Troubleshoot Protection Scores.mobile.phone

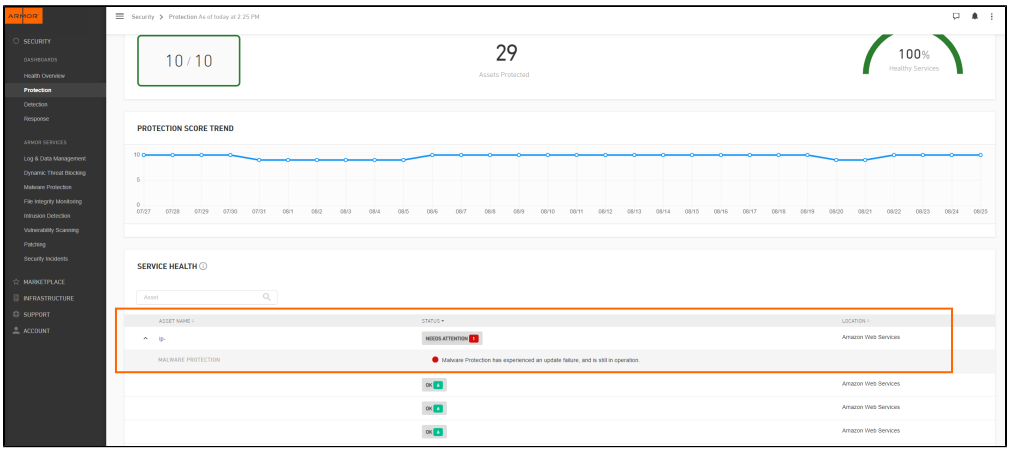
Armor Knowledge Base

Troubleshoot Protection Scores

Topics Covered

You can use this document to troubleshoot issues with your protection score within the Armor Management Portal (AMP).

Specifically, you can use this document to troubleshoot an environment that is in a **Needs Attention** state.



Pre-Troubleshooting Steps

Before you troubleshoot a specific error message, Armor recommends that you confirm the following characteristics for your Trend agent:

- Is installed
- Is running properly
- Can connect to the required IP addresses / ports

Verify that the Trend Agent is Installed

	Instructions

Windows

1. As an administrator, open Powershell.
2. In the Armor Agent command line, run the following command to verify that the subagents are installed:

```
Get-Service -displayname "trend*"
```

```
C:\.armor\opt\armor show subagents
```

1. For Malware Protection, if **Is Installed?** is **False**, then run the following command to install the service:

```
C:\.armor\opt\armor add malwareprotection
```


For Windows, a reboot will be required to complete the first installation.

Linux

1. Obtain root access with (sudo -i).
2. Run the following command:

```
/opt/armor/armor show subagents
```

```
$ /opt/armor/armor show subagents
+------------------------+----------------+---------------+
|        SUBAGENT        |    VERSION     | IS INSTALLED? |
+------------------------+----------------+---------------+
| Malware Protection     | 11.3.0-376.el7 | true          |
| Monitoring             | 2018.19.1-0.1  | true          |
| Logging                | 6.6.2          | true          |
| WinLogging             |                | false         |
| Remote Support         | 15.3.2         | true          |
| Vulnerability Scanning | 1565188176     | true          |
+------------------------+----------------+---------------+
```

3. For Malware Protection, if **Is Installed?** is **False**, then run the following command to install the service:

```
/opt/armor/armor add malwareprotection
```


If the installation is unsuccessful, then contact Armor Support.

Run the following command, and then copy the output into the support ticket to share with Armor Support. Be sure to provide any other output provided in the terminal.

```
echo "-----------------Start-of-Armor-Troubleshooting-Script-Output------------------" ;
uptime ; sudo /opt/armor/armor show db | grep -i -e "coreinstanceid" -e "accountid" ; sudo
/opt/ds_agent/dsa_query -c GetAgentStatus | grep -i -e "AgentStatus.
pluginDownloadInProgress:" -e "AgentStatus.agentState:" -e "AgentStatus.dsmUrl:" ; sudo
/opt/ds_agent/dsa_query -c GetComponentInfo | grep -i -e "Component.AM.driverOffline" -e
"Component.AM.mode" -e "Component.CORE.version" -e "Component.AM.version.pattern.VSAPI" -e
"Component.AM.cap.realtime" -e "Component.FWDPI.mode" -e "Component.IM.mode" ; systemctl -
l status ds_agent ; echo "------------------End-of-Armor-Troubleshooting-Script-
Output------------------"
```

Verify that the Trend agent is running properly

	Instructions

Windows

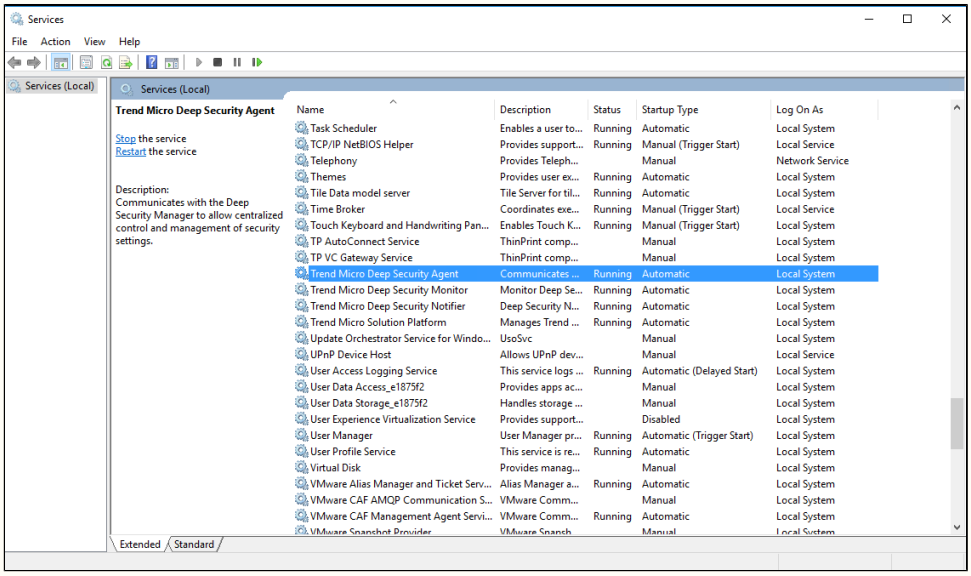
1. As an administrator, open Powershell.
2. Run the following command to verify that Trend is running:

```
Get-Service -displayname "trend*"
```

```
> Get-Service -displayname "trend*"

Status   Name               DisplayName
------   ----               -----------
Running  Amsp               Trend Micro Solution Platform
Running  ds_agent           Trend Micro Deep Security Agent
Running  ds_monitor         Trend Micro Deep Security Monitor
Running  ds_notifier        Trend Micro Deep Security Notifier
```

You can also review the **Services** window for verification.



Linux

1. Using "ps", run the following command to verify that the **ds_agent** is running:

```
ps aux | grep ds_agent | grep -v grep
```

2. The output should list several processes.

```
$ ps aux | grep ds_agent | grep -v grep
root     11565  0.0  0.0 206360   636 ?        S    Aug16   0:00 /opt/ds_agent/ds_agent -w /var
/opt/ds_agent -b -i -e /opt/ds_agent/ext
root     12484  0.1 37.5 835836 381016 ?       Sl   Aug16  11:15 /opt/ds_agent/ds_agent -w /var
/opt/ds_agent -b -i -e /opt/ds_agent/ext
root     12626  0.0  0.0 147196   248 ?        S    Aug16   0:00 /opt/ds_agent/ds_am -g ../diag
-v 5 -d /var/opt/ds_agent/am -P 1 -R
root     12641  0.0 20.7 1312456 210840 ?      Sl   Aug16   3:14 /opt/ds_agent/ds_am -g ../diag
-v 5 -d /var/opt/ds_agent/am -P 1 -R
```

3. If you do not receive any results, verify the service using **systemctl**:

```
systemctl status ds_agent
```

4. If the agent is running, then you will see that **Active** indicates that the process is **active (running)** in the logs:

```
$ sudo systemctl status ds_agent
? ds_agent.service - LSB: Trend Micro Deep Security Agent
   Loaded: loaded (/etc/rc.d/init.d/ds_agent; bad; vendor preset: disabled)
  Drop-In: /etc/systemd/system/ds_agent.service.d
           ??allow_exit.conf
   Active: active (running) since Thu 2019-08-22 19:22:16 UTC; 1h 50min ago
     Docs: man:systemd-sysv-generator(8)
  Process: 16594 ExecStart=/etc/rc.d/init.d/ds_agent start (code=exited, status=0/SUCCESS)
 Main PID: 16612 (ds_agent)
   CGroup: /system.slice/ds_agent.service
           ??16612 /opt/ds_agent/ds_agent -w /var/opt/ds_agent -b -i -e /opt/ds_agent/ext
           ??16616 /opt/ds_agent/ds_agent -w /var/opt/ds_agent -b -i -e /opt/ds_agent/ext

Aug 22 19:22:16 100-064-164-045 systemd[1]: Starting LSB: Trend Micro Deep Security Agent...
Aug 22 19:22:16 100-064-164-045 ds_agent[16594]: Starting ds_agent: [  OK  ]
Aug 22 19:22:16 100-064-164-045 systemd[1]: Started LSB: Trend Micro Deep Security Agent.
```

5. If the ds_agent was stopped on purpose, then you will see the string **"Stopping ds_agent: [OK]"** in the logs:

```
$ systemctl status ds_agent
    ? ds_agent.service - LSB: Trend Micro Deep Security Agent
       Loaded: loaded (/etc/rc.d/init.d/ds_agent; bad; vendor preset: disabled)
      Drop-In: /etc/systemd/system/ds_agent.service.d
               ??allow_exit.conf
       Active: inactive (dead) since Fri 2019-08-23 13:55:51 EDT; 5s ago
         Docs: man:systemd-sysv-generator(8)
      Process: 22612 ExecStop=/etc/rc.d/init.d/ds_agent stop (code=exited, status=0/SUCCESS)
     Main PID: 11565 (code=killed, signal=KILL)

    Aug 16 15:41:52 ip-172-31-34-176.us-east-2.compute.internal systemd[1]: Starting LSB:
Trend Micro Deep Security Agent...
    Aug 16 15:41:52 ip-172-31-34-176.us-east-2.compute.internal ds_agent[11547]: Starting
ds_agent: [  OK  ]
    Aug 16 15:41:52 ip-172-31-34-176.us-east-2.compute.internal systemd[1]: Started LSB:
Trend Micro Deep Security Agent.
    Aug 23 13:55:43 ip-172-31-34-176.us-east-2.compute.internal systemd[1]: Stopping LSB:
Trend Micro Deep Security Agent...
    Aug 23 13:55:46 ip-172-31-34-176.us-east-2.compute.internal ds_agent[22612]: Stopping
ds_agent: [  OK  ]
    Aug 23 13:55:51 ip-172-31-34-176.us-east-2.compute.internal ds_agent[22612]: Unloading
dsa_filter module...
    Aug 23 13:55:51 ip-172-31-34-176.us-east-2.compute.internal ds_agent[22612]: Unloading
dsa_filter_hook module...
    Aug 23 13:55:51 ip-172-31-34-176.us-east-2.compute.internal systemd[1]: Stopped LSB:
Trend Micro Deep Security Agent.
```

6. If the ds_agent was stopped due to the process crashing, or due to OOMM (Out Of Memory Manager) killing the process, then you will see the string "**Stopping ds_agent: [FAILED]"** in the logs:

```
$ systemctl status ds_agent
    ? ds_agent.service - LSB: Trend Micro Deep Security Agent
       Loaded: loaded (/etc/rc.d/init.d/ds_agent; bad; vendor preset: disabled)
      Drop-In: /etc/systemd/system/ds_agent.service.d
               ??allow_exit.conf
       Active: inactive (dead) since Fri 2019-08-23 15:24:54 EDT; 10s ago
         Docs: man:systemd-sysv-generator(8)
      Process: 29281 ExecStop=/etc/rc.d/init.d/ds_agent stop (code=exited, status=0/SUCCESS)
      Process: 28756 ExecStart=/etc/rc.d/init.d/ds_agent start (code=exited, status=0
/SUCCESS)
     Main PID: 28777 (code=exited, status=0/SUCCESS)

    Aug 23 15:23:12 ip-172-31-34-176.us-east-2.compute.internal systemd[1]: Starting LSB:
Trend Micro Deep Security Agent...
    Aug 23 15:23:12 ip-172-31-34-176.us-east-2.compute.internal ds_agent[28756]: Starting
ds_agent: [  OK  ]
    Aug 23 15:23:12 ip-172-31-34-176.us-east-2.compute.internal systemd[1]: Started LSB:
Trend Micro Deep Security Agent.
    Aug 23 15:24:54 ip-172-31-34-176.us-east-2.compute.internal ds_agent[29281]: Stopping
ds_agent: [FAILED]
    Aug 23 15:24:54 ip-172-31-34-176.us-east-2.compute.internal ds_agent[29281]: Unloading
dsa_filter module...
    Aug 23 15:24:54 ip-172-31-34-176.us-east-2.compute.internal ds_agent[29281]: Unloading
dsa_filter_hook module...
```

