



Installation Guide

Advanced Malware Detection On-Premises Engine

v1.2.0

©2023 Forcepoint

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.

Published 2023

Every effort has been made to ensure the accuracy of this document. 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 document or the examples herein. The information in this documentation is subject to change without notice.

Last modified 15-June-2023

Contents

Chapter 1	Introduction	1
Chapter 2	Prerequisites	3
	Hardware	3
	Network connectivity	3
	License	4
	License extensions	4
Chapter 3	Installation Process	5
	Base system installation	5
	Registration and configuration	5
Chapter 4	System Administration	17
	Advanced Malware Detection On-Premises Engine installation wizard	17
	Error handling	17
Chapter 5	Software Upgrades	19
Chapter 6	Copyrights and Trademarks	21
	Copyrights and trademarks	21
	Other acknowledgments	21

1

Introduction

Installation Guide | AMD OP Engine | v1.2.0

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

The Advanced Malware Detection On-Premises Engine component receives artifacts (i.e., executables and documents) from the Advanced Malware Detection On-Premises Manager. It runs these artifacts, then returns analysis results back to the Advanced Malware Detection On-Premises Manager, which then displays results to the users.

The Engine is managed by the Manager. However, as an important part of the installation process, the Engine must be made known to the Manager.

2

Prerequisites

Installation Guide | AMD OP Engine | v1.2.0

Hardware

The Advanced Malware Detection On-Premises Engine 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
- 2x 1TB 7.2K RPM SATA disks (RAID 1)
- Dual PSU (highly recommended)
- ILO/LOM/DRAC (highly recommended)

Forcepoint also offers an option of purchasing dedicated hardware that is suitable for hosting the Advanced Malware Detection On-Premises Engine. Forcepoint delivers the server with the Advanced Malware Detection On-Premises Engine software already installed.

Network connectivity

The Advanced Malware Detection On-Premises Engine requires the following connections:

- log.<<MANAGER>> to TCP port 443
- update.<<MANAGER>> to TCP port 443 and 8443
- update.<<MANAGER>> to UDP port 1194
- update.<<MANAGER>> to UDP port 123 for time synchronization
This can be replaced with a local NTP server.
- user.<<MANAGER>> to TCP port 443.

Replace <<*MANAGER*>> with the Advanced Malware Detection On-Premises Manager's Fully Qualified Domain Name (FQDN).

All HTTPS connections (port 443) can be optionally routed through an explicit HTTP proxy.

License

Before starting the installation, contact Forcepoint Sales to purchase a license for the software.

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 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. After your request is processed, your license expiration date is automatically extended.

3

Installation Process

Installation Guide | AMD OP Engine | v1.2.0

The installation process for the Advanced Malware Detection On-Premises Engine consists of two steps:

1. Install the base system.
2. Collect and apply the basic configuration information to the system.

If you purchased dedicated hardware from Forcepoint with the Advanced Malware Detection On-Premises Engine software already installed, skip to [Registration and configuration](#), page 5. The base system has already been installed.

Base system installation

The Advanced Malware Detection On-Premises Engine uses Ubuntu 16.04 LTS as the underlying operating system. It uses an automated text-based installation process that eliminates the need for user input or a graphical user interface.

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

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

Registration and configuration

The Advanced Malware Detection On-Premises Engine appliance should be connected to the Advanced Malware Detection On-Premises Manager server's **eth1** port (2nd NIC). If there are multiple Advanced Malware Detection On-Premises Engines, a switch or private VLAN should be used to create a private network that connects to the Advanced Malware Detection On-Premises Manager's 2nd NIC. For

more information, see the [Advanced Malware Detection On-Premises Quick Start Guide](#).

To register and apply the software configuration to the Advanced Malware Detection On-Premises Engine, complete the following procedure:

1. Log on to the console using the following credentials:

- username: **lastline**
- password: **lastline**

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. Change the default password to a password that is unique to your organization.

