Implementing Controls in Active Directory: Protecting Against Privileged Credential Sprawl

hub.trimarcsecurity.com/post/implementing-controls-in-active-directory-protecting-against-privileged-credential-sprawl

Scott Blake

November 19, 2021

The Issue

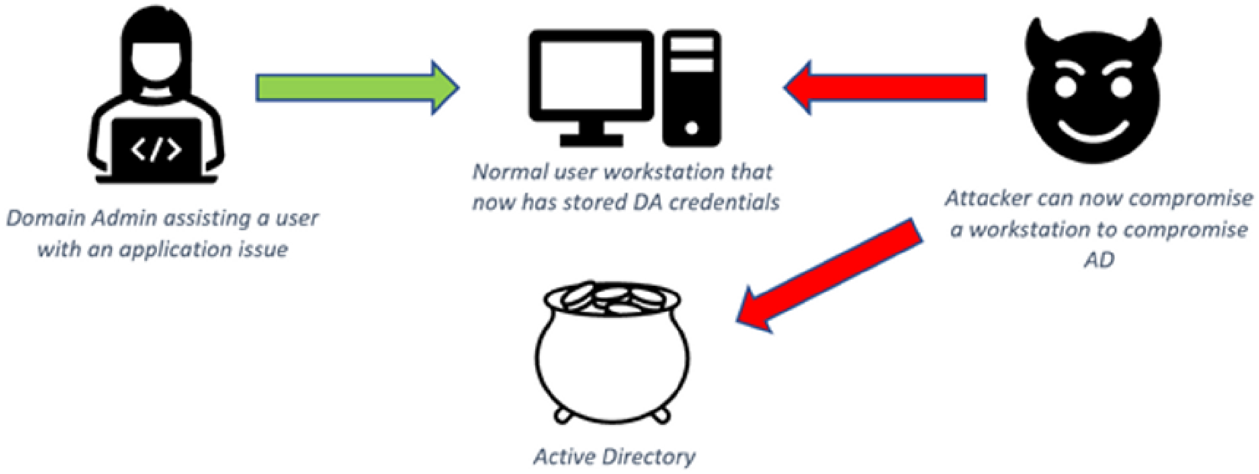
Highly privileged accounts (Domain Admins, Administrators, Enterprise Admins, etc.) are often used to perform tasks on systems that are not well protected. By default, Microsoft adds the Domain Admins group to the local Administrators group on all domain joined servers and workstations which provides this group not only administrative rights to Active Directory (AD) and Domain Controllers, but every domain-joined computer. This is the classic example of “just because you can doesn’t mean you should” (thanks mom!). While well intentioned, privileged AD accounts should ONLY be used in direct service of Active Directory related tasks and ONLY from privileged access systems.

Why It Happens

The “tyranny of the default” is something most operations and security people have dealt with and typically refers to the fact that whatever is set by default in the system rarely gets changed (and can often be a security concern). It’s tough to sit here and point fingers at the systems engineers and administrators taking the path of least resistance in an effort to keep corporate environments operational. Typically, this means using their designated AD admin accounts to manage (troubleshoot, install, configure, etc.) workstations and/or servers in the forest. Or, cringe face, throwing that pesky service account (or several of them!) in Domain Admins to get it working as intended without the hassle of setting up custom delegation. Even worse are the vendors who insist that DA rights are required for just about everything. We’ve all been there and for 99% of admins it is never the intention to introduce additional security risks.

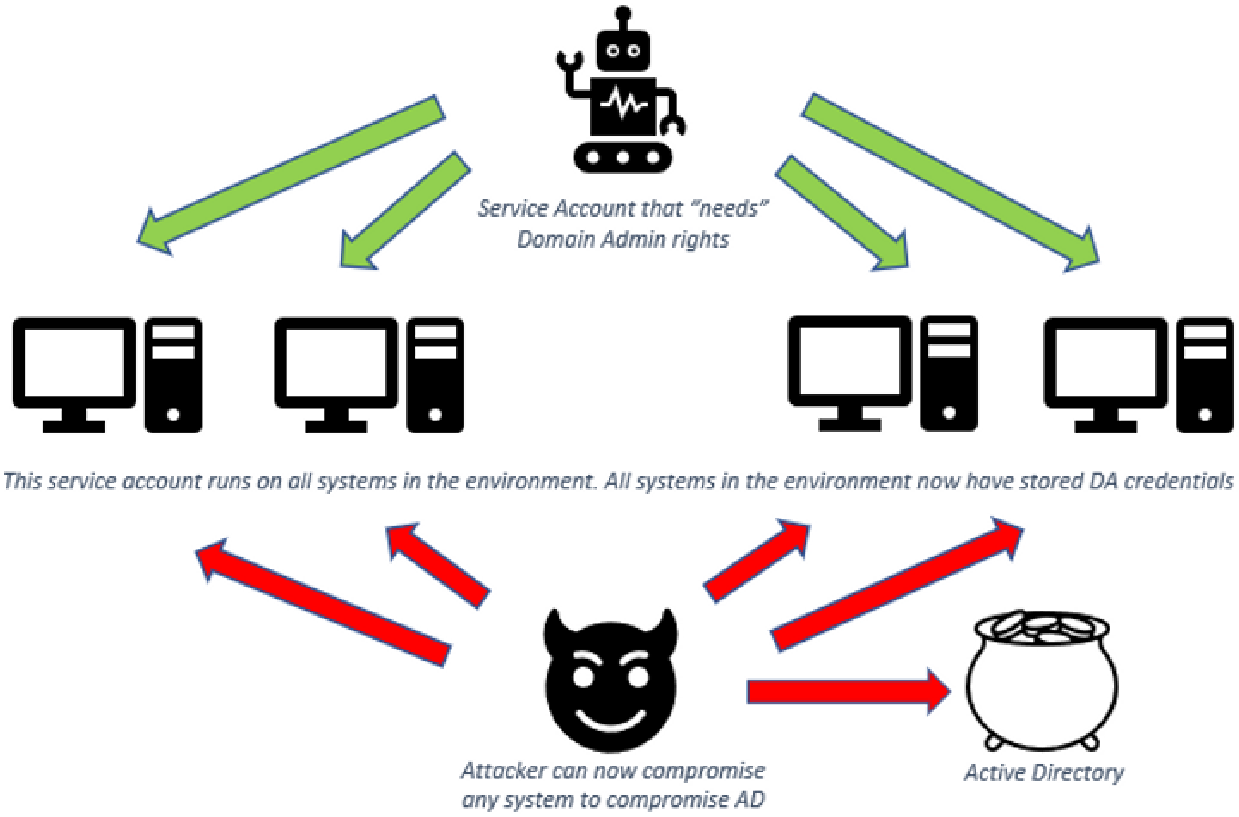
Why It Matters

It’s not a huge surprise that attackers want privileged credentials. Think of each privileged account as the “ultimate” target. Whenever one of these accounts accesses a system (through local logon, remote logon, run as, etc.) those privileged credentials now take up residence. This has the unintended consequence of creating a brand-new target in the environment.


Domain Admin assisting a user with an application issue
Normal user workstation that now has stored DA credentials
Attacker can now compromise a workstation to compromise AD
Active Directory

The figure above is a simple illustration showing how an attacker can compromise a regular workstation/server -> to compromise an AD admin account -> to compromise AD.

Extrapolate this to multiple admin accounts accessing multiple servers and workstations and we end up with lots of targets. To really lose sleep at night, think about those vulnerability scanner service accounts with Domain Admin rights touching every, single system in the domain (mind-blown emoji)!


Service Account that "needs" Domain Admin rights
This service account runs on all systems in the environment. All systems in the environment now have stored DA credentials
Attacker can now compromise any system to compromise AD
Active Directory

The figure above is a simple illustration showing how an attacker can compromise a system -> to compromise a service account -> to compromise AD

Solution

Yelling at admins, mandatory security training, or moving everything to the cloud could be potential solutions (ok, maybe not the first one) but really the best bet is to block the capability altogether. Luckily there are some relatively easy (and free!) methods that can be implemented. These are broken down into 5, easy to consume, solutions.

Limit the number of privileged accounts in the environment

This first one will be the most obvious but as we see this problem in nearly all of our Active Directory Security Assessments, it clearly needs to be mentioned again: Limit the number of privileged accounts in the environment. This goes for individual user admin accounts as well as those needy service accounts. Have a thorough understanding of the rights truly required to perform the role and delegate specific permissions whenever possible. Again, the less “ultimate” targets for an attacker the better.

Sean Metcalf has put together an excellent PowerShell script for the community that will not only provide a breakdown of membership for highly privileged groups but also help diagnose other common AD security issues - Securing Active Directory: Performing an Active Directory Security Review

With the most obvious point out of the way (again), the focus shifts to proactive measures. The following sections highlight and leverage built-in Microsoft security tools/configurations.

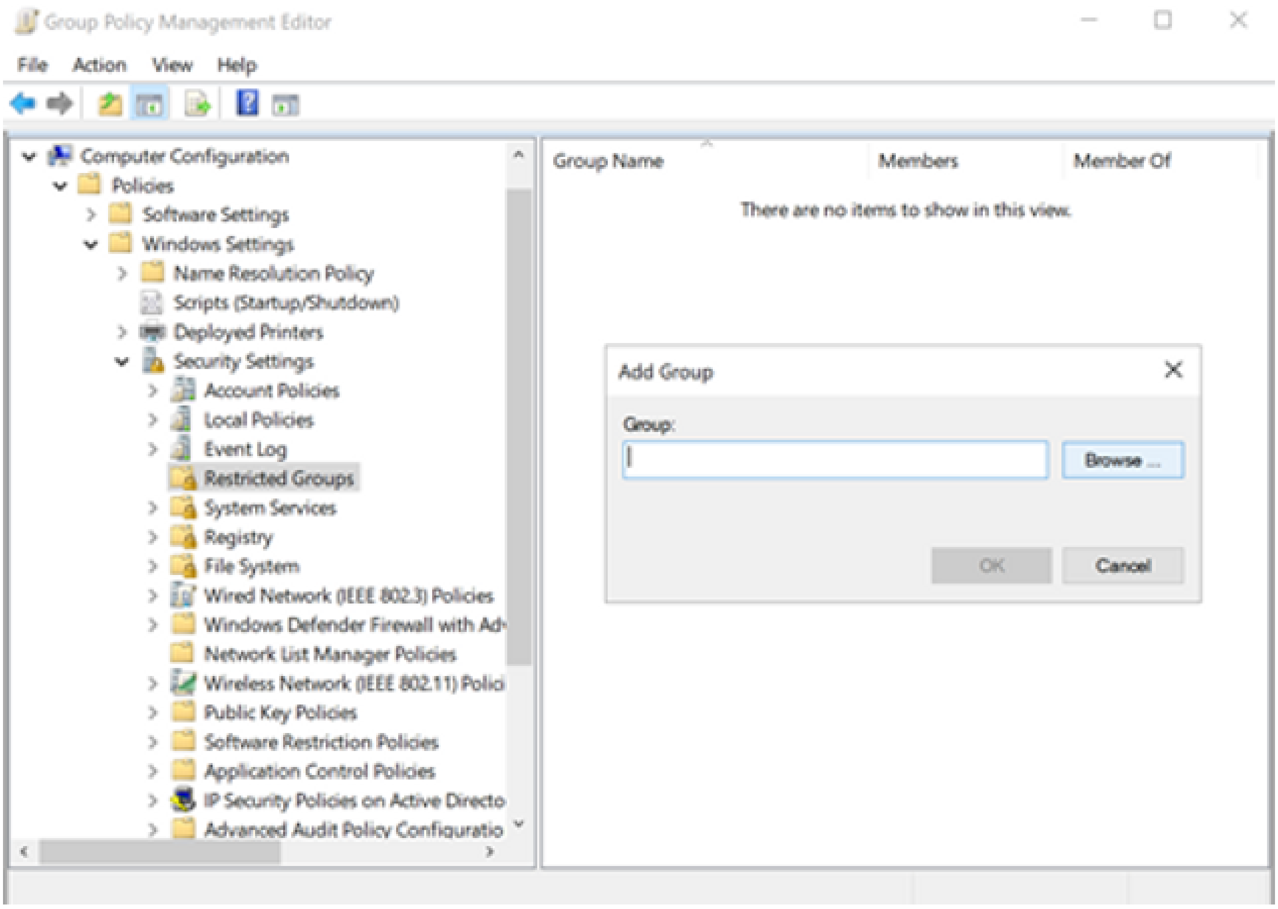
Remove domain admins from having local admin rights on all domain workstations & servers

Replace Domain Admins with the Workstation Admins (or Server Admins) group(s) so Domain Admins don’t have local admin rights on all computers.

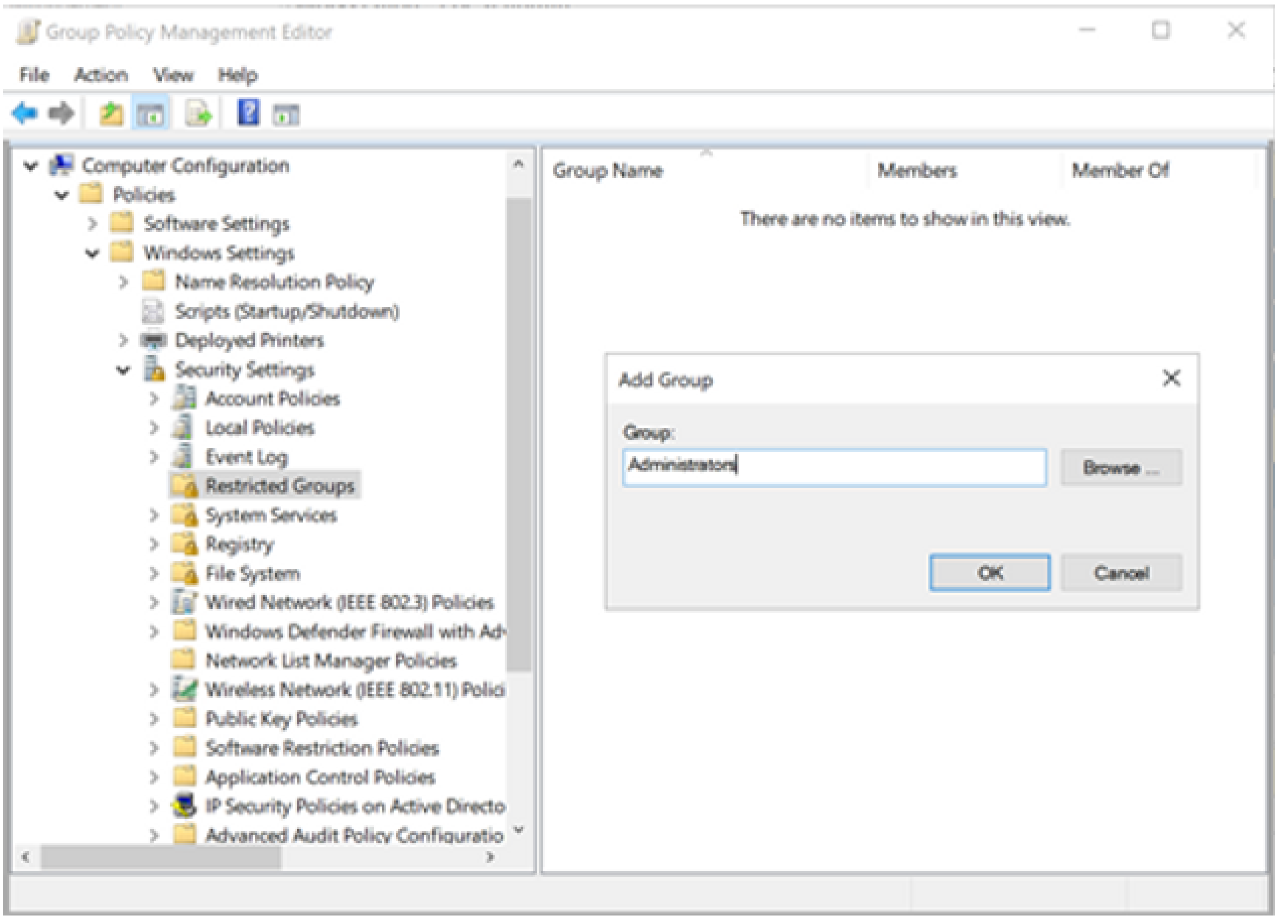
Perform the following steps on OUs containing servers/workstations in the forest (be sure to only target non-Tier 0 systems since workstation admins shouldn’t be able to control admin systems). The outcome will simultaneously remove Domain Admins from having local administrative rights on workstations/servers and assign these permissions to dedicated Workstation and Server Admin groups.

