

**APPLICATION  
SECURITY, INC.**

# **AppDetective Advanced Documentation**

## **Check Point Logging Properties Installation Guide**

**November 8, 2005**

APPLICATION SECURITY, INC.  
WEB: [WWW.APPSECINC.COM](http://WWW.APPSECINC.COM)  
E-MAIL: [INFO@APPSECINC.COM](mailto:INFO@APPSECINC.COM)  
TEL: 1-866-9APPSEC • 1-212-947-8787

**Check Point  
Software  
Technologies Ltd.  
trademark notice**

©2004-2005 Check Point Software Technologies Ltd. All rights reserved. Check Point, Application Intelligence, Check Point Express, the Check Point logo, AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, TrueVector, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Pro, Zone Labs, and the Zone Labs logo, are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, and 6,496,935 and may be protected by other U.S. Patents, foreign patents, or pending applications.

# Check Point Logging Properties Installation Guide

AppDetective 5.0 includes new functionality that forwards AppDetective Pen Test and Audit results to a Check Point® Event Logging Server (SmartCenter Server™). This guide explains how to enable this functionality in AppDetective, and send events to your Check Point SmartCenter Server.

This guide consists of the following topics:

- [Environment](#)
- [Check Point Setup](#)
- [AppDetective Setup](#)
- [Testing AppDetective Integration with Check Point](#)

## Environment

You must install or obtain the following:

- AppDetective 5.0, which includes `Opsec_Full_Cert.exe` and `Opsec_putkey.exe`
- Check Point NG™.

## Check Point Setup

This topic explains how to prepare the Check Point server to receive log events from the AppDetective host.

To set up Check Point:

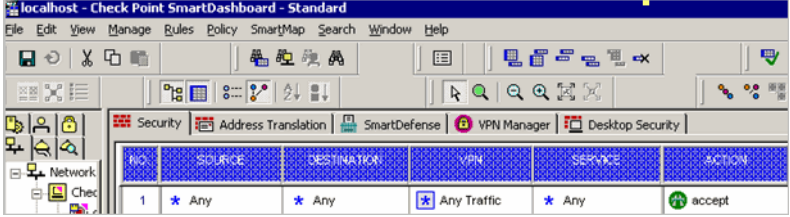
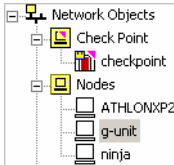


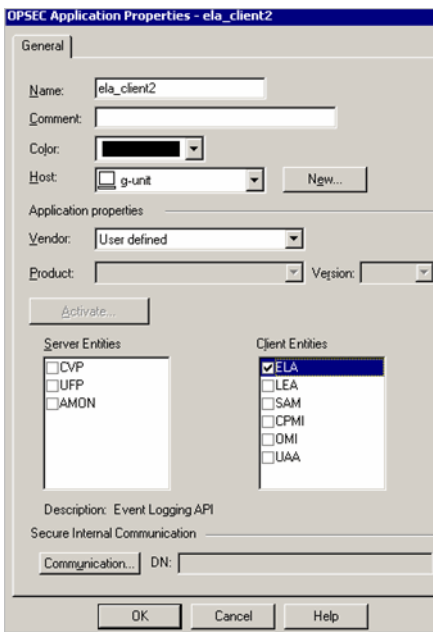
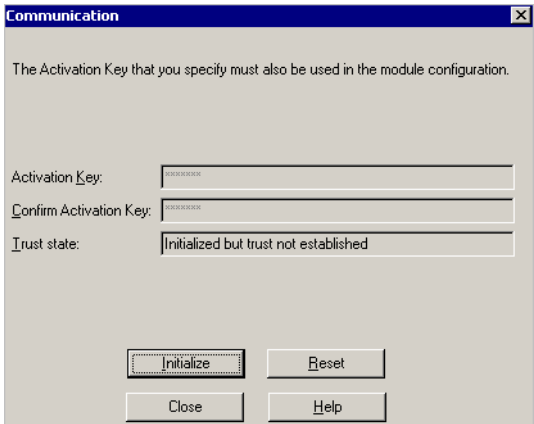
Step	Action												
1	<p>The Check Point suite includes a firewall. Subsequently, you must create a:</p> <ul style="list-style-type: none"> <li>• <b>firewall policy</b> that accepts AppDetective traffic. The policy should allow the traffic between AppDetective node and the Check Point node.</li> <li>• <b>rule</b> that allows the service FW1_ela (TCP port 18187).</li> </ul> <p><b>Note:</b> The service FW1_ica_pull (TCP port 18210) is needed to allow the opsec_pull_cert in Step 6, below.</p> <p>After creating the policy, you must install the policy on the Check Point SmartDashboard (as shown below).</p>  <p>The screenshot shows the Check Point SmartDashboard interface with the Security tab selected. A table displays the configuration for a rule:</p> <table border="1"> <thead> <tr> <th>ID</th> <th>SOURCE</th> <th>DESTINATION</th> <th>VPN</th> <th>SERVICE</th> <th>ACTION</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>* Any</td> <td>* Any</td> <td>* Any Traffic</td> <td>* Any</td> <td>accept</td> </tr> </tbody> </table>	ID	SOURCE	DESTINATION	VPN	SERVICE	ACTION	1	* Any	* Any	* Any Traffic	* Any	accept
ID	SOURCE	DESTINATION	VPN	SERVICE	ACTION								
1	* Any	* Any	* Any Traffic	* Any	accept								

