Authentication

# Authentication

## The base principle

Any access to any data **must** employ adequate authentication techniques to identify the system or user to a suitable level of confidence for the system or data within.

## Passwords

Where appropriate, passwords should be used as a knowledge-based factor for authentication.

The Ministry of Justice (MoJ) has published the [MoJ Password Standard](https://intranet.justice.gov.uk/guidance/security/it-computer-security/ict-security-policy-framework/password-standard/).

## Named individual accounts

Human user access must have unique, named and private accounts issued (with shared accounts being a rare, intentional and considered exception to this rule).

For example: Jonathan Bloggs is issued with a user account only Jonathan uses and may access.

### Account sharing

Accounts must not be shared unless they are defined as shared accounts, where additional authentication and authorisation techniques may be required.

For example:

* individuals must not share a 'root' account, but be issued named accounts with appropriate privileges instead;
* Individuals must not share a single Secure Shell (SSH) private key, but generate private and individual keypairs and their public key associated to locations where authentication is required.

## System-system accounts

Accounts designed for programmatic or system/service integation must be unique for each purpose, particularly in separation between different environments - such as pre-production and production.

System-system accounts must be protected against human intervention.

Token-based methods are preferred over static private key methods.

## Multi-Factor Authentication

Where appropriate, multi-factor authentication (MFA) should be used as a knowledge-based factor for authentication. MFA is sometimes referred to as Two-Factor Authentication (2FA).

MoJ guidance on MFA is available [here](multi-factor-authentication-mfa-guide.html).

### MFA for Administrators

Administrative accounts **must** always have MFA, unless impractical to do so. Ensure there are techniques in-place such that MFA is always enabled and active for each account.

### MFA for important or privileged actions

MFA should be re-requested from the user for important or privileged actions such as changing fundemental configurations such as registered email address or adding another administrator.

MFA can also be used as a validation step, to ensure the user understands and is confirming the action they have requested, such as an MFA re-prompt when attempting to delete data.

## IP addresses

### Trusting IP addresses

IP addresses in and of themselves do not constitute authentication but may be considered a minor authentication *indicator* when combined with other authentication and authorisation techniques.

For example, traffic originating from a perceived known IP address/range does not automatically mean it is the perceived user(s) however it could be used as an indicator to *reduce* (not eliminate) how often MFA is requested *within* an existing session.

### IP address for non-production systems

IP addresses access control lists (and/or techniques such as HTTP basic authentication) should be used to restrict access to non-production systems you do not wish general users to access.

H/T <https://medium.com/@joelgsamuel/ip-address-access-control-lists-are-not-as-great-as-you-think-they-are-4176b7d68f20>