Trend Micro™

Cloud App Security Best Practice Guide
# Table of Contents

Table of Contents ........................................................................................................................................... 2

About this Book ................................................................................................................................................. 5

1.1 Preface......................................................................................................................................................... 5
1.2 Authors ....................................................................................................................................................... 5
1.3 Pre-requisites ................................................................................................................................................ 5
1.4 Abbreviations and Terms ........................................................................................................................... 6
1.5 Conventions ................................................................................................................................................ 7
1.6 Revision ....................................................................................................................................................... 8

Chapter 1: Product Overview ............................................................................................................................. 9

1.1 How Trend Micro Cloud App Security Works ............................................................................................ 9
1.2 How Cloud App Security Protects Your Data Privacy .............................................................................. 10
1.3 Key Features .............................................................................................................................................. 10
1.4 What’s New ............................................................................................................................................... 11
1.5 System Requirements ................................................................................................................................ 11

Chapter 2: How to Provision ............................................................................................................................... 12

2.1 O365 Provision .......................................................................................................................................... 12
  2.1.1 Automatically Provisioning Delegate Account .................................................................................. 12
  2.1.2 Manual Provisioning on Exchange .................................................................................................. 12
  2.1.3 Manually Provisioning SharePoint Online ....................................................................................... 13
2.2 Box Dropbox and Google Drive Provision ................................................................................................ 13
  2.2.1 Before Provision ............................................................................................................................... 13
  2.2.2 Provisioning a Service Account for Box ........................................................................................ 15
  2.2.3 Provisioning a Service Account for Dropbox .............................................................................. 15
  2.2.4 Provisioning a Service Account for Google Drive .................................................................... 15
  2.2.5 RMA Account .................................................................................................................................. 16
2.3 Key to Success ............................................................................................................................................ 16

Chapter 3: Protection for Exchange Online ....................................................................................................... 17

3.1 Recommend Configuration for Each Feature ............................................................................................ 18
  Advanced Spam Protection .......................................................................................................................... 18
  Malware Scanning ....................................................................................................................................... 18
Web Reproduction .............................................................................................................. 19
Virtual Analyzer ................................................................................................................ 19
3.2 Ransomware Protection .............................................................................................. 20
3.3 Smart Protection for Forged Email .............................................................................. 21
Advanced Spam Protection .............................................................................................. 22
Web Reputation .................................................................................................................. 23
Data Loss Prevention ......................................................................................................... 24
Chapter 4: Data Loss Protection ....................................................................................... 26
4.1 Define an DLP Identifier ............................................................................................ 27
    4.1.1 Define “Keyword” Data Identifier ...................................................................... 27
    4.1.2 Define “Regular Expression” Data Identifier ...................................................... 29
4.2 DLP Template Definition ........................................................................................... 31
    Predefined Compliance Template ............................................................................... 31
    Defining a Customized Template ............................................................................... 32
4.3 Define a DLP Policy .................................................................................................... 33
4.4 Data Loss Prevention Criteria ..................................................................................... 34
Chapter 5 Administration ................................................................................................ 35
5.1 Scan Logs ..................................................................................................................... 35
    5.1.1 Log Types ........................................................................................................... 35
    5.1.2 Reports .............................................................................................................. 36
5.2 Service Account .......................................................................................................... 36
5.3 Users and Roles .......................................................................................................... 37
    5.3.1 User Management .............................................................................................. 38
    5.3.2 Role Management .............................................................................................. 38
5.4 Dashboard .................................................................................................................... 40
5.5 License ......................................................................................................................... 40
    5.5.1 What happens to an expired license ................................................................... 40
    5.5.2 How to extend an account ................................................................................. 41
Chapter 6: Central Manager Integration ............................................................................ 41
6.1 Registering with Control Manager ............................................................................. 42
6.2 Single Sign On with Control Manager ......................................................................... 42
6.3 Checking Service Status in Control Manager ............................................................... 43
6.4 Querying Logs with Control Manager ......................................................................... 43
About this Book

1.1 Preface


This document provides in-depth information about TMCAS architecture, configuration and deployment process as well as troubleshooting.

This document should be read in conjunction with the Trend Micro Cloud App Security POC guide and Online Help.

1.2 Authors

This Best Practice Guide is written by Nickel Xu. Additional information was provided by the members of TMCAS Engineering group:

Zhi Zhang
Yuki Wang
Shenfeng Ding
McGrady Chen
Wendell Zhang

Jing Liu
Peter Hong
Iceking Chen
Scott Zheng
Stan Yang

1.3 Pre-requisites

This Best Practice Guide covers the basic administration procedures for CAS as well as common industry technologies. The readers and course participants must have the following knowledge to fully understand the content:

- Good knowledge of the CAS functions and administration (the CAS Online Help may be used as an information source.)
- Basic knowledge of the Microsoft Azure administration
- Good knowledge of Office 365 Exchange online, SharePoint/One Drive Online administration
- Good knowledge of Google Drive, Box and Dropbox
- Good knowledge of the HTTP, HTTPS, and SMTP protocols
- Basic knowledge of VLAN technology
1.4 Abbreviations and Terms

The table below decodes many of the abbreviations used throughout this document. The abbreviations listed include acronyms and other linguistic shortenings of names, along with certain code words, file- and folder-name extensions, and other short-form references.

The table also includes abbreviations not used directly in this document but may be encountered within the various log files, configuration files, file names, directory names, registry sub-keys, additional engineering documents, diagrams, and so forth that may be encountered when working with the product.

However, although this list of terms is intended to be comprehensive, due to the large number of shortenings that necessarily appear in registry entries, filenames, configuration files, and so forth, it is not complete.

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>APT</td>
<td>Advanced Persistent Threat</td>
</tr>
<tr>
<td>ATP</td>
<td>Advanced Threat Protection</td>
</tr>
<tr>
<td>ATSE</td>
<td>Advanced Threat Scan Engine</td>
</tr>
<tr>
<td>CLP</td>
<td>License Portal for Complete User Protection (CUP) Suites</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma Separated Values</td>
</tr>
<tr>
<td>DDAaaS</td>
<td>Deep Discovery Analyzer as a Service</td>
</tr>
<tr>
<td>DLP</td>
<td>Data Loss Prevention</td>
</tr>
<tr>
<td>GA</td>
<td>Global Administrator</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>HTML</td>
<td>Hyper Text Markup Language</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>JSON</td>
<td>JavaScript Object Notation</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest Algorithm 5</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role Based Access Control</td>
</tr>
<tr>
<td>RS</td>
<td>Rating Servers</td>
</tr>
<tr>
<td>SHA1</td>
<td>Secure Hash Algorithm 1</td>
</tr>
<tr>
<td>SCO</td>
<td>Service Conducting Organizer</td>
</tr>
</tbody>
</table>
### Abbreviation | Meaning
--- | ---
SPN | Smart Protection Network
SSH | Secure Shell
SSL | Secure Sockets Layer
SSO | Single Sign On
TLS | Transport Layer Security
TMCM | Trend Micro Control Manager
TMRM | Trend Micro Remote Manager
CAS | Trend Micro Cloud App Security
TMUFE | Trend Micro URL Filtering Engine
URL | Uniform Resource Locator
VA | Virtual Analyzer
WTP | Web Threat Protection

## 1.5 Conventions

The following conventions are used in this Best Practice Guide:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monospace</td>
<td>Registry, logs, configuration file parameters, commands, syntax, file names, and folder names</td>
</tr>
<tr>
<td>Tip ✅</td>
<td>Recommended configuration/actions</td>
</tr>
<tr>
<td>NOTE ⚠️</td>
<td>Brief comment or explanation</td>
</tr>
<tr>
<td>Refer to</td>
<td>References to other documents or sections of this Support Track</td>
</tr>
<tr>
<td>Warning</td>
<td>Critical actions or configurations</td>
</tr>
</tbody>
</table>
1.6 Revision

<table>
<thead>
<tr>
<th>Date Released</th>
<th>Updates/ Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/11/2017</td>
<td>Nickel Xu (TS-CN)</td>
</tr>
</tbody>
</table>
Chapter 1: Product Overview

This chapter contains an overview of the product to give the audience a bird’s eye view of the product.

1.1 How Trend Micro Cloud App Security Works

Trend Micro Cloud App Security provides advanced protection for Microsoft Office 365 services, Box, Dropbox, and Google Drive, enhancing security with powerful enterprise-class threat and data protection control. Cloud App Security provides protection against phishing and Business Email Compromise (BEC) scams, zero-day and hidden malware, and unauthorized transmission of sensitive data.

Cloud App Security integrates cloud-to-cloud with Exchange Online, SharePoint Online, OneDrive for Business, Box, Dropbox and Google Drive to maintain high availability and administrative functionality.

- For email services, scanning occurs when an email message arrives at a protected mailbox.
- For other cloud applications, scanning occurs when a user uploads, creates, synchronizes, or modifies a file.

Below is an illustration on how Cloud App Security works:
1.2 How Cloud App Security Protects Your Data Privacy

Cloud App Security ensures that your data is protected and used in a transparent manner, while providing advanced protection for cloud applications such as Office 365 services, Box, Dropbox and Google Drive.

The efforts to implement privacy and data protection measures fall into the following areas:

- Cloud App Security follows mature and stringent product development processes, and utilizes industry-leading tools and methodologies to perform source code defect scan and vulnerability scan. Professional penetration tests are executed by Trend Micro InfoSec team ensuring the service itself is robust yet secure.

- It stores data in the multi-tenant environment using the solid database service, and applies access control policies that protect sensitive information from unauthorized access. In a mature multi-tenant SaaS architecture, sufficient security checks are adopted to ensure data security, data segregation, and to prevent access to data of one tenant by users from other tenants.

- Cloud App Security is designed by taking a "privacy by design" approach. This is an approach to projects which promotes privacy and data protection compliance from the start. Cloud App Security does not store your data during scanning, and stores quarantined objects within your own cloud application storage.

- At the same time, cache data that Cloud App Security builds is just a hash value and cannot be converted back to original email messages or files. Cloud App Security communicates with supported cloud applications using web services over HTTPS.

- Cloud App Security is hosted on Microsoft Azure in Azure's West US, West Europe and Japan East data centers.

- Its cloud sandbox is hosted on Trend Micro data centers that are certified by ISO 27001. Currently, Cloud App Security in the U.S. (global) and Japan sites connects with the U.S. cloud sandbox data center, and Cloud App Security in the EU site connects with the EU cloud sandbox data center. Cloud App Security environments in different regions operate independently and are not interconnected for data privacy and sovereign considerations. Your data will always stay within your own region and cannot be replicated by other regions.

- To protect privacy during service operation, the Cloud App Security team applies mature operational practices, including management console access control, operation monitoring and auditing.

1.3 Key Features

- Maintain data privacy and control
- Find hidden malware and advanced attacks
- Scalable and high performance architecture
- Optimized for Microsoft Office 365, Box, Dropbox and Google Drive
Click [here](#) for further details and Key Features updates.

### 1.4 What’s New

Click [here](#) to see the Feature Release Information and its updates.

### 1.5 System Requirements

Click [here](#) to see the System Requirements.
Chapter 2: How to Provision

2.1 O365 Provision

This section describes how to provision Microsoft Office 365 services. "Provisioning" means both creating an account, and granting Cloud App Security the ability to access Office 365 services. Provisioning Delegate Accounts requires you to add users and make other modifications to Office 365. To simplify the process, Trend Micro recommends automatically provisioning Delegate Accounts.

