

# Quick Deployment Guide

Trend Micro Cloud App Security



# Contents

Purpose.....	3
Deployment.....	3
Provision CAS to Protect O365 .....	3
Provision CAS to Protect Box, Dropbox And Google Drive .....	4
Provision CAS to Protect Gmail .....	7
Key to Success .....	11
Configure ATP Polices.....	12
Configure Advanced Spam Protection.....	13
Malware Scanning.....	15
File Blocking .....	15
Web Reputation.....	16
Virtual Analyzer.....	17
Displaying Detection Results.....	18
Perform a Manual Scan.....	18
Check the Manual Scan Result.....	19
Dashboard View.....	19
<b>Manage the widgets to show CAS's detections</b> .....	19
Overall Threat Detections.....	20
Log Console.....	20
Export the Logs.....	21
Generate the Report.....	22
Switch the Log View.....	22
Appendix .....	23
TMCAS Related Documentations .....	23
CAS BP .....	23
CAS WR BP.....	23
CAS POC Guide .....	23
CAS L3 .....	23
Apply for a Trial Account.....	23

# Purpose

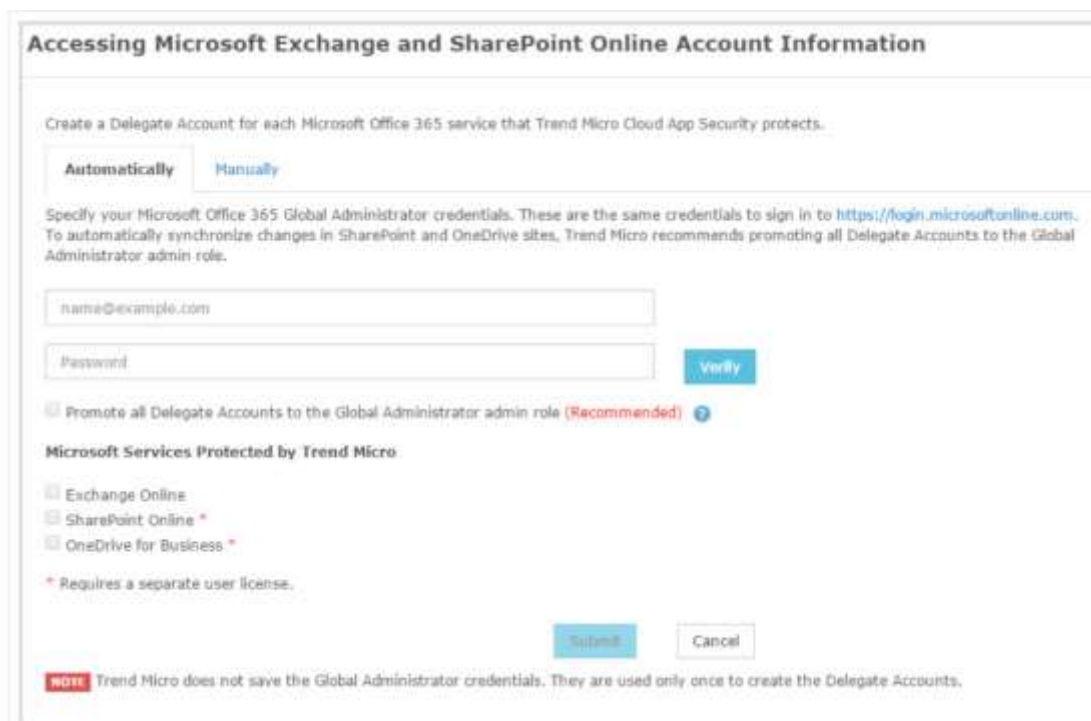
This document is to guide TrendMicro SE and Solution Architect team run a successful Cloud App Security POC with prospective customers. It is an internal use document.

# Deployment

## Provision CAS to Protect O365

It is **RECOMMENDED** to use the [Automatically Provisioning Delegate Accounts](#), because this is very easy.

**NOTE** 📄 We suggest that the customer use a testing environment to run a POC first. Afterwards, we can contact the backend team to help move this account to production environment.



**Accessing Microsoft Exchange and SharePoint Online Account Information**

Create a Delegate Account for each Microsoft Office 365 service that Trend Micro Cloud App Security protects.

**Automatically** **Manually**

Specify your Microsoft Office 365 Global Administrator credentials. These are the same credentials to sign in to <https://login.microsoftonline.com>. To automatically synchronize changes in SharePoint and OneDrive sites, Trend Micro recommends promoting all Delegate Accounts to the Global Administrator admin role.

☐ Promote all Delegate Accounts to the Global Administrator admin role (Recommended) ?

**Microsoft Services Protected by Trend Micro**

☐ Exchange Online

☐ SharePoint Online \*

☐ OneDrive for Business \*

\* Requires a separate user license.

**NOTE** Trend Micro does not save the Global Administrator credentials. They are used only once to create the Delegate Accounts.

For customers who have the security concerns when adding O365 global admin on CAS console, please suggest them to use manually provision.

- [Manually Provisioning an Exchange Online Delegate Account](#)
- [Manually Provisioning a SharePoint Online Delegate Account](#)

**NOTE** 📄 Before starting the provisioning process, follow this [KB1119059](#) to make sure that Control access, from apps that don't use modern authentication, is correctly set on the Office 365 admin center.

## Provision CAS to Protect Box, Dropbox And Google Drive

- [Before Provisioning](#), please make sure that:
  - ✓ You have the administrator's credentials for your cloud application, for example, Box.
  - ✓ You have not logged on to the cloud application using any other user account.
- [Provisioning a Service Account for Box](#) Provision a service account for Box to allow Cloud App Security to scan files stored in Box.
- [Provisioning a Service Account for Dropbox](#) Provision a service account for Dropbox to allow Cloud App Security to scan files stored in Dropbox.

**NOTE** 📄 Dropbox provision needs extra steps to input the team admin account for the provision.



**Provision Service Account for Dropbox**

✓ Step 1: Provide your Dropbox administrator credentials. [Click here](#)

Step 2: Specify the administrator email address you used in Step 1.

Step 3: [Click Done](#)

- [Provisioning a Service Account for Google Drive](#) Provision a service account for Google Drive to allow Cloud App Security to scan files stored in Google Drive

## How to Verify Provision Status

To evaluate the current provision status:

- **Automatic Exchange Online Provision with the delegate account**

During the automatic Exchange Online provision, two statuses display under Task, which will indicate the backend progress:

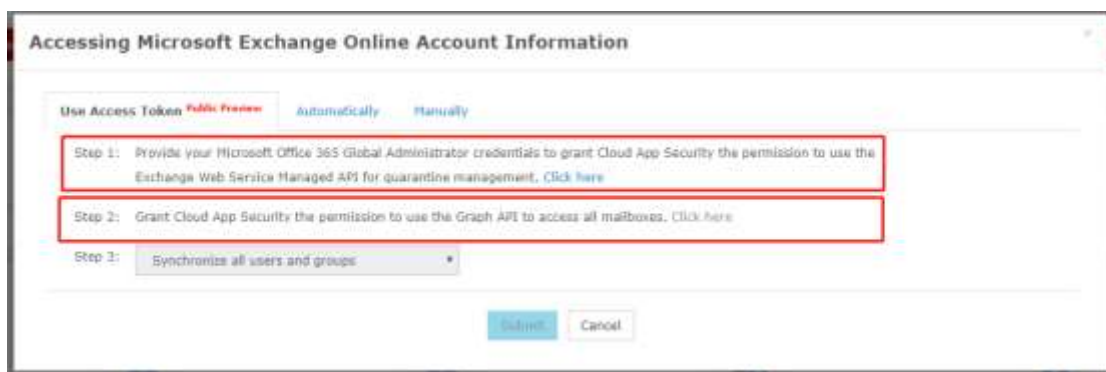
- Creating a delegate account
- Updating users and groups

“Creating the delegate account” means that CAS is creating a delegate account for the customer. Normally it does not take too long, no longer than 30 minutes. If this status keeps pending for more than 30 minutes, there should be something wrong in CAS.

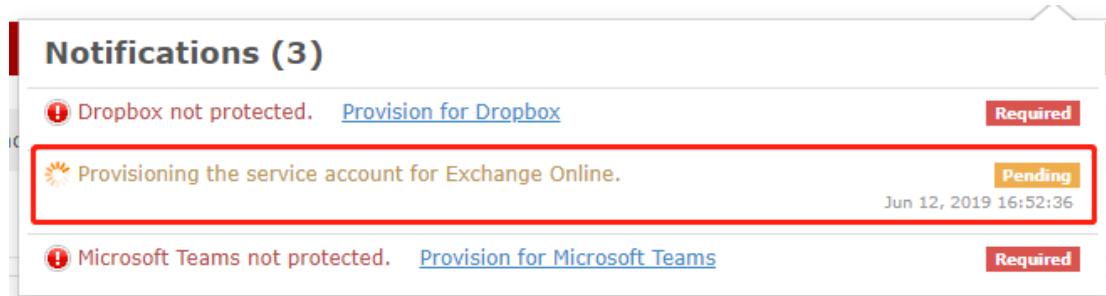
“Updating users and groups” means that CAS is synchronizing the users and groups from the customer’s Office 365. The time required will depend on the scale of the O365 tenant. An estimated time will show for this task, like “this may take about xxx minutes”. If the status is “pending” and keeps for a long time, for example over 30 minutes, there should be something wrong with this synchronization task. If the task status is running but for much more time than the estimated time, for example over 10 hours, there should be something wrong in CAS.

- **Exchange Online Provision with an access token**

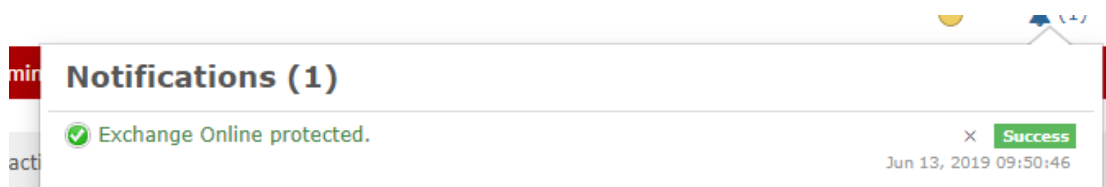
Exchange Online provision using an access token includes three steps, two of which are to grant required permission for the O365 Graph API and EWS API, and the other is to synchronize all users and groups.



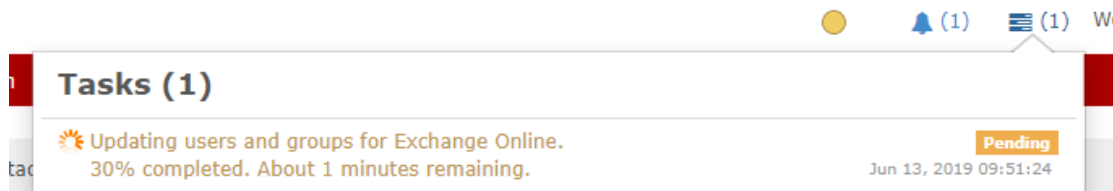
- Step 1:** After this step is done, the status of “Provisioning the service account for Exchange Online” displayed under Notifications is Pending. This step takes only a few seconds. If it lasts for more than one minute, there must be something wrong with this task.

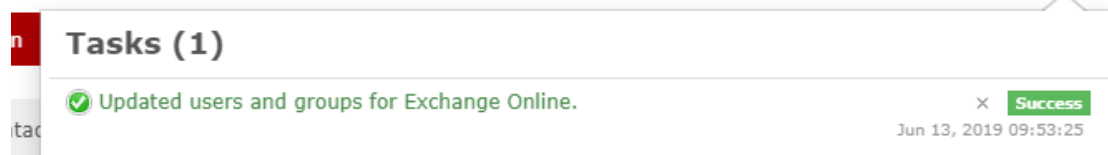


- Step 2:** After this step is done, the status of “Exchange Online protected” displayed under Notifications will indicate that the backend progress is successful. This step takes only a few seconds. If it lasts for more than one minute, there must be something wrong.



- Step 3:** CAS synchronizes users and groups from the customer’s Office 365. The time required will depend on the scale of the O365 tenant. An estimated time will show for this task, like “Update users and groups for Exchange Online. \*\* completed, About \*\* remaining”. If the status is “pending” and keeps for a long time, for example over 30 minutes, there should be something wrong with this synchronization task. If the task status is running but for much more time than the estimated time, for example over 10 hours, there should be something wrong in CAS.





- Automatic SharePoint/OneDrive Provision with the delegate account

During the automatic SharePoint/OneDrive provision, two statuses display under Task, which will indicate the backend progress:

- Creating a delegate account
- Updating SharePoint Online site collections and subsites
- Updating OneDrive for Business users and groups

“Creating the delegate account” means that CAS is creating a delegate account for the customer. Normally it does not take too long, no longer than 30 minutes. If this status keeps pending for more than 30 minutes, there should be something wrong in CAS.

Updating SharePoint Online site collections and subsites”and“updating OneDrive for Business users and groups” mean that CAS is synchronizing the SharePoint/OneDrive sites from the customer’s Office 365. The time required will depend on the scale of the O365 tenant. An estimated time will show for this task, like “this may take about xxx minutes”. If the status is “pending” without estimation time displayed and keeps for a long time, for example over 30 minutes, there should be something wrong with this synchronization task. If the task status is running but for much more time than the estimated time, for example over 10 hours for a company whose size is less than 10,000 users, there should be something wrong in CAS.

## Provision CAS to Protect Gmail

- Before Provisioning, please make sure that:
  - ✓ You have the administrator's credentials for G Suite.
  - ✓ You have not logged on to G Suite using any other user account.
- [Provisioning a Service Account for Gmail](#) Provision a service account for Gmail to allow Cloud App Security to scan emails in Gmail.

## How to Verify Provision Status

After the Gmail App installed, Admin can confirm the following settings:

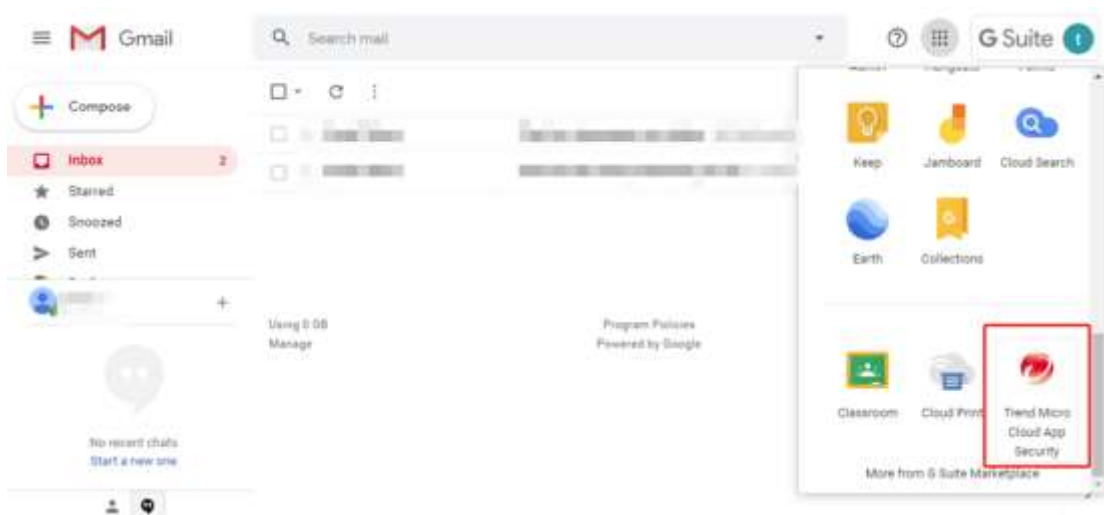
1. Make sure necessary access privileges are granted to CAS in the G Suite admin console: **Apps > Marketplace apps and locate Trend Micro Cloud App Security**. Make sure the Data access section status is “Granted”.




2. Access the Google admin App page to ensure that the CAS App enabled for all uses.




3. Check whether the provisioned user has CAS App.



- 
- Google Admin
- api setting
- Home
  - Dashboard
  - Directory
  - Devices
  - Apps
  - Security
  - Reporting
  - Billing
  - Account
- Alert center
- Security rules
- Settings

- 
- The screenshot shows the Google Admin console interface. At the top, the 'Google Admin' header is visible with a search bar containing 'api setting'. Below the header, the 'Security' section is expanded. Under 'Security', the 'API Permissions' section is visible. Within 'API Permissions', the 'G Suite' category is selected. A table lists the permissions, with 'Gmail' highlighted by a red rectangle. The 'Gmail' row shows the permission is 'Enabled' (indicated by a selected radio button), and it is granted to '1 app, 1 user'. Other permissions like 'Calendar' and 'Contacts' are also listed but not highlighted.
- | API access    | G Suite  |
|---------------|--|
| Gmail         | <input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">all Access</a> |
| 1 app, 1 user |  |
| Calendar      | <input type="radio"/> Enable <input type="radio"/> Disable <a href="#">all Access</a>            |
| Contacts      | <input type="radio"/> Enable <input type="radio"/> Disable <a href="#">all Access</a>            |

- 
- The screenshot shows the Google Admin console interface. At the top, there's a blue header with the Google Admin logo and a search bar. Below the header, the breadcrumb navigation shows 'Security > API Permissions'. There are two tabs: 'INSTALLED' (selected) and 'TRUSTED'. A table lists the installed applications. The first application is 'Trend Micro Cloud App Security'. The 'Permissions' column for this application shows 'Gmail: Drive, Admin', with a red box highlighting the 'Gmail' part.
- | Filters                 | App Name                       | App ID   | App Type        | Permissions         | Users |
|-------------------------|--------------------------------|--|-----------------|---------------------|-------|
| API Permission<br>Gmail | Trend Micro Cloud App Security | 21106683316-d4e33ed957f64a4f72d6f11app.googleusercontent.com | Web Application | Gmail: Drive, Admin | 1     |



During the Gmail provision, one status display under Task, which will indicate the backend progress:

- Updating Gmail users and groups

Updating Gmail users and groups means that CAS is synchronizing the mailboxes and groups from the customer's G Suite organization. The time required will depend on the scale of the G Suite organization. If the task status is running but for much more time than 2 hours for a company whose size is less than 10,000 users, there should be something wrong in CAS.



# Key to Success

The key to success is how to maximize Cloud App Security protection. Below product settings are strongly recommended during POC testing.

- Enable most of the Cloud App Security features (such as: advanced spam prevention, malware scanning etc.)
- After new user is created, suggest to firstly click the “click here” to sync new users before testing
- In the case when mailbox migration from on-prem to cloud, a manual cloud mailbox scan is needed.
- After done the RMS protection provision, go to the policy to enable the RMS protection.

Customers will **NOT** take risks when enabling more testing users or more protections during POC, due to its architecture advantage—Cloud App Security have **“Zero”** impact to customer’s mail, SharePoint/OneDrive and Box/Dropbox/Google Drive flow.

