FolderMaestro File Collaboration Help Manual

Updated Friday, July 11, 2008

Table of Contents

FolderMaestro File Collaboration 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 the help much more useful.

Trademark Information and Copyright

Getting Started

The topics in this section provide some basic information about FolderMaestro File Collaboration, what it is for, what you can do with it and how to install it.

Solutions Overview

FolderMaestro File Collaboration is an enterprise level 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, and 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.

FolderMaestro File Collaboration Key Features

FolderMaestro File Collaboration Features	Standard Edition
Maximum number of running file collaboration sessions.	**Unlimited**
Maximum number of unique participating hosts across all running collaboration sessions	**Based on licensed amount**
Does not require device driver install	✓
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: Propagates native file locking in real time over any distance.	✓
Transparency: Your users and applications keep using the exact same files, in the exact same manner.	✓
Efficient: Binary delta encoding which only sends 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 wildcard 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	✓
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 a file on a target host	✓

Requirements

1. All participating hosts must be highly available file servers, and accessible across highly available and stable networks.

2. FolderMaestro File Collaboration 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, 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.

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 directly. 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 FolderMaestro Agent must be installed on all participating hosts, and each host machine must be running Windows 2000 or Windows 2003 Server with the latest service packs and 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. Also Windows 2008 server is not currently supported at this time.

5. The FolderMaestro 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 Hub must be installed on a highly available Windows 2000 or Windows 2003 server with at least 2GB or RAM, and must have1GB of RAM dedicated to the Hub and Broker applications. This is the default and recommended configuration, but the amount of RAM can be reduced or increased via custom configuration.

7. All participating hosts must have network access to the machine where the Broker is installed, which by default will be the same machine where you installed the Hub. You will also need to configure the FolderMaestro Agent to connect to the Brokers host name or IP Address, and allow firewall access to the configured port, which by default is 61617. You will also need to allow access from all participating hosts to port 8181 of the machine that the Hub is running on.

8. The FolderMaestro File Collaboration software is intended to be installed and maintained by a qualified System Administrator, and not a typical end-user.

Terminology

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

File Collaboration Session	A communication session made up of 2 or more hosts, each with a designated root folder of files that are to be shared or collaborated. 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.
File Access Event	An event that is triggered from opening or closing of a file.
File Change Event	A event that causes a file to be changed in some way e.g. file modify, file delete, file rename, file attribute change, etc.
Quarantined File	A file that has been placed in the quarantine file list because some sort of lock conflict or other error occurred.
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.
FolderMaestro Applet ("Applet")	A solution built for the FolderMaestro framework. An Applet is a distributed application, containing parts, some of which function at a focal point called the Hub and others invoked at remote points designated by Agents.
FolderMaestro Hub ("Hub")	The focal software component where Applets are installed, configured and run. The Hub can host Applets of various types and is where the centralized solution components function. The FolderMaestro Agent is invoked by Applets' distributed components with messages sent through the Broker.
FolderMaestro Broker	The central messaging system of the Applet framework. The

("Broker")	Broker serves to connect the Hub and the Agents, forming a FolderMaestro "network" that can be cast over local- or wide-area network via TCP/IP. A FolderMaestro environment will deploy 1 or more Brokers.
FolderMaestro Agent ("Agent")	A lightweight distributed component that is used to perform operations on the host on which it is running. A FolderMaestro environment will typically contain several Agents, one per participating networked host. Agents invoke the distributed portions of a Applet, and will often run near resources of interest, such as collaborated files. The Agent is designed to be purposed across the entire FolderMaestro solution suite, and will normally be directed to perform functions with messages received from Applets through the Broker.

Architecture Overview

Introduction

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

FolderMaestro File Collaboration Architecture

FolderMaestro solutions, also known as "Applets", have local and remote characteristics that form the basis of a distributed application framework. A FolderMaestro installation is composed of 3 primary components:

1. Hub

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

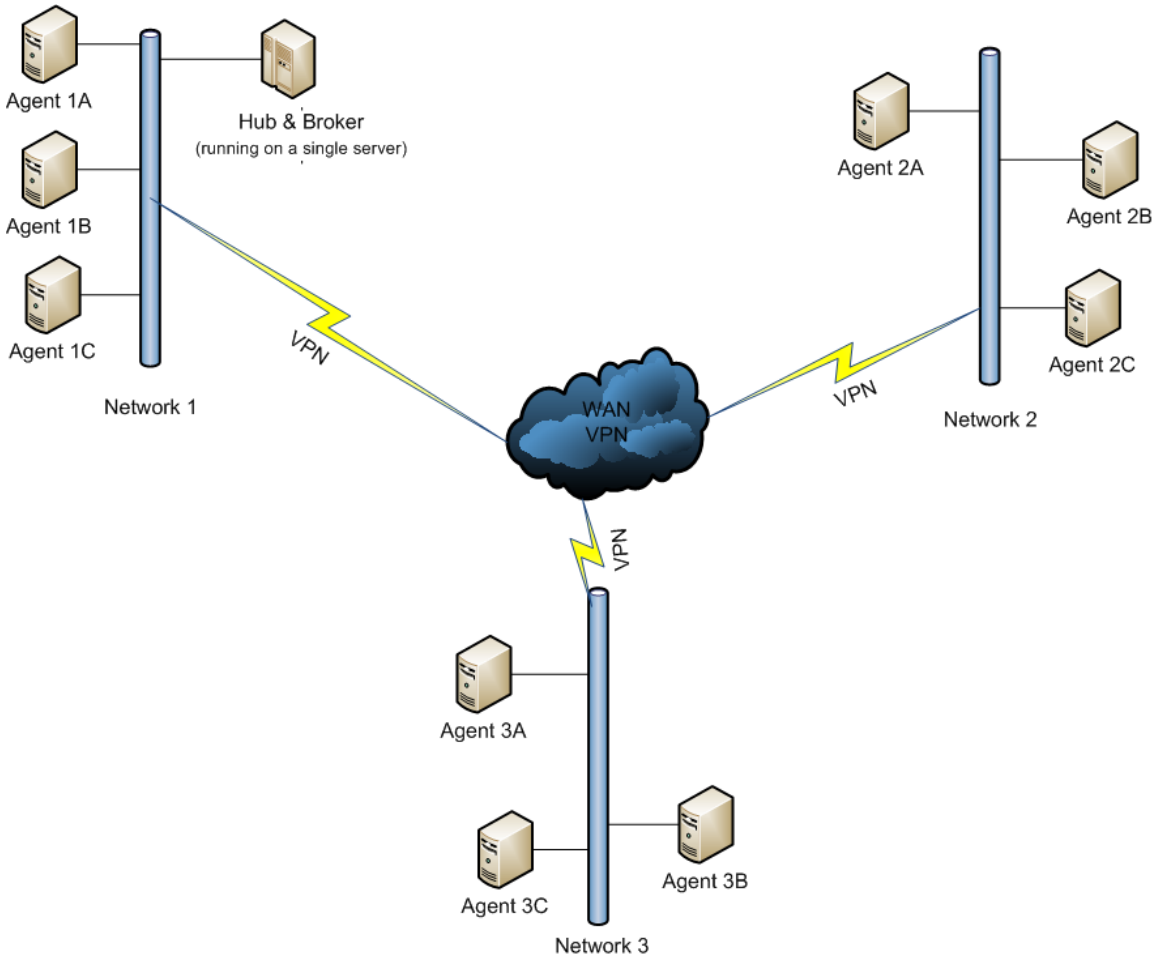
2. FolderMaestro Agent

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

3. Broker

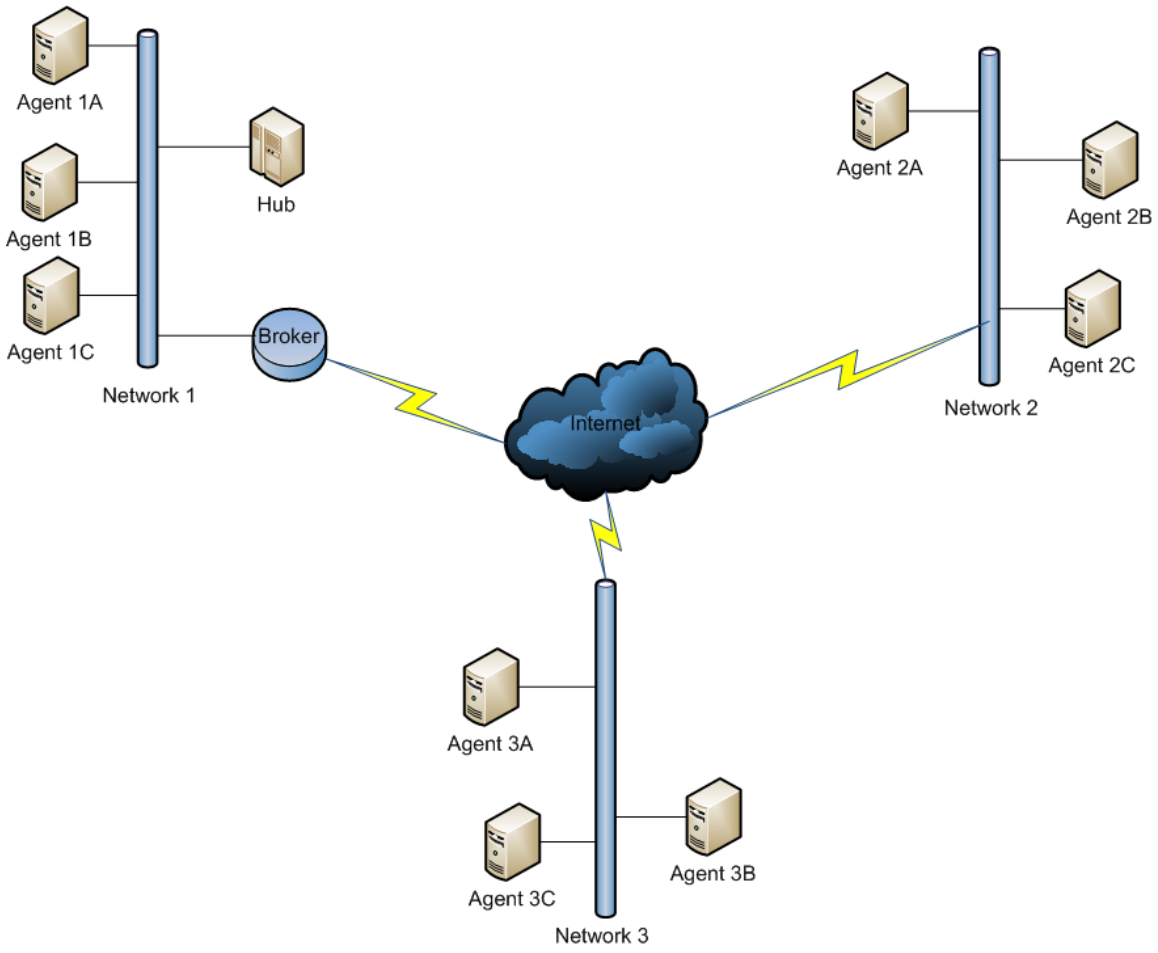
   The Broker makes up the central messaging system that supports FolderMaestro applications. The Broker provides the core communication facility that connects the Hub and Agents in a FolderMaestro environment. Applets running at the Hub interact with the participating Agents through the Broker.

Typical deployment where Hub & Broker and all FolderMaestro Agents are on separate networks connected via a VPN. This deployment also has the Hub & Broker running on the same machine.



Advanced deployment where there are 3 distinct networks located at 3 disparate locations connected via the Internet.

Hub is located on network 1, and a Broker is installed on the edge of each network for performance reasons, with multiple agents located on all 3 networks.



How File Collaboration Works

Introduction

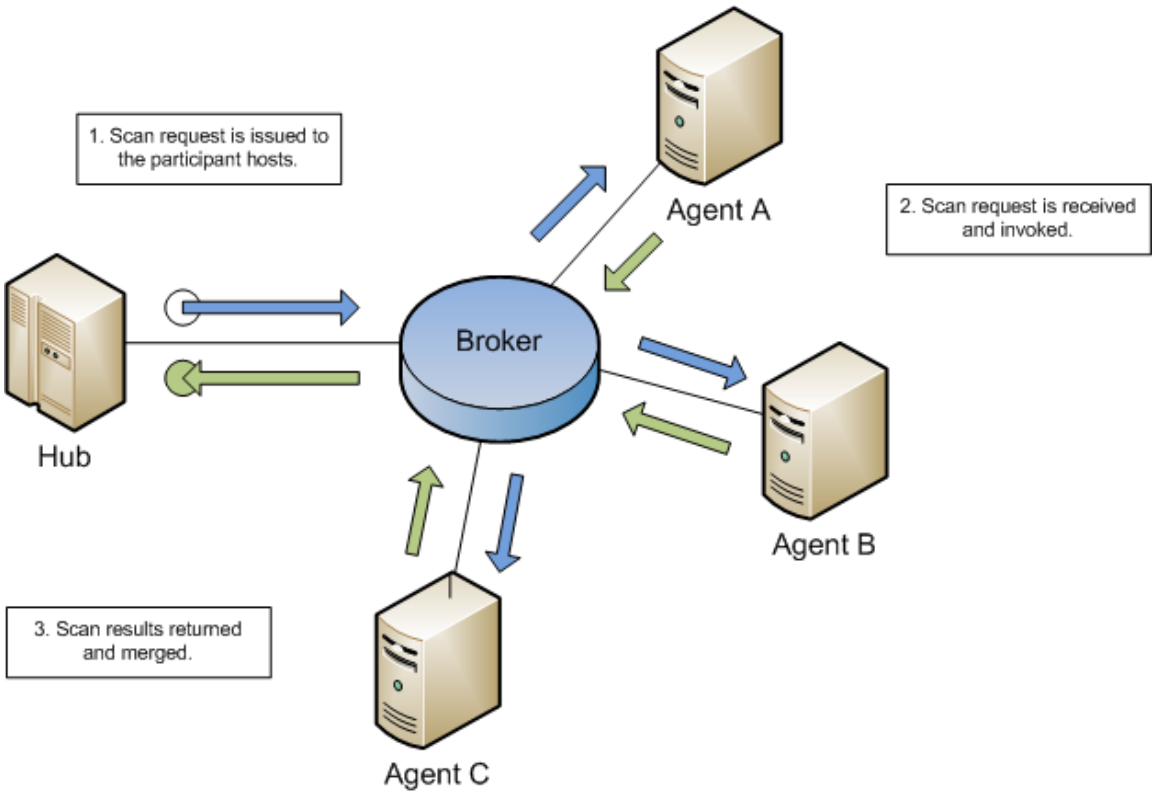
File Collaboration was built as a FolderMaestro solution and complies with Applet conventions. Common to all FolderMaestro solutions is the notion that some functionality is centralized while others are distributed.

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 FolderMaestro Agent, presumably on each participant host storing files of interest. The lock manager is a centralized component running at the Hub that is notified of opening files.

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

Step 1: Session Start

At the start of a file collaboration session, the Applet issues a request to scan each participant host's Root Folder recursively for file content. The scans are performed at the Agents and results are dispatched back to the Hub for merging and file conflict resolution. Transfers are then issued to the Agents to synchronize their hosts' folders. Once complete, the Agents are directed to start detecting access and change events on their respective hosts.

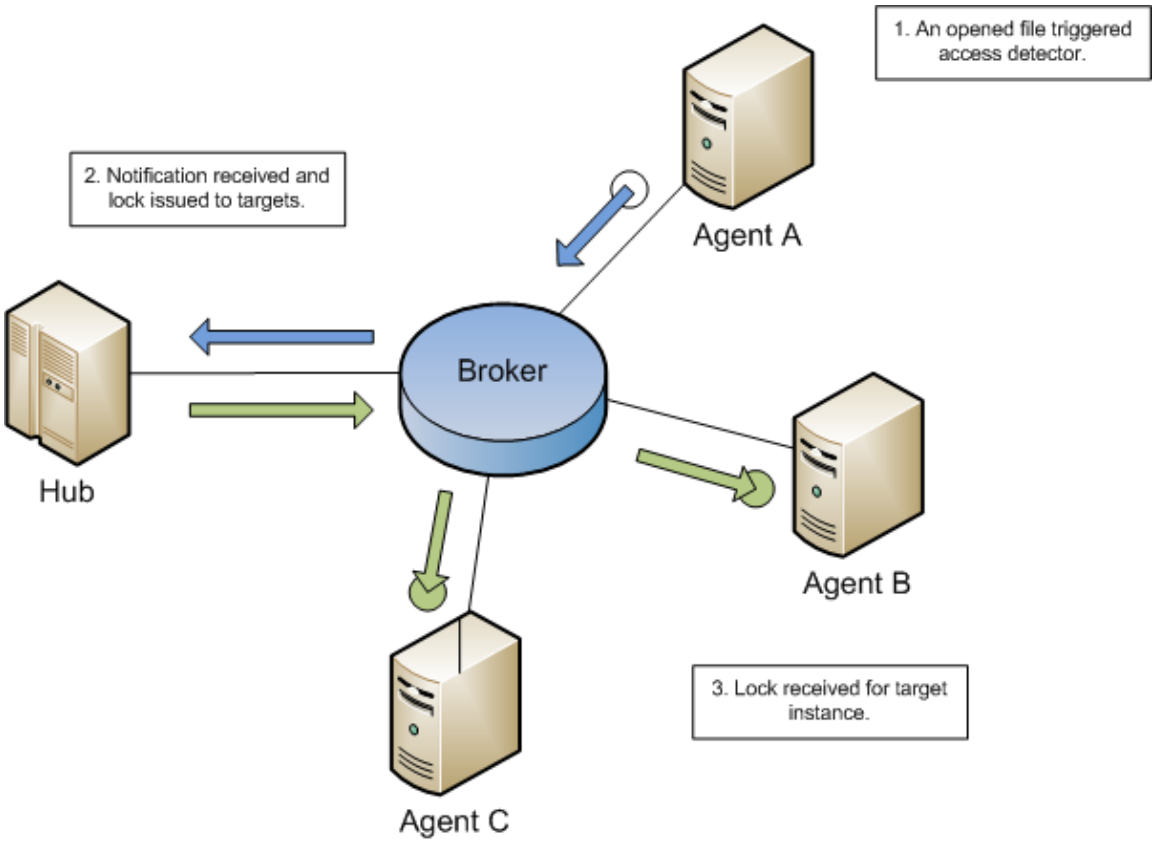


Step 2: File Lock

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 Applet at the 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 1 source instance is allowed for any given file in a session.

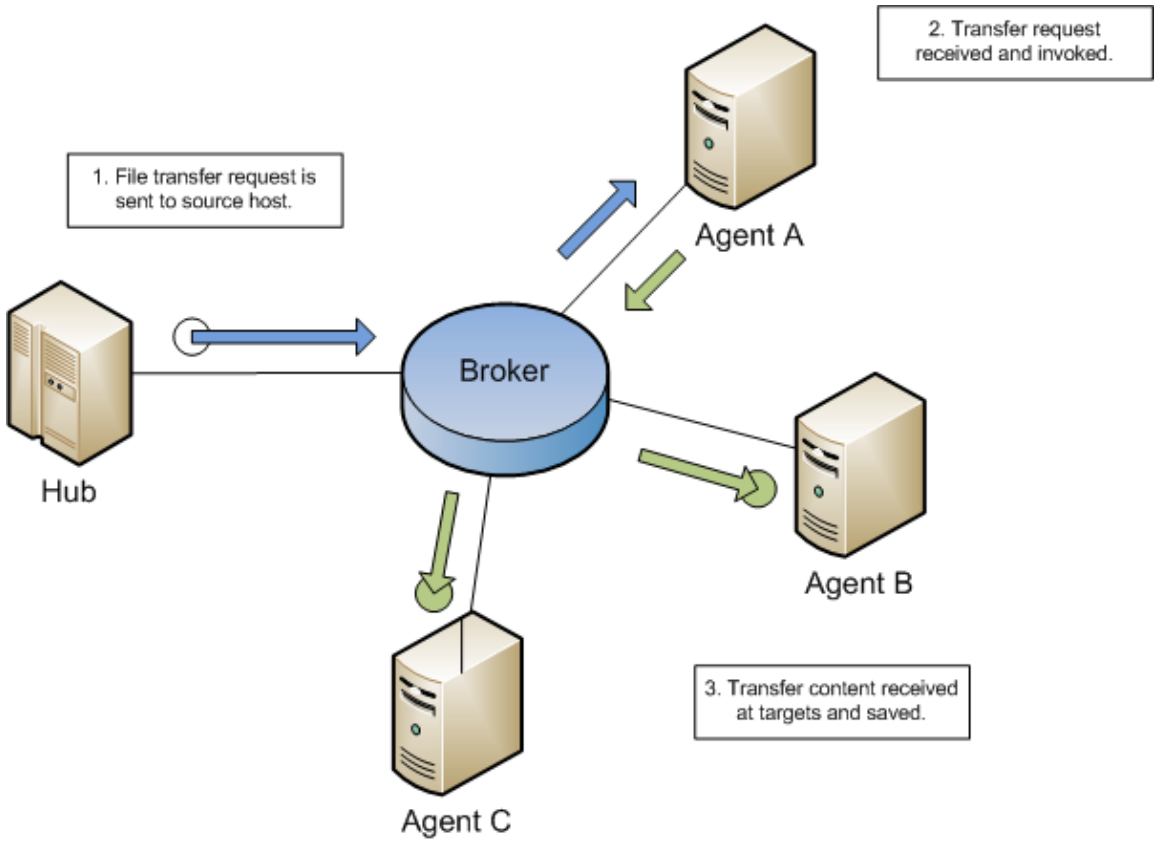
Note: If a file is opened in read-only mode, or if the application that opens the file does not acquire a read-write lock on the file (e.g. NotePad, WordPad, etc.), the lock will not be propagated to the Target Hosts.

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 Hub.



Installation & Configuration

FolderMaestro File Collaboration can be installed in numerous ways based on your needs and your environment. FolderMaestro File Collaboration installation consist of two separate installers:

1. FolderMaestro File Collaboration Hub & Broker installer: (Downloaded from our website).
2. FolderMaestro Agent installer. (Available via http download after Hub installation).

Hub & Broker Installation

Both the Hub and Broker are packaged with the main FolderMaestro File Collaboration installer, and by default, will be installed on the same server.

Basic Requirements

1. The Hub must be installed on a highly available Windows 2000 or Windows 2003 server with at least 2GB or RAM and must have1GB of RAM dedicated to the Hub and Broker applications. This is the default and recommended configuration, but the amount of RAM can be reduced or increased via custom configuration.
2. All installed FolderMaestro Agents must have network access to the server the Broker is installed on, and any firewalls must be configured to allow access for ports 61616 and 8181
3. See the Requirements section for more detailed requirements.

Software Installation & Launching

1. Run the FM-Hub_Installer.exe and follow all instructions.
2. After installation finishes, both the Hub and Broker will be installed. The Broker will automatically be installed as a running Windows service and set to auto-start, and the Hub will need to be started as a normal Windows application.
3. Start the Hub by launching the PLHub.exe executable located in the base installation directory. If the Broker is up and running as a background service then the Hub should successfully start. If not, please make sure the Broker is running as a Windows service via Windows Service Panel (services.msc).

Secure Encrypted SSL Connections

By default, the Hub and Broker will be installed on the same host machine which does not require secure SSL connection between each other. To enable a secure SSL connection between the Hub and Broker, open the **Hub.properties** file located in the Hub\plugins\com.compositeideas.peerlink.ori_1.1.0 directory relative to the installation directory in a text editor, and change the providerURL line below from tcp to ssl and 61616 to 61617, save the changes, then restart the Hub.

