SandBlast Cloud Office 365 to CloudGuard SaaS for Office 365 Migration

Objective: This document's objective is to help customer access CG SaaS portal, and setup their SaaS application(s) (Office 365 emails in this case) and policy to match current SB Cloud policy, before full migration from Sandblast Cloud portal to CG SaaS.

Migration Plan:

- **Checkpoint creates CG SaaS portal for customers.**
- **Customer logs in to CG SaaS portal, connects to CG SaaS to Office 365 API, configures Office 365 policy (ies) as in current SB Cloud & leaves everything in detect (monitor) mode.**
- **After 1 week (ideally), customer disables SB Cloud protections, and enforces CG SaaS protections in prevent (inline) mode.**

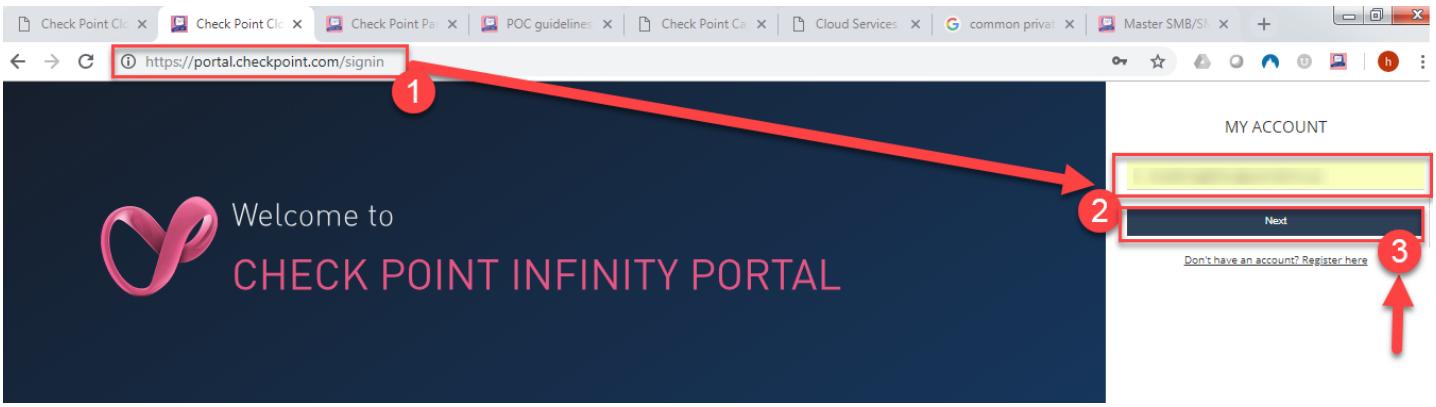
***Disclaimer: This document doesn't include steps for ID Protection – Identity Providers configuration at the moment. It will be added in a later update*.**
Follow SK 133692 - Configure Office 365 & Microsoft ADFS with CGS Authentication service.

Document prepared by Eugene Tcheby - Security Engineer

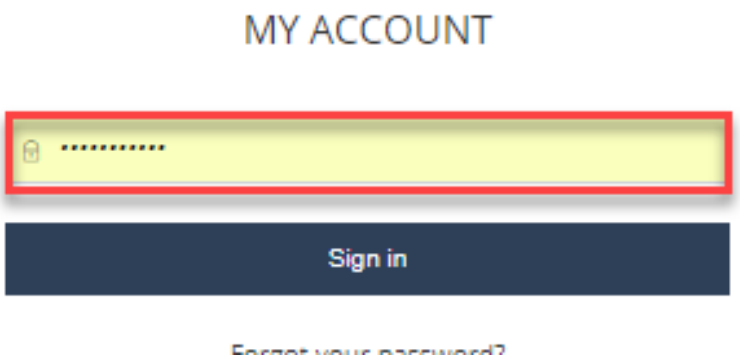
1- CG SaaS portal initial login & Configuration:

This step assumes that GC SaaS portal has already been created by Checkpoint and customer already filled pre-required information necessary to portal creation). An email outlining ALL required information should have been sent by Security Engineer to customer to ensure portal creation and login.

