



Email Security Management Platform



Contents

Contents	. 2
Preface	. 3
1.1 Purpose of this document	. 3
1.2 Overview	. 4
1.2.1 SMG Portal	. 5
1.2.2 SMG Reports	. 5
1.3 Contacting Support	. 5
1.4 Terminology	. 6
Using SMG Portal	. 6
2.1 Accessing SMG Portal	. 6
2.2 Block/Safe List	. 7
2.2.1 Add a Block/Safe sender in the domain Block/Safe list	. 7
2.2.2 Add a Block/Safe sender in the Personal Block/Safe list	. 8
2.2.3 How to find a sender in the Block/Safe list	. 9
2.3 Release Quarantined Emails	. 9
2.3.1 How to find a quarantined email in Personal Quarantine	10
2.3.2 How to find a quarantined email in Domain Quarantine	10
2.3.3 Release a quarantined email	11
Using SMG Report Portal	12
3.1 Accessing SMG Report Portal	12
3.2 Log View	13
3.2.1 Log Browse	13
3.3 Reports	13
3.3.1 Predefined Reports	13
3.3.2 All Reports	14
3.3.3 Generating report	14
3.3.4 Generated Reports	15
3.3.5 Templates	15

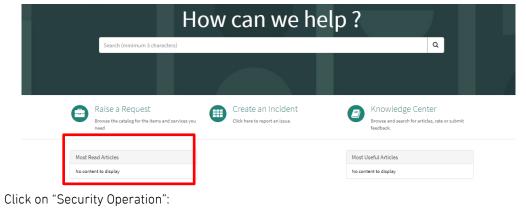
1.1 Purpose of this document

The document guide Deem customers on how to access and manage Deem Email Security Management Platform.

1.2 How to Acquire the Service

To get access to Deem Email Security Management Platform. Please open a ticket through Deem Support Portal as the following:

• Login to the support Portal and click on "Raise a Request":



Categories	Security Operations		
Backup & Restore Email Network & Internet	Add bad sender at email gate Add Bad Sender at Email Gateway	Email Release Request Request to release quatrantine email	Security Assessment This request aims to proceed customer's security testing by getting
Security Operations SharePoint	View Details	View Details	View Details
Support	SMTP Relay Service	Whitelist New External Domain	

• Choose "SMG Portal Access":



• Fill the below form:

Requested For Ali Alahed Contact number 966555875676 ntity/Organizat DEEM uide Plea	ddi (DEEM) er ion see make sure to - Routing for thi - Allow this subr - Add the below <u>SMG</u> .	apply the below points : s subnet 86.60.48.0/24 , het 86.60.48.0/24 with th records to your private D deem.sa 86.60.48.33 eport.deem.sa 86.60.48	e specified port 443 NS server or host file to re	ach SMG and SMC	S Report portal	×	v
Requested For Ali Alahed Contact numbe 966555875676 ntity/Organizat DEEM Jide O Plea	Idi (DEEM) er ion ase make sure to - Routing for thi - Allow this subr - Add the below <u>SMG</u> .	s subnet 86.60.48.0/24 , het 86.60.48.0/24 with th records to your private D <u>deem.sa</u> 86.60.48.33	e specified port 443 NS server or host file to re	ach SMG and SMG	3 Report portal		
Ali Alshed Contact number 966555875676 tity/Organizat DEEM tide Plea	ddi (DEEM) er ion see make sure to - Routing for thi - Allow this subr - Add the below <u>SMG</u> .	s subnet 86.60.48.0/24 , het 86.60.48.0/24 with th records to your private D <u>deem.sa</u> 86.60.48.33	e specified port 443 NS server or host file to re	ach SMG and SMG	3 Report portal		
Contact numbe 966555875676 ntity/Organizat O DEEM uide O Plea	er ion - Routing for thi - Allow this subr - Add the below <u>SMG.4</u>	s subnet 86.60.48.0/24 , het 86.60.48.0/24 with th records to your private D <u>deem.sa</u> 86.60.48.33	e specified port 443 NS server or host file to re	ach SMG and SMC	3 Report portal		
966555875676 ntity/Organizat DEEM uide @ Plea	ion see make sure to - Routing for thi - Allow this subr - Add the below <u>SMG.</u>	s subnet 86.60.48.0/24 , het 86.60.48.0/24 with th records to your private D <u>deem.sa</u> 86.60.48.33	e specified port 443 NS server or host file to re	ach SMG and SMG	3 Report portal	×	
DEEM DEEM uide O Plea	ion ase make sure to - Routing for thi - Allow this subr - Add the below <u>SMG.</u>	s subnet 86.60.48.0/24 , het 86.60.48.0/24 with th records to your private D <u>deem.sa</u> 86.60.48.33	e specified port 443 NS server or host file to re	ach SMG and SMG	3 Report portal	×	
DEEM	ese make sure to - Routing for thi - Allow this subr - Add the below SMG.(s subnet 86.60.48.0/24 , het 86.60.48.0/24 with th records to your private D <u>deem.sa</u> 86.60.48.33	e specified port 443 NS server or host file to re	ach SMG and SMG	3 Report portal	×	
DEEM	ese make sure to - Routing for thi - Allow this subr - Add the below SMG.(s subnet 86.60.48.0/24 , het 86.60.48.0/24 with th records to your private D <u>deem.sa</u> 86.60.48.33	e specified port 443 NS server or host file to re	ach SMG and SMC	3 Report portal	×	
uide 🕜 Plea	- Routing for this - Allow this subr - Add the below <u>SMG.</u>	s subnet 86.60.48.0/24 , het 86.60.48.0/24 with th records to your private D <u>deem.sa</u> 86.60.48.33	e specified port 443 NS server or host file to re	ach SMG and SMG	3 Report portal	×	
Plea	- Routing for this - Allow this subr - Add the below <u>SMG.</u>	s subnet 86.60.48.0/24 , het 86.60.48.0/24 with th records to your private D <u>deem.sa</u> 86.60.48.33	e specified port 443 NS server or host file to re	ach SMG and SMG	3 Report portal		×
	- Routing for this - Allow this subr - Add the below <u>SMG.</u>	s subnet 86.60.48.0/24 , het 86.60.48.0/24 with th records to your private D <u>deem.sa</u> 86.60.48.33	e specified port 443 NS server or host file to re	ach SMG and SMG	3 Report portal		3
	- Allow this subr - Add the below <u>SMG.</u>	net 86.60.48.0/24 with th records to your private D <u>deem.sa</u> 86.60.48.33	NS server or host file to re	ach SMG and SMG	3 Report portal		
	- Add the below <u>SMG.</u>	records to your private D deem.sa 86.60.48.33	NS server or host file to re	ach SMG and SMG	a Report portal		
	SMG.	deem.sa 86.60.48.33		ach SMG and SMG	3 Report portal		
			3.32				
	SMGR	<u>eport.deem.sa</u> 86.60.48	3.32				
Source Public I SMG Users Add	P Addresses (MP Remove All	LS)					
Actions		Admin User Email		Operat	tion		
Actions		Autom Oser Entak		opera	uon		
			No data to display				
otification Ema	ail 🕜						
	-	"Notification of Quarantin	ed Email". Users will send	o this email addres	ss to request email	l release	2
		-					

• Note: the request will take up to 24 hours to be approved and completed.

1.3 Overview

The Email Security Management Platform is an email security solution that protects against a wide range of email-based threats. The solution provides advanced features which assists in preventing, detecting, and responding to email-based threats such as;

- Spam
- Phishing
- Malicious Attachments and URLs
- Zero-day Threats
- Impersonation
- Business Email Compromise (BEC)

This solution is responsible for handling and securing all incoming and outgoing emails with external domains. It does not monitor within-domain emails.

The solution also supports the customization of policies and block/safe list based on the customer needs. Some of these features can be controlled by the customer directly using two portals:

1.3.1 reachability

There are 3 conditions to reach the Email Security Management Platform via MPLS and VDC:

- EaaS Approved and deployed.
- Reachability to the Shared services network.
- Adding the following DNS record to the Host file of the machine or DNS Gateway:

86.60.48.32 SMGReport.deem.sa

86.60.48.33 SMG.deem.sa

1.3.2 Email Security Management Platform Portal

- In the Email Security Management Platform Portal, the customer can manage the following actions:
 - Manage block\safe lists of domains and IP addresses.
 - Release quarantined Email.
 - This portal can be accessed from the following URL: URL: <u>https://SMG.deem.sa/admin</u>
 IP: 86.60.48.32

