

Symantec Email App for QRadar

Version: 1.0.0

Introduction and Deployment Architecture

This chapter includes the following topics:

- [Introduction](#)
- [Deployment Architecture](#)

Introduction

This document is intended to provide overall App Specification for the QRadar App built for Symantec Inc. It contains details of step by step guide to install, setup & configuring Symantec Email Security App for QRadar.

Deployment Architecture

IBM QRadar SIEM is a network security management platform that provides situational awareness and compliance support. It collects, processes, aggregates, and stores network data in real time. IBM Security **QRadar** SIEM (Security Information and Event Management) is a modular **architecture** that provides real-time visibility of your IT infrastructure, which you can use for threat detection and prioritization.

Symantec Email Security App for QRadar utilizes the power of IBM QRadar and provides you a seamless experience for Email Security and phishing by collecting data from Symantec Email Security.Cloud.

Below is the topology of data collection from Symantec Email Security.Cloud to QRadar.

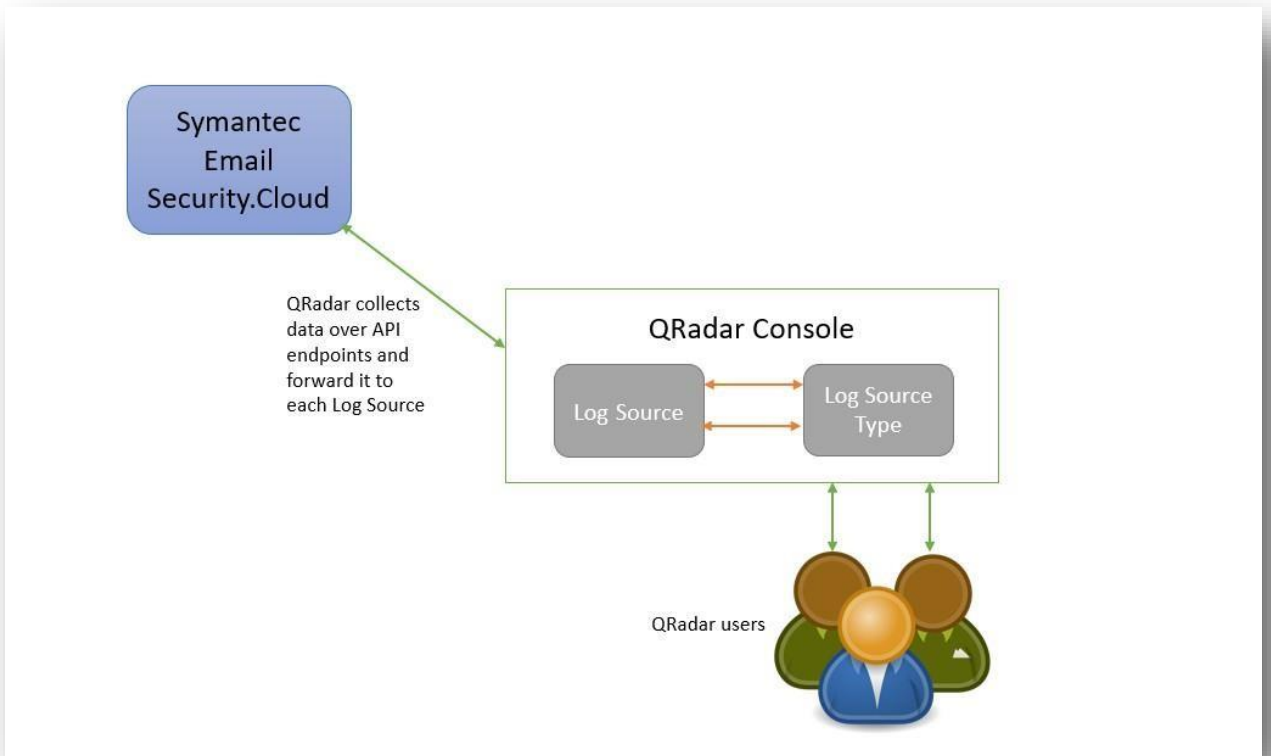


Figure 1: Symantec Email Security.Cloud Integration with IBM QRadar

Symantec Email Security.Cloud is a comprehensive, cloud-based service that safeguards your email while strengthening the built-in security of cloud-based productivity tools such as Office 365 and G Suite. It blocks new and sophisticated email threats such as spear phishing, ransomware, and Business Email Compromise with the highest effectiveness and accuracy through multi-layered detection technologies and insights from the world's largest civilian threat intelligence network.

Note: Email App for QRadar uses an external API call to locate the IP addresses based on Geo Code. App needs to have access to public domain to access this data.

App Architecture

This chapter includes the following topics:

- [App Architecture](#)
 - [Data Collection](#)
 - [Log Sources](#)
 - [Log Source Types](#)
 - [Custom Property Extraction](#)
 - [Event Mappings](#)
 - [Dashboard Queries](#)
 - [Visualizations](#)
 - [Overview Dashboard](#)
 - [Trends Dashboard](#)
 - [Investigation Dashboard](#)
 - [Email Threats](#)

App Architecture

Data Collection

The app use REST API calls to onboard data from Symantec Email Cloud server for core services and Amazon AWS for Email Phishing Data. The application contains python scripts, which makes REST calls to mentioned APIs. These scripts are run on user-defined schedule.

QRadar parses received data using suitable Log source. The log source is made up of two components:

- **APIs**

APIs used for fetching data are:

 1. Symantec Email ATP:

SYNC_API_URL (To check credentials) = <https://api.symanteccloud.com/syncAPI/service.asmx>
RESET_URL (To Reset ATP service) = <https://datafeeds.emailsecurity.symantec.com/all?reset=<<'yyyy-MM-ddTHH:mm:ss'>>>
API URL = <https://datafeeds.emailsecurity.symantec.com/all>
 2. Symantec Email Core:

SYNC_API_URL (To check credentials) = <https://api.symanteccloud.com/syncAPI/service.asmx>
CORE_SERVICE_URL = https://datafeedapi.symanteccloud.com?name=<<CORE_SERVICE_NAME>>&vn=1

3. Symantec Email Phishing:

HOST = s3.amazonaws.com
BUCKET_NAME = customers.securitytraining.io

- **Protocol**

It defines how data gets into QRadar. Symantec Email Security App for QRadar used TCP Syslog protocol for indexing events in QRadar.

Log Sources

Symantec Email App for QRadar creates 3 log sources called “Symantec Email ATP, Symantec Email Core and Symantec Email Phishing” automatically when the app is installed. This log source will identify all events that are coming to QRadar with this log source because all events have log source identifier as follows:

1. Symantec Email ATP: symantecemailatpapp
2. Symantec Email Core: symantecemailcoreapp
3. Symantec Email Phishing: symantecemailapp

Log Source Types

It helps in defining how data is parsed. Log Source Extension and Custom Event Properties can be attached to a Log Source to extend its capability. There are 3 log source types that categorizes the events based on phishing, core and NDF data. Following are the names of the log source type associated with events:

Log Source Type	Event Data Type
Symantec Email Phishing	Phishing Data
Symantec Email Core	Core Services Data
Symantec Email ATP	NDF(ATP) Data

Event Mappings

An event mapping represents an association between an event ID and category combination and a QID record (referred to as event categorization). Event ID and category values are extracted by DSMs from events and are then used to look up the mapped event categorization or QID. These events are mapped to specific High level and low level category.

All events are categorized into High-level and Low-level categories. These categories are pre-defined by QRadar. For all events from Symantec Email Security App, the High-level category is "Application" while the Low-level category is "Mail"

Symantec Email ATP

This log source types includes the event mappings for Symantec Email ATP APIs as mentioned in Data Collection section.

Event Name	Low Level Category	High Level Category
Email ATP(NDF) Events	Mail	Application

Symantec Email Core

This log source types includes the event mappings for Symantec Email Core APIs as mentioned in Data Collection section.

