

ANYWHERE Protection Dashboard

Armor Knowledge Base

Topics Discussed

- [Review Widgets and Graph](#)
- [Understand Service Health](#)
- [Health Rules](#)
- [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 Anywhere**, the **Protection** scores focuses on the following services:

- Malware Protection
- FIM
- IDS
- Filebeat (for Windows and Linux)
- Winlogbeat (for Windows)
- Vulnerability Scanning

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> <p> <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 (heartbeated) with Armor in the last 4 hours are included.</p> <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	<p>This widget displays the number of virtual machines that contain the Armor agent.</p> <p> Newly created virtual machines will not be reflected in the number of Assets Protected until the following day.</p>								
Healthy Services	<p>This widget displays the percentage of agents and subagents that are working properly.</p>								
Protection Score Trend	<p>This graph displays the history of your protection scores.</p>								

Understand Service Health

The **Service Health** section 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. <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 (heartbeated) 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 (heartbeated) 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.

Health Rules

Health Rules calculates the status of several managed services provided or orchestrated by Armor. The status of these checks roll into AMP's *Protection* and help guide our support and remediation efforts.

The health rules are grouped under each Rule Family.

Types of Rule Family

1. Armor Agent
2. File Logging
3. FIM
4. IDS
5. Log Collector
6. Malware Protection
7. OS Monitoring
8. Vulnerability Scanning
9. Windows Event Logging

Rule Family	Rule	Description	Service	Frequency
Armor Agent	HasRecentHeartbeat	If latest CORE heartbeat is > 4 hours	Armor Agent	Hourly
Armor Agent	HasCorrectVersion	If CORE Agent is not running latest version	Armor Agent	Hourly
File Logging	HasCorrectVersion	If Filebeat is not running the latest version	Filebeat	Hourly
File Logging	HasRecentLogs	If last received log for that CoreinstanceId is > 4 hours from ELK	Filebeat	Hourly
File Logging	IsInstalled	If Filebeat agent is not installed	Filebeat	Hourly
Window Event Logging	HasCorrectVersion	If Winlogbeat is not running the latest version	Winlogbeat	Hourly
Window Event Logging	HasRecentLogs	if last received log for that CoreinstanceId is > 4 hours from ELK	Winlogbeat	Hourly
Window Event Logging	IsInstalled	If Winlogbeat agent is not installed	Winlogbeat	Hourly

FIM	HasRecentHeartbeat	If latest Trend heartbeat is > 4 hours	Trend	Hourly
FIM	IsPluginPresent	If FIM is "On, matching module plug-in not found" Example : FIM On but Module Not Found	Trend	Hourly
FIM	IsRealtimeOrHasRules	If FIM is not "On, Realtime", or "On" with > 0 rules (Example: FIM On but No Policy	Trend	Hourly
FIM	ModuleIsOn	If FIM is not "On"	Trend	Hourly
IDS	HasRecentHeartbeat	if latest Trend heartbeat is > 4 hours	Trend	Hourly
IDS	HasRules	If IDS is "On" and has > 0 rules Example: IDS installed but no rules	Trend	Hourly
IDS	IsOnTapMode	If IDS is "On" and has tap mode on	Trend	Hourly
IDS	ModuleIsOn	If IDS is not "On"	Trend	Hourly
Malware Protection	HasAgentFailed	if Anti-Malware update failed	Trend	Hourly
Malware Protection	HasRecentHeartbeat	If latest Trend heartbeat is > 4 hours old	Trend	Hourly
Malware Protection	IsRebootRequired	if Anti-Malware status is "Computer reboot required"	Trend	Hourly
Malware Protection	ModuleIsOn	If Anti-Malware is not "On"	Trend	Hourly
Malware Protection	ModuleOnPluginNotFound	If Anti-Malware is "On, matching module plug-in not found"	Trend	Hourly
OS Monitoring	HasCorrectVersion	If Panopta is not running the latest version	Panopta	Hourly
OS Monitoring	IsInstalled	If Panopta is not Installed	Panopta	Hourly
Vulnerability Scanning	InMostRecentScan	If IR Agent did not scan in previous scan period	IR Agent	10 PM UTC once in Sunday
Vulnerability Scanning	IsInstalled	If IR Agent is not installed	IR Agent	10 PM UTC once in Sunday
Log Collector	HasDelayedLogs	if Events from this Log Collector are averaging longer than 1 hour to be received	Logstash	Hourly
Log Collector	HasRecentLogs	if events from this Log Collector have been received > 80%	Logstash	Hourly


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

	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	<code>gps filebeat, winlogbeat</code>	
	Confirm the configured log endpoint	<code>cat C:\.armor\opt\winlogbeat-5.2.0-windows-x86_64\winlogbeat.yml sls hosts</code>	
Linux	Configurations are stored within /etc/filebeat/filebeat.yml	<code>cat /etc/filebeat/*.yml</code>	
	Verify the operation of the filebeat service	<code>ps aux grep filebeat</code>	
	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 1: Verify the status of filebeat



This section only applies to Windows users.

