

Azure Reference Architecture & Design Guide

v.1.2

Contents

Contents.....	2
Introduction.....	3
Audience.....	3
Use Case Scenarios.....	3
Business Objectives.....	3
30-day Trial or POC (All Azure Deployment).....	3
Hybrid Deployment (On Premise and Azure).....	7
Endpoint Access Using On-premises.....	8
Endpoint Access Using Azure.....	10
Multisite.....	10
Server Components.....	10
Virtual Machine Requirements in Azure.....	12
Virtual Machine Requirements On-premises.....	12
Office-to-office VPN.....	12
All-Azure Deployment.....	12
All in Azure.....	13
Server Components.....	13
Azure Marketplace Virtual Machine Templates.....	14
Configuring Parallels RAS Between Networks.....	15
Azure Network Configuration for Inbound Traffic.....	16
Network Security Groups for Internet Inbound Traffic.....	16
Assign Firewall Rules to RAS Subnet and Virtual Machines.....	17
Virtual Network Configuration.....	18
HALB or Gateway Virtual Machine Security Group Configuration.....	18
Security Rules Test and Access Using Azure.....	20
Best Practices.....	20
Remote Desktop/Terminal Server Performance Settings.....	20
Performance Options Settings.....	20
RemoteFX.....	22
Enable RemoteFX Using Group Policy.....	22
RemoteFX Settings for Server 2012 and 2012 R2.....	22
RemoteFX Settings for Windows Workstations Running Remote PC Agents and VDI Agents.....	23
RemoteFX USB Redirection, Audio Redirection, and Time Zone Redirection.....	24
RemoteFX USB Redirection.....	24
Enable Audio / Recording Redirection.....	25
Time Zone Redirection.....	26
Ensure That Desktop Experience Is Installed on All Terminal Servers.....	27
Windows Server 2016 Specific Group Policies.....	27
Device and Resource Redirection.....	28
Remote Session Environment (H.264, RemoteFX, Adaptive Acceleration).....	28
Windows 2008 R2 RemoteFX Compatibility.....	29
RDP Security.....	30
Skype for Business in Azure.....	31
Windows Licenses and RDS Client Access Licenses (CALs).....	31
References.....	31

Introduction

Parallels® Remote Application Server is an application delivery and virtual desktop solution. It extends Microsoft® Windows Remote Desktop Services by providing centralized management, universal printing, and remote access to Windows® Terminal Services-based applications from virtually any device. The solution also includes a built-in, hypervisor agnostic, Virtual Desktop Infrastructure (VDI) solution.

Application delivery and VDI solutions traditionally can be challenging to set up and manage. Design and implementation can take weeks or even months. In contrast, Parallels Remote Application Server can be installed in days or even hours, providing a quicker return on your investment and an easier path to realizing the benefits of remote desktop computing.

This document describes the best practice guidelines for deploying and configuring Parallels Remote Application Server v15.5.

Audience

Used in conjunction with the Parallels Remote Application Server Modular Reference Architecture, these documents provide basic best practice guidance for companies looking to leverage Parallels and Microsoft cloud technologies to deliver a state-of-the-art solution for their users. Additional information about Azure can be found [here](#).

Use Case Scenarios

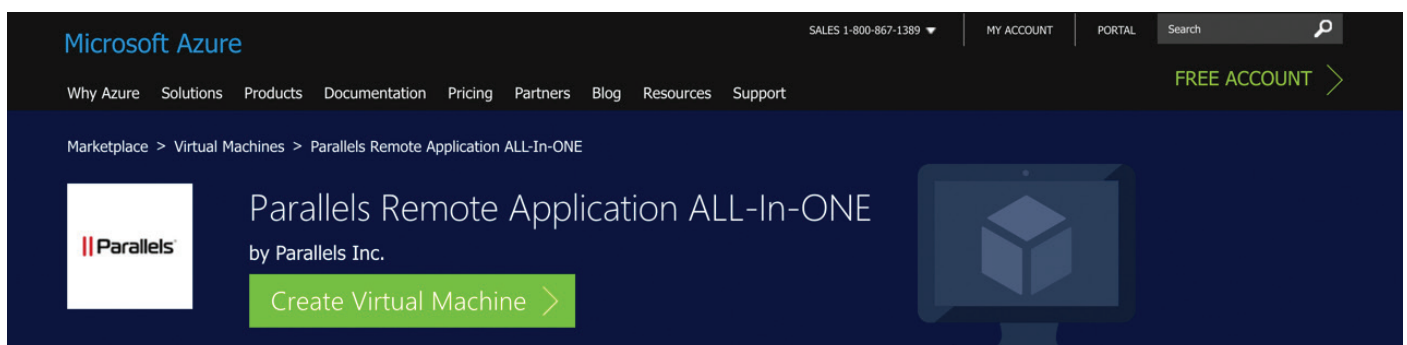
Your business plans to leverage Microsoft and Parallels Remote Application Server to deliver a hosted desktop solution for its accounting department. The solution will provide value to the department by enabling access to Windows desktops and applications from any device. The value of this solution for businesses is most evident in the ability to quickly bring new desktop services online through a subscription to Azure infrastructure services

Business Objectives

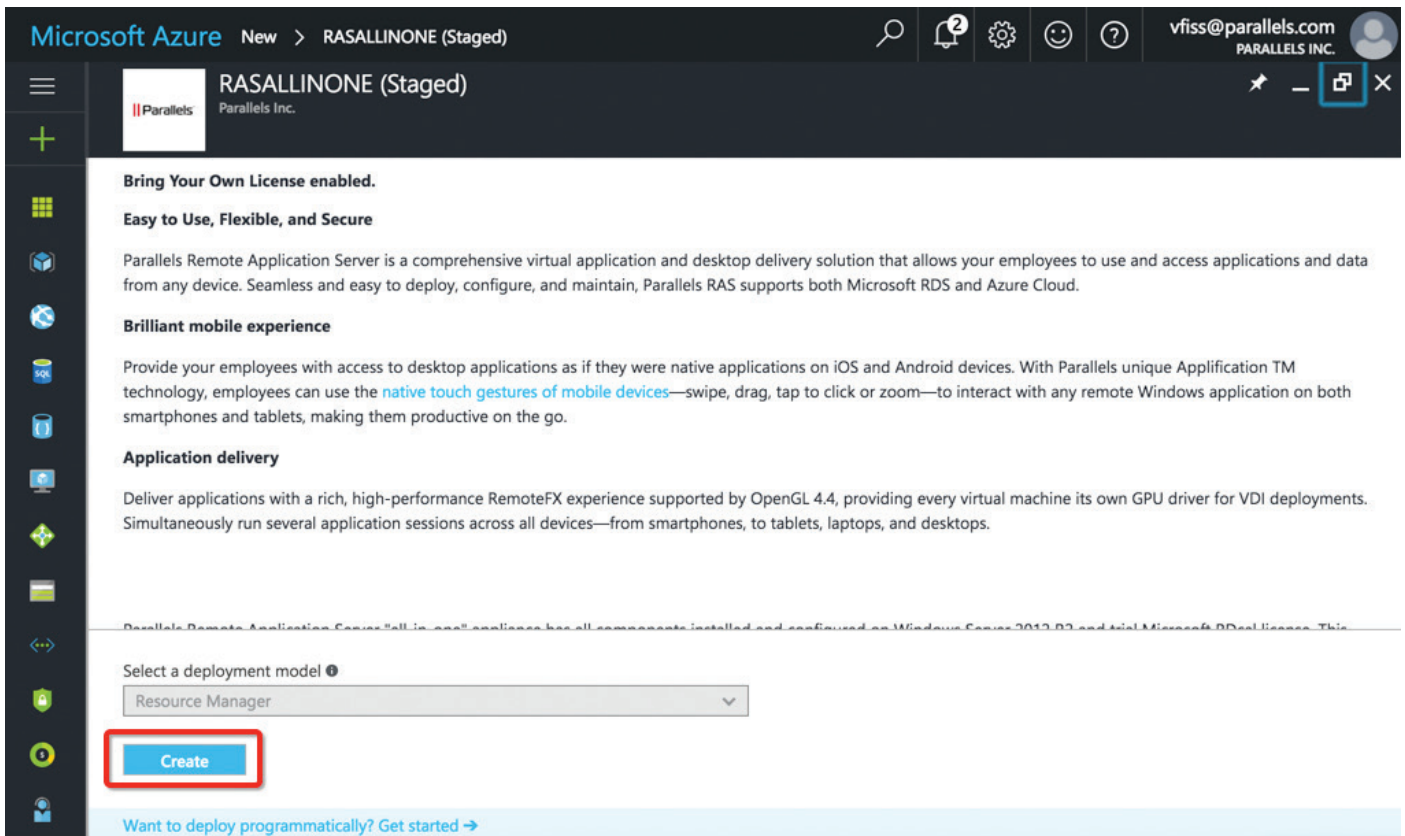
- Provide secure access to desktops and applications for the accounting team
- Avoid the need to build new infrastructure within private deployments and Azure deployments
- Ability to distribute Remote Application Server load between datacenters
- Enable cloud and hybrid load balancing.
- Ability to integrate with Azure Global Load-Balancer
- Resource elasticity leveraging Azure

30-day Trial or POC (All Azure Deployment)

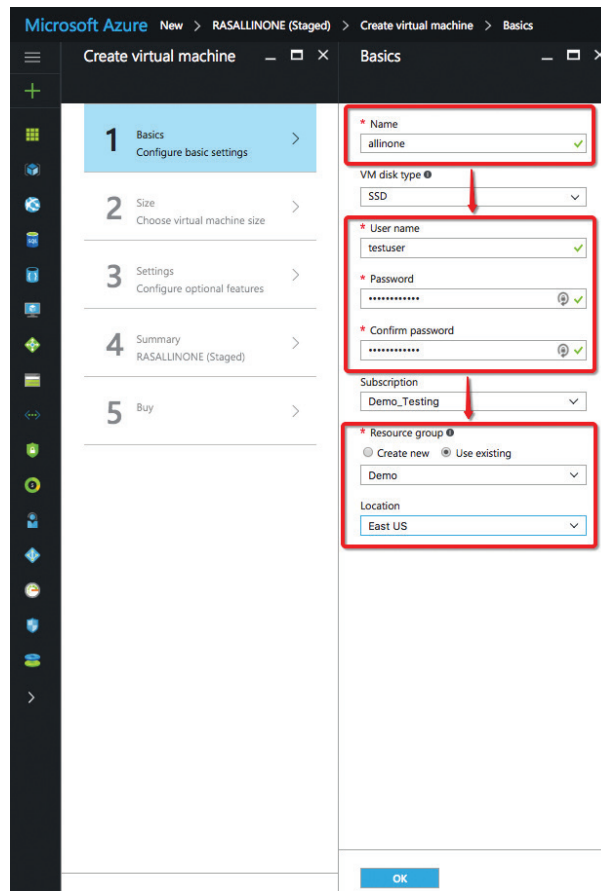
A 30-day trial or POC can be started at any time from Azure Marketplace using this [link](#).



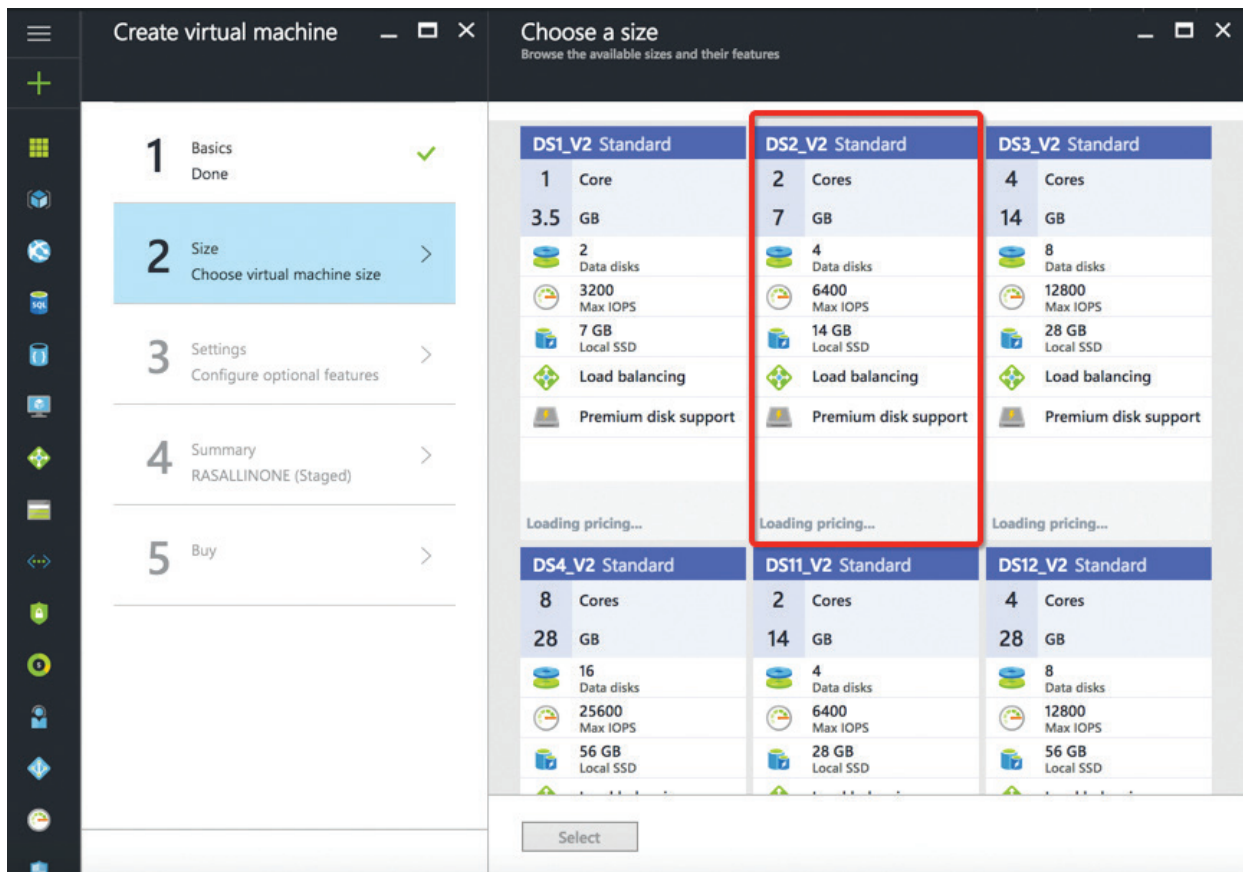
The screenshot shows the Microsoft Azure Marketplace interface. At the top, the Microsoft Azure logo is on the left, and navigation links for 'SALES 1-800-867-1389', 'MY ACCOUNT', 'PORTAL', and 'Search' are on the right. Below the header, a navigation menu includes 'Why Azure', 'Solutions', 'Products', 'Documentation', 'Pricing', 'Partners', 'Blog', 'Resources', and 'Support'. A 'FREE ACCOUNT' button with a right-pointing arrow is also visible. The main content area shows the breadcrumb 'Marketplace > Virtual Machines > Parallels Remote Application ALL-In-ONE'. On the left is the Parallels logo. The central text reads 'Parallels Remote Application ALL-In-ONE by Parallels Inc.' with a prominent green 'Create Virtual Machine' button below it. To the right is a graphic of a computer monitor displaying a 3D cube.



