Check Point Sandblast Cloud for Office 365

Version 5

Activation, Set-up & First Steps Guide

Jonathan Zelman
SandBlast POC Manager
March 2017

Important Information

This guide has been created to assist Check Point SE's, Check Point Support, and Check Point Early Availability Customers in the installation and setup of Check Point's Sandblast Cloud for Office 365 product. The features and functionality described in this document are subject to change at any time.
Due to the fact that at the creation time of this document, Sandblast Cloud is an beta/early availability product still in active development, this document does not necessarily reflect the proper steps, procedures or protections available if used to configure Sandblast Cloud in the future.

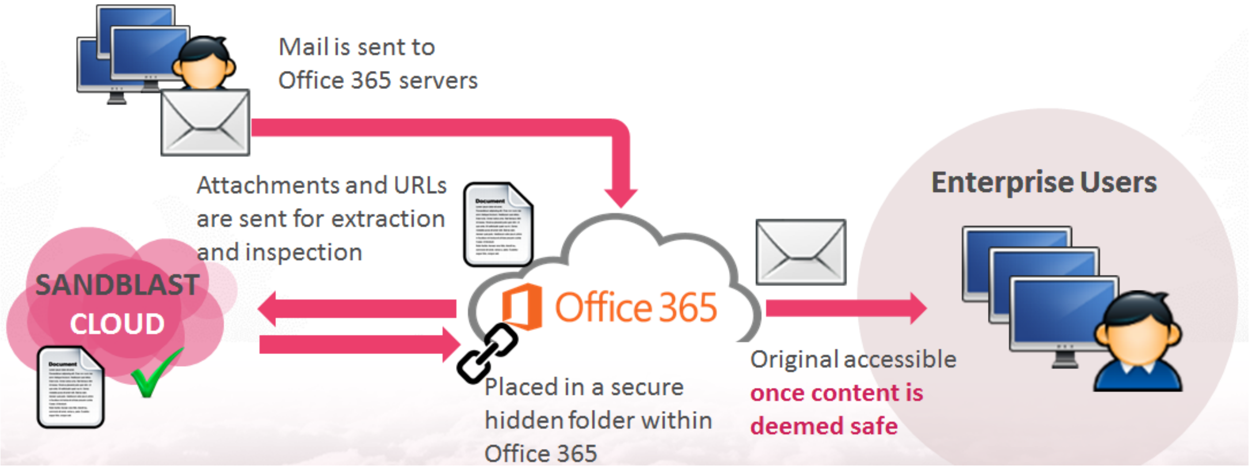
Official documentation will be posted to the Check Point Website at **http://supportcontent.checkpoint.com** once available.

Revision History

Date	**Description**
9 September 2016	First release of this document
November 25, 2016	Update of procedures to version 3b
January 23, 2017	Update of procedures to version 4b
February 15, 2017	Update of procedures to version 4b
March 13, 2017	Update of procedures to version 5

Welcome to Check Point SandBlast Cloud for O365

The Sandblast Cloud provides email protection for accounts in Microsoft's Office 365 product. When mail is sent to Office 365 Servers, Sandblast Cloud pulls the mail out of the user's inbox and places it in a secure hidden folder within Office 365. The attachments and URLs are sent for extraction and inspection to the Check Point Sandblast cloud and once deemed safe delivered to the user.


Mail is sent to Office 365 servers
Attachments and URLs are sent for extraction and inspection
SANDBLAST CLOUD
Office 365
Placed in a secure hidden folder within Office 365
Enterprise Users
Original accessible once content is deemed safe

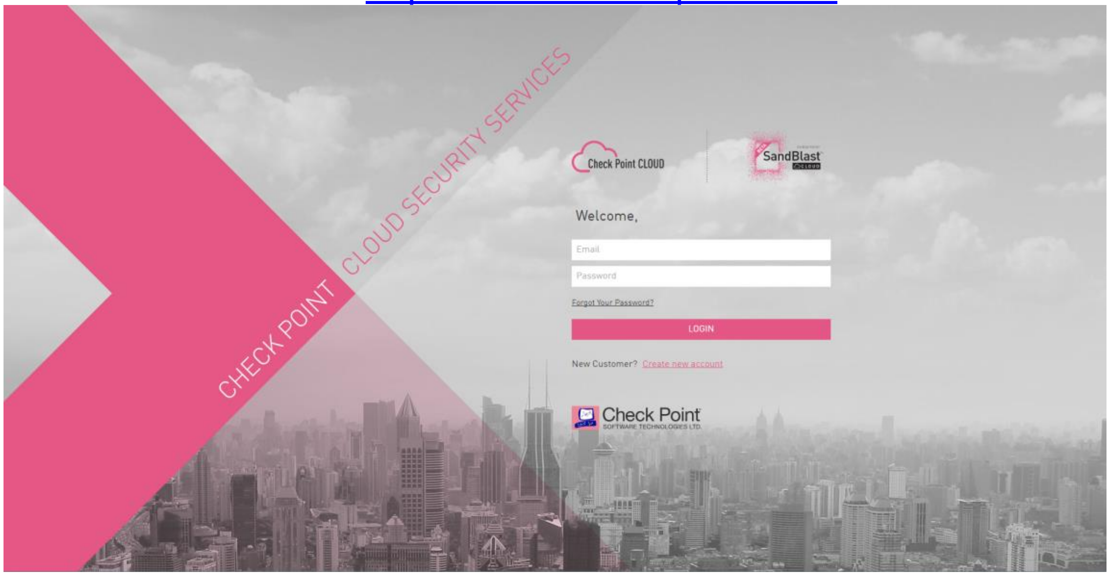
Sandblast Cloud can be configured in two different modes: detect and prevent.

When the policy for Sandblast Cloud is set to **detect**, mail will be inspected but malicious content will not be blocked. This mode is the least disruptive to the organization but also provides very little security.

When the policy is set to **prevent**, mail will be held in a secure folder until either a clean version of the attachment/URL has been created and delivered to the user, or the content has been determined to be safe. Once the determination and any necessary remediation have been made the mail will be returned to the user's inbox.

Creating a new account

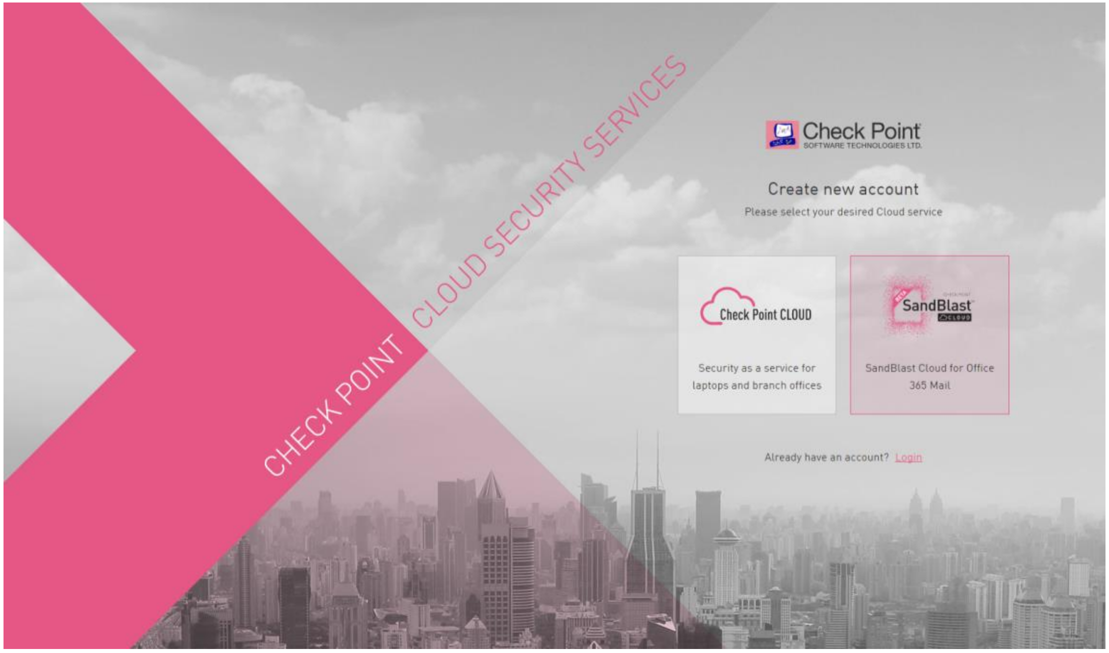
Browse to https://cloud.checkpoint.com



Welcome,

New Customer? Create new account

To create a new account, click on “Create new account” below the Login button.
Make sure you select to create a SandBlast Cloud account by clicking on the icon on the right (shaded in pink).



