



3.4.8.142 Hotfix Release Notes

McAfee Advanced Threat Defense 3.4.8

Revision A

Contents

- ▶ *About this release*
- ▶ *New features*
- ▶ *Enhancements*
- ▶ *Resolved issues*
- ▶ *Installation and upgrade notes*
- ▶ *Known issues*
- ▶ *Product documentation*

About this release

This document contains important information about the current release. We strongly recommend that you read the entire document. McAfee Advanced Threat Defense version 3.4.8 hotfix release addresses certain issues reported by some customers and also includes some CLI commands enhancements.



This is a hotfix release. Automatic upgrade from previous software versions to this hotfix is not supported. McAfee recommends that you work with McAfee Technical Support to apply the hotfix files in your environment.

Release date — October 20, 2015

Release build — ATD software version: 3.4.8.142.52247

Product Name	Version
McAfee Network Security Platform	Network Security Manager: 8.0.5.9 or later Signature set: 8.6.18.10 or later M-series: 8.0.3.10 or later NS-series: 8.0.5.8 or later Virtual IPS: 8.0.7.9 or later
McAfee Web Gateway	7.4.0-16053 or later
McAfee Email Gateway	7.6.3 or later
McAfee Next Generation Firewall (McAfee NGFW)	5.8 or later
McAfee Data Exchange Layer	1.0.0.1070 or later
McAfee Threat Intelligence Exchange	1.0.0.824 or later
McAfee Agent	5.0.0.2710 or later
McAfee VirusScan Enterprise	1247 or later
McAfee Enterprise Security Manager (McAfee ESM)	9.4.1 or later

New features

This hotfix release includes these new CLI commands.

set gti dns check

The `set gti dns check` command requires DNS to be set for GTI to work. By default, this command is set to disabled, which means that if there is no internet access, GTI works fine. If this command is enabled, GTI will not work unless ATD is connected to the Internet and resolves GTI lookup URLs.

remove

The `remove` command removes *original samples* of all the completed samples on ATD. You can also set a daily task to automatically remove *original samples* from newly completed samples at a configured time.

For more details, see the *McAfee Advanced Threat Defense Product Guide*.

Enhancements

This release of the product includes these enhancements.

CLI enhancements

The following existing CLI commands are enhanced for this release.

- `set heuristic_analysis` — This existing command is used for the following purpose. Consider a scenario where there is a very high volume of files submitted by a channel like Network Security Sensor, Web Gateway, or Email Gateway. You want ATD to triage these files based on a need for detailed malware analysis. The intention of this triage is to scale up performance without compromising on security. The `heuristic_analysis` command is introduced to meet such a requirement.

With this release, you do not need to restart `amas` from the CLI after changing (enabling/disabling) the heuristic analysis option using `set heuristic_analysis <enable>/<disable>`.

- With this release, CLI command `set waittime` is available on the ATD UI for configuration. The same has been removed as CLI command.

XMode enhancements

User-interactive mode is enhanced and works with any browser that support HTML5 Canvas.



You do not need to install Java to use the XMode feature.

For this release, Chrome version 44.0.2403 and higher and Mozilla Firefox version 40.0.3 and higher are supported. Microsoft Internet Explorer is not supported.

You need to modify Firefox settings to use the HTML5 feature.

- 1 From the Firefox Home page, click **Options | Advanced | Certificates | View Certificates**.
- 2 From the Certificate Manager window, click **Servers**.
- 3 Click **Add Exception...** and type `https://<Host ATD IP address>:6080` and click **Get Certificate**.
- 4 Click **Confirm Security Exception** and then **OK**.
- 5 Click **Activation** or **XMode**.

Important configuration to be performed in ATD

Following are the set of important instructions issued with this release.

- LDAP configuration must be disabled before upgrading the ATD device beyond version 3.4.8.96.
- For the `atdadmin` user, the `gidNumber` value must be 1024 in the LDAP server.
- Stix report file generation is disabled by default. Use CLI command `set stixreportstatus <enable>` to enable Stix report file generation.
- If a VM license count is shown as *zero* in the UI, manually delete the corresponding VM.
- Whenever you change the IP address of an ATD appliance, reboot the device for the changes to be effective.
- You can modify the SNMP community string and SNMP trap port that was previously fixed.

Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in earlier releases, see the Release Notes for the specific release.

Resolved McAfee Advanced Threat Defense Appliance software issues

The following table lists the resolved **high-severity** issues:

ID #	Issue Description
1098118	Secondary node in a load-balancing cluster rejects samples in queue.
1098062	CLI command <code>set waittime</code> deletes some configuration parameters.
1097267	In case LDAP is enabled, <code>atdadmin</code> ftp user displays incorrect home directory.
1097264	ATD rejects/deletes majority of the samples received from NSP.
1096512	LDAP configuration (ftp) gets deleted after upgrading the ATD appliance.
1096471	When VMcreation fails, sometimes VMcreator states are not cleared.
1096469	AMAS is in deadlock state and samples remain in waiting queue.
1095996	False Positive occurs due to higher rule severity.
1080477	VMs state goes bad over a period of time.

The following table lists the resolved **medium-severity** issues:

ID #	Issue Description
1099139	When you use Mozilla Firefox or Google Chrome, syslog settings are not saved correctly.
1098257	IP address validation in UI fails if the address contains 0 in any of the octet.
1098064	In a load-balancing cluster, <code>waittime</code> from primary node is propagated to all secondary nodes.
1098032	Sample status shows invalid when the IP address of ATD is changed and the device is not re-booted.
1097577	Family Classification is not available for "Emdivi" malware family.
1096842	Invalid JSON report is generated for some samples.
1096729	CLI command <code>set heuristic enable/disable</code> requires AMAS restart for changes to be effective.
1095122	VMcreator entries fail to clear when VMcreator fails.
1095041	ATD-ePO provisioning does not happen if ePO server is not reachable at the first try instance.
1094553	Dashboard shows data based on submit time instead of last change.
1094472	GTI fails with GTI HTTP Proxy setup.
1094069	Sometimes the ATD appliance does not reboot after software upgrade.
1092541	ATD report does not display all the dropped files.
1091996	Logs of converting VMDK does not show "successful" message after conversion.
1089886	Sandbox classifies clean files as malicious.
1089635	ATD becomes non-responsive during manual upload for some large files.
1089627	ATD is unable to route malware internet traffic if interface is segregated from configured DNS.
1088781	In case of Clustered ATD, JobID/TaskID on Syslog shows incorrect file number (totally different from the ones on Analysis Results).

ID #	Issue Description
1088588	A sample blacklisted with score 5 shows score and information on Analysis Result page.
1088477	The option "Skip files if previously analyzed" is not working.
1088458	Clean files are marked as malicious in customer specific VM.
1088272	When you upgrade from 3.4.6 to 3.4.8, a Not Licensed message is displayed on the ATD user interface.
1088161	<code>show filequeue</code> command doesn't show correct results.
1087384	ATD is generating high severity score for clean samples.
1087327	Japanese file (Shift-JIS), which is zipped, gets garbled on Analysis Status page
1086889	"show filequeue" output is not using latest wait time algorithm.
1086487	Amas service crashes when URLs are fed as samples.
1086476	GTI reputation queries are not forwarded to TIE Server if DNS is not configured in the ATD.
1085894	When samples are submitted for analysis, lot of false positives are displayed for files.
1085628	ATD displays "Failed to execute YaraEngineUtility" message.
1085378	GTI Proxy does not connect to GTI.
1084815	Full sample behavior is not available in analysis report.
1084509	XMode is not working in case of non-PE files. ATD is treating these files as normal submission.
1084298	Wrong user name is issued under Syslog Event.
1084189	stack gets corrupted because of buffer overflow.
1083712	VM Validation fails for win7sp1x64 ,win2k8sp1 and win8p0x64 at AutoLogon and Sigcheck verification.
1081563	If you submit a URL having few capital characters via UI for analysis, Invalid URL error message is displayed.
1080462	Results on UI are not in sync with the page numbers displayed.
1078972	During sample execution, Flash Player crashes inside the VM.
1077888	After upgrade to 3.4.6.83, samples from NSM gets queued but are not processed.
1077405	Samples behave inconsistently due to sample crash in the VM.
1077010	After reboot, samples in queue, submitted via URL and URL download are shown as invalid.
1055458	Original sample download and complete result download does not have .zip extension.
1029702	SNMP: Process trapsender not sending traps immediately after the threshold value is exceeded.
1029436	SNMP: User has no option to change community string or Port for SNMP configuration.

