How to: Deploy Microsoft LAPS and Windows LAPS

markswinkels.nl/how-to-deploy-microsoft-laps-and-windows-laps

Mark

August 28, 2023

We've all heard of Microsoft LAPS. This stands for Local Administrator Password Solution and is already available from Windows Server 2008 R2. With Microsoft LAPS it is possible to periodically and fully automatically change the password of the local administrator account.

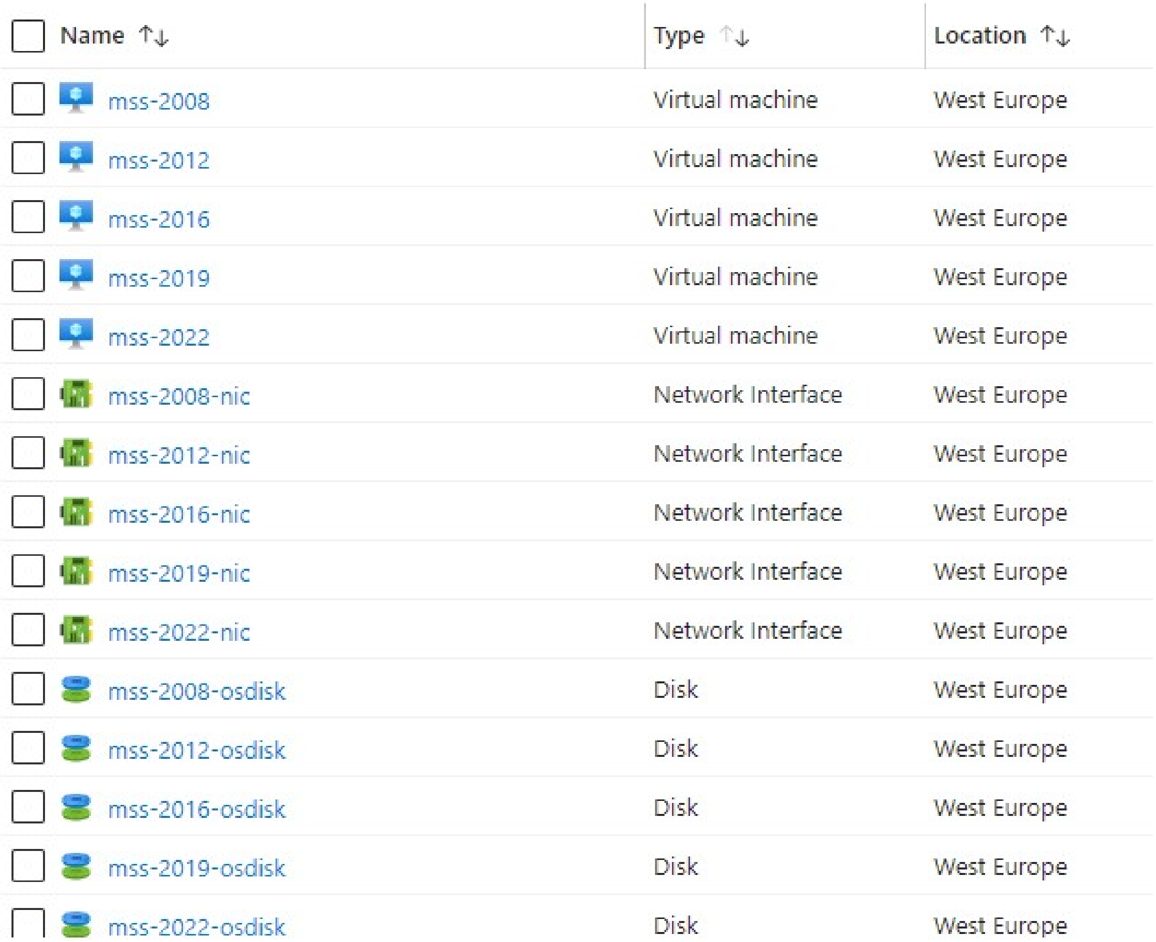
Microsoft recently launched Windows LAPS, as a successor to Microsoft LAPS. A number of new functionalities have been added and it is now also part of the Windows Server operating system (from Server 2019 April Update) and Windows 10 and 11.

In this blog post I will show you what steps are needed to implement and activate Microsoft LAPS and Windows LAPS within a Windows server landscape. We look at legacy operating systems (Windows Server 2008 R2, 2012 R2, 2016) and also the more modern operating systems (Windows Server 2019 and 2022). Of course you see the operation of Microsoft LAPS and Windows LAPS in a hybrid situation.

In my situation, I have built an infrastructure in Microsoft Azure. A domain controller based on Windows Server 2022 and five servers based on Windows Server 2008 R2, 2012 R2, 2016, 2019 and 2022.

- mss-dc01 / Windows Server 2022 / domain controller
- mss-2008 / Windows Server 2008 R2 / Member server
- mss-2012 / Windows Server 2012 R2 / Member server
- mss-2016 / Windows Server 2016 / Member server
- mss-2019 / Windows Server 2019 / Member server
- mss-2022 / Windows Server 2022 / Member server

The entire environment was rolled out with terraform (Infrastructure as Code), so the foundation was built up in a few minutes.



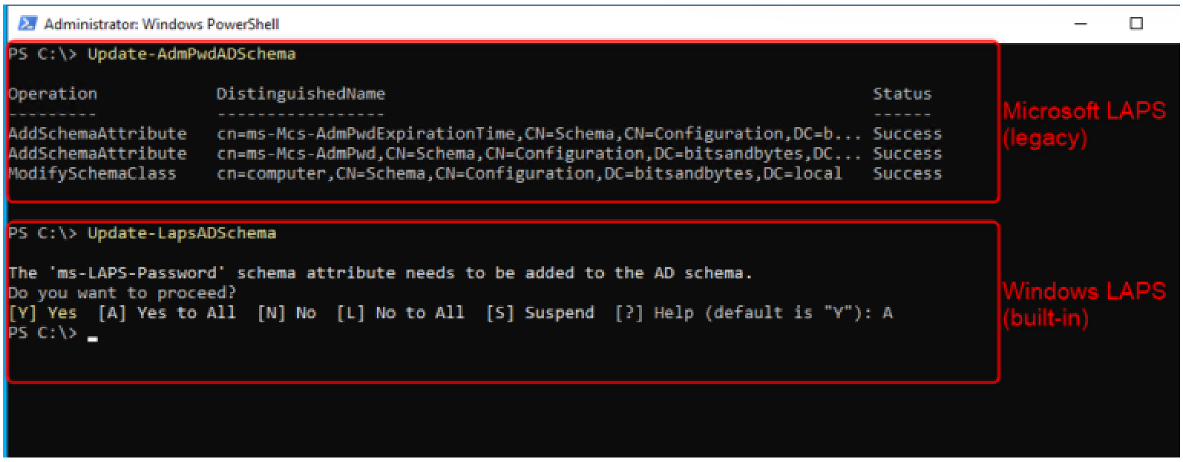
□ Name ↑↓	Type ↑↓	Location ↑↓
□ mss-2008	Virtual machine	West Europe
□ mss-2012	Virtual machine	West Europe
□ mss-2016	Virtual machine	West Europe
□ mss-2019	Virtual machine	West Europe
□ mss-2022	Virtual machine	West Europe
□ mss-2008-nic	Network Interface	West Europe
□ mss-2012-nic	Network Interface	West Europe
□ mss-2016-nic	Network Interface	West Europe
□ mss-2019-nic	Network Interface	West Europe
□ mss-2022-nic	Network Interface	West Europe
□ mss-2008-osdisk	Disk	West Europe
□ mss-2012-osdisk	Disk	West Europe
□ mss-2016-osdisk	Disk	West Europe
□ mss-2019-osdisk	Disk	West Europe
□ mss-2022-osdisk	Disk	West Europe

The steps I went through are.

- Extend the Active Directory Schema for Microsoft LAPS (legacy)
- Extend the Active Directory Schema for Windows LAPS
- Set the right permissions for the computer object to perform a password reset
- Create and configure group policies for Microsoft and Windows LAPS
- Verify the new LAPS configuration in real live

Extend the Active Directory Schema

The first step is to prepare your Active Directory environment for Microsoft and Windows LAPS. Download the Microsoft LAPS installer from the Microsoft website and install the tooling.

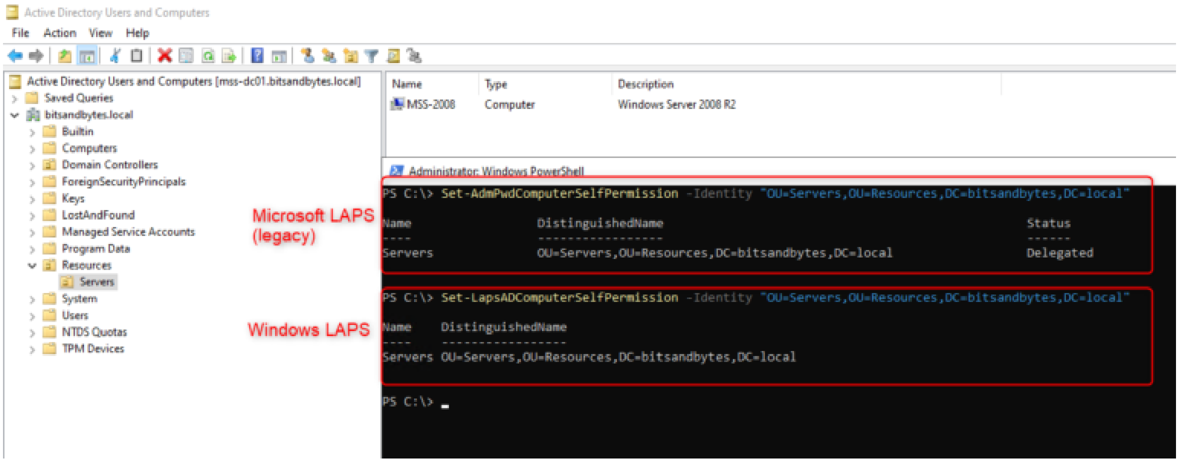


```
PS C:\> Update-AdmPwdADSchema

Operation            DistinguishedName                                           Status
---------            -----------------                                           ------
AddSchemaAttribute   cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=b... Success
AddSchemaAttribute   cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=bitsandbytes,DC... Success
ModifySchemaClass    cn=computer,CN=Schema,CN=Configuration,DC=bitsandbytes,DC=local   Success

PS C:\> Update-LapsADSchema

The 'ms-LAPS-Password' schema attribute needs to be added to the AD schema.
Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): A
PS C:\> _
```

> For Windows Server 2008 R2, 2012 R2, 2016 (legacy)
> Update-AdmPwdAdSchema
>
> For Windows Server 2019 (April Update and higher) and 2022
> Update-LapsADSchema

Configuring the right permissions for the computer objects

A crucial step in the configuration is setting the right permissions for the computer objects to perform the password reset. You need the DN of the organization unit where your computer objects are located. In my environment, all the servers (legacy and new) are located in the OU ‘Resources / Servers’. If your have multiple OU’s, you need to run the command for every OU. Running the command on top level, all the permissions are inherited to the below OU’s.