2. Execute **forcepoint_register** to start the guided registration and configuration process.

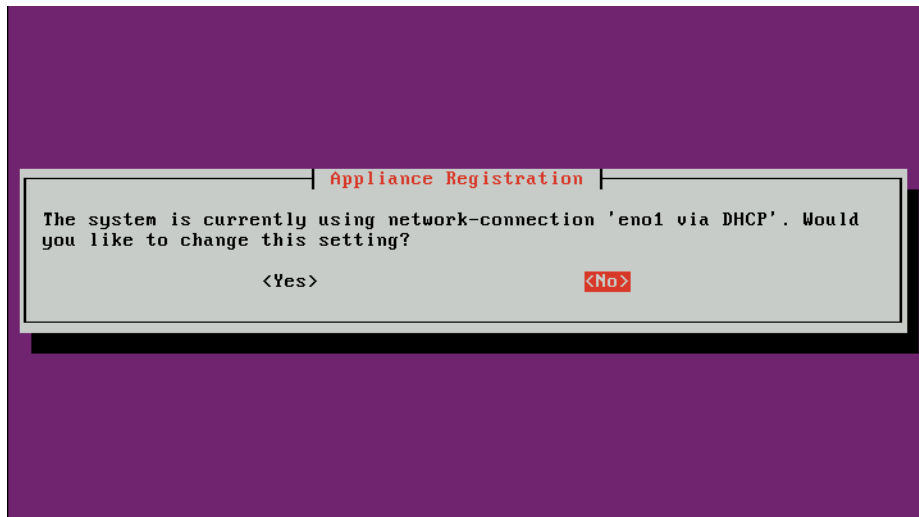
```
Ubuntu 14.04.5 LTS forcepoint-engine tty1
forcepoint-engine login: lastline
Password:
Last login: Fri Jul 14 21:21:11 UTC 2017 on tty1
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 3.13.0-123-generic x86_64)

 * To test the status of this appliance, please execute "forcepoint_test_appliance".

 * This appliance has not been registered yet, please execute "forcepoint_register".

lastline@forcepoint-engine:~$ forcepoint_register_
```

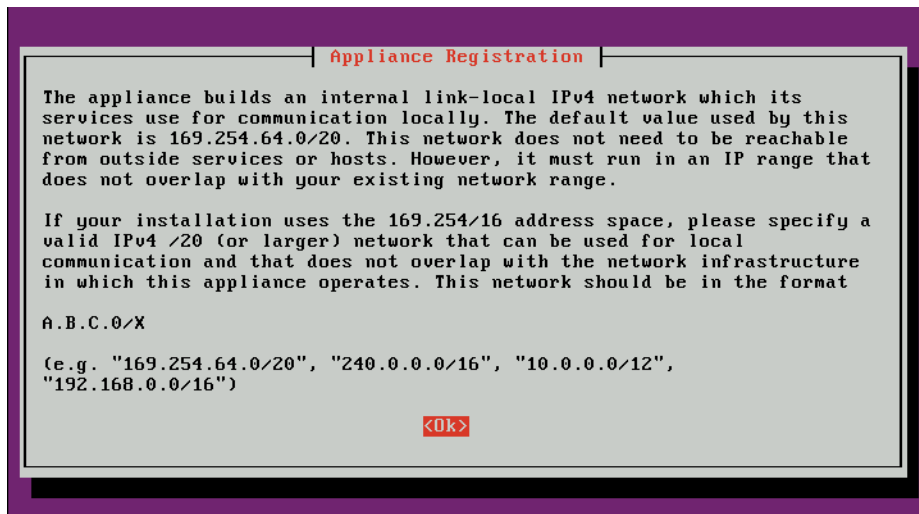
3. You can configure the network via DHCP (**Obtain via DHCP**) or with a static IP address (**Enter static address**).