Description	Command	Extra Information
Configurations are stored in the winlogbeat and filebeat directory within C:\.armor\opt\	<code>cat C:\.armor\opt\winlogbeat-5.2.0-windows-x86_64\winlogbeat.yml</code> <code>cat C:\.armor\opt\filebeat-5.2.0-windows-x86_64\filebeat.yml</code>	<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	<code>gsv -displayname armor-winlogbeat, armor-filebeat</code>	
To verify the operation of the logging service processes, look for winlogbeat	<code>gps filebeat, winlogbeat</code>	
Confirm the configured log endpoint	<code>cat C:\.armor\opt\winlogbeat-5.2.0-windows-x86_64\winlogbeat.yml sls hosts</code>	

Step 1: Check Logging Services

	Description	Command	Extra information
Windows	Configurations are stored in the winlogbeat and filebeat directory within C:\.armor\opt\	<code>cat C:\.armor\opt\winlogbeat-5.2.0-windows-x86_64\winlogbeat.yml</code> <code>cat C:\.armor\opt\filebeat-5.2.0-windows-x86_64\filebeat.yml</code>	<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	<code>gsv -displayname armor-winlogbeat, armor-filebeat</code>	
	To verify the operation of the logging service processes, look for winlogbeat	<code>gps filebeat, winlogbeat</code>	
	Confirm the configured log endpoint	<code>cat C:\.armor\opt\winlogbeat-5.2.0-windows-x86_64\winlogbeat.yml sls hosts</code>	
Linux	Configurations are stored within /etc/filebeat/filebeat.yml	<code>cat /etc/filebeat/*.yml</code>	

	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	<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 Protection

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	<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>
--------------	-----------------------	---

Step 1: Verify the status of the agent

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

Step 2: Check the connectivity of the agent

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

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>

Step 4: Check the components for the agent

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



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	<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

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	& "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	<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	/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



Component.IM.mode describes if the FIM module is installed.

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

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	<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>

Intrusion Detection System (IDS)

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	<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>

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	<pre>/opt/ds_agent/dsa_control -m</pre>

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 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

Windows	<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	<pre>/opt/ds_agent/dsa_control -m</pre>

Vulnerability Scanning

Step 1: Verify the status of the agent

Windows	<ul style="list-style-type: none">IR Agent files are located within C:\Program Files\Rapid7The IR Agent service name is "Rapid7 Insight Agent"
Linux	<ul style="list-style-type: none">IR Agent files are located within /opt/rapid7/ir_agentIR Agent logs are located within /opt/rapid7/ir_agent/agent.log*Upgrade logs are one level above, within /opt/rapid7/upgrade*

Step 2: Check connectivity of the agent

Port	Destination
443/tcp (IR Agent)	<ul style="list-style-type: none">endpoint.ingress.rapid7.com *<ul style="list-style-type: none">(United States)eu.endpoint.ingress.rapid7.com *<ul style="list-style-type: none">(Europe, Middle East, Africa)



* The agent will perform a lookup to the applicable DNS entry, which may resolve to one of [multiple Amazon Web Services based subnets](#). As a result, if your firewall does not support outbound filtering by domain name, then you may need to open all outbound traffic to 443/tcp to accommodate this service.

Step 1: Verify the status of the agent

Windows	<ul style="list-style-type: none">IR Agent files are located within C:\Program Files\Rapid7The IR Agent service name is "Rapid7 Insight Agent"
Linux	<ul style="list-style-type: none">IR Agent files are located within /opt/rapid7/ir_agentIR Agent logs are located within /opt/rapid7/ir_agent/agent.log*Upgrade logs are one level above, within /opt/rapid7/upgrade*

Step 2: Check connectivity of the agent

Port	Destination
443/tcp (IR Agent)	<ul style="list-style-type: none">endpoint.ingress.rapid7.com *<ul style="list-style-type: none">(United States)eu.endpoint.ingress.rapid7.com *<ul style="list-style-type: none">(Europe, Middle East, Africa)



* The agent will perform a lookup to the applicable DNS entry, which may resolve to one of [multiple Amazon Web Services based subnets](#). As a result, if your firewall does not support outbound filtering by domain name, then you may need to open all outbound traffic to 443/tcp to accommodate this service.

Step 1: Verify the status of the agent

Windows	<ul style="list-style-type: none">IR Agent files are located within C:\Program Files\Rapid7The IR Agent service name is "Rapid7 Insight Agent"
Linux	<ul style="list-style-type: none">IR Agent files are located within /opt/rapid7/ir_agentIR Agent logs are located within /opt/rapid7/ir_agent/agent.log*Upgrade logs are one level above, within /opt/rapid7/upgrade*

Step 2: Check connectivity of the agent

Port	Destination
443/tcp (IR Agent)	<ul style="list-style-type: none">endpoint.ingress.rapid7.com *<ul style="list-style-type: none">(United States)eu.endpoint.ingress.rapid7.com *<ul style="list-style-type: none">(Europe, Middle East, Africa)



* The agent will perform a lookup to the applicable DNS entry, which may resolve to one of [multiple Amazon Web Services based subnets](#). As a result, if your firewall does not support outbound filtering by domain name, then you may need to open all outbound traffic to 443/tcp to accommodate this service.

Step 3: Re-install the Armor agent.


Step 1: Verify the status of the agent

Windows	<ul style="list-style-type: none">IR Agent files are located within C:\Program Files\Rapid7The IR Agent service name is "Rapid7 Insight Agent"
----------------	---

Linux	<ul style="list-style-type: none"> • IR Agent files are located within /opt/rapid7/ir_agent • IR Agent logs are located within /opt/rapid7/ir_agent/agent.log* • Upgrade logs are one level above, within /opt/rapid7/upgrade*
--------------	---

Step 2: Check connectivity of the agent

Port	Destination
443/tcp (IR Agent)	<ul style="list-style-type: none"> • endpoint.ingress.rapid7.com * <ul style="list-style-type: none"> • (United States) • eu.endpoint.ingress.rapid7.com * <ul style="list-style-type: none"> • (Europe, Middle East, Africa)

 * The agent will perform a lookup to the applicable DNS entry, which may resolve to one of [multiple Amazon Web Services based subnets](#). As a result, if your firewall does not support outbound filtering by domain name, then you may need to open all outbound traffic to 443/tcp to accommodate this service.

Step 3: Re-install the Armor agent.

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: 13 rates