Check Point
SOFTWARE TECHNOLOGIES LTD.

ONE STEP AHEAD

SandBlast Agent POC Quick Start Guide

December 2017

Introduction to SandBlast Zero-Day Protection

With emerging threats increasingly targeting endpoints, organizations require security that keeps pace with modern business demands. SandBlast Agent **proactively** defends endpoints with a complete set of real-time advanced protection technologies and software blades. Those include:

- Threat Extraction , Threat Emulation and Anti Exploit
- Anti-Ransomware
- Anti-Exploit (available for E80.71. Contact your local SE)
- Anti-Bot
- Zero Phishing
- Automated Incident Analysis

Preparation for POC

Which vectors and assets do you want to protect? These are the blades you need:

a. Network– Threat Emulation, Threat Extraction, Anti-Malware, Anti-Bot, Anti-Exploit Firewall and Application control
b. Data safety – Anti-Ransomware
c. Document security – Capsule Docs
d. Peripheral devices /Removable media - Media Encryption and Port Protection
e. Full Visibility – Check Point Forensics

Recommendations and requirements

- Always use the latest version of SandBlast Agent
- Have an endpoint AV solution deployed (Check Point or 3rd party)
- Contact your Check Point local representative

Contents

Topology Configurations

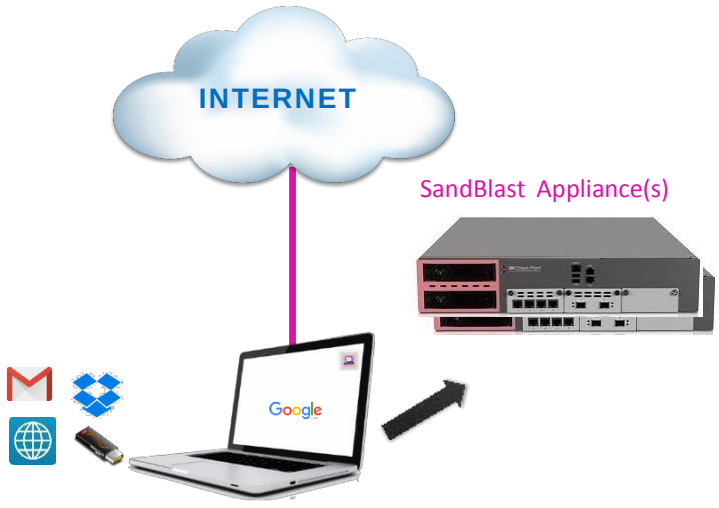
Topology 1 - Cloud

Check Point SandBlast Agent with Threat Emulation and Threat Extraction in the Cloud.
Web download protection by browser extension.

Client installed with SandBlast Agent.
Immediate access to sanitized documents by browser extension.

Topology 2 - Remote

Check Point SandBlast Agent with Threat Emulation and Threat Extraction on an on-premises appliance, based on sizing. Web downloads protection by browser extension.

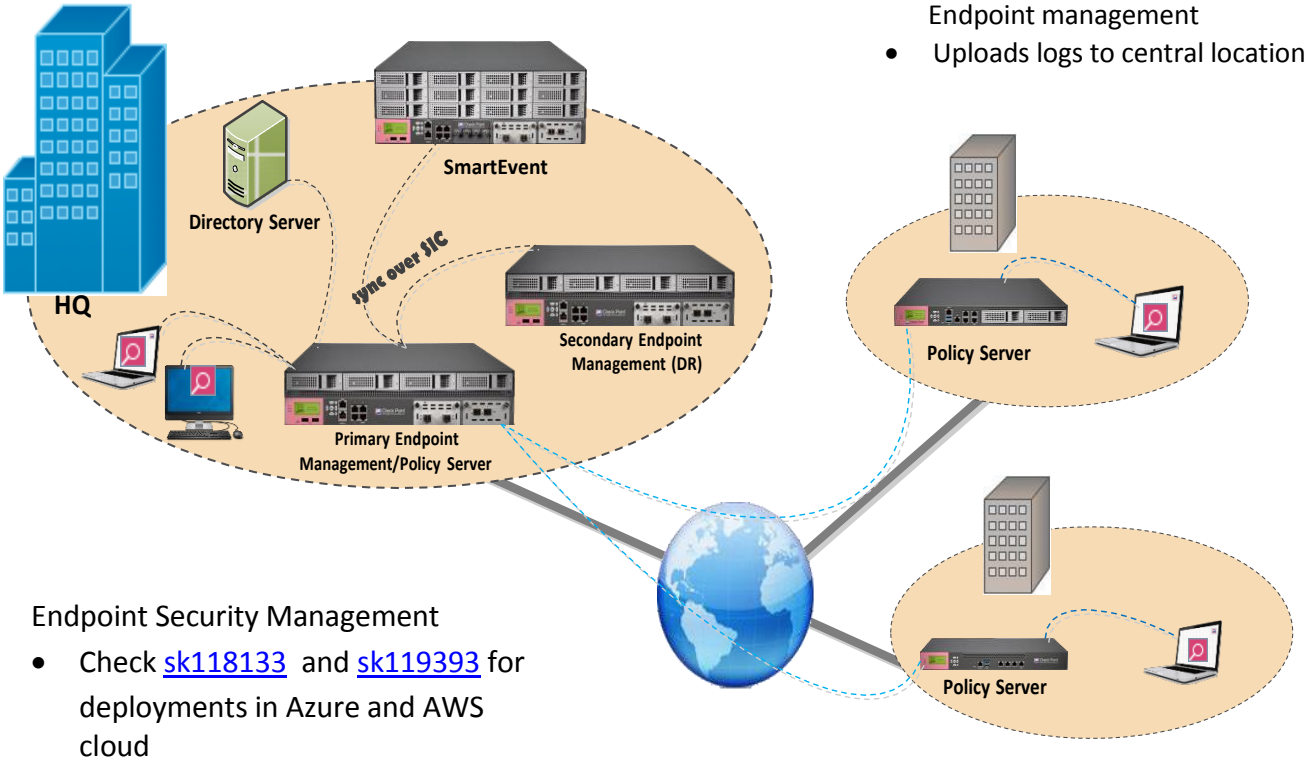


Topology 3 - Global Deployment

Check Point SandBlast Agents communicating with the closest policy server, pulling policy and uploading logs.

Policy servers

- Receives policy from primary Endpoint management
- Uploads logs to central location



Endpoint Security Management

- Check sk118133 and sk119393 for deployments in Azure and AWS cloud

SmartEvent

- Consolidates logs from all policy servers
- Provides rapid data analysis and custom event logs.
- Immediately alerts administrators to anomalous behavior

Check Point
SOFTWARE TECHNOLOGIES LTD.

ONE STEP AHEAD

SandBlast Agent Zero-Day Protection Solution

Extend zero-day protection to web-browsers and end-user devices, to defend against advanced attacks. SandBlast Agent's Zero-Day protection solution delivers these results:

- Protects endpoints from sophisticated attacks and zero-day threats
- Blocks and removes evasive ransomware infections
- Blocks unknown and zero-day phishing attacks targeting user credentials
- Prevents the misuse of corporate passwords
- Neutralizes the impact of malware infections contracted through unprotected channels, minimizing potential damages
- Enables deep understanding of security events for faster response

SandBlast Agent provides continuous data collection, automated incident analysis, and actionable forensics. You can analyze the scope of the attack, it's attack lifecycle, and damage and attack vectors, to maximize response team productivity and minimize resolution times.

SandBlast Agent Installation

To install SandBlast Agent, you must:

1. Install Endpoint Management.
2. Install the R77.30 Jumbo Hotfix for the Endpoint Security Server.
3. Install the R77.30.03 Endpoint Security Server Package for Gaia.

Endpoint Management Installation

1. Install R77.30 Gaia. See sk104859 to find the latest software installation for your platform.
   - We recommend you have a machine with hardware of 4CPU cores / 8GB RAM / 100GB HDD.
   - With the First Time Wizard, configure the machine as Security Management only.
2. See sk119676 for the latest version (R77.30.03 as of November 2017) of Endpoint security server hotfixes.
   Go to the **Endpoint Security Server Downloads** section and download:
   - R77.30 Jumbo Hotfix for Endpoint security server **and**
   - R77.30.03 Endpoint security server package for Gaia

Installing the R77.30 Jumbo Hotfix for the Endpoint Security Server

1. Connect to Endpoint management (EPM) with SSH.
2. Create a temporary directory.
3. To connect via SCP to the EPM, change the administrator default shell to bash:
   ```
   EPM > set user admin shell /bin/bash
   ```
4. Transfer the `R77.30_jhf_T143_EP.tgz` file to the temporary directory.
5. Set an expert level password:
   ```
   EPM > set expert-password <your-password>
   EPM > save config
   ```
6. Enter expert mode:
   ```
   EPM> expert
   ```
7. Go to the temporary directory that has the copied file.

8. Run these commands in expert mode; follow the on-screen instructions:
   ```
   EPM> tar -zxvf R77.30_jhf_T143_EP.tgz
   EPM> ./UnixInstallScript
   ```

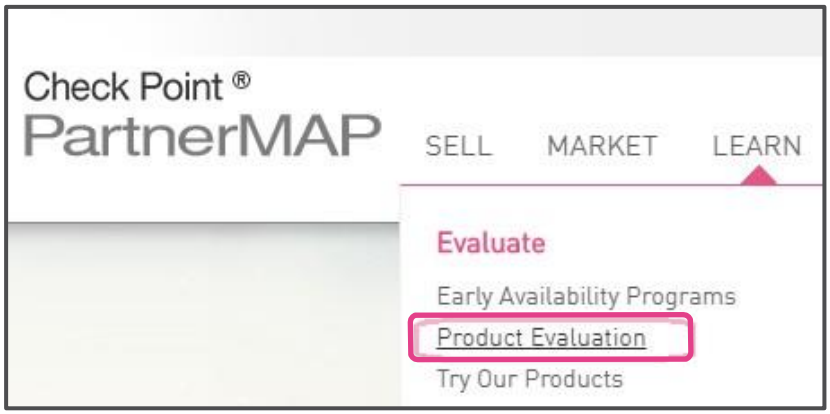
Installing the R77.30.03 Endpoint Security Server Package for Gaia

1. Connect to Endpoint management (EPM) with SSH.
2. Create a temporary directory.
3. Transfer the `R77.30.03_Gaia.tgz` file to the temporary directory.
4. Enter expert mode with the password you defined earlier:
   ```
   EPM > expert
   ```
5. Go to the temporary directory that has the copied file.
6. Run these commands in expert mode; follow the on-screen instructions:
   ```
   EPM > tar -zxvf R77.30.03.Gaia.tgz
   EPM > ./UnixInstallScript
   ```

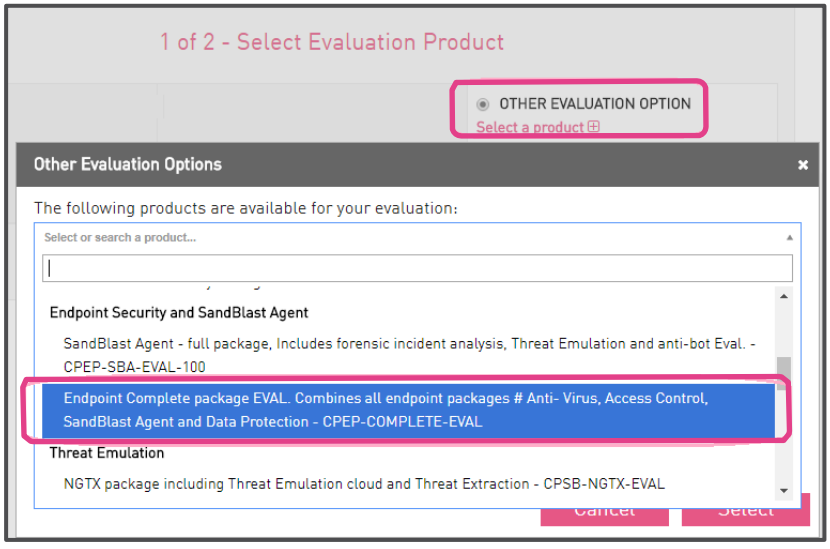
Licensing Endpoint Management

To try SandBlast Agent, go to the Check Point user center to obtain a product evaluation license.

