

Options for enabling a remote workforce

The purpose of this document is to provide guidance and outline some of the options customers have available – including deploying Windows Virtual Desktops - in order to enable a remote workforce in response to COVID-19 office shutdowns. Use the details below to help guide customers to the most efficient, quick, and simple solution needed to get their users access while working remotely. The options below are listed in most simple to most difficult to set up.

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Cost | Difficulty | Timeline |
| 1. Do your end users just need access to [Teams](https://products.office.com/microsoft-teams/free) and [Office](https://www.microsoft.com/microsoft-365) | Low | Low | Hours |
| 1. Do your users have a VPN with a laptop or existing trusted device? Or have access to options such as [IGEL](http://www.igel.com/microsoft-business-continuity) secure operating system on a USB drive | Low | Low | Low - Medium |
| 1. Do you have an existing [Citrix](https://www.citrix.com/products/citrix-virtual-apps-and-desktops/), [VMware Horizon](https://www.vmware.com/products/horizon.html), or RDSH Solution in place today with ENOUGH capacity to handle additional users? | Low | Low | Low - Medium |
| 1. If you have an existing [Citrix](https://docs.citrix.com/en-us/tech-zone/learn/tech-briefs/business-continuity), [VMware Horizon](https://www.vmware.com/products/horizon.html), or RDS Solution in place today, can you use your environment to provide direct access to a user's physical PC in the office? | Low | Medium | Low |
| 1. [Azure VPN Gateway](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways) (or other 3rd party virtual VPN appliances in Azure) to handle increase in user traffic | Medium | Medium | Low |
| 1. Deploy Jumpbox VM utilizing WVD | Medium | low | Low-Medium |
| 1. Deploy WVD with [Nerdio](https://appsource.microsoft.com/en-us/product/web-apps/nerdio.nerdioforazure?tab=Overview), [CloudJumper](https://appsource.microsoft.com/en-us/product/web-apps/cloudjumper.cloud_workspace_for_azure), or other 3rd party tools | Medium | low | Low |
| 1. Existing Citrix Cloud customers: Access your physical PC via [Citrix Cloud](https://www.citrix.com/products/citrix-cloud/) CVAD for Remote PC Access | Medium - High | Medium | Medium |
| 1. Publish remote desktop using Remote Desktop Gateway with Azure AD Application Proxy | Medium | Medium | Low – Medium |
| 1. Simple MVP Windows Virtual Desktop. | Medium | Medium | Medium - High |
| 1. Full Native WVD Deployment | High | High | High |
| 1. RDS Solution On prem | High | High | High |

**Timeline Effort Estimate:** Hours = < ½ day Low = < 1 day Medium = < 2 days High = 2+ days

**Note:** Number of users and locations can affect estimates above

**Customer Documentation**

* [The top 9 ways Microsoft IT is enabling remote work for its employees](https://www.microsoft.com/en-us/microsoft-365/blog/2020/03/12/top-9-ways-microsoft-it-enabling-remote-work-employees/)
* [Our commitment to customers during COVID-19](https://www.microsoft.com/en-us/microsoft-365/blog/2020/03/05/our-commitment-to-customers-during-covid-19/) – providing Teams for free

**Initial Questions to help identify best option**

* How many users need to work from home?
* Do all of those users have sufficient Internet access from home?
* How many users have a laptop or mobile device that they can take home?
* How many users would need to have an alternate method of working like a virtual desktop or access to their physical PC from a remote location?
* Are there specialized/business critical applications users need to access?
* What collaboration tools do you have in place today on devices including laptops, mobile phones? For example: Teams, Skype for Business
* Do you have minimum Azure infrastructure setup? Subscription, Identity, Network, VPN/ER, and Domain Controller?
* Where are your users located?

**Options**

1. **Do your end users just need access to** [**Teams**](https://products.office.com/microsoft-teams/free) **and** [**Office**](https://www.microsoft.com/microsoft-365)**.**

|  |  |  |
| --- | --- | --- |
| Cost | Difficulty | Timeline |
| Low | **Low** | **Hours** |

* Impact on your users
  + Little to no change to current routines
  + Utilize familiar interfaces
  + Access to work resources for collaboration
* Impact on your IT organization
  + Benefits
    - Little to no effort to get working
    - Existing Security / Identity controls are likely already in place
  + Considerations
    - Documents, email, data could be exposed outside corporate environment
  + Requirements
    - Azure Identity Required

1. **Do your users have a VPN with a laptop or existing trusted device?**

|  |  |  |
| --- | --- | --- |
| Cost | Difficulty | Timeline |
| Low | **Low** | **Low - Medium** |

* Impact on users
  + Minimal impact to users as continues to utilize customer’s organization existing best practices and security processes.
* Impact on your IT organization
  + Benefits
    - Little to no effort to get working
    - Existing Security / Identity controls already in place
    - Utilize already deployed HW/SW
  + Drawbacks
    - Current VPN Gateways might not have the capacity to handle extra connection load – getting additional network devices from vendor might be slow
    - Not everyone has a corporate owned mobile device
    - Will you allow BYOD devices to use VPN?
  + Considerations
    - Security Follow industry best practices when considering connecting personal devices / PC to corporate networks
    - Look at options such as [IGEL](http://www.igel.com/microsoft-business-continuity) secure operating system on a USB drive to allow users to connect from BYOD.
    - Can the VPN HW vendor deliver additional HW?
  + Requirements
    - VPN Gateway, License, SSL Certs, Capacity on HW device
    - Sufficient capacity on VPN Gateway– can VPN HW handle increased load?
      * See option 5 below.