From: providerURL=failover:**tcp**://localhost:61616

To: providerURL=failover:**ssl**://localhost:61617

Running a Hub from a private NATed IP Address

If you are running the Hub on a machine with a private IP Address behind a router or firewall using NAT, then you will need to edit the Hub.properties file and specify the public IP Address of the machine. Open the **Hub.properties** file located in the Hub\plugins\com.compositeideas.peerlink.ori_1.1.0 directory relative to the installation directory in a text editor, and add the machines IP Address to the `classServer.hostname=` line, e.g. classServer.hostname=192.168.1.1

Uninstalling

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

FolderMaestro Agent Installation

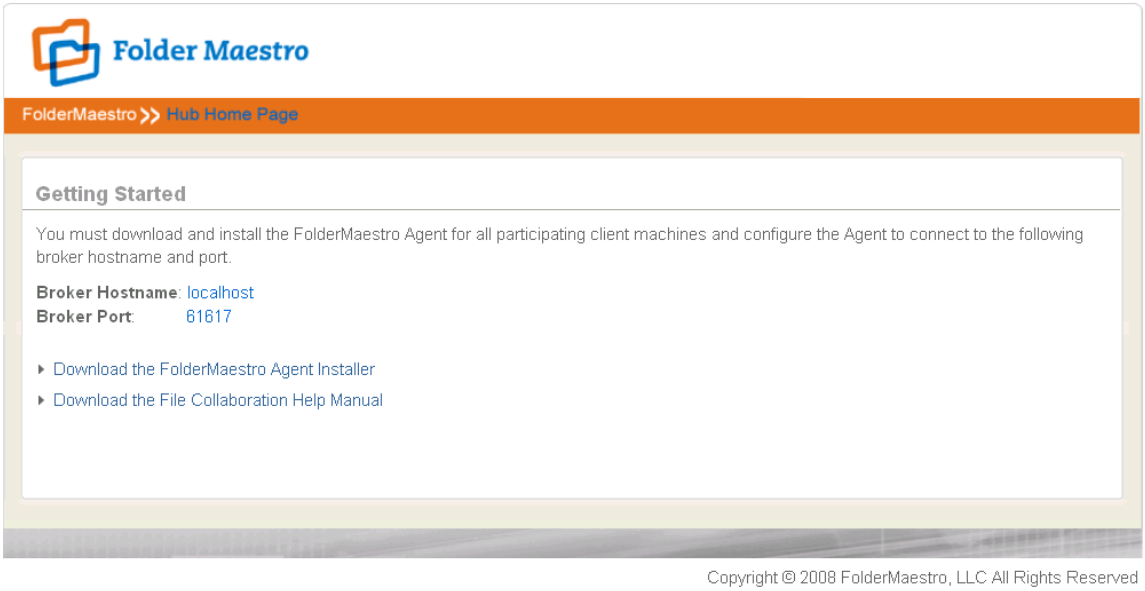
You will need to install a FolderMaestro Agent on each server you plan to include in any of your file collaboration sessions.

Basic Requirements

1. Must be installed running Windows 2000 or Windows 2003 Server with the latest service packs, and acting as a file server where the Root Folder is located on a locally attached storage device.
2. The server that the FolderMaestro Agent is installed on must have direct network access to the server that the Broker is installed on, and any firewalls must be configured to allow access for ports 61616 and 8181 to the Broker server.
3. The FolderMaestro 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. You will need to download the FolderMaestro Agent installer directly from the running Hub via Http using a web browser. Make sure that the Hub is running and type the following URL in from the Hub server http://localhost:8081/ or http://HubIPAddress:8081/ from the server where you are installing the FolderMaestro Agent on (substitute IP Address or computer name of Hub server for HubIPAddress). After the Hub home page is displayed, click on the "Download the FolderMaestro Agent Installer" link. If HubIPAddress:8081/ does not work from the server where you are installing the FolderMaestro Agent, then a firewall may be blocking port 8081. If this is the case then you should download the FolderMaestro Agent installer directly from the Hub server via /localhost:8081/ and then transfer the executable to the remote server.
2. Run the FM-Agent_windows.exe installer and follow all instructions.
3. During installation you will need to specify the Broker Host Name (computer name, domain name or IP Address) of the server where the Broker is running, as well as the configured TCP/IP port number. The host name and port number of the Broker is indicated on the Hub home page where you downloaded the FolderMaestro Agent from (see below).
4. After installation finishes the FolderMaestro Agent will be installed as a Windows service. You will need to verify that the FolderMaestro Agent is running, and that it was able to successfully connect to the Broker. You can do this by opening Windows Service Panel (services.msc) and making sure that the "FolderMaestro Agent Service" is started.
5. Make sure that the FolderMaestro Agent was able to successfully connect to the Broker by going to the FolderMaestro Agent installation folder and opening the output.log text file and make sure that **"Ready."** is displayed on the first line.



Secure Encrypted SSL Connections

By default, the FolderMaestro Agent is installed with SSL encryption enabled, where the FolderMaestro Agent connects to the Broker through a secure, encrypted connection. If you are running FolderMaestro File Collaboration on a secure LAN or via a corporate VPN, you might want to disable SSL to bolster performance. To disable SSL connection, open the agent.properties file located in the FolderMaestro Agent installation directory in a text editor, and change the providerURL line below from ssl to tcp and 61617 to 61616, save

the changes, then restart the FolderMaestro Agent Windows service.

From: providerURL=failover://(**ssl**
://BROKER_HOSTNAME:61617)?jms.prefetchPolicy.all=1

To: providerURL=failover:**tcp**://BROKER_HOSTNAME:61616?jms.prefetchPolicy.all=1

Where BROKER_HOSTNAME is the IP address or host name of the machine that the Broker is running on.

Uninstalling

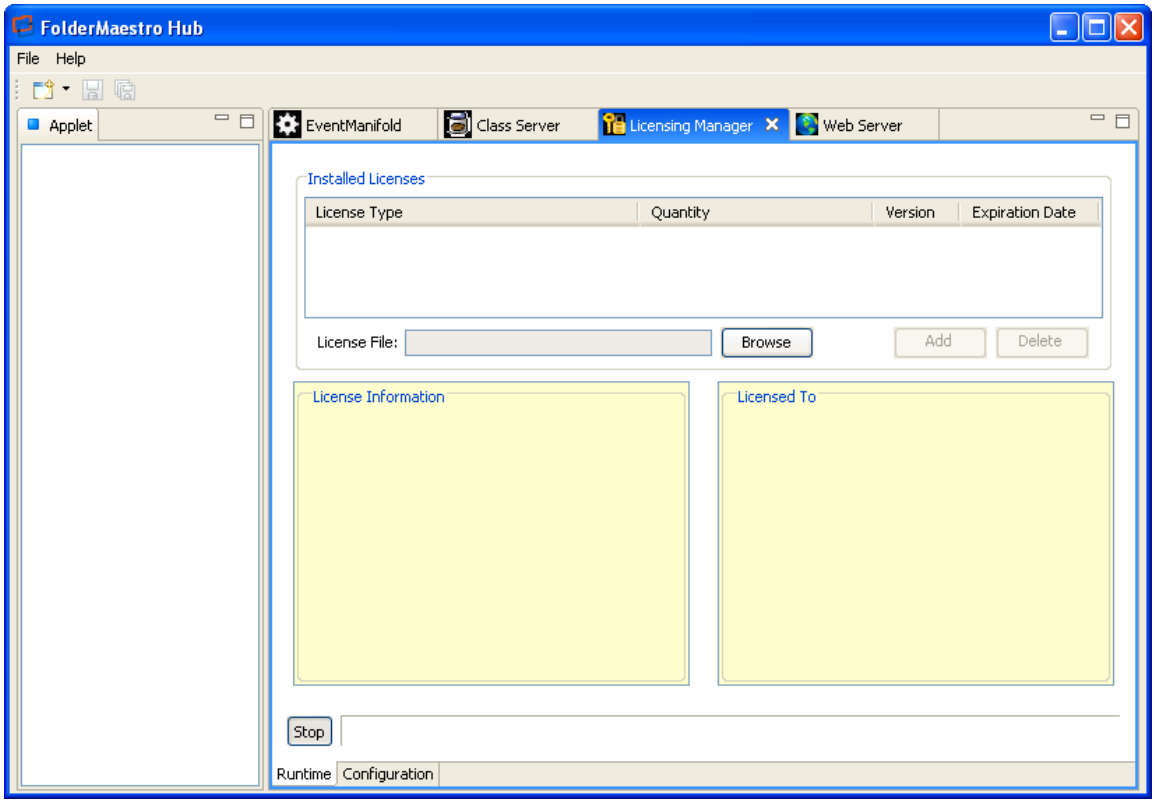
FolderMaestro Agent ships with an uninstaller for the environment it is running in. Please use the standard platform specific method for removing programs/applications to uninstall the **FolderMaestro Agent**.

Licensing

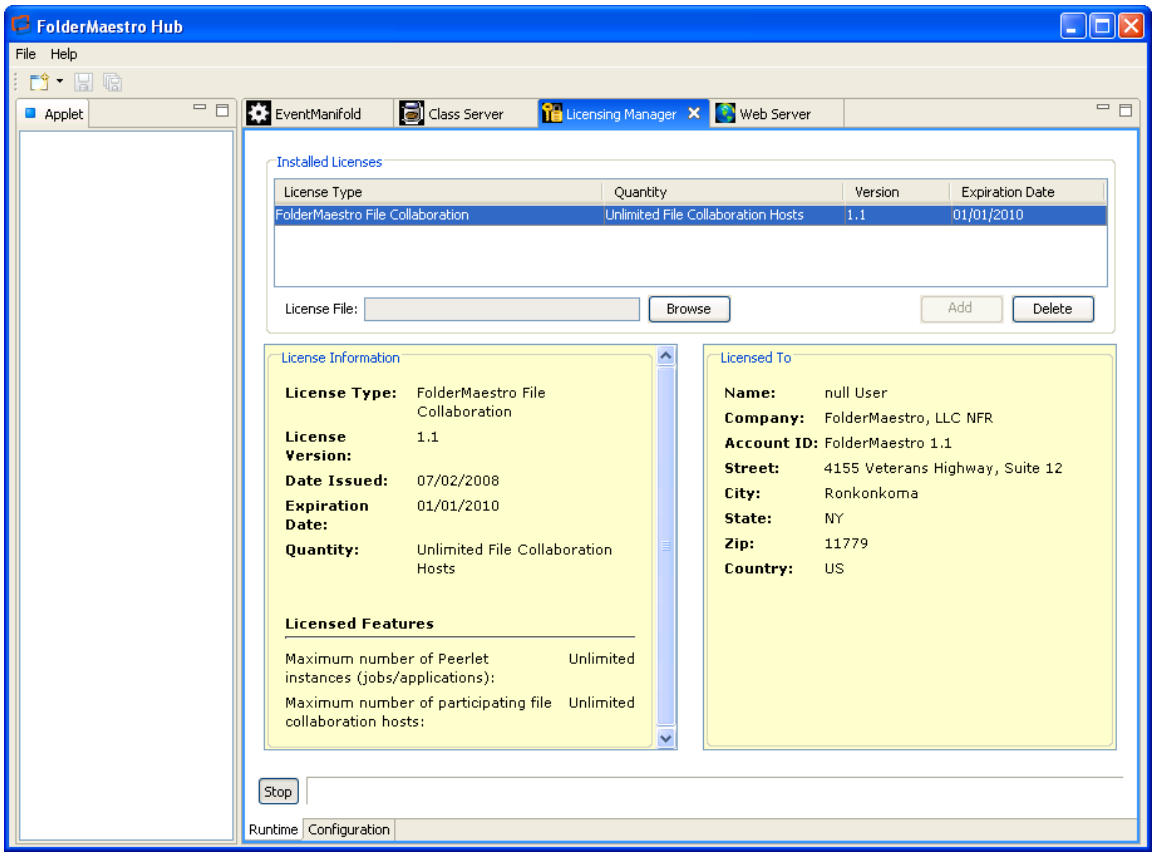
FolderMaestro File Collaboration is licensed by the number of unique participating hosts for all running file collaboration sessions.

Installing or Upgrading a License File

After purchasing or requesting a trial download of FolderMaestro File Collaboration, you will receive a license file that you purchased or requested a trial of. To install a new license file or upgrade an existing license select the **License Manager** Applet tab in the Hub.



Click the browse button and select the new license file to install. Once selected, click the **Add** button to install the license file. If a license already exists for the same File Collaboration Applet, 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 Installed Licenses table along with licensed quantity and an expiration date (if applicable). You will now be able to configure and run file collaboration sessions.

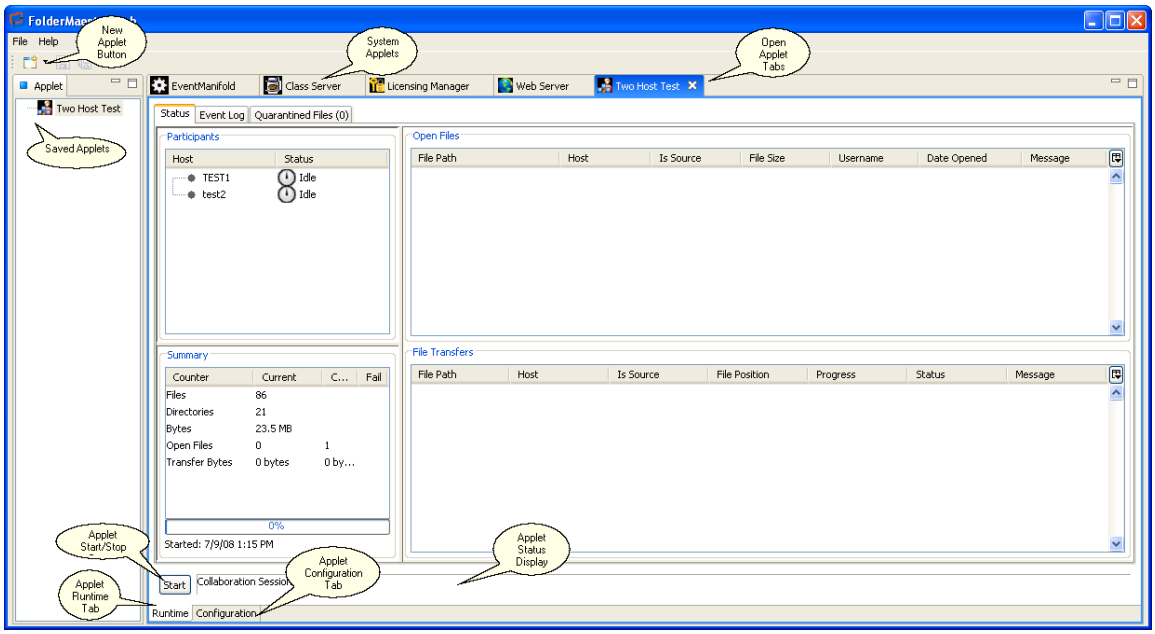


The Hub User Interface

The Hub is a container for configuring and deploying FolderMaestro Applet applications. The Hub graphical user interface enables you to create, view, edit and delete file collaboration sessions, as well as view runtime information for running Applets.

Main View

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



The **Hub Main View** is made up of the following components:

Configured File Collaboration Applets	This is a list of saved File Collaboration Applets that can be opened and started
Applet Start / Stop Button	The button allows you to start and stop any opened Applets
Applet Status Display	Displays information status related messages when the Applet is running
New Applet Button	Opens a drop down list of available Applets to create.
Open Applet Tabs	Selecting any of these tabs switches to the Applet Editor and Runtime Views for the select Applet.
System Applets	The following are system Applets that are automatically started and **SHOULD NOT** be edited or closed: 1. Event Manifold 2. Class Server 3. Web Server 4. Licensing Manager
Applet View Tabs	Consists of the following two tabs: 1) Runtime Tab - Displays Runtime Panel and other application specific controls and views 2) Configuration Tab - Displays a Applets configuration panel used for editing properties.

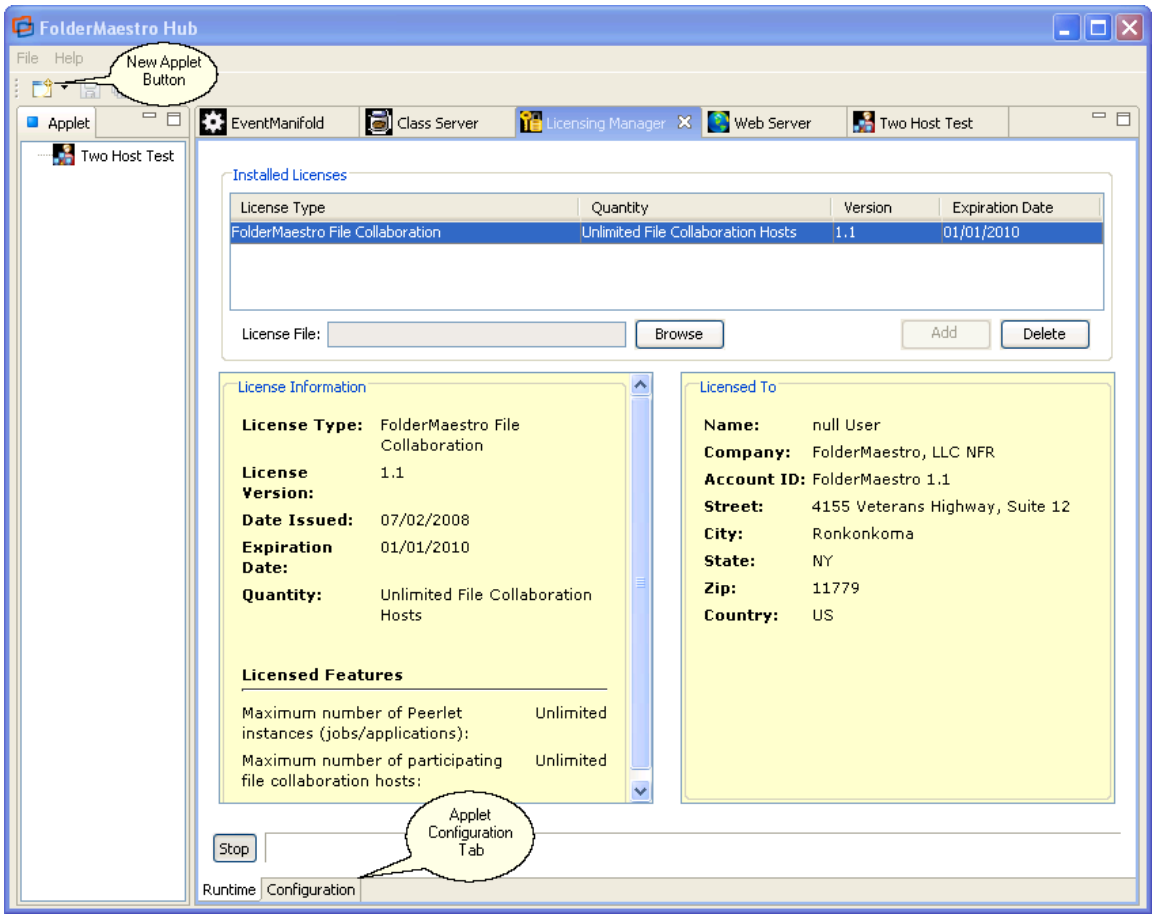
Creating a File Collaboration Session

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

Overview

File Collaboration Sessions are created using the Hub. To create a new file collaboration session, click the Create New Applet button in Hubs toolbar, or you can select the **New** menu item from the **File** menu. A drop down list of all installed Applets will be displayed. Selecting the "File Collaboration" option will open a new file collaboration session Applet Configuration Panel, and the Applet Configuration Tab will be selected.

You can edit an existing file collaboration session by double clicking on a file collaboration session in the Saved Applets list, which will open the file collaboration session Applet configuration Panel and the Applet Configuration Tab will be selected.



Configuring a file collaboration session consists of the following steps:

Step 1 - General Settings

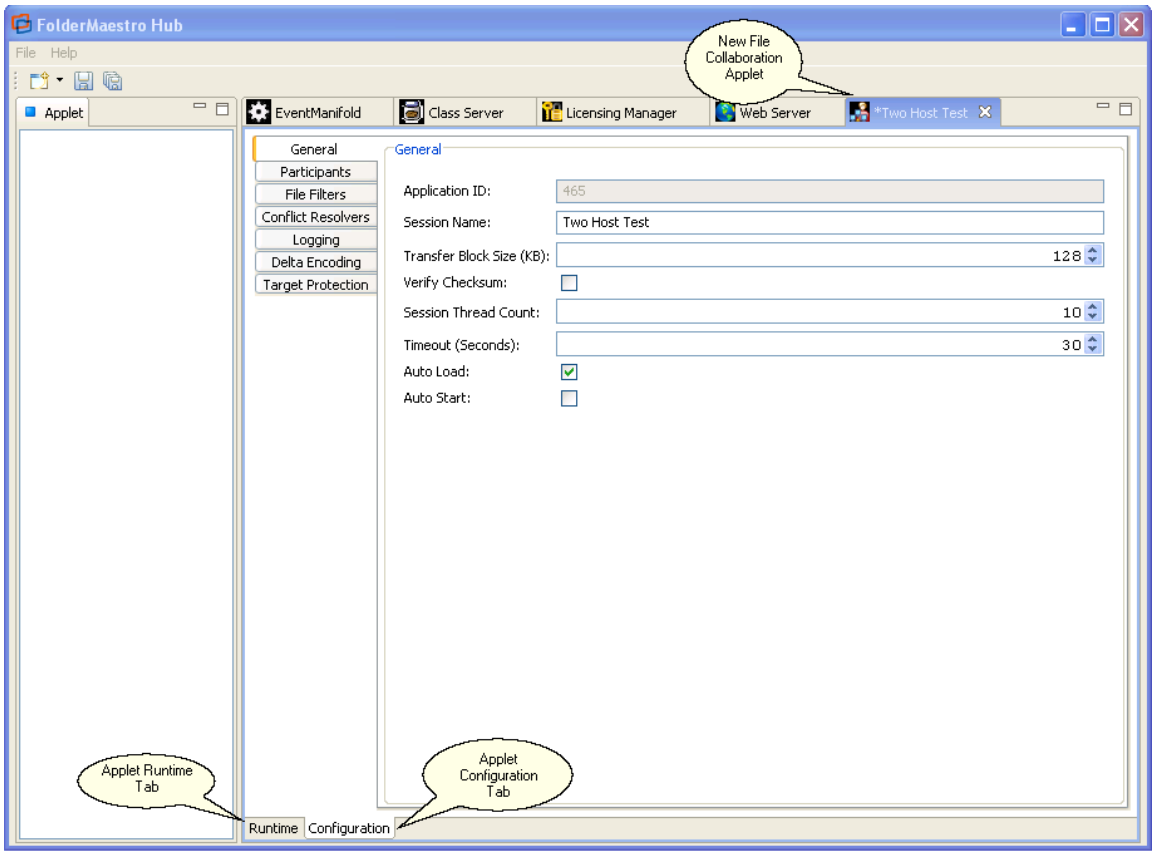
Step 2 - Host Participants & Folders Settings

Step 3 - File Filters Settings

Step 4 - File Conflict Resolver Settings

Step 1 - General Settings

After clicking the Create New File Collaboration Session button, a new File Collaboration Applet is created in the open Applet tabs section called **File Collaboration**.



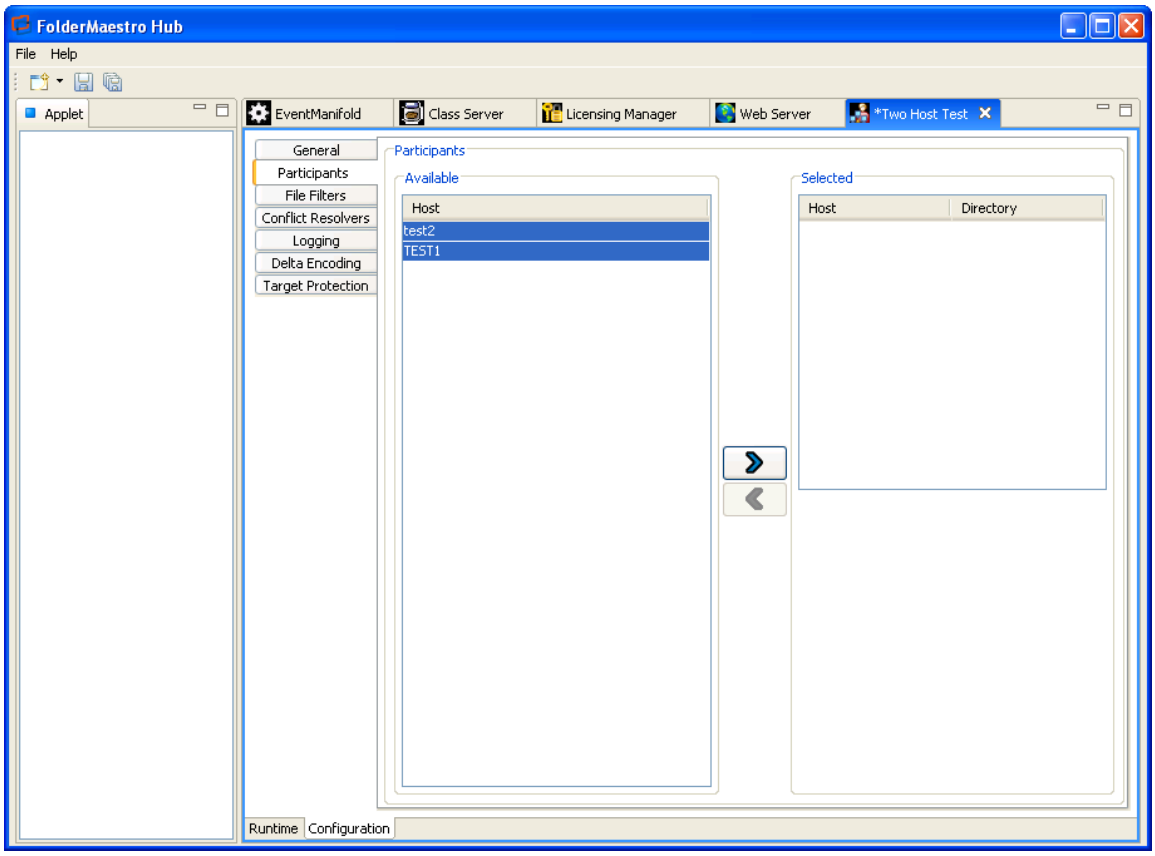
Below are a list of general fields and their descriptions:

Application ID	Unique system generated application identifier
Session Name	Description of this file collaboration session. 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 Broker and agents.
Verify Checksum	If checked then source and target checksums will be calculated and verified for all file transfers. There is a small overhead associated with verifying checksums and we recommend only enabling this options for initial testing or if you suspect files are being corrupted some how.
Session Thread Count	Number of concurrent file operations that may be performed before queuing occurs.
Timeout (Seconds)	Number of seconds to wait for a response from any host before performing retry logic

Auto Load	If checked then this file collaboration session will be automatically loaded (but not necessarily started) when the Hub is started.
Auto Start	If checked then this file collaboration session will automatically be started when the Hub is started. **Note:** The Auto Load checkbox must be enabled for this option to work.

Step 2 - Host Participants & Folders

Next click on the **Participants Tab** of the file collaboration session configuration panel to configure which hosts will be participating in this file collaboration session along with each of the corresponding root directories for each of the hosts.

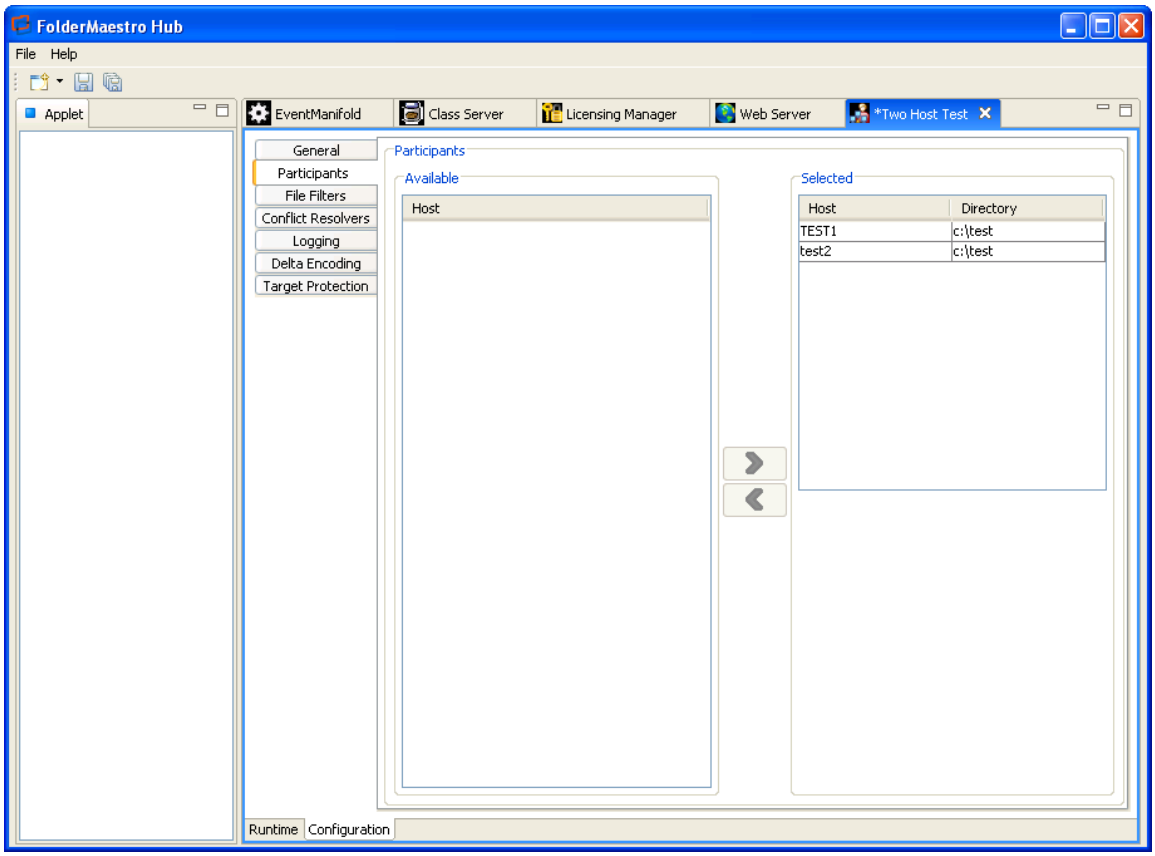


1. A list of all available hosts will appear under the Available Hosts table on the left. Available hosts are any host with a FolderMaestro Agent installed on it that has successfully connected to the configured Broker. The name that will be displayed is the computer name of the server that the FolderMaestro Agent is running on. If a particular host is not displayed in the list then try restarting the FolderMaestro Agent Windows Service on that host, and if it successfully connects to the Broker, then the list will be updated with the computer name of that host.

2. Select two or more hosts from the Available Hosts table and click on the arrow pointing to the right to add the hosts to the Selected Hosts 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.



NOTE: You can probably leave the rest of the configuration settings as their default values and move onto to Step 8 - Save Settings

Step 3 - 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 expression listed below.

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.

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.

Internal Filter Exclusions

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

Zip Files
*.zip

Zip files are currently being excluded from collaboration since Windows Explorer shell extensions interferes will the collaboration process.

Configuration

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

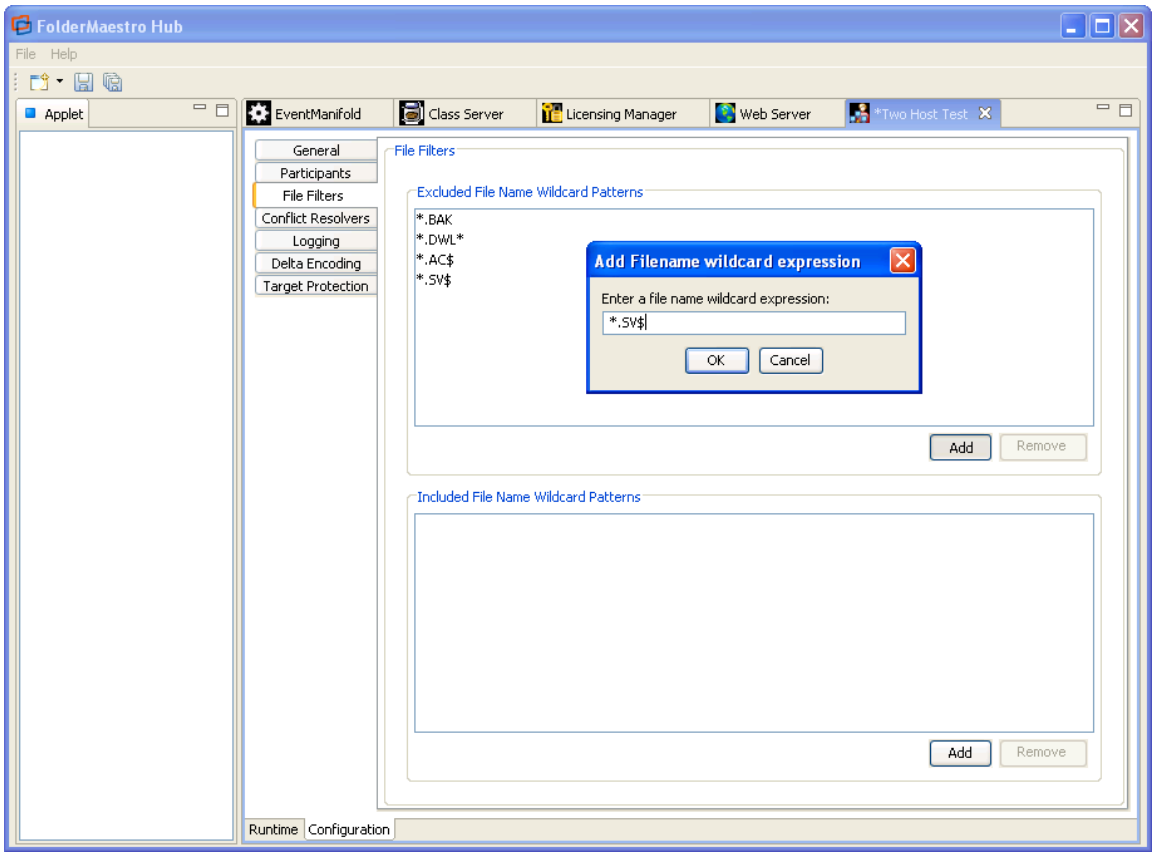
In general, you will want to **exclude all temporary files** created by the applications you use so they are not propagated to the targets hosts. For example, AutoCAD applications should add the following expressions to the Excluded File Name filter table:

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

1. Click the Add button under the Excluded File Name Wildcard Pattern table and enter *.AC$ and then click OK.

2. Do the same thing and add *.SV$, *.DWL* and *.BAK

Your AutoCAD temporary file exclusion filter is now created and all files ending in *.SV$ or *.AC$ or *.DWL or *.BAK will be excluded from collaboration.



Step 4 - File Conflict Resolvers

Overview

Conflict resolution is a key feature of file collaboration that is in effect at the start of a session. When a file collaboration session 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 the participants' content. All files found under the designated folders are subject to collaboration, except for those excluded by filtration (see Step 3 - File Filters for more details).

A conflict occurs when a file path is found to exist on more than 1 host in a file collaboration session. 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 configuration, the file '\release-1.0\readme.txt' is found to be in conflict across 3 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.

