



Installation and Deployment Guide

Forcepoint Endpoint Context Agent

©2018 Forcepoint
All rights reserved.
10900-A Stonelake Blvd, Quarry Oaks 1, Suite 350, Austin, TX 78759, USA
Published 2018

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.

This document might not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Forcepoint. Every effort has been made to ensure the accuracy of this manual. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Contents

Chapter 1	Introducing Forcepoint Endpoint Context Agent	1
	System requirements	1
	Operating system requirements.	1
	Prerequisites	2
Chapter 2	Deploying Forcepoint Endpoint Context Agent in Your Enterprise	3
	Before you begin	3
	Obtaining the Forcepoint Endpoint Context Agent installation package.	4
	Checking file integrity	4
	Deploying the Forcepoint Endpoint Context Agent.	5
	Deploying Forcepoint Endpoint Context Agent manually on an endpoint machine	6
	Testing deployment.	7
	Uninstalling Forcepoint Endpoint Context Agent	7
	Uninstalling Forcepoint Endpoint Context Agent locally from an endpoint machine	8
	Uninstalling Forcepoint Endpoint Context Agent using a deployment server .	8
	Uninstalling Forcepoint Endpoint Context Agent using a distribution system.	9
Chapter 3	Copyrights and Trademarks	11
	Copyrights and trademarks	11
	Other acknowledgments	11

1

Introducing Forcepoint Endpoint Context Agent

ECA | 1.1 | 29-Jan-2018

The Forcepoint Endpoint Context Agent (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). Forcepoint NGFW uses the information from Forcepoint ECA to determine whether connections from the endpoint machines are allowed.

System requirements

Operating system requirements

Forcepoint ECA is currently only available for Windows endpoint machines.

Windows 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)

Windows Server requirements:

- Windows Server 2012
- Windows Server 2016

Prerequisites

To install and use Forcepoint ECA, you must have Forcepoint NGFW 6.3.0 or later installed.

See the [Forcepoint Next Generation Firewall Product Guide](#) for more information about configuring integration with Forcepoint ECA.

2

Deploying Forcepoint Endpoint Context Agent in Your Enterprise

ECA | 1.1 | 29-Jan-2018

Before you begin

- As a best practice, start by deploying and testing the Forcepoint Endpoint Context Agent (Forcepoint ECA) software on a few local network machines, then increase to a limited number of remote machines before deploying the software throughout your enterprise.
- Ensure that there are no network address translation (NAT) devices between the Forcepoint Next Generation Firewall (Forcepoint NGFW) Engine and the endpoint machine.
- Before installing Forcepoint ECA on an end user's endpoint machine, take the following actions:
 - a. Establish a certificate authority (CA) for Forcepoint ECA. This can be accomplished in one of the following methods:
 - Import your existing Active Directory Certificate Services (AD CS) certificates to the Forcepoint NGFW Security Management Center (SMC), if they have already been deployed within your organization.
 - In the domain where the Forcepoint ECA clients are located, create a Certificate Authority (CA), then import the CA to the Forcepoint NGFW Security Management Center as a Trusted Certificate Authority element. For more information, see Knowledge Base article [14099](#).
 - b. In the Management Client, create a Forcepoint ECA Configuration element that uses the newly created CA.
 - c. Enable Forcepoint ECA on the NGFW Engine, and use the newly created Forcepoint ECA Configuration element.

- d. Export the Forcepoint ECA configuration file from the Engine Editor. This configuration file is required before installing Forcepoint ECA on an end user's endpoint machine.



Note

SMC names the configuration file *eca_client_yyyymmdd_hhmmss.xml*. Rename this file to *eca.conf* when you copy it to the Forcepoint ECA installation folder. If you do not rename the file, the Forcepoint ECA installation fails.

See the [Forcepoint Next Generation Firewall Product Guide](#) for more information.

- Forcepoint ECA installation requires local administrator rights to the endpoint machine.

Obtaining the Forcepoint Endpoint Context Agent installation package

The Forcepoint ECA installation package is available for download from the Forcepoint website:

1. Log on to [My Account](#).
2. Open the **Downloads** page.
3. Under **Network Security** section, select an NGFW ECA Client for Windows version, then download the software.

Checking file integrity

Before installing Forcepoint ECA from downloaded files, check that the installation files have not become corrupt or been changed.