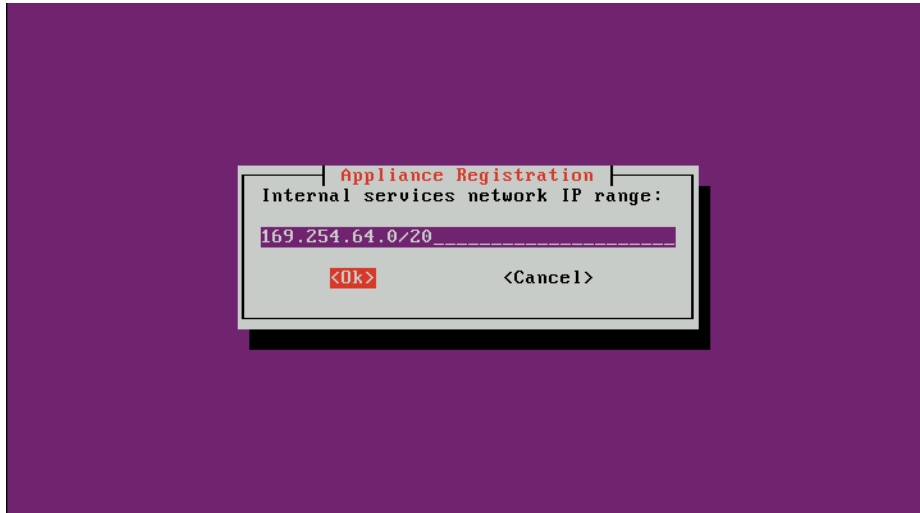
Forcepoint strongly recommends the use of DHCP. An IP in the range of 10.0.0.200-254 will be assigned to each Advanced Malware Detection On-Premises Engine on the private engine network. The Advanced Malware Detection On-Premises Engines will obtain IPs via DHCP from the Advanced Malware Detection On-Premises Manager over the engine network.

If static IPs are issued, use the 10.0.0.11-199 range.

4. On the next screen, read the information regarding the required internal link-local IPv4 network and click **Ok**.



5. On the next screen, click **Ok** to accept the default internal services network IP range, or make changes as needed and then click **Ok**.



If an Advanced Malware Detection On-Premises Manager has been installed in the network, the user has to specify its domain name. For example, if the domain name of the Advanced Malware Detection On-Premises Manager is **amd-manager.mycompany.com**, then this name should be provided.

Note that, as part of the installation of the Advanced Malware Detection On-Premises Manager, the names

