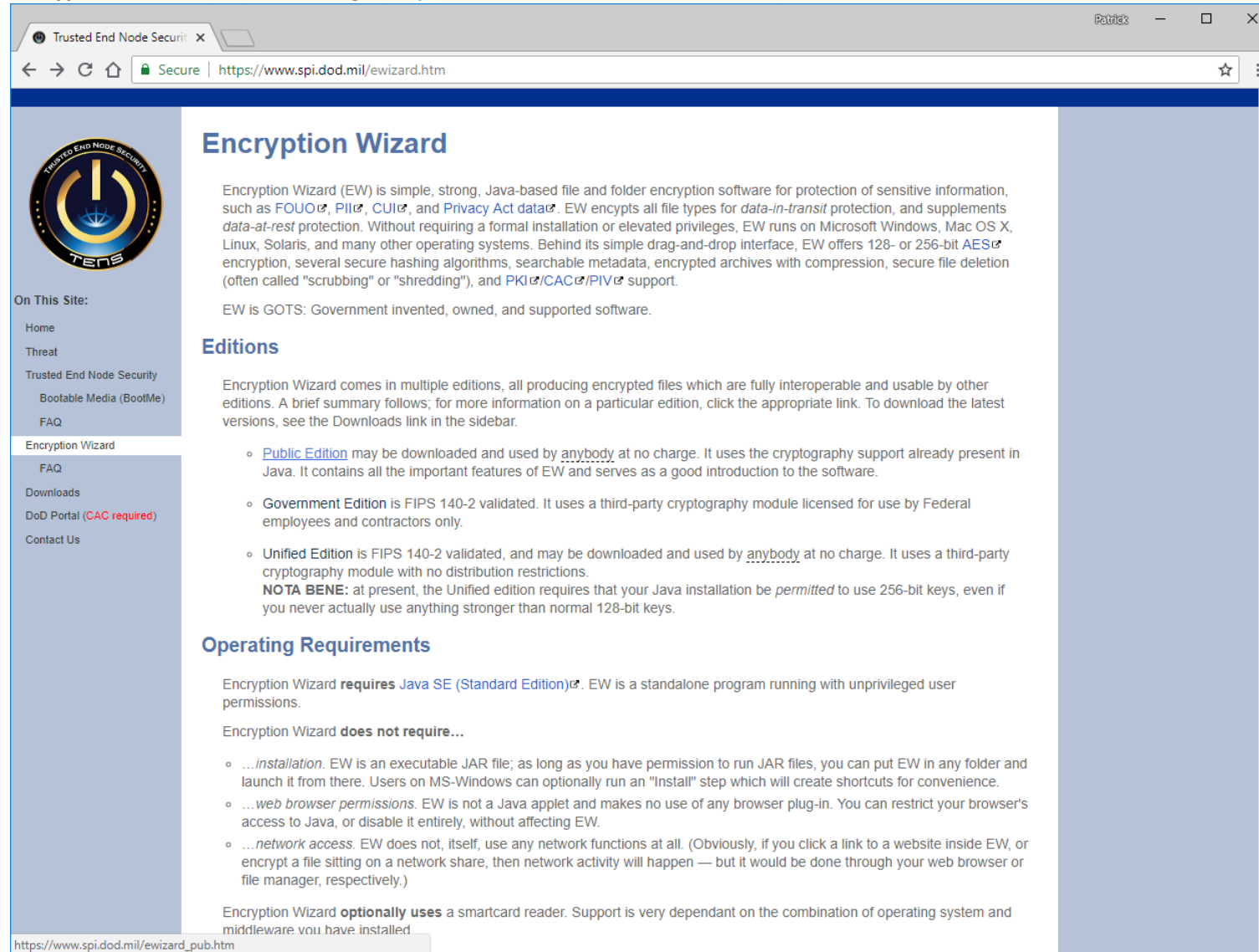


Trusted End Node Security (TENS) Home Page (<https://www.tens.af.mil/index.htm>):


Trusted End Node Security (TENS™) technology is developed and managed by the Air Force Research Laboratory (AFRL) Information Directorate. This program began as the Anti-Tamper Software Protection Initiative in 2001 with its flagship products Lightweight Portable Security and Encryption Wizard. The TENS™ program office offers products that provide network security from the end node perspective while providing user capabilities of remote access, secure web browsing, and file/folder encryption, in addition to other initiatives. The core products sustained by the TENS™ program are TENS-Public, TENS-Professional, Bootable Media, and various forms of Encryption Wizard. These products are intended to be used by the U.S. Department of Defense and the rest of the Federal government, while also providing Public versions of the software to the open source community, when possible. The Public versions are available for download on our website and are not customized. AFRL has a strong legacy of providing secure end node technology, with a supported user base in the hundreds of thousands. Please navigate the sidebar to learn more about the products managed by the TENS™ program office.