2.1.1 Automatically Provisioning Delegate Account

Automatically provisioning Delegate Accounts does the following:

- Creates new Delegate Accounts based on selected Microsoft Office 365 services
- Configures required roles and other settings for the new Delegate Accounts

Click here to see the detailed steps for Auto-Provision.

2.1.2 Manual Provisioning on Exchange

For manual provisioning on Exchange, the delegate account must assigned with ApplicationImpersonation Role and Mailbox Search Role.

Click here to see the detailed steps on manually provisioning for Exchange.
2.1.3 Manually Provisioning SharePoint Online

Provision a SharePoint Online Delegate Account in Microsoft Office 365 to allow Cloud App Security to scan files stored in SharePoint Online or OneDrive for Business. Cloud App Security uses the Delegate Account to run advanced threat protection and data loss prevention scanning when files are uploaded.

Click here to see the detailed steps on manually provisioning for SP/OD.

2.2 Box Dropbox and Google Drive Provision

This section describes how to provision cloud applications such as Box, Dropbox and Google Drive. "Provisioning" means both creating an account, and granting Cloud App Security the ability to access other cloud applications.

Cloud App Security provisions authorized accounts for cloud applications through the OAuth 2.0 flow.

2.2.1 Before Provision

Before you begin provisioning, 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.

There are four ways to begin a provisioning flow:

- In the pop-up wizard that appears at your first log on, select a service that you want to protect to begin provisioning.
On the Dashboard screen, hover over the service that you want to protect and click **Provision** in the tooltip that appears.

Choose **Administration > Service Account**, click **Add**, and click the service that you want to protect.

If you have not finished provisioning last time, hover over the ring icon on the upper right of the management console and click the corresponding provision link in the **Notifications** screen that appears.
2.2.2 Provisioning a Service Account for Box

Provision a service account for Box to allow Cloud App Security to scan files, including Box Notes, stored in Box. Cloud App Security uses the service account to run advanced threat protection and data loss prevention scanning on files in Box.

Click [here](#) to see the detailed steps for Box Provision.

2.2.3 Provisioning a Service Account for Dropbox

Provision a service account for Dropbox to allow Cloud App Security to scan files stored in Dropbox. Cloud App Security uses the service account to run advanced threat protection and data loss prevention scanning on files in Dropbox.

Click [here](#) to see the detailed steps for Dropbox Provision.

2.2.4 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. Cloud App Security uses the service account to run advanced threat protection and data loss prevention scanning on files in Google Drive.

Click [here](#) to see the details steps for Google Drive Provision.
2.2.5 RMA Account

A Rights Management Services (RMS) account is an account that Cloud App Security requires to gain access to Azure RMS protected files shared in Office 365 services. Azure RMS protects your organization’s sensitive information from unauthorized access and controls how this information is used. It uses the Windows Azure Active Directory Service to enforce access restrictions on files.

Click here for steps on adding an RMS Account.

2.3 Key to Success

Most would use a simple formula to evaluate Cloud App Security effectiveness – that is after Office 365 and online Storage service built-in protection, how much additional detections and the FP rate. Trend core technology FP rate is low (according to our internal expertise and 3rd party benchmarking), so the key to success is how to maximize Cloud App Security protection.

The following product settings are strongly recommended during POC testing:

- Enable most of Cloud App Security protection.
- Enable most of Office 365 Mailboxes, SharePoint sites, OneDrive users during testing.
- Enable most of Box/Dropbox/Google Drive users during testing.
- After creating a new user, press click here to sync new users before testing.
- In case of mailbox migration from on-prem to cloud, a manual scan is needed.
- When done with RMS protection provision, go to the policy to enable the RMS protection.

Customers will NOT risk enabling more testing users or more protections during POC due to its architecture advantage—Cloud App Security have “Zero” impact customer’s mail, SharePoint/OneDrive and Box/Dropbox/Google Drive flow.
Chapter 3: Protection for Exchange Online

CAS protects Office 365 Exchange online environment using the following scan methods:

- **Real-time Scan**—scans the following Event types on Exchange online.
  
  (Refer to the Event section for detailed information of activities, which triggers CAS real-time scanning.)

<table>
<thead>
<tr>
<th>Office 365 Services</th>
<th>Event Type</th>
<th>Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Online</td>
<td>NewMail</td>
<td>All folder in Exchange Mailbox</td>
</tr>
<tr>
<td>Exchange Online</td>
<td>Created</td>
<td>Sent Items</td>
</tr>
</tbody>
</table>

- **Manual Scan**—scans selected mailbox on demand, and when triggered by Administrator from the CAS management console

**NOTE** No scheduled scan function is provided in Cloud App Security for Office 365.
3.1 Recommend Configuration for Each Feature

Advanced Spam Protection

- Configure Internal Domains
- Apply to Incoming Message
- Detection level for Medium

Malware Scanning

- Apply to all messages
Web Reproduction

- Apply to Incoming Message
- Detection level for Medium
- Scan Message Attachments

Virtual Analyzer

- Apply to Incoming Message
3.2 Ransomware Protection

Ransomware can spread via email by attaching itself directly or pasting malicious URL on the body of the email.

This article shows you the correct settings of Web Reputation (WRS) and Virtual Analyzer (VA) features on ATP policy of TMCAS to prevent Ransomware infection.

To detect Ransomware, make sure that the following features of TMCAS have these settings:

- **Web Reputation**
  
  ![Web Reputation Settings]

  Note: Make sure that “Scan message attachment content for suspicious URLs” is checked.