update.amd-manager.mycompany.com

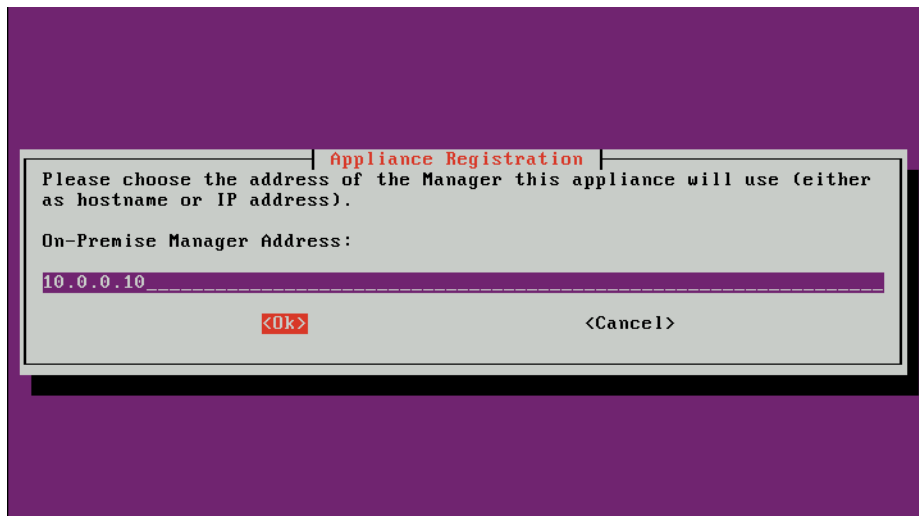
log.amd-manager.mycompany.com

user.amd-manager.compan.y.com

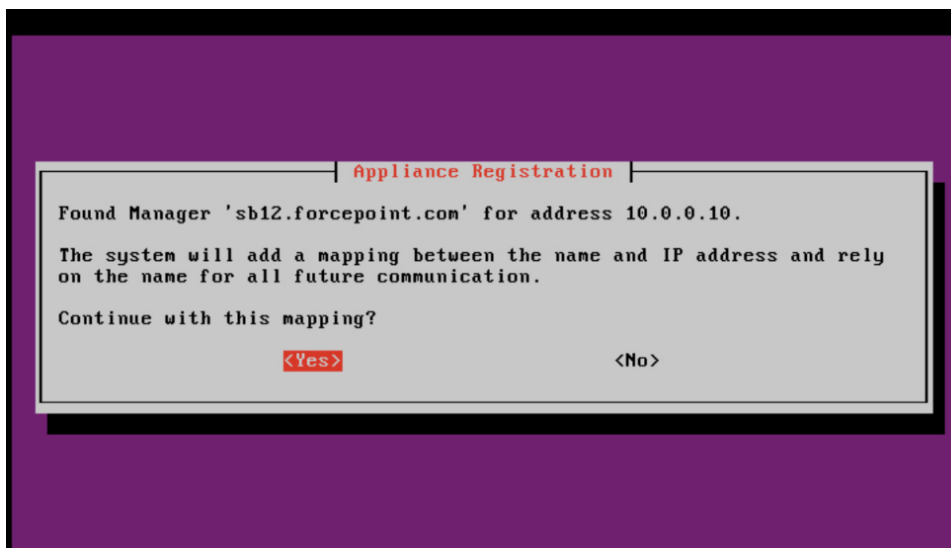
should have also been registered as aliases of **amd-manager.mycompany.com**.

In case an Advanced Malware Detection On-Premises Manager has been installed in the network, but no FQDN has been assigned to it (or the DNS server is not able to resolve its domain name), then the IP address of the Manager can be provided to the installer, as shown below.

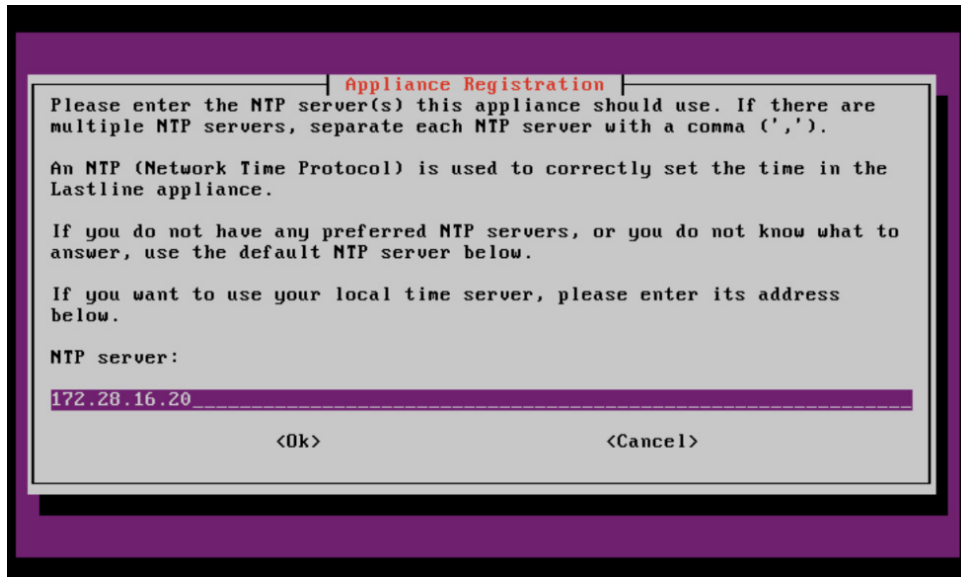
6. The Advanced Malware Detection On-Premises Manager's IP address has automatically been assigned to **10.0.0.10**. Type this address when prompted for the On-Premises Manager Address.



