FORCEPOINT

Installation Guide

Advanced Malware Detection On-Premises Manager

v1.0

Contents

1 | Introduction

This guide describes the process to install the Advanced Malware Detection On-Premises Manager component on hardware provided by the customer.

The Manager is offered as part of the on-premises deployment configuration to customers with stringent privacy and policy constraints. In this configuration, the Manager stores, within the customer's data center, all the information regarding the detection of infected hosts and the analysis of software artifacts.

The Manager collects information from Forcepoint appliances, processes it, and presents it to the user. More precisely, the Manager receives artifacts (i.e., executables and documents) that are received or downloaded by the users and passes them to an Analysis Engine. The results of the analysis are collected and presented to the user via a web portal using an incident-centered approach in which evidence from run-time analysis, network monitoring, and anomaly detection are correlated to provide prioritized and actionable threat intelligence.

The Manager provides a dashboard to manage appliances. It is also responsible for downloading the latest network behavior models that are associated with malware activity.

2 | Prerequisites

Hardware

Advanced Malware Detection On-Premises Manager is a software solution that leverages your existing hardware. The following system requirements provide the minimum specifications for optimal performance and effectiveness.

- 1x Intel Xeon E5 6-core CPU
- 48 GB RAM
- 4x 2TB 7.2K RPM SATA disks (RAID 10)
- Dual PSU (highly recommended)
- ILO/LOM/DRAC (highly recommended)

Forcepoint also offers an option of purchasing a Dell PowerEdge R430 server that is suitable for hosting Advanced Malware Detection On-Premises Manager. Forcepoint delivers the server with the Advanced Malware Detection On-Premises Manager software pre-installed.

Network connectivity

The server needs to be able to connect to:

- log.lastline.com to TCP port 443.
- update.lastline.com to TCP port 443 and optionally to UDP port 123 for time synchronization. The latter can be replaced with a local NTP server.
- management.lastline.com to TCP port 443.
- user.lastline.com to TCP port 443.
- anonvpn.lastline.com to UDP port 1194 (this is not mandatory, but highly recommended, as the lack of it can negatively impact the performance and malware detection capability of the analysis engine).

The domain names above may resolve to any IP addresses in the following ranges:

- 38.95.226.0/24
- 38.142.33.16/28
- 199.91.71.80/28
- 46.244.5.64/28

All the connections can be optionally routed through an explicit HTTP proxy, but proxy authentication is not supported.

License

Before starting the installation, you need to acquire a license for the software. This is done by contacting Forcepoint Sales.

If you have already purchased the product, your license information can be found under the Products tab after you log on to the [Forcepoint Support Portal](). The following license information is provided:

- AMD Portal Username
- API Key
- FQDN

Furthermore, you will need your Lastline Portal password. To retrieve this password:

1. Navigate to the [Lastline Portal]().
2. Click **Forgot your password?**
3. Follow the instructions provided on the Portal. You will need your Lastline Account Username.

License extensions

To renew an expired license, contact Forcepoint Sales. Once your request has been processed, your license expiration date will automatically be extended.

3 | Installation Process

The installation process for the Advanced Malware Detection On-Premises Manager consists of three steps. In the first step, the base system is installed. In the second step, basic configuration information is collected and the configuration is applied to the system. In the final step, required components for the analysis of malicious files are downloaded and installed on the system.

If you purchased a Dell PowerEdge R430 server from Forcepoint with the Advanced Malware Detection On-Premises Manager software pre-installed, skip to *Registration and configuration*, page 6.

Base system installation

Preparing hardware

Before starting the installation of the Advanced Malware Detection On-Premises Manager software, the RAID controller must be configured in RAID10. If you bought a PowerEdge R430 directly from Dell, the RAID controller will likely not be configured appropriately. Please see *RAID Configuration for Dell PowerEdge R430*, page 23 for configuration instructions.

> **Important**
>
> Before you install the software, wire the Advanced Malware Detection On-Premises Manager as shown in the *Quick Start Guide* (included with your Advanced Malware Detection On-Premises server). It is important that the E port (2nd interface/bottom port) be connected to either an Advanced Malware Detection On-Premises Engine or network switch that is powered ON. Software installation should take approximately 30 minutes.

Software installation

The Advanced Malware Detection On-Premises Manager uses CentOS 7 as the underlying operating system. It uses an automated installation process that eliminates the need for user input. The installation is text-based; no graphical user interface is provided.

Before starting the installation, you must obtain an official copy of the latest Advanced Malware Detection On-Premises Manager ISO from Forcepoint. The image may be burned onto a bootable DVD, or simply mounted using the Dell iDRAC interface, if available.

To install Advanced Malware Detection On-Premises Manager, boot the system from the selected medium and let it run to completion. The installation is automatic and will only stop if it encounters a hardware error. The system will reboot twice, and then present you with a log on prompt.

Registration and configuration

To register and apply the software configuration to the Advanced Malware Detection On-Premises Manager, log on to the console using

- username: **root**
- password: **P!L)TP@ssw0rd**

Note, it is possible to log on with the username and password only from a console.

> **Important**
> This is a default password that is available for all Advanced Malware Detection On-Premises Engine installations. It is highly recommended to change the default password to a password that is unique to your organization.

```
##################################################################################
#
#                            WARNING
#
# This system is for the use of authorized users only. Company resources,
# including computers, communications equipment, and associated devices (e.g.
# internet, electronic mail, voice mail, copiers, facsimile machines) are to be
# used for company business purposes. Use of these systems constitutes
# acknowledgement and consent to company monitoring of these systems.
#
##################################################################################
amd-manager login: root
Password:
Last login: Tue Jul 11 21:15:15 on tty1
[root@amd-manager:~]#
```

Execute **amd_register**, which will start the guided configuration and installation process.

```
##################################################################################
#
#                            WARNING
#
# This system is for the use of authorized users only. Company resources,
# including computers, communications equipment, and associated devices (e.g.
# internet, electronic mail, voice mail, copiers, facsimile machines) are to be
# used for company business purposes. Use of these systems constitutes
# acknowledgement and consent to company monitoring of these systems.
#
##################################################################################
amd-manager login: root
Password:
[root@amd-manager:~]# amd_register
```

If asked what interface to use as the primary network interface, select **eth0**. If a different interface is selected, some components may not work properly.
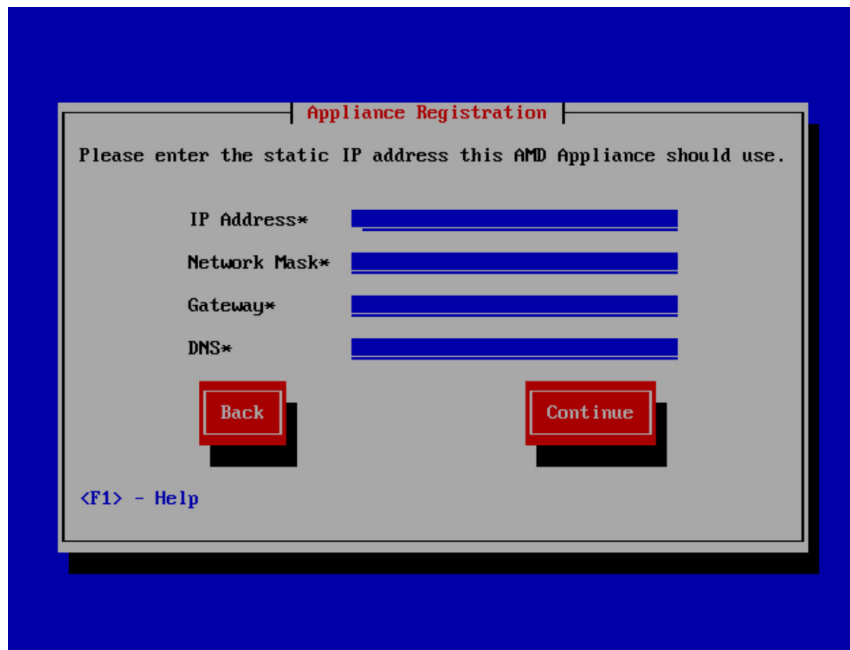
The installation process starts at the Welcome screen. When you are ready to begin the installation process, select **Start**.

The installation process will then give you the opportunity to configure the network via DHCP (**Obtain via DHCP**) or a static IP address (**Enter a static address**). Select your option, then select **Continue**.
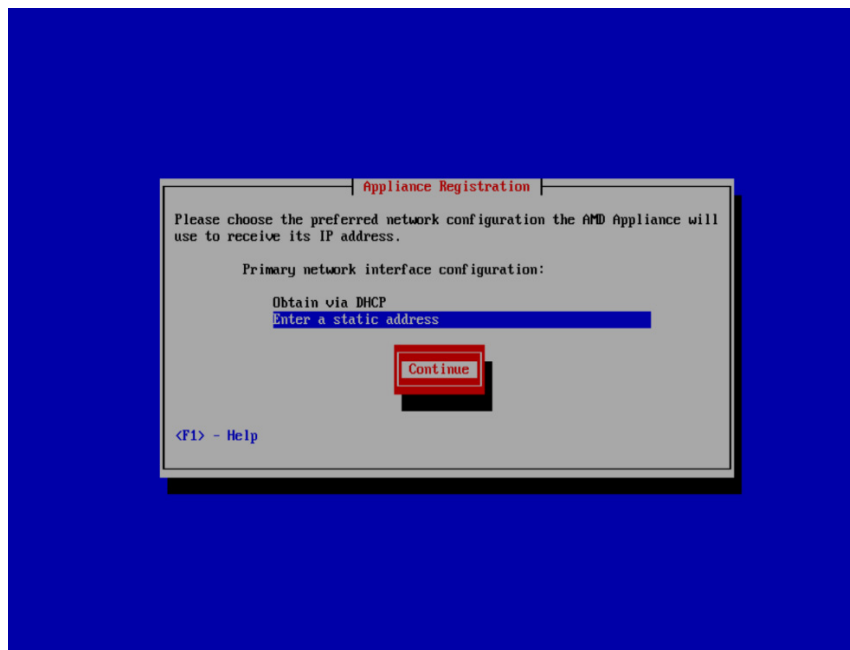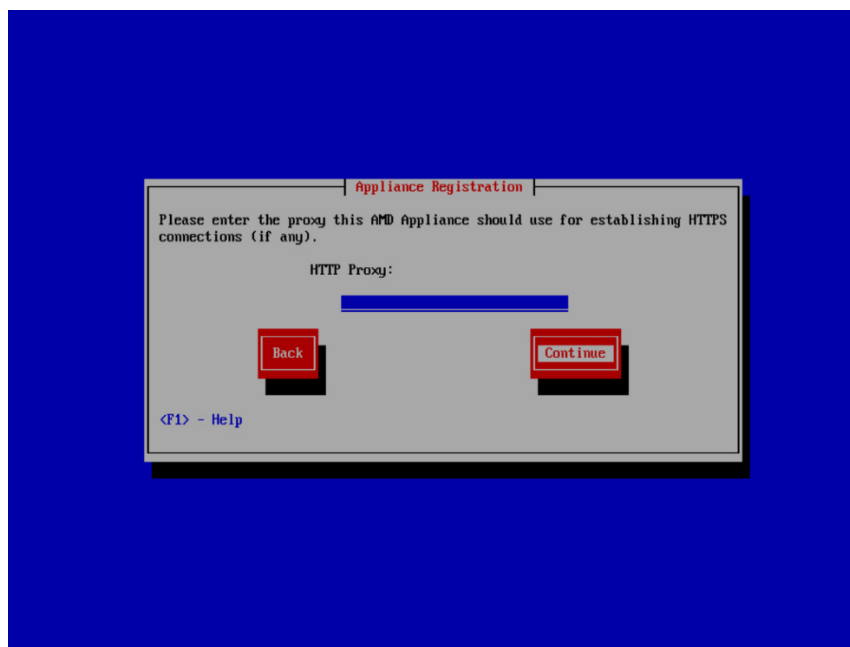
If you selected **Enter static address**, input the **IP Address** to be assigned to the interface, the **Network Mask**, **Gateway** address, and **DNS** address.

You then have the option of configuring an HTTP proxy for connecting to the update servers.

If no proxy configuration is required to access the Internet via HTTPS, this field should be left empty. Otherwise, if all HTTPS connections need to go through an HTTP proxy, the address of the proxy must be entered here. Optionally, a non-default port of the proxy server can be specified. Valid proxy configuration examples are: **my_proxy.my_domain.com:3128** and **192.168.0.1:8080**.

At this point, the network configuration is applied.

In the next step, the system will ask for an NTP server. Unless the use of a different NTP server is needed, keep the default value. The system must be able to reach the chosen NTP server over UDP port 123.


On the next screen, type the **Forcepoint Username** and **Forcepoint Password** provided with the license.
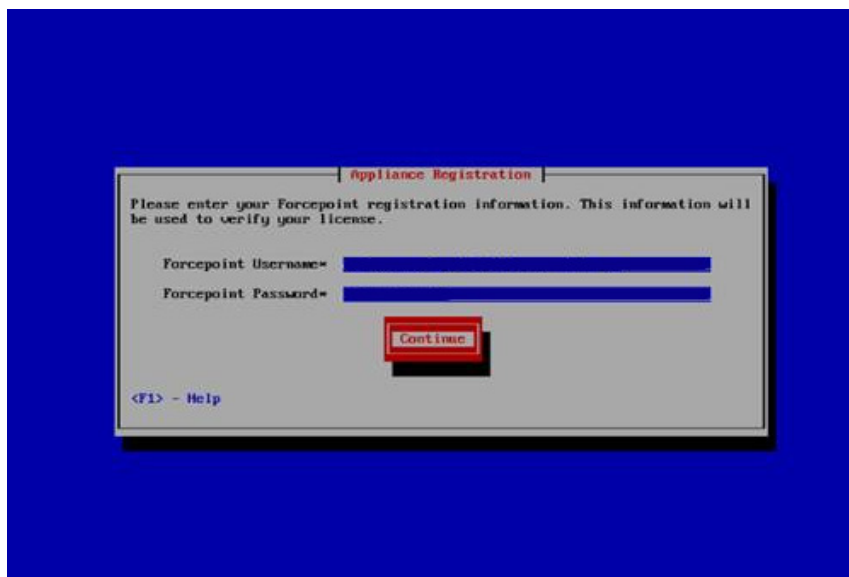
Next, you must provide the license information to the Advanced Malware Detection On-Premises Manager. More precisely, you are required to enter the license key and the assigned FQDN associated with the purchased license. See *License*, page 4 for details on acquiring your license information.
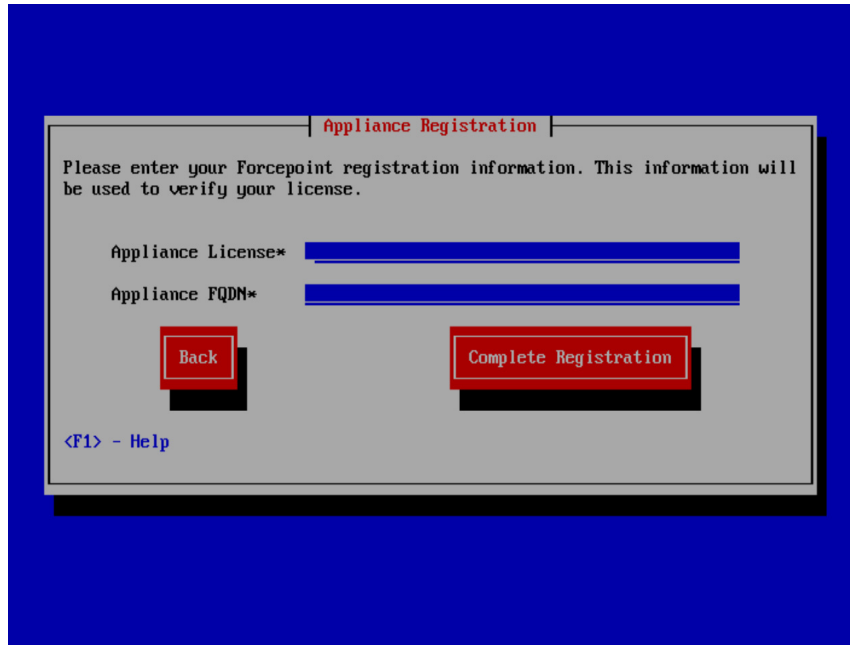
Select **Complete Registration**. You will be prompted to verify your readiness to complete the configuration process. Select **Yes** to begin the system configuration and product registration. Internet access is required throughout this portion of the registration process.
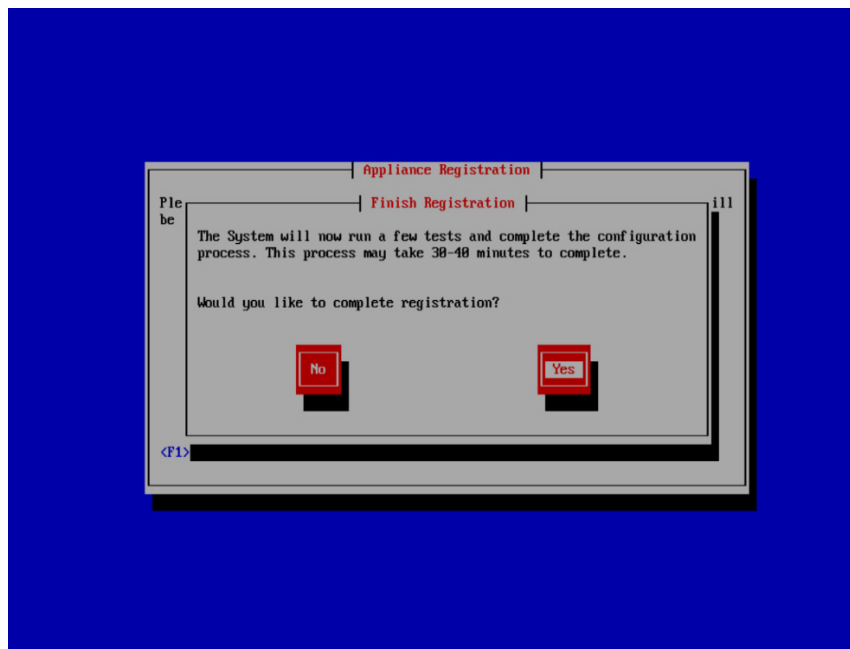
After system configuration is complete, the remaining process will be testing, applying configurations, and registering the Advanced Malware Detection On-Premises Manager. This process may take up to 30 - 40 minutes to complete depending on network connectivity and system characteristics.
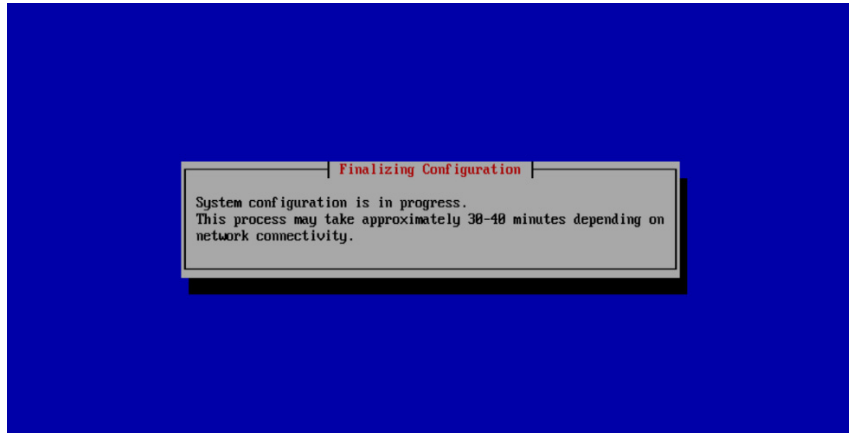
After the installation process completes, select **OK** to exit the installation wizard.