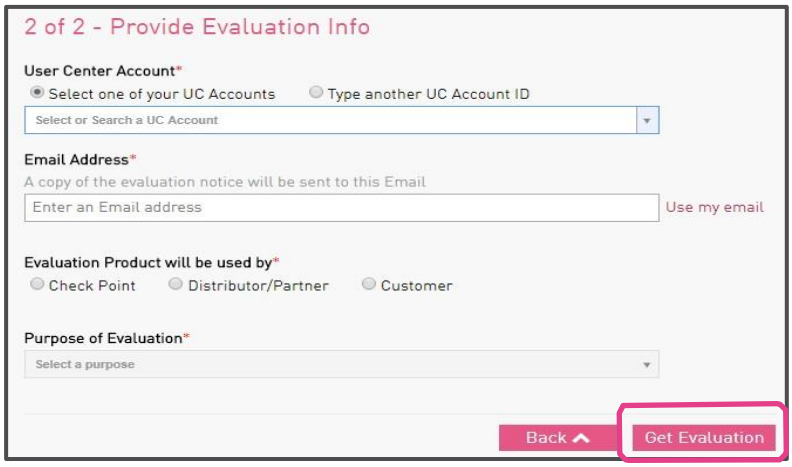
1. Go to **Learn** > **Product Evaluation**.



2. Check **Other Evaluation Option** > **Endpoint Complete package Eval** > **Select** > **Next**.



3. Enter details and click **Get Evaluation**.



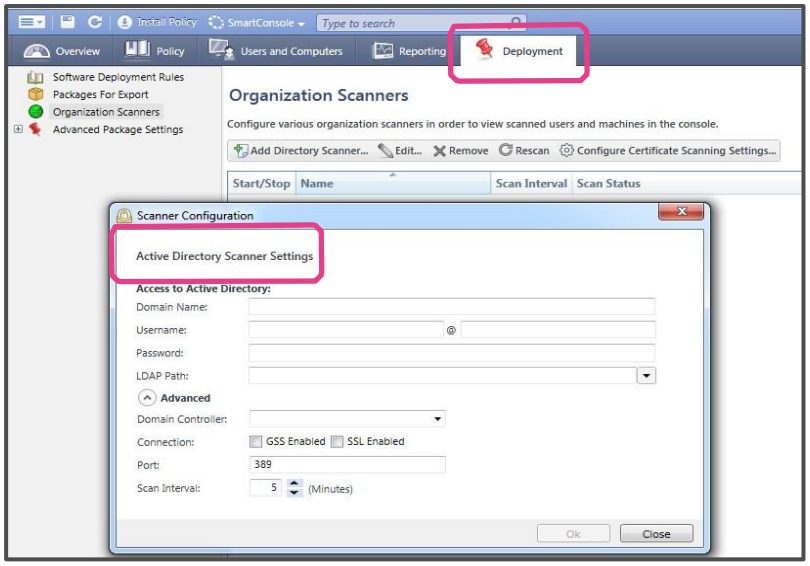
Installing the GUI Client

1. See sk119676 for the latest version of the Endpoint security server hotfixes (SmartConsole for R77.30.03/E80.71 as of November 2017) .
2. Download and install SmartConsole for Endpoint security server R77.30.03/E80.71:
   `Check_Point_SmartConsole_R77.30.03_E80.71.exe`

Adding an Active Directory Scanner

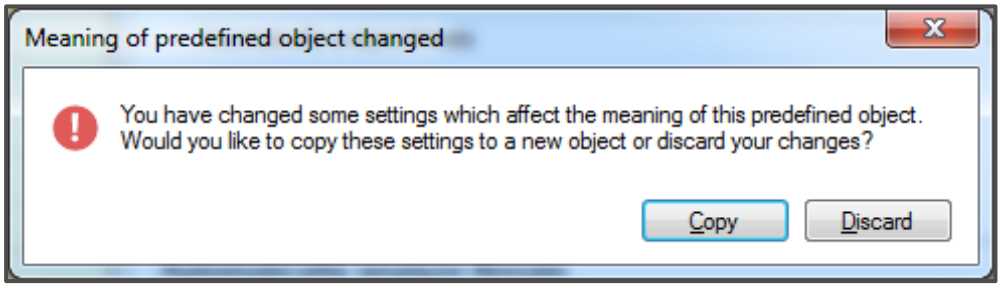
You can sync your organization Active Directory to Endpoint management. After it is synced, you can use any Active Directory entry as the **Applies To** target (similar to *destination*) for Endpoint blades and deployment rules.

1. From the Endpoint GUI, go to the **Deployment** tab > **Organization Scanners**.
2. Click **Add Directory Scanner** and enter the credentials for your domain.
   Note – Providing an Active Directory read-only user with access to the **Deleted objects container** is enough.

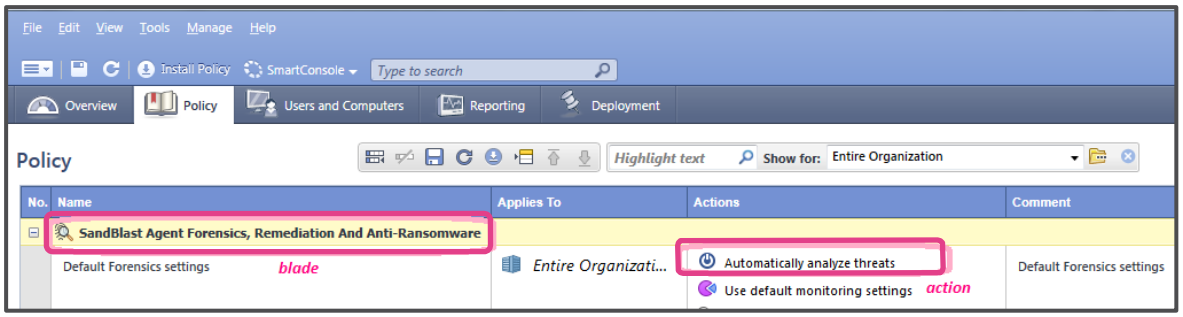


SandBlast Agent Policy Setup for Blades

To change policy, from the Endpoint SmartConsole go to the **Policy** tab > **Action** column. Change the policy by double-clicking on an action for each blade. If you try to change a predefined action, the dialog box below will show. You can save the action with a new name.

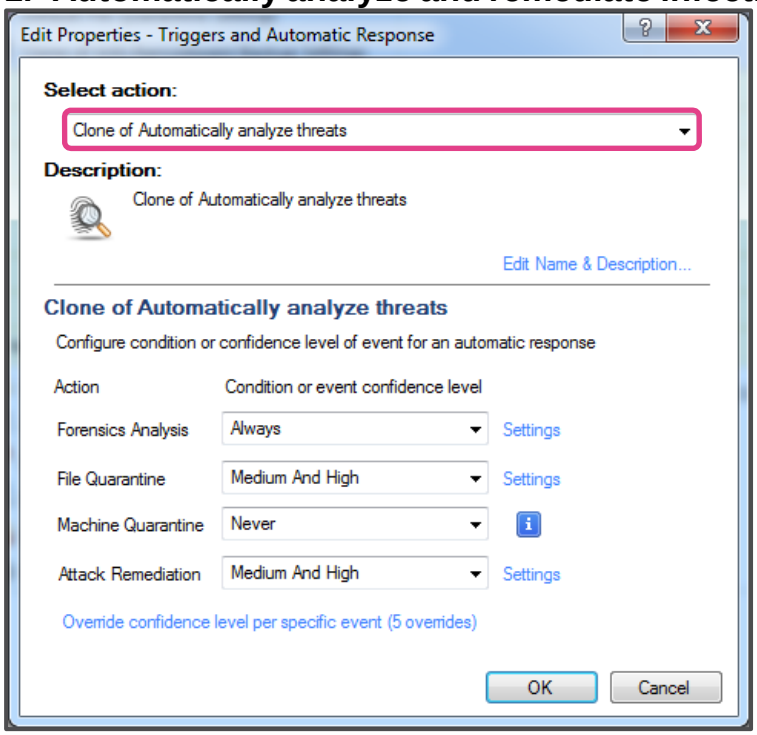


SandBlast Agent Forensic, Remediation and Anti-Ransomware Blades

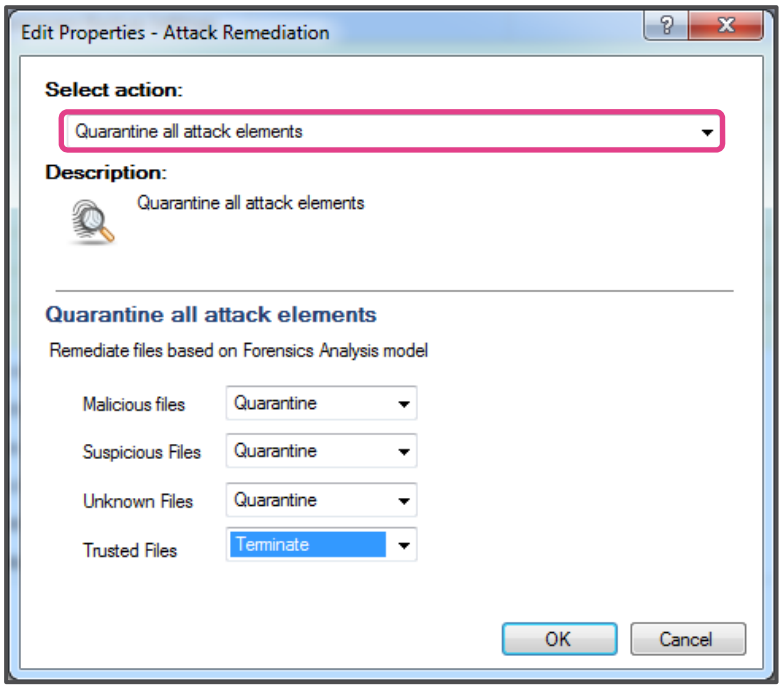


Change the Actions only. Keep the default settings for actions that you do not modify.

