



Parallels Remote Application Server

Administrator's Guide

v16.5 Update 4

Parallels International GmbH
Vordergasse 59
8200 Schaffhausen
Switzerland
Tel: + 41 52 672 20 30
www.parallels.com

Copyright © 1999-2019 Parallels International GmbH. All rights reserved.

This product is protected by United States and international copyright laws. The product's underlying technology, patents, and trademarks are listed at <http://www.parallels.com/about/legal/>.

Microsoft, Windows, Windows Server, Windows Vista are registered trademarks of Microsoft Corporation.
Apple, Mac, the Mac logo, OS X, macOS, iPad, iPhone, iPod touch are trademarks of Apple Inc., registered in the US and other countries.

Linux is a registered trademark of Linus Torvalds.

All other marks and names mentioned herein may be trademarks of their respective owners.

Contents

Introduction	11
About Parallels RAS	11
About This Guide	12
Terms and Abbreviations Used in This Guide	12
Installing Parallels RAS	15
System Requirements	15
Hardware Requirements.....	15
Software Requirements	16
Announcement: Parallels RAS Upcoming Version System Requirements	18
Install Parallels RAS.....	19
Log In and Activate Parallels RAS	20
Getting Started with Parallels RAS	23
The Parallels RAS Console	23
Set Up a Basic Parallels RAS Farm.....	24
Add an RD Session Host.....	26
Publish Applications	27
Invite Users.....	28
Conclusion	32
Parallels RAS Farm and Sites	33
Connecting to a Parallels RAS Farm	33
About Sites	35
Viewing Sites in the RAS Console.....	36
Adding a Site to the Farm.....	38
Replicating Site Settings.....	38
Managing the Licensing Site.....	40
Managing Administrator Accounts	40
Adding an Administrator Account.....	40
Administrator Account Permissions	41
Managing Administrator Accounts.....	42
Configure RAS Console Idle Sessions	43

Using Instant Messaging for Administrators.....	44
Joining Customer Experience Program	44
RD Session Hosts.....	46
RD Session Host Types.....	46
Adding an RD Session Host	47
Installing the Agent Manually	48
Viewing RD Session Hosts	50
Configuring an RD Session Host.....	51
Check RAS RD Session Host Agent Status.....	51
Change RD Session Host Site Assignment.....	52
View and Modify RD Session Host Properties	52
Grouping and Cloning RD Session Hosts.....	56
Using Scheduler.....	60
Managing Sessions	62
Managing Logons	64
Publishing from an RD Session Host.....	65
Publishing a Desktop from an RD Session Host	66
Publishing an Application from an RD Session Host	66
Publishing a Web Application from an RD Session Host.....	68
Publishing a Network Folder from an RD Session Host	69
Publishing a Document from an RD Session Host	70
Publishing Containerized Applications.....	71
Publishing App-V Applications.....	71
Publishing Turbo.net Applications.....	72
Viewing Published Resources Hosted by RD Session Hosts.....	75
VDI and Virtual Desktops	77
Supported Hypervisors.....	77
RAS VDI Agent Information.....	78
RAS VDI Agent Installation Options.....	78
Add a VDI Host.....	80
Installing RAS VDI Agent Manually.....	81
Checking the RAS VDI Agent Status	82

Modifying VDI Host Configuration	82
Change VDI Host Site Assignment.....	85
RAS Templates	85
Template Types and Guest OS Requirements.....	85
Creating a RAS Template	87
How Guest VMs Are Created From a Template.....	94
Managing Guest VMs	95
RAS Template Maintenance	97
VDI Host Pool Management	100
Adding and Deleting Pools	101
Adding and Deleting Pool Members	101
Configuring Guest VMs in a Pool	101
Using a Wildcard to Filter VMs.....	103
Persistent Guest VMs.....	103
Publishing from a Guest VM	104
Publishing a Desktop from a Guest VM	104
Publishing an Application from a Guest VM	105
Publishing a Web Application from a Guest VM.....	106
Publishing a Network Folder from a Guest VM	107
Publishing a Document from a Guest VM.....	108
Viewing VDI Host Summary	109
Managing VDI Sessions.....	109
Remote PCs.....	111
Adding a Remote PC	111
Installing Remote PC Agent Manually.....	112
Configuring a Remote PC.....	113
Viewing Remote PC Summary.....	115
Publishing from a Remote PC.....	115
Publishing a Desktop from a Remote PC.....	115
Publishing an Application from a Remote PC	116
Publishing a Web Application from a Remote PC	116
Publishing a Network Folder from a Remote PC.....	117
Publishing a Document from a Remote PC	117

Managing Published Resources	119
General Management Tasks	119
Manage Published Applications	121
Manage Published Desktops	124
Manage Published Documents	125
Manage Folders	128
Using Filtering Rules	129
Checking Effective Access	132
Specifying Client Settings	134
Quick Keypad	135
RAS Secure Client Gateway.....	137
RAS Secure Client Gateway Overview	137
Adding a RAS Secure Client Gateway.....	139
Manually Adding a RAS Secure Client Gateway	139
Checking the RAS Secure Client Gateway Status	140
Configuring RAS Secure Client Gateway	140
Enable or Disable a Gateway.....	140
Gateway Mode, Forwarding Settings, HSTS.....	140
Set IP Address for Incoming Connections	141
Configure RAS Secure Client Gateway Network Options.....	142
Configure SSL Encryption on a Gateway	142
Configure HTML5 Connectivity	145
Enable Support for Wyse Thin Client OS	147
Filter Access to a RAS Secure Client Gateway	147
Specifying a URL for Web Requests.....	148
Gateway Tunneling Policies	148
Viewing Gateway Summary and Metrics	149
Parallels HTML5 Client.....	150
Configure HTML5 Connectivity	150
Configure Themes.....	151
Common Theme Settings.....	151
HTML5 Client Theme Settings.....	152
Parallels Client for Windows Theme Settings	154
General Theme Tasks.....	154

Create Branded Windows Client for Mass Distribution.....	155
Delegating Session Management Permissions	155
Open Parallels HTML5 Client	157
Main Menu Options	159
Launching Remote Applications and Desktops	160
Using the Toolbar.....	161
Using the Toolbar on Desktop Computers.....	162
Using the Toolbar on Mobile Devices.....	164
Using the Remote Clipboard	165
Hiding Toolbar Items	166
HTML5 Gateway API.....	167
Parallels RAS Web Portal.....	169
RAS Web Portal: Prerequisites and Installation.....	169
Log In to RAS Web Portal.....	171
Farm Settings.....	173
General Settings.....	176
RAS Publishing Agent	182
Configuring RAS Publishing Agents	182
Secondary Publishing Agents	184
Managing Secondary Publishing Agents	186
Load Balancing.....	188
Resource Based & Round Robin Load Balancing.....	188
Load Balancing Advanced Settings	189
High Availability Load Balancing.....	190
Deploying a Parallels HALB Appliance	190
Configuring HALB in the RAS Console	192
Changing HALB Appliance Password.....	193

Universal Printing	195
Managing Universal Printing Settings	195
Universal Printing Drivers	196
Font Management.....	197
Universal Scanning.....	199
Managing Universal Scanning.....	199
Managing Scanning Applications	200
User Device Management.....	202
Inviting Users to Connect to Parallels RAS	202
Enabling Help Desk Support.....	202
Monitoring Devices.....	203
Windows Device Groups	204
Managing Windows Devices.....	205
Windows Desktop Replacement.....	209
Scheduling Windows Devices & Groups Power Cycles.....	212
Client Policies.....	213
Add a New Client Policy	214
Configure Session Settings.....	215
Configure Client Policy Options	226
Configure Control Settings	229
Configure Gateway Redirection	229
Client Policy Backward Compatibility.....	231
Enabling or Disabling Remote File Transfer.....	231
Server Level.....	232
HTML5 Gateway Level	232
Client Policy Level.....	232
Parallels RAS Reporting.....	233
Installing Parallels RAS Reporting.....	233
Advanced Settings	236

Viewing Reports	236
Parallels RAS Performance Monitor	239
Overview	239
Installing Parallels RAS Performance Monitor	240
Using Parallels RAS Performance Monitor	240
Configuring Performance Monitor Security	244
Connection and Authentication Settings	246
RAS Publishing Agent Connection Settings.....	246
Remote Session Settings	247
Restricting Access by Parallels Client Type and Build Number	249
Second Level Authentication	249
Using RADIUS	250
Using Deepnet.....	253
Using SafeNet	267
Configuring Exclusion Rules	269
Common Management Tasks	271
Recovery - Add a Root Administrator.....	271
Site Information.....	271
Site Settings.....	272
Upgrading RAS Agents	273
Licensing	274
Configure HTTP Proxy Settings	275
Configuring Notifications.....	276
Configuring Notification Handlers.....	276
Configuring Notification Scripts.....	278
Configuring SMTP Server Connection for Event Notifications	281
RAS Session Variables	281
Settings Audit	282
Maintenance and Backup.....	285
Exporting and Importing Farm Settings via Command Line	285

Problem Reporting and Troubleshooting	287
Suggest a Feature	288
Appendix.....	289
Port Reference	289
Parallels Client	289
Web Browsers.....	290
RAS Secure Client Gateway	290
RAS Publishing Agent	291
RAS Console.....	292
RAS Agents: RD Session Host, VDI, Guest, Remote PC	293
HALB	293
Common Communication Ports	294
Active Directory and Domain Services Ports.....	294
Parallels Client URL Scheme	294
RAS Performance Counters.....	296
Index	298

CHAPTER 1

Introduction

Welcome to Parallels Remote Application Server (Parallels RAS), an integrated solution to virtualize your applications, desktops and data. Parallels RAS publishes applications and delivers remote and virtual desktops to any device on your network, anywhere.

In This Chapter

About Parallels RAS	11
About This Guide	12
Terms and Abbreviations Used in This Guide	12

About Parallels RAS

Parallels RAS provides vendor independent virtual desktop and application delivery from a single platform. Accessible from anywhere with platform-specific clients and web enabled solutions, like the Parallels RAS HTML5 Gateway, Parallels RAS allows you to publish remote desktops, applications and documents, improving desktop manageability, security and performance.

Parallels RAS extends Windows Remote Desktop Services by using a customized shell and virtual channel extensions over the Microsoft RDP protocol. It supports all major hypervisors from Microsoft, VMware, and other vendors enabling the publishing of virtual desktops and applications to Parallels Client.

The product includes powerful universal printing and scanning functionality, as well as resource-based load balancing and management features.

With Parallels Client Manager Module for Parallels RAS you can also centrally manage user connections and PCs converted into thin clients using the free Parallels Client.

How does it work?

When a user requests an application or a desktop, Parallels RAS finds a least loaded RD Session Host or a guest VM on one of the least loaded VDI hosts and establishes an RDP connection with it. Using Microsoft RDP protocol, the requested application or desktop is presented to the user.

Users can connect to Parallels RAS using Parallels Client (available at no charge), which can run on Windows, Linux, macOS, Android, Chrome, and iOS. Users can also connect via an HTML5 browser or Chromebook.

As newer versions of Windows keep on being developed as time goes by, you need to defend the migration cost to your business. Parallels RAS can help. Desktop replacement allows you to extend the lifespan of your hardware and delay migration to the latest OSs to a time that suits you best. The Parallels RAS solution allows you to be very flexible: you can lock machine configurations on the user side, placing your corporate data in an extremely secure position; or you can opt to allow users to run some local and remote applications. Parallels Client Desktop Replacement is able to reduce the operability of the local machine by disabling the most common local configuration options, while guaranteeing the same level of service and security afforded by thin clients, directly from your existing PCs.

About This Guide

This guide is intended for system administrators responsible for installing, configuring, and administering Parallels RAS. This guide assumes that the reader is familiar with Microsoft Remote Desktop Services and has an intermediate networking knowledge.

Terms and Abbreviations Used in This Guide

Term/Abbreviation	Description
RAS Console	<p>Parallels RAS Console.</p> <p>The RAS console is the primary interface you use to configure, manage, and run Parallels RAS. As an administrator, you use the RAS console to manage farms, sites, RD Session Hosts, published resources, client connections, etc.</p>
Category	<p>In the RAS console, categories are displayed in the left pane of the main window. Each category consists of a number of settings related to a specific task or operation.</p> <p>The categories include Start, Farm, Load Balancing, Publishing, Universal Printing, Universal Scanning, Connection, Client Manager, and others.</p>
Farm	<p>A Parallels RAS farm is a logical grouping of objects for the purpose of centralized management. A farm configuration is stored in a single database which contains information about all objects comprising the farm.</p> <p>A farm consists of at least one site, but may have as many sites as necessary.</p>
Site	<p>A site consists of at least one RAS Publishing Agent, RAS Secure Client Gateway (or multiple gateways), and RAS agents installed on RD Session Hosts, VDI hosts, and Windows PCs. Note that a given RD Session Host, VDI host, or PC can be a member of only one site at any given time.</p>

Licensing Site	<p>The site that manages Parallels RAS licenses in a Parallels RAS farm. By default, the server on which you install Parallels RAS becomes the Licensing Site. If you create additional sites later, you can designate any one of them as the Licensing Site.</p> <p>There can be only one Licensing Site in a given farm. All other sites are called secondary sites.</p> <p>Note: Parallels RAS updates or upgrades must be applied to the Licensing Site first.</p>
RAS Secure Client Gateway	<p>RAS Secure Client Gateway tunnels all traffic needed by applications on a single port and provides secure connections.</p>
HTML5 Client	<p>HTML5 client allows users to view and launch remote applications and desktops in a web browser. The HTML5 client functionality is a part of RAS Secure Client Gateway.</p>
Publishing	<p>The act of making items installed on a Remote Desktop Server, VDI host or Remote PC available to the users via Parallels RAS.</p>
RAS Publishing Agent	<p>RAS Publishing Agent provides load balancing of published applications and desktops.</p>
RAS RD Session Host Agent	<p>RAS RD Session Host Agent collects information from the MS RDS hosts required by the Publishing Agent and transmits to it when required.</p>
Remote PC Agent	<p>Remote PC Agent collects information from Remote PC hosts required by the Publishing Agent and transmits to it when required.</p>
RAS Guest Agent	<p>RAS Guest Agent collects information from the VDI desktop required by RAS Publishing Agent and transmits to it when required.</p>
RAS VDI Agent	<p>RAS VDI Agent collects information from the Parallels RAS Infrastructure and is responsible for controlling VDI through its native API. It also acts as a gateway between a RAS Secure Client Gateway, or the client in direct mode, and an RDP server from the guest VM or VDI depending on a VDI implementation.</p> <p>RAS VDI Agent is a part of RAS Publishing Agent, so it is installed when you install the Publishing Agent. This built-in RAS VDI Agent can be used to control multiple VDI hosts in a Parallels RAS farm.</p> <p>You can also install a dedicated RAS VDI Agent on a particular VDI host and use it to control that host only. See RAS VDI Agent dedicated below.</p>
RAS VDI Agent dedicated	<p>This RAS VDI Agent appears as an installation option in the Parallels RAS installer. It serves the same purpose as the built-in RAS VDI Agent described above. The difference is, you can only use a dedicated agent to control the VDI host on which it is installed. VDI configurations are described in detail in</p>

	the VDI chapter.
RDS	Remote Desktop Services is a Microsoft Windows component that makes applications and the entire desktop of a server running RDS accessible to a remote client device that supports Remote Desktop Protocol (RDP). RDS replaced Terminal Services beginning with Windows 2008 R2.
HALB	High Availability Load Balancing (HALB) is an appliance that provides load balancing for RAS Secure Client Gateways. Parallels HALB virtual appliance is available for the following hypervisors: Hyper-V, VMware, Citrix Hypervisor. HALB deployment is per site, which means that the same HALB deployment cannot be shared between sites. Multiple HALB deployments can run simultaneously, one acting as the master and others as slaves. The more HALB deployments a site has, the lower the probability that end users will experience downtime. Master and slave HALB deployments share a common or virtual IP address (VIP). Should the master HALB deployment fail, a slave is promoted to master and takes its place.
RAS PowerShell	Parallels RAS PowerShell allows you to perform Parallels RAS administrative tasks using PowerShell cmdlets. You can execute cmdlets in the Windows PowerShell console or you can write scripts to perform common Parallels RAS administrative tasks. A complete guide to Parallels RAS PowerShell is available on the Parallels website together with other Parallels RAS documentation.
RAS REST API	Parallels RAS comes with various APIs to help you develop custom applications that integrate with it. The RAS REST API is one of them.
RAS Web Admin Console	RAS Web Admin Console is an HTML5 browser-based application that lets you manage Parallels RAS.
RAS Web Administration Service	A Web service that provides the user interface for RAS Web Admin Console and implements RESTful Web services for the RAS REST API (see above).

CHAPTER 2

Installing Parallels RAS

This chapter describes how to install and activate Parallels RAS.

In This Chapter

System Requirements	15
Install Parallels RAS	19
Log In and Activate Parallels RAS	20

System Requirements

Before installing Parallels RAS, please verify that your hardware and software meet or exceed hardware and software requirements described below. Please note that although Parallels RAS can be used in Workgroup environment, Parallels recommends using Active Directory to manage users, groups, and machine accounts via group policies.

Hardware Requirements

Parallels RAS is extensively tested on both physical and virtual platforms. The minimum hardware requirements approved to run Parallels RAS are outlined below.

- Physical Machines – Dual Core Processor and a minimum of 4GB RAM.
- Virtual Machines – Two Virtual Processors and a minimum of 4GB of RAM.

The server hardware requirements to install and configure Parallels RAS can vary according to end-user requirements.

Typically for an installation of 30 users or under, Parallels RAS can be installed on one high specification server and the resources published directly from it. For more than 30 users, multiple servers may be required.

The below should be considered during the planning stage of a Parallels RAS deployment:

- High specification servers should be used, consisting of multiple CPU cores, a high specification disk transfer rate and plenty of RAM.
- A hypervisor-based virtual machine can be used as long as the resources needed to serve end-users are calculated accordingly.

- It is recommended that RD Session Hosts do not exceed 50 users per RD Session Host in usage.
- It is recommended that RAS Secure Client Gateway does not exceed 1000 users per server for incoming connections using the Gateway SSL mode.
- When planning VDI Hypervisor resource requirements, extra requirements such as RAM usage per virtual machine and disk space should be taken into account.

For port requirements, please see the **Port Reference** section (p. 289).

Software Requirements

RAS Publishing Agent and RAS Secure Client Gateway

RAS Publishing Agent and RAS Secure Client Gateway are supported on the following operating systems:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016 and Windows Server 2016 Server Core.

Note: Parallels RAS should NOT be installed on a domain controller or any other server where a DHCP server is running.

RAS RD Session Host Agent

RAS RD Session Host Agent is supported on the following operating systems:

- Windows Server 2003 SP1 and newer
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2. Note that Server Core installation option is NOT supported.
- Windows Server 2016 and newer must be installed as Server with Desktop Experience.

RAS VDI Agent

RAS VDI Agent is supported on the following operating systems:

- Windows Server 2008
- Windows Server 2008 R2

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

VMware, Nutanix, and Xenserver can use Windows-based RAS VDI agent either integrated into RAS Publishing Agent or installed separately on Windows Server 2012 R2 and Windows Server 2016.

RAS Guest Agent

- Windows 7 and newer
- Windows Server 2008 R2 and newer

Remote PC Agent

- Windows 7 and newer.
- Windows Server 2008 R2 and newer.

Parallels RAS PowerShell

Windows Server 2008 with Service Pack 2 and newer. Windows Management Framework 3.0 must also be installed.

Parallels RAS Console

- Windows Server 2008 and newer
- Windows 7 and newer

RAS HTML5 Gateway

- Windows Server 2008 R2 or higher. Note that RAS HTML5 Gateway will NOT work with Windows Server 2008 (plain, not R2).

Parallels Client

Parallels Client is approved for the following operating systems (both 32 bit and 64 bit systems are supported, where applicable):

- Windows 7, 8.x, 10
- Windows Server 2003 SP1 and newer
- Windows Embedded
- macOS 10.11 and newer
- iOS 9.0 and newer

- Android 4.4 and newer
- Chrome OS

Supported Linux distributions (x64 versions only):

- Ubuntu 16.04
- Ubuntu 18.04
- Linux Mint 19
- Debian 9.5.0
- Fedora 28
- CentOS 7.5

Announcement: Parallels RAS Upcoming Version System Requirements

This is an advance notice about phasing out some of the components in the upcoming versions of Parallels RAS. Please read it to plan your IT strategy accordingly.

Within the next 6–8 months, version 17 of Parallels RAS will be deprecating 32-bit architecture that is no longer supported by software vendors, as well as discontinuing support for certain operating systems. These changes will be made to align Parallels RAS infrastructure to the latest trends and to improve overall performance.

The following describes the components that will be phased out and the operating systems that will no longer be supported in certain cases.

Parallels Client

- 32-bit Parallels Client for Linux will be discontinued. Only the 64-bit version will be available in Parallels RAS v17 and later.
- Parallels Client for Linux will no longer support ARM (all versions) and Raspberry Pi (all versions).
- Parallels Client for Windows will no longer support Windows Server 2003. For server operating systems it will be available on Windows Server 2008 R2 and newer. Support for Windows workstations remains the same: Windows 7 and newer.

Parallels RAS Components

- 32-bit RAS Secure Client Gateway will be discontinued. Only the 64-bit version will be available in Parallels RAS v17 and later.
- 32-bit RAS Publishing Agent will be discontinued. Only the 64-bit version will be available in Parallels RAS v17 and later.
- Parallels RAS Web Portal will not be supported in Parallels RAS v17 and later.

Operating system support

- Windows Server 2003 will no longer be supported for publishing from RD Session Hosts.
- Parallels RAS Console will no longer support Windows Vista and Windows Server 2008. It will support Windows 7 and newer for workstations, or Windows Server 2008 R2 and newer for server operating systems.

Parallels RAS Upgrade Planning

Parallels RAS customers can still use the features listed above in their existing Parallels RAS v16.5 infrastructure until February 28, 2021. For more information, please see the end-of-life announcement at <https://kb.parallels.com/en/123002>.

Install Parallels RAS

To install Parallels RAS:

- 1 Make sure you have administrative privileges on the computer where you are installing Parallels RAS.
- 2 Double click the `RASInstaller.msi` file to launch the Parallels RAS installation wizard.

Note: If you see a message that begins with "This version of Parallels RAS is for testing purposes only", it means that it's not an official build and should NOT be used in a production environment.

- 3 Follow the instructions and proceed to the **Select Installation Type** page. Select from the following:
 - **Parallels Remote Application Server.** The default installation that will install all necessary components for a fully functional Parallels RAS farm on the same machine.
 - **Custom.** Select and install only the components that you require. You can select individual components after you click **Next**. Note that if a component cannot be installed on the current server, it will not be available for installation. See **Software Requirements** (p. 16).
- 4 Click **Next**.
- 5 Review the notice on the **Important Notice** wizard page. If there's a port conflict on your computer, the information will be displayed here. You can resolve the conflict later.
- 6 Click **Next**.
- 7 On the **Firewall Settings** page, select **Automatically add firewall rules** to configure the firewall on this computer for Parallels RAS to work properly. See **Port Reference** for details. (p. 289)
- 8 Click **Next** and then click **Install**. Wait for the installation to finish and click **Finish**.

When you need to install a particular Parallels RAS component on a different server, run the installation wizard again, select **Custom** and choose the component(s) you wish to install.

Log In and Activate Parallels RAS

After you've installed Parallels RAS, run the RAS Console and activate your new Parallels RAS farm.

Start the Parallels RAS Console

By default, the Parallels RAS Console is launched automatically after you click **Finish** on the last page of the installation wizard. To launch the console manually, navigate to **Start > Apps > Parallels** and click on **Parallels Remote Application Server Console**.

When the Parallels RAS Console is launched for the first time, you are presented with the login dialog. In the dialog, specify the following:

- **Farm:** A Parallels RAS farm to connect to. Enter the FQDN or IP address of the server where you have RAS Publishing Agent installed.
- If you've installed the Parallels Single Sign-On component when installing the RAS Console, you will see the **Authentication type** field from which you can select whether to log on using your credentials or SSO. If you reboot after the installation and select SSO, select **Single Sign-On** and then click **Connect**. Your Windows credentials will be used to log in to the RAS farm. If you select **Credentials**, enter your credentials as described below.
- **Username:** A user account with administrative privileges on the server where Parallels RAS is installed (usually a domain or local administrator). The account name must be specified using the UPN format (e.g. `administrator@domain.local`). The specified user will be automatically configured as the Parallels RAS administrator with full access rights.
- **Password:** The specified user account password.
- If you select the **Remember credentials** option, this dialog will not be shown the next time you launch the Parallels RAS Console.

The **Edit Connections** button opens a dialog where you can manage your RAS connection. This dialog becomes useful if this is not the first time you are connecting to one or more of your RAS farms. The left pane of the dialog displays RAS farms to which previously connected (you can remove a farm from the list by clicking the **[-]** icon if you no longer need it). The right pane displays at least the master Publishing Agent for the selected farm. If you've added a secondary Publishing Agents to a farm, you can add it to this list by clicking the **[+]** icon and typing its hostname or IP address (click the "recycle" icon to verify the agent status). This way the RAS Console will try to connect to the master Publishing Agent first and if it fails (e.g. the agent is offline or cannot be reached), it will try to connect to the secondary Publishing Agent. For more information about secondary Publishing Agents, please see **Parallels RAS Publishing Agents** chapter (p. 182).

When you are done entering the connection information, click the **Connect** button to connect to the Parallels RAS farm.

Sign in to Parallels My Account

To activate Parallels RAS, you must register for a Parallels business account. After you logged in to Parallels RAS, you'll see the **Sign In to Parallels My Account** dialog. If you already have an account, type the email address and password you used to register the account and click **Sign In**.

Note: If you use an HTTP proxy server on your network, you will see a dialog asking you to configure the proxy server connection settings. Click the **Configure Proxy** button. In the dialog that opens, select one of the following: **Use system proxy settings** (the default proxy settings from the Internet Explorer will be used) or **Manual HTTP proxy configuration** (specify the settings manually). If your proxy configuration changes, you can re-configure it later by navigating to **Administration > Settings** and clicking the **Configure Proxy** button.

If you don't have a Parallels business account, you can register for one as follows:

- 1 In the **Sign In to Parallels My Account** dialog, click **Register**. The **Register Parallels My Account** dialog opens.

If you have an existing 2X Remote Application Server license and are upgrading to the new Parallels RAS, the **Register Parallels My Account** dialog will be prefilled with the information from your existing license. If you don't have an existing license (or if you've installed Parallels RAS on a new server), you need to fill in the registration information as described in the next step.

- 2 Enter your name and email address, choose and type a password, and enter your company info (all fields are required).
- 3 Click **Register** to register an account. This will create a personal account for yourself and a business account for your organization to which you will be assigned as administrator.

Activate Parallels RAS

After you sign in to Parallels My Account, the **Activate Product** dialog opens asking you to activate the Parallels RAS farm.

If you already have a Parallels RAS license key, select the **Activate using license key** option and enter the key in the field provided. You can click the button next to the field to see the list of subscriptions and/or permanent license keys you have registered in Parallels My Account. If the list is empty, it means that you don't have any subscriptions or license keys and need to purchase one first.

Note: You can manage your Parallels RAS license using the **Licensing** category in the Parallels RAS console. The management tasks include viewing the license information, switching to a different Parallels My Account, and activating the Parallels RAS farm using a different license key. For more information, please see the **Licensing** section (p. 274).

If you don't have a Parallels RAS license key, you have the following options:

- Purchase a subscription online by clicking the **Purchase a license** link.
- Activate Parallels RAS as a trial by selecting the **Activate trial version** option.

After entering a license key (or selecting to activate a trial version), click **Activate**. You should see a message that the Parallels RAS farm was activated successfully. Click **OK** to close the message box.

The first dialog that you see informs you that you have no servers configured that can be used to host published resources. This means that to begin using Parallels RAS, you need at least one RD Session Host, VDI host, or a Remote PC configured. We'll talk about configuring a Parallels RAS farm in the next chapter. For now, click **OK** to close the message box. You will then see the **Applying Settings** dialog. Wait for the initial configuration of Parallels RAS to complete and click **OK**. You will now see the main Parallels RAS Console window where you can begin configuring the Parallels RAS farm.

Read on to learn how to quickly add an RD Session Host, publish resources, and invite your users to Parallels RAS.

CHAPTER 3

Getting Started with Parallels RAS

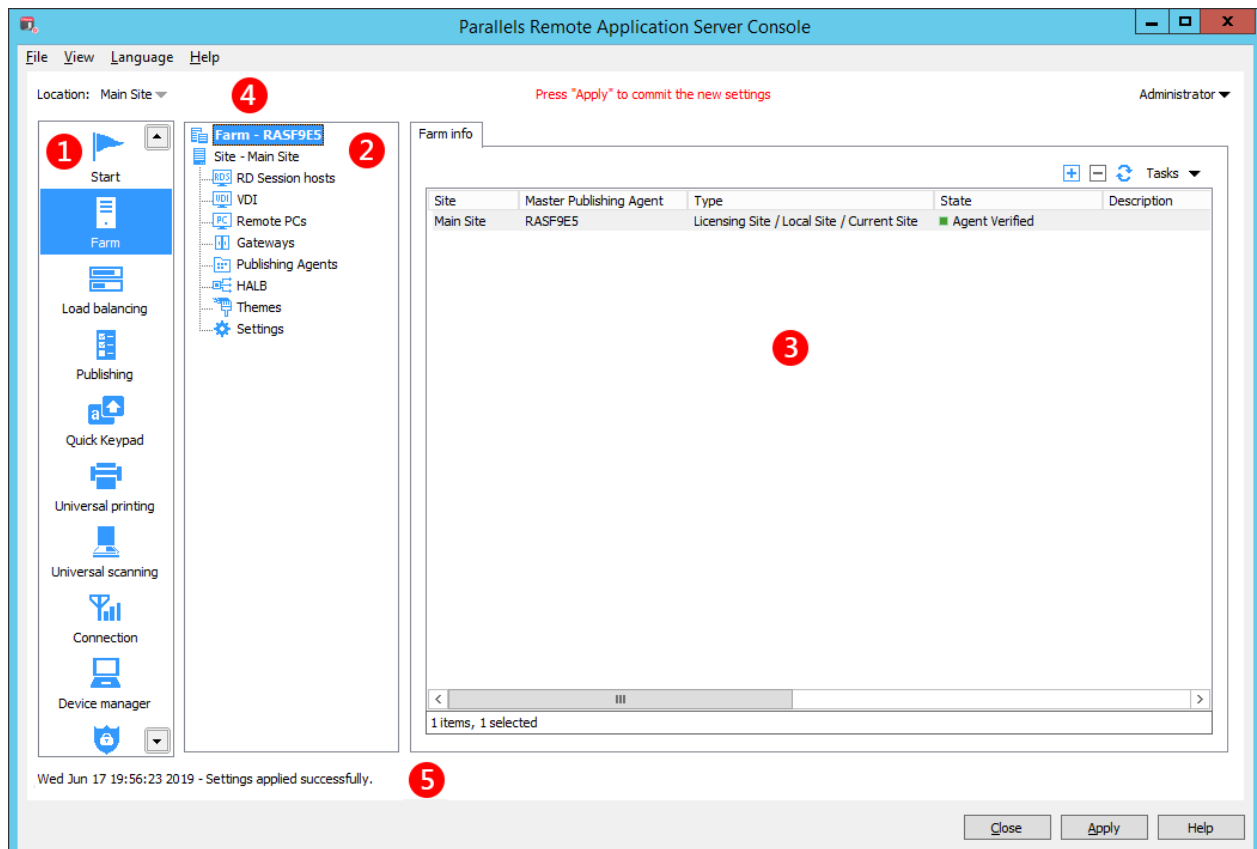
This chapter will help you get started with Parallels RAS. Read it to learn how to use the Parallels RAS Console and how to set up a simple RAS environment.

In This Chapter

The Parallels RAS Console	23
Set Up a Basic Parallels RAS Farm	24

The Parallels RAS Console

The Parallels RAS Console is a Windows application used to configure and administer a Parallels RAS farm.



The Parallels RAS Console consists of the following sections:

- 1 This section lists categories. Selecting a category will populate the right pane with elements relevant to that category.
- 2 This section (the middle pane) is available only for the **Farm** and the **Publishing** categories. The navigation tree allows you to browse through objects related to that category.
- 3 This section displays the selected object or category properties, such as servers in a farm or published application properties, etc.
- 4 The information bar at the top of the console displays the name of the site you are currently logged in to on the left side. If you have more than one site, you can switch between them by clicking the drop-down menu (the site name) and choosing a desired site.

Your administrator account name is displayed on the right side. Clicking on the name opens a drop-down menu from which you can initiate a chat with other administrators, show current sessions, and log off from the console.

The **Press 'Apply' to commit the new settings** message in the middle (in red) appears after you make any changes to any of the components or objects in the console. It reminds you that you have to commit these changes to Parallels RAS for them to become effective. Click the **Apply** button (at the bottom of the screen) to commit the changes.

- 5 The information bar at the bottom of the screen is used to display the most recent console notification (if one is available).

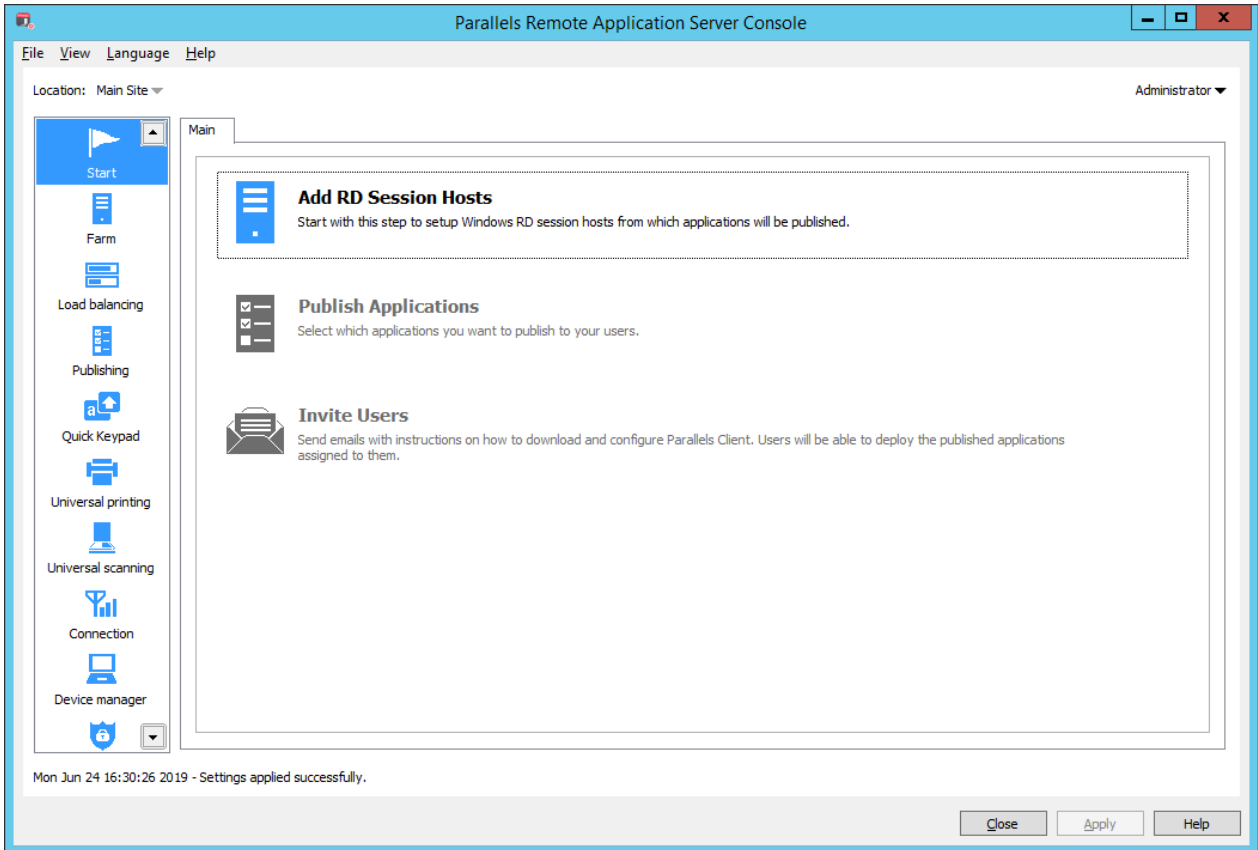
Set Up a Basic Parallels RAS Farm

In this section, we'll set up a basic Parallels RAS farm where all required components run on a single server.

To set up a Parallels RAS farm:

- 1 Log in to the Parallels RAS Console.

- 2 In the console, select the **Start** category. This category gives you access to three wizards that you can use to easily perform essential tasks, such as adding RD Session Hosts, publishing applications, and inviting users to Parallels RAS.

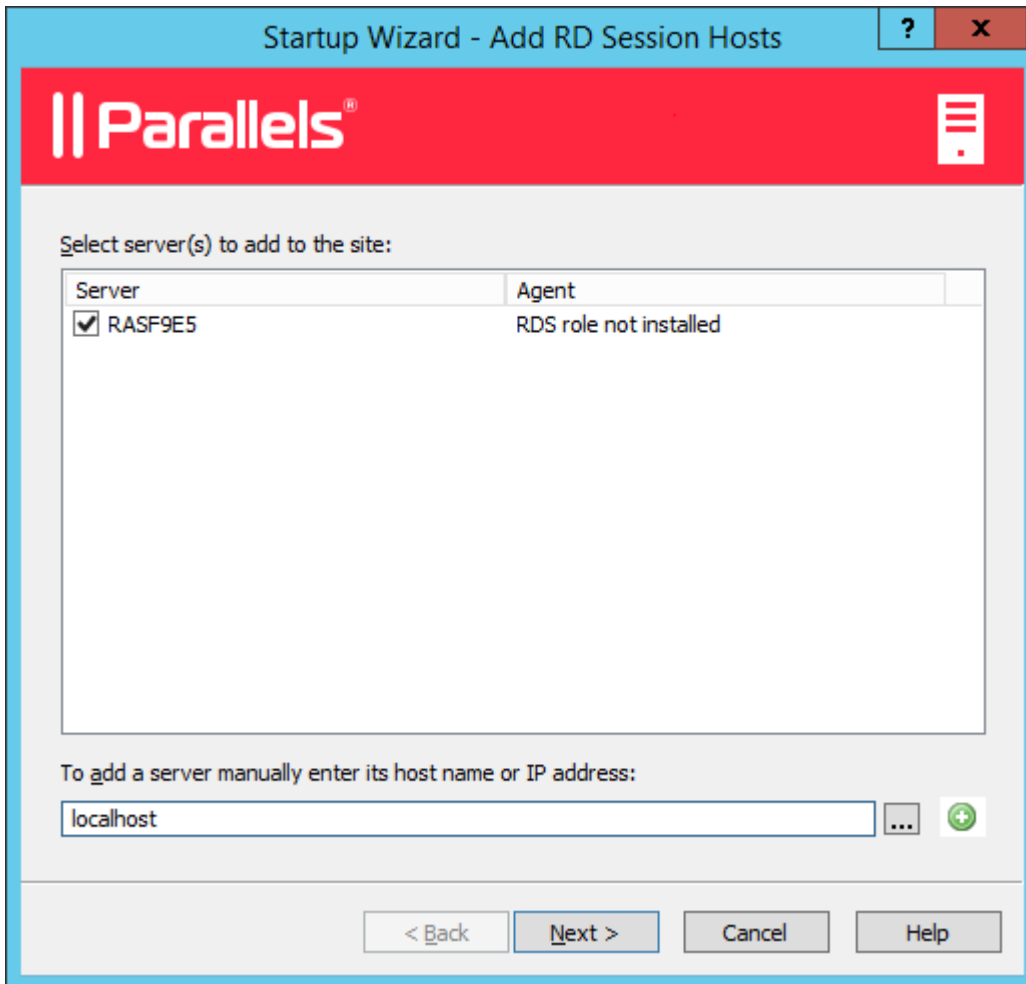


Add an RD Session Host

First, you need to add an RD Session Host to the farm. In this tutorial, we'll add the local server on which Parallels RAS is installed.

To add an RD Session Host to the farm:

- 1 Click **Add RD Session Hosts**. The **Add RD Session Hosts** wizard opens.



- 2 Select one or more servers. You can also type a server name in the edit box at the bottom of the page and then click the plus-sign icon. In this tutorial, we install all Parallels RAS components on a single server, so you can type "localhost".
- 3 Click **Next**.
- 4 On the next page, specify the following options:
 - **Add firewall rules.** Add firewall rules required by Parallels RAS in Windows running on the server. See **Port Reference** for details (p. 289).

- **Install RDS role.** Install the RDS role on the server if it's not installed. You should always select this option.
- **Enable Desktop Experience.** Enable the Desktop Experience feature in Windows running on the server. This option is enabled only if the Install RDS role option (above) is selected. The option applies to Windows Server 2008 R1/R2 and Windows 2012 R1/R2 on which the Desktop Experience feature is not enabled by default.
- **Restart server if required.** Automatically restart the server if necessary. You can restart the server manually if you wish.
- **Add server(s) to group.** Add the server (or servers) to a group. Select the desired group in the list box located below this option. Groups are described in detail in the **Grouping RD Session Hosts** (p. 56) section. If you are just learning how to use this wizard, you can skip this option.

5 Click **Next**.

6 The next page allows you to add users and groups to the Remote Desktop Users group in Windows running on the server. This is necessary for your Parallels RAS users to be able to access published resources hosted by an RD Session Host. To specify users and/or groups, select the option provided and then click the **[+]** icon. In the **Select Users or Groups** dialog, specify a user or a group and click **OK**. The selected user/group will be added to the list on the wizard page.

Note: If you skip this step and your users are not members of the Remote Desktop Users group on the RD Session Host, they will not be able to access resources published from this server. If you wish, you can add users to the group using the standard Windows tools. For more information, please consult the Microsoft Windows documentation.

7 Click **Next**.

8 On the next page, review the settings and click **Next**.

9 The **Install RAS RD Session Host Agent** dialog opens. Follow the instructions and install the agent. When the installation is finished, click **Done** to close the dialog.

10 Back in the wizard, click **Finish** to close it.

If you would like to verify that the RD Session Host has been added to the farm, click the **Farm** category (below the **Start** category in the left pane of the Parallels RAS Console window) and then click **RD Session Hosts** in the navigation tree (the middle pane). The server should be included in the **RD Session Hosts** list. The **Status** column may display a warning message. If it does, reboot the server. The **Status** column should now say, "OK", which means that your RD Session Host is functioning properly.

Read on to learn how to publish an application from an RD Session Host (p. 27)

Publish Applications

Now that you have an RD Session Host added to the RAS farm, you can publish applications from it.

To publish an application:

- 1 In the Parallels RAS Console, select the **Start** category and click the **Publish Applications** item in the right pane.
- 2 The **Publish Applications** wizard opens.
- 3 On the first page of the wizard, select one or more servers from which the application should be published. You can select all servers, server groups, or individual servers.
- 4 Click **Next**.
- 5 On the next page, select one or more applications you want to publish.

If you've selected more than one server on the previous screen, the **Show applications not available on all target servers** option becomes enabled. If the option is cleared (default), the folder tree will contain applications that are available on each and every server that you selected. If the option is enabled, the tree will contain applications that may be available on some server(s), but not on the others.

- 6 Click **Next**. Review the summary information and click **Next** again.
- 7 Click **Finish** when ready.

To verify that an application has been successfully published, select the **Publishing** category in the RAS Console. The application should be included in the **Published Resources** list (the middle pane).

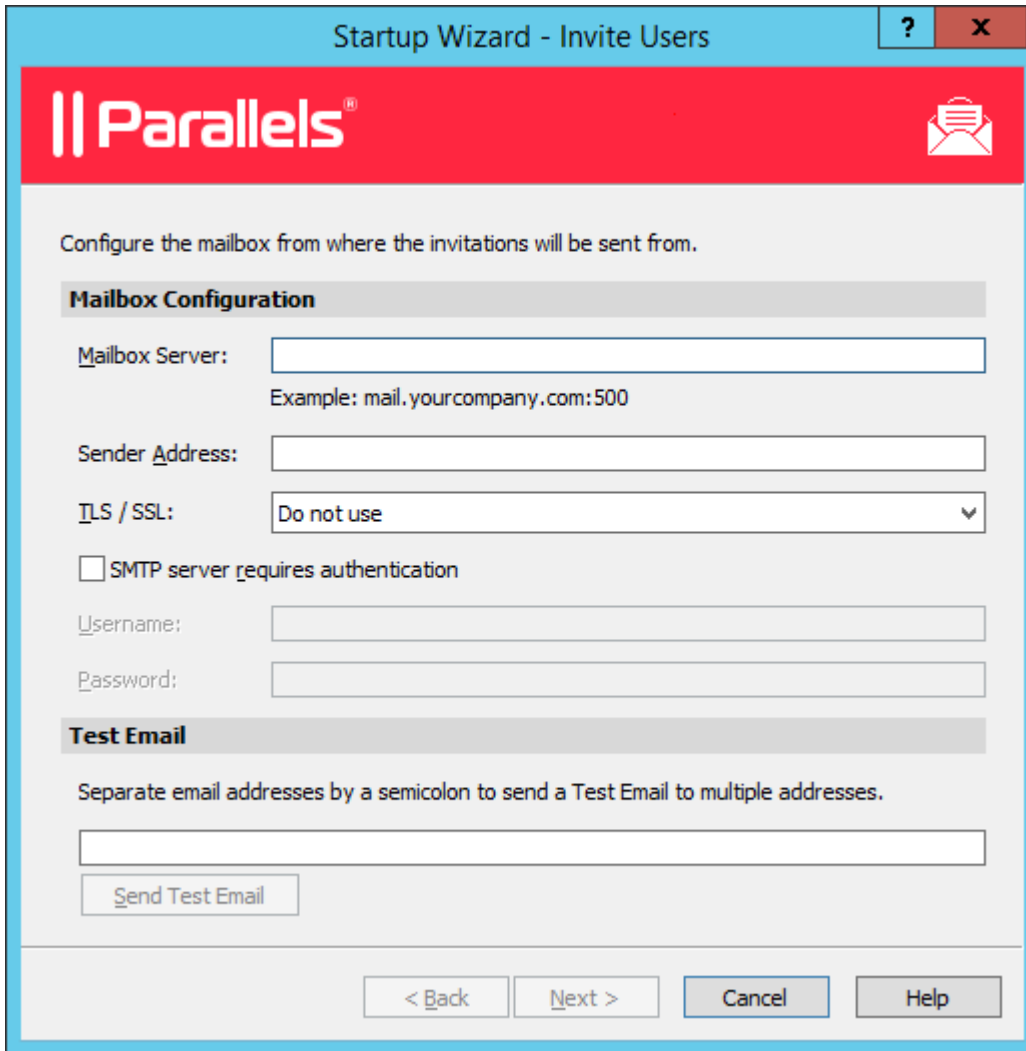
Invite Users

Your Parallels RAS farm is now fully operational. You have an RD Session Host and published application(s). All you need to do now is invite your users to install the Parallels Client software on their devices and connect to the Parallels RAS farm.

To invite users:

- 1 In the Parallels RAS Console, select the Start category and click the **Invite Users** item.

2 The **Invite Users** wizard opens:



The screenshot shows the "Startup Wizard - Invite Users" dialog box. The title bar includes a question mark icon and a close button (X). The Parallels logo is in the top left, and an envelope icon is in the top right. The main content area is titled "Configure the mailbox from where the invitations will be sent from." and is divided into two sections: "Mailbox Configuration" and "Test Email".

Mailbox Configuration

Mailbox Server: [Text Field]
Example: mail.yourcompany.com:500

Sender Address: [Text Field]

TLS / SSL: [Dropdown Menu] (Do not use)

SMTP server requires authentication

Username: [Text Field]

Password: [Text Field]

Test Email

Separate email addresses by a semicolon to send a Test Email to multiple addresses.

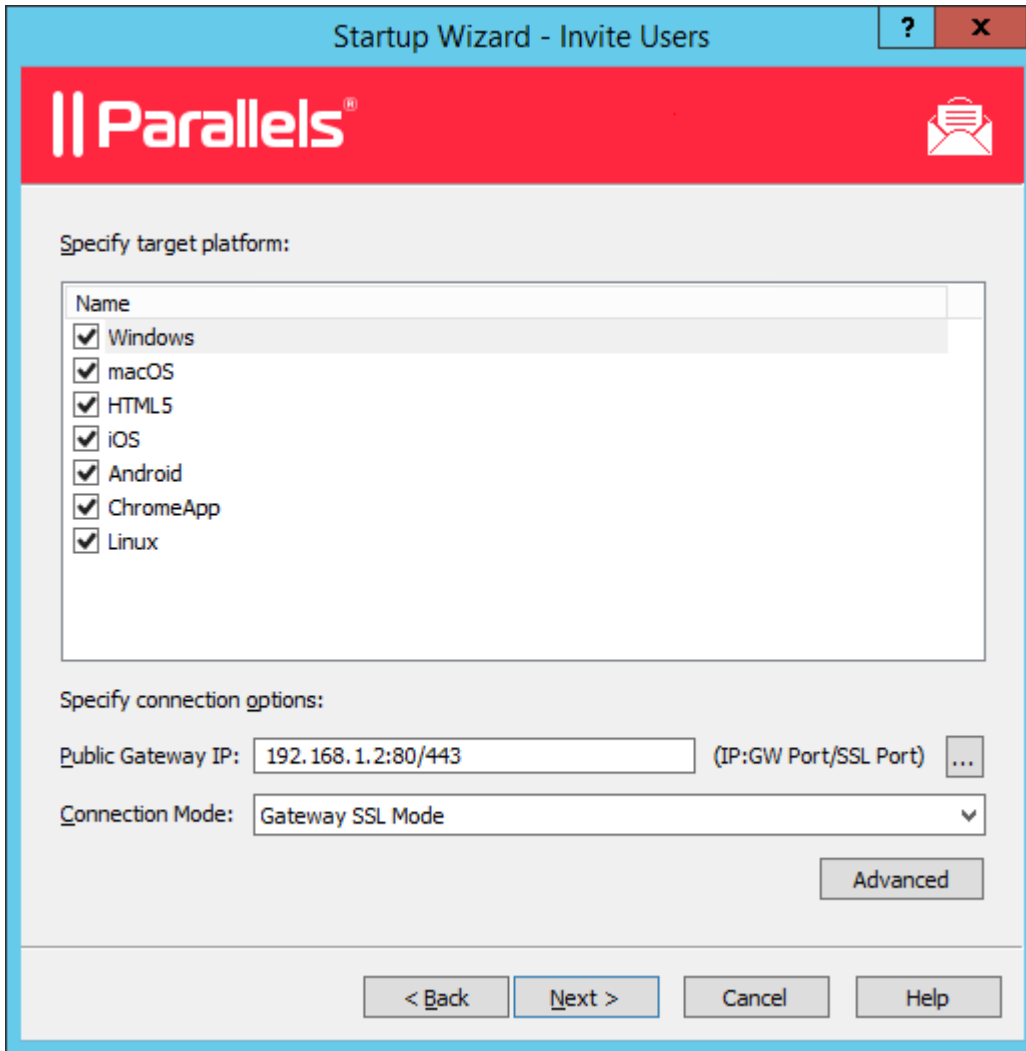
[Text Field]

[Send Test Email Button]

Navigation buttons at the bottom: < Back, Next >, Cancel, Help.

- 3 Specify the mailbox information that should be used to send invitation emails to users:
- **Mailbox Server:** Enter the mailbox server name. For example, mail.company.com:500
 - **Sender Address:** Enter the email address.
 - **TLS / SSL:** Choose whether to use the TLS/SSL protocol.
 - **SMTP server requires authentication:** Select this option if your SMTP server requires authentication. If it does, also type the username and password in the fields provided.
- 4 In the **Test Email** section, type one or more email addresses to which a test email should be sent (separate multiple address with a semicolon). Click the **Send Test Email** button to send the email.
- 5 Click **Next**.

6 On the next page of the wizard, specify target devices and connection options:



- In the target devices list, select the types of devices to send an invitation to. Each target device of a particular type will receive an email with instructions on how to download, install, and configure the Parallels Client software on that device type.
- In the **Public Gateway IP** field, specify the RAS Secure Client Gateway FQDN or IP address. Please note that this can be a public IP address so it can be reached by a remote user. You can click the [...] button to select a gateway from the list.
- In the **Connection Mode** drop-down list, select the RAS Secure Client Gateway connection mode. Please note that SSL modes require the gateway to have SSL configured. More information can be found in the **Configuring RAS Secure Client Gateway** (p. 140) section.
- Click the **Advanced** button to open the **Advanced Settings** dialog. This dialog allows you to specify a third-party credential provider component. If you use such a component to authenticate your users, specify its GUID in this dialog. For more information, see **Configure Client Policy Options > Single Sign-On** (p. 226).

7 Click **Next**.

- 8 On the next page, specify the email recipients. Click the [...] button to select users or groups.

Startup Wizard - Invite Users

Parallels

Specify the list of recipients:

ras-testing@gmail.com

Review the invitation e-mail:

Dear %RECIPIENT%,

You have been invited by %SENDER% to connect to Parallels Remote Application Server.

%INSTRUCTIONS%

%MANUALINSTRUCTIONS%

Thanks,

Preview Default

< Back Next > Cancel Help

- 9 Review the invitation email template displayed in the **Review the invitation e-mail** box. You can modify the template text as needed. The template also uses variables, which are explained below.
- %RECIPIENT% — Specifies the name of a recipient to whom the email message is addressed.
 - %SENDER% — The sender's email address that you specified in the first step of this wizard when you configured the outgoing email server settings.
 - %INSTRUCTIONS% — Includes a custom URL hyperlink for automatic configuration of Parallels Client. For technical information about the URL, see **Parallels Client URL Scheme** (p. 294).
 - %MANUALINSTRUCTIONS% — Includes instructions for manual configuration of Parallels Client.

The variables are defined dynamically depending on the type(s) of the target devices and other settings. Normally, you should always include them in the message, so your users will receive all the necessary instructions and links. To preview the message, click the **Preview** button. This will open the HTML version of the message in a separate window. This is the email message that your users will receive.

- 10** Click **Next**, review the settings that you specified and click **Next** again to send the invitation email to users.

When users receive the invitation email, they will follow the instructions that it contains to install and configure Parallels Client on their devices. Once that's done, the users will be able to connect to Parallels RAS and launch published resources.

Conclusion

In this tutorial, we have configured a simple Parallels RAS farm with a single RD Session Host and one published application. We then configured a mailbox for outgoing emails and sent an invitation email to end users with instructions on how to install Parallels Client, connect to the Parallels RAS farm, and run the published application. Essentially, we've created a fully functional Parallels RAS farm serving remote applications to end users.

If you wish, you can repeat the tutorial and add more RD Session Hosts, publish more applications, or send an invitation email to users who use different types of devices. The instructions remain essentially the same.

The rest of this guide explains in detail how to configure and use various features of Parallels RAS.

CHAPTER 4

Parallels RAS Farm and Sites

Parallels RAS farm is a logical grouping of objects for the purpose of centralized management. A farm configuration is stored in a single database which contains information about all objects comprising the farm. A site is the next level grouping in the farm hierarchy which contains servers and other objects providing connection and remote application services.

In This Chapter

Connecting to a Parallels RAS Farm.....	33
About Sites	35
Viewing Sites in the RAS Console	36
Adding a Site to the Farm	38
Replicating Site Settings	38
Managing the Licensing Site	40
Managing Administrator Accounts	40

Connecting to a Parallels RAS Farm

If you have more than one Parallels RAS farm in your organization, you can use the same Parallels RAS Console instance to manage any of them. By default, the Parallels RAS Console is installed on the same server where you install other Parallels RAS components, but you can install the console on any computer on your network.

Connecting to a Parallels RAS farm for the first time

When you open the Parallels RAS Console for the first time, it displays the logon dialog on which you need to specify the following farm connection properties:

- **Farm:** FQDN or IP address of the server on which Parallels RAS Publishing Agent is installed. If all Parallels RAS components are installed on the same server (e.g. localhost), specify that server.
- **Username:** The username of the Parallels RAS administrator (e.g. local computer Administrator).
- **Password:** The administrator password.

After entering the connection properties, click **Connect** to connect to the farm and open the RAS Console.

Note that the **Edit Connections** button will not display any information on first connect (it is used to edit farm connections that already exist), so you can ignore it at this point. We will talk about using this button closer to the end of this section.

Connecting to a different Parallels RAS farm

When you need to connect to a different Parallels RAS farm, you first need to log off from the Parallels RAS Console in order to see the logon dialog again. To do so:

- 1 In the Parallels RAS Console, click on the arrow icon next to your user name in the upper right-hand corner and then choose **Log Off** in the context menu.
- 2 The console will close and the RAS logon dialog will open. The dialog will be pre-populated with the current farm connection properties.
- 3 To connect to a different farm, type the FQDN or IP address of the server where the other farm is located. Once again, this should be the server where you have the RAS Publishing Agent installed.
- 4 Specify a username and password and click **Connect**. The Parallels RAS Console will connect to the farm using the connection properties that you specified.

Switching between Parallels RAS farms

After you connect to more than one farm from the same Parallels RAS Console instance, you can switch between them as follows:

- 1 In the Parallels RAS Console, click on the arrow icon next to your user name in the upper right-hand corner and then choose **Log Off** in the context menu.
- 2 The console will close and the RAS logon dialog will open. In the dialog, expand the **Farm** drop-down list and select a farm to connect to. If the list doesn't contain any other farms, it means that you haven't connected to them from this console yet, in which case you need to enter the farm connection properties. Once you connect to a farm at least once, it will remain in this list, so you can switch between farms quicker.

Editing Parallels RAS farm connections

As was mentioned in the beginning of this section, the RAS logon dialog has the **Edit Connections** button. When you click it, the **Manage Parallels RAS Farm Connections** dialog opens.

On the left side of the dialog, the **Farm Connections** pane lists Parallels RAS farms to which you connected at least once in the past. If a connection is no longer relevant, you can remove it by selecting it and clicking the "minus sign" icon at the top. Once a connection is removed, it will no longer appear in the RAS logon dialog.

On the right side of the dialog, the **Publishing Agents** pane lists RAS Publishing Agents for the selected farm connection. By default, the master Publishing Agent is included in the list, but you can add more Publishing Agents if needed. When connecting to a farm, the Parallels RAS Console will try the master Publishing Agent first. If a connection cannot be established, it will try other Publishing Agents in the order they are listed in the **Publishing Agents** pane. To add a Publishing Agent to the list, click the "plus sign" icon and then specify the server FQDN or IP address.

About Sites

A Parallels RAS farm consists of at least one site, but may have as many sites as necessary.

Sites are often used to separate management and/or location functions. For example, by creating a site, you can delegate permissions to a site administrator without granting them full farm permissions. Or you can have separate sites for different physical locations with the ability to copy the same settings to each site while using RD Session Hosts, VDI hosts, or PCs that are closer to end users or (depending on your needs) to back-end servers. For instance, it would make sense for a client/server application querying a database to be published from an RD Session Host which is located closer to the database server.

Each site is completely isolated from other sites within the same farm. The farm simply groups sites logically and stores configuration properties of each site (and the objects that comprise it) in a single database. Sites don't communicate with each other and don't share any objects or data. The only exception to this rule is the RAS Licensing Site which periodically communicates with other sites to obtain statistics.

Individual object settings in a given site can be replicated to all other sites. This does not mean that settings will be shared between sites. The settings that you choose will simply be applied to other sites. For more information, see the **Replicating Site Settings** section (p. 38).

When you install Parallels RAS, a farm with a single site is created automatically. This first site becomes the RAS Licensing Site and the host for the main Parallels RAS configuration database. When you add more sites to the farm, the data in this database is automatically synchronized with every site that you add. When changes are applied to a particular site, the main configuration database is automatically updated to reflect the changes.

Each site must have at least the following components installed in order to publish remote applications and desktops for end users:

- Master RAS Publishing Agent
- RAS Secure Client Gateway
- RD Session Host, VDI, or PC

When you install Parallels RAS using default installation options, the master RAS Publishing Agent and the RAS Secure Client Gateway are automatically installed on the server on which you perform the installation. You can then add one or more RD Session Hosts to the site to host published resources. You can also add more sites to the farm if needed and configure individual components for each site as you desire.

Viewing Sites in the RAS Console

To view existing sites, open the Parallels RAS Console and select the **Farm** category in the left pane. Existing sites are listed in the right pane.

Note: The **Farm** node will only be visible to an administrator who has full permissions to manage the farm. For more information about farm/site permissions, please refer to **Managing Administrator Accounts** (p. 40).

The **Farm** category displays the configuration of only one site at a time. If you log in as the farm administrator, the configuration of the RAS Licensing Site will be displayed. If you log in as an administrator who has access to a specific site (but not the farm), the configuration of that site will be displayed.

Current site

Click on the **Farm** item in the middle pane to view the list of available sites. The site which configuration is currently loaded in the console is marked as "Current Site" in the **Type** column. The column also displays other site attributes. For example, "Licensing Site / Local Site / Current Site".

Switching between sites

To switch to a particular site, select **Farm** in the middle pane, then right-click the site in the right pane and choose **Switch to this site**. The site configuration will be loaded into the RAS Console.

Renaming the site

To rename a site, right-click it and choose **Rename Site**.

Site configuration and health view

When you select the **Site** node in the middle pane, the **Site Info** tab page in the right pane displays the list of Parallels RAS components that have been configured for the site with interactive performance monitoring metrics for each component. The list is organized as follows:

- **RD Sessions Hosts.** Lists existing RD Session Hosts.
- **VDI** (if configured). Lists existing VDI hosts.

- **Remote PCs** (if one or more are configured). Lists existing Remote PCs.
- **Gateways**. Lists existing RAS Secure Client Gateway servers.
- **Publishing Agents**. Lists existing RAS Publishing Agent servers.

To collapse or expand a component group, click an "arrow up" or "arrow down" icon on the right side of the list. Note that if no servers of a particular type have been added to the site, the group name will not be displayed in the list.

The following information is displayed for each component (the information is updated at an interval of approximately 2 minutes):

- **Address**. Server FQDN or IP address.
- **Agent**. Indicates whether the agent software is installed on the server and is functioning properly.
- **CPU %**. Current CPU utilization.
- **RAM %**. Current RAM utilization.
- **Disk Read Time %**. Disk read time.
- **Disk Write Time %**. Disk write time.
- **Sessions**. The number of currently active user sessions.
- **Preferred PA**. The name of the RAS Publishing Agent designated as preferred for this server.
- **Operating System**. Operating system version installed on the server.
- **Agent Version**. The agent version installed on the server.

You can customize this view by clicking **Tasks > Monitoring Settings**. This opens a dialog where you can specify which colors should be used to display different performance counters and their values.

Configuring a component

To configure a component, do one of the following:

- While the **Site** node is selected in the middle pane, right-click a component in the right pane and choose **Show in the editor**.
- Select a component category in the middle pane (e.g. RD Session Hosts, VDI hosts, etc.).

Using the Site Designer

Select the **Site** node in the middle and then click the **Designer** tab page in the right pane. The tab page displays a visual representation of the site infrastructure. Use the icons at the top to add more components to the diagram as desired. Note that adding a component to the diagram will actually add it to the site. Double-click a component to view and configure it in a corresponding editor.

Adding a Site to the Farm

To add a site to the farm:

- 1** In the RAS Console, select the **Farm** category in the left pane and then select the farm in the middle pane.
- 2** In the **Tasks** drop-down menu (the right pane, above the Site list), click **Add** (or click the **+** icon).
- 3** In the **Add Site** dialog:
 - In the **Site** field, specify a site name.
 - In the **Server** field, specify the IP address or FQDN of the server where the Master Publishing Agent and Secure Client Gateway should be installed.
 - Select the **Add an SSL certificate and enable HTML5 Gateway** option to automatically create a self-signed certificate, enable SSL, and enable HTML5 support. For more info, please see **Enable HTML5 Support on the Gateway** (p. 145).
- 4** Click **Next**.
- 5** The **Site Master Properties** dialog opens. First, it verifies if RAS Publishing Agent is installed on the specified site server. If it isn't, it will indicate this in the **Status** field.
- 6** Click the **Install** button to install the agent.
- 7** In the **Install RAS Publishing Agent** dialog, highlight the server name on which the RAS Publishing Agent is to be installed.
- 8** (Optional) Select the option **Override system credentials** to specify and use different credentials to connect to the server and install the agent.
- 9** Click **Install** to install the publishing agent and gateway. Click **Done** once it has been successfully installed.

Once a new site is created, you can view and manage its configuration by right-clicking the site in the RAS Console and choosing **Switch to this Site**.

Replicating Site Settings

Site-specific settings configured for a given site can be replicated to all other sites in a farm. Refer to the table below for the information about which settings can be replicated to other sites.

Category	Section	Options
Farm	VDI > RAS templates	Auto removal timeout of guest VMs that fail preparation.
Farm	VDI > Desktops	Auto removal timeout.
Farm	Settings > Auditing	All settings

Farm	Settings > Global Logging	Logging settings
Farm	Settings > URL Redirection	All settings.
Load Balancing	Load Balancing	All settings.
Publishing	Application	Site defaults are replicated. Other settings (name, description, icon, etc.) are global and are common to all sites.
Publishing	Shortcuts	All settings.
Publishing	Extensions	All settings.
Publishing	Licensing	All settings.
Publishing	Display	All settings.
Publishing	Filtering (all types except Gateway)	All settings.
Universal Printing	Universal Printing	Printer renaming.
Universal Printing	Printer Drivers	All settings.
Universal Printing	Fonts Management	All settings.
Universal Scanning	WIA	Scanner renaming.
Universal Scanning	TWAIN	Scanner renaming.
Universal Scanning	TWAIN > TWAIN Applications	Scanning applications.
Connection	Authentication	All settings.
Connection	Settings	All settings.
Connection	Second Level Authentication	All settings.
Connection	Allowed Devices	All settings.
Reporting	Reporting Engine	Reporting engine type.
Reporting	Engine specific settings	All settings.

To replicate site settings to all other sites, select **Farm** / <site> / **Settings** and then select the **Replicate settings** option (at the bottom of the **Auditing** tab). Please note that this option is disabled if you have just one site in the farm.

Overriding Site Replicated Settings

If an administrator who has permissions to enable or disable replication settings makes a change to a specific setting, such setting is replicated to all other sites. If an administrator has access to a particular site only, upon modifying site settings which have been replicated, the replicated settings are overridden and the option **Replicate Settings** is automatically cleared, therefore such settings will no longer be replicated to other sites.

Managing the Licensing Site

The licensing site should always be online even if you have other sites in your farm. If your licensing site goes offline, your other sites can still use the maximum number of individual licenses included in your subscription but only for a period of 72 hours. During this time, you need to do one of the following:

- Restore your licensing site.
- Promote a different site to be the licensing site in the farm (see below for instructions).

Please note that if the licensing site is offline from 48 to 72 hours and back online three times per month, you will be required to re-activate it using your Parallels RAS licensing key after the third time.

To promote a secondary site to be the licensing site in the farm:

- 1** In the RAS Console, navigate to **Farm > Farm**.
- 2** In the right pane select a site and then click **Tasks > Set as licensing site**.
- 3** You will be asked to activate the new licensing site using your Parallels RAS license. Follow the instructions and activate the site.

Managing Administrator Accounts

You can have more than one administrator in Parallels RAS. At least one administrator (called the root administrator) must be present at all times. Other administrators can be configured as a root administrator or power administrators. A root administrator always has full permissions. A power administrator can be configured to have limited permissions to manage certain sites and categories.

Additionally, you can create administrators who can manage specific user groups (called custom administrators). For example, if multiple groups in your organization share the same Parallels RAS resources, you can delegate session management permissions to an administrator of a specific group.

Read on to learn how to create and manage administrator accounts.

Adding an Administrator Account

To add an administrator account to the Parallels RAS farm:

- 1** In the RAS Console, select the **Administration** category and then click the **Accounts** tab in the right pane.
- 2** Click the **Tasks** drop-down menu and choose **Add** (or click the **[+]** icon).

- 3 The **Account Properties** dialog opens.
- 4 Click the [...] button next to the **Name** field. In the **Select User or Group** dialog, select a user or a group.
- 5 Specify an email address and mobile phone number. Both fields are optional and are disabled if the account specified in the **Name** field is a group.
- 6 In the **Permissions** drop-down list select one of the following:
 - **Root administrator.** Select this option to give the user full permissions to manage the farm.
 - **Power administrator.** This option allows you to grant specific permissions to the administrator. To specify permissions, click the **Change Permissions** button.
 - **Custom administrator.** Creates a special type of administrator to delegate session management permissions.
- 7 In the **Receive system notifications via** drop-down list, select **Email** to send all system notifications to the specified email address, or select **None** to disable email system notifications for this account.
- 8 Click **OK** to add the new administrator account to the farm.

Administrator Account Permissions

When you click the **Change Permissions** button in the **Administrator Properties** dialog, the following happens depending on what is selected in the **Permissions** field:

- **Root administrator.** The **Change Permission** button is disabled because the root administrator always has full permissions.
- **Power administrator.** The **Account Permissions** dialog opens. In the left pane, select one or more sites for which to grant the permissions. In the right pane, select specific permissions. See **Permissions** below for details.
- **Custom administrator.** The **Account Permissions** dialog opens displaying one or more themes for which the administrator can manage sessions.

Permissions

- **Allow viewing of Site information.** Can view (but not necessarily modify) site information.
- **Allow site changes.** Can modify the following categories: Site, Load Balancing, Universal Printing, Universal Scanning. This option is disabled if the **Allow viewing of Site information** option is cleared.
- **Allow session management.** Can manage running sessions. This option is disabled if the **Allow viewing of Site information** option is cleared.
- **Allow publishing changes.** Can modify the Publishing category.
- **Allow connection changes.** Can modify the Connection category.
- **Allow viewing of RAS reporting.** Can view reports generated by the RAS Reporting engine.

- **Allow client management changes.** Can modify the Client Manager category.

In the **Global permission** box, select the **Allow policies changes** option to allow the administrator to modify the Policies category.

Enabling or disabling an administrator account

To enable or disable a Parallels RAS administrator account, select or clear the checkbox in front of the account name. You can also enable or disable an account in the **Administrator Properties** dialog by selecting or clearing the **Enable account** option (to open the dialog, right-click an account and choose **Properties**). A disabled account cannot be used to log in to the RAS Console. If it's a group, the members of that group will not be able to log in to the Parallels RAS Console either.

Managing Administrator Accounts

To view existing administrator accounts, select the **Administration** category in the RAS Console. The **Accounts** tab lists existing accounts and their properties, including:

- **Group or user name.** Account name, which can be a user or group name.
- **Type.** Account type. Can be one of the following: **User**, **Group**, **Group User**. The **User** and **Group** are self-explanatory. The **Group User** is a user who receives Parallels RAS administrative permissions via a group membership. When you initially add a group to the list of Parallels RAS administrators, its members are not displayed on the **Accounts** tab. As soon as a member of the group logs in to Parallels RAS, the account name is added to the list of administrators as a **Group User** and remains there. Note that you cannot change Parallels RAS permissions for such an account individually outside the group permissions.
- **Permissions.** A security role assigned to an administrator.
- **Email.** Email address.
- **Mobile.** Mobile phone number.
- **Group.** Group name. This column has a value for Group Users only (see the **Type** column description above).
- **Last Modification By.** The name of the user who modified this account in Parallels RAS the last time.
- **Changed On.** The last account modification date.
- **Created By.** The name of the user who created this account in Parallels RAS.
- **Created On.** The date when this account was added to Parallels RAS.
- **ID.** Internal Parallels RAS ID.

Modifying an account

To modify an account:

- 1 Right-click an account and choose **Properties** in the context menu.
- 2 Use the **Administrator Properties** dialog to modify the necessary information. For more info, see **Adding an Administrator Account** (p. 40).

Handling Locked Objects

When an administrator is working with an object (e.g. a tab page) in the Parallels RAS Console, the object is locked for all other administrators. Therefore, upon trying to access a locked object, an administrator will be alerted with an error that the object is locked and will not be able to access it.

A root administrator (but not power or custom administrator) can release a locked object as follows:

- 1 On the **Administration > Accounts** tab, click the **Tasks** drop-down menu and choose **Show Sessions**.
- 2 In the **Sessions** dialog, select the administrator who is locking an object and then click the **Send Message** icon (at the top).
- 3 If the administrator doesn't reply and doesn't release the object, you have an option to click **Log Off**, which will log them off and will unlock the category.

Configure RAS Console Idle Sessions

If you have a number of administrators using the RAS Console to manage the same farm, you can configure when an idle RAS Console session should be disconnected. By default, when an administrator opens the console and connects to a farm but then forgets to log off and goes away, the session will stay active indefinitely possibly locking some of the categories for other administrators. You can change that by specifying the time period after which an idle session will be disconnected (thus unlocking the categories).

To configure idle sessions:

- 1 In the RAS Console, navigate to **Administration > Settings**.
- 2 Locate the **Miscellaneous** section (at the bottom) and choose a desired time period in the **Reset idle RAS Console session after** drop-down box.

When a session stays idle for close to the specified time period, the administrator (session owner) will be notified a few minutes in advance that the session is about to be disconnected. If the administrator chooses to stay connected, the time period is reset. If the administrator does nothing, the session will be disconnected when the time expires.

Using Instant Messaging for Administrators

Parallels RAS administrators logged on to the same farm can communicate with each other using a built-in instant messenger.

To use the instant messenger:

- 1 In the RAS Console, select the **Administration** category.
- 2 Expand the drop-down menu next to your name (top-right corner of the console screen) and click **Chat**.
- 3 The **Parallels Remote Application Server Chat** window opens.

To send a message:

- 1 Type the message text in the lower input panel.
- 2 In the **Logged on administrators** list box, select a specific administrator or **All** to send the message to an individual or all logged on administrators.
- 3 Click **Send**.

Your message history is displayed in the **Messages** panel. To clear the history, click **Clear All**.

You can also view the chat history listing all messages between all administrators (not just your own messages). To do so, select the **Administration** node in the console and then select the **Chat History** tab.

Joining Customer Experience Program

Parallels Customer Experience Program helps us to improve the quality and reliability of Parallels RAS. If you accept to join the program, we will collect information about the way you use Parallels RAS. We will NOT collect any personal data, like your name, address, phone number, or keyboard input.

To join the program:

- 1 In the RAS Console, select the **Administration** category.
- 2 In the right pane, click the **Settings** tab.
- 3 Select the **Participate in the Customer Experience Program** option.

After you join the program, CEP will automatically start to collect information about how you use Parallels RAS. Data collected from you and other participants is combined and thoroughly analyzed to help us improve Parallels RAS.

Note: This note applies to Parallels RAS v16.5 only. If you install or upgrade an older version of Parallels RAS to version 16.5, the CEP participation will be automatically turned on. You can turn it off if you like at any time. When a newer version of Parallels RAS is released and you upgrade to that version, your selection whether to participate in CEP will be kept.

CHAPTER 5

RD Session Hosts

RD Session Hosts are used to host published resources (applications, desktops, documents, etc.) in a Parallels RAS farm. Read this chapter to learn how to add, configure, and administer RD Session Hosts.

In This Chapter

RD Session Host Types.....	46
Adding an RD Session Host	47
Viewing RD Session Hosts.....	50
Configuring an RD Session Host.....	51
Grouping and Cloning RD Session Hosts.....	56
Using Scheduler.....	60
Managing Sessions	62
Managing Logons	64
Publishing from an RD Session Host.....	65
Publishing Containerized Applications.....	71
Viewing Published Resources Hosted by RD Session Hosts.....	75

RD Session Host Types

Beginning with Parallels RAS v16.5, you can create and add to a RAS farm the following types of RD Session Hosts:

- Individual servers. These can be physical boxes or virtual machines treated as physical servers.
- Virtual machines (VMs) created from a RAS Template, which is a part of RAS Virtual Desktop Infrastructure (VDI). The main advantage of using VMs is the ability to create as many of them as you require from a single RAS Template. RD Session Hosts based on a RAS Template are described in the **Grouping and Cloning RD Session Hosts** section (p. 56).

Considering that RAS Template is a part of RAS VDI, some aspects of creating, provisioning, and managing RD Session Hosts based on a RAS Template differ from the regular RD Session Hosts (individual servers). For example, RAS Template-based hosts are added to a farm automatically from a group, not manually by the administrator. There are some other differences which are described in various sections of this chapter. When reading these sections, please pay attention to whether or not a particular functionality applies to RD Session Hosts based on a RAS Template.

Adding an RD Session Host

RD Session Host requirements

An RD Session Host must have the Remote Desktop Services (RDS) role installed. You can install RDS right from the RAS Console, as described later in this section.

To push install the RAS RD Session Host Agent on a server, the following requirements must be met:

- The firewall must be configured on the server to allow push installation. Standard SMB ports (139 and 445) need to be open. See also **Port Reference (p. 289)** for the list of ports used by Parallels RAS.
- SMB access. The administrative share (\\server\c\$) must be accessible. Simple file sharing must be enabled.
- Your Parallels RAS administrator account must have permissions to perform a remote installation on the server. If it doesn't, you'll be asked to enter credentials of an account that does.
- The RD Session Host should be joined to an AD domain. If it's not, the push installation may not work and you will have to install the Agent on the server manually. See **Installing the Agent manually** section (p. 48).

Note: The rest of this section applies to regular RD Session Hosts only. If you are looking for the information on how to add an RD Session Host based on a RAS Template, see **Grouping and Cloning RD Session Hosts** (p. 56).

Quickly add an RD Session Host

You can quickly add an RD Session Host to a site from the **Start** category in the RAS Console. This process is described in the **Setting Up a Basic Parallels RAS Farm** section (p. 24).

The rest of this section describes how to add an RD Session Host from the **Farm** category. Compared to using the **Start** category, this process consists of more steps but gives you more options.

Adding an RD Session Host

To add an RD Session Host:

- 1** In the RAS Console, navigate to **Farm > Site > RD Session Hosts**.
- 2** Click **Tasks > Add**.
- 3** In the dialog that opens, specify the following:

- **Server.** Specify the server IP address or FQDN.
 - **Add firewall rules.** Automatically configure the firewall on the server to meet Parallels RAS requirements. See **Port Reference (p. 289)** for the list of ports used by Parallels RAS.
 - **Install RDS role.** Install the RDS role in Windows running on the server.
 - **Enable Desktop Experience.** Enable the Desktop Experience feature in Windows running on the server. This option is enabled only if the **Install RDS role** option (above) is selected. The option applies to Windows Server 2008 R1/R2 and Windows 2012 R1/R2 on which the Desktop Experience feature is not enabled by default.
 - **Restart server if required.** Restart the server if necessary. Please note that this option is ignored if a restart is pending on a local machine (i.e. the restart of a local machine will not be forced).
 - **Specify users or groups to be added to the Remote Desktop Users group.** This option allows you to add Parallels RAS users or groups to the Remote Desktop Users group in Windows running on the server. This is necessary for your Parallels RAS users to be able to access published resources hosted by an RD Session Host. If a Parallels RAS user is not a member of the Remote Desktop Users group on a given RD Session Host, they will be denied access to its published resources. Select this option and then use the **[+]** icon below it to specify users or groups.
- 4 Click **Next**.
 - 5 In the next step, a checking is performed if the RAS RD Session Host Agent is installed on the server.
If the agent is not installed:
 - a Click **Install** to push install the agent.
 - b In the **Installing RD Session Host Agent** dialog, select the target server.
 - c (Optional) Select the **Override system credentials** option to specify different credentials to connect to the server. You need to do this if the RAS admin account that you are using doesn't have permissions to perform a remote installation on the target server.
 - d Click **Install** to install the agent. Click **Done** once the agent is installed. If the push installation of the RAS RD Session Host Agent fails for any reason, you have an option to install it manually. Please see **Installing the Agent Manually** (p. 48).
 - 6 In the **Agent Information** dialog, click **Add** to add the RD Session Host to the Parallels RAS farm.
 - 7 Click **Apply** in the Parallels RAS Console to commit the new settings.

Installing the Agent Manually

You may need to install the RAS RD Session Host Agent manually if the automatic push installation cannot be performed. For instance, an SMB share may not be available or the firewall rules may interfere with the push installation, etc.

Installing RAS RD Session Host Agent Manually

- 1 Log in to the server where the RAS RD Session Host Agent is to be installed using an administrator account and close all other applications.
- 2 Copy the Parallels RAS installation file (`RASInstaller.msi`) to the server and double-click it to launch the installation.
- 3 Once prompted, click **Next** and accept the End-User license agreement.
- 4 Specify the path where the RAS RD Session Host Agent should be installed and click **Next**.
- 5 Select **Custom** and click **Next**.
- 6 Click on **RAS RD Session Host Agent** and select **Entire Feature will be installed on local hard drive** from the drop-down menu.
- 7 Ensure that all other components are deselected and click **Next**.
- 8 Click **Install** to start the installation.
- 9 Click **Finish** once the installation is finished.

The RAS RD Session Host Agent doesn't require any configuration. Once the agent is installed, highlight the server name in the RAS Console and click **Troubleshooting > Check Agent** in the **Tasks** drop-down menu to update the server status.

Uninstalling RAS RD Session Host Agent

To uninstall RAS RD Session Host Agent from a server:

- 1 Navigate to **Start > Control Panel > Programs > Uninstall a Program**.
- 2 Find **Parallels Remote Application Server** in the list of installed programs.
- 3 If you don't have any other Parallels RAS components on the server that you want to keep, right-click **Parallels Remote Application Server** and then click **Uninstall**. Follow the instructions to uninstall the program. You may skip the steps below.
- 4 If you have other RAS components that you want to keep on the server, right-click **Parallels Remote Application Server** and then click **Change**.
- 5 Click **Next** on the Welcome page.
- 6 On the **Change, repair, or remove** page, select **Change**.
- 7 On the next page, select **Custom**.
- 8 Select **RAS RD Session Host Agent**, then click the drop-down menu in front of it, and click **Entire feature will be unavailable**.
- 9 Click **Next** and complete the wizard.

Viewing RD Session Hosts

To view the list of RD Session Hosts for the current site:

- 1 In the RAS Console, navigate to **Farm** / <site-name> / **RD Session Hosts**.
- 2 The available RD Session Hosts are displayed on the **RD Session Hosts** tab in the right pane.

You can filter the **RD Session Hosts** list as follows:

- 1 Click the magnifying glass icon, which is located on a toolbar above the list.
- 2 An extra row is displayed at the top of the list where you can type a string in one or more columns that will be used to filter the list.
- 3 For example, if you want to search for a server by its name, enter the text in the **Server** column. You can type the entire server name or the first few characters until a match is found. The list will be filtered as you type and only the matching server(s) will be displayed.
- 4 If you type a filter string in more than one column, they will be combined using the logical AND operator.
- 5 To remove the filter and display the complete list, click the magnifying glass icon again.
- 6 If you click the magnifying glass icon one more time, you'll see that the filter that you specified earlier is still there. To remove it completely, simply delete the filter string(s) from the column(s).

Viewing RD Session Host summary

In addition to the RD Session Hosts editor described above, you can also see the summary about the available RD Session Hosts. To do so:

- 1 In the RAS Console, select the **Farm** category and then select the **Site** node in the middle pane.
- 2 The available servers are displayed in the **RD Session Hosts** group in the right pane.
- 3 To go to the RD Session Host editor (described above), right-click a server and choose **Show in the Editor**.

For additional info, see **Sites in the RAS Console** (p. 36).

Available menu options

You can perform a number of tasks on the an RD Session Host using menus. To do so, click the **Tasks** drop-down menu and choose a desired option, or right-click a host and choose an option from the context menu.

Please note that not all menu options are available for RD Session Hosts based on a RAS Template. If an option is not available for this host type, it will be either disabled or hidden. These include:

- **Remove from group.** Hosts based on a RAS Template can only be removed from a group using the **Group Properties** dialog.
- **Assign to group.** Group assignment is performed automatically for RAS Template-based hosts.
- **Delete.** Deleting a host (which is a VM) can only be done on the RAS Template level (the **Guest VM List** dialog).
- **Properties.** RD Session Hosts of this type don't have individual properties. Some essential properties are inherited from **Default Server Properties** (see View and Modify RD Session Host Properties > Agent Settings (p. 52)).
- **Control** (logon commands). Drain mode is managed automatically by the group to which a RAS Template-based host belongs.

Configuring an RD Session Host

This section describes how to configure and manage an existing RD Session Host.

Read on to learn how to:

- Check RAS RD Session Host Agent Status (p. 51)
- Change an RD Session Host Site Assignment (p. 52)
- View and Modify RD Session Host Properties (p. 52)

Check RAS RD Session Host Agent Status

An RD Session Host must have RAS RD Session Host Agent installed in order to publish remote applications and desktop from it. In addition to this, Remote Desktop Services (formerly Terminal Services) must also be installed.

Normally when you add an RD Session Host to a site, the RD Session Host Agent and Remote Desktop Services are installed by default. However, if you skipped the installation (or uninstalled the agent or RDS from the server), you can check their status and take appropriate actions if needed.

To check the status of RD Session Host Agent and RDS, do the following:

- 1** First, check the **Status** column in the **RD Session Hosts** list. The column should display "OK". If so, the Agent is installed and functioning properly. If not, read on.
- 2** In addition to the description, the **Status** column uses a color code to indicate the agent status as follows:
 - Red — not verified
 - Orange — needs update
 - Green — verified

- 3 Right-click a server and click **Troubleshooting > Check agent** in the context menu. The **Agent Information** dialog opens.
- 4 If the agent is not installed on the server, click the **Install** button and follow the instructions on the screen.

After the agent installation is complete, you may need to reboot the RD Session Host. You can do it right from the Parallels RAS Console by selecting the server and clicking **Tasks > Control > Reboot**.

Change RD Session Host Site Assignment

You can assign an RD Session Host to a different site in your farm if needed. Please note that this functionality is only available if you have more than one site in your farm.

To change the site assignment:

- 1 Right-click an RD Session Host and then click **Change Site** in the context menu. The **Change Site** dialog opens.
- 2 Select a site in the list and click **OK**. The server will be moved to the **RD Session Hosts** list of the target site (**Farm / <new-site-name> / RD Session Hosts**).

View and Modify RD Session Host Properties

Note: The information in this section does NOT apply to RD Session Hosts based on a RAS Template. Hosts of that type don't have individual properties and are managed on the RAS Template level. For more information, see **Grouping and Cloning RD Session Hosts** (p. 56) and **Parallels RAS Templates** (p. 85).

To configure an RD Session Host:

- 1 In the RAS Console, navigate to **Farm / <site> / RD Session Hosts**.
- 2 Select a server and click **Tasks > Properties**.
- 3 The server properties dialog opens where you can configure the RD Session Host properties.

The rest of this section describes individual tab pages of the server properties dialog.

Properties

Select or clear the **Enable Server in site** option to enable or disable a server. By default, a server is enabled. A disabled server cannot serve published applications and virtual desktops to clients.

Other elements on this page are:

- **Server:** Specifies the server name.
- **Description:** Specifies the server description.

- **Change Direct Address:** Select this option if you need to change the direct address that Parallels Client uses to establish a direct connection with the RD Session Host.

Agent Settings

Each RD Session Host in the farm has an RAS RD Session Host Agent installed through which it communicates with other Parallels RAS components. Use the **Agent Settings** tab page to configure the agent.

To use default settings, select the **Inherit default settings** option. The default settings are specified for the entire site. To view and modify these settings, click the **Edit Defaults** link.

If you want to specify custom settings for a given server, clear the **Inherit default settings** option and specify agent properties as follows:

- **Port.** Specifies a different remote desktop connection port number if a non-default port is configured on the server.
- **Max Sessions.** Specifies the maximum number of sessions that this server will handle. The maximum allowed value is 1000 sessions. The default value is 250.
- **Publishing Session Disconnect Timeout.** Specifies the amount of time each session remains connected in the background after the user has closed the published application. This option is used to avoid unnecessary reconnections with the server.
- **Publishing Session Reset Timeout.** This feature allows you to control how long it takes for a session to be logged off after it is marked as "disconnected".
- **Allow Client URL/Mail Redirection.** Select this option to allow "http" and "mailto" links to be opened using a local application on the client computer rather than the server resources. To configure a list of URLs which should not be redirected, navigate to the **URL Redirection** tab in the **Settings** node of a site.
- **Preferred Publishing Agent.** Select a Publishing Agent to which the RD Session Host should connect. This is helpful when site components are installed in multiple physical locations communicating through WAN. You can decrease network traffic by specifying a more appropriate Publishing Agent.
- **Allow 2XRemoteExec to send command to the client.** Select this option to allow a process running on the server to instruct the client to deploy an application on the client side. More about 2XRemoteExec in the **Using RemoteExec** subsection below.
- **Use RemoteApp if available.** Enable this option to allow use of remote apps for shell-related issues when an app is not displayed correctly. This feature is supported on the Parallels Client for Windows only.
- **Enable applications monitoring.** Enable or disable monitoring of applications on the server. Disabling application monitoring stops the WMI monitoring to reduce CPU usage on the server and network usage while transferring the information to RAS Publishing Agent. If the option is enabled, the collected information will appear in a corresponding RAS report. If the option is disabled, the information from this server will be absent from a report.

- **Allow file transfer command.** Allows you to enable or disable the remote file transfer functionality. For more information, see **Enabling or Disabling Remote File Transfer** (p. 231).
- **Allow local to remote drag and drop.** Enables the drag and drop functionality in a remote application. When this option is enabled, users can drag and drop files to a remote application on their local devices. For example, a user can drag and drop a file to the Acrobat Reader to open a PDF file. Or the user can drag and drop a file to Windows Explorer running on a remote server, etc.

Note: At the time of this writing, the drag and drop functionality is only supported on Parallels Client for Windows and Parallels Client for Mac.

Using 2XRemoteExec

2XRemoteExec is a feature that facilitates the servers ability to send commands to the client. This is done using the command line utility `2XRemoteExec.exe`. Command line options include:

Command Line Parameter	Parameter Description
<code>-s</code>	Used to run the 2XRemoteExec command in 'silent' mode. Without this parameter, the command will display pop up messages from the application. If you include the parameter, the messages will not be displayed.
<code>-t</code>	Is used to specify the timeout until the application is started. Timeout must be a value between 5000ms and 30000ms. Note that the value inserted is in 'ms'. If the timeout expires the command returns with an error. Please note that the application might still be started on the client.
<code>-?</code>	Shows a help list of the parameters that 2XRemoteExec uses.
<code>"Path for Remote Application"</code>	The Application that will be started on the client as prompted from the server.

2XRemoteExec examples:

The following command displays a message box describing the parameters that can be used.

```
2XRemoteExec -?
```

This command runs Notepad on the client.

```
2XRemoteExec C:\Windows\System32\notepad.exe
```

In this example, the command opens the `C:\readme.txt` file in the Notepad on the client. No message is shown and 2XRemoteExec would wait for 6 seconds or until the application is started.

```
2XRemoteExec C:\Windows\System32\notepad.exe "C:\readme.txt"
```

User Profile Disks

User profile disks are virtual hard disks that store user application data on a dedicated file share. This disk is mounted to the user session as soon as the user signs in to the RD Session Host, and unmounted when the user logs out.

To use default settings, select the **Inherit default settings** option. The default settings are specified for the entire site. To view and modify these settings, click the **Edit Defaults** link.

To use custom settings, clear the **Inherit default settings** option and specify the options described below.

Enable or disable user profile disks: Use the drop-down list box to specify whether to enable or disable user profile disks on the server. Select from the following options:

- **Do not change.** Keep the current server settings (default).
- **Enabled.** Enable user profile disks.
- **Disabled.** Disable user profile disks.

Disk location: In the text field provided, specify a network location where user profile disks should be created. Use the Microsoft Windows UNC format to specify a location (e.g. \\RAS\users\disks). Please note that the server must have full control permissions on the disk share.

Maximum size: Enter the maximum allowed disk size (in gigabytes).

User profile disks data settings: Click this button to open the **User Profile Disks Data Settings** dialog. In the dialog, you can specify which user folders should be stored on the user profile disk. Select one of the following:

- **Store all user settings and data on the user profile disk.** All folders, except those specified in the exclusion list, will be stored on the user profile disk. To add or remove folders to/from the exclusion list, click the **[+]** or **[-]** buttons.
- **Store only the following folders on the user profile disk.** Only folders specified in the inclusion lists will be stored on the user profile disk. There are two inclusion lists. The first one contains standard user profile folders (e.g. Desktop, Documents, Downloads, etc.) and allows you to select the folders that you want to include. The second list (below the first list) allows you to specify additional folders. Click the **[+]** or **[-]** buttons to add or remove folders.

Desktop Access

The **Desktop Access** tab page allows you to restrict remote desktop access to certain users.

To use default settings, select the **Inherit default settings** option. The default settings are specified for the entire site. To view and modify these settings, click the **Edit Defaults** link.

By default, all users who have access to remote applications on an RD Session Host can also connect to the server via a standard RDP connection. If you want to restrict remote desktop access to certain users, do the following:

- 1 On the **Desktop Access** tab page, select the **Restrict direct desktop access to the following users** option. If you have the **Inherit default settings** option selected, click the **Edit Defaults** link to see (and modify if needed) the default configuration. The rest of the steps apply to both the **Server Properties** and **Default Server Properties** dialogs.

- 2 Click the **Add** button.
- 3 Select the desired users. To include multiple users, separate them by a semicolon.
- 4 Click **OK**.
- 5 The selected users will appear in the list on the **Desktop Access** tab page.

Users in this list will still be able to access remote applications using Parallels Client, but will be denied direct remote desktop access to this server.

Note: **Computer Configuration / Administrative Templates / Windows Components / Remote Desktop Services / Remote Desktop Session Host / Connection / Allow users to connect remotely using remote desktop services** must be set to **Not configured**, otherwise it takes precedence.

Please note that members of the Administrator group will still be able to connect to the remote desktop even if they are included in this list.

RDP Printer

The **RDP Printer** tab page allows you to configure the renaming format of redirected printers. The format may vary depending on which version and language of the server you are using.

To use default settings, select the **Inherit default settings** option. The default settings are specified for the entire site. To view and modify these settings, click the **Edit Defaults** link.

The **RDP Printer Name Format** drop-down list allows you to select a printer name format specifically for the configured server.

Select the **Remove session number from printer name** and the **Remove client name from printer name** options to exclude the corresponding information from the printer name.

Grouping and Cloning RD Session Hosts

When you publish resources in Parallels RAS, you need to specify one or more servers that host them. Groups allow you to combine multiple RD Session Hosts and then publish the resources from the group instead of specifying individual servers.

The main benefits of using RD Session Host groups are as follows:

- They simplify the management of published resources and are highly recommended in multi-server environments.
- They allow you to use RD Session Hosts created from a RAS Template by utilizing the VDI functionality, which is available in Parallels RAS. More on this later in this section.

Note that an RD Session Host can be a member of one group only. You cannot add the same server to multiple groups.

Creating a group

To create an RD Session Host group:

- 1 In the RAS console, navigate to **Farm / <site> / RD Session Hosts**.
- 2 Click the **Groups** tab.
- 3 Click **Tasks > New Group** (or click the **[+]** icon). To modify an existing group, right-click it and then choose **Properties** in the context menu.
- 4 The **Group Properties** dialog opens where you can specify the group settings as described below.

On the **General** tab page, select **Enable Group in site** to enable the group. Type a name and description for the group.

You now need to add one or more servers to the group. You can do this by using the following options (both can be used at the same time):

- Specify a RAS Template on which the servers are based. This will include all RD Session Hosts that have been or will be created from a selected template. To do so, select the **RD session hosts based on a RAS Template** option and then select a template from the drop-down list. Note that you need to create a RAS Template of type RD Session Host before you can select it here. For more information, see the **Using RAS Templates** subsection below.
- Add servers manually one by one by clicking **Tasks > Add** and then selecting a server from the list. You can also add a server later by right-clicking it in the main list and choosing **Assign to group**.

Using RAS Templates

RAS Templates of type RD Session Host utilize the VDI functionality available in Parallels RAS. A template is based on a virtual machine (also known as VM or guest VM) running on a hypervisor. When you create a RAS Template, you select a preconfigured VM with the operating system and resources that you intend to publish already installed. Individual hosts (VMs) are then created as clones of the template. The clones can be created in advance or on as-needed basis (configurable when you create a template). This functionality allows you to essentially create and configure an RD Session Host running in a virtual machine and then create as many copies of it as you require.

For the complete information about using VDI in Parallels RAS see the **VDI** chapter (p. 77). Once you are familiar with adding and configuring a VDI host, read the **Parallels RAS Templates** section (p. 85) which explains how to create a RAS Template of type RD Session Host.

After you select a RAS Template in the **Group Properties** dialog, click the **RAS Template Settings** tab page to specify additional properties described below.

Send a request to the RAS Template when the workload threshold is above (%): Specifies the group workload threshold at which one or more additional servers (guest VMs) should be created from the template. The group workload percentage is calculated using the following formula:

Group Workload = (Current Sessions / Max Sessions) * 100

In the formula above:

- **Current Sessions** is the total number of all sessions on all servers in the group. This includes static (standalone) servers and servers created from the RAS Template (guest VMs). Note that servers that are disabled, being drained, or have the agent status of 'Not Verified' are NOT included in the calculation.
- **Max Sessions** is a setting that you specify in the **Default Server Properties** dialog and it's the maximum number of sessions allowed for the group.

Consider the following examples:

RAS Group 1 — mixed server types (static and guest VMs), different agent status:

- RDSH-1, Status: OK, Max Sessions 10, Current Sessions: 2, Type: Static
- RDSH-2, Status: Disabled, Max Sessions 20, Current Sessions: 0, Type: Static
- RDSH-3, Status: OK, Max sessions 10, Current Sessions: 4, Type: Guest VM
- RDSH-4, Status: Drain Mode, Max sessions 10, Current Sessions: 3, Type: Guest VM

For the group above, the workload is calculated as (Current Sessions / Max Sessions) * 100 or $((2 + 4) / 20) * 100 = 30\%$

Note that servers RDSH-2 and RDSH-4 are not included in the workload because the former has the agent disabled and the latter is in drain mode.

RAS Group 2 — mixed server types (static and guest VMs), different agent status:

- RDSH-1, Status: OK, Max Session 10, Current Sessions: 0, Type: Guest VM
- RDSH-2, Status: OK, Max Sessions 10, Current Sessions: 2, Type: Guest VM
- RDSH-3, Status: Not Verified, Max sessions 10, Current Sessions: 0, Type: Guest VM

Group Workload = (Current Sessions / Max Sessions) * 100 or $((0 + 2) / 20) * 100 = 10\%$

Please note that a group will always make sure that it has at least one server available, even if the workload is zero percent.

Number of servers to be added to the group per request: The number of servers that the template should create per single request from the group. This setting works together with the **Send a request to the RAS Template when the workload threshold is above (%)** setting described above. When a group sends a request to the template to create additional servers, the value specified here will determine the number of servers that will be created.

Max number of servers to be added to the group from the RAS Template: This option allows you to set a limit on how many servers in total can be added to the group from the template. A RAS Template can be shared between groups. By setting a limit for each group, you can ensure that the combined number of servers in each group will not exceed the template limit. Consider the following examples:

- If the RAS Template is used by a single group, then this number can be up to the "Maximum guest VMs" setting of the RAS Template.
- If two or more groups share the same RAS Template, then the combined number from all groups must be less or equal to the "Maximum guest VMs" settings of the RAS Template.

When you save the group, a validation will be performed against other groups (if any) and you will see an error message if the numbers don't match. Note that when a server cannot be created on request due to an error, a "RAS Template error" event is triggered and the administrator will receive an alert message.

Drain and unassign servers from group when workload is below (%): Specifies the group workload percentage value at which one or more servers should be switched to drain mode or unassigned from the group. The server(s) with the least number of sessions will be switched to drain mode. As soon as all users are logged off from a server, it is unassigned from the group. At that point, the server becomes available to other groups on demand.

Note: Parallels recommends setting viable timeouts for idle time and disconnected sessions either in Windows Group Policies or Default Server Properties to make the drain mode effective.

Removing a server from a group

To remove a regular RD Session Host from a group, do one of the following:

- On the **RD Session Hosts** tab page, right-click a server and choose **Remove from group**.
- On the **Groups** tab page, right-click a group and choose **Properties**. In the **Group Properties** dialog, select a server and click **Tasks > Delete**.

To remove an RD Session Host that was added to a group from a RAS Template:

- 1** Go to the **Groups** tab page.
- 2** Select a group and click **Tasks > Properties**.
- 3** In the **Group Properties** dialog, select a server and click **Tasks > Delete**.

Note that this is the only place in the RAS Console where you can remove an RD Session Host of this type from a group. Please also note that when you delete such a host, it is drained first and only then unassigned from the group, which may take a considerable amount of time.

After you create a group and later publish resources from it, you can view the list of resources by right-clicking a group and choosing **Show published resources** (or click **Tasks > Show Published Resources**). For more information, see **Viewing Published Resources Hosted by RD Session Hosts** (p. 75).

Using Scheduler

The **Scheduler** tab page in the **RD Session Hosts** view allows you to reboot or temporarily disable servers according to a schedule.

To create a new scheduler task or modify an existing one:

- 1 In the RAS Console, navigate to **Farm / <site> / RD Session Hosts**.
- 2 In the right pane, click the **Scheduler** tab.
- 3 To create a new task, click **Add** in the **Tasks** drop-down menu and select a desired task from the following options:
 - **Disable Server**
 - **Disable Server Group**
 - **Reboot Server**
 - **Reboot Server Group**

The **RDSH Schedule Properties** dialog opens. In the dialog, specify the following properties:

- Select **Enable Schedule** to enable the task.
- Specify the task name, target server (or server group if you've selected a group task), and an optional description.
- Specify the start date and time, duration, and scope (the **Repeat** property). If you select **Never** in the **Repeat** drop-down box, the task will run only once.
- The **Notify Users Message** section allows you to type a message that will be sent to the users before the task is executed (you can select the time period using the **Send message [] before action is triggered** drop-down list).

The **Options** section will have different options depending on the task type:

- If a task is **Disable Server** or **Disable Server Group**, the available options are **On Disable** and **Enforce schedule for currently inactive RD Session Hosts**. Use the **On Disable** option to specify how the active session states should be handled. Please note that disabling a server group with assigned template will drain and remove RD Session Hosts based on the template from group. See **Maintaining RD Session Hosts based on a RAS Template. (p. 97)**

If you enable the **Enforce schedule for currently inactive RD Session Hosts** option, the schedule will be applied to a currently inactive RD Session Host when it comes back online. If the option is disabled (default), the schedule will have no effect on such servers. Note that it is assumed that a server is inactive (offline) if it is disabled or cannot be reached over the network (registered on RAS Publishing Agent).

- If a task is **Reboot Server** or **Reboot Server Group**, the available options are **Enable Drain Mode** and **Force server reboot after** (the options work together). If you enable the drain mode, the following will happen. When the task triggers, new connections to a server will be refused but active connections will continue to run. A server will be rebooted when all active users end their sessions or when it's time to force reboot it, whichever comes first. For active users not to lose their work, specify a message in the **Notify Users Message** box advising them to save their work and log off. Please also see the **RD Session Host drain mode examples** subsection below.

When done, click **OK** to save the changes and close the dialog.

To modify an existing task, right-click it and select **Properties** in the context menu. To delete a task, right-click it and select **Delete**.

RD Session Host drain mode examples

Example 1: Scheduling a server group for reboot without the drain mode

A server group contains 3 servers: A, B, C

- Date: 6/24/2018
- Start Time: 10:45am
- Send Message: 2 minutes before

Users with active sessions are notified 2 minutes before the server rebooting task is triggered.

Example 2: Scheduling a server group for reboot with the drain mode enabled

A server group containing 3 servers: A, B, C

- Date: 6/24/2018
- Start Time: 10:45am
- Drain mode: enabled
- Force reboot after: 3 hours
- Send Message: 2 minutes before

The session users are notified 2 minutes before the server rebooting task is triggered.

When the task is triggered:

- 1** The drain mode is enabled on the servers.
- 2** Servers A and B have no active or disconnected sessions, so they are restarted immediately.
- 3** Server C still has open/disconnected sessions, so it continues to run until all users end their sessions. If in three hours the server still has active sessions, they are terminated and the server is restarted.

Maintaining RD Session Hosts based on a RAS Template

If you need to do a scheduled maintenance of RD Session Hosts that were created from a RAS Template, please follow these steps:

- 1 Create a schedule that fits your maintenance window to drain a desired RD Session Host group.
- 2 During maintenance (or right before it) switch the template into maintenance mode. Then apply the necessary changes.
- 3 The schedule disables groups provisioned by the template (while the maintenance window lasts) which leads to removing (unassigning) all guest VMs from them.
- 4 Release the template from maintenance and click **Yes** when asked whether to recreate all clones.
- 5 Enable groups which were disabled in step 3 (above). At this point, the groups will begin receiving guest VMs to comply with Keep Available Buffer setting
- 6 From this point forward, groups are provisioned with VMs on demand.

Managing Sessions

The **Sessions** tab page allows you to view and manage current sessions for RD Session Hosts. To view the page, navigate to **Farm** / <site> / **RD Session Hosts** / **Sessions**.

Note: You can also open the **Sessions** tab page by right-clicking a server on the **RD Session Hosts** tab page and choosing **Show Sessions**. This will open the **Sessions** tab page with a filter applied to it to display only the sessions that belong to the selected server.

The **Sessions** lists displays current sessions and includes the following info for each session:

- **Server.** RD Session Host name.
- **Session ID.** Session ID.
- **User.** Session owner.
- **Protocol.** Protocol used: **Console** (Parallels RAS Console connection), **RDP** (remote user connected via RDP).
- **State.** Session state: **Idle**, **Active**, **Disconnected**.
- **Logon Time.** Last date and time the user logged on.
- **Session Length.** Total sessions duration.
- **Idle Time.** Total session idle time.
- **Type.** Session type: **Admin**, **Published Application**, **Published Desktop**.
- **Resolution.** Client display resolution.

- **Color Depth.** Client display color depth.
- **Device Name.** Client device name.
- **IP Address.** Client IP address.

You can sort the **Sessions** list by any session property. Simply click on a desired column heading to sort the list in ascending or descending order.

You can also filter the list using a single or multiple session properties as a criteria. To do so, click the magnifying glass icon (top right) and then type a desired string in a desired column. The list will be filtered as you type.

To manage a session (or multiple sessions at the same time), select one or more sessions and then use the **Tasks** drop-down menu to choose from the following actions:

- **Refresh.** Refresh the list.
- **Disconnect.** Disconnect the selected session(s).
- **Log Off.** Log off the session(s).
- **Send Message.** Opens the **Send Message** dialog where you can type and send a message to the session owner(s).
- **Remote Control.** Remotely control the selected user session. See **User session remote control** below for important information.
- **Show Running Processes.** Display and manage running processes. See below for details.

User session remote control

The **Remote Control** menu option (see above) allows you to shadow a user RDS session. Due to differences in tools used by different versions of Windows Server, this feature has a limitation as described below.

If you need to shadow a user session running on Windows Server 2008 or 2008 R2, the RAS console must also be running on Windows Server 2008 or 2008 R2. If the RAS console is installed on a later version of Windows Server, shadowing will NOT work.

As a workaround for the issue described above, you can add an RD Session Host running Windows Server 2008 or 2008 R2 to the farm, publish the Parallels RAS console from it, and then use the console remotely to manage user RDS sessions running on Windows Server 2008 or 2008 R2. Please note that to finish a remote control session, the administrator must log off from the RAS console remote session. This is a limitation of the shadow.exe utility from Microsoft that doesn't take any arguments that would allow us to add a control like a bar, a button, or a key combination.

Managing running processes

The **Tasks > Show running processes** option opens the **Running Processes** dialog where you can view running processes for one or more RD Session Hosts.

Note: You can also open the **Running Processes** dialog by right-clicking a server on the **RD Session Hosts** tab page and choosing **Show Processes**. This will open the **Running Processes** dialog with a filter applied to it to display only the processes that belong to the selected server.

On the **Running Processes** dialog, use the **Show processes from** drop-down menu to filter the list using the following options:

- **Selected Session.** Displays processes for the session selected in the **Sessions** list.
- **Selected Server.** Displays all running processes for the server on which the selected session is running.
- **All Servers.** Displays all running processes for all available servers.

You can also filter the list by specifying a search criteria for one or more columns. To do so, click the magnifying glass icon (top right) and then type a desired text in one or more columns. The list is filtered as you type to match the specified criteria.

The **Tasks** drop-down menu in the **Running Processes** dialog includes the following options:

- **Refresh.** Refresh the list.
- **Kill process.** Kill the selected process.
- **Go To Published Item.** Enabled when you select a process that belongs to a running published resource. Brings up the main Parallels RAS Console window and navigates to the corresponding published resource.
- **Disconnect.** Disconnect the session.
- **Log off.** Log off the session.
- **Send message.** Send a message to the session owner.
- **Remote control.** Remotely control the selected user session.

Managing Logons

The logon management feature allows you to enable or disable logons from RD Session Hosts. The feature performs the same tasks as the `change logon` command-line utility.

Note: For RD Session Hosts based on a RAS Template, the drain mode (which disables logons) is handled automatically by the group to which a host belongs. For more information see **Using Scheduler** (p. 60).

To manage logons:

- 1 In the Parallels RAS Console, navigate to **Farm / <site> / RD Session Hosts**.
- 2 Select an RD Session Host, click **Tasks > Control** and choose one of the following:

- **Enable logons.** This option performs the same action as the `change logon /enable` command.
- **Disable logons and reconnections.** Disables subsequent logons. Does not affect currently logged on users. This option performs the same action as `change logon /disable` command.
- **Disable logons until server reboot.** Disables logons until the computer is restarted, but allows reconnections to existing sessions. Same action as the `change logon /drainuntilrestart` command.

To see the current logon control mode for an RD Session Host, click **Tasks > Control**. The checked-out option indicates the current logon control mode of the selected RD Session Host. To do this check from the command line, execute the `change logon /QUERY` command on the server.

Please also note the following:

- When applying a logon control mode on a server, ensure that the agent status is updated accordingly.
- You must set the logon control options for the servers one-by-one. If you need to do it for a group of servers, you can use the scheduler (see **Using an RD Session Host Scheduler** (p. 60)).
- There's no option for disabling logons from new client sessions but allowing reconnections to existing sessions (`change logon /DRAIN`) because its behavior is identical to the **Disable logons until server restart option** (`change logon /DRAINUNTILRESTART`).
- **Computer Configuration / Administrative Templates / Windows Components / Remote Desktop Services / Remote Desktop Session Host / Connection / Allow users to connect remotely using remote desktop services** must be set to **Not configured**, otherwise it takes precedence.

Publishing from an RD Session Host

This section describes how to publish resources hosted by an RD Session Host. The publishing functionality described here is accessed from the **Publishing** category in the RAS Console.

You can also publish resources using a publishing wizard in the **Start** category, as described in the **Setting Up a Simple RAS Environment** section (p. 24). The **Start** category publishing wizard is a simplified version that gives you convenient options of selecting the resources that you want to publish. You may try both approaches and choose the one that better suits your needs.

Read on to learn how to publish resources from an RD Session Host.

Publishing a Desktop from an RD Session Host

To publish a remote desktop from an RD Session Host:

- 1 In the RAS Console, select the **Publishing** category and click the **Add** icon below the **Published Resources** tree. This will launch the publishing wizard.

Note: If the wizard has all options disabled, it means that there are no resources (servers) in the farm from which publishing can be configured.

- 2 In the first step of the wizard, select **Desktop** and click **Next**.
- 3 In the **Select Desktop Type** step, select **RD Session Host Desktop** and click **Next**.
- 4 Select one or more RD Session Hosts which desktops you want to publish. You can select all available servers, server group(s), or individual servers. Please note that if you have just one RD Session Host, this page will not be displayed.
- 5 Click **Next**.
- 6 In the next step:
 - Specify a name and description for the desktop, and optionally change the icon.
 - Select the **Connect to administrative session** option if you want users to connect to the administrative session.
 - Select the **Start automatically when user logs on** option if you want to open a desktop as soon as a user logs on.
 - Specify the desired screen resolution using the **Desktop Size** drop-down list. To set a custom width and height of the screen, select **Custom** in the **Size** drop-down list and specify the desired values in the fields provided.
 - In the **Multi-Monitor** drop-down list, select whether the multi-monitor support should be enabled, disabled, or whether the client settings should be used.
- 7 When done, click **Finish** to publish the desktop.

Publishing an Application from an RD Session Host

To publish an application from an RD Session Host follow the below procedure:

- 1 In the RAS Console, select the **Publishing** category and then click the **Add** icon below the **Published Resources** tree (or right-click inside the **Published Resources** box and click **Add** in the context menu). This will launch the publishing wizard.

Note: If the wizard has all options disabled, it means that there are no resources (servers) in the farm from which publishing can be configured.

- 2 On the **Select Item Type** wizard page, select **Application** and click **Next**.
- 3 On the **Select Server Type** page, select **RD Session Host** and click **Next**.
- 4 On the **Select Application Type** page, select one of the following available options:

- **Single Application.** Choose this option to fully configure the application settings yourself such as the executable path etc.
- **Installed Application.** Choose this option to publish an application that is already installed on the server, therefore all of the application settings are automatically configured.
- **Predefined Application.** Choose this option to publish a commonly used Windows application such as Windows Explorer.

5 Click **Next**.

6 On the **Publish From** page, specify from which RD Session Hosts the application should be published. You have the following options:

- **All Servers in Site.** If selected, the application will be published from all servers that are available on the site.
- **Server Groups.** Select this option and then select individual server groups to publish the application from.
- **Individual Servers.** Select this option and select individual servers to publish the application from.

Please note that the **Publish From** wizard page will appear only if you have multiple RD Session Hosts. If you have just one server, this page will be skipped by the wizard. The page will also be skipped if the application type that you are installing is **Predefined Application**.

7 Click **Next**.

8 Depending on the application type that you selected on the **Select Application Type** page, the next wizard page will be one of the following:

- If you selected **Single Application**, the **Application** page will open where you have to specify the application settings manually (more about this option later in this section).
- If you selected **Installed Applications**, the **Installed Applications** page will open listing available applications (the applications are grouped by functionality). Select an application you wish to install and click **Next**. Follows the instructions to complete the wizard.
- If you selected **Predefined Application**, the **Select Predefined Applications** page will open listing available applications. Select an application you wish to publish and click **Finish**.

9 If you selected **Single Application** on the **Select Application Type** wizard page, the **Application** page will open. Specify the application settings as follows (see the screenshot below):

Note that if you populate the **Target** field first using the "browse" button ([...]), the application **Name**, **Description**, and icon will be chosen automatically. You can override this selection if you wish.

- **Name.** Choose and type a name for the application.
- **Description.** Type an optional description.
- **Run.** Select the application window state (normal window, minimized, maximized).

- **Start automatically when user logs on.** Select this option if you want to start an application as soon as a user logs on. This option works on desktop versions of Parallels Client only.
- **Change Icon.** Change the application icon (optional).
- **Server(s).** Allows you to specify the rest of the server parameters individually for each server the application was published from. Select a server from the drop-down list box and specify the parameters. Repeat for other servers in the list.
- **Target.** Specify the application executable path and file name.
- **Start in.** If the **Target** field is valid, this field will be populated automatically. You can specify your own path if needed.
- **Parameters.** If the application accepts startup parameters, you can specify them in this field.

10 When done, click **Finish** to publish the application.

Publishing a Web Application from an RD Session Host

A web application is like any other application that you can publish using the standard application publishing functionality. However, to simplify publishing of straight URL links to web applications, a separate publishing item type is available that allows you to accomplish this task with minimal number of steps.

To publish a web application:

- 1** In the RAS Console, select the **Publishing** category and then click the **Add** icon below the **Published Resources** tree (or right-click inside the **Published Resources** box and click **Add** in the context menu). This will launch the publishing wizard.

Note: If the wizard has all options disabled, it means that there are no resources (servers) in the farm from which publishing can be configured.

- 2** On the **Select Item Type** wizard page, select **Web Application** and click **Next**.
- 3** On the **Select Server Type** page, select **RD Session Host** and click **Next**.
- 4** On the **Publish From** page, select the server(s) to publish from. Note that if you have just one RD Session Host, the **Publish From** page will not appear.
- 5** On the **Web Application** wizard page that opens, specify the web application name, description, window state, and the URL. Select the **Force to use Internet Explorer** option if needed. To browse for a specific application icon, click **Change Icon**.
- 6** When done, click **Finish** to publish the application.

When published, the web application will appear in the **Publishing > Published Resources list**, just like any other application.

Publishing a Network Folder from an RD Session Host

You can publish a filesystem folder via UNC path to open in Windows explorer. To minimize the number of configuration steps, a special publishing item is available that allows you to publish a network folder from an RD Session Host.

To publish a network folder:

- 1 In the RAS Console, select the **Publishing** category and then click the **Add** icon below the **Published Resources** tree (or right-click inside the **Published Resources** box and click **Add** in the context menu). This will launch the publishing wizard.

Note: If the wizard has all options disabled, it means that there are no resources (servers) in the farm from which publishing can be configured.

- 2 On the **Select Item Type** wizard page, select **Folder on the file system** and click **Next**.
- 3 On the **Select Server Type** page, select **RD Session Host** and click **Next**.
- 4 On the **Publish From** page, select the server(s) to publish from. Note that if you have just one RD Session Host, the **Publish From** page will not appear.
- 5 On the **UNC Folder** wizard page, specify the usual application properties.
- 6 In the **UNC path** field, enter the UNC path of the folder you wish to publish. Click the **[...]** button to browse for a folder (it may take some time for the **Browse for Folder** dialog to open).
- 7 Click **Finish** to publish the folder and close the wizard.

When published, the network folder will appear in the **Publishing > Published Resources list**, just like any other application. If you select it and then click the **Application** tab, the application settings will be as follows:

- The **Target** property will always be set to `PublishedExplorer.exe`. This binary is created automatically (via agents pushing) and is simply a copy of the standard `explorer.exe` executable.
- The **Parameters** property specifies the network folder that we want to publish. The folder path can be in any format that the `explorer.exe` can handle.

Please note that although you have all standard application property tabs enabled for this publishing item, at least the following items should be ignored, as they are completely irrelevant:

- **Publish From**
- **File Extensions**

Publishing a Document from an RD Session Host

To publish a document from an RD Session Host, follow the below procedure:

- 1 In the RAS Console, select the **Publishing** category and then click the **Add** icon below the **Published Resources** tree (or right-click inside the **Published Resources** box and click **Add** in the context menu). This will launch the publishing wizard.

Note: If the wizard has all options disabled, it means that there are no resources (servers) in the farm from which publishing can be configured.

- 2 On the **Select Item Type** wizard page, select **Document** and click **Next**.
- 3 Select **RD Session Host** and click **Next**.
- 4 Specify the content type of the document you want to publish. You can select the content type from the predefined list or specify a custom content type in the **Custom content types** input field.
- 5 Click **Next** when ready.
- 6 On the **Publish From** page, specify from which RD Session Hosts the application should be published. You have the following options:
 - **All Servers in Site.** If selected, the application will be published from all servers that are available on the site.
 - **Server Groups.** Select this option and then select individual server groups to publish the application from.
 - **Individual Servers.** Select this option and select individual servers to publish the application from.

Please note that the **Publish From** wizard page will appear only if you have multiple RD Session Hosts. If you have just one server, this page will be skipped by the wizard.

- 7 On the **Application** page, enter a name, an optional description, a Window state, and an icon if needed.
- 8 Use the [...] button next to the **Target** input field to browse for the document. All other fields will be automatically populated. To edit any of the auto populated fields, highlight them and enter the required details.
- 9 (Optional) In the **Parameters** input field, specify the parameters to pass to the application when it starts.

Note: Use the **Server(s)** drop down list to specify different document settings for a specific server in case the document is configured differently on that particular server. The settings will be saved for each server you select individually.

- 10 Click **Finish** to publish the document.

Publishing Containerized Applications

Parallels RAS supports publishing of the following containerized applications:

- App-V applications (p. 71)
- Turbo.net applications (p. 72)

Publishing App-V Applications

Microsoft Application Virtualization (or App-V) is an application streaming solution from Microsoft. Beginning with Parallels RAS v16.5, a support for App-V application publishing is available in the Parallels RAS console.

At the time of this writing, the App-V support implements scenarios where application provisioning is performed by means of App-V components:

- Applications are sequenced by the administrator according to Microsoft guidelines.
- Applications are stored on a network share created by the administrator (SMB, HTTPs).
- App-V Management and Publishing servers are used to publish applications for a specific AD groups that must be synced manually by the administrator with RAS publishing groups used for App-V application publishing.
- App-V client is installed and configured manually by the administrator.

The process of deploying and publishing an App-V application is as follows:

- 1 Package an applications using the App-V Sequencer.
- 2 Deploy the application to an RD Session Host using the App-V Management Console, Microsoft SCCM, etc.
- 3 Provision the application.
- 4 Verify that users can launch the application from the RD Session Host.
- 5 Publish the application from RAS Console (see below for instructions).
- 6 Launch the application from a Parallels RAS Client.

Publish an App-V application from the Parallels RAS console

To publish an App-V application:

- 1 In the Parallels RAS Console, select the **Publishing** category.
- 2 Click the **[+] Add** icon at the bottom of the right pane. The publishing wizard opens.
- 3 On the **Select Item Type** page, select the **App-V application** option.
- 4 Click **Next**.

- 5 Select the server type from which to publish an application and click **Next**.
- 6 Select a server or a group to publish from and click **Next**.
- 7 On the **Installed Applications** page, select one or more App-V applications and click **Next**.
- 8 Review the summary and complete the wizard.

Once an App-V application is published, it can be launched from a Parallels RAS Client.

Note: To avoid launch issues, use AutoLoad=2. More details in https://blogs.technet.microsoft.com/technetsto_sup/2013/11/12/autoload-setting-in-app-v-5-0/

Publishing Turbo.net Applications

Turbo (Turbo.net) is a web-based container platform that runs applications on a Windows desktop with no installation required. Parallels RAS provides you with the ability to publish applications hosted by Turbo.net and make them available to Parallels RAS users just like regular applications hosted by RD Session Hosts.

The ability to publish container-based applications allows Parallels RAS administrators to greatly reduce TtV (time to value) and minimize investment and development resources. The integration of the solution provided by Turbo gives you the following immediate benefits:

- Instant access to an online application repository with hundreds of applications available, including:
 - Most web browsers (Chrome, Firefox, Opera, etc).
 - Most application runtimes (JRE and others).
 - Most add-ons (Flash, etc).
 - Open source applications like LibreOffice, VLC Player, etc.
 - Administrative tools like WinSCP, Putty and so on.
- Instant provisioning of all these applications in any combination possible (i.e. a particular version of Google Chrome with a specific Java runtime and Flash) to all endpoints regardless of the platform and version (supports anything from Windows 7 to Windows Server 2016).

For more information about Turbo, visit <http://www.turbo.net>

Licensing and supported Turbo repositories

- Parallels RAS uses the free edition of Turbo.net, so no subscription is required.
- Parallels RAS supports application publishing from the public Turbo.net repository only. Private repositories are not supported at the time of this writing.

Enabling or disabling the Turbo.net support in Parallels RAS

Before you can publish applications from Turbo.net, you need to enable this functionality in Parallels RAS as follows:

- 1 In the Parallels RAS Console, select the **Administration** category and then click the **Features** tab in the right pane.
- 2 Select the **Enable Turbo.net application publishing** option. This will enable the Turbo.net functionality in the farm and will install the Turbo runtime on every RD Session Host, so they can download and run container-based applications.

If later you decide to disable the Turbo.net support in Parallels RAS (by clearing the **Enable Turbo.net application publishing** option), you will see a message box saying that this action will uninstall Turbo runtime from each RD Session Host that has it installed. If later you enable the Turbo.net support again, the runtime will be reinstalled. If you've already published applications from Turbo.net, the message box will also ask you what should be done with them. The available options are:

- **Disable.** All published Turbo.net applications will be disabled.
- **Delete.** All published Turbo.net applications will be removed from Parallels RAS. If you enable the Turbo.net support later, you will have to publish these applications again.
- **Keep unchanged.** Applications will remain in Parallels RAS as active applications, but end users will not be able to use them. If later you enable the Turbo.net support, the applications will continue to work normally.

Publishing from Turbo.net

To publish a Turbo.net application:

- 1 In the Parallels RAS Console, select the **Publishing** category.
- 2 Click the **[+] Add** icon at the bottom of the right pane. The publishing wizard opens.
- 3 On the **Select Item Type** page, select the **Turbo.net application** option. If the option is disabled (grayed out), it means that the Turbo.net support is disabled in the Parallels RAS farm. See above for the info on how to enable it.
- 4 Click **Next**.
- 5 On the **Configure Turbo.net Repository** page, specify an application you would like to publish. Choose from the following options:
 - Double-click a desired category in the application category list to see apps that it contains. Select an application and click **Next**.

- Expand the drop-down list (on the right side) and select from one of the predefined applications. If the app you are looking for is not in the list, type a search condition in the same field and press Enter. The search string can be a full or partial application name, a publisher name, or anything else that can possibly be a part of the app description. Applications that match the search condition will appear in the list from which you can select the one you need.
- 6** After selecting an application, click **Next**.
 - 7** On the **Application** page, specify the following options:
 - **Name:** A name under which the application will be listed in Parallels RAS.
 - **Description:** An optional description.
 - **Run:** Select the application window state (normal window, minimized, maximized).
 - **Start automatically when user logs on:** Select this option if you want to start the application as soon as a user logs on to Parallels RAS. This option works on desktop versions of Parallels Client only.
 - **Change Icon:** Specify a different application icon (optional).
 - **Server(s):** Allows you to specify **Target**, **Start In**, and **Parameters** settings individually for each RD Session Host through which this application will be published. Select an RD Session Host from the drop-down list and then specify the settings described below.
 - **Target:** Specifies the application executable path and file name. This shouldn't be normally changed for Turbo.net applications.
 - **Start in:** If the value in the **Target** field is valid, the **Start In** field is populated automatically. You can specify your own path if needed.
 - **Parameters:** If the application accepts startup parameters, you can specify them in this field.
 - 8** Click **Finish** to publish the Turbo.net application. The application should appear in the **Published Resources** tree in the **Publishing** category just like any other published resource.

Specifying RD Sessions Hosts through which the Turbo.net application should be published

After you publish a Turbo.net application, you can specify RD Session Hosts through which it should be published. Here's how it works. Application containers reside in the public Turbo.net repository. When you initially publish a containerized Turbo.net application in Parallels RAS, you don't really download it to an RD Session Host. However, as soon as the first user tries to launch a newly published Turbo.net application in Parallels Client, the application container is downloaded to an RD Session Host and the application is started on it. The user then gets access to it just like any other published application.

To specify one or more RD Session Hosts through which the application should be published, select the application in the **Published Resources** tree, choose the **Publishing From** tab and select one of the following options:

- **All Servers in Site.** The application will be published through all available RD Session Hosts.
- **Server Groups.** This option allows you to specify server groups through which the application should be published.
- **Individual Servers.** Select this option to specify one or more individual servers.

How Turbo.net applications are launched in Parallels Client

When a user launches a Turbo.net application in Parallels Client, the RD Session Host handling the request will attempt to start the application. If this is the first time anybody launches this particular application on this server, the server first downloads the application container from Turbo.net. In such a case, the Parallels Client user will see a message box with a progress indicator while the RD Session Host prepares the application. Once the application is running on the server, the user will see its window and can begin using it. Apart from the progress indicator box, a Parallels Client user will not be able to tell whether a published application is a regular or a Turbo.net application.

Viewing Published Resources Hosted by RD Session Hosts

When you want to remove an RD Session Host or an RD Session Host group from a site, you might want to see the list of published resources hosted by the server or servers in a group. This way you can see which resources will be affected. You can do so as follows:

- 1 In the Parallels RAS Console, select **Farm \ RD Session hosts**.
- 2 To see published resources for a specific RD Session Host, select the **RD Session hosts** tab. To see published resources for a group, select the **Groups** tab.
- 3 Right-click a server or a group and choose **Show published resources** (or click **Tasks > Show published resources**).
- 4 The **Published Resources** window opens displaying the list of published resources for the selected server or group. Resource information includes:
 - **Name.** Resource name.
 - **Status.** Enabled or disabled.
 - **Type.** "Application" is used for published applications, URLs, network folders, etc. "Desktop" is used for published desktops.
 - **Path.** For published applications, specifies a path to the execute file, URL, or UNC path.
 - **Parameters.** Published application parameters (if any).
 - **Published from.** Site, group(s), or individual server(s).

- 5** To refresh the list, press F5 or click the "recycle" icon (top-right).
- 6** To filter the list, press Ctrl-F or click the magnifying glass icon and then specify the filter criteria for desired column(s).

CHAPTER 6

VDI and Virtual Desktops

Parallels RAS VDI (Virtual Desktop Infrastructure) enables you to use server virtualization to reduce the number of physical servers required to host published resources. Parallels RAS VDI supports a number of virtualization technologies (hypervisors) and allows you add VDI hosts to your farm and then publish resources hosted by virtual machines running on those hosts. Parallels RAS VDI also includes the RAS Template functionality, which gives you the ability to create a template from a preconfigured virtual machine and then clone guest VMs and RD Session Host VMs from it.

In This Chapter

Supported Hypervisors	77
RAS VDI Agent Information	78
RAS VDI Agent Installation Options	78
Add a VDI Host	80
Modifying VDI Host Configuration.....	82
Change VDI Host Site Assignment	85
RAS Templates	85
VDI Host Pool Management.....	100
Persistent Guest VMs	103
Publishing from a Guest VM	104
Viewing VDI Host Summary	109
Managing VDI Sessions.....	109

Supported Hypervisors

Parallels RAS supports VDI hosts based on the following virtualization technologies:

- Microsoft Hyper-V
- Microsoft Hyper-V Failover Cluster
- VMware vCenter
- VMware ESXi v6.7 (VMware vCenter is required)
- Citrix XenServer
- QEmu KVM with libvirt
- Scale Computing HC3
- Nutanix Acropolis
- Remote PC (this is a special type that allows you to create pools of remote PCs).

RAS VDI Agent Information

RAS VDI Agent is a software that provides an interface to manage a hypervisor through its native API. In Parallels RAS v16.5 and later, RAS VDI Agent is built into the RAS Publishing Agent, so it's already installed in your RAS farm and is ready to be used to manage one or more VDI hosts. Some limitations apply as described below.

Almost all of the hypervisors supported by Parallels RAS can be managed via the built-in RAS VDI Agent. The only exception is **QEmu KVM with libvirt**. This means that for this hypervisor you must deploy a dedicated RAS VDI Agent as a separate step. For other VDI technologies, you have a choice of using the built-in RAS VDI Agent or installing it separately. The difference is as follows:

- When you use a built-in RAS VDI Agent, you manage multiple (or all) VDI hosts in a RAS farm using the same agent that is already installed in your RAS farm. This eliminates the need to install and maintain the agent separately for each VDI host.
- When you install a dedicated RAS VDI Agent on a different host, it can be used to manage a single VDI host only.

Read next:

- If you are adding a VDI host that will use the built-in RAS VDI Agent, you may skip to **Add a VDI Host** (p. 80).
- If you are using QEmu KVM, or if you want to install a dedicated RAS VDI Agent on a different host, read the **RAS VDI Agent Installation Options** section (p. 78), which follows this one.

RAS VDI Agent Installation Options

If you are installing a dedicated RAS VDI Agent, you first need to determine where it will be installed. Depending on the hypervisor type, the following options are available:

- The host on which the hypervisor is running. This option is available for Microsoft Hyper-V only.
- A supported version of Windows Server running on a physical box or in a virtual machine. For supported Windows Server versions, see **Software Requirements > RAS VDI Agent** (p. 16).
- A preconfigured Linux-based virtual appliance (provided by Parallels). The appliance can be deployed on any hypervisor on your network.

The following table lists RAS VDI Agent installation options for each supported hypervisor type:

Hypervisor Type	Built-in Agent (part of PA)	Agent on a VDI Host	Agent on a Windows Server (VM or HW)	Agent in Appliance
Microsoft Hyper-V	Yes	Yes	Yes	No
Microsoft Hyper-V Failover Cluster	Yes	No	Yes	No

VMware vCenter	Yes	No	Yes	Yes (OVA or VMDK)
VMware ESXi	Yes	No	Yes	Yes (OVA or VMDK)
Citrix Hypervisor	Yes	No	Yes	Yes (OVA or VMDK)
QEMU KVM with libvirt	No	No	No	Yes (VMDK)
Scale Computing HC3	Yes	No	Yes	No
Nutanix Acropolis	Yes	No	Yes	Yes (VMDK)
Remote PC (see the Note below)	Yes	No	Yes	No

Note: The **Remote PC** is a special type that can be used to create and manage pools of remote PCs as part of hosted desktop infrastructure (HDI). When you add a VDI host of this type, you can manage it like one of the real VDI hosts with some limitations, such as you cannot create templates and use some other strictly VDI-specific functions. The main feature when using this type is the ability to create pools of HDI-based remote PCs and making PCs persistent by assigning an individual PC to a specific user. For more info, see **Remote PC Pools**.

In the table above, find the hypervisor type that you are using and see where the RAS VDI Agent can be installed. Depending on the available choices, do one of the following:

- **Built-in Agent.** The agent is a part of RAS Publishing Agent, so it is already installed.
- **Agent on a VDI host.** This option is only available if you are using Microsoft Hyper-V. You don't need to do anything special and can simply install the agent on the host, as described in **Add a VDI Host** (p. 80).
- **Agent on a Windows Server (VM or HW).** To use this option, make sure you have a physical box or a virtual machine running a supported version of Windows Server. You will need to specify its FQDN or IP address when adding a VDI host to the farm.
- **Agent in Appliance.** If this is your choice, you need to download and deploy a virtual appliance as described in the **Deploying a Virtual Appliance** subsection below.

Please note that if both Windows Server and virtual appliance can be used with your hypervisor type, you can choose one or the other according to your preferences.

Deploying a virtual appliance

Use these instructions if you plan on deploying RAS VDI Agent as a virtual appliance.

To download and install a virtual appliance:

- 1 Visit <https://www.parallels.com/products/ras/download/links/>
- 2 On the download page, scroll down to the "VDI Agent Appliances" section and click the **VDI Agent Appliance OVA** or the **VDI Agent Appliance VMDK** link to download the appliance. See the table above for the appliance type (OVA or VMDK) compatible with the hypervisor that you are using.
- 3 After downloading the virtual appliance, you need to deploy it on a hypervisor. For the information about deploying a virtual appliance, please refer to your hypervisor documentation.

Add a VDI Host

Searching for VDI hosts

To search for available VDI hosts on your network:

- 1 In the RAS console, navigate to **Farm** / <site> / **VDI**.
- 2 On the **Virtual Desktop hosts** tab page, click **Tasks** > **Discover VDI hosts**.
- 3 A dialog opens displaying the discovered VDI hosts (you may have to wait until the discovery completes). If no VDI hosts are found, you can add a host manually (see **Manually Adding a VDI Host** below).
- 4 You can select the **Show all hosts** option to display all available hosts, including the hosts that don't meet the minimum system requirements. To refresh the list, click **Refresh**.
- 5 Click **OK** to add the VDI host to the Parallels RAS farm.

Manually adding a VDI host

To add a VDI host manually:

- 1 On the **Virtual Desktop host** tab page, click **Tasks** > **Add** to launch the **Add VDI Host** wizard.
- 2 In the **VDI Host type** field, select the hypervisor type.
- 3 In the **VDI host address** field, specify the host's FQDN or IP address.
- 4 Specify a user name and password to log in to the server.
- 5 Type an optional description for the host.
- 6 Click **Next**.
- 7 On the next page, specify the following (optional) properties:
 - **Use dedicated VDI Host Agent:** Select this option if you will install (or have installed) the RAS VDI Agent yourself. This includes the virtual appliance scenario. Clear the option if you will use the built-in RAS VDI Agent (p. 78).
 - **Agent address:** This option becomes enabled if you select the option above it. Specify the FQDN or IP address of the server where the RAS VDI Agent is (or will be) installed. This can be either a virtual appliance (if you use one) or a Windows Server host (physical box or virtual machine).
 - **Preferred Publishing Agent:** Select a RAS Publishing Agent to be the preferred agent for this VDI host. For the built-in RAS VDI Agent, the selection defaults to **Automatically**. Internally, the system selects the least loaded RAS Publishing Agent.
- 8 Click **Next**.

- 9** The wizard will now try to connect to the RAS VDI Agent. If you specified **Use dedicated VDI Host Agent** and **Agent address** options in the previous (optional) step, and if the agent is not installed, you will need to install it. Click **Install** and follow the instructions to push install the agent on the specified host. Please note that for the push installation to work, the following requirements must be met:
- The firewall must be configured on the server to allow push installation. Standard SMB ports (139 and 445) need to be open. See also **Port Reference** (p. 289) for the list of ports used by Parallels RAS.
 - SMB access. The administrative share (\\server\c\$) must be accessible. Simple file sharing must be enabled.
 - Your Parallels RAS administrator account must have permissions to perform a remote installation on the server. If it doesn't, you'll be asked to enter credentials of an account that does.
 - The target server should be joined to an AD domain. If it's not, the push installation may not work and you will have to install the agent manually. For instructions, see **Installing RAS VDI Agent Manually** (p. 81).
- 10** Click **Finish** to close the wizard.

Installing RAS VDI Agent Manually

You may need to install the RAS VDI Agent on a VDI host manually if the automatic push installation cannot be performed for any reason.

Note: You can only use these instructions to install RAS VDI Agent in Windows.

Installing RAS VDI Agent Manually

To install the agent:

- 1** Log in to the server where the RAS VDI Agent is to be installed using an administrator account and close all other applications.
- 2** Copy the Parallels RAS installation file (RASInstaller.msi) to the server and run it. Follow the onscreen instructions.
- 3** On the **Select Installation Type** page, select **Custom** and click **Next**.
- 4** Click on **RAS VDI Agent dedicated** and select **Entire Feature will be installed on local hard drive** from the drop-down menu.
- 5** Ensure that all other components are deselected and click **Next**.
- 6** Click **Install** to start the installation. Click **Finish** once the installation is finished.

The RAS VDI Agent does not require any configuration. Once the agent is installed, highlight the server name in the RAS Console and click **Troubleshooting > Check Agent**. If the agent is installed properly, the status should change to **Agent Installed**.

Uninstalling RAS VDI Agent

To uninstall the RAS VDI Agent from a server:

- 1 Navigate to **Start > Control Panel > Programs > Uninstall a Program**.
- 2 Find **Parallels Remote Application Server** in the list of installed programs.
- 3 If you don't have any other Parallels RAS components on the server that you want to keep, right-click **Parallels Remote Application Server** and then click **Uninstall**. Follow the instructions to uninstall the program. You may skip the rest of these instructions.
- 4 If you have other RAS components that you want to keep on the server, right-click **Parallels Remote Application Server** and then click **Change**.
- 5 Click **Next** on the Welcome page.
- 6 On the **Change, repair, or remove** page, select **Change**.
- 7 On the next page, select **Custom**.
- 8 Select **RAS VDI Agent dedicated**, then click the drop-down menu in front of it, and click **Entire feature will be unavailable**.
- 9 Click **Next** and complete the wizard.

Checking the RAS VDI Agent Status

To verify that the RAS VDI Agent is installed and functions properly, do the following:

- 1 First, you can look at the **Status** column in the **Virtual Desktop hosts** list (**Farm / <site> / VDI / Virtual Desktop hosts**). If there's a problem with the agent, the column will display an appropriate description. Note that in addition to the description, the **Status** column uses a color code to indicate the agent status as follows:
 - Red — Not Verified
 - Orange — Needs Update
 - Green — Verified
- 2 Right-click a host and then click **Troubleshooting > Check Agent** in the context menu.
- 3 The **VDI Agent Information** dialog opens displaying the information about the VDI Agent, VDI Services, and other related info.
- 4 If the VDI Agent is not installed, click the **Install** button and follow the onscreen instructions. See **Adding a VDI Host (Manually Adding a VDI Host subsection)** (p. 78) for more info.

Modifying VDI Host Configuration

Read this section to learn how to modify the configuration of a VDI host in Parallels RAS.

Configuring a VDI host

To configure a VDI host:

- 1 In the RAS Console, navigate to **Farm** / <site> / **VDI**.
- 2 Select the **Virtual Desktop Hosts** tab page in the right pane.
- 3 Select a VDI host in the **Virtual Desktop Hosts** list and click **Tasks** > **Properties**. The **Host Properties** dialog opens.

Note: Some of the properties described below may be unavailable on some servers. This depends on the type of the hypervisor installed on the host.

Enabling or disabling a VDI host in the farm

By default a VDI host is enabled in the farm. When it is disabled, published applications and virtual desktops cannot be served from it. To enable or disable a VDI host, use the **Enable Host in site** option on the **Properties** tab page.

Configuring VDI host connection settings

The following settings can be configured on the **Properties** tab page:

- **VDI Type:** Hypervisor type.
- **VDI Version:** Hypervisor version. If the hypervisor version that you are using is not listed, select **Other**.
- **VDI Host:** The VDI host IP address.
- **VDI Port:** Port number on which the VDI host listens for incoming connections.
- **Description:** An optional description.
- **Dedicated VDI Host Agent:** Select this option if you have a dedicated RAS VDI Agent installed on the VDI host.
- **VDI Agent:** The virtual appliance IP address. This field is enabled if the option above is selected.

Specifying credentials

On the **Credentials** tab page, specify the user name and password to log into the VDI host. Click the **Check Credentials** button to verify the credentials that you've entered.

Configuring the RAS VDI Agent on the server

RAS VDI Agent can be configured on the **Agent Settings** tab page.

- **Max connections:** Specifies the maximum allowable number of connections.

- **Publishing Session Timeout:** Specifies the amount of time each session remains connected in the background after the user has closed the published application. This option is used to avoid unnecessary reconnections with guest VMs.
- **Allow Client URL/Mail Redirection:** Select this option to allow http and mailto links to be opened using a local application on the client computer rather than the server resources.
- **Preferred Publishing Agent:** Select a Publishing Agent with which the RAS VDI Agent should communicate. This can be helpful when site components are installed in multiple physical locations communicating through WAN. You can decrease network traffic by specifying a more appropriate Publishing Agent.
- **Allow file transfer command:** Allows you to enable or disable the remote file transfer functionality. For more information, see **Enabling or Disabling Remote File Transfer (p. 231)**.
- **Allow local to remote drag and drop.** Enables the drag and drop functionality in a remote application. When this option is enabled, an end user can drag and drop files to a remote application on their local device. For example, a user can drag and drop a file to the Acrobat reader to open a PDF file. Or a user can drag and drop a file to Windows Explorer running on a remote server, etc.

Note: At the time of this writing the drag and drop functionality is only supported on Parallels Client for Windows and Parallels Client for Mac.

Configuring RDP printing

The **RDP Printer** tab allows you to configure the renaming format of redirected printers. The format may vary depending on which version and language of the server you are using. Select the **RDP Printer Name Format** option specifically for the configured server:

- **Printrname (from Computername) in Session no.**
- **Session no. (computername from) Printrname**
- **Printrname (redirected Session no)**

The other RDP Printing options available in the RDP Printer tab are:

- **Remove session number from printer name**
- **Remove client name from printer name**

Configuring VDI host maintenance time window

The **Scheduler** tab page allows you to create a maintenance time window for the server. During this time, published resources won't be accessible from that server.

To configure maintenance time window click **Tasks > Add** and then set the following options:

- **Start date**
- **Time**
- **Duration**

- **Repeat**

The **On disable** option allows you to specify what should happen to current sessions when a scheduled task triggers.

Change VDI Host Site Assignment

You can assign a VDI host to a different site in your farm if needed. Please note that this functionality is only available if you have more than one site in your farm.

Note: You cannot assign a VDI host to a different site when there are RAS templates, pools, or guest VMs that are in use on the current site. If you try to do so, you will get an error and will not be able to proceed. To assign such a VDI host to a different site, you need to remove all dependencies in the current site first.

To change the site assignment:

- 1 Right-click a VDI host and then click **Change Site** in the context menu. The **Change Site** dialog opens.
- 2 Select a site in the list and click **OK**. The server will be moved to the **Virtual Desktop hosts** list of the target site (**Farm** / <new-site-name> / **VDI**).

RAS Templates

RAS Templates are used to automate the creation and deployment of guest VMs in Parallels RAS. A RAS Template is created from an existing virtual machine running on one of the hypervisors supported by Parallels RAS. Once a template is ready, it can be used to create guest VM clones that will inherit all of the properties of the template. The resulting guest VMs can then be used to host published resources.

Read the following topics to learn how to create a RAS Template:

- Template Types and Guest OS Requirements (p. 85)
- Creating a RAS Template (p. 87)
- How Guest VMs are Created From a Template (p. 94)
- Manually Adding a Guest VM
- RAS Template Maintenance (p. 97)

Template Types and Guest OS Requirements

There are two types of RAS Templates: **Virtual desktop** and **RD Session Host**. They are described below.

Virtual desktop

Virtual desktop templates are the essential part of the Parallels RAS VDI. They are used to create guest VMs for publishing of desktops, applications, documents, etc. The guest OS support is the same as for RAS Guest Agent (which must be installed in a VM). See **Software Requirements**.

Guest VMs created from a Virtual desktop template normally serve a single user. They are managed entirely from within the RAS VDI, which includes such features as creating persistent VMs, managing VDI sessions, publishing resources from a specific Virtual desktop template, and others.

RD Session Host

RD Session Host templates are designed specifically to give you the ability to replicate RD Session Hosts running in virtual machines. Guest VMs created from an RD Session Host template are treated by Parallels RAS almost like regular RD Session Hosts. The main difference is, you can create as many guest VMs from a single template as you require, thus automating RD Session Host provisioning according to your needs.

RD Session Host templates are supported on the following hypervisor platforms:

- Microsoft Hyper-V
- Microsoft Hyper-V Failover Cluster
- VMware VCenter
- VMware ESXi

RD Session Host templates support Windows Server 2008 R2 and newer as a guest OS. Compared to regular RD Session Hosts (p. 46), servers created from an RD Session Host template do not support earlier versions of Windows Server. The reason is these servers run in VMs and require the RAS Guest Agent installed in them, so the guest OS requirements are limited by Windows Server versions supported by RAS Guest Agent.

Please note that since RD Session Host templates are designed to complement the RD Session Hosts functionality, the following standard RAS VDI features cannot be used with them:

- Pool management
- Persistent guest VMs
- Session management
- Publishing from a specific RAS Template
- Some other strictly RAS VDI specific features.

For the information on how to provision RD Session Hosts created from a template, see **Grouping and Cloning RD Session Hosts** (p. 56).

Creating a RAS Template

Requirements

To complete the tasks described in this section, the following requirements must be met:

- Make sure the hypervisor tools are installed and running in the guest VM.
- Make sure you know account credentials that will allow you to push install the agent software on a VM. If you run the Parallels RAS console using such credentials (e.g. a domain admin), you will not be asked to enter them during the agent installation. If you run the console using a different account, you'll be asked to enter credentials when you install the agent.
- The guest OS (Windows) running in the VM must be configured to obtain an IP address from a DHCP server.
- For users to access published resources in a guest VM, the RDP port must be open locally or via Group Policy in Windows running in the VM. The default RDP port is 3389.
- For RD Session Host templates, Network Discovery UDP port 137 must be enabled for a domain firewall profile in the guest OS. This can be done via domain group policies or manually in the guest OS.

Manual agent installation

Normally, you will push install the necessary agent software in a source VM right from the Parallels RAS console (as described later in this section). However, you can also install the software manually by running the Parallels RAS installer in Windows in the VM. When doing so, use the **Custom** installation option and select the following agent components depending on the type of the template (p. 85) that you are creating:

- **Virtual desktop.** This template type requires RAS Guest Agent to be installed in the source VM.
- **RD Session Host.** This template type requires RAS Guest Agent and RAS RD Session Host Agent to be installed in the source VM.

Create a RAS Template

The process of creating a RAS Template consists of two stages:

Stage 1: (p. 88) During the first stage, the wizard will verify if the agent software is installed and will allow you to install it if needed.

Stage 2 (p. 90): During the second stage, you will need to configure the template.

Each stage is described in detail in the sections that follow this one (or follow the links above).

Stage 1: Check and Install the Agent Software

To begin creating a RAS Template:

- 1 In the RAS Console, navigate to **Farm** / <site> / **VDI**.
- 2 Select the **RAS Templates** tab in the right pane.
- 3 In the **Tasks** drop-down menu, click **Add**.
- 4 In the dialog that opens, select a guest VM from which you would like to create a RAS Template and click **OK**.
- 5 The **Create Parallels RAS Template Wizard** opens. Each wizard page is described below in the order they appear on the screen.

Select Type

On the first page of the wizard, select a template type to create: **Virtual desktop** or **RD Session Host**. For details, see **Template Types** (p. 85).

Check Agent

On the **Check Agent** page, the wizard will check if the selected VM has the agent software installed. Wait for it to finish and then examine the **Status** field (closer to the bottom of the page). Depending on the result, do one of the following:

- If the agent software is installed, click **Next** to continue. You may stop reading here and jump to **Stage 2: Configure the RAS Template** (p. 90).
- If the software is not installed, you need to install it as described below.

To install the agent software, first click the **Customize Guest Agent deployment settings** link and specify the options in the dialog that opens. None of the options are forced, so you can select or clear them depending on your needs. Note that depending on the RAS Template type, the options are different, as described below.

Virtual desktop:

- **Add firewall rules:** Automatically configure firewall rules in the guest VM.
- **Allow remote desktop connections:** Select to automatically configure remote desktop access in the VM.
- **Specify users or groups to be added to the Remote Desktop Users group:** Select this option and then click the **[+]** icon to add specific users to the group.

RD Session Host:

- **Add firewall rules:** Automatically configure firewall rules in the guest VM.

Note: Network Discovery UDP port 137 must be enabled for a domain firewall profile in the guest OS as a separate step. This can be done via domain group policies or manually in the guest OS.

- **Install RDS role:** Install the RDS role in the guest VM.
- **Enable Desktop Experience:** Enable the Desktop Experience feature in Windows.
- **Restart server if required:** Restart the VM if required.
- **Specify users or groups to be added to the Remote Desktop Users group:** Select this option and then click the **[+]** icon to add specific users to the group.

When done specifying the options, click **OK** to close the dialog.

Now click the **Install** button and follow the onscreen instructions to install the agent software.

Hint: If the guest VM cannot be reached by its name specified as a hostname, double-click the guest VM name and change it to the correct IP address.

Once done, verify that the agent software is installed by looking at the **Status** field on the **Check Agent** wizard page. If so, continue to the next section that describes **Stage 2: Configure the RAS Template** (p. 90).

Known Windows Server guest OS support issue

If a VM is running a Windows Server as the guest OS and you see the error that "RAS Guest OS Agent not supported", you can fix that using Parallels RAS PowerShell. If you haven't installed RAS PowerShell, run the Parallels RAS installer and install it.

- 1 Once RAS PowerShell is installed, do the following:
- 2 Exit the Parallels RAS Console.
- 3 Open the Windows PowerShell console.
- 4 Import the RAS module by executing the following commands:

```
Import-Module PSAdmin
```
- 5 Connect to your Parallels RAS farm (substitute the server name with your RAS Licensing Server name or IP address and type a password when prompted):

```
New-RASSession -Server "server.company.dom"
```
- 6 Execute the following command:

```
Get-VDISettings
```

See if the output contains `EnableServerGuests = false`
- 7 Execute another command to change the settings:

```
Set-VDISettings -EnableServerGuests $true
```
- 8 Execute `Get-VDISettings` again and make sure that `EnableServerGuests = true`

Stage 2: Configure the RAS Template

Once the agent software is installed, and the **Status** field on the **Check Agent** wizard page confirms this, click **Next**. The VM will now be powered off (wait for the power off operation to finish). Once the VM is powered off, the template configuration stage begins. The subsequent wizard pages are described below.

Properties

On this page, specify the following options:

- **Template name:** Choose and type a template name.
- **Maximum guest VMs:** Specify the maximum number of guest VMs that can be created from this template.
- **Number of guest VMs deployed on the wizard completion:** The number of guest VMs to deploy once the template is created. Please keep in mind that this will take some time because the VMs will be created one at a time.
- **Guest VM name:** A prefix to use when naming a new guest VM.
- **Clone method:** Whether to create linked or full clones. A full clone is a complete copy of a template. As such, it occupies as much space on the physical hard drive as the source template and takes a significant time to create. A linked clone is a copy of a template made from a snapshot that shares virtual disk with the source template, therefore it takes much less space on the physical hard drive and it takes only a couple of minutes to create.

You should use full clones if your application and OS updates are too slow (full clones take longer to create, but they provide the best possible performance). Otherwise if your updates are fast enough, use linked clones as it takes much less time to create them.

Note: If the **Create a linked clone** option is grayed out, it means that the current version of Parallels RAS does not support linked clones with the hypervisor that you are using. At the time of this writing, support for linked clones is available for VMware, Microsoft Hyper-V, KVM, Scale Computing HC3, and Nutanix. Please note that Citrix XenServer support in Parallels RAS includes full clones only. Linked clones support will be added in the near future.

Additional Properties

On the **Additional Properties** page, specify the following options:

- **Keep available buffer:** The minimum number of guest VMs to always keep on the VDI host and ready to be used in order to provide the fastest access to end users.
- **Delete unused guest VMs after:** Specify what to do with unused guest VMs to save resources.

Advanced

On the **Advanced** page, specify the following:

- **Folder:** Specify a folder where guest VMs created from this RAS Template will be stored. This option is available if you are using Hyper-V, Hyper-V Failover Cluster, VMware vCenter, Citrix XenServer, KVM, or Nutanix.
- **Native Pool:** Specify the native pool to add the VMs to. This option is available if you are using VMware ESX and VMware vCenter.

Preparation

Use the **Preparation** page to select and configure an image preparation tool. First, select whether you want to use RASprep or Sysprep. The advantages of using RASprep and the differences between the two tools are described below.

RASprep is the Parallels RAS tool for preparing Windows in a VM after cloning it from a base image. RASprep performs the following tasks during the initial startup of each new VM:

- Creates a new computer account in Active Directory for each guest VM.
- Gives the guest VM a new name.
- Joins the guest VM to the Active Directory domain.

Compared to Sysprep, RASprep works much faster because it modifies a lower number of configurable parameters and requires less reboots.

Note: Due to API limitations, RASprep cannot be used on Windows Server 2008 machines.

The following table lists the main differences between RASprep and Sysprep:

Operation	RASprep	Sysprep
Delete local accounts	No	Yes
Generate new SIDs	No	Yes
Unjoin the parent guest VM from the domain	No	Yes
Change computer name	Yes	Yes
Join the new instance to the domain	Yes	Yes
Language, regional settings, date and time customization	No	Yes
Number of reboots	1	2 (seal, mini-setup and domain joining)

After selecting the preparation tool, specify the following options:

- **Computer name:** A name pattern that should be used to assign a computer name. For example, Windows10-RAS-%ID%.
- **Owner name:** Owner name (optional).
- **Organization:** Organization name (optional).
- **Administrative password:** Local Windows administrator password.

- **Join domain:** A domain name for the VM to join.
- **Administrator:** Domain account.
- **Password:** Domain account password.
- **Target OU:** Full DN of an organizational unit. Click the [...] button to browse Active Directory and select an OU.

License Keys

On the **License Keys** page, specify the license key information that will be used to activate virtual machines created from this template.

First, select the license key management type that you are using in your organization (KMS or MAK). Parallels recommend to use KMS because MAK has limited activations.

Key Management Service (KMS): If you are using KMS, click the **Finish** button to save the template configuration information. Virtual machines that will be created from this template will look for KMS in DNS (at the end of the OS mini-setup and domain joining) and will be activated accordingly.

Note: If you are using KMS activation and RASPrep, the source guest VM must be activated using KMS before you create a RAS Template from it. If the guest VM has already been activated using another method (retail key or MAK), you need to convert it to KMS activation. For the information on how to do it, please read the following article from Microsoft: <https://technet.microsoft.com/en-us/library/ff793406.aspx>

Multiple Activation Keys (MAK): If you are using MAK, do the following:

- 1 Click the **Add** button and type a valid key in the **License key** field.
- 2 In the **Max. guests** field, specify the key limit. The limit should be greater than or equal to the max guests in the template (which you set on the first page of the wizard)
- 3 Click **OK**.

Note: Parallels RAS does not keep the old MAK key in guest VMs if it was updated in the Parallels RAS Template properties.

Summary

On the **Summary** wizard page, review the template summary information. You can click the **Back** button to correct some of the information if needed.

Select the **Launch Parallels RAS Test Template Wizard on completion** option to start a wizard allowing you to test the health of the template. The wizard allows you to see upon completion that all post-prep activities complete correctly. This includes checking DHCP settings, DNS registration, correct VLAN, joining the AD domain, correct target OU, etc. The wizard is described in the section that follows this one (p. 93).

Finally, click **Finish** to create the template and close the wizard.

If you need to change the template configuration later, select it in the **RAS Templates** list and click **Tasks > Properties**. Use the dialog that opens to view and modify the template properties. The dialog consists of tab pages containing the same properties as the wizard pages described above.

Parallels RAS Test Template Wizard

If you selected the **Launch Parallels RAS Test Template Wizard on completion** option on the last page of the template configuration wizard, the **Parallels RAS Test Template Wizard** opens allowing you to test the health of the RAS Template. The wizard allows you to see upon completion that all post-prep activities complete correctly. This includes checking DHCP settings, DNS registration, correct VLAN, joining the AD domain, correct target OU, etc. You can also open this wizard by right-clicking a RAS Template in the Parallels RAS console and choosing **Test**.

The test procedure consists of the following steps:

- 1 The RAS Template is switched temporarily to the "Test" mode designed specifically for this purpose. Please note that while the template is in this mode, all other operations are blocked until the test is finished and the template exits the test mode.
- 2 A guest VM is cloned from it to be used for testing. The VM is kept on the server for the duration of the test and will be deleted afterwards.
- 3 A series of tests is then run on the guest VM to test the template from which it was created.
- 4 Once the test is complete, a report is displayed on the screen showing the test results.

When the wizard starts:

- 1 The **Welcome** page opens. Read the info that it contains and click **Next** when ready.
- 2 The next page displays the list of individual tests that will be performed, including:
 - **Check guest VM Agent:** This test tries to communicate with the RAS Guest Agent installed in the VM. If the agent responds, it means that the VM has been created and started successfully.
 - **Check domain membership:** Checks that the computer has joined the AD domain.
 - **Check target OU:** Checks that the RDP connection to the computer is possible with domain credentials.
 - **Launch Parallels Client:** This test launches Parallels Client and establishes a connection with the guest VM.
- 3 While the test is running, the progress indicator is displayed on the screen. If needed, you can cancel the test at any time by clicking the **Cancel** button.
- 4 Once all tests are completed, you will see a page displaying the test results:
 - **Success:** If all tests complete successfully, the temporary guest VM will be marked for deletion and the RAS Template will be switched back to the normal operation mode.

- **Failure:** If one or more tests fail, you will see the corresponding info and will be able to download the log file by clicking the **Download log file** link. You will also have an option to switch the RAS Template to maintenance mode, which will prevent creating guest VMs from it until it is fixed.

5 Click **Finish** to close the wizard.

How Guest VMs Are Created From a Template

After a RAS Template is created, Parallels RAS begins creating guest VMs from it, one virtual machine at a time. The number of VMs created at this time is determined by the **Number of guest VMs deployed on the wizard completion** property (all property names here and later refer to the **Create Parallels RAS Template Wizard** described earlier).

The number of VMs available at any time will never go below the number specified in the **Keep available buffer** property. To comply with this rule, a new VM is automatically created when needed. At the same time, the total number of VMs will never exceed the number specified in the **Maximum guest VMs** property.

Please note that creating a new guest VM from a template takes some time, especially when a template is configured to create full clones (linked clones are created much faster). If a guest VM is in the middle of being created, and no other VMs are available, a user (or users) who need it will have to wait until the VM is ready.

If a guest VM encounters a problem during the preparation stage, it will remain on the server in unusable state. You can identify such VMs in the **Guest VM List** dialog (described in the section that follows this one) by the "Failed to create" value in the **Status** column. Unless a VM like this is repaired or recreated, it will be automatically removed after the time period specified in the **Auto remove guest VMs which failed preparation after** field on the **VDI > RAS Templates** tab page. For more information on how to recreate a guest VM, please see the **RAS Template Maintenance** section (p. 97).

Auto-deletion of guest VMs

A guest VM is automatically deleted when it is unassigned from the group and stays unassigned for the time period specified in the **Delete unused guest VMs after** field. The unassignment can happen in one of the following cases:

- A guest VM is removed manually from the group settings.
- A guest VM is removed automatically when the group workload is below the value configured in the group settings. Specifically, the least loaded RD Session Host is put into drain mode after all users are logged off and is then unassigned from the group.

Managing Guest VMs

Viewing guest VMs created from a RAS Template

To view the list of guest VMs created from a RAS Template, select a template on the **RAS Templates** tab page and click **Tasks > Show guest VM list**. The **Guest VM List** dialog opens.

Note that the **Group** column in the list identifies whether a guest VM was created from a Virtual desktop template or an RD Session Host template.

The buttons on the right side of the dialog perform the following actions:

- **Refresh.** Refreshes the list.
- **Delete.** Deletes a selected guest VM (see the **Deleting a guest VM** subsection later in this section).
- **Recreate.** Recreates a selected guest VM (see the **Recreating a guest VM** subsection later in this section).
- **Send message.** Allows you to send a message to the user who is currently connected to a guest VM. For example, when you apply updates to the parent RAS Template, you need all users to be logged off, so you can use this button to send an appropriate message to connected users.
- **Log off.** Logs off the current session from a selected guest VM.

Performing guest VM power operations

The power operations icons at the bottom of the dialog allow you to start, stop, suspend, and reset a guest VM. To perform an action, select a guest VM and click an icon corresponding to the desired action.

Please note that the following requirements and rules/exceptions apply:

- If you are using **Nutanix Acropolis**, the suspend operation is not available (the **Suspend** icon is disabled). The reason for this is Nutanix Acropolis does not support the suspend operation on its virtual machines.
- If you are using **Citrix XenServer**, guest tools must be installed in a guest VM for the **Suspend** operation to work. In addition, if guest tools are not installed, the guest VM cannot be shut down gracefully and will be stopped forcefully when you click the **Stop** icon.

Checking the RAS Guest Agent status

A guest VM should have the RAS Guest Agent installed in it and the agent should match the Parallels RAS version. The agent is installed by default when a guest VM is created from a RAS Template. If a guest VM was created outside the RAS Console using the native hypervisor tools, it may not have the agent installed in it. In such a case, the guest VM will be able to serve only the desktop, but no applications or documents.

Note: Guest VMs based on an RD Session Host template must also have the RAS RD Session Host Agent installed. The functionality described here does not verify if this agent is installed. If needed, you can use **Tasks > Check Agent** on the template itself.

To check if the RAS Guest Agent is installed in a guest VM and is up to date:

- 1 Select a guest VM in the list and then click **Tasks > Check Agent**.
- 2 The **Guest VM Agent Information** dialog opens displaying the information about the RAS Guest Agent.
- 3 If the agent is not installed, click the **Install** button and follow the instructions. The agent will be push installed in Windows running inside the guest VM.

Deleting a guest VM

To delete a guest VM, select it and then click the **Delete** button on the right side of the window.

Important: You should delete a guest VM only from the **Template Guest VMs** dialog in the Parallels RAS Console. You should NOT try to delete a guest VM using the hypervisor's native client or web interface. If you do, it may delete not only the VM but its parent RAS Template as well (which will also invalidate all other guest VMs created as linked clones from this template). The reason for this is some native hypervisor clients treat linked clones as standalone VMs. Parallels RAS treats linked clones as clones, not as standalone VMs.

Managing guest VMs that failed preparation

If a guest VM encounters a problem during the preparation stage (for any reason), it remains on the server but cannot be used. You can identify such VMs in the **Template Guest VMs List** dialog (described above) by the "Failed to create" value in the **Status** column. Unless a VM like this is repaired, it will be automatically removed after the time period specified in the **Auto remove guest VMs which failed preparation after** field on the **RAS Templates** tab page. You can set any of the available time periods by selecting it from the drop-down list or you can type a desired value, such as "8 days" or "12 hours".

Recreating a guest VM

If something happens to a guest VM and it becomes unusable, you don't have to delete it and create a new one. Instead, you can recreate it keeping its name and MAC address (to guarantee that VM will get the same IP address from the DHCP server). This way none of the other site settings, which may rely on a broken guest VM, will be affected. Another reason for recreating a guest VM is to apply changes made to the RAS Template (when you exit from maintenance without executing the Recreate command). Please note that keeping the MAC address is supported on ESXi, vCenter, Hyper-v and Hyper-v Failover Cluster only.

Note: If a guest VM was created from an RD Session Host template and was already assigned to an RD Session Host group, it cannot be recreated.

To recreate one or more guest VMs:

- 1 In the Parallels RAS Console, navigate to **Farm \ <site> \ VDI \ RAS Templates**.
- 2 To recreate all deployed guest VMs, click the **Tasks** drop-down menu and choose **Recreate All Guest VMs**.
- 3 To recreate a specific guest VM (or multiple guest VMs), click **Tasks > Show Guest VMs**.
- 4 In the **Template Guest VMs** dialog, select one or more guest VMs and then click the **Recreate** button.

When you recreate a guest VM:

- The procedure deletes a VM and creates a new one from the same template.
- The new guest VM retains the same computer name as the one it replaces.
- If a guest VM is running, all unsaved data in its memory will be lost. For this reason, an important data should be saved to a disk.

RAS Template Maintenance

In addition to viewing and modifying configuration properties of a RAS Template, you can perform a number of maintenance tasks on it. These tasks are described below.

Updating RAS Guest Agent inside a template

A RAS Template must have the latest version of RAS Guest Agent installed in it. The agent is installed when you create a template. When a new version of RAS Guest Agent becomes available, it should be updated.

When the Parallels RAS Console is started, it may display a message box saying that agents need to be installed or updated. This happens when one or more servers or templates have no agent installed or when an agent is outdated. The message will ask if you want to update all agents. If you click **Yes**, you are presented with a dialog listing all servers and templates on which an agent needs to be updated. You can select or un-select a server/template to include it in the bulk update procedure or exclude it. Once you've made your selection, click **OK** to start the update. Follow the onscreen instructions and update the agents. Read the note below!

Full vs. linked clone templates: When you update RAS Guest Agent in a template, you also need to update Agents in guest VMs that were created from this template. This update is done differently for full and linked clone templates. Please read the instructions below for the explanation.

When you update the Agent in a linked clone template, you'll be asked if you want to recreate all guest VMs that were created from this template. You can click **Yes** and they will be automatically recreated to match the template.

When you update the Agent in a full clone template, full clone guest VMs are NOT recreated at this time. This is due to the fact that full clone VMs are complete machines (as opposed to linked clones which share the virtual hard disk with a snapshot of the template) and so recreating them would be a time consuming procedure. Therefore it is much faster and easier to update the Agent in these VMs by push-installing it from the RAS Console. This can be done by clicking **Tasks > Upgrade all Agents** in one of the following views/dialogs:

- **VDI / Virtual desktop hosts / Virtual Guests Settings**
- **VDI / Pool management > Show guest VMs in pool**
- **VDI / RAS templates > Show guest VMs**
- **VDI / Desktops**

To manually check the RAS Guest Agent status inside a template, click **Tasks > Check agent**. If the agent is up to date, a message box will be displayed confirming this. If a newer version of RAS Guest Agent is available, you'll see a dialog asking if you want to update it. Click **Yes** to update the agent. If you click **No**, you can check the status again later and update the agent at that time. Please note that the difference in updating full and linked clone templates (as described above) applies to this scenario as well.

Using the RAS Template maintenance mode

The RAS Template maintenance mode is used to update software inside a RAS Template. For instance, if you want to install a Windows server pack or a software update, you need to use the maintenance mode.

Depending on whether a RAS Template is configured for full or linked clones, the maintenance mode is used slightly differently.

Full clones:

If your RAS Template is configured to create full clones, do the following:

- 1 Select a RAS Template and click **Tasks > Maintenance**. The template becomes disabled (grayed out), so all operations on it (including creating new guest VMs) are suspended.
- 2 Using native tools of the corresponding hypervisor, start the template as a normal virtual machine.
- 3 Install Windows updates or software as necessary.
- 4 When done, shut down the virtual machine.
- 5 Back in the RAS Console, select the template and click **Tasks > Maintenance** again to exit the maintenance mode.

Note: Please note that any updates applied to a full clone template in the maintenance mode will only affect future clones. Existing guest VMs that were created from this template as full clones will not be affected, so if you want these VMs to include these updates, you will have to recreate them.

Linked clones:

Since linked clones share the virtual hard disk with a snapshot of a RAS Template, you need to take additional steps compared to full clones.

First, you need to notify guest VM users to save their data and log off. This is necessary for existing guest VMs to include the updates that you will install in the template. Once all users are logged off, do the following:

- 1 Select the RAS Template and click **Tasks > Maintenance**. The template becomes disabled (grayed out), so all operations on it (including creating new guest VMs) are suspended.
- 2 Using native tools of the corresponding hypervisor, start the template as a normal virtual machine.
- 3 Install Windows updates or software as necessary.
- 4 When done, shut down the virtual machine.
- 5 Back in the RAS Console, select the template and click **Tasks > Maintenance** again to exit the maintenance mode. A dialog is displayed asking if you would like to recreate existing guest VMs. If you click **No**, then the dialog is closed and the existing guest VMs are left in their current state, which means that the updates that you installed will NOT appear in the existing VMs. If you click **Yes**, read on.
- 6 If you click **Yes** in the previous step, existing guest VMs will be examined for active connections. If an active connection is detected, another dialog opens asking if you want to proceed:
 - If you click **Yes**, all active sessions are forcibly logged off and existing guest VMs (linked clones), together with the corresponding snapshot, are deleted and a new snapshot and VMs are created from the updated RAS Template.

- If you click **No**, the **Template Guest VMs List** dialog opens where you can view the current state of each available guest VM. The dialog gives you full control over a guest VM. You can send a message to the user and you can log the user off. Once all active sessions are logged off, click **OK**. The existing guest VMs and the corresponding snapshot are deleted and a new snapshot and VMs are created from the updated RAS Template.

When you are done configuring a RAS Template, click the **Apply** button on the main RAS Console window to commit the changes to Parallels RAS.

Please note that if you leave the maintenance mode without recreating linking clones, you will have to enter the maintenance mode again to apply the updates.

Maintaining RD Session Hosts based on a RAS Template

If you need to do a scheduled maintenance of RD Session Hosts that were created from a RAS Template, please follow these steps:

- 1 Create a schedule that fits your maintenance window to drain a desired RD Session Host group.
- 2 During maintenance (or right before it) switch the template into maintenance mode. Then apply the necessary changes.
- 3 The schedule disables groups provisioned by the template (while the maintenance window lasts) which leads to removing (unassigning) all guest VMs from them.
- 4 Release the template from maintenance and click **Yes** when asked whether to recreate all clones.
- 5 Enable groups which were disabled in step 3 (above). At this point, the groups will begin receiving guest VMs to comply with **Keep Available Buffer** setting
- 6 From this point forward, groups are provisioned with VMs on demand.

VDI Host Pool Management

Pools offer administrators more flexibility when managing an extensive number of guest VMs, especially when they are implemented in large company infrastructures. The RAS Console provides you with the framework and tools needed to create a complete pool management foundation. To manage pools, in the RAS Console, navigate to **Farm** / <site> / **VDI** and then click the **Pool Management** tab.

Read on to learn how to:

- Add and delete pools (p. 101)
- Add and delete pool members (p. 101)
- Configure guest VMs in a pool (p. 101)
- Use a wildcard to filter VMs (p. 103)

Adding and Deleting Pools

To add a pool, click the **Tasks** drop-down menu above the **Pools** list and then click **Add** (or click the plus-sign icon). Type a pool name and then click anywhere outside the edit field.

To delete a pool, right-click it and then click **Delete** (or click the minus-sign icon, or **Tasks > Delete**).

Adding and Deleting Pool Members

A VDI pool can contain different types of members. These could be all available guest VMs, specific guest VMs, and guest VMs created from a template.

To add a member to a pool:

- 1 Select a pool in the **Pools** list.
- 2 In the **Tasks** drop-down menu above the **Members** list (the upper right-hand corner of the **Members** area), click **Add** and choose a member type from the following list:
 - **All guest VMs in host.** All guest VMs that are located on a particular VDI host. After clicking this options, you'll be able to select a VDI host.
 - **Guest VM.** A specific guest VM located in the farm. After clicking this options, you'll be able to select a guest VM from the list.
 - **Native pool.** A group of guest VMs that were natively configured in the hypervisor as a pool. Please note that a hypervisor may use a different term for pools (e.g. "resource pools"). After clicking this option, you'll be able to select a native pool from the list, if any are available.
 - **RAS Template.** Guest VMs that are automatically created from a RAS Template. After selecting this option, you'll be able to select a RAS Template. For more information about RAS Templates, refer to **Managing RAS Templates** (p. 85).
- 3 After you click one of the above menu items, you will be presented with the list of the available hosts, guest VMs, or templates from which you can make your selection.

To delete a member from a pool, select the pool, then select a pool member you wish to delete, and then click **Tasks > Delete**.

Configuring Guest VMs in a Pool

To configure a guest VM included in a pool, select a pool and then click **Tasks > Show Guest VMs in Pool** to open the **Guest VM List** dialog.

Checking the RAS Guest Agent status

A guest VM must have the RAS Guest Agent installed in it. The agent is installed by default when a guest VM is created from a RAS Template. If a guest VM was created outside the RAS Console using the native hypervisor tools, it may not have the agent installed in it. In such a case, the guest VM will be able to serve only the desktop, but no applications or documents.

To check if the RAS Guest Agent is installed in a guest VM:

- 1 Select a guest VM in the list and then click **Tasks > Troubleshooting > Check agent**.
- 2 The **Guest VM Agent Information** dialog opens displaying the information about the RAS Guest Agent.
- 3 If the agent is not installed, click the **Install** button and follow the instructions. The agent will be push installed in Windows running inside the guest VM.

Performing guest VM power operations

The power operations icons at the bottom of the dialog allow you to start, stop, suspend, and reset a guest VM.

Note: If you are using Nutanix Acropolis, the suspend operation is not available (the **Suspend** icon is disabled). The reason for this is Nutanix Acropolis does not support the suspend operation on its virtual machines.

Configuring guest VM properties

To view and modify properties of a guest VM:

Select a guest VM and click **Tasks > Properties**. The **Guest VM Advanced Settings** dialog opens. In the dialog, configure the following properties:

- **Do not use this guest VM.** If selected, the guest VM will not be used for remote application and desktop publishing.
- **Computer name.** Specifies the network name (domain name / IP address) that the system will use to connect to this guest VM.
- **Port.** Specifies the port number that the system will use to connect to this guest VM.
- **Override default settings.** Allows you to specify your own VM settings. By default, this option is cleared, so a VM is configured using default settings. To specify custom VM settings, select this option and then choose your own values for **Connection timeout**, **Protocol**, **If session disconnects**, and **End a disconnected session** options. For the descriptions of these options, please see the **Configuring Default Guest VM Properties** subsection below.

Configuring default guest VM properties

By default, all guest VMs in a site are configured using the default VM settings which are defined on a site level and automatically applied to all newly created VMs.

To view and modify the default settings, in the **Guest VM List** dialog, click **Tasks > Default settings** (or click the gear icon). The **Default Guest VM Advanced Settings** dialog allows you to view and modify the following properties:

- **Connection timeout.** If a connection with the guest VM cannot be established in this time period, Parallels RAS will cancel the connection attempt.
- **Protocol.** Specifies a protocol that Parallels RAS uses to communicate with the guest VM.
- **If session disconnects.** Specifies the action that should be taken if a user disconnects from a session. Actions include **Suspend, Reset, Keep Current State, Stop**. Use the **after** field to specify the amount of time that has to pass before the selected action takes place.

Note for Nutanix Acropolis users: Nutanix Acropolis does NOT support the suspend operation on its VMs. If **Suspend** is selected in this field, no action will be applied to a Nutanix Acropolis VM when a session disconnect event occurs (a corresponding error will be recorded in the VDI Agent log). Since **Suspend** is the default action, you should consider selecting a different one if you are using Nutanix Acropolis.

Any modifications you make to default VM settings are immediately applied to all VMs in the current site that use them.

Using a Wildcard to Filter VMs

Use the **Wildcard** input field at the bottom of the **Pool management** tab to specify a wildcard to indicate which guest VMs should be available for users. If a VM name matches the wildcard, it will be available. If not, the users will not be able to use it. Use the asterisk operator (*) to specify a wildcard (e.g. ABC*, *ABC*).

Persistent Guest VMs

A guest VM is called persistent when it is assigned to a particular user. To make a guest VM persistent, do the following:

- 1 Begin publishing a desktop or a resource hosted by the guest VM.
- 2 When specifying **Guest VM Settings** options, select **Persistent** (see **Publishing an Application from a Guest VM** (p. 105) for an example of the **Persistent** option; other types of resource also have it).
- 3 Complete the publishing wizard.

As a result, the first user who uses a desktop or a resource from this guest VM will become the owner of the VM (i.e. the VM will be assigned to the user).

To view persistent guest VMs:

- 1 In the Parallels RAS Console, navigate to **Farm** / <site> / **VDI**.
- 2 Select the **Desktops** tab in the right pane.

The tap page lists guest VMs, each of which is currently assigned to a particular user. The information includes the user name, guest VM name, pool name, VDI host, last time a VM was used, etc.

To remove persistence from a guest VM, do one of the following:

- Select a guest VM on the **Desktops** tab page and then click **Tasks** > **Delete**.
- Use the **Auto remove persistence if guest VM was not used for** drop-down menu to define an automatic removal rule. In the menu, select the time period after which persistence should be automatically removed. You can also type any desired time period, such as "1 week 3 days".

Publishing from a Guest VM

This section describes how to publish resources hosted by a guest VM. The publishing functionality described here is accessed from the **Publishing** category in the RAS Console.

Publishing a Desktop from a Guest VM

To publish a virtual desktop from a guest VM or guest VM clone, follow the below procedure:

- 1 In the RAS Console, select the **Publishing** category and click the **Add** icon below the **Published Resources** tree. This will launch the publishing wizard.
- 2 In the first step of the wizard select **Desktop** and click **Next**.
- 3 On the **Select Desktop Type** page, select **Guest VM Desktop** and click **Next**.
- 4 On the **Guest VM Desktop** page, enter a desktop name, an optional description, and change the icon if needed.
- 5 In the **Guest VM settings** section, specify from where the desktop should be published. First, you need to select an option in the **Connect to** drop-down list and then specify an additional parameter in the field below it as follows:
 - **Any guest VM**. Use the **from Pool** drop-down list to specify a pool.

- **Specific guest VM.** To select a guest VM, expand the **Guest** drop-down list. This opens the **Guest VM List** dialog. Please note that in order to select a guest VM, it must have RAS Guest Agent installed. To verify this, look at the **Status** column, which should say "OK". If you select a guest VM that has any other value in the **Status** column, you will be asked to install the RAS Guest Agent in the VM before you can proceed (note that if the selected guest VM was stopped, it will be automatically started).
 - **Guest VM.** Specify the pool in the **from Pool** drop-down list and then specify **where name equals** Username or IP.
 - **Specific RAS Template.** Select a template by expanding the RAS Template drop-down list.
- 6 Select the **Persistent** option to mark a guest VM as persistent the first time a user connects to it.
 - 7 In the **Desktop Size** section, specify the desktop screen resolution and size.
 - 8 Click **Finish** when done.

Publishing an Application from a Guest VM

To publish an application from a guest VM or guest VM clone:

- 1 In the RAS Console, select the **Publishing** category and then click the **Add** icon below the **Published Resources** tree (or right-click inside the **Published Resources** box and click **Add** in the context menu). This will launch the publishing wizard.
- 2 On the **Select Item Type** wizard page, select **Application** and click **Next**.
- 3 On the **Select Server Type** page, select **Guest VM** and click **Next**.
- 4 On the **Select Application Type** page, select **Single application** and click **Next**. The **Application** page opens.
- 5 Enter a name and an optional description.
- 6 In the **Run** drop-down menu, specify if the application should run in a normal window, maximized, or minimized.
- 7 In the **Target** field, specify the application that you want to publish. You may click the **[...]** button to browse for it.
- 8 In the **Start in** field, specify (or browse for) the "start in" folder. Use Windows environment variables if you are manually entering the path.
- 9 (Optional) In the **Parameters** input field, specify the parameters to pass to the application when it starts.
- 10 In the **Guest VM settings** section, specify from where the application should be published. First, you need to select an option in the **Connect to** drop-down list and then specify an additional parameter in the field below it, as explained below:
 - **Any guest VM.** Use the **from Pool** drop-down list to specify a pool.

- **Specific guest VM.** To select a guest VM, expand the **Guest** drop-down list. This opens the **Guest VM List** dialog. Please note that in order to select a guest VM, it must have RAS Guest Agent installed. To verify this, look at the **Status** column, which should say "OK". If you select a guest VM that has any other value in the **Status** column, you will be asked to install the RAS Guest Agent in the VM before you can proceed (note that if the selected guest VM was stopped, it will be automatically started).
 - **Guest VM.** Specify the pool in the **from Pool** drop-down list and then specify **where name equals** Username or IP.
 - **Specific RAS Template.** Select a template by expanding the RAS Template drop-down list.
- 11** Select the **Persistent** option to mark a guest VM as persistent the first time a user connects to it.
- 12** When done, click **Finish** to publish the application.

Publishing a Web Application from a Guest VM

A web application is like any other application that you can publish using the standard application publishing functionality. However, to simplify publishing of straight URL links to web applications, a separate publishing item type is available that allows you to accomplish this task with minimal number of steps.

To publish a web application:

- 1** In the RAS Console, select the **Publishing** category and then click the **Add** icon below the **Published Resources** tree (or right-click inside the **Published Resources** box and click **Add** in the context menu). This will launch the publishing wizard.
- 2** On the **Select Item Type** wizard page, select **Web application** and click **Next**.
- 3** On the **Select Server Type** page, select **Guest VM** and click **Next**.
- 4** On the **Virtual Desktop Web Application** wizard page that opens, specify the web application name, description, window state, and the URL. Select the **Force to use Internet Explorer** option if needed. To browse for a specific application icon, click **Change Icon**.
- 5** Use the **Guest VM settings** section to specify from where the application should be published.

The options are:

- **Any guest VM.** Publish the application from any guest VM in the selected pool. Select this option and then select a pool in the **from Pool** drop-down list.
- **Specific guest VM.** To select a guest VM, expand the **Guest** drop-down list. This opens the **Guest VM List** dialog. Please note that in order to select a guest VM, it must have RAS Guest Agent installed. To verify this, look at the **Status** column, which should say "OK". If you select a guest VM that has any other value in the **Status** column, you will be asked to install the RAS Guest Agent in the VM before you can proceed (note that if the selected guest VM was stopped, it will be automatically started).

- **Guest VM.** Select this option and then select a pool in **from Pool**. In the **where name equals** drop-down list, select **Username** or **IP**. The application will be published from a guest VM from the selected pool whose name/IP matches the username/IP of the user connecting.
- **Specific RAS Template.** Publish the application from a specific RAS Template. Select this option and then select a template in the **RAS Template** drop-down list.

Select the **Persistent** option to mark a guest VM as persistent the first time a user connects to it.

- 6 When done, click **Finish** to publish the application.

Publishing a Network Folder from a Guest VM

You can publishing a filesystem folder via UNC path to open in Windows explorer. To minimize the number of configuration steps, a special publishing item is available that allows you to publish a network folder from a guest VM.

To publish a network folder:

- 1 In the RAS Console, select the **Publishing** category and then click the **Add** icon below the **Published Resources** tree (or right-click inside the **Published Resources** box and click **Add** in the context menu). This will launch the publishing wizard.
- 2 On the **Select Item Type** wizard page, select **Folder on the file system** and click **Next**.
- 3 On the **Select Server Type** page, select **Guest VM** and click **Next**.
- 4 On the **Virtual Desktop UNC Folder** wizard page, specify the usual application properties.
- 5 In the **UNC path** field, enter the UNC path of the folder you wish to publish. Click the **[...]** button to browse for a folder (it may take some time for the **Browse for Folder** dialog to open).
- 6 In the **Guest VM settings** section, specify from where the virtual desktop should be published. First, you need to select an option in the **Connect to** drop-down list and then specify an additional parameter in the field below it, as explained below:
 - **Any guest VM.** Use the **from Pool** drop-down list to specify a pool.
 - **Specific guest VM.** To select a guest VM, expand the **Guest** drop-down list. This opens the **Guest VM List** dialog. Please note that in order to select a guest VM, it must have RAS Guest Agent installed. To verify this, look at the **Status** column, which should say "OK". If you select a guest VM that has any other value in the **Status** column, you will be asked to install the RAS Guest Agent in the VM before you can proceed (note that if the selected guest VM was stopped, it will be automatically started).
 - **Guest VM.** Specify the pool in the **from Pool** drop-down list and then specify **where name equals** Username or IP.
 - **Specific RAS Template.** Select a template by expanding the RAS Template drop-down list.
- 7 Select the **Persistent** option to mark a guest VM as persistent the first time the user connects to it.

- 8 Click **Finish** to publish the folder and close the wizard.

When published, the network folder will appear in the **Publishing > Published resources list**, just like any other application. To view its properties, select it and then click the **Virtual Desktop Application** tab:

- The **Target** property will always be set to `PublishedExplorer.exe`. This binary is created automatically (via agents pushing) and is simply a copy of the standard `explorer.exe` executable.
- The **Parameters** property specifies the network folder that we want to publish. The folder path can be in any format that the `explorer.exe` can handle.

Publishing a Document from a Guest VM

To publish a document from a guest VM or guest VM clone:

- 1 In the RAS Console, select the **Publishing** category and then click the **Add** icon below the **Published Resources** tree (or right-click inside the **Published Resources** box and click **Add** in the context menu). This will launch the publishing wizard.
- 2 On the **Select Item Type** wizard page, select **Document** and click **Next**.
- 3 Select **Guest VM** and click **Next**.
- 4 Specify the content type of the document you want to publish. You can select the content type from the predefined list or specify a custom content type in the **Custom content types** input field.
- 5 Click **Next**.
- 6 On the **Virtual Desktop Application** page, enter a name, an optional description, a Window state, and an icon if needed.
- 7 Use the [...] button next to the **Target** input field to browse for the document. All other fields will be automatically populated. To edit any of the auto populated fields, highlight them and enter the required details.
- 8 (Optional) In the **Parameters** input field, specify the parameters to pass to the application when it starts.

Note: Use the **Server(s)** drop down list to specify different document settings for a specific server in case the document is configured differently on that particular server. The settings will be saved for each server you select individually.

- 9 In the **Guest VM settings** section, specify from where the virtual desktop should be published. First, you need to select an option in the **Connect to** drop-down list and then specify an additional parameter in the field below it, as explained below:
 - **Any guest VM.** Use the **from Pool** drop-down list to specify a pool.

- **Specific guest VM.** To select a guest VM, expand the **Guest** drop-down list. This opens the **Guest VM List** dialog. Please note that in order to select a guest VM, it must have RAS Guest Agent installed. To verify this, look at the **Status** column, which should say "OK". If you select a guest VM that has any other value in the **Status** column, you will be asked to install the RAS Guest Agent in the VM before you can proceed (note that if the selected guest VM was stopped, it will be automatically started).
 - **Guest VM.** Specify the pool in the **from Pool** drop-down list and then specify **where name equals** Username or IP.
 - **Specific RAS Template.** Select a template by expanding the RAS Template drop-down list.
- 10** Select the **Persistent** option to mark a guest VM as persistent the first time the user connects to it.
- 11** Click **Finish** to publish the document.

Viewing VDI Host Summary

In addition to the VDI Hosts editor described in this chapter, you can also see the summary about the available VDI Hosts. To do so:

- 1** In the RAS Console, select the **Farm** category and then select the **Site** node in the middle pane.
- 2** The available servers are displayed in the **VDI** group in the right pane.
- 3** To go to the VDI Hosts editor, right-click a server and choose **Show in the Editor**.

For additional info, see **Sites in the RAS Console** (p. 36).

Managing VDI Sessions

The **Sessions** tab page allows you to view and manage current VDI sessions. To view the page, navigate to **Farm / <site> / VDI / Sessions**.

The **Sessions** lists displays current sessions and includes the following info for each session:

- **Guest VM.** Guest VM name.
- **Theme.** The theme used.
- **User.** Session owner.
- **State.** Session state: **Idle**, **Active**, **Disconnected**.
- **Logon time.** Last date and time the user logged on.
- **Session length.** Total sessions duration.
- **Resolution.** Client display resolution.

- **Color Depth.** Client display color depth.
- **Device Name.** Client device name.
- **IP Address.** Client IP address.

You can sort the list by any session property. Simply click on a desired column heading to sort the list in ascending or descending order.

You can also filter the list using a single or multiple session properties as a criteria. To do so, click the magnifying glass icon (top right) and then type a desired string in a desired column. The list will be filtered as you type.

To manage a session (or multiple sessions at the same time), select one or more sessions and then use the **Tasks** drop-down menu to choose from the following actions:

- **Refresh.** Refresh the list.
- **Disconnect.** Disconnect the selected session(s).
- **Log Off.** Log off the session(s).
- **Send Message.** Opens the **Send Message** dialog where you can type and send a message to the session owner(s).

Remote PCs

In addition to RD Session Hosts and VDI guest VMs, resources can also be published from a standalone remote PC running a supported version of Windows. A remote PC can be a physical box or a virtual machine treated as a physical PC, but typically they are physical computers. If you have virtual machines on your network, it makes sense to use them as part of the VDI infrastructure as was described in the **VDI and Virtual Desktops** chapter (p. 77). However, if you don't need the guest VM cloning functionality or, for example, if your end users require full administrative permissions for customization, you can use a virtual machine as a remote PC. It's up to you.

Note: Remote PCs can also be combined into pools and managed as pool members. Remote PC pools use the RAS VDI infrastructure and work differently than individual Remote PCs described in this chapter. For more information see **Remote PC Pools**.

This chapter describes how to add a remote PC to a site and how to publish remote applications and desktop from it.

In This Chapter

Adding a Remote PC.....	111
Installing Remote PC Agent Manually.....	112
Configuring a Remote PC.....	113
Viewing Remote PC Summary.....	115
Publishing from a Remote PC.....	115

Adding a Remote PC

Requirements to push install RAS Remote PC Agent on a PC

To push install the RAS Remote PC Agent on a PC, the following requirements must be met:

- The firewall must be configured on the server to allow push installation. Standard SMB ports (139 and 445) need to be open. See also **Port Reference** (p. 289) for the list of ports used by Parallels RAS.
- SMB access. The administrative share (\\server\c\$) must be accessible. Simple file sharing must be enabled.
- Your Parallels RAS administrator account must have permissions to perform a remote installation on the PC. If it doesn't, you'll be asked to enter credentials of an account that does.

- The PC should be joined to an AD domain. If it's not, the push installation may not work and you will have to install the Agent on it manually. Please see **Installing Remote PC Agent Manually** (p. 112).

Add a Remote PC to the farm

Follow the below procedure to add a remote PC to the farm:

- 1** In the RAS Console, select the **Farm** category and click the **Remote PCs** node in the navigational tree.
- 2** Click **Add** in the **Tasks** drop-down menu to launch the setup wizard.
- 3** Specify the IP address or FQDN of a remote PC. Click the Get MAC button to obtain the PC's MAC address.
- 4** Click **Next**.
- 5** In this step, the Parallels RAS checks if the Remote PC Agent is installed on the specified PC. If it's not installed, click **Install** to push install the agent on the PC. If the push installation of Remote PC Agent fails for any reason, you can install it manually. See **Installing Remote PC Agent Manually** for details (p. 112).
- 6** Click **Add** to add the Remote PC to the Parallels RAS farm.

Installing Remote PC Agent Manually

You may need to install the Remote PC Agent manually if the automatic push installation cannot be performed for any reason.

Installing Remote PC Agent Manually

- 1** Log into the PC where the Remote PC Agent is to be installed using an administrator account and close all other applications.
- 2** Copy the Parallels RAS installation file (`RASInstaller.msi`) to the PC and double click it to launch the installation.
- 3** Once prompted, click **Next** and accept the End-User license agreement.
- 4** Specify the path where the Remote PC Agent should be installed and click **Next**.
- 5** Select **Custom** and click **Next**.
- 6** Click on the **Remote PC Agent** and select **Entire Feature will be installed on local hard drive** from the drop down menu.
- 7** Ensure that all other components are deselected and click **Next**.
- 8** Click **Install** to start the installation. Click **Finish** once the installation is finished.

Remote PC Agent does not require any configuration. Once the agent is installed, select the Remote PC name in the Parallels RAS Console and click **Troubleshooting > Check Agent**. If the agent is installed properly, the status should change to **Agent Installed**.

Uninstalling Remote PC Agent

To uninstall Remote PC Agent from a server:

- 1 Navigate to **Start > Control Panel > Programs > Uninstall a Program**.
- 2 Find **Parallels Remote Application Server** in the list of installed programs.
- 3 If you don't have any other Parallels RAS components on the server that you want to keep, right-click **Parallels Remote Application Server** and then click **Uninstall**. Follow the instructions to uninstall the program. You may skip the rest of these instructions.
- 4 If you have other RAS components that you want to keep on the server, right-click **Parallels Remote Application Server** and then click **Change**.
- 5 Click **Next** on the Welcome page.
- 6 On the **Change, repair, or remove** page, select **Change**.
- 7 On the next page, select **Custom**.
- 8 Select **Remote PC Agent**, then click the drop-down menu in front of it, and click **Entire feature will be unavailable**.
- 9 Click **Next** and complete the wizard.

Configuring a Remote PC

To access the properties of a Remote PC, highlight the computer in the navigation tree and click **Tasks > Properties**. This opens the Remote PC properties dialog.

Properties

By default, a PC is enabled in the farm. When it is disabled, published applications and virtual desktops cannot be served from it. To enable or disable a PC in the farm, select or clear the **Enable Remote PC** option.

If the IP or MAC address of a remote PC has changed, modify them using the **Remote PC** and **MAC Address** input fields.

The **Change Direct Address** option allows you to specify an IP address that Parallels Client can use to connect to the PC directly. This address is only used in the Direct Connection mode and it could be an internal or external IP address.

Note: The Wake On Lan option should be enabled in BIOS so the machine could be automatically turned on. If you are using a virtual machine, the option is usually supported by a hypervisor natively or via a 3rd party software. To test if the Wake On Lan option is turned on, close the **Remote PC Properties** dialog and then click the **Test Wake on LAN** button, which is located below the **Remote PCs** list.

Agent Settings

Each Remote PC in the farm has a RAS Remote PC Agent installed to provide a connection between the Parallels RAS and the PC. The agent can be configured on the **Agent Settings** tab page.

- **Port.** Specify a different remote desktop connection port number if needed.
- **Connection Timeout.** Select the desired Remote PC connection timeout value.
- **Publishing Session Timeout.** Specify the amount of time each session remains connected in the background after the user has closed the published application. This option is used to avoid unnecessary reconnections with the PC.
- **Allow Client URL/Mail Redirection.** Enable this option to allow "http" and "mailto" links to be opened using a local application on the client computer, rather than the server's resources. To configure a list of URLs which should be excluded, in the RAS Console, navigate to **Farm / <site> / Settings** and click the **URL Redirection** tab.
- **Preferred Publishing Agent.** Select a Publishing Agent with which the Remote PC Agent should communicate. This can be helpful when site components are installed in multiple physical locations communicating through WAN. You can decrease network traffic by specifying a more appropriate Publishing Agent.
- **Allow file transfer command.** Allows you to enable or disable the remote file transfer functionality. For more information, see **Enabling or Disabling Remote File Transfer** (p. 231).
- **Allow local to remote drag and drop.** Enables the drag and drop functionality in a remote application. When this option is enabled, an end user can drag and drop files to a remote application on their local device. For example, a user can drag and drop a file to the Acrobat reader to open a PDF file. Or a user can drag and drop a file to Windows Explorer running on a remote server, etc.

Note: At the time of this writing, the drag and drop functionality is only supported on Parallels Client for Windows and Parallels Client for Mac.

RDP Printer

The **RDP Printer** tab allows you to configure the renaming format of redirected printers. The format may vary depending on which version and language of the server you are using.

Set your RDP Printer Name Format specifically for the configured server by choosing any of the below options from the RDP Printer Name Format drop down menu:

- Printername (from Computername) in Session no.
- Session no. (computername from) Printername

- Printername (redirected Session no)

The other RDP Printing options available in the RDP Printer tab are:

- Remove session number from printer name
- Remove client name from printer name

Viewing Remote PC Summary

In addition to the Remote PCs editor described in this chapter, you can also see the summary about the available Remote PCs. To do so:

- 1 In the RAS Console, select the **Farm** category and then select the **Site** node in the middle pane.
- 2 The available servers are displayed in the **Remote PCs** group in the right pane.
- 3 To go to the Remote PCs editor, right-click a server and choose **Show in the Editor**.

For additional info, see **Sites in the RAS Console** (p. 36).

Publishing from a Remote PC

This section describes how to publish resources hosted by a standalone remote PC. The publishing functionality described here is accessed from the **Publishing** category in the RAS Console.

Read on to learn how to publish resources from a remote PC.

Publishing a Desktop from a Remote PC

To publish a desktop from an RD Session Host:

- 1 In the RAS Console, select the **Publishing** category and click the **Add** icon below the **Published Resources** tree. This will launch the publishing wizard.
- 2 In the first step of the wizard select **Desktop** and click **Next**.
- 3 On the **Select Desktop Type** page, select **Remote Desktop PC** and click **Next**. The **Remote PC Desktop** page opens.
- 4 Specify a name, an optional description, and change the icon if needed.
- 5 Click the **[...]** button next to the **Selected Remote PC** field to specify from which remote PC the desktop should be published. In the box that opens, double-click a PC to select it.
- 6 Select the desired **Desktop Size** properties.
- 7 Click **Finish** to publish the desktop.

Publishing an Application from a Remote PC

To publish an application from a remote PC:

- 1 In the RAS Console, select the **Publishing** category and then click the **Add** icon below the **Published Resources** tree (or right-click inside the **Published Resources** box and click **Add** in the context menu). This will launch the publishing wizard.
- 2 On the **Select Item Type** wizard page, select **Application** and click **Next**.
- 3 On the **Select Server Type** page, select **Remote PC** and click **Next**.
- 4 On the **Select Application Type** page, select **Single Application** and click **Next**. The **Remote PC Application** page opens.
- 5 Enter a name and an optional description.
- 6 In the **Run** drop-down menu, specify if the application should run in a normal window, maximized, or minimized.
- 7 In the **Target** field, specify the application that you want to publish. You may click the **[...]** button to browse for it.
- 8 In the **Start in** field, specify (or browse for) the "start in" folder. Use Windows environment variables if you are manually entering the path.
- 9 (Optional) In the **Parameters** input field, specify the parameters to pass to the application when it starts.
- 10 Click the **[...]** button in the **Remote PC Settings** section to select a remote PC from which the application should be published. In the box that opens, double-click a PC to select it.
- 11 Select the **Persistent** option to mark a guest VM as persistent the first time the user connects to it.
- 12 When done, click **Finish** to publish the application.

Publishing a Web Application from a Remote PC

A web application is like any other application that you can publish using the standard application publishing functionality. However, to simplify publishing of straight URL links to web applications, a separate publishing item type is available that allows you to accomplish this task with minimal number of steps.

To publish a web application:

- 1 In the RAS Console, select the **Publishing** category and then click the **Add** icon below the **Published Resources** tree (or right-click inside the **Published Resources** box and click **Add** in the context menu). This will launch the publishing wizard.
- 2 On the **Select Item Type** wizard page, select **Web Application** and click **Next**.
- 3 On the **Select Server Type** page, select **Remote PC** and click **Next**.

- 4 On the **Remote PC Web Application** wizard page that opens, specify the web application name, description, window state, and the URL. Select the **Force to use Internet Explorer** option if needed. To browse for a specific application icon, click **Change Icon**.
- 5 In the **Remote PC Settings** section, click the [...] button to select a remote PC.
- 6 Click **Finish** to publish the application.

Publishing a Network Folder from a Remote PC

You can publishing a filesystem folder via UNC path to open in Windows explorer. To minimize the number of configuration steps, a special publishing item is available that allows you to publish a network folder from a PC.

To publish a network folder:

- 1 In the RAS Console, select the **Publishing** category and then click the **Add** icon below the **Published Resources** tree (or right-click inside the **Published Resources** box and click **Add** in the context menu). This will launch the publishing wizard.
- 2 On the **Select Item Type** wizard page, select **Folder on the file system** and click **Next**.
- 3 On the **Select Server Type** page, select **Remote PC** and click **Next**.
- 4 On the **Remote PC UNC Folder** wizard page, specify the usual application properties.
- 5 In the **UNC path** field, enter the UNC path of the folder you wish to publish. Click the [...] button to browse for a folder (it may take some time for the **Browse for Folder** dialog to open).
- 6 In the **Remote PC Settings** section, select the [...] button and then select a remote PC from the list.
- 7 Click **Finish** to publish the folder and close the wizard.

Publishing a Document from a Remote PC

To publish a document from a remote PC clone:

- 1 In the RAS Console, select the **Publishing** category and then click the **Add** icon below the **Published Resources** tree (or right-click inside the **Published Resources** box and click **Add** in the context menu). This will launch the publishing wizard.
- 2 On the **Select Item Type** wizard page, select **Document** and click **Next**.
- 3 Select **Remote PC** and click **Next**.
- 4 Specify the content type of the document you want to publish. You can select the content type from the predefined list or specify a custom content type in the **Custom content types** input field.
- 5 Click **Next**.
- 6 On the **Remote PC Application** page, enter a name, an optional description, a desired window state, and an icon if needed.

- 7** Use the [...] button next to the **Target** input field to browse for the document. All other fields will be automatically populated. To edit any of the auto populated fields, highlight them and enter the required details.
- 8** (Optional) In the **Parameters** input field, specify the parameters to pass to the application when it starts.
- 9** Click the [...] button in the **Remote PC Settings** sections to browse for a remote PC from which the document should be published. In the box that opens, double-click a PC to select it.
- 10** Click **Finish** to publish the document.

CHAPTER 8

Managing Published Resources

Publishing is one of the fundamental features of Parallels RAS. The resources that you can publish include:

- Applications
- Containerized applications
- Desktops
- Documents
- Web applications
- Network folders

We've already discussed how to publish resources from various types of servers. You can find this information using the following links:

- **Publishing from an RD Session Host** (p. 65)
- **Publishing from a Guest VM** (p. 104)
- **Publishing from a Remote PC** (p. 115)

This chapter describes management tasks that you can perform on resources that have been already published.

In This Chapter

General Management Tasks	119
Manage Published Applications	121
Manage Published Desktops	124
Manage Published Documents	125
Manage Folders	128
Using Filtering Rules	129
Checking Effective Access	132
Specifying Client Settings	134
Quick Keypad	135

General Management Tasks

To view published resources, select the **Publishing** category in the Parallels RAS Console. In the middle pane, expand the **Published Resources** node (if it's collapsed) to see the resources.

Right-click a resource to open a context menu. The menu has the following options:

- **Add.** Starts the publishing wizard, which you can use to publish a resource.
- **New Folder.** Allows you to add a folder to the **Published Resources** tree. Folders are described in the **Manage Folders** section (p. 128).
- **Find.** Allows you to search the list for a resource by name.
- **Duplicate.** Duplicates a selected resource. You can publish multiple resources of the same type, but configure them differently according to your needs.
- **Disable** or **Enable.** Disables or enables a selected resource. A disabled resource is unavailable to end users.
- **Delete.** Deletes a published resource from the Parallels RAS farm. This only removes the published resource item from the farm. The actual application is not affected. To avoid accidental deletions, a dialog box is displayed asking for your confirmation.
- **Settings audit.** Allows you to see recent changes to published resources and revert them. The changes that can be reverted include Create, Delete, and Update.
- **Verify Target(s).** Verifies that the target specified for the selected resource is valid. To see the target, select a resource and then click the **Application** tab.
- **Convert Filters to Secure Identifiers.** If filtering for a resource is specified using WinNT or LDAP, you can use this option to convert it to SID (Secure Identifier). For more information, see **Using Filtering Rules** (p. 129).
- **Running Instances.** Opens the **Running Processes** dialog. For more information about the dialog, please see **Managing Sessions > Managing running processes** (p. 62). When the dialog is opened, a filter is applied to the process list to include only the processes for the selected published resource (a resource ID is used as a value). You can further filter the list to include only the process for a particular user (the **Username** column).

The action items at the bottom of the screen allow you to perform the following actions:

- **Add.** Same action as the **Add** menu item described above.
- **New Folder.** Same action as the **New Folder** menu item described above.
- **Delete.** Same as the **Delete** menu item described above.
- **Move Up.** Moves a selected published resource item up the list.
- **Move Down.** Moves a selected published resource item down the list.
- **Disable.** Same as the **Disable** menu item described above.
- **Sort.** Sorts resources alphabetically. For this action item to become enabled, you must select the **Published Resources** node (the topmost one) or a folder containing individual items.
- **Find.** Same as the **Find** menu item described above.
- **Running Instances.** Same as the **Running Instances** menu item described above.
- **Effective Access.** Allows you to view which published resources are available for a specific user. For complete details, see **Checking Effective Access** (p. 132).

After making any changes to published resources, please don't forget to click the **Apply** button to commit them to the Parallels RAS farm.

Manage Published Applications

Publishing an application

Publishing an application has been discussed earlier in this guide in the following sections:

- **Publishing an Application from an RD Session Host** (p. 66)
- **Publishing an Application from a Guest VM** (p. 105)
- **Publishing an Application from a Remote PC** (p. 115)

Configuring a published application

When publishing an application using a wizard, you specify multiple application parameters such as name, executable path, etc. You can modify these options after the application has been published.

To modify a published application:

- 1** In the RAS Console, select the **Publishing** category and then select the application in the **Published Resources** tree.
- 2** Use the tab pages in the right pane to change the application options as described in the following subsections.

Configuring from which servers the application is published

You can specify the RD Session Hosts from which an application is published on the **Publish From** tab page. The following options are available:

- **All Servers in Site.** The application will be published from all servers on which it is installed.
- **Server Groups.** Select this option and then select one or more RD Session Host groups from which the application should be published.
- **Individual Servers.** Select this option and then select one or more individual RD Session Hosts.

Configuring application and server settings

The **Application** tab page displays application- and server-specific settings.

You can modify the basic application settings (name, description, etc.) as needed. Select the **Start automatically when user logs on** option to start an application as soon as a user logs on. This option works on desktop versions of Parallels Client only.

The **Server Settings** section contains server-specific options that you can configure. If an application was published from multiple servers, the **Server(s)** drop-down list can be used to select individual servers and set **Target**, **Start in**, and **Parameters** values for a particular server. As an example, you should do this when different servers have the application installed in different folders, so that the **Target** and **Start in** field values would be valid on each server.

To save the currently displayed server settings as default, click the **Save as Default Settings** button. To apply the saved default settings to a server, click the **Use Default Settings** button. These two buttons give you the flexibility of using custom settings or defaults in different server configuration scenarios. Please note that when you save settings as default, Parallels RAS will check if this site has applications with per-server settings and will display a message asking if you would like those servers to use the new default settings. If you say, "No", the servers will keep their unique settings. The defaults will still be saved.

To verify that the specified **Target** and **Start In** values are correct for all servers, click the **Verify Target(s)** button. The **Target Verifier** dialog opens listing each server and the verification status in the **Progress** column. If the application is installed at a different path on one of the servers, the **Progress** column will indicate an error. In such a case, close the **Target Verifier** dialog and then select the server in the **Server(s)** drop-down list. Specify new values in the **Target**, **Start In**, and (if necessary) **Parameters** fields specific for that server. Click **Apply** to save your changes.

The **Target Verifier** dialog can also be used to verify the targets for all published applications at once. To do so, right-click **Published Resources** (the root node of the **Published Resources** tree) and then click **Verify Target(s)** in the context menu. This time, the **Target Verifier** dialog will contain all published applications and their verification status.

The **Quick Keypad** section allows you to select a Quick Keypad template that should be assigned to this application. The **Quick Keypads** link below the drop-down list takes you to the **Quick Keypad** category in the console where you can configure Quick Keypad templates. If you don't see the **Quick Keypad** section, try to maximize the console window. For more information, please see the **Quick Keypad** section (p. 135).

To replicate the currently selected application settings to all sites, select the **Replicate settings** option in the lower right-hand corner. This will make the default application settings on every site to be the same as the displayed settings. If some of the servers on other sites use server-specific settings (not defaults), you will see a message asking if you would like those servers to use the default settings. If you select "No", the servers will keep their unique settings. The default settings will still be synchronized with the selected application settings.

Configuring shortcut options for a published application

Note: This option is not available on all operating systems.

Click the **Shortcuts** tab to enable the creation of shortcuts on the user's desktop, in the Start folder, and shortcut in the Auto Start folder. When the **Auto Start** shortcut option is selected, the application will be started when the operating system on the client is started.

To use the default settings, select the **Inherit default settings** option. You can view or modify the default settings by clicking the **Edit Defaults** link.

Configuring file extension associations

To modify file extension association for a particular published application, click the **File Extensions** tab.

To add, remove, or modify an entry, select the **Associate File Extensions** option. To add a new extension to the list, click **Add** in the **Tasks** drop-down menu (or click the + icon) and specify the desired extension.

To modify an existing association, highlight the extension and click **Properties** in the **Tasks** drop down menu (or double-click the **Parameters** column) and type the parameter.

Configuring licensing options for published applications

Click the **Licensing** tab to configure the following licensing options:

- **Disable session sharing.** If this option is enabled, it allows you to isolate the published application to one session. Therefore if the same application is launched twice, the two instances of the application will run in two isolated sessions.
- **Allow users to start only one instance of the application.** If this option is enabled, a user can only launch a single instance of the application.
- **Concurrent Licenses.** Use this option to specify the maximum number of concurrent instances the application can run. E.g. if the license of the application allows you to only run 10 instances of the application, set the Concurrent licenses option to 10 so once such limit is reached, other users cannot initiate other instances.
- **If limit is exceeded.** From this drop down menu you can specify what action should the Parallels RAS take in case any of the above licensing configured limits are exceeded.

To use the default settings, select the **Inherit default settings** option. You can view or modify the default settings by clicking the **Edit Defaults** link.

Configuring display settings for a published application

Click the **Display** tab to configure the color depth of the published application, resolution, width and height. To use the default settings, select the **Inherit default settings** option. You can view or modify the default settings by clicking the **Edit Defaults** link.

You can also enable the option to wait for the Universal Printers to be redirected before the application is loaded. When enabling this option, you can also configure the maximum wait time (in seconds) for the Universal Printers to be redirected.

Filtering

Filtering is comprehensively described in the **Using Filtering Rules** (p. 129).

Manage Published Desktops

Publishing a desktop

Publishing a remote desktop has been discussed earlier in this guide in the following sections:

- **Publishing a Desktop from an RD Session Host** (p. 66)
- **Publishing a Virtual Desktop from a Guest VM** (p. 104)
- **Publishing a Desktop from a Remote PC** (p. 115)

Configuring a published desktop

When publishing a desktop using a wizard, you have to specify the desktop settings, such as display size, etc. You can modify these options after the desktop has been published.

To modify a published desktop, select it in the **Published Resources** tree in the **Publishing** category.

Configuring from which sites a published desktop is available

By default, a published desktop is available through all of the available sites. To restrict access to a specific site or a site group, select a desktop in the **Published Resources** tree and then click the **Sites** tab in the right pane. Select the sites from which the desktop should be available.

Note: For the **Sites** tab to be available, you need more than site in a farm.

Configuring from which RD Session Hosts a desktop is published

When configuring an RD Session Host desktop, you can specify from which servers it should be published. To do so, click the **Publish From** tab and select the desired servers.

Configuring desktop resolution and other properties

Depending on the desktop type, click the **Desktop**, **Remote PC Desktop**, or **Virtual Desktop** tab to configure the desktop name, description, icon, and resolution.

Connect to administrative session: Select this option if you want users to connect to the administrative session. Note that a user connecting to a desktop with this option enabled must have administrative privileges; otherwise "Access is denied" error will be shown to the user.

Start automatically when user logs on: Select this option if you want to open a desktop as soon as a user logs in.

Desktop Size: Select a desired desktop size from the drop-down list.

Multi-Monitor: Select whether the multi-monitor should be enabled, disabled, or whether the client settings should be used.

Configuring shortcut options for a published desktop

Click the **Shortcuts** tab to enable the creation of shortcuts on the user desktops, shortcuts in the Start folder, and shortcut in the Auto Start folder. When the Auto Start shortcut is enabled, the application will start when the user's computer is started.

Note: This option is not available on all operating systems.

The filtering tab

Filtering is comprehensively described in the **Filtering Rules by User, Client, MAC, and Gateway** section (p. 129).

Manage Published Documents

Publishing a document

Publishing a document has been discussed earlier in this guide in the following sections:

- **Publishing a Document from an RD Session Host** (p. 70)
- **Publishing a Document from a Remote PC** (p. 117)
- **Publishing a Document from a Guest VM** (p. 108)

Configuring a published document

When publishing a document using a wizard, you have to specify the document settings. These options can be modified after the document has been published.

To modify a published document, select it in the **Published Resources** tree in the **Publishing** category and then use the tabs in the right pane to configure the published document settings.

Configuring from which sites a published document is available

By default, a published document is available through all available sites. To restrict access to a specific site or a site group, click the **Sites** tab in the right pane. Select the sites from which the document should be available.

Note: For the **Sites** tab to be available, you need more than one site in a farm.

Configuring from which servers a document is published

Click the **Publish From** tab and select the servers from which the document should be published. Please note that a server must have the application installed that can open this particular document type.

Configuring server-specific document settings

By default, the settings configured in the **Target** (application path), **Start In**, and **Parameters** fields apply to all servers a document is published from. If a document exists in a different folder on one (or more) of the servers, you can specify the above settings for a specific server or servers individually.

To do so:

- 1 Click the **Application** tab and.
- 2 Select a server in the **Server(s)** list.
- 3 Specify the **Target**, **Start In**, and **Parameters** (optional) properties. The values that you specify will apply to the selected server only. Repeat the steps for other servers if needed.
- 4 Click the **Verify Target(s)** button to verify the document path on all servers from which this application is published. The results are displayed in the **Target Verifier** dialog where you can see whether the target is correct or not for each server.

Configuring shortcut options for a published document

Click the **Shortcuts** tab to enable the creation of shortcuts on the user desktops, shortcuts in the **Start** folder and shortcut in the **Auto Start** folder. When the **Auto Start** shortcut is enabled, the application will start when the user's computer is started.

Note: This option is not available on all operating systems.

Configuring file extension associations

To modify file extension association for a particular published document, click the **File Extensions** tab. To add a new extension to the list, click **Tasks** > **Add** and specify the extension. To modify the extension parameters, highlight the extension and click **Tasks** > **Properties**.

Configuring licensing options for published documents

Click the **Licensing** tab to configure any of the below licensing options:

Select the **Inherit default settings** option to use the defaults. To specify your own settings, clear the option and set the following options:

- **Disable session sharing.** If this option is enabled, it allows you to isolate the published application to one session. Therefore if the same application is launched twice, the multiple instances of the application will run in the same isolated session.
- **Allow users to start only one instance of the application.** If this option is enabled, a user can only launch a single instance of the application.
- **Concurrent Licenses.** Use this option to specify the maximum number of concurrent instances the application can run. E.g. if the license of the application allows you to only run 10 instances of the application, set the Concurrent licenses option to 10 so once such limit is reached, other users cannot initiate other instances.
- **If limit is exceeded.** From this drop down menu you can specify what action should the Parallels RAS take in case any of the above licensing configured limits has been exceeded.

Configuring display settings for a published document

Click the **Display** tab to configure the color depth of the published document, resolution, width and height. If these options are left at their default values, the client-specified options will take over.

You can also enable the option to wait for the Universal Printers to be redirected before the application is loaded. When enabling this option, you can also configure the maximum wait time (in seconds) for the Universal Printers to be redirected.

Filtering

Filtering is comprehensively described in the **Filtering Rules by User, Client, IP, MAC and Gateway** section (p. 129).

Manage Folders

Folders are used to organize published resources and to facilitate filtering options.

There are two types of folders that you can create in the **Published Resources** tree in the Parallels RAS Console:

- **Folders for administrative purposes.** Folders of this type are intended for Parallels RAS administrators (users of the Parallels RAS Console). They are used to logically organize published resources in the Parallels RAS Console but they do not appear in the Parallels Client launchpad on user devices. These folders are used to help administrators manage published resources more efficiently.
- **Regular folders.** These folders are similar to administrative folders described above but they do appear in the launchpad on user devices. You normally use these folders to group published resources by type (e.g. office applications, specific business applications, utilities, etc.).

Creating a folder

To create a new folder:

- 1 In the RAS Console, select the **Publishing** category.
- 2 Right-click anywhere in the **Published Resources** tree and choose **New Folder** (or click the **[+] New Folder** icon at the bottom).
- 3 In the **Folder** dialog, specify a folder name and an optional description.
- 4 To make it a folder for administrative purposes, select the **Use for administrative purposes** option. To publish a regular folder, clear the option. See above for the explanation of the two folder types.
- 5 When creating a regular folder, you can change its icon by clicking the **Change icon** button. Administrative folders use a built-in icon that cannot be changed. Icons appear in the **Publishing** category in the Parallels RAS Console and in the Parallels Client launchpad (regular folders only).
- 6 Click **Finish** to create the folder.

Managing folders

To modify an existing folder:

- 1 Select a desired folder in the **Published Resources** tree.
- 2 The **Information tab** in the right pane displays the folder information (read-only).
- 3 On the **Folder** tab, you can see and modify the folder name and description. You can also select or clear the **Use for administrative purposes** option to change the folder type (see above for an explanation). To change the folder icon, click the **Change icon** button. Note that the button is disabled if the **Use for administrative purposes** option is selected.

- 4 The **Filtering** tab specifies filtering options. Once set, these options will be inherited by all published resources in that folder. For more information about filtering, please see **Using Filtering Rules** (p. 129).

Adding published resources to a folder

To add a published resource to a folder, first add it to the root location and then drag it to the desired folder.

Delegating permissions to custom administrators

If you have custom administrators in your farm, you can delegate permissions to them to manage a folder. This is specifically useful when a power administrator needs to grant permissions to a custom admin (they couldn't otherwise do it because they cannot manage user account directly). To grant folder rights, right-click anywhere in the **Published Resources** pane and then click **Delegate Permissions**. In the dialog that opens, select a user to grant folder permissions to. In the lower right pane of the **Delegate Permission - Publishing** dialog, select permissions (view, modify, add, delete) for a desired folder you want the user to have. Note that the custom administrator will be granted permissions to manage the folder and all its child items, including sub-folders. For more information about custom administrators, see **Managing Administrator Accounts** (p. 40).

Using Filtering Rules

Filtering is a feature that allows you to control who can access a particular published resource. You can define filtering rules based on any of the following:

- User
- Client device name
- Client device operating system
- IP address
- MAC address
- Gateway

By default, no filtering rules exist for a published resource, therefore the resource is available to anyone who is connected to the Parallels RAS farm. Once you specify a filtering rule for a published resource, only those users/computers who satisfy the criteria will be able to use it.

To create a filtering rule, select a published resource in the **Published Resources** tree and click the **Filtering** tab. In the **Select Filtering Type** drop-down list, select criteria and then define a filtering rule as described below.

Filtering by user

To allow individual users or a user group to access the published resource:

- 1 Select **User** in the **Search Filtering Type** drop down list.
- 2 Select the **Allow the following Users** option.
- 3 Click **Tasks > Add** and specify a user or a group in the **Select Users** dialog. Click **OK** to add a user/group to the list on the **Filtering** tab.
- 4 In the **Default Object Type** drop-down list, select whether this rule will apply to users, groups, or both.
- 5 In the **Browse Mode** drop-down list, select the browsing mode you would like to use to connect to Active Directory or Windows.

The options are:

- **WinNT.** WinNT is faster than LDAP but does not support group nesting. Used only for backward compatibility.
- **LDAP.** LDAP supports group nesting but is slow. Used only for backward compatibility.
- **Secure Identifier.** This is the preferred and fastest method. It supports group nesting and renaming.

To convert users or groups specified using WinNT or LDAP, select a user entry and then click **Tasks > Convert**.

Filtering by client device name

To allow a specific client device or a list of client devices to access the published resource, follow these steps:

- 1 Select **Client** device name in the **Search Filtering Type** drop-down list.
- 2 Select the **Allow the following Clients** option. You can use the asterisk character (*) as a wildcard in a name. To include a wildcard in a name, select a client in the list and then click **Tasks > Edit**.
- 3 Click **Tasks** and choose one of the following:
 - **Add from network browse.** Opens a dialog where you can select a client from the list populated from the network.
 - **Add from Active Directory.** Opens a dialog where you can specify a computer or search the Active Directory for it.
 - **Add from known devices.** Opens a dialog where you can select a client from the list populated by previously connected clients.
 - **Add custom entry.** Allows you to type the name of a client. To modify the name, select it and then click **Tasks > Edit**.

- **Edit.** Allows you to modify the name of a selected client. If you want to include a wildcard (*) in a name, you can do it using this option. If no client is selected in the list, the option is disabled.
- **Import from CSV.** Allows you to select a CSV file containing the list of names of client devices. The file should contain a single device name on each row. The names must be unique (no duplicates) or you will see an error message.
- **Export to CSV.** Allows you to export the list of client device names to a CSV file.
- **Delete.** Allows you to delete a selected client. If no client is selected in the list, the option is disabled.

4 Click **OK** to add your selection to the **Client** list.

Filtering by Client device operating system

To allow client devices running a particular operating system to access the published resource, follow these steps:

- 1 Select **Client device operating system** in the drop-down list.
- 2 Select the **Allow access to clients on the following operating system:** option to enable the filtering rule.
- 3 Select one or more operating systems.
- 4 Click **Apply** at the bottom of the RAS Console window to save the changes.

When using the **Checking Effective Access** (p. 132) functionality, the filtering rule information will be displayed as "Client device operating system filtering is enabled".

Filtering by IP address

To allow a specific IP address (or multiple addresses) or a range of IP addresses to access the published resource, follow these steps:

- 1 In the **Search Filtering Type** drop-down list, select **IP Address**.
- 2 Select the **Allow the following IPs** option.
- 3 Click **Tasks > Add** in the IPv4 and/or IPv6 sections to specify the IP address or a range of IP addresses and click **OK**.

Filtering by MAC address

To allow a MAC address or a specific list of MAC addresses to access the published resource, follow these steps:

- 1 In the **Select Filtering Type** drop-down list, select **MAC**.
- 2 Select the **Allow the following MACs** option.
- 3 Click **Tasks > Add** and choose one of the following:

- **Add.** Select clients to add to the list **OK**.
- **Import from CSV.** Select a CSV file containing the list of names of client devices. The file should contain a single MAC address on each row. The addresses must be unique (no duplicates) or you will see an error message.
- **Export to CSV.** Allows you to export the list of MAC addresses to a CSV file.

Filtering by gateway

To allow users to connect to a published resource through a specific gateway, follow these steps:

- 1** Select the **Gateway** filtering type.
- 2** Select the **Allow connections from the following gateway** option.
- 3** Click **Tasks > Add** to specify the gateway and its IP address (if it has multiple IP addresses).

Configuring multiple filtering rules

If multiple filtering rules are configured for a specific published resource, the connecting user has to match ALL of them to be allowed access to the published resource.

Please note that if you applied multiple filters, all of them will be visible in the **Information** tab of a published item.

Checking Effective Access

Filtering rules described in the previous section (p. 129) allow you to configure who can access a particular published resource. If a Parallels RAS user cannot see one or more published resources in Parallels Client, you would normally have to check filtering settings for each resource to make sure that it is published for a given user. The Effective Access functionality simplifies this task by allowing you to view in one place which published resources are available for a user and which are not.

To open the **Effective Access** dialog, select the **Publishing** category in the Parallels RAS Console and then click the **Effective Access** item in the toolbar at the bottom of the window (if you don't see the item, maximize the console window). You can also open the dialog by right-clicking anywhere in the **Published Resources** pane and choosing **Effective Access** in the context menu.

The **Effective Access** dialog allows you to specify a user (and optionally additional criteria) and then view published resources this user is allowed to access. To choose a user, do one of the following:

- Type the user name in the **User** field, or click the **[...]** button next to it and use the **Select User or Group** dialog to select a user.

- Select a device owned by this user from the list of known devices. To do so, click the **Select a Device** button then select a device. Note that if a device has never been used to connect to this Parallels RAS farm, it will NOT be included in the list. For more information, see the **Monitoring Devices** section. (p. 203) After selecting a device, click **OK** to return to the **Effective Access** dialog. All of the fields will be automatically populated using properties of the selected device.

Once you specify a user, enter the additional criteria if needed (all fields except **User** are optional):

- **Client.** Client name assigned to a device. This could be a computer name, FQDN, or a custom name that the user could have set in Parallels Client.
- **IP Address.** Client IP address.
- **MAC.** Client MAC address.
- **Gateway.** RAS Secure Client Gateway name through which the client connects to the farm.

The **Manage groups** button allows you to preview how user access changes if the user is added to one or more groups. When you click the button:

- 1 The **Manage Groups** dialog opens listing groups to which the user already belongs.
- 2 Click the **[+]** button to add the user to one or more additional groups. Note that this will only be a simulation; the user will not be actually added to any additional group.
- 3 To remove a "simulated" group, select it in the lower pane and click the **[-]** button.
- 4 Click **Close** to return to the **Effective Access** dialog.

Finally, to view the effective access information for the specified user, click the **View** button. This opens the **Effective Access - Summary** dialog, which displays the following information:

- The left pane contains the complete list of resources published in the current site. To view only the resources that the specified user can access, select the **Show only allowed published resources** option. If the user is not allowed to access a resource, the resource name is highlighted in red.
- The right pane contains information whether the user is allowed to access a resource selected in the left pane and whether filtering is enabled for the selected resource. Additional information may include filtering details and extended group membership.

By looking through the resource list, you can see which resources the user can or cannot access and take appropriate actions if necessary. If needed, you can export the effective access information to a CSV file. To do so, click the **Export** button and specify a file name. The CSV file has the following columns:

- **Name.** Application name.
- **ID.** Application ID.
- **Accessible.** Whether the application is accessible to the user (Yes or No).
- **Rule.** Filtering rule. If no rules are configured for the application, the column will have no value.

Specifying Client Settings

To specify client settings for published resources, navigate to **Farm** / <site> / **Settings** and select the **Client Settings** tab. On this page, you can specify how published application icons are displayed on the client side and some other options.

Select icon resolution

Published resources are displayed in Parallels Client as icons or as a list. You can specify which resolution should be used when the resources are displayed as icons. Select from the following options:

- **Send standard resolution icons.** Standard resolution icons.
- **Send high resolution icons.** High resolution icons. Please note that this option will use more network bandwidth.

Enable or disable the overlay icon

Note: This option is applicable to desktop clients only (Windows, Mac, Linux). It has no effect on mobile and HTML5 clients.

The other option on this tab is **Enable overlay icon**. An overlay icon is placed on a standard application icon to indicate that it's a remote application served by Parallels RAS. When you launch a remote application from Parallels Client, the application icon is displayed on the local desktop (e.g. on the taskbar in Windows or Dock in macOS). By using an overlay icon, you give the user the ability to tell at a glance which of their running applications are remote Parallels RAS applications and which are local (or any other kind).

Parallels RAS uses the Parallels logo as the overlay icon. When the overlay icon option is enabled, an application icon on a local computer will look like the following sample icons:



As you can see, these are standard icons used by the Windows Calculator and Paint applications with the Parallels logo icon (red parallel lines) in the corner. When a user notices the overlay, they'll know right away that this is a remote application served by Parallels RAS, not a local Windows app.

Show password expiration reminder

Note: At the time of this writing, this feature is implemented for Parallels Client for Windows only.

You can automatically remind your Parallels RAS users to change their domain password when it nears the expiration date. To enable this functionality, select the **Show password expiration reminder** option. When it is enabled, a Parallels Client user whose password is about to expire will see a notification right after they connect to Parallels RAS. Note that the option is disabled by default.

Quick Keypad

The **Quick Keypad** category in the Parallels RAS Console allows you to define custom keys to perform common actions in published applications running on mobile devices. Custom keys appear above the standard keyboard in iOS and Android and can be tapped just like any other key on the virtual keyboard.

This feature is designed for users who run published applications on a phone or a tablet. When a particular software requires repeated selection of certain menu or toolbar items, using custom keys can significantly improve user experience. For example, let's say a user has some data entry task which requires them to press **File > New** and **File > Save** menu items over and over again. If you define two custom keys to perform these actions, the user will see them above the standard keyboard in iOS or Android, so instead of tapping the application's native menu items (which can be cumbersome), they can tap these keys, which is much easier and quicker.

To define custom keys, select the **Quick Keypad** category in the Parallels RAS Console. The **Quick Keypads** view in the right pane allows you to create a Quick Keypad template. A template is created for a specific application (or a group of applications with the identical UI design) and contains shortcuts to perform common actions in an application. Once a template is created, you assign it to a published application or a group of applications, so each application (or a group) has its own Quick Keypad.

To create a Quick Keypad template:

- 1 Click the **Tasks** drop-down menu and choose **New Quick Keypad** (or click the **[+]** icon).
- 2 Specify a Quick Keypad template name (e.g. "Office apps").
- 3 You can organize a Quick Keypad using a multi-level menu system. If you want to do this, click the **New menu** item and specify the menu item name. You can add sub-menu items too. To move a menu item across the tree, simply drag and drop it to the desired tree node.
- 4 When you have your basic menu structure defined, you can add shortcuts (or you can do it any order you like).
- 5 To add a shortcut, click the **New shortcut** item.
- 6 In the **Label** field, enter the name (e.g. "New").
- 7 Click the **Shortcut** field and press a shortcut on the keyboard as you would in the target application. For example, the standard shortcut to create a new document in many applications is Ctrl+N, so to input this shortcut, you would press and hold Ctrl and then press N. The shortcut will appear in the field as "Ctrl+N". You can input up to three shortcuts in this field.

8 To add another shortcut to the template, click the **New shortcut** item again. Repeat until all desired shortcuts are defined.

9 Click **OK** to close the dialog. The new template will appear in the **Quick Keypads** list.

To modify the template, right-click it and choose **Properties**.

You now need to assign the template that you created to an application (or multiple applications). To do so:

1 Right-click a template and choose **Assign to Application** (you can also use the **Tasks** drop-down menu or click the "link" icon).

2 In the **Assign Quick Keypad Template** dialog, select one or more applications to which the template should be assigned.

3 Click **OK** when done.

When a remote user runs an application on their mobile device and opens a virtual keyboard, they will see the extra keys corresponding to shortcuts that you defined for a Quick Keypad template. Tapping a key will perform the corresponding action (e.g. Ctrl-N, which will open a new document).

Exporting and importing a Quick Keypad template

To easily move a Quick Keypad template from one Parallels RAS farm to another, use the Import and Export functionality. To export a template, right-click a template and choose **Export**. Specify the file name and location and click **Save**. To import a template, right-click on an empty space in the **Quick Keypads** list and choose **Import**. You can also perform these actions using the **Tasks** drop-down menu.

RAS Secure Client Gateway

RAS Secure Client Gateway tunnels all Parallels RAS data on a single port. It also provides secure connections and is the user connection point to Parallels RAS. At least one RAS Secure Client Gateway must be installed and configured in every site. Multiple gateways can exist depending on your requirements. Read this chapter to learn how to add, configure, and manage RAS Secure Client Gateways.

In This Chapter

RAS Secure Client Gateway Overview.....	137
Adding a RAS Secure Client Gateway.....	139
Manually Adding a RAS Secure Client Gateway.....	139
Checking the RAS Secure Client Gateway Status.....	140
Configuring RAS Secure Client Gateway	140
Gateway Tunneling Policies	148
Viewing Gateway Summary and Metrics	149

RAS Secure Client Gateway Overview

You need to install at least one RAS Secure Client Gateway for Parallels RAS to work. You can add additional Gateways to a RAS site to support more users, load-balance connections, and provide redundancy.

Installing a RAS Secure Client Gateway on a dedicated server

If you are installing a RAS Secure Client Gateway on a dedicated server, you can also install the Parallels RAS console on the same server. The console will have limited functionality but will allow you to perform some important management operations on the Gateway, including:

- Setting the Gateway operation mode (normal or forwarding, see below for details).
- Assigning a RAS Publishing Agent that will manage the Gateway.
- Setting the Gateway communication port.
- Viewing the Gateway information, such as host OS version, Parallels RAS version, available IP addresses, and other.

The RAS Console in such an installation scenario (when connected to the local computer, not the RAS farm) will only have two categories that you can select in the left pane: **Gateway** and **Information**. To manage the Gateway settings, select **Gateway** and then click **Change Ownership** in the right pane. To view the information select the **Information** category.

When the RAS console is connected to a Parallels RAS farm (i.e. the server where RAS Publishing Agent is running), you can manage RAS Secure Client Gateways by navigating to **Farm / <site> / Gateways**.

How a RAS Secure Client Gateway works

The following describes how a RAS Secure Client Gateway handles user connection requests:

- 1 A RAS Secure Client Gateway receives a user connection request.
- 2 It then forwards the request to the RAS Publishing Agent with which it's registered (the Preferred Publishing Agent setting by default).
- 3 The RAS Publishing Agent performs load balancing checks and the Active Directory security lookup to obtain security permissions.
- 4 If the user requesting a published resource has sufficient rights, the RAS Publishing Agent sends a response to the gateway which includes details about the RD Session Host the user can connect to.
- 5 Depending on the connection mode, the client either connects through the gateway or disconnects from it and then connects directly to the RD Session Host server.

RAS Secure Client Gateway operation modes

RAS Secure Client Gateway can operate in one of the following modes:

- **Normal Mode.** A RAS Secure Client Gateway in normal mode receives user connection requests and checks with the RAS Publishing Agent if the user making the request is allowed access. Gateways operating in this mode can support a larger number of requests and can be used to improve redundancy.
- **Forwarding Mode.** A RAS Secure Client Gateway in forwarding mode forwards user connection requests to a preconfigured gateway. Gateways in forwarding mode are useful if cascading firewalls are in use, to separate WAN connections from LAN connections and make it possible to disconnect WAN segments in the event of issues without disrupting the LAN.

Note: To configure the forwarding mode, a Parallels RAS farm must have more than one RAS Secure Client Gateway.

Planning for high availability

When adding RAS Secure Client Gateways to a site, the N+1 redundancy should be configured to ensure uninterrupted service to your users. This is a general rule that also applies to other Parallels RAS components, such as Publishing Agents or RD Sessions Hosts.

Adding a RAS Secure Client Gateway

To add a RAS Secure Client Gateway to a site, follow these steps:

- 1 In the RAS Console, navigate to **Farm** / <site> / **Gateways**.
- 2 With the **Gateways** tab selected in the right pane, click **Tasks** > **Add** to start the **Add RAS Secure Client Gateway** wizard.
- 3 Enter the server FQDN or IP address (or click the [...] button to select a server from the list).
- 4 Select the gateway mode from the **Mode** drop down menu.
- 5 If you selected the **Forwarding** mode in the step above, select the destination gateway in the **Forward To** drop-down list. You can also select a specific IP address in the **On IP** drop-down list if the Gateway server has more than one.
- 6 Select the **Add an SSL certificate and enable HTML5 Gateway** option to automatically create a self-signed certificate, enable SSL, and enable HTML5 support. For more info, please see **Enable HTML5 Support on the Gateway** (p. 145).
- 7 Select the **Add Firewall Rules** to automatically configure the firewall on the server hosting the gateway. See **Port Reference** (p. 289) for details.
- 8 Click **Next**.
- 9 On the next page, click **Install** to start the RAS Secure Client Gateway installation.
- 10 Click **Done** when the installation is finished.

Manually Adding a RAS Secure Client Gateway

To manually install a RAS Secure Client Gateway and add it to the farm, follow these steps:

- 1 Log into the server where you'll be installing the RAS Secure Client Gateway using an administrator account.
- 2 Copy the Parallels RAS installation file (`RASInstaller.msi`) to the server and double click it to launch the installation wizard.
- 3 Once prompted, click **Next** and accept the End-User license agreement.
- 4 Select the path where the RAS Secure Client Gateway should be installed and click **Next**.
- 5 Select **Custom** from the installation type screen and click **Next**.
- 6 Click on **RAS SecureClientGateway** in the feature tree and select **Entire Feature will be installed on local hard drive**.
- 7 Ensure that all other components in the selection tree are cleared and click **Next**.
- 8 Click **Install** to start the installation.

- 9 When the installation is completed, click **Finish** to close the wizard.
- 10 Open the RAS Console and specify the RAS Publishing Agent that will manage the gateway.

Checking the RAS Secure Client Gateway Status

To check the status of a RAS Secure Client Gateway, right-click it in the list and then click **Check Status** in the context menu. The **RAS Secure Client Gateway Information** dialog opens.

The dialog displays the gateway information, including:

- **Server:** The name of the server on which the gateway is installed.
- **Gateway:** The gateway verification status (e.g. Verified).
- **Version:** The gateway software version number. The version number must match the Parallels RAS version number.
- **OS Type:** Operating system type and version.
- **Status:** Display the current RAS Secure Client Gateway status. If the status indicates a problem (e.g. the gateway did not reply or the gateway software version is wrong), click the **Install** button to push install the gateway software on the server. Wait for the installation to complete and check the status again.

Configuring RAS Secure Client Gateway

To configure a RAS Secure Client Gateway:

- 1 In the RAS console, navigate to **Farm / <site> / Gateways**.
- 2 In the right pane, right-click a gateway and click **Properties**.
- 3 The **RAS Secure Client Gateway Properties** dialog opens.

Read on to learn how to configure the RAS Secure Client Gateway properties.

Enable or Disable a Gateway

A RAS Secure Client Gateway is enabled by default. To enable or disable a gateway, use the **Enable RAS Secure Client Gateway in site** option on the **Properties** tab of the **RAS Secure Client Gateway Properties** dialog.

Gateway Mode, Forwarding Settings, HSTS

A RAS Secure Client Gateway can operate in normal and forwarding modes (p. 137). To set the desired mode and configure related settings click the **Properties** tab in the **RAS Secure Client Gateway Properties** dialog.

Setting the normal mode

To set the normal mode, in the **Gateway mode** drop-down list, select **Normal**.

The **Forward requests to HTTP Server** option allows you to forward requests that do not belong to RAS Secure Client Gateways (gateways handle HTML5 traffic, Wyse, and URL scheme). To specify multiple servers, separate them with a semicolon. An HTTP server can be specified using an IPv6 address. Please note that the HTTP server must support the same IP version as the browser making the request.

The **Preferred Publishing Agent** drop-down list allows you to specify a RAS Publishing Agent that the gateway should connect to. This is helpful when site components are installed in multiple physical locations communicating through WAN. You can decrease network traffic by specifying a more appropriate Publishing Agent. For the gateway to select a Publishing Agent automatically, select the **Automatically** option.

Setting the forwarding mode

To configure the forwarding mode, in the **Gateway mode** drop-down list, select **Forwarding**.

Specify (or select) one or more forwarding gateways in the **Forwarding RAS Secure Client Gateway(s)** field.

Note: The forwarding mode allows you to forward data to a gateway listening on IPv6. It is recommended that forwarding gateways are configured to use the same IP version.

Set IP Address for Incoming Connections

The **IP Address** tab is used to set IP address options for incoming client connections.

RAS Secure Client Gateway recognizes both IPv4 and IPv6. By default, IPv4 is enabled. If a gateway has IPv6 and IPv4 configured, you can specify whether clients should be connecting using IPv4, IPv6, or both. To do so, in the **Use IP version** drop-down list:

- 1 Select the IP version to use and then specify the corresponding properties for the selected version (or both if you selected IPv4 and IPv6).
- 2 Click the **Resolve** button to resolve the IP addresses of the RAS Secure Client Gateway depending on the IP version selected.

The **Bind to the following IPv4/IPv6** fields are used to specify one or more IP addresses on which the RAS Secure Client Gateway should listen for incoming connections. To specify multiple IP addresses, separate them with a semicolon.

The **Optimize connection for the following IPv4/ IPv6** fields can be used when the connection between the gateway and the Parallels Client has a high latency (such as the Internet). This option will optimize traffic for better experience on the Parallels Client side. You can select a specific address, all available addresses, or none to disable this option. What this option will do is delay the internal socket to match the performance of the external socket. If the internal network is fast and the external is slow, RDP detects the fast internal socket and sends a lot of data. The problem is that this data cannot be sent so fast from the Gateway to the Client, thus ending up with a bad user experience. Enabling this option will optimize the data exchange.

Configure RAS Secure Client Gateway Network Options

The **Network** tab is used to configure RAS Secure Client Gateway network options.

By default a RAS Secure Client gateway listens on TCP ports 80 and 443 to tunnel all Parallels RAS traffic. To change the port, specify a new port in the RAS Secure Client Gateway Port input field.

RDP port 3389 is used for clients that require basic load balanced desktop sessions. Connections on this port do not support published resources. To change the RDP port on a gateway select the RDP Port option and specify a new port.

Note: If RDP port is changed, the users need to append the port number to their connection string in the remote desktop client (e.g. [ip address]:[port]).

Broadcast RAS Secure Client Gateway Address. This option can be used to switch on the broadcasting of the gateway address, so Parallels Clients can automatically find their primary gateway. The option is enabled by default.

Enable RDP UDP Data Tunneling. To enable UDP tunneling on Windows devices, select this option (default). To disable UDP tunneling, clear the option.

Client Manager Port. Select this option to enable management of Windows devices from the **Client Manager** category. The option is enabled by default.

Enable RDP DOS Attack Filter. When selected, this option denies chains of uncompleted sessions from the same IP address. For example, if a Parallels Client initiates multiple successive sessions with each session waiting for the user to provide credentials, Parallels RAS will deny further attempts. The option is enabled by default.

Configure SSL Encryption on a Gateway

The traffic between Parallels RAS users and a RAS Secure Client Gateway can be encrypted. The **SSL/TLS** tab allows you to configure data encryption options.

By default, a self-signed certificate is installed during a RAS Secure Client Gateway installation and TLS v1.0, v1.1, or v1.2 is used. Each RAS Secure Client Gateway has its own certificate, which should be added to Trusted Root Authorities on the client side to avoid security warnings.

To issue a new self-signed certificate:

- 1 Select the **Enable SSL on Port** option and specify a port number (default is 443).
- 2 (Optional) Select the SSL version accepted by the RAS Secure Client Gateway from the **Accepted SSL Versions** drop-down list.
- 3 (Optional) Select the **Cipher Strength** as a certificate encryption algorithm strength of your choice. The default strength is **Custom**. The **Cipher** field specifies the cipher, which is also set to a default value (for the **Custom** strength, you can change it if needed in accordance with the openssl standards). A stronger cipher allows for stronger encryption, which increases the effort needed to break it.
- 4 To generate a new self-signed certificate, click the **Generate new certificate** button and then enter the required details. Note that you can choose your own certificate expiration date using the **Expire in** field (the default value is 12 months). When done, click **Save** to save the details and generate a new self-signed certificate. The **Private Key file** and **Certificate file** fields will be populated automatically.
- 5 Click **OK** to save your changes and close the dialog.

Encrypting Parallels Client connection

By default, the only type of connection that is encrypted is a connection between a Gateway and backend servers. To encrypt a connection between Parallels Client and a Gateway, you also need to configure connection properties on the client side. To do so, in Parallels Client, open connection properties and set the connection mode to **Gateway SSL**.

To simplify the Parallels Client configuration, it is recommended to use a certificate issued either by a third party Trusted Certificate Authority or Enterprise Certificate Authority (CA).

If an Enterprise CA certificate is used, Windows clients receive a Root or Intermediate Enterprise CA certificate from Active Directory. Client devices on other platforms require manual configuration.

If a third-party certificate issued by a well-known Trusted Certificate Authority (e.g. Verisign) is used, the client device trusts using Trusted Certificate Authority updates for the platform.

Using Third-Party Trusted Certificate Authority

- 1 In the RAS Console, navigate to **Farm > Gateway > Properties** and click the **SSL/TLS** tab.
- 2 Select TLS 1.2 as the SSL settings option.
- 3 Choose CSR.
- 4 Fill in the data.
- 5 Copy and paste the CSR into a text editor and save the file for your records.

- 6 Paste the CSR into the party Vendors Website page or email it to the vendor.
- 7 Request a return certificate in the following format: Apache, with the private, public and intermediate CA all in one file, with extension `.pem`.
- 8 When you receive the file, place it in a secure folder for backup retrieval.
- 9 Click **Import Public Key** and navigate to the folder (or navigate to a secondary location where you have a copy of the single all-in-one cert) and insert the `.pem` file into the **Certificate key** field.
- 10 Click **Apply** and **Test**.

Note: The private key should already be populated from your initial CRS request.

Using Enterprise Certificate Authority

Use IIS to receive a certificate from Enterprise CA and export the certificate in the PFX format.

Install the PFX certificate on RAS Secure Client Gateway as follows:

- 1 Launch the Parallels RAS Console.
- 2 Select a RAS Secure Client Gateway, open its properties and switch to the SSL tab.
- 3 Click [...] next to **Private Key** or **Public Key** fields.
- 4 Browse for the `.pfx` file and click **OK**.
- 5 Click **Apply**.

Note: The `trusted.pem` file on the Parallels Client side must include the intermediate certificate to be able to verify the cert from the third-party vendor. If the intermediate certificate for the vendor is not in the `trusted.pem` file, you will have to paste it in manually or create a `trusted.pem` template file with the proper Intermediate Certificates and then replace the old `trusted.pem` file with the newly updated one. This file resides in the `Program Files\Parallels` or `Program Files(x86)\ Parallels` on the client side.

Enable SSL on Parallels Secure Client Gateway with cert.pem

- 1 On the Parallels Client Gateway page, enable secure sockets layer (SSL) and click [...] to browse for the pem file.
- 2 Place the single file generated in the **Private Key** and **Public Key** fields.
- 3 Click **Apply** to apply the new settings.
- 4 Your browser may not support displaying this image.

Parallels Clients Configuration

In case the certificate is self-signed, or the certificate issued by Enterprise CA, Parallels Clients should be configured as follows:

- 1 Export the certificate in Base-64 encoded X.509 (.CER) format.
- 2 Open the exported certificate with a text editor, such as notepad or WordPad, and copy the contents to the clipboard.

To add the certificate with the list of trusted authorities on the client side and enable Parallels Client to connect over SSL with a certificate issued from an organization's Certificate Authority:

- 1 On the client side in the directory "C:\Program Files\Parallels\Remote Application Server Client\" there should be a file called `trusted.pem`. This file contains certificates of common trusted authorities.
- 2 Paste the content of the exported certificate (attached to the list of the other certificates).

Securing RDP-UDP Connections

A Parallels Client normally communicates with a RAS Secure Client Gateway over a TCP connection. Recent Windows clients may also utilize a UDP connection to improve WAN performance. To provide the SSL protection for UDP connections, DTLS must be used.

To use DTLS on a RAS Secure Client Gateway:

- 1 On the **SSL/TLS** tab, make sure that the **Enable SSL on Port** option is selected (default).
- 2 On the **Network** tab (p. 142), make sure that the **Enable RDP UDP Data Tunneling** option is selected (default).

The Parallels Clients must be configured to use the **Gateway SSL Mode**. This option can be set in the **Connections Settings > Connection Mode** drop-down list on the client side.

Once the above options are correctly set, both TCP and UDP connections will be tunneled over SSL.

Configure HTML5 Connectivity

The **HTML5** tab page is used to configure HTML5 connectivity.

HTML5 connectivity is a functionality built into RAS Secure Client Gateway. When the connectivity is enabled (default), end users can run published resources using Parallels HTML5 Client that runs inside a web browser.

Parallels HTML5 Client works similarly to a platform-specific Parallels Client application with the exception that end users don't have to install any additional software on their computers or devices — all they need is an HTML5-enabled web browser. This section describes how to configure HTML5 connectivity in the Parallels RAS Console. For the information about how to use it, please refer to **Using Parallels HTML5 Client** (p. 150).

Note: To use HTML5 connectivity, SSL must be enabled on the Gateway. When enabling HTML5, please verify that SSL is enabled on the **SLL/TLS** tab page or on your network load balancer. Please also note that the **HTML5** tab is only available if the gateway mode is set to "normal". For more information, see **Set the Gateway Mode and Forwarding Settings** (p. 140).

To configure HTML5 connectivity, set the options described below.

Enable HTML5 Client: Select or clear this option to enable or disable HTML5 on the gateway.

Gateway

Port: Specify a custom port number if necessary.

URL: Specifies the complete URL that end users will need to enter in their web browsers to connect to Parallels RAS. The URL consists of the RAS Secure Client Gateway server FQDN (or computer name) or IP address followed by "RASHTML5Gateway".

Note: You can simplify or even override this URL on the **Web Requests** tab page of the **RAS Secure Client Gateway Properties** dialog. For example, you can make it possible for your users to enter just the server FQDN or IP address (without the "RASHTML5Gateway" part) to access the HTML5 login page. If you use HTML5 Client Themes (a Parallels RAS feature), you can specify a URL that will open a particular theme's login page. For more information, please see **Specifying a URL for Web Requests** (p. 148) and **Configure HTML5 Client Themes** (p. 151).

Client

Launch sessions using: Allows you to specify whether remote applications and desktops will be launched on user computers in a web browser (HTML5 Client) or in a platform-specific Parallels Client. Parallels Client includes a richer set of features compared to HTML5 Client, thus providing end users with a better user experience. Select one of the following:

- **Launch apps in browser only (HTML5 only)** — Users can run remote applications and desktops using Parallels HTML5 Client only. Use this option if you don't want your users to install a platform-specific Parallels Client.
- **Launch apps with Parallels Client** — Users can run remote applications and desktops in Parallels Client only. When a user connects to Parallels RAS using Parallels HTML5 Client, they will be asked to install the platform-specific Parallels Client before they can launch remote applications and desktops. A message will be displayed to the user with a link for downloading the Parallels Client installer. After the user installs Parallels Client, they can still select a remote application or desktop in Parallels HTML5 Client but it will open in Parallels Client instead.
- **Launch apps with Parallels Client and fallback to HTML5** — Both Parallels Client and a browser (HTML5) can be used to launch remote applications and desktops. Parallels Client will be the primary method; Parallels HTML5 Client will be used as a backup method if a published resource cannot be launched in Parallels Client for any reason. A user will be informed if a resource couldn't be opened in Parallels Client and will be given a choice to open it in the browser instead.

Allow users to select a launch method: If selected, users will be able to choose whether to open remote applications in a browser or in Parallels Client. You can enable this option only if the **Launch session using** option (above) is set to **Launch apps in Parallels Client and fallback to HTML5** (i.e. both methods are allowed).

Allow opening applications in a new tab: If selected, a user will be able to open remote applications in a new tab in his/her web browser.

Use Pre Windows 2000 login format: If this option is selected, it allows you to use legacy (pre-Windows 2000) login format.

Restrictions

Allow embedding of Web Client into other web pages: If selected, the Parallels HTML5 Client web page can be embedded in other web pages. Please note that this may be a potential security risk due to the practice known as clickjacking.

Allow file transfer command: Enables or disables the remote file transfer functionality. For more information, see **Enabling or Disabling Remote File Transfer** (p. 231).

Allow clipboard command: Enables or disables the Remote Clipboard. For more information, see **Using the Remote Clipboard** (p. 165).

Enable Support for Wyse Thin Client OS

To publish applications from the Parallels RAS to thin clients using the Wyse thin client OS, select the **Enable Wyse ThinOS Support** option on the **Wyse** tab.

Note: The Wyse tab is only available if the gateway mode is set to normal. See **Set the Gateway Mode and Forwarding Settings** for more info (p. 140).

By enabling this option, the RAS Secure Client Gateway will act as a Wyse broker. You need to make sure that DHCP option 188 on your DHCP server is set to the IP address of this gateway for thin clients that will be booting via this gateway. Once the DHCP server is configured, click the **Test** button to verify the DHCP server settings.

Filter Access to a RAS Secure Client Gateway

You can allow or deny user access to a gateway based on a MAC address. This can be accomplished using the **Security** tab in the **RAS Secure Client Gateway Properties** dialog.

To configure a list of allowed or denied MAC addresses, click the **Security** tab and select one of the following options:

- **Allow all except.** All devices on the network will be allowed to connect to the gateway except those included in this list. Click **Tasks > Add** to select a device or to specify a MAC address.

- **Allow only.** Only the devices with the MAC addresses included in the list are allowed to connect to the gateway. Click **Tasks > Add** to select a device or to specify a MAC address.

Please note that the Gateway MAC address filtering is based on ARP, so client and server must be on the same network for the filtering to work. It does not work across network boundaries.

Specifying a URL for Web Requests

The **Web Requests** tab allows you to specify a URL which will open when a user enters the IP address of the RAS Secure Client Gateway server in a web browser.

Note: The **Web Requests** tab is only available if the gateway mode is set to normal. See **Set the Gateway Mode and Forwarding Settings** for more info (p. 140).

Generally speaking, you can enter any URL on the **Web Requests** tab. As a result, when end users enter the gateway's IP address or FQDN in a web browser, they will be redirected to the URL specified on this tab. Real-world scenarios of using the URL redirection are as follows:

- End users enter the gateway's FQDN or IP address in a web browser and get redirected to the HTML5 Client login page. For this to happen, the **Web Requests** tab must specify the actual HTML5 URL, which is the default value. You can see the actual URL on the **HTML5** tab or you can simply click the **Default** button which will populate the field with it.
- When using HTML5 Client themes, you can specify a URL of a particular theme, such as `https://server.company.com/RASHTML5Gateway/?theme=MyTheme`. This way, when a user enters the server IP address or FQDN, they will be redirected to the specified theme page. For more info about themes, please see **Configuring HTML5 Client Themes** (p. 151).
- If you disabled the HTML5 connectivity on the gateway, you can specify a URL of a completely different page on another web server to which users will be redirected instead of trying to open the HTML5 Client login page.

Note: You can disable the redirection feature altogether by keeping the **Default URL** field empty. This may be useful when you enable the **Forward requests to HTTP Server** option (on the **Properties** tab) and need to redirect all traffic to your HTTP server.

Gateway Tunneling Policies

Tunneling policies can be used to load balance connections by assigning a group of RD Session Hosts to a specific RAS Secure Client Gateway or RAS Secure Client Gateway IP address.

To configure tunneling policies, navigate to **Farm / <site> / Gateways** and then click the **Tunneling Policies** tab in the right pane.

The **<Default>** policy is a preconfigured rule and is always the last one to catch all non-configured gateway IP addresses and load balance the sessions between all servers in the farm. You can configure the **<Default>** policy by right-clicking it and then clicking **Properties** in the context menu.

Adding a New Tunneling Policy

To add a new policy:

- 1 Click **Tasks > Add**.
- 2 Select a gateway IP address.
- 3 Specify to which RD Session Host(s) the users connecting to that specific gateway should be forwarded to.

Managing a Tunneling Policy

To modify an existing Tunneling Policy, right-click it and then click **Properties** in the context menu.

Viewing Gateway Summary and Metrics

You can view the summary information for all available RAS Secure Client Gateways in one place as follows:

- 1 In the RAS Console, select the **Farm** category and then select the **Site** node in the middle pane.
- 2 The available RAS Secure Client Gateways are displayed in the **Gateways** group in the right pane.
- 3 To go to the main Gateway view/editor, right-click a server and choose **Show in the Editor**.

You can also view the detailed information about a RAS Secure Client Gateway by navigating to **Information / Site Information** in the Parallels RAS Console. The information on this page includes general information, such as OS version, RAS version, Gateway mode, as well as the information about various types of connections, sessions, cached sockets, and threads.

Parallels HTML5 Client

Parallels HTML5 Client is a RAS client application that runs in a web browser. Users can use Parallels HTML5 Client to view, launch, and work with remote applications and desktop in a web browser.

Compared to platform-specific Parallels Clients (e.g. Parallels Client for Windows, Parallels Client for iOS, etc.), Parallels HTML5 Client does not require end users to install additional software on their computers or mobile devices. Feature-wise, platform-specific Parallels Clients give users more control over their Parallels RAS experience than Parallels HTML5 Client. Nonetheless, Parallels HTML5 Client is a fully-featured platform-independent client providing end users with an alternate method of working with remote resources published via Parallels RAS.

Please note that the RAS HTML5 Gateway (the server side) requires Windows Server 2008 R2 or higher (it will not work on Windows Server 2008). The only requirement for the client side is an HTML5-enabled web browser.

In This Chapter

Configure HTML5 Connectivity	150
Configure Themes	151
Open Parallels HTML5 Client	157
Main Menu Options	159
Launching Remote Applications and Desktops.....	160
Using the Toolbar	161
HTML5 Gateway API.....	167

Configure HTML5 Connectivity

HTML5 connectivity is a part of RAS Secure Client Gateway. To be used by end users, the HTML5 connectivity must be enabled and configured in the RAS Console as described in **Enabling HTML5 Connectivity on the Gateway** (p. 145).

Session persistence based on a cookie

RAS HTML5 session persistence is normally set by user's IP address (source addressing). If you can't use source addressing in your environment (e.g. your security policy doesn't allow it), you can use the Session Cookie to maintain persistence between a user and a server. To do so, you'll need to set up a load balancer that can use a session cookie for persistence. The cookie that you should use is ASP.NET_SessionId.

Configure Themes

Themes in Parallels RAS is a functionality that defines the look and feel of a client. At the time of this writing the following clients can use customizable themes:

- **HTML5 client.** An HTML5 client theme is a combination of colors, title, icons, display language, and some other items that users will experience when they open the Parallels HTML5 client in their web browsers.
- **Parallels Client for Windows.** A Windows client theme allows you to customize the appearance of Parallels Client for Windows. By doing so, you can provide a Parallels Client for Windows with custom branding to your customers and/or users.

Note that other Parallels clients always use the default theme. This may change in future releases of Parallels RAS.

To manage themes, navigate to **Farm** / <site> / **Themes** in the Parallels RAS Console. The **Themes** view in the right pane displays the available themes. The list contains at least one default theme. This theme cannot be removed but you can customize it as needed. In addition to the default theme, you can create your own themes.

To create a new or modify an existing theme:

- Click **Tasks > New Theme** (or click the **[+]** icon) to create a new theme.
- Double-click an existing theme (or right-click it and choose **Properties**).

The **Theme Properties** dialog opens. Use the dialog to create a new or modify an existing theme. The instructions in the subsequent sections apply to both scenarios.

Common Theme Settings

The theme settings described below apply to both, HTML5 client and Windows client themes.

General

Select **General** in the left pane and specify the following theme properties:

- **Enable Theme:** Enable or disable the theme (the default theme cannot be disabled).

- **Name:** Specify a theme name.
- **Description:** Specify an optional theme description.
- **Limit access to this theme to members of these Active Directory groups:** If this option is cleared, any Parallels RAS user can access the theme if they know its URL. To limit access to a particular group (or groups), select this option and then click **Tasks > Add** (or click the **[+]** icon) and select the desired group(s).

Message

Select **Messages** in the left pane and specify a post-logon message (up to 500 characters). The post-logon message appears as a message box immediately after the user successfully logs in. The message can be overridden for HTML5 client and Windows client individually (see **Messages** for each client in the subsequent sections).

HTML5 Client Theme Settings

Panes under the **HTML5 client** heading allow you to configure theme settings for Parallels HTML5 client. These settings affect how the HTML5 client looks and behaves in a web browser.

Note: To see how your HTML5 client theme looks, click the **Preview HTML5 Theme** button in the lower left-hand corner of the dialog at any time.

URLs

On the **URLs** pane, specify the following properties:

- **Theme login page:** This field is populated automatically with the theme name when you save the theme. You can replace it with a name of your choice if you wish. The complete name (including the read-only `https://FQDN/RASHTML5Gateway/?theme=` part) forms a URL of the theme login page. Users will enter this URL in their web browsers and see the customized Parallels HTML5 Client login page.

For example, if you enter `MyTheme` in this field, the complete URL becomes `https://FQDN/RASHTML5Gateway/?theme=MyTheme`. When you give the URL to end users, replace the "FQDN" part with the actual FQDN or IP address of the RAS Secure Client Gateway server where you have HTML5 connectivity enabled.

Hint: The `https://FQDN/RASHTML5Gateway` part is the same as the URL found on the HTML5 tab page of the **RAS Secure Client Gateway Properties** dialog (p. 145).

- **Show Parallels Client download URL.** If selected, users will see the **Download Client** link on the HTML5 client page, which can be used to download, install, and configure Parallels Client on users' computers.

- **Override download URL for branded Parallels Client (Windows):** Specifies a location from which your Windows users will download Parallels Client for Windows. By default, Parallels Client is downloaded from the Parallels web site. If you use a branded version of Parallels Client, you can specify its location in this field.
- **Footer URLs.** This option allows you to specify custom URLs that will be placed in the HTML5 client footer. To add a URL, click **Tasks > Add** and specify a URL, a text that will appear on the page footer, and a tooltip text. When entering similar URLs, you can duplicate an existing one by right-clicking it and choosing **Duplicate** (or select an entry and click the "duplicate" icon next to the [-] icon). If you've added multiple URLs, you can reorder them by clicking the up or down arrow icons or selecting **Up** or **Down** items in the **Tasks** menu. The URLs will appear in the footer in the order listed (you can click the **Preview HTML4 Theme** button to see how it looks).

Branding

The **Branding** pane allows you to specify the title for HTML5 client web page and customize the graphics displayed on the page header.

Select the **Branding** pane and specify the following:

- **Title:** Specifies the web page title.
- **Company logo:** Displays the image which is displayed on the HTML5 client page header. To change the image, select browse and then specify the image file. Note that changing the logo image also removes the default Remote Application Server part from the page header.
- **Favicon icon:** Displays the currently set favicon icon. To change the icon, click Browse and select an icon file.

Colors

Specify the desired colors for the HTML5 client header and footer.

Messages

On this pane, you can specify pre-logon and post-logon messages:

- A pre-logon message will appear on the **Log in** page.
- To override the default post-logon message (see **Messages** in the beginning of this topic), select the **Override post-logon message** option and enter a message.

The messages must be 500 characters or less.

Language Bar

Select languages that will appear in the language selector on the Parallels HTML5 Client page. The selector appears as a language flag icon on the page header to the right of the user name.

Parallels Client for Windows Theme Settings

Panes under the **Windows client** heading allow you to configure theme settings for Parallels Client for Windows. By configuring a Windows client theme, you can make the client appear to end users as your organization requires.

Branding

On the **Branding** pane, specify the following:

- **Company name:** Used to create the Start menu hierarchy: Start \ Company Name \ App Name.
- **Application name:** Displayed in the app caption and the Start menu entry name.
- **Connection banner:** Displayed when a connection is being established.
- **Application icon:** The application icon used for the Start menu and by the main app window.

Messages

To override the default post-logon message, select the **Override post-logon message** option and enter a message.

After defining a Windows client theme, you can also create a client package for mass distribution. For more information, see **Create Branded Windows Client for Mass Distribution (p. 155)**.

General Theme Tasks

When you are done customizing a theme, click **OK** to save it and return to the Parallels RAS console.

You can also perform the following actions on the **Themes** tab in the Parallels RAS Console:

- **Duplicate a theme** — right-click a theme and choose **Duplicate** (or select a theme and click **Tasks > Duplicate**).
- **Preview HTML5 theme** — right-click a theme and choose **Preview HTML5 Theme** (or **Tasks > Preview...**).
- **Delete a theme** — right-click a theme and choose **Delete** (or **Tasks > Delete**).

When done creating or modifying themes, click **Apply** in the Parallels RAS Console to commit the changes to Parallels RAS. You can now test the theme by opening its URL in an HTML5-enabled web browser.

Create Branded Windows Client for Mass Distribution

To allow IT administrator to deploy a branded Parallels Client for Windows to end user PCs, Parallels RAS includes the functionality that simplifies the process.

First, you need to create a theme that includes the necessary branding features. See **Parallels Client for Windows Theme Settings** (p. 154). After that, you need to create a Parallels Client for Windows installation package that will use the theme. To do so:

- 1 On the **Themes** tab, click **Tasks > Generate Windows Client Package**.
- 2 In the dialog that opens, specify the following options:
 - Select a theme to use to create the package. The theme must have the **Parallels client** settings configured.
 - Specify the target folder on your local computer (e.g. "c:\temp").
 - Select or clear the "Open the folder in Windows Explorer " option as needed.
- 3 Click **Generate**. This will create the ClientDownloader.exe file. When you run the file, it will download the latest version of Parallels Client for Windows installer (MSI) and will apply the custom theme to it.

You can now distribute this installer to end users. When they run the installer, it will install the Parallels Client for Windows with all the customizations (start menu shortcuts, desktop shortcut, images and icons) as specified in the Windows client theme.

In the future, if you need to upgrade an installed copy of Parallels Client for Windows to a newer version, you don't need to repeat the instructions described above. Simply upgrade the older version and the branding features will remain intact.

Delegating Session Management Permissions

If your organization has multiple user groups, all sharing centralized Parallels RAS resources, you have the ability to delegate session management permissions to an administrator of a particular group. When you do, the administrator can see and manage Parallels RAS sessions only for users who belong to that group.

Here's how this functionality works:

- 1 A separate theme is created for each group. Session management permissions for the theme are delegated to a Custom administrator (a special type for this kind of management).
- 2 When a custom administrator logs in to the Parallels RAS Console, they are presented with a limited user interface displaying sessions that belong to the theme (or multiple themes) that the administrator is allowed to manage.

The rest of this section describes how to configure and use this functionality.

Create a theme and delegate session management permissions

If you don't have a theme for a user group, you need to create it. Follow the instructions provided earlier in this chapter (p. 151). To delegate session management permissions, you specifically need to do the following:

- 1** When specifying **Common Theme Settings**, select the **Limit access to this theme to members of these Active Directory groups** option and add one or more groups.
- 2** After creating or configuring the theme, close the **Theme Properties** dialog, then right-click anywhere in the list and choose **Delegate Permissions**.
- 3** If you already have a custom administrator account that you would like to use, it will appear in the list. If you don't have an account, create one as follows:
 - a** Click **Tasks > Add**.
 - b** In the **Account Properties** dialog, click the [...] button next to **Name** and select an account.
 - c** The **Permissions** field is read-only and set to **Custom administrator** (the type that must be used here).
 - d** Populate the rest of the fields (email, mobile, etc.) as needed.
 - e** Click **OK**.
- 4** Back in the **Delegate Permission** dialog, select the administrator and then select the **Manage sessions** option for the desired theme(s) in the lower pane.
- 5** Click **OK**.

Note that you can also create a Custom administrator and see permissions that they have on the **Administrator / Accounts** page. When creating an administrator, select **Custom administrator** in the **Permissions** drop-down list. To see permissions, double-click an administrator and then click **Change Permissions**. The dialog opens displaying permissions. For a Custom administrator, the dialog lists themes to which the administrator has session management rights

Manage sessions

Once the above is complete, the custom administrator can manage sessions that belong to the specified theme(s). To manage sessions:

- 1** Run the Parallels RAS Console and log in using the credentials of a custom administrator.
- 2** The right pane will contain sessions that belong to the members of the group(s) assigned to the theme.
- 3** To manage a session, select it, then click the **Tasks** drop-down menu and choose a desired option (Disconnect, Log off, Send message, etc.).

Settings audit

Any changes to administrator permissions are recorded in the settings audit. Possible actions are create, update, and delete. You can view the changes by going to **Administration / Settings Audit** or **Farm / Themes / Settings Audit**.

Using themes in Parallels Client for Windows

In order for a user to use a corresponding theme, the connection properties must be properly set. To do so:

- 1 In Parallels Client for Windows, right-click a connection and choose **Connection Properties**.
- 2 On the **Connection** tab page, the server name must be followed by the theme name after a forward slash, as in `Server-name/Theme-name`.

When the administrator views sessions in the RAS Console, a client using a theme can be identified by the theme name in the **Theme** column. At the time of this writing, this only works with Windows clients.

Open Parallels HTML5 Client

To open Parallels HTML5 Client, enter its URL in an HTML5-enabled web browser. The URL that you give to your Parallels RAS users depends on how it is configured in the Parallels RAS Console and whether you have HTML5 Client themes (p. 151) configured.

To obtain the HTML5 Client URL:

- 1 In the Parallels RAS Console, navigate to **Farm / <site> / Gateways**.
- 2 Right-click a RAS Secure Client Gateway click **Properties**.
- 3 In the **Properties** dialog, do one of the following:
 - Select the **HTML5** tab and copy the URL from the URL field. This is the actual HTML5 Client URL that opens the default HTML5 Client theme.
 - To open a particular HTML5 Client theme, use the URL from the **HTML5** tab followed by `"/?theme=theme-name"`. For example:
`https://myserver/RASHTML5Gateway/?theme=MyTheme`
 - Select the **Web Request** tab. If the URL specified there is the same as the one on the **HTML5** tab, your users can enter just the FQDN or IP address of the Gateway to open Parallels HTML5 Client.
 - If you (or another Parallels RAS administrator) have specified a URL on the **Web Request** tab that opens a specific HTML5 Client theme, entering the FQDN or IP address of the Gateway will open that theme.

When you open the URL in a web browser, the login page is displayed. Specify the user name and password and click **Login**. What happens next depends on how the HTML5 connectivity is configured on the server side (see Enabling HTML5 Connectivity on the Gateway (p. 145) for details). The following describes the three possible scenarios.

Launch apps in Parallels Client and fallback to HTML5

With this option configured on the server side, you will see a dialog box in the web browser with the following options:

- **Install Parallels Client.** Opens the Parallels Client download and installation page. Follow the instructions and install Parallels Client.

Note: If you don't have administrative permissions on this computer, a dialog will open saying so. The dialog has two buttons: **Install Full Client** and **Install Basic Client**. If you know credentials of an administrative account on this computer, click **Install Full Client** and enter the credentials when asked. The installation will continue using these credentials and the full version of Parallels Client will be installed. If you don't know the credentials, click **Install Basic Client**. The basic version of Parallels Client will still work but some of the functionality will be missing.

After the installation, you should see Parallels HTML5 Client displaying published resources that you can use. Please also note a link in the lower left corner of the screen displaying the Parallels Client version and build number.

You can now run remote applications and desktop in Parallels Client or in a browser (HTML5). The default method for running applications and desktops is Parallels Client. To run a remote application or desktop in a browser, right-click it (or tap and hold on a mobile device) and then choose Parallels HTML5 Client.

- **Open in Parallels HTML5 Client.** Closes this dialog box and opens the main Parallels HTML5 Client screen. Remote applications or desktops will be launched in the web browser. When you open Parallels HTML5 Client the next time, you will again see the same dialog box with the same options.
- **Always open in Parallels HTML5 Client.** This option works similarly to the option above but your selection is remembered the next time you open Parallels HTML5 Client.

Launch apps in Parallels Client

When this option is configured on the server side, you will see a dialog box prompting you to install Parallels Client. Click the link provided to open the Parallels Client download and installation page and follow the instructions. After you install Parallels Client, the main Parallels HTML5 Client screen opens displaying published resources that you can use. If you now double-click or tap a resource, it will be launched in Parallels Client.

Launch apps in browser only (HTML5 only)

With this option configured, the main Parallels HTML5 Client screen opens with no additional prompts. Remote applications and desktops will be launched in the web browser.

Main Menu Options

To open the Parallels HTML5 Client main menu, click or tap the "person" icon in the upper-right. You can select from the menu options described below.

Settings: Allows you to configure the following settings:

- **Sound.** To play the sound on the local computer, select the **Bring to this computer** option. If sound is not supported by your browser, the menu will be disabled and you'll see a corresponding text message below it.
- **Remote audio recording.** Enables or disable the sound input redirection from the local computer to the remote application. For example, if you would like to use a microphone in Skype or a similar app for teleconferencing, you need to enable audio recording in Parallels HTML5 client. Select **Record from this computer** to enable recording or select **Do not record** to disable it.

Note: Audio input is supported in Chrome, Firefox, Edge and Safari 11. If your browser doesn't support audio input, this setting will be disabled and you will see a text message instead.

- **Redirect Links.** Select a desired redirection option from the following: **Do no redirect**, **Redirect URLs**, **Redirect email**, **Redirect all**. When redirection is enabled, a link will be opened on the local computer.
- **Redirect Printers.** Select a printer redirection option: **RAS Universal Printer** (uses the RAS Universal Printing technology) or **Do not redirect** (printers will not be redirected).
- **Keyboard Mode.** Select **Universal Keyboard** or **PC Keyboard**. If you have problems typing certain characters, try selecting **PC Keyboard** and then selecting a proper layout in the **Keyboard Layout** drop-down list (see below).
- **Keyboard Layout.** Select a keyboard layout (e.g. English (US), English (UK), Japanese). To enable this drop-down list, the Keyboard Mode option must be set to PC Keyboard.

Change Password: Allows the user to remotely change their domain password. This option can be disabled through Client Policies (**Control settings > Password > Prohibit changing password**).

Download Client: Click this option to open a web page with instruction on how to download and install Parallels Client. You can also download Parallels Client by clicking the **Parallels Client not installed** link in the lower left corner of the web page.

Logout: Ends your session with Parallels RAS and logs you out.

Launching Remote Applications and Desktops

Launching applications and desktops

To launch a remote application or desktop in Parallels HTML5 Client, do one of the following:

- Double-click (or tap on a mobile device) an application or a desktop icon. The resource will open inside a web browser or in Parallels Client depending on the server-side HTML5 configuration (RAS Secure Client Gateway Properties > HTML5 > Launch sessions using option).
- Right-click (or tap and hold on a mobile device) an application or a desktop to display a context menu. The menu will appear if the **Allow user to select launch method** or **Allow opening applications in a new tab** (or both) options are selected on the **RAS Secure Client Gateway Properties > HTML5** tab in the RAS console. The menu allows you to choose whether to open the resource in Parallels Client or Parallels HTML5 Client (depending on the setting mentioned above) and it also allows you to choose whether to open an application in the same or new tab in the web browser.
- If a resource cannot be opened in Parallels Client due to an error, a message will be displayed with an option to open it in the web browser instead.

Please note that to open a resource in Parallels Client from the HTML5 page, a URL with a custom scheme is used. When you double-click on a resource on the HTML5 page, the URL is executed and is then passed to Parallels Client which uses the instructions that it contains to open the resource. For more information see **RAS HTML5 Gateway API and Parallels Client URL Scheme**.

Using drag and drop functionality

Parallels HTML5 Client supports drag and drop functionality when running remote applications and desktops.

Note: The **Allow file transfer command** option must be enabled on the Gateway for the drag and drop functionality to work. See **Configure HTML5 Connectivity** (p. 145).

Here's how to use drag and drop when working with a remote application:

- 1 Select a file on your local computer.
- 2 Drag and drop the selected file to an app. The 'Save as' window will pop up.
- 3 Enter a name for the file and save it. The file will be saved on the server hosting the app.

You can also drag and drop files between two remote apps running on different hosts.

Here's how to use drag and drop with a remote desktop:

- 1 Select a file on your local computer.
- 2 Drag and drop the selected file to a remote desktop. The 'save as' window will pop up.
- 3 Enter a name for the file and save it. The file will be saved on the desktop on the server that hosts it.

Other useful features

Other useful functionality on the main Parallels HTML5 Client screen includes the following:

- **Favorites list.** You can add a remote application or a desktop to the Favorites list, so you can easily find them. To do so, point to or tap an application or a desktop and then click or tap the "star" icon. To view the list, click or tap the "star" icon on the footer toolbar (in the lower left). To remove a resource from the list, point to it and click the "X" icon (or point to or tap the resource icon and then click or tap the start icon).
- **Search.** To search for a resource, begin typing its name in the **Search** box (upper right). The list will be filtered as you type to contain only the resources with matching names.
- **View a description.** To view a resource description, position the mouse pointer over it. The description will appear as a tooltip. This could be helpful if one or more resources are published using the same name. By reading the description, you can distinguish between them.
- **Taskbar.** When you launch a remote application or a desktop, its icon is added to the taskbar at the bottom of the screen. When the taskbar is full, items of the same type are grouped to save space. You can click or tap on a group to see the list of all running instances and to switch to or close a particular instance.

Using the Toolbar

Parallels HTML5 Client includes a special toolbar that becomes available when you launch a remote application or desktop. The toolbar appears differently for remote desktops and remote applications. The toolbar has also slightly different functions for desktop computers and mobile devices. The differences are explained in the subsequent topics.

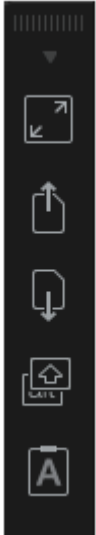
In this section:

- Using the Toolbar on Desktop Computers (p. 162)
- Using the Toolbar on Mobile Devices (p. 164)

Using the Toolbar on Desktop Computers

Remote Desktop Toolbar

When you launch a remote desktop in a web browser on a desktop or laptop computer, the toolbar appears as follows:



The top area of the toolbar is used to drag the toolbar up or down. Click and hold it and then drag the toolbar to the desired position. The arrow icon is used to show or hide the toolbar items.

The main toolbar items are (from top to bottom):

- **Full screen.** Display the remote desktop in full screen on the local computer.
- **Upload a file.** Upload a file from the local computer to the remote server. After clicking this item, you are presented with two dialogs, one after another. In the first dialog, select a file on the local computer you wish to upload. In the second dialog, select a location on the remote server where you want to save the file.
- **Download a file.** Download a file from the remote server to the local computer. After clicking this item, select a file on the remote server you wish to download. Depending on your web browser configuration, the download will start automatically or you will be asked to select a destination folder on your local computer.
- **Shortcuts.** Display the **Shortcuts** menu (see below for the menu description).
- **Clipboard.** Display the remote clipboard. Please see **Using the Remote Clipboard** (p. 165) for more information.

The **Shortcuts** menu allows you to send keystrokes and key sequences to the remote desktop:

- **Escape.** Sends the "Escape" keystroke to the remote desktop.
- **Tab.** Sends the "Tab" keystroke.

- **Backspace.** Sends the "Backspace" keystroke.
- **Print screen.** Sends the "Print Screen" keystroke. The screen will be printed to the clipboard of the remote desktop from where you can paste it into an application (e.g. Paint) running on the same remote computer.
- **Windows Key.** Sends the "Windows logo key" keystroke.
- **Control+Alt+Delete.** Sends the "Ctrl+Alt+Delete" key sequence.

Remote Application Toolbar

When you launch a remote application, the toolbar is embedded into the page footer and it's collapsed by default. To expand the toolbar, click the "arrow-up" icon in the lower right-hand corner.

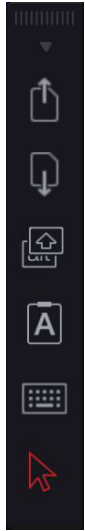
The toolbar items are (from top to bottom):

- **Download.** Download a file from the remote server to the local computer. After clicking this item, select a file on the remote server you wish to download. Depending on your web browser configuration, the download will start automatically or you will be asked to select a destination folder on your local computer.
- **Upload.** Upload a file from the local computer to the remote server. After clicking this item, you are presented with two dialogs, one after another. In the first dialog, select a file on the local computer you wish to upload. In the second dialog, select a location on the remote server where you want to save the file.
- **Clipboard.** Display the remote clipboard. Please see **Using the Remote Clipboard** (p. 165) for more information.

Using the Toolbar on Mobile Devices

Remote Desktop Toolbar

When you launch a remote desktop in a web browser on a mobile device, the toolbar appears as follows:



The small arrow icon at the top is used to show or hide the toolbar items.

The main toolbar items are (from top to bottom):

- **Upload a file.** Upload a file from the local device to the remote server. Note that in iOS, you can upload from the Photos folder only.
- **Download a file.** Download a file from the remote server to the local device (not available in iOS).
- **Shortcuts.** Display the **Shortcuts** menu (see below for the menu description).
- **Clipboard.** Display the remote clipboard. Please see **Using the Remote Clipboard** (p. 165) for more information.
- **Keyboard.** Display the native keyboard. This opens your mobile device native keyboard so you can type in an application on the remote desktop.
- **Arrow.** The arrow icon is used to switch between the two available mouse input modes:
 - Mode 1:** The first mode (the arrow icon is white) follows the movement of your finger on the screen and performs a click on a remote desktop where you tap.
 - Mode 2:** The second mode (the arrow icon is red) displays a virtual mouse pointer on the remote desktop and allows you to move that pointer to a precise position with your finger. When you tap anywhere on the screen, the click on the remote desktop is performed at the precise position of the virtual mouse pointer.

The **Shortcuts** menu allows you to send keystrokes and key sequences to the remote desktop:

- **Escape.** Sends the "Escape" keystroke to the remote desktop.
- **Tab.** Sends the "Tab" keystroke.
- **Backspace.** Sends the "Backspace" keystroke.
- **Print screen.** Sends the "Print Screen" keystroke. The screen will be printed to the clipboard of the remote desktop from where you can paste it into an application (e.g. Paint) running on the same remote computer.
- **Windows Key.** Sends the "Windows logo key" keystroke.
- **Control+Alt+Delete.** Sends the "Ctrl+Alt+Delete" key sequence.

Remote Application Toolbar

When you launch a remote application, the toolbar is embedded into the page footer and it's collapsed by default. To expand the toolbar, click the "arrow-up" icon in the lower right-hand corner.

The toolbar items are (from top to bottom):

- **Download.** Download a file from the remote server to the local device (not available in iOS).
- **Upload.** Upload a file from the local device to the remote server. Note that in iOS, you can upload from the Photos folder only.
- **Clipboard.** Display the remote clipboard. Please see **Using the Remote Clipboard** (p. 165) for more information.
- **Keyboard.** Display the native keyboard. This opens your mobile device native keyboard so you can type in an application on the remote desktop.

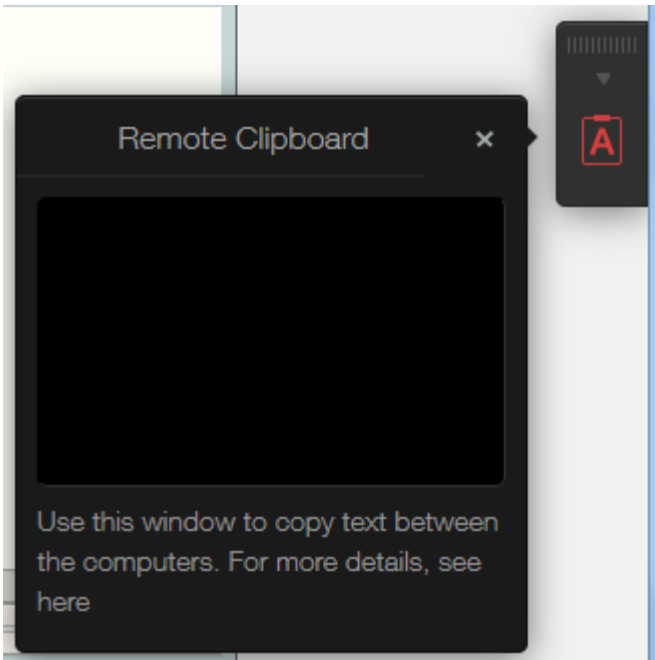
Using the Remote Clipboard

The Remote Clipboard allows you to copy and paste text between a remote application and the local device. The clipboard is accessed from the toolbar.

To use the clipboard:

- 1 Expand the toolbar click the **[A]** icon.

- 2 This opens the **Remote Clipboard** window. On the screenshot below, a remote desktop toolbar is shown. A remote application toolbar looks differently, but it functions exactly the same.



- 3 To copy text from the local computer to a remote application, type (or paste) it in the **Remote Clipboard** window. The text is automatically saved on the remote computer clipboard, so you can use a standard paste command (e.g. Ctrl+V) to paste it into a remote application.
- 4 To copy text from a remote application to the **Remote Clipboard** window, highlight it and use the standard copy command (e.g, Ctrl+C). The text will appear in the **Remote Clipboard** window from where you can copy it to a local application.

Hiding Toolbar Items

You can hide the clipboard and file transfer items on the toolbar if you believe that it's a security risk. The clipboard can be disabled on a RAS Secure Client Gateway or Client Policy level.

To disable the clipboard for a Gateway:

- 1 In the Parallels RAS Console, navigate to **Farms / <site> / Gateways**.
- 2 Right-click a desired RAS Secure Client Gateway and choose **Properties**.
- 3 Select the **HTML5** tab and clear the **Allow clipboard command** option in the **Restrictions** section.

You can also disable the clipboard on the Client Policy level, which will disable it for a given user or user group on any Gateway they connect to:

- 1 In the Parallels RAS Console, select the **Policies** category.

- 2 Right-click a policy and choose **Properties**.
- 3 Select the **Connection Properties** item in the left pane and then select the **Local Resources** tab in the right pane.
- 4 In the **Local devices and resources** section, clear the **Clipboard** option.

Note: Please note that when enabling or disabling the clipboard on a client policy level, this will also affect the clipboard functionality on desktop and mobile versions of Parallels Client. This means that if you disable the clipboard, the desktop and mobile device users will not be able to use their local clipboard when working with a remote application.

You can also disable the file upload and file download items on the toolbar. For instructions, please read the **Enabling or Disabling Remote File Transfer** section (p. 231).

HTML5 Gateway API

The HTML5 Gateway API allows you to use a custom app launcher to launch published applications and desktops via the RAS HTML5 Gateway.

Note: The **HTML5 Client** option must be enabled for the RAS Secure Client Gateway in the Parallels RAS Console and the gateway must be reachable on `https://server-name/RASHTML5Gateway/` where "server-name" is the name of the host.

Link Format

When calling the following link:

```
https://server-name/RASHTML5Gateway/?https://webserver.host/app.js#/launch
```

the RAS HTML5 Gateway will make a request to `https://webserver.host/app.js` and expect a JSONP formatted response as follows:

```
_RASHTML5LoadApp ({
  u: 'username',
  q: 'password',
  a: '#3',
  p: 'c:\\temp\\another.txt',
  extra: {
    redirectPrinter: true,
    redirectLinks: true,
    redirectSound: true
  }
});
```

The RAS HTML5 Gateway will use the received data to launch the app using the options specified in the JSON payload.

Supported JSON parameters

The following table lists currently supported parameters:

Parameter Name	Description
a	Application ID
d	Domain
p	Application arguments
q	Password
u	Username
extra.redirectLinks	Boolean: true = redirect links; false = do not redirect.
extra.redirectPrinter	Boolean: true = redirect printer; false = do not redirect.
extra.redirectSound	Boolean: true = redirect sound; false = do not redirect.

Launching remote applications and desktops

The following steps describe how to use the API to launch remote applications and desktop:

- 1 You build a web application that knows about every user. The application is hosted on "webserver.host" and accepts requests on various "app.js" paths.
- 2 Parallels HTML5 Client is hosted on "server-name": `https://server-name/RASHTML5Gateway`.
- 3 From your portal, Parallels HTML5 Client is started in a new tab of the user's web browser using this link: `https://server-name/RASHTML5Gateway/?https://webserver.host/app.js#/launch`.
- 4 The link loads Parallels HTML5 Client. The first thing that client does is, it connects to `https://webserver.host/app.js` and expects a JSON reply containing user credentials and remote connection settings:

```
RASHTML5LoadApp ({ u: 'username', q: 'password', a: '#3', p: 'c:\\temp\\another.txt', extra: { redirectPrinter: true, redirectLinks: true, redirectSound: true } });
```

where:

- **a: '#3'** is a publishing ID.
- **p:** is a parameter to start the app with.
- **app.js** is a way to pass all necessary parameters to your web application. It should be dynamically generated for every user and every application they have access to through your portal. For example, `notepad_3_username-user123.js`.

Parallels RAS Web Portal

RAS Web Portal is a web page that provides access to published resources via a web browser. It features auto client detection and a client distribution point. This chapter describes how to use RAS Web Portal.

In This Chapter

RAS Web Portal: Prerequisites and Installation 169
 Log In to RAS Web Portal..... 171
 Farm Settings..... 173
 General Settings..... 176

RAS Web Portal: Prerequisites and Installation

Requirements

- Windows Server 2008, 2008 R2, 2012, 2012 R2
- Microsoft .NET Framework 3.5 or 4.5
- ASP.NET role
- IIS 7.0 (Windows Server 2008) or IIS 7.5 (Windows Server 2008 R2)
- IIS 8.0 (Windows Server 2012) or IIS 8.5 (Windows Server 2012 R2)
- Parallels RAS

Supported Client Operating Systems and Browsers

	IE9	IE10	IE11	MS Edge	Chrome	FireFox	Safari
Windows 7	●	●	●		●	●	●
Windows 8		●			●	●	●
Windows 8.1			●		●	●	●
Windows 10			●	●	●	●	●
Linux					●	●	●

macOS					●	●	●
iOS					●	●	●
Android					●	●	

Automatic Client Detection and Installation

	IE9	IE10	IE11	MS Edge	Chrome	FireFox	Safari
Windows 7	●	●	●		●	●	●
Windows 8		●			●	●	●
Windows 8.1			●		●	●	●
Windows 10			●	●	●	●	●
Linux					●	●	●
macOS					●	●	●
iOS					●	●	●
Android					●	●	

Installation

We recommend that you do not install the RAS Web Portal on an Active Directory machine.

To install RAS Web Portal:

- 1 Run the `RASWebPortal.msi` or `RASWebPortal-x64.msi` file on the IIS machine that will be used as your access point to the published applications.
- 2 The **RAS Web Portal Setup** wizard opens.
- 3 Read the info on the **Welcome** page and click **Next**.
- 4 On the next page, read the End-User License Agreement. If agreed, select the **I accept the terms in the License Agreement** option and click **Next**.
- 5 On the **RAS Web Server Port** page, specify the port number. The RAS Secure Client Gateway is installed on port 80 by default and is configured to forward HTTP requests to the local host on port 81. Therefore, clients will still be able to access the RAS Web Portal on port 80. You can choose to install the RAS Web Service on any other port, and also use an existing port used by other web sites.
- 6 Click **Next** and then click **Install**.
- 7 Click **Finish** when the installation is completed.

Please note that IIS7 caches dynamic content as well as static content. To disable the caching for .aspx, .asmx and .ashx pages for the RAS Web Portal directory with an asp.net page that depends on the session state, perform the following on the **RAS Web Server**, **2XWebPortal**, and **2XWebService**.

Disabling Caching for folders consisting on .aspx, .asmx and .ashx

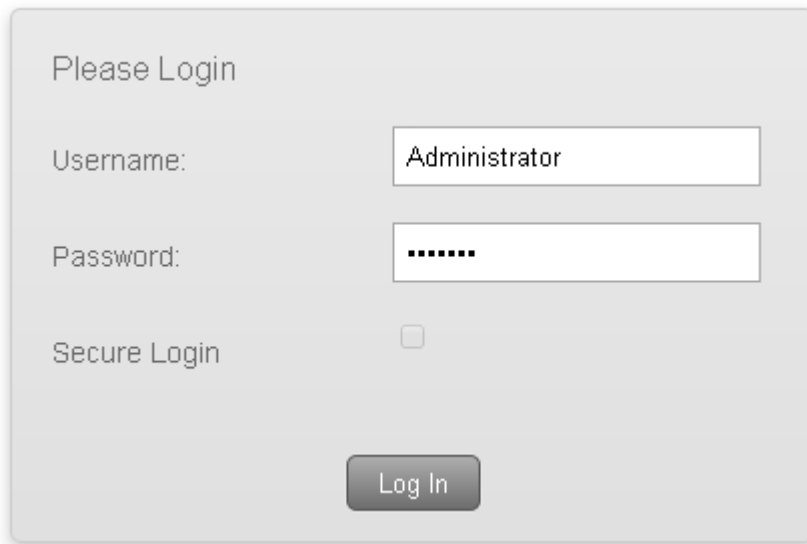
- 1** Run the Server Management console.
- 2** Navigate to **Roles > Web Server (IIS) > Internet Information Services**.
- 3** Repeat steps 4 to 12 for the following sites: **RAS Web Server**, **2XWebPortal**, and **2XWebService**.
- 4** Select the folder that contains the .aspx, .asmx and .ashx pages for which you need to disable caching.
- 5** In the **Feature View**, double-click **Output Caching**.
- 6** If there is a rule there already for the .aspx extension, double click it and continue from step 8. Otherwise right click and select **Add**.
- 7** Enter .aspx for the **File name extension**.
- 8** Check **User-mode caching**.
- 9** Select **Prevent all caching**.
- 10** Check **Kernel-mode caching**.
- 11** Select **Prevent all caching**.
- 12** Click **OK**.
- 13** Close the Server Management Console.

Log In to RAS Web Portal

To log in to RAS Web Portal, open the following URL in a web browser:

`http://localhost/2XWebPortal/Admin.aspx`

This will open the login page:



Please Login

Username: Administrator

Password:

Secure Login

Log In

Enter a user name and password of the user with administrative privileges and click **Log In**.

Note: When you login to the RAS Web Portal, you may see a message about Parallels HTML5 Gateway, which is a newer browser-based client that can also be used to access published resources in a Parallels RAS farm. Compared to RAS Web Portal, Parallels HTML5 Gateway offers simpler setup and configuration and a better user experience. To continue using RAS Web Portal, simply close the message. To learn more about Parallels HTML5 Gateway, use the "Click here for more information" link. In this guide, the HTML5 functionality is described in the **Parallels HTML5 Client (p. 150)** chapter.

Farm Settings

The **Farm Settings** page allows administrators to add multiple farms so that users can launch published applications and desktop from the **User Logon** page.

The screenshot shows the Parallels RAS Web Portal interface. At the top, there is a dark red header with "User Logon Page" on the left and "Welcome Administrator | Logout" on the right. Below the header, the Parallels logo and "RAS Web Portal" text are on the left, and a row of language flags is on the right. A navigation bar contains "Online Manual", "Farm Settings" (which is highlighted), and "General Settings". The main content area is split into two panes. The left pane, titled "RAS Web Portal - Console", has a "List of Farms" section with a globe icon. Underneath, there is a "Farms" list containing one entry: "jb-w2k8r2-srv3...". Below the list is a "Farm Name" input field and an "Add Farm" button. The right pane, titled "Apply Settings", contains instructional text: "RAS Web Portal allows users to launch published applications and desktops from multiple farms. User with administrative rights on the Web Service machine are allowed to add farms from this interface. To add a new farm enter the IP or hostname of the RAS Secure Client Gateway and click 'Add Farm'. Further farm details can be configured once the farm has been added. New settings will get activated once the Apply button has been pressed."

To add a farm, type the IP address or hostname of the RAS Secure Client Gateway and click **Add Farm**. The farm will be added to the left pane under the **List of Farms** tree.

Farm Details

The **Farm Details** page allows the administrator to configure properties. The following are the farm details for the selected farm. These settings are used for the RAS Web Service and the Parallels Client to connect to the RAS Secure Client Gateway.

Farm Details

These settings are used from the RAS Web Service and Parallels Client to connect with the RAS Secure Client Gateway of the selected farm.

RAS Secure Client Gateway Details:

Server Alias:

Primary Hostname / IP:

Secondary Hostname / IP:

Connection type:

Port:

Server Alias. Enter an Alias name that describes better the farm you added. The ‘Alias’ name gives the connection a display name for better readability.

Primary Hostname / IP. This setting is added automatically when adding the farm. This would be the IP / Hostname of the RAS Secure Client Gateway.

Secondary Hostname / IP. A secondary Hostname or IP can be added for another RAS Secure Client Gateway. If the ‘Primary Hostname’ fails, there would be a secondary RAS Secure Client Gateway which will provide published applications and desktops to the user.

Connection Type. This is automatically set to ‘Direct Mode’ when the farm is added. The connection mode is the method the RAS Web Service uses to connect to the RAS Secure Client Gateway. Set the connection mode to ‘SSL mode’ so that a secure connection is tunneled between the RAS Web Service and the RAS Secure Client Gateway.

Port. The default port number is set to port 80. The port must be the same as that set on the RAS Secure Client Gateway.

Advanced Settings

The **Advanced Settings** page is used to overwrite farm settings in the Parallels Client. This will change the settings in the Parallels Client without having the users tampering with the settings.

Set the advanced settings as described below.

Override RAS Secure Client Gateway IP/Host. Select the 'Override RAS Secure Client Gateway IP/Host' to override the 'Primary Hostname/IP' of the farm. Optionally, the **Secondary Hostname/IP** property can be specified.

Override Gateway Port. Select this setting to override the 'Gateway' port other than the default port 80.

Override SSL Gateway Port. Select this setting to override the 'Gateway SSL' port other than the default port 443.

Default Connection Mode. The connection mode for the farm can be overwritten from any of the following:

- **Auto** — The 'Connection Mode' will be set automatically depending on the connection settings configured on the farm.
- **Gateway Mode** — Clients are connected with the RAS Secure Client Gateway and the session connection is tunneled through the first available connection. This mode is ideal for servers which are only reachable via the gateway and do not require a high level of security.
- **Direct Mode** — Clients first connect to the RAS Secure Client Gateway for the best available Server and then connect directly with that particular Server. This is best used when the client and the server are on the same network.
- **Gateway SSL Mode** — Clients connect to the remote RAS Secure Client Gateway in a secure mode. The data being tunneled is encrypted for having a secure connection.
- **Direct SSL Mode** — Clients first connect to the RAS Secure Client Gateway using SSL for the best available server and then connect directly with that particular server. This is best when the client and the server are on the same network and high security safeguards are required.

Applying the Settings

After configuring the settings for a farm, you need to apply your changes by clicking the **Apply Settings** button.

Deleting a Farm

To delete a farm, select the farm in the list and then click **Delete Farm**.

General Settings

On the **General Settings** page, administrators can configure logging, session timeout and other security settings, and can customize the appearance of the Parallels RAS Web Portal. Parallels RAS Web Portal settings can be replicated to other servers for backup purposes. Administrators can also check for the available Parallels RAS Web Portal updates.

Logging

Administrators can enable logging on the Parallels RAS Web Portal so that they can trace changes being performed on the service.

Select **Enable Logging** so that the Parallels RAS Web Portal starts logging any activity that is performed.

You can refresh the log view by clicking the **Refresh** button.

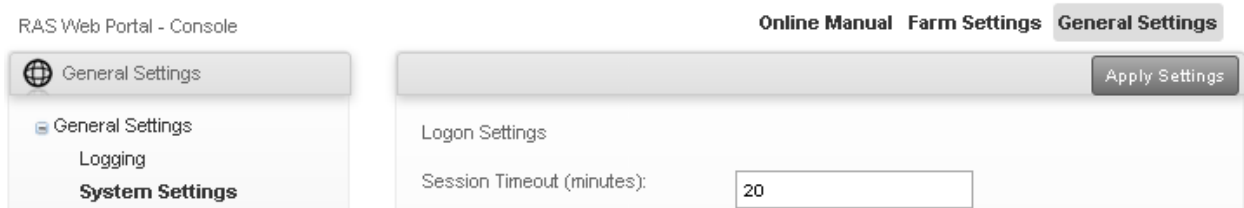
To clear the log entries, click on **Clear Log** and the system will remove the previous logs from the log view.

A copy of current logs can be downloaded from the Parallels RAS Web Portal by clicking the **Download repository** button. By default, a compressed log file is backed up on a weekly basis so that administrators can backtrack any logs if needed. Please note that this function downloads all the available logs (not just the Web Service logs).

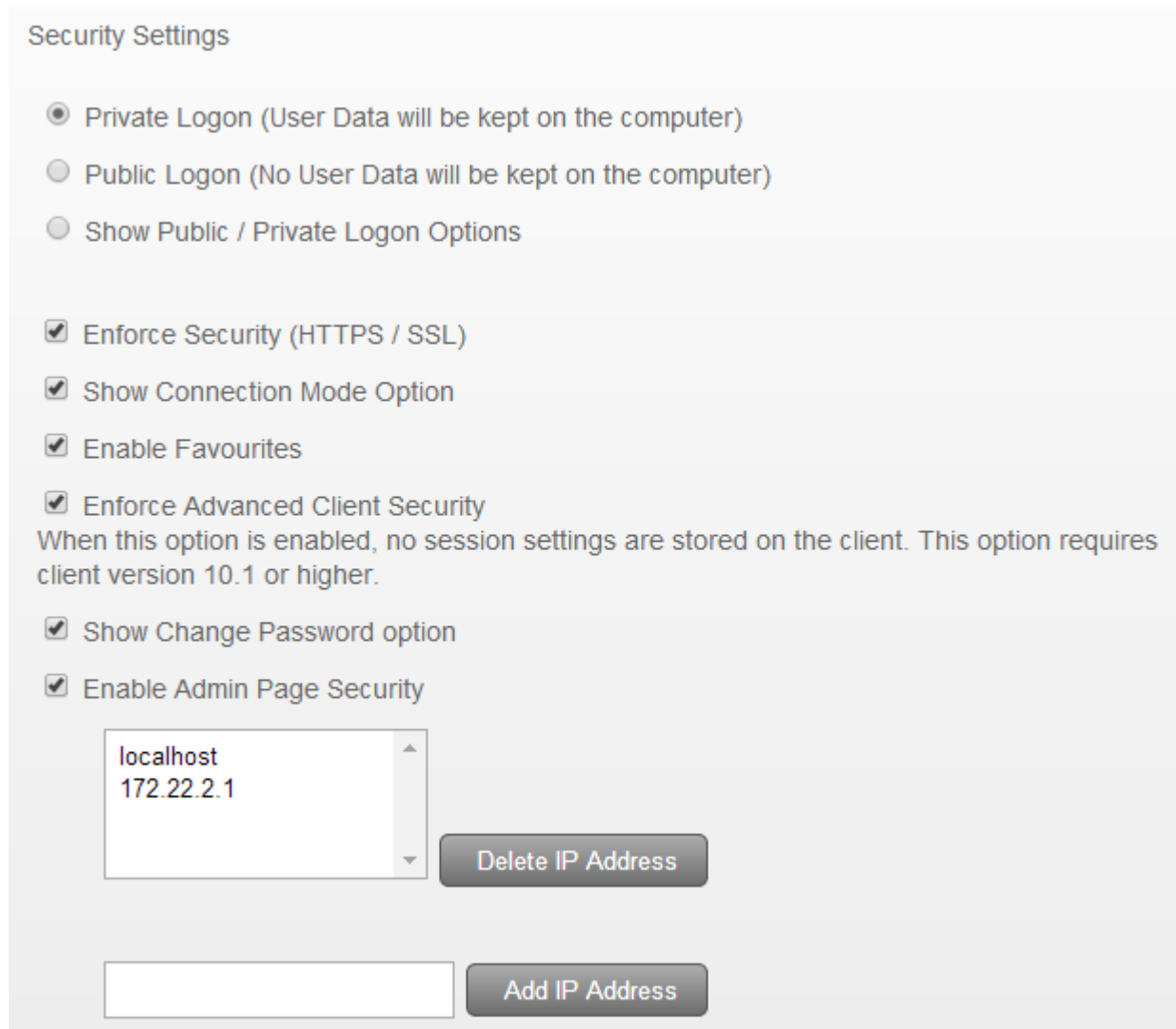
System Settings

System Settings are divided in two sections: **Logon settings** and **Security Settings**.

In the **Logon Settings** section, the **Session Timeout** option specifies the possible idle time that the Parallels RAS Web Portal logon and administrative pages can remain without interaction before the pages prompt the user that the session has timeout and they will be automatically logged off the Parallels RAS Web Portal. The session timeout value is set to 20 minutes.



The **Security Settings** enhance security when logging into Parallels RAS Web Portal and when connecting to a RAS Secure Client Gateway.



Security Settings

- Private Logon (User Data will be kept on the computer)
- Public Logon (No User Data will be kept on the computer)
- Show Public / Private Logon Options

- Enforce Security (HTTPS / SSL)
- Show Connection Mode Option
- Enable Favourites
- Enforce Advanced Client Security
When this option is enabled, no session settings are stored on the client. This option requires client version 10.1 or higher.
- Show Change Password option
- Enable Admin Page Security

localhost
172.22.2.1

Delete IP Address

Add IP Address

The security settings that can be set are described below.

Private Logon. Selecting this option will allow user data to be stored on the local computer. The data remains cached in the browser and will not be cleared when the user logs off the session.

Public Logon. Selecting this option will not allow user data to be stored on the local computer. The data will not remain persistent and will be cleared when the user logs off the session.

Show Public / Private Logon Options. Enable this option to allow the users to choose whether to connect as 'Public' or 'Private'. This option will be displayed on the Parallels RAS Web Portal User Logon Page.

Enforce Security (HTTPS / SSL). Enable this option to force the user to connect to the Parallels RAS Web Portal in SSL (HTTPS) mode. Users will not be allowed to connect to the 'Farm' if SSL is not enabled from the RAS Console.

Enable Favorites. Enable this option to show Favorites inside the User Logon Page.

Enforce Advanced Client Security. Enable this option, to only open the .2xa files when the user is logged on to the Parallels RAS Web Portal. Please note that a user cannot open the .2xa files when the Parallels RAS Web Portal session times out.

Show changed Password option. Enable this option, to show the 'Change Password' option on the User Logon Page.

Enable Admin Page Security. Enable this option so that administrators can only log into the Administrative Page from a machine that matches an IP address from the specified list. To add an IP Address, type it in the field provided and then click **Add IP Address**.

After configuring the System Settings, select **Apply Settings** so that the settings are saved.

Parallels Clients

To launch published applications and desktops, the Parallels Client needs to be installed on the Client. The Parallels RAS Web Portal can be configured to detect the Parallels Client automatically.

To detect Parallels Client Installation, select the **Client Detection** option.

If Parallels client detection fails, users can be notified by means of **Client Detection Failure Options**. The administrator can select from the following:

- **Show error message and allow retest.** Select this option so that an error message is shown and the user is allowed to perform a retest to detect the Parallels Client. This option will not provide the option to install the Parallels Client.
- **Show error message and allow installation or retest.** Select this option so that an error message is shown, providing the option to install the Parallels Client. The user can also choose to perform a retest to detect the Parallels Client.
- **Show error message and allow installation.** Select this option so that an error message is shown and an option is provided to install the Parallels Client. This option will not give the option to retest for Parallels Client detection.
- **Show error message only.** Select this option so that an error message is shown without providing the option to install or retesting for Parallels Client.

The Parallels Client can be downloaded for different OS platforms. The table below illustrates the platforms supported by the Parallels Client and the type of installation packages that can be downloaded for every OS.

OS	Installation Type	Description
Windows	Full Client installation	This will perform the Parallels Client installation installing full resources.
	Basic Client installation	This will perform Parallels Client installation using minimal resources.
Linux	.deb package	This will download the Debian package from the Parallels website.
	.rpm package	This will download the RPM Package Manager from the Parallels website.
	.tar.bz2	This will download Parallels Client for Linux as a compressed file from the Parallels website.
Mac	.pkg	This will download Parallels Client from the Mac store and install it on the macOS desktop.
Android	.apk	This will download Parallels Client from the Google Play and install it on the Android device.
iOS		This will download Parallels Client from App Store and install it on the iOS device.

Customized Appearance

Customized appearance allows administrators to customize how the Parallels RAS Web Portal looks. Administrators can customize the Parallels RAS Web Portal by displaying a different company name, adding a custom banner, changing color themes and more.

To add settings to customize the appearance for Parallels RAS Web Portal, insert a friendly settings name inside the input text fields. Click **Add Settings** or press **Enter** to start customizing appearance settings.

The screenshot shows the 'General Settings' tab in the Parallels RAS Web Portal. At the top, there are navigation tabs: 'Online Manual', 'Farm Settings', and 'General Settings'. Below these are two buttons: 'Delete' and 'Apply Settings'. The main content area is titled 'Customised Appearance' and contains the following text: 'Customised Appearance allows administrators to add the customisation details for multiple logon screens.', 'Users with administrative rights on the Web Service machine are allowed to add customised appearance settings from this interface. To add a new setting, enter the Setting name and click "Add Setting". Further to that, a screen will be displayed prompting you to insert the Company Name, Company Logo and Message.', 'New settings will get activated once the Apply button has been pressed.', and 'These settings are used to configure multiple logon screens.' Below the text are three input fields: 'Company ID:' with a dropdown menu showing 'Personalised', 'Display Company Name:' with a text input field containing 'Personalised', and 'Banner:' with a file upload area. The file upload area shows a preview of a banner image with the Parallels RAS Web Portal logo and text. Below the preview is a text box stating: 'The image file should be in GIF format and ideally scaled to 300 X 40 pixels. Images larger than the mentioned preferred size, will be resized.' At the bottom of the file upload area is a button labeled 'Choose File' and the text 'No file chosen'.

You can customize settings as described below.

Company ID. This setting is set by default in the same name when creating settings to customize the appearance for the Parallels RAS Web Portal.

Display Company Name. Type in a name that you want to display as company name other than the default setting set when creating settings to customize appearance.

Banner. Custom banners can be added to the Parallels RAS Web Portal. The banner should be an image in GIF format, and a size of not more than 300 x 40 pixels.

To upload a banner click the "Browse" button and select the banner. Click "Upload" so that the banner will be uploaded to the RAS Web Service machine.

Message. To display a message underneath the logon section when logging into Parallels RAS Web Portal from the 'User Logon Page', type inside the input text field. This can be used to describe the customized Parallels RAS Web Portal.

URL. The URL states provides the link so that users can connect to the customized Parallels RAS Web Portal. This is automatically generated when creating new customized settings.

Note: The server which has the Parallels RAS Web Portal installation must be publicly accessible so that users can access the **User Logon** page.

Default Domain. Insert the default domain so that users will automatically log with the default domain when logging into the 'User Logon Page'.

Color Modification. From this section, administrators can configure the color scheme for every customized appearance. You can configure the colors by means of the color picker or color themes as illustrated below. More color themes can be created by picking other colors from the color picker. You can reset the Color Themes to default by clicking the **Reset** button.

RAS Publishing Agent

RAS Publishing Agent provides load balancing of published applications and desktops. A RAS Publishing Agent is automatically installed on a server on which you install Parallels RAS and is designated as the master Publishing Agent. Each site must have a master RAS Publishing Agent but can also have secondary Publishing Agents added to it. The purpose of a secondary Publishing Agent is to ensure that users do not experience any interruption of the service due to possible failure of the master RAS Publishing Agent. This chapter describes how to add RAS Publishing Agents to a site and how to configure them.

In This Chapter

Configuring RAS Publishing Agents.....	182
Secondary Publishing Agents	184
Managing Secondary Publishing Agents	186

Configuring RAS Publishing Agents

To view RAS Publishing Agents installed in a site, navigate to **Farm / <site> / Publishing Agents** in the RAS Console. The installed Publishing Agents are listed on the **Publishing Agents** tab page in the right pane.

A site must have at least the master Publishing Agent installed, which is marked "Master" in the **Priority** column. You can also add backup agents to a site (described in the section that follows this one).

To modify the configuration of a RAS Publishing Agent, select a Publishing Agent, then click **Tasks** and choose **Properties**. The **Edit RAS Publishing Agent** dialog opens where you can modify the following properties:

- **Enable Server in site:** Enables or disables the Publishing Agent. The option is enabled for backup Publishing Agents only. It is disabled for the master Publishing Agent.
- **Server:** Specifies the FQDN or IP address of the server that hosts the RAS Publishing Agent.
- **IP:** Specifies the server IP address. Click the **Resolve** button to obtain the IP address automatically using the FQDN specified in the **Server** field. This IP address is used so that multiple Publishing Agents share information in real time.

- **Alternate IPs:** Specifies one or more alternate IP addresses separated by a semicolon. These addresses will be used if RAS Secure Client Gateways fail to connect to the RAS Publishing Agent using its FQDN or the address specified in the **IP** field. This can happen, for example, if Gateways are connecting from a network which is not joined to Active Directory.
- **Description:** A user-defined description.
- **Standby:** If selected, puts a backup Publishing Agent into a standby mode. This means that no agents will connect to this Publishing Agent until another Publishing Agent goes offline. This option is enabled automatically for any new backup Publishing Agent in excess of three that already exist. It is not recommended to have more than three Publishing Agents because it may degrade system performance. This option allows you to have more than three agents, but have them in standby mode until they are needed to take place of the other ones. For more information, see **Backup Publishing Agents** (p. 184).

When you are done making the changes, click **OK** to save them and then click **Apply** in the main RAS console window.

The **Tasks** drop-down menu on the **Publishing Agents** tab page has the following additional items:

- **Add.** Adds a backup RAS Publishing Agent to the site. See the section that follows this one for more information.
- **Check Agent.** Verifies that the RAS Publishing Agent installed on the server is functioning properly. It opens a dialog where you can see the verification results and optionally install (or uninstall) the Publishing Agent software on the server.
- **Promote Backup to Master.** Promotes a backup Publishing Agent to master. Use this option if you would like to make a different server to be the master Publishing Agent. The current master becomes a backup RAS Publishing Agent.
- **Delete.** Deletes a selected backup Publishing Agent from the site. To delete the master Publishing Agent, you first need to promote a backup Publishing Agent to master.
- **Move Up** and **Move Down.** Changes the priority of a backup Publishing Agent (moves it up or down in the priority list).
- **Logging.** Enables extended logging (normal logging is used by default). Also allows you to retrieve logs into a local file and clear all logs.

Viewing RAS Publishing Agent Overview

In addition to the Publishing Agent editor described above, you can also see the summary about the available RAS Publishing Agents. To do so:

- 1 In the RAS Console, navigate to the **Farm** / <site> .
- 2 The available RAS Publishing Agents are displayed in the **Publishing Agents** group on the **Site Info** tab page.
- 3 To go to the Publishing Agents editor, right-click a RAS Publishing Agent and choose **Show in the editor**.

For additional info, see **Viewing Sites in the RAS Console** (p. 36).

Secondary Publishing Agents

A secondary Publishing Agent is added to a site for redundancy. This way if the master Publishing Agent fails, the secondary Publishing Agent is still available to handle the requests. Publishing agents work in active/active manner to ensure high availability. In case of a Publishing Agent failure, the next agent is always ready to handle the load. In general, the N+1 redundancy approach should be used per site. Note that for auto-promotion you shouldn't have more than three Publishing Agents (auto-promotion is described later in this section).

When you have one more secondary Publishing agents installed, the runtime data is replicated on each agent, so if any service fails, the downtime is reduced to a minimum. In addition, any active Publishing Agent is used for authentication purposes with both the AD and any 2nd level authentication provider used.

The master Publishing Agent performs the same tasks as secondary Publishing agents but has additional responsibilities. It manages certain processes that must be managed by a single Publishing Agent. The following table lists processes managed by the master Publishing Agent and secondary Publishing agents:

Process	Master Publishing Agent	Secondary Publishing Agents
Monitor PAs (counters)	Yes	Yes
Monitor RD Session Hosts (counters)	Yes	Yes
Monitor VDI Hosts (counters)	Yes	Yes
Monitor TS Sessions (reconnection)	Yes	Yes
Monitor Deployed TS applications	Yes	Yes
Monitor VDI session (reconnections)	Yes	Yes
Manage system settings	Yes	No
Send licensing information & heart beat	Yes	No
Process and send CEP information	Yes	No
Send information to reporting server	Yes	No
Manage TS scheduler	Yes	No
Reporting engine information	Yes	Future versions

Shadowing	Yes	Future versions
Send email notifications	Yes	No

As a demonstration of how load distribution between multiple Publishing agents works, consider the following example:

- Suppose we have two Publishing agents: PA1 (master) and PA2 (secondary).
- Suppose we also have 10 RD Session Hosts: TS1, TS2 ... TS10

The resulting load will be distributed as follows:

- TS1, TS2 ... TS4 will use PA1 as their preferred Publishing Agent.
- TS5, TS6 ... TS10 will use PA2 as their preferred Publishing Agent.

Planning for secondary publishing agents

RAS Publishing agents running on the same site communicate with each other and share the load. The amount of data being transmitted from one agent to another is quite large, so a reliable high-speed communication channel must be ensured (e.g. a subnetwork can be configured for Publishing Agent communications).

When adding a secondary Publishing Agent to a site, you specify an IP address for it. Make sure that the IP addresses of all agents belong to the same network segment. The port that Publishing Agents use to communicate with each other is TCP 20030.

There's no physical limit to how many Publishing agents you can add to a site. However, the best results are achieved with only 2-3 agents present (the two-agent scenario is recommended). Adding more than 2-3 secondary Publishing agents to a site may have a reverse effect and actually degrade the system performance. Note that this does not apply to secondary Publishing Agents in standby mode, which is explained in **Configuring RAS Publishing Agents** (p. 182).

Adding a secondary RAS Publishing Agent to a site

To add a secondary Publishing Agent:

- 1** In the RAS console, navigate to **Farm / <site> / Publishing Agents**.
- 2** Click the **Tasks** drop-down menu and choose **Add** to launch the **Add RAS Publishing Agent** wizard.
- 3** The **Server** field specifies the FQDN or IP address of the server that hosts the RAS Publishing Agent.
- 4** The **IP** field specifies the server IP address. Click the **Resolve** button to obtain the IP address automatically using the FQDN specified in the **Server** field.

- 5 The **Alternative IPs** field specifies one or more alternative IP addresses, separated by a semicolon. These addresses will be used if RAS Secure Client Gateways fail to connect to the RAS Publishing Agent using its FQDN or the address specified in the **IP** field. This can happen, for example, if Gateways are connecting from a different network, which is not joined to Active Directory.
- 6 Select the **Install a gateway with a publishing agent** option if you also want to install a RAS Secure Client Gateway on the specified server. If you select this option, you may also select the **Add an SSL certificate and enable HTML5 Gateway** option (for more info, please see **Enable HTML5 Support on the Gateway** (p. 145)).
- 7 Select the **Add Firewall Rules** option to automatically configure the firewall on the server. See **Port Reference** (p. 289) for details.
- 8 Click **Next**.
- 9 On the next page, click **Install** to install the RAS Publishing Agent on the server. The **Installing RAS Redundancy Service** dialog opens.
- 10 Select the server on which the RAS Publishing Agent is to be installed and click **Install**.
- 11 Click **Done**.
- 12 Click **OK** to add the server to the farm.

Managing Secondary Publishing Agents

Enabling or disabling a secondary Publishing Agent

To enable or disable a secondary Publishing Agent in a site, select it in the **Publishing agents** list and then select or clear the check box at the beginning of the row.

Changing the secondary Publishing Agent priority

Each secondary Publishing Agent is given a priority. To change the priority, select a secondary Publishing Agent and use the "Up arrow" and "Down arrow" icons (or **Tasks > Move up, Move down**) to move it up or down the list. The higher the agent is in the list, the higher the priority.

Promoting a secondary Publishing Agent to master

If the master Publishing Agent cannot be recovered, you can promote a secondary Publishing Agent to master as follows:

- 1 Open the RAS Console on the Publishing Agent server that you would like to promote (all required files are automatically installed when a server is added to a site as a secondary Publishing Agent).
- 2 Select the **Farm** category and navigate to the **Publishing agents** node.
- 3 Select the Publishing Agent and then click **Tasks > Promote backup to master**.

- 4 Click **OK** once the process is finished.

Configuring auto-promotion

If the master Publishing Agent goes offline, you will need to promote a secondary Publishing Agent to take its place. The auto-promotion feature can do it automatically after a specified time period.

By default, auto-promotion is turned off. To enable it, do the following:

- 1 In the RAS Console, navigate to **Farm / <site> / Publishing agents**.
- 2 Select the **Auto-promotion** tab in the right pane.
- 3 Select the **Enable auto-promotion** option and specify the time period after which the next secondary Publishing Agent should be promoted to master. The time period can be set between 15 minutes and 72 hours (the default value is 30 min).
- 4 Select the **Enable failback** option if you want the original Publishing Agent to become master again should it go back online. For the Licensing Site, this eliminates license activation if failback happens within 72 hours. The license activation countdown is always displayed in the RAS Console, so the administrator can check if the original master Publishing Agent recovers within this time period or not. If the original agent goes back online after the 72-hour period (and if the farm has been already reactivated), it will become a secondary Publishing Agent.

Note: To enable auto-promotion, you need at least three active Publishing agents in a site. If you have less than three, the auto-promotion is ignored.

Please also note that auto-promotion must be disabled if you have a single site with Publishing agents split across different locations with bad WAN links. If there's no link between Publishing Agent located remotely, the third Publishing Agent acts as a witness to prevent split-brain.

When auto-promotion takes place, the RAS administrator will receive notifications via email about the following events:

- A secondary Publishing Agent has been promoted to master.
- Auto-promotion of a secondary Publishing Agent has failed.
- Auto-promotion failback completed.

Deleting a secondary Publishing Agent

To delete a secondary Publishing Agent, select it in the list and then click **Delete** in the **Tasks** drop-down menu.

CHAPTER 13

Load Balancing

This chapter describes load balancing options that you can use in Parallels RAS.

In This Chapter

Resource Based & Round Robin Load Balancing	188
Load Balancing Advanced Settings.....	189
High Availability Load Balancing.....	190

Resource Based & Round Robin Load Balancing

Load Balancer is designed to balance RDS and VDI host connections made from Parallels Clients.

The following types of load balancing methods are available:

- **Resource Based.** Distributes sessions to servers depending on how busy the servers are. Therefore a new incoming session is always redirected to the least busy server.
- **Round Robin.** Redirects sessions in sequential order. For example, the first session is redirected to server 1, the second session is redirected to server 2, and the third session is redirected to server 1 again when there are two RD Session Hosts in the farm.

Both methods are explained in this and the following subsections.

Load Balancing options can be configured from the **Load Balancing** category in the RAS Console.

Enabling Resource Based Load Balancing

Load balancing is enabled by default when more than one server is available in a site. The resource-based load balancing is the default method.

To switch back to resource-based from round-robin, select **Resource Based** in the **Method** drop-down list.

Configuring Resource Counters

Resource-based load balancing uses the following counters to determine if a server is busier than the other/s and vice versa:

- **User sessions.** Redirect users to a server with the least number of sessions

- **Memory.** Redirect users to the server with the best free/used RAM ratio
- **CPU.** Redirect users to the server with the best free/used CPU time ratio

When all of the counters are enabled, the RAS Load Balancer adds the counter ratios together and redirects the session to the server with the most favorable combined ratio.

To remove a counter from the equation, clear the checkbox next to the counter name in the **Counters** section.

Round Robin Load Balancing

Round-robin load balancing redirects sessions in sequential order. For example, with two RD Session Hosts in the farm, the first session is redirected to server 1, the second session is redirected to server 2, and the third session is redirected to server 1 again. To enable round-robin load balancing, select **Round Robin** in the **Method** drop-down list.

Session Options

Reconnect to Disconnected Sessions. Enable this option to redirect incoming user sessions to a previously disconnected session owned by the same user.

Reconnect sessions using client's IP address only. When reconnecting to a disconnected session, the Parallels RAS will match the username requesting reconnection with the username of the disconnected session to match the sessions. With this option enabled, Parallels RAS will determine to which disconnected session to reconnect the session by matching the source IP address.

Limit user to one session per desktop. Enable this option to ensure that the same user does not open multiple sessions. Please note that for this option to work, your RD Session Hosts must also be configured to restrict each user to a single session. In Windows Server 2008, you need to enable the "Restrict each user to a single session" option in Remote Desktop Session Host Configuration. In Windows Server 2012(R2), it's the "Restrict Remote Desktop Services users to a single Remote Desktop Services session" option in Local Group Policy \ Remote Desktop Services \ Remote Desktop Session Host \ Connections.

Disable Microsoft RD Connection Broker. If this option is enabled, the Microsoft RD Connection Broker will not interfere with the RAS brokering done by the RAS Publishing Agent if it is installed. Please note that this option will only work with Windows Server 2012 and above.

Load Balancing Advanced Settings

Excluding a Process from the CPU Counter

To exclude a process so it does not affect the free/used CPU time ratio on a server, follow the procedure below:

- Click the **Configure** button at the bottom of the **Load Balancing** options.
- Select the **Enable CPU Load Balancer** option and click **Exclude List**.
- Click **Add** to select a process in the list of running processes. Alternatively you can specify a process name in the **Please Enter Process Name** input field at the bottom of the dialog.
- Click **OK** to close the **Processes Exclude List** dialog or **Add** to add other processes.

To remove a process from the processes excluded list highlight the process and click **Remove**.

High Availability Load Balancing

High Availability Load Balancing (HALB) is an appliance that provides load balancing for RAS Secure Client Gateways. A Parallels HALB appliance is a preconfigured virtual machine with the operating system installed and all relevant settings configured.

Parallels HALB appliance is available for the following hypervisors:

- Microsoft Hyper-V
- VMware
- Citrix Hypervisor

HALB deployment in Parallels RAS is per site, which means that a site must have at least one Parallels HALB appliance deployed. Since HALB is a single point of contact for the client software, it is recommended to have at least two HALB appliances per site for redundancy.

Multiple HALB deployments can run simultaneously, one acting as the master and others as slaves. The more HALB deployments a site has, the lower the probability that end users will experience downtime. Master and slave HALB deployments share a common or virtual IP address (VIP). Should the master HALB deployment fail, a slave is promoted to master and takes its place.

Note: Please note that when a slave HALB deployment is promoted to master, a user will experience two disconnects: one when the master HALB deployment goes down and one more time when it goes back up since VIP moves from one deployment to the other.

Setting up High Availability Load Balancing consists of the following steps:

- 1** Deploying a Parallels HALB appliance.
- 2** Configuring HALB in the RAS console.

Read on to learn how to download and deploy a Parallels HALB appliance.

Deploying a Parallels HALB Appliance

To download a Parallels HALB appliance, visit <https://www.parallels.com/products/ras/download/links/>

On the **Download Parallels Remote Application Server** web page, scroll down to the **Download Optional Server Components** table and find the **Parallels Remote Application Server HALB Appliances** row. The row contains the following download links:

- HALB Appliance OVA
- HALB Appliance VHD
- HALB Appliance VMDK

The appliance type that you need to download depends on the hypervisor that you are using. Please follow the instructions below for your hypervisor type.

VMware

For VMware, the appliance can be imported with either the OVA or zipped VMDK appliance file. If deployed via the OVA file, the VM is created already configured.

Alternatively, deployment via the VMDK file deploys the VM without preconfigured specifications. The minimum specifications for this VM are outlined below:

- One CPU
- 256 mb RAM
- One network card

Microsoft Hyper-V

For Microsoft Hyper-V, the appliance is imported with the VHD file.

Citrix Hypervisor

For Citrix Hypervisor, the appliance can be imported with either OVA, VMDK, or VHD file.

Deploying a Parallels HALB appliance

After you download a Parallels HALB appliance, you need to import it to a hypervisor running on a separate machine connected to the same local network as Parallels RAS. For the information on how to import a virtual appliance, please consult your hypervisor documentation.

Once the appliance is deployed, you can add it to a Parallels RAS farm. Read on to learn how to do it.

Configuring HALB in the RAS Console

To configure High Availability Load Balancing In the RAS console, navigate to **Farm** / <site> / **HALB**. On the **HALB** tab in the right pane, select the **Enable HALB** option. This will enable the remaining options and will also show the **Devices** tab. Configure the options on each tab as described below.

