Best Practice Guide

Trend Micro Cloud App Security

Contents

Purpose

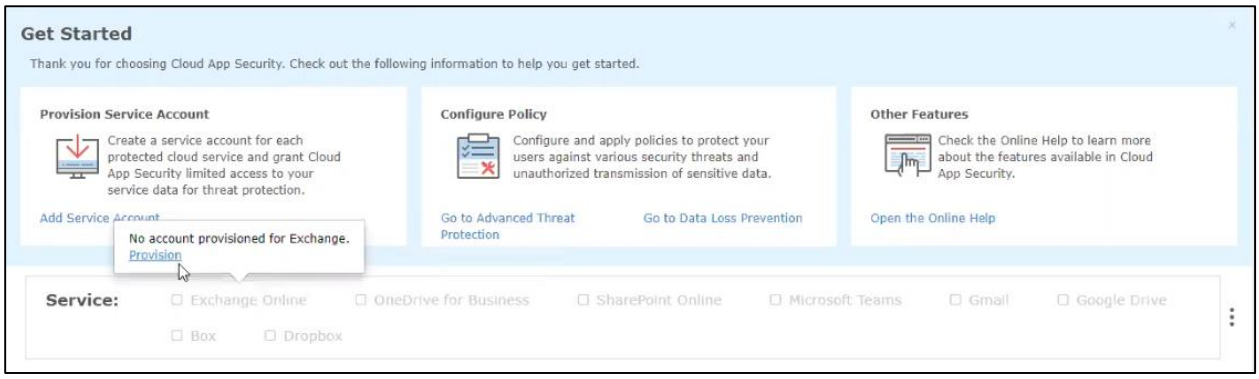
This document serves as a guideline to help customers develop a set of best practices when provisioning and managing Cloud App Security (TMCAS).

Deployment

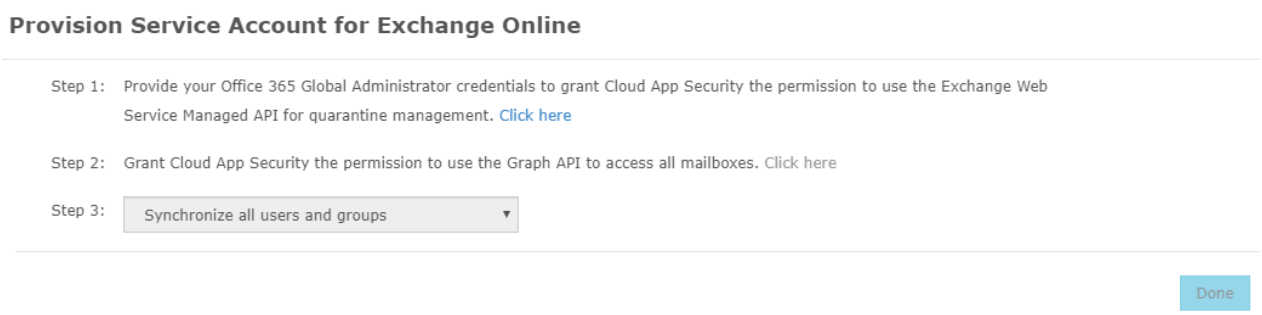
Provision CAS to Protect Exchange Online

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.



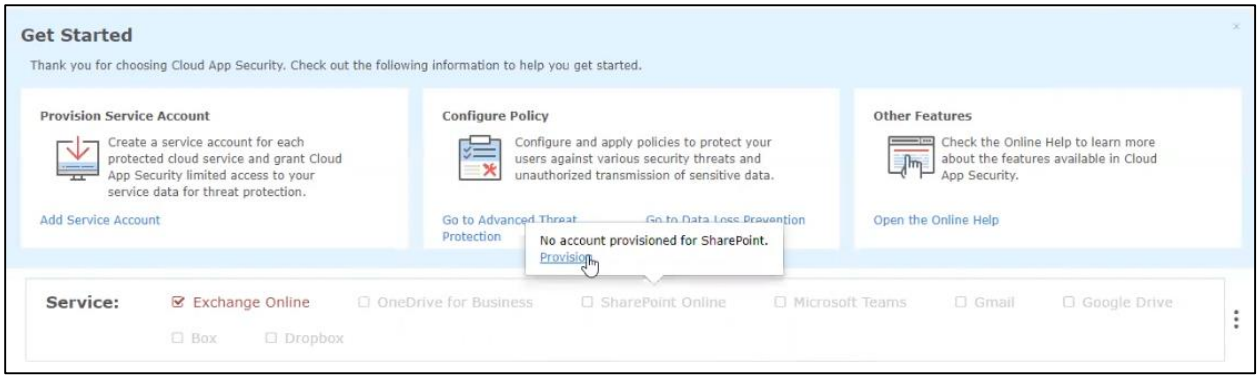
Follow the Steps in Provisioning CAS to protect Exchange Online:

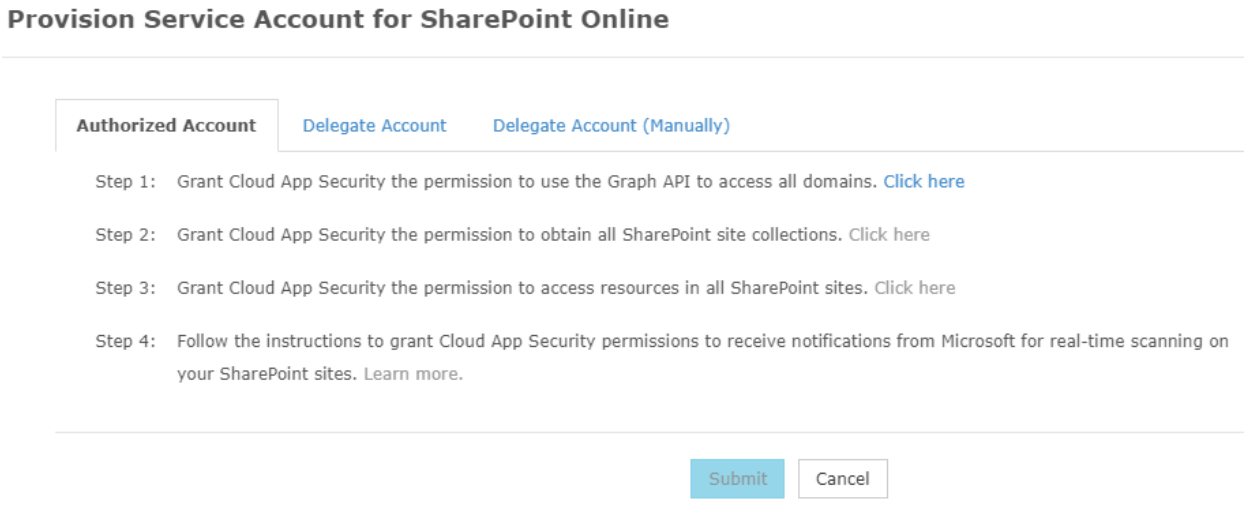


Provision CAS to Protect SharePoint, OneDrive, and Teams

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

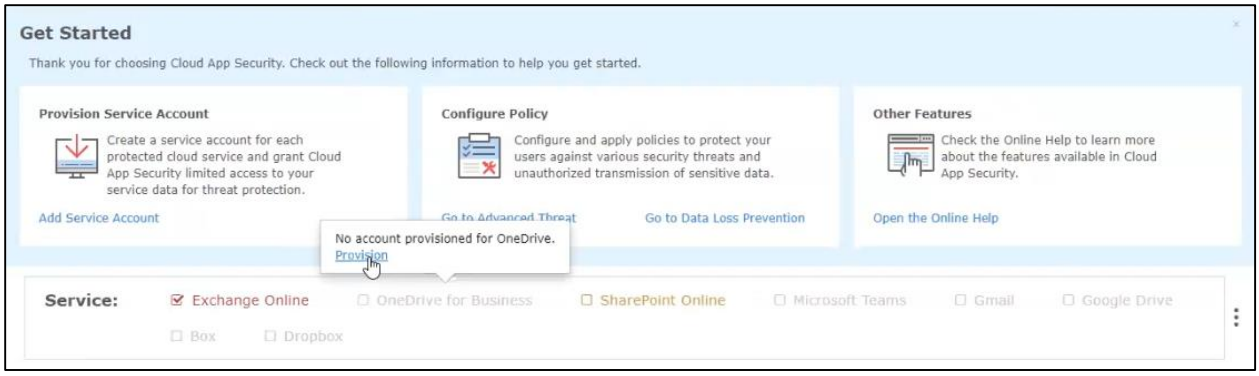
For SharePoint:

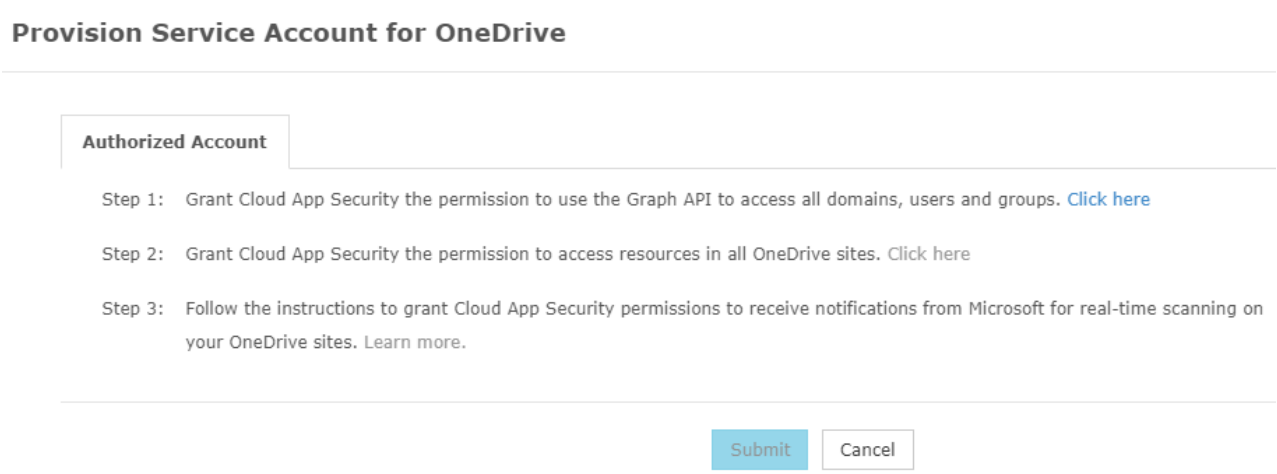




It is **VERY IMPORTANT** to do the instructions in Step 4 by clicking "Learn More" for CAS to receive any file changes notification from Microsoft for Real-time Scanning on your SharePoint sites.

For OneDrive:

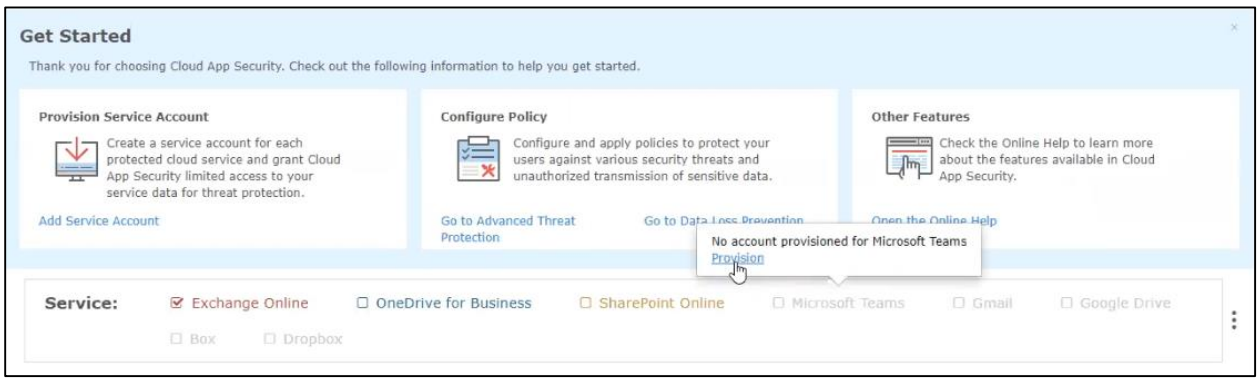


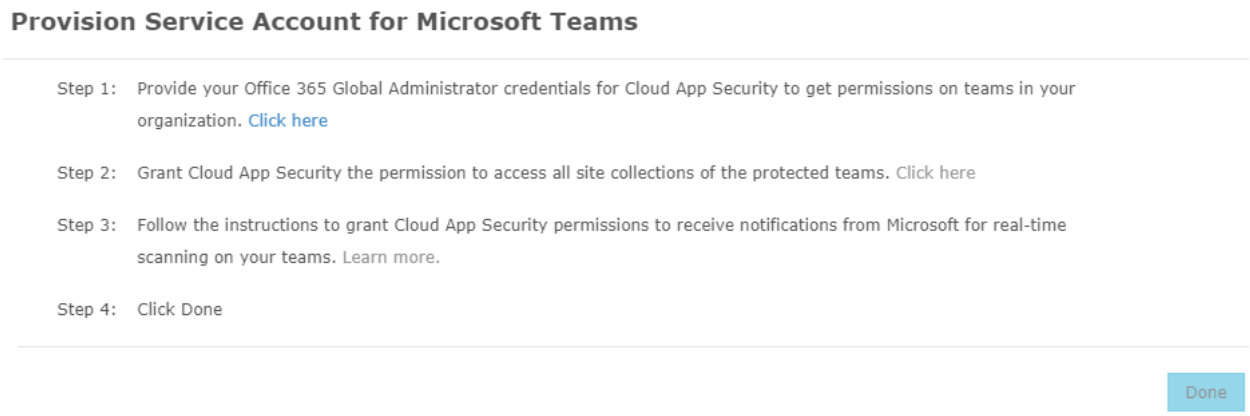


It is **VERY IMPORTANT** to do the instructions in Step 3 by clicking "Learn More" for CAS to receive any file changes notification from Microsoft for Real-time Scanning on your OneDrive sites.

For Teams:

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





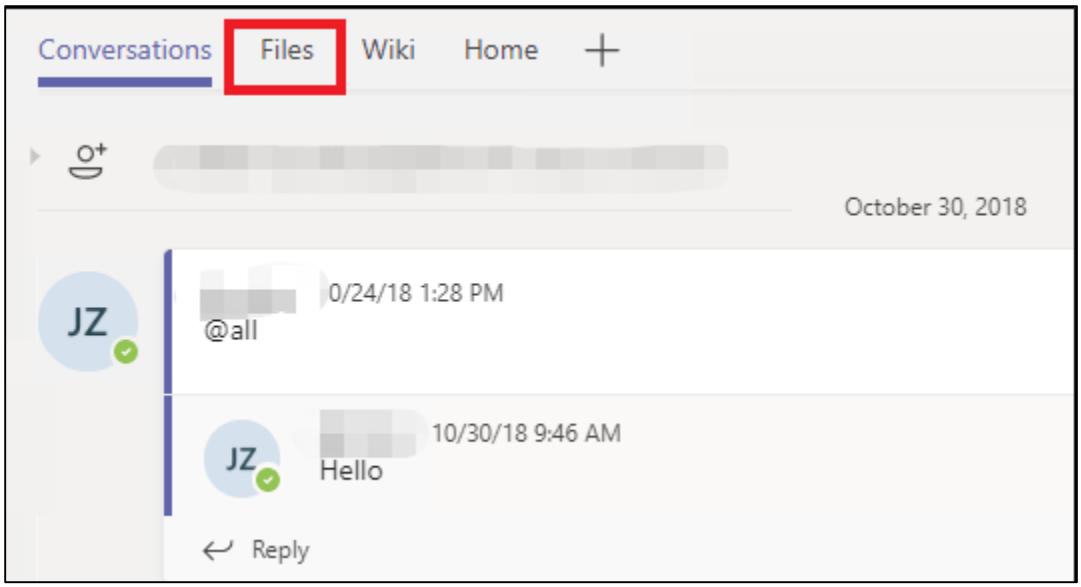
It is **VERY IMPORTANT** to do the instructions in Step 3 by clicking "Learn More" for CAS to receive any file changes notification from Microsoft for Real-time Scanning on your Teams sites.

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.



.

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

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.

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.

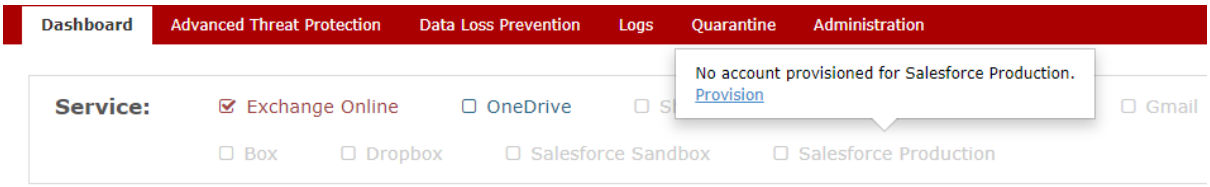
NOTE Dropbox provision needs extra steps to input the team admin account for the provision.

- 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

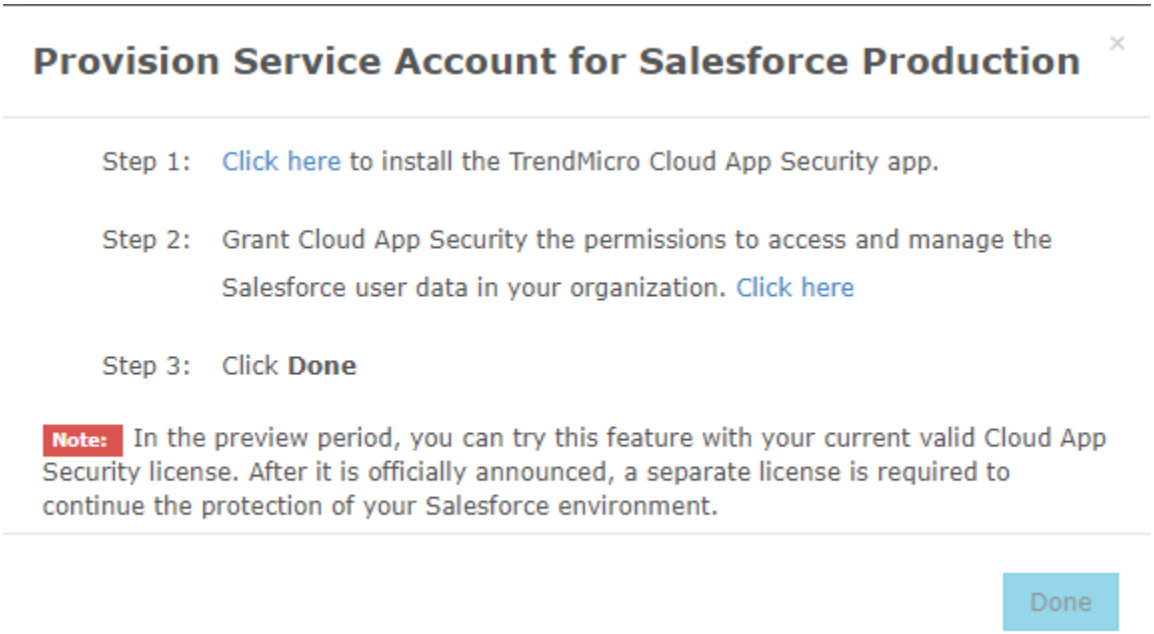
Provision CAS to protect Salesforce Production or/and Salesforce Sandbox

- 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.

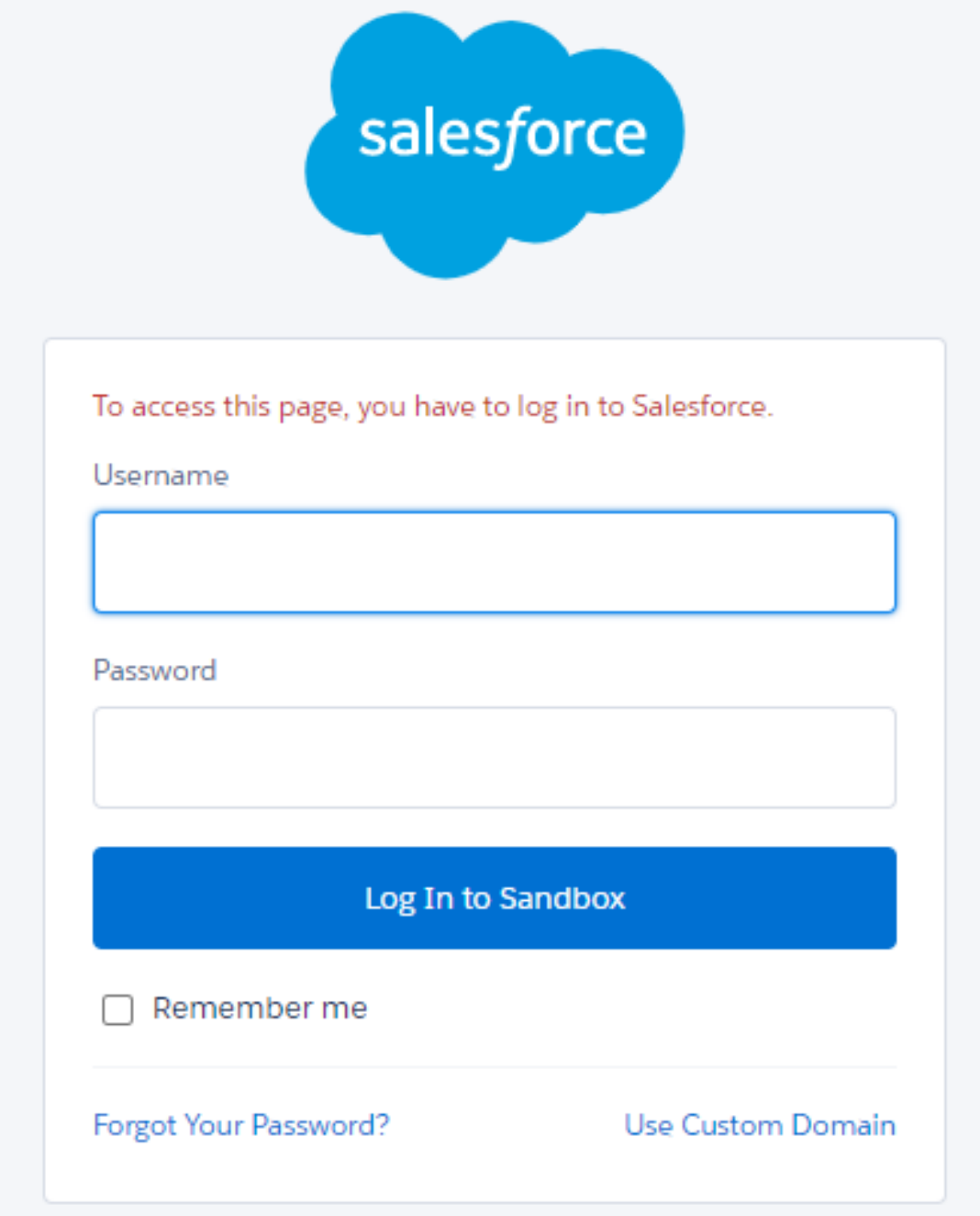


Follow the Steps in Provision Service Account for Salesforce Production:



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.

