Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Restricting administrative privileges

First published: June 2011
Last updated: November 2023

Introduction

Restricting administrative privileges is one of the most effective mitigation strategies in ensuring the security of systems. As such, restricting administrative privileges forms part of the Essential Eight from the *Strategies to mitigate cybersecurity incidents*.

This publication provides guidance on how to effectively restrict administrative privileges.

Why administrative privileges should be restricted

Users with administrative privileges for operating systems and applications are able to make significant changes to their configuration and operation, bypass critical security settings and access sensitive data. Domain administrators have similar abilities for an entire network domain, which usually includes all of the workstations and servers on the network.

Malicious actors often use malicious code (also known as malware) to exploit vulnerabilities in workstations and servers. Restricting administrative privileges makes it more difficult for malicious actors to elevate privileges, spread to other hosts, hide their existence, persist after reboot, obtain sensitive data or resist removal efforts.

An environment where administrative privileges are restricted is more stable, predictable, and easier to administer and support, as fewer users can make significant changes to their operating environment, either intentionally or unintentionally.

Approaches which do not restrict administrative privileges

There are a number of approaches which, while they may appear to provide many of the benefits of restricting administrative privileges, do not meet the intent of this mitigation strategy, and in some cases may actually increase the risk to an organisation's network. These approaches include:

- simply minimising the total number of privileged accounts
- implementing shared non-attributable privileged accounts

- temporarily allocating administrative privileges to user accounts
- placing standard user accounts in user groups with administrative privileges.

How to restrict administrative privileges

The correct approach to restricting administrative privileges is to:

- identify tasks which require administrative privileges to be performed
- validate which staff members are required and authorised to carry out those tasks as part of their duties
- create separate attributable accounts for staff members with administrative privileges, ensuring that their accounts have the least amount of privileges needed to undertake their duties
- revalidate staff members' requirements to have a privileged account on a frequent and regular basis, or when they change duties, leave the organisation or are involved in a cybersecurity incident.

To reduce the risks of using privileged accounts, organisations should ensure that:

- technical controls prevent privileged accounts from accessing the internet, unless explicitly required for the management of cloud services, in which case they are strictly limited to only what is required to undertake their duties
- system administration is undertaken in a secure manner by implementing the guidance in the *Secure administration* publication.

Further information

The *Information security manual* is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with its Essential Eight, complements this framework.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate