Email Security Management Platform

Contents

Preface

1.1 Purpose of this document
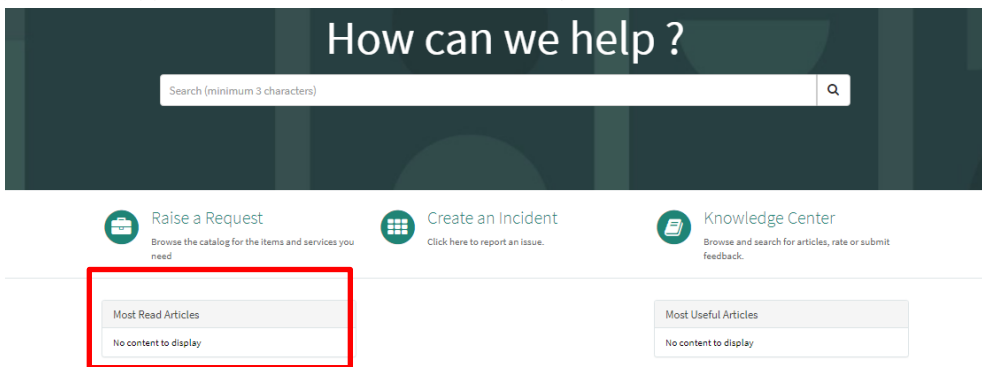
The document guide Deem customers on how to access and manage Deem Email Security Management Platform.
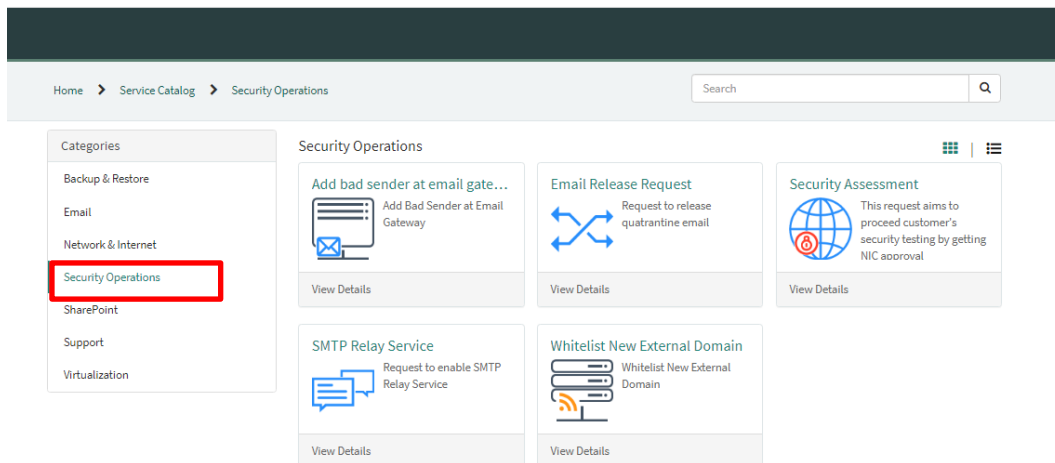
1.2 How to Acquire the Service

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":

- Click on "Security Operation":

- Choose "SMG Portal Access":
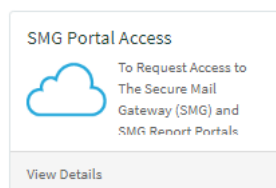
- Fill the below form:

- 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: https://SMG.deem.sa/admin
        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: https://SMGReport.deem.sa/admin
        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 Management Platform	Secure Mail Gateway
Email Security Management Platform Report	Secure Mail Gateway for 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: https://SMG.deem.sa/admin

It requires two-factor authentication using SMS.

