# Implementing Privileged Access Workstation – part 2

michaelfirsov.wordpress.com/implementing-privileged-access-workstation-part-2

October 25, 2018

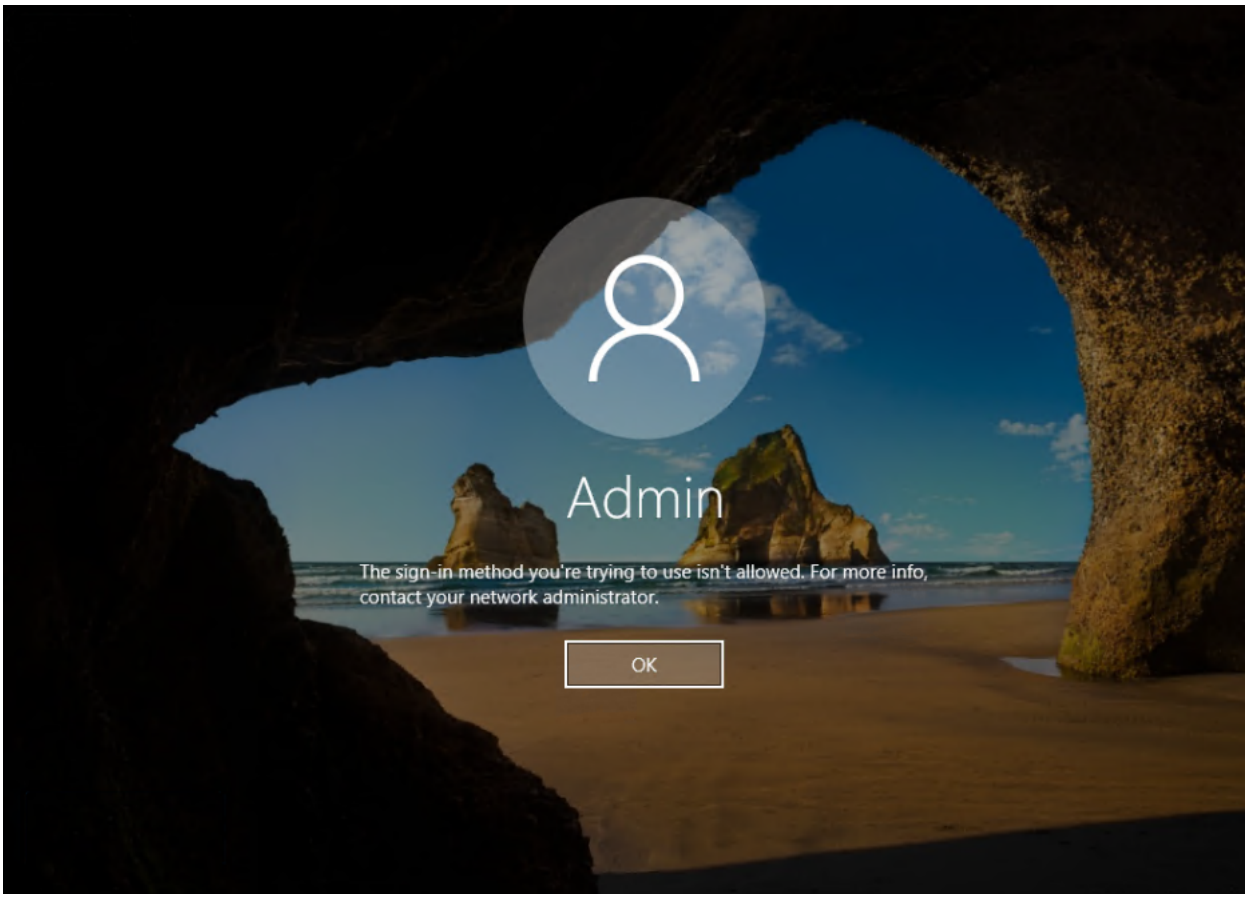
Part1

Now let's try to test how all these settings work on the secured workstation (PAW) – I will install Windows 10 Enterprise into the new VM, add it to the TestENTERPRISE domain (under PAW host name) and try to log on to it. Later we'll check if a tier0 account will be able to log on to an ordinary workstation.

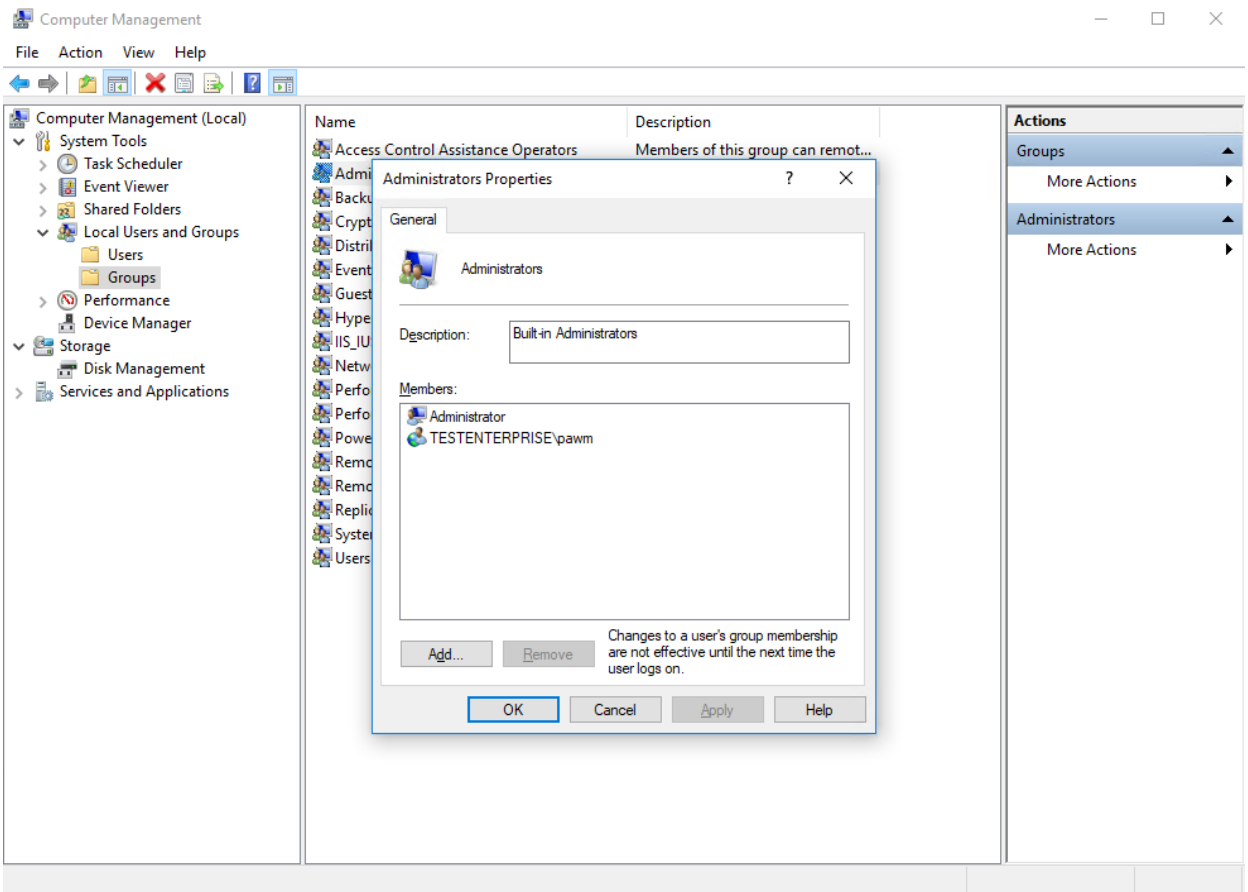
**Test 1**: Once the PAW has been added to the domain I want to check who will have the ability to log on to the PAW:

1) Log on under *Admin* user account – this **local** user account is a member of the local Administrators group but is NOT a member of the TestENTERPRISE\PAWMaintenance group and thus- as was written in part1 – should NOT be able to log on locally because

" the membership of the local Administrators group on paw devices is configured by the respective gpo setting which states that only the *LOCAL Administrator* and the *TestENTERPRISE\pawm* user accounts can be the members of the local Administrators group so in this case it means the *local built-in Administrator* (*PAW\Administrator*) and *TestENTERPRISE\pawm* user account WILL – theoretically! – have the right to log on to PAW locally. Practically it means that ONLY the member of the PAWMaintenance domain group – *TestENTERPRISE\pawm* – will have access because the built-in *PAW\Administrato*r is disabled by default!":

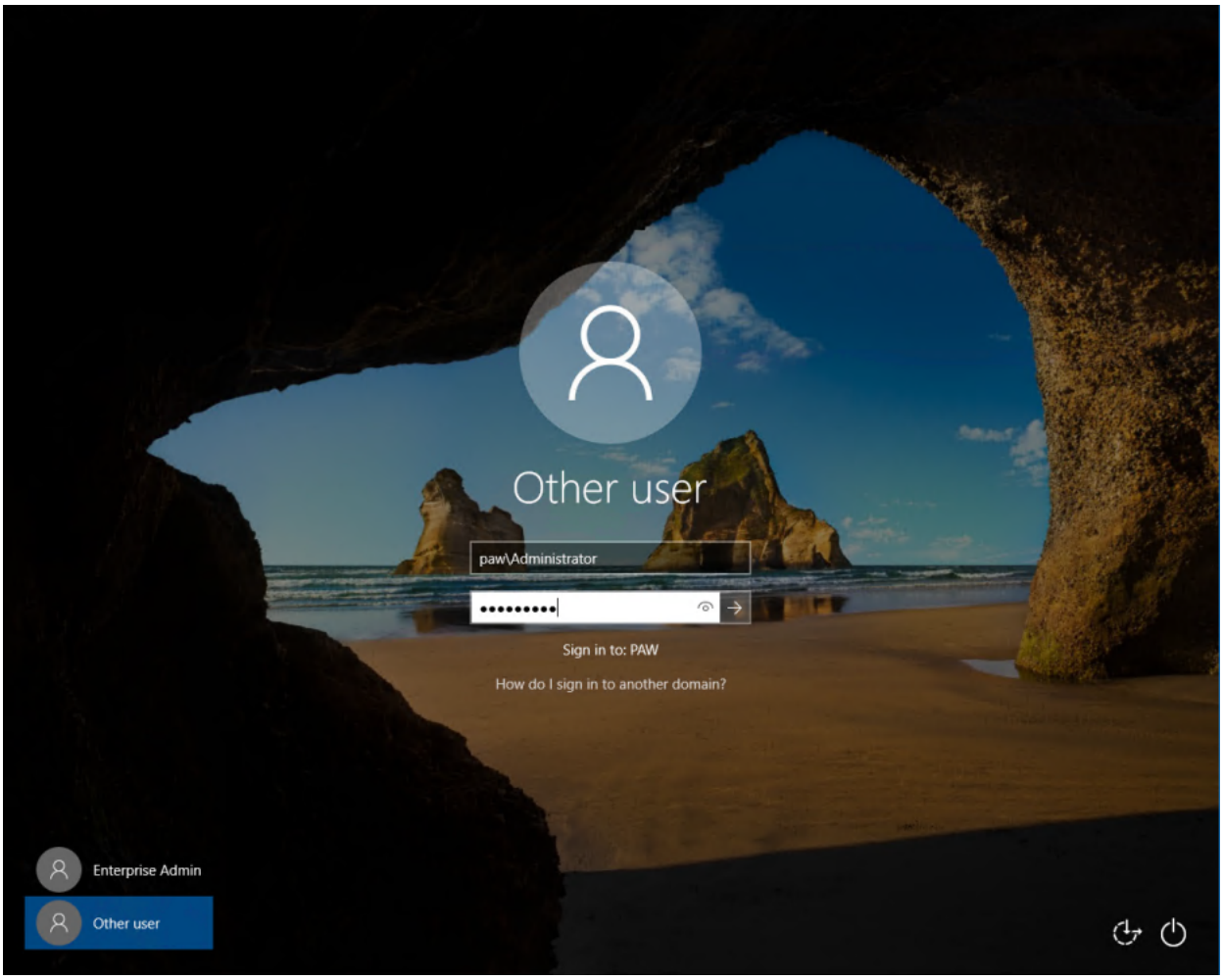


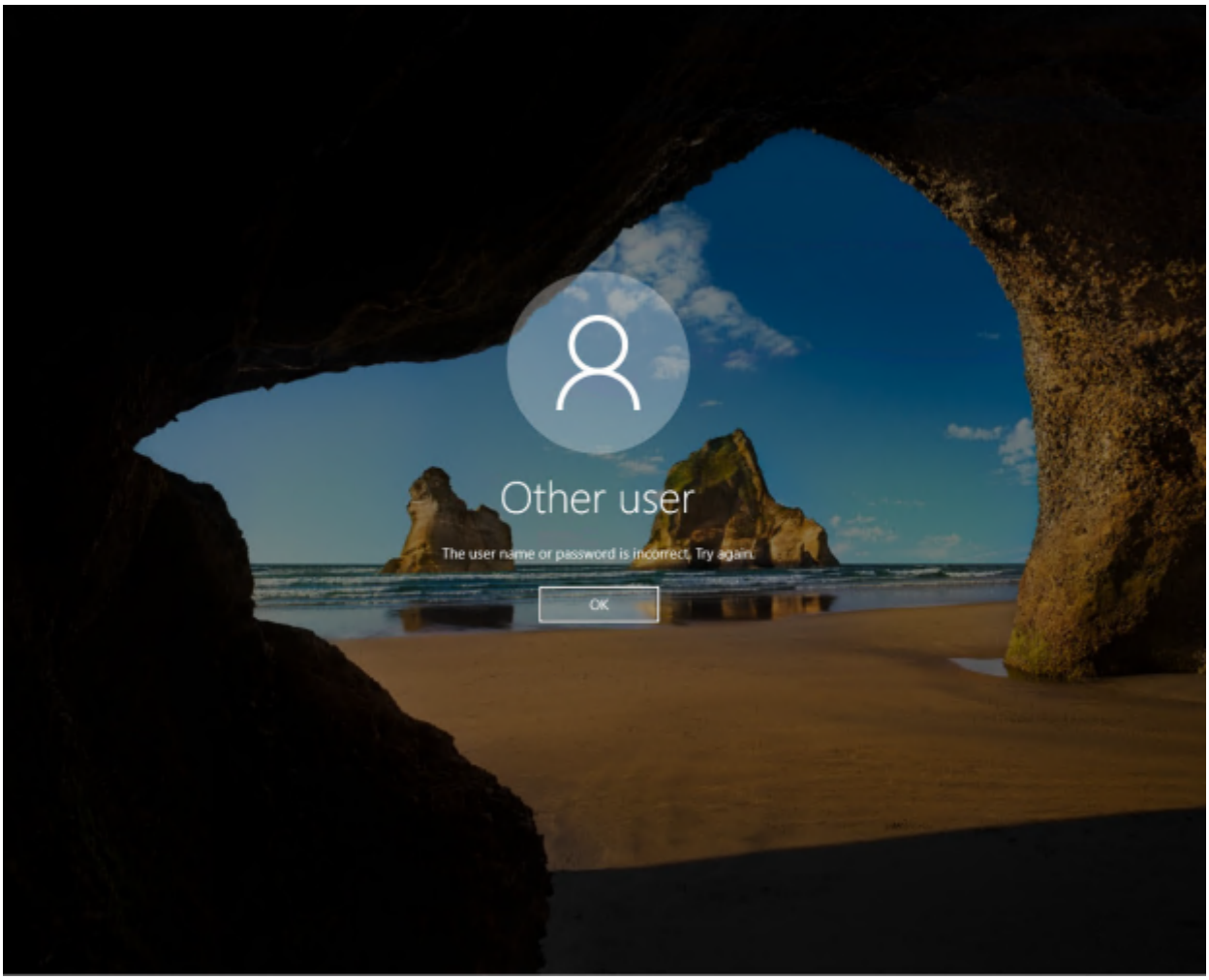

That's correct – local *Admin* user account must have been removed from the local Administrators group once the policies have been applied.



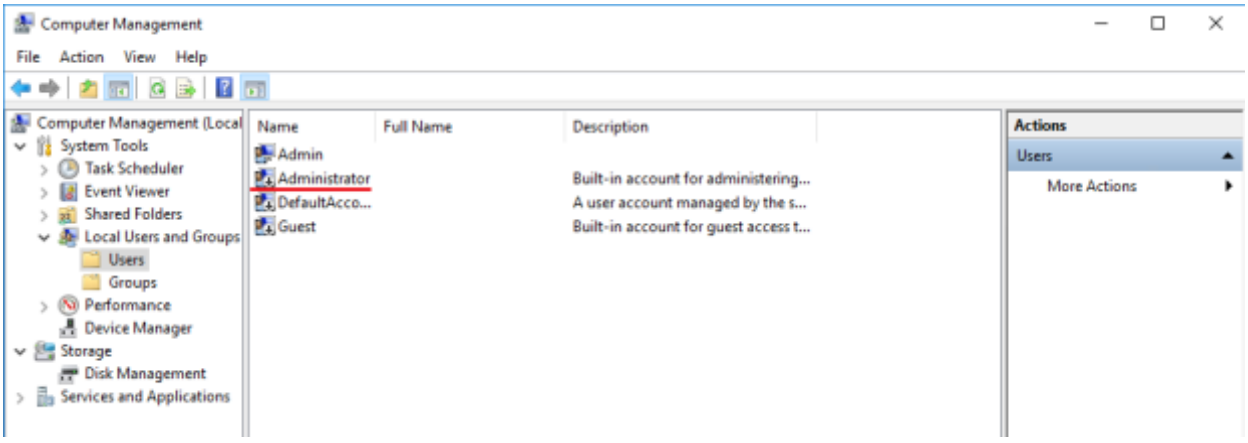

Advertisements

Report this adPrivacy
2) Local *Administrator*:





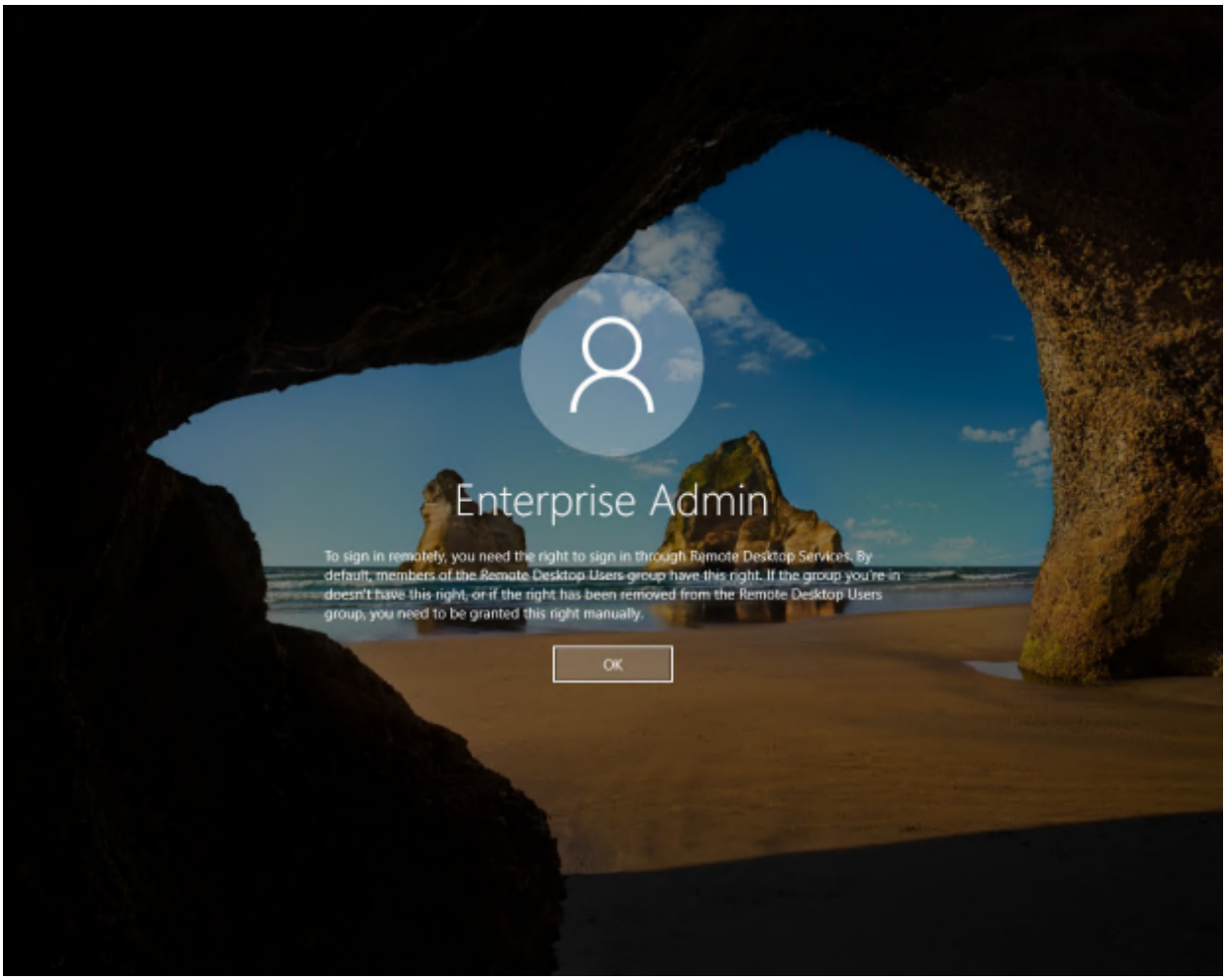

That's correct – local *Administrator* must be disabled by default.



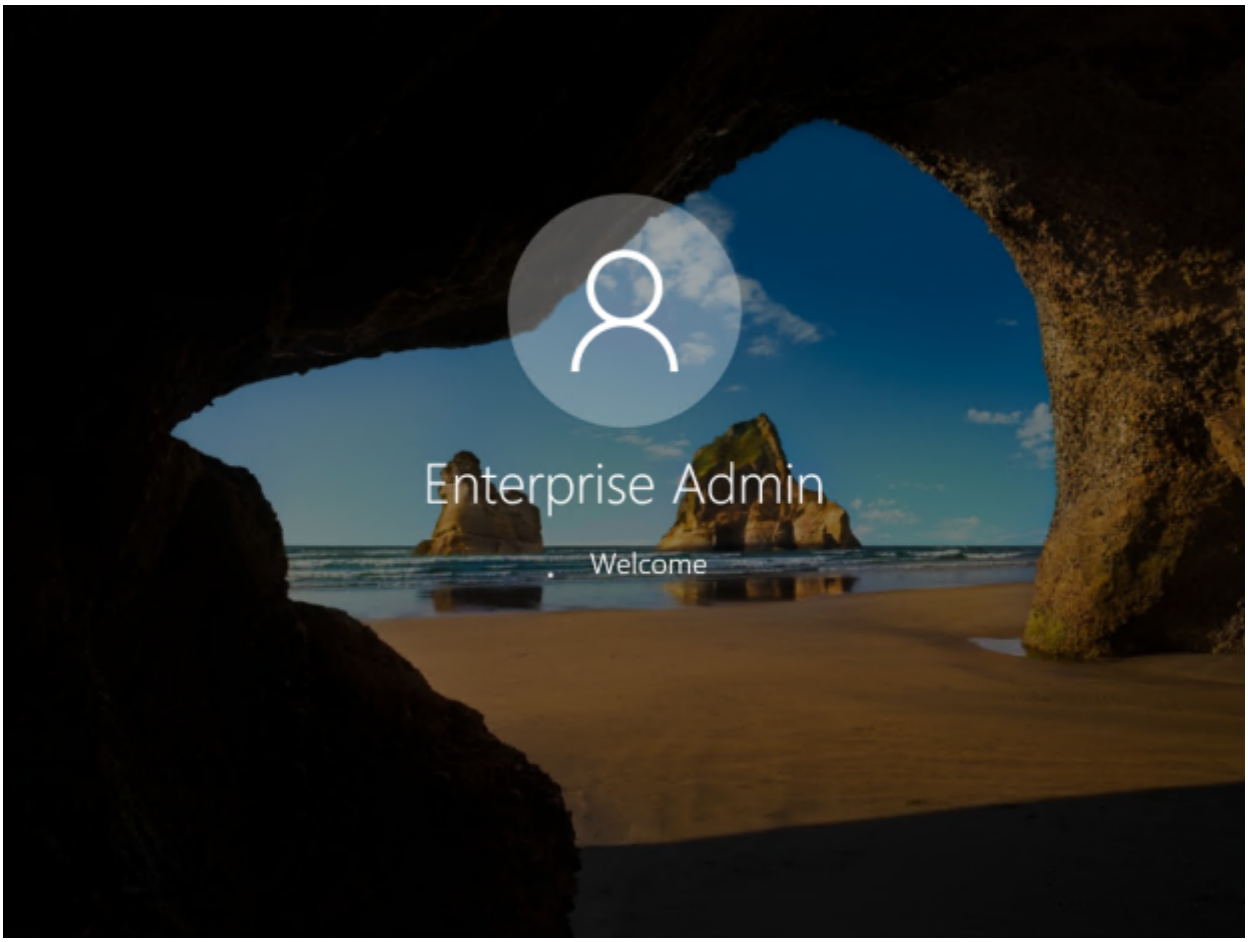



3) *TestENTERPRISE\EntAdmin* – Tier0 user account:

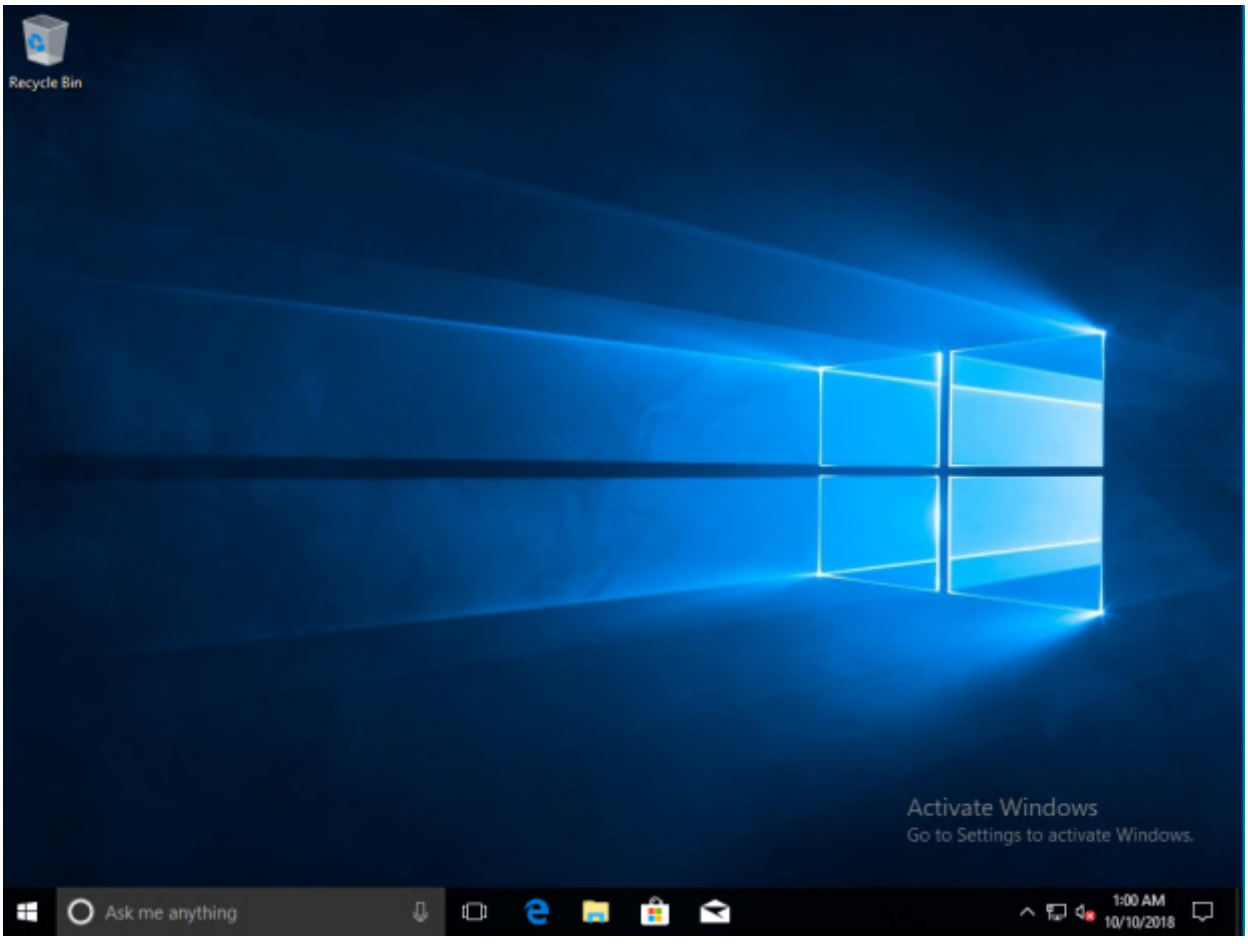
Although it's not a supported scenario, my paw is the virtual machine to which I connect by default using Hyper-V Session Enhanced mode, and providing that Domain Admins are no longer the member of  the local Administrators group the following error would arise should I try to connect to the PAW vm:



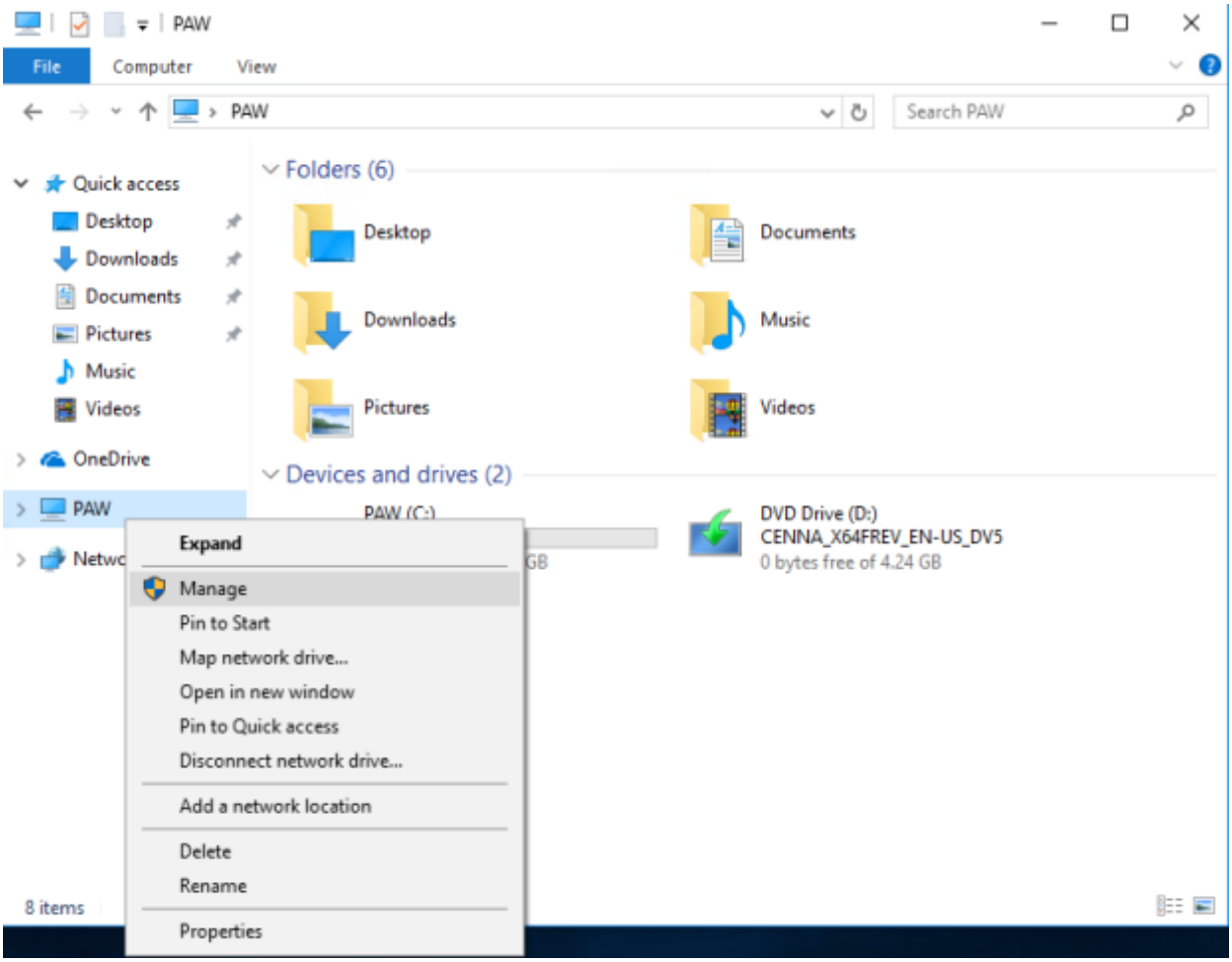

To connect to the paw vm I need either to turn the enchanced mode off in the Hyper-V settings or make several unsuccessfull attempts in the enchanced mode: after several failed attempts Hyper-V Manager will automatically switch to the ordinary mode. Once in this mode *EntAdmin* does log on successfully (if fact it means local logon):



