

# Protection Dashboard

## Armor Knowledge Base

### Topics Discussed

- [Review Widgets and Graph](#)
- [Understand Service Health](#)
- [Improve Your Protection Score](#)
- [Export Protection Screen Data](#)


In the **Protection** screen, the **Protection** score focuses on the stability of Armor services to determine if

- The agent is responding (heartbeating) to Armor
- The agent has registered properly

For **Armor Complete**, the **Protection** scores focuses on the following services:

- Malware Protection
- FIM
- Filebeat (for Linux)
- Winlogbeat (for Windows)

## Review Widgets and Graph

Widget and Graph Type	Description								
<b>Protection Score</b>	<p>This widget displays a calculated score that includes the number of subagents in an unhealthy state.</p> <table border="1"><thead><tr><th>Score Range</th><th>Health Status</th></tr></thead><tbody><tr><td>10 - 8</td><td>Good</td></tr><tr><td>7 - 4</td><td>Fair</td></tr><tr><td>3 - 1</td><td>Poor</td></tr></tbody></table> <ul style="list-style-type: none"><li>• For <b>Armor Complete</b>, only virtual machines that are in a <b>Powered On</b> state are included.</li><li>• For <b>Armor Anywhere</b>, only virtual machines that have communicated (heartbeated) with Armor in the last 4 hours are included.</li></ul> <p>Scores in the security dashboards are calculated and updated every night at 2:00 AM UTC.</p>	Score Range	Health Status	10 - 8	Good	7 - 4	Fair	3 - 1	Poor
Score Range	Health Status								
10 - 8	Good								
7 - 4	Fair								
3 - 1	Poor								
<b>Assets Protected</b>	<p>This widget displays the number of virtual machines that contain the Armor agent.</p> <div style="border: 1px solid #ffc107; padding: 5px;"><p> Newly created virtual machines will not be reflected in the number of Assets Protected until the following day.</p></div>								
<b>Healthy Services</b>	<p>This widget displays the percentage of agents and subagents that are working properly.</p>								
<b>Protection Score Trend</b>	<p>This graph displays the history of your protection scores.</p>								

## Understand Service Health

The **Service Health** table displays the virtual machines that contain the installed Armor agent.



Newly created virtual machines will not be reflected in the Service Health table until the following day.

To view this section, you must have the **Read Virtual Machines(s)** permission assigned to your account.

Column	Description
<b>Asset Name</b>	This column displays the name of the virtual machine. You can click the name of the virtual machine to access the <b>Virtual Machine</b> details screen.
<b>Status</b>	This column displays the security status of the virtual machine. <ul style="list-style-type: none"> <li><b>Unprotected</b> indicates the agent is not installed in the instance. <ul style="list-style-type: none"> <li>Instances without an agent will be labeled as <b>Unprotected</b>. All instances from the public cloud account will be displayed.</li> </ul> </li> <li><b>Needs Attention</b> indicates that the agent is installed, but has not properly communicated (heartbeated) with Armor. <ul style="list-style-type: none"> <li>To troubleshoot a specific error message under <b>Needs Attention</b>, see <a href="#">Troubleshoot Protection Scores</a>.</li> </ul> </li> <li><b>OK</b> indicates that the agent is installed and has communicated (heartbeated) with Armor.</li> </ul>
<b>Location</b>	For <b>Armor Complete</b> , this column will display name of the Armor virtual site. For <b>Armor Anywhere</b> , this column will display the name of the public cloud provider.
<b>Ticket</b>	This column displays the support ticket that troubleshoots the <b>Protection</b> issue. A <b>Protection</b> issue will automatically generate a support ticket.

## Improve Your Protection Score

You can use the information below to troubleshoot the issues displayed in the **Protection** screen.

Armor recommends that you troubleshoot these issues to:

- Improve your Protection scores
- Improve your overall health scores
- Increase the overall security of your environment

Review each step to troubleshoot your problem. If the first step does not resolve the issue, then continue to the second step until the issue has been resolved. As always, you can send a support ticket.



To learn how to send a support ticket, see [Armor Support](#).

## Logging

### Verify the Status of filebeat

	Description	Command	Extra Information
<b>Windows</b>	Configurations are stored in the winlogbeat and filebeat directory within <b>C:\armor\opt\</b>	<pre>cat C:\.armor\opt\winlogbeat-5.2.0- windows-x86_64\winlogbeat.yml cat C:\.armor\opt\filebeat-5.2.0- windows-x86_64\filebeat.yml</pre>	<ul style="list-style-type: none"> <li>• Windows uses both winlogbeat and filebeat.</li> <li>• Commands should run in Powershell.</li> <li>• To review additional configurations, certificates, and service information, review a server's directory: <ul style="list-style-type: none"> <li>• C:\armor\opt\winlogbeat*</li> <li>• C:\armor\opt\filebeat*</li> </ul> </li> </ul>
	To verify the operation of the logging services, look for <b>winlogbeat</b> , <b>filebeat</b>	<pre>gsv -displayname armor-winlogbeat, armor-filebeat</pre>	
	To verify the operation of the logging service processes, look for <b>winlogbeat</b>	<pre>gps filebeat,winlogbeat</pre>	

	Confirm the configured log endpoint	cat C:\.armor\opt\winlogbeat-5.2.0-windows-x86_64\winlogbeat.yml   sls hosts	
<b>Linux</b>	Configurations are stored within <b>/etc/filebeat/filebeat.yml</b>	cat /etc/filebeat/*.yml	
	Verify the operation of the filebeat service	ps aux   grep filebeat	
	Confirm the configured log endpoint	grep -i hosts /etc/filebeat/filebeat.yml	
	Confirm the external_id	grep -i external_id /etc/filebeat/filebeat.yml	
	Confirm the tenant ID	grep -i tenant_id /etc/filebeat/filebeat.yml	



This section only applies to Windows users.

## Verify the Status of winlogbeat

Description	Command	Extra Information
Configurations are stored in the winlogbeat and filebeat directory within <b>C:\armor\opt\</b>	cat C:\.armor\opt\winlogbeat-5.2.0-windows-x86_64\winlogbeat.yml cat C:\.armor\opt\filebeat-5.2.0-windows-x86_64\filebeat.yml	<ul style="list-style-type: none"> <li>Windows uses both winlogbeat and filebeat.</li> <li>Commands should run in Powershell.</li> <li>To review additional configurations, certificates, and service information, review a server's directory: <ul style="list-style-type: none"> <li>C:\armor\opt\winlogbeat*</li> <li>C:\armor\opt\filebeat*</li> </ul> </li> </ul>
To verify the operation of the logging services, look for <b>winlogbeat</b> , <b>filebeat</b>	gsv -displayname armor-winlogbeat, armor-filebeat	
To verify the operation of the logging service processes, look for <b>winlogbeat</b>	gps filebeat, winlogbeat	
Confirm the configured log endpoint	cat C:\.armor\opt\winlogbeat-5.2.0-windows-x86_64\winlogbeat.yml   sls hosts	

