# Upgrade Guide for Advanced Malware Detection On-Premises v1.1

Upgrade Guide | AMD OP | v1.1 | 20-May-2019

| | |
|---|---|
| **Applies to:** | • Advanced Malware Detection On-Premises v1.1 |

Use these instructions to upgrade from Advanced Malware Detection On-Premises v1.0 to Advanced Malware Detection On-Premises v1.1.

This document covers the following topics:



For additional information about this release, see:

- Advanced Malware Detection On-Premises v1.1 Release Notes
- Advanced Malware Detection On-Premises Manager Installation Guide
- Advanced Malware Detection On-Premises Engine Installation Guide

## Installing the latest packages

1. Download the latest packages from Forcepoint:
   a. Log on to the Forcepoint Downloads page.
   b. Go to **Advanced Malware Detection > Advanced Malware Detection On-Premises**, select a version, and then download the zip file containing the v1.1 package.
2. Using the Advanced Malware Detection On-Premises administrator account, transfer the zip file to the **/tmp/** folder on the Advanced Malware Detection On-Premises Manager using a file transfer application (e.g., Winzip or FileZilla).
3. Using SSH, log on as the administrator, then switch to the root user:

   ```
   su -root
   ```
4. Change to the /tmp/ folder:

   ```
   cd /tmp/
   ```

5. Extract the shell script and rpm files from the zip file to the **/tmp/** folder:

   ```
   unzip <filename>
   ```

   where **<filename>** is the name of the zip file downloaded from Forcepoint. For example, if the filename is AMD-r1.1.1-47.zip, the command would be:

   ```
   unzip AMD-r1.1-47.zip
   ```

   The following files are extracted:

   - AMD-monitor-1.0.1-8.26c5762.noarch.rpm
   - AMD-shim-1.0.1-8.26c5762.noarch.rpm
   - AMD-config-1.1.0-47.d8c8baa.noarch.rpm
   - AMD-dhcp-server-config-1.1.0-47.d8c8baa.noarch.rpm
   - AMD-harden-1.1.0-47.d8c8baa.noarch.rpm
   - AMD-monitor-1.1.0-47.d8c8baa.noarch.rpm
   - AMD-network-config-1.1.0-47.d8c8baa.noarch.rpm
   - AMD-rsyslog-client-1.1.0-47.d8c8baa.noarch.rpm
   - AMD-shim-1.1.0-47.d8c8baa.noarch.rpm
   - AMD-yum-client-1.1.0-47.d8c8baa.noarch.rpm
   - update_all.sh

6. After the files are extracted, run the shell script:

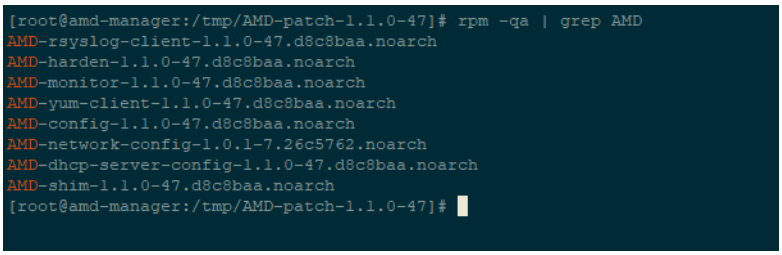
   ```
   sh update_all.sh
   ```

   Running this script updates all of the necessary packages, except for AMD-network-config (which does not require an update).

7. To verify that the files are installed correctly, run the following command:

   ```
   rpm -qa | grep AMD
   ```

   The command output should be similar to the following:




   The version numbers in your output might differ from the version numbers shown in the above image. The version numbers in the output should match the version numbers in the filenames extracted from the zip file.

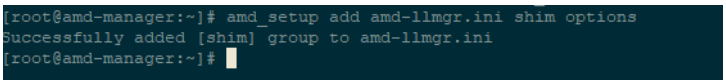
   If your output is similar to the image above, then Advanced Malware Detection On-Premises was successfully updated.

# Configuring Advanced Malware Detection On-Premises after installing the latest packages

1. As the root user, run the following command:

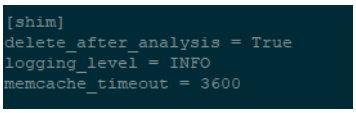
   ```
   amd_setup add amd-llmgr.ini shim options
   ```

   Running this command creates configurable options within the **/etc/lastline/amd-llmgr.ini** file. If it was successful, the command output should be similar to the following:

   Within the **amd-llmgr.ini** file, the following option group can now be configured:

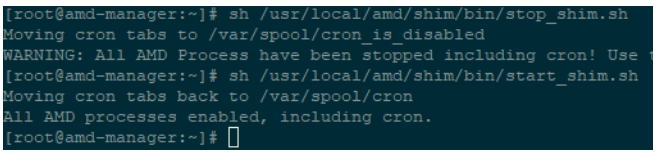
   - **delete_after_analysis**: Removes any records of the file sent to be analyzed. The default value is **True** for GDPR customers. The other available option is **False**.
   - **logging_level**: Adjusts the logging level for improved or minimal logging. The default value is **INFO**. Available values are (from least verbose to most verbose):
     - CRITICAL
     - ERROR
     - WARNING
     - INFO
     - DEBUG
   - **memcache_timeout**: The time interval (in seconds) when the cache is cleared. The default value is **3600** (the cache is cleared every 60 minutes), and can be changed to any value between 1500 (25 minutes) and 3600 (60 minutes).

2. After you configure the new options, run the following two scripts to restart shim and save the changes:

   ```
   sh /usr/local/amd/shim/bin/stop_shim.sh
   sh /usr/local/amd/shim/bin/start_shim.sh
   ```

   If it was successful, the command output should be similar to the following:

# Verifying successful crontab setup

This crontab check is not required for every upgrade, but Forcepoint highly recommends it. If this check is not completed, and crontab is not configured correctly, Advanced Malware Detection On-Premises stops working after a few days because of a lack of disk space.

To verify that the crontab scripts are correctly set up:

1. As the root user, run the following command from the command line:

   ```
   crontab -e
   ```

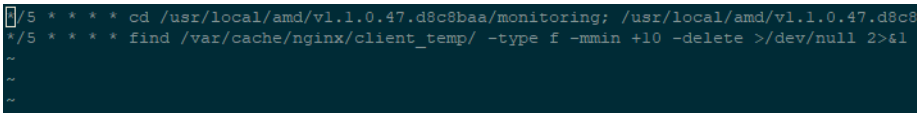
   The following output should be shown:

   ```
   */5 * * * * cd /usr/local/amd/v1.1.0.47.d8c8baa/monitoring;
   /usr/local/amd/v1.1.0.47.d8c8baa/monitoring/amdmon.sh >/dev/
   null 2>&1
   */5 * * * * find /var/cache/nginx/client_temp/ -type f -mmin
   +10 -delete >/dev/null 2>&1
   ```

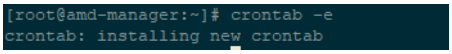
   If the above output is shown (regardless of order), crontab is successfully configured and no further steps are required.

   If the above output is not shown, continue to step 2.

2. Press **i** to enter Insert mode. The word INSERT is shown at the bottom of the window.
3. Copy the output in step 1 above and paste it into the command prompt window.

4. To save the changes and exit, press **Esc**, then type **:wq** and press **Enter**.
5. After the crontab updates are saved, the following status is shown:

6. To verify that the crontab is successfully installed, monitor the **/var/cache/nginx/client_temp/** folder:

   ```
   watch du -sh /var/cache/nginx/client_temp
   ```

7. Verify that the disk memory used is near **0**.

   If the size of disk space used continues to grow after 5 minutes, crontab may be set up incorrectly. Try this procedure again to set up crontab. If you continue to have this issue, contact Forcepoint Support.