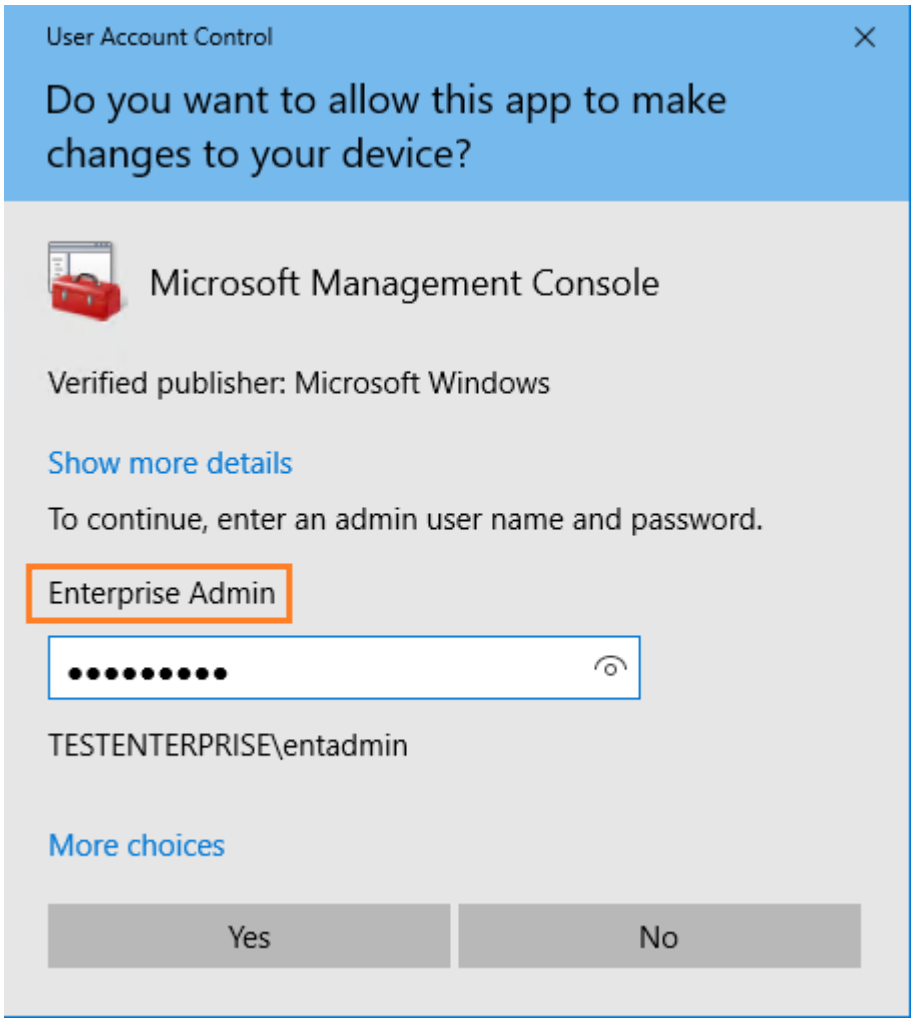


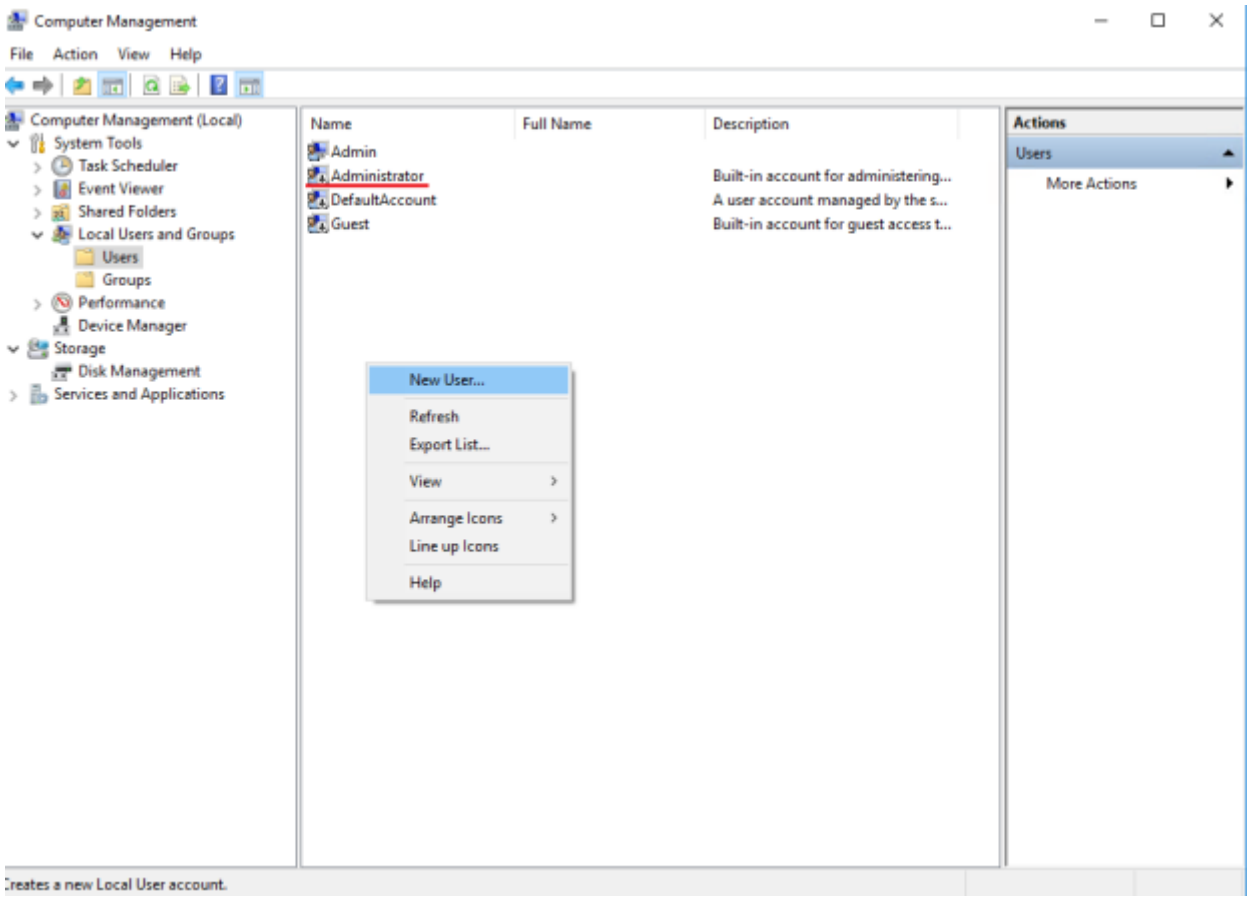



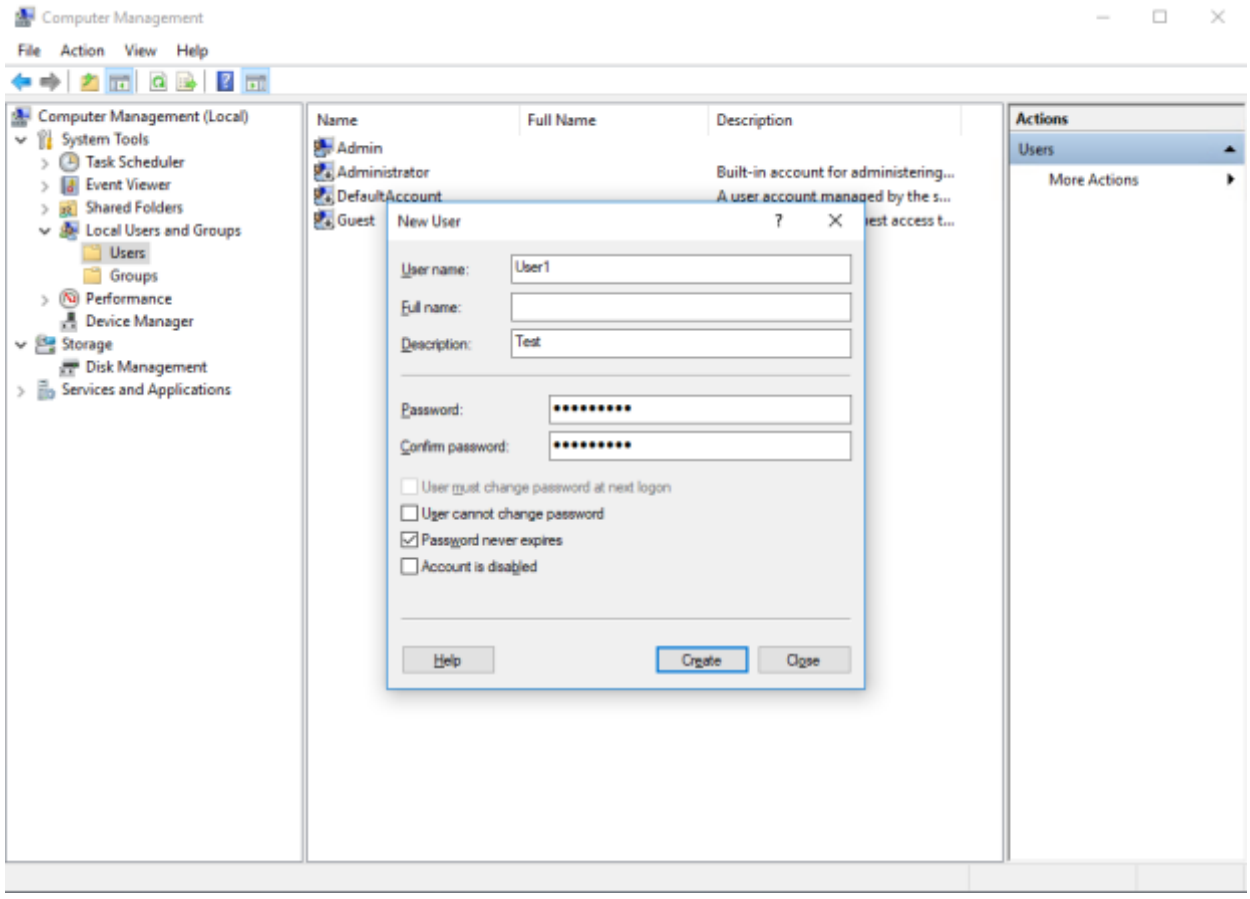
Now if I try to run some program as *Administrator* or this program/mmc requires administrative credentials I should get the dialog window asking for the *administrator*'s credentials:

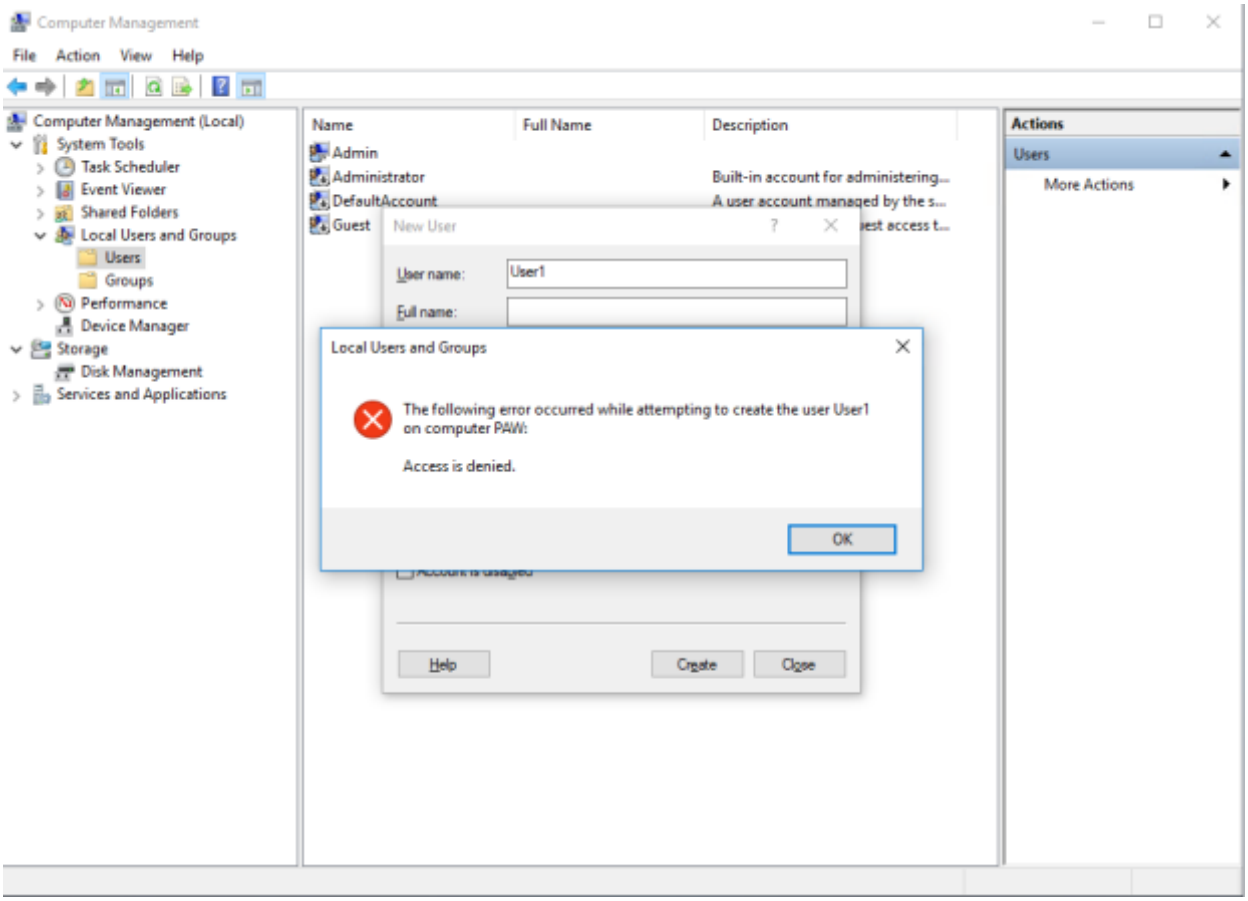



If I enter here *EntAdmin*'s password the console will still open but will not allow to do any administrative tasks:




Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Full Name
Description
Admin
Administrator
Built-in account for administering...
DefaultAccount
A user account managed by the s...
Guest
Built-in account for guest access t...
New User...
Refresh
Export List...
View
Arrange Icons
Line up Icons
Help
Actions
Users
More Actions
Creates a new Local User account.

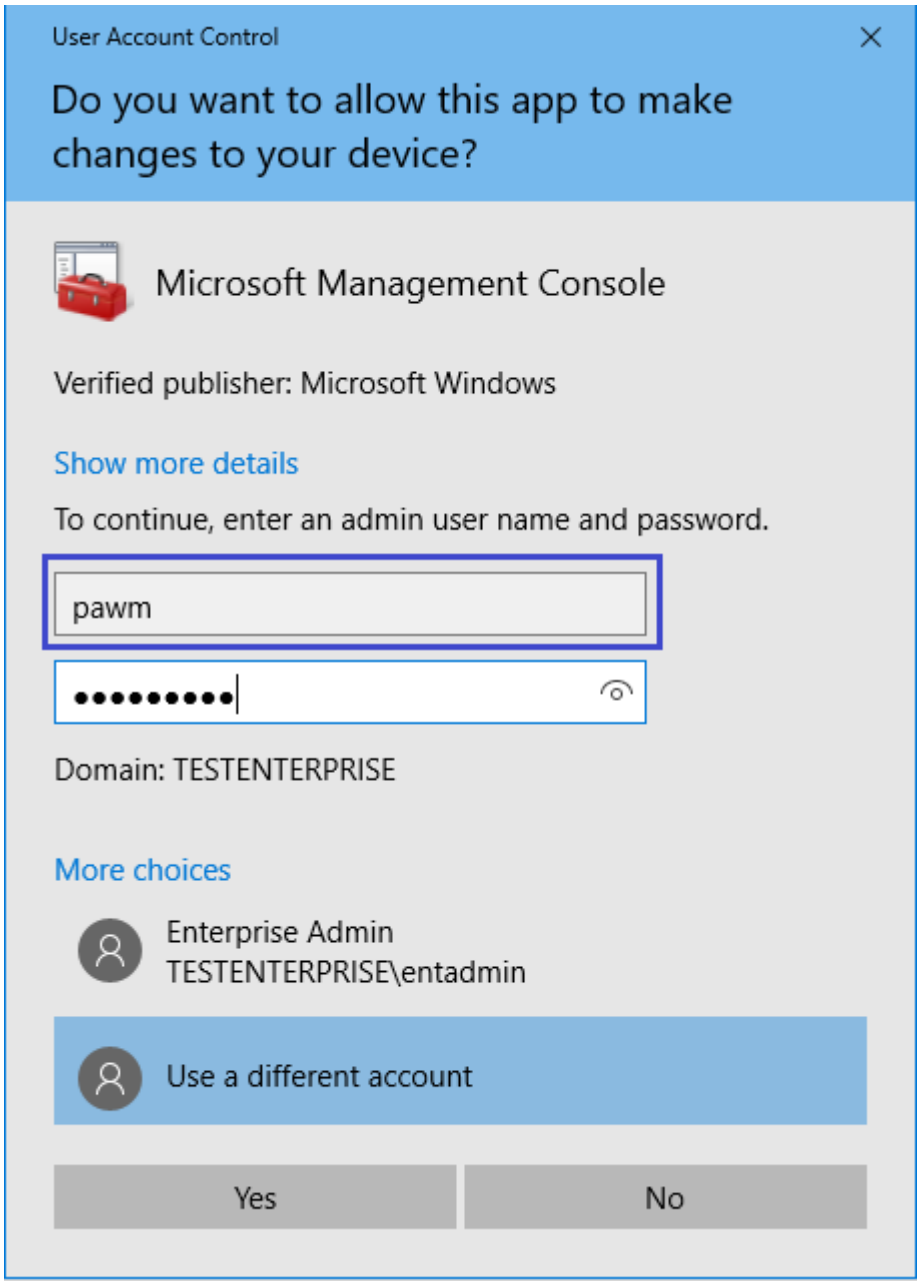

Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Full Name
Description
Admin
Administrator
Built-in account for administering...
DefaultAccount
A user account managed by the s...
Guest
New User
User name:
User1
Full name:
Description:
Test
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
Help
Create
Close
Actions
Users
More Actions

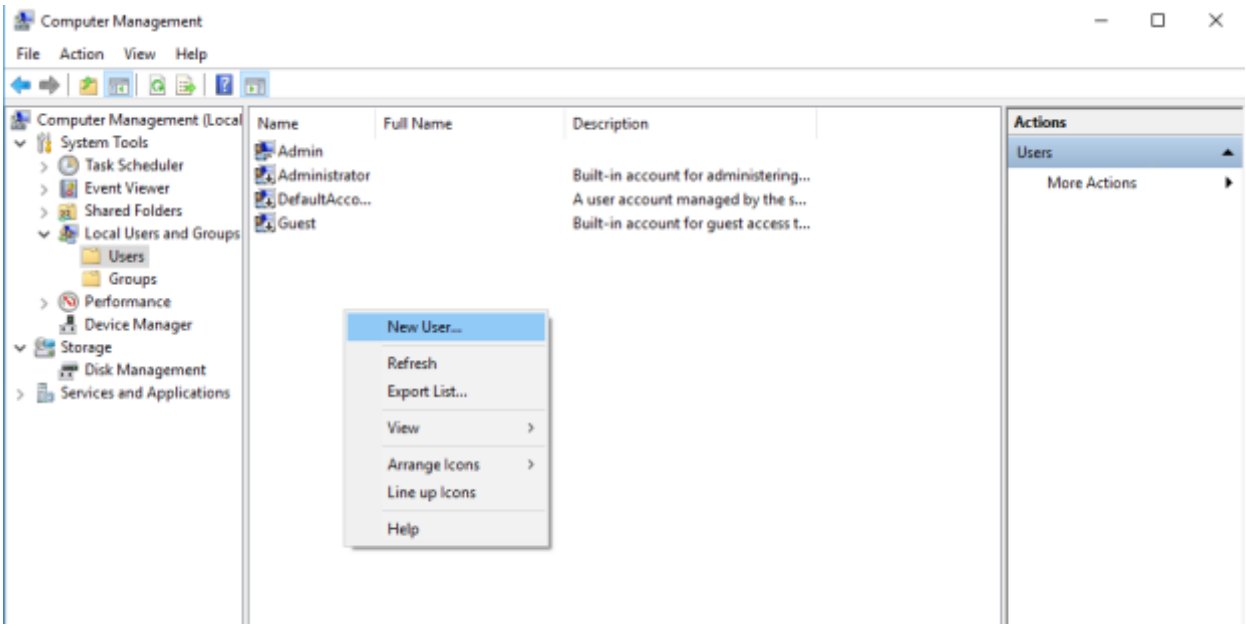


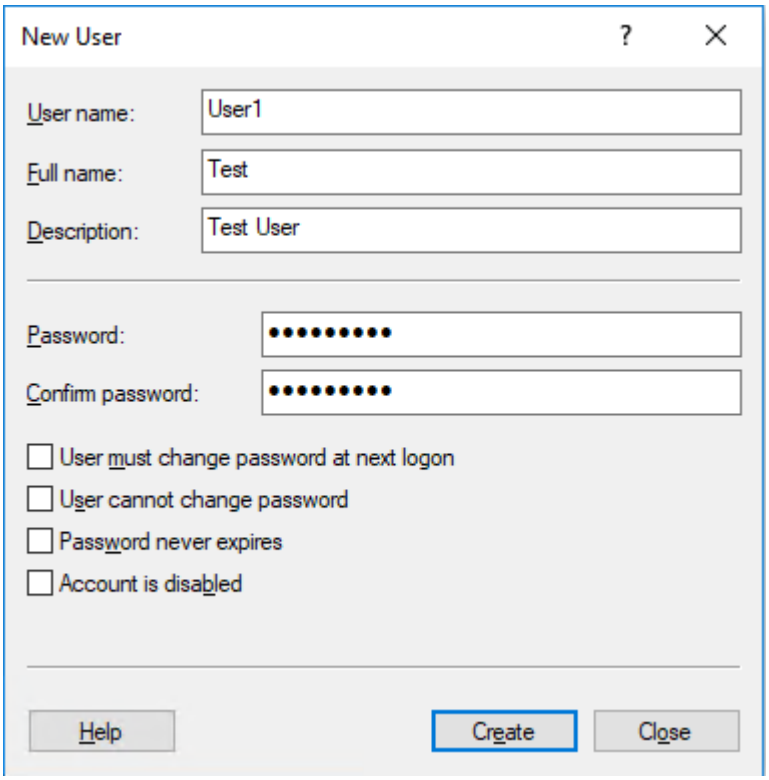


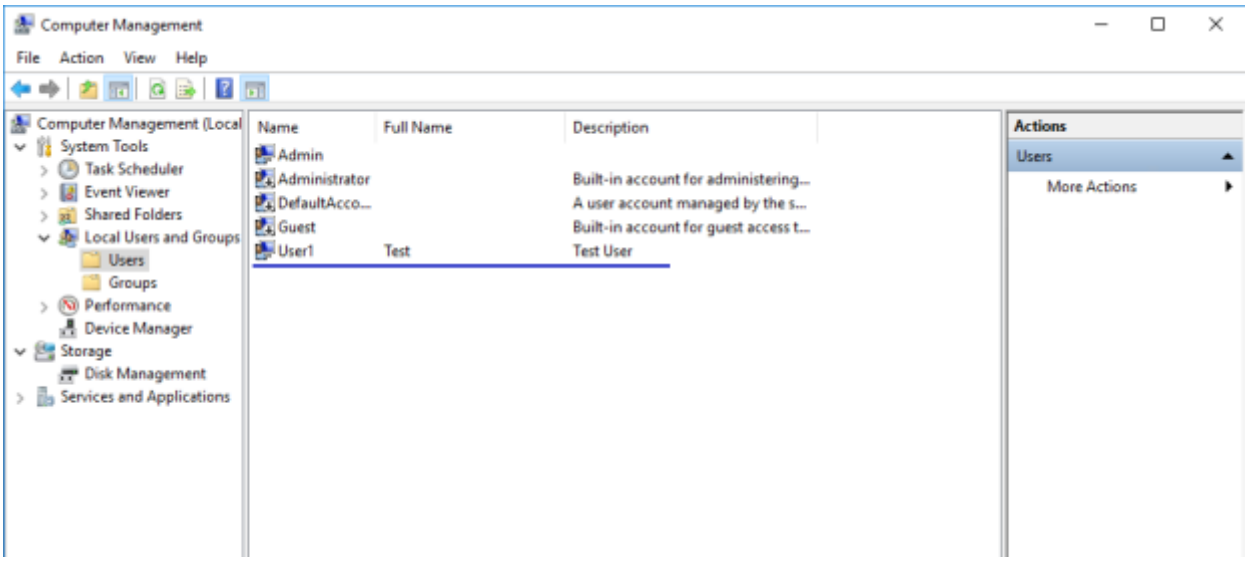

This confirms *EntAdmin* does not have administrative rights on the PAW – and this is one of the goals of the privilaged access workstations: tier0 user accounts should be used only for tier0 (and probably tier1) servers!

If I really wanted to add a new user I would have used the *TestENTERPRISE\pawm*'s creadentials instead:


User Account Control
Do you want to allow this app to make changes to your device?
Microsoft Management Console
Verified publisher: Microsoft Windows
Show more details
To continue, enter an admin user name and password.
pawm
Domain: TESTENTERPRISE
More choices
Enterprise Admin
TESTENTERPRISE\entadmin
Use a different account
Yes
No

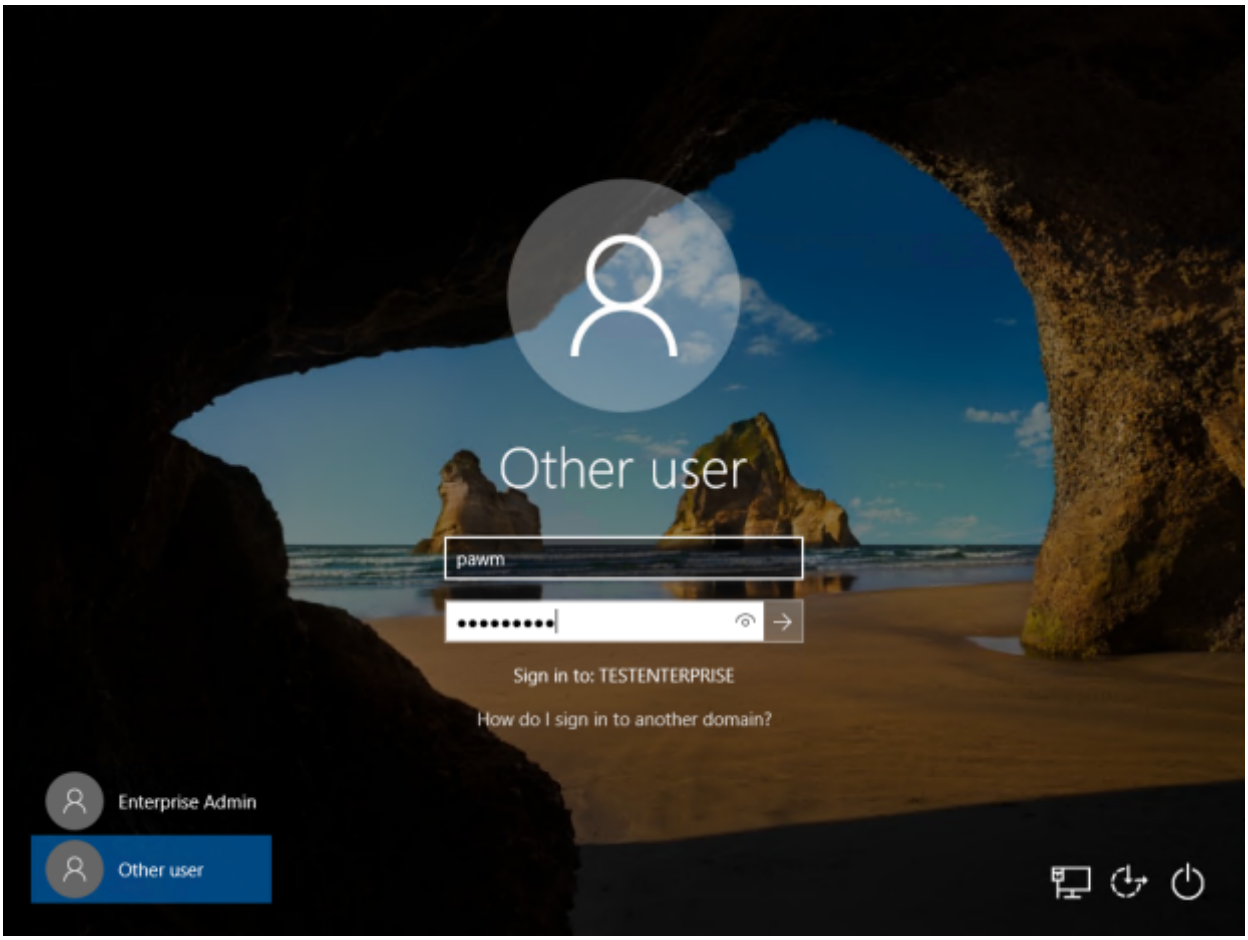

Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Full Name
Description
Admin
Administrator
Built-in account for administering...
DefaultAcco...
A user account managed by the s...
Guest
Built-in account for guest access t...
New User...
Refresh
Export List...
View
Arrange Icons
Line up Icons
Help
Actions
Users
More Actions

