What's new in Windows Server 2025

Article • 11/01/2024 • Applies to: ✅ Windows Server 2025

This article describes some of the newest developments in Windows Server 2025, which boasts advanced features that improve security, performance, and flexibility. With faster storage options and the ability to integrate with hybrid cloud environments, managing your infrastructure is now more streamlined. Windows Server 2025 builds on the strong foundation of its predecessor while introducing a range of innovative enhancements to adapt to your needs.

If you're interested in trying out the latest features of Windows Server 2025 before official release, see Get started with Windows Server Insiders Preview.

What's new

The following new features are specific to Windows Server with Desktop Experience only. Having both the physical devices running the operating system and the correct drivers readily available are required.

Accelerated Networking

Accelerated Networking (AccelNet) simplifies the management of single root I/O virtualization (SR-IOV) for virtual machines (VM) hosted on Windows Server 2025 clusters. This feature uses the high-performance SR-IOV data path to reduce latency, jitter, and CPU utilization. AccelNet also includes a management layer that handles prerequisite checking, host configuration, and VM performance settings.

Active Directory Domain Services

The latest enhancements to Active Directory Domain Services (AD DS) and Active Directory Lightweight Domain Services (AD LDS) introduce a range of new functionalities and capabilities aimed at optimizing your domain management

experience:

- **32k database page size optional feature** - AD uses an Extensible Storage Engine (ESE) database since its introduction in Windows 2000 that uses an 8k database page size. The 8k architectural design decision resulted in limitations throughout AD that are documented in AD Maximum Limits Scalability. An example of this limitation is a single record AD object, which can't exceed 8k bytes in size. Moving to a 32k database page format offers a huge improvement in areas affected by legacy restrictions, including multi-valued attributes are now able to hold up to ~3,200 values, which is an increase by a factor of 2.6.

  New DCs can be installed with a 32k page database that uses 64-bit Long Value IDs (LIDs) and runs in an "8k page mode" for compatibility with previous versions. An upgraded DC continues to use its current database format and 8k pages. Moving to 32k database pages is done on a forest-wide basis and requires that all DCs in the forest have a 32k page capable database.

- **AD schema updates** - Three new Log Database Files (LDF) are introduced that extend the AD schema, `sch89.ldf`, `sch90.ldf`, and `sch91.ldf`. The AD LDS equivalent schema updates are in `MS-ADAM-Upgrade3.ldf`. For learn more about previous schema updates, see Windows Server AD schema updates

- **AD object repair** - AD now allows enterprise administrators to repair objects with missing core attributes **SamAccountType** and **ObjectCategory**. Enterprise administrators can reset the **LastLogonTimeStamp** attribute on an object to the current time. These operations are achieved through a new RootDSE modify operation feature on the affected object called **fixupObjectState**.

- **Channel binding audit support** - Events 3074 and 3075 can now be enabled for Lightweight Directory Access Protocol (LDAP) channel binding. When the channel binding policy is modified to a more secure setting, an administrator can identify devices in the environment that don't support or fail channel binding. These audit events are also available in Windows Server 2022 and later via KB4520412 .

- **DC-location algorithm improvements** - DC discovery algorithm provides new functionality with improvements to mapping of short NetBIOS-style domain names to DNS-style domain names. To learn more, see Active Directory DC locator changes.

> **Note**
>
> Windows doesn't use mailslots during DC discovery operations as Microsoft has announced the **deprecation of WINS and mailslots** for these legacy technologies.

- **Forest and Domain Functional Levels** - The new functional level is used for general supportability and is required for the new 32K database page size feature. The new functional level maps to the value of `DomainLevel 10` and `ForestLevel 10` for unattended installs. Microsoft has no plans to retrofit functional levels for Windows Server 2019 and Windows Server 2022. To perform an unattended promotion and demotion of a Domain Controller (DC), see DCPROMO answer file syntax for unattended promotion and demotion of domain controllers.

  The DsGetDcName Application Programming Interface (API) also supports a new flag `DS_DIRECTORY_SERVICE_13_REQUIRED` that enables location of DCs running Windows Server 2025. You can learn more about functional levels in the following articles:

  - Forest and Domain Functional Levels
  - Raise the Domain Functional Level
  - Raise the Forest Functional Level

  > **Note**
  >
  > New AD forests or AD LDS configuration sets are required to have a functional level of Windows Server 2016 or greater. Promotion of an AD or AD LDS replica requires that the existing domain or config set is already running with a functional level of Windows Server 2016 or greater.
  >
  > Microsoft recommends that all customers begin planning now to upgrade their AD and AD LDS servers to Windows Server 2022 in preparation of the next release.

