Troubleshooting TrendMicro Workload Security Installation:

Trendmicro workload security is one of the TPICAP endpoint security products for servers. This document provides information on how to troubleshoot the application.

Trend Repositories:

EMEA: [\\ldn1ws7001.corp.ad.tullib.com\Patches$\Custom\Trend](file:///\\ldn1ws7001.corp.ad.tullib.com\Patches$\Custom\Trend)

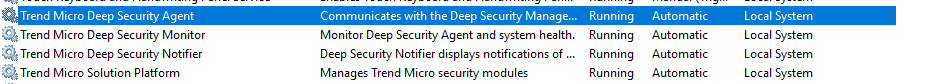
APAC: \\sng1ws7001.corp.ad.tullib.com\Patches$\Custom\Trend

AMER: [\\njc1ws3458.corp.ad.tullib.com\Patches$\Custom\Trend](file:///\\njc1ws3458.corp.ad.tullib.com\Patches$\Custom\Trend)

BRAZIL: \\BRICAPAD3.br.icap.com\Trend

Requirements:

To ensure that the application is performing correctly, please check the following:

1. Connectivity to Trendmicro cloud command and control endpoints and the server should be open. This can be tested by telnet, tcping, or test-netconnection command in Powershell.
   1. Test-NetConnection -ComputerName "app.deepsecurity.trendmicro.com" -port 443
   2. Test-NetConnection -ComputerName "agents.workload.gb-1.cloudone.trendmicro.com" -port 443
   3. Test-NetConnection -ComputerName "dsmim.deepsecurity.trendmicro.com" -port 443
2. Uninstall all other Trend Applications
   1. KB on how to uninstall Apex one trend products, [KB0019952](https://tpicap.service-now.com/kb_knowledge.do?sys_id=59da110e97582554db0b769e2153afd6&sysparm_record_target=kb_knowledge&sysparm_record_row=3&sysparm_record_rows=6&sysparm_record_list=workflow_stateINdraft%2Creview%2Cpublished%2Cpending_retirement%2Cretired%5Eauthor%3Djavascript%3Ags.getUserID%28%29%5EORDERBYDESCnumber)
   2. Run TrendCloudDeployment.ps1 located in the repository or run Agent-Core-Windows.msi to install Trend Workload Security
3. These four services should be established and running:
   1. 
4. Check if the server's IP is seen in this list. [Trend Dump](https://tpicap365-my.sharepoint.com/:x:/g/personal/yazeid_hamarsha_tpicap_com/EUPhq0V38h9DvHg0nF64aVYB1gIUXBSynX_qSM5a_TbHpw?e=2QPLLP&nav=MTVfe0ZGQUIwQzhCLUExNjItNDIwOC05MzNBLUI5MEQzQUJBQTJGM30)

Troubleshooting Trendmico Workload Security.

1. Confirm connectivity exists. Check the windows firewall, dns resolution, or use the proxy servers to register the agent. If the server has issues connecting to the Trend command and control endpoint, please open a ticket to the network team.
2. Ensure that all three services are installed and running.
3. If the application is corrupt, please run the Powershell script in the repository to upgrade automatically. Trendrepository\TrendCloudDeployment.ps1 copy and run this script manually to perform the upgrade. You can copy and run the application manually by copying and running the Agent-Core-Windows.msi package
4. If the application is installed, the ports are open, and the services are running, we need to do the following commands:
   1. "C:\Program Files\Trend Micro\Deep Security Agent\dsa\_control.cmd" -r
      1. You should see an HTTP OK output. If not, use the password via
      2. "C:\Program Files\Trend Micro\Deep Security Agent\dsa\_control.cmd" -r -p WWIQ7G!fHX$19LQZBZD
   2. Register the client via the following commands:
      1. "C:\Program Files\Trend Micro\Deep Security Agent\dsa\_control.cmd" -a "dsm://agents.workload.gb-1.cloudone.trendmicro.com:443/" "tenantID:BE123086-1CAA-5C3A-2027-3BCB78B797A6" "token:9BA0BFE0-65DE-2658-82BB-2AD32ED43100" "policyid:562"
   3. Escalate on the chat if you get errors or upon successful registration. Infosec needs to modify it to the correct policy group.
5. You can use the following proxy servers to route the dsa\_agent traffic and reach the console:
   1. "C:\Program Files\Trend Micro\Deep Security Agent\dsa\_control.cmd" -x dsm\_proxy://10.136.3.46:8080
   2. "C:\Program Files\Trend Micro\Deep Security Agent\dsa\_control.cmd" -y relay\_proxy://10.136.3.46:8080

Note: **do this AFTER the -r commands. -r command reset the client**.

* 1. The following proxy servers can be used if the trend cloud endpoints are closed:  
     AMER: 10.136.3.46

EMEA: 10.72.3.46

APAC: 10.200.3.46

1. For machines that are no longer reachable, please provide evidence in the ticket the device is decommissioned either via email from the owner or confirmation from D42.

A successful computer registration with the console will have the following outputs:

