



## Introduction to Active Directory Application Mode

*Microsoft Corporation*

*Published: August 2002*

---

### **Abstract**

The Microsoft® Windows® 2000 Active Directory® service is the fastest growing directory service for intranets and extranets because of its rich integration of directory and security, scalability, and native Lightweight Directory Access Protocol (LDAP) support. Windows Server 2003 builds on that success by supporting a number of new LDAP capabilities in Active Directory targeted for IT professionals and applications developers. Active Directory Application Mode (ADAM) is one of the new capabilities that is part of Microsoft's fully integrated directory service available with Windows Server 2003. Organizations, independent software vendors, and developers wanting to integrate their applications with a directory service now have an additional capability within Active Directory that provides numerous benefits. This paper introduces ADAM and describes how it can benefit organizations.

*This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.*

*This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.*

*Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.*

*Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*© 2003. Microsoft Corporation. All rights reserved.*

*Microsoft, Active Directory, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.*

*The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

---

# Contents

<b>Introduction</b> .....	<b>1</b>
<b>Simplicity of Application Mode</b> .....	<b>3</b>
<b>ADAM Usage Scenarios</b> .....	<b>4</b>
Application Specific Directory Scenarios .....	4
Tailored Schema .....	5
Local Management in the Enterprise .....	6
Optional Centralized Management.....	6
Microsoft Windows NT 4.0 Domains .....	6
Application Developer Scenarios .....	6
Simple Setup .....	6
Locally Installed, Locally Managed .....	6
Extranet Access Management Scenarios.....	7
Migration Scenarios .....	7
<b>Customer Benefits</b> .....	<b>9</b>
Rich and Extensible Store.....	9
Replication.....	9
Setup and Removal.....	9
Multiple Instance Support.....	10
Backup and Restore.....	10
Tool Support.....	10
Security.....	10
Platform Support .....	11
<b>Summary</b> .....	<b>12</b>
<b>Related Links</b> .....	<b>13</b>

---

## Introduction

Originally inspired by the emergence of Lightweight Directory Access Protocol (LDAP)-based solutions in the mid-1990's, organizations have been deploying directory-enabled business solutions that solve key problems such as white or yellow-pages access, extranet or Web single sign-on capabilities, infrastructure for public key deployment, Network Operating System (NOS) user support, or line-of-business applications.

The result of this success is that, in most organizations today, it is common to find a directory service that is used to handle NOS authentication and authorization, one that is used by a Public Key Infrastructure (PKI) product for remote access (VPN), a white pages directory, and most likely, a directory service that supports extranet or Web single sign-on. Furthermore, it is not uncommon to find that a company has not only deployed multiple directory services, but that these directory services are based on different directory technologies. For example, the NOS directory might be based on the Microsoft Active Directory® service, while the PKI directory is based on an X.500 directory, and the white pages and line-of-business directories are based on yet another directory technology.

If each of these different directories is based on LDAP, the obvious question is: Why haven't organizations been able to standardize on one directory technology? The answer lies in the factors that have contributed to this phenomenon.

- **Lack of directory interoperability** — Numerous directory services simply do not interoperate with each other. A historical example is the original X.500 directories that did not support the LDAP protocol. Today, some products that implement a directory as part of their solution do not support LDAP or other widely used protocols.
- **Lack of choice** — Some vendors ship solutions that are “certified” to work only with a limited subset of the directory services in use today. Their customers may be forced, for support reasons, to implement a directory service that is not already in use within their firms.
- **Lack of coordination** — In some cases, groups in isolation from one another have installed different business solutions. This has resulted in the deployment of multiple directory technologies.
- **Lack of security interoperability** — Business solutions seldom allow the use of identity credentials that are stored in a directory service but not associated with those specific solutions. This means, once again, deploying even more directory services to act as the secure credential stores for each individual business solution.

Many companies are only now starting to come to grips with the hidden costs associated with the proliferation of multiple directory technologies:

- **Increased security risk** — As business solutions that rely on directories proliferate, it becomes increasingly difficult to ensure that those solutions will integrate effectively with business processes. As employees, partners, contractors, or customers initiate or terminate their relationships with a company, it is crucial that their access to VPN, PKI, NOS or other business solutions is initiated or terminated immediately. When management overhead causes slow initiation, productivity is impacted. On the other hand, when termination is not quickly reflected in the various directories, a security risk develops, allowing an unauthorized individual to continue having access to a business solution.
- **High cost of ownership** — Every business solution that is based on a different directory technology requires:

- A staff that is trained on that technology
- Different operational and administrative procedures
- Maintenance of additional software licenses and separate support agreements
- **Increased cost of “success”** — Some directory technologies are licensed according to the number of objects that are created in the directories. This means that licensing and maintenance costs start spiraling as a business solution becomes more and more successful. Today, this unfortunate situation impacts companies planning to deploy extranet access management solutions that are intended to service millions of customers.
- **Lack of Business Process Integration** — Directory information can be volatile. As users move from one group to another, change office locations or telephone numbers, change names or job titles, their information needs to be updated in the directory. If this information is relied upon by other business solutions that have a different directory, then the other directory must also be updated. Without an automated process to effect these changes, data becomes stale and unsynchronized across identity stores.

What customers really need is a directory that they can deploy to support both their NOS infrastructure — such as Active Directory — and application use that can, where appropriate, leverage the security that has been built into their NOS infrastructure. Active Directory in “Application Mode” achieves this goal without the burden of expensive training, additional licensing, or the operational costs incurred by the installation of a different directory technology to support a directory-enabled application.

Active Directory Application Mode (ADAM) is a new capability of Microsoft Active Directory that addresses certain deployment scenarios related to directory-enabled applications. ADAM runs as a non-operating system service and, as such, does not require deployment on a domain controller. Running as a non-operating system service means that multiple instances of ADAM can run concurrently on a single server, with each instance being independently configurable.

While the vision of a single enterprise directory is still unfulfilled, Active Directory Application Mode represents a breakthrough in directory services technology that overcomes these obstacles, maintains flexibility, and helps companies avoid increased infrastructure costs.

---

## Simplicity of Application Mode

Many applications require only a simple application directory. The information stored in this directory might be neither globally interesting nor needful of wide replication. It might require a different service level from the one offered by existing domain controllers hosting a NOS directory. For example, the application data might contain highly volatile information, causing high replication traffic that could strain network resources if stored in the NOS directory. In such cases, ADAM provides locality of data and satisfies the dedicated store requirements of an application.

Application directories evolve over time — business requirements change and force changes in directory schema, or configuration. Active Directory Application Mode runs as an independent service as opposed to, an operating system service. Therefore, you can modify local or targeted ADAM instances without requiring changes to the corporate directory infrastructure.

The ADAM capability is easily installed or uninstalled on developer workstations. This design feature allows rapid restoration to a clean state during the application prototyping and development process.

Furthermore, as detailed in the next section, “ADAM Usage Scenarios,” you can use ADAM effectively in the following scenarios:

- Application-Specific Directory Scenarios
- Application Developer Scenarios
- Extranet Access Management (EAM) Scenarios
- Migration Scenarios

---

## ADAM Usage Scenarios

As an infrastructure directory, the Active Directory service can play a variety of roles within an organization, ranging from the NOS role for managing Windows® networks to supporting directory-enabled e-commerce applications. Active Directory must be used for the purpose of managing security identities in Windows and managing networks comprised of Windows-based clients, Windows-based servers, and security-integrated applications like Microsoft Exchange. Active Directory is also used for data that is shared between applications and with applications that need to distribute their data across entire Windows networks.

Independent software vendors (ISVs) and corporate application developers face a variety of challenges in providing directory-enabled applications to organizations when the organizations have no directory services deployed, or even when the organizations have fully deployed corporate directories. These are some of the typical issues:

- Developers of customized directory service applications are sometimes faced with integrating their products into existing NOS directory deployments that may require extensive planning and implementation.
- Enterprise organizations that use an enterprise directory service require flexibility between departments when business goals or strategies differ. Changes like schema extensions cause friction and affect the entire enterprise directory deployment.
- ISVs are unable to deploy directory-enabled applications in enterprises where a directory does not exist. They have to either wait until a directory is deployed or risk losing the business to a competing application that uses a different store.
- Developers want a simple directory that they can easily program to without requiring extensive setup or hardware support during the development process.

The following scenarios illustrate some solutions that use ADAM to address these challenges.

### Application Specific Directory Scenarios

Consider a scenario where a portal application must store personalization data associated with users authenticated by the NOS Active Directory, but storing this personalization data in the NOS directory would require schema changes to the user class in the NOS directory. In such a case, the application can use Active Directory for authentication and service publication while using ADAM to store user personalization data. Figure 1 portrays this architecture.

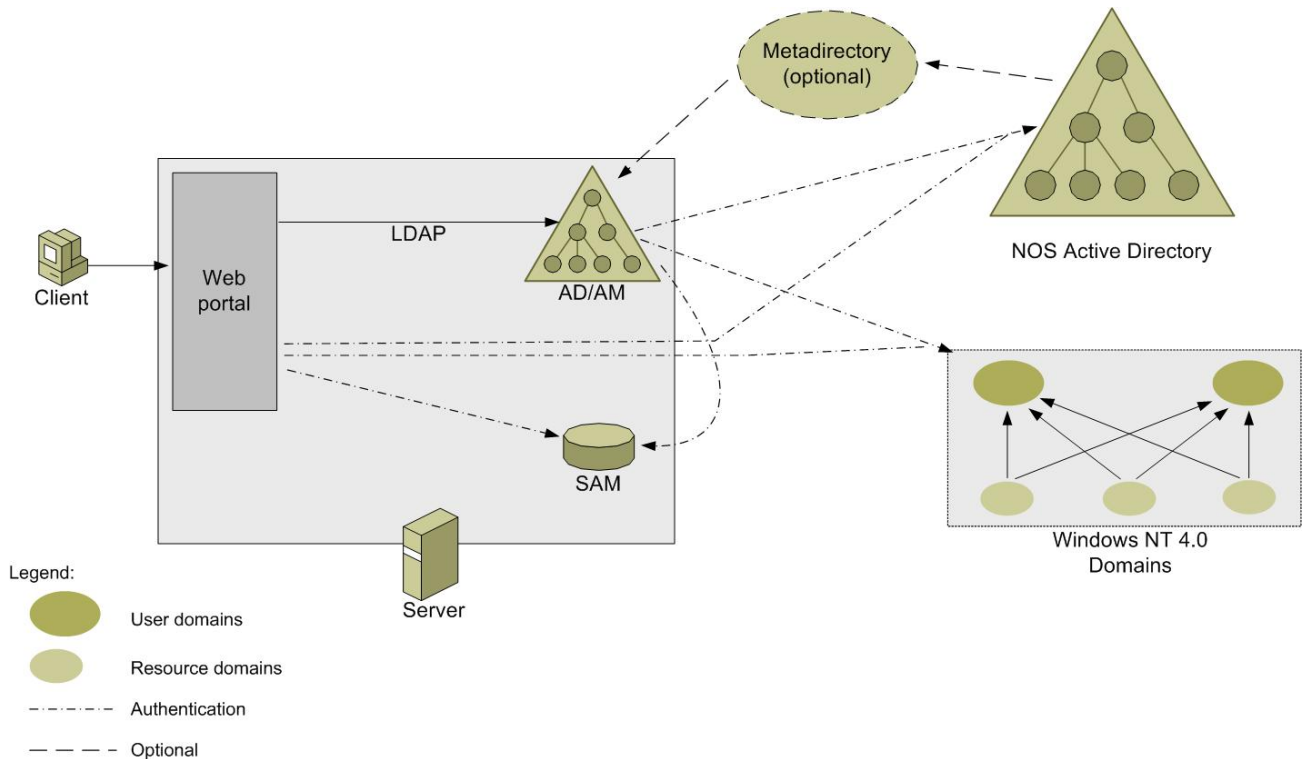


Figure 1: Application Specific Solution

ADAM allows an application to store “private” directory data that is relevant only to the application in a local directory service, perhaps on the same server as the application, without requiring any additional configuration to the NOS directory. The personalization data, which is only interesting to the portal application and does not need to be widely replicated, is now stored solely in the ADAM directory associated with the application. This solution also reduces replication traffic on the network between domain controllers.

Still, the applications can store their data in either Active Directory or in ADAM. If the data is of global interest to NOS directory users, it can be stored in Active Directory domains and exposed via the NOS directory’s Global Catalog. If you want the application to store application-specific data, such as policies and management information that are only needed by this application, you can store this data in ADAM while using the user principals in Active Directory for authentication and for controlling access to objects in ADAM. This avoids the need for each ADAM directory to have its own user database, preventing a proliferation of user IDs and passwords for end users every time a new directory-enabled application is introduced on the network.

### Tailored Schema

Business data is most often organized uniquely for a particular business or organization. When a business must use a directory-enabled application, based on unique business logic or schema, ADAM can fill that role. For instance, an application developer might want to expose application data via LDAP in a way that is unique and specific to the clients of the application. The application requires a different schema from the current NOS Active Directory installation. Without altering the configuration of the NOS Active Directory, the ISV can provide an ADAM-based application with a tailored schema that meets the business needs, data requirements, and workflow processes. This approach allows the workflow and associated data

represented by the application directory to be stored in the most intuitive way possible, independent of the existing NOS directory structure.

In addition, schema conflicts can arise when a variety of directory solutions exist. ADAM avoids schema conflicts by isolating one instance from another.

### **Local Management in the Enterprise**

Within every enterprise, departments seek out applications that are relevant to their operations. Because these applications are department-specific, the information stored by a particular application may be of no interest to the rest of the enterprise. The department might want to independently manage its local directory service because its service level requirements, such as replication schedules, differ from those offered by the enterprise directory. Active Directory Application Mode is a directory solution that is quick and easy to deploy locally in such a scenario.

### **Optional Centralized Management**

You can deploy the ADAM instance on a locally administered, departmental server or on a centrally managed server, thereby delegating the server management to the central IT department. The centrally administered server could host multiple, independently configured instances of ADAM on the same computer, thereby providing greater efficiency through server consolidation and ease of management. The different instances of ADAM can be used by different directory-enabled applications. These ADAM instances can also replicate their data to other replicas, independent of other instances, providing availability of data where needed.

### **Microsoft Windows NT 4.0 Domains**

Directory-enabled applications that use ADAM can work in Windows NT® 4.0 domains. You can install ADAM on a server running Windows Server 2003 that is a member server in a Windows NT 4.0 domain and target the application at ADAM. Since ADAM works with the Windows-integrated security infrastructure, ADAM can also authenticate users from Windows NT 4.0 domains.

### **Application Developer Scenarios**

ADAM could be a perfect fit for developers prototyping an application for Active Directory, since ADAM uses the same programming model and provides virtually the same administration experience as Active Directory. This advantage enables the developer to work with a local instance of ADAM on the developer workstation and then move the application to Active Directory at a later time.

### **Simple Setup**

ADAM installation uses a simple setup wizard that requires minimal manual input. The setup can easily be scripted, which is beneficial for unattended and silent installations as part of application installation. This allows the developer to install and uninstall ADAM or use multiple instances during the development phase. A developer could easily explore different paths by using multiple instances, and easily switch between instances to choose a different path, without reinstalling the directory. You do not need to reboot, either during setup or configuration.

### **Locally Installed, Locally Managed**

Consider the scenario where an application developer is developing a directory-enabled application. Current requirements for having the directory on a server or domain controller cause strain on organizations because the organizations have to provide and manage a server class development server. Moreover,

installing or uninstalling the directory can affect other users. ADAM does not need to be installed on a server or domain controller, and it runs effectively on client computers, so you can deploy an application without the resources of a dedicated IT professional. You can run ADAM on Microsoft Windows XP and servers running Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; or Microsoft Windows Server 2003, Datacenter Edition.

## Extranet Access Management Scenarios

Consider the scenario where there is a Web portal application that handles Extranet Access Management. OpenNetwork's DirectorySmart or Netegrity's SiteMinder solution are examples. The Web portal stores the authorization information as data in the directory and uses the directory for authentication purposes only. Figure 2 shows this extranet scenario.

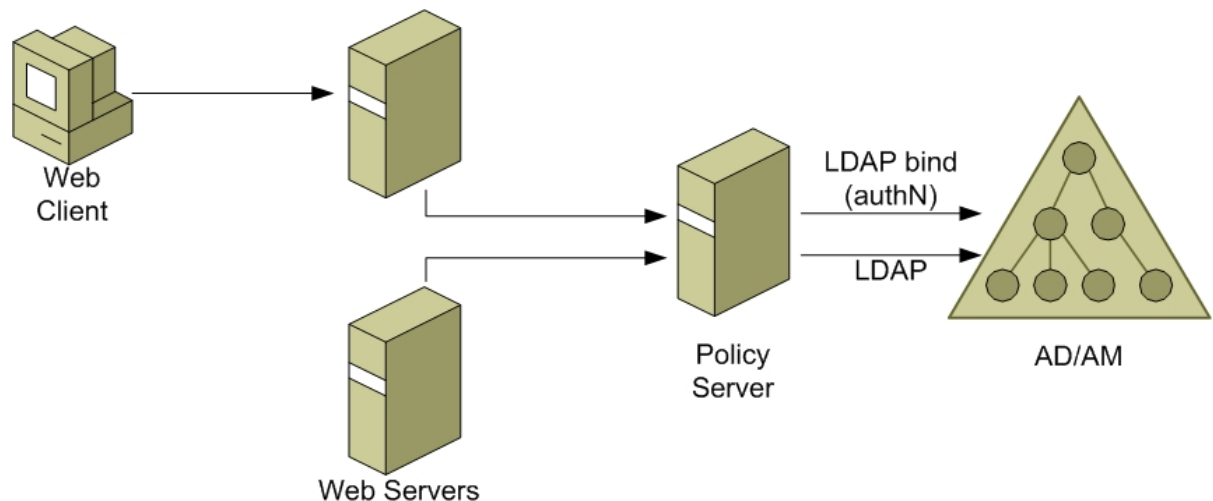
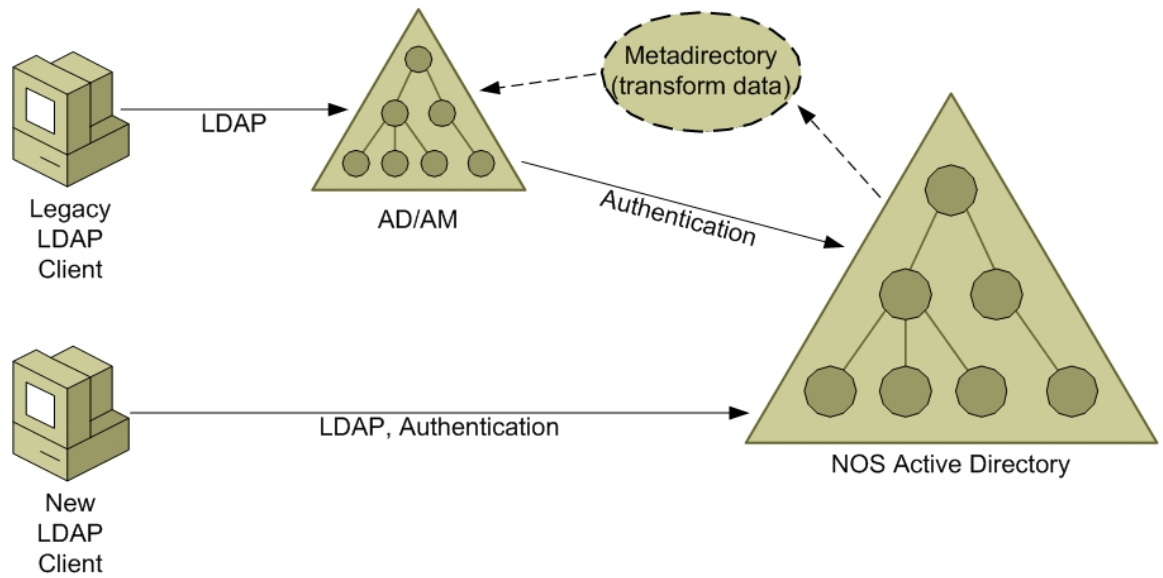


Figure 2: Extranet Access Management

In such cases, ADAM would be a perfect fit. Since ADAM can host user objects that are not Windows security principals but can be authenticated using LDAP simple binds, all the user information, as well as authorization data for these applications can be stored in ADAM. This configuration works well even in heterogeneous environments, and even when the NOS Active Directory is not present as the infrastructure provider. Web clients are serviced by a portal application that can run on any platform while using ADAM as a simple LDAP store.

## Migration Scenarios

Consider a scenario where an organization already has an established directory using X.500 style "O=<organization>, C=<country>" naming and relies on this directory to serve legacy applications. Figure 3 portrays a migration scenario to Active Directory, using ADAM as an interim solution.



*Figure 3: Migration to Active Directory*

In such cases, to enable migration to Active Directory, you can deploy ADAM to serve the applications that rely on X.500 style naming. You can deploy NOS Active Directory in the enterprise to provide a shared security infrastructure while deploying ADAM to provide direct support for the legacy applications. As you migrate applications to Active Directory, you can target them to the NOS Active Directory, as appropriate. You can use a Metadirectory, such as Microsoft Metadirectory Services 2003, to automatically synchronize the data in Active Directory and ADAM to allow for seamless migration experience.

---

## Customer Benefits

ADAM is an expanded capability of Active Directory that allows Active Directory to be deployed as a lightweight directory service for rapid implementation and flexible deployment of a directory service for applications.

### Rich and Extensible Store

ADAM supports a flexible and extensible schema, which allows you to easily customize the schema using tools such as Idifde, the ADAM Schema snap-in, and ADAM ADSI Edit, which are based on familiar Active Directory counterparts. Each instance of ADAM running on the same computer can have a different schema.

A single instance of ADAM can host multiple data partitions. This allows you to define storage, distribution and replication scope of partition data. The store allows for a flexible namespace, permitting both DNS style and X.500 style distinguished names.

The result is faster directory deployments that require less planning related to schema or naming conventions.

### Replication

ADAM uses the same multi-master replication model that Active Directory uses, which ensures that replicated data can be modified on any instance that participates in a replica set, not just one primary source. ADAM replication uses the same site model that Active Directory uses, offering features such as schedulable, compressed inter-site replication. You can manage it with familiar tools such as repadmin.

In Active Directory, replication of application data is intermingled with replication of changes to NOS data. Enterprise directory administrators usually determine the overall replication schedule of the NOS directory so that they can find the best fit for the needs of all applications. With ADAM, they can set the replication schedule of each ADAM instance to best fit the needs of specific applications.

In addition, you can replicate application data between multiple ADAM instances. You can run instances on servers that are members of an Active Directory domain, members of different domains in an Active Directory forest, or computers that are members of workgroups.

### Setup and Removal

The ADAM setup uses the familiar Windows-based installer. Minimal manual input is required and you can easily script setup. This is beneficial for unattended, silent installations that are part of a vendor application install. The installation wizard allows you to create a new instance or to create a replica of an existing instance.

In addition, a removal wizard deletes:

- Instances that you select
- All associated files containing the configuration data
- The associated partition

The ease of setup, installation, and removal saves administrator time and makes it very easy to move ADAM from testing to deployment.

## Multiple Instance Support

Multiple instances of ADAM can run concurrently on a single server, where each instance can be configured independently of other instances and isolated from other instances running on the same computer. Each instance of ADAM is identified by a unique name and port.

ADAM multiple instance support provides significant benefits in the enterprise, such as server consolidation, line of business (LOB) application development, and incremental upgrades to an enterprise suite of applications. In smaller organizations, multiple instance support allows you to configure each instance for specific requirements of different applications, and allows querying of different data stores on the same computer.

## Backup and Restore

ADAM is integrated with the backup and restore capabilities provided by the Windows operating system. Every instance is backed up through a configurable, automated, online process that allows immediate access to critical data. ADAM allows online backup and offline restore using the NTBackup utility.

## Tool Support

Since ADAM is a mode of Active Directory, the administration experience is very similar, using tools based on familiar Active Directory tools. The ADAM administration tools are installed along with the application.

- Ldp (Ldp.exe) permits LDAP operations to be performed against ADAM, and it is part of the support tools for the products in the Microsoft Windows 2000 Server family and the Microsoft Windows Server 2003 family. LDP uses a graphical user interface.
- ADAM ADSI Edit is based on the familiar ADSI Edit tool, and can be used to view all objects in the directory (including schema and configuration information), modify objects, and set access control lists on objects.
- Familiar tools, such as PerfMon, can be used to monitor network and system performance with ADAM. You can collect data from each instance of ADAM in counter and trace logs and customize viewing capabilities with the Microsoft Management Console (MMC).
- Dsadmin, and dsdbutil (similar to ntdsutil) can be used to perform database maintenance, manage and control single master operations, remove unwanted metadata, and create directory partitions.

You save training time and money because you can maintain ADAM with tools very similar to those you use to maintain Active Directory.

## Security

ADAM leverages the security model of the Windows operating system. You can control access to objects inside ADAM as well as the service by using:

- Users from the NOS Active Directory
- A Windows NT 4.0 domain infrastructure
- Accounts stored on the local computer

ADAM supports LDAP authentication with security credentials from an external shared security infrastructure, if one is present. Security principals can be used from the platform locally or from the NOS Active Directory. You can also create user accounts in ADAM to permit applications to rely on the directory

to handle authentication while the applications take care of authorization. In such cases, ADAM provides authentication solely through the LDAP simple bind mechanism.

Authorization to directory objects through ADAM is based on the existing Access Control List (ACL) model in Windows. This access control mechanism allows you to secure detailed access to any object in each instance. This mechanism is based on security descriptors for security principals already present in the existing Windows security infrastructure. Applications can extend this to use their own framework for authorization while using the directory service to provide authentication.

### **Platform Support**

The ADAM capability will be available on computers running on the following platforms:

- Windows Server 2003, Standard Edition
- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Datacenter Edition
- Windows XP Professional

---

## Summary

Companies, independent software vendors, and developers wanting to integrate their applications with a directory service now have an additional capability within Active Directory that provides numerous benefits:

- **Ease of Deployment** — Developers, end-users, and ISVs can easily deploy ADAM as a lightweight directory service on most Windows Server 2003 platforms and Windows XP Professional. You can easily install, re-install, or remove the ADAM application directory, making it the ideal directory service to deploy with an application.
- **Reduced Infrastructure Costs** — By using a single directory technology for both your NOS and application directory needs, you can reduce overall infrastructure costs. Additional investments are not required for training, administration, or management of your application directory. Application programming interfaces (LDAP, ADSI, DSML) are also equivalent, allowing you to build applications on ADAM and migrate them to the corporate NOS directory, as needed, with minimal change.
- **Increased Security** — Integration with the Windows security model allows any application that is deployed using ADAM the ability to authenticate access against a corporate-deployed Active Directory.
- **Increased Flexibility** — The application owner can easily deploy directory-enabled applications without affecting the corporate directory schema, while still using the identity information and credentials that are stored in the NOS directory.
- **Reliability and Scalability** — Applications using ADAM obtain the same reliability, scalability and performance that they have had with deployments of Active Directory in the NOS environment.

For the first time, you can employ a single directory technology in multiple roles while preserving investments made in administrator training, operations, licensing, and most importantly, security. Companies, ISVs and developers can use Active Directory in multiple roles, without having to face the increased costs associated with deploying multiple technologies for both a NOS and an application directory.

---

## Related Links

For the latest information about Windows Server 2003, see the [Windows Server 2003 Web site](http://www.microsoft.com/windowsserver2003/default.mspx) at <http://www.microsoft.com/windowsserver2003/default.mspx>.