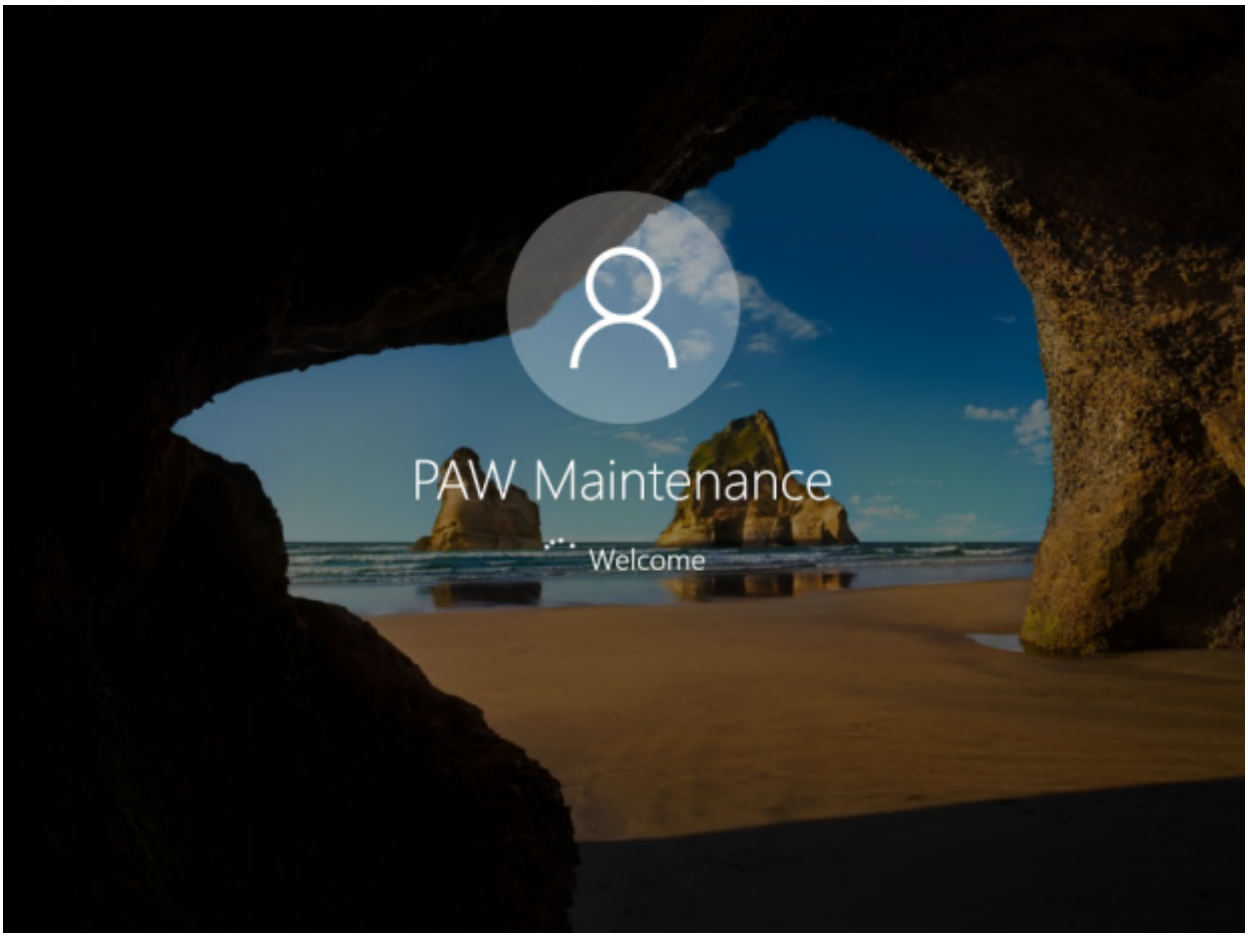


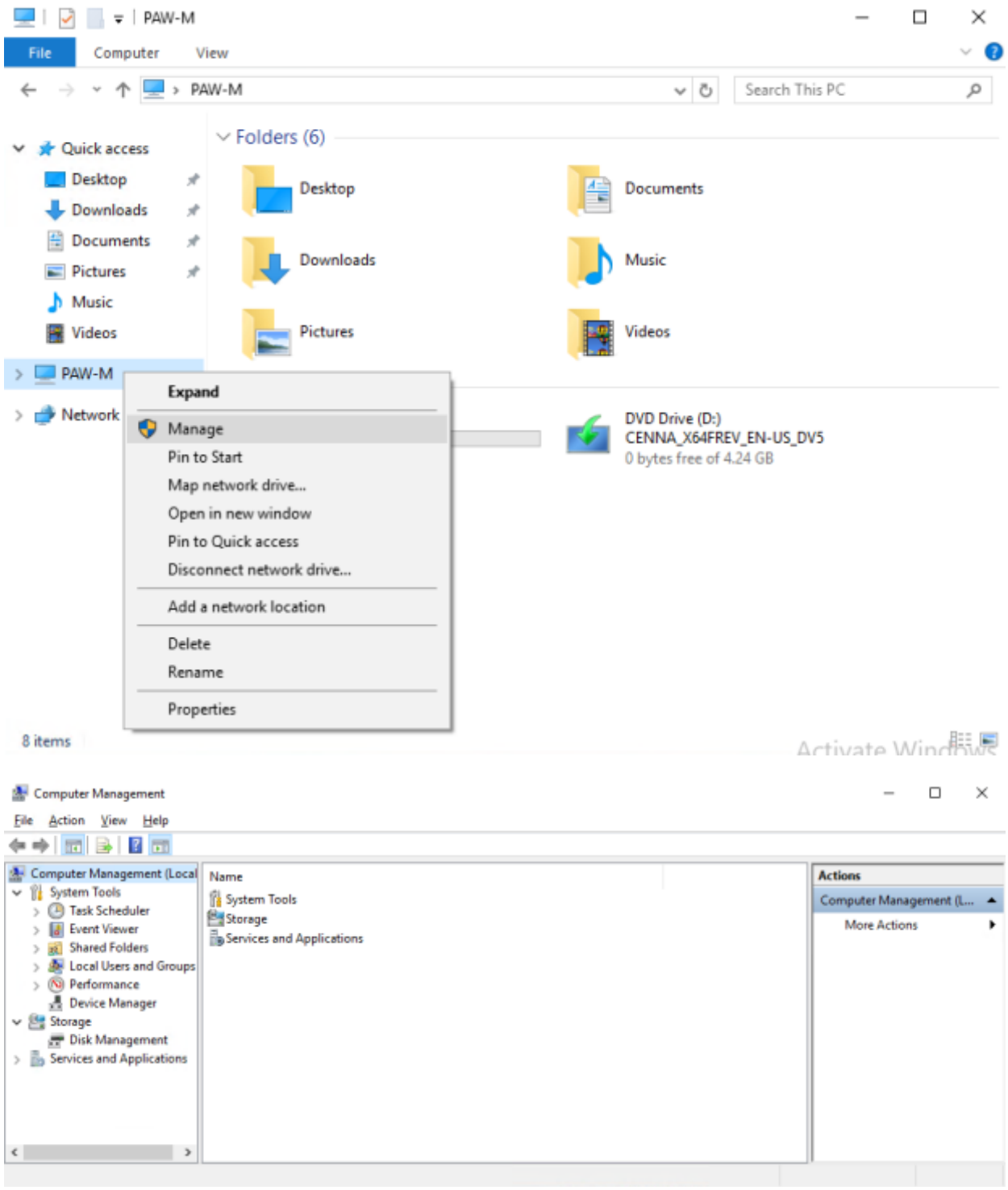



4) PAW Maintenance user account – *TestENTERPRISE\pawm*




No dialog window arises when starting Server Manager (I've renamed This Computer to PAW-**M** to reflect that the PAW maintenance user account is being used):

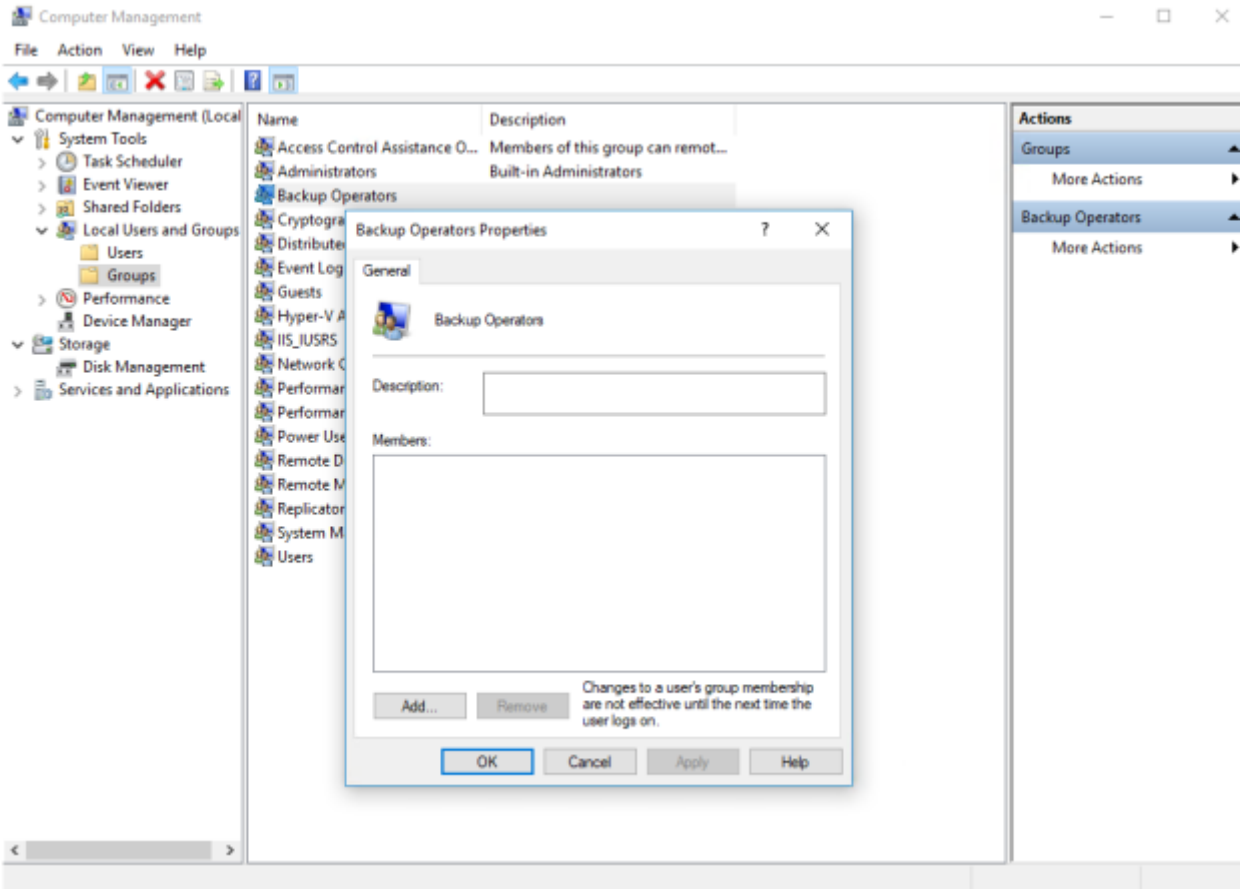




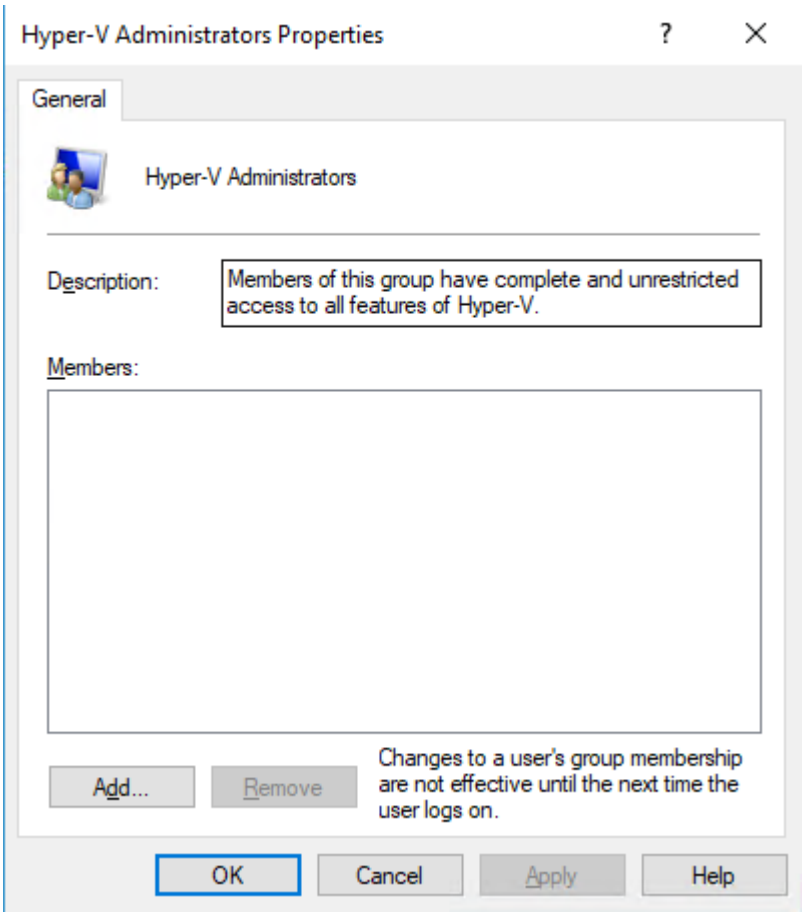

The result of **Allow account logon** user right testing: works as expected.

Test 2: Local group membership

All respective local groups must be empty according to the **PAWConfiguration-Computer** gpo – and they are really empty, for example, Backup Operators (except the membership of the local Administrators group – it was illustrated in 1)) :

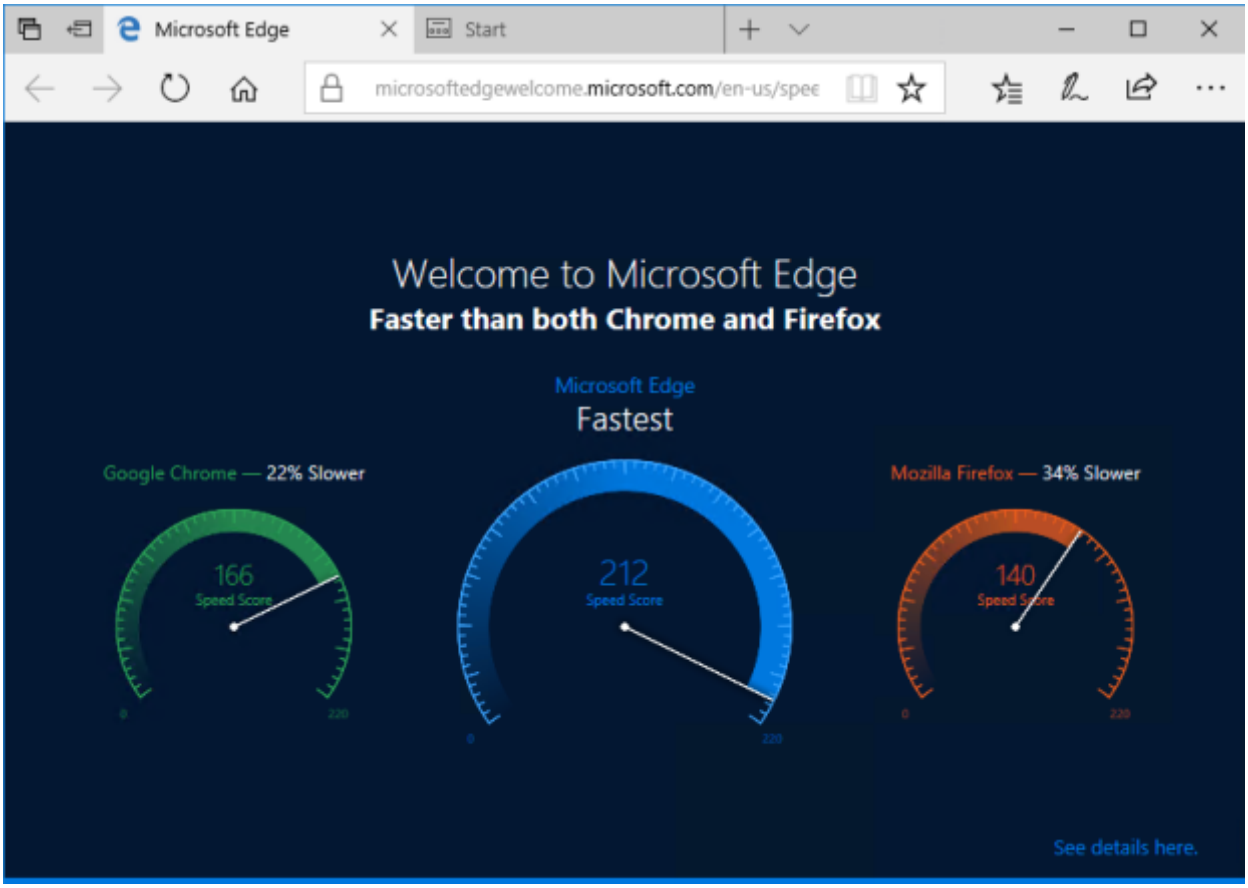


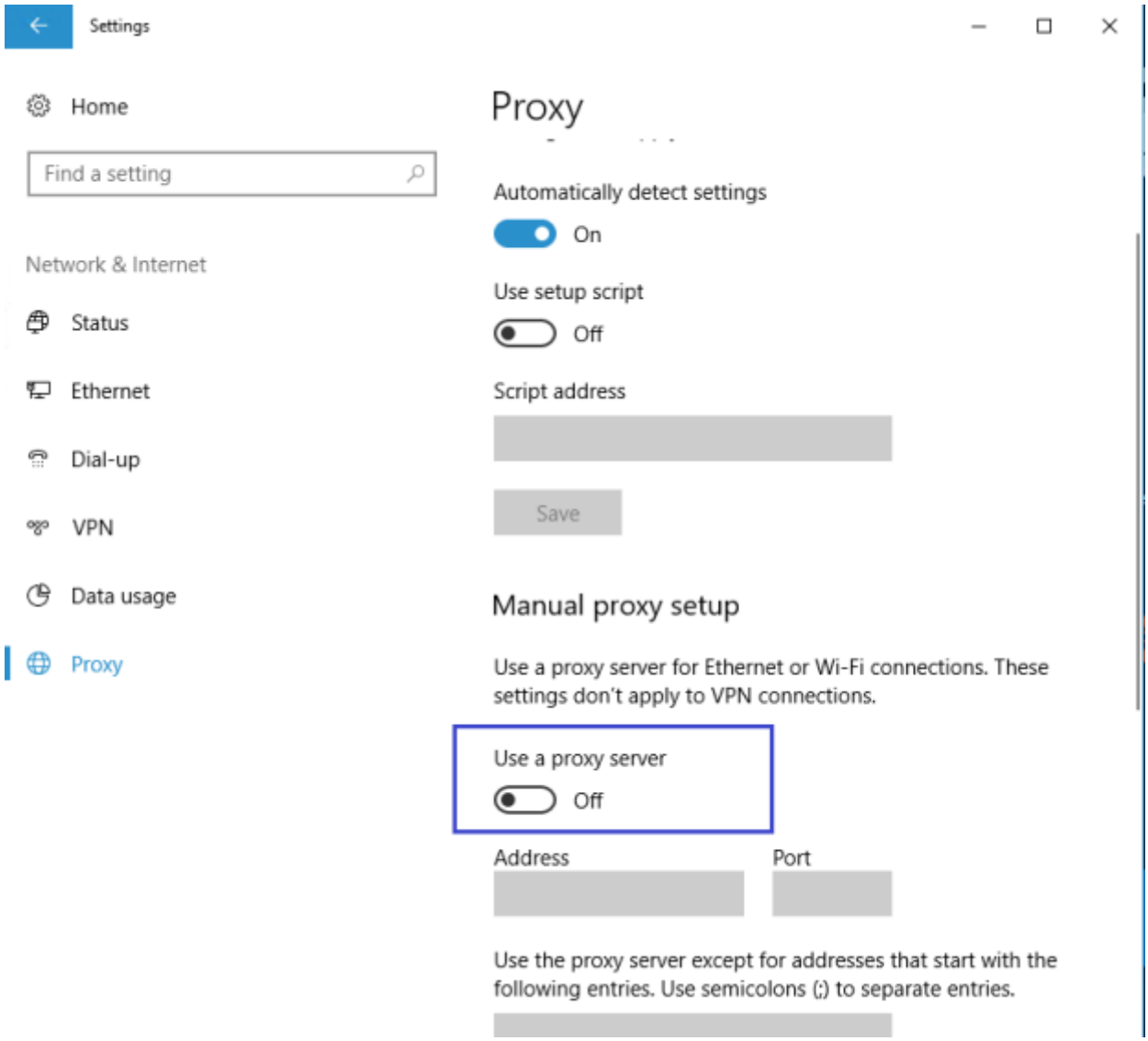

The only local group that can't be managed by gpo is Hyper-V Administrators because there's no such option in the drop-down list in the gpo. On my PAW it nevertheless is empty by default:



**Test 3** – Let's check who is permitted to browse the Internet:

1) PAWMaintenance – *TestENTERPRISE\pawm*

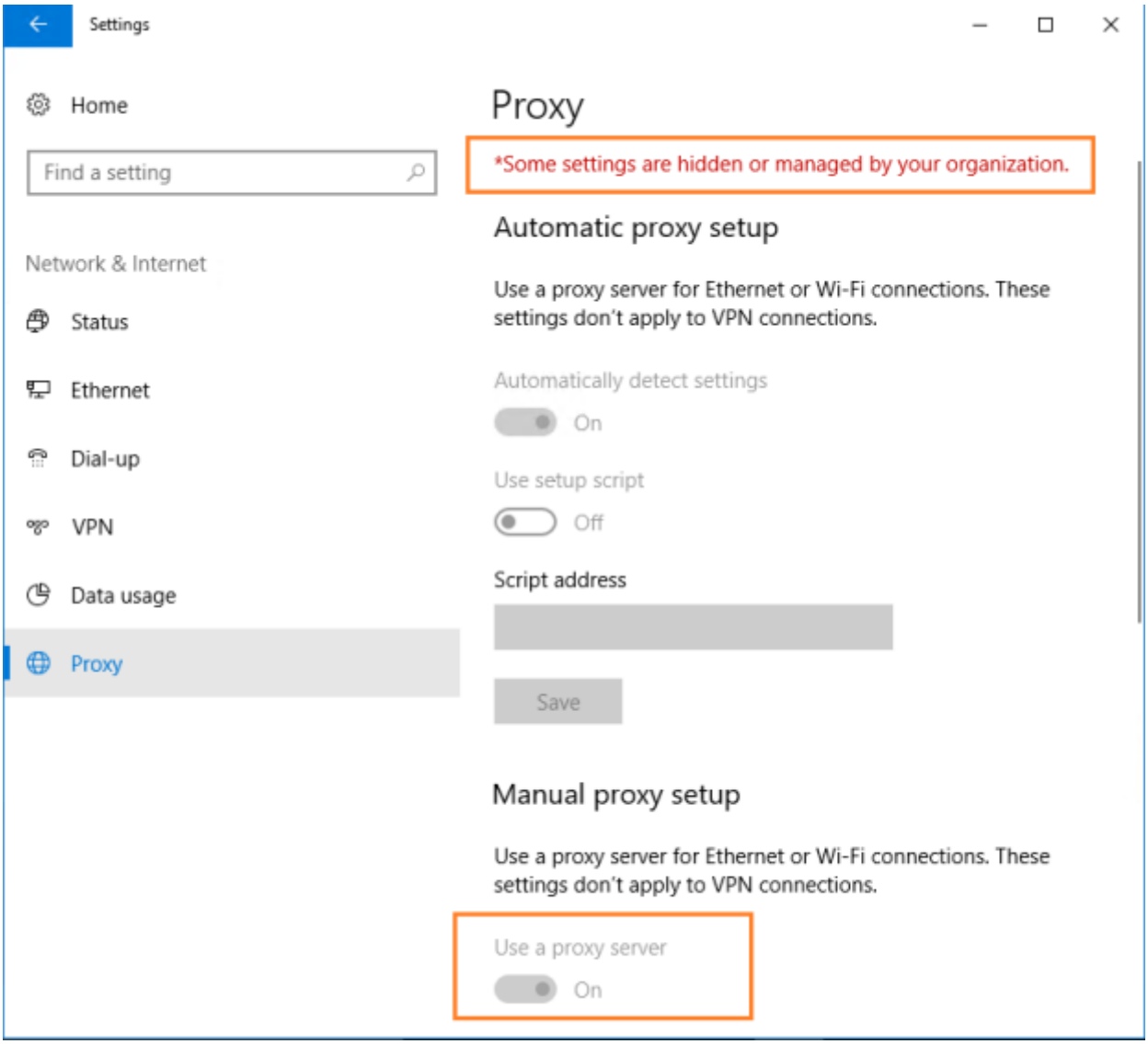


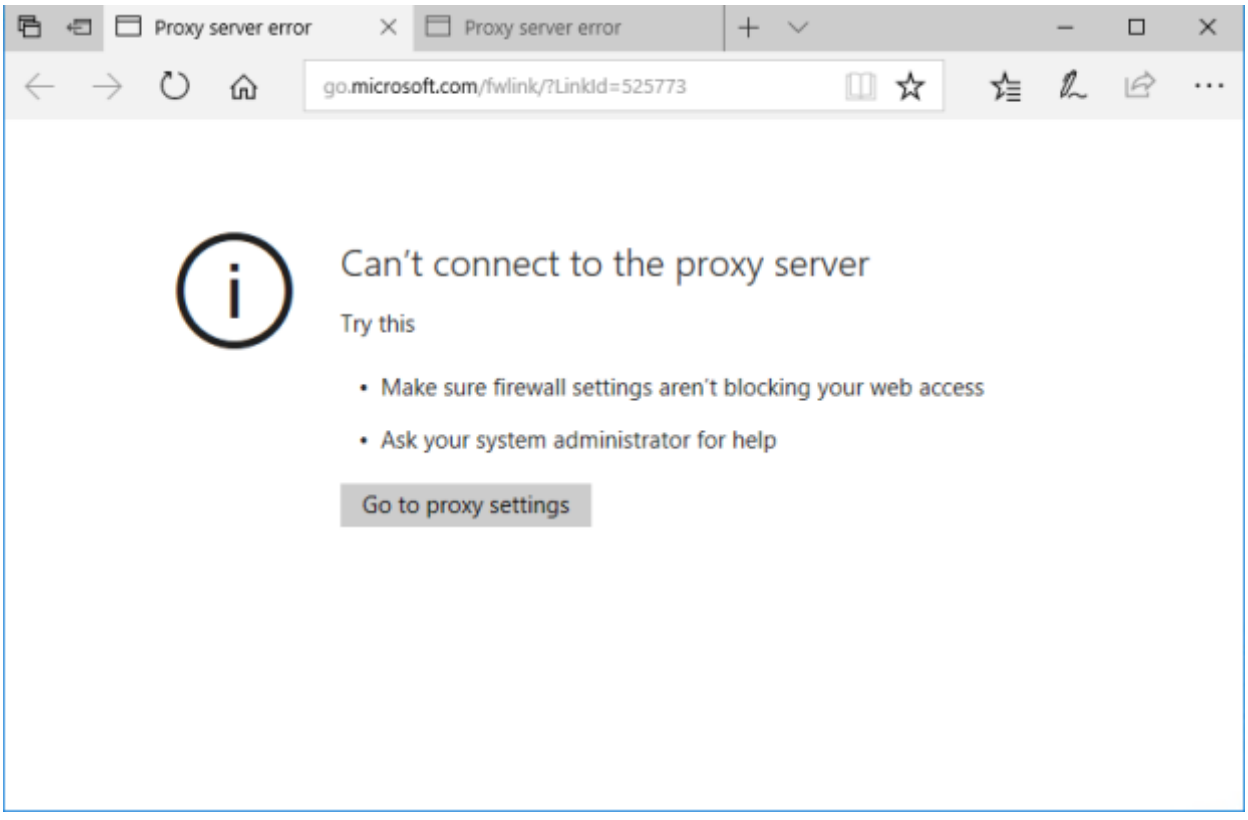





This is the expected result: paw maintenance user (*TestENTERPRISE\pawm*) account should browse the Internet if required: there're no policy settings which prevent Internet browsing.

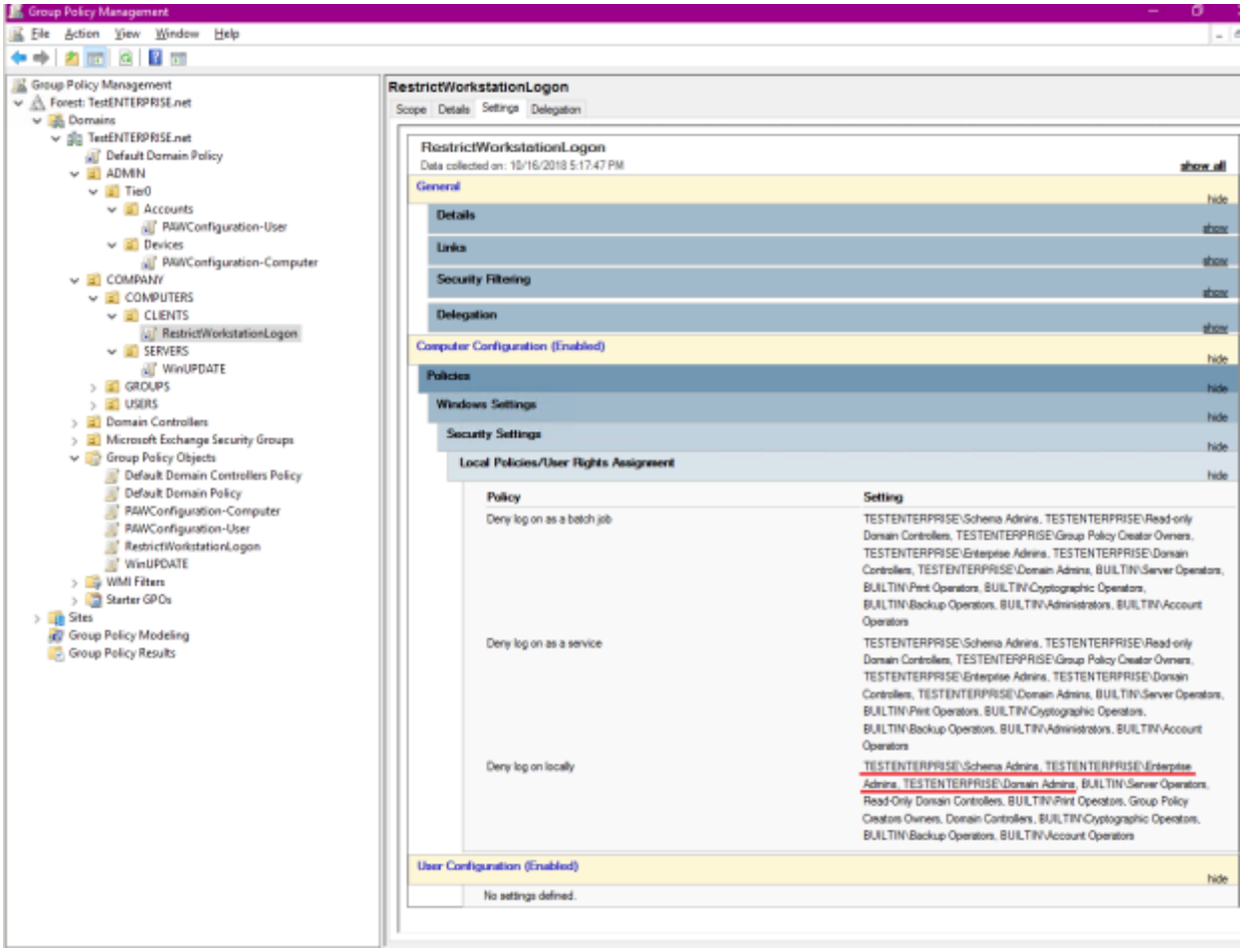
2) *EntAdmin* (Tier0 account)


Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Data usage
Proxy
Proxy
*Some settings are hidden or managed by your organization.
Automatic proxy setup
Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.
Automatically detect settings
On
Use setup script
Off
Script address
Save
Manual proxy setup
Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.
Use a proxy server
On

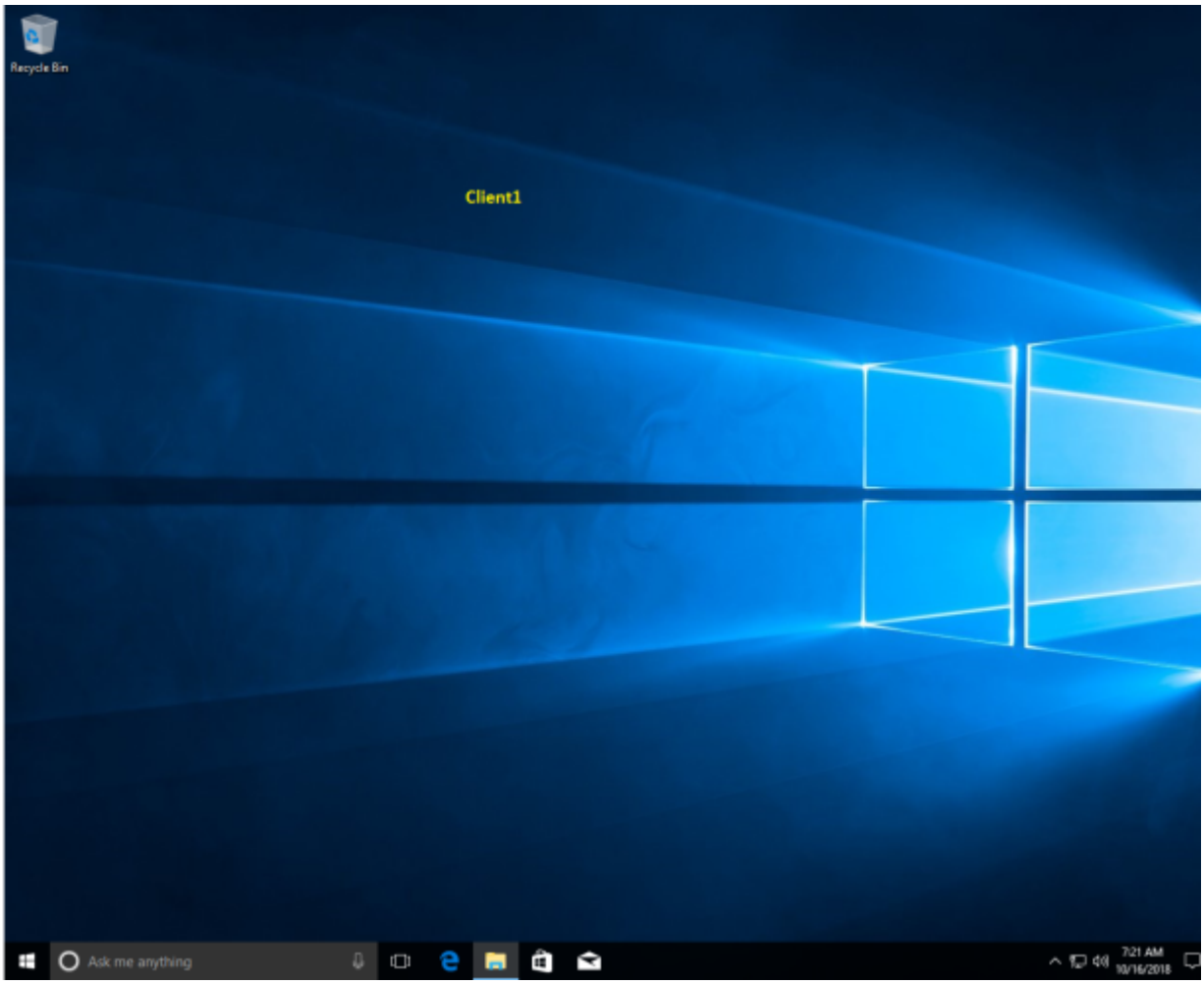

Proxy server error
Proxy server error
go.microsoft.com/fwlink/?LinkId=525773
Can't connect to the proxy server
Try this
• Make sure firewall settings aren't blocking your web access
• Ask your system administrator for help
Go to proxy settings

That's also correct: there are a couple of settings in the **PAWConfiguration-User** gpo for tier0 accounts which prevent such sensitive accounts from accessing the Internet.