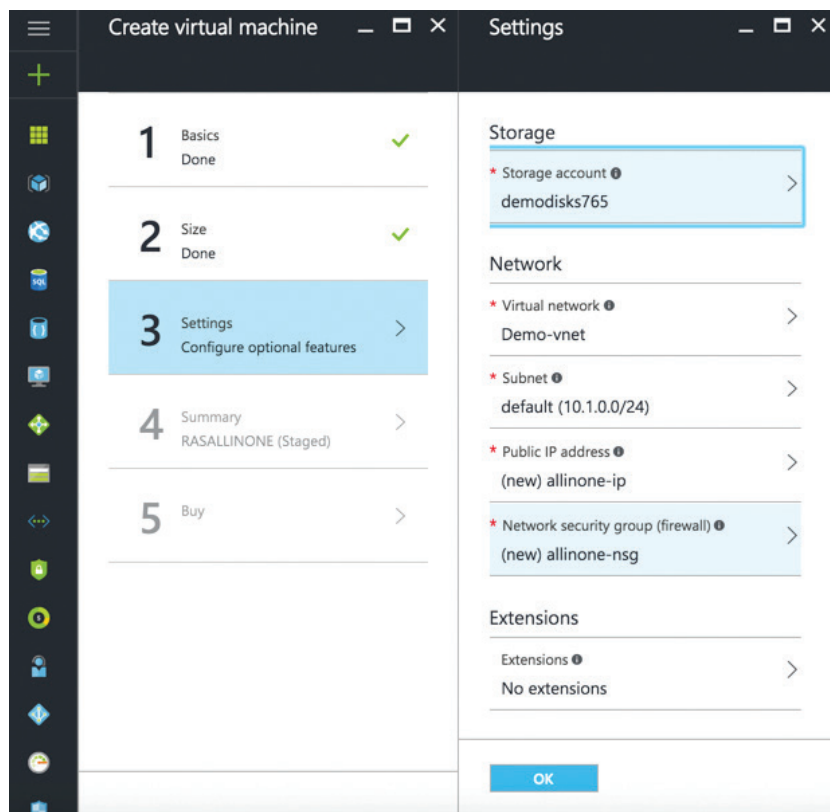
For the VM offering, make sure you use “allinone”, create a “testuser” account (please use your own password), and choose the location you want to deploy.



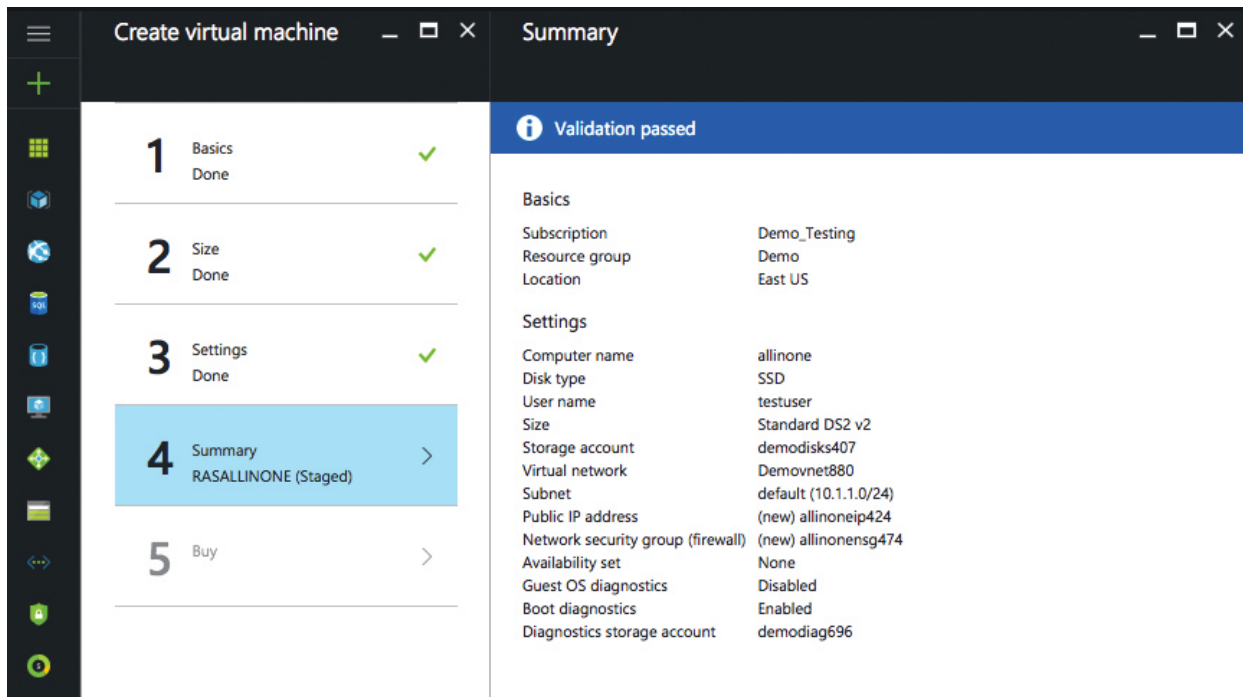
Select Azure Service Offering. We recommend DS2_V2 for POCs:



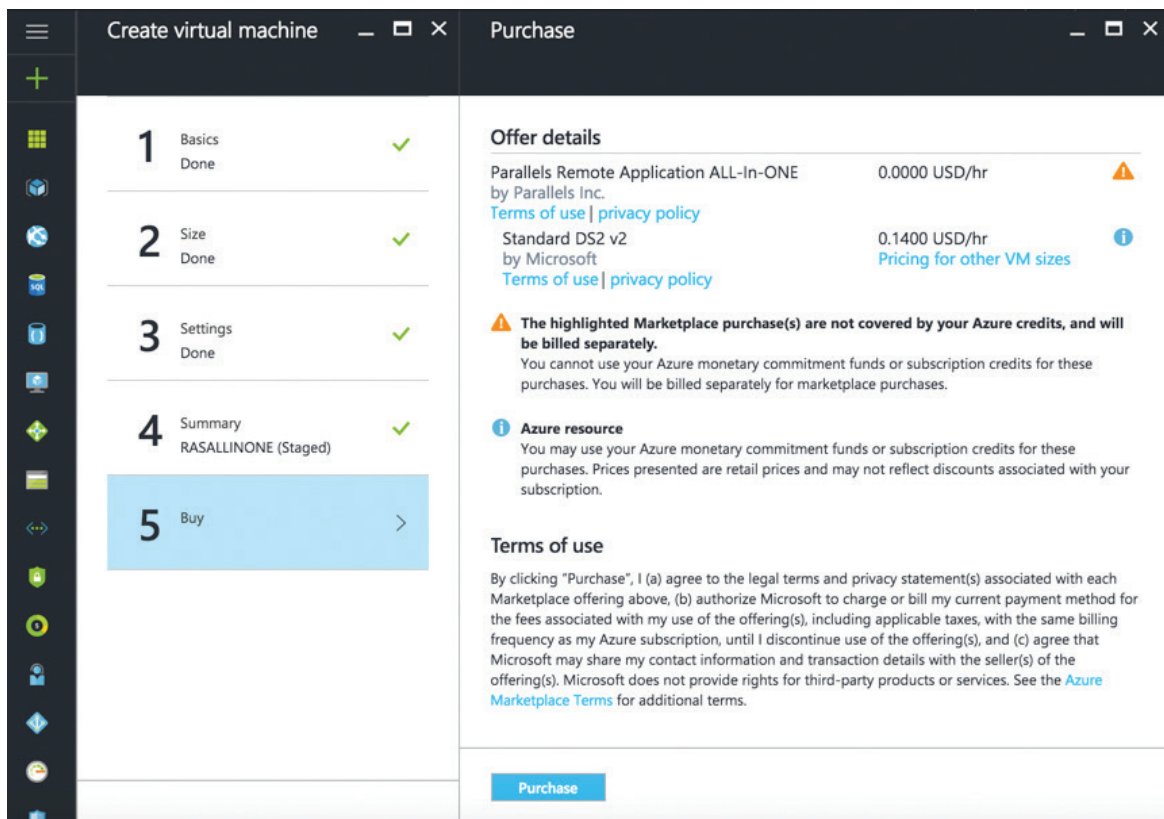
Use default settings for Networking at this point. If you have RAS rules created, use them instead. That is covered in the next chapter of this guide.



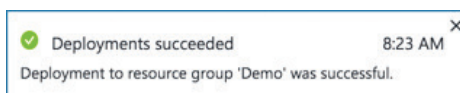
Review Validation settings and click OK.



Remote Application Server is using a bring-your-own-license (BOYL) model and only Azure Infrastructure Services will be charged. Parallels Remote Application Server licenses can be acquired at parallels.com.



The following message will be displayed once provisioning is completed:



To access the VM created, click on Connect using the following credentials:

Username	Password
ras	R@s2017!

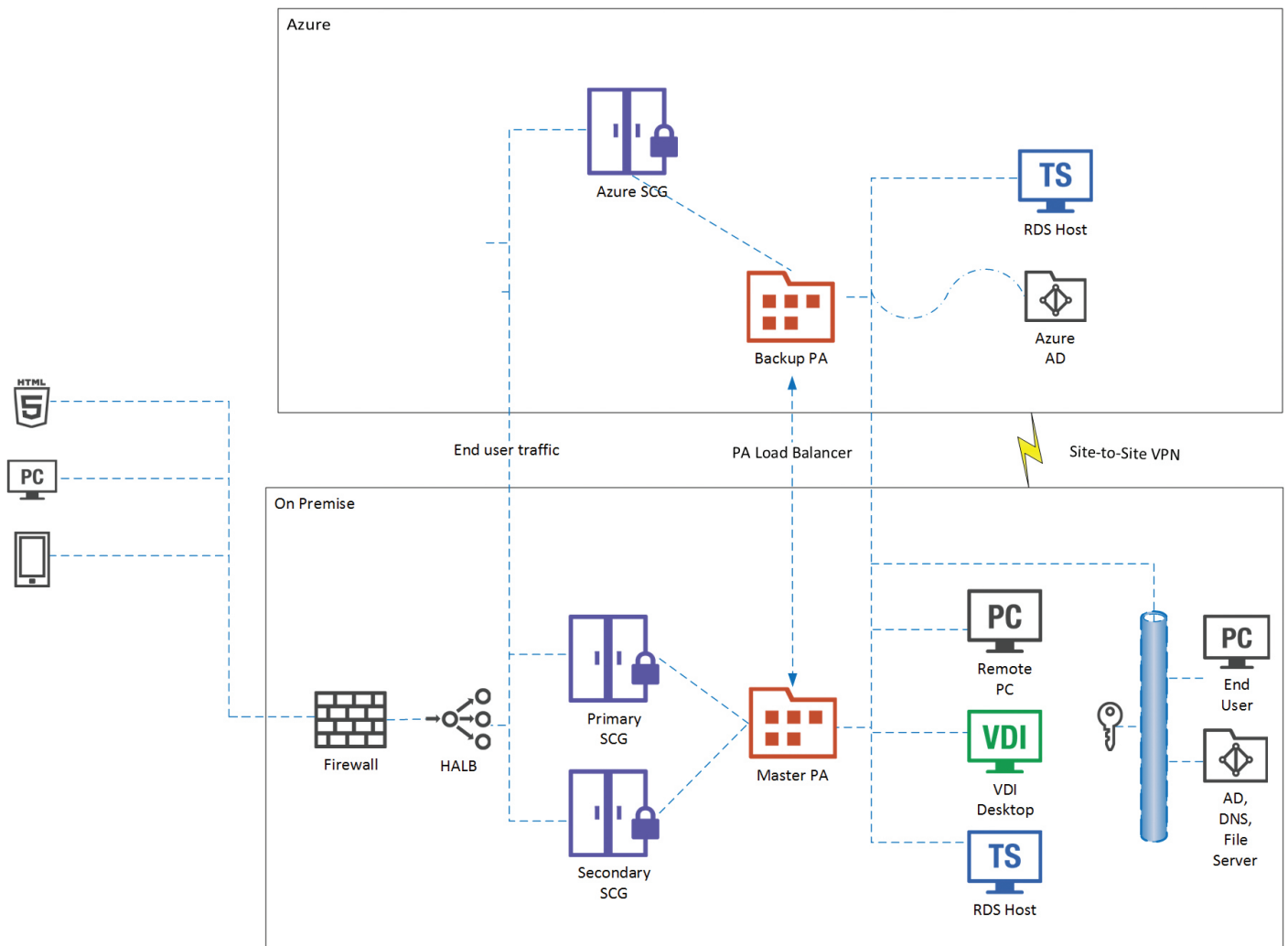
Hybrid Deployment (On Premise and Azure)