In case any error message is displayed, please refer to *Error handling*, page 16.

Final installation steps

As a final step, the Advanced Malware Detection On-Premises Manager needs to download from the update servers the latest images used by the malware analysis sandbox component. The image files consist of 13 GB of data; therefore, this step might take several hours, depending on the available network bandwidth.

After a successful registration, the installation wizard prompts you to complete the installation at a later time or immediately.

There are two methods of running this process:

- Finishing the installation through the wizard: Select **Yes**, and then follow the instructions in *Finishing the installation through the wizard* below.
- Finishing the installation through the command line: Select **No**. At a later time, follow the instructions in *Finishing the installation through the command line* below.

Finishing the installation through the wizard

If you select **Yes** on the Registration Complete screen, the installation wizard displays a screen with instructions on how to monitor the status of the Advanced Malware Detection On-Premises Manager and view the logs. When you select **Finished**, the Advanced Malware Detection On-Premises Manager will automatically start the image updates.

Finishing the installation through the command line

If you select **No** on the Registration Complete screen, the installation wizard displays a screen with instructions on how to download the images from the command line. Select **Proceed to exit** to exit the installation wizard, or select **Return** to go back to the Registration Complete screen, where you may choose to finish the installation immediately.
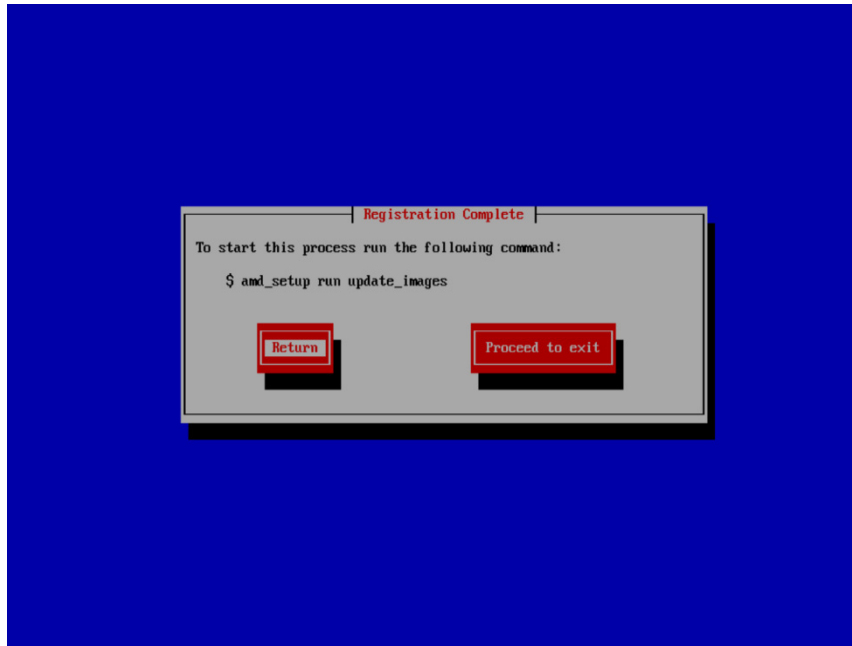
To update the images at another time, outside of the registration wizard, run the following command:

```
amd_setup run update_images
```

At this point, users can direct the browser to https://<<*IP address of AMD Manager*>> or https://<<*assigned FQDN*>> to access the user portal.

4 | System Administration

The Advanced Malware Detection On-Premises Manager is developed to require as little maintenance and administration as possible. The only action that might be required is to change the system's network configuration, as discussed below.

We also provide a troubleshooting guide that allows the administrator to ensure that everything works properly.

Advanced Malware Detection On-Premises Manager installation wizard

The easiest way to modify the system configuration is by re-running the Advanced Malware Detection On-Premises Manager installation wizard tool using the following command:

```
amd_register
```

You will be able to change the latest configuration values provided the last time the installation wizard was run.

Advanced Malware Detection On-Premises configuration tool

The system comes with the Advanced Malware Detection On-Premises configuration tool **amd_setup**, which provides an interface to administrate and manage the Advanced Malware Detection On-Premises Manager. The tool can be started by logging on to the Manager virtual machine:

1. Connect to the Manager through SSH, run the following command from the command line:

```
ssh <<IP address of AMD appliance>>
```

   a. SSH credentials:
      ○ username: **admin**

- ○ password: **D#FP@ssw0rd**

2. Run the following command from the command line:

   ```
   amd_setup <action> <arguments>
   ```

   > **Important**
   > This is a default password that is available for all Advanced
   > Malware Detection On-Premises Engine SSH connections. It is
   > highly recommended to change the default password to a password
   > that is unique to your organization.