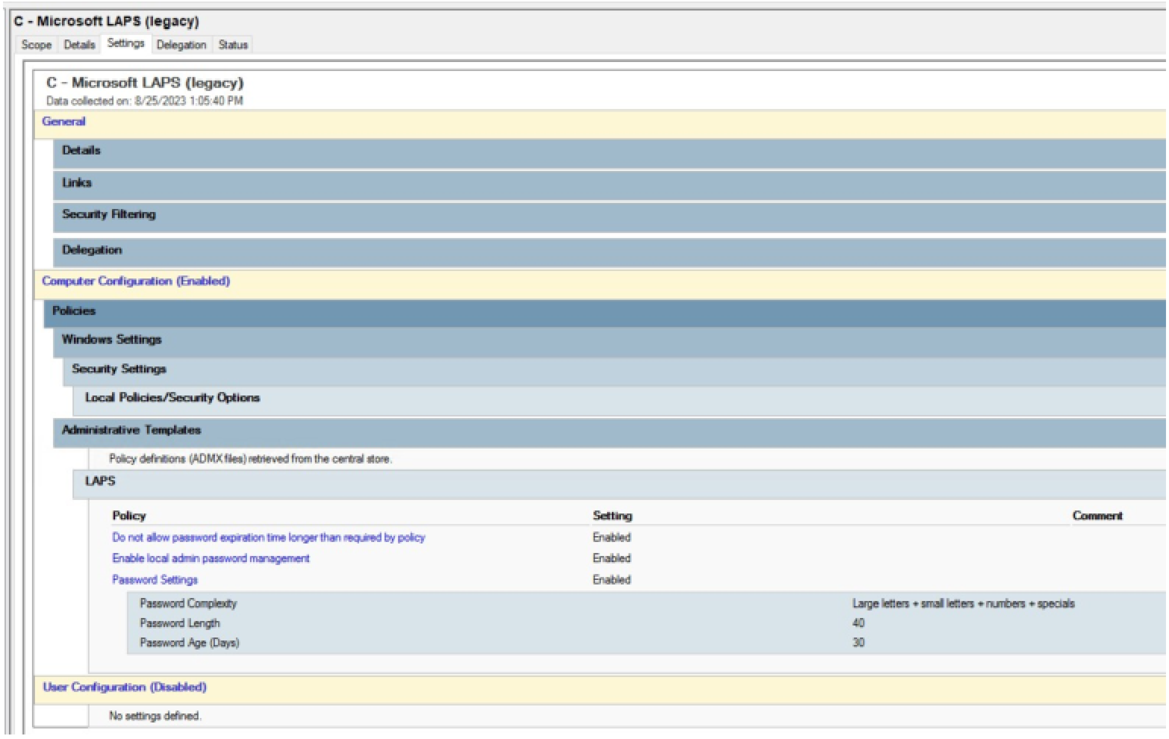
Name	Type	Description
MSS-2008	Computer	Windows Server 2008 R2

```
PS C:\> Set-AdmPwdComputerSelfPermission -Identity "OU=Servers,OU=Resources,DC=bitsandbytes,DC=local"

Name            DistinguishedName                                               Status
----            -----------------                                               ------
Servers         OU=Servers,OU=Resources,DC=bitsandbytes,DC=local                Delegated

PS C:\> Set-LapsADComputerSelfPermission -Identity "OU=Servers,OU=Resources,DC=bitsandbytes,DC=local"

Name    DistinguishedName
----    -----------------
Servers OU=Servers,OU=Resources,DC=bitsandbytes,DC=local

PS C:\> _
```

> For Windows Server 2008 R2, 2012 R2, 2016 (legacy)
> Set-AdmPwdComputerSelfPermission -Identity ‘DN of the organizational unit’
>
> For Windows Server 2019 (April Update and higher) and 2022
> Set-LapsADComputerSelfPermission -Identity ‘DN of the organizational unit’

Create new group policies

Okay, so now the Active Directory Schema and permissions are prepared. The next step is to setup the group policy objects. We need two different policies, because Microsoft LAPS and Windows LAPS have there own settings. Let’s take a look at the Microsoft LAPS group policy settings.



C - Microsoft LAPS (legacy)
Data collected on: 8/25/2023 1:05:40 PM

General

Details

Links

Security Filtering

Delegation

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Local Policies/Security Options

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

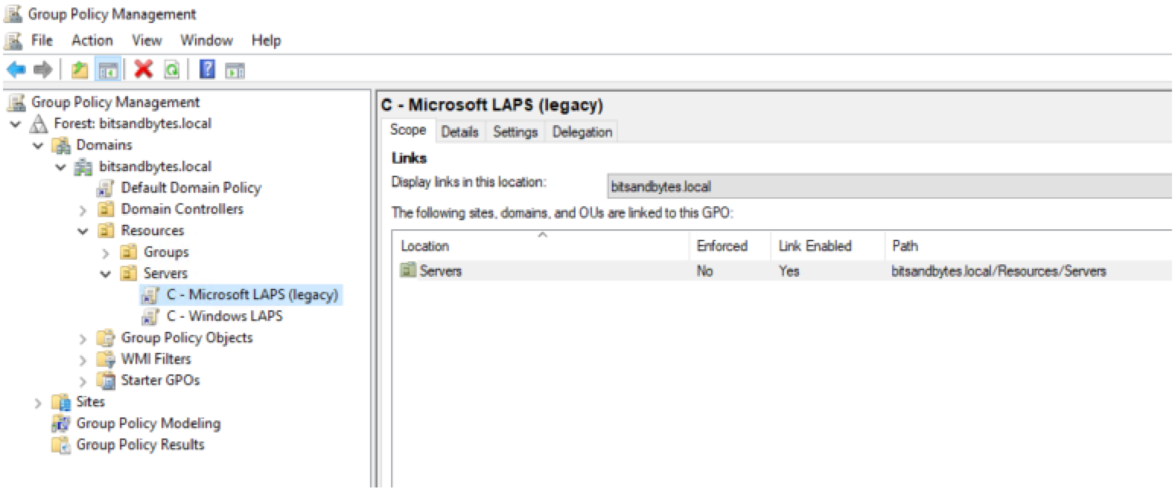
LAPS

Policy	Setting	Comment
Do not allow password expiration time longer than required by policy	Enabled	
Enable local admin password management	Enabled	
Password Settings	Enabled	
Password Complexity		Large letters + small letters + numbers + specials
Password Length		40
Password Age (Days)		30

User Configuration (Disabled)

No settings defined.

> For Windows Server 2008 R2, 2012 R2, 2016 (legacy)
> Computer Configuration / Administrative Templates / LAPS

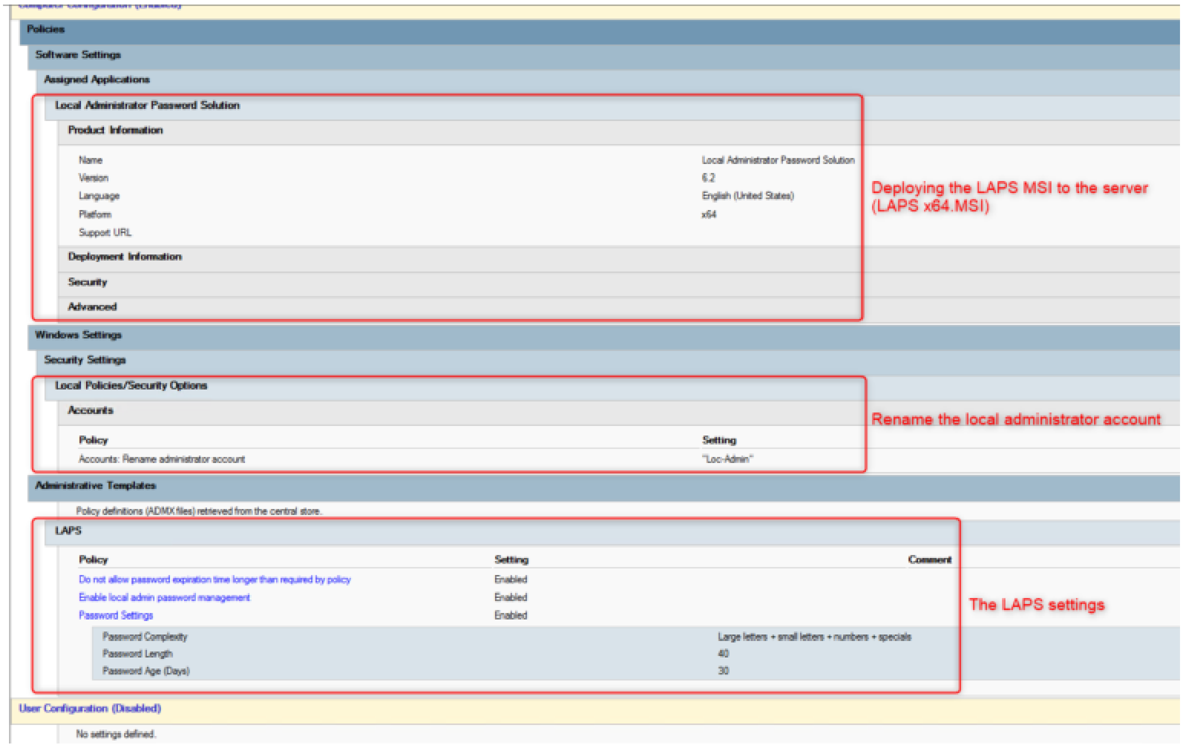


Links

Display links in this location: bitsandbytes.local

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
Servers	No	Yes	bitsandbytes.local/Resources/Servers



Policies

Software Settings

Assigned Applications

Local Administrator Password Solution

Product Information

Name	Local Administrator Password Solution
Version	6.2
Language	English (United States)
Platform	x64
Support URL	

Deployment Information

Security

Advanced

Deploying the LAPS MSI to the server (LAPS x64.MSI)

Windows Settings

Security Settings

Local Policies/Security Options

Accounts

Policy	Setting
Accounts: Rename administrator account	"Loc-Admin"

Rename the local administrator account

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

LAPS

Policy	Setting	Comment
Do not allow password expiration time longer than required by policy	Enabled	
Enable local admin password management	Enabled	
Password Settings	Enabled	

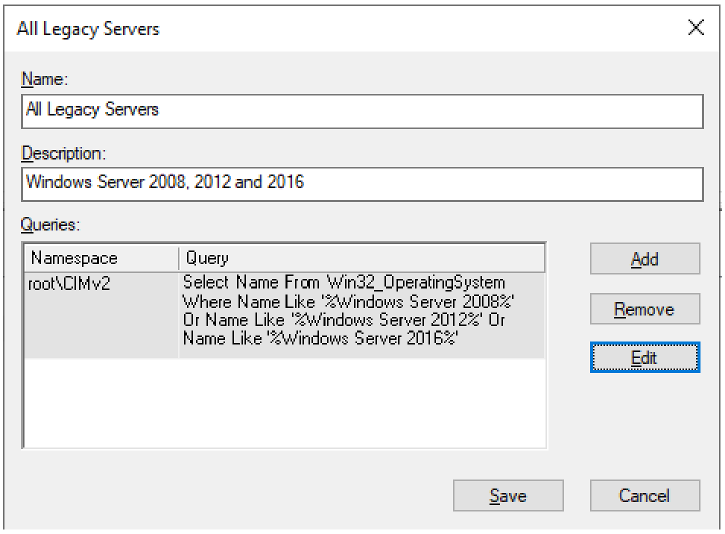
Password Complexity	Large letters + small letters + numbers + specials
Password Length	40
Password Age (Days)	30

The LAPS settings

User Configuration (Disabled)

No settings defined.

Because all of my servers are in the same organization unit and they need different group policies, I've created a WMI filter that filters based on the operation system.



