FIPS 140-2 Certification and Compliance with WinZip

- WinZip Enterprise

Note: The FIPS 140-2 compliance feature requires a **WinZip** Enterprise registration.
Starting with WinZip version 18.5, WinZip Courier version 7.0, and WinZip Command Line Support Add-on version 5.0, WinZip Enterprise can be deployed to take advantage of the Windows FIPS 140-2 validated cryptographic modules when they have been enabled for use on various Windows systems through the local or group security policy. When configured this way, WinZip satisfies all Federal requirements to ensure your organization meets government requirements for FIPS 140-2 certified encryption, both at rest and during exchanges.

About FIPS 140-2

The **Federal Information Processing Standard (FIPS) Publication 140-2** is a U.S. government standard. FIPS is based on Section 5131 of the Information Technology Management Reform Act of 1996. It defines the minimum security requirements for cryptographic modules in IT products, which are validated by Cryptographic Module Validation Program (CMVP).

FIPS 140-2 is a set of governmental regulations. It is not an encryption method or file service. Currently, a Zip file created with the FIPS settings turned on looks no different than other encrypted Zip files.

In WinZip itself that the only encryption method you can use in WinZip is AES 256. So, if you have not entered a GPO to force that situation and that is what you find, you must have FIPS turned on.

WinZip FIPS 140-2 uses certification/validation provided by Microsoft Federal Information Processing Standard (FIPS) 140.

Link to the FIPS Validation Certificate: FIPS Validation Certificate

WinZip can be configured to follow the Windows FIPS security policy or it can be configured itself for FIPS 140-2 compliancy. In either case, WinZip operates in FIPS-approved mode, using only the FIPS 140 approved algorithms for hashing and encryption that are provided by the FIPS-validated Windows cryptographic modules. Also, WinZip supports only the AES method for both encryption and decryption when in this mode.

WinZip's FIPS support can be adjusted to the requirements of your organization. Both a Strict mode and a Relaxed mode are available options.

When the Windows FIPS 140 compliancy is disabled, WinZip uses its own cryptographic modules to provide both AES and Zip 2.0 encryption methods. As with earlier versions of WinZip, these modules are not FIPS 140-2 compliant, though they provide FIPS 197 certified AES encryption technology and implementation. Similarly, for WinZip Enterprise versions and versions earlier than 18.5, neither WinZip nor any of its modules are FIPS 140-2 compliant but earlier versions, when using AES encryption, are FIPS 197 certified.

Implementing FIPS 140-2 Standard with WinZip Enterprise

These are the five usage scenarios of FIPS 140-2 with WinZip:

SharePoint Environment

Installing and using WinZip Enterprise in a domain where SharePoint is the only cloud service made available.

Amazon S3 Environment

Installing and using WinZip Enterprise in a domain where Amazon S3 and Office 365 (OneDrive for Business) are the only cloud services being made available.

Prepare for FIPS 140-2 Compliance

Installing and using WinZip Enterprise as part of a FIPS 140-2 compliant Windows solution. When choosing to encrypt, each Zip file being created will have AES 256-bit encrypted data and certified Windows components will be used for all encrypting of data. This scenario has no cloud services, and no social media usage. Converting to PDF and placing a watermark on files also protects files that you zip.

Multiple Cloud Access Environment

Installing and using WinZip Enterprise in a domain where multiple cloud services are made available, SharePoint being the default.

Use group policy and remove Social Media options

Install WinZip Enterprise by Group Policy and give the maximum feature set to the “Marketing OU”, but remove Social Media options for those who are not in the Marketing organization unit. No default cloud service or share service will be defined. When available, users will be able to set those on their own. The password policy will be the WinZip default, which is a length of 8 characters, and the Password Policy tab in WinZip Options will be available.

The above scenarios are described in the WinZip Enterprise Installation and Configuration Guide, which includes a description, installation preparation, installation steps, and additional information.
