Authorisation

# Authorisation

## 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.

## Least privilege principle

The principle of least privilege (PoLP; also known as the principle of least authority) is effectively conferring only the minimum number of required privileges required in order to perform the required tasks.

This helps reduce the "attack surface" of the computer by eliminating unnecessary privileges.

Day to day examples include: not ordinarily using an 'administrator' login on an end-user device (such as a laptop), logging into a server as 'root' or a user being able to access all records within a database when they only need to access a subset for their work.

### Administrator definition

An administrator is much broader than a technical system administrator to a server, network or service (such as 'domain admin' in Microsoft Active Directory) but someone has who has higher levels of access or control than a required for day to day operation.

Examples include those with high privileges on a Ministry of Justice (MoJ) github.com repository and credentials to the MoJ communications accounts (such as social media).

## AWS assume-role

Amazon Web Services (AWS) Identity and Access Management (IAM) has a Role function, which effectively allows explicitly permitted and explicitly denied activity (within the AWS ecosystem) to be defined on a per role-based.

This allows IAM accounts to be grouped based on role and purpose. This avoids individual IAM accounts being given permissions individually, which can often lead to over or under priviledge configurations.

Where possible, IAM Roles should be used.

## 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](multi-factor-authentication-mfa-guide.html) is requested *within* an existing session.

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