After login
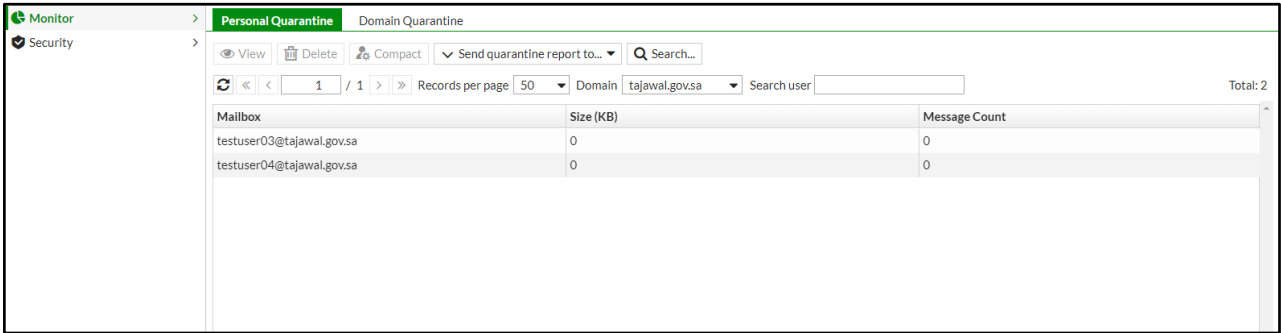
2.2 Block/Safe List

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

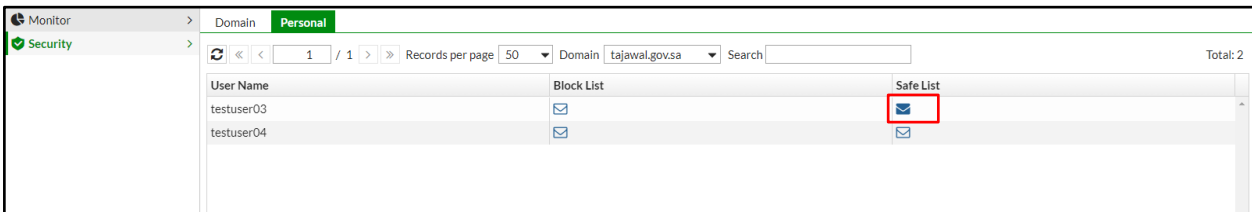Go to **Security** > **Block/Safe List** > click on **Domain** tab > click on **Block or Safe list icon**
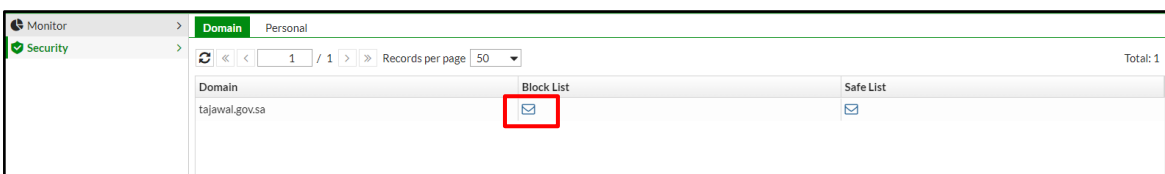
Click on **New** > enter Email address, Domain or IP address > **Create** > **Close**.
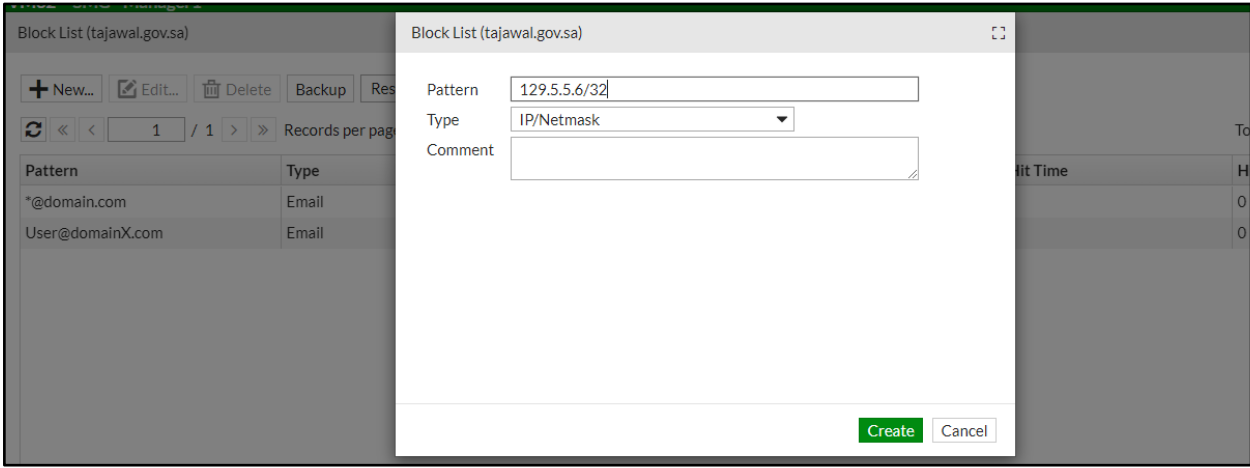
Type	Pattern	Description
Email address	user@domain.com	To block a single address
Email address	*@domain.com	To block the whole domain
IP/Network	X.X.X.X/32	To block an IP address

