Best Practice Guide (BPG) Security Compliance Report Tutorial

Trend Micro

Content

- Objectives
- Security Compliance Report Content and Sample Report
- Recommended Process Steps
- How to Submit a BPG Support Case via Partner Portal
- Recommended Solutions/Opportunities to Discuss with Customers
  - Leverage BPG Report to Discuss Upgrade Opportunity with Customer
- Support Resources

Objectives

- This high-level security compliance report is intended to provide an overview of the customer current status of Trend Micro Apex One™ / Trend Micro™ OfficeScan™ deployment compared with the Trend Micro recommendations of best practice.
- By discussing the security compliance report results with customers, you will be able to generate the upgrade or services opportunity.
- Target Products: Apex One, OfficeScan

Security Compliance Report Content

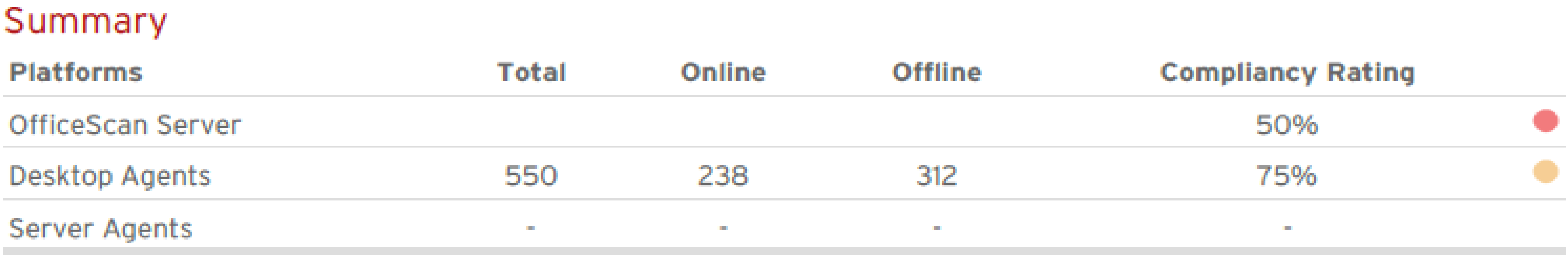
- Security compliance report outlines the current status of endpoints protected by Apex One / OfficeScan and make recommendations specifically targeted at increasing the overall security posture for customers' implementation.
- Security compliance report provides the following information:
  - Recommendations about how to improve the network security provided by Apex One.
  - An overview of the currently deployed Apex One agent versions.
  - An assessment of the current Apex One server build compliance and the availability of hotfixes, patches, or enhancements.
  - An overview of the protected operating systems.

Security Compliance Report Content

Details include:

- OfficeScan agent policy compliance
- Available hotfixes/patches by severity
- Recommended security settings

