

# **FileSurf v7.5 (SR3)**

## **by MDY Advanced Technologies, Inc.**

---

### **FileSurf Summary Report**

The Joint Interoperability Test Command (JITC) tested MDY Advanced Technologies, Inc.'s FileSurf v7.5 (Service Release [SR] 3), a stand-alone records management application (RMA) at the MDY Advanced Technologies, Inc.'s facility in Fair Lawn, New Jersey, from 18 through 27 May 2004. JITC verified the implementation using version 7.1 of the Test Procedures for Chapters 2 (Baseline compliance) and 4 (Classified Records). FileSurf v7.5 (SR3) was compliant with DOD 5015.2-STD, dated June 2002. All mandatory requirements were satisfied.

### **TABLE OF CONTENTS**

- [Section 1. Product Identification](#)
  - [Section 2. Test Configuration](#)
  - [Section 3. RMA Mandatory Requirements](#)
  - [Section 4. Non-Mandatory Features Demonstrated](#)
  - [Section 5. Management of Classified Records](#)
- 

## **1. Product Identification**

FileSurf v7.5 (SR3), hereafter referred to as FileSurf, is a stand-alone RMA.

The FileSurf software package, as tested, consisted of the following component programs and utilities:

- FileSurf Administrator
- FileSurf Web Administrator
- FileSurf Desktop Client
- FileSurf Web Client

## **2. Test Configuration**

The baseline test configuration consisted of:

- One server running the Microsoft (MS) Windows 2000 Server (Service Pack [SP] 4). Installed software included Novell GroupWise Server 6.5.0 and Oracle 9i (Release 1).
- One server running the MS Windows 2000 Server (SP4). Installed software included SQL Server 2000 (v8.0) and MS Exchange 2000.
- One server running the MS Windows 2003 Server. Installed software included Domino Server v6.5.1, Internet Information Services (IIS) 6.0, and FileSurf v7.5 (SR3).
- One client PC running MS Windows 2000 Professional (SP4). Installed software included FileSurf 7.5, Novell GroupWise 6.0, MS Office 2003 (SP1), and Internet Explorer 6.0 (SP2).
- One client PC running MS Windows XP Professional (SP1). Installed software included FileSurf 7.5, Outlook 2003 (SP1), MS Office 2003 (SP1), and Internet Explorer 6.0 (SP2).

- One client PC running MS Windows 2000 Professional (SP4). Installed software included FileSurf 7.5, Outlook 2003 (SP1), Lotus Notes 6.5.1, MS Office 2003 (SP1), and Internet Explorer 6.0 (SP2).
- One client PC running MS Windows XP Professional (SP1). Installed software included FileSurf 7.5, Novell GroupWise 6.0, Lotus Notes 6.5.1, MS Office 2003 (SP1), and Internet Explorer 6.0 (SP2).

During the baseline test, SQL Server 2000 served as the database management system. In a subsequent configuration, JITC repeated the compliance test using the Oracle 9i database.

### **3. RMA Mandatory Requirements**

#### **3.1 *Managing Records [C2.1.1.]***

FileSurf manages electronic, non-electronic, and e-mail records. It stores electronic records in its repository and maintains them in their original, native file format. Users maintain records stored on other media, such as paper, diskette, or tape by adding metadata through the user interface.

#### **3.2 *Accommodating Dates and Date Logic [C2.1.2.]***

FileSurf stores and displays dates using a 4-digit year format, and recognizes leap years including the year 2000. The product accepts user input of valid dates from current, previous, and future centuries.

#### **3.3 *Implementing Standard Data [C2.1.3.]***

FileSurf provides the capability to implement standard data. Records managers create data entry templates. They can create pick lists for user-defined fields to assist the user in filling out the templates.

FileSurf can be configured with all the data elements as defined in DOD 5015.2-STD. The records manager can also configure FileSurf with additional fields for custom use. Custom fields are created in the FileSurf Desktop Administrator and added to the data entry templates using the FileSurf Web Administrator. Administrators can constrain the selection lists presented to users by using filters to partition access.

#### **3.4 *Backward Compatibility [C2.1.4.]***

JITC verified backwards compatibility by successfully importing the FileSurf 2.5 test database into FileSurf 2.5 (SR3).

#### **3.5 *Accessibility [C2.1.5.]***

MDY provided the 508 Voluntary Product Accessibility Templates (VPATS) provided as Appendix C in the detailed test report.

### **3.6     *Implementing File Plans [C2.2.1.]***

FileSurf provides the required capabilities for creating and maintaining disposition instructions and file plans. Disposition instructions are created separately and assigned to record plan components when creating the file plan categories. Subcomponents under that level inherit the same disposition instruction unless another disposition instruction is specified for that lower level component.

