

Trend Micro Cloud App Security





### Contents

Purpose	4
Deployment	4
Provision CAS to Protect Exchange Online	4
Provision CAS to Protect SharePoint, OneDrive, and Teams	5
Provision CAS to Protect Box, Dropbox and Google Drive	8
Provision CAS to protect Salesforce Production or/and Salesforce Sandbox	9
How to Verify Provision Status	
For Office365 services	
For Gmail	
For Salesforce	22
Key to Success	23
Configure ATP Polices	23
Configure Advanced Spam Protection	24
Malware Scanning	26
File Blocking	27
Web Reputation	28
Virtual Analyzer	29
Displaying Detection Results	
Perform a Manual Scan	
Check the Manual Scan Result	
Dashboard View	
Manage the widgets to show CAS's detections	
Overall Threat Detections	
Log Console	
Export the Logs	
Generate the Report	34
Switch the Log View	34
Appendix	35
TMCAS Related Documentations	

Page 3 of 35 | Trend Micro CAS Best Practice Guide



# Purpose

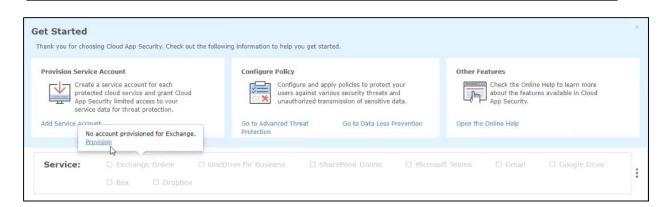
This document serves as a guideline to help customers develop a set of best practices when provisioning and managing Cloud App Security (TMCAS).

# Deployment

# **Provision CAS to Protect Exchange Online**

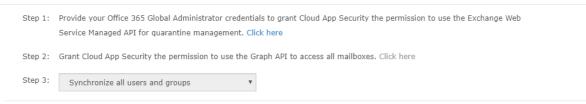
To Provision, hover the mouse to the Exchange Online service in the Dashboard of CAS console and click Provision.

# **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.



#### Follow the Steps in Provisioning CAS to protect Exchange Online:

#### **Provision Service Account for Exchange Online**

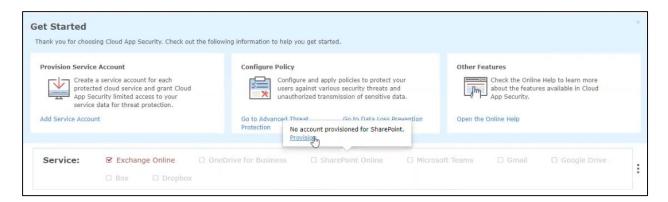




# Provision CAS to Protect SharePoint, OneDrive, and Teams

To Provision, hover the mouse to the SharePoint/OneDrive/Teams service in the Dashboard of CAS console and click Provision.

#### For SharePoint:



#### **Provision Service Account for SharePoint Online**

Authorize	d Account	Delegate Account	Delegate Account (Manually)		
Step 1:	Grant Cloud	App Security the permis	sion to use the Graph API to access all domains. Click here		
Step 2:	Grant Cloud App Security the permission to obtain all SharePoint site collections. Click here				
Step 3:	Grant Cloud App Security the permission to access resources in all SharePoint sites. Click here				
Step 4:	Follow the instructions to grant Cloud App Security permissions to receive notifications from Microsoft for real-time scanning on your SharePoint sites. Learn more.				
			Submit Cancel		

It is **VERY IMPORTANT** to do the instructions in Step 4 by clicking "Learn More" for CAS to receive any file changes notification from Microsoft for Real-time Scanning on your SharePoint sites.

For OneDrive:



Thank you for choo	sing Cloud App Security. Check	k out the following information to help you o	get started.		
Provision Servic	ce Account	Configure Policy		Other Features	
protect App S	e a service account for each ted cloud service and grant Clo ecurity limited access to your te data for threat protection.	oud users again	and apply policies to protect your nst various security threats and red transmission of sensitive data. Go to Data Loss Prevention	Check the Online Help to learn more about the features available in Cloud App Security.	
Add Service Accor	unt	No account provisioned for OneDrive.	GO TO DATA LOSS Prevenuon	open the Unline Help	
Service:	☑ Exchange Online	OneDrive for Business	SharePoint Online     Micros	oft Teams 🛛 Gmail 🔹 Google Drive	:

#### **Provision Service Account for OneDrive**

Authorize	d Account			
Step 1:	Grant Cloud App Security the permission to use the Graph API to access all domains, users and groups. Click here			
Step 2:	Grant Cloud App Security the permission to access resources in all OneDrive sites. Click here			
Step 3:	Step 3: Follow the instructions to grant Cloud App Security permissions to receive notifications from Microsoft for real-time scanning or your OneDrive sites. Learn more.			
	Submit Cancel			

It is **VERY IMPORTANT** to do the instructions in Step 3 by clicking "Learn More" for CAS to receive any file changes notification from Microsoft for Real-time Scanning on your OneDrive sites.