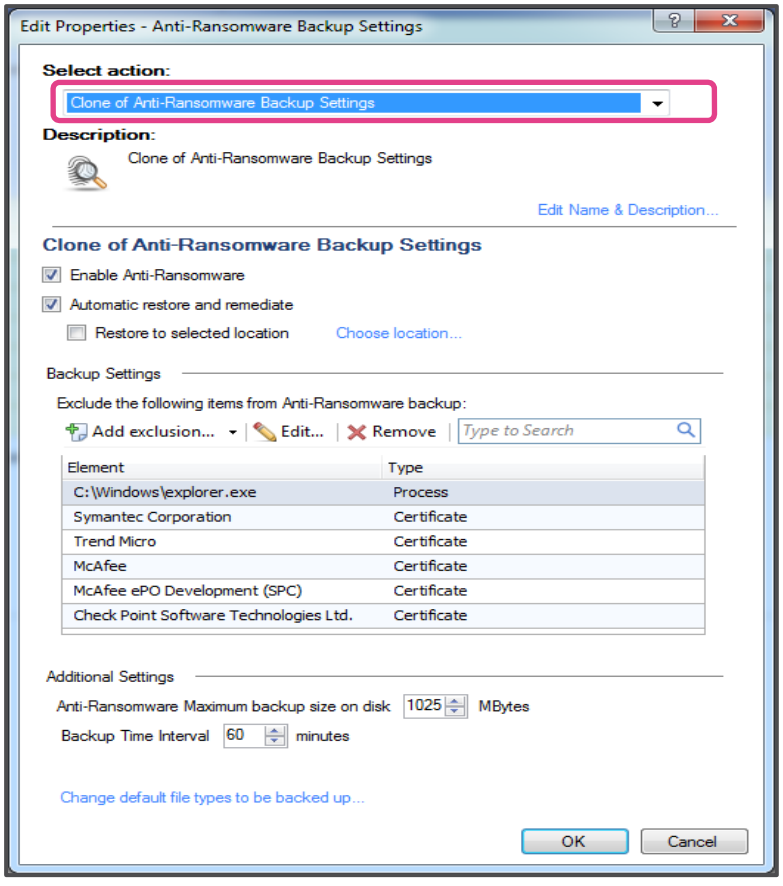
1. Automatically analyze and remediate infections



2. Quarantine all attack elements

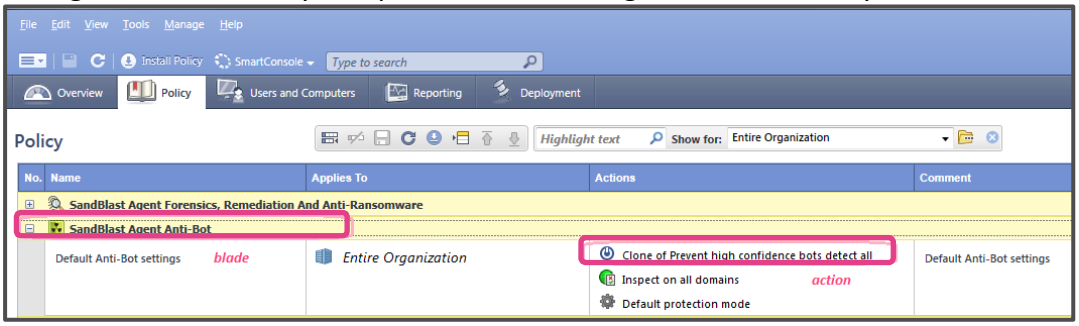


3. Anti-Ransomware backup settings

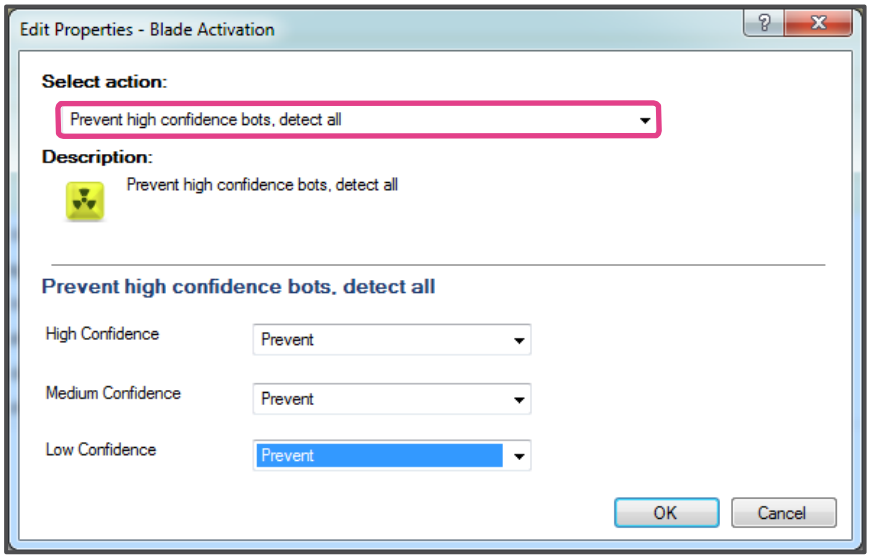


SandBlast Agent Anti-Bot Blade

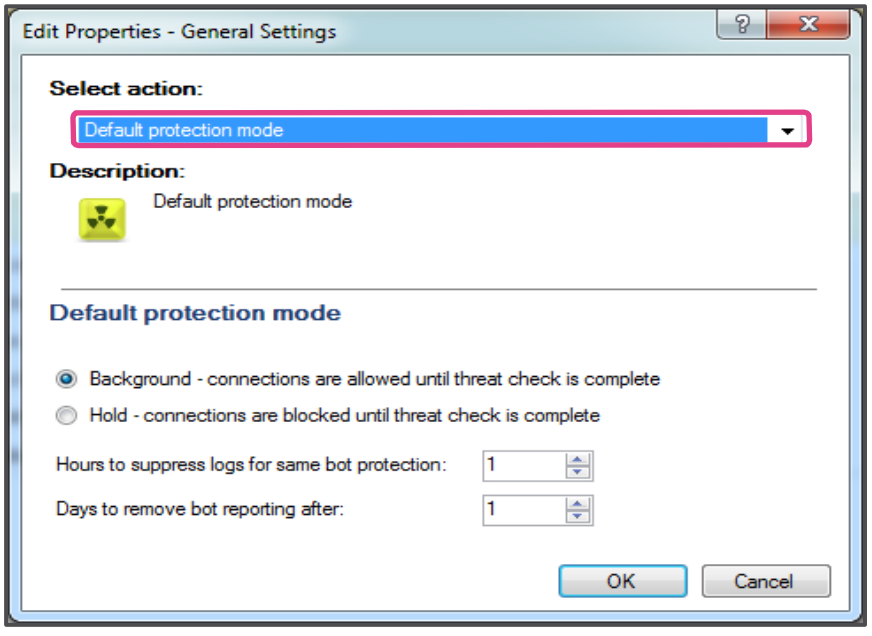
Change the Actions only. Keep the default settings for actions that you do not modify.



1. Prevent high confidence bots, detect all

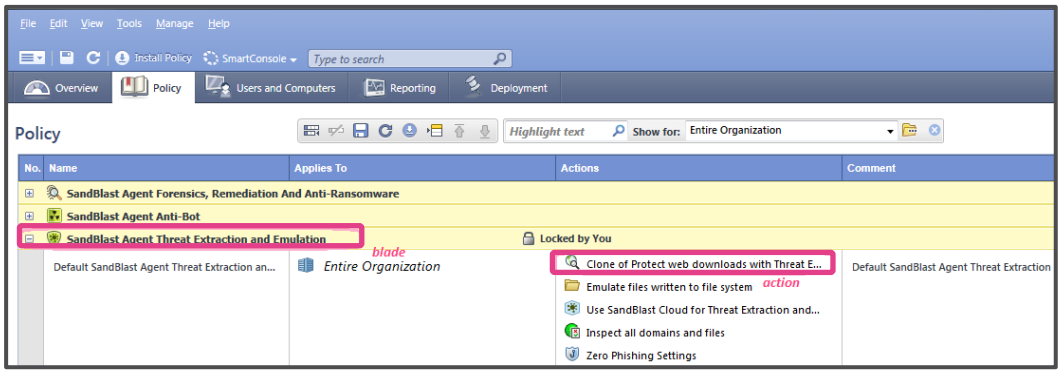


2. Default protection mode

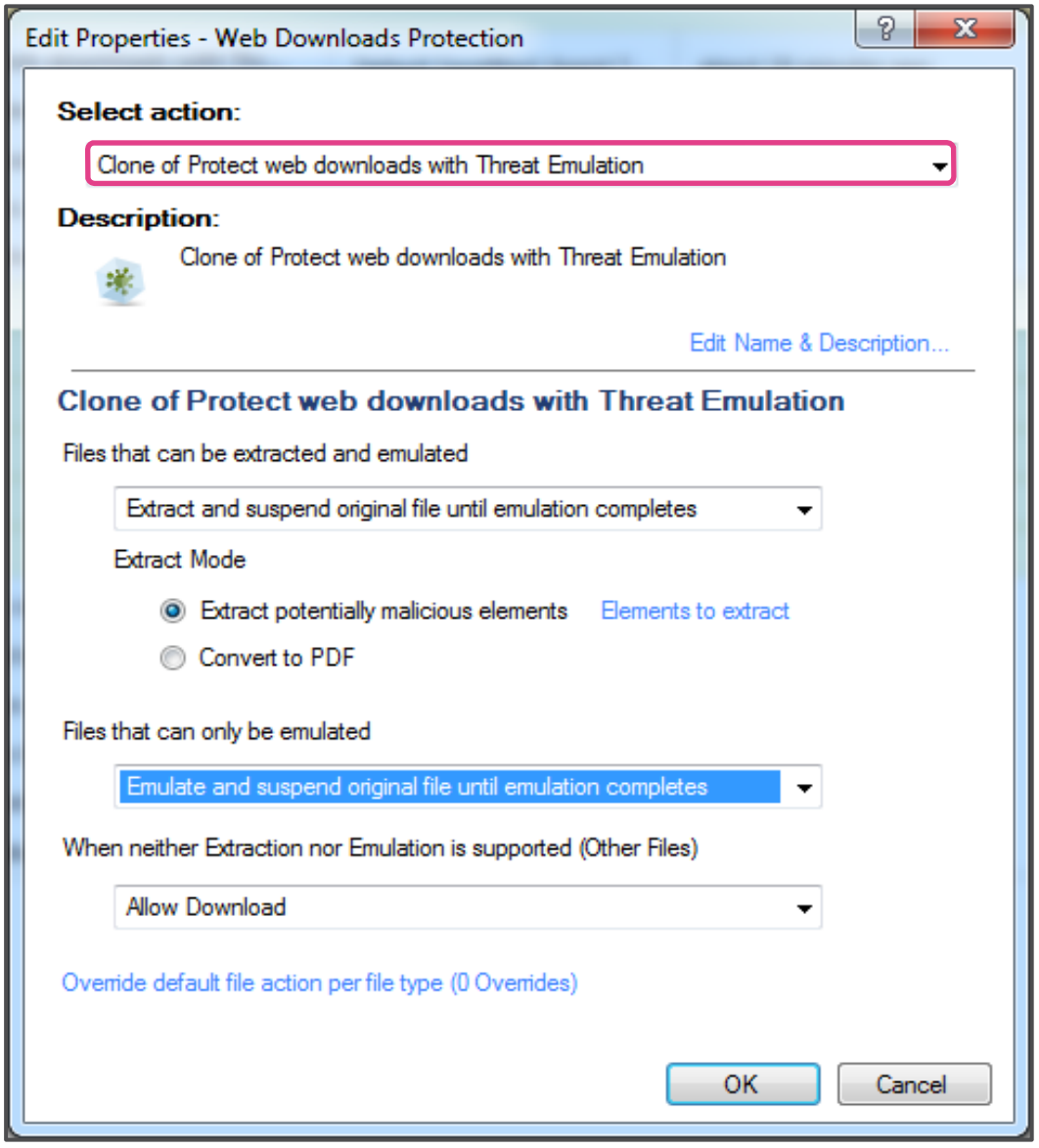


SandBlast Agent Threat Extraction and Threat Emulation Blade

Change the Actions only. Keep the default settings for actions that you do not modify.

