ICT POWER.IT

Microsoft

#POWERCON2023

Implementare e gestire Windows LAPS

Ermanno Goletto
Microsoft MVP Alumni
e.goletto@outlook.it

/devadmin.it
@ermannog
/ermannogoletto

Roberto Massa
Microsoft MVP Alumni
robimassa@outlook.it

/robi.massa.cn
@robi_massa
/robimassa

Speaker

Ermanno Goletto è **laureato in Ingegneria Elettronica** al Politecnico di Torino e **nel 1997 inizia a lavorare nel campo dell'Information Tecnology** presso aziende informatiche occupandosi di **progettazione e sviluppo di applicazioni, amministrazione di database, architettura di sistema e sicurezza su piattaforma Microsoft**

Attualmente in qualità di **Funzionario Informatico presso una Pubblica Amministrazione locale amministra l'infrastruttura informatica e si occupa della gestione della sicurezza informatica**

Ermanno è **certificato sulle tecnologie Microsoft dal 2004** (MCP, MCSA, MCTS su .NET, Exchange, SQL Server e SharePoint, MCITP su Windows Server e Virtualization, MCSE Server Infrastructure), fa parte dello **staff della community IT Pro ICTPower.it** e **collabora con la community Torino Technologies Group**

Microsoft MVP dal 2008 al 2018 nelle categorie Directory Services, Cloud and Datacenter Management e Enterprise Mobility, attualmente è **MVP Alumni** e **dal 2010 interviene come speaker in conferenze ed eventi dedicati al mondo ICT**

Speaker

Roberto Massa si occupa di Informatica dal 1989 nella **gestione di sistemi distribuiti in ambito networking in ambienti Windows Server, Linux, e Netware**, ha approfondito la conoscenza di **sistemi di monitoraggio Open-Source in particolare Nagios e Zenoss**

Attualmente è **Sistemista presso l'Azienda Ospedaliera S. Croce e Carle di Cuneo** dove si occupa anche delle analisi e delle implementazioni di soluzioni legate alla sicurezza dell'infrastruttura

Roberto è **certificato sulle tecnologie Microsoft Hyper-V** e da alcuni anni **si occupa di sicurezza** implementando soluzioni opensource basate su sistemi OpenBSD e OpenVPN ed in generale dell'**analisi di soluzioni tecniche legate alla fruizioni di applicazioni all'esterno del perimetro aziendale**

Microsoft MVP dal 2016 al 2019 per la categoria Cloud and Datacenter Management, attualmente è **MVP Alumni** e **dal 2007 partecipa come speaker ad eventi dedicati a Linux e alle tecnologie Microsoft**

Agenda

- Che cos'è LAPS?
- Funzionamento di Windows LAPS
- Deploy di Windows LAPS
- Gestione di Windows LAPS

ICT POWER.IT

Microsoft

Implementare e gestire Windows LAPS

Che cos'è LAPS?

Ermanno Goletto
Microsoft MVP Alumni
e.goletto@outlook.it

/devadmin.it
@ermannog
/ermannogoletto

Roberto Massa
Microsoft MVP Alumni
robimassa@outlook.it

/robi.massa.cn
@robi_massa
/robimassa

LAPS (Local Administrator Password Solution)

Problema: gestione della password dell'account amministratore locale in infrastrutture basata su Active Directory

Best Practice: utilizzare al posto dell'amministratore locale un account di dominio con privilegi di amministratore locale mediante l'utilizzo della ***Group Policy Preference Computer Control Panel Settings / Local Users and Groups*** **(*)** oppure tramite la ***Group Policy Computer Restricted Groups*** (**)

Bad practice: amministratore locale con la stessa password su ogni computer del dominio

Nel 2016 Microsoft rende disponibile LAPS (ora denominato Microsoft LAPS legacy), una soluzione per automatizzare la gestione della password dell'account che consente di:

- **gestire una password randomica per l'amministratore locale differente su ogni computer** generata localmente senza necessità di un generatore centralizzato di password;
- gestire tramite una GPO client-side extension (CSE) il **nome del local administrator account**, il **periodo di rinnovo** e la **lunghezza e complessità della password**;
- automatizzare la gestione della password dell'amministratore locale tramite una serie di cmdlet PowerShell

(*) Group Policy: Creating A Standard Local Admin Account | Microsoft Learn

(**) KB279301 - Description of group policy restricted groups - Windows Server | Microsoft Learn

Windows LAPS

Rilasciato tramite Windows Updates l'11 aprile 2023 per tutte le edizioni (LTSC compreso) di Windows 11 22H2 e 21H2, Windows 10, Windows Server 2022 e 2019

Windows LAPS è un'**implementazione nativa** disponibile gratuitamente in tutte le versioni di Windows supportate che eredita molti concetti di progettazione da Microsoft LAPS legacy

Windows LAPS aggiunge funzionalità non sono disponibili in Microsoft LAPS legacy:

- **Backup delle password in Azure Active Directory** (è possibile utilizzare Azure AD Free o superiore)
- **Crittografia delle password in Windows Server Active Directory**
- **Archivio della cronologia delle password**

Windows LAPS **non richiede l'installazione di Microsoft LAPS legacy**

Per eseguire la migrazione di una distribuzione Microsoft LAPS legacy esistente, Windows LAPS offre la modalità di emulazione Microsoft LAPS legacy (supporta l'archiviazione delle password in Windows Server Active Directory solo in formato clear-text)

Windows LAPS overview | Microsoft Learn

Get started with Windows LAPS in legacy Microsoft LAPS emulation mode | Microsoft Learn

Restrizioni e limitazioni di Windows LAPS

- Può essere utilizzato **solo con dispositivi a dominio**
- Può gestire la password **di un solo account amministratore locale**
- **Richiede un'estensione delle schema di Active Directory**
- **Su tutti i dispositivi deve essere presente il client di LAPS**
- Non funziona se Windows viene avviato in Safe mode o DSRM mode
- I dispositivi aggiunti solo ad Azure Active Directory possono eseguire il backup delle password solo in Azure Active Directory
- I dispositivi aggiunti solo a Windows Server Active Directory possono eseguire il backup delle password solo in Windows Server Active Directory
- I dispositivi hybrid-joined (aggiunti sia ad Azure Active Directory che Windows Server Active Directory) possono eseguire il backup delle password in Azure Active Directory o in Windows Server Active Directory, **non è possibile eseguire il backup delle password in Azure Active Directory e Windows Server Active Directory**
- **Windows LAPS non supporta gli Azure Active Directory workplace-joined clients**

Windows LAPS overview | Microsoft Learn
Windows LAPS frequently asked questions | Microsoft Learn
Key concepts in Windows LAPS | Microsoft Learn
Join to Workplace from Any Device for SSO and Seamless Second Factor Authentication Across Company Applications | Microsoft Learn

Rischi di sicurezza se non si implementa LAPS

Quando i client usano la **stessa combinazione di account e password locale amministrativa** vi è il **rischio di attacchi pass-the-hash e lateral-traversal**

Se un utente malintenzionato ottiene delle credenziali di amministratore locale comuni a più workstation può tentare di usare tool come Mimikatz o simili per eseguire il dump delle credenziali di accesso recenti allo scopo di ottenere credenziali di un utente Domain Admin

L'accesso a un computer con un account Domain Admin, o l'immissione delle credenziali di amministratore di dominio con RunAs, inserisce le credenziali in LSASS e **un utente malintenzionato con diritti di amministratore locale su questo computer può scaricare le credenziali da LSASS e riutilizzarle**

L'utilizzo di account locali durante un attacco non viene registrato sui controller di dominio, inoltre poche organizzazioni inviano i logs di sicurezza delle workstation a un sistema di registrazione centrale (SIEM)

Se sono presenti servizi distribuiti su tutte le workstation o in tutti i server che vengono eseguiti nel contesto di un account di servizio con diritti di amministratore di dominio, è necessario che un solo sistema venga compromesso per compromettere l'intero dominio di Active Directory, quando un servizio viene avviato con credenziali esplicite, le credenziali vengono caricate in LSASS quindi un utente malintenzionato con privilegi di amministratore locale può scaricare le credenziali da LSASS e riutilizzarle

Attack Methods for Gaining Domain Admin Rights in Active Directory – Active Directory Security (adsecurity.org)

Attacks & Defenses: Dumping LSASS W/ No Mimikatz | White Oak (whiteoaksecurity.com)

Benefici di Windows LAPS e scenari d'uso

- Protezione contro gli **attacchi pass-the-hash e lateral-traversal**
- Miglioramento della sicurezza migliorata per gli scenari di **help desk remoto**
- Possibilità di accedere e ripristinare dispositivi altrimenti inaccessibili
- **Modello di sicurezza granulare** (access control lists e crittografia delle password facoltativa) **per proteggere le password archiviate in Windows Server Active Directory**
- **Supporto per il modello di controllo degli accessi basato sui ruoli di Azure per proteggere le password archiviate in Azure Active Directory**

Scenari chiave di Windows LAPS

- Backup delle password dell'account amministratore locale in Azure Active Directory
- Backup delle password dell'account amministratore locale in Windows Server Active Directory
- Backup delle password dell'account DSRM dei controller di dominio in Windows Server Active Directory
- Backup delle password dell'account amministratore locale per Windows Server Active Directory usando Microsoft LAPS legacy

Windows LAPS overview | Microsoft Learn

ICT POWER.IT

Microsoft

Implementare e gestire Windows LAPS
Funzionamento di Windows LAPS

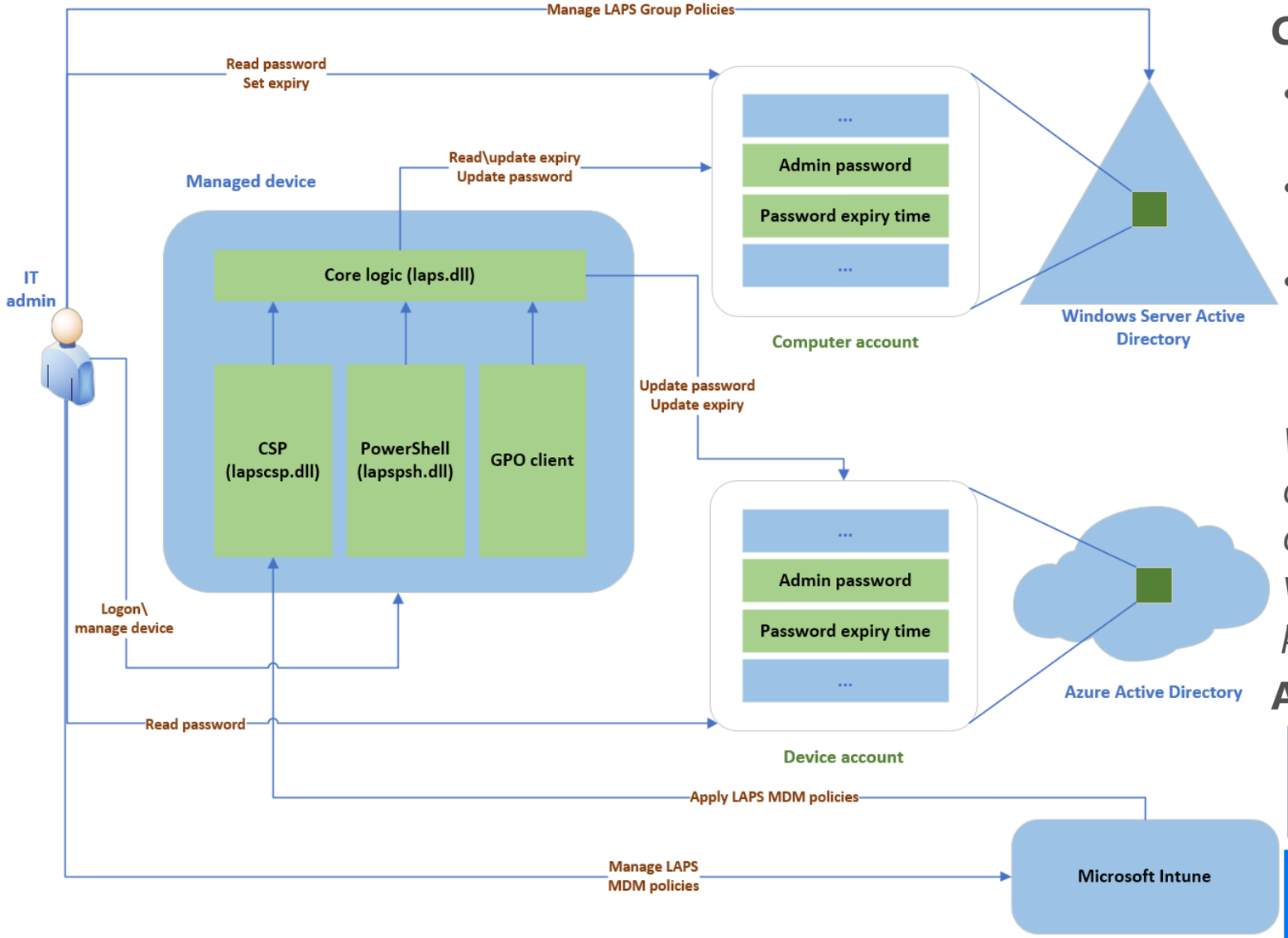
Ermanno Goletto
Microsoft MVP Alumni
e.goletto@outlook.it

/devadmin.it
@ermannog
/ermannogoletto

Roberto Massa
Microsoft MVP Alumni
robimassa@outlook.it

/robi.massa.cn
@robi_massa
/robimassa

Architettura di Windows LAPS



Configurazione dei criteri di Windows LAPS

- **Azure Active Directory-joined devices** usare **Microsoft Intune**
- **Windows Server Active Directory-joined devices** usare i **Criteri di gruppo**
- **Hybrid Azure Active Directory-joined devices** registrati con Microsoft Intune usare **Microsoft Intune**

Windows LAPS usa un'attività in background che viene riattivata ogni ora per elaborare i criteri attualmente attivi. Questa attività non viene implementata tramite Utilità di pianificazione di Windows.

Avvio manuale ciclo di elaborazione criteri

Metodo1: Forzare aggiornamento GPO
gpupdate.exe /target:computer /force

Metodo 2: via Powershell (preferibile)
Invoke-LapsPolicyProcessing

[Key concepts in Windows LAPS | Microsoft Learn]

Deep dive sull'elaborazione dei criteri

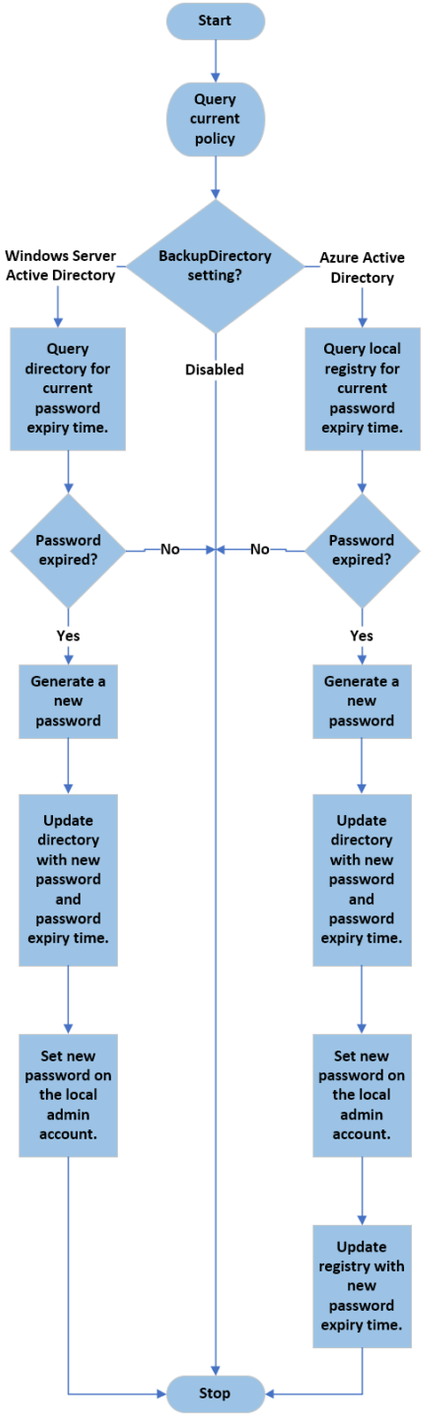
Nello scenario di Azure Active Directory il dispositivo gestito non esegue il polling di Azure Active Directory, l'ora di scadenza della password corrente viene mantenuta localmente nel dispositivo

Nello scenario di Windows Server Active Directory il dispositivo gestito esegue regolarmente il polling della directory per eseguire query sull'ora di scadenza della password e agisce alla scadenza della password

Le versioni precedenti di Microsoft LAPS (legacy Microsoft LAPS) sono basate su Group Policy (GPO) Client Side Extension (CSE), e le GPO CSE vengono caricate e richiamate in ogni ciclo di refresh delle Group Policy

La frequenza del ciclo di polling di Microsoft LAPS legacy corrisponde alla frequenza del ciclo di refresh delle Group Policy

Windows LAPS non è basato su una CSE, quindi il suo ciclo di polling è hardcoded e impostato a una volta all'ora e non è legato al ciclo di refresh delle Group Policy, ma un aggiornamento delle GPO Computer causa anche un refresh dei criteri di Windows LAPS



[Key concepts in Windows LAPS | Microsoft Learn]

LAPS AD schema extensions

L'estensione dello schema di AD aggiunge alcuni attributi all'oggetto Computer

Windows LAPS schema element	Legacy Microsoft LAPS schema element
`msLAPS-PasswordExpirationTime`	`ms-Mcs-AdmPwdExpirationTime`
`msLAPS-Password`	`ms-Mcs-AdmPwd`
`msLAPS-EncryptedPassword`	Doesn't apply
`msLAPS-EncryptedPasswordHistory`	Doesn't apply
`msLAPS-EncryptedDSRMPassword`	Doesn't apply
`msLAPS-EncryptedDSRMPasswordHistory`	Doesn't apply
`ms-LAPS-Encrypted-Password-Attributes`	Doesn't apply

E' possibile estendere lo schema di AD per utilizzare Windows LAPS tramite il cmdlet Powershell: **Update-LapsADSchema**

E' possibile estendere lo schema di AD per utilizzare Legacy Microsoft LAPS tramite il cmdlet Powershell: **Update-AdmPwdADSchema**

[Windows LAPS schema and rights extensions for Windows Server Active Directory | Microsoft Learn]

Archiviazione della password

Le password sono memorizzate nell'oggetto computer

Le password sono protette tramite le ACL definite sulla OU che contengono gli oggetti computer, è possibile specificare chi può leggere la password e chi può impostarne la scadenza tramite i cmdlet:

- **Set-LapsADReadPasswordPermission**
- **Set-LapsADResetPasswordPermission**

Se il livello funzionale di dominio è almeno WS2016 le password possono essere crittografate sul device prima di inviarle ad AD

Azure Active Directory

Le password sono memorizzate nell'Azure Active Directory device object

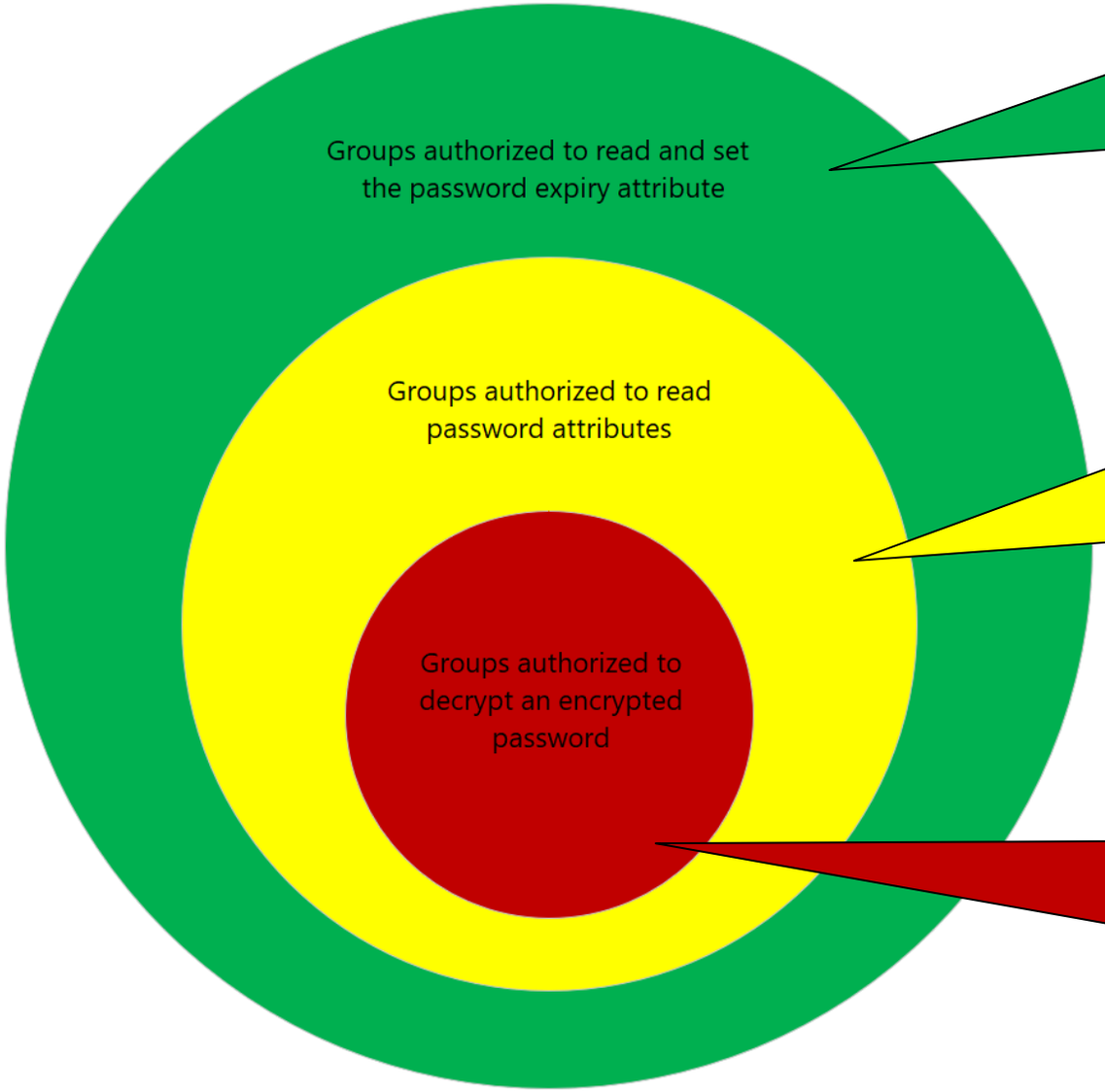
Le password vengono crittografate prima di essere memorizzate

Il layer di cifratura è rimosso prima restituire la password ai client autorizzati

Per default solo i membri dei ruoli Global Administrator, Cloud Device Administrator e Intune Administrator possono ottenere la password in chiaro

Key concepts in Windows LAPS | Microsoft Learn

User group permissions per Windows Server AD



Entità di sicurezza a cui è concessa l'autorizzazione per leggere o impostare l'attributo di scadenza della password sugli oggetti computer nella directory

Un utente malintenzionato che acquisisce questa autorizzazione può forzare i dispositivi gestiti a resettare la password più frequentemente

Entità di sicurezza a cui è concessa l'autorizzazione per leggere o impostare gli attributi della password negli oggetti computer nella directory

Riservare questo livello di autorizzazione per i membri del gruppo di sicurezza Domain Admins

Entità di sicurezza a cui sono concesse autorizzazioni di decrittografia per gli attributi delle password crittografati negli oggetti computer nella directory

Riservare questo livello di autorizzazione per i membri del gruppo Domain Admins

[Key concepts in Windows LAPS | Microsoft Learn]

Funzionalità di crittografia e cronologia password

Si basa sulla **Cryptography API: Next Generation Data Protection API** (CNG DPAPI) che supporta più modalità di crittografia, ma **Windows LAPS supporta la crittografia delle password solo in un'unica entità di sicurezza Windows Server Active Directory** (utente o gruppo) e **la crittografia si basa su AES-256**

Non sono supportate più entità perché causano un aumento delle dimensioni del buffer delle password crittografate

È possibile usare la **GPO ADPasswordEncryptionPrincipal per impostare un'entità di sicurezza per decrittografare la password**, **in caso contrario Windows LAPS solo il gruppo Domain Admins potrà decrittografare la password**, in ogni caso il dispositivo prima di crittografare una password verifica sempre che l'utente o il gruppo specificato sia risolvibile

L'entità di sicurezza autorizzata a decrittografare la password non può essere modificata dopo la crittografia di una password

Windows LAPS **quando è abilitata la crittografia delle password supporta la funzionalità di cronologia delle password** per Windows Server Active Directory

Per consentire il funzionamento della funzionalità della cronologia delle password, **al dispositivo gestito devono essere concesse autorizzazioni SELF** per leggere la versione corrente della password crittografata da Windows Server Active Directory, tale requisito viene **gestito automaticamente eseguendo il cmdlet Set-LapsADComputerSelfPermission** sulla OU che contiene gli account computer

È consigliabile non concedere mai ad un dispositivo gestito le autorizzazioni per decrittografare una password crittografata per qualsiasi dispositivo, incluso per il dispositivo stesso

[Key concepts in Windows LAPS | Microsoft Learn]

[CNG DPAPI - Win32 apps | Microsoft Learn]

Supporto delle password DSRM

- **Se è abilitata la crittografia delle password** Windows LAPS supporta il **backup della password dell'account DSRM nei controller di dominio di Windows Server**
- È possibile eseguire il backup delle password dell'account DSRM **solo per Windows Server Active Directory**
- **Il backup delle password DSRM in Azure Active Directory non è supportato**
- **La password DSRM corrente per qualsiasi controller di dominio è recuperabile se almeno un controller di dominio in tale dominio è accessibile**
- **Windows LAPS non include una strategia di backup dell'archivio esterno**

È consigliabile usare il supporto DSRM di Windows LAPS solo come primo livello di una strategia di backup e ripristino di dominio

È consigliabile estrarre regolarmente le password DSRM dalla directory ed eseguire il backup in un archivio sicuro all'esterno di Windows Server Active Directory

[Key concepts in Windows LAPS | Microsoft Learn]

Reimpostazione automatica e antimanomissione

Windows LAPS supporta la **reimpostazione automatica della password** dell'account amministratore locale **se rileva che l'account amministratore locale è stato usato per l'autenticazione tramite la GPO PostAuthenticationActions**

Tramite la GPO è possibile configurare un periodo di tolleranza (max 24 ore) per concedere a un utente di completare le azioni necessarie

La reimpostazione della password dopo l'autenticazione non è supportata per l'account DSRM nei controller di dominio

Windows LAPS protegge la password dell'account amministratore locale e dell'account DSRM in un controller di dominio Windows Server Active Directory da manomissioni accidentali o involontarie

I tentativi imprevisti di modificare la password dell'account vengono rifiutati da Windows LAPS con un errore STATUS_POLICY_CONTROLLED_ACCOUNT (0xC000A08B) o ERROR_POLICY_CONTROLLED_ACCOUNT (0x21CE\8654)

Ogni rifiuto di questo tipo è indicato con un evento 10031 nella sezione del registro eventi di Windows dedicata a LAPS

[Key concepts in Windows LAPS | Microsoft Learn]

ICT POWER.IT

Microsoft

Implementare e gestire Microsoft LAPS
Deploy di Windows LAPS

Ermanno Goletto
Microsoft MVP Alumni
e.goletto@outlook.it

/devadmin.it
@ermannog
/ermannogoletto

Roberto Massa
Microsoft MVP Alumni
robimassa@outlook.it

/robi.massa.cn
@robi_massa
/robimassa

Deploy di Windows LAPS in Windows Server AD 1/3

1 Soddisfare i requisiti del livello funzionale di Dominio e delle versioni dell'OS dei DC

Domain details	Clear-text password storage supported	Encrypted password storage supported (for domain-joined clients)	DSRM account management supported (for DCs)
Below 2016 DFL	Yes	No	No
2016 DFL with one or more WS2016 DCs	Yes	Yes	Yes but only for WS2019 and later DCs
2016 DFL with only WS2019 and later DCs	Yes	Yes	Yes

2 Update del Windows Server Active Directory schema

Update-LapsADSchema

Utilizzare il parametro **–Verbose** per avere il dettaglio delle operazioni eseguite e **–WhatIf** per non applicare le modifiche

Operazione one-time for l'intera foresta AD eseguibile da DC WS 2022 o 2019 oppure da un computer membro del dominio con il Windows LAPS PowerShell module

I requisiti software per il deploy di Windows LAPS sono stati rilasciati tramite Windows Updates l'11 aprile 2023 per tutte le edizioni (LTSC compreso) di Windows 11 22H2 e 21H2, Windows 10, Windows Server 2022 e 2019

Get started with Windows LAPS and Windows Server Active Directory | Microsoft Learn

Deploy di Windows LAPS in Windows Server AD 2/3

3 Concedere ai device gestiti i privilegi per l'aggiornamento della password

```
# Impostazione dei privilegi ereditabili sull'OU che contiene i device gestiti
Set-LapsADComputerSelfPermission -Identity Laps

# E' possibile impostare i privilegi ereditabili sulla root del Dominio AD utilizzando la sintassi DN
Set-LapsADComputerSelfPermission -Identity 'DC=contoso,DC=com'
```

4 Gestire le Extended Rights permissions per la lettura degli attributi di LAPS

```
# Ricerca di utenti e gruppi in una specifica OU a cui sono concesse le Extended Rights permissions
Find-LapsADExtendedRights -Identity Laps

# Impostazione dei privilegi di lettura della password per utenti e gruppi in una specifica OU
Set-LapsADReadPasswordPermission -Identity Laps -AllowedPrincipals @("LapsAdministrators')

# Impostazione dei privilegi di lettura della password per utenti e gruppi in una specifica OU
Set-LapsADReadPasswordPermission -Identity Laps
```

La revoke deve essere fatta rimuovendo "All extended rights" dall'utente/gruppo

Per default solo le identies SYSTEM e Domain Admins hanno tali privilegi

[Get started with Windows LAPS and Windows Server Active Directory | Microsoft Learn]
[You Might Want to Audit Your LAPS Permissions.... - Microsoft Community Hub]

Deploy di Windows LAPS in Windows Server AD 3/3

5

Configurazione delle Windows LAPS Group Policy

Backup delle password soltanto su Windows Server Active Directory (GPO mandatoria)
Computer Configuration > Administrative Templates > System > LAPS > BackupDirectory = 2

Nome dell'account amministratore locale da gestire (GPO mandatoria nel caso di account custom)
Computer Configuration > Administrative Templates > System > LAPS > AdministratorAccountName
Se non viene specificato per default verrà gestito il built-in local administrator account (per essere gestito l'account deve essere abilitato, Windows LAPS non abilita l'account)

GPO Facoltative:

- **PasswordAgeDays** (1÷365 giorni, Default 30 giorni, se la backup directory è Azure AD il min è 7 giorni)
- **PasswordLength** (8÷64 caratteri, Default 14 caratteri)
- **PasswordComplexity** (Default 4 = Large letters + small letters + numbers + special characters)
- **ADPasswordEncryptionEnabled** (0=False o 1=True che richiede DFL a WS2016 o successivo)

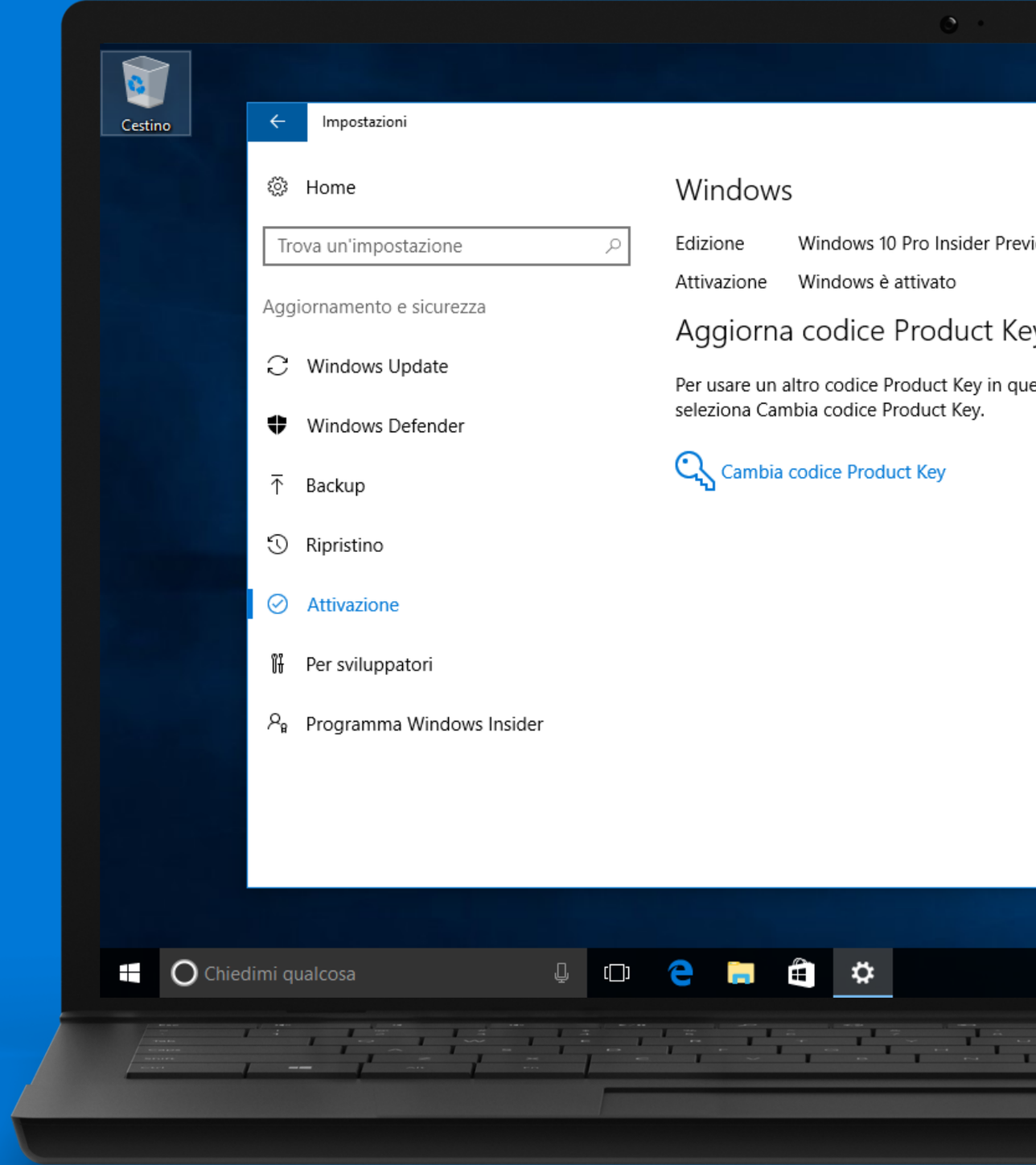
Per l'elenco completo delle GPO si veda Configure policy settings for Windows LAPS | Microsoft Learn

Nel caso di device hybrid-joined ad Azure AD è possible eseguire il deploy delle policy con Microsoft Intune tramite il Windows LAPS configuration service provider (CSP)

Get started with Windows LAPS and Windows Server Active Directory | Microsoft Learn

DEMO

DEPLOY


Cestino
Impostazioni
Home
Trova un'impostazione
Aggiornamento e sicurezza
Windows Update
Windows Defender
Backup
Ripristino
Attivazione
Per sviluppatori
Programma Windows Insider
Windows
Edizione
Windows 10 Pro Insider Previ
Attivazione
Windows è attivato
Aggiorna codice Product Key
Per usare un altro codice Product Key in que
seleziona Cambia codice Product Key.
Cambia codice Product Key
Chiedimi qualcosa

Legacy Microsoft LAPS emulation mode

- E' possible configurare Windows LAPS in **legacy Microsoft LAPS emulation mode** per eseguire la migrazione da una distribuzione Microsoft LAPS legacy a Windows LAPS
- Come Microsoft LAPS, la legacy Microsoft LAPS emulation mode **supporta l'archiviazione delle password in Windows Server Active Directory solo in formato clear-text**
- Quando si configura Windows LAPS in legacy Microsoft LAPS emulation mode **si presuppone che l'ambiente Windows Server Active Directory sia configurato per eseguire Microsoft LAPS legacy**

Estensione dello schema di Active Directory

- *Il cmdlet Windows LAPS **Update-LapsADSchema non aggiunge gli elementi dello schema Microsoft LAPS legacy***
- ***E' necessario usare il cmdlet Update-AdmPwdADSchema** per estendere lo schema installando Microsoft LAPS legacy in un DC o in un client di gestione*

Group Policy

- ***Windows LAPS non installa i Microsoft LAPS legacy Group Policy definition files***
- ***E' necessario installare Microsoft LAPS legacy in un DC o in un client di gestione** per definire e amministrare le Group Policy Microsoft LAPS legacy*

Requisiti minimi Microsoft LAPS

- *Active Directory: Windows 2003 SP1*
- *Client: Windows Vista /Windows 2003*
- *Management: .NET Framework 4.0, PowerShell 2.0*

Active Directory Access Control Lists (ACLs)

- ***Windows LAPS non supporta la gestione delle Active Directory ACLs di Microsoft LAPS legacy***
- *E' necessario usare il cmdlet **Set-AdmPwdComputerSelfPermissions** per gestire le ACLs installando Microsoft LAPS legacy in un DC o in un client di gestione*

Get started with Windows LAPS in legacy Microsoft LAPS emulation mode | Microsoft Learn

Download Local Administrator Password Solution (LAPS) from Official Microsoft Download Center

Legacy Microsoft LAPS emulation mode: Limitazioni

Un criterio Windows LAPS ha sempre la precedenza, ed un eventuale criterio Microsoft LAPS legacy viene sempre ignorato

Microsoft LAPS legacy non deve essere installato nel computer per evitare che Windows LAPS e Microsoft LAPS legacy tentino contemporaneamente di gestire lo stesso account amministratore locale creando un rischio di sicurezza e un scenario non supportato

Microsoft LAPS è considerato installato se la the legacy Microsoft LAPS Group Policy Client Side Extension (CSE) è installata**, è possibile verificare l'esistenza del valore **DllName** nella chiave di registro **HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{D76B9641-3288-4f75-942D-087DE603E3EA}

Se la chiave di registro esiste LAPS funziona in modalità di emulazione

Gestione utenti e computer Windows Server Active Directory non supporta gli attributi dello schema Microsoft LAPS legacy

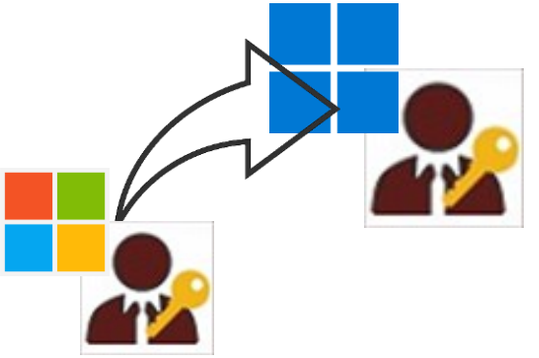
Disabilitazione Legacy Microsoft LAPS emulation mode
Windows LAPS avvia l'applicazione di un criterio Microsoft LAPS legacy non appena viene applicato al dispositivo**, è possibile disabilitare il Legacy Microsoft LAPS emulation mode creando un **valore REG_DWORD denominato BackupDirectory impostato a 0** nella chiave di registro **HKLM\Software\Microsoft\Windows\CurrentVersion\LAPS\Config

***Quando un computer è in modalità di emulazione nel Registro Eventi viene registrato l'evento 10023** in Applications and Services Logs > Microsoft > Windows > LAPS > Operational*

Get started with Windows LAPS in legacy Microsoft LAPS emulation mode | Microsoft Learn

Migrazione di Legacy Microsoft LAPS

- **È possibile usare sia Windows LAPS che legacy LAPS in uno scenario side-by-side**, ma i entrambi i criteri devono essere destinati a account locali diversi
- **Windows LAPS è integrato nel sistema operativo Windows**, è una funzionalità di sicurezza di base di Windows e non può essere disinstallata ed è **sempre attivo** non appena viene applicato un criterio Windows LAPS al dispositivo



Approccio 1: Transizione immediata

1. Disabilitare\rimuovere i criteri LAPS legacy
2. Creare e applicare i criteri di Windows LAPS
3. Monitorare i dispositivi per confermare la riuscita della transizione (ad esempio tramite Get-LapsADPassword)
4. Rimuovere il software LAPS legacy

Approccio 2: Coesistenza temporanea side-by-side

1. Configurare i dispositivi con un secondo account locale
2. Creare e applicare criteri di Windows LAPS
3. Monitorare il dispositivi per confermare la corretta applicazione dei criteri di Windows LAPS
4. Disabilitare\rimuovere i criteri LAPS legacy
5. Rimuovere il software LAPS legacy
6. Rimuovere l'account locale aggiuntivo

- **Rimozione LAPS legacy se installato tramite msi**
  msiexec.exe /q /uninstall {97E2CA7B-B657-4FF7-A6DB-30ECC73E1E28}
- **Rimozione LAPS legacy se installato tramite registrazione dll**
  regsvr32.exe /s /u AdmPwd.dll
  delete AdmPwd.dll

Get started with Windows LAPS deployment and migration scenarios | Microsoft Learn

ICT POWER.IT

Microsoft

Implementare e gestire Microsoft LAPS
Gestione di Windows LAPS

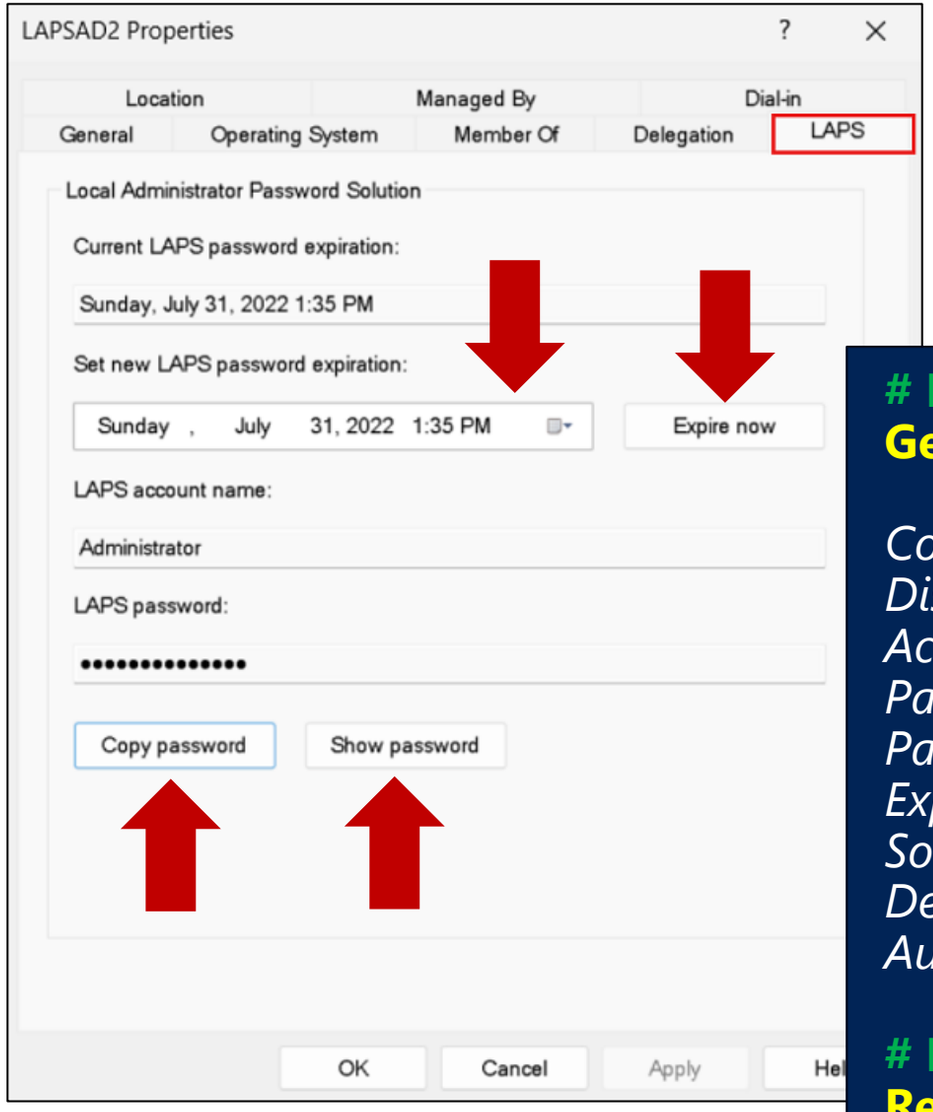
Ermanno Goletto
Microsoft MVP Alumni
e.goletto@outlook.it

/devadmin.it
@ermannog
/ermannogoletto

Roberto Massa
Microsoft MVP Alumni
robimassa@outlook.it

/robi.massa.cn
@robi_massa
/robimassa

Gestione di Windows LAPS in Windows Server AD



Lo snap-in **Utenti e computer di Active Directory** abilitato per Windows LAPS è disponibile su Windows 11 22H2 e 21H2, Windows 10, Windows Server 2022 e 2019 aggionati con l'update dell'11 aprile 2023

Per utilizzare lo snap-in sui OS clinet installare gli **RSAT**:
Remote Server Administration Tools - Windows Server | Microsoft Learn

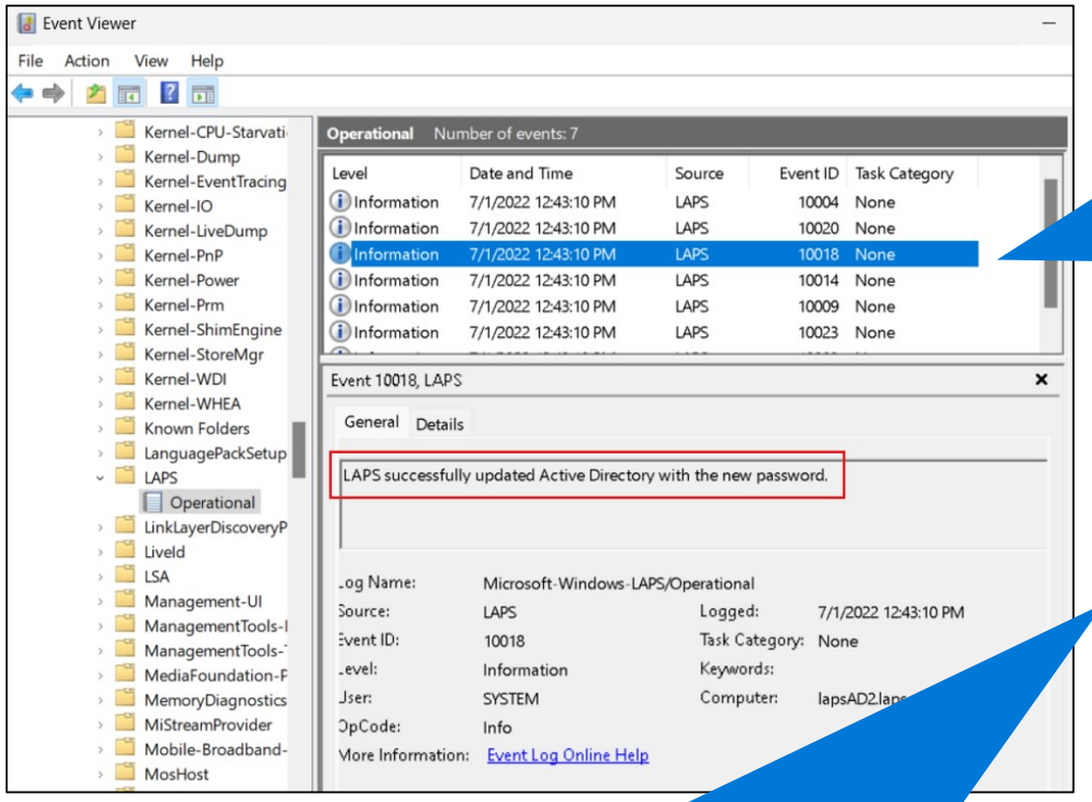
```
# Recuperare una password
Get-LapsADPassword -Identity PC-001 –AsPlainText

ComputerName        : PC-001
DistinguishedName   : CN=PC-001,OU=Laps,DC=contoso,DC=com
Account             : Administrator
Password            : Klh+lyC[0e0/VU
PasswordUpdateTime  : 7/1/2022 1:23:19 PM
ExpirationTimestamp : 7/31/2022 1:23:19 PM
Source              : EncryptedPassword
DecryptionStatus    : Success
AuthorizedDecryptor : CONTOSO\Domain Admins

# Forzare il rinnovo della pssword sul computer locale
Reset-LapsPassword
```

Get started with Windows LAPS and Windows Server Active Directory | Microsoft Learn

Verifica del funzionamento in Windows Server AD



Quando LAPS aggiorna con successo la password in AD registra nel client l'**evento 10018** nel registro eventi **Applications and Services Logs > Microsoft > Windows > LAPS > Operational**

Alcuni eventi generarti dal client Windows LAPS:

- **10003**: LAPS policy processing is now starting
- **10004**: LAPS policy processing succeeded
- **10005**: LAPS policy processing failed
- **10021**: LAPS policy is configured to back up to WS AD
- **10022**: LAPS policy is configured to back up to Azure AD

Per l'elenco completo si veda:

Use Windows LAPS event logs | Microsoft Learn

- Eventi di inizio e fine dell'elaborazione dei criteri
- Dettagli sulla configurazione dei criteri
- Eventi di conferma dell'aggiornamento delle password
- Richiesta di modifica della password esterna bloccata
- Eventi correlati all'autenticazione post-autenticazione

*Windows LAPS event log contiene eventi correlati al computer locale, in un DC contiene solo eventi correlati alla gestione dell'account DSRM locale (se abilitato) e **non contiene eventi correlati ai comportamenti client di dominio***

Windows LAPS troubleshooting guidance - Windows Server | Microsoft Learn

LAPS PowerShell cmdlets

Windows LAPS** include un **modulo PowerShell denominato LAPS

*I cmdlet **Invoke-LapsPolicyProcessing** e **Reset-LapsPassword** sono **supportati sia che la password sia sottoposta a backup in Azure Active Directory o Windows Server Active Directory***

Microsoft LAPS legacy** include un **modulo di PowerShell denominato AdmPwd.PS

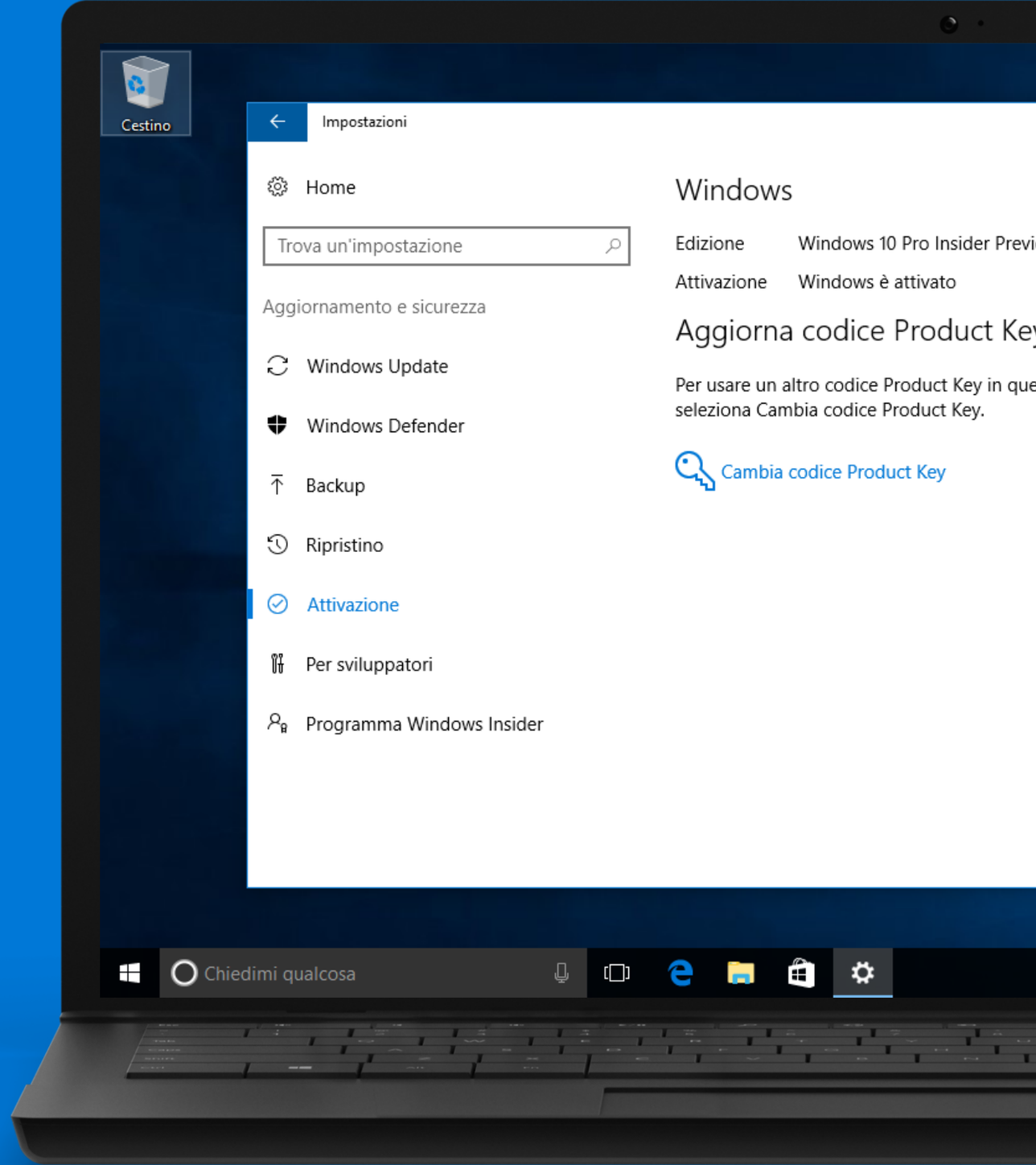
I cmdlet di PowerShell di Windows LAPS per Windows Server Active Directory** operano su un **set completamente diverso di estensioni dello schema

Windows LAPS cmdlet	Legacy Microsoft LAPS cmdlet
`Get-LapsAADPassword`	Doesn't apply
`Get-LapsDiagnostics`	Doesn't apply
`Find-LapsADExtendedRights`	`Find-AdmPwdExtendedRights`
`Get-LapsADPassword`	`Get-AdmPwdPassword`
`Invoke-LapsPolicyProcessing`	Doesn't apply
`Reset-LapsPassword`	Doesn't apply
`Set-LapsADAuditing`	`Set-AdmPwdAuditing`
`Set-LapsADComputerSelfPermission`	`Set-AdmPwdComputerSelfPermission`
`Set-LapsADPasswordExpirationTime`	`Reset-AdmPwdPassword`
`Set-LapsADReadPasswordPermission`	`Set-AdmPwdReadPasswordPermission`
`Set-LapsADResetPasswordPermission`	`Set-AdmPwdResetPasswordPermission`
`Update-LapsADSchema`	`Update-AdmPwdADSchema`

Use Windows LAPS PowerShell cmdlets | Microsoft Learn

DEMO

EXPORT


Cestino
Impostazioni
Home
Trova un'impostazione
Aggiornamento e sicurezza
Windows Update
Windows Defender
Backup
Ripristino
Attivazione
Per sviluppatori
Programma Windows Insider
Windows
Edizione
Windows 10 Pro Insider Previ
Attivazione
Windows è attivato
Aggiorna codice Product Key
Per usare un altro codice Product Key in que
seleziona Cambia codice Product Key.
Cambia codice Product Key
Chiedimi qualcosa

Legacy Microsoft LAPS emulation mode

Supporto amministrativo limitato

La pagina delle proprietà Windows LAPS nella console di gestione utenti e computer di Windows Server Active Directory non supporta la visualizzazione o l'amministrazione degli attributi Microsoft LAPS legacy

Get-LapsADPassword supporta il recupero dell'**attributo password Microsoft LAPS legacy (*ms-Mcs-AdmPwd*)**, mentre **i campi Account e PasswordUpdateTime sono sempre vuoti** nell'output risultante

Set-LapsADPasswordExpirationTime non supporta la scadenza o la modifica dell'attributo di scadenza della password Microsoft LAPS legacy (*ms-Mcs-AdmPwdExpirationTime*)

```
# Recuperare una password
Get-LapsADPassword -Identity PC-002 –AsPlainText

ComputerName       : PC-002
DistinguishedName  : CN=PC-002,OU=Laps,DC=contoso,DC=com
Account            :
Password           : Slm!lyP[0e0/VU
PasswordUpdateTime :
ExpirationTimestamp: 7/31/2022 1:23:19 PM
Source             : LegacyLapsCleartextPassword
DecryptionStatus   : NotApplicable
AuthorizedDecryptor : NotApplicable
```

[Get started with Windows LAPS in legacy Microsoft LAPS emulation mode | Microsoft Learn]

Windows LAPS FAQs

È supportato l'esecuzione di prodotti di gestione password locali di terze parti side-by-side con Windows LAPS?

***Sì**, questo scenario è supportato con la condizione seguente. È necessario prestare attenzione a **configurare Windows LAPS e il prodotto di terze parti per gestire account locali diversi**. Se si configurano erroneamente entrambi per gestire lo stesso account, Windows LAPS rifiuta i tentativi del prodotto di terze parti per modificare la password dell'account*

È necessario distribuire un controller di dominio di Windows Server 2022 o 2019 per estendere lo schema della foresta con le estensioni dello schema di Windows LAPS?

***No**: è possibile eseguire il Update-LapsADSchema cmdlet da qualsiasi sistema operativo aggiornato con la funzionalità LAPS di Windows. L'unico requisito è che le credenziali client siano autorizzate a modificare lo schema di Active Directory.*

È stato installato RSAT e non viene ancora visualizzato il nuovo snap-in Utenti e computer di Active Directory abilitato per LAPS?

*Il nuovo snap-in è **disponibile solo nelle versioni Windows in-box di RSAT su Windows LAPS platforms supportate**.*

E' possibile copiare lo snap-in Utenti e computer Active Directory abilitato per Windows LAPS in un OS precedente?

*Questo scenario **non è supportato**.*

Perché i nuovi criteri di Windows LAPS non vengono visualizzati nel GPO central store?

*I nuovi criteri di Windows LAPS **non vengono installato automaticamente come parte del GPO central store**.*

E' possibile copiare il modulo PowerShell di Windows LAPS in un OS precedente?

*Questo scenario **non è supportato**.*

[Windows LAPS frequently asked questions | Microsoft Learn]

Link

- By popular demand: Windows LAPS available now! - Microsoft Community Hub
- Windows LAPS overview | Microsoft Learn
- How to Configure Microsoft Local Administrator Password Solution (LAPS)
- Microsoft LAPS usage assessment - Microsoft Defender for Identity | Microsoft Learn
- Windows LAPS Configuration Guide | Veeam Community Resource Hub
- Microsoft LAPS deployment and configuration guide (veeam.com)
- Microsoft Intune – Configurazione delle password amministrative locali con Windows LAPS - ICT Power
- Windows LAPS - Local Administrator Password Solution - ICT Power
- Implementare Local Administrator Password Solution (LAPS) - ICT Power
- GitHub - htcfreek/SimpleLapsGui: A simple and fast GUI for Microsoft LAPS (legacy) and Windows LAPS. With this tool you can query passwords and change the expiration timestamp.

Grazie

Ermanno Goletto
Microsoft MVP Alumni
e.goletto@outlook.it

/devadmin.it
@ermannog
/ermannogoletto

Roberto Massa
Microsoft MVP Alumni
robimassa@outlook.it

/robi.massa.cn
@robi_massa
/robimassa