#### For Teams:

NOTE Currently, Cloud App Security scans and protects only files stored on a SharePoint team site.

Provision Service Account Create a service account for each protected cloud service and grant Cloud App Security limited access to your		ply policies to protect your	Other Features	
protected cloud service and grant Cloud App Security limited access to your		ly policies to protect your		
service data for threat protection.	users against value	ous security threats and smission of sensitive data.	Check the Online Help to learn more about the features available in Cloud App Security.	
Add Service Account	Go to Advanced Threat Protection	Go to Data Loss Prevention No account provision Provision	Onen the Online Help oned for Microsoft Teams	



Done

#### **Provision Service Account for Microsoft Teams**

Step 1:	Provide your Office 365 Global Administrator credentials for Cloud App Security to get permissions on teams in your organization. Click here
Step 2:	Grant Cloud App Security the permission to access all site collections of the protected teams. Click here
Step 3:	Follow the instructions to grant Cloud App Security permissions to receive notifications from Microsoft for real-time scanning on your teams. Learn more.
Step 4:	Click Done

It is **VERY IMPORTANT** to do the instructions in Step 3 by clicking "Learn More" for CAS to receive any file changes notification from Microsoft for Real-time Scanning on your Teams sites.

Since Microsoft Teams sites are basically located in SharePoint, CAS Policy scanning priority for Microsoft Teams and SharePoint Sites are as follows:

#### Teams policy > SharePoint policy

Microsoft Teams Support Scope:

CAS only scans uploaded files in Microsoft Teams site.

Conversati	ons Files Wiki Home 🕂
, to	October 30, 2018
JZ	0/24/18 1:28 PM @all
	JZ Hello
	$\leftarrow$ Reply

# **NOTE** Currently, Cloud App Security can only do Real-Time scanning for Microsoft Teams and running Manual Scan is not an option.

Page 7 of 35 | Trend Micro CAS Best Practice Guide



# 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.
- <u>Provisioning a Service Account for Gmail</u> Provision a service account for Gmail to allow Cloud App Security to scan emails in Gmail.

# Provision CAS to Protect Box, Dropbox and Google Drive

- <u>Before Provisioning</u>, please make sure that:
  - ✓ You have the administrator's credentials for your cloud application, for example, Box.
  - $\checkmark$  You have not logged on to the cloud application using any other user account.
- <u>Provisioning a Service Account for Box</u> Provision a service account for Box to allow Cloud App Security to scan files stored in Box.
- <u>Provisioning a Service Account for Dropbox</u> 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.

Provisio	n 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.
	name@example.com
Step 3:	Click Done

• <u>Provisioning a Service Account for Google Drive</u> Provision a service account for Google Drive to allow Cloud App Security to scan files stored in Google Drive



# Provision CAS to protect Salesforce Production or/and Salesforce Sandbox

- Before Provisioning, please make sure that:
  - ✓ You have a valid Cloud App Security for Salesforce license.
  - ✓ You have purchased the Salesforce environment with a license that supports RESTful APIs.
  - ✓ You have the administrator's credentials for your Salesforce environment.
  - ✓ You have not logged on to your Salesforce environment using any other user account.

To Provision, hover the mouse to Salesforce Production in the Dashboard of CAS console and click Provision.

Dashboard	Advanced Threat Protection	Data Loss Prevention	Logs	Quarantine	Administration	
				No account p	rovisioned for Salesforce Production.	
Service:	🗹 Exchange Online	OneDrive		Provision		🗆 Gmail
	🗆 Box 🔹 Drop	obox 🗆 Salesfo	rce Sandt	oox 🛛	Salesforce Production	

Follow the Steps in Provision Service Account for Salesforce Production:

### **Provision Service Account for Salesforce Production**

- Step 1: Click here to install the TrendMicro Cloud App Security app.
- Step 2: Grant Cloud App Security the permissions to access and manage the Salesforce user data in your organization. Click here
- Step 3: Click Done

**Note:** In the preview period, you can try this feature with your current valid Cloud App Security license. After it is officially announced, a separate license is required to continue the protection of your Salesforce environment.

Done

It is **VERY IMPORTANT** to finish the instructions in Step 1 before Step 2. Please do NOT skip Step 1 even if you are doing re-provision.