Event Name	Low Level Category	High Level Category
Anti Malware	Mail	Application
Anti Spam	Mail	Application
Data Protection	Mail	Application
Image Control	Mail	Application
Impersonation Control	Mail	Application
Mail Statistics	Mail	Application
Service Summary	Mail	Application

Symantec Email Phishing

This log source types includes the event mappings for Symantec Email Phishing APIs as mentioned in Data Collection section.

Event Name	Low Level Category	High Level Category
Phishing Events	Mail	Application
Phishing Meta	Mail	Application

Visualizations

All the dashboards consist of individual panels which plot specific metric related to the events from Symantec Email Security.Cloud server. The data in all dashboards is populated from 2 log sources: Symantec Email ATP and Symantec Email Core. All the dashboards allow the user to filter events by time.

Overview Dashboard

This dashboard is built to provide overall visibility into Symantec Email deployment. It gives count of Total Email Scanned, Total Inbound Emails, Total Outbound Emails etc. Filters used for this dashboard are Time Range, Domain Name and Account Name.

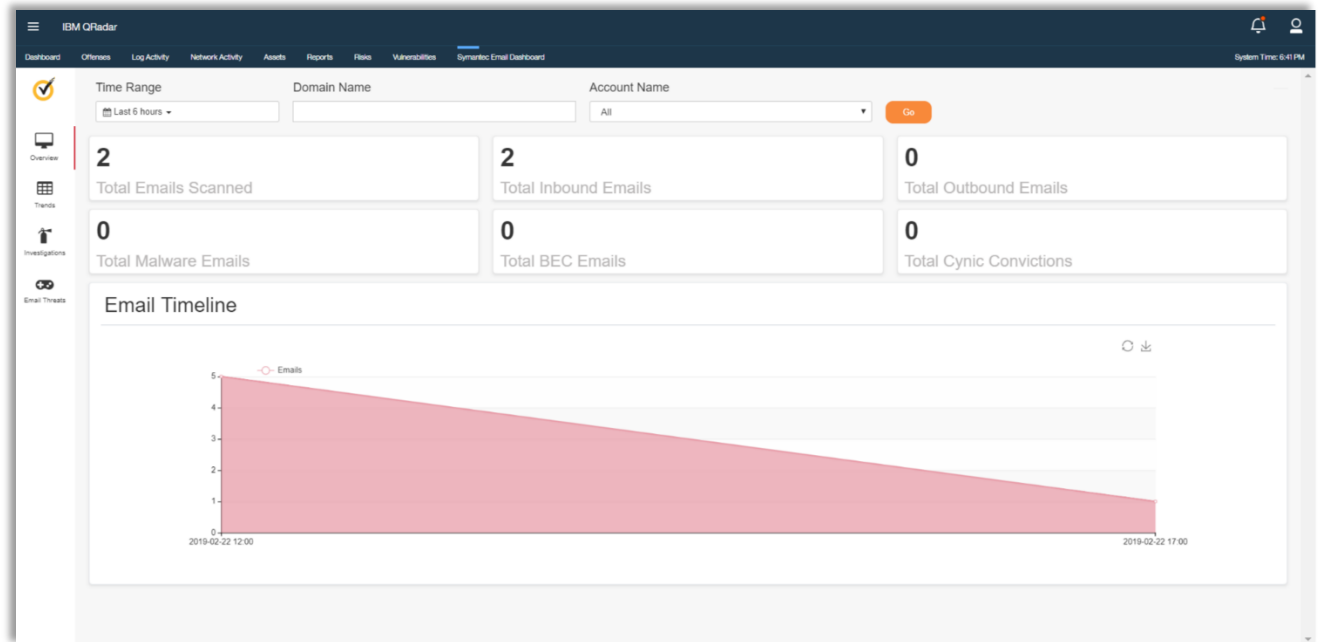


Figure 2: Overview Dashboard

Trends Dashboard

This dashboard is built to provide list of senders, receivers, subjects, etc. which are on the top sorted by unique count (for both Inbound and Outbound). It gives table view of Inbound Email Traffic - Top 10 Recipients, Inbound Email Traffic - Top 10 Senders, Inbound Email Traffic - Top 10 Subject etc. Filters used for this dashboard are Time Range, Service and Account Name.

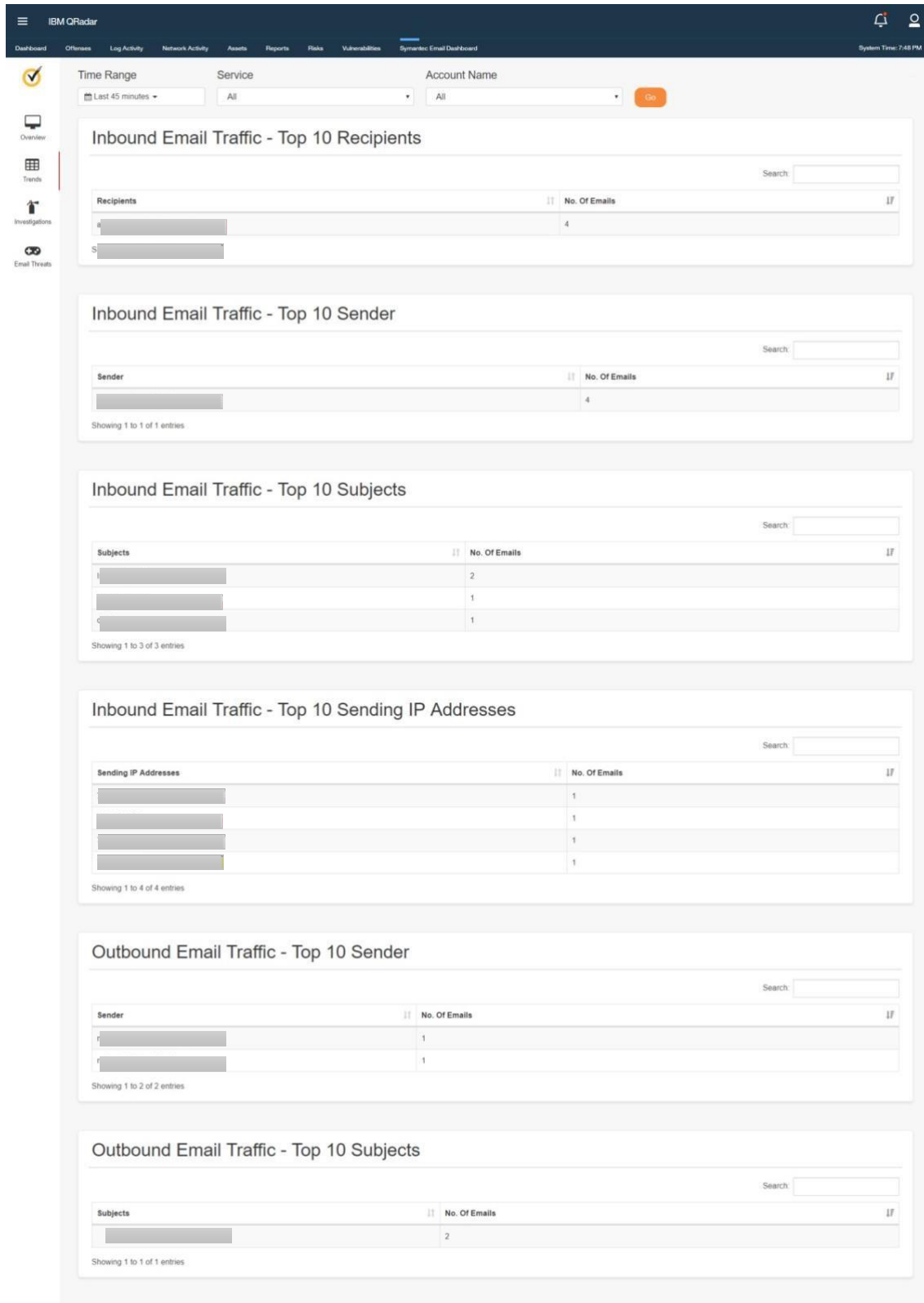
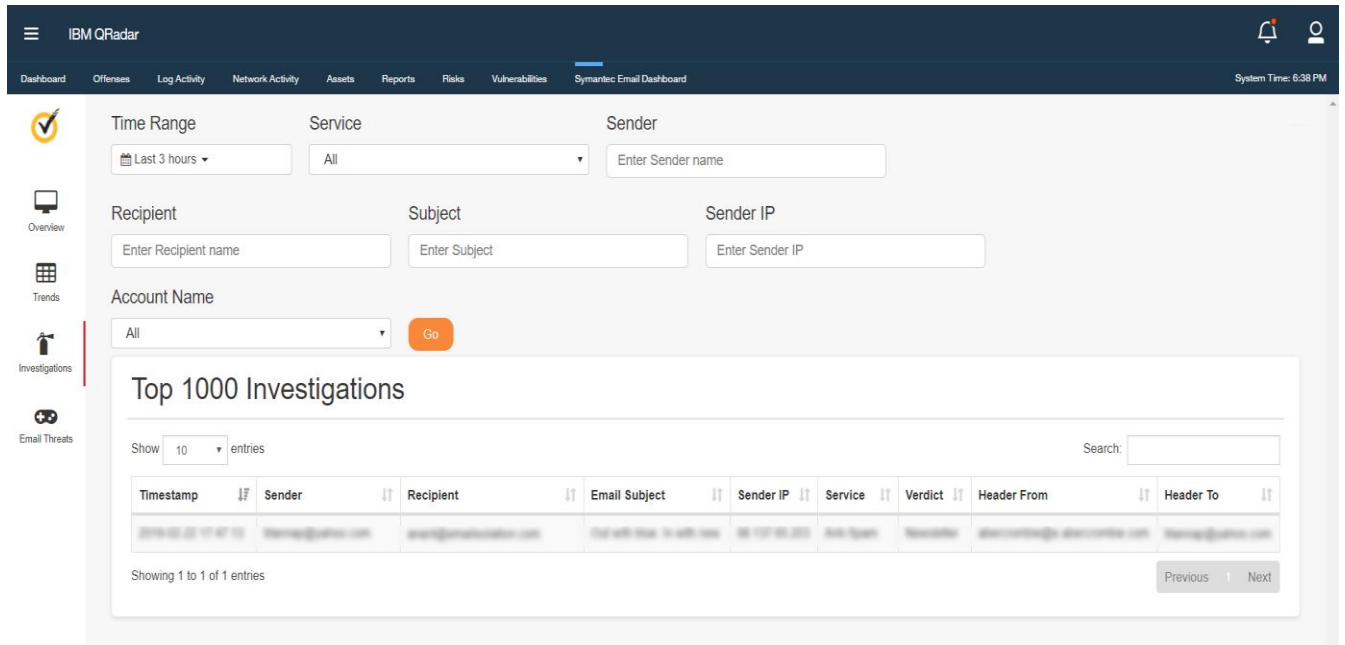


