Parallels Remote Application Server

Management Portal Guide

19.3

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

Contents

CHAPTER 1

Introduction

In This Chapter

Parallels RAS 19 release history

The following table lists the Parallels RAS 19 release history. Parallels RAS documentation is updated for every release. This guide refers to the latest Parallels RAS 19 release from the table below. If you are using a newer Parallels RAS release or version, please download the current version of the guide from https://www.parallels.com/products/ras/resources/.

Parallels RAS Version	Release	Date
19.0	Initial release	07/27/2022
19.0	Update 1	08/31/2022
19.0	Hotfix 1	09/16/2022
19.0	Hotfix 2	09/30/2022
19.0	Hotfix 3	10/14/2022
19.1	Update 2	11/15/2022
19.2	Update 3	07/06/2023
19.3	Initial release	10/17/2023

Overview

Parallels® RAS Management Portal is a modern web-based configuration and administration console designed for Parallels RAS administrators using a desktop/laptop computer or a mobile device to carry out configurations and day-to-day activities.

Parallels RAS Management Portal provides administrators with ability to:

- Centrally deploy, manage, and configure essential Parallels RAS components such as RD Session Hosts, Connection Brokers and Secure Gateways.
- Publish various resources from RD Session Hosts.
- Configure FSLogix Profile Container settings.
- Configure printing and scanning settings.
- Manage SSL certificates.
- Configure connection settings and MFA (Google Authenticator or other Time-based One-time Password (TOTP) apps such as Microsoft Authenticator).
- Monitor and manage user sessions.
- Manage administrative accounts and sessions
- Configure mailbox.
- Manage your license.
- Contact support and provide necessary system reports.

Note: More features and capabilities that are currently available in the desktop-based Parallels RAS Console will be included in Parallels RAS Management Portal in future releases until it becomes the main management tool for Parallels RAS.

Management of Azure Virtual Desktop capabilities included in Parallels RAS Management Portal are experimental and expected to be released in upcoming versions.

What's new

Parallels RAS 19.3

The following new features were added in Parallels RAS 19.3:

- FSLogix Office Containers support and enhanced management for FSLogix (p. 29).
- Added RADIUS as a MFA provider (p. 20).
- Ability to change user password via third-party IdPs (p. 18).

Parallels RAS 19.2

The following new features were added in Parallels RAS 19.2:

- Ability to choose the transport protocol for connections between Parallels Client and a server on RDSH, (p. 37)
- Added Microsoft Authenticator as a TOTP provider (p. 20).

CHAPTER 2

Installation and Configuration

In This Chapter

Prerequisites

RAS Management Portal can run in any modern web browser supporting HTML5 except for Internet Explorer.

Make sure your Windows Server has the following updates installed (RAS Management Portal depends on them):

- Windows Server 2012 R2: KB2999226

Newer versions of Windows Server do not require any specific updates.

The web service listens to web requests on the following ports by default:

- HTTPS: 20443
- HTTP: 20080

Installation

To enable RAS Management Portal in a RAS Farm, you need to install the RAS Web Administration Service component. The component is installed automatically when you do a clean Parallels RAS install using the "Typical" installation option. You can also install the component using the "Custom" installation option and choosing the "RAS Web Administration Service" as the component to install. For example, if you want to install RAS Management Portal on a dedicated machine, you should use the "Custom" installation option and select "RAS Web Administration Service" as a component to install.

After the RAS Web Administration Service is installed, you need to configure it. Specifically, you need to specify a RAS Farm that the RAS Management Portal will be used to manage, and you also need to configure a number of other parameters. For complete instructions, please see **Configure RAS Web Administration Service** (p. 9).

CHAPTER 3

Get Started with RAS Management Portal

In This Chapter

Log in to RAS Management Portal

To open RAS Management Portal on the machine where you've installed the RAS Web Administration Service, navigate to **Apps** > **Parallels** and click **Parallels RAS Management Portal**.

To log in to RAS Management Portal from a remote computer, enter the following URL in a web browser:

```
https://<server-address>:20443
```

The <server-address> is the FQDN or IP address of the server where the RAS Web Administration Service is installed. By default, port 20443 is used for HTTPS connections. You can change the port number if needed as described in **Configure RAS Web Administration Service (p. 9).**

On the **Welcome** page, enter your RAS administrator username and password and click **Sign in**.

Configure RAS Web Administration Service

Before you begin, you may need to configure the RAS Web Administration Service as described below:

1. In RAS Management Portal, click the "User" icon in the upper right-hand corner and choose **Configure Management Portal**.
2. You will be asked to sign in again. Note that the RAS Web Administration Service must be running on the local server for this sign in to work. This is necessary to prevent users from remote servers to enter the RAS Web Administration Service configuration pages.
3. Enter the username and password of a member of local administrators or domain administrators and click **Sign in**.

4 The **RAS Management Portal Configuration** page opens.

5 In the **RAS Farm Address** field, specify the RAS Farm address that this RAS Management Portal will manage. This is the RAS Connection Broker address installed in the Farm.

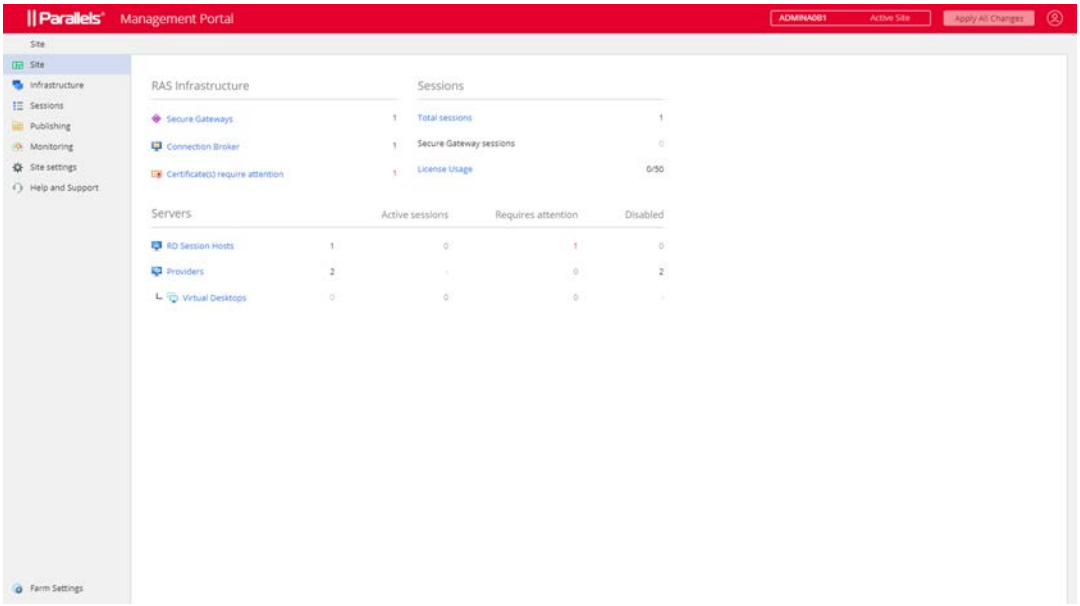
6 In the **Advanced Settings** section, specify the following:

- **Certificate**: A certificate to use for this connection. Click **Upload** to select a certificate.
- **Certificate Password:** The certificate password.
- **Port:** The port number on which RAS Management Portal listens for connections. The default port is 20443. This port number is chosen not to conflict with RAS Secure Gateway ports. You can change it to 443 (if possible), in which case the port number doesn't need to be included in the connection URL. You can also change it to any custom port. For example, the default "URL": "https://*:20443" can be changed to "URL": "http://*:20080".
- **Admin Session Timeout:** The timeout after which the admin session will be disconnected.
- **Polling Interval:** The interval at which RAS Management Portal will update the information displayed in it. You can increase this number up to 30 seconds if you have a large number of admins working at the same time and/or if you have a large number of hosts, sessions, etc.

7 Click **Save** when done.

RAS Management Portal user interface

All navigations in the RAS Management Portal start from the sidebar on the left, which lists management categories. The **Site** category is selected by default.



Categories

The following table lists all available categories that can be managed in the RAS Management Portal. The Root Administrator can see and manage all categories. Administrators of other types (Power, Custom) may need permissions to see a particular category.

Category	Description
Site	Displays the current Site overview.
Infrastructure	RAS infrastructure management, including RD Sessions Hosts, VDI, Gateways, Connection Broker, etc.
Sessions	Session management.
Publishing	Publishing and published resources management.
Monitoring	RAS Performance Monitor.
Site Settings	Connection, authentication, FSLogix, Universal printing and scanning.
Help and Support	Help and support.
Farm Settings	Displayed at the bottom of the sidebar on the left, this category manages global Farm settings, such as Administrators, Mailbox, Licensing.

Each category is described in detail later in this guide.

Admin permissions

Some categories and actions in the RAS Management Portal may not be viewed or allowed depending on the Admin permissions configured in the desktop RAS Console. For the information about how to configure administrator permissions, please refer to the **Parallels RAS Administrator's Guide**. In the guide, look for the **Administrator Account Permissions** topic. The guide is available on the Parallels website at https://www.parallels.com/products/ras/resources/.

Subcategories

Some categories have subcategories (namely **Infrastructure** and **Site Settings**). When you selected a category, the right side of the RAS Management Portal may include one or more additional panes where you can select a subcategory.

Navigation bar

Some components have their settings and information grouped by functionality (e.g. General, Properties, Sessions, etc.). When you view component properties, a navigation bar is displayed in the middle allowing you to browse these settings. When you select an item in the navigation bar, the settings are displayed in the right pane.

Breadcrumbs

As you select categories, subcategories, individual items, a breadcrumb trail is displayed at the top of the page to show where you are. To take one or more steps back, click a link in the trail.

Page header items

The page header includes the following items:

- The Farm and the current Site names. If you have more than one Site, you can select one from the drop-down list. The RAS Management Portal will switch to that site allowing you to manage the Site components.
- The "User" icon is a drop-down list with the following items: Current user name (e.g. **Administrator**); **About** (opens the About dialog); **Give feedback** (takes you to a web page where you can give feedback to Parallels); **Configure Management Portal** (p. 9), **Logout** (logs you out).
- **Apply All Changes**: This button applies changes that you've made in the RAS Management Portal to Farm components. When you create or modify components and objects, the changes are not applied to Farm components automatically and don't have any effect on the Site or Farm. When you click the **Apply All Changes** button, the changes are applied across the Farm or Site. Note that you shouldn't always click this button every time you make a change. If you are working on a task that requires multiple changes in different areas, complete all of them and then click the **Apply All Changes** button, so all changes are applied together.

Editing

When you open a view where you can modify some settings, the view is normally read-only. To enable editing, click the **Edit** button in the upper right-hand corner. The button name changes to **Save**. When done editing, click **Save**. To discard the changes, click **Cancel**.

Please note that an object that is opened for editing by an admin cannot be edited by another admin at the same time. If you try to enable editing for such an object, you will get an error with the name of the admin who has the object locked.

Edit toolbar

Some views (specifically lists) have a toolbar in the upper right-hand corner from which you can execute actions. To see a toolbar item name, hover over it with the mouse. The standard items (icons) on the toolbar are the following:

- **Show filter**: Specify a filter to show only the entries that match it.
- **Select columns**: Select table columns to display or hide.
- **Add**: Add a new entry. For example, add a new Gateway or RD Session Host, etc.
- **Refresh**: Refresh the view.

- **Ellipsis**: The ellipsis menu may have different items in different types of views. Some items have a corresponding toolbar items (e.g. **Add**, **Refresh**).

Other items may be present depending on the view you are in. For example, **Show running processes** and **Show sessions**.

Wizards

When you add a component to a Farm, a wizard usually opens which takes you through a series of pages where you specify component settings and options. A wizard has the usual **Next** and **Back** navigation buttons, and the **Cancel** button that closes the wizard and cancels the operation.

Modal dialogs

Clicking some menu and navigation bar items brings up a modal dialog. These are usually items that require you to confirm an action or enter additional information.

Object properties views

All objects (components) in the RAS Management Portal have properties. To view these properties, you select a category and a subcategory and click the object name in the list. This opens a view where object properties are displayed with its own navigation bar from which you can configure the object, perform actions. and view additional information.

CHAPTER 4

Site Category

The **Site** category gives you an overview of the current Site and displays notification about important events, such as licensing issues, RAS Agents requiring update, etc.

The main view of the Site category consists of the sections described below.

RAS Infrastructure

Displays core RAS components, such as RAS Connection Broker and RAS Secure Gateway. If you have more than one component of a particular type, the number of installed component is displayed on the right side.

You can click a component to go to the management view. You can also open a management view from **Infrastructure** category (more about it later in this guide).

Sessions

This section displays session and license usage information. To jump to the session or license management views, click the corresponding link.

Hosts

The **Hosts** section displays information about available session hosts, including RD Session Hosts and VDI (if available). You can click the available links to go to the management view for a given host type or Provider. The host information includes the number of active sessions on host, whether there's an issues with the host requiring attention, and whether the host is currently disabled.

CHAPTER 5

Farm Settings

To manage global Farm settings, click **Farm Settings** at the bottom of the sidebar.

In This Chapter

Administrators

Accounts

To add an administrator account to a Parallels RAS Farm:

1. Navigate to **Farm Settings** > **Administrators** > **Accounts**.
2. Right-click anywhere in the list and choose **Add**.
3. Specify the new account properties.

   Note that at the time of this writing, only a Root administrator can be added in the Management Portal.
4. In the **System notifications** 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.
5. Click **Create** to create the account.

To modify an account, click the account name and then click **Edit**.

To delete an account, right-click it and choose **Delete**.

Sessions

To see current administrative RAS sessions, navigate to **Farm Settings** > **Administrators** > **Sessions**.

To log off a session, right-click it and choose **Log off session**.

Mailbox

A mailbox configuration in a RAS Farm is used to send invitation emails to users to join a Parallels RAS Farm and to send event notifications to other email addresses. A Farm can have just one mailbox configured.

To configure a mailbox:

1 Navigate to **Farm Settings** > **Mailbox**.

2 Click **Edit** and specify the following:

- **Mail server:** Enter the mailbox server name. For example, mail.company.com:500
- **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.
- **Sender information:** Enter the email address.

3 Click **Save**.

Licensing

To view the Parallel RAS licensing information, navigate to **Farm Settings** > **Licensing**. The following information is displayed:

- **License Type:** The type of Parallels RAS license currently used (e.g. subscription, trial, etc.).
- **Expiration date:** License expiration date (or the number of days remaining, depending on the license type).
- **Maximum allowed concurrent users:** The maximum number of concurrent users that the current license allows.
- **Peak users:** The number of peak concurrent users to date in case of subscription, or monthly peak users and daily usage in case of SPLA license.
- **Current users:** The number of users currently connected to the Farm.

Please note that you can also see this information (and more) in your Parallels Account. For more information, please refer to the **Parallels RAS Licensing Guide**, which is available on the Parallels website.

Manage licensing

Click the **Manage License** link at the top of the **Licensing** page to open the **Manage Licensing** page.

If you have a Parallels Business account, sign in using the account credentials. If you don't have an account, click **Register**, enter the required information and click **Register**. A business account will be created for your organization. For more information about Parallels accounts and the Parallels My Account portal, please refer to the **Parallels RAS Licensing Guide**, which is available on the Parallels website at the following location: https://www.parallels.com/products/ras/resources/.

Once signed in, you can do the following on the Manage Licensing page:

- Activate the Farm using a license key included in your subscription. When you sign in using your Parallels business account, you license information is retrieved and is displayed on the screen. To activate the Farm, select a license key in the list and click **Next**.
- Activate a trial — select the **Activate a trial license** option and click **Next**.
- Deactivate the currently used license — select the **Deactivate license** option and click **Next**. The license key is released and can be used to activate a different Farm. You can re-activate the Farm at any time using the same or a different license key.

When you click **Next** in any of the scenarios above, the **Progress** page is shown displaying the progress of the operation. Once completed, the page is refreshed with results of the operation.

If you activated the Farm, you can begin managing it. If you deactivated the Farm, all controls in the Management Portal become disabled, except **Licensing**.

CHAPTER 6

Site Settings

A Site is the next level grouping in the Farm hierarchy which contains core components, session hosts, and other objects providing connection and remote application services.

To manage global Site settings, click the **Site settings** category in the sidebar.

In This Chapter

Connection and authentication

To manage connection and authentication settings, navigate to **Site Settings** > **Connection**.

Choosing authentication type

When users connect to a Site, they are authenticated before they are logged in. To configure authentication type, in the **Connection** pane, select **Authentication** and then select one of the following:

- **Credentials**. 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 in to an RDP session.
- **Smart Card**. 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.
- **Web (SAML)**. SAML SSO authentication.

Note that if smart card authentication is disabled, RAS Connection Broker will not hook the Local Security Authority Subsystem Service (LSASS). Smart card authentication can be used in Parallels Client for Windows, Mac, and Linux. Please also note that smart cards cannot be used for authentication if Parallels Client is running inside an RDP session.

A valid certificate must be installed on a user device in order to use smart cards. To do so, you need to import the certificate authority root certificate into the device's keystore.

A certificate must meet the following criteria:

- The "Key Usage" field must contain digital signature.
- The "Subject Alternative Name" (SAN) field must contain a user principal name (UPN).
- The "Enhanced Key Usage" field must contain smart card logon and client authentication.

Authentication domains

To specify a domain (or multiple domains) against which the authentication should be performed, select one of the following:

- **Specific:** Select this option and type a specific domain name.
- **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**. Select this option to use the domain specified in the Parallels Client connection properties. If no domain name is specified on the client side, the authentication is performed according to the settings above.
- **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 domain names or some other authentication related changes, you should clear cached session IDs. At this time, this can only be done from the RAS Console, where you need to click the **Clear cached session IDs** button on the **Settings** tab.

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.

Changing domain password

You can configure Parallels Client to use a custom URL for changing domain passwords.

To make Parallels Client use a custom URL for changing domain passwords:

1. Select **Use a custom link fro the "Change domain password" option**.
2. Add the link to the text field below.

Allowed devices

In the Allowed devices pane, specify whether clients must have the latest security patches in order to connect to the Farm. This option must normally be selected to protect your environment from vulnerabilities. You should only clear it if you must use an older version of Parallels Client with no security patches installed. For more information, please see the following KB article: https://kb.parallels.com/en/125112.

Multi-factor authentication

To configure multi-factor authentication (MFA), navigate to **Site Settings** > **Connection** > **Multi-factor authentication**.

When multi-factor authentication is used, users will have to authenticate through two successive stages to get the application list: native authentication (Active Directory / LDAP) and one of the following MFA:

- RADIUS (p. 20)
  - Azure MFA (RADIUS)
  - Duo (RADIUS)
  - FortiAuthenticator (RADIUS)
  - TekRADIUS
  - RADIUS
- TOTP
  - Google Authenticator (p. 22)
  - Microsoft Authenticator
  - TOTP (Time-based one-time password)
- Deepnet
- SafeNet

Please note that at the time of this writing, RAS Management Portal can only be used to add and configure RADIUS or TOTP MFA providers. To configure other providers, you'll need to use the desktop-based Parallels RAS Console.

Using RADIUS

Adding a RADIUS MFA provider

To add a RADIUS MFA provider:

1 Navigate to **Site Settings** > **Connection** > **Multi-factor authentication**.

2 Click the plus sign icon and select the provider you want to add.

3 Specify the following:

- **Name:** Name of the provider.
- **Description:** Description of the provider.
- In the **Themes** table select the Themes that will use this MFA provider.

4 Click **Next**.

5 Specify the following:

- **Display name**: Specify the name of the 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.
- **Primary server** and **Secondary server**: These two fields allow you to specify one or two RADIUS servers to include in the configuration. Specifying two servers gives you an option to configure high availability for RADIUS hosts (see below). Specify a server by entering its hostname or IP address or click the **[...]** button to select a server via Active Directory.

  When two RADIUS servers are specified, select one of the following high availability modes from the **HA mode** drop-down list: **Active-active (parallel)** means the command is sent to both servers simultaneously, the first to reply will be used; **Active-passive (failover)** means failover and timeout are doubled, Parallels RAS will wait for both hosts to reply.
- **HA mode**: See **Primary server** and **Secondary server** above. If only the Primary server is specified, this field is disabled.
- **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.

6 Click **Create** when done.

Configuring a RADIUS MFA provider

To configure a RADIUS MFA provider:

1 Navigate to **Site Settings** > **Connection** > **Multi-factor authentication**.

2 Double-click the name of the provider that you want to configure.

3 Click the **Edit** button.

4 The following categories are available for configuration:

- **General** and **Connection** categories: See above.
- **Attributes**: See https://download.parallels.com/ras/v19/docs/en_US/Parallels-RAS-19-Administrators-Guide/46769.htm.

  Note: Once created, attributes cannot be edited in RAS Management Portal. To edit attributes, the desktop-based Parallels RAS Console.
- **Automation**: See https://download.parallels.com/ras/v19/docs/en_US/Parallels-RAS-19-Administrators-Guide/46770.htm.
- **Restrictions**: See **Configure MFA rules** (p. 24).

5 Click **Save** when done.

Using Google Authenticator

This section explains how to configure Google Authenticator.

To configure Google Authenticator:

1 Navigate to **Site Settings** > **Connection** > **Multi-factor authentication**.

2 Double-click the name of the Google Authenticator provider that you want to configure.

3 Click the **Edit** button.

4 Specify the following:

- **Name:** Name of the provider.
- **Description:** Description of the provider.
- In the **Themes** table select the Themes that will use this MFA provider.
- **Display name:** The default name here is "Google Authenticator. The name will appear on the registration dialog in Parallels Client in the following sentence, "Install Google Authenticator app on your iOS or Android device". If you change the name, the sentence will contain the name you specify, such as "Install <new-name> app on your iOS or Android device". Technically, you can use any authenticator app (hence the ability to change the name), but at the time of this writing only the Google Authenticator app is officially supported.
- Modify the default TOTP tolerance if required.

- The **Enrollment** section allows you to limit user enrollment via Google Authenticator if needed. You can allow all users to enroll without limitations (the **Allow** option), allow enrollment until the specified date and time (**Allow until**), or completely disable enrollment (the **Do not allow** option). If enrollment is disabled due to expired time frame or because the **Do not allow option** is selected, a user trying to log in will see an error message saying that enrollment is disabled and advising the user to contact the system administrator. When you restrict or disable enrollment, Google authenticator or other TOTP provider can still be used, but with added security which would not allow further user enrollment. This is a security measure to mitigate users with compromised credentials to enroll in MFA.
- The **Reset User(s)** field in the **User management** section is used to reset the token that a user receives when they log in to Parallels RAS for the first time using Google Authenticator. If you reset a user, they'll have to go through the registration procedure again (see **Using Google Authenticator in Parallels Client** below). You can search for specific users, reset all users, or import the list of users from a CSV file.
- **Restrictions**: See **Configure MFA rules** (p. 24).

5 Click **Save** when done.

Using Google Authenticator in Parallels Client

Important: To use Google Authenticator or other TOTP provider, the time on a user device must be in sync with the time set on the RAS Connection Broker server. Otherwise, Google authentication will fail.

Google Authenticator is supported in Parallels Client running on all supported platforms, including mobile, desktop, and Web Client.

To use Google Authenticator, a user needs to install the Authenticator app on their iOS or Android device. Simply visit Google Play or App Store and install the app. Once the Authenticator app is installed, the user is ready to connect to Parallels RAS using two-factor authentication.

To connect to Parallels RAS:

1 The user opens Parallels Client or User Portal and logs in using his/her credentials.

2 The multi-factor authentication dialog opens displaying a barcode (also known as QR code) and a secret key.

3 The user opens the Google Authenticator app on their mobile device:

- If this is the first time they use it, they tap **Begin** and then tap **Scan a barcode**.
- If a user already has another account in Google Authenticator, they tap the plus-sign icon and choose **Scan a barcode**.

4 The user then scans the barcode displayed in the Parallels Client login dialog.

If scanning doesn't work for any reason, the user goes back in the app, chooses **Enter a provided key** and then enters the account name and the key displayed in the Parallels Client login dialog.

5 The user then taps **Add account** in the app, which will create an account and display a one-time password.

6 The user goes back to Parallels Client, clicks **Next** and enters the one-time password in the **OTP** field.

On every subsequent logon, the user will only have to type their credentials (or nothing at all if the **Save password** options was selected) and enter a one-time password obtained from the Google Authenticator app (the app will continually generate a new password). If the RAS administrator resets a user (see the **Reset Users(s)** field description at the beginning of this section), the user will have to repeat the registration procedure described above.

Configuring MFA rules

Multi-factor authentication (MFA) can be enabled or disabled for all user connections, but you can configure more complex rules for specific connections. This functionality allows you to create enable or disable MFA for the same user or computer, which will be applied depending on where the user is connecting from and from which device. Each MFA provider has one rule that consists of one or several criteria for matching against user connections. In turn, each criteria consists of one or several specific objects that can be matched.

You can match the following objects:

- User, a group the user belongs to, or the computer the user connects from.
- Secure Gateway the user connects to.
- Client device name.
- Client device operating system.
- IP address.
- Hardware ID. The format of a hardware ID depends on the operating system of the client.

Notice the following about the rules:

- Criteria are connected by the AND operator. For example, if a rule has a criteria that matches certain IP addresses and a criteria that matches client device operating systems, the rule will be applied when a user connection matches one of the IP addresses AND one of the client operating systems.
- Objects are connected by the OR operator. For example, if you only create a criteria for matching client device operating systems, the rule will be applied if one of the operating systems matches the client connection.

To configure a rule:

1 Navigate to **Site Settings** > **Connection** > **Multi-factor authentication**.

2 Double-click the name of the Google Authenticator provider that you want to configure.

3 Click the **Restrictions** link.

4 Click the **Edit** button.

5 Clear the **Inherit Defaults** option.

6 Specify criteria for the rule. You will find the following controls:

- **Allow**: specifies that the MFA provider must be enabled when a user connection matches the criteria. Click **Allow** to change it to **Deny**.
- **Deny**: specifies that the policy the MFA provider must not be enabled when a user connection matches the criteria. Click **Deny** to change it to **Allow**.
- **(+):** adds a new criteria. If you want to match a Secure Gateway, a client device name, a client device operating system, an IP address, or a hardware ID, click **(+)**.
- **is:** specifies that the MFA provider must be enabled (or not not enabled, per **Allow** and **Deny**) when a user connection matches the criteria. Click is to change it to **is not**. This control appears when at least one object is added.
- **is not:** specifies that the MFA provider must be enabled (or not not enabled, per **Allow** and **Deny**) when a user connection does not match the criteria. Click is not to change it to **is**. This control appears when at least one object is added.

You can also disable and enable criteria by clicking on the switch to the left of it.

7 Click **Save** when done.

FSLogix Profile Container

Note: If you have an existing FSLogix Profile Container configuration and would like it to be managed by Parallels RAS, please read additional instructions in **Configure managing existing profiles by Parallels RAS** (p. 27).

Microsoft FSLogix Profile Container is the preferred Profile Management solution as the successor of Roaming Profiles and User Profile Disks (UPDs). It is set to maintain user context in non-persistent environments, minimize sign-in times and provide native profile experience eliminating compatibility issues.

Beginning with version 18, Parallels provides you with the ability to integrate, configure, maintain and support FSLogix Profile Container, supporting Storage Spaces Direct, Azure Files, Azure NetApp files, based on their supported protocols such as SMB and Cloud Cache for resiliency and availability.

Supported FSLogix Profile Container releases

Parallels RAS has been tested with FSLogix Profile Container releases up to and including release 2105.

Prerequisites

FSLogix Profile Container license eligibility, which is included if you have any of the following licenses:

- Microsoft 365 E3,E5
- Microsoft 365 A3,A5, Student Use Benefits
- Microsoft 365 F1, F3
- Microsoft 365 Business
- Windows 10 Enterprise E3,E5
- Windows 10 Education A3,A5
- Windows 10 VDA per user
- Remote Desktop Services (RDS) Client Access License (CAL)
- Remote Desktop Services (RDS) Subscriber Access License (SAL)

Other prerequisites include:

- Profile Container storage configured according to FSLogix recommendations.
- GPO policies related to FSLogix must be disabled on hosts where Parallels RAS manages FSLogix settings

Install FSLogix Profile Container application in Parallels RAS

To install FSLogix Profile Container application in Parallels RAS Management Portal:

1. Navigate to **Site Settings** > **FSLogix**.
2. In the right pane, click **Edit** and select on the following installation methods:
   - **Install manually**: Use the FSLogix Profile Container application installed on a host manually (Parallels RAS will not install the FSLogix agent).
   - **Install online**: Install FSLogix Profile Container from the Microsoft web site. In the drop-down list, select one of the desired supported versions. To specify a custom URL, choose **Custom URL** and then specify a URL in the field provided. To automatically detect the latest supported version, click **Detect latest**. The latest version will be identified and added to the **Install online** drop-down list.
   - **Install from a network share**: Install the FSLogix agent you have available locally (Parallels RAS requires an official ZIP archive as provided by Microsoft).
   - **Push from RAS Connection Broker**: The latest version of the FSLogix agent is downloaded and stored on the RAS Connection Broker side to be pushed to target session hosts.

Configure a session host to use FSLogix Profile Container

Please note that at the time of this writing RAS Management Portal can only be used to configure RD Session Hosts to use FSLogix Profile Container. For other host types, please use the desktop-based RAS Console.

To configure a session host:

1. Navigate to **Infrastructure** > **RD Session Hosts**.
2. Click a host in the list and then click **Properties**.
3. In the middle pane, click **User Profile**.
4. Click **Edit** to enable editing. To override Site or Host pool defaults, clear **Inherit defaults** and specify your own settings. To modify Site or Host pool defaults, click the corresponding link and do the editing in its respective view.
5. Specify the settings according to your needs.

Configure managing existing profiles by Parallels RAS

This topic describes how to configure existing FSLogix Profile Containers to be managed by Parallels RAS. FSLogix Profile Container configuration defines how and where the profile is redirected. Normally, you configure profiles through registry settings and GPO. Parallels RAS gives you the ability to configure profiles from the Parallels RAS Console or RAS Management Portal without using external tools.

Before you begin

Before you configure FSLogix Profile Containers in Parallels RAS, make note of the following:

- You don't have to change the profiles themselves; existing profiles stay the same.
- You can keep using your existing FSLogix Profile Container locations, such as SMB network shares or Cloud Cache.

Preliminary steps

Perform the following preliminary steps:

1. Back up your existing profiles. It is highly unlikely that profile data can be lost or corrupted, but it is best practice to have a valid backup prior to any change in profile configuration.
2. Turn off the GPO configuration of FSLogix Profile Containers. This step is important because you cannot have both GPO and Parallels RAS management of FSLogix profiles enabled at the same time.
3. Before configuring FSLogix profiles for a server in a RAS Farm, make sure there are no user sessions running on the server. As a suggestion, you can make the transition in a maintenance window out of working hours.

Replicate GPO and FSLogix configuration

To configure existing FSLogix Profile Containers in Parallels RAS, you need to replicate your existing GPO to the FSLogix configuration in Parallels RAS. This can be done in the Parallels RAS Console or the Parallels Management Portal.

To configure profiles in the RAS Management Portal:

1. Navigate to **Infrastructure** > **RD Session Hosts**.
2. Click a host in the list and then click **Properties**.
3. In the middle pane, click **User Profile**.
4. In the **Location of profile disks** list box, specify existing SMB or cloud cache locations where you keep your FSLogix profiles. Also, specify the profile disk format, allocation type, and default size.
5. In the middle pane, click **Users and Groups**, **Folders**, and **Advanced** items to configure the rest of FSLogix settings you may have on your servers, such as user exclusions, folder exclusions, and others.

Please note that at the time of this writing RAS Management Portal can only be used to configure RD Session Hosts to use FSLogix Profile Containers. For other host types, please use the desktop-based RAS Console (described below).

To configure profiles in the RAS Console:

1. Open the **User profiles** tab on a host, Site defaults, or Template **Properties** dialog.
2. In the **Location of profile disks** list box, specify existing SMB or cloud cache locations where you keep your FSLogix profiles. Also, specify the profile disk format, allocation type, and default size.
3. Click the **Additional settings** button and configure the rest of FSLogix settings you may have on your servers, such as user exclusions, folder exclusions, and others.

Recommendations and testing

When performing steps in the previous section, do not configure multiple (or all) servers in a RAS farm right away. Begin with a single server (e.g. an RD Session Host) and then test it with a single user connection. After that, configure some other servers and test the same user logging in to multiple servers consecutively to confirm the profile is loaded and personalization is retained irrespective of a session host. If all is good, configure other host, host pools, or Site defaults.

Your RAS users can now connect to Parallels RAS using pre-existing FSLogix Profile Containers, which are now managed centrally through Parallels RAS.

Configure Site defaults and hosts for FSLogix

To configure FSLogix:

1 Do one of the following:

- To configure Site defaults, navigate to **Infrastructure > Host pools > RD Session Hosts > Properties > Site defaults > User Profile**.
- To configure host pools, navigate to **Infrastructure > Host pools > <Host pool name> > Properties > User Profile**.
- To configure individual hosts, navigate to **Infrastructure > RD Session Hosts > <Host name> > Properties > User Profile**.

2 If you want to use Profile Containers, go to **User Profile > FSLogix - Profile Containers**:

- **Users and Groups**: Specify include and exclude user and group lists. By default, Everyone is added to the FSLogix profile include list. If you want some user profiles remain local, you can add those users to the exclude list. Users and group can exist in both lists but exclude takes priority.
- **Folders**: Specify include and exclude lists for folders. You can select from common folders or you can specify your own. Please note that folders must reside in user profile path.
- **Disks**: Specify the settings of the profile disk. **Location type**: Select a location type for profile disks (SMB Location or Cloud Cache) and then specify one or more locations. **Location of profile disks**: Location(s) of profile disks. These are the locations of VHD(X) files (the VHDLocations setting in the registry as specified in the FSLogix documentation). **Profile disk format**: Select from VHD or VHDX according to your requirements. VHDX is a newer format and has more features. **Allocation type**: Select **Dynamic** or **Full**. This setting is used in conjunction with the **Default size** setting (see below) to manage the size of a profile. Dynamic causes the profile container to use the minimum space on disk, regardless of the allocated Default size. As a user profile is filled with more data, the amount of data on disk will grow up to the size specified in Default size, but will never exceed it. **Default size**: Specifies the size of newly created VHD(X) in megabytes.
- **Advanced**: This tab allows you to modify advanced FSLogix registry settings. By default, the settings are disabled. To enable a setting, select the checkbox in front of its name. A description for each setting is provided in the RAS console. For further information regarding FSLogix Profile Containers configurations, visit https://docs.microsoft.com/en-us/fslogix/profile-container-configuration-reference.

3 If you want to use Office Containers, go to **User Profile > FSLogix - Office Containers**:

- **Users and Groups**: Same as above.
- **Disks**: Same as above.
- **Advanced**: Same as above.

4 If you want to configure Cloud Cache, go to **User Profile > FSLogix - Cloud Cache.** For more information about these settings, see https://learn.microsoft.com/en-us/fslogix/reference-configuration-settings?tabs=ccd#fslogix-settings-profile-odfc-cloud-cache-logging.

5 If you want to configure logging, go to **User Profile > FSLogix - Logging.** For more information about these settings, see https://learn.microsoft.com/en-us/fslogix/reference-configuration-settings?tabs=ccd#fslogix-settings-profile-odfc-cloud-cache-logging.

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.

To configure Universal Printing, navigate to **Site Settings** > **Universal Printing**.

Printer settings: Rename 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`.

You can change the default printer renaming pattern by specifying a new pattern in the **Printer rename pattern** field. To see the predefined variables that you can use, click the **Add variable** button. 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 some other characters in a printer renaming pattern. For example, you can define the following commonly used pattern:

`Client/%CLIENTNAME%#/%PRINTERNAME%`.

Using the above pattern (and the user named Alice from the earlier example), 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 settings: 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, set the **Printer retention** option to **Enable printer retention optimization**.

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 in the **Drivers** section:

1. 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 type of driver a printer is using to use redirection privileges.
   - **Allow redirection of printers using one of the listed drivers**: Select this option and add the "allowed" drivers to the list. To add a driver, click the plus-sign icon and type the driver name.
   - **Don't allow redirection of printers that use one of the listed drivers**: This is probably the most useful option in the context of this feature. The printers that use drivers specified in the list will be denied redirection privileges. All other printers will be allowed to use redirection.
2. To delete a printer driver from the list, click the minus-sign icon.

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).

Fonts

Fonts need to be embedded so 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.

Excluding fonts from embedding: To exclude a specific font type from being embedded, select it in the list. To add one or more fonts, slick the plus-sign icon.

Auto install fonts: To automatically install a specific font type on servers and clients, click the plus-sign icon in the **Auto install fonts** section.

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.

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.

To configure Universal Scanning, navigate to **Site Settings** > **Universal Scanning**.

Universal Scanning uses WIA and TWAIN 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.

Note: The server feature **Desktop Experience** is required in order to enable both WIA and TWAIN scanning on RD Session Hosts.

By default, the Universal Scanning driver is automatically installed when a host server is added to a RAS Farm and the Agent software is installed on it.

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.

Adding a scanning application

TWAIN applications that will use the Universal Scanning feature have to be added to the TWAIN configuration. This way they will 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. Select the **TWAIN** category.
2. In the right pane, click the plus-sign icon and type the application executable name.

Note: Some applications might use different or multiple executables. Make sure that all required executables are added to the list of scanning applications.

To delete a scanning application from the list, select it in the list and click minus-sign icon.

Note: If you delete an application from the list, the installation of the application will not be affected.

CHAPTER 7

Infrastructure

In This Chapter

RD Session Hosts

RD Session Hosts are used to host published resources (applications, desktops, documents, etc.) in a RAS Farm.

To manage RD Session Hosts, navigate to **Infrastructure** > **RD Session Hosts**. The main list displays existing RD Session Hosts. To perform management functions (add, delete, show processes and sessions, etc), use the ellipsis menu, context menu (right-click) and in some cases action icons.

Add an RD Session Host

To serve published resources to users, an RD Session Host must have the Remote Desktop Services (RDS) role installed.

To add an RD Session Host to a Farm:

1. Navigate to **Infrastructure** > **RD Session Hosts**.
2. Right-click anywhere in the list and choose **Add** (you can also choose **Add** from the ellipsis menu or click the plus-sign icon).
3. Select a host (or multiple host) from the displayed list or click the **Browse AD** button and browse for a host.
4. Click **Next**.
5. On the next page, specify the following options:

- **Add firewall rules**. Add firewall rules required by Parallels RAS in Windows running on the host. See **Port Reference** for details.
- **Install RDS Role**. Install the RDS role on the host if it's not installed. You should always select this option.
- **Enable Desktop Experience**. Enable the Desktop Experience feature in Windows running on the host. 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 host if necessary. You can restart the host manually if you wish.
- **Add host(s) to host pool**. Add the host (or hosts) to a host pool. Select the desired host pool in the list box located below this option or create a new host pool by typing a name and clicking **Create**. For the information on how to create a host pool, see **RDSH host pools** (p. 46).

6 Click **Next**.

7 In order for end users to access published resources on the RD Session Host, they must be added to the Remote Desktop Users group in Windows running on the host. This can be done one of the following ways:

- Adding each user or group directly on the host using standard Windows administrative tools.
- Adding users or groups through Active Directory.
- Using the wizard page described below, which is provided for your convenience.

If you already added your users to the Remote Desktop Users group on the given host (or if for any reason you want to use one of the other methods listed above), you can simply click **Next** and skip this page.

To add users to the Remote Desktop Users group using the wizard, click **Browse** and specify a user or a group.

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

9 If the host doesn't have RAS RD Session Host Agent installed, you'll see a dialog asking for remote installation credentials. Type a username and password that can be used to remotely install the agent software on the host. Click **Submit** and follow the onscreen instructions.

10 When the installation is finished, click **Done**. Note that if the agent cannot be installed, you can still add a host to the Farm, but you will not be able to use it. You can always installed the agent later.

On successful installation, the host will appear in the **RD Session Hosts** list.

Additional information

To learn how to publish resources from an RD Session Host, see **Publishing** (p. 81).

To learn how to configure and manage an RD Session Host:

- **Configure an RD Session Host** (p. 36)
- **Manage an RD Session Host** (p. 41)

Configure an RD Session Host

To configure an RD Session Host:

1 Navigate to **Infrastructure** > **RD Session Host**.

2 Click a host in the list to open the view displaying the host information.

3 In the navigation bar, click **Properties** (at the bottom). Configure the RD Session Host as described below.

Using Site or host pool defaults

RD Session Host properties are split into categories, which are displayed in the middle pane. Each category has its own set of properties. All categories, except **General** and **Scanning**, have one common link: **Site Defaults** or **Host pool Defaults**, which allows you to view default settings. If you want the properties in a particular category to inherit default settings, select the **Inherit Defaults** option. When you do this, the default settings will be inherited from one of the following:

- **Host pool defaults** if the host is assigned to an RD Session Host host pool. Pools are described in **Grouping and Cloning RD Session Hosts**.
- **Site defaults** if the host is not assigned to an RD Session Host host pool. Note that a host pool may also inherit Site defaults, but this can be overridden in the host pool properties dialog where you can specify custom settings for a host pool.

Click the **Host pool Defaults** or **Site Defaults** link (whichever applies) to open the host pool or Site default properties pane. To modify default settings (if needed), click **Edit**.

General

In the navigation bar, select **General** and specify the following:

- **Enable Host in site**: Enable or disable the host. A disabled host cannot serve published resources to users. When you disable a host, its name becomes grayed out in the main list.
- **Host:** Specifies the host name.
- **Description:** Specifies the host 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** category to configure the agent.

To use default settings, select the **Inherit default settings** option. See **Using Site or Group defaults** (p. 36) for details. To specify custom settings for a given host, clear the **Inherit default settings** option and specify agent properties as follows.

Application session lingering

Setting in this section apply only to sessions with no running applications.

- **Disconnect active session after**: Specifies the amount of time each session remains connected in the background after the user has closed a remote application. This option is used to avoid unnecessary reconnections with the host.
- **Logoff disconnected session after**: This setting allows you to control how long it takes for a session to be logged off after it is marked as "disconnected".

Other settings

- **Port**. Specifies a different remote desktop connection port number if a non-default port is configured on the host.
- **Max sessions**. Specifies the maximum number of sessions.
- **Allow Client URL/Mail redirection**. When a user tries to open a URL or an HTML Mailto link in a remote application, the link can be redirected to the client computer and open in a local default application (a web browser or email client) instead of an application on the remote host. This option allows you to enable or disable the redirection. You can choose from the following options:

  a **Enabled** — select this option to enable the redirection and then select the **Support Windows Shell URL namespace objects** option (bellow the drop-down box). This is the default redirection configuration that works in most common scenarios. The Shell URL namespace objects support means that Parallels RAS can intercept actions in published applications that use Shell namespace API to open links, which is a standard behavior in most applications. The ability to disable the support for Shell URL namespace objects is for compatibility with older versions of Parallels RAS. You may disable this option if you want the behavior of an older version of Parallels RAS (RAS v16.2 or earlier).

  b **Enabled (Replace Registered Application)** — this option uses an alternative method of redirecting a link. It replaces the default web browser and mail client with "dummy" apps on the remote host side. By doing so, it can intercept an attempt to open a link and redirect it to the client computer. You may try this option if the default option above doesn't work with your published application.

  c **Disabled** — this option disables URL/Mail redirection, so URL or Mailto links always open on the remote host.

- **Support Windows Shell URL namespace object**:
- **Drag and drop**. Allows you to set how the drag and drop functionality works in Parallels Clients. You can select from "Disabled" (no drag and drop functionality at all), "Server to client only" (drag and drop to a local application, but not in the opposite direction), "Client to server only" (drag and drop to a remote application only), "Bidirectional" (default). Note that this option has changed since Parallels RAS 17.1. In the past, it was a checkbox that would enable or disable drag and drop which worked in the "Client to server only" mode. When upgrading from an older version of Parallels RAS, and if the checkbox was enabled, the "Client to server only" option is selected by default. If the option was disabled, the "Disabled" option will be set. You can change it to any of the new available options if you wish.

  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.

- **Preferred Connection Broker**. Select a Connection Broker 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 Connection Broker.
- **Allow 2XRemoteExec to send command to the client**. Select this option to allow a process running on the host to instruct the client to deploy an application on the client side. See the **Using RemoteExec** subsection below for more information.
- **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 host. Disabling application monitoring stops the WMI monitoring to reduce CPU usage on the host and network usage while transferring the information to RAS Connection Broker. If the option is enabled, the collected information will appear in a corresponding RAS report. If the option is disabled, the information from this host will be absent from a report.
- **Manage RDP transport protocol**. Select the transport protocol that will be used for connections between Parallels Client and a host.
- **Allow file transfer command (Web and Chrome clients)**. Enables file transfer in a remote session. Select a desired option in the drop-down list. For details, see **Configuring remote file transfer** below.
- **File transfer location.** A UNC path to a folder to be used as the default upload location. This path will also be used as the default source location when a user tries to download a file from a remote host. You can select from one of the locations predefined in the drop-down list or you can specify your own. Standard Windows environment variables, such %USERNAME%, %USERDOMAIN%, %USERPROFILE%, can be used. If the location is not found during an upload or download operation, the standard (default) download location will be used.
- **Do not allow to change location.** Prohibits the user to change the UNC path specified in the **File transfer location** field. If the option is enabled, the user cannot select a different location while trying to upload or download a file. If the option is cleared, the user can specify a different location.

- **Enable drive redirection cache**. Improves user experience by making file browsing and navigation on redirected drives much faster.

Using 2XRemoteExec

2XRemoteExec is a feature that facilitates the hosts 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
`-s`	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.
`-t`	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.
`-?`	Shows a help list of the parameters that 2XRemoteExec uses.
`"Path for Remote Application"`	The Application that will be started on the client as prompted from the host.

