SECMON1

Information Security Guideline

Restricting Administrator Privileges

THIS PAGE INTENTIONALLY LEFT BLANK

Restricting administrative privileges makes it difficult for to spread malware and malicious code inside your network. In terms of access to your valuable business data, administrative accounts are the keys to the kingdom. If malicious code is activated using an administrative account, it can elevate its privileges, spread to other hosts, avoid detection, persist after reboot, obtain sensitive information and IP, and resist removal efforts; in other words, it creates the opportunity for data breaches and attacks against your systems and customers.

The consequences of a compromise are reduced if users have low privileges instead. An environment where administrative privileges are restricted is more stable, predictable and easier to administer and support. This environment is created when by having fewer users who can make significant changes to their operating environment, either intentionally or unintentionally.

Note: Privileged users should use a separate, unprivileged account, and preferably a separate physical computer, for activities that are non-administrative or risky, such as reading emails and searching the web.

In the SECMON1 blog post 'Security Overview - Information Security Essentials', we spoke about what administration privileges are and why restricting them is an essential security measure.

In this document we are going to provide some privilege restriction steps. We are also going to provide you with some interesting and important links where you can educate yourself further on this topic and discuss other available options.

Implementation Guidance

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.

To reduce the risks of using privileged account, 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 ASD's Secure Administration publication.

To assist in restricting the use of privileged accounts, the following procedural and technical controls should be implemented:

a. Ensure that unique, identifiable accounts are linked to individual users and the account is authenticated every time privileged access is granted on a system. This will ensure accountability of all actions.
b. Restrict access for privileged accounts by issuing administrators a standard user account in addition to separate privileged and unprivileged administrator accounts for administrative purposes. Separate user and administrator accounts will provide a logical separation of administrative and user tasks while the use of privileged and unprivileged administrative accounts will provide another layer of protection for the privileged account credentials.
c. Privileged administrator accounts should not be used to run ongoing tasks on a system. In cases where services or applications require additional privileges indefinitely or over a long period of time, a specific service account with the minimum required permissions should be used instead.
d. Enforcing role-based delegation of privileges for privileged administrator accounts will reduce the exposure of an account in the event of compromise by an adversary.
e. Enforcing strong passphrase management for privileged and unprivileged administrator accounts will reduce the risk of passphrase guessing and brute-force attacks against the administrator accounts.
f. Disabling local administrator accounts will reduce risks associated with credential theft.
g. Do not allow service accounts to be members of any built-in administrator groups. This will reduce the risks associated with credential theft.

Further information

Further guidance, including applicability for non-Windows operating systems, is available at ASD Strategies to Mitigate Cyber Security Incidents.

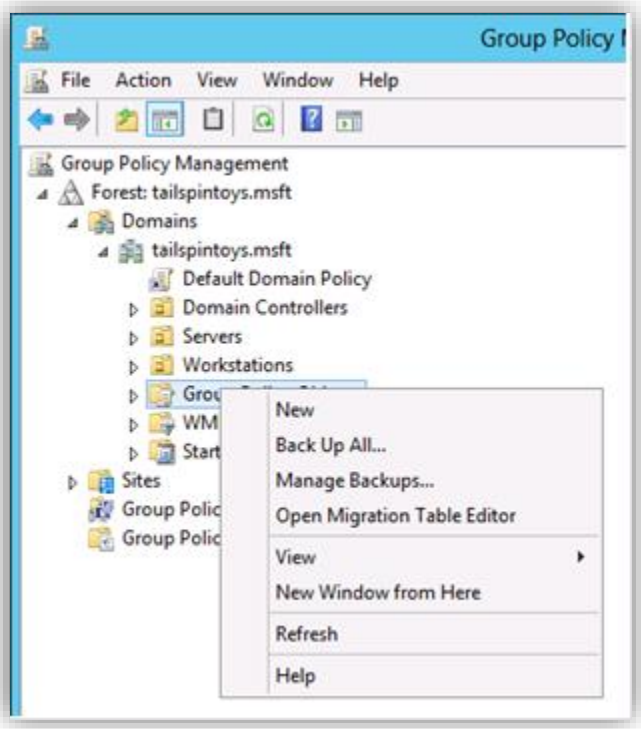
How-To Guide

This guide will be focusing on local administrator accounts. For securing administrator accounts via Active Directory, it is advisable to engage an IT professional if you do not already have one in your organisation. SECMON1 is also available to assist with this.

