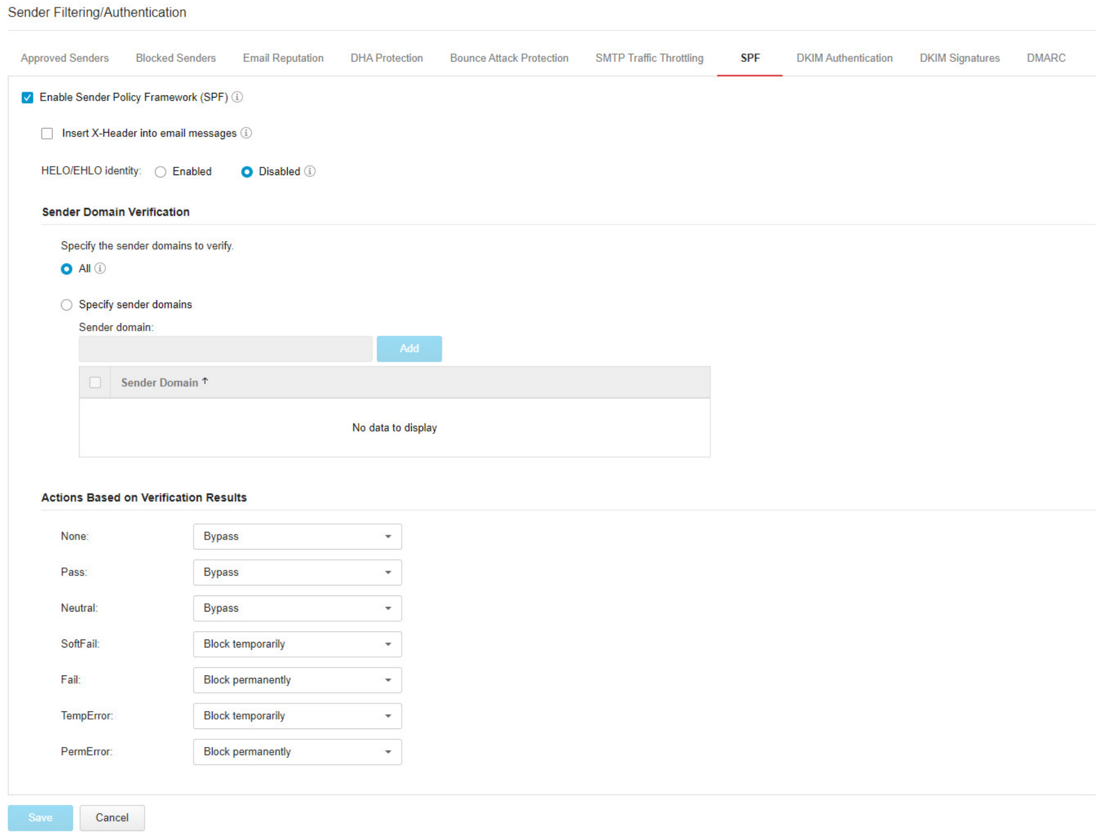
The SPF interaction includes the following steps:


DNS
nslookup -query=TXT mktomail.com
3
4
mktomail.com text = "v=spf1 ip4:199.15.212.0/22
ip4:72.3.185.0/24 ip4:72.32.154.0/24
...
ip4:103.237.104.0/22 ip6:2a04:35c0::/29 ~all"
2
EHLO server.mktomail.com
MAIL FROM: student01@mktomail.com
RCPT TO: ...
DATA
5
IP:
72.3.185.101
1
Internet

To configure this setting, go to **Administration** > **Sender Filtering/Authentication** > **SPF**. This option is off by default and has the following settings:

- Enable/disable SPF authentication
- Enable/disable verification result X-header insert
- Enable/disable HELO/EHLO identity when doing SPF authentication
- Choose all domains or specify some domains for SPF checking

NOTE: Opening all domains may increase latency time in DDEI due to every messages querying the DNS SPF record



☑ Enable Sender Policy Framework (SPF) ⓘ

☐ Insert X-Header into email messages ⓘ

HELO/EHLO identity: ○ Enabled ● Disabled ⓘ

Sender Domain Verification

Specify the sender domains to verify.

● All ⓘ

○ Specify sender domains

Sender domain:

☐	Sender Domain ↑
	No data to display

Actions Based on Verification Results

None:	Bypass
Pass:	Bypass
Neutral:	Bypass
SoftFail:	Block temporarily
Fail:	Block permanently
TempError:	Block temporarily
PermError:	Block permanently

Three actions are available based on the SPF verification result:

- Bypass
- Block temporarily
- block permanently

Evaluation of an SPF record can return any of the following results:

Result	Description
Pass	The SPF record designates the host to be allowed to send.
Fail	The SPF record has designated the host as not being allowed to send.
SoftFail	The SPF record has designated the host as not being allowed to send but is in transition.
Neutral	The SPF record specifies explicitly that nothing can be said about validity.
None	The domain does not have an SPF record or the SPF record does not evaluate to a result.

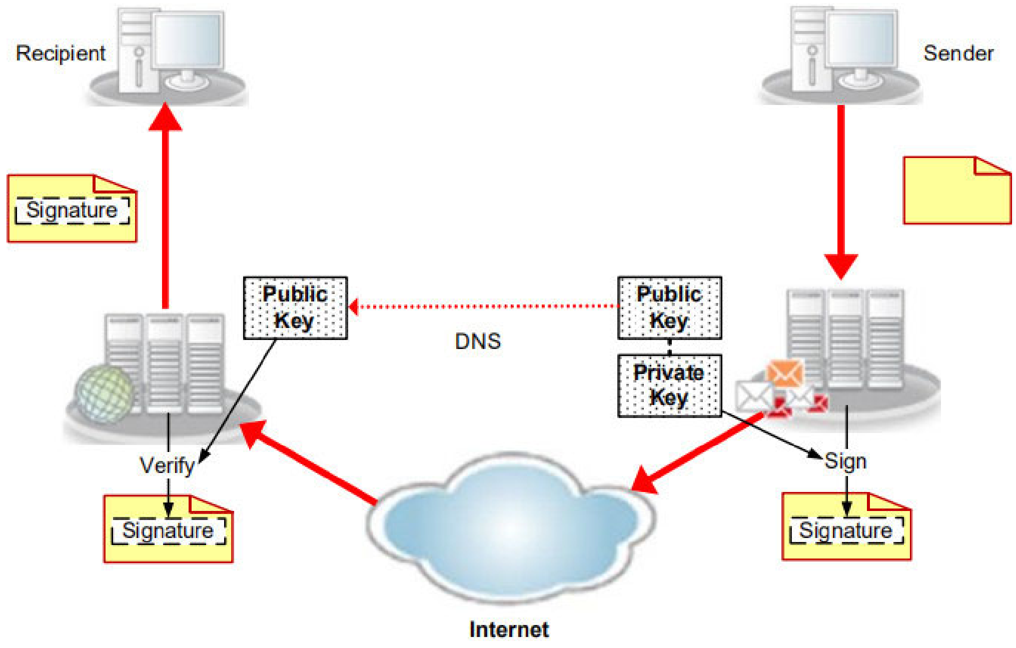
TABLE 6.5.1.1: SPF Result Definition

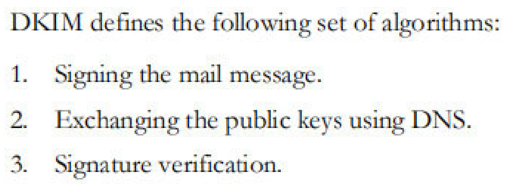
Result	Description
PermError	A permanent error has occurred (for example, badly formatted SPF record).
TempError	A transient error has occurred.

TABLE 6.5.1.1: SPF Result Definition

DKIM

DomainKeys Identified Mail (DKIM) allows the receiver to check that an email claimed to have come from a specific domain was indeed authorized by the owner of that domain. It is intended to prevent forged sender addresses in emails, a technique often used in phishing and email spam.



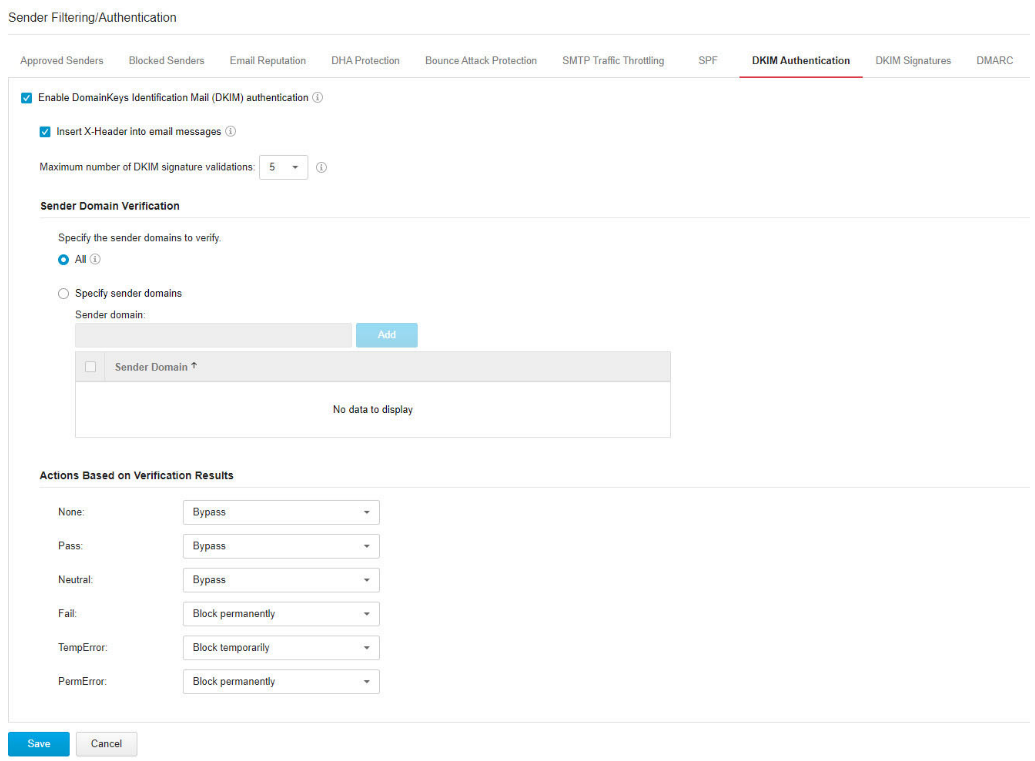

DKIM defines the following set of algorithms:

1. Signing the mail message.
2. Exchanging the public keys using DNS.
3. Signature verification.

To configure this setting, go to **Administration** > **Sender Filtering/Authentication** > **DKIM Authentication**. This option is off by default and has the following options:

- Enable/disable DKIM authentication
- Enable/disable verification result X-Header insert
- DKIM signature count can be specified from 1 – 20 (default 5)
- Choose all domains or specify some sender domains to do DKIM check

NOTE: If specified sender domains are added, it will be compared to the 'From' value in email header to determine whether messages need DKIM authentication or not.



