

Implementing Privileged Access Workstation – part 3

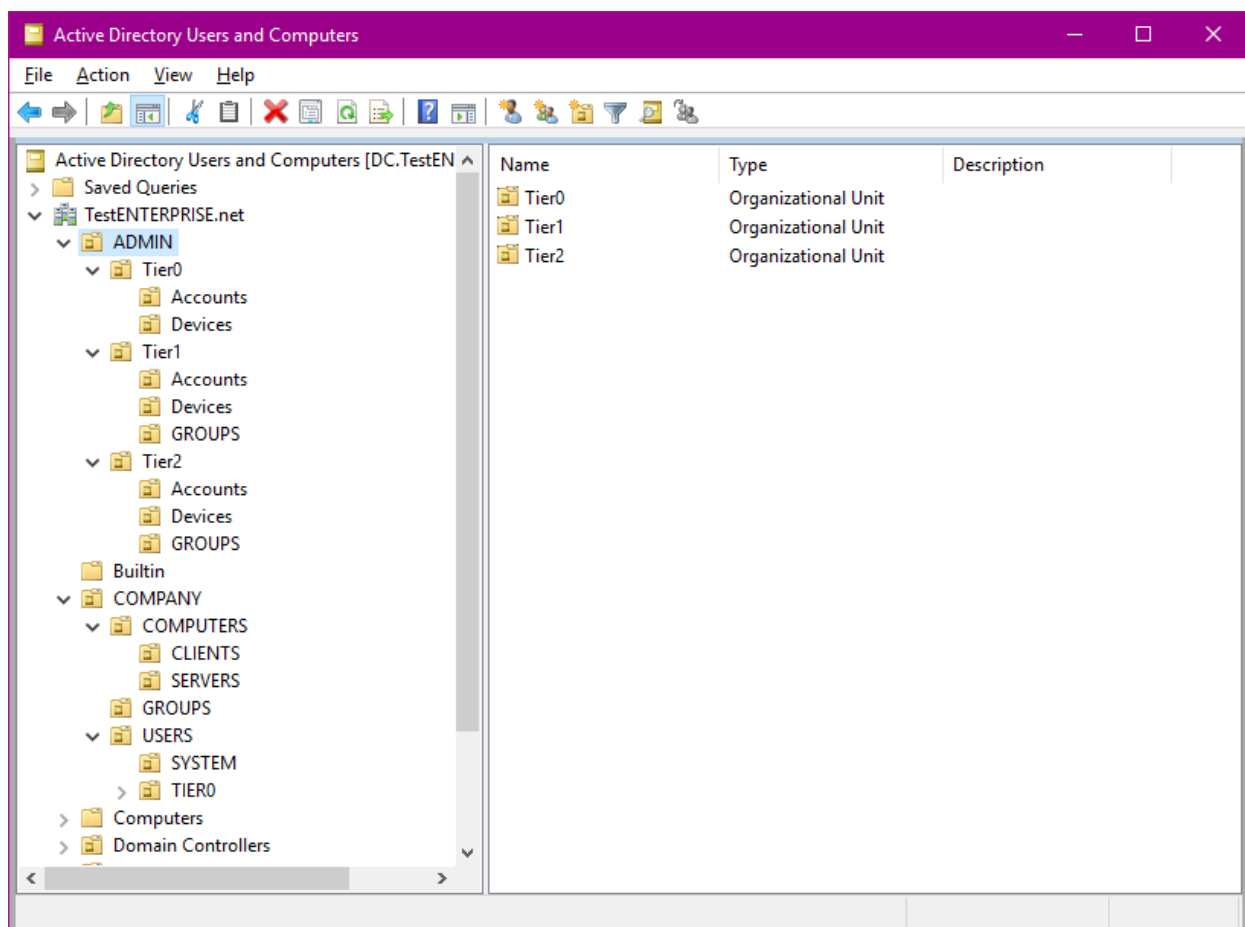
 michaelfirsov.wordpress.com/implementing-privileged-access-workstation-part-3

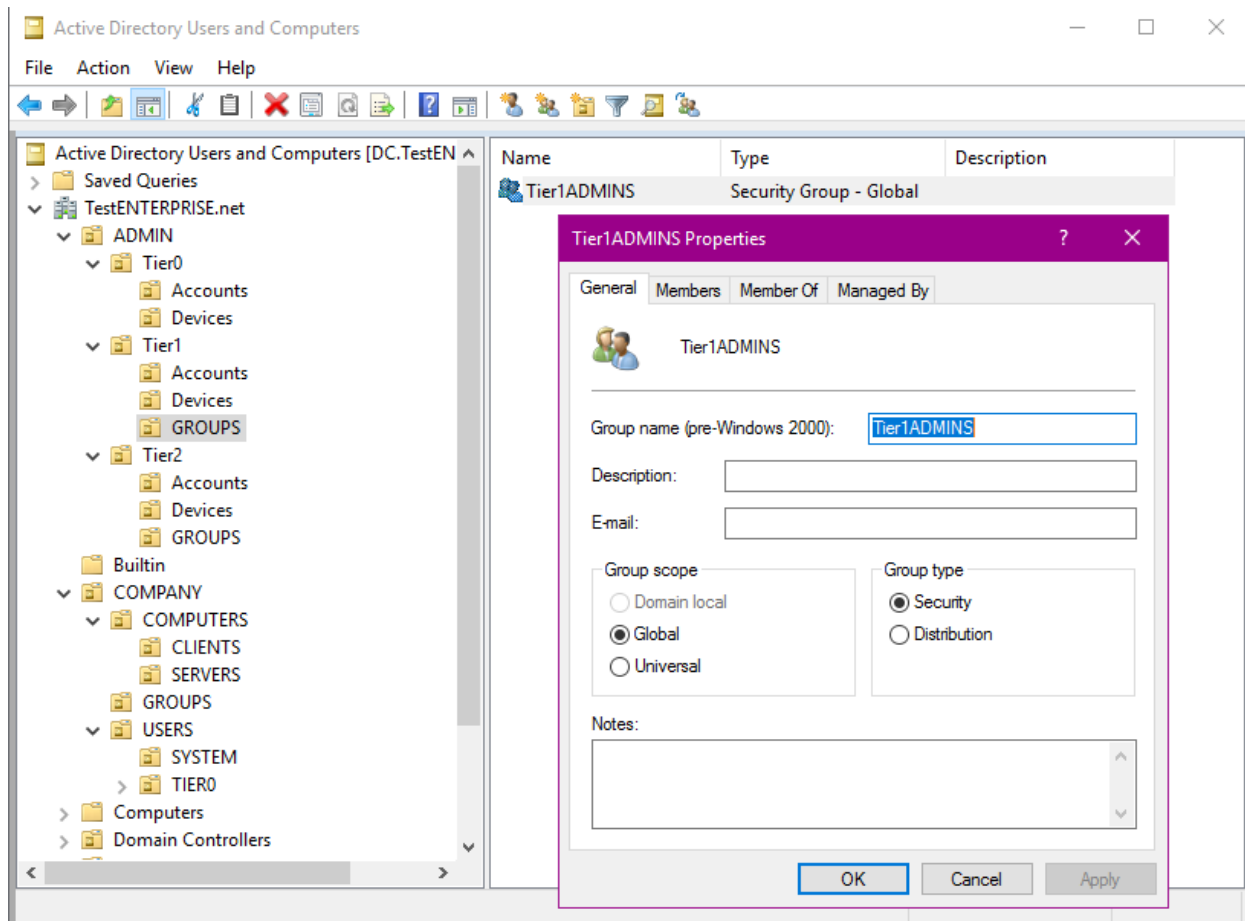
October 25, 2018

Part2

The next phase – **Phase 2** – implies that all tier1 servers (not domain controllers) are moved to the new Admin\Tier1\Devices OU and the user accounts which have administrative rights over these tier1 servers moved to the Admin\Tier1\Accounts OU. During the phase 3 administrators are supposed to move all user workstations to Admin\Tier2\Devices OU and all user accounts to Admin\Tier2\Accounts OU. Both Tier1\Devices and Tier2\Devices OUs should have the **RestrictServerLogon** gpo (I'll be using the same **RestrictWorkstationLogon** gpo as I said in part1) linked to them. The GROUPS OU in Tier1 and Tier2 OUs are supposed to host Tier1Admins\Tier2Admins security groups: only members of these groups should be able to administer the corresponding servers/workstations.

I wouldn't like to change severely the Active Directory "layout" in my testing network so I'll illustrate how the AD should look like but will use my SERVERS OU as Tier1\Devices OU and CLIENTS OU as Tier2\Devices OU (the latter in fact was already used above).

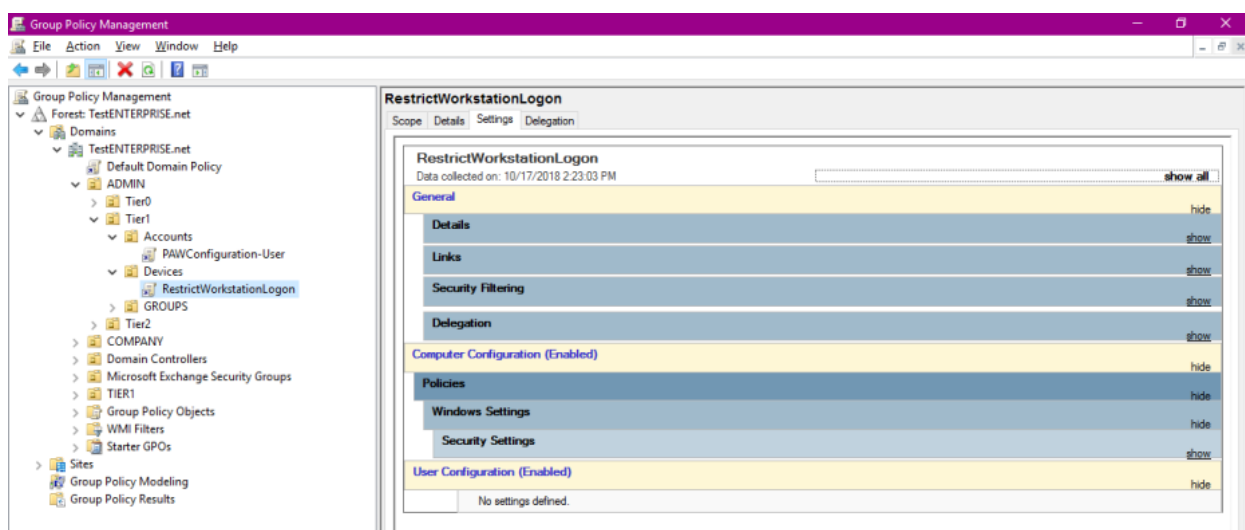




Advertisements

Report this adPrivacy

I link the **RestrictWorkstationLogon** gpo to Tier1\Devices (I will use it instead of RestrictServerLogon gpo because it's the same as RestrictWorkstation gpo) and the **PAWConfiguration-User** gpo to Tier1\Accounts. If you do want to allow your tier1 administrators to browse the Internet you can opt out of linking the **PAWConfiguration-User** gpo to Tier1\Accounts:



To securely connect from the paw to tier1 or tier2 devices (with tier1 or tier2 administrative accounts respectively) at least two more steps must be taken:

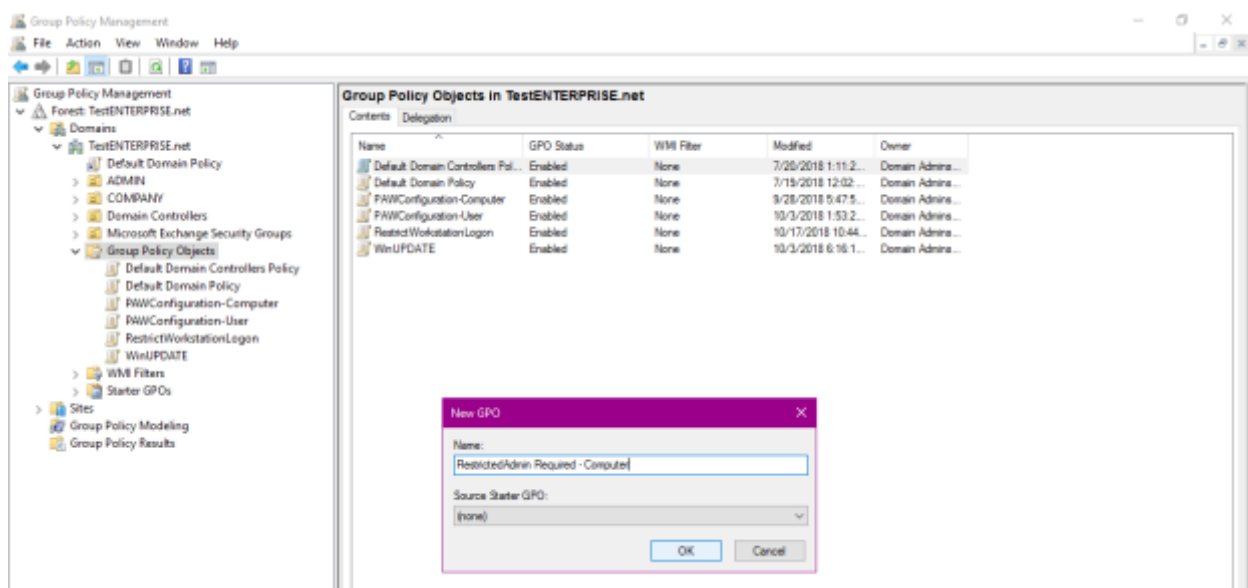
- 1) enable and enforce the use of **Restricted Admin** mode on all servers and workstations and
- 2) enable **Credential Guard** on a) workstations (as per MS's guide) b) servers

To get the most secure configuration MS recommends also to

3) Apply **Windows 10 Security baselines**


1) Enable and enforce the use of **Restricted Admin mode** on all servers and workstations

1-a) First we must enable target systems to receive incoming RDP connections using **RestrictedAdmin** mode:



New Registry Properties [X]

General Common

 Action: Update

Hive: HKEY_LOCAL_MACHINE

Key Path: SYSTEM\CurrentControlSet\Control\Lsa

Value name

☐ Default DisableRestrictedAdmin

Value type: REG_DWORD

Value data: 0

Base


☐ Hexadecimal

☒ Decimal

OK Cancel Apply Help

Group Policy Management Editor [Min] [Max] [X]

File Action View Help



Name	Order	Action	Hive	Key
DisableRestricted...	1	Update	HKEY_LOCAL_MAC...	SYSTEM

< Preferences Extended Standard >

Registry

The path to the key:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LsaName

The name: DisableRestrictedAdmin

The value: 0

The type: REG_DWORD

1-b) Second we must require all outbound RDP requests to use RestrictedAdmin mode:

The path to to the key: Computer Configuration\Policies\Administrative

Templates\System\Credentials Delegation

Restrict delegation of credentials to remote servers

Restrict delegation of credentials to remote servers

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on: At least Windows Server 2012 R2, Windows 8.1 or Windows RT 8.1

