

DS RAZOR

for Windows

Interactive Management and Reporting for
Active Directory and Windows File Systems

Ready-to-Run Applets

Visual Click Software, Inc.

Copyrights

This manual contains proprietary information that is protected by copyright. The information in this manual is subject to change without notice. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose other than the licensee's personal use without prior written permission of Visual Click Software. The software described in this manual is furnished under a license granted by Visual Click Software to the licensee. This software may be used or copied only in accordance with the terms of the license agreement.

© 2008 Visual Click Software, Inc. **All rights reserved.**

Trademarks

DSRAZOR[®] and Visual Click[®] are registered trademarks of Visual Click Software, Inc. Novell[®], NetWare[®], NDS[®], ConsoleOne[®], GroupWise[®], ZENworks[®], and BorderManager[®] are registered trademarks and eDirectory[™], NetWare Loadable Module[™], NLM[™], and Client32[™] are trademarks of Novell, Inc. Microsoft[®], Windows[®], Windows NT[®], and Active Directory[®] are registered trademarks of Microsoft Corporation in the United States and other countries. Other marks cited in this document are the property of their respective owners.

Patents

U.S. Patent No. 6,438,742

Issue Date: August 20, 2002

Documentation Conventions

Special information in this manual is presented using the following conventions:

- **Bold** text indicates commands, command-line options, and interface controls, such as the names of icons, menus, menu items, buttons, checkboxes, and tabs.
- *Italic* text indicates variables that must be replaced with a value. It also indicates book titles and emphasized terms.
- `Monospace` text indicates data to enter, filenames, and code examples.

NOTE:	Provides information that emphasizes or supplements important points in the main text.
IMPORTANT:	Provides information essential to the completion of a task. Do not disregard an important note.

Contact Us

Thanks for using DSRAZOR. Visual Click Software is committed to the ongoing support of its products. For information and the latest downloads of the DSRAZOR product, see the web site at <http://www.visualclick.com/>. For information, help, and to report problems associated with this product, or if needing features or functionality that are not currently offered by Visual Click Software, contact the customer support team at supportw@visualclick.com. To purchase additional licenses, contact the sales team at sales@visualclick.com.

Contact us at the following mailing address:

Visual Click Software, Inc.
P.O. Box 161657
Austin, TX 78716

Pubrev 062709

Introduction

DSRAZOR is an authoring tool that allows you to create network management applications called **applets**. You do not need to know programming or do any scripting. Instead, DSRAZOR uses drag-and-drop controls that you arrange within a familiar tree structure to create applets that perform various tasks.

More than 100 pre-designed applets are included with DSRAZOR for Windows. These applets perform such tasks as listing user accounts with password problems, listing all Windows file system objects in a selected share or directory, and managing group membership via drag-and-drop. DSRAZOR helps you design interactive applets using any of its predefined applets or customizing your own.

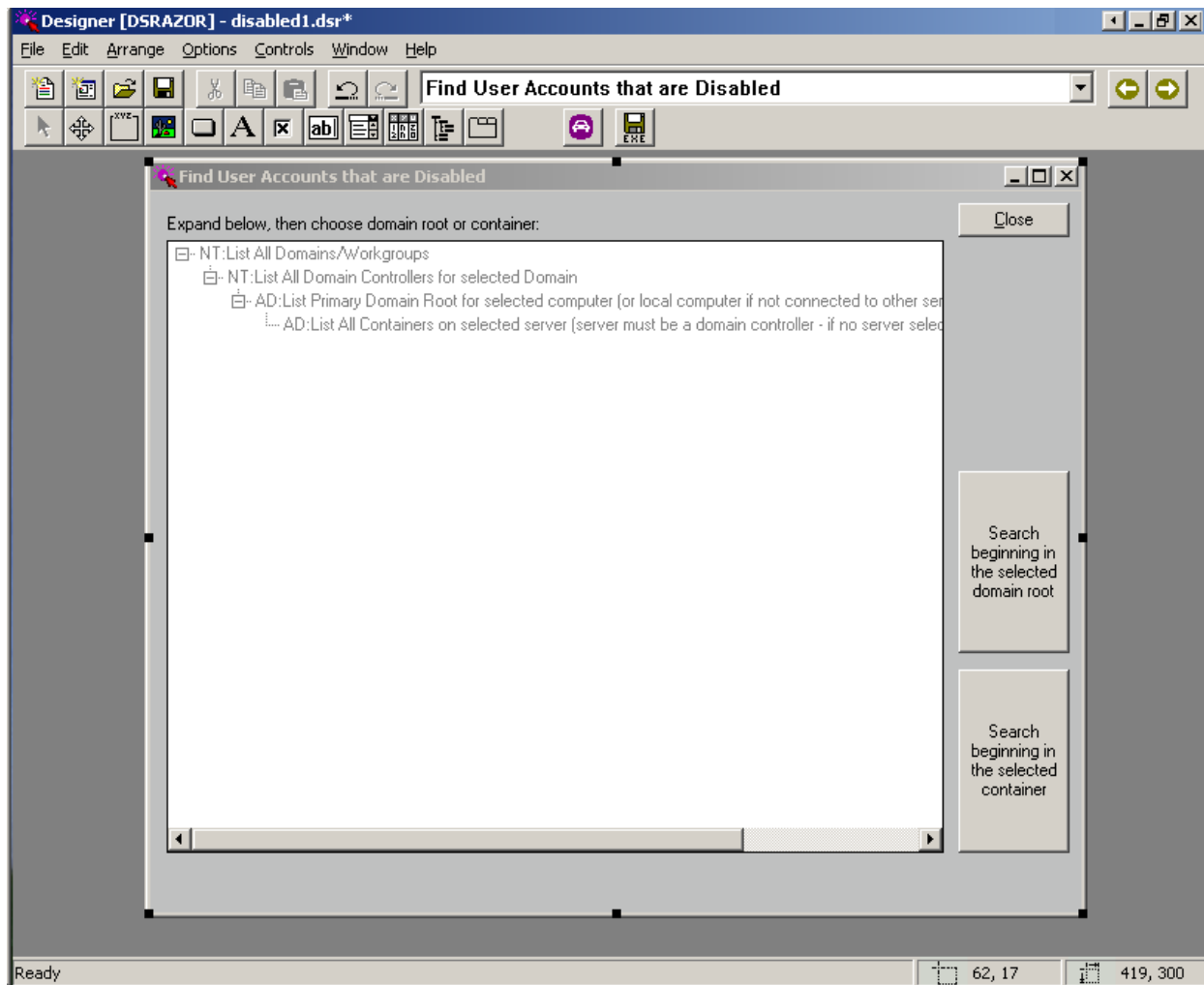
When you first use DSRAZOR for Windows, you are presented with the **Console**, which contains a menu of the predefined, ready-to-run applets.



DSRAZOR for Windows Console

Each applet in the **Console** showcases specific features of DSRAZOR for Windows. The applets run as Windows applications; you can customize an applet functionally and visually using DSRAZOR's **Designer** tool. Since each applet relies on the user's permissions to complete its duties, your user account must be sufficiently privileged for your results to be complete.

DSRAZOR for Windows Ready-to-Run Applets



DSRAZOR for Windows Designer

The DSRAZOR for Windows **Designer** also enables you to create your own applets. The **Designer** provides numerous modular tools (called *services*) to assist you in constructing applets.

You can also perform any of the following tasks using the DSRAZOR for Windows **Designer**:

- Editing an applet so that data is presented in a particular manner
- Combining applets
- Modifying the list of applets displayed in the **Console**
- Displaying your organization's logo or another graphic at the top of the **Console**

DSRAZOR applets are saved as *.DSR files. When you select an applet to use in the **Console**, the executable file DSRRUN.EXE is launched with the selected .DSR. You can open any applet with the **Designer** and save the .DSR as an .EXE file that can be distributed independently of the **Console**.

Descriptions of Windows Ready-to-Run Applets

The following sections describe the applets found in the DSRAZOR for Windows **Console**.

NOTE: DSRAZOR for Windows ready-to-run applets enable you to turn any list of results into an instant report. Right-clicking over a list of results allows you to immediately save and/or export the list results in a variety of formats. This feature is automatic in every DSRAZOR for Windows applet.

The applets are ordered in this section as they are in the **Console**:

- [Assess AD/NTFS Security](#)
- [Query and Search AD](#)
- [HelpDesk Examples](#)
- [AD User Maintenance](#)
- [Examine Servers/Disks](#)

As you use the **Console**, you will notice the following option in all categories **except** HelpDesk Examples:

[Request the Report you need here]

The applets packaged with DSRAZOR for Windows can be readily customized to meet your specific needs. Once you are familiar with the services and control objects used in the applets, you will be able to create almost any solution you need in less than 10 minutes. Double-click this option for information on requesting help to build an applet.

Category: Assess AD/NTFS Security

The applets available from this menu category are generally useful for assessing and maintaining security in the Active Directory forest and Windows Domains. In the sections that follow you will find the title of each applet, its specific filename and description.

Accounts that are disabled

[disabled1.dsr]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root that are flagged as being disabled. If you search via the DNS Domain Root option the selected Domain Root and all child domains are automatically searched.

Accounts that are locked or expired

[exp#lockd1.dsr]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root that are expired or locked. If you search via the DNS Domain Root option the selected Domain Root and all child domains are automatically searched.

Accounts that have never logged in

[neverlog1.dsr]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root that have never logged in. The search can be conducted three (3) different ways:

- Scanning the object's pwdLastSet attribute
- Scanning the object's lastLogonTimeStamp attribute: This attribute is only available on Windows 2003 Domain Functional Mode Domain Controllers; by default, this replicated attribute is only updated once every 7 days.
- Scanning the object's lastLogon attribute on each Domain Controller: This is performed on each Domain Controller because the lastLogon Active Directory attribute is not replicated.

If you search via the DNS Domain Root option the selected Domain Root and all child domains are automatically searched.

Accounts that never expire

[noexpire3.dsr]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root that never expire. If you search via the DNS Domain Root option the selected Domain Root and all child domains are automatically searched.

For accounts found you have the option of setting an account expiration date.

Accounts unused for past 30 days

[nolog301a.dsr]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root with no login in the past 30 days. If you search via the DNS Domain Root option the selected Domain Root and all child domains are automatically searched.

This applet discovers unused accounts by scanning the object's lastLogon attribute on each Domain Controller; this is performed on each Domain Controller because the lastLogon Active Directory attribute is not replicated.

Because scanning the value of the lastLogon attribute can require a noticeable amount of time you can edit the applet in the **Designer** to use one of the following two alternate attribute values for determining the approximate last date of last logon:

- Scanning the object's **pwdLastSet** attribute
- Scanning the object's **lastLogonTimeStamp** attribute: This attribute is only available on Windows 2003 Domain Functional Mode Domain Controllers and, by default, this attribute is current within the past 7 days.

Accounts unused for X days

[nologrule1.dsr]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root with no login in the runtime-specified timeframe. If you search via the DNS Domain Root option the selected Domain Root and all child domains are automatically searched.

This applet discovers unused accounts by scanning the object's lastLogon attribute on each Domain Controller; this is performed on each Domain Controller because the lastLogon Active Directory attribute is not replicated.

Because scanning the value of the lastLogon attribute can require a noticeable amount of time you can edit the applet in the **Designer** to use one of the following two alternate attribute values for determining the approximate last date of last logon:

- Scanning the object's **pwdLastSet** attribute
- Scanning the object's **lastLogonTimeStamp** attribute: This attribute is only available on Windows 2003 Domain Functional Mode Domain Controllers and, by default, this attribute is current within the past 7 days.