Access to the associated FileSurf functions is granted/restricted through the assignment of privilege types to users. FileSurf provides support for multiple levels of file plan access. During the test "privileged" users were able to create and manage folders.

### **3.7     *Scheduling Records [C2.2.2.]***

FileSurf automatically tracks the disposition schedules for screening and disposition processing. Records managers reschedule files by assigning a different disposition instruction to the file or altering the retention period (which reschedules all records associated with that schedule).

Using the FileSurf Web Administrator utility, FileSurf administrators can automate disposition processing as a scheduled service. They select the desired disposition action (e.g., Cutoff, Review, Transfer, Destroy) and apply a schedule to that action (e.g., run daily, monthly, etc.). FileSurf monitors the record folders/categories. When items are due for action, FileSurf automatically sends an e-mail to the records manager advising items are due. The e-mail message contains a link to the folder/category requiring action. Records managers click on the link and can review the items through the web browser. To process the items, records managers must use the desktop client.

### **3.8     *Declaring and Filing Records [C2.2.3.]***

FileSurf includes two user interfaces for filing records. Users file records directly into the FileSurf repository using the FileSurf web interface. They click on the "Add New" hyperlink, select a file code, complete the record metadata, and navigate through the file system to select an electronic file to upload.

Users with access to the FileSurf Desktop Client can file paper and electronic records directly into the FileSurf repository by using the "Insert" menu.

At the time of filing, FileSurf assigns a unique record identifier and a date/time stamp to each record. The date/time stamp serves as the required Date Filed profile field. Users cannot modify either field.

### **3.9 Filing E-mail Messages [C2.2.4.]**

FileSurf provides the capability to file e-mail messages from MS Outlook, Novell GroupWise, and Lotus Notes Mail. FileSurf automatically captures message transmission and receipt data to populate the Author/Originator, Addressee(s), Publication Date, and Subject record profile fields.

When filing e-mail that has an attachment(s), FileSurf gives the user the following options:

- **E-mail Only.** Stores the e-mail and attachments as a single record. Users can save attachments to their hard drives and file them separately as any other electronic record if desired.
- **E-mail and Each Attachment as a Record.** Stores the e-mail only (which does not include the attachments) and, in addition, stores each attachment separately in its native file format.

FileSurf also allows users to file e-mail upon sending, if desired.

### **3.10 Storing Records [C2.2.5.]**

FileSurf uses the server's NT File System (NTFS) for storing and preserving electronic records. The permissions assigned at the file, folder and document levels determine who has access to the records and what they can do with those records. Only users with appropriate access can delete records from the repository.

File plan and document profile data are stored separately from the actual records in a relational database. MS SQL Server 2000 and Oracle 9i provided the databases during the compliance tests.

### **3.11 Screening Records [C2.2.6.1.]**

Records managers perform screening functions using the Disposition Processing template available from the "Browse" menu. From here, they design queries for information relating to folders or records that are qualified for disposition, including cutoff, transfer, accession, or destruction. Records managers enter future dates to identify candidates for disposition for planning purposes.

### **3.12 Closing Record Folders [C2.2.6.2.]**

FileSurf offers records managers and privileged users the ability to close folders by assigning edit privileges to folders. Privileged users can only close folders in the record categories to which they have been assigned folder management privileges.

### **3.13 Cutting Off Record Folders [C2.2.6.3.]**

To cut off record folders, records managers use the Disposition Processing template to search for folders due for Cutoff. A list of folders matching the criteria will display. Records managers select the folder(s) they wish to perform cutoff on and press the "Execute" button. By cutting off the folder, all records within that folder are cut off as well.

### **3.14 Freezing/Unfreezing Records [C2.2.6.4.]**

FileSurf provides the capability to freeze and unfreeze records at all levels of the file plan. If a record series is frozen, all folders and documents in that series do not qualify for disposition. Additionally, the record profiles cannot be modified until the hold is released.

### **3.15 Transferring Records [C2.2.6.5.]**

To transfer records, records managers use the Disposition Processing template to identify folders and/or records due for transfer or accession (referred to as Permanent Storage in FileSurf). In both cases, the records are removed from the repository; however, records managers can choose to retain the metadata of the transferred records by checking the appropriate box before executing the transfer. Additionally, records managers have the option of creating a backup of the records and their metadata by checking the appropriate box and specifying a directory. The extracted metadata is in text format.

### **3.16 Destroying Records [C2.2.6.6.]**

To destroy records, the records manager uses the Disposition Processing template to search for folders and/or records due for destruction, selects them, and verifies that they should be destroyed. FileSurf then deletes the records from the repository and database.

Records cannot be reconstructed once they have been deleted.