All Legacy Servers

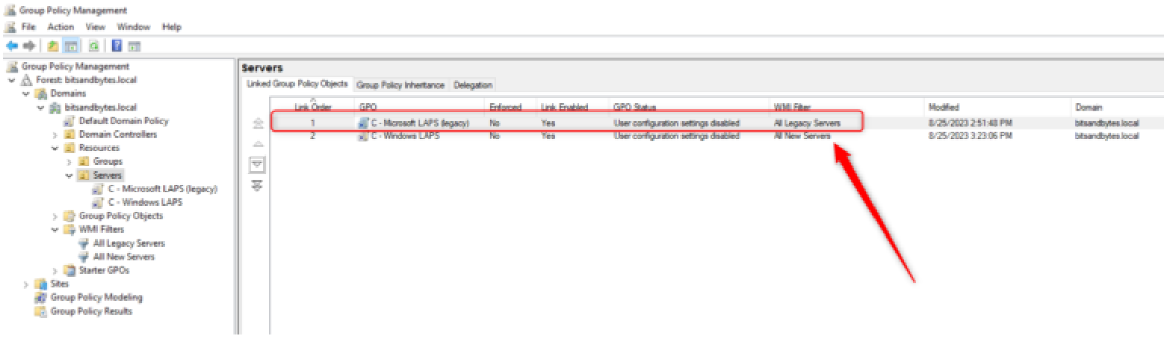
Name:
All Legacy Servers

Description:
Windows Server 2008, 2012 and 2016

Queries:

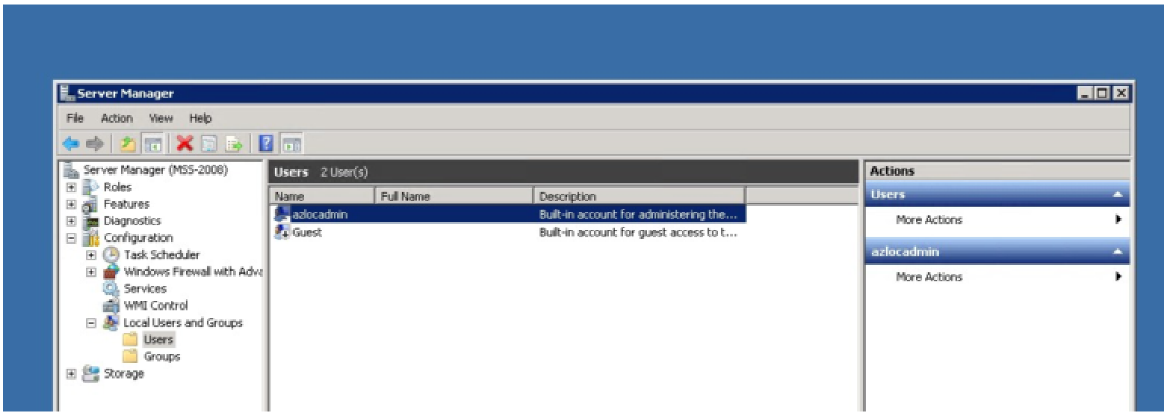
Namespace	Query
root\CIMv2	Select Name From Win32_OperatingSystem Where Name Like '%Windows Server 2008%' Or Name Like '%Windows Server 2012%' Or Name Like '%Windows Server 2016%'

> Select Name From Win32_OperatingSystem Where Name Like '%Windows Server 2008%' Or Name Like '%Windows Server 2012%' Or Name Like '%Windows Server 2016%'

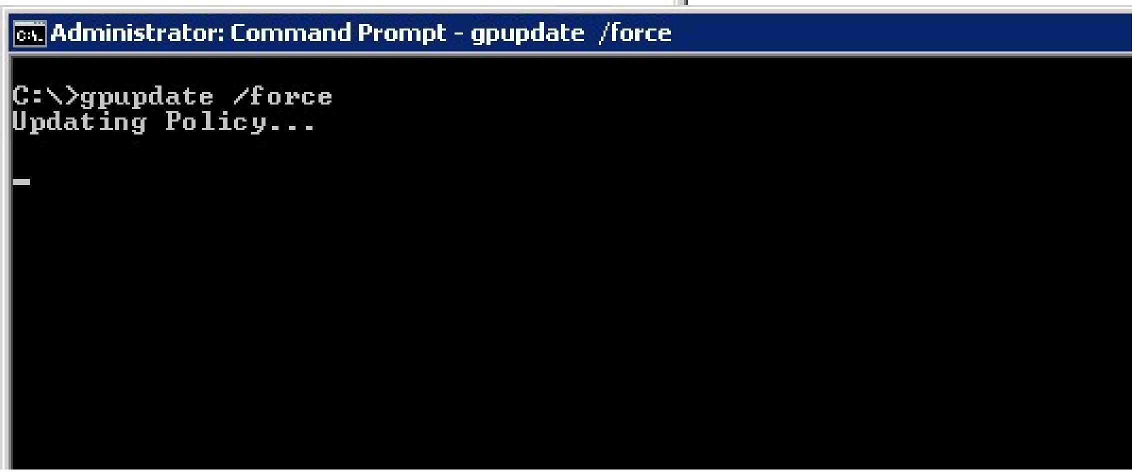


Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	C - Microsoft LAPS (legacy)	No	Yes	User configuration settings disabled	All Legacy Servers	8/25/2023 2:51:48 PM	bitsandbytes.local
2	C - Windows LAPS	No	Yes	User configuration settings disabled	All New Servers	8/25/2023 3:23:06 PM	bitsandbytes.local

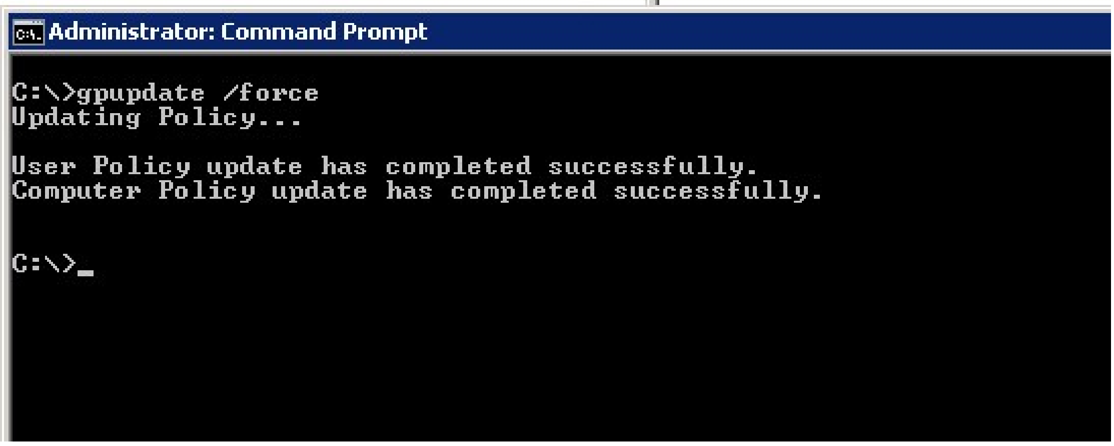
The legacy server 'mss-2008' is joined to the domain. Let's see what is happening when we active the new GPO.



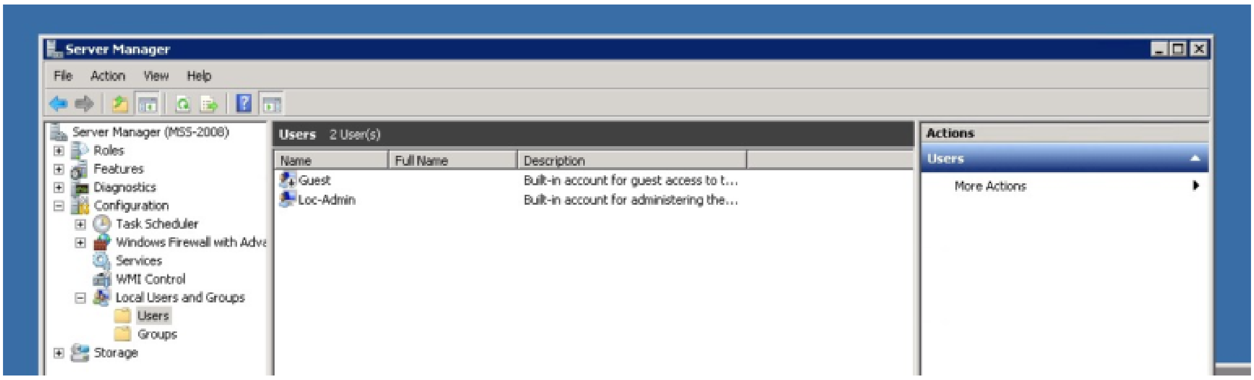
Name	Full Name	Description
azlocadmin		Built-in account for administering the...
Guest		Built-in account for guest access to t...


Administrator: Command Prompt - gpupdate /force

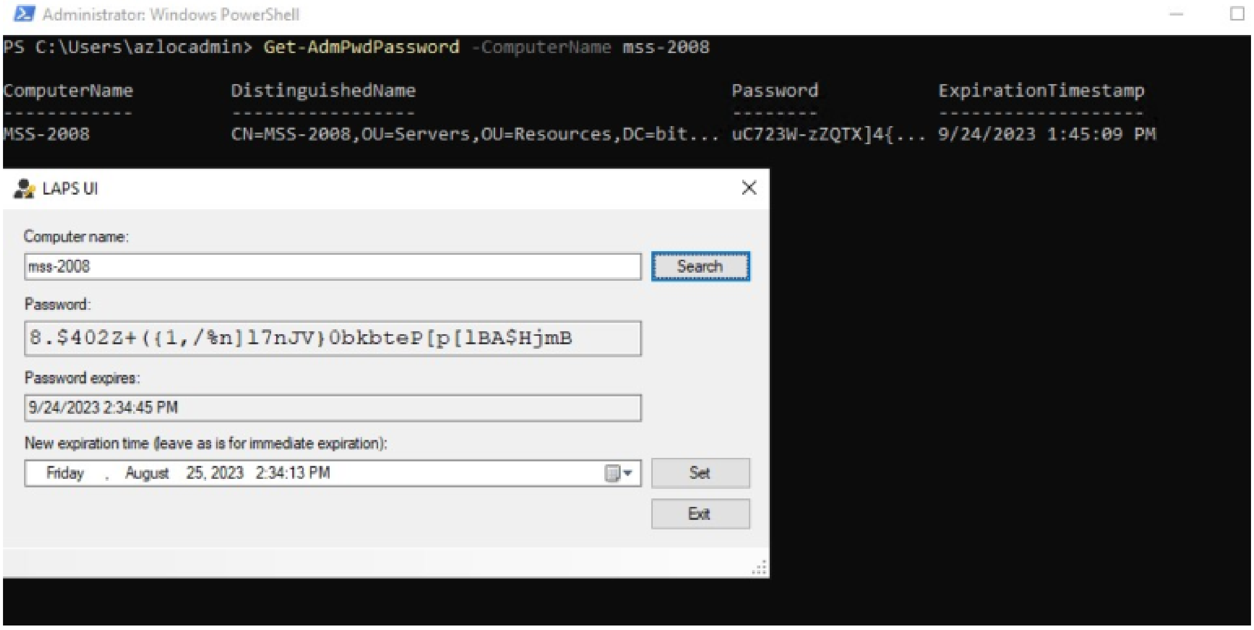
```
C:\>gpupdate /force
Updating Policy...

_
```


Administrator: Command Prompt

```
C:\>gpupdate /force
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.


C:\>_
```



Name	Full Name	Description
Guest		Built-in account for guest access to t...
Loc-Admin		Built-in account for administering the...



Administrator: Windows PowerShell

```
PS C:\Users\azlocadmin> Get-AdmPwdPassword -ComputerName mss-2008

ComputerName          DistinguishedName                                  Password             ExpirationTimestamp
------------          -----------------                                  --------             -------------------
MSS-2008              CN=MSS-2008,OU=Servers,OU=Resources,DC=bit...  uC723W-zZQTX]4{...  9/24/2023 1:45:09 PM
```

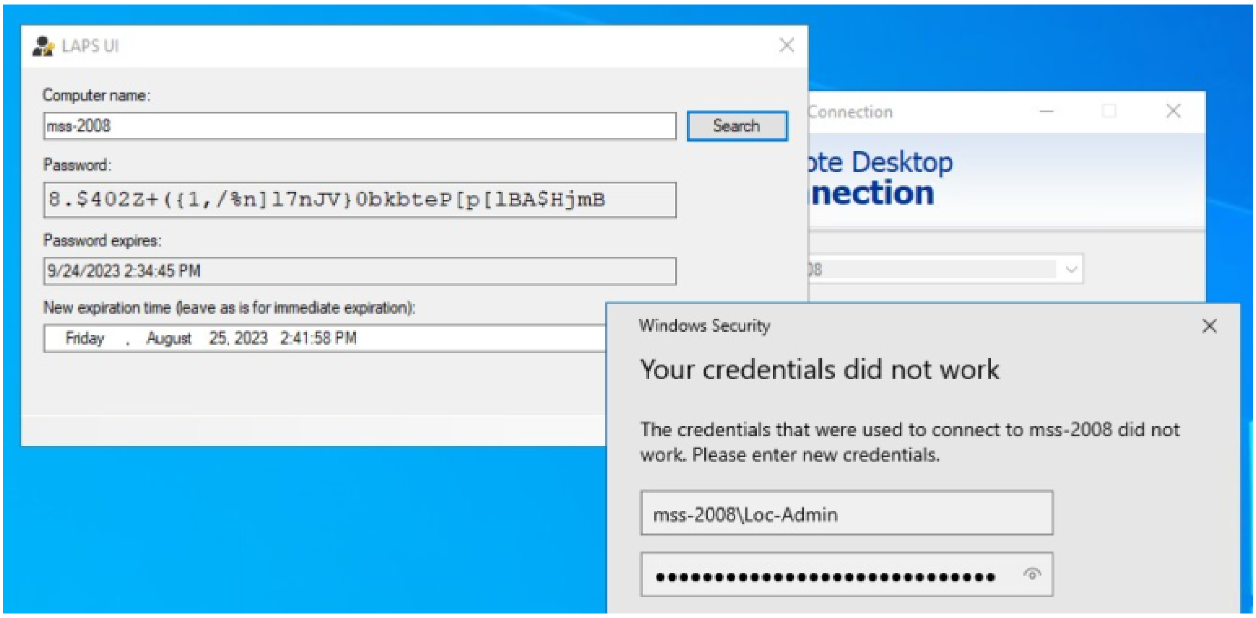
LAPS UI

Computer name: mss-2008

Password: 8.$402Z+({1,/%n]l7nJV}0bkbteP[p[lBA$HjmB

Password expires: 9/24/2023 2:34:45 PM

New expiration time (leave as is for immediate expiration): Friday , August 25, 2023 2:34:13 PM



LAPS UI

Computer name: mss-2008

Password: 8.$402Z+({1,/%n]l7nJV}0bkbteP[p[lBA$HjmB

Password expires: 9/24/2023 2:34:45 PM

New expiration time (leave as is for immediate expiration): Friday , August 25, 2023 2:41:58 PM

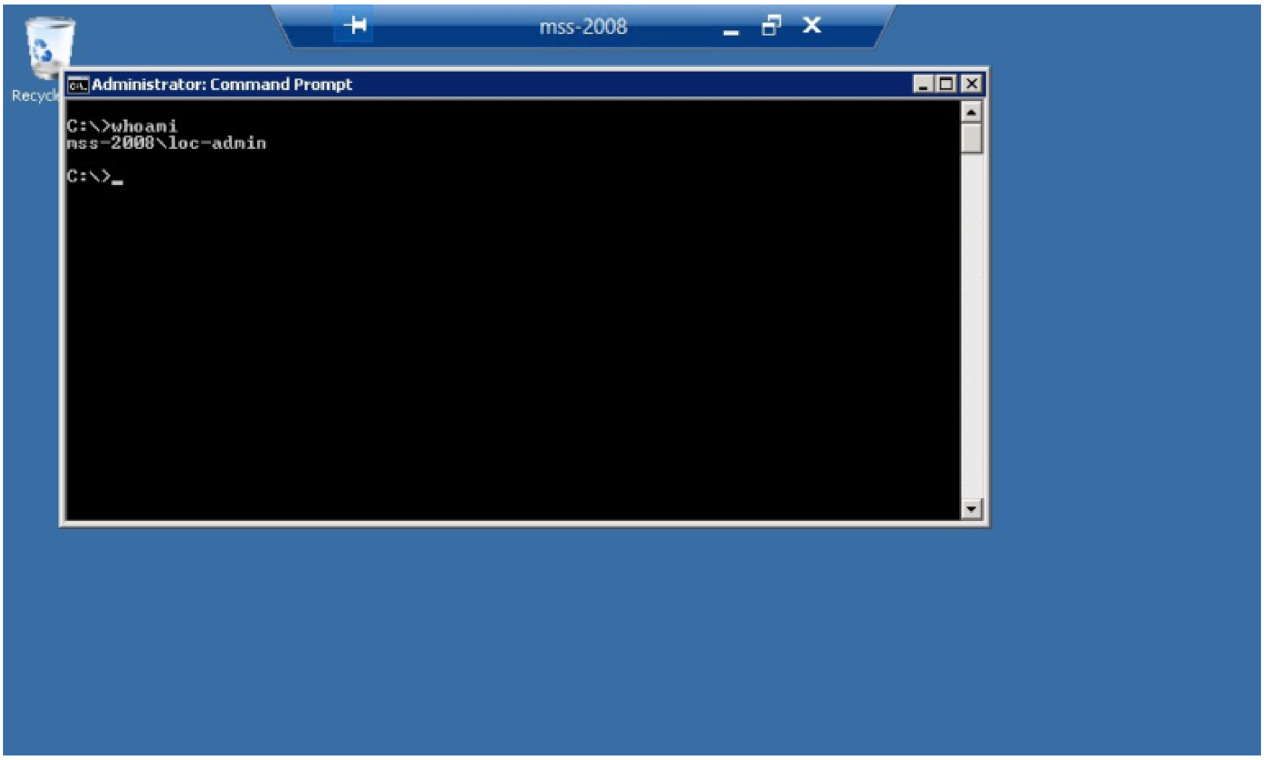
Windows Security

Your credentials did not work

The credentials that were used to connect to mss-2008 did not work. Please enter new credentials.

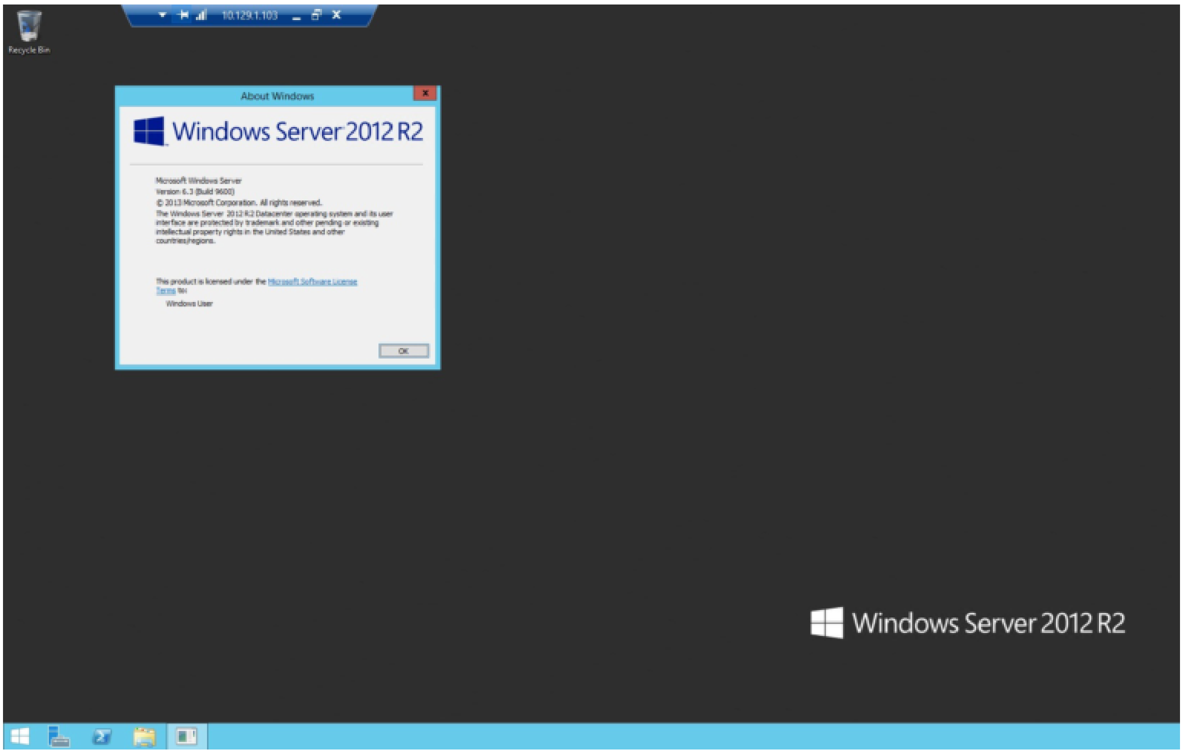
mss-2008\Loc-Admin

••••••••••••••••••••••••••••••••



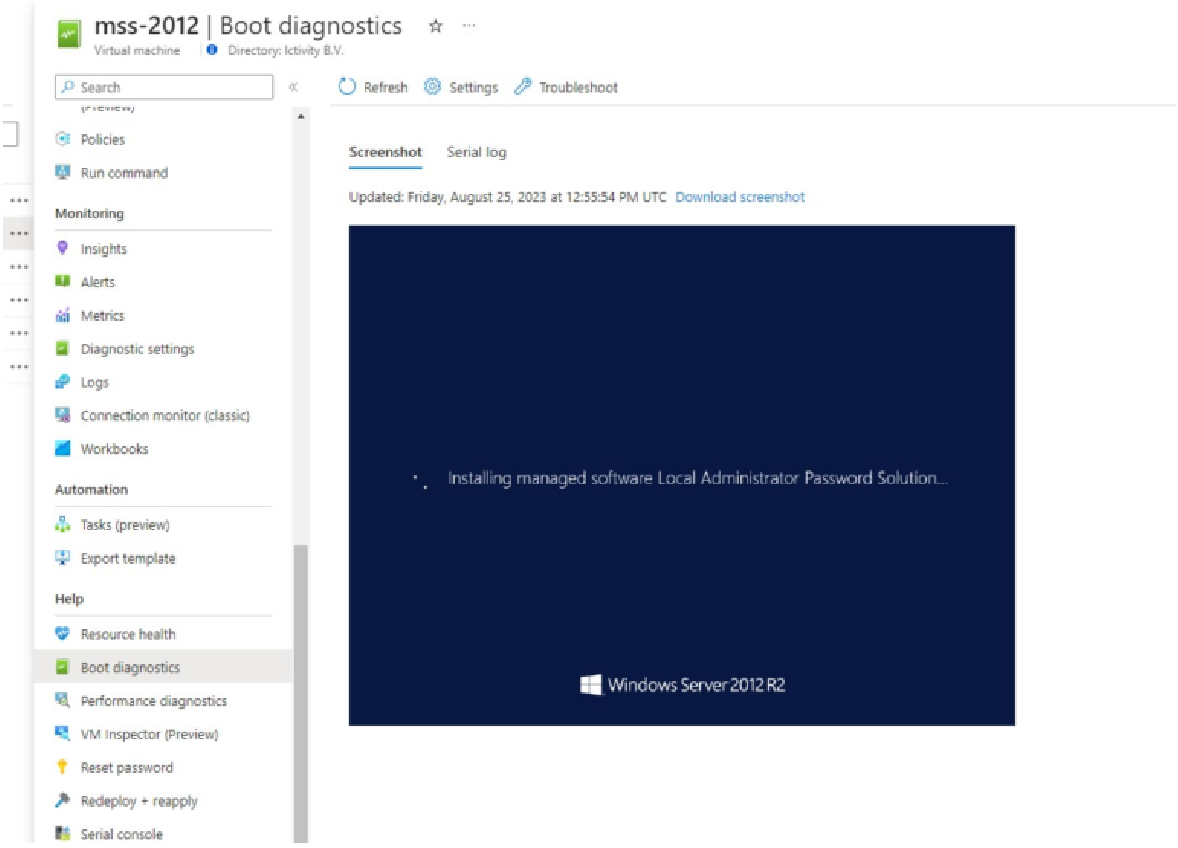
```
C:\>whoami
mss-2008\loc-admin

C:\>_
```