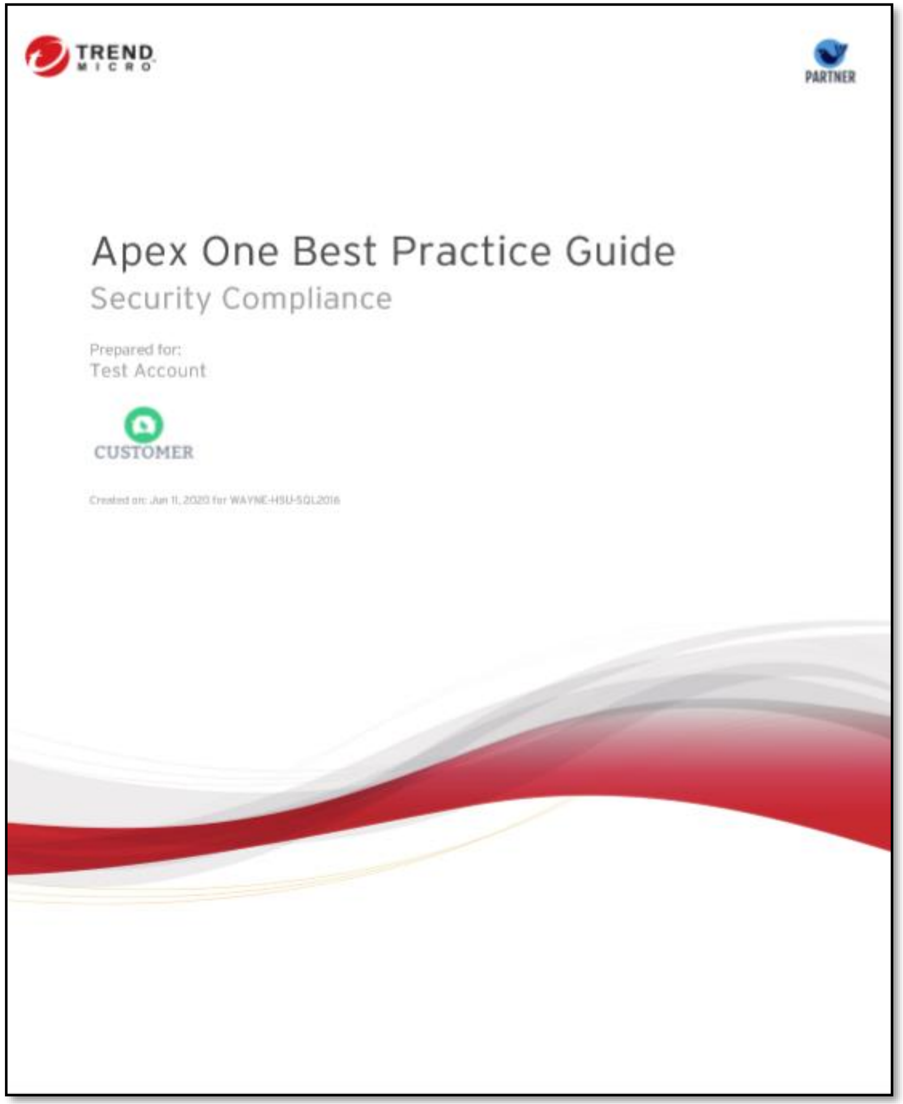
- Provide executives summary score
- Compliancy
- Deployment scope
- Policy recommendations
- Patch/Upgrade recommendations



Summary

Platforms	Total	Online	Offline	Compliancy Rating	
OfficeScan Server				50%	●
Desktop Agents	550	238	312	75%	●
Server Agents	-	-	-	-	

Best Practice Guide – Sample Report (1/2)

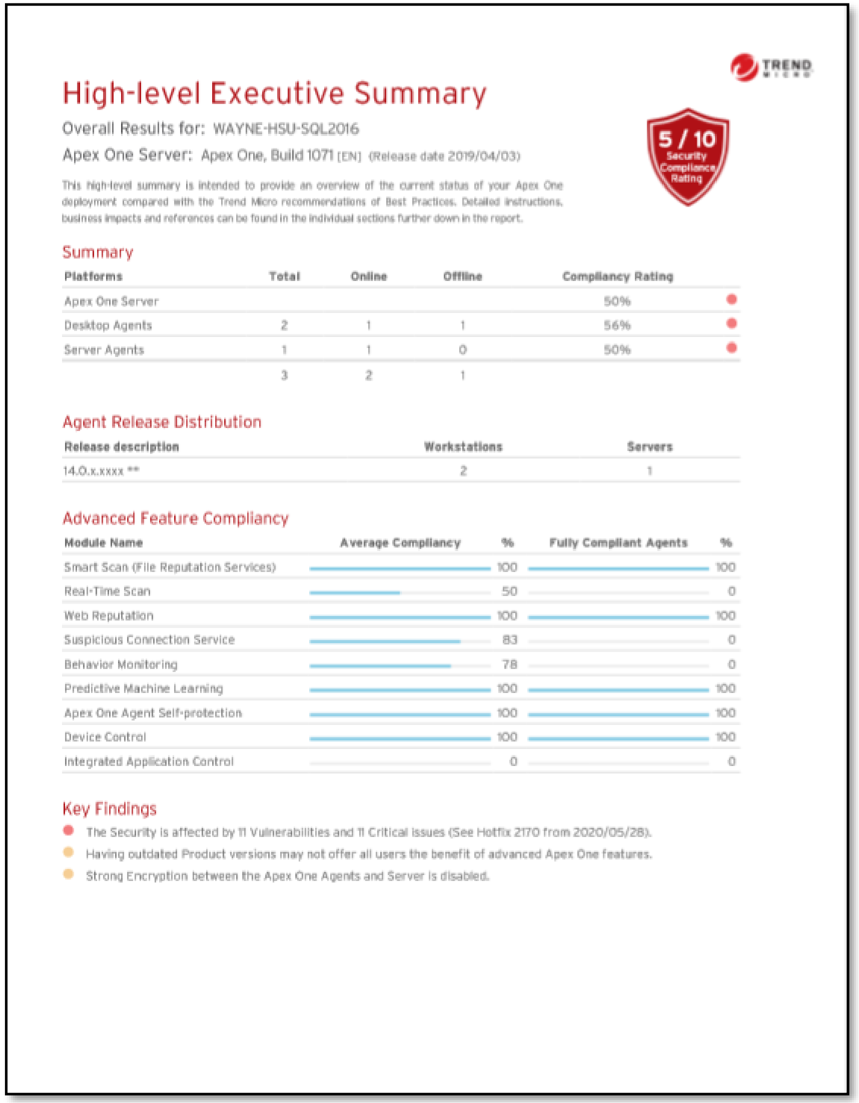


Apex One Best Practice Guide

Security Compliance

Prepared for:
Test Account

Created on: Jun 11, 2020 for WAYNE-HSU-SQL2016



High-level Executive Summary

Overall Results for: WAYNE-HSU-SQL2016

Apex One Server: Apex One, Build 1071 [EN] (Release date 2019/04/03)

5 / 10 Security Compliance Rating

This high-level summary is intended to provide an overview of the current status of your Apex One deployment compared with the Trend Micro recommendations of Best Practices. Detailed instructions, business impacts and references can be found in the individual sections further down in the report.

Summary

Platforms	Total	Online	Offline	Compliancy Rating	
Apex One Server				50%	●
Desktop Agents	2	1	1	56%	●
Server Agents	1	1	0	50%	●
	3	2	1		

Agent Release Distribution

Release description	Workstations	Servers
14.0.x.xxxx **	2	1

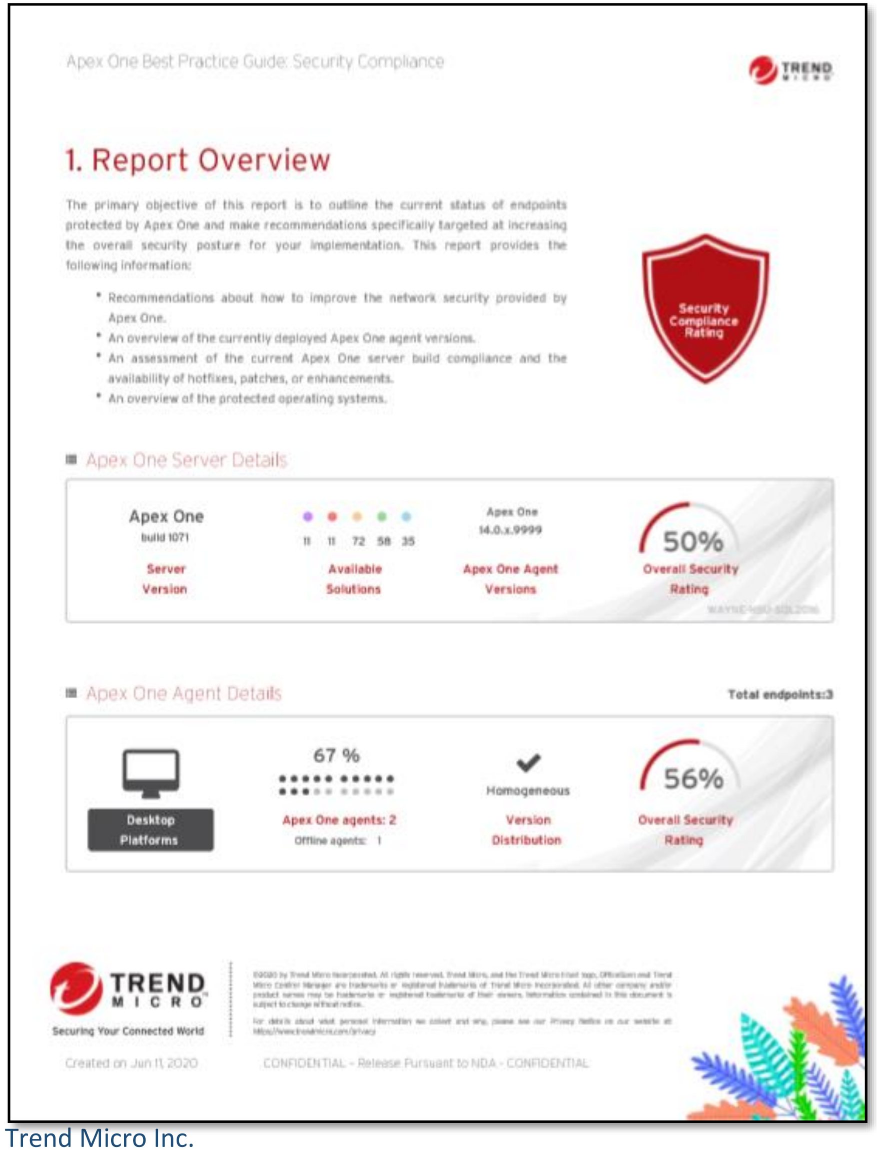
Advanced Feature Compliancy

Module Name	Average Compliancy	%	Fully Compliant Agents	%
Smart Scan (File Reputation Services)		100		100
Real-Time Scan		50		0
Web Reputation		100		100
Suspicious Connection Service		83		0
Behavior Monitoring		78		0
Predictive Machine Learning		100		100
Apex One Agent Self-protection		100		100
Device Control		100		100
Integrated Application Control		0		0

Key Findings

- The Security is affected by 11 Vulnerabilities and 11 Critical issues (See Hotfix 2170 from 2020/05/28).
- Having outdated Product versions may not offer all users the benefit of advanced Apex One features.
- Strong Encryption between the Apex One Agents and Server is disabled.

Best Practice Guide – Sample Report (2/2)



Apex One Best Practice Guide: Security Compliance

1. Report Overview

The primary objective of this report is to outline the current status of endpoints protected by Apex One and make recommendations specifically targeted at increasing the overall security posture for your implementation. This report provides the following information:

- Recommendations about how to improve the network security provided by Apex One.
- An overview of the currently deployed Apex One agent versions.
- An assessment of the current Apex One server build compliance and the availability of hotfixes, patches, or enhancements.
- An overview of the protected operating systems.

Apex One Server Details

Apex One build 1071	● ● ● ● ● 11 11 72 58 35	Apex One 14.0.x.9999	50%
Server Version	Available Solutions	Apex One Agent Versions	Overall Security Rating