## Step 1: Check Logging Services

	Description	Command	Extra information
<b>Windows</b>	Configurations are stored in the winlogbeat and filebeat directory within <b>C:\armor\opt\</b>	cat C:\.armor\opt\winlogbeat-5.2.0-windows-x86_64\winlogbeat.yml cat C:\.armor\opt\filebeat-5.2.0-windows-x86_64\filebeat.yml	<ul style="list-style-type: none"> <li>Windows uses both winlogbeat and filebeat.</li> <li>Commands should run in Powershell.</li> <li>To review additional configurations, certificates, and service information, review a server's directory: <ul style="list-style-type: none"> <li>C:\armor\opt\winlogbeat*</li> <li>C:\armor\opt\filebeat*</li> </ul> </li> </ul>
	To verify the operation of the logging services, look for <b>winlogbeat</b> , <b>filebeat</b>	gsv -displayname armor-winlogbeat, armor-filebeat	
	To verify the operation of the logging service processes, look for <b>winlogbeat</b>	gps filebeat, winlogbeat	
	Confirm the configured log endpoint	cat C:\.armor\opt\winlogbeat-5.2.0-windows-x86_64\winlogbeat.yml   sls hosts	
<b>Linux</b>	Configurations are stored within <b>/etc/filebeat/filebeat.yml</b>	cat /etc/filebeat/*.yml	
	Verify the operation of the filebeat service	ps aux   grep filebeat	

	Confirm the configured log endpoint	<code>grep -i hosts /etc/filebeat/filebeat.yml</code>	
	Confirm the external_id	<code>grep -i external_id /etc/filebeat/filebeat.yml</code>	
	Confirm the tenant ID	<code>grep -i tenant_id /etc/filebeat/filebeat.yml</code>	

## Step 2: Check Connectivity

Port	Destination
515/tcp	<ul style="list-style-type: none"> <li>46.88.106.196 <ul style="list-style-type: none"> <li>(<a href="https://1a.log.armor.com">1a.log.armor.com</a>)</li> </ul> </li> <li>146.88.144.196 <ul style="list-style-type: none"> <li>(<a href="https://2a.log.armor.com">2a.log.armor.com</a>)</li> </ul> </li> </ul>

## Malware

### Step 1: Verify the Status of the Agent

	Description	Command
<b>Windows</b>	Verify that the service is <b>running</b>	<code>gsv -displayname *trend*</code>
<b>Linux</b>	Verify that the service is <b>running</b>	<code>ps_axu   grep ds_agent</code>

### Step 2: Check the Connectivity of the Agent

	Description	Command
<b>Windows</b>	Verify the URL endpoint <b>epsec.armor.com</b>	<code>&amp; "C:\Program Files\Trend Micro\Deep Security Agent\dsa_query.cmd" -c GetAgentStatus   sls -pattern url</code>
	Confirm connection to the URL	<code>new-object System.Net.Sockets.TcpClient('146.88.106.210', 443)</code>
<b>Linux</b>	Verify the URL endpoint <b>epsec.armor.com</b>	<code>/opt/ds_agent/dsa_query -c GetAgentStatus   grep AgentStatus.dsmUrl</code>
	Confirm connection to the URL	<code>telnet 146.88.106.210 443</code>

### Step 3: Manually Heartbeat the Agent

	Description	Command
<b>Windows</b>	Verify a 200 response	<pre>PS C:\Users\Administrator&gt; &amp; "C:\Program Files\Trend Micro\Deep Security Agent\dsa_control.cmd" -m HTTP Status: 200 - OK Response: Manager contact has been scheduled to occur in the next few seconds.</pre>
<b>Linux</b>	Verify a 200 response	<code>/opt/ds_agent/dsa_control -m</code>

### Step 1: Verify the Status of the Agent

	Description	Command
<b>Windows</b>	Verify that the service is <b>running</b>	<code>gsv -displayname *trend*</code>

<b>Linux</b>	Verify that the service is <b>running</b>	<code>ps_axu   grep ds_agent</code>
--------------	---	-------------------------------------

### Step 2: Check the Connectivity of the Agent

	Description	Command
<b>Windows</b>	Verify the URL endpoint <a href="https://c.armor.com">epse.c.armor.com</a>	<code>&amp; "C:\Program Files\Trend Micro\Deep Security Agent\dsa_query.cmd" -c GetAgentStatus   sls -pattern url</code>
	Confirm connection to the URL	<code>new-object System.Net.Sockets.TcpClient('146.88.106.210', 443)</code>
<b>Linux</b>	Verify the URL endpoint <a href="https://c.armor.com">epse.c.armor.com</a>	<code>/opt/ds_agent/dsa_query -c GetAgentStatus   grep AgentStatus.dsmUrl</code>
	Confirm connection to the URL	<code>telnet 146.88.106.210 443</code>