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**
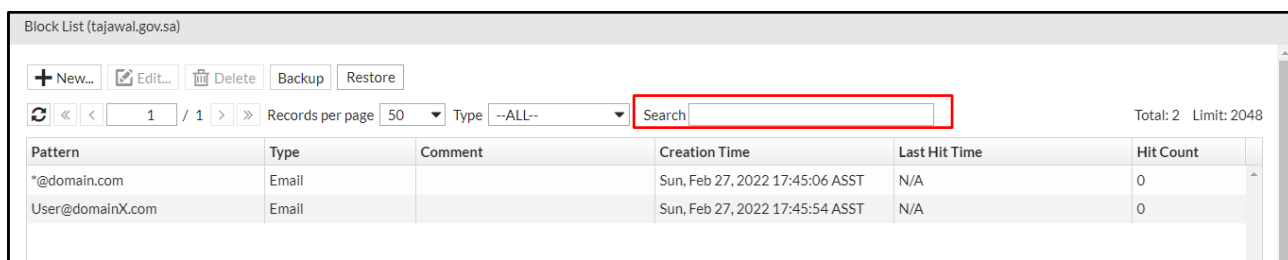

Click on **New** > enter Email addresses, Domain or IP or addresses > **Create** > **Close**.
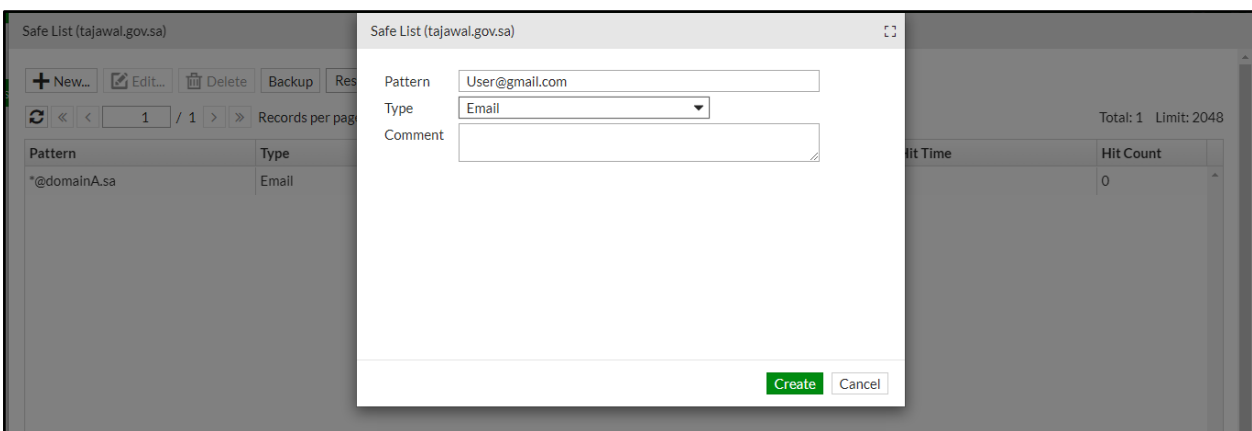
2.2.3 How to find a sender in the Block/Safe list

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.