7. If the service is not running, then run the following command to start the service:

```
sudo systemctl start ds_agent
```


If the service fails to start, then contact Armor Support.

Run the following command, and then copy the output into the support ticket to share with Armor Support.

```
echo "-----------------Start-of-Armor-Troubleshooting-Script-Output------------------" ;
uptime ; sudo /opt/armor/armor show db | grep -i -e "coreinstanceid" -e "accountid" ; sudo
/opt/ds_agent/dsa_query -c GetAgentStatus | grep -i -e "AgentStatus.
pluginDownloadInProgress:" -e "AgentStatus.agentState:" -e "AgentStatus.dsmUrl:" ; sudo
/opt/ds_agent/dsa_query -c GetComponentInfo | grep -i -e "Component.AM.driverOffline" -e
"Component.AM.mode" -e "Component.CORE.version" -e "Component.AM.version.pattern.VSAPI" -e
"Component.AM.cap.realtime" -e "Component.FWDPI.mode" -e "Component.IM.mode" ; systemctl -
l status ds_agent ; echo "------------------End-of-Armor-Troubleshooting-Script-
Output-------------------"
```

Verify that the Trend agent can connect to the required IP addresses / ports

	Instructions

Windows

1. As an administrator, open Powershell.
2. Run the following command to verify that the Trend agent is able to connect to the required outbound IP addresses / ports:

```
tnc -computername 3a.epsec.armor.com -port 4119; tnc -computername 3a.epsec.armor.com -port
4120; tnc -computername 3a.epsec.armor.com -port 4122
```

```
> tnc -computername 3a.epsec.armor.com -port 4119; tnc -computername 3a.epsec.armor.com -
port 4120; tnc -computername 3a.epsec.armor.com -port 4122


ComputerName     : 3a.epsec.armor.com
RemoteAddress    : 52.13.172.208
RemotePort       : 4119
InterfaceAlias   : Ethernet0
SourceAddress    : 100.64.164.44
TcpTestSucceeded : True

ComputerName     : 3a.epsec.armor.com
RemoteAddress    : 52.13.172.208
RemotePort       : 4120
InterfaceAlias   : Ethernet0
SourceAddress    : 100.64.164.44
TcpTestSucceeded : True

ComputerName     : 3a.epsec.armor.com
RemoteAddress    : 52.13.172.208
RemotePort       : 4122
InterfaceAlias   : Ethernet0
SourceAddress    : 100.64.164.44
TcpTestSucceeded : True
```

3. Review the output to ensure that there is a connection.

> ⚠ For any failure connection, you must allow outbound connections to the following ports:
>
> - TCP Port 4119 is required for installation of the malware protection agent.
> - TCP Port 4120 is required for communication (hearbeats) to the Armor Trend Infrastructure.
> - TCP Port 4122 is required for communication to Relays and for updates.

Linux

There are two options available for this test:

Option 1: From a Script File

1. Navigate to a directory where your user can execute permissions, such as the user's home directory:
   - cd ~
2. In this directory, create a new bash script file:
   - touch connectiontest.sh
3. In the text editor of your choice, edit this file to include the entire connection test script:
   - nano connectiontest.sh
   - vim connectiontest.sh
   - emacs connectiontest.sh
4. Save the file using the method dictated by your text editor of choice.
5. Add the executable bit to the file:
   - chmod +x connectiontest.sh
6. Execute the following script:
   - ./connectiontest.sh

Option 2: Directly from BASH

1. Type an open parenthesis:
   - **(**
2. Hit the **Enter** key.
3. Paste the entire connection test script.
4. Hit the **Enter** key.
5. Type a close parenthesis:
   - **)**
6. Hit the **Enter** key to run script.

```
#!/bin/bash

hosts1=(api.armor.com)
ports1=(443)

for host in "${hosts1[@]}"
do
  for port in "${ports1[@]}"
  do
    if echo "Connection test from AA User at $(uname -n)" 2>/dev/null > /dev/tcp/"$host"/"$port"
    then
      echo -e "\e[32mSuccessfully connected to "$host":"$port""
    else
      echo -e "\e[31mFailed to connect to "$host":"$port""
    fi
  done
done

hosts2=(3a.epsec.armor.com)
ports2=(4119 4120 4122)

for host in "${hosts2[@]}"
do
  for port in "${ports2[@]}"
  do
    if echo "Connection test from AA User at $(uname -n)" 2>/dev/null > /dev/tcp/"$host"/"$port"
    then
      echo -e "\e[32mSuccessfully connected to "$host":"$port""
    else
      echo -e "\e[31mFailed to connect to "$host":"$port""
    fi
  done
done

hosts3=(1a.log.armor.com 2a.log.armor.com)
ports3=(515)

for host in "${hosts3[@]}"
do
  for port in "${ports3[@]}"
  do
    if echo "Connection test from AA User at $(uname -n)" 2>/dev/null > /dev/tcp/"$host"/"$port"
    then
      echo -e "\e[32mSuccessfully connected to "$host":"$port""
    else
      echo -e "\e[31mFailed to connect to "$host":"$port""
    fi
  done
done

hosts4=(1a.mon.armor.com 2a.mon.armor.com)
ports4=(8443)

for host in "${hosts4[@]}"
do
  for port in "${ports4[@]}"
  do
    if echo "Connection test from AA User at $(uname -n)" 2>/dev/null > /dev/tcp/"$host"/"$port"
    then
      echo -e "\e[32mSuccessfully connected to "$host":"$port""
    else
      echo -e "\e[31mFailed to connect to "$host":"$port""
    fi
  done
done

hosts5=(1a.rs.armor.com)
ports5=(443)

for host in "${hosts5[@]}"
do
```

```
  for port in "${ports5[@]}"
  do
    if echo "Connection test from AA User at $(uname -n)" 2>/dev/null > /dev/tcp/"$host"/"$port"
    then
      echo -e "\e[32mSuccessfully connected to "$host":"$port""
    else
      echo -e "\e[31mFailed to connect to "$host":"$port""
    fi
  done
done

hosts6=(endpoint.ingress.rapid7.com ca.endpoint.ingress.rapid7.com eu.endpoint.ingress.rapid7.
com au.endpoint.ingress.rapid7.com ap.endpoint.ingress.rapid7.com)
ports6=(443)

for host in "${hosts6[@]}"
do
  for port in "${ports6[@]}"
  do
    if echo "Connection test from AA User at $(uname -n)" 2>/dev/null > /dev/tcp/"$host"/"$port"
    then
      echo -e "\e[32mSuccessfully connected to "$host":"$port""
    else
      echo -e "\e[31mFailed to connect to "$host":"$port""
    fi
  done
done

hosts7=(s3.amazonaws.com s3.ca-central-1.amazonaws.com s3.eu-central-1.amazonaws.com s3.ap-
northeast-1.amazonaws.com s3-ap-southeast-2.amazonaws.com)
ports7=(443)

for host in "${hosts7[@]}"
do
  for port in "${ports7[@]}"
  do
    if echo "Connection test from AA User at $(uname -n)" 2>/dev/null > /dev/tcp/"$host"/"$port"
    then
      echo -e "\e[32mSuccessfully connected to "$host":"$port""
    else
      echo -e "\e[31mFailed to connect to "$host":"$port""
    fi
  done
done
echo -e "\e[0mTest completed."
```

Running this test from a server that has the Armor Agent installed and registered on it will yield a different result than a machine that does not have the Armor Agent installed and/or registered:

```
Successfully connected to api.armor.com:443
Successfully connected to 3a.epsec.armor.com:4119
Successfully connected to 3a.epsec.armor.com:4120
Successfully connected to 3a.epsec.armor.com:4122
Successfully connected to 1a.log.armor.com:515
Failed to connect to 2a.log.armor.com:515
Successfully connected to 1a.mon.armor.com:8443
Failed to connect to 2a.mon.armor.com:8443
Successfully connected to 1a.rs.armor.com:443
Successfully connected to endpoint.ingress.rapid7.com:443
Successfully connected to ca.endpoint.ingress.rapid7.com:443
Successfully connected to eu.endpoint.ingress.rapid7.com:443
Successfully connected to au.endpoint.ingress.rapid7.com:443
Successfully connected to ap.endpoint.ingress.rapid7.com:443
Successfully connected to s3.amazonaws.com:443
Successfully connected to s3.ca-central-1.amazonaws.com:443
Successfully connected to s3.eu-central-1.amazonaws.com:443
Successfully connected to s3.ap-northeast-1.amazonaws.com:443
Successfully connected to s3-ap-southeast-2.amazonaws.com:443
```

```
Successfully connected to api.armor.com:443
Successfully connected to 3a.epsec.armor.com:4119
Successfully connected to 3a.epsec.armor.com:4120
Successfully connected to 3a.epsec.armor.com:4122
Failed to connect to 1a.log.armor.com:515
Failed to connect to 2a.log.armor.com:515
Failed to connect to 1a.mon.armor.com:8443
Failed to connect to 2a.mon.armor.com:8443
Failed to connect to 1a.rs.armor.com:443
Successfully connected to endpoint.ingress.rapid7.com:443
Successfully connected to ca.endpoint.ingress.rapid7.com:443
Successfully connected to eu.endpoint.ingress.rapid7.com:443
Successfully connected to au.endpoint.ingress.rapid7.com:443
Successfully connected to ap.endpoint.ingress.rapid7.com:443
Successfully connected to s3.amazonaws.com:443
Successfully connected to s3.ca-central-1.amazonaws.com:443
Successfully connected to s3.eu-central-1.amazonaws.com:443
Successfully connected to s3.ap-northeast-1.amazonaws.com:443
Successfully connected to s3-ap-southeast-2.amazonaws.com:443
```

If your output does not match the **Expected Output from Registered Server** output, please verify your firewall rules allow the host/port combinations required for Armor Anywhere to function, as listed in ANYWHERE Pre-Installation.

Troubleshooting

Installation or Configuration

You can use this section to troubleshoot the following errors:

- Malware Protection is not installed or configured
- FIM is not installed
- FIM is installed but has not been configured
- IDS is not installed or enabled

⚠ Armor Complete users will never see IDS errors because IDS is only installed with Armor Anywhere.

	Instructions

Windows

1. As an administrator, open PowerShell.
2. Run the following command:

```
& $Env:ProgramFiles"\Trend Micro\Deep Security Agent\dsa_query" -c GetComponentInfo
```

When this error is encountered, the output will be limited.

```
> & $Env:ProgramFiles"\Trend Micro\Deep Security Agent\dsa_query" -c GetComponentInfo

Component.AM.mode: not-capable
Component.FWDPI.driverState: 3
Component.LI.mode: off
```

3. If the above command failed, verify that Anti-Malware has been installed.
4. If you do not see the **C:\Program files\Trend Micro** folder, then remove and re-install Malware protection, and then reboot after 10 minutes.

```
C:\.armor\opt\armor remove antimalware
C:\.armor\opt\armor add antimalware
```

5. As an administrator, open PowerShell, run the following command to confirm that the service is running successfully:

```
get-service -displayname "trend*"
```

6. If the service is in a bad state, then your output will match the following example, with only 3 services listed. This output indicates that the AMSP service is not installed, and that the agent is currently running in a limited capacity. In this case, you may have not received a policy or your agent has not been activated.

```
> get-service -displayname "trend*"

Status      Name             DisplayName
------       ----                -----------
Running   ds_agent       Trend Micro Deep Security Agent
Running   ds_monitor    Trend Micro Deep Security Monitor
Running   ds_notifier     Trend Micro Deep Security Notifier
```

7. If your agent did not activate, then run the following command:

```
C:\.armor\opt\armor add malwareprotection
```

8. After 5 minutes, reboot the service.
9. After the reboot, verify that your services are running, which should return the following output:

```
> get-service -displayname "trend*"

Status      Name             DisplayName
------       ----                -----------
Running   Amsp            Trend Micro Solution Platform
Running   ds_agent       Trend Micro Deep Security Agent
Running   ds_monitor    Trend Micro Deep Security Monitor
Running   ds_notifier     Trend Micro Deep Security Notifier
```

10. If you do not see the AMSP service, then contact Armor Support. Within the ticket, be sure to provide all of the information / results that you have gathered so far.

Linux

1. Run the following command to determine if a component of the anti-malware agent did not install correctly:

```
sudo /opt/ds_agent/dsa_query -c GetComponentInfo
```

2. If the components were installed correctly, then you will see an output similar to the following:

```
$ sudo /opt/ds_agent/dsa_query -c GetComponentInfo
Component.AM.cap.Qrestore: true
Component.AM.cap.realtime: true
Component.AM.cap.spyware: false
Component.AM.configurations: 2
Component.AM.driverOffline: false
Component.AM.licenseExpiry: 1882211783
Component.AM.mode: on
Component.AM.moduleStatus: 0
Component.AM.scan.Manual: 6
Component.AM.scan.Quick: 6
Component.AM.scan.Realtime: 5
Component.AM.scanStatus: 4
Component.AM.scanType: 0
Component.AM.version.pattern.VSAPI: 15.313.00
Component.CORE.version: 11.3
Component.FWDPI.dpiRules: 151
Component.FWDPI.driverState: 3
Component.FWDPI.firewallMode: on-tap
Component.FWDPI.mode: on-tap
Component.IM.highestEntityId: 37184
Component.IM.imScanType: 0
Component.IM.mode: on
Component.IM.pendingScanBitmask: 0
Component.IM.percentComplete: 0
Component.IM.rules: 25
Component.IM.scanStatus: 4
Component.IM.scanType: 1
Component.LI.mode: off
Component.WRS.mode: off
```

3. Verify that the command line **Component.AM.mode**: is **on**, and not **not-capable**.
4. If the previously run command returns the following output, you will need to reinstall the **malwareprotection** sub-agent.

```
$ sudo /opt/ds_agent/dsa_query -c GetComponentInfo
Component.AM.mode: not-capable
Component.FWDPI.driverState: 3
Component.LI.mode: off
```

5. Run the following commands to re-install the **malwareprotection** subagent:

```
sudo /opt/armor/armor remove malwareprotection
sudo /opt/armor/armor add malwareprotection
```

6. After the re-installation process is complete, you must wait between 30 minutes to an hour to download and update the agent's components. You can then run the following command to confirm the desired results:

```
sudo /opt/ds_agent/dsa_query -c GetComponentInfo
```

7. If you still see an error, then contact Armor Support. Within the ticket, paste the output from the following command:

Information Gathering Script for Escalations

```
echo "-----------------Start-of-Armor-Troubleshooting-Script-Output------------------" ;
uptime ; sudo /opt/armor/armor show db | grep -i -e "coreinstanceid" -e "accountid" ; sudo /opt
/ds_agent/dsa_query -c GetAgentStatus | grep -i -e "AgentStatus.pluginDownloadInProgress:" -e
"AgentStatus.agentState:" -e "AgentStatus.dsmUrl:" ; sudo /opt/ds_agent/dsa_query -c
GetComponentInfo | grep -i -e "Component.AM.driverOffline" -e "Component.AM.mode" -e "Component.
CORE.version" -e "Component.AM.version.pattern.VSAPI" -e "Component.AM.cap.realtime" -e
"Component.FWDPI.mode" -e "Component.IM.mode" ; systemctl -l status ds_agent ; echo
"------------------End-of-Armor-Troubleshooting-Script-Output------------------"
```

Heartbeat / Communication

You can use this section to troubleshoot the following errors:

- Malware Protection has not provided a heartbeat in the past 4 hours.
- FIM has not provided a heartbeat in the past 4 hours.
- IDS has not provided a heartbeat in the past 4 hours.

⚠ Armor Complete users will never see IDS errors because IDS is only installed with Armor Anywhere.

	Instructions
Windows	This issue often occurs if a server has been powered off or the network has changed.

1. Run the following command to ensure that the AMSP service is running:

```
get-service -displayname "trend*"
```

2. If the service is running, you will see the following output:

```
> get-service -displayname "trend*"

Status   Name               DisplayName
------   ----               -----------
Running  Amsp               Trend Micro Solution Platform
Running  ds_agent           Trend Micro Deep Security Agent
Running  ds_monitor         Trend Micro Deep Security Monitor
Running  ds_notifier        Trend Micro Deep Security Notifier
```

3. If the service is not running (stopped), then use the following command to start the Malware Protection agent and all other Malware Protection-related services:

```
get-service -displayname "trend*" | start-service
```

```
> get-service -displayname "trend*"

Status   Name               DisplayName
------   ----               -----------
Stopped  Amsp               Trend Micro Solution Platform
Stopped  ds_agent           Trend Micro Deep Security Agent
Stopped  ds_monitor         Trend Micro Deep Security Monitor
Stopped  ds_notifier        Trend Micro Deep Security Notifier


> get-service -displayname "trend*" | start-service
> get-service -displayname "trend*"

Status   Name               DisplayName
------   ----               -----------
Running  Amsp               Trend Micro Solution Platform
Running  ds_agent           Trend Micro Deep Security Agent
Running  ds_monitor         Trend Micro Deep Security Monitor
Running  ds_notifier        Trend Micro Deep Security Notifier
```

4. Run the following command to initiate a heartbeat to the Armor Malware Protection Infrastructure manually:

```
& $Env:ProgramFiles"\Trend Micro\Deep Security Agent\dsa_control" -m
```

5. Review the desired output. This will indicate that your virtual machine is able to connect to the Armor Malware Protection Infrastructure, and the agent will reach out to the Armor Malware Protection Infrastructure to update the status, as well as obtain policy updates and more:

```
> & $Env:ProgramFiles"\Trend Micro\Deep Security Agent\dsa_control" -m
HTTP Status: 200 - OK
Response:
Manager contact has been scheduled to occur in the next few seconds.
```

- In AMP, the **not provided a heartbeat in the past 4 hours** error message will be removed within an hour.

6. If this error message continues to display in AMP, run the following command as an administrator in PowerShell:

```
tnc -computername 3a.epsec.armor.com -port 4119; tnc -computername 3a.epsec.armor.com -port
4120; tnc -computername 3a.epsec.armor.com -port 4122
```

```
> tnc -computername 3a.epsec.armor.com -port 4119; tnc -computername 3a.epsec.armor.com -
port 4120; tnc -computername 3a.epsec.armor.com -port 4122


ComputerName     : 3a.epsec.armor.com
RemoteAddress    : 52.13.172.208
RemotePort       : 4119
InterfaceAlias   : Ethernet
SourceAddress    : 172.31.10.144
TcpTestSucceeded : True

ComputerName     : 3a.epsec.armor.com
RemoteAddress    : 52.13.172.208
RemotePort       : 4120
InterfaceAlias   : Ethernet
SourceAddress    : 172.31.10.144
TcpTestSucceeded : True

ComputerName     : 3a.epsec.armor.com
RemoteAddress    : 52.13.172.208
RemotePort       : 4122
InterfaceAlias   : Ethernet
SourceAddress    : 172.31.10.144
TcpTestSucceeded : True
```

If you encounter a failure, you may have a firewall conflict that requires intervention.

Port Information:

- TCP Port 4119 is required for installation of the malware protection agent.
- TCP Port 4120 is required for Heartbeats and communication to the Armor Malware Protection Infrastructure.
- TCP Port 4122 is required for communication to Antimalware Infrastructure and updates.

7. If connectivity is successful and Armor Support has not yet been contacted, re-register the malware protection agent:

```
> C:\.armor\opt\armor add malwareprotection
```

8. If the error has not cleared, please contact Armor Support. Within the ticket, provide the information / results that you have gathered so far.

Linux

This issue often occurs if a server has been powered off, or if connectivity to the Armor Malware Protection Infrastructure has been blocked.

1. Assuming that the server is powered on, run the following command to ensure that the Malware Protection agent is running:

```
systemctl status ds_agent
```

2. Review the output to verify that there are 4 separate processes, including **/opt/ds_agent/ds_agent** and**/opt/ds_agent/ds_am**:

```
$ systemctl status ds_agent
? ds_agent.service - LSB: Trend Micro Deep Security Agent
   Loaded: loaded (/etc/rc.d/init.d/ds_agent; bad; vendor preset: disabled)
  Drop-In: /etc/systemd/system/ds_agent.service.d
           ??allow_exit.conf
   Active: active (running) since Fri 2019-08-23 16:26:19 EDT; 24h ago
     Docs: man:systemd-sysv-generator(8)
  Process: 29689 ExecStop=/etc/rc.d/init.d/ds_agent stop (code=exited, status=0/SUCCESS)
  Process: 1130 ExecStart=/etc/rc.d/init.d/ds_agent start (code=exited, status=0/SUCCESS)
 Main PID: 1151 (ds_agent)
   CGroup: /system.slice/ds_agent.service
           ??1151 /opt/ds_agent/ds_agent -w /var/opt/ds_agent -b -i -e /opt/ds_agent/ext
           ??1152 /opt/ds_agent/ds_agent -w /var/opt/ds_agent -b -i -e /opt/ds_agent/ext
           ??1272 /opt/ds_agent/ds_am -g ../diag -v 5 -d /var/opt/ds_agent/am -P 1 -R
           ??1289 /opt/ds_agent/ds_am -g ../diag -v 5 -d /var/opt/ds_agent/am -P 1 -R

Aug 23 16:26:19 ip-172-31-34-176.us-east-2.compute.internal systemd[1]: Starting LSB: Trend
Micro Deep Security Agent...
Aug 23 16:26:19 ip-172-31-34-176.us-east-2.compute.internal ds_agent[1130]: Starting
ds_agent: [  OK  ]
Aug 23 16:26:19 ip-172-31-34-176.us-east-2.compute.internal systemd[1]: Started LSB: Trend
Micro Deep Security Agent.
```

3. If you do not find that these processes are running, then you may need to restart the ds_agent, or reinstall the malwareprotection agent.
4. To restart the ds_agent service, run the following command:

```
sudo systemctl stop ds_agent; sudo systemctl start ds_agent
```

5. To reinstall the malwareprotection agent, run the following command:

```
sudo /opt/armor/armor remove malwareprotection; sudo /opt/armor/armor add malwareprotection
```

6. If the ds_agent is running with all 4 expected processes, run the following command to manually heartbeat the agent:

```
sudo /opt/ds_agent/dsa_control -m
```

7. Review the following output for a successful heartbeat:

```
$ sudo /opt/ds_agent/dsa_control -m
HTTP Status: 200 - OK
Response:
Manager contact has been scheduled to occur in the next few seconds.
```

8. If you do not see **HTTP Status: 200 - OK**, then you must test the connectivity to ensure that your firewall rules are working properly.

   There are two ways to test for connectivity:

Option 1: From a Script File

a. Navigate to a directory where your user can execute permissions, such as the user's home directory:
   - cd ~

b. In this directory, create a new bash script file:
   - touch connectiontest.sh

c. In the text editor of your choice, edit this file to include the entire connection test script:
   - nano connectiontest.sh
   - vim connectiontest.sh
   - emacs connectiontest.sh

d. Save the file using the method dictated by your text editor of choice.

e. Add the executable bit to the file:
   - chmod +x connectiontest.sh

f. Execute the following script:
   - ./connectiontest.sh

Option 2: Directly from BASH

a. Type an open parenthesis:
   - **(**

b. Hit the **Enter** key.
c. Paste the entire connection test script.
d. Hit the **Enter** key.
e. Type a close parenthesis:
   - **)**

f. Hit the **Enter** key to run script.

```
#!/bin/bash

hosts1=(api.armor.com)
ports1=(443)

for host in "${hosts1[@]}"
do
  for port in "${ports1[@]}"
  do
    if echo "Connection test from AA User at $(uname -n)" 2>/dev/null > /dev/tcp/"$host"
/"$port"
    then
      echo -e "\e[32mSuccessfully connected to "$host":"$port""
    else
      echo -e "\e[31mFailed to connect to "$host":"$port""
    fi
  done
done

hosts2=(3a.epsec.armor.com)
ports2=(4119 4120 4122)

for host in "${hosts2[@]}"
do
  for port in "${ports2[@]}"
  do
    if echo "Connection test from AA User at $(uname -n)" 2>/dev/null > /dev/tcp/"$host"
/"$port"
    then
      echo -e "\e[32mSuccessfully connected to "$host":"$port""
    else
      echo -e "\e[31mFailed to connect to "$host":"$port""
    fi
  done
done

hosts3=(1a.log.armor.com 2a.log.armor.com)
ports3=(515)

for host in "${hosts3[@]}"
do
  for port in "${ports3[@]}"
  do
    if echo "Connection test from AA User at $(uname -n)" 2>/dev/null > /dev/tcp/"$host"
/"$port"
    then
      echo -e "\e[32mSuccessfully connected to "$host":"$port""
    else
      echo -e "\e[31mFailed to connect to "$host":"$port""
    fi
  done
done

hosts4=(1a.mon.armor.com 2a.mon.armor.com)
ports4=(8443)

for host in "${hosts4[@]}"
do
  for port in "${ports4[@]}"
  do
    if echo "Connection test from AA User at $(uname -n)" 2>/dev/null > /dev/tcp/"$host"
/"$port"
    then
```

```
      echo -e "\e[32mSuccessfully connected to "$host":"$port""
    else
      echo -e "\e[31mFailed to connect to "$host":"$port""
    fi
  done
done

hosts5=(1a.rs.armor.com)
ports5=(443)

for host in "${hosts5[@]}"
do
  for port in "${ports5[@]}"
  do
    if echo "Connection test from AA User at $(uname -n)" 2>/dev/null > /dev/tcp/"$host"
/"$port"
    then
      echo -e "\e[32mSuccessfully connected to "$host":"$port""
    else
      echo -e "\e[31mFailed to connect to "$host":"$port""
    fi
  done
done

hosts6=(endpoint.ingress.rapid7.com ca.endpoint.ingress.rapid7.com eu.endpoint.ingress.
rapid7.com au.endpoint.ingress.rapid7.com ap.endpoint.ingress.rapid7.com)
ports6=(443)

for host in "${hosts6[@]}"
do
  for port in "${ports6[@]}"
  do
    if echo "Connection test from AA User at $(uname -n)" 2>/dev/null > /dev/tcp/"$host"
/"$port"
    then
      echo -e "\e[32mSuccessfully connected to "$host":"$port""
    else
      echo -e "\e[31mFailed to connect to "$host":"$port""
    fi
  done
done

hosts7=(s3.amazonaws.com s3.ca-central-1.amazonaws.com s3.eu-central-1.amazonaws.com s3.ap-
northeast-1.amazonaws.com s3-ap-southeast-2.amazonaws.com)
ports7=(443)

for host in "${hosts7[@]}"
do
  for port in "${ports7[@]}"
  do
    if echo "Connection test from AA User at $(uname -n)" 2>/dev/null > /dev/tcp/"$host"
/"$port"
    then
      echo -e "\e[32mSuccessfully connected to "$host":"$port""
    else
      echo -e "\e[31mFailed to connect to "$host":"$port""
    fi
  done
done
echo -e "\e[0mTest completed."
```

⚠ Running this test from a server that has the Armor Agent installed and registered on it will yield a different result than a machine that does not have the Armor Agent installed and/or registered:

```
Successfully connected to api.armor.com:443
Successfully connected to 3a.epsec.armor.com:4119
Successfully connected to 3a.epsec.armor.com:4120
Successfully connected to 3a.epsec.armor.com:4122
Successfully connected to 1a.log.armor.com:515
Failed to connect to 2a.log.armor.com:515
Successfully connected to 1a.mon.armor.com:8443
Failed to connect to 2a.mon.armor.com:8443
Successfully connected to 1a.rs.armor.com:443
Successfully connected to endpoint.ingress.rapid7.com:443
Successfully connected to ca.endpoint.ingress.rapid7.com:443
Successfully connected to eu.endpoint.ingress.rapid7.com:443
Successfully connected to au.endpoint.ingress.rapid7.com:443
Successfully connected to ap.endpoint.ingress.rapid7.com:443
Successfully connected to s3.amazonaws.com:443
Successfully connected to s3.ca-central-1.amazonaws.com:443
Successfully connected to s3.eu-central-1.amazonaws.com:443
Successfully connected to s3.ap-northeast-1.amazonaws.com:443
Successfully connected to s3-ap-southeast-2.amazonaws.com:443
```

```
Successfully connected to api.armor.com:443
Successfully connected to 3a.epsec.armor.com:4119
Successfully connected to 3a.epsec.armor.com:4120
Successfully connected to 3a.epsec.armor.com:4122
Failed to connect to 1a.log.armor.com:515
Failed to connect to 2a.log.armor.com:515
Failed to connect to 1a.mon.armor.com:8443
Failed to connect to 2a.mon.armor.com:8443
Failed to connect to 1a.rs.armor.com:443
Successfully connected to endpoint.ingress.rapid7.com:443
Successfully connected to ca.endpoint.ingress.rapid7.com:443
Successfully connected to eu.endpoint.ingress.rapid7.com:443
Successfully connected to au.endpoint.ingress.rapid7.com:443
Successfully connected to ap.endpoint.ingress.rapid7.com:443
Successfully connected to s3.amazonaws.com:443
Successfully connected to s3.ca-central-1.amazonaws.com:443
Successfully connected to s3.eu-central-1.amazonaws.com:443
Successfully connected to s3.ap-northeast-1.amazonaws.com:443
Successfully connected to s3-ap-southeast-2.amazonaws.com:443
```

9. If you still see one of the heartbeat errors, then contact Armor Support and paste into the ticket the output from the following command:

```
echo "-----------------Start-of-Armor-Troubleshooting-Script-Output------------------" ;
uptime ; sudo /opt/armor/armor show db | grep -i -e "coreinstanceid" -e "accountid" ; sudo /opt
/ds_agent/dsa_query -c GetAgentStatus | grep -i -e "AgentStatus.pluginDownloadInProgress:" -e
"AgentStatus.agentState:" -e "AgentStatus.dsmUrl:" ; sudo /opt/ds_agent/dsa_query -c
GetComponentInfo | grep -i -e "Component.AM.driverOffline" -e "Component.AM.mode" -e "Component.
CORE.version" -e "Component.AM.version.pattern.VSAPI" -e "Component.AM.cap.realtime" -e
"Component.FWDPI.mode" -e "Component.IM.mode" ; systemctl -l status ds_agent ; echo
"------------------End-of-Armor-Troubleshooting-Script-Output------------------"
```

Failure Update

You can use this section to troubleshoot the following errors:

- Malware Protection has experienced an update failure, and is still in operation.