For accounts found, you can choose from the following:

- Disable accounts
- Move the contents of the home directory
- Move the account to another OU
- Delete the Exchange Mailbox
- Use Smart Delete to delete the user account, the home directory, and the Exchange Mailbox

Accounts where last logon failed

[**badpwd1.dsr**]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root where the last login attempt failed. If you search via the DNS Domain Root option the selected Domain Root and all child domains are automatically searched.

This applet discovers accounts where the last logon failed by scanning the object's badPwdCount attribute on each Domain Controller; this is performed on each Domain Controller because the badPwdCount Active Directory attribute is not replicated.

Unlike scanning for the date of lastLogon there is no alternate attribute to rely upon when determining whether or not the last logon failed.

Accounts with Dialin permission

[**dialin1.dsr**]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root with dialin permissions. If you search via the DNS Domain Root option the selected Domain Root and all child domains are automatically searched.

Accounts with Password problems

[**adpwdp2.dsr**]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root with one or more of the following irregularities:

- Expiration interval has not been set or is greater than 45 days.
- No password is required
- Expiration date/time has already expired
- Account user cannot change their own password

Any of the search criteria can be edited via the **Designer** to fit your organization's standards.

If you search via the DNS Domain Root option the selected Domain Root and all child domains are automatically searched.

For accounts found you can optionally remove the **Password Never Expires** and **Password not Required** Active Directory flags.

ACL Documentation per AD Object

[**listacl1.dsr**]

Lists all objects in the Active Directory container you select. The Document Object ACL Details window displays the object owner, number of applicable Access Control Entries (ACEs), the number of allow and deny ACEs, and the object class of the object. The Viewing Trustees of selected object (unfiltered) window displays the type of ACE (allow or deny), the permissions granted, and whether or not it was inherited. This applet also reports all trustees of the selected object, trustees with effective and non-effective permissions over the object.

ACL stands for "Access Control List" and is sometimes pronounced "AKL".

ACL Documentation per File System Object

[fslistaclp2.dsr]

Lists all Windows file system objects in the selected share or directory.

The Viewing File System Objects on root of selected share Window displays the object owner, whether or not inheritance is blocked, the number of applicable Access Control Entries (ACEs), and the number of allow and deny ACEs. The Viewing Trustees of selected object (unfiltered) window displays the type of ACE (allow or deny), the permissions granted, , and whether or not it was inherited. This applet reports all trustees of the selected object, trustees with effective and non-effective permissions over the object.

This applet can list file system objects per Domain Controller, Windows Member Server and Workstation.

ACL stands for "Access Control List" and is sometimes pronounced "AKL".

ACL Documentation per File System Share

[fsListShareACLp4.dsr]

Lists all Windows file system shares on the selected computer.

The Viewing file system shares on selected path window displays the object owner, the total number of Access Control Entries (ACEs), and the number of allow and deny ACEs. The Viewing all trustees of selected share window displays the type of ACE (allow or deny) and the permissions granted. This applet can list file system shares per Domain Controller, Windows Member Server and Workstation.

ACL stands for "Access Control List" and is sometimes pronounced "AKL".

AD Document Account Security Details

[asd2.dsr]

Searches for Active Directory user accounts within a specific Active Directory container branch or DNS Domain Root that) and reports the following security information:

- Dial-in permission (true/false)
- Enabled/disabled status (true/false)
- Member of Domain Administrators group (true/false)
- Password Never Expires setting (true/false)
- Password age
- Date/time of last login
- Account lockout status (true/false)
- Whether the account has Direct Reports (true/false)
- Account expiration date
- Login time restrictions (true/false)

If you search via the DNS Domain Root option the selected Domain Root and all child domains are automatically searched.

AD Last Logon Report by DC

[lastlogon2.dsr]

Searches for Active Directory user accounts within a specific Active Directory container branch or DNS Domain Root and reports the last logon information including last authenticating server, number of days since last logon and password statistics. If you search via the DNS Domain Root option the selected Domain Root and all child domains are automatically searched.

Additional details include the complete list of Domain Controllers where the selected user account is defined with last logon information.

You can optionally disable selected accounts that were found.

AD Objects with a NULL ACL (no access restrictions)

[ADFindNullAcl3.dsr]

Searches for Active Directory objects within a specific Active Directory container branch or DNS Domain Root where the ACL is NULL. If you search via the DNS Domain Root option the selected Domain Root and all child domains are automatically searched.

The (no access restrictions) designation means all users have full control over the objects that are reported. This has major security implications. A null ACL should not be confused with an empty ACL. An empty ACL is a properly allocated and initialized ACL containing no access-control entries (ACEs). An empty ACL grants no access to the object it is assigned to.

ACL stands for "Access Control List" and is sometimes pronounced "AKL".

AD Objects with a NULL ACL (no access restrictions) OTF

[ADFindNullAcl_OTF3.dsr]

Searches for Active Directory objects within a specific Active Directory container branch or DNS Domain Root where the ACL is NULL. If you search via the DNS Domain Root option the selected Domain Root and all child domains are automatically searched.

Once you select the Active Directory container or DNS Domain Root to search the applet will prompt you for a filename to save the output to and then automatically minimize itself and will return once finished searching. If you would like to stop the applet, click on its System Tray button and you will be prompted to cancel or continue the search.

The (no access restrictions) designation means all users have full control over the objects that are reported. This has major security implications. A null ACL should not be confused with an empty ACL. An empty ACL is a properly allocated and initialized ACL containing no access-control entries (ACEs). An empty ACL grants no access to the object it is assigned to.

ACL stands for "Access Control List" and is sometimes pronounced "AKL".

OTF is our shorthand for Output To File. Applets can be defined as OTF with the Designer. Please note that all search results will be written to the output file you specified.

AD Objects with GPO(s) defined

[gpodef1.dsr]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root for those with a GPO defined on the selected object. If you search via the DNS Domain Root option the selected Domain Root and all child domains are automatically searched.

For each object with a GPO found, lists default domain policies for passwords and accounts.

AD Trustees (users and groups)

[findADtrustee.dsr]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root for all accounts that have privileges over other accounts.

For each object found with delegated privileges you can view the objects controlled. Optionally you can remove the selected object as a trustee.

AD Trustees (users and groups) OTF

[findADtrustee_OTF.dsr]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root for all accounts that have privileges over other accounts.

Once you select the Active Directory container or DNS Domain Root to search the applet will prompt you for a filename to save the output to and then automatically minimize itself and will return once finished searching. If you would like to stop the applet, click on its System Tray button and you will be prompted to cancel or continue the search.

OTF is our shorthand for *Output To File*. Applets can be defined as OTF with the **Designer**. Please note that all search results will be written to the output file you specified.

AD Trustees with Admin privileges (users and groups)

[findadm1.dsr]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root for all accounts that have Administrative privileges over other accounts. Administrative privileges include Create, Delete, Change and Write permissions.

For each object found with an Administrative privilege you can view the objects controlled. Optionally you can remove the selected object as an Administrative Trustee.

AD Trustees with Admin privileges (users and groups) OTF

[findadm_OTF2.dsr]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root for all accounts that have Administrative privileges over other accounts. Administrative privileges include Create, Delete, Change and Write permissions.

Once you select the Active Directory container or DNS Domain Root to search the applet will prompt you for a filename to save the output to and then automatically minimize itself and will return once finished searching. If you would like to stop the applet, click on its System Tray button and you will be prompted to cancel or continue the search.

OTF is our shorthand for *Output To File*. Applets can be defined as OTF with the **Designer**. Please note that all search results will be written to the output file you specified.

AD Trustees with Admin privileges (users)

[findadmu1.dsr]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root for all user accounts that have Administrative privileges over other accounts. Administrative privileges include Create, Delete, Change and Write permissions.

For each user object found with an Administrative privilege you can view the objects controlled. Optionally you can remove the selected user object as an Administrative Trustee.

The (user) designation means only trustees that are user objects will be found and reported; all objects they control will be reported regardless of object type.

AD Trustees with Admin privileges (users) OTF

[findadmu_OTF1.dsr]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root for all user accounts that have Administrative privileges over other accounts. Administrative privileges include Create, Delete, Change and Write permissions.

Once you select the Active Directory container or DNS Domain Root to search the applet will prompt you for a filename to save the output to and then automatically minimize itself and will return once finished searching. If you would like to stop the applet, click on its System Tray button and you will be prompted to cancel or continue the search.

The (user) designation means only trustees that are user objects will be found and reported; all objects they control will be reported regardless of object type.

OTF is our shorthand for *Output To File*. Applets can be defined as OTF with the **Designer**. Please note that all search results will be written to the output file you specified.

AD Trustees with 'Allowed to Authenticate' privilege

[find_ata1.dsr]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root that have the *Allowed to Authenticate* privilege over other objects. If you search via the DNS Domain Root option the selected Domain Root and all child domains are automatically searched.

For each object found with the *Allowed to Authenticate* privilege you can view the objects controlled. Optionally you can remove the selected object as a Trustee.

AD Trustees with invalid (orphaned) SIDs and cleanup

[badsid03.dsr]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root for all accounts that have trustees with unresolved/invalid SIDs.

Typically, an invalid SID is an object that has been deleted from the Active Directory. The SID remains in the object's ACL because Active Directory has no back-linking ability to clean up SIDs after the object that owned the SID is deleted. This means the SID would stay in the selected object's ACL forever if you did not clean it up. This has both security and performance implications.

You can optionally remove trustees with an unresolved/invalid SID.

AD Trustees with 'Send As' privilege

[find_sa1.dsr]

Searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root that have the *Send As* privilege over other objects. If you search via the DNS Domain Root option the selected Domain Root and all child domains are automatically searched.

For each object found with the *Send As* privilege you can view the objects controlled. Optionally you can remove the selected object as a Trustee.

Dir/File Permissions and Owner

[WalkFSACLOwner2.dsr]

Searches from the selected Windows Share or directory (folder) path for all file system objects and lists the following details for each object found:

- Owner Name
- Trustees for the Object
- Permission Type (Allow/Deny), Description, Inheritance Status

Dir/File Permissions and Owner (OTF)

[WalkFSACLOwner_OTF2.dsr]

Searches from the selected Windows Share or directory (folder) path for all file system objects and lists the following details for each object found:

- Owner Name
- Trustees for the Object
- Permission Type (Allow/Deny), Description, Inheritance Status

Once you select the Windows File System Path to search the applet will prompt you for a filename to save the output to and then automatically minimize itself and will return once finished searching. If you would like to stop the applet, click on its System Tray button and you will be prompted to cancel or continue the search.

OTF is our shorthand for *Output To File*. Applets can be defined as OTF with the **Designer**. Please note that all search results will be written to the output file you specified.

Dir/File System Objects with a NULL ACL (no access restrictions)

[FSFindNullAc12.dsr]

Searches from the selected Windows Share or directory (folder) path for all file system objects where the ACL is NULL.

The (no access restrictions) designation means all users have full control over the objects that are reported. This has major security implications. A null ACL should not be confused with an empty ACL. An empty ACL is a properly allocated and initialized ACL containing no access-control entries (ACEs). An empty ACL grants no access to the object it is assigned to.

ACL stands for "Access Control List" and is sometimes pronounced "AKL".

Dir/File System Objects with a NULL ACL (no access restrictions) OTF

[FSFindNullAcl_OTF2.dsr]

Searches from the selected Windows Share or directory (folder) path for all file system objects where the ACL is NULL.

Once you select the Windows File System Path to search the applet will prompt you for a filename to save the output to and then automatically minimize itself and will return once finished searching. If you would like to stop the applet, click on its System Tray button and you will be prompted to cancel or continue the search.

The (no access restrictions) designation means all users have full control over the objects that are reported. This has major security implications. A null ACL should not be confused with an empty ACL. An empty ACL is a properly allocated and initialized ACL containing no access-control entries (ACEs). An empty ACL grants no access to the object it is assigned to.

ACL stands for "Access Control List" and is sometimes pronounced "AKL".

OTF is our shorthand for Output To File. Applets can be defined as OTF with the **Designer**. Please note that all search results will be written to the output file you specified.

Dir/File Trustees (users and groups)

[findFStrustee.dsr]

Searches and reports on trustees of any type on all files and directories in the selected Windows Share or directory (folder) path. Trustees with explicit and/or inherited permissions can be reported separately or in a single list. Results returned include the number of objects the trustees control and you can view a detailed list of file system objects where the trustee has privileges and the privilege level.

Optionally, the trustee can be removed from the ACL of selected file system objects.

Dir/File Trustees (users and groups) OTF

[findFStrustee_OTF.dsr]

Searches and reports on trustees of any type on all files and directories in the selected Windows Share or directory (folder) path. Trustees with explicit and/or inherited permissions can be reported separately or in a single list. Results returned include the number of objects the trustees control.

Once you select the Windows File System Path to search the applet will prompt you for a filename to save the output to and then automatically minimize itself and will return once finished searching. If you would like to stop the applet, click on its System Tray button and you will be prompted to cancel or continue the search.

OTF is our shorthand for *Output To File*. Applets can be defined as OTF with the **Designer**. Please note that all search results will be written to the output file you specified.

Dir/File Trustees w/ Admin privileges (users and groups)

[`fsadmn3.dsr`]

Searches and reports on trustees of any type on all files and directories in the selected Windows Share or directory (folder) path that have administrative privileges over the scanned file system objects. Trustees with explicit and/or inherited permissions can be reported separately or in a single list. Results returned include the number of objects the trustees control and you can view a detailed list of file system objects where the trustee has privileges and the privilege level.

Optionally, the trustee can be removed from the ACL of selected file system objects.

Dir/File Trustees w/ Admin privileges (users and groups) OTF

[`fsadmn_OTF3.dsr`]

Searches and reports on trustees of any type on all files and directories in the selected Windows Share or directory (folder) path that have administrative privileges over the scanned file system objects. Trustees with explicit and/or inherited permissions can be reported separately or in a single list. Results returned include the number of objects the trustees control.

Once you select the Windows File System Path to search the applet will prompt you for a filename to save the output to and then automatically minimize itself and will return once finished searching. If you would like to stop the applet, click on its System Tray button and you will be prompted to cancel or continue the search.

OTF is our shorthand for *Output To File*. Applets can be defined as OTF with the **Designer**. Please note that all search results will be written to the output file you specified.

Dir/File Trustees w/ Admin privileges (users)

[`fsadmnu3.dsr`]

Searches and reports on trustees that are users on all files and directories in the selected Windows Share or directory (folder) path that have administrative privileges over the scanned file system objects. User trustees with explicit and/or inherited permissions can be reported separately or in a single list. Results returned include the number of objects the user trustees control and you can view a detailed list of file system objects where the user trustee has privileges and the privilege level.

Optionally, the user trustee can be removed from the ACL of selected file system objects.

The (user) designation means only trustees that are user objects will be found and reported; all file system objects they control will be reported regardless of object type.

Dir/File Trustee w/ Admin privileges (users) OTF

[fsadmnu_OTF3.dsr]

Searches and reports on user trustees on all files and directories in the selected Windows Share or directory (folder) path that have administrative privileges over the scanned file system objects. User trustees with explicit and/or inherited permissions can be reported separately or in a single list. Results returned include the number of objects the trustees control and you can view a detailed list of file system objects where the trustee has privileges and the privilege level.

Once you select the Windows File System Path to search the applet will prompt you for a filename to save the output to and then automatically minimize itself and will return once finished searching. If you would like to stop the applet, click on its System Tray button and you will be prompted to cancel or continue the search.

The (user) designation means only trustees that are user objects will be found and reported; all file system objects they control will be reported regardless of object type.

OTF is our shorthand for *Output To File*. Applets can be defined as OTF with the **Designer**. Please note that all search results will be written to the output file you specified.

Dir/File Trustees w/ invalid (orphaned) SID

[fsadmnsid3.dsr]

Searches and reports on trustees that have an unresolved/invalid SID on all files and directories in the selected Windows Share or directory (folder) path that have *any privileges* over the scanned file system objects. Trustees that have an unresolved/invalid SID with explicit and/or inherited permissions can be reported separately or in a single list. Results returned include the number of objects the trustees control and you can view a detailed list of file system objects where the trustee has privileges and the privilege level.

Typically, an invalid SID is an object that has been deleted from the Active Directory. The SID remains in the object's ACL because Active Directory has no back-linking ability to clean up SIDs after the object that owned the SID is deleted. This means the SID would stay in the selected object's ACL forever if you did not clean it up. This has both security and performance implications.

You can optionally remove trustees with an unresolved/invalid SID.

Dir/File Trustees w/ invalid (orphaned) SID (OTF)

[fsadmnsID_OTF3.dsr]

Searches and reports on trustees that have an unresolved/invalid SID on all files and directories in the selected Windows Share or directory (folder) path that have *any privileges* over the scanned file system objects. Trustees that have an unresolved/invalid SID with explicit and/or inherited permissions can be reported separately or in a single list. Results returned include the number of objects the trustees control and you can view a detailed list of file system objects where the trustee has privileges and the privilege level.

Once you select the Windows File System Path to search the applet will prompt you for a filename to save the output to and then automatically minimize itself and will return once finished searching. If you would like to stop the applet, click on its System Tray button and you will be prompted to cancel or continue the search.

Typically, an invalid SID is an object that has been deleted from the Active Directory. The SID remains in the object's ACL because Active Directory has no back-linking ability to clean up SIDs after the object that owned the SID is deleted. This means the SID would stay in the selected object's ACL forever if you did not clean it up. This has both security and performance implications.

OTF is our shorthand for *Output To File*. Applets can be defined as OTF with the **Designer**. Please note that all search results will be written to the output file you specified.

Directory Permissions and Owner

[WalkFSACLOwnerDIR2.dsr]

Searches from the selected Windows Share or directory (folder) path for all directories and lists the following details for each directory:

- Owner Name
- Trustees for the directory
- Permission Type (Allow/Deny), Description, Inheritance Status

Directory Permissions and Owner (OTF)

[WalkFSACLOwner_OTFdir2.dsr]

Searches from the selected Windows Share or directory (folder) path for all directories and lists the following details for each directory:

- Owner Name
- Trustees for the directory
- Permission Type (Allow/Deny), Description, Inheritance Status

Once you select the Windows File System Path to search the applet will prompt you for a filename to save the output to and then automatically minimize itself and will return once finished searching. If you would like to stop the applet, click on its System Tray button and you will be prompted to cancel or continue the search.

OTF is our shorthand for *Output To File*. Applets can be defined as OTF with the **Designer**. Please note that all search results will be written to the output file you specified.

Directory Trustees (users and groups)

[findFSDirTrustee.dsr]

Searches and reports on trustees of any type on *directories only* in the selected Windows Share or directory (folder) path. Trustees with explicit and/or inherited permissions can be reported separately or in a single list. Results returned include the number of directories the trustees control and you can view a detailed list of file system directories where the trustee has privileges and the privilege level.

Optionally, the trustee can be removed from the ACL of selected file system directory objects.

Directory Trustees (users and groups) OTF

[findFSDirTrustee_OTF.dsr]

Searches and reports on trustees of any type on *directories only* in the selected Windows Share or directory (folder) path. Trustees with explicit and/or inherited permissions can be reported separately or in a single list. Results returned include the number of objects the trustees control.

Once you select the Windows File System Path to search the applet will prompt you for a filename to save the output to and then automatically minimize itself and will return once finished searching. If you would like to stop the applet, click on its System Tray button and you will be prompted to cancel or continue the search.

OTF is our shorthand for *Output To File*. Applets can be defined as OTF with the **Designer**. Please note that all search results will be written to the output file you specified.

Directory Trustees w/ Admin privileges (users and groups)

[fsadmnd3.dsr]

Searches and reports on trustees of any type on *directories only* in the selected Windows Share or directory (folder) path that have administrative privileges over the scanned file system directories. Trustees with explicit and/or inherited permissions can be reported separately or in a single list. Results returned include the number of directories the trustees control and you can view a detailed list of file system directories where the trustee has privileges and the privilege level.

Optionally, the trustee can be removed from the ACL of selected file system directory objects.

Directory Trustees w/ Admin privileges (users and groups) OTF

[fsadmnd_OTF3.dsr]

Searches and reports on trustees of any type on *directories only* in the selected Windows Share or directory (folder) path that have administrative privileges over the scanned file system directory objects. Trustees with explicit and/or inherited permissions can be reported separately or in a single list. Results returned include the number of objects the trustees control.

Once you select the Windows File System Path to search the applet will prompt you for a filename to save the output to and then automatically minimize itself and will return once finished searching. If you would like to stop the applet, click on its System Tray button and you will be prompted to cancel or continue the search.

OTF is our shorthand for *Output To File*. Applets can be defined as OTF with the **Designer**. Please note that all search results will be written to the output file you specified.

Directory Trustees w/ Administrative privileges (users)

[**fsadmndu3.dsr**]

Searches and reports on trustees that are users on *directories only* in the selected Windows Share or directory (folder) path that have administrative privileges over the scanned file system directory objects. User trustees with explicit and/or inherited permissions can be reported separately or in a single list. Results returned include the number of directory objects the user trustees control and you can view a detailed list of file system directory objects where the user trustee has privileges and the privilege level.

Optionally, the user trustee can be removed from the ACL of selected file system directory objects.

The (user) designation means only trustees that are user objects will be found and reported; all file system directory objects they control will be reported.

Directory Trustees w/ Admin privileges (users) OTF

[**fsadmndu_OTF3.dsr**]

Searches and reports on user trustees on *directories only* in the selected Windows Share or directory (folder) path that have administrative privileges over the scanned file system directory objects. User trustees with explicit and/or inherited permissions can be reported separately or in a single list. Results returned include the number of directory objects the trustees control and you can view a detailed list of file system directory objects where the trustee has privileges and the privilege level.

Once you select the Windows File System Path to search the applet will prompt you for a filename to save the output to and then automatically minimize itself and will return once finished searching. If you would like to stop the applet, click on its System Tray button and you will be prompted to cancel or continue the search.

The (user) designation means only trustees that are user objects will be found and reported; all file system directory objects they control will be reported.

OTF is our shorthand for *Output To File*. Applets can be defined as OTF with the **Designer**. Please note that all search results will be written to the output file you specified.

Directory Trustees w/ invalid (orphaned) SID

[**fsadmndSID3.dsr**]

Searches and reports on trustees that have an unresolved/invalid SID on *directories only* in the selected Windows Share or directory (folder) path that have *any privileges* over the scanned file system objects. Trustees that have an unresolved/invalid SID with explicit and/or inherited permissions can be reported separately or in a single list. Results returned include the number of objects the trustees control and you can view a detailed list of file system objects where the trustee has privileges and the privilege level.

Typically, an invalid SID is an object that has been deleted from the Active Directory. The SID remains in the object's ACL because Active Directory has no back-linking ability to clean up SIDs after the object that owned the SID is deleted. This means the SID would stay in the selected object's ACL forever if you did not clean it up. This has both security and performance implications.

You can optionally remove trustees with an unresolved/invalid SID.

Directory Trustees w/ invalid (orphaned) SID (OTF)

[fsadmndSID_OTF3.dsr]

Searches and reports on trustees that have an unresolved/invalid SID on *directories only* in the selected Windows Share or directory (folder) path that have *any privileges* over the scanned file system objects. Trustees that have an unresolved/invalid SID with explicit and/or inherited permissions can be reported separately or in a single list. Results returned include the number of objects the trustees control and you can view a detailed list of file system objects where the trustee has privileges and the privilege level.

Once you select the Windows File System Path to search the applet will prompt you for a filename to save the output to and then automatically minimize itself and will return once finished searching. If you would like to stop the applet, click on its System Tray button and you will be prompted to cancel or continue the search.

Typically, an invalid SID is an object that has been deleted from the Active Directory. The SID remains in the object's ACL because Active Directory has no back-linking ability to clean up SIDs after the object that owned the SID is deleted. This means the SID would stay in the selected object's ACL forever if you did not clean it up. This has both security and performance implications.

OTF is our shorthand for *Output To File*. Applets can be defined as OTF with the **Designer**. Please note that all search results will be written to the output file you specified.

File System Objects where Permission Inheritance is Blocked

[FSFindInheritanceBlocked2.dsr]

Searches from the selected Windows Share or directory (folder) path for all file system objects where permission inheritance has been specifically removed. The report lists the following details for each object found:

- Owner Name
- Trustees for the Object
- Permission Type (Allow/Deny), Description, Inheritance Status

For any folders or files found, the Trustees shown are the only accounts with access.

File System Objects where Permission Inheritance is Blocked (OTF)

[FSFindInheritanceBlocked_OTF2.dsr]

Searches from the selected Windows Share or directory (folder) path for all file system objects where permission inheritance has been specifically removed. The report lists the following details for each object found:

- Owner Name
- Trustees for the Object
- Permission Type (Allow/Deny), Description, Inheritance Status

For any folders or files found, the Trustees shown are the only accounts with access.

Once you select the Windows File System Path to search the applet will prompt you for a filename to save the output to and then automatically minimize itself and will return once finished searching. If you would like to stop the applet, click on its System Tray button and you will be prompted to cancel or continue the search.

OTF is our shorthand for *Output To File*. Applets can be defined as OTF with the **Designer**. Please note that all search results will be written to the output file you specified.

FSMO Roles for selected Domain

[fsmo2.dsr]

Lists the Flexible Single Master Operation (FSMO) server roles for domain controllers. FSMO roles reported include:

- Domain Naming Master
- Infrastructure Master
- PDC Emulator Master
- RID Master
- Schema Master

List GPOs by Domain

[gpodoc2.dsr]

Lists all GPOs defined at each DNS Domain Root. Details include:

- GPO name
- GUID
- Path
- Status (ENABLED/DISABLED)
- Version
- When Created
- When Changed

Manage AD Object Permission Inheritance

[listacl_inherit.dsr]

Searches from the selected container or Organizational Unit for all Active Directory objects and documents whether permission inheritance has been specifically removed or not . The report lists the following details for each object found:

- Object's Distinguished Name
- Whether or not inheritance is blocked
- Total number of Access Control Entries (ACEs), along with a count of explicit and inherited permissions
- Owner Name
- Number of allow and deny ACEs
- Object class (user, group, computer, etc.)

You can modify objects' inheritance with three buttons to the right of the list. The first option will prevent inheritance of the parent container's permissions, and delete the inherited permissions. The second will prevent inheritance, but make an explicit copy of any permissions that would normally be inherited. The third option will enable inheritance, causing the parent container's permissions to be applied automatically to the selected child object.

There is a fourth button that displays a list of the selected object's ACEs, showing each Trustee's Distinguished Name, permissions granted, whether or not the ACE applies, to which object the ACE applies, and whether or not it was inherited.

Shares permissions on Servers and Workstations

[NTSharePerms2.dsr]

Lists all Windows file system shares on the selected computer. This applet displays trustees and granted share permissions for each share on the selected computer.

Category: Query and Search AD

The applets available from this menu category are generally useful for querying and documenting your Active Directory forest and Windows Domains. In the sections that follow you will find the title of each applet, its specific filename and description.

Computer Accounts with no Password Reset for past 45 days + cleanup

[machine_pwd_set_time1.dsr]

This applet searches for computer objects within a specific Active Directory container branch or DNS Domain Root where the Password Last Set attribute is greater than 45 days. If you search via the DNS Domain Root option the selected Domain Root and all child domains are automatically searched. The applet reports the Date/Time the Password for the computer account was last set. An action button to delete the selected computer account is provided to aid in the cleanup process.

Document Computer Details

[wstndoc3.dsr]

This applet shows details of all Computer objects in a selected container.

Details shown for each Computer found include:

- Creation Date
- Date of last update
- Operating System name
- Operating System version
- Operating System Service Pack level
- Indication whether or not the selected computer is a Domain Controller

Document Group Membership

[grpdoc1c.dsr]

This applet will document Group Membership. This applet will search for all groups from a selected starting point or you can list groups in a selected container. Details include:

- Group Type
- Creation Date
- Number of members

Additionally, you can list an individual group's membership. Details shown include:

- Member AD/LDAP name
- Primary Email Address
- Department
- Account Expiration Date

Options such as the List Groups in selected domain only button list only the group's membership but no details about the members. The advantage of such a query is that it produces results more quickly than the more detailed reports.

Document Group Membership #2

[grpdoc4a.dsr]

This applet will document Group Membership. This applet will search for all groups from a selected starting point. Details include:

- Number of members
- Description
- Number of members that are groups

Membership details for the selected group are displayed in a second list in the same window. Attributes shown include:

- Latest Logon Time (using the lastLogon attribute)
- Telephone Number
- Whether or not Logon Hours are defined

The Latest Logon Time shown is determined by scanning all Domain Controllers where the user object is defined.

Because scanning the value of the lastLogon attribute can require a noticeable amount of time you can edit the applet in the **Designer** to use one of the following two alternate attribute values for determining the approximate last date of last logon:

- Scanning the object's **pwdLastSet** attribute
- Scanning the object's **lastLogonTimeStamp** attribute: This attribute is only available on Windows 2003 Domain Functional Mode Domain Controllers and, by default, this attribute is current within the past 7 days.

NOTE: This applet can be edited in the **Designer** to change the membership attributes displayed.

Document Groups that are members

[grpdoc3a.dsr]

This applet will find Groups that have Groups as members. This applet will search for all groups from a selected starting point. Details include:

- Number of members
- Description

Membership details for the selected group are displayed in a second list in the same window. Attributes shown include:

- Description
- Group Type

NOTE: This Applet can be edited in the **Designer** to change the membership attributes displayed.

Enter your own LDAP Query – optionally search via Global Catalog

[hd_ldap_s3.dsr]

This applet searches for Active Directory objects within a specific Active Directory container branch. The search is performed via a user-specified LDAP query string. LDAP queries can be performed via the Global Catalog (GC) or directly on the Active Directory database. Included buttons are Edit Department, View All Attributes of selected Object, Delete Selected Objects, and Disable Selected User Accounts.

Find Duplicate AD Object Names

[dupobj2.dsr]

This applet will find AD objects with the same common name (CN= portion). This applet will search for objects with duplicate names from a selected starting point. Details include:

- Object's Creation Time
- User principal name (format: name@domain.local) (for user objects only)

When you run this applet it will return the names of all objects in the selected Active Directory path. Once complete you click the **Find Duplicate Object Names** button and it will reduce the list to just those objects with redundant "CN=".

Find User Object Ownership

[docowner1.dsr]

This applet displays the owner of each user object found in the selected Active Directory path. Additional attributes shown for each user found include:

- User's Email Address
- Profile Path
- Home Directory
- GUID

This applet can be edited in the **Designer** to include different object classes and attributes.

Find Users created in past X days

[newusers2.dsr]

This applet will find User accounts created in the runtime-specified time period. This applet will search for new users from a selected starting point. For each user found details returned include:

- Account name
- Account creation time
- Account SAM Name (pre-Active Directory name)
- User principal name (UPN)

Last Logon Date and Time for Computer Accounts

[machine_last_logon2.dsr]

This applet searches for computer objects within a specific Active Directory container branch or DNS Domain Root. If you search via the DNS Domain Root option the selected Domain Root and all child domains are automatically searched. The applet reports the Date/Time the computer account last logged onto the selected domain controller.

Raw AD Object View

[rawad3.dsr]

This applet displays a *raw view* of Active Directory Objects. The raw view is the object plus all of its Active Directory attributes and values. This viewer is like performing an x-ray on your Active Directory objects.

Simple AD User Details View

[user2.dsr]

This applet will search for users from the selected Active Directory path and list the following details for each user found:

- User Account Control Settings
- Group Membership
- Email Addresses
- Direct Reports
- Telephone Numbers

This applet can be edited in **Designer** to modify the attributes to list.

User Creation Time Report

[usercre1.dsr]

This applet will search for users from the selected Active Directory path and display the following details for each user found:

- Creation Time
- Latest Logon Time (using the lastLogon attribute)
- Password Age (in days)

The Latest Logon Time shown is determined by scanning all Domain Controllers where the user object is defined.

Because scanning the value of the lastLogon attribute can require a noticeable amount of time you can edit the applet in the **Designer** to use one of the following two alternate attribute values for determining the approximate last date of last logon:

- Scanning the object's **pwdLastSet** attribute
- Scanning the object's **lastLogonTimeStamp** attribute: This attribute is only available on Windows 2003 Domain Functional Mode Domain Controllers and, by default, this attribute is current within the past 7 days.

Category: HelpDesk Examples

Many of the applets in the **Console** can be used as HelpDesk applets. Those applets available from this menu category are purposefully designed to showcase HelpDesk samples. In the sections that follow, you will find the title of each applet, its specific filename, and description.

With the **Designer**, you can save any DSRAZOR for Windows applet as a stand-alone EXE file that can be deployed via any method you require.

Additionally, with the **Designer** you can modify any of these samples to better suit your requirements.

Begin View in Helpdesk Current User's Context

[aduser1.dsr]

This applet demonstrates how an applet can be configured to begin the Active Directory view from the container where the local user's Active Directory account is defined.

For instance, if the helpdesk user account is:

```
CN=User1,OU=Helpdesk,OU=Support,DC=Acme,DC=Local
```

The first container shown in the applet view is:

```
OU=Helpdesk,OU=Support,DC=Acme,DC=Local
```

To complete the demonstration, this applet lists all groups that exist in the helpdesk user's container. There are also example buttons including Create User, Disable and Rename, Set User Password and Set Account Expiration Date.

Group Membership Management via Drag-n-Drop

[grpm_dd1.dsr]

This applet demonstrates a unique interface for the administration of group membership via drag-and-drop. This applet will search for all groups from a selected starting point or all groups in a selected container. The groups are displayed as well as membership for each group. There is another list displaying all containers and all objects within those containers. The interface allows you to drag-and-drop these objects onto a listed group. You can also press a button to add the selected user to the selected group. To remove a member from a group, right click on the member and choose remove from the breakout menu.

