

# FinalCode for Box

## The Easy, Flexible and Persistent Way to Secure Sensitive Files Shared Outside of Box

In today's collaborative work environments, content access and fluidity is critical. As enterprise employees look to collaborate internally and externally, business users demand convenient, always available access to content and the means to easily share files, at the same time, IT must manage the risks of data leakage and unauthorized disclosure of confidential data. Unfortunately, cloud-based collaboration platforms do not offer the means to ensure governance of shared files taken outside the cloud application's repository.



Box provides an intuitive cloud file sharing and collaboration platform with comprehensive file management and governance capabilities. But once sensitive data is obtained by an authorized recipient outside the secure Box container, file protection and accountability are diminished, as are data privacy breach safe harbors. The challenge is how to ensure that file protection remains active while supporting existing workflow and business collaboration. Organizations need to think "outside the Box" to mitigate file data leakage risks.

### File Security Right Out of the Box

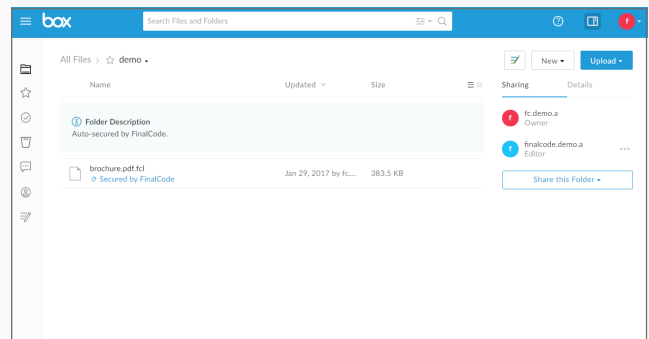
FinalCode for Box addresses this data leakage challenge by ensuring persistent access, usage control and deletion of shared files in a way that is seamless to Box collaborators. With FinalCode, organizations gain strong file encryption, dynamic permission setting, and lifecycle activity tracking – directly invoked within the Box interface as an added SaaS offering.

The solution allows Box files owners and administrators to leverage their investment in Box workflow, user management and security management. Users can manage and change permissions to view or edit files by simply updating Box collaborator types which are linked to FinalCode's file security settings – it's that simple. Once activated, FinalCode security policies are automatically inherited as files and folders are moved within the Box folder hierarchy.

With FinalCode, Box users have dynamic file security control, where by users and organizations can readily change, lock or revoke collaborator access and usage permission to shared files leaving the box repository. Users can now remotely delete files on recipients' devices, on demand or on access attempt violation, even after shared files have been removed from the Box container and even if the files have been forwarded to others. FinalCode security remains enforced at the file, operating system and application level outside of Box.

Employing Box APIs, FinalCode extends Box file governance. FinalCode preserves Box data classification while ensuring encryption and extensive usage control for files taken outside the secure Box container. FinalCode maintains rich file tracking details on FinalCode security policy application and changes, as well as the who, when and where Box shared files are opened, modified, printed and remotely deleted. Organizations gain unified audit records within Box and within log management platforms.

Like Box, FinalCode is cost-effective in that Box Enterprise Edition and Box Business Edition users can purchase FinalCode for internal use by project, department or enterprise-wide with **no cost to Box collaborators outside the organization**. As a result, organizations can readily extend Box file security with FinalCode's enterprise digital rights management (eDRM) in an easy, rapidly deployable and readily scalable manner.



As an option to the extensive file security and governance capabilities of Box, FinalCode for Box offers a persistent file security platform comprised of three components; the FinalCode Encryption Service, the SaaS Server, and the Client. The FinalCode Encryption Service resides on FinalCode's secure SaaS running in Amazon cloud. Once activated through the Box web user interface, file owners simply apply security, in terms of encryption and usage control, based on Box collaborator type. Each collaborator type is mapped to specific FinalCode usage permissions. The FinalCode Encryption Service dynamically takes files from the Box repository, applies security while preserving box metadata, replaces secured file(s) back into the Box repository while deleting the original uploaded file – no sensitive content persists in the FinalCode Encryption service and collaborators can not revert back to the unsecured file. Once the file has been protected, only the security metadata [keys and entitlement] are securely sent to the FinalCode Server. The resulting FinalCode protected file can only be opened by authenticated recipients who have installed the lightweight FinalCode Client application. The FinalCode Client will request access policy from the Server and policy will be enforced at the operating system and application level. Policies can be dynamically modified, and provides for the ability of remote file unlocking and deletion. All file access and usage, both authorized and unauthorized, is logged in the SaaS Server and available to the file owner and enterprise. The entire system is designed for easy and immediate use by Box collaborators with automated Client onboarding for for internal and external recipients. FinalCode Preview app is also available in Box to enable authorized users to view the secured files without installing the FinalCode Client or downloading the files.

