VA FILEMAN (Version 22.0) and KERNEL (Version 8.0)

FILE ACCESS SECURITY

July 2007

Department of Veterans Affairs
Veterans Health Information Technology (VHIT)
Common Services

Documentation Revision History

The following table displays the revision history for this document. Revisions to the documentation are based on a continuous dialogue with the Security Services Technical Writers and evolving industry standards and styles.

Date	Description	Author
7/2007	First release of document.	REDACTED

Table i: Documentation Revision History

Contents

Figures and Tables

Orientation

This manual is intended for use in conjunction with the VA FileMan Version 22.0 as it relates to access security in VistA.

How to Use this Manual

This manual uses several methods to highlight different aspects of the material. The following symbols are used in the manual to alert the reader about special information:

- Various symbols are used throughout the documentation to alert the reader to special information. The following table gives a description of each of these symbols:

Symbol	Description
ℹ	Used to inform the reader of general information including references to additional reading material
⚠	**Used to caution the reader to take special notice of critical information**

Table ii: Documentation Symbol Descriptions

- Descriptive text is presented in a proportional font (as represented by this font).
- "Snapshots" of computer online displays (i.e., character-based screen captures/dialogs) and computer source code are shown in a *non*-proportional font and enclosed within a box. Also included are Graphical User Interface (GUI) Microsoft Windows images (i.e., dialogs or forms).
    - User's responses to online prompts will be boldface type.
    - The "**<Enter>**" found within these snapshots indicate that the user should press the Enter or Return key on their keyboard.
    - Author's comments are displayed in italics.
- All uppercase is reserved for the representation of M code, variable names, or the formal name of options, field and file names, and security keys (e.g., the XUPROGMODE key).
- Conventions for displaying TEST data when used in this document are as follows:
    - The first three digits (prefix) of any Social Security Numbers (SSN) will begin with either "000" or "666".
    - Patient and user names will be formatted as follows: [Application Name]PATIENT,[N] and [Application Name]USER,[N] respectively, where "Application Name" is defined in the Approved Application Abbreviations document, located on the Web site listed below, and where "N" represents the first name as a number spelled out and incremented with each new entry.

The list of Approved Application Abbreviations can be found at the following Web site:

REDACTED

Who Should Read this Manual?

This manual has been written for personnel responsible for implementing security at the Veterans Integrated Service Networks (VISN), to include Information Resource Management (IRM) personnel involved with implementing the same. If you need more information, it is suggested that you look at the various VA OI Health Systems Design & Development (HSD&D) home web pages for a general orientation to VistA at this address:

http://vaww.vista.med.va.gov

Reference Materials

Readers who wish to learn more about VA FileMan should consult the manuals listed below located on the VHA Software Document Library in MS-Word and PDF formats:

http://www.va.gov/vdl/application.asp?appid=5

- *VA FileMan V. 22.0 Release Notes*
- *VA FileMan V. 22.0 Installation Guide*
- *VA FileMan V. 22.0 Technical Manual*
- *VA FileMan V. 22.0 Getting Started Manual*
- *VA FileMan V. 22.0 Advanced User Manual*
- *VA FileMan V. 22.0 Programmer Manual*

VA FileMan documentation can also be accessed in HTML format at the following Web site:

REDACTED

VistA documentation is made available online in Microsoft Word format and in Adobe Acrobat Portable Document Format (PDF). Adobe Acrobat Portable (PDF) documents *must* be read using the Adobe Acrobat Reader (i.e., ACROREAD.EXE), which is freely distributed by Adobe Systems Incorporated at the following web address:

http://www.adobe.com/

For more information on the use of Adobe Acrobat Reader, please refer to the "Adobe Acrobat Quick Guide" at the following web address: http://vista.med.va.gov/iis/acrobat/index.asp

VistA documentation and software can also be downloaded from the Enterprise VistA Support (EVS) anonymous directories:

Preferred Method	**download.vista.med.va.gov**

This method transmits the files from the first available FTP server.

Albany OIFO	REDACTED
Hines OIFO	REDACTED
Salt Lake City OIFO	REDACTED

How to Obtain Technical Information Online

Obtaining Data Dictionary Listings

Technical information about VistA M-based files and their associated fields is stored in data dictionaries. You can use the List File Attributes option on the Data Dictionary Utilities submenu in VA FileMan to print formatted data dictionaries.