Using corrupt files might cause problems at any stage of the installation and use of the system. Check file integrity by generating a file checksum of the files. Compare the checksum of the downloaded files 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 folder that contains the files 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:
 - md5sum filename
 - sha1sum filename
 - sha256sum filename
4. Compare the displayed output to the checksum for the software version. They must match.



Warning

Do not use files that have an invalid checksum. If downloading the files again does not help, contact [Forcepoint support](#) to resolve the issue.

Deploying the Forcepoint Endpoint Context Agent

There are a few ways to distribute the Forcepoint ECA software on Windows endpoint machines:

- Deploy Forcepoint ECA manually on each endpoint machine.
See *Deploying Forcepoint Endpoint Context Agent manually on an endpoint machine*, page 6 below.
- Deploy Forcepoint ECA using a third-party deployment tool for Windows. Forcepoint ECA can be remotely deployed using your preferred deployment server or distribution system, as long as it accepts an MSI (.msi) or ZIP (.zip) file as the input and can run the installation command remotely.

For more information about common deployment tools, see:

- Microsoft Group Policy Object (GPO): [How to use Group Policy to remotely install software](#)
- System Center Configuration Manager (SCCM): [How to Deploy Packages and Programs in Configuration Manager](#)
- Systems Management Server (SMS): [Creating Software Installation Packages with SMS Installer](#)
- IBM BigFix: [Software Distribution Guide](#)



Important

You must copy the *eca.conf* configuration file to the installation folder before installation.

Deploying Forcepoint Endpoint Context Agent manually on an endpoint machine

Before you begin deployment, you must obtain both the configuration file (*eca.conf*) from the SMC and the Forcepoint ECA installation package from Forcepoint. You must also log on to the endpoint machine with local administrator rights.

To manually deploy Forcepoint ECA on individual endpoint machines:

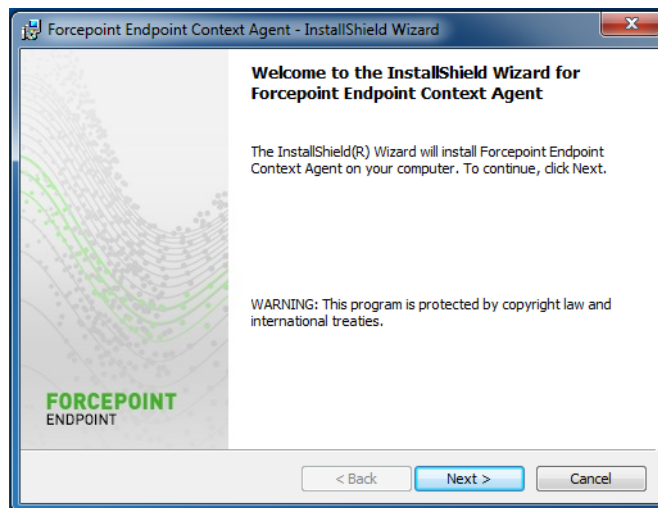
1. Copy the *eca.conf* configuration file into the folder that contains the Forcepoint ECA installation files.



Note

SMC names the configuration file *eca_client_yyyymmdd_hhmmss.xml*. Rename this file to *eca.conf* when you copy it to the Forcepoint ECA installation folder. If you do not rename the file, and the *eca.conf* file is not located in this folder, the Forcepoint ECA installation fails.

2. Double-click **setup.exe**. The Installation Wizard checks that the endpoint machine meets the installation requirements, then the Installation Wizard opens.



3. Click **Next**. The Forcepoint License Agreement appears.
Click **Cancel** at any time during the installation to exit the Installation Wizard.
Click **Back** at any time to return to a previous screen.
4. Select **I accept the terms in the license agreement**, then click **Next**.
5. By default, Forcepoint ECA is installed in **C:\Program Files\Forcepoint\ECA**. To install it in a different folder, click **Change**, then select the folder.
6. When the installation folder is set, click **Next**.
The **Ready to Install the Program** screen appears.


7. To install Forcepoint ECA, click **Install**.

The Installation Wizard shows a progress bar that indicates the status of the installation. To stop the installation, click **Cancel**. Otherwise, wait until the installation is complete.

When the installation is complete, the Installation Wizard shows a confirmation page.

8. Click **Finish** to exit the Installation Wizard.

Testing deployment

After Forcepoint ECA is installed on the endpoint machine, an icon () appears in the endpoint machine's system tray. If you move the mouse over the icon, it shows **FORCEPOINT ECA** along with the connection status to the SMC.

