

Microsoft EEAP Release Notes

Key information	Build validation and feedback	Bug fixes	Known issues	Breaking changes
-----------------	-------------------------------	-----------	--------------	------------------

Windows Server LTSC and SAC preview, build 17661.1001

These release notes describe the new features, bug fixes, known issues, and breaking changes introduced since build 17655.1000 of Windows Server 2019 Long-Term Servicing Channel (LTSC).

This build includes the following:

Long-Term Servicing Channel (LTSC) preview

- Windows Server 2019 Datacenter Edition and Standard Edition with Desktop Experience and Server Core installation options (ISO and VHDX)

Semi-Annual Channel (SAC) preview

- Windows Server Datacenter Edition and Standard Edition with Core installation options (ISO and VHDX)

Additional content (LTSC and SAC)

- Nano Server Container
- Server Core Container
- Microsoft Hyper-V Server preview

Key information

This section has key information required for testing the latest build.

Windows Server activation keys

This build and all future builds will require use of activation keys during setup. The following keys allow for unlimited activations.

Datacenter	6XBNX-4JQGW-QX6QG-74P76-72V67
Standard	MFY9F-XBN2F-TYFMP-CCV49-RMYVH

This Server Insider pre-release build will expire on July 2, 2018.

Symbols for debugging

If you need symbols, you can obtain them from the public symbol server. For details, see [Using the Microsoft Symbol Server](#).

HLK and Certification Guidance

The Windows Hardware Lab Kit (HLK) will be updated to support Windows 10 vNext and Windows Server LTSC vNext.

The HLK is updated each week and available for download on Microsoft Collaborate, you will see the download locations with your weekly build notifications.

The HLK for Windows 10 and Windows Server LTSC vNext will enforce the Windows 10 hardware requirements and policies, which will be posted on MSDN in March, and is designed for testing Windows 10 vNext and Windows Server LTSC vNext (codename RS5).

The support scenarios identified in the following table will be accepted.

HLK VERSION	WINDOWS 10 VERSIONS SUPPORTED	DEVICE/COMPONENT SUBMISSIONS ACCEPTED	SYSTEM SUBMISSIONS ACCEPTED
"RS5"	Code named "RS5"	"RS5" client device/component "vNext" Server device/component	"vNext" Server systems
1709	1709 - client	1709 client device/component	1709 client systems

HLK VERSION	WINDOWS 10 VERSIONS SUPPORTED	DEVICE/COMPONENT SUBMISSIONS ACCEPTED	SYSTEM SUBMISSIONS ACCEPTED
1703	1703 - client 1607 - client	1703 client device/component 1607 client device/component	1703 client systems
1607	1607 - client 1607 - Server, Azure Stack, SDDC 1511 - client	1607 client device/component 1607 Server device/component 1511 client device/component	1607 Server systems

When submitting a Windows 10 RS5 and Windows Server LTSC vNext HLK package for validation, you must use Windows 10 vNext and Windows Server LTSC vNext, version build TBD or newer on the test device. The submission will otherwise be rejected.

You must continue to use the Windows Hardware Certification Kit (HCK) version 2.1 to certify for following operating systems:

- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows Server 2012 R2

You must continue to use the Windows Logo Kit (WLK) version 1.6 to certify for following operating systems:

- Windows Server 2008 R2 (x64 and ia64)
- Windows Server 2008 (x86, x64 and ia64)

Certification for Windows Server 2016, Azure Stack and SDDC must meet the Windows Hardware Compatibility Requirements as stated in version 1607 of the documentation, use the 1607 version of the Windows Server 2016 operating system and use HLK version 1607 build 14393 with matching playlist and supplemental content to generate logs and following the policies stated in the Windows Server Policy. Questions about the Azure Stack or SDDC program or how to submit the results for solution validation should be directed to the appropriate Microsoft contact – technical account manager or partner management contact.