For details about obtaining data dictionaries and about the formats available, please refer to the "List File Attributes" chapter in the "File Management" section of the *VA FileMan Advanced User Manual* located at the following address:

http://www.va.gov/vdl/application.asp?appid=5

DISCLAIMER: The appearance of external hyperlink references in this manual does not constitute endorsement by the Department of Veterans Affairs (VA) of this Web site or the information, products, or services contained therein. The VA does not exercise any editorial control over the information you may find at these locations. Such links are provided and are consistent with the stated purpose of this VA Intranet Service.

Introduction

VA FileMan is VistA's database management system. VA FileMan APIs are divided up into two categories:

- Classic VA FileMan─Certain modules within VA FileMan are callable by other M routines or when using the VA FileMan exported menu options. File access security checking is performed via Classic FileMan APIs.

  Another implementation of file access security checking is done via Kernel File Access Security. This topic is detailed further in this documentation.

- Database Server (DBS)─No file access security checking is performed on VA FileMan Database Server (DBS) calls because they separate interactions with the database created by programmers. They are "silent," meaning there is no interaction with the end-user.

  There is no further discussion about the VA FileMan Database Server (DBS) calls in this documentation.

VA FileMan Reserved Symbols Used to Implement File Access Security

VA FileMan recognizes the two symbols listed below. All other symbols are available to use in order to implement site file access security via Classic FileMan APIs at the developer or VA Facilities discretion. DUZ(0) is set after the user has been validated by the Kernel. The value for any user's DUZ(0) can be found in the NEW PERSON file (#200), FILE MANAGER ACCESS CODE field (#3).

- At-sign (@)─Programmer access in VistA is defined as DUZ(0)="@". It grants the privilege to become a programmer in VistA. Programmer access allows you to work outside many of the security controls enforced by VA FileMan, enables access to all VA FileMan files, access to modify data dictionaries, etc. It is important to proceed with caution when having access to the system in this way.
- Caret (^)─The caret (^) trumps the at-sign (@). For example, if the user's DUZ(0)="@", but WR ACCESS is set to a caret (^), that user cannot write (e.g., via the VA FileMan Enter Or Edit File Entries option) to that file. This is often used at the field level, obstructing all DUZ(0) access to that field.

For information about DUZ(0)="@" programmer access in VistA, consult the *VA FileMan V. 22.0 Programmer Manual*, located on the VHA Software Document Library:

http://www.va.gov/vdl/application.asp?appid=5

What Type of File Access Security is Your Site Using?

Security control for file access at VA Facilities is implemented via either of the following two methods:

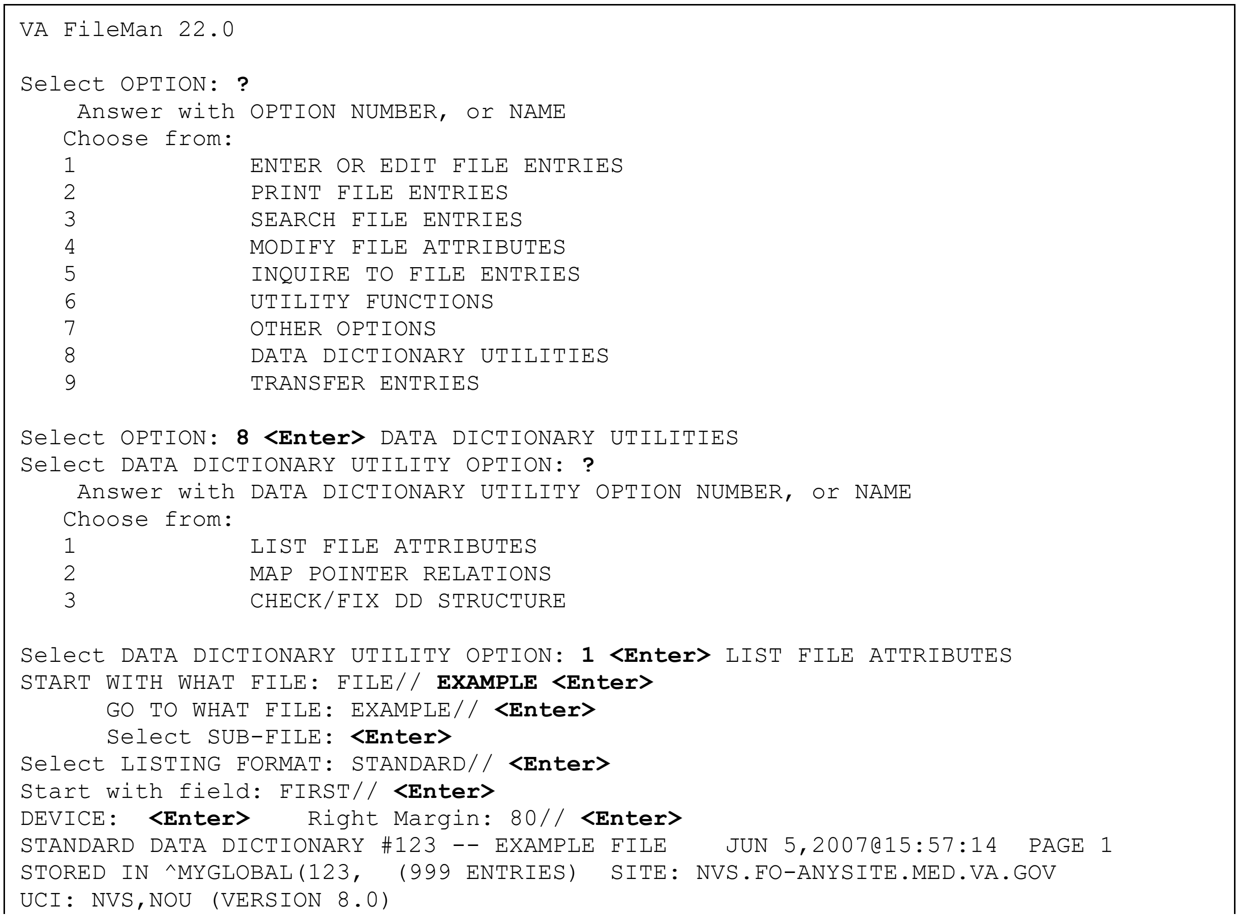
- Classic VA FileMan file access security
- Kernel File Access Security

In order to know how to manage file security at your site, it is first necessary to determine which security implementation your site is using. An easy way to determine if the Kernel File Access Security option [XUFILEACCESS] has been implemented is to use the VA FileMan Data Dictionary Utilities option [DI DDU], as shown in Figure 1.

Select the List File Attributes option [DILIST]. At the "START WITH WHAT FILE:" prompt, select a VistA Fileman file from which to display the data dictionary. If your site is using Kernel File Access Security, the following message will appear after the file description and security access information is displayed, Figure 1:

```
(NOTE: Kernel's File Access Security has been installed in this UCI.)
```

The file used to create the screen capture in Figure 1 is fictitious and used only for the purposes of this example.

