Release Notes

Forcepoint Endpoint Context Agent

1.3

Contents

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

Build version

The Forcepoint ECA for Windows build version is 5184.

Product binary checksums

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

ECA_Client-1.3.5184.zip

SHA1SUM:

```
21cac2b099bf758ec27fc6759cb40487ffe2825f
```

SHA256SUM:

```
4d8c30a12b991bb28d0361193a9b1b1046eb9528fe14a1bcb607a6b837f29b86
```

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

This Forcepoint Endpoint Context Agent release includes the following new features. There are no updates to the Executable List Tool in this release.

ECA Evaluation

Forcepoint ECA can now be deployed to a limited set of endpoint machines using the ECA Evaluation deployment option. This deployment option is beneficial for customers who wish to evaluate Forcepoint ECA without deploying the ECA client software enterprise-wide.

With ECA Evaluation, all of the required certificates for communication between endpoint machines and the NGFW Engine are created automatically. After enabling the ECA Evaluation feature, a web app is hosted on the Management Server. On each endpoint machine, users can browse to the web app, then download and install the ECA client software and the necessary certificates. Windows administrator rights are required for installing ECA on the endpoint machine.

For instructions about deploying ECA for evaluation purposes, see Knowledge Base article 16193.

✓ **Note**

To use the ECA Evaluation feature, you must have Forcepoint NGFW 6.5 deployed in your organization.

Updates to configuration file

When you export the Forcepoint ECA configuration file from the SMC, the file name is formatted as *eca_client_yyyymmdd_hhmmss.xml*. Forcepoint ECA can read this file name format. There is no need to rename the configuration file *eca.conf*.

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.

Updates in ECA tooltip window

New information has been added to the Forcepoint ECA tooltip window. When you move the mouse over the Forcepoint ECA system tray icon, the tooltip window now shows the following Forcepoint ECA information:

- Forcepoint ECA version number
- Connections to the Forcepoint NGFW Engines, including the connection status, IP address, and port. Up to four connections might be shown in this window, depending on the amount of information provided for each connection.
- The total number of active NGFW Engine connections. The maximum number of available connections is 16.

Support for Citrix XenDesktop deployment

You can now deploy Forcepoint ECA to a shared server that hosts Citrix XenDesktop desktop virtualization software. Users can access and use their virtual desktops normally. The Forcepoint ECA client logs the user’s actions from their virtual desktop to the NGFW Engines.

Forcepoint ECA is compatible with the following Citrix products:

- Citrix XenDesktop 7.14 (shared host)
- Citrix XenDesktop 7.14 (dedicated host)

Updates in the communication library

The communication library has been updated to provide the following new features:

Expanded openssl logging

The Forcepoint ECA client now provides more verbose logs for debugging connectivity errors.

Cryptography API: Next Generation certificate authentication support

The Forcepoint ECA client now supports Cryptography API: Next Generation (CNG) certificates. With this update, you can use **Key Storage Provider** as the Cryptography

Provider Category in the certificate template in Active Directory Certificate Services (AD CS). You are no longer restricted to only using the **Legacy Cryptographic Service Provider**.

Resolved issues

These issues are resolved in this release of the product.

Description	Issue number
On Windows 7 endpoint machines, the svchost.exe process does not populate the “Executable Signer” field.	UEP-10698
The Forcepoint Endpoint Context Agent does not show the correct connection status information in the tooltip window available from the system tray icon.	UEP-10814
The Forcepoint Endpoint Context Agent does not send the SHA512 information to the SMC. As a result, the Executable SHA512 field is empty in the log data in the Logs view.	UEP-12125
The Forcepoint Endpoint Context Agent shows that the signature check fails if the custom signer “Forcepoint ECA Trusted Metro App” is used.	UEP-13586
The Forcepoint Endpoint Context Agent process FpECAWfp.sys might cause Windows endpoint machines to become unresponsive.	UEP-15381
The Forcepoint Endpoint Context Agent sends incorrect system metadata to the SMC immediately after the endpoint machine is restarted.	UEP-19317
The Forcepoint Endpoint Context Agent stops responding on Windows 10 endpoint machines after the logged-on user changes or the current user signs back into Windows.	UEP-22909
The Forcepoint Endpoint Context Agent might prevent some software upgrades on the endpoint machine. When the Forcepoint ECA client verifies the software executable with the NGFW Engine, the ECA client locks the executable and prevents the endpoint machine from using the executable.	UEP-24735
The Forcepoint Endpoint Context Agent does not send the endpoint machine’s Computer Name information to the SMC.	NGFW-10224

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 7.

   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.

Known issues

For a list of known issues in the product release, see Knowledge Base article 16136.

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*