1. **Do you have an existing** [**Citrix**](https://www.citrix.com/products/citrix-virtual-apps-and-desktops/)**,** [**VMware Horizon**](https://www.vmware.com/products/horizon.html)**, or RDS solution in place today with ENOUGH capacity to handle additional users?**

|  |  |  |
| --- | --- | --- |
| Cost | Difficulty | Timeline |
| Low | **Low** | **Low - Medium** |

* Impact on your users:
  + Little to no change to current routines, utilize familiar interfaces and have access to work resources for collaboration
* Impact on your IT organization
  + Stay with this solution for the easiest expansion. Consider repurposing underutilized hardware to scale.
  + Quickly publish a virtual desktop or publish applications that allow users to connect to their existing on prem physical desktop.
* Benefits
  + Utilize existing operational controls, identity, and security processes
  + Your support organization is familiar with handling issues
* Drawbacks
  + Possible lack of HW to expand
  + Licensing limits
* Considerations
  + Is the existing HW sufficient to handle load?
  + Do your users need training?
  + Ensure to engage the Citrix or VMware account teams into this discussion

1. **If you have an existing** [**Citrix**](https://docs.citrix.com/en-us/tech-zone/learn/tech-briefs/business-continuity.html)**,** [**VMware Horizon on Azure**](https://www.vmware.com/products/horizon-cloud-virtual-desktops.html)**, or RDS Solution in place today, can you use your environment to provide direct access to a user's physical PC in the office?**

|  |  |  |
| --- | --- | --- |
| Cost | Difficulty | Timeline |
| Low | **Medium – depending on method used to deploy access agents** | **Low unless new HW is required** |

* Impact on your users
  + Relatively low, desktop users will need to be trained on how to access remote consoles
* Impact on your IT organization
  + Low as you will be extending existing VMWare and Citrix solutions.
* Benefits
  + Utilize existing operational control, identity, and security processes
  + Your support organization is familiar with handling issues
  + Additional cost is minimized by using what is already purchased
* Drawbacks
  + Licensing limits
* Considerations
  + Can the existing external network connections handle the extra traffic?
  + Ensure to engage the Citrix or VMware account teams into this discussion

1. **If your VPN Gateway doesn’t have enough capacity, HW licenses, or too small of incoming network connection you can increase capacity by deploying an** [**Azure VPN Gateway**](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways) **(or additional 3rd party VPN appliances in Azure) to handle increase in user traffic**

|  |  |  |
| --- | --- | --- |
| Cost | Difficulty | Timeline |
| Medium | Medium – must have a firm understanding of routes and network setup | Low with Customer network help |

* Impact on users
  + Minimal impact to users as continues to utilize customer’s existing best practices, security processes (and existing VPN client if already implemented).
  + Users may need to change VPN target destination.
* Impact on your IT organization
  + Utilize existing operational control, identity, and security processes
  + Can expand VPN capabilities without need to purchase hardware. Can remove capability once done using it
  + Azure offers all of the most common VPN appliances – Cisco, Citrix, Checkpoint, etc, in easy-to-deploy format. Bring your own license.
* Drawbacks
  + Possible lack of hardware to expand for many users
  + Licensing limits
  + REQUIRES: VPN or Express Route (ER) set up with routes in place to on prem networks.
  + Requires Customer network equipment compatible with VPN connection
  + Can establish this with new appliances.
* Considerations
  + Routing has to be updated
  + 10k max limits on biggest VPN Gateway
  + Must have an established Azure presence

**------------------------------------------------------------------------------------------------------------------------------------------**

*For the options below see minimum requirement for Azure from above Links*

**All the options below require the same basic Azure Infrastructure**

* Azure AD with customer identity sync’d.
* Network, DNS, and common infrastructure services
* Active Director Domain Controller
* VPN or ER circuit to on Prem network
* Knowledge of security practices, and requirements

1. **Deploy WVD utilizing Jumpbox VM**

***IMPORTANT NOTE:*** *Given time constraints and the high demand that the current COVID-19 and remote working could potentially make on overall Azure capacity, one option for WVD deployment is through utilization of Jumpbox (Our own CSEO are implementing this option to drive further scale). Details of how to implement this solution are available* [*here*](https://microsoft.sharepoint.com/sites/Network_Connectivity/SitePages/RemoteDesktopServices/about.aspx)

|  |  |  |
| --- | --- | --- |
| Cost | Difficulty | Timeline |
| Medium | Medium | Medium |