1.3.3 Email Security Management Platform Reports

- In the Email Security Management Platform Reports portal, the customer can do the following actions:
 - Check mail logs
 - Generate reports
 - This portal can be accessed from the following URL URL: <u>https://SMGReport.deem.sa/admin</u> IP: 86.60.48.33

1.4 Contacting Support

If you face any issue, kindly contact DEEM Technical Support:

DEEM Technical Support Contact Options				
Email	Support@deem.sa			
Phone	8001287777			

1.5 Terminology

Terminology	Description
Email Security	Secure Mail Gateway
Management Platform	
Email Security	Secure Mail Gateway for Report
Management Platform	
Report	
SPF	Sender Policy Framework
DMARC	Domain-based Message Authentication, Reporting and Conformance
IP	Internet Protocol
BEC	Business Email Compromise

2 Using Email Security Management Platform Portal

2.1 Accessing Email Security Management Platform Portal

The portal can be accessed using the following URL: <u>https://SMG.deem.sa/admin</u> It requires two-factor authentication using SMS.

Deem Web Services	
Secure Logon for Deem Username Password Logon	دتـم DEEW د تــم
This product is licensed from Deem. © All rights rese	

After login

C Monitor	Personal Quarantine Domain Quarantine				
Security >	Image: Send quarantine region Image: Send quarantine region <td< th=""><th></th><th>Total: 2</th></td<>		Total: 2		
	Mailbox	Size (KB)	Message Count		
	testuser03@tajawal.gov.sa	0	0		
testuser04@tajawal.gov.sa		0	0		

2.2 Block/Safe List

Block/Safe List lets you quarantine or allow email messages based on <u>email addresses</u>, <u>domain</u> <u>names</u>, or

<u>IP addresses</u>. There are two types of block/safe lists:

- Domain-Block/Safe List: applies to all users of the domain
- Personal-Block/Safe List: Specific to the user level

<u>Note:</u> Entries in the Personal Block/Safe list will take precedence over entries in the Domain Block/Safe List.

2.2.1 Add a Block/Safe sender in the domain Block/Safe list

Go to Security > Block/Safe List > click on Domain tab > click on Block or Safe list icon

C Monitor	> Domain Personal		
Security	> 2 « < 1 / 1 > » Records per page 50	•	Total: 1
	Domain	Block List	Safe List
	tajawal.gov.sa		

Click on New > enter Email address, Domain or IP address > Create > Close.

Block List (tajawal.gov.sa)		Block List (taja	awal.gov.sa)		0		
+ New ☑ Edit ⅲ Delete ② < 1 / 1 > »	Backup Res Records per page	Tuno	129.5.5.6/32 IP/Netmask				Тс
Pattern	Туре	Connent				lit Time	Н
*@domain.com	Email						0
User@domainX.com	Email						0
				Create	Cancel		

Туре	Pattern Description	
Email address	user@domain.com	To block a single address
Email address	*@domain.com	To block the whole domain
IP/Network	X.X.X.X/32	To block an IP address

2.2.2 Add a Block/Safe sender in the Personal Block/Safe list

Go to Security > Block/Safe List > click on Personal tab > find the specific user using the Search field > click on Block or Safe list icon

C Monitor	Domain Personal		
Security >	C « < 1 / 1 > » Records per page 50	 Domain tajawal.gov.sa Search 	Total: 2
	User Name	Block List	Safe List
	testuser03		■^
	testuser04		

Click on New > enter Email addresses, Domain or IP or addresses > Create > Close.

Safe List (tajawal.gov.sa)	Safe List (tajawal.gov.sa)	63	
+ New Edit C « < 1 / 1 > » Records Pattern Type	Time Email -	lit Time	
*@domainA.sa Email	Create	ncel	0

2.2.3 How to find a sender in the Block/Safe list

Go to Security > Block/Safe List > click on Domain or Personal tab > click on Block or Safe list icon > in the Search field > enter the input.

