White Paper | Parallels Remote Application Server

Azure Reference Architecture & Design Guide

v.1.2

Contents

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

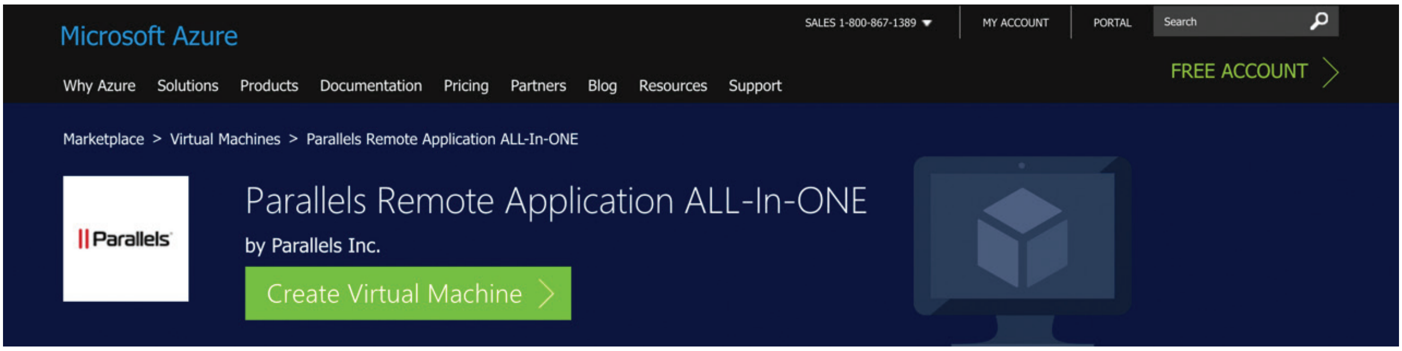
Your business plans to leverage Microsoft and Parallels Remote Application Server to deliver a hosted desktop solution for its accounting department. The solution will provide value to the department by enabling access to Windows desktops and applications from any device. The value of this solution for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

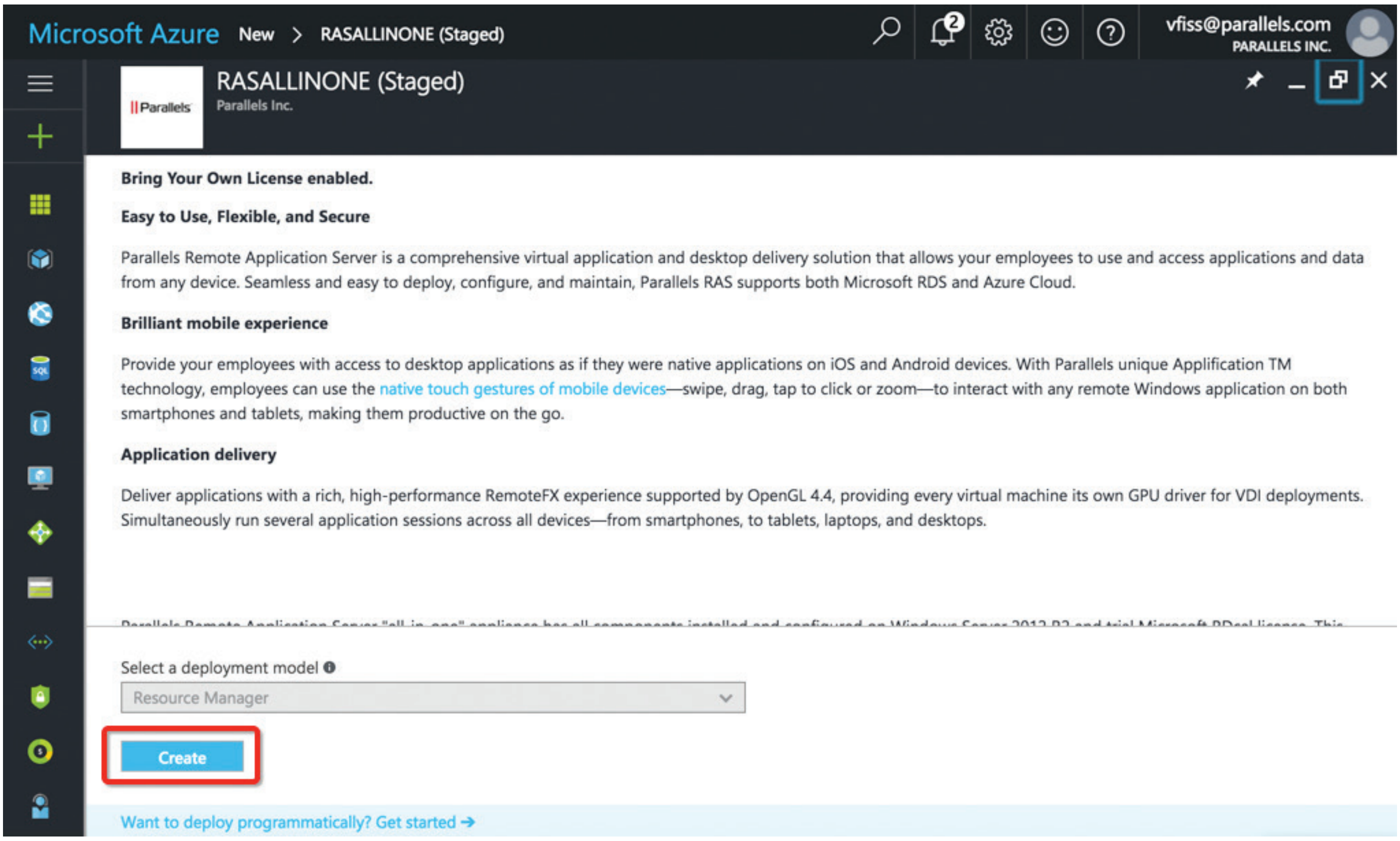
Business Objectives

- 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.





RASALLINONE (Staged)
Parallels Inc.

Bring Your Own License enabled.

Easy to Use, Flexible, and Secure

Parallels Remote Application Server is a comprehensive virtual application and desktop delivery solution that allows your employees to use and access applications and data from any device. Seamless and easy to deploy, configure, and maintain, Parallels RAS supports both Microsoft RDS and Azure Cloud.

Brilliant mobile experience

Provide your employees with access to desktop applications as if they were native applications on iOS and Android devices. With Parallels unique Application TM technology, employees can use the native touch gestures of mobile devices—swipe, drag, tap to click or zoom—to interact with any remote Windows application on both smartphones and tablets, making them productive on the go.

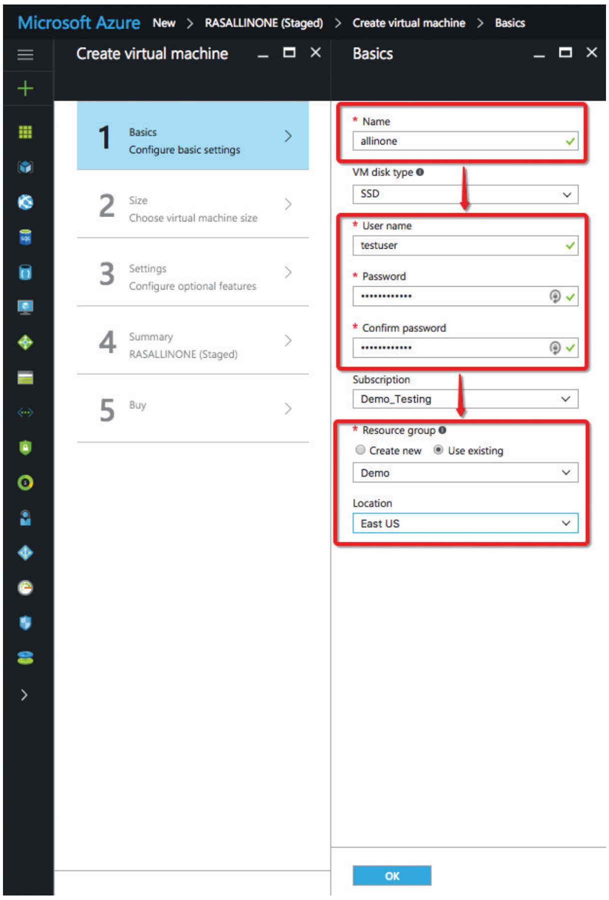
Application delivery

Deliver applications with a rich, high-performance RemoteFX experience supported by OpenGL 4.4, providing every virtual machine its own GPU driver for VDI deployments. Simultaneously run several application sessions across all devices—from smartphones, to tablets, laptops, and desktops.

Parallels Remote Application Server "all-in-one" appliance has all components installed and configured on Windows Server 2012 R2 and trial Microsoft RDcal license. This

Select a deployment model: Resource Manager

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.


Microsoft Azure New > RASALLINONE (Staged) > Create virtual machine > Basics
Create virtual machine
Basics

1 Basics
Configure basic settings

2 Size
Choose virtual machine size

3 Settings
Configure optional features

4 Summary
RASALLINONE (Staged)

5 Buy

* Name: allinone

VM disk type: SSD

* User name: testuser

* Password: ••••••••••••

* Confirm password: ••••••••••••

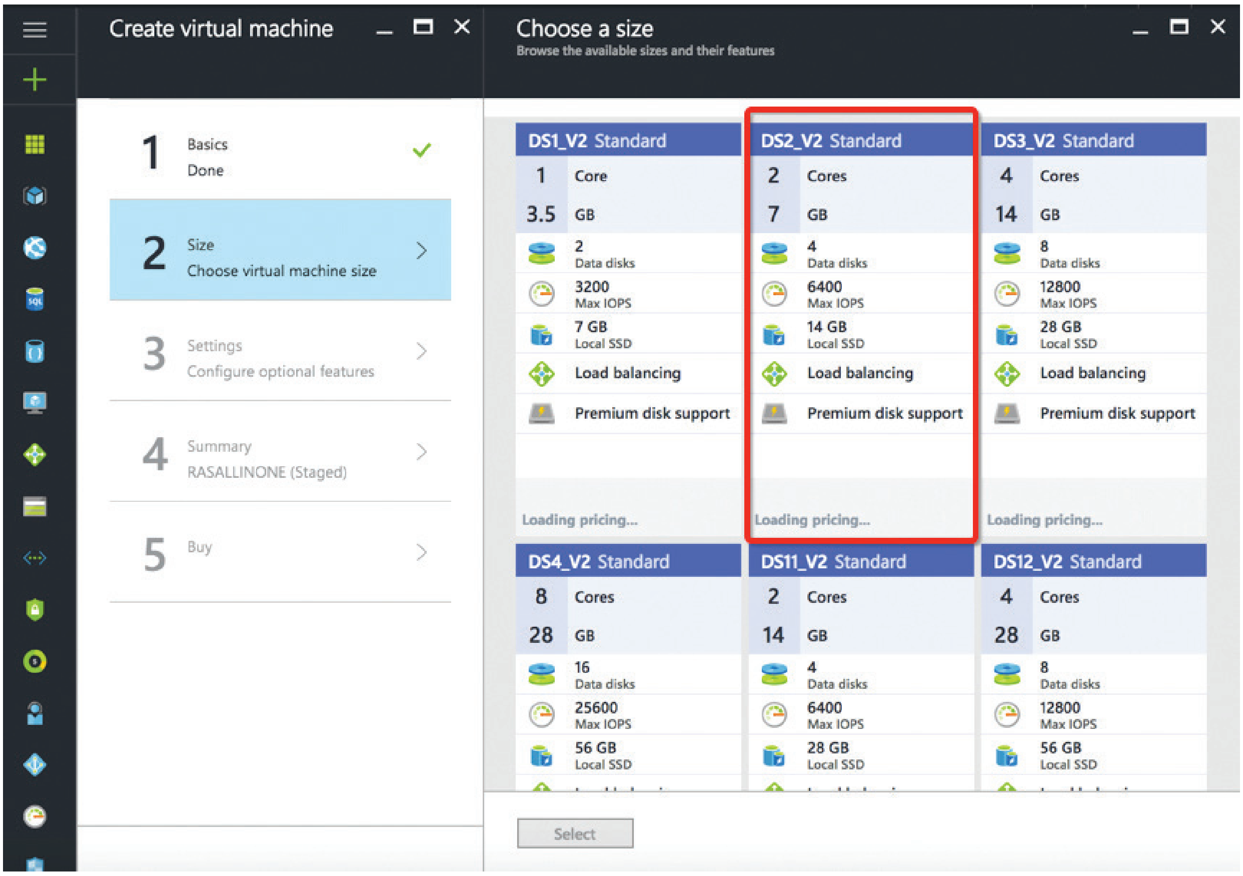
Subscription: Demo_Testing

* Resource group: ○ Create new ● Use existing

Demo

Location: East US

Select Azure Service Offering. We recommend DS2_V2 for POCs:



Create virtual machine

1 Basics
Done ✓

2 Size
Choose virtual machine size

3 Settings
Configure optional features

4 Summary
RASALLINONE (Staged)

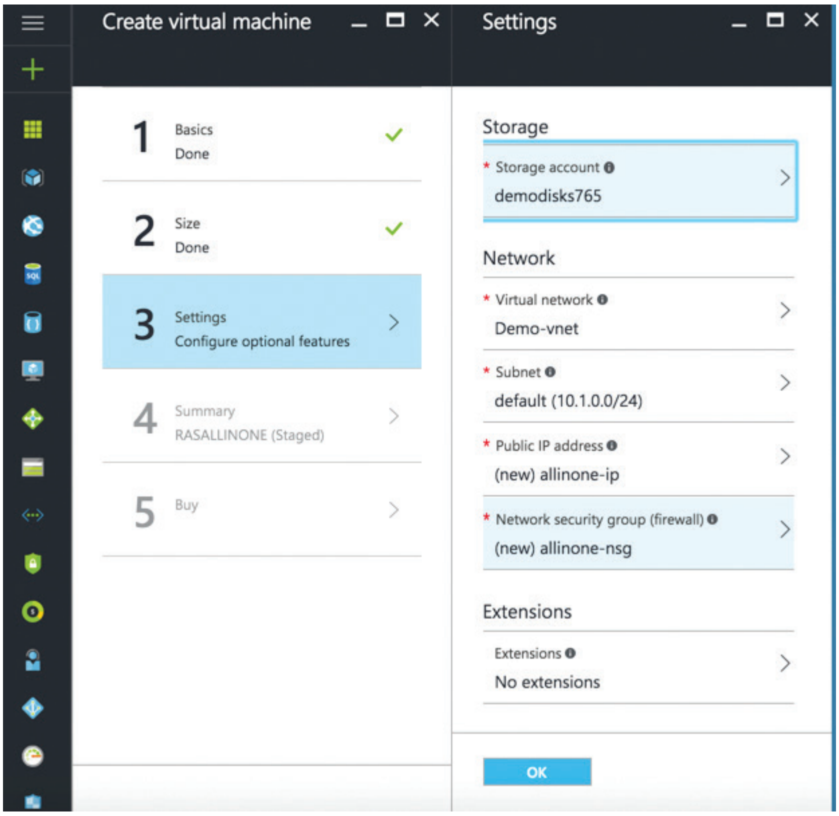
5 Buy

Choose a size
Browse the available sizes and their features

DS1_V2 Standard	DS2_V2 Standard	DS3_V2 Standard
1 Core	2 Cores	4 Cores
3.5 GB	7 GB	14 GB
2 Data disks	4 Data disks	8 Data disks
3200 Max IOPS	6400 Max IOPS	12800 Max IOPS
7 GB Local SSD	14 GB Local SSD	28 GB Local SSD
Load balancing	Load balancing	Load balancing
Premium disk support	Premium disk support	Premium disk support
Loading pricing...	Loading pricing...	Loading pricing...

DS4_V2 Standard	DS11_V2 Standard	DS12_V2 Standard
8 Cores	2 Cores	4 Cores
28 GB	14 GB	28 GB
16 Data disks	4 Data disks	8 Data disks
25600 Max IOPS	6400 Max IOPS	12800 Max IOPS
56 GB Local SSD	28 GB Local SSD	56 GB Local SSD

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.



Create virtual machine

1 Basics
Done ✓

2 Size
Done ✓

3 Settings
Configure optional features

4 Summary
RASALLINONE (Staged)

5 Buy

Settings

Storage

* Storage account
demodisks765

Network

* Virtual network
Demo-vnet

* Subnet
default (10.1.0.0/24)

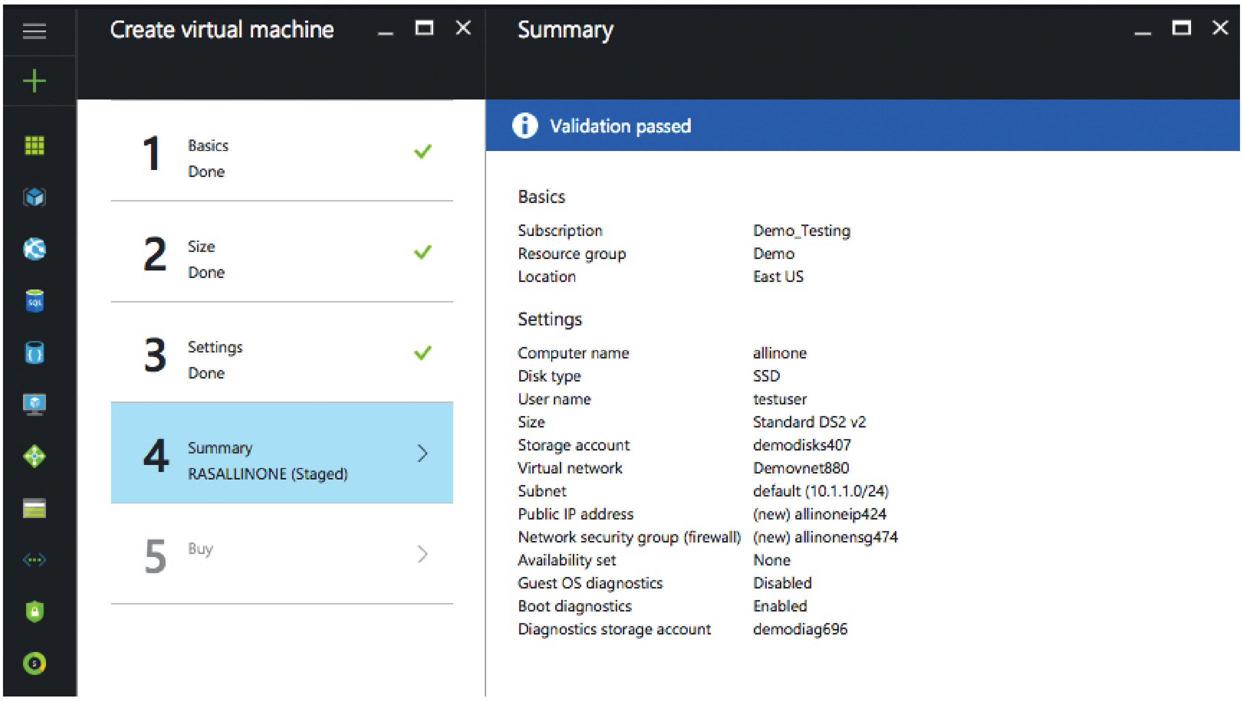
* Public IP address
(new) allinone-ip

* Network security group (firewall)
(new) allinone-nsg

Extensions

Extensions
No extensions

Review Validation settings and click OK.



Summary

Validation passed

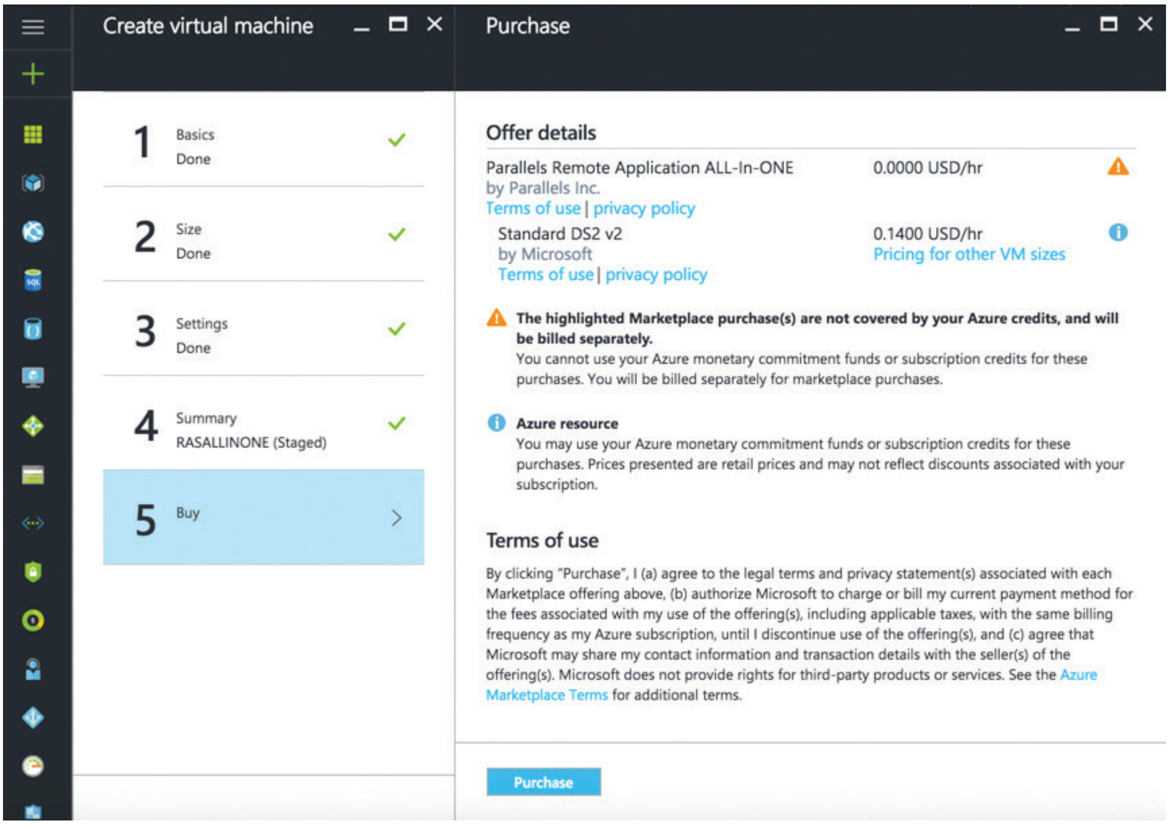
Basics

Subscription	Demo_Testing
Resource group	Demo
Location	East US

Settings

Computer name	allinone
Disk type	SSD
User name	testuser
Size	Standard DS2 v2
Storage account	demodisks407
Virtual network	Demovnet880
Subnet	default (10.1.1.0/24)
Public IP address	(new) allinoneip424
Network security group (firewall)	(new) allinonensg474
Availability set	None
Guest OS diagnostics	Disabled
Boot diagnostics	Enabled
Diagnostics storage account	demodiag696

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.



Purchase

Offer details

Parallels Remote Application ALL-In-ONE by Parallels Inc. Terms of use | privacy policy	0.0000 USD/hr
Standard DS2 v2 by Microsoft Terms of use | privacy policy	0.1400 USD/hr Pricing for other VM sizes

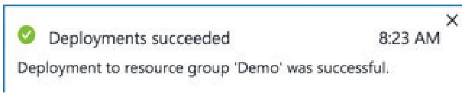
The highlighted Marketplace purchase(s) are not covered by your Azure credits, and will be billed separately. You cannot use your Azure monetary commitment funds or subscription credits for these purchases. You will be billed separately for marketplace purchases.

Azure resource You may use your Azure monetary commitment funds or subscription credits for these purchases. Prices presented are retail prices and may not reflect discounts associated with your subscription.

Terms of use

By clicking "Purchase", I (a) agree to the legal terms and privacy statement(s) associated with each Marketplace offering above, (b) authorize Microsoft to charge or bill my current payment method for the fees associated with my use of the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s), and (c) agree that Microsoft may share my contact information and transaction details with the seller(s) of the offering(s). Microsoft does not provide rights for third-party products or services. See the Azure Marketplace Terms for additional terms.

The following message will be displayed once provisioning is completed:


Deployments succeeded 8:23 AM

Deployment to resource group 'Demo' was successful.

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

Username	Password
ras	R@s2017!

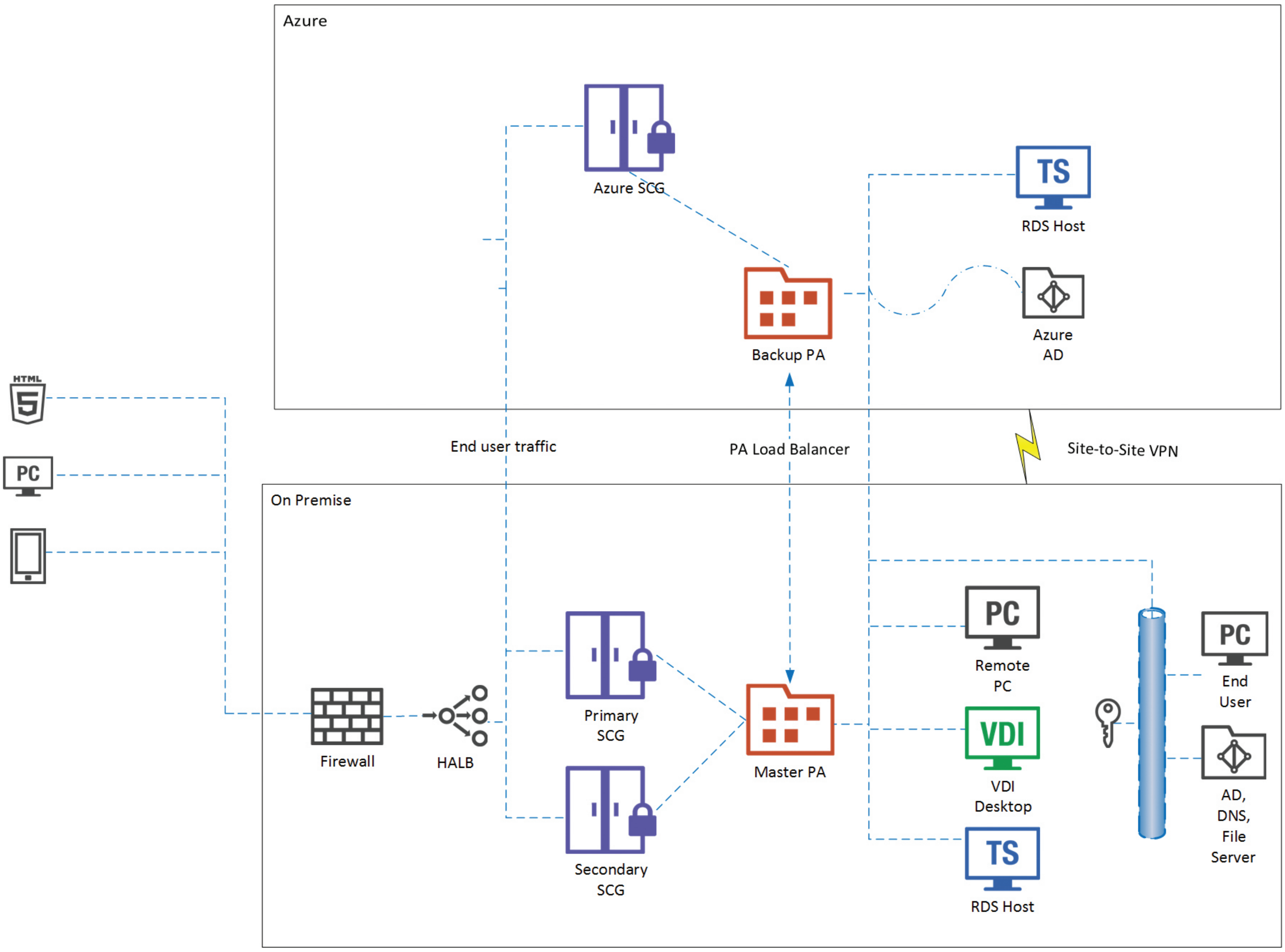
Hybrid Deployment (On Premise and Azure)

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:

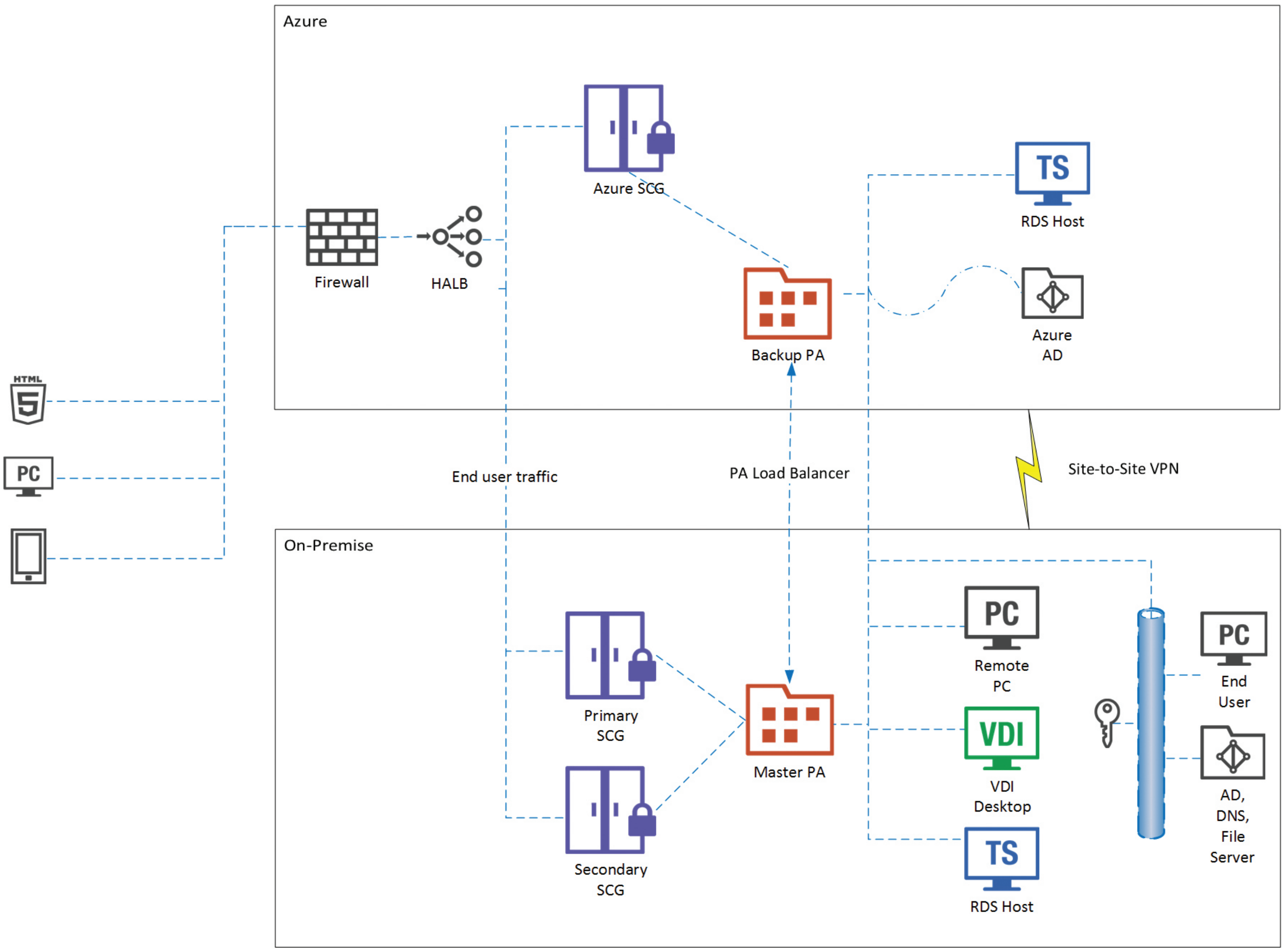
- Publishing Agent (Controller)
- Hosted Shared workers (Session Isolation)
- Server VDI Workers (VM/Server Isolation)
- Azure Active Directory Services or local AD Controller (for failover purposes)
- An Azure local SQL Server VM Instance (for reporting)
- Corporate network and Azure must be connected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

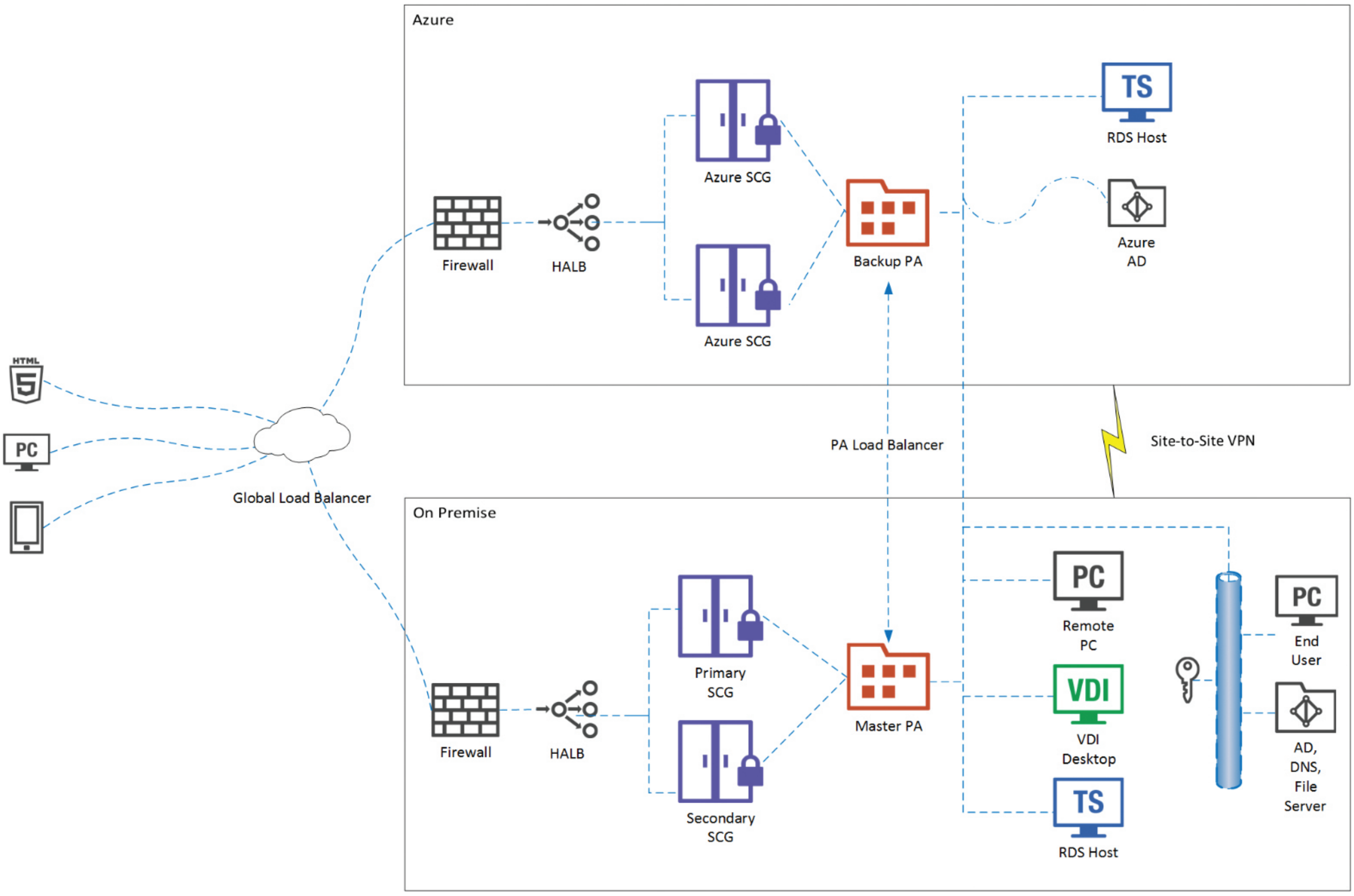
Endpoint Access Using On-premise



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

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

VDI	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-premise 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-premise 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-premise

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-premise network. For example, a DirSync server running on an Azure VM needs to query your on-premise 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-premise network to existing Azure infrastructure.

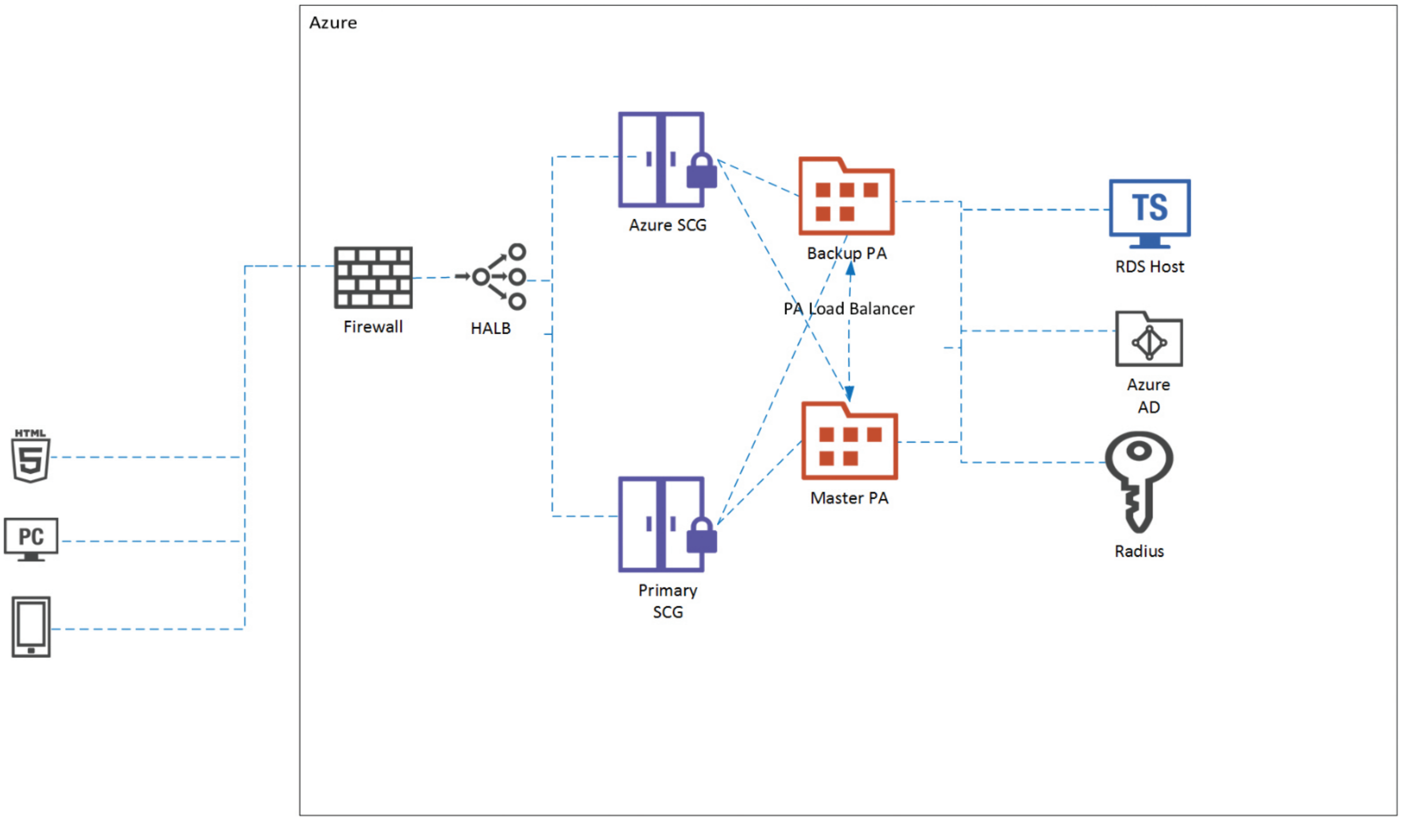
All-Azure Deployment

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	
TS	**Component Installed**	**Installation Method**
	Parallels Terminal Server Agent	Push installation

	Hypervisor Host with VDI Desktops	
VDI	**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.

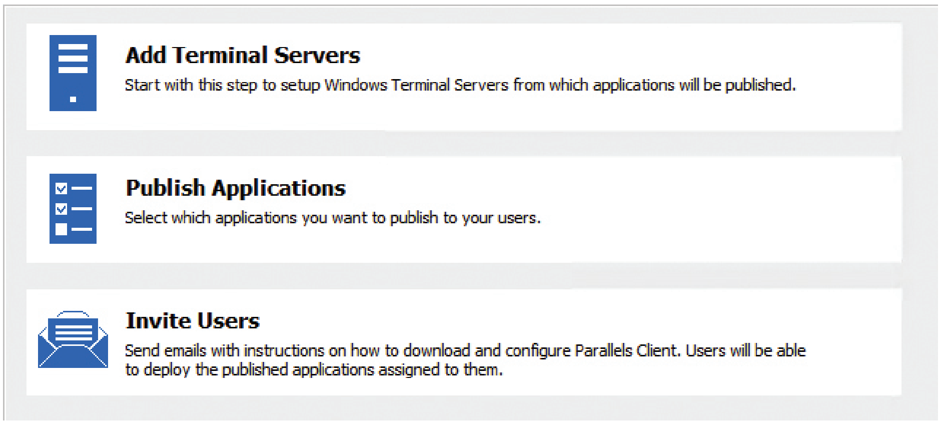
To deploy Remote Application Server using the trial image, go to this section of the document.

Once selected VMs are deployed in Azure or an on-premise 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-premise 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:

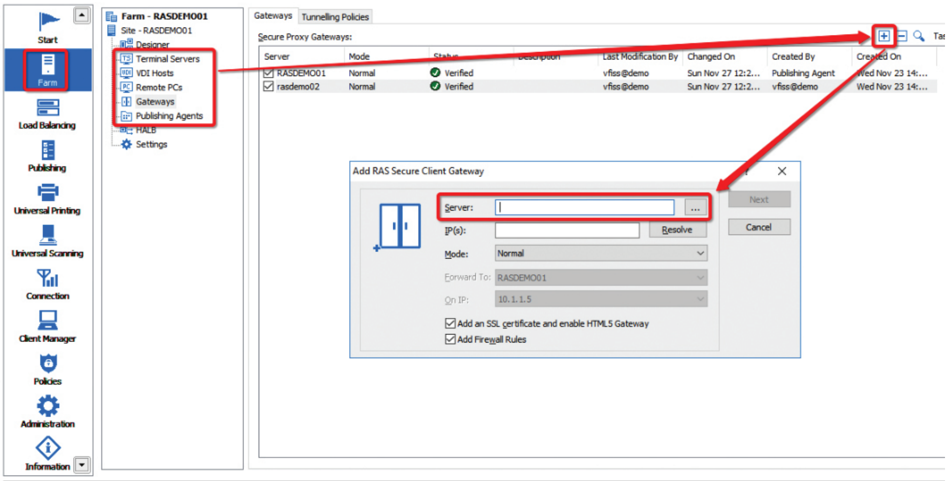


Add Terminal Servers
Start with this step to setup Windows Terminal Servers from which applications will be published.

Publish Applications
Select which applications you want to publish to your users.

Invite Users
Send emails with instructions on how to download and configure Parallels Client. Users will be able to deploy the published applications assigned to them.

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



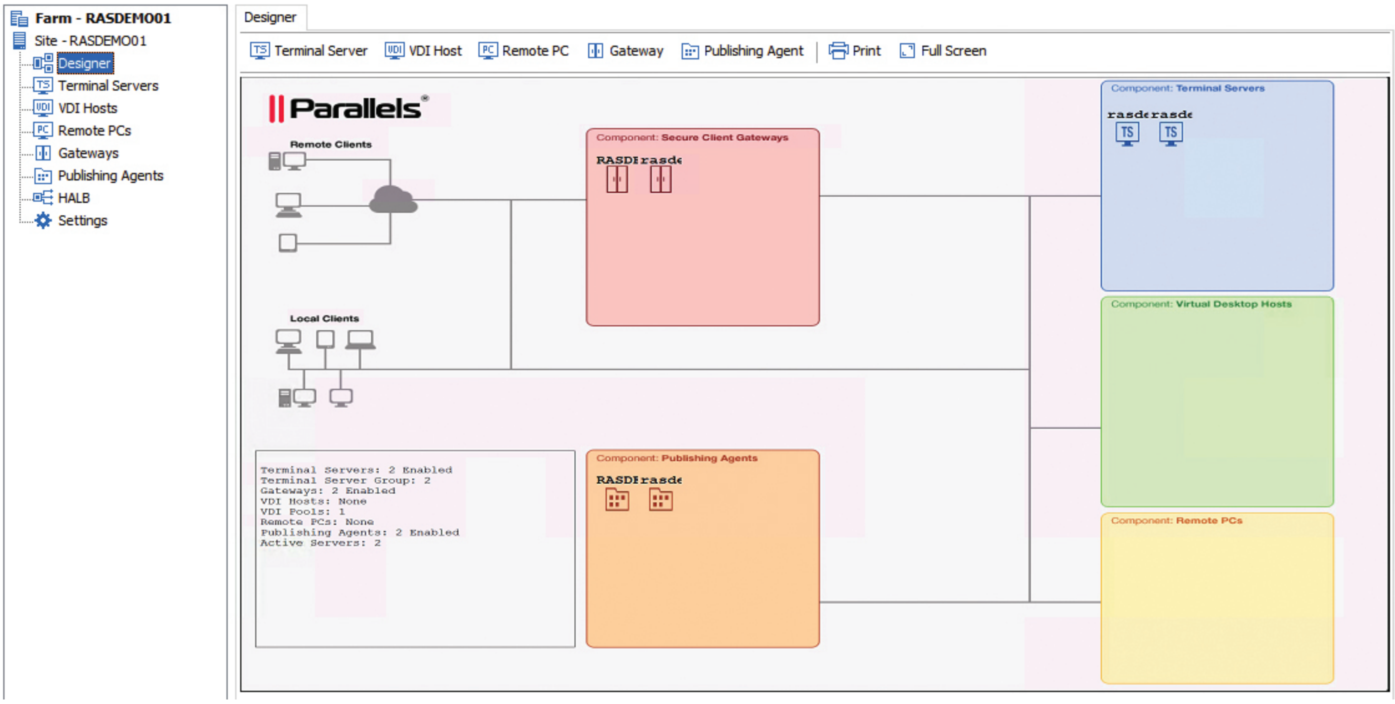
Secure Proxy Gateways:

Server	Mode	Status	Description	Last Modification By	Changed On	Created By	Created On
☑ RASDEMO01	Normal	✓ Verified		vfiss@demo	Sun Nov 27 12:2...	Publishing Agent	Wed Nov 23 14:...
☑ rasdemo02	Normal	✓ Verified		vfiss@demo	Sun Nov 27 12:2...	vfiss@demo	Wed Nov 23 14:...

Add RAS Secure Client Gateway

Server:
IP(s):
Mode: Normal
Forward To: RASDEMO01
On IP: 10.1.1.5
☑ Add an SSL certificate and enable HTML5 Gateway
☑ Add Firewall Rules

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



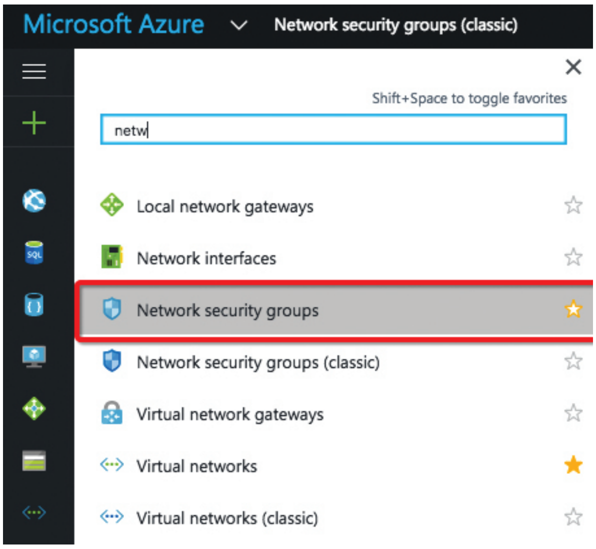
```
Terminal Servers: 2 Enabled
Terminal Server Group: 2
Gateways: 2 Enabled
VDI Hosts: None
VDI Pools: 1
Remote PCs: None
Publishing Agents: 2 Enabled
Active Servers: 2
```

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.

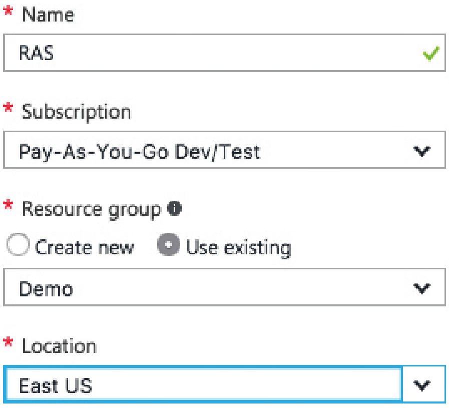
Azure Network Configuration for Inbound Traffic

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


Microsoft Azure
Network security groups (classic)
Shift+Space to toggle favorites
netw
Local network gateways
Network interfaces
Network security groups
Network security groups (classic)
Virtual network gateways
Virtual networks
Virtual networks (classic)

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



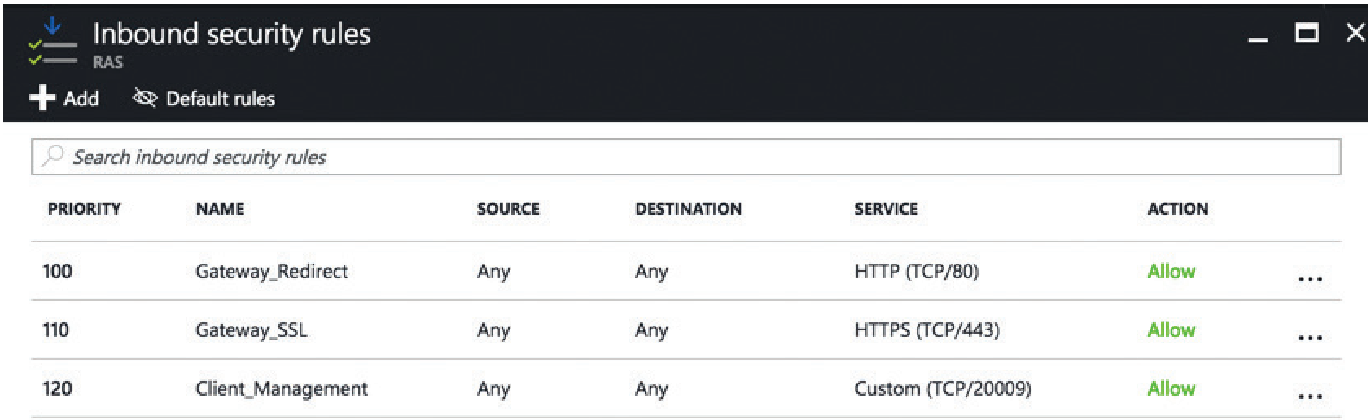
* Name
RAS ✓

* Subscription
Pay-As-You-Go Dev/Test

* Resource group
○ Create new ● Use existing
Demo

* Location
East US

Create the following inbound rules:



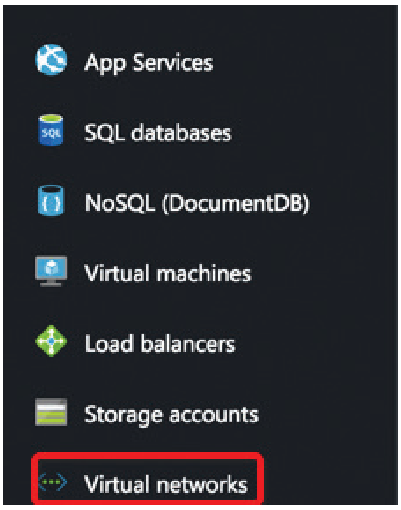
PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION	
100	Gateway_Redirect	Any	Any	HTTP (TCP/80)	Allow	...
110	Gateway_SSL	Any	Any	HTTPS (TCP/443)	Allow	...
120	Client_Management	Any	Any	Custom (TCP/20009)	Allow	...

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.

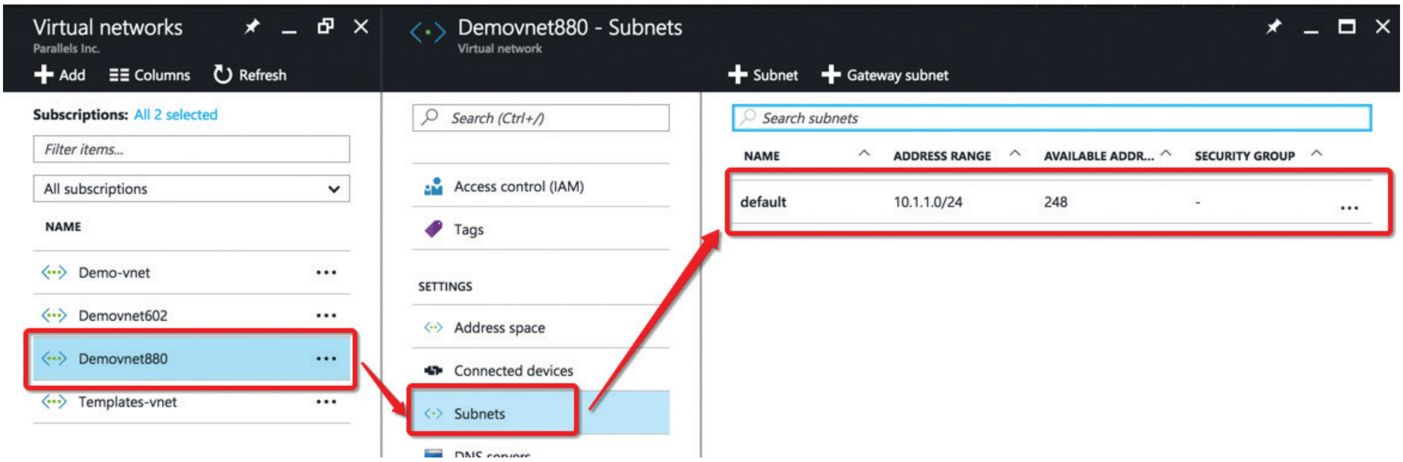
The new network security rule is not assigned to any VM or resources. The next step is to assign the new rule to Remote Application Server VMs.

Assign Firewall Rules to RAS Subnet and Virtual Machines

Virtual Network Configuration
Go to Azure Menu > Virtual networks

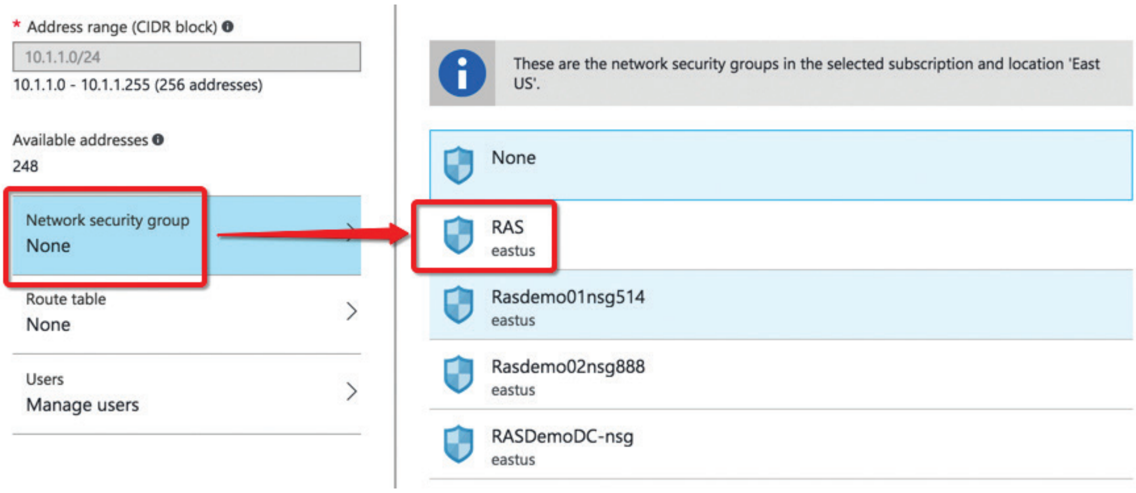


Select the Virtual networks > Subnets > Security group:



NAME	ADDRESS RANGE	AVAILABLE ADDR...	SECURITY GROUP
default	10.1.1.0/24	248	-

Replace your default security rule with “RAS”:



* Address range (CIDR block)

10.1.1.0/24

10.1.1.0 - 10.1.1.255 (256 addresses)

Available addresses

248

Network security group
None

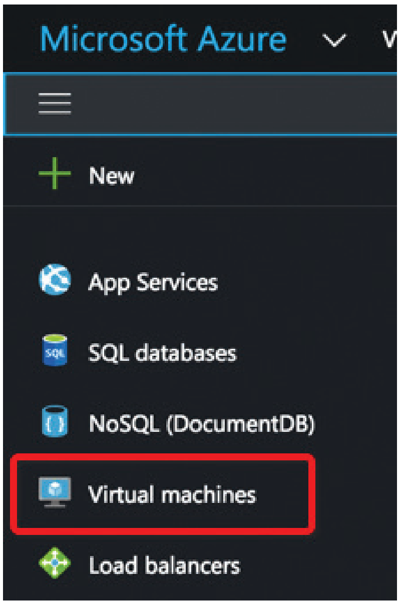
Route table
None

Users
Manage users

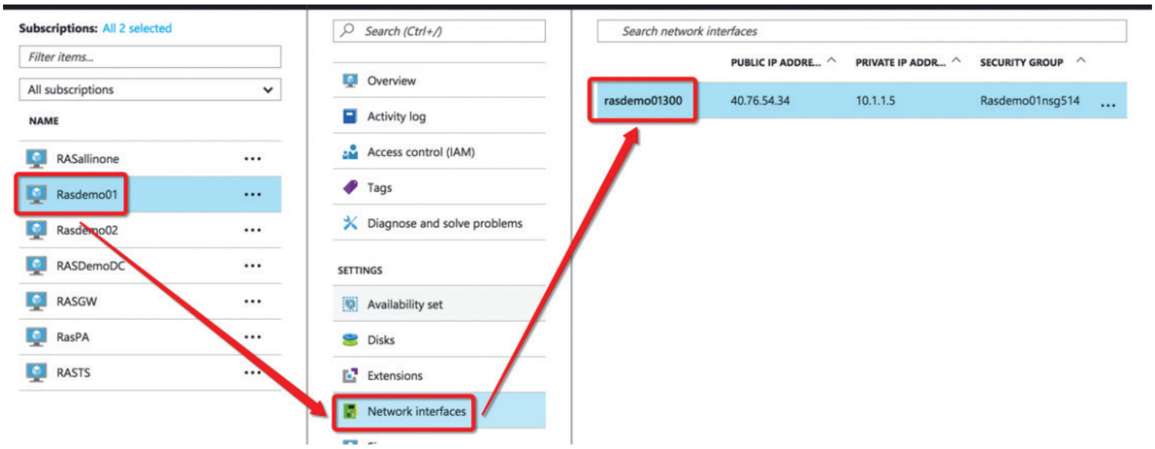
These are the network security groups in the selected subscription and location 'East US'.

HALB or Gateway Virtual Machine Security Group Configuration

Go to Azure Menu > Virtual machines:

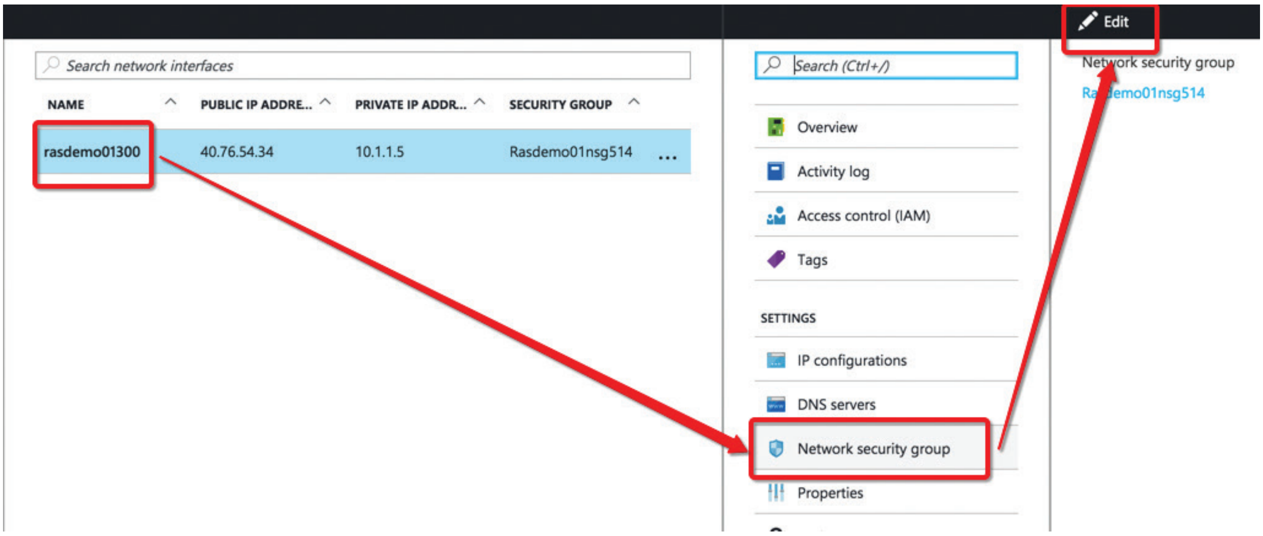


Select either HALB or Gateway Virtual Machine(s) > Network interfaces > Select network interface:



NAME	PUBLIC IP ADDRE...	PRIVATE IP ADDR...	SECURITY GROUP
rasdemo01300	40.76.54.34	10.1.1.5	Rasdemo01nsg514

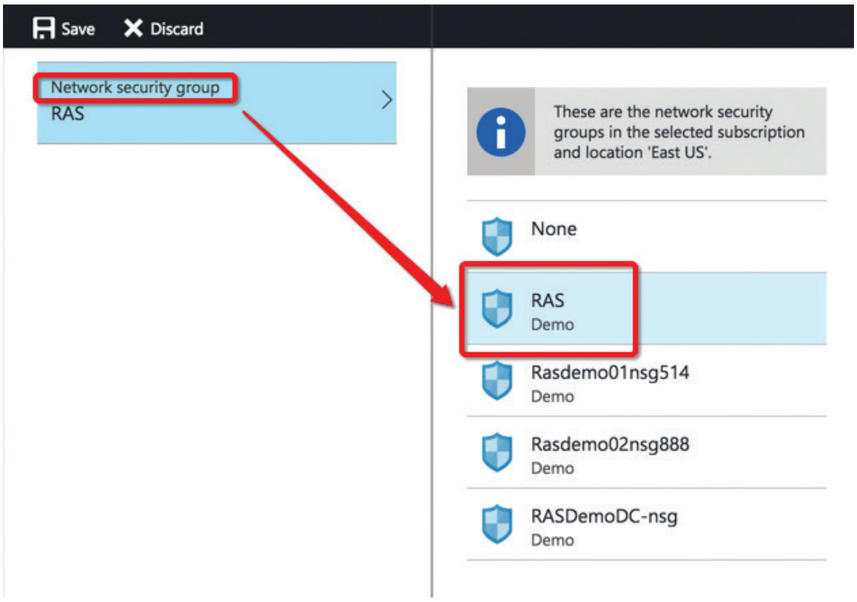
Select Network security group > Edit:



NAME	PUBLIC IP ADDRE...	PRIVATE IP ADDR...	SECURITY GROUP
rasdemo01300	40.76.54.34	10.1.1.5	Rasdemo01nsg514

Network security group
Rasdemo01nsg514

Change existing security group to "RAS":



Network security group
RAS

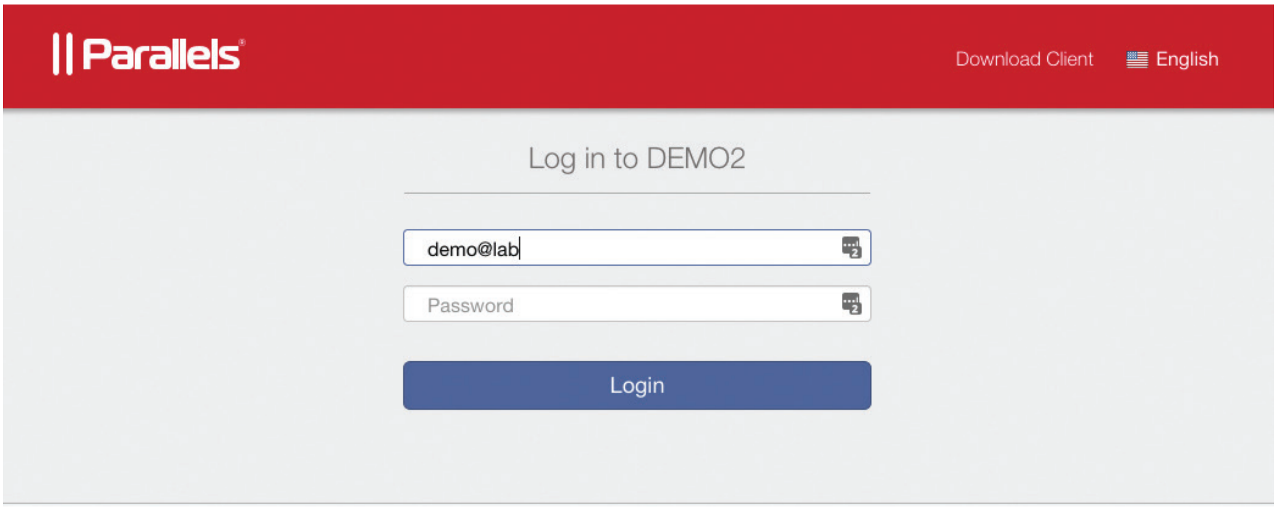
These are the network security groups in the selected subscription and location 'East US'.

- RAS
  Demo
- Rasdemo01nsg514
  Demo
- Rasdemo02nsg888
  Demo
- RASDemoDC-nsg
  Demo

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.

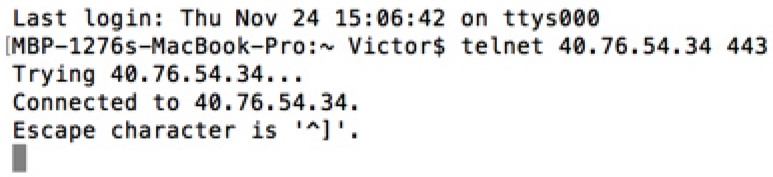


Log in to DEMO2

demo@lab

Password

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-premise deployments.

Remote Desktop/Terminal Server Performance Settings

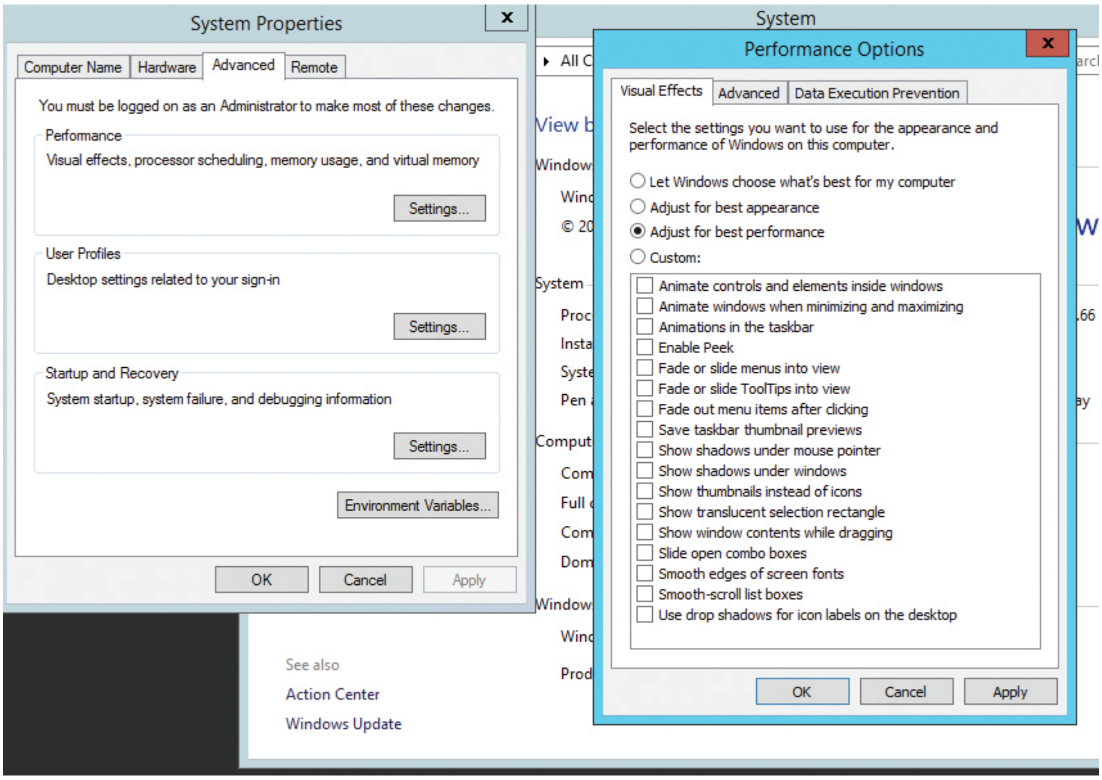
The default Windows performance settings are intended for general purpose servers. In order to maximize application or desktop hosting server performance, the default Windows performance settings should be adjusted on Windows Remote Desktop/Terminal Servers.

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.



System Properties

Computer Name | Hardware | Advanced | Remote

You must be logged on as an Administrator to make most of these changes.

Performance
Visual effects, processor scheduling, memory usage, and virtual memory
Settings...

User Profiles
Desktop settings related to your sign-in
Settings...

Startup and Recovery
System startup, system failure, and debugging information
Settings...

Environment Variables...

OK | Cancel | Apply

System

See also
Action Center
Windows Update

Performance Options

Visual Effects | Advanced | Data Execution Prevention

Select the settings you want to use for the appearance and performance of Windows on this computer.

○ Let Windows choose what's best for my computer
○ Adjust for best appearance
● Adjust for best performance
○ Custom:

□ Animate controls and elements inside windows
□ Animate windows when minimizing and maximizing
□ Animations in the taskbar
□ Enable Peek
□ Fade or slide menus into view
□ Fade or slide ToolTips into view
□ Fade out menu items after clicking
□ Save taskbar thumbnail previews
□ Show shadows under mouse pointer
□ Show shadows under windows
□ Show thumbnails instead of icons
□ Show translucent selection rectangle
□ Show window contents while dragging
□ Slide open combo boxes
□ Smooth edges of screen fonts
□ Smooth-scroll list boxes
□ Use drop shadows for icon labels on the desktop

OK | Cancel | Apply

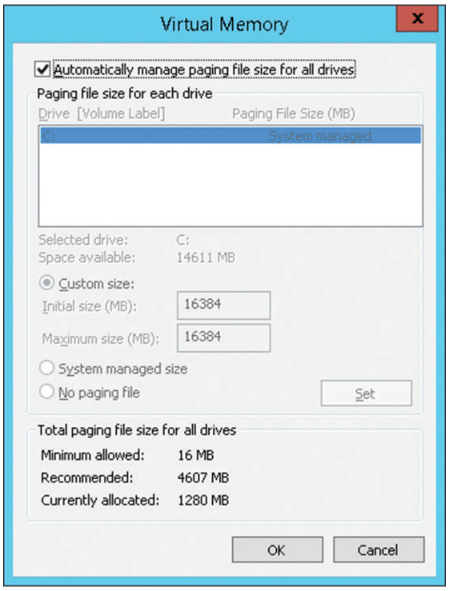
Windows Paging File Settings

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.



Virtual Memory

☑ Automatically manage paging file size for all drives

Paging file size for each drive

Drive [Volume Label]	Paging File Size (MB)
C:	System managed

Selected drive: C:
Space available: 14611 MB

● Custom size:
Initial size (MB): 16384
Maximum size (MB): 16384
○ System managed size
○ No paging file
Set

Total paging file size for all drives
Minimum allowed: 16 MB
Recommended: 4607 MB
Currently allocated: 1280 MB

OK | Cancel

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 erminal 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:

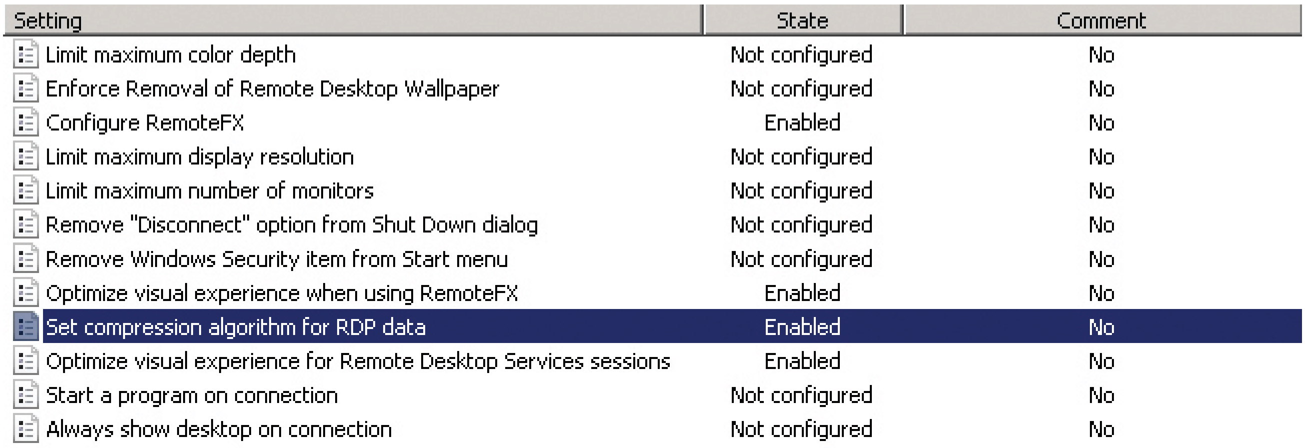
    a. Use Advanced RemoteFX graphics for RemoteApp
        i. Enabled > Set to “Optimize to use less network bandwidth”
    b. Configure compression for RemoteFX dat
        i. Enabled > Optimize to use less network bandwidth
    c. Configure image quality for RemoteFX Adaptive Graphics
        i. Enabled > 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.)

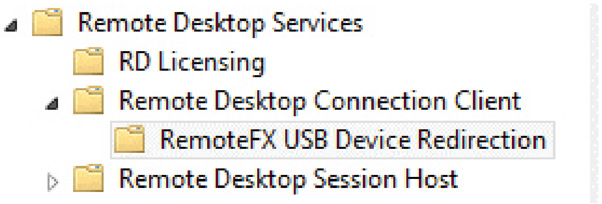
Remote FX USB Redirection, Audio Redirection, and Time Zone Redirection

RemoteFX USB Redirection

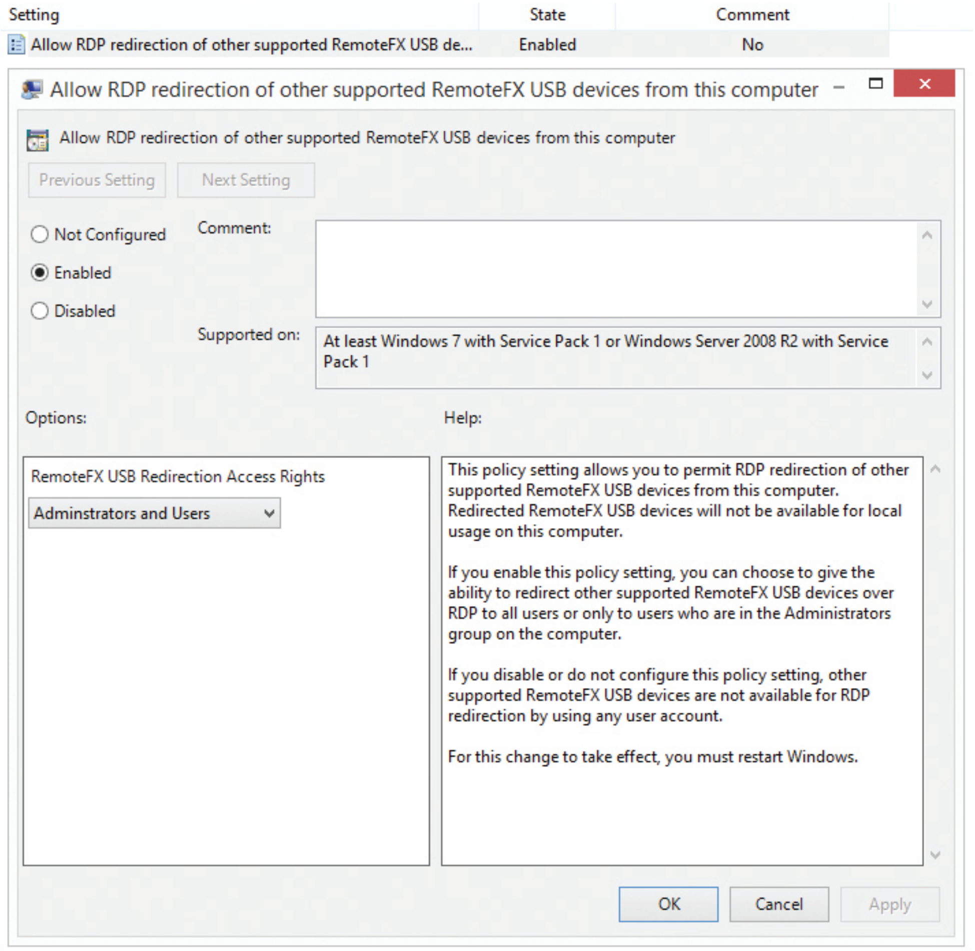
In order to get some Point of Sale / USB scanning devices to work properly with Windows 2008 R2 and higher, you must enable RemoteFX USB redirection.

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:


Remote Desktop Services
RD Licensing
Remote Desktop Connection Client
RemoteFX USB Device Redirection
Remote Desktop Session Host

For additional information, see this KB article from Microsoft.



Setting	State	Comment
Allow RDP redirection of other supported RemoteFX USB de...	Enabled	No

Allow RDP redirection of other supported RemoteFX USB devices from this computer

Allow RDP redirection of other supported RemoteFX USB devices from this computer

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 7 with Service Pack 1 or Windows Server 2008 R2 with Service Pack 1

Options:

RemoteFX USB Redirection Access Rights
Adminstrators and Users

Help:

This policy setting allows you to permit RDP redirection of other supported RemoteFX USB devices from this computer. Redirected RemoteFX USB devices will not be available for local usage on this computer.

If you enable this policy setting, you can choose to give the ability to redirect other supported RemoteFX USB devices over RDP to all users or only to users who are in the Administrators group on the computer.

If you disable or do not configure this policy setting, other supported RemoteFX USB devices are not available for RDP redirection by using any user account.

For this change to take effect, you must restart Windows.

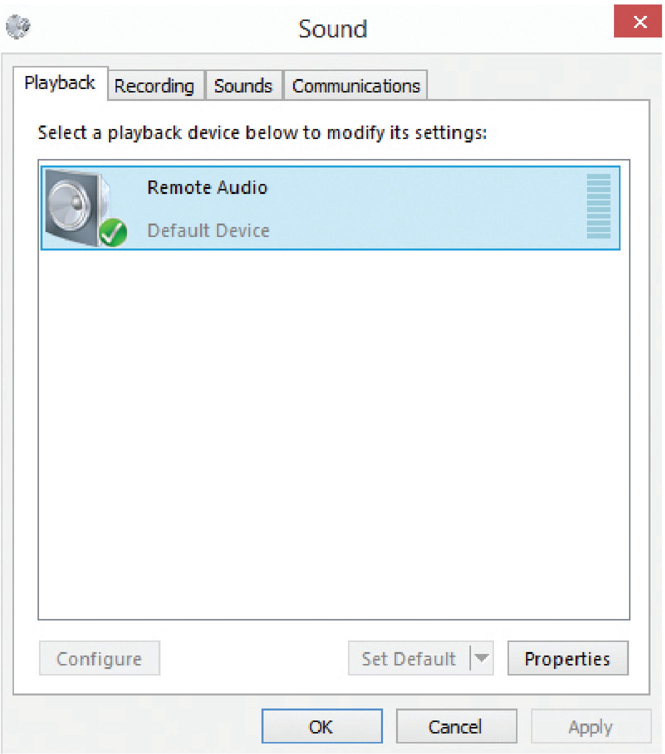
Enable Audio / Recording Redirection

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:

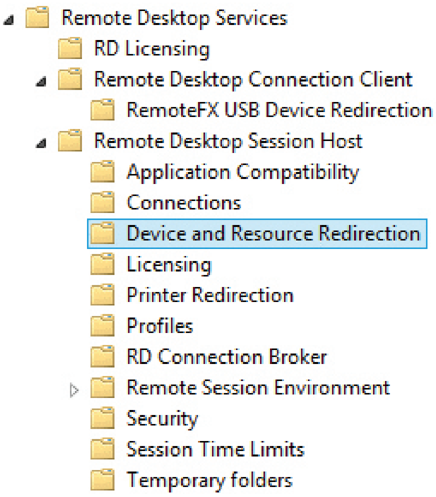
a. Simply right-click the server's sound icon in the Windows system tray. You will then be prompted to enable remote audio.



Select a playback device below to modify its settings:

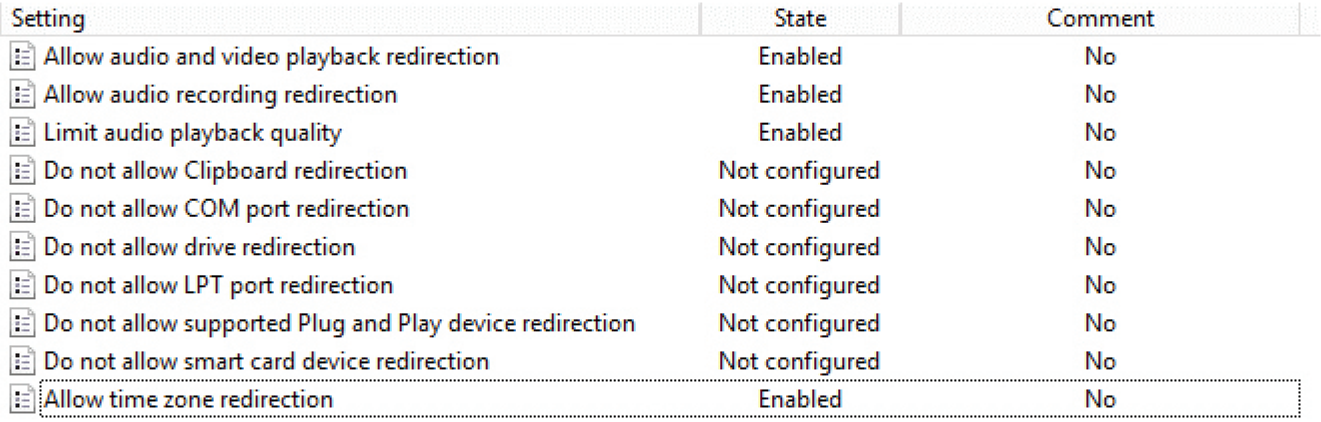
Remote Audio
Default Device

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:

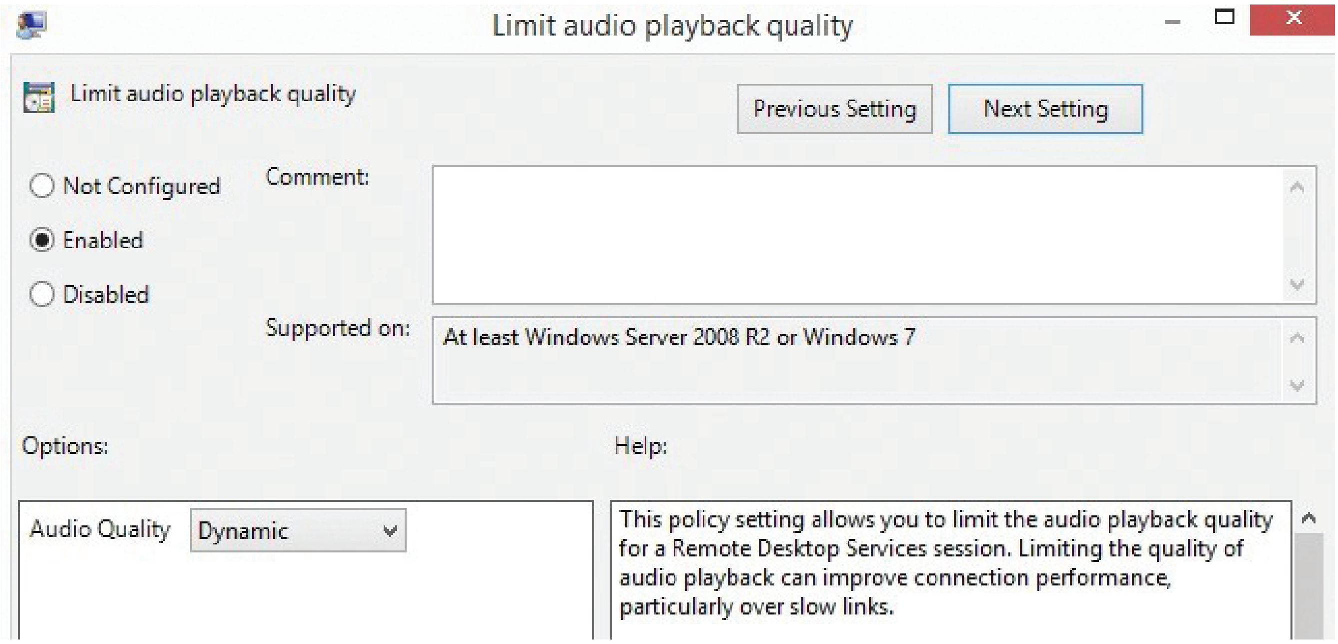


- Remote Desktop Services
  - RD Licensing
  - Remote Desktop Connection Client
    - RemoteFX USB Device Redirection
  - Remote Desktop Session Host
    - Application Compatibility
    - Connections
    - Device and Resource Redirection
    - Licensing
    - Printer Redirection
    - Profiles
    - RD Connection Broker
    - Remote Session Environment
    - Security
    - Session Time Limits
    - Temporary folders

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



○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2008 R2 or Windows 7

Options:

Audio Quality: Dynamic

Help:

This policy setting allows you to limit the audio playback quality for a Remote Desktop Services session. Limiting the quality of audio playback can improve connection performance, particularly over slow links.

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

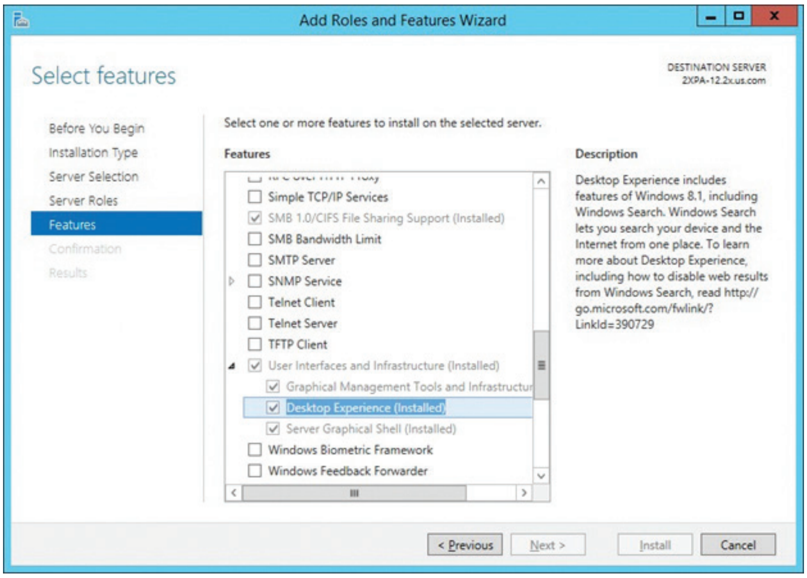
Audio Redirection:

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.



Select one or more features to install on the selected server.

- ☐ Simple TCP/IP Services
- ☑ SMB 1.0/CIFS File Sharing Support (Installed)
- ☐ SMB Bandwidth Limit
- ☐ SMTP Server
- ☐ SNMP Service
- ☐ Telnet Client
- ☐ Telnet Server
- ☐ TFTP Client
- ☑ User Interfaces and Infrastructure (Installed)
  - ☑ Graphical Management Tools and Infrastructur
  - ☑ Desktop Experience (Installed)
  - ☑ Server Graphical Shell (Installed)
- ☐ Windows Biometric Framework
- ☐ Windows Feedback Forwarder

Desktop Experience includes features of Windows 8.1, including Windows Search. Windows Search lets you search your device and the Internet from one place. To learn more about Desktop Experience, including how to disable web results from Windows Search, read http://go.microsoft.com/fwlink/?LinkId=390729

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.

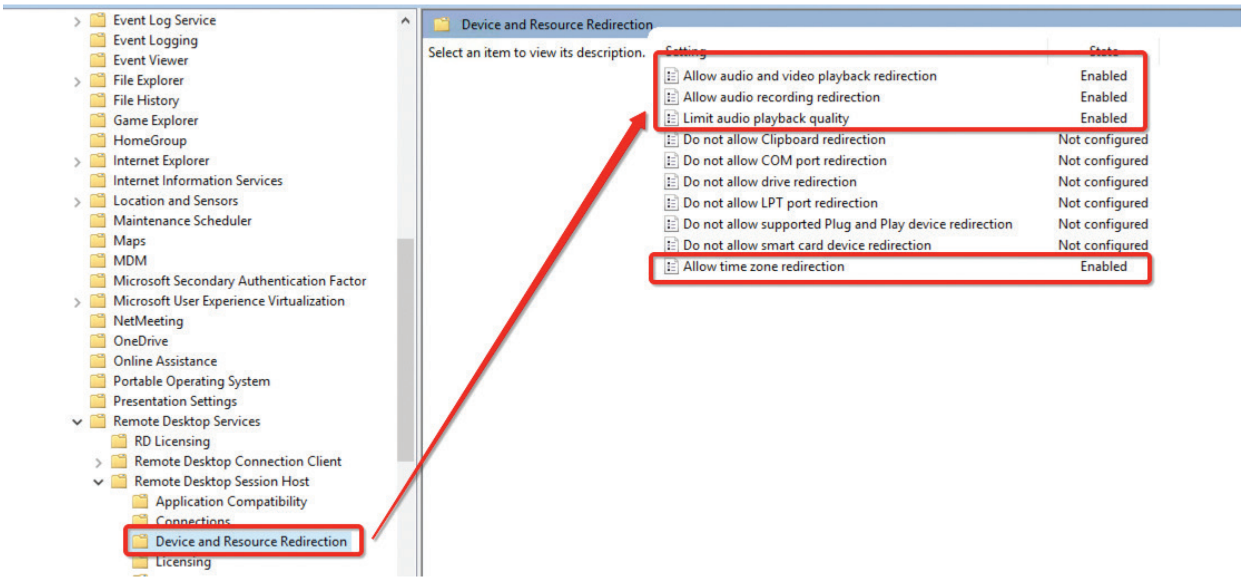
Windows Server 2016 Specific Group Policies

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:

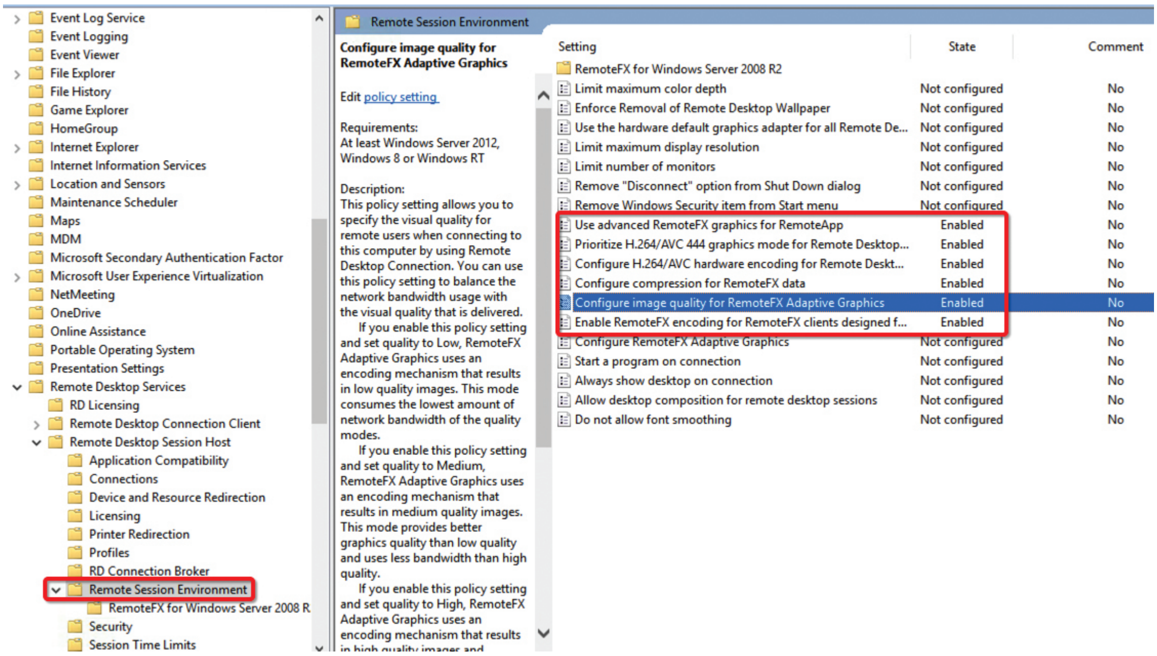
Device and Resource Redirection


Event Log Service
Event Logging
Event Viewer
File Explorer
File History
Game Explorer
HomeGroup
Internet Explorer
Internet Information Services
Location and Sensors
Maintenance Scheduler
Maps
MDM
Microsoft Secondary Authentication Factor
Microsoft User Experience Virtualization
NetMeeting
OneDrive
Online Assistance
Portable Operating System
Presentation Settings
Remote Desktop Services
RD Licensing
Remote Desktop Connection Client
Remote Desktop Session Host
Application Compatibility
Connections
Device and Resource Redirection
Licensing
Device and Resource Redirection

Select an item to view its description.

Setting	State
Allow audio and video playback redirection	Enabled
Allow audio recording redirection	Enabled
Limit audio playback quality	Enabled
Do not allow Clipboard redirection	Not configured
Do not allow COM port redirection	Not configured
Do not allow drive redirection	Not configured
Do not allow LPT port redirection	Not configured
Do not allow supported Plug and Play device redirection	Not configured
Do not allow smart card device redirection	Not configured
Allow time zone redirection	Enabled

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



Configure image quality for RemoteFX Adaptive Graphics

Edit policy setting

Requirements:
At least Windows Server 2012, Windows 8 or Windows RT

Description:
This policy setting allows you to specify the visual quality for remote users when connecting to this computer by using Remote Desktop Connection. You can use this policy setting to balance the network bandwidth usage with the visual quality that is delivered.

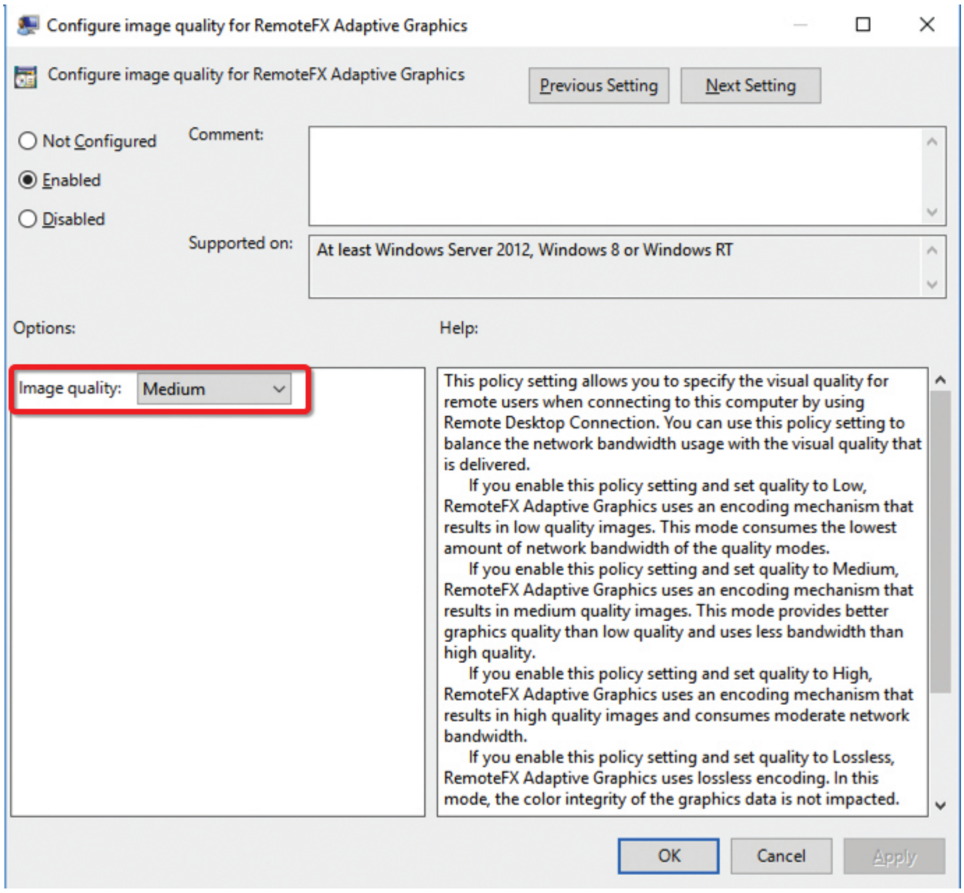
If you enable this policy setting and set quality to Low, RemoteFX Adaptive Graphics uses an encoding mechanism that results in low quality images. This mode consumes the lowest amount of network bandwidth of the quality modes.

If you enable this policy setting and set quality to Medium, RemoteFX Adaptive Graphics uses an encoding mechanism that results in medium quality images. This mode provides better graphics quality than low quality and uses less bandwidth than high quality.

If you enable this policy setting and set quality to High, RemoteFX Adaptive Graphics uses an encoding mechanism that results in high quality images and

Setting	State	Comment
RemoteFX for Windows Server 2008 R2		
Limit maximum color depth	Not configured	No
Enforce Removal of Remote Desktop Wallpaper	Not configured	No
Use the hardware default graphics adapter for all Remote De...	Not configured	No
Limit maximum display resolution	Not configured	No
Limit 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
Use advanced RemoteFX graphics for RemoteApp	Enabled	No
Prioritize H.264/AVC 444 graphics mode for Remote Desktop...	Enabled	No
Configure H.264/AVC hardware encoding for Remote Deskt...	Enabled	No
Configure compression for RemoteFX data	Enabled	No
Configure image quality for RemoteFX Adaptive Graphics	Enabled	No
Enable RemoteFX encoding for RemoteFX clients designed f...	Enabled	No
Configure RemoteFX Adaptive Graphics	Not configured	No
Start a program on connection	Not configured	No
Always show desktop on connection	Not configured	No
Allow desktop composition for remote desktop sessions	Not configured	No
Do not allow font smoothing	Not configured	No

Set “Configure image quality for RemoteFX Adaptive Graphics” to Medium:



Configure image quality for RemoteFX Adaptive Graphics

Configure image quality for RemoteFX Adaptive Graphics

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2012, Windows 8 or Windows RT

Options:

Image quality: Medium

Help:

This policy setting allows you to specify the visual quality for remote users when connecting to this computer by using Remote Desktop Connection. You can use this policy setting to balance the network bandwidth usage with the visual quality that is delivered.