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
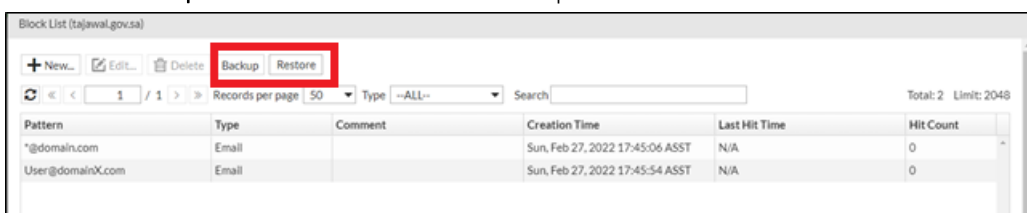
2.3 Release Quarantined Emails

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

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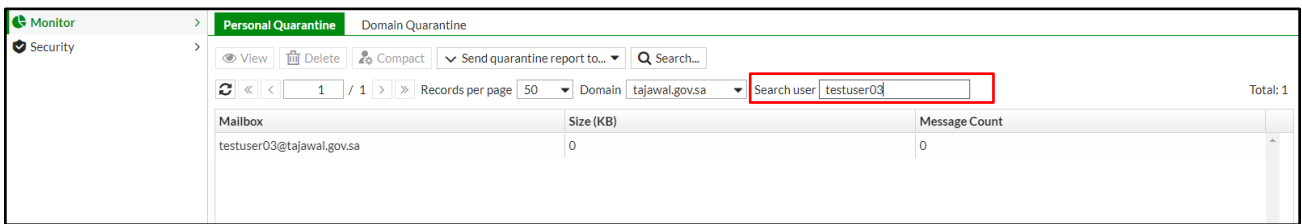- **Domain Quarantine**.

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.
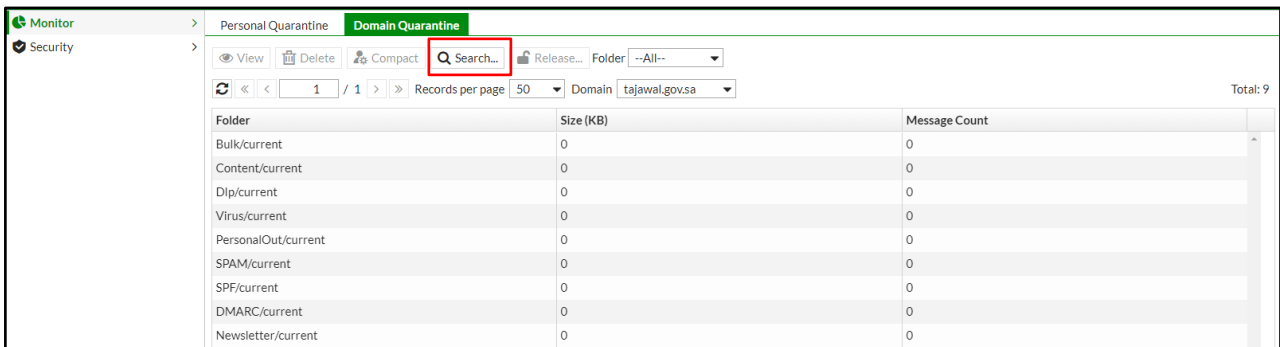
2.3.1 How to find a quarantined email in Personal Quarantine

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

2.3.2 How to find a quarantined email in Domain Quarantine

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

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

2.3.3 Release a quarantined email

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

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

Using SMG Report Portal

3.1 Accessing SMG Report Portal

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

It requires two-factor authentication using SMS.

