Linux Defender MDE Installation Guide

7th September 2021 v3.0

Shane Clarke, Bilal Hassan

Contents

[Executive Summary 3](#_Toc89994783)

[Prerequisites 3](#_Toc89994784)

[System Requirements 3](#_Toc89994785)

[Manual Installation Overview 4](#_Toc89994786)

[Installation process 4](#_Toc89994787)

[Configuring the Linux software repository 4](#_Toc89994788)

[Application installation 4](#_Toc89994789)

[Verifying the onboarding package 4](#_Toc89994790)

[Client Configuration 4](#_Toc89994791)

[Deploying Defender MDE for Linux via Ansible 5](#_Toc89994792)

[Prerequisites and system requirements 5](#_Toc89994793)

[Installation process 5](#_Toc89994794)

[Verifying the onboarding Package 5](#_Toc89994795)

[Create Ansible YAML files 5](#_Toc89994796)

[Deployment 5](#_Toc89994797)

[Deploying Defender MDE for Linux via Puppet 6](#_Toc89994798)

[Prerequisites and system requirements 6](#_Toc89994799)

[Installation process 6](#_Toc89994800)

[Verifying the onboarding Package 6](#_Toc89994801)

[Create a Puppet manifest 6](#_Toc89994802)

[Deployment 6](#_Toc89994803)

[Monitor Puppet Deployment 6](#_Toc89994804)

[Check onboarding status 6](#_Toc89994805)

[References 7](#_Toc89994806)

# Executive Summary

Defender MDE provides the same functionality as the current WPP wide deployed Security Center integration using the Microsoft Monitoring Agent, but also offers several other beneficial security features.

Defender MDE should be the only endpoint protection product running on the device. Running third-party endpoint protection products alongside Defender MDE is likely to cause performance problems and unpredictable system errors.

Defender MDE for Linux can be deployed via two methods:

* The command-line tool:
  + Manual Deployment
* Third-party management tools:
  + Deployment using the Puppet configuration management tools
  + Deployment using Ansible configuration management tools
  + Deploy using Chef configuration management tools

## Prerequisites

* Beginner-level experience in Linux and Bash scripting
* Administrative privileges on the device for manual deployment

## System Requirements

* Supported Linux server distributions and versions
  + Red Hat Enterprise Linux 7.2 or higher
  + CentOS 7.2 or higher
  + Oracle Linux 7.2 or higher
  + Ubuntu 16.04 LTS or higher LTS
  + Debian 9 or higher
  + SUSE Linux Enterprise Server 12 or higher
* Minimum Kernel version 3.10.0-327
* The *fanotify* kernel option must be enabled

Caution: Running Microsoft Defender MDE for Linux side by side with other *fanotify*-based security solutions is not supported. It can lead to unpredictable results, including hanging the operating system.

* Cores: 2 minimum, 4 preferred
* Memory: 1GB minimum, 4 preferred
  + Make sure you have free disk space in /var
* Real time protection for the file system types can be found [here](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint-linux?view=o365-worldwide).

Network or firewall configuration may be required to allow outbound connections between Defender MDE and the endpoints. [Further info can be found here.](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-linux#network-connections)

TVM (Threat and Vulnerability Management) is now available on Linux. More information can be found [here](https://www.microsoft.com/security/blog/2021/05/11/threat-and-vulnerability-management-now-supports-all-major-platforms/).

# Manual Installation Overview

Dependant on the operating system will determine the required steps and commands required to deploy Defender MDE.

Important: If you plan on updating the operating system to a new version, you will be required to first uninstall Microsoft Defender MDE for Linux, and will need to reconfigure Defender MDE.

## Installation process

1. Configure the Linux software repository
2. Application Installation
3. Verifying the onboarding package
4. Client Configuration

## Configuring the Linux software repository

For all Operating Systems, the installation will require a channel to be picked determining the type and frequency of updates that will apply to the device.

* Insiders Fast (First device to receive updates and new features)
* Insiders Slow (Second group of devices to receive updates and new features)
* Prod (Third group of devices to receive updates and new features)

Warning: Switching the channel after the initial installation requires the product to be reinstalled. To switch the product channel: uninstall the existing package, re-configure your device to use the new channel, and follow the steps in this document to install the package from the new location.

Commands to configure the Linux software repository can be found below.

* [RHEL and variants (CentOS and Oracle Linux)](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-manually#rhel-and-variants-centos-and-oracle-linux)
* [SLES and variants](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-manually#sles-and-variants)
* [Ubuntu and Debian Systems](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-manually#ubuntu-and-debian-systems)

## Application installation

Depending on the configuration of the device, you may have multiple Microsoft repositories configured on the end-point. Microsoft allows you to specify which repository you would like to install the package from.

[Commands and details can be found here.](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-manually#application-installation)

## Verifying the onboarding package

WPP Information Security team will provide the onboarding package ([WindowsDefenderATPOnboardingPackage.zip](https://wppcorp.sharepoint.com/sites/SecurityIntegration/Shared%20Documents/Forms/AllItems.aspx?viewid=dfde57c9%2De433%2D4660%2Daa41%2D741f62d23993&id=%2Fsites%2FSecurityIntegration%2FShared%20Documents%2FDefender%20ATP%2FLinux%20Server)), from here you will need to extract the contents of the archive.

[The commands for this process can be found here.](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-manually#download-the-onboarding-package)

## Client Configuration

The final step is to configure the endpoint to the WPP Organisation. This can be completed by following the commands provided by Microsoft.

[Commands for client configuration.](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-manually#client-configuration)

# Deploying Defender MDE for Linux via Ansible

Important: If you plan on updating the operating system to a new version, you will be required to first uninstall Microsoft Defender MDE for Linux, and will need to reconfigure Defender MDE.

## Prerequisites and system requirements

Ansible requires further Prerequisites and system requirements to be achieved for a successful deployment.

[Full details can be found here detailing the requirements.](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-with-ansible#prerequisites-and-system-requirements)

## Installation process

1. Verifying the onboarding Package
2. Create Ansible YAML files
3. Deployment

## Verifying the onboarding Package

WPP Information Security team will provide the onboarding package ([WindowsDefenderATPOnboardingPackage.zip](https://wppcorp.sharepoint.com/sites/SecurityIntegration/Shared%20Documents/Forms/AllItems.aspx?viewid=dfde57c9%2De433%2D4660%2Daa41%2D741f62d23993&id=%2Fsites%2FSecurityIntegration%2FShared%20Documents%2FDefender%20ATP%2FLinux%20Server)), from here you will need to extract the contents of the archive.

[The commands for this process can be found here.](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-manually#download-the-onboarding-package)

## Create Ansible YAML files

You will need to create a subtask or role files that contribute to a playbook or task.

[Full details and commands can be found here.](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-with-ansible#create-ansible-yaml-files)

## Deployment

Please follow Microsoft documentation detailing the steps required to deploy Defender MDE.

[Deployment guide.](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-with-ansible#deployment)

# Deploying Defender MDE for Linux via Puppet

Important: If you plan on updating the operating system to a new version, you will be required to first uninstall Microsoft Defender MDE for Linux, and will need to reconfigure Defender MDE.

## Prerequisites and system requirements

Puppet will require you to be familiar with Puppet administration tasks, have puppets configured, and know how to deploy packages.

[More details can be found here detailing the requirements.](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-with-puppet" \l "prerequisites-and-system-requirements)

## Installation process

1. Verifying the Onboarding Package
2. Create a Puppet manifest
3. Deployment
4. Monitor Puppet Deployment
5. Check Onboarding status

## Verifying the onboarding Package

WPP Information Security team will provide the onboarding package ([WindowsDefenderATPOnboardingPackage.zip](https://wppcorp.sharepoint.com/sites/SecurityIntegration/Shared%20Documents/Forms/AllItems.aspx?viewid=dfde57c9%2De433%2D4660%2Daa41%2D741f62d23993&id=%2Fsites%2FSecurityIntegration%2FShared%20Documents%2FDefender%20ATP%2FLinux%20Server)), from here you will need to extract the contents of the archive.

[The commands for this process can be found here.](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-manually#download-the-onboarding-package)

## Create a Puppet manifest

You will need to create a puppet manifest for deploying Defender MDE to devices managed by a puppet server.

[Full details and commands can be found here.](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-with-puppet" \l "create-a-puppet-manifest)

## Deployment

Please follow Microsoft documentation detailing the steps required to deploy Defender MDE.

[Deployment guide.](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-with-puppet#deployment)

## Monitor Puppet Deployment

You can check the onboarding status on the agent device by running a few commands.

[Onboarding Status Commands.](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-with-puppet" \l "monitor-puppet-deployment)

## Check onboarding status

Please confirm the devices have been onboarded correctly, this can be checked by creating a script.

Script details.

# References

* [Microsoft Defender ATP for Linux.](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-linux#network-connections)
* Deploy Microsoft Defender MDE for Linux Manually [installation guide.](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-manually#configure-the-linux-software-repository)
* Deploy Microsoft Defender MDE for Linux via Ansible [installation guide.](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-with-ansible)
* Deploy Microsoft Defender MDE for Linux via Puppet [installation guide](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-with-puppet).
* For installation issues please follow Microsoft guidance regarding the steps to find the log details. [Log installation Issues.](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-install-manually#log-installation-issues)
* For uninstallation please follow Microsoft guidance [uninstallation Guide.](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/linux-resources#uninstall)
* TVM [Supported OS platforms](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/tvm-supported-os?view=o365-worldwide) and [supporting all major platforms](https://www.microsoft.com/security/blog/2021/05/11/threat-and-vulnerability-management-now-supports-all-major-platforms/)