FORCEPOINT

POWERED BY Raytheon

Executable List Tool Guide

Forcepoint Endpoint Context Agent

10900-A Stonelake Blvd, Quarry Oaks 1, Suite 350, Austin, TX 78759, USA

Published 2018

Contents

1 Using the Executable List Tool

ECA | 24-May-2018

The Executable List Tool scans an endpoint machine and generates a list of all installed executable files. The list is then used by the Forcepoint Next Generation Firewall (Forcepoint NGFW) to identify the permitted executables.

The Executable List Tool creates an XML file that contains the following information:

- Executable file name/product name for all .exe files
- Hash combinations (MD5 or SHA256)

The Executable List Tool must be run on a new endpoint machine to establish a baseline list of executable files. After the Executable List Tool creates the XML file, the XML file is imported into the Forcepoint NGFW Security Management Center (SMC). The SMC then distributes the list of executables to the NGFW Engine on which the Forcepoint Endpoint Context Agent (Forcepoint ECA) has been configured. Forcepoint ECA is a client application monitoring tool installed on the endpoint machine. Forcepoint ECA continually sends information about the endpoint machine to Forcepoint NGFW, including information about installed and accessed executable files.

When a connection is established between Forcepoint NGFW and an endpoint machine running Forcepoint ECA, Forcepoint NGFW collects the application information, then permits connections only from the applications on the list.

For more information about Forcepoint ECA, see the *Forcepoint Endpoint Context Agent Release Notes* and *Forcepoint Endpoint Context Agent Installation and Deployment Guide* on the Forcepoint Documentation site.

You must run the Executable List Tool on each endpoint machine. However, it is only necessary to run the Executable List Tool when there are significant changes on the endpoint machine (for example, when the endpoint machine has just been created or when the endpoint machine has been updated).

Obtaining the Executable List Tool

The Executable List Tool (FileInfoExtract.exe) is available from the Forcepoint Downloads website. You must log on with your Forcepoint My Account credentials.

On the Downloads website, navigate to the **Network Security** section, select the version under NGFW ECA Client for Windows, then select and download the Executable List Tool.

Checking file integrity

Before running the Executable List Tool from the downloaded file, check that the file has not become corrupt or been changed.

Using a corrupt file might cause problems when running the tool. Check file integrity by generating a file checksum of the file. Compare the checksum of the downloaded file with the checksum for the software version in the Forcepoint Endpoint Context Agent Release Notes or on the Downloads page at the Forcepoint website.

> ✓ **Note**
> Windows does not have checksum tools by default, but there are several third-party programs available.

1. Look up the correct checksum at https://support.forcepoint.com.
2. Change to the directory that contains the file to be checked.
3. Generate a checksum of the file using one of the following commands, where filename is the name of the installation file:
   - sha1sum filename
   - sha256sum filename
4. Compare the displayed output to the checksum for the software version. They must match.

> ⚠ **Warning**
> Do not use a file that has an invalid checksum. If downloading the file again does not help, contact Forcepoint support to resolve the issue.

Generating the file list

Run the Executable List Tool on the end user’s endpoint machine before the user obtains the machine, or when the endpoint machine is updated.

1. Copy FileInfoExtract.exe to the top directory where the application list is to be generated. For example, if you run FileInfoExtract.exe from the C:/ directory, it extracts the needed information from the C:/ directory and all subdirectories.
2. Run FileInfoExtract.exe from the command line:
   a. Open a terminal window.

   b. Change to the directory containing FileInfoExtract.exe.

   c. Type the following command with no arguments:

   ```
   FileInfoExtract.exe
   ```

3. The Executable List Tool runs and collects the .exe information for all applications within the directory and its subdirectories.
4. When the process is complete, the Executable List Tool creates a file called filelist.xml in the directory where FileInfoExtract.exe is located. The filelist.xml file contains the application information to be imported into the SMC.
5. Import the filelist.xml file into the SMC. See the Forcepoint Next Generation Firewall Product Guide for more information about loading filelist.xml.