Forcepoint

Datasheet

Forcepoint File Transfer Utilities

Utility pack for moving, mirroring and scheduling file transfers between file stores

Key Benefits

- Simple setup—intuitive GUI and configuration
- Normal and advanced user interface modes
- Automatic checking for the presence of file locks prior to file transfer
- Configurable maximum file size
- Configurable delay and retry intervals
- Multiple concurrent Scraper/ Droppers
- Multiple concurrent mirrors
- Allow list and block list files to process (REGEX support)
- Import and export Scraper/Dropper configurations
- Import and export Mirror TX/Mirror RX configurations
- SSL support

Operating System

- Linux
- Windows

Forcepoint's File Transfer utilities are used to move, mirror, and schedule file transfers between file stores via a Forcepoint Information eXchange (iX) or Forcepoint Policy Engine Guard.

Files are transferred using the Forcepoint File Sharing Protocol (FFSP), a compact and highly secure, efficient proprietary protocol with built-in error checking and re-try capabilities. When used in conjunction with iX, files are transformed using Forcepoint Zero Trust Content Disarm and Reconstruction (CDR) technology. When used in conjunction with a Policy Engine Guard, files are subject to Deep Content Inspection and rigorous policy enforcement.

File Moving

The Mover utility comprises two components – Scraper and Dropper. The Scraper service runs on the source host and the Dropper service runs on the destination host. The Scraper service watches one or more file stores for files to appear. As new files appear, they are passed to iX or the Policy Engine Guard using the FFSP protocol. Once sent, the files are deleted from the watched file store. The Dropper service receives the files on the target host and drops them into a destination folder, preserving the original file path from the root folder.

File Mirroring

The Mirror utility comprises two components – Mirror TX and Mirror RX. The Mirror TX service runs on the server hosting the source file store. The Mirror RX service runs on the server hosting the target file store. Mirroring can be initiated interactively or via script.

During mirroring, the Mirror TX service sends update information to the Mirror RX service, to maintain the mirror's structure and content. The files and update information are passed to iX or the Policy Engine Guard using the FFSP protocol.

Interconnection Requirements

Each pair of networks must be connected by a Forcepoint iX appliance and/or a Policy Engine Guard to enforce the network separation and to control the content of files transferred.

The iX appliance can be a:

→ virtual appliance running on ESXi or KVM (e.g. Proxmox)
→ physical appliance
→ high-assurance physical appliance that includes a High Speed Verifier (HSV) hardware logic verifier unit

The Policy Engine Guard is a software package that runs on CentOS/Red Hat Linux. A single iX appliance or Policy Engine Guard is typically sufficient to handle the traffic generated by an instance of the File Transfer Utilities running on a single server.

Server Requirements

An instance of the File Transfer Utilities is needed on each network. Windows and Linux are supported. A minimal system install is sufficient.

For more information visit Forcepoint Information eXchange (iX) appliance →

forcepoint.com/contact

Forcepoint