ESET Tech Center

Where can I find the diagnostic program?

Anish | ESET Nederland - 2021-06-11 - Reacties (0) - Diagnostics

Issue

- You have been asked to generate a log using the diagnostic utility.

Solution

Running the Diagnostics Utility

The diagnostics utility gathers information about ESET Endpoint Encryption and ESET Full Disk Encryption that can not be obtained if you run it in another user context.

1. Login to Windows as the user experiencing the problem.
2. Click the following link to download the diagnostics utility: ESET Endpoint Encryption Diagnostics Utility

Download the tool each time

You should always download the tool before running it to ensure that you have the latest version. Even if you have previously downloaded the tool, it may have been updated since your initial download.

Version	Last Updated	SHA256 Hash
3.4.0.105	13/08/2019	772aa9589e5bcf7b0a30f58d0e8f7f98a8476512f99358668adb1795e199e071

1. Run the diagnostics utility.
2. Click **Next**.

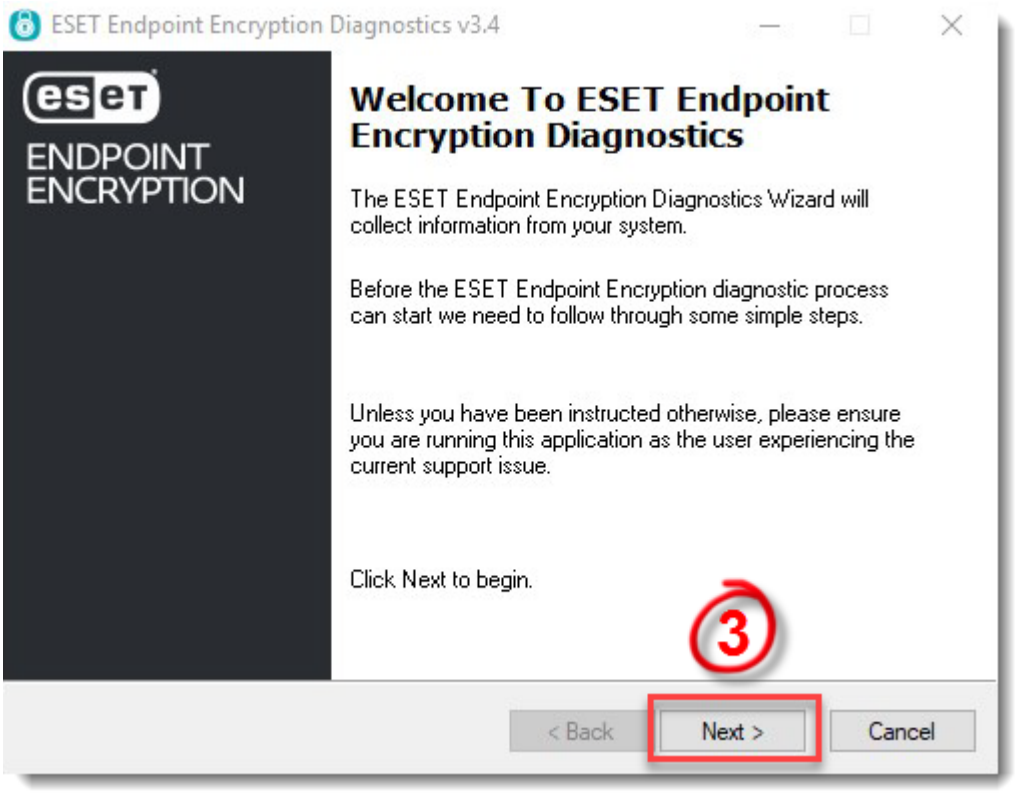

Figure 1-1

1. The diagnostics utility will collect the necessary information.

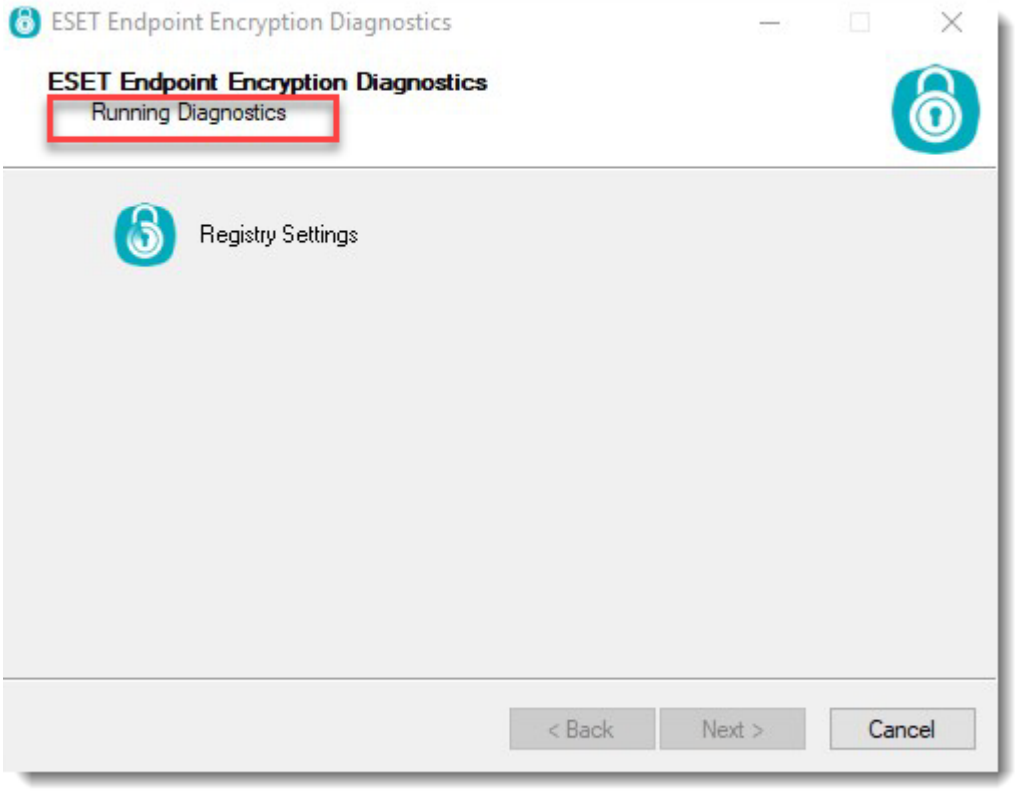

Figure 1-2

1. While collecting information, the diagnostics utility will attempt to elevate to gather additional information.
    1. **Users with Administrator rights**: Click **Yes** to accept the UAC prompt.