The same thing for Windows Server 2012 R2 and 2016.



Microsoft Windows Server
Version 6.3 (Build 9600)
© 2013 Microsoft Corporation. All rights reserved.
The Windows Server 2012 R2 Datacenter operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

This product is licensed under the Microsoft Software License Terms to:
Windows User



mss-2012 | Boot diagnostics

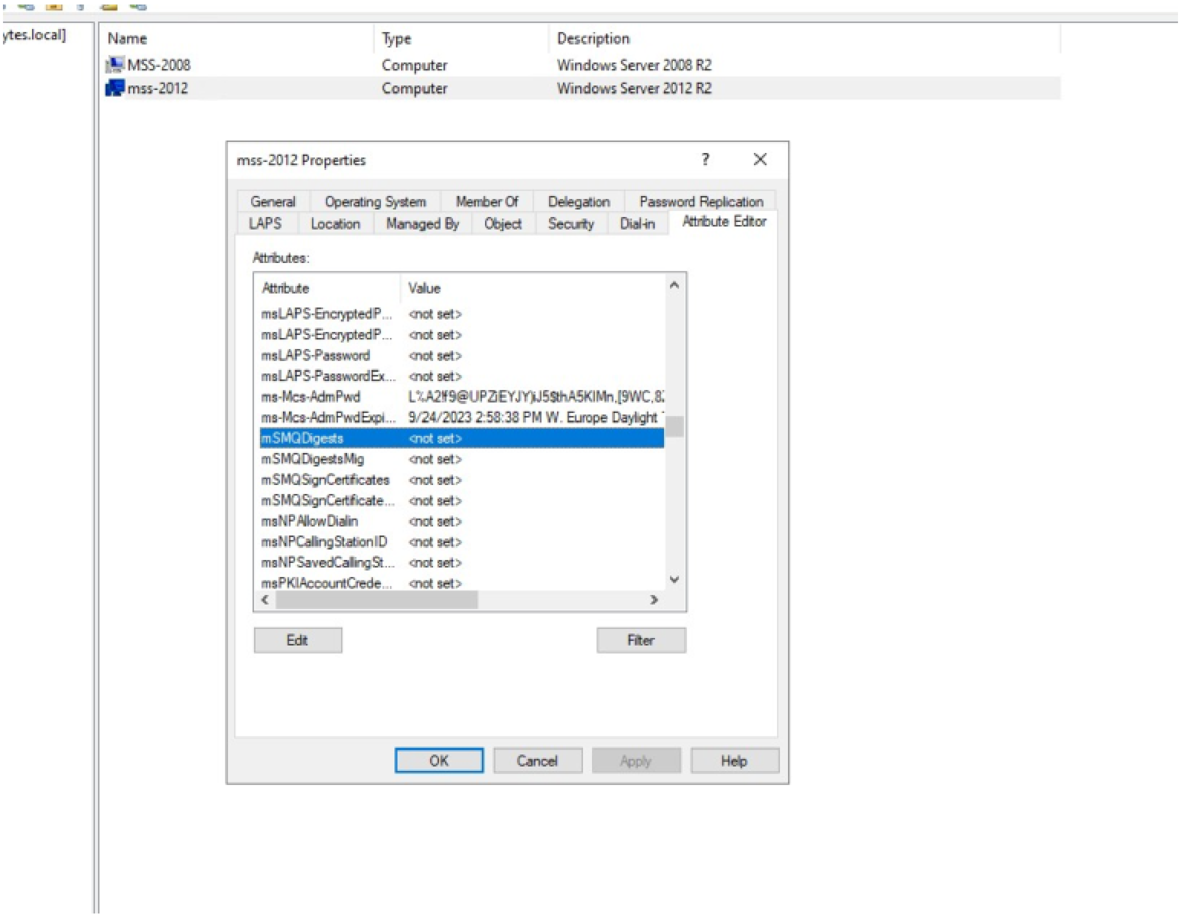
Virtual machine | Directory: Ictivity B.V.

Updated: Friday, August 25, 2023 at 12:55:54 PM UTC Download screenshot

Installing managed software Local Administrator Password Solution...

Windows Server 2012 R2

To view the newly applied password, you can use the LAPS UI tool, but you can also open the Attribute Editor in Active Directory Users & Computers. Look for the attribute ‘ms-Mcs-AdmPwd’.



Name	Type	Description
MSS-2008	Computer	Windows Server 2008 R2
mss-2012	Computer	Windows Server 2012 R2

mss-2012 Properties

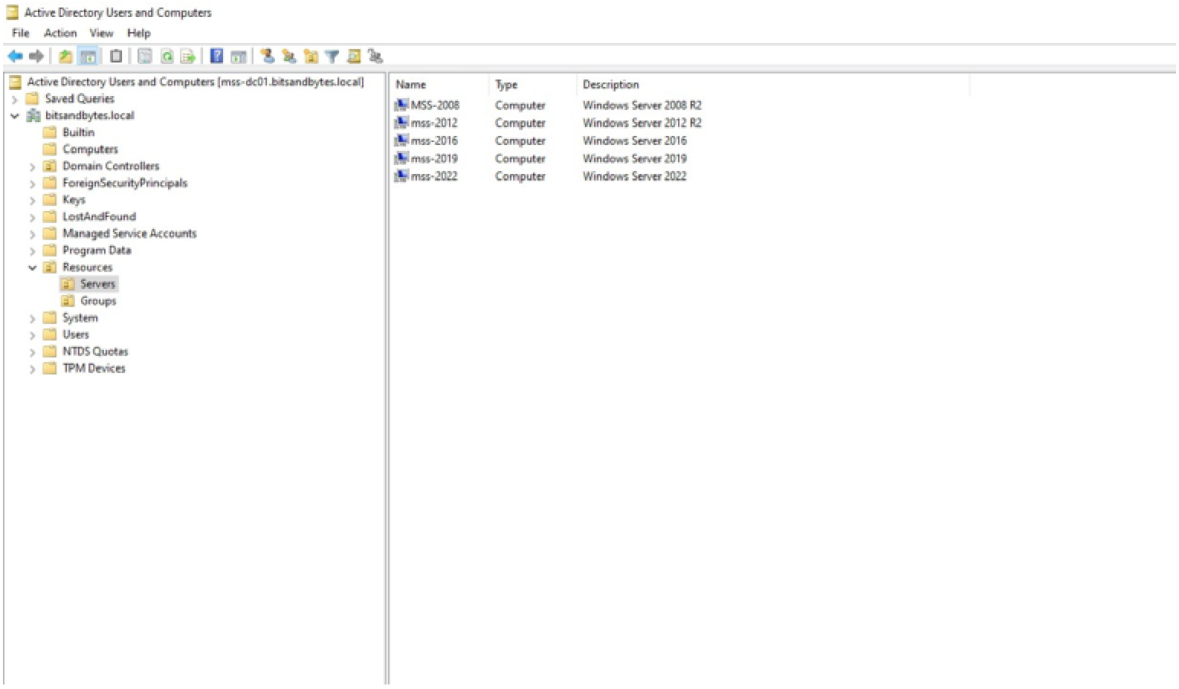
Attributes:

Attribute	Value
msLAPS-EncryptedP...	<not set>
msLAPS-EncryptedP...	<not set>
msLAPS-Password	<not set>
msLAPS-PasswordEx...	<not set>
ms-Mcs-AdmPwd	L'%A2f9@UPZiEYJY)iJ5$thA5KIMn,[9WC,8;
ms-Mcs-AdmPwdExpi...	9/24/2023 2:58:38 PM W. Europe Daylight
mSMQDigests	<not set>
mSMQDigestsMig	<not set>
mSMQSignCertificates	<not set>
mSMQSignCertificate...	<not set>
msNPAllowDialin	<not set>
msNPCallingStationID	<not set>
msNPSavedCallingSt...	<not set>
msPKIAccountCrede...	<not set>

What about Windows Server 2019 and 2022?

Within Windows Server 2019 (April Update) and 2022, Microsoft LAPS in built-in by default. You don't need to install some agents or extenstions. Also, within the Event Viewer, you can find some LAPS logging to see if all the configuration is working fine.

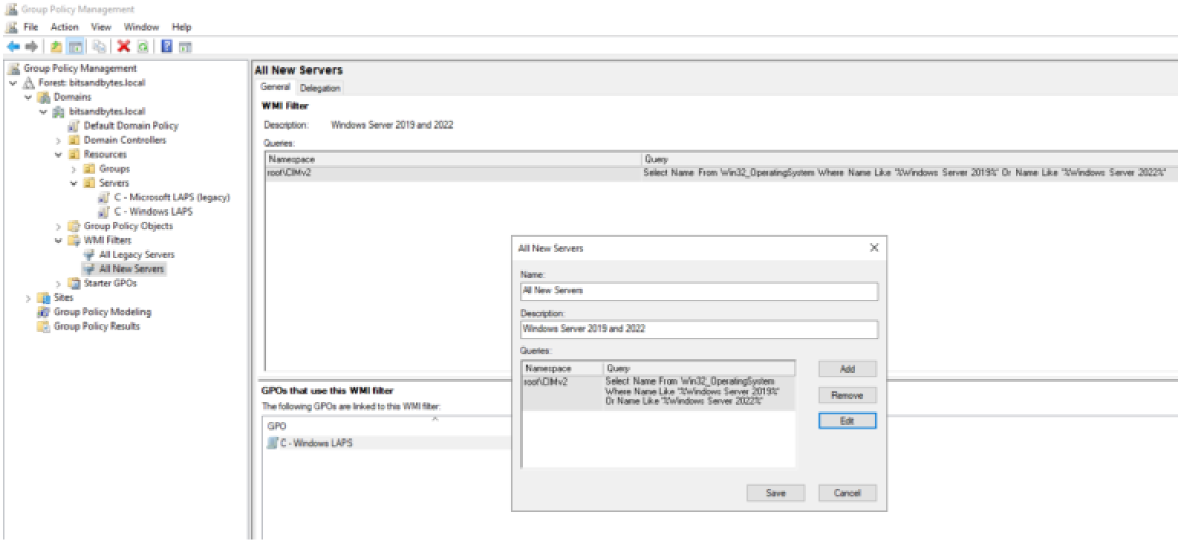
I've joined to newly created servers to my Active Directory environment called 'mss-2019' Windows Server 2019 and 'mss-2022' Windows Server 2022.



