



User Authentication Set Up Guide

Preface

General Information about this guide

by Academic Management Systems

This manual outlines the different types of authentication and how to set up external authentication on a server. The goal of this manual is to provide Academic Management System clients with the information necessary to correctly set up authentication.

CoursEval Authentication Guide

© 2009 Academic Management Systems

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: November 2009 in Amherst, NY
CoursEval Build 60
© 2009 Academic Management Systems

Table of Contents

Foreword	0
Part I User Authentication Set Up	1
1 Introduction	2
2 Supported Types of User Authentication	3
Internal Authentication	3
Benefits of Internal Authentication	3
Disadvantages of Internal Authentication	3
External Authentication Types	3
Domain Authentication	4
Benefits of Domain Authentication	4
Disadvantages of Domain Authentication	4
ADSI Authentication	4
WinNT Provider	5
LDAP Provider	5
NetWare Directory Services Provider (NDS)	5
Novell 3.x Provider (NWCOMPAT)	5
Specifying the ADS Path and other ADSI options	6
Examples of ADS Path values for the available providers	6
ADS Path Samples	6
User Name Mask Samples	7
Other ADSI Connection Options	8
Authenticating Against an LDAP Server	9
ADS Path for LDAP	9
User Name Mask for LDAP	10
Example 1	10
Example 2	12
Other information about LDAP Authentication	13
Benefits of ADSI Authentication	14
Disadvantages of ADSI Authentication	14
Custom Authentication Modules	14
Benefits of Custom Authentication	15
Disadvantages of Custom Authentication	15
Testing Authentication Settings	15
Two ways of Testing	15
Testing Settings from the list view of the "User Authentication Setup" interface	16
Disclaimer	16
Index	17

1 User Authentication Set Up

The Authentication Set Up feature allows the CourseEval Administrator to set up how CourseEval will authenticate faculty and students when they log into the program. By default, individual faculty and students are allowed into their respective portals if the password they provide matches the one stored internally in the CourseEval database.

CourseEval supports many different ways to authenticate user identity prior to granting access. This section is designed to help the CourseEval Administrator and IT Staff decide which type of authentication is best for a school's site and to assist with the configuration and testing of the authentication method that is decided on.

Before determining whether to externally authenticate users, please read this entire section carefully and make sure that the advantages and disadvantages of each approach are understood.

User Authentication Setup List				[Help]
Settings For	Auth. Method	Details	Test	
Faculty and Students (Survey Portal Only)	Internal		N.A.	
1 record found.				
[Help]				

Authentication Test: Faculty and Students (Survey Portal Only)

User Name: testusername

Password: testpassword

Result: Authentication failed. The user name and password were not accepted.

Message from Authentication Module:

The custom module specified does not exist.

Close

User Authentication Setup: Faculty and Students (Survey Portal Only)

Select Authentication Method:

Internal Authentication [?](#)

Domain Authentication (Windows Networks)
 Domain Name(s): [?](#)

MS ADSI Authentication
Choose Provider: (ADSI Namespace)

- WinNT
- LDAP
- Novell Network Directory Services (NDS)
- Novell Netware 3.x (NWCOMPAT)

ADS Path(s):
 [?](#)
[View Samples](#)

User Name Mask(s):
 [?](#)
[View Samples](#)

Other ADSI Connection Options:

<input type="checkbox"/> Secure Authentication ?	<input type="checkbox"/> Encrypt data exchange over network. ?
<input type="checkbox"/> Encrypt channel using SSL ?	<input type="checkbox"/> Write-able domain controller is not required. ?
<input type="checkbox"/> Use fast binding ?	<input type="checkbox"/> Verify data integrity with signing. ?
<input type="checkbox"/> Encrypt data with Kerberos ?	<input type="checkbox"/> Allow ADSI to delegate security context. ?
<input type="checkbox"/> Bind to server ?	

Authenticate using a Custom Module (Provided by AMS)
 Path to Custom Module:
 User name and password are entered and verified remotely

Test Settings: User Name: Password: [Test Now](#)

Back to List Help

1.1 Introduction

CoursEval and eCV support many different ways to authenticate user identity prior to granting access. This document is designed as a guide to help users decide which type of authentication is best for use with CoursEval or eCV and to assist in the configuration and testing of the authentication method chosen.

Before deciding whether to externally authenticate users, please read this entire document carefully and make sure that the advantages and disadvantages of each approach are fully understood.