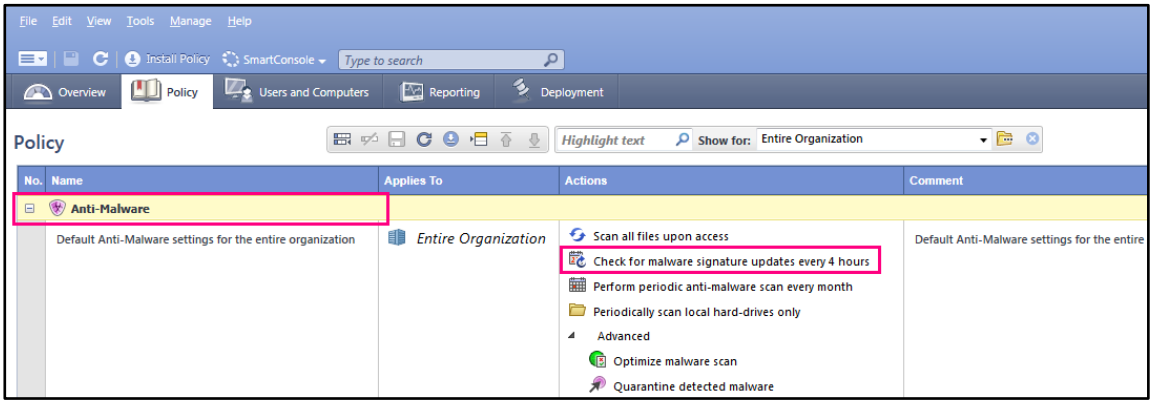


Protect web downloads with Threat Extraction and Threat Emulation

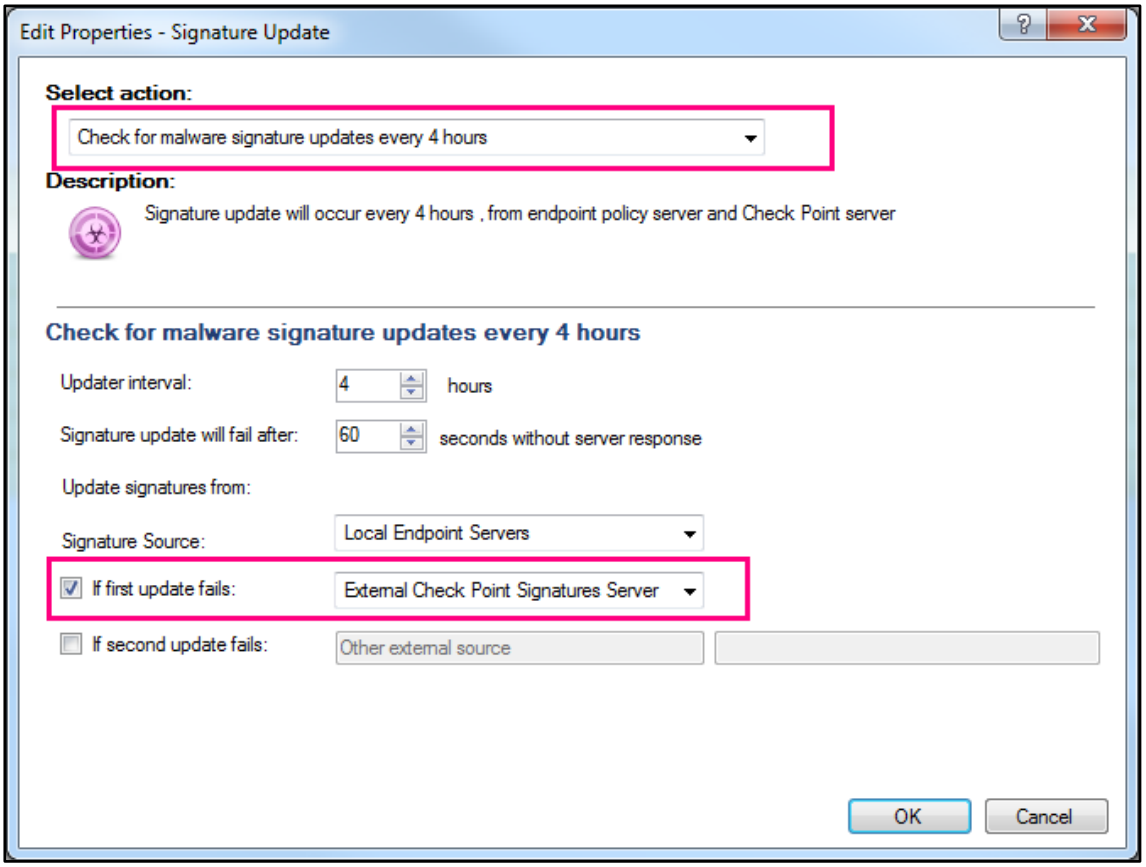


Anti-Malware Blade

Change the Actions only. Keep the default settings for actions that you do not modify.

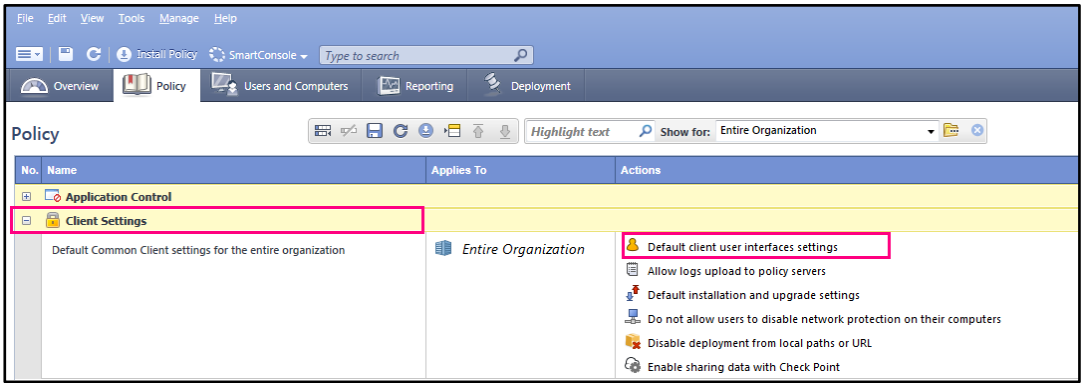


Check for malware signature updates every 4 hours

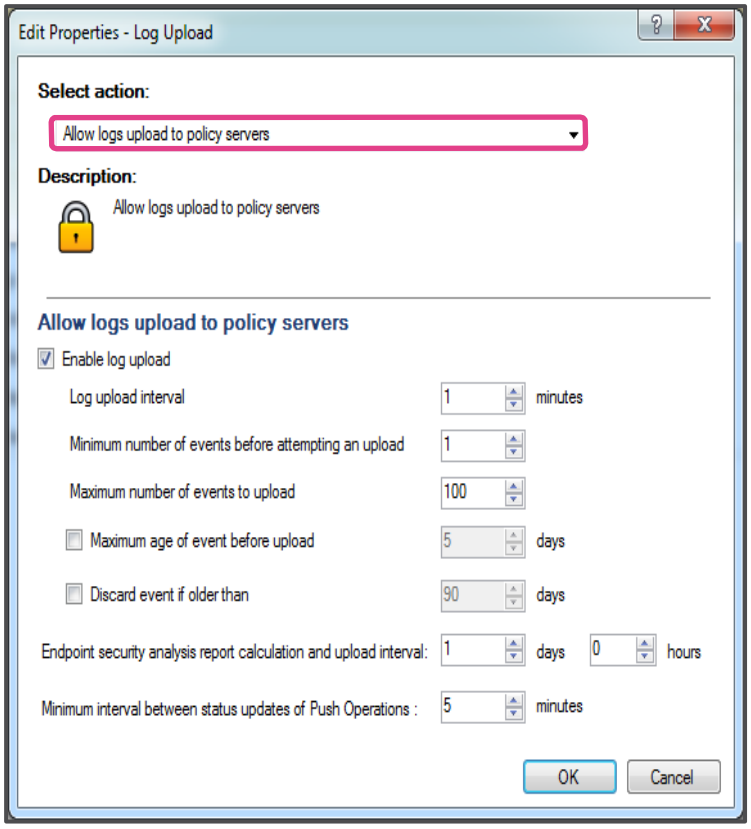


Client Settings Configuration

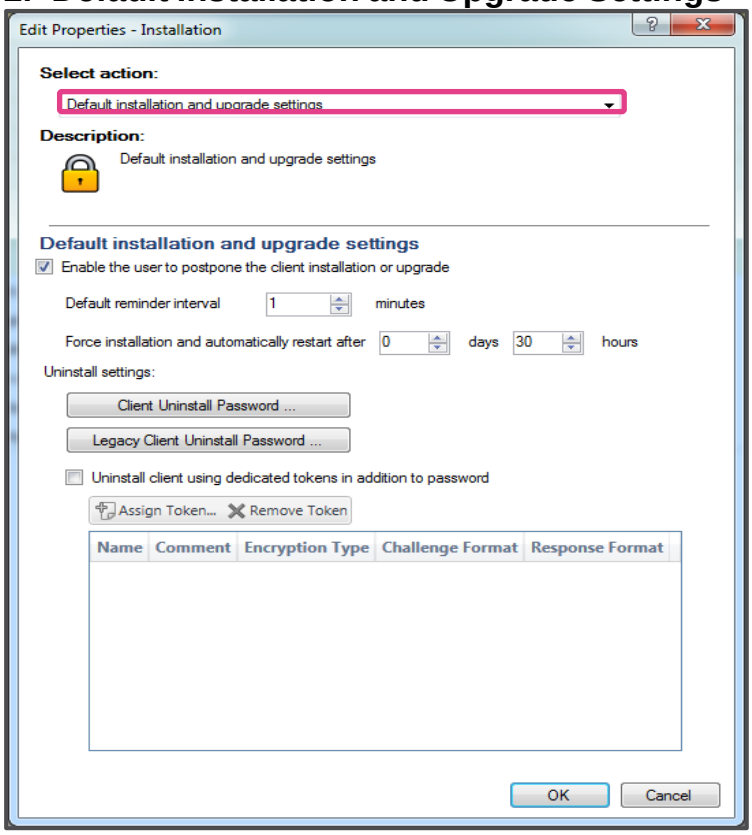
Change the Actions only. Keep the default settings for actions that you do not modify.



1. Allow Log Upload to Policy Servers



2. Default Installation and Upgrade Settings



Configure based on your required deployment policy

SandBlast Client Installation

Important

- Clients must communicate with the Endpoint management server IP address over port 80 and port 443. See sk112099 to configure Endpoint management with static NAT.
- E80.71 client installation is supported on:
  - Windows 7 SP1 and up, Desktop editions
  - Windows 8.1 and Windows 10 up to RS3 (all Endpoint blades)
  - Win2008R2, Win2012, Win2012R2 and up, server editions (Compliance, Anti-malware, Firewall, Capsule docs and SandBlast Agent blades)

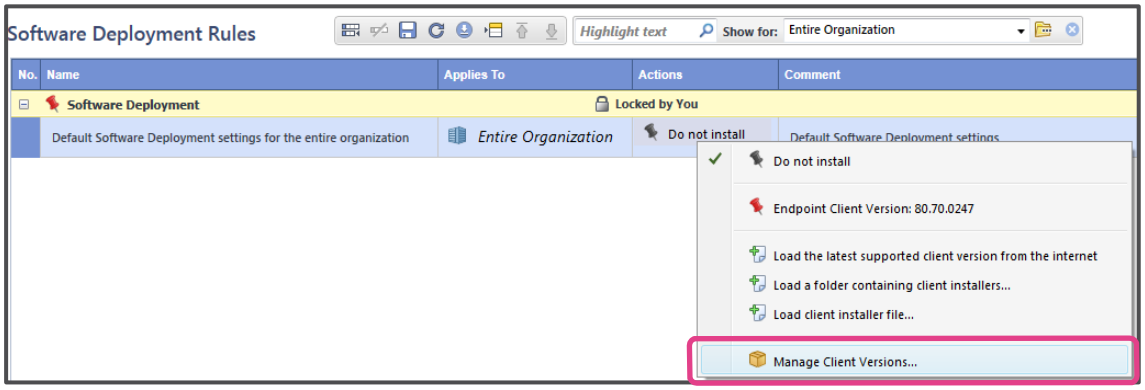
Note - Windows 2008 does not support SandBlast Agent blades