☑ Enable DomainKeys Identification Mail (DKIM) authentication ⓘ

☑ Insert X-Header into email messages ⓘ

Maximum number of DKIM signature validations: 5 ⓘ

Sender Domain Verification

Specify the sender domains to verify.

● All ⓘ

○ Specify sender domains

Sender domain:

□	Sender Domain ↑
	No data to display

Actions Based on Verification Results

None:	Bypass
Pass:	Bypass
Neutral:	Bypass
Fail:	Block permanently
TempError:	Block temporarily
PermError:	Block permanently

The following actions are available based on the DKIM authentication result:

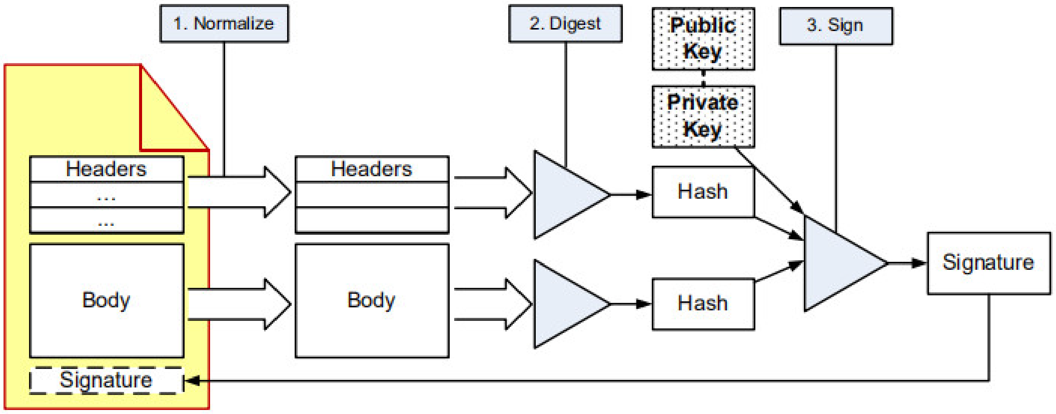
- Bypass
- Block temporarily
- Block permanently

DKIM SIGNATURES

With DKIM Signatures, DDEI adds a digital signature to outgoing email headers to prevent spoofing. Recipients can verify that the domain's administrator authorizes the email messages from a specific domain and that the messages, including attachments, have not been modified during transport. This option is in **Administration** > **Sender Filtering/Authentication** > D**KIM Signatures** and is disabled by default.

NOTE: Configuring DDEI to sign an incoming message that already contains digital signatures from other email services (Such as Gmail) or MTAs, removes all existing signatures from the message before adding the new signature and sending it.

The message signing procedure includes the following major steps:



Below is a sample DKIM signature:

```
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple;
d=cncorelab.com;
s=default; t=1608205449;
bh=o4hKUvcCBRt7Emy/1QHkYU+HVY7EoYC56dlnD5y0DB0=; l=1517; h=From;
b=aFKZLqRmjgt/
BJEyd1RDO5WSCEQMHgM7gAcrsInDeGLL+hRb7VhyJOaAmLvmZRHbN
f3y4XNmcohZ7flSuqkbolT5jZE/So1svJe5iIg4zE8afLyZyw0ogY/
nfykL7kWY9Qz
UxvY5aIx9v2hB6SFaRefdJWtWEmQsQH8Sp5eAZcg=
```

DMARC

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is an email validation system designed to detect and prevent email spoofing. It is useful for detecting specific techniques often used in phishing and email spam, such as emails with forged sender addresses that appear to originate from legitimate organizations.

DMARC provides a way to authenticate email messages for specific domains, send feedback to senders, and conform to a published policy.

DMARC also helps email recipients determine if the purported message aligns with what the recipient knows about the sender. If not, DMARC includes guidance on how to handle the non-aligned messages.

DMARC RECORDS

DMARC records are published to DNS as TXT resource records and indicates what should be done with incoming emails when validation fails.

Refer to the following DMARC record published on the domain named "sender.exampledomain.com":

```
v=DMARC1;p=reject;pct=100;rua=mailto:postmaster@exampledomain.com
```

In this example, the sender requests the receiver to reject the failed email completely and send report to postmaster@exampledomain.com. "reject" could be replaced with "quarantine" or "none".

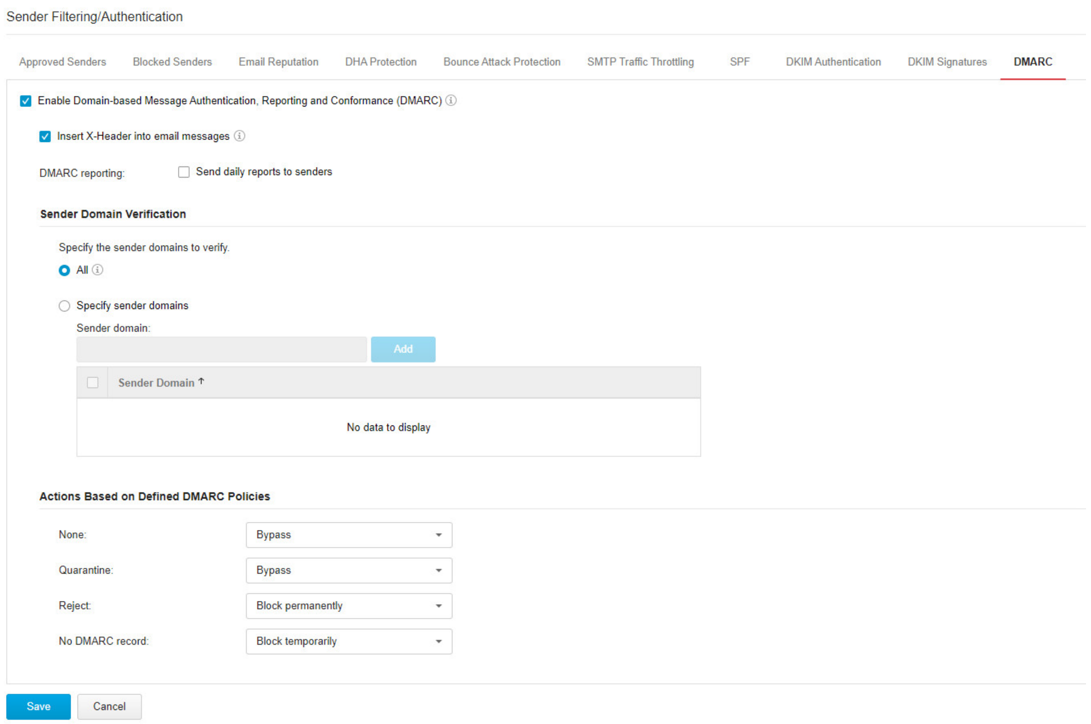
DMARC requires the following:

- A message that passes the SPF check
- A message that passes the DKIM authentication check
- Alignment of identifier domains (Identifier alignment requires that a domain authenticated by SPF and DKIM is the same as the message header domain or parent domain.)

To configure this setting, go to **Administration** > **Sender Filtering/Authentication** > **DMARC**. DMARC is off by default and has the following options:

- Enable/disable DMARC authentication
- Eenable/disable verification result X-Header insert
- Enable/disable DMARC reporting•Choose all domains or specify some domains to do DMARC check.

NOTE: If specified sender domains are added, they will be compared to the 'From' value in the email header to determine whether messages need DMARC authentication or not.



☑ Enable Domain-based Message Authentication, Reporting and Conformance (DMARC)

☑ Insert X-Header into email messages

DMARC reporting: □ Send daily reports to senders

Sender Domain Verification

Specify the sender domains to verify.

● All

○ Specify sender domains

Sender domain:

□	Sender Domain ↑
	No data to display

Actions Based on Defined DMARC Policies

None:	Bypass
Quarantine:	Bypass
Reject:	Block permanently
No DMARC record:	Block temporarily

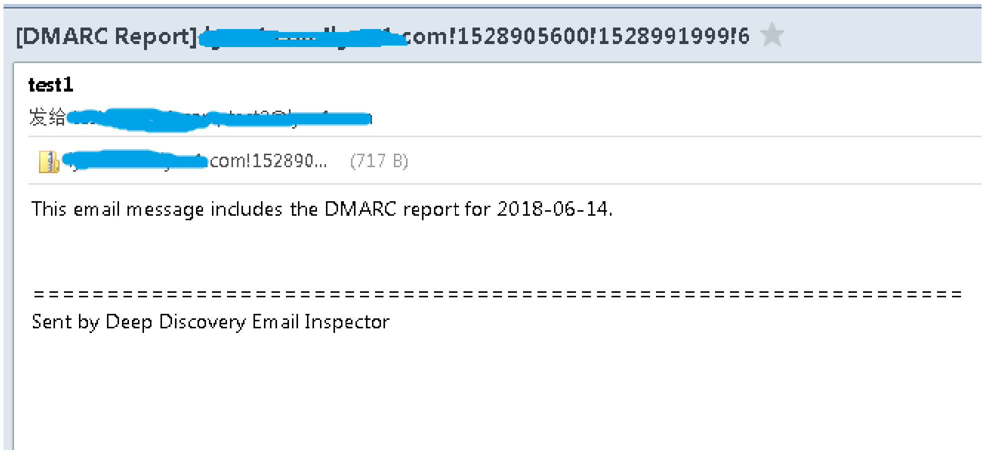
The following actions are available based on the DMARC authentication result:

- Bypass
- Block temporarily
- Block permanently

SPF Validation Result	SPF Alignment Result	DKIM Validation Result	DKIM Alignment Result	DMARC Result	Default Action for DMARC Policy
Pass	Pass	ANY	ANY	Pass	Bypass always
ANY	ANY	Pass	Pass	Pass	Bypass always
Any other situations				Fail	Check actions based on DMARC result Default: • None: Bypass • Quarantine: Bypass • Reject: Block permanently • No DMARC record: Block temporarily

TABLE 6.5.1.2: DMARC Authentication Policy

The following is a sample report content for failed DMARC result with reporting enabled:



[DMARC Report][redacted]com!1528905600!1528991999!6

test1

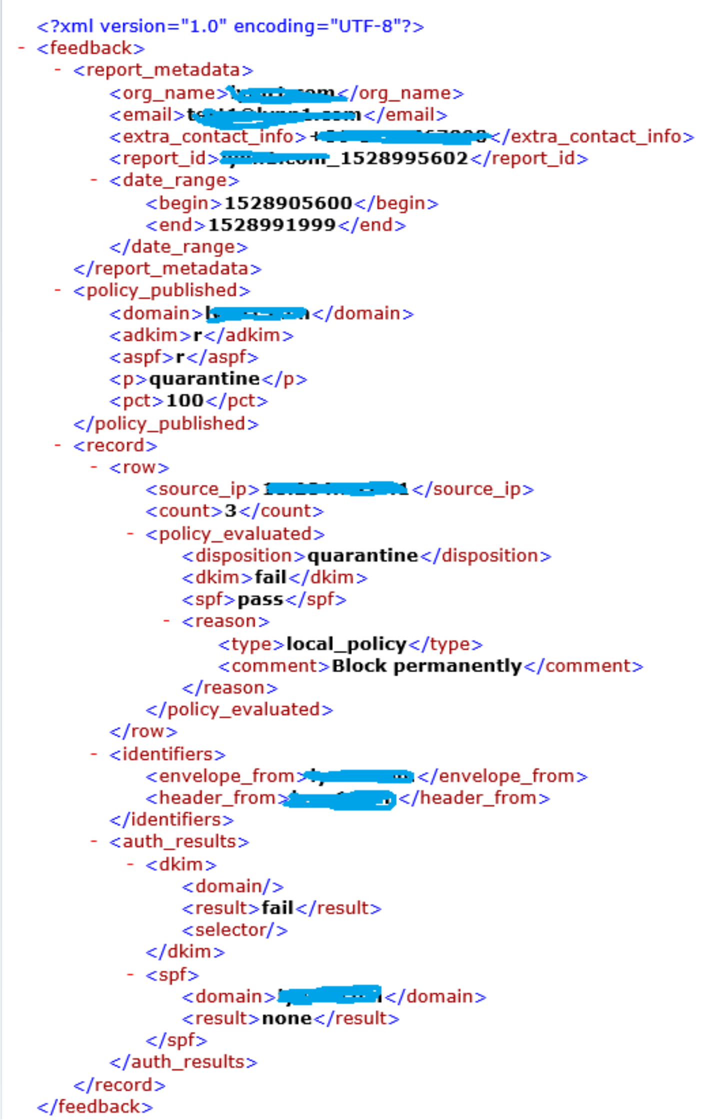
发给[redacted]

[redacted]com!152890... (717 B)

This email message includes the DMARC report for 2018-06-14.

==

Sent by Deep Discovery Email Inspector



```
  <?xml version="1.0" encoding="UTF-8"?>
- <feedback>
  - <report_metadata>
      <org_name>[redacted]</org_name>
      <email>[redacted]</email>
      <extra_contact_info>[redacted]</extra_contact_info>
      <report_id>[redacted]_1528995602</report_id>
    - <date_range>
        <begin>1528905600</begin>
        <end>1528991999</end>
      </date_range>
    </report_metadata>
  - <policy_published>
      <domain>[redacted]</domain>
      <adkim>r</adkim>
      <aspf>r</aspf>
      <p>quarantine</p>
      <pct>100</pct>
    </policy_published>
  - <record>
    - <row>
        <source_ip>[redacted]</source_ip>
        <count>3</count>
      - <policy_evaluated>
          <disposition>quarantine</disposition>
          <dkim>fail</dkim>
          <spf>pass</spf>
        - <reason>
            <type>local_policy</type>
            <comment>Block permanently</comment>
          </reason>
        </policy_evaluated>
      </row>
    - <identifiers>
        <envelope_from>[redacted]</envelope_from>
        <header_from>[redacted]</header_from>
      </identifiers>
    - <auth_results>
      - <dkim>
          <domain/>
          <result>fail</result>
          <selector/>
        </dkim>
      - <spf>
          <domain>[redacted]</domain>
          <result>none</result>
        </spf>
      </auth_results>
    </record>
  </feedback>
```

6.6. NIC Teaming Configuration

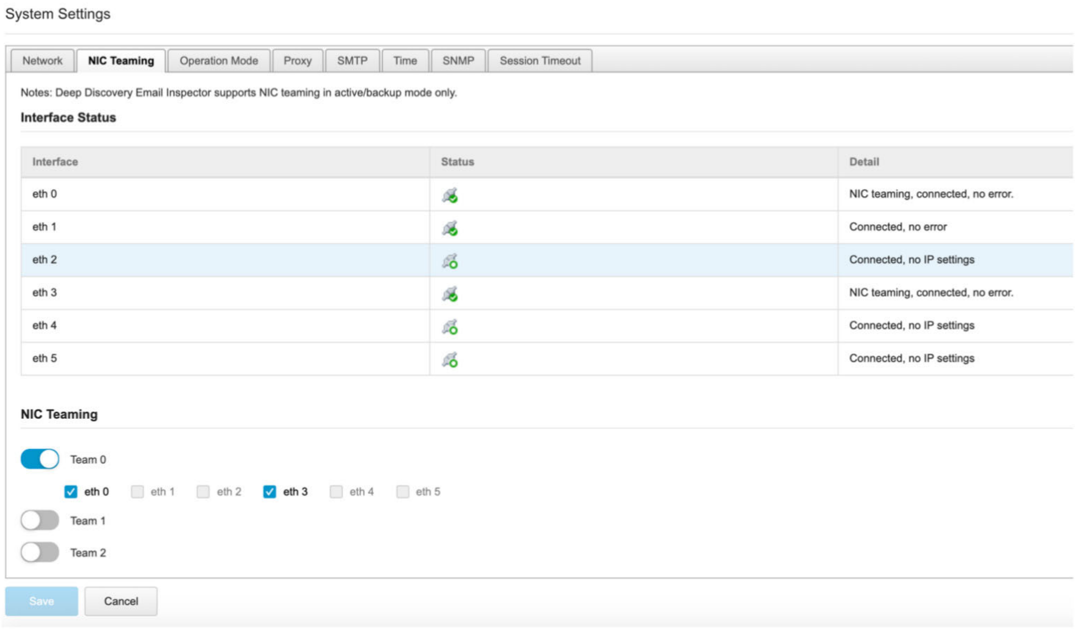
A network interface card (NIC) team is a software-based virtual network interface that provides fault tolerance in the event of a network interface card failure. In DDEI, a NIC team can comprise of one or more network interface cards.

1. Login to the DDEI Web console
2. Go to **Administration** > **System Settings** > **NIC Teaming**
3. Under the NIC Teaming section, do the following:

- Toggle the ***Status*** button to enable a NIC team.
- Select one or more network interface cards to add to the NIC team.

4. Click **Save**.

DDEI will restart and may take some time. Wait for the process to complete before accessing the Web console.



Notes: Deep Discovery Email Inspector supports NIC teaming in active/backup mode only.

Interface Status

Interface	Status	Detail
eth 0	✓	NIC teaming, connected, no error.
eth 1	✓	Connected, no error
eth 2	✓	Connected, no IP settings
eth 3	✓	NIC teaming, connected, no error.
eth 4	✓	Connected, no IP settings
eth 5	✓	Connected, no IP settings

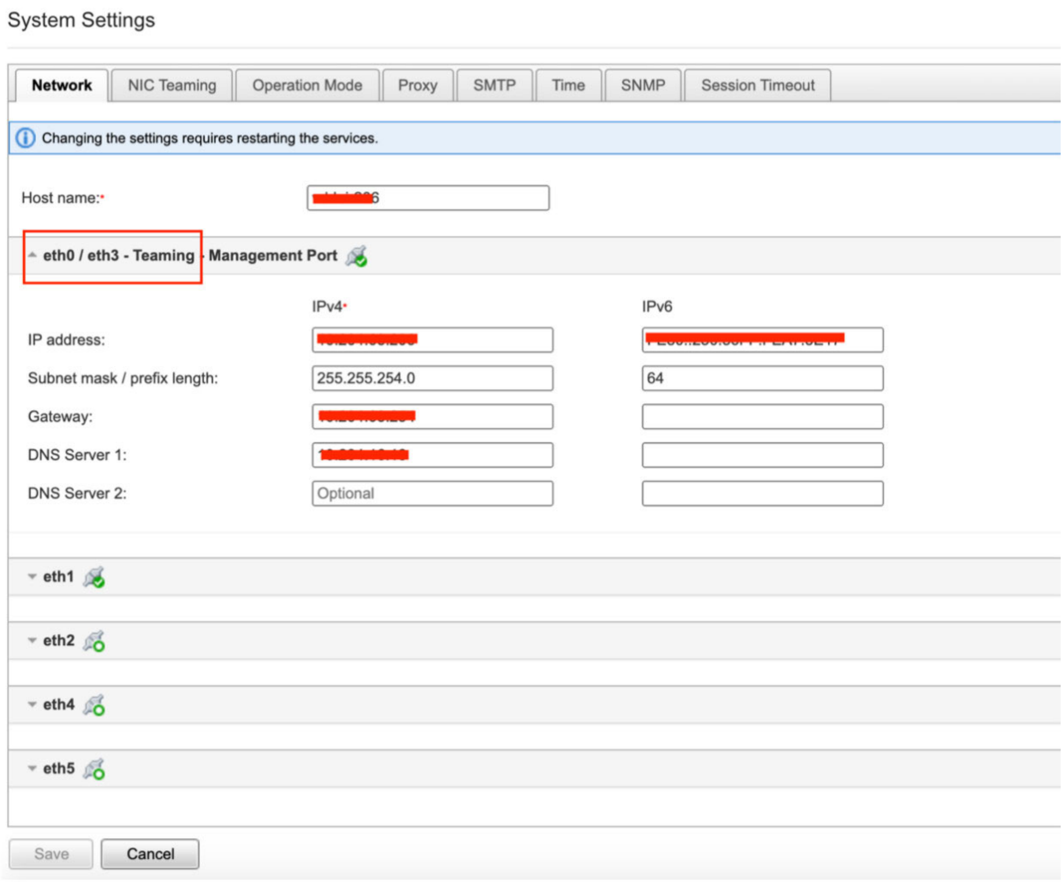
NIC Teaming

● Team 0

☑ eth 0 □ eth 1 □ eth 2 ☑ eth 3 □ eth 4 □ eth 5

○ Team 1

○ Team 2



System Settings

Changing the settings requires restarting the services.