Error handling

In case any error message is displayed when using **amd_setup**, please contact
Forcepoint Support.

Network configuration

The Advanced Malware Detection On-Premises server connects to 2 networks: the
primary (external) network and the private analysis network.

Primary network

The primary (external) network connects to **eno1** and must be able to provide NTP
and DNS services, and be able to connect to the Internet, which is required for product
registration and for downloading images required by the Advanced Malware
Detection On-Premises Engine appliances.

The Advanced Malware Detection On-Premises Manager can also receive network
configuration via DHCP over this interface. This can be configured using the
amd_register utility described in *Advanced Malware Detection On-Premises Manager
installation wizard* above.

Use the IP address assigned to this interface to access the Advanced Malware
Detection On-Premises user interface.

Analysis network

The Advanced Malware Detection On-Premises Manager connects to the analysis
network using the **eno2** interface. This is reserved for connecting the Advanced
Malware Detection On-Premises Engine appliances with the Advanced Malware
Detection On-Premises Manager. Additionally, the Advanced Malware Detection On-
Premises Manager provides network configuration via DHCP to all Advanced
Malware Detection On-Premises Engines connected to this network.

The Advanced Malware Detection On-Premises Manager uses the static IP address 10.0.0.10 for this network. This is not configurable.
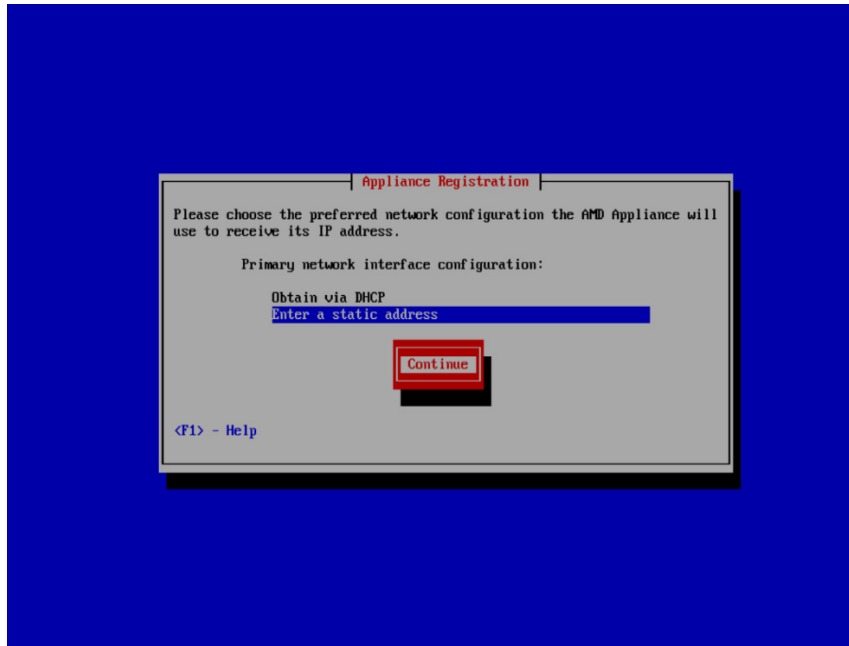
Configuring the network address through DHCP

If you selected a static IP-based network configuration during the initial installation, you may switch this to a DHCP-based network configuration at a later time. To switch to a DHCP-based network configuration, run the Advanced Malware Detection On-Premises Manager installation wizard tool using the following command:

```
amd_register
```

The following installation wizard screen displays.

Select **Start** to begin. The fields should be selected as last entered. For example, if you selected **Enter Static Address** the last time the wizard was run, the following screen displays.

From this screen, you may select the alternate option of how the IP is configured. Select **Obtain via DHCP** to have Advanced Malware Detection On-Premises automatically be configured with DHCP. At this point, no configuration changes have yet been applied. Select **Continue** and iterate through the remaining screens to apply the configuration changes. Select **Complete Registration**, and then select **Yes** to complete the registration and apply the changes.

Configuring the static network address

If you selected a DHCP-based network configuration during the initial installation, you may switch this to a static IP-based network configuration at a later time. To switch to a static IP-based network configuration, run the Advanced Malware Detection On-Premises Manager installation wizard tool using the following command:

```
amd_register
```

The following installation wizard screen displays.

Select **Start** to begin. The fields should be selected as last entered. For example, if you selected **Obtain via DHCP** the last time the wizard was run, that option is highlighted.

From this screen, you may select the alternate option of how the IP is configured. Select **Enter a static address** to have Advanced Malware Detection On-Premises automatically be configured with a static IP address. At this point, no configuration changes have yet been applied. Select **Continue** and type the **IP Address**, **Network Mask**, **Gateway**, and **DNS** to configure the static IP address.
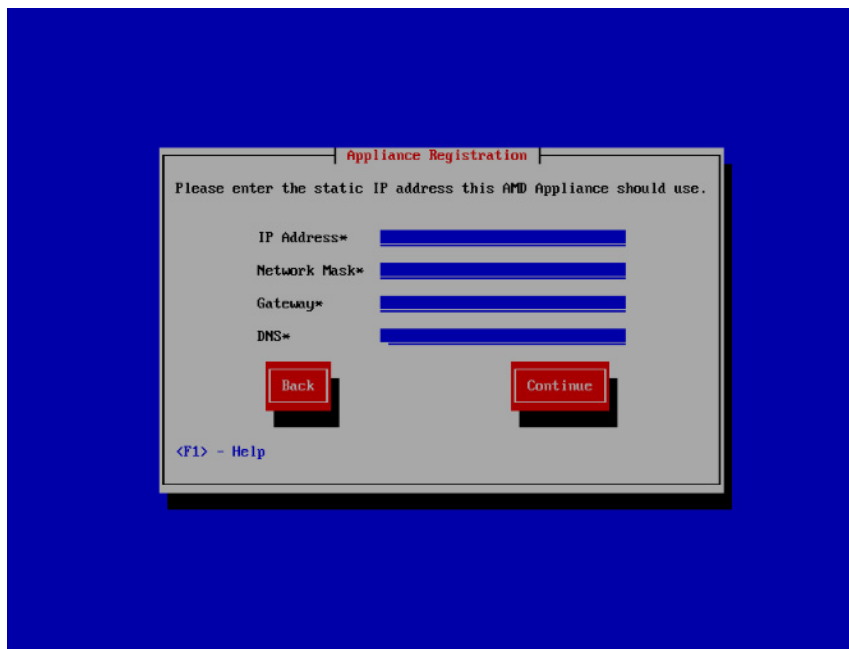
Select **Continue** to iterate through the remaining screens to apply the configuration changes. Select **Complete Registration**, and then select **Yes** to complete the registration and apply the changes.

Configuration update after a network DHCP change

After a new network address has been assigned to the host (e.g., after the DHCP server hands out a new network address), the new configuration needs be applied to all software on the host. To do so, log on to the console of the host and issue the following command (for password, see *Registration and configuration*, page 6):

```
lastline_apply_config
```

5 | Software Upgrades

Forcepoint periodically releases appliance and software upgrades or hotfixes. Available updates will be communicated through email along with Release Notes and upgrade instructions.

If the software has automatic updates enabled, these updates will transparently be applied.

Automatic software updates are enabled by default upon installation. To disable automatic upgrades, or to manually upgrade an appliance with automatic updates disabled, log on to the web interface of the appliance itself and access the appliance configuration page from the Appliances tab.

System appliance updates released by Forcepoint will be communicated through email. To manually check for system updates, log on to the appliance as an administrator and run the following commands:

```
cd /usr/local/amd/shim/bin/
./check_for_updates
```

If updates are available, you will be shown the version available and be instructed to run the following command to install the appliance updates:

```
./update_amd
```

6 | RAID Configuration for Dell PowerEdge R430

Launch PERC Configuration Utility by pressing **<Ctrl>+R** during the server boot sequence:

```
F2  = System Setup
F10 = Lifecycle Controller
F11 = Boot Manager
F12 = PXE Boot

Initializing Serial ATA devices...


Broadcom NetXtreme Ethernet Boot Agent
Copyright (C) 2000-2015 Broadcom Corporation
All rights reserved.
Press Ctrl-S to enter Configuration Menu

PowerEdge Expandable RAID Controller BIOS
Copyright(c) 2015 Avago Technologies
Press <Ctrl><R> to Run Configuration Utility
_
```

Once the configuration utility started, press **F2** on your keyboard and select **Convert to RAID Capable**.
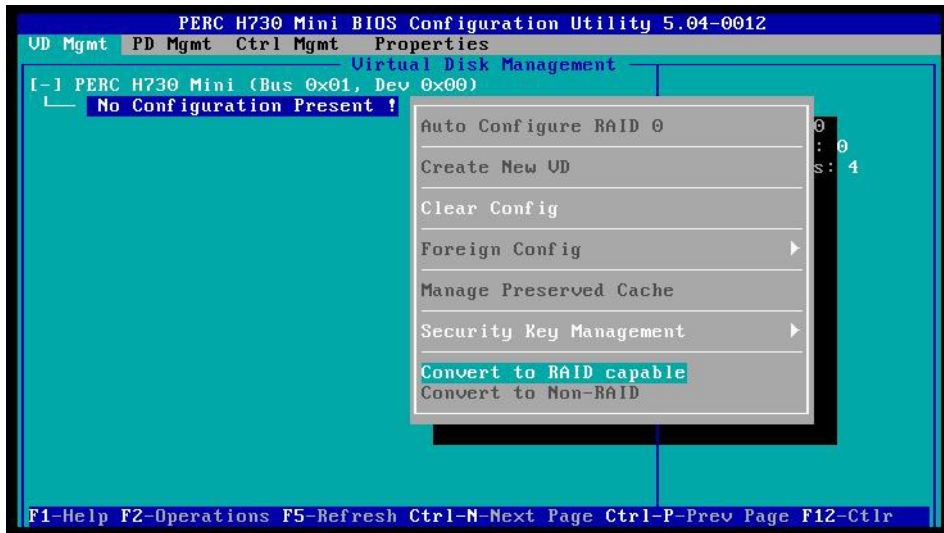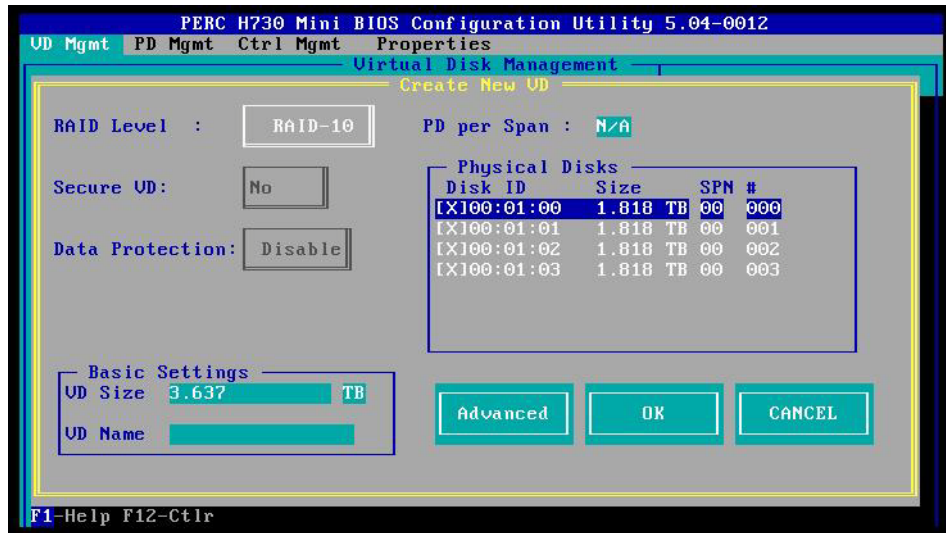
Select all 4 disks and select **OK**.