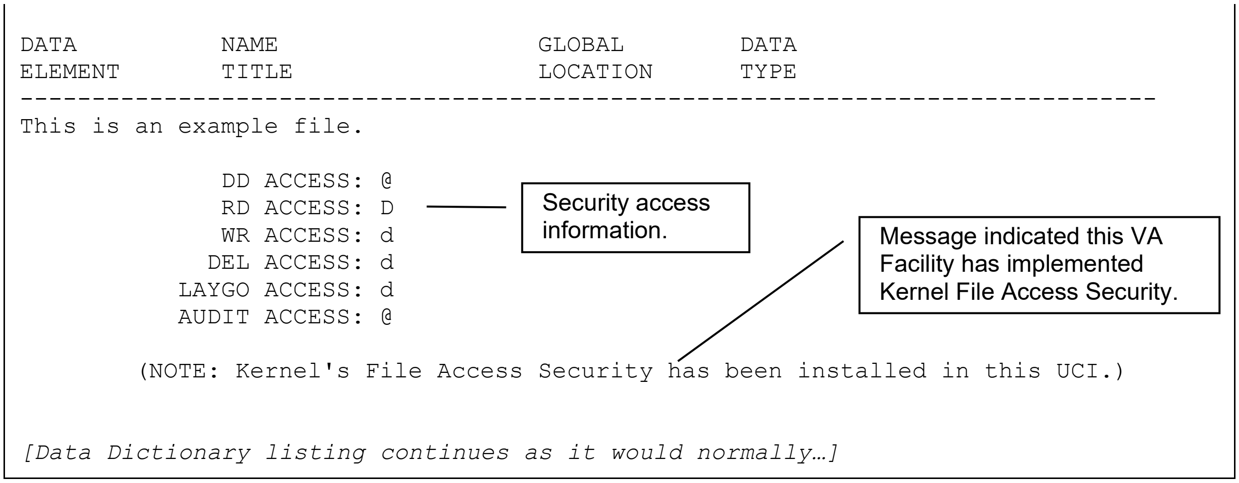


```
VA FileMan 22.0

Select OPTION: ?
    Answer with OPTION NUMBER, or NAME
   Choose from:
   1            ENTER OR EDIT FILE ENTRIES
   2            PRINT FILE ENTRIES
   3            SEARCH FILE ENTRIES
   4            MODIFY FILE ATTRIBUTES
   5            INQUIRE TO FILE ENTRIES
   6            UTILITY FUNCTIONS
   7            OTHER OPTIONS
   8            DATA DICTIONARY UTILITIES
   9            TRANSFER ENTRIES

Select OPTION: 8 <Enter> DATA DICTIONARY UTILITIES
Select DATA DICTIONARY UTILITY OPTION: ?
    Answer with DATA DICTIONARY UTILITY OPTION NUMBER, or NAME
   Choose from:
   1            LIST FILE ATTRIBUTES
   2            MAP POINTER RELATIONS
   3            CHECK/FIX DD STRUCTURE

Select DATA DICTIONARY UTILITY OPTION: 1 <Enter> LIST FILE ATTRIBUTES
START WITH WHAT FILE: FILE// EXAMPLE <Enter>
      GO TO WHAT FILE: EXAMPLE// <Enter>
      Select SUB-FILE: <Enter>
Select LISTING FORMAT: STANDARD// <Enter>
Start with field: FIRST// <Enter>
DEVICE:  <Enter>    Right Margin: 80// <Enter>
STANDARD DATA DICTIONARY #123 -- EXAMPLE FILE    JUN 5,2007@15:57:14  PAGE 1
STORED IN ^MYGLOBAL(123,  (999 ENTRIES)  SITE: NVS.FO-ANYSITE.MED.VA.GOV
UCI: NVS,NOU (VERSION 8.0)
```



```
DATA          NAME                    GLOBAL        DATA
ELEMENT       TITLE                   LOCATION      TYPE
-------------------------------------------------------------------------------
This is an example file.

              DD ACCESS: @
              RD ACCESS: D
              WR ACCESS: d
             DEL ACCESS: d
           LAYGO ACCESS: d
           AUDIT ACCESS: @

        (NOTE: Kernel's File Access Security has been installed in this UCI.)


[Data Dictionary listing continues as it would normally…]
```

Security access information.

Message indicated this VA Facility has implemented Kernel File Access Security.

Figure 1: Example—Use VA FileMan to determine if your site is using Kernel File Access Security

If your VA Facility has implemented Kernel File Access Security, it is not using Classic VA FileMan file access security.

Developers can also verify Kernel File Access Security by checking for the ^VA(200,"AFOF") cross-reference. If it exists, then Kernel File Access Security has been implemented.

Figure 2 shows user field values in the NEW PERSON file (#200) using the same fictitious EXAMPLE file (#123) from Figure 1.

```
NEW PERSON LIST                        JUN  6,2007  06:18    PAGE 1
                                                   FILE MANAGER
NAME                                               ACCESS CODE

                           DD       DEL      LAYGO    RD       WR       AUDIT
FILE                       ACCESS   ACCESS   ACCESS   ACCESS   ACCESS   ACCESS
---------------------------------------------------------------------------------------------

FMUSER,ONE                                         dS

EXAMPLE                                            YES
```

Figure 2: Example—Security property values in the NEW PERSON file (#200)

A Null value is equal to a "NO." In Figure 2, the DUZ(0) for the user named ONE FMUSER is equal to “dS.” Based on the security access shown in Figure 1, this indicates that the user does not have READ (RD) access.

For information on the difference between Kernel and VA Classic FileMan file access security, see the following topic "Difference in Behavior Between Kernel File Access Security and Classic VA FileMan File Access Security" in this documentation.