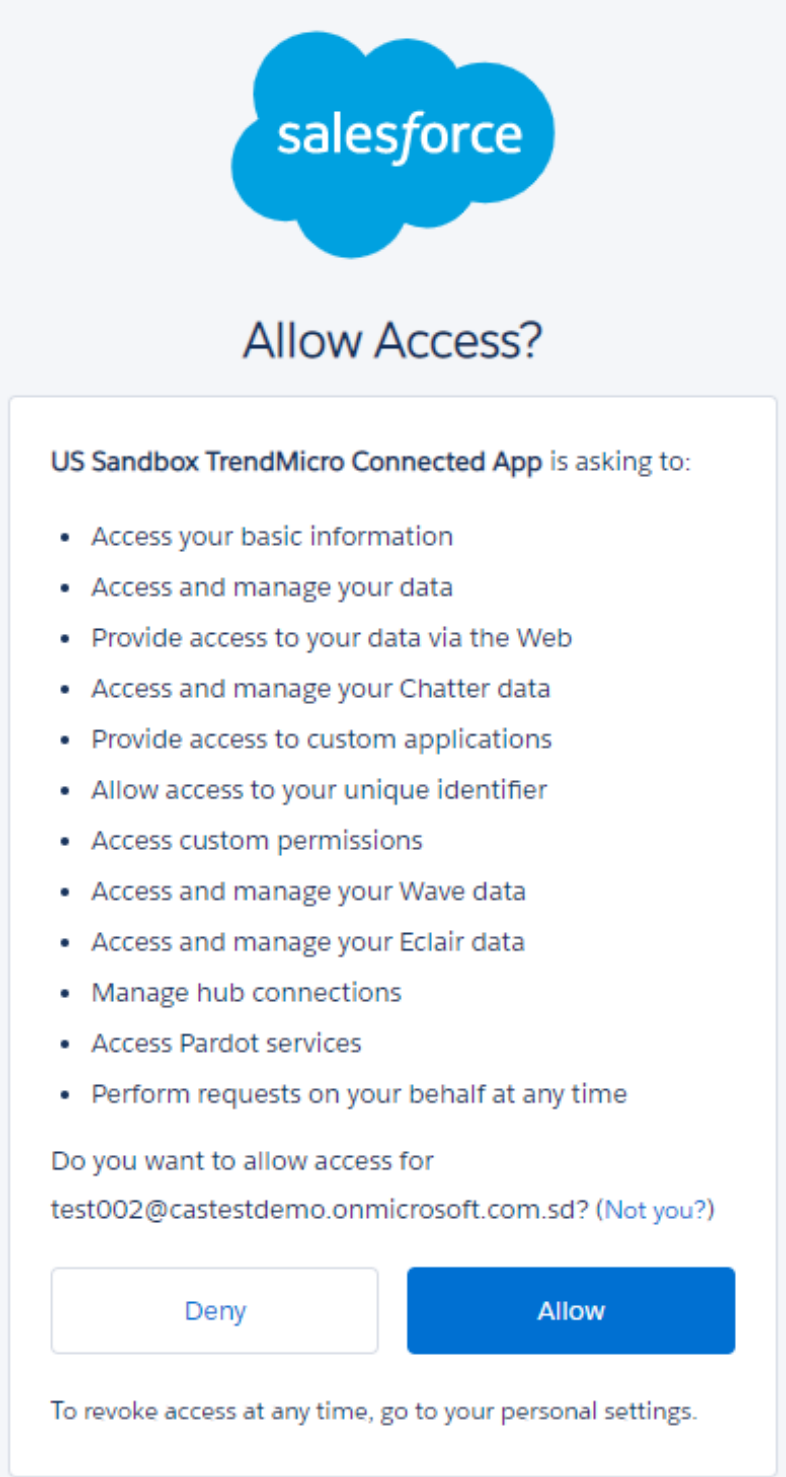
Login to Salesforce with the administrator's credential. Please note that the administrator will not be protected by CAS. You may want to create a dedicated Salesforce administrator account only used to do administrative tasks.



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

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.

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



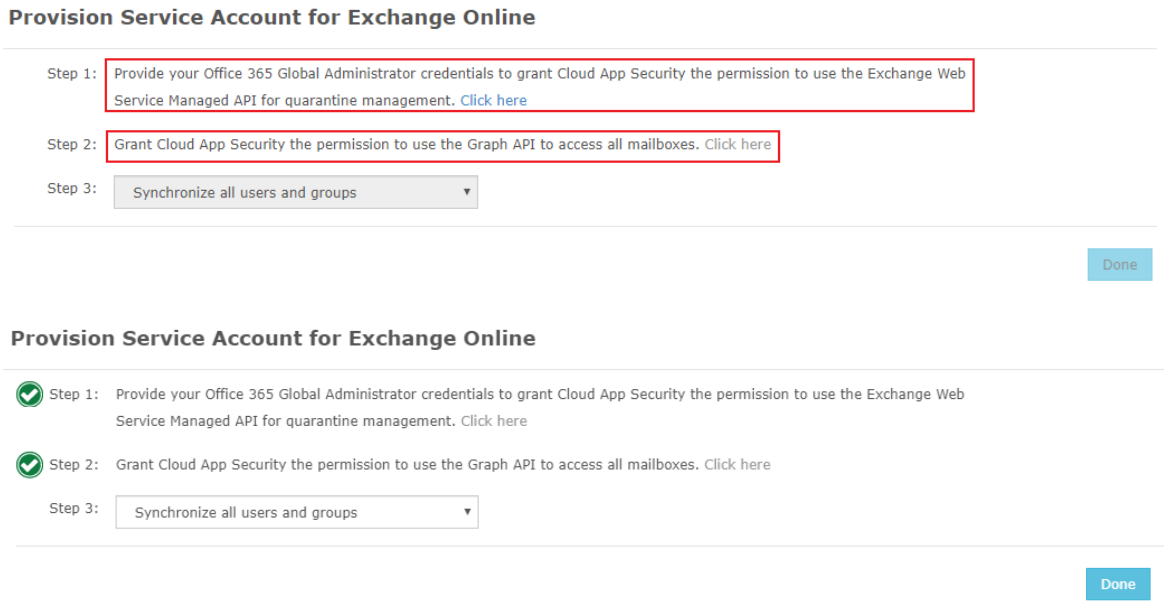
How to Verify Provision Status

For Office365 services

To evaluate the current provision status for Office365 services:

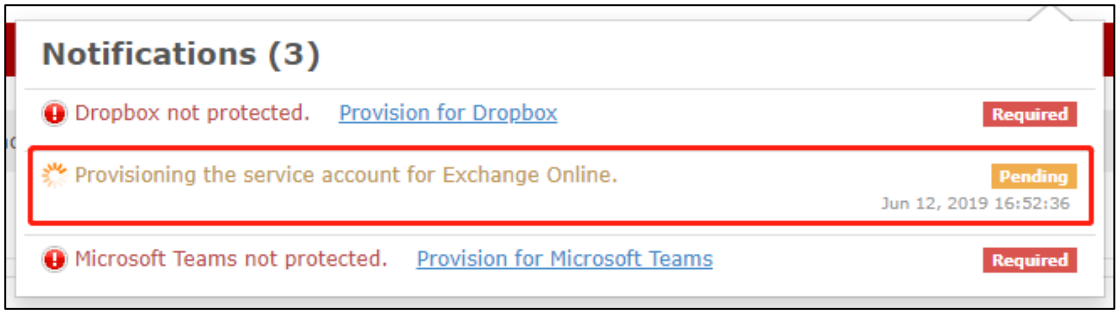
- **Exchange Online Provision with Authorized Account (access token)**

  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.



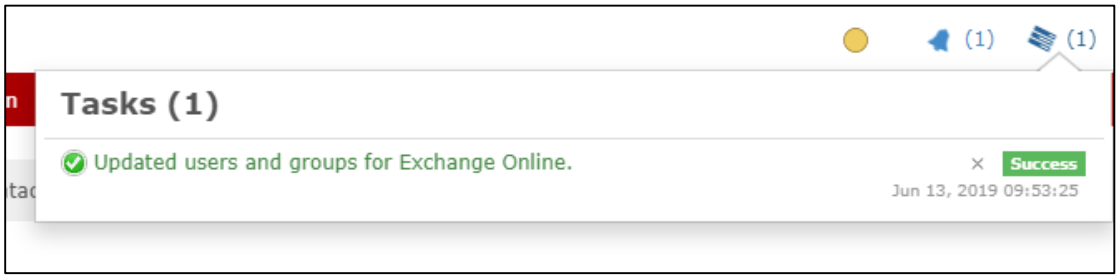
Step 1: After Step 1 is done, the status of "Provisioning the service account for Exchange Online" displayed under Notifications is Pending. This step takes only a few seconds. If it lasts for more than one minute, there must be something wrong.

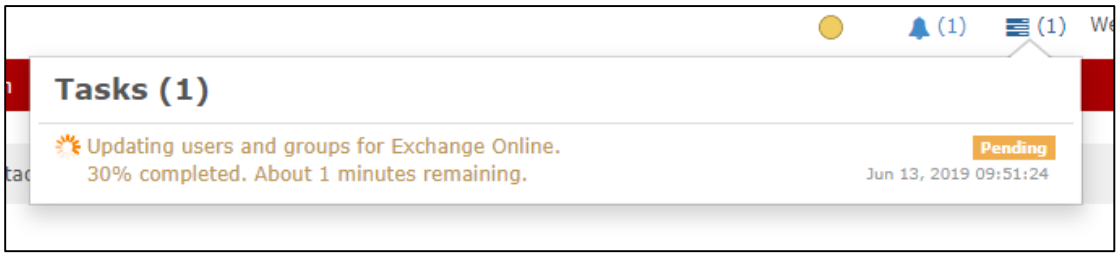
Hover the mouse to this icon in the top-right corner, notification list will show up like below



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.