Create new account

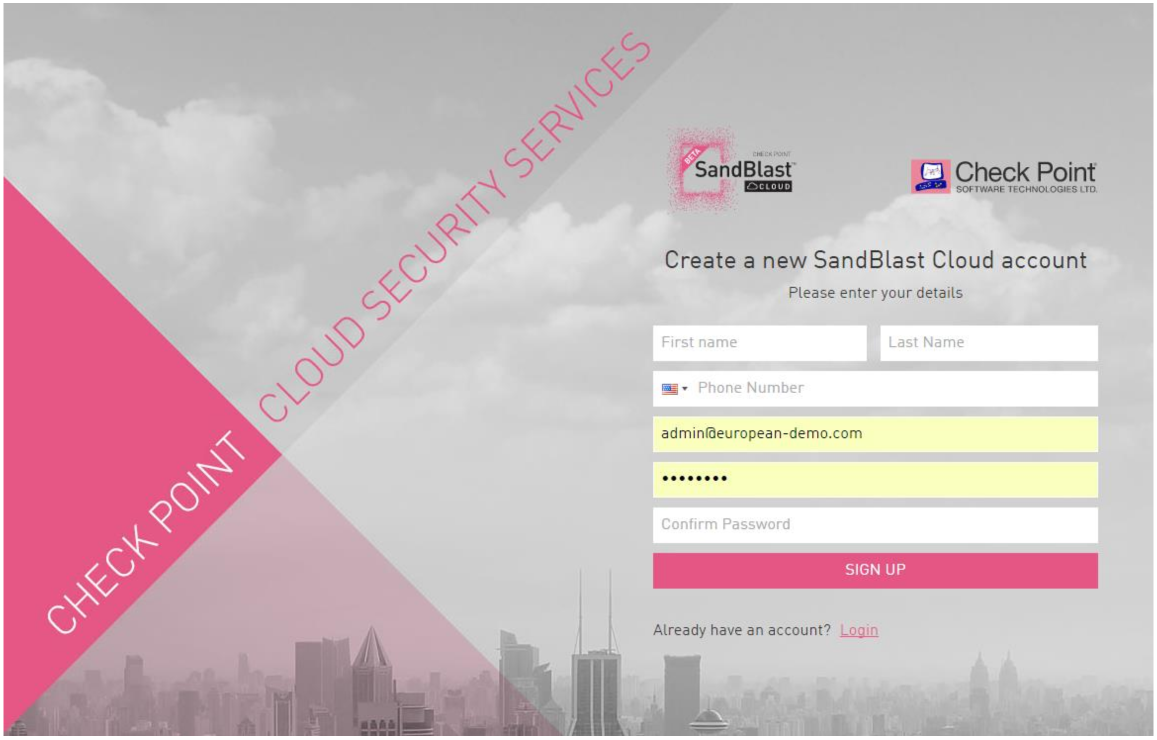
Please select your desired Cloud service

Security as a service for laptops and branch offices

SandBlast Cloud for Office 365 Mail

Already have an account? Login

Fill in your information to register a SandBlast Cloud account.



CHECK POINT
CLOUD SECURITY SERVICES
BETA
CHECK POINT SandBlast CLOUD
Check Point SOFTWARE TECHNOLOGIES LTD.

Create a new SandBlast Cloud account

Please enter your details

First name | Last Name

Phone Number

admin@european-demo.com

••••••••

Confirm Password

SIGN UP

Already have an account? Login

Once you sign up, you will receive an email notifying this. Simultaneously, a registration request will be sent to the SandBlast team to be evaluated.

Please note that to register for a SandBlast Cloud account you will need to use a different user than the one you have used for other Check Point Cloud services including Capsule.

To help speed up the process, please ask your Check Point contact to get in touch with the SandBlast POC team and supply the following information: # of mailboxes you wish to protect, User Center ID, and that you are aware of the current status of the product as explained below.

As you know, Check Point SandBlast Cloud is a Security-as-a-Service (SaaS) solution that protects Microsoft Office 365™ cloud-based email environments using Check Point SandBlast Zero-Day Protection capabilities.

Before you continue, please be aware that this product is currently in Beta version, which allows us to get first impression of our technology integrated in customer environment, for which we recommend to proceed only if there is a clear understanding of this.

The product is under continuous development and expected to be in GA by Q2 2017.

By then we will be introducing missing features & improvements.

Please make sure you are aware of this and wish to proceed.

For more information regarding the current status & roadmap for SandBlast Cloud, please ask your Check Point contact to get in touch with the SandBlast POC team.

Using the Cloud Portal

After logging in, the Cloud Portal opens on the **Overview** tab. Use the:

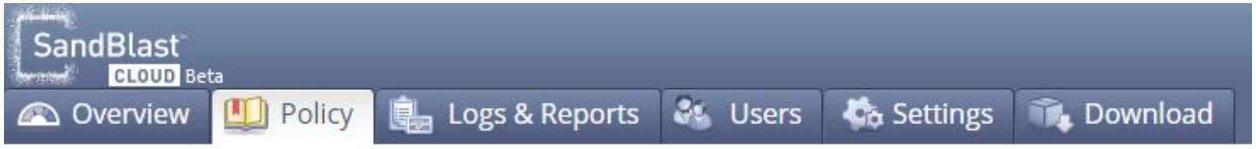
- **Overview** tab to see the Sandblast Cloud activity in your environment.
- **Policy** tab to setup the API connection between Microsoft Office 365 and Check Point.
- **Logs & Reports** tab to see logs of user email and audit logs and to setup scheduled reports.
- **Users & Groups** tab to add and change settings for users that can access the Sandblast Cloud administration portal.
- **Settings** tab to associate your User Center Account with Sandblast Cloud and setup the Log Transport server.
- **Download** tab to download the Log Transport Agent utility.

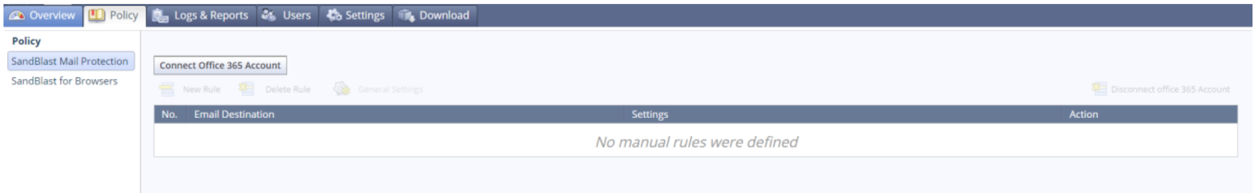
Once you have received notification that your account is active. Please log in via https://cloud.checkpoint.com with your credentials.

Account Association

First we need to set up the association between SandBlast Cloud's API and Microsoft to allow access to your Office365 mailboxes.