For information about Kernel File Access Security, consult the *Kernel Systems Management Guide, Version 8.0*, in the "File Access Security" chapter, located on the VHA Software Document Library:

http://www.va.gov/vdl/application.asp?appid=10

How to Use the File Access Security at Your Site

- If your VA Facility is *not* using Kernel File Access Security, read the section titled "Classic VA FileMan File Access Security"
- If your VA Facility *is* using Kernel File Access Security, read the section titled "Kernel File Access Security"

Classic VA FileMan File Access Security

Given the example in Figure 1, if you *do not* see the message "(NOTE: Kernel's File Access Security has been installed in this UCI.)" when displaying a VistA file in the VA FileMan Data Dictionary Utilities option, then your site has not implemented Kernel File Access Security. This means that file access security at your site is implemented based on VA FileMan symbol(s) that are set into the security access property for a particular file via Classic FileMan APIs. User file access is based upon the VA FileMan symbols contained in the DUZ(0) value.

Example

In this example, the RD ACCESS for the fictitious file, EXAMPLE file (#123), in Figure 1 is equal to "D," and the user’s DUZ(0) is equal to "AaZz." This means that the user will not be able to view the data via VA FileMan’s exported menus because the DUZ(0) does not contain the symbol "D." If that same user’s DUZ(0) was equal to Aa**D**Zz, then the user *is* authorized to view the file's data via the VA FileMan’s exported menus because the DUZ(0) contains the symbol "D."

Difference in Behavior Between Kernel File Access Security and Classic VA FileMan File Access Security

In the Classic VA FileMan file access security environment, the user (shown in the previous example) would *not* be authorized to view the data contained in the EXAMPLE file (#123) via the VA FileMan exported menu option(s) because the user's (ONE FMUSER) FILEMANAGER ACCESS CODE field (#3) does not contain the symbol "D." However, in a Kernel File Access Security environment, the file RD ACCESS is set to Yes for the user. Hence the user *would be able* to view the data.

File Level Security Properties

There are six security properties involved with file access security, Table 3. If a security property is not defined, the value is null. In the Classic VA FileMan file access security environment, properties with null values open up full user access to the VA FileMan exported menu option(s) for that property.

Access	Security Property Description	Property Location (Classic VA FileMan)
AUDIT	The AUDIT security property controls the setting of auditing characteristics and the deletion of audit trails. Examples of the VA	^DIC(<file number>,0,”AUDIT”)=<value>

Access	Security Property Description	Property Location (Classic VA FileMan)
	FileMan options that this property controls are as follows: • Fields Being Audited [DIAUDITED FIELDS] • Data Dictionaries Being Audited [DIAUDIT DD] • Purge Data Audits [DIAUDIT PURGE DATA] • Purge DD Audits [DIAUDIT PURGE DD] • Turn Data Audit On/Off [DIAUDIT TURN ON/OFF]	
DATA DICTIONARY "DD"	The DATA DICTIONARY security property controls who has access to modify the data dictionary. Examples of the VA FileMan options that this property controls are as follows: • Modify File Attributes [DIMODIFY] • Utility Functions [DIUTILITY]/(Data Dictionary [DIDDU])	^DIC(<file number>,0,"DD")=<value>
DELETE "DEL"	The DELETE security property controls who can delete an existing record that is contained within the file. Examples of the VA FileMan options that this property controls are as follows: • Enter or Edit File Entries [DIEDIT] • Transfer Entries [DITRANSFER]	^DIC(<file number>,0,"DEL")=<value>
LAYGO	The LAYGO (Learn As You Go) security property controls who can add a new record to the file. Examples of the VA FileMan options that this property controls are as follows: • Enter or Edit File Entries [DIEDIT] NOTE: You must have LAYGO and WRITE access to a file to add new entries. In addition, you must have WRITE access at the field level for all required identifier fields.	^DIC(<file number>,0,"LAYGO")=<value>
READ "RD"	The Read security property controls who has access to read data contained within a file. Examples of the VA FileMan options that this property controls are as follows: • Print File Entries [DIPRINT] • Search File Entries [DISEARCH] • Inquire to File Entries [DIINQUIRE] • Statistics [DISTATISTICS], List File Attributes [DILIST]	^DIC(<file number>,0,"RD")=<value>

Access	Security Property Description	Property Location (Classic VA FileMan)
	• Transfer File Entries [DITRANSFER] (transfer-from file)	
WRITE "WR"	The WRITE security property controls who can alter data in an existing record that is contained within the file. Examples of the VA FileMan options that this property controls are as follows: • Enter or Edit File Entries [DIEDIT] • Transfer [File] Entries [DITRANSFER] (transfer-to file)	^DIC(<file number>,0,”WR”)=<value>

