Forcepoint

F1E

22.12

Automatic Updates

Revision A

Published 07 December 2022

Contents

Chapter 1

Automatic Updates for Forcepoint F1E (Forcepoint DLP Endpoint)

Contents

This document is divided into two sections:

- *Configuring the auto-update server*
- *Auto-update workflow for advanced configuration*

The first section describes how to set up a server to work with the auto-update feature. The second section helps you understand the workflow of the endpoint auto-update process, how the endpoint and update server communicate with each other, and how you can add flexibility to the endpoint auto-update feature with different parameters.

Related concepts
Auto-update workflow for advanced configuration on page 12

Related tasks
Configuring the auto-update server on page 6

About the Feature

Endpoint auto-update is a feature that lets a network server push a Forcepoint DLP Endpoint installation package to endpoint machines and silently install the package in the background. By doing so, the network server controls the version of the endpoint running on endpoint machines.

The endpoint auto-update feature does not support the initial deployment of the agent — it only supports existing agents. In addition, auto-update:

- Does not apply to Linux or Mac endpoint machines. It works only with Windows endpoint machines.
- Does not apply to updating the Forcepoint Web Security Endpoint. Only Forcepoint DLP Endpoint can be updated through the auto-update server.

Note

Starting with Forcepoint DLP v8.6, Forcepoint DLP Endpoint on the Forcepoint F1E platform became the standard Forcepoint Endpoint agent for Forcepoint DLP and Forcepoint Dynamic Data Protection.

Configuring the auto-update server

The steps provided in this section need to be performed only once. Once this setup is completed, you do not need to repeat this process.

To set up the auto-update system:

Steps

1) Install a Web server.
2) Copy and unzip endpoint server-side files to the Web server.
3) Configure the Web server.
4) Deploy an initial endpoint package.
5) Deploy an endpoint package on the auto-update server.

Installing the Web server

Forcepoint DLP Endpoint performs automatic updates regularly by checking with a Web server to determine if they are at the most current version. If Forcepoint DLP Endpoint on the endpoint machine is not up to date, it tries to download a new package from the Web server and install it.

Your Web server can be any server in your network. For best practice, it should be on a different machine than your servers — such as the management server and secondary Forcepoint DLP servers. This optimizes performance of the servers and preserves them for future upgrades. It also gives you the flexibility to choose the port numbers, the hardware, and the operating system, as well as the security hardening mechanisms to be used, without the risk of collision with Forcepoint components.

You can choose any Web server software that meets your needs and configure it on your machine and network, as long as it meets the following requirements:

- It must support file hosting.
- It must support CGI or other server-side scripting language.
- It must have enough hardware resources to handle I/O from all endpoints. Generally, when endpoints are up to date, they query the server every 120 minutes, with each query and response being approximately 1 KB. But when endpoints are out of date, they try to download the update package, which is typically 100 MB. Therefore, a server that supports 1,200 endpoints should expect 10 requests per minute (1,200 per 120 minutes). When a new package is available, each request can result in a 100 MB file transfer.

  Note that endpoints retry their communication attempts if the server cannot handle the load.
- It must be accessible by the network where the endpoints are installed.
- Its URL must begin with HTTP:// and not HTTPS://. Secure HTTP is not supported.

This document provides instructions on how to use 3 common types of Web servers and provides sample installation instructions for each. See *Configuring your Web server* below for details.

Related tasks

Configuring your Web server on page 7

Copying server-side foundation files

When your server is ready, you need to copy the Endpoint Update Server Kit to your Web server machine and unzip the files. To do so:

Steps

1) Log on to a machine where Forcepoint DLP is installed.

2) Locate the zip file **Endpoint Update Server Kit.zip** under the installation folder (%DSS_HOME%).

3) Copy the file to your Web server machine in a location that is accessible by the Web server process — for example, EP_UPDATE_ROOT.

4) Unzip the file.
   EP_UPDATE_ROOT should now contain the following subfolders:
   a) conf
   b) scripts_windows
   c) scripts_linux
   d) data

Note

This document refers to the Forcepoint DLP folder as %DSS_HOME%. The default %DSS_HOME% location is C:\Program Files (x86)\Websense\Data Security, but may be a different location based on your specific installation.

