TECHNINE
SMB TECHNOLOGY USER GROUP

TECHNINE
SMB TECHNOLOGY USER GROUP

Bart Bultinck
bart@integreat.be
@evilbart

Microsoft

TECHNiNE

SMB TECHNOLOGY USER GROUP

LAPS – Local Admin Password Solution

Microsoft Security Advisory - 3062591

1 may 2015

Microsoft

BAD HABITS

- Bad habits:
  - Excessive alcohol
  - Smoking
  - Every pc same administrator password

SOLUTION : LAPS

- Solution for:
  - AD joined computers
- Authorize which users are authorized to read and reset passwords

- Can LAPS manage a local administrator account not named “administrator”?
  - » Yes.

HOW DOES LAPS WORK

- **How does LAPS work?**
- The core of the LAPS solution is a GPO client-side extension (CSE) that performs the following tasks and can enforce the following actions during a GPO update:

- Checks whether the password of the local Administrator account has expired.
- Generates a new password when the old password is either expired or is required to be changed prior to expiration.
- Validates the new password against the password policy.
- Reports the password to Active Directory, storing it with a confidential attribute with the computer account in Active Directory.
- Reports the next expiration time for the password to Active Directory, storing it with an attribute with the computer account in Active Directory.
- Changes the password of the Administrator account.

LAPS - FEATURES

- Randomly generate passwords that are automatically changed on managed machines.
- Effectively mitigate PtH attacks that rely on identical local account passwords.
- Enforced password protection during transport via encryption using the Kerberos version 5 protocol.
- Use access control lists (ACLs) to protect passwords in Active Directory and easily implement a detailed security model.
- Configure password parameters, including age, complexity, and length.
- Force password reset on a per-machine basis.
- Use a security model that is integrated with ACLs in Active Directory.
- Use any Active Directory management tool of choice; custom tools, such as Windows PowerShell, are provided.
- Protect against computer account deletion.
- Easily implement the solution with a minimal footprint.

LAPS - REQUIREMENTS

- Active Directory:
  - Windows Server 2003 Service Pack 1 (SP1) or later.
- Managed machines:
  - Windows Server 2003 SP2 or later, or Windows Server 2003 x64 Edition SP2 or later.
- NO windows XP !

- Management tools:
  - .NET Framework 4.0
  - Windows PowerShell 2.0 or later

LAPS - IMPLEMENTATION

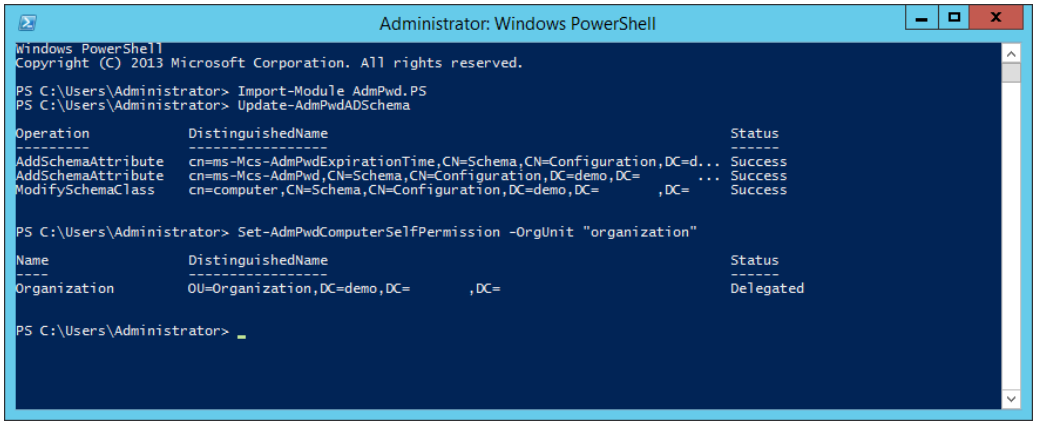
- 1. download laps ☺
  - https://www.microsoft.com/en-us/download/details.aspx?id=46899