- Create a new GPO titled something like “Workstation - Local Admin Lockdown” and link it to the Workstations OU.
- Locate the “Restricted Groups” setting under *Computer Configuration\Windows Settings\Security Settings*

- Right click and select Add Group

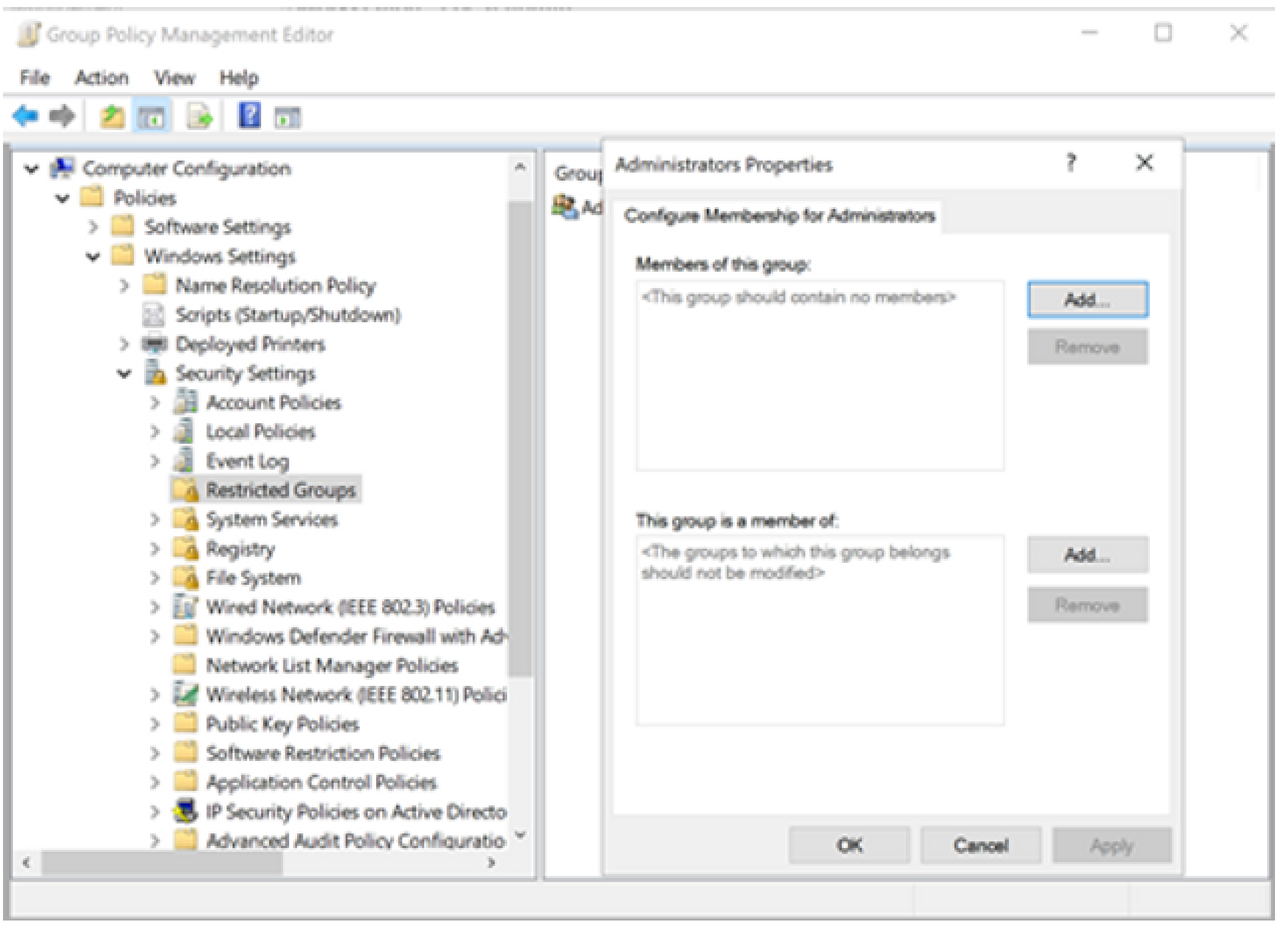

Group Policy Management Editor
File
Action
View
Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Ad
Network List Manager Policies
Wireless Network (IEEE 802.11) Polici
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directo
Advanced Audit Policy Configuratio
Group Name
Members
Member Of
There are no items to show in this view.
Add Group
Group:
Browse ...
OK
Cancel

