



Ten Things to Know About Active Directory Recovery

written by
Guido Grillenmeier, Hewlett Packard
Kevin Sullivan, Aelita Software

White Paper

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. However, because of the possibility of human or mechanical errors, Aelita Software does not guarantee the accuracy, adequacy, or completeness of any information in this publication, and is not responsible for any errors or omissions or the results obtained from use of such information.

Unless otherwise noted, the example companies, organizations, products, people, and events depicted herein are fictitious. No association with any real company, organization, product, person, or event is intended or should be inferred.

Aelita Software does not endorse or accept any responsibility for the content or usage of links and references to non-Aelita Web sites or technical documentation.

No part of this document may be reproduced, stored or transmitted in any form, by any means, or for any purpose, without the express written permission of Aelita Software Corporation.

Aelita, Aelita Software, the Aelita Software Corporation logo, and all Aelita product names and slogans are either registered trademarks or trademarks of Aelita Software Corporation. Other product or company names mentioned herein may be trademarks of their respective owners.

Copyright © 1997-2004, Aelita Software Corporation. All rights reserved.

Last revised February 23, 2004

AELITA SOFTWARE CORPORATION

6500 Emerald Parkway
Suite 400
Columbus, Ohio 43016, USA

Phone: 614-336-9223
1-800-263-0036
Fax: 614-761-9620
Email: info@aelita.com
URL: www.aelita.com

CONTENTS

INTRODUCTION.....	5
TEN THINGS TO KNOW ABOUT ACTIVE DIRECTORY RECOVERY	6
<i>1. Non-Authoritative Restores Are Easy But Often Insufficient.....</i>	<i>6</i>
<i>2. You Need to Know the Exact Path to an Object to Restore It Authoritatively</i>	<i>8</i>
<i>3. Backups Are Only Valid for 60 Days.....</i>	<i>9</i>
<i>4. Recovering Deleted Objects in Windows Server 2003 Isn't As Easy As It May Seem</i>	<i>10</i>
<i>5. Some Changes Can't Be Undone.....</i>	<i>11</i>
<i>6. The Problem May Be Bigger Than You Think.....</i>	<i>12</i>
<i>7. Restoring a User Doesn't Necessarily Restore Group Membership</i>	<i>12</i>
<i>8. SYSVOL Requires Special Restoration Procedures</i>	<i>14</i>
<i>9. You Don't Have to Back Up Every Domain Controller</i>	<i>15</i>
<i>10. Forest-Level Recovery Is Time-Consuming and Error-Prone. Fortunately, You May Be Able to Avoid It</i>	<i>16</i>
SUMMARY	17
ABOUT THE AUTHORS	18
ABOUT AELITA SOFTWARE CORPORATION	19

INTRODUCTION

Active Directory is the gatekeeper to the network resources your employees depend on, so Active Directory is critical to your business. Accordingly, having a reliable and practiced set of recovery strategies is vital. Preparing for a catastrophic event—for example, a hardware failure or physical disaster—is necessary, but so is preparing for “everyday disasters.” Problems can arise in the normal course of day-to-day operations from a variety of causes, including:

- Human error. For example, an administrator might delete an entire organizational unit (OU) instead of a particular user, or accidentally delete a service account, which could affect hundreds of users.
- Unexpected consequences. For example, an administrator might use a script to set one of the Extension Attributes in Active Directory only to find out that Extension Attribute contained data for another mission-critical application that won't work any more because of the changes. The data must be restored as soon as possible.
- Malicious activity. Both current and recently-terminated employees, as well as external service providers, might find ways to access your sensitive systems and data, and their knowledge can enable them to cause significant damage. According to *Entrepreneur*, “four out of five IT-related crimes are committed from within an organization” (http://www.entrepreneur.com/Your_Business/YB_SegArticle/0,4621,298386,00.html). Moreover, *CSO Online* reports that “inside security breaches affect 49% of companies” (<http://www.csoonline.com/metrics/viewmetric.cfm?id=277>). Once your network is under attack, it's too late to plan—you need to have your diagnostic and recovery tools in place.
- Viruses. Viruses can damage Active Directory data, and the replication process propagates those unwanted changes. Anti-virus software, of course, provides protection, but it is critical to be able to respond quickly to viruses that get through.