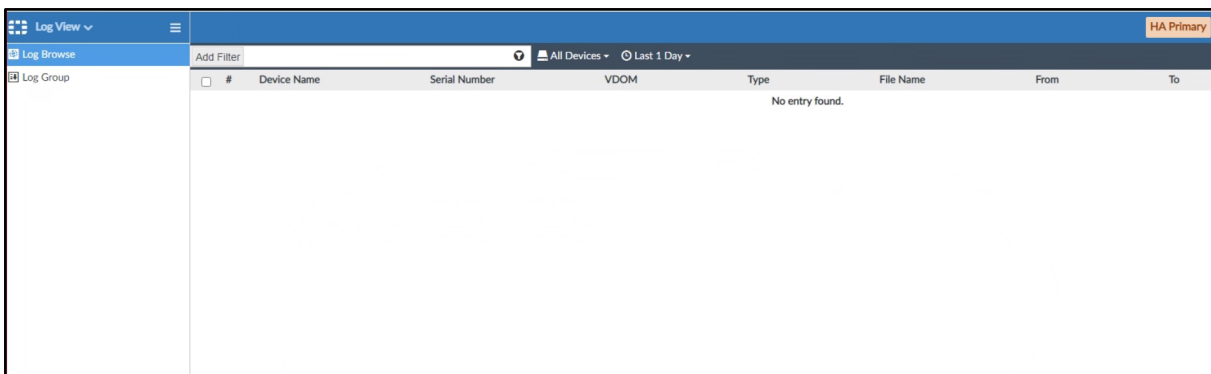After Login, Select Log View to view the Logs
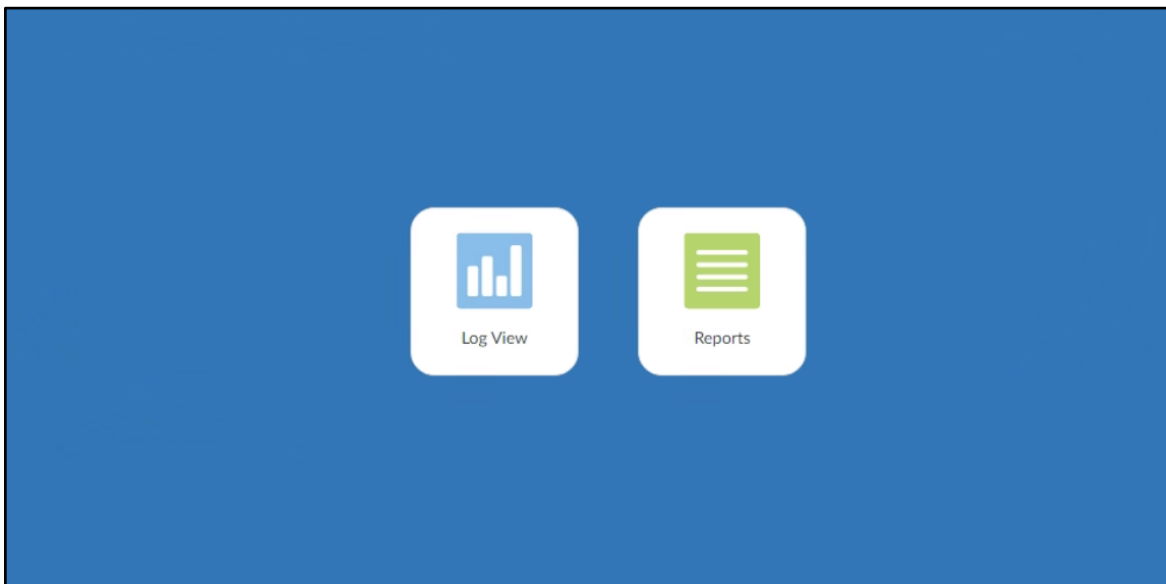
3.2 Log View

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

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
Reports	Reports > Report Definitions > All Reports	You can generate reports directly or with minimum setting configurations. Predefined reports are actually report templates with basic default setting configurations.
Templates	Reports > Report Definitions > Templates	You can use directly or build upon. Report 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.
Charts	Reports > Report Definitions > Chart Library	You can use directly or build upon a report template you are creating, or in the Layout tab of a report that you are creating. Charts specify what data to extract from logs.
Macros	Reports > Report Definitions > Macro Library	You can use directly or build upon a report template that you are creating, or in the 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.**
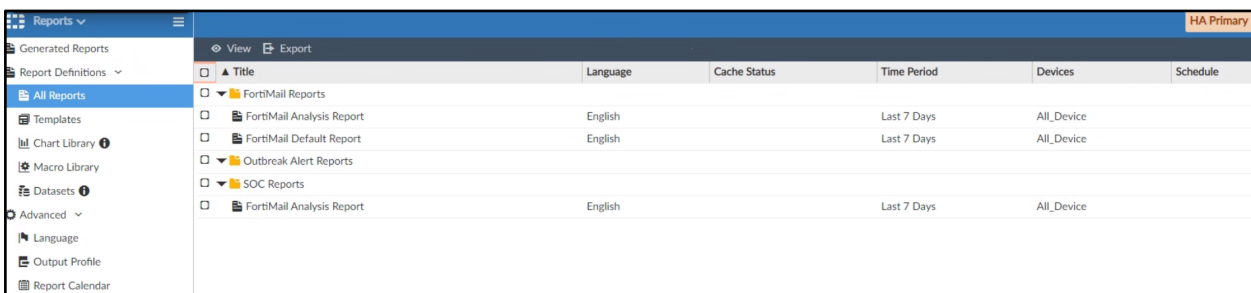
3.3.3 Generating report