### Step 3: Manually Heartbeat the Agent

	Description	Command
<b>Windows</b>	Verify a 200 response	<pre>PS C:\Users\Administrator&gt; &amp; "C:\Program Files\Trend Micro\Deep Security Agent\dsa_control.cmd" -m HTTP Status: 200 - OK Response: Manager contact has been scheduled to occur in the next few seconds.</pre>
<b>Linux</b>	Verify a 200 response	<code>/opt/ds_agent/dsa_control -m</code>

### Step 4: Check the Components for the Agent

<b>Windows</b>	<code>&amp; "C:\Program Files\Trend Micro\Deep Security Agent\dsa_query.cmd" -c GetComponentInfo   sls -pattern Component.AM</code>
<b>Linux</b>	<code>/opt/ds_agent/dsa_query -c GetComponentInfo   grep Component.AM</code>

**Component.AM.mode** describes if the Malware Protection module is installed.

**Component.AM.rules** is the number of rules derived from the Armor Deep Security Manager.

Step 1: Reboot your server

## File Integrity Monitoring (FIM)

### Step 1: Verify the Status of the Agent

	Description	Command
<b>Windows</b>	Verify that the service is <b>running</b>	<code>gsv -displayname *trend*</code>
<b>Linux</b>	Verify that the service is <b>running</b>	<code>ps_axu   grep ds_agent</code>

### Step 2: Check the Connectivity of the Agent

	Description	Command
<b>Windows</b>	Verify the URL endpoint <a href="https://c.armor.com">epse.c.armor.com</a>	<code>&amp; "C:\Program Files\Trend Micro\Deep Security Agent\dsa_query.cmd" -c GetAgentStatus   sls -pattern url</code>

	Confirm connection to the URL	<code>new-object System.Net.Sockets.TcpClient('146.88.106.210', 443)</code>
<b>Linux</b>	Verify the URL endpoint <a href="https://c.armor.com">epse.c.armor.com</a>	<code>/opt/ds_agent/dsa_query -c GetAgentStatus   grep AgentStatus.dsmUrl</code>
	Confirm connection to the URL	<code>telnet 146.88.106.210 443</code>

### Step 3: Manually Heartbeat the Agent

	Description	Command
<b>Windows</b>	Verify a 200 response	<pre>PS C:\Users\Administrator&gt; &amp; "C:\Program Files\Trend Micro\Deep Security Agent\dsa_control.cmd" -m HTTP Status: 200 - OK Response: Manager contact has been scheduled to occur in the next few seconds.</pre>
<b>Linux</b>	Verify a 200 response	<code>/opt/ds_agent/dsa_control -m</code>

### Step 1: Verify the Status of the Agent

	Description	Command
<b>Windows</b>	Verify that the service is <b>running</b>	<code>gsv -displayname *trend*</code>
<b>Linux</b>	Verify that the service is <b>running</b>	<code>ps_axu   grep ds_agent</code>

### Step 2: Check the Connectivity of the Agent

	Description	Command
<b>Windows</b>	Verify the URL endpoint <a href="https://c.armor.com">epse.c.armor.com</a>	<code>&amp; "C:\Program Files\Trend Micro\Deep Security Agent\dsa_query.cmd" -c GetAgentStatus   sls -pattern url</code>
	Confirm connection to the URL	<code>new-object System.Net.Sockets.TcpClient('146.88.106.210', 443)</code>
<b>Linux</b>	Verify the URL endpoint <a href="https://c.armor.com">epse.c.armor.com</a>	<code>/opt/ds_agent/dsa_query -c GetAgentStatus   grep AgentStatus.dsmUrl</code>
	Confirm connection to the URL	<code>telnet 146.88.106.210 443</code>