For the “Group” input, type “Administrators” (no quotes) and select OK

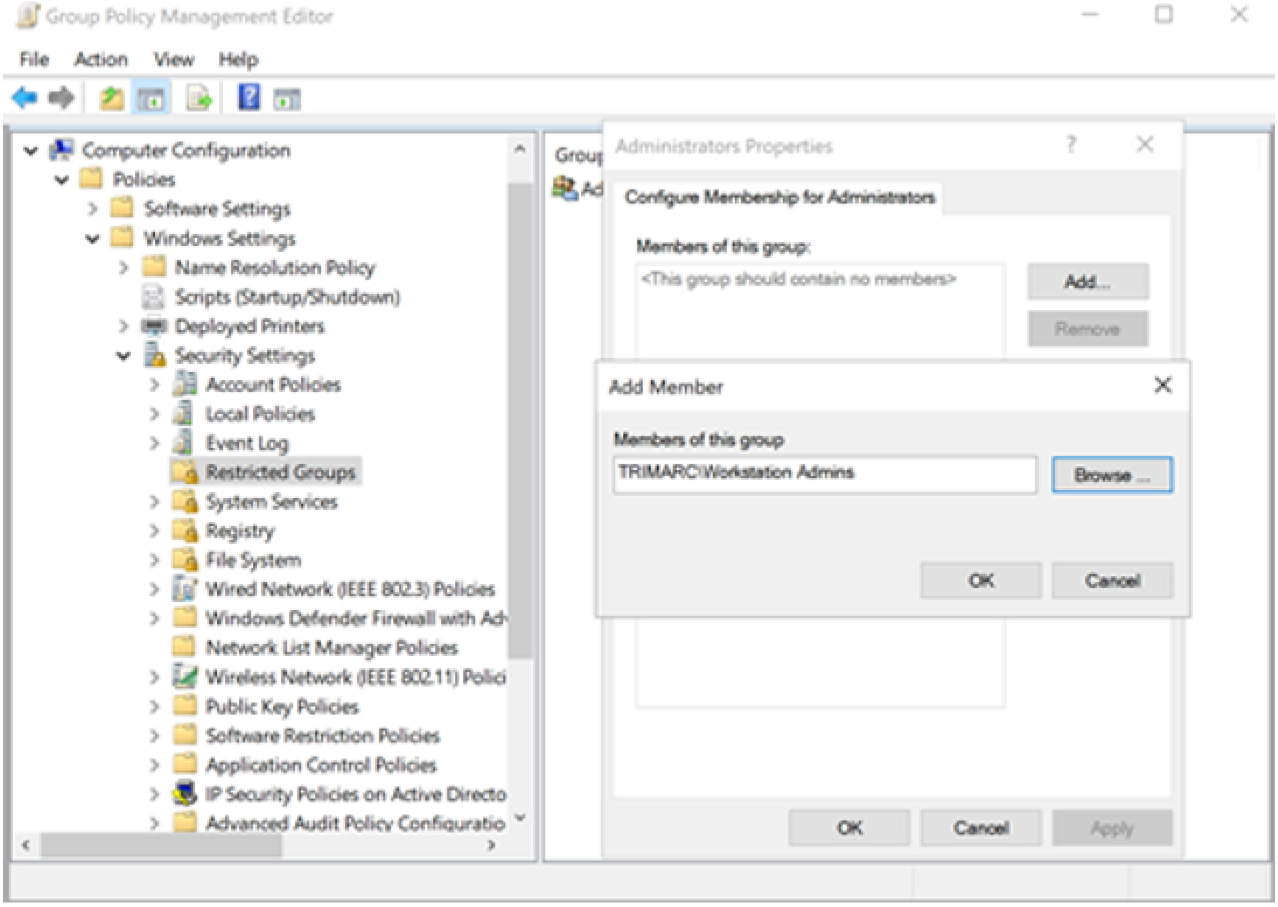

Group Policy Management Editor
File
Action
View
Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Ad
Network List Manager Policies
Wireless Network (IEEE 802.11) Polici
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directo
Advanced Audit Policy Configuratio
Group Name
Members
Member Of
There are no items to show in this view.
Add Group
Browse ...
OK
Cancel

Group: Administrators

Under Administrators Properties, click Add… for “Members of this group:


Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Ad
Network List Manager Policies
Wireless Network (IEEE 802.11) Polici
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directo
Advanced Audit Policy Configuratio
Grou
Ad
Administrators Properties
?
Configure Membership for Administrators
Members of this group:
<This group should contain no members>
Add...
Remove
This group is a member of:
<The groups to which this group belongs should not be modified>
Add...
Remove
OK
Cancel
Apply

Add the AD group being delegated local administrative rights, in this case its “TRIMARC\Workstation Admins” (naming convention is *Domain\ADGroupName*)

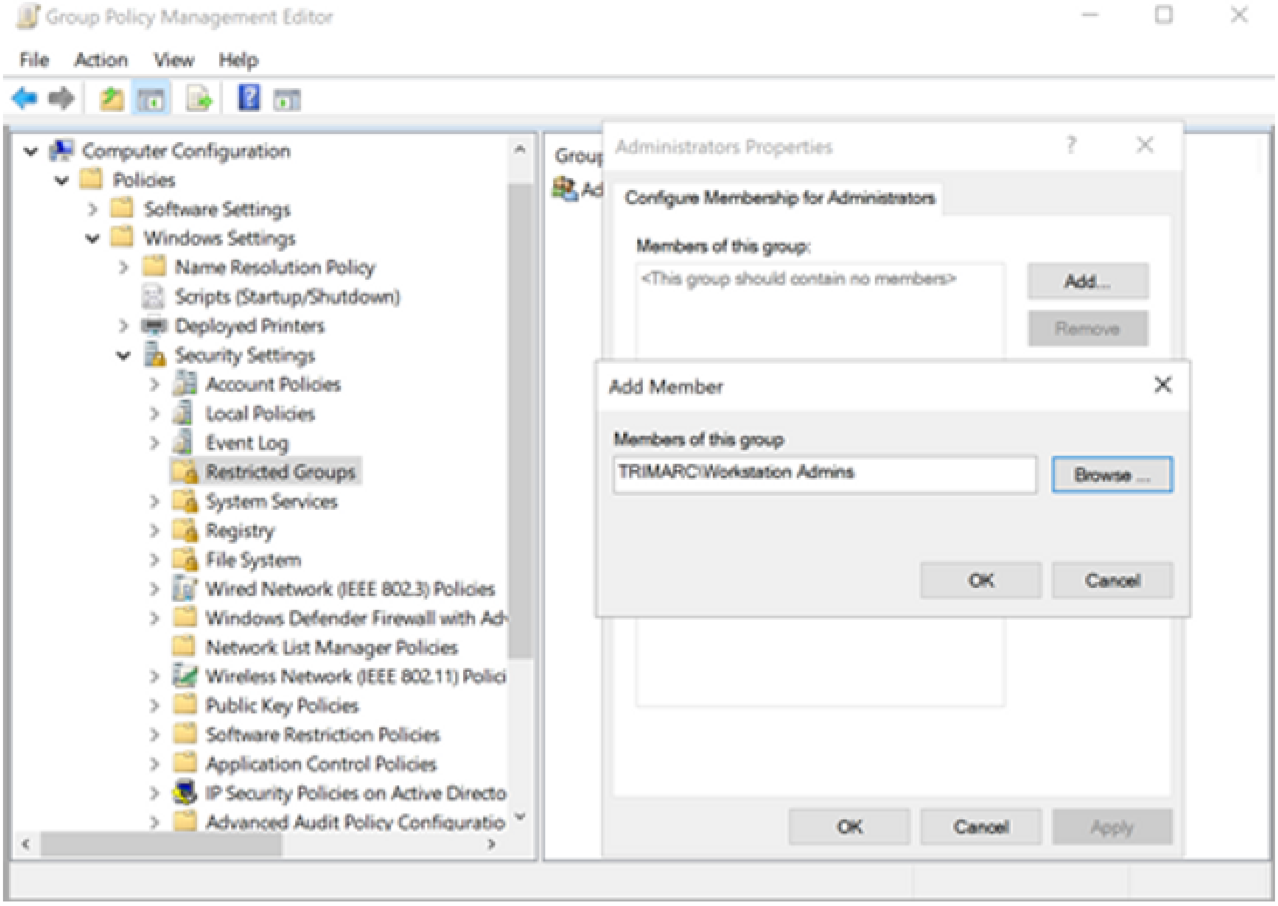

Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Adv
Network List Manager Policies
Wireless Network (IEEE 802.11) Polici
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directo
Advanced Audit Policy Configuratio
Administrators Properties
Configure Membership for Administrators
Add...
Remove
Add Member
Browse ...
OK
Cancel
Apply

Members of this group: <This group should contain no members>

Add Member

Members of this group: TRIMARC\Workstation Admins

Add the AD group being delegated local administrative rights, in this case its "TRIMARC\Workstation Admins" (naming convention is *Domain\ADGroupName*)

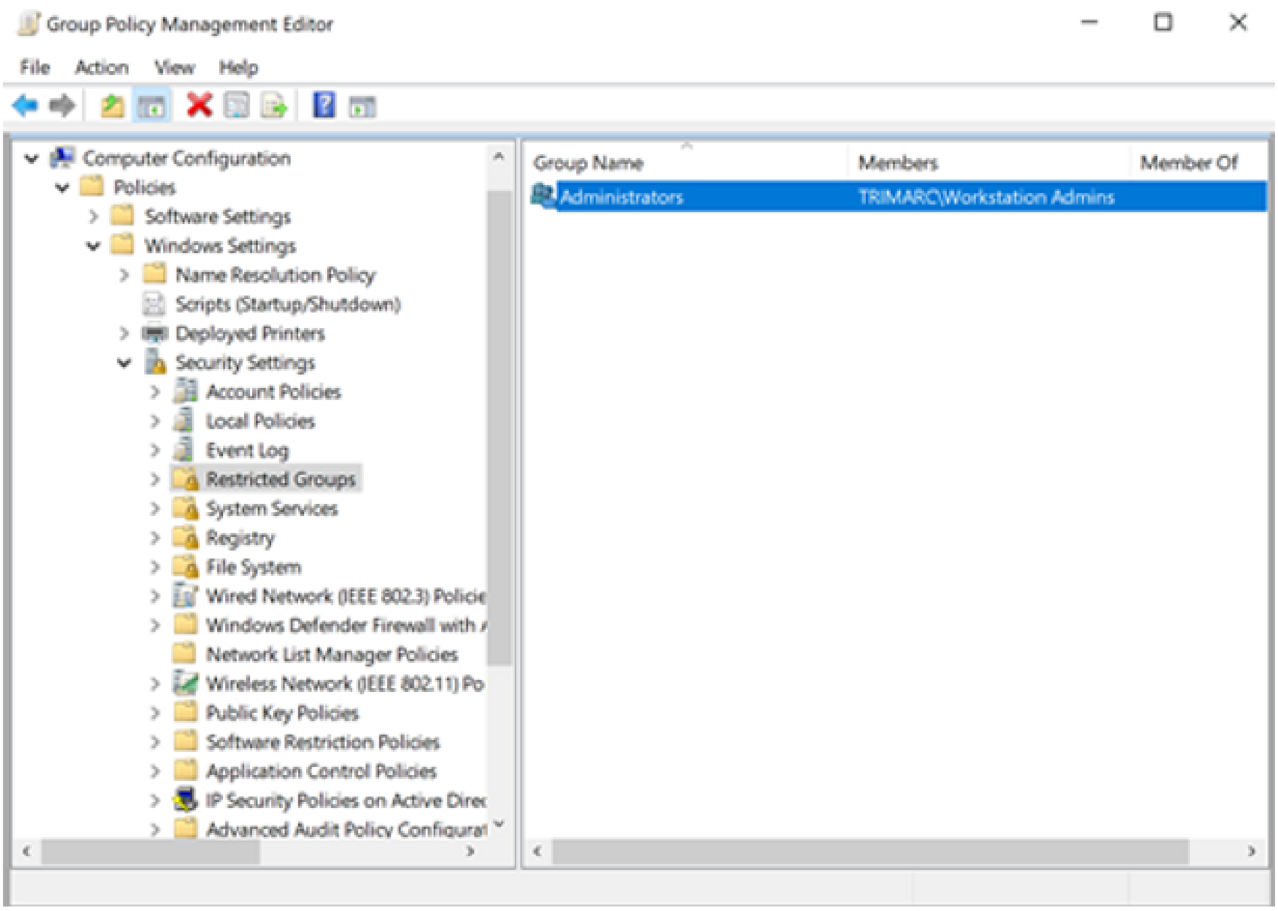

Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Adv
Network List Manager Policies
Wireless Network (IEEE 802.11) Polici
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directo
Advanced Audit Policy Configuratio
Administrators Properties
Configure Membership for Administrators
Add...
Remove
Add Member
Browse ...
OK
Cancel
Apply