HALB tab options

Set the **Virtual IP** address options as follows:

- Select the IP version (IPV4, IPV6, or both) that you would like to use.
- Specify the IP address (or addresses if both version are selected) and their corresponding property (subnet mask, prefix). This is the IP address that clients will connect to. This will also be a floating IP address used by this and other HALB appliances.

Select the **LB Gateway Payload** option to load-balance normal gateway connections and then click **Configure**.

- 1** In the **HALB Configuration** dialog, specify the port number that will be used by HALB appliances to forward traffic to gateways (the port configured on the gateway).
- 2** Select the gateways that the HALB appliance will load-balance.
- 3** Click **OK** to close the **HALB Configuration** dialog and return to the **HALB** tab.

If required, select the **LB SSL Payload** option to load-balance SSL connections and then click **Configure**.

- 1** In the the **HALB Configuration** dialog, specify the port number that will be used by HALB appliances to forward traffic gateways (443 by default).
- 2** In the **Mode** drop-down list, select **Passthrough** or **SSL Offloading** to specify where the SSL decryption process is performed. By default, the SSL connections are tunneled directly to the gateways (referred to as passthrough) where the SSL decryption process is performed.

If you select the **SSL Offloading** mode, click **Configure**. The **SSL** dialog opens.

The SSL Offloading mode requires an SSL certificate to be installed on HALB appliances. Specify the following options in the **SSL** dialog to generate a new certificate:

- **Accepted SSL Versions.** Select an SSL version.
- **Cipher Strength.** Select the cipher strength of your choice. To specify a custom cipher, select **Custom** and then specify the cipher in the **Cipher** field.

Click **Generate new certificate** and enter the required details. The **Private Key file** and **Certificate file** options are populated automatically. Please note that you can set your own certificate expiration date (it is 12 months by default).

Alternatively, click **Generate certificate request**, fill in the details and click **Save** to bring up the certificate request window. Click **Copy** to copy the request. This certificate request should be sent to a certificate authority. Once you receive an SSL certificate from the certificate authority, click the **Import public key** button and select the certificate file containing the public key.

- 3 In the **HALB Configuration** dialog, select the gateways that the HALB appliance will load-balance and click **OK** to close the dialog.

Configure the remaining properties on the **HALB** tab:

- 1 Select the **Client Management** option to enable management of Windows devices connected through HALB.
- 2 Select the **Enable RDP UDP Data Tunneling** option to enable UDP tunneling on Windows devices.
- 3 The **Maximum sessions per device** property specifies the maximum number of simultaneous connections allowed. Use the default value or specify your own.

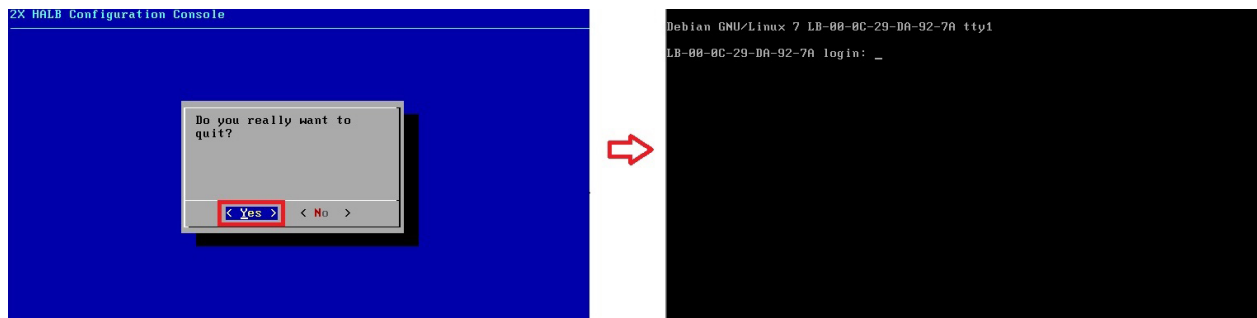
Devices tab options

Click the **Devices** tab to add HALB appliances that will be managed by this farm. To add appliances:

- 1 Click **Tasks > Add** (or click the **+** icon) to bring up the **Add HALB Devices** dialog. Parallels RAS is capable of detecting HALB appliances over the network and display them as a list. Selecting detected HALB appliances from this list is the preferred method for adding new appliances. If an appliance cannot be detected, you can add it manually by specifying the appliance IP address in the **IP Address** field.
- 2 Click **OK** to close the **Add HALB Devices** dialog. The appliance is initialized and added to the list on the **Devices** tab.
- 3 Finally, click **Apply** for the new HALB configuration to be applied to all added HALB appliances.

For additional information, please see the following KB article: <http://kb.parallels.com/123607>

Changing HALB Appliance Password



When the HALB configuration console shown above closes, login credentials are requested to log back in. Follow the steps below to set login credentials for the HALB device:

- 1 Boot the Appliance.
- 2 Press the <ALT> – <F1> key combination. A login prompt should be displayed.

```
Debian GNU/Linux 7 LB-00-0C-29-DA-92-7A tty1
LB-00-0C-29-DA-92-7A login: root
Password: _
```

- 3 Type in the following credentials:

- **login** – root
- **password** – Pa\$w0rd (note that "0" is zero, not the letter "O").

```
Debian GNU/Linux 7 LB-00-0C-29-DA-92-7A tty1
LB-00-0C-29-DA-92-7A login: root
Password:
Linux LB-00-0C-29-DA-92-7A 3.2.0-4-686-pae #1 SMP Debian 3.2.51-1 i686
Welcome to Lb-00-0c-29-da-92-7a, 2X HALB / Debian 7.2 Wheezy

System information (as of Fri Apr 17 09:47:25 2015)

System load: 0.03          Memory usage: 13%
Processes: 63             Swap usage: 0%
Usage of /: 71.5% of 494MB IP address for eth0: 10.124.4.119

root@LB-00-0C-29-DA-92-7A ~# passwd_
```

- 4 Once logged in, execute the password changing command by typing a password.

```
root@LB-00-0C-29-DA-92-7A ~# passwd
Enter new UNIX password: _
```

- 5 Type in and confirm the new password.

Upon completion, you may log in to the HALB device with the new password set after the HALB configuration console is closed.

CHAPTER 14

Universal Printing

Printer redirection enables users to redirect a print job from a remote application or desktop to their local printer, which can be connected to the user's computer or be a local network printer attached via an IP address. RAS Universal Printing simplifies the printing process and solves most printer driver issues by eliminating the need for a remote server to have a printer driver for a specific local printer on the client side. Therefore, a user can print regardless of which printer they have installed locally, and the RAS administrator doesn't have to install a printer driver for each printer connected to the local network.

In This Chapter

Managing Universal Printing Settings	195
Universal Printing Drivers	196
Font Management	197

Managing Universal Printing Settings

To configure RAS Universal Printing, select the **Universal Printing** category in the RAS Console.

By default, the Universal Printing driver is automatically installed together with an RD Session Host Agent, VDI Guest VM Agent, or a Remote PC Agent. Therefore, upon adding a server to the farm, the Universal Printing is already enabled. The Universal Printing driver is available as a 32 bit and 64 bit version.

Enabling and Disabling Universal Printing Support

To enable or disable the Universal Printing support for a server, right-click the server in the **Servers in Site** list and click **Enable** or **Disable** in the context menu.

Configuring a Printer Renaming Pattern

By default, Parallels RAS renames printers using the following pattern: `%PRINTERNAME%` for `%USERNAME%` by `Parallels`. For example, let's say a user named Alice has a local printer named `Printer1`. When Alice launches a remote application or desktop, her printer is named `Printer1 for Alice by Parallels`.

To change the default printer renaming pattern, select the Universal printing category. On the Universal printing tab, specify a pattern in the **Printer rename pattern** field. To see the predefined variables that you can use, click the [...] button next to the input field. The variables are:

- `%CLIENTNAME%` — the name of the client computer.
- `%PRINTERNAME%` — the name of a printer on the client side.
- `%SESSIONID%` — RAS session ID.
- `%USERNAME%` — the name of the user connected to RAS.
- `<2X Universal Printer>` — This is a legacy mode where only one printer object will be created in the RDP session.

You can also use certain other characters in a printer renaming pattern. For example, you can define the following commonly used pattern: `Client/%CLIENTNAME%#/%PRINTERNAME%`. Using this pattern (and the user named Alice from the example above), a local printer will be named `Client/Alice's Computer#/Printer1`

You can specify a different printer renaming pattern for each server in the **Servers in Site** list.

Note: Redirected printers are only accessible by the administrator and the user who redirected the printer.

Printer retention

When client-defined printers are redirected to a remote session, it takes time and impacts overall session establishing time. To improve user experience, you can reuse previously created user's printers. To do so, on the **Universal printing** tab, set the **Printer retention** option to **On**.

Universal Printing Drivers

A system administrator can control the list of client-side printer drivers which should be allowed or denied the Universal Printing redirection privileges.

Using this functionality you can:

- Avoid server resource overloading by non-useful printer redirection. Since the majority of users choose to redirect all local printers (this is default setting), a large number of redirected devices is created on the server which are not really used. It's mostly related to various paperless printers like PDFCreator, Microsoft XPS Writer, or various FAX devices.
- Avoid server instability with certain printers. There are some printers that might create server instability (spooler service component) and as the result deny printing services as a whole for all connected users. It is very important that the administrator has the ability to include such drivers to the "deny" list to continue running printing services.

To specify printer drivers:

- 1 In the Parallels RAS Console, navigate to **Universal Printing / Printer Drivers**.
- 2 In the **Mode** drop-down list, select which printers should be allowed redirection from the following options:
 - **Allow redirection of printers using any driver** — (default) This option places no limitation on the the type of driver a printer is using to use redirection privileges.
 - **Allow redirection of printers using one of the following drivers** — Only the printers using the drivers listed in the box below the **Mode** field are allowed redirection. To add a printer driver to the list, click the **Tasks > Add** (or click the + icon) and type the printer driver name in the edit field provided.
 - **Don't allow redirection of printers that use one of the following drivers** — This is probably the most useful option in the context of this feature. The printers that use the drivers specified in the list will be denied redirection privileges. All other printers will be allowed to use redirection. To add a printer driver to the list, click the **Tasks > Add** (or click the + icon) and type the printer driver name in the edit field provided.
- 3 To delete a printer driver from the list, click **Tasks > Delete** or click the minus-sign icon.
- 4 When done making changes, click the **Apply** button to save the changes.

Please make a note of the following:

- When adding a printer driver to the list, type the printer *driver* name, NOT the printer name.
- The driver names comparison is case insensitive and requires full match (no partial names, no wildcards).
- The settings that you specify on this tab affect the entire site (not an individual server).

Font Management

Fonts need to be embedded so that when printing a document using Universal Printing the document is copied to the local spooler of the client machine to be printed. If the fonts are not present on the client machine the print out would not be correct.

To control the embedding of fonts within a print job use the **Fonts Management** tab page and check/uncheck the option **Embed Fonts**.

Excluding Fonts from Embedding

To exclude a specific font type from being embedded, click **Tasks > Add** in the **Exclude the following Fonts from embedding** section and select a font from the list.

Automatically Install Fonts on Servers and Clients

To automatically install a specific font type on servers and clients, click **Tasks > Add** in the **Auto install fonts** section and select the fonts from the list.

Note: By default, fonts added to the auto install list will be excluded from the embedding list because the fonts would be installed on the Windows clients, therefore there is no need for them to be embedded. Clear the option **Automatically exclude font from embedding** in the select font dialog so the font is not excluded from the embedding list.

Resetting List of Excluded Fonts to Default

To reset the list of excluded fonts to default, click **Tasks > Reset to Default**.

You can also specify a universal printing compression policy. For more info see **Client Policies / Experience** (p. 223).

Universal Scanning

Scanner redirection enables users who are connected to a remote desktop or accessing a published application to make a scan using the scanner that is connected to the client machine. This chapter describes how to configure and use RAS Universal Scanning services.

In This Chapter

Managing Universal Scanning	199
Managing Scanning Applications	200

Managing Universal Scanning

Universal Scanning uses TWAIN and WIA redirection to let any application using either technology hardware connected to the client device for scanning. With Universal Scanning there is no need to install a specific scanner driver on the server. Only one scanner is shown on the server regardless of the number of users and sessions currently in use on the RD Session Host.

Note: The server feature **Desktop Experience** is required in order to enable both WIA and TWAIN scanning on RD Session Hosts.

To configure Universal Scanning, select the **Universal Scanning** category in the RAS Console.

By default, the Universal Scanning driver is automatically installed with the RD Session Host, Guest VM, and Remote PC agents. Therefore, upon adding a server to the farm the Universal Scanning is installed.

Note: The Universal Scanning driver is available as a 32 bit and 64 bit version. Currently, only 32 bit applications are supported.

Configuring a Scanning Rename Pattern

By default, Parallels RAS renames scanners using the following pattern: %SCANNERNAME% for %USERNAME% by RAS. For example, if a user named Lois, who has SCANNER1 installed locally, connects to a remote desktop or published application, her scanner is renamed to "SCANNER1 for Lois by RAS".

To change the pattern used to rename scanners, specify a new pattern in the **Scanner rename pattern** input field. The variables that you can use for renaming are:

- %SCANNERNAME% — client side scanner name.
- %USERNAME% — username of the user connected to the server.
- %SESSIONID% — ID of the active session.

You can configure a different renaming pattern specifically for each server in the list.

Note: Redirected scanners are only accessible by administrator and the user who redirected the scanner.

Enabling and Disabling Universal Scanning Support

To enable or disable the WIA or Twain Universal Scanning support for a particular server, click the **WIA** tab or the **TWAIN** tab, then right-click a server and click **Enable** or **Disable** in the context menu.

Managing Scanning Applications

Adding a Scanning Application

TWAIN applications that will use the Universal Scanning feature have to be added in the TWAIN tab by selecting the **TWAIN Applications** button so they can use the Twain driver, hence making it easier for the administrator to set them up.

To add an application to the list of scanning applications:

- 1 With the **Universal Scanning** category selected in the RAS Console, click the **TWAIN** tab.
- 2 Click the **Twain Applications** button (below the **Servers in Site** list) and then click **Add**.
- 3 In the **TWAIN Applications** dialog, click **Tasks > Add** and browse for the application executable. Select the executable and click **Open**.

Note: Some applications might use different or multiple executables. Make sure that all required executables are added to the list of scanning applications.

Deleting a Scanning Application

To delete a scanning application from the list, highlight it and click **Tasks > Delete**.

Note: If you delete an application from the list, the installation of the application will not be affected.

You can also specify a universal scanning compression policy. For more info see **Client Policies > Experience** (p. 223).

CHAPTER 16

User Device Management

This chapter describes tasks that a Parallels RAS administrator can perform to manage user devices, such as desktop computers, phones, or tablets.

In This Chapter

Inviting Users to Connect to Parallels RAS	202
Enabling Help Desk Support	202
Monitoring Devices	203
Windows Device Groups	204
Managing Windows Devices	205
Scheduling Windows Devices & Groups Power Cycles	212
Client Policies	213
Enabling or Disabling Remote File Transfer	231

Inviting Users to Connect to Parallels RAS

Parallels RAS supports multiple platforms ranging from desktop PCs and Mac computers to mobile devices and ChromeApps. The Invitation Email feature is designed to reduce the complexities involved in the installation and client rollout process. This feature allows the administrator to send client installation and automatic configuration instructions to end users right from the Parallels RAS Console.

Before proceeding, please confirm that you've configured the mailbox as described in **Configuring SMTP Server Connection for Notifications via Email** (p. 281). To send an invitation email to users, use the **Start** category in the RAS Console. For more information see **Invite Users** (p. 28).

Enabling Help Desk Support

Parallels Client provides users with the ability to send a support request, together with a problem report, to your organization's help desk.

Note: At the time of this writing, this functionality is only available in Parallels Client for iOS and Parallels Client for Android. Support for other clients will be added in future releases.

To enable Help Desk support, do the following:

- 1 In the RAS Console, select the **Features** category.
- 2 Select the **Enable Helpdesk functionality in Parallels Client** option and specify your help desk email address in the field provided. This email address will be updated in Parallels Client every time a user connects to Parallels RAS from it.

Help desk can be accessed in Parallels Client from the Help section (or menu). When the user selects the **Request support from helpdesk** item, a local email client will open. The following information will be prefilled in the email:

- Help desk email address (the one you set in the RAS Console).
- Application name.
- A screenshot.
- User name.
- Application version.
- Operating system version.

The user can provide their own description of the request.

Monitoring Devices

Device monitoring allows you to view devices which are connected to the farm or have established a connection at least once in the past. To monitor devices, select the **Client Manager** category in the Parallels RAS Console and click the **Devices** tab. The information for a device includes:

- Device name
- IP address
- State (see below for the list of states)
- Last user (who used a device)
- MAC address
- OS version
- Parallels Client version
- Group (if a device is a member of a device group)
- Gateway (the RAS Secure Client Gateway a device is connected to)

To see the additional device information, right-click a device and choose **Get Device Information** in the context menu. In the dialog that opens, review the following properties:

- **Name:** Device name.
- **IPs:** Device IP address (or multiple addresses if applicable).

- **MAC Address:** MAC address.
- **State:** State (see below for the list of states).
- **Last User:** The user who logged in from this device the last time.
- **Last Logon Time:** The time of last logon.
- **OS Version:** The operating system version running on the device. Windows portable and U3 clients are marked as "Portable".
- **Client Version:** Parallels Client version installed on the device.
- **Gateway Name:** RAS Secure Client Gateway through which the device connect to Parallels RAS.
- **Last Activity:** The date and time when any activity was detected from this device.

Device States

Devices that connect to Parallels RAS can have any of the following states:

- **Off:** Device is switched off.
- **Connected:** Device is connected.
- **Logged On:** Devices is logged on to the system.
- **Standalone:** Device has previously connected to the Parallels RAS but is not using Parallels Client, therefore it cannot be managed.
- **Not Support:** Device is not supported by the Parallels RAS.
- **Foreign Managed:** Connecting to the farm but managed by a different farm.
- **Not Manageable:** Client not manageable due to incompatible client version or uninstalled component.
- **Locked.** Device has an active session in locked status.
- **Pair Pending.** Connection should be refreshed on the client side; port UDP 20009 is blocked from the client to gateway; client management port is disabled on the gateway.

Windows Device Groups

The **Windows Device Groups** tab page (**Client Manager** category) allows you to group managed Windows devices and administer them together.

Creating a Windows Device Group

To create a Windows Device Group:

- 1 Navigate to the **Windows Devices Groups** tab in the **Client Manager** category and click **Tasks > Add**.

- 2 On the **Main** tab page, specify a group name and an optional description.
- 3 On the **OS Settings** tab page, set the following options:
 - **Disable removable drives.** Disable mounting of removable drives on managed Windows device.
 - **Disable Print Screen.** Disable the **Print Screen** key.
 - **Replace desktop.** This feature makes a Windows computer behave like a thin client. It limits users from changing system settings or installing new applications. The administrator can add local apps (which are already installed on a computer) to the app list in addition to published resources from Parallels RAS. If you select this option, specify an administrator password in the **Admin Mode Password** field (below) to be used to switch a computer between user and admin modes.
 - **Kiosk mode.** Enable the kiosk mode. This will disable power cycling functions (reboot, shutdown) on computers in the group.
 - **Use client as desktop.** If this option is selected, Parallels Client will run in full screen mode. A user will not be able to minimize it. Select this option to overcome an issue with Parallels Client breaking out of the kiosk mode on Windows 8.x. The issue may manifest itself in the tile-based UI or while using the "drag to close" feature.
 - **Admin Mode Password.** Specify a password to switch between user and admin modes when a Windows desktop is replaced (see **Replace desktop** above).
- 4 On the **Firewall Settings** tab page, add the inbound ports if necessary.
- 5 On the **Shadowing** tab page, select the **Request Authorization** option to prompt a Windows device user before remotely controlling their desktop. If enabled, the user can choose to decline the connection. For more information, see **Managing Windows Devices** (p. 205).

Adding a Windows Device to a Group

To add a Windows device to a group:

- 1 Navigate to the **Client Manager / Devices** tab page.
- 2 Right-click a managed Windows device and choose **Move to Group** in the context menu.
- 3 Select a group and click **OK** to save the settings.

The administrator can now perform standard Windows power operations (Power On, Power Off, Reboot, Logoff, Lock) on groups of devices.

Managing Windows Devices

The Client Manager feature allows the administrator to convert Windows devices running Windows 7 up to Windows 10 into a thin-client-like OS. In order to be managed, Windows devices must be running the latest version of Parallels Client for Windows.

Read the instructions below to learn how to set up Parallels Client on a Windows computer and how to enroll and manage it in Parallels RAS.

Install Parallels Client on a Windows computer

To install and configure Parallels Client for Windows, follow the steps below. You can also read the **Parallels Client for Windows User's Guide** for the complete instructions on how to install and configure Parallels Client.

- 1 Download the Parallels Client for Windows from <https://www.parallels.com/products/ras/download/client/>
- 2 Double click the `RASClient.msi` or `RASClient-x64.msi` and follow the on-screen instructions to complete the installation wizard.
- 3 Create a new Parallels RAS connection by clicking **File > Add New Connection**.
- 4 Select **Parallels Remote Application Server** and click **OK**.
- 5 Next, configure the following connection properties:
 - **Primary Connection** — Specify the Parallels RAS FQDN or IP address.
 - **User Credentials** — Enter username, password, and domain.
- 6 Click **OK** to create the connection and then double-click it to connect to Parallels RAS.

Upon completion, the Windows device will appear in the Parallels RAS Console in **Client Manager / Devices**.

Windows device enrollment

You can configure Parallels RAS to enroll a Windows device automatically or you can opt to do it manually.

To manually enroll a Windows device in Parallels RAS:

- 1 In the RAS Console, navigate to **Client Manager / Devices**.
- 2 Select a device on the **Devices** tab.
- 3 Click **Tasks > Manage Device**.

The device state will change to **Pair pending** until the device reconnects. Ensure the **Client Manager Port** option is enabled for a gateway. To verify this:

- 1 Navigate to **Farm / <site> / Gateways**.
- 2 Select a gateway and click **Tasks > Properties**.
- 3 Click the **Network** tab and make sure that the **Client Manager Port** option is selected

Once the device reconnects, the enrollment process is complete and the device state is updated to **Logged On**, which indicates that it's now managed by Parallels RAS. The user running Parallels Client on their Windows PC can also verify that the PC is managed by clicking **Help > About** on the main Parallels Client menu. The information includes the RAS Secure Client Gateway information that the Parallels Client uses to communicate with Parallels RAS.

You can also set Parallels RAS to automatically manage Windows devices. To do so:

- 1 In the RAS Console, select the **Client Manager** category.
- 2 Click the **Options** tab.
- 3 Enable the **Automatically manage Windows devices** option.

The administrator can now check the state of the device and perform power operations, such as Power On, Power Off, Reboot, and Logoff.

Note: Devices running some older versions of Parallels Client cannot be managed and are marked as **Not Supported**.

Lock a Windows device

To lock a Windows device that has an active session, select it in the list and then click the **Lock** item in the toolbar at the bottom. Note that the **Lock** icon is only enabled when the selected device is in the **Logged On** state.

You can also lock a device (or a device group) using the scheduler, which is described in the **Scheduling Windows Devices & Group Power Cycles** section (p. 212).

Shadow a Windows device

By shadowing a Windows device, you gain full access to the Windows desktop on the device and can control local and remote applications.

To shadow a Windows device:

- 1 In the RAS Console, navigate to **Client Manager / Devices**.
- 2 Select a device and click the **Shadow** item in the toolbar at the bottom.

The Windows user will be prompted to allow the administrator to take control over the device and can choose to deny access. The **Request Authorization** prompt can be deactivated by the administrator. To do so:

- 1 In the Parallels RAS Console, select the **Client Manager** category and click the **Windows Device Groups** tab in the right pane.
- 2 Right-click a group and choose **Properties**.
- 3 In the **Windows Device Group** dialog, select the **Shadowing** tab and clear the **Request Authorization** option.

Desktop replacement

The **Replace desktop** feature limits users from changing system settings or installing new applications. When this feature is enabled, the Windows desktop is replaced by Parallels Client, which converts it into a thin-client-like OS without actually replacing the operating system. This way the user can only deploy applications from Parallels Client, which gives the administrator a higher level of control over connected devices.

Additionally, the Kiosk mode allows you to limit the user from power cycling a device (power actions are still available in the Admin mode; see below for details.).

To enable the **Replace desktop** feature:

- 1 In the **Client Manager** category, select the **Windows Device Groups** tab.
- 2 Right-click a group and choose **Properties**.
- 3 Click the **OS Settings** tab.
- 4 Enable the **Replace desktop** option and optionally the **Kiosk mode** option.
- 5 Click **OK**.

Note: This feature requires an administrative password set to switch between User and Admin mode on the Windows device.

Switching to Admin mode

In User mode, the user is restricted to use only the applications provided by the administrator. In order to change system settings, switch the device to the Admin mode.

To switch to the Admin mode, right-click on the system tray icon and select **Switch to admin mode**. Type the password when prompted.

The following table outlines features that are available in Admin and User modes.

Feature	User Mode	Admin Mode
Parallels Client Global Options		x
Parallels Client Farm Connection Properties		x
Configuration of Local Applications		x
Add a new RAS Connection		x
Add a new RDP Connection		x

Manage Standard RDP Connections and Folders		x
Display Settings	x	x
Mouse Settings	x	x
Printer Settings		x
Task Manager		x
Control Panel		x
Command Prompt		x
Windows Explorer		x
Import / Export Settings		x

Configuring local applications when using Parallels Client desktop replacement

With the **Replace Desktop** option enabled, the administrator's goal should be to deploy remote applications or remote desktops and use the native OS to simply deploy the software needed to connect remotely. However, in some instances, local applications may be required. The administrator still has the ability to configure local applications to be shown within the Parallels Client Desktop Replacement, however it is necessary to switch to the Admin mode prior to it.

Publish a local application according to the following steps:

- 1 Shadow the user's session or use the user device station directly.
- 2 Switch the Parallels Client Desktop Replacement to admin mode.
- 3 Click **File > Add New Application**
- 4 Fill in the application information
- 5 Applications added will be visible in the Application Launcher.
- 6 Switch back to user mode once all the applications needed are configured.

Windows Desktop Replacement

This section explains what happens when the **Replace Desktop** option is enabled, and why it is useful to administrators.

When enabled, the Replace Desktop feature allows the administrator to convert a standard desktop into a limited device similar to a Thin Client, without replacing the operating system.

The end user will not have access to Windows Explorer, Taskbar or any other Windows components that usually allow them to install new applications or change system settings. The user can now only deploy applications configured within the Parallels Client, including remote applications, remote desktops, and locally configured applications. Local applications are allowed, so if a specific application is needed, but is not available remotely (e.g. a software which communicates with specific peripherals), the user can still deploy it.

When the **Replace Desktop** option is enabled, the following features take effect on the corresponding versions of Windows (7, 8, 8.1, 10):

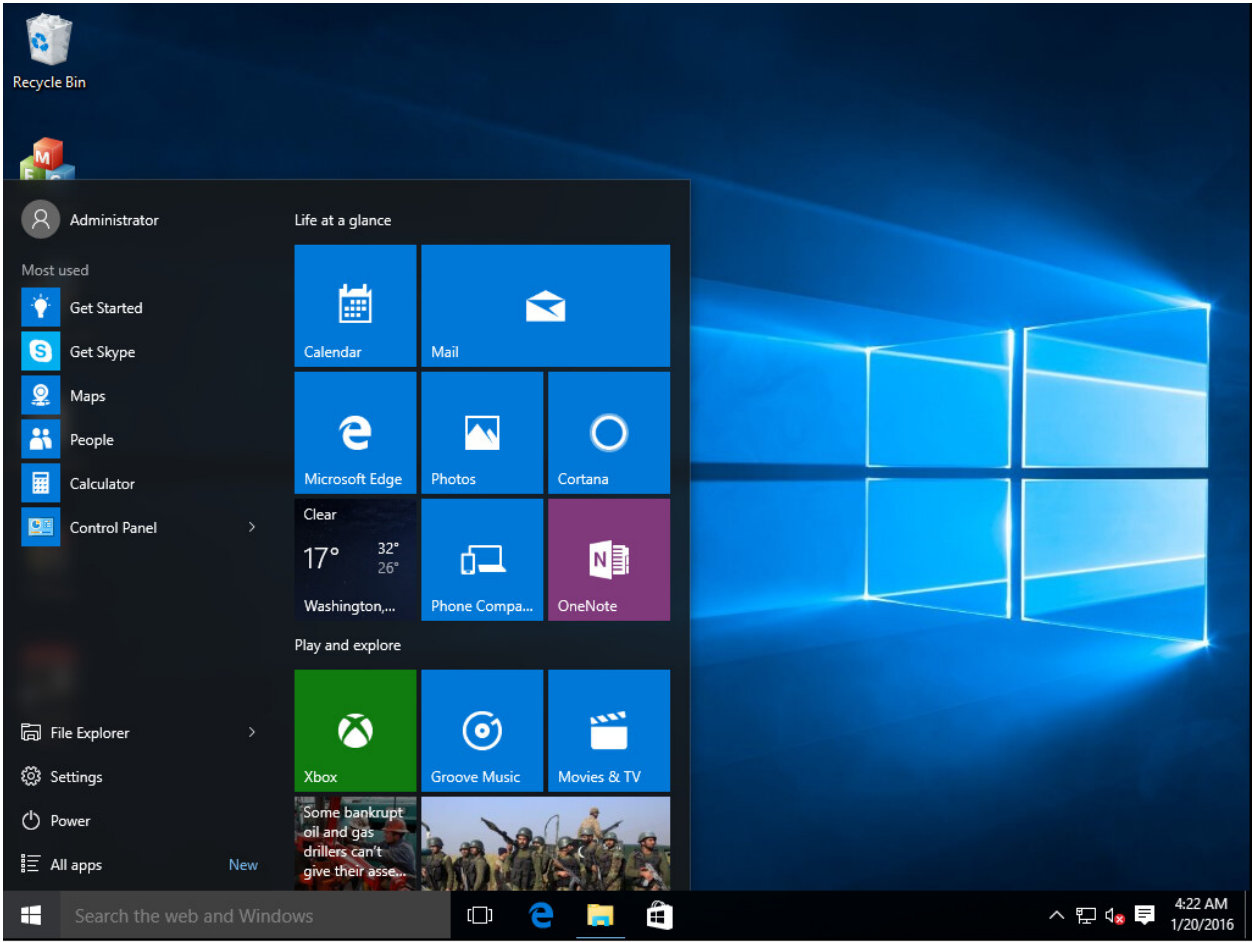
Feature	7	8	8.1	10
Replace Desktop with Parallels Client	x	x	x	x
Disable Start Button	x	x	x	x
Restrict Control Panel Access	x	x	x	x
Disable Windows Key	x	x	x	x
Disable the Task Manager	x	x	x	x
Disable Quick Access Toolbar	n/a	n/a	n/a	n/a
Disable Security Manager/Action Center Notifications	x	x	x	x
Lock the Taskbar	x	x	x	x
Remove Pinned Applications	x	x	x	x
Disable Metro Screen (user logs directly to desktop)	n/a	x	x	x
Disable Hot Corners	n/a	x	x	x
Disable Charm Hints	n/a	x	x	x
Disable Help Aids	n/a	x	x	x
Disable Windows Sidebar	x	n/a	n/a	n/a

In this mode, the user also has access to the Mouse and Display Control Panel applets. The user cannot change the Parallels Client Global Options and the Client Farm Connection Options. Advanced management features can be enabled if the device is switched into administration mode.

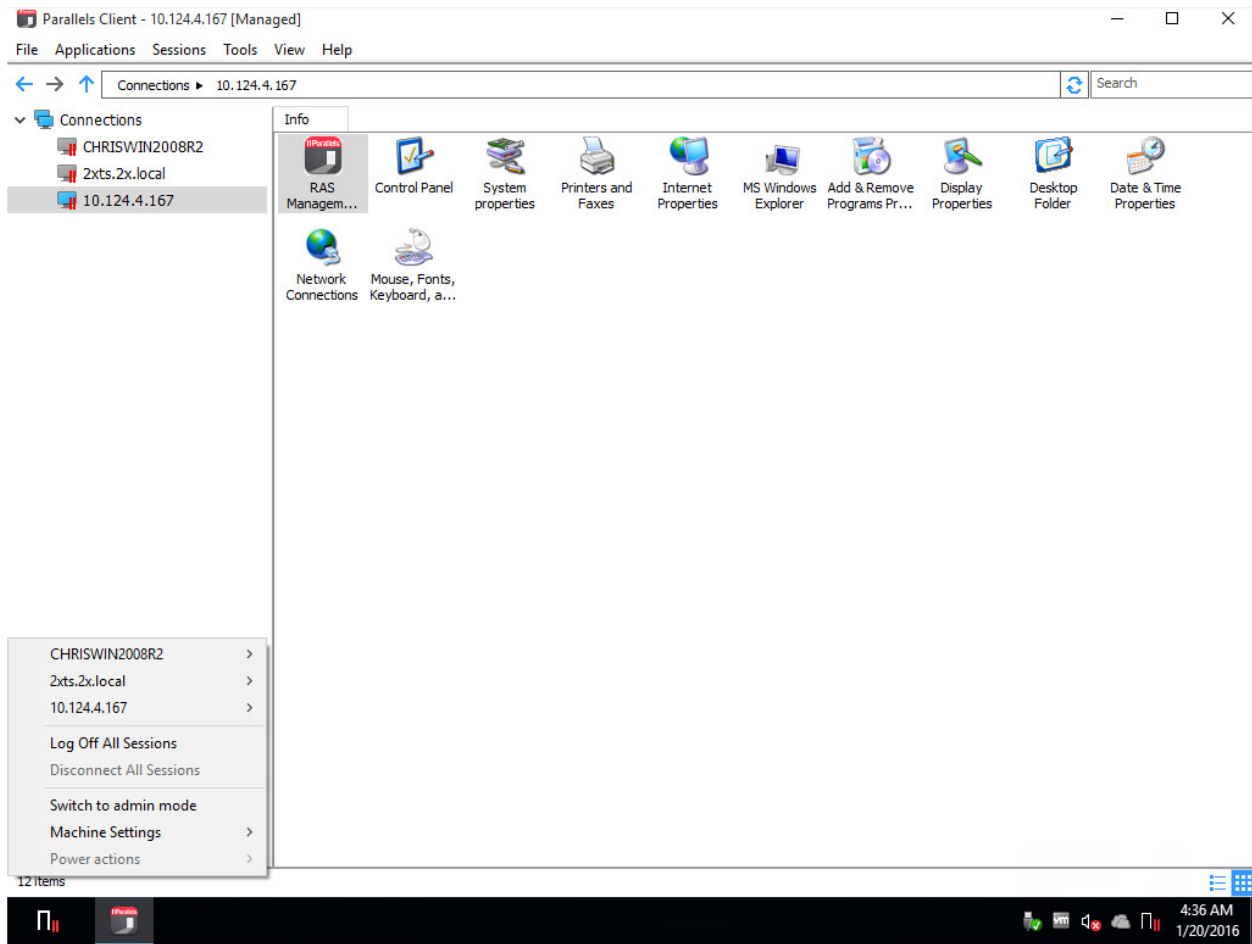
If the Windows Desktop Replacement feature is switched off, all the restrictions are removed and the standard desktop is made available to the user.

The following are the screenshots of a Windows 10 desktop before and after the **Replace Desktop** option is enabled.

Before



After



Scheduling Windows Devices & Groups Power Cycles

The **Scheduler** tab of the **Client Manager** category can be used to schedule automatic power operations on devices.

Adding a New Scheduler Task

To schedule a task:

- 1 On the **Scheduler** tab, click **Tasks > Add** to open the **Device Scheduler Properties** dialog.
- 2 Select the **Enable this scheduled entry** option.
- 3 Select an action in the **Action** drop-down list:

- **Device Group Switch On**
 - **Device Group Log Off**
 - **Device Group Switch Off**
 - **Device Group Reboot**
 - **Device Group Lock**
- 4** Select a device group in the **Target** drop-down list.
 - 5** Specify the task start date and time.
 - 6** Select the **Repeat** option from the following choices:
 - **Never** (a task will run only once, as specified in the **Start** and **Time** fields)
 - **Every day**
 - **Every week**
 - **Every 2 weeks**
 - **Every month**
 - **Every year**
 - 7** Enter a task description in the **Description** field.
 - 8** Click **OK** to create the task.

Managing Scheduled Tasks

To modify an existing task, right-click it in the **Schedule List** and click **Properties** in the context menu.

To enable or disable an event, right-click it, click **Properties**, and then select or clear the **Enable this scheduled entry** option.

To execute a scheduled task immediately, right-click it and click **Execute Now** in the context menu.

To delete a task, right-click it and then click **Delete**.

Client Policies

The **Policies** category allows you to manage Parallels Client policies for users connecting to a farm. By adding client policies, you can group users and push different Parallels Client settings to user devices forcing them to function as your organization requires.

Settings that can be enforced on user devices include RAS connection properties, display, printing, scanning, audio, keyboard, device, and others. Once you create a policy and push it to a client device, the user of the device cannot modify the settings that the policy enforces. In Parallels Client this will manifest itself as hidden or disabled connection properties and global preferences.

Supported Parallels Client versions

- Parallels Client for Windows / macOS / Linux / Chrome
- Parallels HTML5 Client
- On iOS and Android devices, Session settings (p. 215), Control settings (p. 229) and Gateway redirection (p. 229) are supported.

Note: Starting with Parallels RAS v16.5, a new approach is used to manage client policies. In the previous versions, a client policy would apply the full set of parameters and replace the client settings completely hiding an enforced category. In RAS v16.5 and newer, client policy settings are split into smaller groups with the ability to configure and enforce each group on the client side individually. For the information on how this affects existing client policies that were created in earlier version of Parallels RAS, please read **Client Policy Backward Compatibility** (p. 231).

In this section:

- Add a new client policy (p. 214)
- Configure session settings (p. 215)
- Configure client policy options (p. 226)
- Configure control settings (p. 229)
- Configure gateway redirection (p. 229)
- Client Policy Backward Compatibility (p. 231)

Add a New Client Policy

To add a new client policy:

- 1** Select the **Policies** category and then click **Tasks > Add** in the right pane. The **Policy Properties** dialog opens.
- 2** The left pane contains a navigation tree allowing you to select a group of options to configure.
- 3** Make sure the **Policy** node is selected and then specify a policy name and an optional description.
- 4** In the **Browse Mode** drop-down list, select how you want to browse for users and groups. The preferred mode is **Secure Identifier** (default). Other options exist for backward compatibility.
- 5** In the **Apply policy to** section, click **Tasks > Add** (or click the plus sign icon) and specify the target users and/or groups.

Configure criteria for the client policy

By default, a client policy applies to configured users and groups in all situations. You can optionally define a criteria when the policy should apply. This functionality allows you to create different policies for the same user, which will be applied depending on where the user is connecting from and from which device.

To create a new criteria:

- 1 Select **Criteria** (under the **Policy** node) in the left pane.
- 2 In the "gateway criteria" section, select the criteria type in the first drop-down list and then specify the values (if applicable) in the second drop-down list.
- 3 In the "MAC address criteria" section, select the criteria type in the first drop-down list and then specify the values (if applicable) in the second drop-down list.
- 4 In the "Parallels Clients" section, select the version of Parallels Client to which this policy should apply.

Configure Session Settings

Items under the **Session** node in the **Policy Properties** dialog include connection, display, printing, network, and other settings that will be enforced on a client if defined and enabled.

For a particular group of settings to be enforced on a client device, it must be selected (checked). Unselected groups will not be enforced, so end users will be able to configure them themselves. For example, you can check the **Connection** node, but only check the **Primary connection** and **Secondary connections** groups under it. This will enforce only the two selected groups of settings on client devices.

In this section:

- Connection (p. 216)
- Display (p. 217)
- Printing (p. 218)
- Scanning (p. 220)
- Audio playback (p. 221)
- Keyboard (p. 221)
- Local devices and resources (p. 222)
- Experience (p. 223)
- Network (p. 224)
- Server authentication (p. 224)
- Advanced settings (p. 224)

Connection

To configure connection properties, select the **Connection** node and then go through each child node configuring their respective properties.

Primary connection

The primary connection always defaults to the primary RAS Secure Client Gateway, but you can modify the following connection properties:

- 1 Specify a friendly name for the connection.
- 2 Select the **Auto Logon** option to enable Parallels Client to connect automatically without displaying the **Logon** dialog every time a user connects to a remote server.
- 3 In the **Authentication type** drop-down list, select the desired method of authentication:
 - **Single Sign-On**. This option will be included in the list only if the Single Sign-On module is installed during Parallels Client installation. Select this option to use local system credentials to connect to the remote server.
 - **Smart Card**. Select this option to authenticate using a smart card. When connecting to the remote server, a user will need to insert a smart card into the card reader and then enter a PIN when prompted.

Note: The allowed authentication type(s) must be specified in the RAS Console in **Connection / Authentication**.

- 4 Select or clear **Save password** as needed (if credentials are used for authentication). This means forcing a client to save the password for this connection.
- 5 Specify the domain name (if credentials are used for authentication).

Secondary Connection

If you have more than one RAS Secure Client Gateway, you can define a secondary connection, which will be used as a backup connection in case the primary gateway connection fails.

To add a secondary connection:

- 1 Select the **Secondary connections** item.
- 2 In the **Secondary connections** pane, click **Tasks > Add** and specify a server name or IP address.
- 3 Select the connection mode and modify the default port number if necessary.

If you have multiple secondary connections, you can move them up or down in the list. If the primary connection cannot be established, Parallels Client will use secondary connections in the order listed.

Reconnection

In this pane, specify what to do if the connection is dropped:

- **Reconnect if connection is dropped.** If this option is selected, Parallels Client will try to reconnect if the connection is dropped. The **Connection retries** property specifies the number of retries.
- **Show connection banner if reconnection is not established within.** Specifies the number of seconds after which the connection banner will be displayed in Parallels Client. This will inform the user that the connection was dropped and will allow them to take actions on their own.

Computer name

Specify the name that a computer will use during a remote desktop session. If set, this will override the default computer name. Any filtering set by the administrator on the server side will make use of the **Override computer name** setting.

Advanced settings

- **Connection timeout.** The Parallels Client connection timeout value.
- **Show connection banner if connection is not established within.** Specifies the number of seconds after which the connection banner will be displayed. This will inform the user that the connection cannot be established and will allow them to take actions on their own.
- **Show desktop if published application does not start within.** If a published application is not launched within the time period specified in this field, the host server desktop will be shown instead. This is helpful if an error occurs on the server side while launching an application. By showing the server desktop, the user can see the error message.

Display

To configure display settings, select the **Display** node and then configure the groups of settings described below.

Settings

Select the desired video acceleration mode and color depth.

Multi-monitor

Specify whether all monitors should be used for a desktop session if more than one monitor is connected to the user's computer.

Published applications

Select the **Use primary monitor only** option to start published applications on the primary monitor. Other monitors connected to a user's computer will not be used.

Desktop options

Specify the desktop options as follows:

- **Smart-sizing.** Desktop smart sizing will scale a remote desktop to fit the connection window.
- **Embed desktop in launcher.** Enable this option to access a published desktop inside Parallels Client.
- **Span desktop across all monitors.** Enable this option to span published desktops across all connected monitors.
- **Connection bar in full screen.** Specify whether the connection bar should be pinned, unpinned, or hidden when connecting in full screen mode.

Browser

This section applies to Parallels HTML5 client only. Specify whether a remote application should open in the same or a new tab in a web browser by default.

Printing

The **Printing** pane allows you to configure printing options.

In the **Technology** section, select the technology to use when redirecting printers to a remote computer:

- **None.** No printer redirection will be used.
- **RAS Universal Printing technology.** Select this option if you want to use RAS Universal Printing technology.
- **Microsoft Basic Printing Redirection technology.** Select this option if you want to use Microsoft Basic printing technology.
- **RAS Universal Printing and Microsoft Basic redirection technologies.** Select this option to use both Parallels RAS and Microsoft technologies.

RAS Universal Printing

If you selected **RAS Universal Printing technology**, use the **Redirect Printers** drop-down list to specify whether to redirect all printer on the client side, default printer only, or specific printers.

If you select **Specific only** in the step above, click **Tasks > Add**. Type a printer name and then click the **Options** button. In the dialog that opens, specify settings described below.

In the **Choose Format** drop-down list, select a data format for printing:

- **Print Portable Document Format (PDF).** Adobe PDF. This option does NOT require you to install any local applications capable of printing a PDF document. All the necessary libraries are already installed together with Parallels Client.
- **View PDF with external application.** To use this option you must have a local application installed which is capable of viewing a PDF document. Note that not all applications are supported. For example, the built-in PDF viewer in Windows is not supported, so you must have Adobe Acrobat Reader (or a similar application) installed.
- **Print PDF with external application.** This option works similar to the View PDF option above. It also requires an application capable of printing a PDF document installed locally.
- **Enhanced Meta File (EMF).** Use vector format and embedded fonts.
- **Bitmap (BMP).** Bitmap images.

In the **Client printer preferences** section, select one of the following:

- **Use server preferences for all printers.** If this option is selected, a generic printer preferences dialog will be shown when a user clicks **Print** in a remote application. The dialog has only a minimal set of options that they can choose.
- **Use client preferences for all printers.** With this option selected, a local printer preferences dialog will open when a user clicks **Print** in an application. The dialog will contain a full set of options for a particular printer that the user has installed on their local computer. If they have more than one printer installed, a native preferences dialog will open for any particular printer that they choose to print to.
- **Use client preferences for the following printers.** This option works similar to the **Use client preferences for all printers option** (above), but allows users to select which printers should use it. Select this option and then select one or more printer in the list below. If a printer is not selected, it will use the generic printer preferences dialog, similar to the first option in this list.

Default printer settings

To configure default printer settings, click the **Change Default Printer settings** button.

The default printer list shows printers that can be redirected by the client to the remote computer:

- To disable the default printer, select **<none>**.
- To redirect the default local printer, select **<defaultlocalprinter>**.
- When **<custom printer>** is selected, you can specify a custom printer. The first local printer that matches the printer name inserted in the **Custom** field will be set as the default printer on the remote computer.

Select **Match exact printer name** to match the name exactly as inserted in the **Custom** field. Please note that the remote printer name may not match the original printer name. Also note that local printers may not redirect due to server settings or policies.

The **Force Default printer for** option specifies the the time period, during which a printer will be forced as default. If the default printer is changed during this time after the connection is established, the printer is reset as default.

Select the **Update the remote default printer if the local default printer is changed** option to change the remote default printer automatically when the local default printer is changed. Please note that the new printer must have been previously redirected.

A Windows 10 note

Windows 10 has a feature that automatically sets the default printer to the one used most recently or more often. This can break the default printer control on RD Sessions Hosts, guest VMs, and Remote PCs. To resolve this issue, the default printer management in Windows 10 should be disabled. To disable this feature using the Group Policy, do the following:

- 1 Open the group policy editor.
- 2 Navigate to **User Configuration > Administrative Templates > Control Panel > Printers**.
- 3 Find the **Turn off Windows default printer management** policy and enable it.
- 4 Force the group policy to all computers attached to the domain.

You can also disable the default printer management in Windows 10 locally by using the GUI or the registry editor:

- 1 On a Windows 10 computer, click **Start**, then click the "gear" icon which will open the **Settings** page.
- 2 On the **Printers and Scanners** tab, set the **Let Windows manage my default printer** option to **OFF**.

Using the registry editor:

- 1 Open the registry editor (regedit).
- 2 Navigate to HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows.
- 3 Create a new DWORD item and name it **LegacyDefaultPrinterMode**.
- 4 Change the item's Value data to hexadecimal and set the value data to **1**.

In addition to disabling the default printer management, the **Download over metered connections** option should be enabled in **Settings > Devices > Printers & Scanners**.

Scanning

On the **Scanning** pane, you can specify a scanner that should be used when one is required by a published application:

- **Use.** Allows you to select a scanning technology. RAS Universal Scanning uses TWAIN and WIA redirection allowing an application to use either technology depending on the hardware type connected to the local computer. If you select **None**, scanning will be disabled.
- **Redirect Scanners.** Select scanners attached to your computer for redirection. You can select **All** (all attached scanners will be redirected) or **Specific only** (only the scanners you select in the provided list will be redirected).

Audio Playback

This pane allows you to configure remote audio settings.

Use the **Remote computer** drop-down list to select one of the following remote audio playback options:

- **Bring to this computer.** Audio from the remote computer will play on your local computer.
- **Do not play.** Audio from the remote computer will not play on your local computer and will be muted on the remote computer as well.
- **Leave at remote computer.** Audio will not play on your local computer but will play normally on the remote computer.

Use the **Quality** drop-down list to adjust the audio quality:

- **Dynamically adjust based on available bandwidth.** This option will increase or decrease the audio quality based on your connection speed. The faster the connection, the higher audio quality setting will be used.
- **Always use medium audio quality.** The audio quality is fixed at the medium level. You can use this option when you don't require the best possible audio quality and would rather use the available bandwidth for graphics.
- **Always use uncompressed audio quality.** The audio quality is fixed at the highest level. Select this option if you have a very fast connection and require the best possible audio quality.

The **Recording (if applicable)** option allows you to enable audio recording on the remote computer. For example, you can speak into a microphone on the local computer and use a sound recording application on the remote computer to record yourself.

Keyboard

On the **Keyboard** pane, select how you want to apply key combinations (e.g. Alt+Tab) that you press on the keyboard:

- **On the local computer.** Key combinations will be applied to Windows running on the local computer.
- **On the remote computer.** Key combinations will be applied to Windows running on the remote computer.
- **In full screen mode only.** Key combinations will be applied to the remote computer only when in the full-screen mode.

Select or clear the **Send unicode characters** as needed.

Local Devices and Resources

Use the **Local devices and resources** pane to configure how local resources are used in a remote session.

Clipboard

Select the **Allow clipboard redirection** option to enable the local clipboard in a remote session.

Note: When you clear this option, it will also disable the Remote Clipboard functionality for affected users in Parallels HTML5 client. For more information, please see **Using the Remote Clipboard** (p. 165).

Disk drives

Select the **Allow disk drives redirection** option and select local drives you want to redirect, or select **Use all disk drives available**.

If you select the **Use also disk drives that I plug in later** option, disk drives that you connect to a local computer later will be automatically available in a remote session. Note that this option applies to Parallels Client for Windows only.

Devices

On this pane, specify whether to redirect local devices in general, use all devices available, and also devices that will be plugged in later.

Local devices that can be redirected include supported Plug and Play devices, media players based on the Media Transfer Protocol (MTP), and digital cameras based on the Picture Transfer Protocol (PTP).

Please note that disk drives and smart cards are redirected using dedicated **Disk drives** and **Smart cards** options.

Ports

Select whether to redirect LPT and COM ports.

Smart cards

Select whether to redirect smart cards. Note that if smart card is selected as the authentication type in the **Primary connection** pane, the smart card redirection is automatically enabled and this option is grayed out.

File transfer

Select whether to allow remote file transfer. For additional information, see **Enabling or Disabling Remote File Transfer** (p. 231).

Experience

The **Experience** pane allows you to tweak connection speed and compression.

Performance

Choose your connection speed to optimize performance: Choose a connection type according to your situation and then select experience options you want enabled. If you are connecting to a remote server on a local network that runs at 100 Mbps or higher, it is usually safe to have all of the experience options enabled. If you choose **Detect connection quality automatically**, the experience options will be enabled by default, but some may be dynamically disabled depending on the actual connection speed.

Enhance windows move/size: Enable this option if your users experience graphics artifacts (black squares) while moving or resizing a remote application window on their desktops. The issue may manifest itself when a remote application is hosted on a Windows Server 2016 or 2019 and when the **Show contents of window while dragging** option is enabled. The issue does not appear with any other versions of Windows.

Compression

It is recommended to enable compression to have a more efficient connection. The available compression options are described below.

Enable RDP Compression: Enables compression for RDP connections.

Universal printing compression policy: The compression type should be selected based on your environment specifics. You can choose from the following options:

- **Compression disabled.** No compression is used.
- **Best speed (uses less CPU).** Compression is optimized for best speed.
- **Best size (uses less network traffic).** Compression is optimized to save network traffic.
- **Based on connection speed.** The faster the connection speed, the lower compression level and the minimum data size to compress are used.

Universal scanning compression policy: This drop-down list has the same options as the universal printing compression above. Select the compression type based on your environment specifics.

Network

Use the **Network** pane to configure a proxy server if you have one.

Select the **Use proxy server** option and then select the protocol from the following list:

- **SOCKS4**. Enable this option to transparently use the service of a network firewall.
- **SOCKS4A**. Enable this option to allow a client that cannot connect to resolve the destination host's name to specify it.
- **SOCKS5**. Enable this option to be able to connect using authentication.
- **HTTP 1.1**. Enable this option to connect using a standard HTTP 1.1 protocol connection.

Specify the proxy host's domain name or IP address and the port number.

For SOCKS5 and HTTP 1.1 protocols, select the **Proxy requires authentication** option. For authentication, select the **Use user logon credentials** option or specify a user name and password in the fields provided.

Server Authentication

Use the **Server authentication** pane to specify what should happen if authentication of an RD Session Host, Remote PC, or Guest VM fails.

In the **If authentication fails** drop-down list, select one of the following options:

- **Connect**. The user can ignore the certificate of the server and still connect.
- **Warn**. The user is alerted about the certificate and still has the ability to choose whether to connect or not.
- **Do not connect**. The user is not allowed to connect.

Advanced Settings

The **Advanced Settings** pane allows you to customize the default behavior of Parallels Client.

You can specify the following properties:

- **Use client system colors**. Enable this option to use the client system colors instead of those specified on the remote desktop.
- **Use client system settings**. Enable this option to use the client system settings instead of those specified on the RD Session Host.
- **Create shortcuts configured on server**. For each published application, the administrator can configure shortcuts that can be created on the client's desktop and the Start menu. Select this option to create the shortcuts, or clear the option if you don't want to create them.

- **Register file extensions associated from the server.** For each published application, the administrator can create file extension associations. Use this option to either register the associated file extensions or not.
- **Redirect URLs to the client device.** Enable this option to use the local web browser when opening 'http:' links.
- **Redirect MAILTO to the client device.** Enable this option to use the local mail client when opening 'mailto:' links.
- **Always ask for credentials when starting applications.** If this option is enabled, the user will be prompted to enter their credentials when starting applications.
- **Allow Server to send commands to be executed by client.** Enable this option to allow commands being received from the server to be executed by the client.
- **Confirm Server commands before executing them.** If this option is enabled, a message is displayed on the client to confirm any commands before they are executed from the server.
- **Network Level Authentication.** Check this option to enable network level authentication, which will require the client to authenticate before connecting to the server.
- **Redirect POS devices.** Enables the Point of Service (POS) devices such as bar code scanners or magnetic readers that are attached to the local computer to be used in the remote connection.
- **Use Pre Windows 2000 login format.** If this option is selected, it allows you to use legacy (pre-Windows 2000) login format.
- **Disable RDP-UDP for gateway connections.** Disables RDP UDP data tunneling on the client side. You can use this option when some clients experience random disconnects when RDP UDP data tunneling is enabled on the RAS Secure Client Gateway (the **Network** tab in the gateway **Properties** dialog), while other clients are not.
- **Do not show drive redirection dialog.** This option affects Parallels Client for Mac. By default, the **Grant access to Home folder** (drive redirection) dialog opens automatically when a Mac user connects to Parallels RAS. This happens when this option is disabled or when there's no client policy at all. The dialog allows the user to configure which folders on the local disk drive should be available to remote applications. If you enable this option, the dialog will NOT be shown a user. Read below for more explanation.

Drive redirection cannot be configured via client policies, so Mac users have to do this themselves. By automatically showing the dialog, you can invite the user to go through the local folder configuration procedure. On the other hand, if there's no need for your users to redirect their local drives, you can disable the automatic opening of the dialog. Note that the dialog can still be run manually in Parallels Client for Mac at any time by opening **Connection Properties > Local Resources**, selecting the **Disk drives** option and clicking **Configure**.

When the option is disabled (or when there's no client policy defined), the dialog opens at least once when the user connects to Parallels RAS for the first time. At that time, the user can either configure local folders or select the **Never ask me** again option. In both cases, the dialog will NOT be shown to the user anymore. The Mac user can reset the **Never ask me** selection by going to **Connection Properties > Advanced** and clearing the **Do not show drive redirection dialog** option.

Configure Client Policy Options

The **Client options** node allows you configure client policy options. Select the node and then select and configure individual items under it as described below.

Connection

On the **Connection** pane, specify the following options:

- **Connection Banner.** Select a banner to display while establishing a connection.
- **Automatically refresh connected RAS connections every [] minutes.** Select this option and specify the time interval to automatically refresh a connection. This will refresh the published resources list in Parallels Client.

Update

Select **Check for updates on startup** and specify an update URL if you want Parallels Client to check for updates when it starts. The URL can point to the Parallels website or you can store updates on your local network and use this local URL. For the information on how to configure a local update server, please read <http://kb.parallels.com/123658>.

Note: This option works with Parallels Client for Windows only. Parallels Client for Mac can be updated only from the App Store. Parallels Client for Linux does not support this feature.

PC keyboard

To force a particular keyboard to be used, select the Force use PC keyboard and select a keyboard layout from the drop-down list. Note that the selected layout can and will only be used in a Parallels Client version that supports this particular layout.

Single Sign-On

Parallels Client for Windows comes with its own SSO component that you can install and use to sign in to Parallels RAS. If you already use a third-party credential provider component on your Windows computers, you first need to try if the single sign-on works right out of the box. If it doesn't, you need to configure Parallels RAS and Parallels Client to use the Parallels RAS SSO component to function as a wrapper for the third-party credential provider component.

To use Parallels RAS SSO as a wrapper, specify a third-party component, select the **Force to wrap third party credential provider component** option and specify the component's GUID in the field provided. You can obtain the GUID in Parallels Client as follows:

- 1 Install Parallels Client on a computer that has the third-party component installed.
- 2 In Parallels Client, navigating to **Tools > Options > Single Sign-On** (tab page).

- 3 Select the "Force to wrap..." option and then select your provider in the drop-down list.
- 4 Click the **Copy GUID to Clipboard** button to obtain the component's GUID.

You will also need to specify the component's GUID when setting up an invitation email in the RAS Console. If you haven't set up an invitation email yet, you can do it as follows:

- 1 In the RAS Console, select the **Start** category and then click the **Invite Users** item in the right pane.
- 2 On the second page of the wizard (target platform and connection options), click the **Advanced** button.
- 3 In the dialog that opens, select the **Force to wrap third party SSO component** option and specify the GUID of the component.

For more information, see the **Invite Users** section (p. 28).

After the policies are applied on Windows computers, Parallels Client will be automatically configured to use the specified third-party credentials provider.

Advanced

Use this pane to specify advanced client option:

Global

- **Always on Top.** With this feature enabled, other applications will no longer mask the launcher.
- **Show connection tree.** Displays the connection tree.
- **Minimize to tray on close or escape.** Enable this feature to place the Parallels Client into the System Tray when you click on the **Close** button or hit escape.
- **Enable graphic acceleration (Chrome client).**
- **Do not warn if server certificate is not verified.** When connected to a RAS Secure Client Gateway over SSL, and the certificate is not verified, a warning message will be displayed. You can disable this warning message by enabling this option.
- **Swap mouse buttons.** When enabling this setting, the mouse buttons will be swapped on the remote computer.
- **DPI aware.** This will force a published application to be DPI-aware depending on the client's DPI settings. This feature works on Windows 8.1 or higher.
- **Add RAS Connection automatically when starting web or shortcuts items.** This option will add the connection preferences in the Parallels Client when starting an item contained in a connection that is not yet listed.
- **Do not show prompt message for auto add RAS connection.** Enable this option to disable prompt messages when adding auto connections.
- **Close error messages automatically.** When a session disconnects because of an error, the error is automatically dismissed after 15 seconds.

- **Clear session cookies on exit.** When a user logs on, a Parallels RAS logon cookie is kept on the client side. This will allow the user to connect again with Parallels RAS without re-authenticating. Check this option to delete any cookies when the user closes the Parallels Client.
- **Enable extended logging.** Enables extended logging.

Language

Specify a language that Parallels Client should use. The **Default** option uses the main language used by the client's operating system.

Printing

- **Install missing fonts automatically.** If automatic fonts are installed on the server, they will be available when a session connects.
- **Redirect vendor paper sizes for RAS Universal Printing.** When enabling this setting, non-standard paper sizes which are not included in the standard options will be redirected to the client. Sizes may vary depending on the vendor.
- **Raw printing support.** When enabling this setting, printing will still work for applications sending data in RAW format.
- **Convert non distributable fonts data to images.** During RAS Universal Printing, if a document includes non-distributable fonts, each page is converted to an image.
- **Cache printers hardware information.** Caching of printer hardware information locally to speed-up RAS universal printer redirection.
- **Refresh printer hardware information every 30 days.** Forces the printer hardware information cache update even if nothing has changed in 30 days. When this option is off, the cache will only be refreshed if there were known changes.
- **Cache RAS Universal Printing embedded fonts.** Caching of embedded fonts locally to speed-up RAS universal printing process time.

Windows client

- **Hide Launcher when application is launched.** If this option is enabled, the launcher will be minimized in the system tray after an application is launched.
- **Launch automatically at Windows startup.** This option will place a shortcut in the start menu folder of the client and the Parallels Client will launch automatically on Windows startup.

Configure Control Settings

Control settings options allow you to control various actions on the client side. These options affect the following Parallels Clients:

- Windows
- Linux
- Mac
- Android
- iOS

Connections

On the **Connections** pane, select (or clear) the following options:

- **Prohibit adding of RAS connections.** When a user presses the **Add Connection** button, an RDP connection is always created.
- **Prohibit adding standard RDP connections.** When a user presses the **Add Connection** button, a RAS connection is always created

Password

On the **Password** pane, specify the following options:

- **Prohibit saving password.** The option to save the password will not be shown to the user for that particular connection. A password is never saved on a disk, but kept in memory until the user closes the application.
- **Prohibit changing password.** The option to change the password will not be shown in the context menu for that particular connection.

Import and export

On the **Import and Export** pane:

- **Prohibit import/export connection setting.** If this option is selected, the **Import** and **Export** buttons will not be shown to the user.

Configure Gateway Redirection

Redirection options allow you to move your existing users from one RAS Secure Client Gateway to another gateway within the same farm, or you can even redirect users to a gateway in a different farm.

Note: When setting gateway redirection, make sure that the gateway criteria (the **Criteria** node) does not conflict with it. Read the **Gateway criteria** subsection at the end of this section for the explanation.

To configure redirection options:

- 1 Select the **Redirection** node in the left pane of the **Policy Properties** dialog.
- 2 In the right pane, specify the new connection properties, including:
 - **Gateway address**
 - **Connection mode**
 - **Port number**
 - **Alternative address**

When this policy is applied to user devices, the following will happen:

- Parallels Client connection settings are automatically updated on each device.
- Parallels Client tests the new connection. If succeeded, the current connection policies are removed and new policies are added.
- If Parallels Client cannot connect to Parallels RAS using new settings, the application list will not be shown and an error message will be displayed saying that the redirection policy has failed to apply. The user will be advised to contact the system administrator.

Gateway criteria

If a policy has both **Redirection** and **Criteria** settings enabled and configured, a situation may occur when the policy is applied in an infinite loop on the client side, which will result in an error. Consider the following possible scenarios when this may happen:

- Parallels Client connects to gateway "A" and applies a policy, which redirects it back to gateway "A". This will continue to loop until Parallels Client gives up and displays an error to the user, which will say, "Failed to apply redirection policy....".
- Parallels Client connects to gateway "A" and applies policy "P1", which redirects it to gateway "B". As expected, Parallels Client connects to gateway "B" and applies policy "P2", which redirects it back to gateway "A" where it all began. This will also continue to loop until Parallels Client gives up and displays the same error message as described above.

Once again, this may only happen if the **Criteria** node is enabled and specified gateways conflict with each other. To avoid it, make sure that the **Gateway criteria** option on the **Criteria** pane is set to **if Client is connected to one of the following gateways** and that the same policy is not applied again when Parallels Client is redirected to a new gateway.

Client Policy Backward Compatibility

Starting with Parallels RAS v16.5, a new approach is used to manage client policies. In the previous versions, a client policy would apply the full set of parameters and replace the client settings completely hiding an enforced category. In RAS v16.5 (or newer), client policy settings are split into smaller groups with the ability to configure and enforce each group on the client side individually. For example, the administrator wants to re-design the policies to disable clipboard redirection only, leaving the rest of the local devices and resources settings available for the end users to control. In the previous version, this would not be possible. The new design allows an administrator to easily achieve this goal.

This section explains how the backward compatibility is achieved with older clients and how new clients retain compatibility with older server-side installations.

The new client policies implementation handles compatibility issues as follows:

- All settings found in older policies are sent to the client as if being sent from an older Parallels RAS server. When a client receives the policy, the **Connection properties** and **Options/Preferences** settings are set correctly from the old design point of view. If, however, the policy is configured in such a way that the user cannot change anything, the entire tab will be hidden (no need to display the options if all of them are disabled).
- The Parallels RAS Console handles old-style policy settings as if they are new and displays them using the updated graphical user interface.
- In terms of policies, when a Parallels RAS v16.5 client connects to a previous version of Parallels RAS, the client keeps working normally and all of the policy settings are functioning as expected.

Enabling or Disabling Remote File Transfer

Parallels RAS provides end users with the ability to transfer files remotely to and from a remote server.

Note: At the time of this writing, file transfer is supported in Parallels HTML5 Client and Parallels Client for Chrome only.

As a Parallels RAS administrator, you have the ability to enable or disable file transfer capabilities if you believe that it presents a security risk. To make this functionality as flexible as possible, Parallels RAS allows you to enable/disable file transfer on the following three levels:

- RD Session Host, VDI host, or Remote PC
- Parallels HTML5 gateway
- Client policy

Whatever file transfer settings you configure on each level, they take precedence in the order listed above. For example, if you enable it on a Parallels HTML5 gateway but disable it on an RD Session Host, file transfer will be disabled for all users who connect to the given RD Session Host through the given HTML5 gateway. As another example, you can enable file transfer on an RD Session Host and then disable it for a particular Client policy (or an HTML5 gateway). This way you can control which clients can use file transfer and which cannot.

Read the subsequent sections to learn how to enable or disable file transfer on each level.

Server Level

To enable or disable remote file transfer capabilities on an RD Session Host, VDI host, or Remote PC, do the following:

- 1 In the Parallels RAS Console, select the **Farm** category and then select a desired server type (RD Session Host, VDI host, Remote PCs) in the middle pane.
- 2 Right-click a desired server in the right pane and choose **Properties**.
- 3 Select the **Agent Settings** tab.
- 4 Select or clear the **Allow file transfer command** option (at the bottom). If the server is using default settings, click the **Edit Defaults** link in the top-right corner and then select or clear the same option in the **Default Server Properties** dialog.

HTML5 Gateway Level

To enable or disable remote file transfer capabilities on an HTML5 gateway, do the following:

- 1 In the Parallels RAS Console, navigate to **Farm / <site> / Gateways**.
- 2 Right-click a desired RAS Secure Client Gateway in the right pane and choose **Properties**.
- 3 Select the HTML5 tab and select or clear the **Allow file transfer command** option (at the bottom).

Client Policy Level

To enable or disable remote file transfer capabilities on a Client policy, do the following:

- 1 In the RAS Console, select the **Policies** category.
- 2 Right-click a desired policy in the right pane and choose **Properties**.
- 3 Select the **Connection Properties** item in the left pane.
- 4 Select the **Local Resources** tab in the right pane.
- 5 Select or clear the **Allow file transfer command** (at the bottom).

Parallels RAS Reporting

Parallels RAS Reporting Service is an optional component that allows Parallels RAS administrator to run and view predefined and custom Parallels RAS reports. Predefined reports include user and group activity, device information, session information, and application usage. You can also create custom reports using your own criteria. Read this chapter to learn how to install and configure Parallels RAS Reporting Service and how to use it.

In This Chapter

Installing Parallels RAS Reporting.....	233
Viewing Reports.....	236

Installing Parallels RAS Reporting

To use Parallels RAS Reporting, you need to install and configure Microsoft SQL Server and the RAS Reporting Service. This section contains installation requirements followed by RAS Reporting Service installation instructions.

Note: For more information and examples, please download the **Parallels RAS Reporting Service Guide** from the Parallels website: <https://www.parallels.com/products/ras/resources/>

Operating System Requirements

The RAS Reporting Service must be installed on a server running one of the following Windows Server versions:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

.NET Framework 4.5.2 must be installed.

User Account Requirements

To view RAS reports, a default AD user account will be created by the RAS Reporting Service installer. The account name is `RASREPORTINGVIEW`. You can specify a different user during the RAS Reporting Service setup if you wish.

Microsoft SQL Server Requirements

The following Microsoft SQL Server versions are supported:

- Microsoft SQL Server 2008 SP1
- Microsoft SQL Server 2008 R2 SP1
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016

The Microsoft SQL Server instance must have the following features installed:

- Database Engine Services
- Reporting Services - Native
- Management Tools

The SQL Server instance must be configured as follows:

- Must be a named instance. The default instance name and instance ID used by Parallels RAS Reporting Service is `RASREPORTING`. You can specify a different name, but you have to make sure that you use the same name when configuring the RAS Reporting Service (as described later in this section).
- The SQL Server administrators must include system administrator, AD administrator, "System" user.

SQL Server Reporting Services must be configured as follows:

- Report Server Web Service virtual directory must be set to `ReportServer_RASREPORTING`.
- Report Server Web Service TCP port must be set to 8085.
- Report Manager TCP port must be set to 8085.

Note: For installations running on a multi-server farm environment, it is recommended that Microsoft SQL Server is installed on a dedicated server.

Installing the RAS Reporting Service

To install the RAS Reporting Service:

- 1** Log in to the server running Microsoft SQL Server with an account that has administrative privileges (AD).
- 2** Download the latest version of the Parallels RAS Reporting Service from <https://www.parallels.com/products/ras/download/links/>
- 3** Once downloaded, double-click the `RASReporting-xxx.msi` file to run the installation wizard.
- 4** Click **Next** when prompted.
- 5** Review and approve the end-user license agreement and click **Next**.
- 6** Specify the target folder for the installation and click **Next**.
- 7** Specify the SQL Server instance name. The default instance name is `RASREPORTING`. If you would like to use a different instance, you can specify it on this page. If the instance doesn't exist, you need to create it first.
- 8** Specify the user account that will be used to view reports. The default user is `RASREPORTINGVIEW`. If you would like to use a different user, you can specify it on this page. If the user doesn't exist, you need to create it first.
- 9** Click **Install**.
- 10** When the installation is complete, click **Finish**.

Configuring RAS Reporting Service in the RAS Console

To configure the RAS Reporting Service:

- 1** Select the **Administration** category in the RAS Console and then click the **Reporting** tab in the right pane.
- 2** On the **Reporting** tab, specify the following options:
 - **Enable RAS Reporting:** Select this option to enable the RAS reporting functionality.
 - **Server:** Specify the FQDN or IP address of the server hosting your SQL Server database where the Reporting Service is installed.
 - **Port:** The port specified here is used by the service which receives data from the RAS Publishing Agent. The default port is 30008.
 - **Prompt user for login details.** Will prompt the user for AD credentials when generating reports.
 - **Use following credentials.** Specify AD username and password to be used each time a report is generated. The default user name is `RASREPORTINGVIEW`. If you specified a different user when you installed the RAS Reporting module, you can use it here.
- 3** When done, click the **Test connection** button to test the configuration.

Advanced Settings

Advanced settings allow the administrator to fine-tune the data collected by the reporting service and define for how long this data is retained before purged.

In the RAS Console, navigate to **Administration / Reporting**. On the **Reporting** tab, click the **Tracking Settings** button. The **Advanced Setting** dialog opens.

In the **Session Information** section, configure the following options:

- **Enable Tracking**. Records sessions data (affects all reports except Server Reports).
- **Retain information for**. Specify the period session information is retained for before purged.

In the **Server Counters** Information section, configure the following:

- **Enable Tracking**. Records server counter data (affects Server Reports only).
- **Retain information for**. Specify the period server counters information is retained for before purged.
- **Track CPU / Memory counter when change is more than**. Set the minimum CPU/Memory resource usage required to record data.

Viewing Reports

To view Parallels RAS reports, select the **Reporting** category in the RAS Console. The report viewing interface consists of the following elements:

- The middle pane displays the available reports. See the **Predefined reports** subsection below for the complete list. The "blue folders" icon (at the top of the list) groups reports by type or displays all of them as a single list. The "refresh" icon refreshes the report list by retrieving it from the database (this can be useful when you enable/disable the reporting functionality or when you add custom reports, which may not appear in the list automatically).
- When you initially open the **Reporting** category, the right pane contains just the **Information** tab, which informs you whether Parallels RAS Reporting is active.
- The "blue square" icon in front of the **Tasks** drop-down menu (upper right-hand side of the RAS Console) expands the reporting interface into full screen. The **Tasks** drop-down menu allows you to perform the following actions: **Duplicate** (duplicates a report tab), **Full screen** (on/off), various **Close Report** options, **Delegate Permissions** (allows you to grant permissions to view reports to other users).

To run a report, double-click it in the middle pane. The report opens in a tab in the right pane:

- Most reports include controls that you can interact with, such as **From/To** dates, **Sort By**, **Sort Order**, **Chart Type**, **Server Name**, and others depending on the report type. When you change a value in any of these controls, click the **View Report** button to apply the new criteria and re-run the report.

- The main report area (lower portion where the data is represented as a graph, text, or numbers) includes a menu bar with icons that allow you to change the view magnification, list through report pages (if more than one is included), search for text, save a report to a file, print a report, and export it to data feed.

Note: The first time the reports are viewed, you may be requested to add `http://<server domain/ IP>` as a trusted website. This will appear depending on the Parallels RAS machine's "Internet Explorer Enhanced Security Configuration".

Predefined reports

Parallels RAS Reporting Service includes a number of predefined reports in the following groups:

- 1 User Reports.** This group includes reports about how end users are interacting with Parallels RAS:
 - **User Activity** — shows all sessions produced by all users in the system. The report shows information about each session and includes active time, idle time, and disconnected time.
 - **User Session Activity** — shows all sessions produced by a single user. The report shows information about each session and includes active time, idle time, and disconnected time.
 - **Application Usage by User** — shows applications used by a specified user, including number of times used and total time.
 - **Devices Used by User** — shows information about devices used by a user. The report includes information such as device vendor, device model, and total time used.
 - **Client Operating System Used by User** — shows the operating system being used by a specified user.
 - **Full User Information** — shows detailed information about a specified user.
- 2 Group Reports.** These reports obtain information about how groups of users are interacting with Parallels RAS:
 - **Groups Activity** — shows all sessions produced by all groups in the system. The report includes active, idle, and disconnected time.
 - **Group Sessions Activity** — shows all sessions produced by a group in the system. The report shows information about each session produced by each user in the group and includes start, end, active, idle, disconnect and total time.
 - **Applications Used by Group** — shows applications used by a specified group, including number of times used and total time.
 - **Devices Used by Group** — shows information about devices used by users as members of a specified group. The report includes device vendor, model and total time used.
 - **Client Operating System Used by Group** — shows the operating system used by members of a particular group.
- 3 Devices Reports.** This group includes reports about the devices that are connecting to Parallels RAS:

- **Devices Used** — shows all devices using the system. The report includes a device manufacturer, model, and the number of sessions opened by the device.
- **Client Operating System Used** — shows devices and corresponding operating systems that are using the system.
- **Parallels Client Version Used** — shows information about a device model, Parallels Client version used, and session information.

4 **Server Reports.** This group includes reports about the activity of Parallels RAS server components:

- **Sessions Activity on Server** — shows the session activity of users on a particular server. Report includes start, end, active, idle and disconnect time.
- **Farm Health by Server** — shows server CPU and RAM usage for a specified server in the farm.
- **Farm Health by Machine** — shows server CPU and RAM usage for a specified computer.
- **Gateway Tunnelled Sessions** — shows tunneled session information for a specified Gateway.

5 **Application Reports.** Reports related to applications.

- **Applications Usage** — shows information about applications used in the system. Report includes information such as application name, number of times used and the total usage time. When viewing this report, select "All applications" or "RAS published applications" depending on your needs. When the second option is selected, the report will not include non-published applications and duplicates.

Note that if you have enabled the "custom reports" functionality (Administration > Reporting > Tracking settings > Enable custom reports), you will also see the custom reports group with a single demo report in it. As you add more custom reports, they will all appear in this folder. When the "custom reports" functionality is disabled, this group is NOT shown in the report list.

Custom reports are described in detail in the **Parallels RAS Reporting Service Guide**, which can be downloaded from the Parallels website. For quick how-to instructions, see the following KB article: <https://kb.parallels.com/en/124648>

Parallels RAS Performance Monitor

Parallels RAS Performance Monitor is a browser-based dashboard designed to help administrators analyze a Parallels RAS deployment bottlenecks and resource usage. The dashboard provides a visual display of performance metrics, which can be viewed in the Parallels RAS Console or in a web browser.

In This Chapter

Overview	239
Installing Parallels RAS Performance Monitor.....	240
Using Parallels RAS Performance Monitor	240
Configuring Performance Monitor Security	244

Overview

Components

Parallels RAS Performance Monitor consists of the following components:

- **InfluxDB database** — a database for storage of system performance data.
- **Grafana dashboard** — a browser-based dashboard providing a visual display of performance metrics.
- **Telegraf service** — a service that collects performance data on a server where it is installed. The service is installed automatically when you add a server to a Parallels RAS farm and install a corresponding RAS Agent on it (e.g. RAS Secure Client Gateway Agent, RD Session Host Agent, Remote PC Agent, etc.).

How it works

The Telegraf service is stopped by default, so it doesn't collect any data. To start the service on each server in the farm, the performance monitoring functionality must be configured and enabled in the Parallels RAS Console. Once enabled, the Telegraf service begins collecting a predefined set of performance counters at a fixed time interval (10 seconds). It then sends the collected data to the InfluxDB database for storage. To view performance metrics, the Parallels RAS administrator uses the dashboard (Grafana), which displays the visual representation of performance counters in real time.

The performance metrics are grouped in the dashboard by type (Session, CPU, Memory, Disk, etc.), so the administrator can view each group of metrics separately. The administrator can also select whether to view performance metrics for one or more specific servers or for all servers in the farm or site. In addition, the administrator can select a specific site for which the data should be displayed.

Installing Parallels RAS Performance Monitor

Requirements

Parallels RAS Performance Monitor can be installed on a dedicated server or on a server hosting any of the Parallels RAS components. The installation comes down to installing the InfluxDB database and the Grafana dashboard service, which is done automatically using the installation wizard as described in the **Installation** subsection below.

The server on which you'll be installing Parallels RAS Performance Monitor must have the following communication ports open:

- TCP port 8086 (used by the InfluxDB database).
- TCP port 3000 (used by the Grafana performance dashboard).

Installation

To install Parallels RAS Performance Monitor:

- 1** Download the Parallels RAS Performance Monitor installer from <https://www.parallels.com/products/ras/download/links/>
- 2** Run the installation wizard (the RASPerformanceMonitor.msi file) and follow the onscreen instructions.
- 3** Close the wizard when finished.

The next step is to configure access to Parallels RAS Performance Monitor in the RAS Console.

Using Parallels RAS Performance Monitor

Configure access to Parallels RAS Performance Monitor

To enable data collection and view the dashboard:

- 1** In the RAS Console, navigate to **Administration > Reporting**.
- 2** Select the **Enable RAS Performance Dashboard** option (the lower section of the tab page).

- 3 Enter the FQDN or IP address of the server where you have the InfluxDB database and Grafana dashboard installed.
- 4 Click **Apply** to commit the changes.

Once you perform the steps above, the Telegraf service is started on each server in the site and the data collection begins.

Open the dashboard

Note: You should give Parallels RAS Performance Monitor some time to collect performance data before you can view it (about 1 hour on initial installation).

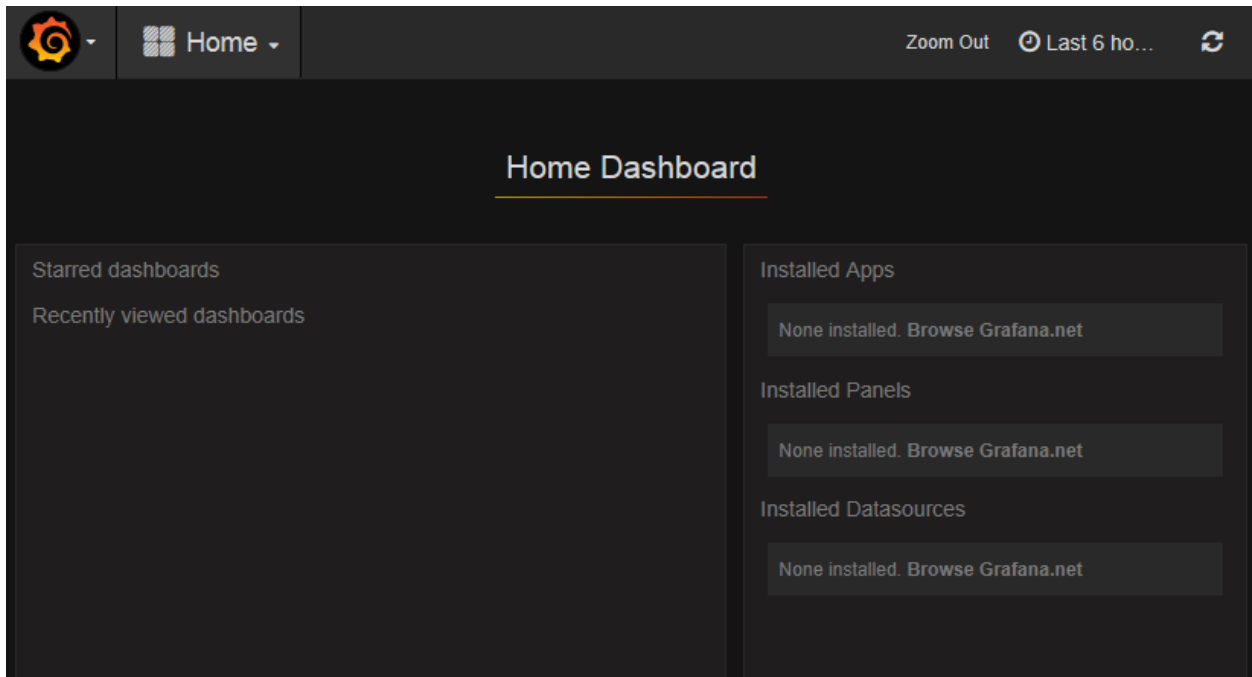
To view the dashboard, do the following:

- 1 In the RAS Console, select the **Monitoring** category.
- 2 The dashboard is displayed in the right pane of the console. The logon to the dashboard is performed automatically, so no logon credentials are required.

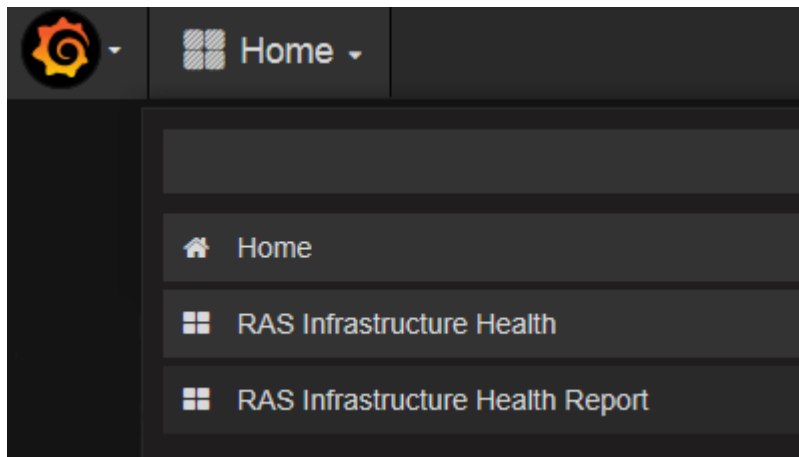
The buttons on the **Performance Monitoring Dashboard** tab (below the dashboard area) are as follows:

- **Home.** Displays the **Home Dashboard** page. The button is useful when you click on an external link in the dashboard, which may take you to an external web page.
- **Refresh.** Reloads the current page.
- **Open in browser.** Opens the performance dashboard in a web browser.

When you open the dashboard for the first time, the **Home Dashboard** page is displayed.



To view performance metrics, click the **Home** drop-down menu at the top of the dashboard and then click **RAS Infrastructure Health**.



This will open the page displaying performance metrics (please note that the other menu item, RAS Infrastructure Health Report, is for internal use only and should be ignored).

The menu bar on the **RAS Infrastructure Health** page includes the following items:

- **Hosts.** Allows you to select one or multiple servers for which the performance metrics should be displayed. To display the data for all servers in the site, select **All**. Please note that if you don't see any servers in the list, you need to wait for Parallels RAS Performance Monitor to collect the initial set of statistics. This only happens on initial installation.

- **Instance.** This item allows you to select a specific counter instance (if there's more than one). For Network counters it is usually the name of a network interface. For Disk counters it is a disk name. Other types of counters don't usually have multiple instances.
- **Site.** Select a site for which to display the data. Selecting **All** displays the data for all sites in the farm. If you have another RAS farm, and the RAS Performance Monitor is configured and enabled in it, you can also select a site from that farm.
- **Agent Type.** Select a RAS agent type.
- **Groups.** Select an RDS group.

To view metrics of a specific type, expand the desired category in the main area of the dashboard. The categories include:

- **Session Information.** Displays the information about active sessions (act_sess) and disconnected sessions (disc_sess).
- **CPU usage.** CPU counters.
- **Free memory.** Physical memory counters.
- **Disk usage.** Disk I/O counters.
- **Network usage.** Network interface I/O counters.
- **System information.** System information counters.

Performance metrics are displayed in the dashboard as a graph. Different counters are displayed using different colors. The legend is displayed below the graph.

To zoom in on a particular area of a graph, select a rectangular block with a mouse. You can also use the **Zoom** controls at the top of the dashboard for time range zoom out, shift time forward, or shift time backwards.

To select a specific time range, click the "clock icon" item at the top and then specify a time range or select one from the **Quick ranges** list.

To go the **Home Dashboard** page, click the **Home** drop-down menu and choose **Home**. If you are viewing the dashboard in the Parallels RAS Console, you can also click the **Home** button in the console itself.

For more information about performance metrics and their meaning, please refer to the following articles from Microsoft:

- <https://technet.microsoft.com/en-us/library/cc976785.aspx>
- <https://technet.microsoft.com/en-us/library/2008.08.pulse.aspx>

See also **RAS Performance Counters** (p. 296).

Configuring Performance Monitor Security

By default, any user can access the Performance Monitor page and view the the performance matrix. You can set up RAS Performance Monitor to use credentials, so that only authorized users can view it.

First, remove anonymous authentication from the Grafana configuration file as follows:

1 Open file C:\Program Files (x86)\Parallels\RAS Performance Monitor\conf\defaults.ini.

2 In the file, look for the following:

```
##### Anonymous Auth
#####

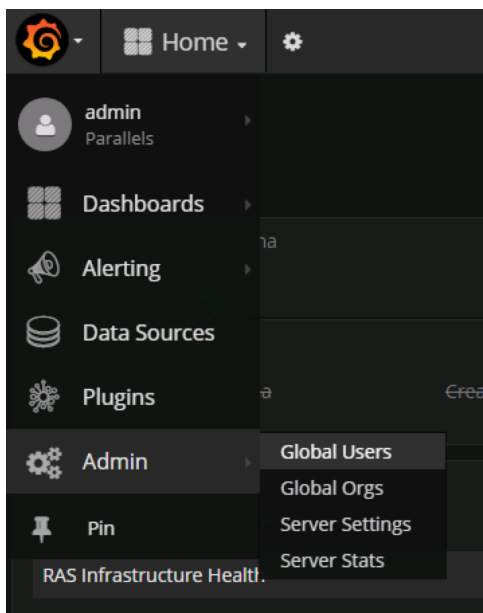
[auth.anonymous]
# enable anonymous access
enabled = true
```

3 Change "enabled = true" to "enabled = false".

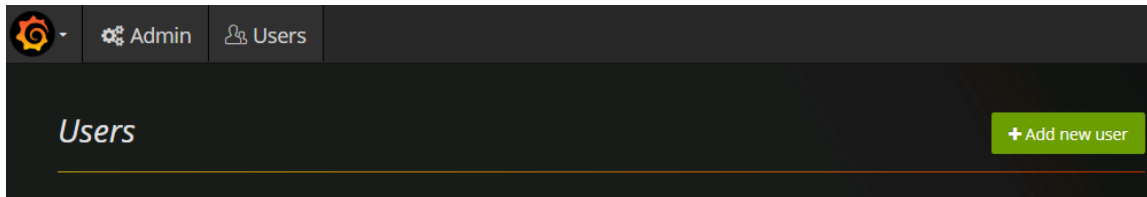
Restart the Grafana service and log in to Grafana console as follows:

- **URL:** <http://yourserver:3000/login?redirect=%2Fdashboard%2Fdb%2Fras-infrastructure-health>
- **User:** admin
- **Password:** admin

Once logged in, go to the Users admin page:



Click on **Add new user**:



Add a users by specifying the account name, email address, username and password, and click **Create**:

A screenshot of the 'Add new user' form. The form has a title 'Add new user' and four input fields: 'Name', 'Email', 'Username', and 'Password'. A green 'Create' button is located at the bottom left of the form.

You know need to add the user to your organization's list. To do so, in the **Users** list, click **Edit** to edit the user and then set the organization and make the user a **Viewer**:



Click **Add** to add the user to your organization's list. The user can now view the RAS Performance Monitor statistics.

Connection and Authentication Settings

A Parallels RAS administrator has the ability to customize how users connect to Parallels RAS. This chapter describes connection and authentication settings that can be configured according to your organization requirements. It then explains how to use second level authentication for even higher level of security.

In This Chapter

RAS Publishing Agent Connection Settings.....	246
Remote Session Settings.....	247
Restricting Access by Parallels Client Type and Build Number	249
Second Level Authentication.....	249

RAS Publishing Agent Connection Settings

RAS Publishing Agent connection settings can be accessed from the **Connection** category.

Choosing Authentication Type

Select the **Authentication** tab page. In the **Authentication Type** drop-down list, select one of the following options:

- **Username/Password.** The user credentials are validated by the Windows system on which RAS is running. The credentials used for Windows authentication are also used to log into an RDP session.
- **Smart Card.** Uses smart card authentication. Similar to Windows authentication, smart card credentials can be shared between both RAS and RDP. Hence, smart card credentials only need to be entered once. Unlike Windows authentication, the user only needs to know the smart card's PIN. The username is obtained automatically from the smart card, so the user doesn't need to provide it.
- **Username/Password or Smart Card.** Uses both Windows and smart card authentication.

Note that if smart card authentication is disabled, RAS Publishing Agent will not hook the Local Security Authority Subsystem Service (LSASS).

Smart card support is available on Windows Server 2008 and newer. Smart card authentication can be used in Parallels Client for Windows, Mac, and Linux.

Enforcing Authentication

By default, all users are required to authenticate the connection against Parallels RAS before even viewing the list of the available published applications or desktops. By disabling the option **Always require user credentials for application list** on the **Authentication** tab page you can allow users to see the list of published resources without being authenticated. As a result, the user will be able to see the list, but as soon as the user tries to open an application or a desktop, the server will ask to supply credentials.

Configuring Authentication

Once authentication is enforced, you can configure Parallels RAS to authenticate users against a specific domain by entering the domain name in the **Domain** input field.

- **All Trusted Domains.** If the information about users connecting to Parallels RAS is stored in different domains within a forest, select the **All Trusted Domains** option to authenticate against multiple domains.
- **Use client domain if specified.** If this option is cleared, the domain name specified by the administrator will be automatically populated in Parallels Client.
- **Force clients to use NetBIOS credentials.** If this option is selected, the Parallels Client will replace the username with the NetBIOS username.

Note: If a certificate on your smart card does not contain a user principal name (UPN) in the "Subject Alternative Name" (SAN) field (or if it doesn't have the "Subject Alternative Name" field at all) you have to disable the **Force clients to use NETBIOS credentials** option.

Recommendation: After changing the domain names or some other authentication related changes, click the **Clear cached session IDs** button on the **Settings** tab page.

Authenticating Against Non Domain Users

In order to authenticate users sessions against users specified on a standalone machine you must enter the [workgroup_name] / [machine_name] instead of the domain name. For example if you would like to authenticate users against a list of local users on a machine called SERVER1 that is a member of the workgroup WORKGROUP, enter the following in the domain field: WORKGROUP/SERVER1.

Remote Session Settings

The **Settings** tab in the **Connection** category allows you to configure the following remote session options:

- **Declare remote session idle after:** This option affects reporting statistics, whereby a session is declared idle after the amount of time specified without any activity.

- **Automatically logoff RAS idle session after:** Specifies the time period after which an idle session (a user RAS connection) should be logged off. Once the session is logged off, the user is disconnected from Parallels RAS and is presented with the **Connections** dialog in Parallels Client as a way to notify them that they were logged off. They can use the dialog to log back on if desired.
- **Cached Session Timeout:** Specify the amount of time that a session is cached for (higher amount of time reduces AD transactions).
- **Clear cached session IDs:** Clears all cached session information.

FIPS 140-2 encryption

The **FIPS 140-2 encryption** property allows you to specify whether FIPS-encrypted connections are allowed or even enforced on RAS Secure Client Gateways. When you allow (or enforce) the encryption, the Gateways will use the FIPS 140-2 encryption module. You can choose from the following options:

- **Disabled.** FIPS 140-2 encryption is disabled on RAS Secure Client Gateways.
- **Allowed.** RAS Secure Client Gateways accept both FIPS-encrypted and non-FIPS-encrypted connections.
- **Enforced.** RAS Secure Client Gateways accept FIPS-encrypted connections and will drop any non-FIPS-encrypted connection.

Note: For FIPS 140-2 encryption to work, a FIPS compliant certificate must be installed on each RAS Secure Client Gateway.

When you enable FIPS 140-2 encryption, the encryption status is displayed on the **Information / Site Information** tab in the RAS Console. Look for the **Encryption** property of a RAS Secure Client Gateway.

The following versions of Parallels Client support FIPS 140-2 encryption:

- Parallels Client for Windows 64-bit
- Parallels Client for Linux 64-bit

Please note that HALB is not supported when using a FIPS-encrypted connection.

By default, the values on the **Settings** tab are replicated to all sites in a Parallels RAS farm (the **Replicate settings** option in the lower right corner is enabled). If you would like to have these settings defined differently for different sites, clear the **Replicate settings** option in all sites and then set the options for each site individually.

Restricting Access by Parallels Client Type and Build Number

You can specify a minimum requirement for the Parallels Client type and version number in order for it to connect to the Parallels RAS farm or to list published resources.

To specify Parallels Client requirements:

- 1 In the RAS Console, select the **Connection** category and click the **Allowed Devices** tab.
- 2 In the **Mode** drop-down list, select from the following options:
 - **Allow all clients to connect to the system.** No restrictions. All Parallels Client types and versions are allowed full access.
 - **Allow only the selected clients to connect to the system.** Allows you to specify Parallels Client types and versions that are allowed to connect to the Parallels RAS farm. Select the desired Parallels Client types in the **Clients** list. To set the **Minimum build** value, right-click the client type and choose **Edit**. Type the version number directly in the **Minimum build** column.
 - **Allow only the selected clients to list the published items.** Allows you to specify Parallels Client types and versions that can list published resources. Compared to the option above, this one does not restrict Parallels Clients connecting to Parallels RAS. Select this option and then select the desired Parallels Client types in the **Clients** list. To set the **Minimum build** value, right-click the client type and then click **Edit** in the context menu. Type the version number directly in the **Minimum build** column.

If a restriction is configured and a Parallels Client is excluded from the list, the user running it will receive a corresponding error message and will be advised to contact the system administrator.

Second Level Authentication

Parallels RAS allows you to use two-factor authentication for access control by configuring a second level authentication. When second level authentication is used, users will have to authenticate through two successive stages to get the application list. While the first level will always use native authentication (Active Directory / LDAP), the second level can use one of the following solutions:

- Azure MFA server (RADIUS)
- Duo (RADIUS)
- FortiAuthenticator (RADIUS)
- TekRADIUS
- RADIUS (p. 250)

Connection and Authentication Settings

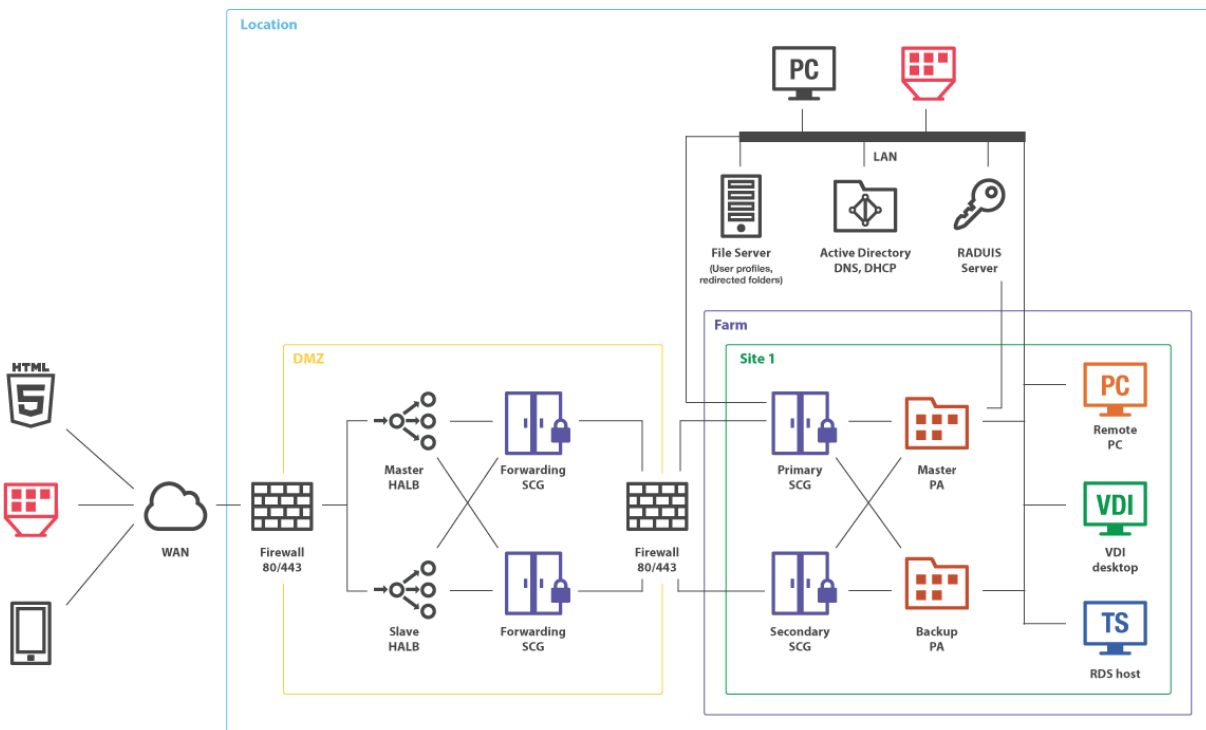
- Deepnet
- SafeNet (p. 267)
- Google Authenticator

Second level of authentication is more secure because instead of using a standard user name and password, it uses a static user name and a one-time password generated by a token.

Second Level Authentication can be configured in the Parallels RAS Console in **Connection / Second Level Authentication**.

Using RADIUS

The below diagram shows a typical Parallels RAS scenario with RAS Publishing Agent connected to a RADIUS server.



To configure RADIUS properties:

- 1 In the Parallels RAS Console, navigate to **Connection / Second Level Authentication**.
- 2 In the **Provider** drop-down list, select a RADIUS solution that you use in your organization. The following options are available:
 - Azure MFA server (RADIUS)
 - Duo (RADIUS)

- FortiAuthenticator (RADIUS)
- TekRADIUS
- RADIUS

Note: For specifics about configuring some of the solutions, please read corresponding subsections at the end of this section.

- 3** Click the **Settings** button. In the dialog that opens, select the **Connections** tab and specify the following options:
 - **Type Name:** Specify the name of the OTP connection type that will be displayed on the Logon screen on the client side. This should be the name that your users will clearly understand.
 - **Server:** Enter the hostname or IP address of your RADIUS server.
 - **Port:** Enter the port number for the RADIUS Server. Click the **Default** button to use the default value.
 - **Timeout:** Specify the packet timeout in seconds.
 - **Retries:** Specify the number of retries when attempting to establish a connection.
 - **Secret Key:** Type the secret key.
 - **Password Encoding:** Choose from PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol), according to the setting specified in your RADIUS server.
- 4** Click the **Check connection** button to validate the connection. If the connection is configured correctly, you will see a confirmation message.
- 5** Select the **Forward username only to RADIUS server** as required.
- 6** Select the **Forward the first password to Windows authentication provider** option to avoid a prompt to enter the password twice (RADIUS and Windows AD). Note that for Azure MFA server, this option is always enabled and cannot be changed.
- 7** Please also read a note at the bottom of the dialog (if available) suggesting a certain setting specific for your RADIUS solution.
- 8** If your RADIUS solution requires configuring attributes, click the **Attribute** tab and then click **Add**. In the dialog that opens, specify the following:
 - In the **Vendor** drop-down list, select a vendor.
 - In the **Attribute** list, select a vendor attribute.
 - In the **Value** field, enter a value for the selected attribute type (numeric, string, IP address, date, etc).
- 9** Click **OK** and then click **OK** again to close all dialogs.

Configuring Azure MFA

Depending on the user location there are four scenarios for the cloud MFA service:

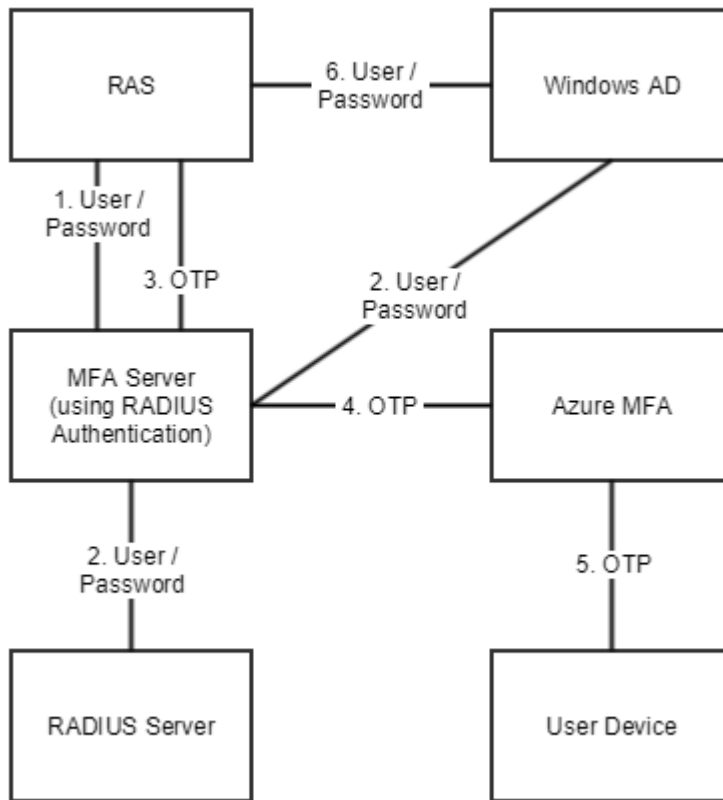
User Location	MFA in the cloud	M FA Server
Azure Active Directory	Yes	
Azure AD and on-premises AD using federation with AD FS (is required for SSO)	Yes	Yes
Azure AD and on-premises AD using DirSync, Azure AD Sync, Azure AD Connect - no password sync	Yes	Yes
Azure AD and on-premises AD using DirSync, Azure AD Sync, Azure AD Connect - with password sync	Yes	
On-premises Active Directory		Yes

An Azure account with Global Administrator role is required to download and activate MFA Server. Syncing with Azure AD (via AD Connect) or a custom DNS domain aren't required to setup an MFA Server which runs exclusively on-premises.

Users need to be imported into MFA Server and be configured for MFA authentication.

Parallels RAS authenticates users with MFA Server using the RADIUS second level authentication provider. MFA Server thus needs to be configured to allow RADIUS client connections from the RAS server.

The authentication process goes through the following stages:



In stage 2 the user can be authenticated using either RADIUS or Windows AD. A prompt to enter the credentials twice (in stage 1 and 6) is avoided by enabling the option to forward the password.

Configuring DUO

For instructions on how to configure Parallels RAS with DUO RADIUS, please read the following Parallels KB article: <https://kb.parallels.com/124429>

Using Deepnet

This section describes how to configure and use Deepnet for second level authentication.

In this section:

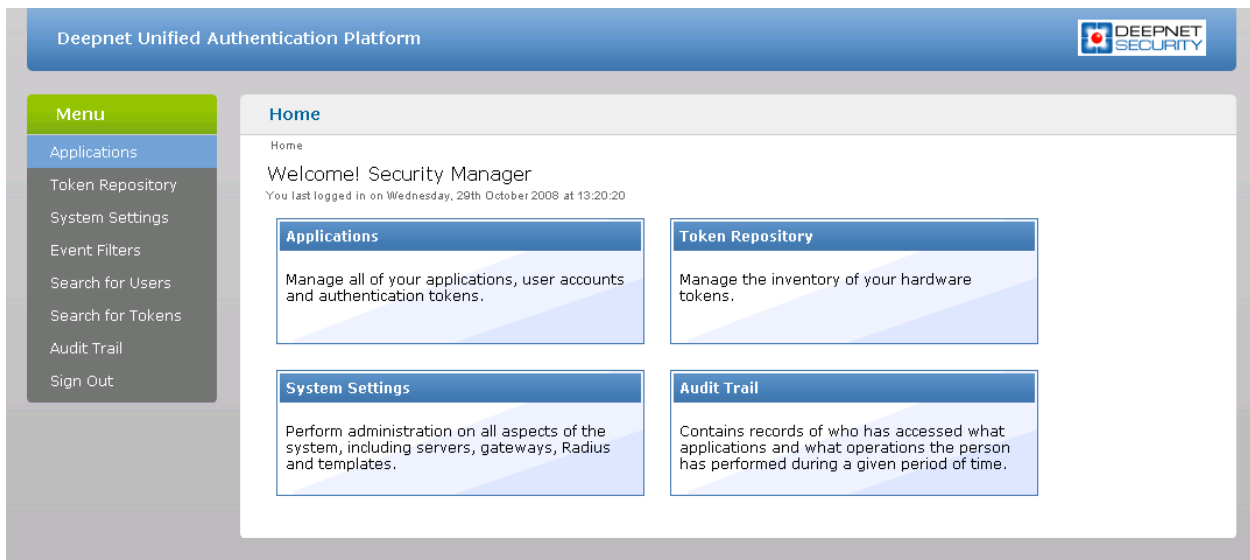
- Configuring Deepnet (p. 254)
- Configuring Parallels RAS for Deepnet (p. 257)
- Creating User Accounts on Deepnet (p. 258)
- Connecting to a RAS Farm with Deepnet (p. 259)

- Working with DualShield (p. 260)

Configuring Deepnet

Start by logging into the machine where Deepnet Unified Authentication is installed and open your Internet browser. Since Deepnet is installed locally, use 'localhost' as the URL followed by the port number which the Deepnet server will use to communicate with your applications (ex: <http://localhost:8080/>).

You must then log into the Deepnet Management Console with the credentials that you had set during the installation.



Servers

Ensure that the Communication Server, Connection Server and Authentication Server are properly configured. For further information please refer to Deepnet Unified Authentication Platform Administration Guide.

Deepnet Unified Authentication Platform

DEEPNET SECURITY

Menu

- Applications
- Token Repository
- System Settings
- Event Filters
- Search for Users
- Search for Tokens
- Audit Trail
- Sign Out

Connection Server Settings

Home > System Settings > Connection Server

Connection Configuration

External

Server Address: *

Server Port: *

Use SSL:

Internal

Server Address: *

Server Port: *

Use SSL:

Save Cancel

RAS Publishing Agent will communicate with the Authentication Server. It is highly recommended to have this behind a Firewall for security reasons. Make sure that the **Server Address** and **Server Port** are correct.

Gateways

Email or SMS Gateways must be configured correctly so that the Deepnet server is able to send information, such as Activation codes, to the users.

Deepnet Unified Authentication Platform

DEEPNET SECURITY

Menu

- Applications
- Token Repository
- System Settings
- Event Filters
- Search for Users
- Search for Tokens
- Audit Trail
- Sign Out

Email Gateway Settings

Home > System Settings > Email Gateway Settings

SMTP Server Address: *

SMTP Server Port:

Requires Authentication:

Transport Layer Security (TLS):

User Name:

Password:

Save Cancel

The E-Mail Gateway and/or SMS Gateway must be configured to be able to send messages to the user. Enter the **SMTP Server Address** and **SMTP Server Port** of the server which will be used by the Deepnet Unified Authentication to send e-mails. Remember to enter any username or password used for the SMTP server.

Templates

Templates are used to set the structure of e-mails and SMS messages sent by the server. The SMS template allows you to set the text for the **Sender** field, the message content and an optional subject. Make sure that you use the preset wildcards to send unique information such as the One-Time Password ([[OTP]]).

Deepnet Unified Authentication Platform

DEEPNET SECURITY

Menu

- Applications
- Token Repository
- System Settings
- Event Filters
- Search for Users
- Search for Tokens
- Audit Trail
- Sign Out

Send One-time Password Templates

Home > System Settings > OTP Template

SMS Template SMTP Template

From: admin@company.com *

Subject: One-Time Password *

Body:

(for One-Way OTP)

Your one-time password: [[OTP]] *

(for Two-Way OTP)

Your one-time password: [[OTP]] *

Server one-time password: [[SOTP]] *

Format: HTML Plain Text

Priority: Low Mid High

Note: Use the following wildcards:

- [[OTP]] : User's One-Time Password
- [[SOTP]] : Server's One-Time Password

Save Cancel

The E-mail template allows you to set the e-mail address that the user can reply to. This should be set to the administrator's e-mail. You can also set the e-mail's **Subject**, **Priority** and **Format**. The **Body** contains the actual content of the e-mail which should include the preset wildcard for the unique information along with a message.

Applications

Deepnet Unified Authentication Platform

DEEPNET SECURITY

Menu

- Applications
- Token Repository
- System Settings
- Event Filters
- Search for Users
- Search for Tokens
- Audit Trail
- Sign Out

New Application

Home > Application > New

Icon	<input type="text"/>	Browse...
Name	VirtualDesktopServer	*
Description	<input type="text"/>	
ID	001	*
Service URL	http://deepnet:8081/dcs/service	
Application URL	<input type="text"/>	
Primary	<input type="checkbox"/>	
Connect to LDAP	<input type="checkbox"/>	

Save Cancel

Click on **New** to add a new application. From the new form that loads you only need to set a **Name** and an **ID**. Once this is done, click **Save** to save your settings.

Token Repository

If using hardware tokens such as SafelD the token information must first be imported using the XML file provided. Click on **Import** and browse for the XML file provided. After the XML file has been imported each hardware token must be assigned to a user.

Configuring Parallels RAS for Deepnet

List of Supported Tokens

- SafelD
- FlashID
- MobileID
- QuickID
- GridID
- SecureID (RSA)
- DigiPass (Vasco)

Connect to Deepnet Unified Authentication

- 1 In the RAS Console, select the **Connection** category and then click the **Second Level Authentication** tab.

- 2** In the **Provider** drop-down list, select **Deepnet** and click the **Settings** button. The **Deepnet Properties** dialog opens.
- 3** On the **Connection** tab, enter the server name and port that you saved while setting up your Authentication Sever. By default, the port number is set to 8080. Click on **Check Connection** to test that your Authentication Server can be reached. You can choose to connect over SSL to your Deepnet server.
- 4** Click the **Application** tab.
- 5** Select the application profile that will use Deepnet to authenticate its users. You can also create an application which will be added on the Deepnet server.
- 6** The **Default Domain** field enables you to choose the default domain user for authentication and when users are added. Any Deepnet user accounts imported or verified will be done so using this default domain.
- 7** Select the **Use LDAP** option when importing Deepnet user accounts and a group that contains other sub-groups.
- 8** Click the **Import Deepnet user accounts...** button to automatically add the specified users/groups to the Deepnet application.
- 9** Click the **Verify Deepnet user account names** button to check that all users in the Deepnet application are in the following format: `\\domain\username`. Users added in the format of `username@domain` will be automatically changed to the appropriate format and users without a domain will have the default domain assigned to them.
- 10** Click the **Authentication** tab.
- 11** In the **Mode** drop-down list, select the mode how you want your users to be authenticated:
 - **Mandatory for all users** means that every user using the system must log in using two-factor authentication.
 - **Create token for Domain Authenticated Users** will allow Parallels RAS to automatically create software tokens for Domain Authenticated Users. Choose a token type from the drop down list. Note that this option only works with software tokens.
 - **Use only for users with a Deepnet account** will allow users that do not have a Deepnet account to use the system without having to log in using two-factor authentication. Note that if a user has a Deepnet account, but the account is configured as not required to use 2FA, the AD authentication will be used instead.
- 12** In the **Allow Channels** section, you can specify what channels are available to the user to activate the token or when requesting a Quick ID OTP. For example, if you select **Email**, the activation code can be sent only via email. If you select **SMS**, the activation code is sent via SMS.

Creating User Accounts on Deepnet

When adding new user accounts on Deepnet, it is important that the domain name is included with the **Login Name** of the user, therefore the entry should be in the following format:
`\\domain\username`.

Users created automatically by Parallels applications are already in that format but users imported from the Deepnet console must be corrected.

To correct the usernames:

- 1 Open the **Deepnet Properties** dialog (**Connection > Second Level Authentication > Settings**).
- 2 Select the **Application** tab.
- 3 Click the **Verify Deepnet user account names** button.

Note that users added in the format of username@domain will be automatically changed to the appropriate format (\\domain\username).

Connecting to a RAS Farm with Deepnet

Parallels Client

Once Deepnet is enabled, the users will have two-factor authentication. If using software tokens such as QuickID the administrator does not have to create a token for each user. RAS Publishing Agent will automatically create the token when the user tries to log in for the first time.

When a user tries to access a Parallels Connection from Parallels Client, he/she is first prompted for the Windows username and password. If the credentials are accepted, RAS Publishing Agent will communicate with the Deepnet server to create a unique token for that user.

The token then needs to be activated. Click on a button to send the activation code by e-mail or by SMS depending on the channel selected when configuring Authentication section. A message will then be sent containing the token activation code which will need to be inserted in the **Activation code** text box.

If using MobileID or FlashID, an email about where you can download the appropriate software will be sent to the user.

If using QuickID tokens, the application will ask for a One-Time Password which is sent by e-mail or SMS.

If using a GridID, the user is given the opportunity to print the grid from the client itself. Note that this is only available the first time the user logs on.

Parallels Web Portal

If Deepnet Unified Authentication is enabled, logging into Parallels Web Portal also requires Second-Level Authentication.

Working with DualShield

DualShield 5.6+ Authentication Platform

This section explains how to integrate Deepnet DualShield Authentication Platform 5.6 or higher with Parallels RAS 10.6 or higher. If using any other version prior to the stated version please use RADIUS interface.

You may also read the following documentation on DualShield Authentication Platform:

- 1 DualShield Authentication Platform – Installation Guide
- 2 DualShield Authentication Platform – Quick Start Guide
- 3 DualShield Authentication Platform – Administration Guide

List of Supported Tokens by Parallels RAS

MobileID (FlashID is not integrated with MobileID)

- 1 QuickID
- 2 GridID
- 3 SafeID
- 4 SecureID (RSA)
- 5 DigiPass (Vasco)

If using hardware tokens such as SafeID the token information must first the XML file provided. Click on 'Import' and browse for the XML file provided. After the XML file has been imported each hardware token must be assigned to a user.

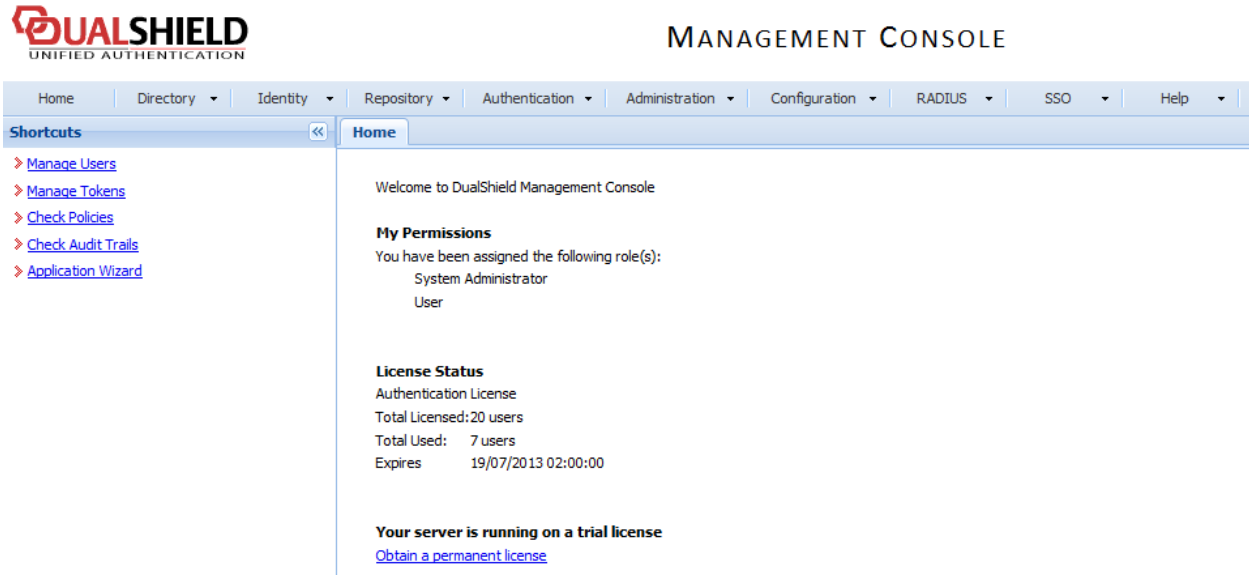
In this section:

- Configuring DualShield 5.6+ Authentication Platform (p. 260)
- Configuring Parallels RAS to Use DualShield Authentication Platform (p. 264)
- Connect to a RAS Farm (p. 266)
- Parallels Web Portal (p. 267)

Configuring DualShield 5.6+ Authentication Platform

After following all the specified steps in “DualShield Authentication Platform – installation Guide” a URP is automatically opened on your internet browser ([http:// LOCALHOST:8073](http://LOCALHOST:8073)) which allows you to logon to the Management Console of DualShield.

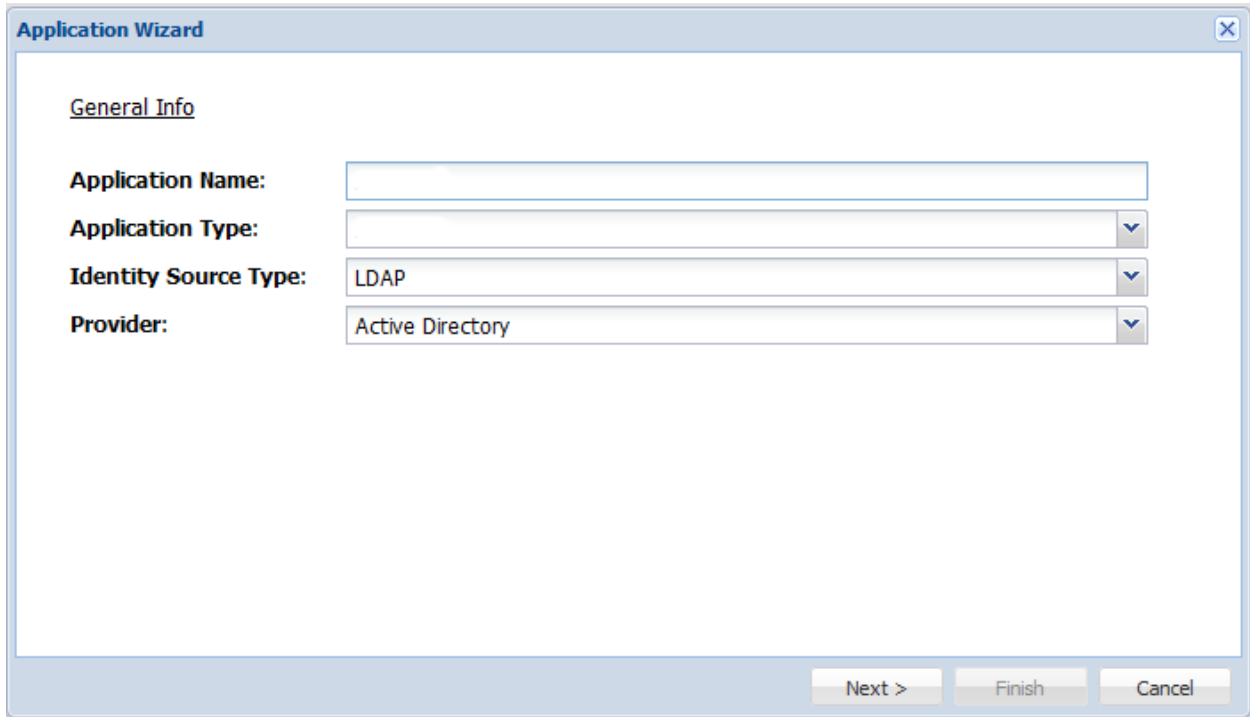
Login in to the DualShield Management Console with the default credentials (User: sa, Password: sa). You will be prompted to change the default password.



Applications are set to provide a connection to realm, as the realm contains domains of users who will be allowed the access to the application.

Realm is set for multiple domain users to be able to access the same application.

You need to create an Application which Parallels RAS will communicate with. Click on **Authentication > Application Wizard** and enter the information shown below and press **Next**.

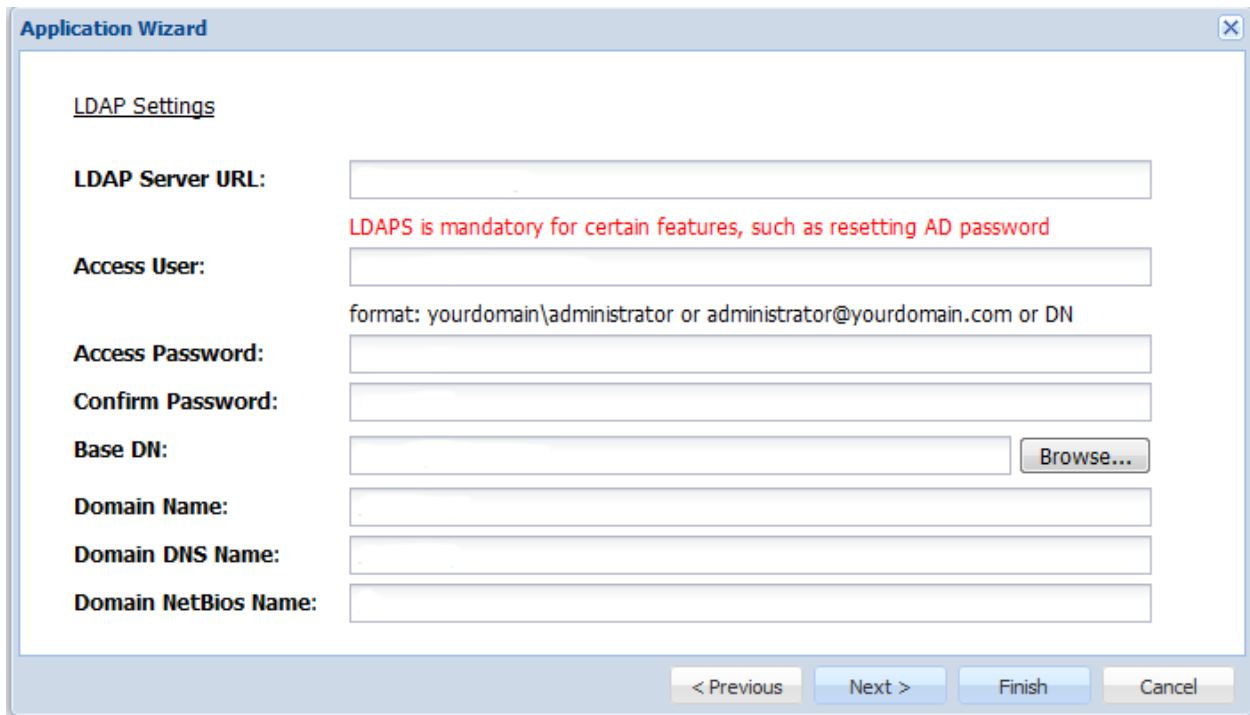


The screenshot shows the 'Application Wizard' dialog box with the 'General Info' tab selected. The fields are as follows:

Application Name:	<input type="text"/>
Application Type:	<input type="text"/>
Identity Source Type:	LDAP
Provider:	Active Directory

At the bottom right, there are three buttons: 'Next >', 'Finish', and 'Cancel'.

Specify the LDAP Server settings as shown below and press **Finish**.



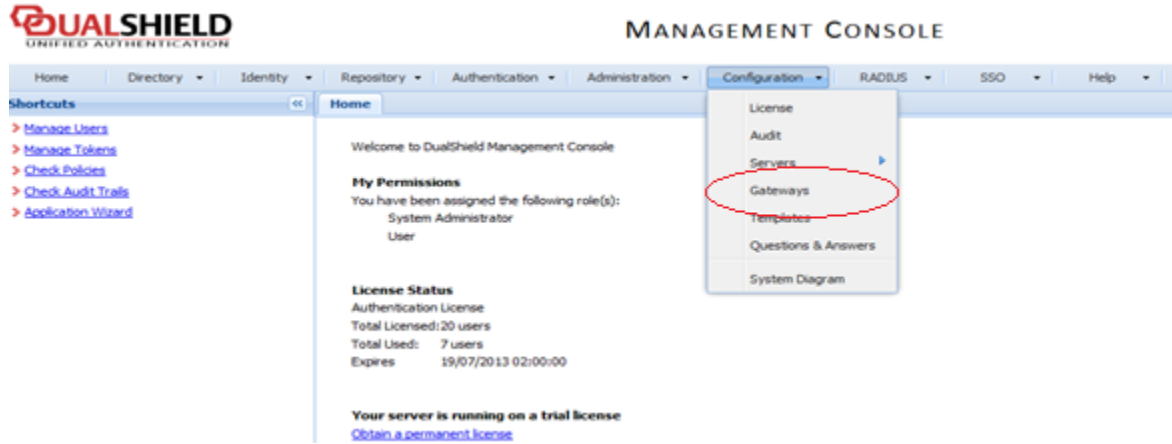
The screenshot shows the 'Application Wizard' dialog box with the 'LDAP Settings' tab selected. The fields and text are as follows:

LDAP Server URL:	<input type="text"/>
Access User:	<input type="text"/>
Access Password:	<input type="password"/>
Confirm Password:	<input type="password"/>
Base DN:	<input type="text"/> <input type="button" value="Browse..."/>
Domain Name:	<input type="text"/>
Domain DNS Name:	<input type="text"/>
Domain NetBios Name:	<input type="text"/>

Below the 'Access User' field, there is a red text note: "LDAPS is mandatory for certain features, such as resetting AD password". Below that, there is a format instruction: "format: yourdomain\administrator or administrator@yourdomain.com or DN".

At the bottom right, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

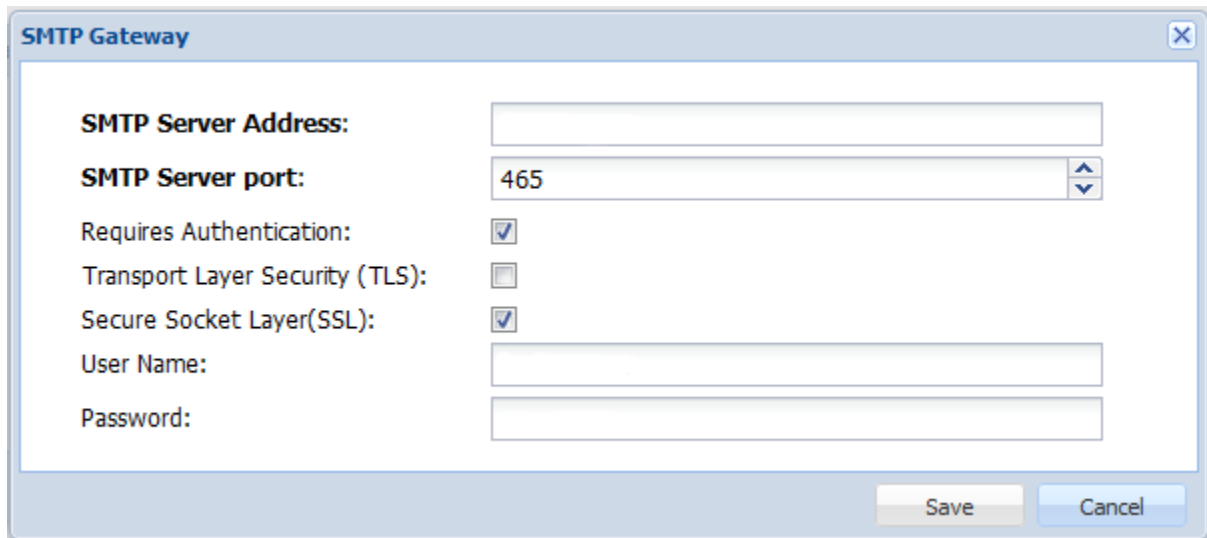
After you have configured the application you need to configure an Email or SMS gateway which are used by DualShield server to communicate with the end user. In this document we will be using an Email gateway. Select Gateways from the Configuration menu.



Configure your email gateway.

The image shows a dialog box titled 'Message Gateway -- Edit'. It contains several fields and controls: 'Type:' is a dropdown menu set to 'EMAIL'; 'Name:' is an empty text input field; 'Description:' is an empty text input field; 'Configuration:' is a button labeled 'Edit...'; 'Domains:' is a dropdown menu; 'Enable:' is a checked checkbox. At the bottom right are 'Save' and 'Cancel' buttons.

Click **Edit** to enter your SMTP server information



The screenshot shows a dialog box titled "SMTP Gateway" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- SMTP Server Address:** A text input field.
- SMTP Server port:** A spin box containing the value "465".
- Requires Authentication:** A checked checkbox.
- Transport Layer Security (TLS):** An unchecked checkbox.
- Secure Socket Layer(SSL):** A checked checkbox.
- User Name:** A text input field.
- Password:** A text input field.

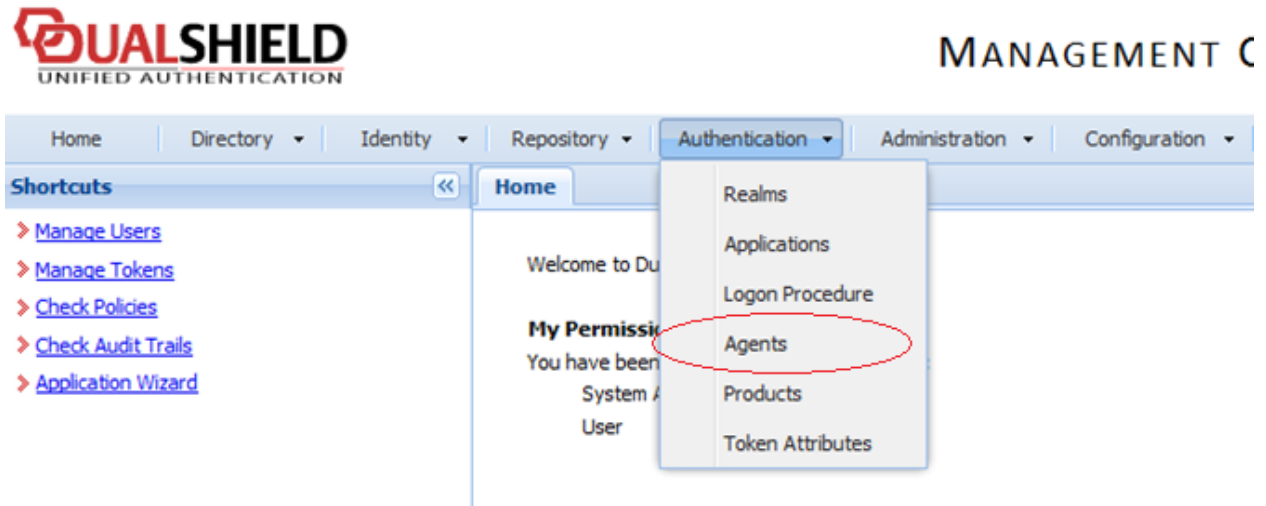
At the bottom right of the dialog, there are two buttons: "Save" and "Cancel".

Configuring Parallels RAS to Use the DualShield Authentication Platform

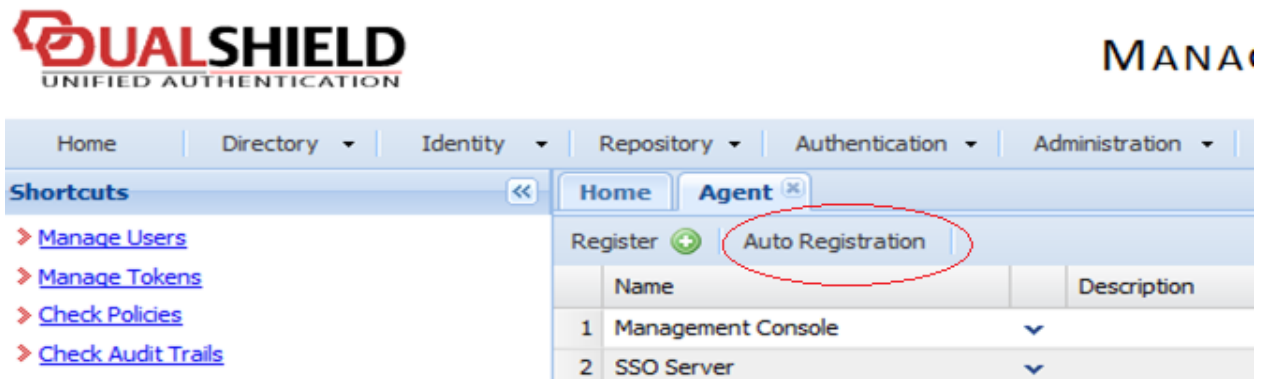
To begin:

- 1 In the RAS Console, navigate to the **Connection / Second Level Authentication** tab.
- 2 In the **Provider** drop-down list, select **Deepnet**.
- 3 Click the **Settings** button.
- 4 Click the **Check Connection** button to test that the authentication server can be reached and to verify that the RAS Console is registered as a DualShield agent. If you see the "DeepNet server not valid" message, you have either specified an incorrect server information or you need to allow auto registration of the Parallels components as a DualShield agent.

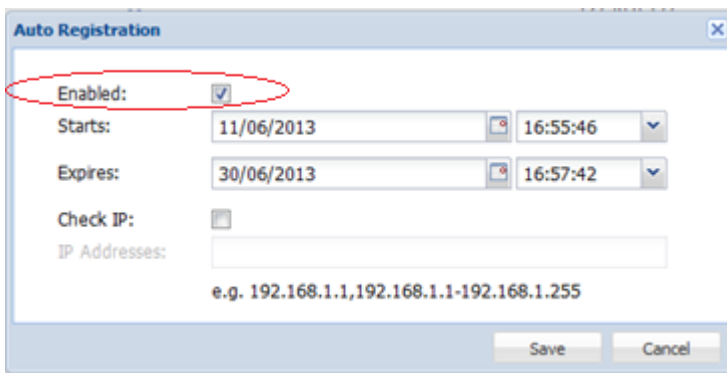
- Go back to the DualShield Management Console and select **Agents** from the **Authentication** menu as shown below.



- Select **Auto Registration**.



- Select the **Enabled** option and set the date range.



- Once the Agent Auto Registration is set, go back to the RAS Console and select **Yes**. You should see a message that the Dual Shield agent has been successfully registered.

Please note that All RAS Publishing Agents must be registered with Deepnet DualShield server. If you are using secondary Publishing Agents, you need to close all open windows until you can press **Apply** in the RAS Console. This will inform all the agents to self-register as DualShield agents.

- 9 In the Deepnet Properties dialog, click the **Applications** tab and browse for the Application name previously created from the DualShield Management Console.
- 10 Click the **Authentication** tab and select how you want your users to be authenticated:
 - **Mandatory for all users** means that every user using the system must log in using two-factor authentication.
 - **Create token for Domain Authenticated Users** will allow Parallels RAS to automatically create software tokens for Domain Authenticated Users. Choose a token type from the drop down list. Note that this option only works with software tokens, such as QuickID and MobileID
 - **Use only for users with a DualShield account** will allow users that do not have a DualShield account to use the system without have to login using two-factor authentication.
- 11 Go back to the **Connection > Second Level Authentication** tab.
- 12 In the Exclusion section, specify the exclusion rules:
 - **User / Group exclude list** allows you to add users or groups within your active directory that will be excluded from using DualShield Authentication.
 - **Client IP exclude list** allows you to add IP addresses or a range of IP addresses that will be excluded from using DualShield Authentication.
 - **Client MAC exclude list** allows you to add MAC addresses that will be excluded from using DualShield Authentication. You can also specify a MAC address range using double question marks as a wildcard in any part of the address. For example, 00-14-22-01-23-??, 00-14-22-01-??-??, or 00-14-22-??-??-??.
 - **Connection to the following Gateway IPs** allows you to set a Gateway where users connected to the Gateway will be excluded from using DualShield Authentication.

Connect to a RAS Farm

Parallels Client

Once DualShield has been enabled the users will have two-factor authentication. If using software tokens such as QuickID the administrator does not have to create a token for each user. RAS Publishing Agent will automatically create the token when the user tries to log in for the first time.

When a user tries to access a RAS Connection from Parallels Client, he/she is first prompted for the Windows username and password. If the credentials are accepted, RAS Publishing Agent will communicate with the DualShield server to create a unique token for that user.

If using MobileID or QuickID an email about where you can download the appropriate software will be sent to the user.

If using QuickID tokens, the application will ask for a One-Time Password which is sent by e-mail or SMS.

When asked for OTP, enter the One-Time Password to log into the Parallels ApplicationServer XG Gateway.

Parallels Web Portal

If DualShield Unified Authentication is enabled, logging to Parallels Web Portal also requires Second-Level Authentication.

Using SafeNet

SafeNet Token Management System provides a high-value of protection via secure tokens which makes it a perfect tool for second-level authentication in Parallels RAS.

In this section:

- Configuring SafeNet (p. 267)
- Configure Parallels RAS Web Portal for SafeNet (p. 268)

Configuring SafeNet

To configure SafeNet:

- 1 In the Parallels RAS console, navigate to the **Connection / Second Level Authentication** tab.
- 2 In the **Provider** drop-down list, select **SafeNet**.
- 3 Click the **Settings** button. The **SafeNet Properties** dialog opens.
- 4 On the **Connection** tab, enter the valid URL into the **OTP Service URL** field. To verify that the connection with the OTP Service can be established, click the **Check connection** button.

Note: RAS Publishing Agent communicates with the SafeNet Token Management System Server. It is highly recommended to have this behind a firewall for security reasons.

- 5 Click the **Authentication** tab.
- 6 In the **Mode** drop-down list, select how you want your users to be authenticated.

Mandatory for all users: every user using the system must login using two-factor authentication.

The available modes are:

- **Create token for Domain Authenticated Users:** Allows Parallels RAS to automatically create software tokens for Domain Authenticated Users. Choose a token type from the drop down list. Note that this option only works with software tokens.
- **Use only for users with a SafeNet account:** Allows users that do not have a SafeNet account to use the system without having to login using two-factor authentication.

- 7 In the **TMS Web API URL** field, enter the location of the SafeNet API URL.
- 8 In the **User Repository** field, enter the user repository destination.
- 9 Click **OK** to save the values and close the **SafeNet Properties** dialog.

Parallels Client

In **Parallels Client — New Account Info** dialog:

- 1 Enter any four digits in the **OTP PIN** number field (these digits will be required further on in the process).
- 2 Enter your email address and then click on **OK**.
- 3 Log into your email account and retrieve the email containing the information you will need to activate your SafeNet authentication. An example of this email is shown below.

Activation Key: YZQHoczZWw3cBCNo

Token Serial: 4F214C507612A26A

Download MobilePASS client from:

<http://localhost:80/TMSService/ClientDownload/MobilePASSWin.exe>

**Login with domain credentials.*

**Place the attached seed file in the same folder as the MobilePASS client.*

Enter the One-Time Password to log into the RD Session Host Connection.

Application PIN: 4089

- 4 Download the MobilePASS client from the URL provided in the email.
- 5 Enter the Activation Key found in the SafeNet email.
- 6 Next, input the application PIN found in the email into the **MobilePASS PIN** field.
- 7 Click **Generate** to generate the eToken number and then click **Copy**.
- 8 Combine the OTP PIN and eToken in this order: OTP + eToken.
- 9 Enter this value into the Parallels Client and click **OK** to log in.

Configure Parallels RAS Web Portal for SafeNet

If SafeNet second level Authentication is enabled, logging to Parallels RAS Web Portal also requires second level authentication.

- 1 Enter any four digits in the **OTP Pin** number field (these digits will be required further on in the process).
- 2 Enter your email address and then click the **Send OTP** button.
- 3 Log into your email account and retrieve the email containing the information you will need to activate your SafeNet authentication. An example of this email is shown below.

Activation Key: YZQHoczZWw3cBCNo

Token Serial: 4F214C507612A26A

Download MobilePASS client from:

<http://localhost:80/TMSService/ClientDownload/MobilePASSWin.exe>

*Login with domain credentials.

*Place the attached seed file in the same folder as the MobilePASS client.

Enter the One-Time Password to log into the RD Session Host Connection.

Application PIN: 4089

- 4 Download the MobilePASS client from the URL provided in the email.
- 5 Enter the Activation Key found in the SafeNet email.
- 6 Next, input the application PIN found in the email into the **MobilePASS PIN** field.
- 7 Click **Generate the eToken** number and subsequently **Copy**.
- 8 Combine the OTP PIN and eToken in this order: OTP + eToken.
- 9 Enter this value into the Parallels RAS Web Portal and click **OK** to log in.

Configuring Exclusion Rules

When second-level authentication is enabled in the farm, user connecting to it will have to go through it before they can use published resources. If needed, you can exclude select client computers from this requirement and let them authenticate through Active Directory only.

Exclusions rules can be specified in the **Exclusion** section of the **Second Level Authentication** tab as described below.

To exclude client IP addresses:

- 1 Select the **Client IP exclude list** option and click **Configure**.
- 2 Click **Tasks > Add** and then specify a single IP address or a range of addresses.
- 3 Click **OK**.
- 4 Add additional IP addresses if needed.
- 5 When done, click **OK** to return to the **Second Level Authentication** tab.

To exclude client MAC addresses:

- 1 Select the **Client MAC exclude list** option and click **Configure**.
- 2 Click the **Add** button and select a client MAC address from the list. You can also specify a MAC address range using double question marks as a wildcard in any part of the address. For example, 00-14-22-01-23-??, 00-14-22-01-??-??, or 00-14-22-??-??-??.

To exclude gateway IP addresses:

- 1 Select the **Connection to the following Gateway IPs** option.

Connection and Authentication Settings

- 2** Type a gateway IP address or expand the drop-down list and select one or more IP addresses from the list. Click the plus sign icon to add the available gateways to the list.
- 3** Click **OK** to save the selection and close the dialog. The IP addresses will appear in the **Connection to the following Gateway IPs** edit box.

CHAPTER 20

Common Management Tasks

This chapter describes common Parallels RAS management tasks, including farm status monitoring, license management, backup management, and others.

In This Chapter

Recovery - Add a Root Administrator.....	271
Site Information.....	271
Site Settings.....	272
Upgrading RAS Agents.....	273
Licensing.....	274
Configure HTTP Proxy Settings.....	275
Configuring Notifications.....	276
RAS Session Variables.....	281
Settings Audit.....	282
Maintenance and Backup.....	285
Problem Reporting and Troubleshooting.....	287
Suggest a Feature.....	288

Recovery - Add a Root Administrator

This topic addresses a possible issue when the root administrator is not available or the domain is changed. In such events, the system becomes inaccessible. If you encounter this issue, you can quickly add a root administrator by executing the following command on the server hosting the master RAS Publishing Agent:

```
2XRedundancy -c -AddRootAccount user [domain]
```

Please note that an open Parallels RAS console will not be notified about the new account since this is an emergency recovery. You need to log out and then log in again to see the new account in the **Administration** area.

Site Information

To view the site information, select the **Information** category in the RAS Console.

The **Site Information** tab displays information about available servers, Publishing Agents, Secure Client Gateways (see **Viewing Gateway Summary and Metrics** (p. 149)), and sessions on the local computer. To view information about running applications, select the **Show application information** option (at the bottom of the page).

The **Local Information** tab shows the status of RAS components running on the local server.

Site Settings

To view and configure common site settings in the RAS Console, navigate to **Farm / <site> / Settings**.

Auditing

The **Auditing** tab page allows you to configure application auditing. When enabled, application auditing monitors processes running in the site and records this information in the audit file. To view the information, click the **View Audit** button (at the bottom of the page). The information is also displayed on the **Information / Site information** page and in RAS Reports.

To enable or disable application auditing, use the **Auditing** drop-down list (at the bottom of the page). The **Clear Audit File** button clears the current audit.

The **Filtering the following processes** list allows you to specify processes that will be excluded from the audit. Use the **Tasks** drop-down menu to add or delete a process. You can also use the **Task** menu to import and export a process list from/to a CSV file. The **Task > Properties** menu item allows you to edit a process name. The **Default** menu item resets the list to contain the default set of standard processes.

Global Logging

Standard logging is always enabled for all servers in a given site, but you have an option to enable or disable extended logging. Extended logs contain more data than default logs and can provide more information needed to resolve an issue. Please note that extended logs take more disk space compared to default logs.

The **Global Logging** tab page lists servers for which you can configure extended logging. The list has the following columns:

- **Server** — server name.
- **Type** — server type (e.g. RD Session Host, Publishing Agent, Gateway).
- **State** — logging state (level). Can be one of the following: Default and Extended (see the first paragraph above).

To enable or disable extended logging, select a server in the list and click the **Extended Logging** item. The **State** column indicates which level is currently set. To switch the level again, click the **Extended Logging** item one more time.

The **Retrieve** item retrieves all logs and saves them to a file (you'll need to specify a file name and location). The **Clear** item clears all logs. Note that once you click this item, the logs will be cleared with no additional warning.

URL redirection

The **URL redirection** tab page allows you to specify URLs that should never be redirected when the **Allow Client URL/Mail redirection** option is enabled for **RAS RD Session Host Agent** or **RAS Remote PC Agent**. This option is set on **Agent Settings** tab page of a corresponding server. When the option is enabled, "http" and "mailto" links are opened using a local application on the client computer rather than the server resources.

Client settings

See **Specifying Client Settings** (p. 134)

Upgrading RAS Agents

When you add Parallels RAS components to a farm, you install a corresponding RAS Agent on them. This includes RAS Publishing Agent, RD Session Host Agent, VDI Agent, Guest Agent, Remote PC Agent. In addition to the functionality that allows you to check agent status, and update it if necessary, you can do a bulk agent update or upgrade.

There are two ways you can find out if agents need to be updated. You can be notified by Parallels RAS or you can check the status and initiate the update procedure manually.

When the Parallels RAS Console starts, you may see a message box saying that Agents need to be installed or updated. You can start the update procedure by clicking **Yes** in this dialog. You will then see a list of all servers on which an Agent needs to be updated where you can decide whether to include a server in the bulk update procedure or exclude it. Once you've made your selection, follow the onscreen instructions and update the Agents.

To initiate the procedure manually, click the **Task > Upgrade all Agents** in the RAS Console where this menu is available (most of the views where it makes sense). You can also right-click inside the view and choose **Upgrade all Agents**. Follow the onscreen instructions and select the servers on which an Agent requires an update or upgrade. Please note that if all Agents on all servers displayed on a given pane are up to date, the menu option will be disabled.

For example, to upgrade all master Publishing Agents in all sites, select **Farm / Farm** and then click **Tasks > Upgrade all Agents** (or right-click inside the pane and choose **Upgrade all Agents**). To upgrade all Agents on all servers in a site, select **Farm / <site>** and click **Tasks > Upgrade all Agents**. Similarly, to upgrade Agents on all RAS Secure Client Gateways, select **Farm / <site> / Gateways** and use the same **Tasks > Upgrade all Agents** menu item. For other components, do exactly the same. Note that if you use the same credentials on all servers, you will have to enter them only once. The update procedure will remember the last entered credentials and will try to use them on all servers. If the credentials don't work on a server, you'll be asked to enter them again.

Please note that after you click the **Tasks > Upgrade all Agents** menu, the dialog that opens will contain the hosts on which an Agent needs updating or upgrading. The **Status** column in the list will indicate that and the host will be preselected for the upgrade. Unverified Agents will also be included in the list but will not be preselected. You can select them if you believe that an Agent has to be upgraded on them too.

Note: When updating an agent in a RAS Template (VDI), full and linked clone templates are updated differently. For important information, please read the **RAS Template Maintenance** section (p. 97).

Licensing

The **Licensing** category allows you to manage your Parallels RAS license. When you click on the **Licensing** category, the **License Details** tab displays the following information:

- **License Type:** The type of your Parallels RAS license (e.g. subscription, trial, etc.).
- **Expiration Date:** Your license expiration date (or the number of days remaining).
- **Maximum allowed concurrent users:** The maximum number of concurrent users that your license allows. For example, if you own a Parallels RAS subscription and need more concurrent connections, you need to upgrade your subscription.
- **Peak Users:** Your peak concurrent users to date. You can use this value to evaluate whether you might need to upgrade your subscription to include more concurrent users.
- **Current Users:** The number of users currently connected to your Parallels RAS farm.

Please note that you can also see these values (and more) in your Parallels Account. For more information, please read the **Parallels RAS Licensing Guide**, which is available on the Parallels website.

The **View Active Users** button opens a dialog where you can view currently active users and license usage. Use the toolbar buttons to refresh the list and to copy the information to the clipboard.

The **Manage license** button allows you to switch to a different Parallels account and to activate Parallels RAS using a different license key. Click the button to open the **Sign in to Parallels My Account** dialog. Use the dialog to sign in using an existing account or click **Register** to create a new account. If you are creating a new account, you'll also have to register a Parallels RAS license key in it and activate your Parallels RAS farm using that key (see below).

To activate Parallels RAS using a different license key:

- 1 In the **Sign In to Parallels My Account** dialog, type the email address and password you used to register your account and click **Sign In**. You'll see the **Activate Product** dialog.
- 2 Select the **Activate using license key** option and enter the key in the field provided. You can click the button next to the field to see the list of subscriptions and/or permanent license keys you have registered with Parallels My Account. If the list is empty, it means that you don't have a subscription yet and need to purchase one first.
- 3 To purchase a subscription online, click the **Purchase a license** link.
- 4 After entering a license key, click **Activate**. You should see the confirmation message that your Parallels RAS was activated successfully.

Configure HTTP Proxy Settings

If you use an HTTP proxy server on your network, you need to configure it in the RAS Console. The proxy server settings will be used during Parallels RAS license updates and by other features that communicate with the Parallels cloud.

To configure a proxy server:

- 1 In the RAS Console, navigate to **Administration > Settings**.
- 2 In the **HTTP Proxy settings** section, click the **Configure Proxy** button.
- 3 In the dialog that opens, select one of the following options:
 - **No Proxy server** — if you don't use a proxy server.
 - **Use system proxy settings** — if this option is selected, the proxy server configured in the Internet Explorer will be used.
 - **Manual HTTP proxy configuration** — select this option if you would like to specify the settings manually. The **Detect Settings** button will attempt to detect the proxy settings automatically.
- 4 Click **OK** to save the settings.

Configuring Notifications

On the **Notifications** tab in the **Administration** category, you can configure system event notifications and actions. Notifications are used to alert the administrator about system events via email. Actions are used to perform automatic tasks using scripts when a system event occurs. When you configure notifications, the settings apply to all servers in the farm.

To configure notifications, you first need to configure notification handlers where you can specify threshold values (where available) and whether an administrator should be notified via email. You can also configure notification scripts, which will be automatically executed when an event occurs.

In this section:

- Configuring Notification Handlers (p. 276)
- Configuring Notification Scripts (p. 278)
- Configuring SMTP Server Connection for Event Notifications (p. 281)

Configuring Notification Handlers

To configure notification handlers:

- 1** In the RAS Console, select the **Administration** category and then click the **Notifications** tab.
- 2** Click **Tasks > New** (or click the plus-sign icon) and choose an event for which to create a handler. For the list of events and their descriptions, please see the **System Events** subsection below.
- 3** A dialog opens where you can specify the event handler setting.

On the **General** tab, specify the following options:

- The threshold value (a number or percentage). Not available for some events (such as Licensing, Agent, and some other events).
- The direction (whether the event should trigger when the value rises above or drops below the specified value). Not available for some event (same as above).
- Whether to notify the administrator via email.
- Additional emails (separated by commas or semi-colons) to which to send an event message.
- Whether to execute a script when the event triggers. Here you need to select the **Execute a notification script** option and then choose a script from the drop-down list. Before you can use this option, you need to create one or more scripts as described in **Configuring Notification Scripts** (p. 278).

On the **Settings** tab, specify the following:

- **Use default settings:** Select this option to use default settings. To edit defaults, click the **Edit Defaults** link. To use custom settings, clear this option and specify the options as described below.
- **Notification handler grace period:** Specify a time period (in minutes) to wait from the event occurrence until the notification is triggered. Some events may trigger but last for a very short period of time. For example, a CPU usage can sharply jump above the specified threshold but quickly return to normal. For such events, it would probably make sense not to trigger the notification right away. This option allows you to specify the delay.
- **Notification interval:** Specify the minimum time interval (in minutes) between the last and the next notification. Allows to prevent multiple notifications to be emailed to administrators in rapid succession (i.e. prevents spamming).
- **Send one notification and suspend further notifications until recovered:** When this setting is enabled, a notification will be raised only once, and after that it will be suspended until the values monitored by the notification have recovered. For example, if the CPU usage is above the threshold for the whole day, instead of executing the notification handler multiple times, RAS would execute it only once.

4 When done, click **OK** to save the notification handler.

Please note that the mailbox should be configured in the RAS Console for the outgoing email functionality to work. This mailbox is usually set up when you run the RAS Console for the first time and then use the **Start** category to set up your RAS environment. You can also set up a mailbox as described in **Configuring SMTP Server Connection for Event Notifications** (p. 281).

To enable or disable an event handler, select or clear the checkbox in the first column, or right-click an event and choose **Enable** or **Disable**. To modify a handler, right-click it and choose **Properties**. To delete a handler right-click and choose **Delete**.

System Events

You can create notification handlers for the following system events:

- **CPU utilization.** Triggers when CPU utilization rises above or drops below a specified value.
- **Memory utilization.** Triggers when memory utilization rises above or drops below a specified value.
- **Number of RDSH sessions.** Triggers when the number of active sessions rises above or drops below a specified value.
- **Number of disconnected RDSH sessions.** Triggers when the number of disconnected sessions rises above or drops below a specified value.
- **RDSH session utilization.** Triggers when the number of RDSH sessions rises above or drops below a specified percentage of the maximum number of sessions.
- **RDSH disconnected sessions utilization.** Triggers when the the number of RDSH disconnected sessions rises above or drops below a specified percentage of the maximum number of sessions.

- **Number of gateway tunnelled sessions.** Triggers when the number of gateway tunnelled sessions rises above or drops below a specified value.
- **RAS Agents events.** Triggers when an agent event occurs (e.g. agent disconnects or reconnects).
- **Licensing events.** Triggers when a licensing event occurs. One notable event here is the license usage reaching a predefined threshold. Specifically, when the license usage reaches 90% of all available licenses, you will receive an email, so you have time to decide whether you have enough licenses or need to add more. Other events include license activation/deactivation, license expiration, grace period starting/ending, license information changes, problem communicating with the licensing server.
- **Authentication server events.** Triggers when a connection issues occurs with an authentication server.
- **Published items events.** Triggers when a published item event occurs (e.g. the concurrent instance limit for an application is reached).
- **VDI events.** Triggers when a VDI event occurs (e.g. a template is not found).

Please also see the **Notification Types** table in the **Configuring Notification Scripts** section (p. 278).

Configuring Notification Scripts

To configure notification scripts:

- 1** On the **Administration / Notifications** tab, click **Tasks > New** (or click the plus-sign icon) in the **Notifications scripts** section.
- 2** In the dialog that open, specify the following options:
 - **Script name:** Enter a friendly name for the script.
 - **Command:** The command to execute.
 - **Arguments:** Command line arguments to pass to the command. An argument can be one of the predefined variables, which Parallels RAS will automatically replace with an actual value. See the **Command Line Variables** table below (the ID column contains the values that can be used here).
 - **Initial directory:** The full path to the current directory for the process. The string can also specify a UNC path.
 - **User name, Password:** These are optional fields that you can specify if you would like to execute the command under a specific user account.
- 3** When done, click **OK** to save the notification script item.

To modify a notification script, right-click it and choose **Properties**.

To delete a script, right-click and choose **Delete**. Please note that if a script is used by a notification handler, you will see a warning message. If you choose to delete it anyway, the script association will be removed from all notification handlers where it is used and all affected handlers will be automatically configured to send an email alert.

Command Line Variables

The following table list command line variables that you can use as arguments when executing a script (see the **Arguments** option description above):

Variable	Description
(\$FARM-NAME)	Name of the RAS farm which has raised the notification.
(\$SITE-NAME)	Name of the RAS site which has raised the notification.
(\$SERVER-ADDRESS)	IP address or FQDN of the server which has raised the notification. It could be an RDSH server, the server hosting a RAS Publishing Agent, RAS Secure Client Gateway, etc.
(\$TRIGGER-ADDRESS)	IP address or FQDN of the Publishing Agent that has raised the notification.
(\$THRESHOLD-VALUE)	The threshold value that is assigned to the notification handler. If a notification type doesn't support thresholds, the argument should be replaced with an empty string.
(\$NOTIFICATION-TIME)	<p>GMT time and date of when the event has occurred. String format shall use the "R" or "r" format specifier. Please see the following article from Microsoft for details:</p> <p>https://docs.microsoft.com/en-us/dotnet/standard/base-types/standard-date-and-time-format-strings</p> <p>Note: The time should represent the time when the notification has occurred, and not when the notification handler has been executed. The notification handler may be executed with a delay if a grace period is enabled.</p>
(\$NOTIFICATION-TYPE)	A numeric value that is assigned to each particular notification type. Notification type values are listed in the Notification Types table below.

Notification Types

The following table lists supported notification types (the ID column represents values that are passed to the (\$NOTIFICATION-TYPE) command line variable):

Type	Priority	ID	Notes
CPU utilization	L	1	
Memory utilization	L	2	
Number of active session	M	3	
Number of disconnected sessions	M	4	
RAS Agent connect	H	5	
RAS Agent disconnect	H	6	

Common Management Tasks

VDI template is missing	H	7	
Published application limit exceeded	M	8	
Multi PA communication error	H	9	
Authentication provider not reachable	H	10	
% of RDSH session out of the maximum specified value	H	11	
Gateway is tunneling X number of sessions	H	12	
Reserved		13	Used internally.
Licensing events	M	14	All licensing notifications are controlled through this item.
Session degradation	H	18	Parallels Client determines abnormal round trip time.
Application startup time	M	19	Time to start an application. The measurement is done on the client side.
Publishing Agent auto promotion		20	
Publishing Agent auto promotion failed		21	
Publishing Agent auto promotion failback		22	
License activated		100	Controlled through "Licensing events"
License deactivated		101	Controlled through "Licensing events"
License max usage		102	Controlled through "Licensing events"
License about to expire		103	Controlled through "Licensing events"
License expired		104	Controlled through "Licensing events"
License trial expired		105	Controlled through "Licensing events"
License grace period start		106	Controlled through "Licensing events"
License grace period end		107	Controlled through "Licensing events"
License disabled		108	Controlled through "Licensing events"
License information changed		109	Controlled through "Licensing events"
License failed to communicate with server		110	Controlled through "Licensing events"
License no file		111	Controlled through "Licensing events"
License invalid version		112	Controlled through "Licensing events"
License invalid signature		113	Controlled through "Licensing events"
License invalid license		114	Controlled through "Licensing events"
License invalid MAC address		115	Controlled through "Licensing events"

Configuring SMTP Server Connection for Event Notifications

The **Mailbox** tab in the **Administration** category allows you to configure an SMTP server for outgoing emails. The SMTP server is required for the administrator to receive system event alerts (as described in the previous sections) and to send invitation emails to users.

To configure an SMTP server:

- 1 In the RAS Console, select the **Administration** category and then click the **Mailbox** tab.
- 2 In the **Mail Server** field, type your mail server FQDN or IP address.
- 3 In the **TLS / SSL** drop-down list, select whether to use it the protocol.
- 4 Select the **SMTP server requires authentication** option if required and then type the SMTP server username and password in the fields provided.
- 5 In the **Sender information** section, type the sender email address (e.g. your email).
- 6 The **Test mailbox settings** section can be used to test your SMTP server configuration. Enter one or more email addresses separated by a semicolon. Click **Send Test Email** to test the settings.

RAS Session Variables

When a remote user starts a published application or desktop, a set of session variables is created by Parallels RAS on the host server. The variables contain information about the client machine, which you can examine if needed. The variables are always updated, so on connect/reconnect they always contain the latest values.

The following RAS session variables are available:

Variable Name	Description
TUX_REMOTECLIENT_PLATFORM	Name and version of the operating system running on the client machine. For example, "Windows 8.1 Enterprise Edition (WOW 64)", "iPhone OS 9.2.1", "Android 6.0", etc.
TUX_REMOTECLIENT_MAC	MAC address of the client machine.
TUX_REMOTECLIENT_IP	IP address of the client machine as seen by the client.
TUX_REMOTECLIENT_LANG	Language used by the GUI on the client machine: EN, FR, RU, DE, ES, IT, PT, CS (Chinese Simplified), CT (Chinese Traditional), KR (Korean). Note that on macOS, iOS, and Android devices, the language is reported as the one used in the OS but only if it's a supported language. If it's not supported, it will default to EN.
TUX_REMOTECLIENT_MACHINE	Client's computer name. For example, "Bob's iPad mini 1st generation", "BobPC", "Bob's iMac", etc.
TUX_REMOTECLIENT_LOGIN	The username (including domain) that was used to log in to

	Parallels RAS. For example, myuser@somedomain.
TUX_REMOTECLIENT_VERSION	Parallels Client version.
TUX_REMOTECLIENT_VENDOR	Device vendor name. For example, "Asus", "Apple", "Google", etc.
TUX_REMOTECLIENT_MODEL	Device model name. For example, "Nexus 5", "iPad2.6", etc.

You can view RAS session variables and their values using one of the following two methods:

- By examining the Windows registry on the host server.
- By executing the GetRASVariable.exe utility (provided by Parallels RAS).

Each method is described below.

Examine the registry

To see the variables, run `regedit` and navigate to `HKEY_CURRENT_USER\Software\Parallels\Shell\<Session-ID>`, where `<Session-ID>` is the ID of a session as displayed in the RAS Console (e.g. 2, 3, 4, etc.) The variables for a particular session are listed under the session ID node. On user connect/reconnect they are updated to reflect the actual client configuration. The variables exist for the duration of a session and are removed from the registry once the session is terminated.

Please note that in addition to the variables listed in the table above you may see other (undocumented) variables under a session ID. Those are for internal Parallels RAS use only and should be ignored.

Using GetRASVariable.exe utility

The `GetRASVariable.exe` utility is located in the Parallels RAS installation folder (e.g. `C:\Program Files (x86)\Parallels\ApplicationServer`). To obtain a value of a variable, execute the utility from the command line passing the variable name as parameter (see the table above). The utility will output the value to the screen.

The following example displays the value of the `TUX_REMOTECLIENT_MACHINE` variable:

```
GetRASVariable.exe TUX_REMOTECLIENT_MACHINE
```

Settings Audit

Parallels RAS gives you the ability to audit the modifications that were done to a Parallels RAS farm, including changes to any of the components, objects, resources, and users. This information is stored in a database, so it can be reviewed and possibly reverted, if needed. The information is stored in the master database but is replicated in a local database on the computer where Parallels RAS Console is running.

You can view the list of modifications using one of the following options:

- By navigating to **Administration / Settings audit**. The tab displays the master list of all changes to any components/objects in the farm. If a modification can be reverted, you can do it here.
- By clicking **Tasks > Settings audit** on any pane in the RAS Console that supports this functionality. Compared to the master list (described above), you will only see modifications to the same types of components or objects that are managed on a given pane. You can also revert a modification here if it can be reverted. If the **Settings audit** menu option is not available on a particular pane, it means that the functionality is not available for the types of components or objects that this pane manages.

The following describes in detail how to view and revert farm modifications.

View the master settings audit list

To view the master list of all modifications for a farm, do the following:

- 1** In the Parallels RAS Console, select the **Administration** category and then click the **Settings audit** tab.
- 2** The sync process will check that the local audit database is in sync with the master database and will do an update if necessary (you may see a progress indicator while the syncing is in progress).
- 3** Once the syncing is complete, the **Settings audit** tab will be populated with data. Each entry in the list corresponds to a modification that was done either by a RAS administrator or a system service.

The information for each entry in the list includes the following:

- **Date:** Date and time of the modification.
- **Session:** Session ID.
- **Username:** The name of the administrator or RAS service that was responsible for the modification. RAS services may include System (redundancy service) and Publishing Agent (controller service).
- **Action:** The action that was performed, such as Connect, Disconnect, Create, Update, Switch site, and others.
- **ID:** The affected object's ID.
- **Site:** The number and name of the affected site. "Global" means the change affected all sites.
- **Type:** The modification type. This usually makes sense when viewed together with the **Action** value.
- **Name:** The value in this column is displayed for some entries and can provide additional information, such as the name of the changed object.

You can perform the following actions on the list:

- To refresh the list, click the "recycle" icon (top right).
- To view details for an entry, double-click it (or select an entry and click **Tasks > View entry**).
- To search for a specific entry (or entries), click the magnifying glass icon (top right). An extra row is added at the top of the list allowing you to enter the search criteria. You can type a string to search for in one or multiple columns. The search is performed as you type and the list is filtered to include only the matching entries. To cancel filtering and display the complete list, click the magnifying glass icon again.

Reverting a modification

To revert a modification in the master list:

- 1** Double-click a desired entry on the **Settings Audit** tab.
- 2** The **Audit Entry** dialog opens. While here, you can click **Next** and **Previous** buttons to go to the next or previous item as they are displayed in the master list.
- 3** To revert the change, click the **Revert** button. If the button is disabled, it means that the change cannot be reverted.

Changes that can never be reverted include the following:

- Any changes done by System or Publishing Agent (as displayed in the **Username** column).
- Changes that were done in previous versions of Parallels RAS where this feature did not exist.
- Changes related to administrator accounts.

View a local settings audit list

You can also view and revert configuration changes for a specific type of RAS components or objects. When you are on a particular pane (or tab) in the RAS Console, look for the **Tasks > Settings audit** menu option (or right-click > **Settings audit**). If it's there, then you can view the changes and revert them if needed. Consider the example below.

Let's say you want to see changes that were done to RD Session Hosts. To do so:

- 1** In the RAS Console, navigate to **Farm / <site> / RD Session Hosts**.
- 2** Click **Tasks > Settings audit**.
- 3** The **Settings Audit** dialog opens listing all known modifications that were done to RD Session Hosts. The modifications may include creating, moving, deleting, or updating an RD Session Host. The type of the modification is displayed in the **Action** column in the list.
- 4** To revert a modification, select it and click the **Revert** button (in the lower right of the dialog). If the button is disabled when you select a particular entry, it means that the modification cannot be reverted.

The local settings audit functionality is available for most of the major components and objects in the Parallels RAS Console. This includes RD Session Hosts (including Groups and Scheduler), VDI, Remote PCs, Gateways, Publishing Agents, Themes, Publishing, Quick Keypad, and many others. Once again, when you view a particular pane, look for the **Tasks > Settings audit** menu option (or right-click > **Settings audit**). If it's there, then you can view the changes and revert them if needed.

Maintenance and Backup

Keeping Parallels RAS up to date

By default, Parallels RAS checks for updates each time the RAS Console is started. If you wish to change this behavior:

- 1 Select the **Administration** category and click the **Settings** tab.
- 2 Select or clear the **Check for updates when launching Parallels RAS Console** option according to your needs.
- 3 To check for updates manually, click the **Check Now** button.

Backing up the Parallels RAS farm configuration

To backup the Parallels RAS farm configuration:

- 1 Select the **Administration** category and then click the **Settings** tab.
- 2 Click the **Export Settings** button.
- 3 You'll see a message box saying that all sites will be synchronized. Click **Yes** to continue with export or click **No** to abort it.
- 4 Specify the file name and target folder and click **Save**.

Note: The export procedure only exports the Parallels RAS farm configuration data. Unrelated objects, such as downloaded OS, etc. are not included in the exported file.

To restore a Parallels RAS farm configuration from a backup file, click the **Import Settings** button and select a backup file (the default file extension is `.dat2`). When you import a configuration from a file, your existing farm configuration will be completely replaced with it.

You can also export and import a Parallels RAS farm configuration from the command line. For complete instructions, please read on.

Exporting and Importing Farm Settings via Command Line

Parallels RAS PowerShell allows you to perform the majority of Parallels RAS administration tasks from the command line.

This section contains information about using PowerShell to export and import farm settings. To learn more about Parallels RAS PowerShell, please visit <http://www.parallels.com/products/ras/resources/> and download (or view online) the **Parallels RAS PowerShell Guide**.

One of the uses of exporting and importing farm settings is running automated tests. Specific configurations can be created, exported, and then imported for specific test scenarios. You can also use this functionality with Windows task scheduler for regular backups of farm settings.

Installing Parallels RAS PowerShell

RAS PowerShell is installed by default when you run the default Parallels RAS installation. If you haven't installed it (or to install it on a different computer), do the following:

- 1 Run the Parallels RAS installer.
- 2 Select **Custom** and then select the **Parallels RAS PowerShell** component.
- 3 Complete the wizard and install Parallels RAS PowerShell.

Using Parallels RAS PowerShell

The complete up-to-date information about Parallels RAS PowerShell can be found in the **Parallels RAS PowerShell Guide**. The guide includes the **Getting Started** chapter to help you quickly get started with Parallels RAS PowerShell, as well as the complete reference and code samples. Please visit <http://www.parallels.com/products/ras/resources/> to view or download the guide.

Use the instructions below to export and import Parallels RAS farm settings.

To import the Parallels RAS PowerShell module, open the PowerShell console and execute the following command:

```
Import-Module PSAdmin
```

Create a Parallels RAS session (use the name or IP address of the server where you have Parallels RAS installed):

```
New-RASSession -Server "server.company.dom"
```

To export farm settings, execute the following command (substitute the path and filename of the backup file with your own):

```
Invoke-ExportSettings "C:\Backup\RAS-backup.dat2"
```

To import farm settings:

```
Invoke-ImportSettings "C:\Backup\RAS-backup.dat2"
```

Problem Reporting and Troubleshooting

If you are experiencing an issue with Parallels RAS, you can search for a solution right from the RAS Console. If you can't find a solution, you can send a support request to Parallels. This section describes how to accomplish these tasks.

Search for a solution

To search for a solution from the RAS Console:

- 1 In the console, click **Help** on the main menu and choose **Troubleshooting and Request Support**.
- 2 The **Troubleshooting** dialog opens.
- 3 In the **Select Category** drop-down list, select a category you are having a problem with. The area in the middle of the dialog will be populated with a list of existing KB articles related to that category.
- 4 Click an article of interest to read in a web browser.
- 5 You can also click **Knowledge Base Index** or **Forums** links to go to the Parallels knowledge base or Parallels forums.

Request support

If you can't find a solution for your problem using the options described above, you can send a support request to Parallels. When you do, the collected logging information is retrieved and attached to the email, so that Parallels Support can analyze it. See **Logging** for more information.

Note: A support request creates a support ticket, which is then sent to Parallels Support. If you already have a request support ticket, you can send just the system report to Parallels without creating an additional (and identical) ticket. See the **Send a report** subsection below. Please note that if you don't have a valid RAS subscription or a support contract, the ticket will NOT be created. In order to receive support, you will need to purchase a subscription or support contract.

Before you request support, please make sure that you have a mailbox setup in the RAS Console. If you haven't set up a mailbox yet, do it as follows:

- 1 In the RAS Console, navigate to **Administration / Mailbox Setup**.
- 2 Enter your outgoing email server information, your email address, and the security/authentication information if needed.
- 3 You can send a test email by entering an email address in the field provided and clicking the **Send Test Email** button.

To send a support request to Parallels:

- 1 In the **Troubleshooting** dialog, click the **Send Support Request** button.

- 2 The **Contact Support** dialog opens.
- 3 Enter your full name and your company name.
- 4 Enter the subject. This will be used as a subject in the email that will be sent to Parallels Support.
- 5 In the **Enter your query** box, describe the issue the best you can.
- 6 Use the **Attachment** field to attach a file to the email. Click the [...] button to browse for a file. You can attach a picture or any other file that you think might help the Parallels Support to find a solution. Please note that the log files and the Parallels RAS settings are collected and attached to the email automatically, so you don't have to do it yourself.
- 7 In the drop-down list at the bottom of the dialog, select whether you want to send the email or save it (including the automatically collected information) as a zip file.
- 8 Depending on the action selected in the previous step, click **Send** to send the email or **Save** to save it as a zip file on your local drive or a network folder.

Send a report

If you already have a support request ticket, you can send just a system report to Parallels without creating a new ticket.

To send a report:

- 1 In the console, click **Help** on the main menu and choose **Upload System Report to Parallels**.
- 2 A dialog opens displaying the progress bar.
- 3 Once the system report data is collected and sent to Parallels, a message box is displayed containing the report number.
- 4 Click **OK** to finish.

Suggest a Feature

If you have an idea of a new feature for Parallels RAS, we would like to hear from you! To suggest a feature, in the RAS Console, click **Help** on the main menu and choose **Suggest a Feature**. This will take you to the **Parallels RAS Feature Suggestion** web page where you can communicate your ideas to us. Please note that you must be signed in using your Parallels account email address and password to post in the feature suggestion forum.

Appendix

In This Chapter

Port Reference	289
Parallels Client URL Scheme.....	294
RAS Performance Counters.....	296

Port Reference

Parallels RAS v16.1 and newer

Parallels Client

Source	Destination	Protocols	Ports	Description
Parallels Client	HALB	TCP	80, 443, 3389	TCP 3389 if RDP load balancing is enabled.
		UDP	80, 443	If RDP-UDP is used.
		TCP, UDP	20009	Client Manager, shadowing via FW.
	RAS Secure Client Gateway (Normal and Forwarding modes)	TCP	80, 443, 3389	TCP 3389 if RDP load balancing is enabled.
		UDP	80, 443	If RDP-UDP is used.
		TCP, UDP	20009	Client Manager, shadowing via FW only for Normal mode. Since RAS v16, forwarding gateways don't support client management.
		UDP	20000	Gateway lookup broadcast.
	RDP Session	TCP, UDP	3389	Connections in Direct mode 3389 is used. RDP connection is always encrypted.

Web Browsers

Source	Destination	Protocols	Ports	Description
HTML5 web browser	RAS Secure Client Gateway	TCP	443	HTML5 (in Normal mode only).
Web browser	Web Portal	TCP	81	Web portal UI. An actual session uses the Parallels Client information.
		TCP	443	If SSL is enabled.
Web Portal	RAS Secure Client Gateway	TCP	80, 443	If SSL is enabled.

RAS Secure Client Gateway

Source	Destination	Protocols	Ports	Description
RAS Secure Client Gateway in Forwarding mode	RAS Secure Client Gateway in Normal mode	TCP	80, 443, 3389	TCP 3389 if RDP load balancing is enabled.
		UDP	80, 443	If RDP-UDP is used. Note: Since RAS v16, forwarding gateways don't support client management.
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.
RAS Secure Client Gateway in Normal mode	Remote Desktop Services	TCP, UDP	3389	RDP Connections
	RAS Publishing Agent	TCP	20002	TCP 20002 Publishing Agent Service Port - communications with RAS Secure Client Gateways and RAS Console (in Normal mode only).
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.
	Localhost	TCP	20020	Communication with NodeJS web server.

RAS Publishing Agent

Source	Destination	Protocols	Ports	Description
RAS Publishing Agent	RAS Publishing Agent	TCP	20001, 20030	TCP 20001 Redundancy Service. TCP 20030 Communication between Publishing Agents running in the same site.
		UDP	20021	RAS Publishing Agent lookup broadcast.
	Parallels Licensing Server	TCP	443	Outbound TCP 443 - RAS Publishing Agent (Master RAS Publishing Agent in Licensing Site) communicates with Parallels Licensing Server (https://ras.parallels.com)
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.
	RAS RD Session Host Agent	TCP	30004	TCP 30004 Server for RAS Publishing Agent requests.
	RAS VDI Agent	TCP	30006	TCP 30006 - RAS VDI Agent communication port.
	RAS Guest Agent	TCP	30004 (30010 on RAS v16.5 and later) 30005	TCP 30004 (30010 on RAS v16.5 and later) is used by RAS Console during RAS Template creation. TCP 30005 is used by components on the destination RDS/Guest/Remote PC for internal communication. Client does not use it.
	RAS Remote PC Agent	TCP	30004	RAS Remote PC Agent communication port (Agent status, counters and session information).
	2FA Server(s)	TCP, UDP	8080, 80, 1812, 1813	Deepnet / Safenet / Radius.

RAS Console

Source	Destination	Protocols	Ports	Description
RAS Console	SQL host with SSRS and Reporting component	TCP	30008	RAS Publishing Agent (RAS Console and reporting).
	HALB	TCP, UDP	31006	TCP, UDP 31006 configuration.
	Parallels Client	TCP	50005	Shadowing from RAS Console in case of direct network connection.
	RAS Guest Agent RAS RD Session Host Agent RAS Remote PC Agent RAS Publishing Agent RAS Secure Client Gateway	TCP	135, 445, 49179	Remote install push/takeover of software.
	RAS Guest Agent	TCP	30004 (30010 on RAS v16.5 and later)	Used for the "Check Agent" task.
		UDP	30004 (30009 on RAS v16.5 and later)	Used to manage components.
	RAS Remote PC Agent RAS RD Sessions Host Agent	TCP, UDP	30004	Used for the "Check Agent" task. Used to manage components.
	RAS VDI Agent	TCP, UDP	30006	Used for the "Check Agent" task. Used to manage component.
	2FA Server/s	TCP, UDP	8080, 80, 1812, 1813	Deepnet / Safenet / Radius.
	www.turbo.net	TCP	80, 443	When Turbo containerized apps publishing is enabled and used. Used to obtain app categories and available apps metadata for further publishing.
	RAS Performance Monitor	TCP	3000	Performance Dashboard in the Monitoring category (Grafana connection).
	RAS Publishing Agent	TCP	20002, 20001	Communication with RAS Publishing Agent and Redundancy.

RAS Agents: RD Session Host, VDI, Guest, Remote PC

Source	Destination	Protocols	Ports	Description
RAS RD Session Host Agent	RAS Publishing Agent	TCP	20003	TCP, UDP 20003 Communications with RAS Publishing Agents.
	Localhost	TCP	30005	For internal commands - memshell, printer redirector).
	www.turbo.net	TCP	80, 443	When Turbo support is enabled and used. Used to download Turbo installation package and install / update application containers.
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.
RAS VDI Agent	RAS Publishing Agent	TCP	20003	RAS Publishing Agent communication port.
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB - applicable to Hyper-V only.
RAS Guest Agent	RAS VDI Agent	TCP	30006	Communication with RAS VDI Agent
	Localhost	TCP	30005	For internal commands - memshell, printer redirector).
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.
RAS Remote PC Agent	RAS Publishing Agent	TCP	20003	RAS Publishing Agent communication.
	Localhost	TCP	30005	For internal commands - memshell, printer redirector).
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.

HALB

Source	Destination	Protocols	Ports	Description
HALB	HALB	VRRP	112	RAW

Common Communication Ports

Source	Destination	Protocols	Ports	Description
RAS Console	Any host to which Agents are pushed	TCP	135, 445, 49179	Remote install push/takeover of software.
Master RAS Publishing Agent	AD DS controllers	TCP	389, 3268	LDAP
		TCP	636, 3269	LDAPS
		TCP	88	Kerberos
		UDP	53	DNS
	2FA Server/s	TCP, UDP	8080, 80, 1812, 1813	Deepnet / Safenet / Radius.

Active Directory and Domain Services Ports

For Active Directory and Active Directory Domain Services port requirements, please see the following article: <https://technet.microsoft.com/en-us/library/dd772723%28v=ws.10%29.aspx>

Parallels Client URL Scheme

Parallels RAS uses the following URL schemes to perform actions in Parallels Client installed on end user devices:

- `prlclient://` — the scheme that is currently used in Parallels RAS (RAS v15.5 and later versions).
- `tuxclient://` — this is a legacy scheme kept for backward compatibility with older versions of Parallels Client.

The actions that can be performed in Parallels Client include the following:

- Configure a Parallels RAS or RDS connection using specific settings.
- Launch a remote application by specifying the host, the application itself, and some other parameters.

Parallels Client URL schemes are supported on the following platforms:

- Windows
- macOS
- Linux
- iOS
- Android

Parallels RAS uses URL schemes in invitation emails and in the HTML5 Client. For more information, see **Invite Users** (p. 28) and **Launching Remote Applications and Desktops** (p. 160).

The following table can be used as a reference to parameters used in a Parallels Client URL:

Key	Datatype	Value
Command	String	"LaunchApp" This tells Parallels Client that the intent is to create a connection and / or launch a published resource.
AppID	Int	The application ID to launch (the ID is displayed in the Publishing category in the Parallels RAS Console). If this parameter is empty, Parallels Client will only list the available resources.
Alias	String	A connection name (when creating a new connection).
ConnType	Int	Connection type: <ul style="list-style-type: none"> • 2 — Standard RDP Connection • 0 — Parallels RAS Connection
ConnMode	Int	Connection mode: <ul style="list-style-type: none"> • 0 — Gateway • 1 — Direct • 2 — Gateway SSL • 3 — Direct SSL
Server	String	The server FQDN or IP address.
Backup	String	The secondary connection server (if available and required).
Port	Int	The port number.
UserName	String	User name. If this parameter is empty, the user will be prompted to enter a name when connecting to Parallels RAS.
EncPass	String	Encrypted ('hashed') password. If not specified, a user will be prompted for password when connecting.
SessionID	String	The Auth Session ID.
Connect	Boolean	Whether to connect to Parallels RAS right after the connection is configured.
Save	Boolean	Whether to save the connection settings in Parallels Client.
Request Page	String	Used by HTML5 Client to obtain information from Parallels Client.
SSO	String	[Optional] Custom 3rd party SSO GUID. Used only by Windows clients. Currently only used by invitation emails.
HelpDeskEmail	String	[Optional] Help desk/support contact email. Currently only used by Android and iOS clients.
OverrideArgs	String	Override application parameters. Currently only used by Mac client.

Example:

```
prlclient:///?Command=LaunchApp&AppID=2360&Alias=Leonardo+IPv4&ConnType=0&ConnMode=0&Server=10.125.0.50&Backup=&Port=80&UserName=tester56%402x&EncPass=16Y1%2bfOryvNHysI0nWIW4g%3d%3d&SessionID=A78399FE-7077-43AD-8D0A-03641F1C759B&Connect=YES&Save=NO&RequestPage=http://leonardo.2x.testing/2xwebportal/Dashboard.aspx
```

RAS Performance Counters

The following table lists performance counters available in Parallels RAS per component:

Parallels RAS Gateway (2XProxyGateway.exe)

Available since	ID	Name	Description	Notes
v16.5	ras_gw_tot_conn	Total connections	The total number of Connections with the Gateway.	
v16.5	ras_gw_tot_threads	Total threads	The total number of threads running on the Gateway.	
v16.5	ras_gw_rpd_sess	RDP tunneled sessions	The number of tunneled RDP sessions.	
v16.5	ras_gw_rpd_sess_s	RDP SSL tunneled sessions	The number of tunneled RDP sessions over SSL.	
v16.5	ras_gw_html	HTTP connections	The number of tunneled HTTP sockets	
v16.5	ras_gw_html_s	HTTPS connections	The number of tunneled HTTPS sockets	
v16.5	ras_gw_html5	HTML5 connections	The number of tunneled HTTP5 sockets	
v16.5	ras_gw_html5_s	HTML5 SSL connections	The number of tunneled HTTP5 sockets over SSL	
v16.5	ras_gw_cm	Client Manager connections	The number of RAS Client Manager connections	
v16.5	ras_gw_cm_s	Client Manager SSL connections	The number of RAS Client Manager connections over SSL	
v16.5	ras_gw_wyse	Wyse connections	The number of Wyse connections	
v16.5	ras_gw_wyse_s	Wyse SSL connections	The number of Wyse connections over SSL	
v16.5	ras_gw_rdpudp	RDP UDP tunneled sessions	The number of RDP UDP connections	
v16.5	ras_gw_rdpudp_s	RDP UDP DTLS tunneled sessions	The number of RDP UDP connections over DTLS	

v16.5	ras_gw_cache_sock	Cached sockets	The number of cached sockets between Gateway and Publishing Agent	
v16.5	ras_gw_idle_threads	Idle threads	The number of idle threads on the Gateway	
v16.5.1	ras_gw_client	Client connections	The number of Parallels Client connections	
v16.5.1	ras_gw_client_s	Client SSL connections	The number of Parallels Client connections over SSL	

Parallels RAS Publishing Agent (2XController.exe)

Available since	ID	Name	Description	Notes
v16.5	ras_pa_avg_client_connection_time	Average time for client connection	The average client connection time.	
v16.5	ras_pa_avg_client_auth_time	Average time for user authentication	The average time taken to authenticate a user.	
v16.5	ras_pa_avg_client_policy_time	Average time to retrieve user policy	The average time taken to retrieve the user's policy.	
v16.5	ras_pa_avg_client_rep_time	Average time to send client telemetry	The average time taken to send client telemetry.	CEP
v16.5	ras_pa_avg_client_applist_time	Average time to retrieve user's published items	The average time taken to retrieve user's published items list.	
v16.5	ras_pa_avg_client_appicons_time	Average time to retrieve icons	The average time taken to retrieve published items icons.	
v16.5	ras_pa_avg_client_getidle_time	Average time to start up a request	The average time taken for the start up request.	

Parallels RAS RDS Agent (2XAgent.exe)

Available since	ID	Name	Description	Notes
v16.5	act_sess	Active RDS sessions	The number of active RDS Sessions.	
v16.5	disc_sess	Disconnected RDS sessions	The number of disconnected RDS Sessions.	

Index

A

About Parallels RAS - 11
About Sites - 35
About This Guide - 12
Active Directory and Domain Services Ports - 294
Add a New Client Policy - 214
Add a VDI Host - 80
Add an RD Session Host - 26
Adding a RAS Secure Client Gateway - 139
Adding a Remote PC - 111
Adding a Site to the Farm - 38
Adding an Administrator Account - 40
Adding an RD Session Host - 47
Adding and Deleting Pool Members - 101
Adding and Deleting Pools - 101
Administrator Account Permissions - 41
Advanced Settings - 224, 236
Announcement
 Parallels RAS Upcoming Version System Requirements - 18
Appendix - 289
Audio Playback - 221

C

Change RD Session Host Site Assignment - 52
Change VDI Host Site Assignment - 85
Changing HALB Appliance Password - 193
Check RAS RD Session Host Agent Status - 51
Checking Effective Access - 132
Checking the RAS Secure Client Gateway Status - 140
Checking the RAS VDI Agent Status - 82
Client Policies - 213
Client Policy Backward Compatibility - 231
Client Policy Level - 232
Common Communication Ports - 294
Common Management Tasks - 271

Common Theme Settings - 151
Conclusion - 32
Configure Client Policy Options - 226
Configure Control Settings - 229
Configure Gateway Redirection - 229
Configure HTML5 Connectivity - 145, 150
Configure HTTP Proxy Settings - 275
Configure Parallels RAS Web Portal for SafeNet - 268
Configure RAS Console Idle Sessions - 43
Configure RAS Secure Client Gateway Network Options - 142
Configure Session Settings - 215
Configure SSL Encryption on a Gateway - 142
Configure Themes - 151
Configuring a Remote PC - 113
Configuring an RD Session Host - 51
Configuring Azure MFA - 252
Configuring Deepnet - 254
Configuring DualShield 5.6+ Authentication Platform - 260
Configuring DUO - 253
Configuring Exclusion Rules - 269
Configuring Guest VMs in a Pool - 101
Configuring HALB in the RAS Console - 192
Configuring Notification Handlers - 276
Configuring Notification Scripts - 278
Configuring Notifications - 276
Configuring Parallels RAS for Deepnet - 257
Configuring Parallels RAS to Use the DualShield Authentication Platform - 264
Configuring Performance Monitor Security - 244
Configuring RAS Publishing Agents - 182
Configuring RAS Secure Client Gateway - 140
Configuring SafeNet - 267
Configuring SMTP Server Connection for Event Notifications - 281
Connect to a RAS Farm - 266

Connecting to a Parallels RAS Farm - 33
Connecting to a RAS Farm with Deepnet - 259
Connection - 216
Connection and Authentication Settings - 246
Create Branded Windows Client for Mass Distribution - 155
Creating a RAS Template - 87
Creating User Accounts on Deepnet - 258

D

Delegating Session Management Permissions - 155
Deploying a Parallels HALB Appliance - 190
Display - 217

E

Enable or Disable a Gateway - 140
Enable Support for Wyse Thin Client OS - 147
Enabling Help Desk Support - 202
Enabling or Disabling Remote File Transfer - 231
Experience - 223
Exporting and Importing Farm Settings via Command Line - 285

F

Farm Settings - 173
Filter Access to a RAS Secure Client Gateway - 147
Font Management - 197

G

Gateway Mode, Forwarding Settings, HSTS - 140
Gateway Tunneling Policies - 148
General Management Tasks - 119
General Settings - 176
General Theme Tasks - 154
Getting Started with Parallels RAS - 23
Grouping and Cloning RD Session Hosts - 56

H

HALB - 293
Hardware Requirements - 15
Hiding Toolbar Items - 166
High Availability Load Balancing - 190

How Guest VMs Are Created From a Template - 94
HTML5 Client Theme Settings - 152
HTML5 Gateway API - 167
HTML5 Gateway Level - 232

I

Install Parallels RAS - 19
Installing Parallels RAS - 15
Installing Parallels RAS Performance Monitor - 240
Installing Parallels RAS Reporting - 233
Installing RAS VDI Agent Manually - 81
Installing Remote PC Agent Manually - 112
Installing the Agent Manually - 48
Introduction - 11
Invite Users - 28
Inviting Users to Connect to Parallels RAS - 202

J

Joining Customer Experience Program - 44

K

Keyboard - 221

L

Launching Remote Applications and Desktops - 160
Licensing - 274
Load Balancing - 188
Load Balancing Advanced Settings - 189
Local Devices and Resources - 222
Log In and Activate Parallels RAS - 20
Log In to RAS Web Portal - 171

M

Main Menu Options - 159
Maintenance and Backup - 285
Manage Folders - 128
Manage Published Applications - 121
Manage Published Desktops - 124
Manage Published Documents - 125
Managing Administrator Accounts - 40, 42
Managing Guest VMs - 95
Managing Logons - 64
Managing Published Resources - 119
Managing Scanning Applications - 200

Managing Secondary Publishing Agents - 186
Managing Sessions - 62
Managing the Licensing Site - 40
Managing Universal Printing Settings - 195
Managing Universal Scanning - 199
Managing VDI Sessions - 109
Managing Windows Devices - 205
Manually Adding a RAS Secure Client Gateway - 139
Modifying VDI Host Configuration - 82
Monitoring Devices - 203

N

Network - 224

O

Open Parallels HTML5 Client - 157
Overview - 239

P

Parallels Client - 289
Parallels Client for Windows Theme Settings - 154
Parallels Client URL Scheme - 294
Parallels HTML5 Client - 150
Parallels RAS Farm and Sites - 33
Parallels RAS Performance Monitor - 239
Parallels RAS Reporting - 233
Parallels RAS Test Template Wizard - 93
Parallels RAS Web Portal - 169
Parallels Web Portal - 267
Persistent Guest VMs - 103
Port Reference - 289
Printing - 218
Problem Reporting and Troubleshooting - 287
Publish Applications - 27
Publishing a Desktop from a Guest VM - 104
Publishing a Desktop from a Remote PC - 115
Publishing a Desktop from an RD Session Host - 66
Publishing a Document from a Guest VM - 108
Publishing a Document from a Remote PC - 117
Publishing a Document from an RD Session Host - 70

Publishing a Network Folder from a Guest VM - 107
Publishing a Network Folder from a Remote PC - 117
Publishing a Network Folder from an RD Session Host - 69
Publishing a Web Application from a Guest VM - 106
Publishing a Web Application from a Remote PC - 116
Publishing a Web Application from an RD Session Host - 68
Publishing an Application from a Guest VM - 105
Publishing an Application from a Remote PC - 116
Publishing an Application from an RD Session Host - 66
Publishing App-V Applications - 71
Publishing Containerized Applications - 71
Publishing from a Guest VM - 104
Publishing from a Remote PC - 115
Publishing from an RD Session Host - 65
Publishing Turbo.net Applications - 72

Q

Quick Keypad - 135

R

RAS Agents
 RD Session Host, VDI, Guest, Remote PC - 293
RAS Console - 292
RAS Performance Counters - 296
RAS Publishing Agent - 182, 291
RAS Publishing Agent Connection Settings - 246
RAS Secure Client Gateway - 137, 290
RAS Secure Client Gateway Overview - 137
RAS Session Variables - 281
RAS Template Maintenance - 97
RAS Templates - 85
RAS VDI Agent Information - 78
RAS VDI Agent Installation Options - 78
RAS Web Portal
 Prerequisites and Installation - 169
RD Session Host Types - 46
RD Session Hosts - 46

Recovery - Add a Root Administrator - 271
Remote PCs - 111
Remote Session Settings - 247
Replicating Site Settings - 38
Resource Based & Round Robin Load
Balancing - 188
Restricting Access by Parallels Client Type
and Build Number - 249

S

Scanning - 220
Scheduling Windows Devices & Groups
Power Cycles - 212
Second Level Authentication - 249
Secondary Publishing Agents - 184
Server Authentication - 224
Server Level - 232
Set IP Address for Incoming Connections -
141
Set Up a Basic Parallels RAS Farm - 24
Settings Audit - 282
Site Information - 271
Site Settings - 272
Software Requirements - 16
Specifying a URL for Web Requests - 148
Specifying Client Settings - 134
Stage 1
Check and Install the Agent Software - 88
Stage 2
Configure the RAS Template - 90
Suggest a Feature - 288
Supported Hypervisors - 77
System Requirements - 15

T

Template Types and Guest OS Requirements
- 85
Terms and Abbreviations Used in This Guide
- 12
The Parallels RAS Console - 23

U

Universal Printing - 195
Universal Printing Drivers - 196
Universal Scanning - 199
Upgrading RAS Agents - 273
User Device Management - 202
Using a Wildcard to Filter VMs - 103

Using Deepnet - 253
Using Filtering Rules - 129
Using Instant Messaging for Administrators -
44
Using Parallels RAS Performance Monitor -
240
Using RADIUS - 250
Using SafeNet - 267
Using Scheduler - 60
Using the Remote Clipboard - 165
Using the Toolbar - 161
Using the Toolbar on Desktop Computers -
162
Using the Toolbar on Mobile Devices - 164

V

VDI and Virtual Desktops - 77
VDI Host Pool Management - 100
View and Modify RD Session Host Properties
- 52
Viewing Gateway Summary and Metrics - 149
Viewing Published Resources Hosted by RD
Session Hosts - 75
Viewing RD Session Hosts - 50
Viewing Remote PC Summary - 115
Viewing Reports - 236
Viewing Sites in the RAS Console - 36
Viewing VDI Host Summary - 109

W

Web Browsers - 290
Windows Desktop Replacement - 209
Windows Device Groups - 204
Working with DualShield - 260