Name	Type	Description
MSS-2008	Computer	Windows Server 2008 R2
mss-2012	Computer	Windows Server 2012 R2
mss-2016	Computer	Windows Server 2016
mss-2019	Computer	Windows Server 2019
mss-2022	Computer	Windows Server 2022

I've created a WMI filter that filters based on the operation system.

> For Windows Server 2019 (April Update and higher) and 2022
> Select Name From Win32_OperatingSystem Where Name Like '%Windows Server 2019%' Or Name Like '%Windows Server 2022%'



All New Servers

WMI Filter

Description: Windows Server 2019 and 2022

Queries:

Namespace	Query
root\CIMv2	Select Name From Win32_OperatingSystem Where Name Like '%Windows Server 2019%' Or Name Like '%Windows Server 2022%'

GPOs that use this WMI filter

The following GPOs are linked to this WMI filter:

GPO
C - Windows LAPS

All New Servers

Name: All New Servers

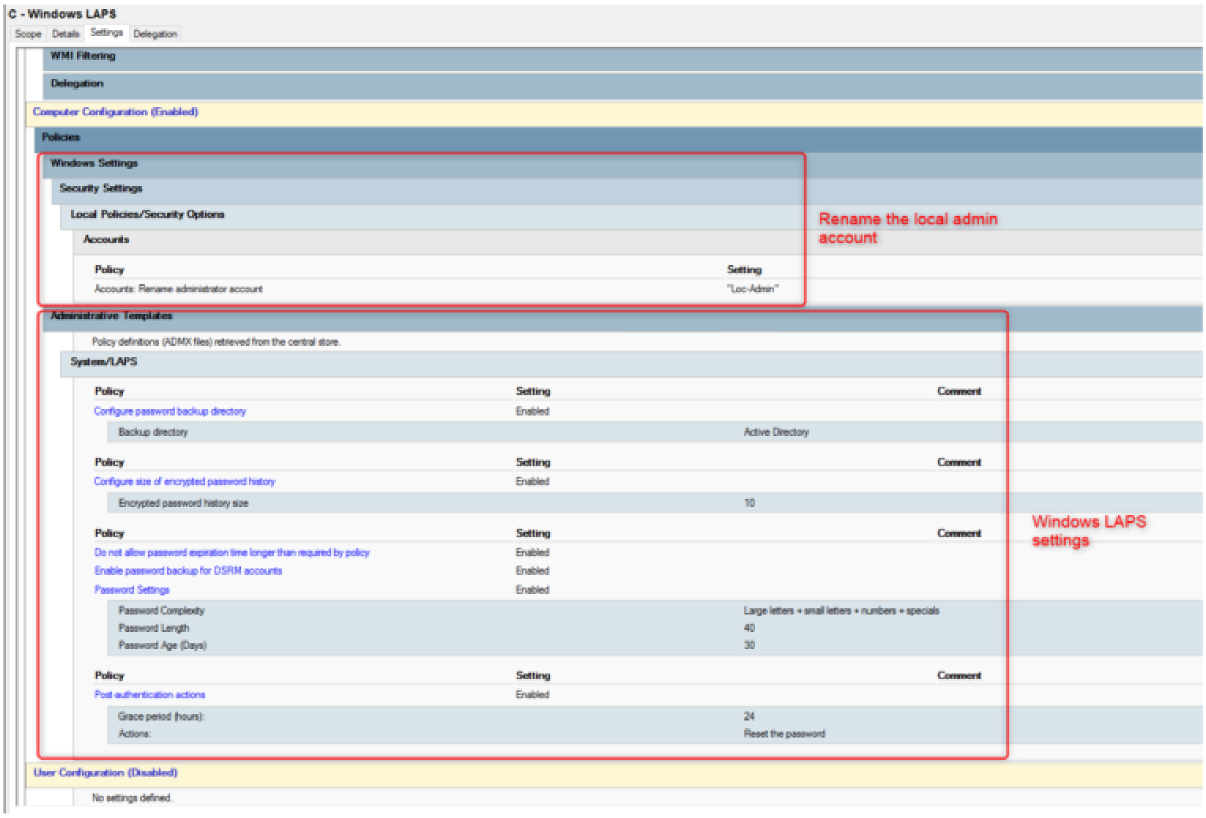
Description: Windows Server 2019 and 2022

Queries:

Namespace	Query
root\CIMv2	Select Name From Win32_OperatingSystem Where Name Like '%Windows Server 2019%' Or Name Like '%Windows Server 2022%'

Next step is to create a group policy for the modern operating systems.

> For Windows Server 2019 (April Update and higher) and 2022
> Select Name From Win32_OperatingSystem Where Name Like ‘%Windows Server 2019%’ Or Name Like ‘%Windows Server 2022%’



C - Windows LAPS

WMI Filtering

Delegation

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Local Policies/Security Options

Accounts

Policy	Setting
Accounts: Rename administrator account	"Loc-Admin"

Rename the local admin account

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

System/LAPS

Policy	Setting		Comment
Configure password backup directory	Enabled		
Backup directory		Active Directory	

Policy	Setting		Comment
Configure size of encrypted password history	Enabled		
Encrypted password history size		10	

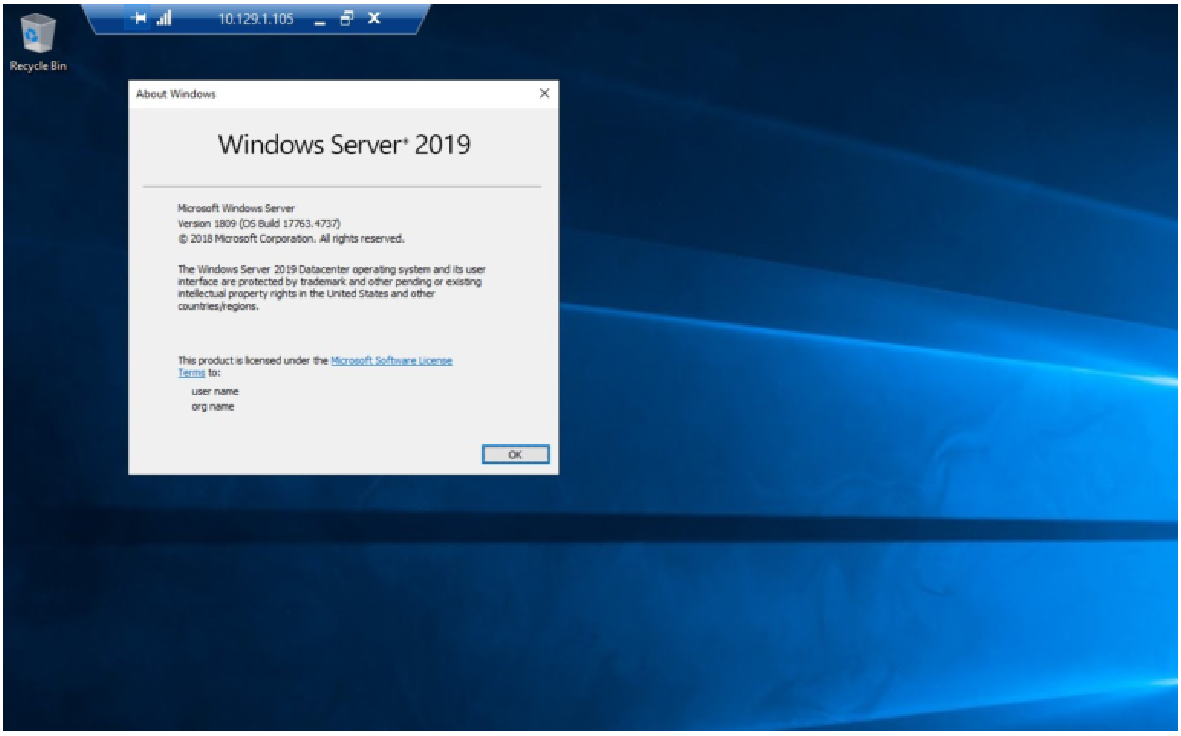
Policy	Setting		Comment
Do not allow password expiration time longer than required by policy	Enabled		
Enable password backup for DSRM accounts	Enabled		
Password Settings	Enabled		
Password Complexity		Large letters + small letters + numbers + specials	
Password Length		40	
Password Age (Days)		30	

Policy	Setting		Comment
Post-authentication actions	Enabled		
Grace period (hours):		24	
Actions:		Reset the password	

Windows LAPS settings

User Configuration (Disabled)

No settings defined.



About Windows

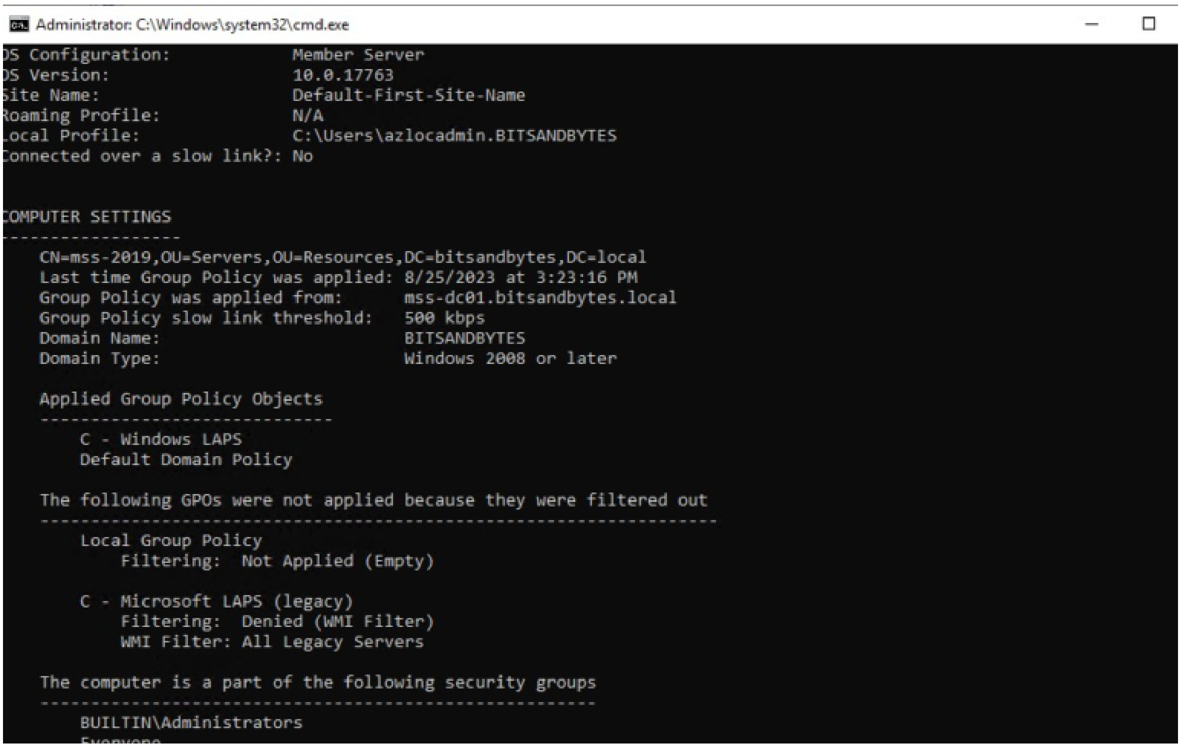
Windows Server® 2019

Microsoft Windows Server
Version 1809 (OS Build 17763.4737)
© 2018 Microsoft Corporation. All rights reserved.