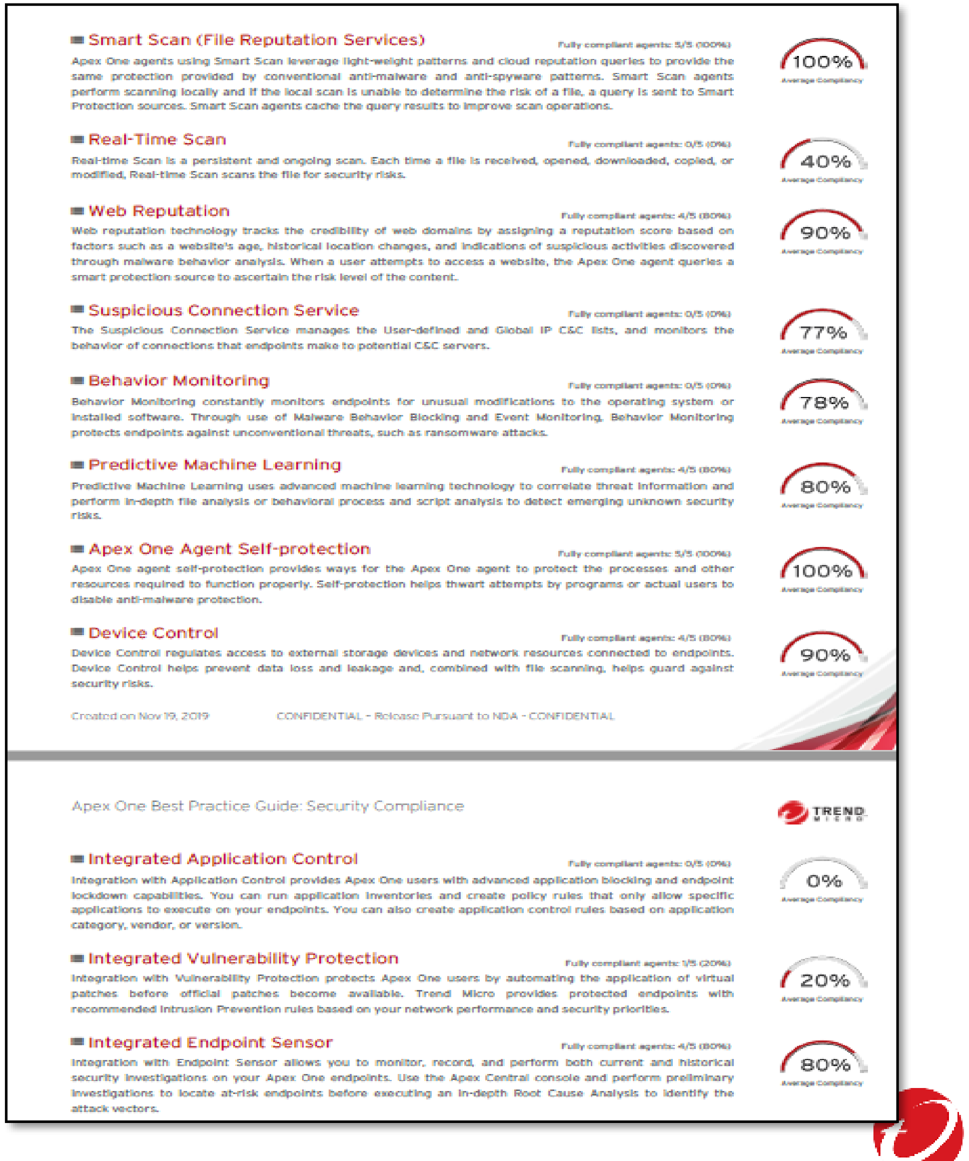
Apex One Agent Details

Total endpoints:3

	67 % Apex One agents: 2 Offline agents: 1	✓ Homogeneous	56%
Desktop Platforms		Version Distribution	Overall Security Rating

TREND MICRO
Securing Your Connected World

Created on Jun 11, 2020 CONFIDENTIAL - Release Pursuant to NDA - CONFIDENTIAL



Smart Scan (File Reputation Services)

Fully compliant agents: 5/5 (100%)

Apex One agents using Smart Scan leverage light-weight patterns and cloud reputation queries to provide the same protection provided by conventional anti-malware and anti-spyware patterns. Smart Scan agents perform scanning locally and if the local scan is unable to determine the risk of a file, a query is sent to Smart Protection sources. Smart Scan agents cache the query results to improve scan operations.

100% Average Compliancy

Real-Time Scan

Fully compliant agents: 0/5 (0%)

Real-time Scan is a persistent and ongoing scan. Each time a file is received, opened, downloaded, copied, or modified, Real-time Scan scans the file for security risks.

40% Average Compliancy

Web Reputation

Fully compliant agents: 4/5 (80%)

Web reputation technology tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes, and indications of suspicious activities discovered through malware behavior analysis. When a user attempts to access a website, the Apex One agent queries a smart protection source to ascertain the risk level of the content.

90% Average Compliancy

Suspicious Connection Service

Fully compliant agents: 0/5 (0%)

The Suspicious Connection Service manages the User-defined and Global IP C&C lists, and monitors the behavior of connections that endpoints make to potential C&C servers.

77% Average Compliancy

Behavior Monitoring

Fully compliant agents: 0/5 (0%)

Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or installed software. Through use of Malware Behavior Blocking and Event Monitoring, Behavior Monitoring protects endpoints against unconventional threats, such as ransomware attacks.

78% Average Compliancy

Predictive Machine Learning

Fully compliant agents: 4/5 (80%)

Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis or behavioral process and script analysis to detect emerging unknown security risks.

80% Average Compliancy

Apex One Agent Self-protection

Fully compliant agents: 5/5 (100%)

Apex One agent self-protection provides ways for the Apex One agent to protect the processes and other resources required to function properly. Self-protection helps thwart attempts by programs or actual users to disable anti-malware protection.

100% Average Compliancy

Device Control

Fully compliant agents: 4/5 (80%)

Device Control regulates access to external storage devices and network resources connected to endpoints. Device Control helps prevent data loss and leakage and, combined with file scanning, helps guard against security risks.

90% Average Compliancy

Created on Nov 19, 2019 CONFIDENTIAL - Release Pursuant to NDA - CONFIDENTIAL

Apex One Best Practice Guide: Security Compliance

Integrated Application Control

Fully compliant agents: 0/5 (0%)

Integration with Application Control provides Apex One users with advanced application blocking and endpoint lockdown capabilities. You can run application inventories and create policy rules that only allow specific applications to execute on your endpoints. You can also create application control rules based on application category, vendor, or version.

0% Average Compliancy

Integrated Vulnerability Protection

Fully compliant agents: 1/5 (20%)

Integration with Vulnerability Protection protects Apex One users by automating the application of virtual patches before official patches become available. Trend Micro provides protected endpoints with recommended Intrusion Prevention rules based on your network performance and security priorities.

20% Average Compliancy

Integrated Endpoint Sensor

Fully compliant agents: 4/5 (80%)

Integration with Endpoint Sensor allows you to monitor, record, and perform both current and historical security investigations on your Apex One endpoints. Use the Apex Central console and perform preliminary investigations to locate at-risk endpoints before executing an in-depth Root Cause Analysis to identify the attack vectors.

80% Average Compliancy

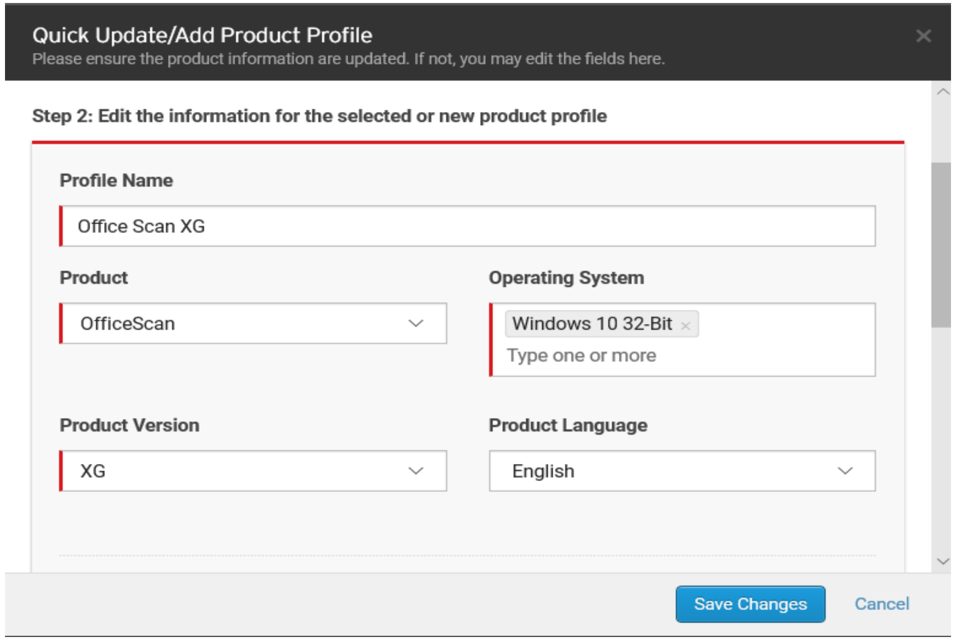
Recommend Process Steps

- Leverage "Best Practice Guide - Customer Presentation Slide" to brief customers.
- Sign agreement with customer if customer is willing to perform the assessment.
- Download the Extraction Tool.
- Login to partner portal and submit a support case for "compliancy report". Read the KB: How to Generate a Best Practice Guide Report for Apex One or OfficeScan for detailed step by step of case submission.
- Compliance report will be generated by Trend Micro after submission. The status of the support case can be checked in MySupport -> Support Requests. Once the report has been generated, you will receive an email to indicate it is available for download and review. The report in PDF file can be found under Support Requests -> File Attachments.
- For Trend Micro Apex One™ SaaS customers, please open a support ticket and one of our Customer Support Engineers will help to generate the Compliancy Report on customer Apex One SaaS instance for you.
- Review the report for upgrade or service opportunity. You can reference the KB: How to create a BPG Report and use the Trend Micro Apex One Migration Checklist.
- Discuss the report results with your customers for the action plan.
- Submit the Deal Registration through partner poral and note the code "BPG Compliance Report" to gain additional discount.

How to Submit a BPG Support Case via Partner Portal (1/2)

Read the KB: How to Generate a Best Practice Guide Report for Apex One or OfficeScan for detailed steps of case submission.

1. Login to partner portal and create a new support request.
2. Enter the Customer Account details.
3. Select “Add a new profile” and enter the desired name.
   - Select OfficeScan in the product section.
4. Download the extraction tool and run it on your OfficeScan server.
5. Unzip and execute the ExtractionTool_v4.0.exe. Further instructions are included in the README.txt. Follow the onscreen prompts to complete.



Quick Update/Add Product Profile

Please ensure the product information are updated. If not, you may edit the fields here.