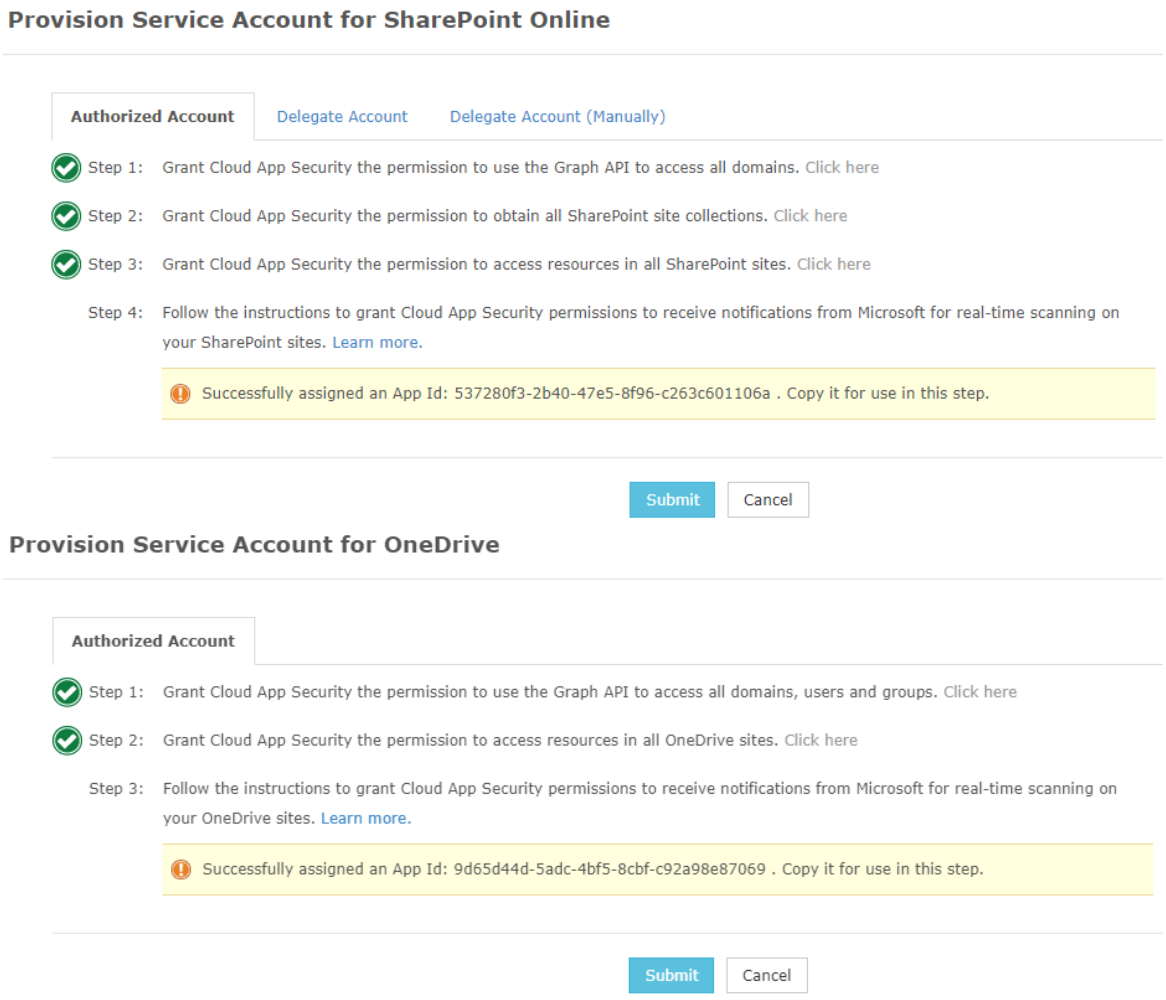
Step 3: CAS synchronizes users and groups from the customer's Office 365. The time required will depend on the scale of the O365 tenant. An estimated time will show for this task, like "Update users and groups for Exchange Online. ** completed, About ** remaining". If the status is "pending" and keeps 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.

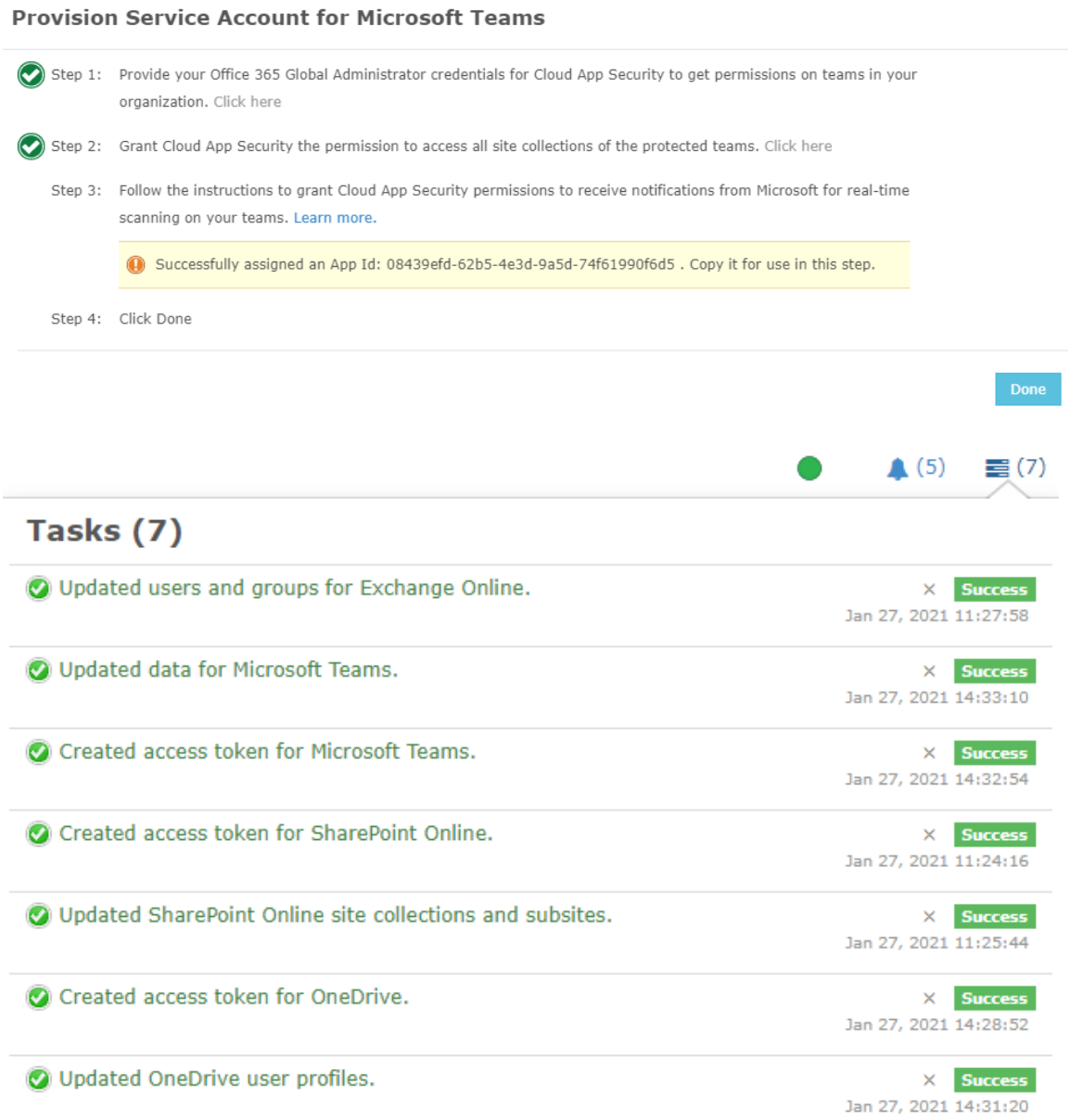


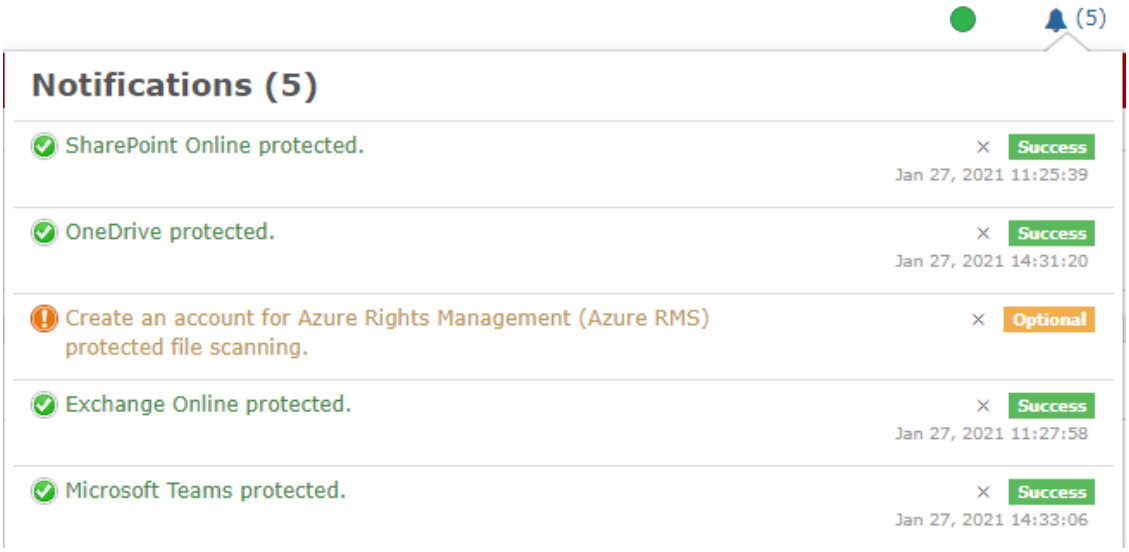


- **SharePoint, OneDrive and Teams with Authorized Account**
  Verifying SharePoint, OneDrive and Teams provision status with Authorized Account (access token) is similar to Exchange Online provision with Authorized Account.

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

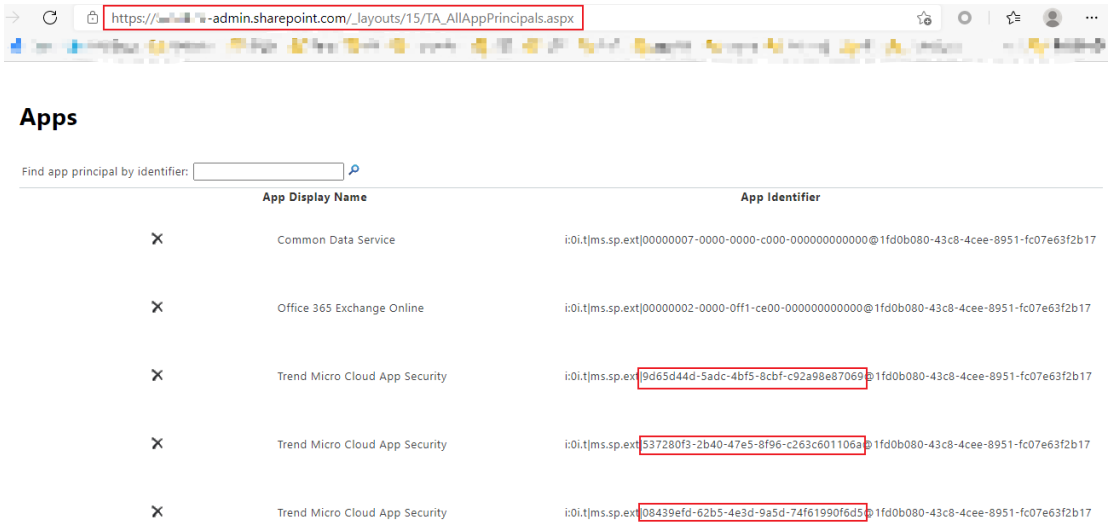



Provision Service Account for Microsoft Teams
Step 1: Provide your Office 365 Global Administrator credentials for Cloud App Security to get permissions on teams in your organization. Click here
Step 2: Grant Cloud App Security the permission to access all site collections of the protected teams. Click 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.
Successfully assigned an App Id: 08439efd-62b5-4e3d-9a5d-74f61990f6d5 . Copy it for use in this step.
Step 4: Click Done
Done
(5)
(7)
Tasks (7)
Updated users and groups for Exchange Online.
Success
Jan 27, 2021 11:27:58
Updated data for Microsoft Teams.
Success
Jan 27, 2021 14:33:10
Created access token for Microsoft Teams.
Success
Jan 27, 2021 14:32:54
Created access token for SharePoint Online.
Success
Jan 27, 2021 11:24:16
Updated SharePoint Online site collections and subsites.
Success
Jan 27, 2021 11:25:44
Created access token for OneDrive.
Success
Jan 27, 2021 14:28:52
Updated OneDrive user profiles.
Success
Jan 27, 2021 14:31:20

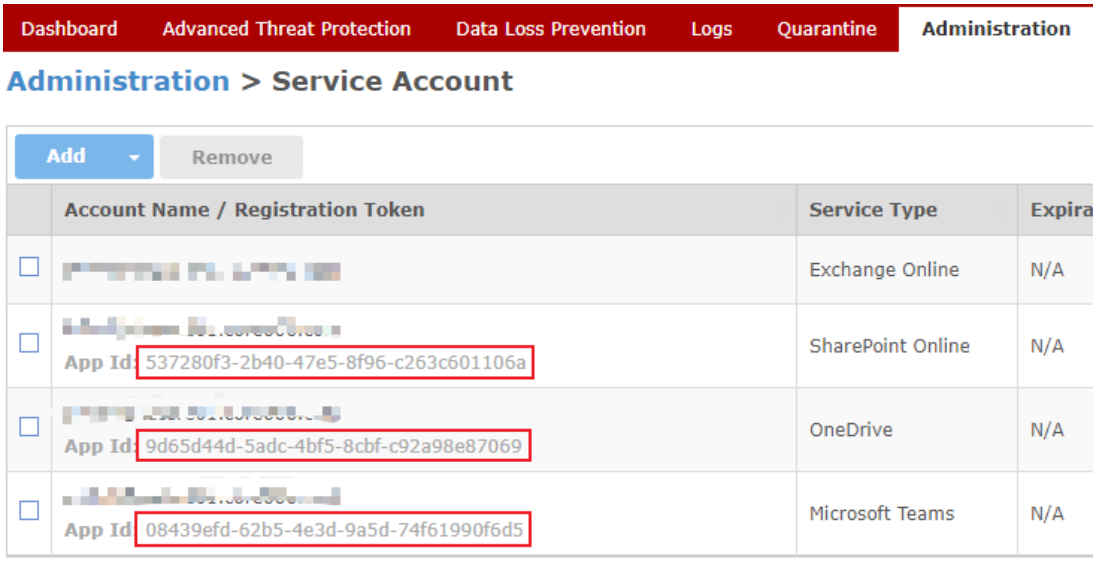


Confirm if you have successfully granted Cloud App Security permissions to receive notifications from Microsoft upon any change to the files on your SharePoint sites, for SharePoint, OneDrive and/or Teams.

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 :



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



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:

- SharePoint Step 11
- OneDrive Step 9
- Microsoft Teams 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
  - Updating SharePoint Online site collections and subsites
  - Updating OneDrive for Business users and groups

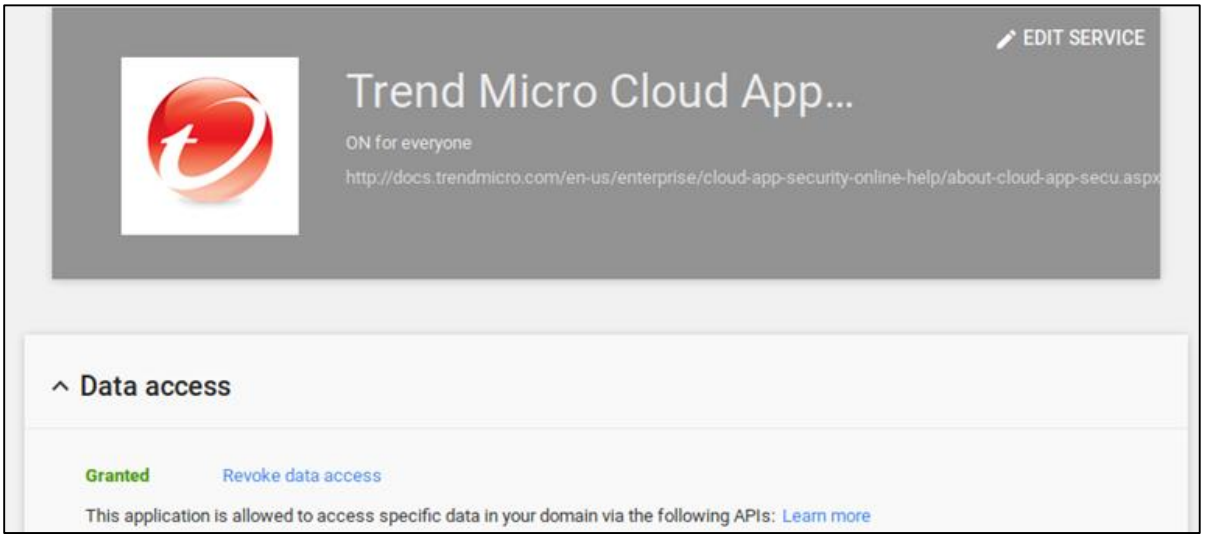
  "Creating the delegate account" means that CAS is creating a delegate account for the customer. Normally it does not take too long, no longer than 30 minutes. If this status keeps pending for more than 30 minutes, there should be something wrong in CAS.

  "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.

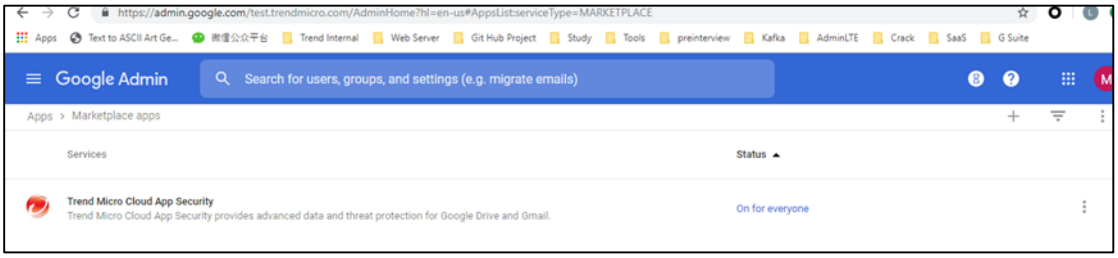
For Gmail

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

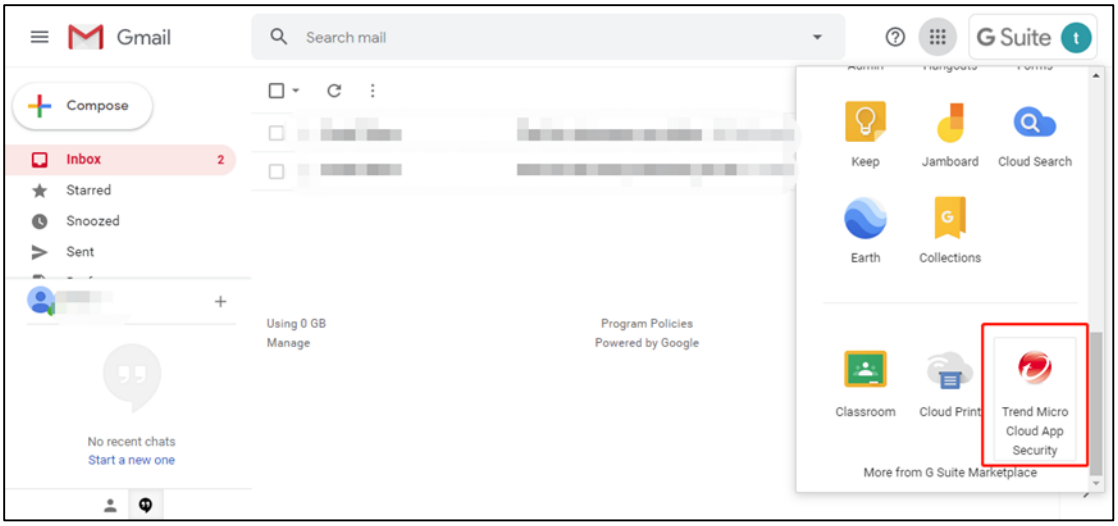
1. Make sure necessary access privileges are granted to CAS in the G Suite admin console: **Apps** > **Marketplace apps and locate Trend Micro Cloud App Security**. Make sure the Data access section status is "Granted".



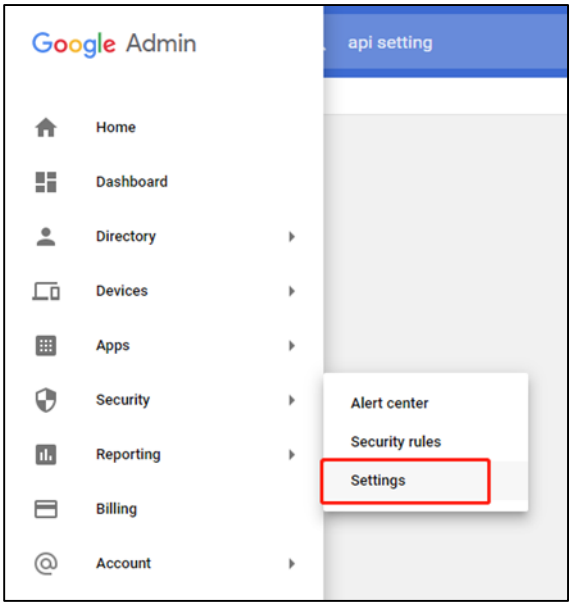
2. Access the Google admin App page to ensure that the CAS App enabled for all uses.



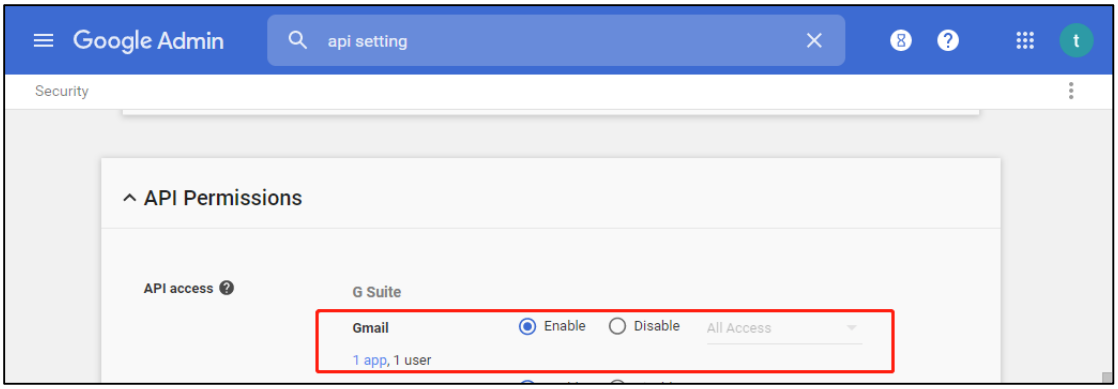
3. Check whether the provisioned user has CAS App.