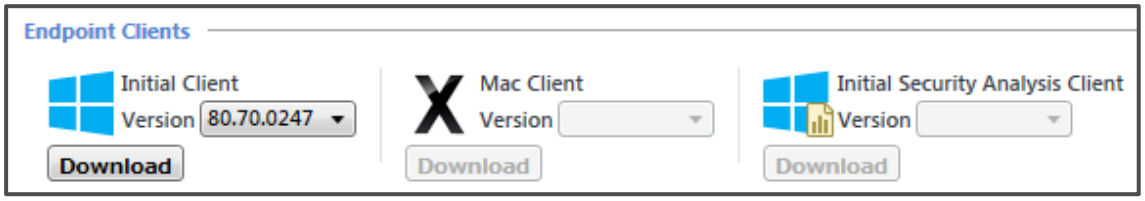
Deployment by Initial Client

1. Verify that the client Windows machine is activated, has the latest .NET installed, and KB3033929 is applied (relevant to Windows 7 editions).
2. Verify that the Apache server is running on Endpoint management. SSH to the Endpoint management server and run:

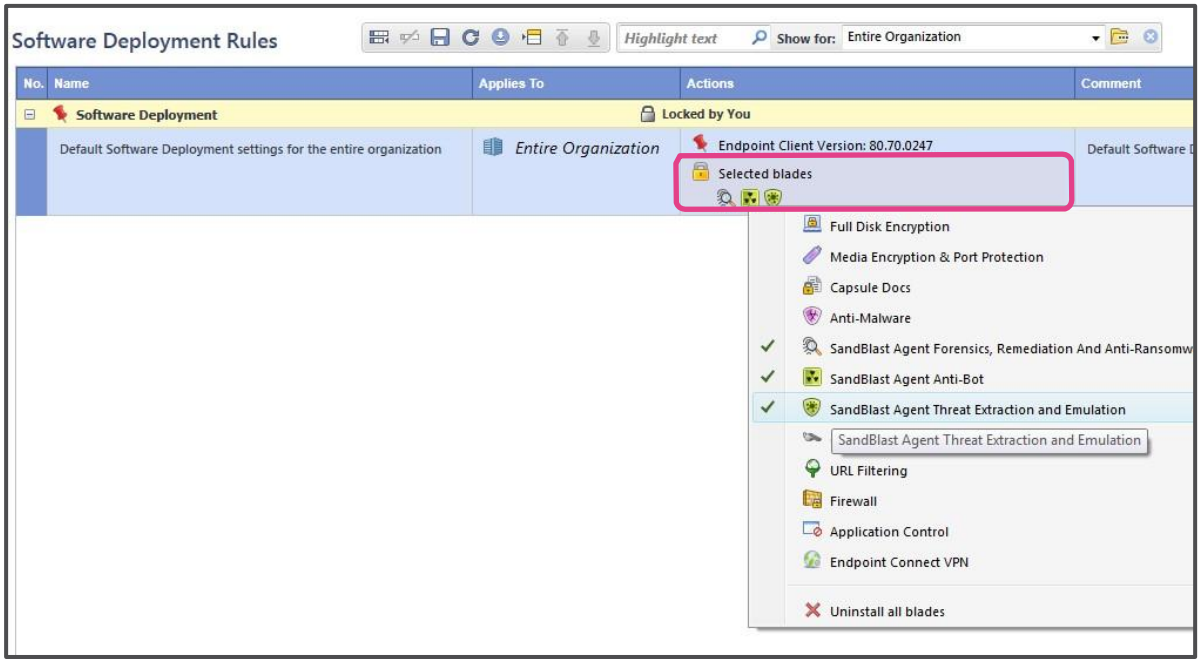
```
[Expert@SBA-Mgmt:0]# ps aux | grep apache22
admin     16205  0.0  0.1  33884  7996 ?        Ss   Aug07   0:00
/opt/CPuepm-R77/apache22/bin/httpd -d /opt/CPuepm-R77/apache22 -k
start
```

3. See sk119676 for the latest version (E80.71 as of November 2017) of Endpoint security clients downloads.
4. Open the Endpoint SmartConsole and go to the **Deployment** tab > **Actions** > **Load Client installer files**.
5. Choose the relevant `EPS.msi` files of the full package and initial package.
6. At the bottom of the GUI, choose **Manage Client Versions** to check that the **Initial Client** version was updated.

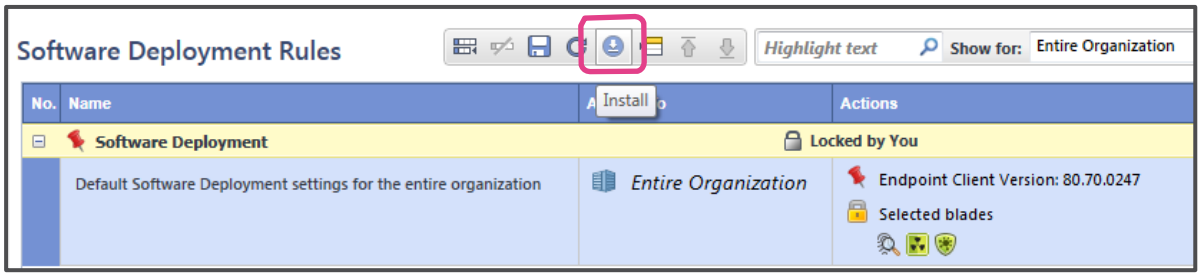


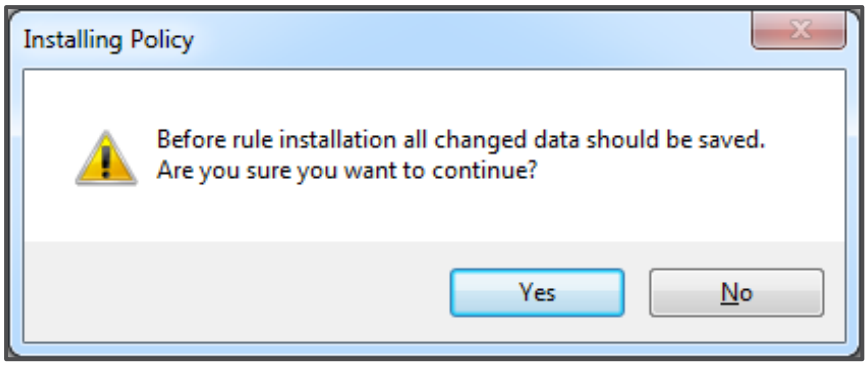


7. From the **Actions** column, choose **Selected Blades**.
8. For *SandBlast Agent only* deployment, choose **SandBlast Agent Threat Extraction and Emulation**.

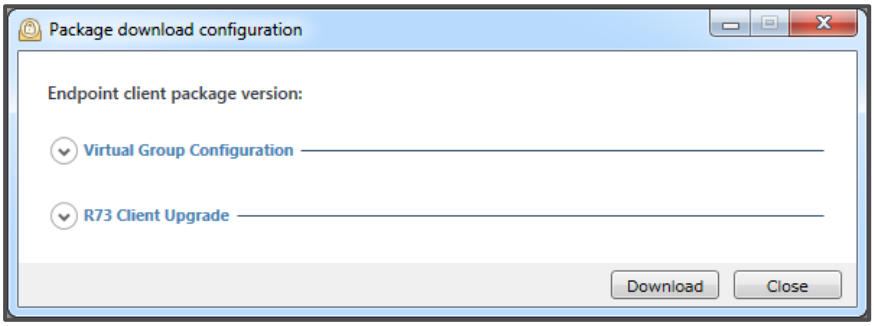


9. Install the policy.



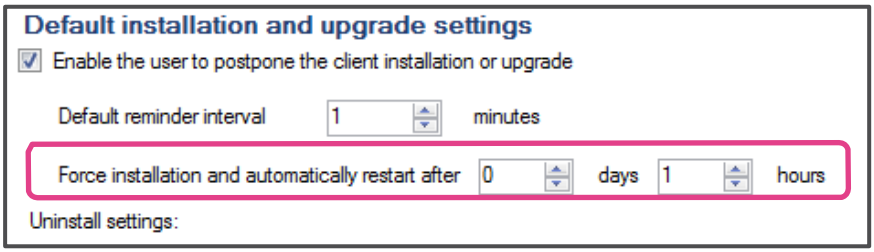


10. From the **Initial Client** window, click **Download** and follow the instructions to locally save the exported initial client. The exported package already contains the IP information of Endpoint management.

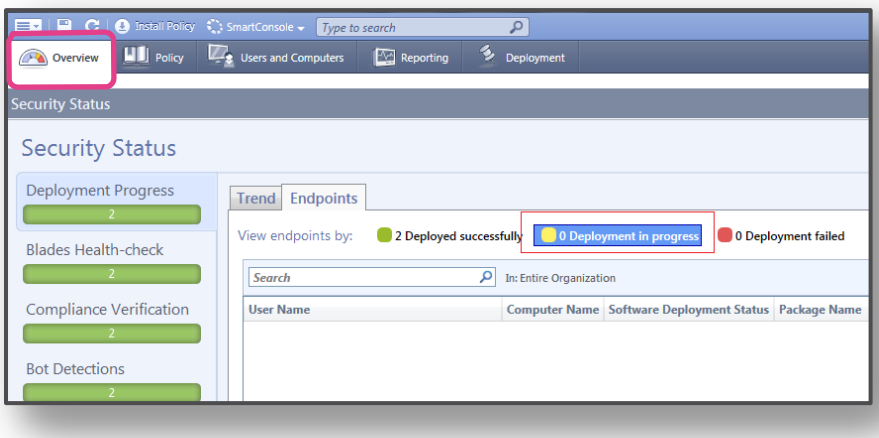


11. Copy the exported Initial Client to the client machine and install it using administrative privileges for the command line. You can also use system management software like SCCM to distribute the initial client (see sk103395 - *Best Practices - Endpoint Security* (*videos*)).
12. The Initial client pulls the installation package from the Endpoint management server and shows a message to the user, to agree to start the installation.
13. After the Initial Client is installed, the client reboots automatically.
14. Configure the Endpoint management policy **Client Settings** entry of **Default Installation and upgrade settings**, for default reminder settings and forced installation interval.

    In the example below, installation was initiated at 10:17 and if no *Install Now* button is pressed, it will be installed automatically at 11:18. Automatic restart after installation is done after 90sec (this is hard coded.)



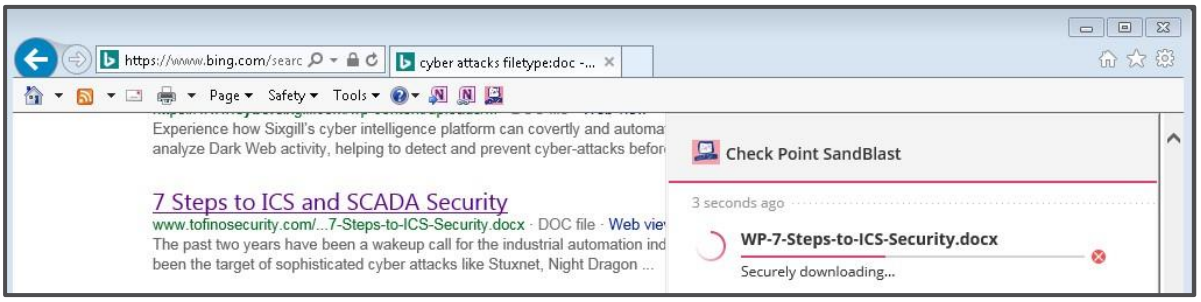
15. Open the Endpoint SmartConsole and go to the **Overview** tab. Monitor the client installation status from the **Security Status** window.