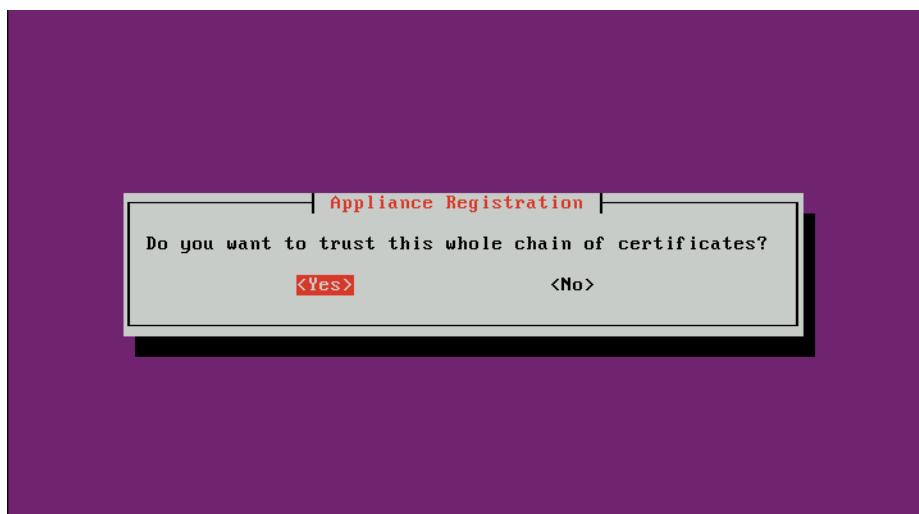
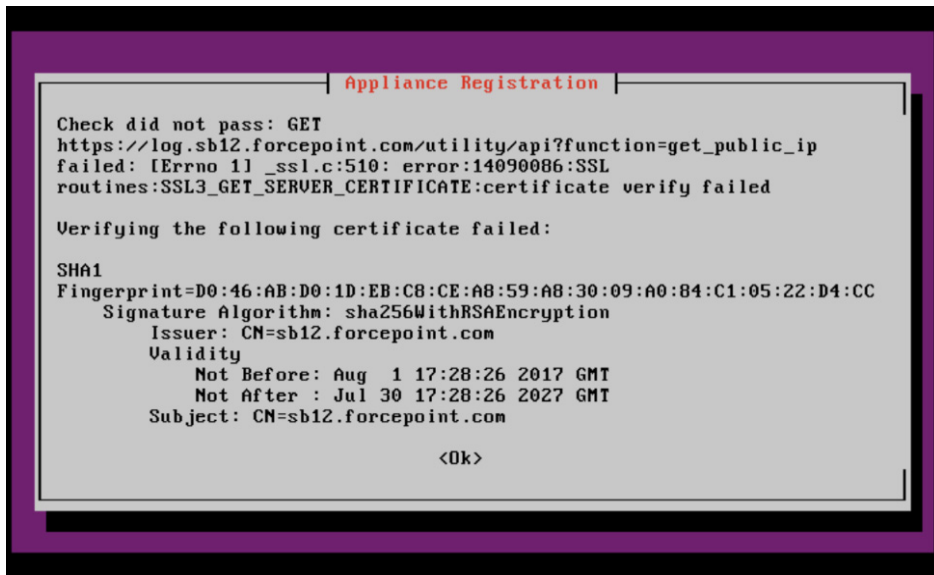
7. Select **Yes** to configure the Advanced Malware Detection On-Premises Engine by using the IP address of the Advanced Malware Detection On-Premises Manager.



8. Type the IP address or FQDN for the NTP server, then select **Ok**. 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.



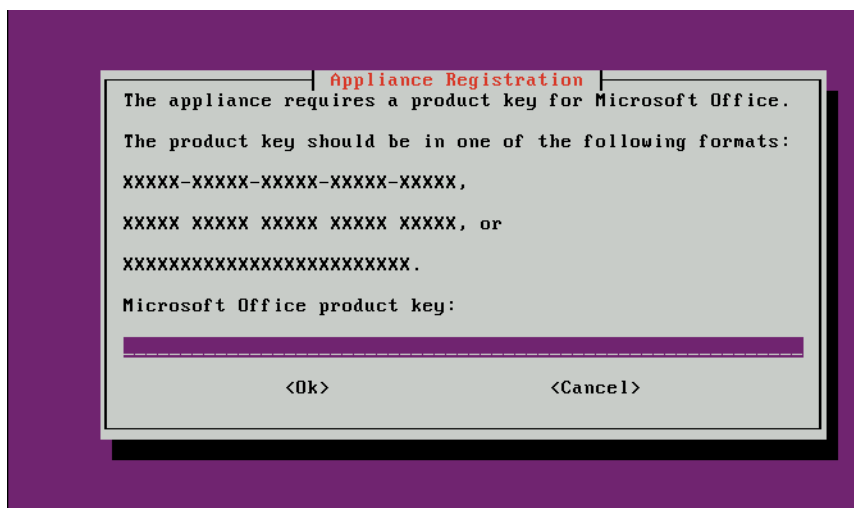
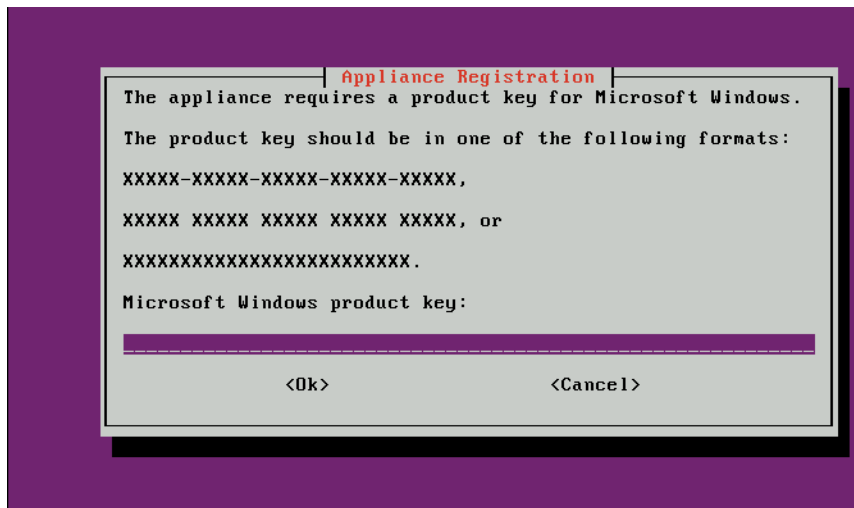
9. You may see a certificate error page similar to the screen below:



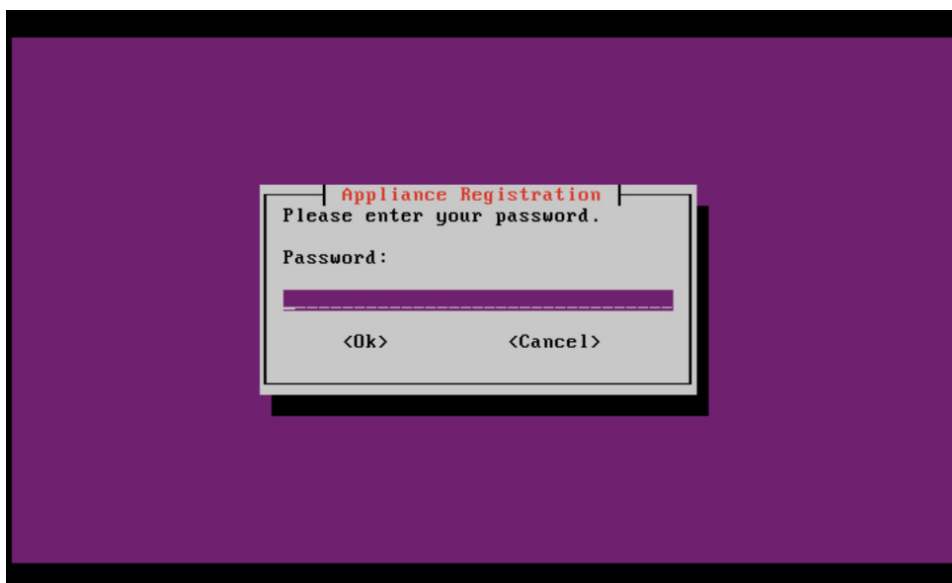
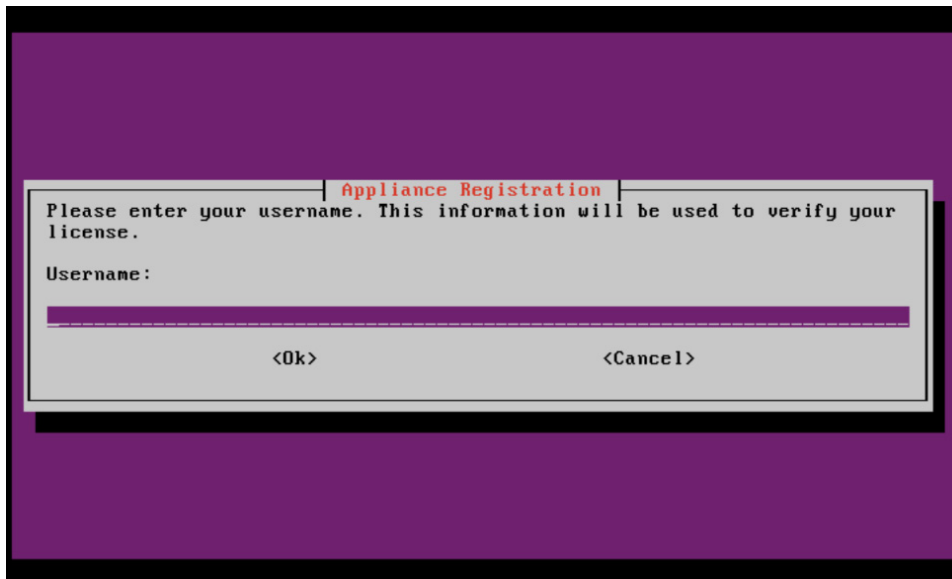
Select **Ok** on this screen, then **Yes** on the next screen when asked to trust the certification. Verifying that the certificate failed does not negatively impact the Advanced Malware Detection On-Premises Engine registration process.

10. The Engine uses Microsoft Windows operating systems and Microsoft Office applications in the sandbox to perform its analysis of potentially malicious downloads and attachments. You are required to have valid Product Keys for

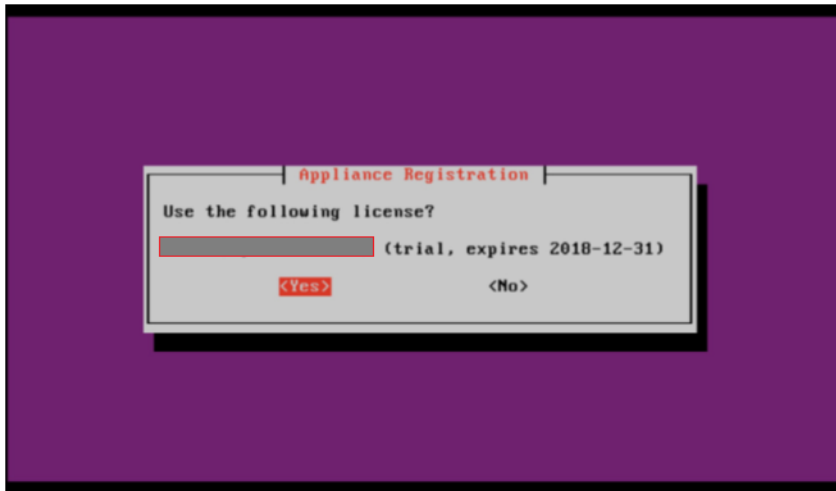
Windows and Office before you can complete the registration of the Engine and required to ensure the validity of your license. Therefore the registration process prompts you for these Product Keys.