Pass AD Attribute as Parameter to EXE

[pass2a.dsr]

This applet demonstrates how you can easily pass almost any Active Directory attribute as a parameter to an EXE file. This example passes the user's Logon Name to `NOTEPAD.EXE`.

Remote Assist Computer

[wstn_ra2.dsr]

This applet demonstrates how you can use DSRAZOR for Windows to launch an unsolicited remote assistance session using `MSTSC.EXE`. Details shown for each computer found include:

- Creation Date
- Date of last update
- Operating System name
- Operating System version
- Operating System Service Pack level
- Indication whether or not the selected computer is a Domain Controller

Update User Details

[editUserDetails3.dsr]

This applet searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root for all user accounts. The applet demonstrates an interface to modify specific user attribute values and a button to apply the changes made. User details include:

- First Name
- Middle Initial
- Last Name
- Description
- Office Phone
- Fax
- Cell Phone
- Home Phone
- Company
- Title
- Department
- Office

This applet can be modified using the **Designer** to include the attributes you require, including any custom attributes you may have added to the Active Directory Schema.

Update User Details (tabbed)

[editUserDetails_tab3.dsr]

This applet searches for Active Directory accounts within a specific Active Directory container branch for user accounts. The applet demonstrates a tab control interface to modify specific user attribute values and a button to apply the changes made. User details include:

- Display Name
- First Name
- Middle Initial
- Last Name
- Office Phone
- Fax
- Cell Phone
- Home Phone
- Company
- Title
- Department
- Office

This applet can be modified using the Designer to include the attributes you require, including any custom attributes you may have added to the Active Directory Schema.

User “Self-Update” of selected attributes

[editPersonalInformation2.dsr]

This applet runs in the context of the logged-on user. It allows users to modify their own selected attributes. Attributes include:

- Home Phone
- Pager
- Mobile Phone
- Vehicle License
- Office

This applet can be modified using the **Designer** to include the attributes you require, including any custom attributes you may have added to the Active Directory Schema.

User Password and Intruder Lockout Reset Helpdesk

[hd_pwdr2a.dsr]

This applet demonstrates an example Helpdesk system. This applet searches for Active Directory accounts within an Active Directory DNS Domain Root for user accounts by name. You can use an asterisk (*) to perform wildcard matching. For instance B* will match all users where the name begins with the letter “B”. Additionally, *eve* will match any name that contains the letters “eve”.

Finally, *th will match names ending with “th”. Search results are filtered to exclude Administrative users to demonstrate the use of rules. The results include attributes such as:

- SAM Account
- Lockout Status
- Last Name
- Telephone

This applet can be modified using the **Designer** to include the attributes you require, including any custom attributes you may have added to the Active Directory Schema.

Several buttons are included as examples. The buttons allow you to Set User Password, Reset Intruder Lockout, Assign Single-Use Password, Edit and Update the Phone Number and View User Account Flags.

User Password and Intruder Lockout Reset Helpdesk – Specify Containers

[hd_pwdr3a.dsr]

This applet demonstrates an example Helpdesk system. This applet searches for Active Directory accounts within pre-specified (modifiable using the **Designer**) Active Directory containers for user accounts by name. You can use an asterisk (*) to perform wildcard matching. For instance B* will match all users where the name begins with the letter "B". Additionally, *eve* will match any name that contains the letters "eve". Finally, *th will match names ending with "th". Search results are filtered to exclude Administrative users to demonstrate the use of rules. The results include attributes such as:

- SAM Account
- Lockout Status
- Last Name
- If the user has an Exchange Mailbox

This applet can be modified using the **Designer** to include the attributes you require, including any custom attributes you may have added to the Active Directory Schema.

Several buttons are included as examples. The buttons allow you to Set User Password, Reset Intruder Lockout, Assign Single-Use Password, Edit and Update the Last Name and Enable User Account.

Category: AD User Maintenance

The applets available from this menu category are generally useful for maintaining your Active Directory user accounts. In the sections that follow you will find the title of each applet, its specific filename and description.

Add Exchange Mailbox to Selected Accounts (Exchange 2000/2003)

[`addexch2.dsr`]

This applet searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root for all user accounts that do not have an associated Exchange Mailbox. This applet allows you to create the mailbox by selecting a user and the Exchange Information Store where the mailbox should reside.

Add Exchange Mailbox to Selected Accounts (Exchange 2007/2010)

[`x64_exch7_mb_add.dsr`]

This applet searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root for all user accounts that do not have an associated Exchange Mailbox. This applet allows you to create the mailbox by selecting a user and the Exchange Mailbox Database where the mailbox should reside.

Usage Note: Path Modifications

This note describes how to use the Modify Path Attribute function used within several DSRAZOR for Windows applets. This function utilizes a Universal Naming Convention (UNC) format where the components of the UNC are broken into three separate parts: server, share, and path, as shown in the following screenshot.

Modify Path Attribute

Modify Object:
CN=Charlie Brown,CN=Users,DC=dsrazor,DC=local

Attribute:
homeDirectory

Note:
Path attribute is presumed to be a string value in the format:
\\Server\Share\Path\...
This modify function can be used to establish a new value for objects that do not already have the a value for the selected attribute. To do so, all fields below must be filled in. The checkbox value will be ignored for such objects.

Important: Modifications will only be made to those path components where the fields have values. Any path components where the field remains empty will not have any changes made.

New Server Name:
 (Slashes are not required)

New Share Name:
 (Slashes are not required)

New Path:

Check here if the last component of the Path is specific to the object (such as a user name) and must be preserved.

Cancel Change Path

Modify Path Attribute Template

Each of the respective parts of the UNC can be changed without entering the entire UNC using this methodology. For example, if the share and path to the users home directory will remain the same but the server name will change, only the server name needs to be entered to perform the required modification.

NOTE: You cannot enter the complete UNC path in the New Path field; you must enter each UNC component in the appropriate field.

Change Home Directory

[chghd2.dsr]

This applet will search Active Directory from the path you select for all user objects with a home directory defined.

For those users found you can choose to modify their home directory path in Active Directory only *or* you can choose to modify the users' home directory path in Active Directory *and* create the new path *and* assign the user as the home directory path owner and give full control of the directory to its user.

This applet can be modified in the **Designer** to find users without a home directory path so you can establish one for any such users found.

Change Manager for Users

[**organization.dsr**]

This applet will allow you to drill down through your Active Directory structure and select the user you would like to modify. Once a user is chosen you have the ability to change the Title, Department, Company, and Manager fields for that user. To assign a new Manager press the **Search for Manager** button and enter a search query to locate the desired Manager's user account. Highlight the Manager in the ListView and press the **Make Selected User the Manager** button. The new manager will be reflected in the display after a 3-second refresh period.

Change Profile Path

[**chgpp2.dsr**]

This applet will search Active Directory from the path you select for all user objects with a profile path defined.

For those users found you can choose to modify any portion of their profile path.

This applet can be modified in the **Designer** to find users without a profile path so you can establish one for any such users found.

Copy Existing Group

[**CopyGroup.dsr**]

This applet will copy an existing group, including all of its membership. By hitting the Next button, you can display membership in all groups created in the past day. You can copy the membership of any Distribution List or Security Group easily, avoiding potential errors that can occur when an IT employee is tasked with manually copying membership.

Copy Existing User

[CopyUser.dsr]

This applet will copy an existing User object, including many more attributes than the native tools copy by default. Copied attributes include the address, telephone number, and numerous other attributes that are not natively copied. Please note that attributes that are typically unique to a given user, such as mobile phone number and the user's name, will not be copied, which will help prevent mistaken information being copied into your Active Directory.

Create Users from a Template

[UserTemplate1.dsr]

This powerful applet demonstrates how to use DSRAZOR to force attributes you select to be populated before the user will be created. By using this applet as a base, you can pre-populate a number of fields based on your company's organization. The provided example allows creation of Software Engineers, Hardware Engineers, Marketing Employees, Sales Employees, HR Employees, and IT Employees.

This applet can be modified using the **Designer** to include the user types and attributes you require, including any custom attributes you may have added to the Active Directory Schema. You can create templates for classes of users you define, and can filter available groups for group membership so, for instance, engineers at your company can't be added to your sales groups.

This user provisioning applet is an example of how to streamline and make user creation tasks more uniform within your organization. Highlights include: automatic field completion (UPN Login name and Pre-AD Login name), data masks to ensure data is entered in a required format, dropdown lists to ensure data is consistently entered, automatic assignment of group membership, selection of Home Directory location, and drag-and-drop group management. By pre-selecting default values for departmentally specific fields, you can save time and standardize account creation for very different classes of users.

Create Users with Required Attributes

[cura04c.dsr]

This applet demonstrates how to use DSRAZOR to force attributes you select to be populated *before* the user will be created. This applet allows you to ensure user objects are created with the attributes you or your organization requires.

This applet can be modified using the **Designer** to include the attributes you require, including any custom attributes you may have added to the Active Directory Schema.

This user provisioning applet is an example of how to streamline and make user creation tasks more uniform within your organization. Highlights include: automatic field completion (UPN Login name and Pre-AD Login name), data masks to ensure data is entered in a required format, dropdown lists to ensure data is consistently entered, automatic population of an attribute from contents of other attributes, and drag-and-drop group membership.

Create Users with Required Attributes + Exchange 2000/2003 Mailbox

[cura04exc.dsr]

This applet demonstrates how to use DSRAZOR to force attributes you select to be populated before the user will be created. This applet allows you to ensure user objects are created with the attributes you or your organization requires.

This applet can be modified using the **Designer** to include the attributes you require, including any custom attributes you may have added to the Active Directory Schema.

This user provisioning applet is an example of how to streamline and make user creation tasks more uniform within your organization. Highlights include: automatic field completion (UPN Login name and Pre-AD Login name), data masks to ensure data is entered in a required format, dropdown lists to ensure data is consistently entered, automatic population of an attribute from contents of other attributes, drag-and-drop group management, and Exchange Mailbox creation.

Create Users with Required Attributes + Exchange 2007/2010 Mailbox

[x64_exch7_mb_cura.dsr]

This applet demonstrates how to use DSRAZOR to force attributes you select to be populated before the user will be created. This applet allows you to ensure user objects are created with the attributes you or your organization requires.

This applet can be modified using the **Designer** to include the attributes you require, including any custom attributes you may have added to the Active Directory Schema.

This user provisioning applet is an example of how to streamline and make user creation tasks more uniform within your organization. Highlights include: automatic field completion (UPN Login name and Pre-AD Login name), data masks to ensure data is entered in a required format, dropdown lists to ensure data is consistently entered, automatic population of an attribute from contents of other attributes, drag-and-drop group management, and Exchange Mailbox creation.

Delete Exchange Mailbox for Selected Accounts (Exchange 2000/2003)

[delexch2.dsr]

This applet searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root for all user accounts. This applet allows you to delete the mailbox by selecting a user and clicking the Delete Mailbox button. User Details include:

- Display Name
- Exchange Mailbox Status

Delete Exchange Mailbox for Selected Accounts (Exchange 2007/2010)

[x64_exch7_mb_del.dsr]

This applet searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root for all user accounts. This applet allows you to delete the mailbox by selecting a user and clicking the Delete Mailbox button. User Details include:

- Display Name
- Exchange Mailbox Status

Delete Exchange Mailboxes from CSV File

[import_removeExchange1.dsr]

This applet deletes Exchange Accounts for users from a comma-delimited file. The file name must use a *.**CSV** extension (Comma Separated Value). The file must be in the following format:

```
"User", "<ignored text>",  
"User", "<ignored text>",
```

where *User* is the account name (Common Name or Distinguished Name), and the second column is a place holder. Note that each line of data requires a trailing comma. For an example, see **importde.csv** in the DSRAZOR for Windows install directory.

