[Title]

[Subject]

Revision history

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Status | By | Changes |
| 1.0 | 22-04-2015 | Draft | Angkana T. | Initial version. |
| 2.0 | 27-04-2015 | Draft | Angkana T. | Update information by specific details. |
| 3.0 | 19-05-2015 | Draft | Thitivat P. | Update password history configuration. |

Distribution

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Status | To |
| 1.0 | 08-05-2014 | Draft | Team |

References

|  |  |
| --- | --- |
| Document number | Document title |
| PS-NW-TD-XXXX |  |

**Table of Contents**

[1 Preface 1](#_Toc419822564)

[1.1 Who should read this document 1](#_Toc419822565)

[2 Glossary 1](#_Toc419822566)

[3 Overview 1](#_Toc419822567)

[4 Password Policies 1](#_Toc419822568)

[4.1 Minimum Password Age 2](#_Toc419822569)

[4.2 Maximum Password Age 2](#_Toc419822570)

[4.3 Minimum Password Length 3](#_Toc419822571)

[4.4 Passwords Must Meet Complexity Requirements 3](#_Toc419822572)

[4.5 Store Password Using Reversible Encryption for All Users 3](#_Toc419822573)

[4.6 Enforce Password History 3](#_Toc419822574)

[5 Password Policies XML Structure 4](#_Toc419822575)

[6 Appendices 5](#_Toc419822576)

# Preface

A password policy is a set of rules designed to enhance computer security by encourage user to employ strong password and use them properly. A password policy is often part of an organization's official regulations and may be taught as part of security awareness training. The password policy may either be advisory or mandated by technical means. Some governments have national authentication frameworks that define requirements for user authentication to government services, including requirements for passwords.

## Who should read this document

This document has the information to support the developer and technician regarding about the application that need to working with Password adding and Password updating. This Document to understand about password policy that force the user to follow up.

# Glossary

**Policy** A policy is a deliberate system of principles to guide decisions and achieve rational outcomes. A policy is a statement of intent, and is implemented as a procedure or protocol. Policies are generally adopted by the Board of or senior governance body within an organization whereas procedures or protocols would be developed and adopted by senior executive officers. Policies can assist in both subjective and objective decision making.

# Overview

A password policy can be defined with a set of constrains which must be met before a user password change will be accepted. There are some experts that argue that password policies in many organizations are too stringent and actually decrease the organization's computer security. When user are required to change passwords often, meet minimum complexity requirements, and not repeat a password for a minimum amount of time, they may begin to break the rules and start writing passwords down simply because they cannot remember passwords that change so often. The reason for changing passwords is due to the fact that if an attacker gets a hashed or encrypted copy of a password, they can eventually break the password using a brute force attack.

# Password Policies

Those setting password requirements must remember that making the password rules too difficult may actually decrease security if users decide the rules are impossible or too difficult to meet. If passwords are changed too often, users may tend to write them down or make their password a variant of an old password which an attacker with the old password could guess. The following password requirements will be set by the IT security department:

| Password Policies |  |
| --- | --- |
| Minimum password age | 2 Days |
| Maximum password age | 60 Days |
| Minimum length | 8 Characters recommended |
| Password complexity | • Passwords must have at least eight characters.  • Passwords can’t contain the user name or parts of the user’s full name, such as his first name.  • Passwords must use at least three of the four available character types:   * Lowercase letters (a-z English characters only) * Uppercase letters (A-Z English characters only) * Numbers (0-9 only) * Symbols (~!@#$%^&\*\_-+=`|\(){}[]:;"'<>,.?/ only) |
| Password history | Require a number of unique passwords before an old password may be reused. This number should be no less than 24. |
| Store passwords using reversible encryption | This should not be done without special authorization by the IT department since it would reduce the security of the user's password. |

## Minimum Password Age

This determines how long users must keep a password before they can change it. You can use this field to prevent users from bypassing the password system by entering a new password and then changing it right back to the old one. If the minimum password age is set to 0, users can change their passwords immediately. To prevent this, set a specific minimum age. Reasonable settings are from three to seven days. In this way you make sure that users are less inclined to switch back to an old password but are able to change their passwords in a reasonable amount of time if they want to.

**Note:** Keep in mind that a minimum password age could prevent a user from changing a compromised password. If a user can’t change the password, an administrator has to make the change.

## Maximum Password Age

This determines how long users can keep a password before they have to change it. The aim is to force users to change their passwords periodically. Generally, you use a shorter period when security is very important and a longer period when security is less important. You can set the maximum password age to any value from 0 to 999, where a value of 0 specifies that passwords don’t expire. Although you might be tempted to set no expiration date, users should change passwords regularly to ensure the network’s security. Where security is a concern, good values are 30, 60, or 90 days. Where security is less important, good values are 120, 150, or 180 days.

**Note:** Windows Server 2008 R2 notifies users when the password expiration date is approaching. Any time the expiration date is less than 30 days away, users see a warning when they log on that they have to change their password within a specific number of days.

## Minimum Password Length

This sets the minimum number of characters for a password. If you haven’t changed the default setting, you should do so immediately. The default in some cases is to allow empty passwords (passwords with zero characters), which is definitely not a good idea. For security reasons you’ll generally want passwords of at least eight characters because long passwords are usually harder to crack than short ones. If you want greater security, set the minimum password length to 14 characters.

## Passwords Must Meet Complexity Requirements

Beyond the basic password and account policies, Windows Server 2008 R2 includes facilities for creating additional password controls. These facilities enforce the use of secure passwords that follow these guidelines:

* Passwords must have at least six characters.
* Passwords can’t contain the user name or parts of the user’s full name, such as his first name.
* Passwords must use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and symbols.

To enforce these rules, enable the Passwords Must Meet Complexity Requirements policy.

## Store Password Using Reversible Encryption for All Users

Passwords in the password database are encrypted. This encryption can’t normally be reversed. The only time you would want to change this setting is when your organization uses applications that need to read the password. If this is the case, enable Store Password Using Reversible Encryption for All Users. But with this policy enabled, passwords might as well be stored as plain text—it presents the same security risks. With this in mind, a much better technique is to enable the option on a per-user basis and then only as required to meet the user’s actual needs.

## Enforce Password History

This sets how frequently old passwords can be reused. With this policy, you can discourage users from alternating between several common passwords. Windows Server 2008 R2 can store up to 24 passwords for each user in the password history. To disable this feature, set the value of the password history to 0. To enable this feature, set the value of the password history using the Passwords Remembered field. Windows Server 2008 R2 then tracks old passwords using a password history that’s unique for each user, and users aren’t allowed to reuse any of the stored passwords.

**Note:** To prevent users from working around the Enforce Password History settings, you should prevent users from changing passwords immediately. This stops users from changing their passwords several times to wipe the history and get back to the old password. You can set the time required to keep a password

# Password Policies XML Structure

This section provides XML Structure for password policies. You can set value following password policies table above to this xml file. Then let the password policies function to read and check following xml structure specified.

<configuration name="PasswordPolicy">

<settings>

<setting key="MinimumLength" value="8" />

<setting key="MinimumUpperCase" value="1" />

<setting key="MinimumLowerCase" value="1" />

<setting key="MinimumDigits" value="1" />

<setting key="AllowCharacter"

value="abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789" />

<setting key="SpecialCharacter" value="`~!@#$%^&amp;\*()\_+-={}|[]:;'\&quot;&lt;&gt;,.?]" />

<setting key="MinimumSpecialCharacters" value="1" />

<setting key="MinimumAge" value="2" />

<setting key="MaxPasswordHistory" value="24" />

</settings>

</configuration>

# Appendices

<https://technet.microsoft.com/en-us/magazine/ff741764.aspx>

<http://www.comptechdoc.org/independent/security/policies/password-policy.html>