



F1E

23.11

**Deploying Forcepoint DLP Endpoint on Citrix
virtual environments**

© 2023 Forcepoint

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.

Published 22 November 2023

Every effort has been made to ensure the accuracy of this document. 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

1 Deploying Forcepoint DLP Endpoint on Citrix XenApp, XenDesktop, and Virtual Apps Clients.....	5
Introduction.....	5
Supported Citrix versions.....	5
Forcepoint DLP Endpoint channel support.....	6
Deployment and Installation.....	6

Chapter 1

Deploying Forcepoint DLP Endpoint on Citrix XenApp, XenDesktop, and Virtual Apps Clients

Contents

- Introduction on page 5
- Supported Citrix versions on page 5
- Forcepoint DLP Endpoint channel support on page 6
- Deployment and Installation on page 6

Introduction

Forcepoint DLP Endpoint can be deployed on Citrix XenApp, XenDesktop, and Virtual Apps (hereafter referred to as “Citrix virtual environments”). In non-virtual environments, Forcepoint DLP Endpoint serves one person working on an individual endpoint machine, such as a desktop or laptop. Citrix virtual environments, on the other hand, connect many users to the same server and serve one Forcepoint DLP Endpoint software installation to all users.



Note

This document only describes the Forcepoint DLP Endpoint deployment to a Citrix server. Forcepoint Web Security Endpoint has not been tested, and is not supported, in a Citrix virtual environment.

Supported Citrix versions

Supported versions are listed in the [Certified Product Matrix](#).

Forcepoint DLP Endpoint channel support

Forcepoint DLP Endpoint supports the following endpoint destination channels in Citrix virtual environments:

- **HTTP/S:** Analyzes data being posted to the Web via Internet Explorer, Edge, Chrome, or Firefox browsers.
- **Email:** Analyzes email messages sent from Forcepoint DLP Endpoint users, even if they send them to external Web mail services such as Yahoo.
- **Print:** Monitors data being sent from an endpoint machine to a local or network printer. The system supports drivers that print to a physical device, not those that print to file or PDF.
- **Application file access:** Monitors access to files in supported applications. Cloud is supported if accessed through Firefox.

Forcepoint DLP Endpoint does not support the following endpoint destination channels in Citrix virtual environments:

- Removable media
- CD/DVD writers
- Application controls (cut/copy/paste)
- Print screen
- LANs



Note

Forcepoint DLP endpoint only supports flash based removable media devices on Windows endpoints. It does not support SCSI over USB or similar.

Forcepoint DLP Endpoint supports the **Confirm**, **Permit**, and **Block** actions in Citrix virtual environments, but does not support **Encrypt with user password** or **Encrypt with profile key**.

Deployment and Installation

Building the package

The first step in your deployment is to generate the Forcepoint DLP Endpoint software package using the package builder utility provided by Forcepoint. This package will be installed in your Citrix virtual environment.

For instructions on generating the installation package, see the [Forcepoint F1E Solutions Installation and Deployment Guide](#).

On the package builder's **Installation Platform and Security** screen, select **Windows 64-bit** for your XenApp clients. Mac deployments are not supported.

Deploying and installing the package

Follow the steps in the [Forcepoint F1E Solutions Installation and Deployment Guide](#) for deploying and installing Forcepoint DLP Endpoint on Windows endpoint machines.

Instead of deploying the software to each endpoint machine, deploy it to a network server.

Removing duplicate EndpointID values

Forcepoint F1E v18 introduced an EndpointID value to track and distinguish physical machines that send RAP events back to Forcepoint DLP through the Forcepoint DLP Endpoint. If you deploy Forcepoint F1E v18 or later using a golden image, then the RAP-enabled endpoint machines might report the same EndpointID value.

Deleting EndpointID before creating a golden image

You can delete the EndpointID GUID manually from the golden image before running Sysprep. When you delete EndpointID here, the endpoint machine automatically creates a unique EndpointID value specific to the endpoint machine.

Steps

- 1) Install Forcepoint F1E on Windows.
- 2) As Domain/Administrator, open regedit.
- 3) Go to HKEY_LOCAL_MACHINE\SOFTWARE\Forcepoint\Agent\
HKEY_LOCAL_MACHINE\SOFTWARE\Forcepoint\Agent\
- 4) Delete the value for DWORD "EndpointID".
WARNING: Do not delete the entire EndpointID DWORD, just the value.
- 5) Run your Sysprep script to prepare your golden image.
- 6) Deploy the golden image to your endpoint machines.
- 7) Verify that the EndpointID is unique. If the EndpointID is a duplicate, check the registry entry in the golden image or remove the value using the procedure below.