Figure 3: Trends Dashboard

Investigation Dashboard

This dashboard is built to provide list of Top 1000 Investigations sorted on the basis of Time. Filters used for this dashboard are Time Range, Service, Sender, Recipient, Subject, Sender IP and Account Name.



The screenshot displays the IBM QRadar Investigation Dashboard. The interface includes a navigation menu on the left with options like Overview, Trends, Investigations, and Email Threats. The main area features several filter sections: Time Range (Last 3 hours), Service (All), Sender (Enter Sender name), Recipient (Enter Recipient name), Subject (Enter Subject), Sender IP (Enter Sender IP), and Account Name (All). Below the filters is a table titled "Top 1000 Investigations" with a search bar and a "Go" button. The table has columns for Timestamp, Sender, Recipient, Email Subject, Sender IP, Service, Verdict, Header From, and Header To. A single entry is visible in the table.

Timestamp	Sender	Recipient	Email Subject	Sender IP	Service	Verdict	Header From	Header To
2019-02-22 17:47:15	sender@domain.com	recipient@domain.com	Test with data: 123456789	192.168.1.100	Out-Office	Benign	sender@domain.com	recipient@domain.com

Figure 4: Investigation Dashboard

Email Threats

This dashboard is built to provide visibility to Top Spam Detections and Top 10 Countries – Malware. Filters used for this dashboard are Time Range and Account Name.

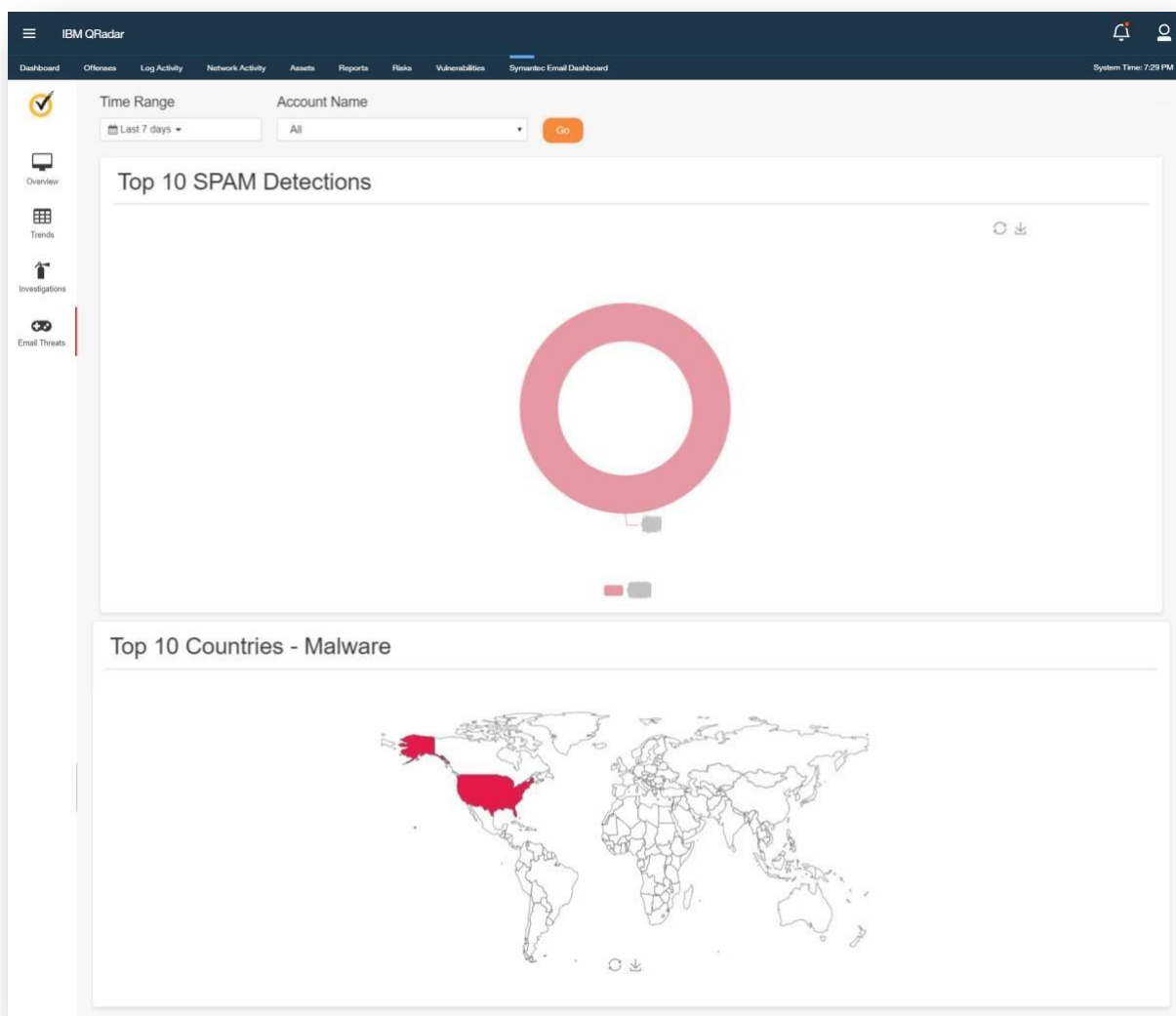


Figure 5: Email Threats Dashboard

App Installation and Configuration

This chapter includes the following topics:

- [App Installation and Configuration](#)
 - [Pre-requisites](#)
 - [Installation](#)
 - [QRadar Configuration](#)
 - [App Configuration](#)
 - [Uninstalling the App](#)
 - [QRadar Cloud Support](#)

App Installation and Configuration

Prerequisites

Below is a list of requirements needed to run Symantec Email app v1.0.0 on QRadar

- Symantec Email App Bundle (v1.0.0)
- QRadar version: 7.2.8 Patch 10 and above
- Access to Symantec Email Endpoint
- Symantec Email Credentials for both AWS as well as Cloud.

Installation

The application installation requires access to QRadar console machine via a web interface. The web interface can be accessed via <https://<<QRadarconsoleIP>>/>. The installation process is as follows:

- a. Login to QRadar console



Figure 6: IBM QRadar 7.3.1 login screen

b. Go to Admin → Extension Management

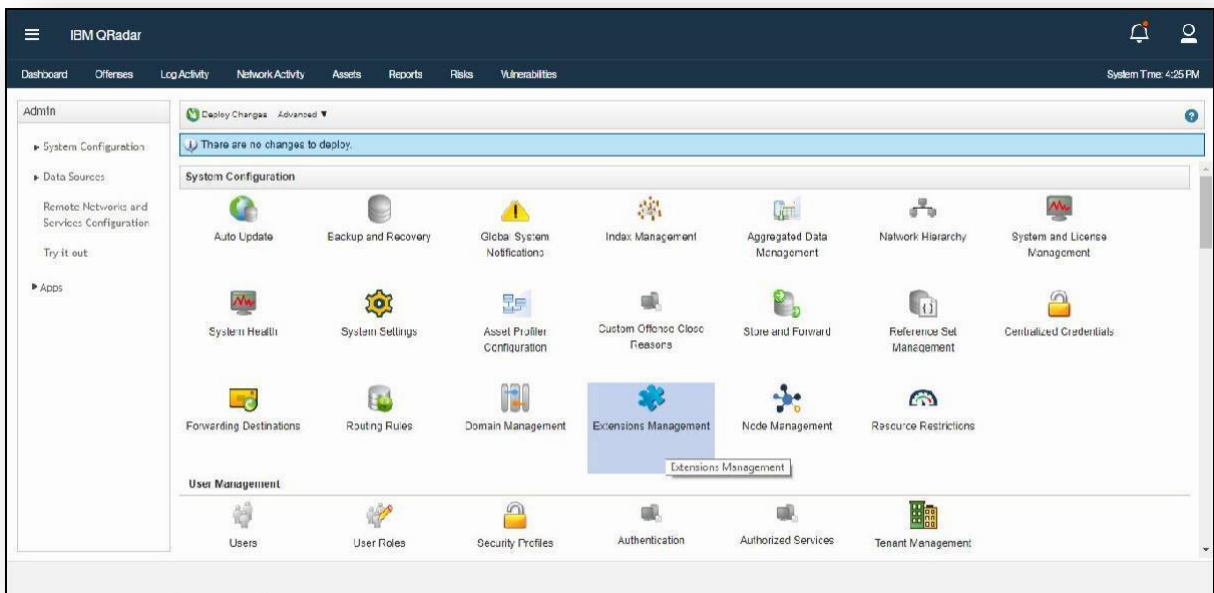


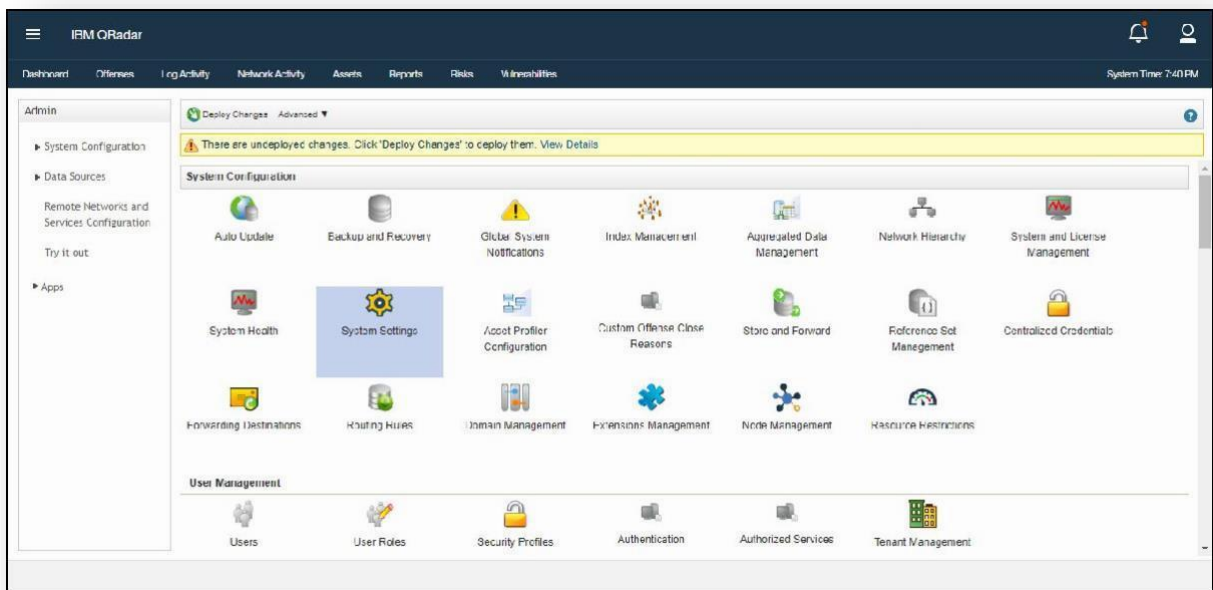
Figure 7: IBM QRadar Admin Panel

- c. Choose the downloaded zip file by clicking on **Add**.
- d. The QRadar will prompt list of changes being made by the app. Click on install button. After the Application is installed it will create a Docker container in the backend.
- e. Deploy changes on Admin Panel and refresh the browser window for configuration page to show up on the Admin Panel.

QRadar Configuration

IBM QRadar has a default setting for payload length. The term "Payload" is defined as the raw event that is being forwarded as TCP/UDP syslog messages to QRadar. So, the default setting is 4096 bytes per event. But in Symantec Email Security there are few events that exceed that limit which results in the truncated payload that hinders custom property extractions for that particular event. Following are few simple steps to increase the payload limit to 12000 bytes:

1. Log in to IBM QRadar
2. Navigate to Admin Panel



3. As shown in figure 3 below, click on System Settings.
Figure 8: QRadar Admin Panel - System Settings

4. Settings window pop out. Now switch to Advanced view to unlock more settings.

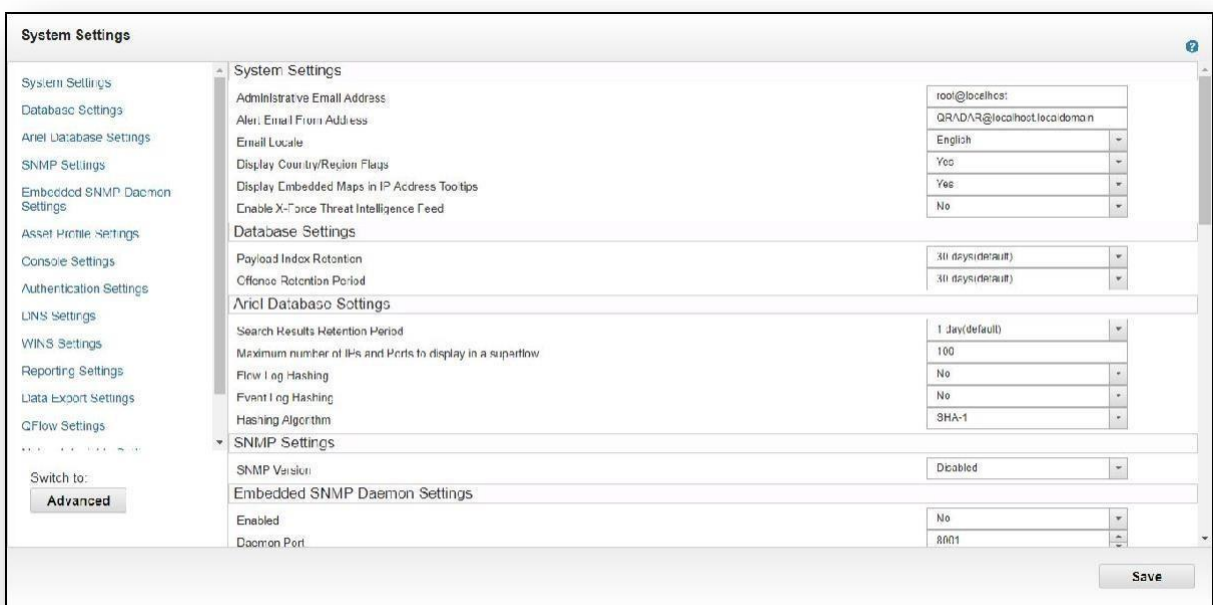
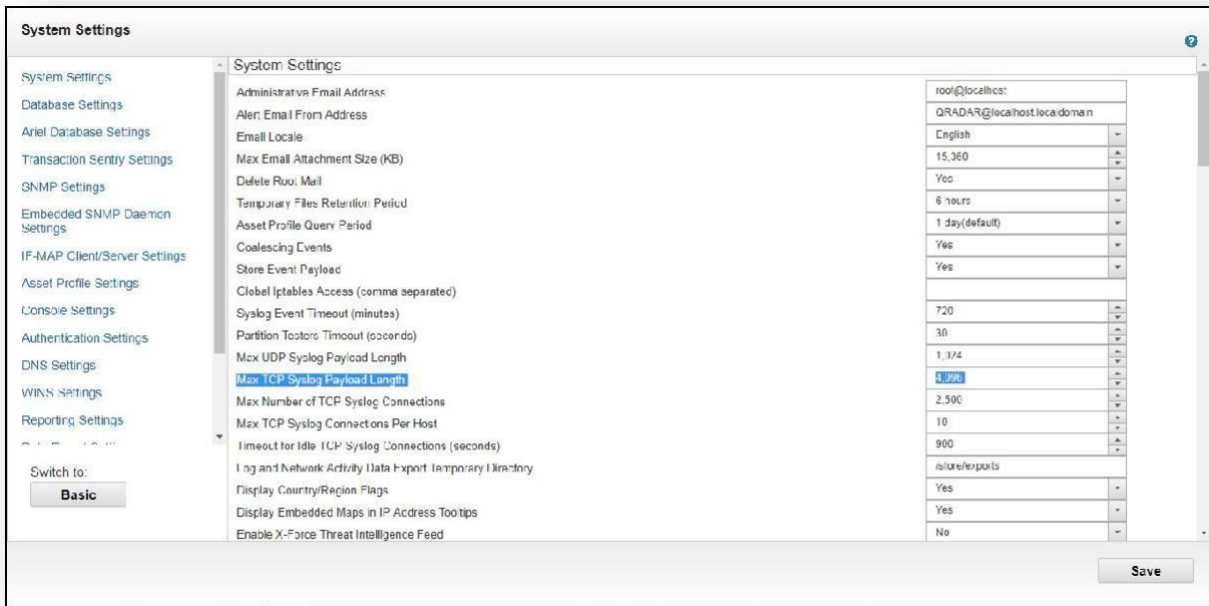


Figure 9: Admin Panel - Basic Settings

- Now find this option Max TCP Syslog Payload Length and update its value to 12000 from



4,096 and then Save.

Figure 10: QRadar Admin Panel - Advanced Settings

- Now near to Deploy Changes button there is an Advanced drop-down. In that first click on **Deploy Full Configuration** and then click on **Restart Event Collection Services**.

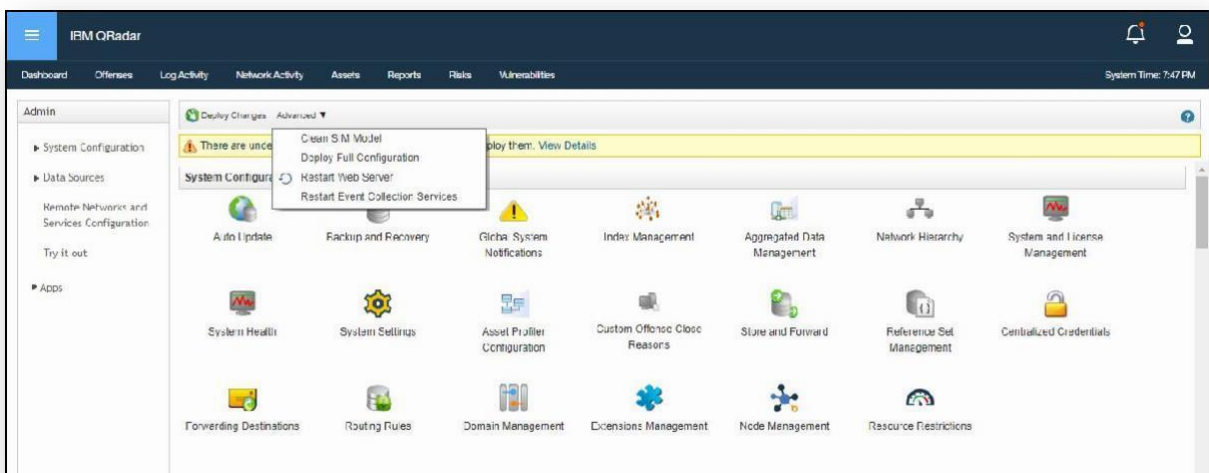


Figure 11: QRadar Admin Panel - Restart Event Collection Services

- After that, the payload length gets updated and now you can configure Symantec Email Security App for data collection.

App Configuration

After completing the installation, you must complete the configuration to start the data collection.

The setup process for configuring is as follows:

- Find the installed app on Admin Panel under Apps as shown in fig.

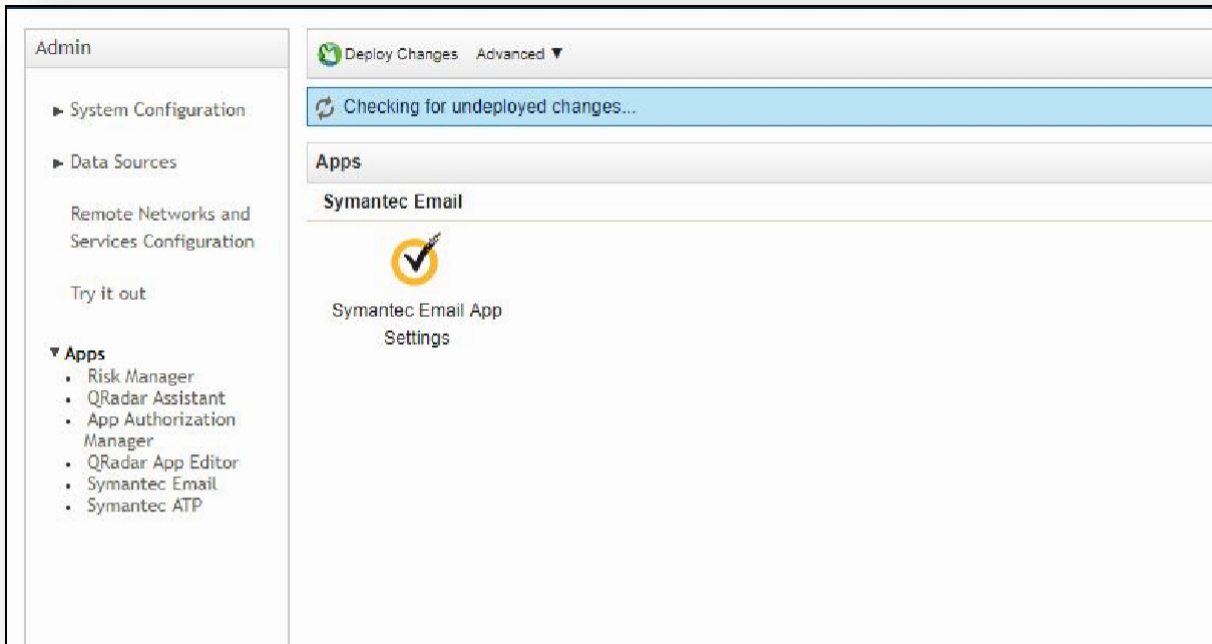


Figure 12: Installed apps configuration page

- Open configuration page and it shows setup page as follows:

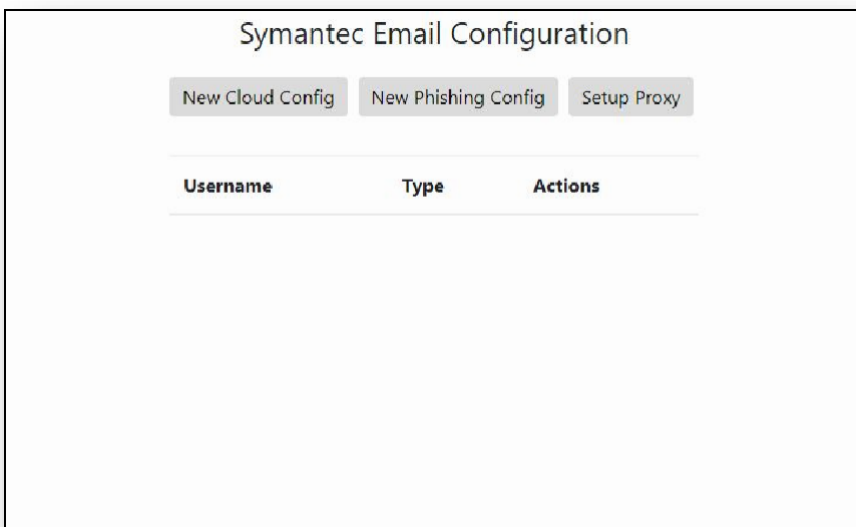
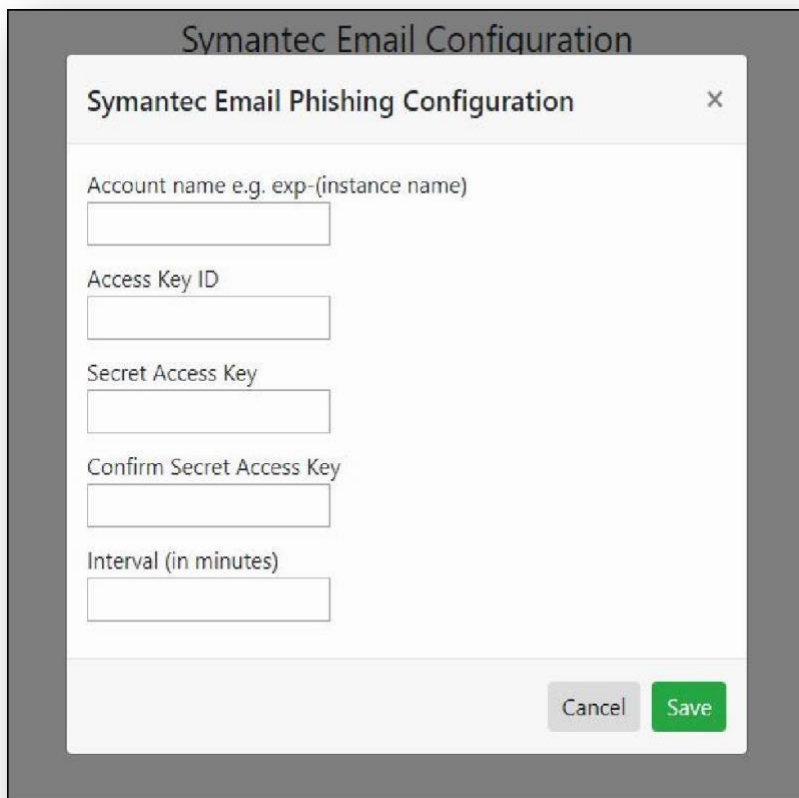
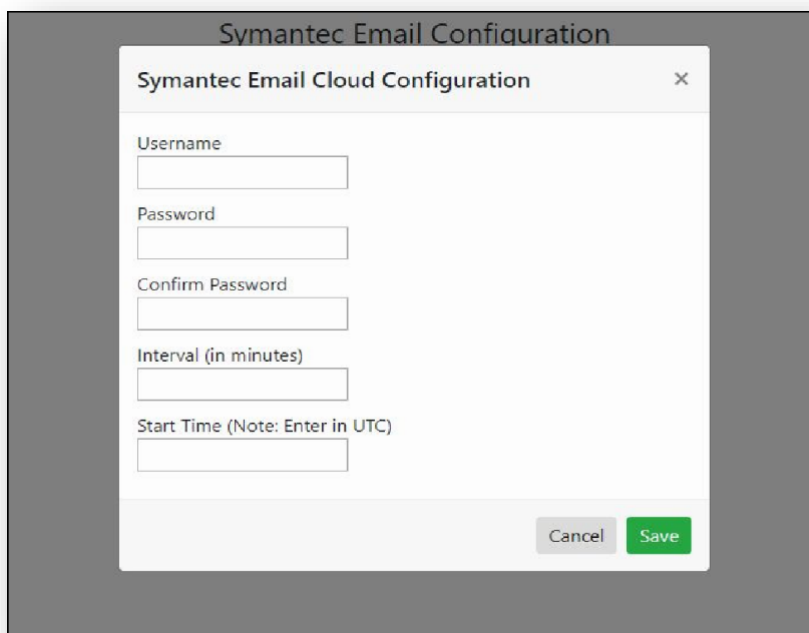


Figure 13: Symantec Email Security App configuration page

Note: The app supports multiple accounts for Cloud configuration and only single account for Phishing configurations.



The screenshot shows a dialog box titled "Symantec Email Configuration" with a sub-dialog titled "Symantec Email Phishing Configuration". The sub-dialog contains the following fields: "Account name e.g. exp-(instance name)", "Access Key ID", "Secret Access Key", "Confirm Secret Access Key", and "Interval (in minutes)". At the bottom right, there are "Cancel" and "Save" buttons.



The screenshot shows a dialog box titled "Symantec Email Configuration" with a sub-dialog titled "Symantec Email Cloud Configuration". The sub-dialog contains the following fields: "Username", "Password", "Confirm Password", "Interval (in minutes)", and "Start Time (Note: Enter in UTC)". At the bottom right, there are "Cancel" and "Save" buttons.

Figure 14 and 15: Cloud and Phishing configuration form

- Configure your Symantec Email cloud credentials (For NDF (ATP) data and Core data) and your Symantec Email phishing credentials (For Phishing data) and your data collection will start.
- Save credentials can be found in the table below where you can edit/delete the same.
- You can set proxy to fetch data from Symantec Servers.

The image shows a 'Setup Proxy' configuration window. At the top, there is a title bar for 'Symantec Email Configuration' and a sub-header 'Setup Proxy' with a close button (X). The main content area includes a green toggle switch labeled 'Enable/Disable Proxy'. Below this are several input fields: 'IP/Hostname (Please don't mention http or https in URL)', 'Port', 'Username', 'Password', and 'Confirm Password'. A checkbox labeled 'Require Authentication for Proxy' is checked. At the bottom right, there are two buttons: 'Cancel' and 'Save'.

Figure 16: Proxy configuration form

User Roles / Capabilities

The QRadar supports ACL configurations for restricting access different actions/dashboards. This app adds new capability called Symantec Email, which controls access to Symantec Email dashboard. For accessing Symantec Email dashboard, the user should be assigned a role that has this capability. By default, admin users have access to all the capabilities. To configure Role in QRadar, use following steps.

Login to QRadar console, go to Admin User Roles.

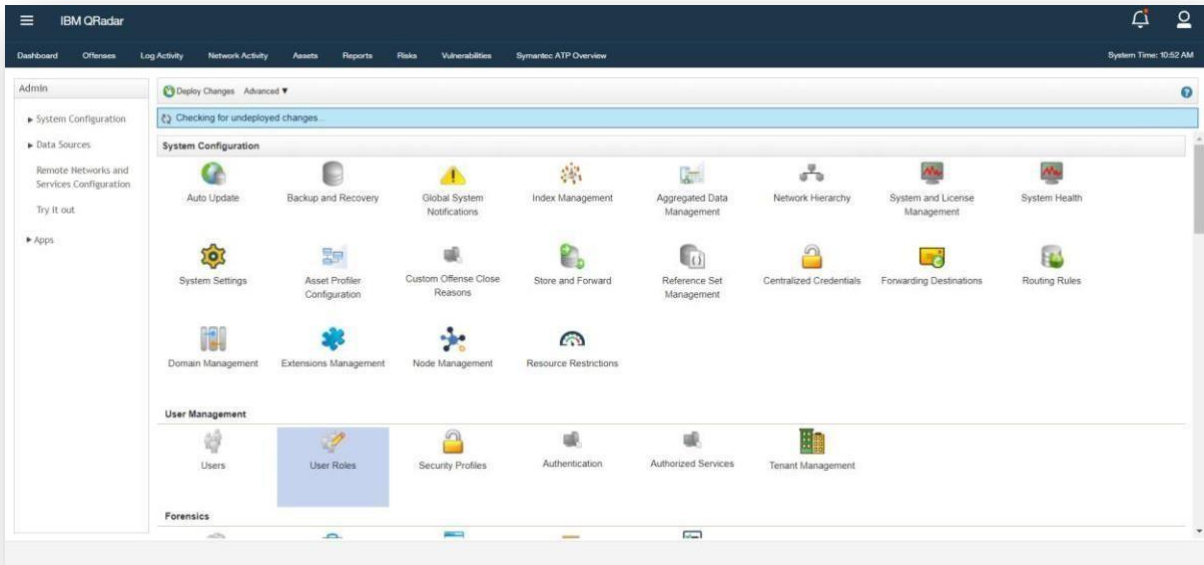


Figure 17: User Role

1. Click on New button.
2. Enter the name of the role. Assign required capabilities as shown in the screenshot. Assign these roles to Users who should be able to view Symantec Email Dashboard.

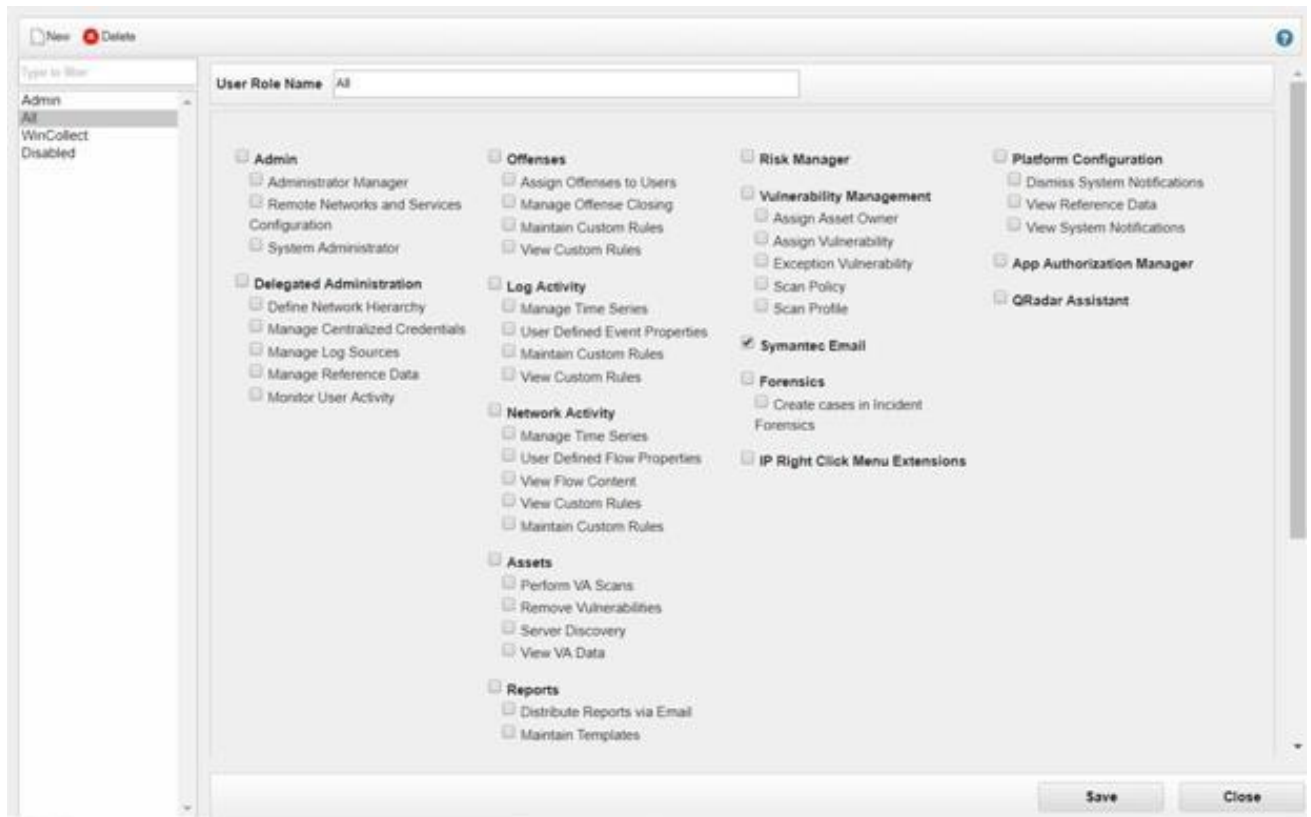


Figure 18: Assign App Permissions

Uninstalling the Application

To uninstall the application, the user needs to perform following steps.

1. Go to Admin Page
2. Open Extension Management
3. Select Symantec Email App for QRadar application
4. Click on Uninstall

QRadar Cloud Support

Symantec Email QRadar v1.0.0 supports all its functionalities on QRadar cloud.

Troubleshooting

This chapter includes the following topics:

- [Troubleshooting](#)
 - [Case #1 - App configuration fails with various error messages](#)
 - [Case #2 – Data is not getting collected in the app](#)
 - [Case #3 – UI related issues in the app](#)
 - [Case #4 – Events are coming as Unknown in App Log Source](#)
 - [Case #5 – All other issues which are not a part of the document](#)

Troubleshooting

This section describes the common issues that might happen during the deployment or the running of the app and the steps to resolve the issues.

Case #1 – App configuration fails with various error messages

Problem: New configuration fails with error message “Same configuration already exists. Please try different username”. Below is a screenshot for quick reference.

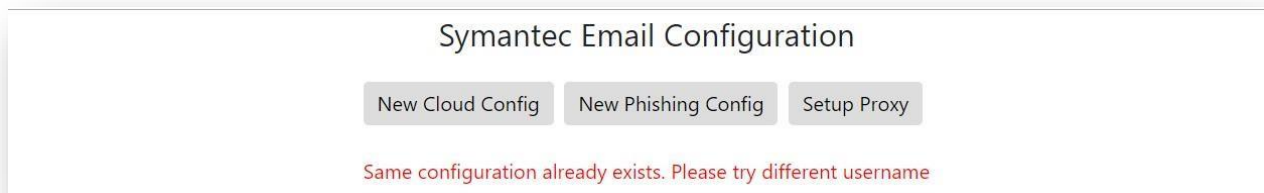


Figure 19: Duplicate credentials error

Troubleshooting Steps: User might have entered account which is already configured. User is recommended to enter new credentials which are not already provided

Problem: New configuration fails with error message “Authentication failed for cloud service. Please enter correct credentials”. Below is a screenshot for quick reference.