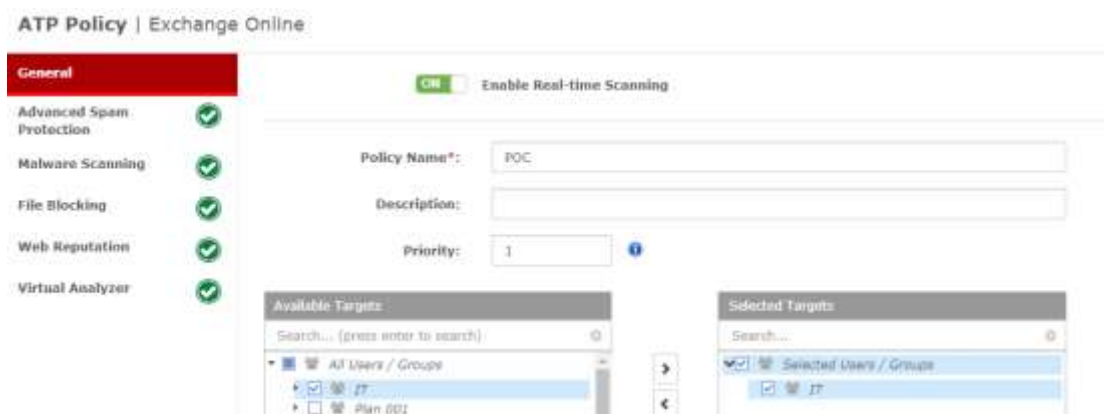
# Configure ATP Policies

We suggest our customer to create a new policy for the specific targets, instead of using the default policy.

- ✓ Create a new policy.



- ✓ Select the specific targets.



**NOTE** In order to run a successful POC, we suggest our customer selecting the target group which can contains several hundred **users**. **It's NOT RECOMMENDED** select only individual users for POC customers.

## Configure Advanced Spam Protection

- ✓ Apply the Rules to the **<All messages>**.

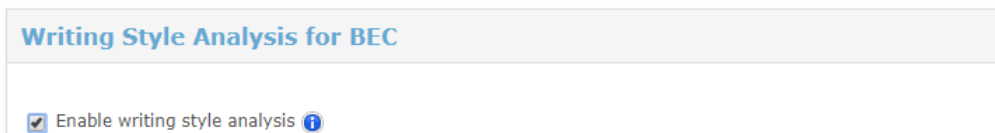


**Rules**

Apply to: All messages ⓘ

Detection Level: ☒ High Detects the most spam with a greater chance of false positives  
☐ Medium Detects a high rate of spam with a moderate chance of false positives  
☐ Low Detects obvious spam with the lowest chance of false positives

- ✓ [Enable the Writing Style Analysis](#)

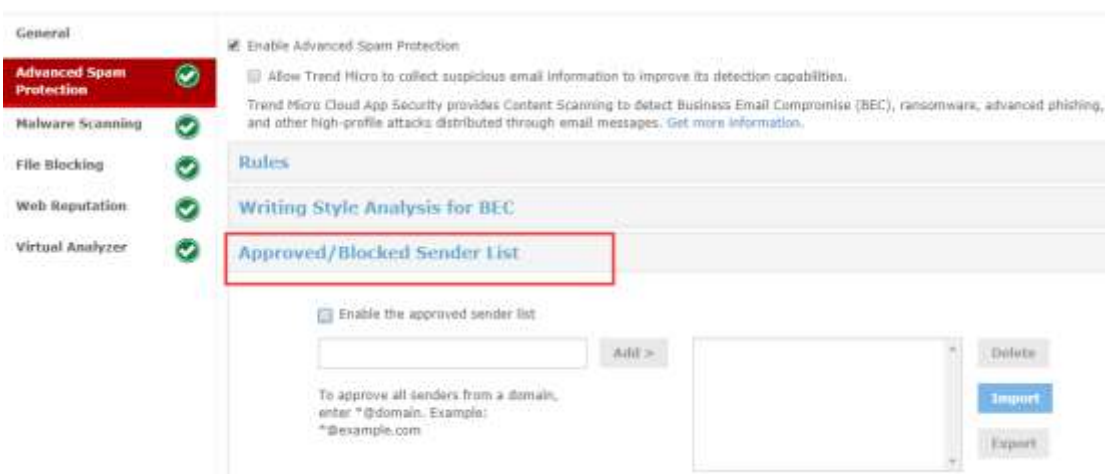


**Writing Style Analysis for BEC**

☒ Enable writing style analysis ⓘ

NOTE ⓘ Please click [HERE](#) to get the writing style BP.

- ✓ In order to reduce the FP, we suggest the customer to add the trust sender into CAS Approved Sender List.



**General**

☒ Enable Advanced Spam Protection

☐ Allow Trend Micro to collect suspicious email information to improve its detection capabilities.

Trend Micro Cloud App Security provides Content Scanning to detect Business Email Compromise (BEC), ransomware, advanced phishing, and other high-profile attacks distributed through email messages. [Get more information.](#)

**Rules**

**Writing Style Analysis for BEC**

**Approved/Blocked Sender List**

☒ Enable the approved sender list

Add >

To approve all senders from a domain, enter \*@domain. Example: \*@example.com

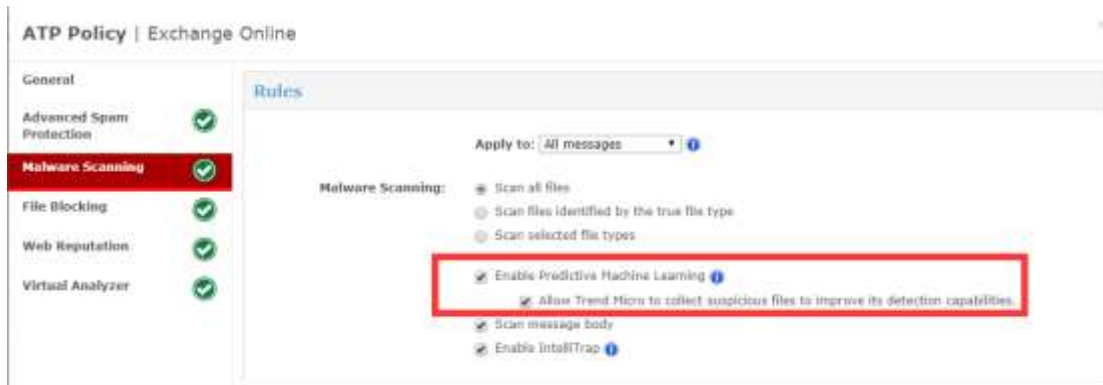
Delete Import Export




## Malware Scanning

Setup a malware policy to detect malicious files, which uses the virus scan engine to detect emerging threats. User can set a scan for all file types, and enable all of Trend Micro's technology.

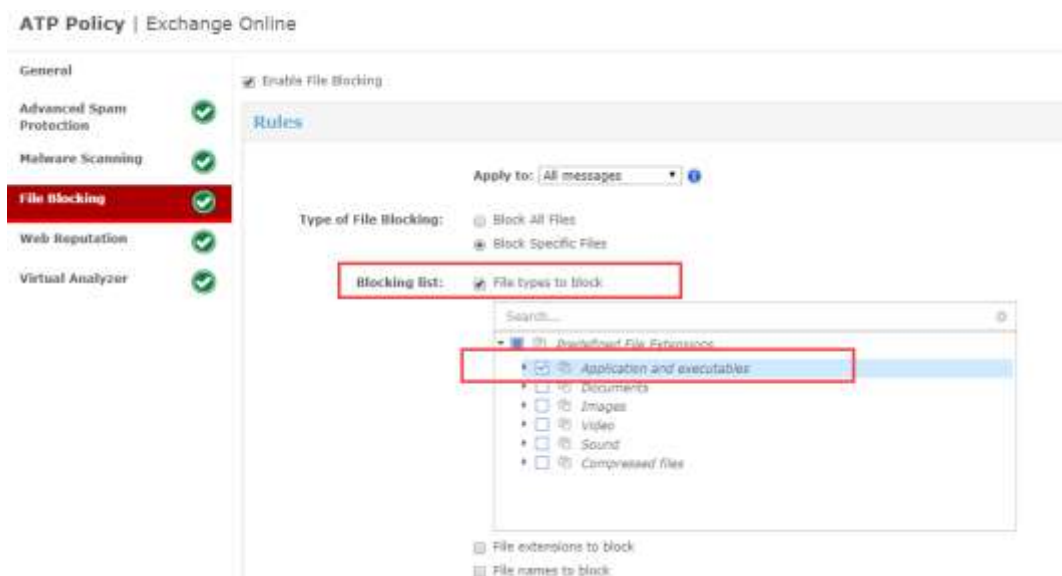
Click [HERE](#) to get testing sample.



NOTE  Predictive Machine Learning is disabled by default.

## File Blocking

Setup a File Blocking policy to block according to the file type.

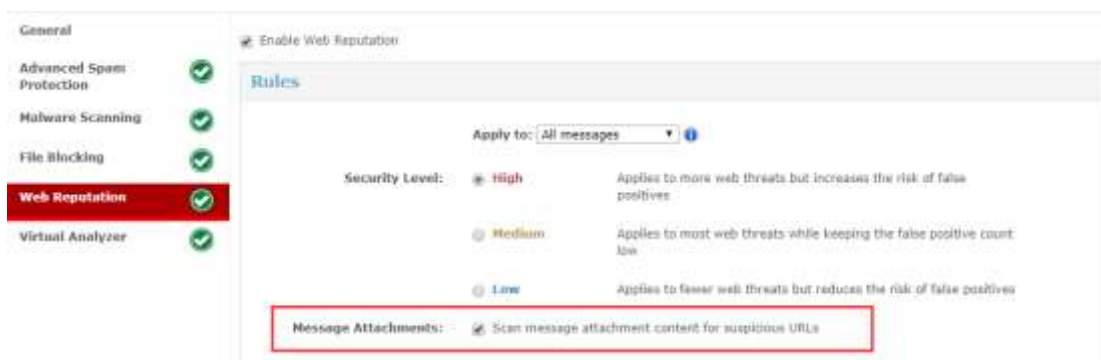


NOTE 

Normally, we'd like to suggest the customer blocking exe files, but this depends on the customer's company's specific security policy.

## Web Reputation

Setup a web reputation policy to detect the bad URLs. (Especially, we have a ability to detect the **O365 credential phishing URL**.)

NOTE 

“scan message attachment for suspicious URLs” is disabled by default, we suggest our customer enabling it for POC purpose.

It's also highly recommended the customer add “internal domains to the approved URL List”.





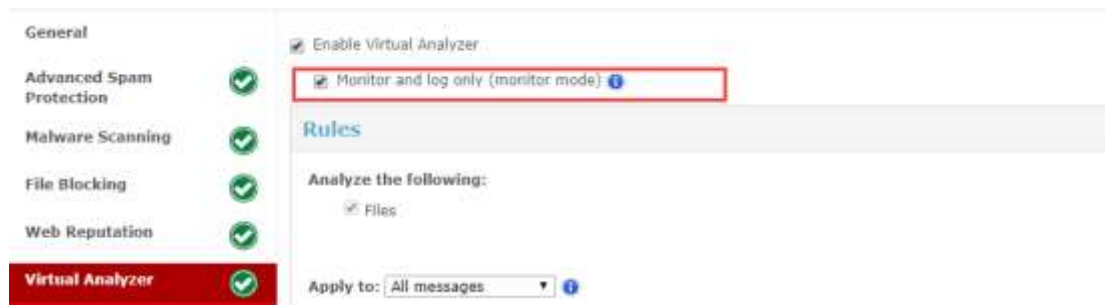
## Virtual Analyzer

Setup a virtual analyzer policy to test sand boxing capability. A cloud-based virtual environment designed for analyzing suspicious files.

Click [HERE](#) to get testing sample.

**NOTE**

In order to make our customer understand this feature better, we suggest the customer to use monitor mode first. In this mode, CAS's VA feature will only record the VA detection result, but will not take any action.



# Displaying Detection Results

## Perform a Manual Scan

Running a manual scan performs an on-demand scan of targets based on the selected policy configuration. It can detect the potential threat before the customer uses CAS.



Then there will be new pop-up window:

**Manual Scan For Advanced Threat Protection**
×

---

**Selected Policy for Manual Scan**

Policy Name	Type	Targets	Rules	Scan Details
POC	Exchange Online	All Users	AS, Q, E, WR, VA	Estimated time required: 30 minutes

Showing 1 to 1 of 1 entries

**Scan Type**

☒ Scan and protect  
☐ Scan only ⓘ

**Scope:**

☐ Scan recently: 1 day(s)  
☒ Scan between: Sep 01, 2018 and Sep 07, 2018

**Report Recipients**

☒ POC@trendmicro.com

**Note** Manual scan does not include Virtual Analyzer scanning.

Scan Now
Cancel

- ✓ Customer can refer to the **Scan Result** to see how long the manual scan will take.
- ✓ Add **Report Recipient** then this users can receive the notification when the manually scan is finished
- ✓ If the customer wants more detection, you might need run the manual scan for more users
- ✓ For trail account, it only supports select the scan scope for 1 day.
- ✓ Manual Scan does not contain the Virtual Analyzer scanning.

## Check the Manual Scan Result

Click the scan history to get the manual scan result.

➔ Show details

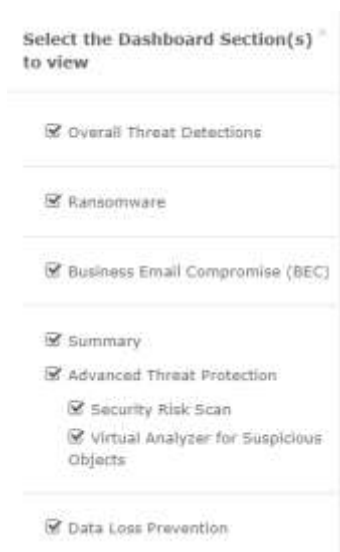


## Dashboard View


### Manage the widgets to show CAS's detections

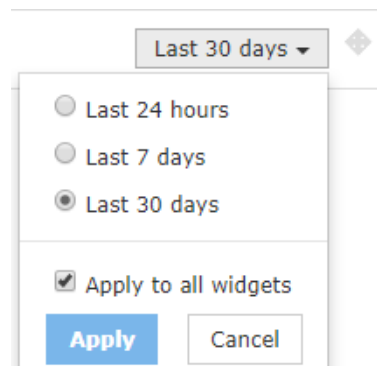


Then, please select all:



Threat Type	Count
Suspicious Messages and Virus Scanned	635
IOC	9
Missing	16
Fingerprint	2
Malicious File	2
Malicious URL	38


NOTE  Select the right time range for the detection result that will be displayed on dashboard.  
( you can select “Apply to all widgets”).