Page 9 of 35 | Trend Micro CAS Best Practice Guide



Login to Salesforce with the administrator's credential. Please note that the administrator will not be protected by CAS. You may want to create a dedicated Salesforce administrator account only used to do administrative tasks.

salesf	orce
To access this page, you have to lo	og in to Salesforce.
Username	
Password	
Log In to Sa	ndbox
Remember me	



When prompted to install TrendMicro Cloud App Security, make sure to install the APP for All Users.

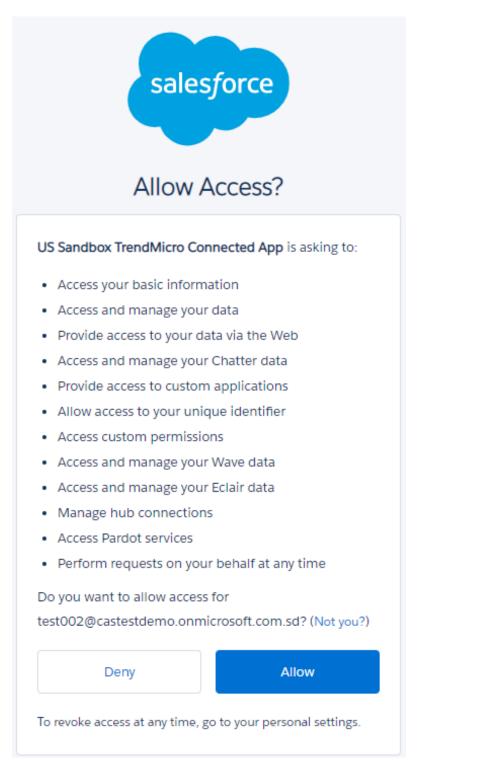
By TrendMicr		ro Cloud App Sed	curity
Install for Adn	nins Only	O Install for All Users	Install for Specific Profiles
App Name	Publisher	Version Name	Version Number
TrendMicro Cloud App Security	TrendMicro	Spring 2021	1.3
Additional Details Viev	v Components		

If you are doing re-provision, you will be prompted to Upgrade the App, please also choose "Install for All Users" option and click on Upgrade button.

Upgrad By TrendMice		licro Cloud App S	ecurity
	r version is instal Spring 2021 (1.3)	lled. It can be upgraded while p New Version: Spring 2021 (1.3)	preserving the existing data.
Install for Adr	mins Only	Install for All Users	Install for Specific Profiles
			<b>Upgrade</b> Cancel
App Name	Publisher	Version Name	Version Number
FrendMicro Cloud App Security	TrendMicro	Spring 2021	1.3
dditional Details View	w Components		



In Step 2, please also make sure to use the same administrator as used in Step 1 to grant the permission.





# How to Verify Provision Status

### For Office<sub>365</sub> services

To evaluate the current provision status for Office365 services:

• Exchange Online Provision with Authorized Account (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:	Provide your Office 365 Global Administrator credentials to grant Cloud App Security the permission to use the Exchange Web	
	Service Managed API for quarantine management. Click here	
Step 2:	Grant Cloud App Security the permission to use the Graph API to access all mailboxes. Click here	
Step 3:	Synchronize all users and groups	
visio	n Service Account for Exchange Online	
Step 1:	n Service Account for Exchange Online Provide your Office 365 Global Administrator credentials to grant Cloud App Security the permission to use the Exchange Web	
	Provide your Office 365 Global Administrator credentials to grant Cloud App Security the permission to use the Exchange Web	

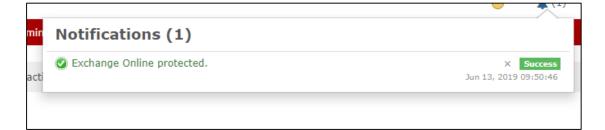
Step 1: After Step 1 is done, the status of "Provisioning the service account for Exchange Online" displayed under Notifications is Pending. This step takes only a few seconds. If it lasts for more than one minute, there must be something wrong.

Hover the mouse to this icon  $\checkmark$  in the top-right corner, notification list will show up like below

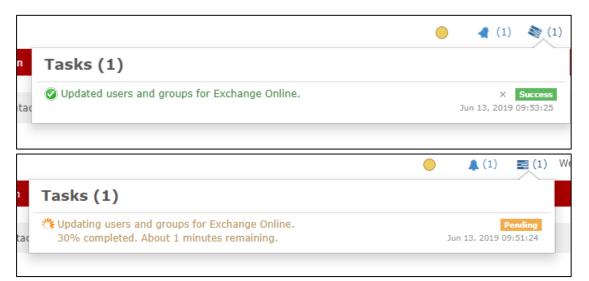


Notifications (3)	
Dropbox not protected. <u>Provision for Dropbox</u>	Required
Provisioning the service account for Exchange Online.	<b>Pending</b> Jun 12, 2019 16:52:36
Microsoft Teams not protected. <u>Provision for Microsoft Teams</u>	Required

**Step 2:** After Step 2 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.





#### • SharePoint, OneDrive and Teams with Authorized Account

Verifying SharePoint, OneDrive and Teams provision status with Authorized Account (access token) is similar to Exchange Online provision with Authorized Account.

The provision status can be found by hovering the mouse to Tasks icon and Notifications icon

#### **Provision Service Account for SharePoint Online**

Authorize	d Account Delegate Account (Manually)						
Step 1:	Grant Cloud App Security the permission to use the Graph API to access all domains. Click here						
Step 2:	Grant Cloud App Security the permission to obtain all SharePoint site collections. Click here						
Step 3: Grant Cloud App Security the permission to access resources in all SharePoint sites. Click here							
Step 4:	Follow the instructions to grant Cloud App Security permissions to receive notifications from Microsoft for real-time scanning on your SharePoint sites. Learn more.						
	Successfully assigned an App Id: 537280f3-2b40-47e5-8f96-c263c601106a. Copy it for use in this step.						
ovision S	Submit Cancel						
ovision S	ervice Account for OneDrive						
	ervice Account for OneDrive						
Authorize	d Account						
Authorize	d Account Grant Cloud App Security the permission to use the Graph API to access all domains, users and groups. Click here						
Authorize	Account for OneDrive						



**Provision Service Account for Microsoft Teams** 

Oreated access token for SharePoint Online.

Oreated access token for OneDrive.

Opdated OneDrive user profiles.

Opdated SharePoint Online site collections and subsites.

Step 1:	Provide your Office 365 Global Administrator credentials for Cloud App Security to get permissions or organization. Click here	n teams in your	
Step 2:	Grant Cloud App Security the permission to access all site collections of the protected teams. Click he	ere	
Step 3:	Follow the instructions to grant Cloud App Security permissions to receive notifications from Microsof scanning on your teams. Learn more.	t for real-time	
	Successfully assigned an App Id: 08439efd-62b5-4e3d-9a5d-74f61990f6d5. Copy it for use in	this step.	
Step 4:	Click Done		
			Done
		)	5) 🔳 (7)
Task	s (7)	. (5	5) 📑 (7)
_	s (7) ted users and groups for Exchange Online.	×	
🖉 Upda		X Jan 27, 20; X	< Success 21 11:27:58
🕑 Upda 🔮 Upda	ted users and groups for Exchange Online.	X Jan 27, 20 X Jan 27, 20 X	<ul> <li>Success</li> <li>21 11:27:58</li> <li>Success</li> <li>21 14:33:10</li> <li>Success</li> </ul>
🕑 Upda 🔮 Upda	ted users and groups for Exchange Online. ted data for Microsoft Teams.	X Jan 27, 20 X Jan 27, 20 X	< Success 21 11:27:58 < Success 21 14:33:10

Page 16 of 35 | Trend Micro CAS Best Practice Guide



X Success Jan 27, 2021 11:24:16

X Success Jan 27, 2021 11:25:44

X Success Jan 27, 2021 14:28:52

X Success Jan 27, 2021 14:31:20



Notifications (5)	
SharePoint Online protected.	X Success
	Jan 27, 2021 11:25:3
OneDrive protected.	× Succes
	Jan 27, 2021 14:31:2
Create an account for Azure Rights Management (Azure RMS) protected file scanning.	X Optiona
S Exchange Online protected.	× Succes
	Jan 27, 2021 11:27:5
Microsoft Teams protected.	× Succes
	Jan 27, 2021 14:33:0

Confirm if you have successfully granted Cloud App Security permissions to receive notifications from Microsoft upon any change to the files on your SharePoint sites, for SharePoint, OneDrive and/or Teams.

In the SharePoint admin hidden page

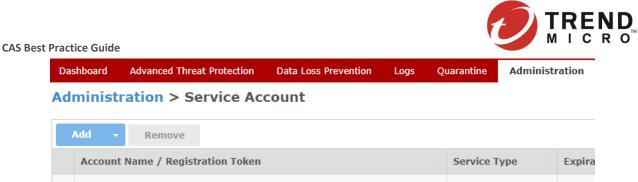
{sharepoint\_admin\_site}/\_layouts/15/TA\_AllAppPrincipals.aspx, an App with corresponding App Identifier should appear for SharePoint, OneDrive and/or Teams :

$\rightarrow$	→ C 🗈 https://====-admin.sharepoint.com/_layouts/15/TA_AllAppPrincipals.aspx					x			τô	0	€≦				
4	(m, r)	Contract of the second	2.00	Stee Set	<ul> <li>A series</li> </ul>	4.4	<b>e</b> 9	${\rm Spin}_{\rm c}$	Sec. 1	Annual Mitchell Spills	$h_{\rm c}$ (e)		$\sim 1.5$	10	8-0