The Windows Server 2019 Datacenter operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

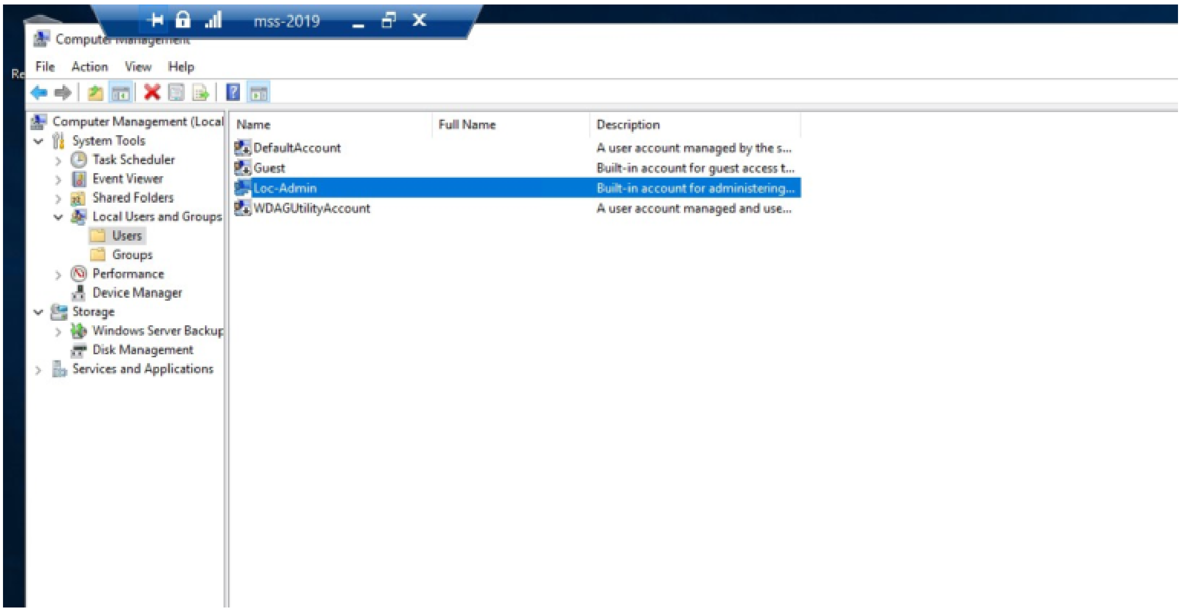
This product is licensed under the Microsoft Software License Terms to:

user name
org name

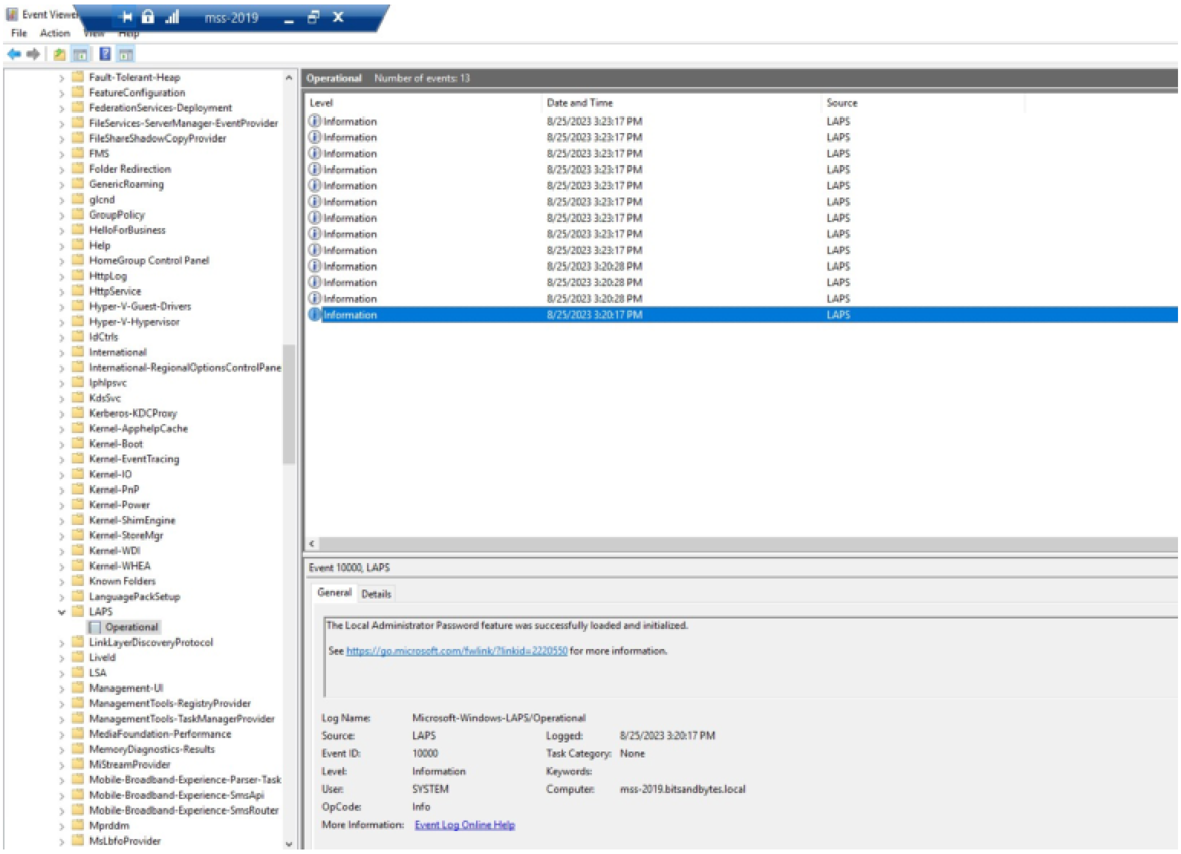


Administrator: C:\Windows\system32\cmd.exe

```
OS Configuration:            Member Server
OS Version:                  10.0.17763
Site Name:                   Default-First-Site-Name
Roaming Profile:             N/A
Local Profile:               C:\Users\azlocadmin.BITSANDBYTES
Connected over a slow link?: No


COMPUTER SETTINGS
-----------------
    CN=mss-2019,OU=Servers,OU=Resources,DC=bitsandbytes,DC=local
    Last time Group Policy was applied: 8/25/2023 at 3:23:16 PM
    Group Policy was applied from:      mss-dc01.bitsandbytes.local
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        BITSANDBYTES
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    ----------------------------
        C - Windows LAPS
        Default Domain Policy

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)

        C - Microsoft LAPS (legacy)
            Filtering:  Denied (WMI Filter)
            WMI Filter: All Legacy Servers

    The computer is a part of the following security groups
    -------------------------------------------------------
        BUILTIN\Administrators
        Everyone
```



Name	Full Name	Description
DefaultAccount		A user account managed by the s...
Guest		Built-in account for guest access t...
Loc-Admin		Built-in account for administering...
WDAGUtilityAccount		A user account managed and use...



Operational Number of events: 13

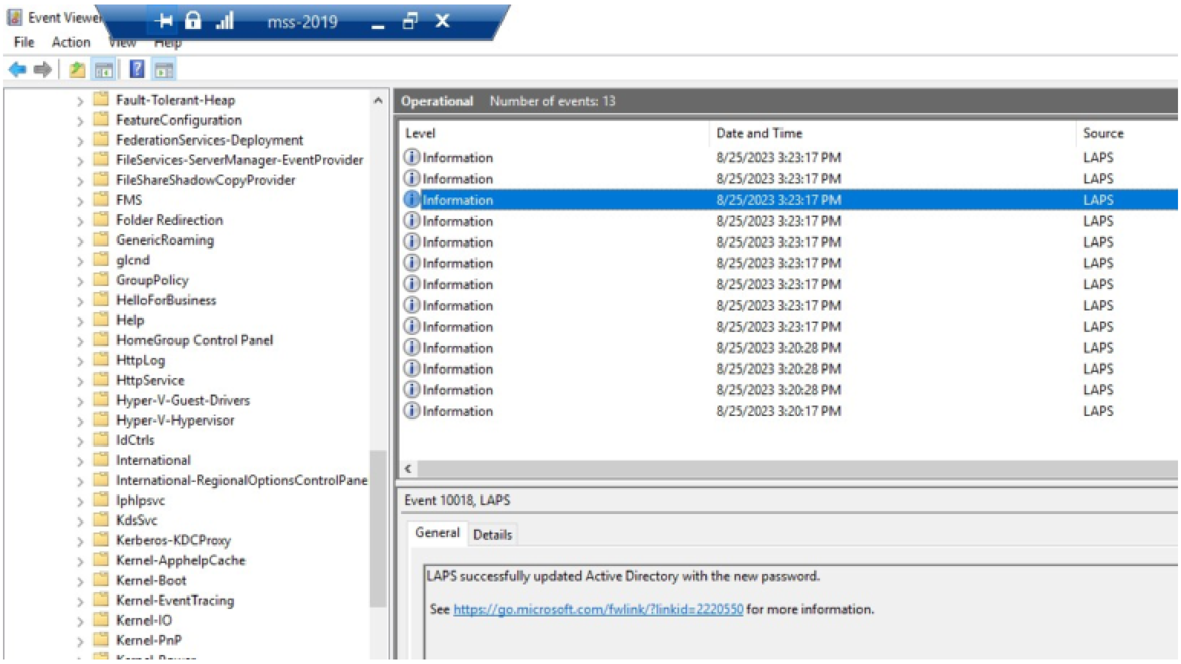
Level	Date and Time	Source
Information	8/25/2023 3:23:17 PM	LAPS
Information	8/25/2023 3:23:17 PM	LAPS
Information	8/25/2023 3:23:17 PM	LAPS
Information	8/25/2023 3:23:17 PM	LAPS
Information	8/25/2023 3:23:17 PM	LAPS
Information	8/25/2023 3:23:17 PM	LAPS
Information	8/25/2023 3:23:17 PM	LAPS
Information	8/25/2023 3:23:17 PM	LAPS
Information	8/25/2023 3:23:17 PM	LAPS
Information	8/25/2023 3:20:28 PM	LAPS
Information	8/25/2023 3:20:28 PM	LAPS
Information	8/25/2023 3:20:28 PM	LAPS
Information	8/25/2023 3:20:17 PM	LAPS

Event 10000, LAPS

The Local Administrator Password feature was successfully loaded and initialized.

See https://go.microsoft.com/fwlink/?linkid=2220550 for more information.