## Log Console

On CAS console, the user is provided with a place to view the scan logs that are collected from different CAS server roles and detections.

The screenshot shows the Cisco Talos Threat Intelligence Center (TIC) interface. The 'Logs' tab is selected in the top navigation bar. On the left, the 'Security Risk Score' filter is highlighted with a red box. The main table displays a list of threats with columns: Threat Name, Risk Score, Severity, Security Filter, Security Risk Name, Detected by, and Risk Level. The table shows various threats detected by Cisco Talos, including 'Exchange Online', 'SharePoint Online', and 'Exchange Online', with risk scores ranging from 10 to 100. The 'Security Risk Score' filter is set to '100'.

NOTE  Select the right time range for the detection result on log view console.

 Select Date Range ▾

Default: all dates

Last 24 hours

Last 1 week

Last 1 month

Date Range

« September 2018


« September 2018



Su	Mo	Tu	We	Th	Fr	Sa
26	27	28	29	30	31	1
2	3	4	5	6	7	8

Su	Mo	Tu	We	Th	Fr	Sa
26	27	28	29	30	31	1
2	3	4	5	6	7	8

## Export the Logs

Prevention Anomaly Detection **Logs** Quarantine Administration

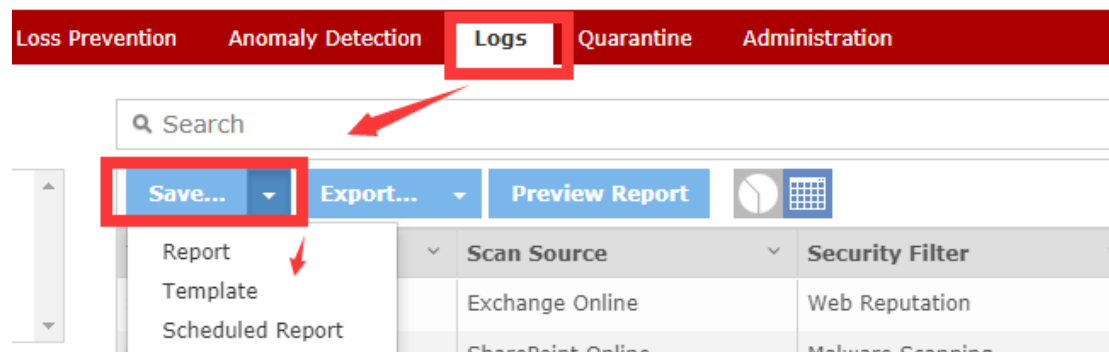
 Search

Save... ▾ Export... ▾ Preview Report  

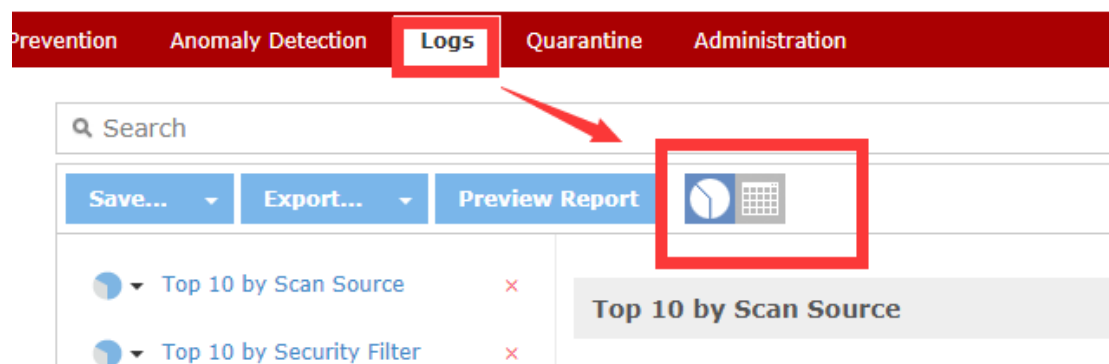
Timestamp ▾ Current View All Records ⓘ Source ▾ Security Filter

Sep 05, 2018 17 Online Web Reputation

## Generate the Report



## Switch the Log View





# Appendix

## TMCAS Related Documentations

[CAS BP](#)

[CAS WR BP](#)


[CAS POC Guide](#)

[CAS L3](#)

## Apply for a Trial Account

Go to Cloud App Security Console to Apply a Trial Account

- For EU customers/partners go to <https://admin-eu.tmcas.trendmicro.com/#!/>
- For JP customers/partners go to <https://admin.tmcas.trendmicro.co.jp/#!/>
- Other region customers/partners go to <https://admin.tmcas.trendmicro.com/#!/>

NOTE  CAS trial license will expire within 2 months. You can contact product team to extend trial license.



Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit [www.trendmicro.com](http://www.trendmicro.com).

©2018 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and Smart Protection Network are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.