Encryption Wizard (EW) Home Page (<https://www.tens.af.mil/ewizard.htm>):



Trusted End Node Security

Secure | <https://www.spi.dod.mil/ewizard.htm>



Encryption Wizard

Encryption Wizard (EW) is simple, strong, Java-based file and folder encryption software for protection of sensitive information, such as FOUO, PII, CUI, and Privacy Act data. EW encrypts all file types for *data-in-transit* protection, and supplements *data-at-rest* protection. Without requiring a formal installation or elevated privileges, EW runs on Microsoft Windows, Mac OS X, Linux, Solaris, and many other operating systems. Behind its simple drag-and-drop interface, EW offers 128- or 256-bit AES encryption, several secure hashing algorithms, searchable metadata, encrypted archives with compression, secure file deletion (often called "scrubbing" or "shredding"), and PKI/CAC/PIV support.

EW is GOTS: Government invented, owned, and supported software.

Editions

Encryption Wizard comes in multiple editions, all producing encrypted files which are fully interoperable and usable by other editions. A brief summary follows; for more information on a particular edition, click the appropriate link. To download the latest versions, see the Downloads link in the sidebar.

- [Public Edition](#) may be downloaded and used by anybody at no charge. It uses the cryptography support already present in Java. It contains all the important features of EW and serves as a good introduction to the software.
- Government Edition is FIPS 140-2 validated. It uses a third-party cryptography module licensed for use by Federal employees and contractors only.
- Unified Edition is FIPS 140-2 validated, and may be downloaded and used by anybody at no charge. It uses a third-party cryptography module with no distribution restrictions.
NOTA BENE: at present, the Unified edition requires that your Java installation be *permitted* to use 256-bit keys, even if you never actually use anything stronger than normal 128-bit keys.

Operating Requirements

Encryption Wizard **requires** Java SE (Standard Edition). EW is a standalone program running with unprivileged user permissions.

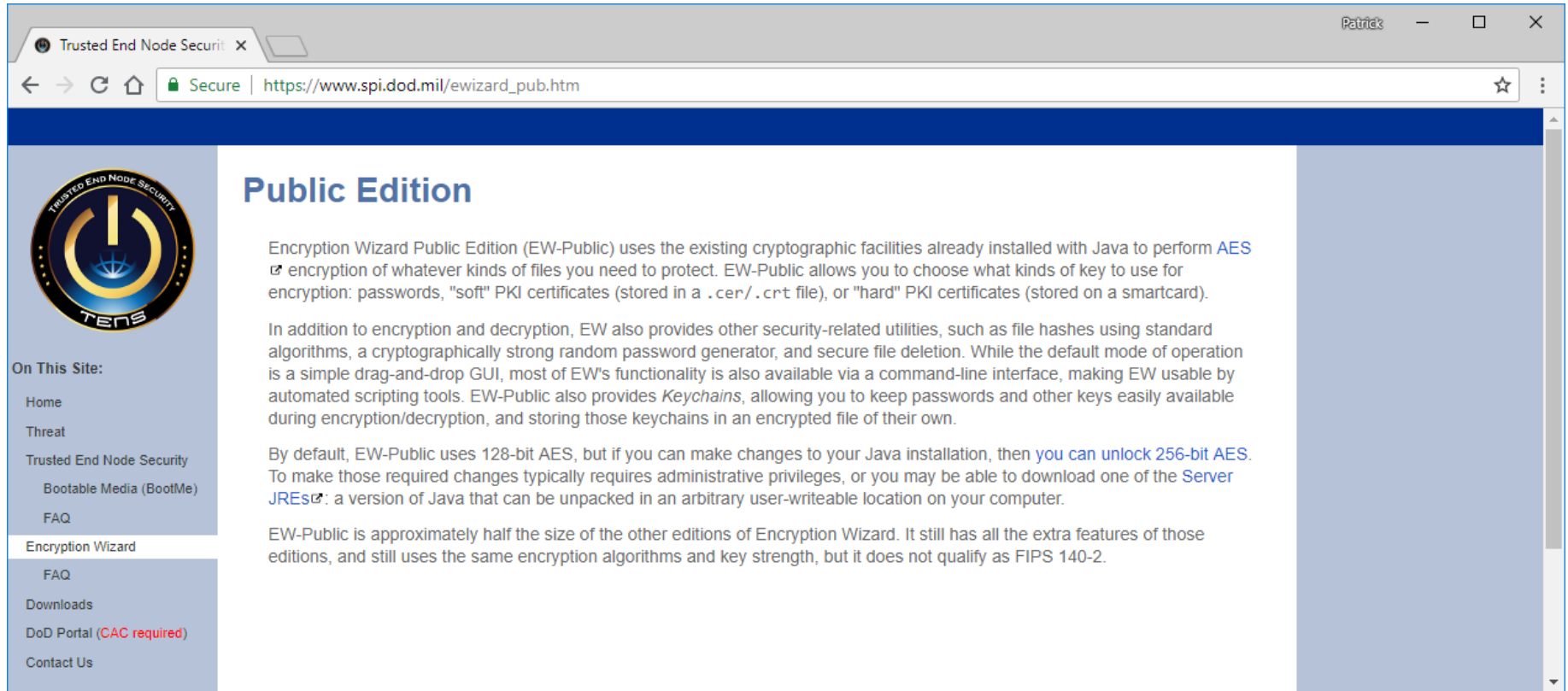
Encryption Wizard **does not require...**

- ...installation.* EW is an executable JAR file; as long as you have permission to run JAR files, you can put EW in any folder and launch it from there. Users on MS-Windows can optionally run an "Install" step which will create shortcuts for convenience.
- ...web browser permissions.* EW is not a Java applet and makes no use of any browser plug-in. You can restrict your browser's access to Java, or disable it entirely, without affecting EW.
- ...network access.* EW does not, itself, use any network functions at all. (Obviously, if you click a link to a website inside EW, or encrypt a file sitting on a network share, then network activity will happen — but it would be done through your web browser or file manager, respectively.)

Encryption Wizard **optionally uses** a smartcard reader. Support is very dependant on the combination of operating system and middleware you have installed.


https://www.spi.dod.mil/ewizard_pub.htm

Encryption Wizard Public Edition (EW-Public) Page (https://www.tens.af.mil/ewizard_pub.htm):



Trusted End Node Security X Patrick

Secure | https://www.spi.dod.mil/ewizard_pub.htm



Public Edition

Encryption Wizard Public Edition (EW-Public) uses the existing cryptographic facilities already installed with Java to perform [AES](#) encryption of whatever kinds of files you need to protect. EW-Public allows you to choose what kinds of key to use for encryption: passwords, "soft" PKI certificates (stored in a .cer/.crt file), or "hard" PKI certificates (stored on a smartcard).

In addition to encryption and decryption, EW also provides other security-related utilities, such as file hashes using standard algorithms, a cryptographically strong random password generator, and secure file deletion. While the default mode of operation is a simple drag-and-drop GUI, most of EW's functionality is also available via a command-line interface, making EW usable by automated scripting tools. EW-Public also provides *Keychains*, allowing you to keep passwords and other keys easily available during encryption/decryption, and storing those keychains in an encrypted file of their own.

By default, EW-Public uses 128-bit AES, but if you can make changes to your Java installation, then [you can unlock 256-bit AES](#). To make those required changes typically requires administrative privileges, or you may be able to download one of the [Server JREs](#): a version of Java that can be unpacked in an arbitrary user-writeable location on your computer.

EW-Public is approximately half the size of the other editions of Encryption Wizard. It still has all the extra features of those editions, and still uses the same encryption algorithms and key strength, but it does not qualify as FIPS 140-2.

On This Site:

- Home
- Threat
- Trusted End Node Security
 - Bootable Media (BootMe)
 - FAQ
- Encryption Wizard
 - FAQ
 - Downloads
 - DoD Portal (CAC required)
 - Contact Us

Encryption Wizard Download Page (<https://www.tens.af.mil/download.htm#ew>):

Encryption Wizard (EW)

Make sure you choose the edition that's right for your needs!

Read the [Release Notes and version history](#).

Version 3.5.3, released 26 Sep 2018:

- ✔ [Encryption Wizard, Public Edition](#)
8.7 MiB
- [Encryption Wizard, Government FIPS Edition](#)
This is automated and is the quickest way to obtain the Government FIPS edition. Internet Explorer and a DoD CAC are required; if you do not have both, fill out the request form below.
13.0 MiB
- ✔ [Encryption Wizard, Unified Edition](#)
12.0 MiB

Version 3.5.2, released 04 May 2018:

- ✔ [Encryption Wizard, Public Edition](#)
4.7 MiB
- [Encryption Wizard, Government FIPS Edition](#)
This is automated and is the quickest way to obtain the Government FIPS edition. Internet Explorer and a DoD CAC are required; if you do not have both, fill out the request form below.
8.0 MiB

On This Site:

- Home
- Threat
- Trusted End Node Security
 - Bootable Media (BootMe)
 - FAQ
- Encryption Wizard
 - FAQ

Downloads

- DoD Portal (CAC required)
- Contact Us

Recommendation: Manufacturers obtain the Public Edition (download file: "EncryptionWizard-Public-3.5.3.zip").

