Remediation steps to improve Protection scores

Overview

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.

Logging

Armor Service	Issue	Remediation

Logging	The filebeat logging agent is not installed.

	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 winlogbeat,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`	

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Support**.
2. Click **Tickets**.
3. Click **Create A Ticket**.
   - A new tab will appear in your web browser.

   > In the top right corner of the **Armor Ticketing System** screen, click the **Open AMP** button to easily return to your AMP account. A new tab will appear in your web browser.

4. On the **Armor Ticketing System** screen, review the categories for ticket request types. These request types are used internally to automatically route your ticket to the appropriate department for a more efficient response.

Category	Support for Urgent Issues	Common Requests	Other Requests	Account Requests
Request Type	• **Outage** - Report an Outage • **Performance Issue** - Report device performance or degradation issue • **General Incident** - Report an Unlisted Incident • **Potential Security Incident** - Report a Potential Security Issue	• **Armor Services** - Armor Agent Services, Logging, Monitoring, etc. • **VPN** - VPN Inquiries • **Armor Portal** - AMP Inquiries and Requests • **L2L Tunnels** • **WAF** - WAF Exceptions and Requests • **Firewall** - Inquiries on Self-Service Firewall Rules • **SSL Certificate**	• **Backup Service** - Backup Services Request • **Disaster Recovery Service** • **DNS** - Add/Configure DNS Records • **Encryption Service** - Encryption Service Request • **Load Balancer** - Load Balancer Appliance Request • **OS Patching / Updates** - Request for OS Patching and Updates • **Vulnerability Scanning** - Vulnerability Scanning Services • **Recurring Issue** - Report a Recurring or Periodically Repeating Problem • **Professional Services** - Request a Statement of Work for Out of Scope Services	• **Access & Users** - Request for Access & User Management • **Billing / Invoices** - General Billing or Invoice Request • **Compliance** - Compliance or Audit Requests • **Legal / TOS / SLA** - Legal Inquiries • **Professional Services** - Request Statement of Work for Out of Scope Services • **Account Cancellation** - Cancel an Armor Account

5. In **Account**, select the AMP account that relates to the ticket.
6. Complete the missing fields.
   a. In **Summary**, enter a very brief description. You can only enter a maximum of 255 characters.
   b. In **Description**, enter useful details that can help Armor quickly troubleshoot the problem. For example, consider the following questions:
      - What is the specific issue?
      - What are the steps to reproduce the issue?
      - What is the level of business impact?
      - Are there additional contacts that should be notified?
      - Have there been any troubleshooting steps already performed?
      - Are there any error messages or screenshots to share?

   c. If applicable, in **Device**, enter the name of the affected virtual machine.
7. If applicable, add any screenshots to help explain the issue.
8. Click **Create**.
   - After you create the ticket, you will receive updates on the ticket via an email notification.

   > You can easily review the details and status of your existing ticket by clicking the **View Request** link provided within the email notifications that are generated from the ticketing system.

9. (Optional) After you create a ticket, you can add additional users or organizations to the ticket.
   a. On the ticket detail screen, in the right-side menu, click **Share**.
   b. Type the name of the user or the user's email address. To share with a specific organization, type the account name, and then select the desired organization (**Admin**, **Billing**, **Technical**, or **Security**).

   > The ticket can be shared with multiple users and organizations.

   c. Click **Share**.
10. (Optional) To view the status of this newly created ticket, in the **Tickets** screen, click **View Existing Tickets**.

<table>
<tr>
<td>Logging</td>
<td>The winlogbeat logging agent is not installed.

⚠ This section only applies to Windows users.</td>
<td>
<table>
<tr><th>Description</th><th>Command</th><th>Extra information</th></tr>
<tr><td>Configurations are stored in the winlogbeat and filebeat directory within C:\.armor\opt\</td><td><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></td><td>• 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*</td></tr>
<tr><td>To verify the operation of the logging services, look for winlogbeat, filebeat</td><td><code>gsv -displayname winlogbeat,filebeat</code></td><td></td></tr>
<tr><td>To verify the operation of the logging service processes, look for winlogbeat</td><td><code>gps filebeat,winlogbeat</code></td><td></td></tr>
<tr><td>Confirm the configured log endpoint</td><td><code>cat C:\.armor\opt\winlogbeat-5.2.0-windows-x86_64\winlogbeat.yml | sls hosts</code></td><td></td></tr>
</table>
Click the following link to open a support ticket in AMP: https://amp.armor.com/support/tickets/new
</td>
</tr>
<tr>
<td>Logging</td>
<td>Armor has not received a log in the past 4 hours.</td>
<td>
<table>
<tr><th></th><th>Description</th><th>Command</th><th>Extra information</th></tr>
<tr><td>Windows</td><td>Configurations are stored in the winlogbeat and filebeat directory within C:\.armor\opt\</td><td><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></td><td>• 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*</td></tr>
<tr><td></td><td>To verify the operation of the logging services, look for winlogbeat, filebeat</td><td><code>gsv -displayname winlogbeat,filebeat</code></td><td></td></tr>
<tr><td></td><td>To verify the operation of the logging service processes, look for winlogbeat</td><td><code>gps filebeat,winlogbeat</code></td><td></td></tr>
<tr><td></td><td>Confirm the configured log endpoint</td><td><code>cat C:\.armor\opt\winlogbeat-5.2.0-windows-x86_64\winlogbeat.yml | sls hosts</code></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>Linux</td><td>Configurations are stored within /etc/filebeat/filebeat.yml</td><td><code>cat /etc/filebeat/*.yml</code></td><td></td></tr>
<tr><td></td><td>Verify the operation of the filebeat service</td><td><code>ps aux | grep filebeat</code></td><td></td></tr>
<tr><td></td><td>Confirm the configured log endpoint</td><td><code>grep -i hosts /etc/filebeat/filebeat.yml</code></td><td></td></tr>
<tr><td></td><td>Confirm the external_id</td><td><code>grep -i external_id /etc/filebeat/filebeat.yml</code></td><td></td></tr>
<tr><td></td><td>Confirm the tenant ID</td><td><code>grep -i tenant_id /etc/filebeat/filebeat.yml</code></td><td></td></tr>
</table>
<table>
<tr><th>Port</th><th>Destination</th></tr>
<tr><td>515/tcp</td><td>• 46.88.106.196
  • (1a.log.armor.com)
• 146.88.144.196
  • (2a.log.armor.com)</td></tr>
</table>
</td>
</tr>
</table>

Malware Protection

<table>
<tr><th>Armor Service</th><th>Issue</th><th>Remediation</th></tr>
<tr>
<td>Malware Protection</td>
<td>Malware Protection has not provided a heartbeat in the past 4 hours.</td>
<td>
<table>
<tr><th></th><th>Description</th><th>Command</th></tr>
<tr><td>Windows</td><td>Verify that the service is running</td><td><code>gsv -displayname *trend*</code></td></tr>
<tr><td>Linux</td><td>Verify that the service is running</td><td><code>ps_axu | grep ds_agent</code></td></tr>
</table>
</td>
</tr>
</table>

	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`

	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`

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Support**.
2. Click **Tickets**.
3. Click **Create A Ticket**.
   - A new tab will appear in your web browser.

   > In the top right corner of the **Armor Ticketing System** screen, click the **Open AMP** button to easily return to your AMP account. A new tab will appear in your web browser.

4. On the **Armor Ticketing System** screen, review the categories for ticket request types. These request types are used internally to automatically route your ticket to the appropriate department for a more efficient response.