### **3.17 Cycling Vital Records [C2.2.6.7.]**

FileSurf provides the ability to gather records based on cycling dates and to do updates of cycle dates after records have been reviewed. During the test, MDY attached logic to the folder vital record review date fields that sent email to a specified records manager when the folders were due for vital records review.

### **3.18 Searching for and Retrieving Records [C2.2.6.8.]**

FileSurf provides the required capability for searching for and retrieving records. Users can enter multiple values in search fields to perform nested searches. FileSurf allows users to export copies of the records to their hard drives.

### **3.19 Access Controls [C2.2.7.]**

Records managers assign FileSurf functional access to files, folders and/or documents at the user and/or group level. Permissions are set at the record category or folder level to assign file and/or search and retrieve access to users/groups.

FileSurf supports multiple-user access. At time during the compliance test, two users worked simultaneously performing various functions including filing system maintenance, record filing, record retrieval, reporting, and disposition activities.

### **3.20 System Audits [C2.2.8.]**

Administrators determine what events to log for FileSurf items by accessing the Actions tab from the Audits template in the FileSurf Desktop Client. Examples of audited events include insert, modify, delete, assign security, and update.

FileSurf collects the audit metadata specified in the Standard, however, it does not collect sufficient data to adequately reconstruct a user's attempt at unauthorized access.

### **3.21 System Management Requirements [C2.2.9.]**

The operating system (MS Windows 2003 Server) and database management systems (MS SQL 2000 and Oracle 9i) provided the required system management capabilities.

## **4. Non-Mandatory Features Demonstrated**

### **4.1 Interfaces to Other Software Applications [C3.2.3.]**

FileSurf integrates with MS Office applications. Users can right click on any MS Word, Excel, or Power Point document and file it directly to the FileSurf repository.

### **4.2 Retrieval Assistance Capability [C3.2.9.]**

FileSurf has advanced searching tools for folders and documents, including full text searching capability.

### **4.3 Internal Viewer Capability [C3.2.14.]**

FileSurf uses INSO viewers to view documents from within FileSurf. The Inso Viewer has the capability to view over 250 different document types. FileSurf can be configured to open records in their native application, or in the INSO viewer.

### **4.4 Web Capability [C3.2.15]**

The FileSurf Web Client allows users to file and search/retrieve records via a web browser. Users add new paper, electronic, or imaged records to the FileSurf repository and enter metadata to describe the records. Full searching capabilities are also available in the FileSurf Web Client, allowing users to view a record, view the metadata, or download a copy of a record to their workstations. Typical users requiring only file and search/retrieve capabilities can use the FileSurf Web Client exclusively.

## **5 Management of Classified Records**

FileSurf was configured to satisfy all Chapter 4 requirements. The following paragraphs highlight FileSurf's implementation of specific Chapter 4 requirements.

### **5.1 Managing Classified Records [C4.1.]**

FileSurf provides the capability to manage classified records. When filing classified records, users click on the "Classified" link on the record template. FileSurf presents a template for users to enter the classified metadata.

### **5.2 Mandatory Metadata [C4.1.1.]**

FileSurf is configured to provide all the classified metadata elements as specified in Table C4.T1. of the DOD 5015.2-STD.

### **5.3 Classification Guides [C4.1.10.]**

FileSurf implements classification guides as tables. Users click on the classification guide link to display the available classification guide indicators. They select the classification guide indicator they want to use and then select a topic. FileSurf copies the information from the guide entry into the relevant fields of the classified metadata template.

### **5.4 Editing Records [C4.1.12.]**

Authorized users can search for classified records due for downgrade or declassification. If the classification status of the record changes, authorized users are allowed to edit the classified record metadata.

### **5.5 Restricted Data and Formerly Restricted Data [C4.1.13.]**

FileSurf provides the capability to handle classified records with the "Restricted Data" and "Formerly Restricted Data" supplemental markings. When users select either marking, FileSurf blanks out the "Downgrade On" and "Declassify On" fields.

### **5.6 Record History Audit [C4.1.16.]**

FileSurf's record history audit captures replaced metadata values, and the user who entered that value. Users can view, copy, save, and print the audit log based on their access permissions.

### **5.7 Access Control [C4.1.20.]**

FileSurf provides the capability to restrict access to records and their metadata based on access criteria. Users are assigned a classification (security) level of Top Secret, Secret, Confidential, or Unclassified. Security levels are hierarchical, therefore, those users assigned a "Secret" security level will only see documents marked Secret and below.

Users are also assigned supplemental markings. Supplemental markings do not override a user's access, but work in conjunction with the user's designated classification level to partition access. Additionally, FileSurf has the ability to restrict access on user-defined fields.

---

Last revision: **9 July 2004**