- **Malware Scanning**
  
  ![Malware Scanning Settings]

- **Virtual Analyzer**
Once these settings are enabled, TMCAS will track the number of infections that were blocked. The number and statistics of Ransomware can be found on the TMCAS Dashboard.

3.3 Smart Protection for Forged Email

Trend Micro Cloud App Security provides enhanced protection for the mentioned hosted services, enhancing security with powerful enterprise-class threat and data protection control. It provides protection against spam, phishing and Business Email Compromise (BEC) scam, zero-day and hidden malware, and unauthorized transmission of sensitive data.

TMCAS can stop the following forged mail attack, as well as detect the internal compromised mails.

- Forged Message From
- Cousin Domain Abuse
- Free Email Account Abuse
- Compromised Email Account

To prevent forged email attacks, it is recommended enable both Advanced Spam Protection, Web Reputation and Data Loss Prevention.
Advanced Spam Protection

1. Go to TMCAS admin console and navigate to Advanced Threat Protection.

2. Select Enable Advanced Spam Protection.

3. Configure the Internal Domains.

4. Configure High Profile Users.

5. Configure Rules settings:
   Select the scope of email messages that Advanced Spam Protection applies to <All Messages>.

   Note: “Incoming messages” means that this policy applies only to incoming email messages sent from non-internal domains.

6. Select a detection level for Medium. The detection level may be adjusted later on as needed based on the amount of spam attacks received.

7. Configure Approved Sender list (optional).

8. Configure the Action settings for each spam category.
   For the BEC, phishing, and ransomware spam categories, the default action is Quarantine. For other spam types, it is Move to Junk Email folder.

10. Save the settings.

### Web Reputation

1. Go to TMCAS admin console and navigate to **Advanced Threat Protection**.

![Advanced Threat Protection](image)

2. Select **Enable Web Reputation**.

![Enable Web Reputation](image)

   Select the scope of email messages that **Web Reproduction** applies to `<All Messages>`.
Note: “Incoming messages” means that this policy applies only to incoming email messages sent from non-internal domains.

4. Select a detection level for Medium. The detection level may be adjusted based on the company’s preference and the amount of false positive or false negatives.

Note: It is also recommended to check the “Scan message attachment content for suspicious URLs”.

5. Configure Approved Sender List settings (optional).

6. Configure Approved URL List settings (optional).

7. Configure the Action to “Quarantine” (recommended).


9. Save the settings.

Data Loss Prevention

1. Go to Data Loss Prevention > Add > Add Exchange Online Policy.

2. Configure policy settings:
   - General
• **Data Loss Prevention**

3. If you have configured multiple policies for one service, adjust policy priorities as required.
   a. Select a policy and use the arrow change its priority.
   b. Drag a policy and place it to the desired priority.

4. Click **Save**.
Chapter 4: Data Loss Protection

With the prevalence and damaging effects of data breaches, organizations now see digital asset protection as a critical component of their security infrastructure. Data Loss Prevention safeguards an organization’s sensitive data against accidental or deliberate leakage.

Data Loss Prevention allows you to:

- Identify the sensitive information that requires protection using data identifiers
- Create policies that limit or prevent the transmission of digital assets through common transmission channels, such as email messages and uploaded files
- Enforce compliance to established privacy standards
4.1 Define an DLP Identifier

There are two kinds of data identifier in DLP:

- Keyword
- Regular expression

Examples:

- A work file which contains Trend Micro Keyword
- A text which looks like xxxx-xxxx-xxxx-xxxx, where x is all made from 0 ~ 9 Regular expression: `[^\d](\d{4}-\d{4}-\d{4}-\d{4})[^\d]`

4.1.1 Define “Keyword” Data Identifier

1. Log on to Cloud App Security console. Go to Data Loss Prevention > DLP Identifiers.

2. Input keyword in Keyword field and click Add. One or more keywords can be created. It can be defined to meet any keyword, all keywords or All keywords within <x> characters (see details below). Combined score for keywords exceeds threshold.
• **Any keyword**: A file must contain at least one keyword in the keyword list that will trigger the DLP policy.

• **All keywords**: A file must contain all the keywords in the keyword list that will trigger the DLP policy. For mail file, DLP will combine subject, body, attachment violation together to trigger policy.

• **All keywords within <x> characters**: A file must contain all the keywords in the keyword list. In addition, each keyword pair must be within <x> characters of each other.

Combined score for keywords exceeds threshold:

• A file must contain one or more keywords in the keyword list. If only one keyword is detected, its score must be higher than the threshold. If there are several keywords, their combined score must be higher than the threshold.

• Assign each keyword a score of 1 to 10. A highly confidential word or phrase, such as "salary increase" for the Human Resources department, should have a relatively high score. Words or phrases that, by themselves, do not carry much weight can have lower scores.

• Consider the scores that you assigned to the keywords when configuring the threshold. For example, if you have five keywords and three of those keywords are high priority, the threshold can be equal to or lower than the combined score of the three high priority keywords. This means that the detection of these three keywords is enough to treat the file as sensitive.
3. After keywords are all added, click **Save** to finish the keyword data identifier creation.

