



## Fortis® Security Overview

### Introduction

**Fortis** electronic document management (EDM) software runs on Windows networks. It allows multiple users to store data and documents in standard SQL databases and access them via our Windows-based clients or via thin-client through the use of **Fortis Web**. This document describes the various levels of security that can be implemented within **Fortis** and its surrounding network and Web environment.

### What happens when a document is stored in Fortis?

**Fortis** allows administrators to define databases that function as the repository for the descriptive information pertaining to each document. In addition to storing user-entered data used to locate documents and store pertinent information related to the document, a **Fortis** database record also contains pointers to the documents physical location in the file system. Each **Fortis** record consists of two parts: The pointer to the document (scanned image or electronic document), and the index data (the descriptive information). At the time of indexing a document, the index data is stored in a database and the document is moved to a shared network folder.

During the design phase, the administrator defines the structure that will contain the database records. Users gain access to documents by searching the database for certain criteria, then can view the associated documents because the path information to that image is stored in the database record.

### Security Levels

There are eight basic elements to the **Fortis** security schema. The first five are Application Access, System Access, Database Access, Database Object Access, and Web Access. These five security elements are comprised of security features made available through core functionality in **Fortis**. The last three security elements are the SQL Database Engine, Image Storage Media, and a Proprietary File Structure.

#### Application Access:

Administrators decide who will access the **Fortis** system. Each workstation must have **Fortis** installed and configured locally. If a workstation is not configured, that particular workstation will not be able to run **Fortis**. This can be further secured by locking down the **Fortis** network share and only allowing access to users and groups who should be accessing **Fortis**.

#### System Access:

Once a workstation has been configured to run **Fortis**, an administrator must grant the user access to the **Fortis** system. Each user who will access the system must have a User Name and Password. The Password can be altered by the end user, but is initially setup by the **Fortis** administrator.

With System Access the user will have the ability to scan documents as well as edit and annotate documents in an In Basket. In Baskets (a network folder presented through the **Fortis** GUI) can be either Public or Private, where private means they are restricted to a group or single user. In Baskets can be further secured by implementing the security features of the Network Operating System (NOS).

## Database Access:

While users may have access at the System level, they are only allowed to open databases that they have been specifically granted access to. **Fortis Web** (Westbrook's Web component) takes this a step further and exposes the ability to hide the list of available databases. Users that have NO access to databases are only allowed to capture documents and view them from In Baskets.

The **Fortis** system maintains an encrypted list of system users that contains user names, passwords, and the databases each user has access to. The file is encrypted using Microsoft's standard encryption tools.

## Database Object Access:

A **Fortis** database contains four core objects that may have security policies applied to them. The objects are Document Types, Folders, Fields, and Queries. There may be multiple instances of each object defined by the administrator, and each instance can take advantage of its own security policies. In the case of Document Types, a Model Type can be created that can contain a default set of permissions. New Folders and Query Sets inherit the permissions of their parent, making the replication of Folder and Query Set security very simple as well.

A user may have the ability to access a database, but without permissions to the objects within it, the most they can do is see the Folder structure (Document Explorer) that has been put in place to store the documents. In order to add, modify, delete, or view documents, users need appropriate access to the document type and the folder. These four security levels can be set at the Document Type, Folder and Query Set level. If users were to view documents via the Document Explorer, they would need a minimum of View rights at the Document Type and Folder level. This level of flexibility allows the system administrator a great deal of control when designing a secure system.

**Fortis** allows for an unlimited number of Folder and Document Type combinations, allowing for an extremely flexible system. Multiple Document Types may reside in one Folder or Multiple Folders, and Folders may be nested inside other Folders. Each Document Type and Folder maintains its own securities to achieve the most secure system possible.

Query Sets (Folders containing pre-defined searches) can also be secured. Users may not have rights to the Document Type, Folder or the Query Set. Clearly having view rights on the Query Set typically indicates they can view the resulting documents, but this is not required or enforced.

## Web Access:

Our **Fortis Web** product allows access to the **Fortis** system via the Web. It is a standard HTTP application that runs on Microsoft's IIS web server. **Fortis Web** maintains the full security schema of the LAN or WAN based **Fortis** system. This means all the aforementioned security features apply here as well. To **Fortis**, the **Fortis Web** server is nothing more than another network client. While it supports multiple simultaneous users, each one is treated uniquely.

Additionally, the **Fortis Web** interface can be completely customized to suit the needs the users. Through the **Fortis** Web interface users can be dynamically directed to a specific location of the database Folder Structure, or to a specific Query Set.

**Fortis Web** allows the use of Secure Socket Layers (SSL), which can virtually guarantee secure access to **Fortis** documents. **Fortis Web** is fully functional behind a firewall. **Fortis** and **Fortis Web** typically sit behind the company Firewall and enjoy the protection it provides. Use of firewall software to protect **Fortis** on the network is strongly encouraged.

## Image Storage Media:

Documents indexed into **Fortis** can be stored on a variety of locations: RAID, Network shares, Local drives, CD ROM and Optical Disks. Within a given database, the administrator can decide which documents are stored in various locations. Each Archive Path, as it is called in **Fortis**, is configurable per Folder.

Using the Network Operating System security settings, access can be granted or removed from users consistent with the defined database design security model in **Fortis**. This further prevents tampering of the documents stored in the system. Additionally, media such as WORM may be selected, thereby eliminating the possibility of accidental or intentional deletion of documents.

## SQL Database Engine:

**Fortis** supports several ODBC compliant SQL based database systems such as Oracle, SQL Server, and SQL Server Express. **Fortis** clients, including the **Fortis Web** server, all communicate with the database server via ODBC prompted by the instructions the **Fortis** client requests. **Fortis** takes full advantage of the security provided by the database engine. In addition, **Fortis** only requires that a single administrative user be created on the database engine. This prevents having myriad individual users created in the database server, which poses a definite security risk.

## File Structure:

**Fortis** images are stored in a .Mag file format. This format is unique to Westbrook Technologies, thereby eliminating the possibility of viewing documents without a **Fortis** document viewer. The .Mag format not only provides greater flexibility to the **Fortis** application, it eliminates the possibility of users without an associated viewer from seeing any document. Document within **Fortis** can be exportable to their native format (i.e. Word, Excel, Gif, Tiff), converted to PDF or group 4 tiff, in the event users outside the **Fortis** system did need to view documents.

## Summary

The robust security features of **Fortis** are one of the key elements that have made it one of the most sought after enterprise wide document management systems in the industry. The five core security components create a system that meets even the most rigorous security standards. The ability of **Fortis** to take advantage of three additional security components outside the scope of the core product makes it even more impenetrable. These eight elements combined have met the security standards of numerous government and military installations, medical organizations, insurance organizations, and too many others to mention. It is without question the powerful security schema of **Fortis** is what continues to make it a success everywhere security is a concern.



Westbrook Technologies, Inc.  
22 Summit Place, Branford, CT 06405 U.S.A.  
Tel: +1 203 483 6666 · Fax: +1 203 483 3350

THIS DOCUMENT IS PROVIDED TO YOU FOR INFORMATIONAL PURPOSES ONLY. The information furnished in this document, believed by Westbrook Technologies, Inc. to be accurate as of the date of this publication, is subject to change without notice. Westbrook assumes no responsibility for any errors or omissions in this document and shall have no obligation to you as a result of having this document available to you or based upon the information it contains. Certain images and/or photos on these pages are the copyrighted property of EPICTURA Limited, their Contributors or Licensed Partners and are being used with permission under license. These images and/or photos may not be copied or downloaded without permission from EPICTURA Limited.

Westbrook and **Fortis** are registered trademarks of Westbrook Technologies, Inc. All other products and services are the registered trademarks of their respective holders.

© Copyright 1997-2012, Westbrook Technologies, Inc. All Rights Reserved.