## Granular Entitlement Control

- Apply encryption and usage control to files and folders invoked directly within Box GUI
- Enforce policy to files outside the secure Box container, both online and offline
- FinalCode file permissions automatically mapped to Box collaborator types
- Security policy inheritance as files and folders move within Box folder hierarchy
- Preserves Box metadata, negates user means to revert to unprotected file
- Persistent file security via lightweight FinalCode Client
- Read-only, able to block editing or saving
- Edit/save only in encrypted file
- Allow / deny copy, paste, screenshot
- Allow / deny printing
- Printing with custom watermark
- Remote delete, on-demand
- Remote delete, unauthorized access
- Online file activity logging and search
- Dynamic file permission updates according to Box collaborator type changes
- Application whitelisting

## Powerful Security Management

- FIPS 140-2 Level 1 validated
- Suite-B compliant
- AES 256 file encryption
- RSA 2048 PKI - based user authentication
- TLS/SSL communication between client and server
- AWS KMS integration
- Transparent FinalCode Encryption Service:
  - Securely pulls content uploaded to Box
  - Dynamically applies file security settings
  - Replaces protected file in Box repository
  - Deletes original file from Box repository
  - No files are written or persist in service
- Preview secured files in Box
- Set a watermark on preview and downloaded files
- Automated, secure on-boarding
- Lightweight Client install does not require admin privileges
- Web management console
- Global user management
- Roles-based access control
- User and device authentication
- Extensive file security, usage and violation logs supporting Box logging, well as CEF format and SYSLOG
- App and OS level file-IRM control without relying on MS-Azure RMS

## Extensive File IRM Coverage

- Microsoft Excel 2016, 2013, 2010, 2007
- Microsoft Word 2016, 2013, 2010, 2007
- Microsoft PowerPoint 2016, 2013, 2010, 2007
- Microsoft Access 2016, 2013, 2010, 2007
- Microsoft Visio 2016, 2013, 2010, 2007
- Microsoft Viewer Word, Excel, PowerPoint
- Microsoft Windows Media
- Microsoft WordPad, Paint, Notepad
- Adobe Reader DC XI, X
- Adobe Acrobat, Pro/Std. DC XI, X
- OpenOffice.org Writer, Calc, Impress 4.1, 4.0
- Libre Writer, Calc, Impress 5.2, 5.1, 5.0, 4.4, 4.3, 4.2, 4.1, 4.0
- Microsoft Windows Picture and FAX Viewer, Photo Gallery, Photo Viewer
- Broad Photo, Video and Music format support

### CAD Option:

- AutoDesk AutoCAD 2016-2010
- AutoDesk AutoCAD LT 2016-2010
- AutoDesk DWG TrueView 2016-2013
- Dassault SolidWorks 2016-2013

*Abbreviated list, subject to change*

## FinalCode Client

### Client for Windows OS

- Windows 7 Ultimate/Professional SP1 32bit/64bit
- Windows 8.1 Pro/Enterprise 32bit/64bit
- Windows 10 Home/Pro/Education/Enterprise 32bit/64bit
- Windows Server 2012 R2
- Windows Storage Server 2012 R2

### Client for Mac

- Mac OS 10.12 Sierra
- PDF Reader App for iOS
- iOS 9.3 – 10.2

### PDF Reader App for Android

- Android 4.0, 4.1, 4.2.3, 4.4

### Network Folder Security

- Windows Server 2008 R2 SP1 64bit
- Windows Storage Server 2012 R2
- Windows Server 2012 R2
- Windows Server 2016

## FinalCode for Box Specifications

- Available only in SaaS
- FinalCode Encryption Service hosted in US AWS
- FinalCode Server hosted in US AWS
- FinalCode secured files do not support full text search
- Maximum file size to be secured by FinalCode is 100MB
- Up to 1,000 files can be secured by FinalCode in one process

## Take the Next Step

With FinalCode for Box, your employees can share sensitive files internally and externally with confidence, knowing that unauthorized recipients will not have access outside the Box secure container. Better yet, your company can rapidly implement strong file protection, entitlement and auditing capability that preserves user experience and your investment in Box. As a result, organizations can readily extend Box file security with FinalCode's enterprise digital rights management (eDRM) in an easy, rapidly deployable and readily scalable manner). Visit the FinalCode website to schedule a demo or get a free trial license.