Step 2: Edit the information for the selected or new product profile

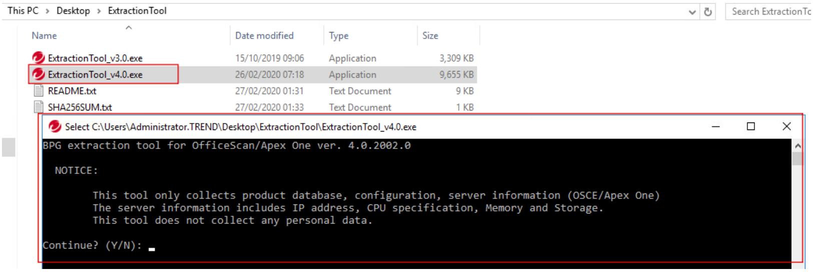
Profile Name: Office Scan XG

Product: OfficeScan

Operating System: Windows 10 32-Bit ×
Type one or more

Product Version: XG

Product Language: English



Name	Date modified	Type	Size
ExtractionTool_v3.0.exe	15/10/2019 09:06	Application	3,309 KB
ExtractionTool_v4.0.exe	26/02/2020 07:18	Application	9,655 KB
README.txt	27/02/2020 01:31	Text Document	9 KB
SHA256SUM.txt	27/02/2020 01:33	Text Document	1 KB

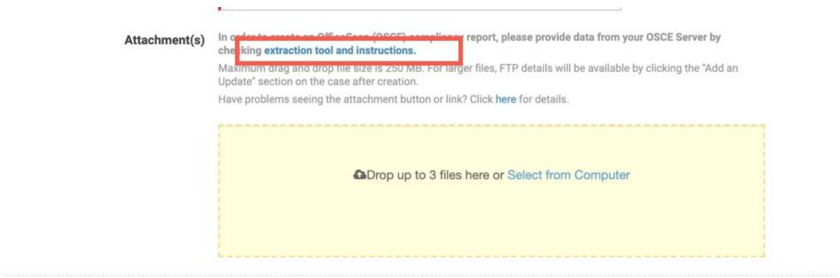
Select C:\Users\Administrator.TREND\Desktop\ExtractionTool\ExtractionTool_v4.0.exe

```
BPG extraction tool for OfficeScan/Apex One ver. 4.0.2002.0

 NOTICE:

        This tool only collects product database, configuration, server information (OSCE/Apex One)
        The server information includes IP address, CPU specification, Memory and Storage.
        This tool does not collect any personal data.

Continue? (Y/N): _
```



Attachment(s): In order to create an OfficeScan (OSCE) compliancy report, please provide data from your OSCE Server by checking extraction tool and instructions.

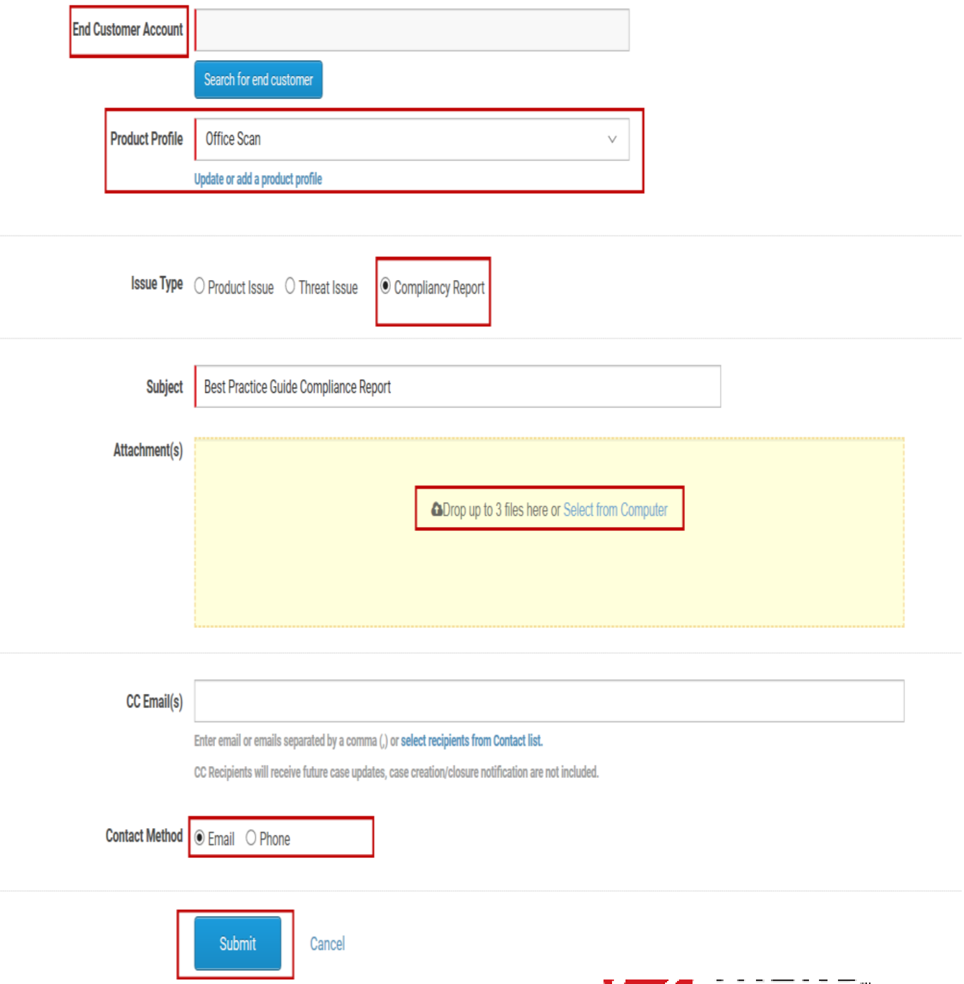
Maximum drag and drop file size is 250 MB. For larger files, FTP details will be available by clicking the "Add an Update" section on the case after creation.