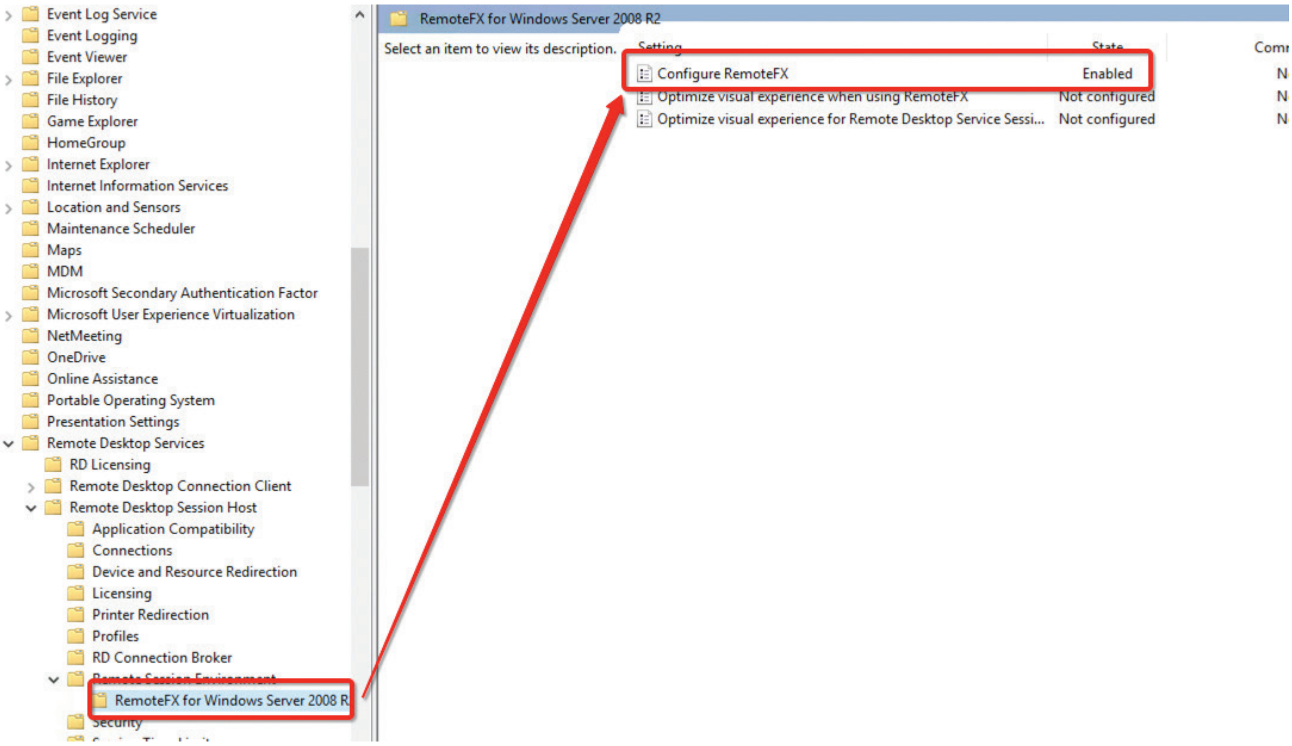
If you enable this policy setting and set quality to Low, RemoteFX Adaptive Graphics uses an encoding mechanism that results in low quality images. This mode consumes the lowest amount of network bandwidth of the quality modes.

If you enable this policy setting and set quality to Medium, RemoteFX Adaptive Graphics uses an encoding mechanism that results in medium quality images. This mode provides better graphics quality than low quality and uses less bandwidth than high quality.

If you enable this policy setting and set quality to High, RemoteFX Adaptive Graphics uses an encoding mechanism that results in high quality images and consumes moderate network bandwidth.

If you enable this policy setting and set quality to Lossless, RemoteFX Adaptive Graphics uses lossless encoding. In this mode, the color integrity of the graphics data is not impacted.

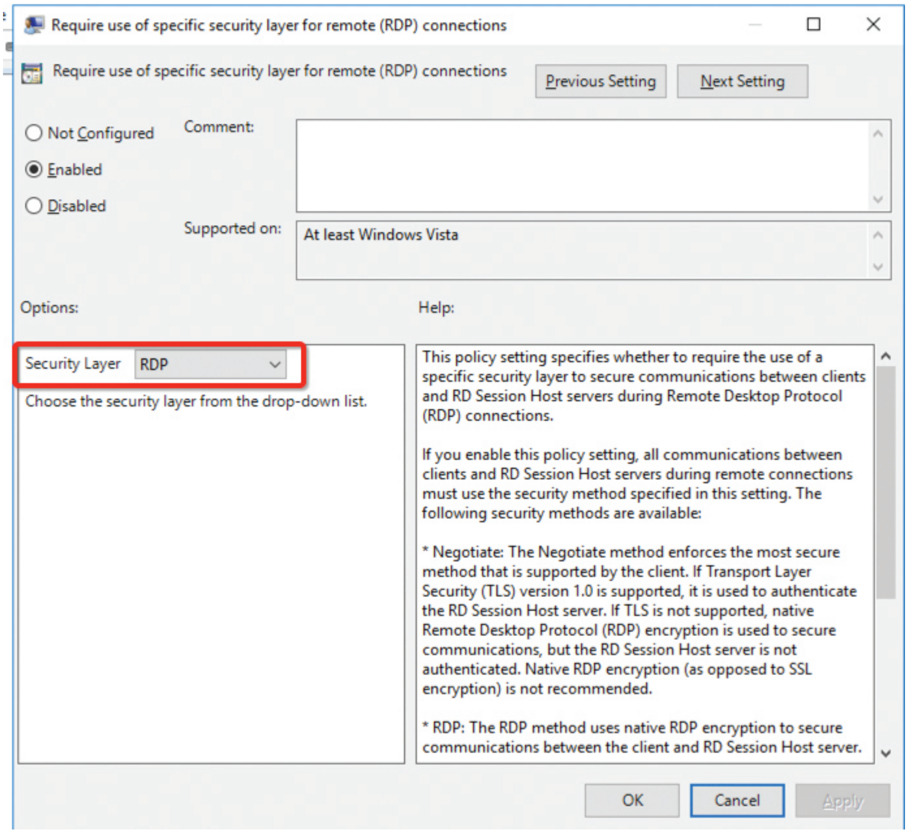
Windows 2008 R2 RemoteFX Compatibility



RemoteFX for Windows Server 2008 R2

Select an item to view its description.

Setting	State	Comm
Configure RemoteFX	Enabled	N
Optimize visual experience when using RemoteFX	Not configured	N
Optimize visual experience for Remote Desktop Service Sessi...	Not configured	N



Require use of specific security layer for remote (RDP) connections

Require use of specific security layer for remote (RDP) connections

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Security Layer: RDP

Choose the security layer from the drop-down list.

Help:

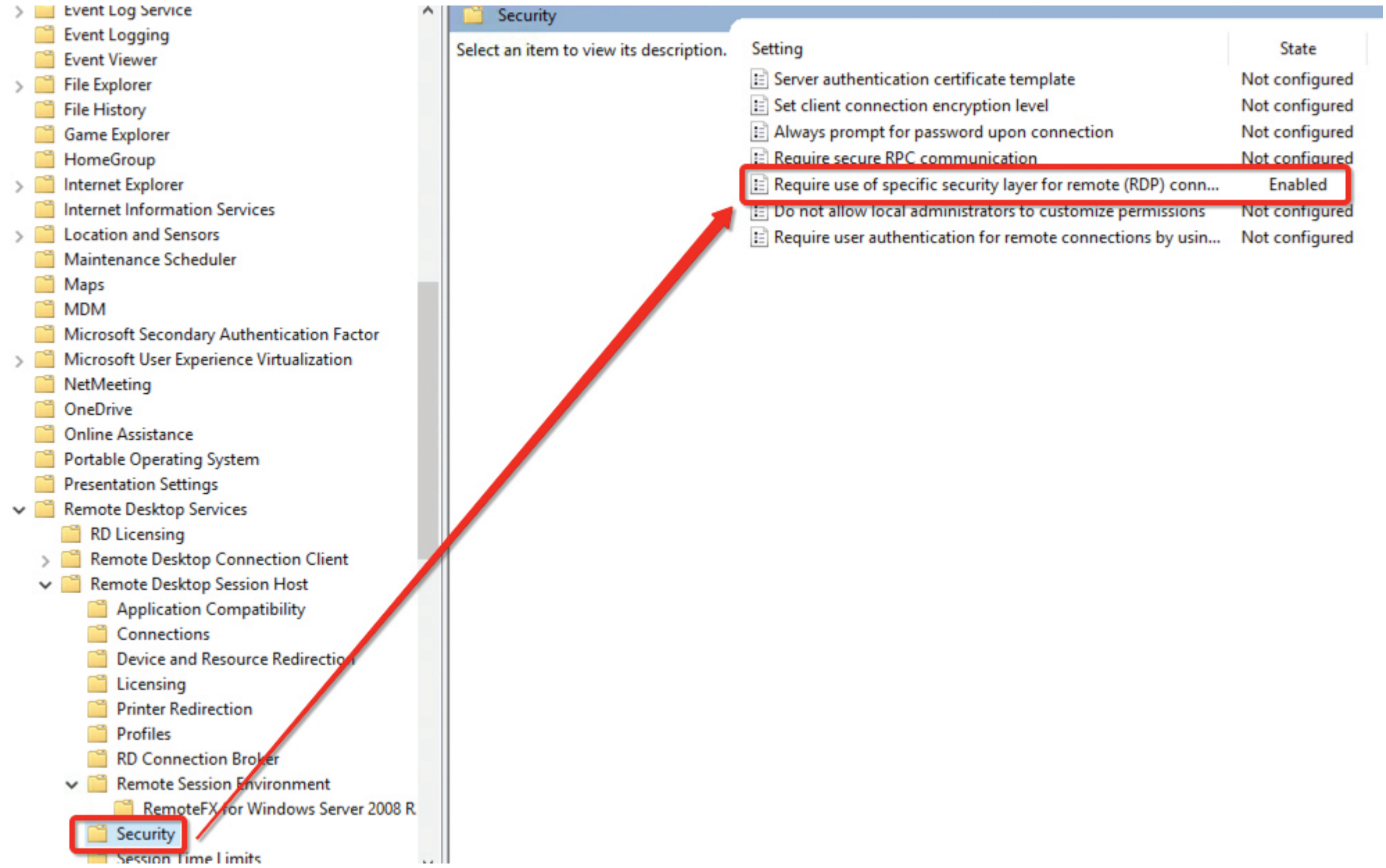
This policy setting specifies whether to require the use of a specific security layer to secure communications between clients and RD Session Host servers during Remote Desktop Protocol (RDP) connections.

If you enable this policy setting, all communications between clients and RD Session Host servers during remote connections must use the security method specified in this setting. The following security methods are available:

* Negotiate: The Negotiate method enforces the most secure method that is supported by the client. If Transport Layer Security (TLS) version 1.0 is supported, it is used to authenticate the RD Session Host server. If TLS is not supported, native Remote Desktop Protocol (RDP) encryption is used to secure communications, but the RD Session Host server is not authenticated. Native RDP encryption (as opposed to SSL encryption) is not recommended.

* RDP: The RDP method uses native RDP encryption to secure communications between the client and RD Session Host server.

RDP Security



- Event Log Service
- Event Logging
- Event Viewer
- File Explorer
- File History
- Game Explorer
- HomeGroup
- Internet Explorer
- Internet Information Services
- Location and Sensors
- Maintenance Scheduler
- Maps
- MDM
- Microsoft Secondary Authentication Factor
- Microsoft User Experience Virtualization
- NetMeeting
- OneDrive
- Online Assistance
- Portable Operating System
- Presentation Settings
- Remote Desktop Services
  - RD Licensing
  - Remote Desktop Connection Client
  - Remote Desktop Session Host
    - Application Compatibility
    - Connections
    - Device and Resource Redirection
    - Licensing
    - Printer Redirection
    - Profiles
    - RD Connection Broker
    - Remote Session Environment
      - RemoteFX for Windows Server 2008 R
    - Security
    - Session Time Limits

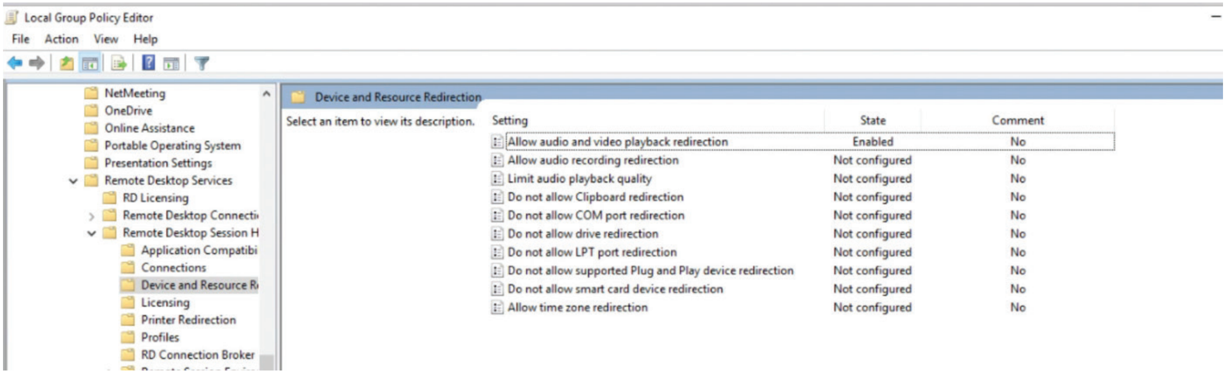
Security

Select an item to view its description.

Setting	State
Server authentication certificate template	Not configured
Set client connection encryption level	Not configured
Always prompt for password upon connection	Not configured
Require secure RPC communication	Not configured
Require use of specific security layer for remote (RDP) conn...	Enabled
Do not allow local administrators to customize permissions	Not configured
Require user authentication for remote connections by usin...	Not configured

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).



Select an item to view its description.

Setting	State	Comment
Allow audio and video playback redirection	Enabled	No
Allow audio recording redirection	Not configured	No
Limit audio playback quality	Not configured	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	Not configured	No

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-pportal

parallels.com/products/ras/resources/