



Mercurion Systems, Inc.

Information Technology Consulting and Support Services

Phone: 919.266.5957 Fax: 919.217.5769
<http://www.mercurionsystems.com>

MASS PASSWORD CHANGES IN ACTIVE DIRECTORY

Products: Windows Server 2003; Windows Server 2003 Resource Kit Tools

Overview

There may be occasions in which the passwords for large numbers of accounts in Active Directory need to be reset in some automated fashion. For example, during a migration to Active Directory from another directory service, it may be necessary to set an initial password on large numbers of accounts at once in an automated fashion.

This technical note describes the use of several tools, including LDIFDE, grep, Notepad, and dsmod (from the *Windows Server 2003 Resource Kit Tools*) to perform automated mass password changes to Active Directory accounts.

More Information

The tools and utilities needed to perform the steps listed here are LDIFDE (included with Windows Server 2003), grep (available on Linux or Mac OS X by default, Win32-compatible versions available on the Internet), Notepad or another text editor with find/replace functionality (advanced Linux and Mac OS X users may be able to use sed instead), and dsmod (from the *Windows Server 2003 Resource Kit*).

The basic steps to perform a mass password change are listed below.

1. First, export the list of user accounts out of Active Directory using LDIFDE. The command might look something like this:

```
ldifde -d "CN=Users,DC=company,DC=com" -r "(objectclass=user)"  
-f c:\export-1.ldif
```

This command creates a file named "export-1.ldif" that will be used again in later steps.

2. Using grep, filter out only the line that specifies the user account's full distinguished name. The command would look something like:

```
less export-1.ldif | grep `dn: ` > export-2.ldif
```

The "less" command outputs the contents of the file, which are piped to grep. Grep returns only those lines that have the "dn: " pattern, and those matches are redirected into a second file (do not overwrite the original file).

Some of these commands may have to be modified (for example, using “type” instead of “less”) if this command is not being run on a *NIX-based system (such as Linux or Mac OS X). Similarly, grep on a Win32 platform requires the use of double quotes instead of single quotes around the pattern to be matched.

- Using a text editor, edit output file from the previous step (named “export-2.ldif” in these examples) to remove “dn: “ from the beginning of every line, and to add double quotes around the full distinguished name (necessary in situations where the user’s name is spelled out, like “John A. Smith” instead of “jasmith”). Perform the following changes:

- Replace all occurrences of “dn: ” (there is a space after the colon) with nothing
- Replace all occurrences of CN= with “CN= (add a double quote before CN)
- Replace all occurrences of DC=com with DC=com” (add double quote after last DC component)

Save the modified file as export-3.ldif (or whatever appropriate file name, but don’t overwrite the previous version).

- Pipe the final output file (“export-3.ldif” in our examples) to the dsmod command from the Windows Server 2003 Resource Kit Tools using the following syntax:

```
type export-3.ldif | dsmod user -pwd newpass1 -mustchpwd yes
```

In this syntax, “newpass1” is the one-time password that will be the same for all users upon their next logon to Active Directory. The “-mustchpwd yes” switch forces the user to change their password upon their next logon to Active Directory.

Note that complete details of the results of the dsmod user command can be captured in a log file by redirecting the output of the command listed above (using a > symbol) to a text file. This text file can then be parsed using grep or a similar utility to ensure that the command was successful for all users.

Upon the completion of this procedure, all accounts will have a generic initial password that must be changed upon their next logon.

Other Notes

Although this procedure was only tested specifically with Windows Server 2003, it should work equally well against Windows 2000.

Related Articles/Resources

None

Legal Information

This document was created by Mercurion Systems, Inc., and may be freely distributed as long as it is distributed without modification and in its entirety. Mercurion Systems assumes no liability as a result of using the information contained in this document.