Leveraging Microsoft Azure capabilities, Remote Application Server supports the use case where backend services such as Active Directory® (AD) are either deployed on premise or using Azure. Therefore, Microsoft Office 365, Azure AD, and SQL server mixed with Federation Services are supported. Parallels Remote Application Server hosted on Azure consists of a small number of components:

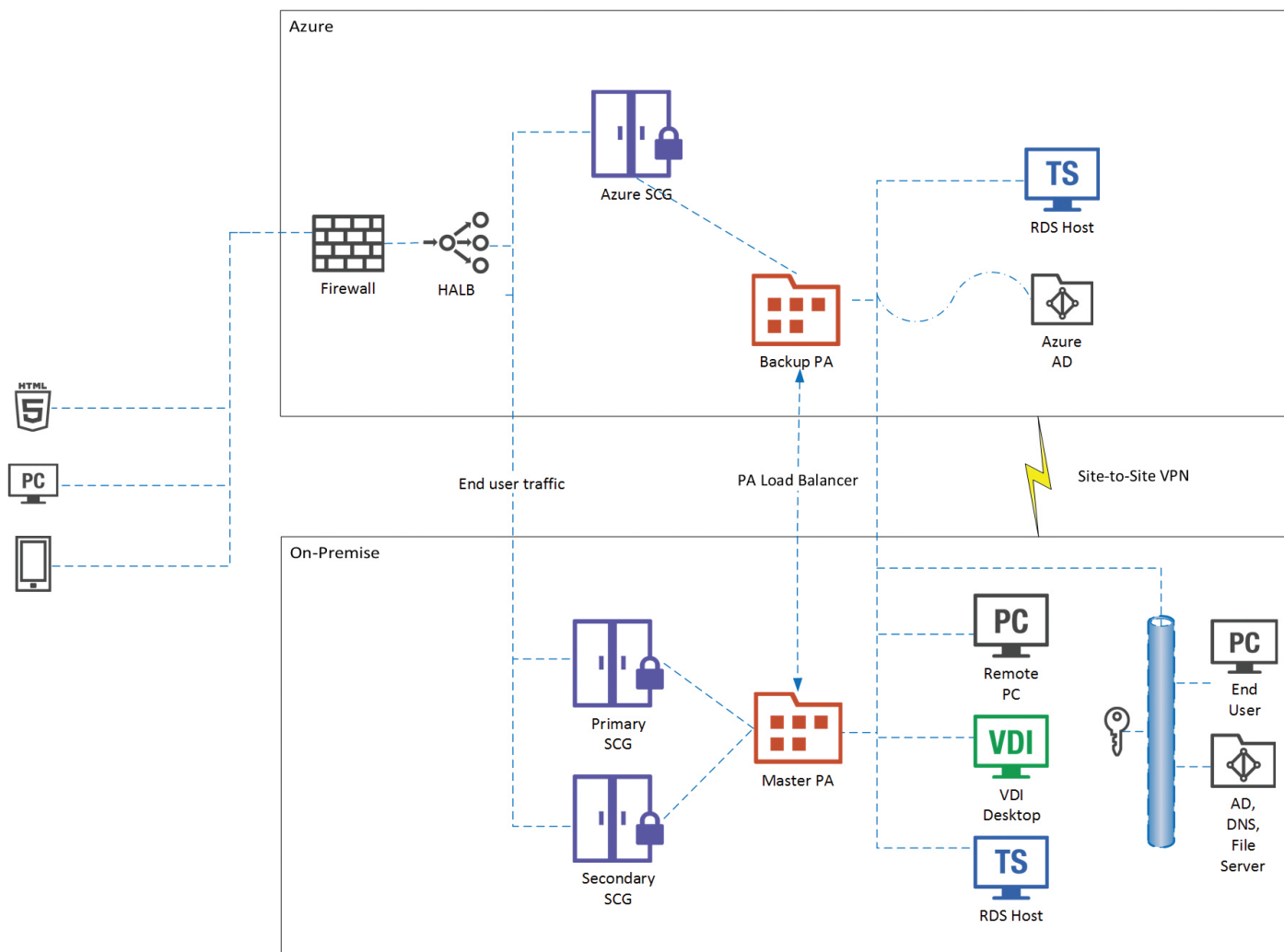
- Publishing Agent (Controller)
- Hosted Shared workers (Session Isolation)
- Server VDI Workers (VM/Server Isolation)
- Azure Active Directory Services or local AD Controller (for failover purposes)
- An Azure local SQL Server VM Instance (for reporting)
- Corporate network and Azure must be connected via Site-to-Site VPN.

NOTE: All roles are supported in Azure, and the final architecture may vary depending on how much Azure will be utilized. Additional information about Remote Application Server requirements can be found in the [Solution Guide](#).

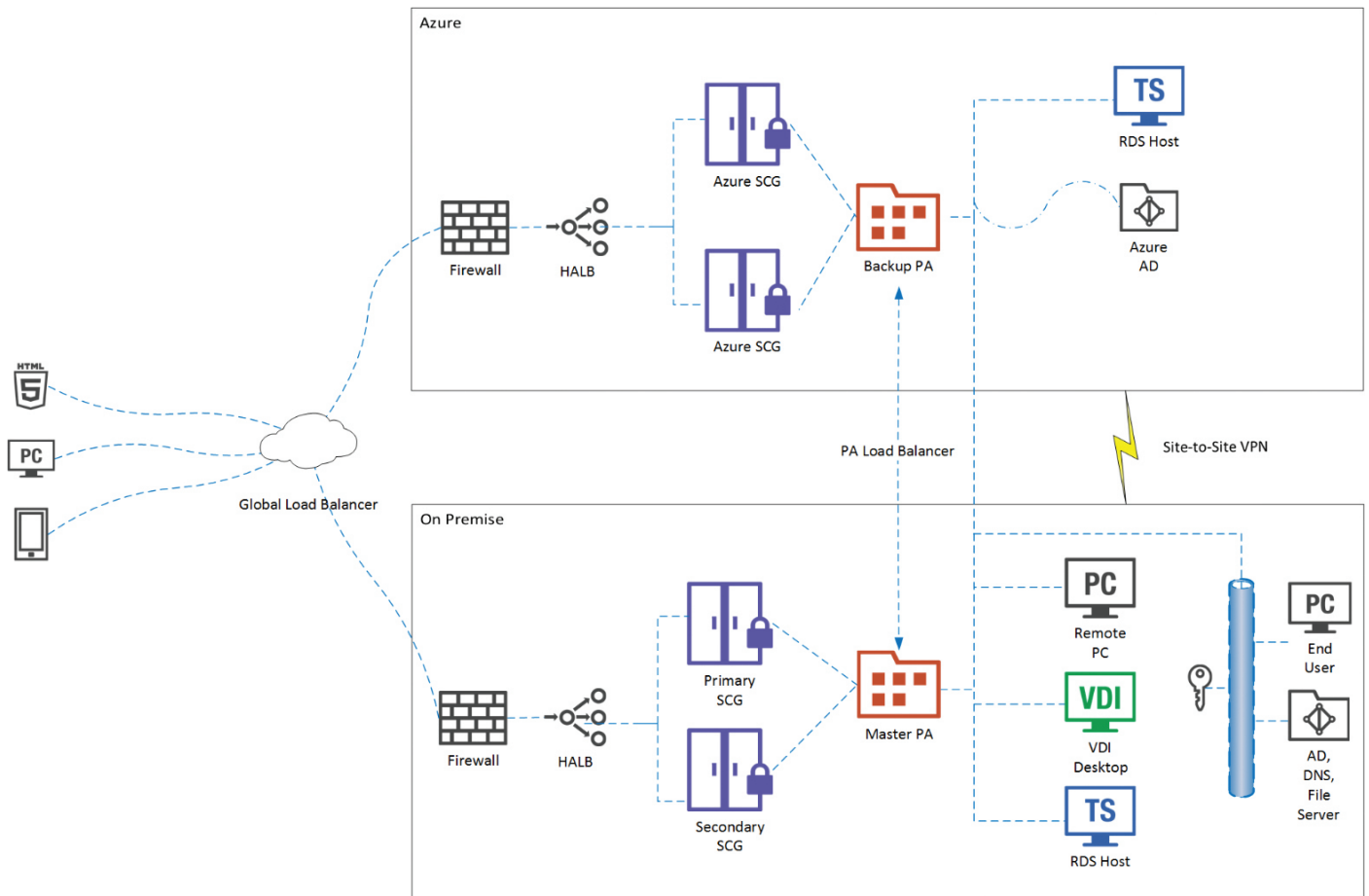
Endpoint Access Using On-premises




Endpoint Access Using Azure





Multisite





Server Components


	Master Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Windows Installer (standard installation)

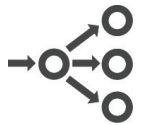
	Backup Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Push installation

	Primary Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Secondary Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Microsoft Remote Desktop Services Server	
	Component Installed	Installation Method
	Parallels Terminal Server Agent	Push installation

	Hypervisor Host with VDI Desktops	
	Component Installed	Installation Method
	Parallels VDI Agent Parallels Guest Agent	Push installation or Virtual Appliance

	High Availability and Load Balancing Virtual Appliance	
	Component Installed	Installation Method
	Ready-to-use virtual appliance	Virtual Appliance

For end user access, a couple of options should be considered:

- A. Existing customer end users can continue to use an existing URL (or gateway access) to leverage hybrid cloud deployment from an existing on-premises network and can also add additional failover gateways from Azure Internet inbound networks.
- B. New customer end users can receive inbound traffic through Azure and use on-premises deployments later on.

Virtual Machine Requirements in Azure

VM Role	OS	CPU	Memory	Disk Requirements
Publishing Agent	Windows Server® 2012, 2012 R2/2016	2 vCPUs	8 GB	40 GB
Gateway	Windows Server® 2012, 2012 R2/2016	2 vCPUs	8 GB	40 GB
Terminal Server/RDS/ Application Servers	Windows Server® 2012, 2012 R2/2016	4 vCPUs	16 GB	Depends on use case
High Availability Gateways	Debian	2 vCPUs	4 GB	10 GB

Virtual Machine Requirements On-premises

VM Role	OS	CPU	Memory	Disk Requirements
Publishing Agent	Windows Server 2003SP1, > Windows Server 2016	2 vCPUs	8 GB	40 GB
Gateway	Windows Server 2003SP1, > Windows Server 2016	2 vCPUs	8 GB	40 GB
Terminal Server/RDS/ Application Servers	Windows Server 2003SP1, > Windows Server 2016	4 vCPUs	16 GB	Depends on use case
High Availability Gateways	Debian	2 vCPUs	4 GB	10 GB

Office-to-office VPN

A cross-premises Azure virtual network allows your virtual machines in Azure to directly access resources on your on-premises network. For example, a DirSync server running on an Azure VM needs to query your on-premises domain controllers for changes to accounts and synchronize those changes with your Office 365® subscription.

Microsoft Azure provides [this knowledge base article](#) on how to connect an on-premises network to existing Azure infrastructure.

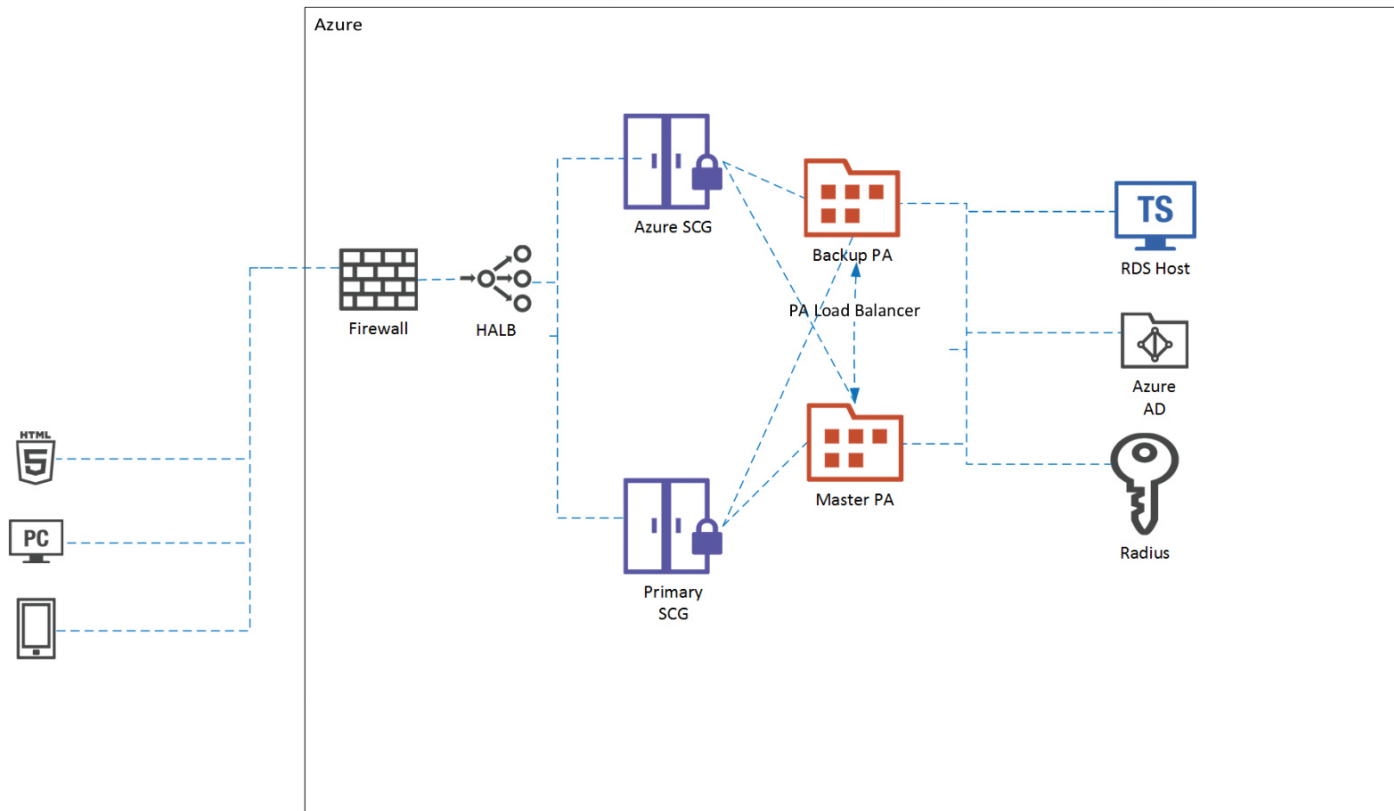
All-Azure Deployment

Leveraging Microsoft Azure capabilities, Remote Application Server supports the use case in which backend services such as Active Directory are deployed either on premise or using Azure. Therefore, Microsoft Office 365, Azure AD, and SQL server mixed with Federation Services are supported. Parallels Remote Application Server hosted on Azure consists of a small number of components:


- Publishing Agent (Controller)
- Hosted Shared Workers (Session Isolation)
- Server VDI Workers (VM/Server Isolation)
- Azure Active Directory Services
- An Azure Local SQL Server VM Instance (for reporting)


NOTE: All roles are supported in Azure, and the final architecture may vary depending on how much Azure will be utilized. Additional information about Remote Application Server requirements can be found in the [Solution Guide](#).


All in Azure





Server Components


	Master Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Windows Installer (standard installation)

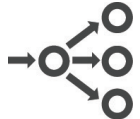
	Backup Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Push installation

	Primary Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Secondary Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Microsoft Remote Desktop Services Server	
	Component Installed	Installation Method
	Parallels Terminal Server Agent	Push installation

	Hypervisor Host with VDI Desktops	
	Component Installed	Installation Method
	Parallels VDI Agent Parallels Guest Agent	Push installation or Virtual Appliance

	High Availability and Load Balancing Virtual Appliance	
	Component Installed	Installation Method
	Ready-to-use virtual appliance	Virtual Appliance

Azure Marketplace Virtual Machine Templates

With the infrastructure requirements completed, Parallels Remote Application Server VMs can be deployed. There are two approaches:

- Virtual Machine Templates from Azure Marketplace (preferred method)
- Deploy Windows Server Datacenter instances in Azure, and push Remote Application Server components. If this method is used, we recommend following Remote Application Server documentation, [YouTube](#) videos, or the [Solution Guide](#).

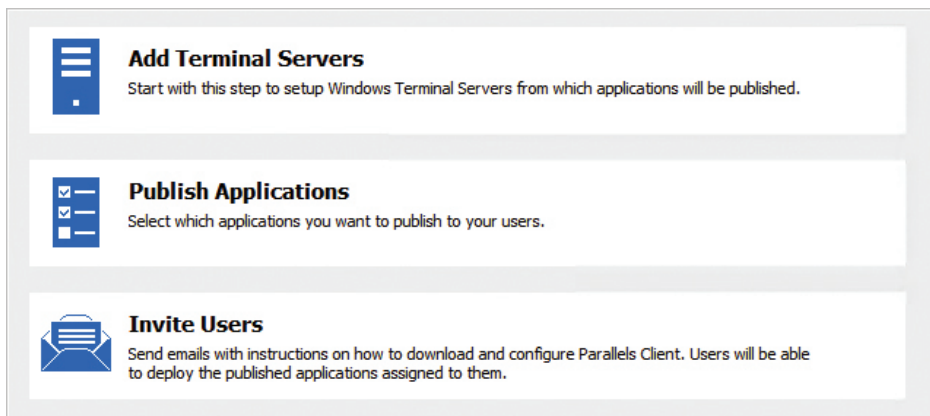
To deploy Remote Application Server using the trial image, go to [this section of the document](#).

Once selected VMs are deployed in Azure or an on-premises datacenter, you must connect them from the Remote Application Server Publishing Agent.

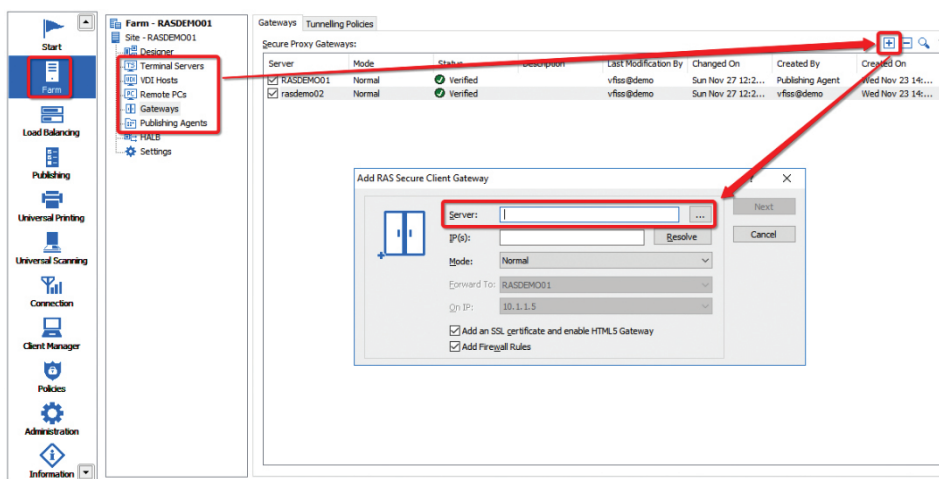
Configuring Parallels RAS Between Networks

When using a site-to-site VPN, both on-premises networks and Azure networks are integrated. The same steps are used to add Publishing Agents, Gateways, and Terminal Servers (RDS). If the Publishing Agent(s) is(are) already deployed on premise, start adding a new RAS from this server.

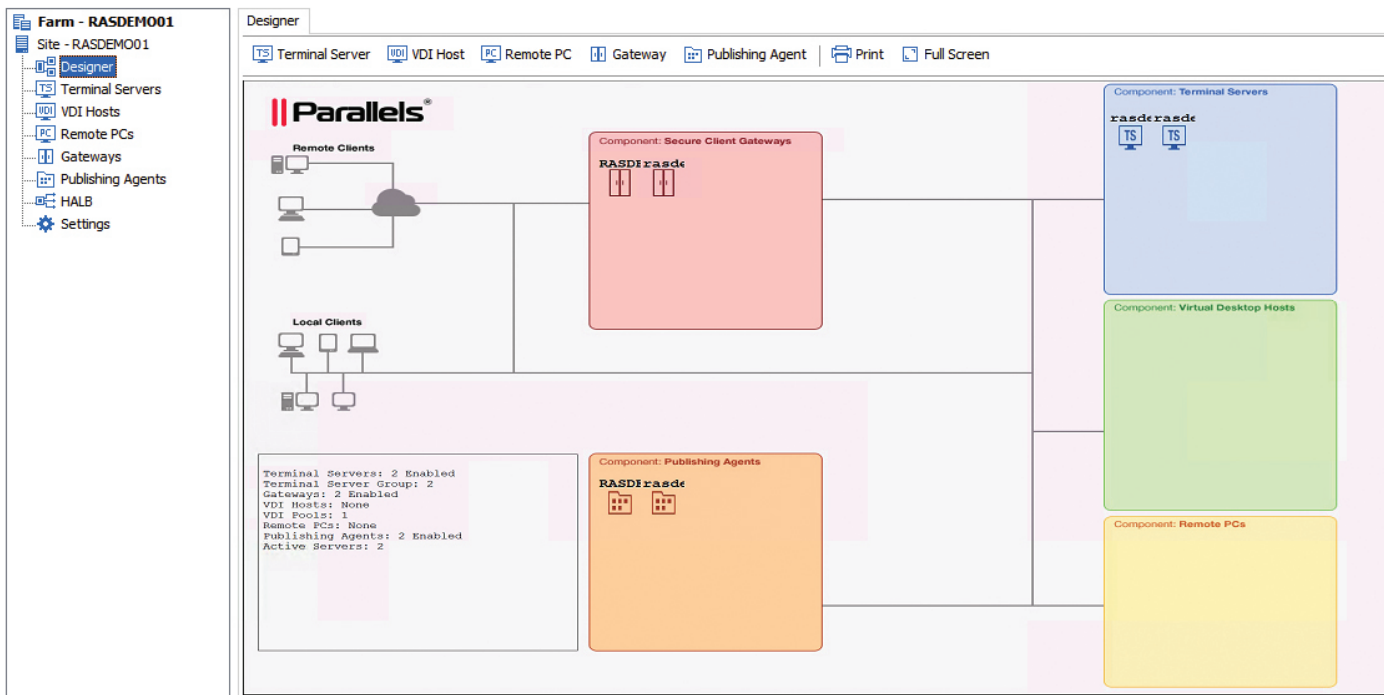
Remote Application Server provides wizards for deployment or configuration. These wizards should be started from the main console:



Once the initial deployment is completed, new roles can be added from the Farm menu:



Once the deployment is completed (or functional), the farm configuration will be displayed in the Farm > Designer Menu:

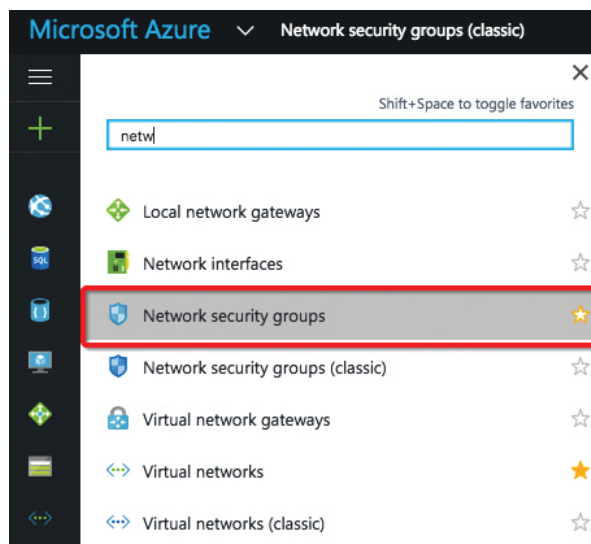


For additional information on how to deploy these roles, refer to the Parallels [Knowledge Base](#) or [Administration Guide](#), or consult the Parallels Partners or Sales teams.

Azure Network Configuration for Inbound Traffic

You can use a network security group (NSG) to control traffic to one or more VMs, role instances, network adapters (NICs), or subnets in your virtual network. An NSG contains access control rules that allow or deny traffic based on traffic direction, protocol, source address and port, and destination address and port. The rules of an NSG can be changed at any time, and changes are applied to all associated instances.

Network Security Groups for Internet Inbound Traffic



Create a new security group for RAS, such as “RAS Farm”, in the datacenter in which you have RAS deployed.

* Name
 ✓

* Subscription
 ▼

* Resource group ⓘ
 Create new Use existing
 ▼

* Location
 ▼

Create the following inbound rules:

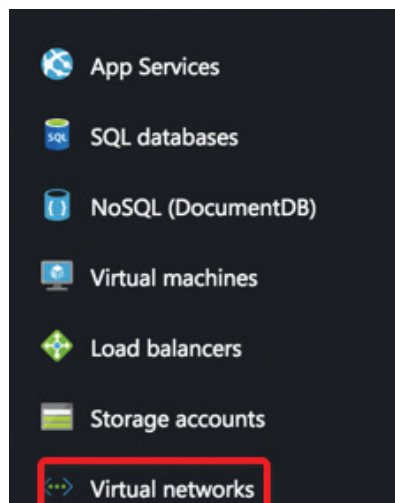
PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
100	Gateway_Redirect	Any	Any	HTTP (TCP/80)	Allow
110	Gateway_SSL	Any	Any	HTTPS (TCP/443)	Allow
120	Client_Management	Any	Any	Custom (TCP/20009)	Allow

Note: If RDP access is necessary, add another inbound rule for port 3389 and/or other ports used. It is not recommended to have the RDP port open.

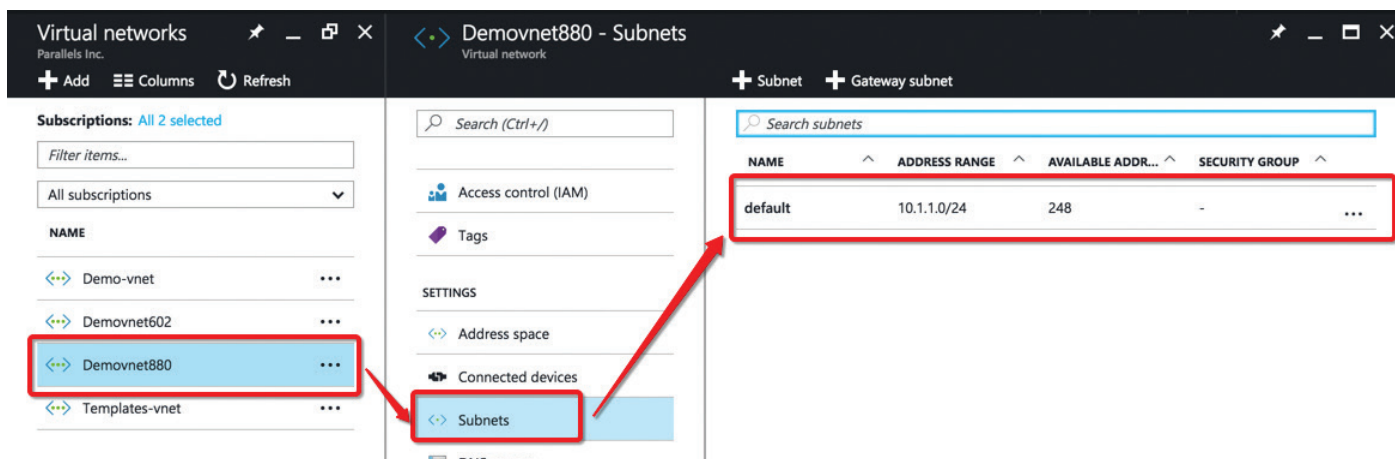
The new network security rule is not assigned to any VM or resources. The next step is to assign the new rule to Remote Application Server VMs.

Assign Firewall Rules to RAS Subnet and Virtual Machines

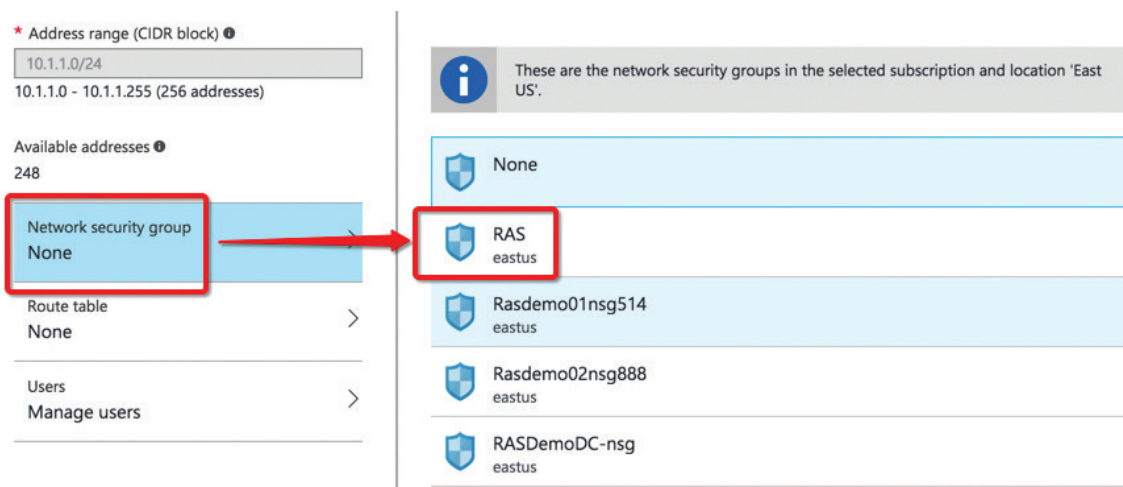
Virtual Network Configuration
 Go to Azure Menu > Virtual networks



Select the Virtual networks > Subnets > Security group:

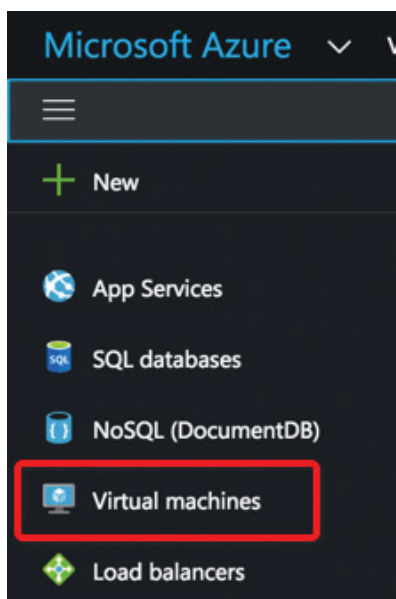


Replace your default security rule with "RAS":

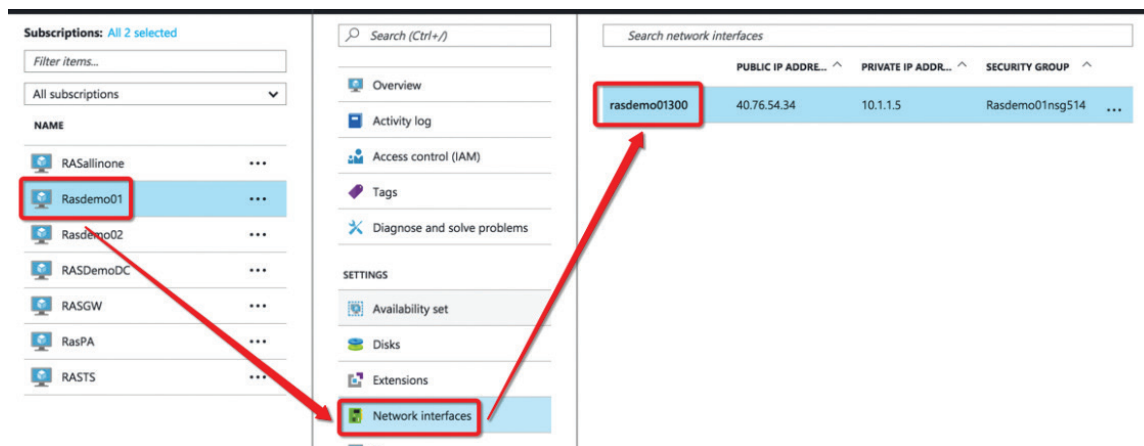


HALB or Gateway Virtual Machine Security Group Configuration

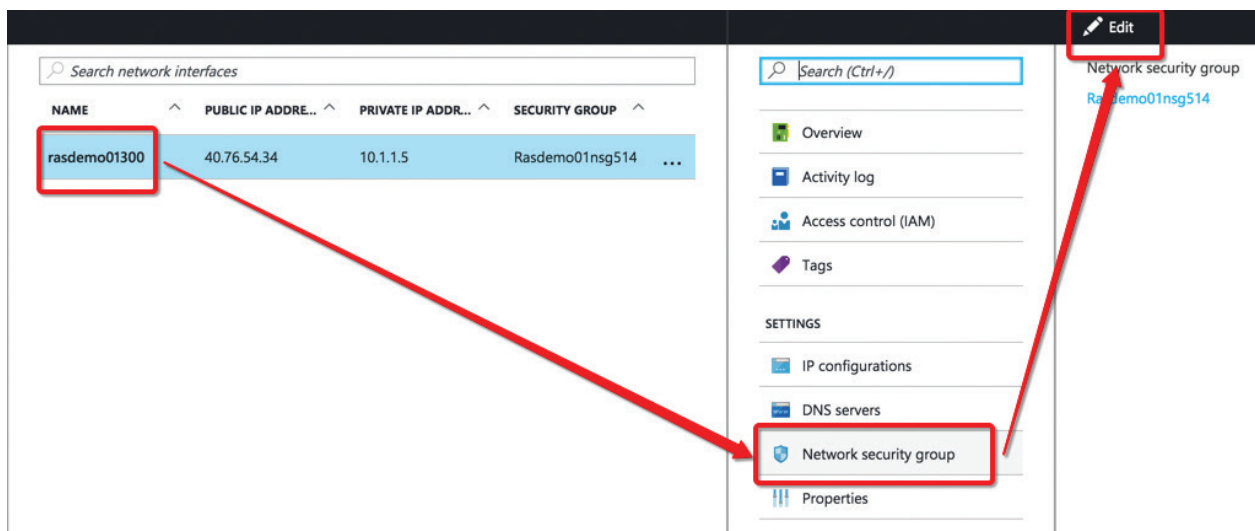
Go to Azure Menu > Virtual machines:



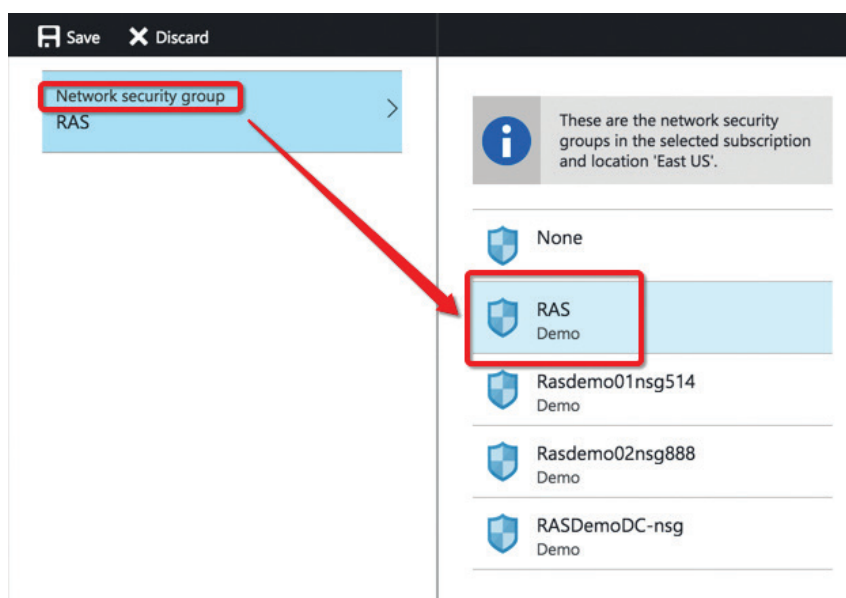
Select either HALB or Gateway Virtual Machine(s) > Network interfaces > Select network interface:



Select Network security group > Edit:



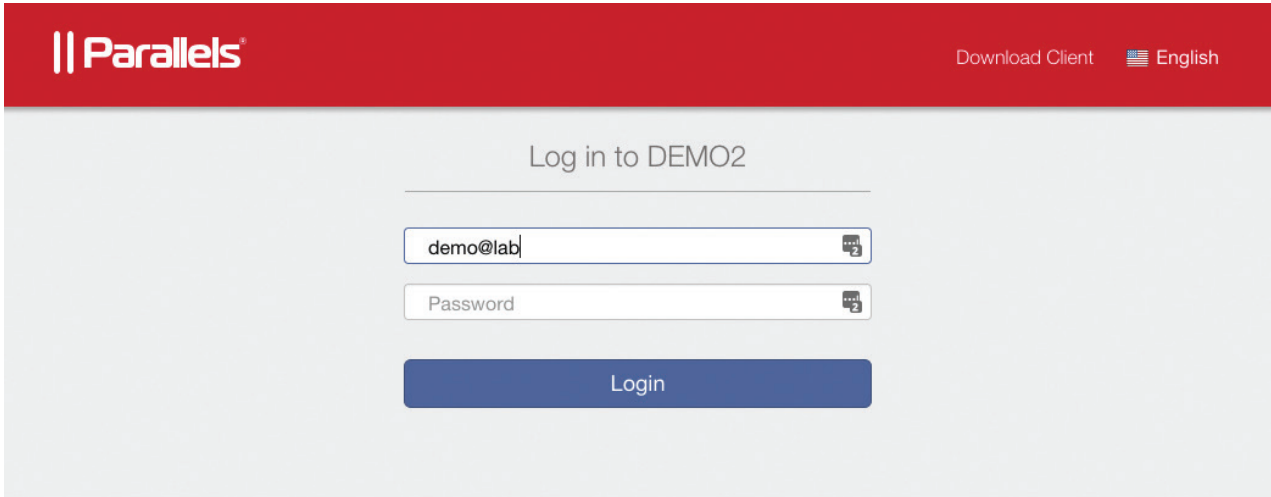
Change existing security group to "RAS":



Click Save and restart the VM.

Security Rules Test and Access Using Azure

From your local browser and VMs, up connect to https://your Azure IP_addr_or_hostname/RASHTML5Gateway.



If the page is not open, check routing rules in Parallels Desktop and/or pfsense. Another test option is to open Terminal and run a telnet to localhost on port 443. The result should be:

```
Last login: Thu Nov 24 15:06:42 on ttys000
[MBP-1276s-MacBook-Pro:~ Victor$ telnet 40.76.54.34 443
Trying 40.76.54.34...
Connected to 40.76.54.34.
Escape character is '^]'.
█
```

Best Practices

These optimizations are available in Remote Application Server VM templates in Azure Marketplace, and the following steps are for either custom VM or on-premises deployments.

Remote Desktop/Terminal Server Performance Settings

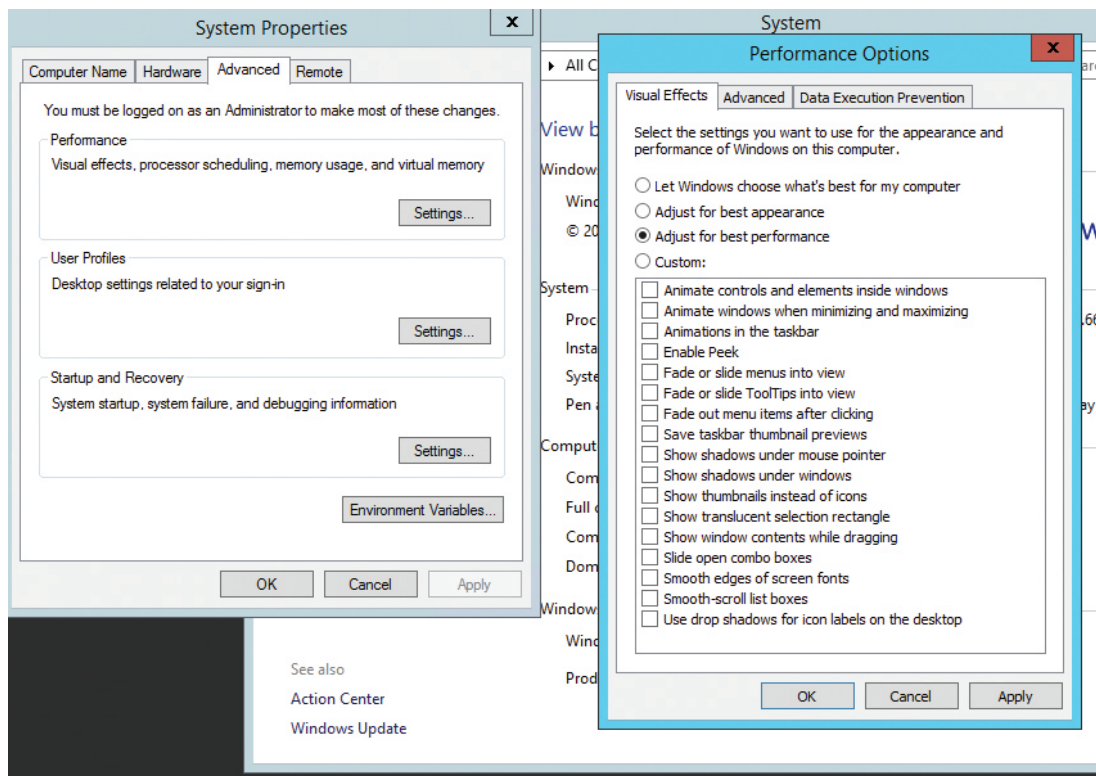
The default Windows performance settings are intended for general purpose servers. In order to maximize application or desktop hosting server performance, the default Windows performance settings should be adjusted on Windows Remote Desktop/Terminal Servers.

From the Control Panel, go to System and click on Advanced System Settings. Under the Advanced tab on the System Properties dialog box, click on Settings... under the Performance section.

Performance Options Settings

Under the Visual Effects tab from the Performance Options dialog box, change the setting to “Adjust for best performance.”

If a specific application has a custom setting recommendation, that approach should be used instead, but in general, “Adjust for best performance” will provide the best overall performance in a Parallels RAS environment.



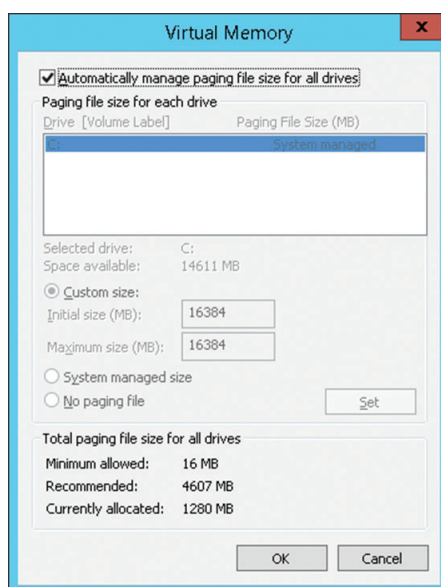
Windows Paging File Settings

Set the Windows paging file to twice the amount of RAM. For heavier workloads, a paging file of three times the amount of physical memory might be required.

Microsoft Windows page files start small by default and grow as necessary. However, as the system ramps up to intended capacity, dynamic page file growth can result in a fragmented page file, so it is best to set a fixed page file size up front.

Typically, page file settings are configured when the server is first installed. However, if the server has been in production for a while, Parallels recommends optimizing and defragmenting the drive prior to setting the following paging options.

In the example below, the server has 8 GB of RAM.



- A. Notice that Microsoft set the paging file size at 1280 MB, but the recommended size is 4607 MB.
- B. We are going to double the size, and it will use a new page file that will be in one location on the disk. The number should be 16384. 8 GB in a block of 8192 x2 = 16384.
- C. You will need enough free disk space in order to set this.

RemoteFX

RemoteFX[®] is a set of Microsoft Windows technologies that greatly enhances the end user visual and performance experience over the RDP protocol. It is available in Windows Server 2008 R2 SP1 and later. Windows 7 was the first client-side operating system to support RemoteFX. Both the client and server versions must be able to support RemoteFX in order for these enhancements to take effect.

Although RAS supports earlier versions of Windows Server, certain performance capabilities will not be available in older Windows operating systems. RemoteFX has been improved with subsequent releases of Windows. The best performance will always occur when running the latest server version of Microsoft Windows being accessed from the latest workstation version. Older versions of Windows can connect with newer versions (e.g., Windows XP to Windows 2012 R2 or Windows 10 to Windows 2003), and while this might be acceptable for certain workloads, RemoteFX capabilities will not be available.

Parallels RAS supports RemoteFX on the following clients: Parallels Windows Clients for Windows 7 SP1 and higher, Mac[®] clients, iOS, Android[™], Linux[®], and the ChromeApp for Chromebook[™].

Enable RemoteFX Using Group Policy

RemoteFX is enabled on Windows systems using Group Policy. If using local Group Policy settings, these settings must be completed on every Terminal Server/Remote PC/VDI Guest in the RAS farm. RemoteFX can also be configured centrally in Active Directory environments using Group Policy at the Domain level. This guide describes the process for enabling local Group Policy settings.

Hint: To edit local Group Policy, from the Windows Run command, type GPEDIT.MSC. Once the Group Policy settings are completed, run GPUPDATE /FORCE from the Run command to apply them.













RemoteFX settings for Server 2012 and 2012 R2

1. Enable and disable the following options with gpedit.msc on all terminal servers in your farm. This must also be completed on all virtual PC VDI systems that support RemoteFX
2. Under Local Computer Policy > Computer Configurations > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment, enable and disable the following:
 - a. Use Advanced RemoteFX graphics for RemoteApp
 - i. Enabled > Set to "Optimize to use less network bandwidth"
 - b. Configure compression for RemoteFX data
 - i. Enabled > Optimize to use less network bandwidth
 - c. Configure image quality for RemoteFX Adaptive Graphics
 - i. Enabled > Set to Medium
 - d. RemoteFX encoding for RemoteFX clients designed for Windows Server 2008 R2 SP1
 - i. Enabled
 - e. Configure RemoteFX Adaptive Graphics
 - i. Enabled > Let the system choose the experience for network conditions
 - f. Allow Desktop Composition for remote desktop sessions
 - i. Enabled

RemoteFX Settings for Windows Workstations Running Remote PC Agents and VDI Agents

1. RemoteFX Settings for Windows 7 SP1

- a. Enable and disable the following options with gpedit.msc virtual PC VDI systems that support RemoteFX:
Under Local Computer Policy, Computer Configurations, open Administrative Templates, Windows Components, Remote Desktop Services. Open Remote Desktop Session Host. Then open Remote Session Environment.
- b. Under Remote Session Environment, enable and disable the following:

Setting	State	Comment
 Limit maximum color depth	Not configured	No
 Enforce Removal of Remote Desktop Wallpaper	Not configured	No
 Configure RemoteFX	Enabled	No
 Limit maximum display resolution	Not configured	No
 Limit maximum number of monitors	Not configured	No
 Remove "Disconnect" option from Shut Down dialog	Not configured	No
 Remove Windows Security item from Start menu	Not configured	No
 Optimize visual experience when using RemoteFX	Enabled	No
 Set compression algorithm for RDP data	Enabled	No
 Optimize visual experience for Remote Desktop Services sessions	Enabled	No
 Start a program on connection	Not configured	No
 Always show desktop on connection	Not configured	No

- c. Configure RemoteFX
 - i. Enabled
- d. Optimize visual experience when using RemoteFX
 - i. Enabled
 - ii. Medium Default
- e. Set compression algorithm for RDP data
 - i. Enabled
 - ii. Optimize to use less network bandwidth
- f. Optimize visual experience for Remote Desktop Services sessions
 - i. Enabled
 - ii. Rich Multimedia
- g. Configure image quality for RemoteFX Adaptive Graphics (Image Quality set to Medium)
 - i. Enabled
 - ii. Configure RemoteFX Adaptive Graphics (Let the system choose experience for network conditions.)
- h. Use advanced RemoteFX graphics for RemoteApp
 - i. Enabled
- i. Configure compression for RemoteFX data
 - i. Enabled
 - ii. Optimize to use less network bandwidth
- j. Configure image quality for RemoteFX Adaptive Graphics.
 - i. Enabled
 - ii. Medium
- k. Configure RemoteFX Adaptive Graphics
 - i. Enabled (Let the system choose the experience for network conditions.)

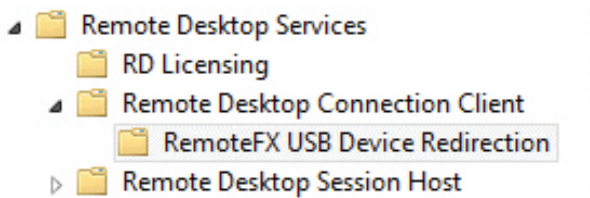
Remote FX USB Redirection, Audio Redirection, and Time Zone Redirection

RemoteFX USB Redirection

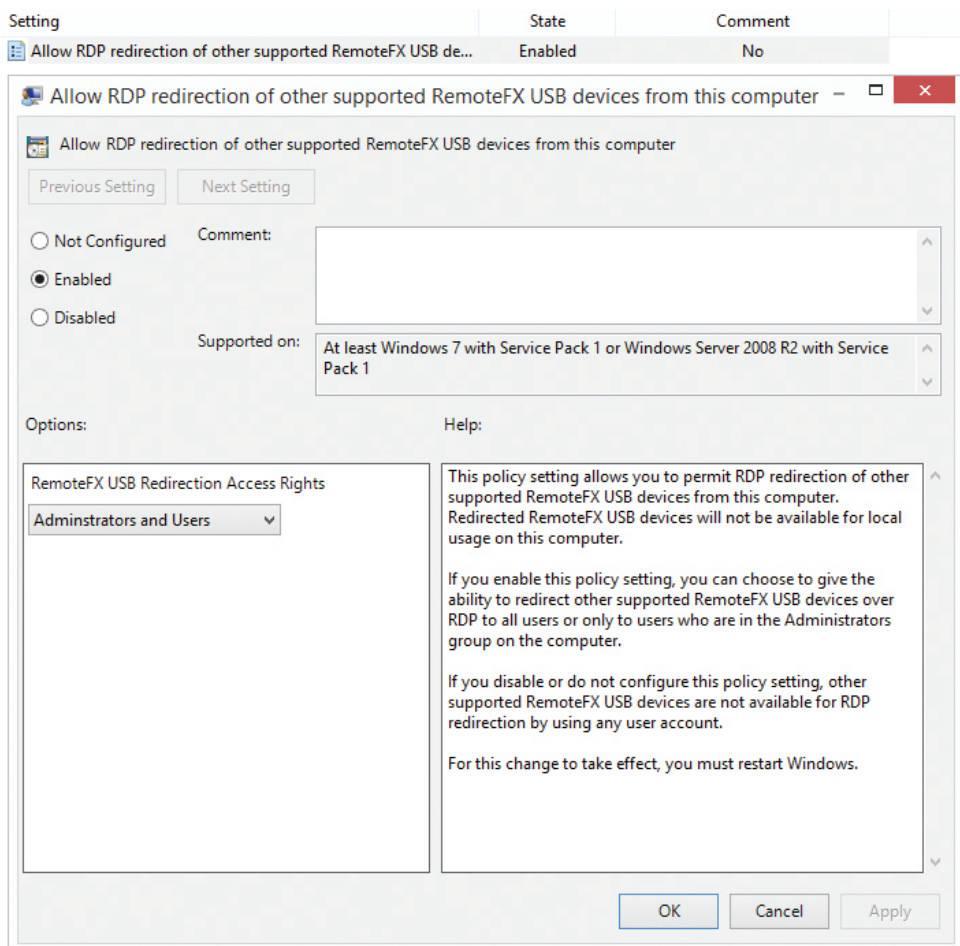
In order to get some Point of Sale / USB scanning devices to work properly with Windows 2008 R2 and higher, you must enable RemoteFX USB redirection.

Make sure that you set RemoteFX USB Redirection Access Rights to Administrators and Users. This is configured within Group Policy using GPEDIT.MSC:

Local Computer Policy > Computer Configurations > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Desktop Connection Client:



For additional information, see [this KB article](#) from Microsoft.



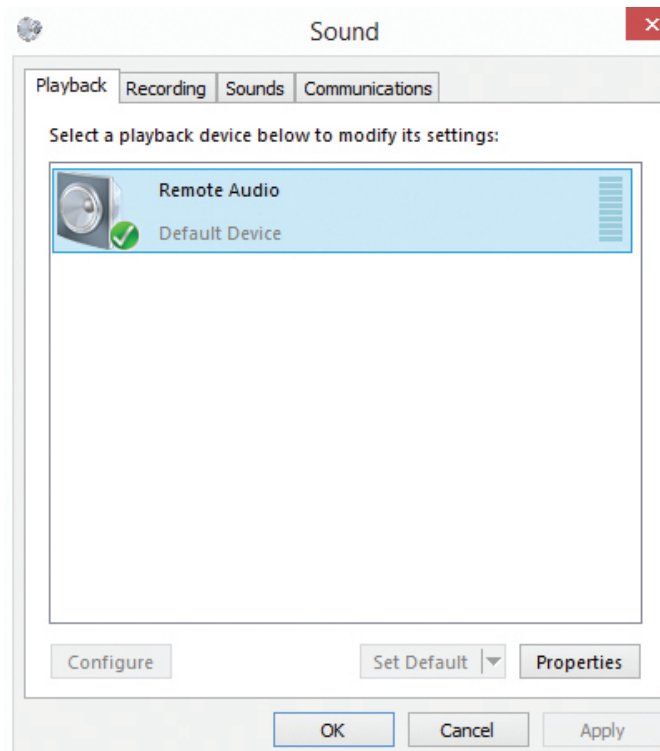
Enable Audio / Recording Redirection

In order to allow audio / recording redirection, first enable remote audio using the server's playback device, and then enable these functions using group policy via gpedit.msc.