* Solution:
  + Stand up MVP Windows Virtual Desktop environment, publish full desktop with app locker configured to only allow the Remote Desktop Connection Client (mstsc.exe) to run. User can then use the Jumpbox VM to connect to an on-prem physical PC.
* Benefits
  + Secure – built into connection
  + Can Limit Hardware/Software/Clipboard redirects
  + Direct access to Physical PC
* Drawbacks:
  + Setup time
  + Does not handle Federation
* Considerations
  + Must have established Azure presence
  + Must have generous VPN or ER connection to on prem
  + Must have Pre-reqs above in place for quick deploy

1. **Deploy WVD with** [**Nerdio**](https://appsource.microsoft.com/en-us/product/web-apps/nerdio.nerdioforazure?tab=Overview)**,** [**CloudJumper**](https://appsource.microsoft.com/en-us/product/web-apps/cloudjumper.cloud_workspace_for_azure) **or other 3rd party tools.** [**CloudJumper**](https://cloudjumper.com/microsoft-wvd-business-continuity/) **and** [**Nerdio**](https://getnerdio.com/nerdio-manager-for-wvd/) **public COVID-19 response offering to quickly deploy WVD in a customer environment**

|  |  |  |
| --- | --- | --- |
| Cost | Difficulty | Timeline |
| Medium/High | Medium | Low – Medium with help from Partner/CSA |

* Impact on your users:
  + Relatively low, desktop users will need to be trained on how to access remote consoles
* Impact on IT
  + Quick tool deployment and automated deployment of WVD environment
  + Advanced feature set over current WVD Management tools
  + Enterprise grade Operational control
* Drawbacks:
  + Cost: Long term 3rd party have additional licensing cost associated usually on a per user per month basis. However, in many cases ROI is very low: <1 year. The extra benefits in many cases outweigh the cost difference.
* Considerations
  + **Must** have Pre-reqs setup as outlined above

1. **Existing Citrix Cloud customers: Access your physical PC via Citrix Cloud CVAD for Remote PC Access.**

Users can easily connect via Citrix Cloud to their physical desktop PCs at their Offices via the VDA agent that will be installed locally.

|  |  |  |
| --- | --- | --- |
| Cost | Difficulty | Timeline |
| Medium | **Medium** | **Low – Medium with help from Citrix** |

IMPORTANT NOTE: [Required Citrix Cloud Workspace Premium Plus license](https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/install-configure/remote-pc-access.html).

* Impact on your users:
  + Relatively low, desktop looks and feels the same. Users need to be educated to access the desktop via the Citrix Workspace portal.
* Impact on your IT organization
  + Simple to Deploy 2 hours set up time for minimum deploy
    - Every desktop needs to be enrolled with the Citrix VDA agent
  + Secure
  + Minimal HW or Virtual HW
* Drawbacks
  + No Azure components involved
  + Ensure to engage the Citrix or VMware account teams into this discussion

1. **Publish Remote Desktop with Azure AD Application Proxy.** Users connect to [Azure AD App Proxy](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-integrate-with-remote-desktop-services) to get to RDP client then remote into their physical app servers or physical desktops.

|  |  |  |
| --- | --- | --- |
| Cost | Difficulty | Timeline |
| Medium | **Medium** | **Low – Medium with help from Partner/CSA** |

IMPORTANT NOTE: [Active Directory Federation Services are a pre-requisite.](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/how-to-connect-fed-azure-adfs)

* Impact on your users:
  + Relatively low, desktop users will need to be trained on how to access remote consoles
* Impact on your IT organization
  + Simple to Deploy 4-6 hours set up time for minimum deploy
  + Secure
  + Minimal Hardware or Virtual Hardware
* Drawbacks
  + Limited support for full VDI desktop
  + New connection model has to be tested / approved by security team
  + Must have established Azure presence
* Considerations
  + **Must** have Pre-reqs setup as outlined above

1. **Full Native WVD Deployment**

|  |  |  |
| --- | --- | --- |
| Cost | Difficulty | Timeline |
| High | **High** | **High** |

* Impact on your users:
  + New access method. End users will need training.
  + Changes the working model for Administrators
* Impact on IT
  + Need to quickly train and learn Azure model
  + Building WVD images is not trivial
  + New Operational controls need to be put in place
* Benefits
  + Full Desktops
  + Meets internal security posture
  + Secure – built into connection
  + Can Limit HW/SW/Clipboard redirects
* Drawbacks:
  + Long Setup time
  + New Management
  + Image setup and infra setup is tedious
  + Does not handle Federation
* Considerations
  + Must have established Azure presence
  + Must have generous VPN or ER connection to on prem
  + Must have Pre-reqs above in place for quick deploy

1. **RDS Solution On prem**

|  |  |  |
| --- | --- | --- |
| Cost | Difficulty | Timeline |
| High | **High** | **High** |

* Solution:
  + Solution: Legacy RDSH Environment stand up
* Benefits
  + Full Desktops
  + Meets internal security posture
  + Secure – built into connection
  + Can handle Federation
* Drawbacks
  + Long Setup time
  + HW Requirements
  + Built on prem
* Considerations
  + Must Network / VPN connections available on Prem
  + Must have bandwidth available