Managing User Access Guide

# Managing User Access Guide

## Introduction

This guide provides information on the authentication methods which should be used to manage user access to systems and information in the Ministry of Justice (MoJ). This is a sub-page to the [Access Control Guide](access-control-guide.html).

## Managing access to MoJ systems

The following methods can be used to manage access to the MoJ's systems. They are in order of preference for their use, with 1 providing more secure management features than 3.

|  |  |  |
| --- | --- | --- |
| Rank | Method | Comment |
| 1 | Application Program Interface (API) | Where possible, APIs should be used instead of remote server configuration tools such as Secure Shell (SSH) and Remote Desktop (RDP). This is because APIs offer greater technical control over security systems without the need for parsing commands required by remote server configuration tools. |
| 2 | Automated diagnostic data collection | It should be considered the exception for administrators to directly administer a server/node when there is automated diagnostic data collection. Diagnostic data collection allows the underlying technical data to be easily correlated and analysed. |
| 3 | Remote server configuration tools | If you cannot use APIs then remote server configuration tools can be used with the following controls. |

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

The need to use remote server configuration tools to interact with a server or node can be reduced through improved infrastructure and server design. For instance, the use of stateless cluster expansion or contraction, and the automated diagnostic data capture, can reduce the need to use SSH.

System Admins should only login to a server or node via SSH to execute commands with elevated privileges (typically, root) under exceptional circumstances.

* 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.
* Do not allow direct logging in as root through SSH. Administrators must have a separate account that they regularly use and sudo to root when necessary.
* SSHs must be limited to users who need shell, in contrast to users who might use SSH as a port forwarding tunnel.
* Joiners/Movers/Leavers processes must be strictly enforced (optimally and preferably automated) on SSH servers, as they are a critical and privileged access method.
* SSH access should not be password-based. It should use individually created and purposed SSH key pairs. Private keys must not be shared or re-used.

The Government Digital Service (GDS) recommends the use of the open authorisation standard '[OAuth2](https://oauth.net/2/)' as a means to authenticate users. See the [GDS guide](https://www.gov.uk/guidance/gds-api-technical-and-data-standards) for more information.

## Contact details

Contact the Cyber Assistance Team for advice - [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk)