Protection Dashboard

Armor Knowledge Base

Topics Discussed

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

- The agent is responding (hearbeating) 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

<table>
<tr><th>Widget and Graph Type</th><th>Description</th></tr>
<tr><td>Protection Score</td><td>This widget displays a calculated score that includes the number of subagents in an unhealthy state.

<table><tr><th>Score Range</th><th>Health Status</th></tr><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></table>
• For Armor Complete, only virtual machines that are in a Powered On state are included.
• For Armor Anywhere, only virtual machines that have communicated (heartbeated) with Armor in the last 4 hours are included.

Scores in the security dashboards are calculated and updated every night at 2:00 AM UTC.</td></tr>
<tr><td>Assets Protected</td><td>This widget displays the number of virtual machines that contain the Armor agent.

⚠ Newly created virtual machines will not be reflected in the number of Assets Protected until the following day.</td></tr>
<tr><td>Healthy Services</td><td>This widget displays the percentage of agents and subagents that are working properly.</td></tr>
<tr><td>Protection Score Trend</td><td>This graph displays the history of your protection scores.</td></tr>
</table>

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
Asset Name	This column displays the name of the virtual machine. You can click the name of the virtual machine to access the **Virtual Machine** details screen.

Status	This column displays the security status of the virtual machine.
	
	• **Unprotected** indicates the agent is not installed in the instance.
	  ◦ 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 (heartbeated) with Armor.
	  ◦ To troubleshoot a specific error message under **Needs Attention**, see Troubleshoot Protection Scores.
	• **OK** indicates that the agent is installed and has communicated (hearbeated) with Armor.

Location	For **Armor Complete**, this column will display name of the Armor virtual site. For **Armor Anywhere**, this column will display the name of the public cloud provider.
Ticket	This column displays the support ticket that troubleshoots the **Protection** issue. A **Protection** 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

Windows	Configurations are stored in the winlogbeat and filebeat directory within **C:\.armor\opt**	`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`
			• Windows uses both winlogbeat and filebeat.
			• Commands should run in Powershell.
			• To review additional configurations, certificates, and service information, review a server's directory:
			  ◦ C:\.armor\opt\winlogbeat*
			  ◦ C:\.armor\opt\filebeat*

	To verify the operation of the logging services, look for **winlogbeat**, **filebeat**	`gsv -displayname armor-winlogbeat, armor-filebeat`	
	To verify the operation of the logging service processes, look for **winlogbeat**	`gps filebeat,winlogbeat`	

	Confirm the configured log endpoint	`cat C:\.armor\opt\winlogbeat-5.2.0-windows-x86_64\winlogbeat.yml | sls hosts`	
Linux	Configurations are stored within **/etc/filebeat/filebeat.yml**	`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 **C:\.armor\opt**	`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`
		• Windows uses both winlogbeat and filebeat.
		• Commands should run in Powershell.
		• To review additional configurations, certificates, and service information, review a server's directory:
		  ◦ C:\.armor\opt\winlogbeat*
		  ◦ C:\.armor\opt\filebeat*

To verify the operation of the logging services, look for **winlogbeat**, **filebeat**	`gsv -displayname armor-winlogbeat, armor-filebeat`	
To verify the operation of the logging service processes, look for **winlogbeat**	`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

Windows	Configurations are stored in the winlogbeat and filebeat directory within **C:\.armor\opt**	`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`
			• Windows uses both winlogbeat and filebeat.
			• Commands should run in Powershell.
			• To review additional configurations, certificates, and service information, review a server's directory:
			  ◦ C:\.armor\opt\winlogbeat*
			  ◦ C:\.armor\opt\filebeat*

	To verify the operation of the logging services, look for **winlogbeat**, **filebeat**	`gsv -displayname armor-winlogbeat, armor-filebeat`	
	To verify the operation of the logging service processes, look for **winlogbeat**	`gps filebeat,winlogbeat`	
	Confirm the configured log endpoint	`cat C:\.armor\opt\winlogbeat-5.2.0-windows-x86_64\winlogbeat.yml | sls hosts`	
Linux	Configurations are stored within **/etc/filebeat/filebeat.yml**	`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`	

Step 2: Check Connectivity

Port	Destination

515/tcp	• 46.88.106.196
	  • (1a.log.armor.com)
	• 146.88.144.196
	  • (2a.log.armor.com)

Malware

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 **epsec.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 **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	`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**	`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 **epsec.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 **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	`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 **epsec.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 **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	`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**	`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 **epsec.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 **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	`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.IM`
Linux	`/opt/ds_agent/dsa_query -c GetComponentInfo | grep Component.IM`

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 **epsec.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 **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	`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`

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	For **Armor Complete**, the **Protection** scores focuses on the following services: • Malware Protection • FIM • Filebeat (for Linux) • Winlogbeat (for Windows) For **Armor Anywhere**, the **Protection** scores focuses on the following services: • Malware Protection • FIM • IDS • Filebeat (for Linux) • Winlogbeat (for Windows) • Vulnerability Scanning
Status	This column displays the security status of the virtual machine (or instance), which can be: • Warning • Needs Attention • OK
Message	This column displays a brief message to explain the reason for the **Warning** or **Needs Attention** status.