Members of this group: <This group should contain no members>

Add Member

Members of this group: TRIMARC\Workstation Admins

The final product should look like the following:


Group Policy Management Editor
File
Action
View
Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policie
Windows Defender Firewall with A
Network List Manager Policies
Wireless Network (IEEE 802.11) Po
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Direc
Advanced Audit Policy Configurat

Group Name	Members	Member Of
Administrators	TRIMARC\Workstation Admins	

Repeat this process for servers (replace workstation with server).

Really important notes regarding this configuration:

- When you set Restricted Groups in the manner outlined above, it will REMOVE any accounts/groups that previously had membership (not including the local administrator account). This is not necessarily a bad thing and for the purpose of this article is convenient - Domain Admins will no longer have their default administrative rights on all servers and workstations!

- **DO NOT** modify Restricted Groups on a GPO linked to the domain root or on Domain Controllers. This can affect membership in the highly privileged Administrators AD group.

- Yes, Doman Admins can modify Group Policy Objects and therefore could easily revert these settings. The counterpoint to this is that if Domain Admins are acting nefariously in your environment, you have bigger problems. Also, setup monitoring on GPOs so events are logged when GPO changes occur and configure ad event monitoring system to receive alerts when changes occur (Audit Directory Service Changes = Success).

- Group Policy Preferences (GPP) can be used to manage group membership, but in this configuration, we are using Restricted Groups to ensure that only the groups/accounts configured in the GPO remain in the Administrators group.

Control systems Domain Admins & Enterprise Admins can access

Prevent Domain Admins and Enterprise Admins from being able to logon or connect over the network on workstations and servers (not DCs and other Tier 0 systems).

What better way to limit potential targets than blocking the capability altogether? This reads somewhat like the old IT security joke - the most secure system is one that's unplugged and encased with concrete at the bottom of the ocean. It is true in this context; control the systems highly privilged accounts are allowed to access. This can also be accomplished through some straightforward GPO settings.

Perform the following steps on OUs that house servers and workstations with the one exception being the Domain Controllers and Tier 0 OUs.

1. Create a new GPO called something like "Disable Privileged Access" and link it to your designated OUs.

2. Browse to *Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment*

3. The settings below are the ones to target and will be configured identically:

a. "Deny access to this computer from the network"

b. "Deny log on as a batch job"

c. "Deny log on as service"

d. "Deny log on locally"

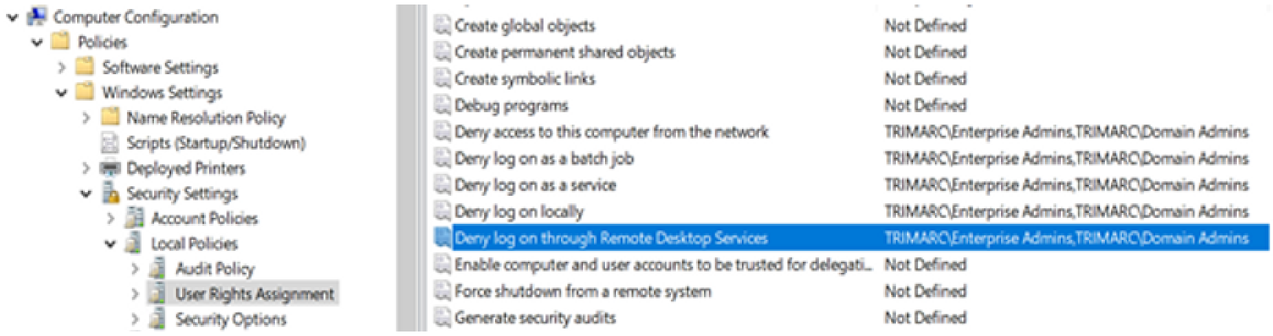
e. "Deny log on through Remote Desktop Services"

4. For each of these policy items you will add the following groups:

a. Domain Admins

b. Enterprise Admins

c. Any additional highly privileged custom AD groups that should be limited



Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options

Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Not Defined
Deny access to this computer from the network	TRIMARC\Enterprise Admins,TRIMARC\Domain Admins
Deny log on as a batch job	TRIMARC\Enterprise Admins,TRIMARC\Domain Admins
Deny log on as a service	TRIMARC\Enterprise Admins,TRIMARC\Domain Admins
Deny log on locally	TRIMARC\Enterprise Admins,TRIMARC\Domain Admins
Deny log on through Remote Desktop Services	TRIMARC\Enterprise Admins,TRIMARC\Domain Admins
Enable computer and user accounts to be trusted for delegati...	Not Defined
Force shutdown from a remote system	Not Defined
Generate security audits	Not Defined

Note that this setting will block service accounts that are members of Domain Admins & Enterprise Admins from being able to connect to these Windows systems. You will need to add service accounts that require local administrative rights to the appropriate groups ("Workstation Admins" and/or "Server Admins").