### Data Identifiers

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Sample : Trend Micro</td>
<td>Words commonly associated with the adult entertainment industry, including pornographic websites</td>
<td>User Defined</td>
</tr>
<tr>
<td>Adult</td>
<td>Terms used by hospitals and other health care providers</td>
<td>Predefined</td>
</tr>
<tr>
<td>Common Medical Terms</td>
<td>Common use of the (First), (Middle) and (Last Name) fields in documents such as forms</td>
<td>Predefined</td>
</tr>
<tr>
<td>Forms: (First), (Middle), Name</td>
<td>Common use of the [Birth Date], [Birthdate], or [Date of Birth] fields in documents such as forms</td>
<td>Predefined</td>
</tr>
</tbody>
</table>

### 4.1.2 Define “Regular Expression” Data Identifier

1. Go to **Data Loss Prevention > DLP Identifiers > Expression** and click **Add**.

   **Basic Properties**
   
   **Name**: A Sample : Regular Expression
   
   **Expression**: `[^\d-]\d{4}-\d{2}-\d{2}-\d{2}-\d{2}\]^\d-\[

   **Displayed data**: `0000-0000-0000-0000`

   **Examples**: `1111-2222-3333-4444`

   **Validation**: None

   **NOTE** Criteria contains another type (specific characters, suffix, Single-char separator)

2. If the expression works, click **Save**.
<table>
<thead>
<tr>
<th>Test Area</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Test data:</strong></td>
</tr>
<tr>
<td><strong>Test result:</strong></td>
</tr>
</tbody>
</table>
4.2 DLP Template Definition

A DLP Template is composed of one or multiple data identifier and their relationship.

Example:

A work file which contains Trend Micro or a text which looks like xxxx-xxxx-xxxx-xxxx keyword or regular expression.

Predefined Compliance Template

1. Log on to Cloud App Security console. Go to Data Loss Prevention > Compliance Templates.

<table>
<thead>
<tr>
<th>Compliance Template</th>
<th>Name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Adult</td>
<td>Words commonly associated with the adult</td>
<td></td>
<td>Predefined</td>
</tr>
</tbody>
</table>
Defining a Customized Template

1. Go to Data Loss Prevention > Compliance Templates and click Add.

   Compliance Template

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adult</td>
<td>Words commonly associated with the adult entertainment industry, including</td>
<td>Predefined</td>
</tr>
<tr>
<td></td>
<td>pornographic websites</td>
<td></td>
</tr>
<tr>
<td>Albania: International Bank Account Number</td>
<td>An international standard for identifying bank accounts with minimal risk of</td>
<td>Predefined</td>
</tr>
<tr>
<td></td>
<td>transcription errors</td>
<td></td>
</tr>
<tr>
<td>All File Extension</td>
<td>All File Extension</td>
<td>Predefined</td>
</tr>
<tr>
<td>All Personally Identifiable Information</td>
<td>Information that can be used singly or with other sources to uniquely</td>
<td></td>
</tr>
<tr>
<td>(English)</td>
<td>identify, contact</td>
<td></td>
</tr>
</tbody>
</table>

2. Choose a data identifier customized (Expression or Keyword), or use a predefined data identifier, and set the Operator (And, Or) to set the relationship.

   Add Compliance Template

   Basic Properties
   
   Template Name*: A Sample Template
   
   Description:

   Rule Definitions

   Define rules for this template's keywords and expressions, then click Add.

   Template Rules

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OR</td>
<td>A Sample: Regular Expression</td>
</tr>
</tbody>
</table>

3. Click Save. A compliance template will be created.
4.3 Define a DLP Policy

The DLP rules that a data administrator can control are classified into three parts:

- **Template** - the critical data
- **Action** - If a violation is found, how to handle the data is determined.
- **Notification** - If a violation is found, how to send notification is determined.

To perform this:

1. Go to **Data Loss Prevention > Add**. Select the policy to create based on the service:

   - Add Exchange Online Policy
   - Add SharePoint Online Policy
   - Add OneDrive for Business Policy
   - Add Box Policy
   - Add Dropbox Policy
   - Add Google Drive Policy
2. Type the policy name and description. You may enable Real-time Scanning if this policy is used in a real-time scan.

3. Select targets using the check boxes on the left pane, and click Save.

4. A policy will be created. Enable this policy optionally by turn on the left tab.

4.4 Data Loss Prevention Criteria

- One user matches only one policy.
- The default policy is used if no other policy has been created for the user. If there is a specific policy for a user, the default policy will lose efficacy.
- If multiple policies are defined for a user, only the highest priority policy takes effect.
- The smaller the policy number, the higher the priority is. The policy priority can be changed by dragging the policy up and down.
- For sent items in Exchange Online, CAS only records the violation. It cannot take Quarantine or Delete actions for the items.
• Short length keyword terms like “anal” might cause violation when matched to word “analysis” which is not an adult-sensitive word.

Chapter 5 Administration

5.1 Scan Logs

The CAS console provides a place to view the audit and scan logs collected from different CAS server roles.

5.1.1 Log Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Risk Scan</td>
<td>Information about messages with security risks based on pattern matching. Advanced threat protection scanning policies includes Security Risk Scan and Virtual Analyzer events.</td>
</tr>
<tr>
<td>Virtual Analyzer</td>
<td>Information about the message attachments and files scanned and heuristically analyzed for threats in a virtual sandbox. Advanced threat protection scanning policies includes Security Risk Scan and Virtual Analyzer events.</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>Information about messages and files that triggered Data Loss Prevention policy incidents</td>
</tr>
<tr>
<td>Quarantine</td>
<td>Information about messages and files quarantined due to threats or policy violations</td>
</tr>
</tbody>
</table>
5.1.2 Reports

Cloud App Security provides log reports to assist in mitigating threats and optimizing system settings. Generate reports on demand or set a daily, weekly, or monthly schedule based on log search results.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Logs</td>
<td>Information about user log-on sessions, policy change events, and other management events</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report</td>
<td>Generate a one-time report. This report shows static data, based on the log search results.</td>
</tr>
<tr>
<td>Template</td>
<td>Create a report template that can be viewed anytime. This report shows dynamic data, based on the time a report generates.</td>
</tr>
<tr>
<td>Scheduled Report</td>
<td>Create a report that generates at a recurring time. This report shows static data, based on log search results and the time frame.</td>
</tr>
</tbody>
</table>

5.2 Service Account

Cloud App Security protects:

- Microsoft Office 365 services, including Exchange Online, SharePoint Online and One Drive for Business
- Other cloud applications, including Box, Dropbox and Google Drive

Cloud App Security requires service accounts to integrate with the services that it protects. The service accounts can be categorized as:

- Delegate accounts to integrate with Office 365 services
- Authorized accounts to integrate with other cloud applications

Cloud App Security requires an RMS account to get access to and scan RMS-protected files for those services it protects.
5.3 Users and Roles

In addition to the administrator who has full access to the management console, Cloud App Security supports customizing roles to grant limited access to users or groups who need to perform tasks. This enables more fine-grained, role-based access control, and lowers the risk of corporate data exposure to attackers.

Cloud App Security comes with a default administrator role and up to four custom roles that you can create to fit the specific needs of your organization. Cloud App Security role-based access control provides the following:

- Define a role by specifying permissions to it and an option to add users or groups to this role.
- Create a user account by adding a user and assigning an appropriate role to it.
- Only a user with the administrator role can add a user account, create a custom role, and assign users or groups to the role.
5.3.1 User Management

Users can enter an email address or enter a name to search in the Active Directory. Once done, an existing role may be assigned or a new one may be defined.

Cloud App Security sends an email message to notify the user how to reset the password for the user account.

After logging on to the Cloud App Security management console, the user will be redirected to the first allowed page based on the permissions of the assigned role.

5.3.2 Role Management

Instead of providing only the administrator role with unrestricted permissions, you can allow only certain actions. For example, a role may be specified to let a user view and manage only the Advanced Threat Protection policies, while another can view the existing Data Loss Prevention policies without having the ability to edit them.
From the drop-down list, the administrator may specify either full control or view only.

- **View only**: Users can view the existing ATP or DLP policies, query logs and reports, or view quarantined messages and files, without the ability to edit them.

- **Full control**: Users can view and manage ATP or DLP policies, logs and reports, or quarantined messages and files.

Take note that the users created on the Users screen and the Azure AD users and groups (if an Exchange Online Delegate Account is provisioned), are displayed under Available Targets.

**NOTE** A maximum of 20 users can be assigned to a role.
When an Azure AD group is selected, all the users that belong to the group (rather than the group itself), are added and displayed under Selected Targets.
5.4 Dashboard

Monitor your network integrity with the dashboard. Each management console user account has an independent dashboard. Changes made to one user account dashboard do not affect other user account dashboards.

Widgets represent the core dashboard components. They contain visual charts and graphs that allow you to track threats and associate them with the logs accumulated from log sources.

Each dashboard section contains widgets that capture specific data.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware</td>
<td>Shows ransomware detection statistics such as the total number of detections, top five ransomware email senders, top five ransomware domains, and top five ransomware detected in files</td>
</tr>
<tr>
<td>Summary</td>
<td>View widgets that show security risk summary over selected time periods.</td>
</tr>
<tr>
<td>Advance Threat Protection</td>
<td>View security risks based on signature-based scanning method (Security Risk Scan) and heuristic analysis (Virtual Analyzer for Suspicious Objects). Security Risk Scan refers to the three security filters: malware scanning, file blocking, and web reputation.</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>View violations by policy, compliance template, destination, and source.</td>
</tr>
</tbody>
</table>

5.5 License

5.5.1 What happens to an expired license

A 30-day grace period is extended to an account whose license is expired. During the grace period, everything is kept the same as before where Exchange, SharePoint and One Drive are under CAS’s protection with the latest engine and Pattern loaded.

Beyond the grace period, the CAS account turns to a “locking” status, and no one is allowed to log in. CAS automatically cleans up a company after the grace period is over.
* Disables all policies
* Stops scheduled tasks
* Removes SPOD event receivers
* Cleans up CAS added data in Office 365
* DB data cleanup after 90 days

### 5.5.2 How to extend an account

When an account currently uses a trial license, and attempts to buy an official license, TrendMicro strongly recommends extending the original account (instead of opening a new account). Otherwise, a case should be filed to the Trend Micro support team to clean the registered Office 365 information from CAS’s back-end database.

### Chapter 6: Central Manager Integration

Trend Micro Control Manager 6.0 SP3 Patch 1 or above supports Cloud App Security. Cloud App Security integrates with Control Manager. It includes the following features and capabilities if managed from Control Manager:

* Single Sign-On (SSO) access to the Cloud App Security management console from the Control Manager console
* Virus information for Control Manager on the Threat Detection Results widget
* Current Cloud App Security connection status
* Query scanning logs submitted by Cloud App Security

**NOTE** Currently, Cloud App Security submits only Malware scanning, Date Loss Prevention, File Blocking, Web Prevention, Virtual Analyzer (exclude URL Sandbox Log) to Control Manager.
6.1 Registering with Control Manager

Make sure you have a Customer Licensing Portal account, and it is integrated both with Cloud App Security and Control Manager.

1. In Control Manager, go to Administration > Manager Servers.
3. Click Cloud Service Settings.
4. Specify your Customer Licensing Portal account credentials and click OK.

The Cloud App Security server appears in the Managed Servers list.

6.2 Single Sign On with Control Manager

Below would be the steps to perform single sign on with Control Manager:

1. In Control Manager, go to Administration > Managed Servers.
3. Under Server, click the server address.

The Dashboard screen of the Cloud App Security management console opens in a new browser tab.
6.3 Checking Service Status in Control Manager

Below are the steps to check the server status in Control Manager.

1. In Control Manager, go to the Dashboard.
2. Click the Summary tab.
3. Scroll down and find the Product Connection Status widget.

You can check the status of any Cloud App Security server registered with Control Manager.

6.4 Querying Logs with Control Manager

Cloud App Security virus logs are available in Control Manager. Below are the steps to check logs using Control Manager.

