Password Creation and Authentication Guide

# Password Creation and Authentication Guide

## Introduction

This guide sets out considerations for creating passwords and authenticating users for access to Ministry of Justice (MoJ) systems. This includes ensuring that there are appropriate authentication methods for information, accounts and systems. For more information, see the [Password Management Guide](password-management-guide.html).

This guide has been written to align with [NCSC guidance](https://www.ncsc.gov.uk/collection/passwords/updating-your-approach).

## Default passwords

All default passwords must be changed before using any system. Default passwords should not be 'guessable'. This applies to all new, modified or replaced systems, applications and end-user devices or endpoints.

## Password length and complexity

Best practice for creating a strong password is to create a passphrase consisting of a string of words that is easy to remember. If using this approach, have a minimum of three words in the passphrase. Passwords must be complex and difficult to guess. When selecting a password, ensure that:

* It has a minimum of 8 characters for personal accounts.
* It has a minimum of 15 characters for high value accounts, for example administrator accounts, password managers or service accounts.
* It does not contain usernames or personal information, such as date of birth, address, phone number or family or pet names.
* It is used alongside system monitoring tools such as last login attempt notifications, rather than enforcing regular password expiry.
* You have alternative or additional authentication options, such as Single-Sign On (SSO) and Multi-Factor Authentication (MFA), depending on a system's security classification or where otherwise required.

Stronger passwords typically at least one instance of each of the following character types: upper case, lower case, numbers, and special characters. Special characters include: @, &, $, % or ^. However, there is no specific obligation to incude special characters for a password to be acceptable.

For more details about passwords for service accounts, see the [Passwords](passwords.html) guidance.

## Password history and block listing

The MoJ requires a password allow list to help users create strong passwords. This is a list of commonly used passwords, which can be easily guessed or brute forced by threat actors, and so must not be used. To understand trends in bad passwords and set up password allow listing, refer to 'SecLists', found on [GitHub](https://github.com/danielmiessler/SecLists/tree/master/Passwords).

The MoJ requires password history management, to prevent an old password being reused. This prevents threat actors using previously compromised passwords in an attack, and helps to enforce MoJ strong password requirements.

## Multi-factor authentication

MFA provides an additional layer of security for login and access controls. Two-Factor Authentication (2FA), Time-based One-Time Password Algorithm (TOTP), and hardware and software tokens and biometric authentication are all forms of MFA that might be used within MoJ systems. The [Access Control Guide](access-control-guide.html) provides further information.

If a service supports MFA, it must be enabled and used by default. An MFA prompt must appear when attempting to access an OFFICIAL system, where:

* The system relies upon 'cloud' applications, cloud-based APIs, or other internet-connected services.
* A new device is used to log on to the service.
* A password change is in progress for a privileged account.

Further guidance around the use of Multi-Factor Authentication can be found in the [Authentication](authentication.html) guide.

## Single-Sign On

MoJ SSO solutions include Office 365, and Digital and Technology G-Suite. SSO solutions must be integrated within the MoJ application development and service delivery environment, to improve user experience by authenticating to systems using existing MoJ credentials. SSO must:

* Have a pre-defined identity source for users, such as Active Directory, Google Directory or LDAP. This means a developer or service provider must use an established MoJ SSO solution rather than creating a new one.
* Normally be based on applications rather than groups of people. This means that SSO is to a specific application or service, rather than saying something like 'all administrators of the Widget application have SSO-managed access'. Instead, SSO must be enabled for the 'Widget'application. It can be based on groups of people or roles if these have been defined.

## Contact details

For any further questions relating to security, contact: [security@digital.justice.gov.uk](mailto:security@digital.justice.gov.uk).