11. Type the username and password provided during registration. Click **Ok**.



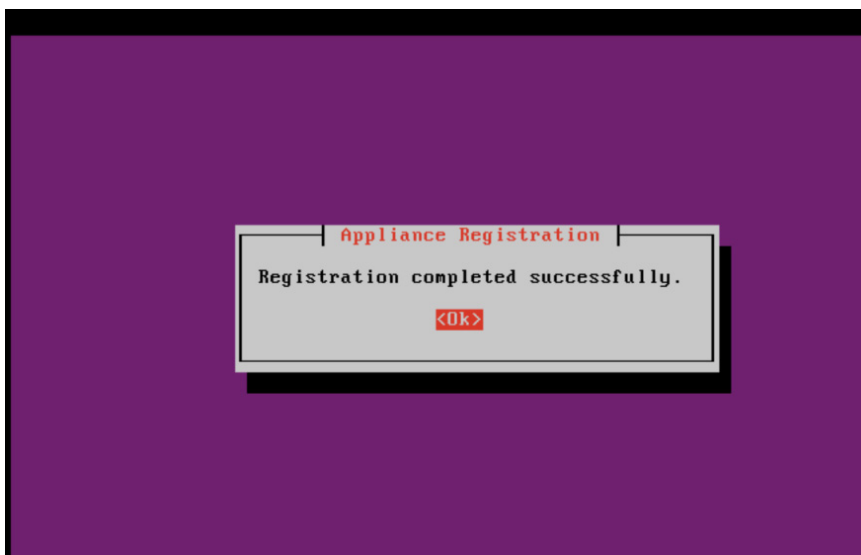
12. If the provided credentials are valid, you are shown the available license keys. If the list of license keys is not retrieved correctly, please contact Forcepoint Support, mentioning the corresponding error message.



If the license information is correct, select **Yes**.

If you select **No**, you are asked if you want to restart the configuration process. Select **Yes** to restart the configuration, or **No** to stop the configuration process.

13. Verify your readiness to complete the configuration process. Select **Yes** to begin the system configuration and product registration. Internet access is required to complete the rest of the registration process. The setup program applies the configuration to the machine. This process may take several minutes (20 – 40) depending on network connectivity and system characteristics.



Upon completion of registration and configuration, users can access the user portal:

<https://<<IP address of AMD Manager>>> or <https://<<assigned FQDN>>>

If any error message is displayed, please refer to [Error handling](#), page 17.

4

System Administration

Installation Guide | AMD OP Engine | v1.2.0

The Advanced Malware Detection On-Premises Engine 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.

See the [Advanced Malware Detection On-Premises Troubleshooting Guide](#) for additional information.

Advanced Malware Detection On-Premises Engine installation wizard

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

```
forcepoint_register
```

Then, you can change the configuration values provided the last time the installation wizard ran.

Error handling

If any error message is shown, please contact [Forcepoint Support](#).

5

Software Upgrades

Installation Guide | AMD OP Engine | v1.2.0

Forcepoint periodically releases appliance and software upgrades or hotfixes.

If the software has automatic updates enabled, these updates are transparently 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.

6

Copyrights and Trademarks

Installation Guide | AMD OP Engine | v1.2.0

Published 2023

Printed in the United States of America

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

© 2023 Forcepoint. This document may not, in whole or in part, be reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Forcepoint.

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.

Other acknowledgments

This Forcepoint product uses the third-party software listed in [this file](#).