1. In Control Manager, go to Logs > Log Query. A Data Scope screen appears.
2. Select Product Tree.
4. Expand the data view list to go to Security Threat Information:
   - Malware Log: System Events > Virus/Malware detections
   - Virtual Analyzer log: System Events > Virtual Analyzer Detections
   - Web Reputation/File Blocking log: Network Events > Content Violation
Chapter 7: Troubleshooting

7.1 Uploaded Eicar file in Office 365 SharePoint is not detected by Cloud App Security

To find out the cause of the issue, check the information below:

There are two ways to create a SharePoint site:

From Office 365

1. Log on to Office 365, then click SharePoint.
2. Click Create Site.
3. Provide the information requested, and proceed with creating the site.

From Central Administration

1. Go to Admin Centers > SharePoint.
2. Click New to create a new site collection.

The issue happens when SharePoint site is created through Office 365, because TMCAS can only hook to a SharePoint site that is created from the Central Administration.
7.2 Manual provision for SharePoint and OneDrive by Cloud App

Security fails

Doing a manual provision results to failure for SharePoint and OneDrive, and is only successful in Exchange.

TMCAS provision process will be improved in the future. In the meantime, do the following as a workaround:

1. Log on to the Office 365 portal, then click **Admin**.

2. Under Admin Centers, click **SharePoint**.
3. Click **Device Access**.

SharePoint admin center

**site collections**

- infopath
- user profiles
- bcs
- term store
- records management
- search
- secure store
- apps
- sharing
- settings
- configure hybrid

**device access**

- [https://stan10stg.sharepoint.com](https://stan10stg.sharepoint.com)
- [https://stan10stg.sharepoint.com/portals/hub](https://stan10stg.sharepoint.com/portals/hub)
- [https://stan10stg.sharepoint.com/search](https://stan10stg.sharepoint.com/search)
- [https://stan10stg-my.sharepoint.com](https://stan10stg-my.sharepoint.com)
4. Select **Allow**, and save.

5. Wait for about 30 minutes before adding the service account again.

### 7.3 Types of SharePoint Sites Supported by Cloud App Security

When signing up for Office 365 SharePoint, the list of all the site collections in your organization can be seen. All the site collections in SharePoint Online either start or contain the domain name by default.
Skipped Sites

The SharePoint Protection of TMCAS does not support the following two types of SharePoint Site:

- Special Purpose Sites
  - companyname.sharepoint.com/portals/hub
  - companyname.sharepoint.com/search
  - companyname.sharepoint.com/sites/CompliancePolicyCenter

**NOTE**: these sites are default site collections, it should not have risk.

Supported Sites

Except for the items mentioned under the Unsupported Sites section, TMCAS SharePoint protection supports the rest of the admin site collections and sub sites.
7.4 Files are not protected by the SharePoint Protection of Cloud App Security

After a successful SharePoint Provision, malicious files are not detected, and the TMCAS policies are not working.

This happens because the "Require check-out of file" option had been enabled on the SharePoint Site. This option causes uploaded files to be checked-out. Once the files are checked-out, only the uploader can see or access them.

Because of the access restrictions applied to the files when they are checked-out, TMCAS will not be able to find or scan them.

To allow TMCAS to scan the file(s), do the steps below:

1. Login to the SharePoint site.

2. Go to Settings > Library settings.
3. Click Versioning settings.

4. Scroll to the bottom, then set the "Require documents to be checked out before they can be edited?" option to Yes.

5. Enable a TMCAS policy, then upload a file.

6. Click the file option, then click Check in.
After completing these steps, TMCAS will be able to scan the file, even when the check-out option is enabled.

Appendix I: Script to Identify O365 Customer

The objective of the script is to help discover whether customer has been on Microsoft Office 365 (O365) in Cloud App Security (TMCAS).
To know if customer is on O365

1. Edit the email-list.txt.

2. Run the powershell script: ./mslookup.ps1

3. The script will print out the O365 domain.

```powershell
PS E:\Document\CAS\mxlookup\mxlookup> .\mxlookup.ps1

Cmdlet mxlookup.ps1 at command pipeline position 1
Supply values for the following parameters:
(Type ?? for Help.)
FilePath: E:\Document\CAS\mxlookup\mxlookup\email-list.txt

Found 4 email address
Found 4 valid domains

Printing Office365 domain list:

outlook.com
```
Cloud App Security retrieves data from Windows Azure Active Directory and Office 365 services when provisioning service accounts.

The following table lists all the data that Cloud App Security retrieves from the Office 365 environment.

| Windows Azure Active Directory | • Names of all domains  
|                                | • Display names of all users  
|                                | • User Principal Names (UPNs) of all users  
|                                | • License status of all users  
|                                | • Display names of all groups  
|                                | • Types of all groups  
|                                | • Relationships between users and groups, and between groups  
| Exchange Online                | • Creation time of all mailboxes on the Microsoft Exchange Server  
|                                | • Primary SMTP addresses of all mailboxes  
|                                | • Types of all mailboxes  
| SharePoint Online              | • URLs of all SharePoint site collections and their subsites  
|                                | • Descriptions of all SharePoint site collections and their subsites  

<table>
<thead>
<tr>
<th>OneDrive for Business</th>
<th>• Relationships between site collections and subsites</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• IDs of all OneDrive for Business users</td>
</tr>
<tr>
<td></td>
<td>• Descriptions of all OneDrive for Business users</td>
</tr>
<tr>
<td></td>
<td>• URLs of all OneDrive for Business user sites</td>
</tr>
</tbody>
</table>
# Appendix III: Deployment Criteria

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td>CAS automatically synchronizes new users daily at midnight, so before CAS syncs the user, this user isn’t protected by CAS. To sync up the users immediately, suggest to synchronize the new users first before testing.</td>
</tr>
</tbody>
</table>

CAS adopts an API-based architecture rather than a proxy-based architecture to provide advanced protection. It starts scanning when an email message arrives at a protected mailbox or a file is saved to cloud storage. This unique API-based architecture guarantees that Cloud App Security has "zero impact" on your email message delivery or file sharing as well as commitments defined in your service level agreements. First, it can be seen that the mail is delivered to the inbox:

![Email inbox](image1)

After a short time, CAS took action on the mail:

![Email inbox with action](image2)

If one policy is added or updated, it takes one or two minutes to synchronize the change before the updated policy takes effect. CAS only scans the new mail for exchange, it will not scan calendar.  