### Step 3: Manually Heartbeat the Agent

	Description	Command
<b>Windows</b>	Verify a 200 response	<pre>PS C:\Users\Administrator&gt; &amp; "C:\Program Files\Trend Micro\Deep Security Agent\dsa_control.cmd" -m HTTP Status: 200 - OK Response: Manager contact has been scheduled to occur in the next few seconds.</pre>
<b>Linux</b>	Verify a 200 response	<code>/opt/ds_agent/dsa_control -m</code>

### Step 4: Check the Components for the Agent

<b>Windows</b>	& "C:\Program Files\Trend Micro\Deep Security Agent\dsa_query.cmd" -c GetComponentInfo   sls -pattern Component.IM
<b>Linux</b>	/opt/ds_agent/dsa_query -c GetComponentInfo   grep Component.IM

### Step 1: Verify the Status of the Agent

	Description	Command
<b>Windows</b>	Verify that the service is <b>running</b>	gsv -displayname *trend*
<b>Linux</b>	Verify that the service is <b>running</b>	ps_axu   grep ds_agent

### Step 2: Check the Connectivity of the Agent

	Description	Command
<b>Windows</b>	Verify the URL endpoint <a href="https://c.armor.com">epse c.armor.com</a>	& "C:\Program Files\Trend Micro\Deep Security Agent\dsa_query.cmd" -c GetAgentStatus   sls -pattern url
	Confirm connection to the URL	new-object System.Net.Sockets.TcpClient('146.88.106.210', 443)
<b>Linux</b>	Verify the URL endpoint <a href="https://c.armor.com">epse c.armor.com</a>	/opt/ds_agent/dsa_query -c GetAgentStatus   grep AgentStatus.dsmUrl
	Confirm connection to the URL	telnet 146.88.106.210 443

### Step 3: Manually Heartbeat the Agent

	Description	Command
<b>Windows</b>	Verify a 200 response	PS C:\Users\Administrator> & "C:\Program Files\Trend Micro\Deep Security Agent\dsa_control.cmd" -m HTTP Status: 200 - OK Response: Manager contact has been scheduled to occur in the next few seconds.
<b>Linux</b>	Verify a 200 response	/opt/ds_agent/dsa_control -m

## Export Protection Screen Data

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Protection**.
3. (Optional) Use the search bar to customize the data displayed.
4. Below the table, click **CSV**. You have the option to export all the data (**All**) or only the data that appears on the current screen (**Current Set**).

Column	Description
<b>Asset Name</b>	This column display the name of the virtual machine (or instance).
<b>Location</b>	This column displays the data center location for for the virtual machine (or instance).

<b>Service</b>	<p>For <b>Armor Complete</b>, the <b>Protection</b> scores focuses on the following services:</p> <ul style="list-style-type: none"> <li>• Malware Protection</li> <li>• FIM</li> <li>• Filebeat (for Linux)</li> <li>• Winlogbeat (for Windows)</li> </ul> <p>For <b>Armor Anywhere</b>, the <b>Protection</b> scores focuses on the following services:</p> <ul style="list-style-type: none"> <li>• Malware Protection</li> <li>• FIM</li> <li>• IDS</li> <li>• Filebeat (for Linux)</li> <li>• Winlogbeat (for Windows)</li> <li>• Vulnerability Scanning</li> </ul>
<b>Status</b>	<p>This column displays the security status of the virtual machine (or instance), which can be:</p> <ul style="list-style-type: none"> <li>• Warning</li> <li>• Needs Attention</li> <li>• OK</li> </ul>
<b>Message</b>	<p>This column displays a brief message to explain the reason for the <b>Warning</b> or <b>Needs Attention</b> status.</p>



Was this helpful? \*

Your Rating: ☆☆☆☆☆

Results: ★★★★★ 5 rates