Category	Support for Urgent Issues	Common Requests	Other Requests	Account Requests
Request Type	• **Outage** - Report an Outage • **Performance Issue** - Report device performance or degradation issue • **General Incident** - Report an Unlisted Incident • **Potential Security Incident** - Report a Potential Security Issue	• **Armor Services** - Armor Agent Services, Logging, Monitoring, etc. • **VPN** - VPN Inquiries • **Armor Portal** - AMP Inquiries and Requests • **L2L Tunnels** • **WAF** - WAF Exceptions and Requests • **Firewall** - Inquiries on Self-Service Firewall Rules • **SSL Certificate**	• **Backup Service** - Backup Services Request • **Disaster Recovery Service** • **DNS** - Add/Configure DNS Records • **Encryption Service** - Encryption Service Request • **Load Balancer** - Load Balancer Appliance Request • **OS Patching / Updates** - Request for OS Patching and Updates • **Vulnerability Scanning** - Vulnerability Scanning Services • **Recurring Issue** - Report a Recurring or Periodically Repeating Problem • **Professional Services** - Request a Statement of Work for Out of Scope Services	• **Access & Users** - Request for Access & User Management • **Billing / Invoices** - General Billing or Invoice Request • **Compliance** - Compliance or Audit Requests • **Legal / TOS / SLA** - Legal Inquiries • **Professional Services** - Request Statement of Work for Out of Scope Services • **Account Cancellation** - Cancel an Armor Account

5. In **Account**, select the AMP account that relates to the ticket.
6. Complete the missing fields.
   a. In **Summary**, enter a very brief description. You can only enter a maximum of 255 characters.
   b. In **Description**, enter useful details that can help Armor quickly troubleshoot the problem. For example, consider the following questions:
      - What is the specific issue?
      - What are the steps to reproduce the issue?
      - What is the level of business impact?
      - Are there additional contacts that should be notified?
      - Have there been any troubleshooting steps already performed?
      - Are there any error messages or screenshots to share?

   c. If applicable, in **Device**, enter the name of the affected virtual machine.
7. If applicable, add any screenshots to help explain the issue.
8. Click **Create**.
   - After you create the ticket, you will receive updates on the ticket via an email notification.

   > You can easily review the details and status of your existing ticket by clicking the **View Request** link provided within the email notifications that are generated from the ticketing system.

9. (Optional) After you create a ticket, you can add additional users or organizations to the ticket.
   a. On the ticket detail screen, in the right-side menu, click **Share**.
   b. Type the name of the user or the user's email address. To share with a specific organization, type the account name, and then select the desired organization (**Admin**, **Billing**, **Technical**, or **Security**).

   > The ticket can be shared with multiple users and organizations.

   c. Click **Share**.
10. (Optional) To view the status of this newly created ticket, in the **Tickets** screen, click **View Existing Tickets**.

<table>
<tr>
<td>Malware Protection</td>
<td>Malware Protection is not installed or configured.</td>
<td>
<table>
<tr><th></th><th>Description</th><th>Command</th></tr>
<tr><td>Windows</td><td>Verify that the service is running</td><td><code>gsv -displayname *trend*</code></td></tr>
<tr><td>Linux</td><td>Verify that the service is running</td><td><code>ps_axu | grep ds_agent</code></td></tr>
</table>
<table>
<tr><th></th><th>Description</th><th>Command</th></tr>
<tr><td>Windows</td><td>Verify the URL endpoint epsec.armor.com</td><td><code>& "C:\Program Files\Trend Micro\Deep Security Agent\dsa_query.cmd" -c GetAgentStatus | sls -pattern url</code></td></tr>
<tr><td></td><td>Confirm connection to the URL</td><td><code>new-object System.Net.Sockets.TcpClient('146.88.106.210', 443)</code></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Linux</td><td>Verify the URL endpoint epsec.armor.com</td><td><code>/opt/ds_agent/dsa_query -c GetAgentStatus | grep AgentStatus.dsmUrl</code></td></tr>
<tr><td></td><td>Confirm connection to the URL</td><td><code>telnet 146.88.106.210 443</code></td></tr>
</table>
<table>
<tr><th></th><th>Description</th><th>Command</th></tr>
<tr><td>Windows</td><td>Verify a 200 response</td><td><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></td></tr>
<tr><td>Linux</td><td>Verify a 200 response</td><td><pre>/opt/ds_agent/dsa_control -m</pre></td></tr>
</table>
<table>
<tr><td>Windows</td><td><pre>& "C:\Program Files\Trend Micro\Deep Security Agent\dsa_query.cmd" -c GetComponentInfo | sls -pattern Component.AM</pre></td></tr>
<tr><td>Linux</td><td><pre>/opt/ds_agent/dsa_query -c GetComponentInfo | grep Component.AM</pre></td></tr>
</table>
⚠ 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.
Click the following link to open a support ticket in AMP: https://amp.armor.com/support/tickets/new
</td>
</tr>
<tr>
<td>Malware Protection</td>
<td>Reboot is required for Malware Protection.</td>
<td>Step 1: Reboot your server