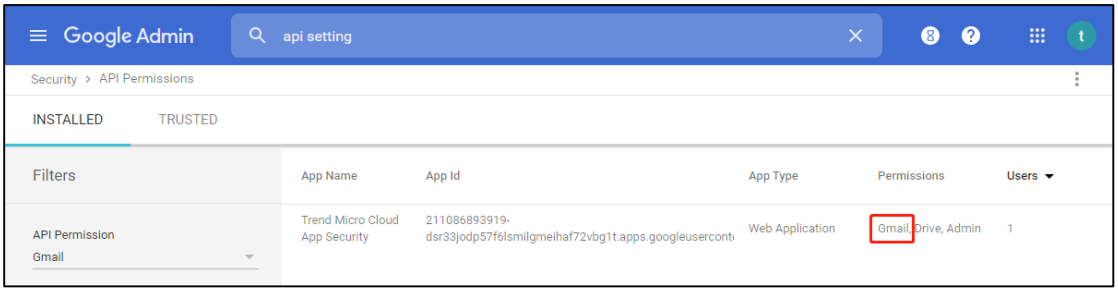
4. Check Google Admin page about the advanced G Suite API setting. On the Google Admin console, go to **Security** > **Settings**.



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



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

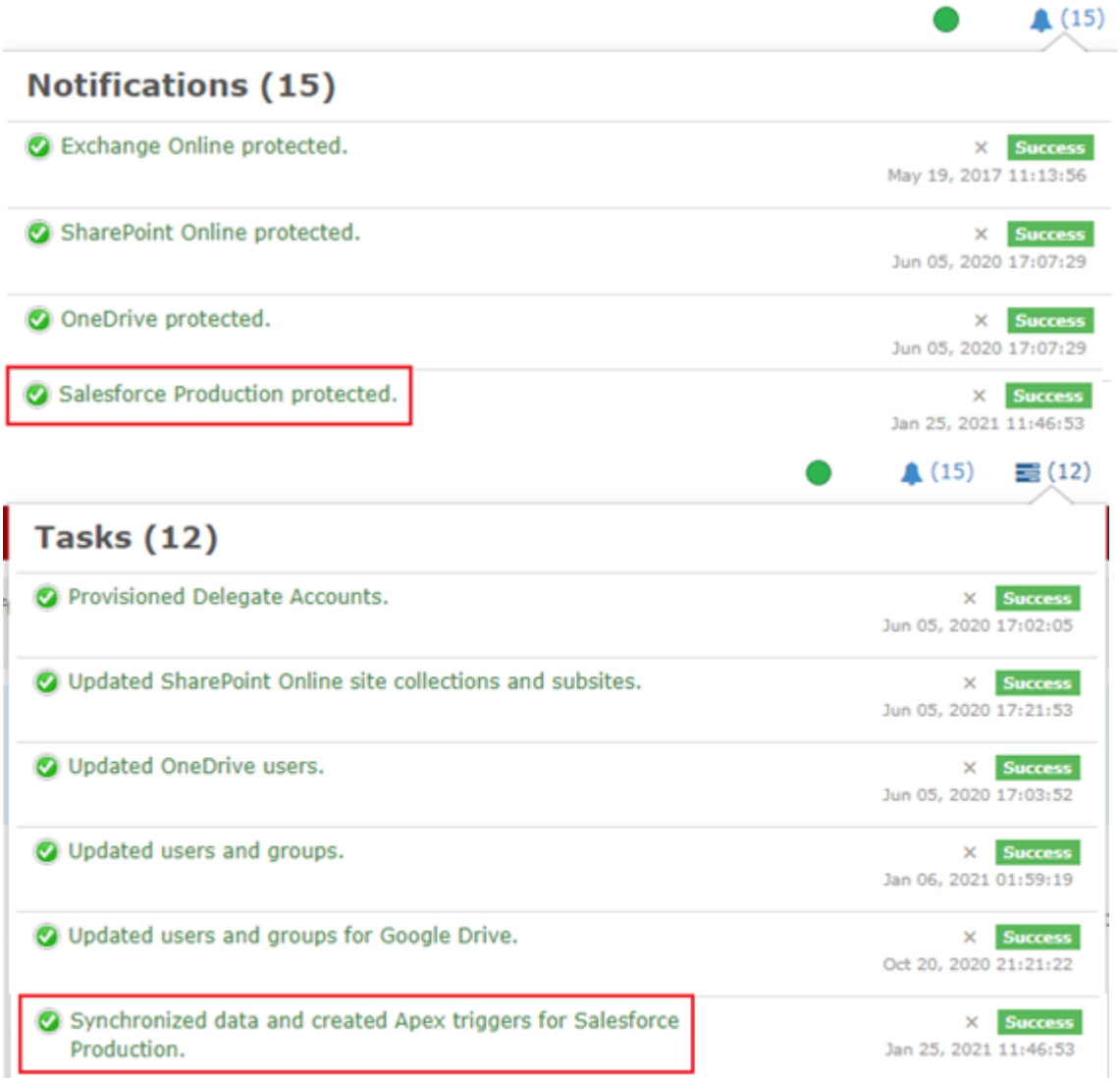


During the Gmail provision, one status display under Task, which will indicate the backend progress:

- 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.

- **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.

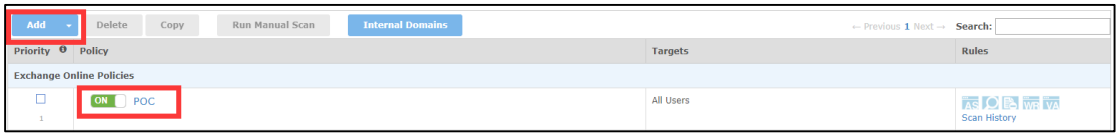
- Enable most of the Cloud App Security features (such as: advanced spam prevention, malware scanning etc.)
- After new user is created, suggest to firstly click the "click here" link to sync new users before testing
- When a mailbox is newly migrated from on-prem to cloud, a manual cloud mailbox scan 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.

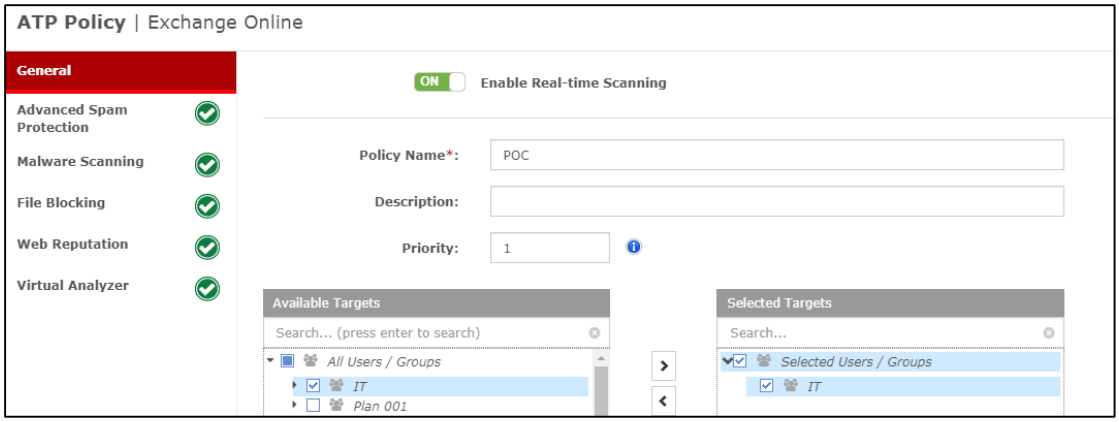
Configure ATP Polices

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

✓ Create a new policy.



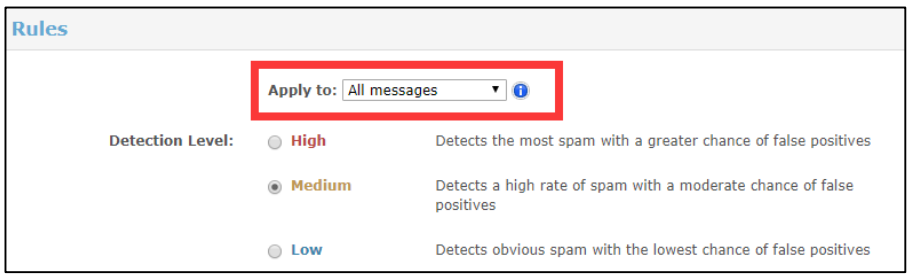
✓ Select the specific targets.



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

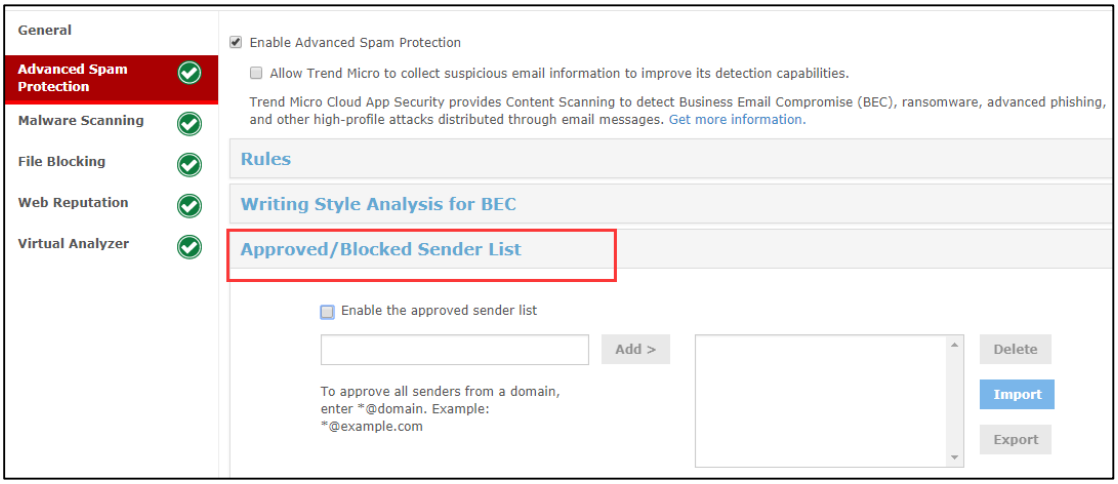
✓ Apply the Rules to the **<All messages>.**



✓ Enable the Writing Style Analysis

NOTE Please click **HERE** to get the Writing Style BP.

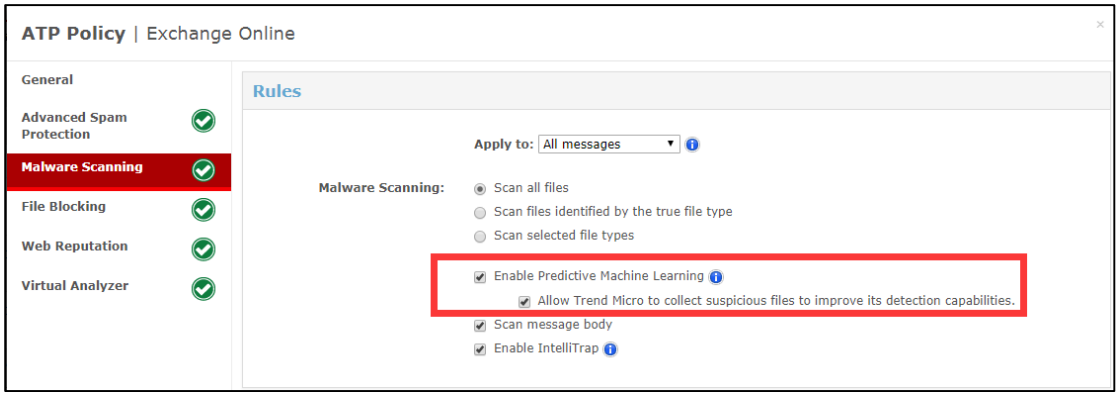
✓ In order to reduce the FP, we suggest the customer to add the trust sender into CAS Approved Sender List.



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.

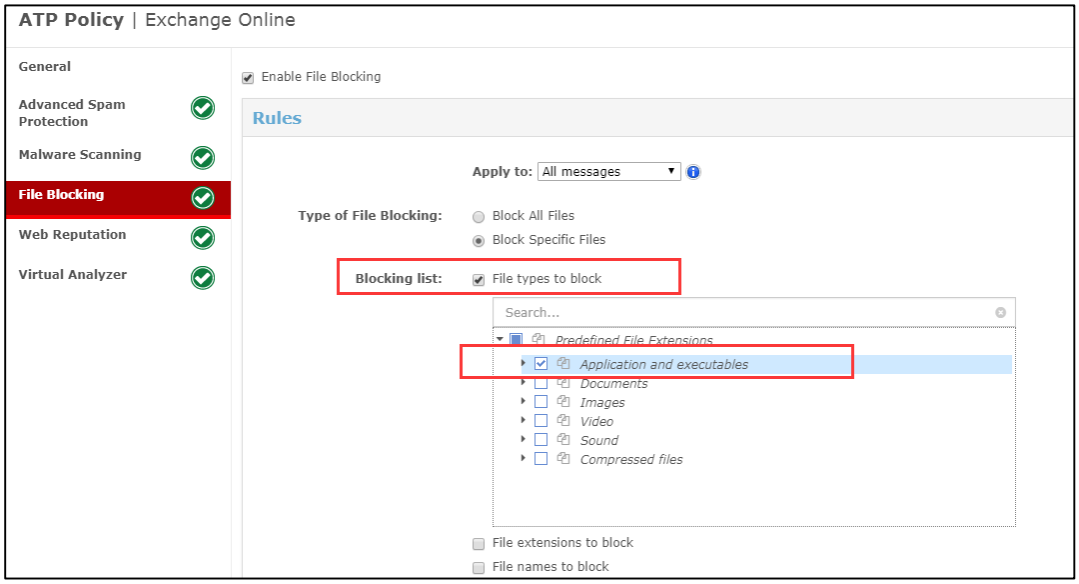
Click HERE to get testing sample.



NOTE Predictive Machine Learning is disabled by default.

File Blocking

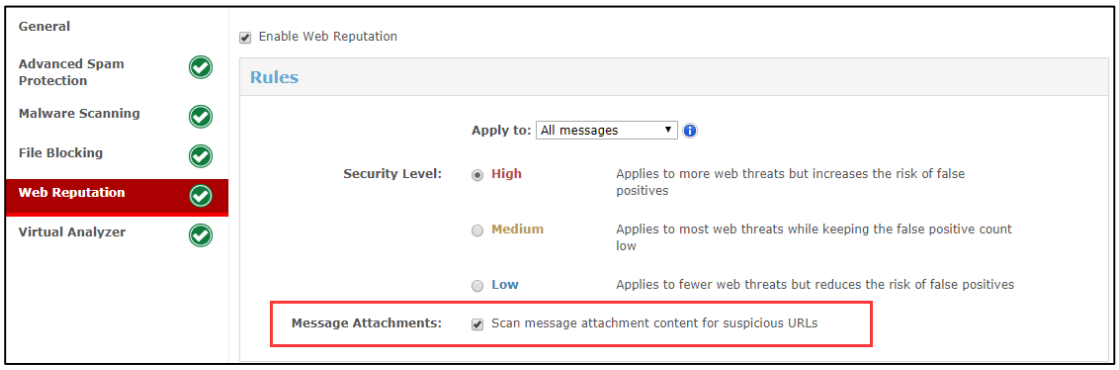
Setup a File Blocking policy to block according to the file type.



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

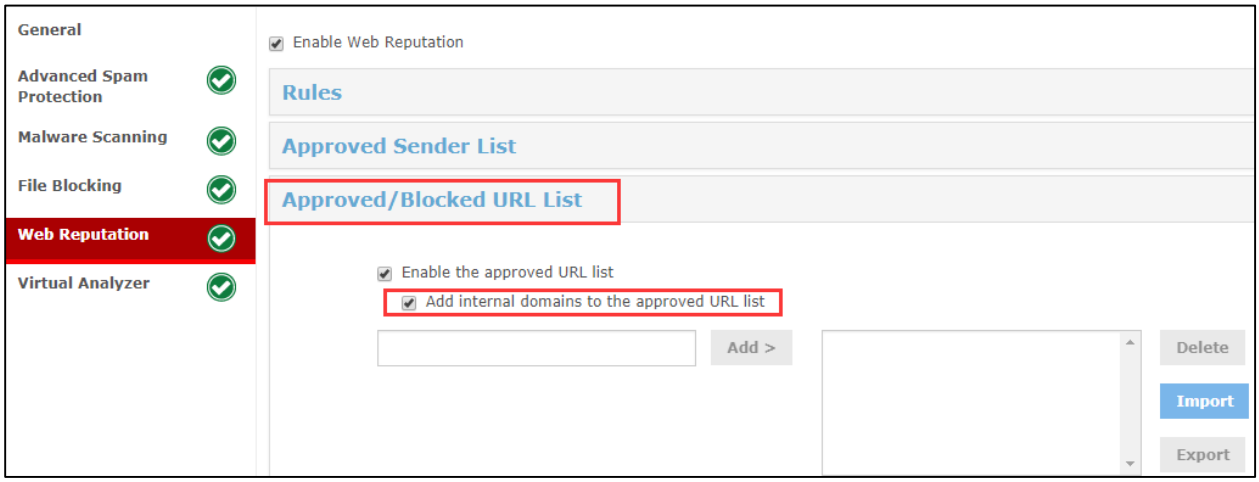
Web Reputation

Setup a web reputation policy to detect the bad URLs. (Especially, we have 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 is also highly recommended the customer add "internal domains to the approved URL List".

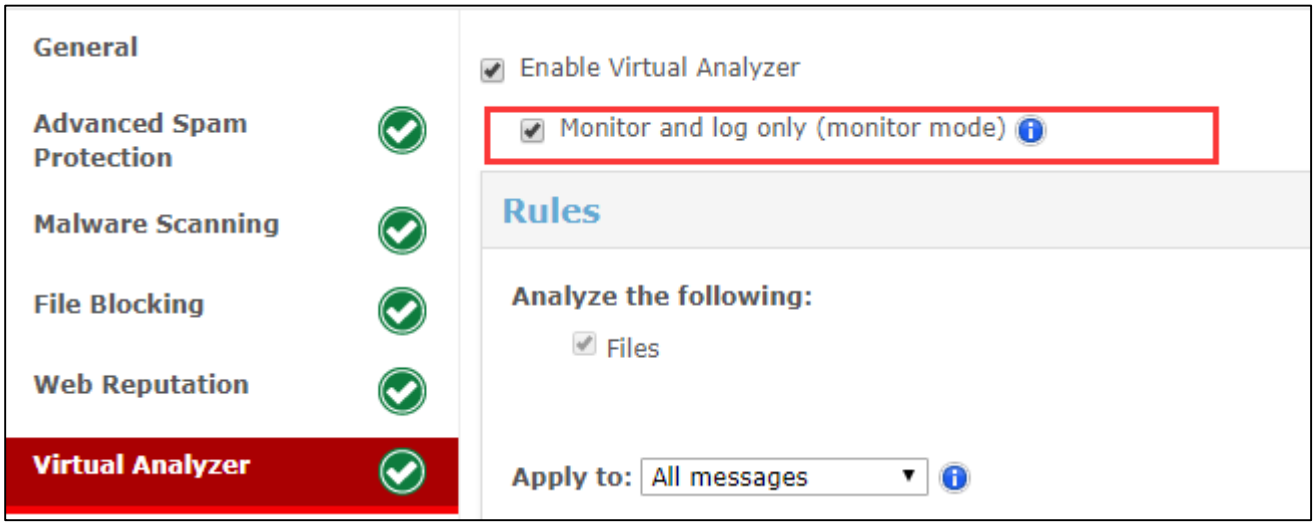


Virtual Analyzer

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.

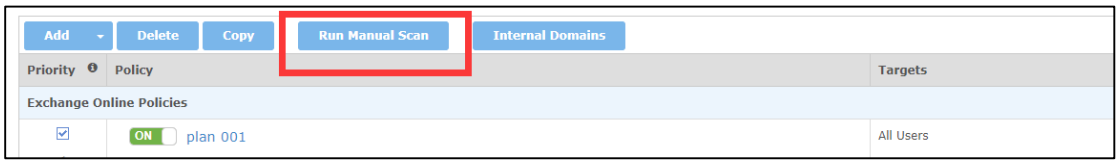
NOTE In order to make our customer understand this feature better, we suggest the customer to use monitor mode first. In this mode, CAS's VA feature will only record the VA detection result, but will not take any action.



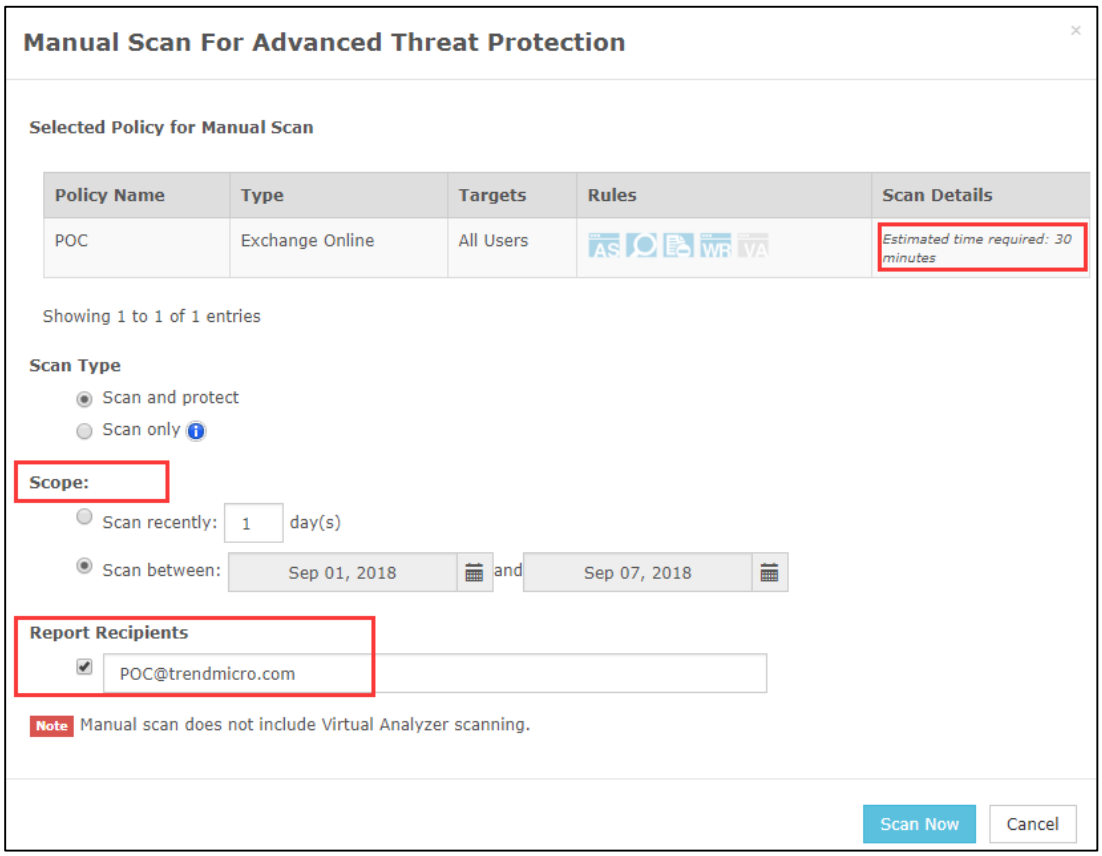
Displaying Detection Results

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 existing before the customer deploys CAS.



Then there will be new pop-up window:

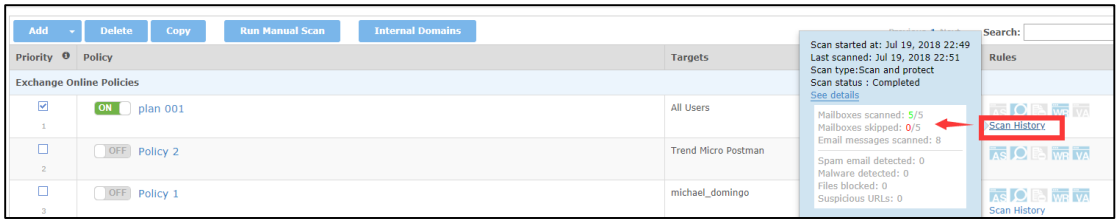


- ✓ The estimated completion time is shown during a scan.
- ✓ Refer to the **Scan Result** to see how long the manual scan took.
- ✓ Add **Report Recipient** to set users who will receive the notification when the manual scan is finished
- ✓ For trial account users, it allows you to select the Scope 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.

Check the Manual Scan Result

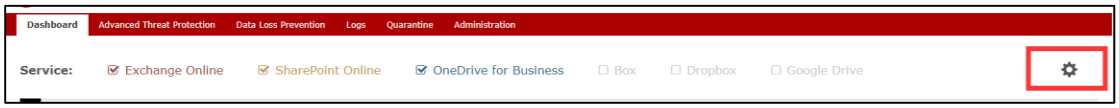
Click the scan history to get the manual scan result.

➔ Show details

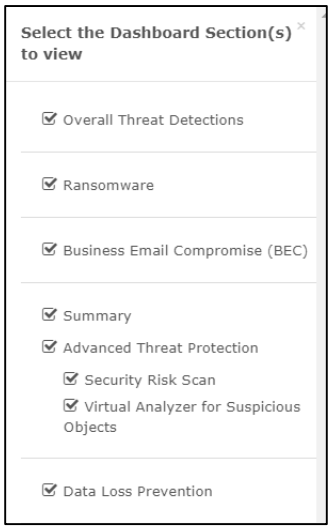


Dashboard View

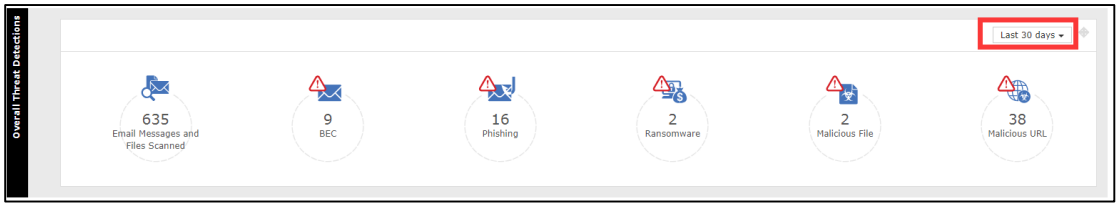
Manage the widgets to show CAS's detections



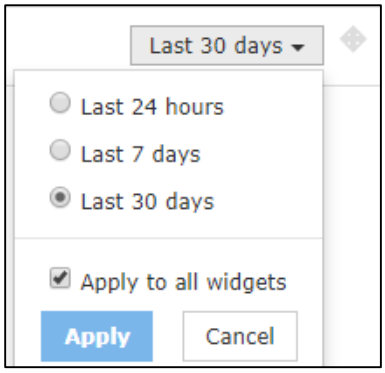
Then, please select all:



Overall Threat Detections

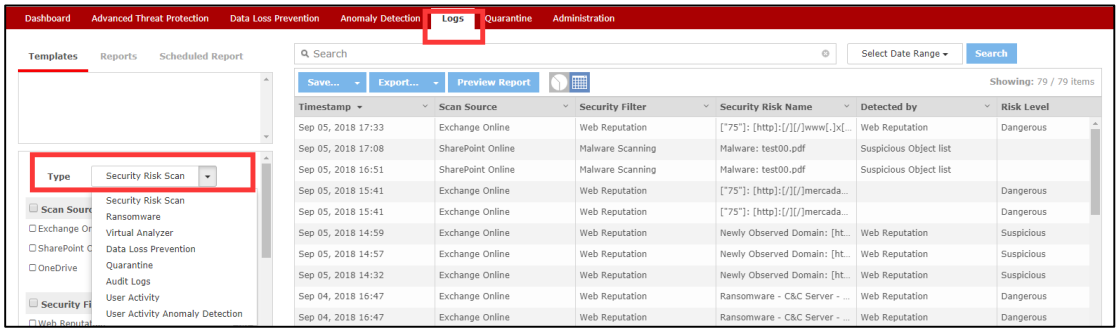


NOTE Select the right time range for the detection result that will be displayed on dashboard. (You can select "Apply to all widgets").

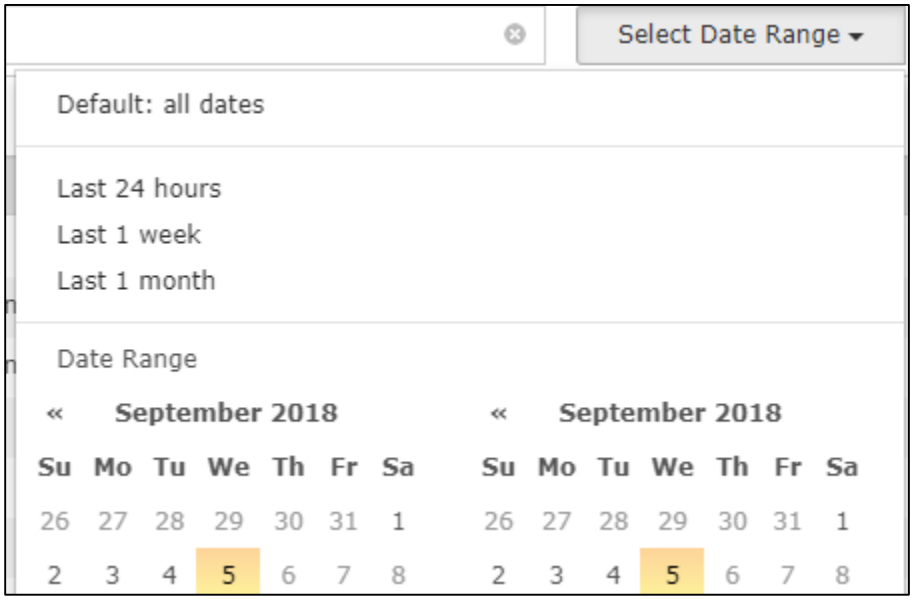


Log Console

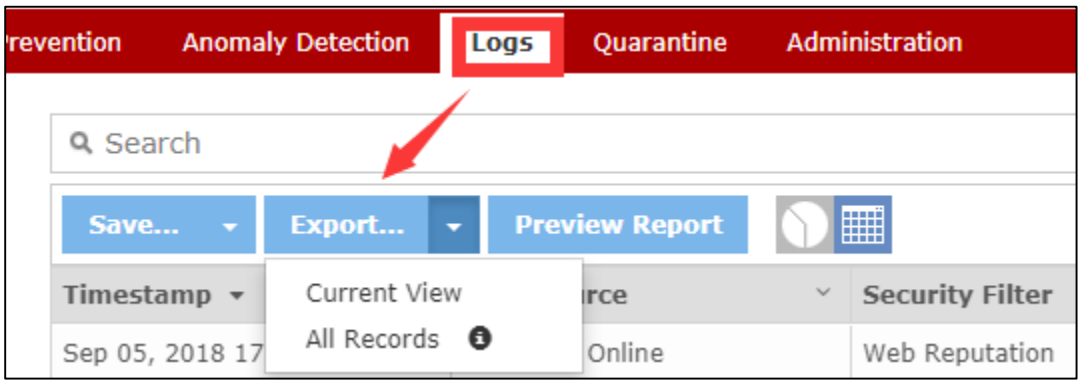
On CAS console, the user is provided with a place to view the scan logs that are collected from different CAS server roles and detections.



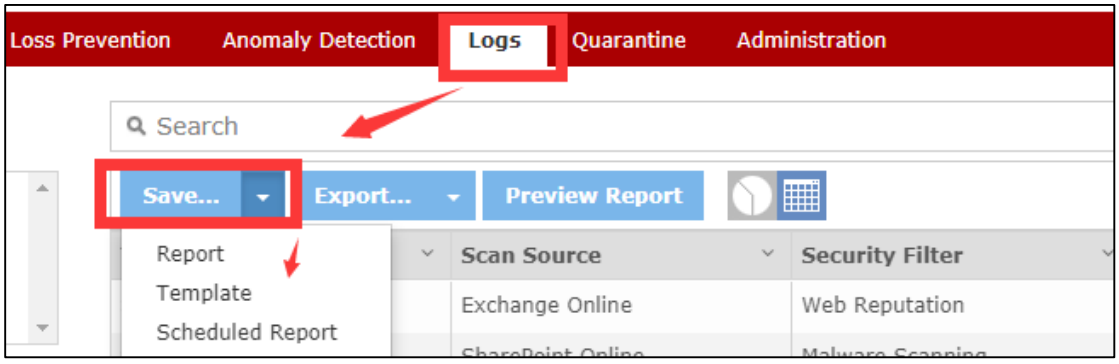
NOTE Select the right time range for the detection result on log view console.



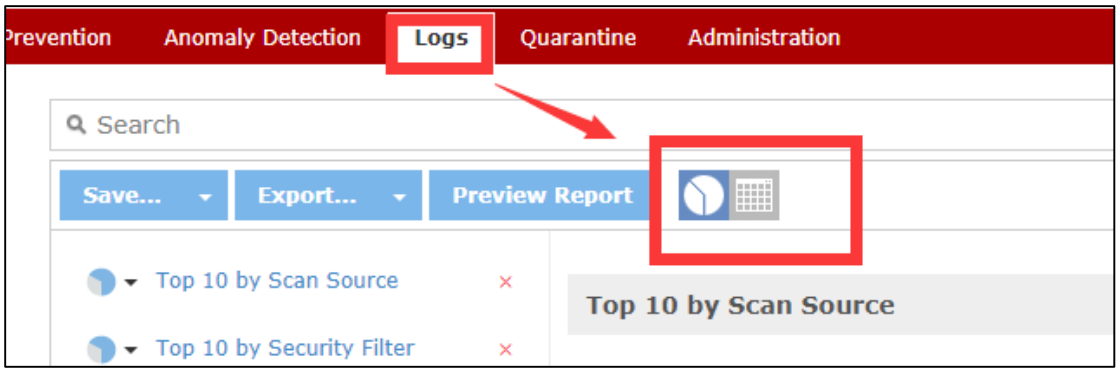
Export the Logs



Generate the Report



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 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 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™ Smart Protection Network™, 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.