



PeerLink
File Collaboration

PeerLink Help Manual

Copyright (c) 1993-2014 Peer Software, Inc. All Rights Reserved

Updated Wednesday, April 30, 2014

Table of Contents

PeerLink Help	1
Getting Started	1
Solution Overview	1
Terminology	3
Requirements	5
Architecture Overview	6
How File Collaboration Works	8
Installation and Configuration	11
Licensing	13
The PeerLink Hub User Interface	15
Main View	15
Web Interface	17
Menus	22
Job View	24
Agent Summary View	25
Alerts View	29
Job Alerts View	30
Creating a File Collaboration Job	31
Overview	31
Global Configuration	31
SMTP Email Configuration	32
Global Email Alerts	33
Global SNMP Notifications	35
Global File Filters	37
Step 1 - Host Participants and Directories	43
Step 2 - General Settings	45
Step 3 - File Filters	46
Step 4 - File Conflict Resolution	48
Step 5 - Delta Compression	50
Step 6 - File Metadata	52
Step 7 - File Locking	54
Step 8 - Logging and Alerts	56
Step 9 - Target Protection	58
Step 10 - Email Alerts and SNMP Notifications	59
Step 11 - Save Settings	61
Running and Managing a File Collaboration Job	62
Overview	62
Starting and Stopping	64
Collaboration Summary View	65
Multi-Job Edit Support	66
Host Connectivity Issues	68
Runtime Job Views	70
Summary View	70
Session View	73
Event Log View	74
File Conflict View	75
Alerts View	78
Participants View	79

Configuration View.....	81
Advanced Configuration	82
NetApp Configuration	82
Prerequisites and Configuration.....	82
Advanced fPolicy Configuration.....	86
Troubleshooting	89
Custom SSL Intergration	89
Use Existing Certificate.....	89
Create New Certificate.....	93
Scan Manager	100
Event Detection	101
Locking	102
Central Agent Configuration	103
Broker Configuration.....	104
General	105
Logging	106
Performance	108
VM Options	109
Index	0

PeerLink Help

Using this help file

This help is designed to be used on-screen. It is cross-linked so that you can find more relevant information to any subject from any location. If you prefer reading printed manuals, a PDF version of the entire help is available from our website. This may be useful as a reference, but you will probably find that the active hyperlinks, cross-references, and active index make the on-screen electronic version of this document much more useful.

Trademark Information and Copyright

Copyright (c) 1993-2014 Peer Software, Inc. All Rights Reserved. Although we try to provide quality information, Peer Software makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained in this document. Peer Software, PeerLink and their respective logos are registered trademarks of Peer Software, Inc. Microsoft, Windows, Windows Server and their respective logos are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. NetApp, the NetApp logo, Data ONTAP, and FPolicy are trademarks or registered trademarks of NetApp, Inc. in the United States. and/or other countries. "Amazon Web Services", "AWS", "Amazon S3", "Amazon Simple Storage Service", "Amazon SNS", "Amazon Simple Notification Service", and their respective graphics, logos, and service names are trademarks, registered trademarks or trade dress of Amazon Web Services LLC and/or its affiliates in the U.S. and/or other countries. All other trademarks are the property of their respective companies. Peer Software, Inc. vigorously protects and defends its trade name, trademarks, patents, designs, copyrights, and other intellectual property rights. Unless otherwise specified, no person has permission to copy, redistribute, reproduce, or republish in any form the information in this document.

Getting Started

The topics in this section provide some basic information about PeerLink, including installation, configuration, and deployment.

Solution Overview



PeerLink

File Collaboration



Overview

PeerLink is an enterprise real-time, multi-directional, distributed, file locking and synchronization technology that ensures the same data exists on all participating host servers regardless of where changes occur. It also prevents users on disparate networks from accessing a file

that is in use by a user on another network. A file collaboration session consists of two or more participating hosts, and a folder hierarchy called the Watch Set, located on each host, which will be kept synchronized by propagating file locks and modifications to all participating hosts in real-time.

PeerLink Key Features

PeerLink Features	Standard Edition
Maximum number of running file collaboration sessions.	Depends on licensed amount
Maximum number of unique participating hosts across all running collaboration sessions.	Depends on licensed amount
Real-time Updates: Changes made to files on any server immediately mirror on all other servers. Files remain accessible at all sites.	✓
Distributed File Locking: Native file locks are propagated in real time over any distance.	✓
Transparency: Your users and applications keep using the exact same files, in the exact same manner.	✓
Efficient Bandwidth Usage: Binary delta compression sends only the bytes of a file that have changed between hosts.	✓
Secure: SSL encrypted end-to-end session communication.	✓
Ability to configure file inclusion and exclusion filters based on wild-card matching.	✓
Ability to view all currently opened and locked files.	✓
Ability to view all file transfers in progress.	✓
Ability to view a summary of file collaboration statistics for a running collaboration session.	✓
Ability to view a summary of file collaboration statistics across all running collaboration sessions.	✓
Configurable event logging facility with the ability to select specific events to log.	✓
Ability to select from various file conflict resolution schemes.	✓
Ability to handle file conflicts and other errors via a file quarantine service.	✓
Target file trash bin protection which saves a copy of a file before deleting or modifying the file on a target host. Also includes support for automatic maintenance and cleanup of this trash bin.	✓
Web-based interface with all of the functionality of the rich client user interface.	✓
Portal system tied into the web-based interface, allowing for administrators and help desk users. The latter of which can be used for remote conflict resolution.	✓

Sync-On-Save support for most Microsoft Office file types.	
Email and SNMP Alerts for critical errors occurring in a running collaboration session, for example, when a file is quarantined.	
Support for NetApp Storage Devices (for more information, please view the NetApp section).	Based on License

Terminology

Introduction

Before getting started, it is important to have a good understanding of key concepts and terminology used throughout this help document.

Terms

File Collaboration Session	A communication session made up of two or more hosts, each with a designated root of folders and files that are to be shared or collaborated on. A collaboration session coordinates the primary functions of file locking and synchronization.
Participating Host	A host that is participating in a file collaboration session.
Directory Watch Set	The configured root folder and all sub folders that are being watched and collaborated on for a participating host.
Source Host	The host where a file access or change event originated from.
Target Host	One or more hosts where file access and change events will be propagated to.
Initial Synchronization Process	The background process that occurs at the start of a file collaboration session, where the directory watch set is recursively scanned on all participating hosts, file conflict resolution is performed, and any files that require updating are synchronized with the most current copy of the file.
File Access Event	An event that is triggered from the opening or closing of a file.
File Change Event	A event that causes a file to be changed in some way, for example: file modify, file delete, file rename, file attribute change, etc.
File Lock Conflict	A file collaboration condition that exists when two users open a file at the same time and both hold exclusive locks on the file.
Quarantined File	A file that has been removed from a file collaboration session as a result of a file lock conflict that could not be resolved. This file will remain quarantined until the user manually removes it from quarantine.
Peerlet	A solution built for the PeerLink framework . An Peerlet is a distributed application containing various parts, some of which function at a focal point called the PeerLink Hub and others invoked at remote points designated as PeerLink Agents.

File Collaboration Job	<p>A specific instance of a Peerlet that can be created, saved, modified, and run. A Peerlet represents a type of Job.</p> <p>In the case of File Collaboration, a File Collaboration Job represents a single configurable file collaboration session. The two terms may be used interchangeably throughout the interface and this document.</p>
PeerLink Hub	<p>The focal software component where Peerlets are installed, configured and ran. The PeerLink Hub can host Peerlets of various types and is where the components of a centralized solution function. The PeerLink Agent is invoked by Peerlets', distributing components with messages sent through the PeerLink Broker.</p> <p>The PeerLink Hub runs as three parts: a Windows Service that is set to run all the time, along with a rich client application and a web server component that both connect to the primary service for configuration and monitoring.</p>
Views	<p>Individual sections of the PeerLink Hub's user interface, each providing unique information and control.</p> <p>Examples: Main View, Job View, Agent Summary View, Alerts View, Job Alerts View, etc.</p>
Peerlet Editor	<p>A container within the user interface of the PeerLink Hub which shows runtime and configuration information for a single file collaboration job. A Peerlet Editor is represented by a single tab, typically in the large center section of the PeerLink Hub's interface. The editor itself consists of multiple sub-tabs, with various runtime and configuration information dispersed amongst the sub-tabs. For more information, see the help section on Runtime Job Views.</p> <p>Editors for multiple file collaboration jobs can be opened in several different editor tabs, allowing for quick movement between jobs.</p> <p>The Peerlet Editor area of the PeerLink Hub will be referred to as the File Collaboration Runtime View throughout this document.</p>
PeerLink Broker	<p>The central messaging system of the Peerlet framework. The PeerLink Broker serves to connect the PeerLink Hub and the Agents, forming a PeerLink "network" that can be cast over local- or wide-area networks via TCP/IP. A PeerLink environment will deploy one or more PeerLink Brokers.</p>
PeerLink Agent (or "Agent")	<p>A lightweight, distributed component that is used to perform operations on the host on which it is running. A PeerLink environment will typically contain several Agents, one per participating networked host. Agents invoke the distributed portions of a Peerlet, and will often run near resources of interest, such as collaborated files. The Agent is designed to be purposed across the entire PeerLink solution suite, and will normally be directed to perform functions with messages received from Peerlets through the PeerLink Broker.</p>

Heartbeat	A communication mechanism used between the the PeerLink Hub and all connected PeerLink Agents to ensure that Agents are alive and responsive. Heartbeats share information about the Agent's host server with the PeerLink Hub, aid in verifying when an Agent is no longer available, and signal when a disconnected Agent has reconnected. All heartbeat information is sent through the PeerLink Broker.
------------------	---

Requirements

1. All participating hosts must be highly available file servers, accessible across highly available and stable networks.
2. PeerLink only propagates locks when a file is opened with a read-write lock (e.g. MS Word, MS Excel, etc.). If a file is opened in read-only mode without an exclusive write lock, or if the application closes all handles to the file (e.g. Notepad, WordPad, etc.), the lock will not be propagated to the [Target Hosts](#).
3. In order for file collaboration to work correctly, all end-user file access and modifications must be done through a network share or network mapped drive, and not performed locally on the [participating host](#). If you access a file in the [Watch Set](#) locally on the participating host, then file locks will not be propagated to the Target Hosts.
4. A PeerLink [Agent](#) must be installed on all participating hosts. Each host machine must be running Windows 2003 Server or later with the latest service packs and a minimum of 1GB of RAM (512MB of which is dedicated to the PeerLink Agent service). Depending on the level of activity on the system and the number of running applications, required system RAM will likely be higher. The host machine must be acting as a file server where the Watch Set is located on a locally attached storage device. The Watch Set cannot be located on a NAS device that is mapped through a network share. Support for NetApp storage devices (licensed separately) is available, but configuration is handled in a different manner. Please see the [NetApp Configuration](#) section for more information.
5. The PeerLink Agent is installed as a Windows service under the default SYSTEM user account. The user that the service is running under should have read+write access to the Watch Set
6. The PeerLink [Hub](#) must be installed on a highly available Windows 2003 Server or later with at least 2GB of RAM, and must have at least 512MB of RAM dedicated each to the PeerLink Hub and PeerLink [Broker](#) applications. This is the default minimum recommended configuration, but the amount of RAM can be increased via custom configuration to optimize performance.
7. All participating file servers must be NTFS formatted. Support for NetApp storage devices (licensed separately) is also available.
8. All participating hosts must have network access to the machine where the PeerLink Broker is installed, which by default will be the same machine where you installed the PeerLink Hub. You will also need to configure the PeerLink Agent to connect to the PeerLink Broker's host name or IP Address, and allow firewall access to the configured port, which is 61617 by default. You will also need to allow access from all participating hosts to port 8181 of the machine that the PeerLink Hub is running on.
9. PeerLink is intended to be installed and maintained by a qualified System Administrator and not a typical end-user.

Important Notes

Collaboration of the Users Home directories (Redirected Folders, Roaming Profiles, etc) are not supported. Overlaying File Locking (which is inherent within the PeerLink framework) with these file types and the nature of these folders will cause conflicts.

Architecture Overview

Introduction

This overview describes the functional components of a PeerLink environment. In this discussion, we identify the primary components of a PeerLink installation.

PeerLink Architecture

PeerLink solutions, also known as "Peerlets", have local and remote characteristics that form the basis of a distributed application framework. A PeerLink installation is composed of three primary components:

1. PeerLink Hub

The PeerLink Hub is the central component of the PeerLink framework. All PeerLink solutions are installed, configured and started at the PeerLink Hub. Peerlets are comprised of central and distributed components that function in the PeerLink Hub and PeerLink Agents respectively. The PeerLink Hub requires connectivity to the PeerLink Broker for all messaging activity.

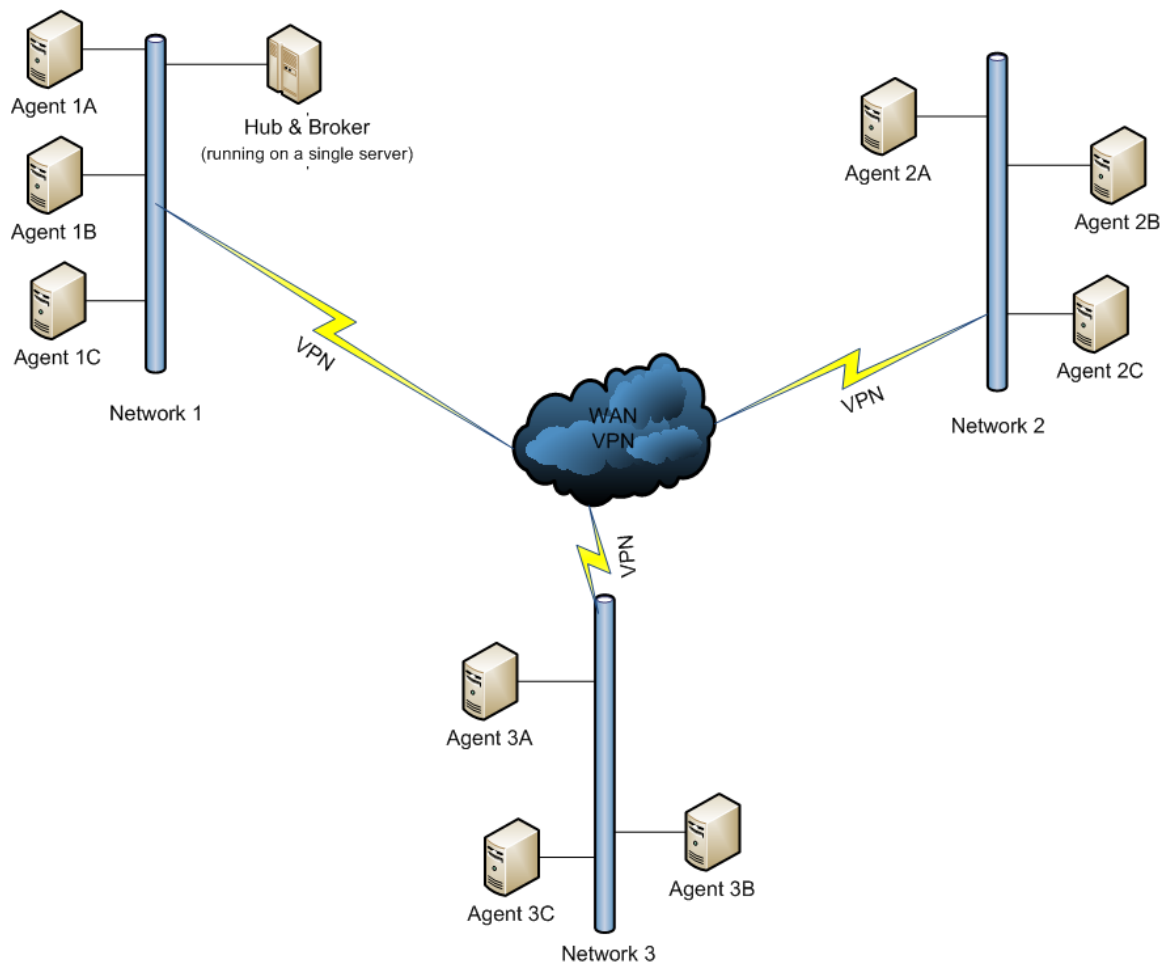
2. PeerLink Agent

The PeerLink Agent is a lightweight component that is installed on a networked host that enables it to participate in a PeerLink solution. A PeerLink Agent invokes the distributed functions of a Peerlet from messages received through the PeerLink Broker. Like the PeerLink Hub, the PeerLink Agent connects to the PeerLink Broker to send and receive messages.

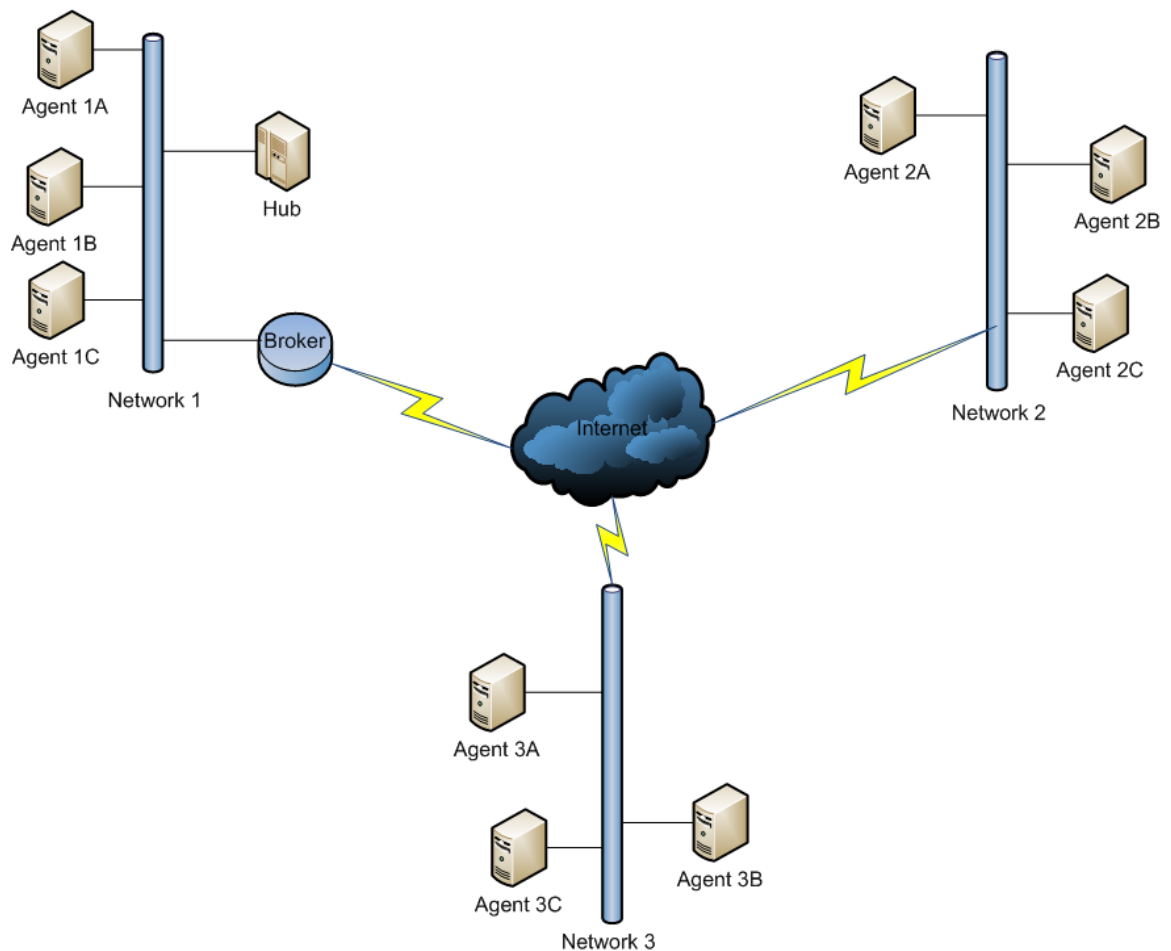
3. PeerLink Broker

The PeerLink Broker makes up the central messaging system that supports PeerLink applications. The PeerLink Broker provides the core communication facility that connects the PeerLink Hub and Agents in a PeerLink environment. Peerlets running at the PeerLink Hub interact with the participating Agents through the PeerLink Broker.

Below is a diagram of a typical deployment where the PeerLink Hub & PeerLink Broker and all PeerLink Agents are on separate networks connected via a VPN. This deployment also has the PeerLink Hub & PeerLink Broker running on the same machine.



The following diagram shows an advanced deployment where there are three distinct networks located at three disparate locations connected via the Internet. The PeerLink Hub is located on network 1, and a PeerLink Broker is installed on the edge of each network for performance reasons, with multiple agents located on all three networks.



How File Collaboration Works

Introduction

File Collaboration was built as a PeerLink solution and complies with [Peerlet](#) conventions. Common to all PeerLink solutions is the notion that some functions are centralized while others are distributed.

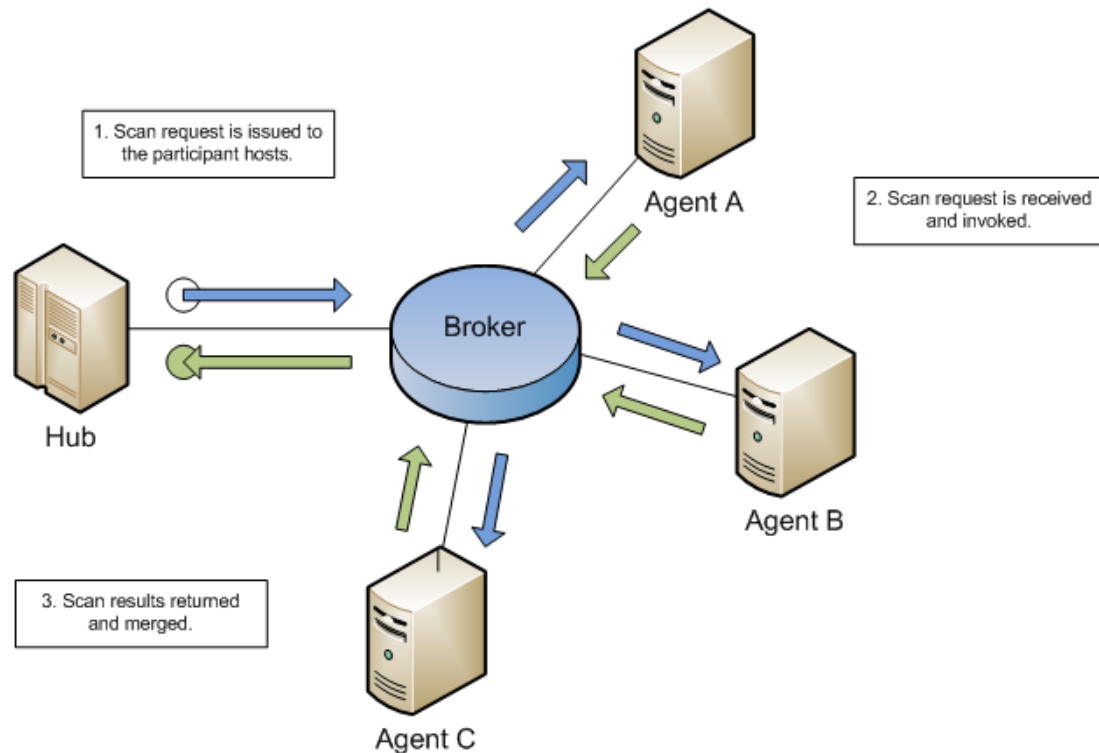
File locking for example, is a principle feature of this solution that has both central and distributed aspects. The access detection mechanism that is triggered in response to an opening file is deployed in the [PeerLink Agent](#), presumably on each participant host storing files of interest. The lock manager is a centralized component running at the [PeerLink Hub](#) that is notified of opening files.

We describe some scenarios below to further detail how collaboration functionally overlays the PeerLink architecture.

Step 1: Session Start

At the start of a [file collaboration session](#), the Peerlet starts the [initial synchronization process](#) by issuing a request to scan each host participant's Root Folder recursively for file content. The scans are performed at the Agents and results are dispatched back to the PeerLink Hub for merging and [file conflict resolution](#). Transfers are then issued to the Agents to syn-

chronize their hosts' root folders. While the initial synchronization process is performed in the background, the Agents are directed to start detecting access and change events on their respective hosts.

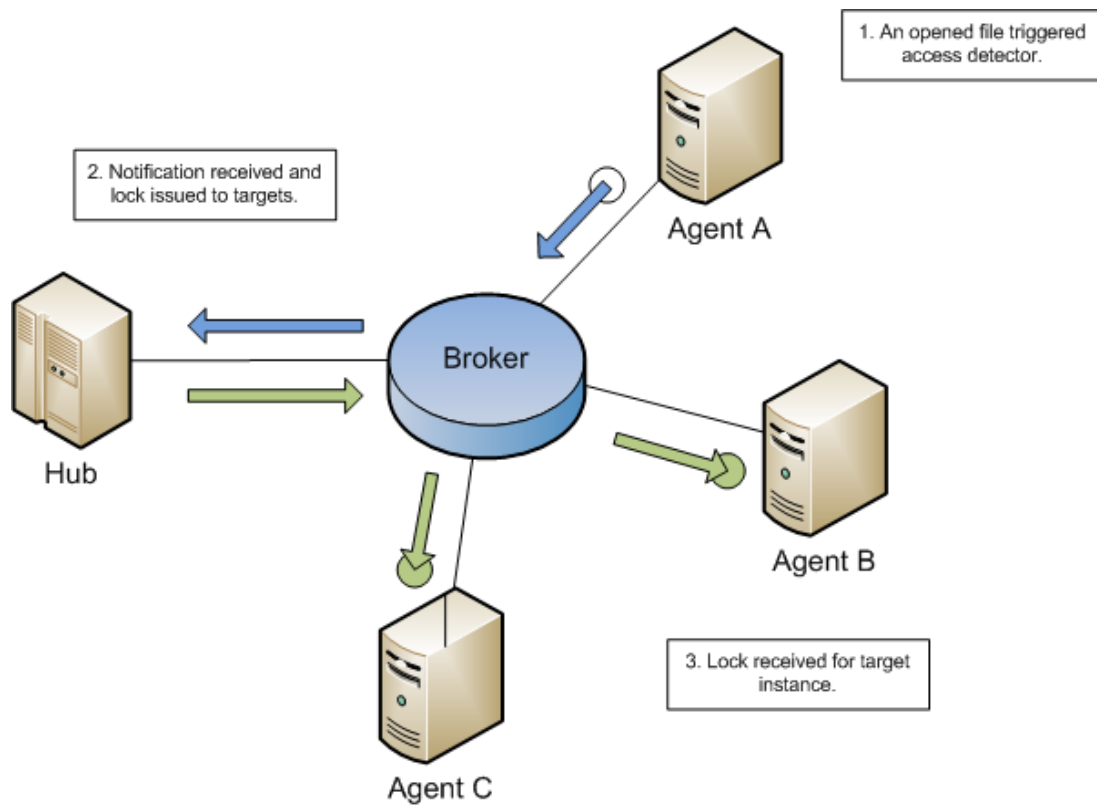


Step 2: File Lock

Files will be opened by users during the course of a file collaboration session. When a file opening for modification is detected by an Agent, the Peerlet at the PeerLink Hub will be notified of the occurrence and effectively issue a lock for the analogous file across the session. The issuing host contains the source instance of that file for the time it remains open, implying the remaining hosts' copies are designated targets. Only one source instance is allowed for any given file in a session.

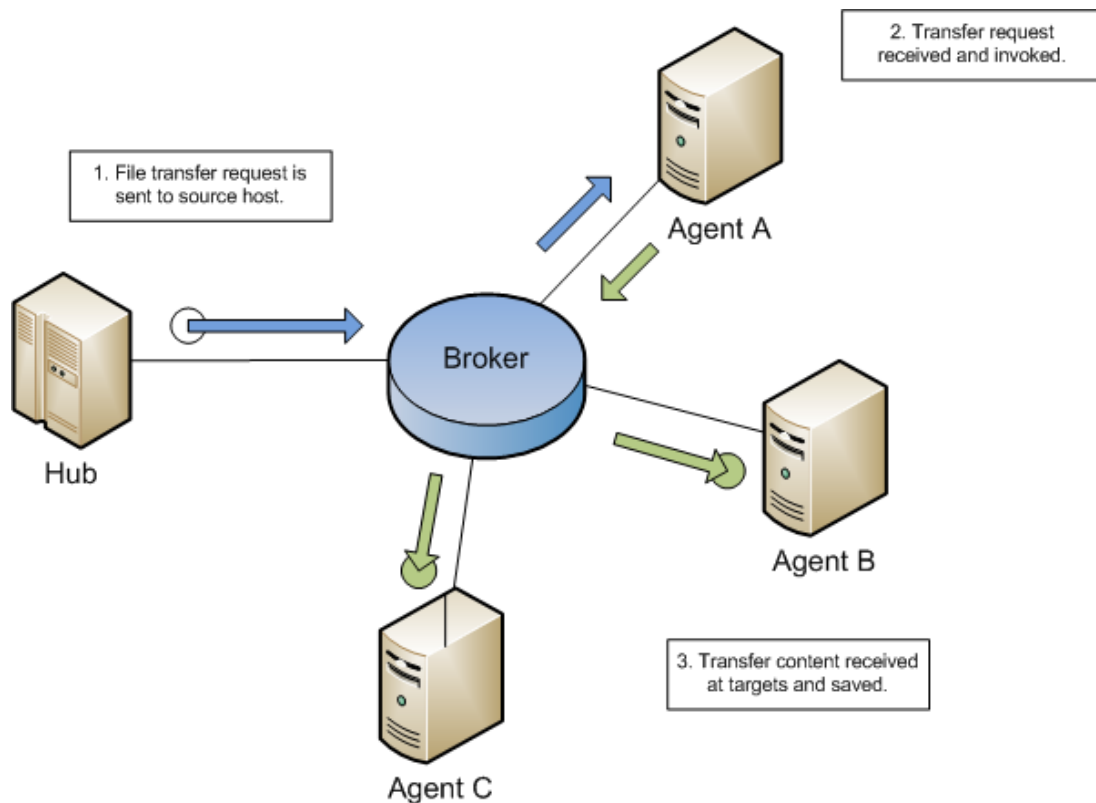
Note: If a file is opened in read-only mode or if the application that opens the file does not acquire a read-write lock on the file (e.g. NotePad, WordPad, etc.), the lock will not be propagated to the [Target Hosts](#).

When a source copy is closed with no modifications, the target files will be released across the remaining hosts in the session.



Step 3: File Transfer

When a source instance is closed with modifications, a synchronizing transfer is issued. The session first acquires a lock on the source instance to facilitate a stable transfer. The locks on the target copies are preserved during the lock transition at the source. The revised source content is propagated to the target instances and the locks are released. Transfers are conducted only among Agents, but coordinated through the PeerLink Hub.



Installation and Configuration

PeerLink can be installed in numerous ways based on your needs and environment. The PeerLink installation consist of two separate installers, both of which are available for download from our website:

1. PeerLink installer, containing the PeerLink Hub and PeerLink Broker
2. PeerLink Agent installer

PeerLink Hub & PeerLink Broker Installation

Both the [PeerLink Hub](#) and [PeerLink Broker](#) are packaged with the main PeerLink installer and by default, will be installed on the same server.

Basic Requirements

1. The PeerLink Hub must be installed on a highly available Windows 2003 Server or later with at least 2GB of RAM and must have 512MB of RAM dedicated each to the PeerLink Hub and PeerLink Broker applications. This is the default minimum recommended configuration, but the amount of RAM can be reduced or increased via custom configuration.
2. All installed [PeerLink Agents](#) must have network access to the server that the PeerLink Broker is installed on, and any firewalls must be configured to allow access for ports 61617 and 8181.
3. See the [Requirements](#) section for more detailed requirements.

Software Installation & Launching

1. Run the PL-Hub_Installer.exe installer and follow all instructions.
2. After the installation finishes, both the PeerLink Hub and PeerLink Broker will be installed. The PeerLink Broker will automatically be installed as a running Windows service and set to auto-start. The PeerLink Hub is installed in two parts: a Windows service that is set to auto-start, and a client for interacting with the Windows service. The client is started as a normal Windows application.
3. Start the PeerLink Hub Client by launching the PL-Hub.exe executable located in the base installation directory. If the both the PeerLink Broker and PeerLink Hub Service are up and running as background services, then the PeerLink Hub should successfully start. If not, please make sure that both the PeerLink Broker and PeerLink Hub Service are running as Windows services via the Windows Service Panel (services.msc).

Secure Encrypted SSL Connections

By default, the PeerLink Hub and PeerLink Broker will be installed on the same host machine which does not require secure SSL communication between each other. To enable a secure SSL connection between the PeerLink Hub and PeerLink Broker, first stop the PeerLink Hub Service via the Windows Service Panel (services.msc). Once stopped, navigate to the directory, 'Hub\workspace\prefs', relative to the installation directory. Within this directory, open the com.ci.pl.hub.runtime.prefs file in a text editor. If the file does not contain a line starting with "hub.jms.providerURL", then add the following line in it's entirety:

```
hub.jms.providerURL=failover\:(ssl://localhost:61617)?jms.alwaysSyncSend=true
```

Otherwise, making the following changes to the line starting with "hub.jms.providerURL" (changes are **bold** and underlined):

From: hub.jms.providerURL=failover\:(tcp://localhost:61616)?jms.alwaysSyncSend=true
To: hub.jms.providerURL=failover\:(ssl://localhost:61617)?jms.alwaysSyncSend=true

Once these changes are complete, save the file, then restart the PeerLink Hub Service.

Uninstalling

PeerLink ships with an uninstaller for the environment it is running in. Please use the standard platform specific method for removing programs/applications to uninstall PeerLink.

PeerLink Agent Installation

You will need to install a PeerLink Agent on each server you plan to include in any of your [file collaboration sessions](#).

Basic Requirements

1. Must be installed on a system running Windows 2003 Server or later with the latest service packs acting as a file server where the Root Folder is located on a locally attached storage device. The system must have a minimum of 1GB of RAM, 512MB of which should be dedicated to the PeerLink Agent. Depending on the level of activity on the system and the number of running applications, required system RAM will likely be higher.
2. The server that the PeerLink Agent is installed on must have direct network access to the server that the PeerLink Broker is installed on, and any firewalls must be configured to al-

low access for ports 61617 and 8181 to the PeerLink Broker server.

3. The PeerLink Agent is installed as a Windows service under the default SYSTEM user account. The user that the service is running under should have read+write access to the Root Folder.
4. See the [Requirements](#) section for more detailed requirements.

Software Installation & Launching

1. Run the PL-Agent_windows.exe installer on the target server and follow all instructions.
2. During installation you will need to specify the PeerLink Broker Host Name (computer name, fully qualified domain name, or IP Address) of the server where the PeerLink Broker is running, as well as the configured TCP/IP port number (the default port for SSL communication is 61617).
3. After the installation finishes, the PeerLink Agent will be installed as a Windows service. You will need to verify that the PeerLink Agent is running, and that it was able to successfully connect to the PeerLink Broker. You can do this by opening Windows Service Panel (services.msc) and making sure that the "PeerLink Agent Service" is started.
4. Make sure that the PeerLink Agent was able to successfully connect to the PeerLink Broker by going to the PeerLink Agent installation folder, opening the output.log text file, and making sure that "Ready" is displayed on the first line.

Secure Encrypted SSL Connections

By default, the PeerLink Agent is installed with SSL encryption enabled, where the PeerLink Agent connects to the PeerLink Broker through a secure, encrypted connection. If you are running PeerLink on a secure LAN or via a corporate VPN, you might want to disable SSL to boost performance. For more details on disabling or enabling encryption for the PeerLink Agent, please see the [broker page of the Central Agent Configuration section](#).

Uninstalling

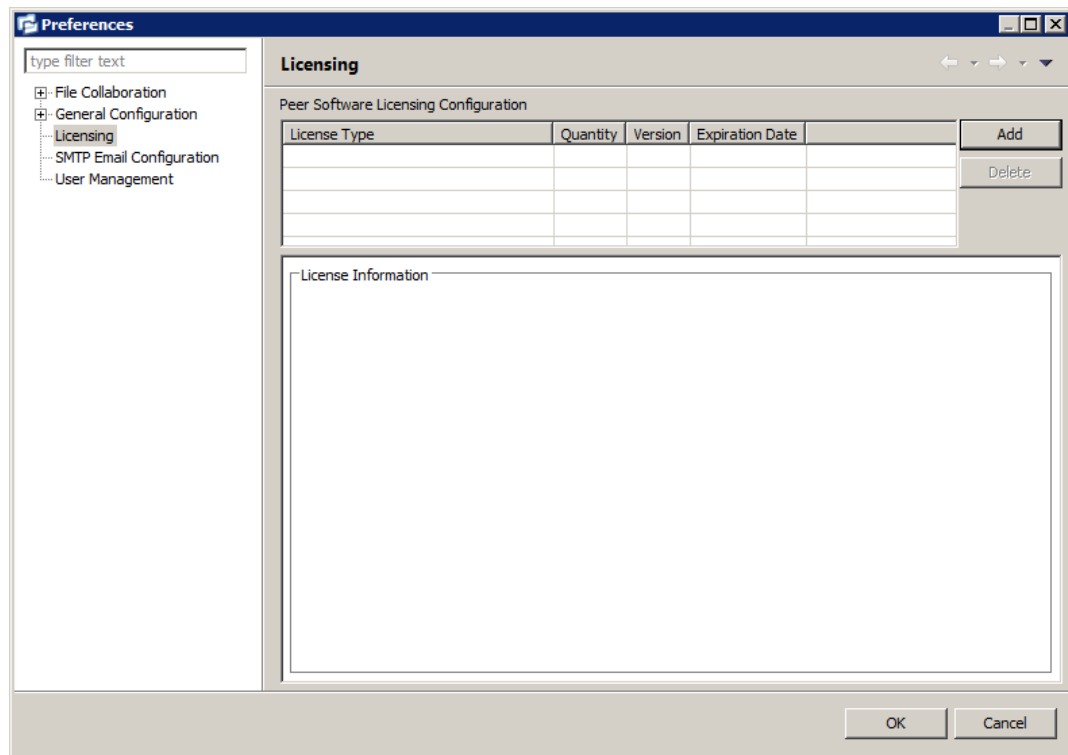
PeerLink Agent ships with an uninstaller for the environment it is running in. Please use the standard platform specific method for removing programs/applications to uninstall the PeerLink Agent.

Licensing

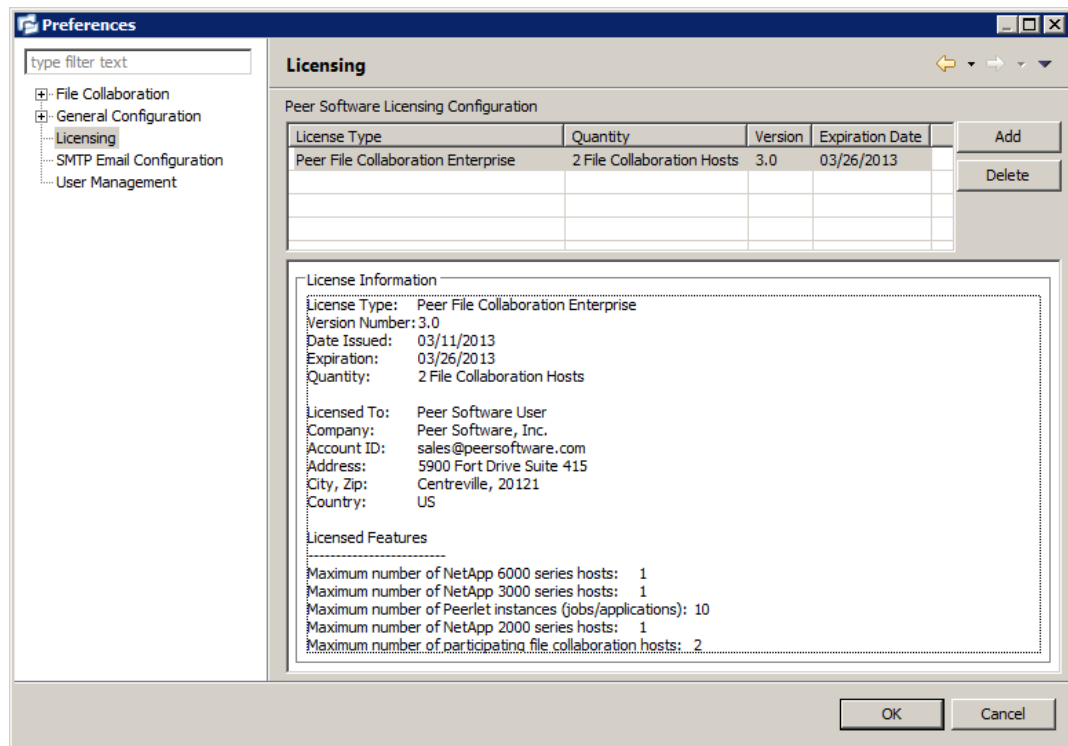
PeerLink is licensed by the number of unique [participating hosts](#) and by the number of running [file collaboration sessions](#).

Installing or Upgrading a License File

After purchasing or requesting a trial download of PeerLink, you will receive a license file representing your purchase or trial. To install a new license file or upgrade an existing license, navigate to the **Window** menu in the [PeerLink Hub](#) and select **Preferences**. Next, select the **Licensing** item in the tree on the left of the **Preferences** dialog.



Click the **Add** button to browse for and install the license file. If a license already exists for the same type, then the existing license will be overridden with the new license. After successful installation of the license file, the license will be displayed in the **License Configuration** table along with licensed quantity and an expiration date (if applicable). You will now be able to create, configure, and run file collaboration sessions.



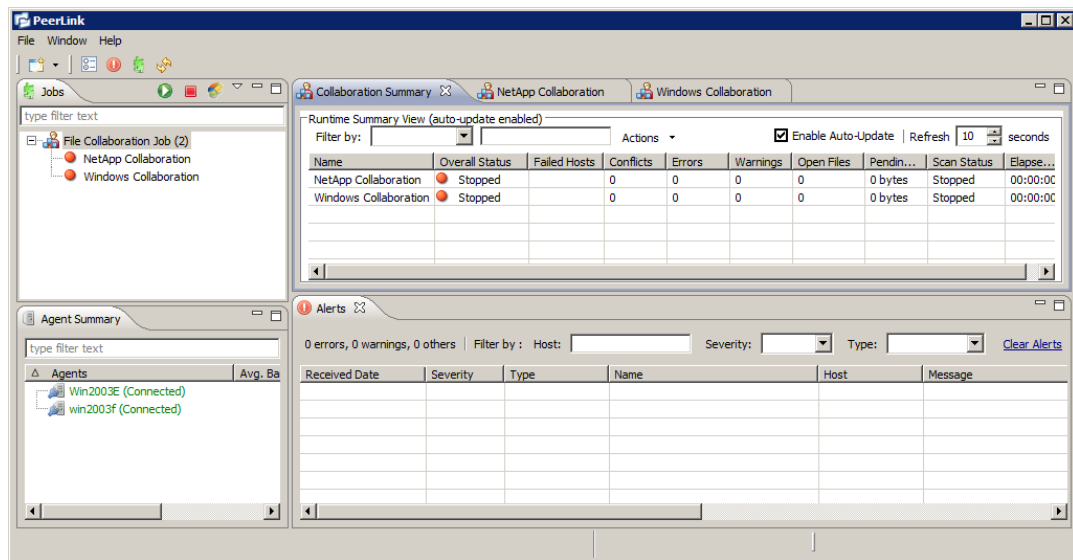
The PeerLink Hub User Interface

The PeerLink Hub is a container for configuring and deploying PeerLink Peerlet applications, including File Collaboration. The PeerLink Hub graphical user interface enables you to create, view, edit and delete your File Collaboration Sessions, as well as view runtime information for running Peerlets.

The graphical user interface of the PeerLink Hub now has two separate options: a rich client installed and run on the server running the PeerLink Hub, and a web service that when configured, can be accessed from remote systems via a web browser.

Main View

After starting up the PeerLink Hub Client, the following Main View is displayed:



The [PeerLink Hub](#) is made up of the following [Views](#):

<p>Jobs View</p>	<p>This is a list of all created file collaboration jobs that can be modified, viewed, and started. The list is grouped by Peerlet type, where the primary type is File Collaboration.</p> <p>The following buttons are available within this panel:</p> <ul style="list-style-type: none"> • Start and Stop buttons allow you to start and stop any selected jobs. • View Runtime Summary button displays a table of summary information for all jobs of a selected Peerlet type.
<p>Agent Summary View</p>	<p>Displays a list of known PeerLink Agents and connection status for each. Individual Agents can be updated and restarted from this view as well by right-clicking on one or more items and selecting the appropriate item from the popup menu.</p>
<p>Alerts View</p>	<p>Displays a list of PeerLink Hub alerts that have occurred with detailed information about each alert. Alerts relating to PeerLink Agent connection status changes will be reported here.</p>
<p>Job Alerts View</p>	<p>Displays a list of all job-specific alerts that have occurred (including those for file collaboration sessions) with detailed information about each alert. Alerts relating to the automatic stopping and re-starting of jobs will be reported here.</p>
<p>File Collaboration Runtime View (tabbed View in center of screen)</p>	<p>The Peerlet Editors View is the default location of the Collaboration Summary View, in addition to runtime and configuration sub-views for all open jobs.</p> <p>For each open file collaboration job, the following sub-views are available as tabs:</p> <ul style="list-style-type: none"> • Summary Tab - Displays current synchronization summary and session statistics. • Session Tab - Shows currently opened files, session locks, and files being synchronized. • Event Log Tab - Displays a log of recent file activity.

- **[File Conflicts Tab](#)** - Shows a list of current file conflicts and quarantined files.
- **[Alerts Tabs](#)** - Displays alerts tied specifically to the selected job.
- **[Participants Tab](#)** - List of currently configured and associated [host participants](#) for the selected job, in addition to connection status for each.
- **[Configuration Tab](#)** - Shows a summary of all configurable items for the selected job.

Table Detail Viewer

Most tables shown throughout the PeerLink Hub support double-clicking on any row. This action will bring up a popup dialog containing all of the details pertaining to the information in that row. An example is shown below:

Hub Alert Details	
Received at:	03-11-2013 20:26:35
Severity:	Fatal
Category:	Auto Stop Job
Locally Generated at:	03-11-2013 20:26:35
Name:	Windows Collaboratin
Message:	Quorum lost for job Windows Collaboratin. Session will restart when minimum required hosts become available. Session elapsed time was 00:01:11 before quorum was lost.
Ref ID:	100

Click outside of popup to close

In addition, most right-click context menus contain the ability to copy this detailed information on one or more rows all at the same time. This information can then be pasted into any document editor.

Web Interface

PeerLink now offers a new way to manage and monitor collaboration jobs via a robust web interface. Unlike many other web management consoles, PeerLink's web interface is very responsive and is built to mirror the functionality of the rich client (which is still included with the PeerLink Hub installer for use by system administrators). When properly configured, the web interface allows system administrators to manage PeerLink's collaboration jobs from any location without the need to remotely login to the PeerLink Hub server.

In addition, this web interface includes a role-based login system with two out-of-the-box roles: **admin** and **helpdesk**. The former has complete access to all functionality found in the PeerLink Hub's rich client, while the latter only has a read-only view of collaboration jobs along with the ability to release conflicts for any running jobs.

How to Set Up

The setup process for the web interface is driven by following screen within the installer for the PeerLink Hub:

The options on this screen are as follows:

Local Access	Selecting this option will allow access to the web interface only when remotely connected into and using a web browser on the local PeerLink Hub server.
Public Access	Selecting this option will allow access to the web interface via the configured hostname or IP address. Please note that Public Access does not necessarily mean that anyone on the Internet will be able to access the web interface. This access should be further limited via NAT and network firewall policies.
Disable Web Service	Selecting this option will completely disable the web interface and set the PeerLink Web Service to manual.
Hostname or IP	This is the hostname or IP address via which clients can access the web interface. If Local Access is set, this will be forced to use "localhost".
Enable HTTP (using Port)	Enables HTTP access to the web interface using the specified port.
Enable	Enables HTTPS access to the web interface using the specified port

HTTPS (using Port)	and a built-in SSL certificate. More details on changing SSL certificates can be found here .
---------------------------	---

If you need to make changes to the configuration of the web interface, you will need to stop the **PeerLink Hub Web Service** in **services.msc** and use Notepad to modify the **config.ini** file located under **PEERLINK_INSTALL_FOLDER\Hub\web-configuration** (where **PEERLINK_INSTALL_FOLDER** represents the root installation directory of PeerLink). Once modifications are complete, save the file and restart the **PeerLink Hub Web Service**. The important items to configure within this file are:

org.eclipse.equinox.http.jetty.http.enabled	Set to "true" to enable HTTP access to the web interface. If set to "true", the org.eclipse.equinox.http.jetty.http.host and org.osgi.service.http.port items must also be configured in order to enable HTTP access to the web interface. If set to "false", HTTP access will be disabled and the other HTTP-related settings will be ignored.
org.eclipse.equinox.http.jetty.http.host	Set this to the hostname or IP address via which the web interface can be accessed using HTTP. Set this to "localhost" to enable local access only for HTTP.
org.osgi.service.http.port	Set this to the port to be used for HTTP access.
org.eclipse.equinox.http.jetty.https.enabled	Set to "true" to enable HTTPS access to the web interface. If set to "true", the org.eclipse.equinox.http.jetty.https.host and org.osgi.service.http.port.secure items must also be configured in order to enable HTTPS access to the web interface. If set to "false", HTTPS access will be disabled and the other HTTPS-related settings will be ignored.
org.eclipse.equinox.http.jetty.https.host	Set this to the hostname or IP address via which the web interface can be accessed using HTTPS. Set this to "localhost" to enable local access only for HTTPS.
org.osgi.service.http.port.secure	Set this to the port to be used for HTTPS access.

IMPORTANT NOTES FOR THE CONFIG.INI FILE:

- All settings listed above must be followed by an "=" and a value. For example, to enable HTTP access, the line in the **config.ini** file with **org.eclipse.equinox.http.jetty.http.enabled** should look like:

org.eclipse.equinox.http.jetty.http.enabled=true

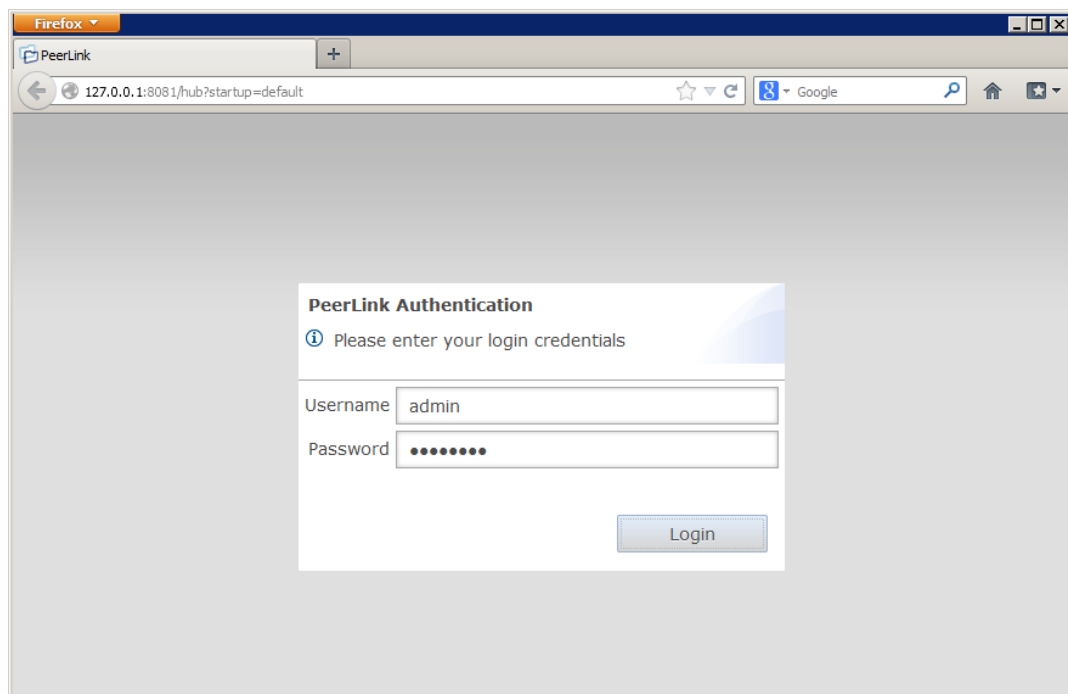
- HTTP and HTTPS are configured independently of one another in the **config.ini** file and as such, can be set to different modes. For example, HTTPS could be configured in a public mode, while HTTP is set to private ("localhost").
- DO NOT modify any other settings in the **config.ini**. Doing so may result in the inability of

the web interface to start.

- Duplicate entries in the **config.ini** file may also result in the inability of the web interface to start.

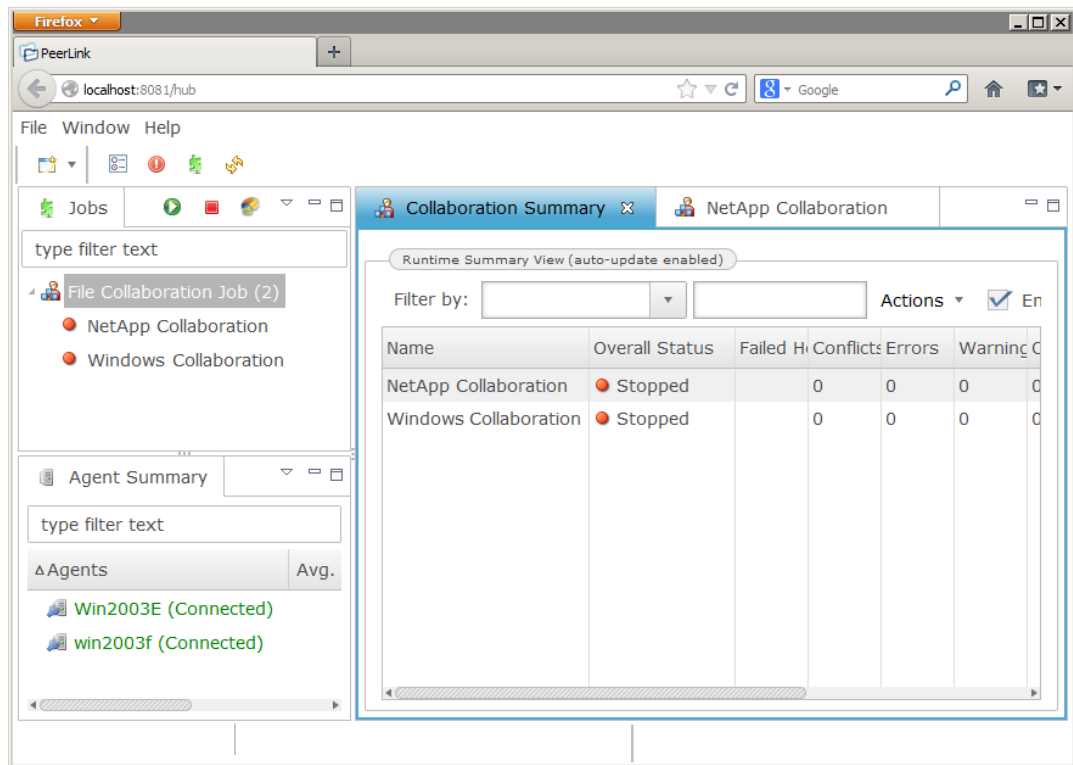
How to Use

Once PeerLink has been installed and all services have been started, open up a web browser and enter the following URL: `http://localhost:8081`. Please note that the exact URL will vary depending on the settings you have selected in the [How To Set Up](#) section above (for example: `http` vs `https`, appropriate hostname or IP, and appropriate port). In the page that loads, select the **PeerLink Hub Management Portal** link. The following page will then be displayed:



The default user name is "admin" with a default password of "password". We highly recommend that you change this password. See the [User Management](#) section for more information on changing account passwords.

If logged in with an **admin** account, the following will be displayed:



As mentioned above, those with **admin** accounts will have complete access to the PeerLink Hub's UI. For more details on how to use the full PeerLink Hub interface, please see the [Main View](#) section of this help document.

Those with **helpdesk** accounts are limited to read-only access of the following:

- The [Job View](#)
- The [Collaboration Summary](#) view
- The [Summary](#) and [Session](#) tabs of each job.

In addition, these accounts have read-write access to the [File Conflicts](#) tab of each job, with the ability to release conflicts.

How to Secure Access

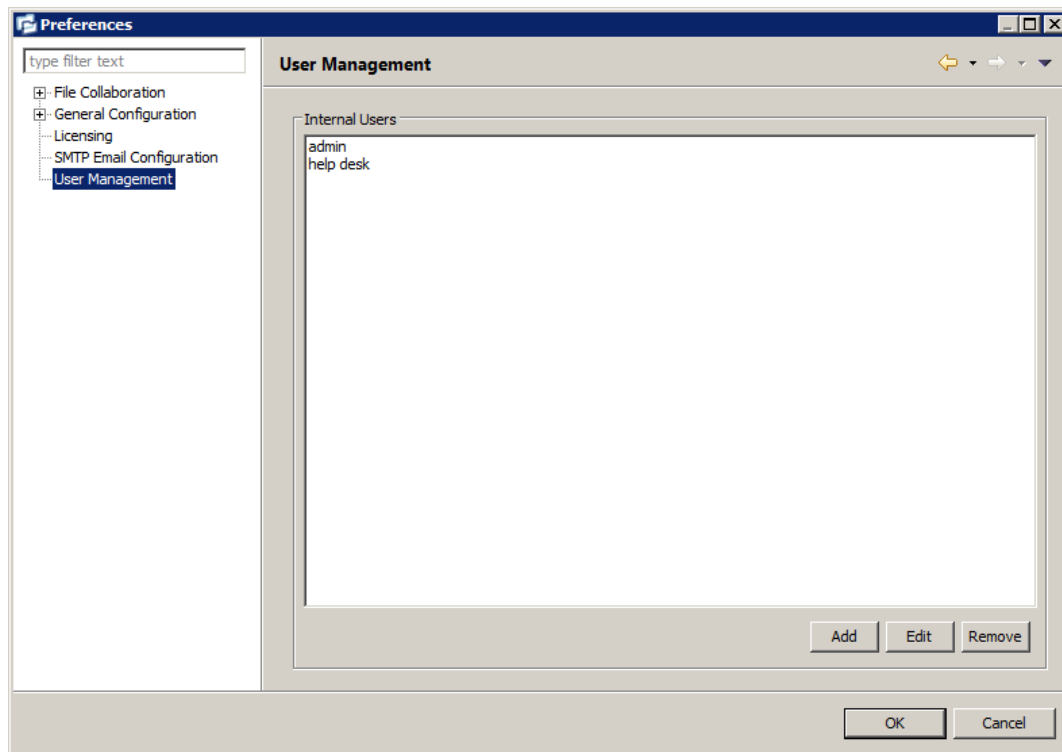
There are several important things to keep in mind when it comes to securing access to PeerLink's web interface:

- The default **admin** account password should be changed immediately. For details, see the [User Management](#) section below.
- Access to the web interface can be in the form of both HTTP and HTTPS. The latter will ensure that all communication between the client browser and the service hosting the web interface is encrypted. Regardless of which is enabled, the hostname or IP address through which clients can reach the web interface can be configured to limit access. See [How to Set Up](#) section for more details.
- While HTTPS access to the web interface is secured out of the box with a built-in certificate, this certificate can be swapped for a custom one. For more details on this process, please contact Peer Software's support team via email: support@peersoftware.com.

User Management

Management of users with access to PeerLink's web interface can be performed through either the Hub's rich client, or through an **admin** account logged into the web interface.

To access the **User Management** configuration page, navigate to the **Window** menu, select **Preferences**, then select **User Management** from the tree on the left. The following will be displayed:



From this screen, you can add, edit, and remove user accounts. Adding an account requires a username, a password, an email address, and a selected role. For more details on the available roles, see the [How to Use](#) section. Once an account has been created, its username, password, email address and role can all be changed.

Notes:

- The default **admin** user cannot be renamed, nor can its role be changed.
- These user accounts have no impact on access to the rich client.
- LDAP/AD support for users and groups will be available in the official release of v3.0.

Menus

After starting up the [PeerLink Hub](#) Client, the following menu & toolbar actions are available:

File Menu

New	Selecting this option will present you with a list of installed Peerlet types from which you can create a new job . The options are based on which
------------	--

	PeerLink solution is installed. For example, if you installed the File Collaboration solution, then clicking the New menu item will provide you with an option to create a new file collaboration job. The New action is available in the toolbar as well.
Save / Save All	This button will be enabled if any of the open jobs have been modified. Selecting Save will result in the currently open and selected job to be saved to disk. Save All saves all open and modified jobs to disk.
Exit	Selecting this option will exit the PeerLink Hub Client application. Note that as long as the PeerLink Hub Service remains running, all running jobs will continue to operate.

Window Menu

Open Perspective	Open a predefined layout of views geared towards a specific purpose. For example, one perspective is for job creation and management, while another is for managing PeerLink Agents .
Reset Perspective...	Selecting this option will reset all current windows, views and editors to their default size and layout.
Preferences	Opens the Preferences window allowing the user to configure settings for the PeerLink Hub, as well as global settings for file collaboration sessions .
Refresh	Refreshes all current views and tabs.
View Progress	Opens the progress view which displays information pertaining to any running background tasks within the PeerLink Hub.
View Job Alerts	Opens the Job Alert view which displays alerts such as job restarts, etc.
View Alerts	Opens the Alert view which displays PeerLink Hub alerts such as PeerLink Agent connection status changes, etc.

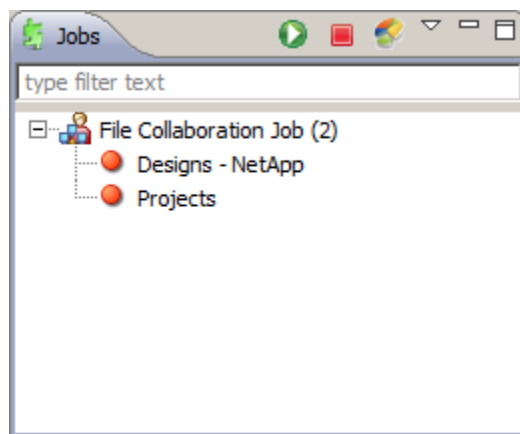
Help Menu

User Guide	Selecting this option will open this help manual.
Download Agent Installer	This operation takes you to our website where you can download the PeerLink Agent installer compatible with this version of the PeerLink Hub.
Retrieve Hub & Agent Logs	This operation will collect and retrieve all useful log files for specified PeerLink Agents, the PeerLink Hub, and all configured jobs. All of this information will be assembled in a single zip file that can optionally be uploaded to our technical support Amazon Web Services account. The collection and retrieval of the log and support files will be performed in the background which might take awhile depending on content size and network speed. Upon completion, you will be notified and will be able to view

	the zip file yourself.
Retrieve Broker Statistics	This will display detailed statistical information about all messaging that has transpired for all connections (PeerLink Agents and the PeerLink Hub) to the PeerLink Broker .
Generate Thread Dump File	This will generate a thread dump of the running PeerLink Hub Client and Service which can be used by our technical support to debug certain issues.
About	Displays version information about the PeerLink Hub along with which components are installed.

Job View

The Job View is located in the top left section of the [PeerLink Hub](#) and contains a list of all [Peerlet](#) types and saved instances.



Double-clicking on any [job](#) will open the selected job in the [File Collaboration Runtime View](#), while double-clicking on the Peerlet type **File Collaboration** will open the [Collaboration Summary View](#) in the open tabs section.

Context Menu

Right-clicking on any job will open a context popup menu with the following options:

Open	Open the selected job in an already open tab within the File Collaboration Runtime View. Otherwise, a new tab will be opened for the selected job.
Open in New Tab	Open the selected job in a new tab within the File Collaboration Runtime View.
Start	Start the selected job if it is not already running.
Stop	Stop the selected job if it is already running.
Delete	Delete the selected job from the PeerLink Hub and from disk.
Edit Con-	Edit the configuration for the selected job.

figura- tion(s)	
Copy	Copy the selected job while assigning it a unique name.
Rename	Rename the selected job.