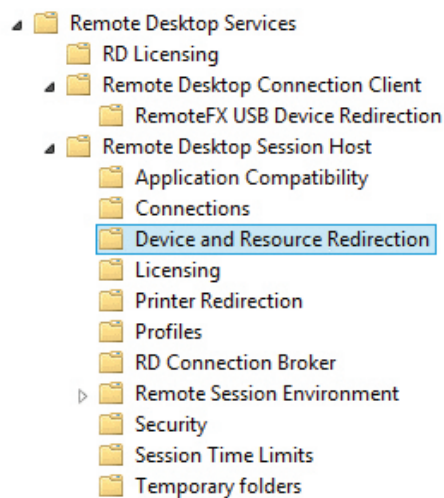
The Terminal Servers do not need a sound card to do this.

Enable the sound option on all Terminal Servers:











- a. Simply right-click the server's sound icon in the Windows system tray. You will then be prompted to enable remote audio.

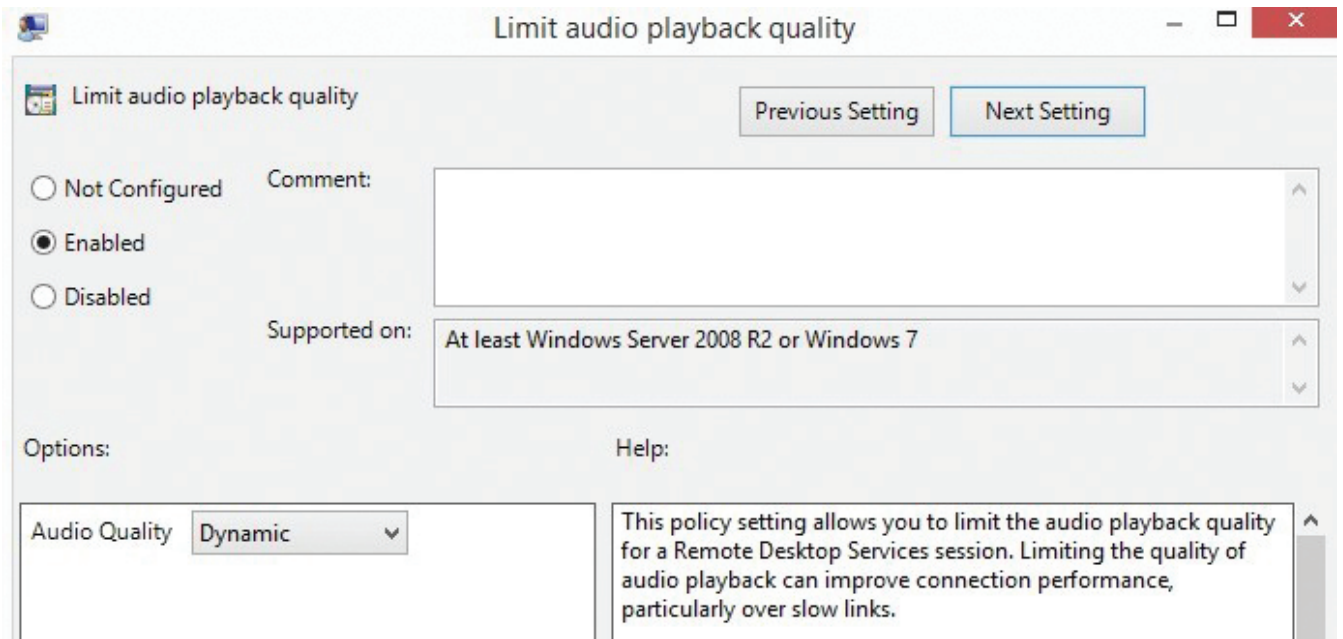


Run gpedit.msc and enable the sound redirection options. Local Computer Policy > Computer Configurations > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection:



- b. Allow audio and video playback redirection
 - i. Enabled
- c. Allow audio recording redirection
 - i. Enabled
- d. Limit audio playback quality
 - i. Enabled
 - ii. Set to "Dynamic"

Setting	State	Comment
 Allow audio and video playback redirection	Enabled	No
 Allow audio recording redirection	Enabled	No
 Limit audio playback quality	Enabled	No
 Do not allow Clipboard redirection	Not configured	No
 Do not allow COM port redirection	Not configured	No
 Do not allow drive redirection	Not configured	No
 Do not allow LPT port redirection	Not configured	No
 Do not allow supported Plug and Play device redirection	Not configured	No
 Do not allow smart card device redirection	Not configured	No
 Allow time zone redirection	Enabled	No



Time Zone Redirection

If you have users that login from different time zones, you may want to enable this setting. This setting will redirect the local time to the app, remote PC, or VM. Time Zone Redirection is configured in the same Group Policy location as

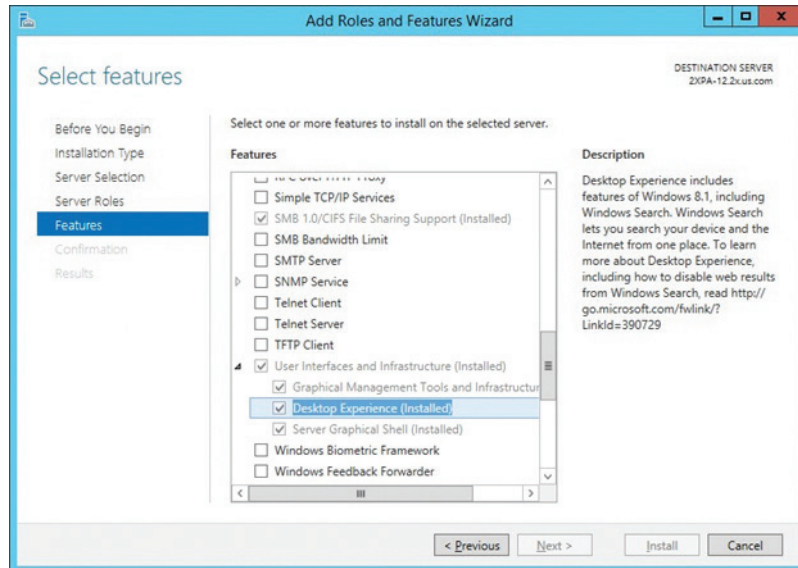
Audio Redirection:

Local Computer Policy > Computer Configurations > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Desktop Session Host > Device and Resource Redirection

Ensure That Desktop Experience Is Installed on All Terminal Servers

When a user connects to the Parallels RAS server, the desktop that exists on the RD Session Host server is reproduced, by default, in the remote session. To make the remote session look and feel more like the user's local Windows desktop experience, install the Desktop Experience feature on an RD Session Host server that is running Windows Server 2008 R2, Windows 2012, or Windows 2012 R2. This also makes the graphics look better using the Windows aero theme once the Desktop Experience feature is installed.

Desktop Experience is a feature that you can install from Server Manager.



Once enabled, you will notice the apps have better graphics, and if you publish a remote desktop for a user to use, it will look more like an actual desktop workstation. This will allow the user to personalize the remote desktop.

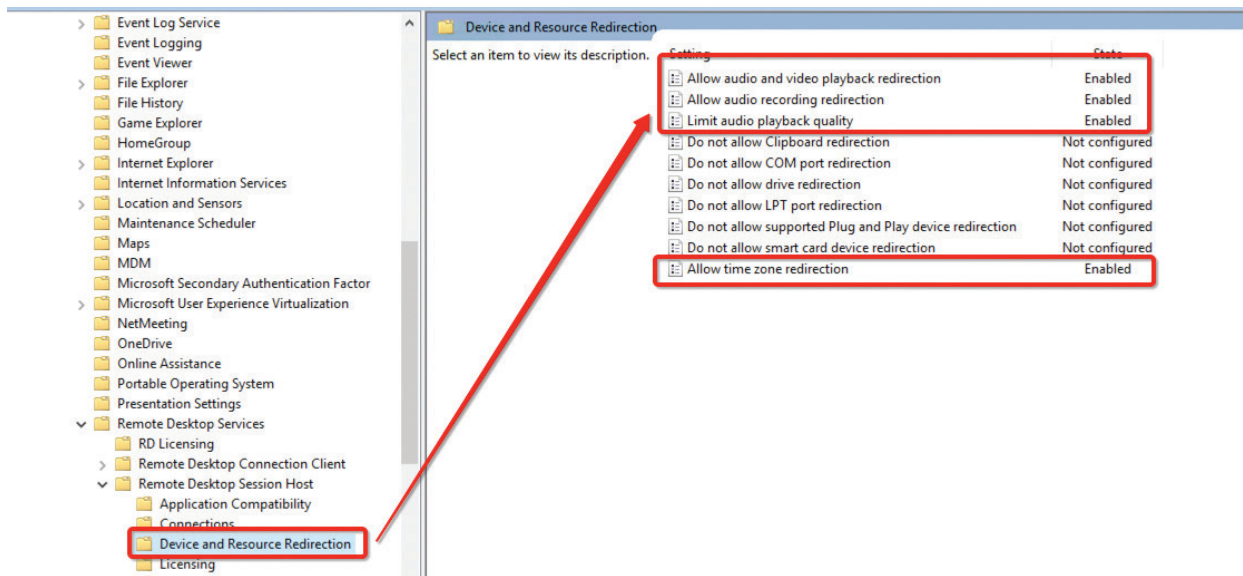
Windows Server 2016 Specific Group Policies

In Windows Server 2016, a few GPOs were moved, and Windows Server 2008 R2 backward compatibility was split in another folder's structure. Essentially, the GPOs folder is:

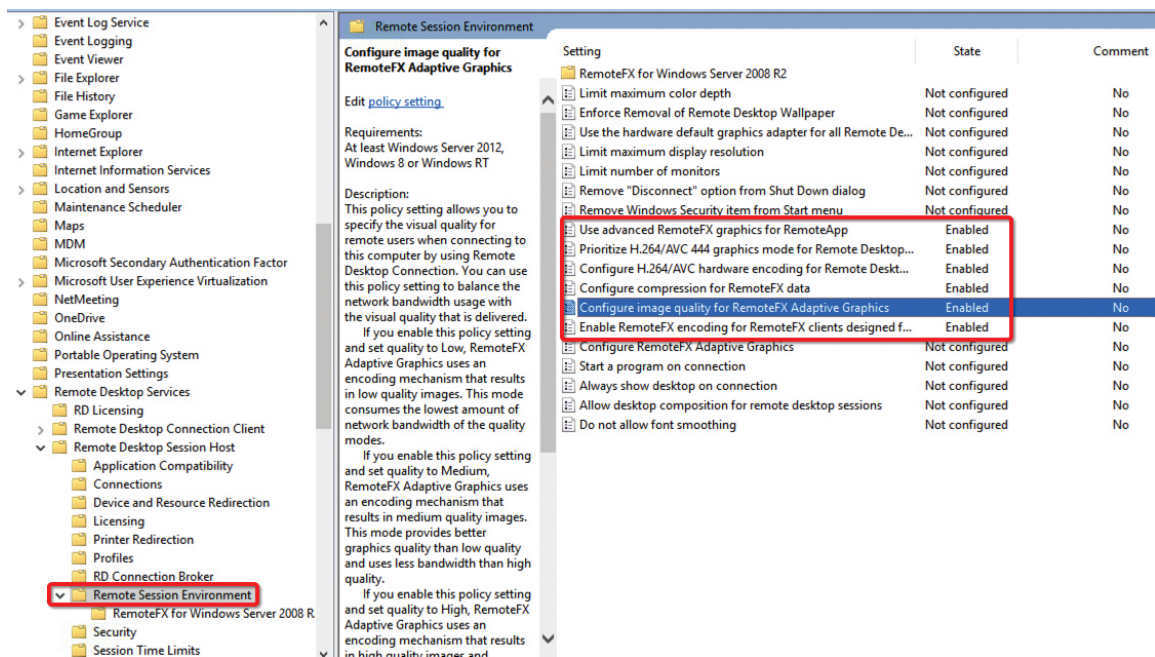
Local Computer Policy > Computer Configurations > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Desktop Session Host >

Make sure the following GPOs marked as "Not Configured" are changed to Enabled:

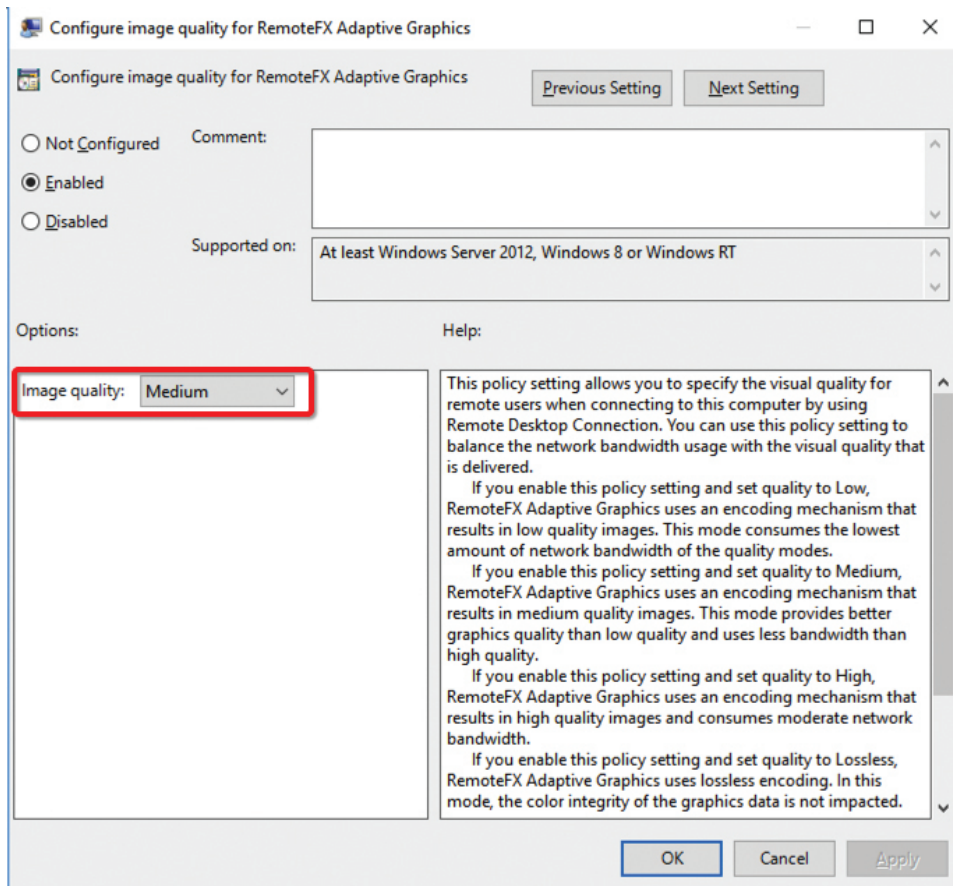
Device and Resource Redirection



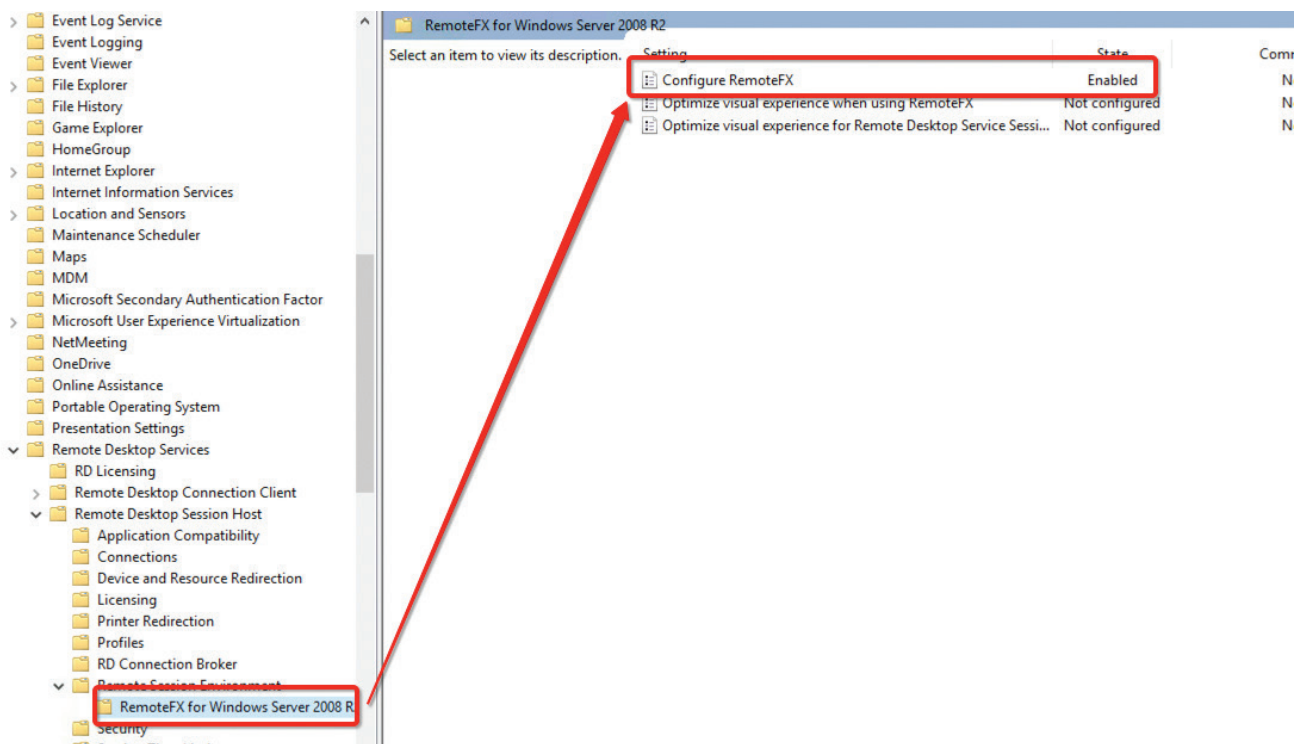
Remote Session Environment (H.264, RemoteFX, Adaptive Acceleration)

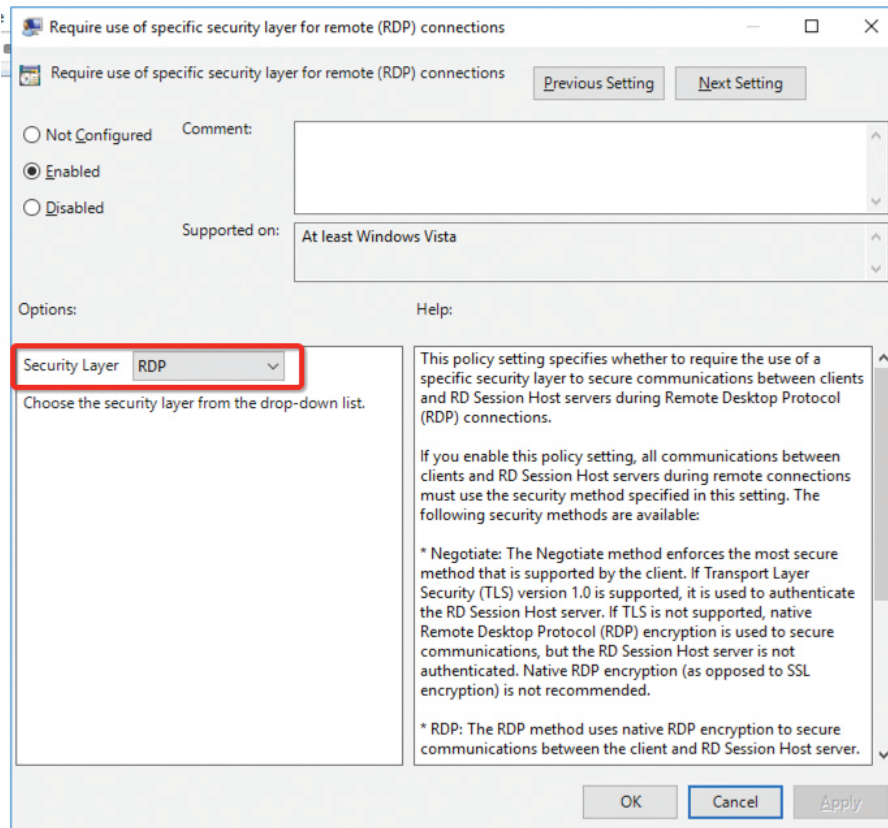


Set "Configure image quality for RemoteFX Adaptive Graphics" to Medium:

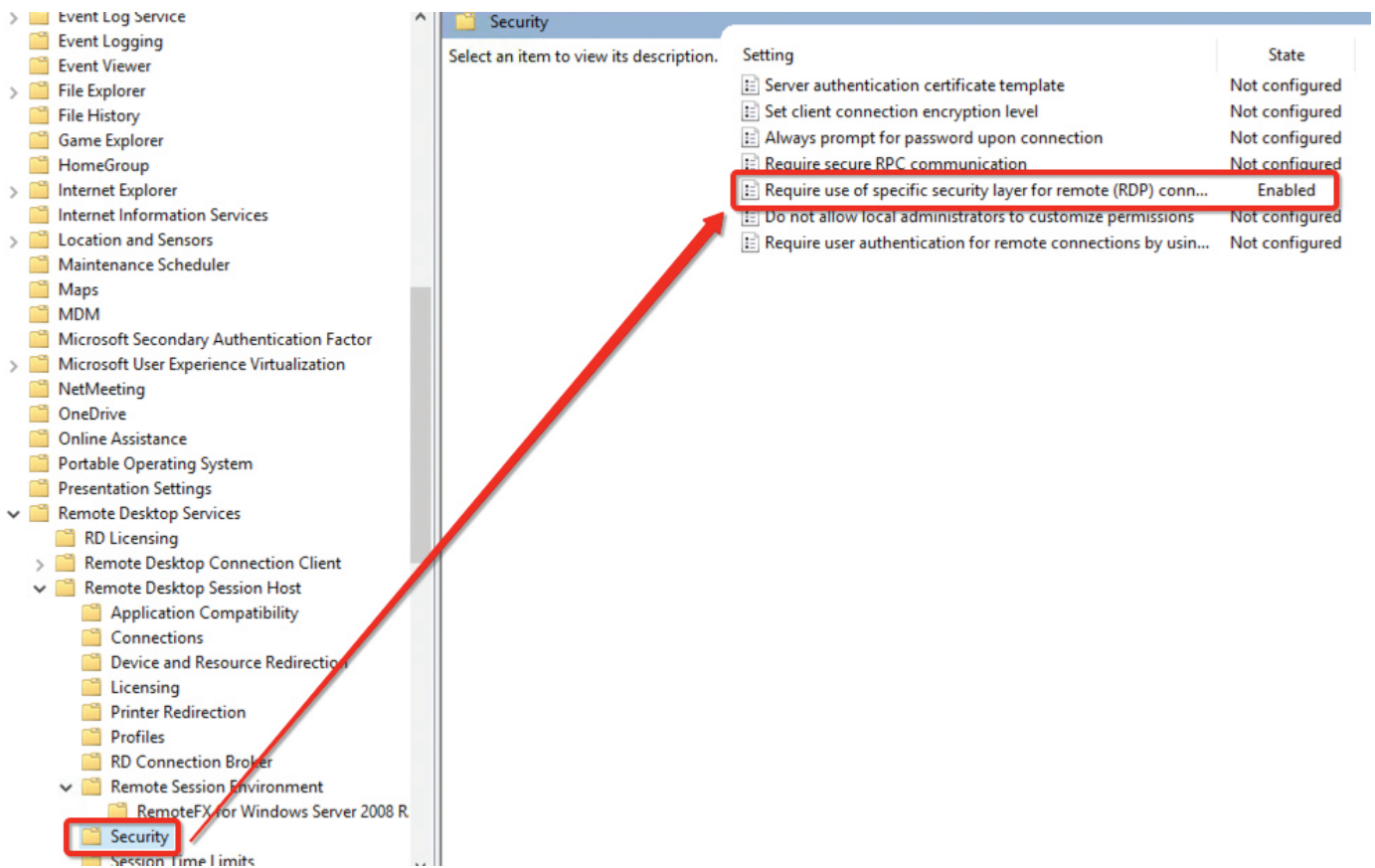


Windows 2008 R2 RemoteFX Compatibility



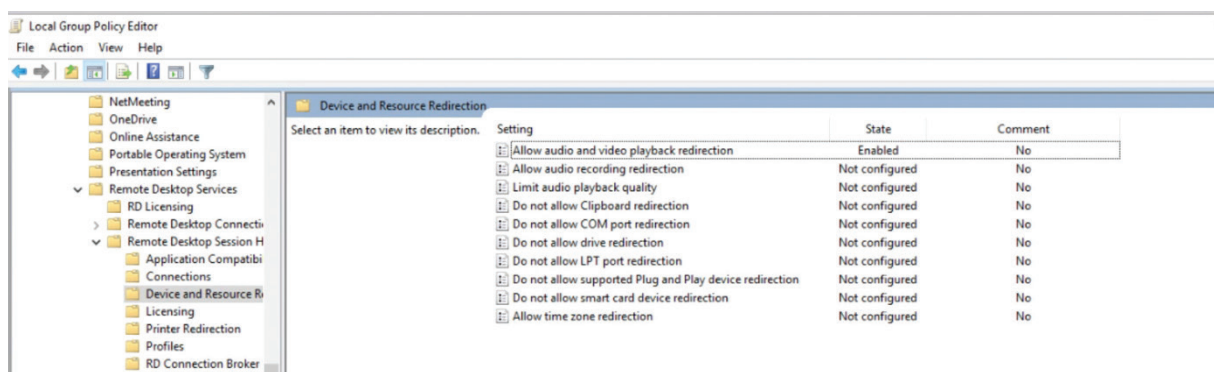


RDP Security



Skype for Business in Azure

To allow audio and video playback when connecting to a computer running Windows Server 2008 R2, you must enable the **Allow audio and video playback redirection** Group Policy setting. The Allow audio and video playback redirection Group Policy setting is located in **Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection** and can be configured by using either Local Group Policy Editor or the Group Policy Management Console (GPMC).



Windows Licenses and RDS Client Access Licenses (CALs)

Parallels does not resell Microsoft licenses, and Windows licenses and RDS licenses are running in trial mode. It is highly recommended to replace these licenses as soon as possible. In a typical deployment, the following licenses are required:

Description	Azure	On Premise
Microsoft Windows Server CAL	Included in Azure deployment	License needs to be added to the final cost
Remote Desktop Server CAL	Not included	Not included
Microsoft SPLA	N/A	Enterprise License count
Parallels Remote Application Server	Not included	Not included
Microsoft SQL Server Express (advanced features)	FREE	FREE

References

- <https://portal.azure.com/#blade/HubsExtension/Resources/resourceType/Microsoft.Network%2FNetworkSecurityGroups>
- docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-create-nsg-arm-portal
- parallels.com/products/ras/resources/