Configuring your Web server

To configure your Web server, follow these basic steps:

1) Choose a scripts folder to use from **EP_UPDATE_ROOT** (either **scripts_windows** or **scripts_linux**).

2) Create a virtual directory called /**EPUpdate** that is CGI-enabled, and is linked to **EP_UPDATE_ROOT/scripts**.

3) Create another virtual directory called /EPPackages that links to **EP_UPDATE_ROOT/data**.

Note that each Web server installation has different configuration steps. Listed below are steps for the 3 most common Web servers:

Related tasks

Apache HTTPD on Windows on page 8
Apache HTTPD on Linux on page 8
Microsoft IIS on Windows Server 2016 on page 9

Apache HTTPD on Windows

Steps

1) Rename the **EP_UPDATE_ROOT/scripts_windows** folder to scripts (EP_UPDATE_ROOT/scripts).

2) Edit the configuration file **EP_UPDATE_ROOT/conf/httpd.conf** with a text editor and replace the string **${EP_UPDATE_ROOT}** with the actual value of EP_UPDATE_ROOT. **Important:** Use forward slash (/) characters to separate folders. Do not use back slash characters (\).

3) Locate the text file, **httpd.conf**, in the Apache-HTTPD installation folder. Edit the file and append a single line at its end: **include EP_UPDATE_ROOT/conf/httpd.conf**

4) Restart the Apache HTTPD service. Make sure that the service starts up.

Next steps

For additional information, refer to the installation instructions provided on the Apache Web site for compiling and installing on Windows.

Apache HTTPD on Linux

Steps

1) Rename the **EP_UPDATE_ROOT/scripts_linux** folder to **scripts** (EP_UPDATE_ROOT/scripts).

2) Run the following command to make sure **EP_UPDATE_ROOT/scripts/update** has execute permissions: **chmod +x EP_UPDATE_ROOT/scripts/update**

3) If your Linux server is running SELinux (Security Enhanced Linux), use the semanage or the chcon command to label the file-type **EP_UPDATE_ROOT/ scripts/update** as **httpd**_sys_**content_t**. To do this, run the following commands as a Linux root user:

   - /usr/sbin/semanage fcontext –a –t httpd_sys_content_t EP_UPDATE_ROOT/scripts/update
   - /sbin/restorecon EP_UPDATE_ROOT/scripts/update

4) Edit the configuration file **EP_UPDATE_ROOT/conf/httpd.conf** with a text editor, and replace the string **${EP_UPDATE_ROOT}** with the actual value of EP_UPDATE_ROOT.

5) Edit the file **/etc/httpd/conf/httpd.conf**, and append a single line at its end: include **EP_UPDATE_ROOT/ conf/httpd.conf**

6) Restart the Apache HTTPD service. Make sure that the service starts up.

Next steps

For additional information, see the installation instructions provided on the Apache Web site.

Microsoft IIS on Windows Server 2016

Steps

1) Open the **Control Panel**, select **Administrative Tools**, then click **Internet Information Services (IIS)** to open the IIS Manager.

2) In the left pane, click on the machine name, then double-click the option **ISAPI and CGI Restrictions** in the right pane.
   a) Right-click an empty area in the right pane, select **Add**, and fill in the following values:
      - ISAPI or CGI path: **EP_UPDATE_ROOT\scripts_windows\update.bat**
      - Description: **Forcepoint DLP Endpoint Auto-Update**
   b) Check the option **Allow extension path to execute**.
   c) Click **OK**.

3) On the tree in the left pane, locate the site where you want to host your autoupdate server (the default is **Default Web Site**).

4) Right-click the site, choose **Add Virtual Directory**, and enter the following details:
   - Alias: **EPUpdate**
   - Physical path: **EP_UPDATE_ROOT\scripts_windows**

5) Click on the newly created **EPUpdate** virtual folder in the left pane, and doubleclick **Handler Mappings** in the right pane.

