

# What's new in Windows Server 2019

Article • 07/31/2024

This article describes some of the new features in Windows Server 2019. Windows Server 2019 is built on the strong foundation of Windows Server 2016 and brings numerous innovations on four key themes: Hybrid Cloud, Security, Application Platform, and Hyper-Converged Infrastructure (HCI).

## General

### Windows Admin Center

Windows Admin Center is a locally deployed, browser-based app for managing servers, clusters, hyper-converged infrastructure, and Windows 10 PCs. It comes at no extra cost beyond Windows and is ready to use in production.

You can install Windows Admin Center on Windows Server 2019 and Windows 10 and earlier versions of Windows and Windows Server, and use it to manage servers and clusters running Windows Server 2008 R2 and later.

For more info, see [Windows Admin Center](#).

## Desktop experience

Because Windows Server 2019 is a Long-Term Servicing Channel (LTSC) release, it includes the **Desktop Experience**. Semi-Annual Channel (SAC) releases don't include the Desktop Experience by design; they're strictly Server Core and Nano Server container image releases. As with Windows Server 2016, during setup of the operating system you can choose between Server Core installations or Server with Desktop Experience installations.

## System Insights

System Insights is a new feature available in Windows Server 2019 that brings local predictive analytics capabilities natively to Windows Server. These predictive capabilities, each backed by a machine-learning model, locally analyze Windows Server system data, such as performance counters and events. System Insights allows you to understand how your servers are functioning and helps you reduce the operational expenses associated with reactively managing issues in your Windows Server deployments.

# Hybrid Cloud

## Server Core App Compatibility Feature on Demand

[Server Core App Compatibility Feature on Demand \(FOD\)](#) significantly improves the app compatibility by including a subset of binaries and components from Windows Server with the Desktop Experience. Server Core is kept as lean as possible by not adding the Windows Server Desktop Experience graphical environment itself, increasing the functionality and compatibility.

This optional feature on demand is available on a separate ISO and can be added to Windows Server Core installations and images only, using DISM.

## Windows Deployment Services (WDS) Transport Server role added to Server Core

Transport Server contains only the core networking parts of WDS. You can now use Server Core with the Transport Server role to create multicast namespaces that transmit data (including operating system images) from a standalone server. You can also use it if you want to have a PXE server that allows clients to PXE boot and download your own custom setup application.

## Remote Desktop Services integration with Azure AD

With Azure AD integration you can use Conditional Access policies, Multifactor Authentication, Integrated authentication with other SaaS Apps using Azure AD, and many more. For more information, see [Integrate Azure AD Domain Services with your RDS deployment](#).

## Networking

We made several improvements to the core network stack, such as TCP Fast Open (TFO), Receive Window Autotuning, IPv6, and more. For more information, see the [Core Network Stack feature improvement](#) [post](#).

## Dynamic vRSS and VMMQ

In the past, Virtual Machine Queues and Virtual Machine Multi-Queues (VMMQs) enabled much higher throughput to individual VMs as network throughputs first reached the 10GbE mark and beyond. Unfortunately, the planning, baselining, tuning,

and monitoring required for success became a much larger undertaking than IT administrators anticipated.

Windows Server 2019 improves these optimizations by dynamically spreading and tuning the processing of network workloads as needed. Windows Server 2019 ensures peak efficiency and removes the configuration burden for IT administrators. To learn more, see [Host network requirements for Azure Stack HCI](#).


## Security

### Windows Defender Advanced Threat Protection (ATP)

ATP's deep platform sensors and response actions expose memory and kernel level attacks and respond by suppressing malicious files and terminating malicious processes.

- For more information about Windows Defender ATP, see [Overview of Windows Defender ATP capabilities](#).
- For more information on onboarding servers, see [Onboard servers to Windows Defender ATP service](#).

**Windows Defender ATP Exploit Guard** is a new set of host-intrusion prevention capabilities enabling you to balance security risk and productivity requirements. Windows Defender Exploit Guard is designed to lock down the device against a wide variety of attack vectors and block behaviors commonly used in malware attacks. The components are:

- [Attack Surface Reduction \(ASR\)](#) is a set of controls that enterprises can enable to prevent malware from getting on the machine by blocking suspicious malicious files. For example, Office files, scripts, lateral movement, ransomware behavior, and email-based threats.
- [Network protection](#) protects the endpoint against web-based threats by blocking any outbound process on the device to untrusted hosts/IP addresses through Windows Defender SmartScreen.
- [Controlled folder access](#)  protects sensitive data from ransomware by blocking untrusted processes from accessing your protected folders.
- [Exploit protection](#) is a set of mitigations for vulnerability exploits (replacing EMET) that can be easily configured to protect your system and applications.

- [Windows Defender Application Control](#) (also known as Code Integrity (CI) policy) was released in Windows Server 2016. We've made deployment easier by including default CI policies. The default policy allows all Windows in-box files and Microsoft applications, such as SQL Server, and blocks known executables that can bypass CI.

## Security with Software Defined Networking (SDN)

[Security with SDN](#) delivers many features to increase customer confidence in running workloads, either on-premises, or as a service provider in the cloud.

These security enhancements are integrated into the comprehensive SDN platform introduced in Windows Server 2016.

For a complete list of what's new in SDN see, [What's New in SDN for Windows Server 2019](#).

## Shielded Virtual Machines improvements

We made the following improvements to Shielded Virtual Machines.

### Branch office improvements

You can now run shielded virtual machines on machines with intermittent connectivity to the Host Guardian Service by using the new [fallback HGS](#) and [offline mode](#) features. Fallback HGS allows you to configure a second set of URLs for Hyper-V to try if it can't reach your primary HGS server.

Even if you can't reach the HGS, offline mode lets you continue to start up your shielded VMs. Offline mode also lets you start your VMs as long as the VM has started successfully once and the host's security configuration hasn't changed.

### Troubleshooting improvements

We also made it easier to troubleshoot your shielded VMs by enabling support for VMConnect Enhanced Session Mode and PowerShell Direct. These tools are useful when you lose network connectivity to your VM and need to update its configuration to restore access. To learn more, see [Guarded fabric and shielded VMs](#).

You don't need to configure these features because they become automatically available when you place a shielded VM on a Hyper-V host running Windows Server version 1803 or later.

## Linux support

If you run mixed-OS environments, Windows Server 2019 now supports running Ubuntu, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server inside shielded virtual machines.

## HTTP/2 for a faster and safer Web

- Improved coalescing of connections to deliver an uninterrupted and properly encrypted browsing experience.
- Upgraded HTTP/2's server-side cipher suite negotiation for automatic mitigation of connection failures and ease of deployment.
- Changed our default TCP congestion provider to Cubic to give you more throughput!

## Encrypted networks

Virtual network encryption encrypts virtual network traffic between virtual machines within subnets that have the **Encryption Enabled** label. Encrypted networks also use Datagram Transport Layer Security (DTLS) on the virtual subnet to encrypt packets. DTLS protects your data from eavesdropping, tampering, and forgery by anyone with access to the physical network.

For more information, see [Encrypted networks](#).

## Firewall auditing

[Firewall auditing](#) is a new feature for SDN firewall that records any flow processed by SDN firewall rules and access control lists (ACLs) that have logging enabled.

## Virtual network peering

[Virtual network peering](#) lets you connect two virtual networks seamlessly. Once peered, the virtual networks appear in monitoring as one.

## Egress metering

[Egress metering](#) offers usage meters for outbound data transfers. Network Controller uses this feature to keep an allowlist of all IP ranges used within SDN per virtual

network. These lists consider any packet heading to a destination not included within the listed IP ranges to be billed as outbound data transfers.

## Storage

Here are some of the changes we've made to Storage in Windows Server 2019. Storage is also affected by updates to [Data deduplication](#), particularly its update to DataPort API for optimized ingress or egress to deduplicated volumes.

## File Server Resource Manager

It's now possible to prevent the File Server Resource Manager service from creating a change journal (also known as a USN journal) on all volumes when the service starts. Preventing the creation of the change journey can conserve space on each volume, but will disable real-time file classification. For more information, see [File Server Resource Manager overview](#).

## SMB

- Windows Server no longer installs the SMB1 client and server by default. Additionally, the ability to authenticate as a guest in SMB2 and later is off by default. For more information, see [SMBv1 is not installed by default in Windows 10 version 1709, Windows Server version 1709 and later versions](#) [↗](#).
- You can now disable oplocks in SMB2+ for legacy applications. You can also require signing or encryption on per-connection basis from a client. For more information, see [SMBShare PowerShell module help](#).

## Storage Migration Service

Storage Migration Service makes it easier to migrate servers to a newer version of Windows Server. This graphical tool inventories data on servers, then transfers the data and configuration to newer servers. The Storage Migration Service can also move the identities of the old servers to the new servers so users don't have to reconfigure their profiles and apps. For more information, see [Storage Migration Service](#).

Windows Admin Center version 1910 added the ability to deploy Azure virtual machines. This update integrates Azure VM deployment into Storage Migration Service. For more information, see [Azure VM migration](#).

You can also access the following post-release-to-manufacturing (RTM) features when running the Storage Migration Server orchestrator on Windows Server 2019 with [KB5001384](#) installed or on Windows Server 2022:

- Migrate local users and groups to the new server.
- Migrate storage from failover clusters, migrate to failover clusters, and migrate between standalone servers and failover clusters.
- Migrate storage from a Linux server that uses Samba.
- Sync migrated shares more easily into Azure by using Azure File Sync.
- Migrate to new networks such as Azure.
- Migrate NetApp Common Internet File System (CIFS) servers from NetApp Federated Authentication Service (FAS) arrays to Windows servers and clusters.

## Storage Spaces Direct

Here's what's new in Storage Spaces Direct. For more information about how to acquire validated Storage Spaces Direct systems, see [Azure Stack HCI solution overview](#).

- Deduplication and compression for ReFS volumes. Variable-size chunk store with optional compression maximizes savings rates, while multi-threaded post-processing architecture minimizes performance impact. This feature supports volumes up to 64 TB and deduplicates the first 4 MB of each file.
- Native support for persistent memory, which lets you manage persistent memory like any other drive in PowerShell or Windows Admin Center. This feature supports Intel Optane DC PM and NVDIMM-N persistent memory modules.
- Nested resiliency for two-node hyper-converged infrastructure at the edge. With the help of a new software resiliency option based on RAID 5+1, you can now survive two hardware failures simultaneously. A two-node Storage Spaces Direct cluster provides continuously accessible storage for apps and virtual machines even if one server node goes down and another server node has a drive failure.
- Two-server clusters can now use a USB flash drive as a witness. If a server goes down and then back up, the USB drive cluster knows which server has the most up-to-date data. For more information, see our [Storage Spaces Direct announcement blog post](#) and [Configure a file share witness for Failover Clustering](#).
- Windows Admin Center supports a dashboard that lets you manage and monitor Storage Spaces direct. You can monitor IOPS and IO latency from the overall cluster level down to individual SSDs or HDDs at no extra cost. To learn more, see [What is Windows Admin Center?](#).

- Performance history is a new feature that provides effortless visibility into resource utilization and measurements. To learn more, see [Performance history for Storage Spaces Direct](#).
- Scale up to 4 PB per cluster using a capacity of up to 64 volumes of up to 64 TB. You can also stitch multiple clusters together into a [cluster set](#) for even greater scale within a single storage namespace.
- By utilizing mirror-accelerated parity, it is possible to construct Storage Spaces Direct volumes that incorporate both mirror and parity strategies, similar to a blend of RAID-1 and RAID-5/6. Mirror-accelerated parity is now two times faster than Windows Server 2016.
- Drive latency outlier detection automatically identifies slow drives in PowerShell and Windows Admin Center with an "Abnormal Latency" status.
- Manually delimit the allocation of volumes to increase fault tolerance. For more information, see [Delimit the allocation of volumes in Storage Spaces Direct](#).

## Storage Replica

Here's what's new in Storage Replica.

- Storage Replica is now available in Windows Server 2019 Standard Edition and Windows Server 2019 Datacenter Edition. However, with the Standard Edition, you can only replicate one volume, and that volume can only go up to 2 TB in size.
- Test failover is a new feature that allows you to temporarily mount a snapshot of the replicated storage on a destination server for testing or backup purposes. For more information, see [Frequently asked questions about Storage Replica](#).
- Storage Replica log performance improvements, such as improved replication throughput and latency on all-flash storage and Storage Spaces Direct clusters that replicate between each other.
- Windows Admin Center support, including graphical management of replication using Server Manager for server-to-server, cluster-to-cluster, and stretch cluster replication.

## Data deduplication

Windows Server 2019 now supports the Resilient File System (ReFS). ReFS lets you store up to ten times more data on the same volume with deduplication and compression for



the ReFS filesystem. The variable-size chunk store comes with an optional compression feature that can maximize savings rates, while the multi-threaded post-processing architecture keeps performance impact minimal. ReFS supports volumes up to 64 TB and deduplicates the first 4 TB of each file. To learn more, see [How to turn on deduplication and compression in Windows Admin Center](#) for a quick video demonstration.

## Failover Clustering

We added the following features to failover clustering in Windows Server 2019:

- Cluster sets group multiple clusters together into a loosely coupled grouping of multiple failover clusters that come in three types: compute, storage, and hyper-converged. This grouping increases the number of servers in a single software-defined datacenter (SDDC) solution beyond the current limits of a cluster. With cluster sets, you can move online virtual machines between clusters within the cluster set. For more information, see [Deploy a cluster set](#).
- Clusters are now Azure-aware by default. Azure-aware clusters automatically detect when they're running in Azure IaaS virtual machines, then optimize their configuration to achieve the highest levels of availability. These optimizations include proactive failover and logging of Azure planned maintenance events. Automated optimization makes deployment simpler by removing the need to configure the load balancer with Distributed Network Name for the cluster name.
- Cross-domain cluster migration lets failover clusters dynamically move from one Active Directory domain to another, simplifying domain consolidation and allowing hardware partners to create clusters and join them to the customer's domain at a later time.
- The USB witness feature lets you use a USB drive attached to a network switch as a witness in determining quorum for a cluster. This feature includes extended File Share Witness support for any SMB2-compliant device.
- The CSV cache is now enabled by default to boost virtual machine performance. MSDTC now supports Cluster Shared Volumes to allow deploying MSDTC workloads on Storage Spaces Direct, such as with SQL Server. Enhanced logic to detect partitioned nodes with self-healing to return nodes to cluster membership. Enhanced cluster network route detection and self-healing.
- Cluster Aware Updating (CAU) is now integrated and aware of Storage Spaces Direct, validating and ensuring data resynchronization completes on each node.

Cluster Aware Updating inspects updates to intelligently restart only if necessary. This feature lets you restart all servers in the cluster for planned maintenance.

- You can now use file share witnesses in the following scenarios:
  - Absent or poor Internet access because of a remote location, preventing the use of a cloud witness.
  - Lack of shared drives for a disk witness. For example, a configuration that doesn't use shared disks, such as Storage Spaces Direct hyperconverged configuration, a SQL Server Always On Availability Groups (AG), or an Exchange Database Availability Group (DAG).
  - Lack of domain controller connection due to the cluster being behind a DMZ.
  - A workgroup or cross-domain cluster that doesn't have an Active Directory cluster name object (CNO). Windows Server now also blocks using a DFS Namespaces share as a location. Adding a file share witness to a DFS share can cause stability issues for your cluster, and this configuration has never been supported. We added logic to detect if a share uses DFS Namespaces, and if DFS Namespaces is detected, Failover Cluster Manager blocks creation of the witness and displays an error message about not being supported.
- A cluster hardening feature has been implemented that enhances the security of intra-cluster communication over Server Message Block (SMB) for Cluster Shared Volumes and Storage Spaces Direct. This feature leverages certificates to provide the most secure platform possible. By doing so, Failover Clusters can now operate without any dependencies on NTLM, which enables security baselines to be established.
- Failover Clusters no longer use NTLM authentication. Instead, Windows Server 2019 clusters now exclusively use Kerberos and certificate-based authentication. Users don't need to make any changes or deploy anything to take advantage of this security enhancement. This change also lets you deploy failover clusters in environments where NTLM is disabled.