Table 3: File level security properties in Classic VA FileMan file access security

Kernel File Access Security

Given the example in Figure 1, if you *do* see the message "(NOTE: Kernel's File Access Security has been installed in this UCI.)" when displaying a VistA file in the VA FileMan Data Dictionary Utilities option, file access security is controlled by the ACCESSIBLE FILE multiple (#32) in the NEW PERSON file (#200). This means that file access security to a particular file is *not* based on the VA FileMan Access Code DUZ(0) value. Rather, a lookup is done on the user's ACCESSIBLE FILE multiple (#32) record in the NEW PERSON file (#200) to determine which accesses are allowed to the file in question via VA FileMan exported menus. If the users VA FileMan Access Code [i.e., DUZ(0)] is equal to the at-sign (@), they are allowed access to all files.

Kernel File Access Security is known as an Access Control List in other systems.

File Level Security Properties

There are six security properties involved with file access security that are equivalent to the Classic VA FileMan file access security, Table 4. Unlike Classic VA FileMan file access security, in a Kernel File Access Security environment, if the security property is not defined, the VA FileMan exported menu option(s) for that property are *not* open to full access for users.

These same security properties left undefined in a Classic VA FileMan file access security environment open the related VA FileMan exported menu option(s) up to full access for users.

Access	**Security Property Description**	**Property Location (Kernel File Access Security)**
AUDIT	The AUDIT security property controls the setting of auditing characteristics and the deletion of audit trails. Examples of the VA FileMan options that this property controls are as follows: • Fields Being Audited [DIAUDITED FIELDS] • Data Dictionaries Being Audited [DIAUDIT DD] • Purge Data Audits [DIAUDIT PURGE DATA] • Purge DD Audits [DIAUDIT PURGE DD] • Turn Data Audit On/Off [DIAUDIT TURN ON/OFF]	File: NEW PERSON (#200) Multiple: ACCESSIBLE FILE (#32) Property: AUDIT ACCESS (#6)
DATA DICTIONARY "DD"	The DATA DICTIONARY security property controls who has access to modify the data dictionary. Examples of the VA FileMan options that this property controls are as follows: • Modify File Attributes [DIMODIFY]	File: NEW PERSON (#200) Multiple: ACCESSIBLE FILE (#32) Property: DATA DICTIONARY ACCESS (#1)

Access	Security Property Description	Property Location (Kernel File Access Security)
	• Utility Functions [DIUTILITY]/(Data Dictionary [DIDDU])	
DELETE "DEL"	The DELETE security property controls who can delete an existing record that is contained within the file. Examples of the VA FileMan options that this property controls are as follows: • Enter or Edit File Entries [DIEDIT] • Transfer Entries [DITRANSFER]	File: NEW PERSON (#200) Multiple: ACCESSIBLE FILE (#32) Property: DELETE ACCESS (#2)
LAYGO	The LAYGO (Learn As You Go) security property controls who can add a new record to the file. Examples of the VA FileMan options that this property controls are as follows: • Enter or Edit File Entries [DIEDIT] NOTE: You must have LAYGO as well as WRITE access to a file to add new entries. Additionally, you must have WRITE access at the field level for all required identifier fields.	File: NEW PERSON (#200) Multiple: ACCESSIBLE FILE (#32) Property: LAYGO ACCESS (#3)
READ "RD"	The READ security property controls who has access to read data contained within a file. Examples of the VA FileMan options that this property controls are as follows: • Print File Entries [DIPRINT] • Search File Entries [DISEARCH] • Inquire to File Entries [DIINQUIRE] • Statistics [DISTATISTICS], List File Attributes [DILIST] • Transfer File Entries [DITRANSFER] (transfer-from file)	File: NEW PERSON (#200) Multiple: ACCESSIBLE FILE (#32) Property: READ ACCESS (#4)
WRITE "WR"	The WRITE security property controls who can alter data in an existing record that is contained within the file. Examples of the VA FileMan options that this property controls are as follows: • Enter or Edit File Entries [DIEDIT] • Transfer [File] Entries [DITRANSFER] (transfer-to file)	File: NEW PERSON (#200) Multiple: ACCESSIBLE FILE (#32) Property: WRITE ACCESS (#5)

Table 4: File level security properties in Kernel File Access Security

Index