Figure 20: Incorrect Credentials error

Troubleshooting Steps: This happens when user has entered wrong credentials so authentication failed while saving new configuration. User is recommended to check the credentials and try again

Problem: New configuration fails with error message “Something went wrong. Please check logs for more details”. Below is a screenshot for quick reference.

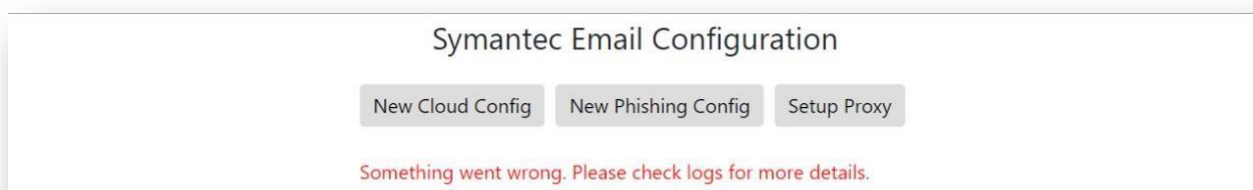


Figure 21: General error

Troubleshooting Steps: This happens when user has entered wrong credentials so authentication failed while saving the configuration. User is recommended to follow the troubleshooting steps as mentioned in Case #5.

Problem: Configuration of Symantec Email fails with error message “No connection could be made. The target machine refused it.”. Below is a screenshot for quick reference



Figure 22: Connection Timeout

Troubleshooting Steps: This happens when there is connection issue while connecting to Symantec Email Security.Cloud instance. User is recommended to check the connectivity or firewall rules on the QRadar machine.

Problem: Configuration of Symantec Email fails with error message “Authentication failed for the new credentials in cloud service”. Below is a screenshot for quick reference

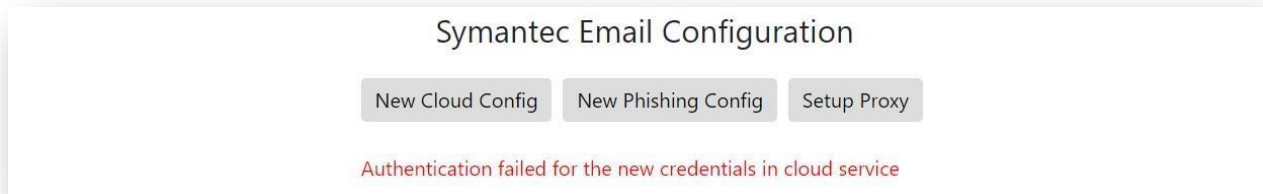


Figure 23: Incorrect credentials while updating configurations error

Troubleshooting Steps: This happens when user has entered wrong credentials so authentication failed while updating the configuration. User is recommended to check the credentials and try again.

Problem: New configuration of Symantec Email fails with error message "Updating the configuration failed". Below is a screenshot for quick reference

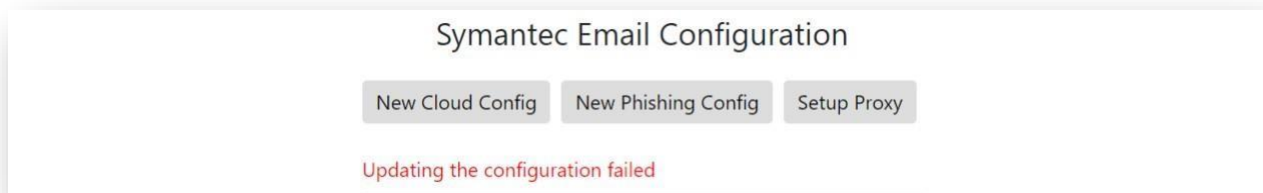


Figure 24: Updating configuration error

Troubleshooting Steps: This happens when updating the configuration in the file. User is recommended to follow the troubleshooting steps as mentioned in Case #5.

Problem: New configuration of Symantec Email fails with error message "Authentication failed for phishing service. Please enter correct credentials". Below is a screenshot for quick reference

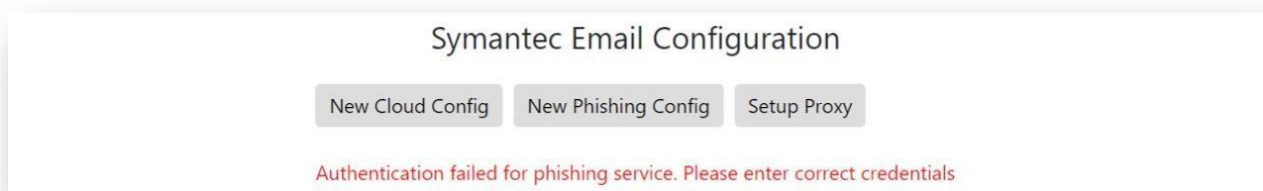


Figure 25: Incorrect Credentials error

Troubleshooting Steps: This happens when user has entered wrong credentials so authentication failed while saving new configuration. User is recommended to check the credentials and try again

Problem: Configuration of Symantec Email fails with error message "Authentication failed for the new credentials in phishing service". Below is a screenshot for quick reference



Figure 26: Incorrect credentials while updating configurations error

Troubleshooting Steps: This happens when user has entered wrong credentials so authentication failed while updating the configuration. User is recommended to check the credentials and try again.

Case #2 – Data is not getting collected in the app

Problem: Data is not getting collected by the app

Troubleshooting steps:

1. Click on System and License Management in Admin Panel
2. Select the host on which Symantec Email App is installed
3. Click on Actions in top panel and select the option Collect Log Files
4. A pop-up named Log File Collection will open
5. Click on Advance Options
6. Select the checkbox to Include Debug Logs, Application Extension Logs, Setup Logs (Current Version)
7. Click on Collect Log Files Button after selecting 2 days as datainput.
8. Click on "Click here to download files"
9. This will download all the log files in a single zip on your local machine
10. Create support case with Symantec and attach this log file

Case #3 – UI related issues in the app

Problem: Any dashboard panel, configuration pages, charts shows errors or unintended behavior.

Troubleshooting Steps:

1. Clear the browser cache and reload the webpage
2. Try reducing the time range of the filter and retry. It has been seen that QRadar queries expire if too much data is being matched in the query.
3. In Email Threats, if **Top 10 Countries – Malware** panel shows **No data** and on running the dashboard query of the above panel in Log Activity shows the results, then user is recommended to check whether http://geoip.nekudo.com/api/<<ip_address>> API is blocked or not for their QRadar instance (since we are using above API to map the countries with their respective IP address)

Case #4 – Events are coming as Unknown in App Log Source

Problem: Symantec email events come as Unknown

Troubleshooting steps:

1. Go to Log Activity.
2. Add Filter Log Source [Indexed] Equals Any of
 - a. Symantec Email ATP
 - b. Symantec Email Core
 - c. Symantec Email Phishing
3. Select Last 7 Days in Views filter.
4. If any events come as **Unknown**,
 - a. Right click on that particular event.
 - b. View in DSM editor.

- c. Check the value of Event ID, Event Category and Event Name under Log activity Preview
- d. If Event ID and Event Category value is extracted properly and Event Name value comes as unknown, create support ticket with Symantec Support.

Case #5 – All other issues which are not part of the document

Problem: If the problem is not listed in the document, please follow below steps.

Troubleshooting Steps: Please follow below steps:

1. Click on System and License Management in Admin Panel
2. Select the host on which Symantec Email App is installed
3. Click on Actions in top panel and select the option Collect Log Files
4. A pop-up named Log File Collection will open
5. Click on Advance Options
6. Select the checkbox to Include Debug Logs, Application Extension Logs, Setup Logs (Current Version)
7. Click on Collect Log Files Button after selecting 2 days as data input.
8. Click on "Click here to download files"
9. This will download all the log files in a single zip on your local machine
10. Create support case with Symantec and attach this log file

End of Document