╋ New 🗹 Edit 🛗 🛙	Delete Backup Restore				
2 « < 1 / 1	> > Records per page 50	▼ TypeALL ▼	Search		Total: 2 Limit: 2048
Pattern	Туре	Comment	Creation Time	Last Hit Time	Hit Count
*@domain.com	Email		Sun, Feb 27, 2022 17:45:06 ASST	N/A	0
User@domainX.com	Email		Sun, Feb 27, 2022 17:45:54 ASST	N/A	0

2.2.4 How to Backup and restore Block/Safe list

Go to Security > Block/Safe List > click on Domain or Personal tab > click on Block or Safe list icon > click on Backup or Restore to download or upload a list

+ New	Backup Restore				
Ø ≪ < 1 > >> Records per page 50 ▼ Type ALL ▼ Search				Total: 2 Limit: 2048	
Pattern	Туре	Comment	Creation Time	Last Hit Time	Hit Count
*@domain.com	Emall		Sun, Feb 27, 2022 17:45:06 ASST	N/A	0

2.3 Release Quarantined Emails

Quarantined emails can be found under the Quarantine tab, there are two types of quarantine:

- Personal Quarantine. (Not Used for now)
- Domain Quarantine.

Under domain quarantine there are four folders:

- SPF Folder: For emails with SPF violations.
- DMARC Folder: For emails with DMARC violations.
- Content Folder: For emails containing attachment with non-allowed extensions.
- Virus Folder: For emails contain Virus.
- SPAM Folder: For emails contain SPAM
- Newsletter Folder: Marketing emails.

Note: Adding senders to a Safe List only prevents SPAM and Newsletter from getting quarantined. Emails that fail other conditions will still be quarantined even if they are in the safe list e.g. SPF violation.

2.3.1 How to find a quarantined email in Personal Quarantine

Go to **Monitor** > **Quarantine** > **Personal Quarantine** > in the Search field > enter the email address.

C Monitor	Personal Quarantine Domain Quarantine		
Security >	💿 View 🛍 Delete 🗟 Compact 🗸 Send quarantine re		
	♥ <	✓ Domain tajawal.gov.sa ✓ Search user testuser03	Total: 1
	Mailbox	Size (KB)	Message Count
	testuser03@tajawal.gov.sa	0	0

2.3.2 How to find a quarantined email in Domain Quarantine

Go to Monitor > Quarantine > Domain Quarantine > click on Search

C Monitor	Personal Quarantine Domain Quarantine				
Security >	Image: Search and Search				
	Folder	Size (KB)	Message Count		
	Bulk/current	0	0	^	
	Content/current	0	0		
	Dlp/current	0	0		
	Virus/current	0	0		
	PersonalOut/current	0	0		
	SPAM/current	0	0		
	SPF/current	0	0		
	DMARC/current	0	0		
	Newsletter/current	0	0		

Click on **New** to search emails logs with specified time range, match conditions and keywords > **Search**.

Domain Quarantine Search	0
Description Quarantine	
Time Range	
Start time 2022/02/26 III At hour 09:00 III End time 2022/02/27 IIII At hour 15:00 IIII	
Search Filter Relationship And Or	
View Field Operation Value	
From Contains VMware.com	
Domain tajawal.gov.sa Folder folder	
Available folders (6) All Bulk Content Dlp Virus PersonalOut	
Search Can	cel

2.3.3 Release a quarantined email

Go to Monitor > Quarantine > Domain Quarantine or Personal Quarantine > select the folder

🕓 Monitor	>	Personal Quarantine Domain Quarantine	Personal Quarantine Domain Quarantine				
Security >							
		2 ≪ < 1 / 1 > ≫ Records per page 50	▼ Domain tajawal.gov.sa ▼		Total: 9		
		Folder	Size (KB)	Message Count			
		Bulk/current	0	0	^		
		Content/current	0	0			
		Dlp/current	0	0			
		Virus/current	0	0			
		PersonalOut/current	0	0			
		SPAM/current	0	0			
		SPF/current	0	0			
		DMARC/current	0	0			
		Newsletter/current	0	0			

By selecting the email message > click on **Release**.