Host name:* [redacted]

eth0 / eth3 - Teaming - Management Port

	IPv4*	IPv6
IP address:	[redacted]	[redacted]
Subnet mask / prefix length:	255.255.254.0	64
Gateway:	[redacted]	
DNS Server 1:	[redacted]	
DNS Server 2:	Optional	

Take note of the following when using NIC teaming:

1. 1. DDEI supports NIC teaming for active/backup mode only. Active/backup mode is used in binding NICs for Linux and is not related to the DDEI working mode. In this mode, traffic goes through the active NIC first. If the active NIC is down, the system will switch to the backup.
2. The management port is always bound to the eth0 interface. When grouped with the eth0 interface, the other network interface acts as a backup interface.
3. A NIC team group can have up to two network interface cards. A network interface card can only belong to one NIC team.

- TAPPING/SNAP ports or disconnected ports cannot be used for teaming
- DDEI supports up to 3 groups of teaming
  - Based on the max 6 NIC ports (4 onboard + 2 plug-ins)

4. For SPAN/TAP mode, at least 3 NICs are required. The last two are for receiving tapping traffic. When configuring NIC teaming, do not select at least the last two NICs for NIC teaming.
5. All NICs can be used for teaming except for the tapping NIC. This ultimately depends on the environmental requirements.

Lesson 7: End User Quarantine

The End-User Quarantine (EUQ) feature enhances the antispam capabilities in DDEI to reduce false-positives and allow users to manage quarantined spam email messages.

This feature needs a Gateway Module license to be activated.

Take note that in DDEI 5.1, only the messages quarantined by Antispam Rules are shown in EUQ, while the messages quarantined by Content Filtering Rules would not appear in EUQ.

7.1. Enable EUQ

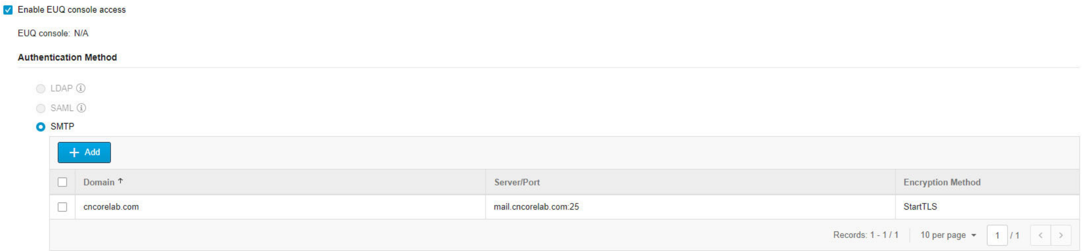
Follow the steps below to enable EUQ:

1. Login to the DDEI Web console
2. Go to **Administration** > **End-User Quarantine** > **Use Quarantine Access** and select **Enable EUQ console access**

   There are three types of authentication methods:

- Use Active Directory for EUQ authentication - Select this option to authenticate users based on their Active Directory account credentials for EUQ console acces
- Use SMTP server for EUQ authentication - Select this option to authenticate users based on their email address account credentials for EUQ console access. Click **+ Add** to add an SMTP server.
- Use SAML for EUQ authentication - Select this option to authenticate users based on SAML single sign-on account credentials from an identity provider.

NOTE: When using a mail system other than Exchange, or in any scenario where AD cannot be used for EUQ authentication, an SMTP server may be used for EUQ authentication



☑ Enable EUQ console access

EUQ console: N/A

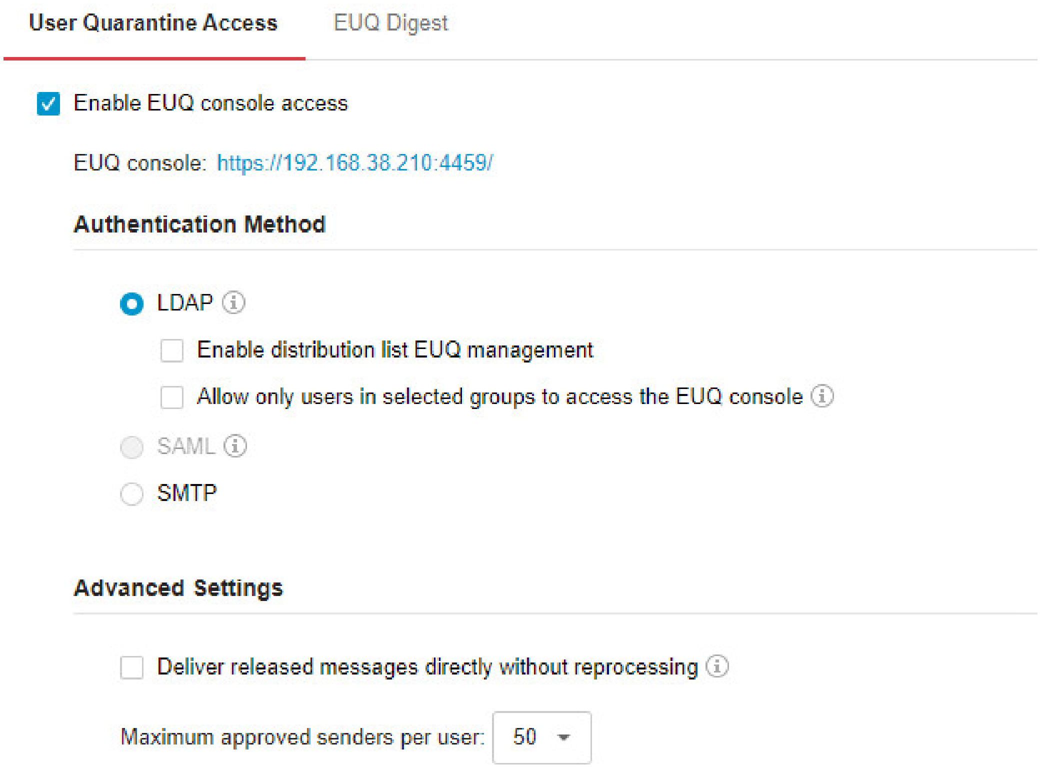
Authentication Method

○ LDAP ⓘ
○ SAML ⓘ
● SMTP

□	Domain ↑	Server/Port	Encryption Method
□	cncorelab.com	mail.cncorelab.com:25	StartTLS

Records: 1 - 1 / 1   10 per page   1 / 1

3. Configure other settings as shown in the following screenshot. After saving the configuration the EUQ console will then contain the URL



☑ Enable EUQ console access

EUQ console: https://192.168.38.210:4459/

Authentication Method

● LDAP ⓘ

□ Enable distribution list EUQ management

□ Allow only users in selected groups to access the EUQ console ⓘ

○ SAML ⓘ

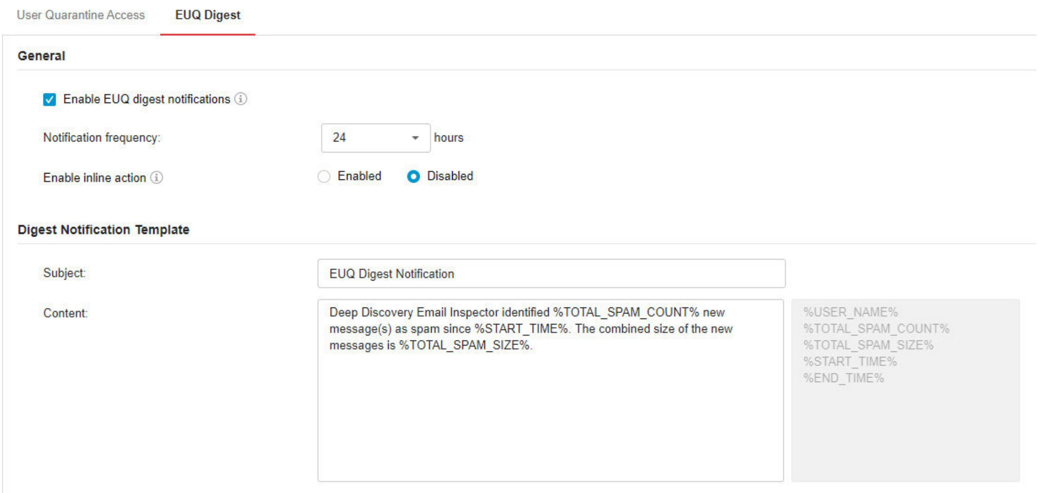
○ SMTP

Advanced Settings

□ Deliver released messages directly without reprocessing ⓘ

Maximum approved senders per user: 50

4. Go to **Administration** > **End-User Quarantine** > **EUQ digest** and configure the EUQ digest



General

☑ Enable EUQ digest notifications ⓘ

Notification frequency: 24 hours

Enable inline action ⓘ ○ Enabled ● Disabled

Digest Notification Template

Subject: EUQ Digest Notification

Content: Deep Discovery Email Inspector identified %TOTAL_SPAM_COUNT% new message(s) as spam since %START_TIME%. The combined size of the new messages is %TOTAL_SPAM_SIZE%.