Click the following link to open a support ticket in AMP: https://amp.armor.com/support/tickets/new</td>
</tr>
</table>

File Integrity Monitoring (FIM)

Armor Service	Issue	Remediation

<table>
<tr>
<td>File Integirty Monitoring (FIM)</td>
<td>FIM has not provided a heartbeat in the past 4 hours.</td>
<td>
<table>
<tr><th></th><th>Description</th><th>Command</th></tr>
<tr><td>Windows</td><td>Verify that the service is running</td><td><code>gsv -displayname *trend*</code></td></tr>
<tr><td>Linux</td><td>Verify that the service is running</td><td><code>ps_axu | grep ds_agent</code></td></tr>
</table>
<table>
<tr><th></th><th>Description</th><th>Command</th></tr>
<tr><td>Windows</td><td>Verify the URL endpoint epsec.armor.com</td><td><code>& "C:\Program Files\Trend Micro\Deep Security Agent\dsa_query.cmd" -c GetAgentStatus | sls -pattern url</code></td></tr>
<tr><td></td><td>Confirm connection to the URL</td><td><code>new-object System.Net.Sockets.TcpClient('146.88.106.210', 443)</code></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Linux</td><td>Verify the URL endpoint epsec.armor.com</td><td><code>/opt/ds_agent/dsa_query -c GetAgentStatus | grep AgentStatus.dsmUrl</code></td></tr>
<tr><td></td><td>Confirm connection to the URL</td><td><code>telnet 146.88.106.210 443</code></td></tr>
</table>
<table>
<tr><th></th><th>Description</th><th>Command</th></tr>
<tr><td>Windows</td><td>Verify a 200 response</td><td><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></td></tr>
<tr><td>Linux</td><td>Verify a 200 response</td><td><pre>/opt/ds_agent/dsa_control -m</pre></td></tr>
</table>
Click the following link to open a support ticket in AMP: https://amp.armor.com/support/tickets/new
</td>
</tr>
</table>

File Integrity Monitoring (FIM)

FIM is installed but has not been configured.

	Description	Command
Windows	Verify that the service is **running**	`gsv -displayname *trend*`
Linux	Verify that the service is **running**	`ps_axu | grep ds_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`

	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`

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.

Click the following link to open a support ticket in AMP: https://amp.armor.com/support/tickets/new

<table>
<tr>
<td>File Integirty Monitoring (FIM)</td>
<td>FIM is not installed.</td>
<td>
<table>
<tr><th></th><th>Description</th><th>Command</th></tr>
<tr><td>Windows</td><td>Verify that the service is running</td><td><code>gsv -displayname *trend*</code></td></tr>
<tr><td>Linux</td><td>Verify that the service is running</td><td><code>ps_axu | grep ds_agent</code></td></tr>
</table>
<table>
<tr><th></th><th>Description</th><th>Command</th></tr>
<tr><td>Windows</td><td>Verify the URL endpoint epsec.armor.com</td><td><code>& "C:\Program Files\Trend Micro\Deep Security Agent\dsa_query.cmd" -c GetAgentStatus | sls -pattern url</code></td></tr>
<tr><td></td><td>Confirm connection to the URL</td><td><code>new-object System.Net.Sockets.TcpClient('146.88.106.210', 443)</code></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Linux</td><td>Verify the URL endpoint epsec.armor.com</td><td><code>/opt/ds_agent/dsa_query -c GetAgentStatus | grep AgentStatus.dsmUrl</code></td></tr>
<tr><td></td><td>Confirm connection to the URL</td><td><code>telnet 146.88.106.210 443</code></td></tr>
</table>
<table>
<tr><th></th><th>Description</th><th>Command</th></tr>
<tr><td>Windows</td><td>Verify a 200 response</td><td><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></td></tr>
<tr><td>Linux</td><td>Verify a 200 response</td><td><pre>/opt/ds_agent/dsa_control -m</pre></td></tr>
</table>
Click the following link to open a support ticket in AMP: https://amp.armor.com/support/tickets/new
</td>
</tr>
</table>

Intrusion Detection System (IDS)

Armor Service	Issue	Remediation

<table>
<tr>
<td>IDS</td>
<td>IDS has not provided a heartbeat in the past 4 hours.</td>
<td>
<table>
<tr><th></th><th>Description</th><th>Command</th></tr>
<tr><td>Windows</td><td>Verify that the service is running</td><td><code>gsv -displayname *trend*</code></td></tr>
<tr><td>Linux</td><td>Verify that the service is running</td><td><code>ps_axu | grep ds_agent</code></td></tr>
</table>
<table>
<tr><th></th><th>Description</th><th>Command</th></tr>
<tr><td>Windows</td><td>Verify the URL endpoint epsec.armor.com</td><td><code>& "C:\Program Files\Trend Micro\Deep Security Agent\dsa_query.cmd" -c GetAgentStatus | sls -pattern url</code></td></tr>
<tr><td></td><td>Confirm connection to the URL</td><td><code>new-object System.Net.Sockets.TcpClient('146.88.106.210', 443)</code></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Linux</td><td>Verify the URL endpoint epsec.armor.com</td><td><code>/opt/ds_agent/dsa_query -c GetAgentStatus | grep AgentStatus.dsmUrl</code></td></tr>
<tr><td></td><td>Confirm connection to the URL</td><td><code>telnet 146.88.106.210 443</code></td></tr>
</table>
<table>
<tr><th></th><th>Description</th><th>Command</th></tr>
<tr><td>Windows</td><td>Verify a 200 response</td><td><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></td></tr>
<tr><td>Linux</td><td>Verify a 200 response</td><td><pre>/opt/ds_agent/dsa_control -m</pre></td></tr>
</table>
Click the following link to open a support ticket in AMP: https://amp.armor.com/support/tickets/new
</td>
</tr>
</table>

<table>
<tr>
<td>IDS</td>
<td>IDS is installed but has not been configured.</td>
<td>
<table>
<tr><th></th><th>Description</th><th>Command</th></tr>
<tr><td>Windows</td><td>Verify that the service is running</td><td><code>gsv -displayname *trend*</code></td></tr>
<tr><td>Linux</td><td>Verify that the service is running</td><td><code>ps_axu | grep ds_agent</code></td></tr>
</table>
<table>
<tr><th></th><th>Description</th><th>Command</th></tr>
<tr><td>Windows</td><td>Verify the URL endpoint epsec.armor.com</td><td><code>& "C:\Program Files\Trend Micro\Deep Security Agent\dsa_query.cmd" -c GetAgentStatus | sls -pattern url</code></td></tr>
<tr><td></td><td>Confirm connection to the URL</td><td><code>new-object System.Net.Sockets.TcpClient('146.88.106.210', 443)</code></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Linux</td><td>Verify the URL endpoint epsec.armor.com</td><td><code>/opt/ds_agent/dsa_query -c GetAgentStatus | grep AgentStatus.dsmUrl</code></td></tr>
<tr><td></td><td>Confirm connection to the URL</td><td><code>telnet 146.88.106.210 443</code></td></tr>
</table>
<table>
<tr><th></th><th>Description</th><th>Command</th></tr>
<tr><td>Windows</td><td>Verify a 200 response</td><td><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></td></tr>
<tr><td>Linux</td><td>Verify a 200 response</td><td><pre>/opt/ds_agent/dsa_control -m</pre></td></tr>
</table>
Click the following link to open a support ticket in AMP: https://amp.armor.com/support/tickets/new
</td>
</tr>
</table>

<table>
<tr>
<td>IDS</td>
<td>IDS is not installed or enabled.</td>
<td>
<table>
<tr><th></th><th>Description</th><th>Command</th></tr>
<tr><td>Windows</td><td>Verify that the service is running</td><td><code>gsv -displayname *trend*</code></td></tr>
<tr><td>Linux</td><td>Verify that the service is running</td><td><code>ps_axu | grep ds_agent</code></td></tr>
</table>
<table>
<tr><th></th><th>Description</th><th>Command</th></tr>
<tr><td>Windows</td><td>Verify the URL endpoint epsec.armor.com</td><td><code>& "C:\Program Files\Trend Micro\Deep Security Agent\dsa_query.cmd" -c GetAgentStatus | sls -pattern url</code></td></tr>
<tr><td></td><td>Confirm connection to the URL</td><td><code>new-object System.Net.Sockets.TcpClient('146.88.106.210', 443)</code></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Linux</td><td>Verify the URL endpoint epsec.armor.com</td><td><code>/opt/ds_agent/dsa_query -c GetAgentStatus | grep AgentStatus.dsmUrl</code></td></tr>
<tr><td></td><td>Confirm connection to the URL</td><td><code>telnet 146.88.106.210 443</code></td></tr>
</table>
<table>
<tr><td>Windows</td><td><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></td></tr>
<tr><td>Linux</td><td><pre>/opt/ds_agent/dsa_control -m</pre></td></tr>
</table>
Click the following link to open a support ticket in AMP: https://amp.armor.com/support/tickets/new
</td>
</tr>
</table>

Vulnerability Scanning

Armor Service	Issue	Remediation

<table>
<tr>
<td>Vulnerability Scanning</td>
<td>If IR Agent is not installed</td>
<td>
<table>
<tr><td>Windows</td><td>• IR Agent files are located within C:\Program Files\Rapid7
• The IR Agent service name is "Rapid7 Insight Agent"</td></tr>
<tr><td>Linux</td><td>• 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*</td></tr>
</table>
<table>
<tr><th>Port</th><th>Destination</th></tr>
<tr><td>443/tcp (IR Agent)</td><td>• endpoint.ingress.rapid7.com *
  ◦ (United States)
• eu.endpoint.ingress.rapid7.com *
  ◦ (Europe, Middle East, Africa)</td></tr>
</table>
⚠ * 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.

Click the following link to open a support ticket in AMP: https://amp.armor.com/support/tickets/new
</td>
</tr>
<tr>
<td>Vulnerability Scanning</td>
<td>The Vulnerability Scanning agent did not run during the most recent scan.</td>
<td>
<table>
<tr><td>Windows</td><td>• IR Agent files are located within C:\Program Files\Rapid7
• The IR Agent service name is "Rapid7 Insight Agent"</td></tr>
<tr><td>Linux</td><td>• 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*</td></tr>
</table>
<table>
<tr><th>Port</th><th>Destination</th></tr>
<tr><td>443/tcp (IR Agent)</td><td>• endpoint.ingress.rapid7.com *
  ◦ (United States)
• eu.endpoint.ingress.rapid7.com *
  ◦ (Europe, Middle East, Africa)</td></tr>
</table>
⚠ * 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.

Click the following link to open a support ticket in AMP: https://amp.armor.com/support/tickets/new
</td>
</tr>
</table>