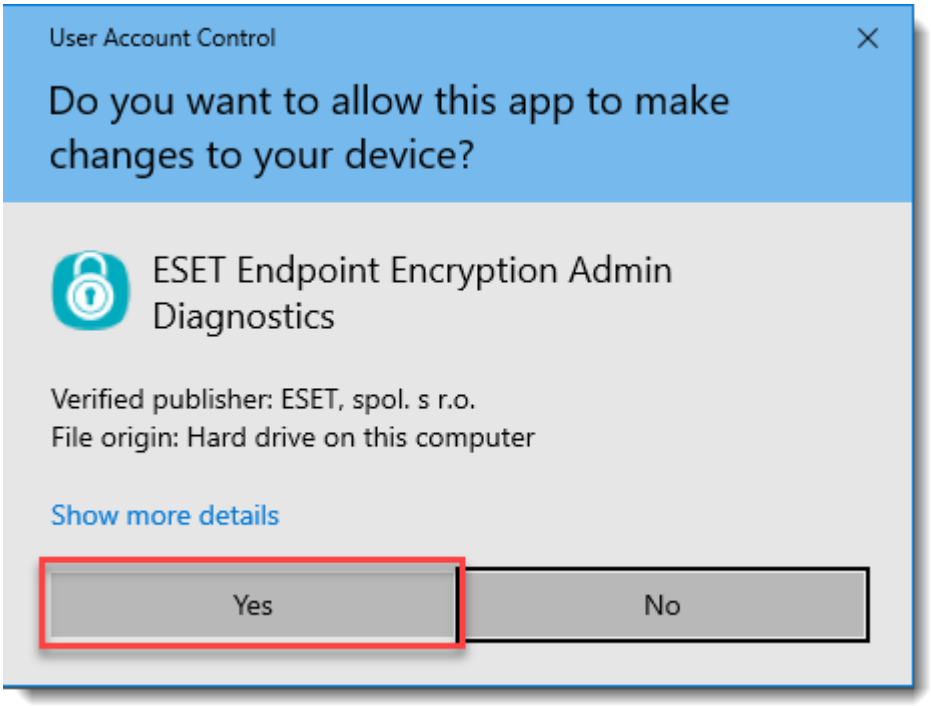

Figure 1-3

1. **Users without Administrator rights**: Click **OK** and enter Administrator credentials when prompted.

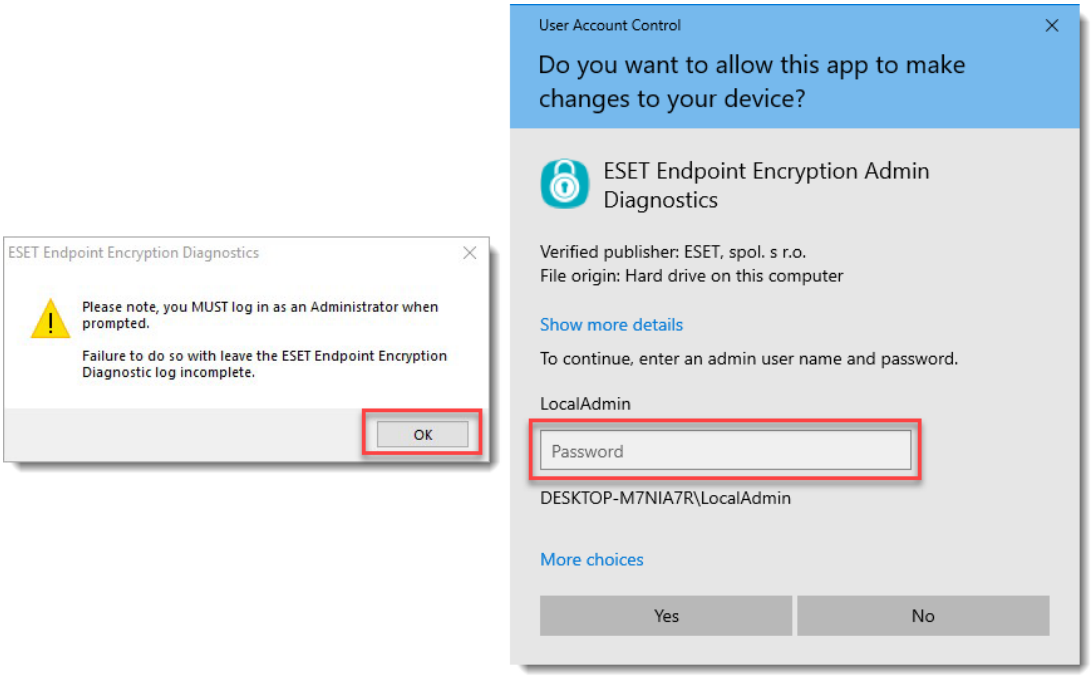

Figure 1-4

1. **Unable to run with Administrator rights**: If it is not possible to elevate the diagnostics utility, then additional information may be requested.
   Click **No** to skip the Administrative component. If you entered the credentials incorrectly, click **Yes** and enter them again.

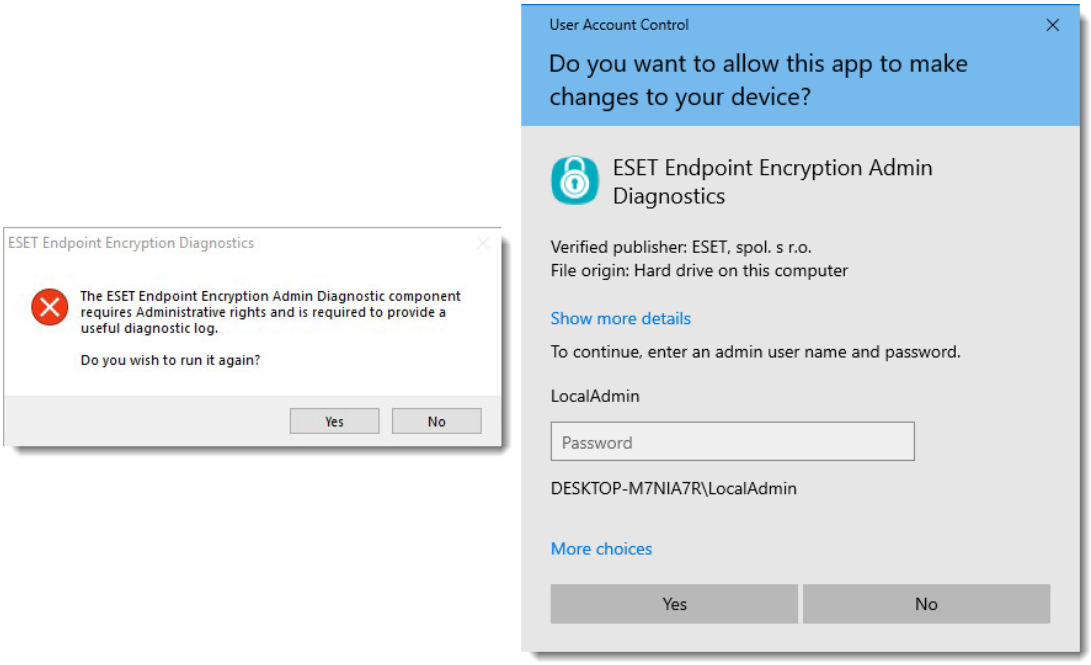

Figure 1-5

1. The Admin activity window will now run. The diagnostics utility searches the system for specific EEE and EFDE files. It does not read, catalog, analyze or store anything relating to other files, unless if they are **.dat** files. In these instances, the file will be read to determine if it matches our specific header and ignored otherwise.