Log Name:	Microsoft-Windows-LAPS/Operational		
Source:	LAPS	Logged:	8/25/2023 3:20:17 PM
Event ID:	10000	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	mss-2019.bitsandbytes.local
OpCode:	Info		
More Information:	Event Log Online Help		



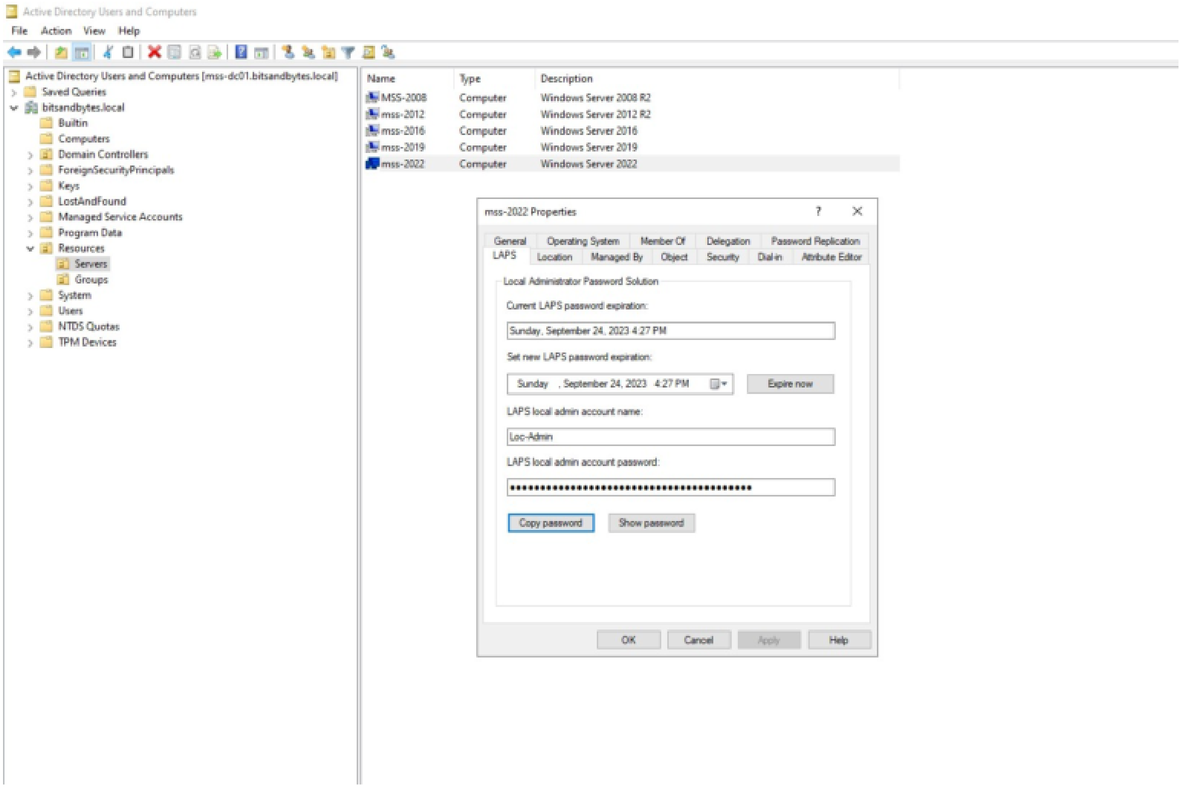
Operational Number of events: 13

Level	Date and Time	Source
Information	8/25/2023 3:23:17 PM	LAPS
Information	8/25/2023 3:23:17 PM	LAPS
Information	8/25/2023 3:23:17 PM	LAPS
Information	8/25/2023 3:23:17 PM	LAPS
Information	8/25/2023 3:23:17 PM	LAPS
Information	8/25/2023 3:23:17 PM	LAPS
Information	8/25/2023 3:23:17 PM	LAPS
Information	8/25/2023 3:23:17 PM	LAPS
Information	8/25/2023 3:23:17 PM	LAPS
Information	8/25/2023 3:20:28 PM	LAPS
Information	8/25/2023 3:20:28 PM	LAPS
Information	8/25/2023 3:20:28 PM	LAPS
Information	8/25/2023 3:20:17 PM	LAPS

Event 10018, LAPS

LAPS successfully updated Active Directory with the new password.

See https://go.microsoft.com/fwlink/?linkid=2220550 for more information.


Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [mss-dc01.bitsandbytes.local]
Saved Queries
bitsandbytes.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Keys
LostAndFound
Managed Service Accounts
Program Data
Resources
Servers
Groups
System
Users
NTDS Quotas
TPM Devices

Name	Type	Description
MSS-2008	Computer	Windows Server 2008 R2
mss-2012	Computer	Windows Server 2012 R2
mss-2016	Computer	Windows Server 2016
mss-2019	Computer	Windows Server 2019
mss-2022	Computer	Windows Server 2022

mss-2022 Properties

General Operating System Member Of Delegation Password Replication
LAPS Location Managed By Object Security Dial-in Attribute Editor

Local Administrator Password Solution

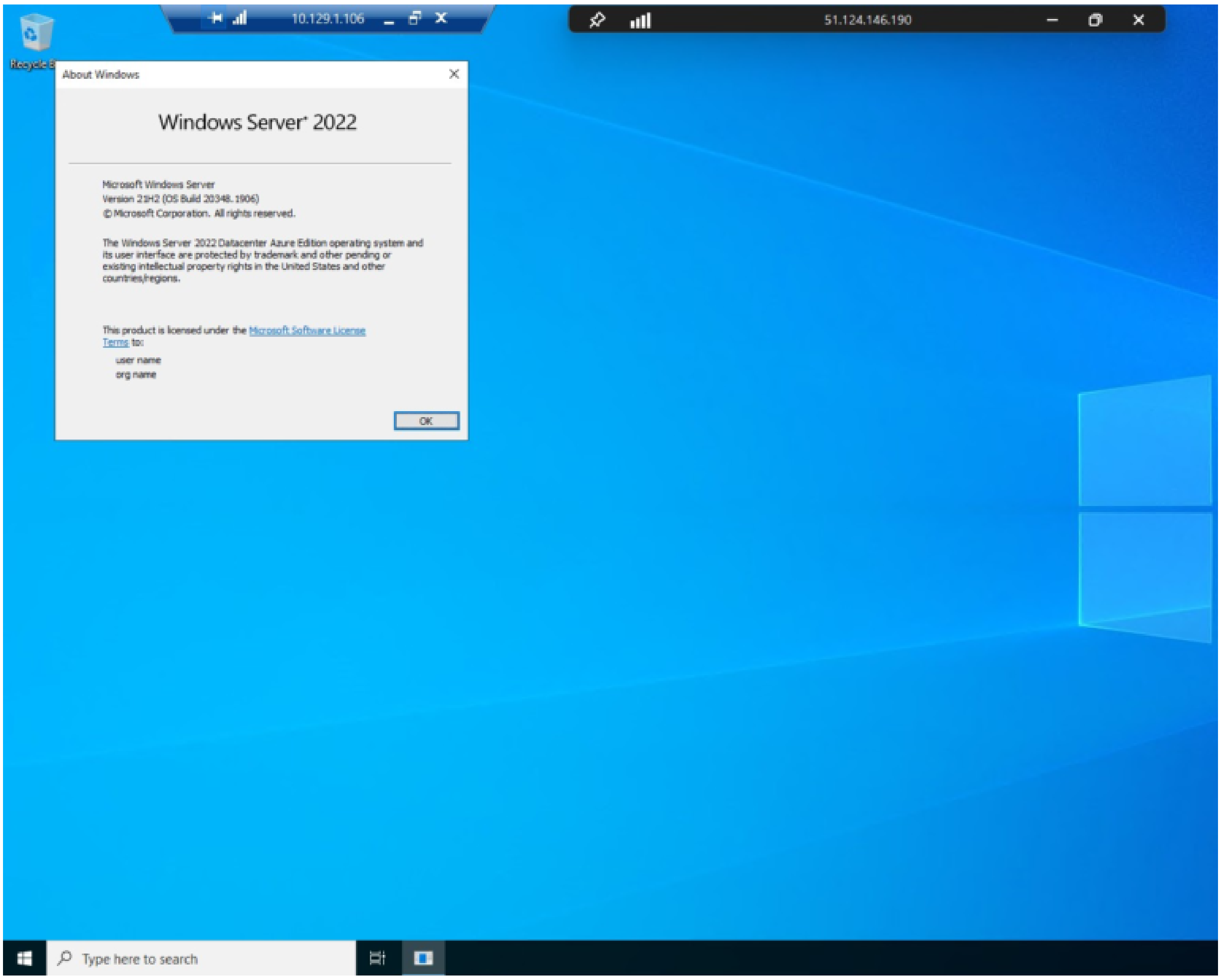
Current LAPS password expiration:
Sunday, September 24, 2023 4:27 PM

Set new LAPS password expiration:
Sunday , September 24, 2023 4:27 PM

LAPS local admin account name:
Loc-Admin

LAPS local admin account password:
••

When opening Active Directory Users & Computers, you see directly the ‘LAPS’ tab. Here you can find the local admin usersname and the newly applied password. And yes, you can login with the new account!!



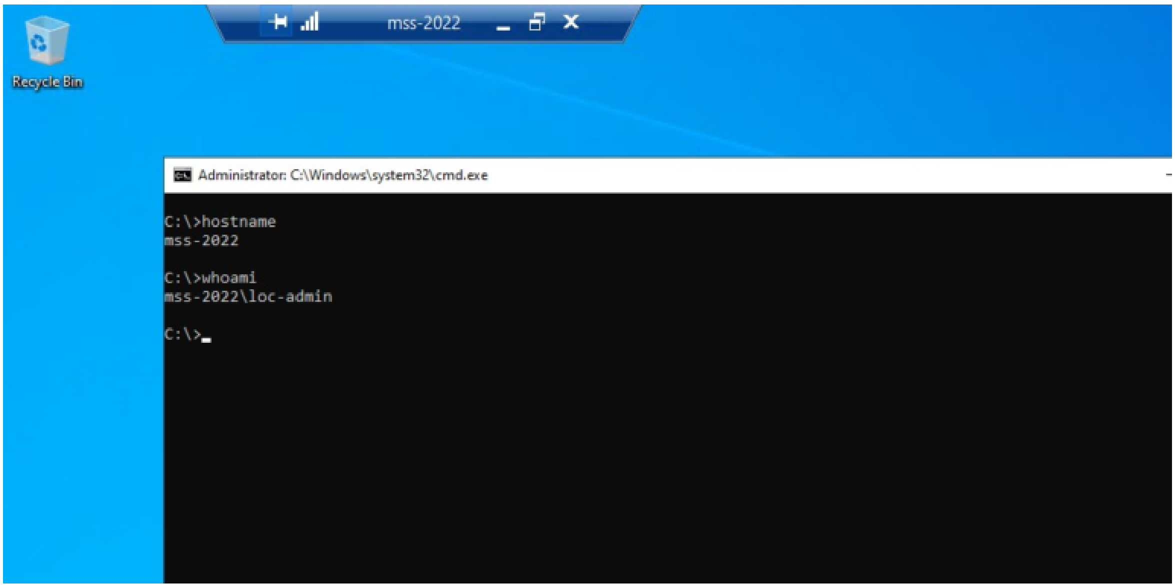
About Windows

Windows Server 2022

Microsoft Windows Server
Version 21H2 (OS Build 20348.1906)
© Microsoft Corporation. All rights reserved.

The Windows Server 2022 Datacenter Azure Edition operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

This product is licensed under the Microsoft Software License Terms to:
user name
org name



```
C:\>hostname
mss-2022

C:\>whoami
mss-2022\loc-admin

C:\>_
```

Wrap up

In this post we've succesfully prepared our environment for Microsoft LAPS (legacy) and the new Windows LAPS. We've configured the right group policies (these are my own settings! Review and choose you're own baseline).

After the GPO's are applied, the new settings are live and we can sign-in with RDP to our Windows servers. Hopefully this blogpost was usefull! If you have any questions or comments, please feel free to reach out to me.