

PeerLock

PeerLock secures a user's files across a network of machines, ensuring that all copies of the files are locked while the user has them open. The network file locking afforded by PeerLock protects against multiple revisions occurring simultaneously on different machines.

When a user opens a file in a watched folder on his/her local machine, the file is immediately locked on the other machines specified in the user selection list. Other users cannot make modifications to this file. When the user closes the file, the files residing on the other machines are immediately unlocked, and can now be used to make changes. PeerLock is designed to integrate seamlessly with PeerSync editions to offer a total locking and synchronisation solution. PeerLock also adds much needed functionality to Microsoft DFS R2 which has no locking capabilities at all.

PeerLock gives you highly granular file management which translates directly into improved collaboration. PeerLock has locking options for precise control, increased visibility into locked files across collaborative environments, and offers a number of enhancements to streamline overall performance.

PeerLock eliminates several critical file management barriers (i.e., now files can be locked on any location even if the location requires different logon credentials) and facilitates more seamless collaboration by reducing file "release" intervals (longer "release" intervals increases the risk of "version conflict," one of the main reasons collaborative projects are late, over-budget or fail).

Details

PeerLock is a powerful and innovative program that ensures that when a user is modifying a file, no other user will be allowed to make changes to that file on any machine that the user has chosen to lock. Installed on the two watched server machines, PeerLock Server makes sure that no file from the watched folders is accessed with write access while it is in use on the correspondent location. PeerLock Server is configured by selecting "Source/Target folder pairs". PeerLock Server allows for 255 unique selections with each selection allowing for up to three target folders.

PeerLock makes network file locking possible while local files are in use and integrates seamlessly with PeerSync Server and PeerSync High Volume Server. This innovative program ensures that when a user is modifying a file, no other user will be allowed to make changes to that file on any machine that the user has chosen to lock. Furthermore, if Microsoft DFS is being utilised, PeerLock allows any files opened in a DFS resource to be locked on all other DFS servers. Seamlessly and transparently.

Cross Domain File Locking - Locks files on any location even if the location is on a different domain or on another machine requiring specific credentials for access.

Performance - Improved Locking and Releasing Time: Files are locked and released in milliseconds instead of approximately one second per file.

Detection Options - Dual Detection - Uses both local and file server mode detection for complete locking on machines that may have files opened from users connecting over the network as well as accessing the files locally.

Lock Options - Allow Access based on Source File: Lock target files with the same access based on the source file. When using this feature files on the source and their corresponding target(s) will be accessible by other users in the same manner.

Display - Release List - Stores recently released files and all information pertaining to the locking and releasing of those files including why the file was released

Failed Connections Retry - PeerLock stores failed connections and retry them on a ten minute cycle. This can improve overall performance when connection losses occur.

Furthermore, PeerLock lets you define:

- Real-Time Detection of File Use and Immediate Remote Locking.
- Instant file locking and synchronization.
- Easy installation and unobtrusive operation.
- Allows up to 255 source selections.
- Allows up to 100 targets per source selection.
- Allows for remote source selections.
- Can be run as a service.
- Feature to Create/View and close folder selections in MS Windows Explorer.
- Source/Target Folder File Mask: Each Source/Target pair contains an option for masking of file types you wish to include.
- Support for UNC folder/path names: This includes dynamic mapped drive creation, as well as local drives.
- Variable Path Selection: You can insert variables into the source or target path to create unique synchronisations. Usable Variables include Date, Day of the Week, Username, etc.
- Reporting: This option allows for log file reporting.

Supplementing Microsoft DFS

Microsoft's DFS provides a simple and easily implemented solution for co-locating files on multiple servers, permitting a more collaborative way of working. The problems come when more than one user wants to change the same file which is located at different locations. There is no locking mechanism to prevent one of them from doing this until the other has completed their work. The result, version conflict which someone then has to manually manage. Even in a small organisation, this can result in hundreds, if not thousands, of conflicted files.

The best and most complete way to eradicate version conflicts when utilising DFS is to employ a true file locking solution. Such a solution needs to provide as a minimum, real-time detection of file use coupled with immediate remote locking. Such a solution is Peerlock. This assures that when a file is open at one location, that all other versions are locked down, preventing anyone from opening and revising it. However, when the file closes, the file lock is immediately released and ready for synchronisation by DFS in the normal way.

PeerLock is a registered trademark of Peer Software. Windows and Microsoft are registered trademarks of Microsoft Corp. Purple Rage and the Purple Rage logo are trademarks of Purple Rage Limited.