Encryption Wizard FAQ Page (<https://www.tens.af.mil/ewizardFAQ.htm>):

Trusted End Node Security x

Patrick

Secure | <https://www.tens.af.mil/ewizardFAQ.htm>

Encryption Wizard Frequently Asked Questions

On This Site:

- Home
- Threat
- Trusted End Node Security
 - Bootable Media (BootMe)
 - FAQ
 - Encryption Wizard
 - FAQ
- Downloads
- DoD Portal (CAC required)
- Contact Us

▼ Download and Installation Issues Collapse All

- My MacOS X says I don't have permission to open the EW .jar file!
- The internet says Java is full of security holes! How can I protect myself?

▼ Government FIPS versus Public

- I work for the DoD or U.S. Government...
- ...but my colleague is an offsite contractor. What now?
- ...and I forgot my password.
- ...and I want to exchange encrypted files with a Foreign Government Partner.
- ...and my EW doesn't look like the screenshots in your manual.

▼ Operational Issues

- Why can't Encryption Wizard read my CAC/PIV/smartcard?
- Why is the 256-bit AES option disabled?

▼ Feature-related Questions

- Can I make a self-extracting encrypted file?

▼ Common Issues, Known Problems, Other Questions

- Why can't I use a smartcard under 64-bit Microsoft Windows?
- I got an Error 17 while decrypting this enormous file. Why?
- How do I know your software isn't full of backdoors?

/

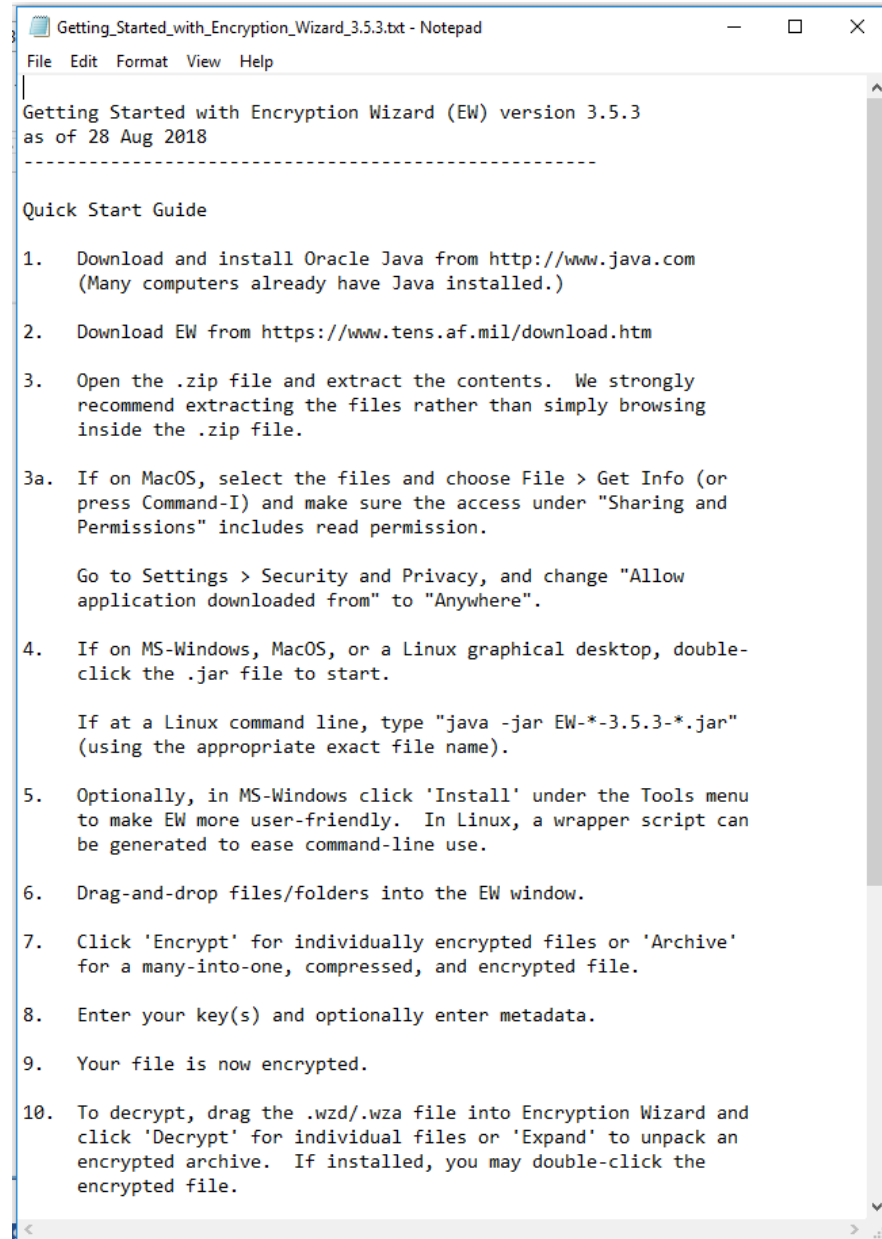
Files in folder "EncryptionWizard-3.5.3" after unzipping "EncryptionWizard-Public-3.5.3.zip":

The screenshot shows the WinZip Enterprise interface with the folder 'EncryptionWizard-Public-3.5.3' open. The left sidebar shows navigation options like 'Files', 'Frequent Folders', 'This PC', 'Network', and 'Homegroup'. The main pane displays a list of four files:

File Name	Type	Date modified	Size
Encryption Wizard homepage.url	Internet Shortcut	9/26/2018 4:03 PM	135 bytes → 118 bytes
Encryption Wizard User Manual v353.pdf	Adobe Acrobat Document	9/26/2018 4:03 PM	1.26 MB → 1.08 MB
EW-Public-3.5.3.jar	Executable Jar File	9/26/2018 4:03 PM	7.90 MB → 7.58 MB
Getting_Started_with_Encryption_Wizard_3.5.3.txt	Text Document	9/26/2018 4:03 PM	2.32 KB → 1.20 KB

At the bottom of the file list, it indicates '4 item(s)' and 'Zip File: 4 item(s), 8.66 MB'. The right sidebar contains 'Actions' such as 'Unzip All Files', 'Convert & Protect Files' (with options for Encrypt, Reduce Photos, Convert to PDF, and Watermark), and 'Save or Share Zip'.

Contents of file "Getting_Started_with_Encryption_Wizard_3.5.2.txt":



Getting Started with Encryption Wizard (EW) version 3.5.3
as of 28 Aug 2018

Quick Start Guide

1. Download and install Oracle Java from <http://www.java.com>
(Many computers already have Java installed.)
2. Download EW from <https://www.tens.af.mil/download.htm>
3. Open the .zip file and extract the contents. We strongly recommend extracting the files rather than simply browsing inside the .zip file.
- 3a. If on MacOS, select the files and choose File > Get Info (or press Command-I) and make sure the access under "Sharing and Permissions" includes read permission.

Go to Settings > Security and Privacy, and change "Allow application downloaded from" to "Anywhere".
4. If on MS-Windows, MacOS, or a Linux graphical desktop, double-click the .jar file to start.

If at a Linux command line, type "java -jar EW-*-3.5.3-*.jar"
(using the appropriate exact file name).
5. Optionally, in MS-Windows click 'Install' under the Tools menu to make EW more user-friendly. In Linux, a wrapper script can be generated to ease command-line use.
6. Drag-and-drop files/folders into the EW window.
7. Click 'Encrypt' for individually encrypted files or 'Archive' for a many-into-one, compressed, and encrypted file.
8. Enter your key(s) and optionally enter metadata.
9. Your file is now encrypted.
10. To decrypt, drag the .wzd/.wza file into Encryption Wizard and click 'Decrypt' for individual files or 'Expand' to unpack an encrypted archive. If installed, you may double-click the encrypted file.

Contents of file "Encryption Wizard User Manual v352.pdf":

Air Force Research Laboratory

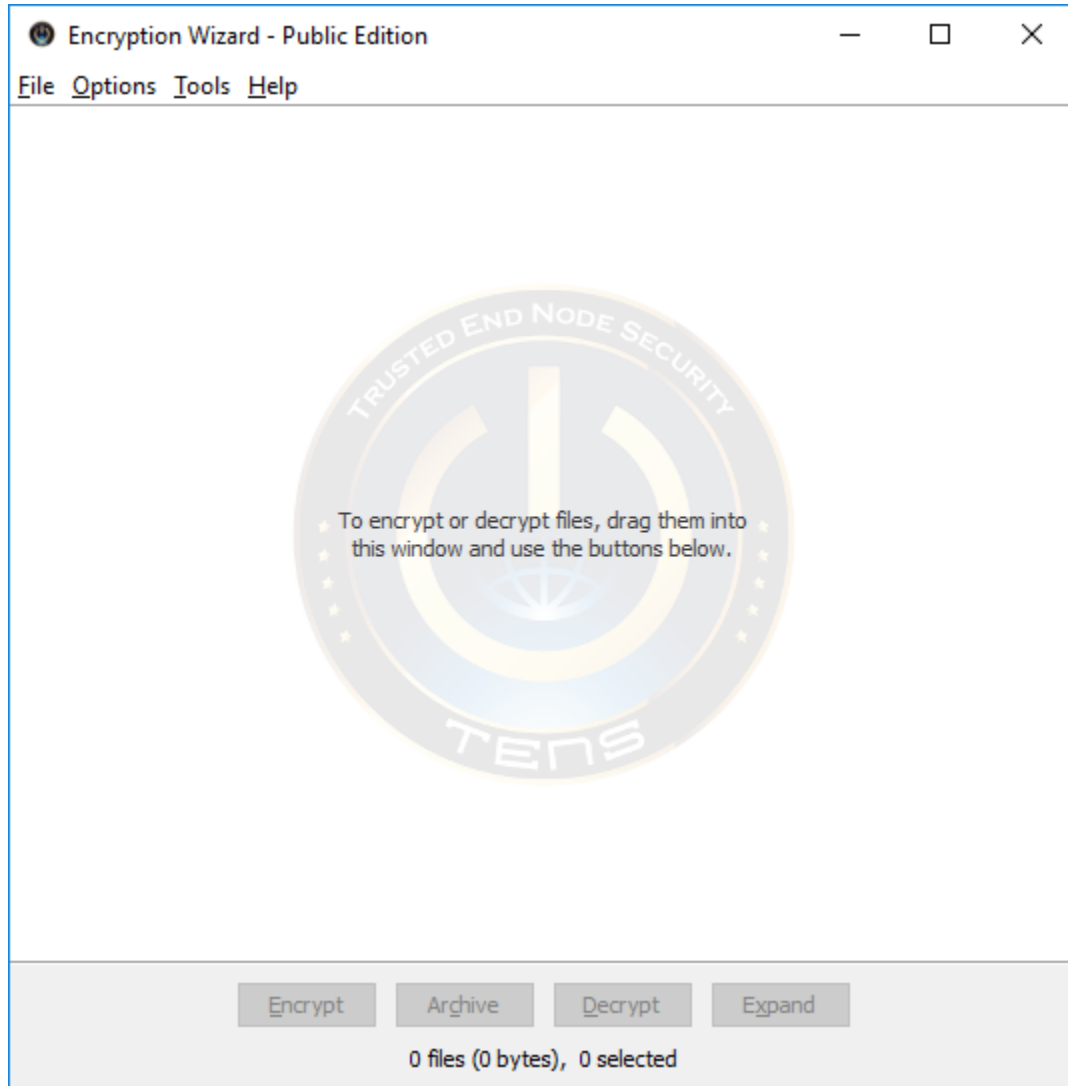
Trusted End Node Security (TENS) Encryption Wizard (EW) User's Guide