## Application Platform

### Linux containers on Windows

It's now possible to run Windows and Linux-based containers on the same container host, using the same docker daemon. You can now have a heterogeneous container

host environment providing flexibility to application developers.

## Built-in support for Kubernetes

Windows Server 2019 continues the improvements to compute, networking, and storage from the Semi-Annual Channel releases needed to support Kubernetes on Windows. More details are available in upcoming Kubernetes releases.

- [Container Networking](#) in Windows Server 2019 greatly improves usability of Kubernetes on Windows. We've enhanced platform networking resiliency and support of container networking plugins.
- Deployed workloads on Kubernetes are able to use network security to protect both Linux and Windows services using embedded tooling.

## Container improvements

- **Improved integrated identity**

We've made integrated Windows authentication in containers easier and more reliable, addressing several limitations from prior versions of Windows Server.

- **Better application compatibility**

Containerizing Windows-based applications just got easier: The app compatibility for the existing **windowsservercore** image has been increased. For applications with more API dependencies, there's now a third base image: **windows**.

- **Reduced size and higher performance**

The base container image download sizes, size on disk and startup times have been improved to speed up container workflows.

- **Management experience using Windows Admin Center (preview)**

We've made it easier than ever to see which containers are running on your computer and manage individual containers with a new extension for Windows Admin Center. Look for the "Containers" extension in the [Windows Admin Center public feed](#).

## Compute improvements

- **VM Start Ordering** VM Start Ordering is also improved with OS and Application awareness, bringing enhanced triggers for when a VM is considered started before

starting the next.

- **Storage-class memory support for VMs** enables NTFS-formatted direct access volumes to be created on non-volatile DIMMs and exposed to Hyper-V VMs. Hyper-V VMs can now use the low-latency performance benefits of storage-class memory devices.
- **Persistent Memory support for Hyper-V VMs** To use the high throughput and low latency of persistent memory (also known as storage class memory) in virtual machines, it can now be projected directly into VMs. Persistent memory can help to drastically reduce database transaction latency or reduce recovery times for low latency in-memory databases on failure.
- **Container storage – persistent data volumes** Application containers now have persistent access to volumes. For more info, see [Container Storage Support with Cluster Shared Volumes \(CSV\), Storage Spaces Direct \(S2D\), SMB Global Mapping](#) [↗](#).
- **Virtual machine configuration file format (updated)** The VM guest state file (`.vmgs`) has been added for virtual machines with a configuration version of 8.2 and higher. The VM guest state file includes device state information that was previously part of the VM runtime state file.

## Encrypted Networks

[Encrypted Networks](#) - Virtual network encryption allows encryption of virtual network traffic between virtual machines that communicate with each other within subnets marked as **Encryption Enabled**. It also utilizes Datagram Transport Layer Security (DTLS) on the virtual subnet to encrypt packets. DTLS protects against eavesdropping, tampering, and forgery by anyone with access to the physical network.

## Network performance improvements for virtual workloads

[Network performance improvements for virtual workloads](#) maximizes the network throughput to virtual machines without requiring you to constantly tune or over-provision your host. Improved performance lowers the operations and maintenance cost while increasing the available density of your hosts. These new features are:

- Dynamic Virtual Machine Multi-Queue (d.VMMQ)
- Receive Segment Coalescing in the vSwitch

## Low Extra Delay Background Transport

Low Extra Delay Background Transport (LEDBAT) is a latency optimized, network congestion control provider designed to automatically yield bandwidth to users and applications. LEDBAT consumes bandwidth available while the network isn't in use. The technology is intended for use when deploying large, critical updates across an IT environment without impacting customer facing services and associated bandwidth.

