

Protection Dashboard

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

- The agent is responding (heartbeat) 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								
Protection Score	<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">• For Armor Complete, only virtual machines that are in a Powered On state are included.• For Armor Anywhere, only virtual machines that have communicated (heartbeat) with Armor in the last 4 hours are included. <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								
Assets Protected	This widget displays the number of virtual machines that contain the Armor agent.								
Healthy Services	This widget displays the percentage of agents and subagents that are working properly.								
Protection Score Trend	This graph displays the history of your protection scores.								

Understand Service Health

The **Service Health** section displays the virtual machines that contain the installed Armor agent. To view this section, you must have the **Read Virtual Machines(s)** permission assigned to your account.

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

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 [Support Tickets](#).

Logging

Verify the Status of filebeat

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



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

Step 1: Check Logging Services

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

Step 2: Check Connectivity

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

Malware

Step 1: Verify the Status of the Agent

	Description	Command

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

Step 2: Check the Connectivity of the Agent

	Description	Command
Windows	Verify the URL endpoint epse.c.armor.com	<code>& "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>
Linux	Verify the URL endpoint epse.c.armor.com	<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
Windows	Verify a 200 response	<pre>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.</pre>
Linux	Verify a 200 response	<code>/opt/ds_agent/dsa_control -m</code>

Step 1: Verify the Status of the Agent

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

Step 2: Check the Connectivity of the Agent

	Description	Command
Windows	Verify the URL endpoint epse.c.armor.com	<code>& "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>
Linux	Verify the URL endpoint epse.c.armor.com	<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
--	-------------	---------

Windows	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.
Linux	Verify a 200 response	/opt/ds_agent/dsa_control -m

Step 4: Check the Components for the Agent

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

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
Windows	Verify that the service is running	gsv -displayname *trend*
Linux	Verify that the service is running	ps_axu grep ds_agent

Step 2: Check the Connectivity of the Agent

	Description	Command
Windows	Verify the URL endpoint epse c.armor.com	& "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)
Linux	Verify the URL endpoint epse c.armor.com	/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
Windows	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.
Linux	Verify a 200 response	/opt/ds_agent/dsa_control -m

Step 1: Verify the Status of the Agent

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

Step 2: Check the Connectivity of the Agent

	Description	Command
Windows	Verify the URL endpoint epse c.armor.com	<code>& "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>
Linux	Verify the URL endpoint epse c.armor.com	<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
Windows	Verify a 200 response	<pre>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.</pre>
Linux	Verify a 200 response	<code>/opt/ds_agent/dsa_control -m</code>

Step 4: Check the Components for the Agent

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

Step 1: Verify the Status of the Agent

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

Step 2: Check the Connectivity of the Agent

	Description	Command
Windows	Verify the URL endpoint epse c.armor.com	<code>& "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>

Linux	Verify the URL endpoint epsec.armor.com	/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
Windows	Verify a 200 response	<pre>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.</pre>
Linux	Verify a 200 response	<pre>/opt/ds_agent/dsa_control -m</pre>

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



Was this helpful? *

Your Rating: 

Results:  3 rates