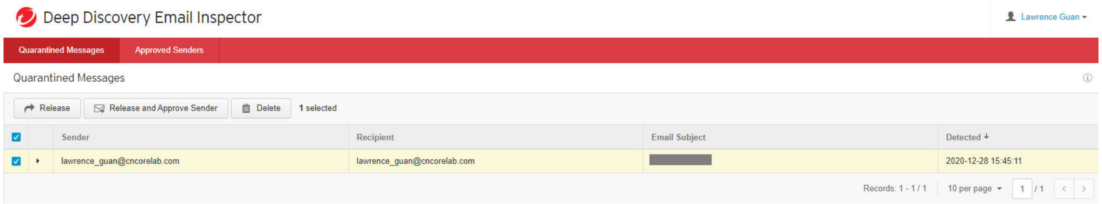
%USER_NAME%
%TOTAL_SPAM_COUNT%
%TOTAL_SPAM_SIZE%
%START_TIME%
%END_TIME%

7.1. Use EUQ

After access the EUQ console, obtain the EUQ console address on **Administration** > **End-User Quarantine** > **User Quarantine Access**. The EUQ console address would be *https://<DDEI_IP>:4459*

After logging in to the EUQ console, the end user can:

- Release quarantined emails
- Release the quarantine emails and add the senders to the Approved Senders list
- Delete the quarantined emails
- Manage the Approved Senders list



Quarantined Messages

1 selected

☑		Sender	Recipient	Email Subject	Detected ↓
☑	▸	lawrence_guan@cncorelab.com	lawrence_guan@cncorelab.com	[redacted]	2020-12-28 15:45:11

Records: 1 - 1 / 1   10 per page   1 / 1

Lesson 8: Connected Threat Defense

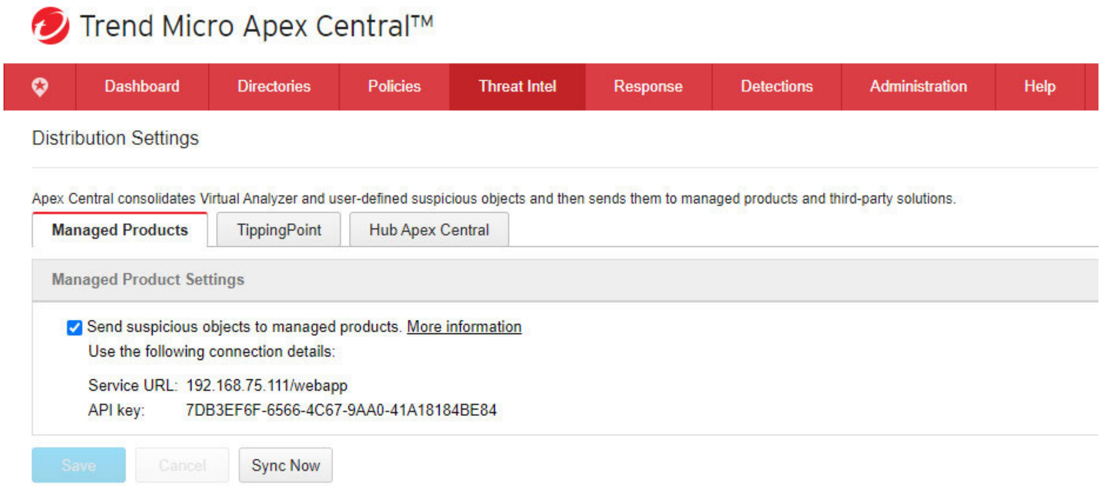
DDEI 5.1 supports Connected Threat Defense (CTD) solution. Configure DDEI to subscribe to the Suspicious Objects (SO) lists from the Apex Central server. Using the Apex Central console create customized actions for objects detected by the suspicious object lists to provide custom defense against threats in Trend Micro products.

8.1. Register to Apex Central

8.1.1. Register DDEI to Central

Do the following to register DDEI to Apex Central and allow DDEI to sync SOs from Apex Central:

1. Login to the Apex Central Web console
2. Go to **Administration** > **Threat Intel** > **Distribution Settings** and get the API key



Distribution Settings

Apex Central consolidates Virtual Analyzer and user-defined suspicious objects and then sends them to managed products and third-party solutions.

Managed Product Settings

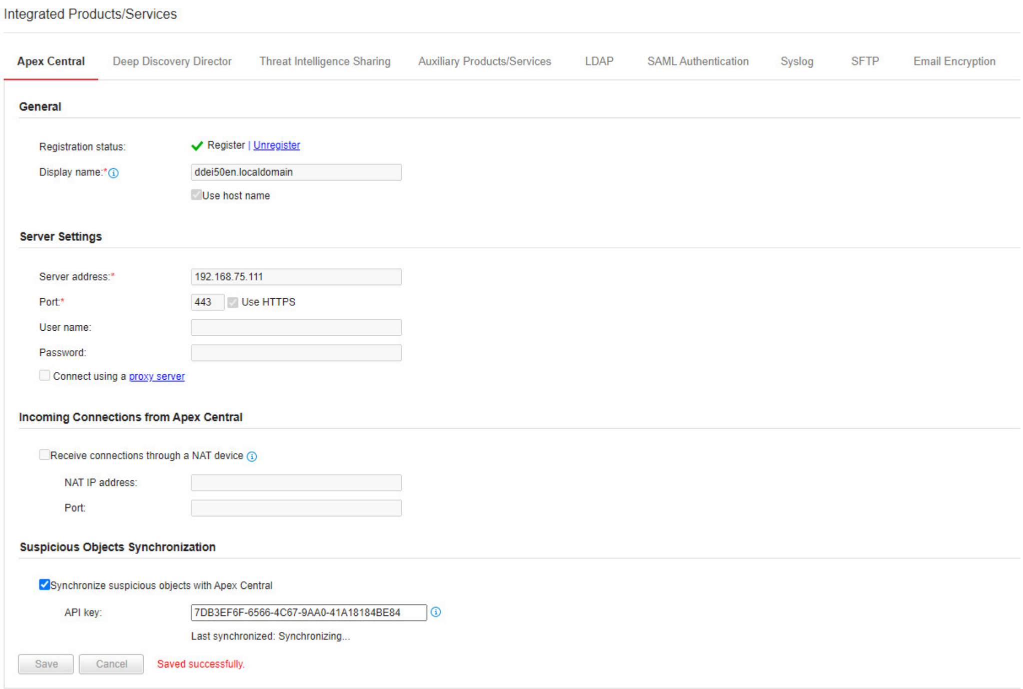
☑ Send suspicious objects to managed products. More information

Use the following connection details:

Service URL: 192.168.75.111/webapp

API key: 7DB3EF6F-6566-4C67-9AA0-41A18184BE84

3. Login to the DDEI Web console
4. Go to **Administration** > **Integrated Products/Services** > **Apex Central** and provide the Apex Central server information. For the **Suspicious Objects Synchronization** section, enable **Synchronize suspicious objects with Apex Central** and provide the Apex Central API key mentioned in step 2



Integrated Products/Services

General

Registration status: ✓ Register | Unregister

Display name:* ddei50en.localdomain

☑ Use host name

Server Settings

Server address:* 192.168.75.111

Port:* 443 ☑ Use HTTPS

User name:

Password:

□ Connect using a proxy server

Incoming Connections from Apex Central

□ Receive connections through a NAT device

NAT IP address:

Port:

Suspicious Objects Synchronization

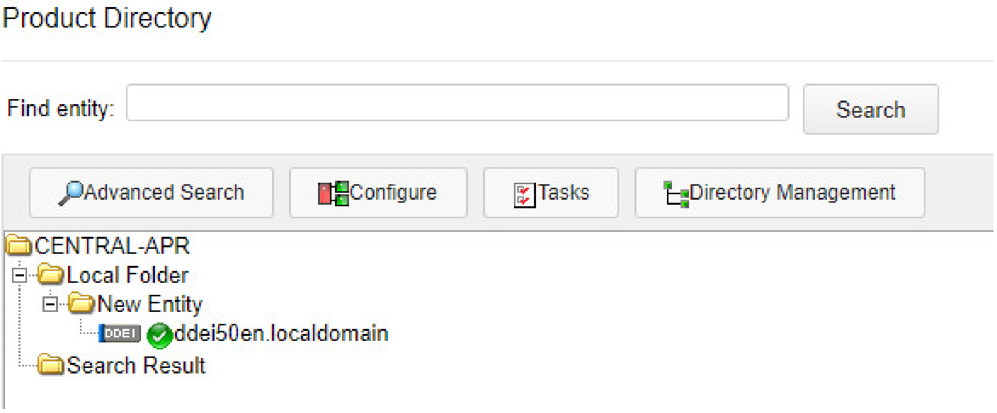
☑ Synchronize suspicious objects with Apex Central

API key: 7DB3EF6F-6566-4C67-9AA0-41A18184BE84

Last synchronized: Synchronizing...

Saved successfully.

5. Save the settings. It may take several minutes for DDEI to register to Apex Central
6. Switch to the Apex Central web console, go to **Directories** > **Products** and verify that DDEI has been successfully registered to Apex Central



Product Directory

8.1.2. Register DDAN to Apex Central

If there is DDAN implemented in the environment, register DDAN to Apex Central so that DDAN can contribute the SO to Apex Central.

1. On the Apex Central web console, go to **Administration** > **Managed Servers**
2. For the Sever Type, select Deep Discovery Analyzer
3. If DDAN server is not on the list, click the **Add** icon to add the dedicated DDAN server

8.1. Synchronize Suspicious Objects

Below are some scenarios for contributing and synchronizing SOs to Apex Central

- DDEI contribute SO to Apex Central - When using the internal virtual analyzer, DDEI contributes the SO to Apex Central and syncs the SO from Apex Central at the same time.
- DDAN contribute SO to Apex Central - With DDAN implemented, DDAN contributes the SO to Apex Central
- Sync SO from Apex Central - After registering to Apex Central, DDEI syncs the SO from Apex Central.
- Sync SO from DDAN - When using the external virtual analyzer (DDAN), DDEI can sync the SO from DDAN. In this situation, DDEI can sync SO from both Apex Central and DDAN

To check the synchronized objects on DDEI web console, go to **Detections** > **Suspicious Objects** > **Synchronized Suspicious Objects**

DDEI synchronizes all types of SOs but only use File type/File Sha-1 type and URL type objects to detect suspicious messages

8.1. Suspicious Objects Detections

8.1.1. Suspicious Object Types

There are two categories of suspicious objects:

- Virtual Analyzer Suspicious Objects
- User-Defined Suspicious Objects

Each category contains several types of Suspicious Objects:

- Files(SHA-1)
- IP Addresses
- URLs
- Domains

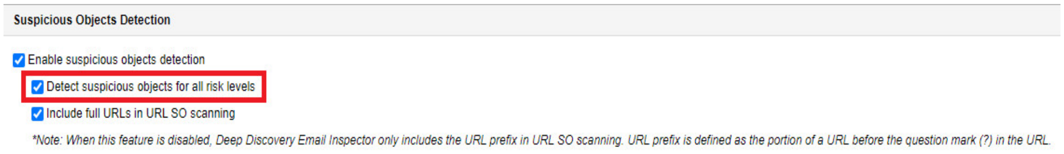
DDEI supports SO File/File SHA-1 type and URLs type with the following detection names:

- Virtual Analyzer Suspicious Objects detection names:
  - *CSO_SUSPICIOUS_FILE.UMXX*
  - *CSO_SUSPICIOUS_URL.UMXX*
- User-Defined Suspicious Objects detection names:
  - *USR_SUSPICIOUS_URL.UMXX*
  - *USR_SUSPICIOUS_FILE.UMXX*

8.1.2. Enable Suspicious Objects Detection

By default, DDEI enables SOs detection only for those with high risk level. Set DDEI to detect SOs for all risk levels.