## Windows Time Service

The [Windows Time Service](#) includes true UTC-compliant leap second support, a new time protocol called Precision Time Protocol, and end-to-end traceability.

## High performance SDN gateways

[High performance SDN gateways](#) in Windows Server 2019 greatly improves the performance for IPsec and GRE connections, providing ultra-high-performance throughput with much less CPU utilization.

## New Deployment UI and Windows Admin Center extension for SDN

Now, with Windows Server 2019, it's easy to deploy and manage through a new deployment UI and Windows Admin Center extension that enable anyone to harness the power of SDN.

## Windows Subsystem for Linux (WSL)

WSL enables server administrators to use existing tools and scripts from Linux on Windows Server. Many improvements showcased in the [command line blog](#) [↗](#) are now part of Windows Server, including Background tasks, DriveFS, WSLPath, and much more.

## Active Directory Federation Services

Active Directory Federation Services (AD FS) for Windows Server 2019 includes the following changes.

## Protected sign ins

Protected sign ins with AD FS now include the following updates:

- Users can now use third-party authentication products as their first factor without exposing passwords. In cases where the external authentication provider can prove two factors, it can use multifactor authentication (MFA).
- Users can now use passwords as an extra factor after using a non-password option as the first factor. This in-box support improves overall experience from AD FS 2016, which required downloading a GitHub adapter.
- Users can now build their own plug-in risk assessment modules to block certain types of requests during the preauthentication stage. This feature makes it easier to use cloud intelligence such as identity protection to block risky users or transactions. For more information, see [Build Plug-ins with AD FS 2019 Risk Assessment Model](#).
- Improves Extranet Smart Lockout (ESL) quick-fix engineering (QFE) by adding the following capabilities:
  - You can now use audit mode while protected by classic extranet lockout functionality.
  - Users can now use independent lockout thresholds for familiar locations. This feature lets you run multiple instances of apps within a common service account to roll over passwords with minimal disruption.

## Other security improvements

AD FS 2019 includes the following security improvements:

- Remote PowerShell using SmartCard Sign-in lets users remote connect to AD FS with SmartCards by running PowerShell commands. Users can also use this method to manage all PowerShell functions including multi-node cmdlets.
- HTTP header customization lets users customize HTTP headers created during AD FS responses. Header customization includes the following types of headers:
  - HSTS, which only lets you use AD FS endpoints on HTTPS endpoints for a compliant browser to enforce.
  - X-frame-options, which lets AD FS admins allow specific relying parties to embed iFrames for AD FS interactive sign-in pages. You should only use this header on HTTPS hosts.
  - Future header. You can also configure multiple future headers.

For more information, see [Customize HTTP security response headers with AD FS 2019](#).

## Authentication and policy capabilities

AD FS 2019 includes the following authentication and policy capabilities:

- Users can now create rules to specify which authentication provider their deployment invokes for extra authentication. This feature helps with transitioning between authentication providers and securing specific apps that have special requirements for extra authentication providers.
- Optional restrictions for Transport Layer Security (TLS)-based device authentications so that only applications that require TLS can use them. Users can restrict client TLS-based device authentications so that only applications doing device-based conditional access can use them. This feature prevents unwanted prompts for device authentication for applications that don't require TLS-based device authentication.
- AD FS now supports redoing second-factor credentials based on the second factor credential freshness. This feature allows users to only require TFA for the first transaction, then only require the second factor on a periodic basis. You can only use this feature on applications that can provide an extra parameter in the request, since it's not a configurable setting in AD FS. Microsoft Entra ID supports this parameter if you configure the **Remember my MFA for X Days** setting to have *supportsMFA* set to **True** in the Microsoft Entra ID federated domain trust settings.