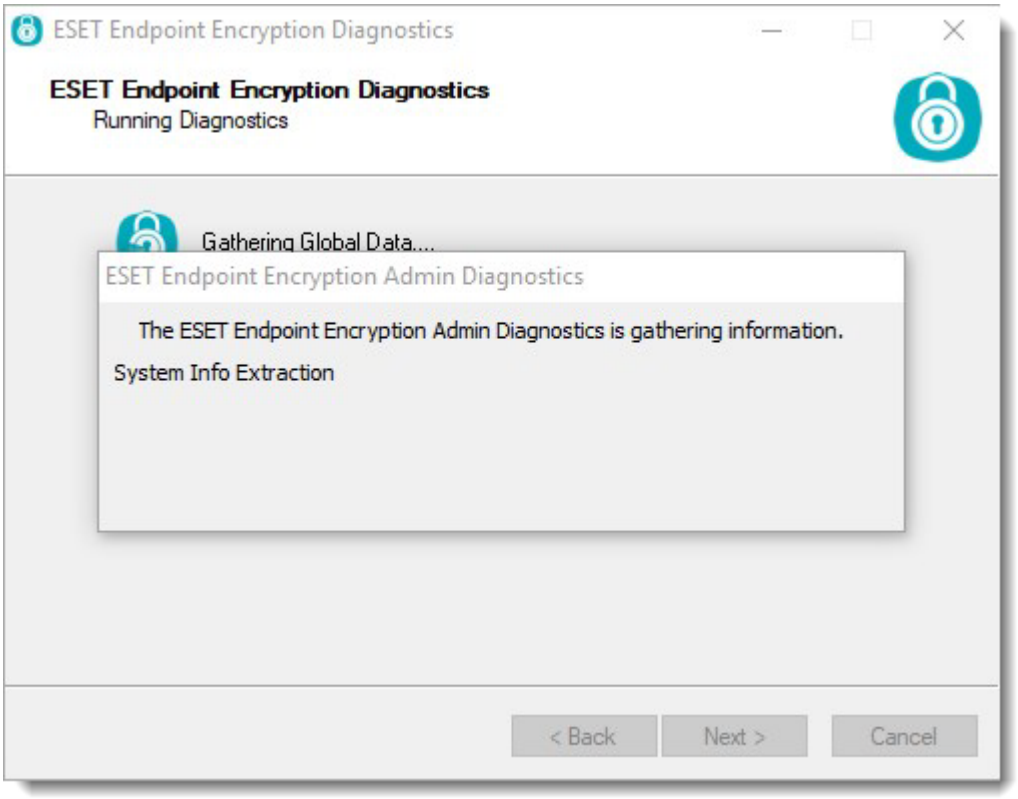

Figure 1-6

1. Once the diagnostics utility has completed, a .zip file will be created on the Desktop with a filename beginning **eediag_log** followed by the current time and date in UTC format.

Figure 1-7

About the Diagnostics Utility

The diagnostics utility gathers information about the machine's configuration and the user's settings. Information regarding the machine's Full Disk Encryption and the server cloud packets are kept in an encrypted state, which are inaccessible by anyone outside of your organization.

As of Version 3.3.0.88 and later, the following files may appear in the ZIP file:

Filename	Purpose	Presence
admin_log.txt	Contains information gathered via the Administrative component, locations of software files, Key-Files, active processes, driver information and disk information	Always (Admin)
blat_log.txt	Contains information related to upgrade processes used during installation and upgrades	Always
current_dlploy.txt	Contains logging information about cloud communications within a managed environment	Managed
dlpcrashdumps.txt	Contains information about any components that have generated crash dumps	Always
eediag_log_ _.txt	Contains information gathered whilst running in the User context, including current Key-File state and some system information	Always
evt_application.txt	Contains recent entries in the machines Application event log	Always
evt_crash.txt	Contains a log of all application crashes recorded in the Application event log	Always
evt_deslock.txt	Contains recent entries in the machines Endpoint Encryption event log	Always
evt_power.txt	Contains a log of power events, start up, shutdown and power interruptions	Always
evt_system.txt	Contains recent entries in the System event log	Always
SafeStart.txt	Contains information reported by FDE Safe Start, if it was used	Always
Services.txt	Contains information about all currently installed Services	Always
sysinfo.txt	Contains information that is normally sent back to an Enterprise Server	Always
system.nfo	Contains an export from MSInfo32, a Microsoft system information tool	Always (Admin)
update_db.xml	Contains encrypted copies of updates and responses when is used in a managed environment	Managed
x_dlploadr.bin	Contains the FDE meta data, where x will be the drive letter the file was found on	FDE Encrypted

Filename	Purpose	Presence
_dlploy.txt	Contains logging information about cloud communications within a managed environment, one for each user profile found	Managed (Admin)
_esdirect.txt	Contains logging information for the auto-enrollment feature in a managed environment, one for each user profile found	Managed (Admin)
efde_ais_	Contains logging information for the EFDE service	EFDE Only
Status	Contains information in relation to the current EFDE status	EFDE Only

Please do not modify the contents of the ZIP file.