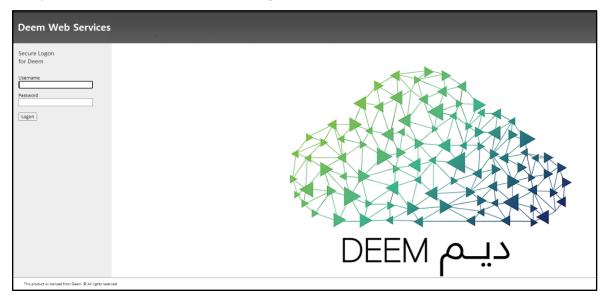
Personal Quarantine Domain Quarantine							
← Back ● View Im Delete Im Release							
C 1 > > Records per page 50 Filter Unreleased Selected: 1 / 3 > > > > > >							
Subject	From	То	Rcpt To	Session ID	Received	Size (KB)	
Test DKIM without whiteli	"Hanan K	"testuser03@tajawal.gov.sa" < testuser	testuser03@tajawal.gov.sa	21G9HZxq030374	Wed, Feb 16, 2022 12:17:	11	*
blacklist 3	"Anas S. F	"testuser03@TAJAWAL.gov.sa" <testu< td=""><td>testuser03@tajawal.gov.sa</td><td>21ED0QeO013418</td><td>Mon, Feb 14, 2022 16:00:2</td><td>11</td><td></td></testu<>	testuser03@tajawal.gov.sa	21ED0QeO013418	Mon, Feb 14, 2022 16:00:2	11	
test blacklist	"Anas S. F	"testuser03@TAJAWAL.gov.sa" <testu< td=""><td>testuser03@tajawal.gov.sa</td><td>21ECU0OK012335</td><td>Mon, Feb 14, 2022 15:30:0</td><td>11</td><td></td></testu<>	testuser03@tajawal.gov.sa	21ECU0OK012335	Mon, Feb 14, 2022 15:30:0	11	

Using SMG Report Portal

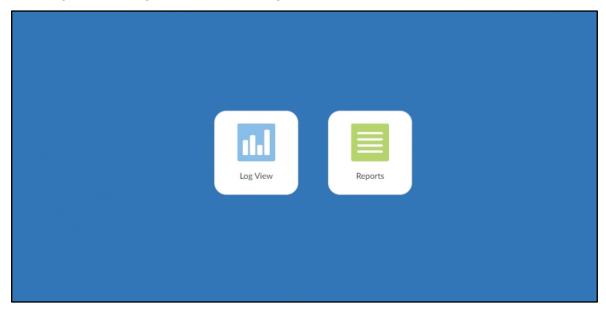
3.1 Accessing SMG Report Portal

The portal can be accessed using the following URL: <u>https://SMGReport.deem.sa/admin</u>

It requires two-factor authentication using SMS.



After Login, Select Log View to view the Logs



3.2 Log View

3.2.1 Log Browse

To view log files:

Go to Log View > Log Browse > Select a log file and click Display to open the log file and display the log messages in formatted view.

To search specific log, Add Filter and provide the search criteria

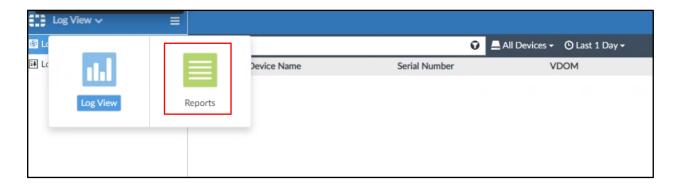
Log View → 🛛 🗮								HA Primary
🕸 Log Browse	Add Filter		G	All Devices 🗸 🕥 Last 1 Day 🗸				
💷 Log Group	. #	Device Name	Serial Number	VDOM	Туре	File Name	From	То
2010					No entry fou	und.		

3.3 Reports

You can generate data reports from logs by using the Reports feature. You can do the following:

- Use predefined reports. Predefined report templates, charts, and macros are available to help you create new reports.
- Create custom reports.

To go to **Reports** > go back to main page and select **Reports**.



3.3.1 Predefined Reports

SMG Report includes a number of predefined elements you can use to create and/or build reports.

Predefined	GUI Location	Purpose
		You can generate reports directly or with
Reports	Reports > Report Definitions	minimum setting configurations.
	> All Reports	Predefined reports are actually report
		templates with basic default setting
		configurations.
	Reports > Report Definitions	You can use directly or build upon. Report
Templates	> Templates	templates include charts and/or macros
		and specify the layout of the report. A
		template populates the Layout tab of a
		report that is to be created.
		You can use directly or build upon a report
Charts	Reports > Report Definitions	template you are creating, or in the Layout
	> Chart Library	tab of a report that you are creating. Charts
		specify what data to extract from logs.
		You can use directly or build upon a report
Macros	Reports > Report Definitions	template that you are creating, or in the
	> Macro Library	Layout tab of a report that you are creating.
		Macros specify what data to extract from
		logs.