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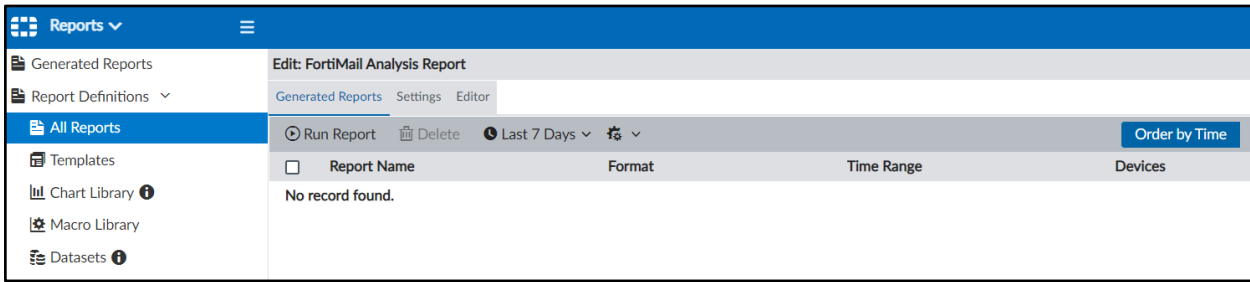
3.3.4 Generated Reports

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.
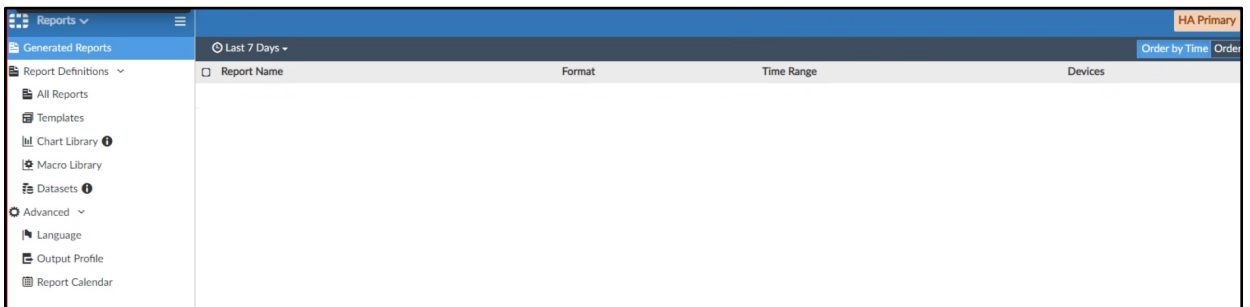

3.3.5 Templates

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**
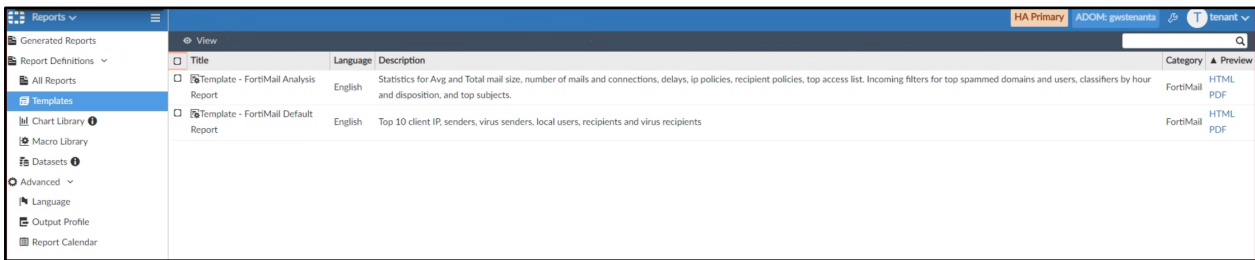
3.3.6 How to Import/Export Report and Charts

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.