Windows 365 Cloud PC

- Cloud PC Basics
- Components for Cloud PC deployment
- Target audience for Cloud PC
- Comparison of variants (CPC vs. AVD vs. Citrix)

Cloud PC Basics

Cloud PC keywords

- Virtual Windows desktop from the Microsoft Cloud
- Desktop as a Service (DaaS) solution
- VDI solution from Microsoft
- Management via Intune admin center
- Independent of end device (browser, apps)
- License-based payment model
- Easy to use for end user
- Easy to administer for engineers and supporter

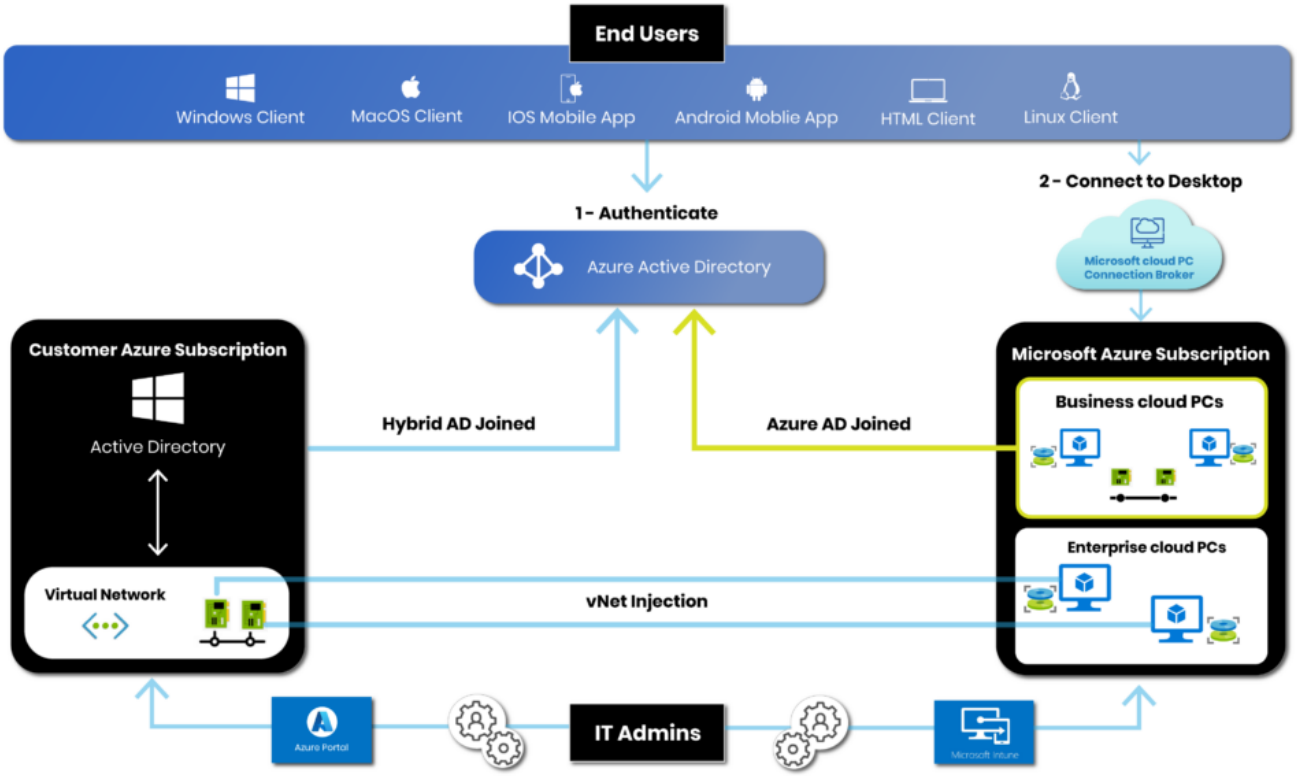
Cloud PC architecture

In the background, Cloud PC is based on Azure Virtual Desktop (AVD), but with a lot of standardized automations and cost management. To interact with the backend, the Cloud PC service from Microsoft uses the standardized Microsoft Graph API. Accordingly, automations and API queries can also be carried out very easily.

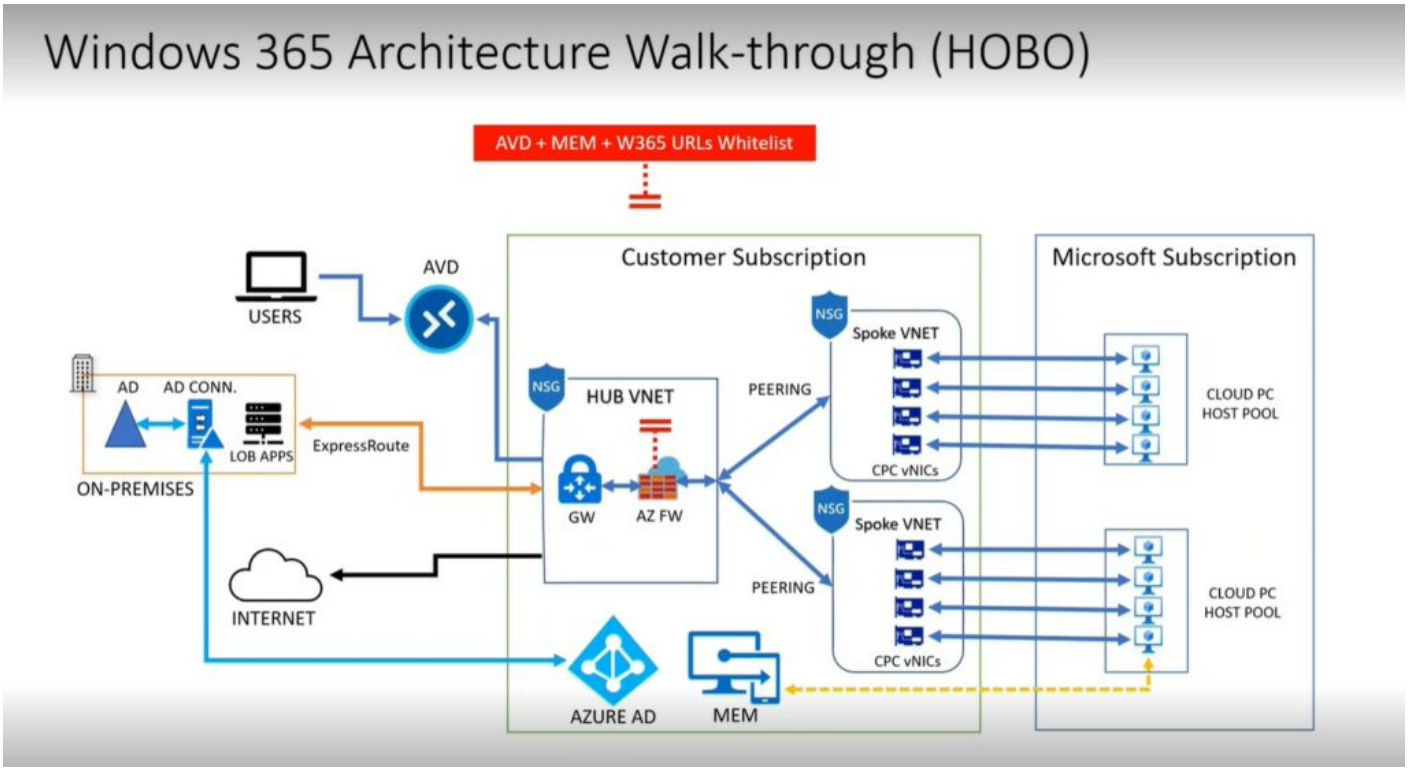
The network cards of cloud pcs can be self-administered if required. Cloud PCs can join an azure virtual network and connect to existing infrastructure, either in the cloud or on premise. All VMs and disks cannot be viewed in your own azure portal. These resources run in an Azure subscription from Microsoft.

The end user can access their Cloud PC via the Remote Desktop App on their device or via Webbrowser and the AVD portal, on which you can see both AVD and Windows 365 resources.. In addition, there is an app for devices and a website for connecting to the cloud PC.

Access schema



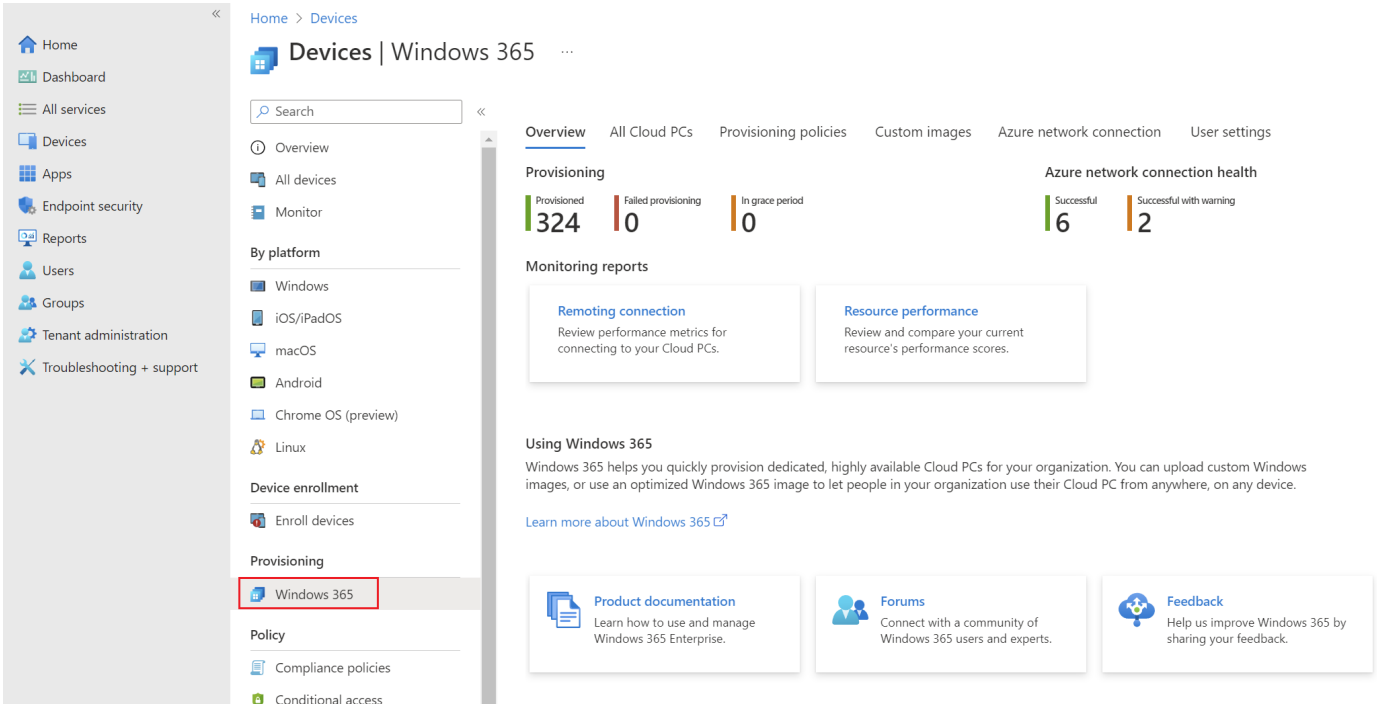
Network schema



Components for Cloud PC deployment

Windows 365 license

To enable the Windows 365 GUI in Intune admin center, you have to own at least one Windows 365 license. Afterwards the GUI will be visible under Devices.



