McAfee Advance Threat Defense 3.x Troubleshooting Tree

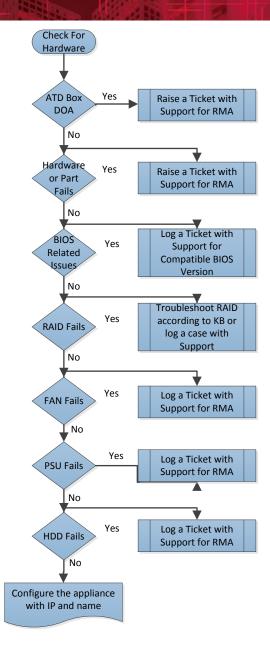Updated on April 20.2015

McAfee
An Intel Company

Quick Launch

Click on topics below to start using the tree

ATD General Hardware Issues

ATD General Software Issues

Installation/Upgradation Issues

General Issues

General Configuration Issues

Detection Failures/False Positives

Logging/Reporting

Cluster Issues

Best Practices

Integration Issues

General Error Codes

Known Issues

End of Life ATD Builds

How to..

FAQs

Download McAfee Documentation   **Log A Support Case**   **Feedback**

McAfee
An Intel Company

ATD General Hardware Issues

Check For Hardware

↓

ATD Box DOA —Yes→ Raise a Ticket with Support for RMA

No ↓

Hardware or Part Fails —Yes→ Raise a Ticket with Support for RMA

No ↓

BIOS Related Issues —Yes→ Log a Ticket with Support for Compatible BIOS Version

No ↓

RAID Fails —Yes→ Troubleshoot RAID according to KB or log a case with Support

No ↓

FAN Fails —Yes→ Log a Ticket with Support for RMA

No ↓

PSU Fails —Yes→ Log a Ticket with Support for RMA

No ↓

HDD Fails —Yes→ Log a Ticket with Support for RMA

No ↓

Configure the appliance with IP and name

ATD General Software Issues

- Loading ATD 3.0 Analysis Status and Analysis Results Page takes an excessive amount of time

- Troubleshooting boot failures with the ATD appliance

- Search field under Analysis Status and Analysis Results tab is removed when the page is refreshed

- Engine/DAT updation Fails after adding MWG as proxy

- Unicode characters in the filename of a file contained inside a zip are replaced

- ATD fails to boot in Xen when you boot from the backup disk and perform an upgrade

- ATD blacklist or whitelist detections do not show in the UI

- ATD fails to boot in Xen when you boot from the backup disk and perform an upgrade

- Ethernet Port is automatically getting down

- Service is not getting started (Like GTI Reputation, Anti-Malware Engine Service etc.)

- Memory Utilization is high

- Manual submission of Infected File for analysis is getting failed

- VM Images not booting/loading

- Unable to boot the device using external drive/USB

- ATD Health Status is showing Bad on Dashboard

- Performance Issues

- **Interactive Mode is not loading or trouble loading Interactive Mode**

- **Password is invalid (Unable to save Advanced Threat Defense FTP password)**

- **Advanced Threat Defense scheduled backup to FTP server fails when it executes the SIZE command**

- **5n. flash not exist OK (Adobe Flash Player is not validated by Advanced Threat Defense)**

- **Virtual machine creation fails with ATD**

- **ATD Auto OS selection fails and the sample is sent to the default OS**

- **Unable to connect to intfport 1/2/3 using Secure FTP**

- **ATD appliance fails to boot from the backup disk using an old image after your upgrade to 3.2.0.35**

- **ATD appliance fails to boot after upgrading the active disk from 3.2.0 to 3.2.2**

- **Uploaded VMDK file is not listed in ATD Software Management list**

General Configuration Issues

- **Error: access denied ("java.netSocketPermission" "X.X.X.X.6000" "connect, resolve") after clicking the Activation button on the VM Profile Page**

- **ATD appliance always boots to the EFI shell**

- **Windows VM image creation fails on the ATD appliance**

- **Required BIOS settings for McAfee Advanced Threat Defense appliances**

- **Sample transfer from Network Security Sensor to Advanced Threat Defense appliance times out**

- **NSM does not show results for files sent for sandbox analysis from NSP to ATD**

- **Infected File submission from NSP/MEG/MWG is getting failed but manual upload is working fine**

- **Advanced Threat Defense 3.4.x**

- **Advanced Threat Defense 3.2.x**

- **Advanced Threat Defense 3.0.4.x**

- **Advanced Threat Defense 3.0**

- **End of Life for Advanced Threat Defense 3.x.x.**

- **How to remove all blacklist entries from Advanced Threat Defense**

- **How to whitelist and blacklist files with Advanced Threat Defense**

- **How to submit Advanced Threat Defense virus and anti-malware samples (false positives or false negatives) for analysis**

- **How to enable RMM for ATD Appliances**

- **How to manually create an Intel Diagnostic Tool CD or USB**

- **How to obtain a list of current Global Threat Intelligence (FTI) IP addresses**

- **How to modify reputation scores in Threat Intelligence Exchange**

- **How to interpret Time Taken in Advanced Threat Defense Summary Report**

- **FAQs for Advanced Threat Defense**

- **ATD "show nsp scandetails" command output field and counters information**

- **Advanced Threat Defense 3.x response to CVE-2015-0235**

- **Tests performed during the ATD Windows VM validation process**