Removing the duplicate EndpointID value on deployed endpoint machines

If you deployed the image without removing the EndpointID, you can remove it after deployment:

Steps

- 1) On the endpoint machine, stop the F1E services.

- 2) As Domain/Administrator, open regedit.
- 3) Go to HKEY_LOCAL_MACHINE\SOFTWARE\Forcepoint\Agent\.
- 4) Delete the value for DWORD "EndpointID".
WARNING: Do not delete the entire EndpointID DWORD, just the value.
- 5) Restart the F1E services (or restart the machine) to generate a new "EndpointID" GUID value.

Configuring the package to improve resource usage

To support hardware resources in Citrix virtual environments, Forcepoint DLP Endpoint must be configured to support additional threads and improve memory usage. This change needs to be made on each Citrix server running Forcepoint DLP Endpoint.

To customize the configuration:

Steps

- 1) Open the [AlternateResource.config.xml](#) file in a text editor.

- 2) Complete the following:
 - a) Set **<numOfThreads>** (the number of threads per processor). There are two options:
 - Set **<numOfThreads>** to **-1**. If you set this to **-1**, the system automatically doubles the number of cores. Forcepoint recommends this option.
 - Manually set **<numOfThreads>** to at least twice the number of cores on the Terminal Services server. For example, if you have 4 cores on the Terminal Services server, set **<numOfThreads>8</numOfThreads>**.
 - b) Change all resource IDs in the document to reflect the number of threads you wish to use.
 - c) Increase **<MaxRamSpace>** to optimize endpoint memory usage. To do so:
 - i) Multiply the number of supported sessions by 50 then by 0.125. For example, if there are 8 supported sessions, multiply $8 \times 50 \times 0.125 = 50$.
 - ii) Round up the result to the nearest integer in multiples of 50MB, but no less than 100MB. For example, using the result from the first step (50), you get 100 (a multiple of 50, but not less than 100).
 - iii) Convert the result from megabytes to bytes. For example, using the result from the second step (100MB) converted to bytes, you get 100000000.
 - iv) Set **<MaxRamSpace>** to this value. For example, using the result from the third step, you would set this value to **<MaxRamSpace>100000000</MaxRamSpace>**.
- 3) Save the **AlternateResource.config.xml** file.
- 4) In the Windows Task Manager, stop the **EndpointClassifier** service.
- 5) Copy the **AlternateResource.config.xml** file to C:\Program Files\WebSense\WebSense Endpoint:
 - a) From the command line, go to C:\Program Files\WebSense\WebSense Endpoint.
 - b) Run the following command:

```
WDEUtil.exe -set disableantitampering=true
```
 - c) Copy **AlternateResource.config.xml** file to the directory.
- 6) In Windows Task Manager, restart the **EndpointClassifier** service.

- 7) Restart the WDEUtil service through the command line.
 - a) From the command line, go to C:\Program Files\WebSense\WebSense Endpoint.
 - b) Run the following commands:


```
WDEUtil.exe -stop wsdlp
```

```
WDEUtil.exe -start wsdlp
```

Sample File:

```
<policyEngineConfig xmlns:fn="http://www.w3.org/2005/02/xpath-functions"
GlobalVersion="1">
- <resourcesConfig isServer="false">
- <resource id="0">
  <numOfThreads>-1</numOfThreads>
  <numOfQueues>10000</numOfQueues>
</resource>
- <resource id="1">
  <numOfThreads>-1</numOfThreads>
  <numOfQueues>10000</numOfQueues>
</resource>
- <resource id="2">
  <numOfThreads>-1</numOfThreads>
  <numOfQueues>10000</numOfQueues>
</resource>
- <resource id="3">
  <numOfThreads>-1</numOfThreads>
  <numOfQueues>10000</numOfQueues>
</resource>
+ <resource id="4">
- <resource id="5">
  <numOfThreads>-1</numOfThreads>
  <numOfQueues>10000</numOfQueues>
</resource>
- <resource id="6">
  <numOfThreads>-1</numOfThreads>
  <numOfQueues>10000</numOfQueues>
</resource>
- <resource id="7">
  <numOfThreads>-1</numOfThreads>
  <numOfQueues>10000</numOfQueues>
</resource>
</resourcesConfig>
- <MemoryInfo isServer="true">
  <MaxRAMSpace>100000000</MaxRAMSpace>
  <MaxDiskSpace>500000000</MaxDiskSpace>
</MemoryInfo>
</policyEngineConfig>
```