Version:	Date Published:
6.1	7/7/2015
File Name:	**File Size:**
LAPS.x64.msi	956 KB
LAPS.x86.msi	932 KB
LAPS_Datasheet.docx	100 KB
LAPS_OperationsGuide.docx	589 KB
LAPS_TechnicalSpecification.docx	71 KB

LAPS – IMPLEMENTATION – EXTENDING AD

- 2. Extending the Active Directory schema
- The first atribute is used to store the password of the built-in Administrator account for each device
  - (**ms-Mcs-AdmPwd**)
- The second attribute is used to store the timestamp of password expiration
  - (**ms-Mcs-AdmPwdExpirationTime**).
- When using RODC – beware !:
  - change the 10th bit of the **searchFlags** attribute value for **ms-Mcs-AdmPwd** schema object to **0** (substract 512 from the current value of the searchFlags attribute) to add it to the Filtered Attribute Set.

LAPS IMPLEMENTATION – ALLOW DEVICES TO WRITE PASSWORDS

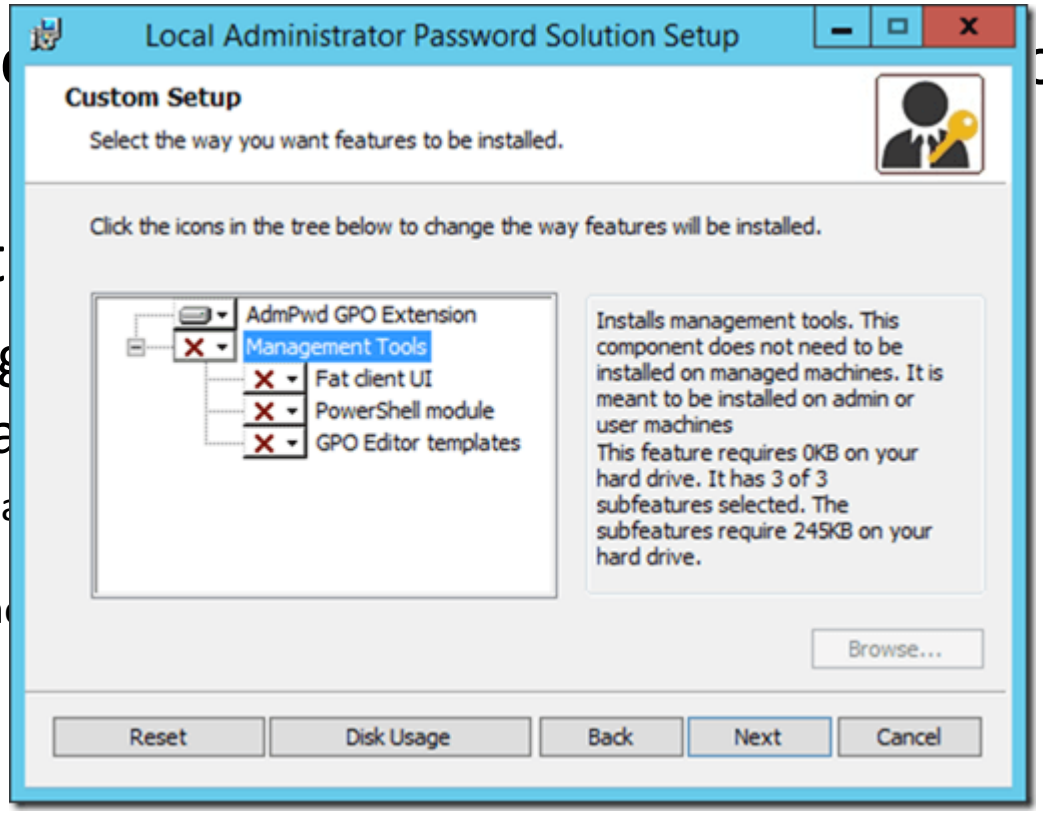
- The Write permission on the ms-Mcs-AdmPwd and ms-Mcs-AdmPwdExpirationTime attributes of all computer accounts has to be added to the SELF built-in account. This is also done using PowerShell, per Organizational Unit (OU):
  - **Set-AdmPwdComputerSelfPermission -OrgUnit** "*OU ShortName*"
- 

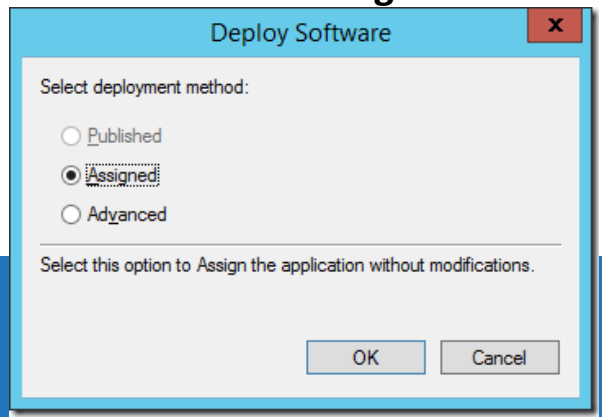
- You do not have to run this command for Organizational Units (OUs) that are subcontainers of configured Organizational Units (OUs).

Microsoft

LAPS – INSTALL CSE ON CLIENT DEVICES

- The laps client si… every pc !
- Easy : deploy wit…
  - Computer Config… Software Installa…
  - right-click every Organiza… want to assign the Local … **Existing GPO…** to link th…





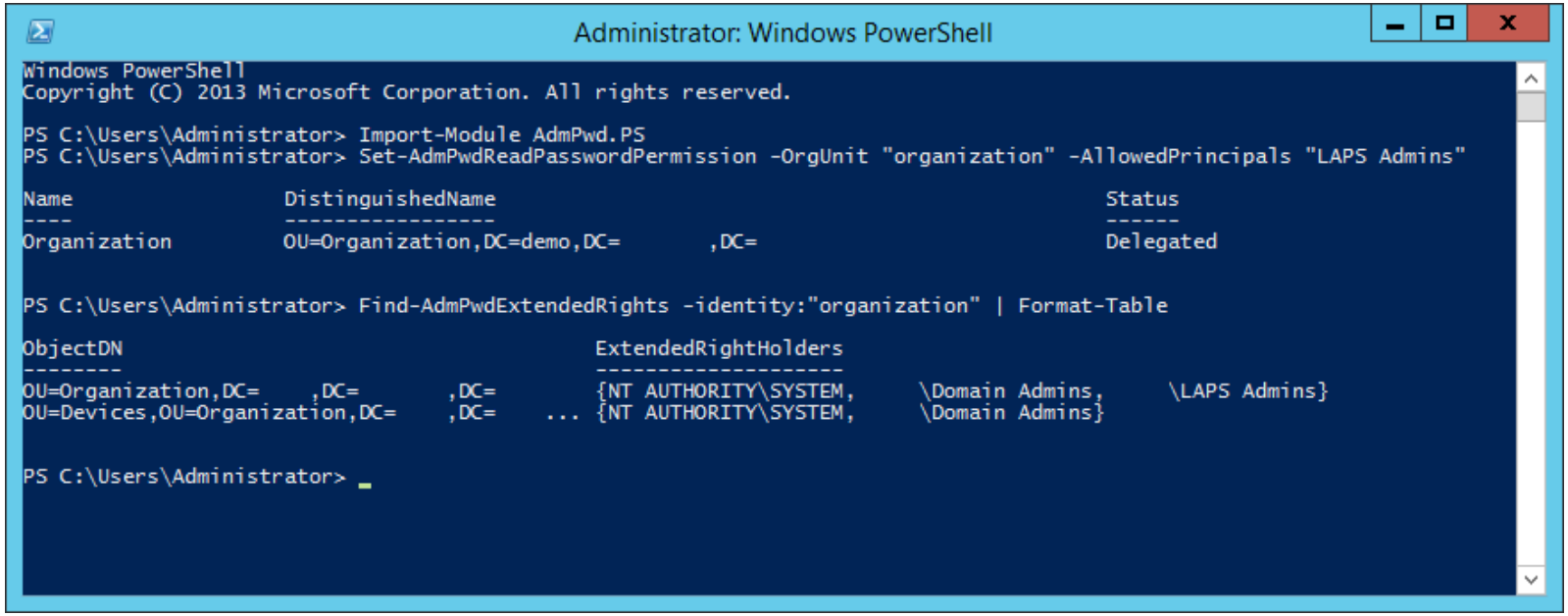
Microsoft

LAPS – DELEGATING ACCESS

- By default, members of the **Enterprise Admins** and **Domain Admins** groups have access to the attributes.
- Fortunately, you can granularly delegate access to the password values. You can even remove the **Enterprise Admins** and **Domain Admins** groups, although Microsoft didn't test this scenario.
- **Set-AdmPwdReadPasswordPermission -OrgUnit** "*OU ShortName*" **-AllowedPrincipals** "*users or groups shortname*"