Have problems seeing the attachment button or link? Click here for details.

How to Submit a BPG Support Case via Partner Portal (2/2)

Read the KB: How to Generate a Best Practice Guide Report for Apex One or OfficeScan for detailed steps of case submission.

6. After a few minutes, it will complete the compliancy scan of OfficeScan server. It will create a zipped folder.
7. Upload the resulting files in the section shown.
8. Enter the email address at where you wish to receive the report.
9. Click Submit.
10. The "Request Sent" pop-up message will appear informing you that a new Support Case has been created, including the case number.
11. Once the report has been generated you will receive an email to indicate that it is available for download and review.



End Customer Account

Search for end customer

Product Profile: Office Scan

Update or add a product profile

Issue Type: ○ Product Issue ○ Threat Issue ● Compliancy Report

Subject: Best Practice Guide Compliance Report

Attachment(s): Drop up to 3 files here or Select from Computer

CC Email(s)

Enter email or emails separated by a comma (,) or select recipients from Contact list.

CC Recipients will receive future case updates, case creation/closure notification are not included.

Contact Method: ● Email ○ Phone

Submit Cancel

Recommended Solutions/Opportunity to Discuss with Customers

- Upgrade to the latest version
- Switch to a suite that has additional features
- Professional Services (to assist with upgrade)
- Trend Micro™ XDR Add-on
- Trend Micro™ MDR Service
- Connected Threat Defense - Trend Micro™ Deep Discovery ™

Leverage BPG Report to Discuss Upgrade Opportunity with Customer - Using the Apex One Migration Checklist

After creating the BPG report, click **Section 4** to go directly to the Apex One Upgrade Checklist.

Section 4.1	Checks your operating system to see if it is supported by Apex One and if HTTPS is enabled.
Section 4.2	Checks your agents and make sure that the operating systems of your endpoints are supported by Apex One. It lists which operating systems you have that are not supported, and notes beside each OS if there is a version or patch of the operating system that is supported. This section also states whether the OfficeScan Agent Version supports migration to Apex One or not.
Section 4.3	Checks your SQL Server. If you wish to use Apex One with Endpoint Sensor, it will show if your SQL Server Version is compatible and confirms if your SQL Server Browser and SQL TCP/IP are both enabled. Endpoint Sensor requires that SQL Full Text Search is enabled.

Support Resources

- Trend Micro Assessments and Best Practices Fact Sheet
- Customer Agreement for Performing BPG Compliance Report
- Support email: partnersupport@trendmicro.com
- KB: Step-by-step help to submit a support case – compliancy report through partner portal
  - How to Generate a Best Practice Guide Report for Apex One or OfficeScan
- KB: Helps you read the BPG compliance report and upgrade to Apex One
  - How to create a BPG Report and use the Trend Micro Apex One Migration Checklist

THE ART OF CYBERSECURITY

Trend Micro deployment shifts over time—from on-premises to SaaS-based solutions. **Created with real data by artist Stefanie Posavec.**