Ensure the local administrator password changes regularly

The real problem with local accounts on a computer in an enterprise environment is that the term "local" is a misnomer. If 50 computers on a network have the local administrator account of "Administrator" and a password of "P@55w0rd1!", first of all that's a HORRIBLE password. Second of all and more to the point, if one of those computers is compromised, they will all be compromised. Windows is very helpful. So helpful that if you pass the local admin credentials to another computer with the same local credentials, access is granted as if you logged on with the target system credentials. Dump administrator credentials on one to get admin on all! The best way to mitigate this issue is to ensure every computer has a different local administrator account password that is long, complex, and random and that changes on a regular basis.

Ransomware and all types of attackers love taking advantage of environments where the local Administrator password is the same on all workstations (and many times servers all have the same local admin password too!).

The solution to managing all of these local Administrator passwords is simple, just deploy the Microsoft Local Administrator Password Solution ("LAPS"). It's a free solution and works well, even in environments with over 100k workstations. We have seen organizations deploy to both workstations and servers. As the famous tag line goes, "Just Do It" and deploy LAPS.

Organizations that don’t leverage something like LAPS to automatically change local Administrator passwords to unique values discover that attackers (& ransomware) take advantage of this configuration to expand access through “lateral movement.”

This article at ADSecurity.org describes LAPS deployment: https://adsecurity.org/?p=1790

Limit local administrator control

Prevent local accounts from being able to logon or connect over the network on workstations and servers (they can still logon locally as they should). Even if you use something like Microsoft LAPS to ensure the local Administrator password changes to a unique value regularly, we still recommend implementing the steps to control local accounts since it controls all local accounts, not just the only managed by LAPS.

Perform the following steps on OUs that house servers and workstations with the one exception being the Domain Controllers and Tier 0 OUs.

In 2014, Microsoft released KB2871997 which added two new SIDS to Windows systems older than Windows 8.1/2021R2 (already built-in to newer versions):

- SID S-1-5-113 (LOCAL_ACCOUNT) – Any local account will inherit this SID
- SID S-1-5-114 (LOCAL_ACCOUNT_AND_MEMBER_OF_ADMINISTRATORS_GROUP) - Any local account that is a member of the Administrators group will inherit this SID

These can be used to build a policy preventing local accounts from connecting over the network. Oh, and if you needed further convincing this helps mitigate against ransomware attacks.

1. Create a new GPO called something like “Disable Local Account Network Access” and link it to your designated OUs.

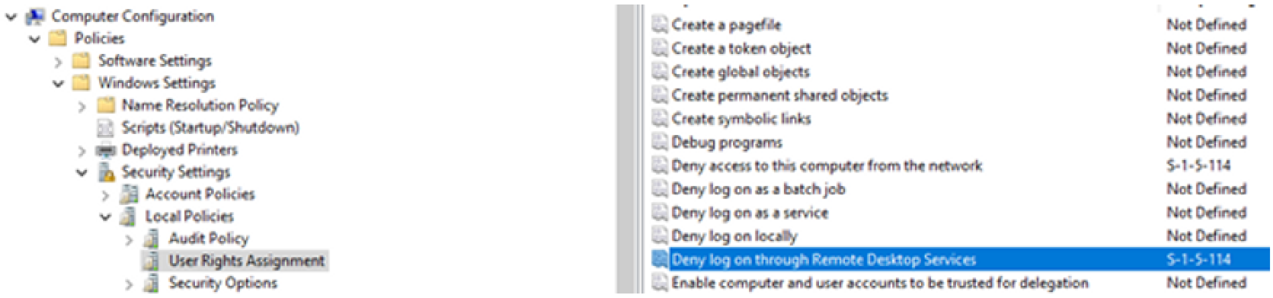
2. Browse to *Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment*

3. The settings below are the ones to target and will be configured identically:

a. “Deny access to this computer from the network”

b. “Deny log on through Remote Desktop Services”

4. Configure these with the SID “S-1-5-114” to block Local accounts that are members of the local administrators group. Alternatively, you can use SID “S-1-5-113” to block all local accounts.



Create a pagefile	Not Defined
Create a token object	Not Defined
Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Not Defined
Deny access to this computer from the network	S-1-5-114
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Remote Desktop Services	S-1-5-114
Enable computer and user accounts to be trusted for delegation	Not Defined

Conclusion

Privileged credentials can be challenging to deal with due to default Windows and Active Directory configurations as well as traditional administration methods. This article describes ways to effectively mitigate privileged credential exposure and usage.

With ransomware running rampant on corporate environments, it has never been more important to implement security practices to limit exposure. The 5 methods outlined above are simple, free, and effective ways to cut down on privileged credential sprawl which ultimately makes for a more secure environment.

References

- There’s Something About Service Accounts https://adsecurity.org/?p=4115
- Securing Active Directory: Performing an Active Directory Security Review Securing Active Directory: Performing an Active Directory Security Review (trimarcsecurity.com)
- Appendix F: Securing Domain Admins Groups in Active Directory https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-f--securing-domain-admins-groups-in-active-directory
- Description of group policy restricted groups Description of group policy restricted groups - Windows Server | Microsoft Docs

- Microsoft KB2871997 https://adsecurity.org/?p=559
- LAPS deployment https://adsecurity.org/?p=1790

By: Scott W Blake

Trimarc Security Consultant with 10+ years building, configuring, and securing enterprise environments.

Trimarc provides leading expertise in security solutions including security reviews, strategy, architecture, and implementation. Our methodology leverages our internal research and custom tooling which better discovers multiple security issues attackers could exploit to compromise the environment. Trimarc security services fit between traditional compliance/audit reviews and standard penetration testing/red teaming engagements, providing deep understanding of Microsoft and Virtualization technologies, typical security issues and misconfigurations, and provide recommendations based on our own best practices custom-tailored to balance operational and security challenges.