**Malware Scanning**

To improve the performance, CAS will not add the product tag in the mail header after the mail scanned by CAS. Mail subject doesn't support malware scanning.
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAS</td>
<td>If a user attaches a malware file to “attach as an OneDrive file”, CAS will detect malware from OneDrive; but if attached from OneDrive as shared link, the file will not be detected.</td>
</tr>
<tr>
<td></td>
<td>CAS has a 150MB size limitation for mail attachment or file.</td>
</tr>
<tr>
<td></td>
<td>Compressed file limitation:</td>
</tr>
<tr>
<td></td>
<td>• The number of extracted files exceeds 9999.</td>
</tr>
<tr>
<td></td>
<td>• The size of extracted files exceeds 100 MB.</td>
</tr>
<tr>
<td></td>
<td>• The number of recursive compression layers exceeds 5.</td>
</tr>
<tr>
<td>File Blocking</td>
<td>CAS uses the full name to trigger the policy. Use the full name or use * instead of the extension.</td>
</tr>
<tr>
<td></td>
<td>• If the target is test.txt, put the full name “test.txt”.</td>
</tr>
<tr>
<td></td>
<td>• If the target is for all files named test, add “test.*”. All files named “test”, whatever the file extension, will still hint the policy.</td>
</tr>
<tr>
<td>Web Reputation</td>
<td>To scan the URL in attachment, check message attachments item. This setting is unchecked by default.</td>
</tr>
<tr>
<td>Virtual Analyzer</td>
<td>CAS will use the SHA1 to query the DDASaaS cache. If the file matches SHA1, it will not send to DDASaaS again instead of getting the last result directly.</td>
</tr>
<tr>
<td></td>
<td>The default timeout value for DDAn is 30mins.</td>
</tr>
<tr>
<td></td>
<td>DDA analysis timeout or network timeout, or unsupported file type will present “unrate” in the VA report.</td>
</tr>
<tr>
<td>DLP</td>
<td>One user matches only one policy.</td>
</tr>
<tr>
<td></td>
<td>The default policy is used if no other policy has been created for the user. If there is a specific policy for a user, the default policy will lose efficacy.</td>
</tr>
</tbody>
</table>
If multiple policies are defined for a user, only the highest priority policy takes effect.

The smaller the policy number, the higher the priority is. The policy priority can be changed by dragging the policy up and down.

If one policy is added or updated, it takes one or two minutes to synchronize the change before the updated policy takes effect.

For sent items in Exchange Online, CAS only records the violation. It cannot take Quarantine or Delete actions for the items.

Short length keyword terms like “anal” may cause a violation when it matches the word “analysis”, which is not an adult-sensitive word.

<table>
<thead>
<tr>
<th>Manual Scan</th>
<th>Removes VA support</th>
</tr>
</thead>
</table>

**Manual Scan trial control**
- A user cannot select a period longer than 1 day.
- Limited to 25 mailboxes for exchange
- Limited to 5 SharePoint sites for SharePoint
- Limited to 5 users for OneDrive/Box/Dropbox/Google Drive

**Notification**

To send to multiple recipients, use “;”.

<table>
<thead>
<tr>
<th>Notify Administrator</th>
<th>Notify User</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To: nickel_us@trendmicro.com.cn;nickel@test.com
Appendix IV: Known Issues

Email messages with "Do not forward" flag are not scanned.

If a user composing an email chooses the “Do not forward” option from Options > Permission, Cloud App Security cannot scan email message contents.

Automatic provisioning of Microsoft Office 365 services fails.

If multi-factor authentication (MFA) is enabled in Office 365 services, Cloud App Security does not support automatic provisioning of Exchange online, SharePoint online and OneDrive for Business. To complete provisioning, either disable MFA or use the manual provisioning procedure.

This issue does not affect Box, Dropbox and Google Drive.

Newly added users do not immediately appear on the Exchange Policy configuration page.

After registering Cloud App Security, newly added users will not immediately appear on the Exchange policy configuration page. Click Click here if you do not see new users when you create/update the Exchange Online policy. The page automatically updates after Cloud App Security synchronizes with Active Directory once per day.

Newly added SharePoint site does not appear immediately on the SharePoint Policy Configuration page.

After registering Cloud App Security, newly added SharePoint sites will not immediately appear on the SharePoint policy configuration page. Click Click here if you do not see new sites when you create/update the SharePoint Online policy. The page automatically updates after Cloud App Security synchronizes with SharePoint Online once per day.

Newly added OneDrive, Box, Dropbox or Google Drive users do not appear immediately on the OneDrive, Box, Dropbox or Google Drive Policy configuration page.

After registering Cloud App Security, newly added OneDrive for Business, Box, Dropbox or Google Drive users will not immediately appear on the OneDrive, Box, Dropbox or Google Drive policy configuration page. Click Click here if you do not see new OneDrive for Business, Box, Dropbox or Google Drive users when you create or update the OneDrive for Business, Box, Dropbox or Google Drive policy. The page automatically updates after Cloud App Security synchronizes with OneDrive for Business, Box, Dropbox or Google Drive once per day.