Personal File Exchange (PX)

Stop Malware.
Prevent Leaks.
Allow users to copy files between disconnected networks.

PX is a Personal Exchange application, allowing a user with a footprint on two separate networks to send files from one network to themselves on the other network.

It is deployed with an iX Appliance to ensure delivered files are rendered completely safe by Deep Secure's Threat Removal technology, and/or a Policy Engine Guard for Deep Content Inspection and rigorous policy enforcement.

Use Cases

PX can be employed where the user:

- has "swivel chair" access to two or more disconnected networks;
- uses a form of remote desktop access, including Garrison SAVI, from their protected network to reach a Virtual Desktop Infrastructure on an untrusted connected network;
- accesses the Internet from a protected system using a Garrison SAVI remote browsing solution.

PX can be configured to allow bi-directional file transfers or only permit one-way transfers.

Authentication

Users can authenticate to the PX application:

- using Windows Integrated Authentication for single sign on;
- using a simple username/password; or
- seamlessly with Garrison remote browsing integration.

The PX application components authenticate to each other using HTTPS with mutual authentication.

Review and Release Control

Where PX is used to pass information out of a system handling sensitive information, it can be configured to:

- require a second person to review released files;
- retain a full audit log that includes the content of all transferred files;
- check to ensure files have appropriate security labels, where the file format supports this.

Desktop Requirements

A modern HTML5 browser is used to access the PX web app.

For single-sign-on, the users' workstations must run Windows and be on-domain, and the browser must support IWA.

With Garrison SAVI remote browsing, the user needs a Windows desktop that supports the Garrison App.

Interconnection Requirements

Each pair of networks must be connected by a Deep Secure 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 an HSV hardware logic verifier unit.

The Policy Engine Guard is a software package that runs on CentOS 7 / Red Hat Linux.

A single iX Appliance or Policy Engine Guard is typically sufficient to handle the file transfer traffic generated by the size of user community that is handled by a single server.

Users' files can alternatively be delivered into a simple file store or to a service via a WebDAV interface.

Server Requirements

A PX server is generally needed on each network. Windows and Linux are supported. A minimal system install is sufficient.

With Garrison SAVI remote browsing a PX server is required on the protected network only.

A single PX server, with 4 cores and 16G RAM, can handle 750 concurrent users, but additional RAM may be required to accommodate files in transit. Disk space is required to meet operating system needs and to store all files in transit at any one time. Further disk storage will be needed if journalling is enabled.

Scaling

Multiple PX servers and multiple iX Appliances and Policy Engine Guards can be deployed together in farms to support more users and a provide a non-stop service. In this case a resilient shared file store is required to hold all the files in transit, such as GlusterFS on Linux or DFS on Windows.

Learn More

For more information on how PX is deployed with the Deep Secure Information Exchange (iX) Appliance or Policy Engine Guard, visit **www.deep-secure.com.**

Key Benefits

- Secure file transfers between isolated networks
- Review and release control mechanism
- Windows Integrated Authentication
- Simple setup – software package installs with minimal configuration
- Simple usage – Web App or close integration with Garrison remote browsing
- Choice of operating system platforms – Windows or Linux
- Scalable and non-stop operation