Version 3.5.3 – 28 Aug 2018

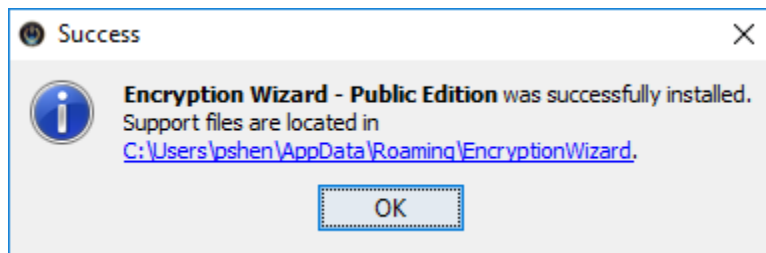
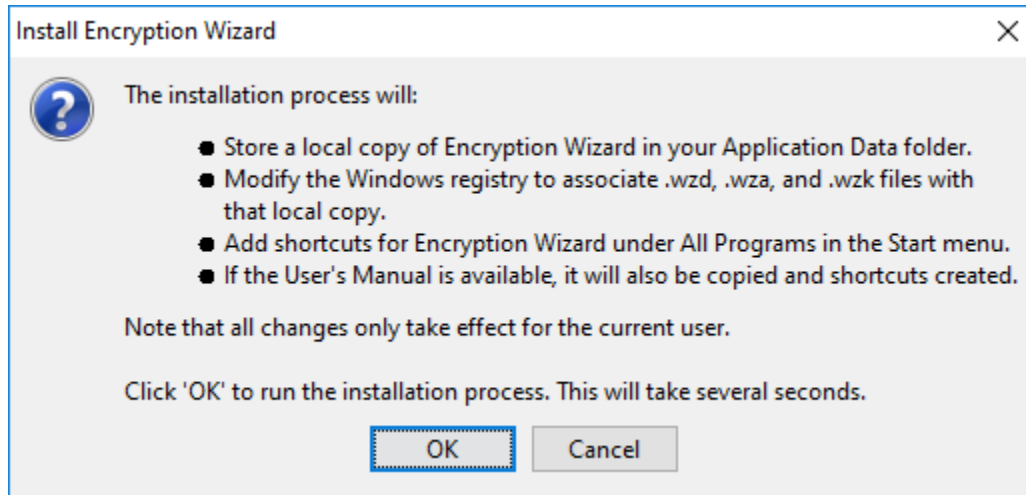


Distribution A: Approved for public release; distribution is unlimited [88ABW-12-0630]. Refer other requests to the TENS program office, AFRL/RIEB, TENS@us.af.mil, 525 Brooks Rd, Rome, NY 13441.

Start EW for the first time by running (i.e., double-clicking) file "EW-Public-3.5.3.jar":



Optional: Take the following steps to install EW on a Windows PC (in default location "C:\Users\xxxxx\AppData\Roaming\EncryptionWizard"):
Tools → Platform Support: MS-Windows → Install shortcut... → OK.

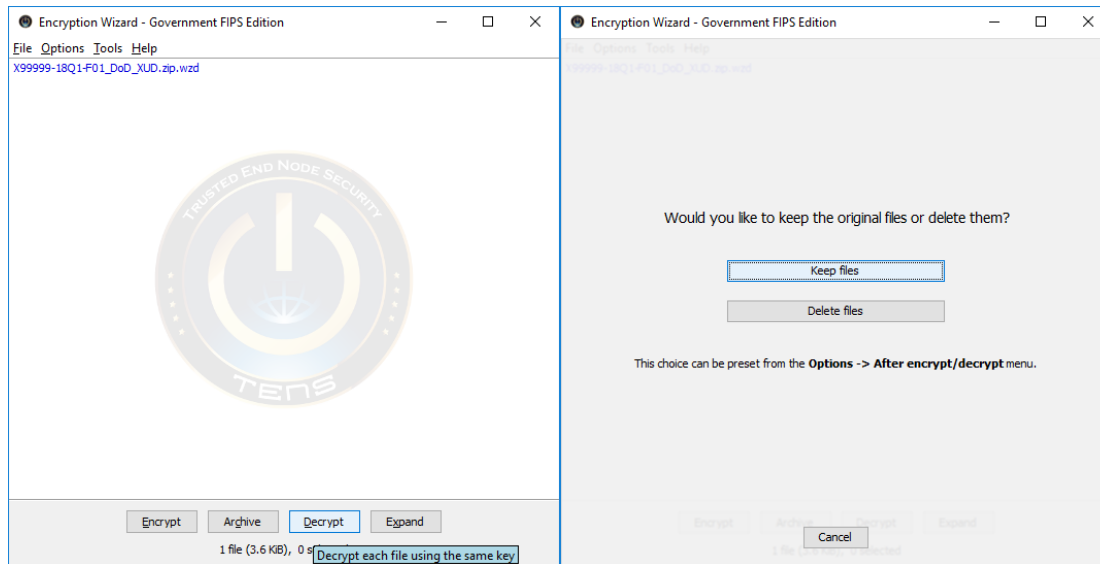
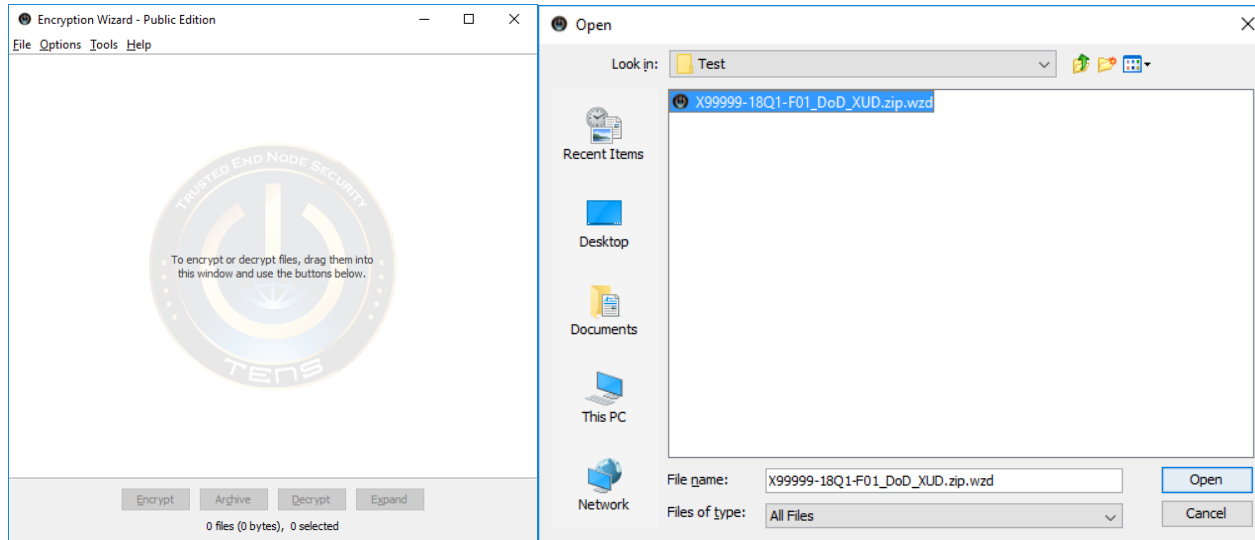