<p>Installing kits on released operating systems</p>	<p>If you are installing the Windows 10 kits on a publicly released OS such as Windows 10, version 1703, Windows 10, version 1607, Windows 10, version 1511, Windows 10, Windows 8.1, Windows 8, or Windows 7, you must disable strong name-signing and manually install two additional test certificates. To do this, perform the following installation procedure once for each test computer, using an account with administrator privileges on the controller computer:</p> <ul style="list-style-type: none"> • From the KitPreinstall folder, install the TestRoot.cer and TestRoot-SHA2.cer test certificates using the following steps: <ol style="list-style-type: none"> 1. From the controller computer, right-click the certificate. 2. Click Install Certificate. 3. Click Next. 4. Accept the default for the certificate store, and click Next. 5. Click Finish. • From the same folder, disable strong name signing by installing the StrongNameBypass.reg and WOW64StrongNameBypass.reg registry keys, as follows: <ol style="list-style-type: none"> 1. From the controller computer, right-click the registry key. 2. Click Merge. 3. Click Run. 4. Click Yes.
--	--

Build validation and feedback

In each preview release, there are two major areas that we would like you to try out:

- **In-place OS Upgrade** (from Windows Server 2012 R2, Windows Server 2016 or a previous preview build).
- **Application compatibility** – please let us know if any server roles or applications stops working or fails to function as it used to.

Please report any issues you find.

In addition, please also validate functionality that was introduced in previous preview

releases. For a list of new features introduced in earlier releases, see aka.ms/ServerInsider-WhatsNew.

As always, we welcome your feedback.

Bug fixes

The bug fixes described in the following table are new in this build.

WORK ITEM	DESCRIPTION OF BUG FIX
16412874	We fixed an issue that prevented use of full-width characters in a computer name when support for Unicode UTF-8 is enabled.
15091678, 17066730	We fixed an issue that prevented input of Japanese in the Input Method Editor (IME) on recent preview builds of the operating system.

Known issues

The following known issues are new in this build, or they were not resolved in the last build.

WORK ITEM	DESCRIPTION OF KNOWN ISSUE
17327138	[NEW] The ISO file for a recent preview release, Windows Server 2019, build 17639.1000, cannot be opened by Windows System Image Manager (Windows SIM), due to duplicate descriptors.
00000000	In-place OS upgrade: Domain Controllers. Active Directory (AD) Domain Controllers (DC) might not be upgraded correctly by an in-place upgrade unless the NT Directory Service (NTDS) is stopped before initiating the upgrade. To ensure recoverability in the case of failure, back up any AD DC before performing an in-place OS upgrade.

WORK ITEM	DESCRIPTION OF KNOWN ISSUE
16616234	The size of a file according to NTFS and a stream control block can become different from the size according to Cache Manager. This might cause a bug check if a read operation is out of bounds for the file size that Cache Manager has stored.
12139737	Editing or creating policies for AppLocker can cause the MMC snap-in to crash when generated rules for a packaged app.
16060707	After upgrading the operating system, the AppX database may have corrupted entries, which causes problems for components that use those entries. An administrator might notice this issue when generating packaged app rules or when managing an installed package, resulting in error messages such as "This wizard has encountered a fatal error and cannot continue" and "MMC has detected an error in a snap-in and will unload it."

Breaking changes

The breaking changes described in the following table are included in this build.

BREAKING CHANGE	DESCRIPTION OF BREAKING CHANGE
Print as an optional component	<p>To reduce resource use, Print-Server will now be an optional component, staged by default, on Server Core. The executable files will be staged, but not in \Windows\System32\, and they will not be enabled by default. To enable printing, administrators can run a PowerShell command: Install-WindowsFeature Print-Server. This command can be added to setup scripts for configuring print servers.</p> <p>This arrangement is different from previous versions of Windows Server. On Windows Server Core 2012, Print-Server was an optional feature and deactivated by default. On Windows Server Core 2016, the executable files were present and running, but the Print-Server feature did not operate unless enabled (which added required RPC endpoints).</p>