Azure network connection

Azure Virtual Network with corresponding subnet is needed if you want to connect the Cloud PCs to your existing infrastructure. You have the option to connect the Cloud PC directly to the internet without having to configure an azure environment.

Attention: You have to size the vnet and subnet before deploying the first network cards or Cloud PCs to this network. Resizing in Azure Virtual Networks or Subnets is not possible with deployed workload! In addition, at least the owner role must be present at the subscription level during creation. Cloud PC unfortunately checks the name of the assigned role of the user and not the effective permissions (custom roles do not work!).

On the azure network connection, you can specify which method of join you want to perform to these specific Cloud PCs. You can choose between Windows Server Active Directory or Microsoft Entra ID only. Either way you need an Object in your Microsoft Entra ID, so the least cloud deployment is Windows Server AD with Hybrid Microsoft Entra ID Join.

Configuration on azure vnet

You have to configure the routing, dns and dhcp on your vnet properly so that the deployment of new Cloud PCs will be successful. If you use AD Joins for your Cloud PCs, the AD Domain Controller must all be accessible.

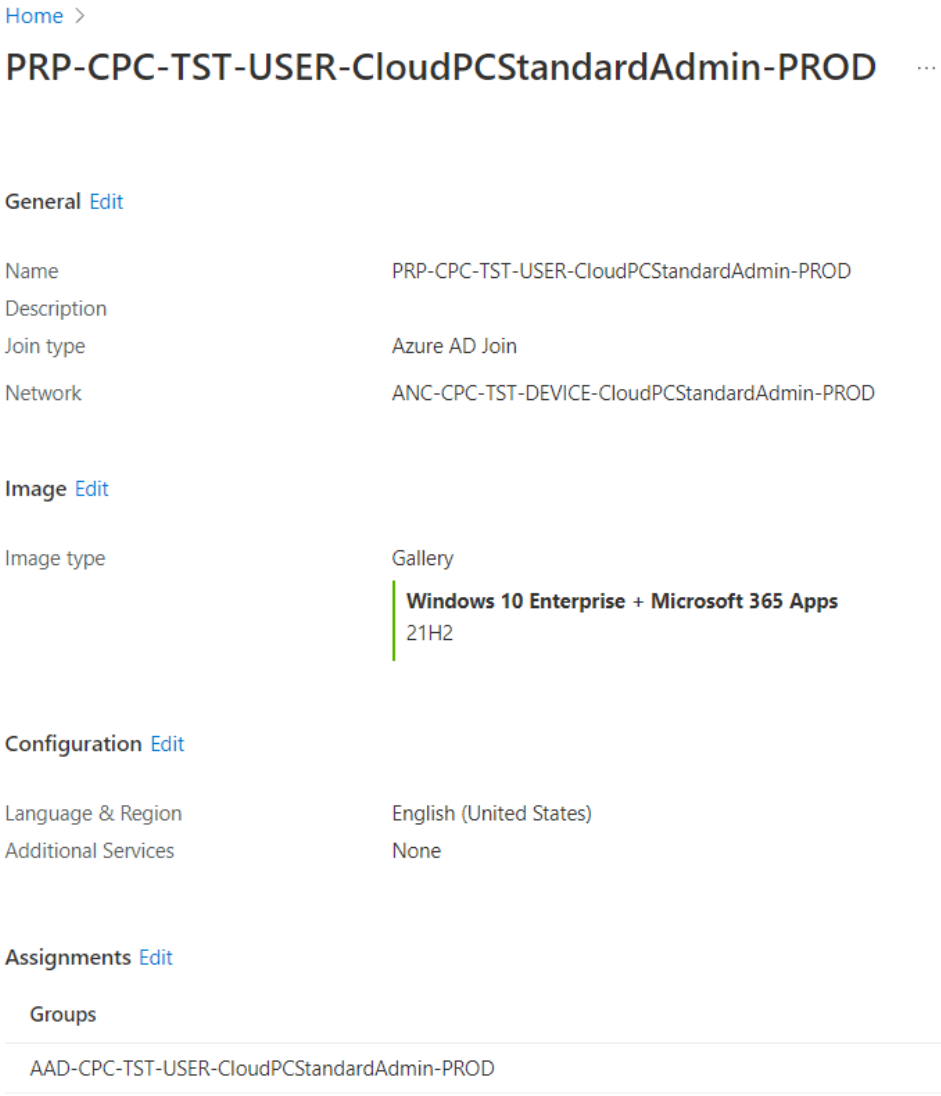
URLs to directly connect to internet

Windows 365 Cloud PC needs a few URLs wich cannot be routed through a proxy. These URLs have to go directly to the internet and needed to be allowed from the whole Cloud PC network to the internet:

- graph.microsoft.com:443
- *.core.windows.net:443
- *.wvd.microsoft.com:443
- global.azure-devices-provisioning.net:5671

Provisioning policy

Provisioning policies contain the whole configuration summary for Cloud PCs. In this policy, the windows image used, and the azure network connection is contracted and assigned to an Microsoft Entra ID group. A Cloud PC is then provided for the users in this group, if the user has a corresponding Windows 365 licence.



Windows images

You can choose between two options for the Windows images. One is the so-called "Gallery Images". These are provided by Microsoft and do not contain any pre-installed software. The latest patches are also installed directly by Microsoft.
The second option is the use of custom images. These custom images must be managed by the user and kept up to date. However, software can be pre-installed, and configurations can also be included in the image. Cloud PC images can be created from Azure VM images.

