Contents

- Remote Desktop Services
  - Get started
    - What's new in RDS?
    - Supported configurations for RDS
    - Supported security configurations for Windows 10 VDI
    - Planning poster for Remote Desktop Services
    - Remote Desktop Services hosting partners
  - Plan and design
    - Build anywhere
    - Remote Desktop workloads
    - Network guidance
    - Virtual machine sizing guidance
    - Access from anywhere
    - High availability
    - Multifactor Authentication
    - Secure data storage
    - GPU acceleration
    - Connect from any device
    - Choose how you pay
    - Office 2016 in RDS and VDI deployments
      - Dealing with Outlook search in non-persistent environments
      - OneDrive for Business and VDI environments
    - Desktop Hosting Reference Architecture
      - Remote Desktop Services architecture
      - Desktop hosting service
      - Remote Desktop Services roles
      - Azure services and considerations for desktop hosting
  - Build and deploy
    - Deploy a proof-of-concept RDS environment with ARM and Azure Marketplace

- Migrate your Remote Desktop Services deployments to Windows Server 2016
- Migrate your Remote Desktop Services Client Access Licenses (RDS CALs)
- Upgrade your Remote Desktop Services deployments to Windows Server 2016
  - Upgrade Remote Desktop Session Host servers
  - Upgrade Remote Desktop Virtualization Host servers
- Deploy a Remote Desktop Services infrastructure
- Create and deploy a Remote Desktop Services collection
- Set up the Remote Desktop web client for your users
- Set up email discovery for your users
- License your Remote Desktop deployment
  - Activate the license server
  - Install RDS CALs on the license server
  - Track the CALs used in your deployment
- Integrate Azure services
  - Learn how to use Multi-factor Authentication with RDS
  - Integrate Azure AD Domain Services with your RDS deployment
  - Publish Remote Desktop with Azure AD Application Proxy
- Extend your RDS environment for high availability
  - Scale out an existing RDS collection with an RD Session Host farm
  - Add high availability to the RD Connection Broker infrastructure
  - Add high availability to the RD Web and RD Gateway web front
  - Deploy a two-node Storage Spaces Direct file system for UPD storage
  - Deploy and manage a personal session desktops environment
  - Create VMs for RDS
- Set up disaster recovery for your RDS environment
  - Create a geo-redundant RDS deployment
  - Set up Azure Site Recovery for RDS
    - Enable disaster recovery for RDS components
    - Create your disaster recovery plan

Run and tune

- Manage personal desktop session collections
- Recommended configuration for VDI desktops

- Optimizing Windows 10, version 1803, for a Virtual Desktop Infrastructure (VDI) role
- Manage users in your RDS collection
- Customize the RDS title “Work Resources” using PowerShell on Windows Server
- Diagnose app performance issues with performance counters

Access your Remote Desktop resources

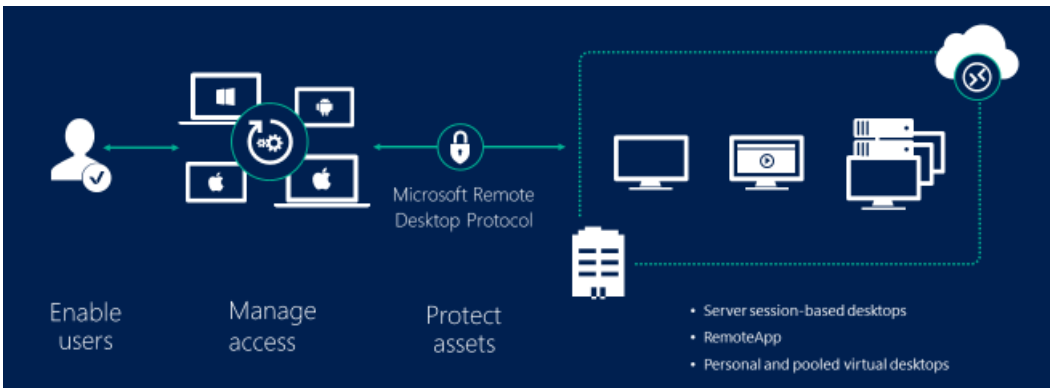
- Available Remote Desktop clients
- Windows Desktop client
  - Get started with the Windows Desktop client
  - Windows Desktop client for admins
  - What's new in the Windows Desktop client
- Windows Store client
  - Get started with the Windows Store client
  - What's new in the Windows Store client
- Android client
  - Get started with the Android client
  - What's new in the Android client
- iOS client
  - Get started with the iOS client
  - What's new in the iOS client
- macOS client
  - Get started with the macOS client
  - What's new in the macOS client
- Web client
  - Get started with the web client
  - What's new in the web client
- Setting up your PC for Remote Desktop
  - Supported PCs
  - Grant Remote Desktop access to your PC
  - Grant access to your PC from outside your network
  - Change the RD listening port on your PC
- Advanced information
  - Which client works best for you?

Remote Desktop RDP file settings
Remote Desktop URI scheme
Remote Desktop client FAQ
Privacy settings for managed apps and desktops
Known issues
General Remote Desktop connection troubleshooting
Clients can't connect and get the "Class not registered" error
Clients can't connect and see "No licenses available" error
User can't authenticate or must authenticate twice
"Remote Desktop Service is currently busy" error on connecting
Remote Desktop client disconnects and can't reconnect to the same session
Remote laptop disconnects from wireless network
Poor performance or application problems during remote desktop connection
Additional resources

Welcome to Remote Desktop Services

9/27/2019 • 2 minutes to read • Edit Online

Remote Desktop Services (RDS) is the platform of choice for building virtualization solutions for every end customer need, including delivering individual virtualized applications, providing secure mobile and remote desktop access, and providing end users the ability to run their applications and desktops from the cloud.



RDS offers deployment flexibility, cost efficiency, and extensibility—all delivered through a variety of deployment options, including Windows Server 2016 for on-premises deployments, Microsoft Azure for cloud deployments, and a robust array of partner solutions.

Depending on your environment and preferences, you can set up the RDS solution for session-based virtualization, as a virtual desktop infrastructure (VDI), or as a combination of the two:

- **Session-based virtualization**: Leverage the compute power of Windows Server to provide a cost-effective multi-session environment to drive your users' everyday workloads.
- **VDI**: Leverage Windows client to provide the high performance, app compatibility, and familiarity that your users have come to expect of their Windows desktop experience.

Within these virtualization environments, you have additional flexibility in what you publish to your users:

- **Desktops**: Give your users a full desktop experience with a variety of applications that you install and manage. Ideal for users that rely on these computers as their primary workstations or that are coming from thin clients, such as with MultiPoint Services.
- **RemoteApps**: Specify individual applications that are hosted/run on the virtualized machine but appear as if they're running on the user's desktop like local applications. The apps have their own taskbar entry and can be resized and moved across monitors. Ideal for deploying and managing key applications in the secure, remote environment while allowing users to work from and customize their own desktops.

For environments where cost-effectiveness is crucial and you want to extend the benefits of deploying full desktops in a session-based virtualization environment, you can use MultiPoint Services to deliver the best value.

With these options and configurations, you have the flexibility to deploy the desktops and applications your users need in a remote, secure, and cost-effective fashion.

Next steps

Here are some next steps to help you get a better understanding of RDS and even start deploying your own environment:

- Understand the supported configurations for RDS with the various Windows and Windows Server versions

- Plan and design an RDS environment to accommodate various requirements, such as high availability and multi-factor authentication.
- Review the Remote Desktop Services architecture models that work best for your desired environment.
- Start to deploy your RDS environment with ARM and Azure Marketplace.

Get started with Remote Desktop Services in Windows Server 2016

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server 2016

Use the following information to begin exploring and using Remote Desktop Services in Windows Server 2016.

- What's new in Remote Desktop Services? - Check out the new features added in Windows Server 2016, as well as improvements to existing features and scenarios.
- Remote Desktop Services planning poster - We've created a poster that walks you through all the considerations for planning your Remote Desktop Deployment.
- Host Windows desktops and applications - learning path - Need to create a desktop hosting solution on virtual machines? Learn about the new Remote Desktop Services learning path, as well as identify partners that can help you build your environment.

Once you've reviewed the information about, take the next step and start planning your deployment.

What's new in Remote Desktop Services

9/27/2019 • 2 minutes to read • Edit Online

Remote Desktop Services (RDS) built on Windows Server 2016 is a virtualization platform enabling a wide range of customer scenarios. Improvements in the overall RDS solution incorporates the work done by both the Remote Desktop team and other technology partners at Microsoft. The following scenarios and technologies are new or improved in Windows Server 2016.

Also be sure to check out our session from Ignite 2016: Harness RDS improvements in Windows Server 2016. In this video, the product team reviews all of the new and improved features in Remote Desktop Services, including vGPU support.

App Compatibility - Windows Server 2016 and Windows 10

Built on the same foundation of Windows 10, Windows Server 2016 not only has the same look and feel you expect out of a desktop but can also run many of the same applications. Pairing Windows Server 2016 with the graphics capabilities (below) gives you an environment for all users to be productive.

Azure SQL Database - the new database for your highly available environment

The RD Connection Broker is able to store all of the deployment information (like connection states and user/host mappings) in a shared SQL database, such as an Azure SQL database. Ditch the SQL Server Always On Availability Group deployment manual, grab the connection string to the Azure SQL database, and start using your highly available environment.

Additional information: Use Azure SQL DB for your Remote Desktop Connection Broker high availability environment

Graphics - solving graphics needs across various scenarios

Thanks to Hyper-V's Discrete Device Assignment, you can now map GPUs on a host machine directly to a VM to be consumed by its GPU-requiring applications. Improvements have also been made in RemoteFX vGPU, including support for OpenGL 4.4, OpenCL 1.1, 4k resolution, and Windows Server virtual machines.

Additional information: Discrete Device Assignment

RD Connection Broker - improved connection handling during logon storms

With improved connection handling, the RD Connection Broker is now able to handle over 10,000 concurrent logon requests, sometimes seen during "logon storms". The improved RD Connection Broker also makes maintenance of the deployment simpler by being able to more quickly add servers back into the environment.

Additional information: Improved Remote Desktop Connection Broker Performance

RDP 10 - new capabilities built into the protocol

RDP 10 now uses the H.264/AVC 444 codec, appropriately optimizing across both video and text. With this release, pen remoting is also supported. With these capabilities, your remote sessions start to feel even more like a local session.

Additional information: RDP 10 AVC/H.264 improvements in Windows 10 and Windows Server 2016

Personal session desktops - providing individual desktops to any end-user

Personal session desktops is a new way to have your own personal desktop hosted for you in the cloud. Administrative privileges and dedicated session hosts removes the complexity of hosting environments where users want to manage the desktop like it's their own.

Additional information: Personal Session Desktops

Supported configurations for Remote Desktop Services

11/19/2019 • 5 minutes to read • Edit Online

Applies To: Windows Server 2016, Windows Server 2019

When it comes to supported configurations for Remote Desktop Services environments, the largest concern tends to be version interoperability. Most environments include multiple versions of Windows Server - for example, you may have an existing Windows Server 2012 R2 RDS deployment but want to upgrade to Windows Server 2016 to take advantage of the new features (like support for OpenGL\OpenCL, Discrete Device Assignment, or Storage Spaces Direct). The question then becomes, which RDS components can work with different versions and which need to be the same?

So with that in mind, here are basic guidelines for supported configurations of Remote Desktop Services in Windows Server.

> **NOTE**
> Make sure to review the system requirements for Windows Server 2016 and system requirements for Windows Server 2019.

Best practices

- Use Windows Server 2019 for your Remote Desktop infrastructure (the Web Access, Gateway, Connection Broker, and license server). Windows Server 2019 is backward-compatible with these components, which means a Windows Server 2016 or Windows Server 2012 R2 RD Session Host can connect to a 2019 RD Connection Broker, but not the other way around.
- For RD Session Hosts - all Session Hosts in a collection need to be at the same level, but you can have multiple collections. You can have a collection with Windows Server 2016 Session Hosts and one with Windows Server 2019 Session Hosts.
- If you upgrade your RD Session Host to Windows Server 2019, also upgrade the license server. Remember that a 2019 license server can process CALs from all previous versions of Windows Server, down to Windows Server 2003.
- Follow the upgrade order recommended in Upgrading your Remote Desktop Services environment.
- If you are creating a highly available environment, all of your Connection Brokers need to be at the same OS level.

RD Connection Brokers

Windows Server 2016 removes the restriction for the number of Connection Brokers you can have in a deployment when using Remote Desktop Session Hosts (RDSH) and Remote Desktop Virtualization Hosts (RDVH) that also run Windows Server 2016. The following table shows which versions of RDS components work with the 2016 and 2012 R2 versions of the Connection Broker in a highly available deployment with three or more Connection Brokers.

3+ CONNECTION BROKERS IN HA	RDSH OR RDVH 2019	RDSH OR RDVH 2016	RDSH OR RDVH 2012 R2
Windows Server 2019 Connection Broker	Supported	Supported	Supported
Windows Server 2016 Connection Broker	N/A	Supported	Supported
Windows Server 2012 R2 Connection Broker	N/A	N/A	Not Supported

Support for graphics processing unit (GPU) acceleration

Remote Desktop Services support systems equipped with GPUs. Applications that require a GPU can be used over the remote connection. Additionally, GPU-accelerated rendering and encoding can be enabled for improved app performance and scalability.

Remote Desktop Services Session Hosts and single-session client operating systems can take advantage of the physical or virtual GPUs presented to the operating system in many ways, including the Azure GPU optimized virtual machine sizes, GPUs available to the physical RDSH server, RemoteFX vGPUs (Only on Windows Server 2016), and GPUs presented to the VMs by supported hypervisors.

See Which graphics virtualization technology is right for you? for help figuring out what you need. For specific information about DDA, check out Plan for deploying Discrete Device Assignment.

GPU vendors may have a separate licensing scheme for RDSH scenarios or restrict GPU use on the server OS, verify the requirements with your favorite vendor.

GPUs presented by a non-Microsoft hypervisor or Cloud Platform must have drivers digitally-signed by WHQL and supplied by the GPU vendor.

Remote Desktop Session Host support for GPUs

The following table shows the scenarios supported by different versions of RDSH hosts.

FEATURE	WINDOWS SERVER 2008 R2	WINDOWS SERVER 2012 R2	WINDOWS SERVER 2016	WINDOWS SERVER 2019
Use of hardware GPU for all RDP sessions	No	Yes	Yes	Yes
H.264/AVC hardware encoding (if suppported by the GPU)	No	No	Yes	Yes
Load balancing between multiple GPUs presented to the OS	No	No	No	Yes
H.264/AVC encoding optimizations for minimizing bandwidth usage	No	No	No	Yes

FEATURE	WINDOWS SERVER 2008 R2	WINDOWS SERVER 2012 R2	WINDOWS SERVER 2016	WINDOWS SERVER 2019
H.264/AVC support for 4K resolution	No	No	No	Yes

VDI support for GPUs

The following table shows support for GPU scenarios in the client OS.

FEATURE	WINDOWS 7 SP1	WINDOWS 8.1	WINDOWS 10
Use of hardware GPU for all RDP sessions	No	Yes	Yes
H.264/AVC hardware encoding (if suppported by the GPU)	No	No	Windows 10 1703 and later
Load balancing between multiple GPUs presented to the OS	No	No	Windows 10 1803 and later
H.264/AVC encoding optimizations for minimizing bandwidth usage	No	No	Windows 10 1803 and later
H.264/AVC support for 4K resolution	No	No	Windows 10 1803 and later

RemoteFX 3D Video Adapter (vGPU) support

Remote Desktop Services supports RemoteFX vGPUs when VM is running as a Hyper-V guest on Windows Server 2012 R2 or Windows Server 2016. The following guest operating systems have RemoteFX vGPU support:

- Windows 7 SP1
- Windows 8.1
- Windows 10 1703 or later
- Windows Server 2016 in a single-session deployment only
- Windows Server 2019 in a single-session deployment only

Discrete Device Assignment support

Remote Desktop Services supports Physical GPUs presented with Discrete Device Assignment from Windows Server 2016 or Windows Server 2019 Hyper-V hosts. See Plan for deploying Discrete Device Assignment for more details.

VDI deployment – supported guest OSes

Windows Server 2016 and Windows Server 2019 RD Virtualization Host servers support the following guest OSes:

- Windows 10 Enterprise
- Windows 8.1 Enterprise
- Windows 7 SP1 Enterprise

NOTE

- Remote Desktop Services doesn't support heterogeneous session collections. The OSes of all VMs in a collection must be the same version.
- You can have separate homogeneous collections with different guest OS versions on the same host.
- The Hyper-V host used to run VMs must be the same version as the Hyper-V host used to create the original VM templates.

Single sign-on

Windows Server 2016 and Windows Server 2019 RDS supports two main SSO experiences:

- In-app (Remote Desktop application on Windows, iOS, Android, and Mac)
- Web SSO

Using the Remote Desktop application, you can store credentials either as part of the connection info (Mac) or as part of managed accounts (iOS, Android, Windows) securely through the mechanisms unique to each OS.

To connect to desktops and RemoteApps with SSO through the inbox Remote Desktop Connection client on Windows, you must connect to the RD Web page through Internet Explorer. The following configuration options are required on the server side. No other configurations are supported for Web SSO:

- RD Web set to Forms-Based Authentication (Default)
- RD Gateway set to Password Authentication (Default)
- RDS Deployment set to "Use RD Gateway credentials for remote computers" (Default) in the RD Gateway properties

NOTE

Due to the required configuration options, Web SSO is not supported with smartcards. Users who login via smartcards might face multiple prompts to login.

For more information about creating VDI deployment of Remote Desktop Services, check out Supported Windows 10 security configurations for Remote Desktop Services VDI.

Using Remote Desktop Services with application proxy services

You can use Remote Desktop Services, except for the web client, with Azure AD Application Proxy. Remote Desktop Services does not support using Web Application Proxy, which is included in Windows Server 2016 and earlier versions.

Supported Windows 10 security configurations for Remote Desktop Services VDI

9/27/2019 • 2 minutes to read • Edit Online

Applies To: Windows Server 2016

Windows 10 and Windows Server 2016 have new layers of protection built into the operating system to further safeguard against security breaches, help block malicious attacks and enhance the security of virtual machines, applications, and data.

> **NOTE**
> Make sure to review the Remote Desktop Services supported configuration information.

The following table outlines which of these new features are supported in a VDI deployment using RDS.

VDI COLLECTION TYPE	MANAGED POOLED	MANAGED PERSONAL	UNMANAGED POOLED	UNMANAGED PERSONAL
Credential Guard	Yes	Yes	Yes	Yes
Device Guard	Yes	Yes	Yes	Yes
Remote Credential Guard	No	No	No	No
Shielded & Encryption Supported VMs	No	No	Encryption supported VMs with additional configuration	Encryption supported VMs with additional configuration

Remote Credential Guard:

Remote Credential Guard is only supported for direct connections to the target machines and not for the ones via Remote Desktop Connection Broker and Remote Desktop Gateway.

> **NOTE**
> If you have a Connection Broker in a single-instance environment, and the DNS name matches the computer name, you may be able to use Remote Credential Guard, although this is not supported.

Shielded VMs and Encryption Supported VMs:

- Shielded VMs are not supported in Remote Desktop Services VDI

For leveraging Encryption Supported VMs:

- Use an unmanaged collection and a provisioning technology outside of the Remote Desktop Services collection creation process to provision the virtual machines.
- User Profile Disks are not supported as they rely on differential disks

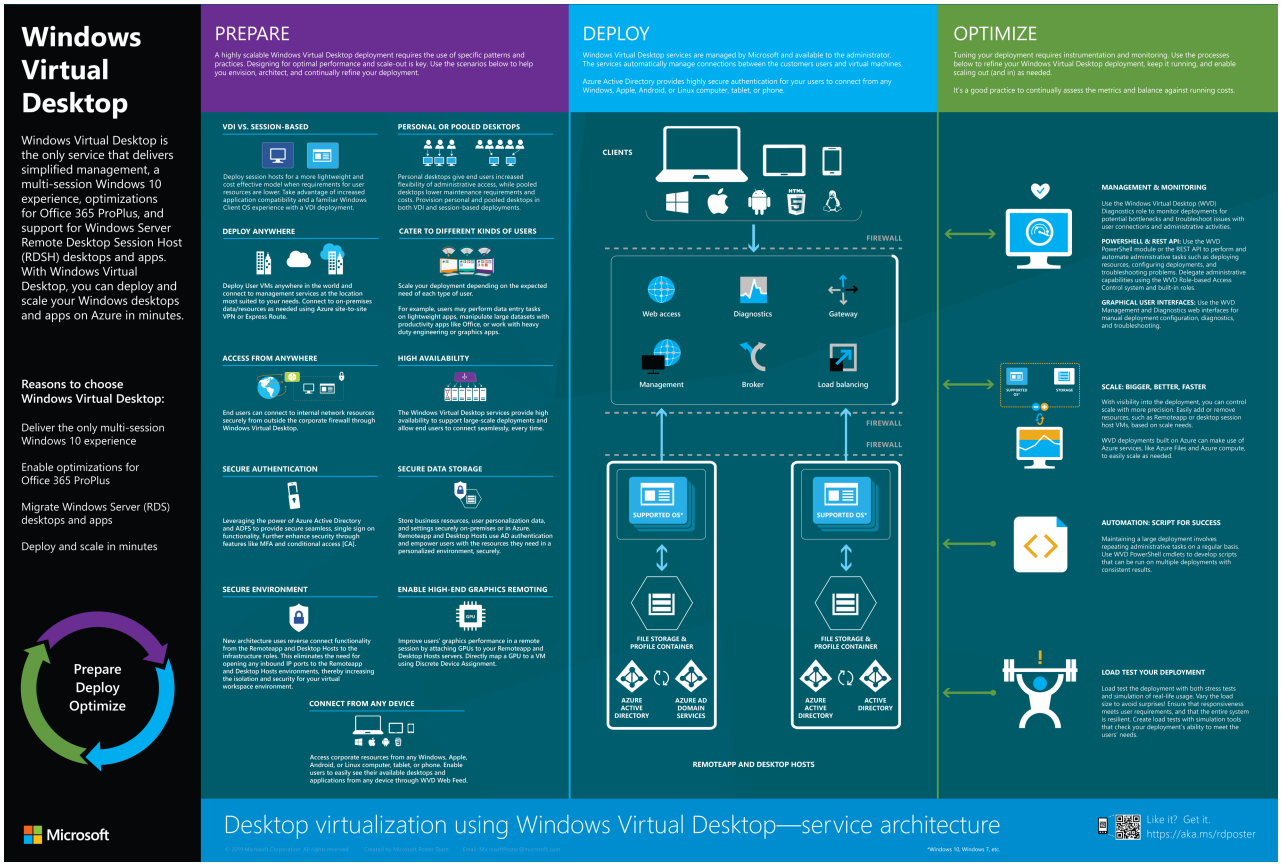
Remote Desktop Services - planning poster

11/6/2019 • 2 minutes to read • Edit Online

Windows Virtual Desktop

You may have heard us talk about a new “modern infrastructure” for Remote Desktop. Maybe you've heard us use the phrase “RDmi.” The phrase you need to know is “Windows Virtual Desktop." Learn more at our Windows Virtual Desktop documentation page.

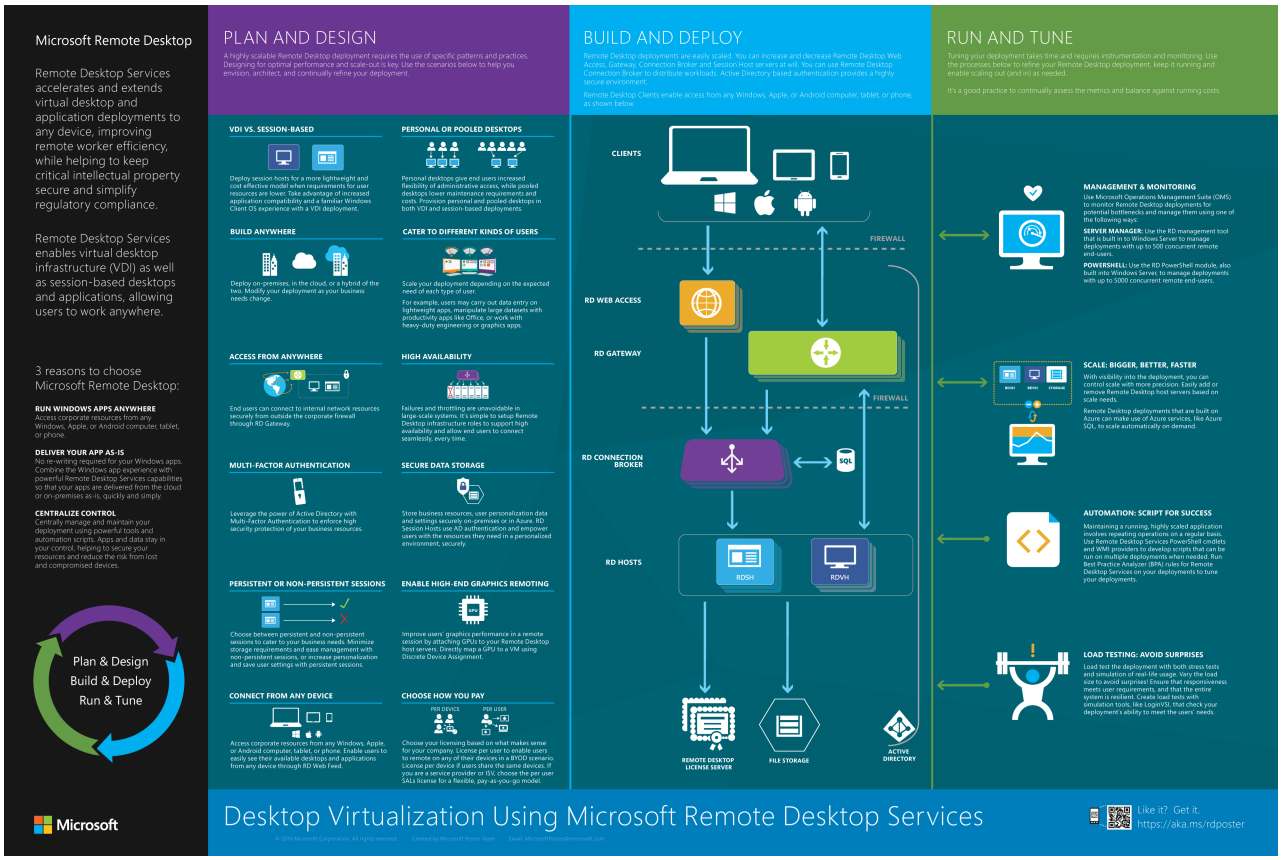
The Remote Desktop Services team have created a poster to help you plan, build, and run your Windows Virtual Desktop environment.



You can get a copy of the poster by right-clicking the image and saving it to your local system.

Remote Desktop Services in Windows Server

The Remote Desktop Services team have created a poster to help you plan, build, and run your RDS environment.



You can get a copy of the poster by right-clicking the image and saving it to your local system.

Check out the following topics to learn more about planning:

- Plan and design your RDS deployment
- Build and deploy RDS
- Run and tune your RDS environment

Remote Desktop Services hosting partners and assessment

1/14/2020 • 2 minutes to read • Edit Online

Recently, Microsoft delivered a new learning path within the Microsoft Partner Network: "Hosting Windows Desktop and Applications using Remote Desktop Services in Azure."

If you are a Microsoft partner and want to be included in the list of partners who have passed the assessment, here are the steps you can take to complete the learning path:

1. Become a Microsoft Partner, if you're not already.
2. Watch the Hosting Windows and Applications using Remote Desktop Services in Azure training session.
3. Take the technical assessment.
4. Make sure you meet the requirements for the Cloud Platform competency.

Already a Microsoft Partner and have questions? Contact the Remote Desktop team at rdhostingpartners@microsoft.com.

Partners who have passed the learning path assessment

If you are a customer looking for a partner to help you host Windows desktops and applications in Azure for your users, we have compiled a list of partners who have passed the assessment. Here is a list of those partners, as of 03/28/2017, that you can download.

You can find more information on each partner using these steps:

1. Open Find a partner.
2. Clear the **Location** field.
3. Enter the name of the partner in the **I'm looking for help with** field.

Plan and design your Remote Desktop Services environment

12/12/2019 • 2 minutes to read • Edit Online

A highly scalable Remote Desktop deployment requires the use of specific patterns and practices. Designing for optimal performance and scale-out is key. Use the scenarios below to help you envision, architect, and continually refine your deployment.

Use the following information to plan and design your deployment:

- Build anywhere
- Network guidance
- Access from anywhere
- High availability
- MultiFactor Authentication
- Secure data storage
- GPU acceleration
- Connect from any device
- Choose how you pay

Be sure to also review the Desktop Hosting Reference Architecture, which provides an overview of the Remote Desktop architecture and helps you plan a hybrid RDS environment that includes Azure infrastructure.

Remote Desktop Services - Build anywhere

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

Deploy on-premises, in the cloud, or a hybrid of the two. Modify your deployment as your business needs change.

Regardless of where you are, the underlying architecture of the Remote Desktop Services environment remains the same:

- You still must have an internet-facing server to utilize RD Web Access and RD Gateway for external users
- You still must have an Active Directory and--for highly available environments--a SQL database to house user and Remote Desktop properties
- You still must have communication access between the RD infrastructure roles (RD Connection Broker, RD Gateway, RD Licensing, and RD Web Access) and the end RDSH or RDVH hosts to be able to connect end-users to their desktops or applications.

This flexibility allows you to get the best of both worlds:

- The simplicity and pay-as-you-go methods associated with the cloud and the online world.
- The familiarity and hassle-free way of leveraging heavy resources that already exist on-premises.

For additional information, look at how to build and deploy your Remote Desktop Services deployment.

Remote Desktop workloads

1/10/2020 • 2 minutes to read • Edit Online

Users can run different types of workloads on the virtual machines managed by Remote Desktop Services or Windows Virtual Desktop. Scale your deployment depending on the expected need of each type of user. The following table provides examples of a range of workload types to help you estimate what size your virtual machines need to be. After you set up your virtual machines, you should continually monitor their actual usage and adjust their size accordingly. If you end up needing a bigger or smaller virtual machine, you can easily scale your existing deployment up or down in Azure.

The following table describes each workload. "Example users" are the types of users that might find each workload most helpful. "Example apps" are the kinds of apps that work best for each workload.

WORKLOAD TYPE	EXAMPLE USERS	EXAMPLE APPS
Light	Users doing basic data entry tasks	Database entry applications, command-line interfaces
Medium	Consultants and market researchers	Database entry applications, command-line interfaces, Microsoft Word, static web pages
Heavy	Software engineers, content creators	Database entry applications, command-line interfaces, Microsoft Word, static web pages, Microsoft Outlook, Microsoft PowerPoint, dynamic web pages
Power	Graphic designers, 3D model makers, machine learning researchers	Database entry applications, command-line interfaces, Microsoft Word, static web pages, Microsoft Outlook, Microsoft PowerPoint, dynamic web pages, Adobe Photoshop, Adobe Illustrator, computer-aided design (CAD), computer-aided manufacturing (CAM)

For information about sizing recommendations, see Virtual machine sizing guidance.

Network guidance

1/10/2020 • 2 minutes to read • Edit Online

When using a remote Windows session, your network's available bandwidth greatly impacts the quality of your experience. Different applications and display resolutions require different network configurations, so it's important to make sure your network is configured to meet your needs.

> **NOTE**
> The following recommendations apply to networks with less than 0.1% loss. These recommendations apply regardless of how many sessions you're hosting on your virtual machines (VMs).

Applications

The following table lists the minimum recommended bandwidths for a smooth user experience. These recommendations are based on the guidelines in Remote Desktop workloads.

WORKLOAD TYPE	RECOMMENDED BANDWIDTH
Light	1.5 Mbps
Medium	3 Mbps
Heavy	5 Mbps
Power	15 Mbps

Keep in mind that the stress put on your network depends on both your app workload's output frame rate and your display resolution. If either the frame rate or display resolution increases, the bandwidth requirement will also rise. For example, a light workload with a high-resolution display requires more available bandwidth than a light workload with regular or low resolution.

Other scenarios can have their bandwidth requirements change depending on how you use them, such as:

- Voice or video conferencing
- Real-time communication
- Streaming 4K video

Make sure to load test these scenarios in your deployment using simulation tools like Login VSI. Vary the load size, run stress tests, and test common user scenarios in remote sessions to better understand your network's requirements.

Display resolutions

Different display resolutions require different available bandwidths. The following table lists the bandwidths we recommend for a smooth user experience at typical display resolutions with a frame rate of 30 frames per second (fps). These recommendations apply to single and multiple user scenarios. Keep in mind that scenarios involving a frame rate under 30 fps, such as reading static text, require less available bandwidth.

TYPICAL DISPLAY RESOLUTIONS AT 30 FPS	RECOMMENDED BANDWIDTH
About 1024 × 768 px	1.5 Mbps
About 1280 × 720 px	3 Mbps
About 1920 × 1080 px	5 Mbps
About 3840 × 2160 px (4K)	15 Mbps

Additional resources

The Azure region you're in can affect user experience as much as network conditions. Check out the Windows Virtual Desktop experience estimator to learn more.

Virtual machine sizing guidance

1/10/2020 • 2 minutes to read • Edit Online

Whether you're running your virtual machine on Remote Desktop Services or Windows Virtual Desktop, different types of workloads require different session host virtual machine (VM) configurations. For the best possible experience, scale your deployment depending on your users' needs.

Multi-session recommendations

The following table lists the maximum suggested number of users per virtual central processing unit (vCPU) and the minimum VM configuration for each workload. These recommendations are based on Remote Desktop workloads.

WORKLOAD TYPE	MAXIMUM USERS PER VCPU	VCPU/RAM/OS STORAGE MINIMUM	EXAMPLE AZURE INSTANCES	PROFILE CONTAINER STORAGE MINIMUM
Light	6	2 vCPUs, 8 GB RAM, 16 GB storage	D2s_v3, F2s_v2	30 GB
Medium	4	4 vCPUs, 16 GB RAM, 32 GB storage	D4s_v3, F4s_v2	30 GB
Heavy	2	4 vCPUs, 16 GB RAM, 32 GB storage	D4s_v3, F4s_v2	30 GB
Power	1	6 vCPUs, 56 GB RAM, 340 GB storage	D4s_v3, F4s_v2, NV6	30 GB

Single-session recommendations

For VM sizing recommendations for single-session scenarios, we recommend at least two physical CPU cores per VM (typically four vCPUs with hyperthreading). If you need more specific VM sizing recommendations for single-session scenarios, ask the software vendors specific to your workload. VM sizing for single-session VMs will likely align with physical device guidelines.

General virtual machine recommendations

For VM requirements to run the operating system, see Windows 10 computer specifications and system requirements.

We recommend you use Premium SSD storage in your OS disk for production workloads that require a service level agreement (SLA). For more details, see the SLA for virtual machines.

Graphics processing units (GPUs) are a good choice for users who regularly use graphics-intensive programs for video rendering, 3D design, and simulations. To learn more about graphics acceleration, see Choose your graphics rendering technology. Azure has several graphics acceleration deployment options and multiple available GPU VM sizes. Learn more at GPU optimized virtual machine sizes.

B-series burstable VMs are a good choice for users who don't always need maximum CPU performance. For more information about VM types and sizes, see Sizes for Windows virtual machines in Azure and the pricing information on our Virtual Machine series page.

Test your workload

Finally, we recommend you use simulation tools to test your deployment with both stress tests and real-life usage simulations. Make sure your system is responsive and resilient enough to meet user needs, and remember to vary the load size to avoid surprises.

Remote Desktop Services - Access from anywhere

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

End users can connect to internal network resources securely from outside the corporate firewall through RD Gateway.

Regardless of how you configure the desktops for your end-users, you can easily plug the RD Gateway into the connection flow for a fast, secure connection. For end-users connecting through published feeds, you can configure the RD Gateway property as you configure the overall deployment properties. For end-users connecting through to their desktops without a feed, they can easily add the name of the organization's RD Gateway as a connection property no matter which Remote Desktop client application they use.

The three primary purposes of the RD Gateway, in the order of the connection sequence, are:

1. **Establish an encrypted SSL tunnel between the end-user's device and the RD Gateway Server**: In order to connect through any RD Gateway server, the RD Gateway server must have a certificate installed that the end-user's device recognizes. In testing and proofs of concepts, self-signed certificates can be used, but only publicly trusted certificates from a certificate authority should be used in any production environment.
2. **Authenticate the user into the environment**: The RD Gateway uses the inbox IIS service to perform authentication, and can even utilize the RADIUS protocol to leverage multi-factor authentication solutions such as Azure MFA. Aside from the default policies created, you can create additional RD Resource Authorization Policies (RD RAPs) and RD Connection Authorization Policies (RD CAPs) to more specifically define which users should have access to which resources within the secure environment.
3. **Pass traffic back and forth between the end-user's device and the specified resource**: The RD Gateway continues to perform this task for as long as the connection is established. You can specify different timeout properties on the RD Gateway servers to maintain the security of the environment in case the user walks away from the device.

You can find additional details on the overall architecture of a Remote Desktop Services deployment in the desktop hosting reference architecture.

Remote Desktop Services - High availability

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

Failures and throttling are unavoidable in large-scale systems. It's simple to set up Remote Desktop infrastructure roles to support high availability and allow end users to connect seamlessly, every time.

In Remote Desktop Services, the following items represent the Remote Desktop infrastructure roles, with their respective guidance to establish high availability:

- Remote Desktop Connection Broker
- Remote Desktop Gateway
- Remote Desktop Licensing
- Remote Desktop Web Access

High availability is established by duplicating each of the roles services on a second machines. In Azure, you can receive a guaranteed uptime by placing the set of the two virtual machines (hosting the same role) in an availability sets.

Along with availability sets, you can now leverage the power of Azure SQL Database and its Azure-backed SLA to ensure that you always have connection information and can redirect users to their desktops and applications.

For best practices on creating your RDS environment, please see the desktop hosting architecture.

Remote Desktop Services - Multi-Factor Authentication

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

Leverage the power of Active Directory with Multi-Factor Authentication to enforce high security protection of your business resources.

For your end-users connecting to their desktops and applications, the experience is similar to what they already face as they perform a second authentication measure to connect to the desired resource:

- Launch a desktop or RemoteApp from an RDP file or through a Remote Desktop client application
- Upon connecting to the RD Gateway for secure, remote access, receive an SMS or mobile application MFA challenge
- Correctly authenticate and get connected to their resource!

For more details on the configuration process, check out Integrate your Remote Desktop Gateway infrastructure using the Network Policy Server (NPS) extension and Azure AD.

Remote Desktop Services - Secure data storage with UPDs

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

Store business resources, user personalization data, and settings securely on-premises or in Azure. RD Session Hosts use AD authentication and empower users with the resources they need in a personalized environment, securely.

Ensuring users have a consistent experience, regardless of the endpoint from which they access their remote resources, is an important aspect of managing an RDS deployment. User Profile Disks (UPDs) allow user data, customizations, and application settings to follow a user within a single collection. A UPD is a per-user, per-collection VHD file saved in a central share that is mounted to a user's session when they sign in - the UPD is treated as a local drive for the duration of that session.

From the user's perspective, the UPD provides a famililar experience - they save their documents to their Documents folder (on what appears to be a local drive), change their app settings as usual, and make any customizations to their Windows environment. All this data, including the registry hive, is stored on the UPD and persists in a central network share. UPDs are only available to the user when the user is actively connected to a desktop or RemoteApp. UPDs can only roam within a collection because the user's entire `C:\Users\<username\>` directory (including AppData\Local) is stored on the UPD.

You can use PowerShell cmdlets to designate the path to the central share, the size of each UPD, and which folders should be included or excluded from the user profile saved to the UPD. Alternatively, you can enable UPDs through Server Manager by going to **Remote Desktop Services** > **Collections** > **Desktop Collection** > **Desktop Collection Properties** > **User Profile Disks**. Note that you enable or disable UPDs for all users of an entire collection, not for specific users in that collection. UPDs must be stored on a central file share where the servers in the collection have full control permissions.

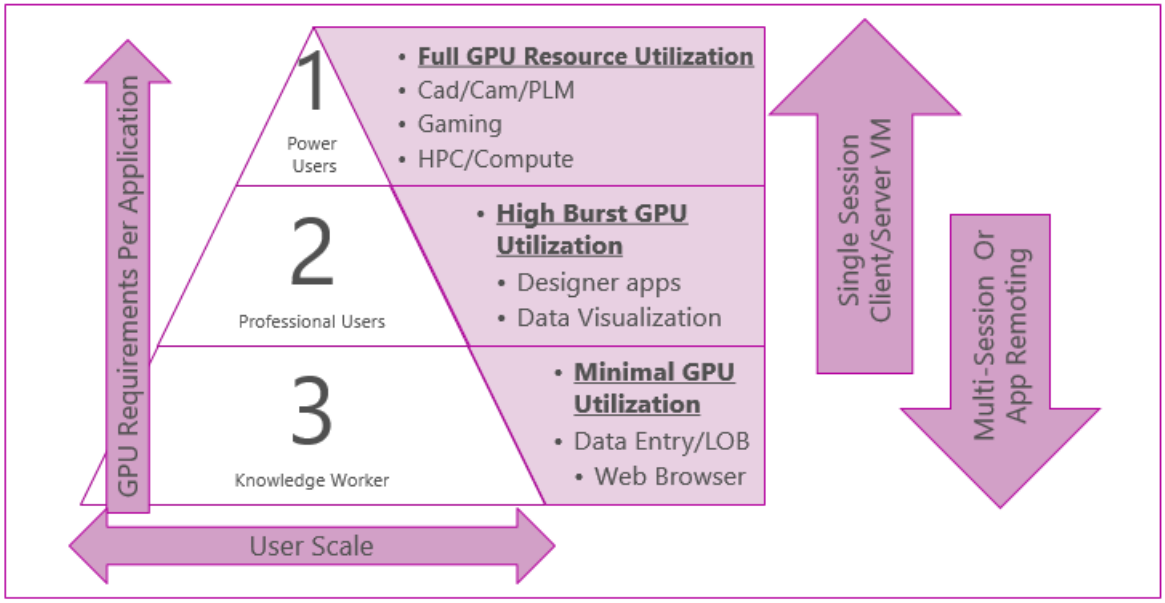
You can achieve high availability for your UPDs by storing them in Azure with Storage Spaces Direct.

Remote Desktop Services - GPU acceleration

10/25/2019 • 2 minutes to read • Edit Online

Remote Desktop Services works with native graphics acceleration as well as the graphics virtualization technologies supported by Windows Server. For information on those technologies, their differences, and how to deploy them, see Plan for GPU acceleration in Windows Server.

When planning for graphics acceleration in your RDS environment, your choice of user scale and user workloads will drive your choice of graphics rendering technology:



Remote Desktop Services - Connect from any device

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

Access corporate resources from any Windows, Apple, or Android computer, tablet, or phone. Enable users to easily see their available desktops and applications from any device through RD Web Feed.

Learn more about Microsoft Remote Desktop clients.

Remote Desktop Services - Choose how you pay

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

Choose your licensing based on what makes sense for your company. License per user to enable users to remote on any of their devices in a BYOD scenario. License per device if users share the same devices. If you are a service provider (HSP or MSP) or ISV, choose the per user SALs license for a flexible, pay-as-you-go model.

For more information, check out License your RDS deployment with client access licenses (CALs).

Desktop Hosting Reference Architecture

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

This article defines a set of architectural blocks for using Remote Desktop Services (RDS) and Microsoft Azure virtual machines to create multitenant, hosted Windows desktop and application services, which we call "desktop hosting." You can use this architecture reference to create highly secure, scalable, and reliable desktop hosting solutions for small- and medium-sized organizations with 5 to 5000 users.

The primary audience for this reference architecture are hosting providers who want to leverage Microsoft Azure Infrastructure Services to deliver desktop hosting services and Subscriber Access Licenses (SALs) to multiple tenants via the Microsoft Service Provider Licensing Agreement (SPLA) program. A second audience for this reference architecture are end customers who want to create and manage desktop hosting solutions in Microsoft Azure Infrastructure Services for their own employees using RDS User CALs extended rights through Software Assurance (SA).

To deliver a desktop hosting solutions, hosting partners and SA customers leverage Windows Server to deliver Windows users an application experience that is familiar to business users and consumers. Built on the foundations of Windows 10, Windows Server 2016 provides familiar application support and user experience.

The scope of this document is limited to:

- Architectural design guidance for a desktop hosting service. Detailed information, such as deployment procedures, performance, and capacity planning is explained in separate documents. For more general information about Azure Infrastructure Services, see Microsoft Azure Virtual Machines.
- Session-based desktops, RemoteApp applications, and server-based personal desktops that use Windows Server 2016 Remote Desktop Session Host (RD Session Host). Windows client-based virtual desktop infrastructures are not covered because there is no Service Provider License Agreement (SPLA) for Windows client operating systems. Windows Server-based virtual desktop infrastructures are allowed under the SPLA, and Windows client-based virtual desktop infrastructures are allowed on dedicated hardware with end-customer licenses in certain scenarios. However, client-based virtual desktop infrastructures are out-of-scope for this document.
- Microsoft products and features, primarily Windows Server 2016 and Microsoft Azure Infrastructure Services.
- Desktop hosting services for tenants ranging in size from 5 to 5000 users. For larger tenants, you may need to modify this architecture to provide adequate performance. The Server Manager RDS graphical user interface (GUI) is not recommended for deployments over 500 users. PowerShell is recommended for managing RDS deployments between 500 and 5000 users.
- The minimum set of components and services required for a desktop hosting service. There are many optional components and services that can be added to enhance a desktop hosting service, but these are out-of-scope for this document.

After reading this document, the reader should understand:

- The building blocks that are necessary to provide a secure, reliable, multitenant desktop hosting solution based in Microsoft Azure Services.
- The purpose of each building block and how they fit together.

There are multiple ways to build a desktop hosting solution based on this architecture. This architecture outlines integration and improvements in Azure with Windows Server 2016. Other deployment options are available with the Desktop Hosting Reference Architecture Guide for Windows Server 2012 R2.

The following topics are covered:

- Desktop hosting logical architecture
- Understand the RDS Roles
- Understand the desktop hosting environment
- Azure services and considerations for desktop hosting

Remote Desktop Services architecture

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

Below are various configurations for deploying Remote Desktop Services to host Windows apps and desktops for end-users.

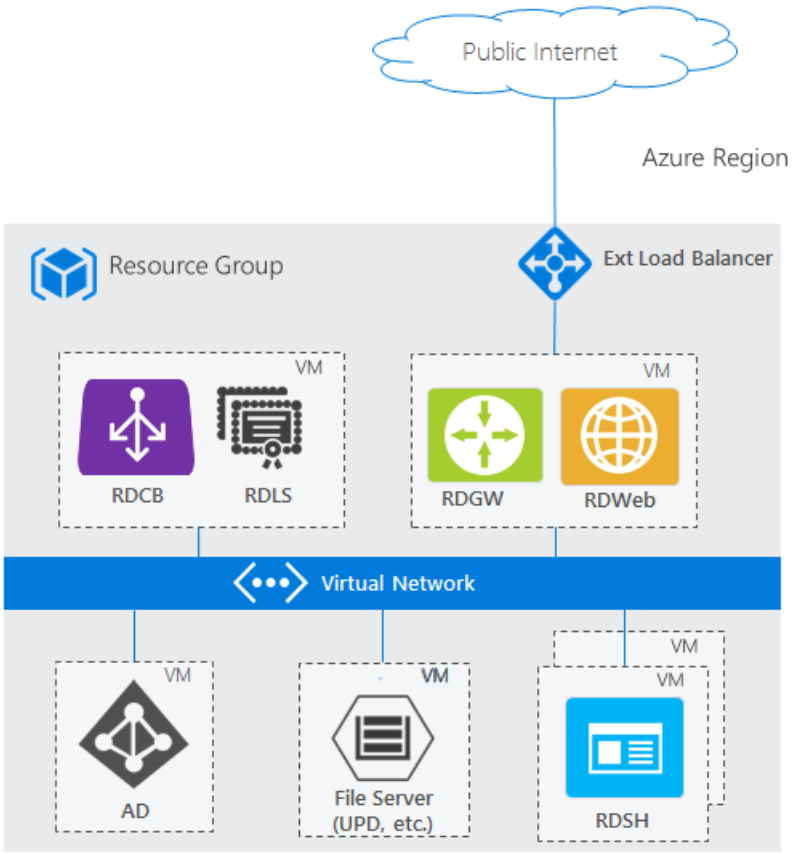
> **NOTE**
> The architecture diagrams below show using RDS in Azure. However, you can deploy Remote Desktop Services on-premises and on other clouds. These diagrams are primarily intended to illustrate how the RDS roles are colocated and use other services.

Standard RDS deployment architectures

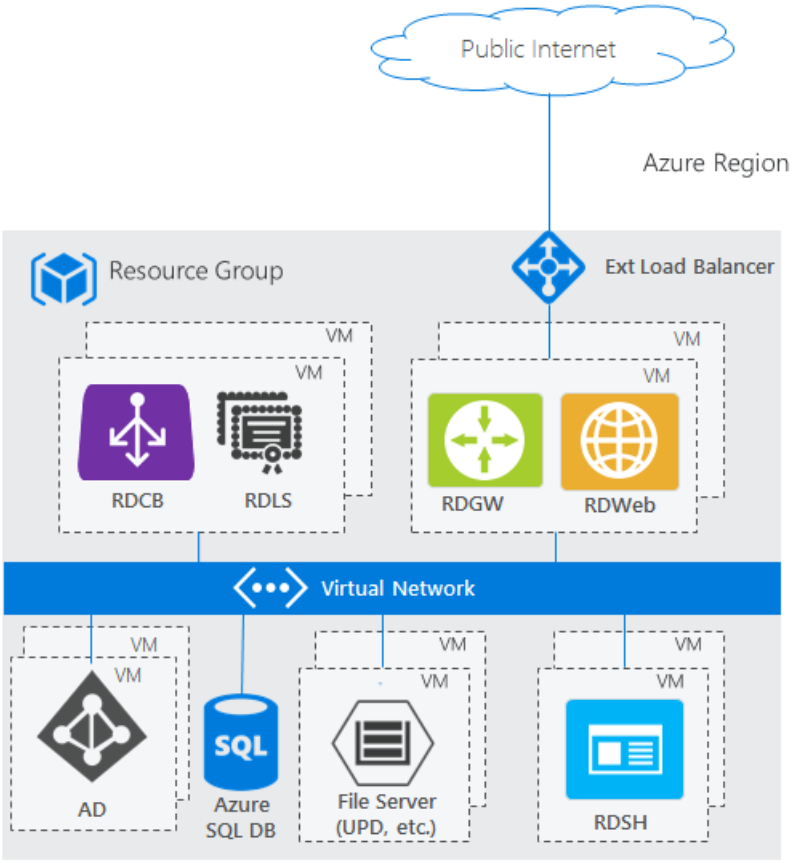
Remote Desktop Services has two standard architectures:

- Basic deployment – This contains the minimum number of servers to create a fully effective RDS environment
- Highly available deployment – This contains all necessary components to have the highest guaranteed uptime for your RDS environment

Basic deployment



Highly available deployment

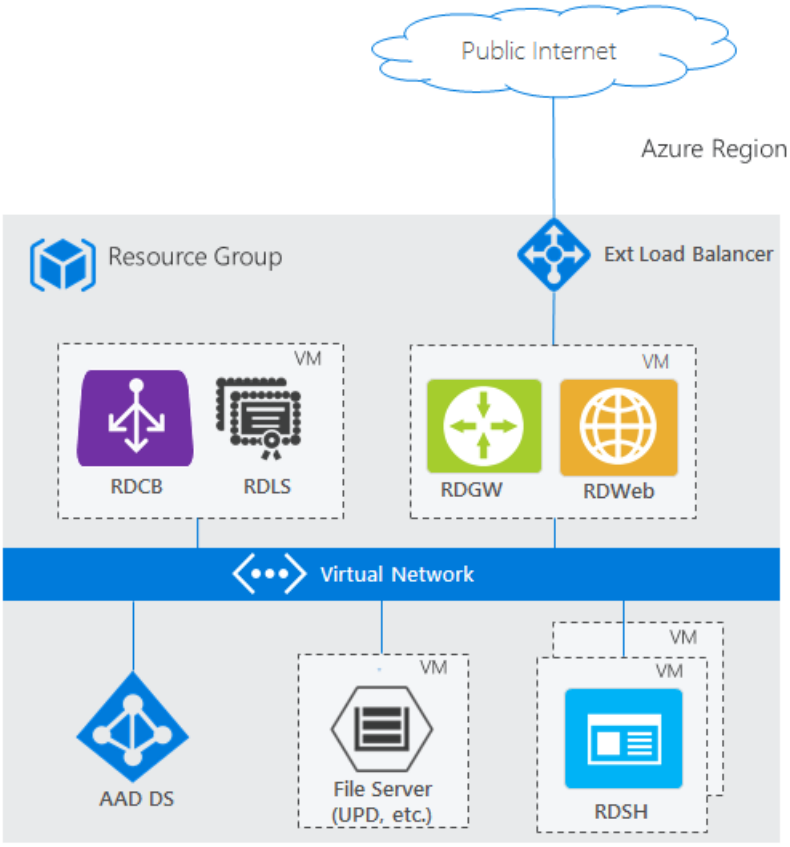


RDS architectures with unique Azure PaaS roles

Though the standard RDS deployment architectures fit most scenarios, Azure continues to invest in first-party PaaS solutions that drive customer value. Below are some architectures showing how they incorporate with RDS.

RDS deployment with Azure AD Domain Services

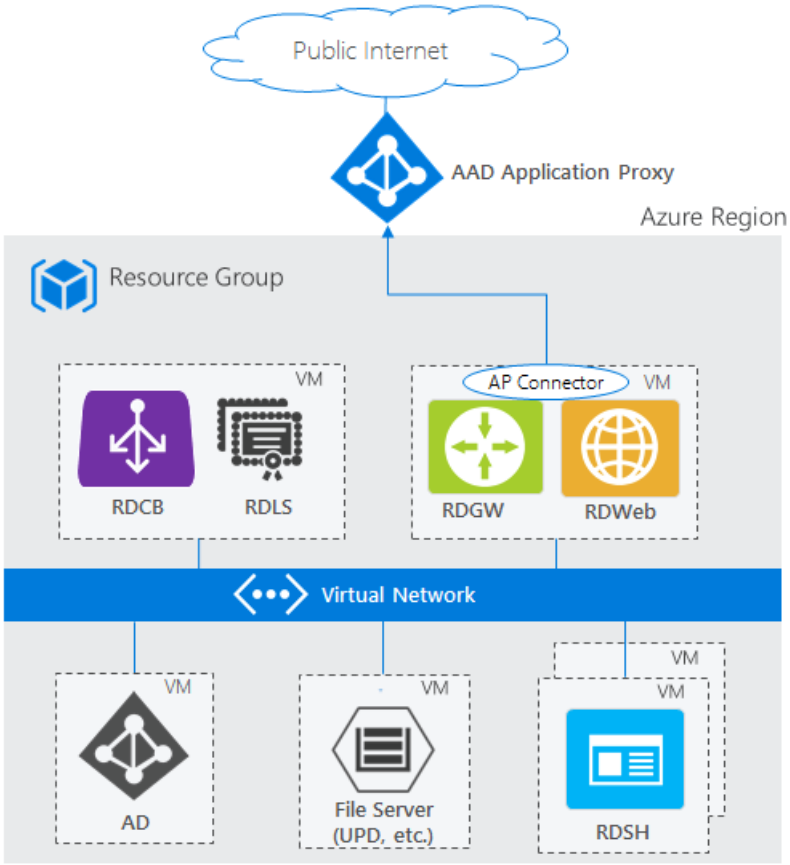
The two standard architecture diagrams above are based on a traditional Active Directory (AD) deployed on a Windows Server VM. However, if you don't have a traditional AD and only have an Azure AD tenant—through services like Office365—but still want to leverage RDS, you can use Azure AD Domain Services to create a fully managed domain in your Azure IaaS environment that uses the same users that exist in your Azure AD tenant. This removes the complexity of manually syncing users and managing more virtual machines. Azure AD Domain Services can work in either deployment: basic or highly available.



RDS deployment with Azure AD Application Proxy

The two standard architecture diagrams above use the RD Web/Gateway servers as the Internet-facing entry point into the RDS system. For some environments, administrators would prefer to remove their own servers from the perimeter and instead use technologies that also provide additional security through reverse proxy technologies. The Azure AD Application Proxy PaaS role fits nicely with this scenario.

For supported configurations and how to create this setup, see how to publish Remote Desktop with Azure AD Application Proxy.


Public Internet
AAD Application Proxy
Azure Region
Resource Group
VM
RDCB
RDLS
AP Connector
VM
RDGW
RDWeb
Virtual Network
VM
AD
VM
File Server
(UPD, etc.)
VM
VM
RDSH

Desktop hosting service

1/10/2020 • 3 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

This article will tell you more about the desktop hosting service's components.

Tenant environment

As described in Remote Desktop service roles, each role plays a distinct part in the tenant envrionment.

The provider's desktop hosting service is implemented as a set of isolated tenant environments. Each tenant's environment consists of a storage container, a set of virtual machines, and a combination of Azure services, all communicating over an isolated virtual network. Each virtual machine contains one or more of the components that make up the tenant's hosted desktop environment. The following subsections describe the components that make up each tenant's hosted desktop environment.

Active Directory Domain Services

Active Directory Domain Services (AD DS) provides the domain and forest information, such that the tenant's users can sign in to the desktops and applications to carry out their workloads. This also enables you to set up or connect to required file shares and databases that may be required for Windows applications.

The tenant's forest does not require any trust relationship with the provider's management forest. A domain administrator account may be set up in the tenant's domain to allow the provider's technical personnel to perform administrative tasks in the tenant's environment (such as monitoring system status and applying software updates) and to assist with troubleshooting and configuration.

There are multiple ways to deploy AD DS:

1. Enable Azure Active Directory Domain Services in the tenant's virtual networking environment. This will create a managed AD DS instance for the tenant based on the users and groups that exist in Azure AD.
2. Set up a stand-alone AD DS server in the tenant's virtual networking environment. This gives you all of the full control of the AD DS instance running on virtual machines.
3. Create a site-to-site VPN connection to an AD DS server located on the tenant's premises. This allows the tenant to connect to their existing AD DS instance and reduce duplication of users, groups, organizational units, and so on.

For more information, see the following articles:

- Azure Active Directory Domain Services documentation
- Desktop Hosting Reference Architecture Guide for Windows Server 2012 R2
- Create a site-to-site connection in the Azure portal

SQL database

A highly-available SQL database is used by the Remote Desktop Connection Broker to store deployment information, such as the mapping of current users' connections to the host servers.

There are multiple ways to deploy an SQL database:

1. Create an Azure SQL Database in the tenant's environment. This provides you with the functionality of a

redundant SQL database without you having to manage the servers themselves. This also allows you to pay for what you consume instead of investing in infrastructure.

2. Create an SQL Server AlwaysOn cluster. This allows you to leverage existing SQL Server infrastructure and gives you complete control over the SQL Server instances.

For more information about how to set up a highly-available SQL database infrastructure, see the following articles:

- What is the Azure SQL Database service?
- Creation and configuration of availability groups (SQL Server).
- Add the RD Connection Broker server to the deployment and configure high availability.

File server

The file server uses the Server Message Block (SMB) 3.0 protocol to provide shared folders. These shared folders are used to create and store user profile disk files (.vhdx) to back up data and let users share data with each other within the tenant's cloud service.

The virtual machine that deploys the file server must have an Azure data disk attached and configured with shared folders. Azure data disks use write-through caching, guaranteeing that writes to the disk will not be erased whenever the virtual machine is restarted.

Small tenants can reduce costs by combining the file server and RD Licensing role on a single virtual machine in the tenant's environment.

For more information, see the following articles:

- Storage in Windows Server
- How to attach a managed data disk to a Windows VM in the Azure portal

User profile disks

User profile disks allow users to save personal settings and files when they are signed in to a session on an RD Session Host server in one collection, then access the same settings and files when signing in to a different RD Session Host server in the collection. When the user first signs in, the tenant's file server creates a user profile disk that gets mounted to the RD Session Host server that the user is currently connected to. For each subsequent sign-in, the user profile disk is mounted to the appropriate RD Session host server, and it is unmounted with each sign-out. Only the user can access the profile disk's contents.

Remote Desktop Services roles

1/14/2020 • 7 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

This article describes the roles within a Remote Desktop Services environment.

Remote Desktop Session Host

The Remote Desktop Session Host (RD Session Host) holds the session-based apps and desktops you share with users. Users get to these desktops and apps through one of the Remote Desktop clients that run on Windows, MacOS, iOS, and Android. Users can also connect through a supported browser by using the web client.

You can organize desktops and apps into one or more RD Session Host servers, called "collections." You can customize these collections for specific groups of users within each tenant. For example, you can create a collection where a specific user group can access specific apps, but anyone outside of the group you designated won't be able to access those apps.

For small deployments, you can install applications directly onto the RD Session Host servers. For larger deployments, we recommend building a base image and provisioning virtual machines from that image.

You can expand collections by adding RD Session Host server virtual machines to a collection farm with each RDSH virtual machine within a collection assigned to same availability set. This provides higher collection availability and increases scale to support more users or resource-heavy applications.

In most cases, multiple users share the same RD Session Host server, which most efficiently utilizes Azure resources for a desktop hosting solution. In this configuration, users must sign in to collections with non-administrative accounts. You can also give some users full administrative access to their remote desktop by creating personal session desktop collections.

You can customize desktops even more by creating and uploading a virtual hard disk with the Windows Server OS that you can use as a template for creating new RD Session Host virtual machines.

For more information, see the following articles:

- Remote Desktop Services - Secure data storage
- Upload a generalized VHD and use it to create new VMs in Azure
- Update RDSH collection (ARM template)

Remote Desktop Connection Broker

Remote Desktop Connection Broker (RD Connection Broker) manages incoming remote desktop connections to RD Session Host server farms. RD Connection Broker handles connections to both collections of full desktops and collections of remote apps. RD Connection Broker can balance the load across the collection's servers when making new connections. If a session disconnects, RD Connection Broker will reconnect the user to the correct RD Session Host server and their interrupted session, which still exists in the RD Session Host farm.

You'll need to install matching digital certificates on both the RD Connection Broker server and the client to support single sign-on and application publishing. When developing or testing a network, you can use a self-generated and self-signed certificate. However, released services require a digital certificate from a trusted certification authority. The name you give the certificate must be the same as the internal Fully Qualified Domain Name (FQDN) of the RD Connection Broker virtual machine.

You can install the Windows Server 2016 RD Connection Broker on the same virtual machine as AD DS to reduce cost. If you need to scale out to more users, you can also add additional RD Connection Broker virtual machines in the same availability set to create an RD Connection Broker cluster.

Before you can create an RD Connection Broker cluster, you must either deploy an Azure SQL Database in the tenant's environment or create an SQL Server AlwaysOn Availability Group.

For more information, see the following articles:

- Add the RD Connection Broker server to the deployment and configure high availability
- SQL database in Desktop hosting service.

Remote Desktop Gateway

Remote Desktop Gateway (RD Gateway) grants users on public networks access to Windows desktops and applications hosted in Microsoft Azure's cloud services.

The RD Gateway component uses Secure Sockets Layer (SSL) to encrypt the communications channel between clients and the server. The RD Gateway virtual machine must be accessible through a public IP address that allows inbound TCP connections to port 443 and inbound UDP connections to port 3391. This lets users connect through the internet using the HTTPS communications transport protocol and the UDP protocol, respectively.

The digital certificates installed on the server and client have to match for this to work. When you're developing or testing a network, you can use a self-generated and self-signed certificate. However, a released service requires a certificate from a trusted certification authority. The name of the certificate must match the FQDN used to access RD Gateway, whether the FQDN is the public IP address' externally facing DNS name or the CNAME DNS record pointing to the public IP address.

For tenants with fewer users, the RD Web Access and RD Gateway roles can be combined on a single virtual machine to reduce cost. You can also add more RD Gateway virtual machines to an RD Gateway farm to increase service availability and scale out to more users. Virtual machines in larger RD Gateway farms should be configured in a load-balanced set. IP affinity isn't required when you're using RD Gateway on a Windows Server 2016 virtual machine, but it is when you're running it on a Windows Server 2012 R2 virtual machine.

For more information, see the following articles:

- Add high availability to the RD Web and Gateway web front
- Remote Desktop Services - Access from anywhere
- Remote Desktop Services - Multi-factor authentication

Remote Desktop Web Access

Remote Desktop Web Access (RD Web Access) lets users access desktops and applications through a web portal and launches them through the device's native Microsoft Remote Desktop client application. You can use the web portal to publish Windows desktops and applications to Windows and non-Windows client devices, and you can also selectively publish desktops or apps to specific users or groups.

RD Web Access needs Internet Information Services (IIS) to work properly. A Hypertext Transfer Protocol Secure (HTTPS) connection provides an encrypted communications channel between the clients and the RD Web server. The RD Web Access virtual machine must be accessible through a public IP address that allows inbound TCP connections to port 443 to allow the tenant's users to connect from the internet using the HTTPS communications transport protocol.

Matching digital certificates must be installed on the server and clients. For development and testing purposes, this can be a self-generated and self-signed certificate. For a released service, the digital certificate must be obtained from a trusted certification authority. The name of the certificate must match the Fully Qualified Domain Name

(FQDN) used to access RD Web Access. Possible FQDNs include the externally facing DNS name for the public IP address and the CNAME DNS record pointing to the public IP address.

For tenants with fewer users, you can reduce costs by combining the RD Web Access and Remote Desktop Gateway workloads into a single virtual machine. You can also add additional RD Web virtual machines to an RD Web Access farm to increase service availability and scale out to more users. In an RD Web Access farm with multiple virtual machines, you'll have to configure the virtual machines in a load-balanced set.

For more information about how to configure RD Web Access, see the following articles:

- Set up the Remote Desktop web client for your users
- Create and deploy a Remote Desktop Services collection
- Create a Remote Desktop Services collection for desktops and apps to run

Remote Desktop Licensing

Activated Remote Desktop Licensing (RD Licensing) servers let users connect to the RD Session Host servers hosting the tenant's desktops and apps. Tenant environments usually come with the RD Licensing server already installed, but for hosted environments you'll have to configure the server in per-user mode.

The service provider needs enough RDS Subscriber Access Licenses (SALs) to cover all authorized unique (not concurrent) users that sign in to the service each month. Service providers can purchase Microsoft Azure Infrastructure Services directly, and can purchase SALs through the Microsoft Service Provider Licensing Agreement (SPLA) program. Customers looking for a hosted desktop solution must purchase the complete hosted solution (Azure and RDS) from the service provider.

Small tenants can reduce costs by combining the file server and RD Licensing components onto a single virtual machine. To provide higher service availability, tenants can deploy two RD License server virtual machines in the same availability set. All RD servers in the tenant's environment are associated with both RD License servers to keep users able to connect to new sessions even if one of the servers goes down.

For more information, see the following articles:

- License your RDS deployment with client access licenses (CALs)
- Activate the Remote Desktop Services license server
- Track your Remote Desktop Services client access licenses (RDS CALs)
- Microsoft Volume Licensing: licensing options for service providers

Azure services and considerations for desktop hosting

1/10/2020 • 4 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

The following sections describe Azure Infrastructure Services.

Azure portal

After the provider creates an Azure subscription, the Azure portal can be used to manually create each tenant's environment. This process can also be automated using PowerShell scripts.

For more information, visit the Microsoft Azure website.

Azure Load Balancer

The tenant's components run on virtual machines that communicate with each other on an isolated network. During the deployment process, you can externally access these virtual machines through the Azure Load Balancer using Remote Desktop Protocol endpoints or a Remote PowerShell endpoint. Once a deployment is complete, these endpoints will typically be deleted to reduce the attack surface area. The only endpoints will be the HTTPS and UDP endpoints created for the virtual machine running the RD Web and RD Gateway components. This allows clients on the internet to connect to sessions running in the tenant's desktop hosting service. If a user opens an application that connects to the internet, such as a web browser, the connections will be passed through the Azure Load Balancer.

For more information, see What is Azure Load Balancer?

Security considerations

This Azure Desktop Hosting Reference Architecture Guide is designed to provide a highly secure and isolated environment for each tenant. System security also depends on safeguards taken by the provider during deployment and operation of the hosted service. The following list describes some considerations the provider should take to keep their desktop hosting solution based on this reference architecture secure.

- All administrative passwords must be strong, ideally randomly generated, changed frequently, and saved in a secure central location only accessible to a select few provider administrators.
- When replicating the tenant environment for new tenants, avoid using the same or weak administrative passwords.
- The RD Web Access site URL, name, and certificates must be unique and recognizable to each tenant to prevent spoofing attacks.
- During the normal operation of the desktop hosting service, all public IP addresses should be deleted for all virtual machines except the RD Web and RD Gateway virtual machine that lets users securely connect to the tenant's desktop hosting cloud service. Public IP addresses may be temporarily added when necessary for management tasks, but they should always be deleted afterwards.

For more information, see the following articles:

- Security and protection
- Security best practices for IIS 8

- Secure Windows Server 2012 R2

Design considerations

It's important to consider the constraints of Microsoft Azure Infrastructure Services when designing a multitenant desktop hosting service. The following list describes considerations the provider must take to achieve a functional and cost-effective desktop hosting solution based on this reference architecture.

- An Azure subscription has a maximum number of virtual networks, VM cores, and Cloud Services that can be used. If a provider needs more resources than this, they may need to create multiple subscriptions.
- An Azure Cloud Service has a maximum number of virtual machines that can be used. The provider may need to create multiple Cloud Services for larger tenants that exceed the maximum.
- Azure deployment costs are based partially on the number and size of virtual machines. The provider should optimize the number and size of the virtual machines for each tenant to provide a functional and highly secure Desktop Hosting environment at the lowest cost.
- The physical computer resources in the Azure data center are virtualized by using Hyper-V. Hyper-V hosts are not configured in host clusters, so the availability of the virtual machines is dependent on the availability of the individual servers used in the Azure infrastructure. To provide higher availability, multiple instances of each role service virtual machine can be created in an availability set, then guest clustering can be implemented within the virtual machines.
- In a typical storage configuration, a service provider will have a single storage account with multiple containers (for example, one for each tenant), and multiple disks within each container. However, there is a limit to the total storage and performance that can be achieved for a single storage account. For service providers that support large numbers of tenants or tenants with high storage capacity or performance requirements, the service provider may need to create multiple storage accounts.

For more information, see the following articles:

- Sizes for Cloud Services
- Microsoft Azure virtual machine pricing details
- Hyper-V overview
- Azure Storage scalability and performance targets

Azure Active Directory Application Proxy

Azure Active Directory (AD) Application Proxy is a service provided in paid SKUs of Azure AD that allow users to connect to internal applications through Azure's own reverse-proxy service. This allows the RD Web and RD Gateway endpoints to be hidden inside of the virtual network, eliminating the need to be exposed to the internet by a public IP address. Hosters can use Azure AD Application Proxy to condense the number of virtual machines in the tenant's environment while still maintaining a full deployment. Azure AD Application Proxy also enables many of the benefits that Azure AD provides, such as conditional access and multi-factor authentication.

For more information, see Get started with Application Proxy and install the connector.

Build and deploy your Remote Desktop Services deployment

9/27/2019 • 2 minutes to read • Edit Online

A Remote Desktop Services deployment is the infrastructure used to share apps and resources with your users. Depending on the experience you want to provide, you can make it as small or complex as you need. Remote Desktop deployments are easily scaled. You can increase and decrease Remote Desktop Web Access, Gateway, Connection Broker and Session Host servers at will. You can use Remote Desktop Connection Broker to distribute workloads. Active Directory based authentication provides a highly secure environment.

Remote Desktop clients enable access from any Windows, Apple, or Android computer, tablet, or phone.

See Remote Desktop Services architecture for a detailed discussion of the different pieces that work together to make up your Remote Desktop Services deployment.

Have an existing Remote Desktop deployment built on a previous version of Windows Server? Check out your options for moving to WIndows Server 2016, where you can take advantage of new and better functionality around performance and scale:

- Migrate your RDS deployment to Windows Server 2016
- Upgrade your RDS deployment to Windows Server 2016

Want to create a new Remote Desktop deployment? Use the following information to deploy Remote Desktop in Windows Server 2016:

- Deploy the Remote Desktop Services infrastructure
- Create a session collection to hold the apps and resources you want to share
- License your RDS deployment
- Have your users install a Remote Desktop client so they can access the apps and resources.
- Enable high availability by adding additional Connection Brokers and Session Hosts:
  - Scale out an existing RDS collection with an RD Session Host farm
  - Add high availability to the RD Connection Broker infrastructure
  - Add high availability to the RD Web and RD Gateway web front
  - Deploy a two-node Storage Spaces Direct file system for UPD storage

If you're a hosting partner interested in using Remote Desktop to provide apps and resources to customers or a customer looking for someone to host your apps, check out Remote Desktop Services hosting partners for information about an assessment you can take about using RDS in Azure as a hosting environment, as well as a list of partners who've passed it.

Seamlessly deploy RDS with ARM and Azure Marketplace

9/27/2019 • 4 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2

Remote Desktop Services (RDS) is the platform of choice to cost-effectively host Windows desktops and applications. You can use an Azure Marketplace offering or a quickstart template to quickly create an RDS on Azure IaaS deployment. Azure marketplace creates a test domain for you, making it a simple and easy mechanism for testing and proof-of-concepts. The quickstart templates, on the other hand, allow you to use an existing domain, making them a great tool to build out a production environment. Once set up, you can connect to the published desktops and applications from various platforms and devices, using the Microsoft Remote Desktop apps for Windows, Mac, iOS, and Android.

Basic RDS through the Azure Marketplace

Creating your deployment through the Azure Marketplace is the quickest way to get up and running. When everything is completed, your environment will look like the basic RDS architecture. The offering creates all the RDS components that you need - all you need to do is supply some information.

You'll need to supply the following information when you deploy the Marketplace offering:

- Administrator user name and password. This is a new user that will manage the deployment.
- DNS name and AD domain name. These are NEW resources that are created. Make sure the names are meaningful.
- VM size. You get to choose the size of VMs to use for the RDSH endpoints. You can also manually change the sizes after the initial deployment to help you optimize the VMs for your workloads and for cost.

Use these steps to create your small-footprint RDS deployment from the Azure Marketplace:

1. Launch the Azure Marketplace RDS deployment:
   a. Sign into the Azure portal.
   b. Click **New** to add your deployment.
   c. Type "RDS" in the search field and press Enter.
   d. Click **Remote Desktop Services (RDS) - Basic - Dev/Test**, and then click **Create**.
   e. Follow the steps in the portal to create and deploy RDS. You'll add key configuration details, like the information listed above.
2. Connect to your deployment. When the deployment finishes, check the outputs section for final steps to complete and connect to your deployment.
   a. Download and run this PowerShell script on your test device to install any certificates needed to connect to the RDS deployment.

      This step is only necessary during the testing phase. When you deploy RDS in Azure in production, make sure to follow best practices like purchasing and using a publicly trusted SSL certificate on your web servers.

   b. When prompted, sign into your Azure account. Select the Azure subscription, resource group, and public IP address created for this new deployment.

c. When the script is finished, the RD Web page launches in your default browser. You can double-check the RD Web page by comparing the URL for the page to the DNS address you provided during deployment.

   Sign in with the admin credentials you created during deployment to see the default desktop published for you. You can also send users the RD Web site to test their desktops and applications.

> **TIP**
> Forget the domain name or admin user? You can go back to the new Resource Group in the portal, click **Deployments**, and then view the parameters you entered.

Now that you have an RDS deployment, you can add and manage users.

Customized RDS using Quickstart templates

You can use Azure Resource Manager templates to deploy RDS in Azure. This is especially useful if you want a basic RDS deployment but have existing components (like AD) that you want to use. Unlike the Marketplace offering, you can make further customizations, such as using an existing AD on a virtual network, using a custom OS image for the RDSH VMs, and layering on high availability for RDS components. After adding on high availability to each component, your environment will look like the highly availabile RDS architecture.

Use these steps to create your small-footprint RDS deployment with an Azure RDS template:

1. Pick your Azure Quickstart template:
   a. Go to the RDS Azure Quickstart Templates site.
   b. Choose the template that matches what you are trying to do. Make sure you meet any prerequisites for that specific template. (For example, if you are want to use a custom image for your VMs, make sure you have already uploaded that image to an Azure storage account.)
   c. Click **Deploy to Azure**.
   d. You'll need to provide some details (like admin user name, AD domain name) in the Azure portal. This varies based on the template you choose.
   e. Click **Purchase**.
2. Connect to your deployment.
   a. Download and run this PowerShell script on your test device to install any certificates needed to connect to the RDS deployment.

      This step is only necessary during the testing phase. When you deploy RDS in Azure in production, make sure to follow best practices like purchasing and using a publicly trusted SSL certificate on your web servers.

   b. When prompted, sign into your Azure account. Select the Azure subscription, resource group, and public IP address created for this new deployment.

   c. When the script is finished, the RD Web page launches in your default browser. You can double-check the RD Web page by comparing the URL for the page to the DNS address you provided during deployment.

      Sign in with the admin credentials you created during deployment to see the default desktop published for you. You can also send users the RD Web site to test their desktops and applications.

> **TIP**
>
> Forget the domain name or admin user? You can go back to the new Resource Group in the portal, click **Deployments**, and then view the parameters you entered.

Now that you have an RDS deployment, you can add and manage users.

Migrate your Remote Desktop Services deployment to Windows Server 2016

9/27/2019 • 5 minutes to read • Edit Online

If you are currently running Remote Desktop Services in Windows Server 2012 R2, you can move to Windows Server 2016 to take advantage of new features like support for Azure SQL and Storage Spaces Direct.

Migration for a Remote Desktop Services deployment is supported from source servers running Windows Server 2016 to destination servers running Windows Server 2016. In other words, there is no direct in-place migration from RDS in Windows Server 2012 R2 to Windows Server 2016. Instead, for most of the RDS components, you first upgrade to Windows Server 2016 and then migrate data and licenses. The only components with a direct migration are RD Web, RD Gateway, and the licensing server.

For more information on the upgrade process and requirements, see upgrading your Remote Desktop Services deployments to Windows Server 2016.

Use the following steps to migrate your Remote Desktop Services deployment:

- Migrate RD Connection Broker servers
- Migrate session collections
- Migrate virtual desktop collections
- Migrate RD Web Access servers
- Migrate RD Gateway servers
- Migrate RD Licensing servers
- Migrate certificates

Migrate RD Connection Broker servers

This is the first and most important step for migrating: migrating your RD Connection Brokers to destination servers running Windows Server 2016.

> **IMPORTANT**
> The Remote Desktop Connection Broker (RD Connection Broker) source servers must be configured for high availability to support migration. For more information, see Deploy a Remote Desktop Connection Broker cluster.

1. If you have more than one RD Connection Broker server in the high availability setup, remove all the RD Connection Broker servers except the one that is currently active.
2. Upgrade the remaining RD Connection Broker server in the deployment to Windows Server 2016.
3. Add Windows Server 2016 RD Connection Broker servers into the high availability deployment.

NOTE

A mixed high availability configuration with Windows Server 2016 and Windows Server 2012 R2 is not supported for RD Connection Broker servers. An RD Connection Broker running Windows Server 2016 can serve session collections with RD Session Host servers running Windows Server 2012 R2, and it can serve virtual desktop collections with RD Virtualization Host servers running Windows Server 2012 R2.

Migrate session collections

Follow these steps to migrate a session collection in Windows Server 2012 R2 to a session collection in Windows Server 2016.

IMPORTANT

Migrate session collections only after successfully completing the previous step, Migrate RD Connection Broker servers.

1. Upgrade the session collection from Windows Server 2012 R2 to Windows Server 2016.
2. Add the new RD Session Host server running Windows Server 2016 to the session collection.
3. Sign out of all sessions in the RD Session Host servers, and remove the servers that require migration from the session collection.

NOTE

If the UVHD template (UVHD-template.vhdx) is enabled in the session collection and the file server has been migrated to a new server, update the User Profile Disks: Location collection property with the new path. The User Profile Disks must be available at the same relative path in the new location as they were on the source server.

A session collection of RD Session Host servers with a mix of servers running Windows Server 2012 R2 and Windows Server 2016 is not supported.

Migrate virtual desktop collections

Follow these steps to migrate a virtual desktop collection from a source server running Windows Server 2012 R2 to a destination server running Windows Server 2016.

IMPORTANT

Migrate virtual desktop collections only after successfully completing the previous step, Migrate RD Connection Broker servers.

1. Upgrade the virtual desktop collection from the server running Windows Server 2012 R2 to Windows Server 2016.
2. Add the new Windows Server 2016 RD Virtualization Host servers to the virtual desktop collection.
3. Migrate all virtual machines in the current virtual desktop collection that are running on RD Virtualization Host servers to the new servers.
4. Remove all RD Virtualization Host servers that required migration from the virtual desktop collection in the source server.

NOTE

If the UVHD template (UVHD-template.vhdx) is enabled in the session collection and the file server has been migrated to a new server, update the User Profile Disks: Location collection property with the new path. The User Profile Disks must be available at the same relative path in the new location as they were on the source server.

A virtual desktop collection of RD Virtualization Host servers with a mix of servers running Windows Server 2012 R2 and Windows Server 2016 is not supported.

Migrate RD Web Access servers

Follow these steps to migrate RD Web Access servers:

- Join the destination servers running Windows Server 2016 to the Remote Desktop Services deployment and install the RD Web role
- Use IIS Web Deploy tool to migrate the RD Web website settings from the current RD Web Access servers to the destination servers running Windows Server 2016.
- Migrate certificates to the destination servers running Windows Server 2016.
- Remove the source servers from the Remote Desktop Services deployment.

Migrate RD Gateway servers

Follow these steps to migrate RD Gateway servers:

- Join the destination servers running Windows Server 2016 to the Remote Desktop Services deployment and install the RD Gateway role
- Use IIS Web Deploy tool to migrate the RD Gateway endpoint settings from the current RD Gateway servers to the destination servers running Windows Server 2016.
- Migrate certificates to the destination servers running Windows Server 2016.
- Remove the source servers from the Remote Desktop Services deployment.

Migrate RD Licensing servers

Follow these steps to migrate an RD Licensing server from a source server running Windows Server 2012 or Windows Server 2012 R2 to a destination server running Windows Server 2016.

1. Migrate the Remote Desktop Services client access licenses (RDS CALs) from the source server to the destination server.
2. Edit the **Deployment Properties** in **Server Manager** on the Remote Desktop management server (which is typically being run on the first RD Connection Broker server) to include only the new RD Licensing servers running Windows Server 2016.
3. Deactivate the source RD Licensing server: In **Remote Desktop Licensing Manager**, right-click the appropriate server, hover over **Advanced** to select **Deactivate Server**, and then follow the steps in the wizard.
4. Remove the source RD Licensing servers from the deployment in **Server Manager** on the Remote Desktop management server.

Migrate certificates

Successful certificate migration requires both the actual process of migrating certificates and updating certificate information in the Remote Desktop Services Deployment Properties.

Typical certificate migration includes the following steps:

- Export the certificate to a PFX file with the private key.
- Import the certificate from a PFX file.

After migrating the appropriate certificates, update the following required certificates for the Remote Desktop Services deployment in server manager or PowerShell:

- RD Connection Broker - single sign-on
- RD Connection Broker - RDP file publishing
- RD Gateway - HTTPS connection
- RD Web Access - HTTPS connection and RemoteApp/desktop connection subscription

Migrate your Remote Desktop Services Client Access Licenses (RDS CALs)

9/27/2019 • 6 minutes to read • Edit Online

You have three options to migrate your RDS CALs:

1. Automatic connection method: This recommended method communicates via internet directly to the Microsoft Clearinghouse outbound over TCP port 443.
2. Using a web browser: This method allows migration when the server running the Remote Desktop Licensing Manager tool does not have internet connectivity, but the administrator has internet connectivity on a separate device. The URL for the Web migration method is displayed in the Manage RDS CALs Wizard.
3. Using a telephone: This method allows the administrator to complete the migration process over the phone with a Microsoft representative. The appropriate telephone number is determined by the country/region that you chose in the Activate Server Wizard and is displayed in the Manage RDS CALs Wizard.

In this article, the Establish RDS CAL migration method highlights the general steps common across any RDS CAL migration method, while Migrate RDS CALs highlights the steps specific to each migration method.

Regardless of migration method, you must, at a minimum, be a member of the local Administrators group to perform the migration steps.

Establish RDS CAL migration method

1. On the license server, open **Remote Desktop Licensing Manager**. (Click **Start > Administrative Tools**. Enter the **Remote Desktop Services** directory, and launch **Remote Desktop Licensing Manager**.)
2. Verify the connection method for the Remote Desktop license server: right-click the license server to which you want to migrate the RDS CALs, and then click **Properties**. On the **Connection Method** tab, verify the **Connection method** - you can change it in the dropdown menu. Click **OK**.
3. Right-click the license server to which you want to migrate the RDS CALs, and then click **Manage RDS CALs**.
4. Follow the steps in the wizard to the **Action Selection** page. Click **Migrate RDS CALs from another license server to this license server**.
5. Choose the reason for migrating the RDS CALs, and then click **Next**. You have the following choices:
   - The source license server is being replaced by this license server.
   - The source license server is no longer functioning.
6. The next page in the wizard depends on the migration reason that you chose.
   - If you chose **The source license server is being replaced by this license server** as the reason for migrating the RDS CALs, the **Source License Server Information** page is displayed.

     On the Source License Server Information page, enter the name or IP address of the source license server.

     If the source license server is available on the network, click **Next**. The wizard contacts the source license server. If the source license server is running an operating system earlier than Windows Server 2008 R2 or the source license server is deactivated, you are reminded that you must remove the RDS CALs manually from the source license server after the wizard has completed. After you confirm that you understand this requirement, the **Obtain Client License Key Pack** page appears.

     If the source license server is not available on the network, select **The specified source license server is not available on the network**. Specify the operating system that the source license server

is running, and then provide the license server ID for the source license server. After you click **Next**, you are reminded that you must remove the RDS CALs manually from the source license server after the wizard has completed. After you confirm that you understand this requirement, the **Obtain Client License Key Pack** page appears.

- If you chose **The source license server is no longer functioning** as the reason for migrating the RDS CALs, you are reminded that you must remove the RDS CALs manually from the source license server after the wizard has completed. After you confirm that you understand this requirement, the **Obtain Client License Key Pack** page appears.

The next step is to migrate the CALs - use the information below to complete the wizard. Note that what you see in the wizard depends on the connection method you identified in Step 2 above.

Migrate RDS CALs

There are three mechanisms to migrate licenses to the destination license server; continue the steps corresponding to the **Connection method** verified in Step 2:

- Automatic connection method
- Using a web browser
- Using a telephone

Automatic connection method

1. On the **License Program** page, select the appropriate program through which you purchased your RDS CALs, then click **Next**.
2. Enter the required information (typically a license code or an agreement number, depending on the **License program**), and then click **Next**. Consult the documentation provided when you purchased your RDS CALs.
3. Select the appropriate product version, license type, and quantity of RDS CALs for your environment based on your RDS CAL purchase agreement, and then click **Next**.
4. The Microsoft Clearinghouse is automatically contacted and processes your request. The RDS CALs are then migrated onto the license server.
5. Click **Finish** to complete the RDS CAL migration process.

Using a web browser

1. On the **Obtain Client License Key Pack** page, click the hyperlink to connect to the Remote Desktop Services Licensing Web site. If you are running Remote Desktop Licensing Manager on a computer that does not have Internet connectivity, note the address for the Remote Desktop Services Licensing Web site, and then connect to the Web site from a computer that has Internet connectivity.
2. On the Remote Desktop Services Licensing Web page, under **Select Option**, select **Manage CALs**, and then click **Next**.
3. Provide the following required information, then click **Next**:
   - **Target License Server ID**: A 35-digit number, in groups of 5 numerals, which is displayed on the **Obtain Client License Key Pack** page in the Manage RDS CALs Wizard.
   - **Reason for recovery**: Choose the reason for migrating the RDS CALs.
   - **License Program**: Choose the program through which you purchased your RDS CALs.
4. Provide the following required information, then click **Next**:
   - Last name or surname
   - First name or given name
   - Company name

- Country/region

  You can also provide the optional information requested, such as company address, e-mail address, and phone number. In the organizational unit field, you can describe the unit within your organization that this license server serves.

5. The License Program that you selected on the previous page determines what information you need to provide on the next page. In most cases, you must provide either a license code or an agreement number. Consult the documentation provided when you purchased your RDS CALs. In addition, you need to specify which type of RDS CAL and the quantity that you want to migrate to the license server.
6. After you have entered the required information, click **Next**.
7. Verify that all of the information that you have entered is correct, then click **Next** to submit your request to the Microsoft Clearinghouse. The web page then displays a license key pack ID generated by the Microsoft Clearinghouse.

   > **IMPORTANT**
   > Keep a copy of the license key pack ID. Having this information with you facilitates communications with the Microsoft Clearinghouse, should you need assistance with recovering RDS CALs.

8. On the same **Obtain Client License Key Pack** page, enter the license key pack ID, and then click **Next** to migrate the RDS CALs to your license server.
9. Click **Finish** to complete the RDS CAL migration process.

Using a telephone

1. On the **Obtain Client License Key Pack** page, use the displayed telephone number to call the Microsoft Clearinghouse. Give the representative your Remote Desktop license server ID and the required information for the licensing program through which you purchased your RDS CALs. The representative then processes your request to migrate the RDS CALs, and gives you a unique ID for the RDS CALs. This unique ID is referred to as the **license key pack ID**.

   > **IMPORTANT**
   > Keep a copy of the license key pack ID. Having this information with you facilitates communications with the Microsoft Clearinghouse should you need assistance with recovering RDS CALs.

2. On the same **Obtain Client License Key Pack** page, enter the license key pack ID, and then click **Next** to migrate the RDS CALs to your license server.
3. Click **Finish** to complete the RDS CAL migration process.

Upgrading your Remote Desktop Services deployments to Windows Server 2016

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

Supported OS upgrades with RDS role installed

Upgrades to Windows Server 2016 are supported only from Windows Server 2012 R2 and Windows Server 2016.

Flow for deployment upgrades

In order to keep the down-time to a minimum, it is best to follow the steps below:

1. **RD Connection Broker servers** should be the first to be upgraded. If there is active/active setup in the deployment, remove all but one server from the deployment and perform an in-place upgrade. Perform upgrades on the remaining RD Connection Broker servers offline and then re-add them to the deployment. The deployment will not be available during RD Connection Broker servers upgrade.

   > **NOTE**
   > It is mandatory to upgrade RD Connection Broker servers. We do not support Windows Server 2012 R2 RD Connection Broker servers in a mixed deployment with Windows Server 2016 servers. Once the RD Connection Broker server(s) are running Windows Server 2016 the deployment will be functional, even if the rest of the servers in the deployment are still running Windows Server 2012 R2.

2. **RD License servers** should be upgraded before you upgrade your RD Session Host servers.

   > **NOTE**
   > Windows Server 2012 and 2012 R2 RD license servers will work with Windows Server 2016 deployments, but they can only process CALs from Windows Server 2012 R2 and older. They cannot use Windows Server 2016 CALs. See License your RDS deployment with client access licenses (CALs) for more information about RD license servers.

3. **RD Session Host servers** can be upgraded next. To avoid down time during upgrade the admin can split the servers to be upgraded in 2 steps as detailed below. All will be functional after the upgrade. To upgrade, use the steps described in Upgrading Remote Desktop Session Host servers to Windows Server 2016.

4. **RD Virtualization Host servers** can be upgraded next. To upgrade, use the steps described in Upgrading Remote Desktop Virtualization Host servers to Windows Server 2016.

5. **RD Web Access servers** can be upgraded anytime.

   > **NOTE**
   > Upgrading RD Web may reset IIS properties (such as any configuration files). To not lose your changes, make notes or copies of customizations done to the RD Web site in IIS.

> **NOTE**
> Windows Server 2012 and 2012 R2 RD Web Access servers will work with Windows Server 2016 deployments.

6. **RD Gateway servers** can be upgraded anytime.

> **NOTE**
> Windows Server 2016 does not include Network Access Protection (NAP) policies - they will have to be removed. The easiest way to remove the correct policies is by running the upgrade wizard. If there are any NAP policies you must delete, the upgrade will block and create a text file on the desktop that includes the specific policies. To manage NAP policies, open the Network Policy Server tool. After deleting them, click **Refresh** in the Setup tool to continue with the upgrade process.

> **NOTE**
> Windows Server 2012 and 2012 R2 RD Gateway servers will work with Windows Server 2016 deployments.

VDI deployment – supported guest OS upgrade

Administrators will have the following options to upgrade of VM collections:

Upgrade Managed Shared VM collections

Administrators will need to create VM templates with the desired OS version and use it to patch all the VMs in the pool.

We support the following patching scenarios:

- Windows 7 SP1 can be patched to Windows 8 or Windows 8.1
- Windows 8 can be patched to Windows 8.1
- Windows 8.1 can be patched to Windows 10

Upgrade unmanaged shared VM collections

End users cannot upgrade their personal desktops. Administrators should perform the upgrade. The exact steps are still to be determined.

Upgrading your Remote Desktop Session Host to Windows Server 2016

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

IMPORTANT

All applications must be uninstalled before the upgrade and reinstalled after the upgrade to avoid any app compatibility issues that may rise because of the upgrade.

Supported OS upgrades with RDS role installed

Upgrades to Windows Server 2016 are supported only from Windows Server 2012 R2 and Windows Server 2016 TP5.

Upgrading a RDS session-based collection

In order to keep the down-time to a minimum, it is best to follow the steps below while upgrading a RDS session-based collection:

1. Identify the servers to be upgraded, say, half the servers in the collection.
2. Prevent new connections to these servers by setting **Allow New Connections** to false.
3. Log off all sessions on these servers.
4. Remove these servers from the collection.
5. Upgrade the servers to Windows Server 2016.
6. Set **Allow New Connections** to "false" on the remaining servers in the collection.
7. Add the upgraded servers back to their corresponding collections.
8. Remove the remaining set of servers to be upgraded from the collection.
9. Set **Allow New Connections** to "true" on the upgraded servers in the collection.
10. Now upgrade the remaining servers in the deployment by following steps 3 through 9 above.

Upgrading a standalone RD Session Host server

A standalone RD Session Host server can be upgraded anytime.

Upgrading your Remote Desktop Virtualization Host to Windows Server 2016

9/27/2019 • 3 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016

Supported OS upgrades with RDS role installed

Upgrades to Windows Server 2016 are supported only from Windows Server 2012 R2 and Windows Server 2016 TP5.

RD Virtualization Host servers in the deployment where VMs are stored locally

These servers should be upgraded all at once. Follow the following steps to upgrade:

1. Log off all users.
2. Turn off or save all virtual machines on each host.
3. Upgrade the servers to Windows Server 2016.
4. All collections should be available and functional after the upgrades are complete.

RD Virtualization Host servers in the deployment where VMs are stored in Cluster Shared Volumes (CSV)

1. Determine an upgrade strategy where some of the RDVH servers will be upgraded and some will continue to host VMs on Windows Server 2012 R2.
2. Isolate one or more of the RDVH servers, targeted for the initial round of upgrading, by migrating all VMs to other 'not to be upgraded yet' RDVH servers that will remain part of the original 2012 R2 cluster.
   a. Open Failover Cluster Manager.
   b. Click **Roles**.
   c. Select one or more VMs. Right-click to open the context menu.
   d. Click **Move** and choose either **Live** or **Quick Migration** to move the VMs to one or more of the RD Virtualization Host Servers that are not part of the initial upgrade. Use **Live** or **Quick** Migration depending on factors such as hardware compatibility or online requirements.
3. Evict the RDVH servers, prepared for upgrading, from the original cluster.
4. Upgrade the isolated RDVH servers.
5. After the targeted RDVH servers have been successfully upgraded, create a new cluster and CSV, which needs to be on an entirely different SAN volume.
6. Join all upgraded RDVH servers to the new cluster.
7. Create a folder structure in the new CSV that mimics the existing folder structure in the existing CSV. This will include the collection folders and each VM's top level sub-folders.
8. From the various VM Collection folders on the original CSV, copy over the /IMGS folder and contents to the new collection folders in the same locations on the new CSV.
9. On the source RDVH machine, use Cluster Manager to remove the VM's configuration for high availability:
   a. Launch Cluster Manager.
   b. Click **Roles**.

c. Right-click the VM objects, and then click **Remove**.

10. On one of the non-upgraded RDVH servers, use Hyper-V Manager to move all VMs to one of the upgraded RDVH servers and new Cluster CSV:

    a. Open Hyper-V Manager.

    b. Select one of the non-upgraded RDVH servers.

    c. Right-click one of the VMs to be moved, and then click **Move**.

    d. Choose **Move the virtual machine**, and then click **Next**.

    e. Provide the targeted upgraded RDVH server's name on the **Specify Destination Computer** page, and then click **Next**.

    f. Choose **Move the virtual machine's data to a single location**, and then click **Next**.

    g. Browse to the destination location.

    > **IMPORTANT**
    > Ensure this path is to an empty folder for the specific VM.

    > **NOTE**
    > As mentioned, you will need to have already created a new destination sub folder prior to this step. The Select Folder dialog will not allow you to create a sub folder in this step.

    Click **Next**, and then click **Finished**.

11. Once the VMs are relocated, add them as cluster **High Availability** objects:
    a. Open Failover Cluster Manager on an upgraded RD Virtualization Host Server.
    b. Right-click the **Roles** node, and then click **Configure Role**. Click **Next** on the **Start** page of the High Availability wizard.
    c. Choose **Virtual Machine** from the list of available roles, and then click **Next**. A list of VMs that are not configured will be shown.
    d. Select all the VMs. Click **Next** and then click **Next** again on the confirmation page to start the configuration task.
12. Once you have relocated all VMs, upgrade the remaining RDVH servers. Use the above steps for balancing VM locations as appropriate.

> **NOTE**
> Heterogeneous Hyper-V servers in a cluster are not supported.

Deploy your Remote Desktop environment

9/27/2019 • 5 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

Use the following steps to deploy the Remote Desktop servers in your environment. You can install the server roles on physical machines or virtual machines, depending on whether you are creating an on-premises, cloud-based, or hybrid environment.

If you are using virtual machines for any of the Remote Desktop Services servers, make sure you have prepared those virtual machines.

1. Add all the servers you're going to use for Remote Desktop Services to Server Manager:
    a. In Server Manager, click **Manage** > **Add Servers**.
    b. Click **Find Now**.
    c. Click each server in the deployment (for example, Contoso-Cb1, Contoso-WebGw1, and Contoso-Sh1) and click **OK**.
2. Create a session-based deployment to deploy the Remote Desktop Services components:
    a. In Server Manager, click **Manage** > **Add Roles and Features**.
    b. Click **Remote Desktop Services installation**, **Standard Deployment**, and **Session-based desktop deployment**.
    c. Select the appropriate servers for the RD Connection Broker server, RD Web Access server, and RD Session Host server (for example, Contoso-Cb1, Contoso-WebGw1, and Contoso-SH1, respectively).
    d. Select **Restart the destination server automatically if required**, and then click **Deploy**.
    e. Wait for the deployment to complete successfully
3. Add RD License Server:
    a. In Server Manager, click **Remote Desktop Services > Overview > +RD Licensing**.
    b. Select the virtual machine where the RD license server will be installed (for example, Contoso-Cb1).
    c. Click **Next**, and then click **Add**.
4. Activate the RD License Server and add it to the License Servers group:
    a. In Server Manager, click **Tools > Terminal Services > Remote Desktop Licensing Manager**.
    b. In RD Licensing Manager, select the server, and then click **Action > Activate Server**.
    c. Accept the default values in the Activate Server Wizard. Continue accepting default values until you reach the **Company information** page. Then, enter your company information.
    d. Accept the defaults for the remaining pages until the final page. Clear **Start Install Licenses Wizard now**, and then click **Finish**.
    e. Click **Action > Review Configuration > Add to Group > OK**. Enter credentials for a user in the AAD DC Administrators group, and register as SCP. This step might not work if you are using Azure AD Domain Services, but you can ignore any warnings or errors.
5. Add the RD Gateway server and certificate name:
    a. In Server Manager, click **Remote Desktop Services > Overview > + RD Gateway**.
    b. In the Add RD Gateway Servers wizard, select the virtual machine where you want to install the RD Gateway server (for example, Contoso-WebGw1).
    c. Enter the SSL certificate name for the RD Gateway server using the external fully qualified DNS Name

(FQDN) of the RD Gateway server. In Azure, this is the **DNS name** label and uses the format servicename.location.cloudapp.azure.com. For example, contoso.westus.cloudapp.azure.com.

d. Click **Next**, and then click **Add**.

6. Create and install self-signed certificates for the RD Gateway and RD Connection Broker servers.

> **NOTE**
> If you are providing and installing certificates from a trusted certificate authority, perform the procedures from step h to step k for each role. You will need to have the .pfx file available for each of these certificates.

a. In Server Manager, click **Remote Desktop Services > Overview > Tasks > Edit Deployment Properties**.

b. Expand **Certificates**, and then scroll down to the table. Click **RD Gateway > Create new certificate**.

c. Enter the certificate name, using the external FQDN of the RD Gateway server (for example, contoso.westus.cloudapp.azure.com) and then enter the password.

d. Select **Store this certificate** and then browse to the shared folder you created for certificates in a previous step. (For example,\Contoso-Cb1\Certificates.)

e. Enter a file name for the certificate (for example, ContosoRdGwCert), and then click **Save**.

f. Select **Allow the certificate to be added to the Trusted Root Certificate Authorities certificate store on the destination computers**, and then click **OK**.

g. Click **Apply**, and then wait for the certificate to be successfully applied to the RD Gateway server.

h. Click **RD Web Access > Select existing certificate**.

i. Browse to the certificate created for the RD Gateway server (for example, ContosoRdGwCert), and then click **Open**.

j. Enter the password for the certificate, select **Allow the certificate to be added to the Trusted Root Certificate store on the destination computers**, and then click **OK**.

k. Click **Apply**, and then wait for the certificate to be successfully applied to the RD Web Access server.

l. Repeat substeps 1-11 for the **RD Connection Broker - Enable Single Sign On** and **RD Connection Broker - Publishing services**, using the internal FQDN of the RD Connection Broker server for the new certificate's name (for example, Contoso-Cb1.Contoso.com).

7. Export self-signed public certificates and copy them to a client computer. If you are using certificates from a trusted certificate authority, you can skip this step.

a. Launch certlm.msc.

b. Expand **Personal**, and then click **Certificates**.

c. In the right-hand pane right-click the RD Connection Broker certificate intended for client authentication, for example **Contoso-Cb1.Contoso.com**.

d. Click **All Tasks > Export**.

e. Accept the default options in the Certificate Export Wizard accept defaults until you reach the **File to Export** page.

f. Browse to the shared folder you created for certificates, for example \Contoso-Cb1\Certificates.

g. Enter a File name, for example ContosoCbClientCert, and then click **Save**.

h. Click **Next**, and then click **Finish**.

i. Repeat substeps 1-8 for the RD Gateway and Web certificate, (for example contoso.westus.cloudapp.azure.com), giving the exported certificate an appropriate file name, for example **ContosoWebGwClientCert**.

j. In File Explorer, navigate to the folder where the certificates are stored, for example \Contoso-Cb1\Certificates.

k. Select the two exported client certificates, then right-click them, and click **Copy**.

l. Paste the certifcates on the local client computer.

8. Configure the RD Gateway and RD Licensing deployment properties:

   a. In Server Manager, click **Remote Desktop Services > Overview > Tasks > Edit Deployment Properties**.
   b. Expand **RD Gateway** and clear the **Bypass RD Gateway server for local addresses** option.
   c. Expand **RD licensing** and select **Per User**
   d. Click **OK**.

9. Create a session collection. These steps create a basic collection. Check out Create a Remote Desktop Services collection for desktops and apps to run for more information about collections.

   a. In Server Manager, click **Remote Desktop Services > Collections > Tasks > Create Session Collection**.
   b. Enter a collection Name (for example, ContosoDesktop).
   c. Select an RD Session Host Server (Contoso-Sh1), accept the default user groups (Contoso\Domain Users), and enter the Universal Naming Convention (UNC) Path to the user profile disks created above (\Contoso-Cb1\UserDisks).
   d. Set a Maximum size, and then click **Create**.

You've now created a basic Remote Desktop Services infrastructure. If you need to create a highly-available deployment, you can add a connection broker cluster or a second RD Session Host server.

Create a Remote Desktop Services collection for desktops and apps to run

10/23/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

Use the following steps to create a Remote Desktop Services session collection. A session collection holds the apps and desktops you want to make available to users. After you create the collection, publish it so users can access it.

Before you create a collection, you need to decide what kind of collection you need: pooled desktop sessions or personal desktop sessions.

- **Use pooled desktop sessions for session-based virtualization**: Leverage the compute power of Windows Server to provide a cost-effective multi-session environment to drive your users' everyday workloads
- **Use personal desktop sessions for to create a virtual desktop infrastructure (VDI)**: Leverage Windows client to provide the high performance, app compatibility, and familiarity that your users have come to expect of their Windows desktop experience.

With a pooled session, multiple users access a shared pool of resources, while with a personal desktop session, users are assigned their own desktop from within the pool. The pooled session provides lower overall cost, while personal sessions enable users to customize their desktop experience.

If you need to share graphics-intensive hosted applications, you can combine personal session desktops with the new Discrete Device Assignment (DDA) capability to also provide support for hosted applications that require accelerated graphics. Check out Which graphics virtualization technology is right for you for more information.

Regardless of the type of collection you choose, you'll populate those collections with RemoteApps - programs and resources that users can access from any supported device and work with as though the program was running locally.

Create a pooled desktop session collection

1. In Server Manager, click **Remote Desktop Services > Collections > Tasks > Create Session Collections**.
2. Enter a name for the collection, for example **ContosoAps**.
3. Select the RD Session Host server you created (for example, Contoso-Shr1).
4. Accept the default **User Groups**.
5. Enter the location of the file share you created for the user profile disks for this collection (for example, **\Contoso-Cb1\UserDisksr**).
6. Click **Create**. When the collection is created, click **Close**.

Create a personal desktop session collection

Use the New-RDSessionCollection cmdlet to create a personal session desktop collection. The following three parameters provide the configuration information required for personal session desktops:

- **-PersonalUnmanaged** - Specifies the type of session collection that lets you assign users to a personal session host server. If you don't specify this parameter, then the collection is created as a traditional RD Session Host collection, where users are assigned to the next available session host when they sign in.

- **-GrantAdministrativePrivilege** - If you use **-PersonalUnmanaged**, specifies that the user assigned to the session host be given administrative privileges. If you don't use this parameter, users are granted only standard user privileges.
- **-AutoAssignUser** - If you use **-PersonalUnmanaged**, specifies that new users connecting through the RD Connection Broker are automatically assigned to an unassigned session host. If there are no unassigned session hosts in the collection, the user will see an error message. If you don't use this parameter, you have to manually assign users to a session host before they sign in.

You can use PowerShell cmdlets to manage your personal desktop session collections. See Manage your personal desktop session collections for more information.

Publish RemoteApp programs

Use the following steps to publish the apps and resources in your collection:

1. In Server Manager, select the new collection (**ContosoApps**).
2. Under RemoteApp Programs, click **Publish RemoteApp programs**.
3. Select the programs you want to publish, and then click **Publish**.

Set up the Remote Desktop web client for your users

1/14/2020 • 12 minutes to read • Edit Online

The Remote Desktop web client lets users access your organization's Remote Desktop infrastructure through a compatible web browser. They'll be able to interact with remote apps or desktops like they would with a local PC no matter where they are. Once you set up your Remote Desktop web client, all your users need to get started is the URL where they can access the client, their credentials, and a supported web browser.

> **IMPORTANT**
> The web client does not currently support using Azure Application Proxy and does not support Web Application Proxy at all. See Using RDS with application proxy services for details.

What you'll need to set up the web client

Before getting started, keep the following things in mind:

- Make sure your Remote Desktop deployment has an RD Gateway, an RD Connection Broker, and RD Web Access running on Windows Server 2016 or 2019.
- Make sure your deployment is configured for per-user client access licenses (CALs) instead of per-device, otherwise all licenses will be consumed.
- Install the Windows 10 KB4025334 update on the RD Gateway. Later cumulative updates may already contains this KB.
- Make sure public trusted certificates are configured for the RD Gateway and RD Web Access roles.
- Make sure that any computers your users will connect to are running one of the following OS versions:
  - Windows 10
  - Windows Server 2008R2 or later

Your users will see better performance connecting to Windows Server 2016 (or later) and Windows 10 (version 1611 or later).

> **IMPORTANT**
> If you used the web client during the preview period and installed a version prior to 1.0.0, you must first uninstall the old client before moving to the new version. If you receive an error that says "The web client was installed using an older version of RDWebClientManagement and must first be removed before deploying the new version," follow these steps:
>
> 1. Open an elevated PowerShell prompt.
> 2. Run **Uninstall-Module RDWebClientManagement** to uninstall the new module.
> 3. Close and reopen the elevated PowerShell prompt.
> 4. Run **Install-Module RDWebClientManagement -RequiredVersion <old version> to install the old module.**
> 5. Run **Uninstall-RDWebClient** to uninstall the old web client.
> 6. Run **Uninstall-Module RDWebClientManagement** to uninstall the old module.
> 7. Close and reopen the elevated PowerShell prompt.
> 8. Proceed with the normal installation steps as follows.

How to publish the Remote Desktop web client

To install the web client for the first time, follow these steps:

1. On the RD Connection Broker server, obtain the certificate used for Remote Desktop connections and export it as a .cer file. Copy the .cer file from the RD Connection Broker to the server running the RD Web role.
2. On the RD Web Access server, open an elevated PowerShell prompt.
3. On Windows Server 2016, update the PowerShellGet module since the inbox version doesn't support installing the web client management module. To update PowerShellGet, run the following cmdlet:

   ```
   Install-Module -Name PowerShellGet -Force
   ```

   > **IMPORTANT**
   > You'll need to restart PowerShell before the update can take effect, otherwise the module may not work.

4. Install the Remote Desktop web client management PowerShell module from the PowerShell gallery with this cmdlet:

   ```
   Install-Module -Name RDWebClientManagement
   ```

5. After that, run the following cmdlet to download the latest version of the Remote Desktop web client:

   ```
   Install-RDWebClientPackage
   ```

6. Next, run this cmdlet with the bracketed value replaced with the path of the .cer file that you copied from the RD Broker:

   ```
   Import-RDWebClientBrokerCert <.cer file path>
   ```

7. Finally, run this cmdlet to publish the Remote Desktop web client:

   ```
   Publish-RDWebClientPackage -Type Production -Latest
   ```

   Make sure you can access the web client at the web client URL with your server name, formatted as https://server_FQDN/RDWeb/webclient/index.html. It's important to use the server name that matches the RD Web Access public certificate in the URL (typically the server FQDN).

   > **NOTE**
   > When running the **Publish-RDWebClientPackage** cmdlet, you may see a warning that says per-device CALs are not supported, even if your deployment is configured for per-user CALs. If your deployment uses per-user CALs, you can ignore this warning. We display it to make sure you're aware of the configuration limitation.

8. When you're ready for users to access the web client, just send them the web client URL you created.

NOTE

To see a list of all supported cmdlets for the RDWebClientManagement module, run the following cmdlet in PowerShell:

```
Get-Command -Module RDWebClientManagement
```

How to update the Remote Desktop web client

When a new version of the Remote Desktop web client is available, follow these steps to update the deployment with the new client:

1. Open an elevated PowerShell prompt on the RD Web Access server and run the following cmdlet to download the latest available version of the web client:

   ```
   Install-RDWebClientPackage
   ```

2. Optionally, you can publish the client for testing before official release by running this cmdlet:

   ```
   Publish-RDWebClientPackage -Type Test -Latest
   ```

   The client should appear on the test URL that corresponds to your web client URL (for example, https://server_FQDN/RDWeb/webclient-test/index.html).

3. Publish the client for users by running the following cmdlet:

   ```
   Publish-RDWebClientPackage -Type Production -Latest
   ```

   This will replace the client for all users when they relaunch the web page.

How to uninstall the Remote Desktop web client

To remove all traces of the web client, follow these steps:

1. On the RD Web Access server, open an elevated PowerShell prompt.
2. Unpublish the Test and Production clients, uninstall all local packages and remove the web client settings:

   ```
   Uninstall-RDWebClient
   ```

3. Uninstall the Remote Desktop web client management PowerShell module:

   ```
   Uninstall-Module -Name RDWebClientManagement
   ```

How to install the Remote Desktop web client without an internet connection

Follow these steps to deploy the web client to an RD Web Access server that doesn't have an internet connection.

> **NOTE**
> Installing without an internet connection is available in version 1.0.1 and above of the RDWebClientManagement PowerShell module.

> **NOTE**
> You still need an admin PC with internet access to download the necessary files before transferring them to the offline server.

> **NOTE**
> The end-user PC needs an internet connection for now. This will be addressed in a future release of the client to provide a complete offline scenario.

From a device with internet access

1. Open a PowerShell prompt.
2. Import the Remote Desktop web client management PowerShell module from the PowerShell gallery:

```
Import-Module -Name RDWebClientManagement
```

3. Download the latest version of the Remote Desktop web client for installation on a different device:

```
Save-RDWebClientPackage "C:\WebClient\"
```

4. Download the latest version of the RDWebClientManagement PowerShell module:

```
Find-Module -Name "RDWebClientManagement" -Repository "PSGallery" | Save-Module -Path "C:\WebClient\"
```

5. Copy the content of "C:\WebClient" to the RD Web Access server.

From the RD Web Access server

Follow the instructions under How to publish the Remote Desktop web client, replacing steps 4 and 5 with the following.

4. Import the Remote Desktop web client management PowerShell module from the local folder:

```
Import-Module -Name "C:\WebClient\"
```

5. Deploy the latest version of the Remote Desktop web client from the local folder (replace with the appropriate zip file):

```
Install-RDWebClientPackage -Source "C:\WebClient\rdwebclient-1.0.1.zip"
```

Connecting to RD Broker without RD Gateway in Windows Server 2019

This section describes how to enable a web client connection to an RD Broker without an RD Gateway in Windows Server 2019.

Setting up the RD Broker server

Follow these steps if there is no certificate bound to the RD Broker server

1. Open **Server Manager** > **Remote Desktop Services**.
2. In **Deployment Overview** section, select the **Tasks** dropdown menu.
3. Select **Edit Deployment Properties**, a new window titled **Deployment Properties** will open.
4. In the **Deployment Properties** window, select **Certificates** in the left menu.
5. In the list of Certificate Levels, select **RD Connection Broker - Enable Single Sign On**. You have two options: (1) create a new certificate or (2) an existing certificate.

Follow these steps if there is a certificate previously bound to the RD Broker server

1. Open the certificate bound to the Broker and copy the **Thumbprint** value.
2. To bind this certificate to the secure port 3392, open an elevated PowerShell window and run the following command, replacing **"< thumbprint >"** with the value copied from the previous step:

   ```
   netsh http add sslcert ipport=0.0.0.0:3392 certhash="<thumbprint>" certstorename="Remote Desktop"
   appid="{00000000-0000-0000-0000-000000000000}"
   ```

   > **NOTE**
   >
   > To check if the certificate has been bound correctly, run the following command:
   >
   > ```
   > netsh http show sslcert
   > ```
   >
   > In the list of SSL Certificate bindings, ensure that the correct certificate is bound to port 3392.

3. Open the Windows Registry (regedit) and nagivate to `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp` and locate the key **WebSocketURI**. The value must be set to **https://+:3392/rdp/**.

Setting up the RD Session Host

Follow these steps if the RD Session Host server is different from the RD Broker server:

1. Create a certificate for the RD Session Host machine, open it and copy the **Thumbprint** value.
2. To bind this certificate to the secure port 3392, open an elevated PowerShell window and run the following command, replacing **"< thumbprint >"** with the value copied from the previous step:

   ```
   netsh http add sslcert ipport=0.0.0.0:3392 certhash="<thumbprint>" appid="{00000000-0000-0000-0000-
   000000000000}"
   ```

   > **NOTE**
   >
   > To check if the certificate has been bound correctly, run the following command:
   >
   > ```
   > netsh http show sslcert
   > ```
   >
   > In the list of SSL Certificate bindings, ensure that the correct certificate is bound to port 3392.

3. Open the Windows Registry (regedit) and nagivate to

`HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp` and locate the key **WebSocketURI**. The value must be set to https://+:3392/rdp/.

General Observations

- Ensure that both the RD Session Host and RD Broker server are running Windows Server 2019.
- Ensure that public trusted certificates are configured for both the RD Session Host and RD Broker server.

> **NOTE**
> If both the RD Session Host and the RD Broker server share the same machine, set the RD Broker server certificate only. If the RD Session Host and RD Broker server use different machines, both must be configured with unique certificates.

- The **Subject Alternative Name (SAN)** for each certificate must be set to the machine's **Fully Qualified Domain Name (FQDN)**. The **Common Name (CN)** must match the SAN for each certificate.

How to pre-configure settings for Remote Desktop web client users

This section will tell you how to use PowerShell to configure settings for your Remote Desktop web client deployment. These PowerShell cmdlets control a user's ability to change settings based on your organization's security concerns or intended workflow. The following settings are all located in the **Settings** side panel of the web client.

Suppress telemetry

By default, users may choose to enable or disable collection of telemetry data that is sent to Microsoft. For information about the telemetry data Microsoft collects, please refer to our Privacy Statement via the link in the **About** side panel.

As an administrator, you can choose to suppress telemetry collection for your deployment using the following PowerShell cmdlet:

```
Set-RDWebClientDeploymentSetting -Name "SuppressTelemetry" $true
```

By default, the user may select to enable or disable telemetry. A boolean value **$false** will match the default client behavior. A boolean value **$true** disables telemetry and restricts the user from enabling telemetry.

Remote resource launch method

> **NOTE**
> This setting currently only works with the RDS web client, not the Windows Virtual Desktop web client.

By default, users may choose to launch remote resources (1) in the browser or (2) by downloading an .rdp file to handle with another client installed on their machine. As an administrator, you can choose to restrict the remote resource launch method for your deployment with the following Powershell command:

```
Set-RDWebClientDeploymentSetting -Name "LaunchResourceInBrowser" ($true|$false)
```

By default, the user may select either launch method. A boolean value **$true** will force the user to launch resources in the browser. A boolean value **$false** will force the user to launch resources by downloading an .rdp file to handle with a locally installed RDP client.

Reset RDWebClientDeploymentSetting configurations to default

To reset a deployment-level web client setting to the default configuration, run the following PowerShell cmdlet and use the -name parameter to specify the setting you want to reset:

```
Reset-RDWebClientDeploymentSetting -Name "LaunchResourceInBrowser"
Reset-RDWebClientDeploymentSetting -Name "SuppressTelemetry"
```

Troubleshooting

If a user reports any of the following issues when opening the web client for the first time, the following sections will tell you what to do to fix them.

What to do if the user's browser shows a security warning when they try to access the web client

The RD Web Access role might not be using a trusted certificate. Make sure the RD Web Access role is configured with a publicly trusted certificate.

If that doesn't work, your server name in the web client URL might not match the name provided by the RD Web certificate. Make sure your URL uses the FQDN of the server hosting the RD Web role.

What to do if the user can't connect to a resource with the web client even though they can see the items under All Resources

If the user reports that they can't connect with the web client even though they can see the resources listed, check the following things:

- Is the RD Gateway role properly configured to use a trusted public certificate?
- Does the RD Gateway server have the required updates installed? Make sure that your server has the KB4025334 update installed.

If the user gets an "unexpected server authentication certificate was received" error message when they try to connect, then the message will show the certificate's thumbprint. Search the RD Broker server's certificate manager using that thumbprint to find the right certificate. Verify that the certificate is configured to be used for the RD Broker role in the Remote Desktop deployment properties page. After making sure the certificate hasn't expired, copy the certificate in .cer file format to the RD Web Access server and run the following command on the RD Web Access server with the bracketed value replaced by the certificate's file path:

```
Import-RDWebClientBrokerCert <certificate file path>
```

Diagnose issues with the console log

If you can't solve the issue based on the troubleshooting instructions in this article, you can try to diagnose the source of the problem yourself by watching the console log in the browser. The web client provides a method for recording the browser console log activity while using the web client to help diagnose issues.

- Select the ellipsis in the upper-right corner and navigate to the **About** page in the dropdown menu.
- Under **Capture support information** select the **Start recording** button.
- Perform the operation(s) in the web client that produced the issue you are trying to diagnose.
- Navigate to the **About** page and select **Stop recording**.
- Your browser will automatically download a .txt file titled **RD Console Logs.txt**. This file will contain the full console log activity generated while reproducing the target issue.

The console may also be accessed directly through your browser. The console is generally located under the developer tools. For example, you can access the log in Microsoft Edge by pressing the **F12** key, or by selecting the ellipsis, then navigating to **More tools** > **Developer Tools**.

Get help with the web client

If you've encountered an issue that can't be solved by the information in this article, you can report it on Tech Community. You can also request or vote for new features at our suggestion box.

Set up email discovery to subscribe to your RDS feed

9/27/2019 • 2 minutes to read • Edit Online

Have you ever had trouble getting your end users connected to their published RDS feed, either because of a single missing character in the feed URL or because they lost the email with the URL? Nearly all Remote Desktop client applications support finding your subscription by entering your email address, making it easier than ever to get your users connected to their RemoteApps and desktops.

> **IMPORTANT**
> The Microsoft Remote Desktop app in the Microsoft Store does not support email address subscription at this time.

Before you set up email discovery, do the following:

- Make sure you have permission to add a TXT record to the domain associated with your email (for example, if your users have @contoso.com email addresses, you would need permissions for the contoso.com domain)
- Create an RD Web feed URL (https://<rdweb-dns-name>.domain/RDWeb/Feed/webfeed.aspx, such as https://rdweb.contoso.com/RDWeb/Feed/webfeed.aspx)

Now, use these steps to set up email discovery:

1. In your browser, connect to the website of the domain name registrar where your domain is registered.
2. Navigate to the appropriate page for your registered domain where you can view, add, and edit DNS records.
3. Enter a new DNS record with the following properties:

   - **Host:** _msradc
   - **Text:** <RD Web Feed URL>
   - **TTL:** 300

   The names of the DNS records fields vary by domain name registrar, but this process will result in a TXT record named _msradc.<domain_name> (such as _msradc.contoso.com) that has a value of the full RD Web feed.

That's it! Now, launch the Remote Desktop application on your device and subscribe yourself!

License your RDS deployment with client access licenses (CALs)

9/27/2019 • 3 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

Each user and device that connects to a Remote Desktop Session host needs a client access licenses (CAL). You use RD Licensing to install, issue, and track RDS CALs.

When a user or a device connects to an RD Session Host server, the RD Session Host server determines if an RDS CAL is needed. The RD Session Host server then requests an RDS CAL from the Remote Desktop license server. If an appropriate RDS CAL is available from a license server, the RDS CAL is issued to the client, and the client is able to connect to the RD Session Host server and from there to the desktop or apps they're trying to use.

Although there is a licensing grace period during which no license server is required, after the grace period ends, clients must have a valid RDS CAL issued by a license server before they can log on to an RD Session Host server.

Use the following information to learn about how client access licensing works in Remote Desktop Services and to deploy and manage your licenses:

- License your RDS deployment with client access licenses (CALs)
  - Understanding the CALs model
  - Note about CAL versions

Understanding the CALs model

There are two types of CALs:

- RDS Per Device CALs
- RDS Per User CALs

The following table outlines the differences between the two types of CALs:

PER DEVICE	PER USER
CALs are physically assigned to each device.	CALs are assigned to a user in Active Directory.
CALs are tracked by the license server.	CALs are tracked by the license server.
CALs can be tracked regardless of Active Directory membership.	CALs cannot be tracked within a workgroup.
You can revoke up to 20% of CALs.	You cannot revoke any CALs.
Temporary CALs are valid for 52–89 days.	Temporary CALs are not available.
CALs cannot be overallocated.	CALs can be overallocated (in breach of the Remote Desktop licensing agreement).

When you use the Per Device model, a temporary license is issued the first time a device connects to the RD Session Host. The second time that device connects, as long as the license server is activated and there are available CALs, the license server issues a permanent RDS Per Device CAL.

When you use the Per User model, licensing is not enforced and each user is granted a license to connect to an RD Session Host from any number of devices. The license server issues licenses from the available CAL pool or the Over-Used CAL pool. It's your responsibility to ensure that all of your users have a valid license and zero Over-Used CALs—otherwise, you're in violation of the Remote Desktop Services license terms.

To ensure you are in compliance with the Remote Destkop Services license terms, track the number of RDS Per User CALs used in your organization and be sure to have a enough Per User CALs installed on the license server for all of your users.

You can use the Remote Desktop Licensing Manager to track and generate reports on RDS Per User CALs.

Note about CAL versions

The CAL used by users or devices must correspond to the version of Windows Server that the user or device is connecting to. You can't use older CALs to access newer Windows Server versions, but you can use newer CALs to access earlier versions of Windows Server.

The following table shows the CALs that are compatible on RD Session Hosts and RD Virtualization Hosts.

	2008 R2 AND EARLIER CAL	2012 CAL	2016 CAL	2019 CAL
2008, 2008 R2 license server	Yes	No	No	No
2012 license server	Yes	Yes	No	No
2012 R2 license server	Yes	Yes	No	No
2016 license server	Yes	Yes	Yes	No
2019 license server	Yes	Yes	Yes	Yes

Any RDS license server can host licenses from all previous versions of Remote Desktop Services and the current version of Remote Desktop Services. For example, a Windows Server 2016 RDS license server can host licenses from all previous versions of RDS, while a Windows Server 2012 R2 RDS license server can only host licenses up to Windows Server 2012 R2.

Activate the Remote Desktop Services license server

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

The Remote Desktop Services license server issues client access licenses (CALs) to users and devices when they access the RD Session Host. You can activate the license server by using the Remote Desktop Licensing Manager.

Install the RD Licensing role

1. Sign into the server you want to use as the license server using an administrator account.
2. In Server Manager, click **Roles Summary**, and then click **Add Roles**. Click **Next** on the first page of the roles wizard.
3. Select **Remote Desktop Services**, and then click **Next**, and then **Next** on the Remote Desktop Services page.
4. Select **Remote Desktop Licensing**, and then click **Next**.
5. Configure the domain - select **Configure a discovery scope for this license server**, click **This domain**, and then click **Next**.
6. Click **Install**.

Activate the license server

1. Open the Remote Desktop Licensing Manager: click **Start > Administrative Tools > Remote Desktop Services > Remote Desktop Licensing Manager**.
2. Right-click the license server, and then click **Activate Server**.
3. Click **Next** on the welcome page.
4. For the connection method, select **Automatic connection (recommended)**, and then click **Next**.
5. Enter your company information (your name, the company name, your geographic region), and then click **Next**.
6. Optionally enter any other company information (for example, email and company addresses), and then click **Next**.
7. Make sure that **Start Install Licenses Wizard now** is not selected (we'll install the licenses in a later step), and then click **Next**.

Your license server is now ready to start issuing and managing licenses.

Install RDS client access licenses on the Remote Desktop license server

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

Use the following information to install Remote Desktop Services client access licenses (CALs) on the license server. Once the CALs are installed, the license server will issue them to users as appropriate.

Note you need Internet connectivity on the computer running Remote Desktop Licensing Manager but not on the computer running the license server.

1. On the license server (usually the first RD Connection Broker), open the Remote Desktop Licensing Manager.
2. Right-click the license server, and then click **Install licenses**.
3. Click **Next** on the welcome page.
4. Select the program you purchased your RDS CALs from, and then click **Next**. If you are a service provider, select **Service Provider License Agreement**.
5. Enter the information for your license program. In most cases, this will be the license code or an agreement number, but this varies depending on the license program you're using.
6. Click **Next**.
7. Select the product version, license type, and number of licenses for your environment, and then click **Next**. The license manager contacts the Microsoft Clearinghouse to validate and retrieve your licenses.
8. Click **Finish** to complete the process.

Track your Remote Desktop Services client access licenses (RDS CALs)

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

You can use the Remote Desktop Licensing Manager tool to create reports to track the RDS Per User CALs that have been issued by a Remote Desktop license server.

> **NOTE**
> If you are using Azure AD Domain Services in your environment, the Remote Desktop Licensing Manager tool won't work to obtain Per User CALs. Instead, you need to track licensing manually, either through logon events, polling active Remote Desktop connections through the Connection Broker, or another mechanism that works for you.

Use the following steps to generate a per User CALs report:

1. In Remote Desktop Licensing Manager right-click the license server, click **Create Report**, and then click **Per User CAL Usage**.
2. Set the scope for the report - select one of the following:
   - Entire domain - the domain in which the license server is a member.
   - Organizational Unit - Any OU within the domain in which the license server is a member.
   - Entire domain and all trusted domains - Can include domains in other forests. Selecting this option can increase the time that it takes to create the report.

   The selection that you make determines which user accounts in AD DS are searched for RDS Per User CAL information to generate the report.
3. Click **Create Report**. The report is created and a message appears to confirm that the report was successfully created. Click **OK** to close the message.

The report that you created appears in the Reports section under the node for the license server. The report provides the following information:

- Date and time the report was created
- The scope of the report (e.g., Domain, OU=Sales, or All trusted domains)
- The number of RDS Per User CALs that are installed on the license server
- The number of RDS Per User CALs that have been issued by the license server specific to the scope of the report

You can also save the report as a CSV file to a folder location on the computer. To save the report, right-click the report that you want to save, click Save As, and then specify the file name and location to save the report.

Reports that you create are listed in the Reports node under the node for the license server in Remote Desktop Licensing Manager. If you no longer need a report, you can delete it.

Remote Desktop Services - Integrating with Azure services

9/27/2019 • 2 minutes to read • Edit Online

Windows Server 2016 combines the powerful secure delivery of desktops and apps through Remote Desktop Services with the flexible, scalable services provided by Microsoft Azure. You can deploy RDS with Azure services to help reduce infrastructure maintenance cost for on-premises servers, increase stability by using Azure services to ensure high availability, improve security by using Multi-factor Authentication, and improve your users' experience by using existing identities to access resources in RDS.

Use the following information to integrate Azure into your Remote Desktop deployment:

- Learn how to use Multi-factor Authentication with RDS
- Integrate Azure AD Domain Services with your RDS deployment
- Publish Remote Desktop with Azure AD Application Proxy

To see how these services simplify the architecture of your Remote Desktop deployment, check out RDS architectures with unique Azure PaaS roles.

Integrate Azure AD Domain Services with your RDS deployment

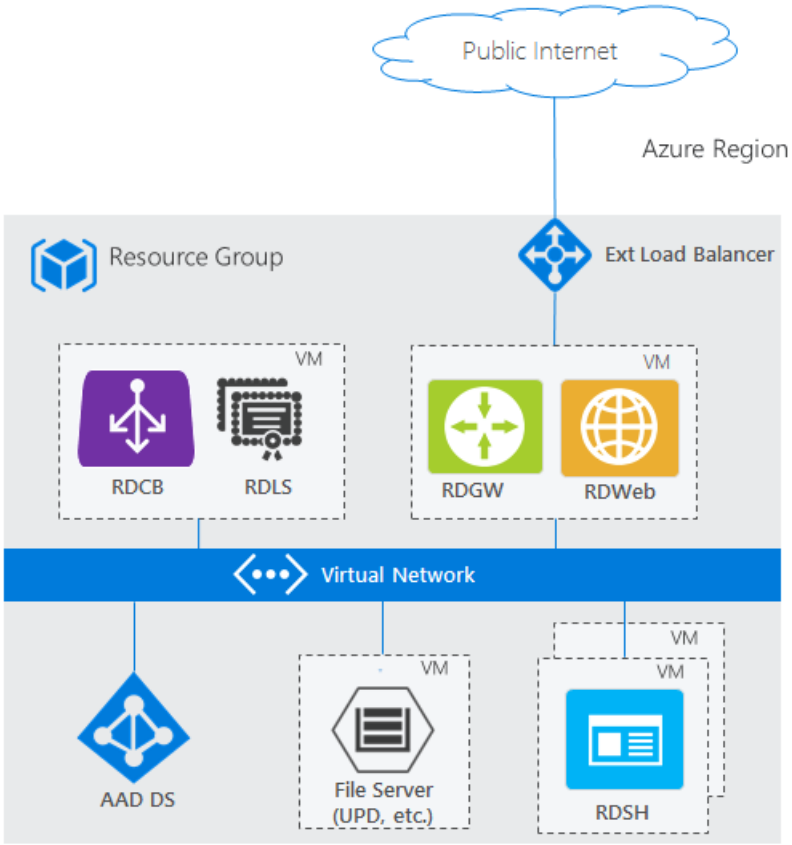
9/27/2019 • 2 minutes to read • Edit Online

You can use Azure AD Domain Services (Azure AD DS) in your Remote Desktop Services deployment in the place of Windows Server Active Directory. Azure AD DS lets you use your existing Azure AD identities in with classic Windows workloads.

With Azure AD DS you can:

- Create an Azure environment with a local domain for born-in-the-cloud organizations.
- Create an isolated Azure environment with the same identities used for your on-premises and online environment, without needing to create a site-to-site VPN or ExpressRoute.

When you finish integrating Azure AD DS into your Remote Desktop deployment, your architecture will look something like this:



To see how this architecture compares with other RDS deployment scenarios, check out Remote Desktop Services architectures.

To get a better understanding of Azure AD DS, check out the Azure AD DS overview and How to decide if Azure AD DS is right for your use-case.

Use the following information to deploy Azure AD DS with RDS.

Prerequisites

Before you can bring your identities from Azure AD to use in an RDS deployment, configure Azure AD to save the hashed passwords for your users' identities. Born-in-the-cloud organizations don't need to make any additional changes in their directory; however, on-premises organizations need to allow password hashes to be synchronized and stored in Azure AD, which may not be permissible to some organizations. Users will have to reset their passwords after making this configuration change.

Deploy Azure AD DS and RDS

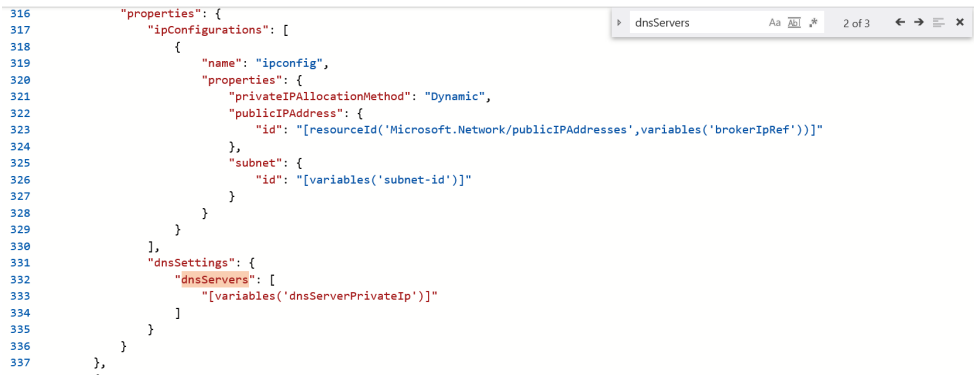
Use the following steps to deploy Azure AD DS and RDS.

1. Enable Azure AD DS. Note that the linked article does the following:
   - Walk through creating the appropriate Azure AD groups for domain administration.
   - Highlight when you might have to force users to change their password so their accounts can work with Azure AD DS.
2. Set up RDS. You can either use an Azure template or deploy RDS manually.
   - Use the Existing AD template. Make sure to customize the following:
     - **Settings**
       - **Resource group**: Use the resource group where you want to create the RDS resources.

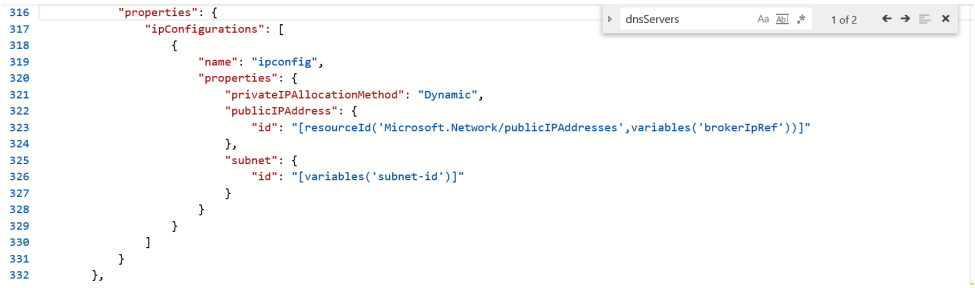
         > **NOTE**
         > Right now this has to be the same resource group where the Azure resource manager virtual network exists.

       - **Dns Label Prefix**: Enter the URL that you want users to use to access RD Web.
       - **Ad Domain Name**: Enter the full name of your Azure AD instance, for example, "contoso.onmicrosoft.com" or "contoso.com".
       - **Ad Vnet Name** and **Ad Subnet Name**: Enter the same values that you used when you created the Azure resource manager virtual network. This is the subnet to which the RDS resources will connect.
       - **Admin Username** and **Admin Password**: Enter the credentials for an admin user that's a member of the **AAD DC Administrators** group in Azure AD.
     - **Template**
       - Remove all properties of **dnsServers**: after selecting **Edit template** from the Azure quickstart template page, search for "dnsServers" and remove the property.

         For example, before removing the **dnsServers** property:



And here's the same file after removing the property:



- Deploy RDS manually.

Scale out your Remote Desktop Services deployment by adding an RD Session Host farm

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

You can improve the availability and scale of your RDS deployment by adding a Remote Desktop Session Host (RDSH) farm.

Use the following steps to add another RD Sesssion Host to your deployment:

1. Create a server to host the second RD Session Host. If you are using Azure virtual machines, make sure to include the new VM in the same availability set that holds your first RD Session Host.
2. Enable remote management on the new server or virtual machine:
    a. In Server Manager, click **Local Server > Remote management current setting (disabled)**.
    b. Select **Enable remote management for this server**, and then click **OK**.
    c. Optional: You can temporarily set Windows Update to not automatically download and install updates. This helps prevent changes and system restarts while you deploy the RDSH server. In Server Manager, click **Local Server > Windows Update current setting**. Click **Advanced options > Defer upgrades**.
3. Add the server or vm to the domain:
    a. In Server Manager, click **Local Server > Workgroup current setting**.
    b. Click **Change > Domain**, and then enter the domain name (for example, Contoso.com).
    c. Enter the domain administrator credentials.
    d. Restart the server or vm.
4. Add the new RD Session Host to the farm:

    NOTE
    Step 1, creating a public IP address for the RDMS virtual machine, is only necessary if you are using a vm for the RDMS and if it does not already have an IP address assigned.

    a. Create a public IP address for the virtual machine running Remote Desktop Management Services (RDMS). The RDMS virtual machine will typically be the virtual machine running the first instance of the RD Connection Broker role.
        a. In the Azure portal, click **Browse > Resource groups**, click the resource group for the deployment and then click the RDMS virtual machine (for example, Contoso-Cb1).
        b. Click **Settings > Network interfaces**, and then click the corresponding network interface.
        c. Click **Settings > IP address**.
        d. For **Public IP address**, select **Enabled**, and then click **IP address**.
        e. If you have an existing public IP address you want to use, select it from the list. Otherwise, click **Create new**, enter a name, and then click **OK** and then **Save**.
    b. Sign into the RDMS.
    c. Add the new RDSH server to Server Manager:
        a. Launch Server Manager, click **Manage > Add Servers**.

b. In the Add Servers dialog, click **Find Now**.
c. Select the server you want to use for the RD Session Host or the newly created virtual machine (for example, Contoso-Sh2) and click **OK**.

d. Add the RDSH server to the deployment
   a. Launch Server Manager .
   b. Click **Remote Desktop Services > Overview > Deployment Servers > Tasks > Add RD Session Host Servers**.
   c. Select the new server (for example, Contoso-Sh2), and then click **Next**.
   d. On the Confirmation page, select **Restart remote computers as needed**, and then click **Add**.

e. Add RDSH server to the collection farm:
   a. Launch Server Manager.
   b. Click **Remote Desktop Services** and then click the collection to which you want to add the newly created RDSH server (for example, ContosoDesktop).
   c. Under **Host Servers**, click **Tasks > Add RD Session Host Servers**.
   d. Select the newly created server (for example, Contoso-Sh2), and then click **Next**.
   e. On the Confirmation page, click **Add**.

Add the RD Connection Broker server to the deployment and configure high availability

9/27/2019 • 6 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

You can deploy a Remote Desktop Connection Broker (RD Connection Broker) cluster to improve the availability and scale of your Remote Desktop Services infrastructure.

Pre-requisites

Set up a server to act as a second RD Connection Broker—this can be either a physical server or a VM.

Set up a database for the Connection Broker. You can use Azure SQL Database instance or SQL Server in your local environment. We talk about using Azure SQL below, but the steps still apply to SQL Server. You'll need to find the connection string for the database and make sure you have the correct ODBC driver.

Step 1: Configure the database for the Connection Broker

1. Find the connection string for the database you created - you need it both to identify the version of ODBC driver you need and later, when you're configuring the Connection Broker itself (step 3), so save the string someplace where you can reference it easily. Here's how you find the connection string for Azure SQL:
   a. In the Azure portal, click **Browse > Resource groups** and click the resource group for the deployment.
   b. Select the SQL database you just created (for example, CB-DB1).
   c. Click **Settings** > **Properties** > **Show database connection strings**.
   d. Copy the connection string for **ODBC (includes Node.js)**, which should look like this:

```
Driver={SQL Server Native Client 13.0};Server=tcp:cb-
sqls1.database.windows.net,1433;Database=CB-DB1;Uid=sqladmin@contoso;Pwd=
{your_password_here};Encrypt=yes;TrustServerCertificate=no;Connection Timeout=30;
```

   e. Replace "your_password_here" with the actual password. You'll use this entire string, with your included password, when connecting to the database.

2. Install the ODBC driver on the new Connection Broker:
   a. If you are using a VM for the Connection Broker, create a public IP address for the first RD Connection Broker. (You only have to do this if the RDMS virtual machine does not already have a public IP address to allow RDP connections.)
      a. In the Azure portal, click **Browse** > **Resource groups**, click the resource group for the deployment, and then click the first RD Connection Broker virtual machine (for example, Contoso-Cb1).
      b. Click **Settings > Network interfaces**, and then click the corresponding network interface.
      c. Click **Settings > IP address**.
      d. For **Public IP address**, select **Enabled**, and then click **IP address**.
      e. If you have an existing public IP address you want to use, select it from the list. Otherwise, click

Create new, enter a name, and then click **OK** and then **Save**.

b. Connect to the first RD Connection Broker:

   a. In the Azure portal, click **Browse** > **Resource groups**, click the resource group for the deployment, and then click the first RD Connection Broker virtual machine (for example, Contoso-Cb1).

   b. Click **Connect > Open** to open the Remote Desktop client.

   c. In the client, click **Connect**, and then click **Use another user account**. Enter the user name and password for a domain administrator account.

   d. Click **Yes** when warned about the certificate.

c. Download the ODBC driver for SQL Server that matches the version in the ODBC connection string. For the example string above, we need to install the version 13 ODBC driver.

d. Copy the sqlincli.msi file to the first RD Connection Broker server.

e. Open the sqlincli.msi file and install the native client.

f. Repeat steps 1-5 for each additional RD Connection Brokers (for example, Contoso-Cb2).

g. Install the ODBC driver on each server that will run the connection broker.

Step 2: Configure load balancing on the RD Connection Brokers

If you are using Azure infrastructure, you can create an Azure load balancer; if not, you can set up DNS round-robin.

Create a load balancer

1. Create an Azure Load Balancer
   a. In the Azure portal click **Browse > Load balancers > Add**.
   b. Enter a name for the new load balancer (for example, hacb).
   c. Select **Internal** for the **Scheme**, **Virtual Network** for your deployment (for example, Contoso-VNet), and the **Subnet** with all of your resources (for example, default).
   d. Select **Static** for the **IP address assignment** and enter a **Private IP address** that is not currently in use (for example, 10.0.0.32).
   e. Select the appropriate **Subscription**, the **Resource group** with all of your resources, and the appropriate **Location**.
   f. Select **Create**.
2. Create a probe to monitor which servers are active:
   a. In Azure portal, click **Browse > Load Balancers**, and then click the load balancer you just created, (for example, CBLB). Click **Settings**.
   b. Click **Probes > Add**.
   c. Enter a name for the probe (for example, **RDP**), select **TCP** as the **Protocol**, enter **3389** for the **Port**, and then click **OK**.
3. Create the backend pool of the Connection Brokers:
   a. In **Settings**, Click **Backend address pools > Add**.
   b. Enter a name (for example, CBBackendPool), then click **Add a virtual machine**.
   c. Choose an availability set (for example, CbAvSet), and then click **OK**.
   d. Click **Choose the virtual machines**, select each virtual machine, and then click **Select > OK > OK**.
4. Create the RDP load balancing rule:
   a. In **Settings**, click **Load balancing rules**, and then click **Add**.
   b. Enter a name (for example, RDP), select **TCP** for the **Protocol**, enter **3389** for both **Port** and **Backend port**, and click **OK**.
5. Add a DNS record for the Load Balancer:
   a. Connect to the RDMS server virtual machine (for example, Contoso-CB1). Check out the Prepare the

RD Connection Broker VM article for steps on how you connect to the VM.

b. In Server Manager, click **Tools > DNS**.

c. In the left-hand pane, expand **DNS**, click the DNS machine, click **Forward Lookup Zones**, and then click your domain name (for example, Contoso.com). (It might take a few seconds to process the query to the DNS server for the information.)

d. Click **Action > New Host (A or AAAA)**.

e. Enter the name (for example, hacb) and the IP address specified earlier (for example, 10.0.0.32).

Configure DNS round-robin

The following steps are an alternative to creating an Azure Internal Load Balancer.

1. Connect to the RDMS server in the Azure portal. using Remote Desktop Connection client
2. Create DNS records:
   a. In Server Manager, click **Tools > DNS**.
   b. In the left-hand pane, expand **DNS**, click the DNS machine, click **Forward Lookup Zones**, and then click your domain name (for example, Contoso.com). (It might take a few seconds to process the query to the DNS server for the information.)
   c. Click **Action** and **New Host (A or AAAA)**.
   d. Enter the **DNS Name** for the RD Connection Broker cluster (for example, hacb), and then enter the **IP address** of the first RD Connection Broker.
   e. Repeat steps 3-4 for each additional RD Connection Broker, providing each unique IP address for each additional record.

For example, if the IP addresses for the two RD Connection Broker virtual machines are 10.0.0.8 and 10.0.0.9, you would create two DNS host records:

- Host name: hacb.contoso.com , IP address: 10.0.0.8
- Host name: hacb.contoso.com , IP address: 10.0.0.9

Step 3: Configure the Connection Brokers for high availability

1. Add the new RD Connection Broker server to Server Manager:
   a. In Server Manager, click **Manage > Add Servers**.
   b. Click **Find Now**.
   c. Click the newly created RD Connection Broker server (for example, Contoso-Cb2) and click **OK**.
2. Configure high availability for the RD Connection Broker:
   a. In Server Manager, click **Remote Desktop Services > Overview**.
   b. Right-click **RD Connection Broker**, and then click **Configure High Availability**.
   c. Page through the wizard until you get to the Configuration type section. Select **Shared database server**, and then click **Next**.
   d. Enter the DNS name for the RD Connection Broker cluster.
   e. Enter the connection string for the SQL DB, and then page through the wizard to establish high availability.
3. Add the new RD Connection Broker to the deployment
   a. In Server Manager, click **Remote Desktop Services > Overview**.
   b. Right-click the RD Connection Broker, and then click **Add RD Connection Broker Server**.
   c. Page through wizard until you get to Server Selection, then select the newly created RD Connection Broker server (for example, Contoso-CB2).
   d. Complete the wizard, accepting the default values.
4. Configure trusted certificates on RD Connection Broker servers and clients.

Add high availability to the RD Web and Gateway web front

9/27/2019 • 6 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

You can deploy a Remote Desktop Web Access (RD Web Access) and Remote Desktop Gateway (RD Gateway) farm to improve the availability and scale of a Windows Server Remote Desktop Services (RDS) deployment

Use the following steps to add an RD Web and Gateway server to an existing Remote Desktop Services basic deployment.

Pre-requisites

Set up a server to act as an additional RD Web and RD Gateway - this can be either a physical server or VM. This includes joining the server to the domain and enabling remote management.

Step 1: Configure the new server to be part of the RDS environment

1. Connect to the RDMS server in the Azure portal, using Remote Desktop Connection client.
2. Add the new RD Web and Gateway server to Server Manager:
   a. Launch Server Manager, click **Manage > Add Servers**.
   b. In the Add Servers dialog, click **Find Now**.
   c. Select the newly created RD Web and Gateway server (for example, Contoso-WebGw2) and click **OK**.
3. Add RD Web and Gateway servers to the deployment
   a. Launch Server Manager .
   b. Click **Remote Desktop Services > Overview > Deployment Servers > Tasks > Add RD Web Access Servers**.
   c. Select the newly created server (for example, Contoso-WebGw2), and then click **Next**.
   d. On the Confirmation page, select **Restart remote computers as needed**, and then click **Add**.
   e. Repeat these steps to add the RD Gateway server, but choose **RD Gateway Servers** in step b.
4. Re-install certificates for the RD Gateway servers:
   a. In Server Manager on the RDMS server, click **Remote Desktop Services > Overview > Tasks > Edit Deployment Properties**.
   b. Expand **Certificates**.
   c. Scroll down to the table. Click RD **Gateway Role Service > Select existing certificate.**
   d. Click **Choose a different certificate** and then browse to the certificate location. For example, \Contoso-CB1\Certificates). Select the certificate file for the RD Web and Gateway server created during the prerequisites (e.g. ContosoRdGwCert), and then click **Open**.
   e. Enter the password for the certificate, select **Allow the certificate to be added to the Trusted Root Certificate Authorities certificate store on the destination computers**, and then click **OK**.
   f. Click **Apply**.

> **NOTE**
> You may need to manually restart the TSGateway service running on each RD Gateway server, either through Server Manager or Task Manager.

g. Repeat steps a through f for the RD Web Access Role Service.

Step 2: Configure RD Web and RD Gateway properties on the new server

1. Configure the server to be part of an RD Gateway farm:
   a. In Server Manager on the RDMS server, click **All Servers**. Right-click one of the RD Gateway servers, and then click **Remote Desktop Connection**.
   b. Sign into to the RD Gateway server using a domain admin account.
   c. In Server Manager on the RD Gateway server, click **Tools > Remote Desktop Services > RD Gateway Manager**.
   d. In the navigation pane, click the local computer (e.g. Contoso-WebGw1).
   e. Click **Add RD Gateway Server Farm members**.
   f. On the **Server Farm** tab, enter the name of each RD Gateway server, then click **Add** and **Apply**.
   g. Repeat steps a through f on each RD Gateway server so that they recognize each other as RD Gateway servers in a farm. Do not be alarmed if there are warnings, as it might take time for DNS settings to propagate.
2. Configure the server to be part of an RD Web Access farm. The steps below configure the Validation and Decryption Machine Keys to be the same on both RDWeb sites.
   a. In Server Manager on the RDMS server, click **All Servers**. Right-click the first RD Web Access server (e.g. Contoso-WebGw1) and then click **Remote Desktop Connection**.
   b. Sign into the RD Web Access server using a domain admin account.
   c. In Server Manager on the RD Web Access server, click **Tools > Internet Information Services (IIS) Manager**.
   d. In the left pane of IIS Manager, expand the **Server (e.g. Contoso-WebGw1) > Sites > Default Web Site**, and then click **RDWeb**.
   e. Right-click **Machine Key**, and then click **Open Feature**.
   f. On the Machine Key page, in the **Actions** pane, select **Generate Keys**, and then click **Apply**.
   g. Copy the validation key (you can right-click the key and then click **Copy**.)
   h. In IIS Manager, under **Default Web Site**, select **Feed**, **FeedLogon** and **Pages** in turn.
   i. For each:
      a. Right-click **Machine Key**, and then click **Open Feature**.
      b. For the Validation Key, clear **Automatically generate at runtime**, and then paste the key you copied in step g.
   j. Minimize the RD Connection window to this RD Web server.
   k. Repeat steps b through e for the second RD Web Access server, ending on the feature view of **Machine Key**.
   l. For the Validation Key, clear **Automatically generate at runtime**, and then paste the key you copied in step g.
   m. Click **Apply**.
   n. Complete this process for the **RDWeb**, **Feed**, **FeedLogon** and **Pages** pages.
   o. Minimize the RD Connection window to the second RD Web Access server, and then maximize the RD Connection window to the first RD Web Access server.

p. Repeat steps g through n to copy over the Decryption Key.

q. When validation keys and decryption keys are identical on both RD Web Access servers for the **RDWeb**, **Feed**, **FeedLogon** and **Pages** pages, sign out of all RD Connection windows.

Step 3: Configure load balancing for the RD Web and RD Gateway servers

If you are using Azure infrastructure, you can create an external Azure load balancer; if not, you can set up a separate hardware or software load balancer. Load balancing is key so that traffic will be evenly distributed the long-lived connections from Remote Desktop clients, through the RD Gateway, to the servers that users will be running their workloads.

> **NOTE**
> If your previous server running RD Web and RD Gateway was already set up behind an external load balancer, skip ahead to step 4, select the existing backend pool, and add the new server to the pool.

1. Create an Azure Load Balancer:
   a. In the Azure portal click **Browse > Load balancers > Add**.
   b. Enter a name, for example **WebGwLB**.
   c. Select **Public** for the **Scheme**.
   d. Under **Public IP address**, select **Choose a public IP address**, and then pick an existing public IP address or create a new one.
   e. Select the appropriate **Subscription**, **Resource Group**, and **Location**.
   f. Click **Create**.
2. Create a probe to monitor which servers are alive:
   a. In the Azure portal, select **Browse** > **Load Balancers**, and then choose the load balancer that you created in the previous step.
   b. Select **All settings** > **Probes** > **Add**.
   c. Enter a name, for example, **HTTPS**, for the probe. Select **TCP** as the **Protocol**, and enter **443** for the **Port**, then click **OK**.
3. Create the HTTPS and UDP load balancing rules:
   a. In **Settings**, click **Load balancing rules**.
   b. Select **Add** for the **HTTPS rule**.
   c. Enter a name for the rule, for example, HTTPS, and select **TCP** for the **Protocol**. Enter **443** for both **Port** and **Backend port**, and click **OK**.
   d. In **Load balancing rules**, click **Add** for the **UDP rule**.
   e. Enter a name for the rule, for example, **UDP**, and select **UDP** for the **Protocol**. Enter **3391** for both **Port** and **Backend port**, and click **OK**.
4. Create the backend pool for the RD Web and RD Gateway servers:
   a. In **Settings**, click **Backend address pools > Add**.
   b. Enter a name (for example, **WebGwBackendPool**), then click **Add a virtual machine**.
   c. Choose an availability set (for example, WebGwAvSet), and then click **OK**.
   d. Click **Choose the virtual machines**, select each virtual machine, and then click **Select > OK > OK**.

Deploy a two-node Storage Spaces Direct scale-out file server for UPD storage in Azure

9/27/2019 • 5 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

Remote Desktop Services (RDS) requires a domain-joined file server for user profile disks (UPDs). To deploy a high availability domain-joined scale-out file server (SOFS) in Azure, use Storage Spaces Direct with Windows Server 2016. If you're not familiar with UPDs or Remote Desktop Services, check out Welcome to Remote Desktop Services.

> **NOTE**
> Microsoft just published an Azure template to deploy a Storage Spaces Direct scale-out file server! You can use the template to create your deployment, or use the steps in this article.

We recommend deploying your SOFS with DS-series VMs and premium storage data disks, where there are the same number and size of data disks on each VM. You will need a minimum of two storage accounts.

For small deployments, we recommend a 2-node cluster with a cloud witness, where the volume is mirrored with 2 copies. Grow small deployments by adding data disks. Grow larger deployments by adding nodes (VMs).

These instructions are for a 2-node deployment. The following table shows the VM and disk sizes you'll need to store UPDs for the number of users in your business.

USERS	TOTAL (GB)	VM	# DISKS	DISK TYPE	DISK SIZE (GB)	CONFIGURATION
10	50	DS1	2	P10	128	2x(DS1 + 2 P10)
25	125	DS1	2	P10	128	2x(DS1 + 2 P10)
50	250	DS1	2	P10	128	2x(DS1 + 2 P10)
100	500	DS1	2	P20	512	2x(DS1 + 2 P20)
250	1250	DS1	2	P30	1024	2x(DS1 + 2 P30)
500	2500	DS2	3	P30	1024	2x(DS2 + 3 P30)
1000	5000	DS3	5	P30	1024	2x(DS3 + 5 P30)

USERS	TOTAL (GB)	VM	# DISKS	DISK TYPE	DISK SIZE (GB)	CONFIGURATION
2500	12500	DS4	13	P30	1024	2x(DS4 + 13 P30)
5000	25000	DS5	25	P30	1024	2x(DS5 + 25 P30)

Use the following steps to create a domain controller (we called ours "my-dc" below) and two node VMs ("my-fsn1" and "my-fsn2") and configure the VMs to be a 2-node Storage Spaces Direct SOFS.

1. Create a Microsoft Azure subscription.
2. Sign into the Azure portal.
3. Create an Azure storage account in Azure Resource Manager. Create it in a new resource group and use the following configurations:
   - Deployment model: Resource Manager
   - Type of storage account: General purpose
   - Performance tier: Premium
   - Replication option: LRS
4. Set up an Active Directory forest by either using a quickstart template or deploying the forest manually.
   - Deploy using an Azure quickstart template:
     - Create an Azure VM with a new AD forest
     - Create a new AD domain with 2 domain controllers (for high availability)
   - Manually deploy the forest with the following configurations:
     - Create the virtual network in the same resource group as the storage account.
     - Recommended size: DS2 (increase the size if the domain controller will host more domain objects)
     - Use an automatically generated VNet.
     - Follow the steps to install AD DS.
5. Set up the file server cluster nodes. You can do this by deploying the Windows Server 2016 Storage Spaces Direct SOFS cluster Azure template or by following steps 6-11 to deploy manually.
6. To manually set up the file server cluster nodes:
   a. Create the first node:
      a. Create a new virtual machine using the Windows Server 2016 image. (Click **New > Virtual Machines > Windows Server 2016.** Select **Resource Manager**, and then click **Create**.)
      b. Set the basic configuration as follows:
         - Name: my-fsn1
         - VM disk type SSD
         - Use an existing resource group, the one that you created in step 3.
      c. Size: DS1, DS2, DS3, DS4, or DS5 depending on your user needs (see table at beginning of these instructions). Ensure premium disk support is selected.
      d. Settings:
         - Storage account: Choose the storage account you created in step 3.
         - High Availability - create a new availability set. (Click **High Availability > Create new**, and then enter a name (for example, s2d-cluster). Use the default values for **Update domains** and **Fault domains**.)
   b. Create the second node. Repeat the step above with the following changes:
      - Name: my-fsn2

- High Availability - select the availability set you created above.

7. Attach data disks to the cluster node VMs according to your user needs (as seen in the table above). After the data disks are created and attached to the VM, set **host caching** to **None**.
8. Set IP addresses for all VMs to **static**.
   a. In the resource group, select a VM, and then click **Network interfaces** (under **settings**). Select the listed network interface, and then click **IP Configurations**. Select the listed IP configuration, select **static**, and then click **Save**.
   b. Note the domain controller (my-dc for our example) private IP address (10.x.x.x).
9. Set primary DNS server address on NICs of the cluster node VMs to the my-dc server. Select the VM, and then click **Network Interfaces > DNS servers > Custom DNS**. Enter the private IP address you noted above, and then click **Save**.
10. Create an Azure storage account to be your cloud witness. (If you use the linked instructions, stop when you get to "Configuring Cloud Witness with Failover Cluster Manager GUI" - we'll do that step below.)
11. Set up the Storage Spaces Direct file server. Connect to a node VM, and then run the following Windows PowerShell cmdlets.
    a. Install Failover Clustering Feature and File Server Feature on the two file server cluster node VMs:

```
$nodes = ("my-fsn1", "my-fsn2")
icm $nodes {Install-WindowsFeature Failover-Clustering -IncludeAllSubFeature -
IncludeManagementTools}
icm $nodes {Install-WindowsFeature FS-FileServer}
```

    b. Validate cluster node VMs and create 2-node SOFS cluster:

```
Test-Cluster -node $nodes
New-Cluster -Name MY-CL1 -Node $nodes –NoStorage –StaticAddress [new address within your addr
space]
```

    c. Configure the cloud witness. Use your cloud witness storage account name and access key.

```
Set-ClusterQuorum –CloudWitness –AccountName <StorageAccountName> -AccessKey
<StorageAccountAccessKey>
```

    d. Enable Storage Spaces Direct.

```
Enable-ClusterS2D
```

    e. Create a virtual disk volume.

```
New-Volume -StoragePoolFriendlyName S2D* -FriendlyName VDisk01 -FileSystem CSVFS_REFS -Size 120GB
```

    To view information about the cluster shared volume on the SOFS cluster, run the following cmdlet:

```
Get-ClusterSharedVolume
```

    f. Create the scale-out file server (SOFS):

```
Add-ClusterScaleOutFileServerRole -Name my-sofs1 -Cluster MY-CL1
```

    g. Create a new SMB file share on the SOFS cluster.

```
New-Item -Path C:\ClusterStorage\Volume1\Data -ItemType Directory
New-SmbShare -Name UpdStorage -Path C:\ClusterStorage\Volume1\Data
```

You now have a share at `\\my-sofs1\UpdStorage`, which you can use for UPD storage when you enable UPD for your users.

Use personal session desktops with Remote Desktop Services

10/23/2019 • 3 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

You can deploy server-based personal desktops in a cloud-computing environment by using personal session desktops. (A cloud-computing environment has a separation between the fabric Hyper-V servers and the guest virtual machines, such as Microsoft Azure Cloud or the Microsoft Cloud Platform.) The personal session desktop capability extends the session-based desktop deployment scenario in Remote Desktop Services to create a new type of session collection where each user is assigned to their own personal session host with administrative rights.

Use the following information to create and manage a personal session desktop collection.

Create a personal session desktop collection

Use the New-RDSessionCollection cmdlet to create a personal session desktop collection. The following three parameters provide the configuration information required for personal session desktops:

- **-PersonalUnmanaged** - Specifies the type of session collection that lets you assign users to a personal session host server. If you don't specify this parameter, then the collection is created as a traditional RD Session Host collection, where users are assigned to the next available session host when they sign in.
- **-GrantAdministrativePrivilege** - If you use **-PersonalUnmanaged**, specifies that the user assigned to the session host be given administrative privileges. If you don't use this parameter, users are granted only standard user privileges.
- **-AutoAssignUser** - If you use **-PersonalUnmanaged**, specifies that new users connecting through the RD Connection Broker are automatically assigned to an unassigned session host. If there are no unassigned session hosts in the collection, the user will see an error message. If you don't use this parameter, you have to manually assign users to a session host before they sign in.

Manually assign a user to a personal session host

Use the **Set-RDPersonalSessionDesktopAssignment** cmdlet to manually assign a user to a personal session host server in the collection. The cmdlet supports the following parameters:

-CollectionName <string>

-ConnectionBroker <string>

-User <string>

-Name <string>

- **–CollectionName** - specifies the name of the personal session desktop collection. This parameter is required.
- **–ConnectionBroker** - specifies the Remote Desktop Connection Broker (RD Connection Broker) server for your Remote Desktop deployment. If you don't supply a value, the cmdlet uses the fully qualified domain name (FQDN) of the local computer.
- **–User** - specifies the user account to associate with the personal session desktop, in DOMAIN\User format. This parameter is required.
- **–Name** - specifies the name of the session host server. This parameter is required. The session host identified

here must be a member of the collection that the **-CollectionName** parameter specifies.

The **Import-RDPersonalSessionDesktopAssignment** cmdlet imports associations between user accounts and personal session desktops from a text file. The cmdlet supports the following parameters:

-CollectionName <string>

-ConnectionBroker <string>

-Path <string>

–Path specifies the path and file name of a file to import.

Removing a User Assignment from a Personal Session Host

Use the **Remove-RDPersonalSessionDesktopAssignment** cmdlet to remove the association between a personal session desktop and a user. The cmdlet supports the following parameters:

-CollectionName <string>

-ConnectionBroker <string>

-Force

-Name <string>

-User <string>

–Force forces the command to run without asking for user confirmation.

Query user assignments

Use the **Get-RDPersonalSessionDesktopAssignment** cmdlet to get a list of personal session desktops and associated user accounts. The cmdlet supports the following parameters:

-CollectionName <string>

-ConnectionBroker <string>

-User <string>

-Name <string>

You can run the cmdlet to query by collection name, user name, or by session desktop name. If you specify only the **–CollectionName** parameter, the cmdlet returns a list of session hosts and associated users. If you also specify the **–User** parameter, the session host associated with that user is returned. If you provide the **–Name** parameter, the user associated with that session host is returned.

The **Export-RDPersonalPersonalDesktopAssignment** cmdlet exports the current associations between users and personal virtual desktops to a text file. The cmdlet supports the following parameters:

-CollectionName <string>

-ConnectionBroker <string>

-Path <string>

All new cmdlets support the common parameters: -Verbose, -Debug, -ErrorAction, -ErrorVariable, -OutBuffer, and -OutVariable. For more information, see about_CommonParameters.

Create virtual machines for Remote Desktop

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

You can install Remote Desktop Services components on physical servers or on virtual machines.

The first step is to create Windows Server virtual machines in Azure. You'll want to create three VMs: one for the RD Session Host, one for the Connection Broker, and one for the RD Web and RD Gateway. To ensure the availability of your RDS deployment, create an availability set (under **High availablility** in the VM creation process) and group multiple VMs in that availability set.

After you create your VMs, use the following steps to prepare them for RDS.

1. Connect to the virtual machine using the Remote Desktop Connection (RDC) client:
   a. In the Azure portal open the Resource groups view, and then click the resource group to use for the deployment.
   b. Select the new RDSH virtual machine (for example, Contoso-Sh1).
   c. Click **Connect > Open** to open the Remote Desktop client.
   d. In the client, click **Connect**, and then click **Use another user account**. Enter the user name and password for the local administrator account.
   e. Click **Yes** when warned about the certificate.
2. Enable remote management:
   a. In Server Manager, click **Local Server > Remote management current setting (disabled)**.
   b. Select **Enable remote management for this server**.
   c. Click **OK**.
3. Optional: You can temporarily set Windows Update to not automatically download and install updates. This helps prevent changes and system restarts while you deploy the RDSH server.
   a. In Server Manager, click **Local Server > Windows Update current setting**.
   b. Select **Advanced options > Defer upgrades**.
4. Add the server to the domain:
   a. In Server Manager, click **Local Server > Workgroup current setting**.
   b. Click **Change > Domain**, and then enter the domain name (for example, Contoso.com).
   c. Enter the domain administrator credentials.
   d. Restart the virtual machine.
5. Repeat steps 1 through 4 for the RD Web and GW virtual machine.
6. Repeat steps 1 through 4 for the RD Connection Broker virtual machine.
7. Initialize and format the attached disk on the RD Connection Broker virtual machine:
   a. Connect to the RD Connection Broker virtual machine (step 1 above).
   b. In Server Manager, click **Tools > Computer Management**.
   c. Click **Disk Management**.
   d. Select the attached disk, then **MBR (Master Boot Record)**, and then click **OK**.
   e. Right-click the new disk (marked as **Unallocated**) and click **New Simple Volume**.
   f. In the **New Simple Volume** wizard, accept the default values but provide a applicable name for the **Volume label** (like Shares).
8. On the RD Connection Broker virtual machine create file shares for the user profile disks and certificates:

a. Open File Explorer, click **This PC**, and open the disk that you added for file shares.
b. Click **Home** and **New Folder**.
c. Enter a name for the user disks folder, for example, **UserDisks**.
d. Right-click the new folder and click **Properties > Sharing > Advanced Sharing**.
e. Select **Share this folder** and click **Permissions**.
f. Select **Everyone**, and then click **Remove**. Now click **Add**, enter **Domain Admins**, and click **OK**.
g. Select **Allow Full Control**, and then click **OK > OK > Close**.
h. Repeat steps c. to g. to create a shared folder for certificates.

Configure disaster recovery for Remote Desktop Services

9/27/2019 • 2 minutes to read • Edit Online

When you deploy Remote Desktop Services into your environment, it becomes a critical part of your infrastructure, particularly the apps and resources that you share with users. If the RDS deployment goes down due to anything from a network failure to a natural disaster, users can't access those apps and resources, and your business is negatively impacted. To avoid this, you can configure a disaster recovery solution that allows you to failover your deployment - if your RDS deployment is unavailable, for whatever reason, there is a backup available to automatically take over.

To keep your RDS deployment running in the case of a single component or machine going down, we recommend configuring your RDS deployment for high availability. You can do this by setting up an RDSH farm and ensuring your Connection Brokers are clustered for high availability.

The disaster recovery solutions we recommend here are to protect your deployment from catastrophic disaster - something that takes down your entire RDS deployment (including redundant roles configured for high availability). If such a disaster hits, having a disaster recovery solution built into your deployment will allow you to failover the entire deployment and quickly get apps and resources up and running for your users.

Use the following information to deploy disaster recovery solutions in RDS:

- Leverage multiple Azure data centers to ensure users can access your RDS deployment, even if one Azure data center goes down (geo-redundancy)
- Deploy Azure Site Recovery to provide failover for RDS components in site-to-site or site-to-Azure failovers

Create a geo-redundant, multi-data center RDS deployment for disaster recovery

9/27/2019 • 11 minutes to read • Edit Online

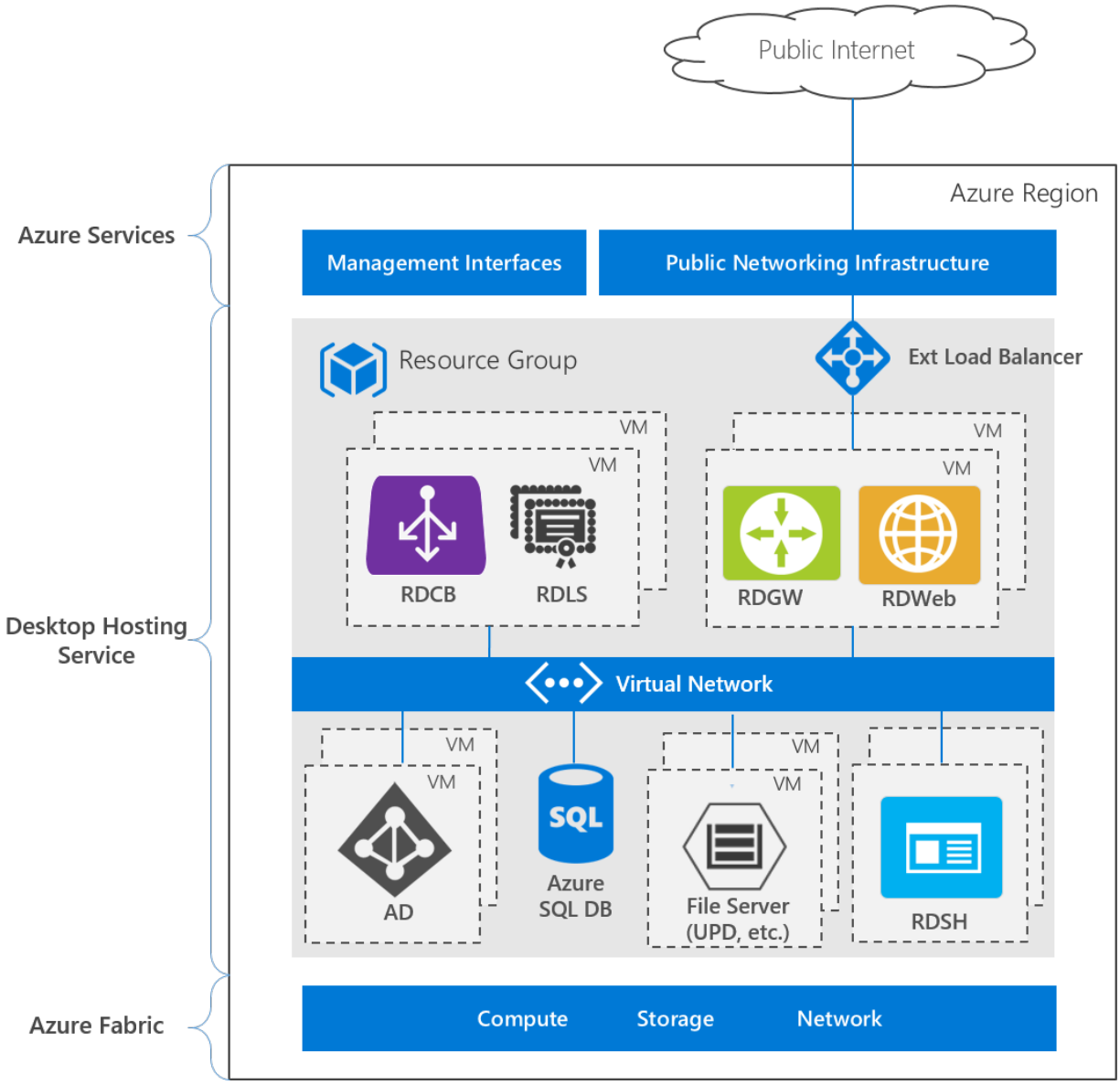
Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

You can enable disaster recovery for your Remote Desktop Services deployment by leveraging multiple data centers in Azure. Unlike a standard highly available RDS deployment (as outlined in the Remote Desktop Services architecture), which uses data centers in a single Azure region (for example, Western Europe), a multi-data center deployment uses data centers in multiple geographic locations, increasing the availability of your deployment - one Azure data center might be unavailable, but it is unlikely that multiple regions would go down at the same time. By deploying a geo-redundant RDS architecture, you can enable failover in the case of catastrophic failure of an entire region.

You can use the instructions below to leverage Microsoft Azure infrastructure services and RDS to deliver geo-redundant desktop hosting services and Subscriber Access Licenses (SALs) to multiple tenants through the Microsoft Service Provider License Agreement (SPLA) program. You can also use the steps below to create a geo-redundant hosting service for your own employees using RDS User CALs extended rights through Software Assurance.

Logical architecture for high availability - single and multiple regions

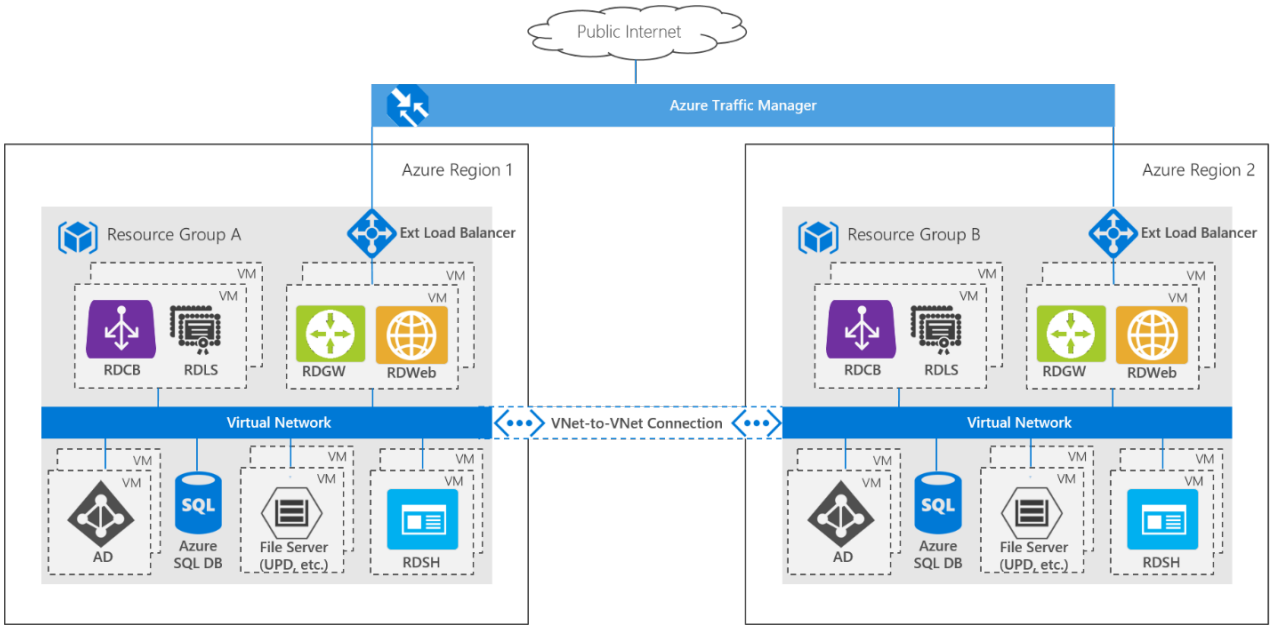
The following image shows the architecture for a highly available deployment in a single Azure region:



The deployment consists of three layers:

- Azure services - the Azure Management interfaces, including the Azure portal and APIs, and public networking services, such as DNS and public IP addressing.
- Desktop hosting service - Virtual machines, networks, storage, Azure services, and Windows Server role services
- Azure Fabric - Windows Server operating systems running the Hyper-V role, used to virtualize physical servers, storage units, network switches, and routers. Using Azure Fabric lets you create VMs, networks, storage, and applications independent from underlying hardware.

In comparison, here is the architecture for a deployment that uses multiple Azure data centers:



The entire RDS deployment is replicated in a second Azure region to create a geo-redundant deployment. This architecture uses an active-passive model, where only one RDS deployment is running at a time. A VNet-to-VNet connection lets the two environments communicate with each other. The RDS deployments are based on a single Active Directory forest/domain, and the AD servers replicate across the two deployments, meaning users can sign into either deployment using the same credentials. User settings and data stored in User Profile Disks (UPD) are stored on a two-node cluster Storage Spaces Direct scale-out file server (SOFS). A second identical Storage Spaces Direct cluster is deployed in the second (passive) region, and Storage Replica is used to replicate the user profiles from the active to passive deployment. Azure Traffic Manager is used to automatically direct end users to whichever deployment is currently active - from the end user perspective, they access the deployment using a single URL and are not aware of which region they end up using.

You *could* create a non-highly available RDS deployment in each region, but if even a single VM is restarted in one region, a failover would occur, increasing the likelihood of failovers occurring with associated performance impacts.

Deployment steps

Create the following resources in Azure to create a geo-redundant multi-data center RDS deployment:

1. Two resource groups in two separate Azure regions. For example RG A (the active deployment, RG stands for "resource group") and RG B (the passive deployment).
2. A highly-available Active Directory deployment in RG A. You can use the New AD Domain with 2 Domain Controllers template to create the deployment.
3. A highly-available RDS deployment in RG A. Use the RDS farm deployment using existing active directory template to create the basic RDS deployment, and then follow the information in Remote Desktop Services - High availability to configure the other RDS components for high availability.
4. A VNet in RG B - make sure to use an address space that does not overlap the deployment in RG A.
5. A VNet-to-VNet connection between the two resource groups.
6. Two AD virtual machines in an availability set in RG B - make sure the VM names are different from the AD VMs in RG A. Deploy two Windows Server 2016 VMs in a single availability set, install the Active Directory Domain Services role, and then promote them to the domain controller in the domain you created in step 1.
7. A second highly-available RDS deployment in RG B.
    a. Use the RDS farm deployment using existing active directory template again, but this time make the following changes. (To customize the template, select it in the gallery, click **Deploy to Azure** and then

Edit template.)

a. Adjust the address space of the DNS server private IP to correspond to the VNet in RG B.

   Search for "dnsServerPrivateIp" in variables. Edit the default IP (10.0.0.4) to correspond to the address space you defined in the VNet in RG B.

b. Edit the computer names so that they don't collide with those in the deployment in RG A.

   Locate the VMs in the **Resources** section of the template. Change the **computerName** field under **osProfile**. For example, "gateway" can become"gateway-**b**"; "[concat('rdsh-', copyIndex())]" can become "[concat('rdsh-b-', copyIndex())]", and "broker" can become "broker-**b**".

   (You can also change the names of the VMs manually after you run the template.)

b. As in step 3 above, use the information in Remote Desktop Services - High availability to configure the other RDS components for high availability.

8. A Storage Spaces Direct scale-out file server with Storage Replica across the two deployments. Use the PowerShell script to deploy the template across the resource groups.

> **NOTE**
> You can provision storage manually (instead of using the PowerShell script and template):
>
> 1. Deploy a two-node Storage Spaces Direct SOFS in RG A to store your user profile disks (UPDs).
> 2. Deploy a second, identical Storage Spaces Direct SOFS in RG B - make sure to use the same amount of storage in each cluster.
> 3. Set up Storage Replica with asynchronous replication between the two.

Enable UPDs

Storage Replica replicates data from a source volume (associated with the primary/active deployment) to a destination volume (associated with the secondary/passive deployment). By design, the destination cluster appears as **Online (No Access)** - Storage Replica dismounts the destination volumes and their drive letters or mount points. This means that enabling UPDs for the secondary deployment by providing the file share path will fail, because the volume is not mounted.

Want to learn more about managing replication? Check out Cluster to cluster Storage Replication.

To enable UPDs on both deployments, do the following:

1. Run the Set-RDSessionCollectionConfiguration cmdlet to enable the user profile disks for the primary (active) deployment - provide a path to the file share on the source volume (which you created in Step 7 in the deployment steps).

2. Reverse the Storage Replica direction so that the destination volume becomes the source volume (this mounts the volume and makes it accessible by the secondary deployment). You can run **Set-SRPartnership** cmdlet to do this. For example:

```
Set-SRPartnership -NewSourceComputerName "cluster-b-s2d-c" -SourceRGName "cluster-b-s2d-c" -
DestinationComputerName "cluster-a-s2d-c" -DestinationRGName "cluster-a-s2d-c"
```

3. Enable the user profile disks in the secondary (passive) deployment. Use the same steps as you did for the primary deployment, in step 1.

4. Reverse the Storage Replica direction again, so the original source volume is again the source volume in the SR Partnership, and the primary deployment can access the file share. For example:

```
Set-SRPartnership -NewSourceComputerName "cluster-a-s2d-c" -SourceRGName "cluster-a-s2d-c" -
DestinationComputerName "cluster-b-s2d-c" -DestinationRGName "cluster-b-s2d-c"
```

Azure Traffic Manager

Create an Azure Traffic Manager profile, and make sure to select the **Priority** routing method. Set the two endpoints to the public IP addresses of each deployment. Under **Configuration**, change the protocol to HTTPS (instead of HTTP) and the port to 443 (instead of 80). Take note of the **DNS time to live**, and set it appropriately for your failover needs.

Note that Traffic Manager requires endpoints to return 200 OK in response to a GET request in order to be marked as "healthy." The publicIP object created from the RDS templates will function, but do not add a path addendum. Instead, you can give end users the Traffic Manager URL with "/RDWeb" appended, for example: `http://deployment.trafficmanager.net/RDWeb`

By deploying Azure Traffic Manager with the Priority routing method, you prevent end users from accessing the passive deployment while the active deployment is functional. If end users access the passive deployment and the Storage Replica direction hasn't been switched for failover, the user sign-in hangs as the deployment tries and fails to access the file share on the passive Storage Spaces Direct cluster - eventually the deployment will give up and give the user a temporary profile.

Deallocate VMs to save resources

After you configure both deployments, you can optionally shut down and deallocate the secondary RDS infrastructure and RDSH VMs to save cost on these VMs. The Storage Spaces Direct SOFS and AD server VMs must always stay running in the secondary/passive deployment to enable user account and profile synchronization.

When a failover occurs, you'll need to start the deallocated VMs. This deployment configuration has the advantage of being lower cost, but at the expense of fail-over time. If a catastrophic failure occurs in the active deployment, you'll have to manually start the passive deployment, or you'll need an automation script to detect the failure and start the passive deployment automatically. In either case, it may take several minutes to get the passive deployment running and available for users to sign in, resulting in some downtime for the service. This downtime depends on the amount of time it takes to start the RDS infrastructure and RDSH VMs (typically 2-4 minutes, if the VMs are started in parallel rather than serially), and the time to bring the passive cluster online (which depends on the size of the cluster, typically 2-4 minutes for a 2-node cluster with 2 disks per node).

Active Directory

The Active Directory servers in each deployment are replicas within the same Forest/Domain. Active Directory has a built-in synchronization protocol to keep the four domain controllers in sync. However, there may be some lag so that if a new user is added to one AD server, it may take some time to replicate across all the AD servers in the two deployments. Consequently, be sure to warn users to not try to sign in immediately after being added to the domain.

RD License Server

Provide a per-user RD CAL for each named user that is authorized to access the geo-redundant deployment. Distribute the per user CALs evenly across the two RD License Servers in the active deployment. Then, duplicate these CALs to the two RD License Servers in the passive deployment. Because the CALs are duplicated between the active and passive deployment, at any given time only one deployment can be active with users connecting; otherwise, you violate the license agreement.

Image Management

As you update your RDSH images to provide software updates or new applications, you'll need to separately update the RDSH collections in each deployment to maintain a common user experience across both deployments. You can use the Update RDSH collection template, but note that the passive deployment's RDS infrastructure and

RDSH VMs must be running to run the template.

Failover

In the case of the Active-Passive deployment, failover requires you to start the VMs of the secondary deployment. You can do this manually or with an automation script. In the case of a catastrophic failover of the Storage Spaces Direct SOFS, change the Storage Replica partnership direction, so that the destination volume becomes the source volume. For example:

```
Set-SRPartnership -NewSourceComputerName "cluster-b-s2d-c" -SourceRGName "cluster-b-s2d-c" -
DestinationComputerName "cluster-a-s2d-c" -DestinationRGName "cluster-a-s2d-c"
```

You can learn more in Cluster to cluster Storage Replication.

Azure Traffic Manager automatically recognizes that the primary deployment failed and that the secondary deployment is healthy (in the RD Gateway VMs have been started in RG B) and directs user traffic to the secondary deployment. Users can use the same Traffic Manager URL to continue working on their remote resources, enjoying a consistent experience. Note that the client DNS cache will not update the record for the duration of the TTL set in Azure Traffic Manager configuration.

Test failover

In a Storage Replica partnership, only one volume (the source) can be active at a time. This means when you switch the SR Partnership direction, the volume in the primary deployment (RG A) becomes the destination of replication and is therefore hidden. Thus, any users connecting to RG A will no longer have access to their UPDs stored on the SOFS in RG A.

To test the failover while allowing users to continue logging in:

1. Start the infrastructure VMs and RDSH VMs in RG B.
2. Switch the SR Partnership direction (cluster-b-s2d-c becomes the source volume).
3. Disable the endpoint of RG A in the Azure Traffic Manager profile to force the ATM to direct traffic to RG B. Alternatively, use a PowerShell script:

   ```
   Disable-AzureRmTrafficManagerEndpoint -Name publicIpA -Type AzureEndpoints -ProfileName
   MyTrafficManagerProfile -ResourceGroupName RGA -Force
   ```

RG B is now the active primary deployment. To switch back to RG A as the primary deployment:

1. Switch the SR Partnership direction (cluster-a-s2d-c becomes the source volume):

   ```
   Set-SRPartnership -NewSourceComputerName "cluster-a-s2d-c" -SourceRGName "cluster-a-s2d-c" -
   DestinationComputerName "cluster-b-s2d-c" -DestinationRGName "cluster-b-s2d-c"
   ```

2. Re-enable the endpoint of RG A in the Azure Traffic Manager profile:

   ```
   Enable-AzureRmTrafficManagerEndpoint -Name publicIpA -Type AzureEndpoints -ProfileName
   MyTrafficManagerProfile -ResourceGroupName RGA
   ```

Considerations for on-premises deployments

While an on-premises deployment couldn't use the Azure Quickstart Templates referenced in this article, you can implement all the infrastructure roles manually. In an on-premises deployment where cost is not driven by Azure

consumption, consider using an active-active model for quicker failover.

You can use Azure Traffic Manager with on-premises endpoints, but it requires an Azure subscription. Alternatively, for the DNS provided to end users, give them a CNAME record that simply directs users to the primary deployment. In the case of failover, modify the DNS CNAME record to redirect to the secondary deployment. In this way, the end user uses a single URL, just like with Azure Traffic Manager, that directs the user to the appropriate deployment.

If you are interested in creating an on-premises-to-Azure-site model, consider using Azure Site Recovery.

Set up disaster recovery for RDS using Azure Site Recovery

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

You can use Azure Site Recovery to create a disaster recovery solution for your Remote Desktop Services deployment.

Azure Site Recovery is an Azure-based service that provides disaster recovery capabilities by orchestrating replication, failover, and recovery of virtual machines. Azure Site Recovery supports a number of replication technologies to consistently replicate, protect, and seamlessly failover virtual machines and applications to private/public or hoster's clouds.

Use the following information to create and validate the disaster recovery solution.

Disaster recovery deployment options

You can deploy RDS on either physical servers or virtual machines running Hyper-V or VMWare. Azure Site Recovery can protect both on-premises and virtual deployments to either a secondary site or to Azure. The following table shows the different supported RDS deployments in site-to-site and site-to-Azure disaster recvoery scenarios.

DEPLOYMENT TYPE	HYPER-V SITE-TO-SITE	HYPER-V SITE-TO-AZURE	VMWARE SITE-TO-AZURE	PHYSICAL SITE-TO-AZURE
Pooled virtual desktop (unmanaged)	Yes	No	No	No
Pooled virtual desktop (managed, no UPD)	Yes	No	No	No
RemoteApps and desktop sessions (no UPD)	Yes	Yes	Yes	Yes

Prerequisites

Before you can configure Azure Site Recovery for your deployment, make sure you meet the following requirements:

- Create an on-premises RDS deployment.
- Add Azure Site Recovery Services vault to your Microsoft Azure subscription.
- If you are going to use Azure as your recovery site, run the Azure Virtual Machine Readiness Assessment tool on your VMs to ensure they are compatible with Azure VMs and Azure Site Recovery Services.

Implementation checklist

We'll cover the various steps to enable Azure Site Recovery Services for your RDS deployment in more detail, but

here are the high-level implementation steps.

STEP 1 - CONFIGURE VMS FOR DISASTER RECOVERY
Hyper-V - Download the Microsoft Azure Site Recovery Provider. Install it on your VMM server or Hyper-V host. See Prerequisites for replication to Azure by using Azure Site Recovery for information.
VMWare - Configure protection server, configuration server, and master target servers
Step 2 - Prepare your resources
Add an Azure Storage account.
Hyper-V - Download the Microsoft Azure Recovery Services agent and install it on Hyper-V host servers.
VMWare - Make sure the mobility service is installed on all VMs.
Enable protection for VMs in VMM cloud, Hyper-V sites, or VMWare sites.
Step 3 - Design your recovery plan.
Map your resources - map on-premises networks to Azure VNETs.
Create the recovery plan.
Test the recovery plan by creating a test failover. Ensure all VMs can access required resources, like Active Directory. Ensure network redirections are configured and working for RDS. For detailed steps on testing your recovery plan, see Run a test failover
Step 4 - Run a disaster recovery drill.
Run a disaster recovery drill using planned and unplanned failovers. Ensure that all VMs have access to required resources, such as Active Directory. Ensure that all VMs have access to required resources, such as Active Directory. For detailed steps on failovers and how to run drills, see Failover in Site Recovery.

Enable disaster recovery of RDS using Azure Site Recovery

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

To ensure that your RDS deployment is adequately configured for disaster recovery, you need to protect all of the components that make up your RDS deployment:

- Active Directory
- SQL Server tier
- RDS components
- Network components

Configure Active Directory and DNS replication

You need Active Directory on the disaster recovery site for your RDS deployment to work. You have two choices based on how complex your RDS deployment is:

- Option 1 - If you have a small number of applications and a single domain controller for your entire on-premises site, and you will be failing over the entire site together, use ASR-Replication to replicate the domain controller to the secondary site (true for both site-to-site and site-to-Azure scenarios).
- Option 2 - If you have a large number of applications and you're running an Active Directory forest, and you'll failover a few applications at a time, set up an additional domain controller on the disaster recovery site (either a secondary site or in Azure).

See Protect Active Directory and DNS with Azure Site Recovery for details on making a domain controller available on the disaster recovery site. For the rest of this guidance, we assume that you've followed those steps and have the domain controller available.

Set up SQL Server replication

See Protect SQL Server using SQL Server disaster recovery and Azure Site Recovery for the steps to set up SQL Server replication.

Enable protection for the RDS application components

Depending on your RDS deployment type you can enable protection for different component VMs (as listed in the table below) in Azure Site Recovery. Configure the relevant Azure Site Recovery elements based on whether your VMs are deployed on Hyper-V or VMWare.

DEPLOYMENT TYPE	PROTECTION STEPS
Personal virtual desktop (unmanaged)	1. Make sure all virtualization hosts are ready with the RDVH role installed. 2. Connection Broker. 3. Personal desktops. 4. Gold template VM. 5. Web Access, License server, and Gateway server

DEPLOYMENT TYPE	PROTECTION STEPS
Pooled virtual desktop (managed with no UPD)	1. All virtualization hosts are ready with the RDVH role installed. 2. Connection Broker. 3. Gold template VM. 4. Web Access, License server, and Gateway server.
RemoteApps and Desktop Sessions (no UPD)	1. Session Hosts. 2. Connection Broker. 3. Web Access, License server, and Gateway server.

Create your disaster recovery plan for RDS

9/27/2019 • 5 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

You can create a disaster recovery plan in Azure Site Recovery to automate the failover process. Add all RDS component VMs to the recovery plan.

Use the following steps in Azure to create your recovery plan:

1. Open Azure Site Recovery Vault in the Azure portal, and then click **Recovery Plans**.
2. Click **Create** and enter a name for the plan.
3. Select your **Source** and **Target**. The target is either a secondary RDS site or Azure.
4. Select the VMs that host your RDS components, and then click **OK**.

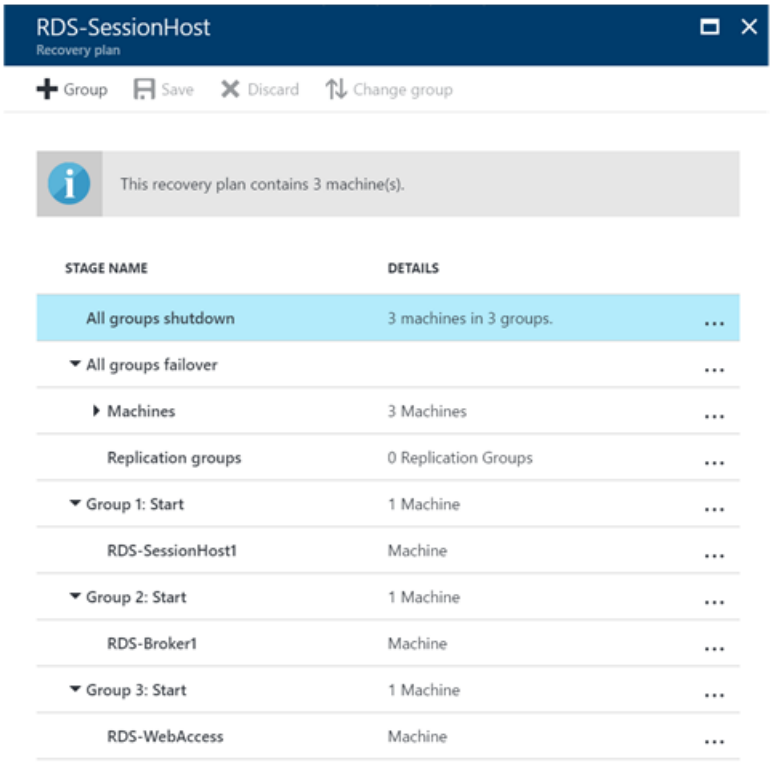
The following sections provide additional information about creating recovery plans for the different types of RDS deployment.

Sessions-based RDS deployment

For an RDS sessions-based deployment, group the VMs so they come up in sequence:

1. Failover group 1 - Session Host VM
2. Failover group 2 - Connection Broker VM
3. Failover group 3 - Web Access VM

Your plan will look something like this:



Pooled desktops RDS deployment

For an RDS deployment with pooled desktops, group the VMs so they come up in sequence, adding manual steps and scripts.

1. Failover group 1 - RDS Connection Broker VM
2. Group 1 manual action - Update DNS

   Run PowerShell in an elevated mode on the Connection Broker VM. Run the following command and wait for a couple of minutes to ensure the DNS is updated with the new value:

   ```
   ipconfig /registerdns
   ```

3. Group 1 script - add Virtualization hosts

   Modify the script below to run for each virtualization host in the cloud. Typically after you add a virtualization host to a Connection Broker, you need to restart the host. Ensure that the host doesn't have a reboot pending before the script runs, or else it will fail.

   ```
   Broker - broker.contoso.com
   Virtualization host - VH1.contoso.com

   ipmo RemoteDesktop;
   add-rdserver –ConnectionBroker broker.contoso.com –Role RDS-VIRTUALIZATION –Server VH1.contoso.com
   ```

4. Failover group 2 - Template VM
5. Group 2 script 1 - Turn off Template VM

   The template VM when recovered to the secondary site will start, but it is a sysprepped VM and cannot start completely. Also RDS requires that the VM be shutdown to create a pooled VM configuration from it. So, we need to turn it off. If you have a single VMM server, the template VM name is the same on the primary and the secondary. Because of that, we use the VM ID as specified by the *Context* variable in the script below. If you have multiple templates, turn them all off.

   ```
   ipmo virtualmachinemanager;
   Foreach($vm in $VMsAsTemplate)
   {
      Get-SCVirtualMachine -ID $vm | Stop-SCVirtualMachine –Force
   }
   ```

6. Group 2 script 2 - Remove existing pooled VMs

   You need to remove the pooled VMs on the primary site from the Connection Broker so new VMs can be created on the secondary site. In this case you need to specify the exact host on which to create the pooled VM. Note that this will delete the VMs from only the collection.

   ```
   ipmo RemoteDesktop
   $desktops = Get-RDVirtualDesktop -CollectionName Win8Desktops;
   Foreach($vm in $desktops){
      Remove-RDVirtualDesktopFromCollection -CollectionName Win8Desktops -VirtualDesktopName
   $vm.VirtualDesktopName –Force
   }
   ```

7. Group 2 manual action - Assign new template

You need to assign the new template to the Connection Broker for the collection so you can create new pooled VMs on the recovery site. Go to the RDS Connection Broker and identify the collection. Edit the properties and specify a new VM image as its template.

8. Group 2 script 3 - Recreate all pooled VMs

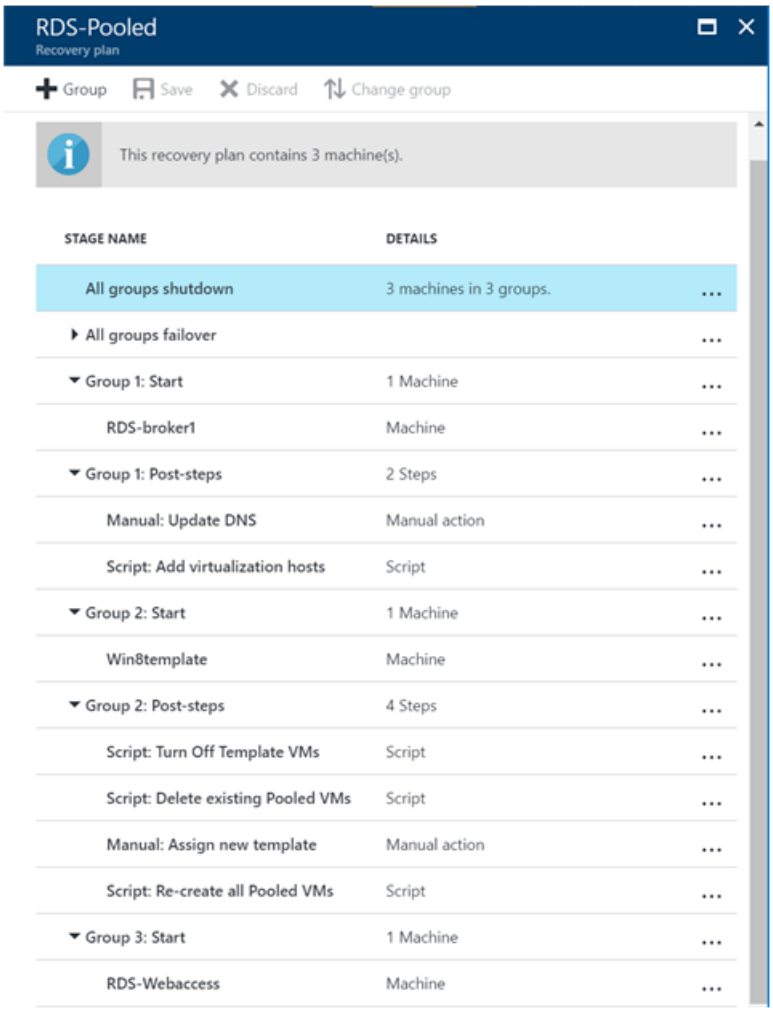
   Recreate the pooled VMs on the recovery site through the Connection Broker. In this case, you need to specify the exact host on which to create the pooled VM.

   The pooled VM name needs to be unique, using the prefix and suffix. If the VM name already exists, the script will fail. Also, if the primary side VMs are numbered from 1-5, the recovery site numbering will continue from 6.

   ```
   ipmo RemoteDesktop;
   Add-RDVirtualDesktopToCollection -CollectionName Win8Desktops -VirtualDesktopAllocation
   @{"RDVH1.contoso.com" = 1}
   ```

9. Failover group 3 - Web Access and Gateway server VM

The recovery plan will look like this:



Personal desktops RDS deployment

For an RDS deployment with personal desktops, group the VMs so they come up in sequence, adding manual steps and scripts.

1. Failover group 1 - RDS Connection Broker VM
2. Group 1 manual action - Update DNS

Run PowerShell in an elevated mode on the Connection Broker VM. Run the following command and wait for a couple of minutes to ensure the DNS is updated with the new value:

```
ipconfig /registerdns
```

3. Group 1 script - Add Virtualization hosts

   Modify the script below to run for each virtualization host in the cloud. Typically after you add a virtualization host to a Connection Broker, you need to restart the host. Ensure that the host doesn't have a reboot pending before the script runs, or else it will fail.

```
Broker - broker.contoso.com
Virtualization host - VH1.contoso.com

ipmo RemoteDesktop;
add-rdserver –ConnectionBroker broker.contoso.com –Role RDS-VIRTUALIZATION –Server VH1.contoso.com
```

4. Failover group 2 - Template VM
5. Group 2 script 1 - Turn off template VM

   The template VM when recovered to the secondary site will start, but it is a sysprepped VM and cannot start completely. Also RDS requires that the VM be shutdown to create a pooled VM configuration from it. So, we need to turn it off. If you have a single VMM server, the template VM name is the same on the primary and the secondary. Because of that, we use the VM ID as specified by the *Context* variable in the script below. If you have multiple templates, turn them all off.

```
ipmo virtualmachinemanager;
Foreach($vm in $VMsAsTemplate)
{
   Get-SCVirtualMachine -ID $vm | Stop-SCVirtualMachine –Force
}
```

6. Failover group 3 - Personal VMs
7. Group 3 script 1 - Remove existing personal VMs and add them

   Remove the personal VMs on the primary site from the Connection Broker so new VMs can be created on the secondary site. You need to extract the VMs' assignments and re-add the virtual machines to the Connection Broker with the hash of assignments. This will only remove the personal VMs from the collection and re-add them. The personal desktop allocation will be exported and imported back into the collection.

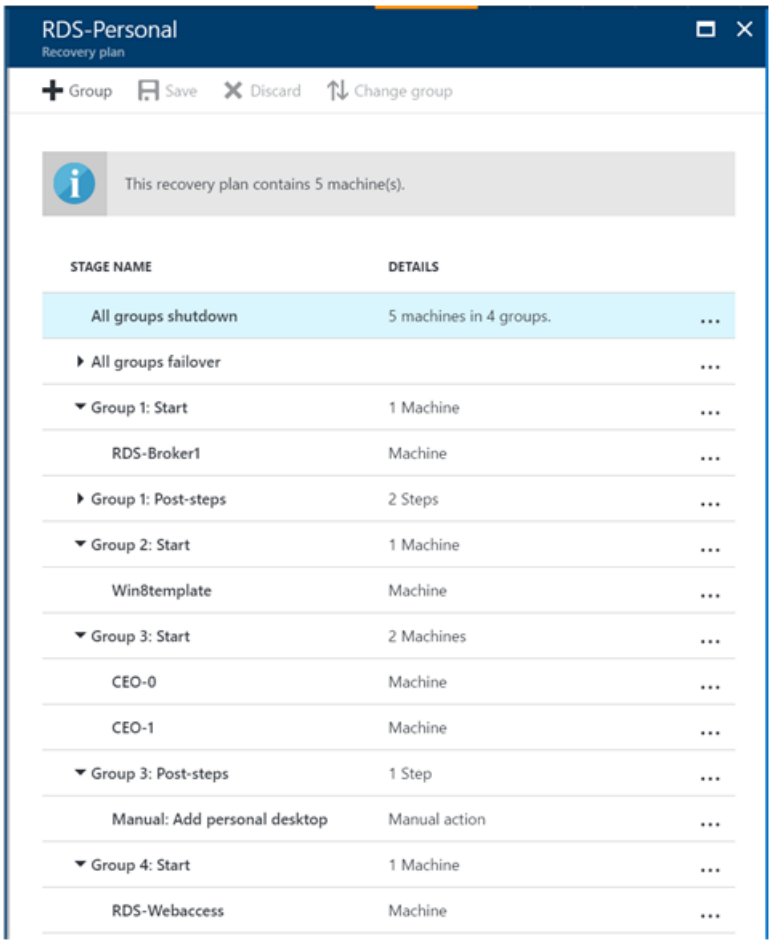
```
ipmo RemoteDesktop
$desktops = Get-RDVirtualDesktop -CollectionName CEODesktops;
Export-RDPersonalVirtualDesktopAssignment -CollectionName CEODesktops -Path ./Desktopallocations.txt -
ConnectionBroker broker.contoso.com

Foreach($vm in $desktops){
  Remove-RDVirtualDesktopFromCollection -CollectionName CEODesktops -VirtualDesktopName
$vm.VirtualDesktopName –Force
}

Import-RDPersonalVirtualDesktopAssignment -CollectionName CEODesktops -Path ./Desktopallocations.txt -
ConnectionBroker broker.contoso.com
```

8. Failover group 3 - Web Access and Gateway server VM

Your plan will look something like this:



Run and tune your Remote Desktop Services environment

9/27/2019 • 2 minutes to read • Edit Online

Tuning your deployment takes time and requires instrumentation and monitoring. Use the processes below to refine your Remote Desktop deployment, keep it running and enable scaling out (and in) as needed.

It's a good practice to continually assess the metrics and balance against running costs.

Management and monitoring

CHeck out Manage users in your RDS collection for information about how to manage access to your desktops and remote resources.

Use **Microsoft Operations Management Suite (OMS)** to monitor Remote Desktop deployments for potential bottlenecks and manage them using one of the following ways:

- **Server Manager**: Use the RD management tool that is built in to Windows Server to manage deployments with up to 500 concurrent remote end-users.
- **PowerShell**: Use the RD PowerShell module, also built into Windows Server, to manage deployments with up to 5000 concurrent remote end-users.

Scale: Bigger, better, faster

With visibility into the deployment, you can control scale with more precision. Easily add or remove Remote Desktop host servers based on scale needs.

Remote Desktop deployments that are built on Azure can make use of Azure services, like Azure SQL, to scale automatically on demand.

Automation: Script for success

Maintaining a running, highly scaled application involves repeating operations on a regular basis. Use Remote Desktop Services PowerShell cmdlets and WMI providers to develop scripts that can be run on multiple deployments when needed. Run Best Practice Analyzer (BPA) rules for Remote Desktop Services on your deployments to tune your deployments.

Load testing: Avoid surprises

Load test the deployment with both stress tests and simulation of real-life usage. Vary the load size to avoid surprises! Ensure that responsiveness meets user requirements, and that the entire system is resilient. Create load tests with simulation tools, like LoginVSI, that check your deployment's ability to meet the users' needs.

Manage your personal desktop session collections

1/14/2020 • 2 minutes to read • Edit Online

Use the following information to manage a personal desktop session collection in Remote Desktop Services.

Manually assign a user to a personal session host

Use the **Set-RDPersonalSessionDesktopAssignment** cmdlet to manually assign a user to a personal session host server in the collection. The cmdlet supports the following parameters:

-CollectionName <string>

-ConnectionBroker <string>

-User <string>

-Name <string>

- **–CollectionName** - specifies the name of the personal session desktop collection. This parameter is required.
- **–ConnectionBroker** - specifies the Remote Desktop Connection Broker (RD Connection Broker) server for your Remote Desktop deployment. If you don't supply a value, the cmdlet uses the fully qualified domain name (FQDN) of the local computer.
- **–User** - specifies the user account to associate with the personal session desktop, in DOMAIN\User format. This parameter is required.
- **–Name** - specifies the name of the session host server. This parameter is required. The session host identified here must be a member of the collection that the **-CollectionName** parameter specifies.

The **Import-RDPersonalSessionDesktopAssignment** cmdlet imports associations between user accounts and personal session desktops from a text file. The cmdlet supports the following parameters:

-CollectionName <string>

-ConnectionBroker <string>

-Path <string>

–Path specifies the path and file name of a file to import.

Removing a User Assignment from a Personal Session Host

Use the **Remove-RDPersonalSessionDesktopAssignment** cmdlet to remove the association between a personal session desktop and a user. The cmdlet supports the following parameters:

-CollectionName <string>

-ConnectionBroker <string>

-Force

-Name <string>

-User <string>

–Force forces the command to run without asking for user confirmation.

Query user assignments

Use the **Get-RDPersonalSessionDesktopAssignment** cmdlet to get a list of personal session desktops and associated user accounts. The cmdlet supports the following parameters:

-CollectionName <string>

-ConnectionBroker <string>

-User <string>

-Name <string>

You can run the cmdlet to query by collection name, user name, or by session desktop name. If you specify only the **–CollectionName** parameter, the cmdlet returns a list of session hosts and associated users. If you also specify the **–User** parameter, the session host associated with that user is returned. If you provide the **–Name** parameter, the user associated with that session host is returned.

The **Export-RDPersonalPersonalDesktopAssignment** cmdlet exports the current associations between users and personal virtual desktops to a text file. The cmdlet supports the following parameters:

-CollectionName <string>

-ConnectionBroker <string>

-Path <string>

All new cmdlets support the common parameters: -Verbose, -Debug, -ErrorAction, -ErrorVariable, -OutBuffer, and -OutVariable. For more information, see about_CommonParameters.

Recommended settings for VDI desktops

9/27/2019 • 24 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016, Windows 10

Microsoft Desktop Virtualization automatically detects device configurations and network conditions to get users up and running sooner by enabling the instant setup of corporate applications and desktops, and it equips IT to provide access to legacy applications during migration to Windows 10.

Although the Windows 10 operating system is very well tuned out of the box, there are opportunities for you to refine it further specifically for the corporate Microsoft Virtual Desktop Infrastructure (VDI) environment. In the VDI environment, many background services and tasks are disabled from the beginning.

This topic is not a blueprint, but rather a guide or starting point. Some recommendations might disable functionality that you would prefer to use, so you should consider the cost versus the benefit of adjusting any particular setting in your scenario.

These instructions and recommended settings are relevant to Windows 10 1607 (version 10.0.1393).

> **NOTE**
> Any settings not specifically mentioned in this topic can be left at their default values (or set per your requirements and policies) without appreciable impact on VDI functionality.

When you create an image to base the VDI deployment, be sure to use the **Current Branch**. For more information about Current Branch, see Windows 10 release information.

Creating the Windows 10 image

The first step is to install a reference image of Windows 10 1607 (version 10.0.1393) on either a physical or virtual machine. Installing to a virtual machine is easy and allows you to save versions of the virtual hard-disk (VHD) file, in case you want to roll back to an earlier version.

During installation, you can choose either **Express Settings** or **Customize**. The settings offered during the **Customize** option are adjustable by using Group Policy, so the method of installing the base OS is not that important.

If you chose **Customize**, you can adjust these settings during installation:

In "Customize settings"

You can also adjust these after installation with Group Policy Editor; see the "Group Policy settings" section of this topic.

SETTING	DEFAULT VALUE	RECOMMENDED VALUE FOR VDI USE
Personalization		

SETTING	DEFAULT VALUE	RECOMMENDED VALUE FOR VDI USE
Personalize your speech, typing, and inking input by sending your input data to Microsoft.	On	Off
Send typing and inking data to Microsoft to improve the recognition and suggestion platform.	On	Off
Let apps use your advertising ID for experience across apps.	On	Off
Let Skype (if installed) help you connect with friends in your address book and verify your mobile number. SMS and data charges may apply.	On	Off
Location		
Turn on Find My Device and let Windows and apps request your location, including location history	On	Off
Connectivity and error reporting		
Automatically connect to suggested open hotspots. Not all networks are secure.	On	Off
Automatically connect to open hotspots temporarily to see if paid network services are available.	On	Off
Send full diagnostic and usage data to Microsoft. Turning this off sends only basic data.	On	Off
Browser, protection, and update		
Use SmartScreen online services to help protect against malicious content and downloads in sites loaded by Windows browsers and Store apps	On	On (If there is no Internet access, then set to Off.)
Use page prediction to improve reading, speed up browsing, and make your overall experience better in Windows browsers. Your browsing data will be sent to Microsoft.	On	Off
Get updates from and send updates to other PCs on the Internet to speed up app and Windows Update downloads	On	Off

Once installation is complete, you can continue adjusting settings starting with **Windows Settings**.

In Windows Settings

To access Windows Settings, click **Start** (the Windows icon on the taskbar), and then click the **Settings** icon (shaped like a gear).

In the "System" area of Windows Settings

In Windows Settings area, clicking the **System** icon gives you access to a number of system-related settings. Not all of them need adjustment for optimum VDI use--these settings are the most important:

Apps and features

To remove an app, thereby excluding it from your VDI image, click the app, and then click **Uninstall**. If **Uninstall** is grayed out, you cannot remove it by this method; you might be able to remove it with Windows PowerShell, or try these steps:

1. Click **Manage optional features** (immediately below the **Apps and features** heading on the same page).
2. Click the optional feature, and then click **Uninstall**.

Features to consider removing (if present) include the following:

- **Contact support**
- **English (United States) Retail Demo Content**
- **Neutral Retail Demo Content**
- **Quick Assist**

Default apps

This area defines the app to be used by default for certain generic functions such as e-mail, web browsing, and maps. If you want a different app to be used for a particular function, click the current entry, and then click the app you prefer to be used in the VDI image. For a non-Microsoft app to be an available choice, you must install the app prior to adjusting this setting.

Notifications and actions

These recommended values will reduce notifications and background network activity in a VDI environment:

SETTING	DEFAULT VALUE	RECOMMENDED VALUE FOR VDI USE
Get notifications from apps and other senders	On	Off
Show notifications on the lock screen.	On	Off
Show alarms, reminders, and incoming VoIP calls on the lock screen.	On	Off
Show tips, tricks, and suggestions as you use Windows.	On	Off

Offline maps

This setting is only applicable if the Maps app is installed. Its default value is **On**; for VDI use the recommended value is **Off**.

Tablet mode

SETTING	DEFAULT VALUE	RECOMMENDED VALUE FOR VDI USE
When I sign in	Use the appropriate mode for my hardware	Use desktop mode

SETTING	DEFAULT VALUE	RECOMMENDED VALUE FOR VDI USE
When this device automatically switches mode on or off	Always ask me before switching	Don't ask me and don't switch
Hide app icons on the taskbar in tablet mode	On	Off

In the "Devices" area of Windows Settings

In Windows Settings area, clicking the **Devices** icon gives you access to a number of system-related settings. Not all of them need adjustment for optimum VDI use--these settings are the most important:

Autoplay

SETTING	DEFAULT VALUE	RECOMMENDED VALUE FOR VDI USE
Use Autoplay for all media and devices	On	Off
Removable drive:	Choose a default	Take no action
Memory card	Choose a default	Take no action

In the "Personalization" area of Windows Settings

In Windows Settings area, clicking the **Personalization** icon gives you access to a number of system-related settings. Not all of them need adjustment for optimum VDI use--these settings are the most important:

Background

Sometimes the default black background can cause users to think the computer is not responding. Changing the background color can help make it clearer. To do this, follow these steps:

1. In the **Background** area, click the pulldown menu.
2. To change the background color, click **Solid color**, and then click any of the colors other than black. Alternately, you could click **Picture** and then select an image to use as the background.

Start

SETTING	DEFAULT VALUE	RECOMMENDED VALUE FOR VDI USE
Occasionally show suggestions in Start	On	Off
Show most used apps	On	Off
Show recently added apps	On	Off
Show recently opened items in Jump Lists on Start or the Taskbar	On	Off

Taskbar

The default setting is to use large taskbar buttons (that is, a value of "Off" for **Use small taskbar buttons**). This setting causes the Cortana item to use a lot of taskbar area. To avoid this, set **Use small taskbar buttons** to "On." If you prefer that the taskbar items stay larger, but prefer not to have Cortana taking up so much space, right-click the taskbar, point to **Cortana**, and in the menu that flies out, select **Hidden**.

In the "Privacy" area of Windows Settings

In Windows Settings area, clicking the **Privacy** icon gives you access to a number of system-related settings. Not

all of them need adjustment for optimum VDI use--these settings are the most important:

General

Some of these settings are also set from the "Customize settings" window, discussed at the beginning of this topic.

SETTING	DEFAULT VALUE	RECOMMENDED VALUE FOR VDI USE
Let apps use my advertising ID for experiences across apps (turning this off will reset your ID)	On	Off
Let websites provide locally relevant content by accessing my language list	On	Off
Let apps on my other devices open apps and continue experiences on this device	On	Off

Camera

The default value for "Let apps use my camera" is **On**; for VDI use the recommended value is **Off**.

Microphone

The default value for "Let apps use my microphone" is **On**; for VDI use the recommended value is **Off**.

Notifications

The default value for "Let apps access my notifications" is **On**; for VDI use the recommended value is **Off**.

Contacts

The default value for "Let apps access my contacts" is **On**; for VDI use the recommended value is **Off**.

Calendar

The default value for "Let apps access my calendar" is **On**; for VDI use the recommended value is **Off**.

Call history

The default value for "Let apps access my call history" is **On**; for VDI use the recommended value is **Off**.

Email

The default value for "Let apps access and send email" is **On**; for VDI use the recommended value is **Off**.

Messaging

The default value for "Let apps read or send messages (text or MMS)" is **On**; for VDI use the recommended value is **Off**.

Radios

The default value for "Let apps control radios" is **On**; for VDI use the recommended value is **Off**.

Other devices

The default value for "Let your apps automatically share and sync info with wireless devices that don't explicitly pair with your PC, tablet, or phone" is **On**; for VDI use the recommended value is **Off**.

Feedback and diagnostics

The default value for "Windows should ask for my feedback" is **Automatically**; for VDI use, the recommended value is **Never**.

Background apps

Listed apps have a default value of **On**, which allows them to receive information, send notifications, and update themselves whether they are being used or not. You should disable (set to **Off**) any apps you don't want running in the background in the VDI image.

Update and security

Windows Update

In the **Update settings** area, click **Advanced options** to adjust these settings:

SETTING	DEFAULT VALUE	RECOMMENDED VALUE FOR VDI USE
Give me updates for other Microsoft products when I update Windows	cleared	selected
Defer feature updates	cleared	selected
Use my sign in info to automatically finish setting up my device after an update	cleared	Depends on specific VDI configuration

On the **Advanced options** page, click **Choose how updates are delivered** to access the setting for "Updates from more than one place." The default value is **On**; for VDI use the recommended value is **Off**.

In Control Panel and other system utilities

The settings in this section are adjustable either by navigating through Control Panel or opening the utility directly.

> **NOTE**
> Any settings not specifically mentioned in this topic can be left at their default values (or set per your requirements and policies) without appreciable impact on VDI functionality.

Task Scheduler

The fastest way to open Task Scheduler is to push the Windows button and type *task scheduler* or *taskschd.msc*. In the results that return, click **Task Scheduler** to open the utility. In Task Scheduler, expand **Task Scheduler Library**, expand **Microsoft**, and then expand **Windows**. You now have access to the list of task collections. To change the state of each scheduled task, right-click it, and then click the desired state (typically, **Disabled** for VDI use).

TASK COLLECTION	TASK NAME	DEFAULT STATE	RECOMMENDED STATE FOR VDI USE
Customer Experience Improvement Program			
	Consolidator	Enabled	Disabled
	KernelCeipTask	Enabled	Disabled
	UsbCeip	Enabled	Disabled
Defrag			
	ScheduledDefrag	Enabled	Disabled
Location			
	Notifications	Enabled	Disabled
	WindowsActionDialog	Enabled	Disabled

TASK COLLECTION	TASK NAME	DEFAULT STATE	RECOMMENDED STATE FOR VDI USE
Maintenance			
	WinSAT	Enabled	Disabled
Maps			
	MapsToastTask	Enabled	Disabled
	MapsUpdateTask	Enabled	Disabled
Mobile Broadband Accounts			
	MNO Metadata Parser	Enabled	Disabled
Power Efficiency Diagnostics			
	Analyze System	Enabled	Disabled
Recovery Environment			
	VerifyWinRE	Enabled	Disabled
Retail Demo			
	CleanupOfflineContent	Enabled	Disabled
Shell			
	FamilySafetyMonitor	Enabled	Disabled
	FamilySafetyRefreshTask	Enabled	Disabled
Windows Error Reporting			
	QueueReporting	Enabled	Disabled
Windows Media Sharing			
	UpdateLibrary	Enabled	Disabled

Click **Windows** again to collapse it, then click **XblGameSave**. This gives you access to the tasks **XBLGameSaveTask** and **XBLGameSaveTaskLogon**; both of these can be set to **Disabled**.

Performance Monitor

The fastest way to open Performance Monitor is to push the Windows button and type *performance monitor* or *perfmon.msc*. In the results that return, click **Performance Monitor**. In Performance Monitor, click **Data Collector Sets** and then double-click **Event Trace Sessions**. Right-click **WiFiSession**; if it is in the default state of **Running**, then click **Stop**.

Click **StartupEventTraceSessions**, then right-click **ReadyBoot**; if it is running, click **Stop**. Click **Event Trace Sessions**, right-click **ReadyBoot**, and then click **Properties**. In the dialog that opens, click the **Trace Session** tab.

Clear the **Enabled** check box.

Services

The fastest way to manage Services is to push the Windows button and type *services*. In the results that return, click **Services**. The following services are good candidates to disable for use in VDI scenarios; however, you might need to do some testing to verify that they aren't needed for your purposes. To disable a service, in the **Services** snap-in, right-click the service name, and then click **Properties**. On the **General** tab, click the **Startup type** pulldown menu, and then click **Disabled**. Click **OK**.

- BranchCache
- Delivery Optimization
- Diagnostic Service Host
- Windows Mobile Hotspot Service
- Xbox Live Auth Manager
- Xbox Live Game Save
- Xbox Live Networking Service

File Explorer Options

Push the Windows button and type *control panel*. In the results that return, click **Control Panel**. In Control Panel, click **File Explorer Options**. In the dialog that opens, click the **Search** tab, and then in the **When searching non-indexed locations** area, clear the check box for **Include system directories**. Click **OK** to save.

Flash settings

Push the Windows button and type *control panel*. In the results that return, click **Control Panel**. In Control Panel, click **Flash Player** to open the Flash Player Settings Manager. On the **Storage** tab, select the radio button for **Block all sites from storing information on this computer**. In the dialog that opens, click **OK**.

On the **Camera and Mic** tab, in the **Camera and Microphone Settings** area, select the radio button for **Block all sites from using the camera and microphone**.

On the **Playback** tab, in the **Peer-assisted Networking** area, select the radio button for **Block all sites from using peer-assisted networking**. Close the Flash Player Settings Manager.

Internet Options

Push the Windows button and type *control panel*. In the results that return, click **Control Panel**. In Control Panel, click **Internet Options** to open Internet Properties. In the **Home page** area, enter the URL for the web site you want users to see as the home page in browsers. This could be a web site for your company or you can set it to a blank home page by entering *about:blank*.

In the **Browsing history** area, select the check box for **Delete browsing history on exit**.

Power Options

Push the Windows button and type *control panel*. In the results that return, click **Control Panel**. In Control Panel, click **Power Options** to open the Power Options control panel. In the **Choose or customize a power plan** area, click the down arrow for **Show additional plans**, and then select the radio button for **High performance**. This setting will have very little impact on the VDI host.

System

Push the Windows button and type *control panel*. In the results that return, click **Control Panel**. In Control Panel, click **System** to open the System control panel. In the left pane, click **Advanced system settings**. In the dialog that opens, click the **Advanced** tab. In the **Performance** area, click the **Settings** button, then on **Visual Effects** tab in the dialog that opens, select the **Adjust for best performance** radio button. Click **OK** to save and exit.

Group Policy settings

To edit Group Policy settings, press the Windows button and type *group policy* or *gpedit.msc*. In the results that return, click **Edit group policy** to open Local Group Policy Editor.

> **NOTE**
> Any settings not specifically mentioned in this topic can be left at their default values (or set per your requirements and policies) without appreciable impact on VDI functionality.

Under **Computer Configuration**, expand **Windows Settings**, and then expand **Security Settings**. Click **Network List Manager Policies**, and then double-click **All Networks**. In the dialog that opens, in the **Network location** area, select the radio button for **User cannot change location**. Click the **OK** button to save.

Collapse **Windows Settings**, and then expand **Administrative Templates**. Click or expand **Network**, and then adjust each setting as follows by double-clicking it, then selecting the radio button for the indicated value and clicking the **OK** button:

SETTING AREA	SETTING	RECOMMENDED VALUE FOR VDI USE
Background Intelligent Transfer Service (BITS)		
	Do not allow the BITS client to use Windows Branch Cache	Enabled
	Do not allow the computer to act as a BITS Peercaching client	Enabled
	Do not allow the computer to act as a BITS Peercaching server	Enabled
	Allow BITS Peercaching	Disabled
BranchCache		
	Turn on BranchCache	Disabled
Hotspot Authentication		
	Enable Hotspot Authentication	Disabled
Microsoft Peer-to-Peer Networking Services		
	Turn off Microsoft Peer-to-Peer Networking Services	Enabled
Offline Files		
	Allow or Disallow use of the Offline Files feature	Disabled

Collapse **Network**, and then expand **System**. Adjust each setting as follows double-clicking it, then selecting the radio button for the indicated value and clicking the **OK** button:

SETTING AREA	SETTING	RECOMMENDED VALUE FOR VDI USE
Device Installation		
	Do not send a Windows error report when a generic driver is installed on a device	Enabled
	Prevent creation of a system restore point during device activity that would normally prompt creation of a restore point	Enabled
	Prevent device metadata retrieval from the Internet	Enabled
	Prevent Windows from sending an error report when a device driver requests additional software during installation	Enabled
	Turn off "Found New Hardware" balloons during device installation	Enabled

Expand **Filesystem**, double-click **NTFS**, double-click **Short name creation options**, select the radio button for **Enabled**, and then use the **Options** pulldown menu to select **Enable on all volumes**. Click the **OK** button to save.

Collapse **Filesystem**, and then expand **Internet Communication Management**. Click **Internet Communication settings**. Adjust each setting as follows by double-clicking it, then selecting the radio button for **Enabled**, and then clicking the **OK** button:

- Turn off Event Viewer "Events.asp" links
- Turn off handwriting personalization data sharing
- Turn off handwriting recognition error reporting
- Turn off Help and Support Center "Did you know?" content
- Turn off Help and Support Center Microsoft Knowledge Base search
- Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com
- Turn off Internet download for Web publishing and online ordering wizards
- Turn off Internet File Association service
- Turn off Registration if URL connection is referring to Microsoft.com
- Turn off the "Order Prints" picture task
- Turn off the "Publish to Web" task for files and folders
- Turn off the Windows Messenger Customer Experience Improvement Program
- Turn off Windows Customer Experience Improvement Program
- Turn off Windows Error Reporting
- Turn off Windows Update device driver searching

Click **Power Management** and then double-click **Select an active power plan**. Select the radio button for **Enabled**, and then use the **Options** pulldown menu to select **High Performance**. Click the **OK** button to save.

Click **Recovery**, and then double-click **Allow restore of system to default state**. Select the radio button for **Enabled**, and then click the **OK** button to save.

Expand **Troubleshooting and Diagnostics**. Click **Scheduled Maintenance**, double-click **Configure Scheduled**

Maintenance Behavior, and then select the radio button for **Disabled**. Click the **OK** button to save.

For each of the following settings areas, click it, then double-click **Configure Scenario Execution Level**, select the radio button for **Disabled**, and then click the **OK** button to save:

- Windows Boot Performance Diagnostics
- Windows Memory Leak Diagnostics
- Windows Resource Exhaustion Detection and Resolution
- Windows Shutdown Performance Diagnostics
- Windows Standby/Resume Performance Diagnostics
- Windows System Responsiveness Performance Diagnostics

Collapse **System**, and then expand **Windows Components**. Adjust each setting as follows by double-clicking it, then selecting the radio button for the indicated value and clicking the **OK** button:

SETTING AREA	SETTING	RECOMMENDED VALUE FOR VDI USE
Add features to Windows 10		
	Prevent the wizard from running	Enabled
Autoplay Policies		
	Set the default behavior for AutoRun	Enabled, then use the **Options** pulldown menu to select **Do not execute any autorun commands**
Cloud Content		
	Do not show Windows tips	Enabled
	Turn off Microsoft consumer experiences	Enabled
Data Collection and Preview Builds		
	Allow Telemetry	Enabled, then use the **Options** pulldown menu to select **1- Basic**
	Disable pre-release features or settings	Disabled
	Do not show feedback notifications	Enabled
	Toggle user control over Insider builds	Disabled
Desktop Window Manager		
	Do not allow Flip3D invocation	Enabled
	Do not allow window animations	Enabled
	Use solid color for Start background	Enabled
Edge UI		

SETTING AREA	SETTING	RECOMMENDED VALUE FOR VDI USE
	Allow edge swipe	Disabled
	Disable help tips	Enabled
File Explorer		
	Do not show the 'new application installed' notification	Enabled
Game Explorer		
	Turn off downloading of game information	Enabled
	Turn off game updates	Enabled
	Turn off tracking of last play time of games in the Games folder	Enabled
Homegroup		
	Prevent the computer from joining a homegroup	Enabled
Internet Explorer		
	Allow Microsoft services to provide enhanced suggestions as the user types in the Address bar	Disabled
	Disable Periodic Check for Internet Explorer software updates	Enabled
	Disable showing the splash screen	Enabled
	Install new versions of Internet Explorer automatically	Disabled
	Prevent participation in the Customer Experience Improvement Program	Enabled
	Prevent running First Run wizard Go directly to home page	Enabled, then use the **Options** pulldown menu to select **Go directly to home page**
	Set tab process growth	Enabled, then type the following in the **Tab Process Growth** box: *Low*.
	Specify default behavior for a new tab	Enabled, then use the **Options** pulldown menu to select **New tab page**

SETTING AREA	SETTING	RECOMMENDED VALUE FOR VDI USE
	Turn off add-on performance notifications	Enabled
	Turn off browser geolocation	Enabled
	Turn off Reopen Last Browsing Session	Enabled
	Turn off suggestions for all user-installed providers	Enabled
	Turn on Suggested Site	Disabled

At the same level as the **Internet Explorer** settings you just adjusted in the preceding table, note another level of folders ranging from **Accelerators** to **Toolbars**. In other words, you are now at Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Internet Explorer.

Open the **Delete Browsing History** folder, double-click **Allow deleting browsing history on exit**, select **Enable**, and then click **OK** to save and exit.

Use the back arrow in the upper left of Local Group Policy Editor to go back to the **Internet Explorer** level. Double-click **Internet Settings**, double-click **Advanced Settings**, and then adjust the settings in the subfolders as follows:

SETTING FOLDER UNDER ADVANCED SETTINGS	SETTING	RECOMMENDED VALUE FOR VDI USE
Browsing		
	Turn off phone number detection	Enabled
Multimedia		
	Allow Internet Explorer to play media files that use alternative codecs	Disabled

Go back up to the level of **Internet Explorer**, then double-click **Internet Settings**. In this folder, set these two settings under **AutoComplete** to **Enabled**:

- Turn off URL Suggestions
- Turn off Windows Search AutoComplete

Go back up four levels to **Windows Components**, double-click **Location and Sensors**, and then set these three settings to **Enabled** (for each, click **OK** to save and exit):

- Turn off location
- Turn off location scripting
- Turn off sensors

While at the level of **Location and Sensors**, double-click **Windows Location Provider** and set **Turn off Windows Location Provider** to **Enabled**. Click **OK** to save and exit.

In the left pane, click **Maps**, set these settings to **Enabled**; for each, then click **OK** to save and exit:

- Turn off Automatic Download and Update of Map Data

- Turn off unsolicited network traffic on the Offline Maps settings page

Using the left pane, enter each of the following settings subfolders and adjust the individual settings as follows:

SETTINGS FOLDER UNDER WINDOWS COMPONENTS	SETTING	RECOMMENDED VALUE FOR VDI USE
OneDrive		
	Prevent the usage of OneDrive for file storage	Enabled
	Save documents to OneDrive by default	Disabled
RSS Feeds		
	Prevent automatic discovery of feeds and Web Slices	Enabled
Search		
	Allow Cortana	Disabled
	Allow Cortana above lock screen	Disabled
	Allow search and Cortana to use location	Disabled
	Do not allow web search	Enabled
	Don't search the web or display web results in Search	Enabled
	Prevent adding UNC locations to index from Control Panel	Enabled
	Prevent indexing files in offline files cache	Enabled
Store		
	Turn off the offer to update to the latest version of Windows	Enabled
Windows Error Reporting		
	Automatically send memory dumps for OS-generated error reports	Disabled
	Disable Windows Error Reporting	Enabled
Windows Installer		

SETTINGS FOLDER UNDER WINDOWS COMPONENTS	SETTING	RECOMMENDED VALUE FOR VDI USE
	Control maximum size of baseline file cache	Enabled, then use the spinbox in the **Options** area to set **Baseline file cache maximum size** to *5*.
	Turn off creation of System Restore checkpoints	Enabled
Windows Mail		
	Turn off the communities feature	Enabled
Windows Media Player		
	Do Not Show First Use Dialog Boxes	Enabled
	Prevent Media Sharing	Enabled
Windows Mobility Center		
	Turn off Windows Mobility Center	Enabled
Windows Reliability Analysis		
	Configure Reliability WMI Providers	Disabled
Windows Update		
	Allow Automatic Updates immediate installation	Enabled
	Remove access to all Windows Update features	Enabled
In the **Windows Update** folder, open **Defer Windows Update**		
	Select when feature updates are received	Enabled, then in the **Options** area, use the **Select the branch readiness level for the feature updates you want to receive** pulldown menu to select **Current Branch for Business**. Set the **After a feature update is released, defer receiving it for this many days** spinbox to *180 days*.
	Select when Quality Updates are received	Enabled, then in the **Options** area, Set the **After a quality update is released, defer receiving it for this many days** spinbox to *30 days* and select the check box for **Pause quality updates**.

In the left pane of Local Group Policy Editor, click **User Configuration**. Using the left pane, click **Administrative**

Templates and then enter each of the following settings subfolders and adjust the individual settings as follows:

SETTINGS FOLDER UNDER ADMINISTRATIVE TEMPLATES	SETTING	RECOMMENDED VALUE FOR VDI USE
Desktop		
	Do not add shares of recently opened documents to Network Locations	Enabled
In the **Desktop** folder, open **Active Directory**		
	Maximum size of Active Directory searches	Enabled, then in the **Options** area, use the spinbox to set **Number of objects returned** to *5000*.
Start Manu and Taskbar		
	Clear the recent programs list for new users	Enabled
	Do not display or track items in Jump Lists from remote locations	Enabled
	Turn off feature advertisement balloon notifications	Enabled
	Turn off user tracking	Enabled
In the **Start Menu and Taskbar** folder, open **Notifications**		
	Turn off toast notifications	Enabled
In the **Windows Components** folder, open:		
Cloud Content		
	Turn off all Windows spotlight features	Enabled
File Explorer		
	Turn off caching of thumbnail pictures	Enabled
	Turn off display of recent search entries in the File Explorer search box	Enabled
	Turn off the caching of thumbnails in hidden thumbs.db file	Enabled

Microsoft Store apps

There are a number of Microsoft Store apps that you might want to remove from the VDI image; removing them

will decrease CPU usage and conserve disk space. Good candidates for removal include:

- Get Office
- Skype (preview)
- Get Started (especially if there is no Internet connection)
- Feedback Hub
- Microsoft Solitaire Collection
- Paid Wi-Fi and Cellular

To customize the default user profile used for creating VDI images, use the built-in Administrator account. If it is not already enabled, do so by using Local Users and Groups in Computer Management. Then log in to the Administrator account to complete the following steps.

> **NOTE**
> Don't remove system apps such as the Store app. They are difficult to reinstall. Other apps are easily reinstallable from the Store.

Delete unwanted apps from the Administrator user profile

1. In Windows PowerShell, run `Get-AppxPackage | ft PackageFamilyName` to see the list of installed apps.
2. For each app packager you want to uninstall run cmdlets of this example format:

   ```
   Get-AppxPackage *messaging* | Remove-AppxPackage
   ```

   ```
   Get-AppxPackage *WindowsMaps* | Remove-AppxPackage
   ```

   ```
   Get-AppxPackage *ZuneMusic* | Remove-AppxPackage
   ```

Delete the payload of unwanted Store apps

This will prevent the apps from being reinstalled.

1. List Store apps and other items that have provisioned data in storage with this cmdlet: `Get-AppxProvisionedPackage -Online`.
2. Remove a given package with `Remove-AppxProvisionedPackage -Online -PackageName MyAppPackage`, using the appropriate MyAppPackage returned from Step 1. For example, to remove the Zune-related package, you would run

   ```
   Remove-AppxProvisionedPackage -Online -PackageName
   Microsoft.ZuneMusic_2019.17012.10311.0_neutral_~_8wekyb3d8bbwe
   ```

   .

Removing other items

You can remove the OneDrive icon and app, turn off system icons, and delete downloaded updates.

Remove OneDrive icon and app

1. Click **Start** and scroll to the **OneDrive** icon.
2. Right-click the **OneDrive** icon, point to **More**, and then click **Open file location**.
3. Right-click the **OneDrive** icon in its file location, and click **Delete**.

To remove the OneDrive app:

1. Click **Start** and scroll to the **OneDrive** icon.
2. Right-click the **OneDrive** icon, and then click **Uninstall**. Programs and Features opens.
3. In Programs and Features, right-click **Microsoft OneDrive** and click **Uninstall**.

Programs and Features (from previous versions of Control Panel)

1. Push the **Start** button, type *Control*, and then press ENTER.
2. Tap or double-click **Programs and Features**.
3. On the far left, under **Control Panel Home**, tap or click **Turn Windows features on or off**. A new user interface will open.
4. Clear the check boxes for any items that you do not want or need in the base image, for example: **SMB 1.0/CIFS File Sharing Support**.

Turn system icons off

1. Push or click **Start**, and then click **Settings** (the gear icon).
2. In the **Find a Setting** text area, type *Taskbar*, and then click **Taskbar Settings**.
3. Under the **Taskbar** section, scroll or swipe down to the **Notification area** section.
4. Click or tap **Turn system icons on or off**, and then turn each system icon on or off as you prefer for the image.

Delete downloaded updates

1. Using File Explorer, navigate to **C:\Windows\Software Distribution\Download**.
2. Delete all files and folders in that directory.

Optimizing Windows 10, version 1803, for a Virtual Desktop Infrastructure (VDI) role

1/14/2020 • 47 minutes to read • Edit Online

This article helps you choose settings for Windows 10, version 1803 (build 17134) that should result in the best performance in a Virtualized Desktop Infrastructure (VDI) environment. All settings in this guide are *recommendations to be considered* and are in no way requirements.

In a VDI environment the key ways to optimize Windows 10 performance are to minimize app graphic redraws, background activities that have no major benefit to the VDI environment, and generally reduce running processes to the bare minimum. A secondary goal is to reduce disk space usage in the base image to the bare minimum. With VDI implementations, the smallest possible base, or "gold" image size, can slightly reduce memory usage on the hypervisor, as well as a small reduction in overall network operations required to deliver the desktop image to the consumer.

> **NOTE**
> Settings recommended here can be applied to other installation of Windows 10, version 1803, including those on physical or other virtual devices. No recommendations in this topic should affect the supportability of Windows 10, version 1803.

> **TIP**
> A script that implements the optimizations discussed in this topic--as well as a GPO export file that you can import with **LGPO.exe**--is available at TheVDIGuys on GitHub.

VDI optimization principles

A VDI environment presents a full desktop session, including applications, to a computer user over a network. VDI environments usually use a base operating system image, which then becomes the basis for the desktops subsequently presented to the users for work. There are variations of VDI implementations such as "persistent", "non-persistent", and "desktop session." The persistent type preserves changes to the VDI desktop operating system from one session to the next. The non-persistent type does not preserve changes to the VDI desktop operating system from one session to the next. To the user this desktop is little different than other virtual or physical device, other than it is accessed over a network.

The optimization settings would take place on a reference device. A VM is an ideal place to build the image, because you can save the state, make checkpoints and backups can be made, and other useful tasks. Start by installing default operating system on the base VM, and then optimize the base VM for VDI use by removing unneeded apps, installing Windows updates, installing other updates, deleting temporary files, applying settings, etc.

There are other types of VDI such as persistent and Remote Desktop Services (RDS). An in-depth discussion regarding these technologies is outside the scope of this topic, which focuses on the Windows base image settings with reference to other factors in the environment such as host optimization.

Persistent VDI

Persistent VDI is, at the basic level, a VM that saves operating system state in between restarts. Other software layers of the VDI solution provide the users easy and seamless access to their assigned VMs, often with a single

sign-on solution.

There are several different implementations of persistent VDI:

- Traditional virtual machine, where the VM has its own virtual disk file, starts up normally, saves changes from one session to the next, and is essentially just a normal VM. The difference is how the user accesses this VM. There might be a web portal the user logs into that automatically directs the user to their one or more assigned VDI VMs.
- Image-based persistent virtual machine, with personal virtual disks. In this type of implementation there is a base/gold image on one or more host servers. A VM is created, and one or more virtual disks are created and assigned to this disk for persistent storage.
    - When the VM is started, a copy of the base image is read into the memory of the VM. At the same time, a persistent virtual disk assigned to that VM, with any previous operating system changes merged through a complex process.
    - Changes such as event log writes, log writes, etc. are redirected to the read/write virtual disk assigned to that VM.
    - In this circumstance, operating system and app servicing might operate normally, using traditional servicing software such as Windows Server Update Services or other management technologies.

Non-Persistent VDI

When a non-persistent VDI implementation is based on a base or "gold" image, the optimizations are mostly performed in the base image, and then through local settings and local policies.

With image-based non-persistent VDI, the base image is read-only. When a non-persistent VDI VM is started, a copy of the base image is streamed to the VM. Activity that occurs during startup and thereafter until the next reboot is redirected to a temporary location. Usually the users are provided network locations to store their data. In some cases, the user's profile is merged with the standard VM to provide the user their settings.

One important aspect of non-persitent VDI that is based on a single image is servicing. Updates to the operating system are delivered usually once per month. With image-based VDI, there is a set of processes to perform in order to get updates to the image:

- On a given host, all the VMs on that host that are derived from the base image must be shut down or turned off. This means the users are redirected to other VMs.
- The base image is then opened and started up. All maintenance activities are then performed, such as operating system updates, .NET updates, app updates, etc.
- Any new settings that need to be applied are applied at this time.
- Any other maintenance is performed at this time.
- The base image is then shut down.
- The base image is sealed and set to go back into production.
- Users are allowed to log back on.

NOTE

Windows 10 performs a set of maintenance tasks automatically, on a periodic basis. There is a scheduled task that is set to run at 3:00 AM local time every day by default. This scheduled task performs a list of tasks, including Windows Update cleanup. You can view all the categories of maintenance that take place automatically with this PowerShell command:

```
Get-ScheduledTask | ? {$_.Settings.MaintenanceSettings}
```

One of the challenges with non-persistent VDI is that when a user logs off, nearly all the operating system activity is discarded. The user's profile and or state might be saved, but the virtual machine itself discards nearly all changes that were made since the last boot. Therefore, optimizations intended for a Windows computer that saves state from one session to the next are not applicable.

Depending on the architecture of VDI VM, things like PreFetch and SuperFetch are not going to help from one session to the next, as all the optimizations are discarded on VM restart. Indexing might be a partial waste of resources, as would be any disk optimizations such as a traditional defragmentation.

To Sysprep or not Sysprep

Windows 10 has a built-in capability called the System Preparation Tool, (often abbreviiated to "Sysprep"). The Sysprep tool is used to prepare a customized Windows 10 image for duplication. The Sysprep process assures the resulting operating system is properly unique to run in production.

There are reasons for and against running Sysprep. In the case of VDI, you might want the ability to customize the default user profile which would be used as the profile template for subsequent users that log on using this image. You might have apps that you want installed, but also able to control per-app settings.

The alternative is to use a standard .ISO to install from, possibly using an unattended installation answer file, and a task sequence to install applications or remove applications. You can also use a task sequence to set local policy settings in the image, perhaps using the Local Group Policy Object Utility (LGPO) tool.

VDI Optimization Categories

- Global operating system settings
  - UWP app cleanup
  - Optional Features cleanup
  - Local policy settings
  - System services
  - Scheduled tasks
  - Apply Windows updates
  - Automatic Windows traces
  - Disk cleanup prior to finalizing (sealing) image
- User settings
- Hypervisor/Host settings

Global VDI operating system optimization

Global VDI settings include the following:

- Universal Windows Platform (UWP) app cleanup
- Clean up optional features

- Local policy settings
- System services
- Scheduled tasks
- Apply Windows and other updates
- Automatic Windows traces
- Windows Defender optimization with VDI
- Tuning Windows 10 network performance by using registry settings
- Additional settings from the Windows Restricted Traffic Limited Functionality Baseline guidance.
- Disk cleanup

Universal Windows Platform app cleanup

One of the goals of a VDI image is to be as small as possible. One way to reduce the size of the image is to remove UWP applications that will not be used in the environment. With UWP apps, there are the main application files, also known as the payload. There is a small amount of data stored in each user's profile for application specific settings. There is also a small amount of data in the All Users profile.

Connectivity and timing are everything when it comes to UWP app cleanup. If you deploy your base image to either a device with no network connectivity, Windows 10 cannot connect to the Microsoft Store and download apps and try to install them while you are trying to uninstall them.

If you modify your base .WIM that you use to install Windows 10 and remove unneeded UWP apps from the .WIM before you install, the apps will not be installed to begin with and your profile creation times should be shorter. Later in this section, you'll find information on how to remove UWP apps from your installation .WIM file.

A good strategy for VDI is to provision the apps you want in the base image, then limit or block access to the Microsoft Store afterward. Store apps are updated periodically in the background on normal computers. The UWP apps can be updated during the maintenance window when other updates are applied.

Delete the payload of UWP apps

UWP apps that are not needed are still in the file system consuming a small amount of disk space. For apps that will never be needed, the payload of unwanted UWP apps can be removed from the base image using PowerShell commands.

In fact, if you remove those from the installation .WIM file using the links provided later in this section, you should be able to start from the beginning with a very slim list of UWP apps.

Run the following command to enumerate provisioned UWP apps from a running Windows 10 operating system, as in this truncated example output from PowerShell:

```
Get-AppxProvisionedPackage -Online

DisplayName  : Microsoft.3DBuilder
Version      : 13.0.10349.0
Architecture : neutral
ResourceId   : \~
PackageName  : Microsoft.3DBuilder_13.0.10349.0_neutral_\~_8wekyb3d8bbwe
Regions      :
...
```

UWP apps that are provisioned to a system can be removed during operating system installation as part of a task sequence, or later after the operating system is installed. This might be the preferred method because it makes the

overall process of creating or maintaining an image modular. Once you develop the scripts, if something changes in a subsequent build you edit an existing script rather than repeat the process from scratch. Here are some links to information on this topic:

Removing Windows 10 in-box apps during a task sequence

Removing Built-in apps from Windows 10 WIM-File with Powershell - Version 1.3

Windows 10 1607: Keeping apps from coming back when deploying the feature update

Then run the Remove-AppxProvisionedPackage PowerShell command to remove UWP app payloads:

```
Remove-AppxProvisionedPackage -Online -PackageName
```

Each UWP app should be evaluated for applicability in each unique environment. You will want to install a default installation of Windows 10, version 1803, then note which apps are running and consuming memory. For example, you might want to consider removing apps that start automatically, or apps that automatically display information on the Start menu, such as Weather and News, and that might not be of use in your environment.

One of the "inbox" UWP apps called Photos, has a default setting called **Show a notification when new albums are available**. The Photos app can use approximately 145 MB of memory; specifically private working set memory, even if not being used. Changing the **Show a notification when new albums are available** setting for all users is not practical at this time, hence the recommendation to remove the Photos app if it is not needed or desired.

Clean up optional features

Managing optional features with PowerShell

To enumerate currently installed Windows Features, run this PowerShell command:

```
Get-WindowsOptionalFeature -Online
```

You can enable or disable a specific Windows optional feature as in this example:

```
Enable-WindowsOptionalFeature -Online -FeatureName "DirectPlay" -All
```

For more about this, see Windows 10: Managing optional features with PowerShell.

Enable or disable Windows features by using DISM

You can use the built-in **Dism.exe** tool to enumerate and control Windows optional features. You can set up a Dism.exe script to run during a task sequence that installs the operating system.

Local policy settings

Many optimizations for Windows 10 in a VDI environment can be made using Windows policy. The settings listed here can be applied locally to the base image. Then if the equivalent settings are not specified in any other way such as by group policy, the settings would still apply.

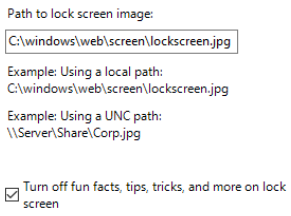
Some decisions might be based on the specifics of the environment, for example:

- Is the VDI environment allowed to access the Internet?
- Is the VDI solution persistent or non-persistent?

The following settings specifically do not counter or conflict with any setting that has anything to do with security. These settings were chosen to remove settings that might not be applicable to VDI environments.

NOTE

In this table of group policy settings, items marked with an asterisk are from the Windows Restricted Traffic Limited Functionality Baseline.

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
Local Computer Policy \ Computer Configuration \ Windows Settings \ Security Settings			
Network List Manager Policies	All Networks Properties	Network Location	User cannot change location
Local Computer Policy \ Computer Configuration \ Administrative Templates \ Control Panel			
***Control Panel**	Allow Online Tips		Disabled (Settings will not contact Microsoft content services to retrieve tips and help content)
***Control Panel**\ Personalization	Do not display the lock screen		Enabled (This policy setting controls whether the lock screen appears for users. If you enable this policy setting, users that are not required to press CTRL + ALT + DEL before signing in will see their selected tile after locking their PC.)
***Control Panel**\ Personalization	Force a specific default lock screen and logon image		Enabled (This setting lets you specify the default lock screen and logon image shown when no user is signed in, and also sets the specified image as the default for all users--it replaces the default image.) A low resolution, non-complex image would cause less data transmitted over the network each time the image is rendered.
***Control Panel**\ Regional and Language Options\Handwriting personalization	Turn off automatic learning		Enabled (If you enable this policy setting, automatic learning stops, and any stored data is deleted. Users cannot configure this setting in Control Panel)

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
Local Computer Policy \ Computer Configuration \ Administrative Templates \ Network			
Background Intelligent Transfer Service (BITS)	Do not allow the BITS client to use Windows Branch Cache		Enabled
Background Intelligent Transfer Service (BITS)	Do not allow the computer to act as a BITS Peercaching client		Enabled
Background Intelligent Transfer Service (BITS)	Do not allow the computer to act as a BITS Peercaching server		Enabled
Background Intelligent Transfer Service (BITS)	Allow BITS Peercaching		Disabled
BranchCache	Turn on BranchCache		Disabled
***Fonts**	Enable Font Providers		Disabled (Windows does not connect to an online font provider and only enumerates locally installed fonts.)
Hotspot Authentication	Enable hotspot authentication		Disabled
Microsoft Peer-to-Peer Networking Services	Turn off Microsoft Peer-to-Peer Networking Services		Enabled
Network Connectivity Status Indicator (Note that there are other settings in this section that can be used in isolated networks)	Specify passive polling	Disable passive polling (checkbox)	Enabled (Use this setting if on an isolated network, or using static IP addresses.)
Offline Files	Allow or Disallow use of the Offline Files feature		Disabled
***TCPIP Settings**\ IPv6 Transition Technologies	Set Teredo State	Disabled State	Enabled (In the disabled state no Teredo interfaces are present on the host.)

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
***WLAN Service**\ WLAN Settings	Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services		Disabled (**Connect to suggested open hotspots**, **Connect to networks shared by my contacts**, and **Enable paid services** will be turned off and users on this device will be prevented from enabling them.)
Local Computer Policy \ Computer Configuration \ Administrative Templates \ Start Menu and Taskbar			
***Notifications**	Turn off notifications network usage		Enabled (If you enable this policy setting, applications and system features will not be able to receive notifications from the network from WNS or by using notification-polling APIs.)
Local Computer Policy \ Computer Configuration \ Administrative Templates \ System			
Device Installation	Do not send a Windows error report when a generic driver is installed on a device		Enabled
Device Installation	Prevent creation of a system restore point during device activity that would normally prompt creation of a restore point		Enabled
Device Installation	Prevent device metadata retrieval from the Internet		Enabled
Device Installation	Prevent Windows from sending an error report when a device driver requests additional software during installation		Enabled
Device Installation	Turn off **Found New Hardware** balloons during device installation		Enabled
Filesystem\NTFS	Short name creation options	Disabled on all volumes	Enabled

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
***Group Policy**	Configure web-to-app linking with app URL handlers		Disabled (Disables web-to-app linking and http(s) URIs will be opened in the default browser instead of starting the associated app.)
***Group Policy**	Continue experiences on this device		Disabled (The Windows device is not discoverable by other devices, and cannot participate in cross-device experiences.)
Internet Communication Management Internet Communication settings	Turn off access to all Windows Update features		Enabled (If you enable this policy setting, all Windows Update features are removed. This includes blocking access to the Windows Update website at https://windowsupdate.microsoft.com, from the Windows Update hyperlink on the Start menu, and also on the Tools menu in Internet Explorer. Windows automatic updating is also disabled; you will neither be notified about nor will you receive critical updates from Windows Update. This policy setting also prevents Device Manager from automatically installing driver updates from the Windows Update website.)
Internet Communication Management Internet Communication settings	Turn off Automatic Root Certificates Update		Enabled (If you enable this policy setting, when you are presented with a certificate issued by an untrusted root authority, your computer will not contact the Windows Update website to see if Microsoft has added the CA to its list of trusted authorities.) **NOTE:** Only use this policy if you have an alternate means to the latest certificate revocation list.
Internet Communication Management Internet Communication settings	Turn off Event Viewer "Events.asp" links		Enabled
Internet Communication Management Internet Communication settings	Turn off handwriting personalization data sharing		Enabled

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
Internet Communication Management\ Internet Communication settings	Turn off handwriting recognition error reporting		Enabled
Internet Communication Management\ Internet Communication settings	Turn off Help and Support Center "Did you know?" content		Enabled
Internet Communication Management\ Internet Communication settings	Turn off Help and Support Center Microsoft Knowledge Base search		Enabled
Internet Communication Management\ Internet Communication settings	Turn off Internet Connection wizard if URL connection is referring to Microsoft.com		Enabled
Internet Communication Management\ Internet Communication settings	Turn off Internet download for Web publishing and online ordering wizards		Enabled
Internet Communication Management\ Internet Communication settings	Turn off Internet File Association service		Enabled
Internet Communication Management\ Internet Communication settings	Turn off Registration if URL connection is referring to Microsoft.com		Enabled
Internet Communication Management\ Internet Communication settings	Turn off the "Order Prints" picture task		Enabled
Internet Communication Management\ Internet Communication settings	Turn off the "Publish to Web" task for files and folders		Enabled
Internet Communication Management\ Internet Communication settings	Turn off the Windows Messenger Customer Experience Improvement Program		Enabled
Internet Communication Management\ Internet Communication settings	Turn off Windows Customer Experience Improvement Program		Enabled

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
***Internet Communication Management**\ Internet Communication settings	Turn off Windows Network Connectivity Status indicator active tests		Enabled (This policy setting turns off the active tests performed by the Windows Network Connectivity Status Indicator (NCSI) to determine whether your computer is connected to the Internet or to a more limited network As part of determining the connectivity level, NCSI performs one of two active tests: downloading a page from a dedicated Web server or making a DNS request for a dedicated address. If you enable this policy setting, NCSI does not run either of the two active tests. This might reduce the ability of NCSI, and of other components that use NCSI, to determine Internet access) NOTE: There are other policies that allow you to redirect NCSI tests to internal resources, if this functionality is desired.
Internet Communication Management\ Internet Communication settings	Turn off Windows Error Reporting		Enabled
Internet Communication Management\ Internet Communication settings	Turn off Windows Update device driver searching		Enabled
Logon	Show first sign-in animation		Disabled
Logon	Turn off app notifications on the lock screen		Enabled
Logon	Turn off Windows Startup sound		Enabled
Power Management	Select an active power plan	High Performance	Enabled
Recovery	Allow restore of system to default state		Disabled
***Storage Health**	Allow downloading updates to the Disk Failure Prediction Model		Disabled (Updates would not be downloaded for the Disk Failure Prediction Failure Model)

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
*__Windows Time Services__\ Time Providers	Enable Windows NTP Client		Disabled (If you disable or do not configure this policy setting, the local computer clock does not synchronize time with NTP servers) **NOTE**: *Consider this setting very carefully*. Windows devices that are joined to a domain should use **NT5DS**. DC to parent domain DC might use NTP. PDCe role might use NTP. Virtual machines sometimes use "enhancements" or "integration services".
Troubleshooting and Diagnostics\ Scheduled Maintenance	Configure Scheduled Maintenance Behavior		Disabled
Troubleshooting and Diagnostics\ Windows Boot Performance Diagnostics	Configure Scenario Execution Level		Disabled
Troubleshooting and Diagnostics\ Windows Memory Leak Diagnostics	Configure Scenario Execution Level		Disabled
Troubleshooting and Diagnostics\ Windows Resource Exhaustion Detection and Resolution	Configure Scenario Execution Level		Disabled
Troubleshooting and Diagnostics\ Windows Shutdown Performance Diagnostics	Configure Scenario Execution Level		Disabled
Troubleshooting and Diagnostics\ Windows Standby/Resume Performance Diagnostics	Configure Scenario Execution Level		Disabled
Troubleshooting and Diagnostics\ Windows System Responsiveness Performance Diagnostics	Configure Scenario Execution Level		Disabled
*__User Profiles__	Turn off the advertising ID		Enabled (If you enable this policy setting, the advertising ID is turned off. Apps can't use the ID for experiences across apps.)

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
Local Computer Policy \ Computer Configuration \ Administrative Templates \ Windows Components			
Add features to Windows 10	Prevent the wizard from running		Enabled
***App Privacy**	Let Windows apps access account information	Default for all apps: Force Deny	Enabled (If you choose the **Force Deny** option, Windows apps are not allowed to access account information and employees in your organization cannot change it)
***App Privacy**	Let Windows apps access call history	Default for all apps: Force Deny	Enabled (If you choose the **Force Deny** option, Windows apps are not allowed to access the call history and employees in your organization cannot change it.)
***App Privacy**	Let Windows apps access contacts	Default for all apps: Force Deny	Enabled (If you choose the **Force Deny** option, Windows apps are not allowed to access contacts and employees in your organization cannot change it.)
***App Privacy**	Let Windows apps access diagnostic information about other apps	Default for all apps: Force Deny	Enabled (If you disable or do not configure this policy setting, employees in your organization can decide whether Windows apps can get diagnostic information about other apps by using Settings > Privacy on the device)
***App Privacy**	Let Windows apps access email	Default for all apps: Force Deny	Enabled (If you choose the "Force Allow" option, Windows apps are allowed to access email and employees in your organization cannot change it)
***App Privacy**	Let Windows apps access location	Default for all apps: Force Deny	Enabled (If you choose the **Force Deny** option, Windows apps are not allowed to access location and employees in your organization cannot change it.)

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
***App Privacy**	Let Windows apps access messaging	Default for all apps: Force Deny	Enabled (If you choose the **Force Deny** option, Windows apps are not allowed to access location and employees in your organization cannot change it.)
***App Privacy**	Let Windows apps access motion	Default for all apps: Force Deny	Enabled (If you choose the **Force Deny** option, Windows apps are not allowed to access motion data and employees in your organization cannot change it.)
***App Privacy**	Let Windows apps access notifications	Default for all apps: Force Deny	Enabled (If you choose the **Force Deny** option, Windows apps are not allowed to access notifications and employees in your organization cannot change it)
***App Privacy**	Let Windows apps access Tasks	Default for all apps: Force Deny	Enabled (If you choose the **Force Deny** option, Windows apps are not allowed to access tasks and employees in your organization cannot change it.)
***App Privacy**	Let Windows apps access the calendar	Default for all apps: Force Deny	Enabled (If you choose the **Force Deny** option, Windows apps are not allowed to access the calendar and employees in your organization cannot change it.)
***App Privacy**	Let Windows apps access the camera	Default for all apps: Force Deny	Enabled (If you choose the **Force Deny** option, Windows apps are not allowed to access the camera and employees in your organization cannot change it.)
***App Privacy**	Let Windows apps access the microphone	Default for all apps: Force Deny	Enabled (If you choose the **Force Deny** option, Windows apps are not allowed to access the microphone and employees in your organization cannot change it.)

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
***App Privacy**	Let Windows apps access trusted devices	Default for all apps: Force Deny	Enabled (If you choose the **Force Deny** option, Windows apps are not allowed to access trusted devices and employees in your organization cannot change it.)
***App Privacy**	Let Windows apps communicate with unpaired devices	Default for all apps: Force Deny	Enabled (If you choose the **Force Deny** option, Windows apps are not allowed to communicate with unpaired wireless devices and employees in your organization cannot change it.)
***App Privacy**	Let Windows apps access radios	Default for all apps: Force Deny	Enabled (If you choose the **Force Deny** option, Windows apps will not have access to control radios and employees in your organization cannot change it.)
App Privacy	Let Windows apps make phone calls	Default for all apps: Force Deny	Enabled (Windows apps are not allowed to make phone calls and employees in your organization cannot change it.)
***App Privacy**	Let Windows apps run in the background	Default for all apps: Force Deny	Enabled (If you choose the **Force Deny** option, Windows apps are not allowed to run in the background and employees in your organization cannot change it.)
AutoPlay Policies	Set the default behavior for AutoRun	Do not execute any autorun commands	Enabled
***AutoPlay Policies**	Turn off Autoplay		Enabled (If you enable this policy setting, Autoplay is disabled on CD-ROM and removable media drives, or disabled on all drives.)
***Cloud Content**	Do not show Windows tips		Enabled (This policy setting prevents Windows tips from being shown to users.)

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
***Cloud Content**	Turn off Microsoft consumer experiences		Enabled (If you enable this policy setting, users will no longer see personalized recommendations from Microsoft and notifications about their Microsoft account.)
***Data Collection and Preview Builds**	Allow Telemetry	0 – Security [Enterprise Only]	Enabled (Setting a value of 0 applies to devices running Enterprise, Education, IoT, or Windows Server editions only.)
***Data Collection and Preview Builds**	Do not show feedback notifications		Enabled
***Data Collection and Preview Builds**	Toggle user control over Insider builds		Disabled
Delivery Optimization	Download Mode	Download Mode: Simple (99)	99 = Simple download mode with no peering. Delivery Optimization downloads using HTTP only and does not attempt to contact the Delivery Optimization cloud services.
Desktop Window Manager	Do not allow Flip3D invocation		Enabled
Desktop Window Manager	Do not allow window animations		Enabled
Desktop Window Manager	Use solid color for Start background		Enabled
Edge UI	Allow edge swipe		Disable
Edge UI	Disable help tips		Enabled
***File Explorer**	Configure Windows Defender SmartScreen		Disabled (SmartScreen will be turned off for all users. Users will not be warned if they try to run suspicious apps from the Internet.)
			NOTE: If not connected to the internet, this will prevent the computers from trying to contact Microsoft for SmartScreen information.

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
File Explorer	Do not show the **new application installed** notification		Enabled
***Find My Device**	Turn On/Off Find My Device		Disabled (When Find My Device is off, the device and its location are not registered and the Find My Device feature will not work. The user will also not be able to view the location of the last use of their active digitizer on their device.)
Game Explorer	Turn off downloading of game information		Enabled
Game Explorer	Turn off game updates		Enabled
Game Explorer	Turn off tracking of last play time of games in the Games folder		Enabled
Homegroup	Prevent the computer from joining a homegroup		Enabled
***Internet Explorer**	Allow Microsoft services to provide enhanced suggestions as the user types in the Address bar		Disabled (users won't receive enhanced suggestions while typing in the Address bar. In addition, users won't be able to change the Suggestions setting.)
Internet Explorer	Disable Periodic Check for Internet Explorer software updates		Enabled
Internet Explorer	Disable showing the splash screen		Enabled
Internet Explorer	Install new versions of Internet Explorer automatically		Disabled
Internet Explorer	Prevent participation in the Customer Experience Improvement Program		Enabled
Internet Explorer	Prevent running First Run wizard	Go directly to home page	Enabled
Internet Explorer	Set tab process growth	Low	Enabled
Internet Explorer	Specify default behavior for a new tab	New tab page	Enabled

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
Internet Explorer	Turn off add-on performance notifications		Enabled
***Internet Explorer**	Turn off the auto-complete feature for web addresses		Enabled (If you enable this policy setting, user will not be suggested matches when entering Web addresses. The user cannot change the auto-complete for setting web addresses.)
***Internet Explorer**	Turn off browser geolocation		Enabled (If you enable this policy setting, browser geolocation support is turned off.)
Internet Explorer	Turn off Reopen Last Browsing Session		Enabled
***Internet Explorer**	Turn on Suggested Sites		Disabled (If you disable this policy setting, the entry points and functionality associated with this feature are turned off.)
***Internet Explorer**\ Compatibility View	Turn off Compatibility View		Enabled (If you enable this policy setting, the user cannot use the Compatibility View button or manage the Compatibility View sites list.)
Internet Explorer\ Internet Control Panel**** Advanced Page	Play animations in web pages		Disabled
Internet Explorer\ Internet Control Panel\ Advanced Page	Play videos in web pages		Disabled
***Internet Explorer**\ Internet Control Panel\ Advanced Page	Turn off the flip ahead with page prediction features		Enabled (Microsoft collects your browsing history to improve how flip ahead with page prediction works. This feature isn't available for Internet Explorer for the desktop. If you enable this policy setting, flip ahead with page prediction is turned off and the next webpage isn't loaded into the background.)
Internet Explorer\ Internet Settings\ Advanced Settings\ Browsing	Turn off phone number detection		Enabled

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
Internet Explorer\ Internet Settings\ Advanced Settings\ Multimedia	Allow Internet Explorer to play media files that use alternative codecs		Disabled
***Location and Sensors**	Turn off location		Enabled (f you enable this policy setting, the location feature is turned off, and all programs on this computer are prevented from using location information from the location feature.)
Location and Sensors	Turn off sensors		Enabled
Locations and Sensors / Windows Location Provider	Turn off Windows Location Provider		Enabled
***Maps**	Turn off Automatic Download and Update of Map Data		Enabled (If you enable this setting the automatic download and update of map data is turned off.)
***Maps**	Turn off unsolicited network traffic on the Offline Maps settings page		Enabled (If you enable this policy setting, features that generate network traffic on the Offline Maps settings page are turned off. Note: This might turn off the entire settings page.)
***Messaging**	Allow Message Service Cloud Sync		Disabled (This policy setting allows backup and restore of cellular text messages to Microsoft's cloud services.)
***Microsoft Edge**	Allow Address bar drop-down list suggestions		Disabled
***Microsoft Edge**	Allow configuration updates for the Books Library		Disabled (Turns off compatibility lists in Microsoft Edge.)
***Microsoft Edge**	Allow Microsoft Compatibility List		Disabled (If you disable this setting, the Microsoft Compatibility List isn't used during browser navigation.)
***Microsoft Edge**	Allow web content on New Tab page		Disabled (Directs Edge to open with blank content when a new tab is opened.)
***Microsoft Edge**	Configure Autofill		Disabled (Disables autofill on address bar.)

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
*__Microsoft Edge__	Configure Do Not Track		Enabled (If you enable this setting, Do Not Track requests are always sent to websites asking for tracking info.)
*__Microsoft Edge__	Configure Password Manager		Disabled (If you disable this setting, employees can't use Password Manager to save their passwords locally.)
*__Microsoft Edge__	Configure search suggestions in Address bar		Disabled (Users can't see search suggestions in the Address bar of Microsoft Edge.)
*__Microsoft Edge__	Configure Start pages		Enabled (If you enable this setting, you can configure one or more Start pages. If this setting is enabled, you must also include URLs to the pages, separating multiple pages by using angle brackets in this format: <support.contoso.com> <support.microsoft.com> Windows 10, version 1703 or later: If you don't want to send traffic to Microsoft, you can use the <about:blank> value, which is honored for devices whether joined to a domain or not, when it's the only configured URL.
*__Microsoft Edge__	Configure Windows Defender SmartScreen		Disabled (Windows Defender SmartScreen is turned off and employees can't turn it on.)
			NOTE: Consider this setting within the environment. If not connected to the Internet, this will prevent the computers from trying to contact Microsoft for SmartScreen information.
*__Microsoft Edge__	Prevent the First Run web page from opening on Microsoft Edge		**Enabled** (Users won't see the First Run page when opening Microsoft Edge for the first time.)

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
OneDrive	Prevent OneDrive from generating network traffic until the user signs in to OneDrive		**Enabled** (Enable this setting to prevent the OneDrive sync client (OneDrive.exe) from generating network traffic (checking for updates, etc.) until the user signs in to OneDrive or starts syncing files to the local computer.)
***OneDrive**	Prevent the usage of OneDrive for file storage		**Enabled** (unless OneDrive is used on- or off-premises.)
OneDrive	Save documents to OneDrive by default		**Disabled** (unless OneDrive is used on- or off-premises.)
RSS Feeds	Prevent automatic discovery of feeds and Web Slices		**Enabled**
***RSS Feeds**	Turn off background synchronization for feeds and Web Slices		**Enabled** (If you enable this policy setting, the ability to synchronize feeds and Web Slices in the background is turned off.)
***Search**	Allow Cortana		**Disabled** (When Cortana is off, users will still be able to use search to find things on the device.)
Search	Allow Cortana above lock screen		**Disabled**
***Search**	Allow search and Cortana to use location		**Disabled**
Search	Do not allow web search		**Enabled**
***Search**	Don't search the web or display web results in Search		**Enabled** (If you enable this policy setting, queries won't be performed on the web and web results won't be displayed when a user performs a query in Search.)
Search	Prevent adding UNC locations to index from Control Panel		**Enabled**
Search	Prevent indexing files in offline files cache		**Enabled**

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
***Search**	Set what information is shared in Search	Anonymous info	**Enabled** (Share usage information but don't share search history, Microsoft account info or specific location.)
***Software Protection Platform**	Turn off KMS Client Online AVC Validation		**Enabled** (Enabling this setting prevents this computer from sending data to Microsoft regarding its activation state.)
***Speech**	Allow Automatic Update of Speech Data		**Disabled** (will not periodically check for updated speech models)
***Store**	Turn off Automatic Download and Install of updates		**Enabled** (If you enable this setting, the automatic download and installation of app updates is turned off.)
***Store**	Turn off Automatic Download of updates on Win8 devices		**Enabled** (If you enable this setting, the automatic download of app updates is turned off.)
Store	Turn off the offer to update to the latest version of Windows		**Enabled**
***Sync your settings**	Do not sync	Allow users to turn syncing on (not selected)	**Enabled** (If you enable this policy setting, "sync your settings" will be turned off, and none of the "sync your setting" groups will be synced on this device.
Text Input	Improve inking and typing recognition		**Disabled**
Windows Defender Antivirus\ MAPS	Join Microsoft MAPS		**Disabled** (If you disable or do not configure this setting, you will not join Microsoft MAPS.)
Windows Defender Antivirus\ MAPS	Send file samples when further analysis is required	Never send	**Enabled** (only if not opted-in for MAPS diagnostic data)
Windows Defender Antivirus\ Reporting	Turn off enhanced notifications		**Enabled** (If you enable this setting, Windows Defender Antivirus enhanced notifications will not display on clients.)

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
Windows Defender Antivirus\ Signature Updates	Define the order of sources for downloading definition updates	FileShares	**Enabled** (If you enable this setting, definition update sources will be contacted in the order specified. Once definition updates have been successfully downloaded from one specified source, the remaining sources in the list will not be contacted.)
Windows Error Reporting	Automatically send memory dumps for operating system-generated error reports		**Disabled**
Windows Error Reporting	Disable Windows Error Reporting		**Enabled**
Windows Game Recording and Broadcasting	Enables or disables Windows Game Recording and Broadcasting		**Disabled**
Windows Installer	Control maximum size of baseline file cache	5	**Enabled**
Windows Installer	Turn off creation of System Restore checkpoints		**Enabled**
Windows Mail	Turn off the communities feature		**Enabled**
Windows Media Player	Do Not Show First Use Dialog Boxes		**Enabled**
Windows Media Player	Prevent Media Sharing		**Enabled**
Windows Mobility Center	Turn off Windows Mobility Center		**Enabled**
Windows Reliability Analysis	Configure Reliability WMI Providers		**Disabled**
Windows Update	Allow Automatic Updates immediate installation		**Enabled**

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
Windows Update	Do not connect to any Windows Update Internet locations		**Enabled** (Enabling this policy will disable that functionality, and might cause connection to public services such as the Windows Store to stop working. **Note:** This policy applies only when this device is configured to connect to an intranet update service using the "Specify intranet Microsoft update service location" policy.
Windows Update	Remove access to all Windows Update features		**Enabled**
***Windows Update**\ Windows Update for Business	Manage preview builds	Set the behavior for receiving preview builds:	**Enabled** (Selecting **Disable preview builds** will prevent preview builds from installing on the device. This will prevent users from opting into the Windows Insider Program, through Settings -> Update and Security.)
		Disable preview builds	
***Windows Update**\ Windows Update for Business	Select when Preview Builds and Feature Updates are received	Semi-Annual Channel	**Enabled** (Enable this policy to specify the level of Preview Build or feature updates to receive, and when.)
		Deferment: 365 days,	
		Pause start: yyyy-mm-dd	
Windows Update\ Windows Update for Business	Select when Quality Updates are received	1. 30 days 2. Pause quality updates starting yyyy-mm-dd	**Enabled**
Windows Restricted Traffic Custom Policy Settings	Prevent OneDrive from generating network traffic until the user signs in to OneDrive		**Enabled** (Enable this setting if you would like to prevent the OneDrive sync client (OneDrive.exe) from generating network traffic (checking for updates, etc.) until the user signs in to OneDrive or starts syncing files to the local computer.)

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
Windows Restricted Traffic Custom Policy Settings	Turn off Windows Defender Notifications		**Enabled** (If you enable this policy setting, Windows Defender will not send notifications with critical information about the health and security of your device.)
Local Computer Policy \ User Configuration \ Administrative Templates			
Control Panel\ Regional and Language Options	Turn off offer text predictions as I type		**Enabled**
Desktop	Do not add shares of recently opened documents to Network Locations		**Enabled**
Desktop	Turn off Aero Shake window minimizing mouse gesture		**Enabled**
Desktop / Active Directory	Maximum size of Active Directory searches	2500	**Enabled**
Start Menu and Taskbar	Do not allow pinning Store app to the Taskbar		**Enabled**
Start Menu and Taskbar	Do not display or track items in Jump Lists from remote locations		**Enabled**
Start Menu and Taskbar	Do not use the search-based method when resolving shell shortcuts		**Enabled** (The system does not conduct the final drive search. It just displays a message explaining that the file is not found.)
Start Menu and Taskbar	Remove the People Bar from the taskbar		**Enabled** (The people icon will be removed from the taskbar, the corresponding settings toggle is removed from the taskbar settings page, and users will not be able to pin people to the taskbar.)
Start Menu and Taskbar	Turn off feature advertisement balloon notifications		**Enabled** (Users cannot pin the Store app to the Taskbar. If the Store app is already pinned to the Taskbar, it will be removed from the Taskbar on next sign in.)
Start Menu and Taskbar	Turn off user tracking		**Enabled**

POLICY SETTING	ITEM	SUB-ITEM	POSSIBLE SETTING AND COMMENTS
Start Menu and Taskbar / Notifications	Turn off toast notifications		**Enabled**
Windows Components / Cloud Content	Turn off all Windows spotlight features		**Enabled**
Edge UI	Turn off tracking of app usage		**Enabled**
File Explorer	Turn off caching of thumbnail pictures		**Enabled**
File Explorer	Turn off display of recent search entries in the File Explorer search box		**Enabled**
File Explorer	Turn off the caching of thumbnails in hidden thumbs.db file		**Enabled**

Notes about Network Connectivity Status indicator

The group policy settings above include settings to turn off checking to see if the system is connected to the Internet. If your environment does not connect to the Internet at all, or connects indirectly, you can set a group policy setting to remove the Network icon from the Taskbar. The reason you might want to remove the Network icon from the Taskbar is if you turn off Internet connectivity checks, there will be a yellow flag on the Network icon, even though the network might be functioning normally. If you would like to remove the network icon as a group policy setting, you can find that in this location:

WINDOWS UPDATE OR WINDOWS UPDATE FOR BUSINESS	SELECT WHEN QUALITY UPDATES ARE RECEIVED	1. 30 DAYS 2. PAUSE QUALITY UPDATES STARTING YYYY-MM-DD	ENABLED
Local Computer Policy \ User Configuration \ Administrative Templates			
Start Menu and Taskbar	Remove the networking icon		**Enabled** (the networking icon is not displayed in the system notification area.)

For more about the Network Connection Status Indicator (NCSI), see: The Network Connection Status icon

System services

If you are considering disabling system services to conserve resources, take great care that the service being considered is not in some way a component of some other service.

Also, most of these recommendations mirror recommendations for Windows Server 2016 with Desktop Experience; for more information, see Guidance on disabling system services in Windows Server 2016 with Desktop Experience.

Note that a lot of services that might seem to be good candidates to disable are set to manual service start type. This means that the service will not automatically start and is not started unless a specific application or service triggers a request to the service being consider for disabling. Services that are already set to start type manual are usually not listed here.

WINDOWS SERVICE	ITEM	COMMENT
CDPUserService	This user service is used for Connected Devices Platform scenarios	NOTE: This is a per-user service, and as such, the *template service* must be disabled.
Connected User Experiences and Telemetry	Enables features that support in-application and connected user experiences. Additionally, this service manages the event-driven collection and transmission of diagnostic and usage information (used to improve the experience and quality of the Windows Platform) when the diagnostics and usage privacy option settings are enabled under Feedback and Diagnostics.	Consider disabling if on disconnected network
Contact Data	Indexes contact data for fast contact searching. If you stop or disable this service, contacts might be missing from your search results.	(PimIndexMaintenanceSvc) NOTE: This is a per-user service, and as such, the *template service* must be disabled.
Diagnostic Policy Service	Enables problem detection, troubleshooting and resolution for Windows components. If this service is stopped, diagnostics will no longer function.	
Downloaded Maps Manager	Windows service for application access to downloaded maps. This service is started on-demand by application accessing downloaded maps. Disabling this service will prevent apps from accessing maps.	
Geolocation Service	Monitors the current location of the system and manages geofences	
GameDVR and Broadcast user service	This user service is used for Game Recordings and Live Broadcasts	NOTE: This is a per-user service, and as such, the template service must be disabled.
MessagingService	Service supporting text messaging and related functionality.	NOTE: This is a per-user service, and as such, the *template service* must be disabled.
Optimize drives	Helps the computer run more efficiently by optimizing files on storage drives.	VDI solutions do not normally benefit from disk optimization. These “drives” are not traditional drives and often just a temporary storage allocation.
Superfetch	Maintains and improves system performance over time.	Generally doesn't improve performance on VDI, especially non-persistent, given that the operating system state is discarded each reboot.

WINDOWS SERVICE	ITEM	COMMENT
Touch Keyboard and Handwriting Panel Service	Enables Touch Keyboard and Handwriting Panel pen and ink functionality	
Windows Error Reporting	Allows errors to be reported when programs stop working or responding and allows existing solutions to be delivered. Also allows logs to be generated for diagnostic and repair services. If this service is stopped, error reporting might not work correctly, and results of diagnostic services and repairs might not be displayed.	With VDI, diagnostics are often performed in an offline scenario, and not in mainstream production. And in addition, some customers disable WER anyway. WER incurs a tiny amount of resources for many different things, including failure to install a device, or failure to install an update.
Windows Media Player Network Sharing Service	Shares Windows Media Player libraries to other networked players and media devices using Universal Plug and Play	Not needed unless customers are sharing WMP libraries on the network.
Windows Mobile Hotspot Service	Provides the ability to share a cellular data connection with another device.	
Windows Search	Provides content indexing, property caching, and search results for files, e-mail, and other content.	Probably not needed especially with non-persistent VDI

Per-user services in Windows

Per-user services are services that are created when a user signs into Windows or Windows Server and are stopped and deleted when that user signs out. These services run in the security context of the user account - this provides better resource management than the previous approach of running these kinds of services in Explorer, associated with a preconfigured account, or as tasks.

Scheduled tasks

Like other items in Windows, ensure that an item is not needed before you consider disabling it.

The following list of tasks are those that perform optimizations or data collections on computers that maintain their state across reboots. When a VDI VM task reboots and discards all changes since last boot, optimizations intended for physical computers are not helpful.

You can get all of the current scheduled tasks, including descriptions, with the following PowerShell code:

```
Get-ScheduledTask | Select-Object -Property TaskPath,TaskName,State,Description |Export-CSV -Path
C:\Temp\W10_1803_SchTasks.csv -NoTypeInformation
```

Valid **Scheduled Task Name** values include:

- OneDrive Standalone Update Task v2
- Microsoft Compatibility Appraiser
- ProgramDataUpdater
- StartupAppTask
- CleanupTemporaryState
- Proxy
- UninstallDeviceTask
- ProactiveScan
- Consolidator
- UsbCeip

- Data Integrity Scan
- Data Integrity Scan for Crash Recovery
- ScheduledDefrag
- SilentCleanup
- Microsoft-Windows-DiskDiagnosticDataCollector
- Diagnostics
- StorageSense
- DmClient
- DmClientOnScenarioDownload
- File History (maintenance mode)
- ScanForUpdates
- ScanForUpdatesAsUser
- SmartRetry
- Notifications
- WindowsActionDialog
- WinSAT Cellular
- MapsToastTask
- ProcessMemoryDiagnosticEvents
- RunFullMemoryDiagnostic
- MNO Metadata Parser
- LPRemove
- GatherNetworkInfo
- WiFiTask
- Sqm-Tasks
- AnalyzeSystem
- MobilityManager
- VerifyWinRE
- RegIdleBackup
- FamilySafetyMonitor
- FamilySafetyRefreshTask
- IndexerAutomaticMaintenance
- SpaceAgentTask
- SpaceManagerTask
- HeadsetButtonPress
- SpeechModelDownloadTask
- ResPriStaticDbSync
- WsSwapAssessmentTask
- SR
- SynchronizeTimeZone
- Usb-Notifications
- QueueReporting
- UpdateLibrary
- Scheduled Start
- sih
- XblGameSaveTask

Apply Windows and other updates

Whether from Microsoft Update, or from your internal resources, apply available updates including Windows Defender signatures. This is a good time to apply other available updates including those for Microsoft Office if installed.

Automatic Windows traces

Windows is configured, by default, to collect and save limited diagnostic data. The purpose is to enable diagnostics, or to record data in the event that further troubleshooting is necessary. You can find automatic system traces by starting the Computer Management app, and then expanding **System Tools**, **Performance**, **Data Collector Sets**, and then selecting **Event Trace Sessions**.

Some of the traces displayed under **Event Trace Sessions** and **Startup Event Trace Sessions** cannot and should not be stopped. Others, such as the **WiFiSession** trace can be stopped. To stop a running trace under **Event Trace Sessions** right-click the trace and then select **Stop**. To prevent the traces from starting automatically on startup, follow these steps:

1. Select the **Startup Event Trace Sessions** folder
2. Locate the trace of interest, and then double-click that trace.
3. Select the **Trace Session** tab.
4. Clear the box labeled **Enabled**.
5. Select **OK**.

Here are some system traces to consider disabling for VDI use:

NAME	COMMENT
AppModel	A collection of traces, one of which is phone
CloudExperienceHostOOBE	
DiagLog	
NtfsLog	
TileStore	
UBPM	
WiFiDriverIHVSession	If not using a WiFi device
WiFiSession	

Servicing the operating system and apps

At some point during the image optimization process available Windows updates should be applied. You can set Windows Update to install updates for other Microsoft products as well as Windows. To set this, open **Windows Settings**, then select **Update & Security**, and then select **Advanced options**. Select **Give me updates for other Microsoft products when I update Windows** to set it to **On**.

This would be a good setting in case you are going to install Microsoft applications such as Microsoft Office to the base image. That way Office is up to date when the image is put in service. There are also .NET updates and certain non-Microsoft components such as Adobe that have updates available through Windows Update.

One very important consideration for non-persistent VDI VMs are security updates, including security software definition files. These updates might be released once or even more than once per day. There might be a way to

retain these updates, including Windows Defender and non-Microsoft components.

For Windows Defender it might be best to allow the updates to occur, even on non-persistent VDI. The updates are going to apply nearly every logon session, but the updates are small and should not be a problem. Plus, the VM won't be behind on updates because only the latest available will apply. The same might be true for non-Microsoft definition files.

> **NOTE**
> Store apps (UWP apps) update through the Windows Store. Modern versions of Office such as Office 365 update through their own mechanisms when directly connected to the Internet, or via management technologies when not.

Windows Defender optimization with VDI

Microsoft has recently published documentation regarding Windows Defender in a VDI environment. See Deployment guide for Windows Defender Antivirus in a virtual desktop infrastructure (VDI) environment for details.

The above article contains procedures to service the gold VDI image, and how to maintain the VDI clients as they are running. To reduce network bandwidth when VDI computers need to update their Windows Defender signatures, stagger reboots, and schedule reboots during off hours where possible. The Windows Defender signature updates can be contained internally on file shares, and where practical, have those files shares on the same or close networking segments as the VDI virtual machines.

See the paper listed at the beginning of this section for much more information about optimizing Windows Defender with VDI.

Tuning Windows 10 network performance by using registry settings

This is especially important in environments where the VDI or physical computer has a workload that is primarily network based. The settings in this section bias performance to favor networking, by setting up additional buffering and caching of things like directory entries and so on.

Note that some settings in this section are *registry-based only* and should be incorporated in the base image before the image is deployed for production use.

The following settings are documented in the Windows Server 2016 Performance Tuning Guideline information, published on Microsoft.com by the Windows Product Group.

DisableBandwidthThrottling

HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\DisableBandwidthThrottling

Applies to Windows 10. The default is **0**. By default, the SMB redirector throttles throughput across high-latency network connections, in some cases to avoid network-related timeouts. Setting this registry value to **1** disables this throttling, enabling higher file transfer throughput over high-latency network connections, so you should consider this setting.

FileInfoCacheEntriesMax

HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\FileInfoCacheEntriesMax

Applies to Windows 10. The default is **64**, with a valid range of 1 to 65536. This value is used to determine the amount of file metadata that can be cached by the client. Increasing the value can reduce network traffic and increase performance when many files are accessed. Try increasing this value to **1024**.

DirectoryCacheEntriesMax

HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\DirectoryCacheEntriesMax

Applies to Windows 10. The default is **16**, with a valid range of 1 to 4096. This value is used to determine the amount of directory information that can be cached by the client. Increasing the value can reduce network traffic

and increase performance when large directories are accessed. Consider increasing this value to **1024**.

FileNotFoundCacheEntriesMax

HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\FileNotFoundCacheEntriesMax

Applies to Windows 10. The default is **128**, with a valid range of 1 to 65536. This value is used to determine the amount of file name information that can be cached by the client. Increasing the value can reduce network traffic and increase performance when many file names are accessed. Consider increasing this value to **2048**.

DormantFileLimit

HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\DormantFileLimit

Applies to Windows 10. The default is **1023**. This parameter specifies the maximum number of files that should be left open on a shared resource after the application has closed the file. Where many thousands of clients are connecting to SMB servers, consider reducing this value to **256**.

You can configure many of these SMB settings by using the Set-SmbClientConfiguration and Set-SmbServerConfiguration Windows PowerShell cmdlets. You can configure registry-only settings by using Windows PowerShell as well, as in the following example:

```
Set-ItemProperty -Path "HKLM:\\SYSTEM\\CurrentControlSet\\Services\\LanmanWorkstation\\Parameters"
RequireSecuritySignature -Value 0 -Force
```

Additional settings from the Windows Restricted Traffic Limited Functionality Baseline guidance

Microsoft has released a baseline created using the same procedures as the Windows Security Baselines, for environments that are either not connected directly to the Internet, or want to reduce data sent to Microsoft and other services.

The Windows Restricted Traffic Limited Functionality Baseline settings are marked in the Group Policy table with an asterisk.

Disk cleanup (including using the Disk Cleanup wizard)

Disk cleanup can be especially helpful with master image VDI implementations. After the master image is prepared, updated, and configured, one of the last tasks to perform is disk cleanup. The Disk Cleanup wizard built into Windows can help clean up most potential areas of disk space savings.

> **NOTE**
> The Disk Cleanup wizard is no longer being developed. Windows will use other methods to provide disk cleanup functions.

Here are suggestions for various disk cleanup tasks. You should test these before implementing any of them:

1. Run the Disk Cleanup wizard (elevated) after applying all updates. Include the categories **Delivery Optimization** and **Windows Update Cleanup**. You can automate this process with **Cleanmgr.exe** with the **/SAGESET:11** option. This option sets registry values that can be used later to automate disk cleanup, using every available option in the Disk Cleanup wizard.

   a. On a test VM, from a clean installation, running **Cleanmgr.exe /SAGESET:11** reveals that there are only two automatic disk cleanup options enabled by default:

   - Downloaded Program Files
   - Temporary Internet Files

   b. If you set more options, or all options, those options are recorded in the registry, according to the index value provided in the previous command (**Cleanmgr.exe /SAGESET:11**). In this example, we use the value *11* as our index, for a subsequent automated disk cleanup procedure.

   c. After running **Cleanmgr.exe /SAGESET:11** you will see a number of categories of disk cleanup

options. You can select every option, and then select **OK**. You will notice that the Disk Cleanup wizard just disappears. However, the settings you selected are saved in the registry, and can be invoked by running **Cleanmgr.exe /SAGERUN:11**.

2. Clean up Volume Shadow Copy storage, if any is in use. To do this, run the following commands in an elevated prompt:

   - **vssadmin list shadows**
   - **vssadmin list shadowstorage**

     If the output from these commands is *No items found that satisfy the query.*, then there is no VSS storage in use.

3. Cleanup temporary files and logs. From an elevated command prompt, run these commands:

   - **Del C:*.tmp /s**
   - **Del C:\Windows\Temp\.**
   - **Del %temp%\.**

4. Delete any unused profiles on the system with this command:

   wmic path win32_UserProfile where LocalPath="c:\\users\\<user>" Delete

Remove OneDrive

Removing OneDrive involves removing the package, uninstalling, and removing *.lnk files. You can use following sample PowerShell code to assist in removing OneDrive from the image:

```
Taskkill.exe /F /IM "OneDrive.exe"
Taskkill.exe /F /IM "Explorer.exe"`
    if (Test-Path "C:\\Windows\\System32\\OneDriveSetup.exe")`
     { Start-Process "C:\\Windows\\System32\\OneDriveSetup.exe"`
         -ArgumentList "/uninstall"`
         -Wait }
    if (Test-Path "C:\\Windows\\SysWOW64\\OneDriveSetup.exe")`
     { Start-Process "C:\\Windows\\SysWOW64\\OneDriveSetup.exe"`
         -ArgumentList "/uninstall"`
         -Wait }
Remove-Item -Path
"C:\\Windows\\ServiceProfiles\\LocalService\\AppData\\Roaming\\Microsoft\\Windows\\Start
Menu\\Programs\\OneDrive.lnk" -Force
Remove-Item -Path "C:\\Windows\\ServiceProfiles\\NetworkService\\AppData\\Roaming\\Microsoft\\Windows\\Start
Menu\\Programs\\OneDrive.lnk" -Force \# Remove the automatic start item for OneDrive from the default user
profile registry hive
Start-Process C:\\Windows\\System32\\Reg.exe -ArgumentList "Load HKLM\\Temp C:\\Users\\Default\\NTUSER.DAT" -
Wait
Start-Process C:\\Windows\\System32\\Reg.exe -ArgumentList "Delete
HKLM\\Temp\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run /v OneDriveSetup /f" -Wait
Start-Process C:\\Windows\\System32\\Reg.exe -ArgumentList "Unload HKLM\\Temp" -Wait Start-Process -FilePath
C:\\Windows\\Explorer.exe -Wait
```

For any questions or concerns about the information in this paper, contact your Microsoft account team, research the Microsoft VDI blog, post a message to Microsoft forums, or contact Microsoft for questions or concerns.

Manage users in your RDS collection

9/27/2019 • 4 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016

As an admin, you can directly manage which users have access to specific collections. This way, you can create one collection with standard applications for information workers, but then create a separate collection with graphics-intensive modeling applications for engineers. There are two primary steps to managing user access in a Remote Desktop Services (RDS) deployment:

1. Create users and groups in Active Directory
2. Assign users and groups to collections

Create your users and groups in Active Directory

In an RDS deployment, Active Directory Domain Services (AD DS) is the source of all users, groups, and other objects in the domain. You can manage Active Directory directly with PowerShell, or you can use built in UI tools that add ease and flexibility. The following steps will guide you to install those tools — if you do not have them already installed — and then use those tools to manage users and groups.

Install AD DS tools

The following steps detail how to install the AD DS tools on a server already running AD DS. Once installed, you can then create users or create groups.

1. Connect to the server running Active Directory Domain Services. For Azure deployments:
   a. In the Azure portal, click **Browse > Resource groups**, and then click the resource group for the deployment
   b. Select the AD virtual machine.
   c. Click **Connect > Open** to open the Remote Desktop client. If **Connect** is grayed out, the virtual machine might not have a public IP address. To give it one perform the following steps, then try this step again.
      a. Click **Settings > Network interfaces**, and then click the corresponding network interface.
      b. Click **Settings > IP address**.
      c. For **Public IP address**, select **Enabled**, and then click **IP address**.
      d. If you have an existing public IP address you want to use, select it from the list. Otherwise, click **Create new**, enter a name, and then click **OK** and **Save**.
   d. In the client, click **Connect**, and then click **Use another account**. Enter the user name and password for a domain administrator account.
   e. Click **Yes** when asked about the certificate.
2. Install the AD DS tools:
   a. In Server Manager click **Manage > Add Roles and Features**.
   b. Click **Role-based or feature-based installation**, and then click the current AD server. Follow the steps until you get to the **Features** tab.
   c. Expand **Remote Server Administration Tools > Role Administration Tools > AD DS and AD LDS Tools**, and then select **AD DS Tools**.
   d. Select **Restart the destination server automatically if required**, and then click **Install**.

Create a group

You can use AD DS groups to grant access to a set of users that need to use the same remote resources.

1. In Server Manager on the server running AD DS, click **Tools > Active Directory Users and Computers**.
2. Expand the domain in the left-hand pane to view its subfolders.
3. Right-click the folder where you want to create the group, and then click **New > Group**.
4. Enter an appropriate group name, then select **Global** and **Security**.

Create a user and add to a group

1. In Server Manager on the server running AD DS, click **Tools > Active Directory Users and Computers**.
2. Expand the domain in the left-hand pane to view its subfolders.
3. Right-click **Users**, and then click **New > User**.
4. Enter, at minimum, a first name and a user logon name.
5. Enter and confirm a password for the user. Set appropriate user options, like **User must change password at next logon**.
6. Add the new user to a group:
   a. In the **Users** folder right-click the new user.
   b. Click **Add to a group**.
   c. Enter the name of the group to which you want to add the user.

Assign users and groups to collections

Now that you've created the users and groups in Active Directory, you can add some granularity regarding who has access to the Remote Desktop collections in your deployment.

1. Connect to the server running the Remote Desktop Connection Broker (RD Connection Broker) role, following the steps described earlier.
2. Add the other Remote Desktop servers to the RD Connection Broker's pool of managed servers:
   a. In Server Manager click **Manage > Add Servers**.
   b. Click **Find Now**.
   c. Click each server in your deployment that is running a Remote Desktop Services role, and then click **OK**.
3. Edit a collection to assign access to specific users or groups:
   a. In Server Manager click **Remote Desktop Services > Overview**, and then click a specific collection.
   b. Under **Properties**, click **Tasks > Edit properties**.
   c. Click **User groups**.
   d. Click **Add** and enter the user or group that you want to have access to the collection. You can also remove users and groups from this window by selecting the user or group you want to remove, and then clicking **Remove**.

> **NOTE**
> The User groups window can never be empty. To narrow the scope of users who have access to the collection, you must first add specific users or groups before removing broader groups.

Customize the RDS title “Work Resources” using PowerShell on Windows Server

9/27/2019 • 2 minutes to read • Edit Online

When using Windows Server to access RemoteApps or desktops through RD WebAccess or the new Remote Desktop app, you may have noticed that the workspace is titled “Work Resources" by default. You can easily change the title by using PowerShell cmdlets.

To change the title, open up a new PowerShell window on the connection broker server and import the RemoteDesktop module with the following command.

```
Import-Module RemoteDesktop
```

Next, use the Set-RDWorkspace command to change the workspace name.

```
Set-RDWorkspace [-Name] <string> [-ConnectionBroker <string>]  [<CommonParameters>]
```

For example, you can use the following command to change the workpsace name to "Contoso RemoteApps":

```
Set-RDWorkspace -Name "Contoso RemoteApps" -ConnectionBroker broker01.contoso.com
```

If you are running multiple Connection Brokers in High Availability mode, you must run this against the active broker. You can use this command:

```
Set-RDWorkspace -Name "Contoso RemoteApps" -ConnectionBroker (Get-
RDConnectionBrokerHighAvailability).ActiveManagementServer
```

For more information about the Set-RDWorkspace cmdlet, see the Set-RDSWorkspace reference.

Use performance counters to diagnose app performance problems on Remote Desktop Session Hosts

1/14/2020 • 5 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows 10

One of the most difficult problems to diagnose is poor application performance—the applications are running slow or don't respond. Traditionally, you start your diagnosis by collecting CPU, memory, disk input/output, and other metrics and then use tools like Windows Performance Analyzer to try to figure out what's causing the problem. Unfortunately, in most situations this data doesn't help you identify the root cause because resource consumption counters have frequent and large variations. This makes it hard to read the data and correlate it with the reported issue. To help you solve your app performance issues quickly, we've added some new performance counters (available to download through the Windows Insider Program) that measure user input flows.

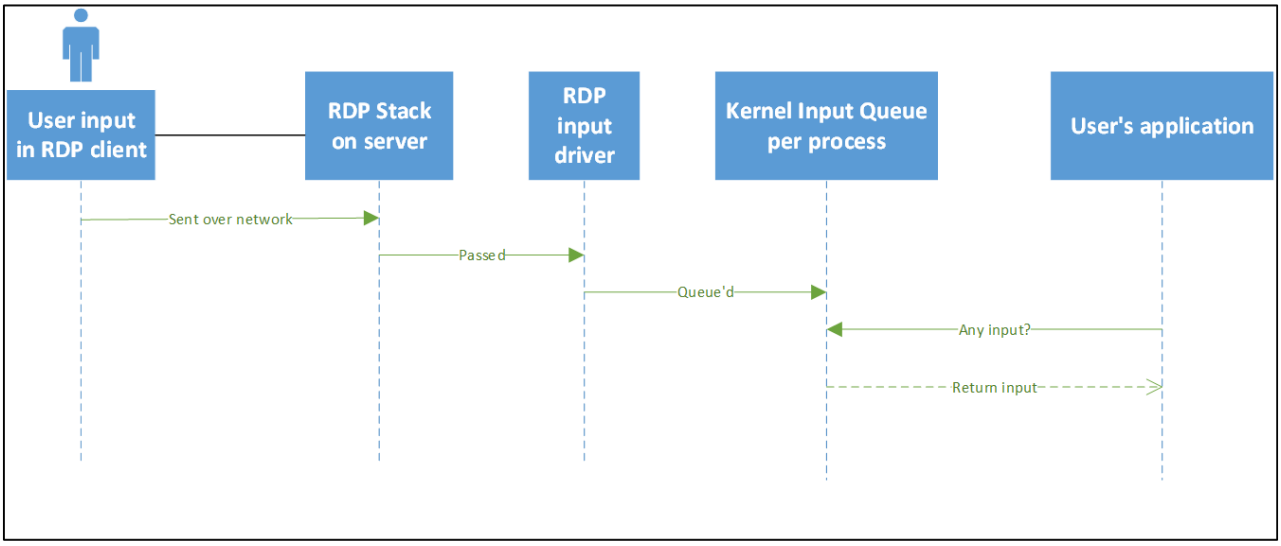
NOTE

The User Input Delay counter is only compatible with:

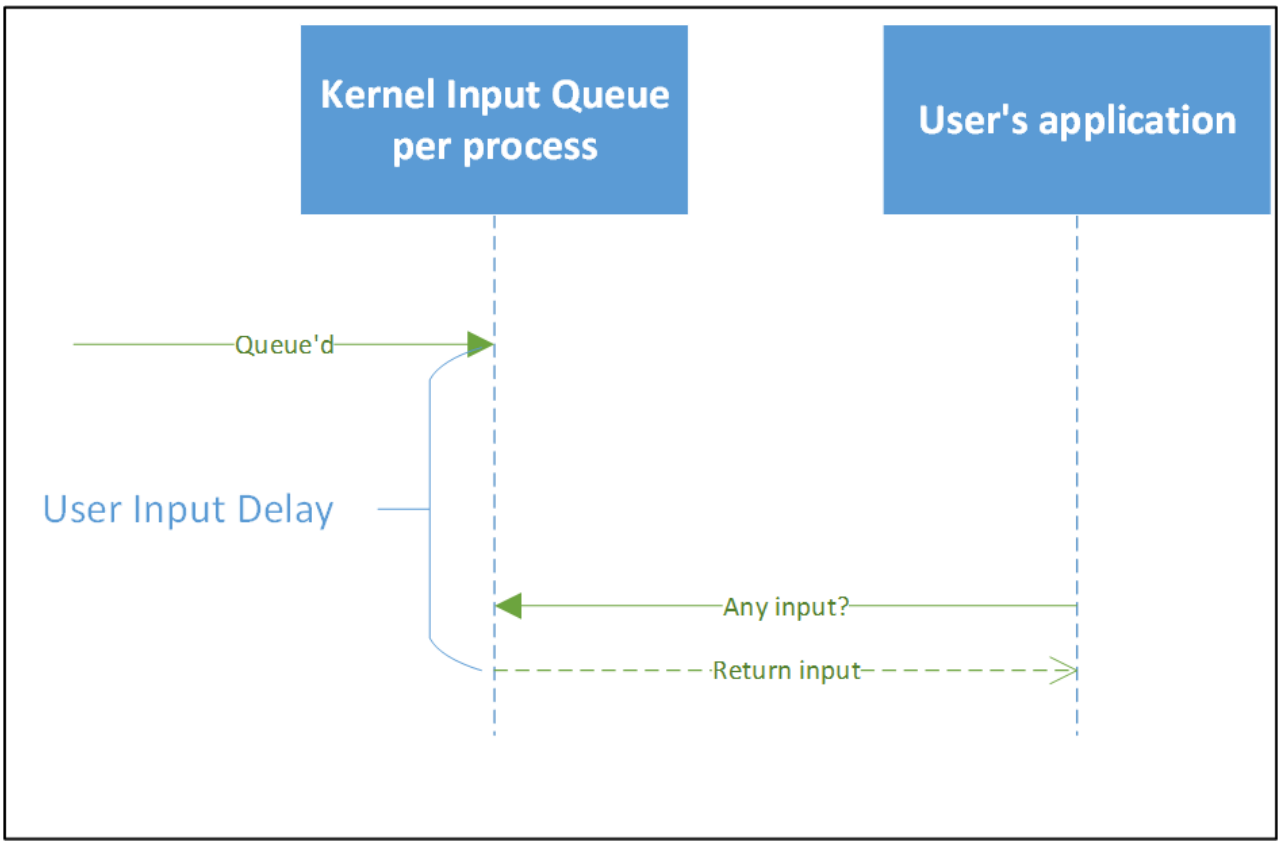
- Windows Server 2019 or later
- Windows 10, version 1809 or later

The User Input Delay counter can help you quickly identify the root cause for bad end user RDP experiences. This counter measures how long any user input (such as mouse or keyboard usage) stays in the queue before it is picked up by a process, and the counter works in both local and remote sessions.

The following image shows a rough representation of user input flow from client to application.



The User Input Delay counter measures the max delta (within an interval of time) between the input being queued and when it's picked up by the app in a traditional message loop, as shown in the following flow chart:



One important detail of this counter is that it reports the maximum user input delay within a configurable interval. This is the longest time it takes for an input to reach the application, which can impact the speed of important and visible actions like typing.

For example, in the following table, the user input delay would be reported as 1,000 ms within this interval. The counter reports the slowest user input delay in the interval because the user's perception of "slow" is determined by the slowest input time (the maximum) they experience, not the average speed of all total inputs.

NUMBER	0	1	2
Delay	16 ms	20 ms	1,000 ms

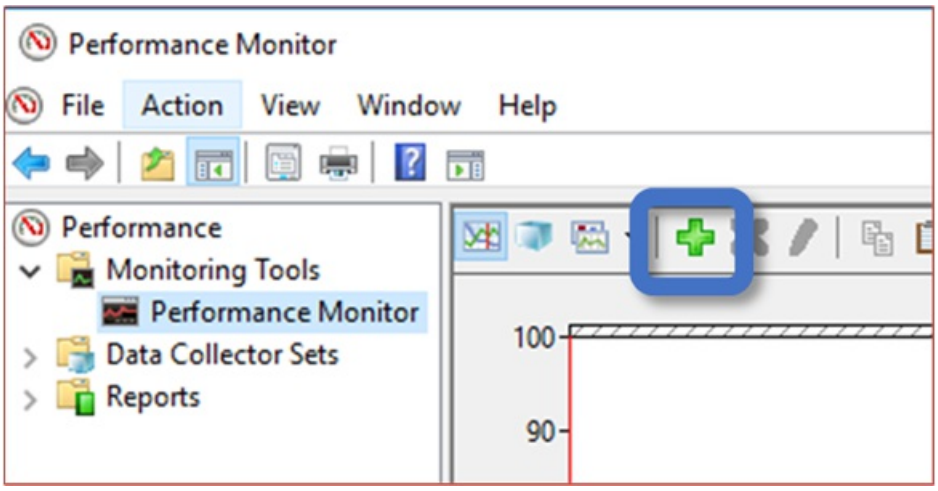
Enable and use the new performance counters

To use these new performance counters, you must first enable a registry key by running this command:

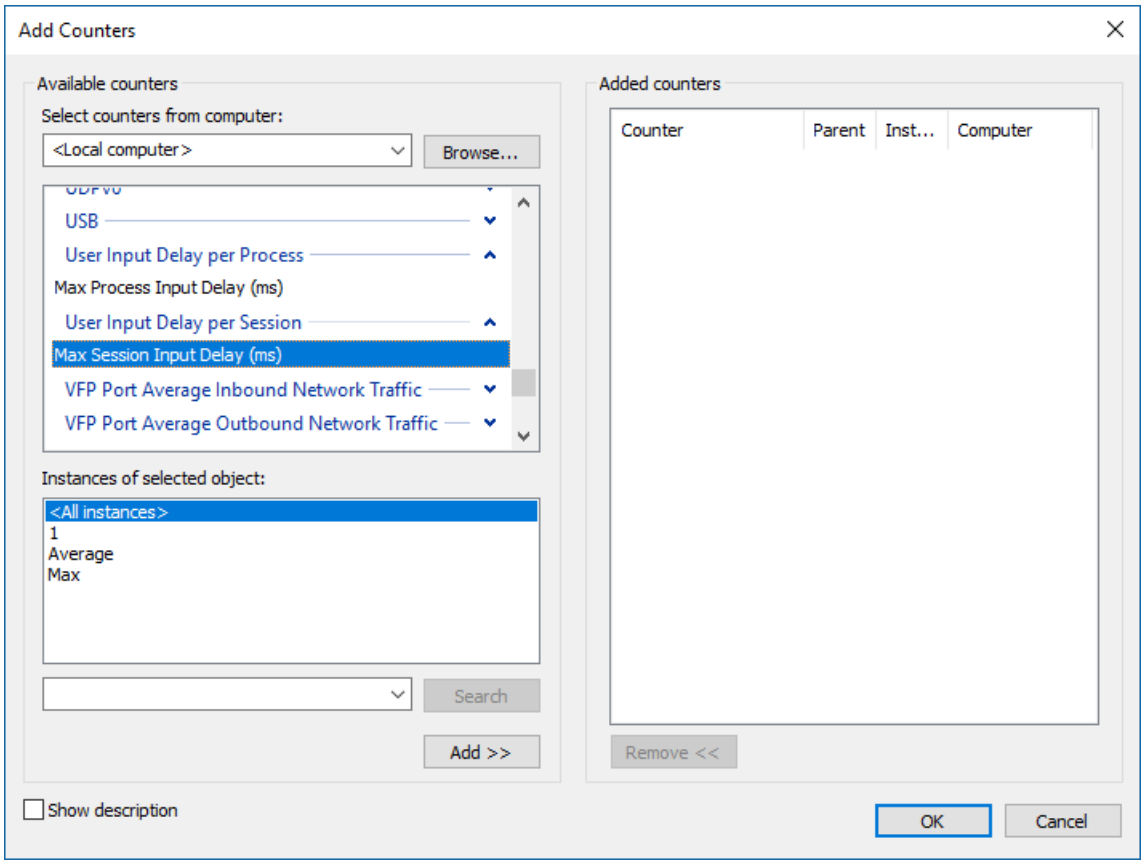
```
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v "EnableLagCounter" /t REG_DWORD /d 0x1 /f
```

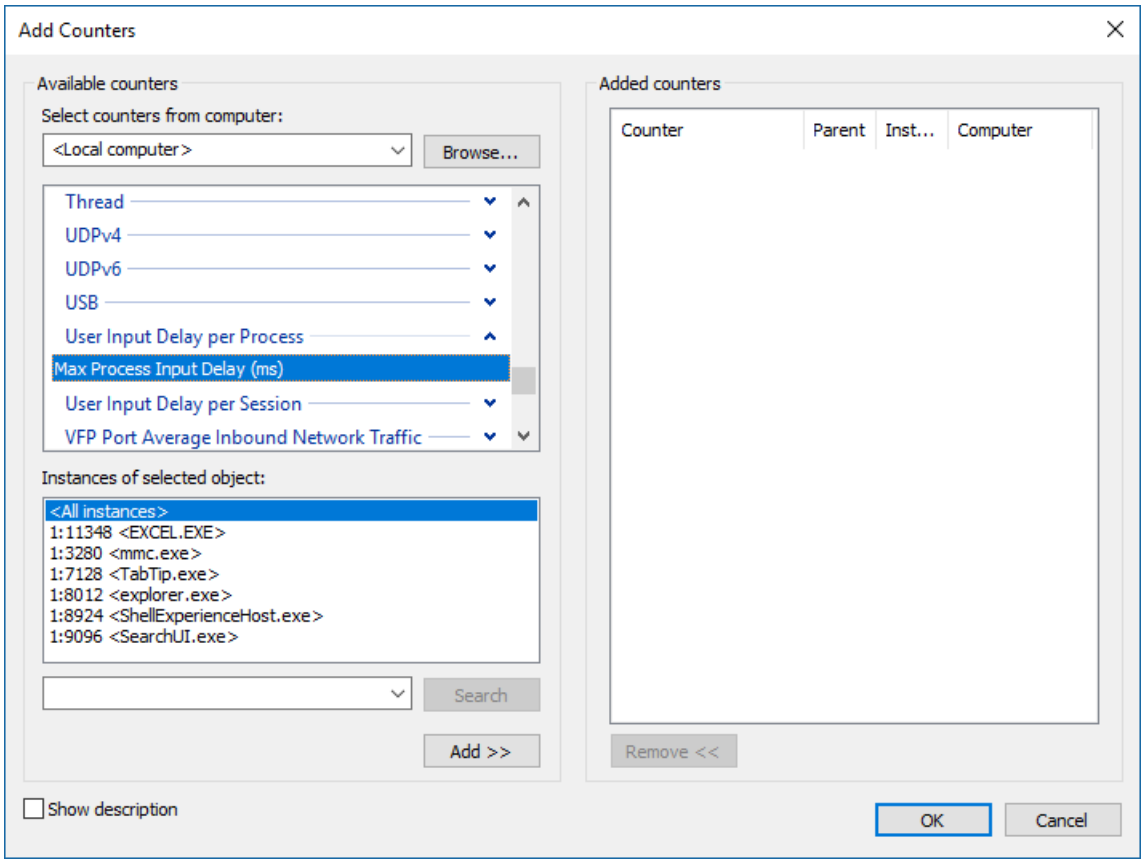
> **NOTE**
> If you're using Windows 10, version 1809 or later or Windows Server 2019 or later, you won't need to enable the registry key.

Next, restart the server. Then, open the Performance Monitor, and select the plus sign (+), as shown in the following screen shot.



After doing that, you should see the Add Counters dialog, where you can select **User Input Delay per Process** or **User Input Delay per Session**.



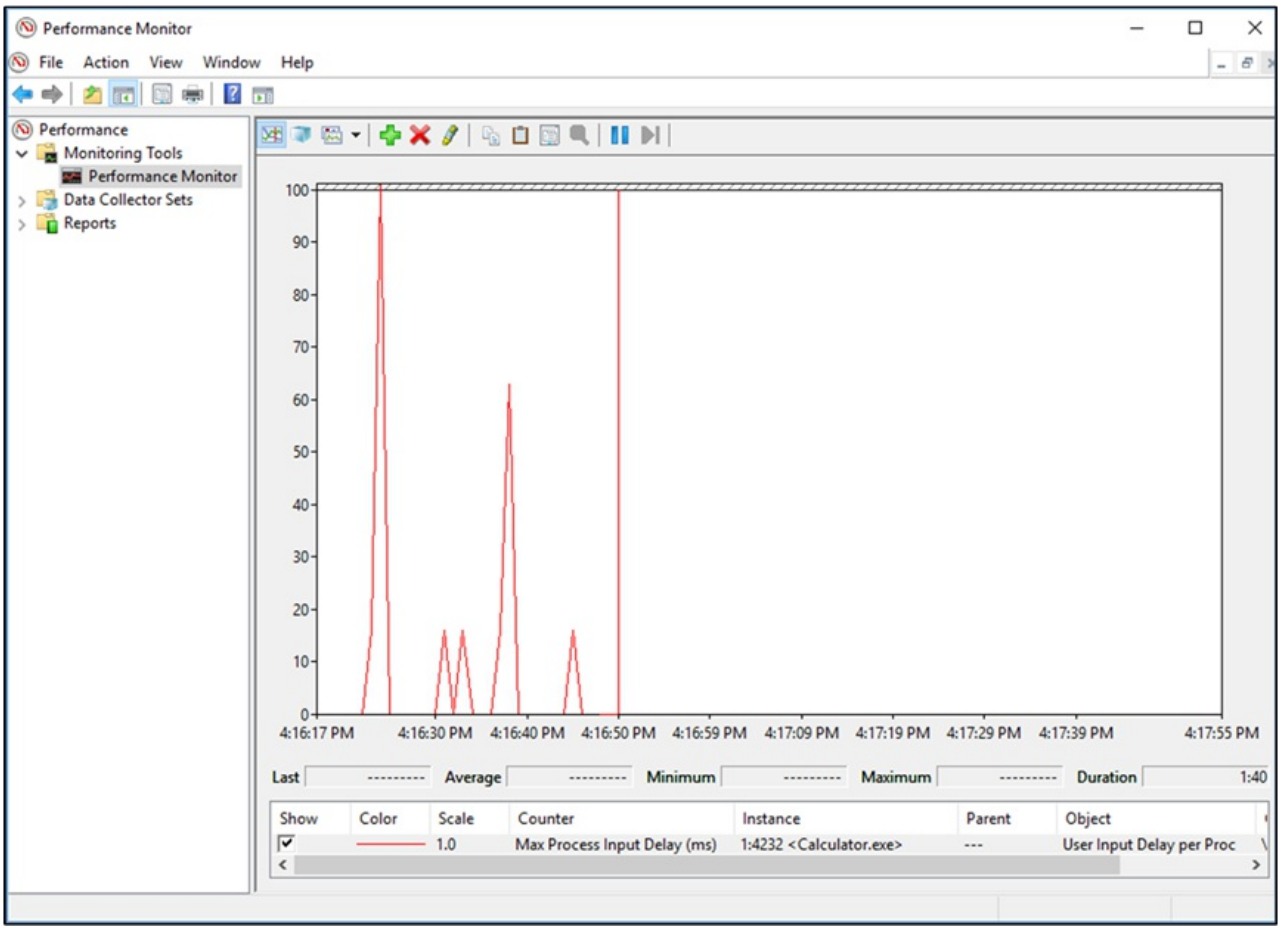


If you select **User Input Delay per Process**, you'll see the **Instances of the selected object** (in other words, the processes) in `SessionID:ProcessID <Process Image>` format.

For example, if the Calculator app is running in a Session ID 1, you'll see `1:4232 <Calculator.exe>`.

> **NOTE**
>
> Not all processes are included. You won't see any processes that are running as SYSTEM.

The counter starts reporting user input delay as soon as you add it. Note that the maximum scale is set to 100 (ms) by default.



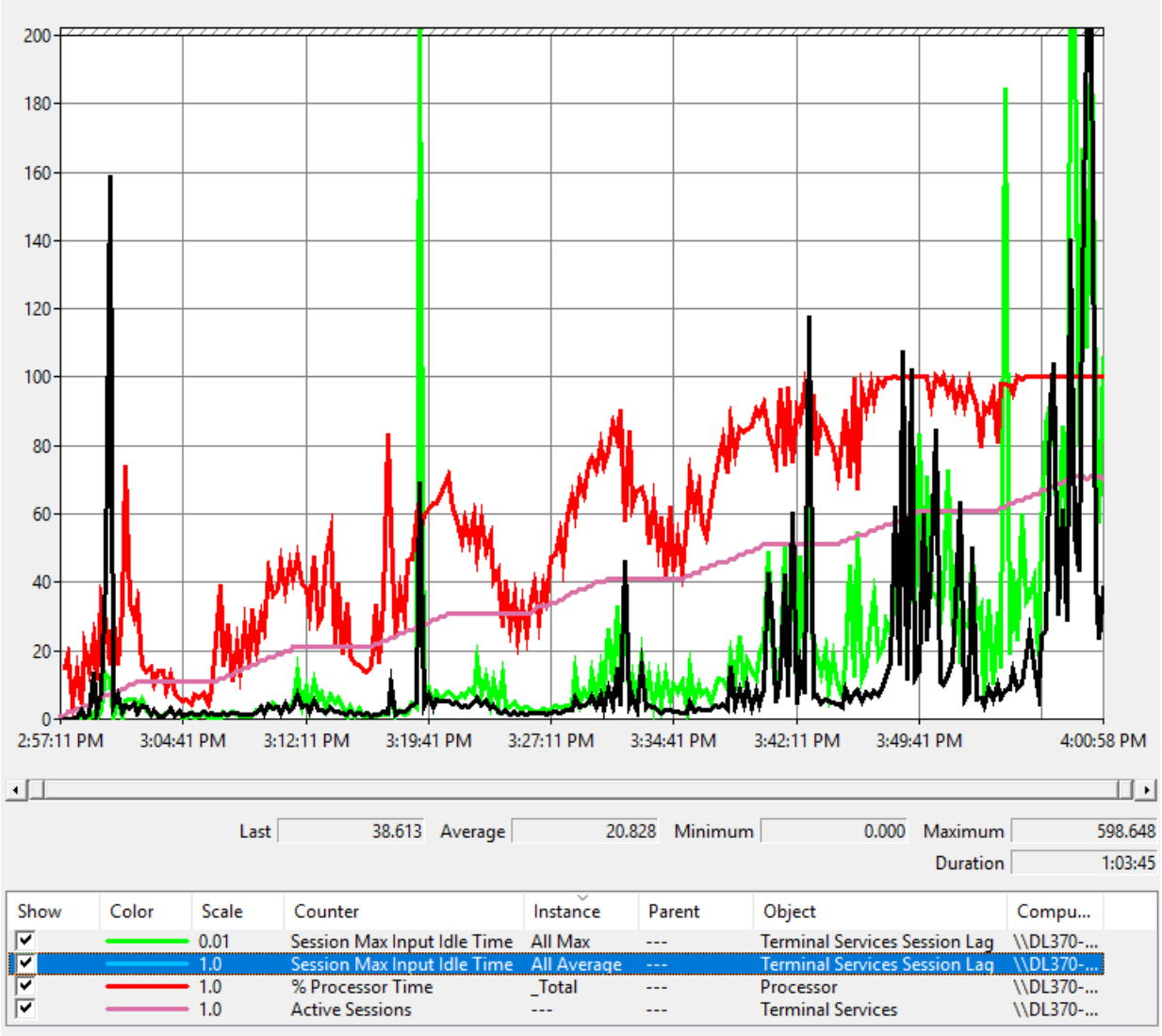
Next, let's look at the **User Input Delay per Session**. There are instances for each session ID, and their counters show the user input delay of any process within the specified session. In addition, there are two instances called "Max" (the maximum user input delay across all sessions) and "Average" (the average acorss all sessions).

This table shows a visual example of these instances. (You can get the same information in Perfmon by switching to the Report graph type.)

TYPE OF COUNTER	INSTANCE NAME	REPORTED DELAY (MS)
User Input Delay per process	1:4232 <Calculator.exe>	200
User Input Delay per process	2:1000 <Calculator.exe>	16
User Input Delay per process	1:2000 <Calculator.exe>	32
User Input Delay per session	1	200
User Input Delay per session	2	16
User Input Delay per session	Average	108
User Input Delay per session	Max	200

Counters used in an overloaded system

Now let's look at what you'll see in the report if performance for an app is degraded. The following graph shows readings for users working remotely in Microsoft Word. In this case, the RDSH server performance degrades over time as more users log in.



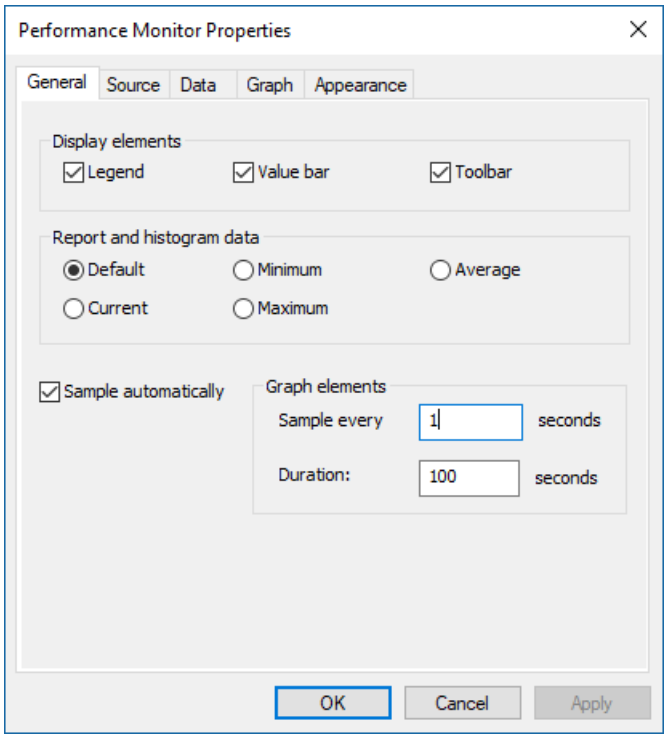
Here's how to read the graph's lines:

- The pink line shows the number of sessions signed in on the server.
- The red line is the CPU usage.
- The green line is the maximum user input delay across all sessions.
- The blue line (displayed as black in this graph) represents average user input delay across all sessions.

You'll notice that there's a correlation between CPU spikes and user input delay—as the CPU gets more usage, the user input delay increases. Also, as more users get added to the system, CPU usage gets closer to 100%, leading to more frequent user input delay spikes. While this counter is very useful in cases where the server runs out of resources, you can also use it to track user input delay related to a specific application.

Configuration Options

An important thing to remember when using this performance counter is that it reports user input delay on an interval of 1,000 ms by default. If you set the performance counter sample interval property (as shown in the following screenshot) to anything different, the reported value will be incorrect.



To fix this, you can set the following registry key to match the interval (in milliseconds) that you want to use. For example, if we change Sample every x seconds to 5 seconds, we need to set this key to 5000 ms.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]

"LagCounterInterval"=dword:00005000
```

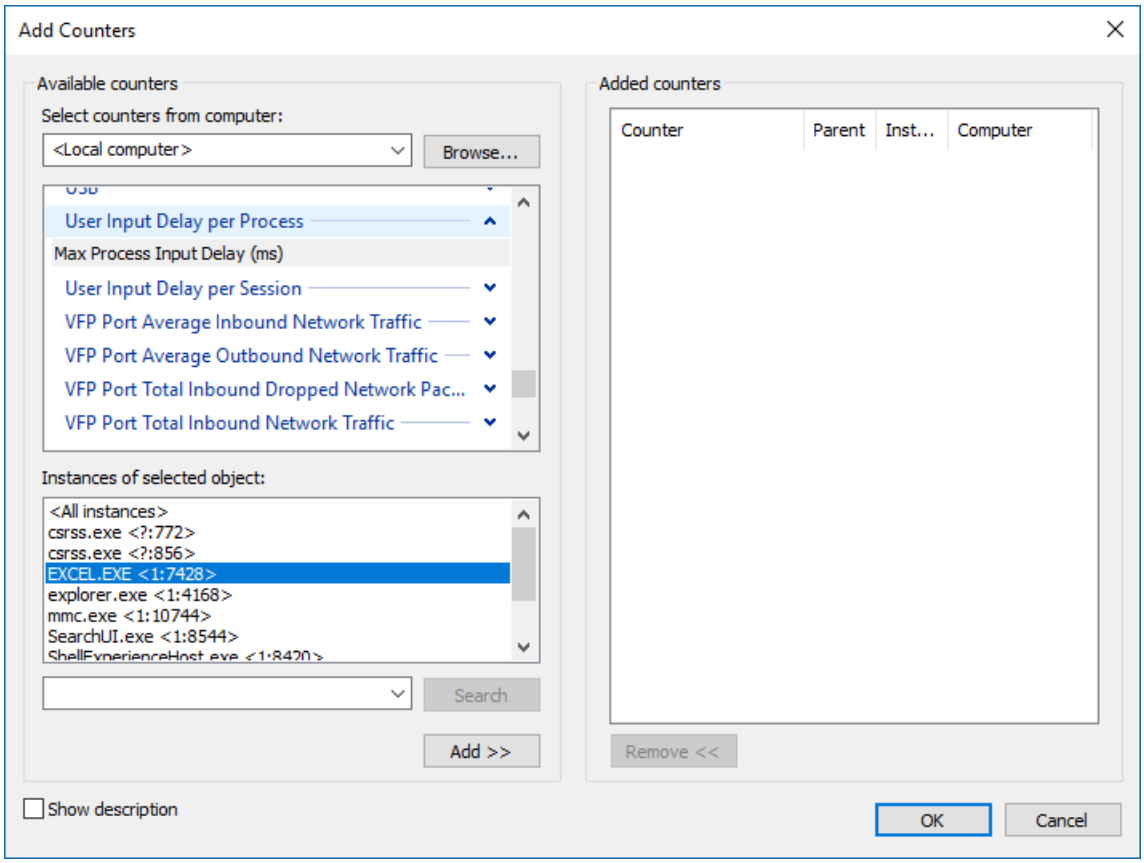
> **NOTE**
> If you're using Windows 10, version 1809 or later or Windows Server 2019 or later, you don't need to set LagCounterInterval to fix the performance counter.

We've also added a couple of keys you might find helpful under the same registry key:

LagCounterImageNameFirst — set this key to `DWORD 1` (default value 0 or key does not exist). This changes the counter names to "Image Name SessionID:ProcessId." For example, "explorer <1:7964>." This is useful if you want to sort by image name.

LagCounterShowUnknown — set this key to `DWORD 1` (default value 0 or key does not exist). This shows any processes that are running as services or SYSTEM. Some processes will show up with their session set as "?."

This is what it looks like if you turn both keys on:



Using the new counters with non-Microsoft tools

Monitoring tools can consume this counter by using the Perfmon API.

Download Windows Server Insider software

Registered Insiders can navigate directly to the Windows Server Insider Preview download page to get the latest Insider software downloads. To learn how to register as an Insider, see Getting started with Server.

Share your feedback

You can submit feedback for this feature through the Feedback Hub. Select **Apps > All other apps** and include "RDS performance counters—performance monitor" in your post's title.

For general feature ideas, visit the RDS UserVoice page.

Remote Desktop clients

1/10/2020 • 2 minutes to read • Edit Online

Applies to: Windows 10, Windows 8.1, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2

You can use a Microsoft Remote Desktop client to connect to a remote PC and your work resources from almost anywhere using just about any device. You can connect to your work PC and have access to all of your apps, files, and network resources as if you were sitting at your desk. You can leave apps open at work and then see those same apps at home - all by using the RD client.

Before you start, make sure you check out the supported configuration article, which discusses the PCs that you can connect to using the Remote Desktop clients. Also check out the client FAQ.

The following client apps are available:

DEVICE	GET THE APP	SET UP INSTRUCTIONS
Windows Desktop	Windows Desktop client	Get started with the Windows Desktop client
Windows Store	Windows 10 client in the Microsoft Store	Get started with the Windows Store client
Android	Android client in Google Play	Get started with the Android client
iOS	iOS client in the iTunes store	Get started with the iOS client
macOS	macOS client in the iTunes store	Get started with the macOS client

Configuring the remote PC

To configure your remote PC before accessing it remotely, Allow access to your PC.

Remote Desktop client URI scheme

You can integrate features of Remote Desktop clients across platforms by enabling a Uniform Resource Identifier (URI) scheme. Check out the supported URI attributes that you can use with the iOS, Mac, and Android clients.

Get started with the Windows Desktop client

1/10/2020 • 5 minutes to read • Edit Online

Applies to: Windows 10, Windows 10 IoT Enterprise, and Windows 7

You can use the Remote Desktop client for Windows Desktop to access Windows apps and desktops remotely from a different Windows device.

NOTE

- This documentation is not for the Remote Desktop Connection (MSTSC) client that ships with Windows. It's for the new Remote Desktop (MSRDC) client.
- This client currently only supports accessing remote apps and desktops from Windows Virtual Desktop.
- Curious about the new releases for the Windows Desktop client? Check out What's new in the Windows Desktop client

Install the client

Choose the client that matches the version of Windows. The new Remote Desktop client (MSRDC) supports Windows 10, Windows 10 IoT Enterprise, and Windows 7 client devices.

- Windows 64-bit
- Windows 32-bit
- Windows ARM64

You can install the client for the current user, which doesn't require admin rights, or your admin can install and configure the client so that all users on the device can access it.

Once you've installed the client, you can launch it from the Start menu by searching for **Remote Desktop**.

Update the client

You'll be notified whenever a new version of the client is available as long as your admin hasn't disabled notifications. The notification will appear in either the Connection Center or the Windows Action Center. To update your client, just select the notification.

You can also manually search for new updates for the client:

1. From the Connection Center, tap the overflow menu (**...**) on the command bar at the top of the client.
2. Select **About** from the drop-down menu.
3. Tap **Check for updates**.
4. If there's an update available, tap **Install update** to update the client.

Feeds

Get the list of managed resources you can access, such as apps and desktops, by subscribing to the feed your admin provided you. When you subscribe, the resources become available on your local PC. The Windows Desktop client currently supports resources published from Windows Virtual Desktop.

Subscribe to a feed

1. From the main page of the client, also known as the Connection Center, tap **Subscribe**.

2. Sign in with your user account when prompted.
3. The resources will appear in the Connection Center grouped by Workspace.

You can launch resources with one of the following methods:

- Go to the Connection Center and double-click a resource to launch it.
- You can also go to the Start menu and look for a folder with the Workspace name or enter the resource name in the search bar.

Workspace details

After subscribing, you can view additional information about a Workspace on the Details panel:

- The name of the Workspace
- The URL and username used to subscribe
- The number of apps and desktops
- The date/time of the last update
- The status of the last update

Accessing the Details panel:

1. From the Connection Center, tap the overflow menu (**...**) next to the Workspace.
2. Select **Details** from the drop-down menu.
3. The Details panel appears on the right side of the client.

After you've subscribed, the Workspace will update automatically on a regular basis. Resources may be added, changed, or removed based on changes made by your admin.

You can also manually look for updates to the resources when needed by selecting **Update now** from the Details panel.

Unsubscribe from a feed

This section will teach you how to unsubscribe from a feed. You can unsubscribe to either subscribe again with a different account or remove your resources from the system.

1. From the Connection Center, tap the overflow menu (**...**) next to the Workspace.
2. Select **Unsubscribe** from the drop-down menu.
3. Review the dialog box and select **Continue**.

Managed desktops

Workspaces can contain multiple managed resources, including desktops. When accessing a managed desktop, you have access to all the apps installed by your admin.

Desktop settings

You can configure some of the settings for desktop resources to ensure the experience meets your needs. To access the list of available settings:

1. From the Connection Center, right-click on a desktop resource.
2. Select **Settings** from the drop-down menu.
3. The Settings panel appears on the right side of the client displaying the name of the desktop.

The client will use the settings configured by your admin unless you turn off the **Use default settings** option. Doing so allows you to configure the following options:

- **Use all monitors** switches the desktop session between using all available local monitors and only one monitor.

- **Start in full screen** determines whether the session will launch in full-screen or windowed mode. This setting is automatically enabled when using all monitors.
- **Update the resolution on resize** changes the behavior when you resize the session in windowed mode. If enabled, the resolution of the remote desktop will update to match the size of the local window. If disabled, the session will retain the resolution specified in **Resolution** for its entire duration. This setting is automatically enabled when using all monitors.
- **Resolution** lets you specify the resolution of the remote desktop. The session will retain this resolution for its entire duration. This setting is automatically disabled if the resolution is set to update on resize.
- **Change the size of the text and apps** specifies the size of the content of the session. This setting only applies when connecting to Windows 8.1 and later or Windows Server 2012 R2 and later. This setting is automatically disabled if the resolution is set to update on resize.
- **Fit session to window** determines how the session is displayed when the resolution of the remote desktop differs from the size of the local window. When enabled, the session content will be resized to fit inside the window while preserving the aspect ratio of the session. When disabled, scrollbars or black areas will be shown when the resolution and window size don't match.

Provide feedback

Have a feature suggestion or want to report a problem? Tell us using the Feedback Hub. You can also access the Feedback Hub through the client:

1. From the Connection Center, tap the **Send feedback** option on the command bar at the top of the client to open the Feedback Hub app.
2. Enter the required information in the **Summary** and **Details** fields. When you're done, tap **Next**.
3. Select whether it's a **Problem** or **Suggestion**.
4. Check to see if the category is in **Apps** > **Remote Desktop**. If it is, tap **Next**.
5. Review the existing feedback topics to see if someone else has reported the same problem. If not, select **Make a new bug**, then tap **Next**.
6. On the next page, you can give us more information so we can help you solve the problem. You can write more detailed information, submit screenshots, and even create a recording of the problem to show us what happened. To make a recording, select **Start recording**, then do what you did up to the point where the problem happened. When you're done, return to the Feedback Hub and select **Stop recording**.
7. When you're satisfied with the information, tap **Submit**.
8. On the "Thank you for your feedback!" page, tap **Share my feedback** to generate a link to your feedback that you can share with others as needed.

Access client logs

You might need the client logs when investigating a problem.

To retrieve the client logs:

1. Open **File Explorer**.
2. Navigate to the **%temp%\DiagOutputDir\RdClientAutoTrace** folder.

Windows Desktop client for admins

1/24/2020 • 2 minutes to read • Edit Online

Applies to: Windows 10 and Windows 7

This topic has additional information about the Windows Desktop client that admins will find useful. For basic usage information, see Get started with the Windows Desktop client.

Installation options

Although your users can install the client directly after downloading it, if you're deploying to multiple devices, you may want to also deploy the client to them through other means. Deploying using group policies or the Microsoft Endpoint Configuration Manager lets you run the installer silently using a command line. Run the following commands to deploy the client per-device or per-user.

Per-device installation

```
msiexec.exe /I <path to the MSI> /qn ALLUSERS=1
```

Per-user installation

```
msiexec.exe /i `<path to the MSI>` /qn ALLUSERS=2 MSIINSTALLPERUSER=1
```

Configuration options

This section describes the new configuration options for this client.

Configure update notifications

By default, the client notifies you whenever there's an update. To turn notifications off, set the following registry information:

- **Key:** HKLM\Software\Microsoft\MSRDC\Policies
- **Type:** REG_DWORD
- **Name:** AutomaticUpdates
- **Data:** 0 = Disable notifications. 1 = Show notifications.

Configure user groups

You can configure the client for one of the following types of user groups, which determines when the client receives updates.

Insider group

The Insider group is for early validation, and consists of admins and their selected users. The Insider group serves as a test run to detect any issues in the update that can impact performance before it's released to the Public group.

> **NOTE**
> We recommend each organization have some users in the Insider group to test updates and catch issues early.

In the Insider group, a new version of the client is released to the users on the second Tuesday of each month for

early validation. If the update doesn't have issues, it gets released to the Public group two weeks later. Users in the Insider group will receive update notifications automatically whenever updates are ready. You can find more detailed information about changes to the client at What's new with the Windows Desktop client.

To configure the client for the Insider group, set the following registry information:

- **Key:** HKLM\Software\Microsoft\MSRDC\Policies
- **Type:** REG_SZ
- **Name:** ReleaseRing
- **Data:** insider

Public group

This group is for all users and is the most stable version. You don't need to do anything to configure this group.

The Public group receives the version of the client that was tested by the Insider group every fourth Tuesday of each month. All users in the Public group will receive an update notification if that setting is enabled.

What's new in the Windows Desktop client

1/14/2020 • 2 minutes to read • Edit Online

You can find more detailed information about the Windows Desktop client at Get started with the Windows Desktop client. You'll find the latest updates to client below.

Latest client versions

The client can be configured for different user groups. The following table lists the current versions available for each user group:

USER GROUP	VERSION
Public	1.2.535
Insider	1.2.594

Updates for version 1.2.594

Date published: 01/14/2020

Download: Windows 64-bit, Windows 32-bit, Windows ARM64

- You can now select which displays to use for desktop connections. To change this setting, right-click the icon of the desktop connection and select **Settings**.
- Fixed an issue where the connection settings didn't display the correct available scale factors.
- Fixed an issue where Narrator couldn't read the dialogue shown while the connection initiated.
- Fixed an issue where the wrong user name displayed when the Azure Active Directory and Active Directory names didn't match.
- Fixed an issue that made the client stop responding when initiating a connection while not connected to a network.
- Fixed an issue that caused the client to stop responding when attaching a headset.

Updates for version 1.2.535

Date published: 12/04/2019

Download: Windows 64-bit, Windows 32-bit, Windows ARM64

- You can now access information about updates directly from the more options button on the command bar at the top of the client.
- You can now report feedback from the command bar of the client.
- The Feedback option is now only shown if the Feedback Hub is available.
- Ensured the update notification is not shown when notifications are disabled through policy.
- Fixed an issue that prevented some RDP files from launching.
- Fixed a crash on startup of the client caused by corruption of some persistent settings.

Updates for version 1.2.431

Date published: 11/12/2019

Download: Windows 64-bit, Windows 32-bit, Windows ARM64

- The 32-bit and ARM64 versions of the client are now available!
- The client now saves any changes you make to the connection bar (such as its position, size, and pinned state) and applies those changes across sessions.
- Updated gateway information and connection status dialogs.
- Addressed an issue that caused two credentials to prompt at the same time while trying to connect after the Azure Active Directory token expired.
- On Windows 7, users are now properly prompted for credentials if they had saved credentials when the server disallows it.
- The Azure Active Directory prompt now appears in front of the connection window when reconnecting.
- Items pinned to the taskbar are now updated during a feed refresh.
- Improved scrolling on the Connection Center when using touch.
- Removed the empty line from the resolution drop-down menu.
- Removed unnecessary entries in Windows Credential Manager.
- Desktop sessions are now properly sized when exiting full screen.
- The RemoteApp disconnection dialog now appears in the foreground when you resume your session after entering sleep mode.
- Addressed accessibility issues like keyboard navigation.

Updates for version 1.2.247

Date published: 09/17/2019

Download: Windows 64-bit

- Improved the fallback languages for localized version. (For example, FR-CA will properly display in French instead of English.)
- When removing a subscription, the client now properly removes the saved credentials from Credential Manager.
- The client update process is now unattended once started and the client will relaunch once completed.
- The client can now be used on Windows 10 in S mode.
- Fixed an issue that caused the update process to fail for users with a space in their username.
- Fixed a crash that happened when authenticating during a connection.
- Fixed a crash that happened when closing the client.

Get started with the Windows Store client

9/27/2019 • 10 minutes to read • Edit Online

Applies to: Windows 10

You can use the Remote Desktop client for Windows to work with Windows apps and desktops remotely from a different Windows device.

Use the following information to get started. Be sure to check out the FAQ if you have any questions.

NOTE

- Curious about the new releases for the Windows Store client? Check out What's new in the Windows Store client
- You can run the client on any supported version of Windows 10.

Get the RD client and start using it

Follow these steps to get started with Remote Desktop on your Windows 10 device:

1. Download the Remote Desktop client from Microsoft Store.
2. Set up your PC to accept remote connections.
3. Add a Remote Desktop connection or a remote resource. You use a connection to connect directly to a Windows PC and a remote resource to use a RemoteApp program, session-based desktop, or virtual desktop published by your admin.
4. Pin items so you can get to Remote Desktop quickly.

Add a Remote Desktop connection

To create a Remote Desktop connection:

1. In the Connection Center tap **+ Add**, and then tap **Desktop**.
2. Enter the following information for the computer you want to connect to:
   - **PC name** – the name of the computer. This can be a Windows computer name, an Internet domain name, or an IP address. You can also append port information to the PC name (for example, **MyDesktop:3389** or **10.0.0.1:3389**).
   - **User account** – The user account to use to access the remote PC. Tap **+** to add a new account or select an existing account. You can use the following formats for the username: *user_name*, *domain\user_name*, or *user_name@domain.com*. You can also specify whether to prompt for a user name and password during the connection by selecting **Ask me every time**.
3. You can also set additional options by tapping on **Show more**:
   - **Display name** – An easy-to-remember name for the PC you are connecting to. You can use any string, but if you do not specify a friendly name, the PC name is displayed.
   - **Group** – Specify a group to make it easier to find your connections later. You can add a new group by tapping **+** or select one from the list.
   - **Gateway** – The Remote Desktop gateway that you want to use to connect to virtual desktops, RemoteApp programs, and session-based desktops on an internal corporate network. Get the information about the gateway from your system administrator.
   - **Connect to admin session** - Use this option to connect to a console session to administrate a Windows server.

- **Swap mouse buttons** – Use this option to swap the left mouse button functions for the right mouse button. (This is especially useful if the remote PC is configured for a left-handed user but you use a right-handed mouse.)
- **Set my remote session resolution to:** – Select the resolution you want to use in the session. **Choose for me** will set the resolution based on the size of the client.
- **Change the size of the display:** – When selecting a high static resolution for the session, you have the option to make items on the screen appear larger to improve readability. Note: This only applies when connecting to Windows 8.1 or above.
- **Update the remote session resolution on resize** – When enabled, the client will dynamically update the session resolution based on the size of the client. Note: This only applies when connecting to Windows 8.1 or above.
- **Clipboard** – When enabled, allows you to copy text and images to/from the remote PC.
- **Audio Playback** – Select the device to use for audio during your remote session. You can choose to play sound on the local devices, the remote PC, or not at all.
- **Audio Recording** – When enabled, allows you to use a local microphone with applications on the remote PC.

4. Tap **Save**.

Need to edit these settings? Tap the overflow menu (**...**) next to the name of the desktop, and then tap **Edit**.

Want to delete the connection? Again, tap the overflow menu (**...**), and then tap **Remove**.

Add a remote resource

Remote resources are RemoteApp programs, session-based desktops, and virtual desktops published by your admin using Remote Desktop Services.

To add a remote resource:

1. On the Connection Center screen, tap **+ Add**, and then tap **Remote resources**.
2. Enter the **Feed URL** provided by your admin and tap **Find feeds**.
3. When prompted, provide the credentials to use to subscribe to the feed.

The remote resources will be displayed in the Connection Center.

To delete remote resources:

1. In the Connection Center, tap the overflow menu (**...**) next to the remote resource.
2. Tap **Remove**.

Pin a saved desktop to your Start menu

To pin a connection to your Start menu, tap the overflow menu (**...**) next to the name of the desktop, and then tap **Pin to Start**.

Now you can start the remote desktop connection directly from your Start menu by tapping it.

Connect to an RD Gateway to access internal assets

A Remote Desktop Gateway (RD Gateway) lets you connect to a remote computer on a corporate network from anywhere on the Internet. You can create and manage your gateways using the Remote Desktop client.

To set up a new gateway:

1. In the Connection Center, tap **Settings**.
2. Next to Gateway, tap **+** to add a new gateway. Note: A gateway can also be added when adding a new connection.

3. Enter the following information:
    - **Server name** – The name of the computer you want to use as a gateway. This can be a Windows computer name, an Internet domain name, or an IP address. You can also add port information to the server name (for example: **RDGateway:443** or **10.0.0.1:443**).
    - **User account** - Select or add a user account to use with the Remote Desktop Gateway you are connecting to. You can also select **Use desktop user account** to use the same credentials as those used for the remote desktop connection.
4. Tap **Save**.

Global app settings

You can set the following global settings in your client by tapping **Settings**:

MANAGED ITEMS

- **User account** - Allows you to Add, edit and delete user accounts saved in the client. This is a good way to update the password for an account after it has changed.
- **Gateway** - Allows you to Add, edit and delete gateway servers saved in the client.
- **Group** - Allows you to Add, edit and delete groups saved in the client. These allow you to easily group connections.

SESSION SETTINGS

- **Start connections in full screen** - When enabled, anytime a connection is launched, the client will use the entire screen of the current monitor.
- **Start each connection in a new window** - When enabled, each connection is launched in a separate window, allowing you to place them on different monitors and switch between them using the taskbar.
- **When resizing the app:** - Allows you control over what happens when the client window is resized. Defaults to **Stretch the content, preserving aspect ratio**.
- **Use keyboard commands with:** - Let's you specify where keyboard commands like *WIN* or *ALT+TAB* are used. The default is to only send them to the session when the connection is in full screen.
- **Prevent the screen from timing out** - Allows you to keep the screen from timing out when a session is active. This is helpful when the connection does not require any interaction for long periods of time.

APP SETTINGS

- **Show Desktop Previews** - Lets you see a preview of a desktop in the Connection Center before you connect to it. By default, this is set to **on**.
- **Help improve Remote Desktop** - Sends anonymous data to Microsoft. We use this data to improve the client. To learn more about how we treat this anonymous, private data, see the Microsoft Privacy Statement. By default, this setting is **on**.

Manage your user accounts

When you connect to a desktop or remote resources, you can save the user accounts to select from again. You can also define user accounts in the client itself, as opposed to saving the user data when you connect to a desktop.

To create a new user account:

1. In the Connection Center, tap **Settings**.
2. Next to User account, tap **+** to add a new user account.
3. Enter the following information:
    - **Username** - The name of the user to save for use with a remote connection. You can enter the user name in any of the following formats: user_name, domain\user_name, or user_name@domain.com.
    - **Password** - The password for the user you specified. This can be left blank to be prompted for a

password during the connection.

4. Tap **Save**.

To delete a user account:

1. In the Connection Center, tap **Settings**.
2. Select the account to delete from the list under User account.
3. Next to User account, tap the edit icon.
4. Tap **Remove this account** at the bottom to delete the user account.
5. You can also edit the user account and tap **Save**.

Navigate the Remote Desktop session

When you start a remote desktop connection, there are tools available that you can use to navigate the session.

Start a Remote Desktop connection

1. Tap the Remote Desktop connection to start the session.
2. If you haven't saved credentials for the connection, you will be prompted to provide a **Username** and **Password**.
3. If you are asked to verify the certificate for the remote desktop, review the information and ensure this is a PC you trust before tapping **Connect**. You can also select **Don't ask about this certificate again** to always accept this certificate.

Connection Bar

The connection bar gives you access to additional navigation controls. By default, the connection bar is placed in the middle at the top of the screen. Tap and drag the bar to the left or right to move it.

- **Pan Control** - The pan control enables the screen to be enlarged and moved around. Note that pan control is only available on touch-enabled devices and using the direct touch mode.
  - Enable / Disable the pan control: Tap the pan icon in the connection bar to display the pan control and zoom the screen. Tap the pan icon in the connection bar again to hide the control and return the screen to its original resolution.
  - Use the pan control - Tap and hold the pan control and then drag in the direction you want to move the screen.
  - Move the pan control - Double tap and hold the pan control to move the control on the screen.
- **Additional options** - Tap the additional options icon to display the session selection bar and command bar (see below).
- **Keyboard** - Tap the keyboard icon to display or hide the on-screen keyboard. The pan control is displayed automatically when the keyboard is displayed.

Command bar

Tap the **...** on the connection bar to display the command bar on the right-hand side of the screen.

- **Home** - Use the Home button to return to the connection center from the command bar.
  - Alternatively you can use the back button for the same action.
  - Your active session will not be disconnected.
  - This allows you to launch additional connections.
- **Disconnect** - Use the Disconnect button to terminate the connection.
  - Your apps will remain active as long as the session is not terminated on the remote PC.
- **Full-screen** - Enters or exits full screen mode.
- **Touch / Mouse** - You can switch between the mouse modes (Direct Touch and Mouse Pointer).

Use direct touch gestures and mouse modes in a remote session

Two mouse modes are available to interact with the session.

- **Direct touch**: Passes all of the touch contacts to the session to be interpreted remotely.
  - Used in the same way you would use Windows with a touch screen.
- **Mouse pointer**: Transforms your local touch screen into a large touchpad allowing to move a mouse pointer in the session.
  - Used in the same way you would use Windows with a touchpad.

> **NOTE**
> Interacting with Windows 8 or newer the native touch gestures are supported in Direct Touch mode.

MOUSE MODE	MOUSE OPERATION	GESTURE
Direct touch	Left click	1 finger tap
Direct touch	Right click	1 finger tap and hold
Mouse pointer	Left click	1 finger tap
Mouse pointer	Left click and drag	1 finger double tap and hold, then drag
Mouse pointer	Right click	2 finger tap
Mouse pointer	Right click and drag	2 finger double tap and hold, then drag
Mouse pointer	Mouse wheel	2 finger tap and hold, then drag up or down
Mouse pointer	Zoom	Use 2 fingers and pinch to zoom in or move fingers apart to zoom out.

> **TIP**
> Questions and comments are always welcome. However, please do NOT post a request for troubleshooting help by using the comment feature at the end of this article. Instead, go to the Remote Desktop client forum and start a new thread. Have a feature suggestion? Tell us using the Feedback Hub.

What's new in the Windows Store client

1/10/2020 • 2 minutes to read • Edit Online

We regularly update the Windows Store client, adding new features and fixing issues. Here's where you'll find the latest updates.

Updates for version 10.1.1107

Date published: 09/04/2019

- You can now copy files between local and remote PCs.
- You can now use your email address to access remote resources (if enabled by your admin).
- You can now change user account assignments for remote resource feeds.
- The app now shows the proper icon for .rdp files assigned to this app in File Explorer instead of a blank default icon.

Updates for version 10.1.1098

Date published: 03/15/2019

- You can now set a display name for user accounts so you can save the same username with different passwords.
- It is now possible to select an existing user account when adding Remote Resources.
- Fixed an issue where the client wasn't terminating correctly.
- The client now properly handles being suspended when secondary windows are open.
- Additional bug fixes.

Updates for version 10.1.1088

Date published: 11/06/2018

- Connection display name is now more discoverable.
- Fixed a crash when closing the client window while a connection is still active.
- Fix a hang when reconnecting after the client is minimized.
- Allow desktops to be dragged anywhere in a group.
- Ensure launching a connection from the jumplist results in a separate window when needed.
- Additional bug fixes.

Updates for version 10.1.1060

Date published: 09/14/2018

- Addressed an issue where double-clicking a desktop connection caused two sessions to be launched.
- Fixed a crash when switching between virtual desktops locally.
- Moving a session to a different monitor now also updates the session scale factor.
- Handle additional system keys like AltGr.
- Additional bug fixes.

Updates for version 10.1.1046

Date published: 06/20/2018

- Bug fixes.

Updates for version 10.1.1042

Date published: 04/02/2018

- Updates to address CredSSP encryption oracle remediation described in CVE-2018-0886.
- Additional bug fixes.

Get started with the Android client

1/10/2020 • 11 minutes to read • Edit Online

Applies to: Android 4.1 and later

You can use the Remote Desktop client for Android to work with Windows apps and desktops directly from your Android device or a Chromebook that supports the Google Play Store.

Use the following information to get started. Be sure to check out the FAQ if you have any questions.

NOTE

- Curious about the new releases for the Android client? Check out What's new for the Android client.
- The Android client supports devices running Android 4.1 and later, as well as Chromebooks with ChromeOS 53 and later. Learn more about Android applications on Chrome here.

Set up the Remote Desktop client for Android

Download the Remote Desktop client from the Google Play store

Here's how to set up the Remote Desktop client on your Android device:

1. Download the Microsoft Remote Desktop client from Google Play.
2. Launch **RD client** from your list of apps.
3. Add a Remote Desktop connection or remote resources. You use a connection to connect directly to a Windows PC and remote resources to access apps and desktops published to you by an admin.

NOTE

If you want to test new features before they're released, we recommend downloading our Microsoft Remote Desktop Beta client from the Google Play store.

Add a Remote Desktop connection

If you haven't done so already, set up your PC to accept remote connections.

To create a Remote Desktop connection:

1. In the Connection Center, tap **+**, and then tap **Desktop**.
2. Enter the name of the remote PC into **PC name**. This can be a Windows computer name, an Internet domain name, or an IP address. You can also append port information to the PC name (for example, MyDesktop:3389 or 10.0.0.1:3389). This is the only required field.
3. Select the **User name** you use to access the Remote PC.
   - Select **Enter every time** for the client to ask for your credentials every time you connect to the remote PC.
   - Select **Add user account** to save an account that you use frequently so you don't have to enter credentials every time you sign in. See manage your user accounts for more details.
4. You can also tap on **Show additional options** to set the following optional parameters:
   - In **Friendly name**, you can enter an easy-to-remember name for the PC you're connecting to. If you don't specify a friendly name, the PC name is displayed instead.

- The **Gateway** is the Remote Desktop gateway you'll use to connect to a computer from an external network. Contact your system administrator for more information.
- **Sound** selects the device your remote session uses for audio. You can choose to play sound on your local device, the remote device, or not at all.
- **Customize display resolution** sets the resolution for the remote session. When turned off, the resolution specified in global settings is used.
- **Swap mouse buttons** switches the commands sent by right and left mouse gestures. Ideal for left-handed users.
- **Connect to admin session** lets you connect to an admin session on the remote PC.
- **Redirect local storage** enables local storage redirection. This setting is disabled by default.

5. When you're done, tap **Save**.

Need to edit these settings? Tap the **More options** menu (**...**) next to the name of the desktop, and then tap **Edit**.

Want to remove the connection? Again, tap the **More options** menu (**...**), and then tap **Remove**.

> **TIP**
> If you get error 0xf07 about a bad password ("We couldn't connect to the remote PC because the password associated with the user account has expired"), change your password and try again.

Add remote resources

Remote resources are RemoteApp programs, session-based desktops, and virtual desktops published by your admin. The Android client supports resources published from **Remote Desktop Services** and **Windows Virtual Desktop** deployments. To add remote resources:

1. In the Connection Center, tap **+**, and then tap **Remote Resource Feed**.
2. Enter the **Feed URL**. This can be a URL or email address:
   - The **URL** is the RD Web Access server provided to you by your admin. If accessing resources from Windows Virtual Desktop, you can use `https://rdweb.wvd.microsoft.com`.
   - If you plan to use **Email**, enter your email address in this field. This tells the client to search for an RD Web Access server associated with your email address if it was configured by your admin.
3. Tap **Next**.
4. Provide your sign in information when prompted. This can vary based on the deployment and can include:
   - The **User name** that has permission to access the resources.
   - The **Password** associated with the user name.
   - **Additional factor**, which you may be prompted for a if authentication was configured that way by your admin.
5. When you're done, tap **Save**.

The remote resources will be displayed in the Connection Center.

To remove remote resources:

1. In the Connection Center, tap the overflow menu (**...**) next to the remote resource.
2. Tap **Remove**.
3. Confirm the removal.

Use a widget to pin a saved desktop to your home screen

The Remote Desktop client supports pinning connections to your home screen by using the Android widget feature. The way that you add a widget depends on the type of Android device you are using and its operating system. Here is the most common way to add a widget:

1. Tap **Apps** to launch the apps menu.
2. Tap **Widgets**.
3. Swipe through the widgets and look for the Remote Desktop icon with the description: "Pin Remote Desktop."
4. Tap and hold that Remote Desktop widget and move it to the home screen.
5. When you release the icon, you'll see the saved remote desktops. Choose the connection that you want to save to your home screen.

Now you can start the remote desktop connection directly from your home screen by tapping it.

> **NOTE**
> If you rename the desktop connection in the Remote Desktop client, its pinned label won't update.

Manage general app settings

To change the general app settings, go to the Connection Center, tap **Settings**, and then tap **General**.

You can set the following general settings:

- **Show desktop previews** lets you see a preview of a desktop in the Connection Center before you connect to it. This setting is enabled by default.
- **Pinch to zoom remote session** lets you use pinch-to-zoom gestures. If the app you're using through Remote Desktop supports multi-touch (introduced in Windows 8), disable this feature.
- Enable **Use scancode input when available** if your remote app doesn't respond properly to keyboard input sent as scancode. Input is sent as unicode when disabled.
- **Help improve Remote Desktop** sends anonymous data about how you use Remote Desktop for Android to Microsoft. We use this data to improve the client. To learn more about our privacy policy and what kinds of data we collect, see the Microsoft Privacy Statement. This setting is enabled by default.

Manage display settings

To change the display settings tap **Settings**, and then tap **Display** from the Connection Center.

You can set the following display settings:

- **Orientation** sets the preferred orientation (landscape or portrait) for your session.

  > **NOTE**
  > If you connect to a PC running Windows 8 or earlier, the session won't scale correctly if the orientation of the device changes. To make the client scale correctly, disconnect from the PC, then reconnect in the orientation you want to use. You can also ensure correct scaling by using a PC with Windows 10 instead.

- **Resolution** sets the remote resolution you want to use for desktop connections globally. If you have already set a custom resolution for an individual connection, this setting won't change that.

  > **NOTE**
  > When you change the display settings, the changes only apply to new connections you make after the you changed the setting. To apply your changes to the session you're currently connected to, refresh your session by disconnecting and reconnecting.

Manage your RD Gateways

A Remote Desktop Gateway (RD Gateway) lets you connect to a remote computer on a private network from anywhere on the Internet. You can create and manage your gateways using the Remote Desktop client.

To set up a new RD Gateway:

1. In the Connection Center, tap **Settings**, and then tap **Gateways**.
2. Tap **+** to add a new gateway.
3. Enter the following information:
   - Enter the name of the computer you want to use as a gateway into **Server name**. This can be a Windows computer name, an Internet domain name, or an IP address. You can also add port information to the server name (for example: RDGateway:443 or 10.0.0.1:443).
   - Select the **User account** you'll use to access the RD Gateway.
     - Select **Use desktop user account** to use the same credentials that you specified for the remote PC.
     - Select **Add user account** to save an account that you use frequently so you don't have to enter credentials every time you sign in. For more information, see Manage your user accounts.

To delete an RD Gateway:

1. In the Connection Center, tap **Settings**, and then tap **Gateways**.
2. Tap and hold a gateway in the list to select it. You can select multiple gateways at once.
3. Tap the trash can to delete the selected gateway.

Manage your user accounts

You can save user accounts to use whenever you connect to a remote desktop or remote resources.

To save a user account:

1. In the Connection Center, tap **Settings**, and then tap **User accounts**.
2. Tap **+** to add a new user account.
3. Enter the following information:
   - The **User Name** to save for use with a remote connection. You can enter the user name in any of the following formats: user_name, domain\user_name, or user_name@domain.com.
   - The **Password** for the user you specified. Every user account that you want to save to use for remote connections needs to have a password associated with it.
4. When you're done, tap **Save**.

To delete a saved user account:

1. In the Connection Center, tap **Settings**, and then tap **User accounts**.
2. Tap and hold a user account in the list to select it. You can select multiple users at the same time.
3. Tap the trash can to delete the selected user.

Navigate the Remote Desktop session

Here's a brief introduction to how to open and navigate your Remote Desktop session.

Start a Remote Desktop connection

1. Tap **the name of your Remote Desktop connection** to start the session.
2. If you're asked to verify the certificate for the remote desktop, tap **Connect**. You can also select **Don’t ask me again for connections to this computer** to always accept the certificate by default.

Connection bar

The connection bar gives you access to additional navigation controls. By default, the connection bar is placed in the middle at the top of the screen. Drag the bar to the left or right to move it.

- **Pan Control**: The pan control enables the screen to be enlarged and moved around. Pan control is only available for direct touch.
  - To show the pan control, tap the pan icon in the connection bar to display the pan control and zoom the screen. Tap the pan icon again to hide the control and return the screen to its original size.
  - To use the pan control, tap and hold it, then drag it in the direction you want to move the screen.
  - To move the pan control, double-tap and hold it to move the control around on the screen.
- **Additional options**: Tap the additional options icon to display the session selection bar and command bar.
- **Keyboard**: Tap the keyboard icon to display or hide the keyboard. The pan control is displayed automatically when the keyboard is displayed.

Session selection bar

You can have multiple connections open to different PCs at the same time. Tap the connection bar to display the session selection bar on the left-hand side of the screen. The session selection bar lets you view your open connections and switch between them.

When you're connected to remote resources, you can switch between apps within that session by tapping the expander menu (**>**) and choosing from the list of available items.

To start a new session within your current connection, tap **Start New**, then choose from the list of available items.

To disconnect a session, tap **X** in the left-hand side of the session tile.

Command bar

Tap the connection bar to display the command bar on the right-hand side of the screen. On the command bar, you can switch between mouse modes (direct touch and mouse pointer) or tap the Home button to return to the Connection Center. You can also tap the Back button to return to the Connection Center. Returning to the Connection Center won't disconnect your active session.

Use touch gestures and mouse modes in a remote session

The client uses standard touch gestures. You can also use touch gestures to replicate mouse actions on the remote desktop. The following table explains which gestures match which mouse actions in each mouse mode.

> **NOTE**
> Native touch gestures are supported in Direct Touch mode in Windows 8 or later.

MOUSE MODE	MOUSE ACTION	GESTURE
Direct touch	Left-click	Tap with one finger
Direct touch	Right-click	Tap with one finger and hold, then release
Mouse pointer	Zoom	Use two fingers and pinch to zoom out or move fingers apart to zoom in.
Mouse pointer	Left-click	Tap with one finger

MOUSE MODE	MOUSE ACTION	GESTURE
Mouse pointer	Left-click and drag	Double-tap and hold with one finger, then drag
Mouse pointer	Right-click	Tap with two fingers
Mouse pointer	Right-click and drag	Double-tap and hold with two fingers, then drag
Mouse pointer	Mouse wheel	Tap and hold with two fingers, then drag up or down

What's new in the Android client

1/10/2020 • 2 minutes to read • Edit Online

We regularly update the Remote Desktop client for Android, adding new features and fixing issues. Here's where you'll find the latest updates.

Updates for version 8.1.71

Date published: 06/05/2019

- Removed support for Android versions 4.0.3 and 4.0.4.
- Fixed an issue where remote resources of the same name didn't show correctly.
- Updated the app icon.
- Minor bug fixes and improvements.

Updates for version 8.1.70

Date published: 05/06/2019

- Addressed issues that caused the session content to not be sized properly on devices with notch display.
- Fixed an issue where the Enter key didn't work on some Chromebook devices.
- Fixed an issue where some Remote Resource Feed URL didn't load.

Updates for version 8.1.69

Date published: 04/22/2019

- Minor bug fixes and improvements.

Updates for version 8.1.68

Date published: 04/15/2019

- Fixed an issue where the Remote Resource Feed URL didn't load.
- Fixed an issue where the app started in phone size on first launch on Samsung DeX running Android 9.0.
- Updated the app icon.
- Additional bug fixes.

Updates for version 8.1.67

Date published: 03/28/2019

- Fixed an issue where key presses were repeated while typing in a remote session.

Updates for version 8.1.66

Date published: 03/19/2019

- Added initial support for Windows Virtual Desktop.
- Fixed an issue that caused a black area to be shown at the bottom of the screen on some Chromebook devices and DeX scenarios.

- Added immersive mode support for Samsung DeX, hiding the bottom taskbar.
- Added support for sending Meta and Alt keys from the physical keyboard to the remote session for Samsung DeX.
- The mouse pointer now updates based on the content of the remote session (Android 7.0+)
- Additional bug fixes.

Updates for version 8.1.61

Date published: 07/05/2018

- Added initial support for Samsung DeX (Android 8.0+).

Updates for version 8.1.60

Date published: 04/30/2018

- Updates to address CredSSP encryption oracle remediation described in CVE-2018-0886.
- Fixed a crash when launching connections carried over from a previous version.

Get started with the iOS client

1/14/2020 • 11 minutes to read • Edit Online

Applies to: Windows 10, Windows 8.1, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2

You can use the Remote Desktop client for iOS to work with Windows apps, resources, and desktops from your iOS device (iPhones and iPads).

Use the following information to get started. Be sure to check out the FAQ if you have any questions.

NOTE

- Curious about the new releases for the iOS client? Check out What's new for Remote Desktop on iOS?
- The iOS client supports devices running iOS 6.x and newer.

Get the Remote Desktop Beta client and start using it

The iOS Beta client available today through Apple TestFlight supports connections to Windows Virtual Desktop resources.

Download the Remote Desktop iOS Beta client from Apple TestFlight

Here's how to set up the Remote Desktop Beta client on your iOS device:

1. Install the Apple TestFlight app on your iOS device.
2. On your iOS device, open a browser and navigate to aka.ms/rdiosbeta.
3. Under the label **Step 2 Join the Beta** select **Start Testing**.
4. When you are redirected to the TestFlight app, select **Accept** and then **Install** the client.

Add a connection to a PC

To create a remote connection to a PC:

1. In the Connection Center, tap **+**, and then tap **Add PC**.
2. Enter the name of the remote PC into **PC Name**. This can be a Windows computer name, an Internet domain name, or an IP address. You can also append port information to the PC name (for example, **MyDesktop:3389** or **10.0.0.1:3389**).
3. Select the **User Account** you'll use to access the remote PC.
   - Select **Ask Every Time** for the client to ask for your credentials every time you connect to the remote PC.
   - Select **Add User Account** to save an account that you use frequently so you don't have to enter credentials every time you sign in. Follow these instructions to manage your user accounts.
4. You can also set the following optional parameters:
   - In **Friendly Name**, you can enter an easier-to-remember name for the PC you're connecting to.
   - **Admin Mode** lets you connect to an admin session on the remote PC.
   - **Swap Mouse Buttons** switches the commands sent by right and left mouse gestures. Ideal for left-handed users.
   - The **Gateway** is the Remote Desktop gateway you'll use to connect to a computer from an external network. Contact your system administrator for more information.

- **Sound** selects the device your remote session uses for audio. You can choose to play sound on your local device, the remote device, or not at all.
- **Microphone** enables microphone redirection. This setting is disabled by default.
- **Camera** enables camera redirection. This setting is disabled by default.
- **Clipboard** enables clipboard redirection. This setting is enabled by default.
- **Storage** enables local storage redirection. This setting is disabled by default.

5. Select **Save** to add the remote PC connection.

Add remote resources

Remote resources are RemoteApp programs, session-based desktops, and virtual desktops published by your admin. The iOS client supports resources published from **Remote Desktop Services** and **Windows Virtual Desktop** deployments. To add remote resources:

1. In the Connection Center tap **+**, and then tap **Add Workspace**.
2. Enter the **Feed URL**. This can be a URL or email address:
   - The **URL** is the RD Web Access server's URL, provided to you by your admin. If accessing resources from Windows Virtual Desktop, you can use `https://rdweb.wvd.microsoft.com`.
   - If you plan to use **Email**, enter your email address in this field. This tells the client to search for an RD Web Access server associated with your email address if it was configured by your admin.
3. Tap **Next**.
4. Provide your sign in information when prompted. This can vary based on the deployment and can include:
   - **User name**, the user name that has permission to access the resources.
   - **Password**, the password associated with the user name.
   - **Additional factor**, which you may be prompted for if authentication was configured that way by your admin.
5. Tap **Save**.

The remote resources will be displayed in the Connection Center.

Get the Remote Desktop client and start using it

Download the Remote Desktop client from the iOS store

Follow these steps to get started with Remote Desktop on your iOS device:

1. Download the Microsoft Remote Desktop client from iTunes.
2. Set up your PC to accept remote connections.
3. Add a Remote Desktop connection or a remote resource. You use a connection to connect to a directly to a Windows PC and a remote resource to use a RemoteApp program, session-based desktop, or a virtual desktop published on-premises using RemoteApp and Desktop Connections. This feature is typically available in corporate environments.

Add a Remote Desktop connection

To create a remote desktop connection:

1. In the Connection Center tap **+**, and then tap **Add PC or Server**.
2. Enter the following information for the remote desktop connection:
   - **PC name** – the name of the computer. This can be a Windows computer name, an Internet domain name, or an IP address. You can also append port information to the PC name (for example, **MyDesktop:3389** or **10.0.0.1:3389**).
   - **User name** – The user name to use to access the remote PC. You can use the following formats: *user_name*, *domain**user_name*, or `user_name@domain.com`. You can also specify whether to prompt for a user name and password.

3. You can also set the following additional options:
   - **Friendly name (optional)** – An easy-to-remember name for the PC you are connecting to. You can use any string, but if you do not specify a friendly name, the PC name is displayed.
   - **Gateway (optional)** – The Remote Desktop gateway that you want to use to connect to virtual desktops, RemoteApp programs, and session-based desktops on an internal corporate network. Get the information about the gateway from your system administrator.
   - **Sound** – Select the device to use for audio during your remote session. You can choose to play sound on the local devices, the remote device, or not at all.
   - **Swap mouse buttons** – Whenever a mouse gesture would send a command with the left mouse button, it sends the same command with the right mouse button instead. This is necessary if the remote PC is configured for left-handed mouse mode.
   - **Admin Mode** - Connect to an administration session on a server running Windows Server 2003 or later.
4. Tap **Save**.

Need to edit these settings? Press and hold the desktop you want to edit, and then tap the settings icon.

Add a remote resource

Remote resources are RemoteApp programs, session-based desktops, and virtual desktops published using RemoteApp and Desktop Connections.

- The URL displays the link to the RD Web Access server that gives you access to RemoteApp and Desktop Connections.
- The configured RemoteApp and Desktop Connections are listed.

To add a remote resource:

1. On the Connection Center screen, tap **+**, and then tap **Add Remote Resources**.
2. Enter information for the remote resource:
   - **Feed URL** - The URL of the RD Web Access server. You can also enter your corporate email account in this field – this tells the client to search for the RD Web Access Server associated with your email address.
   - **User name** - The user name to use for the RD Web Access server you are connecting to.
   - **Password** - The password to use for the RD Web Access server you are connecting to.
3. Tap **Save**.

The remote resources will be displayed in the Connection Center.

Manage your user accounts

When you connect to a desktop or remote resources, you can save the user accounts to select from again.

To create a new user account:

1. In the Connection Center, tap **Settings**, and then tap **User Accounts**.
2. Tap **Add User Account**.
3. Enter the following information:
   - **User Name** - The name of the user to save for use with a remote connection. You can enter the user name in any of the following formats: user_name, domain\user_name, or user_name@domain.com.
   - **Password** - The password for the user you specified. Every user account that you want to save to use for remote connections needs to have an associated password.
4. Tap **Save**.

To delete a user account:

1. In the Connection Center, tap **Settings**, and then tap **User Accounts**.
2. Select the account you would like to delete.
3. Tap **Delete**.

Connect to an RD Gateway to access internal assets

A Remote Desktop Gateway (RD Gateway) lets you connect to a remote computer on a corporate network from anywhere on the Internet. You can create and manage your gateways using the Remote Desktop client.

To set up a new gateway:

1. In the Connection Center, tap **Settings** > **Gateways**.
2. Tap **Add Remote Desktop gateway**.
3. Enter the following information:
   - **Server name** – The name of the computer you want to use as a gateway. This can be a Windows computer name, an Internet domain name, or an IP address. You can also add port information to the server name (for example, **RDGateway:443** or **10.0.0.1:443**).
   - **User name** - The user name and password to be used for the Remote Desktop gateway you are connecting to. You can also select **Use connection credentials** to use the same user name and password as those used for the remote desktop connection.

Navigate the Remote Desktop session

When you start a remote desktop session, there are tools available that you can use to navigate the session.

Start a Remote Desktop Connection

1. Tap the remote desktop connection to start the remote desktop session.
2. If you are asked to verify the certificate for the remote desktop, tap **Accept**. You can choose to always accept by sliding the **Don't ask me again for connections to this computer** toggle to **ON**.

Connection Bar

The connection bar gives you access to additional navigation controls.

- **Pan Control**: The pan control enables the screen to be enlarged and moved around. Note that pan control is only available using direct touch.
  - Enable / Disable the pan control: Tap the pan icon in the connection bar to display the pan control and zoom the screen. Tap the pan icon in the connection bar again to hide the control and return the screen to its original resolution.
  - Use the pan control: Tap and hold the pan control and then drag in the direction you want to move the screen.
  - Move the pan control: Double tap and hold the pan control to move the control on the screen.
- **Connection name**: The current connection name is displayed. Tap the connection name to display the session selection bar.
- **Keyboard**: Tap the keyboard icon to display or hide the keyboard. The pan control is displayed automatically when the keyboard is displayed.
- **Move the connection bar**: Tap and hold the connection bar, and then drag and drop to a new location at the top of the screen.

Session selection

You can have multiple connections open to different PCs at the same time. Tap the connection bar to display the session selection bar on the left-hand side of the screen. The session selection bar enables you to view your open connections and switch between them.

- Switch between apps in an open remote resource session.

  When you are connected to remote resources, you can switch between open applications within that session by tapping the expander menu and choosing from the list of available items.

- Start a new session

  You can start new applications or desktop sessions from within your current connection: tap **Start New**, and then choose from the list of available items.

- Disconnection a session

  To disconnect a session tap X in the left-hand side of the session tile.

Command bar

The command bar replaced the Utility bar starting in version 8.0.1. You can switch between the mouse modes and return to the connection center from the command bar.

Use touch gestures and mouse modes in a remote session

The client uses standard touch gestures. You can also use touch gestures to replicate mouse actions on the remote desktop. The mouse modes available are defined in the table below.

> **NOTE**
> Interacting with Windows 8 or newer the native touch gestures are supported in Direct Touch mode. For more information on Windows 8 gestures see Touch: Swipe, tap, and beyond.

MOUSE MODE	MOUSE OPERATION	GESTURE
Direct touch	Left click	1 finger tap
Direct touch	Right click	1 finger tap and hold
Mouse pointer	Left click	1 finger tap
Mouse pointer	Left click and drag	1 finger double tap and hold, then drag
Mouse pointer	Right click	2 finger tap
Mouse pointer	Right click and drag	2 finger double tap and hold, then drag
Mouse pointer	Mouse wheel	2 finger tap and hold, then drag up or down
Mouse pointer	Zoom	Pinch 2 fingers to zoom in or spread 2 fingers to zoom out

Supported input devices

The Remote Desktop iOS beta client supports the Swiftpoint GT and ProPoint physical mice. Swiftpoint is offering an exclusive discount on the GT for iOS beta client users.

The iOS client currently only supports Swiftpoint mice. Refer to the What's new in the iOS client page and the iOS App Store for news about support for other devices in the future.

Use a keyboard in a remote session

You can use either an on-screen keyboard or physical keyboard in your remote session.

For on-screen keyboards, use the button on the right edge of the bar above the keyboard to switch between the standard and additional keyboard.

If Bluetooth is enabled for your iOS device, the client automatically detects the Bluetooth keyboard.

Be aware that, due to limitations on the OS, special keys such as Ctrl, Option, and Function will not work as expected with a Bluetooth keyboard. The following keys work:

- Alphanumeric keys
- Cursor keys
- Tab: Tab works, but Shift+Tab does not work
- Home / Pos1: Alt+Left = Home
- End: Alt+Right = End
- Page Up: Alt+Up = Page Up
- Page Down: Alt+Down = Page Down
- Select All: Command+A = Ctrl+A (Select all in most programs)
- Cut: Command+X = Ctrl+X (Cut in most programs)
- Copy: Command+C = Ctrl+C (Copy in most programs)
- Paste: Command+V = Ctrl+V (Paste in most programs)
- Symbols: Alt+Alphanumeric keys will produce different symbols depending on the language configured

> **TIP**
> Questions and comments are always welcome. However, please do NOT post a request for troubleshooting help by using the comment feature at the end of this article. Instead, go to the Remote Desktop client forum and start a new thread. Have a feature suggestion? Tell us in the client user voice forum.

What's new in the iOS client

1/10/2020 • 2 minutes to read • Edit Online

We regularly update the Remote Desktop client for iOS, adding new features and fixing issues. You'll find the latest updates on this page.

Updates for version 10.0.0

Date published: 12/13/19

It's been well over a year since we last updated the Remote Desktop Client for iOS. However, we're back with an exciting new update, and there will be many more updates to come on a regular basis from here on out. Here's what's new in version 10.0.0:

- Support for the Windows Virtual Desktop service.
- A new Connection Center UI.
- A new in-session UI that can switch between connected PCs and apps.
- New layout for the auxiliary on-screen keyboard.
- Improved external keyboard support.
- SwiftPoint Bluetooth mouse support.
- Microphone redirection support.
- Local storage redirection support.
- Camera redirection support (only available for Windows 10, version 1809 or later).
- Support for new iPhone and iPad devices.
- Dark and light theme support.
- Control whether your phone can lock when connected to a remote PC or app.
- You can now collapse the in-session connection bar by pressing and holding the Remote Desktop logo button.

Updates for version 8.1.42

Date published: 06/20/2018

- Bug fixes and performance improvements.

Updates for version 8.1.41

Date published: 03/28/2018

- Updates to address CredSSP encryption oracle remediation described in CVE-2018-0886.

How to report issues

We're committed to making this app the best it can be and value your feedback. You can report issues to us by navigating to **Settings** > **Report an Issue** in the client.

Get started with the macOS client

1/14/2020 • 7 minutes to read • Edit Online

Applies To: Windows 10, Windows 8.1, Windows Server 2012 R2, Windows Server 2016

You can use the Remote Desktop client for Mac to work with Windows apps, resources, and desktops from your Mac computer. Use the following information to get started - and check out the FAQ if you have questions.

NOTE

- Curious about the new releases for the macOS client? Check out What's new for Remote Desktop on Mac?
- The Mac client runs on computers running macOS 10.10 and newer.
- The information in this article applies primarily to the full version of the Mac client - the version available in the Mac AppStore. Test-drive new features by downloading our preview app here: beta client release notes.

Get the Remote Desktop client

Follow these steps to get started with Remote Desktop on your Mac:

1. Download the Microsoft Remote Desktop client from the Mac App Store.
2. Set up your PC to accept remote connections. (If you skip this step, you can't connect to your PC.)
3. Add a Remote Desktop connection or a remote resource. You use a connection to connect directly to a Windows PC and a remote resource to use a RemoteApp program, session-based desktop, or a virtual desktop published on-premises using RemoteApp and Desktop Connections. This feature is typically available in corporate environments.

What about the Mac beta client?

We're testing new features on our preview channel on HockeyApp. Want to check it out? Go to Microsoft Remote Desktop for Mac and click **Download**. You don't need to create an account or sign into HockeyApp to download the beta client.

If you already have the client, you can check for updates to ensure you have the latest version. In the beta client, click **Microsoft Remote Desktop Beta** at the top, and then click **Check for updates**.

Add a Remote Desktop connection

To create a remote desktop connection:

1. In the Connection Center, click **+**, and then click **Desktop**.
2. Enter the following information:

   - **PC name** - the name of the computer.
     - This can be a Windows computer name (found in the **System** settings), a domain name, or an IP address.
     - You can also add port information to the end of this name, like *MyDesktop:3389*.
   - **User Account** - Add the user account you use to access the remote PC.
     - For Active Directory (AD) joined computers or local accounts, use one of these formats: *user_name*, *domain\user_name*, or *user_name@domain.com*.

    - For Azure Active Directory (AAD) joined computers, use one of these formats: *AzureAD\user_name* or *AzureAD\user_name@domain.com*.
    - You can also choose whether to require a password.
    - When managing multiple user accounts with the same user name, set a friendly name to differentiate the accounts.
    - Manage your saved user accounts in the preferences of the app.
3. You can also set these optional settings for the connection:

    - Set a friendly name
    - Add a Gateway
    - Set the sound output
    - Swap mouse buttons
    - Enable Admin Mode
    - Redirect local folders into a remote session
    - Forward local printers
    - Forward Smart Cards
4. Click **Save**.

To start the connection, just double-click it. The same is true for remote resources.

Export and import connections

You can export a remote desktop connection definition and use it on a different device. Remote desktops are saved in separate .RDP files.

1. In the Connection Center, right-click the remote desktop.
2. Click **Export**.
3. Browse to the location where you want to save the remote desktop .RDP file.
4. Click **OK**.

Use the following steps to import a remote desktop .RDP file.

1. In the menu bar, click **File** > **Import**.
2. Browse to the .RDP file.
3. Click **Open**.

Add a remote resource

Remote resources are RemoteApp programs, session-based desktops, and virtual desktops published using RemoteApp and Desktop Connections.

- The URL displays the link to the RD Web Access server that gives you access to RemoteApp and Desktop Connections.
- The configured RemoteApp and Desktop Connections are listed.

To add a remote resource:

1. In the Connection Center click **+**, and then click **Add Remote Resources**.
2. Enter information for the remote resource:
    - **Feed URL** - The URL of the RD Web Access server. You can also enter your corporate email account in this field – this tells the client to search for the RD Web Access Server associated with your email address.
    - **User name** - The user name to use for the RD Web Access server you are connecting to.
    - **Password** - The password to use for the RD Web Access server you are connecting to.

3. Click **Save**.

The remote resources will be displayed in the Connection Center.

Connect to an RD Gateway to access internal assets

A Remote Desktop Gateway (RD Gateway) lets you connect to a remote computer on a corporate network from anywhere on the Internet. You can create and manage your gateways in the preferences of the app or while setting up a new desktop connection.

To set up a new gateway in preferences:

1. In the Connection Center, click **Preferences > Gateways**.
2. Click the **+** button at the bottom of the table Enter the following information:
   - **Server name** – The name of the computer you want to use as a gateway. This can be a Windows computer name, an Internet domain name, or an IP address. You can also add port information to the server name (for example: **RDGateway:443** or **10.0.0.1:443**).
   - **User name** - The user name and password to be used for the Remote Desktop gateway you are connecting to. You can also select **Use connection credentials** to use the same user name and password as those used for the remote desktop connection.

Manage your user accounts

When you connect to a desktop or remote resources, you can save the user accounts to select from again. You can manage your user accounts by using the Remote Desktop client.

To create a new user account:

1. In the Connection Center, click **Settings** > **Accounts**.
2. Click **Add User Account**.
3. Enter the following information:
   - **User Name** - The name of the user to save for use with a remote connection. You can enter the user name in any of the following formats: user_name, domain\user_name, or user_name@domain.com.
   - **Password** - The password for the user you specified. Every user account that you want to save to use for remote connections needs to have a password associated with it.
   - **Friendly Name** - If you are using the same user account with different passwords, set a friendly name to distinguish those user accounts.
4. Tap **Save**, and then tap **Settings**.

Customize your display resolution

You can specify the display resolution for the remote desktop session.

1. In the Connection Center, click **Preferences**.
2. Click **Resolution**.
3. Click **+**.
4. Enter a resolution height and width, and then click **OK.**

To delete the resolution, select it, and then click **-**.

Displays have separate spaces If you are running Mac OS X 10.9 and disabled **Displays have separate spaces** in Mavericks (**System Preferences > Mission Control**), you need to configure this setting in the remote desktop client using the same option.

Drive redirection for remote resources

Drive redirection is supported for remote resources, so that you can save files created with a remote application locally to your Mac. The redirected folder is always your home directory displayed as a network drive in the remote session.

> **NOTE**
> In order to use this feature, the administrator needs to set the appropriate settings on the server.

Use a keyboard in a remote session

Mac keyboard layouts differ from the Windows keyboard layouts.

- The Command key on the Mac keyboard equals the Windows key.
- To perform actions that use the Command button on the Mac, you will need to use the control button in Windows (e.g.: Copy = Ctrl + C).
- The function keys can be activated in the session by pressing additionally the FN key (e.g.: FN + F1).
- The Alt key to the right of the space bar on the Mac keyboard equals the Alt Gr/right Alt key in Windows.

By default, the remote session will use the same keyboard locale as the OS you're running the client on. (If your Mac is running an en-us OS, that will be used for the remote sessions as well.) If the OS keyboard locale is not used, check the keyboard setting on the remote PC and change it manually. See the Remote Desktop Client FAQ for more information about keyboards and locales.

Support for Remote Desktop gateway pluggable authentication and authorization

Windows Server 2012 R2 introduced support for a new authentication method, Remote Desktop Gateway pluggable authentication and authorization, which provides more flexibility for custom authentication routines. You can now this authentication model with the Mac client.

> **IMPORTANT**
> Custom authentication and authorization models before Windows 8.1 are not supported, although the article above discusses them.

To learn more about this feature, check out https://aka.ms/paa-sample.

> **TIP**
> Questions and comments are always welcome. However, please do NOT post a request for troubleshooting help by using the comment feature at the end of this article. Instead, go to the Remote Desktop client forum and start a new thread. Have a feature suggestion? Tell us in the client user voice forum.

What's new in the macOS client

1/10/2020 • 13 minutes to read • Edit Online

We regularly update the Remote Desktop client for macOS, adding new features and fixing issues. Here's where you'll find the latest updates.

If you encounter any issues, you can always contact us by navigating to **Help** > **Report an Issue**.

Updates for version 10.3.7

Date published: 1/6/20

In our final update of the year, we finetuned some code and fixed the following behaviors:

- Copying things from the remote session to a network share or USB drive no longer creates empty files.
- Specifying an empty password in a user account no longer causes a double certificate prompt.

Updates for version 10.3.6

Date published: 1/6/20

In this release, we addressed an issue that created zero-length files whenever you copied a folder from the remote session to the local machine using file copy and paste.

Updates for version 10.3.5

Date published: 1/6/20

We made this update with the help of everyone who reported issues. In this version, we've made the following changes:

- Redirected folders can now be marked as read-only to prevent their contents from being changed in the remote session.
- We addressed a 0x607 error that appeared when connecting using RPC over HTTPS RD Gateway scenarios.
- Fixed cases where users were double-prompted for credentials.
- Fixed cases where users received the certificate warning prompt twice.
- Added heuristics to improve trackpad-based scrolling.
- The client no longer shows the "Saved Desktops" group if there are no user-created groups.
- Updated UI for the tiles in PC view.
- Fixes to address crashes sent to us via application telemetry.

> **NOTE**
> In this release, we now accept feedback for the Mac client only through UserVoice.

Updates for version 10.3.4

Date published: 11/18/19

We've been hard at work listening to your feedback and have put together a collection of bug fixes and feature updates.

- When connecting via an RD Gateway with multifactor authentication, the gateway connection will be held open to avoid multiple MFA prompts.
- All the client UI is now fully keyboard-accessible with Voiceover support.
- Files copied to the clipboard in the remote session are now only transferred when pasting to the local computer.
- URLs copied to the clipboard in the remote session now paste correctly to the local computer.
- Scale factor remoting to support Retina displays is now available for multimonitor scenarios.
- Addressed a compatibility issue with FreeRDP-based RD servers that was causing connectivity issues in redirection scenarios.
- Addressed smart card redirection compatibility with future releases of Windows 10.
- Addressed an issue specific to macOS 10.15 where the incorrect available space was reported for redirected folders.
- Published PC connections are represented with a new icon in the Workspaces tab.
- "Feeds" are now called "Workspaces," and "Desktops" are now called "PCs."
- Fixed inconsistencies and bugs in user account handling in the preferences UI.
- Lots of bug fixes to make things run smoother and more reliably.

Updates for version 10.3.3

Date published: 11/18/19

We've put together a feature update and fixed bugs for the 10.3.3 release.

First, we've added user defaults to disable smart card, clipboard, microphone, camera, and folder redirection:

- ClientSettings.DisableSmartcardRedirection
- ClientSettings.DisableClipboardRedirection
- ClientSettings.DisableMicrophoneRedirection
- ClientSettings.DisableCameraRedirection
- ClientSettings.DisableFolderRedirection

Next, the bug fixes:

- Resolved an issue that was causing programmatic session window resizes to not be detected.
- Fixed an issue where the session window contents appeared small when connecting in windowed mode (with dynamic display enabled).
- Addressed initial flicker that occurred when connecting to a session in windowed mode with dynamic display enabled.
- Fixed graphics mispaints that occurred when connected to Windows 7 after toggling fit-to-window with dynamic display enabled.
- Fixed a bug that caused an incorrect device name to be sent to the remote session (breaking licensing in some third-party apps).
- Resolved an issue where remote app windows would occupy an entire monitor when maximized.
- Addressed an issue where the access permissions UI appeared underneath local windows.
- Cleaned up some shutdown code to ensure the client closes more reliably.

Updates for version 10.3.2

Date published: 11/18/19

In this release, we fixed a bug that made the display low resolution while connecting to a session

Updates for version 10.3.1

Date published: 11/18/19

We've put together some fixes to address regressions that managed to sneak into the 10.3.0 release.

- Addressed connectivity issues with RD Gateway servers that were using 4096-bit asymmetric keys.
- Fixed a bug that caused the client to randomly stop responding when downloading feed resources.
- Fixed a bug that caused the client to crash while opening.
- Fixed a bug that caused the client to crash while importing connections from Remote Desktop, version 8.

Updates for version 10.3.0

Date published: 8/27/19

It's been a few weeks since we last updated, but we've been hard at work during that time. Version 10.3.0 brings some new features and lots of under-the-hood fixes.

- Camera redirection is now possible when connecting to Windows 10 1809, Windows Server 2019 and later.
- On Mojave and Catalina we've added a new dialog that requests your permission to use the microphone and camera for device redirection.
- The feed subscription flow has been rewritten to be simpler and faster.
- Clipboard redirection now includes the Rich Text Format (RTF).
- When entering your password you have the option to reveal it with a "Show password" checkbox.
- Addressed scenarios where the session window was jumping between monitors.
- The Connection Center displays high resolution remote app icons (when available).
- Cmd+A maps to Ctrl+A when Mac clipboard shortcuts are being used.
- Cmd+R now refreshes all of your subscribed feeds.
- Added new secondary click options to expand or collapse all groups or feeds in the Connection Center.
- Added a new secondary click option to change the icon size in the Feeds tab of the Connection Center.
- A new, simplified, and clean app icon.

Updates for version 10.2.13

Date published: 5/8/2019

- Fixed a hang that occurred when connecting via an RD Gateway.
- Added a privacy notice to the "Add Feed" dialog.

Updates for version 10.2.12

Date published: 4/16/2019

- Resolved random disconnects (with error code 0x904) that took place when connecting via an RD Gateway.
- Fixed a bug that caused the resolutions list in application preferences to be empty after installation.
- Fixed a bug that caused the client to crash if certain resolutions were added to the resolutions list.
- Addressed an ADAL authentication prompt loop when connecting to Windows Virtual Desktop deployments.

Updates for version 10.2.10

Date published: 3/30/2019

- In this release we addressed instability caused by the recent macOS 10.14.4 update. We also fixed mispaints that appeared when decoding AVC codec data encoded by a server using NVIDIA hardware.

Updates for version 10.2.9

Date published: 3/6/2019

- In this release we fixed an RD gateway connectivity issue that can occur when server redirection takes place.
- We also addressed an RD gateway regression caused by the 10.2.8 update.

Updates for version 10.2.8

Date published: 3/1/2019

- Resolved connectivity issues that surfaced when using an RD Gateway.
- Fixed incorrect certificate warnings that were displayed when connecting.
- Addressed some cases where the menu bar and dock would needlessly hide when launching remote apps.
- Reworked the clipboard redirection code to address crashes and hangs that have been plaguing some users.
- Fixed a bug that caused the Connection Center to needlessly scroll when launching a connection.

Updates for version 10.2.7

Date published: 2/6/2019

- In this release we addressed graphics mispaints (caused by a server encoding bug) that appeared when using AVC444 mode.

Updates for version 10.2.6

Date published: 1/28/2019

- Added support for the AVC (420 and 444) codec, available when connecting to current versions of Windows 10.
- In Fit to Window mode, a window refresh now occurs immediately after a resize to ensure that content is rendered at the correct interpolation level.
- Fixed a layout bug that caused feed headers to overlap for some users.
- Cleaned up the Application Preferences UI.
- Polished the Add/Edit Desktop UI.
- Made lots of fit and finish adjustments to the Connection Center tile and list views for desktops and feeds.

> **NOTE**
>
> There is a bug in macOS 10.14.0 and 10.14.1 that can cause the ".com.microsoft.rdc.application-data_SUPPORT/_EXTERNAL_DATA" folder (nested deep inside the ~/Library folder) to consume a large amount of disk space. To resolve this issue, delete the folder content and upgrade to macOS 10.14.2. Note that a side-effect of deleting the folder contents is that snapshot images assigned to bookmarks will be deleted. These images will be regenerated when reconnecting to the remote PC.

Updates for version 10.2.4

Date published: 12/18/2018

- Added dark mode support for macOS Mojave 10.14.
- An option to import from Microsoft Remote Desktop 8 now appears in the Connection Center if it is empty.
- Addressed folder redirection compatibility with some third-party enterprise applications.
- Resolved issues where users were getting a 0x30000069 Remote Desktop Gateway error due to security protocol fallback issues.

- Fixed progressive rendering issues some users were experiencing with fit to window mode.
- Fixed a bug that prevented file copy and paste from copying the latest version of a file.
- Improved mouse-based scrolling for small scroll deltas.

Updates for version 10.2.3

Date published: 11/06/2018

- Added support for the "remoteapplicationcmdline" RDP file setting for remote app scenarios.
- The title of the session window now includes the name of the RDP file (and server name) when launched from an RDP file.
- Fixed reported RD gateway performance issues.
- Fixed reported RD gateway crashes.
- Fixed issues where the connection would hang when connecting through an RD gateway.
- Better handling of full-screen remote apps by intelligently hiding the menu bar and dock.
- Fixed scenarios where remote apps remained hidden after being launched.
- Addressed slow rendering updates when using "Fit to Window" with hardware acceleration disabled.
- Handled database creation errors caused by incorrect permissions when the client starts up.
- Fixed an issue where the client was consistently crashing at launch and not starting for some users.
- Fixed a scenario where connections were incorrectly imported as full-screen from Remote Desktop 8.

Updates for version 10.2.2

Date published: 10/09/2018

- A brand new Connection Center that supports drag and drop, manual arrangement of desktops, resizable columns in list view mode, column-based sorting, and simpler group management.
- The Connection Center now remembers the last active pivot (Desktops or Feeds) when closing the app.
- The credential prompting UI and flows have been overhauled.
- RD Gateway feedback is now part of the connecting status UI.
- Settings import from the version 8 client has been improved.
- RDP files pointing to RemoteApp endpoints can now be imported into the Connection Center.
- Retina display optimizations for single monitor Remote Desktop scenarios.
- Support for specifying the graphics interpolation level (which affects blurriness) when not using Retina optimizations.
- 256-color support to enable connectivity to Windows 2000.
- Fixed clipping of the right and bottom edges of the screen when connecting to Windows 7, Windows Server 2008 R2 and earlier.
- Copying a local file into Outlook (running in a remote session) now adds the file as an attachment.
- Fixed an issue that was slowing down pasteboard-based file transfers if the files originated from a network share.
- Addressed a bug that was causing to Excel (running in a remote session) to hang when saving to a file on a redirected folder.
- Fixed an issue that was causing no free space to be reported for redirected folders.
- Fixed a bug that caused thumbnails to consume too much disk storage on macOS 10.14.
- Added support for enforcing RD Gateway device redirection policies.
- Fixed an issue that prevented session windows from closing when disconnecting from a connection using RD Gateway.
- If Network Level Authentication (NLA) is not enforced by the server, you will now be routed to the login screen if your password has expired.

- Fixed performance issues that surfaced when lots of data was being transferred over the network.
- Smart card redirection fixes.
- Support for all possible values of the "EnableCredSspSupport" and "Authentication Level" RDP file settings if the ClientSettings.EnforceCredSSPSupport user default key (in the com.microsoft.rdc.macos domain) is set to 0.
- Support for the "Prompt for Credentials on Client" RDP file setting when NLA is not negotiated.
- Support for smart card-based login via smart card redirection at the Winlogon prompt when NLA is not negotiated.
- Fixed an issue that prevented downloading feed resources that have spaces in the URL.

Updates for version 10.2.1

Date published: 08/06/2018

- Enabled connectivity to Azure Active Directory (AAD) joined PCs. To connect to an AAD joined PC, your username must be in one of the following formats: "AzureAD\user" or "AzureAD\user@domain".
- Addressed some bugs affecting the usage of smart cards in a remote session.

Updates for version 10.2.0

Date published: 07/24/2018

- Incorporated updates for GDPR compliance.
- MicrosoftAccount\username@domain is now accepted as a valid username.
- Clipboard sharing has been rewritten to be faster and support more formats.
- Copy and pasting text, images or files between sessions now bypasses the local machine's clipboard.
- You can now connect via an RD Gateway server with an untrusted certificate (if you accept the warning prompts).
- Metal hardware acceleration is now used (where supported) to speed up rendering and optimize battery usage.
- When using Metal hardware acceleration we try to work some magic to make the session graphics appear sharper.
- Got rid of some instances where windows would hang around after being closed.
- Fixed bugs that were preventing the launch of RemoteApp programs in some scenarios.
- Fixed an RD Gateway channel synchronization error that was resulting in 0x204 errors.
- The mouse cursor shape now updates correctly when moving out of a session or RemoteApp window.
- Fixed a folder redirection bug that was causing data loss when copy and pasting folders.
- Fixed a folder redirection issue that caused incorrect reporting of folder sizes.
- Fixed a regression that was preventing logging into an AAD-joined machine using a local account.
- Fixed bugs that were causing the session window contents to be clipped.
- Added support for RD endpoint certificates that contain elliptic-curve asymmetric keys.
- Fixed a bug that was preventing the download of managed resources in some scenarios.
- Addressed a clipping issue with the pinned connection center.
- Fixed the checkboxes in the Display tab of the Add a Desktop window to work better together.
- Aspect ratio locking is now disabled when dynamic display change is in effect.
- Addressed compatibility issues with F5 infrastructure.
- Updated handling of blank passwords to ensure the correct messages are shown at connect-time.
- Fixed mouse scrolling compatibility issues with MapInfra Pro.
- Fixed some alignment issues in the Connection Center when running on Mojave.

Updates for version 10.1.8

Date published: 05/04/2018

- Added support for changing the remote resolution by resizing the session window!
- Fixed scenarios where remote resource feed download would take an excessively long time.
- Resolved the 0x207 error that could occur when connecting to servers not patched with the CredSSP encryption oracle remediation update (CVE-2018-0886).

Updates for version 10.1.7

Date published: 04/05/2018

- Made security fixes to incorporate CredSSP encryption oracle remediation updates as described in CVE-2018-0886.
- Improved RemoteApp icon and mouse cursor rendering to address reported mispaints.
- Addressed issues where RemoteApp windows appeared behind the Connection Center.
- Fixed a problem that occurred when you edit local resources after importing from Remote Desktop 8.
- You can now start a connection by pressing ENTER on a desktop tile.
- When you're in full screen view, CMD+M now correctly maps to WIN+M.
- The Connection Center, Preferences, and About windows now respond to CMD+M.
- You can now start discovering feeds by pressing ENTER on the **Adding Remote Resources** page.
- Fixed an issue where a new remote resources feed showed up empty in the Connection Center until after you refreshed.

Updates for version 10.1.6

Date published: 03/26/2018

- Fixed an issue where RemoteApp windows would reorder themselves.
- Resolved a bug that caused some RemoteApp windows to get stuck behind their parent window.
- Addressed a mouse pointer offset issue that affected some RemoteApp programs.
- Fixed an issue where starting a new connection gave focus to an existing session, instead of opening a new session window.
- We fixed an error with an error message - you'll see the correct message now if we can't find your gateway.
- The Quit shortcut (⌘ + Q) is now consistently shown in the UI.
- Improved the image quality when stretching in "fit to window" mode.
- Fixed a regression that caused multiple instances of the home folder to show up in the remote session.
- Updated the default icon for desktop tiles.

Get started with the web client

11/19/2019 • 3 minutes to read • Edit Online

The Remote Desktop web client lets you use a compatible web browser to access your organization's remote resources (apps and desktops) published to you by your admin. You'll be able to interact with the remote apps and desktops like you would with a local PC no matter where you are, without having to switch to a different desktop PC. Once your admin sets up your remote resources, all you need are your domain, user name, password, the URL your admin sent you, and a supported web browser, and you're good to go.

> **NOTE**
> Curious about the new releases for the web client? Check out What's new for Remote Desktop web client?

What you'll need to use the web client

- For the web client, you'll need a PC running Windows, macOS, ChromeOS, or Linux. Mobile devices are not supported at this time.
- A modern browser like Microsoft Edge, Internet Explorer 11, Google Chrome, Safari, or Mozilla Firefox (v55.0 and later).
- The URL your admin sent you.

> **NOTE**
> The Internet Explorer version of the web client does not have audio at this time. Safari may display a gray screen if the browser is resized or enters fullscreen multiple times.

Start using the Remote Desktop client

To sign in to the client, go to the URL your admin sent you. At the sign in page, enter your domain and user name in the format `DOMAIN\username`, enter your password, and then select **Sign in**.

> **NOTE**
> By signing in to the web client, you agree that your PC complies with your organization's security policy.

After you sign in, the client will take you to the **All Resources** tab, which contains all items published to you under one or more collapsible groups, such as the "Work Resources" group. You'll see several icons representing the apps, desktops, or folders containing more apps or desktops that the admin has made available to the work group. You can come back to this tab at any time to launch additional resources.

To start using an app or desktop, select the item you want to use, enter the same user name and password you used to sign in to the web client if prompted, and then select **Submit**. You might also be shown a consent dialog to access local resources, like clipboard and printer. You can choose to not redirect either of these, or select **Allow** to use the default settings. Wait for the web client to establish the connection, and then start using the resource as you would normally.

When you're finished, you can end your session by either selecting the **Sign Out** button in the toolbar at the top of your screen or closing the browser window.

Printing from the Remote Desktop web client

Follow these steps to print from the web client:

1. Start the printing process as you would normally for the app you want to print from.
2. When prompted to choose a printer, select **Remote Desktop Virtual Printer**.
3. After choosing your preferences, select **Print**.
4. Your browser will generate a PDF file of your print job.
5. You can choose to either open the PDF and print its contents to your local printer or save it to your PC for later use.

Copy and paste from the Remote Desktop web client

The web client currently supports copying and pasting text only. Files can't be copied or pasted to and from the web client. Additionally, you can only use **Ctrl+C** and **Ctrl+V** to copy and paste text.

Use an Input Method Editor (IME) in the remote session

To use an Input Method Editor to enter complex characters in the remote session, select the gear icon in the navigation bar to open the **Settings** side panel and set the **Enable Input Method Editor** switch to **On**. You must have an Input Method Editor installed and enabled in the remote session.

Get help with the web client

If you've encountered an issue that can't be solved by the information in this article, you can get help with the web client by emailing the address on the web client's About page.

What's new in the web client

1/10/2020 • 3 minutes to read • Edit Online

We regularly update the Remote Desktop web client, adding new features and fixing issues. Here's where you'll find the latest updates.

> **NOTE**
> We've changed the versioning system for the web client. Starting with version 1.0.18.0, all web client release versions will contain numbers (in the format of "W.X.Y.Z"). Release numbers for the Remote Desktop web client will always end with a 0 (for example, W.X.Y.0). Each Windows Virtual Desktop web client release will change the last digit until the next Remote Desktop web client release (for example, 1.0.18.1).

Updates for version 1.0.21.0

Date published: 11/15/2019

- Added support for using an Input Method Editor (IME) in the remote session to input complex characters.
- Fixed a regression where users could not copy and paste into the remote session on macOS devices.
- Fixed a regression where local Windows Key was sent to the remote session on Firefox.
- Added link to RDWeb password change when enabled by your administrator.

Updates for version 1.0.20.0

Date published: 10/18/2019

- Added support for connections to Windows 7 and Windows Server 2008 R2 hosts.
- Fixed an issue where certain app icons were shown as transparent tiles.
- Fixed connection issues for Internet Explorer browser on Windows 7.
- Fixed unexpected disconnects that happened when the browser was resized.
- Accessibility improvements.
- Updated third-party libraries.

Updates for version 1.0.18.0

Date published: 5/14/2019

- Added Resource Launch Method configuration in the Settings tab, enabling users to either open resources in the browser or download an .rdp file to handle with another client. This setting may be configured by your admin. Details regarding admin configurations for this feature can be found in the web client setup documentation.
- Fixed color rendering issues, enabling more vivid colors in your remote session.
- Revised error messages related to remote resource feed errors.
- Added support for more office shortcuts, such as paste special (Ctrl+Alt+V).
- Added keyboard shortcut for users to invoke the Windows Key in the remote session (Alt+F3)
- Updated error message for users attempting to authenticate using an expired password.
- Refreshed feed UI on the All Resources page.
- Resolved overlapping dialogues that occurred during session reconnect.

- Fixed remote resource icon sizing in the resource taskbar.

Updates for version 1.0.11

Date published: 2/22/2019

- Enabled connection to RD Broker without an RD Gateway in Windows Server 2019.
- Sorted feeds alphabetically (i.e., RemoteApps first, Desktops second).
- Fixed multiple accessibility bugs improving screen reader compatibility.
- Updated our build tools.
- Various bug fixes.

Updates for version 1.0.7

Date published: 1/24/2019

- Offline use on internal networks is now supported.
- Improved rendering on non-Microsoft Edge browsers.
- Implemented limit for feed retrieval retry attempts to prevent DoS.
- Fixed accessibility bugs, enabling users with visual disabilities to use the web client.
- Improved error messages displayed to the user for feed errors.
- Added Ctrl + Alt + End (Windows) and fn + control + option + delete (Mac) shortcuts to invoke Ctrl + Alt + Del in remote machine.
- Improved telemetry for crash events.
- Improved our build pipeline and build tools.
- Various bug fixes.

Updates for version 1.0.1

Date published: 10/29/2018

- Added an option to **Capture support information** on the About page to diagnose issues.
- InPrivate mode is now supported.
- Improved support for non-English keyboards.
- Fixed an issue where tooltips with non-English characters showed incorrectly.
- Fixed graphics rendering issue which affected Chrome users.
- Updated time zone redirection with full DST support.
- Improved the error message for out-of-memory error.
- Various bug fixes.

Updates for version 1.0.0

Date published: 07/16/2018

- Remote Desktop web client is now generally available.
- Admins can globally turn off telemetry for the web client.
- Various bug fixes.

Updates for version 0.9.0

Date published: 07/05/2018

- New sign in experience within the web client.

- No longer prompted for credentials when launching a desktop or app connection (Single sign on).
- Moved the web client to a new URL: https://server_FQDN/RDWeb/webclient/index.html
- Added time zone redirection.
- Various bug fixes.

Updates for version 0.8.1

Date published: 05/17/2018

- Updates to address CredSSP encryption oracle remediation described in CVE-2018-0886.
- Fixed connection failures for some languages when printing is enabled.
- Improved error message when a gateway is not part of the deployment.
- **Help** and **Feedback** options were added.

Updates for version 0.8.0

Date published: 03/28/2018

- Initial public preview release of the web client.
- Copy/paste text through the clipboard with **CTRL+C** and **CTRL+V**.
- Print to a PDF file.
- Localized in 18 languages.

Remote Desktop client - supported configuration

9/27/2019 • 2 minutes to read • Edit Online

Supported PCs

You can connect to PCs that are running the following Windows operating systems:

- Windows 10 Pro
- Windows 10 Enterprise
- Windows 8 Enterprise
- Windows 8 Professional
- Windows 7 Professional
- Windows 7 Enterprise
- Windows 7 Ultimate
- Windows 7 Ultimate
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Multipoint Server 2011
- Windows Multipoint Server 2012
- Windows Small Business Server 2008
- Windows Small Business Server 2011

The following computers can run the Remote Desktop gateway:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Small Business Server 2011

The following operating systems can serve as RD Web Access or RemoteApp servers:

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Unsupported Windows Versions and Editions

The Remote Desktop client will not connect to these Windows Versions and Editions:

- Windows 7 Starter
- Windows 7 Home
- Windows 8 Home

- Windows 8.1 Home
- Windows 10 Home

If you want to access computers that have one of these Windows versions installed, we recommend you upgrade to a Windows version that supports RDP.

RD Gateway messaging is not supported

Remote Desktop Client does not support RD Gateway messaging. Verify that the Remote Desktop Resource Access Policy (RD RAP) for your RD Gateway server does not specify **Only allow computers with support for RD Gateway Messaging** or you will not be able to connect.

Remote Desktop - Allow access to your PC

1/17/2020 • 3 minutes to read • Edit Online

Applies to: Windows 10, Windows 8.1, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2

You can use Remote Desktop to connect to and control your PC from a remote device by using a Microsoft Remote Desktop client (available for Windows, iOS, macOS and Android). When you allow remote connections to your PC, you can use another device to connect to your PC and have access to all of your apps, files, and network resources as if you were sitting at your desk.

> **NOTE**
> You can use Remote Desktop to connect to Windows 10 Pro and Enterprise, Windows 8.1 and 8 Enterprise and Pro, Windows 7 Professional, Enterprise, and Ultimate, and Windows Server versions newer than Windows Server 2008. You can't connect to computers running a Home edition (like Windows 10 Home).

To connect to a remote PC, that computer must be turned on, it must have a network connection, Remote Desktop must be enabled, you must have network access to the remote computer (this could be through the Internet), and you must have permission to connect. For permission to connect, you must be on the list of users. Before you start a connection, it's a good idea to look up the name of the computer you're connecting to and to make sure Remote Desktop connections are allowed through its firewall.

How to enable Remote Desktop

The simplest way to allow access to your PC from a remote device is using the Remote Desktop options under Settings. Since this functionality was added in the Windows 10 Fall Creators update (1709), a separate downloadable app is also available that provides similar functionality for earlier versions of Windows. You can also use the legacy way of enabling Remote Desktop, however this method provides less functionality and validation.

Windows 10 Fall Creator Update (1709) or later

You can configure your PC for remote access with a few easy steps.

1. On the device you want to connect to, select **Start** and then click the **Settings** icon on the left.
2. Select the **System** group followed by the **Remote Desktop** item.
3. Use the slider to enable Remote Desktop.
4. It is also recommended to keep the PC awake and discoverable to facilitate connections. Click **Show settings** to enable.
5. As needed, add users who can connect remotely by clicking **Select users that can remotely access this PC**.
   a. Members of the Administrators group automatically have access.
6. Make note of the name of this PC under **How to connect to this PC**. You'll need this to configure the clients.

Windows 7 and early version of Windows 10

To configure your PC for remote access, download and run the Microsoft Remote Desktop Assistant. This assistant updates your system settings to enable remote access, ensures your computer is awake for connections, and checks that your firewall allows Remote Desktop connections.

All versions of Windows (Legacy method)

To enable Remote Desktop using the legacy system properties, follow the instructions to Connect to another

computer using Remote Desktop Connection.

Should I enable Remote Desktop?

If you only want to access your PC when you are physically using it, you don't need to enable Remote Desktop. Enabling Remote Desktop opens a port on your PC that is visible to your local network. You should only enable Remote Desktop in trusted networks, such as your home. You also don't want to enable Remote Desktop on any PC where access is tightly controlled.

Be aware that when you enable access to Remote Desktop, you are granting anyone in the Administrators group, as well as any additional users you select, the ability to remotely access their accounts on the computer.

You should ensure that every account that has access to your PC is configured with a strong password.

Why allow connections only with Network Level Authentication?

If you want to restrict who can access your PC, choose to allow access only with Network Level Authentication (NLA). When you enable this option, users have to authenticate themselves to the network before they can connect to your PC. Allowing connections only from computers running Remote Desktop with NLA is a more secure authentication method that can help protect your computer from malicious users and software. To learn more about NLA and Remote Desktop, check out Configure NLA for RDS Connections.

If you're remotely connecting to a PC on your home network from outside of that network, don't select this option.

Remote Desktop - Allow access to your PC from outside your PC's network

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows 10, Windows Server 2016

When you connect to your PC by using a Remote Desktop client, you're creating a peer-to-peer connection. This means you need direct access to the PC (sometimes called "the host"). If you need to connect to your PC from outside of the network your PC is running on, you need to enable that access. You have a couple of options: use port forwarding or set up a VPN.

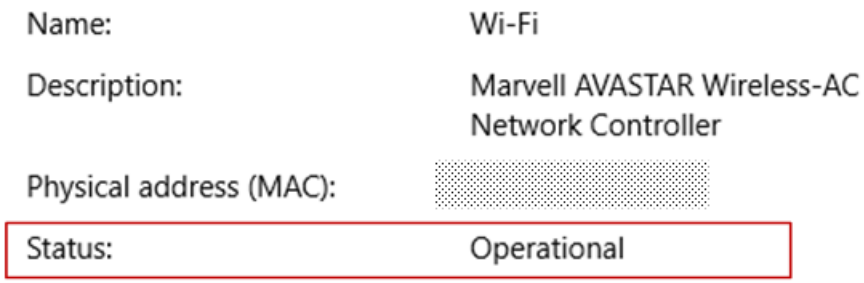
Enable port forwarding on your router

Port forwarding simply maps the port on your router's IP address (your public IP) to the port and IP address of the PC you want to access.

Specific steps for enabling port forwarding depend on the router you're using, so you'll need to search online for your router's instructions. For a general discussion of the steps, check out wikiHow to Set Up Port Forwarding on a Router.

Before you map the port you'll need the following:

- PC internal IP address: Look in **Settings > Network & Internet > Status > View your network properties**. Find the network configuration with an "Operational" status and then get the **IPv4 address**.



- Your public IP address (the router's IP). There are many ways to find this - you can search (in Bing or Google) for "my IP" or view the Wi-Fi network properties (for Windows 10).
- Port number being mapped. In most cases this is 3389 - that's the default port used by Remote Desktop connections.
- Admin access to your router.

> **WARNING**
> You're opening your PC up to the internet - make sure you have a strong password set for your PC.

After you map the port, you'll be able to connect to your host PC from outside the local network by connecting to the public IP address of your router (the second bullet above).

The router's IP address can change - your internet service provider (ISP) can assign you a new IP at any time. To avoid running into this issue, consider using Dynamic DNS - this lets you connect to the PC using an easy to

remember domain name, instead of the IP address. Your router automatically updates the DDNS service with your new IP address, should it change.

With most routers you can define which source IP or source network can use port mapping. So, if you know you're only going to connect from work, you can add the IP address for your work network - that lets you avoid opening the port to the entire public internet. If the host you're using to connect uses dynamic IP address, set the source restriction to allow access from the whole range of that particular ISP.

You might also consider setting up a static IP address on your PC so the internal IP address doesn't change. If you do that, then the router's port forwarding will always point to the correct IP address.

Use a VPN

If you connect to your local area network by using a virtual private network (VPN), you don't have to open your PC to the public internet. Instead, when you connect to the VPN, your RD client acts like it's part of the same network and be able to access your PC. There are a number of VPN services available - you can find and use whichever works best for you.

Change the listening port for Remote Desktop on your computer

9/27/2019 • 2 minutes to read • Edit Online

> Applies to: Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2008 R2

When you connect to a computer (either a Windows client or Windows Server) through the Remote Desktop client, the Remote Desktop feature on your computer "hears" the connection request through a defined listening port (3389 by default). You can change that listening port on Windows computers by modifying the registry.

1. Start the registry editor. (Type regedit in the Search box.)
2. Navigate to the following registry subkey: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber
3. Click **Edit > Modify**, and then click **Decimal**.
4. Type the new port number, and then click **OK**.
5. Close the registry editor, and restart your computer.

The next time you connect to this computer by using the Remote Desktop connection, you must type the new port. If you're using a firewall, make sure to configure your firewall to permit connections to the new port number.

Compare the client apps

9/27/2019 • 2 minutes to read • Edit Online

> Applies to: Windows 10, Windows 8.1, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2

We're often asked how the different Remote Desktop client apps compare to each other. Do they all do the same thing? Here are the answers to those questions.

Redirection support

The following tables compare support for device and other redirections on the Remote Desktop Connection app, Universal app, Android app, iOS app, macOS app and web client. These tables cover the redirections that you can access once in a remote session.

If you remote into your personal desktop, there are additional redirections that you can configure in the **Additional Settings** for the session. If your remote desktop or apps are managed by your organization, your admin can enable or disable redirections through Group Policy settings.

Input redirection

REDIRECTION	REMOTE DESKTOP CONNECTION	UNIVERSAL	ANDROID	IOS	MACOS	WEB CLIENT
Keyboard	X	X	X	X	X	X
Mouse	X	X	X	X*	X	X
Touch	X	X	X	X		X (Edge and IE not supported)
Other	Pen					

*View the list of supported input devices for the Remote Desktop iOS Beta client.

Port redirection

REDIRECTION	REMOTE DESKTOP CONNECTION	UNIVERSAL	ANDROID	IOS	MACOS	WEB CLIENT
Serial port	X					
USB	X					

When you enable USB port redirection, any USB devices attached to the USB port are automatically recognized in the remote session.

Other redirection (devices, etc)

REDIRECTION	REMOTE DESKTOP CONNECTION	UNIVERSAL	ANDROID	IOS	MACOS	WEB CLIENT
Cameras	X					
Clipboard	X	text, image	text	text, image	X	text
Local drive/storage	X		X		x	
Location	X					
Microphones	X	X			X	
Printers	X				X (CUPS only)	PDF print
Scanners	X					
Smart Cards	X				X (Windows authentication not supported)	
Speakers	X	X	X	X	X	X (except IE)

*For printer redirection - the macOS app supports the Publisher Imagesetter printer driver by default. They do not support redirecting native printer drivers.

Supported Remote desktop RDP file settings

9/27/2019 • 9 minutes to read • Edit Online

The following table includes list of supported RDP file settings that you can use with the Windows and HTML clients. An “x” in the platform column indicates that the setting is supported. However, this list is not a complete list of supported settings for the Windows and HTML5 clients. We'll continue to update this table to include more supported RDP settings for the Windows and HTML5 clients as well as the macOS, iOS, and Android clients.

Please refer to this documentation detailing how to use PowerShell to customize RDP properties for a host pool.

RDP SETTING	DESCRIPTION	VALUES	DEFAULT VALUE	WINDOWS VIRTUAL DESKTOP	WINDOWS	HTML5
alternate full address:s:value	Specifies an alternate name or IP address of the remote computer.	Any valid name or IP address of the remote computer, such as "10.10.15.15"		x	x	x
alternate shell:s:value	Determines whether a program starts automatically when you connect with RDP. To specify an alternate shell, enter a valid path to an executable file for the value, such as "C:\ProgramFiles\Office\word.exe". This setting also determines which path or alias of the Remote Application to be started at connection time if RemoteApplicationMode is enabled.	"C:\ProgramFiles\Office\word.exe"		x	x	x

RDP SETTING	DESCRIPTION	VALUES	DEFAULT VALUE	WINDOWS VIRTUAL DESKTOP	WINDOWS	HTML5
audiocapturemode:i:value	Indicates whether audio input/output redirection is enabled.	- 0: Disable audio capture from the local device - 1: Enable audio capture from the local device and redirection to an audio application in the remote session	0	x	x	
audiomode:i:value	Determines whether the local or remote machine plays audio.	- 0: Play sounds on local computer (Play on this computer) - 1: Play sounds on remote computer (Play on remote computer) - 2: Do not play sounds (Do not play)	0	x	x	x

RDP SETTING	DESCRIPTION	VALUES	DEFAULT VALUE	WINDOWS VIRTUAL DESKTOP	WINDOWS	HTML5
authentication level:i:value	Defines the server authentication level settings.	- 0: If server authentication fails, connect to the computer without warning (Connect and don't warn me) - 1: If server authentication fails, don't establish a connection (Don't connect) - 2: If server authentication fails, show a warning and allow me to connect or refuse the connection (Warn me) - 3: No authentication requirement specified.	3	x	x	
autoreconnection enabled:i:value	Determines whether the client computer will automatically try to reconnect to the remote computer if the connection is dropped, such as when there's a network connectivity interruption.	- 0: Client computer does not automatically try to reconnect - 1: Client computer automatically tries to reconnect	1	x	x	x
bandwidthautodetect:i:value	Determines whether automatic network type detection is enabled	- 0: Disable automatic network type detection - 1: Enable automatic network type detection	1	x	x	x

RDP SETTING	DESCRIPTION	VALUES	DEFAULT VALUE	WINDOWS VIRTUAL DESKTOP	WINDOWS	HTML5
camerastoredirect:s:value	Configures which cameras to redirect. This setting uses a semicolon-delimited list of KSCATEGORY_VIDEO_CAMERA interfaces of cameras enabled for redirection.	- * : Redirect all cameras - One can exclude a specific camera by prepending the symbolic link string with "-", such as camerastoredirect:s:\?\usb#vid_0bda&pid_58b0&mi		x	x	
compression:i:value	Determines whether bulk compression is enabled when it is transmitted by RDP to the local computer.	- 0: Disable RDP bulk compression - 1: Enable RDP bulk compression	1	x	x	x
desktop size id:i:value	Specifies dimensions of the remote session desktop from a set of pre-defined options. This setting is overridden if either desktopheight or desktopwidth are specified.	-0: 640×480 - 1: 800×600 - 2: 1024×768 - 3: 1280×1024 - 4: 1600×1200	0	x	x	x

RDP SETTING	DESCRIPTION	VALUES	DEFAULT VALUE	WINDOWS VIRTUAL DESKTOP	WINDOWS	HTML5
desktopheight :i:value	Determines the resolution height (in pixels) on the remote computer when you connect by using Remote Desktop Connection. This setting corresponds to the selection in the Display configuration slider on the Display tab under Options in RDC.	Numerical value between 200 and 2048	The default value is set to the resolution on the local computer	x	x	x
desktopwidth:i :value	Determines the resolution width (in pixels) on the remote computer when you connect by using Remote Desktop Connection. This setting corresponds to the selection in the Display configuration slider on the Display tab under Options in RDC.	Numerical value between 200 and 4096	The default value is set to the resolution on the local computer	x	x	x

RDP SETTING	DESCRIPTION	VALUES	DEFAULT VALUE	WINDOWS VIRTUAL DESKTOP	WINDOWS	HTML5
disableconnectionsharing:i:value	Determines whether the remote desktop client reconnects to any existing open connections or initiate a new connection when a RemoteApp or desktop is launched	- 0: Reconnect to any existing session - 1: Initiate new connection	0	x	x	x
domain:s:value	Specifies the name of the domain in which the user account that will be used to log on to the remote computer is located.	A valid domain name, such as "CONTOSO"	No Default Value	x	x	x
drivestoredirect:s:value	Determines which local disk drives on the client computer will be redirected and available in the remote session.	- No value specified: don't redirect any drives - * : Redirect all disk drives, including drives that are connected later - DynamicDrives: redirect any drives that are connected later - The drive and labels for one or more drives, such as "drivestoredirect:s:C:;E:;": redirect the specified drive(s)	No value specified: don't redirect any drives	x	x	

RDP SETTING	DESCRIPTION	VALUES	DEFAULT VALUE	WINDOWS VIRTUAL DESKTOP	WINDOWS	HTML5
enablecredsspsupport:i:value	Determines whether RDP will use the Credential Security Support Provider (CredSSP) for authentication if it is available.	- 0: RDP will not use CredSSP, even if the operating system supports CredSSP - 1: RDP will use CredSSP if the operating system support CredSSP	1	x	x	
encode redirected video capture:i:value	Enables or disables encoding of redirected video.	- 0: Disable encoding of redirected video - 1: Enable encoding of redirected video	1	x	x	x
full address:s:value	This setting specifies the name or IP address of the remote computer that you want to connect to	A valid computer name, IPv4 address, or IPv6 address.		x	x	x
gatewaycredentialssource:i:value	Specifies or retrieves the RD Gateway authentication method.	- 0: Ask for password (NTLM) - 1: Use smart card - 4: Allow user to select later	0	x	x	x
gatewayhostname:s:value	Specifies the RD Gateway host name.	Valid gateway server address.		x	x	x
gatewayprofileusagemethod:i:value	Specifies whether to use default RD Gateway settings	- 0: Use the default profile mode, as specified by the administrator - 1: Use explicit settings, as specified by the user	0	x	x	x

RDP SETTING	DESCRIPTION	VALUES	DEFAULT VALUE	WINDOWS VIRTUAL DESKTOP	WINDOWS	HTML5
gatewayusagemethod:i:value	Specifies when to use the RD Gateway server	- 0: Don't use an RD Gateway server - 1: Always use an RD Gateway server - 2: Use an RD Gateway server if a direct connection cannot be made to the RD Session Host - 3: Use the default RD Gateway server settings - 4: Don't use an RD Gateway, bypass server for local addresses Setting this property value to 0 or 4 are is effectively equivalent, but setting this property to 4 enables the option to bypass local addresses.		x	x	x
networkautodetect:i:value	Determines whether or not to use automatic network bandwidth detection. Requires the option bandwidthautodetect to be set and correlates with connection type 7.	- 0: Don't use automatic network bandwidth detection - 1: Use automatic network bandwidth detection	1	x		x

RDP SETTING	DESCRIPTION	VALUES	DEFAULT VALUE	WINDOWS VIRTUAL DESKTOP	WINDOWS	HTML5
promptcredentialonce:i:value	Determines whether a user's credentials are saved and used for both the RD Gateway and the remote computer.	- 0: Remote session will not use the same credentials - 1: Remote session will use the same credentials	1	x	x	
redirectclipboard:i:value	Determines whether clipboard redirection is enabled.	- 0: Clipboard on local computer isn't available in remote session - 1: Clipboard on local computer is available in remote session	1	x	x	x
redirected video capture encoding quality:i:value	Controls the quality of encoded video.	- 0: High compression video. Quality may suffer when there is a lot of motion - 1: Medium compression - 2: Low compression video with high picture quality	0	x	x	x
redirectprinters:i:value	Determines whether printers configured on the client computer will be redirected and available in the remote session when you connect to a remote computer by using Remote Desktop Connection.	- 0: The printers on the local computer are not available in the remote session - 1: The printers on the local computer are available in the remote session	1	x	x	x

RDP SETTING	DESCRIPTION	VALUES	DEFAULT VALUE	WINDOWS VIRTUAL DESKTOP	WINDOWS	HTML5
redirectsmartcards:i:value	Determines whether smart card devices on the client computer will be redirected and available in the remote session when you connect to a remote computer.	- 0: The smart card device on the local computer is not available in the remote session - 1: The smart card device on the local computer is available in the remote session	1	x	x	
remoteapplicationcmdline:s:value	Optional command-line parameters for the RemoteApp.		x	x	x	
remoteapplicationexpandcmdline:i:value	Determines whether environment variables contained in the RemoteApp command line parameter should be expanded locally or remotely.	- 0: Environment variables should be expanded to the values of the local computer - 1: Environment variables should be expanded on the remote computer to the values of the remote computer		x	x	x

RDP SETTING	DESCRIPTION	VALUES	DEFAULT VALUE	WINDOWS VIRTUAL DESKTOP	WINDOWS	HTML5
remoteapplicationexpandworkingdir	Determines whether environment variables contained in the RemoteApp working directory parameter should be expanded locally or remotely.	- 0: Environment variables should be expanded to the values of the local computer - 1: Environment variables should be expanded on the remote computer to the values of the remote computer. The RemoteApp working directory is specified through the shell working directory parameter.		x	x	x
remoteapplicationfile:s:value	Specifies a file to be opened on the remote computer by the RemoteApp. For local files to be opened, you must also enable drive redirection for the source drive.		x	x	x	
remoteapplicationicon:s:value	Specifies the icon file to be displayed in the client UI while launching a RemoteApp. If no file name is specified, the client will use the standard Remote Desktop icon. Only ".ico" files are supported.		x	x	x	

RDP SETTING	DESCRIPTION	VALUES	DEFAULT VALUE	WINDOWS VIRTUAL DESKTOP	WINDOWS	HTML5
remoteapplicationmode:i:value	Determines whether a RemoteApp connection is launched as a RemoteApp session.	- 0: Don't launch a RemoteApp session - 1: Launch a RemoteApp session	1	x	x	x
remoteapplicationname:s:value	Specifies the name of the RemoteApp in the client interface while starting the RemoteApp.	For example, "Excel 2016."	x	x	x	
remoteapplicationprogram:s:value	Specifies the alias or executable name of the RemoteApp.	For example, "EXCEL."	x	x	x	
screen mode id:i:value	Determines whether the remote session window appears full screen when you connect to the remote computer by using Remote Desktop Connection.	- 1: The remote session will appear in a window - 2: The remote session will appear full screen	2	x	x	x
smart sizing:i:value	Determines whether or not the client computer can scale the content on the remote computer to fit the window size of the client computer.	- 0: The client window display won't scale when resized - 1: The client window display will scale when resized	0	x	x	

RDP SETTING	DESCRIPTION	VALUES	DEFAULT VALUE	WINDOWS VIRTUAL DESKTOP	WINDOWS	HTML5
use multimon:i:value	Configures multiple monitor support when you connect to the remote computer by using Remote Desktop Connection.	- 0: Don't enable multiple monitor support - 1: Enable multiple monitor support	0	x	x	
username:s:value	Specifies the name of the user account that will be used to log on to the remote computer.	Any valid username.		x	x	x
videoplaybackmode:i:value	Determines if Remote Desktop Connection will use RDP-efficient multimedia streaming for video playback.	- 0: Don't use RDP efficient multimedia streaming for video playback - 1: Use RDP-efficient multimedia streaming for video playback when possible	1	x	x	
workspaceid:s:value	Defines the RemoteApp and Desktop ID associated with the RDP file that contains this setting.	A valid RemoteApp and Desktop Connection ID	x	x		

Remote Desktop client Universal Resource Identifier (URI) scheme support

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows Server, version 1803, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2

Enabling a Uniform Resource Identifier (URI) scheme gives IT professionals and developers a way to integrate features of the Remote Desktop clients across platforms and enriches the user experience by allowing:

- Third-party applications to launch Microsoft Remote Desktop and start remote sessions with predefined settings (provided as part of the URI string).
- End users to start remote connections using pre-configured URLs.

> **NOTE**
> Using a URI to connect to the RD client is NOT supported for Windows operating systems - use the URI with MacOS, iOS, and Android devices.

Microsoft Remote Desktop uses the URI scheme rdp://query_string to store pre-configured attribute settings that are used when launching the client. The query strings represent a single or set of RDP attributes provided in the URL.

The RDP attributes are separated by the ampersand symbol (&). For example, when connecting to a PC, the string is:

```
rdp://full%20address=s:mypc:3389&audiomode=i:2&disable%20themes=i:1
```

This table gives a complete list of supported attributes that may be used with the iOS, Mac, and Android Remote Desktop clients. (An "x" in the platform column indicates the attribute is supported. The values denoted by chevrons (<>) represent the values that are supported by the Remote Desktop clients.)

RDP ATTRIBUTE	ANDROID	MAC	IOS
allow desktop composition=i:<0 or 1>	x	x	x
allow font smoothing=i:<0 or 1>	x	x	x
alternate shell=s:<string>	x	x	x
audiomode=i:<0, 1, or 2>	x	x	x
authentication level=i:<0 or 1>	x	x	x

RDP ATTRIBUTE	ANDROID	MAC	IOS
connect to console=i:<0 or 1>	x	x	x
disable cursor settings=i:<0 or 1>	x	x	x
disable full window drag=i:<0 or 1>	x	x	x
disable menu anims=i:<0 or 1>	x	x	x
disable themes=i:<0 or 1>	x	x	x
disable wallpaper=i:<0 or 1>	x	x	x
drivestoredirect=s:* (this is the only supported value)	x	x	
desktopheight=i:<value in pixels>		x	
desktopwidth=i:<value in pixels>		x	
domain=s:<string>	x	x	x
full address=s:<string>	x	x	x
gatewayhostname=s:<string>	x	x	x
gatewayusagemethod=i:<1 or 2>	x	x	x
prompt for credentials on client=i:<0 or 1>		x	
loadbalanceinfo=s:<string>	x	x	x
redirectprinters=i:<0 or 1>		x	
remoteapplicationcmdline=s:<string>	x	x	x
remoteapplicationmode=i:<0 or 1>	x	x	x
remoteapplicationprogram=s:<string>	x	x	x
shell working directory=s:<string>	x	x	x

RDP ATTRIBUTE	ANDROID	MAC	IOS
Use redirection server name=i:<0 or 1>	x	x	x
username=s:<string>	x	x	x
screen mode id=i:<1 or 2>		x	
session bpp=i:<8, 15, 16, 24, or 32>		x	
use multimon=i:<0 or 1>		x	

Frequently asked questions about the Remote Desktop clients

1/14/2020 • 12 minutes to read • Edit Online

Applies to: Windows 10, Windows 8.1, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2

Now that you've set up the Remote Desktop client on your device (Android, Mac, iOS, or Windows), you may have questions. Here are answers to the most commonly asked questions about the Remote Desktop clients.

- Setting up
- Connections, gateway, and networks
- Web client
- Monitors, audio, and mouse
- Mac hardware
- Specific error messages

The majority of these questions apply to all of the clients, but there are a few client specific items.

If you have additional questions that you'd like us to answer, leave them as feedback on this article.

Setting up

Which PCs can I connect to?

Check out the supported configuration article for information about what PCs you can connect to.

How do I set up a PC for Remote Desktop?

I have my device set up, but I don't think the PC's ready. Help?

First, have you seen the Remote Desktop Setup Wizard? It walks you through getting your PC ready for remote access. Download and run that tool on your PC to get everything set.

Otherwise, if you prefer to do things manually, read on.

For Windows 10, do the following:

1. On the device you want to connect to, open **Settings**.
2. Select **System** and then **Remote Desktop**.
3. Use the slider to enable Remote Desktop.
4. In general, it's best to keep the PC awake and discoverable to facilitate connections. Click **Show settings** to go to the power settings for your PC, where you can change this setting.

   > **NOTE**
   > You can't connect to a PC that's asleep or hibernating, so make sure the settings for sleep and hibernation on the remote PC are set to **Never**. (Hibernation isn't available on all PCs.)

Make note of the name of this PC under **How to connect to this PC**. You'll need this to configure the clients.

You can grant permission for specific users to access this PC - to do that, click **Select users that can remotely**

access this PC. Members of the Administrators group automatically have access.

For Windows 8.1, follow the instructions to allow remote connections in Connect to another desktop using Remote Desktop Connections.

Connection, gateway, and networks

Why can't I connect using Remote Desktop?

Here are some possible solutions to common problems you might encounter when trying to connect to a remote PC. If these solutions don't work, you can find more help on the Microsoft Community website.

- **The remote PC can't be found.** Make sure you have the right PC name, and then check to see if you entered that name correctly. If you still can't connect, try using the IP address of the remote PC instead of the PC name.
- **There's a problem with the network.** Make sure you have internet connection.
- **The Remote Desktop port might be blocked by a firewall.** If you're using Windows Firewall, follow these steps:

  1. Open Windows Firewall.
  2. Click **Allow an app or feature through Windows Firewall**.
  3. Click **Change settings**. You might be asked for an admin password or to confirm your choice.
  4. Under **Allowed apps and features**, select **Remote Desktop**, and then tap or click **OK**.

     If you're using a different firewall, make sure the port for Remote Desktop (usually 3389) is open.

- **Remote connections might not be set up on the remote PC.** To fix this, scroll back up to How do I set up a PC for Remote Desktop? question in this topic.
- **The remote PC might only allow PCs to connect that have Network Level Authentication set up.**
- **The remote PC might be turned off.** You can't connect to a PC that's turned off, asleep, or hibernating, so make sure the settings for sleep and hibernation on the remote PC are set to **Never** (hibernation isn't available on all PCs.).

Why can't I find or connect to my PC?

Check the following:

- Is the PC on and awake?
- Did you enter the right name or IP address?

  > **IMPORTANT**
  > Using the PC name requires your network to resolve the name correctly through DNS. In many home networks, you have to use the IP address instead of the host name to connect.

- Is the PC on a different network? Did you configure the PC to let outside connections through? Check out Allow access to your PC from outside your network for help.
- Are you connecting to a supported Windows version?

> **NOTE**
> Windows XP Home, Windows Media Center Edition, Windows Vista Home and Windows 7 Home or Starter are not supported without 3rd party software.

Why can't I sign in to a remote PC?

If you can see the sign-in screen of the remote PC but you can't sign in, you might not have been added to the Remote Desktop Users Group or to any group with administrator rights on the remote PC. Ask your system admin to do this for you.

Which connection methods are supported for company networks?

If you want to access your office desktop from outside your company network, your company must provide you with a means of remote access. The RD Client currently supports the following:

- Terminal Server Gateway or Remote Desktop Gateway
- Remote Desktop Web Access
- VPN (through iOS built-in VPN options)

VPN doesn't work

VPN issues can have several causes. The first step is to verify that the VPN works on the same network as your PC or Mac computer. If you can't test with a PC or Mac, you can try to access a company intranet web page with your device's browser.

Other things to check:

- **The 3G network blocks or corrupts VPN.** There are several 3G providers in the world who seem to block or corrupt 3G traffic. Verify VPN connectivity works correctly for over a minute.
- **L2TP or PPTP VPNs.** If you are using L2TP or PPTP in your VPN, please set Send All Traffic to ON in the VPN configuration.
- **VPN is misconfigured.** A misconfigured VPN server can be the reason why the VPN connections never worked or stopped working after some time. Ensure testing with the iOS device's web browser or a PC or Mac on the same network if this happens.

How can I test if VPN is working properly?

Verify that VPN is enabled on your device. You can test your VPN connection by going to a webpage on your internal network or using a web service which is only available via the VPN.

How do I configure L2TP or PPTP VPN connections?

If you are using L2TP or PPTP in your VPN, make sure to set **Send all traffic** to **ON** in the VPN configuration.

Web client

Which browsers can I use?

The web client supports Microsoft Edge, Internet Explorer 11, Mozilla Firefox (v55.0 and later), Safari, and Google Chrome.

What PCs can I use to access the web client?

The web client supports Windows, macOS, Linux, and ChromeOS. Mobile devices are not supported at this time.

Can I use the web client in a Remote Desktop deployment without a gateway?

No. The client requires a Remote Desktop Gateway to connect. Don't know what that means? Ask your admin about it.

Does the Remote Desktop web client replace the Remote Desktop Web Access page?

No. The Remote Desktop web client is hosted at a different URL than the Remote Desktop Web Access page. You can use either the web client or the Web Access page to view the remote resources in a browser.

Can I embed the web client in another web page?

This feature is not supported at the moment.

Monitors, audio, and mouse

How do I use all of my monitors?

To use two or more screens, do the following:

1. Right-click the remote desktop that you want to enable multiple screens for, and then click **Edit**.
2. Enable **Use all monitors** and **Full screen**.

Is bi-directional sound supported?

Bi-directional sound can be configured in the Windows client on a per-connection basis. The relevant settings can be accessed in the **Remote audio** section of the **Local Resources** options tab.

What can I do if the sound won't play?

Sign out of the session (don't just disconnect, sign all the way out), and then sign in again.

Mac client - hardware questions

Is retina resolution supported?

Yes, the remote desktop client supports retina resolution.

How do I enable secondary right-click?

In order to make use of the right-click inside an open session you have three options:

- Standard PC two button USB mouse
- Apple Magic Mouse: To enable right-click, click **System Preferences** in the dock, click **Mouse**, and then enable **Secondary click**.
- Apple Magic Trackpad or MacBook Trackpad: To enable right-click, click **System Preferences** in the dock, click **Mouse**, and then enable **Secondary click**.

Is AirPrint supported?

No, the Remote Desktop client doesn't support AirPrint. (This is true for both Mac and iOS clients.)

Why do incorrect characters appear in the session?

If you are using an international keyboard, you might see an issue where the characters that appear in the session do match the characters you typed on the Mac keyboard.

This can occur in the following scenarios:

- You are using a keyboard that the remote session does not recognize. When Remote Desktop doesn't recognize the keyboard, it defaults to the language last used with the remote PC.
- You are connecting to a previously disconnected session on a remote PC and that remote PC uses a different keyboard language than the language you are currently trying to use.

You can fix this issue by manually setting the keyboard language for the remote session. See the steps in the next section.

How do language settings affect keyboards in a remote session?

There are many types of Mac keyboard layouts. Some of these are Mac specific layouts or custom layouts for which an exact match may not be available on the version of Windows you are remoting into. The remote session

maps your keyboard to the best matching keyboard language available on the remote PC.

If your Mac keyboard layout is set to the PC version of the language keyboard (for example, French – PC) all your keys should be mapped correctly and your keyboard should just work.

If your Mac keyboard layout is set to the Mac version of a keyboard (for example, French) the remote session will map you to the PC version of the French language. Some of the Mac keyboard shortcuts you are used to using on OSX will not work in the remote Windows session.

If your keyboard layout is set to a variation of a language (for example, Canadian-French) and if the remote session cannot map you to that exact variation, the remote session will map you to the closest language (for example, French). Some of the Mac keyboard shortcuts you are used to using on OSX will not work in the remote Windows session.

If your keyboard layout is set to a layout the remote session cannot match at all, your remote session will default to give you the language you last used with that PC. In this case, or in cases where you need to change the language of your remote session to match your Mac keyboard, you can manually set the keyboard language in the remote session to the language that is the closest match to the one you wish to use as follows.

Use the following instructions to change the keyboard layout inside the remote desktop session:

On Windows 10 or Windows 8:

1. From inside the remote session, open Region and Language. Click **Start > Settings > Time and Language**. Open **Region and Language**.
2. Add the language you want to use. Then close the Region and Language window.
3. Now, in the remote session, you'll see the ability to switch between languages. (In the right side of the remote session, near the clock.) Click the language you want to switch to (such as **Eng**).

You might need to close and restart the application you are currently using for the keyboard changes to take effect.

Specific errors

Why do I get an "Insufficient privileges" error?

You are not allowed to access the session you want to connect to. The most likely cause is that you are trying to connect to an admin session. Only administrators are allowed to connect to the console. Verify that the console switch is off in the advanced settings of the remote desktop. If this is not the source of the problem, please contact your system administrator for further assistance.

Why does the client say that there is no CAL?

When a remote desktop client connects to a Remote Desktop server, the server issues a Remote Desktop Services Client Access License (RDS CAL) stored by the client. Whenever the client connects again it will use its RDS CAL and the server will not issue another license. The server will issue another license if the RDS CAL on the device is missing or corrupt. When the maximum number of licensed devices is reached the server will not issue new RDS CALs. Contact your network administrator for assistance.

Why did I get an "Access Denied" error?

The "Access Denied" error is a generated by the Remote Desktop Gateway and the result of incorrect credentials during the connection attempt. Verify your username and password. If the connection worked before and the error occurred recently, you possibly changed your Windows user account password and haven't updated it yet in the remote desktop settings.

What does "RPC Error 23014" or "Error 0x59e6" mean?

In case of an **RPC error 23014** or **Error 0x59E6 try again after waiting a few minutes**, the RD Gateway server has reached the maximum number of active connections. Depending on the Windows version running on

the RD Gateway the maximum number of connections differs: The Windows Server 2008 R2 Standard implementation limits the number of connections to 250. The Windows Server 2008 R2 Foundation implementation limits the number of connections to 50. All other Windows implementations allow an unlimited number of connections.

What does the "Failed to parse NTLM challenge" error mean?

This error is caused by a misconfiguration on the remote PC. Make sure the RDP security level setting on the remote PC is set to "Client Compatible." (Talk to your system admin if you need help doing this.)

What does "TS_RAP You are not allowed to connect to the given host" mean?

This error happens when a Resource Authorization Policy on the gateway server stops your user name from connecting to the remote PC. This can happen in the following instances:

- The remote PC name is the same as the name of the gateway. Then, when you try to connect to the remote PC, the connection goes to the gateway instead, which you probably don't have permission to access. If you need to connect to the gateway, do not use the external gateway name as PC name. Instead use "localhost" or the IP address (127.0.0.1), or the internal server name.
- Your user account isn't a member of the user group for remote access.

Privacy settings for managed apps and desktops

9/27/2019 • 2 minutes to read • Edit Online

Applies to: Windows 10, Windows 7, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019

When accessing managed resources (apps or desktops) provided by your IT administrator, the privacy settings for the remote system have been preconfigured by your IT administrator. These settings may be different than the privacy settings on your local system. If you have questions, contact your IT administrator.

> **NOTE**
> Using managed resources in regions other than the United States may result in data transfer to the United States.

These are some of the Windows 10 privacy settings you can configure in your managed desktop:

- Speech recognition
- Find my device
- Inking & typing
- Advertising ID
- Location
- Diagnostic data
- Tailored experiences

You can always review the information collected and sent to Microsoft by accessing your Privacy Dashboard.

Learn more about privacy settings

If your IT administrator has provided you with a managed desktop, you can follow the instructions in the next section to learn more about these settings and change any settings not locked by your IT Administrator.

How to change privacy settings in Windows 10 remote desktops

To change privacy settings in a Windows 10 remote desktop:

1. From the remote desktop, select the Windows button on the taskbar or press the Windows key on your keyboard to open the Start menu.
2. Select the gear icon to open Settings.
3. Search for the names of the configurable privacy settings listed earlier in this topic to learn more about it.

> **NOTE**
> If your IT Administrator has configured the managed desktop to not retain user configuration settings between connections, any changes you make to these settings won't be saved.

General Remote Desktop connection troubleshooting

1/18/2020 • 8 minutes to read • Edit Online

Use these steps when a Remote Desktop client can't connect to a remote desktop but doesn't provide messages or other symptoms that would help identify the cause.

Check the status of the RDP protocol

Check the status of the RDP protocol on a local computer

To check and change the status of the RDP protocol on a local computer, see How to enable Remote Desktop.

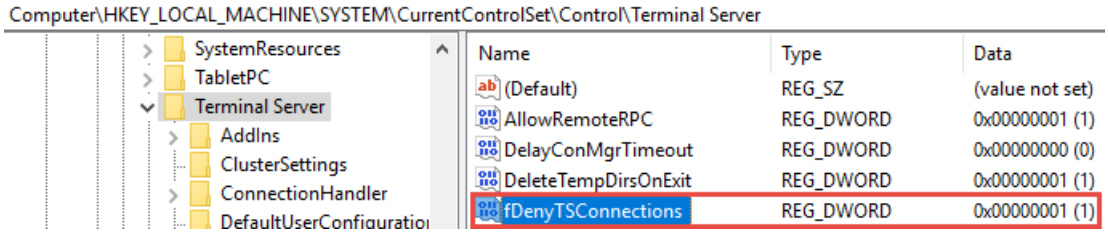
> **NOTE**
> If the remote desktop options are not available, see Check whether a Group Policy Object is blocking RDP.

Check the status of the RDP protocol on a remote computer

> **IMPORTANT**
> Follow this section's instructions carefully. Serious problems can occur if the registry is modified incorrectly. Before you starty modifying the registry, back up the registry so you can restore it in case something goes wrong.

To check and change the status of the RDP protocol on a remote computer, use a network registry connection:

1. First, go to the **Start** menu, then select **Run**. In the text box that appears, enter **regedt32**.
2. In the Registry Editor, select **File**, then select **Connect Network Registry**.
3. In the **Select Computer** dialog box, enter the name of the remote computer, select **Check Names**, and then select **OK**.
4. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server**.



   - If the value of the **fDenyTSConnections** key is **0**, then RDP is enabled.
   - If the value of the **fDenyTSConnections** key is **1**, then RDP is disabled.
5. To enable RDP, change the value of **fDenyTSConnections** from **1** to **0**.

Check whether a Group Policy Object (GPO) is blocking RDP on a local computer

If you can't turn on RDP in the user interface or the value of **fDenyTSConnections** reverts to **1** after you've changed it, a GPO may be overriding the computer-level settings.

To check the group policy configuration on a local computer, open a Command Prompt window as an administrator, and enter the following command:

```
gpresult /H c:\gpresult.html
```

After this command finishes, open gpresult.html. In **Computer Configuration\Administrative**

Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections, find the **Allow users to connect remotely by using Remote Desktop Services** policy.

- If the setting for this policy is **Enabled**, Group Policy is not blocking RDP connections.
- If the setting for this policy is **Disabled**, check **Winning GPO**. This is the GPO that is blocking RDP connections.

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Connections

Policy	Setting	Winning GPO
Allow users to connect remotely by using Remote Desktop Services	Disabled	Block RDP

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Connections

Policy	Setting	Winning GPO
Allow users to connect remotely by using Remote Desktop Services	Disabled	Local Group Policy

Check whether a GPO is blocking RDP on a remote computer

To check the Group Policy configuration on a remote computer, the command is almost the same as for a local computer:

```
gpresult /S <computer name> /H c:\gpresult-<computer name>.html
```

The file that this command produces (**gpresult-<computer name>.html**) uses the same information format as the local computer version (**gpresult.html**) uses.

Modifying a blocking GPO

You can modify these settings in the Group Policy Object Editor (GPE) and Group Policy Management Console (GPM). For more information about how to use Group Policy, see Advanced Group Policy Management.

To modify the blocking policy, use one of the following methods:

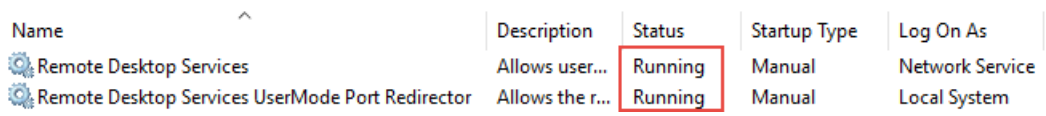
- In GPE, access the appropriate level of GPO (such as local or domain), and navigate to **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Connections** > **Allow users to connect remotely by using Remote Desktop Services**.
  1. Set the policy to either **Enabled** or **Not configured**.
  2. On the affected computers, open a command prompt window as an administrator, and run the **gpupdate /force** command.
- In GPM, navigate to the organizational unit (OU) in which the blocking policy is applied to the affected computers and delete the policy from the OU.

Check the status of the RDP services

On both the local (client) computer and the remote (target) computer, the following services should be running:

- Remote Desktop Services (TermService)
- Remote Desktop Services UserMode Port Redirector (UmRdpService)

You can use the Services MMC snap-in to manage the services locally or remotely. You can also use PowerShell to manage the services locally or remotely (if the remote computer is configured to accept remote PowerShell cmdlets).



Name	Description	Status	Startup Type	Log On As
Remote Desktop Services	Allows user...	Running	Manual	Network Service
Remote Desktop Services UserMode Port Redirector	Allows the r...	Running	Manual	Local System

On either computer, if one or both services are not running, start them.

> **NOTE**
>
> If you start the Remote Desktop Services service, click **Yes** to automatically restart the Remote Desktop Services UserMode Port Redirector service.

Check that the RDP listener is functioning

> **IMPORTANT**
>
> Follow this section's instructions carefully. Serious problems can occur if the registry is modified incorrectly. Before you starty modifying the registry, back up the registry so you can restore it in case something goes wrong.

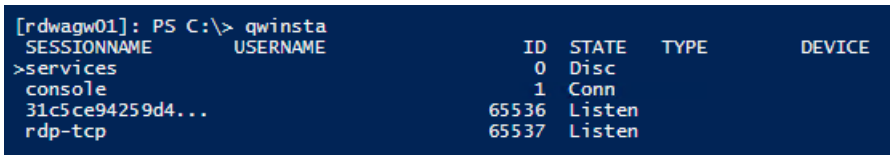
Check the status of the RDP listener

For this procedure, use a PowerShell instance that has administrative permissions. For a local computer, you can also use a command prompt that has administrative permissions. However, this procedure uses PowerShell because the same cmdlets work both locally and remotely.

1. To connect to a remote computer, run the following cmdlet:

   ```
   Enter-PSSession -ComputerName <computer name>
   ```

2. Enter **qwinsta**.

3. If the list includes **rdp-tcp** with a status of **Listen**, the RDP listener is working. Proceed to Check the RDP listener port. Otherwise, continue at step 4.

4. Export the RDP listener configuration from a working computer.

   a. Sign in to a computer that has the same operating system version as the affected computer has, and access that computer's registry (for example, by using Registry Editor).

   b. Navigate to the following registry entry:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

   c. Export the entry to a .reg file. For example, in Registry Editor, right-click the entry, select **Export**, and then enter a filename for the exported settings.

   d. Copy the exported .reg file to the affected computer.

5. To import the RDP listener configuration, open a PowerShell window that has administrative permissions on the affected computer (or open the PowerShell window and connect to the affected computer remotely).

   a. To back up the existing registry entry, enter the following cmdlet:

   ```
   cmd /c 'reg export "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-tcp"
   C:\Rdp-tcp-backup.reg'
   ```

   b. To remove the existing registry entry, enter the following cmdlets:

   ```
   Remove-Item -path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-tcp' -
   Recurse -Force
   ```

c. To import the new registry entry and then restart the service, enter the following cmdlets:

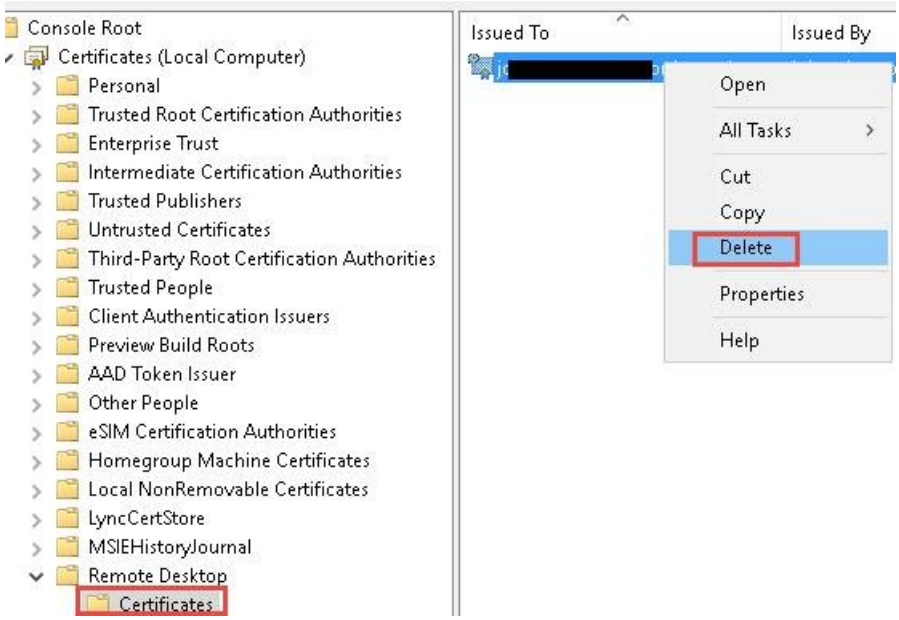
```
cmd /c 'regedit /s c:\<filename>.reg'
Restart-Service TermService -Force
```

Replace <filename> with the name of the exported .reg file.

6. Test the configuration by trying the remote desktop connection again. If you still can't connect, restart the affected computer.
7. If you still can't connect, check the status of the RDP self-signed certificate.

Check the status of the RDP self-signed certificate

1. If you still can't connect, open the Certificates MMC snap-in. When you are prompted to select the certificate store to manage, select **Computer account**, and then select the affected computer.
2. In the **Certificates** folder under **Remote Desktop**, delete the RDP self-signed certificate.



3. On the affected computer, restart the Remote Desktop Services service.
4. Refresh the Certificates snap-in.
5. If the RDP self-signed certificate has not been recreated, check the permissions of the MachineKeys folder.

Check the permissions of the MachineKeys folder

1. On the affected computer, open Explorer, and then navigate to **C:\ProgramData\Microsoft\Crypto\RSA**.
2. Right-click **MachineKeys**, select **Properties**, select **Security**, and then select **Advanced**.
3. Make sure that the following permissions are configured:
   - Builtin\Administrators: Full control
   - Everyone: Read, Write

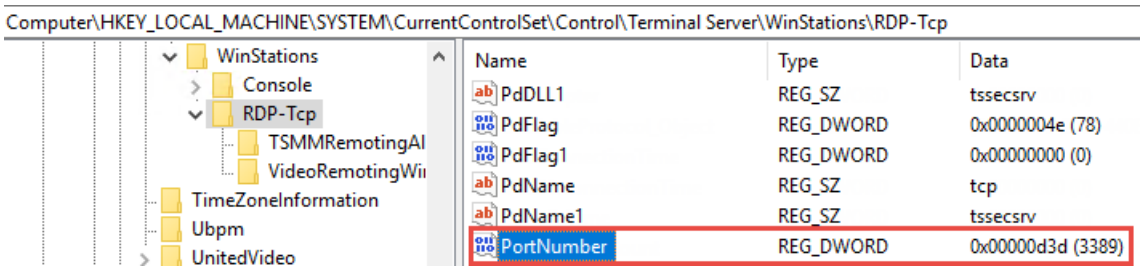
Check the RDP listener port

On both the local (client) computer and the remote (target) computer, the RDP listener should be listening on port 3389. No other applications should be using this port.

> **IMPORTANT**
>
> Follow this section's instructions carefully. Serious problems can occur if the registry is modified incorrectly. Before you starty modifying the registry, back up the registry so you can restore it in case something goes wrong.

To check or change the RDP port, use the Registry Editor:

1. Go to the Start menu, select **Run**, then enter **regedt32** into the text box that appears.
   - To connect to a remote computer, select **File**, and then select **Connect Network Registry**.
   - In the **Select Computer** dialog box, enter the name of the remote computer, select **Check Names**, and then select **OK**.
2. Open the registry and navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\<listener>**.



3. If **PortNumber** has a value other than **3389**, change it to **3389**.

> **IMPORTANT**
>
> You can operate Remote Desktop services using another port. However, we don't recommend you do this. This article doesn't cover how to troubleshoot that type of configuration.

4. After you change the port number, restart the Remote Desktop Services service.

Check that another application isn't trying to use the same port

For this procedure, use a PowerShell instance that has administrative permissions. For a local computer, you can also use a command prompt that has administrative permissions. However, this procedure uses PowerShell because the same cmdlets work locally and remotely.

1. Open a PowerShell window. To connect to a remote computer, enter **Enter-PSSession -ComputerName <computer name>**.
2. Enter the following command:

```
cmd /c 'netstat -ano | find "3389"'
```

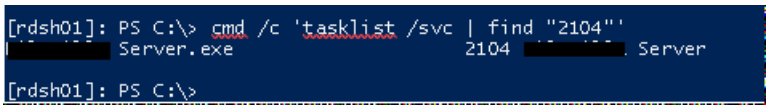
```
[rdsh01]: PS C:\> cmd /c 'netstat -ano | find "3389"'
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       2104
  TCP    [::]:3389              [::]:0                 LISTENING       2104
```

3. Look for an entry for TCP port 3389 (or the assigned RDP port) with a status of **Listening**.

> **NOTE**
>
> The process identifier (PID) for the process or service using that port appears under the PID column.

4. To determine which application is using port 3389 (or the assigned RDP port), enter the following command:

```
cmd /c 'tasklist /svc | find "<pid listening on 3389>"'
```



5. Look for an entry for the PID number that is associated with the port (from the **netstat** output). The services or processes that are associated with that PID appear on the right column.
6. If an application or service other than Remote Desktop Services (TermServ.exe) is using the port, you can resolve the conflict by using one of the following methods:
   - Configure the other application or service to use a different port (recommended).
   - Uninstall the other application or service.
   - Configure RDP to use a different port, and then restart the Remote Desktop Services service (not recommended).

Check whether a firewall is blocking the RDP port

Use the **psping** tool to test whether you can reach the affected computer by using port 3389.

1. Go to a different computer that isn't affected and download **psping** from https://live.sysinternals.com/psping.exe.
2. Open a command prompt window as an administrator, change to the directory in which you installed **psping**, and then enter the following command:

   ```
   psping -accepteula <computer IP>:3389
   ```

3. Check the output of the **psping** command for results such as the following:
   - **Connecting to <computer IP>**: The remote computer is reachable.
   - **(0% loss)**: All attempts to connect succeeded.
   - **The remote computer refused the network connection**: The remote computer is not reachable.
   - **(100% loss)**: All attempts to connect failed.
4. Run **psping** on multiple computers to test their ability to connect to the affected computer.
5. Note whether the affected computer blocks connections from all other computers, some other computers, or only one other computer.
6. Recommended next steps:
   - Engage your network administrators to verify that the network allows RDP traffic to the affected computer.
   - Investigate the configurations of any firewalls between the source computers and the affected computer (including Windows Firewall on the affected computer) to determine whether a firewall is blocking the RDP port.

Clients can't connect and get the "Class not registered" error

1/18/2020 • 2 minutes to read • Edit Online

When you try to connect to a remote computer using a client running Windows 10, version 1709 or later, the client may not connect while the Remote Desktop Session Host server reports a message that contains the "Class not registered (0x80040154)" error code.

This issue occurs when the user who's trying to connect has a mandatory user profile. To resolve this issue, install the July 24, 2018—KB4338817 (OS Build 16299.579) Windows 10 update.

Clients can't connect and see "No licenses available" error

1/18/2020 • 2 minutes to read • Edit Online

This situation applies to deployments that include an RDSH server and a Remote Desktop Licensing server.

First, identify which behavior the users are seeing:

- The session was disconnected because no licenses are available or no license server is available.
- Access was denied because of a security error.

Sign in to the RD Session Host as a domain administrator and open the RD License Diagnoser. Look for messages like the following:

- The grace period for the Remote Desktop Session Host server has expired, but the RD Session Host server hasn't been configured with any license servers. Connections to the RD Session Host server will be denied unless a license server is configured for the RD Session Host server.
- License server <computer name> is not available. This could be caused by network connectivity problems, the Remote Desktop Licensing service is stopped on the license server, or RD Licensing isn't available.

These problems tend to be associated with the following user messages:

- The remote session was disconnected because there are no Remote Desktop client access licenses available for this computer.
- The remote session was disconnected because there are no Remote Desktop License Servers available to provide a license.

In this case, configure the RD Licensing service.

If the RD License Diagnoser lists other problems, such as "The RDP protocol component X.224 detected an error in the protocol stream and has disconnected the client," there may be a problem that affects the license certificates. Such problems tend to be associated with user messages, such as the following:

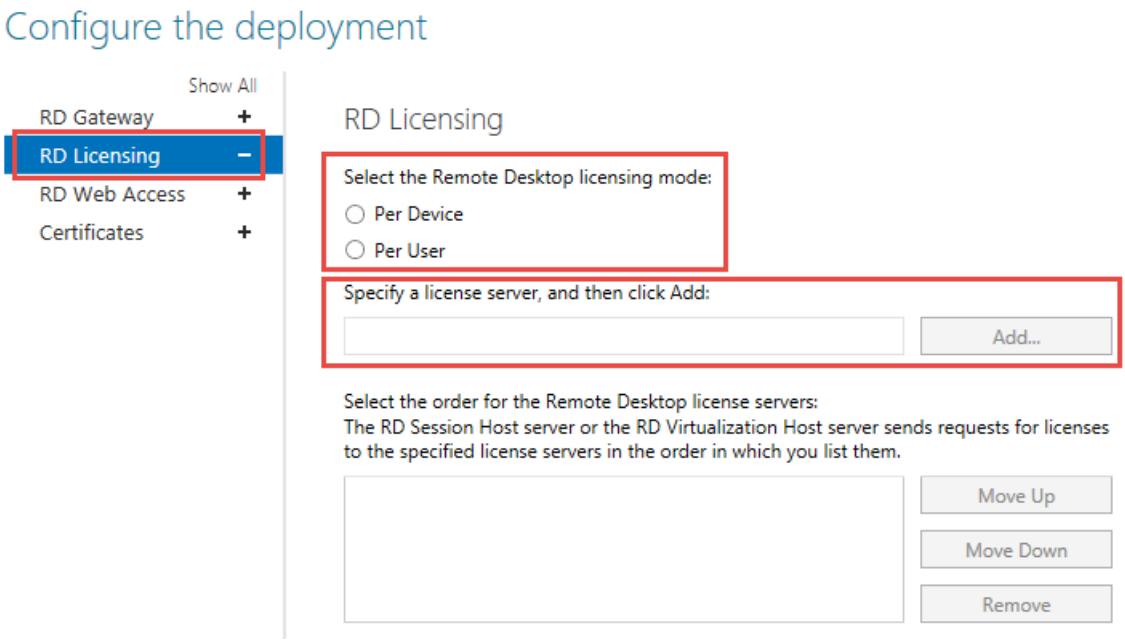
Because of a security error, the client could not connect to the Terminal server. After making sure that you are signed in to the network, try connecting to the server again.

In this case, refresh the X509 Certificate registry keys.

Configure the RD Licensing service

The following procedure uses Server Manager to make the configuration changes. For information about how to configure and use Server Manager, see Server Manager

1. Open **Server Manager** and navigate to **Remote Desktop Services**.
2. On **Deployment Overview**, select **Tasks**, and then select **Edit Deployment Properties**.
3. Select **RD Licensing**, then select the appropriate licensing mode for your deployment (**Per Device** or **Per User**).
4. Enter the fully qualified domain name (FQDN) of your RD License server, and then select **Add**.
5. If you have more than one RD License server, repeat step 4 for each server.



Refresh the X509 Certificate registry keys

> **IMPORTANT**
>
> Follow this section's instructions carefully. Serious problems can occur if the registry is modified incorrectly. Before you starty modifying the registry, back up the registry so you can restore it in case something goes wrong.

To resolve this problem, back up and then remove the X509 Certificate registry keys, restart the computer, and then reactivate the RD Licensing server. Follow these steps.

> **NOTE**
>
> Perform the following procedure on each of the RDSH servers.

Here's how to reactivate the RD Licensing server:

1. Open the Registry Editory and navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\RCM**.
2. On the Registry menu, select **Export Registry File**.
3. Enter **exported- Certificate** into the **File name** box, then select **Save**.
4. Right-click each of the following values, select **Delete**, and then select **Yes** to verify the deletion:
   - **Certificate**
   - **X509 Certificate**
   - **X509 Certificate ID**
   - **X509 Certificate2**
5. Exit the Registry Editor and restart the RDSH server.

User can't authenticate or must authenticate twice

1/18/2020 • 10 minutes to read • Edit Online

This article addresses several issues that can cause problems that affect user authentication.

Access denied, restricted type of logon

In this situation, a Windows 10 user attempting to connect to Windows 10 or Windows Server 2016 computers is denied access with the following message:

> Remote Desktop Connection:
> The system administrator has restricted the type of logon (network or interactive) that you may use. For assistance, contact your system administrator or technical support.

This issue occurs when Network Level Authentication (NLA) is required for RDP connections, and the user is not a member of the **Remote Desktop Users** group. It can also occur if the **Remote Desktop Users** group has not been assigned to the **Access this computer from the network** user right.

To solve this issue, do one of the following things:

- Modify the user's group membership or user rights assignment.
- Turn off NLA (not recommended).
- Use remote desktop clients other than Windows 10. For example, Windows 7 clients do not have this issue.

Modify the user's group membership or user rights assignment

If this issue affects a single user, the most straightforward solution to this issue is to add the user to the **Remote Desktop Users** group.

If the user is already a member of this group (or if multiple group members have the same problem), check the user rights configuration on the remote Windows 10 or Windows Server 2016 computer.

1. Open Group Policy Object Editor (GPE) and connect to the local policy of the remote computer.
2. Navigate to **Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment**, right-click **Access this computer from the network**, and then select **Properties**.
3. Check the list of users and groups for **Remote Desktop Users** (or a parent group).
4. If the list doesn't include either **Remote Desktop Users** or a parent group like **Everyone**, you must add it to the list. If you have more than one computer in your deployment, use a group policy object.
   For example, the default membership for **Access this computer from the network** includes **Everyone**. If your deployment uses a group policy object to remove **Everyone**, you may need to restore access by updating the group policy object to add **Remote Desktop Users**.

Access denied, A remote call to the SAM database has been denied

This behavior is most likely to occur if your domain controllers are running Windows Server 2016 or later, and users attempt to connect by using a customized connection app. In particular, applications that access the user's profile information in Active Directory will be denied access.

This behavior results from a change to Windows. In Windows Server 2012 R2 and earlier versions, when a user signs in to a remote desktop, the Remote Connection Manager (RCM) contacts the domain controller (DC) to query the configurations that are specific to Remote Desktop on the user object in Active Directory Domain Services (AD DS). This information is displayed in the Remote Desktop Services Profile tab of a user's object

properties in the Active Directory Users and Computers MMC snap-in.

Starting in Windows Server 2016, RCM no longer queries the user's object in AD DS. If you need RCM to query AD DS because you're using Remote Desktop Services attributes, you must manually enable the query.

> **IMPORTANT**
> Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, back up the registry for restoration in case problems occur.

To enable the legacy RCM behavior on a RD Session Host server, configure the following registry entries, and then restart the **Remote Desktop Services** service:

- **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services**
- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\<Winstation name>**
  - Name: **fQueryUserConfigFromDC**
  - Type: **Reg_DWORD**
  - Value: **1** (Decimal)

To enable the legacy RCM behavior on a server other than a RD Session Host server, configure these registry entries and the following additional registry entry (and then restart the service):

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server**

For more information about this behavior, see KB 3200967 Changes to Remote Connection Manager in Windows Server.

User can't sign in using a smart card

This section addresses three common scenarios where a user can't sign in to a remote desktop using a smart card.

Can't sign in with a smart card in a branch office with a read-only domain controller (RODC)

This issue occurs in deployments that include an RDSH server at a branch site that uses a RODC. The RDSH server is hosted in the root domain. Users at the branch site belong to a child domain, and use smart cards for authentication. The RODC is configured to cache user passwords (the RODC belongs to the **Allowed RODC Password Replication Group**). When users try to sign in to sessions on the RDSH server, they receive messages such as "The attempted logon is invalid. This is either due to a bad username or authentication information."

This issue is caused by how the root DC and the RDOC manage user credential encryption. The root DC uses an encryption key to encrypt the credentials and the RODC gives the client the decryption key. When a user receives the "invalid" error, that means the two keys don't match.

To work around this issue, try one of the following things:

- Change your DC topology by turning off password caching on the RODC or deploy a writeable DC to teh branch site.
- Move the RDSH server to the same child domain as the users.
- Allow users to sign in without smart cards.

Be advised that all of these solutions require compromises in either performance or security level.

User can't sign in to a Windows Server 2008 SP2 computer using a smart card

This issue occurs when users sign in to a Windows Server 2008 SP2 computer that has been updated with KB4093227 (2018.4B). When users attempt to sign in using a smart card, they are denied access with messages such as “No valid certificates found. Check that the card is inserted correctly and fits tightly.” At the same time, the

Windows Server computer records the Application event "An error occurred while retrieving a digital certificate from the inserted smart card. Invalid Signature."

To resolve this issue, update the Windows Server computer with the 2018.06 B re-release of KB 4093227, Description of the security update for the Windows Remote Desktop Protocol (RDP) denial of service vulnerability in Windows Server 2008: April 10, 2018.

Can't stay signed in with a smart card and Remote Desktop Services service hangs

This issue occurs when users sign in to a Windows or Windows Server computer that has been updated with KB 4056446. At first, the user may be able to sign in to the system by using a smart card, but then receives a "SCARD_E_NO_SERVICE" error message. The remote computer may become unresponsive.

To work around this issue, restart the remote computer.

To resolve this issue, update the remote computer with the appropriate fix:

- Windows Server 2008 SP2: KB 4090928, Windows leaks handles in the lsm.exe process and smart card applications may display "SCARD_E_NO_SERVICE" errors
- Windows Server 2012 R2: KB 4103724, May 17, 2018—KB4103724 (Preview of Monthly Rollup)
- Windows Server 2016 and Windows 10, version 1607: KB 4103720, May 17, 2018—KB4103720 (OS Build 14393.2273)

If the remote PC is locked, the user needs to enter a password twice

This issue may occur when a user attempts to connect to a remote desktop running Windows 10 version 1709 in a deployment in which RDP connections don't require NLA. Under these conditions, if the remote desktop has been locked, the user needs to enter their credentials twice when connecting.

To resolve this issue, update the Windows 10 version 1709 computer with KB 4343893, August 30, 2018—KB4343893 (OS Build 16299.637).

User can't sign in and receives "authentication error" and "CredSSP encryption oracle remediation" messages

When users try to sign in using any version of Windows from Windows Vista SP2 and later versions or Windows Server 2008 SP2 and later versions, they're denied access and recieve messages like these:

```
An authentication error has occurred. The function requested is not supported.
...
This could be due to CredSSP encryption oracle remediation
...
```

"CredSSP encryption oracle remediation" refers to a set of security updates released in March, April, and May of 2018. CredSSP is an authentication provider that processes authentication requests for other applications. The March 13, 2018, "3B" and subsequent updates addressed an exploit in which an attacker could relay user credentials to execute code on the target system.

The initial updates added support for a new Group Policy Object, Encryption Oracle Remediation, that has the following possible settings:

- Vulnerable: Client applications that use CredSSP can fall back to insecure versions, but this behavior exposes the remote desktops to attacks. Services that use CredSSP accept clients that have not been updated.
- Mitigated: Client applications that use CredSSP can't fall back to insecure versions, but services that use CredSSP accept clients that have not been updated.
- Force Updated Clients: Client applications that use CredSSP can't fall back to insecure versions, and services

that use CredSSP will not accept unpatched clients.

> **NOTE**
> This setting should not be deployed until all remote hosts support the newest version.

The May 8, 2018 update changed the default Encryption Oracle Remediation setting from Vulnerable to Mitigated. With this change in place, Remote Desktop clients that have the updates can't connect to servers that don't have them (or updated servers that have not been restarted). For more information about the CredSSP updates, see KB 4093492.

To resolve this issue, update and restart all systems. For a full list of updates and more information about the vulnerabilities, see CVE-2018-0886 | CredSSP Remote Code Execution Vulnerability.

To work around this issue until the updates are complete, check KB 4093492 for allowed types of connections. If there are no feasible alternatives you may consider one of the following methods:

- For the affected client computers, set the Encryption Oracle Remediation policy back to **Vulnerable**.
- Modify the following policies in the **Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security** group policy folder:
  - **Require use of specific security layer for remote (RDP) connections**: set to **Enabled** and select **RDP**.
  - **Require user authentication for remote connections by using Network Level authentication**: set to **Disabled**.

    > **IMPORTANT**
    > Changing these group policies reduces your deployment's security. We recommend you only use them temporarily, if at all.

For more information about working with group policy, see Modifying a blocking GPO.

After you update client computers, some users need to sign in twice

When users sign in to Remote Desktop using a computer running Windows 7 or Windows 10, version 1709, they immediately see a second sign-in prompt. This issue happens if the client computer has the following updates:

- Windows 7: KB 4103718, May 8, 2018—KB4103718 (Monthly Rollup)
- Windows 10 1709: KB 4103727, May 8, 2018—KB4103727 (OS Build 16299.431)

To resolve this issue, ensure that the computers that the users want to connect to (as well as RDSH or RDVI servers) are fully updated through June, 2018. This includes the following updates:

- Windows Server 2016: KB 4284880, June 12, 2018—KB4284880 (OS Build 14393.2312)
- Windows Server 2012 R2: KB 4284815, June 12, 2018—KB4284815 (Monthly Rollup)
- Windows Server 2012: KB 4284855, June 12, 2018—KB4284855 (Monthly Rollup)
- Windows Server 2008 R2: KB 4284826, June 12, 2018—KB4284826 (Monthly Rollup)
- Windows Server 2008 SP2: KB4056564, Description of the security update for the CredSSP remote code execution vulnerability in Windows Server 2008, Windows Embedded POSReady 2009, and Windows Embedded Standard 2009: March 13, 2018

Users are denied access on a deployment that uses Remote Credential Guard with multiple RD Connection Brokers

This issue occurs in high-availability deployments that use two or more Remote Desktop Connection Brokers, if Windows Defender Remote Credential Guard is in use. Users can't sign in to remote desktops.

This issue occurs because Remote Credential Guard uses Kerberos for authentication, and restricts NTLM. However, in a high-availability configuration with load balancing, the RD Connection Brokers can't support Kerberos operations.

If you need to use a high-availability configuration with load-balanced RD Connection Brokers, you can work around this issue by disabling Remote Credential Guard. For more information about how to manage Windows Defender Remote Credential Guard, see Protect Remote Desktop credentials with Windows Defender Remote Credential Guard.

On connecting, user receives "Remote Desktop Service is currently busy" message

1/18/2020 • 2 minutes to read • Edit Online

To determine an appropriate response to this issue, see the following:

- Does the Remote Desktop Services service becomes unresponsive (for example, the remote desktop client appears to “hang” at the Welcome screen).
  - If the service becomes unresponsive, see RDSH server memory issue.
  - If the client appears to be interacting with the service normally, continue to the next step.
- If one or more users disconnect their remote desktop sessions, can users connect again?
  - If the service continues to deny connections no matter how many users disconnect their sessions, see RD listener issue.
  - If the service begins accepting connections again after a number of users have disconnected their sessions, check the connection limit policy.

RDSH server memory issue

A memory leak has been found on some Windows Server 2012 R2 RDSH servers. Over time, these servers begin to refuse both remote desktop connections and local console sign-ins with messages like the following:

> The task you are trying to do can't be completed because Remote Desktop Service is currently busy. Please try again in a few minutes. Other users should still be able to sign in.

Remote Desktop clients attempting to connect also become unresponsive.

To work around this issue, restart the RDSH server.

To resolve this issue, apply KB 4093114, April 10, 2018—KB4093114 (Monthly Rollup), to the RDSH servers.

RD listener issue

An issue has been noted on some RDSH servers that have been upgraded directly from Windows Server 2008 R2 to Windows Server 2012 R2 or Windows Server 2016. When a Remote Desktop client connects to the RDSH server, the RDSH server creates an RD listener for the user session. The affected servers keep a count of the RD listeners that increases as users connect, but never decreases.

You can work around this issue with the following methods:

- Restart the RDSH server to reset the count of RD listeners
- Modify the connection limit policy, setting it to a very large value. For more information about managing the connection limit policy, see Check the connection limit policy.

To resolve this issue, apply the following updates to the RDSH servers:

- Windows Server 2012 R2: KB 4343891, August 30, 2018—KB4343891 (Preview of Monthly Rollup)
- Windows Server 2016: KB 4343884, August 30, 2018—KB4343884 (OS Build 14393.2457)

Check the connection limit policy

You can set the limit on the number of simultaneous remote desktop connections at the individual computer level or by configuring a group policy object (GPO). By default, the limit is not set.

To check the current settings and identify any existing GPOs on the RDSH server, open a command prompt window as an administrator and enter the following command:

```
gpresult /H c:\gpresult.html
```

After this command finishes, open **gpresult.html**. In **Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections**, find the **Limit number of connections** policy.

- If the setting for this policy is **Disabled**, then group policy is not limiting RDP connections.
- If the setting for this policy is **Enabled**, then check **Winning GPO**. If you need to remove or change the connection limit, edit this GPO.

To enforce policy changes, open a command prompt window on the affected computer, and enter the following command:

```
gpupdate /force
```

Remote Desktop client disconnects and can't reconnect to the same session

1/18/2020 • 2 minutes to read • Edit Online

After Remote Desktop client loses its connection to the remote desktop, the client can't immediately reconnect. The user recieves one of the following error messages:

- The client couldn't connect to the terminal server because of a security error. Make sure you are signed in to the network, then try connecting again.
- Remote Desktop disconnected. Because of a security error, the client could not connect to the remote computer. Verify that you are logged onto the network and then try connecting again.

When the Remote Desktop client reconnects, the RDSH server reconnects the client to a new session instead of the original session. However, when you check the RDSH server, it says that the original session is still active and didn't enter a disconnected state.

To work around this issue, you can enable the **Configure keep-alive connection interval** policy in the **Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections** group policy folder. If you enable this policy, you must enter a keep-alive interval. The keep-alive interval determines how often, in minutes, the server checks the session state.

This issue can also be fixed by reconfiguring your authentication and configuration settings. You can reconfigure these settings at either the server level or by using group policy objects (GPOs). Here's how to reconfigure your settings: **Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security** group policy folder.

1. On the RD Session Host server, open **Remote Desktop Session Host Configuration**.
2. Under **Connections**, right-click the name of the connection, then select **Properties**.
3. In the **Properties** dialog box for the connection, on the **General** tab, in **Security** layer, select a security method.
4. Go to **Encryption level** and select the level you want. You can select **Low**, **Client Compatible**, **High**, or **FIPS Compliant**.

NOTE

- When communications between clients and RD Session Host servers require the highest level of encryption, use FIPS-compliant encryption.
- Any encryption level settings you configure in Group Policy override the settings you configured using the Remote Desktop Services Configuration tool. Also, if you enable the System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing policy, this setting overrides the **Set client connection encryption level** policy. The system cryptography policy is in the **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options** folder.
- When you change the encryption level, the new encryption level takes effect the next time a user signs in. If you require multiple levels of encryption on one server, install multiple network adapters and configure each adapter separately.
- To verify your certificate has a corresponding private key, go to Remote Desktop Services Configuration, right-click the connection that you want to view the certificate for, select **General**, then select **Edit**. After that, select **View certificate**. When you go to the **General** tab, you should see the statement, "You have a private key that corresponds to this certificate" if there's a key. You can also view this information with the Certificates snap-in.
- FIPS-compliant encryption (the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** policy or the **FIPS Compliant** setting in Remote Desktop Server Configuration) encrypts and decrypts data sent between the server and client with the Federal Information Processing Standard (FIPS) 140-1 encryption algorithms that use Microsoft cryptographic modules. For more information, see FIPS 140 Validation.
- The **High** setting encrypts data sent between the server and client by using strong 128-bit encryption.
- The **Client Compatible** setting encrypts data sent between the client and the server at the maximum key strength supported by the client.
- The **Low** setting encrypts data sent from the client to the server using 56-bit encryption.

Remote laptop disconnects from wireless network

1/18/2020 • 2 minutes to read • Edit Online

This issue may occur when a Remote Desktop client connects to a laptop computer by using an 802.1x wireless network. The laptop intermittently disconnects from the wireless network and doesn't automatically reconnect.

This is a known issue that occurs when the network authentication setting for the wireless network connection is **User authentication**.

To work around this issue, set the network authentication setting to **User or computer authentication** or **Computer authentication**.

> **NOTE**
> To change the network authentication settings on a single computer, you may need to use the Network and Sharing Center control panel to create a new wireless connection with the new settings.

For a full description of how to configure wireless network settings using GPOs, see Configure Wireless Network (IEEE 802.11) Policies.

Poor performance or application problems during remote desktop connection

1/18/2020 • 2 minutes to read • Edit Online

This article addresses several common issues that users can experience when they use remote desktop functionality.

Intermittent problems with new Microsoft Azure virtual machines

This issue affects virtual machines that have been recently provisioned. After the user connects to the virtual machine, the remote desktop session does not load all the user's settings correctly.

To work around this issue, disconnect from the virtual machine, wait for at least 20 minutes, and then connect again.

To resolve this issue, apply the following updates to the virtual machines, as appropriate:

- Windows 10 and Windows Server 2016: KB 4343884, August 30, 2018—KB4343884 (OS Build 14393.2457)
- Windows Server 2012 R2: KB 4343891, August 30, 2018—KB4343891 (Preview of Monthly Rollup)

Video playback issues on Windows 10 version 1709

This issue occurs when users connect to remote computers that are running Windows 10, version 1709. When these users play video using the VMR9 (Video Mixing Renderer 9) codec, the player shows only a black window.

This is a known issue in Windows 10, version 1709. The issue doesn't occur in Windows 10, version 1703.

Desktop sharing issues on Windows 10

This issue occurs when the user has a read-only user profile (and associated registry hive), such as in a kiosk scenario. When such a user connects to a remote computer that is running Windows 10, version 1803, they can't share their desktop.

To fix this issue, apply the Windows 10 update 4340917, July 24, 2018—KB4340917 (OS Build 17134.191).

Performance issues when mixing versions of Windows 10 if NLA is disabled

This issue occurs when Remote Desktop client computers running Windows 10 connect to remote desktops that run different versions of Windows 10 while NLA is disabled. Users of Remote Desktop clients on computers running Windows 10, version 1709 or earlier experience poor performance when they connect to remote desktops running Windows 10, version 1803 or later.

This occurs because, when NLA is disabled, the older client computers use a slower protocol when they connect to Windows 10, version 1803 or a later version.

To resolve this issue, apply KB 4340917, July 24, 2018—KB4340917 (OS Build 17134.191).

Black screen issue

This issue occurs in Windows 8.0, Windows 8.1, Windows 10 RTM, and Windows Server 2012 R2. A user launches multiple applications in a remote desktop, then disconnects from the session. Periodically, the user reconnects to the remote desktop to interact with the applications, and then disconnects again. At some point, when the user reconnects, the remote desktop session only shows a black screen. To get the session to display properly again, the user then has to end their session from either the remote computer's console or the RDSH server console and stop their session's applications.

To resolve this issue, apply the following updates as appropriate:

- Windows 8 and Windows Server 2012: KB4103719, May 17, 2018—KB4103719 (Preview of Monthly Rollup)
- Windows 8.1 and Windows Server 2012 R2: KB4103724, May 17, 2018—KB4103724 (Preview of Monthly Rollup) and KB 4284863, June 21, 2018—KB4284863 (Preview of Monthly Rollup)
- Windows 10: Fixed in KB4284860, June 12, 2018—KB4284860 (OS Build 10240.17889)

Additional Remote Desktop resources

9/27/2019 • 2 minutes to read • Edit Online

In addition to the information here in the Windows Server 2016 library, you can use the following resources to learn about and get help with Remote Desktop Services:

- On Twitter? So are we: @RDS4U
- Participate in general discussions about Remote Desktop Services in the RDS TechNet forum.
- For discussion about Remote Desktop applications/clients for Windows, Android, iOS, and Mac, visit the Remote Desktop clients TechNet forum.
- For MultiPoint, check out the MultiPoint TechNet forum.

If you have ideas about Remote Desktop Services that you want to share with us, post a topic in our UserVoice forum.