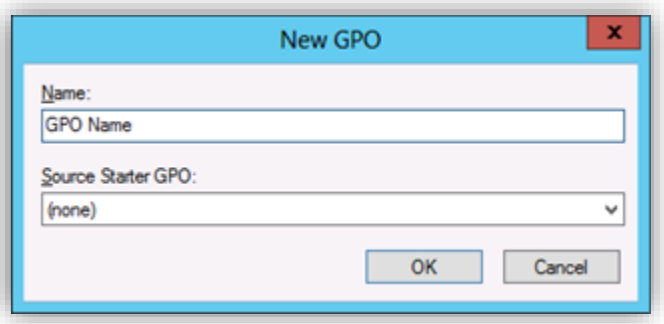
Securing Local Administrator Accounts

On all current versions of Windows (7-10), the local Administrator account is disabled by default, which makes the account unusable for credential theft attacks. However, in domains containing legacy operating systems or in which local Administrator accounts have been enabled, these accounts can be used to spread compromise across member servers and workstations. For this reason, the following controls are recommended for all local Administrator accounts on domain-joined systems

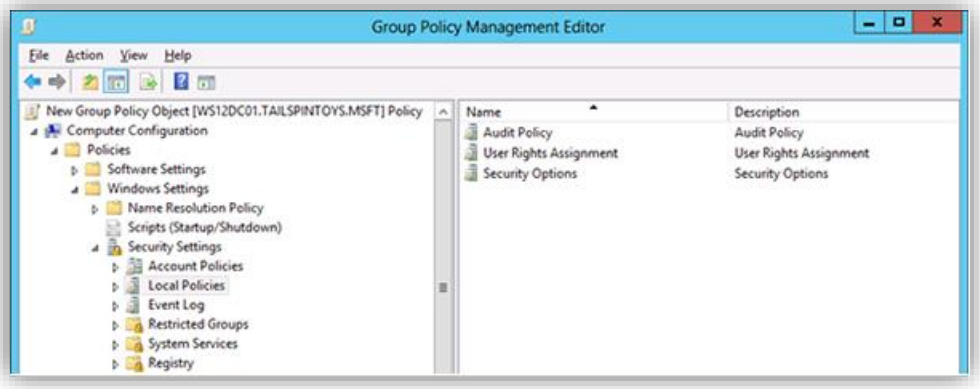
1. To open Group Policy Management Console in Windows Server 2008, either press the Windows logo key +R to open the **RUN** dialog box or click **Start**, click **All Programs**, click **Accessories**, then click **Run**. Then type **gpmc.msc** in the text box and click **OK** or press **ENTER**.
   To open Group Policy Management Console in Windows Server 2012, on the **Start** screen, click the **Apps** arrow. On the **Apps** screen, type **gpmc.msc** and then click **OK** or press **ENTER**.
2. In the console tree, expand \Domains\, and then **Group Policy Objects**
3. In the console tree, right-click (click the mouse button on the right) **Group Policy Objects**, and click **New**.



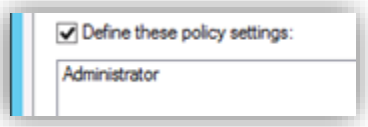
4. In the **New GPO** dialog box, type the name of the new object, and click **OK**.



5. In the details pane, right-click the new object, and click **Edit**
6. Navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies** and click **User Rights Assignment**.

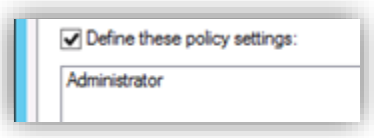


7. Configure the user rights to prevent the local Administrator account from accessing members servers and workstations over the network by doing the following:
    a. Double-click **Deny access to this computer from the network** and select **Define these policy settings**.
    b. Click **Add User or Group**, type the user name of the local Administrator account, and click **OK**. This user name will be **Administrator**, the default when Windows is installed.

