Management access

# Management access

## The base principle

Management or administrative access **must** be limited to authorised authenticated users and utilise multi-factor authentication wherever possible.

## Application Program Interface (API)

APIs are preferred over Secure Shell (SSH) connections, as by comparison they generally offer greater technical security limitations without the need for parsing commands.

## Automated diagnostic data collection

It should be exceptional to directly administer a server/node when adequate diagnositic data collection sends underlying technical data to a place where it can be correlated and analysed.

## Pre-defined, pre-audited

Tools such as [Systems Manager](https://aws.amazon.com/systems-manager/) and comparable techniques over preferred over manual intervention (such as human interaction over SSH) as the intervention path can be carefully designed to avoid human error and effectively instruct pre-audited actions to be taken on an administrator's behalf.

## Secure Shell (SSH)

Use of bastion or 'jump' boxes for access into systems is a useful technical security design that also helps 'choke' and control such sessions.

Through immutable infrastructure and server design, state-less cluster expansion/contraction and automated diagnostic data capture the need to SSH into a server/node should be increasingly less common.

It should be exceptional for an individual to login to a server/node via SSH and execute commands with elevated privledges (typically, root).

### Using SSH

SSH must be strictly controlled, and environments should be segregated so that no single bastion or 'jump' SSH server can access both production and non-production accounts.

SSH shells must be limited to users who need shell (by comparison to users who will use SSH as a port forwarding tunnel).

Joiners/Movers/Leavers processes must be strictly enforced (optimally, automated) on SSH servers as they are a critical and priviledged access method.

SSH should not be password-based, and should use individually created and purposed SSH keypairs. *Private keys must not be shared or re-used*.