1.2 Supported Types of User Authentication

- [Internal Authentication](#)
- [Domain Authentication](#)
- [ADSI Authentication](#) (Windows AD, LDAP, NDS, and Novell 3.x)
- [Custom Authentication Modules](#)

1.2.1 Internal Authentication

Internal authentication is the default method of verifying user identity. When using internal authentication, encrypted passwords are stored in the local database and matched with those entered by the user when they attempt to log in. With this method of authentication, users are given a 'default password' based on a field selected when user information is imported into the program. For example, default faculty passwords might be their University ID, or even a combination of their University ID number and date of birth.

1.2.1.1 Benefits of Internal Authentication

- Easy to set up and administer
- Allows for login information to be sent to the user
- Allows the user to change the password they use to access the program
- Does not rely on external servers or network services to authenticate users, so there is no chance a network connection or configuration problem will result in erroneous login failures

1.2.1.2 Disadvantages of Internal Authentication

- Users must remember (and safeguard) an additional password
- Depending upon the default password selected when user data are imported, it might pose a security risk if the default value is well-known and the login portal is made public

1.2.2 External Authentication Types

The following types of external authentication are supported by CoursEval:

- Domain Authentication
- ADSI Authentication
 - WinNT

- LDAP
- Netware Directory Services
- Novell 3.x Provider
- Custom Authentication

1.2.2.1 Domain Authentication

This method of authentication relies on the Microsoft LogonUser() Win32 API. It works by passing the user name and password provided by the user to the domain controller or server specified in the "Domain" field on the User Authentication Setup form. The name entered here is the NetBIOS name of the network resource.

Of all the external authentication choices, this one will provide the best performance for sites where a lot of users (2000+) are logging in frequently.

1.2.2.1.1 Benefits of Domain Authentication

- Users can continue to utilize the user name and password they normally enter to access other network resources on campus
- Very fast external authentication mechanism
- Very easy to set up if there is a single domain controller or server managing the targeted group of users

1.2.2.1.2 Disadvantages of Domain Authentication

- It will only work if there are domain controllers or servers running Windows operating systems.
- It is limited to authenticating user accounts managed on one domain controller or server. So, if a school has student accounts scattered across multiple domains, this method will not work. (At the same time, it is important to remember that this also makes it a more secure choice.)
- If the DC is unavailable due to network problems, users will not be able to log into the application.

1.2.2.2 ADSI Authentication

ADSI (Active Directory Services Interface) is a relatively new technology from Microsoft which attempts to abstract the capabilities of many different types of directory services and provide a common way of communicating with those services. Schools do not have to have Active Directory deployed campus-wide to use this authentication method. ADSI Authentication will work best if the web server is running any version of Windows 2000 Server or Windows Server 2003. Schools can use it with Windows NT 4.0 servers as well, but the latest version of ADSI needs to be downloaded from the [Microsoft web site](#). ADSI is installed by default with Windows 2000 Server and Windows Server 2003 operating systems.

By looking at the MS ADSI Authentication setting section on the User Authentication Setup form, one can see that this approach is by far the most flexible and is a good choice for sites which utilize non-Windows directory services, such as LDAP and Novell NDS.

To setup ADSI Authentication, choose a 'Provider,' which tells ADSI what type of directory service it will be accessing. This is also sometimes called the 'ADSI Namespace.' The following choices are available:

- WinNT
- LDAP
- Novell Network Directory Services (NDS)
- Novell Network 3.x (NWCOMPAT)

A description of each ADSI Provider appears below, followed by details regarding the ADS Path, User Name Mask, and Connection Options fields.

1.2.2.2.1 WinNT Provider

The WinNT provider allows a school to authenticate user credentials against Windows-based domain controllers or servers. Some of this functionality is present in the "Domain Authentication" option, but there may be cases where either local computer or network security policies prevent the "Domain Authentication" module from accessing the remote domain controller or server.

1.2.2.2.2 LDAP Provider

The LDAP provider allows schools to authenticate users stored in LDAP v.2 or v.3 directories. Schools can also use this provider to authenticate against any MS Windows 2000 Active Directory service.

1.2.2.2.3 NetWare Directory Services Provider (NDS)

The NDS provider allows authentication through Novell directory services and should be selected if the school is running IntraNetWare 4.x or 5.x. IntraNetware is also LDAP compliant, so the LDAP provider can be used if preferred. **The Gateway (and Client) Services for Netware must be installed on the server to use this provider.** For more information, click [here](#).

1.2.2.2.4 Novell 3.x Provider (NWCOMPAT)

This provider facilitates authentication against the Novell NetWare bindery. Schools should select this provider if they are running NetWare 4.x, 3.2, 3.12 or

3.11 servers in bindery-emulation mode.

1.2.2.2.5 Specifying the ADS Path and other ADSI options

For all ADSI providers, except for LDAP, the ADS Path must point to a unique user object. **This is very important because it is possible that the current directory configuration allows anonymous binding to a given resource and this could unintentionally allow any user name and password to be accepted.** For LDAP authentication, the ADS Path can almost always contain the server's base DN, with the User Name Mask pointing to a unique user in the directory. This often depends upon the structure of the directory. Regardless of the provider being used, always thoroughly test the settings before saving. Be sure to read the section on "Testing Authentication Settings" below.

Entering the path to a unique user object is the only way to ensure that the user is being authenticated properly. In order to ensure the path is unique, the user name must become part of the connection string. To accomplish this, the interface allows the administrator to enter the placeholder string #UNAME# where the user's name should be inserted into the ADS Path. Again, this does not usually apply to LDAP server authentication unless the structure of the directory requires it.

1.2.2.2.6 Examples of ADS Path values for the available providers

1.2.2.2.6.1 ADS Path Samples

ADSI Provider	Example
WinNT	<p>The following example assumes ADSI will connect to a domain with a NetBIOS name of "NT4DOMAIN".</p> <p>NT4DOMAIN/#UNAME#, User</p>
WinNT	<p>This example assumes ADSI will connect to a server named "ETALUS" located in a domain named "NT4DOMAIN".</p> <p>NT4DOMAIN/ETALUS/#UNAME#, User</p> <p>Note the ", User" string that follows the user name placeholder. This is a reference to the 'object class' to which the authentication operation will attempt to bind. While specifying the object class is not necessary, it will most likely improve the performance of the bind operation and should be used unless</p>

	there is a valid reason for doing otherwise.
LDAP	This example binds to a user object through a specific server identified by its NetBIOS name. Note the port specification after the server name. This may or may not be required. StuServer:636/ou=people,dc= yourschool.dc=edu
LDAP	This example binds to a user object through a specific server identified with a fully qualified domain name. ldap.yourschool.edu:636/dc=yourschool,dc=edu
LDAP	This example shows multiple LDAP paths, using a semicolon to separate them. ldap3.urd.edu:636/ou=stu,dc=roland,dc=edu; ldap1.urd.edu:636/ou=fac,dc=roland,dc=edu
LDAP	This example shows multiple domains using an organizational unit (OU). ldap1.urd.edu:636/ou=[stu~fac~staff],dc=roland,dc=edu
NDS	This example binds to a user object in an organizational unit named stuorg, which resides in an intraNetWare tree named StuTree StuTree/o=stuorg/dc=edu,dc=yourschool,cn=#UNAME#
NWCO-MPAT	This example binds to a user object that exists on a server named STUSERVER in the NetWare bindery. STUSERVER/#UNAME#

1.2.2.2.6.2 User Name Mask Samples

ADSI Provider

Example

WinNT

A user name mask should not be needed if a school is using the WinNT provider.

LDAP

uid=#UNAME#,ou=student,dc=buffalo,dc=edu

NDS Check with the NDS administrator to verify whether or not the user name needs to be referenced by group. If so, it will most likely look like the example below.

students.#UNAME#

NWCOMPAT A mask should not be needed.

The [Authenticating Against an LDAP Server](#) section explains advanced syntax for the User Name Mask Field and provides more detail about configuring the server for LDAP authentication

1.2.2.2.6.3 Other ADSI Connection Options

Option	Comments
Secure Authentication	When using the WinNT provider, AD will use Kerberos and possibly NTLM to authenticate the user. Unless the school has a valid reason for doing otherwise, this option should always be checked.
Encrypt data exchange over network	This option forces ADSI to use encryption for data exchange over your network. It is not supported by the WinNT provider.
Encrypt channel using SSL	Enabling this option will encrypt the channel using SSL. ADSI requires the Certificate Server be installed to support SSL. This option is not supported by the WinNT provider.
Write-able domain controller is not required	This option has no effect on a Windows Server 2003 or Windows 2000 network. The school may need to enable it if they have a Windows NT 4.0 network.
Use fast binding	This option may increase performance as it limits the amount of information ADSI needs to extract from the target service during the bind operation.
Verify data integrity with signing	If enabled, the Secure Authentication option must also be selected. This option is not supported by the WinNT provider.
Encrypt data with Kerberos	Enables Kerberos encryption (sealing). If enabled, the Secure Authentication option must also be selected. This option is not supported by the

	WinNT provider.
Allow ASDI to delegate security context.	This option may be needed if authentication occurs across domains.
Bind to server	Check this option if the school is using the LDAP provider and the ADS Path includes a server name. Do not select this option if the ADS Path includes a domain name or for a serverless bind. If a server name is specified in the ADS Path and do not check this option, unnecessary network traffic can result.

1.2.2.2.7 Authenticating Against an LDAP Server

Configuring for external authentication against an LDAP server can be confusing if the school has a very complex directory and the simple examples shown above do not seem to be helpful. While it is true the values entered into the **ADS Path** and **User Name Mask** fields can be more verbose for LDAP than those entered for the other ADS providers, the information in this section should provide all the information needed to understand the purpose of these fields and exactly what should be entered for the school.

1.2.2.2.7.1 ADS Path for LDAP

- Unlike the other ADS providers, the ADS Path for LDAP will most likely always be the server's base DN. There are cases where the path needs to be more unique or multiple paths are needed, but these are rare
- If the LDAP server does not support SSL, Academic Management Systems recommends that a school NOT use it for authentication. The reason for this is the application will be attempting to bind to the LDAP server by sending the entered User Name and Password. Without SSL encryption, these values would be sent in plain text over the wire, which is extremely risky
- If the LDAP server supports secured and unsecured connections, the port for secure communication should always be appended to the server URL. For example: ldap1.buffalo.edu:636/dc=buffalo,dc=edu

Note: A fully qualified path is not required, for example the protocol "ldap://" does not need to be included.

1.2.2.2.7.2 User Name Mask for LDAP

For LDAP authentication, the User Name Mask can be thought of as a 'template' for the full path to individuals in the directory. Since individual records are usually located in different sections of the directory, multiple User Name Mask entries are often entered and separated by semicolons. Do not worry if the directory is very complex as there is special syntax supported to avoid having to enter repetitive values. (See examples below)

The easiest way to understand what should be entered into the ADS Path and User Name Mask fields is to see some "real world" examples.

Root or Base DN (dc=southmore,dc=edu)

ou=students

uid=abnerj

uid=acerm

uid=addek

ou=faculty

uid=alfredson

uid=brunswick

uid=chambers

ADS Path:

ldap1.southmore.edu:636/dc=southmore,dc=edu

User Name Mask:

uid=#UNAME#ou=students,dc=southmore,dc=edu

uid=#UNAME#ou=faculty,dc=southmore,dc=edu

The User Name Mask above is repetitive. Had there been further divisions, faculty by departments for example, there could have been dozens of separate User Name Masks required. In cases where the values that need to be entered are the same except for one value, such as 'students' and 'faculty' above, use the syntax shortcut shown below.

Simplified User Name Mask for Example 1:

```
uid=#UNAME#, ou=[students~faculty].dc=southmore.dc=edu
```

When this syntax is used, the bind operation will try each value between the square brackets [] until one succeeds or all fail. Because of this, it is wise to put the most likely value first. For example, if thousands of students will be logging into the application and only a few hundred faculty members, it would be best to list 'students' first in the example above.

As many values as needed can be entered between the square brackets [] – separated by a tilde character ~.

Root or Base DN (dc=buffalo,dc=edu)**ou=students****ou=A****uid=Abnerj****uid=Acerm****uid=Addelk**

...

ou=B**ou=C**

...

ou=X**ou=Y****ou=Z****ou=faculty****ou=art****uid=alfredson****uid=brunswick****uid=chambers****ou=biology****ou=chemistry****ou=education****ou=math****ADS Path:**

ldaps:buffalo.edu:636/dc=buffalo,dc=edu

User Name Mask:

uid=#UNAME# ou=students ou=[a~b~c~d~e~f~g~h~i~j~k~l~m~n~o~p~q~r~s~t~u~v~w~x~y~z],dc=buffalo,dc=edu;

uid=#UNAME# ou=faculty ou=[art~biology~chemistry~education~math],dc=buffalo,dc=edu

The ADS Path above is straightforward and similar to the first example. The User Name Mask, however, is far more complicated. There are two User Name Masks entered, one for the section of the LDAP directory where student information is stored and another for the location of individual faculty records. Even though these User Name Mask entries make use of the square bracket notation `[]` introduced in the previous example, they are still more verbose than they need to be. The example below demonstrates a different way of writing these User Name Masks using two other shortcut notation features.