## Single sign-on improvements

AD FS 2019 also includes the following single sign-on (SSO) improvements:

- AD FS now uses a [paginated UX flow](#) and a centered user interface (UI) that provides a smoother sign-in experience for users. This change mirrors functionality offered in Azure AD. You may need to update your organization's logo and background images to suit the new UI.
- We fixed an issue that caused the MFA state to not persist when using Primary Refresh Token (PRT) authentication on Windows 10 devices. Users should now be prompted for second factor credentials less often. The experience should now be consistent when device authentication is successful on client TLS and PRT authentication.

# Support for building modern line-of-business apps

AD FS 2019 includes the following features to support building modern line-of-business (LOB) apps:

- AD FS now includes OAuth device flow profile support for signing in using devices without a UI surface area to support rich sign-in experiences. This feature lets users finish signing in on a different device. The Azure Command-Line Interface (CLI) experience in Azure Stack requires this functionality, and you can also use it in other scenarios.
- You no longer require the *Resource* parameter to use AD FS, which is in line with current OAuth specifications. Clients now only need to provide the relying party trust identifier as the scope parameter long with requested permissions.
- You can use cross-origin resource sharing (CORS) headers in AD FS responses. These new headings let users build single-page applications that allow client-side JavaScript libraries to validate the *id\_token* signature by querying for the signing keys from the Open ID Connect (OIDC) discovery document on AD FS.
- AD FS includes Proof Key for Code Exchange (PKCE) support for secure auth code flow within OAuth. This extra layer of security prevents malicious actors from hijacking the code and replaying it from a different client.
- We fixed a minor issue that caused AD FS to only send the x5t claim. AD FS now also sends a kid claim to denote the key ID hint for signature verification.

## Supportability improvements

Admins can now configure AD FS to allow users to send error reports and debug logs to them as a ZIP file for troubleshooting. Admins can also configure a Simple Mail Transfer Protocol (SMTP) connection to automatically send the ZIP file to a triage email account. Another setting lets admins automatically create a ticket for their support system based on that email.

## Deployment updates

The following deployment updates are now included in AD FS 2019:

- AD FS has [a similar function to its Windows Server 2016 version](#) that makes it easier to upgrade Windows Server 2016 server farms into Windows Server 2019 server farms. A Windows Server 2019 server added to a Windows Server 2016 server farm will only behave like a Windows Server 2016 server until you're ready



to upgrade. For more information, see [Upgrading to AD FS in Windows Server 2016](#).

## SAML updates

AD FS 2019 includes the following Security Assertion Markup Language (SAML) updates:

- We fixed issues in aggregated federation support, such as InCommon, in these areas:
  - Improved scaling for many entities in the aggregated federation metadata document. Previously, scaling for these entities would be unsuccessful and return an ADMIN0017 error message.
  - You can now make queries using the *ScopeGroupID* parameter by running the `Get-AdfsRelyingPartyTrustsGroup` PowerShell cmdlet.
  - Improved handling of error conditions for duplicate *entityID* values.

## Azure AD style resource specification in scope parameter

Previously, AD FS required the desired resource and scope to be in a separate parameter in any authentication request. For example, the following example OAuth request contains a scope parameter:

HTTP

```
https://fs.contoso.com/adfs/oauth2/authorize?
response_type=code&client_id=claimsxrayclient&resource=urn:microsoft:ads:cl
aimsxray&scope=oauth&redirect_uri=https://adfshelp.microsoft.com/
ClaimsXray/TokenResponse&prompt=login
```

With AD FS on Windows Server 2019, you can now pass the resource value embedded in the scope parameter. This change is consistent with authentication against Microsoft Entra ID.

The scope parameter can now be organized as a space-separated list that structures each entity as a resource or scope.

### ⓘ Note

You can only specify one resource in the authentication request. If you include more than one resource in the request, AD FS returns an error and authentication

doesn't succeed.

---

## Feedback

Was this page helpful?

 Yes

 No