	Instructions

Windows	This error usually resolves itself after the agent has heartbeated a few times; however, if it hasn't, then a manual update will be required.
	1. As an administrator, open PowerShell.
	2. Run the following command:
	`& $Env:ProgramFiles"\Trend Micro\Deep Security Agent\dsa_control" -U`
	`> & $Env:ProgramFiles"\Trend Micro\Deep Security Agent\dsa_control" -U`
	`HTTP Status: 200 - OK`
	`'SecurityUpdate' process started.`
	`Response:`
	`<Message>`
	`<Response code='0' cmd='UpdateComponent'/>`
	`</Message>`
	This will specifically request an update for security definitions from the Armor Malware Protection Infrastructure, and should resolve the error in about an hour.
	3. If the above command failed, run the following commands IN ORDER to make sure the modules are set to be updated automatically:
	`& $Env:ProgramFiles"\Trend Micro\Deep Security Agent\dsa_control" -m "UpdateComponent:true"`
	`& $Env:ProgramFiles"\Trend Micro\Deep Security Agent\dsa_control" -m "UpdateConfiguration:true"`
	`& $Env:ProgramFiles"\Trend Micro\Deep Security Agent\dsa_control" -m`
	4. If the issue still persists, then contact Armor Support. Within the ticket, be sure to provide the output from the previously run commands.

Linux	This error usually resolves itself after the agent has heartbeated a few times; however, if it hasn't, then a manual update will be required.
	1. Run the following command:
	`sudo /opt/ds_agent/dsa_control -U`
	`$ sudo /opt/ds_agent/dsa_control -U`
	`HTTP Status: 200 - OK`
	`'SecurityUpdate' process started.`
	`Response:`
	`<Message>`
	`<Response code='0' cmd='UpdateComponent'/>`
	`</Message>`
	2. This will specifically request an update for security definitions from the Armor Malware Protection Infrastructure, and should resolve the error in about an hour.
	3. If the error is not resolved, run the following command to make sure the modules are set to be updated automatically:
	`sudo /opt/ds_agent/dsa_control -m "UpdateComponent:true" ; sudo /opt/ds_agent/dsa_control -m "UpdateConfiguration:true" ; sudo /opt/ds_agent/dsa_control -m`
	4. If you still see an error, then contact Armor Support. Within the ticket, paste the output from the following command:
	`echo "-----------------Start-of-Armor-Troubleshooting-Script-Output-------------------" ; uptime ; sudo /opt/armor/armor show db | grep -i -e "coreinstanceid" -e "accountid" ; sudo /opt/ds_agent/dsa_query -c GetAgentStatus | grep -i -e "AgentStatus.pluginDownloadInProgress:" -e "AgentStatus.agentState:" -e "AgentStatus.dsmUrl:" ; sudo /opt/ds_agent/dsa_query -c GetComponentInfo | grep -i -e "Component.AM.driverOffline" -e "Component.AM.mode" -e "Component.CORE.version" -e "Component.AM.version.pattern.VSAPI" -e "Component.AM.cap.realtime" -e "Component.FWDPI.mode" -e "Component.IM.mode" ; systemctl -l status ds_agent ; echo "-------------------End-of-Armor-Troubleshooting-Script-Output-------------------"`

Reboot after Installation

You can use this section to troubleshoot the following error:

- Reboot is required for Malware Protection.

	Instructions

Windows

When installed for the first time, Windows requires a reboot to finalize the changes being made to the registry. If you reboot when the installation prompts you, then you should not receive this error.

If you do receive this error, it means too much time has passed between installation & rebooting, and you'll need to contact Armor Support to manually refresh your Malware Protection Agent status via the Armor Malware Protection Infrastructure.

1. Run the following command, and include the output within the ticket:

```
Write-Host "-----------------Start-of-Armor-Troubleshooting-Script-Output------------------" ;
systeminfo | Select-String "System Boot*" ; C:\.armor\opt\armor show db | Select-String -
Pattern '(AccountId)|(CoreInstanceId)' ; & $Env:ProgramFiles"\Trend Micro\Deep Security
Agent\dsa_query" -c GetAgentStatus | Select-String -Pattern '\.
(agentState|dsmUrl|pluginDownloadInProgress)' ; & $Env:ProgramFiles"\Trend Micro\Deep Security
Agent\dsa_query" -c GetComponentInfo | Select-String -Pattern '(Component.AM.driverOffline)|
(Component.AM.mode)|(Component.CORE.version)|(Component.AM.version.pattern.VSAPI)|(Component.AM.
cap.realtime)|(Component.FWDPI.mode)|(Component.IM.mode)' ; Get-Service -displayname "trend*" |
ft ; Write-Host "------------------End-of-Armor-Troubleshooting-Script-
Output------------------"
```

```
-----------------Start-of-Armor-Troubleshooting-Script-Output------------------

System Boot Time:          8/14/2019, 5:00:10 PM
| AccountId         | 3804                                 |
| CoreInstanceId    | 38a6a50a-0553-4f47-b628-912280ae7c8a |
AgentStatus.agentState: green
AgentStatus.dsmUrl: https://3a.epsec.armor.com:4120/
AgentStatus.pluginDownloadInProgress: false
Component.AM.cap.realtime: true
Component.AM.driverOffline: false
Component.AM.mode: on
Component.AM.version.pattern.VSAPI: 15.315.00
Component.CORE.version: 11.3
Component.FWDPI.mode: on-tap
Component.IM.mode: real-time



Status   Name               DisplayName
------   ----               -----------
Running  Amsp               Trend Micro Solution Platform
Running  ds_agent           Trend Micro Deep Security Agent
Running  ds_monitor         Trend Micro Deep Security Monitor
Running  ds_notifier        Trend Micro Deep Security Notifier


------------------End-of-Armor-Troubleshooting-Script-Output------------------
```

Was this helpful?

Your Rating:

Results:

0 rates