1. Open the DDEI RDQA hidden page ***https://ddei_ip/hidden/rdqa.php***
2. Go to the ***Suspicious Objects Detection*** page and select **Detect suspicious objects for all risk levels**



Suspicious Objects Detection

☑ Enable suspicious objects detection

☑ Detect suspicious objects for all risk levels

☑ Include full URLs in URL SO scanning

Note: When this feature is disabled, Deep Discovery Email Inspector only includes the URL prefix in URL SO scanning. URL prefix is defined as the portion of a URL before the question mark (?) in the URL.

8.1.3. Action Mapping

The DDEI threat protection module can use SOs to detect suspicious messages.In Apex Central, each SO contains the Risk Level info and Scan Action info. DDEI does not use SOs Actions defined in Apex Central. It takes the action based on its own threat protection rule setting. The threat protection rule defines the actions for different Risk Levels.

In other words, DDEI takes action based on the SOs Risk Level info.

8.1.4. Detection Priority

SOs detection has a lower priority level than virus pattern/WRS detection, but has a higher priority level than Virtual Analyzer checking. If a message is detected as a suspicious object, this message will not be sent to Virtual Analyzer for future analysis.

FILES TYPE OF SUSPICIOUS OBJECTS

Virus Pattern detection > Predictive Machine Learning detection > User defined Suspicious Objects detection > Virtual Analyzer Suspicious Objects detection > YARA Rules detection > TLSH / Macroware detection > Virtual Analyzer detection

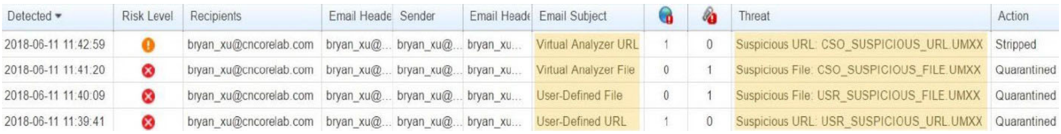
URLS TYPE OF SUSPICIOUS OBJECTS

WRS detection > User defined Suspicious Objects detection > Virtual Analyzer Suspicious Objects detection > Virtual Analyzer detection.

8.1. Verify Suspicious Object Detection

To check if the SOs are synchronized successfully in DDEI:

1. Login to DDEI Web console
2. Go to Detections > Suspicious Objects > Synchronized Suspicious Objects and check if the Suspicious Objects are synchronized successfully
3. Go to Detections > Detected Messages, query the detections logs with the Threat name that contains the suspicious keyword. The following is an example:



Detected ▾	Risk Level	Recipients	Email Heade	Sender	Email Heade	Email Subject	🌐	📎	Threat	Action
2018-06-11 11:42:59	!	bryan_xu@cncorelab.com	bryan_xu@...	bryan_xu@...	bryan_xu...	Virtual Analyzer URL	1	0	Suspicious URL: CSO_SUSPICIOUS_URL.UMXX	Stripped
2018-06-11 11:41:20	⊗	bryan_xu@cncorelab.com	bryan_xu@...	bryan_xu@...	bryan_xu...	Virtual Analyzer File	0	1	Suspicious File: CSO_SUSPICIOUS_FILE.UMXX	Quarantined
2018-06-11 11:40:09	⊗	bryan_xu@cncorelab.com	bryan_xu@...	bryan_xu@...	bryan_xu...	User-Defined File	0	1	Suspicious File: USR_SUSPICIOUS_FILE.UMXX	Quarantined
2018-06-11 11:39:41	⊗	bryan_xu@cncorelab.com	bryan_xu@...	bryan_xu@...	bryan_xu...	User-Defined URL	1	0	Suspicious URL: USR_SUSPICIOUS_URL.UMXX	Quarantined

If there is no SO detection logs, test using the user-defined objects.

1. Temporarily add one user-defined URL object and one user-defined file object on the Apex Central web console: **Administration** > **Threat Intel** > **Custom Intelligence**.
2. On the DDEI web console, the newly added user-defined objects are synchronized to DDEI successfully.
3. Send two test mails to DDEI. One mail contains the user-defined URL object and the other mail contains the user-defined file object.
4. Check the DDEI detection log. The URL test mail should be detected as *USR_SUSPICIOUS_URL.UMXX*, and the file test mail should be detected as *USR_SUSPICIOUS_FILE.UMXX*.

Lesson 9: Verification

The purpose of verification is to make sure that all configurations and functions work as expected. The administrator can double check to make sure that DDEI is working properly.

- On the DDEI Web console, check each Dashboard tab especially the following:
  - Overview tab - The Message Queues widget is very useful
  - Threat Monitoring tab - Contains the threat detection information
  - Top Trends - View Top Trends widgets to understand the top activity in the network, including suspicious message content and callback destinations, to understand the threat characteristics affecting your network
  - System Status tab - Contains the hardware status widget
  - Virtual Analyzer tab - On the Messages Submitted to Virtual Analyzer widget, the administrator will know Virtual Analyzer's working status. A number of emails queued in the Virtual Analyzer may indicate a problem
- Send test emails to make sure that DDEI can process the emails successfully
- Check all kinds of logs to make sure that the logging is working
- Check and verify that the Component Updates module is up to date
- Check the notification setting and Alerts/Reports setting
- Check the Policies and Rules to make sure the correct policies and rules are configured
- If Apex Central is integrated, check on the Apex Central side if DDEI can co-work with Apex Central smoothly
- If CTD is enabled, check the suspicious objects part and detection logs
- Check the Virtual Analyzer settings and make sure that the dedicated files are submitted to Virtual Analyzer successfully and that Virtual Analyzer can also analyze the files
- Check the back-end service status
  - Go to **Administration** > **System Maintenance** > **Network Services Diagnostics** page and test the back-end services.

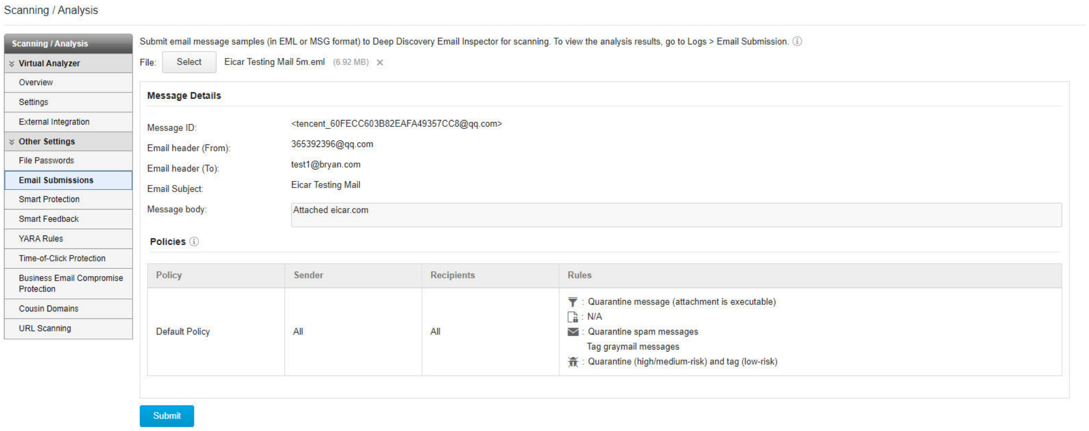
EMAIL SUBMISSIONS

Sample emails (In EML or MSG format) can be submitted directly to DDEI for analysis. However, DDEI does not perform the following actions for manually submitted samples:

- Send message copies to archive servers or detection notifications as specified in matched policies
- Analyze content based on Email Reputation Service (ERS) or sender filtering/authentication settings
- Generate message tracking logs
- Quarantine and generate log entries for End-User Quarantine (EUQ)
- Send email submission logs to syslog servers, Apex Central, or Deep Discovery Director
- If a threat detection occurs on submitted message samples, DDEI sends the detection logs to syslog servers, Apex Central, or Deep Discovery Director

- Deliver messages when DDEI is configured in MTA mode

Once the file upload process is complete, view the message summary information (Such as email header, recipients, and policy match).



Submit email message samples (in EML or MSG format) to Deep Discovery Email Inspector for scanning. To view the analysis results, go to Logs > Email Submission.

File: Eicar Testing Mail 5m.eml (6.92 MB)

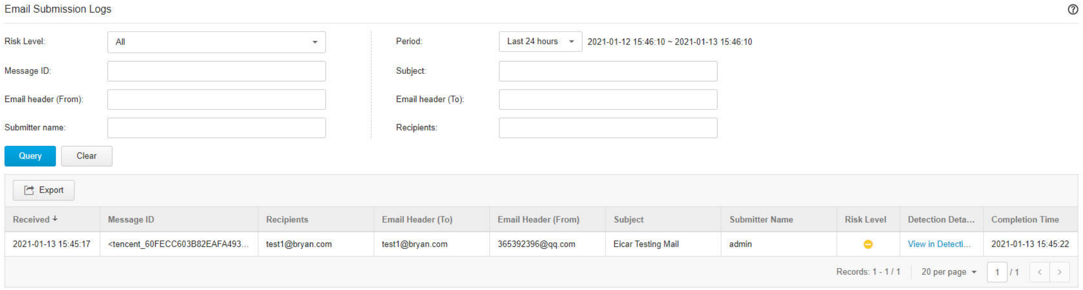
Message Details

Message ID:	<tencent_60FECC603B82EAFA49357CC8@qq.com>
Email header (From):	365392396@qq.com
Email header (To):	test1@bryan.com
Email Subject:	Eicar Testing Mail
Message body:	Attached eicar.com

Policies

Policy	Sender	Recipients	Rules
Default Policy	All	All	: Quarantine message (attachment is executable) : N/A : Quarantine spam messages Tag graymail messages : Quarantine (high/medium-risk) and tag (low-risk)

After submitting to Virtual Analyzer and the analysis processing is complete, do an email submission log query to view the submission results.



Risk Level:	All	Period:	Last 24 hours 2021-01-12 15:46:10 ~ 2021-01-13 15:46:10
Message ID:		Subject:	
Email header (From):		Email header (To):	
Submitter name:		Recipients:	

Received ↓	Message ID	Recipients	Email Header (To)	Email Header (From)	Subject	Submitter Name	Risk Level	Detection Deta...	Completion Time
2021-01-13 15:45:17	<tencent_60FECC603B82EAFA493...	test1@bryan.com	test1@bryan.com	365392396@qq.com	Eicar Testing Mail	admin	●	View in Detecti...	2021-01-13 15:45:22

Records: 1 - 1 / 1 20 per page 1 / 1

Lesson 10: Backup and Disaster Recovery

10.1. Backup and Restore from GUI

Export settings from the management console to back up the DDEI configuration. If a system failure occurs, restore the settings by importing the configuration file back up. To do a backup or restore:

1. Login to the DDEI Web console
2. Go to Administration > System Maintenance > Back Up / Restore
3. Either export or restore the configuration in this page

NOTE:

DDEI 5.1 only supports restoring configuration settings from other DDEI servers with a compatible license status and same firmware version, hardware model, and locale. For example, DDEI 5.1 cannot restore the configuration settings exported from DDEI 3.6.

Configuration backup and restore is limited depending on the AC type as can be seen in the following table:

License Activation	Advanced Threat Protection + Gateway Module	Gateway Module Only	Advanced Threat Protection Only
Advanced Threat Protection + Gateway module	Compatible	Compatible	Compatible
Gateway module only	Not compatible	Compatible	Not compatible
Advanced Threat Protection only	Not compatible	Not compatible	Compatible

TABLE 10.1.1.1: Backup and Restore Compatibility Across DDEI License Types

10.1. Reset to Factory Settings

A factory reset may be necessary to fix critical or difficult non-hardware related issues. However, keep in mind that the factory reset wipes out all customized settings and user data and reverts DDEI to the original version and configuration. For example, if DDEI 5.1 is upgraded from DDEI 3.6, the factory reset will revert the DDEI box to version 3.6. Below are the steps on how to do factory reset:

1. Open the hidden page ***https://DDEI_IP/hidden/rdqa.php***
2. Go to the **Factory Reset** page.
3. Click the **Reset** button to proceed with the factory reset
4. Reconfigure DDEI after the factory reset

Lesson 11: Troubleshooting

11.1. SSH Access

In DDEI 2.6 and 3.0, root access to DDEI requires a Public Key and password via SSH. However, anyone that has the SSH key would be able to access DDEI through SSH if they have the root password as the key is always valid for DDEI.

Beginning with DDEI 3.1, user logon as root via SSH now uses token and password. This method has the following advantages:

- Token has validation period
- Access is controlled
- Token has one-to-one correspondence with activation code

NOTE: Token requirement is only applicable for root access. Access to the "admin" account still uses the username/password method. XShell cannot be used due to its 80 characters support limit. Instead, use PuTTY version 0.63 or higher.

To request for a token, contact the Trend Micro Technical Support Team.

11.1. Component Update Issue

Most of the time, components update issue is due to network issue where DDEI cannot connect to Trend Micro active update server to get the latest components. Go to the **Administration** > **Component Updates** page to check if all components are up-to-date. Use the following steps if there are any issues:

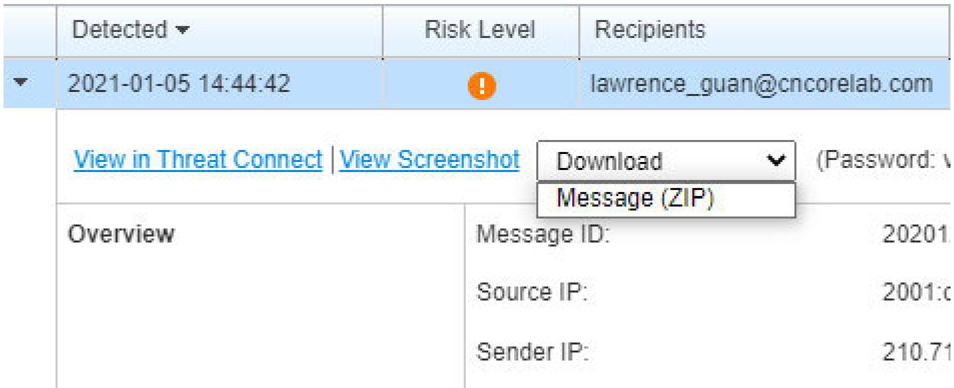
1. Go to **Administration** > **Component Updates** > **Schedule** and make sure that scheduled update is enabled. It is recommended to check for an update every 15 minutes.
2. Go to the **Administration** > **Component Updates** > **Source** page and make sure that DDEI is set to get updates from the Trend Micro ActiveUpdate server.
3. Go to the **Administration** > **System Settings** > **Network** page and make sure that *eth0* has the correct gateway and DNS settings.
4. If DDEI has no direct access to the Internet, go to **Administration** > **System Settings** > **Proxy** and make sure that DDEI has the correct Proxy settings.
5. If all of those settings are correct but you still cannot get an update, export the debug logs then contact Trend Micro Technical Support.

   Go to **Administration** > **System Maintenance** > **Debug Logs** set the log level to *Error* and export the debug log.

11.1. Threat Related False Positive Detection

For any false positive detections, collect the following information and file a case with Trend Micro Technical Support.

1. In the DDEI web console, go to the **Administration** > **Component Updates** page and make sure all components are updated to the latest version.
2. Go to **Detections** > **Detected Messages**.
3. Find the false positive message detection logs then click the left triangle icon to check the detailed detection log.
4. Download the detected message sample on the detailed detection log page then take a screenshot of this page.



	Detected ▾	Risk Level	Recipients
▾	2021-01-05 14:44:42	!	lawrence_guan@cncorelab.com

View in Threat Connect | View Screenshot | Download | (Password: v

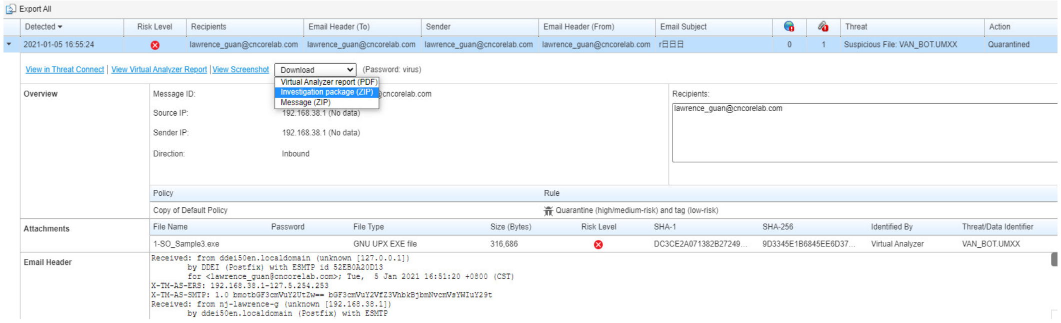
Overview

Message ID: 20201

Source IP: 2001:c

Sender IP: 210.71

5. If the detection is from a Virtual Analyzer, download the Virtual Analyzer report (PDF) and Investigation package (ZIP) on the detailed detection log page, then take a screenshot of the page.



Export All

	Detected ▾	Risk Level	Recipients	Email Header (To)	Sender	Email Header (From)	Email Subject	🌐	📎	Threat	Action
▾	2021-01-05 16:55:24	⊗	lawrence_guan@cncorelab.com	lawrence_guan@cncorelab.com	lawrence_guan@cncorelab.com	lawrence_guan@cncorelab.com	r日日日	0	1	Suspicious File: VAN_BOT.UMXX	Quarantined

View in Threat Connect | View Virtual Analyzer Report | View Screenshot | Download | (Password: virus)

Overview

Message ID: cncorelab.com

Source IP: 192.168.38.1 (No data)

Sender IP: 192.168.38.1 (No data)

Direction: Inbound

Recipients: lawrence_guan@cncorelab.com

Policy	Rule
Copy of Default Policy	Quarantine (high/medium-risk) and tag (low-risk)

Attachments

File Name	Password	File Type	Size (Bytes)	Risk Level	SHA-1	SHA-256	Identified By	Threat/Data Identifier
1-SO_Sample3.exe		GNU UPX EXE file	316,686	⊗	DC3CE2A071382B27249...	9D3345E1B6845EE6D37...	Virtual Analyzer	VAN_BOT.UMXX

Email Header

```
Received: from ddei50en.localdomain (unknown [127.0.0.1])
        by DDEI (Postfix) with ESMTP id 52EB0A20D13
        for <lawrence_guan@cncorelab.com>; Tue,  5 Jan 2021 16:51:20 +0800 (CST)
X-TM-AS-ERS: 192.168.38.1-127.5.254.253
X-TM-AS-SMTP: 1.0 bmotbGF3cmVuY2UtZw== bGF3cmVuY2VfZ3VhbkBjbmNvcmVsYWIuY29t
Received: from nj-lawrence-g (unknown [192.168.38.1])
        by ddei50en.localdomain (Postfix) with ESMTP
```

6. Take a screenshot of the following pages:

- The detailed detection log page
- **Administration** > **Component Updates** page
- **Administration** > **Scanning/Analysis** page

7. Go to **Administration** > **System Maintenance** > **Backup / Restore** and export the configuration file
8. Contact Trend Micro Technical Support and provide all the collected information

As a temporary solution, add the false positive detected files to the exception list while the Trend Micro Technical Support team is investigating it.