This document details important considerations when creating and testing your Active Directory recovery plan. It discusses restoration of data using native tools provided by Microsoft, particularly Ntdsutil.exe, Microsoft's command-line tool for managing Active Directory, including restoring data. The document does not attempt to serve as a comprehensive guide; instead, it provides administrators with important insights into the finer points of Active Directory recovery.

TEN THINGS TO KNOW ABOUT ACTIVE DIRECTORY RECOVERY

1 Non-Authoritative Restores Are Easy But Often Insufficient

The domain controllers (DCs) in each domain keep a variety of information in the *directory data store* (or simply the *directory*). Changes made to the directory are *replicated* from one DC to other DCs in the domain. Replication occurs at intervals, not continuously. Therefore, the directory on any DC is normally in *loose consistency* with those on other DCs, since the most recent changes on each DC may not have been replicated to the others. Objects' attributes are assigned version numbers that are incremented when the attributes are changed so that the replication process can determine which changes are the most current.

Directory data stored on DCs and replicated between them includes information about objects, configuration data (such as a list of all domains and the locations of their DCs), and schema data, which defines the types of objects that can be stored in the directory and the attributes they can have. This information is used by network applications and services.

The first step in restoring Active Directory data is to boot a domain controller into Directory Services Restore Mode (DSRM). Then the Active Directory database (NTDS.dit) can be restored with a utility such as the native Backup utility provided by Microsoft. The restore of the actual database file can only be performed in non-authoritative mode; however, it is important to understand the concepts of *non-authoritative* and *authoritative* restores with respect to the objects stored in the database:

- Using native tools provided by Microsoft, the default method is the **non-authoritative** restore: settings and entries maintain the version numbers they had at the time of backup. After the DC is restored, it is updated using normal replication methods. Note that any object that was deleted after the last backup will be restored with the database file, but if the DC is then booted to normal Active Directory mode, the object will be deleted again during the replication process.

- An **authoritative** restore, on the other hand, allows you to selectively increment the version numbers of attributes to make them authoritative in the directory. That is, during the replication following the restoration, when the version numbers of objects are compared, the objects and attributes on the restored DC that were restored authoritatively will have higher version numbers than those on the other DCs, and will replicate out to the other DCs instead of themselves being overwritten as out-of-date. This allows you to recover deleted objects even after the deletion has been replicated throughout the enterprise. Usually, an authoritative restore of selected objects and attributes follows a non-authoritative restore of the whole database (for example, from a backup tape).

Accordingly, when you need to recover deleted objects from a backup or roll back changes to objects, you typically first need to perform a non-authoritative restore and then do an authoritative restore, even though it is more difficult.

Simple non-authoritative restores are valuable primarily if you need to recover a DC that has crashed and that has a slow connection to the next DC. This restores an old version of Active Directory and only the differences between the restored DC and its replication partners need to be transmitted. If bandwidth is not a concern, you do not need to do a restore at all: if a DC crashes, you can simply promote a Windows 2000/2003 server to be a DC, and a clean version of Active Directory will replicate to it from an existing DC. If you're running Windows Server 2003, you can do this very efficiently by promoting a server to be a DC using the Install from Media feature.

Note that when you perform a non-authoritative or an authoritative restore, the DC must be offline for user access. Specifically, the DC must be booted into a special mode, Directory Services Restore Mode. The machine at that point is online but is not functioning as a DC in the Active Directory. While the DC is in Directory Services Restore Mode, it is unavailable for any functions associated with Active Directory, such as validating logons or replicating directory data.

2

You Need to Know the Exact Path to an Object to Restore It Authoritatively

An authoritative restore is an extension of a non-authoritative restore: once you've done a non-authoritative restore, you can mark particular objects to be restored authoritatively using the Ntdsutil utility from the command line.

The first step is to locate and retrieve the object. This requires knowing its distinguished name (DN). The DN is made up of the nodes from the root domain down through the hierarchy of directory containers to the object. The DN of each object is unique within a given Active Directory forest. The following is an example of a distinguished name:

```
CN=Chris Smith,OU=Sales,OU=North America,DC=Acme,DC=com
```

This uses the following abbreviations:

CN: common name

OU: organizational unit

DC: domain component

Accordingly, authoritatively recovering a single object is not too much additional work—provided that you have this detailed information about its name. However, if many non-contiguous objects have been mistakenly deleted, restoration is difficult, time-consuming, and error-prone, since all the data must be keyed into a command-line interface. In any case, reconstructing a deleted object's distinguished name may not be a simple matter; you will need to have procedures in place to capture this information in case an authoritative restore is necessary.

3

Backups Are Only Valid for 60 Days

When an object is deleted from Active Directory, Windows does not remove it right away. Instead, most of the attributes associated with that object are removed, and the object is renamed and moved to the Deleted Objects container, a special hidden container in Active Directory. The object is now referred to as a “tombstone.” At the next replication interval, this tombstone is replicated to the other DCs. A deleted object is permanently removed at a set interval after being tombstoned. By default, this interval is 60 days. (The lifetime of tombstones can be set on the Directory Service (NTDS) config object.) During this interval, the tombstone can be reanimated and the object restored, at least in part, to its previous state.

After 60 days, a backup of one DC may contain objects whose tombstones have been permanently removed on other DCs. Even though the backup includes these objects, they cannot be restored. So if a user account was removed in error and the error wasn’t discovered until sometime later (for example, in the case of an employee on an extended leave), the user account cannot be recovered.

Note that this process of tombstoning can lead to a problematic situation if you disconnect a DC from your network for more than 60 days: if an object is deleted during this time, this change cannot, of course, be replicated to the disconnected DC. If that DC is reconnected after the object’s tombstones have been removed from the other DCs, then it will have an object that the other DCs do not, sometimes called a *lingering object*. For Microsoft’s best practice recommendations for managing long DC disconnections, see:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/ad/windows2000/maintain/opsguide/Part1/adogd14.asp>.

4

Recovering Deleted Objects in Windows Server 2003 Isn't As Easy As It May Seem

In Windows Server 2003, Microsoft introduced an online facility for recovering deleted objects. This facility does not allow you to selectively restore attributes or roll back changes to an object, nor does it provide any method for determining which objects or attributes have been changed. Moreover, it does not include a GUI. Rather, it is a programming interface that allows you to reanimate a deleted object's tombstone. It requires you to first retrieve and then restore the deleted object, once you have managed to ascertain its fully qualified distinguished name (DN). For samples of code from Microsoft for both steps in this operation, see:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ad/ad/retrieving_deleted_objects.asp

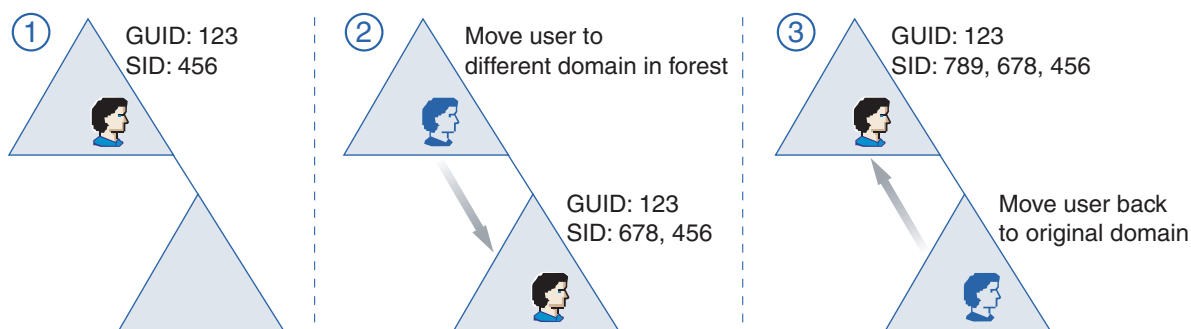
and

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ad/ad/restoring_deleted_objects.asp.

As mentioned in the previous section, most of the attributes associated with an object are removed when the object is deleted and its tombstone is created. Although you can configure in the schema which attributes of the original object are to be kept in the tombstone, by default only a very limited number of attributes are retained in the tombstone. So, if you do manage to use the online recovery facility, the object will be only partially restored: only the attributes of the object that are required for its existence are restored. Other attributes, which may be equally critical for your business, such as SIDHistory and password, are not restored.

5 Some Changes Can't Be Undone

Active Directory objects are sometimes moved between domains in a forest, such as when organizational or administrative functions change (for example, when an employee moves from one department to another, or you decide to outsource a function). When an object is moved to a new domain, no tombstone is left in the domain where the object was moved from. This is because each object is assigned a globally unique identifier (GUID) when it is created. Unlike a security identifier (SID), a GUID is unique within a forest and never changes, even if the object is moved or renamed. Applications can store the GUID of an object and use the GUID to retrieve that object regardless of its current distinguished name (DN). Therefore, when an object is moved between domains in a forest, it is assigned a new SID but retains its unique GUID. No tombstone object can be created in the old domain, since it would have the same GUID.



Accordingly, a move of an object between domains in a forest cannot be undone without performing a labor-intensive authoritative restore. The object can be moved back, but its SIDHistory becomes increasingly complex: it includes information about the object's original existence in the first domain, its existence in the second domain after the move, and its new existence in the first domain after its move back. Increased complexity of SIDHistory can cause a variety of issues, including longer logon and authentication time.

6

The Problem May Be Bigger Than You Think

Whenever you discover a problem in Active Directory, it is critical to evaluate it carefully and determine its scope. For example, if a user reports that he can't log in, and you determine that the user account was deleted, check further to see if the entire OU was deleted—the user may simply be the first user to call in. Or if a user reports access problems, consider whether an administrator may have run a script to make certain changes and affected many users in unanticipated ways.

When problems are reported in Active Directory, it's useful to be able to compare the current state with a last-known good state to help troubleshoot the problem. This can save a lot of time and headache and help you accurately diagnose and solve the problem quickly. Time is critical here: it is best to find and repair the problem before it can impact your business.

7

Restoring a User Doesn't Necessarily Restore Group Membership

... and in fact, an authoritative restore can lead to inconsistent group membership on different DCs.

Restoring group membership presents unique challenges. Users are usually members of various groups, and correctly restoring these group memberships along with the user object is critical. Each user who is a member of a group has all the access permissions and rights assigned to that group. Losing group membership means loss of those permissions and rights. Additionally, in an Exchange 2000/2003 environment, losing membership in a group means no longer receiving email sent to that group. Therefore, when restoring a user, you must also restore the group membership information.

Group membership information is stored with the group object (in the group's member attribute) as a so-called "forwardlink." The user object itself contains (in the memberOf attribute) a backlink to each group where the user is a member. When a user is deleted, the group objects in the Active Directory forest are cleaned appropriately—that is, the user is removed from each group's member attribute. As the deleted user object (tombstone) replicates to other DCs in the forest, the DCs also clean their local copies of the respective groups and remove the membership of the deleted user without actually changing the version numbers of the groups themselves. There are other linked attributes between Active Directory objects (for example, the manager and directReports attributes), which behave the same way during object deletion; however, they are not as security-sensitive as group membership.

If any DC in the forest is running Windows 2000, restoring a deleted user using native tools will not restore group membership. Even when all Windows 2000 DCs have been upgraded, the native tools will not restore group memberships that existed before the forest was switched to Windows Server 2003 Forest-functional level. Instead, you have to determine which groups to update and then update each of those groups to correctly restore the membership. Alternatively, once you have determined which groups the user belonged to, you can do an authoritative restore of those groups; however, this can potentially lead to inconsistent group membership on different DCs. Specifically, if the group object is authoritatively restored before the user object, during the replication of the group to other DCs, Active Directory detects that the restored group object has members that do not exist and removes those users from the group's member attribute. When the users are then authoritatively restored, the group's member attribute is not updated.

To prevent this problem, users must be restored and replicated first, and then groups can be restored and replicated.

Similarly, contact objects are often members of mail-enabled groups and are thus affected in the same way as a deleted user object. Even computer objects may be made members of security groups, for example, to control Group Policy application to specific computers in an OU. Like in the previous examples, losing the group membership of a computer object can have a negative impact on a computer's behavior in the Active Directory infrastructure. Furthermore, groups can be members of other groups (nesting global groups in local groups or even nesting groups of the same type in Windows 2000 native mode or in Windows Server 2003 Domain-functional Level domains). As a result, restoring a group object that is a member of other group objects leads to the same challenges as restoring a user object.

Cross-domain group membership in a multi-domain Active Directory forest presents particular problems. Consider a user who has an account in domain A, and is a member of a universal or domain local group in domain B. This is *cross-domain membership*. If the user is deleted from domain A, the group in domain B is also cleaned—the member attribute of the group is updated to reflect the deletion. If the user's account is restored, however, the group is not updated to reflect the user's membership. This is even the case if you are running Windows Server 2003 Forest-functional level. The administrator must determine which groups the user was previously a member of and either add the user back to those groups manually or restore the groups in domain B from a backup of domain B.

SYSVOL is the system volume, a component of the System State. On domain controllers, SYSVOL provides a standard Active Directory location for files that must be shared for common access throughout a domain. SYSVOL contains user logon scripts, Group Policy objects, Net Logon shares, and file replication service (FRS) staging directories and files that must be available and synchronized between DCs. It is critical that SYSVOL data be complete and accurate. Loss of Group Policy information, for example, can lead to serious security vulnerabilities and make it impossible for users to log on to the domain.

Since SYSVOL is a series of files and directories and not a database, restoring it requires special care. If at least one other DC in the domain is still functioning, then—similar to object-level restores in the Active Directory database—SYSVOL can be restored either *non-authoritatively* or *authoritatively*:

- If you choose a non-authoritative restore, then when the restored DC reboots, the SYSVOL information will be compared with the other DCs in the domain and updated.
- If you restore SYSVOL authoritatively, the local SYSVOL will be replicated to the other DCs in the domain, enabling you to recover from an error that has been replicated to the other DCs, such as accidental deletion of a Group Policy object. Note that using native tools, authoritative restore of SYSVOL is not automatic upon an authoritative restore of other objects in Active Directory; you must take additional steps.

If no other DC in the domain is functioning, you must do a *primary* restore of SYSVOL. This builds a new ntfrs (Windows NT File Replication Service) database by loading the data present under SYSVOL on the local DC. This method is the same as a non-authoritative restore except that SYSVOL is marked as primary. It is even more challenging to restore specific files or subfolders of SYSVOL (for example, a logon script that was accidentally deleted) because the normal method to do a *primary* restore affects the whole SYSVOL folder.

9

You Don't Have to Back Up Every Domain Controller

Because changes made to the directory are replicated from one DC to other DCs, the directory on any DC is normally in loose consistency with those on other DCs. Therefore, you do not need to back up every DC: if one DC fails, you can either restore it from backup (if you have backed up that particular DC) or by Active Directory replication from its partner DCs.

The number of DCs you should back up depends on a variety of factors, including WAN performance. It is wise to back up at least two DCs for redundancy, and also to back up your Flexible Single Master Operations (FSMO) roles (also known as operations master roles).

Note: Correct restoration of a failed relative ID (RID) master is particularly critical: if the RID master is restored improperly, you risk having objects with duplicate SIDs created in the domain. Therefore, rather than restoring the RID master, the recommended procedure is to seize the RID FSMO role to a different domain controller.

It may at first seem beneficial to perform a full backup to tape of DCs that are connected across slow WAN links: this would allow restoration from tape in case of a hardware failure. However, tape handling in this scenario becomes increasingly complex and risky. Instead, it may be a better to store the backup to a local disk on the DC. Although this doesn't provide the same restore capabilities, it allows quick restore of Active Directory in case of non-disk related hardware failures and is also easier to manage and secure.

How often you should back up your data depends, of course, on how often it changes and how critical those changes are. In general, you should back up at least once a day. You should also back up before and after you make changes to Active Directory; for instance, if you run a script to update user objects, back up Active Directory both before and after running the script. If your script runs via a scheduled process, make sure that your backup solution is scheduled to run (and has enough time to finish) before and after the script is automatically run.

10 Forest-Level Recovery Is Time-Consuming and Error-Prone. Fortunately, You May Be Able to Avoid It

Forest-level recovery is extremely difficult, time-consuming, and error-prone. In addition, it can result in the loss of all changes since the last good backup was made. Microsoft has published a 22-page guide titled *Best Practice Recommendation for Recovering your Active Directory Forest* (available for download from <http://www.microsoft.com/windows2000/downloads/tools/redir-netdom.asp>).