Options:

Use the following restricted mode:

Require Restricted Admin

Help:

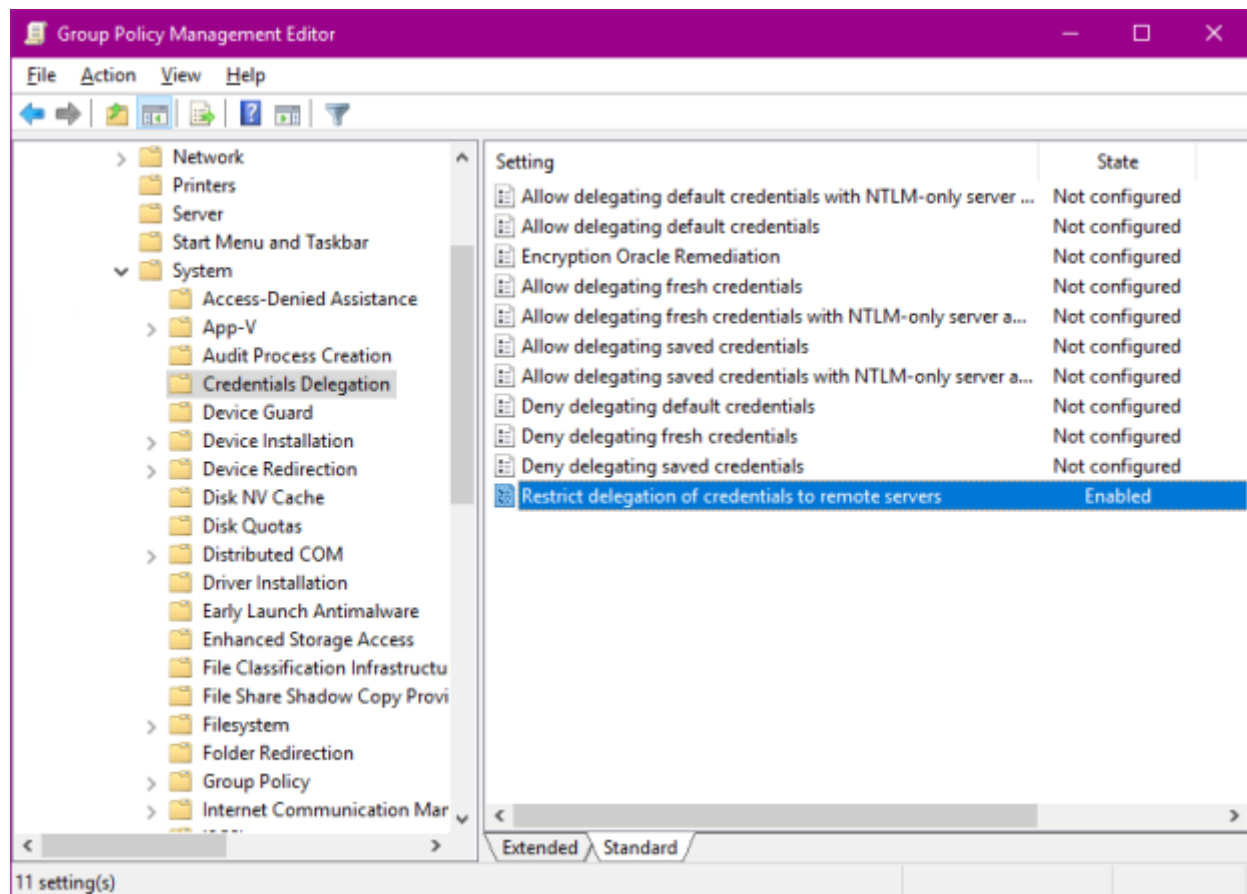
When running in Restricted Administration mode or if the device is using Remote Credential Guard, participating apps do not expose credentials to remote devices (regardless of the delegation method). Restricted Administration mode may limit access to resources located on other servers or networks beyond the target computer because credentials are not delegated. Remote Credential Guard does not limit access to resources by redirecting all requests back to the client device.

Participating apps:
Remote Desktop Client

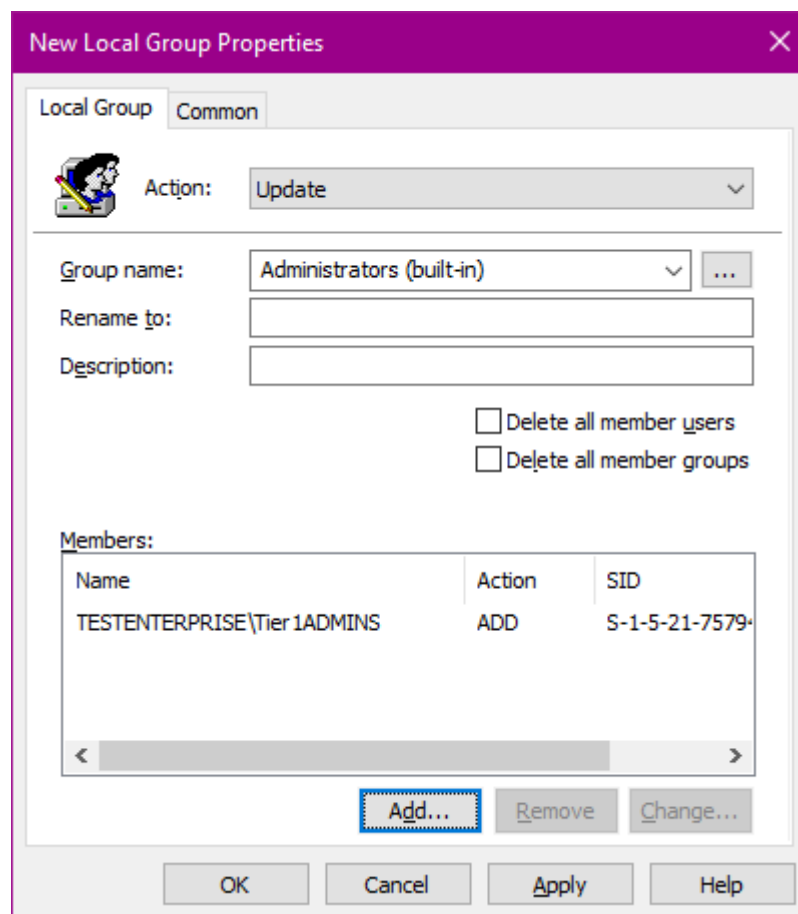
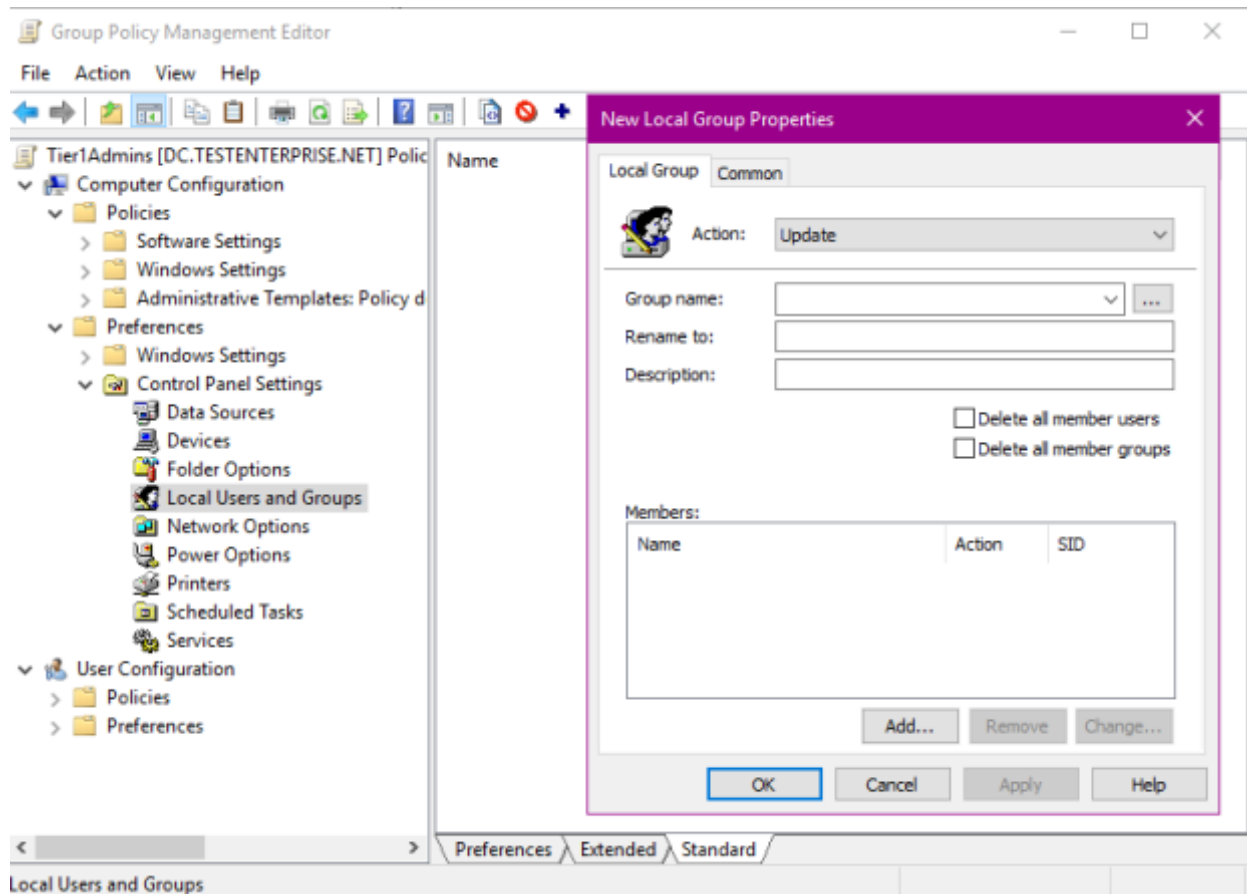
If you enable this policy setting, Restricted Administration mode or Remote Credential Guard is enforced and participating apps will not delegate credentials to remote devices.

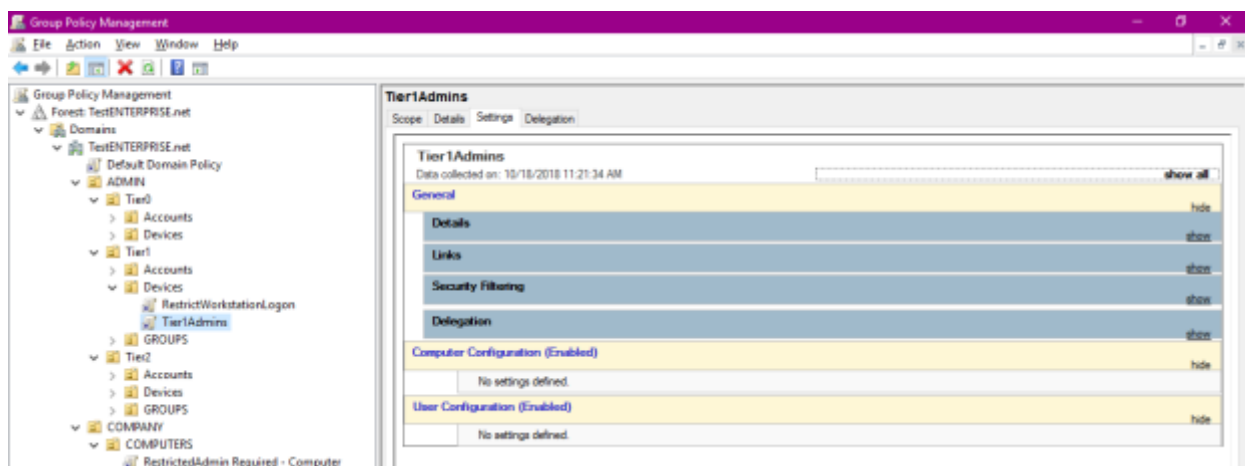
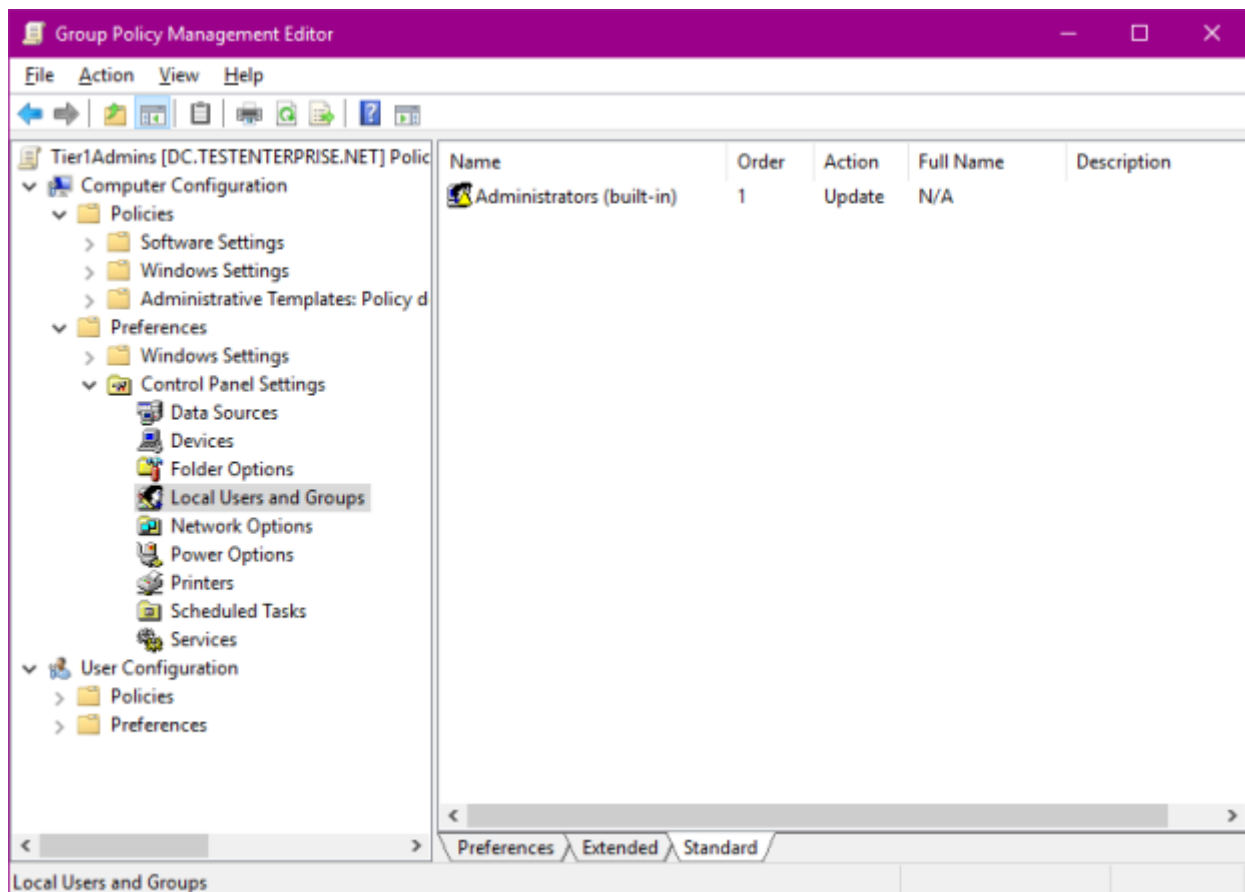
If you disable or do not configure this policy setting, Restricted Administration mode and Remote Credential Guard are not enforced and participating apps can delegate credentials to remote devices.

OK Cancel Apply



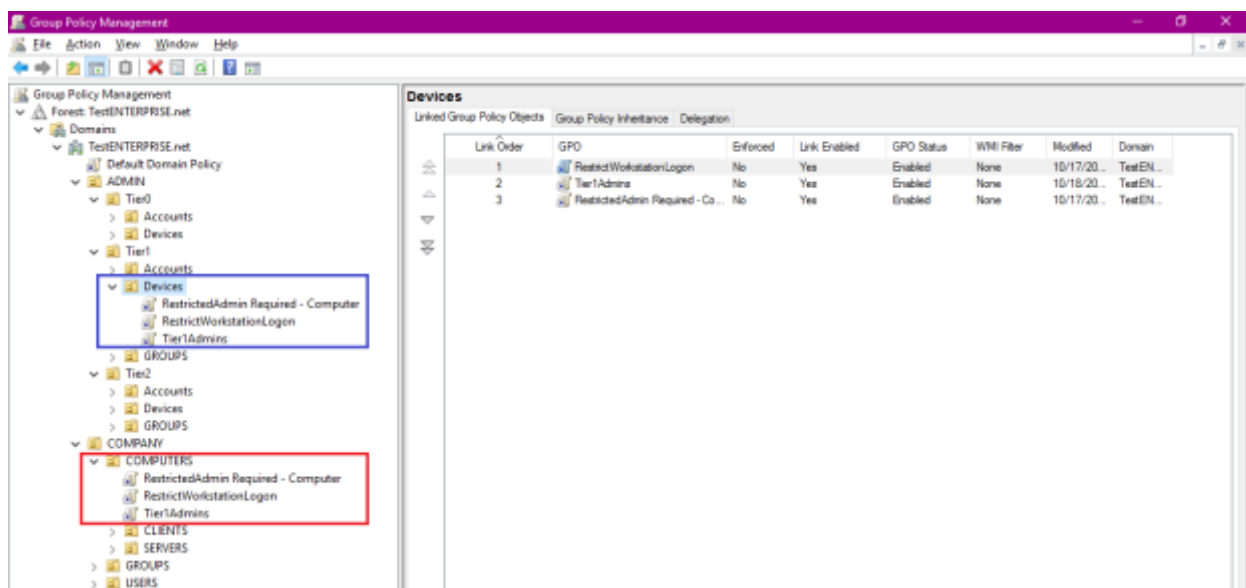
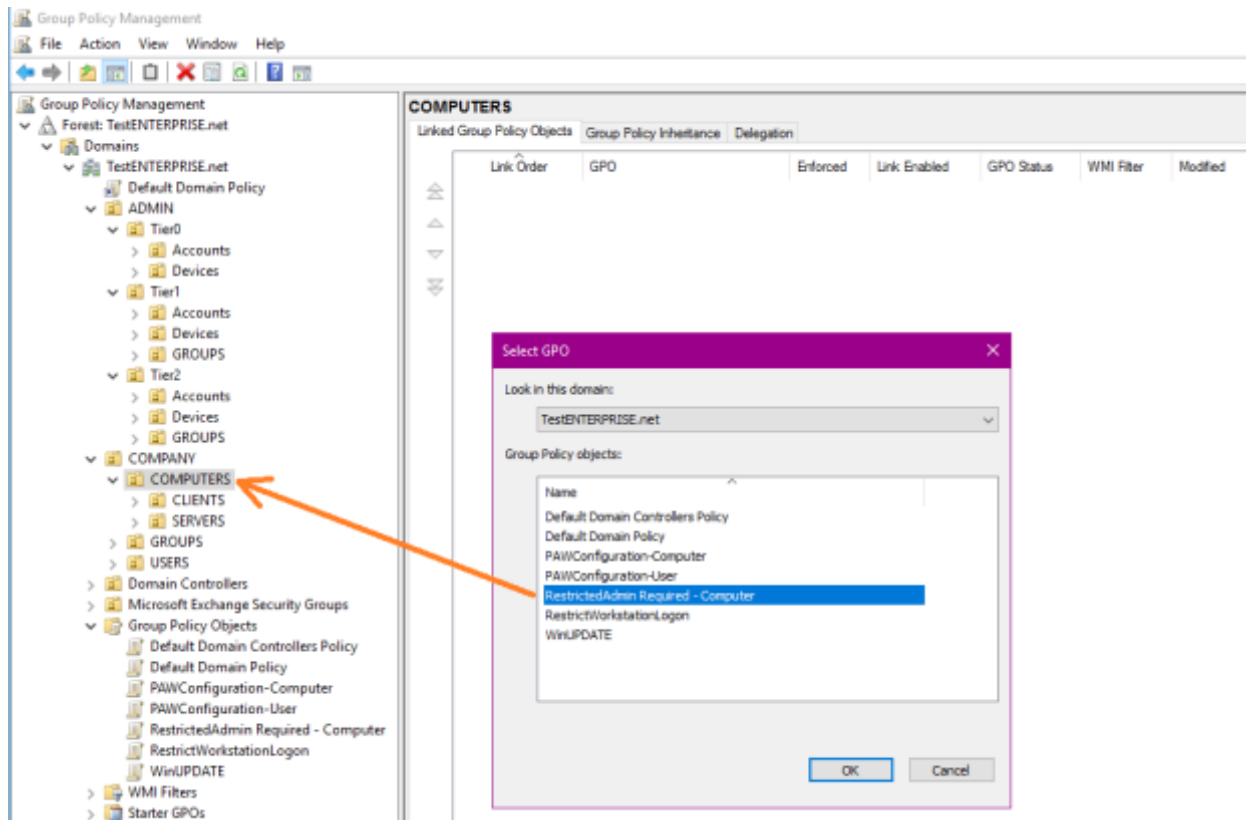
1-c) Third a new gpo must be created – **Tier1Admins** – that would add the group Tier1Admins to each local built-in Administrators group on each server: I'll be connecting to tier1 servers using the tier1 account (Michael Firsov) which will be the member of the each tier1 servers' local built-in Administrators group. (similarly Tier2Admins OU and Tier2Admining global groups should be created for administering Tier2\Devices but for the sake of bravery I'll demonstrate phase 2 using Tier1 only):





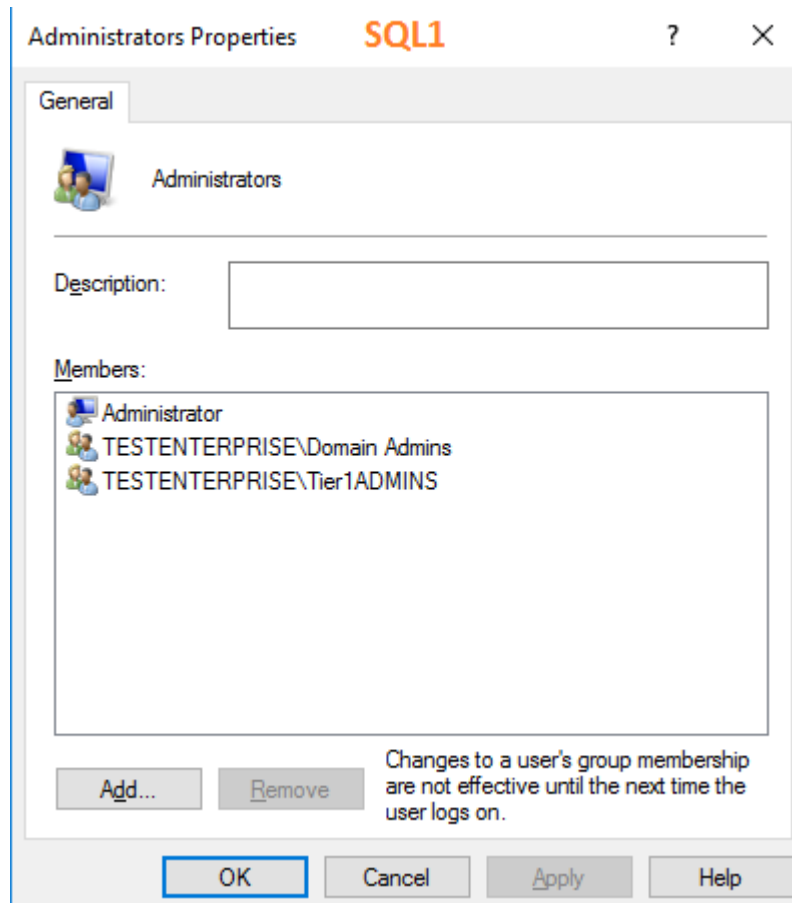
Eventually Tier1\Devices OU should have the following GPOs linked to it:
RestrictedWorkstationLogon (MS recommends creating a separate
 RestrictedServerLogon GPO but I'm going to link the existing one for simplicity),
RestrictedAdminRequired and **Tier1Admins**.

As I didn't move my server and workstation computer accounts to Tier1\Devices and Tier2\Devices I'll be using COMPANY\COMPUTERS OU instead, so I'll link all these GPOs to COMPUTERS OU:

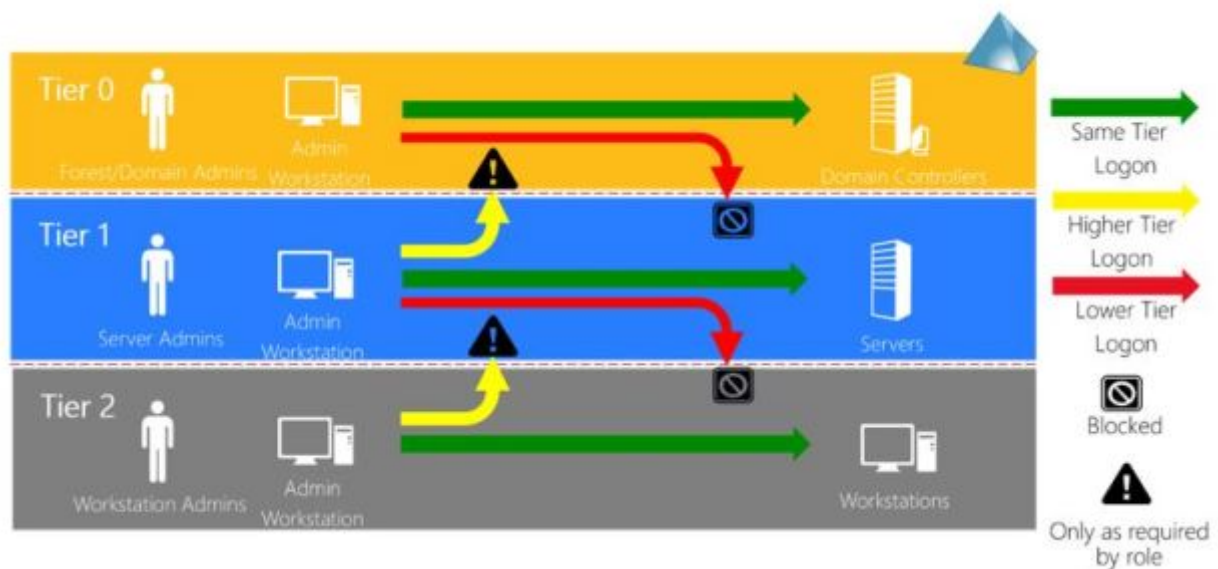


Let's now try to RDP from the paw into the virtual server named SQL1:

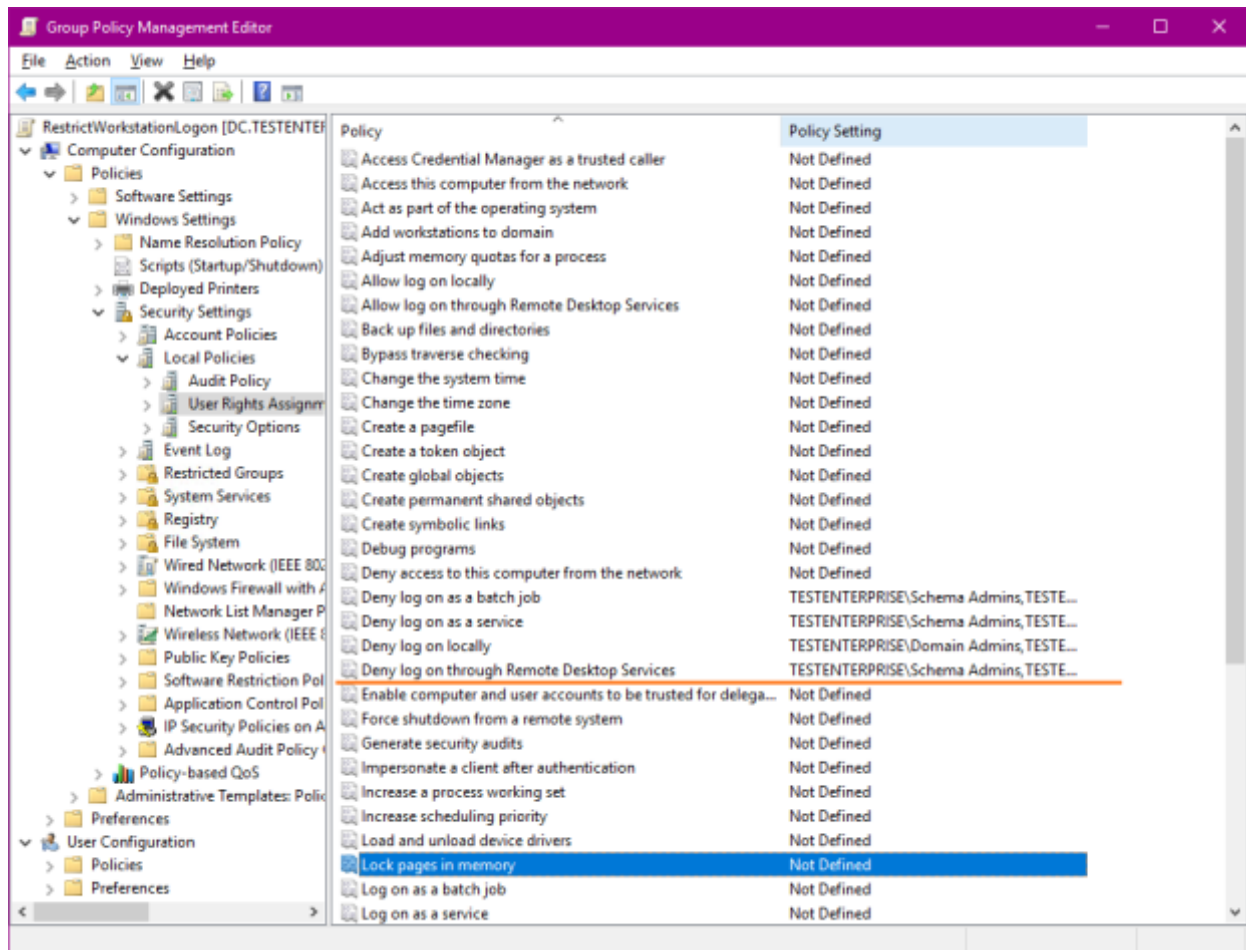
a) log on to SQL1 as *TestENTERPRISE\EntAdmin* – this account IS a member of local Administrators group (via membership in DomainAdmins group) and SHOULD HAVE the remote access to the server:



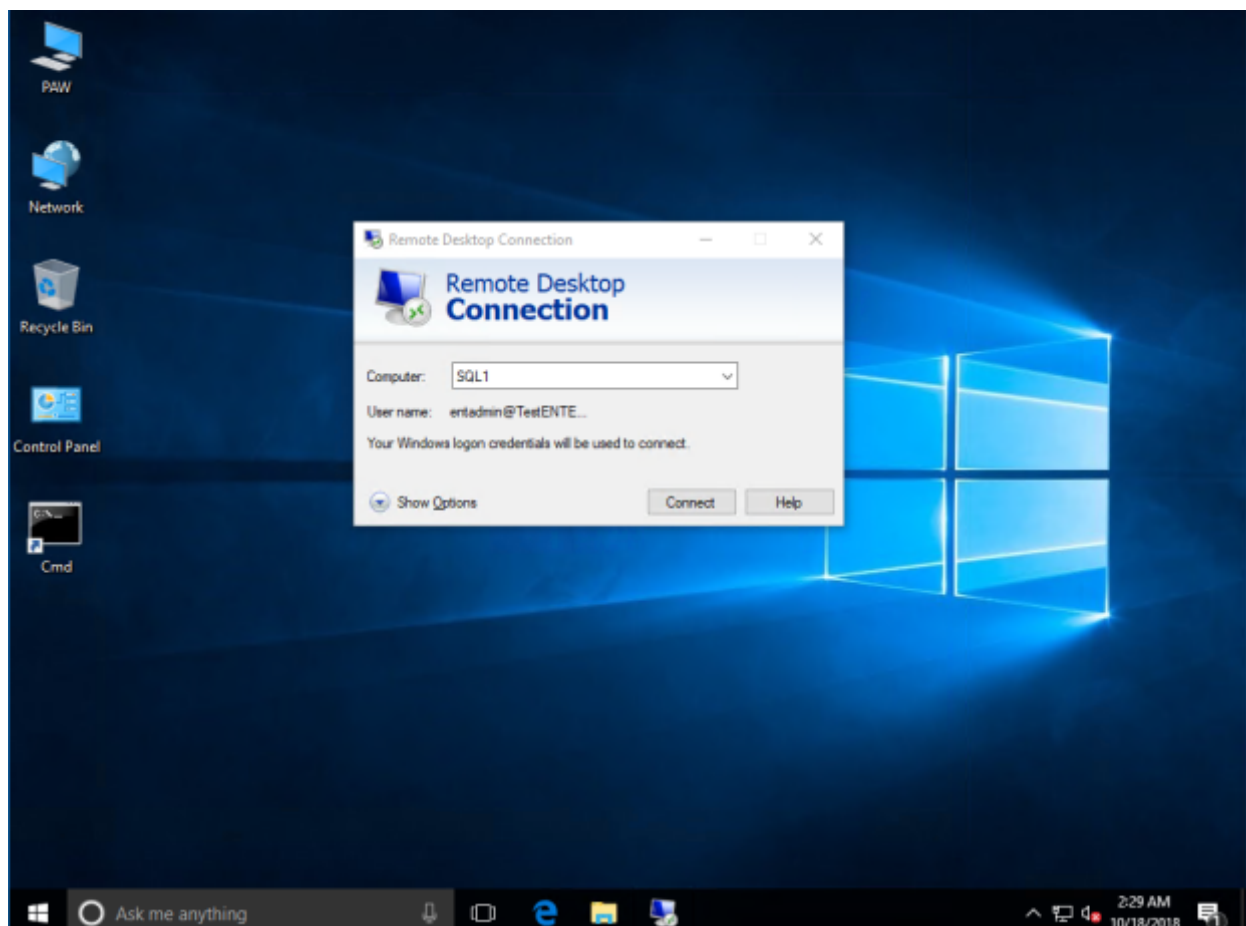
– and this contradicts the paw theory deccribed here:

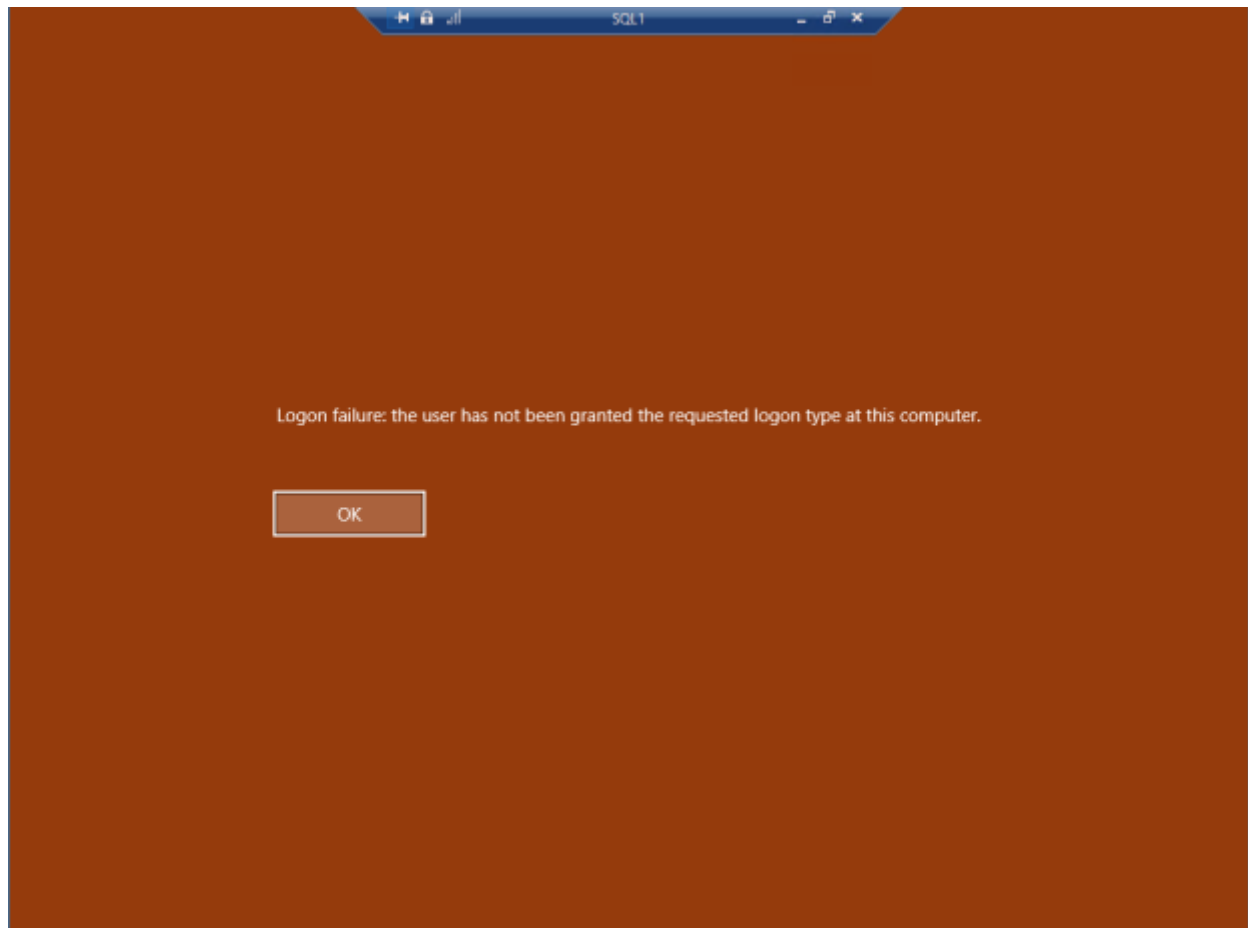


As you see tier0 administrators (*EntAdmin*) should NOT have access to tier1 servers: *Deny Logon Locally* user right does really prevents tier0 admins from logging onto tier1 servers LOCALLY, but if you follow MS guide there will be no restriction for the remote access: no policy setting would prevent tier0 admins from connecting to tier1 servers (of course if Remote Access is enabled on them) – that's why I have added *Deny Logon through Remote Service* restriction in the **RestrictWorkstationLogon** gpo:

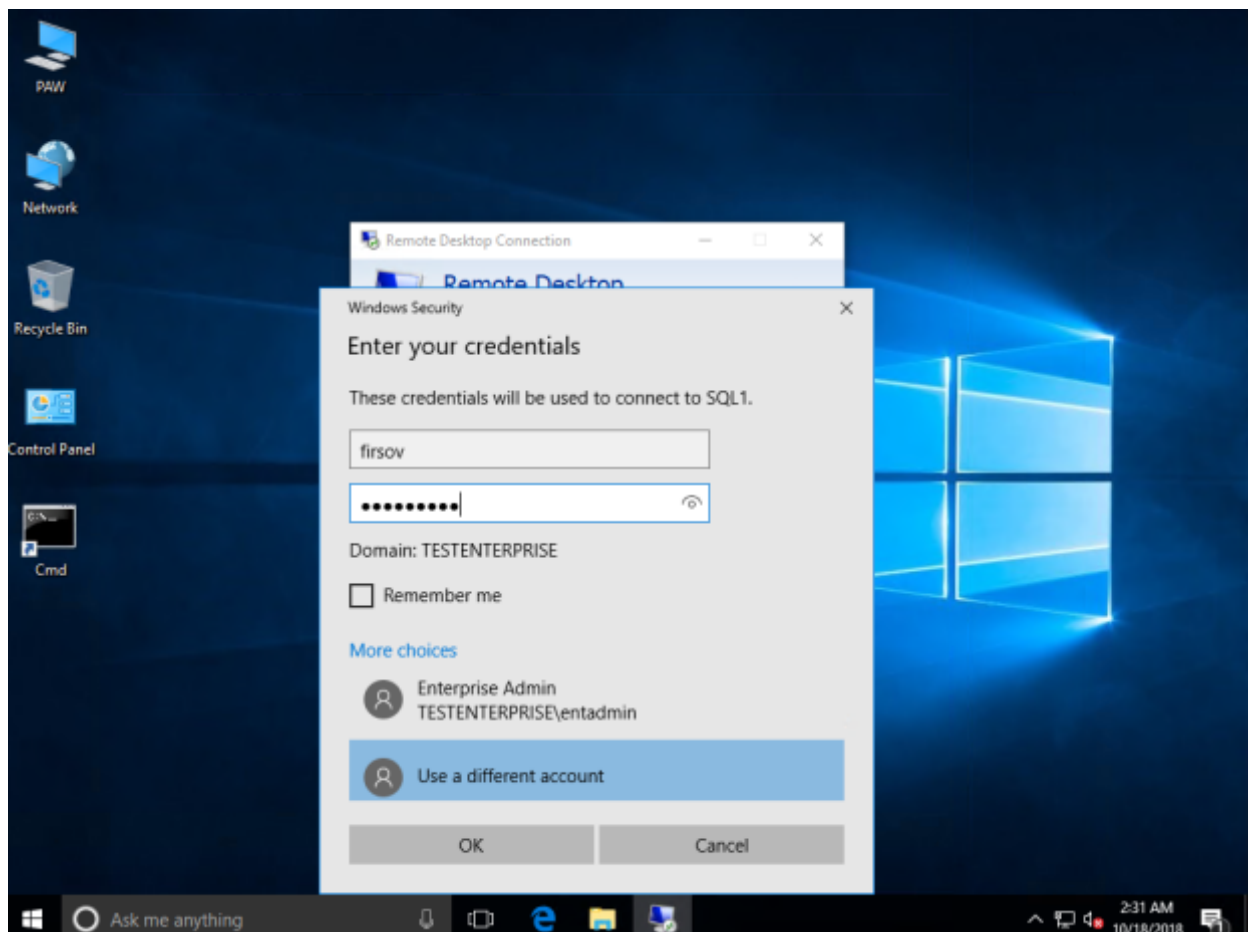


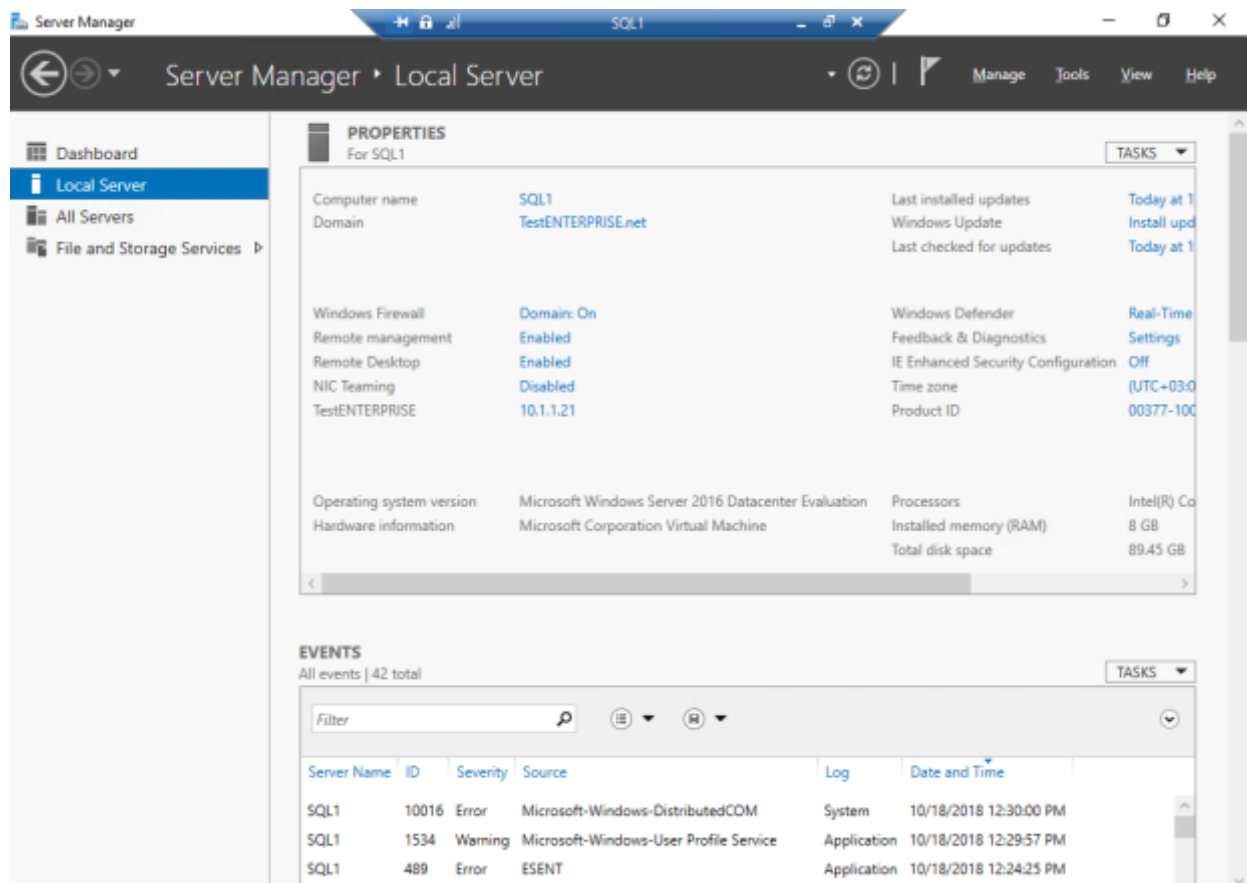
So with this setting *EntAdmin* should NOT be able to connect to SQL1:



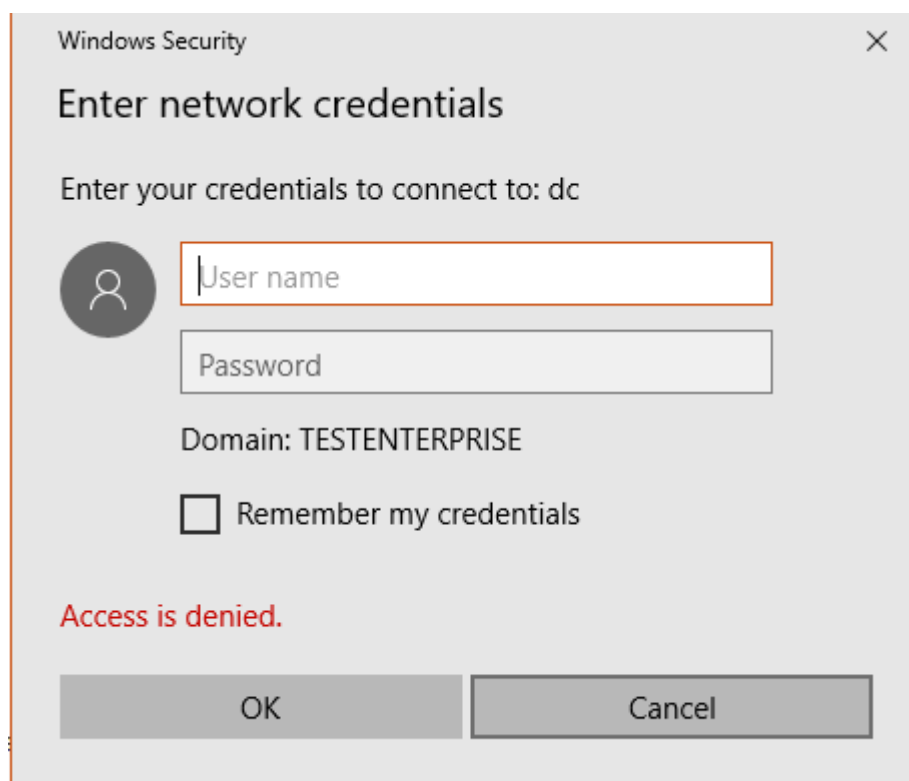


Michael Firsov user account – which is a member of the Tier1Admins group – should be able to log on:

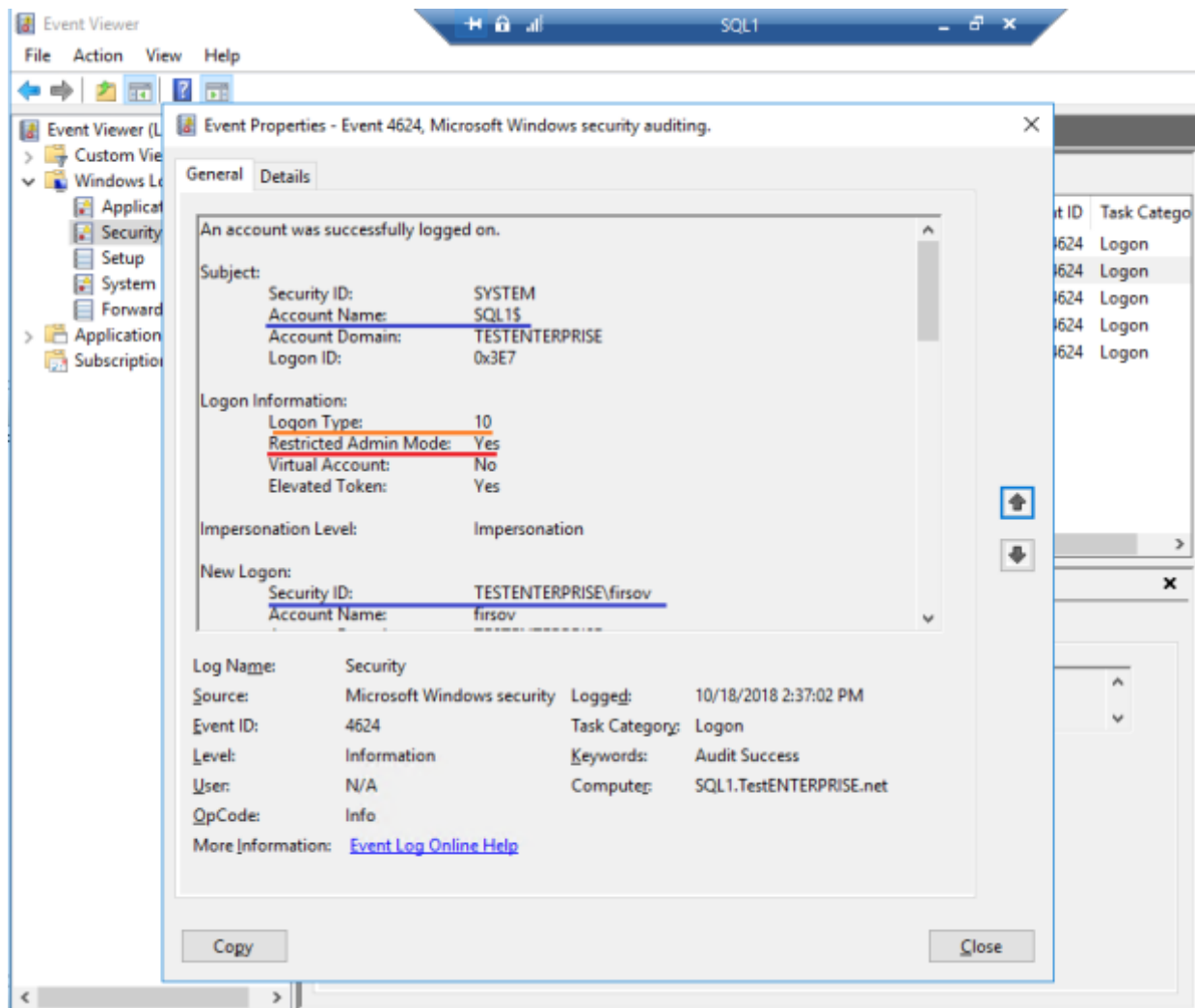




If I now try to access some administrative shared folder – for example, \\dc\\c\$ – I'll be faced with the authentication dialog window:

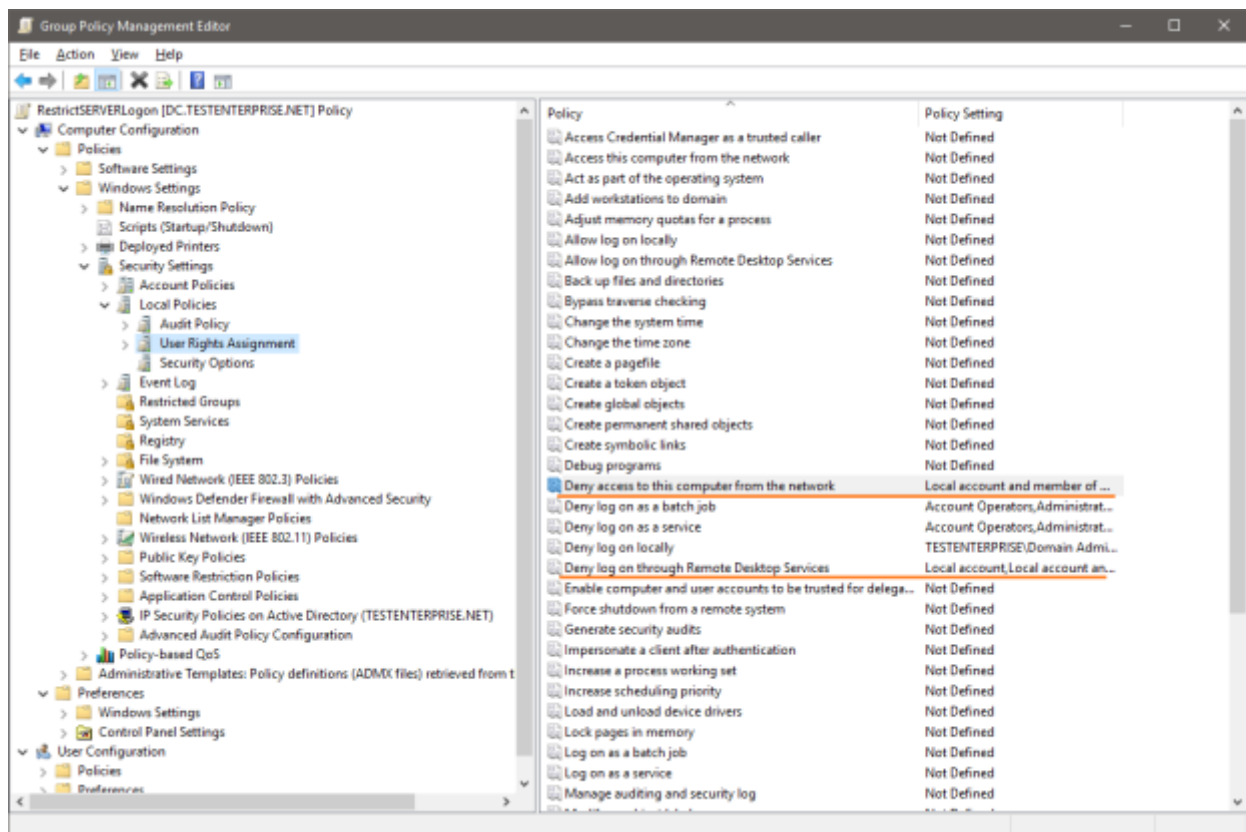
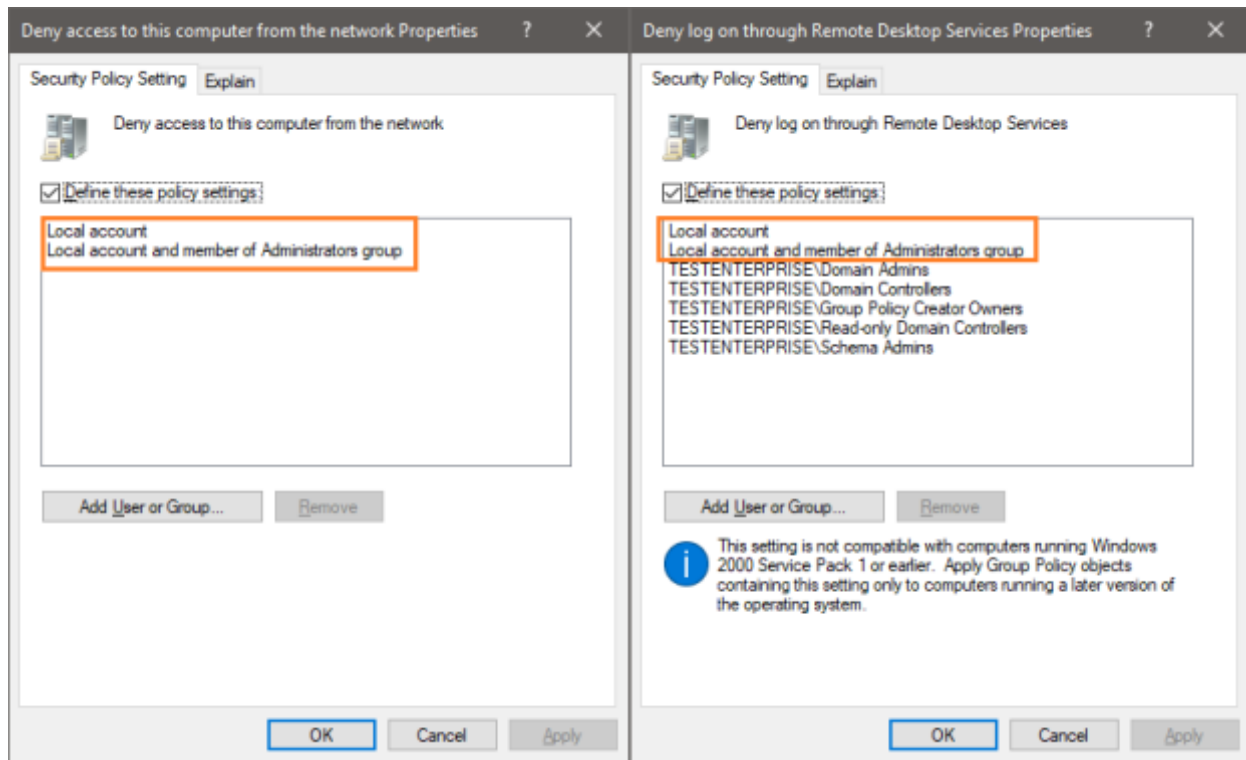


That is because in the **Restricted Admin Mode** user works under the computer account to which he/she is connecting(SQL1\$), not under the account he/she has actually logged on. You can see it in the SQL1's security log:



UPDATE: To prevent using local accounts for network and RDP access the following two SIDs may be added to these policy settings (more information is [here](#)):

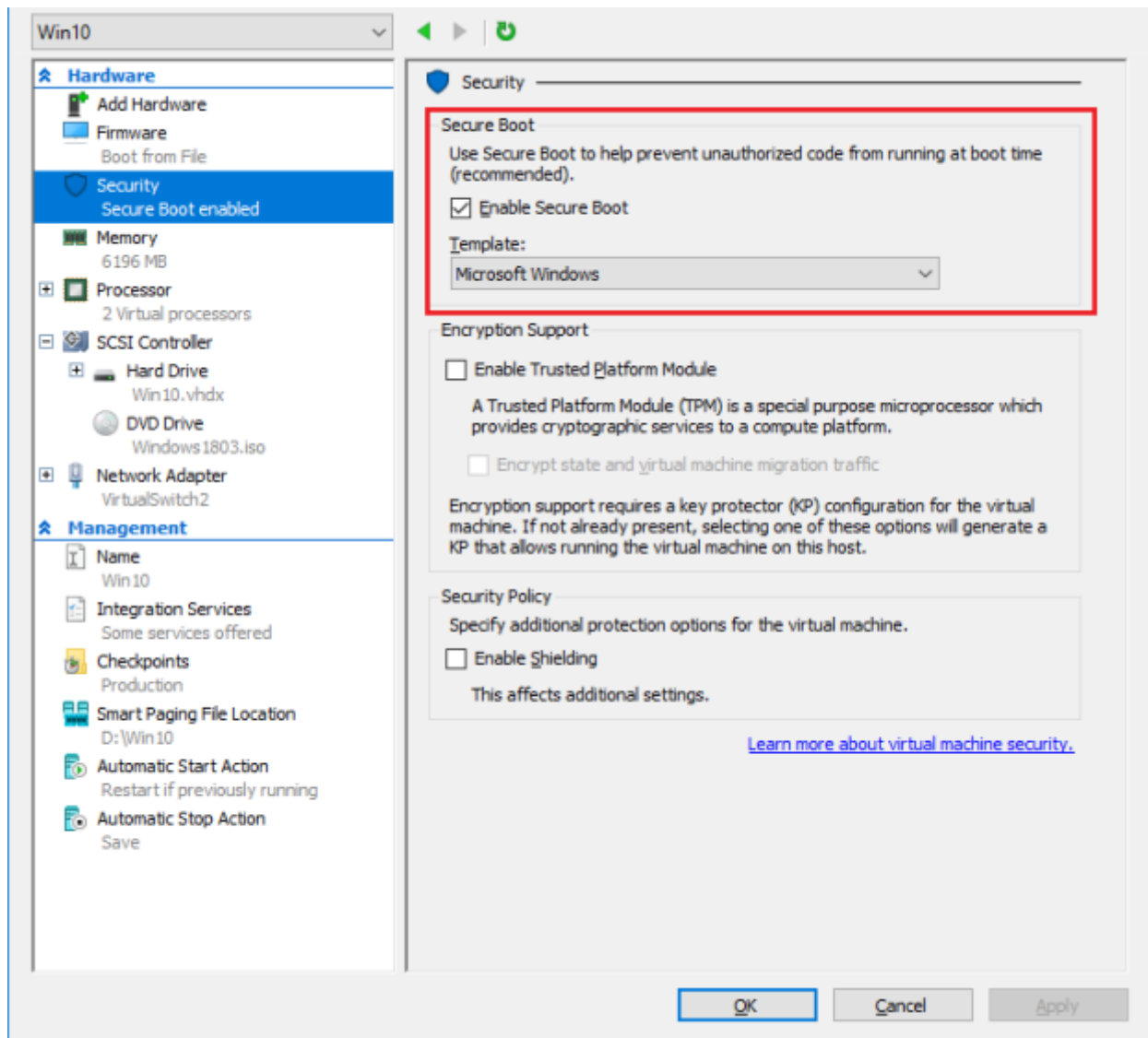
- **S-1-5-113: NT AUTHORITY\Local account**
- **S-1-5-114: NT AUTHORITY\Local account and member of Administrators group**



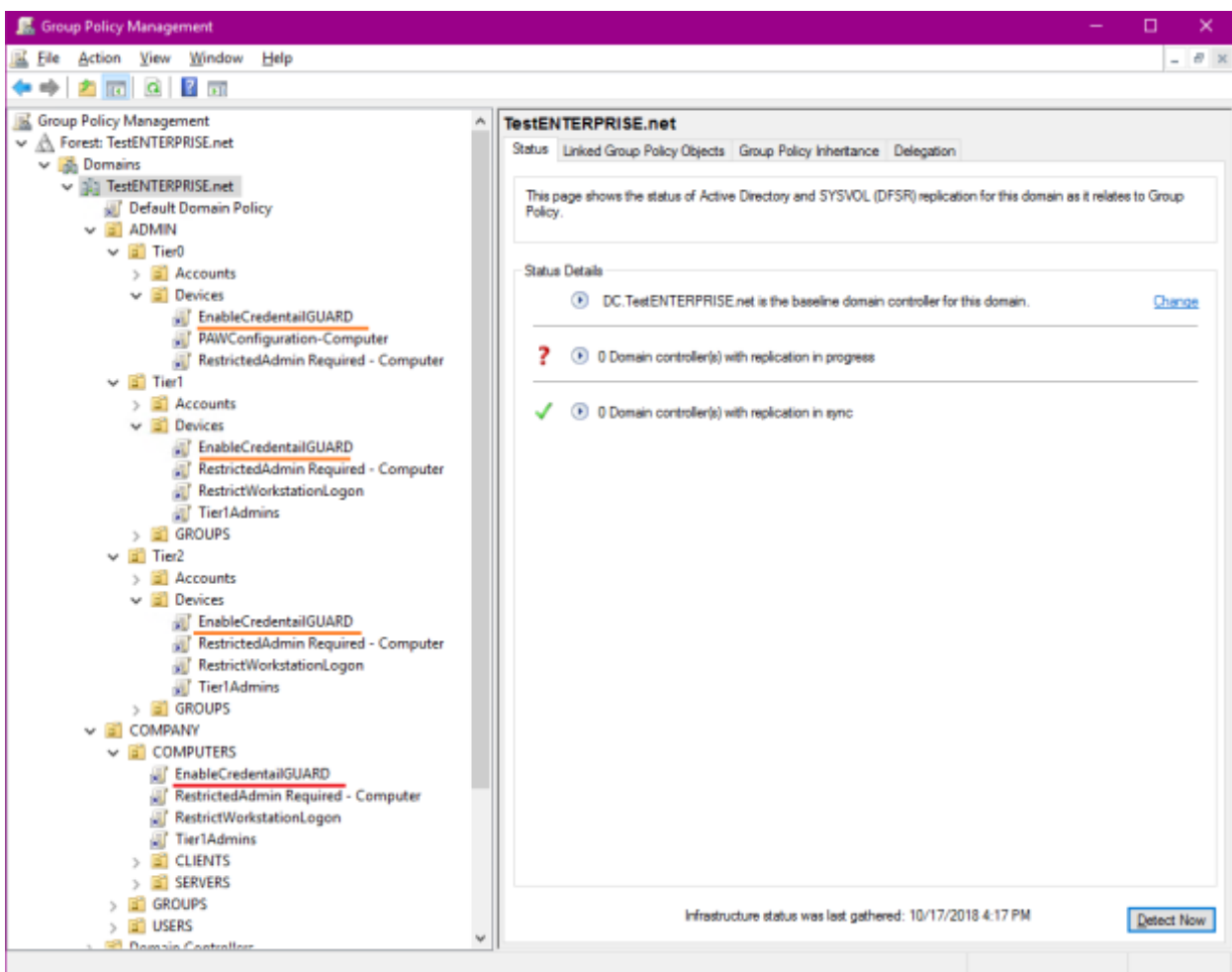
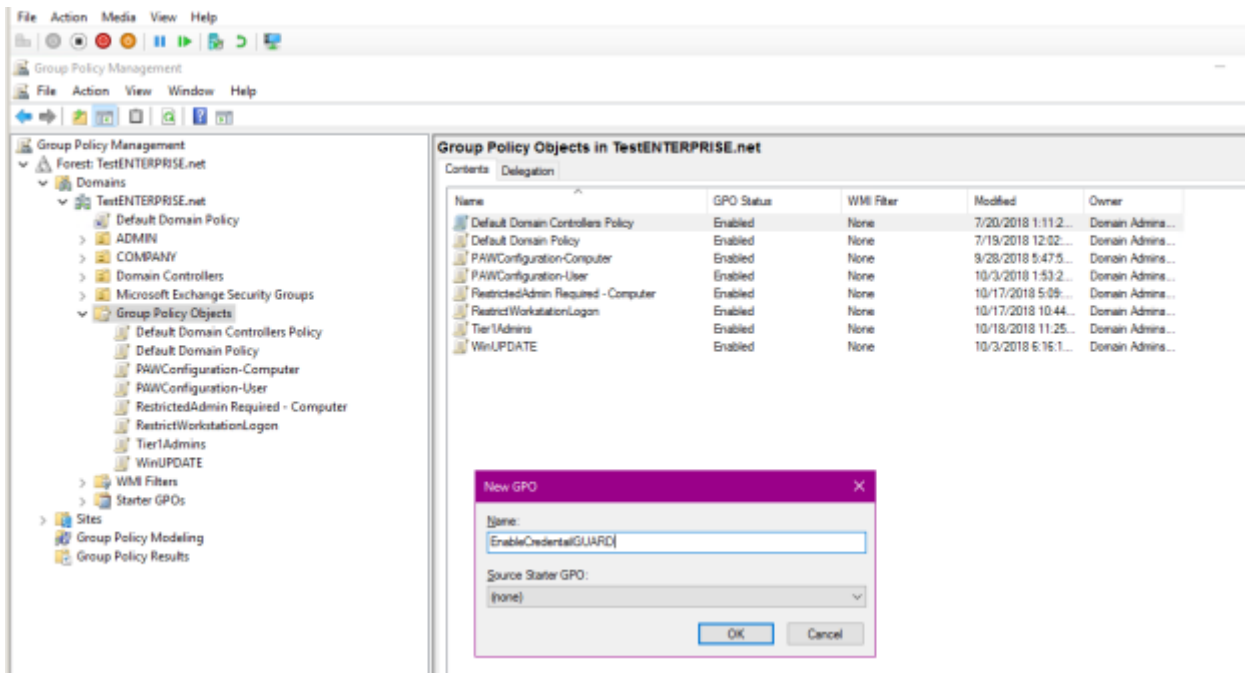
2) enable Credential Guard

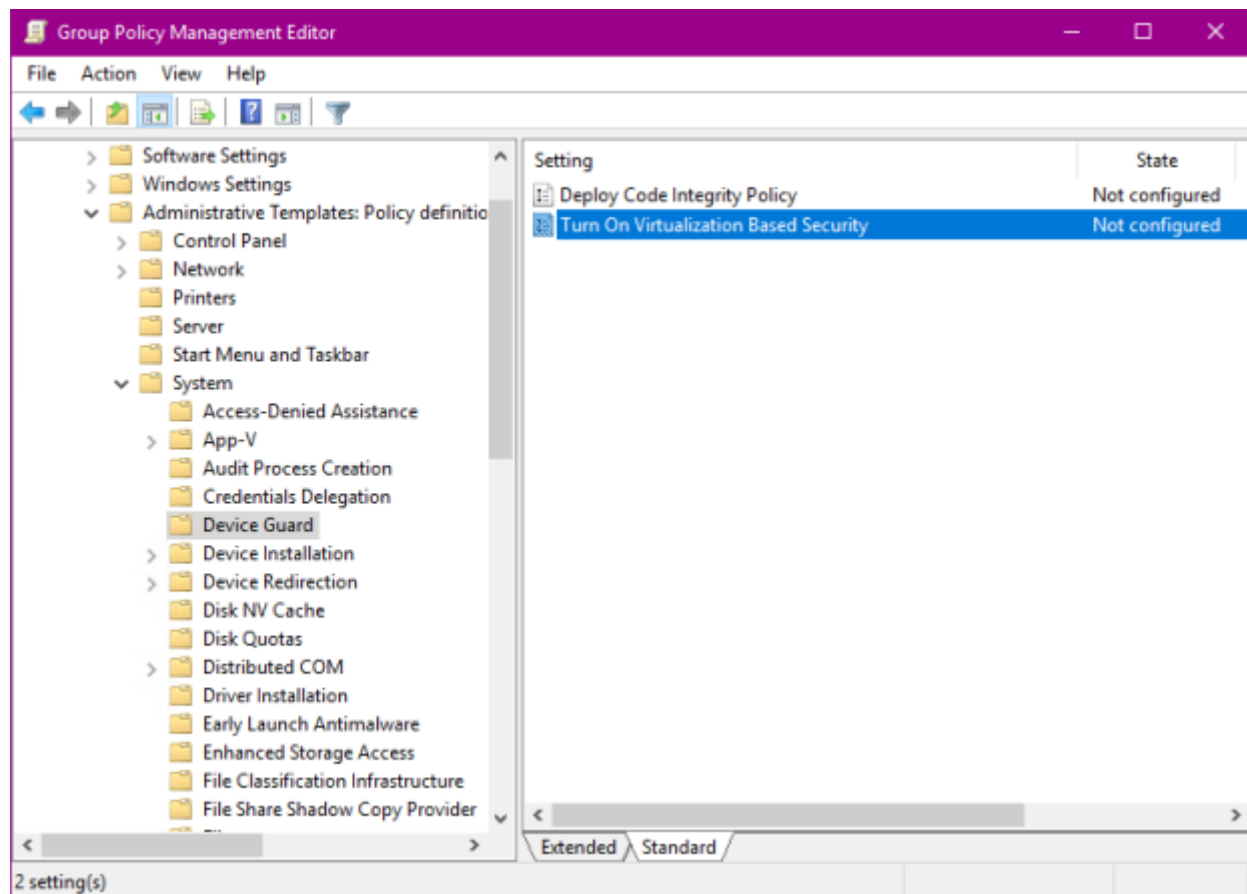
MS recommends enabling Credential Guard on Windows 10 computers – I will try to enable it on all my client and server computers (virtual!!!) in the COMPUTERS OU – or if my server and client computer accounts had been moved according to MS paw deployment guide I would Credential Guard for Tier0\Devices, Tier1\Devices and Tier2\Devices.

Please remember that by default Secure Boot which is required for CG is enabled both for virtual machines and (generally) for physical machines.



To turn on CG for my server and client computers I create a new gpo – **EnableCredentialGUARD**, navigate to Computer Configuration\Administrative Templates\System\ Device Guard and set *Select Platform Security Level* to Secure Boot and DMA Protection and *Credential Guard Configuration* to *Enabled without lock*. For testing purposes I link the **EnableCredentialGUARD** gpo to Tier0\Tier1\Tier2\Devices OUs as well as to COMPANY\COMPUTERS OU. According to MS it should be linked only to Tier2\Devices (client machines with Windows 10).





Turn On Virtualization Based Security
Previous Setting
Next Setting

☐ Not Configured
Comment:
☒ Enabled
☐ Disabled

Supported on:

At least Windows Server 2016, Windows 10

Options:

Select Platform Security Level:

Secure Boot and DMA Protection

Virtualization Based Protection of Code Integrity:

Disabled

Credential Guard Configuration:

Enabled without lock

Help:

Specifies whether Virtualization Based Security is enabled.

Virtualization Based Security uses the Windows Hypervisor to provide support for security services. Virtualization Based Security requires Secure Boot, and can optionally be enabled with the use of DMA Protections. DMA protections require hardware support and will only be enabled on correctly configured devices.

Virtualization Based Protection of Code Integrity

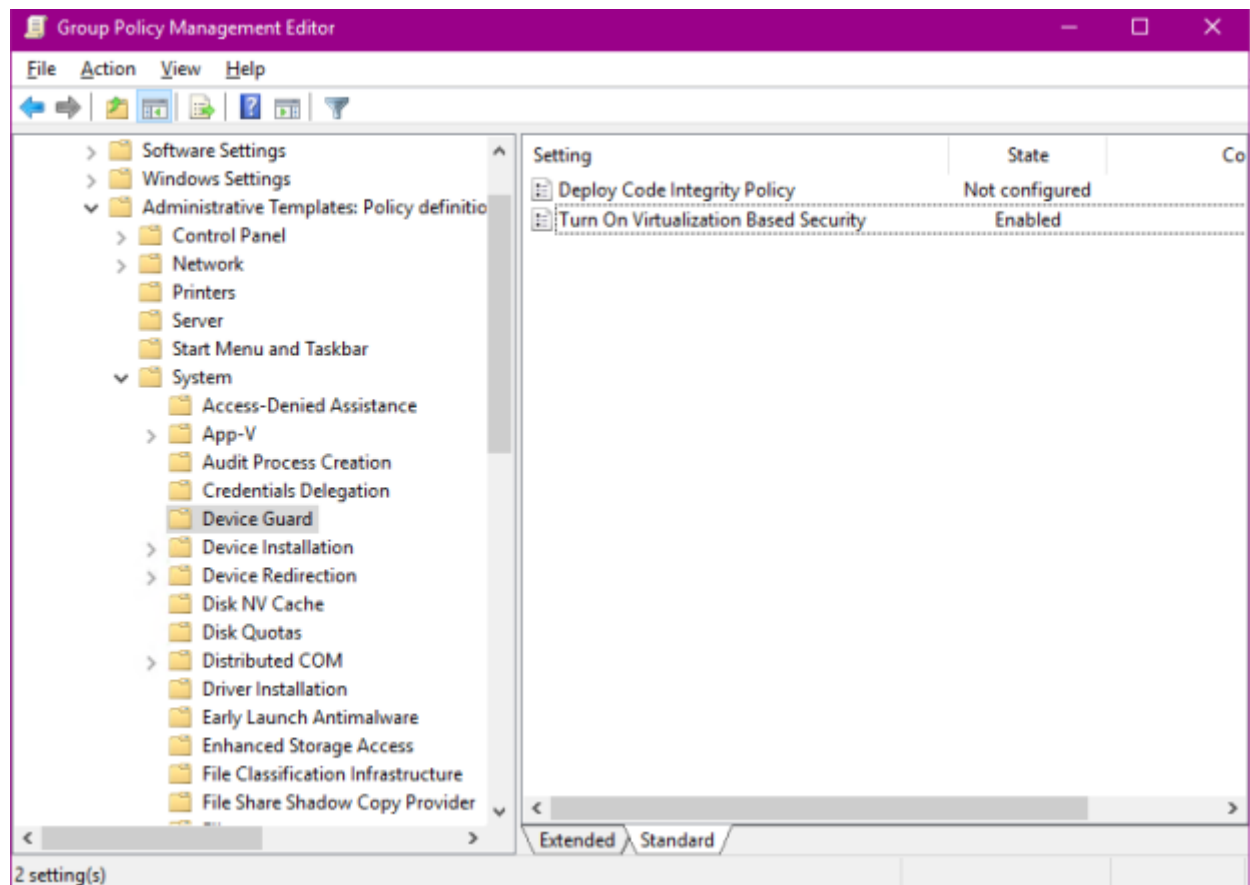
This setting enables virtualization based protection of Kernel Mode Code Integrity. When this is enabled, kernel mode memory protections are enforced and the Code Integrity validation path is protected by the Virtualization Based Security feature.

The "Disabled" option turns off Virtualization Based Protection of Code Integrity remotely if it was previously turned on with the "Enabled without lock" option.

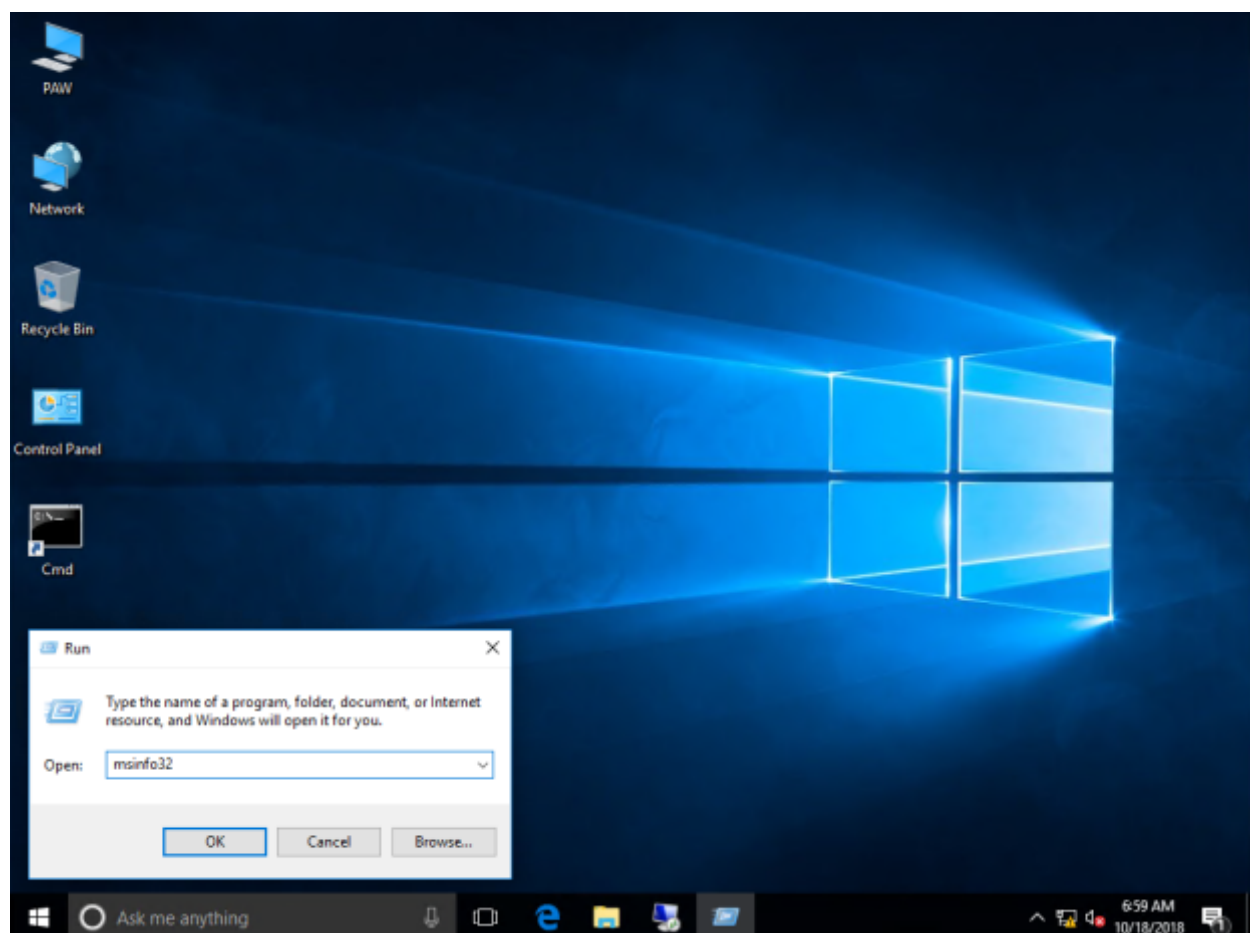
OK

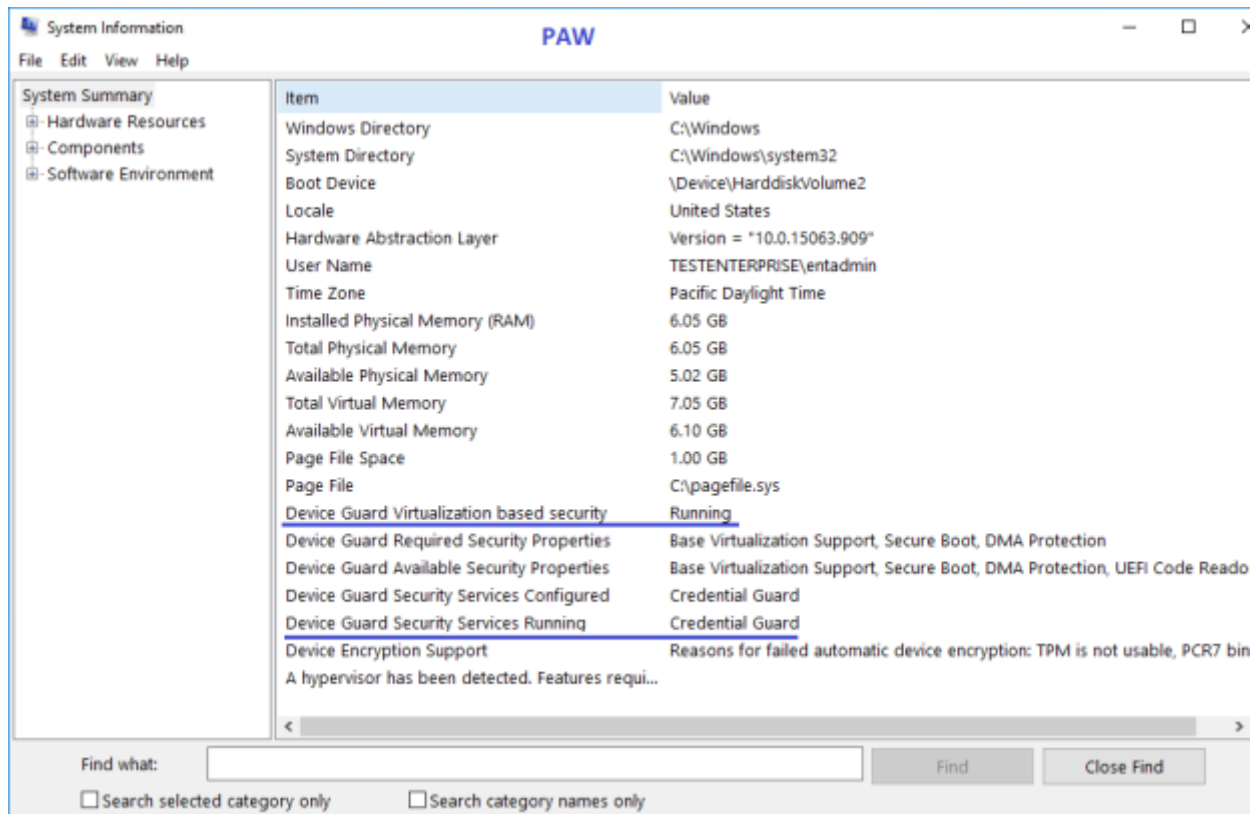
Cancel

Apply



2-a) Let's check if Credential Guard is running on the PAW virtual machine (Windows 10 Enterprise version 1703) :





As you see **Device Guard Virtualization based security** has the status of **Running** – as expected: Credential Guard does work on Windows 10 Enterprise 1703.

We can also check it using MS DG_Readiness_Tool:

```

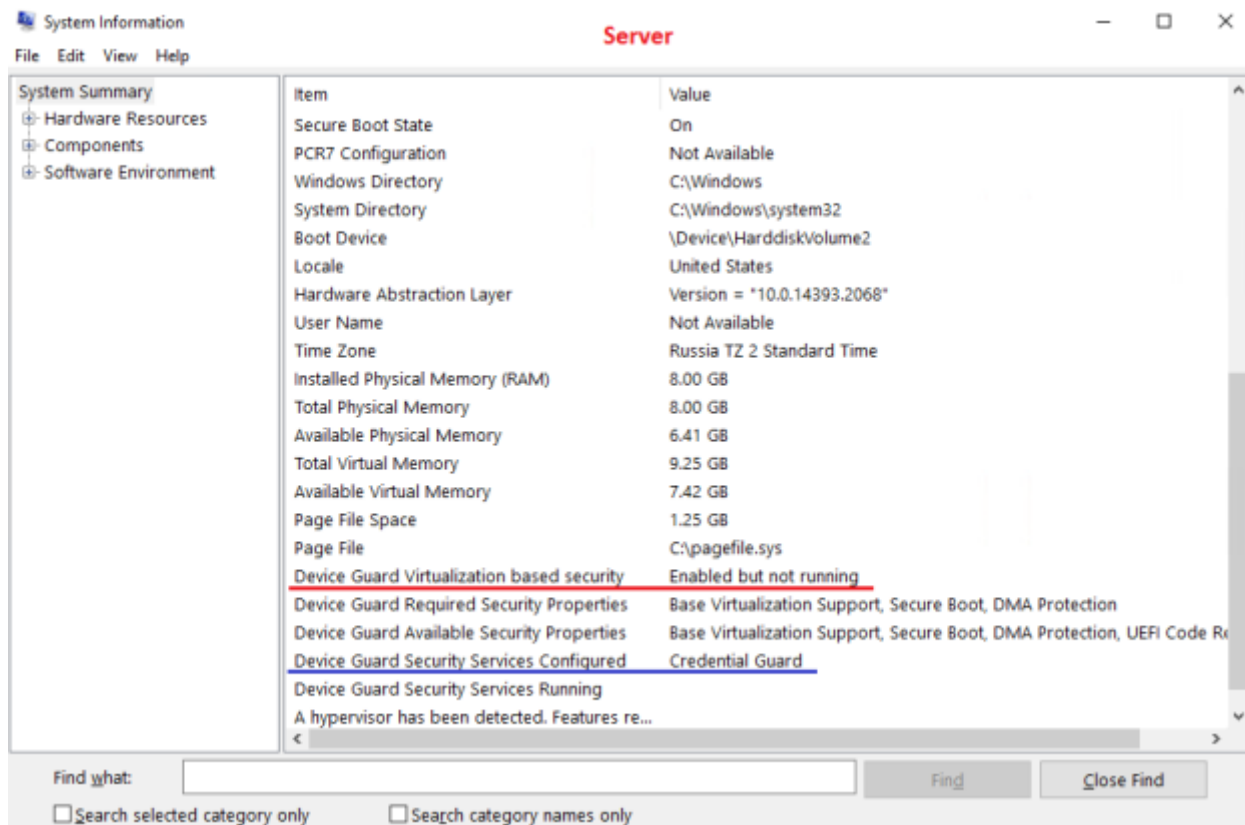
Administrator: Windows PowerShell

Running on a Virtual Machine. DG/CG is supported only if both guest VM and host machine are running with Windows 10, ver
sion 1703 or later with English localization.
=====
OS and Hardware requirements for enabling Device Guard and Credential Guard
1. OS SKUs: Available only on these OS Skus - Enterprise, Server, Education, Enterprise IoT, Pro, and Home
2. Hardware: Recent hardware that supports virtualization extension with SLAT
To learn more please visit: https://aka.ms/dgwhcr
=====
Credential-Guard is enabled and running.
HVCI is not running.
Config-CI is not running. (Not Enabled)
Not all services are running.

PS C:\Distr\DG_Readiness_Tool_v3.5>