Resolving a Conflict

The goal of conflict resolution is to designate 1 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 files' meta data 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 paths listed in the previous section, if our session was configured to resolve conflicts based on file-size and all instances of '\release-1.0\readme.txt' were the same size, then all 3 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 the source copies of conflict winners as well as files that are missing from participants.

Resolution Types

The conflict resolvers we currently provide are listed as follows:

Latest Modification Time	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.
Largest File Size	This resolver will select instances of a file based on size. The larger a file's size is, the more likely it will be a resolution candidate.
Prioritized Host	Resolution candidates will be selected based on the host on which a file resides. Hosts in a collaboration session may be assigned varying priority levels to influence the probability of candidate selection.

All the types listed above have the potential for producing multiple resolution candidates. A collaboration session can be configured with any 1 of the available conflict resolvers. If a resolver produces more than 1 candidate for a conflicted file, a winner will be selected arbitrarily.

A session may also be configured with multiple resolvers in a sequence. When any one resolver generates multiple selection candidates, the candidate set is supplied to the next resolver in the sequence to further reduce the candidate set. Conflicted files will be processed through resolvers until either a single winner is selected or the resolver sequence is exhausted. If multiple candidates arrive in the latter case, 1 will be arbitrarily selected.

Configuration

In most cases the default file conflict resolver which is by **Latest Modification Time** will suffice. If you would like to customize this, click on the **Conflict Resolvers** tab and follow the instructions below:

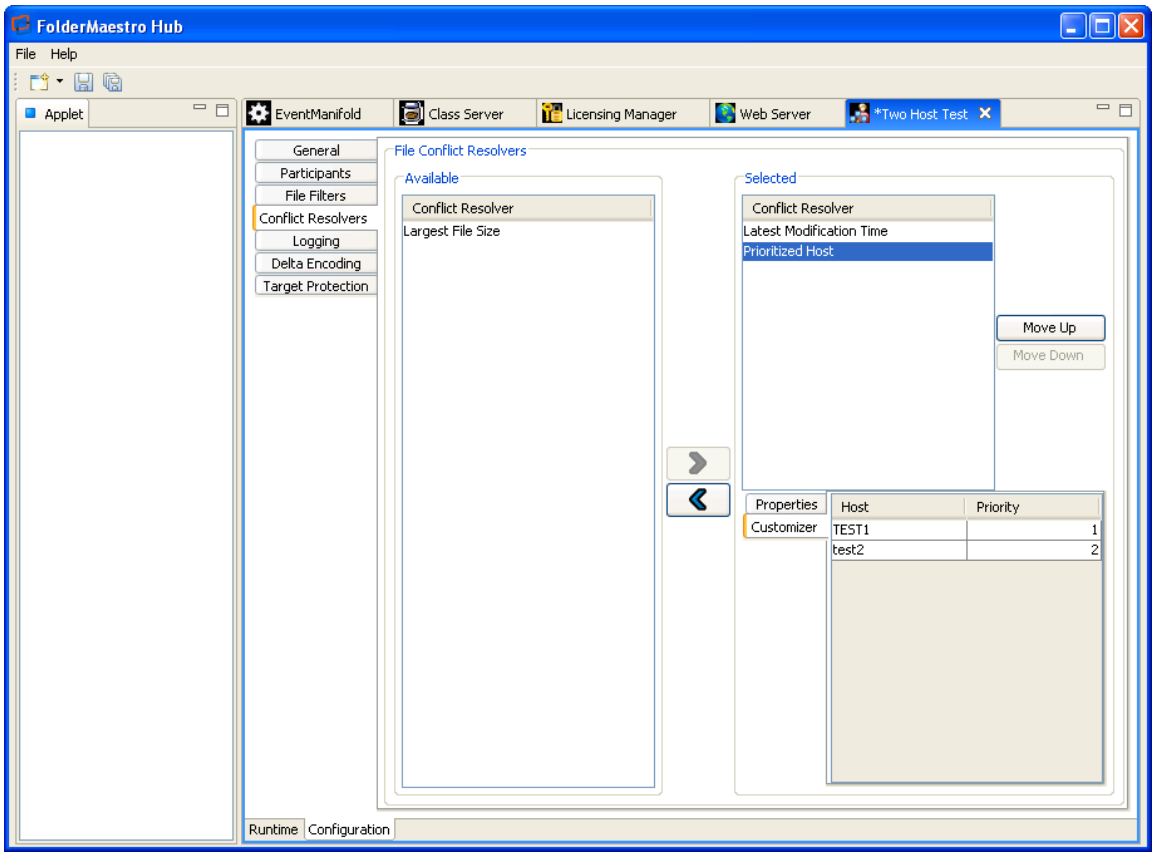
1. A list of currently selected file conflict resolvers will be displayed on the right and a list of other available one will be displayed in the left table.

2. Select one or more file conflict resolvers to add from the Available Conflict Resolver table, and click on the arrow pointing to the right to add the resolvers to the Selected Hosts table. To

remove a conflict resolver from the selected conflict resolvers table, select the resolver and press the Left arrow.

3. You can select the order of precedence by selecting a file conflict resolver from the Select list, and using the "Move Up" and "Move Down" buttons.

4. The **Prioritized Host** conflict resolver must be customized by using the property editor below the Select Conflict Resolver table and assigning each host a priority under the "Customizer" tab. You can also specify whether the priority is in ascending or descending order by selecting the "Properties" tab in the Property Editor.



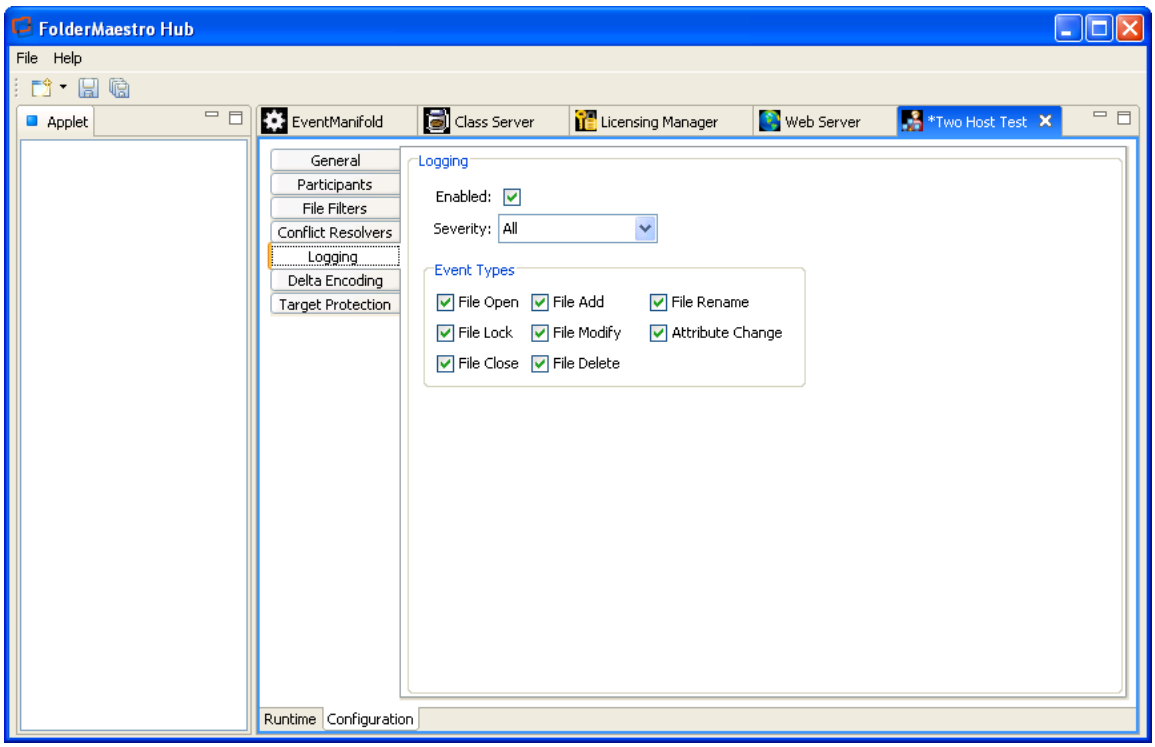
Step 5 - File Event Logging

Various types of file collaboration events can be logged to a log file and to the event viewer located on the **Runtime** tab of the File Collaboration Applet. Each file collaboration session will have its own file event log located in the **Hub\logs** folder of the installation directory and is uniquely identified by the system generated Application ID. Each log file will be named fc_event_log_AppId.txt, where AppId is the unique system generated ID visible under the General Settings tab of the Applet **Configuration Panel**. 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.

By default all file collaboration session file activity is logged, and for all severity levels. You can enable or disable file event logging as well as select the level of granularity on what to log by clicking on the **Logging** tab and configuring the following options



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: 1) All (Informational, Warnings, Error, Fatal) 2) 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

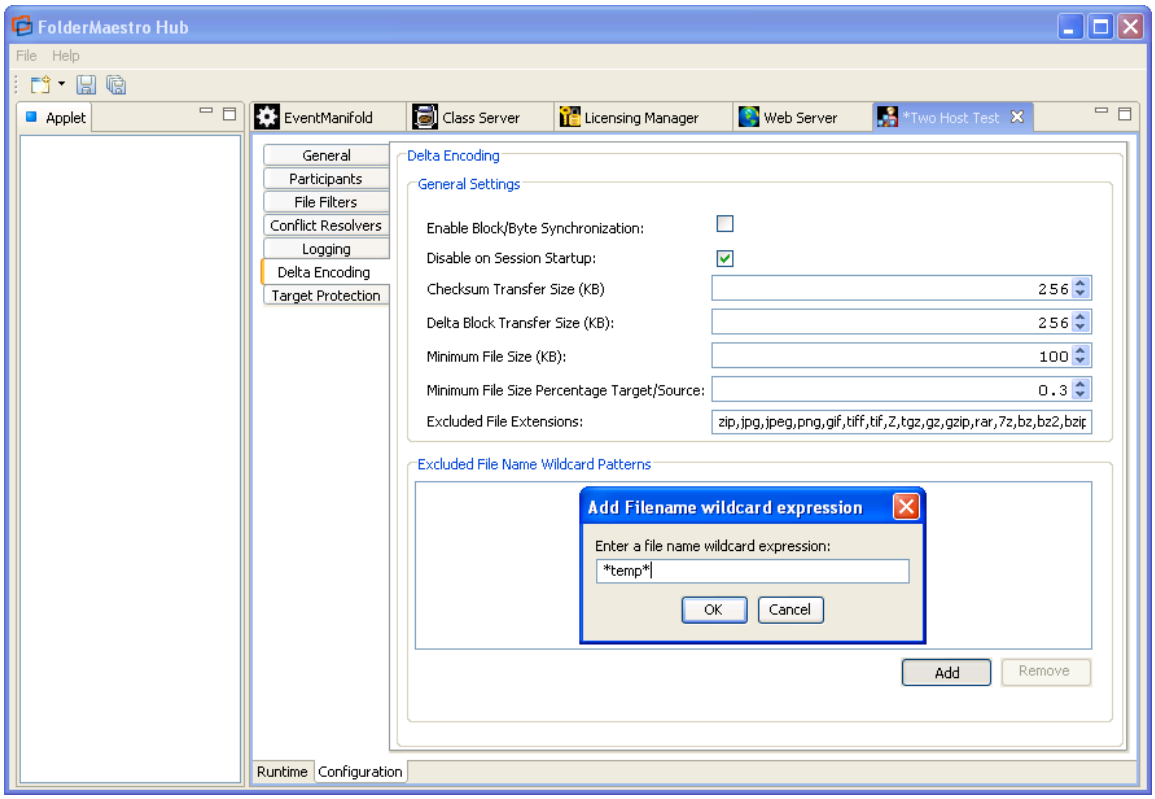
File Lock	A file lock was acquired on a Target Host by the File Collaboration Applet
File Close	A file was closed
File Add	A file was added to the Watch Set
File Modify	A file was modified in the Watch Set
File Delete	A file was deleted
File Rename	A file was renamed
Attribute Change	A file attribute was changed

Step 6 - Delta Encoding

Overview

Delta Encoding is a byte replication technology that enables block/byte level synchronization for a file collaboration session. Through the use of this feature FolderMaestro 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 a high volume LAN.

You enable Delta encoding on a per file collaboration session basis, and it generally affects all files in the Watch Set. You will only benefit from delta encoding for files that don't change much between file modifications, which includes most document editing programs.



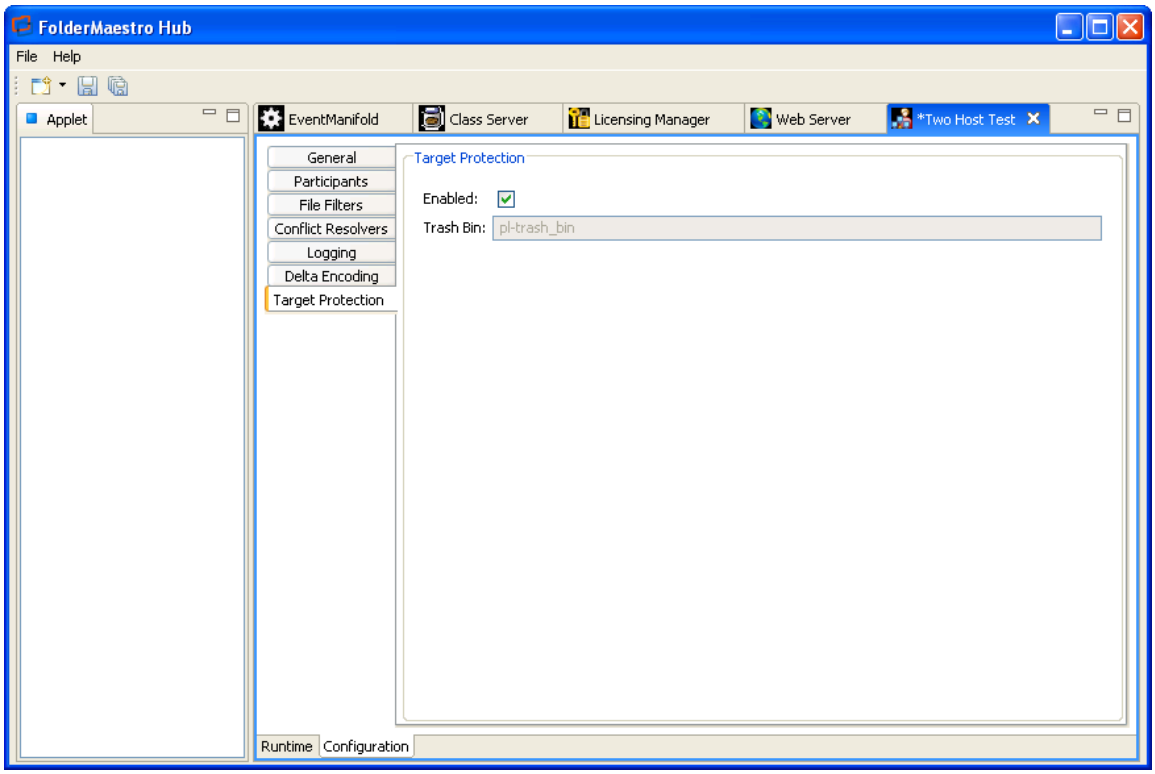
Below are a list of general fields and their descriptions:

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 encoding 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 in 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 in agents.
Minimum File Size (KB)	Minimum size of files in Kilobytes to perform delta encoding for. If 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. If a file extension matches any of these patterns then it will be excluded from delta. 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 Filters: wildcard expressions section for more information on specifying wildcard expressions.

Step 7 - 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 this option is enabled, then whenever a file is deleted or modified on the source host, and before the changes are propagated to the targets, a copy of the existing file on the target is moved to the FolderMaestro File Collaboration recycle bin.

The trash bin is located in a hidden folder named **pl-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.

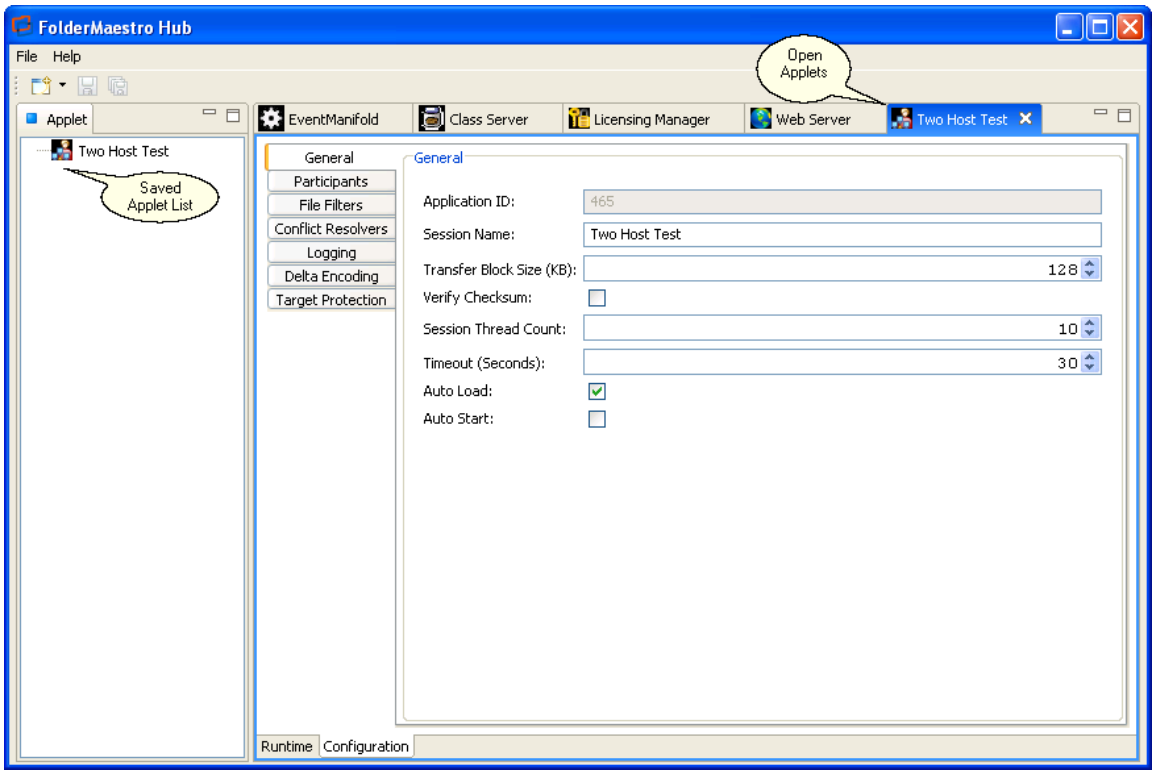


Below are a list of general fields and their descriptions:

Enabled	Enables target protection
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.

Step 8 - Save Settings

Once you have finished configuring the file collaboration session, you will need to save the changes by pressing **Ctrl-S** or selected **Save** from the **File** menu. After saving the configuration the file collaboration session configuration will be displayed in the Applet List in the left panel and you are now ready to start the File Collaboration Session Applet, see Running a File Collaboration Session for more information.

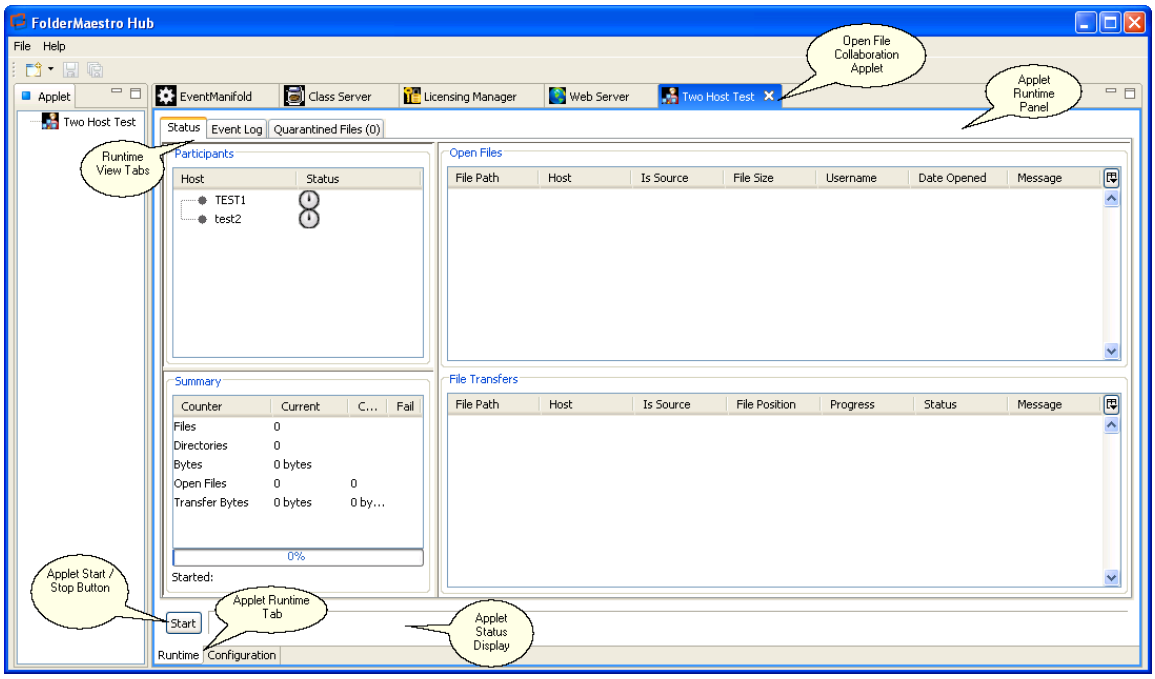


Running a File Collaboration Session

The topics in this section provide some basic information about starting, stopping and other runtime information for File Collaboration Session Applets.

Overview

File Collaboration Sessions are started and stopped from the **Applet Runtime View** of the opened File Collaboration Applet. Clicking the Runtime Tab will display the following **Runtime Panel View**.



The **Runtime Panel View** is made up of the following components:

Runtime View Tabs	These tabs allow you to select from the various Runtime Views e.g. Status, Event Log & Quarantined Files views. The illustration above is displaying the Status view.
Applet Start / Stop Button	The button allows you to start and stop the File Collaboration Applet
Applet Status Display	Displays information status related messages when the Applet is running
Applet View Tabs	Consist of the Runtime and Configuration Tabs

Starting & Stopping

Starting a File Collaboration Session

Before you start a file collaboration session for the first time, you need to decide how you would like the initial synchronization to be performed. There are basically two main options:

1. Have the File Collaboration Session FolderMaestro 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 Applet.

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 Session FolderMaestro.

After you have chose an option, press the **Start** button to begin collaboration session initialization. A file collaboration session must go through a serious of initialization steps before the collaboration session is started:

Initialization Process

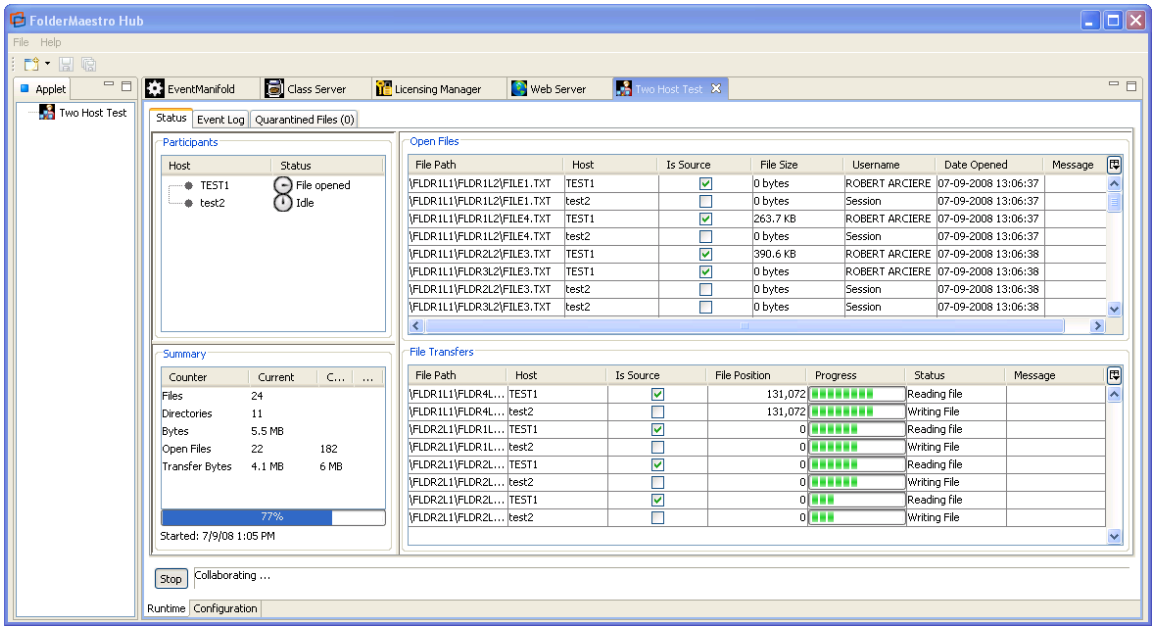
1. All participating hosts are contacted to make sure they are online and properly configured.

