



State of Michigan
Department of Information Technology
TECHNICAL POLICY MANUAL

SUBJECT

Active Directory Password Standard

Type	NUMBER	DATE ISSUED	REVISION DATE	REVISION NUMBER	
Standard	1310.03	11-04-05			

Purpose

The purpose of this standard is to provide the necessary password requirements for all users who access the SOM Network

Scope

This standard applies to maintaining documentation of the Global Password and Account Policy used in the SOM Active Directory implementation.

Standard Statement

The State of Michigan's Active Directory Policy will be as follows:

Password Policy

- Maximum password age = 120 days
- Enforce password history = 10 passwords
- Minimum password age = 1 days
- Minimum password length = 8 characters
- Passwords must meet complexity requirements = Enabled

- Is not based on the user's account name
- Contains at least eight characters
- Contains characters from three of the following four categories:
 - Uppercase alphabet characters (A-Z)
 - Lowercase alphabet characters (a-z)
 - Arabic numerals (0-9)
 - Non alphanumeric characters (for example, !\$,#,%)

Account Policy

- Account lockout threshold = 5 invalid attempts
- Account lockout duration = 30 minutes
- Reset account lockout counter after = 30 minutes



State of Michigan
Department of Information Technology
TECHNICAL POLICY MANUAL

SUBJECT

Active Directory Password Standard

Type	NUMBER	DATE ISSUED	REVISION DATE	REVISION NUMBER
Standard	1310.03	11-04-05		

Revision History

Revision Level	Effective Date	Description of Enhancements
	11-04-05	Initial Release

Terms and Definitions

Account lockout threshold	Determines the number of failed logon attempts that will cause a user account to be locked out. A locked out account cannot be used until an administrator resets it or the account lockout duration has expired. You can set values between 1 and 999 failed logon attempts, or you can specify that the account will never be locked out by setting the value to 0.
Account lockout duration	Determines the number of minutes a locked out account remains locked out before automatically becoming unlocked. The range is 1 to 99999 minutes. You can specify that the account will be locked out until an administrator explicitly unlocks it by setting the value to 0.
Enforce password history	This setting determines the number of unique new passwords that have to be associated with a user account before an old password can be reused. It also rejects new passwords that are too similar to previous passwords. This feature prevents users from circumventing password lifetime restrictions by reusing their old password.
Maximum password age	This setting determines the period of time (in days) that a password can be used before the system requires the user to change it. The best defense against impersonation is to require that users change their passwords regularly. This reduces the amount of time available for attackers to crack unknown passwords, and it periodically invalidates any password that has been stolen by other means.
Minimum password age	This setting determines the number of days that must pass before a user can change his or her password. Defining a minimum password age prevents users from circumventing the password history policy by defining multiple passwords in rapid succession until they can use their old password again. The default value is 0, but it is recommended that this be reset. A value of a few days discourages



State of Michigan
Department of Information Technology
TECHNICAL POLICY MANUAL

SUBJECT

Active Directory Password Standard

Type	NUMBER	DATE ISSUED	REVISION DATE	REVISION NUMBER
Standard	1310.03	11-04-05		

	rapid password recycling while still permitting users to change their own passwords if desired. Note that setting this parameter to a value higher than the maximum password age forces users to call the IT department to change their passwords, which increases costs to the organization.
Minimum password length	The setting determines the minimum number of characters that a user's password must contain. It is recommended that you change this setting from the default value of 0. A minimum password length of seven characters is considered standard.
Passwords must meet complexity requirements	This setting enables Windows Server 2003 to verify that new passwords meet complexity requirements. The default password filter (Passfilt.dll) included with Windows Server 2003 requires that a password meet the complexity requirements.
Reset account lockout counter after	Determines the number of minutes that must elapse after a failed logon attempt before the bad logon attempt counter is reset to 0 bad logons. The range is 1 to 99999 minutes.

Related Documents

Windows 2000 Group Policy Reference @ www.microsoft.com
 State Of Michigan Active Directory Design

Forms