



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
	Authenticating Forcepoint ECA using client certificates.	3
	Configuring Forcepoint ECA settings in the SMC.	4
	Obtaining the Forcepoint Endpoint Context Agent installation package.	5
	Checking file integrity	5
	Deploying the Forcepoint Endpoint Context Agent.	5
	Deploying Forcepoint Endpoint Context Agent manually on an endpoint machine	6
	Viewing connection status	7
	Testing deployment.	8
	Troubleshooting deployment	8
	Uninstalling Forcepoint Endpoint Context Agent	9
	Uninstalling Forcepoint Endpoint Context Agent locally from an endpoint machine	10
	Uninstalling Forcepoint Endpoint Context Agent using a deployment server	10
	Uninstalling Forcepoint Endpoint Context Agent using a distribution system.	10
Chapter 3	Copyrights and Trademarks	13
	Copyrights and trademarks	13
	Other acknowledgments	13

1

Introducing Forcepoint Endpoint Context Agent

ECA | 1.3 | 20-Sep-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

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

Prerequisites

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

For information about configuring the Forcepoint ECA settings in 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>.

2

Deploying Forcepoint Endpoint Context Agent in Your Enterprise

ECA | 1.3 | 20-Sep-2018

This section provides the steps required to configure settings for Forcepoint Endpoint Context Agent (Forcepoint ECA) in the Forcepoint NGFW Security Management Center (SMC) and install the Forcepoint ECA client software on the endpoint machines within your organization.

Before you begin

- As a best practice, start by deploying and testing the Forcepoint ECA client software on a few local network machines, then install the software 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.
- Forcepoint ECA installation requires local administrator rights on the endpoint machine.

Authenticating Forcepoint ECA using client certificates

Using a client certificate, the Forcepoint NGFW Engines authenticate the endpoint machines running Forcepoint ECA. This certificate must be installed on the endpoint machine before installing Forcepoint ECA. Otherwise, the Forcepoint ECA client will not be able to connect to the Forcepoint NGFW Engines.

1. In the Management Client component of the SMC, establish a certificate authority (CA) for Forcepoint ECA in one of the following ways:
 - a. Import your existing Active Directory Certificate Services (AD CS) CA certificates to the SMC, if they have already been used to deploy client computer authentication certificates within your organization. The deployed certificates must have the **Client Authentication** application policy enabled. If such certificates have been deployed to each endpoint machine where the Forcepoint ECA client will be deployed, skip step 2.

- b. In the domain where the Forcepoint ECA clients are located, create a CA, then import the CA to the SMC as a Trusted Certificate Authority element. For more information, see Knowledge Base article [14099](#).

Forcepoint ECA uses the customer-provided CA to authenticate the endpoint machine and uses the SMC's internal CA to authenticate the NGFW Engines.

2. After the CA is established, create a new certificate template in AD CS and enroll it to each endpoint machine where Forcepoint ECA is to be installed. This certificate is required to authenticate the endpoint machine with the Forcepoint NGFW Engines.

When you create the certificate template in AD CS, you must select the **Client Authentication** application policy extension.



Note

Each endpoint machine must have a unique certificate. Only computer certificates are supported. User certificates are not supported.

After the CA is established and each endpoint machine has a valid client certificate, continue with the configuration steps in the next section.

Configuring Forcepoint ECA settings in the SMC

These high-level steps provide an overview of the configuration process.

For information about configuring the Forcepoint ECA settings in 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, create a Forcepoint ECA Configuration element that uses the newly created CA.
2. Enable Forcepoint ECA on the NGFW Engine, and use the newly created Forcepoint ECA Configuration element.
3. Export the Forcepoint ECA configuration XML file (eca_client_yyyymmdd_hhmmss.xml) from the Engine Editor. You must copy this file to the installation folder before you install the Forcepoint ECA client software on the endpoint machines.

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

After you configure settings for Forcepoint ECA in the SMC, save the configuration file, and update the policy on the NGFW Engines, you are ready to install the Forcepoint ECA client software on the endpoint machines. Follow the steps in the

next sections to obtain and verify the software, then deploy it on your endpoint machines.

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 the **Network Security** section, select **All versions** under NGFW ECA Client for Windows, 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 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.

1. Look up the correct checksum at <https://support.forcepoint.com>.
2. Change to the folder that contains the files to be checked.
3. Using your preferred tool, generate a checksum of the file.
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.

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 to a limited set of endpoint machines using the ECA Evaluation deployment option. Forcepoint NGFW 6.5 is required to use the ECA Evaluation feature.

For more information, see Knowledge Base article [16193](#).

- Deploy Forcepoint ECA to a shared server that hosts Citrix XenDesktop desktop virtualization software. This deployment method is similar to the manual deployment, but you deploy the Forcepoint ECA client software to a network server instead of each endpoint machine.

You can deploy Forcepoint ECA to the following Citrix products:

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

For more information, see the [Citrix XenDesktop documentation](#).

- 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 Executable (.exe) 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

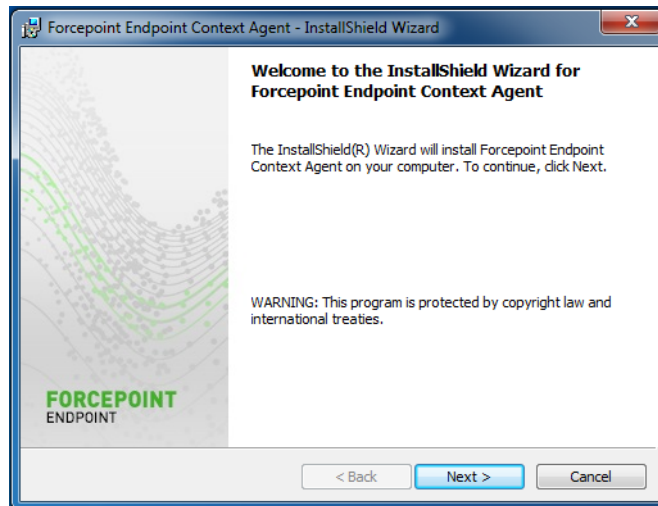
You must copy the Forcepoint ECA configuration file to the installation folder before installation.

Deploying Forcepoint Endpoint Context Agent manually on an endpoint machine

Before you begin deployment, you must obtain both the configuration file 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_client_yyyymmdd_hhmmss.xml* configuration file into the folder that contains the Forcepoint ECA installation files. If there are multiple configuration files in the folder, Forcepoint ECA uses the configuration file with the most recent modification date.
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.
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** page 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.

Viewing connection status

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 version number, build number, and connection status to the Forcepoint NGFW.

The connection status can be one of the following:

- **DISCONNECTED:** Forcepoint ECA is not connected to the Forcepoint NGFW Engine.
- **WAITING_RECONNECT:** The connection between the Forcepoint ECA client and the Forcepoint NGFW Engine was stopped. Forcepoint ECA is trying to establish the connection again.
- **CONNECTING:** Forcepoint ECA is connecting to the Forcepoint NGFW Engine.
- **CONNECTED:** Forcepoint ECA is connected to the Forcepoint NGFW Engine.
- **HANDSHAKING:** Forcepoint ECA is establishing a communication link to the Forcepoint NGFW Engine.
- **CONFIGURING:** Forcepoint ECA is getting configuration information from the Forcepoint NGFW Engine.
- **CONFIGURED:** Forcepoint ECA is successfully configured on the endpoint machine and is sending data to the Forcepoint NGFW Engine.

Testing deployment

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

1. Go to the Windows Administrative Tools, and open the list of services.
2. Verify that **Forcepoint Endpoint Context Agent** is present in the Services list and is started.

Troubleshooting deployment

If you encounter issues during the Forcepoint ECA installation, review the following checklist, then try 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.
- Check the certificates installed in the endpoint machine's certificate stores using mmc.exe and the Certificates snap-in. The certificate issuer (CA certificate) must be configured in the SMC. Verify that the policy on the NGFW Engine is up to date. The endpoint machine receives the network-side CA certificate in the Forcepoint ECA configuration file.
- The certificate generated by the SMC is valid from the time it was created in the SMC. If the time on the endpoint machine is different from the time in the SMC, the endpoint machine might not accept the generated certificate. After the endpoint machine's time reaches the certificate's validity start time, the certificate is accepted on the endpoint machine.

The Forcepoint ECA client initiates connections to certificate revocation list (CRL) servers to verify the signatures of the executables that are initiating connections from

the endpoint machine. When an executable connects to the network for the first time, the Forcepoint ECA client checks the executable's signature against the CRL.

If the executable has been modified, or if the code signing certificate has been revoked, Forcepoint ECA does not trust the executable fields, such as product name, product version, or signer name, when it tries to match the executable in the Forcepoint NGFW. The executable's signature check status is then logged in the SMC logs as "Failed"

The following list shows common connectivity error messages and troubleshooting steps:

- Error message: **Failed to accept SSL-connection . . . : SSL error: peer did not return a certificate**
 - Check that the certificate is installed in the certificate store on the endpoint machine.
 - Check that the client certificate has the **Client Authentication** Application Policy enabled.
 - Check that the issuer of the client certificate on the endpoint machine matches the issuer of the client certificate in the ECA configuration in the SMC.
- Error message: **Failed to accept SSL-connection . . . : SSL error: sslv3 alert bad certificate**
 - Check the DebugDump.txt file in the Forcepoint ECA installation folder on the endpoint machine for the actual error.
 - If the error message is **Verify failure . . . certificate is not yet valid**, check the time difference between the endpoint machine and the SMC.
- Error message: **Same client connected to adjacent node**
 - If the Forcepoint ECA client disconnects immediately after proceeding to the CONFIGURED connection state and shows the **Same client connected to adjacent node** message in the DebugDump.txt file or in the Information Message field in the SMC, make sure that the Forcepoint ECA clients use different certificates. Forcepoint NGFW does not allow two or more connections to share a client certificate. Each Forcepoint ECA client must have a unique client certificate.

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. Use the Add/Remove Programs tool in Windows to uninstall the Forcepoint Endpoint Context Agent.
You are prompted to confirm that you want to delete Forcepoint ECA.
2. Click **Yes**.
After Forcepoint ECA is uninstalled, you are prompted to restart the endpoint machine.
3. 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, include 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, you can modify the packages and use them to uninstall 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 | 1.3 | 20-Sep-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