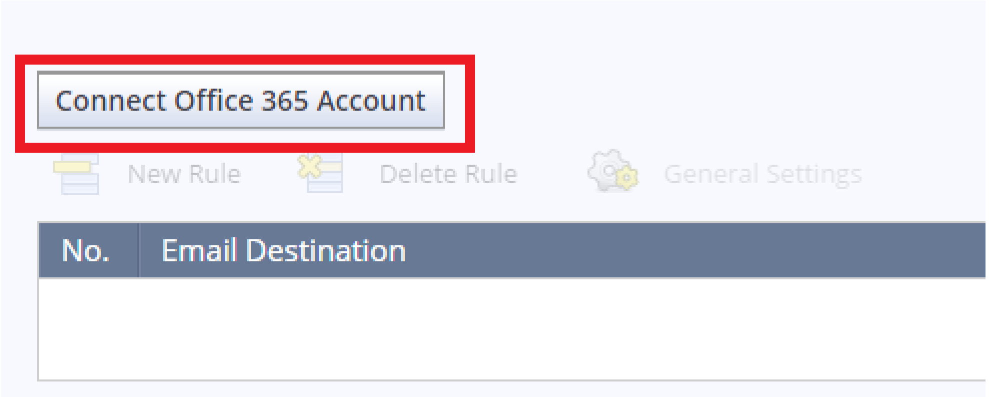
Navigate to the Policy tab



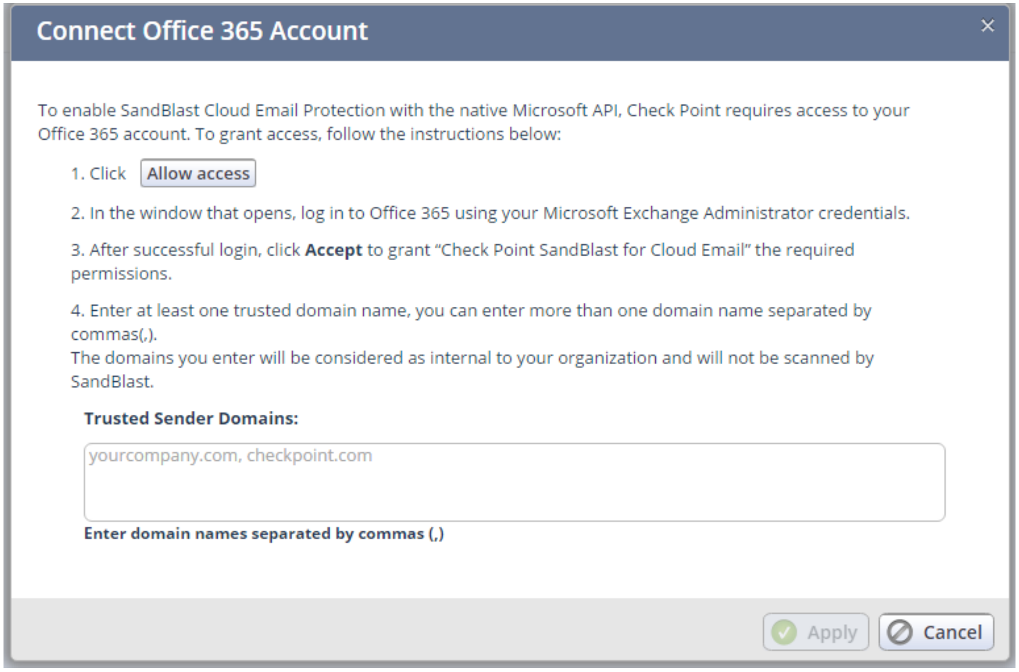


No.	Email Destination	Settings	Action
	No manual rules were defined		

Click on the "Connect Office 365 Account" button to create the association.



After clicking on “Connect Office 365 Account”, the following pop-up window will appear:



Connect Office 365 Account

To enable SandBlast Cloud Email Protection with the native Microsoft API, Check Point requires access to your Office 365 account. To grant access, follow the instructions below:

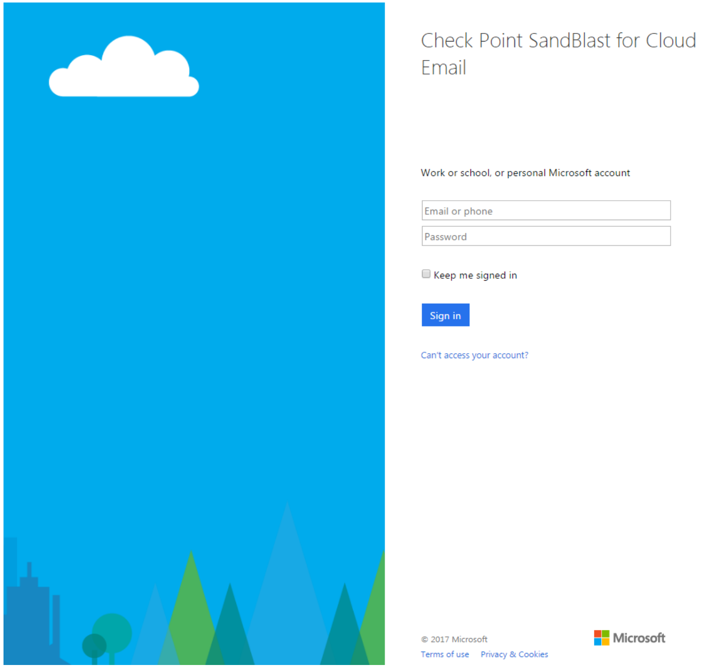
1. Click Allow access
2. In the window that opens, log in to Office 365 using your Microsoft Exchange Administrator credentials.
3. After successful login, click **Accept** to grant “Check Point SandBlast for Cloud Email” the required permissions.
4. Enter at least one trusted domain name, you can enter more than one domain name separated by commas(,).
The domains you enter will be considered as internal to your organization and will not be scanned by SandBlast.

Trusted Sender Domains:

yourcompany.com, checkpoint.com

Enter domain names separated by commas (,)

Follow the instructions in this window to connect the O365 account. Clicking the “Allow Access” button will redirect you to a MS O365 login landing page. Log in the MS O365 Administrator credentials to continue.



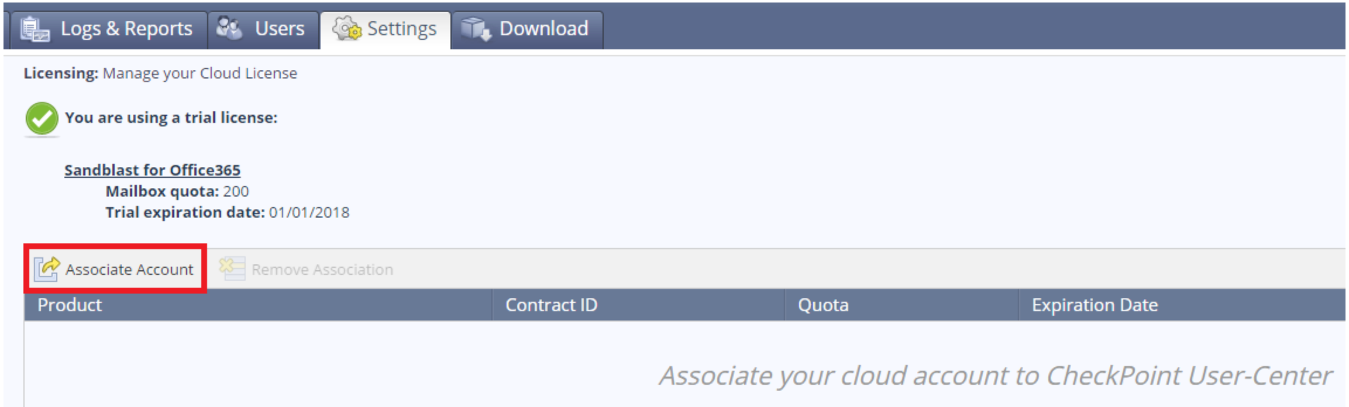
Check Point SandBlast for Cloud Email

Work or school, or personal Microsoft account

To finish, please input the internal domain into the Trusted Sender Domains box seen at the bottom of the “Connect Office 365 Account” page.

Please note that the current license model for SB Cloud only supports incoming external emails, not internal emails. Due to this, you must input your internal domain in the “Trusted Sender Domains” box shown above. If you have several domains or wish to add more, you can also add them here.

In order to associate or view the account’s license, click on the settings tab. Here you can view the current license SandBlast Cloud has, including quota and expiration date.



Licensing: Manage your Cloud License

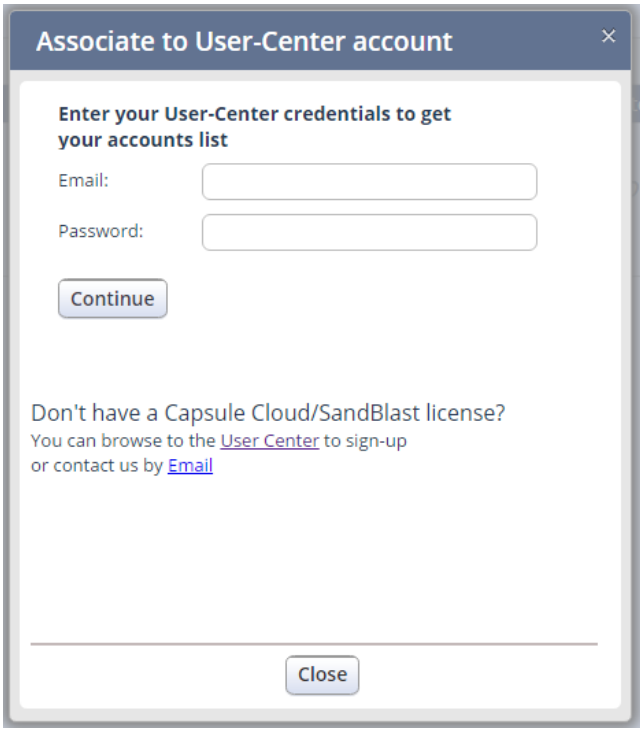
You are using a trial license:

Sandblast for Office365
Mailbox quota: 200
Trial expiration date: 01/01/2018

Product	Contract ID	Quota	Expiration Date

Associate your cloud account to CheckPoint User-Center

To associate a license, click on the ‘Associate Account’ button as seen above and the following window will appear:



Associate to User-Center account

Enter your User-Center credentials to get your accounts list

Email:

Password:

Don't have a Capsule Cloud/SandBlast license?
You can browse to the User Center to sign-up
or contact us by Email

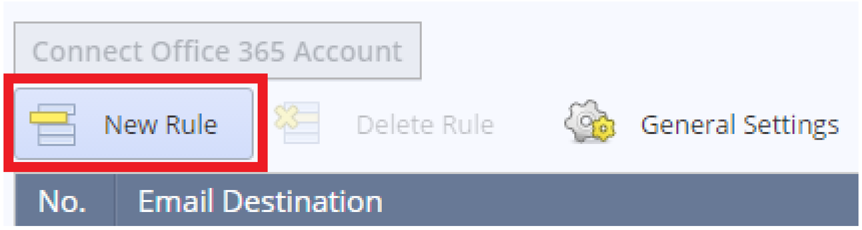
Log in with the User Center account credentials and click continue to view the licenses associated to this account. Click on the relevant license and the contract will be associated.