6) Right-click an empty area in the right pane, choose **Add Module Mapping**, and enter the following values:
   - Request path: **update.bat**
   - Module: **CgiModule**
   - Executable: (leave empty)
   - Name: **Forcepoint DLP Endpoint Auto-Update**

7) Right-click anywhere on the site, select the option **Add Virtual Directory**, and enter the following details:
   - Alias: **EPPackages**
   - Physical path: **EP_UPDATE_ROOT\data**

Next steps

For additional information, refer to the installation instructions provided on the IIS Web site.

Deploying the initial endpoint package on your endpoint machines

Use the Forcepoint F1E Package Builder to create an initial installation package, then deploy this installation package to your endpoint machines. For more information on deploying Forcepoint Endpoint, see the Installation and and Deployment Guide for Forcepoint F1E.

Important

- The wepsvc service must be running on the endpoint machine for auto-update to run properly.
- At the completion of any update, you must restart the endpoint to ensure the update takes effect.

Deploying an endpoint package on the auto-update server

Follow these steps to deploy a new package using the auto-update mechanism.

Steps

1) Create the package.

   Use the endpoint package builder to create a new package. The package builder generates a folder with several installation packages, one per each version of the operating system.

   Note: If you plan to use auto-update frequently, make sure that new packages point to an auto-update server. This option is configured on the Server Connection screen in the package builder:

   a) Select the Receive automatic software updates option.

   b) In the URL field, set up a URL for automatic updates:

      - If you have installed an Apache HTTPD server (Windows or Linux), the URL should be: http://<server:port>/EPUpdate/update
      - If you have installed an IIS server, the URL should be http://<server:port>/EPUpdate/update.bat

   c) In the How often should endpoint clients check for updates field, set up a schedule for how often the endpoint machines should check for updates. Forcepoint recommends setting this option 10 minutes.

2) Add package metadata:

   a) On the management server, open a command prompt and change to the %DSS_HOME% directory:

   cd %DSS_HOME%

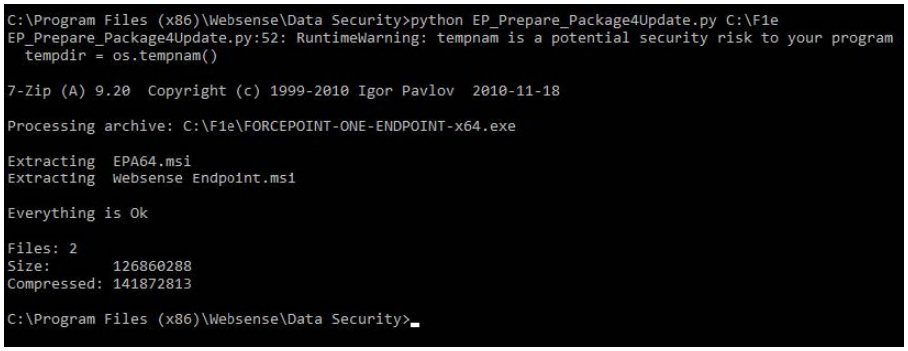
   Note

   This document refers to the Forcepoint DLP folder as %DSS_HOME%. The default %DSS_HOME% location is C:\Program Files (x86)\Websense\Data Security, but may be a different location based on your specific installation.

   b) Run the following command (in a single line):

   python EP_Prepare_Package4Update.py <Path-to-folder-withpackages>

   where <Path-to-folder-with-packages> is the location of the Forcepoint F1E package created in the previous step.



   After running this command, a new subfolder called .private is created inside the folder with the generated package. This subfolder contains metadata about the package.

3) Copy the package to the Web server machine:

   Copy the entire contents of the generated package folder (along with the .private folder containing the metadata) to the Web server machine (into EP_UPDATE_ROOT/data). For example, the Win32 installation will be located in EP_UPDATE_ROOT/data/FORCEPOINT-ONE-ENDPOINT-x32.exe.

   Be aware that if you copy an older endpoint package to the Web server (inadvertently or otherwise), the endpoint machine will download and install the older version.

