



This document contains important information about this Windows driver release. Be sure to read this information before proceeding with the installation.

Fiery PostScript Driver version 5.0 has been released to support Windows 10.

OS Versions supported:

The Fiery PostScript Driver version 5.0 can be installed on the following Windows OS versions:

- Windows 7 (32 bit and 64 bit)
- Windows Server 2008 (32 bit and 64 bit)
- Windows Server 2008 R2
- Windows 8 (32 bit and 64 bit)
- Windows Server 2012 (32 bit and 64 bit)
- Windows Server 2012 R2
- Windows 10 (32 bit and 64 bit)

Installation:

Microsoft Windows 8 and later, including Windows 10, only allows installation of digitally signed drivers. To meet this requirement, the Fiery Driver installer includes EFI's VeriSign digital signature. By including EFI's digital signature, the user will not see the 'Windows Security' dialog box with the message, "Windows can't verify the publisher of this driver software".

Fiery Driver 5.0 includes the Fiery Driver Updater, which notifies the user when a driver update is available and allows the user to apply updates.

Disclaimer

This hardware, software/patches, or technology may contain cryptographic functions as defined in Article 8 (ix) (h) because the cryptographic capability is not user-accessible, and are designed to have only one or more of the following cryptographic functionality(ies):

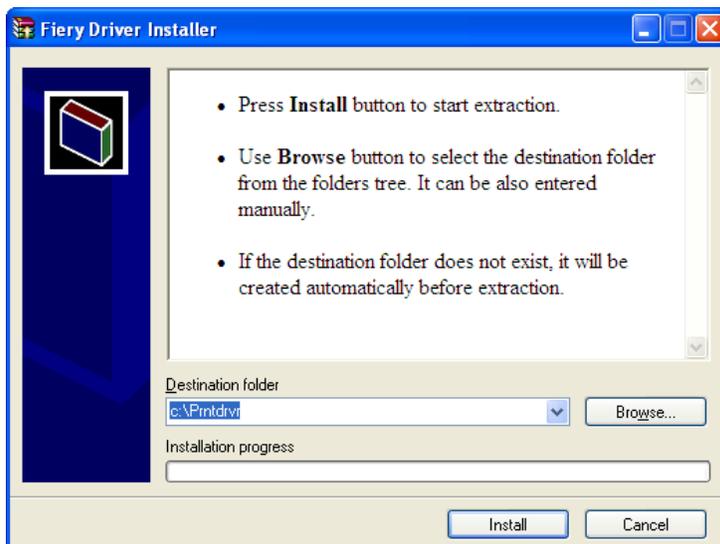
1. Functionality to execute copy-protected programs
2. Functionality to access to digital contents stored on copy-protected read-only media
3. Functionality to access to encrypted and memorized digital contents on a medium that will be sold to the public with the same content
4. Functionality for copying control of copyright protected audio/video data
5. Functionality to encrypt and/or decrypt to protect libraries, design attributes, or associated data for the design of semiconductor devices or integrated circuits

To begin installation:

1. Select the filename.zip file.
2. Right-click the .zip file.
3. Select 'Extract All'.
4. Click the "Show extracted files when complete" checkbox.
5. Click 'Extract'.

NOTE: Remember the location of the extracted files.

6. In the directory where the Fiery Driver files have been extracted, double-click the 'PRNTDRV.EXE' file to start the installation. The following screen will be displayed while the files are being extracted.



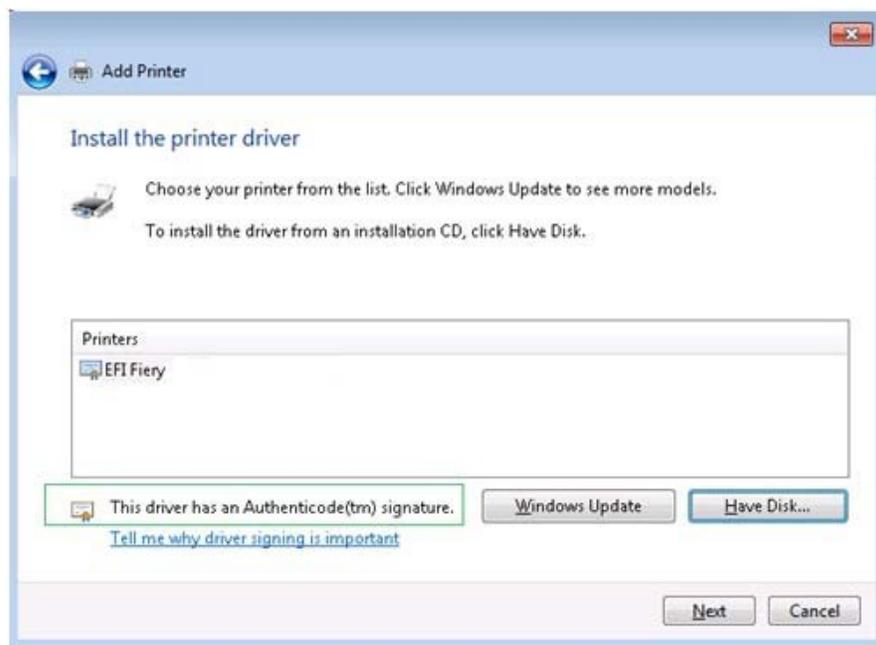
7. After extracting the Fiery Driver files, go to "Devices and Printers" in the 'Start' menu.
8. Click 'Add a Printer'.
9. Browse to the directory location of the extracted Fiery Driver files.

Disclaimer

This hardware, software/patches, or technology may contain cryptographic functions as defined in Article 8 (ix) (h) because the cryptographic capability is not user-accessible, and are designed to have only one or more of the following cryptographic functionality(ies):

1. Functionality to execute copy-protected programs
2. Functionality to access to digital contents stored on copy-protected read-only media
3. Functionality to access to encrypted and memorized digital contents on a medium that will be sold to the public with the same content
4. Functionality for copying control of copyright protected audio/video data
5. Functionality to encrypt and/or decrypt to protect libraries, design attributes, or associated data for the design of semiconductor devices or integrated circuits

10. Select the printer model/OEMSETUP.INF file for the driver to be installed. In the example below, the resulting dialog box will have a line at the bottom that says, “This driver has an Authenticode (™) signature.” This is EFI’s VeriSign signature that is included with the Fiery Driver.



Disclaimer

This hardware, software/patches, or technology may contain cryptographic functions as defined in Article 8 (ix) (h) because the cryptographic capability is not user-accessible, and are designed to have only one or more of the following cryptographic functionality(ies):

1. Functionality to execute copy-protected programs
2. Functionality to access to digital contents stored on copy-protected read-only media
3. Functionality to access to encrypted and memorized digital contents on a medium that will be sold to the public with the same content
4. Functionality for copying control of copyright protected audio/video data
5. Functionality to encrypt and/or decrypt to protect libraries, design attributes, or associated data for the design of semiconductor devices or integrated circuits

11. After selecting your printer, click 'Next'. The following dialog box will be displayed. By clicking the “Always trust software from EFI software” checkbox, this message will no longer be displayed on the current computer.



12. Follow the on-screen instructions to complete the installation.

Disclaimer

This hardware, software/patches, or technology may contain cryptographic functions as defined in Article 8 (ix) (h) because the cryptographic capability is not user-accessible, and are designed to have only one or more of the following cryptographic functionality(ies):

1. Functionality to execute copy-protected programs
2. Functionality to access to digital contents stored on copy-protected read-only media
3. Functionality to access to encrypted and memorized digital contents on a medium that will be sold to the public with the same content
4. Functionality for copying control of copyright protected audio/video data
5. Functionality to encrypt and/or decrypt to protect libraries, design attributes, or associated data for the design of semiconductor devices or integrated circuits