#### Apps

Find app principal by identifier:	٩	
	App Display Name	App Identifier
×	Common Data Service	i:0i.t[ms.sp.ext]00000007-0000-0000-0000000000000@1fd0b080-43c8-4cee-8951-fc07e63f2b17
×	Office 365 Exchange Online	i:0i.t ms.sp.ext 00000002-0000-0ff1-ce00-00000000000@1fd0b080-43c8-4cee-8951-fc07e63f2b17
×	Trend Micro Cloud App Security	i:0i.t ms.sp.ex <mark>1</mark> 9d65d44d-5adc-4bf5-8cbf-c92a98e87069 <mark></mark> 91fd0b080-43c8-4cee-8951-fc07e63f2b17
×	Trend Micro Cloud App Security	i:0i.t[ms.sp.ext <mark>[537280f3-2b40-47e5-8f96-c263c601106ab</mark> 1fd0b080-43c8-4cee-8951-fc07e63f2b17
×	Trend Micro Cloud App Security	i:0i.t ms.sp.ex <mark>f08439efd-62b5-4e3d-9a5d-74f61990f6d5</mark> p1fd0b080-43c8-4cee-8951-fc07e63f2b17

The App Id can be found from CAS Administration > Service Account list:



Presentation and Array and	Exchange Online	N/A
App Id: 537280f3-2b40-47e5-8f96-c263c601106a	SharePoint Online	N/A
App Id: 9d65d44d-5adc-4bf5-8cbf-c92a98e87069	OneDrive	N/A
App Id 08439efd-62b5-4e3d-9a5d-74f61990f6d5	Microsoft Teams	N/A

In case any of the Apps doesn't exist in the SharePoint admin hidden page, you may find the guidance from the following online help pages to add the App:

- o <u>SharePoint</u> Step 11
- o <u>OneDrive</u> Step 9
- o <u>Microsoft Teams</u> Step 9

#### • 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
- o Updating SharePoint Online site collections and subsites
- o 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.



### For Gmail

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".

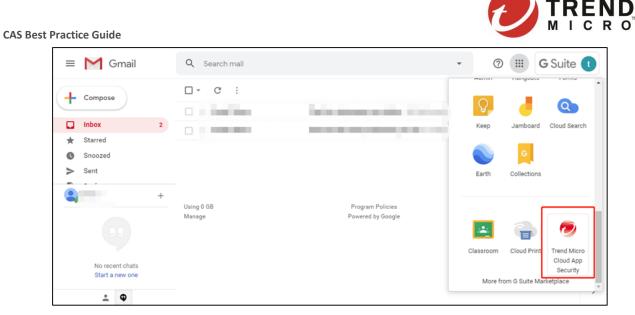
	► EDIT SERVICE Trend Micro Cloud App ON for everyone http://docs.trendmicro.com/en-us/enterprise/cloud-app-security-online-help/about-cloud-app-secu.aspx
<ul> <li>Data acce</li> </ul>	ss
Granted This applicatio	Revoke data access n is allowed to access specific data in your domain via the following APIs: Learn more

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

← →		bgle.com/test.trendmicro.com/AdminHome?N=en-us#AppsListserviceType=MARKETPLACE ) 部電公記平台 📑 Trend Internal 📑 Web Server 📑 Git Hub Project 📑 Study 📑 Tools 📑 preinterview 📑 Kafka 📑 AdminLTE 📑 Crack 🚦	SaaS	☆ G Suite	0	C (
	Google Admin	Q Search for users, groups, and settings (e.g. migrate emails)	8	?		M
Apps	> Marketplace apps			+	Ŧ	:
	Services	Status 🔺				
۲	Trend Micro Cloud App Secur Trend Micro Cloud App Secur	ty provides advanced data and threat protection for Google Drive and Gmail. On for everyone				:

3. Check whether the provisioned user has CAS App.





4. Check Google Admin page about the advanced G Suite API setting. On the Google Admin console, go to **Security** > **Settings**.

Goo	o <mark>gle</mark> Admin	api setting	
ħ	Home		
	Dashboard		
•	Directory	+	
	Devices	<b>&gt;</b>	
	Apps	•	
0	Security	•	Alert center
ıĿ	Reporting		Security rules
	Billing		Settings
0	Account	•	

5. Refer to the <u>G Suite Admin help article</u> to enable API access, then check the apps for Gmail.



≡ Goog	le Admin	Q api setting				×	8	?	
Security									:
^	API Permission	S							
	API access	G Suite							
		Gmail	Enable	O Disable	All Access		-		
		1 app, 1 user							_
			<u> </u>	<u> </u>					

6. Ensure Trend Micro Cloud App Security has permission for Gmail.

$\equiv$ Google	Admin	Q	api setting		×	8	?		
Security > API P	ermissions								:
INSTALLED	TRUSTED								
Filters			App Name	App Id	Арр Туре	Permissions		Users 🔻	
API Permission Gmail		~	Trend Micro Cloud App Security	211086893919- dsr33Jodp57f6lsmilgmeihaf72vbg1t.apps.googleusercontr	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

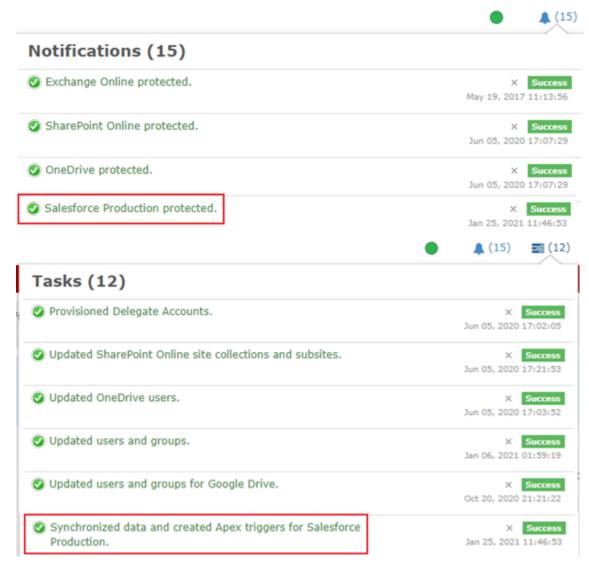
Updating Gmail users and groups means that CAS is synchronizing the mailboxes and groups from the customer's G Suite organization. The time required will depend on the scale of the G Suite organization. If the task status is running but for much more time than 2 hours for a company whose size is less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





### For Salesforce

• The provision status can be found by hovering the mouse to Tasks icon and Notifications icon



**NOTE** Before uploading test files or inputting URLs in Salesforce to verify the provision, please make sure to login to Salesforce with a regular user rather than the administrator user, because the administrator user used to grant the permissions will NOT be protected by 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" link to sync new users before testing
- When a mailbox is newly migrated 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** have any risk when enabling more testing users or more protections during POC, due to Cloud App Security architecture advantage—Cloud App Security have "Zero" impact to customer's mail, SharePoint/OneDrive/Teams and Box/Dropbox/Google Drive/Salesforce flow.

# **Configure ATP Polices**

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

✓ Create a new policy.

Add -	Delete Copy Run Manual Scan Internal Domains	$\leftarrow Previous \ 1 \ Next \to$	Search:				
Priority O P	olicy	Targets	Rules				
Exchange Onlin	Exchange Online Policies						
1	ON POC	All Users	AS OB WR VA Scan History				

✓ Select the specific targets.





ATP Policy   Ex	change	Online				
General		ON	Enable Real-time S	canning		
Advanced Spam Protection	$\bigcirc$					
Malware Scanning		Policy Name*:	POC			
File Blocking	$\bigcirc$	Description:				
Web Reputation	$\bigcirc$	Priority:	1	0		
Virtual Analyzer	$\bigcirc$	Available Targets			Selected Targets	
		Search (press enter to search)	0		Search	0
		🔻 🔳 營 All Users / Groups	<b>^</b>	>	✓ ✓ 👻 Selected Users / Groups	
		▶ 🗹 😤 IT ▶ 🗌 😤 Plan 001		<	✓ 營 IT	

**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 <<u>All messages</u>>.

Rules		
	Apply to: All me	ssages 🔻 🕕
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
	O 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 <u>HERE</u> 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				
Advanced Spam Protection	$\bigcirc$	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,				
Malware Scanning	$\bigcirc$	and other high-profile attacks distributed through email messages. Get more information.				
File Blocking	$\bigcirc$	Rules				
Web Reputation		Writing Style Analysis for BEC				
Virtual Analyzer	$\bigcirc$	Approved/Blocked Sender List				
		Enable the approved sender list				
		Add > ^ Delete				
		To approve all senders from a domain, enter *@domain. Example: *@example.com				
		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 <u>HERE</u> to get testing sample.

ATP Policy   Ex	change (	Online		×
General		Rules		
Advanced Spam Protection			Apply to: All messages 🔹 🕡	
Malware Scanning	$\bigcirc$	Malware Scanning:	Scan all files	
File Blocking	$\bigcirc$	Harware Scanning.	<ul> <li>Scan files identified by the true file type</li> </ul>	
Web Reputation			Scan selected file types	
Virtual Analyzer	٢		<ul> <li>Enable Predictive Machine Learning ()</li> <li>Allow Trend Micro to collect suspicious files to improve its detection capabilities.</li> </ul>	
			Scan message body	

NOTE Predictive Machine Learning is disabled by default.





# File Blocking

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

ATP Policy   Exchang	e Online
General	
Advanced Spam Protection	Rules
Malware Scanning 📀	Apply to: All messages 🔻 🚺
File Blocking 🥥	Type of File Blocking: O Block All Files
Web Reputation	Block Specific Files
Virtual Analyzer 📀	Blocking list: 🕢 File types to block
	Search O
	🔻 🔳 🖓 Predefined File Extensions
	Application and executables
	▶ □ <sup>4</sup> 2 Video
	Compressed mes
	File extensions to block
L	File names to block

# **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 ability to detect the **O365 credential phishing URL**.)

General		<ul> <li>Enable Web Reputation</li> </ul>		
Advanced Spam Protection	$\bigcirc$	Rules		
Malware Scanning	$\bigcirc$		Apply to: All me	ssages 🔻 🕕
File Blocking	$\bigcirc$	Security Level:	High	Applies to more web threats but increases the risk of false
Web Reputation	$\bigcirc$			positives
Virtual Analyzer	$\bigcirc$		Medium	Applies to most web threats while keeping the false positive count low
			O Low	Applies to fewer web threats but reduces the risk of false positives
		Message Attachments:	🖉 Scan message	attachment content for suspicious URLs
		-		
NOTE 🗎		5		ous URLs" is disabled by default, we suggest our
	CUS	tomer enabling it for P	OC purpose.	

It is also highly recommended the customer add "internal domains to the approved URL List".

General		✓ Enable Web Reputation
Advanced Spam Protection	$\bigcirc$	Rules
Malware Scanning	$\bigcirc$	Approved Sender List
File Blocking	$\bigcirc$	Approved/Blocked URL List
Web Reputation	$\bigcirc$	
Virtual Analyzer	۲	<ul> <li>Enable the approved URL list</li> <li>Add internal domains to the approved URL list</li> </ul>
		Add > ^ Delete
		Import
		- Export



# Virtual Analyzer

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

#### Click <u>HERE</u> 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.

General	Enable Virtual Analyzer
Advanced Spam Protection	Monitor and log only (monitor mode) 1
Malware Scanning 📀	Rules
File Blocking	Analyze the following:
Web Reputation	Files
Virtual Analyzer 🔗	Apply to: All messages 🔻 🕕





# **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 existing before the customer deploys CAS.

Add -	Delete Copy Run Manual Scan	Internal Domains					
Priority 0	Policy		Targets				
Exchange O	Exchange Online Policies						
	ON plan 001		All Users				

Then there will be new pop-up window:

Manual Scan F	Manual Scan For Advanced Threat Protection									
Selected Policy for N	4anual Scan									
Policy Name	Туре	Targets	Rules	Scan Details						
POC	Exchange Online	All Users		Estimated time required: 30 minutes						
Showing 1 to 1 of 1	entries									
Scan Type Scan and pro Scan only () Scope: Scan recently Scan between	/: 1day(s)	and and	Sep 07, 2018							
Report Recipients          POC@trend         Note	Imicro.com es not include Virtual Analy	zer scanning.								
				Scan Now Cancel						

- $\checkmark$  The estimated completion time is shown during a scan.
- ✓ Refer to the **Scan Result** to see how long the manual scan took.
- ✓ Add **Report Recipient** to set users who will receive the notification when the manual scan is finished
- ✓ For trial account users, it allows you to select the Scope period as 1 day only. For example, you can select "Scan recently: 1 day" or Scan between Sep 01, 2018 and Sep 02, 2018.
- ✓ Manual Scan does not contain the Virtual Analyzer scanning.

Page **30** of **35**| Trend Micro CAS Best Practice Guide



## Check the Manual Scan Result

Click the scan history to get the manual scan result.

#### $\rightarrow$ Show details

Add 👻	Delete Copy Run Manual Scan Internal Domains	Scan started at: Jul 19, 2018 22:49	Search:	
Priority 0	Policy	Targets	Last scanned: Jul 19, 2018 22:51 Scan type:Scan and protect	Rules
Exchange On	line Policies	Scan status : Completed See details		
1	ON plan 001	All Users	Mailboxes scanned: 5/5 Mailboxes skipped: 0/5	Scan History
2	OFF Policy 2	Trend Micro Postman	Email messages scanned: 8	
3	OFF Policy 1	michael_domingo	Files blocked: 0 Suspicious URLs: 0	AS O EA WR VA Scan History

# **Dashboard View**

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



Then, please select all:

Select the Dashboard Section(s) $^{ imes}$ to view
☑ Overall Threat Detections
☑ Ransomware
☑ Business Email Compromise (BEC)
<ul> <li>✓ Summary</li> <li>✓ Advanced Threat Protection</li> <li>✓ Security Risk Scan</li> <li>✓ Virtual Analyzer for Suspicious Objects</li> </ul>
☑ Data Loss Prevention

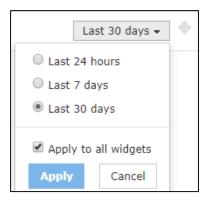




### **Overall Threat Detections**



**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.

Dashboard A	Advanced Threat Protection Data I	Loss Prev	ention Anomaly Detection	Logs Quarantine A	Administration							
Templates	Reports Scheduled Report		Q Search			٢	Select Date Range 🕶	Search				
		*	Save Export Preview Report 🕥 🏢									
			Timestamp 👻	Scan Source	<ul> <li>Security Filter</li> </ul>	Security Risk Name	Detected by	Kisk Level     Kevel     Kev				
			Sep 05, 2018 17:33	Exchange Online	Web Reputation	["75"]: [http]:[/][/]www[.]x[	Web Reputation	Dangerous				
-		1	Sep 05, 2018 17:08	SharePoint Online	Malware Scanning	Malware: test00.pdf	Suspicious Object list					
Type Security Risk Scan 👻	Security Risk Scan 👻		Sep 05, 2018 16:51	SharePoint Online	Malware Scanning	Malware: test00.pdf	Suspicious Object list					
1.164	Security Risk Scan		Sep 05, 2018 15:41	Exchange Online	Web Reputation	["75"]: [http]:[/][/]mercada		Dangerous				
Scan Source	Ransomware		Sep 05, 2018 15:41	Exchange Online	Web Reputation	["75"]: [http]:[/][/]mercada		Dangerous				
Exchange Or Virtual Analyzer		Sep 05, 2018 14:59	Exchange Online	Web Reputation	Newly Observed Domain: [ht	Web Reputation	Suspicious					
□ SharePoint C			Sep 05, 2018 14:57	Exchange Online	Web Reputation	Newly Observed Domain: [ht	Web Reputation	Suspicious				
OneDrive			Sep 05, 2018 14:32	Exchange Online	Web Reputation	Newly Observed Domain: [ht	Web Reputation	Suspicious				
Security Fi	User Activity		Sep 04, 2018 16:47	Exchange Online	Web Reputation	Ransomware - C&C Server	Web Reputation	Dangerous				
Web Reputat	User Activity Anomaly Detection		Sep 04, 2018 16:47	Exchange Online	Web Reputation	Ransomware - C&C Server	Web Reputation	Dangerous				

NOTE 🗎

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

									8		S	elect	Date	Ran	ge 🗸
	Default: all dates														
	Last 24 hours														
	Last 1 week														
n	La	st 1	mont	th											
n	Da	ate R	ange												
	« September 2018								~~	Se	epte	mber	201	8	
	Su	Мо	Tu	We	Th	Fr	Sa		Su	Мо	Tu	We	Th	Fr	Sa
	26	27	28	29	30	31	1		26	27	28	29	30	31	1
	2	3	4	5	6	7	8		2	3	4	5	6	7	8





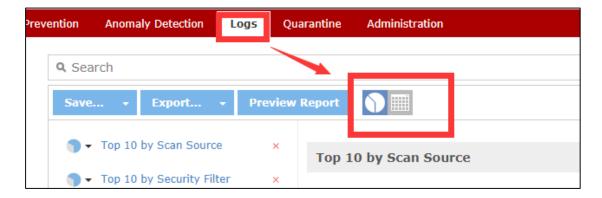
# Export the Logs

revention	Anoma	ly Detection	L	Logs Quarantine			Administration			
<b>Q</b> Se	earch	1	/							
Sav	∕e ▼	Export	•	Pre	view Report					
Time	stamp 👻	Current Vi	iew		rce	~	Security Filter			
Sep 0	5, 2018 17	, All Record	s 0	)	Online		Web Reputation			

# Generate the Report

Loss Prev	ention Anomaly Detect	ion Log	S Quarantine	Admi	nistration			
	🔍 Search 🥢							
-	Save 👻 Export	<b>-</b>	Preview Report	0				
	Report	× Scar	n Source	~	Security Filter	~		
	Template	Exch	ange Online		Web Reputation			
Ť	Scheduled Report	Shar	Point Online		Malwaro Scanning			

# Switch the Log View





# Appendix

# **TMCAS** Related Documentations

CAS Writing Style Best Practice Guide

# Apply for a Trial Account

Go to Cloud App Security Console to Apply a Trial Account

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

NOTE CAS trial license will expire within 2 months. You may contact Trend Micro Support to extend trial license.



Securing Your Journey to the Cloud

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<sup>™</sup> Smart Protection Network<sup>™</sup>, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

©2020 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.