After that, you should see the 4 disks.
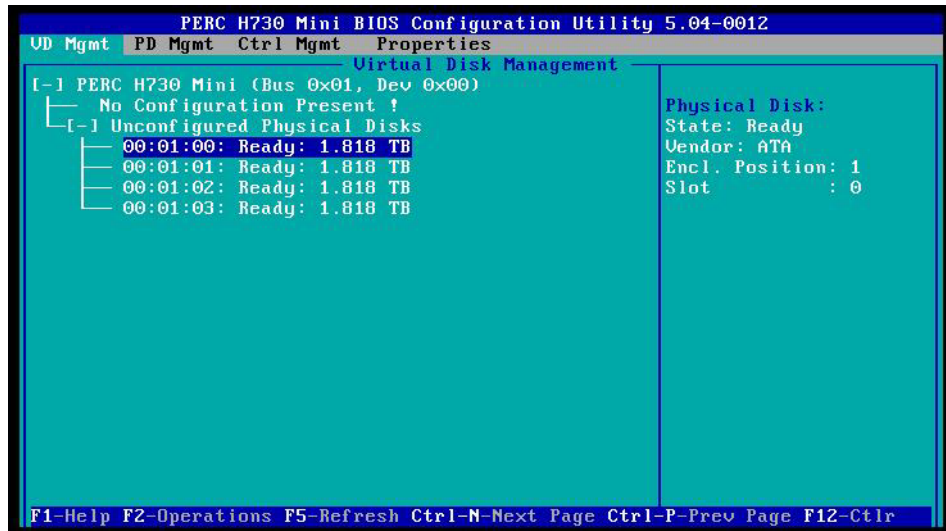
Press **F2** on your keyboard and select **Create New VD**.

Select all 4 disks, make sure **RAID Level** is set to **RAID-10**, then select **Advanced**.

Make sure **Write Policy** is set to **Write Back**, **Disk cache policy** is set to **Disable** and **Force WB with no battery** is not select. Then select the **Initialize** option (select **OK** if an initialization confirmation pop-up appears).
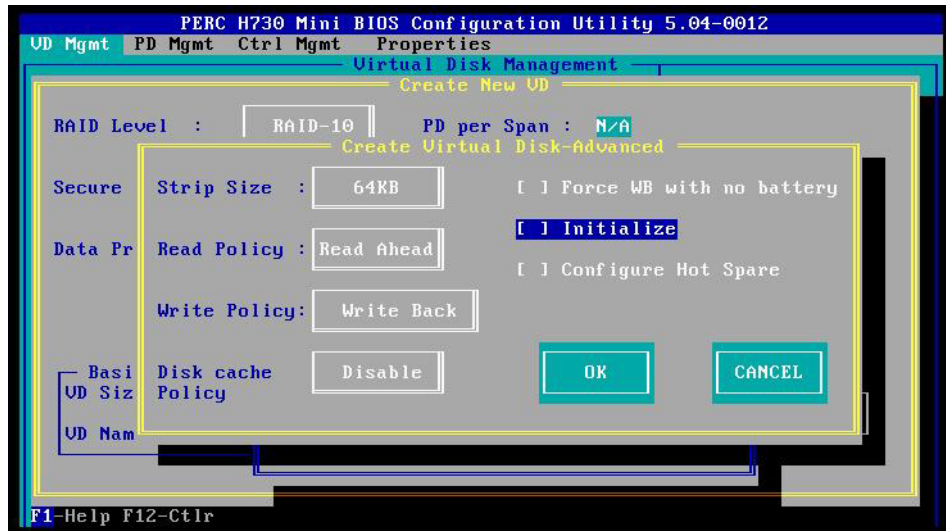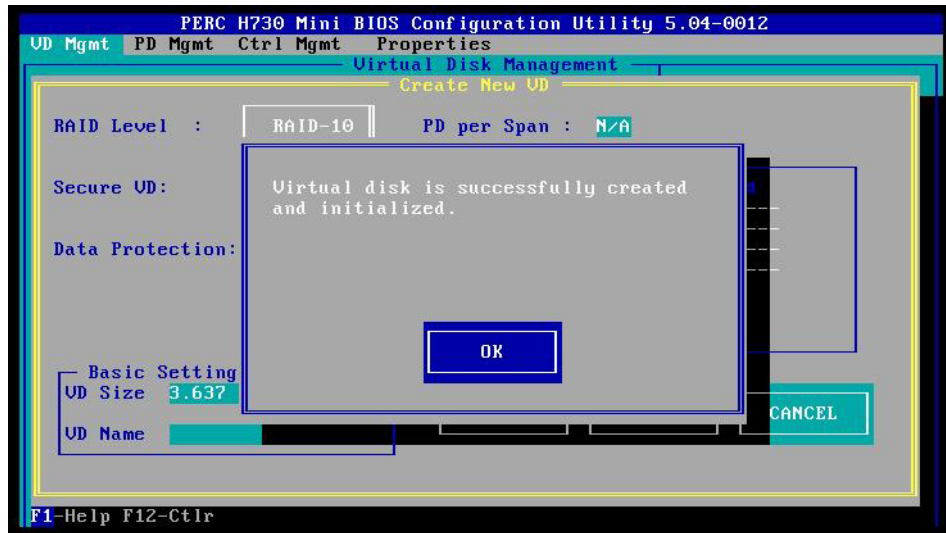