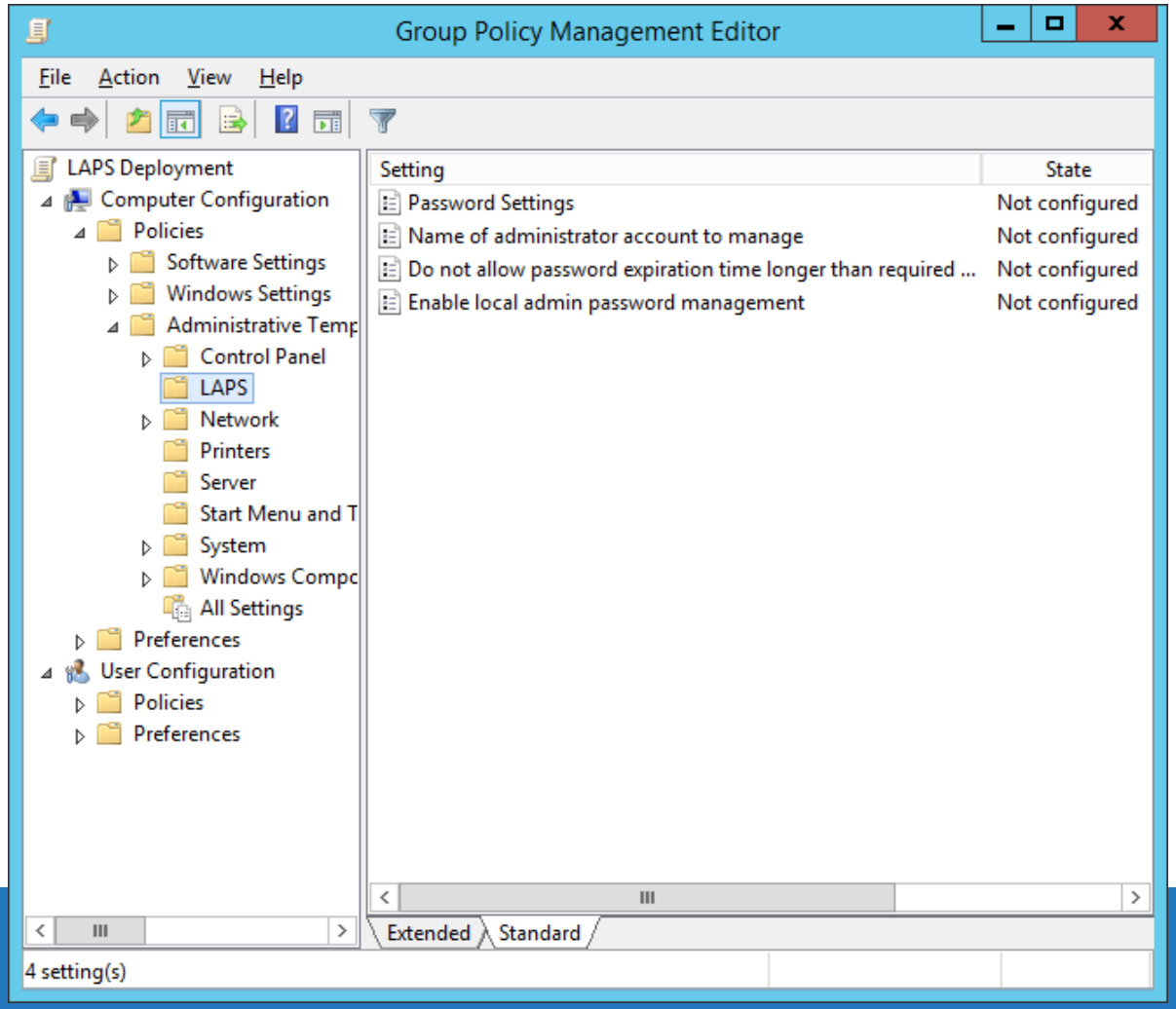
LAPS – DELEGATING ACCESS

- **Find-AdmPwdExtendedRights -identity:"***OU Shortname***" | Format-Table**



Microsoft

LAPS - MANAGEMENT



- Details: next slide
- ☺

Microsoft

LAPS - MANAGEMENT

- To manage password settings, first, enable the **Enable local admin password management** Group Policy setting.
  Its default setting is **Not Configured**.

- Then, open the **Password Settings** Group Policy setting and select appropriate settings for the local administrator passwords.
  Options include
  - password complexity
  - password length
  - password age (in days).

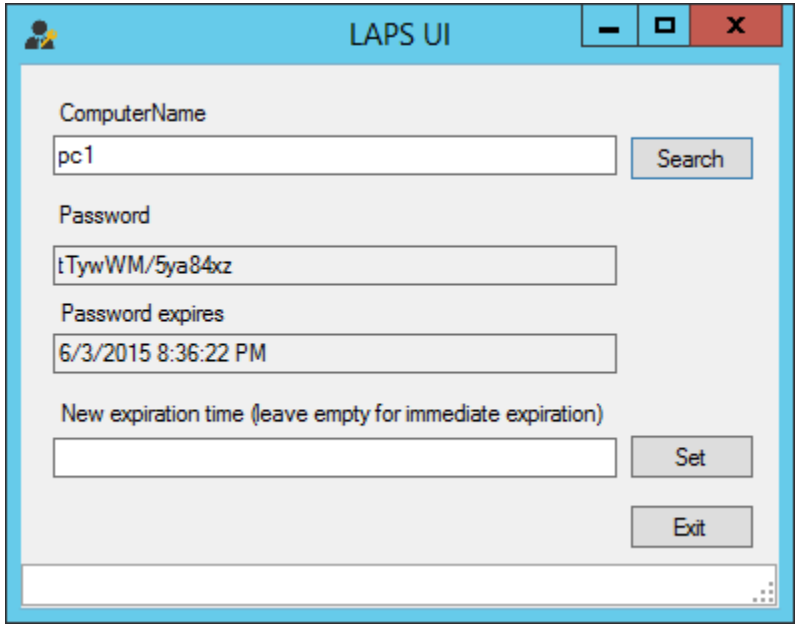
- The **Do not allow password expiration time longer than required by policy** Group Policy setting, when enabled, will make the Local Administrator Password Solution (LAPS) change passwords before they expire (as configured in the previous **Password Settings** Group Policy setting).

- The **Name of the administrator account to manage** Group Policy setting allows you to manage **custom local administrator accounts**.
  You do not need to use this setting when you have renamed the local administrator account (LAPS detects the local administrator account using its RID).

- Instead, you can use this setting for any of your own local administrator account when you've opted for one and kept the local administrator accounts on devices disabled.

LAPS – READING PASSWORDS

- LAPS UI



- POWERSHELL:
  - **Get-AdmPwdPassword cmdlet**
- **Auditing read permission usage**
  - The Local Administrator Password Solution (LAPS) also has granular accounting as a feature.
- **Set-AdmPwdAuditing -OrgUnit "***OU ShortName***" -AuditedPrincipals "***users or groups shortname***"**

LAPS – REQUIRED READING

- https://dirteam.com/sander/2015/05/02/security-thoughts-microsoft-local-administrator-password-solution-laps-kb3062591/
- https://4sysops.com/?s=LAPS

- Questions?

- Pause !