If you are experiencing any issues with quota or expiration date, please click the “Remove Association” button and repeat the above steps to re-associate the account’s license.

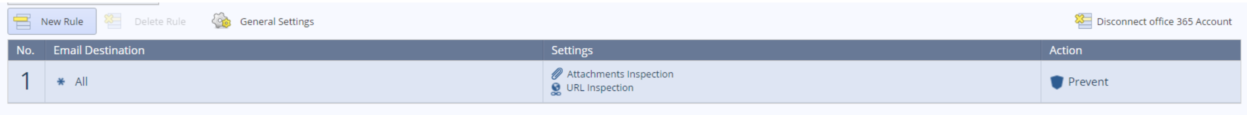
NOTE: Associating your User Center Account is only necessary if you have PURCHASED Sandblast Cloud, you do not need to associate a User Center Account if you are doing a trial.

Policy and Rule Set-up

Once the O365 account and license association is completed, you can proceed to create relevant rules. Do this by clicking “New Rule” button

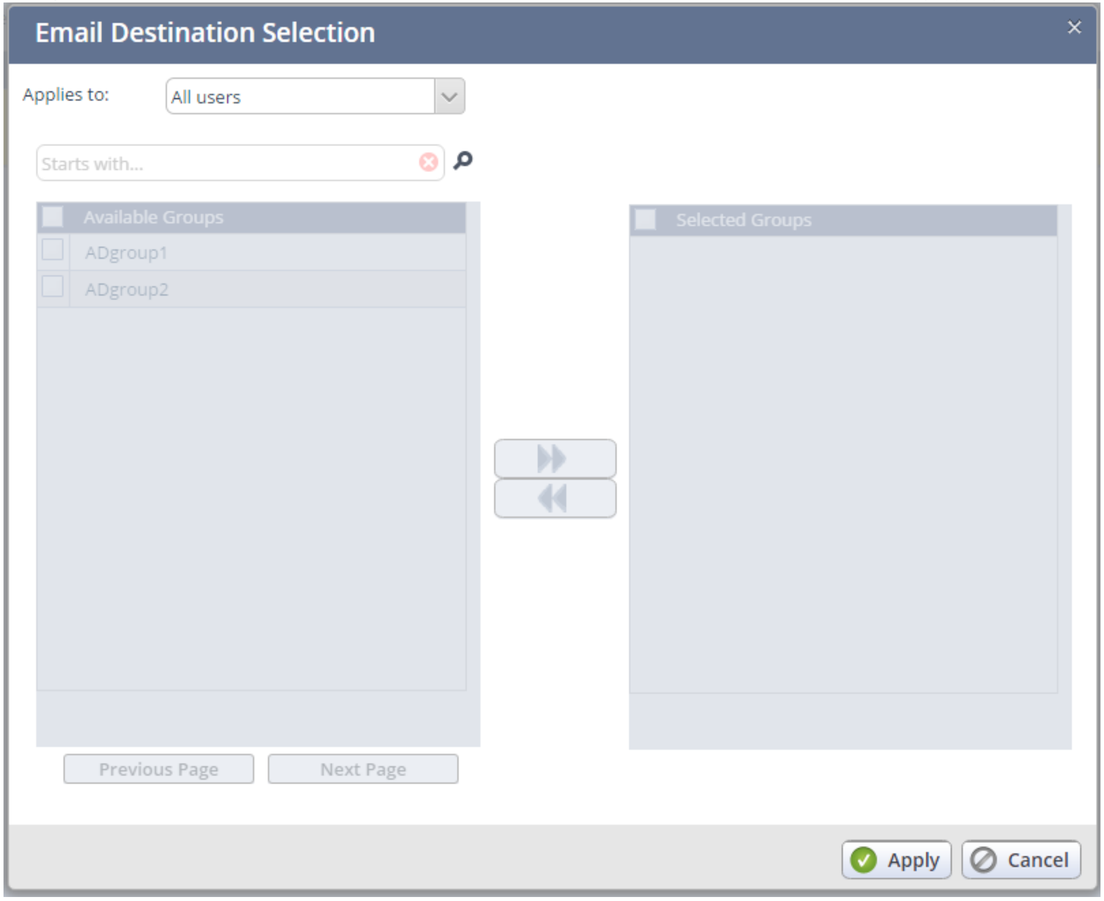


By default, you will see this rule below. Double click on each section of the rule itself to modify.



No.	Email Destination	Settings	Action
1	✱ All	Attachments Inspection URL Inspection	Prevent

Double-clicking on the rule in the “Email Destination” column, you will see this window pop up:

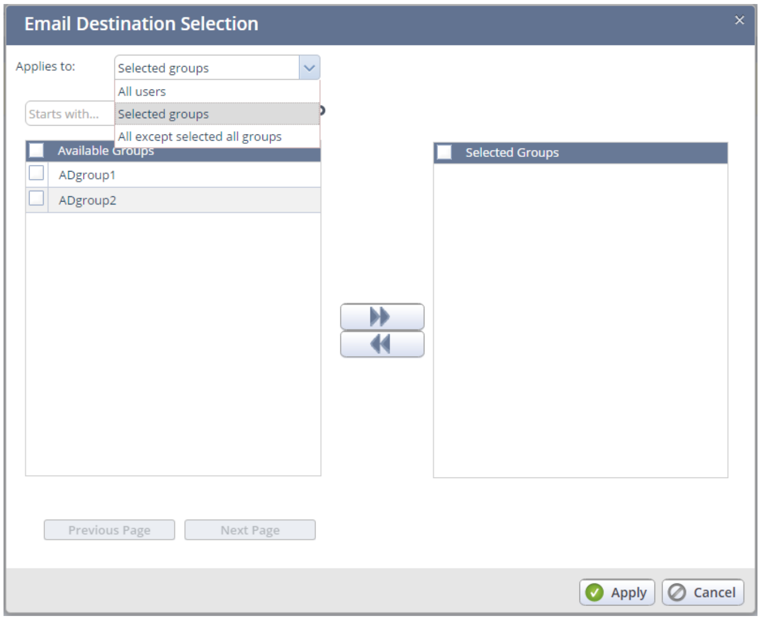


Email Destination Selection

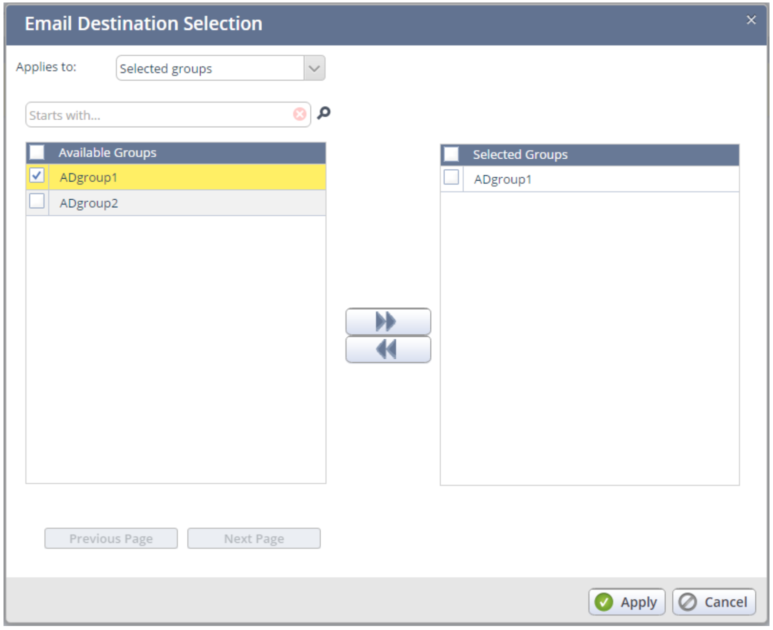
Applies to: All users

This window allows you to select the AD groups that the rule will be applied to. Selection mode all will apply the rule to all AD groups.

Choose selection mode: “Selected” to select the AD groups that the rule will be applied to.
Choose selection mode: “All except selected” to negate the selected AD groups from the rule (it will be applied to all other AD groups)

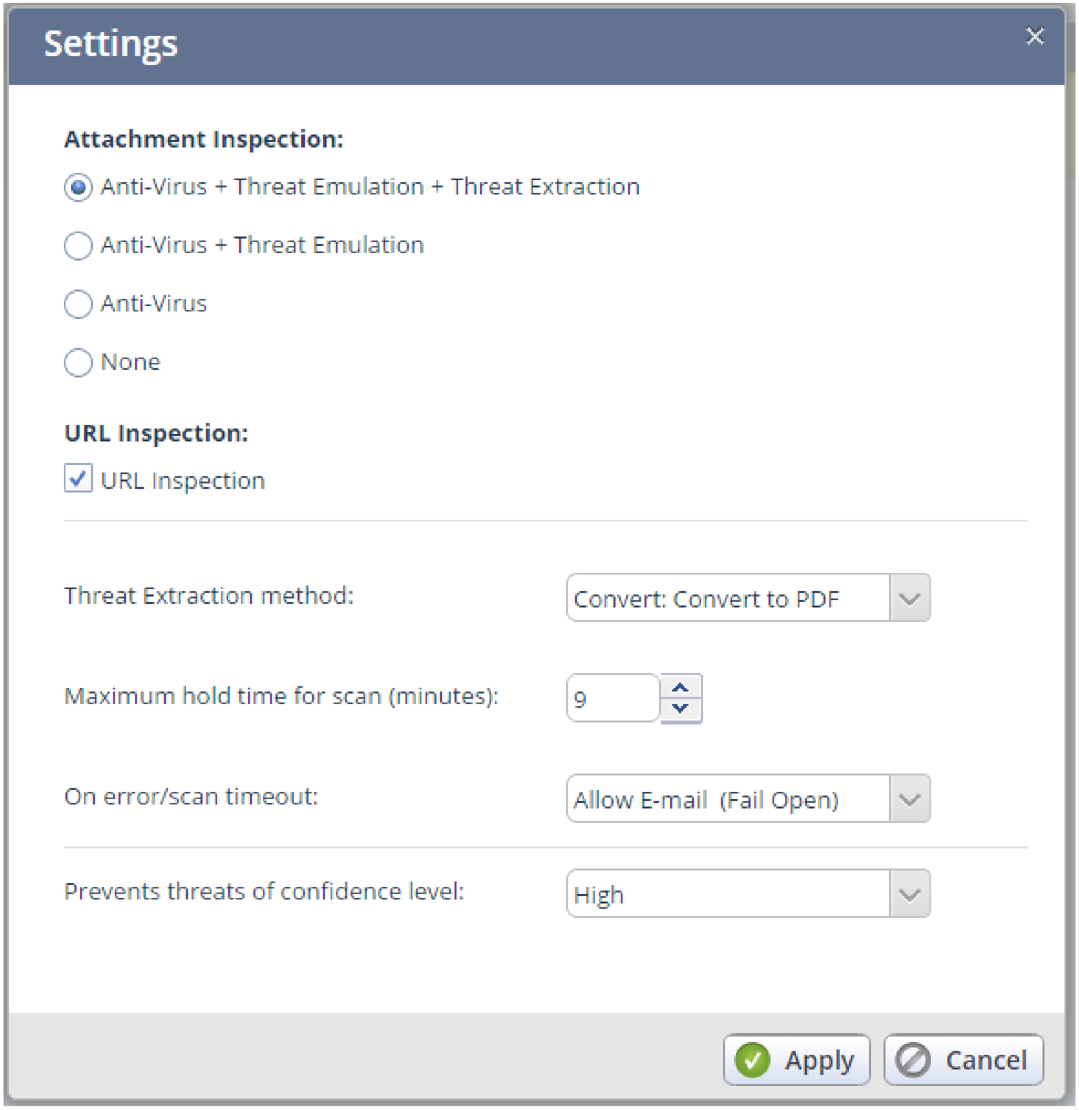


We can then go ahead and define the groups selected for this rule. In the example below, ADgroup1 is selected so the rule will be for that AD group.



Please note that the rules are per mailbox, but set up per O365 AD group.
For example: Let’s say user “John Smith” is both in the “Accounting” and “Finance” AD group.
If we create rule 1 with a Prevent action for “Accounting” AD group, and rule 2 with “No Inspection” action for “Finance” AD group, user “John Smith will be scanned as the rule that applies to him is the first relevant rule.

Modifying the “Settings” column will pop up the below window:



Settings

Attachment Inspection:

● Anti-Virus + Threat Emulation + Threat Extraction

○ Anti-Virus + Threat Emulation

○ Anti-Virus

○ None

URL Inspection:

☑ URL Inspection

Threat Extraction method: Convert: Convert to PDF

Maximum hold time for scan (minutes): 9

On error/scan timeout: Allow E-mail (Fail Open)

Prevents threats of confidence level: High

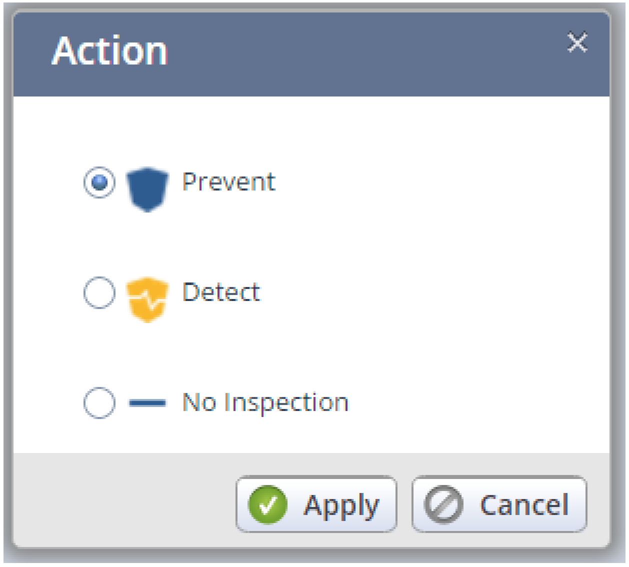
In this screen we can determine the different settings of the inspections as well as the emulation hold time. What you see in the screenshot above are the default settings & best practice.

- **Attachment Inspection**: Here we can decide what type of inspection we would like done on the attachment of the email for this rule. Here we can choose if we want “Anti-Virus + Threat Emulation + Threat Extraction” (Threat Extraction technology with full inspection using AV and SandBlast), “Anti-Virus + Threat Emulation” (same as before but without TEX), “Anti-Virus” (Only AV inspection),“ or “None” (no inspection).

- **URL Inspection**: By checking this box, we activate URL inspection for this rule. SandBlast Cloud inspects links on the email subject & body. If a URL with malicious content is found, then all the text in the section where the URL is found is removed and replace by a text informing the user of this. In the near future, we will only be removing and replacing the malicious content and preserving all benign content such as text in the email body.

- **Confidence Level**: This determines the level of confidence we want to use to determine the inspection of the attachments and URLs for this rule. If we select ‘Low to high’, all content with a Low, Medium or High confidence level will be prevented (assuming that the rule is set to prevent action). By setting, ‘Medium to high’ the same is done for Medium and High confidence level content, while selecting ‘High’ only affects content with a High confidence level.
  By choosing ‘Low’ we will experience a higher catch rate, however more false positives might occur, and vice-versa by choosing ‘High’
  If a rule includes URL inspection, we currently advise to select ‘High’ as confidence level.
- **Maximum hold time**: In this field we can select the maximum amount of time in minutes (must be between 4-60mins) for which we would like SandBlast Cloud to hold the content to be scanned. Note this is the maximum time, so content will be delivered as soon as emulation has reached a verdict.
  It is advised to leave this field in 9 minutes. Although the vast majority of emulations will be completed within 4-5 minutes, there are a small number of emulations which could take up to 9 minutes.
- **On error/scan timeout**: In this last field we establish what will happen once the maximum hold time elapses. If we choose Fail Open, the content which has been under hold will be released after the 9 minutes and will be delivered the recipient’s inbox with no scan. If we choose Fail Close, the content will still be held for emulation regardless of those 9 minutes elapsing.
  Nevertheless, we have introduced retroactive handling for the Fail Open cases – no need to configure any additional settings. This means that if we choose Fail Open and the maximum hold time has elapsed, SandBlast Cloud will still be scanning the content of the email and in the event that any malicious content is found, SandBlast Cloud will retroactively remove it from the user’s email.