Installation and upgrade notes

Review the following before you install McAfee Advanced Threat Defense in your network.

If you have already deployed McAfee Advanced Threat Defense and you require information on how to upgrade to this release of McAfee Advanced Threat Defense, refer to step 3 below.

If you are installing McAfee Advanced Threat Defense, then review the steps below.

- 1 Review the *Warnings and cautions* and the *Usage restrictions* sections in the *McAfee Advanced Threat Defense 3.4.8 Product Guide*.
- 2 Refer to *McAfee Advanced Threat Defense 3.4.8 Product Guide* for information on how to install the McAfee Advanced Threat Defense Appliance. You can also refer to the *McAfee Advanced Threat Defense 3.4.8 Quick Start Guide* for information on how to quickly set up the McAfee Advanced Threat Defense Appliance.
- 3 Refer to the *Upgrade McAfee Advanced Threat Defense and Android VM* section in the *McAfee Advanced Threat Defense 3.4.8 Product Guide* and upgrade the embedded McAfee Advanced Threat Defense software to 3.4.8.x.
 - If the current version is below than 3.4.2.32 and you want to upgrade to 3.4.8.x, you upgrade the McAfee Advanced Threat Defense to 3.4.2.32 or above and then upgrade to 3.4.8.x.
 - If the current version is 3.4.2.32 or above, you can directly upgrade to 3.4.8.x.



Once you upgrade, you cannot downgrade by loading the backup image using the `reboot backup` command.



Once you upgrade to 3.4.8.x, you cannot downgrade by using `system.msu` files.



Once you upgrade to 3.4.8.x, use `copyto backup` command to ensure that the Active disk and Backup disk remain on the same software version of McAfee Advanced Threat Defense.



Boot from Backup disk is not supported in case the Backup disk and Active disk reside at different software versions of McAfee Advanced Threat Defense.

The Android version in the default Android analyzer VM is 2.3. After you upgrade McAfee Advanced Threat Defense software to 3.4.8.x, you can upgrade the Android version to 4.3.



We strongly recommend you to upgrade your McAfee Advanced Threat Defense Appliance to 3.4.2.32 or later versions.

- 4 Refer to *McAfee Advanced Threat Defense 3.4.8 Product Guide* and configure it for malware analysis.
- 5 To integrate with Network Security Platform, refer to the corresponding Network Security Platform release notes as well as the latest *Network Security Platform Integration Guide*. Recall that you need a Manager and a Sensor on version 8.0 or later.
- 6 To integrate with McAfee Web Gateway, you need McAfee Web Gateway 7.4.0-16053 or later. Refer to the *McAfee Web Gateway 7.4.0 Product Guide*.
- 7 To integrate with McAfee ePO, you need version 4.6 or later. In order to integrate McAfee Advanced Threat Defense with McAfee® Threat Intelligence Exchange (TIE), you need 5.1.1 or above version of McAfee ePO. The information for this integration is in the *McAfee Advanced Threat Defense 3.4.8 Product Guide*.

Known issues

McAfee Advanced Threat Defense software issues in this release: [KB83259](#).

Product documentation

Every McAfee product has a comprehensive set of documentation.

Find product documentation

- 1 Go to the McAfee ServicePortal at <http://mysupport.mcafee.com> and click **Knowledge Center**.
- 2 Enter a product name, select a version, then click **Search** to display a list of documents.

3.4.8 product documentation list

The following software guides are available for Advanced Threat Defense 3.4.8 release:

- Quick Start Guide
- Product Guide
- API Reference Guide

Copyright © 2015 McAfee, Inc. www.intelsecurity.com

Intel and the Intel logo are trademarks/registered trademarks of Intel Corporation. McAfee and the McAfee logo are trademarks/registered trademarks of McAfee, Inc. Other names and brands may be claimed as the property of others.

0A-00