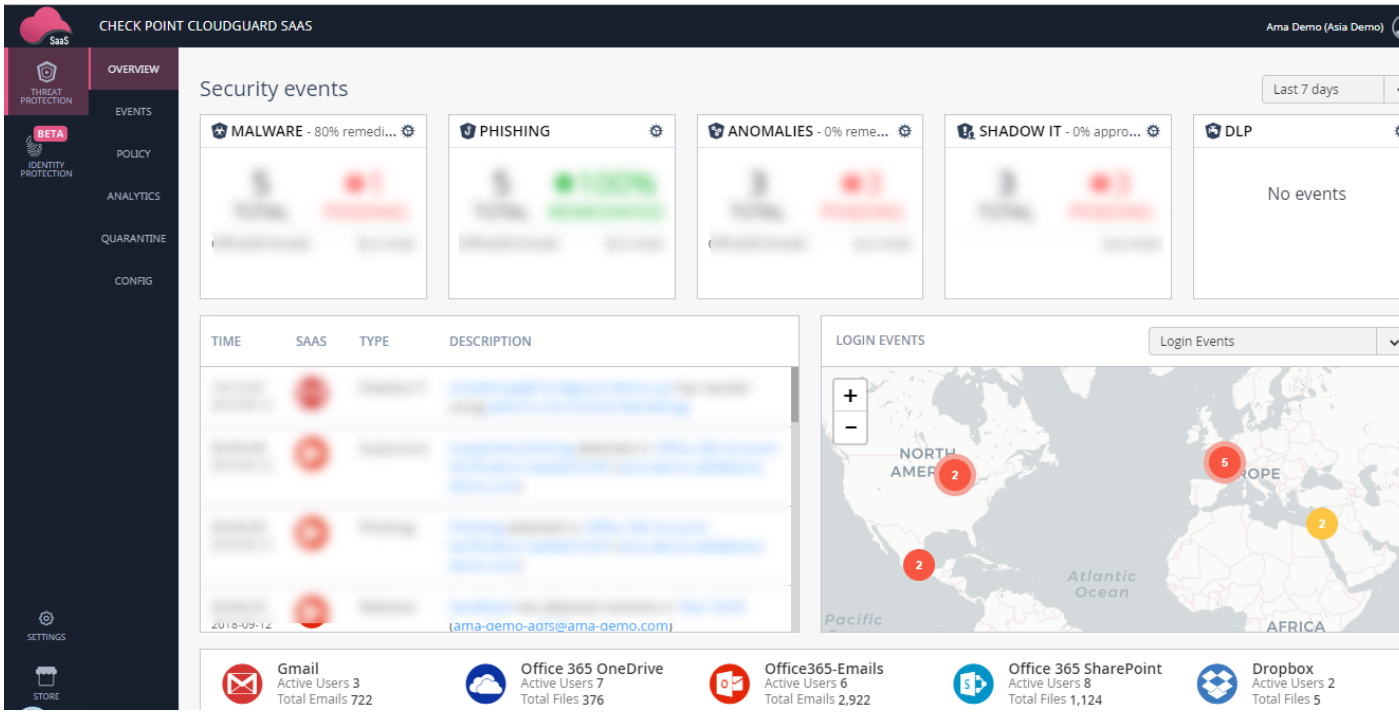
a. Login to the CG SaaS dashboard: https://portal.checkpoint.com/signin