FIGURE: Check Point SmartDashboard (Security tab)

**Result:** AppDetective traffic can now reach your Check Point SmartCenter Server.

Step	Action
2	<p>On the Check Point SmartDashboard, under the <b>Network Objects</b> branch in the left pane, right click <b>Nodes</b> &gt; <b>New Nodes</b> &gt; <b>Host</b>.</p> <p><b>Note:</b> In this example, the Check Point node is named <b>checkpoint</b> and the AppDetective node is <b>g-unit</b>.</p>  <p><b>FIGURE: Check Point SmartDashboard (Network Objects branch)</b></p> <p><b>Result:</b> The <b>Host Node</b> pop-up displays.</p>  <p><b>FIGURE: Host node pop-up</b></p>
3	<p>Do the following:</p> <ul style="list-style-type: none"> <li>• In the <b>Name</b> field, enter the hostname where AppDetective is installed.</li> <li>• Click the <b>Get Address</b> button.</li> </ul> <p><b>Result:</b> Check Point populates the <b>IP Address</b> field.</p> <ul style="list-style-type: none"> <li>• Click the <b>OK</b> button.</li> </ul>

Step	Action
4	<p>On the Check Point SmartDashboard, under the <b>Servers and OPSEC Applications</b> branch in the left pane, right click <b>OPSEC Applications</b> and choose <b>OPSEC Application</b>.</p>  <p><b>FIGURE: Check Point SmartDashboard (Servers and OPSEC Applications branch)</b></p> <p><b>Result:</b>The <b>OPSEC Application Properties</b> pop-up displays.</p>  <p><b>FIGURE: OPSEC Application Properties pop-up</b></p>

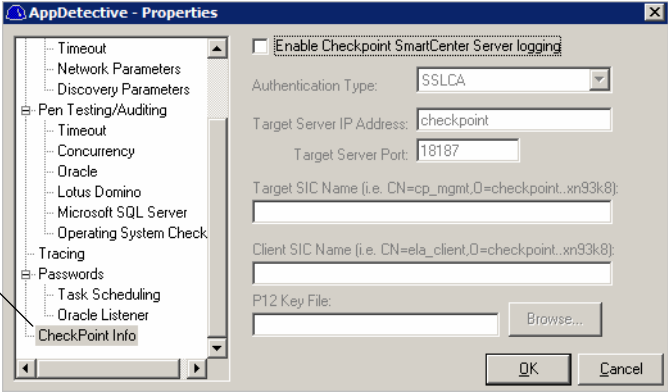
Step	Action
5	<p>Do the following:</p> <ul style="list-style-type: none"><li>• In the <b>Name</b> field of the <b>OPSEC Application Properties</b> pop-up, enter a name for the object (e.g., <code>ela_client2</code>). You will need this in Step 7.</li><li>• Use the <b>Host</b> drop-down to select the node where AppDetective is installed (i.e., <b>g-unit</b>).</li><li>• In the <b>Client Entities</b> section, check <b>ELA</b>.</li><li>• Click the <b>Communications</b> button.</li></ul> <p><b>Result:</b>The <b>Communication</b> pop-up displays.</p>  <p><b>FIGURE: Communication pop-up</b></p> <ul style="list-style-type: none"><li>• Enter your activation key in the <b>Activation Key</b> field.</li><li>• Confirm your activation key in the <b>Confirm Activation Key</b> field.</li><li>• Click the <b>Initialize</b> button.</li><li>• Click the <b>Close</b> button.</li></ul>

Step	Action
6	<p>Retrieve a certificate from Check Point's internal Certificate Authority (CA).</p> <ul style="list-style-type: none"> <li>On the AppDetective host (e.g., <b>g-unit</b>), open a command prompt window.</li> </ul>  <pre> Select C:\WINNT\system32\cmd.exe C:\Program Files\AppSecInc\AppDetective&gt;opsec_pull_cert -h checkpoint -n ela_client2 -p yankees The full entity sic name is: CN=ela_client2.0=checkpoint..xn93k8 Certificate was created successfully and written to "opsec.p12". C:\Program Files\AppSecInc\AppDetective&gt; </pre> <p><b>FIGURE: Command prompt window (AppDetective host)</b></p> <ul style="list-style-type: none"> <li>Change the directory to the Check Point folder under which AppDetective is installed. Make sure utility <code>opsec_pull_certificate.exe</code> is there.</li> <li>Enter: <code>opsec_pull_cert -h host -n object_name -p password</code>.</li> </ul> <p>where:</p> <ul style="list-style-type: none"> <li><code>host</code> is the location where Check Point is installed.</li> <li><code>object_name</code> was created in Step 5.</li> <li><code>password</code> was created in Step 6.</li> </ul> <p><b>Result:</b> Communication is established. Check Point is now ready to receive events from AppDetective.</p>

## AppDetective Setup

On the AppDetective side, you must enable the sending of events to Check Point after a Pen Test or Audit.

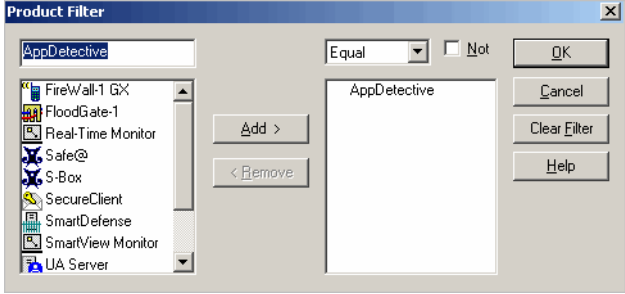
To set up AppDetective to send events to Check Point after a Pen Test or Audit:

Step	Action
1	<p>In AppDetective, choose <b>Edit &gt; Properties</b>.  <b>Result:</b>The <b>Properties</b> dialog box displays.</p>  <p><b>Check Point Info</b> branch</p> <p><b>FIGURE: Properties dialog box</b></p>
2	Check <b>Enable Checkpoint SmartCenter Server logging</b> .

Step	Action
3	<p>Configure the following parameters:</p> <ul style="list-style-type: none"> <li>• <b>Authentication Type.</b> By default, Check Point servers use <b>SSLCA</b> to communicate with their objects. However, you can use this drop-down to select <b>Clear Text</b>, if necessary.</li> </ul> <p>Contact Check Point Tech Services for assistance with changing the ELA server to accept clear connections.</p> <p><b>Note:</b> <b>SIC Name</b> and the <b>P12 key file</b>, explained below, are only needed if you select <b>SSLCA</b>.</p> <ul style="list-style-type: none"> <li>• <b>Target Server IP Address.</b> Enter the hostname or IP address where the Check Point SmartCenter Server is located.</li> <li>• <b>Target Server Port.</b> By default, a Check Point SmartCenter Server uses port <b>18187</b>.</li> <li>• <b>Target SIC Name.</b> To locate the target Secure Internal Communication (SIC) name (example: <code>cn=cp_mgmt,o=checkpoint.abc.com.48tcd4</code>): <ul style="list-style-type: none"> <li>- Under the <b>Network Objects</b> branch (in the left pane of the Check Point SmartDashboard), double click the <b>Check Point</b> node to display its properties.</li> <li>- Copy the value in the <b>DN</b> field (<b>Secure Internal Communication</b> portion).</li> <li>- Paste the value into the <b>Target SIC Name</b> field in the AppDetective <b>Properties</b> dialog box.</li> </ul> </li> <li>• <b>Client SIC Name.</b> To locate the target Secure Internal Communication (SIC) name: <ul style="list-style-type: none"> <li>- Under the <b>Servers and OPSEC Applications</b> branch (in the left pane of the Check Point SmartDashboard), double click the node to which AppDetective is mapped to display its properties.</li> <li>- Copy the value in the <b>DN</b> field (<b>Secure Internal Communication</b> portion).</li> <li>- Paste the value into the <b>Target SIC Name</b> field in the AppDetective <b>Properties</b> dialog box.</li> </ul> </li> <li>• <b>P12 Key File.</b> Specify the location of the <b>.p12</b> file that was generated when you executed the <code>opsec_pull_cert.exe</code>; for more information, see Step 8 in <a href="#">Check Point Setup</a>. By default, this file should be located under the directory where AppDetective is installed.</li> </ul>
4	<p>Click the <b>OK</b> button.</p> <p><b>Result:</b> AppDetective PenTest or Audit results are sent to Check Point.</p>
5	<p>On the SmartDashboard:</p> <ul style="list-style-type: none"> <li>• Choose <b>Policy &gt; Install</b>.</li> <li>• Select the Check Point target.</li> <li>• Click the <b>OK</b> button.</li> </ul> <p><b>Note:</b> You can use the <b>Check Point SmartView Tracker</b> to view all AppDetective event logs.</p>

## Testing AppDetective Integration with Check Point

To test AppDetective integration with Check Point:

Step	Action
1	<p>Do the following:</p> <ul style="list-style-type: none"> <li>• Create an AppDetective query.</li> <li>• Right click the <b>Product</b> field.</li> <li>• On the <b>Product Filter</b> pop up, add <b>Equal</b> to <b>AppDetective</b>.</li> </ul>  <p><b>FIGURE: Product Filter pop up</b></p>
2	<p>Save the custom query, by choosing <b>Query &gt; Save As...</b> and entering AppDetective.</p>