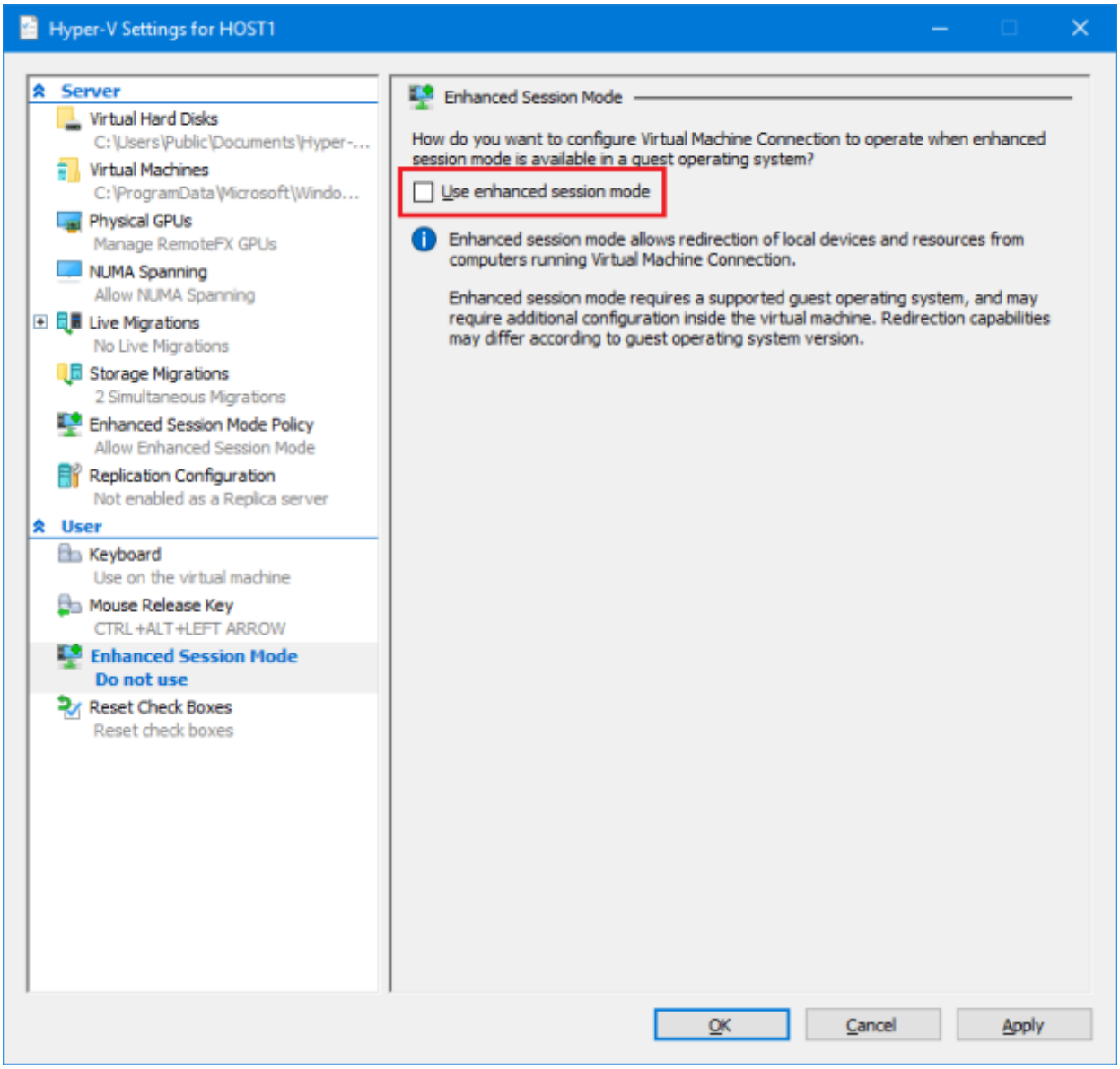
Test 4: no tier0 accounts should be able to logon to user workstations (and to tier1 servers):

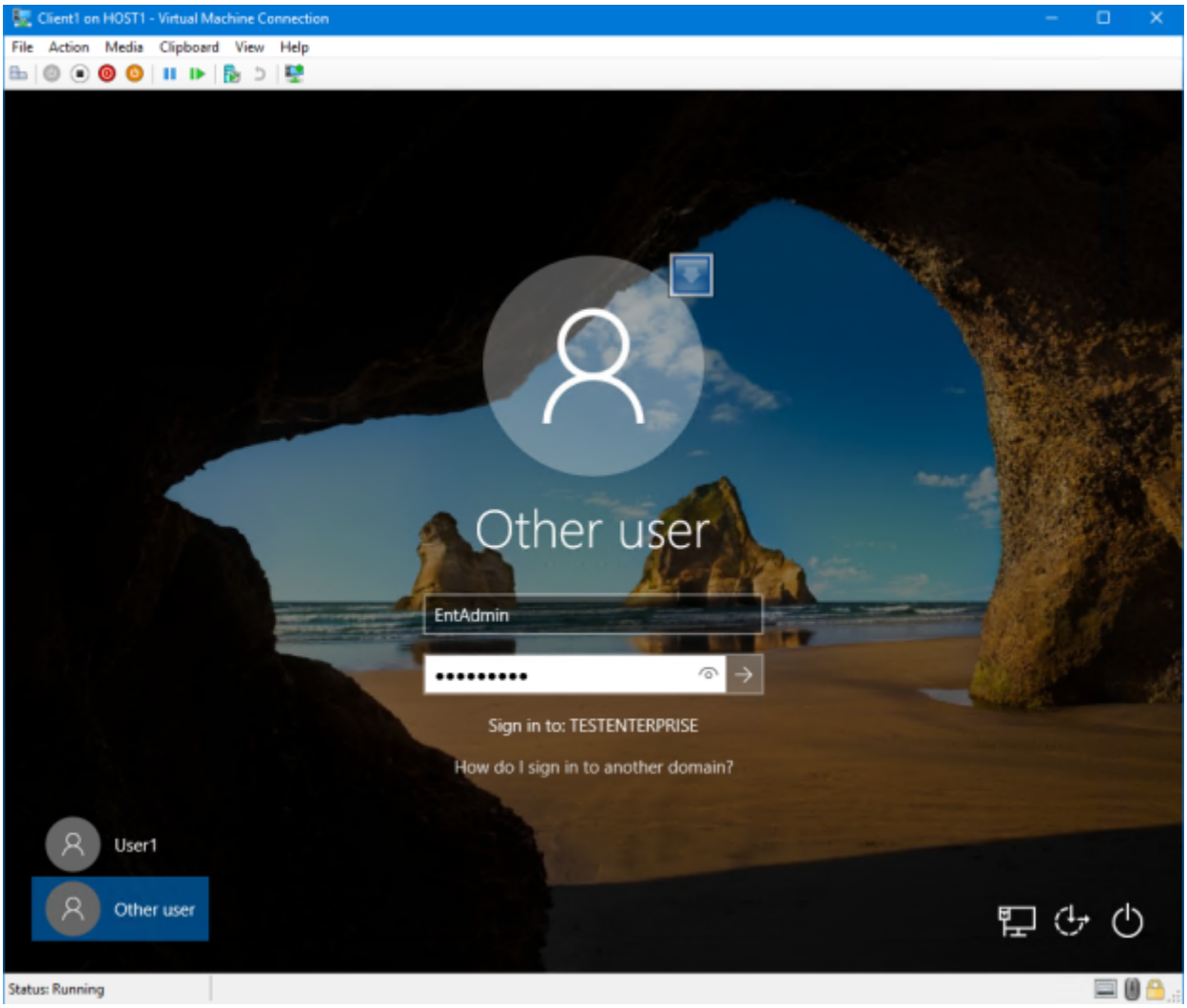


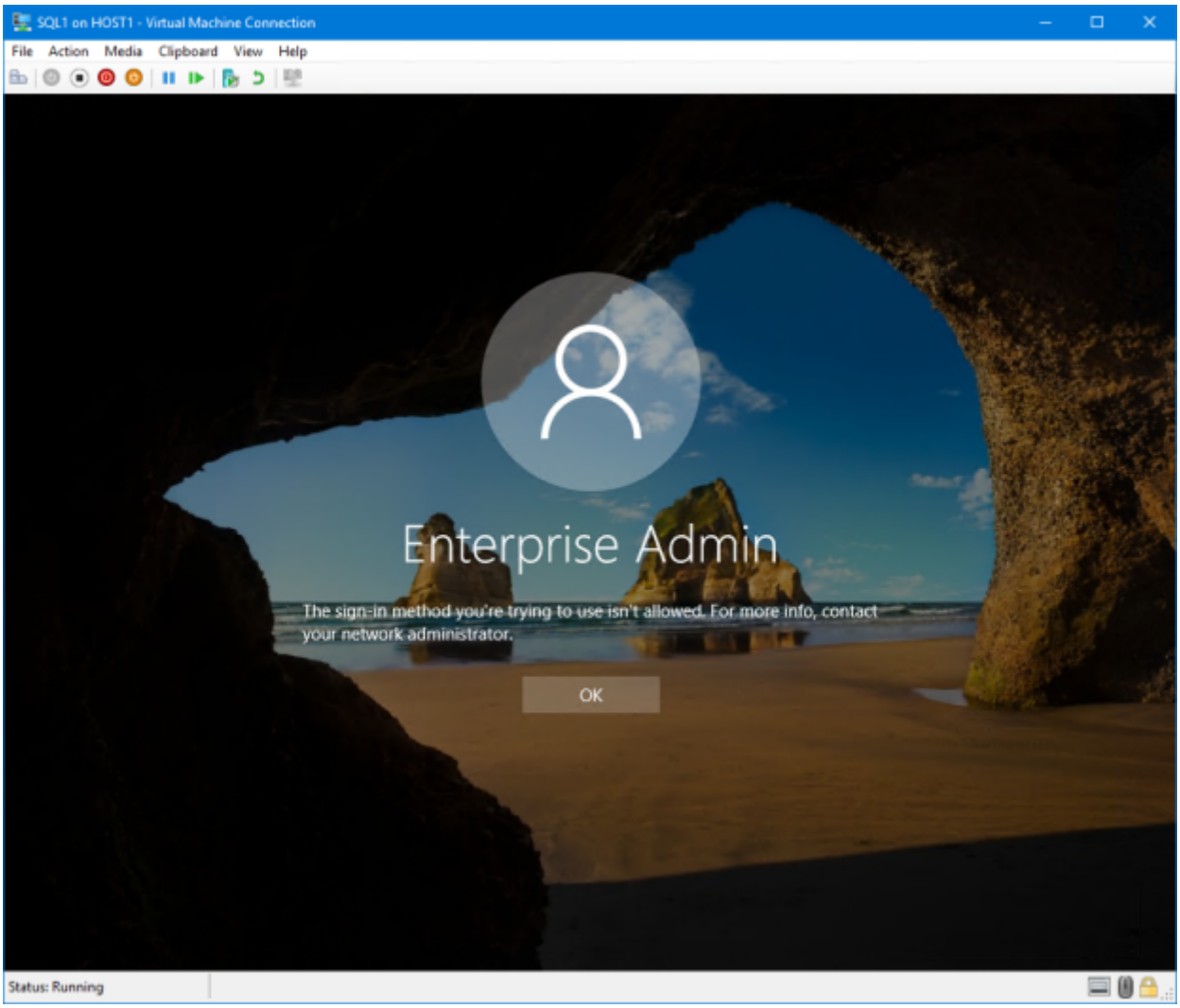

But *TestENTERPRISE\Entadmin* does log on to Client1:



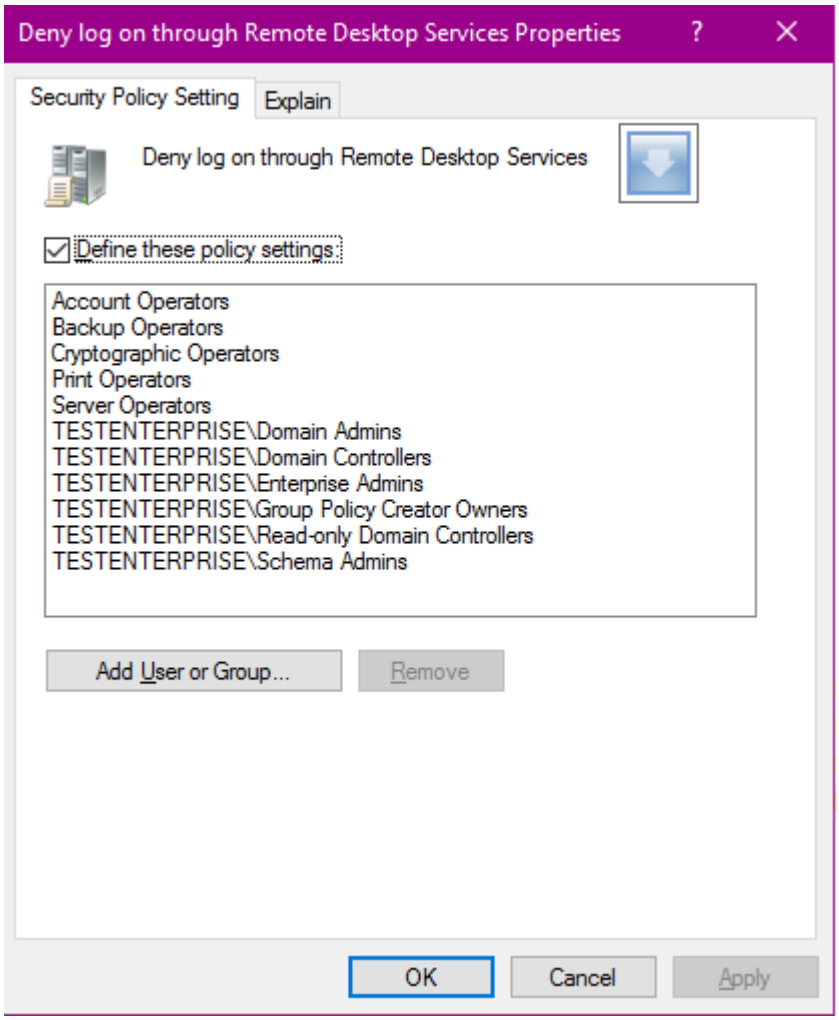

Why? Because Client1 is a virtual machine and by default we connect to virtual machines on Hyper-V using the Enchanced Session mode which is in fact the RDP – if I turn this mode off I won't be able to log on:

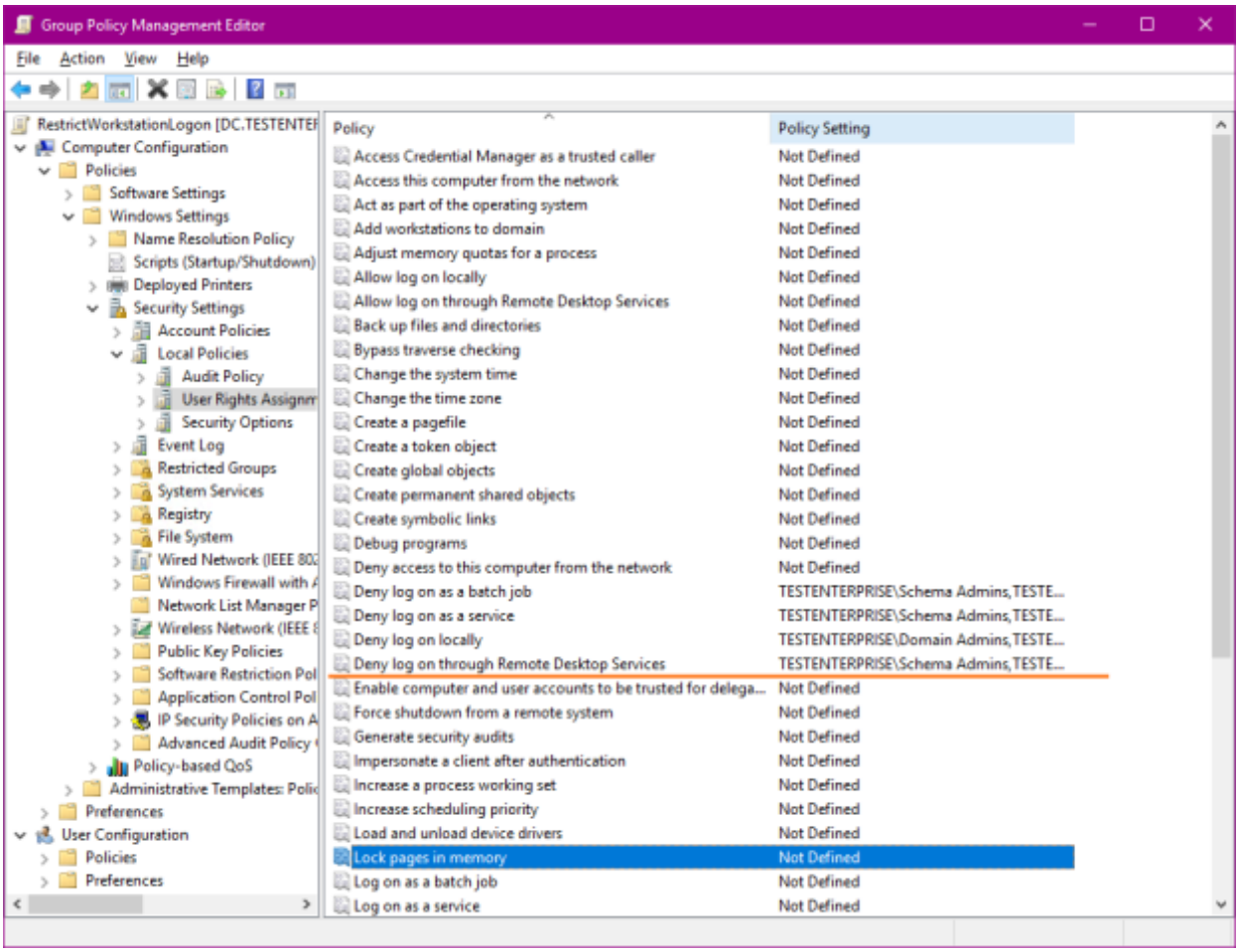

Hyper-V Settings for HOST1
Server
Virtual Hard Disks
C:\Users\Public\Documents\Hyper-...
Virtual Machines
C:\ProgramData\Microsoft\Windo...
Physical GPUs
Manage RemoteFX GPUs
NUMA Spanning
Allow NUMA Spanning
Live Migrations
No Live Migrations
Storage Migrations
2 Simultaneous Migrations
Enhanced Session Mode Policy
Allow Enhanced Session Mode
Replication Configuration
Not enabled as a Replica server
User
Keyboard
Use on the virtual machine
Mouse Release Key
CTRL+ALT+LEFT ARROW
Enhanced Session Mode
Do not use
Reset Check Boxes
Reset check boxes
Enhanced Session Mode
How do you want to configure Virtual Machine Connection to operate when enhanced session mode is available in a guest operating system?
Use enhanced session mode
Enhanced session mode allows redirection of local devices and resources from computers running Virtual Machine Connection.
Enhanced session mode requires a supported guest operating system, and may require additional configuration inside the virtual machine. Redirection capabilities may differ according to guest operating system version.
OK
Cancel
Apply


Client1 on HOST1 - Virtual Machine Connection
File Action Media Clipboard View Help
Other user
EntAdmin
Sign in to: TESTENTERPRISE
How do I sign in to another domain?
User1
Other user
Status: Running

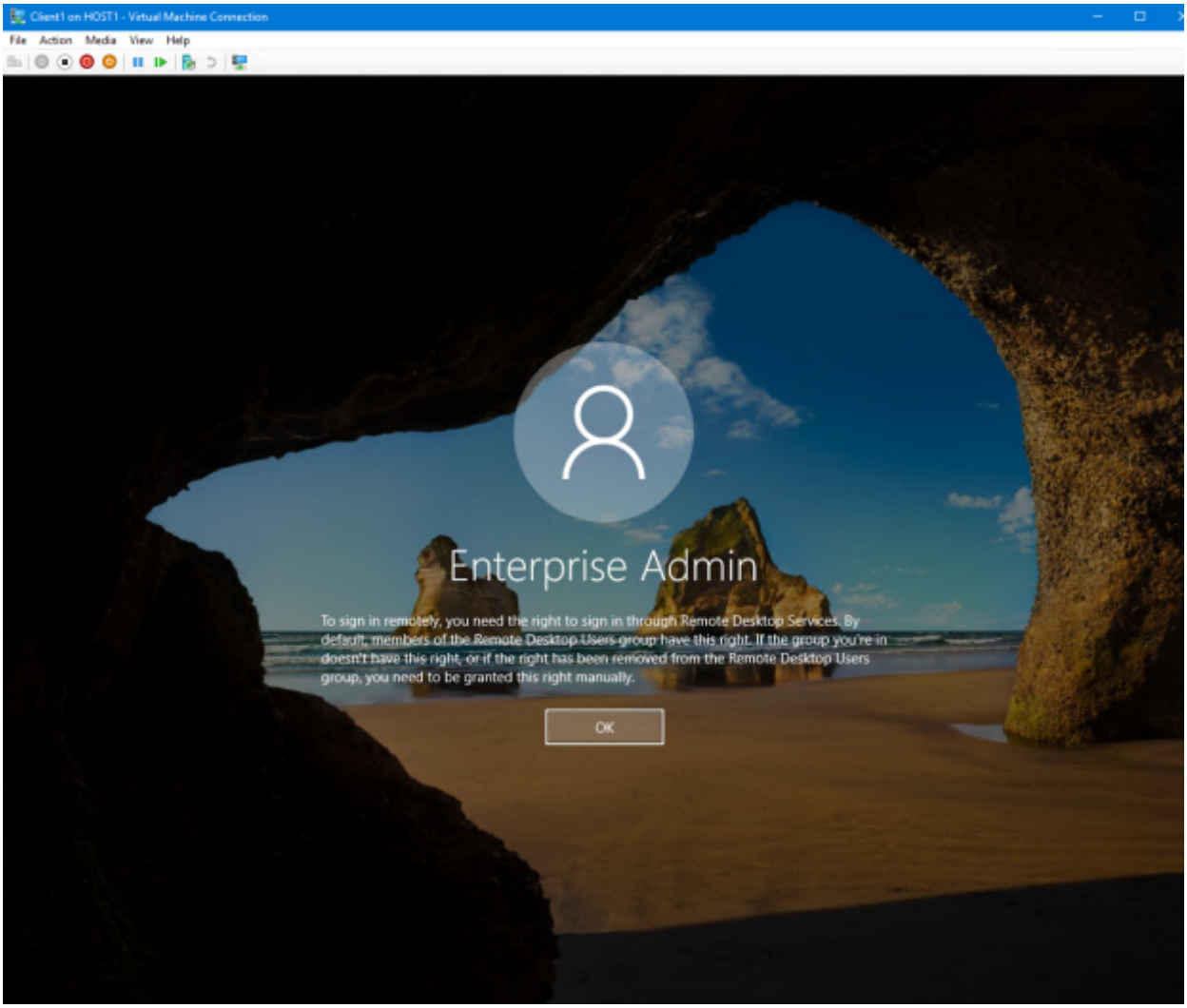



It means that it could be a good idea to configure **Deny Log on through Remote Desktop Services** policy setting as well:


Deny log on through Remote Desktop Services Properties
Security Policy Setting
Explain
Deny log on through Remote Desktop Services
Define these policy settings:
Account Operators
Backup Operators
Cryptographic Operators
Print Operators
Server Operators
TESTENTERPRISE\Domain Admins
TESTENTERPRISE\Domain Controllers
TESTENTERPRISE\Enterprise Admins
TESTENTERPRISE\Group Policy Creator Owners
TESTENTERPRISE\Read-only Domain Controllers
TESTENTERPRISE\Schema Admins
Add User or Group...
Remove
OK
Cancel
Apply

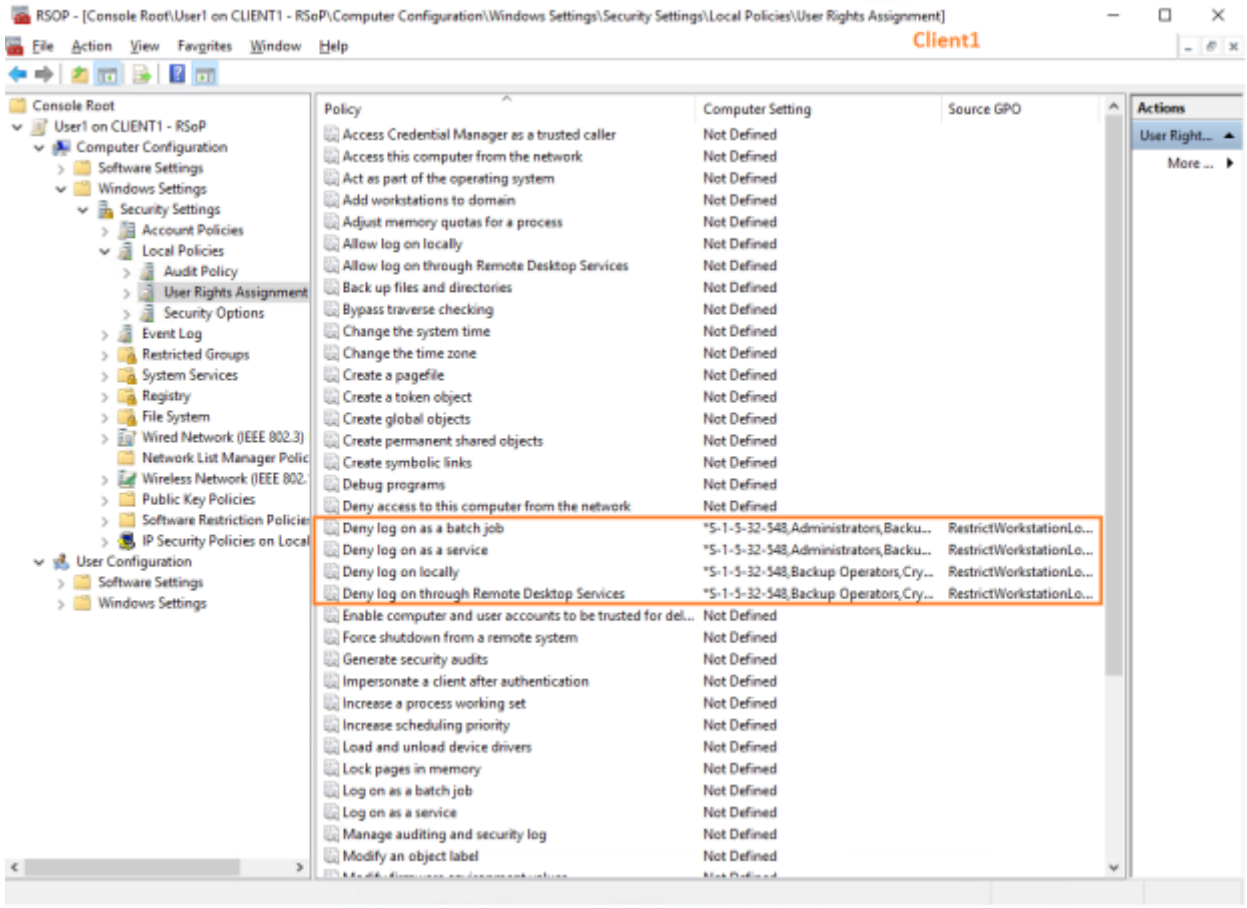

Group Policy Management Editor
File Action View Help
RestrictWorkstationLogon [DC.TESTENTER
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignm
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802
Windows Firewall with A
Network List Manager P
Wireless Network (IEEE
Public Key Policies
Software Restriction Pol
Application Control Pol
IP Security Policies on A
Advanced Audit Policy
Policy-based QoS
Administrative Templates: Polic
Preferences
User Configuration
Policies
Preferences
Policy
Policy Setting
Access Credential Manager as a trusted caller Not Defined
Access this computer from the network Not Defined
Act as part of the operating system Not Defined
Add workstations to domain Not Defined
Adjust memory quotas for a process Not Defined
Allow log on locally Not Defined
Allow log on through Remote Desktop Services Not Defined
Back up files and directories Not Defined
Bypass traverse checking Not Defined
Change the system time Not Defined
Change the time zone Not Defined
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 Not Defined
Deny log on as a batch job TESTENTERPRISE\Schema Admins, TESTE...
Deny log on as a service TESTENTERPRISE\Schema Admins, TESTE...
Deny log on locally TESTENTERPRISE\Domain Admins, TESTE...
Deny log on through Remote Desktop Services TESTENTERPRISE\Schema Admins, TESTE...
Enable computer and user accounts to be trusted for delega... Not Defined
Force shutdown from a remote system Not Defined
Generate security audits Not Defined
Impersonate a client after authentication Not Defined
Increase a process working set Not Defined
Increase scheduling priority Not Defined
Load and unload device drivers Not Defined
Lock pages in memory Not Defined
Log on as a batch job Not Defined
Log on as a service Not Defined

And after turning on Enchanced Session mode…



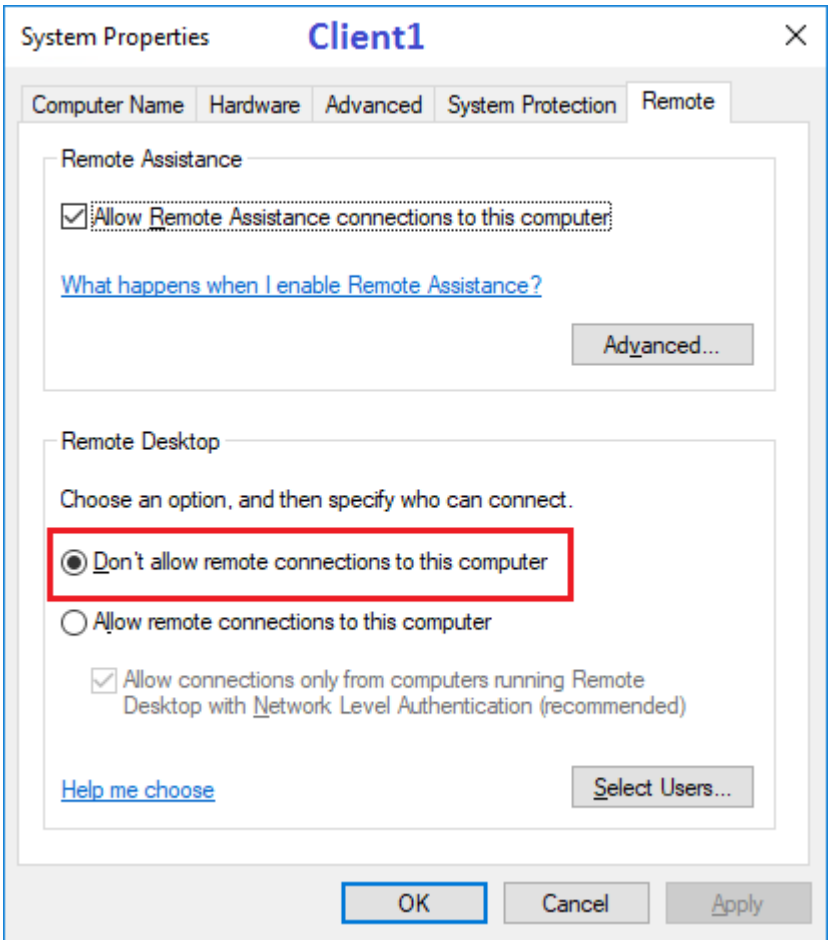


The local Client1’s policy after applying the gpo:




As you see some of the group names cannot be resolved on Windows 10 because these groups exist only on server operating systems (Server Operators, Account Operators…).

I'd like to stress that the ability to connect to a virtual machine under a tier0 account (which is set to *Deny Logon Locally* on that vm!) is possible even when the Remote Access is NOT enabled in this virtual machine:






In fact it means that there may be the situation when configuring the paw according to MS's PAW implementation guide will not allow to reach the stated goal: ~"Tier0 accounts must be prohibited from logging onto Tier1/Tier2 devices".

**Phase1** is now completed – we can use the paw for administerning tier0 servers – domain controllers – with tier0 accounts (*TestENTERPRISE\EntAdmin* or any other domain administrative account). No tier0 account can be used to logon locally or via RDP to user workstations.

In part3 we'll proceed to implementing Phase2.