SECMON1

Information Security Guideline

Disabling Local Administrator Accounts

THIS PAGE INTENTIONALLY LEFT BLANK

The Administrator account (NT AUTHORITY\Administrator) exists by default on all Microsoft Windows (Windows NT-based) systems and Active Directory domains. It is typically used as a setup and disaster recovery account.

If you must use the local administrator account, only use it during setup and to join the machine to the domain. After this, it should no longer be needed. If the account is needed for recovery or to boot into safe mode, the account will be automatically re-enabled for use only in troubleshooting. Once the system is booted again normally, it is disabled.

Conversely, you could assign passphrases that are random and unique for each computer's local administrator account. This would prevent propagation using shared local administrator credentials. However, ideally this account should just be disabled.

In the SECMON1 blog post 'Security Overview - Information Security Essentials', we spoke about what the Local Administrator account is for and why it is an essential security measure to disable it.

In this document, we are going to provide some basic steps to assist in disabling this account, as well as providing you with some interesting and important links where you can educate yourself further on this topic and identify other options available to you.

Implementation Guidance

If disabling the Local Administrator account is not an option for your organisation, please see the SECMON1 Guide to Restricting Administration Privileges.

Further information

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

How-To Guide

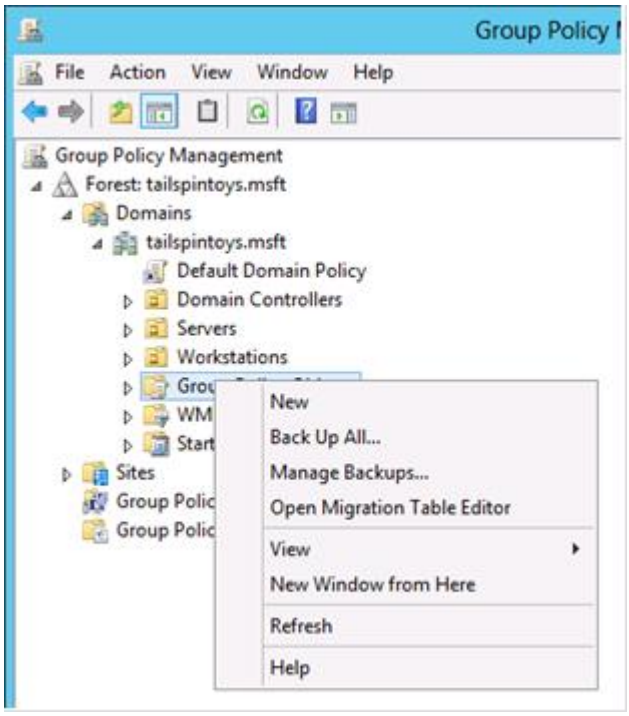
This guide will focus on securing the Local Administrator accounts. For securing administrator accounts via Active Directory, it is advisable to engage an IT professional if you do not already have one in your organisation. SECMON1 is also available to assist with this.

Securing Local Administrator Accounts

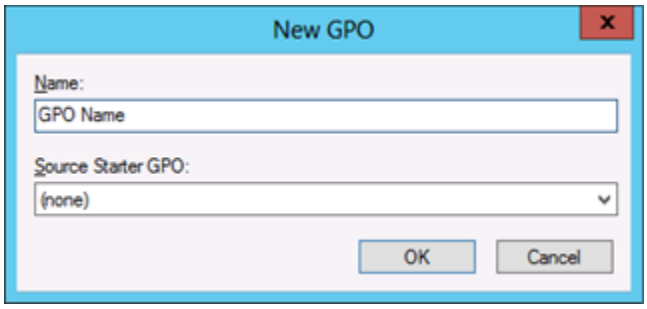
On all current versions of Windows (7-10), the Local Administrator account is **disabled by default**, which makes the account unusable for credential theft attacks. However, in domains

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.

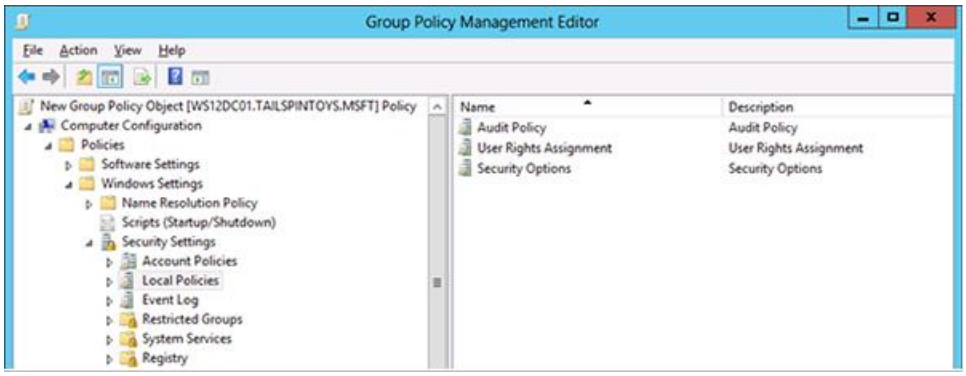
1. To open Group Policy Management Console in Windows Server 2008, either press the Windows logo key +R to open the **RUN** dialog box or click **Start**, click **All Programs**, click **Accessories**, then click **Run**. Then type **gpmc.msc** in the text box and click **OK** or press **ENTER**.
   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**.



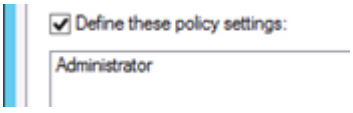
4. In the **New GPO** dialog box, type the name of the new object, and click **OK**.



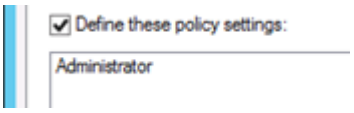
5. In the details pane, right-click the new object, and click **Edit**
6. Navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies** and click **User Rights Assignment**.



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.

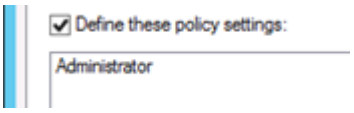


    c. Click **OK**.
8. Configure the user rights to prevent the local Administrator account from logging on as a batch job by doing the following:
    a. Double-click **Deny log on as batch job** and select **Define these policy settings**.
    b. Click **Add User or Group**, type the user name of the local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



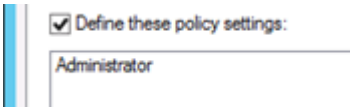
c. Click **OK**.

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**.

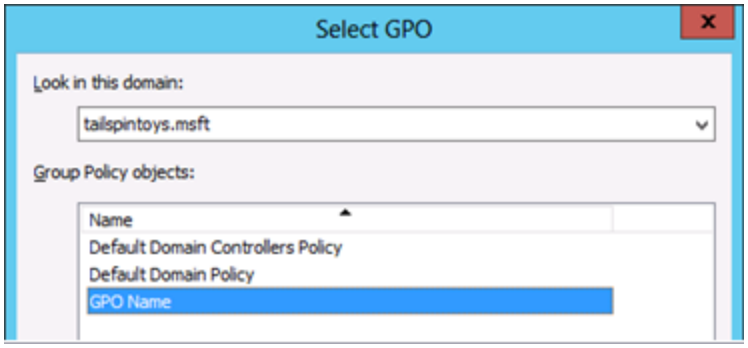
10. Configure the user rights to prevent the local Administrator account from accessing member servers and workstations via Remote Desktop Services by doing the following:
    a. Double-click **Deny log on through Remote Desktop Services** and select **Define these policy settings**.
    b. Click **Add 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 Local Administrator account settings and strategies with you and advise on troubleshooting as well as potential improvements and solutions. We are also available to implement disabling of Local Administrator accounts and/or 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