The following instructions describe how to use the **Designer** to edit this applet to accept data in a different format. Perform the following procedure to import using a different file format:

1. Open the applet with the **Designer**. The Select Window dialog page is displayed. You can do this by right-clicking on the applet's name while viewing it in the **Console**.
2. Select **Automatically Remove Exchange Mailbox** and click **OK**. The selected window is displayed.
3. Right click over the white rectangle in the window to reveal the data element screen for editing.
4. Select the first entry that is highlighted:

```
Existing User to Delete Exchange Mailbox: | | AD:IMPORT:Receive  
CSV file, ["data",] for Mass User [or Other Object] Create -  
Connected to: Use Import function to remove Exchange Mailbox from  
Existing Accounts...
```

Click the **Edit...** button.

5. Select the file format to be imported. Click **OK**.
6. The **Update Connected Controls** page is displayed. Click **OK**.
7. You will be returned to the **ListView Columns** page. Click **OK**.
8. Save the applet and then close **Designer**.

Edit Single-Valued Attribute for Selected Accounts

[sved_text4.dsr]

This applet searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root for all user accounts. You then select one or more user accounts and update the specified attribute for all selected users. The applet is configured to modify the Fax Number attribute but can be changed in the Designer to modify any single-valued attribute in your Active Directory schema. There are buttons that enable you to prepend text, append text, or replace the value of the fax number.

Exchange Mailbox GUID and Mailbox Store (Exchange 2000/2003)

[exchguid1.dsr]

This applet searches for Active Directory accounts within a specific Active Directory container branch or DNS Domain Root for all user accounts with an Exchange Mailbox. Report Details include:

- User Canonical Name
- Exchange Mailbox GUID

DSRAZOR for Windows Ready-to-Run Applets

- Mailbox Store

Usage Note: Import Functions

DSRAZOR for Windows import functions are contained in services that accept data in various formats. The format to select depends on the method that the import file was created. The formats accepted include:

- Quote encapsulated with trailing comma. For example:

```
"data1", "data2", "data3",
```

For this format select the service:

```
AD:Import:Receive CSV file,["data",] for MASS USER [or OTHER  
OBJECT] Create
```

- No Quotes, commas ONLY, with trailing comma. For example:

```
data1,data2,data3,
```

For this format select the service:

```
AD:Import:Receive CSV file,[NO Quotes, Commas ONLY] for MASS USER  
[or OTHER OBJECT] Create
```

- EXCEL STYLE – No Quotes, commas only, with no trailing comma. For example:

```
data1,data2,data3
```

For this format select the service:

```
AD:Import:Receive CSV file, EXCEL STYLE [NO Quotes, Commas ONLY,  
No trailing comma] for MASS USER [or OTHER OBJECT] Create
```

It is important to select the proper service for importing the different data types. The service names shown are selected when editing the applet in the Designer. The following ready-to-run applets use these services.

Import AD Password to new or existing accounts

[impuppl1.dsr]

This applet imports users' passwords from a comma-delimited file. The file name must use a *.CSV extension (Comma Separated Value). The file must be in the following format:

```
"User", "password",  
"User", "password",
```

where *User* is the account name (Common Name or Distinguished Name), and *Password* is the user's password to be assigned. Note that each line of data requires a trailing comma. For an example, see **importp.csv** in the DSRAZOR for Windows install directory.

The following instructions describe how to use the **Designer** to edit this applet to accept data in a different format. Perform the following procedure to import using a different file format:

1. Open the applet with the **Designer**. The Select Window dialog page is displayed. You can do this by right-clicking on the applet's name while viewing it in the **Console**.
2. Select **Import new password for users to selected container** and click **OK**. The selected window is displayed.
3. Right click over the white rectangle in the window to reveal the data element screen for editing.
4. Select the first entry that is highlighted:

DSRAZOR for Windows Ready-to-Run Applets

```
Existing User to import new password for: || AD:IMPORT:Receive
CSV file, ["data",] for Mass User [or Other Object] Create -
Connected to: Import new password for Users from CSV...
```

Click the **Edit...** button.

5. Select the file format to be imported. Click **OK**.
6. The **Update Connected Controls** page is displayed. Click **OK**.
7. You will be returned to the **ListView Columns** page. Click **OK**.
8. Save the applet and then close **Designer**.

Import Exchange Contacts from CSV File (Automated) (Exchange 2000-2010)

[import_contact_auto.dsr]

This applet imports contacts from a comma-delimited file and Exchange enables them. The main differences between this applet and the non-automated version are:

1. The CSV file is pre-specified in the Manual Entry Text field for the following service:
Contact Name (auto-create): || AD:IMPORT:AUTO_CREATE:Receive CSV
file, ["data",] for Mass User [or Other Object] Create -
Connected to: Import Contacts into specified Container...
2. There is no button on the second window to initiate the import; it will proceed without requiring user input. Fully automating the container selection on the first window, such as in applet [import_contact_auto1a.dsr], will allow unattended contact creation.

The file name must use a ***.CSV** extension. The file must be in the following format:

```
"Contact", "attribute", "attribute", "attribute",
"Contact", "attribute", "attribute", "attribute",
```

where *Contact* is the account name (Common Name or Distinguished Name), and *Attribute* is any contact attribute in Active Directory. For an example, see **import_contact_auto1.csv** in the DSRAZOR for Windows install directory.

Alternatively, you can remove the targetAddress and the Exchange Org columns in the Designer and in the CSV file to make a contact that is not Exchange enabled. You can then populate the "mail" attribute with an SMTP address if you like.

The following instructions describe how to use the **Designer** to edit this applet to accept data in a different format. Perform the following procedure to import using a different file format:

1. Open the applet with the **Designer**. The Select Window dialog page is displayed. You can do this by right-clicking on the applet's name while viewing it in the **Console**. The Select Window dialog page is displayed.
2. Select **Importing Contacts** and click **OK**. The selected window is displayed.
3. Right click over the white rectangle in the window to reveal the data element screen for editing.
4. Select the first entry that is highlighted:

```
Contact Name (auto-create): || AD:IMPORT:AUTO_CREATE:Receive CSV
file, ["data",] for Mass User [or Other Object] Create -
Connected to: Import Contacts into specified Container...
```

Click the **Edit...** button.

5. Select the file format to be imported. Click **OK**.
6. The **Update Connected Controls** page is displayed. Click **OK**.

DSRAZOR for Windows Ready-to-Run Applets

7. You will be returned to the **List View Columns** page. Click **OK**.
8. Save the applet and then close **Designer**.

Perform the following procedure to change the attributes to be imported:

1. Open the applet in **Designer**. The Select Window dialog page is displayed. You can do this by right-clicking on the applet's name while viewing it in the **Console**. The Select Window dialog page is displayed.
2. Select **Importing Contacts** and click **OK**. The selected window is displayed.
3. Right click over the white rectangle in the window to reveal the data element screen for editing.
4. Select the last user attribute in the list, click **Add**. The Add Column window is displayed.
5. Click the **Search Manual Entry** button.
6. Select the attribute to be imported from the CSV file. If no names appear and you know the name of the attribute you can type it in the manual entry field.
7. Change the column name to be displayed to the right of the **Column Name:** data entry field. Click **OK**. You are returned to the **List View Columns** page.
8. The order of the import fields can be adjusted by selecting the import field then clicking the **Move Up** or **Move Down** buttons. Click **OK**.
9. You will be returned to the **Importing Contacts** page.
10. Save the applet then close the **Designer**.

Import Exchange Contacts from CSV File (Exchange 2000-2010)

[**importcon.dsr**]

This applet imports contacts from a comma-delimited file and Exchange enables them. The file name must use a ***.CSV** extension. The file must be in the following format:

```
"Contact", "attribute", "attribute", "attribute",  
"Contact", "attribute", "attribute", "attribute",
```

where *Contact* is the account name (Common Name or Distinguished Name), and *Attribute* is any contact attribute in Active Directory. For an example, see **importcon.csv** in the DSRAZOR for Windows install directory.

Alternatively, you can remove the targetAddress and the Exchange Org columns in the Designer and in the CSV file to make a contact that is not Exchange enabled. You can then populate the Mail attribute with an SMTP address.

The following instructions describe how to use the **Designer** to edit this applet to accept data in a different format. Perform the following procedure to import using a different file format:

1. Open the applet with the **Designer**. The Select Window dialog page is displayed. You can do this by right-clicking on the applet's name while viewing it in the **Console**. The Select Window dialog page is displayed.
2. Select **Import Contacts Sample** and click **OK**. The selected window is displayed.
3. Right click over the white rectangle in the window to reveal the data element screen for editing.
4. Select the first entry that is highlighted:

```
Contact Name: || AD:IMPORT:Receive CSV file, ["data",] for Mass  
User [or Other Object] Create - Connected to: Import Contacts...
```

DSRAZOR for Windows Ready-to-Run Applets

Click the **Edit...** button.

5. Select the file format to be imported. Click **OK**.
6. The **Update Connected Controls** page is displayed. Click **OK**.
7. You will be returned to the **ListView Columns** page. Click **OK**.
8. Save the applet then close **Designer**.

Perform the following procedure to change the attributes to be imported:

1. Open the applet in **Designer**. The Select Window dialog page is displayed. You can do this by right-clicking on the applet's name while viewing it in the **Console**. The Select Window dialog page is displayed.
2. Select **Import Contacts Sample** and click **OK**. The selected window is displayed.
3. Right click over the white rectangle in the window to reveal the data element screen for editing.
4. Select the last user attribute in the list, click **Add**. The Add Column window is displayed.
5. Click the **Search Manual Entry** button.
6. Select the attribute to be imported from the CSV file. If no names appear and you know the name of the attribute you can type it in the manual entry field.
7. Change the column name to be displayed to the right of the **Column Name:** data entry field. Click **OK**. You are returned to the **ListView Columns** page.
8. The order of the import fields can be adjusted by selecting the import field then clicking the **Move Up** or **Move Down** buttons. Click **OK**.
9. You will be returned to the **Import Contacts Sample** page.
10. Save the applet then close the **Designer**.

Ensure that the data in the CSV file is in the same field order as in the applet.

Import Users + Attributes from CSV File

[**import7.dsr**]

This applet imports users and selected attributes from a comma-delimited file. The file name must use a ***.CSV** extension. The file must be in the following format:

```
"User", "attribute", "attribute", "attribute",  
"User", "attribute", "attribute", "attribute",
```

where *User* is the account name (Common Name or Distinguished Name), and *Attribute* is any user attribute in Active Directory. For an example, see **import7.csv** in the DSRAZOR for Windows install directory.

The following instructions describe how to use the **Designer** to edit this applet to accept data in a different format. Perform the following procedure to import using a different file format:

1. Open the applet with the **Designer**. The Select Window dialog page is displayed. You can do this by right-clicking on the applet's name while viewing it in the **Console**. The Select Window dialog page is displayed.
2. Select **Import users to selected container** and click **OK**. The selected window is displayed.
3. Right click over the white rectangle in the window to reveal the data element screen for editing.
4. Select the first entry that is highlighted:

DSRAZOR for Windows Ready-to-Run Applets

```
User to import: || AD:IMPORT:Receive CSV file, ["data",] for Mass
User [or Other Object] Create - Connected to: Import and selected
attributes from CSV...
```

Click the **Edit...** button.

5. Select the file format to be imported. Click **OK**.
6. The **Update Connected Controls** page is displayed. Click **OK**.
7. You will be returned to the **ListView Columns** page. Click **OK**.
8. Save the applet then close **Designer**.

Perform the following procedure to change the attributes to be imported:

1. Open the applet in **Designer**. The Select Window dialog page is displayed. You can do this by right-clicking on the applet's name while viewing it in the **Console**. The Select Window dialog page is displayed.
2. Select **Import users to selected container** and click **OK**. The selected window is displayed.
3. Right click over the white rectangle in the window to reveal the data element screen for editing.
4. Select the last user attribute in the list, click **Add**. The Add Column window is displayed.
5. Click the **Search Manual Entry** button.
6. Select the attribute to be imported from the CSV file. If no names appear and you know the name of the attribute you can type it in the manual entry field.
7. Change the column name to be displayed to the right of the **Column Name:** data entry field. Click **OK**. You are returned to the **ListView Columns** page.
8. The order of the import fields can be adjusted by selecting the import field then clicking the **Move Up** or **Move Down** buttons. Click **OK**.
9. You will be returned to the **Import users to selected container** page.
10. Save the applet then close the **Designer**.

Ensure that the data in the CSV file is in the same field order as in the applet.

Import Users + Attributes from CSV File (Automated)

[import_user_auto1.dsr]

This applet imports users and selected attributes from a comma-delimited file.

The main differences between this applet and the non-automated version are:

- The CSV file is pre-specified in the Manual Entry Text field for the following service:

```
User Name (auto-create): || AD:IMPORT:AUTO_CREATE:Receive CSV
file, ["data",] for Mass User [or Other Object] Create -
Connected to: Import Users into specified Container...
```
- There is no button on the second window to initiate the import, it will proceed without requiring user input. Fully automating the container selection on the first window such as in applet [import_user_auto1a.dsr] will allow unattended user creation.

The file name must use a ***.CSV** extension. The file must be in the following format:

```
"User", "attribute", "attribute", "attribute",
"User", "attribute", "attribute", "attribute",
```

DSRAZOR for Windows Ready-to-Run Applets

where *User* is the account name (Common Name or Distinguished Name), and *Attribute* is any user attribute in Active Directory. For an example, see **import_user_auto1.csv** in the DSRAZOR for Windows install directory.

The following instructions describe how to use the **Designer** to edit this applet to accept data in a different format. Perform the following procedure to import using a different file format:

1. Open the applet with the **Designer**. The Select Window dialog page is displayed. You can do this by right-clicking on the applet's name while viewing it in the **Console**. The Select Window dialog page is displayed.
2. Select **Import users** and click **OK**. The selected window is displayed.
3. Right click over the white rectangle in the window to reveal the data element screen for editing.
4. Select the first entry that is highlighted:

```
User to import: || AD:IMPORT:AUTO_CREATE:Receive CSV file,  
["data",] for Mass User [or Other Object] Create - Connected to:  
Import Users into specified Container...
```


Click the **Edit...** button.
5. Select the file format to be imported. Click **OK**.
6. The **Update Connected Controls** page is displayed. Click **OK**.
7. You will be returned to the **ListView Columns** page. Click **OK**.
8. Save the applet then close **Designer**.

Perform the following procedure to change the attributes to be imported:

1. Open the applet in **Designer**. The Select Window dialog page is displayed. You can do this by right-clicking on the applet's name while viewing it in the **Console**. The Select Window dialog page is displayed.
2. Select **Import users** and click **OK**. The selected window is displayed.
3. Right click over the white rectangle in the window to reveal the data element screen for editing.
4. Select the last user attribute in the list, click **Add**. The Add Column window is displayed.
5. Click the **Search Manual Entry** button.
6. Select the attribute to be imported from the CSV file. If no names appear and you know the name of the attribute you can type it in the manual entry field.
7. Change the column name to be displayed to the right of the **Column Name:** data entry field. Click **OK**. You are returned to the **ListView Columns** page.
8. The order of the import fields can be adjusted by selecting the import field then clicking the **Move Up** or **Move Down** buttons. Click **OK**.
9. You will be returned to the **Import users** page.
10. Save the applet then close the **Designer**.

Ensure that the data in the CSV file is in the same field order as in the applet.

Import Users + Exchange Mailbox from CSV File (Exchange 2000/2003)

[`import2e.dsr`]

This applet imports users and selected attributes from a comma-delimited file. A column both the applet and the comma-delimited file is configured for specifying an information store for each user. The file name must use a ***.CSV** extension. The file must be in the following format:

```
"User", "exchange mailbox store", "attribute", "attribute",  
"User", "exchange mailbox store", "attribute", "attribute",
```

where *User* is the account name (Common Name or Distinguished Name), and *Attribute* is any user attribute in Active Directory. The information store can be specified in four different formats, and information stores can be specified differently for each user. For an example, see **import2e.csv** in the DSRAZOR for Windows install directory.

The following instructions describe how to use the **Designer** to edit this applet to accept data in a different format. Perform the following procedure to import using a different file format:

1. Open the applet with the **Designer**. The Select Window dialog page is displayed. You can do this by right-clicking on the applet's name while viewing it in the **Console**. The Select Window dialog page is displayed.
2. Select **Import Users and Create Exchange Account Sample** and click **OK**. The selected window is displayed.
3. Right click over the white rectangle in the window to reveal the data element screen for editing.
4. Select the first entry that is highlighted:

```
User to create: || AD:IMPORT:Receive CSV file, ["data",] for Mass  
User [or Other Object] Create - Connected to: Import Users and  
Create Exchange Account...
```


Click the **Edit...** button.
5. Select the file format to be imported. Click **OK**.
6. The **Update Connected Controls** page is displayed. Click **OK**.
7. You will be returned to the **ListView Columns** page. Click **OK**.
8. Save the applet then close **Designer**.

Perform the following procedure to change the attributes to be imported:

1. Open the applet in **Designer**. The Select Window dialog page is displayed. You can do this by right-clicking on the applet's name while viewing it in the **Console**. The Select Window dialog page is displayed.
2. Select **Import Users and Create Exchange Account Sample** and click **OK**. The selected window is displayed.
3. Right click over the white rectangle in the window to reveal the data element screen for editing.
4. Select the last user attribute in the list, click **Add**. The Add Column window is displayed.
5. Click the **Search Manual Entry** button.
6. Select the attribute to be imported from the CSV file. If no names appear and you know the name of the attribute you can type it in the manual entry field.

DSRAZOR for Windows Ready-to-Run Applets

7. Change the column name to be displayed to the right of the **Column Name:** data entry field. Click **OK**. You are returned to the **ListView Columns** page.
8. The order of the import fields can be adjusted by selecting the import field then clicking the **Move Up** or **Move Down** buttons. Click **OK**.
9. You will be returned to the **Import Users and Create Exchange Account Sample** page.
10. Save the applet then close the **Designer**.

Ensure that the data in the CSV file is in the same field order as in the applet.

Import Users + Exchange Mailbox from CSV File (Exchange 2007/2010)

`[x64_exch7_mb_import.dsr]`

This applet imports users and selected attributes from a comma-delimited file. A column both the applet and the comma-delimited file is configured for specifying an information store for each user. The file name must use a ***.CSV** extension. The file must be in the following format:

```
"User", "exchange mailbox store", "attribute", "attribute",  
"User", "exchange mailbox store", "attribute", "attribute",
```

where *User* is the account name (Common Name or Distinguished Name), and *Attribute* is any user attribute in Active Directory. The information store can be specified in four different formats, and information stores can be specified differently for each user. For an example, see **import2e.csv** in the DSRAZOR for Windows install directory.

The following instructions describe how to use the **Designer** to edit this applet to accept data in a different format. Perform the following procedure to import using a different file format:

9. Open the applet with the **Designer**. The Select Window dialog page is displayed. You can do this by right-clicking on the applet's name while viewing it in the **Console**. The Select Window dialog page is displayed.
10. Select **Import Users and Create Exchange Account Sample** and click **OK**. The selected window is displayed.
11. Right click over the white rectangle in the window to reveal the data element screen for editing.
12. Select the first entry that is highlighted:

```
User to create: || AD:IMPORT:Receive CSV file, ["data",] for Mass  
User [or Other Object] Create - Connected to: Import Users and  
Create Exchange Account...
```

Click the **Edit...** button.
13. Select the file format to be imported. Click **OK**.
14. The **Update Connected Controls** page is displayed. Click **OK**.
15. You will be returned to the **ListView Columns** page. Click **OK**.
16. Save the applet then close **Designer**.

Perform the following procedure to change the attributes to be imported:

11. Open the applet in **Designer**. The Select Window dialog page is displayed. You can do this by right-clicking on the applet's name while viewing it in the **Console**. The Select Window dialog page is displayed.
12. Select **Import Users and Create Exchange Account Sample** and click **OK**. The selected window is displayed.

DSRAZOR for Windows Ready-to-Run Applets

13. Right click over the white rectangle in the window to reveal the data element screen for editing.
14. Select the last user attribute in the list, click **Add**. The Add Column window is displayed.
15. Click the **Search Manual Entry** button.
16. Select the attribute to be imported from the CSV file. If no names appear and you know the name of the attribute you can type it in the manual entry field.
17. Change the column name to be displayed to the right of the **Column Name:** data entry field. Click **OK**. You are returned to the **ListView Columns** page.
18. The order of the import fields can be adjusted by selecting the import field then clicking the **Move Up** or **Move Down** buttons. Click **OK**.
19. You will be returned to the **Import Users and Create Exchange Account Sample** page.
20. Save the applet then close the **Designer**.

Ensure that the data in the CSV file is in the same field order as in the applet.

Import Users with Group Membership

[importg.dsr]

This applet will import Users with Group Membership from comma-delimited file. The file name must use a ***.CSV** extension. The file must be in the following format:

```
"UserName", "SAM Name", "Given Name", "Group1 FQDN", "Group2
FQDN",
"UserName", "SAM Name", "Given Name", "Group1 FQDN", "Group2
FQDN",
```

where *UserName* is the account name (Common Name or Distinguished Name), *SAM Name* is the NTV4 style user name (pre-Active Directory name), *Given Name* is the user's first name, and *Group* must be in the canonical name format. For an example, see **importg.csv** in the DSRAZOR for Windows install directory.

Perform the following procedure to change the attributes and group memberships to be imported:

1. Open the applet in **Designer**. The Select Window dialog page is displayed. You can do this by right-clicking on the applet's name while viewing it in the **Console**. The Select Window dialog page is displayed.
2. Select **Import users to selected container** and click **OK**. The selected window is displayed.
3. Right click over the white rectangle in the window to reveal the data element screen for editing.
4. Select the last user attribute in the list, click **Add**. The Add Column window is displayed.
5. Click the **Search Manual Entry** button.
6. Select the attribute to be imported from the CSV file. If no names appear and you know the name of the attribute you can type it in the manual entry field.
7. Select the user attribute to be imported
8. Select the attribute **Group Membership** to add groups where the user will become a member.

DSRAZOR for Windows Ready-to-Run Applets

9. Change the column name to be displayed to the right of the **Column Name:** data entry field. Click **OK**. You are returned to the **ListView Columns** page.
 10. The order of the import fields can be adjusted by selecting the import field then clicking the **Move Up** or **Move Down** buttons. Click **OK**.
 11. You will be returned to the **Import users to selected container** page.
 12. Save the applet and then close the **Designer**.
- Ensure that the data in the CSV file is in the same field order as in the applet.

Manage Terminal Services Profile

[TermSvcProf.dsr]

This applet will allow you to select a user in Active Directory and modify the Terminal Services profile, session, and environment attributes for that user.

Move AD Object to a New Container

[MoveADObject.dsr]

This applet will search Active Directory from the path you select for all objects. After selecting a starting container or Organizational Unit (OU), you can move user, group, and contact objects you highlight on the left into any container or OU on the right with the press of a button.

Remove SID History

[sIDHistory.dsr]

This applet will find all user accounts in the selected container or Organizational Unit. A column in the resulting report will show if a user has any values for the sIDHistory attribute. A button allows you to delete the SID History on selected user accounts.

Smart Delete of User Accounts (Home Directory and Exchange Mailbox)

[smartd3.dsr]

This applet will search Active Directory from the path you select for all user objects. The user objects found will be presented with their creation time and number of days since their last domain logon.

This applet determines the last logon by scanning the object's lastLogon attribute on each Domain Controller; this is performed on each Domain Controller because the lastLogon Active Directory attribute is not replicated. If you are using Windows 2003 domain mode you can modify the applet to use rely upon the lastLogonTimeStamp attribute that is replicated between domain controllers and is updated, by default, once a week.

When you "Smart Delete" user accounts you are actually deleting the user account and completely removing its home directory structure and files as well as their Exchange Mailbox. The applet user must have sufficient privileges to delete the user and the user's home directory and contents for the applet to be successful.

Unlock User Accounts

[unlock2.dsr]

This applet will search Active Directory from the path you select for all user objects that are locked. Accounts become locked only if Active Directory is configured to detect intruder logon attempts and lock accounts based upon this detection.

For all locked users found, you can use the applet to unlock them. This applet also includes the ability to disable and rename selected locked user accounts.

View Home Directory Sizes and Contents

[viewhd03.dsr]

This applet will list all user accounts in the selected Active Directory container that have a home directory defined. Details for each user found with a home directory include:

- Path to home directory
- Number of files in home directory path
- Overall size of all files in home directory path

You may view the home directory structure and contents for each user on a user-by-user basis.

Category: Examine Servers/Disks

The applets available from this menu category are generally useful for maintaining, documenting, and querying your servers, disk space, and active server connections. In the sections that follow you will find the title of each applet, its specific filename and description.

IMPORTANT: These applets all operate within the abilities of your logon account. If your logon account is not sufficiently privileged you will not be able to successfully use the applets listed below.

Directories/Files with no owner (orphaned SID)

[`fownerSID2.dsr`]

This applet searches from the selected Windows Share or directory (folder) path for all file system objects that have an invalid SID as the object's owner.

Typically, an invalid SID is an object that has been deleted from the Active Directory. The SID remains as the object's owner because Active Directory has no back-linking ability to clean up SIDs after the object that owned the SID is deleted. This means the SID would remain as the selected object's owner forever if you did not clean it up. This has both security and performance implications.

Details included per file system object found include:

- Owner SID
- Creation date
- Last Access date
- Number of days since last access

Directory/File Ownership

[`fowner2.dsr`]

This applet searches from the selected Windows Share or directory (folder) path for all files and directories.

Details included per file system object found include:

- Owner Name
- Creation date
- Last Access date
- Number of days since last access

Discover all file extensions in-use

[`fsext2.dsr`]

This applet searches from the selected Windows Share or directory (folder) path for all files. For each file found, its extension is recorded. The resulting list will list each extension found, the number of files found with that extension and the accumulated file size of the files found with that extension.

Document Share Permissions

[`fsListShareACLp4EXA.dsr`]

Searches from the selected computer for all file system shares and lists the following details for each share found:

- Trustees for the Object
- Permission Type (Allow/Deny) and Description

Domain Controller Status

[dcstatus1.dsr]

This applet lists domains and for each domain found it lists each Domain Controller. Details shown for each Domain Controller include the current DC time and a list of Mounted Drives. You can optionally view all Control Panel Services installed on the selected DC and the status of each service.

Domain Disk Space Report

[fssize1.dsr]

This applet lists domain and for each domain found it lists all servers/workstations. Details shown per server/workstation include:

- List of Public Shares
- Volume name where the share is defined
- Serial number of the volume
- Percent full
- Overall disk size
- Space in use
- Space available

NOTE: Disks must have public shares to be included by this applet. The applet may be edited in the **Designer** to change the include criteria for displaying of disk data.

Exchange Mailbox Sizes (Exchange 2007/2010)

[x64_exch7_mb_sizes.dsr]

This applet searches the domain for Exchange Mailbox Databases. The results window shows:

- All Exchange Mailboxes
 - Mailbox Display Name
 - Database
 - Primary SMTP Email Address
 - Number of Emails
 - Total Size of Emails
 - Number of Deleted Emails
 - Total Size of Deleted Emails
 - Storage Limit Status
 - Last Logon Account Name for Mailbox
 - Last Logon Date and Time for Mailbox

Exchange Server Details (Exchange 2000/2003)

[listexch1.dsr]

This applet searches the domain for Exchange servers. The results window shows three panes of information that includes:

- All Exchange servers
 - Storage Groups on the server
 - Mailbox Stores in the Storage Group
 - Users with Mailboxes in the Mailbox Store
- All Exchange Storage Groups
 - Log File Prefix
 - Transaction Log Location
 - System Path Location
- All Exchange Mailbox Stores
 - Information about Mailboxes
 - .edb path
 - .stm path
 - Organization
 - Administrative Group
 - Storage Group

Exchange Server Details (Exchange 2007/2010)

[x64_exch7_mb_stats.dsr]

This applet searches the domain for Exchange servers. The results window shows:

- All Exchange Mailbox Stores
 - Storage Group
 - Server
 - Organization
 - GUID
 - Database Path (.edb)
 - Name
 - Administrative Group
- All Exchange Mailboxes
 - Mailbox Display Name
 - Database
 - User's Mail Alias
 - Primary SMTP Email Address
 - User's Logon Name
 - Number of Emails
 - Total Size of Emails
 - Number of Deleted Emails
 - Total Size of Deleted Emails
 - Storage Limit Status
 - Last Logon Account Name for Mailbox
 - Last Logon Date and Time for Mailbox
 - Was Last Logon by Account Holder?

Find Duplicate FS Object Names

[**fsdups2.dsr**]

This applet searches from the selected Windows Share or directory (folder) path for all files and folders. Once files and folders are found you can press a button that will sort through the results and display objects that have duplicate names. Information for each file and folder includes:

- Full Path to File/Directory
- File/Directory Name
- Owner
- Date Last Accessed
- Number of Days Since Last Access

You can edit the applet in the **Designer** to include a button that will delete objects.

Find Files unused for past 365 days

[**fs365b.dsr**]

This applet searches from the selected Windows Share or directory (folder) path for all files. Files with a last access date more than 365 days ago will be included in the results.

You can edit the number of days from 365 to the value you require in the **Designer**.

List All Servers/Workstations in Domain

[**servers2.dsr**]

This applet lists all domains. When you select a domain a list is created that includes all server and workstations in that domain. The current time for each machine found is included as well as the mounted drives.

You may optionally view all control panel services and status of each on the selected machine.

List Local Group Membership

[**localgroups1.dsr**]

This applet will document Local User Accounts, Local Groups and Group Membership on selected workstations or servers. Three lists are displayed on a single window for ease of use. The first list displays the local groups. The second list displays the local users. Details for local users include:

- Account Name
- Administrator Status
- SID of Local User

The third list displays group membership details for the selected local group. Details for group membership include:

- User Account
- SID of User or Group Member

List NT Domain Group Membership

[NT4_dom_groups.dsr]

This applet will document Domain group membership in Windows NT Domains. Expanding the Primary Domain Controller [PDC] in an NT Domain will display all Domain global groups in the Domain, and expanding those groups will display the SAM account names of members of those groups.

Local Admin Password Reset

[LocalAdminPass.dsr]

This applet connects to workstations and servers with the purpose of resetting the local administrator password. The applet identifies the administrator account by its SID so it does not matter if the account has been renamed.

You may choose workstations and servers by doing a NetBIOS search or by locating computer accounts in your Active Directory.

For each machine you will see the Current Time, Drives Mounted, Local Users, and Local Groups. You may also view all control panel services and status of each on the selected machine.

Logging File Usage

[logfileb.dsr]

This applet provides a simple method to audit remote file usage. Remote file use is that use which is accomplished when a file on the selected machine is opened via a share from a remote computer.

This applet begins by listing all domains and Domain Controllers within each domain. To continue, select a Domain Controller and you will be presented with a screen that shows all files open on that DC. To audit file usage, click on the **Log File Use at Specified Interval** button. Follow the instructions presented to audit remote file use on that DC.

Scan for all MP3 files

[findmp3b.dsr]

This applet searches for all *.MP3 files from the selected Windows Share or directory (folder) path. The details returned with each file found include:

- File Size
- File Owner
- Date last accessed
- Days since last access

To search for other file extensions, edit this applet in the **Designer**.

Search DCs for service not running

[dcs2.dsr]

This applet provides a demonstration of DSRAZOR's ability to scan all Domain Controllers for a specific Control Panel service where that service is not running (stopped).

In this sample applet, a search is conducted on all Domain Controllers in the selected domain for a service name that contains the word "alert" and the status is "stopped".

This applet allows the service to be restarted.

Edit this applet in the **Designer** to establish your own search criteria.

View File Details per Directory

[viewfiles2.dsr]

This applet lists all domains and all servers/workstations within each domain. Upon opening a server/workstation you will be presented with a list of public shares and directories within each. When you select a directory you will be present with a list of all files in that directory including the following details per file:

- File name
- Owner
- Owner type
- File size in KB
- File size in bytes
- File system attributes
- Date created
- Date of last access
- Date modified

View Sessions on Domain Controller

[sessdc1.dsr]

This applet lists all domains and Domain Controllers per domain. When you select a Domain Controller you will be able to view active sessions in a number of different ways including:

- By NT name (pre-Active Directory) or SAM name
- By Computer where sessions originated
- By User Principal Name (such as: user@acme.local)
- By LDAP name (Active Directory name)

Details shown for each session include subset of the following (depending on the view selected):

- Name of user (in one of the formats above)
- Domain of user
- Workstation name where user originated
- Base Operating System of user
- Session Active Time
- Session Idle Time
- Full Active Directory name of user

View Shares Usage

[shares2.dsr]

This applet lists all domains and Domain Controllers per domain. When you select a Domain Controller you will be able to view public and hidden shares and a count of the number of active sessions for each. If the share includes a value for the comment field it is displayed.

Some views include a list of files open for each session including a count of file locks in use per open file.

Who has Files Open on Server + Close

[whofile2.dsr]

This applet lists all domains and Domain Controllers per domain. When you select a Domain Controller you will be able to view all open files. Details shown include:

- User who has the file open
- Number of file locks in use
- Access allowed

Additionally you can *force close* any file or open resource shown.

The list of open files is updated every 10 seconds.