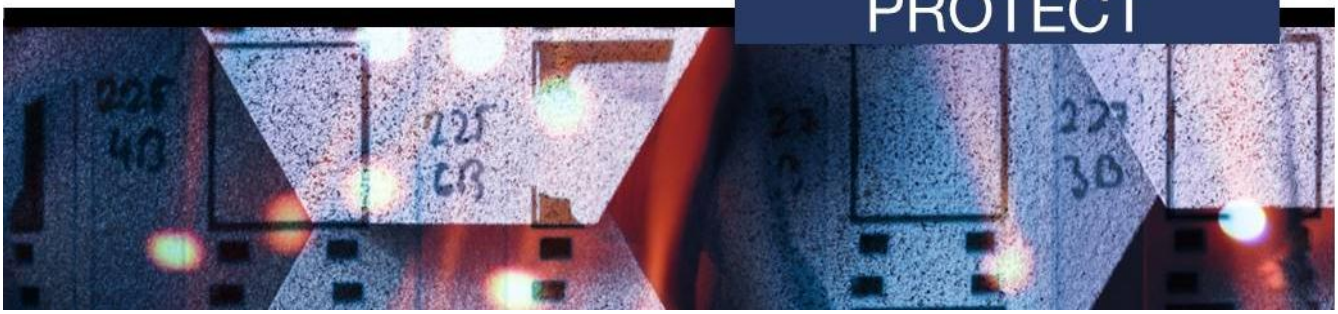

JANUARY 2018

Restricting Administrative Privileges

Introduction

1. 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 Cyber Security Incidents*.
2. This document provides guidance on how to effectively restrict administrative privileges.

Why administrative privileges should be restricted

3. 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 information. Domain administrators have similar abilities for an entire network domain, which usually includes all of the workstations and servers on the network.
4. Adversaries often use malicious code (also known as malware) to exploit security vulnerabilities in workstations and servers. Restricting administrative privileges makes it more difficult for an adversary's malicious code to elevate its privileges, spread to other hosts, hide its existence, persist after reboot, obtain sensitive information or resist removal efforts.
5. 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

6. 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:
    a. simply minimising the total number of privileged accounts
    b. implementing shared non-attributable privileged accounts
    c. temporarily allocating administrative privileges to user accounts
    d. placing standard user accounts in user groups with administrative privileges.

How to restrict administrative privileges

7. The correct approach to restricting administrative privileges is to:
   a. identify tasks which require administrative privileges to be performed
   b. validate which staff members are required and authorised to carry out those tasks as part of their duties
   c. 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
   d. 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 cyber security incident.
8. To reduce the risks of using privileged accounts, organisations should ensure that:
   a. technical controls prevent privileged accounts from undertaking risky activities such as reading emails and opening attachments or browsing the Web
   b. system administration is undertaken in a secure manner by implementing the guidance in the *Secure Administration* publication.

Further information

9. The *Australian Government Information Security Manual* (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. This publication can be found at https://www.acsc.gov.au/infosec/ism/.
10. The *Strategies to Mitigate Cyber Security Incidents* complements the advice in the ISM. The complete list of mitigation strategies and supporting publications can be found at https://www.acsc.gov.au/infosec/mitigationstrategies.htm.
11. The *Secure Administration* publication provides guidance on how to implement a secure and resilient enterprise administration environment. It can be found at https://www.acsc.gov.au/publications/protect/secure-administration.htm.

Contact details

12. Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).