3.3.2 All Reports

To find all the reports listed in Reports.

Go to Reports > Report Definitions > All Reports.

Reports 🗸 📃						HA Primary
Generated Reports	⊙ View 🗗 Export					
Report Definitions ~	□ ▲ Title	Language	Cache Status	Time Period	Devices	Schedule
🖹 All Reports	🛛 🔻 📴 FortiMail Reports					
Templates	FortiMail Analysis Report	English		Last 7 Days	All_Device	
🔟 Chart Library 🚯	D E FortiMail Default Report	English		Last 7 Days	All_Device	
Acro Library	Outbreak Alert Reports					
Datasets 0	□ ▼ ¹ SOC Reports					
Advanced ~	🖸 🛛 🖹 FortiMail Analysis Report	English		Last 7 Days	All_Device	
🍽 Language						
E Output Profile						
Report Calendar						

3.3.3 Generating report

- Go to **Reports** > **Report Definitions** > **All Reports**.
- In the content pane, select a report from the list.
- In the toolbar, click **Run Report**.

Reports ∽ ≡				
Generated Reports	Edit: FortiMail Analysis Report			
Report Definitions ~	Generated Reports Settings Editor			
🖹 All Reports	🕑 Run Report 🛗 Delete 🛛 Last 7 Days 🗸	構 ~		Order by Time
🖬 Templates	Report Name	Format	Time Range	Devices
🔟 Chart Library	No record found.			
🖄 Macro Library				
🔁 Datasets 🚯				

3.3.4 Generated Reports

After you generate reports, you can view completed reports in **Reports** > **Generated Reports** or **Reports** > **Report Definitions** > **All Reports**. You can view reports in the following formats: HTML, PDF, XML, and CSV.

To view completed reports in Generated Reports:

- Go to Reports > Generated Reports: This view shows all generated reports for the specified time period.
- To sort the report list <u>by date</u>, click **Order by Time**. To sort the report list <u>by report name</u>, click
 Order by Name.
- Locate the report and click the format in which you want to view the report to open the report in that format. For example, if you want to review the report in HTML format, click the HTML link.

Reports 🗸	=			HA Primary
Generated Reports	🛇 Last 7 Days 🗸			Order by Time Orde
🖺 Report Definitions 🗸	Report Name	Format	Time Range	Devices
All Reports				
🖬 Templates				
🔟 Chart Library 🚯				
Acro Library				
🔁 Datasets 🚯				
🗘 Advanced 🖌				
Anguage				
E Output Profile				
Report Calendar				

3.3.5 Templates

A report template defines the charts and macros that are in the report, as well as the layout of the content. Datasets for charts and macros specify what data are used from the Analytics logs when you generate the report.

SMG report templates:

FortiMail Analysis Report

🜲 FortiMail Default Report

To view Templates, Go to the Reports > Report Definitions > Templates

Reports 🗸 📃			HA Primary ADOM: gwstenanta	& T	tenant 🗸
Generated Reports					Q
Report Definitions	Title	Language	Description	Category	A Preview
All Reports	 Template - FortiMail Analysis 	English	Statistics for Avg and Total mail size, number of mails and connections, delays, ip policies, recipient policies, top access list. Incoming filters for top spammed domains and users, classifiers by hour and disposition, and top subjects.	FortiMail	HTML
🖬 Templates	Report	e. g. j.			PDF
🔟 Chart Library	 Report 	English	Top 10 client IP, senders, virus senders, local users, recipients and virus recipients	FortiMail	HTML PDF
🔯 Macro Library					
🔁 Datasets 🚯					
Advanced ~					
🍽 Language					
E Output Profile					
Report Calendar					

3.3.6 How to Import/Export Report and Charts

Export: After selecting a report(s) in All Reports tap or a chart(s) in Chart Library go to more option on the top and select export to download a back up image of them.

Import: go to the option more and select Import t open a pop up to either drag or brows for the report or chart to be imported.