Selecting multiple jobs and right-clicking will show a subset of the above context popup menu. Doing so, will allow you to open, start, stop, and edit multiple jobs at once. For more information, see the [Multi-Job Edit Section](#) of this help document.

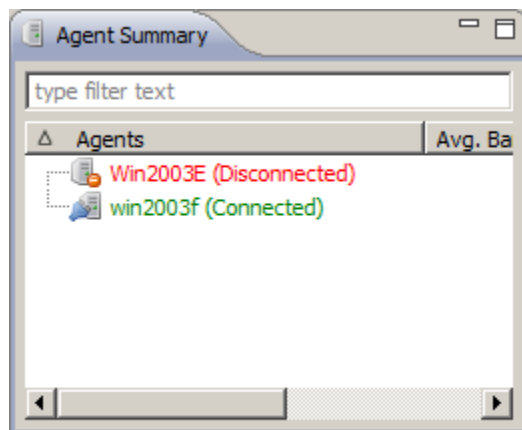
Toolbar

The following buttons are available on the toolbar within the Job View:

Start Job	Start one or more selected and currently stopped jobs.
Stop Job	Stop one or more selected and currently running jobs.
View Runtime Summary	View a table of summary information for all jobs of a selected Peerlet type. The View is defined and opened by simply clicking on a job ("Such as "Document Collaboration" in the image above) or it's parent Peerlet type (or "File Collaboration" in the image above), then pressing the View Runtime Summary button.

Agent Summary View

The Agent Summary View is located in the bottom left section of the [PeerLink Hub](#) below the [Job View](#). This view contains a list of all known [PeerLink Agents](#) installed in your environment and displays the current connection status for each.



Valid connection statuses are:

Con- nec- ted	Indicates Agent is currently connected to the PeerLink Broker .
Discon-	Indicates that Agent has disconnected from the PeerLink Broker. This can be a result of stopping the PeerLink Agent, or if the network connec-

nected	tion between the PeerLink Agent and the PeerLink Broker was severed.
Pending Disconnect	This indicates that a heartbeat for the Agent was not received within the configured threshold and that the Agent is in the process on being disconnected if a heartbeat is not received soon. This status can also occur if the Agent does not respond to a pending ping.
Unknown	If no connection status is displayed, then either the PeerLink Agent was not running on that host when the PeerLink Hub was started, or the first heartbeat message has not been received from that host.

Agent Menu Options

Right clicking on one or more host names in the Agent list will open a context popup menu with the following options:

Remove	This will remove the selected Agent(s) from the view, but if the Agent is still running or connects again, then it will be added back to the list when the next heartbeat is received.
View Properties	Displays properties for the selected Agent, e.g. heartbeat information, host machine configuration, messaging statistics, performance statistics, etc. See the section View Agent Properties Dialog for more details.
Edit Configuration	Clicking on this menu item will display a dialog where you can edit user configurable properties for the selected Agent.
Restart Agent Service	If the selected Agent is connected, this menu item will restart the PeerLink Agent Windows service running on the corresponding host. In the event that the Agent is not connected to the Broker, an attempt will be made to restart the PeerLink Agent Windows service using the Windows sc command. Please note that this will only work if the user running the PeerLink Hub Client can access the remote Agent system and has the appropriate domain permissions to start and stop services on the remote Agent system.
Edit Agent Configuration	This action displays a dialog through which the selected Agent can be configured. Configurable options include PeerLink Broker connectivity, Agent logging, Agent memory usage, among others. For more information, see the page on Central Agent Configuration .
Test Agent Bandwidth Speed	If the selected Agent is connected, this menu item will start a bandwidth speed test to be performed in the background. You will be notified at completion with the results of the test.
Retrieve Log Files	This action retrieves log files for the selected Agent containing information used by our technical support staff to assist in debugging issues. The log files will be located in the support folder of the PeerLink Hub installation directory and can optionally be uploaded to our technical support Amazon Web Services account.
Generate Debug File	This action generates a file on the selected Agent containing information used by our technical support staff to assist in debugging issues. The debug file will be located in the Agent's installation directory.

Copy File	This action copies a specified file from the PeerLink Hub to the designated target folder on each selected Agent. The target folder is relative to the Agent installation directory.
Transfer Rate Report	This action displays a time series performance chart of average transfer rate for the selected Agent over the last 24 hours.

Agent Updates

Additionally, if the Agent software running on a host is out of date, the host will be shown as having a pending update in the Agent Summary View. When right-clicking on the host, the option to automatically update the Agent software will also be available. This process can be done right from the PeerLink Hub and usually does not require any additional actions on the host server itself.

View Agent Properties Dialog

Selecting "View Agent Properties" menu item for a selected host will result in the opening of the following Agent Properties dialog:

View Agent Properties

General | Performance | Heartbeat | Machine | JVM Performance | Messaging

Processors: 1

Computer Description:

Computer Name: WIN2003F

Domain Name: BYTEMETRICS

IP Address: 192.168.171.108

Installed Memory: 536248320 Bytes

OS: Windows 2003

Processor 64-bit: ☐

Processor Desc.: Intel(R) Xeon(R) CPU X5365 @ 3.00GHz

Processor Frequency: 2992

Processor Vendor: GenuineIntel

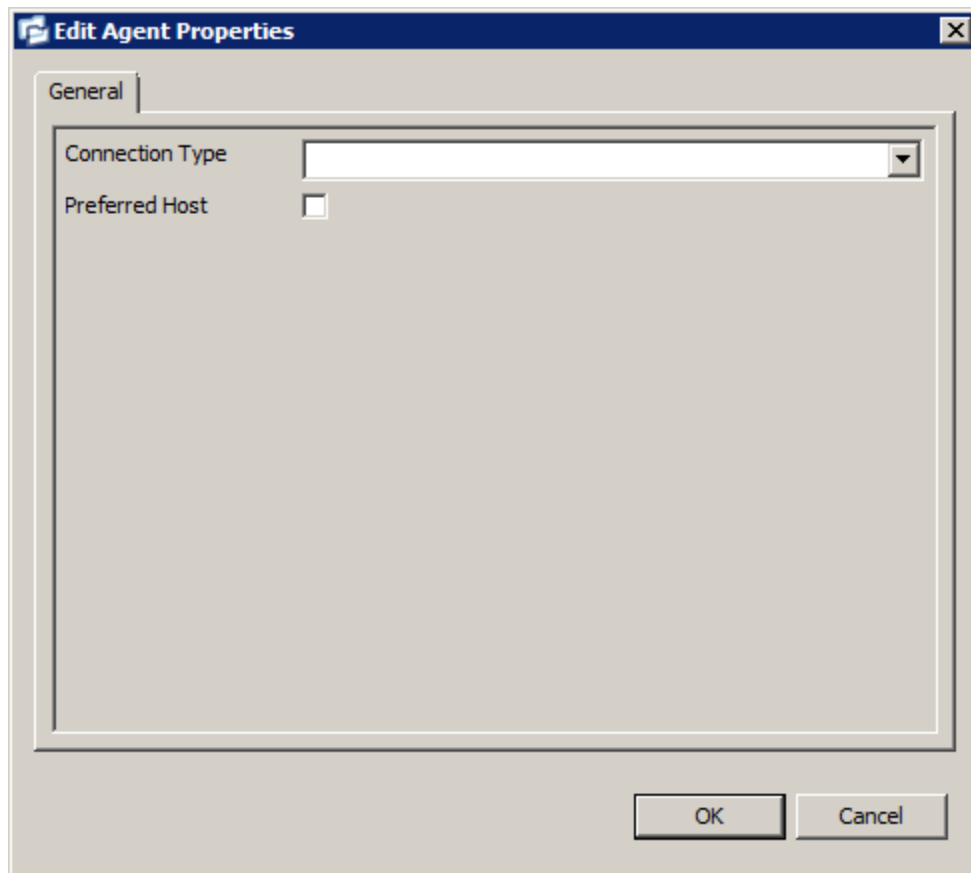
OK Cancel

This dialog displays Agent and host machine information across the following categories:

Machine	Displays machine information of the host that the PeerLink Agent is running on such as, # of processors, computer name, domain name, IP address, installed memory, O/S, etc.
Heartbeat	Displays heartbeat information and statistics such as, heartbeat frequency, avg heartbeat time, last heartbeat time, total Agent disconnects, total missing heartbeats, etc.
Performance	Displays general performance statistics for the underlying host machine such as, available virtual memory, available physical memory, memory load, etc.
JVM Performance	Displays JVM performance statistics for the running PeerLink Agent application such as active # of threads, heap memory used, non-heap memory used, etc.
Messaging	Displays general PeerLink Broker messaging statistics for the selected host, such as, total messages received, total messages sent, # errors, etc.
General	Displays general Agent runtime information such as, discovery time, local time, SSL use, Agent startup time, Agent version, user name Agent service is running as, etc.

Edit Agent Properties Dialog

Selecting "Edit Agent Properties" menu item for a selected host will result in the opening of the following Agent Properties dialog:



This dialog displays the following configurable Agent and host machine options:

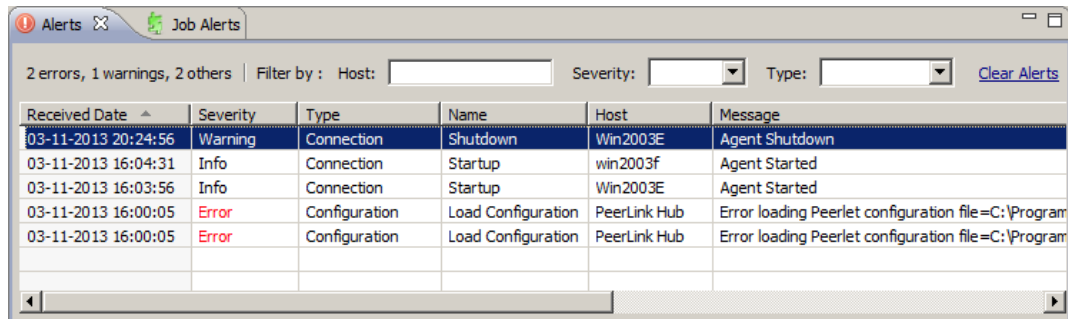
Connection Type	Allows for the selection of a connection type between selected Agent and it's associated PeerLink Broker. When set, optimizations are made to the communication between the two parties based on the selected connection type.
Preferred Host	A best practice optimization for selecting which Agent has the fastest connection to the PeerLink Broker (or in appropriate cases, for selecting which Agents are on the same subnet as the PeerLink Broker)

Alerts View

The Alerts View is automatically displayed when a critical system (Error or Fatal) alert is received. By default, the Alerts View is displayed under the [File Collaboration Runtime View](#). You can close the view at anytime by clicking on the **X** (close) button on the Alerts tab. You can open the Alerts view at any time by clicking on the **View Alerts** button located on the [PeerLink Hub](#) toolbar or by selecting the **Window** menu, then the **Show View** submenu, followed by the **View Alerts** menu item.

Alert severity is broken down into four main categories: Informational (containing Info, Debug, and Trace), Warning, Error and Fatal. An example of an Informational alert is when an [Agent](#) connects to the [PeerLink Broker](#). If an Agent's network connection is severed, then an Error alert will be logged. All alerts are also logged to the file **hub_alert.log**, available under the 'Hub\logs' subdirectory within the PeerLink Hub installation directory.

You can filter alerts based on host name, severity level, or type, and you can sort alerts by clicking on a specific column header. You can also clear all alerts in the table by clicking the **Clear Alerts** link.



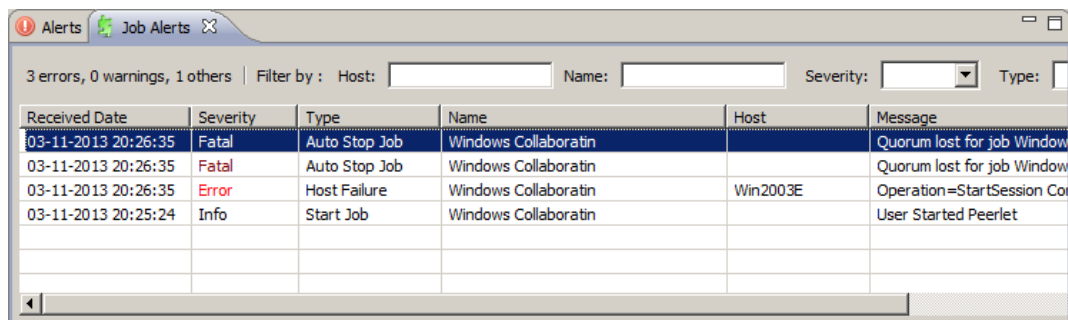
You can also resize the Alerts View by dragging the separator between the upper view and the Alerts View, or you can double-click on the Alerts tab to maximize the view. You can restore the view to its original, non-maximized size by double-clicking on the Alerts tab again.

Job Alerts View

The Job Alerts View is automatically displayed when a critical [job](#)-related (Error or Fatal) alert is received. By default, the Job Alerts View is displayed under the [File Collaboration Runtime View](#), alongside the standard [Alerts View](#). You can close the view at anytime by clicking on the **X** (close) button on the Job Alerts tab. You can open the Job Alerts view at any time by clicking on the **View Job Alerts** button located on the PeerLink Hub toolbar or by selecting the **Window** menu, then the **Show View** submenu, followed by the **View Job Alerts** menu item.

Job alert severity is broken down into four primary categories: Informational (containing Info, Debug, and Trace), Warning, Error and Fatal. An example of an Informational alert is when a job is started or stopped manually by the user. If a job loses one of its [participating hosts](#) and as a result, cannot keep a quorum and shuts down, then a Fatal alert will be logged. All alerts are also logged to the file **job_alert.log**, available under the 'Hub\logs' subdirectory within the [PeerLink Hub](#) installation directory.

You can filter alerts based on host name, job name, severity level, or type, and you can sort alerts by clicking on a specific column header. You can also clear all alerts in the table by clicking the **Clear Alerts** link.



You can also resize the Job Alerts View by dragging the separator between the upper view

and the Job Alerts View, or you can double-click on the Job Alerts tab to maximize the view. You can restore the view to its original, non-maximized size by double-clicking the Job Alerts tab again.

Creating a File Collaboration Job

The topics in this section provide some basic information about creating and editing File Collaboration Jobs.

Overview

[File Collaboration Jobs](#) are created using the [PeerLink Hub](#). When configuring your first job, we strongly recommend that you first configure the Global File Collaboration settings, as well as global settings like SMTP configuration, which is specific to the PeerLink Hub. Details on what and how to configure these global options can be found in the [Global Configuration](#) section.

To create a new job, once global options are set, click the **Create New** button in toolbar of the PeerLink Hub, or you can select the **New** menu item from the **File** menu. A list of all installed Peerlet types will be displayed. Selecting the **File Collaboration** option will prompt you for a unique name for the job, then open the File Collaboration Configuration dialog.

You can edit an existing job by selecting one or more jobs in the [Job View](#), right-clicking, and selecting **Edit Configuration(s)**. The PeerLink Hub now has support for editing multiple jobs at once. Please see the section on [Multi-Job Edit Support](#) for more details.

Configuring a file collaboration session will require the following steps:

- [Global Configuration](#) (important to configure before setting up your first job)
- [Step 1 - Host Participants & Folders Settings](#) (the beginning process of creating an individual file collaboration job)
- [Step 2 - General Settings](#)
- [Step 3 - File Filters Settings](#)
- [Step 4 - File Conflict Resolver Settings](#)
- [Step 5 - Delta Compression](#)
- [Step 6 - File Metadata](#)
- [Step 7 - File Locking](#)
- [Step 8 - Logging and Alerts](#)
- [Step 9 - Target Protection](#)
- [Step 10 - Email Alerts](#)
- [Step 11 - Save Settings](#)

Global Configuration

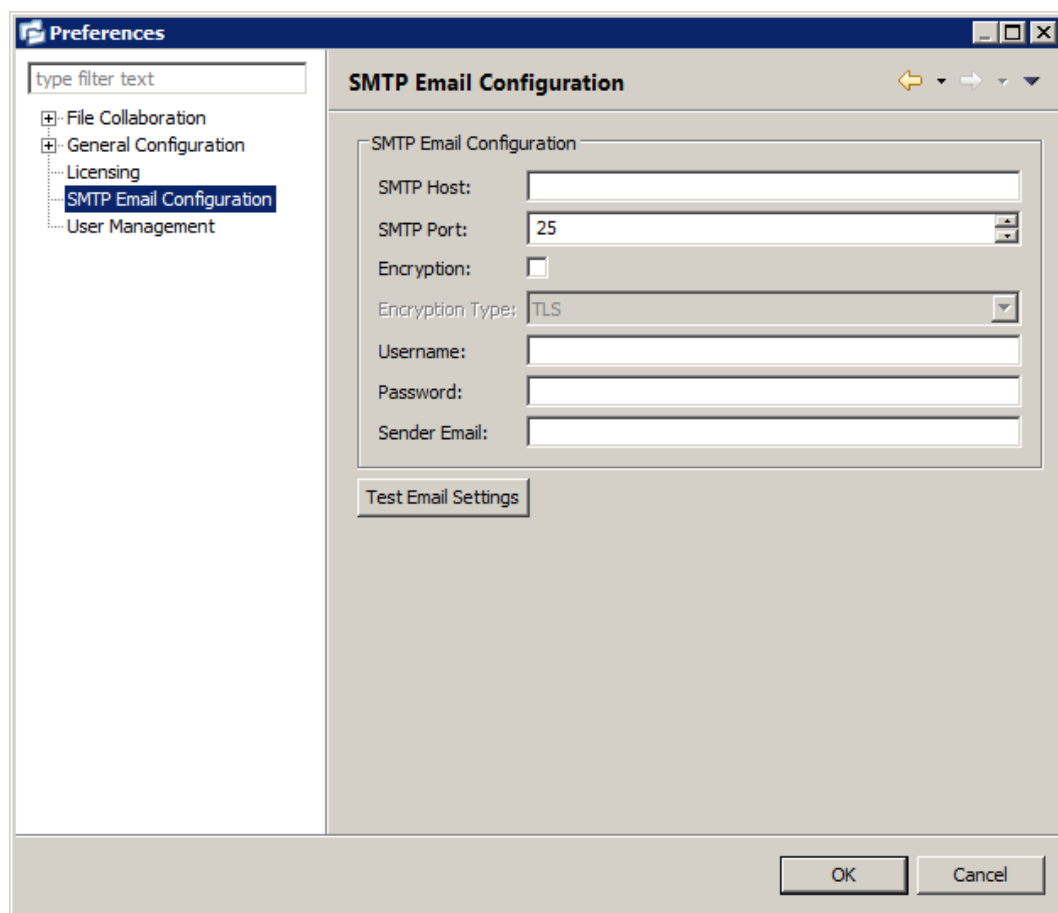
Before configuring the individual aspects of a file collaboration session, we first recommend pre-configuring a number of global options that can be applied towards all file collaboration sessions.

The following configuration items are not always required, but highly recommended:

- [SMTP Email Configuration](#)
- [Email Alerts](#)
- [SNMP Alerts](#)
- [File Filters](#)

1. SMTP Email Configuration

Before the [PeerLink Hub](#) can send emails on behalf of any file collaboration job, a few key SMTP settings must be configured. To set these values, click on the **Window** menu from within the PeerLink Hub, and select **Preferences**. Within the dialog that pops up, select **SMTP Email Configuration** on the left-hand side of the dialog. The following screen will be displayed.



SMTP Host (required)	The host name or IP address of the SMTP mail server through which the PeerLink Hub will send emails.
SMTP Port	TCP/IP connection port (default is 25 and 465 for encryption) on which the mail server is hosting the SMTP service. It is recommended that you leave the default setting unless your email provider specifies otherwise.

Encryption	Check this box if the SMTP mail server requires an encrypted connection.
Encryption Type	If encryption is enabled, an encryption method must be selected. TLS and SSL are the available options. If you do not know which one your mail server requires, try one then the other.
User	The username to authenticate as on the SMTP mail server (optional).
Password	The password of the username specified above (optional).
Sender Email (required)	The email address that will appear in the From field of any sent emails. This email address sometimes needs to have a valid account on the SMTP mail server.

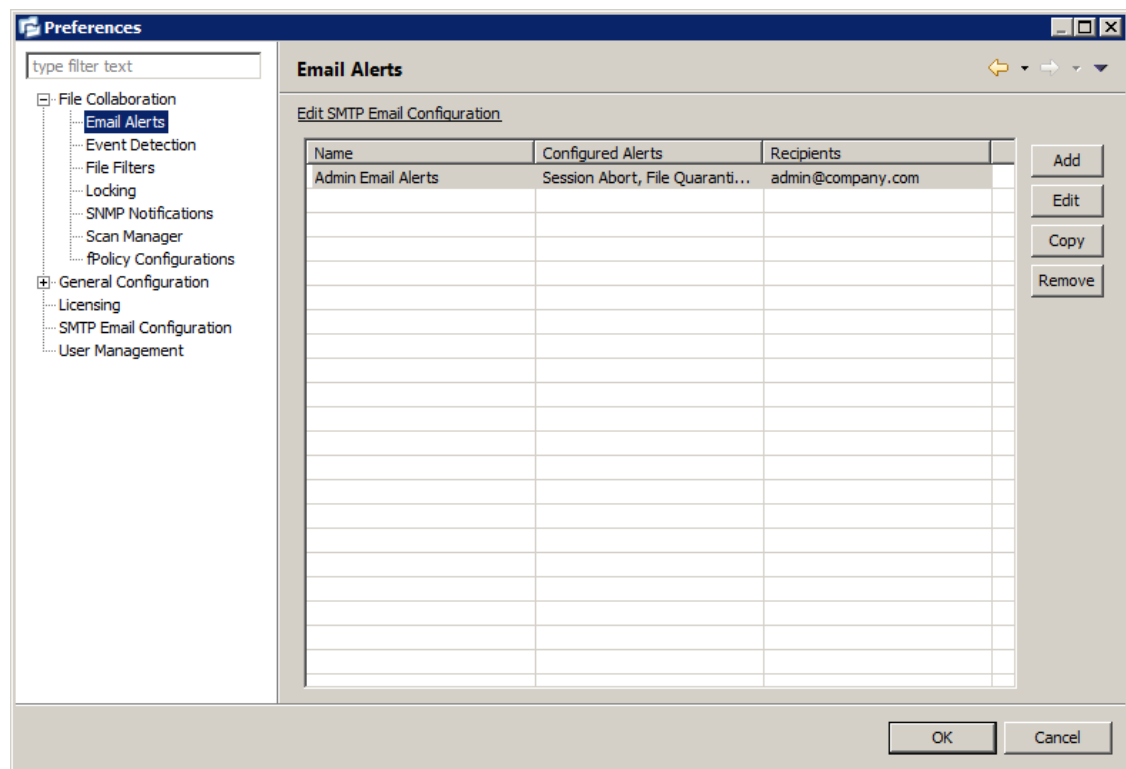
It is highly recommended that you test your SMTP settings before saving them. To do so, click on the **Test Email Settings** button. You will be prompted for an email address to send the test message to. Upon submission, the PeerLink Hub will attempt to send a test message using the specified settings.

2. Global Email Alerts

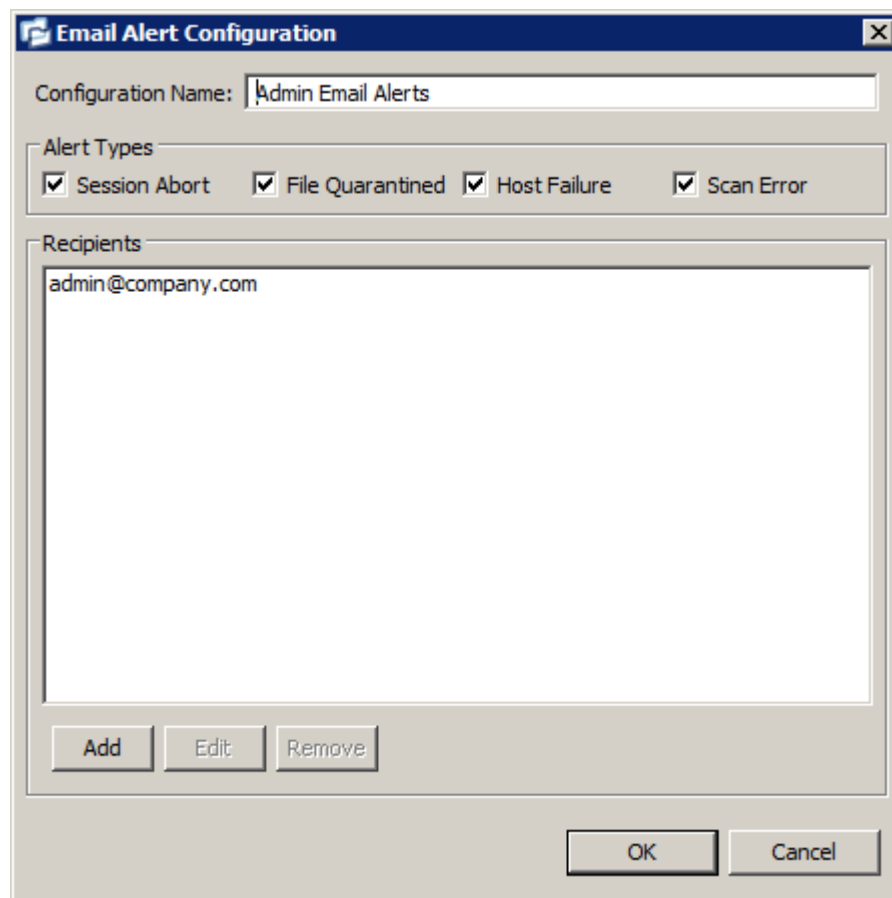
Overview

The [PeerLink Hub](#) supports the concept of "Email Alert Configurations" where a single configuration (consisting of a unique name, a selection of alert types along with a list of email addresses) can be applied to multiple [file collaboration jobs](#) without requiring repeat entry for each job. When an Email Alert configuration is applied to a job, an email will be sent to all listed recipients anytime a selected alert type is triggered by that job.

To manage these configurations, navigate to the Window menu of the PeerLink Hub, select Preferences, then navigate to and select Email Alerts from the tree node on the left. The following screen represents the list of defined Email Alert configurations, along with buttons to add new ones and edit, copy and remove existing ones.



Upon adding or editing an Email Alert configuration, the following dialog is displayed:



Within this dialog, you can select specific alert triggers on which an email will be generated and configure the list of email recipients of the alert(s). Alert types are defined below.

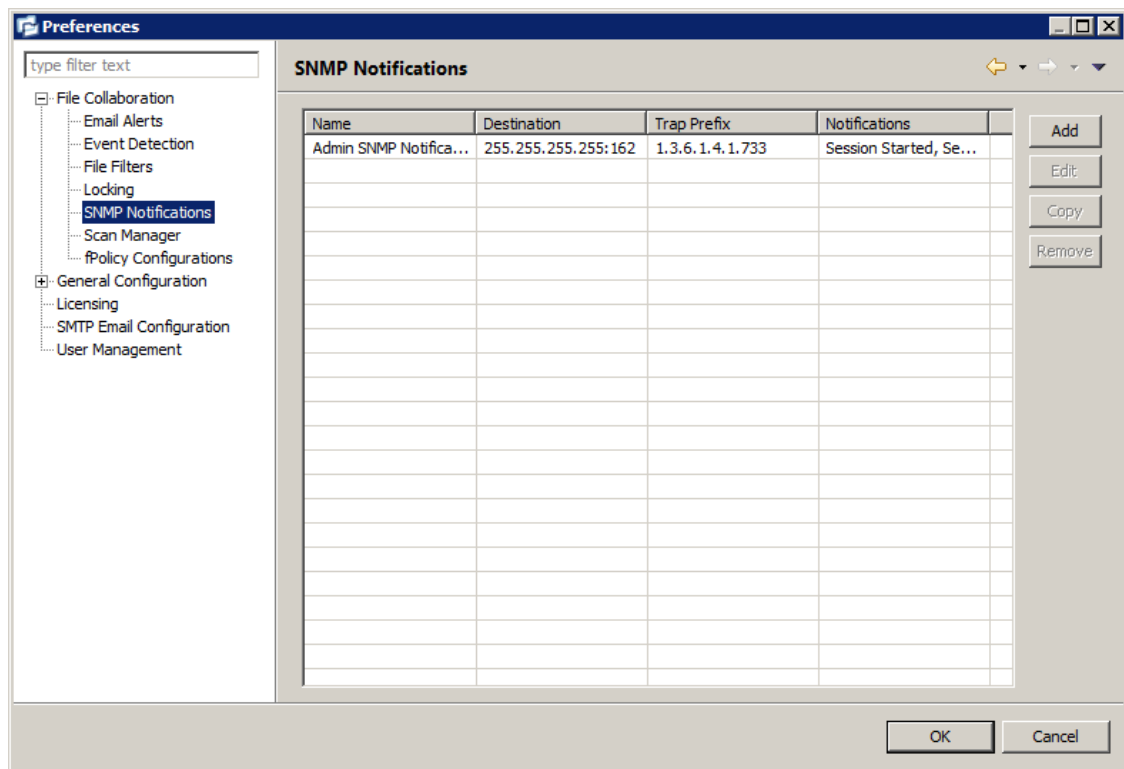
Alert Types

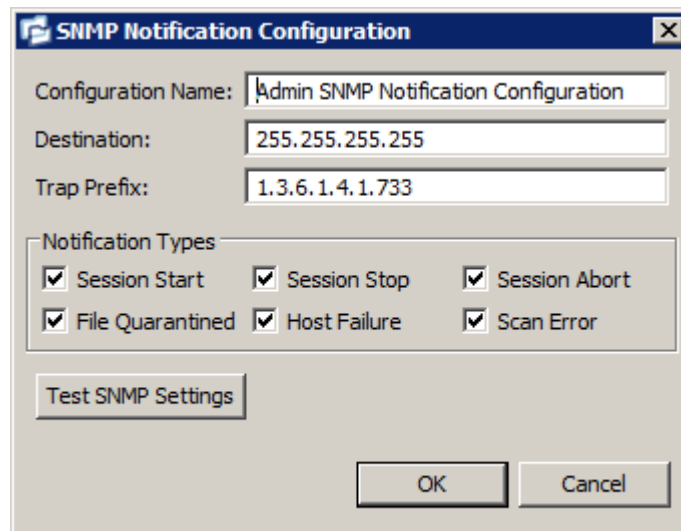
Session Abort	Enables sending an alert when a session is aborted because of lack of quorum due to one or more failed hosts.
File Quarantined	Enables sending an alert when a file is marked as quarantined because a file conflict was not able to be resolved.
Host Timeout	Enables sending an alert when a host timeout occurs and the host is taken out of session.
Scan Error	Enables sending an alert when an error occurs during the initial synchronization process .

3. Global SNMP Notifications

Overview

To manage these configurations, navigate to the Window menu of the PeerLink Hub, select Preferences, then navigate to and select SNMP Notifications from the tree node on the left. The following screen represents the list of defined SNMP Notification configurations, along with buttons to add new ones and edit, copy and remove existing ones.





Within this dialog, you can select specific triggers on which an SNMP trap will be generated, configure the destination host name, IP address, or broadcast address, set the prefix that is attached to every message (helping to identify messages coming from specific instances of the PeerLink Hub or jobs across a network), and test the aforementioned settings. Notification types are listed below.

Notification Types

Session Start	Enables sending a notification when a session is started.
Session Stop	Enables sending a notification when a session is stopped.
Session Abort	Enables sending a notification when a session is aborted because of lack of quorum due to a failed host(s).
File Quarantined	Enables sending a notification when a file is marked as quarantined because a file conflict was not able to be resolved.
Host Timeout	Enables sending a notification when a host timeout occurs and the host is taken out of session.
Scan Error	Enables sending a notification when an error occurs during the initial synchronization process .

4. Global File Filters

Overview

Filter expressions govern the inclusion and exclusion of files under the [Watch Set](#). Included files are subject to scan and event detection, while excluded files are not. Initially, all files are included and no files are excluded, except for the internal expressions listed below under [Auto Excluded Filter](#).

Filtration can be configured with wildcard expressions to more easily cover well-known file extensions or names that follow established patterns. When a single expression is insufficient for configuring filtration, multiple expressions may be supplied. You can also filter file based on a file's last modified time and file size.

Usage Notes

Since inclusions and exclusions are expressed separately, it is possible to submit conflicting expressions. The expression evaluator addresses this by exiting when a file is determined to be excluded. Therefore, exclusions expressions override inclusion expressions.

Rename operations may subject files to an inclusion status change. Renaming a file out of the Watch Set will trigger a target deletion, while renaming into the Watch Set triggers a target addition.

Folder deletions only affect included files, possibly leading to folder structure inconsistencies. When a session participant deletes a folder, the target outcome will vary depending on whether excluded files are present. Folder deletions are propagated in detail to the targets as to the exact files that have been affected.

Auto Excluded Filter

The following wild card expressions are automatically applied as exclusion expressions and cannot be changed:

Temporary files generated by common applications

~\$*.
*.tmp
*.\$\$\$

Any file without a file extension, e.g. abcdefg

Explorer System Files

desktop.ini, thumbs.db, and Windows shortcut file e.g. *.lnk

Configuration Notes

The excluded and included file name filters take one or more standard wildcard expressions that are combined by performing a logical OR of each wildcard expression.

Standard Wildcard Expressions

*	Matches zero or more characters of any value
?	Matches one character of any value

The following examples show the use of wildcard syntax to enter a file exclusion or inclusion:

***.ext** Filter files that end with the .ext extension
ext Filter files that contain the string ext
ext* Filter files that start with the string ext

PeerLink also supports the use of complex regular expressions, e.g. <<regEx>>. These ex-

pressions can be used for either included or excluded patterns. For information on where to enter a regular expression, see the Configuration section immediately below.

A good reference on regular expressions can be found here: <http://www.regular-expressions.info/reference.html>

Filtering on Folders

In addition to filtering on files, you can filter on folders using the following syntax: **\Folder** or **\Folder*** or **\Folder***

Presently, PeerLink only supports included expressions for a full folder path, and does not support wildcard matching on parent paths. For example, the following expression is not valid: **\Folder*\Folder**

Reduce the Number of Jobs Using Folder Filtering

For management purposes, we recommend keeping the total number of jobs as low as possible, preferably to no more than 10. Using folder filters, you can reduce the total number of jobs without sacrificing efficiency. This process involves analyzing all existing jobs, identifying all the folders and hosts that will be collaborating, and consolidating them into fewer jobs by watching a few root folders at a higher level. Filters will then be added to include or exclude only the folders of interest. Here is a small example which demonstrates this concept:

Example:

Reduce existing four jobs down to two:

		Server 1		Server 2	
		Drive D	Drive E	Drive D	Drive F
Old Jobs	Job 1	D:\General		D:\General	
	Job 2		E:\Common		F:\Common
	Job 3	D:\Projects		D:\Projects	
	Job 4		E:\Documents		F:\Documents

After consolidation:

		Server 1	Server 2	Filter Option 1 INCLUDE	Filter Option 2 EXCLUDE
New Jobs	Job 1	D:\	D:\	\General* \Projects*	All other files
	Job 2	E:\	F:\	\Common* \Documents*	All other files

Jobs 1 and 3 were merged into a single job watching the root D drive on both servers while using Filter Option 1 or 2.

Jobs 2 and 4 were merged into a single job watching the root E drive on Server 1 and the root F drive on Server 2 while using Filter Option 1 or 2.

Please note the following regarding regular expressions:

- PeerLink does not support the ability to use Regular Expressions for multi-level folder inclusions such as **\Level1\Level2\FolderName**.
- PeerLink does not currently support the ability to filter on certain parts of a path, like **\Folder*\Folder** and **\Folder***.

Additional Folder Filter Examples

To exclude a specific folder from anywhere within the Watch Set:

```
*\FolderName  
*\FolderName\FolderName
```

To exclude a specific folder from the ROOT of the Watch Set:

```
\FolderName  
\FolderName\FolderName
```

To exclude folders that END with a specific name from anywhere within the Watch Set:

```
*FolderName\
```

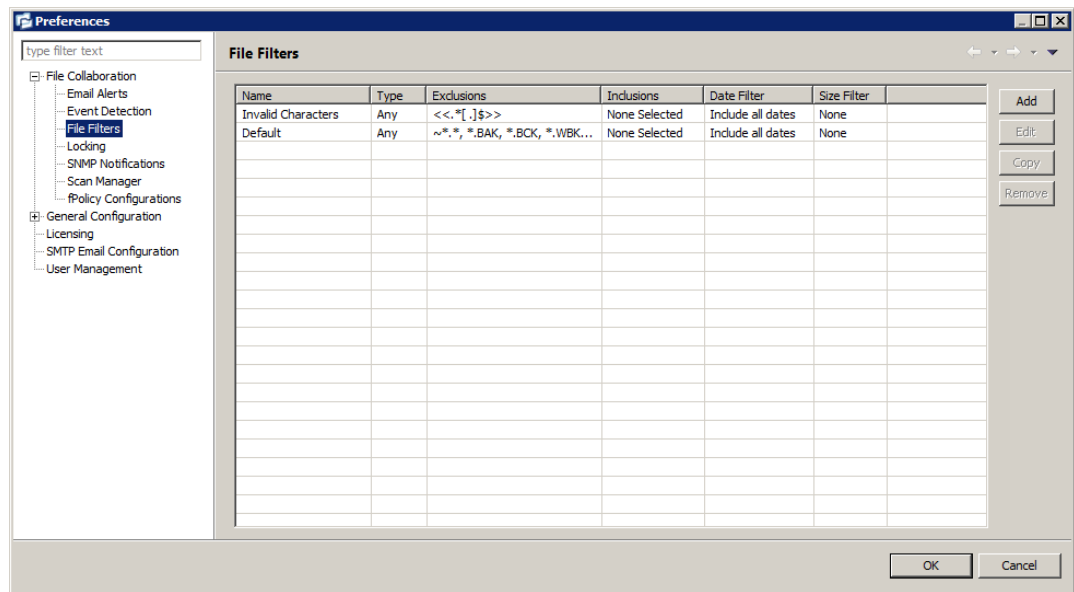
To include a specific folder from the ROOT of the Watch Set:

```
\FolderName  
\FolderName\FolderName
```

Configuration

The [PeerLink Hub](#) supports the concept of "File Filter Configurations" where a single configuration (consisting of a unique name, and lists of inclusion and exclusion expressions) can be applied to multiple [file collaboration jobs](#) without requiring repeat entry for any job. This capability also allows you to define File Filter combinations for use with specific collaboration scenarios.

To manage these configurations, navigate to the Window menu of the PeerLink Hub, select Preferences, then navigate to and select File Filter Configurations from the tree node on the left. The following screen represents the list of defined File Filter configurations, along with buttons to add new ones and edit, copy and remove existing ones. To increase flexibility, multiple File Filters can be applied to a single job, combining elements of each to form one large filter. For more information on selecting multiple filters, see the page on [File Filter Selection](#).



Upon adding or editing a File Filter configuration, the following dialog is displayed:

File Filter Configuration

Configuration Name:

Filter Type:

Auto Excluded

To see a list of file types that are automatically excluded from collaboration, [click here](#).

Excluded File Name & Path Wildcard Patterns

~*,*
*.BAK
*.BCK
*.WBK
*.ASD
*.XLK

[Add Default Exclusions](#)

Included File Name & Path Wildcard Patterns

Included Last Modified Dates

days

Excluded File Sizes

bytes

When creating a File Filter configuration, you will generally want to exclude all temporary files created by the applications you use so they are not propagated to the targets hosts. For example, AutoCAD applications should add the following expressions to the Excluded File Name filter table:

*.AC\$
*.SV\$
.DWL
*.BAK

To do so:

1. Click the Add button under the Excluded File Name Wildcard Pattern table and enter *.AC\$ and then click OK.
2. Repeat Step 1 to add *.SV\$, *.DWL* and *.BAK

Your AutoCAD temporary file exclusion filter configuration is now created and all files ending in *.SV\$ or *.AC\$ or *.DWL or *.BAK will be excluded from collaboration within any running file collaboration job that uses this configuration..

Additionally, complex regular expressions in the format **<<regEx>>** can be used in both the inclusion and exclusion pattern lists. An example is shown in the dialog screenshot above (**<<^.*\\atmp[0-9]{4,}\$>>**).

The following regular expression excludes any path containing a folder "XX" which also contains a child folder "YY"

<<^.*\\XX\\YY(\\.*\$)\$>>

The following files and folders MATCH the above expression:

```
\\projects\\xx\\yy
\\accounting\\projects\\xx\\yy\\file.txt
\\accounting\\projects\\xx\\yy\\zz\\file.txt
```

The following files and folders DO NOT MATCH the above expression:

```
\\projects\\accounting\\file.txt
\\projects\\xx\\y
\\projects\\xx\\yyy\\file.txt
\\accounting\\projects\\xx\\file.txt
\\accounting\\projects\\yy\\xx\\zz\\file.txt
```

Filtering on Last Modified Time

In addition to filtering on file names, file extensions, folder paths, or partial path wildcard pattern matching, you can filter based on a file's last modified time. PeerLink only supports filtering on a file's last modified time and does not support filtering on a folders last modified time.

In addition, if you have a folder hierarchy that contains files which are all being filtered based on last modified time, then all folders will still be created during the initial scan process on all hosts. If a file is excluded from collaboration based on last modified, then the initial scanning process will not synchronize the file even if the file's last modified time and size do not match, or the file does not exist on all hosts. However, the file will be synchronized, if and when the file is modified in the future, and if a user deletes or renames the file on any host, the file will be deleted or renamed from all other hosts where the file exists.

Included Last Modified Date Filter Options

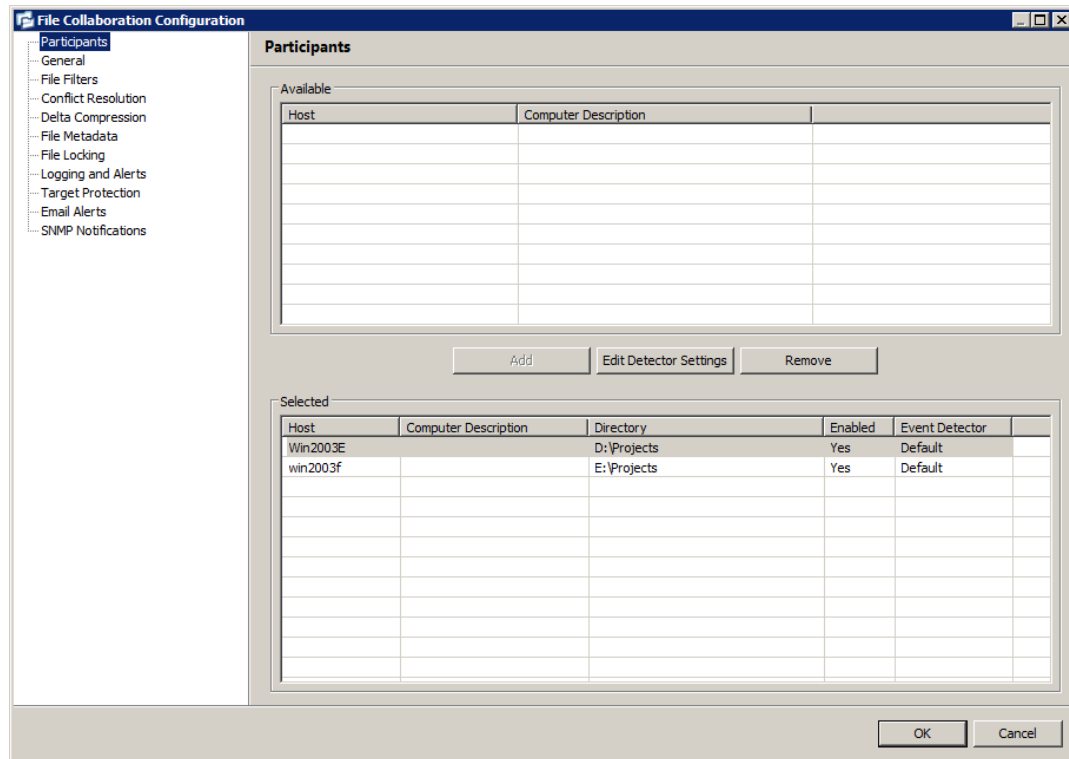
Include all dates	This is the default option and will include all folder and files regardless of it's last modified time.
Include today and past	Includes all files whose last modified date are more recent then the specified number days. For example, you can exclude all files that have not been modified for the last year (365 days).
Include older than	Includes all files whose last modified date are older then the specified number days.

Step 1 - Host Participants and Directories

Once [global options](#) have been configured, create a new [file collaboration job](#) by clicking on the **Create New** button in toolbar of the [PeerLink Hub](#), or by selecting the **New** menu item

from the **File** menu. A drop down list of all installed [Peerlet](#) types will be displayed. Selecting the **File Collaboration** option will prompt you for a unique name for the job, then open the File Collaboration Configuration dialog..

The first page of configuration will be for [Host Participants](#) of the file collaboration job. On this page, you will select and configure which hosts will be participating in this job.



Participant configuration steps are as follows:

1. A list of all available hosts will appear in the **Available** table on the top of the page. Available hosts are any host with a [PeerLink Agent](#) installed that has successfully connected to the configured [PeerLink Broker](#). The name that will be displayed is the computer name of the server that the PeerLink Agent is running on. If a particular host is not displayed in the list then try restarting the PeerLink Agent Windows Service on that host, and if it successfully connects to the PeerLink Broker, then the list will be updated with the computer name of that host.

NOTE: Computer Description is defined through Windows on a per-computer basis.

2. Select two or more hosts from the **Available** table and click on the **Add** button to add the hosts to the **Selected** table.
3. For each selected host you will need to type in the path to the Root Folder, and then press enter. The Root Folder for all hosts can be identical, or they can have different absolute path names based on your needs.
4. Optionally, if you would like to exclude real time events from certain users, this can be done by selecting the desired host in the **Selected** table and clicking **Edit Detector Settings**. This is helpful if you are trying to prevent events generated from backup and/or archival tools from triggering activity. Usernames should be separated by commas.

5. If you are properly licensed to and wish to include a NetApp storage device within a file collaboration job, additional configuration is required for each selected host that is to interface with a NetApp storage device via the NetApp FPolicy API. For more information, please review the [NetApp Configuration](#) section.

NOTE: From this point on, no other configuration items are mandatory. You can leave the rest of the configuration settings as their default values and move onto to [Step 10 - Save Settings](#). If you wish to continue configuring the job, please continue to [Step 2 - General Settings](#).

Step 2 - General Settings

The General Settings page contains miscellaneous configuration items pertaining to a [file collaboration job](#) and is available by selecting **General** from the tree node within the File Collaboration Configuration dialog.

The screenshot shows the 'File Collaboration Configuration' dialog box with the 'General' tab selected. The left sidebar contains a tree view with the following items: Participants, General (selected), File Filters, Conflict Resolution, Delta Compression, File Metadata, File Locking, Logging and Alerts, Target Protection, Email Alerts, and SNMP Notifications. The main area displays the following settings:

- Application ID: 100
- Session Name: Projects
- Transfer Block Size (KB): 128
- Verify Checksum: ☒
- Session Threads: 10
- File Copy Threads: 5
- Background Sync. Threads: 5
- Timeout (Seconds): 180
- Scan Delay (Seconds): 10
- Remove Filtered Files On Folder Delete: ☐
- Require All Hosts At Start: ☐
- Auto Start: ☐

At the bottom right, there are 'OK' and 'Cancel' buttons.

Configurable settings for this page are as follows:

Application ID	Unique, system-generated application identifier that cannot be edited.
Session Name	Description of this file collaboration job. This name should be unique.
Transfer Block Size (KB)	The block size in Kilobytes used to transfer files to hosts. Larger sizes will yield faster transfers on fast networks, but will consume more memory in the PeerLink Broker and Agents .
Verify	If checked, then source and target checksums will be calculated and

Checksum	verified for all file transfers. There is a small overhead associated with verifying checksums and we recommend only enabling this option for initial testing or if you suspect files are somehow being corrupted.
Session Threads	Number of concurrent file lock and change event session operations that can be performed at the same time.
File Copy Threads	Number of concurrent file transfers resulting from real-time event detection that can be performed at the same time. Set to low value for increased bandwidth throttling.
Background Sync Threads	Number of concurrent background file transfers resulting from the initial synchronization process that may be performed at one time.
Timeout (Seconds)	Number of seconds to wait for a response from any host before performing retry logic.
Allow Write Access During Sync.	If enabled, users will be allowed write access to source files that are currently being synchronized. If not checked, then users will be denied write access to source files during synchronization, but will be able to open them in read-only mode.
Convert Short File Names	If enabled, short file names containing ~ will be converted to long file name. Note that this has a slight performance hit and usually is not necessary unless users are accessing a file via its short file name from DOS prompt.
Remove Filtered Files On Folder Delete	If enabled, then all child files on target hosts will be deleted when it's parent folder is deleted on another source host. Otherwise, filtered files will be left intact on targets when a parent folder is deleted on another source host.
Require All Hosts At Start	This option requires all participating hosts to be online and available at the start of the file collaboration job in order for the job to successfully start.
Auto Start	If checked then this file collaboration session will automatically be started when the PeerLink Hub Service is started.

Once all settings are configured to your liking, you can either [save the configuration](#) and exit the dialog, or you can continue with the configuration process by going to [Step 3 - File Filters](#).

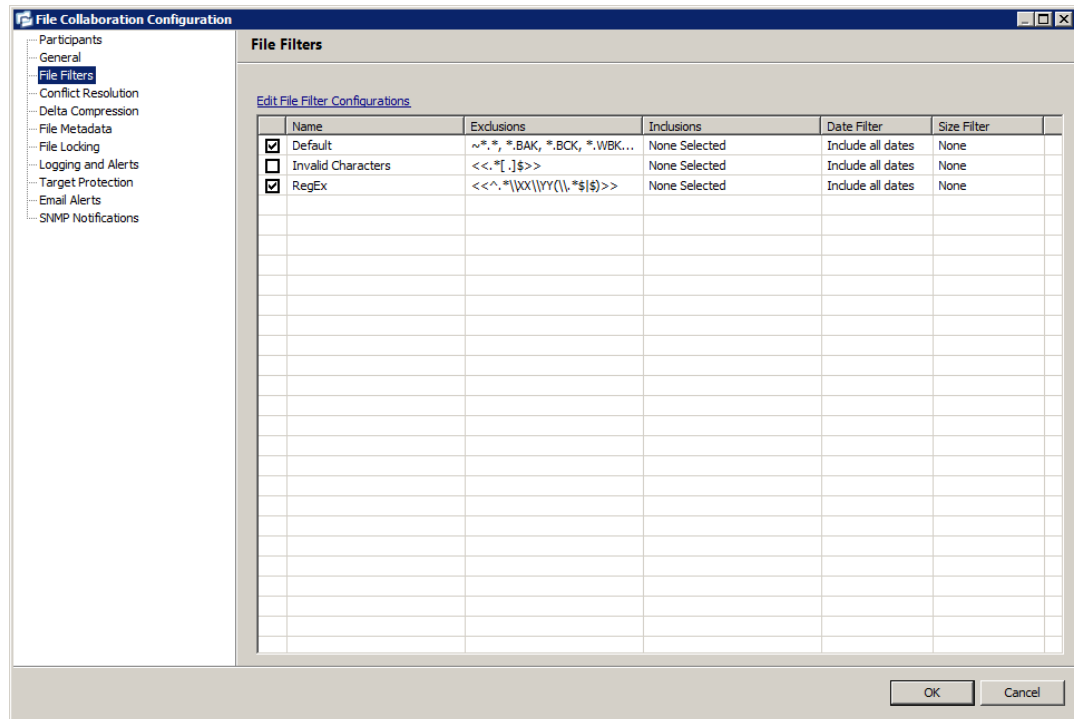
Step 3 - File Filters

File Filter configuration allows you to specify file and folder path expressions to include and/or exclude from a [file collaboration job](#), and is available by selecting **File Filters** from the tree node within the File Collaboration Configuration dialog.

File Filters are configured on a global basis within the [PeerLink Hub](#), where individual configurations can be applied to multiple jobs without having to manually re-enter each part of the configuration. For more information on what exactly a file filter is, please see the [Global File Filters](#) page. For details on how to configure File Filter configurations within the PeerLink Hub, please see the section on [Global File Filter Configuration](#).

The following screenshot shows how individual File Filter configurations can be applied to a

single job.



Each global File Filter configuration will be displayed in the table on this page. If you need to create a new file filter configuration, or edit an existing configuration via the [Global File Filter configuration](#) screen, click on the **Edit File Filter Configurations** link. Once all necessary configurations are in place, check all that you would like to apply to the current job. Each checked item will be combined into one large filter when the job is run (by combining all exclusions and inclusions together). In general, you should have at least one default global file filter that is applied to all jobs and possibly other file filters that apply to specific jobs. However, for most environments, only a single default global file filter is necessary.

Once all File Filter configurations are set and selected to your liking, you can either [save the configuration](#) and exit the dialog, or you can continue with the configuration process by going to [Step 4 - Conflict Resolvers](#).

Folder Filter Examples:

To exclude a specific folder from anywhere within the PeerLink watch set:

```
*\FolderName
*\FolderName\FolderName
```

To exclude a specific folder from the ROOT of the PeerLink watch set:

```
\FolderName
\FolderName\FolderName
```

To exclude folders that END with a specific name from anywhere within the PeerLink watch set:

```
*FolderName\
```

To include a specific folder from the ROOT of the PeerLink watch set:

```
\FolderName  
\FolderName\FolderName
```

Step 4 - File Conflict Resolution

File Conflict Resolution allows you to specify the type of file conflict resolution to use during the initial scan when a file conflict exists for a file between two or more hosts. Configuration is available by selecting **Conflict Resolution** from the tree node within the File Collaboration Configuration dialog.

Overview

Conflict resolution is a key feature of file collaboration that is in effect at the start of a session. When a [file collaboration job](#) begins, the [host participants](#)' configured folders are synchronized by a scan and merge phase, during which conflicts can be detected. Below, we will define file conflicts, describe our detection scheme, and the configuration options we provide to resolve them.

Defining a Conflict

When a session begins, the participants' folders are first scanned then merged to form a collective view of all participants' content. All files found under the designated folders are subject to collaboration, except for those excluded by filtration (see [Global File Filter Configuration](#) for more details).

A potential conflict occurs when a file path is found to exist on more than one host in a file collaboration job. For example, the following files are found to be in conflict:

```
\\Host-A\FC-Session-UserGuide\release-1.0\readme.txt  
\\Host-B\FileCollab-UG\release-1.0\readme.txt  
\\Host-C\FCS-UserGuide\release-1.0\readme.txt
```

In this example, the file 'release-1.0\readme.txt' is found to be in conflict across three hosts. Note that each host can designate varying root folders. Content below the Root Folder resides under a shared namespace. Conflicts may occur across a partial or total set of participant hosts.

A file conflict can occur for any of the following reasons:

- Two users open a file at the same time, or in-and-around the same time.
- A file is open at the start of a job and has been modified on a host where the configured conflict resolution strategy selects a different host as the winner.
- Two or more users have the same file open on different hosts when a collaboration job is started.
- A file was modified on two or more hosts between job restarts or network outages.
- PeerLink is unable to obtain a lock on a target host file for various reasons.
- PeerLink may conflict a file when an unexpected error occurs or a file is in an unexpected state.

Resolving a Conflict

The goal of conflict resolution is to designate one instance of a conflicted file as the "winning" copy or the one designated as the source for synchronization. The criteria for resolving conflicts are based on the file's metadata such as size, modification time or host name.

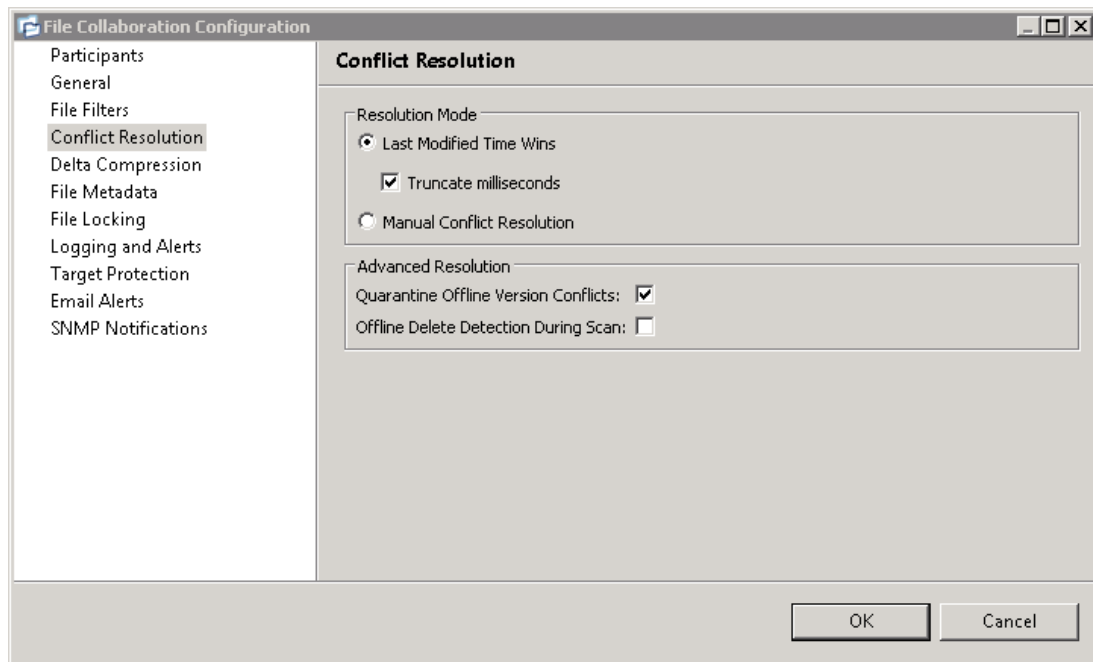
It is important to note that conflict resolution must select a single instance of a file, although it is quite possible that several copies of a file are potential candidates. Drawing from the examples listed in the previous section, if our session was configured to resolve conflicts based on a file's last modified time and all instances of 'release-1.0\readme.txt' had the same size and last modified time, then all three would be resolution candidates. In this case, the winner would be arbitrarily selected from the candidate set. This concept applies to all resolution types that are prone to multiple candidate selection.

Once the merge and conflict resolution phases have completed for the session, synchronization transfers begin to distribute the source content. This includes all source copies of conflict winners as well as files that are missing from participants.

See the [File Conflict View](#) for a more detailed explanation on how the file conflict process works and how to remove file conflicts and quarantines.

Configuration

The following is a view of the Conflict Resolution configuration page.



The conflict resolution types that are currently available are listed as follows:

Last Modified Time Wins	<p>A file's modification time will be used to designate an instance as a resolution candidate. The later the modification time, the greater the likelihood for a file's selection.</p> <p>Options: Truncate milliseconds: When comparing the time stamps of a file on two or more hosts, truncate the millisecond value from each time</p>
--------------------------------	--

	stamp.
None (Manual Resolution)	When selected, any file conflicts that are encountered during the initial synchronization process will result in quarantines that are added to the File Conflict List . These file conflicts must be resolved manually by selecting the host with the correct version of the file from the conflict list.

All the types listed above have the potential for producing multiple resolution candidates. A collaboration session can be configured with any one of the available conflict resolvers. If a resolver produces more than one candidate for a conflicted file, a winner will be selected arbitrarily.

Advanced Conflict Resolution options are list as follows:

Quarantine Offline Version Conflicts	Enable this option if you want PeerLink to quarantine a file that was updated in two or more locations while the collaboration session was not running.
Offline Delete Detection During Scan	If this option is enabled and target protection is enabled, and it can be determined that a file or folder has been deleted since the session was stopped, then the file or folder will be deleted from all hosts. If this option is not enabled then the deleted file or folder will be brought back to any host where it was removed.
Delete Detection Master Host (optional)	Only available when Allow Delete Detection During Scan is enabled. If enabled and a Master Host is specified, then if a file or folder was deleted while the job was stopped from a host other than the Master Host, the deleted file or folder will be brought back to any host where it was removed from. However, if a file or folder was deleted from the master host and the file or folder existed on the master host the last time the job was running, then the file or folder will be deleted from all other hosts regardless of the current last modification times.

Once all File Conflict Resolvers are selected and set to your liking, you can either [save the configuration](#) and exit the dialog, or you can continue with the configuration process by going to [Step 5 - Delta Compression](#).

Step 5 - Delta Compression

Delta Compression configuration is available by selecting **Delta Compression** from the tree node within the File Collaboration Configuration dialog.

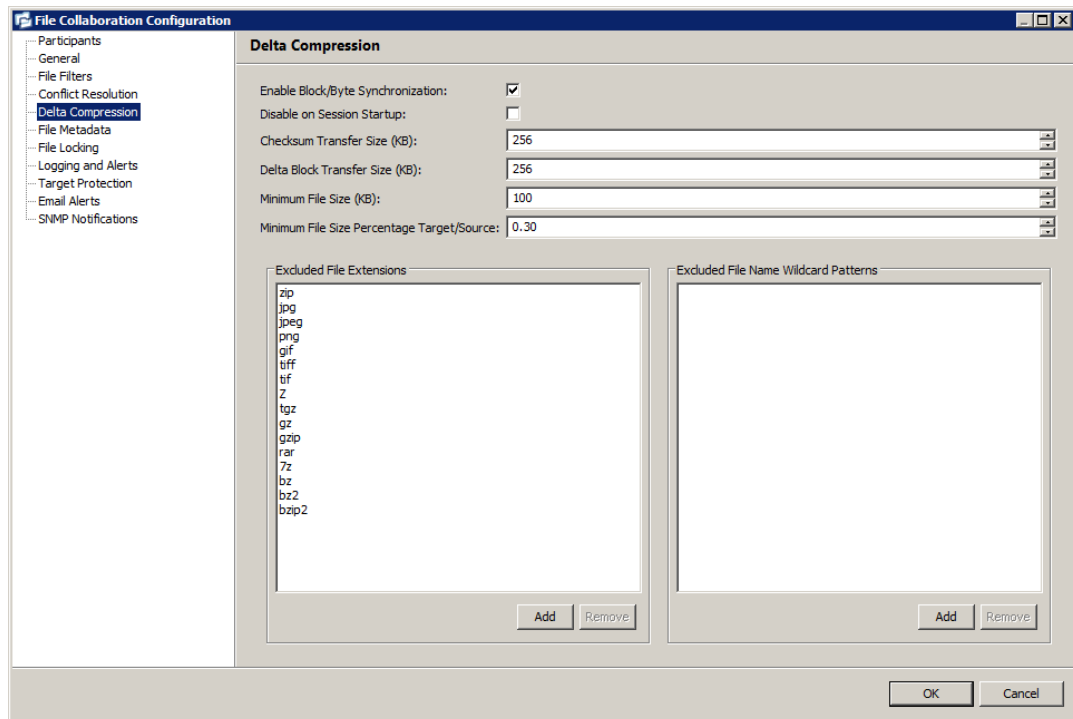
Overview

Delta Compression is a byte replication technology that enables block/byte level synchronization for a file collaboration job. Through the use of this feature, PeerLink will be able to transmit only the bytes/blocks of a file that have changed instead of transferring the entire file. This results in much lower network bandwidth utilization which can be an enormous benefit if you are transferring files across a slow WAN or VPN, as well as across a high volume LAN.

Configuration

Delta Compression is enabled on a per [file collaboration job](#) basis and generally affects all

files in the [Watch Set](#). You will only benefit from delta compression for files that do not change much between file modifications, which includes most document editing programs.



Below is a list of configuration items and their descriptions:

Enable Block/Byte Synchronization	Enables delta encoded file transfers which only sends the file blocks that are different between source and target(s). If this is disabled, the standard file copy method will be used to synchronize files.
Disable on Session Startup	Disables delta compression during file collaboration session startup where the state of all hosts and files is not known. If enabled, delta encoding would need to be performed between source and each target separately since the state of any files is not known.
Checksum Transfer Size (KB)	The block size in kilobytes used to transfer checksums from target to source at one time. Larger sizes will result in faster checksum transfer, but will consume more memory on the Agents.
Delta Block Transfer Size (KB)	The block size in kilobytes used to transfer delta encoded data from target to source at one time. Larger sizes will result in faster overall file transfers, but will consume more memory on the Agents.
Minimum File Size (KB)	Minimum size of files in kilobytes to perform delta encoding for. If a file is less than this size then delta encoding will not be performed.
Minimum File Size Percentage Target/Source	The minimum allowed file size difference between source and target, as a percentage, to perform delta encoding. If the target file size is less than this percentage of the source file size then delta encoding will not be performed.

Excluded File Extensions	List of comma separated wildcard patterns of file extensions to be excluded from delta encoding, e.g. zip,jpg,png. In general, compressed files should be excluded from delta encoding and the most popular compressed file formats are excluded by default.
Excluded File Name Wildcard Patterns	A list of file name wildcard patterns to exclude from delta encoding. If a filename matches any wild card pattern in this list then it will be excluded from delta encoding transfers and a regular file transfer will be performed. See the File Filter wildcard expressions section for more information on specifying wildcard expressions.

Once all Delta Compression settings are set, you can either [save the configuration](#) and exit the dialog, or you can continue with the configuration process by going to [Step 6 - File Metadata](#).

Step 6 - File Metadata

File Metadata configuration is available by selecting **File Metadata** from the tree node within the File Collaboration Configuration dialog.

Overview

File Metadata is additional information stored as part of the file. The main component of File Metadata is Security Descriptor Information, comprised of attributes such as DACLS, SACLs, Owner, Group, ACLs, etc.

By default, enabling real time file metadata synchronization will cause any real-time modifications of metadata to be synchronized with all other target hosts. This alone, however, will not enable synchronizing file metadata during the [initial synchronization process](#). In order to enable file metadata synchronization during the initial synchronization process, you must enable this option and select a MASTER host to use as the conflict winner.

ACL Guidelines and Best Practices

- Enabling ACL synchronization requires that all participating hosts be members of any referenced domains that are configured in the ACL(s) or as the owner of the file. Failure to do so may render the file unreadable on the offending target host.
- All PeerLink Agents must be run under a domain Administrator account and cannot be run under a local or System account.
- In order to ensure accurate and consistent ACL propagation the security settings for the root folder being watched by PeerLink must match EXACTLY across all the participants. The best and easiest way to ensure the security settings match is to compare the permissions in the Advanced Security Settings dialog for the root folder being watched.

More detailed information about [ACL Guidelines](#) can be found at the URL below:

<http://www.peersoftware.com/support/knowledgebase/item/peerlink-acl-guidelines.html>

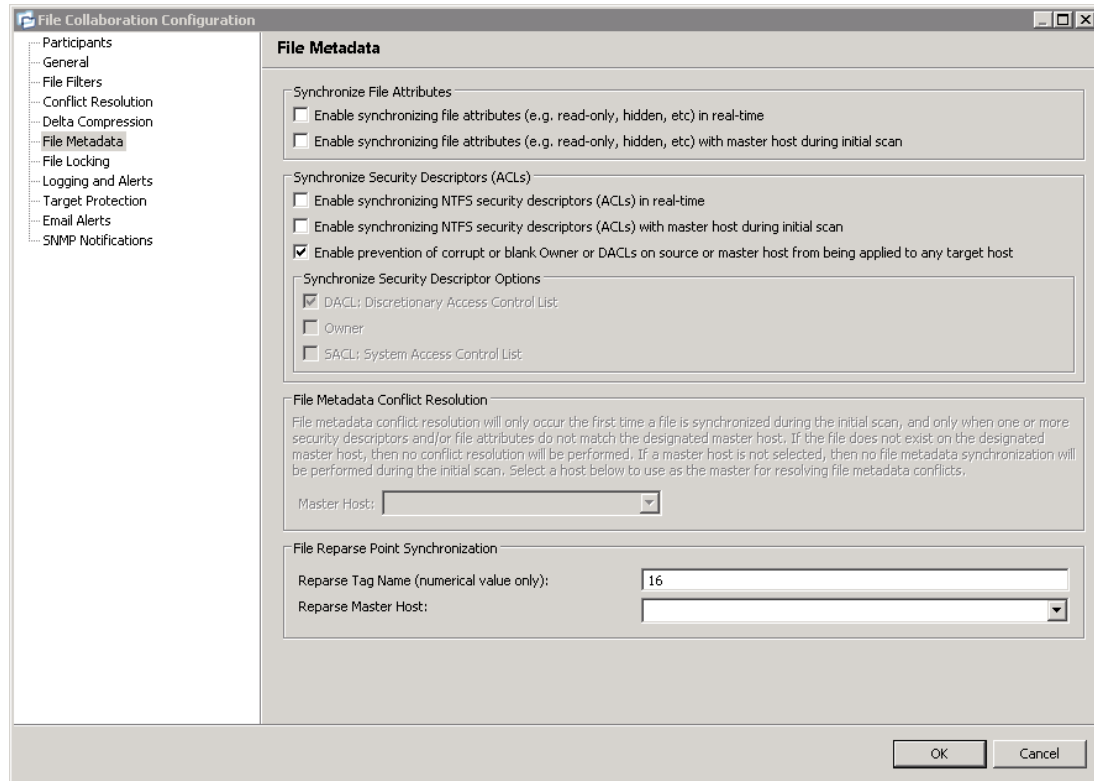
File Metadata Conflict Resolution

File Metadata Conflict Resolution will only occur the first time a file is synchronized during the initial scan, and only when one or more security descriptors do not match the designated master host. If the file does not exist on the designated master host, then no conflict resolu-

tion will be performed. If a master host is not selected, then no file metadata synchronization will be performed during the initial scan.

Configuration

The following screen presents available File Metadata configuration options:



Below is a list of file metadata options along with their descriptions:

Enable synchronizing NTFS security descriptors (ACLs) in real-time	If enabled, changes to the configured security descriptor component (e.g. DACL, SACL, Owner, etc.) will be transferred to the target host file(s) as they occur.
Enable synchronizing NTFS security descriptors (ACLs) during initial scan	If enabled, changes to the configured security descriptor component (e.g. DACL, SACL, Owner, etc.) will be synchronized during the initial scan (if a Master Host is selected).
Enable prevention of	If enabled, then corrupt or blank Owner or DACLs on source or master host will not be applied on any target host file.

corrupt or blank Owner or DACLS	
Synchronize Security Descriptor Options	You can select which security descriptor components are synchronized. Choices are DACL, SACL and Owner. In general, you will usually only need to synchronize DACLS. If you need to synchronize SACLs or Owner, then the user that a PeerLink Agent service is run under on each participating host must have permission to read and write SACLs and Owner.
Master Host	The master host to use for conflict resolution during the initial synchronization process.

File Reparse Point Data Synchronization

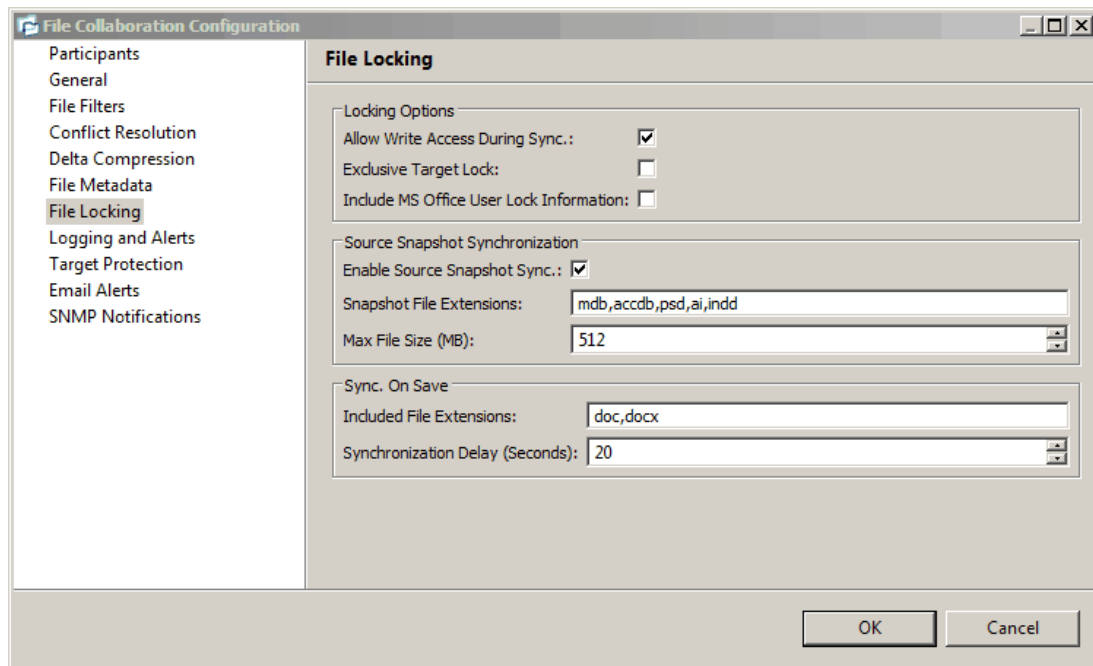
This option should only be used if you are utilizing archiving or hierarchical storage solutions that make use of NTFS file reparse points to access data in a remote location, such as, Symantec's Enterprise Vault. Enabling this option will allow synchronizing a file's reparse data, and not the actual offline content, to target hosts, and will prevent the offline file from being recalled from the remote storage device.

Reparse Tag Name	A single numerical value. Must be either empty (reparse synchronization will be disabled), or greater than/equal to 0. The default for Symantec Enterprise Vault is '16'. A value of 0 will enable reparse point synchronization for all reparse file types. If you are unsure as to what value to use, then either contact our technical support, or you can use a value of 0 if you are sure that you are only utilizing one vendor's reparse point functionality.
Reparse Master Host	If a master host is selected then when the last modified times and file sizes match on all hosts, but the file reparse attribute differs (e.g. archived/offline verse unarchvied on file server), then the file reparse data will be synchronized to match the file located on the master host. For Enterprise Vault, this should be the server where you run the archiving task on. If the value is left blank, then no reparse data synchronization will be performed, and the files will be left in their current state.

Once all File Metadata settings are set, you can either [save the configuration](#) and exit the dialog, or you can continue with the configuration process by going to [Step 7 - Logging & Alerts](#).

Step 7 - File Locking

The File Locking settings page contains miscellaneous configuration items pertaining to a how source and target files are locked by PeerLink, and is available by selecting **File Locking** from the tree node within the File Collaboration Configuration dialog.



Below are a list of general fields and their descriptions:

Allow Write Access During Sync.	If enabled, users will be allowed write access to source files that are currently being synchronized. If not checked, then users will be denied write access to source files during synchronization, but will be able to open them in read-only mode.
Exclusive Target Lock	If enabled, then whenever possible, an exclusive lock will be obtained on target file handles, which will prevent users from opening the file (even in read-only mode) while a user has the file opened on the source host. When this option is disabled, then users will be allowed to open files for read-only if the application allows for this.
Include MS Office User Lock Information	If enabled, user lock information (if available) will be propagated to target locks for supported Microsoft Office files (e.g. Word, Excel & PowerPoint).
Enable Source Snapshot Sync.	If enabled, a snapshot copy of the source file will be created for files that meet the snapshot configuration criteria below, and this copy will be used for synchronization purposes. In addition, no file handle will be held on the source file except while making a copy of the file.
Snapshot File Extensions	A comma separated list of file extensions for which source snapshot synchronization will be utilized.
Max File Size (MB)	The maximum file size for which source snapshot synchronization will be utilized.
Sync. On Save: Included File Extensions	A comma separated list of file extensions for which to enable the Sync. On Save feature. Enabling this feature will allow supported files types to be synchronized after a user saves a file, rather than waiting for file to close.

Sync. On Save: Synchronization Delay	The number of seconds to wait after a file has been saved before initiating a synchronization of the file.
---	--

Step 8 - Logging and Alerts

File Event Logging

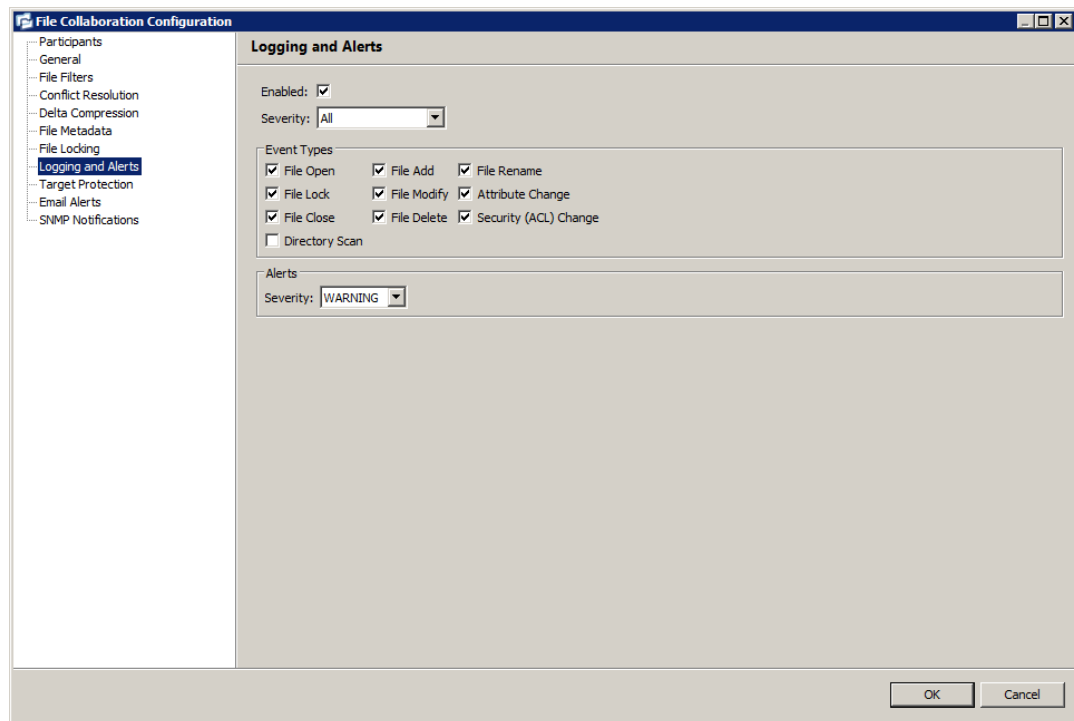
Various types of file collaboration events can be written to a log file and to the [Event Log](#) tab located within the [File Collaboration Runtime View](#) for the selected [file collaboration job](#). Each job will log to the **fc_event.log** file located in the 'Hub\logs' subdirectory within the [PeerLink Hub](#) installation directory. All log files are stored in a tab delimited format that can easily be read by Microsoft Excel or other Database applications.

Log Entry Severity Levels

Informational	Informational log entry, e.g. File was opened.
Warning	Some sort of warning occurred that did not produce an error, but was unexpected or may need further investigation.
Error	An error occurred performing some type of file activity.
Fatal	A fatal error occurred that caused a host to be taken out of the session, a file to be quarantined, or a session to become invalid.

Configuration

By default, all file collaboration activity is logged for all severity levels. You can enable or disable file event logging as well as select the level of granularity on what to log through the **Logging and Alerts** page, available by selecting **Logging and Alerts** from the tree node within the File Collaboration Configuration dialog.



Below is a list of logging fields and their descriptions:

Enabled	Checking this option will enable file event logging based on the other settings. Un-checking this option will completely disable all logging.
Severity	Determines what severity levels will be logged. There are two options: <ul style="list-style-type: none"> • All (Informational, Warnings, Error, Fatal) • Errors and Warnings (Warnings, Error, Fatal)
Event Types	If checked, the corresponding event type will be logged.
File Open	A file was opened by a remote application on a Source Host .
File Lock	A file lock was acquired on a Target Host by the file collaboration job.
File Close	A file was closed.
File Add	A file was added to the Watch Set .
File Modify	A file was modified in the Watch Set.
File Delete	A file was deleted.
File Re-name	A file was renamed.
Attribute	A file attribute was changed.

Change	
Security (ACL) Change	The security descriptor of a file or folder was changed.
Directory Scan	Indicates when a directory was scanned as a result of the initial synchronization process .

Alerts

Configured in the screen shown above, various types of alerts will be logged to a log file and to the [Alerts](#) table located within the [File Collaboration Runtime View](#) for the selected job. Each file collaboration job will log to the **fc_alert.log** file located in the 'Hub\logs' subdirectory within the [PeerLink Hub](#) installation directory. All log files are stored in a tab delimited format that can easily be read by Microsoft Excel or other database applications.

The default log level is WARNING which will show any warning or error alerts that occur during a running session. Depending on the severity of the alert, the session may need to be restarted.

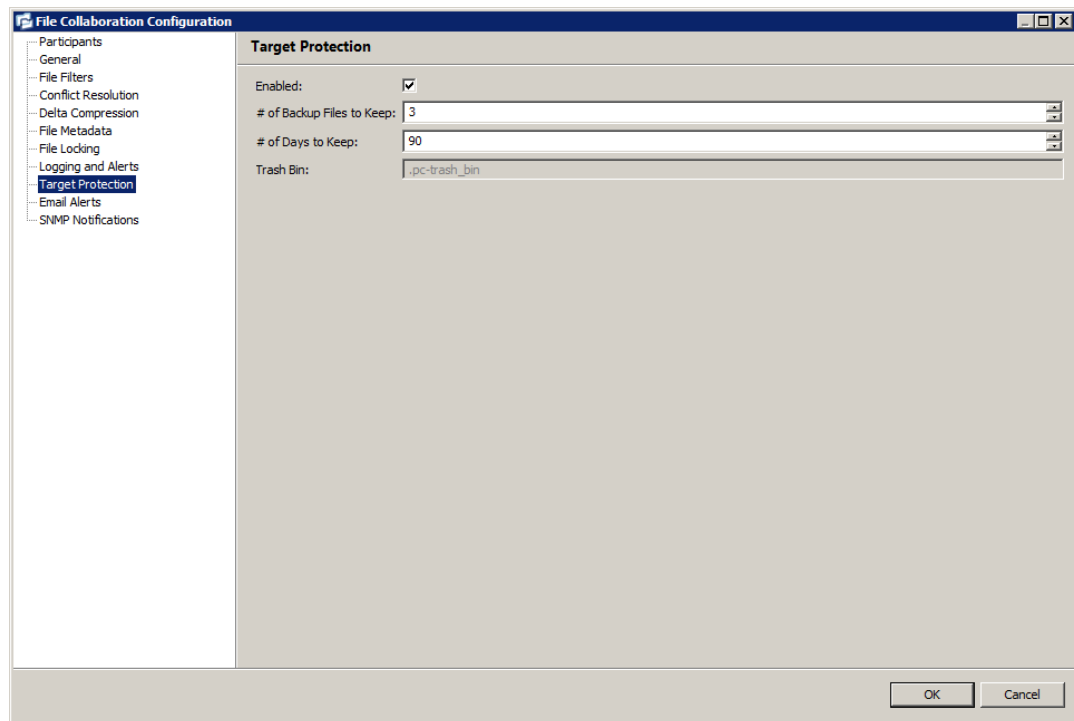
Once all Logging and Alerts settings are set, you can either [save the configuration](#) and exit the dialog, or you can continue with the configuration process by going to [Step 8 - Target Protection](#).

Step 9 - Target Protection

Target Protection is used to protect files on [target hosts](#) by saving a backup copy before a file is either deleted or overwritten on the target host. If enabled, then whenever a file is deleted or modified on the source host, but before the changes are propagated to the targets, a copy of the existing file on the target is moved to the PeerLink trash bin.

The trash bin is located in a hidden folder named **.pc-trash_bin** found in the root directory of the [Watch Set](#) of the target host. A backup file is placed in the same directory hierarchy location as the source folder in the Watch Set within the recycle bin folder. If you need to restore a previous version of a file then you can copy the file from the recycle bin into the corresponding location in the Watch Set and the changes will be propagated to all other collaboration hosts.

Target Protection configuration is available by selecting **Target Protection** from the tree node within the File Collaboration Configuration dialog.



Below are a list of general fields and their descriptions:

Enabled	Enables target protection.
# of Backup Files to Keep	The maximum number of backup copies of an individual file to keep in the trash bin before purging the oldest copy.
# of Days to Keep	The number of days to keep a backup archive copy around before deleting from disk. A value of 0 will disable purging any files from archive.
Trash Bin	The trash bin folder name located in the root directory of the Watch Set. This is a hidden folder and the name cannot be changed by the end-user.

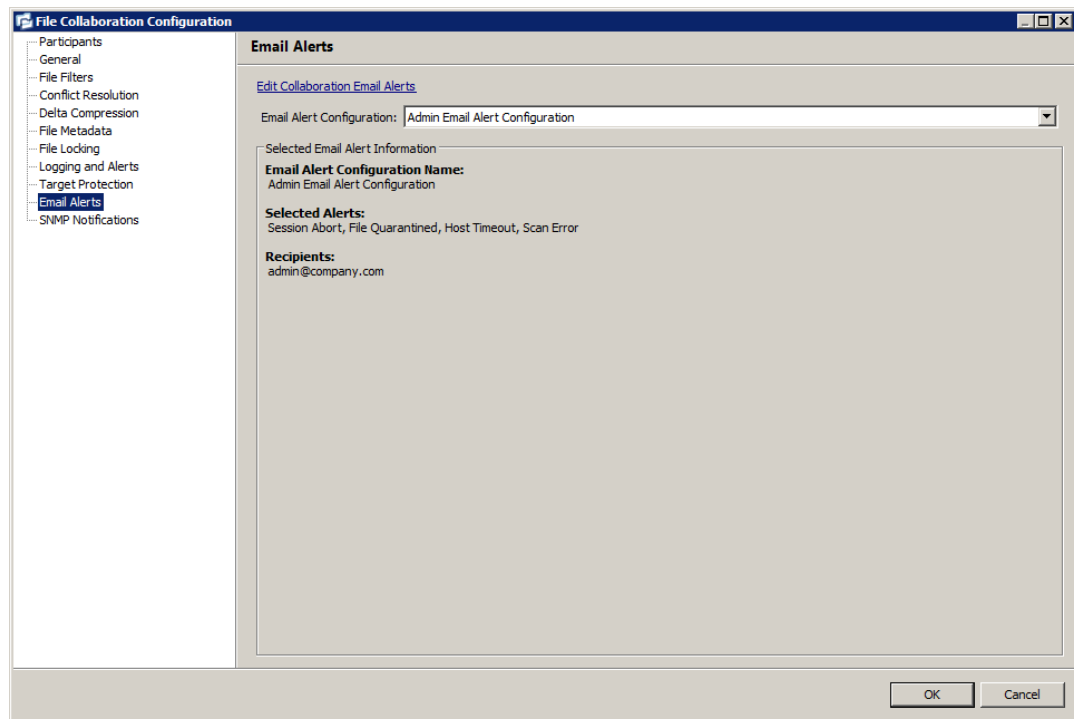
Once all Target Protection settings are set, you can either [save the configuration](#) and exit the dialog, or you can continue with the configuration process by going to [Step 9 - Email and SNMP Alerts](#).

Step 10 - Email Alerts and SNMP Notifications

Email Alerts

Email Alerts configuration is available by selecting **Email Alerts** from the tree node within the File Collaboration Configuration dialog.

Email Alerts are configured at a global level, then applied to individual [file collaboration jobs](#). The following screen shows how this is accomplished.

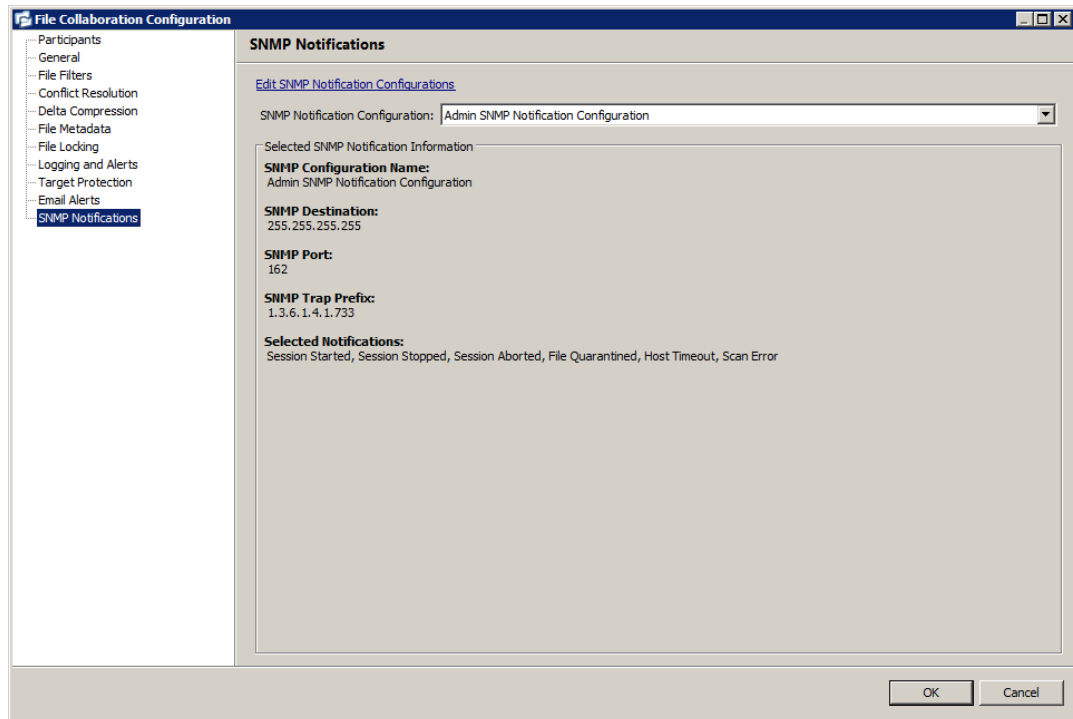


To enable Email Alerts for this particular job, select an Email Alert Configuration from the drop down list. To disable, select **None - Disabled**. To edit the list of available configurations, select [Edit Collaboration Email Alerts](#).

SNMP Notifications

SNMP Notification configuration is available by selecting **SNMP Notifications** from the tree node within the File Collaboration Configuration dialog.

SNMP Notifications, like Email Alerts, are also configured at a global level, then applied to individual jobs. The following screen shows how this is accomplished:



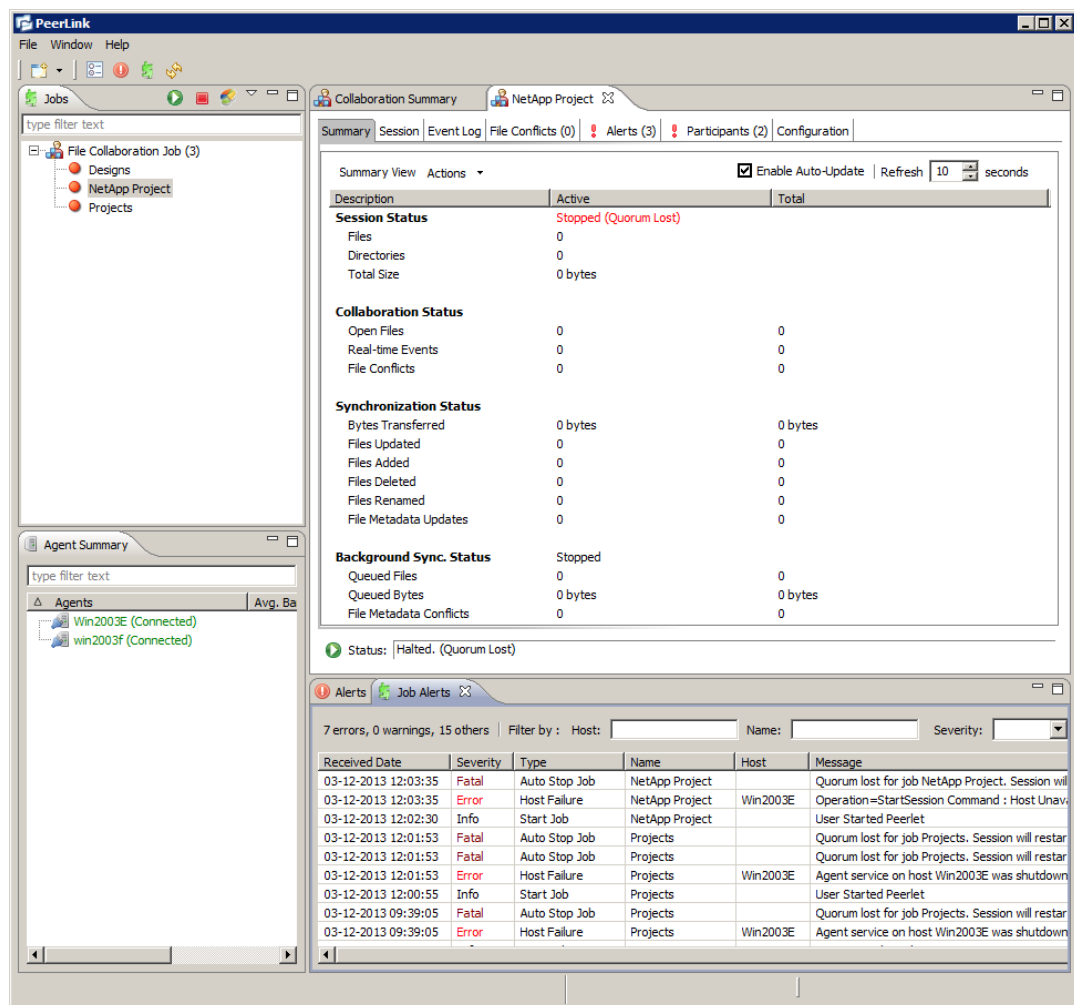
To enable SNMP Notifications for this particular job, select an SNMP Notification Configuration from the drop down list. To disable, select **None - Disabled**. To edit the list of available configurations, select [Edit SNMP Notification Configurations](#).

Once all Email Alert and SNMP Notification settings are set, you have completed the configuration process and can now [save the configuration](#).

Step 11 - Save Settings

Once you have finished configuring the [file collaboration job](#), you will need to save the changes by pressing the **OK** button at the bottom of the configuration window.

After saving the configuration, the job will be displayed in the [Job View](#) in the top left panel of the [PeerLink Hub](#). You will also be able to open the job in a tab of the [File Collaboration Runtime View](#) as shown below:



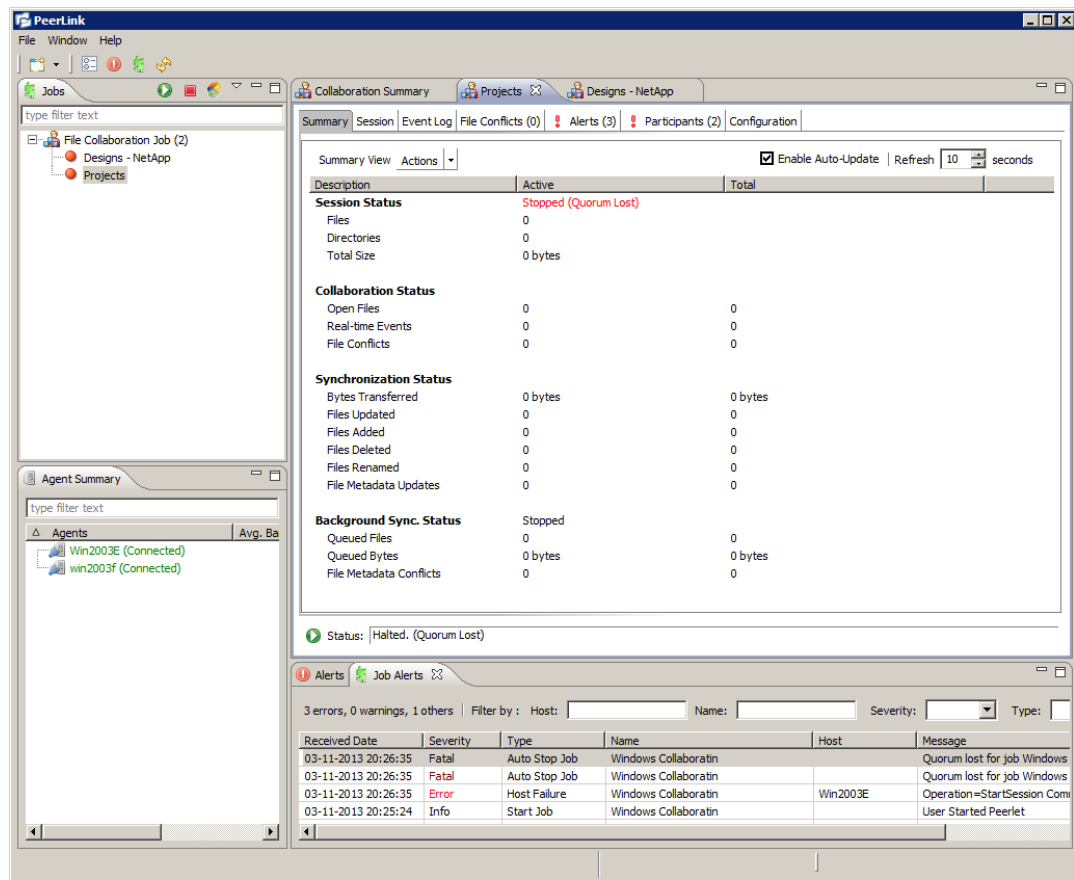
You are now ready to start the job. See [Running and Managing a File Collaboration Job](#) for more information.

Running and Managing a File Collaboration Job

The topics in this section provide some basic information about starting, stopping and managing File Collaboration Jobs.

Overview

[File Collaboration Jobs](#) are manually started and stopped in three ways: by right-clicking on one or more jobs in the [Jobs View](#), by right-clicking on one or more jobs in the [Collaboration Summary View](#), or by opening a specific job and pressing the Start/Stop button at the bottom of the job's tab (shown below).



The File Collaboration Runtime View is located in the large center section of the PeerLink Hub. It is comprised of various tabs (or editors) representing individual file collaboration jobs and/or cross-job [summary information](#). The tabs representing individual jobs consist of the following components:

Runtime View Sub Tabs	<p>These tabs allow you to select from the various job-specific views. These views include:</p> <ul style="list-style-type: none"> • Summary (or Status) View - Shows overall statistics for the file collaboration job. The illustration above is displaying the Summary View. • Session View - Shows active open files and files that are currently in transit between participating hosts. • Event Log View - Shows a list of all runtime activity that has occurred within the selected file collaboration job. • File Conflicts View - Shows a list of all files that are quarantined for the session or are in conflict between two or more participating hosts. • Alerts View - Shows a list of all Job Alerts specifically tied to the selected job. • Participants View - Shows a list of all hosts participating in the file collaboration job. • Configuration View - Shows a summary of all configurable options for the selected job.
Job Start /	<p>The button allows you to start and stop the File Collaboration file collaboration job.</p>

Stop	
Job Status Display	Displays status related messages when the job is running.

Starting and Stopping

Starting a File Collaboration Job

Before you start a [file collaboration job](#) for the first time, you need to decide how you would like the initial synchronization to be performed. There are two main options:

1. Have the file collaboration job perform the initial synchronization based on the configured [File Conflict Resolver](#) strategy.
2. Pre-seed all [participating hosts](#) with the correct folder and file hierarchy for the configured Root Folders before starting the session.

If you have a large data set, we strongly recommend that you perform the initial synchronization manually by copying the data from a host with the most current copy to all other participating hosts. This will only need to be done the first time that you run the file collaboration job.

If you choose Option 1, simply press the **Start** button to begin collaboration session initialization. Otherwise, pre-seed each participating host with the necessary data, then press the **Start** button.

Initialization Process

The initialization process consists of the following steps:

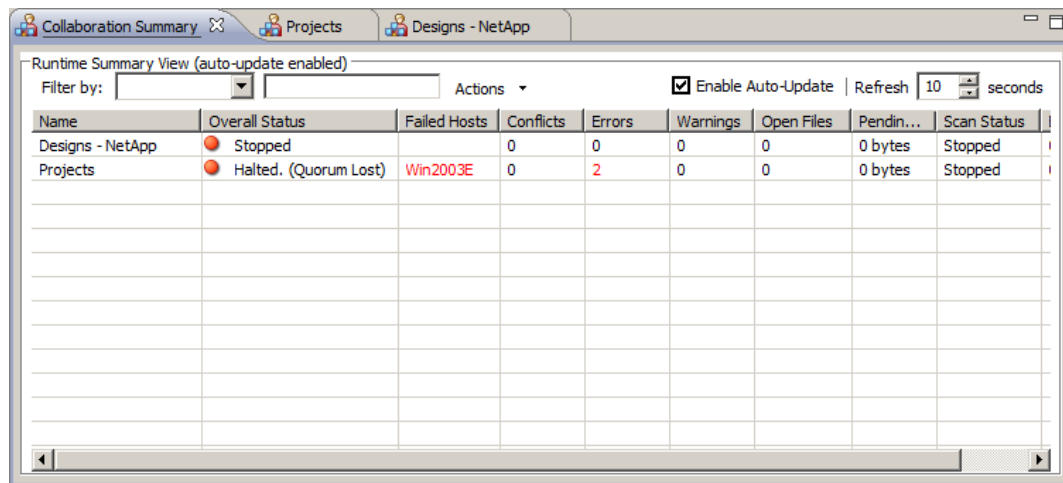
1. All participating hosts are contacted to make sure they are online and properly configured.
2. Realtime event detection is initialized on all participating hosts where file locks and changes will be propagated in real-time to all participating hosts. You can view real-time activity and history via the various [Runtime Views](#) for the open job.
3. The [initial synchronization process](#) is started, all of the configured Root Folders on the participating hosts are scanned in the background, and a listing of all folders and files are sent back to the running job.
4. The background directory scan results are analyzed and directory structures compared to see which files are missing from which hosts. In addition, file conflict resolution is performed to decide which copy to use as the master for any detected file conflicts based on the configured [File Conflict Resolver](#) settings.
5. After the analysis is performed, all files that need to be synchronized are copied to the pertinent host(s).

Stopping a File Collaboration Job

You can stop a file collaboration job at any time by pressing the **Stop** button. Doing this will shutdown the real-time file event detection and close all running operations (eg. file transfers, etc.).

Collaboration Summary View

The Collaboration Summary View is a view that aggregates critical status and statistical information from all configured [File Collaboration Jobs](#) in a single table view. It is automatically displayed when the [PeerLink Hub](#) client is started and can be opened at any other time by double-clicking on the **File Collaboration** parent tree node in the [Jobs View](#) or by clicking on the **View Runtime Summary** icon in the toolbar of the Jobs View. Information in this view can be sorted and filtered. Operations such as starting, stopping, and editing multiple job at once are available, in addition to the ability to clear [Job Alerts](#) and purge [file conflicts](#) from stopped jobs.



Unlike other views within the PeerLink Hub, the Collaboration Summary View is not updated in real-time. This is done for performance reasons. Instead, the table can be set to automatically update itself every few seconds. Checking **Enable Auto-Update** will enable this functionality, while the refresh interval (in seconds) can be set right beside the checkbox. Additional columns can be added to and removed from the table from the right-click context menu.

Double-clicking on any item in the table will automatically open the selected File Collaboration Job in a tab within the [File Collaboration Runtime View](#), allowing you to drill down and view specific information about that single job. Items in the summary table can be filtered by job name, running status, and [host participant](#) name.

Selecting one or more items in the table, then right-clicking will bring up a context menu of available actions that can be performed on the selected jobs. The actions that are unique to this table are as follows:

Purge All Conflicts	Purges all file conflicts from the selected jobs. This can only be performed on jobs that are not running.
Clear Alerts	Clears all alerts for the selected jobs. This can be performed while a job is running.

Clicking on the **Actions** table menu provides the following options:

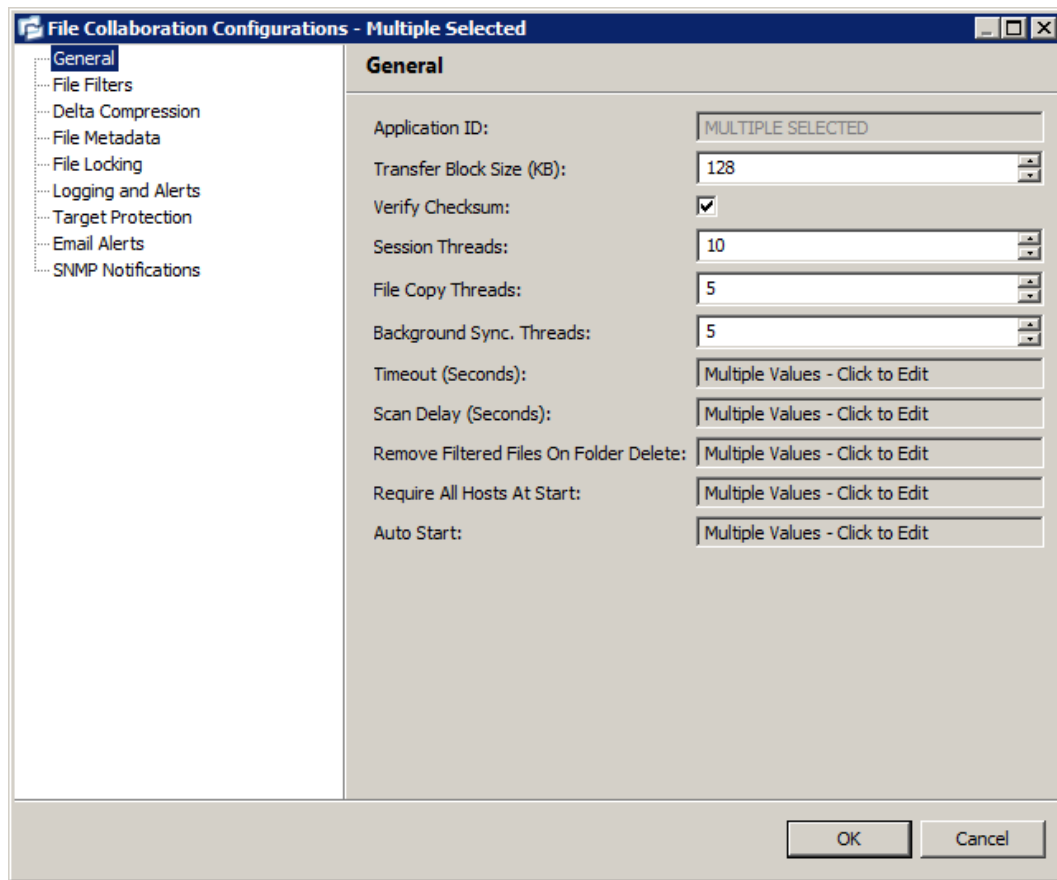
Refresh	Refresh all information provided in the table.
----------------	--

View	
Copy All Filtered Statistics	Copy detailed information to the system clipboard for all items current displayed in the table, taking any filters into account. This information can then be pasted into a document editor.
Export Entire Table to File	Dump the entire contents of the table to a text file that can be viewed in any document editor.

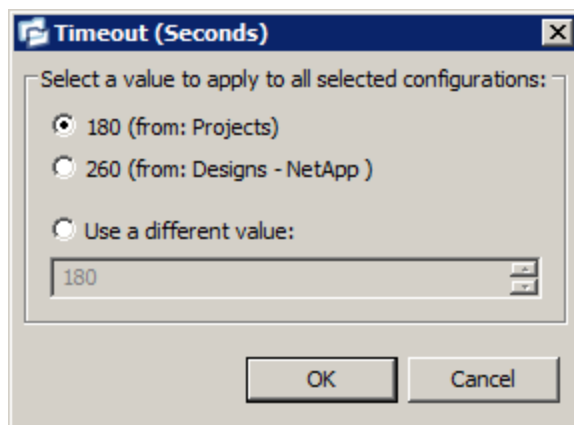
Multi-Job Edit Support

The [PeerLink Hub](#) supports Multi-Job Editing, allowing you to quickly and effectively manipulate multiple [File Collaboration Jobs](#) at once. For example, you can use this feature to change a single configuration item such as **Auto Start** for any number of already configured jobs in one operation instead of having to change the item individually on each. While this feature does cover most of the options available on a per-job basis, certain options are unavailable in multi-job edit mode, specifically ones tied to [participants](#). Please see the section on [Creating a File Collaboration Job](#) for more details on specific configuration items.

For the most part, the original configuration dialog remains the same with a few minor differences depending on similarities between the selected file collaboration jobs. A sample dialog is as follows:



In this dialog, any discrepancies between multiple selected file collaboration jobs will generally be illustrated by a read-only text field with the caption, "Multiple Values - Click to Edit". Clicking on this field will bring up a dialog similar to the following:



This dialog gives you the option of choosing a value that is already used by one or more selected file collaboration jobs, in addition to the ability to use your own value. Please note that variances in the look and feel of this popup dialog above depend on the type of information it is trying to represent (for example, text vs. a checkbox vs. a list of items).

Upon pressing **OK**, the read-only text field you originally clicked on will be updated to reflect the new value. Any fields that have changed will be marked by a small caution sign. On saving this multi-job edit dialog, the changed values will be applied to all selected jobs.

PLEASE NOTE: Read all information on each configuration page carefully when using the multi-job edit dialog. A few screens operate in a slightly different manner than mentioned above. All of the necessary information is provided at the top of these screens in **bold** writing.

Host Connectivity Issues

Unavailable Hosts

PeerLink is designed to be run in an environment where all [participating hosts](#) are highly available and on highly available networks.

If a host becomes unavailable while a File Collaboration Job is running, and is unreachable within the configured timeout period (specified within the job's [General Settings](#)), it may be removed from collaboration. If no response is received while performing a file collaboration operation within the timeout period then the host will be pinged, and if still no response, the host will be taken out of the running session, a FATAL event will be logged, and the [Participants View](#) for the job will be updated to indicate that the host has failed. In addition, if [Email Alerts](#) and/or [SNMP Notifications](#) are configured and enabled for **Host Timeouts**, then the appropriate message(s) will be sent.

If auto-restart support (see below) is not enabled, you will need to Stop and Start the file collaboration job in order to bring any failed hosts back into the session. As a result, all Root Folders on all hosts will need to be scanned again to detect any inconsistencies. Therefore, if you are operating over a WAN with low bandwidth you will want to set the timeout to a higher value on each related job.

Quorum

In order for a File Collaboration Job to run correctly, a quorum of available hosts must be met. Quorum is currently set to at least 2 hosts, and if quorum is not met then the collaboration session will automatically be terminated. If [Email Alerts](#) and/or [SNMP Notifications](#) are configured and enabled for **Session Aborts**, then the appropriate message(s) will be sent.

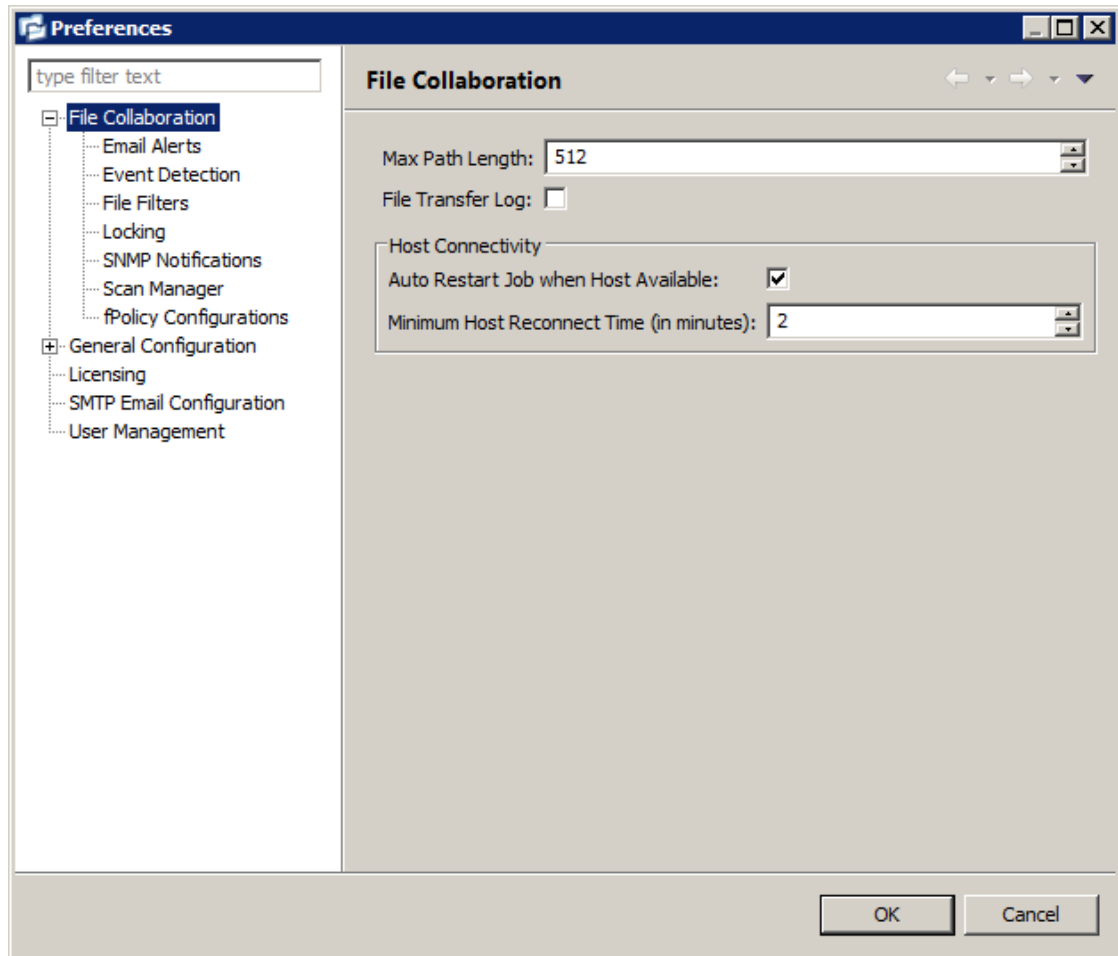
Auto-Restart

PeerLink includes support for automatically restarting file collaboration jobs that include [participating hosts](#) that have been disconnected, and have reconnected and are once again available. After a host becomes unavailable and quorum is lost on a running file collaboration job, the job will automatically stop running and enter a pending state, waiting for one or more hosts to become available again so that quorum can be met. Once quorum is met, the pending job will automatically be restarted, beginning with a scan of all Root Folders. In a job where a host becomes unavailable but quorum is not lost, the remaining hosts will continue collaborating. If the unavailable host becomes available once again, it will be brought back into the running job and a background scan will begin on all participating hosts, similar in fashion to the initial background scan at the start of a job.

Configuration

This functionality is enabled on a global level for all file collaboration jobs and is configured by

clicking on the **Window** menu within the [PeerLink Hub](#), then selecting **Preferences**. Within the opening dialog, select **File Collaboration** in the tree on the left. The following screen will be displayed:



Host Connectivity options are as follows:

Auto Restart Job when Host Available	If checked, auto-restart functionality will be enabled for all running file collaboration jobs.
Minimum Host Reconnect Time (in minutes)	The minimum time in minutes a host must be reconnected before reestablishing the host within any relevant file collaboration jobs.

Disabling auto-restart on a per-job and host instance is performed within the Participant View for the desired file collaboration job. For more information on managing and disabling auto-restart at the job level, please see the section on the [Participant View](#).

Runtime Job Views

Each file collaboration job has seven primary Runtime Views used for viewing a combination of real-time file I/O activity, history, and configuration. These views also provide the ability to manage specific collaboration runtime functionality.

The seven views are as follows:

- [Summary View](#)
- [Session View](#)
- [Event Log View](#)
- [File Conflicts](#)
- [Alerts View](#)
- [Participants View](#)
- [Configuration](#)

1. Summary View

The Summary View allows you to view current and cumulative file collaboration and synchronization statistics, as well background synchronization status.

Summary Session Event Log File Conflicts (0) Alerts (0) Participants (2) Configuration		
Summary View	Actions ▾	<input checked="" type="checkbox"/> Enable Auto-Update Refresh 10 seconds
Description	Active	Total
Session Status	Collaborating	Started: 3/12/13 8:24 AM
Files	76	
Directories	39	
Total Size	19.3 MB	
Collaboration Status		
Open Files	0	0
Real-time Events	0	0
File Conflicts	0	0
Synchronization Status		
Bytes Transferred	636.9 KB	17.8 MB
Files Updated	5	74
Files Added	0	0
Files Deleted	0	0
Files Renamed	0	0
File Metadata Updates	0	0
Background Sync. Status	Scanning Directories	\\FLDR3\FLDR3L1\FLDR1L2
Queued Files	6	75
Queued Bytes	2.1 MB	19.3 MB
File Metadata Conflicts	0	0

The Session Summary View is made up of the following sections:

Session Status

This section displays current statistics for all files/folders contained in the running [file collaboration job](#).

Files	Current number of files in the running file collaboration job. Files that are excluded by filtration will not be included in this statistic.
Directories	Current number of subfolders under the Watch Sets of the running

	file collaboration job.
Total Size	Cumulative number of bytes of all files in the running file collaboration job.
Start Time	The date and time of the last start of the file collaboration job, manual or automatic.

Collaboration Status

Open Files (Active)	Displays the number of files that are currently being collaborated on, where a user has a file open on the source host and the system is holding locks on all target hosts.
Open Files (Total)	Displays the total number of files that have been opened since the session was started, where locks were propagated to target hosts.
Real-Time Events (Active)	Displays the current number of real-time file events that are pending action.
Real-Time Events (Total)	Displays the total number of realtime event received since the running file collaboration job was started.
File Conflicts (Active)	Displays the current number of files that are in some type of conflicted state.
File Conflicts (Total)	Displays the total number of file conflicts (including pending initial synchronization) that have occurred since the running file collaboration job was started.

Synchronization Status

This section displays current and cumulative statistics for all files that have been added, removed, renamed or modified since the running file collaboration job was started.

Bytes Transferred (Active)	Total number of bytes currently being transferred to target hosts by the running file collaboration job.
Bytes Transferred (Total)	<p>Total number of bytes that have be transferred to target hosts since the file collaboration job was started. If delta compression is enabled then the total delta encoding savings will also be displayed as percentage along with the actual cumulative size of the source files.</p> <p>For example a value of 3.9MB --> Delta Savings 47.75% (7.6MB) should be interrupted as a total of 3.9MB were transferred corresponding to the actual total source size of 7.6MB for a savings of 47.75% or 3.7MB.</p> <p>Keep in mind that the delta savings also averages in files where delta encoding may not have been used.</p>
Files Updated (Active)	Total number of files currently being updated or that are scheduled to be updated.
Files Updated (Total)	Total number of files that have been modified since the file collaboration job was started.

Files Added (Active)	Total number of files currently being added to the session or that are scheduled to be added.
Files Added (Total)	Total number of files that have been added since the file collaboration job was started.
Files Deleted (Active)	Total number of files currently being deleted or that are scheduled to be deleted.
Files Deleted (Total)	Total number of files that have been deleted since the file collaboration job was started.
Files Renamed (Active)	Total number of files currently being renamed or that are scheduled to be renamed.
Files Renamed (Total)	Total number of files that have been renamed since the file collaboration job was started.
File Metadata Updates (Active)	Total number of files pending file metadata (file attributes and security descriptor) updates.
File Metadata Updates (Total)	Total number of file metadata (file attributes and security descriptor) changes that have occurred since the file collaboration job was started.

Background Synchronization Status

This section displays overall status of the [initial synchronization process](#) performed at the start of the session, as well as current and cumulative statistics for files that needed to be synchronized.

Background Sync. Statusd	<p>Text label indicating the current status of the initial synchronization process. Valid values are:</p> <ul style="list-style-type: none"> • Stopped: Session is stopped. • Completed: Initial scan and synchronization processes have completed. • Synchronizing Files: Background scan and initial synchronization processes are currently running. • When the status is Synchronizing Files, the Total column will display the directory that is currently being synchronized.
Queued Files (Active)	Total number of files currently being synchronized or that are scheduled to be synchronized.
Queued Files (Total)	Total number of files that have been synchronized by the session as a result of the initial synchronization process.
Queued Bytes (Active)	Total number of bytes currently being synchronized or that are scheduled to be synchronized by the initial synchronization process.
Queued Bytes (Total)	Total number of bytes that have been synchronized by the session as a result of the initial synchronization process.
File Metadata Conflicts (Active)	Total number of file metadata conflicts that are currently being acted on as a result of the initial synchronization process.

ive)	
File Metadata Conflicts (Total)	Total number of file metadata conflicts that were found as a result of the initial synchronization process.

2. Session View

The Session View allows you to view real-time file collaboration activity and the current session status. You can see which files are currently open in the running session, as well as any file that is currently being synchronized between hosts.

The screenshot displays the 'Session View' window. At the top, there are tabs: Summary, Session (selected), Event Log, File Conflicts (0), Alerts (0), Participants (2), and Configuration. Below the tabs, the 'Session Status' is 'Collaborating'. There are filters for 'Filter by Host' and 'Filter by', both with dropdown menus. An 'Actions' dropdown and a checked 'Enable Auto Sync' checkbox are also present. The main area is titled 'Open Files (1)' and contains a table with the following data:

File Path	Host	Is Source	User Name	Sync. Status	File Size	Last Modified	Date
Project Notes.docx	win2003f	true	MONIKAC		12.0 KB	03-11-2013 21:42:49	03-12
Project Notes.docx	Win2003E	false	Session		12.0 KB	03-11-2013 21:42:49	03-12

The **Session View** is made up of the following components:

Session Status	<p>Text label indicating the current status of the session. Valid values are:</p> <ul style="list-style-type: none"> • Stopped: Session is stopped. • Starting: Session is starting up. • Collaborating: Real-time event detection is enabled and session is collaborating. • Stopping: Session is in the process of stopping.
Open Files Table	<p>A table showing all currently open files on the source host, any internal file locks being held by the running file collaboration job on the target host(s), and file summary information. This table will also show all file transfers currently in progress along with file summary information, status and overall progress. Clicking on any column headers will sort by that column in ascending or descending order.</p>

	All items listed in this table are grouped by file path. Each associated lock and/or transfer for each participating host will be available as a hidden child item of a root row. The root row represents the file on the source host . Pressing the + next to the root will show all associated file transfers and/or locks.
Host Filter	A drop down list of participating hosts to filter on. Selecting a specific host will filter the Open Files to just show files on that host.
Filter By Combo	A drop down list of additional filters that can be applied to the Open Files table. including filtering by user name (associated with the opening, adding, deleting, or modification of a file), and by file name.
Actions Menu	<p>Menu items include:</p> <ul style="list-style-type: none"> • Refresh View: Refresh the entire Open Files table to show the latest list of file transfers and locks. • Validate Session Locks: Clicking this link will perform validation of all locks in the session and will report any potential issues. You should perform this action if you believe a file is not open in the session, but the user interface indicates that the file is open, or vice-versa. • File System Report: Generate a text file listing all files and folders being collaborating on within the running file collaboration job.

3. Event Log View

The Event Log View allows you to view recent file event history for the currently running [file collaboration job](#) based on your [Logging and Alerts](#) settings. You can specify the maximum number of events to store in the table by adjusting the Display Events spinner located in the top right corner of the panel. The maximum number of events that can be viewed is 3,000. If you need to view more events or events from a prior session, then you can use the log files saved in the 'Hub\logs' directory located in the installation directory. The event log files will start with **fc_event.log** and are written in a tab delimited format. Microsoft Excel is a good tool to use to view and analyze a log file. See the [Logging and Alerts](#) settings for more information about log files.

You can click on any column header to sort by the column. For example, clicking on the File column will sort by filename and you will be able to view all file events for that file in chronological order. Warnings are highlighted in light gray, Errors are highlighted in red and Fatal errors are highlighted in orange. Error records will also contain an error message in the Message column.

Summary	Session	Event Log	File Conflicts (0)	Alerts (0)	Participants (2)	Configuration
Event Log (real-time updates disabled)						
0 errors, 0 warnings, 510 others			Filter by Severity:		Filter by:	
			Actions		En	
Date	Severity	Type	Host	Is Source	File	Comments
03-12-2013 09:13:28	INFO	File Delete	Win2003E	false	Project Notes - old.docx	
03-12-2013 09:13:28	INFO	File Delete	win2003f	true	Project Notes - old.docx	
03-12-2013 09:05:36	INFO	File Rename	Win2003E	false	Project Notes.docx	New FileName:
03-12-2013 09:05:36	INFO	File Rename	win2003f	true	Project Notes.docx	New FileName:
03-12-2013 08:57:26	INFO	File Close	win2003f	true	Project Notes.docx	
03-12-2013 08:57:26	INFO	File Close	Win2003E	false	Project Notes.docx	
03-12-2013 08:57:26	INFO	File Modify	Win2003E	false	Project Notes.docx	
03-12-2013 08:57:26	INFO	File Lock	win2003f	true	Project Notes.docx	
03-12-2013 08:57:26	INFO	File Modify	win2003f	true	Project Notes.docx	
03-12-2013 08:57:25	INFO	File Close	win2003f	true	Project Notes.docx	
03-12-2013 08:56:22	INFO	File Lock	Win2003E	false	Project Notes.docx	
03-12-2013 08:56:22	INFO	File Open	win2003f	true	Project Notes.docx	
03-12-2013 08:31:24	INFO	File Close	win2003f	true	Project Notes.docx	
03-12-2013 08:31:24	INFO	File Close	Win2003E	false	Project Notes.docx	
03-12-2013 08:31:24	INFO	File Modify	Win2003E	false	Project Notes.docx	
03-12-2013 08:31:23	INFO	File Lock	win2003f	true	Project Notes.docx	
03-12-2013 08:31:23	INFO	File Modify	win2003f	true	Project Notes.docx	
03-12-2013 08:31:23	INFO	File Close	win2003f	true	Project Notes.docx	
03-12-2013 08:30:34	INFO	File Lock	Win2003E	false	Project Notes.docx	
03-12-2013 08:30:34	INFO	File Open	win2003f	true	Project Notes.docx	
03-12-2013 08:29:44	INFO	File Close	Win2003E	false	Project Notes.docx	

Clicking on the **Actions** table menu provides the following options:

Refresh View	Refresh all information provided in the table. This can also be done from the right-click context menu of the table.
Clear Events	Remove all items from the table. This can also be done from the right-click context menu of the table.

4. File Conflict View

Introduction

Files conflicts can occur for the following reasons:

1. Two or more users open a file at the same time before all files can be locked down by the running [file collaboration job](#).
2. A file is already opened by a user when a file collaboration job is started and the file size and timestamp does not match the other target hosts.
3. A file is already opened by two or more users when a file collaboration job is started.
4. A file was modified on two or more hosts between job restarts or network outages.
5. A general I/O failure occurs on the [Source Host](#) after the file has been modified, but before the file is synchronized to all [Target Hosts](#). In this case, the file will automatically be quarantined.

When a file conflict is detected, the file is placed in the File Conflict list (shown below) with a specific status which will determine how the conflict is resolved. The three possible file conflict statuses along with their resolution strategies are as follows:

Conflict Status	Resolution Strategy
Pending Conflict Resolution	<p>This status will be assigned to files that have already been verified or synchronized by the session via the initial synchronization process. When all files in use are closed by users on the source hosts, the files will be analyzed to determine if a file conflict has occurred as follows:</p> <ul style="list-style-type: none"> • If more than one file has been modified then the file will be quarantined by updating the file conflict status to quarantined. • If only one file has been modified then that file will be used as the source, synchronized with all other participating hosts, and removed from the File Conflict list • If no files have been modified then no action will be taken and the file will be removed from the File Conflict list
Pending Initial Synchronization	<p>This status will be assigned to files that have not been verified or synchronized by session via the initial synchronization process. When all files in use are closed by users on the source hosts, then standard file conflict resolution will be performed based on the configured File Conflict Resolvers. However, if the "Quarantine Offline Multi-Edits" option is enabled, then if a file is modified on 2 or more hosts while the collaboration session is not running, and the last modified timestamps are all newer than the last timestamp recorded by the collaboration session, then the file will be quarantined.</p>
Quarantined	<p>A file will be quarantined when a file conflict with "Pending Conflict Resolution" status cannot be resolved or a fatal I/O error occurs. Quarantined files will need to be explicitly removed from the File Conflict list.</p>

When a file conflict occurs, the status will be set to **Pending Conflict Resolution** if the file has already been verified or synchronized by the initial synchronization process, otherwise the file conflict status will be set to **Pending Initial Synchronization**. If the conflict is a result of a fatal I/O error on the source then the file conflict status will be set to **Quarantined**.

NOTE: If a file collaboration job is stopped before a file conflict with a status of **Pending Conflict Resolution** is resolved, then that file will automatically be quarantined the next time the file collaboration job is started.

File Conflict and Quarantine Scenarios

A job is started and **Initial Scan Logic** is performed on a file

If file has never been synchronized by PeerLink and if file sizes and last modified times do not match on all collaboration hosts, or if file does not exist on one or more hosts, then the file will be synchronized based on the configured file conflict resolver, which is typically most recent last modified time. Files that have previously been synchronized by PeerLink where just a single file's last modified timestamp is newer than the last recorded timestamp, then that file will be synchronized to all other hosts; however, if two or more files have a more recent last modified timestamp than was last recorded timestamp, then the file will be quarantined (this is the default behavior and can be disabled by de-selecting the File Conflict Resolvers "Quarantine Offline Version Conflicts" configuration option).

A single user has a file opened before starting a collaboration job

A file conflict will be created with a status of "Pending Initial Synchronization". After the user closes the file, if all file sizes and timestamps match then the file conflict is removed and no synchronization is performed. However, if any file last modified times or file sizes do not match, the file will be synchronized or quarantined based on the configured file conflict resolution strategy and according to the initial scan logic detailed above. Once the file is synchronized, the file conflict will be removed.

Two or more users have a file open before starting a collaboration job

A file conflict will be created with a status of "Pending Conflict Resolution". After the users close all files the conflict will be removed if the last modified timestamp matches on all files, otherwise if the file has never been synchronized by PeerLink then the file conflict will be updated to quarantined. However, if the file has previously been synchronized by PeerLink, then the file will be synchronized or quarantined based on the configured file conflict resolution strategy and according to the initial scan logic detailed above.

Two or more users open a file at the same time

In the rare situation when two users open a file at the same time, or in-and-around the same time and PeerLink is unable to obtain corresponding locks on target hosts before this happens (this is dependent on WAN latency and other factors), then a file conflict will be created with a status of "Pending Conflict Resolution". After all users close the files, file lock conflict resolution will be performed as follows:

- If all files last modified timestamps and file sizes match, then the file conflict will be removed.
- If only a single file has been modified, then the file that changed is synchronized or quarantined based on the configured file conflict resolver and according to the initial scan logic detailed above.
- If two or more files have been modified since it was opened, then the file conflict status will be updated to quarantined.

Quarantined Files

Once a file is marked as **Quarantined**, the file will no longer participate in collaboration, and thus changes to any version of the file will not be propagated to other hosts. However, subsequent file activity on a quarantined file will be logged in the event log as a warning so you can determine who modified the file while it was quarantined. Quarantined files are saved to disk and will survive session restarts. The File Conflict list displays the time and date of the quarantine along with an error message indicating the reason for the quarantine (see below). A Quarantined File event is also logged in the Event Log and you can obtain a more detailed reason for the quarantine by analyzing the Event Log file(s). In addition, if [Email Alerts](#) and/or [SNMP Notifications](#) are configured and enabled for **File Quarantines**, then the appropriate message(s) will be sent.

Removing a file from Quarantine

You must explicitly remove a file from quarantine in order to have it participate in the collaboration session once again. To remove a file from quarantine, select the file in the File Conflict list, select the host with the correct version, and press the **Release Conflict** button. After doing this all hosts are checked to make sure the file is not currently locked by anybody. If no locks are found, then locks are obtained on all versions of the file and the targets that are out-of-date are synchronized with the selected source host. You may also choose to perform

[illegible]

The following right-click menu items are unique to this particular table:

Refresh View	Refresh all information provided in the table. This can also be done from the right-click context menu of the table.
Clear Events	Remove all items from the table. This can also be done from the right-click context menu of the table.

6. Participants View

The Participants View shows a list of all currently configured [host participants](#) for the selected [file collaboration job](#) and contains a column used to display activity status occurring on the hosts. If a host has become unavailable, an error message will be displayed next to the failed host in red.

Summary	Session	Event Log	File Conflicts (1)	Alerts (3)	Participants (2)	Configuration
---------	---------	-----------	--------------------	------------	------------------	---------------

Host Participants				
Host	Root Path	Status	State	Message
Win2003E	C:\Projects	Agent Service Shut...	Inactive (P...	Agent service on host Win2003E was shu
win2003f	C:\Projects	Not Collaborating	Inactive	Job Stopped

Host Participant State Change Log				
Filter by :	Host: <input type="text"/>	Status: <input type="text"/>	State: <input type="text"/>	
Date	Host	Status	State	Message
03-12-2013 09:39:05	win2003f	Not Collaborating	Inactive	Job Stopped
03-12-2013 09:39:05	Win2003E	Agent Service Shutd...	Inactive (Pendi...	Agent service on host Win2003E wa...
03-12-2013 09:33:30	win2003f	Collaborating	Active	
03-12-2013 09:33:30	Win2003E	Collaborating	Active	
03-12-2013 09:31:15	win2003f	Not Collaborating	Inactive	Job Stopped
03-12-2013 09:31:15	Win2003E	Not Collaborating	Inactive	Job Stopped
03-12-2013 09:27:08	win2003f	Collaborating	Active	

The Participants View also contains a table that displays the most recent host participant state changes, e.g. when a host was removed from collaboration session, or when a host came back online, etc. This functionality is broken down into two parts: right-click context menu items and a subview entitled **Host Participant State Change Log**.

The following unique items are available in a right-click context menu for the top part of the Participants View:

Disable Host Participant	Temporarily disables the selected participant from taking part in the file collaboration job. You might want to do this if the host is experiencing temporary network outages.
Cancel Auto Restart	This menu item is only available if the global auto-restart functionality enabled and the selected host has been removed from the file collaboration job that is currently being viewed. The cancelling of the auto-restart functionality for the host will only be in effect until the next time you start the file collaboration job. If quorum has been lost for the job, cancelling auto-restart on all unavailable hosts will prevent the job from automatically restarting. If quorum has not been lost, cancelling auto-restart will simply prevent a host from automatically re-joining collaboration.

The **Host Participant State Change Log** is a log of all host participant status changes (Collaborating, Not Collaborating, etc.) and/or state changes (Active, Pending Restart, etc.) of a host participant. This table is currently limited to 250 rows and can be filtered by host, by status, and by state.

The following items are available in the right-click context menu for this table:

Refresh View	Refresh all information provided in the table.
Clear	Remove all items from the table.

Events

7. Configuration View

This view displays a quick summary of all configurable items for the selected [file collaboration job](#). Each page of the [File Collaboration Configuration](#) dialog is represented in it's own part of the view and can be collapsed if desired. Clicking Edit this File Collaboration Configuration will immediately bring you to the File Collaboration Configuration dialog where you can edit the current configuration.

Summary | Session | Event Log | File Conflicts (1) | Alerts (3) | Participants (2) | Configuration

[Edit this File Collaboration Configuration](#)

Currently Running Configuration Summary

- ▼ **Selected Participants and Configurations**
 - Win2003E C:\Projects (Detector Type: Default)
 - win2003f C:\Projects (Detector Type: Default)
- ▼ **General Settings**

Session Name:	Projects
Session ID:	100
Transfer Block Size:	128 KB
Verify Checksum:	true
Session Threads:	10
File Copy Threads:	5
Background Sync. Threads:	5
Timeout:	180 Seconds
Scan Delay:	10
Remove Filtered Files On Folder Delete:	false
Require All Hosts At Start:	false
Auto Start:	false
- ▼ **Selected File Filters**
 - Default (Any)
 - Excluded Wildcard Expressions: ~*, *, *.BAK, *.BCK, *.WBK, *.ASD, *.XLK, *.EXE, *.DLL, *.DWL*, *.AC\$, *.SV\$, <<^\.*\atmp[0-9]{4,}\$>> ,
 - Included Wildcard Expressions: None Selected
 - Date Filter: Include all dates
 - Size Filter: None
- ▶ **Locking**
- ▶ **Conflict Resolution**
- ▶ **Delta Compression Settings**
- ▶ **File Metadata Settings**
- ▶ **Logging Alerts**
- ▶ **Target Protection Settings**
- ▶ **Email Alerts**

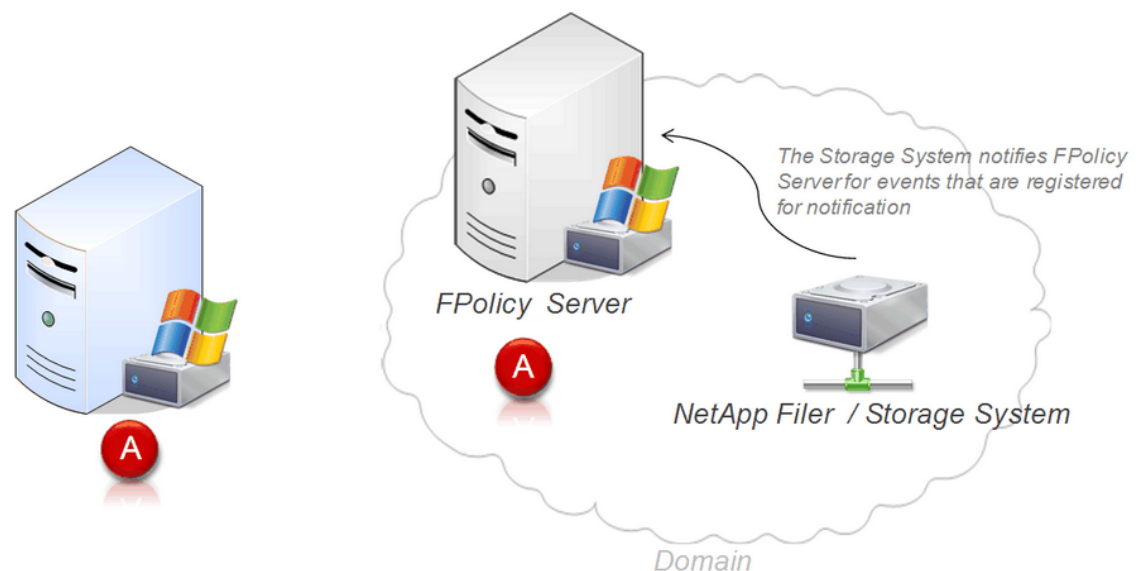
Advanced Configuration

The topics in this section provide information on advanced functionality and configuration options available in PeerLink.

NetApp Configuration

Overview

PeerLink supports the ability to include content from CIFS shares on a NetApp storage device within a [file collaboration session](#). In order for content from a NetApp storage device to be included in a file collaboration session, an additional Windows proxy server is required on the same subnet and domain as the NetApp device. The connection between the proxy server and the NetApp device must be as fast as possible. The [PeerLink Agent](#) will be installed on this proxy server and will use special NetApp API calls to serve as a bridge between the NetApp device and the file collaboration session. This proxy server is also known as an FPolicy Server. The diagram below illustrates the relationship between the FPolicy Server and the NetApp device.



In this diagram, communication between the two Agents (represented by the red circles) is handled by a common [PeerLink Broker](#).

For an in-depth look at how PeerLink works with NetApp and the FPolicy system, please email support@peersoftware.com with a request for more information on NetApp support.

1. Prerequisites and Configuration

Prerequisites

For an up-to-date list of prerequisites, please see <https://www.peersoftware.com/resources/tech-briefs.html?view=document&id=57>.

Configuration

1. Review the prerequisites above before beginning the installation and configuration process.
2. Follow the general PeerLink installation steps that can be found [here](#).
3. Launch the PeerLink Hub Client.

Note: Before you can start the PeerLink Hub interface/client, the PeerLink Hub Service needs to be running. See the [installation](#) section for more information.

4. Install your license within the PeerLink Hub. For more information, see the [licensing](#) section. You must contact our sales team to request a license which supports NetApp. Unless requested, all licenses that are issued do not include NetApp support by default.
5. Create a new file collaboration job. For more information, visit the section on [creating a job](#).
6. During the job configuration process, one or more [participating hosts](#) must be configured to interface with NetApp. To do so, view the [Participants page](#) of the File Collaboration Configuration dialog, and add the desired available host to the job. After the host is added to the job, enter the UNC path of the appropriate share on the NetApp Filer to the configured directory of the participant that is to act as a FPolicy Server. Then select **NetApp** as the participant's configured Event Detector. An example is shown below. As a result of the selection, a configuration dialog will be displayed requesting additional configuration for the FPolicy Server. The only mandatory field is for the local path. The rest of the dialog represents [Advanced FPolicy Configuration](#).

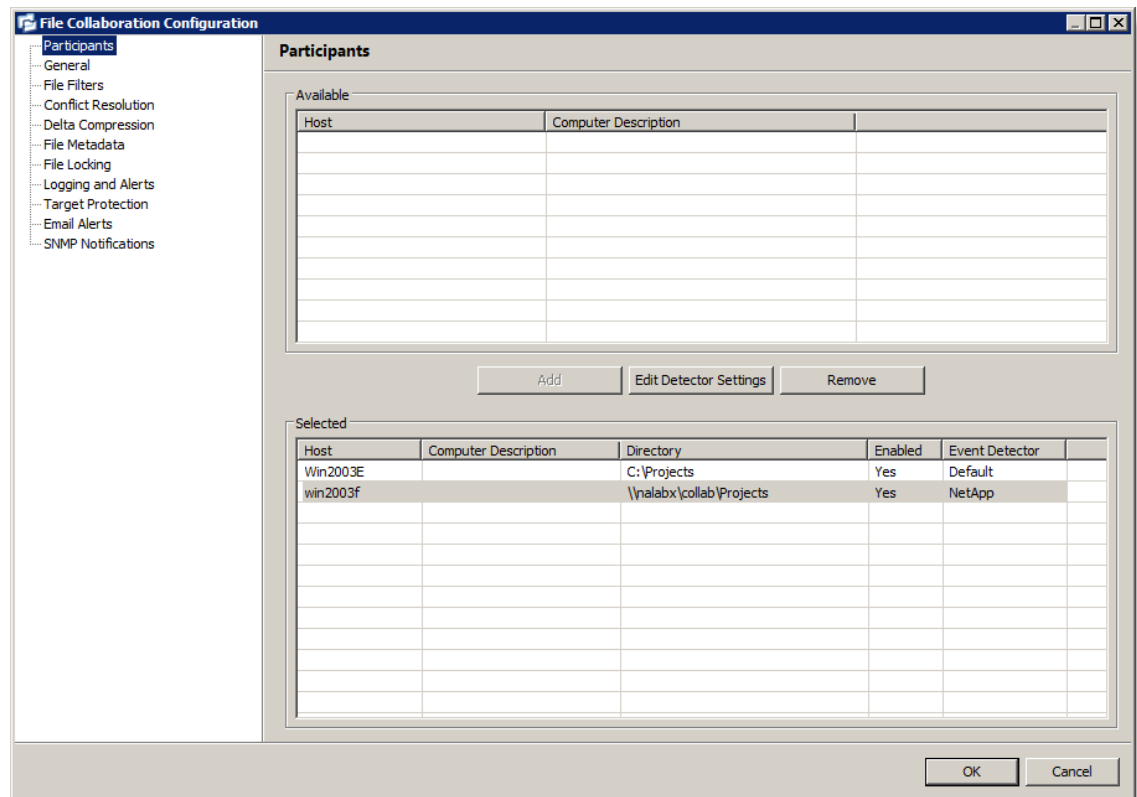


Image 1

7. In order for a file collaboration job to be able to detect files that are already opened, a local

mapping to the CIFS share on the NetApp device is required. By default, PeerLink will automatically look this up. If necessary, you can also enter your own. This local mapping should not include any sub-folders for the root UNC path. This local path must be entered into the NetApp Options dialog for each participant (as highlighted in Step 7). An example is listed below.

Example:

UNC path to NetApp Filer (shown in Image 1 above):
Local Path (obtained for share "collab" in Image 2 below):
Value Entered in NetApp Options (Image 3 below):

\\nalabx\collab\Projects
C:\vol\nalabx_vol1
C:\vol\nalabx_vol1\collab

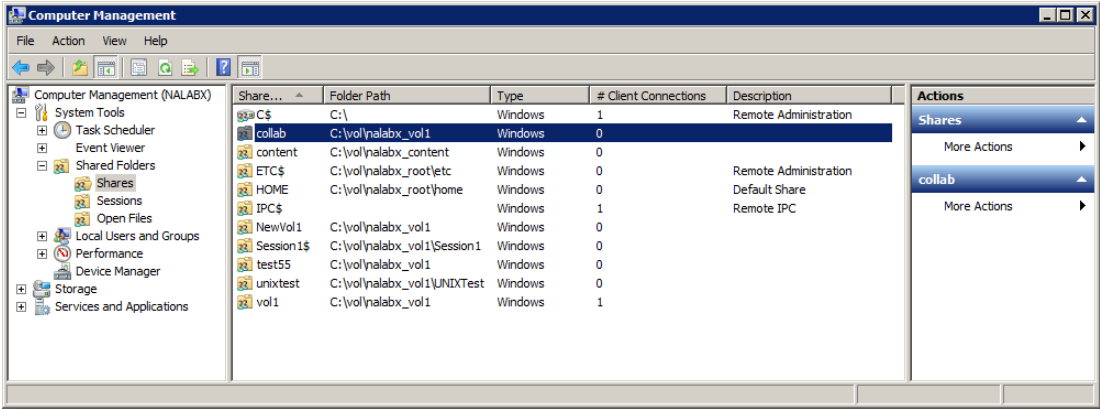


Image 2

NetApp Options

NetApp Options for this Job

Local Path to CIFS Share: *

Automatically detect local path: ☒

User SID Conversion Type: Cache Lookup

Filter events from these users:

Access Event Suppression Time: 1

A '*' represents a required configuration item.

Advanced (Optional) fPolicy Settings for: win2003f

Manually configure fPolicy on Filer: ☐

fPolicy Name:

Excluded Extensions:

Include or Exclude Volumes

☒ Include ☐ Exclude

Add Edit Remove

NOTE: Any changes made to these Advanced fPolicy Settings will be used with every other session in which this fPolicy Server is connecting with a NetApp Filer.

OK Cancel

Image 3

8. In addition to setting a local path, some additional host-specific NetApp configuration options are available (as shown in Image 3 above):

Local Path to CIFS Share	See above .
Automatically detect local path	Uncheck this option to manually enter in the local path to the CIFS share on the NetApp device.
User SID	By default, events returned from NetApp do not include a user name, but

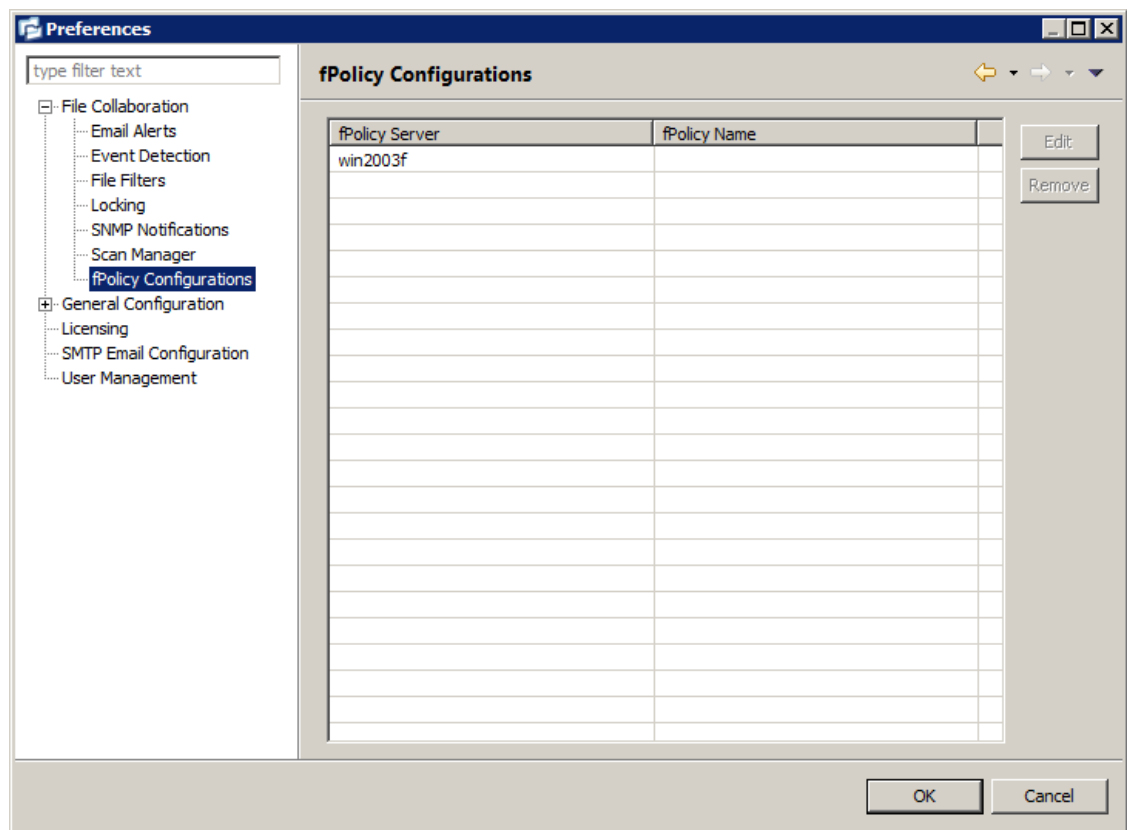
Conversion Type	rather the user's SID. If this option is set to Cache Lookup, PeerLink will automatically lookup the user name tied to this SID value the first time it is detected. In the future, PeerLink will then use a cache to quickly convert the SID.
Filter events from these users	A comma-separated list of user account names from which events will be ignored. Ideal for filtering out events from backup and/or archival services by filtering on the username under which a backup and/or archival service is running.
Access Event Suppression Time	Represents how long an open event will be delayed before being processed. Used to help reduce the amount of real time chatter in several scenarios. The default value is 1 second. A value of 0 will allow for a dynamically changing amount of time that an open event will be delayed based on the load of the system.

2. Advanced fPolicy Configuration

For optimum performance, it is best practice to only listen for file events on CIFS shares and file types that are relevant to your configured file collaboration jobs. The advanced FPolicy options highlighted below provide a way to restrict listening for file events to specific volumes and by file types. We strongly advise that you configure these options accordingly.

Global FPolicy Configuration

FPolicy Configurations represent advanced settings that are used when communicating with a NetApp storage device. In PeerLink, they are set on a per FPolicy Server (or participating host) basis. As a result, all file collaboration jobs that use a particular host for NetApp collaboration will each use the same FPolicy settings, no matter which shares are being accessed. These FPolicy settings are initially set when configuring a [participant](#) within a file collaboration job to use NetApp support. For more information on this process, see the [NetApp Configuration](#) section. Please note that FPolicy Configurations can only be created during [job configuration](#). Once created, they can be viewed and modified on a global level through the PeerLink Hub. To do so, click on the **Window** menu from with the PeerLink Hub, and select **Preferences**. On the left-hand side of the dialog that pops up, open the tree node titled **File Collaboration** and select **FPolicy Configurations**. The following screen will be displayed.



From this dialog, you can edit a selected FPolicy Configuration by clicking the **Edit** button, or remove a selected configuration by clicking the **Remove** button. Editing a configuration will bring up the following dialog:

NetApp Options

Advanced (Optional) fPolicy Settings for: win2003f

Manually configure fPolicy on Filer: ☐

fPolicy Name:

Excluded Extensions:

Include or Exclude Volumes

☒ Include ☐ Exclude

Add Edit Remove

NOTE: Any changes made to these Advanced fPolicy Settings will be used with every other session in which this fPolicy Server is connecting with a NetApp Filer.

OK Cancel

Configurable options are as follows:

Manually configure FPolicy on Filer	When enabled, the specified FPolicy name must already exist on the NetApp Filer and have all required features enabled. When this option is enabled, all configured advanced FPolicy options will be ignored.
FPolicy Name:	The name of the FPolicy configuration as used by the FPolicy Server to register and communicate with the NetApp Filer.
Excluded Extensions	Extensions entered here are excluded from event detection on the NetApp Filer. Values are comma separated and must not contain any periods. More information on screening by extensions is below.
Include or Exclude Volumes	List all volumes on the NetApp Filer to exclude or include based on selected choice. More information on screening by volumes is below.

Advanced FPolicy Settings

Screening by Volume

FPolicy enables you to restrict a policy to a certain list of volumes by including or excluding volumes that need to be screened.

Using the include list, you can request notifications for the specified volume list. Using the exclude list, you can request notifications for all volumes except the specified volume list. However, by default, both the include and exclude list are empty.

Wildcard information for screening with volumes

You can use the question mark (?) or asterisk (*) wildcard characters to specify the volume. The question mark (?) wildcard character stands for a single character. For example, entering vol? in a list of volumes that contain vol1, vol2, vol23, vol4, will result in only vol1 and vol2 being matched.

The asterisk (*) wildcard character stands for any number of characters that contain the specified string. Entering *test* in a list of volumes to exclude from file screening excludes all volumes that contain the string such as test_vol and vol_test.

Screening by Extension

FPolicy enables you to restrict a policy to a certain list of file extensions by excluding extensions that need to be screened.

Note: The maximum length of a file name extension supported for screening is 260 characters. Screening by extensions is based only on the characters after the last period (.) in the file name. For example, for a file named fle1.txt.name.jpg, file access notification takes place only if a file policy is configured for the jpg extension.

3. Troubleshooting

Troubleshooting

For an up-to-date list of troubleshooting information, please see <https://www.peersoftware.com/resources/tech-briefs.html?view=document&id=68>.

Custom SSL Intergration

Overview

PeerLink supports the ability to use custom or private SSL certificates to connect Agents to the Broker. The Keytool certificate management utility will be used to store the key and certificate into a keystore file which protects the private keys with a password.

Please note the the paths in the following sections reference a default install directory for both the PeerLink Hub and PeerLink Agent.

[Use Existing Certificate](#)

[Create New Certificate](#)

1. Use Existing Certificate

Perform the necessary commands using the keytool application bundled with your PeerLink Hub or Agent installation (Java 6).

Keytool location on Hub

system: C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin

Keytool location on Agent

system: C:\Program Files\Peer Software\PeerLink Agent\jre\bin

Broker and Agent Keystore Generation

You will need to have two custom/private certificates. One for the Broker and one for all the participating Agents. You may select different algorithms and encryption key size (i.e. RSA, DSA with 1024 or 2048 key size).

Step 1.

View/list the contents of the custom/private certificates. Perform these steps for both certificates (Broker and Agent). Make a note of the Alias of the certificate, if it exists.

```
keytool -list -v -keystore HubCert.pfx -storetype pkcs12
```

HubCert.pfx	Represents the custom/private certificate for the Broker.
AgentCert.pfx	Represents the custom/private certificate for the Agents.

Note: The command will prompt you to enter the password you set on your custom certificate, if applicable.

Step 2:

Add the custom/private Broker certificate into the Broker keystore.

```
keytool -importkeystore -deststorepass plBroker4321 -destkeypass plBroker4321 -destkeystore broker.ks -srckeystore HubCert.pfx -srcstoretype PKCS12 -srcstorepass PASSWORD -alias ALIAS -destalias broker
```

plBroker-4321	The password you assign to the new Broker keystore.
broker.ks	Destination keystore that will be created containing the custom/private certificate.
HubCert.pfx	Custom/private certificate being imported into the new keystore.
PASSWORD	The password of the custom/private certificate, if it exists. If you omit the -srcstorepass command you will be prompted for the certificate password if needed.
ALIAS	The Alias of the custom/private certificate you discovered in Step 1 above.
broker	The Alias of the new keystore containing the custom/private.

Note: The broker.cer and broker.ks files will be created in the \jre\bin folder where the keytool application resides.

Step 3:

Add the custom/private Agent certificate into the Client keystore.

```
keytool -importkeystore -deststorepass plClient4321 -destkeypass
plClient4321 -destkeystore client.ks -srckeystore AgentCert.pfx -
srcstoretype PKCS12 -srcstorepass PASSWORD -alias ALIAS -
destalias client
```

plClient4321	The password you assign to the new Broker keystore.
client.ks	Destination keystore that will be created containing the custom/private certificate.
AgentCert.pfx	Custom/private certificate being imported into the new keystore.
PASSWORD	The password of the custom/private certificate, if it exists. If you omit the -srcstorepass command you will be prompted for the certificate password if needed.
ALIAS	The Alias of the custom/private certificate you discovered in Step 1 above.
client	The Alias of the new keystore containing the custom/private.

Note: The client.cer and client.ks files will be created in the jre\bin folder where the keytool application resides.

Step 4:

Export the broker's certificate so it can be shared with clients.

```
keytool -export -alias broker -keystore broker.ks -file broker.cer
```

broker	The Alias of the broker keystore containing the custom/private certificate created in Step 2 above.
broker.ks	The keystore file created in Step 2 above containing the custom/private certificate for the Broker.
broker.cer	The certificate file created in Step 2 above.

The command will prompt you to enter the password for the broker keystore (i.e. plBroker4321).

Step 5:

Export the client's certificate so it can be shared with broker.

```
keytool -export -alias client -keystore client.ks -file client.cer
```

client	The Alias of the client keystore containing the custom/private certificate created in Step 3 above.
client.ks	The keystore file created in Step 3 above containing the custom/private certificate for the Agents.
client.cer	The certificate file created in Step 3 above.

The command will prompt you to enter the password for the client keystore (i.e. plClient4321).

Step 6:

Create a truststore for the broker, and import the client's certificate. This establishes that the broker "trusts" the client:

```
keytool -import -alias client -keystore broker.ts -file client.cer
```

client	The Alias of the client keystore containing the custom/private certificate created in Step 3 above.
broker.ts	The broker truststore to be created.
client.cer	The certificate file created in Step 3 above.

The command will prompt you to enter the password for the broker keystore (i.e. plBroker4321).

Step 7:

Create a truststore for the client, and import the broker's certificate. This establishes that the client "trusts" the broker.

```
keytool -import -alias broker -keystore client.ts -file broker.cer
```

broker	The Alias of the client keystore containing the custom/private certificate created in Step 3 above.
client.ts	The client truststore to be created.
client.cer	The certificate file created in Step 2 above.

The command will prompt you to enter the password for the client keystore (i.e. plClient4321).

Copy the generated keystore file into their appropriate location

On the Hub system: Copy the following files from the "C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin" directory into the "C:\Program Files\Peer Software

"File Collaboration Enterprise\Broker\keys" directory on the Hub system. Overwrite the existing files.

```
broker.ks
broker.ts
```

On the Agent system: Copy the following files from the "C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin" directory into the "C:\Program Files\Peer Software\PeerLink Agent\keys" directory on the Agent systems. Overwrite the existing files.

```
client.ks
client.ts
```

Restart all PeerLink services for the changes to take effect

Note: We recommend you create a folder outside the PeerLink Hub/Agent installation directories in which to store the keystore files. This will ensure that upgrades will not clear/overwrite these files. The steps outlining this process will be posted shortly.

2. Create New Certificate

Perform the necessary commands using the **keytool** application bundled with your PeerLink Hub or Agent installation (Java 6).

Keytool location on Hub PEERLINK_HUB_INSTALLATION_FOLDER\jre\bin

system:

Keytool location on Agent PEERLINK_AGENT_INSTALLATION_FOLDER\jre\bin

system:

Broker Keystore generation

Step 1.

Using keytool, create a certificate for the Broker.

```
keytool -genkey -alias broker -keyalg RSA -keystore broker.ks -
storepass plBroker4321 -validity 3000
```

broker	The alias of the new broker keystore containing the new certificate.
broker.ks	Destination broker keystore that will be created containing the new certificate.
plBroker-4321	The password you assign to the new broker keystore.

Note: The broker.ks file will be created in the \jre\bin folder.

Example:


```

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>keytool -genkey -
broker -keyalg RSA -keystore broker.ks -storepass plBroker4321 -validity 3000
What is your first and last name?
[Unknown]: Monika Cuellar
What is the name of your organizational unit?
[Unknown]: Peer Software, Inc.
What is the name of your organization?
[Unknown]: Peer Software, Inc.
What is the name of your City or Locality?
[Unknown]: Centreville
What is the name of your State or Province?
[Unknown]: VA
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centreville
ST=VA, C=US
correct?
[no]: yes

Enter key password for <broker>
(RETURN if same as keystore password):

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>

```

Step 2:

Export the broker's certificate so it can be shared with clients.

```
keytool -export -alias broker -keystore broker.ks -file broker.cer
```

broker	The alias of the new broker keystore containing the new certificate..
broker.ks	Destination broker keystore that will be created containing the new certificate.
broker.cer	The name of the broker's certificate to be created.

Note: The broker.cer file will be created in the \jre\bin folder.

Example:

```

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>keytool -export -
broker -keystore broker.ks -file broker.cer
Enter keystore password: plBroker4321
Certificate stored in file <broker.cer>

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>

```

Step 3:

Create a certificate/keystore for the client.

```
keytool -genkey -alias client -keyalg RSA -keystore client.ks -
storepass plClient4321 -validity 3000
```

client	The alias of the new client keystore containing the new certificate.
client.ks	Destination keystore for the client that will be created containing the new certificate.
plClient4321	The password you assign to the new client keystore.

Note: The client.ks file will be created in the \jre\bin folder.

Example:

```
C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>keytool -genkey -
client -keyalg RSA -keystore client.ks -storepass plClient4321 -validity 3000
What is your first and last name?
[Unknown]: Monika Cuellar
What is the name of your organizational unit?
[Unknown]: Peer Software, Inc.
What is the name of your organization?
[Unknown]: Peer Software, Inc.
What is the name of your City or Locality?
[Unknown]: Centreville
What is the name of your State or Province?
[Unknown]: VA
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centreville
C=US
correct?
[no]: yes

Enter key password for <client>
(RETURN if same as keystore password):

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>
```

Step 4:

Create a truststore for the client, and import the broker's certificate. This establishes that the client "trusts" the broker.

```
keytool -import -alias broker -keystore client.ts -file broker.cer
-storepass plClient4321
```

broker	The alias of the broker keystore created in step 1.
client.ts	Destination truststore for the client that will be created containing the broker's certificate.
broker.cer	The broker's certificate created in step 2.
plClient4321	The password assigned to the client keystore in step 3.

Example:

```
C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>keytool -import -
broker -keystore client.ts -file broker.cer -storepass plClient4321
Owner: CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centre
ST=VA, C
=US
Issuer: CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centre
ST=VA,
C=US
Serial number: 4fa7f34f
Valid from: Mon May 07 12:07:43 EDT 2012 until: Fri Jul 24 12:07:43 EDT 2020
Certificate fingerprints:
    MD5: 2C:18:DD:B5:CD:C5:3D:B2:9B:E3:93:50:D6:74:2B:64
    SHA1: 30:77:94:9B:34:63:6C:DE:2C:98:9C:00:C2:B9:F6:21:AE:22:D7:DE
Trust this certificate? [no]: yes
Certificate was added to keystore

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>
```

Optional:

List the certificates in the broker keystore.

```
keytool -list -v -keystore broker.ks -storepass plBroker4321
```

Example:

```

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>keytool -list -v
keystore broker.ks -storepass plBroker4321

Keystore type: jks
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: broker
Creation date: May 7, 2012
Entry type: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centrev
ST=VA, C=US
Issuer: CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centre
ST=VA, C=US
Serial number: 4fa7f34f
Valid from: Mon May 07 12:07:43 EDT 2012 until: Fri Jul 24 12:07:43 EDT 2020
Certificate fingerprints:
    MD5:  2C:18:DD:B5:CD:C5:3D:B2:9B:E3:93:50:D6:74:2B:64
    SHA1: 30:77:94:9B:34:63:6C:DE:2C:98:9C:00:C2:B9:F6:21:AE:22:D7:DE

*****
*****

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>

```

Verify Client Certificate

If you want to verify client certificates, you need to take a few extra steps.

Step 1:

Export the client's certificate so it can be shared with broker.

```
keytool -export -alias client -keystore client.ks -file client.cer
-storepass plClient4321
```

Note: The client.cer file will be created in the \jre\bin folder.

Example:

```

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>keytool -export -
client -keystore client.ks -file client.cer -storepass plClient4321
Certificate stored in file <client.cer>

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>

```

Step 2:

Create a truststore for the broker, and import the client's certificate. This establishes that the broker "trusts" the client:

```
keytool -import -alias client -keystore broker.ts -file client.cer  
-storepass plBroker4321
```

Example:

```
C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>keytool -import -  
client -keystore broker.tx -file client.cer -storepass plBroker4321  
Owner: CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centrev  
ST=VA, C  
=US  
Issuer: CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centrev  
ST=VA,  
C=US  
Serial number: 4fa7f982  
Valid from: Mon May 07 12:34:10 EDT 2012 until: Fri Jul 24 12:34:10 EDT 2020  
Certificate fingerprints:  
    MD5: A7:D9:6E:78:8B:A9:AD:32:96:2D:51:6B:53:0B:E4:BD  
    SHA1: 16:05:7C:C4:D5:AB:E7:D3:7D:5B:2E:02:B5:3B:69:54:D1:C3:53:52  
Trust this certificate? [no]: yes  
Certificate was added to keystore  
  
C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>
```

Optional:

List the certificates in the client keystore.

```
keytool -list -v -keystore client.ks -storepass plClient4321
```

Example:

```

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>keytool -list -v
keystore client.ks -storepass plClient4321

Keystore type: jks
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: client
Creation date: May 7, 2012
Entry type: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centrev
ST=NY,
C=US
Issuer: CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centrev
ST=NY,
C=US
Serial number: 4fa80618
Valid from: Mon May 07 13:27:52 EDT 2012 until: Fri Jul 24 13:27:52 EDT 2020
Certificate fingerprints:
    MD5: 06:11:97:71:D6:23:91:63:2F:19:F4:05:EA:2F:9D:14
    SHA1: A7:26:80:9E:18:2B:46:8E:92:BB:AD:89:44:0A:8A:9C:8C:1F:62:38

*****
*****

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>

```

Copy the generated keystore file into their appropriate location

On the Hub system: Copy the following files from the "C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin" directory into the "C:\Program Files\Peer Software\File Collaboration Enterprise\Broker\keys" directory on the Hub system. Overwrite the existing files.

```
broker.ks
broker.ts
```

On the Agent system: Copy the following files from the "C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin" directory into the "C:\Program Files\Peer Software\PeerLink Agent\keys" directory on the Agent systems. Overwrite the existing files.

```
client.ks
client.ts
```

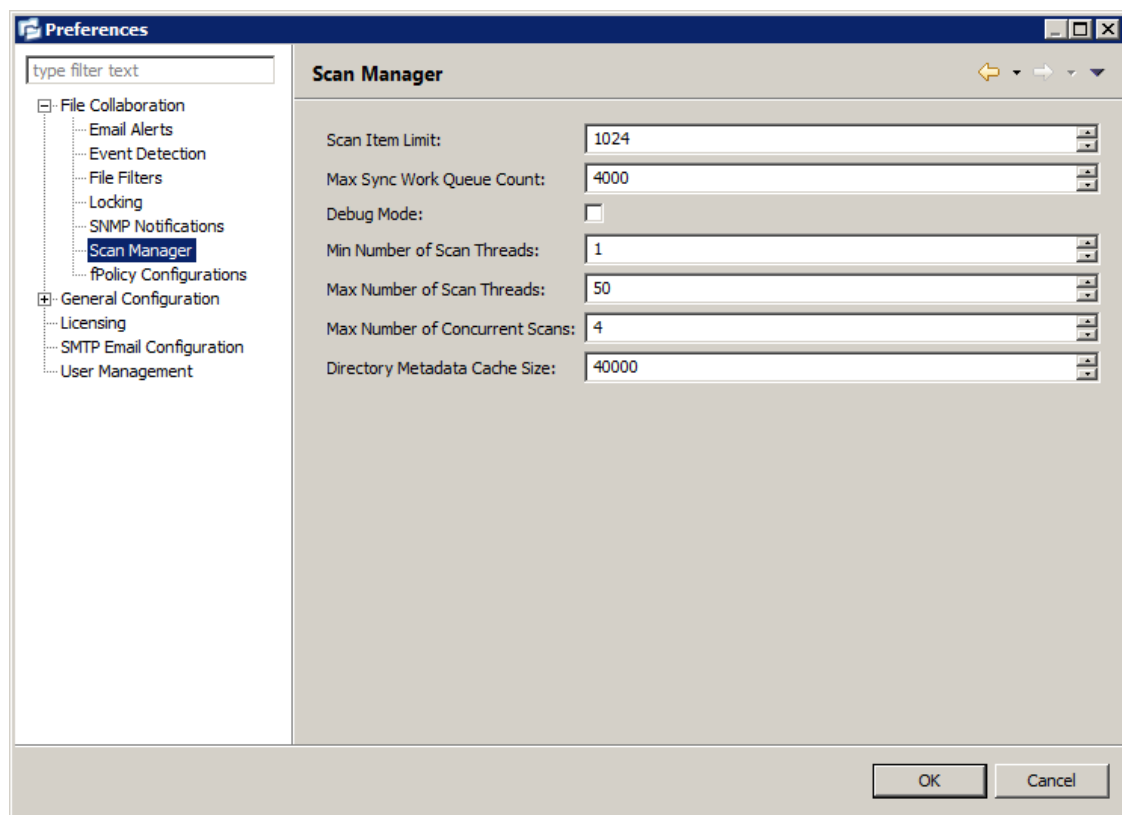
Restart all PeerLink services for the changes to take effect

Note: We recommend you create a folder outside the PeerLink Hub/Agent installation dir-

ectories in which to store the keystore files. This will ensure that upgrades will not clear/overwrite these files. The steps outlining this process will be posted shortly.

Scan Manager

A number of options are available to tune the way scans are performed for all [file collaboration jobs](#). These settings are configured on a global level. To view and modify these settings, click on the **Window** menu from with the [PeerLink Hub](#), and select **Preferences**. On the left-hand side of the dialog that pops up, open the tree node titled **File Collaboration** and select **Scan Manager**. The following screen will be displayed.



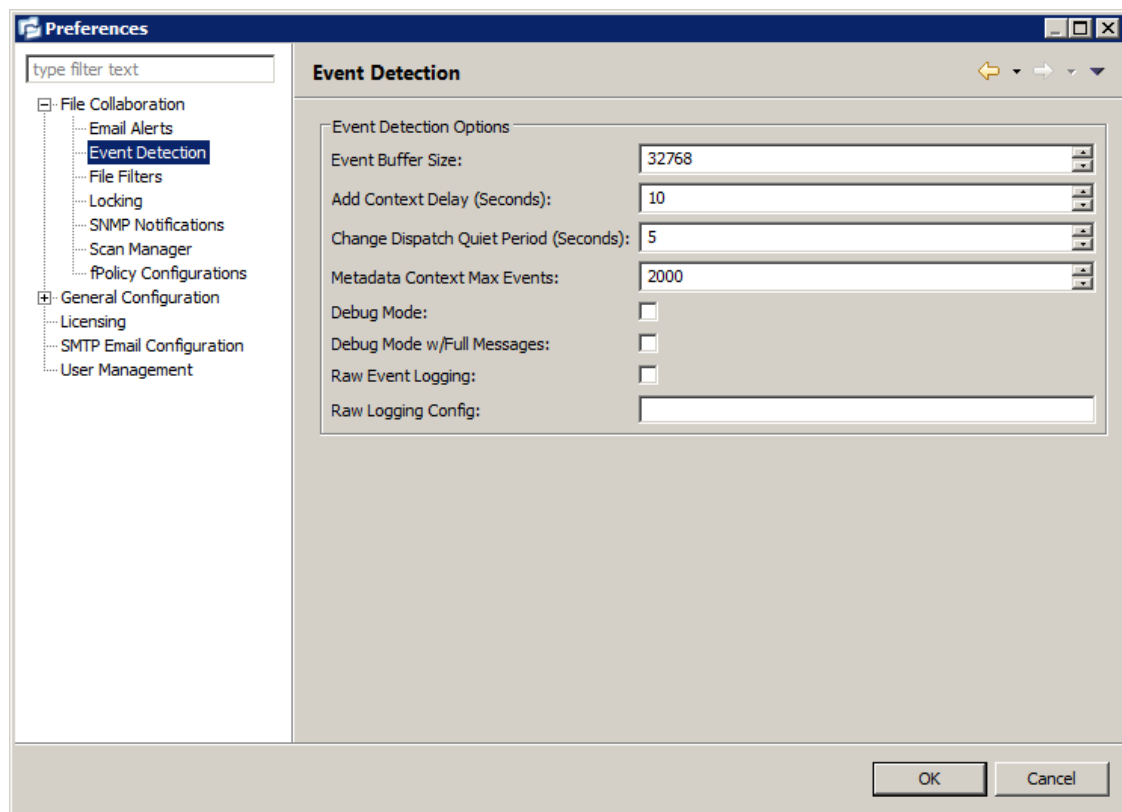
Available options are as follows:

Scan Item Limit	The maximum number of file and folder scan results that are returned in one scan iteration during a job's initial scan. This value is used to constrain the amount of memory used when performing initial scans with a large number of sessions.
Max Sync Work Queue Count	The maximum number of pending file transfers (as a result of the initial scan) that are queued in memory before pausing the current scan. This value only has an effect on sessions that require a massive amount of initial synchronization.
Debug Mode	If enabled, log debug information generated during all scans.

Min Number of Scan Threads	The minimum number of threads that are kept alive, even when all scans have been completed.
Max Number of Scan Threads	The maximum number of threads that can be created for use when scanning folders and files. This number should be set to at least the number of jobs that you are running.
Max Number of Concurrent Scans	The maximum number of scan threads that can be actively working at the same time. This differs from the Max Number of Scan Threads in that not all created scan threads can be simultaneously doing work.
Directory Metadata Cache Size	The number of directory metadata scan results to store in memory cache before persisting to disk.

Event Detection

A number of options are available to tune the way event detection occurs for all [file collaboration jobs](#). These settings are configured on a global level. To view and modify these settings, click on the **Window** menu from with the [PeerLink Hub](#), and select **Preferences**. On the left-hand side of the dialog that pops up, open the tree node titled **File Collaboration** and select **Event Detection**. The following screen will be displayed.

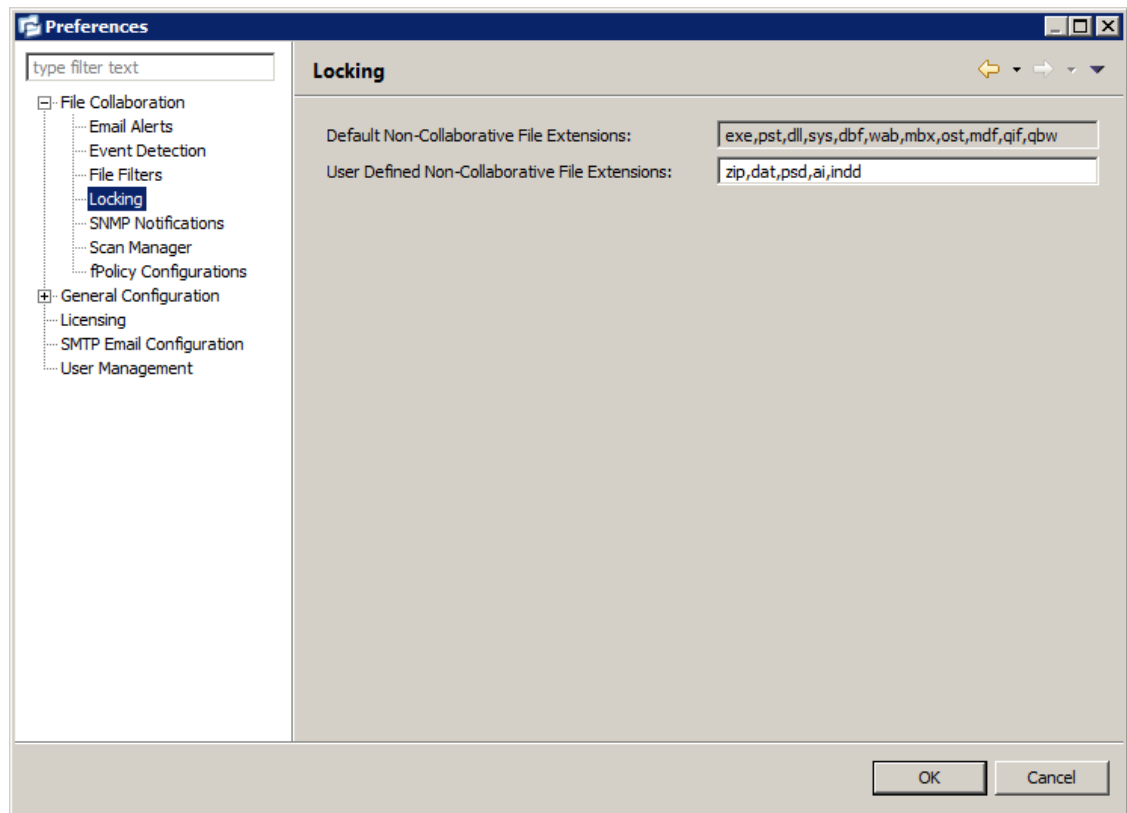


Available options are as follows:

Event Buffer Size	The size in bytes of the buffer used to store real-time events. If you receive Buffer Overflow alerts then try doubling the size of this buffer to 65536.
Add Context Delay (Seconds)	The number of seconds to wait before scheduling the synchronization of a newly created file.
Change Dispatch Quiet Period (Seconds)	The number of seconds to wait after a file is closed before scheduling the synchronization of the file
Metadata Context Max Events	This is the maximum number of security ACL or file attribute events stored in a batch before sending them to the PeerLink Hub. Reduce this number if you consistently make bulk security descriptor changes on a large number of files and/or have a very complex security model that requires a large size security descriptor.
Debug Mode	Enables advanced debug logging and alerts. Technical support may ask you to enable this feature if you are experiencing certain issues.
Debug Mode w/Full Messages	Enables advanced debug logging and alerts with Full Message information. Technical support may ask you to enable this feature if you are experiencing certain issues.
Raw Event Logging	Enables raw event logging for NetApp or device driver event detection. Technical support may ask you to enable this feature if you are experiencing certain issues.
Raw Logging Config	Advanced setting for Raw Event Logging that will override the defaults. Technical support will provide you with a value to put in this field if you are experiencing certain issues.

Locking

An option is available to mark certain file types as non-collaborative, changing the way locks on the specified file types are handled. These settings are configured on a global level for all [file collaboration jobs](#) and are critical for certain file types so that the file collaboration solution is able to correctly read any part of these files, ensuring any managed database type files are synchronized in a consistent and usable state. To view and modify these settings, click on the **Window** menu from with the [PeerLink Hub](#), and select **Preferences**. On the left-hand side of the dialog that pops up, open the tree node titled **File Collaboration** and select **Locking**. The following screen will be displayed.



Available options are as follows:

Default Non-Collaborative File Extensions	The default, non-editable, comma separated list of file extensions of non-collaborative file types (e.g. database files, etc.). Write access to source files of these types will be denied while the files are being synchronized.
User Defined Non-Collaborative File Extensions	An editable, comma separated list of file extensions of non-collaborative file types (e.g. database files, etc.). Write access to source files of these types will be denied while the files are being synchronized.

Central Agent Configuration

The ability to remotely manage the configuration for connected [PeerLink Agents](#) is available from within the [PeerLink Hub Client](#). To access, right click on any connected Agent, and select Edit Agent Configuration. The Agent Configuration dialog will be displayed, with three pages of available configuration items. In order for any configuration change to take effect, the selected Agent must be restarted. If no [Jobs](#) are running, you will have the option of restarting the Agent at the close of the configuration dialog.

WARNING: Changes to any option on the three pages of this dialog may result in problems when the Agent starts. Please ensure all settings are correct before saving the dialog and restarting the selected Agent.

1. Broker Configuration

Agent Configuration

Broker Configuration

WARNING: Changes to this page may make the Agent unable to start.
These changes will only take affect after the Agent is restarted.

Primary Broker Host:

Connection Type:

Broker Port:

Use Compression: ☒

Prefetch:

Socket Buffer Size (in KB):

Advanced Parameters:

(separate parameters with ';')

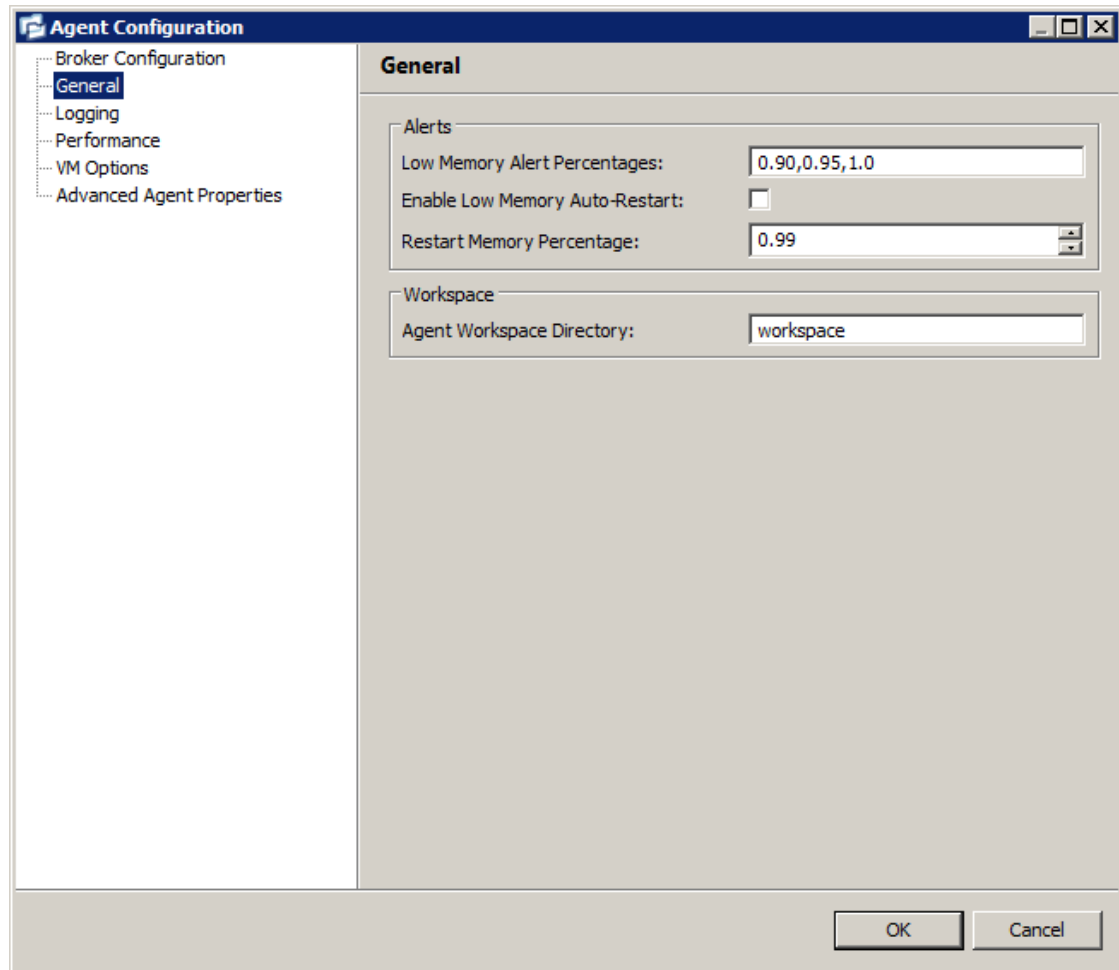
OK Cancel

Please note that these settings only apply to communication between the selected Agent and Broker and not to communication between the PeerLink Hub and Broker.

Primary Broker Host	The IP address or fully qualified host name of the server running the PeerLink Broker.
Connection Type	The type of connection to use when communicating with the PeerLink Broker. Types include ssl (encrypted) and tcp (not encrypted).
Broker Port	The port on which to communicate with the PeerLink Broker.
Use Compression	When enabled, all communication between the selected Agent and the PeerLink Broker will be compressed.
Prefetch	The number of messages pre-fetched from the PeerLink Broker. The higher the number, the more memory required by the Agent.
Socket Buffer Size (in KB)	TCP/IP socket buffer size in kilobytes
Advanced	A field for any additional parameters that may apply to communication

Parameters

between the Broker and the selected Agent. Parameters should be separated by semi-colons.

2. General**Alerts**

Notification and response settings for when the selected Agent runs low on memory.

Low Memory Alert Percentages	Memory percentages at which the Agent will post an alert to the PeerLink Hub's Alert list. Multiple percentages can be set, separated by commas. For example: .85,.90,.99
Enable Low Memory Auto-Restart	When enabled, the Agent will attempt to restart itself when its memory usage hits a certain threshold.
Restart	If Enable Low Memory Auto-Restart is enabled, the Agent will at-

Memory Percentage	tempt to restart itself at this memory threshold, for example: .98
--------------------------	---

Workspace

Agent Work-space Directory	Agent workspace directory where log files and other application data is stored. This path is relative to the Agent's installation directory. This can also be set to an explicit full path.
-----------------------------------	---

3. Logging

Agent Configuration

- Broker Configuration
 - General
 - Logging**
 - Performance
 - VM Options
 - Advanced Agent Properties

Logging

Agent Logging

Agent Logging Directory:

Agent Log File Size (in MB):

Max number of Agent log files:

STDOUT Log File Size (in MB):

Max number of STDOUT log files:

STDERR Log File Size (in MB):

Max number of STDERR log files:

JMS Messaging Log File Size (in MB):

Max number of JMS Messaging log files:

Profiler Log File Size (in MB):

Max number of Profiler log files:

JMS Message Logging

Enable Command Receiving Logging: ☐

Enable JMS Message Logging: ☐

Enable JMS Control Message Logging: ☐

Agent Profiler Logging Frequency:

Enable Agent Profiler Broker Statistics: ☒

OK Cancel

Agent Logging

Settings for tuning Agent logging. Depending on these settings, large log files may be produced.

Agent Log-ging Direct-	Agent logging directory relative to the Agent's installation directory. This can also be set to an explicit full path. Selected folder must
-------------------------------	---

ory	already exist before the Agent is restarted.
Agent Log File Size (in MB)	The maximum size to which each Agent.log file will grow before rolling over to a new file.
Max number of Agent log files	The maximum number of rolling Agent.log files to keep.
STDOUT Log File Size (in MB)	The maximum size to which each output log file will grow before rolling over to a new file.
Max number of STDOUT log files	The maximum number of rolling output log files to keep.
STDERR Log File Size (in MB)	The maximum size to which each error log file will grow before rolling over to a new file.
Max number of STDERR log files	The maximum number of rolling error log files to keep.
JMS Messages Log File Size (in MB)	The maximum size to which each JMS message log file will grow before rolling over to a new file.
Max number of JMS Message log files	The maximum number of rolling JMS message log files to keep.
Profiler Log File Size (in MB)	The maximum size to which each profiler log file will grow before rolling over to a new file.
Max number of Profiler log files	The maximum number of rolling profiler log files to keep.

JMS Message Logging

Settings for enabling and tuning JMS Message logging. These settings are useful for debugging purposes but will affect performance and produce large log files. Changes to these settings should only be made at the request of the Peer Support Team.

4. Performance

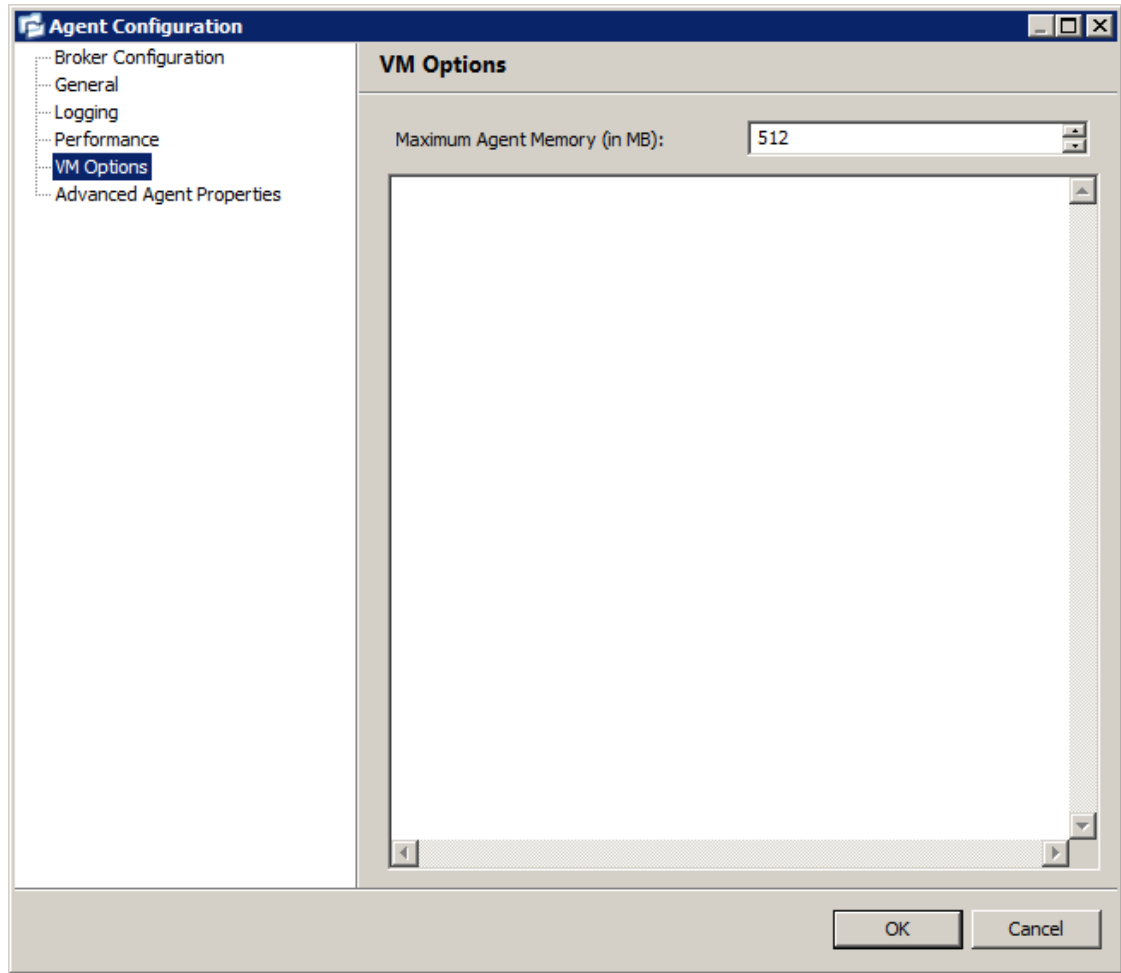
The screenshot shows the 'Agent Configuration' window with the 'Performance' tab selected. The left sidebar lists 'Broker Configuration', 'General', 'Logging', 'Performance' (highlighted), 'VM Options', and 'Advanced Agent Properties'. The main area contains two sections: 'Blob Transfers' and 'Command Audit Log'. 'Blob Transfers' has 'Blob Command Number of Threads' set to 2 and 'Blob Command Prefetch Size' set to 6. 'Command Audit Log' has 'Maximum # Log Entries' set to 10000 and 'Maximum Time to Live (Minutes)' set to 5. 'OK' and 'Cancel' buttons are at the bottom right.

Performance	
Blob Transfers	
Blob Command Number of Threads:	2
Blob Command Prefetch Size:	6
Command Audit Log	
Maximum # Log Entries:	10000
Maximum Time to Live (Minutes):	5

Blob Command Number of Threads	This setting should only be modified at the instruction of the Peer Support Team.
Blob Command Prefetch Size	This setting should only be modified at the instruction of the Peer Support Team.

Maximum # Log Entries	The maximum number of command audit log entries to hold in memory cache.
Maximum Time to Live (Minutes)	The maximum number of minutes that audit log entries will be retained for before purging from the in memory cache.

5. VM Options



The first option on the page allows for the ability to tune the maximum amount of system memory that the Agent service will use on the server where it is installed. The maximum amount is 1.5GB. We strongly recommend that this value not be set below 512MB.

The text field below this option should only be used under the direction of the Peer Support Team.