4) Rename the executable files:

   The executable files in the EP_UPDATE_ROOT/data folder, as well as the metadata file in the .private folder, need to be renamed from FORCEPOINTONE- ENDPOINT to WebsenseEndpoint:

   - WebsenseEndpoint_32bit.exe
   - WebsenseEndpoint_64bit.exe
   - WebsenseEndpoint_32bit.exe.txt
   - WebsenseEndpoint_64bit.exe.txt

Result

Now your server is ready. Whenever there is a new Forcepoint DLP Endpoint release, copy the updated release binaries to your auto-update server, and the endpoints will update at the next scheduled time.

Important

At the completion of any endpoint update, you must restart the endpoint machine to ensure the update takes effect.

Auto-update workflow for advanced configuration

Read this section to understand the workflow of the endpoint auto-update process, how the endpoint and update server communicate with each other, and how you can add flexibility to the endpoint auto-update feature.

The endpoint machines check the management server for configuration updates to the data endpoint profile.

This is how the endpoint auto-update process works:

1) The endpoint sends a GET request URL to the auto-update server with local information that the server needs to identify the endpoint machine.

2) The auto-update server responds (in XML-like format) with information about the version of the endpoint installation package, as well as the desired version of the Forcepoint F1E.

3) If the desired Forcepoint DLP Endpoint version is different from the current version, Forcepoint DLP Endpoint downloads the installation package from the download URL that was sent as part of the server's response.

4) After the download is complete, the endpoint machine checks if it is ready to install the software.

   a) If the endpoint machine is ready, the installation package runs silently in the background.

   b) If the endpoint machine is not ready, it postpones the installation until the endpoint machine is ready.

How the endpoint and update server communicate

When the endpoint sends a GET request URL to the auto-update server, the URL contains many pre-defined parameters.

For example:

<UpdateServer URL= "http://download.forcepoint.com/update" />

GET/update?Bits=64bit&Platform=Windows&Domain=forcepoint.com&User=EPUser&SID=xxxxxx& LocalVersion=7.6.1218& LocalDSSVersion=7.6.3.16&ProtocalVersion=1.2&WSCookie=4f3h&DLP=Yes& WEB=Yes&RF=No&CI=No HTTP/1.1

Host: download.forcepoint.com

These parameters provide local information about the endpoint machine. The table below lists the parameters in the GET request URL sent by the endpoint and their description:

Name	Type	Description
Bits	String	Type of OS: 32- or 64-bit
Platform	String	Windows
User	String	First log on user name
Domain	String	Domain name
SID	String	Session ID of the first log on user
LocalVersion	String	Version number of the local Forcepoint F1E or Forcepoint DLP Endpoint
LocalDSSVersion	String	Version number of Forcepoint DLP
ProtocolVersion	String	Protocol version of the proxy server
WSCookie	String	Data received from the server
DLP	String	Whether the local machine has Forcepoint DLP Endpoint installed or not: Yes or No
WEB	String	Whether the local machine has Forcepoint Web Security Endpoint installed or not: Yes or No
RF	String	Whether the local machine has Remote Filtering Client installed or not: Yes or No
CI	String	Whether the local machine has the Citrix Integration service installed or not: Yes or No

Similarly, when the auto-update server returns a string in XML-like format, it also includes many pre-defined parameters. For example:

<?xml version="1.0" encoding="utf-8" ?>

<UpdateServer>

<CurrentVersion="7.6.1219">

<CurrentDSSVersion="7.6.3.17">

<CheckSum="A15BCDE9393288EFACDB3493827ABEFD">

<URL="http://download.forcepoint.com/upgrade/installpackage_1219.exe">

<IncludeEP="Yes">

<IncludeDSS="Yes">

</UpdateServer>

The table below provides descriptions of the elements in the XML-like file returned by the auto-update server:

Name	Type	Description
CurrentVersion	String	Version number of the designated installation package on server

Name	Type	Description
CurrentDSSVersion	String	Version number of the designated installation package on the server
CheckSum	String	MD5 checksum of the designated installation package on the server
URL	String	The URL of the installation package on server (maximum size: 2K)
IncludeEP	String	Whether the installation package shouldinclude endpoint software or not: Yes or No
IncludeDSS	String	Whether the installation package should include Forcepoint DLP software or not: Yes or No

Depending on the response of the update server, endpoints can retrieve the install package and install it silently.