2. All of the configured Root Folders on the participating hosts are scanned, and the contents of all folders and files are sent back to the Applet.

3. The 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 based on the configured File Conflict Resolver settings for any detected file conflicts.

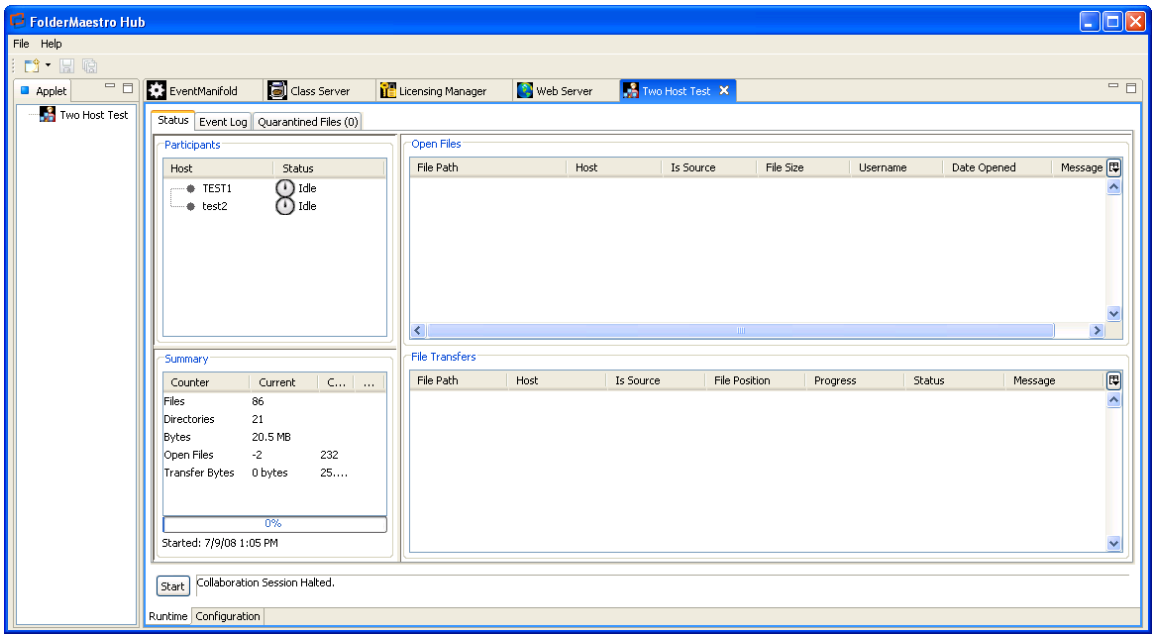
4. After the analysis is performed all files that need to by synchronized are copied to the pertinent host(s).

Below is a screen shot showing the initial synchronization process and the transferring of out-of-date files. Once all files are synchronized the collaboration session is started 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.



Stopping a File Collaboration Session

You can stop a file collaboration session at any time by pressing the **Stop** button. Doing this will shutdown the real-time file event detection and the File Collaboration Applet will wait for all currently running task to complete before shutting down e.g. file transfers in progress, etc.



Unavailable Hosts

Unavailable Hosts

FolderMaestro File Collaboration 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 during a file collaboration session, the host may be taken out of the file collaboration session if the host is unreachable within the configured timeout period specified in the General Settings. If no response is received during any file collaboration activity 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 and a FATAL event will be logged and the Host Participant Table status field will be updated to indicate that the host has failed.

You will need to Stop and Start the file collaboration session 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.

Note: We currently have plans to add the ability to dynamically add and remove a host from a running file collaboration session.

Quorum

In order for a file collaboration session 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.

Runtime Views

The File Collaboration Session Applet has three main Runtime Views used for viewing a combination of real-time file I/O activity, history and other related actions.

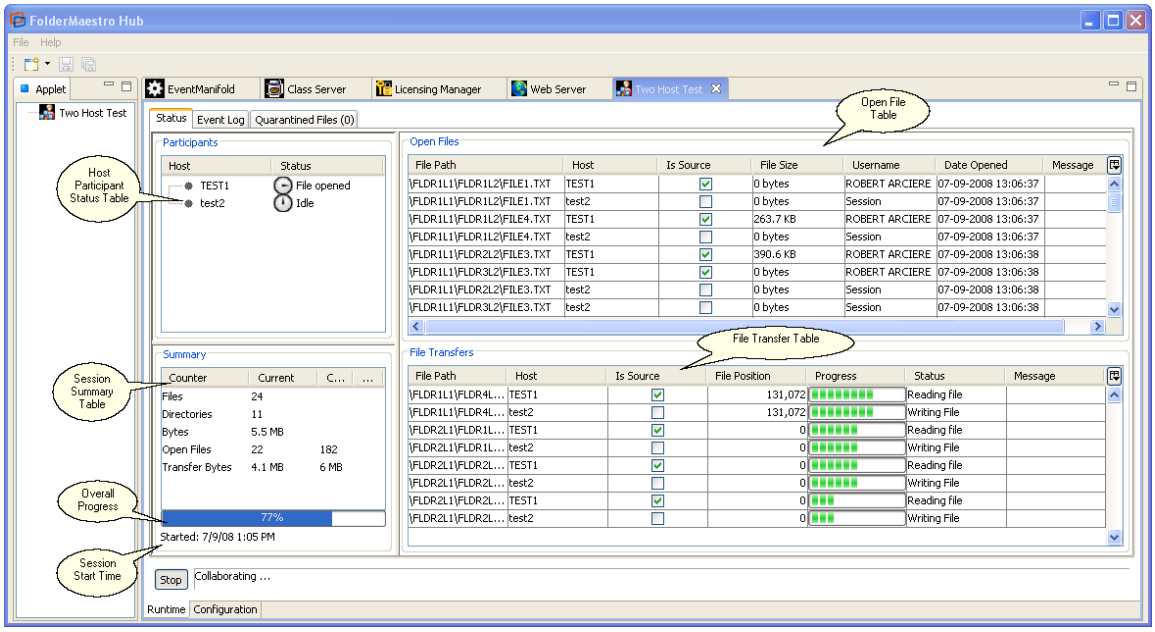
- **Runtime Views**

Status View
Event Log

Quarantined Files

1. Status View

The Status View allows you to see real-time file collaboration activity, participating host status and file collaboration statistics.



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

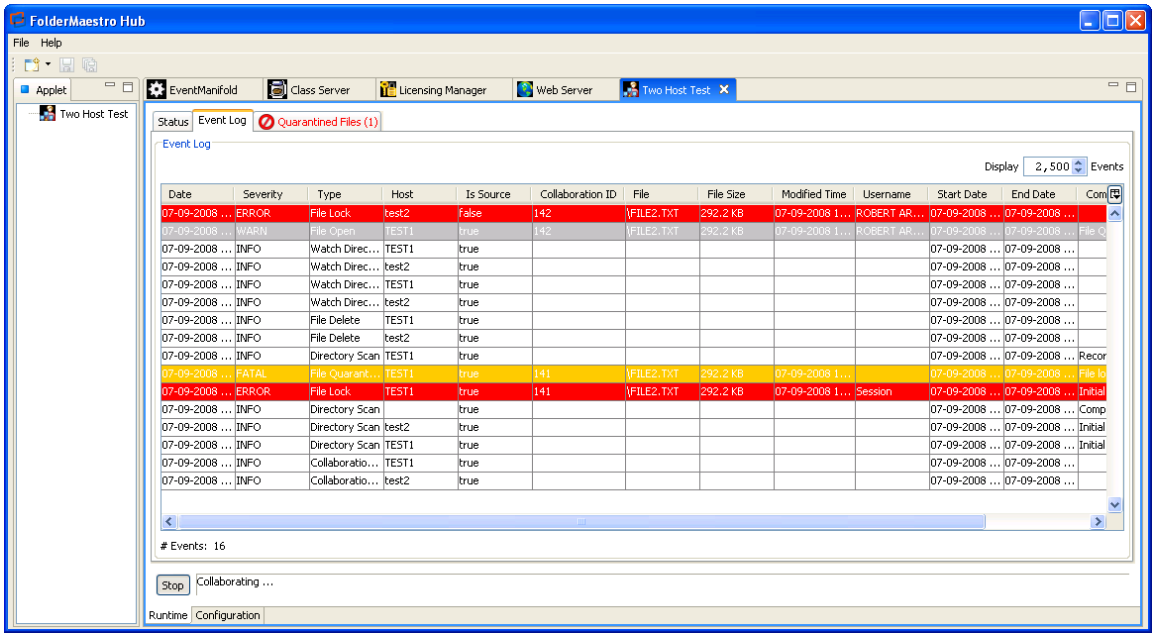
Host Participant Table	Show a list of all currently configured host participants, and contains a status column used to display activity status happening on host(s). Selecting one or more hosts will also filter the Open Files and File Transfer tables to just show activity from the selected host(s). Clicking on any column headers will sort by that column in ascending or descending order.
Open Files Table	A table showing all currently open files on the source host along with any internal file locks being held by the file collaboration session on the target host(s) along with file summary information. Clicking on any column headers will sort by that column in ascending or descending order.
File Transfer Table	A table showing all file transfers currently in progress along with file summary information, status and overall progress.
Session Summary Table	A table showing summary statistics for the currently running file collaboration session.

2. Event Log Viewer

The Event Log View allows you to view recent file event history for the currently running file collaboration session based on your File Event Logging settings. You can specify the maximum number of events to store in the table by adjusting the Display Events slider 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 log files are written in a tab delimited format, and Microsoft Excel is a good tool to use to view and analyze a log file. See the

File Event Logging 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.



3. Quarantined Files

Introduction

Files can be quarantined if various conflicts or I/O errors occur in the system, but the most common reasons are as follows:

1. File Lock Conflict occurs when two or more users open a file at the same time before all files can be locked down by the file collaboration session. This can also happen during the file collaboration initial directory scan.
2. A general I/O failure occurs on the Source Host after the file has been modified, and before the file is synchronized to all Target Hosts

Once a file is placed in the **Quarantined Files List**, 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. The quarantined file list is saved to disk and will survive session restarts. The quarantined file 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).

Removing a file from Quarantine

You must explicitly remove a file from quarantine in order to have it participate in the collaboration session again. To remove a file from quarantine, select the file in the table, and then select the host with the correct version and press the **Release Quarantine** button. After doing this all hosts

are checked to make sure the file is not currently locked by anybody, and if so, 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 chose to perform no action, in which case the file is removed from quarantine but none of the file versions are modified; therefore if the files are not currently in-sync, then the next time the file is modified, changes will be propagated to the other hosts. If an error occurs while removing the quarantine, then the Status field in the Quarantined Files table is updated to reflect the error.

You may also select multiple files to remove from quarantine in one operation.