```

2-b) Now let's run *msinfo32* on the SQL1 virtual machine (Windows Server 2016)



That's the most interesting situation:

Credential Guard is configured but does not work because – probably – it relies on Virtualization based security. Why? According to this [article](#) the following requirements must be met to enable CG on a virtual machine:

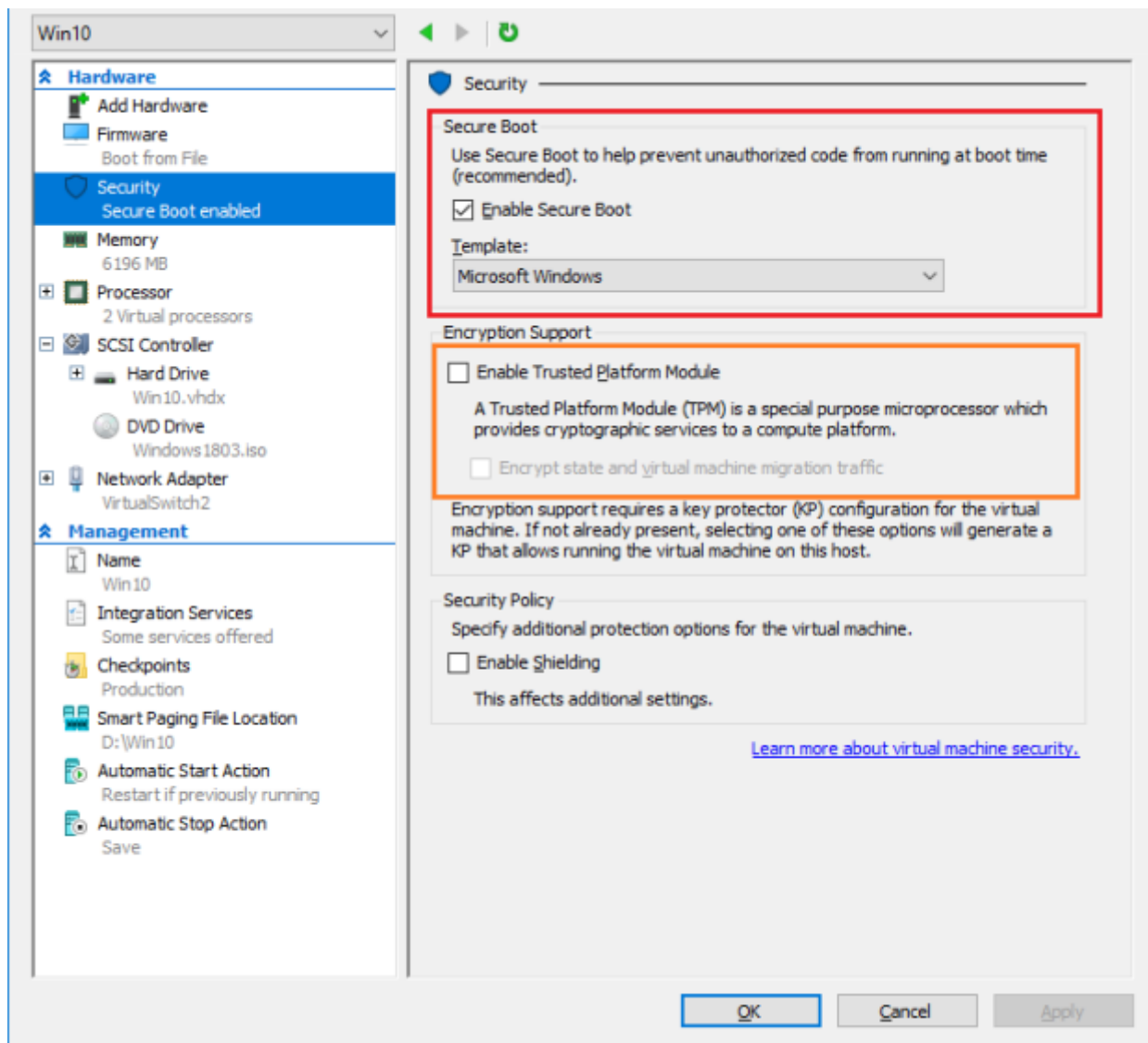
Requirements for running Windows Defender Credential Guard in Hyper-V virtual machines

- *The Hyper-V host must have an IOMMU, and run at least Windows Server 2016 or Windows 10 version 1607.*
- *The Hyper-V virtual machine must be Generation 2, have an enabled virtual TPM, and be running at least Windows Server 2016 or Windows 10.*

The key takeaways here:

- 1) the minimum supported version for BOTH Windows 10 and Windows 2016 is 1607
- 2) a virtual TPM must be enabled

This requirement – a virtual TPM must be enabled – is not correct because the paw machine does NOT have its virtual TPM running but CG works perfect:



2) Both Windows 10 and Windows Server 2016 (1603 and higher) are supported.

And according to [this](#) document CG is supposed to be running if you see “Credential Guard” next to the *Device Guard Security Services configured* field:

Review Windows Defender Credential Guard performance

Is Windows Defender Credential Guard running?

You can view System Information to check that Windows Defender Credential Guard is running on a PC.

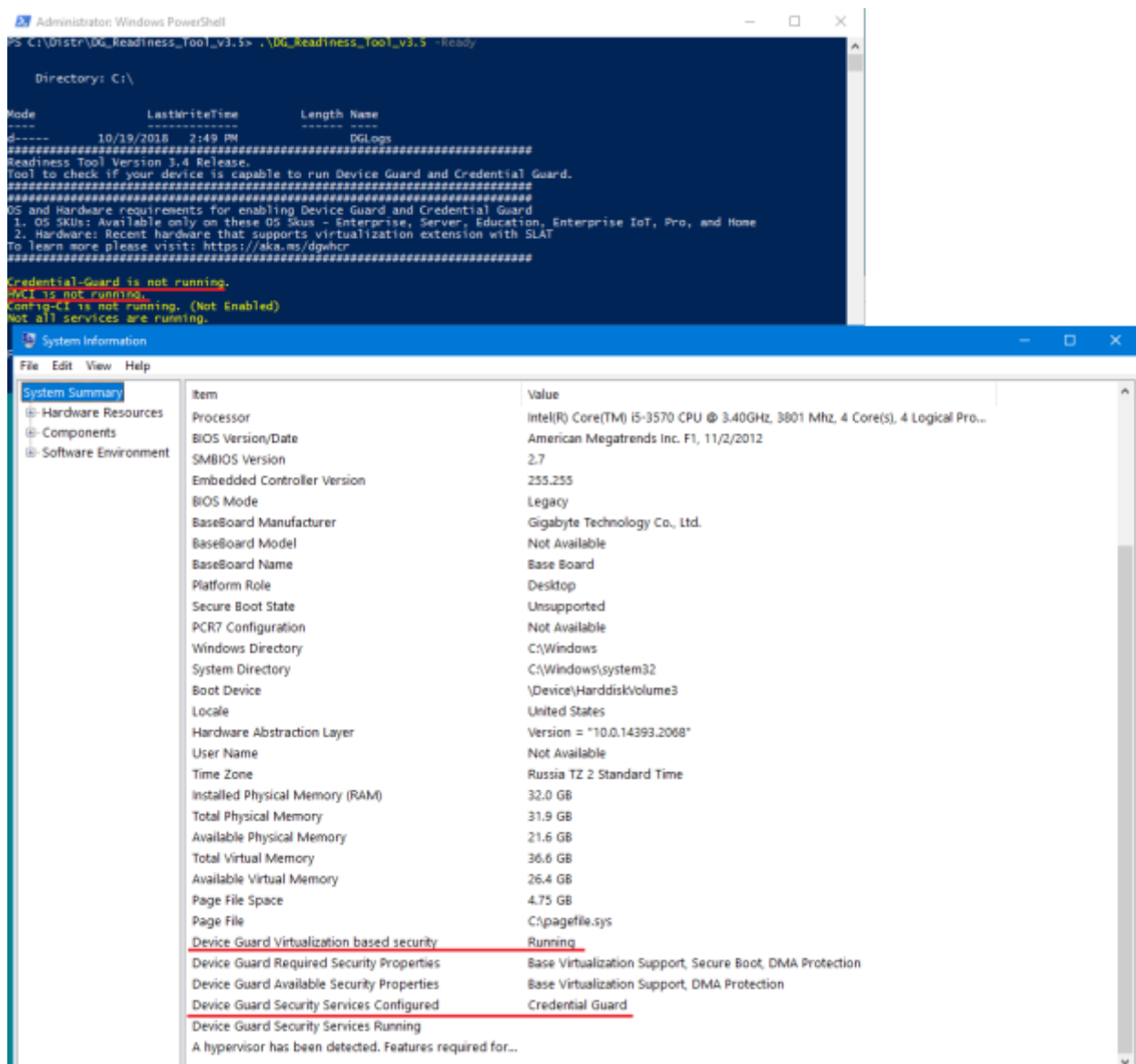
1. Click **Start**, type **msinfo32.exe**, and then click **System Information**.
2. Click **System Summary**.
3. Confirm that **Credential Guard** is shown next to **Virtualization-based security Services Configured**.

Here's an example:

Property	Value
Virtualization-based security	Running
Virtualization-based security Required Security Properties	Base Virtualization Support, Secure Boot, DMA Protection
Virtualization-based security Available Security Properties	Base Virtualization Support, Secure Boot, DMA Protection, UEFI Code Integrity
Virtualization-based security Services Configured	Credential Guard, Hypervisor enforced Code Integrity
Virtualization-based security Services Running	

But DG_Readiness_Tool shows that CG is not running in this case, as well as in the next one:

if I enable Credential Guard on a physical machine it seems to be running when checked using msinfo32.exe but NOT running if checked by DG_Readiness tool:



This leads me to the most basic question: how can you be sure CG is running? Most posts and videos regarding CG on the Internet shows the ms32info.exe's output (as illustrated above) as the proof the CG is running. As you've just seen CG may be actually not working in some cases even when *Device Guard Virtualization based security* displays Running and *Device Guard Services Configured* displays Credential Guard. As of this writing I don't have the answer to this question yet. Once I get it I'll post the explanation.

Update: if the *Device Guard Security Services Configured* displays Credential Guard next to it then it's enough to be sure the CG is running, regardless of the state of Device Guard Virtualization based security. *DG_Readiness_Tool* displays the state of CG incorrectly.

It means the CG is really enabled on SQL1.

3) The final optional step – you may download and apply Windows 10 Security baselines to user workstations (Tier2\Devices) – here are the links to some Windows 10 Security baselines:

<https://blogs.technet.microsoft.com/secguide/2016/10/17/security-baseline-for-windows-10-v1607-anniversary-edition-and-windows-server-2016/>

<https://blogs.technet.microsoft.com/secguide/2018/10/01/security-baseline-draft-for-windows-10-v1809-and-windows-server-2019/>

By the way: the latest security baseline changes the Credential Manager's default setting from *Secure Boot and DMA protection* to *Secure Boot* only:

Policy Setting	MSFT Win10 v1809-RSS FINAL	MSFT Win10 v1809-RSS DRAFT	MSFT Win10 v1809-RSS DRAFT	MSFT Win10 v1809-RSS DRAFT	MSFT Win10 v1809-RSS DRAFT	MSFT Win10 v1809-RSS DRAFT	MSFT Win10 v1809-RSS DRAFT
1. Allow Windows Update	On	On	On	On	On	On	On
2. Configure Windows Firewall	On	On	On	On	On	On	On
3. Windows Defender	On	On	On	On	On	On	On
4. Windows Defender Security Center	On	On	On	On	On	On	On
5. Windows Defender Security Center	On	On	On	On	On	On	On
6. Windows Defender Security Center	On	On	On	On	On	On	On
7. Windows Defender Security Center	On	On	On	On	On	On	On
8. Windows Defender Security Center	On	On	On	On	On	On	On
9. Windows Defender Security Center	On	On	On	On	On	On	On
10. Windows Defender Security Center	On	On	On	On	On	On	On
11. Windows Defender Security Center	On	On	On	On	On	On	On
12. Windows Defender Security Center	On	On	On	On	On	On	On
13. Windows Defender Security Center	On	On	On	On	On	On	On
14. Windows Defender Security Center	On	On	On	On	On	On	On
15. Windows Defender Security Center	On	On	On	On	On	On	On
16. Windows Defender Security Center	On	On	On	On	On	On	On
17. Windows Defender Security Center	On	On	On	On	On	On	On
18. Windows Defender Security Center	On	On	On	On	On	On	On
19. Windows Defender Security Center	On	On	On	On	On	On	On
20. Windows Defender Security Center	On	On	On	On	On	On	On
21. Windows Defender Security Center	On	On	On	On	On	On	On
22. Windows Defender Security Center	On	On	On	On	On	On	On
23. Windows Defender Security Center	On	On	On	On	On	On	On
24. Windows Defender Security Center	On	On	On	On	On	On	On
25. Windows Defender Security Center	On	On	On	On	On	On	On
26. Windows Defender Security Center	On	On	On	On	On	On	On
27. Windows Defender Security Center	On	On	On	On	On	On	On
28. Windows Defender Security Center	On	On	On	On	On	On	On
29. Windows Defender Security Center	On	On	On	On	On	On	On
30. Windows Defender Security Center	On	On	On	On	On	On	On
31. Windows Defender Security Center	On	On	On	On	On	On	On
32. Windows Defender Security Center	On	On	On	On	On	On	On
33. Windows Defender Security Center	On	On	On	On	On	On	On
34. Windows Defender Security Center	On	On	On	On	On	On	On
35. Windows Defender Security Center	On	On	On	On	On	On	On
36. Windows Defender Security Center	On	On	On	On	On	On	On
37. Windows Defender Security Center	On	On	On	On	On	On	On
38. Windows Defender Security Center	On	On	On	On	On	On	On
39. Windows Defender Security Center	On	On	On	On	On	On	On
40. Windows Defender Security Center	On	On	On	On	On	On	On
41. Windows Defender Security Center	On	On	On	On	On	On	On
42. Windows Defender Security Center	On	On	On	On	On	On	On

Summary:

Odds are the “tiered” Active Directory administration will soon become a new baseline for all new and existing deployments: it really does help reduce the risks of credentials theft. Privileged Access Workstations take the art of protecting hashes of domain high privileged accounts to the next level but administrators must be aware of some discrepancies in the paw documentation and be ready to conduct thorough testing before putting them into production.

Additional LSA protection and with Mimikatz example are described in [Part 4](#)