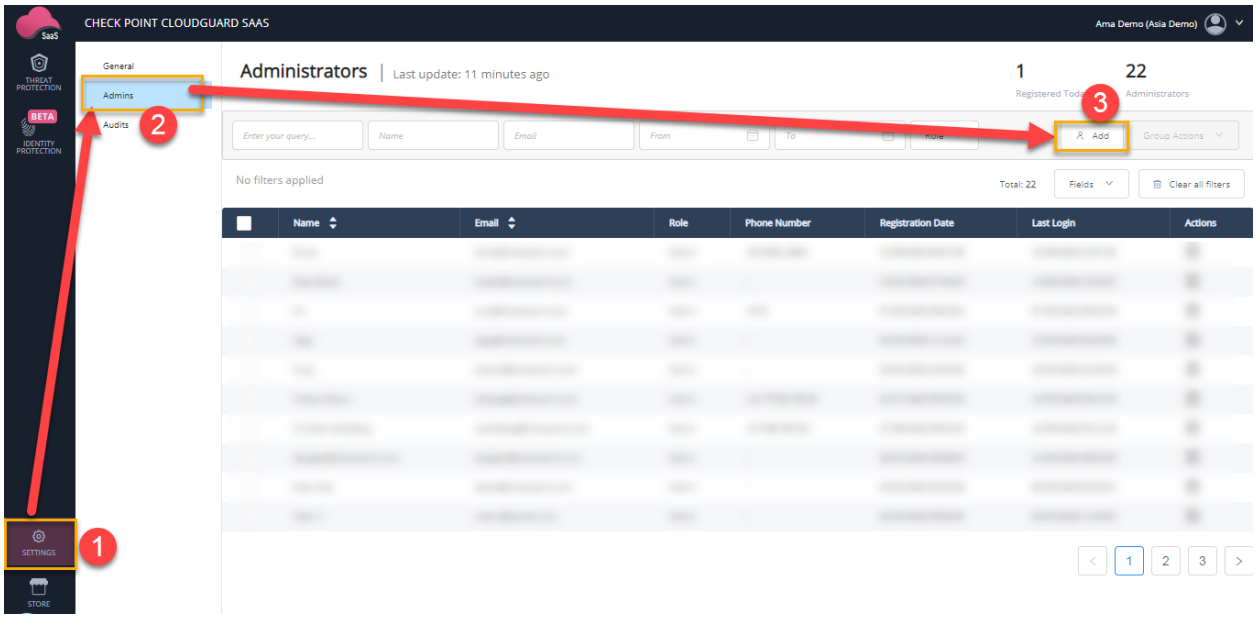
b. In step 2, enter full CG SaaS portal admin email address (provided by customer in the additional information form to fill out for portal creation)
c. Click Next,
d. On the following prompt, enter full CG SaaS portal admin password, and click "Sign In"



e. If login successful you should be presented with CG SaaS portal overview page. The below, is a demo dashboard, actual dashboard shouldn't display any malware, phishing, anomalies, DLP, nor shadow IT security events at all.



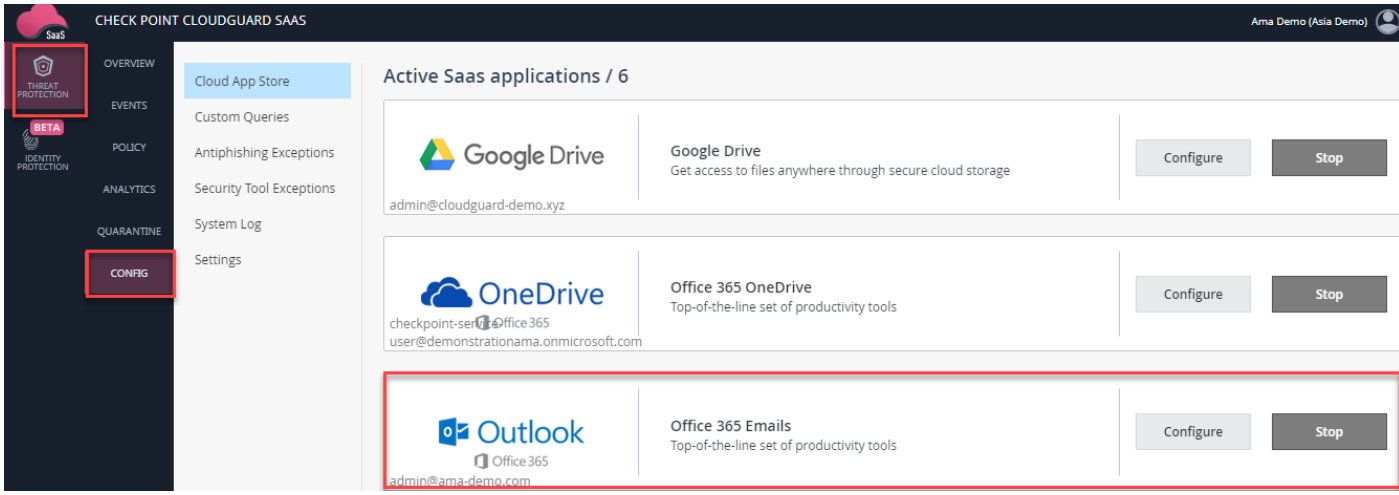
f. From the dashboard, select ***Settings---> Administrators ---> Add*** to add additional administrators with their relevant roles.



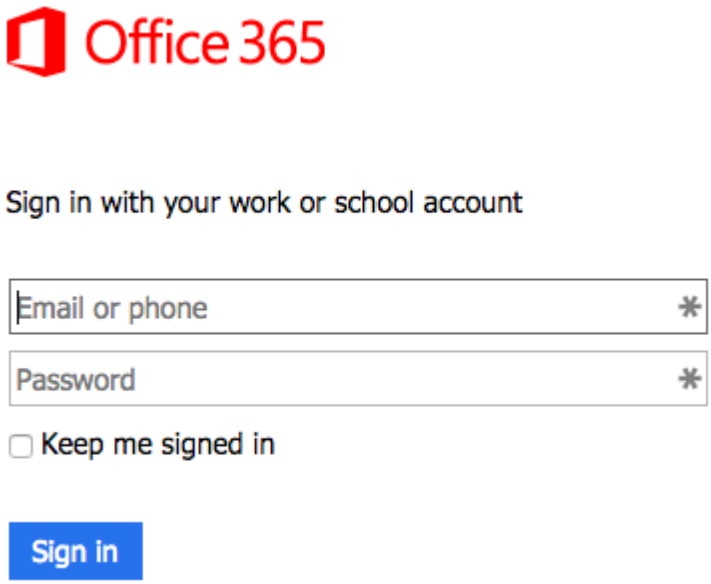
2. **<u>Connection to SaaS application:</u>**

Check Point's CG SaaS leverages Microsoft public API, and authentication to Office 365 is based on approving CG SaaS in the corporate Office 365 account. Essentially, the user will select the SaaS application to activate (Office 365 for emails) from the CG SaaS portal, and then user will be redirected to an authorization page, and using the company's Office 365 admin account the user approve CG SaaS access to their tenant account.

a. From the dashboard, select ***Threat Prevention --> Config --> Outlook Office 365 Emails --> Start***



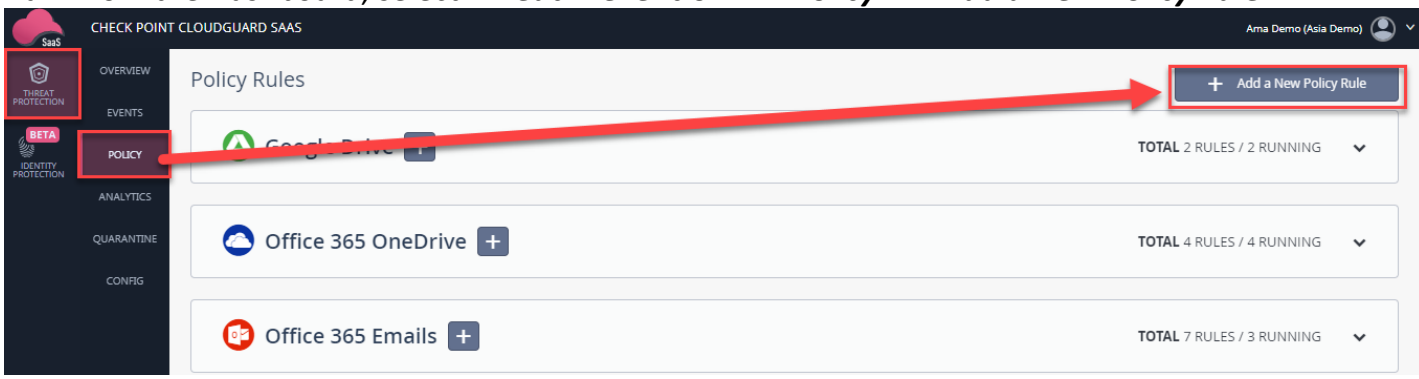
b. User will be redirected to an authorization page https://login.microsoftonline.com and prompted to enter Office 365 admin account credentials.



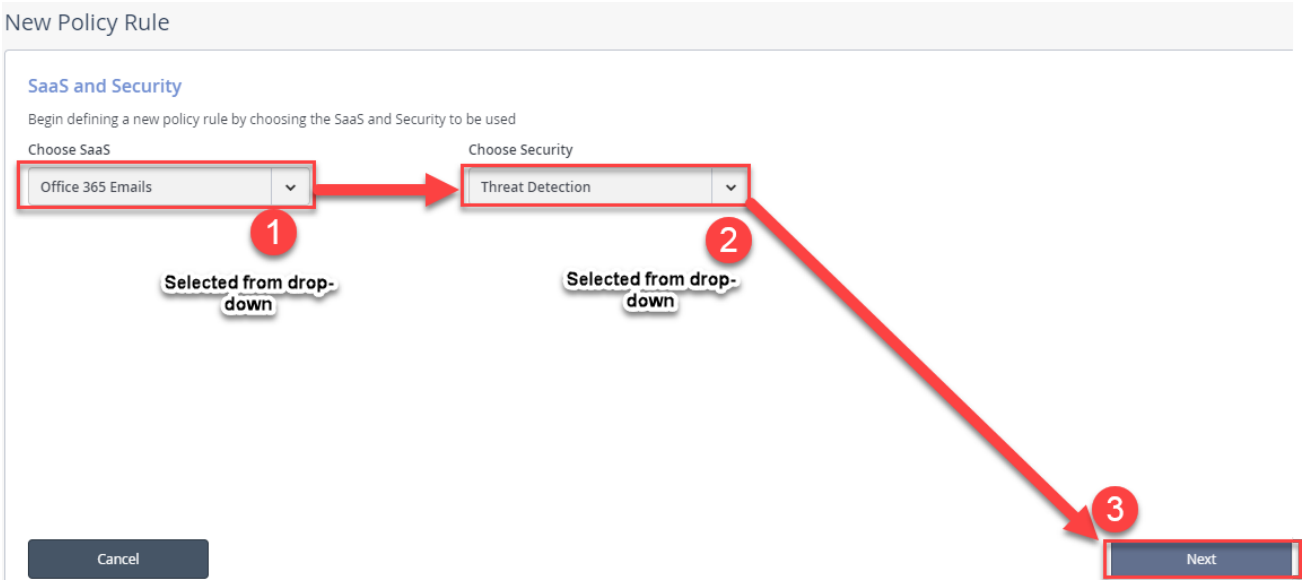
Once authentication is completed, CG SaaS will retrieve information from Office 365 such as user information (name, groups, and phone), files/folders, file and email content, metadata for Office 365 applications etc.…

3. **SaaS application policy configuration**

a. From the Dashboard, select ***Threat Prevention ---> Policy ---> Add a New Policy Rule***



b. On the next menu option, select the SaaS application you want to protect and the security blades you want to apply, and then click next. (Office 365 emails, Threat Detection are to be selected).



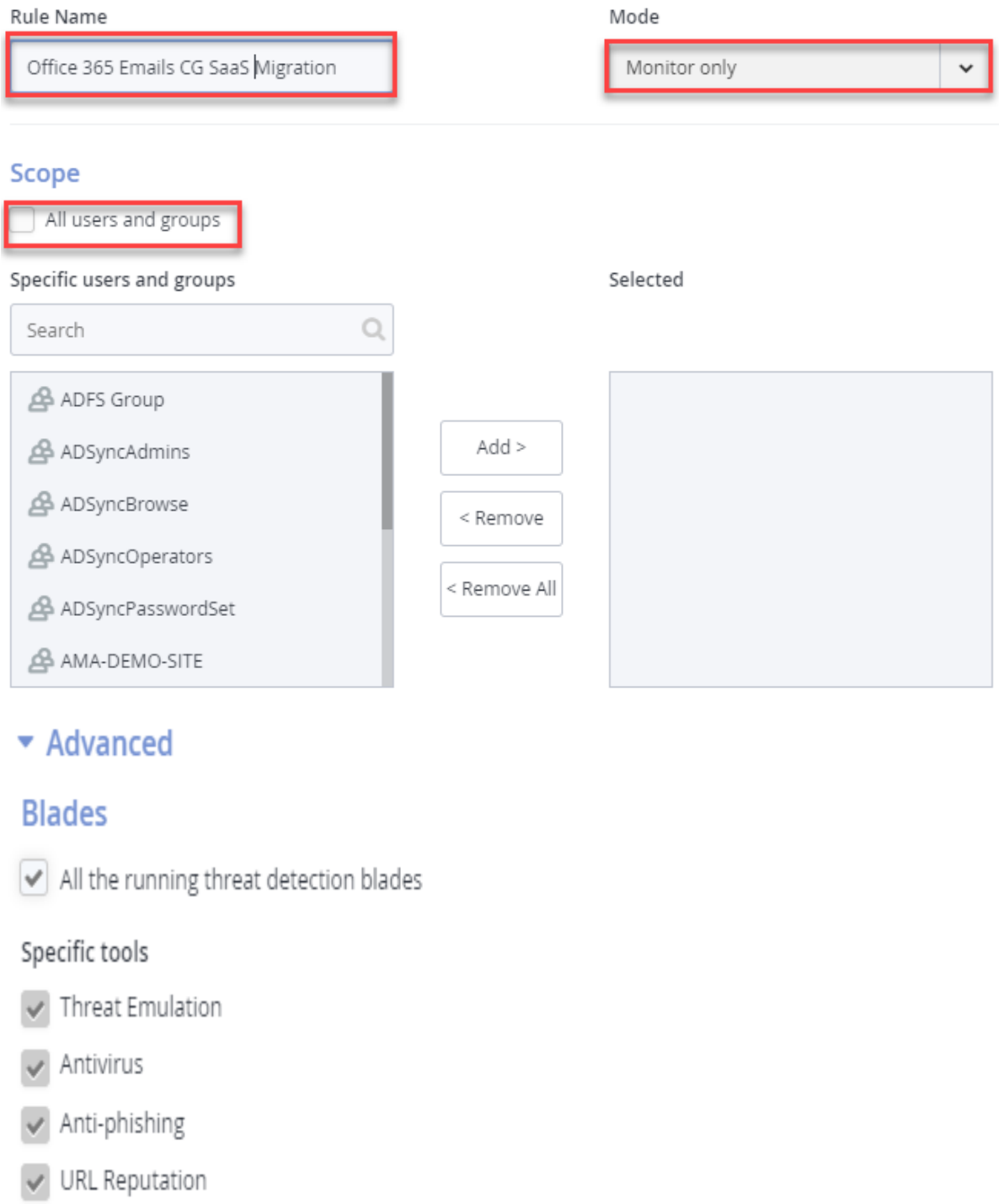
c. On the following page, we will configure rule name, protection mode, Scope, blades to be activated and Alerts.

Select options as indicated below:

Rule name: name on screenshot is optional, could be one chosen as per your naming convention.

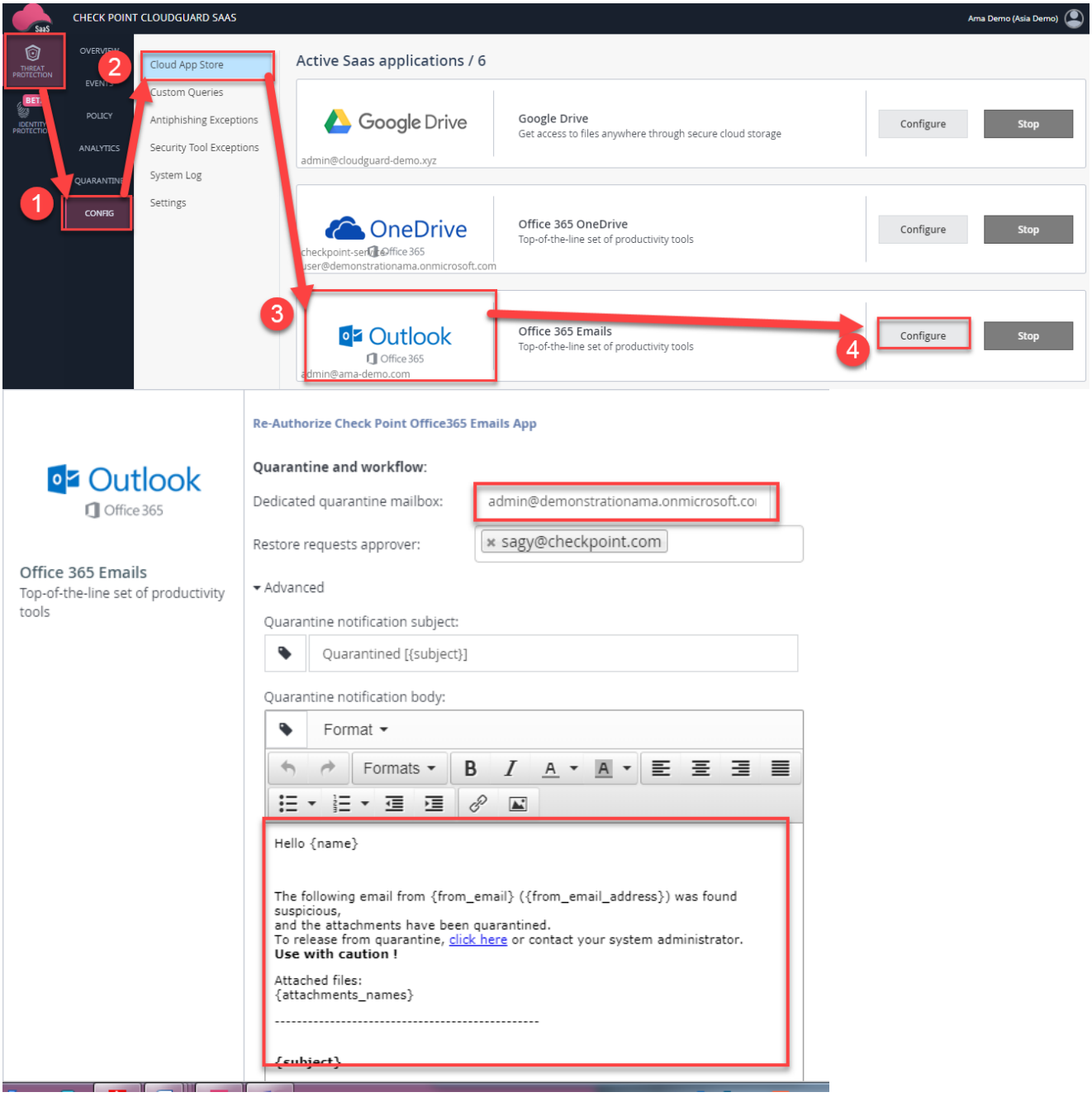
Mode: Monitor – We will leave this protection mode running for a week, and once all anomalies and security events have been checked, we will then turn it to inline (prevent) mode during effective migration.

