



Release Notes

Forcepoint Endpoint Context Agent

Contents

About this release, page 2

System requirements, page 3

Build version, page 3

Product binary checksums, page 3

Compatibility, page 4

New features, page 4

Resolved issues, page 4

Installation instructions, page 5

Upgrade instructions, page 6

Known issues, page 6

Find product documentation, page 6

About this release

This document contains important information about the current Forcepoint Endpoint Context Agent (Forcepoint ECA) release. We strongly recommend that you read the entire document.

Forcepoint ECA is a client application monitoring tool. It intercepts network system calls on Windows endpoint machines and provides user and application information to the Forcepoint Next Generation Firewall (Forcepoint NGFW).

You can use the Executable List Tool together with Forcepoint ECA and the Forcepoint NGFW. You first use the Executable List Tool to generate a list of executables on endpoint machines, then use the list of executables in the Forcepoint NGFW to identify permitted executable files on the endpoint machines.



Note

The Executable List Tool is a stand-alone tool. It is not included in the Forcepoint ECA installation package.

For detailed information about running the Executable List Tool, see the *Forcepoint Endpoint Context Agent Executable List Tool Guide*. This guide is available for download at <https://support.forcepoint.com>.

System requirements

Endpoint machine requirements:

- Windows 10
 - x64 and 86 (Pro and Enterprise)
- Win 8/8.1 with [KB2999226](#)
 - x64 and 86 (Pro and Enterprise)
- Win 7 SP1 with [KB3033929](#) and [KB2999226](#)
 - x64 and 86 (Pro, Enterprise, and Ultimate)
- Citrix XenDesktop 7.14

Windows Server requirements:

- Windows Server 2012
- Windows Server 2016

For more information, see the [Forcepoint Endpoint Context Agent Product Matrix](#).

Build version

The Forcepoint ECA for Windows build version is 6063.

Product binary checksums

Use the checksums to make sure that the installation files downloaded correctly.

ECA_Client-1.4.6063.zip

SHA1SUM:

34987f9609113203722fdf1c905aa9eae17d7793

SHA256SUM:

33ad10d2d449369da92485c8ac958c98563d603712f78ee634e7d42a8e6eec90

Compatibility

Forcepoint ECA is recommended for use with these Forcepoint NGFW component versions.

Component	Minimum compatible version	Recommended version
Forcepoint Next Generation Firewall (Forcepoint NGFW)	6.3.0	Latest 6.5.x maintenance version or newer
Forcepoint NGFW Security Management Center (SMC)	6.3.0	Latest 6.5.x maintenance version or newer

New features

There are no new features for the Forcepoint Endpoint Context Agent or Executable List Tool in this release.

Resolved issues

These issues are resolved in this release of the product.

Description	Issue number
The text might overlap in the Forcepoint Endpoint Context Agent Installation Wizard.	UEP-11169
For network connections produced by the SYSTEM process, the Forcepoint Endpoint Context Agent shows “SYSTEM” in the “Executable File” metadata, but does not show other metadata.	UEP-11398
The Forcepoint Endpoint Context Agent only resolves the user’s domain name through a DNS query. The domain name might not be shown if the DNS query is delayed.	UEP-19604
The SMC logs might not show the “Executable Signer” value even if it is collected from the Forcepoint Endpoint Context Agent client.	UEP-22980
The Forcepoint Endpoint Context Agent does not read or send group information to Forcepoint NGFW.	UEP-25745
The Forcepoint Endpoint Context Agent might not be able to communicate with Forcepoint NGFW. The following message appears in the log file: “Connection severed: CORRUPTION”.	UEP-26302

Description	Issue number
The Forcepoint Endpoint Context Agent leaks Windows resources, which produces a large number of handles for the FpEcaSvc.exe process.	UEP-26441
The Forcepoint Endpoint Context Agent stops responding after the endpoint machine allows 255 logons without a restart.	UEP-27400

Installation instructions

Use these high-level steps to configure Forcepoint ECA in the SMC, then install the Forcepoint ECA client software on the endpoint machines.

For complete installation instructions for Forcepoint ECA, see the *Forcepoint Endpoint Context Agent Installation and Deployment Guide*.

For detailed information about running the Executable List Tool, see the *Forcepoint Endpoint Context Agent Executable List Tool Guide*.

All guides are available for download at <https://support.forcepoint.com>.

Configure Forcepoint ECA settings in the SMC

For information about configuring the Forcepoint ECA in the SMC, and about exporting the Forcepoint ECA configuration file from the SMC, see the *Integrating Endpoint Context Agent* chapter in the *Forcepoint Next Generation Firewall Product Guide*. This guide is available for download at <https://support.forcepoint.com>.

1. In the Management Client component of the SMC, establish a certificate authority (CA) for the Forcepoint ECA client. Forcepoint ECA uses the customer-provided CA to authenticate the endpoint machine and uses the SMC internal CA to authenticate the NGFW Engines.
2. After the CA is established for the Forcepoint ECA client, create a new client certificate in AD CS and deploy it to the endpoint machines where Forcepoint ECA is to be installed. The **Client Authentication** application policy must be enabled.
3. In the Management Client, configure ECA for the NGFW Engines.
4. In the Management Client, export the Forcepoint ECA configuration XML file (eca_client_yyyymmdd_hhmmss.xml). You must copy this file to the installation folder before you install the Forcepoint ECA client software on the endpoint machines, as described in the next section [Install the Forcepoint ECA client on the endpoint machines](#), page 6.

The configuration file contains the details of all the NGFW Engines that use the same Forcepoint ECA Configuration element. If additional NGFW Engines are added to the Forcepoint ECA configuration, the updated configuration file is automatically sent to the endpoint machines when they connect to the NGFW Engines.

Install the Forcepoint ECA client on the endpoint machines

1. On the endpoint machine, copy the Forcepoint ECA configuration XML file that you exported from the SMC (eca_client_yyyymmdd_hhmmss.xml) into the folder that contains the Forcepoint ECA installation files.

If there are multiple configuration files in the ECA installation folder, the Forcepoint ECA Configuration Wizard uses the configuration file that has the most recent modification date.

2. Run the Installation Wizard (setup.exe) to install the Forcepoint ECA client on the endpoint machine.
3. (Optional) Install and run the Executable List Tool to get a baseline list of all software executables installed on the endpoint machine.

Upgrade instructions

If you have a lower version of the Forcepoint ECA client installed on your endpoint machines, you can upgrade your endpoint machines to this newer version by running the new setup.exe file. When you install the new version, the old version is automatically removed from the endpoint machine. The new installation uses your existing configuration file.

For more information, see the *Forcepoint Endpoint Context Agent Installation and Deployment Guide*. This guide is available for download at <https://support.forcepoint.com>.

Known issues

For a list of known issues in the product release, see Knowledge Base article [16416](#).

Find product documentation

On the Forcepoint support website, you can find information about a released product, including product documentation, technical articles, and more.

You can get additional information and support for your product on the Forcepoint support website at <https://support.forcepoint.com>. There, you can access product documentation, Knowledge Base articles, downloads, and contact information.

Product documentation

Every Forcepoint product has a comprehensive set of documentation.

- *Forcepoint Endpoint Context Agent Installation and Deployment Guide*
- *Forcepoint Endpoint Context Agent Executable List Tool Guide*
- *Forcepoint Next Generation Firewall Product Guide*
- *Forcepoint Next Generation Firewall online Help*

© 2018 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. Raytheon is a registered trademark of Raytheon Company. All other trademarks used in this document are the property of their respective owners.