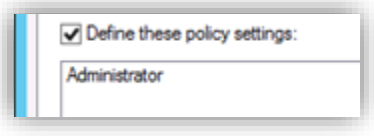


    c. Click **OK**.

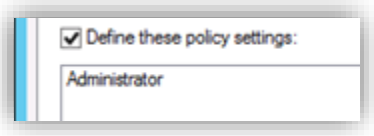
8. Configure the user rights to prevent the local Administrator account from logging on as a batch job by doing the following:
    a. Double-click **Deny log on as batch job** and select **Define these policy settings**.
    b. Click **Add User or Group**, type the user name of the local Administrator account, and click **OK**. This user name will be **Administrator**, the default when Windows is installed.



    c. Click **OK**.
9. Configure the user rights to prevent the local Administrator account from logging on as a service by doing the following:
    a. Double-click **Deny log on as a service** and select **Define these policy settings**.
    b. Click **Add User or Group**, type the user name of the local Administrator account, and click **OK**. This user name will be **Administrator**, the default when Windows is installed.

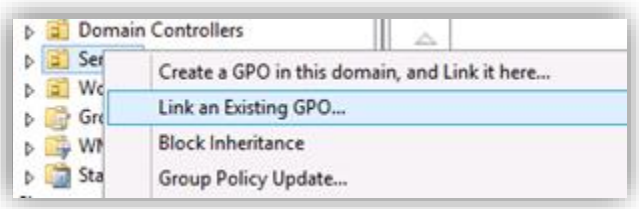


    c. Click **OK**.
10. Configure the user rights to prevent the local Administrator account from accessing member servers and workstations via Remote Desktop Services by doing the following:
    a. Double-click **Deny log on through Remote Desktop Services** and select **Define these policy settings**.
    b. Click **Add User or Group**, type the user name of the local Administrator account, and click **OK**. This user name will be **Administrator**, the default when Windows is installed.

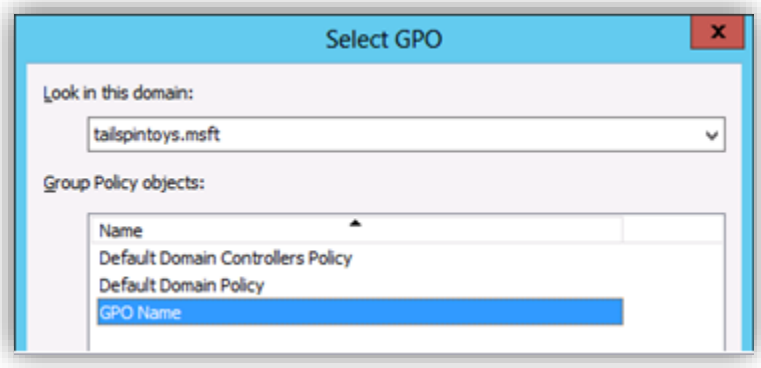


c. Click **OK**.

11. To exit the **Group Policy Management Editor**, click **File**, and click **Exit**.
12. In **Group Policy Management**, link the GPO to the member server or workstation units by doing the following:
    a. Navigate to the **\Domains**
    b. Right-click the unit that the GPO will be applied to and click **Link an existing GPO**



    c. Select the GPO that you created and click **OK**.



    d. Create links to all other units that contain workstations.
    e. Create links to all other units that contain member servers.

Further information as well as information around securing administrator accounts via Active Directory can be found here.

If you are using another product for account management, please review the product's supporting documentation.

Final Note

SECMON1 are available to review your administration privilege strategies with you and advise on troubleshooting as well as potential improvements and solutions. We are also available to implement administration privilege restriction for your company.

Please feel free to visit our website at www.secmon1.com.

You can also reach us by phone at 1300 410 900 or by e-mail at contact@secmon1.com.