Simplified User Name Mask for Example 2:

```
uid=#UNAME#.ou=students.ou=[A-Z].dc=buffalo.dc=edu;
```

```
uid=#UNAME#.ou=faculty.ou=[?].dc=buffalo.dc=edu
```

The first part of the User Name Mask uses a 'Rolodex' type shortcut `[A-Z]` to indicate a node for each letter of the alphabet under the Student node. This only works for the letters of the alphabet since it is a commonly used organizational convention in LDAP structures.

The second part of the User Name Mask uses a question mark `[?]` inside of square brackets. This tells the authentication parser to do a sub-tree search for every node found along that path. So, if there were 30 faculty departments instead of just five as shown in the example, they would be discovered dynamically. There is intelligent caching done behind the scenes to prevent this discovery from happening every time a user is authenticated and to optimize the search based on where people are actually found when a successful bind occurs.

Note: In the example above, the `[A-Z]` shortcut in the first User Name Mask could be replaced with `[?]` and the letter nodes would be discovered dynamically. However, this would be asking the authentication engine to do more work than necessary since the available nodes are already known and unlikely to change, which is not the case with list of department nodes in the second User Name Mask.

1.2.2.2.7.3 Other information about LDAP Authentication

- **If the LDAP server does not support SSL, Academic Management Systems recommends that the school *NOT* use it for authentication.** The reason for this is the application will be attempting to bind to the LDAP server by sending the entered User Name and Password. Without SSL encryption, these values would be sent in plain text over the wire, which is extremely risky.
- If the LDAP server supports secured and unsecured connections, the port for secure communication should always be appended to the server URL. For

example: ldap1.buffalo.edu:636/dc=buffalo,dc=edu

- If it is convenient to use the `=[?]` wildcard notation in the User Name Mask field to dynamically get a list of LDAP entities during the authentication request, this convention should only be used once per User Name Mask entry. It is okay to have more than one in the field, as long as each entered User Name Mask, separated by a semicolon, only contains one.
- It is not necessary to provide a User Name Mask for every LDAP path to user records in the directory. Only enter User Name Masks to locations in the directory where users who will be logging into CourseEval exist, (faculty and students).
- Whenever possible, enter the most likely location for a bind first into the User Name Mask field. For example, it is often best to assume most users logging in to the program will be students. So, the User Name Mask pointing to the location of student records should appear before one pointing to faculty records in the directory. Again, this assumes faculty and student records exist in different locations, which may not be the case at a school.

1.2.2.2.8 Benefits of ADSI Authentication

- Users can continue to use the user name and password they normally enter to access other network resources on campus.
- Very flexible and can be configured to work well in almost any network environment with most common directory services.

1.2.2.2.9 Disadvantages of ADSI Authentication

- If the directory service becomes unavailable, users will not be able to log into the application
- Requires a good understanding of directory service conventions and object binding to configure

1.2.2.3 Custom Authentication Modules

A custom authentication module is a good choice if a school wishes to externally authenticate users, but is working in an environment that does not utilize any of the directory services or technologies supported by the built-in external authentication interface. Choosing this method of authentication requires a custom module. A custom module is a special program written for the school by Academic Management Systems.

To discuss the unique needs of your school, or if you have other questions about

custom authentication, please contact [us](#).

1.2.2.3.1 Benefits of Custom Authentication

- Allows for external authentication against any non-standard or currently unsupported directory service

1.2.2.3.2 Disadvantages of Custom Authentication

- The customer must pay for the development and testing of the custom authentication module

1.2.2.4 Testing Authentication Settings

Unless a school is using Internal Authentication, it is extremely important to thoroughly test the settings before saving. When external authentication is configured and enabled, there are three possible results:

1. The authentication mechanism will work as expected.
2. None of the users will be able to log in.
3. All users will be granted access, regardless of the password entered.

Obviously, only one of these possible outcomes is desirable. In order to ensure the other two do not occur, schools will need to test the settings before saving changes on the User Authentication Setup form.

To test settings click the "Test Now" link at the bottom of the form. When this is done a new "Authentication Test" window will pop up and contain the details of the test results.

