

Sending Files to Viasystems Americas via Secure FTP

TECHNICAL BULLETIN

OVERVIEW

When sending files to Viasystems Americas sites, the following secure transfers are supported:

- Implicit FTPS with SSLv3 or TLS encryption to ftps.viasystems.com
- HTTPS with SSLv3 or TLS encryption to <https://ftps.viasystems.com>
- SFTP with SSHv2 encryption to ftps.viasystems.com

When connecting for the first time using a secure option, you will need to verify and accept or install the security certificate or fingerprint. If the fingerprint does not match the values listed below, please contact Viasystems Help Desk. For SSLv3 or TLS encryption used by Implicit FTPS and HTTPS, the security certificate for the Viasystems FTP server is:

Public Key: RSA (1024 bits)

Issuer: CN=ftps.viasystems.com
OU=Information Technology
O=Viasystems Group, Inc.
L=St. Louis S=MO C=US

Subject: CN=ftps.viasystems.com
OU=Information Technology
O=Viasystems Group, Inc.
L=St. Louis S=MO C=US

Valid From: 05/13/2011

Valid To: 05/10/2021

SHA1 Fingerprint:

e0:74:59:5b:74:83:da:3e:20:0a:11:47:ea:8d:33:34:e1:ce:5f:45

MD5 Fingerprint:

ab:27:29:a3:79:81:55:72:9c:54:dc:c4:ef:e8:53:3c

For SSHv2 encryption used by SFTP, the fingerprint for the Viasystems FTP server is:

22:dc:82:d9:5f:b7:ea:0c:aa:50:ce:2d:8f:cf:00:23

After verifying the fingerprint, use your company's given username and password to log in.

To get a username and password, please contact Viasystems Help Desk: (503) 992-4444
helpdesk@viasystems.com .

Sending Files to Viasystems Americas via Secure FTP

- Please create a text file (i.e. README) listing the filenames being sent and the content or function for each file in the dataset. Include the intended purpose of the file being sent, i.e. quote, purchase order, DFM etc. Also, include the engineering and/or purchasing contact information and any special instructions.
- Please use a routine to encapsulate all files (one output file per board design) and compress the dataset. Use a unique naming convention for the compressed file so multiple parts can be sent but will not overwrite each other.
- Please use the following extensions for encapsulated files: zip (.zip or .exe), Gzip (.gz), tar (.tar), compress (.Z), tar/Gzip (.tgz), PGP (.pgp), and RAR (.rar). Multiple routines may be used if corresponding extensions are appended to the filename.
- The name of the encapsulated file must be made of only alphanumeric, ".", "_", and "-". It should not begin with a "." or "-".
- **Files which contain ITAR board designs should be uploaded into the "itar" subdirectory.**

Make sure that you set your transfer type to "binary" when sending compressed files. You may send several at once (i.e. mput *.zip). Again, please make sure that everything you send is compressed for convenience and saving both time and bandwidth on the network.

If you have any questions or problems regarding the file transfer, please contact Viasystems Help Desk: (503) 992-4444 helpdesk@viasystems.com .

Preferred Transfer Method and Format

- Internet transfer FTP, HTTP, Implicit, SFTP, and HTTPS
- E-Mail: Please contact Viasystems Customer Service before e-mailing files
- CD

Data Package Options

If data compression is used, a description of the compression technique should be included with the data set. Data should be packaged into a single file in one of the following formats.

- zip (all platforms)
- Gzip (.gz)
- tar (UNIX) with standard compression applied
- PGP (encryption)
- tar/Gzip (.tgz)
- Compress (UNIX)
- RAR (.rar)

Information Files

Special Instructions - Examples:

- Stencil file/film delivery instructions
- Electrical test instructions
- Customer identified test point image file(s)
- Special notes for manufacturing
- Explanation of drawing changes or partial design changes