Double-clicking on the rule in the “Action” column, you will see this window pop up:



Action

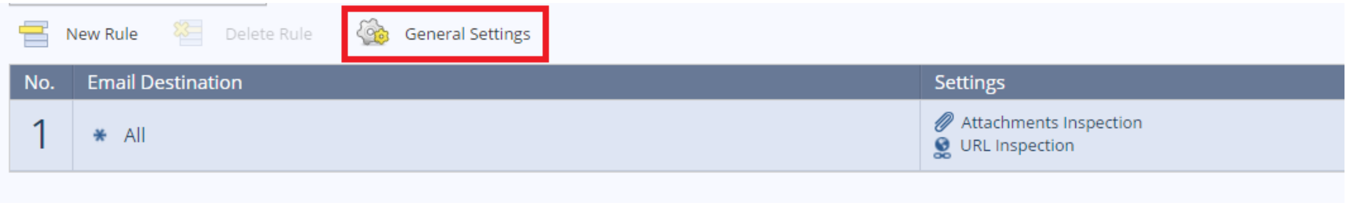
● Prevent

○ Detect

○ No Inspection

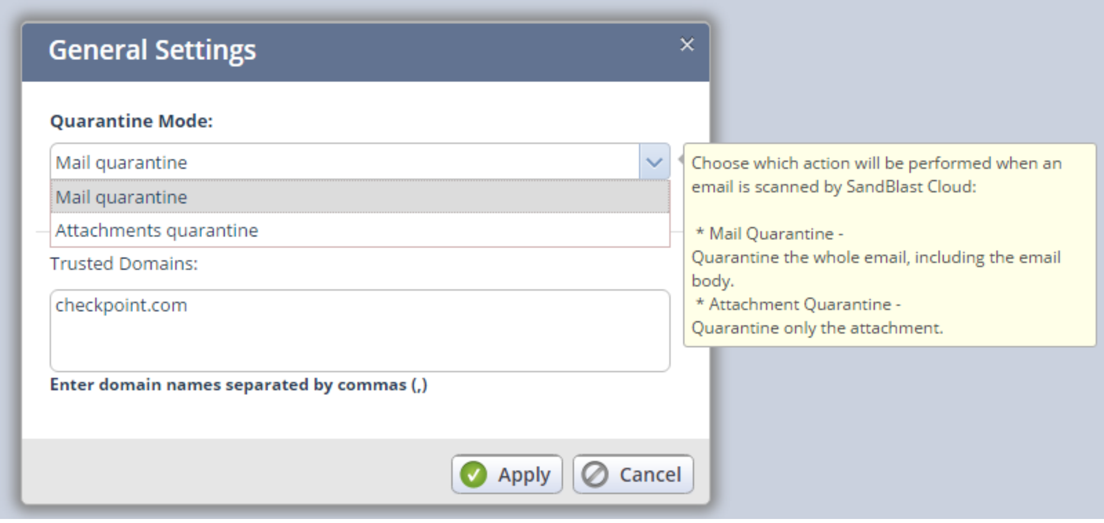
In this window we select what action you would like SandBlast Cloud to perform on the specified rule.

Next, click on the ‘General Settings’ button at the top



No.	Email Destination	Settings
1	* All	Attachments Inspection URL Inspection

Clicking the “general Settings” button will open the following window:



Quarantine Mode:

Mail quarantine

Mail quarantine

Attachments quarantine

Trusted Domains:

checkpoint.com

Enter domain names separated by commas (,)

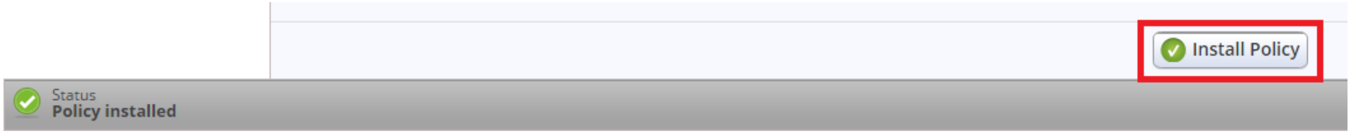
Choose which action will be performed when an email is scanned by SandBlast Cloud:

* Mail Quarantine - Quarantine the whole email, including the email body.
* Attachment Quarantine - Quarantine only the attachment.

This window will allow you to configure Mail flow method and trusted sender domains:

- **Mail flow method**: this selection allows us to configure how we want the mail to flow through the user’s inbox and what contents are going to be held in quarantine until the verdict has been reached by the emulation.
- **Trusted Sender Domains**: Any emails originating from domains listed in this box will not be held and scanned. Here we input the organization’s own internal domain so that internal emails will not need to go through inspection, resulting in a quicker and better user experience for internal emails. According to our statistics, about 80% of emails received by users are internal emails. We can select more than one domain to include other domains we are confident are trusted, or in the event the organization has more than one domain in their emails.

To apply the policy that was configured, click the Install Policy button at the bottom of the screen.
Please note that changes won’t be applied until policy is installed.

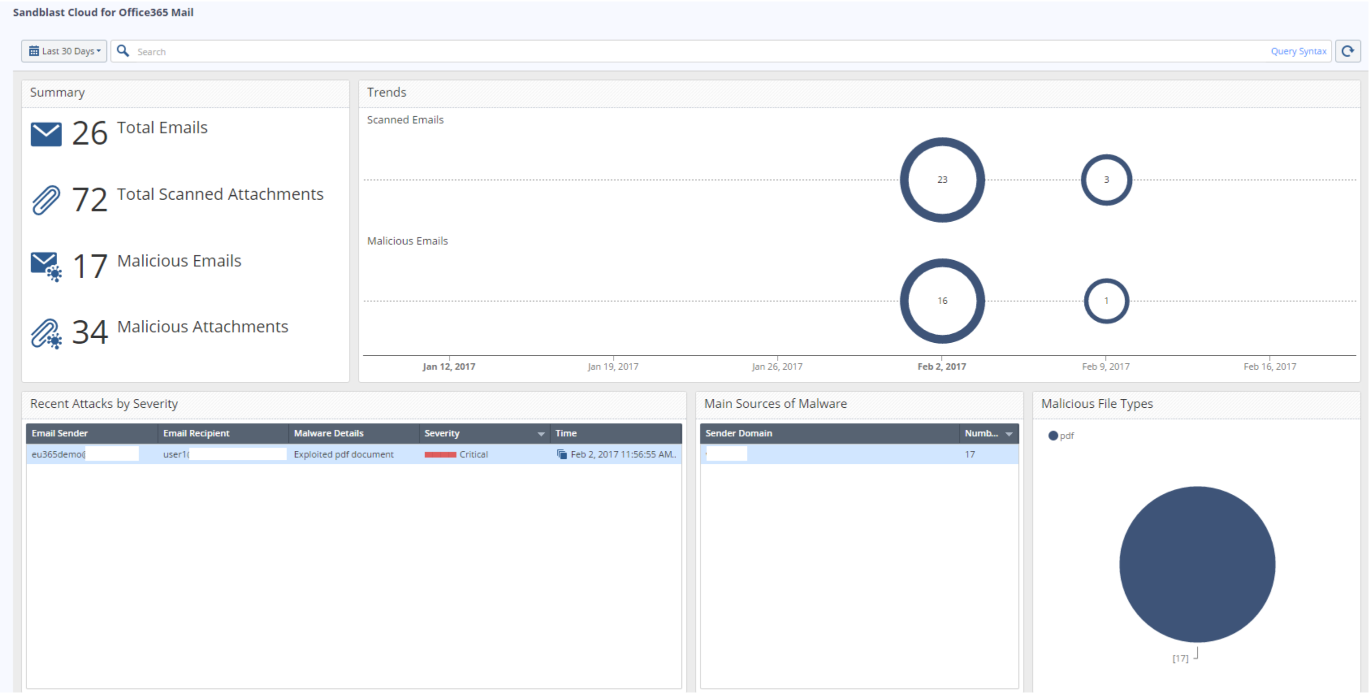


Status
Policy installed

Please wait until the indicator on the bottom left corner shows that the policy is installed.

Overview

The Overview tab shows a summary of the scanned activity.
On the top left corner of the tab you can choose what timeframe you would like the data to show. You can choose any timeframe ranging from Last Hour to Last 30 days. You can also select a Date



Sandblast Cloud for Office365 Mail

Summary

26 Total Emails

72 Total Scanned Attachments

17 Malicious Emails

34 Malicious Attachments

Recent Attacks by Severity

Email Sender	Email Recipient	Malware Details	Severity	Time
eu365demo@[redacted]	user1[redacted]	Exploited pdf document	🟥 Critical	Feb 2, 2017 11:56:55 AM..

Main Sources of Malware

Sender Domain	Numb...
[redacted]	17

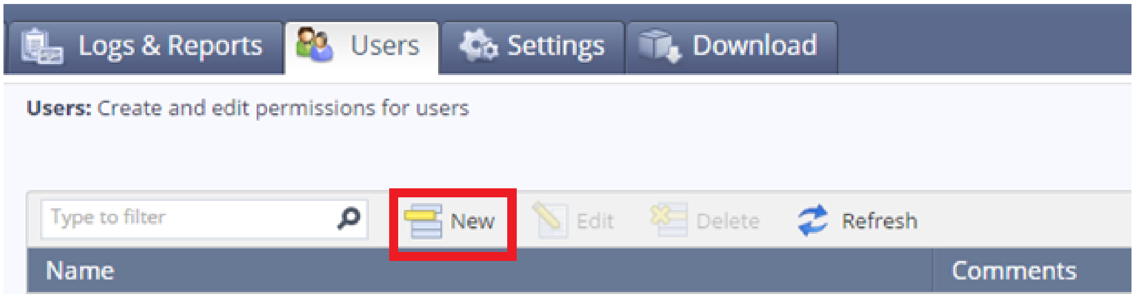
In this screen we can see a brief summary showing the amount of Emails & attachments that were scanned (Total Emails & Scanned Attachments) as well as how many of them were found to be Malicious (Malicious Emails & Malicious Attachments).
We also see a timeline for the trends, as well as Recent Attacks by Severity, Main Sources of Malware, and Malicious File Types.

Users

Users are people who can sign into the Sandblast Cloud portal and perform administrative tasks.
There are two kinds of user accounts available:

- Admin
- Help Desk Admin

Admin can modify and enter any function available in the cloud portal.
Help Desk Admin can access the Overview, Logs & Reports, Users, and Download tabs. They do not have access to the Policy or the Settings tabs.



Users: Create and edit permissions for users

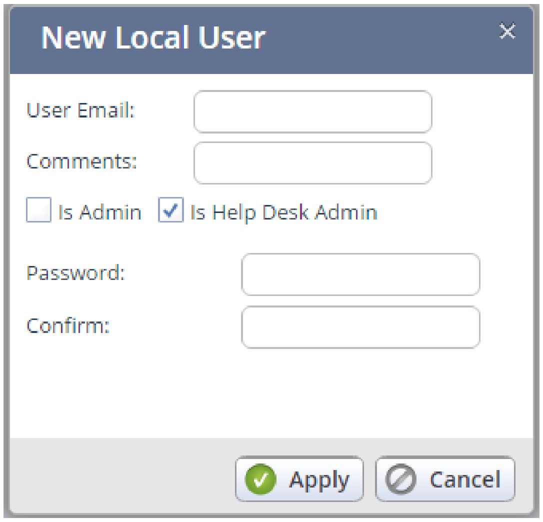
Go to the Users tab.

To create a new user:

1. Click New.

2. The New Local User window opens.
   a. Enter the user’s email address
   b. Optional: Enter related comments
   c. Select Is Admin if the user is a Sandblast Cloud Portal administrator
   d. Select Is Help Desk Admin if the user is a technical support administrator
   e. Set a password for the administrator account and enter it again to confirm

3. Click Apply.



User Email:

Comments:

☐ Is Admin ☑ Is Help Desk Admin

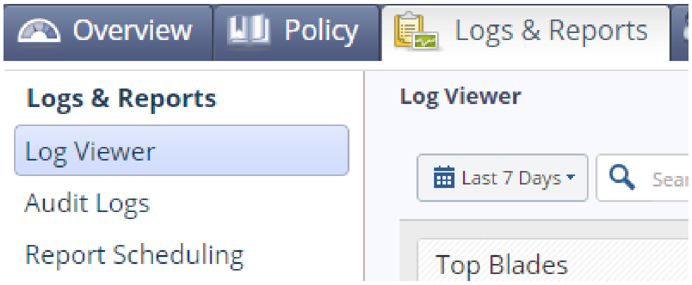
Password:

Confirm:

Logs & Reports

The **Logs and Reports** tab contains:

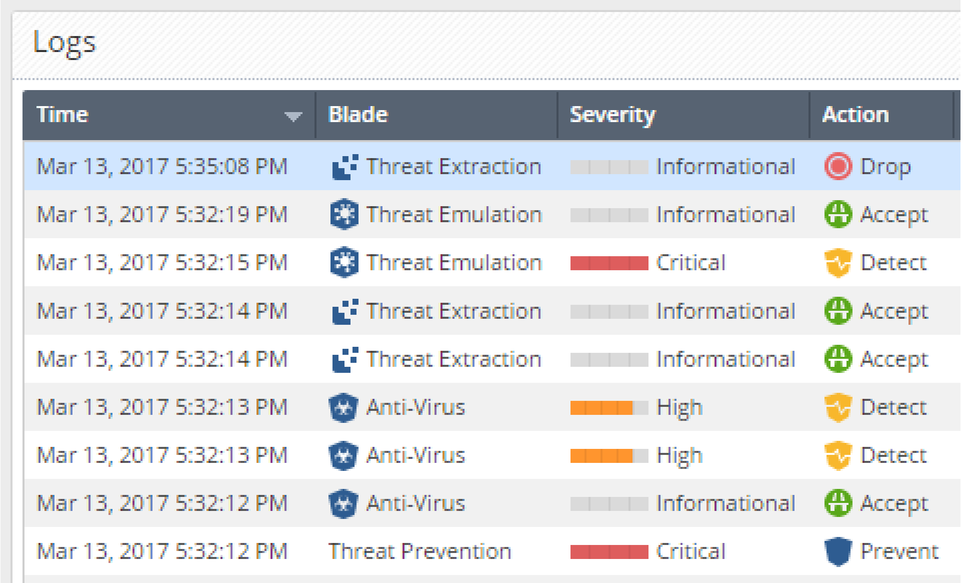
- **Log Viewer** – Logs for user activities.
- **Audit Logs** – Logs for activities on the Sandblast Cloud Portal.
- **Report Scheduling** – Schedule Threat Prevention and Sandblast for Office365 Mail reports.



The **Log Viewer** page shows all the email logs for incoming mail activity. Currently, you will find 4 types of logs:

- **Threat Prevention**:
  - One log for every e-mail that has been scanned.
    This can be considered as the "master" log for the email as the action that is shown here is the action that was done on the email.
- **Threat Emulation**:
  - One log for every scanned attachment
- **Threat Extraction**:
  - One log for every extracted attachment
  - One log for every restoration attempt:
    - Action: Allow --> Email restoration successful – benign content
    - Action: Drop --> Email restoration denied – malicious content found
- **Anti-Virus**:
  - You will see one log for every scanned attachment
  - You will see logs for the URL inspection of the subject & the body of the email. In the event of a clickable link, you will see an additional log

The screenshot below refers to an email that was sent with two attachments (one malicious & one benign) and & malicious link within the body of the email.



Logs

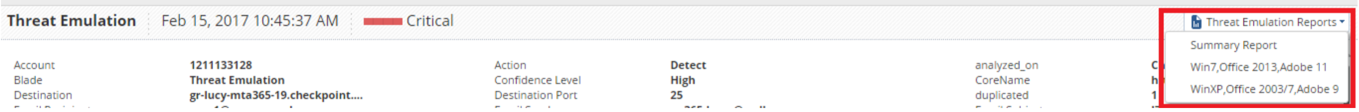
Time	Blade	Severity	Action
Mar 13, 2017 5:35:08 PM	Threat Extraction	Informational	Drop
Mar 13, 2017 5:32:19 PM	Threat Emulation	Informational	Accept
Mar 13, 2017 5:32:15 PM	Threat Emulation	Critical	Detect
Mar 13, 2017 5:32:14 PM	Threat Extraction	Informational	Accept
Mar 13, 2017 5:32:14 PM	Threat Extraction	Informational	Accept
Mar 13, 2017 5:32:13 PM	Anti-Virus	High	Detect
Mar 13, 2017 5:32:13 PM	Anti-Virus	High	Detect
Mar 13, 2017 5:32:12 PM	Anti-Virus	Informational	Accept
Mar 13, 2017 5:32:12 PM	Threat Prevention	Critical	Prevent

By seeing the **Threat Prevention** log, we can see that a **Prevent** action was done on the email. We also see:

- **Threat Emulation** logs
  - One log for the benign attachment (**Accept** action) & one log for the malicious attachment (**Detect** action)
- **Threat Extraction** logs
  - One log for each extracted attachment (**Accept** action) generated regardless of the verdict.
  - One log for the restoration request which was denied due to malicious content (**Drop** action)
- **Anti-Virus** logs
  - One log for the benign attachment (**Accept** action) & one log for the malicious attachment (**Detect** action)
  - URL inspection conducted in the subject and in the body of the email, as well as an additional log in the event that there is a clickable link (no malicious URL = **Accept** action & malicious URL = **Detect** action)

Threat Emulation Report:

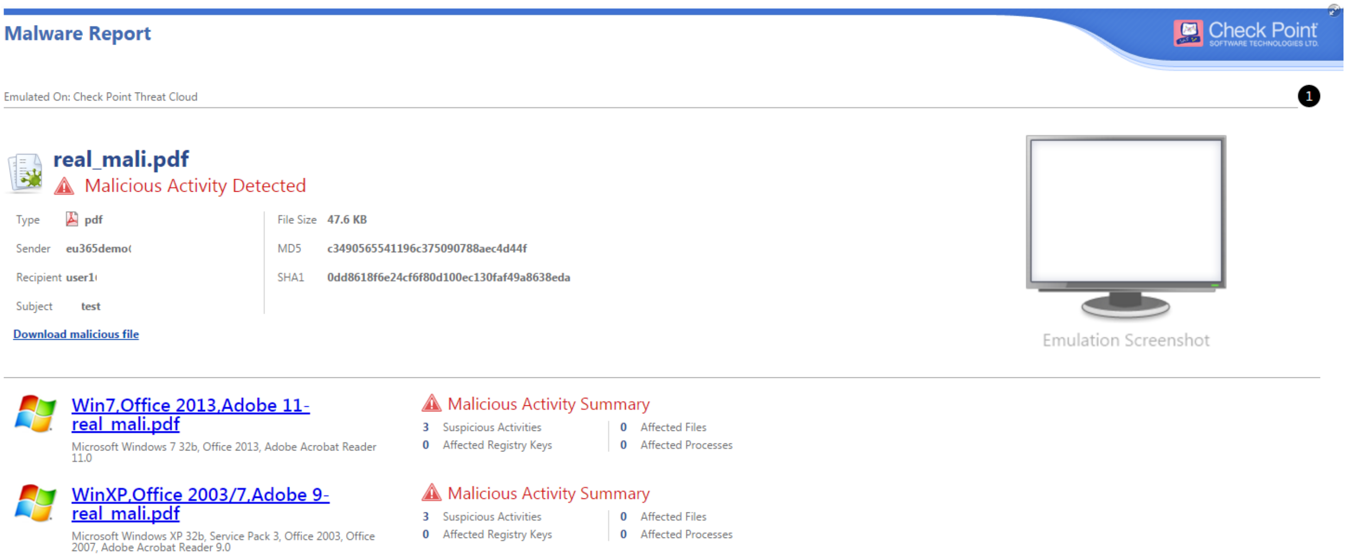
Clicking on the Threat Emulation log specific to a malicious attachment will show an option to open a Threat Emulation Report on the top-right corner of the log card. Clicking on the Threat Emulation Reports button will show a drop down dialog where you can choose a Summary Report or an Operating System specific report.



Threat Emulation Feb 15, 2017 10:45:37 AM Critical

Account	1211133128	Action	Detect	analyzed_on	C
Blade	Threat Emulation	Confidence Level	High	CoreName	h
Destination	gr-lucy-mta365-19.checkpoint....	Destination Port	25	duplicated	1

After clicking on the **Summary Report**, we will see the following pop-up screen:



Malware Report

Emulated On: Check Point Threat Cloud

real_mali.pdf

Malicious Activity Detected

Type	pdf	File Size	47.6 KB
Sender	eu365demo(	MD5	c3490565541196c375090788aec4d44f
Recipient	user1(	SHA1	0dd8618f6e24cf6f80d100ec130faf49a8638eda
Subject	test		

Download malicious file

Win7,Office 2013,Adobe 11-real_mali.pdf
Microsoft Windows 7 32b, Office 2013, Adobe Acrobat Reader 11.0

Malicious Activity Summary
3 Suspicious Activities | 0 Affected Files
0 Affected Registry Keys | 0 Affected Processes

WinXP,Office 2003/7,Adobe 9-real_mali.pdf
Microsoft Windows XP 32b, Service Pack 3, Office 2003, Office 2007, Adobe Acrobat Reader 9.0

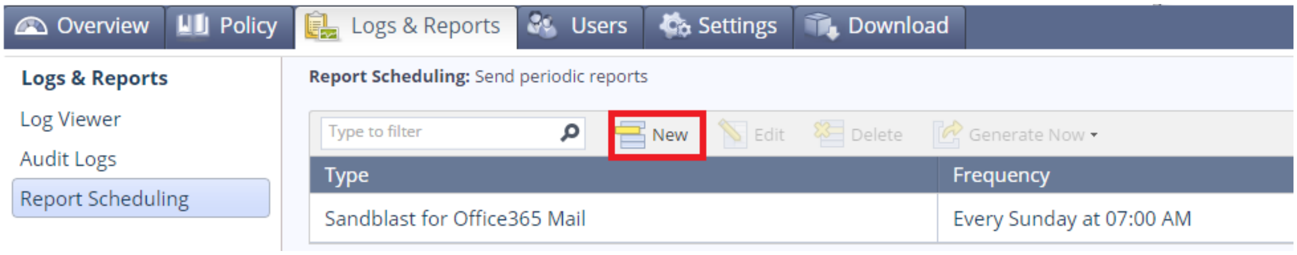
Malicious Activity Summary
3 Suspicious Activities | 0 Affected Files
0 Affected Registry Keys | 0 Affected Processes

NOTE: Windows XP and Windows 7 are the only two operating systems available for emulation at the moment. This may change in the future.

NOTE: In the event of a false-positive for an attachment, the admin can obtain the original file (downloaded locally to the computer) by clicking on the link “Download malicious file” located below the email information. <u>CAUTION</u>: Proceed with the download at your own risk and only if you are sure it is a false positive.

Scheduling Reports

On the Report Scheduling page, you can configure periodic reports on Threat Prevention activity and Sandblast for Cloud – Office 365 activity. The Threat Prevention report will show a more generic report based on Threats and Malware. The Sandblast for Cloud report will show a much more specific report custom tailored to Email. This report will highlight: Number of Scanned emails, Malicious Emails, Attacker locations, Targets, Files, and malware used.
It is recommended you use the Sandblast for Cloud report and not the Threat Prevention report.

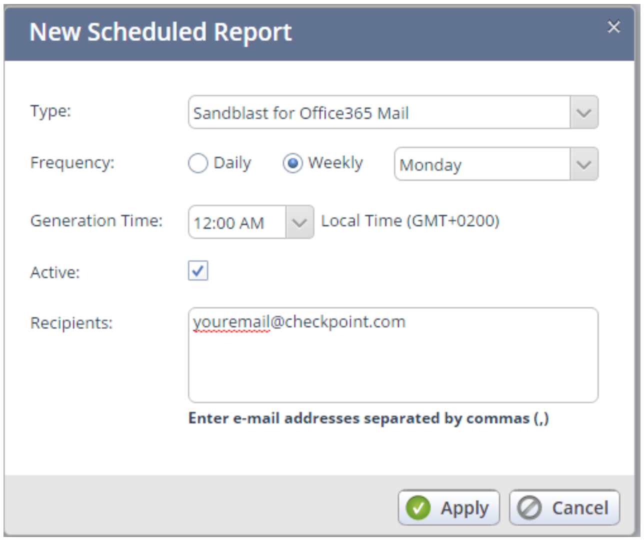


Report Scheduling: Send periodic reports

Type	Frequency
Sandblast for Office365 Mail	Every Sunday at 07:00 AM

To Schedule reports:

1. On the Report Scheduling page, click New.
2. Select the type of report:
   a. Threat Prevention
   b. Sandblast for Office365 Mail (Recommended!)
3. Select Frequency and scope:
   a. Daily (default) – to collect data for the last 24-hours, up to the time of report generation.
   b. Weekly, select day of the week – to collect data for the week prior to the specified day of the week, and up to the time of report generation.
4. Select Generation Time in your local time zone, on the hour.
5. Enter report Recipients – email addresses, separated by commas.
6. Make sure Active is selected if you want to start generating reports as scheduled, or cleared if you want to save the report settings, but not generate the reports.
7. Click Apply



New Scheduled Report

Type: Sandblast for Office365 Mail

Frequency: ○ Daily ● Weekly Monday

Generation Time: 12:00 AM Local Time (GMT+0200)

Active: ☑

Recipients: youremail@checkpoint.com

Enter e-mail addresses separated by commas (,)

You can also delete or edit reports by selecting the relevant report and hitting the appropriate button. On-demand reports can also be generated by selecting the appropriate report and hitting the on-demand button. You can specify the period for which you want to generate the report: Last 24 hours, or Last 7 days.

If you have any questions, issues or feedback please contact your Check Point representative or Jonathan Zelman (SandBlast POC Manager) at jonathanze@checkpoint.com