1. Get the false positive detected file's SHA1 value.

2. Add the SHA1 value to the **Policies** > **Exceptions** > **Objects exceptions** list.

11.1. False Negative Detection

For any false negative detections where DDEI could not detect the suspicious message, the suspicious message might have already been sent to the end users' mailbox.

For this scenario, collect the following information and file a case with Trend Micro Technical Support.

1. On the DDEI web console, go to the **Administration** > **Component Updates** page and make sure all components are updated to the latest version
2. Go to the **Logs** > **Message Tracking** page and check the detailed message tracking log for the false negative message. If the risk level is *Unrated* and the detailed log shows a timeout for Sandbox analyzing, this means the suspicious file was not analyzed by Virtual Analyzer successfully because of a timeout issue.

   Skip the following steps and refer to Q2: How do you reduce the number of bypassed (time out) messages? in Chapter 13: FAQ of this document.

3. Get the sample suspicious message from the end user then compress the file in a ZIP file format with the password: "*virus*"..
4. Take screenshots of the following pages:

- **Logs** > **Message Tracking** - the detailed message tracking log of the false negative message
- **Dashboard** > **Virtual Analyzer** > **Messages Submitted to Virtual Analyzer** widget
- **Administration** > **Component Updates** page
- **Administration** > **Scanning / Analysis** > **Overview** > **Status** page
- **Administration** > **Scanning / Analysis** > **Overview** > **Images** page
- **Administration** > **Scanning / Analysis** > **Settings** page
- *RDQA hidden page* > **Detect Mode** page.

5. Export the debug logs:

   Go to **Administration** > **System Maintenance** > **Debug Logs** set the log level to *Error* and export the debug log.

6. Export the email statistics:

   Go to *RDQA hidden page* > **Email Statistics Export** and export the email statistics

7. Contact Trend Micro Technical Support and provide all the collected information.

As a temporary solution, add the false negative detected files to User-Defined Suspicious Objects list while the Trend Micro Technical Support team is investigating it.

1. Get the false negation detected file's SHA1 value.

2. If the CTD solution is implemented, as an administrator, open the TMCM web console and go to **Administration** > **Suspicious Objects** > **User-Defined Suspicious Objects** then add this false negative file's SHA1 value into the list.

11.1. Messages Queued/Delayed Issue

Issues with emails queuing in DDEI can occur in Postfix or Virtual Analyzer queue.

11.1.1. Messages Queued/Delayed in Postfix

1. Go to **Dashboard** > **Overview** and check the ***Message Queues*** widget. If there are lots of queued messages here, it indicates that the messages are queued in Postfix.
2. Go to **Logs** > **Message Tracking** and check the message tracking logs to get information about the queued emails.
3. Go to the **Administration** > **Mail Settings** > **Message Delivery** page. Make sure the settings are correct and the destination MTA is accessible from DDEI.
4. Go to **Logs** > **MTA** and query the MTA logs with the keyword "`status=deferred`". This could give some clues that will help the info and reason on the messages queued issue.
5. If the issue still persists, see "Collect Information" on page 96 then contact Trend Micro Technical Support.

11.1.2. Messages Queued for Sandbox Analysis

1. Go to **Dashboard** > **Virtual Analyzer** > **Message Submitted to Virtual Analyzer**. Suppose lots of messages are queued in Virtual Analyzer for Sandbox analysis (Such that there are 10 instances for each Sandbox image, while there are more than 30 samples queued for Sandbox analysis.). In that case, the current Sandbox environment's performance might not be enough to analyze all samples.
2. Go to **Logs** > **Message Tracking**. Query the logs with Unrated as ***Risk level***. If the detailed logs show a timeout for Sandbox analyzing, that means the Sandbox resource is not enough to analyze all samples. Refer to Q2: How do you reduce the number of bypassed (time out) messages? in Chapter 13: FAQ of this document.
3. Make sure that DDEI has the latest patches
4. If this does not help and the same issue occurs for new incoming messages, see "Collect Information" on page 96, then contact Trend Micro Technical Support.

11.1.3. Collect Information

If the message queued issue still occurs for the new incoming messages, collect the following, then contact Trend Micro Technical Support:

1. Screenshot of:

- **Logs** > **Message Tracking** - the detailed message tracking log of the problem message
- **Dashboard** > **Overview** > **Message Queues** widget

- **Dashboard** > **Virtual Analyzer** > **Messages Submitted to Virtual Analyzer** widget
- **Administration** > **Scanning / Analysis** > **Overview** > **Status** page
- **Administration** > **Scanning / Analysis** > **Overview** > **Images** page
- **Administration** > **Scanning / Analysis** > **Settings** page
- *RDQA hidden page* > **Detect Mode** page
- *RDQA hidden page* > **URL Extraction Setting** page
- *RDQA hidden page* > **URL Filter Setting** page

2. Export the debug logs:

   Go to **Administration** > **System Maintenance** > **Debug Logs**, set the log level to *Error*, and export the debug log.

3. Contact Trend Micro Technical Support and provide all the collected information.

11.1.4. Span Related False Positive/Negative Issue

For any spam related false positive or negative issues, collect the sample and then contact Trend Micro Technical Support.

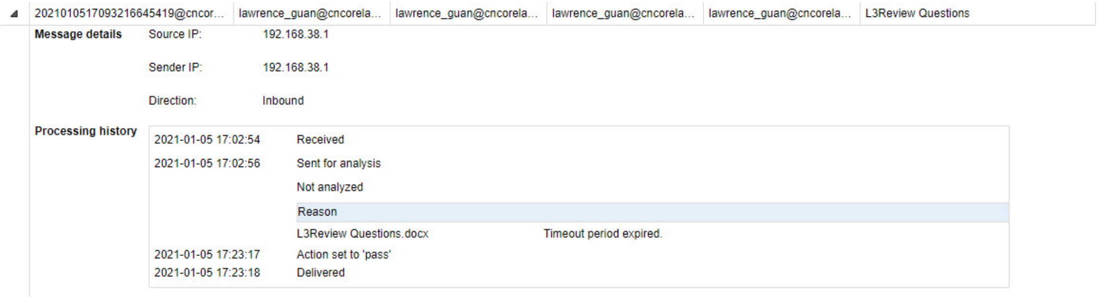
Lesson 12: FAQ

12.1.1. How to check how many emails were bypassed (Timed out) in DDEI?

1. Go to the *DDEI hidden page https://<DDEI_IP/hidden/rdqa.php* > **Email Statistics Export**
2. Export the email statistics
3. Check the Bypassed Emails column, these are the emails that are not analyzed by Virtual Analyzer due to timeout. The risk level usually would be Unrated for this situation

12.1.2. How to reduce the number of bypassed (Timed out) messages

When a number of messages are queued in Virtual Analyzer (Queued for Sandbox Analysis), timeout may occur. DDEI will bypass the files and deliver it directly without sandbox analysis. The related message tracking log is similar to the following:



```
◢ 20210105170932166454l9@cncor... | lawrence_guan@cncorela... | lawrence_guan@cncorela... | lawrence_guan@cncorela... | lawrence_guan@cncorela... | L3Review Questions
  Message details   Source IP:     192.168.38.1

                    Sender IP:     192.168.38.1

                    Direction:     Inbound

  Processing history  2021-01-05 17:02:54   Received
                      2021-01-05 17:02:56   Sent for analysis
                                            Not analyzed
                                            Reason
                                            L3Review Questions.docx          Timeout period expired.
                      2021-01-05 17:23:17   Action set to 'pass'
                      2021-01-05 17:23:18   Delivered
```

This might cause a false negative detection. Refer to the following steps to reduce the number of bypassed messages. This could also reduce the number of queued messages for Sandbox Analysis.

1. Increase the instance number to a proper value. see "Performance" on page 9.
2. Reduce the file types which will be submitted to Virtual Analyzer (**Administration** > **Scanning / Analysis** > **Settings**).
3. Extend the Submission Timeout Setting on the same page (This will extend the mails queued time in DDEI in MTA mode.).
4. Reduce the image number (This will reduce the detection rate). Go to **Administration** > **Scanning / Analysis** > **Overview** > Images and delete the not so commonly used images.

12.1.3. How to reduce the queued messages in Virtual Analyzer?

Follow the suggestions in the previous item.

12.1.4. How to temporarily bypass false positive detections?

1. Get the false positive detected file's SHA1 value
2. Add this file's SHA1 value to into **Policies** > **Exceptions** > **Objects Exceptions** list

12.1.5. How to disable Predictive Machine Learning (TrendX)?

WARNING: Disabling TrendX is not recommended. Only do this when isolating issues.

1. Go to the ***DDEI Hidden Page: (https://<DDEI_IP>/hidden/rdqa.php)*** > **Scan Settings**.
2. Uncheck ***Enable Predictive Machine Learning before processing by Virtual Analyzer.***

12.1.6. How to enable URL extraction from attachment?

1. Go to the ***DDEI Hidden Page: (https://<DDEI_IP>/hidden/rdqa.php)*** > **Scan Settings**
2. Select enable ***URL Extraction from Attachment***

12.1.7. How to enable the most aggressive detection mode?

1. Go to the ***DDEI Hidden Page: (https://<DDEI_IP>/hidden/rdqa.php)*** > **Detect mode**
2. WRS mode for scanner uses Standard mode by default. This can be set to Aggressive mode.

- Standard mode – URLs with WRS score 51~80 will be detected as normal URLs.
- Aggressive mode - URLs with WRS score 51~80 will be detected as low risk URLs.

3. ATSE mode for Virtual Analyzer uses ***All*** by default.

12.1.8. How to enable outbound message scanning?

1. To allow the mail server to relay messages to DDEI, add the mail server into the Permitted Senders of Relayed Mail list on **Administration** > **Mail Settings** > **Limits and Exceptions**
2. Send outbound test mails from the mail server to DDEI and make sure the test mails are sent successfully
3. Configure the mail server to relay all outbound mails to DDEI

4. Monitor the outbound mail traffic to make sure it works as expected.

12.1.9. How to replace a TLS certificate with another?

see “Transport Layer Security (TLS)” on page 67.

12.1.10. Why does DDEI only detect high risk suspicious objects?

DDEI enables suspicious objects detection only for high risk level by default. To detect suspicious objects for all risk levels, see “Enable Suspicious Objects Detection” on page 87.