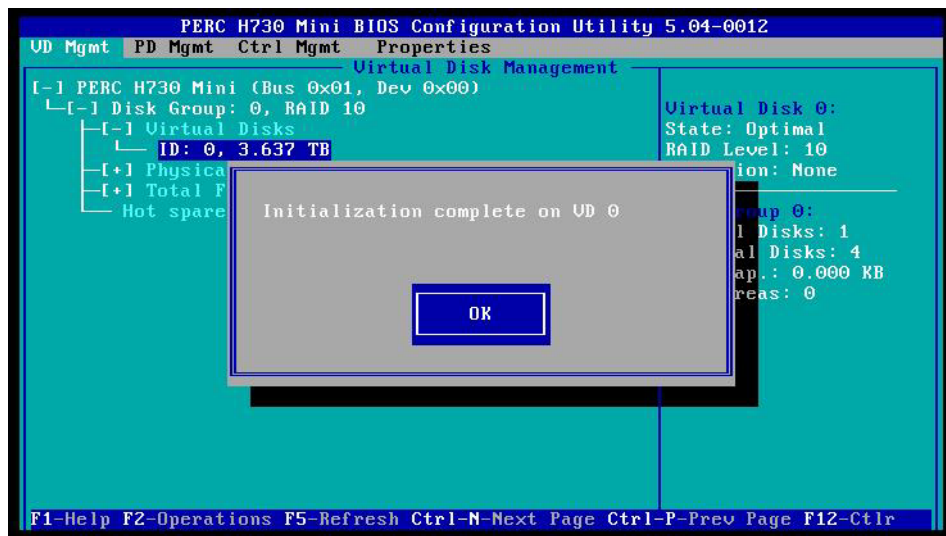After initialization is complete, select **OK** to save the advanced settings.
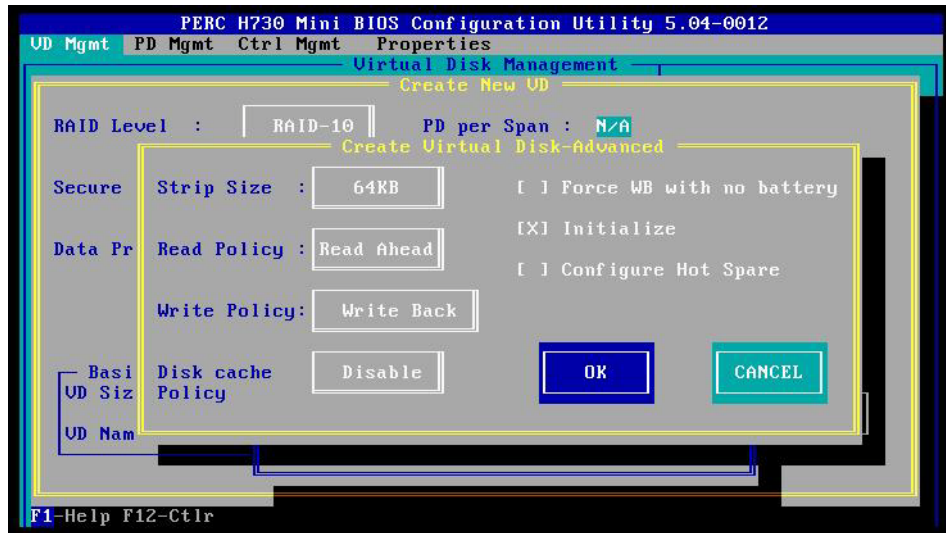
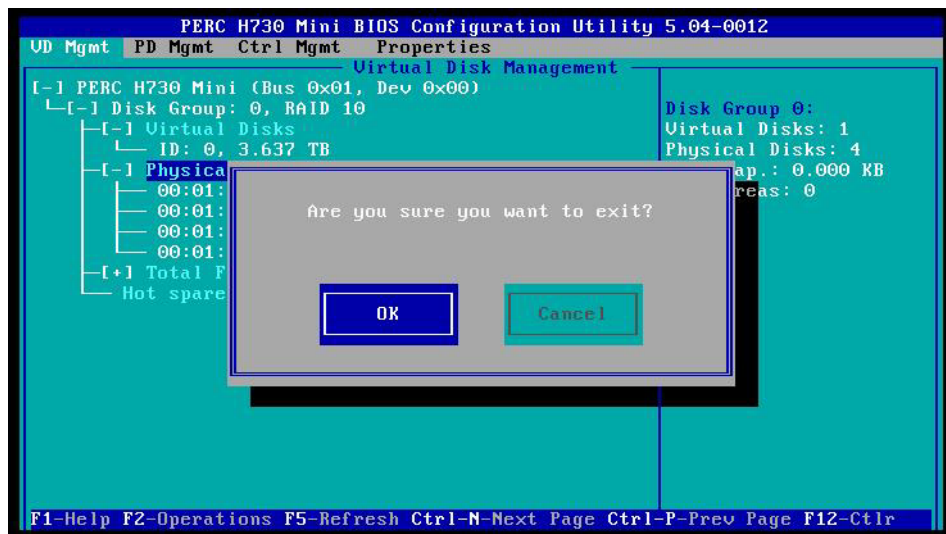Select **OK** to create the virtual drive.

Select **OK** to confirm.

Select **OK** to confirm the initialization.

This is what the virtual and physical disks should look like.

Press **ESC** on your keyboard and then select **OK** to exit.

7 | Copyrights and Trademarks

Every effort has been made to ensure the accuracy of this manual. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Copyrights and trademarks

Other acknowledgments

This Forcepoint product uses the third-party software listed in this file. In addition, this Advanced Malware Detection On-Premises product includes or may include the following open source components:

NGINX 1.10.3, © 2002-2017 Igor Sysoev, © 2011-2017 Nginx, Inc., is distributed under the BSD 2-Clause License (opensource.org/licenses/BSD-2-Clause) ▪ PYTHON 2.7.5, © 2001-2017 Python Software Foundation, is distributed under the Python License (docs.python.org/3/license.html) ▪ UWSGI V2.0.14, © 2016 anthon, unbit, is distributed under the GNU General Public License, version 2 with Classpath Exception (gnu.org/software/classpath/license.html) ▪ UWSGI-PLUGIN-COMMON V2.0.14, © 2016 anthon, unbit, is distributed under the GNU General Public License, version 2 with Classpath Exception (gnu.org/software/classpath/license.html) ▪ UWSGI-PLUGIN-PYTHON V2.0.14, © 2016 anthon, unbit, is distributed under the GNU General Public License, version 2 with Classpath Exception (gnu.org/software/classpath/license.html)

Some third-party software included in Forcepoint Advanced Malware Detection On-Premises is licensed under the following open source license(s):

GNU General Public License with Classpath Exception

If you would like a copy of the source code for such third-party software included in Forcepoint Advanced Malware Detection On-Premises, you may email your request to opensource@forcepoint.com.