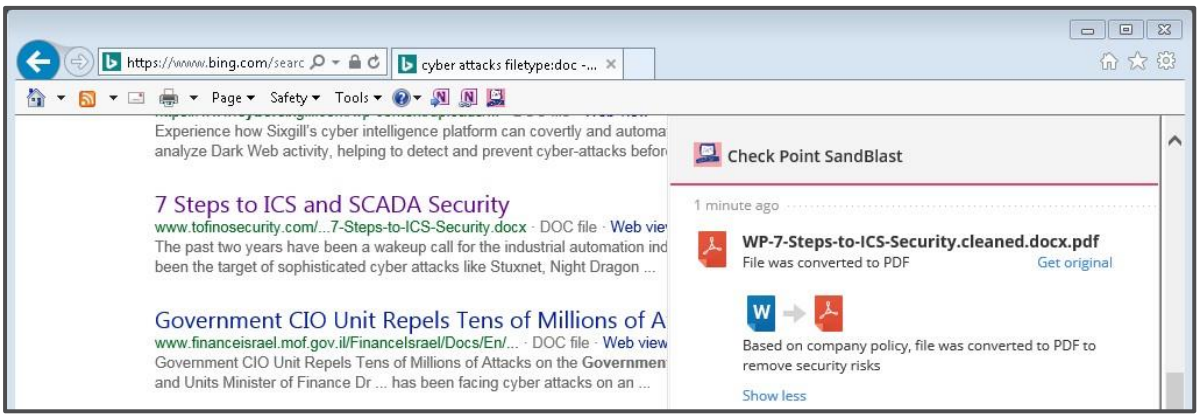


SandBlast Agent Browsers Extension

SandBlast Agent for Browsers is a browser extension for preventing attacks that use web browsers as a main entry point. It includes Threat Emulation, Threat Extraction, Zero Phishing and credential protection. The client should be part of the domain, for the Chrome browser extension to be installed (not required for IE11 extension).

SandBlast Agent for Browsers is available as a stand-alone solution. It can be implemented using a simple browser plugin and is an ideal fit for organizations looking for rapid deployment with a minimal footprint, see sk108695.

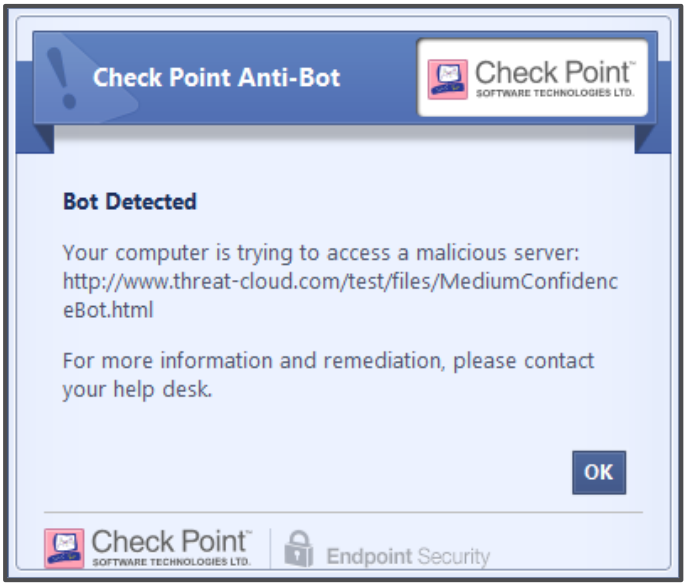


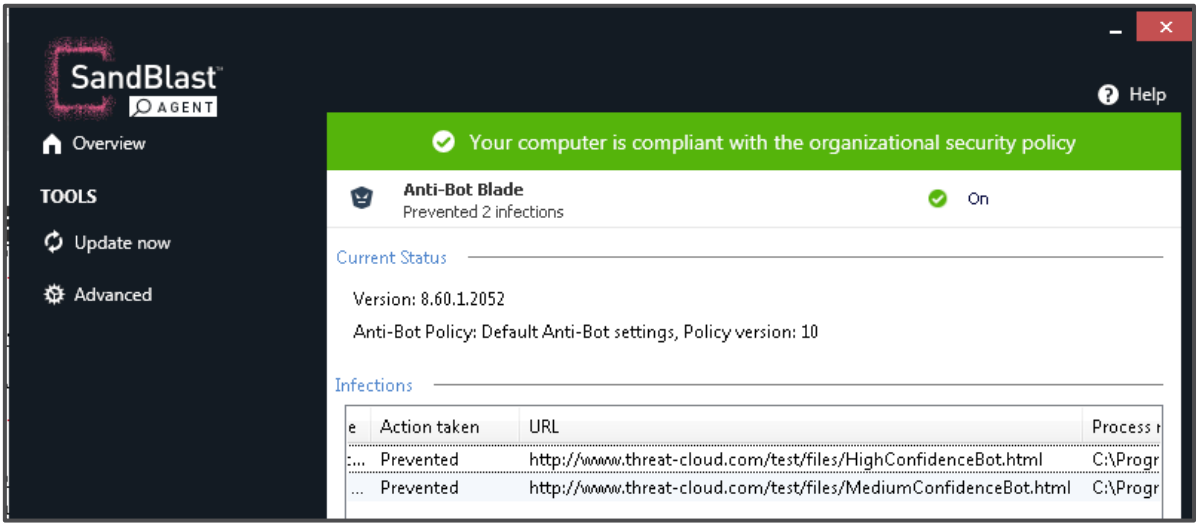


Testing SandBlast Agent

Anti-Bot Blade

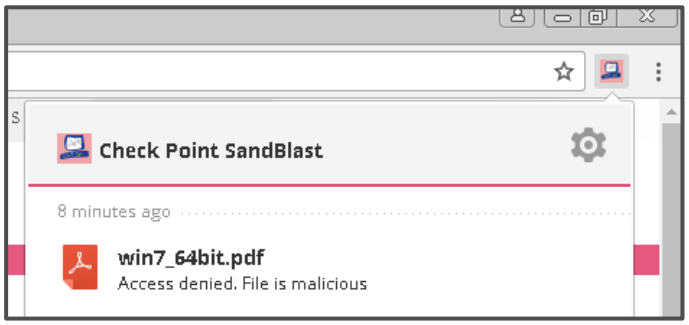
Browsing to the URLs below triggers an Anti-Bot and pop-up tray notification. Details can be viewed in client UI logs:
http://www.threat-cloud.com/test/files/MediumConfidenceBot.html
http://www.threat-cloud.com/test/files/HighConfidenceBot.html

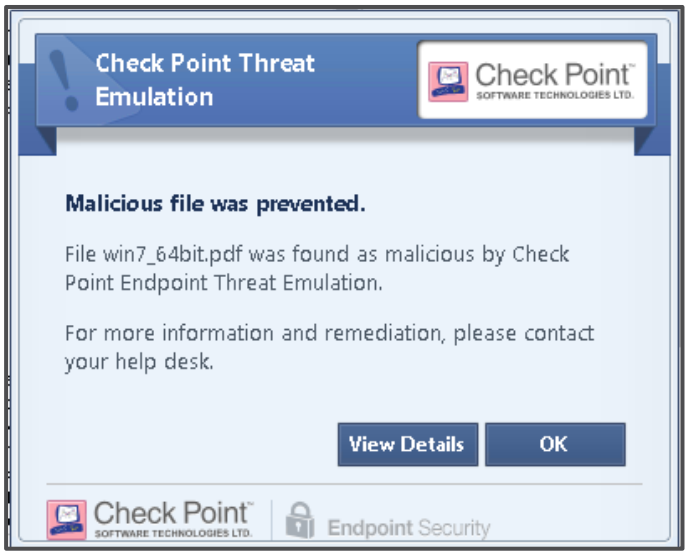


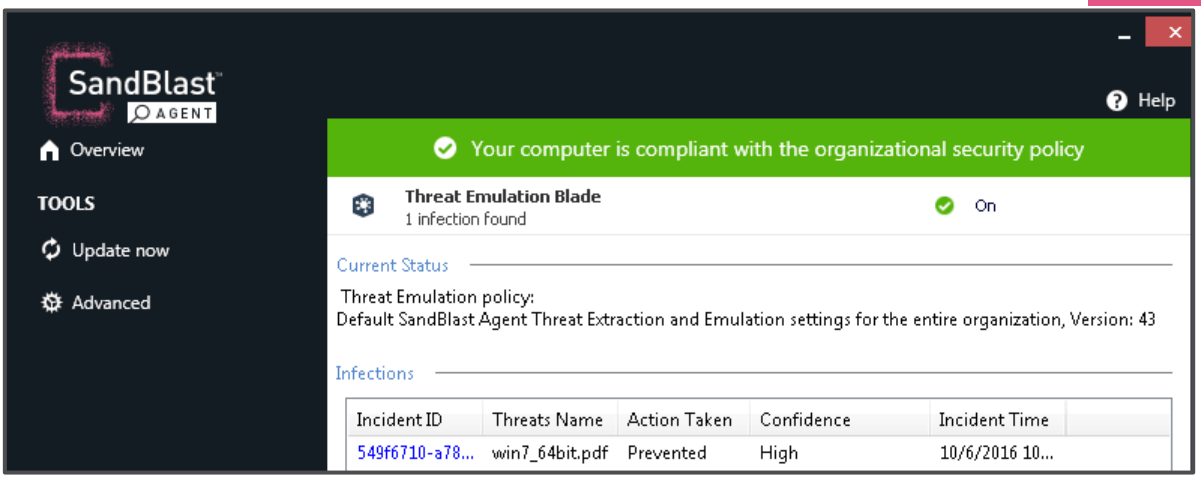


Threat Emulation Blade

- Go to https://threatwiki.checkpoint.com/threatwiki/public.htm and download the test Threat Emulation file.
- Go to POC repository of malicious files http://poc-files.threat-cloud.com/demo/poc/.
- Log in with the user name: *malicious_demo* and password: *malicious*
  Check that the file is detected as malicious and blocked by the Chrome extension.
  The client pop-up is displayed and the log can be seen in the client UI.

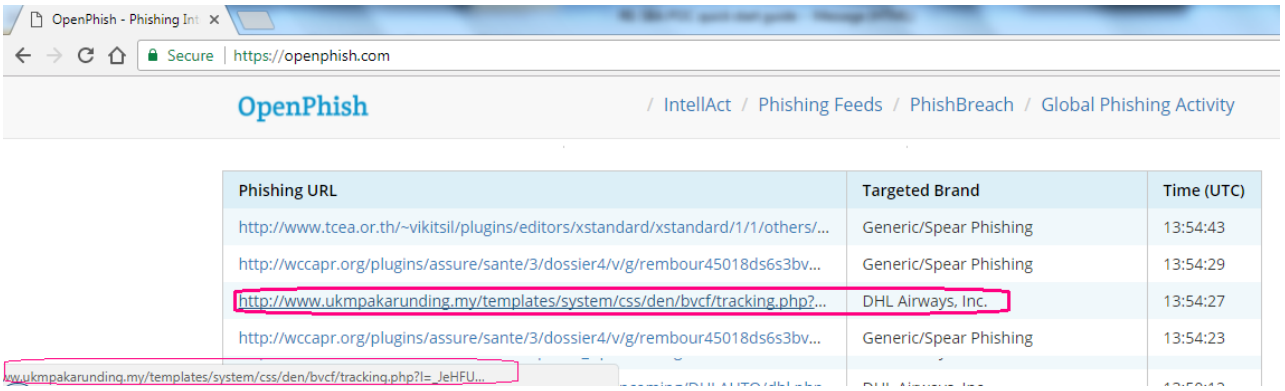


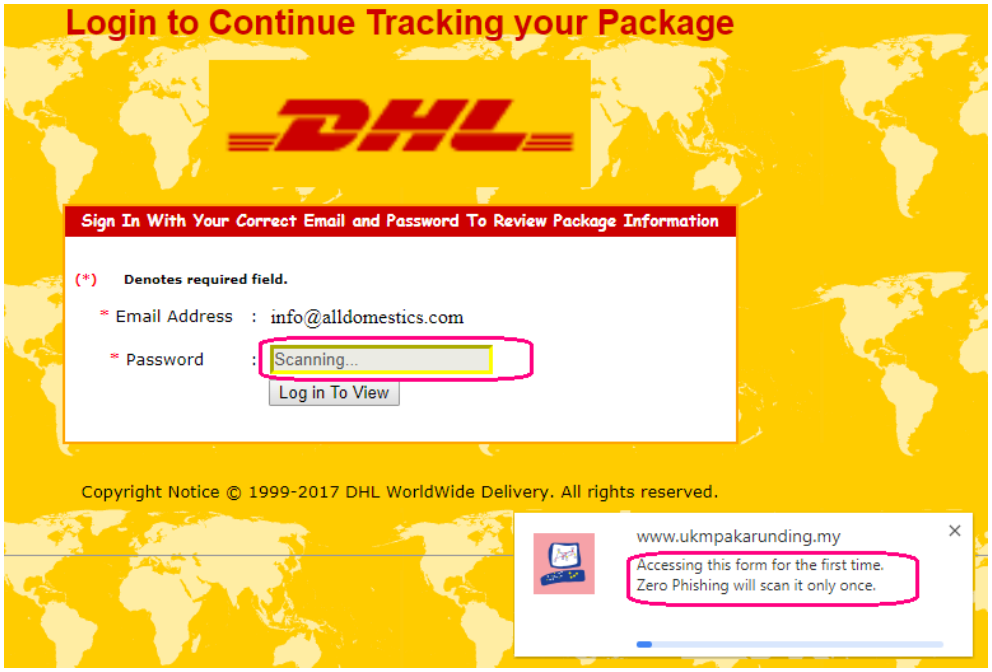


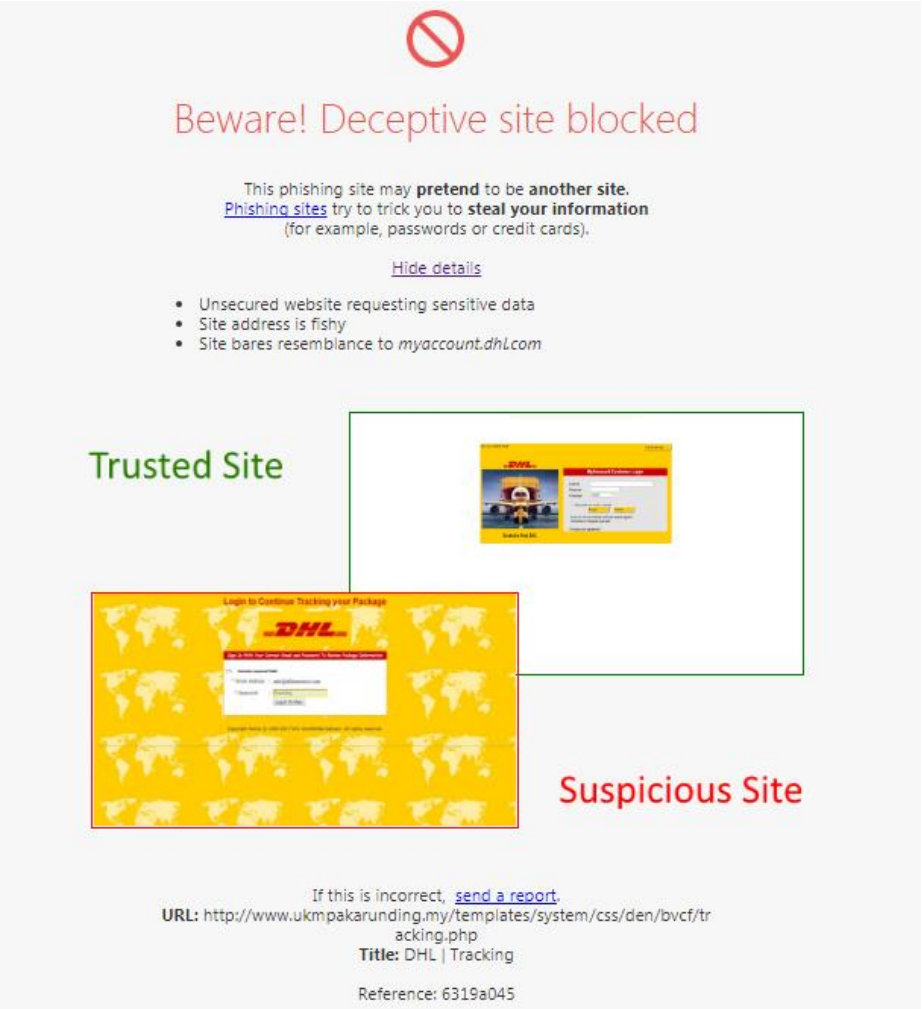


Zero Phishing

- Browse to some known phishing site (you can use online repository at h**p://openphish.com)
- If using Chrome, disable the embedded protection from dangerous sites (Settings->Advanced)
- Once you try to fill in data in the form, extension show “Scanning” status and will prompt pop-up
- If site found malicious you’ll receive Deceptive Site block page with detailed explanation and ability to report false positive detection