Attention: The image must be in the same subscription as the Azure Network Connection.

User settings

In user settings you can specify if the end user has local admin rights on their Cloud PCs. Furthermore, the settings for point-in-time restore service can be adjusted here.

Add user setting

Windows 365

1 Settings 2 Assignments 3 Review + Create

General

Name *

Enter a name

Enable Local admin

Point-in-time restore service

The point-in-time restore service can be used to restore a user's Cloud PC to a backup made at a specific point in time.Users will lose any data stored on their Cloud PC disk between the current time and recovery time. Learn more

Allow user to initiate restore service

Frequency of restore-point service *

12 hours

Target audience for Cloud PC

Suitable for these user groups

- Special network access (e.g., administratornetwork)
- Bring your own device employees
- External service profiders
- Temporary employees
- Work from home without VPN
- Run unattended for a long time
- Fast reliable access to other cloud services at the same location

Not suitable for this user group

- Complex work in the 3d area (CAD)
- Highly demanding latencies for application access to on premise resources
- Everything that has to do with graphics-intensive programmes
- People who want to have several virtual clients with the same performance

Comparison of variants (CPC vs. AVD vs. Citrix)

Cloud PC

Desktop as a service solution from Microsoft.

Benefits	Cons
• Scalable • Simplicity for deployment • Simplicity for administration • License model / fixed costs per user • Massive time savings • Easy automation possibility • Management through one web portal (Intune admin center)	• 1:1 license limit (1 Cloud PC per Useraccount) • No flexibility in environment design • Cloud networkusage very high • Performance models predefined

Azure Virtual Desktop

Plattform as a service solution from Microsoft.

Benefits	Cons
• Ultra scalable • More flexibility in environment design • Powerful plattform	• Usage-based billing • Cloud networkusage very high

Citrix XenDesktop

Softwareproduct for onpremise VDI solution.

Benefits	Cons

• Established standard solution of the last decades • Much experience and knowhow available • Most flexibility in environment design • Stable VHDX access protocol	• Exact sizing onpremise environment needed • Buy onpremise hardware • Buy expensive licenses • More infrastructure knowhow needed • Automation very complex • Microsoft Entra ID join only not possible