Accordingly, forest-level recovery should be undertaken only as a last resort. Fortunately, careful research using the proper tools can enable you to determine the cause of the failure and evaluate possible remedies. In particular, comparison of the current state of your Active Directory to a good backup can help you determine what changes have occurred, and selective restoration of objects may be all that's needed to solve the problem. In particular, examination of the critical objects in your Configuration container can help you resolve problems without a full-forest recovery.

SUMMARY

Because your Active Directory is critical to your business, you need a good understanding of how Active Directory recovery really works, as well as tools to help you quickly diagnose and rectify problems.

Aelita Recovery Manager for Active Directory (formerly *ERDisk for Active Directory*) does just that. It maintains a historical repository of directory data and offers remote, online, granular restore options to repair the entire directory, a portion of it, or a single directory object or object attribute. Recovery Manager provides easy-to-use wizards and clear reports that reduce your recovery time, increase Active Directory and Group Policy reliability, reduce administrator workload, and lower your overall costs. In particular, Recovery Manager offers the following solutions:

- Troubleshooting tools, including quick snapshot comparisons of backups with the live Active Directory and granular comparison of directory objects at the attribute level. This helps you to quickly and accurately determine what changes have taken place so you can evaluate what might need to be rolled back.
- Restoration tools, including online, granular restore options that let you easily restore individual objects or attributes without having to know their fully qualified distinguished names and container information. Objects can be fully restored, with all their attributes, including group membership, without the need for separate backups or additional steps.
- “What if” tools, including comparison reports that show how properties of objects would change during a proposed restoration, without actually applying changes to Active Directory.
- Administrative tools, such as remote restoration of Active Directory and Group Policy data from one central location, without requiring the administrator to go to the DC.
- Backup tools, including centralized management of the creation and storage of System State backups for Active Directory domain controllers and scheduling of backups during off-peak hours.
- User-friendly GUIs and wizards that eliminate the need for painful and often inaccurate typing to a command-line facility.
- A choice of offline or fully online recovery, eliminating the need to reboot DCs and interfere with the work of your users and your business. In addition, you can control the recovery process remotely, instead of moving physically to each affected DC.
- Easy and effective backup and restore of SYSVOL to assist in the total management of your Group Policy environment.

ABOUT THE AUTHORS

Guido Grillenmeier is a senior consultant in the Technology Solutions Group at Hewlett Packard. Based in Germany, Guido joined HP in 1996 and has been working with directory security and delegation of administrative rights since the early days of Windows NT. Today, Guido deals primarily with global Windows 2000/2003 deployments and migrations, designing and implementing efficient Active Directory security and delegation models for HP's customers. He has further specialized in disaster recovery methodologies for Active Directory and is working closely with Microsoft to investigate and understand this critical task. Guido is a frequent speaker at technical conferences such as the Microsoft Exchange Conference, Microsoft IT Forum and NetPro's Directory Experts Conference.

Kevin Sullivan, MCSE, is a product manager at Aelita Software. As a product manager, he is responsible for collecting market requirements and working with development to ensure that the needs of the market are met with Aelita solutions. With a background as an independent consultant and technical advisory lead/project manager for IBM Global Services, Kevin has worked on very large-scale network implementations. Additionally he has contributed to many technical articles and books, and has designed and implemented in-depth training programs related to Windows NT, Systems Management Server, Active Directory, and Windows Server 2000 deployment. Kevin is primarily responsible for Active Directory-related products for Aelita.

ABOUT AELITA SOFTWARE CORPORATION

Aelita Software provides systems management solutions to organizations that rely on Microsoft Windows technologies. Aelita's proven expertise with Active Directory and Exchange helps customers improve productivity, system availability and security. IT professionals choose Aelita solutions to administer, migrate, recover and audit these critical systems. The company's customers and partners include Bristol-Myers Squibb, HMS Host (formerly known as Host Marriott Services), Kmart Corporation, Pitney Bowes, Textron, Inc., Hewlett-Packard and Microsoft. Aelita is a global organization with headquarters in Columbus, Ohio. Contact Aelita at 800.263.0036 or visit www.aelita.com

Contacting Aelita Software Corporation:

Web: www.aelita.com
Technical Support: support@aelita.com
Sales: sales@aelita.com
General Inquiries: services@aelita.com
Phone: 614-336-9223 1-800-263-0036
Fax: 614-761-9620

Aelita Software Corporation

6500 Emerald Parkway
Suite 400
Columbus, Ohio 43016
USA