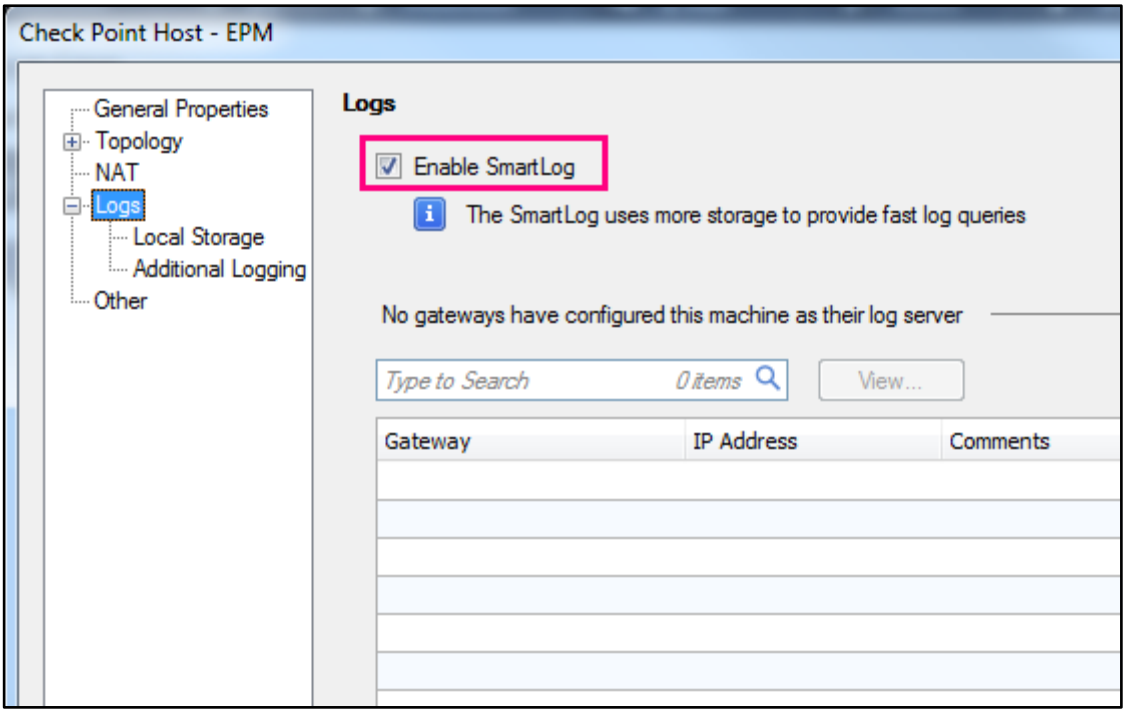


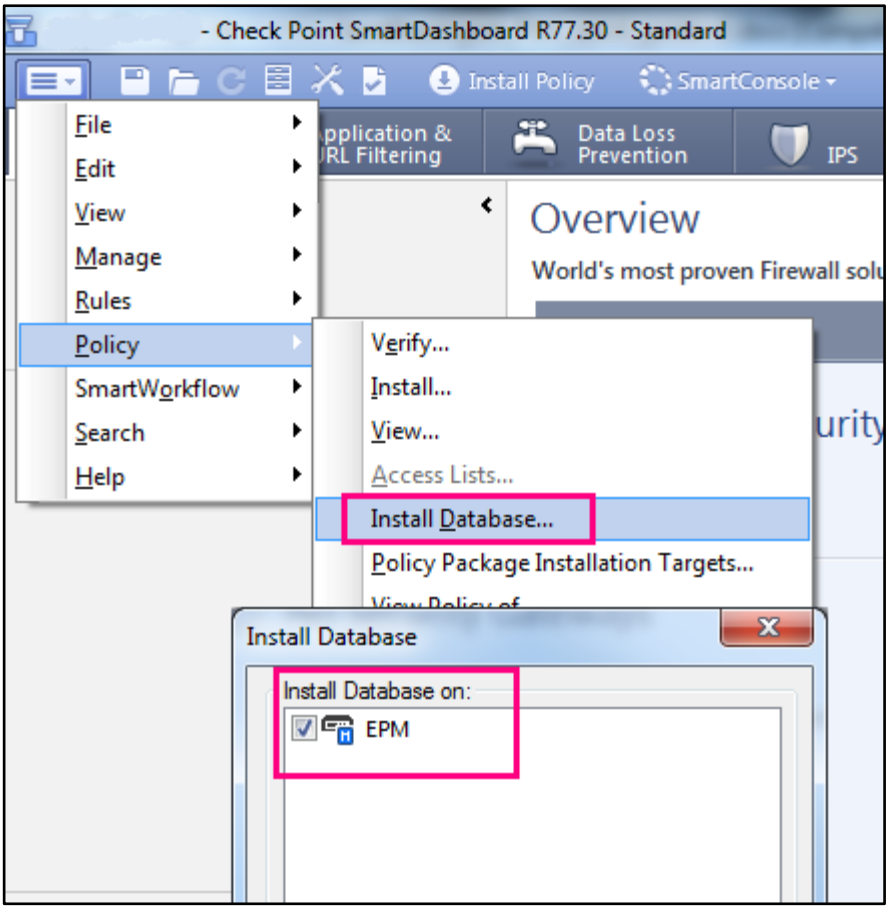


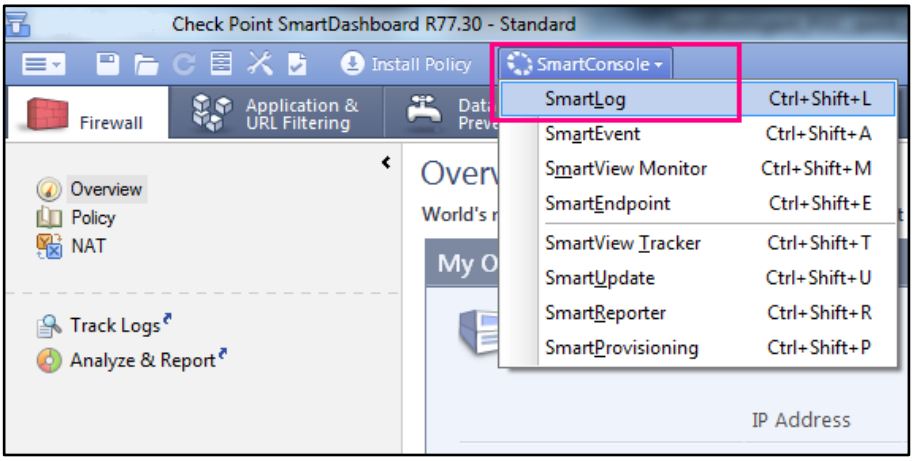
Opening Forensic Analysis Report

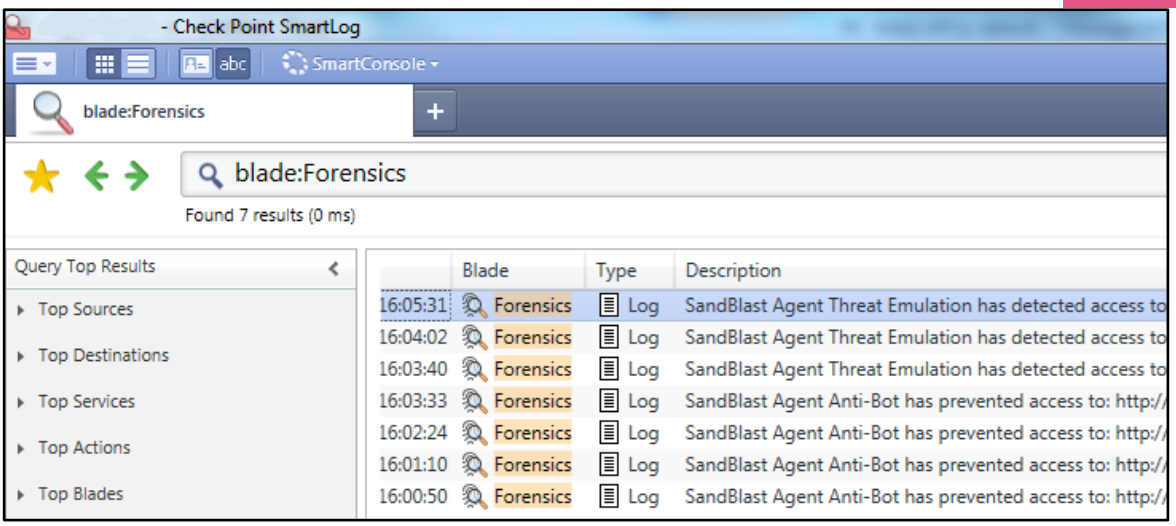
SandBlast Agent Forensic report can be opened from SmartLog application.

Open SmartDashboard and enable SmartLog on Endpoint management object

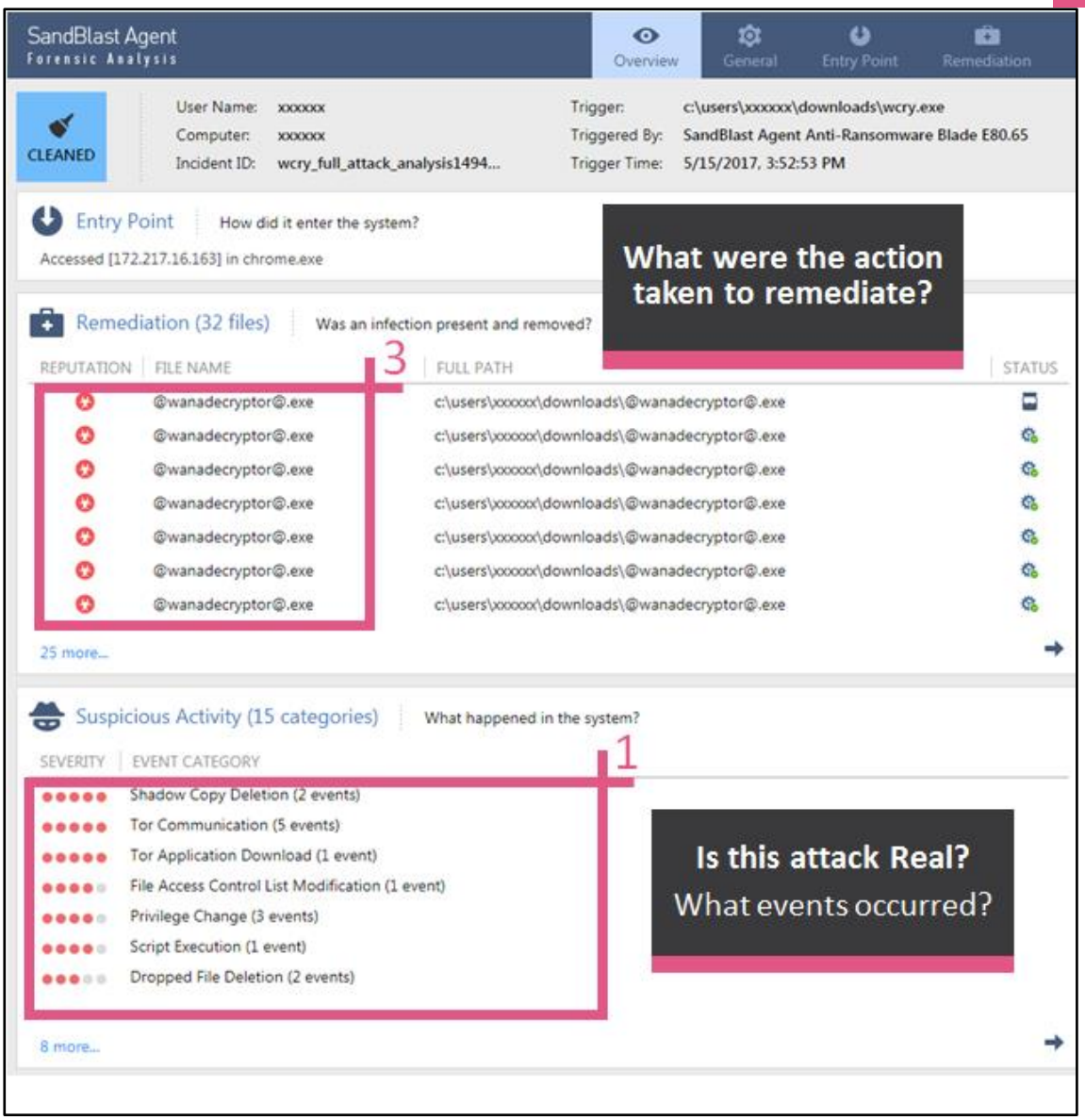


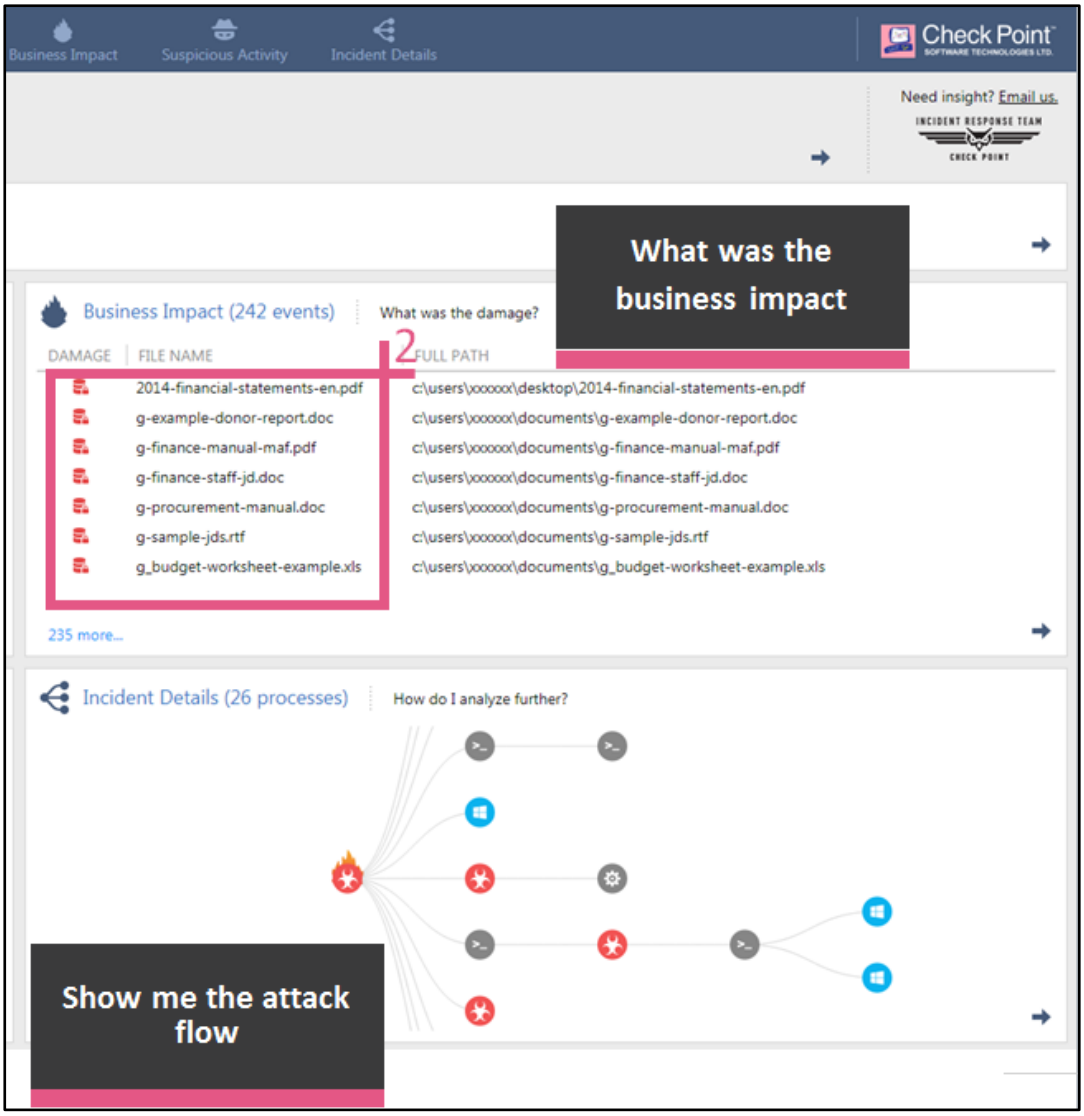






Visit the Check Point forensic blog for online examples of the latest forensic analysis:
http://blog.checkpoint.com/tag/sandblast-agent-forensics/





Forensic Analysis Triggered by Third Party Solutions

SandBlast Agent can be integrated with third party Anti-Malware solutions. The forensic blade can analyze file history and URL history incidents that were triggered by third party Anti-Malware. Monitoring integration is seamless with the Windows system of third party vendors.

See sk116024 - SandBlast Integration with Third Party Anti-Virus Vendors.

Sizing POC environment

- Using SandBlast Agent with the Check Point cloud supports any amount of Endpoint client deployment. For deployments of more than 3,000 clients, contact your local Check Point representative.
- Contact your local Check Point representative for a SandBlast Agent POC using a Sandblast appliance.

Troubleshooting Logs

Problem	Logfile	Comment
Browser extension errors	**Chrome Extension** <*Chrome download folder*>\sandblast_logs.txt **IE11 extension** C:\Users\<username>\AppData\LocalLow\ CheckPoint\SandBlast\Logs	**Chrome Extension** Right click on Browser extension and Collect Logs. **IE11 extension** Left click on Browser extension and click again on Collect Logs. Provide URL that caused the issue.
SandBlast Agent UI errors, deployment errors	SandBlast client logs (cpinfo)	Collect logs from SandBlast agent client: Advanced -> Collect
Crashes / Dump Files	C:\Windows\Internet Logs\CP_EFR Crash*	
Deployment issues	C:\Program Files (x86)\CheckPoint\Endpoint Security Agent\Endpoint Common\Logs\cpda.log (or	
False Positive/ False Negative	SandBlast client logs (cpinfo) Forensic DB: C:\ProgramData\CheckPoint\DBStore\EFR.db C:\ProgramData\CheckPoint\DBStore\Events\<event ID>	Wait 15 minutes after FP/FN and then copy EFR.db aside and compact it. Contact your local SE.