- **Improved algorithms for Name/Sid Lookups** - Local Security Authority (LSA)

Name and Sid lookup forwarding between machine accounts no longer uses the legacy Netlogon secure channel. Kerberos authentication and DC Locator algorithm are used instead. To maintain compatibility with legacy operating systems, it's still possible to use the Netlogon secure channel as a fallback option.

- **Improved security for confidential attributes** - DCs and AD LDS instances only allow LDAP to add, search, and modify operations involving confidential attributes when the connection is encrypted.

- **Improved security for default machine account passwords** - AD now uses random generated default computer account passwords. Windows 2025 DCs block setting computer account passwords to the default password of the computer account name.

  This behavior can be controlled by enabling the GPO setting *Domain controller: Refuse setting default machine account password* located in: **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**

  Utilities like Active Directory Administrative Center (ADAC), Active Directory Users and Computers (ADUC), `net computer`, and `dsmod` also honors this new behavior. Both ADAC and ADUC no longer allow creating a pre-2k Windows account.

- **Kerberos PKINIT support for cryptographic agility** - The Kerberos Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) protocol implementation is updated to allow for cryptographic agility by supporting more algorithms and removing hardcoded algorithms.

- **LAN Manager GPO setting** - The GPO setting *Network security: Don't store LAN Manager hash value on next password change* is no longer present nor applicable to new versions of Windows.

- **LDAP encryption by default** - All LDAP client communication after a Simple Authentication and Security Layer (SASL) bind utilizes LDAP sealing by default. To learn more about SASL, see SASL Authentication.

- **LDAP support for TLS 1.3** - LDAP uses the latest SCHANNEL implementation and supports TLS 1.3 for LDAP over TLS connections. Using TLS 1.3 eliminates obsolete cryptographic algorithms, enhances security over older versions, and aims to

encrypt as much of the handshake as possible. To learn more, see Protocols in TLS/SSL (Schannel SSP) and TLS Cipher Suites in Windows Server 2022.

- **Legacy SAM RPC password change behavior** - Secure protocols such as Kerberos are the preferred way to change domain user passwords. On DCs, the latest SAM RPC password change method SamrUnicodeChangePasswordUser4 using AES is accepted by default when called remotely. The following legacy SAM RPC methods are blocked by default when called remotely:

  - SamrChangePasswordUser
  - SamrOemChangePasswordUser2
  - SamrUnicodeChangePasswordUser2

  For domain users that are members of the Protected Users group and for local accounts on domain member computers, all remote password changes through the legacy SAM RPC interface are blocked by default including `SamrUnicodeChangePasswordUser4`.

  This behavior can be controlled using the following Group Policy Object (GPO) setting:

  Computer Configuration > Administrative Templates > System > Security Account Manager > Configure SAM change password RPC methods policy

- **NUMA support** - AD DS now takes advantage of Non-uniform Memory Access (NUMA) capable hardware by utilizing CPUs in all processor groups. Previously, AD would only use CPUs in group 0. Active Directory can expand beyond 64 cores.

- **Performance counters** - Monitoring and troubleshooting the performance of the following counters are now available:

  - *DC Locator* - Client and DC specific counters available.
  - *LSA Lookups* - **Name** and **SID** lookups through the **LsaLookupNames**, **LsaLookupSids**, and equivalent APIs. These counters are available on both Client and Server SKUs.
  - *LDAP Client* - Available in Windows Server 2022 and later via KB 5029250

update.

- **Replication priority order** - AD now allows administrators to increase the system calculated replication priority with a particular replication partner for a particular naming context. This feature allows more flexibility in configuring the replication order to address specific scenarios.

Azure Arc

By default, the Azure Arc setup Feature-on-Demand is installed, which offers a user-friendly wizard interface and a system tray icon in the taskbar to facilitate the process of adding servers to Azure Arc. Azure Arc extends the capabilities of the Azure platform, allowing for the creation of applications and services that can operate in diverse environments. These include data centers, the edge, multicloud environments, and provide increased flexibility. To learn more, see Connect Windows Server machines to Azure through Azure Arc Setup.

Block cloning support

Starting with Windows 11 24H2 and Windows Server 2025, Dev Drive now supports Block cloning. As Dev Drive uses the ReFS file system format, Block cloning support provides significant performance benefits when copying files. With Block cloning, the file system can copy a range of file bytes on behalf of an application as a low-cost metadata operation, rather than performing expensive read and write operations to the underlying physical data. This results in faster completion of file copying, reduced I/O to the underlying storage, and improved storage capacity by enabling multiple files to share the same logical clusters. To learn more, see Block cloning on ReFS.

Bluetooth

You can now connect mice, keyboards, headsets, audio devices, and more via bluetooth in Windows Server 2025.

Credential Guard

Starting with Windows Server 2025, Credential Guard is now enabled by default on devices that meet the requirements. For more information about Credential Guard, see Configure Credential Guard.

Desktop shell

When you sign in for the first time, the desktop shell experience conforms to the style and appearance of Windows 11.

Delegated Managed Service Account

This new type of account enables migration from a service account to a delegated Managed Service Account (dMSA). This account type comes with managed and fully randomized keys ensuring minimal application changes while disabling the original service account passwords. To learn more, see Delegated Managed Service Accounts overview.

Dev Drive

Dev Drive is a storage volume that aims to enhance the performance of crucial developer workloads. Dev Drive utilizes ReFS technology and incorporates specific file system optimizations to offer greater control over storage volume settings and security. This includes the ability to designate trust, configure antivirus settings, and exercise administrative control over attached filters. To learn more, see Set up a Dev Drive on Windows 11.

DTrace

Windows Server 2025 comes equipped with `dtrace` as a native tool. DTrace is a command-line utility that enables users to monitor and troubleshoot their system's performance in real-time. DTrace allows users to dynamically instrument both the kernel and user-space code without any need to modify the code itself. This versatile tool supports a range of data collection and analysis techniques, such as aggregations, histograms, and tracing of user-level events. To learn more, see DTrace for command line help and DTrace on Windows for other capabilities.

Email & accounts

You can now add the following accounts in **Settings** > **Accounts** > **Email & accounts** for Windows Server 2025:

- Microsoft Entra ID
- Microsoft account
- Work or school account

It's important to keep in mind that domain join is still required for most situations.

Feedback Hub

Submitting feedback or reporting problems encountered while using Windows Server 2025 can now be done using the Windows Feedback Hub. You can include screenshots or recordings of the process that caused the issue to help us understand your situation and share suggestions to enhance your Windows experience. To learn more, see Explore the Feedback Hub.

File Compression

Build 26040 has a new compression feature when compressing an item by performing a right-click called **Compress to**. This feature supports **ZIP**, **7z**, and **TAR** compression formats with specific compression methods for each.

Hyper-V Manager

When users create a new VM through the Hyper-V Manager, **Generation 2** is now set as the default option in the **New Virtual Machine Wizard**.

Hypervisor-enforced paging translation

Hypervisor-enforced paging translation (HVPT) is a security enhancement to enforce the integrity of linear address translations. HVPT protects critical system data from write-what-where attacks where the attacker writes an arbitrary value to an arbitrary location,

often as the result of a buffer overflow. HVPT guards page tables that configure critical system data structures. HVPT includes everything already secured with hypervisor-protected code integrity (HVCI). HVPT is enabled by default where hardware support is available. HVPT isn't enabled when Windows Server runs as a guest in a VM.

Network ATC

Network ATC streamlines the deployment and management of network configurations for Windows Server 2025 clusters. It utilizes an intent-based approach, where users specify their desired intents, such as management, compute, or storage for a network adapter, and the deployment is automated based on the intended configuration. This approach reduces the time, complexity, and errors associated with host networking deployment, ensures configuration consistency across the cluster, and eliminates configuration drift. To learn more, see Deploy host networking with Network ATC.

NVMe

NVMe is a new standard for fast solid-state drives (SSDs). Experience NVMe optimization in Windows Server 2025 with improved performance, resulting in an increase in IOPS and decrease in CPU utilization.

OpenSSH

In earlier versions of Windows Server, the OpenSSH connectivity tool required a manual install before use. Starting with build 26080, the OpenSSH server-side component is installed by default in Windows Server 2025. The Server Manager UI also includes a one-click option under **Remote SSH Access** that enables or disables the `sshd.exe` service. Also, you can add users to the **OpenSSH Users** group to allow or restrict access to your devices. To learn more, see OpenSSH for Windows overview.

Pinned apps

Pinning your most used apps is now available through the **Start** menu and is customizable to suit your needs. As of build 26085, the default pinned apps are currently:

- Azure Arc Setup
- Feedback Hub
- File Explorer
- Microsoft Edge
- Server Manager
- Settings
- Terminal
- Windows PowerShell

Remote Access

By default new Routing and Remote Access Services (RRAS) setups don't accept VPN connections based on PPTP and L2TP protocols. You can still enable these protocols if necessary. SSTP and IKEv2 based VPN connections are still accepted without any change.

Existing configurations retain their behavior. For example, if you're running Windows Server 2019 and accept PPTP and L2TP connections, after updating to Windows Server 2025 using an in-place update, L2TP and PPTP based connections are still accepted. This change doesn't affect Windows clients operating systems. To learn more about how-to re-enable PPTP and L2TP, see Configure VPN protocols.

Secure certificate management

Searching or retrieving certificates on Windows now supports SHA-256 hashes, as described in the functions CertFindCertificateInStore, and CertGetCertificateContextProperty. TLS server authentication is more secure across Windows, and now requires a minimum RSA key length of 2048 bits. For more information, read TLS server authentication: Deprecation of weak RSA certificates .

Security Baseline

By implementing a customized security baseline, you can establish security measures right from the beginning for your device or VM role based on the recommended security posture. This baseline comes equipped with over 350 preconfigured Windows

security settings that enable you to apply and enforce specific security settings that align with the best practices recommended by Microsoft and industry standards. To learn more, see OSConfig overview.

Server Message Block

Server Message Block (SMB) is one of the most widely used protocols in networking by providing a reliable way to share files and other resources between devices on your network. Windows Server 2025 brings the following SMB capabilities.

Starting with build 26090, another set of SMB protocol changes are introduced for disabling QUIC, signing, and encryption.

- **SMB over QUIC disablement**

  Administrators can disable SMB over QUIC client through Group Policy and PowerShell. To disable SMB over QUIC using Group Policy, set the **Enable SMB over QUIC** policy in these paths to **Disabled**.

  - **Computer Configuration\Administrative Templates\Network\Lanman Workstation**
  - **Computer Configuration\Administrative Templates\Network\Lanman Server**

  To disable SMB over QUIC using PowerShell, run this command in an elevated PowerShell prompt:

  ```PowerShell
  Set-SmbClientConfiguration -EnableSMBQUIC $false
  ```

- **SMB signing and encryption auditing**

  Administrators can enable auditing of the SMB server and client for support of SMB signing and encryption. If a third-party client or server lacks support for SMB encryption or signing, it can be detected. When your third-party device or software states it supports SMB 3.1.1, but fails to support SMB signing, it violates the SMB 3.1.1 Pre-authentication integrity protocol requirement.

You can configure SMB signing and encryption auditing settings using Group Policy or PowerShell. These policies can be changed in the following Group Policy paths:

- **Computer Configuration\Administrative Templates\Network\Lanman Server\Audit client does not support encryption**
- **Computer Configuration\Administrative Templates\Network\Lanman Server\Audit client does not support signing**
- **Computer Configuration\Administrative Templates\Network\Lanman Workstation\Audit server does not support encryption**
- **Computer Configuration\Administrative Templates\Network\Lanman Workstation\Audit server does not support signing**

To perform these changes using PowerShell, run these commands in an elevated prompt where `$true` is to enable and `$false` to disable these settings:

PowerShell

```
Set-SmbServerConfiguration -AuditClientDoesNotSupportEncryption
$true
Set-SmbServerConfiguration -AuditClientDoesNotSupportSigning
$true

Set-SmbClientConfiguration -AuditServerDoesNotSupportEncryption
$true
Set-SmbClientConfiguration -AuditServerDoesNotSupportSigning
$true
```

Event logs for these changes are stored in the following Event Viewer paths with their given Event ID.

Expand table

Path	Event ID
Applications and Services Logs\Microsoft\Windows\SMBClient\Audit	31998 31999
Applications and Services Logs\Microsoft\Windows\SMBServer\Audit	3021

	3022

- **SMB over QUIC auditing**

  SMB over QUIC client connection auditing captures events that are written to an event log to include the QUIC transport in the Event Viewer. These logs are stored in the following paths with their given Event ID.

  Expand table

Path	Event ID
Applications and Services Logs\Microsoft\Windows\SMBClient\Connectivity	30832
Applications and Services Logs\Microsoft\Windows\SMBServer\Connectivity	1913

- The SMB over QUIC server feature, which was only available in Windows Server Azure Edition, is now available in both Windows Server Standard and Windows Server Datacenter versions. SMB over QUIC adds the benefits of the QUIC, which provides low-latency, encrypted connections over the internet.

  Previously, SMB server in Windows mandated inbound connections to use the IANA-registered port TCP/445 while the SMB TCP client only allowed outbound connections to that same TCP port. Now, SMB over QUIC allows for SMB alternative ports where QUIC-mandated UDP/443 ports are available for both server and client devices. To learn more, see Configure alternative SMB ports.

  Another feature that's introduced to SMB over QUIC is client access control, which is an alternative to TCP and RDMA that supplies secure connectivity to edge file servers over untrusted networks. To learn more, see How client access control works.

- Previously, when a share was created, the SMB firewall rules would be automatically configured to enable the "File and Printer Sharing" group for the relevant firewall profiles. Now, the creation of an SMB share in Windows results in the automatic configuration of the new "File and Printer Sharing (Restrictive)" group, which no longer permits inbound NetBIOS ports 137-139. To learn more, see Updated firewall rules.

- Starting with build 25997, an update is made to enforce SMB encryption for all outbound SMB client connections. With this update, administrators can set a mandate that all destination servers support SMB 3.x and encryption. If a server lacks these capabilities, the client is unable to establish a connection.

- Also in build 25997, the SMB authentication rate limiter, which limits the number of authentication attempts that can be made within a certain time period, is enabled by default. To learn more, see How SMB authentication rate limiter works

- Starting with build 25951, the SMB client supports NTLM blocking for remote outbound connections. Previously, the Windows Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) would negotiate Kerberos, NTLM, and other mechanisms with the destination server to determine a supported security package. To learn more, see Block NTLM connections on SMB

- A new feature in build 25951 allows you to manage SMB dialects in Windows where the SMB server now controls which SMB 2 and SMB 3 dialects it negotiates compared to the previous behavior matching only the highest dialect.

- Beginning with build 25931, SMB signing is now required by default for all SMB outbound connections where previously it was only required when connecting to shares named **SYSVOL** and **NETLOGON** on AD domain controllers. To learn more, see How signing works.

- The Remote Mailslot protocol is disabled by default starting in build 25314 and may be removed in a later release. To learn more, see Features we're no longer developing.

- SMB compression adds support for industry standard LZ4 compression algorithm, in addition to its existing support for XPRESS (LZ77), XPRESS Huffman (LZ77+Huffman), LZNT1, and PATTERN_V1.

Software Defined Networking (SDN)

SDN is an approach to networking that allows network administrators to manage network services through abstraction of lower-level functionality. SDN enables the separation of the network control plane, which is responsible for managing the network, from the data plane, which handles the actual traffic. This separation allows for

increased flexibility and programmability in network management. SDN provides the following benefits in Windows Server 2025:

- The Network Controller, which is the control plane for SDN, is now hosted directly as Failover Cluster services on the physical host machines. This eliminates the need to deploy VMs, simplifying deployment and management while conserving resources.

- Tag-based segmentation allows administrators to use custom service tags to associate Network Security Groups (NSGs) and VMs for access control. Instead of specifying IP ranges, administrators can now use simple, self-explanatory labels to tag workload VMs, and apply security policies based on these tags. This simplifies the process of managing network security and eliminates the need to remember and retype IP ranges. To learn more, see Configure network security groups with tags in Windows Admin Center.

- Default network policies in Windows Server 2025 bring Azure-like protection options to NSGs for workloads deployed through Windows Admin Center. The default policy denies all inbound access, allowing selective opening of well-known inbound ports while permitting full outbound access from workload VMs. This ensures workload VMs are secured from the point of creation. To learn more, see Use default network access policies on virtual machines on Azure Stack HCI, version 23H2.

- SDN Multisite provides native Layer 2 and Layer 3 connectivity between applications across two locations without any extra components. This feature allows for seamless movement of applications without the need to reconfigure the application or networks. It also offers unified network policy management for workloads, ensuring that policies don't need to be updated when a workload VM moves from one location to another. To learn more, see What is SDN Multisite?.

- The performance of SDN Layer 3 gateways has been enhanced, achieving higher throughput, and reduced CPU cycles. These improvements are enabled by default. Users will automatically experience better performance when an SDN gateway Layer 3 connection is configured through PowerShell or Windows Admin Center.

Storage Replica Enhanced Log

Enhanced Logs help the Storage Replica log implementation to eliminate the performance costs associated with file system abstractions, leading to improved block replication performance. To learn more, see Storage Replica Enhanced Log.

Task Manager

Build 26040 now sports the modern Task Manager app with mica material conforming to the style of Windows 11.

Virtualization-based security (VBS) enclaves

A VBS enclave is a software-based trusted execution environment (TEE) inside the address space of a host application. VBS enclaves use underlying VBS technology to isolate the sensitive portion of an application in a secure partition of memory. VBS enclaves enable isolation of sensitive workloads from both the host application and the rest of the system.

VBS enclaves enable applications to protect their secrets by removing the need to trust admins and hardening against malicious attackers. For more information, read the VBS enclaves Win32 reference.

Virtualization-based security (VBS) key protection

VBS key protection enables Windows developers to secure cryptographic keys using virtualization-based security (VBS). VBS uses the virtualization extension capability of the CPU to create an isolated runtime outside of the normal OS. When in use, VBS keys are isolated in a secure process, allowing key operations to occur without exposing the private key material outside of this space. At rest, private key material is encrypted by a TPM key, which binds VBS keys to the device. Keys protected in this way can't be dumped from process memory or exported in plain text from a user's machine, preventing exfiltration attacks by any admin-level attacker. VBS must be enabled to use key protection. See Enable memory integrity for information about how to enable VBS.

Wi-Fi

It's now easier to enable wireless capabilities as the Wireless LAN Service feature is now installed by default. The wireless startup service is set to manual and can be enabled by running `net start wlansvc` in the Command Prompt, Windows Terminal, or PowerShell.

Windows containers portability

Portability is a crucial aspect of container management and has the ability to simplify upgrades by applying enhanced flexibility and compatibility of containers in Windows. Portability is a feature of Windows Server Annual Channel for container hosts that allows users to move container images, and their associated data, between different hosts or environments without requiring any modifications. Users can create a container image on one host and then deploy it on another host without having to worry about compatibility issues. To learn more, see Portability for containers.

Windows Insider Program

The Windows Insider Program provides early access to the latest Windows OS releases for a community of enthusiasts. As a member, you can be among the first to try out new ideas and concepts that Microsoft is developing. After registering as a member, you can opt to participate in different release channels by going to go to **Start** > **Settings** > **Windows Update** > **Windows Insider Program**.

Windows Local Administrator Password Solution (LAPS)

Windows LAPS helps organizations manage local administrator passwords on their domain-joined computers. It automatically generates unique passwords for each computer's local administrator account, stores them securely in AD, and updates them regularly. This helps to improve security by reducing the risk of attackers gaining access to sensitive systems using compromised or easily guessable passwords.

Several features are introduced to Microsoft LAPS that bring the following

improvements:

- **New automatic account management feature**

  The latest update allows IT admins to create a managed local account with ease. With this feature, you can customize the account name, enable or disable the account, and even randomize the account name for enhanced security. Additionally, the update includes improved integration with Microsoft's existing local account management policies. To learn more about this feature, see Windows LAPS account management modes.

- **New image rollback detection feature**

  Windows LAPS now detects when an image rollback occurs. If a rollback does happen, the password stored in AD may no longer match the password stored locally on the device. Rollbacks can result in a "torn state" where the IT admin is unable to sign into the device using the persisted Windows LAPS password.

  To address this issue, a new feature was added that includes an AD attribute called **msLAPS-CurrentPasswordVersion**. This attribute contains a random GUID written by Windows LAPS every time a new password is persisted in AD and saved locally. During every processing cycle, the GUID stored in **msLAPS-CurrentPasswordVersion** is queried and compared to the locally persisted copy. If they're different, the password is immediately rotated.

  To enable this feature, it's necessary to run the latest version of the `Update-LapsADSchema` cmdlet. Once complete, Windows LAPS recognizes the new attribute and begins using it. If you don't run the updated version of the `Update-LapsADSchema` cmdlet, Windows LAPS logs a 10108 warning event in the event log, but continues to function normally in all other respects.

  No policy settings are used to enable or configure this feature. The feature is always enabled once the new schema attribute is added.

- **New passphrase feature**

  IT admins can now utilize a new feature in Windows LAPS that enables the generation of less complex passphrases. An example would be a passphrase such as **EatYummyCaramelCandy**, which is easier to read, remember, and type,

compared to a traditional password like **V3r_b4tim#963?**.

This new feature also allows the *PasswordComplexity* policy setting to be configured to select one of three different passphrase word lists, all of which are included in Windows without requiring a separate download. A new policy setting called *PassphraseLength* controls the number of words used in the passphrase.

When you're creating a passphrase, the specified number of words are randomly selected from the chosen word list and concatenated. The first letter of each word is capitalized to enhance readability. This feature also fully supports backing passwords up to either Windows Server AD or Microsoft Entra ID.

The passphrase word lists used in the three new *PasswordComplexity* passphrase settings are sourced from the Electronic Frontier Foundation's article, Deep Dive: EFF's New Wordlists for Random Passphrases . The Windows LAPS Passphrase Word Lists is licensed under the CC-BY-3.0 Attribution license and is available for download.

> **Note**
>
> Windows LAPS doesn't allow for customization of the built-in word lists nor the use of customer-configured word lists.

- **Improved readability password dictionary**

  Windows LAPS introduces a new *PasswordComplexity* setting that enables IT admins to create less complex passwords. This feature allows you to customize LAPS to use all four character categories (upper case letters, lower case letters, numbers, and special characters) like the existing complexity setting of 4. However, with the new setting of 5, the more complex characters are excluded to enhance password readability and minimize confusion. For example, the number "**1**" and the letter "**l**" are never used with the new setting.

  When *PasswordComplexity* is configured to 5, the following changes are made to the default password dictionary character set:

  1. Don’t use these letters: '**I**', '**O**', '**Q**', '**l**', '**o**'
  2. Don’t use these numbers: '**0**', '**1**'

3. Don’t use these "special" characters: '**,**', '**.**', '**&**', '**{**', '**}**', '**[**', '**]**', '**(**', '**)**', '**;**'
4. Start using these "special" characters: '**:**', '**=**', '**?**', '*****'

The Active Directory Users and Computers snap-in (via Microsoft Management Console) now features an improved Windows LAPS tab. The Windows LAPS password is now displayed in a new font that enhances its readability when shown in plain text.

- **PostAuthenticationAction support for terminating individual processes**

  A new option is added to the PostAuthenticationActions (PAA) Group Policy setting, "*Reset the password, sign out the managed account, and terminate any remaining processes*" located in **Computer Configuration** > **Administrative Templates** > **System** > **LAPS** > **Post-authentication actions**.

  This new option is an extension of the previous "*Reset the password and sign out the managed account*" option. Once configured, the PAA notifies and then terminates any interactive sign-in sessions. It enumerates and terminates any remaining processes that are still running under the Windows LAPS-managed local account identity. It's important to note that no notification precedes this termination.

  Furthermore, the expansion of logging events during post-authentication-action execution provides deeper insights into the operation.

To learn more about Windows LAPS, see What is Windows LAPS?.

Windows Terminal

The Windows Terminal, a powerful and efficient multishell application for command-line users, is available in this build. Search for "Terminal" in the search bar.

Winget

Winget is installed by default, which is a command line Windows Package Manager tool that provides comprehensive package manager solutions for installing applications on Windows devices. To learn more, see Use the winget tool to install and manage applications.

Accelerated Networking

Accelerated Networking simplifies the management of single root I/O virtualization (SR-IOV) for virtual machines hosted on Windows Server 2025 clusters. This feature uses the high-performance SR-IOV data path to reduce latency, jitter, and CPU utilization. Accelerated Networking also adds a management layer that handles prerequisite checking, host configuration, and VM performance settings.

See also

- Windows Server Insiders Community discussions

Feedback

Was this page helpful? Yes No