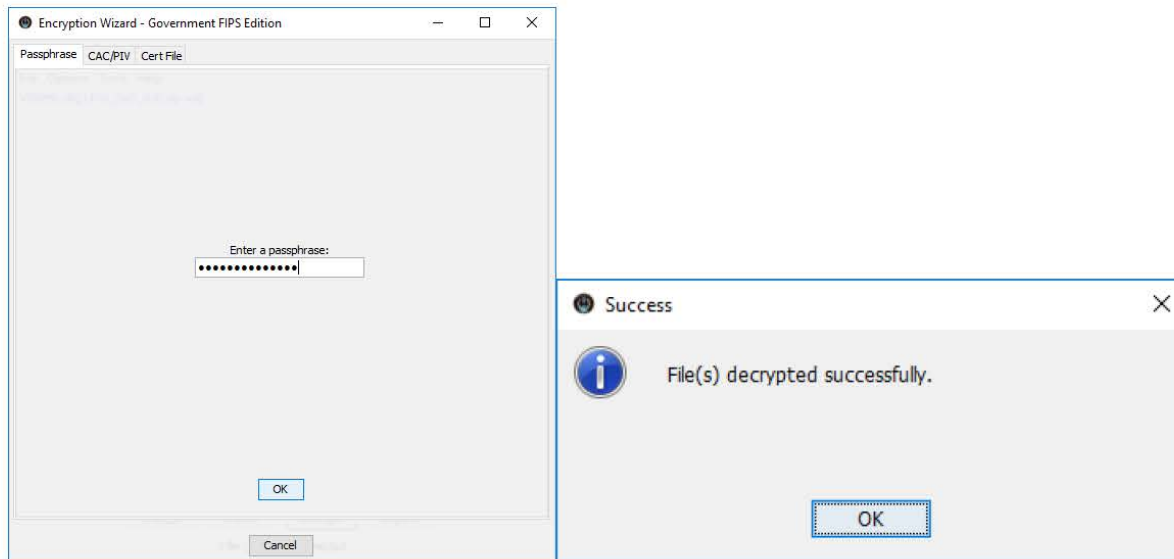
There should be no needs to make any changes to the default settings.

Once installed, EW can be started on a Windows PC by double-clicking the "EW-Public-3.5.3.jar" shortcut in the Start menu.

To decrypt an EW-encrypted file from DHA (e.g., "X99999-18Q2-F01_DoD_XUD.zip.wzd" in folder "...\Test"), start EW and then:

File → Add file/directory → locate and Open file "...\Test\X99999-18Q2-F01_DoD_XUD.zip.wzd" → Decrypt → enter the passphrase provided by DHA → OK → Keep files.





A decrypted file (“X99999-18Q2-F01_DoD_XUD.zip”) will be created by EW in the same folder (“...\Test”) as the encrypted file (“X99999-18Q2-F01_DoD_XUD.zip.wzd”).