Scope: Select specific users or groups that are matching current SB Cloud policy – or select all users by default.



Advanced ---> Blades: Match selected blades with currently activated as per your current policy or leave all selected blades checked by default.

Advanced ---> Alerts: At this stage we're recommending to setup an email account where all email alerts will be sent to. The same will be used for quarantined items.
Once policy is configured, click "save and apply".
Email address for quarantined items alerts can be added & email content configured by following steps:



Click Ok once you're done.

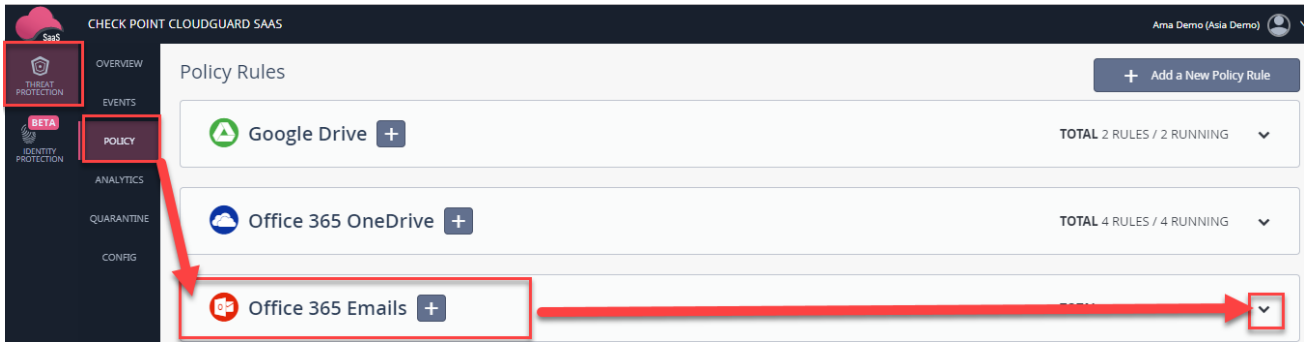
3. CG SaaS protection mode switch from Monitor Only --> Inline (Prevent)

The migration process from SB Cloud ---> CG SaaS is implemented in two phases. Phase 1 involves configuring CG SaaS portal; policy and protecting set in detect monitor mode for week after we've applied the configurations from sections 1 to 3.

Once week has passed, and after we've checked the anomalies, and security events or alerts, we can now enforce prevent mode (Inline) in CG SaaS.

A pre-requisite to enforcing prevent mode would be first disabling the protections in SB Cloud and Installing Policy.

Prevent mode in CG SaaS is achieved by following steps below: ***Threat prevention --> Policy ---> Office 365 emails---> Click on the drop down arrow***



Select the targeted underlined policy, click on the drop down under Mode and select protect (inline).