To confirm that the Forcepoint ECA software is installed and running on an endpoint machine:

1. Go to **Start > Control Panel > Administrative Tools > Services**.
2. Verify that **Forcepoint Endpoint Context Agent** is present in the Services list and is started.

If you encounter issues during the Forcepoint ECA installation, review the following checklist, then attempt to install Forcepoint ECA again.

- Verify that you installed Forcepoint ECA using an account with local administrator rights. Forcepoint ECA installation requires local administrator rights.
- Check the connection between the endpoint machine and Forcepoint NGFW. Ping the Forcepoint NGFW listening interface from the endpoint machine.
- Check the installed certificates using `mmc.exe` and the Certificates snap-in. The certificate issuer (CA certificate) must be configured in the SMC. The endpoint machine receives the network side CA certificate in the `eca.conf` configuration file.
- The certificate generated by the SMC is valid from the time it was created on the SMC. If the clock time on the endpoint machine is different from the time on the SMC, the endpoint machine might not accept the generated certificate. After the endpoint machine's clock reaches the certificate's validity start time, the certificate is accepted on the endpoint machine.

Uninstalling Forcepoint Endpoint Context Agent

There are three ways to uninstall Forcepoint ECA:

- Locally on each endpoint machine
- Remotely through a deployment server

- Remotely through a distribution system

Uninstalling Forcepoint Endpoint Context Agent locally from an endpoint machine

1. Go to **Start > Control Panel > Add/Remove Programs**.
The Add/Remove Programs screen appears.
2. In the list of installed programs, select **Forcepoint Endpoint Context Agent**, then click **Uninstall**.
You are prompted to confirm that you want to delete Forcepoint ECA.
3. Click **Yes**.
After Forcepoint ECA is uninstalled, you are prompted to restart the endpoint machine.
4. Click **Yes** to restart the endpoint machine now, or **No** to restart later. The configuration changes are applied only when the endpoint machine has restarted.

Uninstalling Forcepoint Endpoint Context Agent using a deployment server

If you deployed Forcepoint ECA through GPO, you can uninstall the software through the Active Directory Users and Computers snap-in. For more information, see [How to use Group Policy to remotely install software](#).

You can also silently uninstall Forcepoint ECA by running the following command:

```
msiexec /x {product_code} /qn
```

where {product_code} is a unique identifier (GUID) that can be found in the setup.ini file of each installation package. The GUID is different for each version and bit type (32-bit or 64-bit).

To find the setup.ini file, use a file compression tool such as WinZip or 7-Zip to extract the contents of the installation package executable.

To silently uninstall Forcepoint ECA without a reboot, add the **/norestart** parameter as follows:

```
msiexec /x {product_code} /qn /norestart
```

The command switches are summarized below.

Function	Switch
Silent uninstallation	<code>msiexec /x {product_code} /qn</code>
Silent uninstallation without reboot	<code>msiexec /x {product_code} /qn /norestart</code>

Uninstalling Forcepoint Endpoint Context Agent using a distribution system

If you used the Microsoft SMS distribution system to create the Forcepoint ECA installation packages, those packages can be reused, with a slight modification, for uninstalling the software. If you did not create a package for deploying Forcepoint ECA, you must create a new package for uninstallation.

For more information about creating SMS installation packages, see [Creating Software Installation Packages with SMS Installer](#).

After deploying the package, Forcepoint ECA is uninstalled from the defined list of endpoint machines.

3

Copyrights and Trademarks

ECA | 1.1 | 29-Jan-2018

Every effort has been made to ensure the accuracy of this manual. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Copyrights and trademarks

© 2018 Forcepoint. This document might not, in whole or in part, be reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from 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.

Other acknowledgments

This Forcepoint product includes the following open source software:

OpenSSL, developed by the OpenSSL Project for use in the OpenSSL Toolkit (<https://www.openssl.org>), © 1998-2017 The OpenSSL Project, © 1995-1998 Eric Young (eay@cryptsoft.com), and is distributed under a double license, the OpenSSL License and the original SSLeay License (<https://www.openssl.org/source/license.html>) ■ LIBEVENT 2.0.22-STABLE, © 2000-2007 Niels Provos <provos@citi.umich.edu>, © 2007-2012 Niels Provos and Nick Mathewson, is distributed under the BSD 3-Clause License (<https://opensource.org/licenses/BSD-3-Clause>) ■ EZXML, © 2004, 2005 Aaron Voisine, is distributed under the MIT License (<https://opensource.org/licenses/mit-license>)

© 2018 Forcepoint