1.2.2.4.1 Two ways of Testing

- 1. Test by entering an invalid user name and password into the fields provided.** The purpose of doing this is to make sure the target service properly rejects invalid credentials. If the settings are correct, the "Authentication Test" window should show a message from the authentication module indicating that the user name could not be found or the user name and/or password were invalid. Above all else, this confirms that the authentication module is properly communicating with the remote directory service or computer and verifies that anonymous binding is not allowed.
- 2. Test by entering a valid user name and password of a user that has an active account in the remote directory service or domain to which the server is connecting.** If user credentials are valid, the "Authentication Test" window will confirm with a message indicating that the authentication succeeded. Once this happens, test this again with a valid user name and an invalid

password to make sure the remote directory service or domain properly denies the request.

1.2.2.4.2 Testing Settings from the list view of the "User Authentication Setup" interface

To test the settings from the list view of the "User Authentication Setup" interface, click the "test" icon in the last column of the site list. In this case, the test call will send a user name of "testuser" and a password of "testpassword" to the authentication module. The purpose is to simply verify the connection and should be expected to fail with a message of "User name not found" or "Invalid User Name / Password."

1.2.2.4.3 Disclaimer

Enabling external authentication is a serious decision and should be treated as such. If a school decides to use external authentication to verify the identities of the users, it is the school's responsibility to understand the technologies involved and to test the settings thoroughly before saving the configuration.

Academic Management Systems will not be held responsible for unauthorized access to any of its applications and/or the subsequent misuse or destruction of data that might result from unauthorized access.

By selecting any user authentication option other than Internal, a school is agreeing to accept sole responsibility for the proper configuration of external authentication at the school's site and furthermore agrees not to hold Academic Management Systems responsible for any loss that might result from invalid or inappropriate User Authentication settings.

Index

- A -

- ADS Path for LDAP 9
- ADS Path Samples 6
- ADSI Authentication 4
 - Benefits of ADSI Authentication 14
 - Disadvantages of ADSI Authentication 14
 - LDAP Provider 5
 - NetWare Directory Services Provider (NDS) 5
 - Novell 3.x Provider (NWCOMPAT) 5
 - Specifying the ADS Path and other ADSI options 6, 7, 8, 9, 10, 12, 13
- Appendix
 - User Authentication Set Up 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16
- Authenticating Against an LDAP Server 9, 13
 - ADS Path for LDAP 9
 - User Name Mask for LDAP 10, 12

- B -

- Benefits of ADSI Authentication 14
- Benefits of Custom Authentication 15
- Benefits of Domain Authentication 4
- Benefits of Internal Authentication 3

- C -

- Custom Authentication Modules 14
 - Benefits of Custom Authentication 15
 - Disadvantages of Custom Authentication 15

- D -

- Disadvantages of ADSI Authentication 14
- Disadvantages of Custom Authentication 15
- Disadvantages of Domain Authentication 4
- Disadvantages of Internal Authentication 3
- Domain Authentication 4
 - Benefits of Domain Authentication 4
 - Disadvantages of Domain Authentication 4

- E -

- Examples of ADS Path values for the available providers 6
 - ADS Path Samples 6
 - Other ADSI Connection Options 8
 - User Name Mask Samples 7
- External Authentication 3

- I -

- Internal Authentication 3
 - Benefits of Internal Authentication 3
 - Disadvantages of Internal Authentication 3
- Introduction 2

- L -

- LDAP Provider 5

- N -

- NetWare Directory Services Provider (NDS) 5
- Novell 3.x Provider (NWCOMPAT) 5

- O -

- Other ADSI Connection Options 8

- S -

- Specifying the ADS Path and other ADSI options 6
 - Authenticating Against an LDAP Server 9, 10, 12, 13
 - Examples of ADS Path values for the available providers 6, 7, 8
- Supported Types of User Authentication 3
 - ADSI Authentication 4, 5, 6, 7, 8, 9, 10, 12, 13, 14
 - Custom Authentication Modules 14, 15
 - Domain Authentication 4
 - External Authentication 3
 - Internal Authentication 3

- T -

Testing Authentication Settings	15
Testing Settings from the list view of the "User Authentication Setup" interface	16
Two ways of Testing	15
Testing Settings from the list view of the "User Authentication Setup" interface	16
Two ways of Testing Authentication Settings	15

- U -

User Authentication Set Up	1
Disclaimer	16
Introduction	2
Supported Types of User Authentication	3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15
Testing Authentication Settings	15, 16
User Name Mask for LDAP	10
Example 1	10
Example 2	12
User Name Mask Samples	7