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"
```

Configuring remote file transfer

Parallels RAS provides end users with the ability to transfer files remotely to and from a remote host.

Note: At the time of this writing, file transfer is supported in Parallels User Portal and Parallels Client for Chrome only. Note that bidirectional file transfer is supported in Parallels User Portal only.

To make the remote file transfer functionality flexible, Parallels RAS allows you to configure it on the following three levels:

- RD Session Host, Provider, or Remote PC
- User Portal
- Client policy

File transfer settings that you configure on each level take precedence in the order listed above. For example, if you enable file transfer on a User Portal, 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 User Portal. As another example, you can enable file transfer on an RD Session Host and then disable it for a particular Client policy (or a User Portal). This way you can control which clients can use file transfer and which cannot.

To configure remote file transfer:

1 In the **Allow file transfer command** drop-down list, select one of the following options:
   - **Disabled**: Remote file transfer is disabled.
   - **Client to Server**: Transfer files from client to server only.
   - **Server to Client**: Transfer files from server to client only.
   - **Bidirectional**: Transfer files in both directions.

2 In the **File transfer location** field, specify a UNC path to a folder to be used as the default upload location. This path will also be used as the default source location when a user tries to download a file from a remote server. Standard Windows environment variables, such %USERNAME%, %USERDOMAIN%, %USERPROFILE%, can be used. If the location is not found during an upload or download operation, the standard (default) download location will be used.

3 The **Do not allow to change location** option prohibits the user to change the UNC path specified in the **File transfer location** field. If the option is enabled, the user cannot select a different location while trying to upload or download a file. If the option is cleared, the user can specify a different location.

Important: Please note that the **Do not allow to change location** option cannot prevent the user from accessing the specified remote location directly. For example, a user can try to upload a file, note the default location's UNC path (to which he/she has access), then open it in File Explorer and copy it to any folder in his/her profile. To prevent such a scenario from happening, you need to implement additional measures to control locations other than the location that you specify here.

User Profile

If you would like to configure user profiles for the host based on the FSLogix technology, select **FSLogix** in the Technology drop-down list and specify the settings according to your needs. For the information about how to configure FSLogix Profile Container in Parallels RAS, see **FSLogix Profile Container** (p. 25).

Desktop Access

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

To use default settings, select the **Inherit default settings** option. See the **Using default settings** subsection above.

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

1. 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 **Host Properties** and **Default Host Properties** dialogs.
2. Click the plus-sign icon.
3. Select the desired users. To include multiple users, separate them by a semicolon.
4. Click **OK**.

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 host.

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.

Printing and Scanning

Printing

The **Printing** category allows you to configure the renaming format of redirected printers. The format may vary depending on which version and language of the host you are using.

To use default settings, select the **Inherit default settings** option. See the **Using default settings** subsection above.

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

Select the **Remove session number from printer** option to exclude the corresponding information from the printer name.

Scanning

In the **Scanning** view, configure which imaging interfaces should be enabled on the host(s). Select from WIA, TWAIN, or both.

Manage an RD Session Host

To perform RD Session Host management tasks:

1 Navigate to **Infrastructure** > **RD Session Hosts**.

2 Click a host to open the host properties view.

3 Use the navigation bar to switch between different views where you can view additional information and perform actions. These views are described below.

Overview

The **Overview** screen displays the following information:

- The **Information** section displays the RD Session Host information similar to what is shown on the main RD Session Host list but in one convenient view.
- The **Actions** section lists actions that you can perform on a host (see below). Please note that you can also perform actions from the main RD Session Host list view by selecting a host and choosing an option from the ellipsis menu.

You can perform the following actions on an RD Session Host:

- **Message all**: Send a message to users connected to the host.
- **Disconnect all**: Disconnect all current users.
- **Logoff all sessions**: Log off all current sessions.
- **Update agent**: Update the RD Session Host Agent, if required.
- **Disable agent**: Temporarily disable the agent.

The **Control** sub-menu contains the following items:

- **Enable logons**: Enables logons from client sessions, but not from the console. This option performs the same action as the `change logon /enable` command.
- **Disable logons**: Disables subsequent logons from client sessions, but not from the console. Does not affect currently logged on users. This option performs the same action as `change logon /disable` command.
- **Drain**: Disables logons from new client sessions, but allows reconnections to existing sessions. Drain is kept even after reboot until the admin enables logons.

  Note that while a host is in drain mode, administrators may still log on to the physical console or remotely log on using the /admin or /console command-line option for MSTSC. This allows administrators to remotely maintain the RDS host via **Tools** > **Remote Desktop.**
- **Drain until reboot**: Disables logons from new client sessions until the computer is restarted, but allows reconnections to existing sessions. Drain is kept until the host is restarted. Same action as the `change logon /drainuntilrestart` command.
- **Cancel pending reboot (scheduler)**: Cancel pending reboot.
- **Cancel disabled state (scheduler)**: Cancel disabled state.
- **Install RDS role**: Allows to install the RDS role on the host.
- **Reboot**: Reboot the host.

- **Shutdown**: Shut down the host.

The **Logs** sub-menu contains the following items:

- **Configure**: Allows you to configure logging. For the explanation of log levels, please see below.
- **Retrieve**: Retrieves a ZIP archive containing the log files to the specified location.
- **Clear**: Clears all existing logs.

The available log levels are:

- **Standard**: This is the standard log level that records only the most important events. Unless you are asked by Parallels RAS support to use one of the log levels described below, you should always use this one.
- **Extended**: This logging involves more information than the standard logging, but it slows down the system because of the additional information that it needs to collect.
- **Verbose**: Verbose logging involves even more information than the extended logging and can slow down your system significantly.

Please note that to avoid degraded performance, extended and verbose logging should only be enabled for a limited time period (enough to collect the necessary information for analysis). You can set this time period using **Reset to the standard level after** option. The default value is 12 hours. In specific cases, a Parallels support engineer will advise you whether this time period should be set to a different value. Once this time period is over, the log level will be reset back to standard.

The remaining items include:

- **Assign to host pool**: Assigns the host to a host pool.
- **Remove from host pool**: Removes a host from a host pool.
- **Refresh**: Refreshes the host information displayed on the screen.
- **Site Defaults**: Opens the **RDSH site defaults** screen where you can view and configure site defaults.
- **Delete**: Deletes the host from the RAS Farm.

Active Sessions

To view and manage active session on the RD Session Host, click **Active Sessions** in the navigation bar. To see the detailed session information, click the user name in the list. This opens the **Session Info** view. For a detailed description of session metrics, please see **Session information** (p. 75).

To perform an action on a session (or multiple sessions), select it in the list and click the ellipsis menu. Choose from one of the following items:

- **Show session info**: Opens the Session Info view.
- **Message**: Send a message to the session owner.

- **Disconnect**: Disconnect the session.
- **Log off**: Log off the session.
- **Show resources**: Opens a view displaying running resources.
- **Show running processes**: Opens a view displaying running processes.
- **Monitoring settings**: Opens **a** dialog where you can configure monitoring settings to highlight values in session metrics for RD Session Hosts. The dialog lists available metrics and allows you to set Warning and Critical thresholds for a given metric. To set a threshold, select the checkbox in front of a metric name and specify the desired values. During the RAS Farm operation, when a threshold is reached, a session metric value is highlighted as follows: Warning threshold — orange; Critical threshold — red.

  To reset values for a given threshold, select it and choose **Reset** from the ellipsis menu (or right-click > **Reset**). You can also enable or disable threshold color coding for a metric. To do so, select a metric and choose **Enable** or **Disable** from the ellipsis menu.
- **Refresh**: Refreshes the list.
- **Export**: Exports the information to a CSV file.

Running Resources

To view running resources for an RD Session Host, click the **Running Resources** item in the navigation bar. To see the detailed resource information, click the resource name. This opens a view displaying the basic resource information (ID, name, target, etc) and the corresponding session information. For the detailed information about session metrics, please see **Session information** (p. 75).

To perform an action on a resource, select it in the list and click the ellipsis menu. Choose from one of the following:

- **Message**: Send a message to the session owner.
- **Disconnect**: Disconnect the session.
- **Log off**: Log off the session.
- **Show running processes**: Opens a view displaying running processes.
- **Show user session**: Open a view displaying the information about the session.
- **Show information**: Opens a view displaying the resource information.
- **Monitoring settings**: See the description in **Active Sessions** (p. 43).
- **Refresh**: Refreshes the list.
- **Export**: Save the list into a CSV file.

Running Processes

To view running processes for an RD Session Host, click the **Running Processes** item in the navigation bar. This opens a view displaying all running processes.

To kill one or multiple processes, select them in the list and chose **Kill processes** from the ellipsis menu. To refresh the list, choose **Refresh**.

Troubleshooting

For troubleshooting information and tasks, select **Troubleshooting** in the navigation bar.

The data displayed in the **Troubleshooting** view is retrieved by the RAS Management Portal directly from the RD Session Host, not through the RAS Connection Broker. This view can show data important to troubleshoot issues with the RAS RD Session Host Agent even if the agent cannot be reached by the RAS Connection Broker or is currently registered with a different RAS Connection Broker.

The following data is displayed:

- **Host**: The RD Session Host name.
- **Agent**: Agent status (e.g. OK).
- **Version**: Agent version.
- **RDS role**: Whether RDS role is enabled on the RD Session Host.
- **OS type**: Operating system type installed on the host.
- **Status**: Displays a long version of the agent status. If the agent is OK, it will say so. If there's an issue, this field explains what is wrong with the agent. You can use this information to troubleshoot the issue.

You can also perform the following actions in the **Troubleshooting** view:

- **Retrieve logs**: Retrieve host logs as a single ZIP archive.
- **Configure logs**: Allows you specify a log level for Parallels RAS Components. Note that you should use Extended and Verbose logging for troubleshooting only. When selecting one of these levels, you can also set the time period after which the log level will go back to Standard.
- **Clear logs**: Clear all existing logs.
- **Reboot agent**: Reboot the RAS RD Session Host Agent.
- **Uninstall agent**: Uninstall the agent.
- **Refresh**: Refresh the agent information.

RDSH groups

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

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

- They simplify the management of published resources and are highly recommended in multi-host environments.
- They allow you to use RD Session Hosts created from a template by utilizing the VDI infrastructure. More on this later in this section.

Note that an RD Session Host can be a member of one host pool only. You cannot add the same host to multiple host pools.

Creating a host pool

To create an RDSH host pool:

1. Navigate to **Infrastructure** > **RD Session Hosts** > **Host pools**.
2. Choose **New host pool** from the ellipsis menu (or click the plus-sign icon).
3. Type a host pool name and press **Enter**.
4. Click the new host pool name in the list to open the host pool editing screen.
5. Click **Properties** in the middle pane and configure the host pool. Settings here are similar to settings of an individual RD Session Host. See **Configure an RD Session Host** (p. 36).

Using host pool defaults

RD Sessions Hosts assigned to a host pool have various settings that they can inherit from the host pool defaults. This makes it simpler to configure a single set of settings for all hosts instead of configuring each host individually. A Site also has its own default settings (Site defaults). Moreover, an RD Session Host host pool can inherit these Site defaults. This gives you the following choices when inheriting default settings by an RD Session Host:

- Configure Site defaults and make the host pool inherit these settings. The RD Session Hosts assigned to the host pool will therefore also inherit Site defaults. This is the default scenario for a new host pool.
- Configure default settings for a given host pool. This way you can have multiple host pools, each having its own host pool defaults (different from Site defaults). Therefore, the hosts assigned to a host pool will inherit the host pool defaults.

Virtual Desktops Infrastructure

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 numerous virtualization technologies, including hypervisor and cloud-based platforms.

Parallels RAS VDI also includes the Template functionality, which gives you the ability to create a template from a preconfigured guest VM (virtual machine) and then automatically clone hosts from it.

Please note that at the time of this writing, the VDI functionality in Parallels RAS Management Portal is limited to viewing existing virtual desktops, recreating hosts, and performing power operations on them. For other VDI tasks, please use the desktop-based Parallels RAS Console.

Virtual desktop list

To see the list of virtual desktops that exist in the Farm, navigate to **Infrastructure** > **Virtual Desktops**.

To add or remove columns to/for the **Virtual Desktops** table, click the gear icon and select or clear desired columns.

To perform a power operation, select a virtual desktop and then choose one of the following from the ellipsis menu:

- **Start**
- **Stop**
- **Restart —** The Restart operation (graceful) has a 10 min timeout. If not completed during this time, the Reset operation (forced) will be used.
- **Reset**
- **Suspend**
- **Refresh**
- **Recreate** — see more info below.

Recreating a host

If something happens to a template-based host 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 host, will be affected. Another reason for recreating a host is to apply changes made to the 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 host was created from an RD Session Host template and was already assigned to an RD Session Host host pool, it cannot be recreated.

When you recreate a host:

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

See also

Providers (p. 73)

Certificates

The Parallels RAS Management Portal includes a certificate management interface that allows you to manage all of your SSL certificates in one place.

Certificates are managed on a Site level. Once a certificate is added to a Site, it can be used with any RAS Secure Gateway or HALB that also exist in this Site.

To manage certificates, navigate to **Infrastructure** > **Certificates**. The **Certificates** list displays existing certificates. When you install Parallels RAS, the <Default> self-signed certificate is created automatically, so you will see at least this certificate in the list. The default certificate is also automatically assigned to all new RAS Secure Gateways and HALB.

The subsequent sections describe certificate management tasks in detail and provide additional certificate information and instructions.

Generate a self-signed certificate

To generate a self-signed certificate, navigate to **Infrastructure** > **Certificates**. Choose **Add** > **Generate self-signed certificate** from the ellipsis menu and specify the following options:

- **Name:** Type a name for this certificate. This field is mandatory.
- **Description**: An optional description.
- **Usage**: Specify whether the certificate should be used for RAS Secure Gateways or HALB, or both. This selection is mandatory.
- **Key size:** The certificate key size, in bits. Here you can select from the predefine values. The default is 2048 bit, which is the minimum required length according to current industry standards.
- **Expire in**: The certificate expiration date.

- **Country code**: Select your country.
- **Full state or province:** Your state or province info.
- **City:** City name.
- **Organization:** The name of your organization.
- **Organization unit:** Organizational unit.
- **E-mail:** Your email address. This field is mandatory.
- **Common name:** The Common Name (CN), also known as the Fully Qualified Domain Name (FQDN). This field is mandatory.
- **Subject Alternative Names:** Add one or more subject alternative names (SANs). Note that because mobile Parallels Client don't support the Subject Alternative Name field, it is recommended to choose a common name that most mobile devices will be using.

Click **Generate** to generate the certificate. When done, the certificate will appear in the **Certificates** list with the **Status** column indicating **Self-signed**.

To view and modify certificate properties:

1. In the **Infrastructure** > **Certificates** view, click the certificate name.
2. In the right pane, review the certificate properties in the **Information** section.
3. In **Actions** section, you can enable or disable the certificate. You can also export a certificate to a file (p. 52). If you wish to delete the certificate, click **Delete**.
4. To modify some of the certificate properties, click **Properties** in the middle pane.
5. Click **Edit** in the upper left-hand corner to modify the settings if needed. You can change the certificate name and description and you can also change whether the certificate should be used for Gateways, HALB, or both.

Generate a certificate signing request (CSR)

To generate a CSR:

1. Navigate to **Infrastructure** > **Certificates**.
2. Choose **Add** > **Generate** a certificate request from the ellipsis menu and specify the required information. The information is exactly the same as described in **Generate a self-signed certificate** (p. 48).
3. After entering the information, click **Generate**. The certificate information view will open.
4. Click **Certificate Request** in the middle pane to view the request data. Copy and paste it into a text editor and save the file for your records. This view also also allows you to import a public key at this time. You can submit the request to a certificate authority now, obtain the public key, and import it without closing the view, or you can do it later.

To submit the request to a certificate authority and import a public key:

1 If the certificate request view is closed, open it (click the request in the main list and click **Certificate Request**).

2 Copy the request and paste it into the certificate authority web page (or email it, in which case you will need to come back to this view later).

3 Obtain the certificate file from the certificate authority.

4 Click the **Import public key** button and finalize the certificate registration by specifying the key file and the certificate file.

Let's Encrypt certificates

Working with Let's Encrypt certificates

Let’s Encrypt is a global Certificate Authority (CA). This organization is a non-profit and does not charge fees for their certificates. Each certificate is valid for 90 days. RAS Console allows you to issue, automatically renew and revoke Let's Encrypt certificates.

Issuing a Let's Encrypt certificate

To issue a new Let’s Encrypt certificate:

1 Navigate to **Infrastructure > Certificates**.

2 Click the ellipsis menu (the **[...]** icon) and choose **Let's Encrypt Settings**.

3 Select the **I have read and accept Let's Encrypt EULA** option.

4 In the **Expiration emails** field list specify the email addresses that will receive notifications from Let’s Encrypt.

5 Optionally, change the time when certificates are renewed automatically in the **Automatically renew certificates before expiration** field.

6 Navigate back to **Infrastructure > Certificates**.

7 Choose **Add > Issue Let's Encrypt** certificate from the **[...]** menu and specify the following options:

- **Name:** Name of the certificate.
- **Description:** Description of the certificate.
- **Usage:** HALB and/or Secure Gateway.
- **Key size:** Key size.
- **Country code:** Code of your country.
- **Full state or province:** Name of your state or province.
- **City:** Your city.
- **Organization:** Name of your organization.

- **Organization unit:** Name of your organization unit.
- **E-mail**: Email address of your organization.
- **Common name:** Valid domain name of a HALB or Secure Gateway.
- **Alternative names:** Valid domain names of HALBs or Secure Gateways.

8 Click **Issue certificate**.

Renewing a Let's Encrypt certificate manually

To manually renew a Let's Encrypt certificate:

1 Navigate to **Infrastructure > Certificates**.

2 Select the certificate that you want to renew.

3 Select **Control > Renew** from the **[...]** menu.

Revoking a Let's Encrypt certificate

To revoke a Let's Encrypt certificate:

1 Navigate to **Infrastructure > Certificates**.

2 Select the certificate that you want to renew.

3 Select **Control > Revoke** from the **[...]** menu.

How Parallels RAS requests certificates from Let's Encrypt

When you create a new Let's Encrypt certificate using Parallels RAS, the following process is carried out:

1 Parallels RAS Primary Connection Broker that hosts the licensing role makes the initial request to the Let's Encrypt server to create an account.

2 Account creation confirmation is received. Parallels RAS creates a CSR and sends it to the Let's Encrypt server.

3 A list of challenges is received, and Connection Broker reads the HTTP token sent by the Let's Encrypt server.

4 Secure Gateway or HALB retrieves the tokens from the Connection Broker.

5 Once ready, Connection Broker notifies the Let's Encrypt Server.

6 Let's Encrypt starts the verification process by going to the Secure Gateway or HALB and confirming the availability of the token.

7 Challenges are completed including confirmation that the Secure Gateways or HALB can reply to the domain mentioned.

8 Assuming that the challenge is completed successfully, Parallels RAS requests a certificate.

9 Valid certificate is downloaded from the Let's Encrypt server to Connection Broker.

10 Connection Broker distributes the certificate to the Secure Gateways or HALB.

Import a certificate from a file

To import a certificate from a file, choose **Add** > **Import certificate** from the ellipsis menu and specify the following:

- **Name:** Type a name for the certificate.
- **Description:** An optional description.
- **Usage:** Specify whether the certificate will be used for RAS Secure Gateways or HALB, or both.
- **Private key file:** Specify a file containing the private key. Click **Browse** to browse for the file.
- **Certificate file:** When you specify a private key file (above) and have a matching certificate file, it will be inserted in this field automatically. Otherwise, specify a certificate file.

Click **OK** when done. The certificate will appear in the list with the **Status** column indicating **Imported**.

Export a certificate to a file

To export a certificate to a file, select it in the list and choose **Export certificate** from the ellipsis menu.

You can later import the certificate to a different Farm or Site by using **Import certificate** and specifying the certificate file in the **Private key file** field.

Assign a certificate to Gateways and HALB

After you add a certificate, you can assign it to a RAS Secure Gateway, HALB, or both depending on the usage type that you specified when you created the certificate. More on the certificate **Usage** option below.

Certificate Usage

Certificate **Usage** is an option that specifies whether the certificate should be available for RAS Secure Gateways, HALB, or both. See **Generate a self-signed certificate** (p. 48). When you configure SSL for a RAS Secure Gateway or HALB later, you need to specify an SSL certificate. When you select a certificate, the following options will be available depending on how the **Usage** option is configured for a particular certificate:

- **<All matching usage>**: This is the default option, which is always available. It means that any certificate on which the **Usage** selection matches the object type (Gateway or HALB) will be used. For example, if you are configuring a Gateway and have a certificate that has **Usage** set to "Gateway", it will be used. If a certificate has both, Gateway and HALB usage options selected, it can also be used with the given gateway. This works the same way for HALB when you configure the LB SSL Payload. Please note that if you select this option for a Gateway or HALB, but not a single matching certificate exists, you will see a warning and will have to create a certificate first.
- Other items in the **Certificates** drop-down list are individual certificates, which will or will not be present depending on the certificate's **Usage** settings. For example, if you configure LB SSL Payload for HALB and have a certificate with the **Usage** option set to "HALB", the certificate will appear in the drop-down list. On the other hand, certificates with **Usage** set to "Gateway" will not be listed.

As another example, if you need just one certificate, which you would like to use for all of your Gateways, you need to create a certificate and set the **Usage** option to "Gateways". You can then configure each Gateway to use this specific certificate or you can keep the default **<All matching usage>** selection, in which case the certificate will be picked up by a Gateway automatically. Same exact scenario also works for HALB.

Gateways

To assign a certificate to a RAS Secure Gateway:

1. Navigate to **Infrastructure** > **Gateways**.
2. Click a Gateway in the list.
3. Click **Properties** in the middle pane.
4. Select the **SSL/TLS** category.
5. In the **Certificates** drop-down list, select the certificate that you created.

Please note that you can also select the **<All matching usage>** option, which will use any certificate that has the usage set to Gateway or both Gateway and HALB.

HALB

At the time of this writing, HALB cannot be managed in the RAS Management Portal. Please use the desktop-based RAS Console.

Gateways

RAS Secure Gateway tunnels all Parallels RAS data on a single port. It also provides secure connections and is the user connection point to Parallels RAS.

In a single tenant environment, you need to install at least one RAS Secure 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.

The following describes how RAS Secure Gateway handles user connection requests:

1. RAS Secure Gateway receives a user connection request.
2. It then forwards the request to the RAS Connection Broker with which it's registered (the Preferred Connection Broker setting by default).
3. The RAS Connection Broker 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 Connection Broker 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 host.

RAS Secure Gateway operation modes

RAS Secure Gateway can operate in one of the following modes:

- **Normal Mode**: RAS Secure Gateway receives user connection requests and checks with RAS Connection Broker 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**: RAS Secure Gateway 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, the RAS Site must have more than one RAS Secure Gateway installed.

Planning for high availability

When adding RAS Secure 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 Connection Brokers or RD Sessions Hosts.

Add a Gateway

To add a RAS Secure Gateway:

1. Navigate to **Infrastructure** > **Secure Gateways**.
2. In the right pane, choose **Add** from the ellipsis menu. The **Gateway - Add new** wizard opens.

3 Enter the server FQDN or IP address or click **Browse AD** to select a server from the list. To resolve IP address to FQDN or vice versa, click **Resolve IP** or **Resolve Name**.

4 Click **Next**.

5 Select the gateway mode from the **Mode** drop down menu (Normal or Forwarding).

6 If you selected the **Forwarding** mode in the previous step, 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.

7 Add an optional description for this Gateway.

8 Select the **Enable User Portal** option to enable the RAS User Portal support (a browser-based client that can be used to connect to Parallels RAS and launch published resources).

9 Select the **Enable firewall rules** to automatically configure the firewall on the server hosting the gateway.

10 Click **Next**.

11 Review the settings and click **Create** to add the Gateway to the Site.

Additional information

To learn how to configure and manage a RAS Secure Gateway:

- **Configure a Gateway** (p. 55)
- **Manage a Gateway** (p. 67)

Configure a Gateway

To configure a RAS Secure Gateway:

1 Navigate to **Infrastructure** > **Secure Gateways**.

2 Click a Gateway in the list to open the view displaying the Gateway details.

3 In the middle pane, click **Properties**.

Configure Gateway properties as described in the subsequent sections.

General

Select or clear the **Enable RAS Secure Gateway in Site** option.

- **Host**: Select a different host if needed.
- **Description**: Set or modify an optional description.
- **Public address**: Specify a public address for the Gateway server.

Set IP addresses for client connections

Specify the following IP options:

- **Use IP version:** Select the IP version(s) to use. RAS Secure Gateway recognizes both IPv4 and IPv6. By default, IPv4 is used.
- **IP(s):** Specify one or more IP addresses separated by a semicolon, or click **Resolve** to resolve the IP address automatically. These are the available addresses on the Gateway server. To specify IP addresses that should be used for client connections, use the **Bind to IP** section (see below).
- **Bind to IP:** Use this section to specify on which IP address (or addresses) the Gateway will listen for client connections. You can select a specific address or **All available addresses**, in which case all of the IP addresses specified in the **IP(s)** field will be used.
- **Remove system buffers for:** This option 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 one or more specific addresses, all available addresses, or none. 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 fast enough from the Gateway to the Client, thus ending up with a bad user experience. Enabling this option will optimize the data exchange.

Mode

RAS Secure Gateway can operate in one of the following modes:

- **Normal Mode**: RAS Secure Gateway receives user connection requests and checks with RAS Connection Broker 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**: RAS Secure Gateway 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, the RAS Site must have more than one RAS Secure Gateway installed.

To use Site default settings, click the **Inherit Defaults** option. To specify your own settings, clear the option.

Setting the normal mode

To set the normal mode, in the **Gateway mode** drop-down list, select **Normal**.

The **Preferred Connection Broker** drop-down list allows you to specify a RAS Connection Broker that the gateway will 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 Connection Broker. For the gateway to select a Connection Broker automatically, select the **Automatic** option.

The **Forward requests to HTTP Server** option allows you to forward requests that do not belong to RAS Secure 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 if necessary. Please note that the HTTP server must support the same IP version as the browser making the request.

Setting the forwarding mode

To configure the forwarding mode, in the **Gateway mode** drop-down list, select **Forwarding** and specify one or more Gateways. A gateway in forwarding mode will forward all the user connection requests to a pre-configured gateway. Gateways in forward 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.

Network

The **Network** category is used to configure RAS Secure Gateway network options.

To use Site default settings, click the **Inherit Defaults** option. To specify your own settings, clear the option and set the following:

- **RAS Secure Gateway port**: By default RAS Secure Gateway listens on TCP port 80 to tunnel all Parallels RAS traffic. To change the port, specify a new port.
- **RDP port**: 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. When setting your own port, make sure that the port does not conflict with the standard "RD Session Host Port" setting.

  Note: If the RDP port is changed, users need to append the port number to their connection string in the remote desktop client (e.g. [ip address]:[port]).

- **Broadcast RAS Secure 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.
- **Device Manager port**: Select this option to enable management of Windows devices. 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.

SSL/TLS

The traffic between Parallels RAS users and a RAS Secure Gateway can be encrypted. The **SSL/TLS** category allows you to configure data encryption options.

To use Site default settings, click the **Inherit default settings** option. To specify your own settings, clear the option.

HSTS

The **HSTS** section allows you to enforce HTTP Strict Transport Security (HSTS), which is a mechanism that makes a web browser to communicate with the web server using only secure HTTPS connections. When HSTS is enforced for a RAS Secure Gateway, all web requests to it will be forced to use HTTPS. This specifically affects User Portal, which can normally accept only HTTPS requests.

- **Enforce HTTP strict transport security (HSTS):** Enables or disables HSTS for the gateway.
- **Max-age:** Specifies the max age in months that the web browser should remember that it can only communicate with the gateway using HTTPS. The default (and recommended) value is 12 months. Acceptable values are 4 to 120 months.
- **Include subdomains:** Specifies whether to include subdomains (if applicable).
- **Preload:** Enables or disables HSTS preloading. This is a mechanism whereby a list of hosts that wish to enforce the use of SSL/TLS on their Site is hardcoded into a web browser. The list is compiled by Google and is used by Chrome, Firefox, Safari, and Edge browsers. When HSTS preload is used, a web browser will not try to send a request using HTTP, but will use HTTPS every time. Please also read the important note below.

Note: To use HSTS preload, you have to submit your domain name for inclusion in Chrome's HSTS preload list. Your domain will be hardcoded into all web browser that use the list. **Important:** Inclusion in the preload list cannot easily be undone. You should only request inclusion if you are sure that you can support HTTPS for your entire Site and all its subdomains in the long term (usually 1-2 years).

Please also note the following requirements:

- Your website must have a valid SSL certificate.
- All subdomains (if any) must be covered in your SSL Certificate. Consider ordering a Wildcard Certificate.

Encryption

By default, a self-signed certificate is assigned to a RAS Secure Gateway when the gateway is installed. Each RAS Secure Gateway must have a certificate assigned and the certificate should be added to Trusted Root Authorities on the client side to avoid security warnings.

SSL certificates are created on the Site level. Once a certificate is created, it can be assigned to a RAS Secure Gateway. For the information about creating and managing certificates, see **Certificates** (p. 48).

To configure encryption:

1. Select the **Enable SSL on port** option and specify a port number (default is 443).
2. In the **Accepted SSL versions** drop-down list, select the SSL version.
3. In the **Cipher Strength** field, select a desired cipher strength.
4. In the **Cipher** field, specify the cipher. A stronger cipher allows for stronger encryption, which increases the effort needed to break it.
5. The **Use ciphers according to server preference** option is ON by default. You can use client preferences by disabling this option.
6. In the **Certificates** drop-down list, select a desired certificate. The **<All matching usage>** option will use any certificate configured to be used by gateways. When you create a certificate, you specify the "Usage" property where you can select "Gateway", "HALB", or both. If this property has the "Gateway" option selected, it can be used with a gateway. Please note that if you select this option, but not a single certificate matching it exists, you will see a warning and will have to create a certificate first.

Additional information

Client and Server configurations (p. 59)

Client and Server configurations

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 the 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 is used, the client device trusts using Trusted Certificate Authority updates for the platform.

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 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 Gateway:

1. In the **SSL/TLS** category, make sure that the **Enable SSL on port** option is selected.
2. In the **Network** category, make sure that the **Enable RDP UDP Data Tunneling** option is selected.

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.

SSL server configuration

When configuring RAS Secure Gateway to use SSL encryption, you should pay attention to how the SSL server is configured to avoid possible traps and security issues. Specifically, the following SSL components should be rated to determine how good the configuration is:

- The certificate, which should be valid and trusted.
- The protocol, key exchange, and cipher should be supported.

The assessment may not be easy to perform without specific knowledge about SSL. That's why we suggest that you use the SSL Server Test available from Qualys SSL Labs. This is a free online service that performs an analysis of the configuration of an SSL web server on the public Internet. To perform the test on a RAS Secure Gateway, you may need to temporarily move it to the public Internet.

The test is available at the following URL: https://www.ssllabs.com/ssltest/

You can read a paper from Qualys SSL Labs describing the methodology used in the assessment at the following URL: https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide.

User Portal

Parallels User Portal is built into RAS Secure Gateway. It allows users to connect to Parallels RAS and open published resources from a web browser.

Note: To use User Portal, SSL must be enabled on a RAS Secure Gateway. When enabling the client, please verify that SSL is enabled in the **SLL/TLS** category or on your network load balancer. Please also note that the **User Portal** category is only available if the Gateway mode is set to **Normal**.

For the information on how to configure the User Portal URL and how to access the client from a web browser, please see the **Web** section (p. 64).

- To use Site default settings on the **User Portal** tab, click the **Inherit default settings** option. To specify your own settings, clear the option.
- To enable or disable RAS User Portal, select or clear the **Enable User Portal** option.

Client

The **Client** section allows you to specify application launch methods and other User Portal settings.

- **Launch sessions using:** Specifies which Parallels Client will be used to open a published resource. This can be the User Portal or a platform-specific Parallels Client. Compared to Web Client, platform-specific Parallels Client includes a richer set of features and provides end users with a better overall user experience. Select one of the following:
  - **a** **Browser only**: Users can run remote applications and desktops using Web Client only. Use this option if you don't want your users to install a platform-specific Parallels Client.
  - **b** **Parallels Client only**: Users can run remote applications and desktops in Parallels Client only. When a user connects to Parallels RAS using Parallels Web 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 containing the Parallels Client download link. After the user installs Parallels Client, they can still launch a remote application or desktop in Web Client but the resource will open in Parallels Client.

c **Parallels Client and fallback to browser**: Both Parallels Client and a browser (HTML5) can be used to launch remote applications and desktops. Parallels Client will be the primary method; Parallels Web Client will be used as a backup if a published resource cannot be launched in Parallels Client for any reason. A user will be informed if Parallels Client cannot be used 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 **Parallels Client and fallback to browser** (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.

Network Load Balancer access

The **Network Load Balancers access** section is intended for deployment scenarios where third-party front-end load balancers such as Amazon Web Services (AWS) Elastic Load Balancers (ELBs) are used. It allows you to configure an alternate hostname and port number to be used by the Network Load Balancer (NLB). This is needed to separate hostnames and ports on which TCP and HTTPS communications are carried out because AWS load balancers don't support both specific protocols over the same port.

The following options are available:

- **Use alternate hostname:** Select this option and specify an alternate hostname. When the alternate hostname is enabled, all platform-specific Parallels Clients will use this hostname to connect to the RAS Farm or Site.
- **Use alternate port:** Select this option and specify an alternate port number. The port must not be used by any other component in the RAS Farm or Site. To reset the port number to the default value, click **Default**. When the alternate port is enabled, all platform-specific Parallels Clients will use this port to connect to the RAS Farm or Site. Note that RDP sessions in Web Client will still be connecting to the standard SSL port (443).

Note: Please note that using an alternate host or port is not suitable in a multi-tenant environment as Tenant Broker RAS Secure Gateways are shared between Tenants, which would require different configurations.

In addition, the AWS Application Load Balancer (ALB), which handles HTTP/s traffic required by the Parallels Web Client, only supports specific cookies that are usually automatically generated. When a load balancer first receives a request from a client, it routes the request to a target and generates a cookie named `AWSALB`, which encodes information about the selected target. The load balancer then encrypts the cookie and includes it in the response to the client. When sticky sessions are enabled, the load balancer uses the cookie received from the client to route the traffic to the same target, assuming the target is registered successfully and is considered healthy. By default, Parallels RAS uses its own ASP.NET cookie named `_SessionId`, however in this case you must customize the cookie specifying the mentioned AWS cookie for sticky sessions. This can be configured using the **Web cookie** field in the **User Portal** > **Web** subcategory.

Restrictions

The **Restrictions** section is used to allow or restrict the following User Portal functions:

- **Use Pre Windows 2000 login format:** Enables legacy (pre-Windows 2000) login format.
- **Allow embedding of Parallels User Portal into other web pages:** If selected, the Parallels User Portal 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.
- **File transfer command:** Enables file transfer in a remote session. Select a desired option in the drop-down list. For more information, see **Configuring remote file transfer** below.
- **Clipboard redirection:** Select a clipboard option that should be allowed in a remote session. Choose from **Client to server only** (copy/paste from client to server only), **Server to client only** (copy and paste from server to client only), **Bidirectional** (copy and paste in both directions).
- **Allow cross-origin resource sharing (CORS):** Enables cross-origin resource sharing (CORS). To enable CORS, select this option and then specify one or more domains for which access to resources should be allowed. If you don't specify any domains, the option will be automatically disabled. In the **Browser cache time** field, specify for how long the end-user's browser will cache a resource.

Configuring 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 Web Client and Parallels Client for Chrome only. Note that bidirectional file transfer is supported in Parallels Web Client only.

To make the remote file transfer functionality flexible, Parallels RAS allows you to configure it on the following three levels:

- RD Session Host, Provider, or Remote PC
- User Portal
- Client policy

File transfer settings that you configure on each level take precedence in the order listed above. For example, if you enable file transfer in User Portal, 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 User Portal. As another example, you can enable file transfer on an RD Session Host and then disable it for a particular Client policy (or an User Portal). This way you can control which clients can use file transfer and which cannot.

To configure remote file transfer for a User Portal, select one of the following options in the **File transfer command** drop-down list:

- **Disabled**: Remote file transfer is disabled.
- **Client to Server**: Transfer files from client to server only.
- **Server to Client**: Transfer files from server to client only.
- **Bidirectional**: Transfer files in both directions.

Web

Note: The **Web** subcategory is only available if the gateway mode is set to normal.

The **Web** category allows you to tweak settings necessary for load balancing in certain scenarios. Here you can specify a redirection URL for web requests and a session cookie name to maintain persistence between a client and a server.

Redirection URL

The original web request can reach the gateway one of the following two ways:

- The request is sent directly to the Gateway over the local network using its IP address or FQDN. For example, https://192.168.10.10.
- The request is sent to a HALB device that load-balances this and other gateways in the Farm. The HALB device often faces the Internet (i.e. located in DMZ) and so its DNS name can be used in the original request URL. For example, https://ras.msp.com. The HALB device is then distributes the request to a gateway.

When the gateway receives the web request, it takes the URL specified in the **Web** category and sends it back to the web browser for redirection.

Technically, you can enter any URL here, and the original web request will be redirected to that URL. The primary purpose of this field, however, is to give end users an easy way to access the User Portal from their web browsers. Here's how it works:

1. A user enters the Load Balancer DNS name in a web browser. For example, https://ras.msp.com.
2. The Load Balancer receives the request and distributes it to the least-busy RAS Secure Gateway for processing.
3. The gateway receives the original URL and replaces it with the URL specified in the **Default URL** field. See the **Default URL format** subsection below.
4. The replaced URL is then sent back to the web browser, which uses it to open the User Portal login page.

Default URL format

The default URL format is the following:

```
https://%hostname%/userportal
```

- The `%hostname%` variable is automatically replaced with the name of the server that received the original request, which in our example is the Load Balancer DNS name. If you wish, you can replace the variable with a specific host name or IP address (e.g. this or some other gateway). For example, `https://192.168.5.5/userportal`. If you do this, the web requests will always be forwarded to the specified host and will open the User Portal on it. Hard-coding a host may not be very practical, but you can do this nevertheless.
- `userportal` is a constant and is the path to the User Portal login page.

In our example, the resulting URL that the web browser will use to access the User Portal is the following:

```
https://ras.msp.com/userportal
```

The fact is, a user could simply use the above URL from the start, but thanks to the redirection feature, users only need to enter the server DNS name (or FQDN/IP-address on the local network) instead of the entire URL.

Opening a specific User Portal Theme

User Portal Themes is a feature that allows you to custom design the User Portal look and feel for different groups of users.

The default web request URL opens the default Theme. To make it open a specific Theme, add the Theme name at end of the URL as follows:

```
https://%hostname%/userportal/?theme=<theme-name>
```

where `<theme-name>` is the name of a Theme without brackets or quotes.

For users to open a specific Theme, the URL that they enter in a web browser must contain the Theme name, but in this case the format is as simple as the following:

```
https://<server-name>/<theme-name>
```

Using our Load Balancer DNS name example from above, the URL may look like the following:

```
https://ras.msp.com/Theme-E1
```

For additional information, please see **User Portal Theme Settings** > **URLs**.

Open User Portal

The **Open User Portal** button uses the specified gateway address and opens User Portal on this particular gateway in a new tab. You can use this button to test your deployment.

Web cookie

The Web cookie field is used to specify a session cookie name. 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 client and a server. To do so, you'll need to set up a load balancer that can use a session cookie for persistence. The default cookie name is ASP.NET_SessionId.

If you are using a third-party load balancer, such as Amazon Web Services (AWS), you need to specify its own cookie name. In case of AWS, when the load balancer first receives a request from a client, it routes the request to a target and generates a cookie named AWSALB, which encodes information about the selected target. The load balancer then encrypts the cookie and includes it in the response to the client. When sticky sessions are enabled, the load balancer uses the cookie received from the client to route the traffic to the same target, assuming the target is registered successfully and is considered healthy.

Wyse

To publish applications from the Parallels RAS to thin clients using the Wyse thinOS, select the **Enable Wyse ThinOS support** option.

Note: The Wyse category is only available if the Gateway mode is set to normal.

By enabling this option, the RAS Secure 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.

The **Do not warn if server certificate is not verified** option can be selected (enabled) if a Wyse device shows an SSL warning when connecting to a RAS Secure Gateway because the hostname does not match the certificate. When the option is selected, the Gateway will send Wyse clients the following parameters in the wnos.ini file: SecurityPolicy=low TLSCheckCN=no, which will disable SSL checks. Note that the option is not required if a certificate has the following:

- The CNAME set to the FQDN of the RAS Secure Gateway.
- The SAN set to the RAS Secure Gateway IP address.

Note that if you use a custom wnos.ini in "C:\Program Files (x86)\Parallels\ApplicationServer\AppData\wnos" folder on Gateway, the Gateway will not send the SSL check parameters.

Security

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 Gateway Properties** dialog.

To use Site default settings, click the **Inherit default settings** option. To specify your own settings, clear the option.

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.

Managing Gateways

To perform RAS Secure Gateway management tasks:

1. Navigate to **Infrastructure** > **Secure Gateways**.
2. From here, you can either select a Gateway and use the ellipsis menu to perform a management task. You can also click a Gateway to open a view displaying Gateway details where you can also perform the same tasks. The tasks are described below.

Control

Allows you to enable or disable the Gateway.

Logs

A RAS Secure Gateway is monitored and logs are created containing relevant information. To configure logging click one of the following:

- **Configure**: Allows you to configure logging. For the explanation of log levels, please see below.
- **Retrieve**: Retrieves a ZIP archive containing the log files to the specified location.
- **Clear**: Clears all existing logs.

The available log levels are:

- **Standard**: This is the standard log level that records only the most important events. Unless you are asked by Parallels RAS support to use one of the log levels described below, you should always use this one.
- **Extended**: This logging involves more information than the standard logging, but it slows down the system because of the additional information that it needs to collect.
- **Verbose**: Verbose logging involves even more information than the extended logging and can slow down your system significantly.

Please note that to avoid degraded performance, extended and verbose logging should only be enabled for a limited time period (enough to collect the necessary information for analysis). You can set this time period using **Reset to the standard level after** option. The default value is 12 hours. In specific cases, a Parallels support engineer will advise you whether this time period should be set to a different value. Once this time period is over, the log level will be reset back to standard.

Other actions

- **Refresh**: Refreshes the displayed Gateway information.
- **Site defaults**: Opens the Site defaults view.
- **Delete**: Removes the Gateway from the Farm.

Connection Brokers

RAS Connection Broker provides load balancing of published applications and desktops. A RAS Connection Broker is automatically installed on a server on which you install Parallels RAS and is designated as the primary Connection Broker. Each Site must have a primary RAS Connection Broker but can also have secondary Connection Brokers added to it. The purpose of a secondary Connection Broker is to ensure that users do not experience any interruption of the service due to possible failure of the primary RAS Connection Broker.

Configure RAS Connection Broker

To view RAS Connection Brokers installed in a Site, navigate to **Infrastructure** > **Connection Broker**.

A Site must have at least the primary Connection Broker installed, which is marked so in the **Priority** column. You can also add secondary agents for redundancy (p. 69).

To modify the configuration of a Connection Broker, click it in the list and then click **Properties** in the middle pane. Click **Edit** and specify the following options:

- **Enable:** Enables or disables the Connection Broker.
- **IP:** Specifies the server IP address.
- **Alternate IPs:** Specifies one or more alternate IP addresses separated by a semicolon. These addresses will be used if RAS Secure Gateways fail to connect to the RAS Connection Broker using 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.

- **Standby:** If selected, puts a secondary Connection Broker into a standby mode. This means that no agent will connect to this Connection Broker until another Connection Broker goes offline. This option is enabled automatically for any new secondary Connection Broker in excess of the three agents that already exist. It is not recommended to have more than three active Connection Brokers because it may degrade system performance. Using this option you can have more than three agents, but have them in standby mode until they are needed. For more information, see **Add a secondary Connection Broker** (p. 69).

When done making the changes, click **Save** and then click **Apply All Changes**.

The ellipsis menu on the main **Connection Brokers** view has the following items:

- **Add**: Adds a RAS Connection Broker to the Site. See the section that follows this one for the information on how to add secondary Connection Brokers.
- **Update agent**: Update the agent.
- **Disable/Enable agent**: Enable or disable the agent.
- **Logs**: Allows to manage logging.
- **Promote to primary**: Promotes a secondary Connection Broker to primary.
- **Rise priority**: Rises the priority of a secondary Connection Broker (moves it up in the priority list).
- **Lower priority**: Lowers the priority of a secondary Connection Broker (moves it down in the list).
- **Refresh**. Refreshes the **Connection Brokers** list.
- **Delete**. Deletes a secondary Connection Broker from the Site. To delete the current primary Connection Broker, you first need to promote a secondary Connection Broker to primary.

Additional information

- Add a secondary Connection Broker (p. 69)
- Manage RAS Connection Brokers (p. 72)

Add a secondary Connection Broker

A secondary Connection Broker is added to a Site for redundancy. This way if the primary Connection Broker fails, the secondary Connection Broker is still available to handle the requests. Connection Brokers work in active/active manner to ensure high availability. In case of a Connection Broker 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 Connection Brokers (auto-promotion is described later in this section).

When you have one more secondary Connection Brokers 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 Connection Broker is used for authentication purposes with both the AD and any 2nd level authentication provider used.

The primary Connection Broker performs the same tasks as secondary Connection Brokers but has additional responsibilities. It manages certain processes that must be managed by a single Connection Broker. The following table lists processes managed by the primary Connection Broker and secondary Connection Brokers:

Process	Primary Connection Broker	Secondary Connection Brokers
Monitor PAs (counters)	Yes	Yes
Monitor RD Session Hosts (counters)	Yes	Yes
Monitor Providers (counters)	Yes	Yes
Monitor RDS Sessions (reconnection)	Yes	Yes
Monitor Deployed RDS 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 RDS 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 Connection Brokers works, consider the following example:

- Suppose we have two Connection Brokers: PA1 (primary) and PA2 (secondary).
- Suppose we also have 10 RD Session Hosts: RDS1, RDS2 ... RDS10

The resulting load will be distributed as follows:

- RDS1—RDS5 will use PA1 as their preferred Connection Broker.
- RDS6—RDS10 will use PA2 as their preferred Connection Broker.

Planning for secondary Connection Brokers

RAS Connection Brokers 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 Connection Broker communications).

When adding a secondary Connection Broker 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 Connection Brokers use to communicate with each other is TCP 20030.

There's no physical limit to how many Connection Brokers you can add to a Site. However, the best results are achieved with only two-three agents present. The three-agent scenario is highly recommended, especially when you have Providers and want to enable high availability for VDI. Adding more than two secondary Connection Brokers to a Site may have a reverse effect and actually degrade the system performance. Note that this does not apply to secondary Connection Brokers in standby mode, which is explained in **Configuring RAS Connection Brokers**.

Adding a secondary RAS Connection Broker to a Site

To add a secondary Connection Broker:

1. Navigate to **Infrastructure** > **Connection Brokers**.
2. Choose **Add** from the ellipsis menu (or click the plus-sign icon). The **Add new** wizard opens.
3. On the **Host** page, specify the following:
   - **Host name**: FDQN of the host that hosts the RAS Connection Broker. Click **Resolve IP** to obtain the host IP address automatically.
   - **IP address**: The host IP address. Click **Resolve Name** to obtain the host FQDN automatically.
4. On the **Agent Settings** page, specify the following:
   - **Alternative IPs**: One or more alternative IP addresses, separated by a semicolon. These addresses will be used if RAS Secure Gateways fail to connect to the RAS Connection Broker using its FQDN or the address specified on the previous page. This can happen, for example, if Gateways are connecting from a different network, which is not joined to Active Directory.
   - **Description**: Add an optional description.
   - **Enable firewall rules**: Select to automatically configure the firewall on the host.
   - **Restart host if required**: Automatically restart host after the installation, if it is required.
   - **Install a gateway with a Connection Broker**: Select this option if you also want to install a RAS Secure Gateway on the specified host. If you select this option, you may also select the **Enable HTML5 Gateway** option to automatically enable User Portal on the Gateway.
5. On the **Summary** page, review the settings and click **Create**.

From this point, follow the onscreen instructions and add the Connection Broker to the Farm.

Additional information:

Manage RAS Connection Brokers (p. 72)

Manage RAS Connection Brokers

To perform RAS Connection Broker management tasks:

1. Navigate to **Infrastructure** > **Connection Brokers**.
2. Select a Connection Broker in the list and click the ellipsis.
3. In the menu, choose one of the options describe below.

Add

See **Add a secondary Connection Broker**.

Update agent, Disable/Enable agent

Update, disable or enable the Connection Broker.

Logs

To configure logging choose one of the following:

- **Configure**: Allows you to configure logging. For the explanation of log levels, please see below.
- **Retrieve**: Retrieves a ZIP archive containing the log files to the specified location.
- **Clear**: Clears all existing logs.

The available log levels are:

- **Standard**: This is the standard log level that records only the most important events. Unless you are asked by Parallels RAS support to use one of the log levels described below, you should always use this one.
- **Extended**: This logging involves more information than the standard logging, but it slows down the system because of the additional information that it needs to collect.
- **Verbose**: Verbose logging involves even more information than the extended logging and can slow down your system significantly.

Please note that to avoid degraded performance, extended and verbose logging should only be enabled for a limited time period (enough to collect the necessary information for analysis). You can set this time period using **Reset to the standard level after** option. The default value is 12 hours. In specific cases, a Parallels support engineer will advise you whether this time period should be set to a different value. Once this time period is over, the log level will be reset back to standard.

Promote to primary

This option is enabled for secondary Connection Brokers only. In the event that the primary Connection Broker is down and cannot be recovered, you can promote a secondary Connection Broker to primary.

Rise priority / Lower priority

This option is enabled for secondary Connection Broker only. Each secondary Connection Broker is given a priority. To change the priority, choose **Rise priority** or **Lower priority**. The Connection Broker will move up or down the main list. The higher the agent is in the list, the higher the priority.

Refresh

Refreshes the current view.

Delete

Remove the Connection Broker from the Farm.

Providers

Providers are hypervisors or cloud-based virtualization solutions that can be added to a RAS Farm to use virtual machines as Virtual Desktops.

Please note that at the time of this writing, the Provider functionality in the RAS Management Portal is limited to viewing the available providers, hosts, and active sessions. To perform other Provider tasks, please use the desktop-based Parallels RAS Console.

Provider list

To see the list of providers, navigate to **Infrastructure** > **Providers**.

To add or remove columns to/from the **Providers** table, click the gear icon and select or clear desired columns.

To perform a task, select a provider in the list and choose one of the following from the ellipsis menu:

- **Show hosted VDI desktops**: Opens the Host list (p. 47) with a filter applied to show only the hosts that belong to this provider.
- **Show active sessions**: Opens the Sessions list (p. 75) with a filter applied to show only session that belong to this provider.

Site defaults

The Site defaults category allows you to configure default settings for various RAS components and services. At the time of this writing, you can configure Site defaults for the following:

- **Publishing** — See **Site defaults (Publishing)** (p. 89).
- **Gateways** — See **Configure a Gateway** (p. 55).
- **RD Session Hosts and Host pools** — see **Agent Settings** (p. 37).
- **Multi-factor Authentication** — see **Multi-factor authentication** (p. 20).

When you add a component to a RAS Farm, or when you publish a resource, Site defaults are used so you don't have to enter the values manually every time. You can easily override the defaults with your own values if necessary.

To view Site defaults, click any of the available categories. To modify the default settings, click **Edit** in the Site defaults view.

CHAPTER 8

Sessions

In This Chapter

Overview

The **Session** category displays user sessions for all available host types, including RD Sessions Hosts and VDI. This is the place where you can view all current sessions irrespective of the type of a server hosting a session.

When you select the **Sessions** category, the following two items are displayed in the **Sessions** navigation bar:

- **User Sessions**: Lists user sessions for all available hosts.
- **Running Resources**: Lists currently running published resources (apps and desktops) from all hosts.

Please note that when you open the **Sessions** category or an **Active Sessions** tab, some of the columns in a list may not be populated right away. This is because it takes some time to calculate these values. The examples of such columns include **Logon duration**, **UX Evaluator**, **Latency**. Simply wait a few seconds and the values will appear in the list.

Session information

To view user sessions, navigate to **Sessions** > **User Sessions**. The list contains user sessions from hosts of all available types, including RD Session Hosts and VDI.

To show or hide table columns, click the gear icon and select or clear column names.

To view session details, choose a session and click the user name. This opens the **Session Info** view displaying the session information.

The following groups are displayed:

- **Session Setup**: Contains general session information.
- **Session Details**: Displays the current session state, logon time, in/out data size, and general session information.
- **User Experience**: Displays metrics that can be used to evaluate user experience.
- **Logon Details**: Displays logon metrics that can be used to evaluate the logon process.
- **Connection Details**: Displays connection and authentication details.
- **Client Details**: Displays information about the user device and Parallels Client type and version.

Parallels RAS 18 introduces over 25 new session detail metrics available. The tables below give an overview of these new and some of the important preexisting metrics.

Note: The latest Parallels Client is required for some of the new metrics to be shown.

Session Setup

Metric	Description
Session host*	Session host name
Source*	**Sessions** category only. Host type: RDSH (even if its through VDI), VDI, RemotePC (through VDI only), Azure Virtual Desktop.

* New since Parallels RAS 18.1

Session Details

Metric	Description
Session State	Active, Idle, Disconnected, etc
Logon time	Time and date when the session was established
Session Length	Time the session has been established
Idle Time	Time the session has been idle
Incoming Data*	Amount of data received from the client
Outgoing Data*	Amount of data sent to the client
Resolution	Session resolution
Color Depth	Session colors depth
Bandwidth Usage*	Bandwidth used by the client

* New since Parallels RAS 18.0

User Experience

Metric	Description
UX Evaluator*	This is the time interval measured at the client between the first step (user action) and the last step (graphical response displayed).
Connection quality*	Connection quality rating (poor – excellent)
Latency*	Network latency
Transport Protocol*	TCP or UDP (over RDP)
Bandwidth availability*	Bandwidth availability as seen from the client
Reconnects*	Number of reconnects the current session suffered from inception (excluding graceful ones)
Last Reconnects*	Number of reconnects suffered from the current device session (excluding graceful ones)
Disconnect reason*	The last session disconnect reason

* New in Parallels RAS 18.0

Logon Details

Metric	Description
Logon duration*	Time taken to logon excluding the time waiting on UI.
Logon duration breakdown*	Connection time Authentication duration Host preparation (inc. load balancing algorithm) User profile load time RAS Policies lookup Group Policy processing Desktop loading Other
User Profile*	User Profile method in use: FSLogix, User Profile Disk, or Other (also contains additional information, such as error code).

* New since Parallels RAS 18.0

Connection Details

Metric	Description
Connection mode	Connection mode used by the client (e.g. GW SSL).
Authentication type	Authentication type used by the client (e.g. Credentials).
MFA provider	MFA provider used by the client, if any.

Flow	Lists all hosts the connection goes through on the way to the resource host (HALB, Gateway, Session host).

Client Details

Metric	Description
Device name	Name of the device from which the session was established
IP Address	Client private IP address
Client OS*	The operating system on which the client is running
Client OS version*	The operating system version on which the client is running
Client version*	The RAS client version is use

***** New since Parallels RAS 18.0

Export session information

To export the session information to a CSV file, click **Export** in the navigation bar and specify the location and file name.

You can also export session information from the main session list by clicking the ellipsis menu and choosing **Export**. Note that depending on what is selected in the list, the following will be exported:

- A single session — the information about that session is exported.
- Multiple sessions — the information for all selected sessions is exported.
- No selection — the information about all current sessions is exported. Exported CSV includes the exported session details along with export detail in the following format:

Session details (%Server type% such as RD Session Hosts) from Parallels RAS Farm %Farm name% and Site %Site name% exported by %Administrator% on %date% at %time%

User sessions

To manage a user session (or multiple sessions at the same time), select one or more sessions and then use the ellipsis menu to choose from the following actions:

- **Show session info**: Takes you to the **Session Info** view (p. 75). This option is only available if a single session is selected.
- **Message**: Opens the **Send Message** dialog where you can type and send a message to the session owner(s).
- **Disconnect**: Disconnect the selected session(s).
- **Log off**: Log off the session(s).
- **Show resources**: Switches to the **Running Resources** view (p. 79).

- **Show running processes**: Opens a view that lists running processes for the selected session. This option is only available if a single session is selected. See **Running processes** below.
- **Monitoring settings**: Opens **a** dialog where you can configure monitoring settings to highlight values in session metrics for RD Session Hosts. The dialog lists available metrics and allows you to set Warning and Critical thresholds for a given metric. To set a threshold, select the checkbox in front of a metric name and specify the desired values. During the RAS Farm operation, when a threshold is reached, a session metric value is highlighted as follows: Warning threshold — orange; Critical threshold — red.

  To reset values for a given threshold, select it and choose **Reset** from the ellipsis menu (or right-click > **Reset**). You can also enable or disable threshold color coding for a metric. To do so, select a metric and choose **Enable** or **Disable** from the ellipsis menu.
- **Refresh**: Refresh the list.
- **Export**: Export session information to a CSV file. See **Session information** (p. 75).

Running processes

The **Show running processes** menu option opens the **Running Processes** view for the session host with a filter applied to show processes for the selected session only.

The ellipsis menu allows you perform the following actions on a process:

- **Kill process**. Kill the selected process.
- **Refresh**. Refreshes the list.

Running resources

To see the list of published resources currently running on all hosts, navigate to **Sessions** > **Running Resources**.

Some of the notable columns in the list are:

- **Published name**: Published resource name (as seen in the **Publishing** category).
- **ID**: The published resource ID (as seen in the **Publishing** category).
- **Description**: Published resource description.
- **Process name**: The corresponding process name.
- **User**: Session owner.
- **Session ID**: Session ID.
- **Session host**: Session host name.
- **Source**: Session source (RDSH, VDI).

To perform a task on a resource, select it in the list and click the ellipsis menu. Some of the tasks include:

- **Message**: Send a message to the session owner.
- **Disconnect**: Disconnects the session.
- **Log off**: Log off the session.
- **Show running processes**: Opens the **Running Processes** view for the session host with the corresponding PID filter applied.
- **Show user session**: Opens to the **Session Info** view (p. 75).
- **Show information**: Displays the resource summary info and the session information. The session information includes the same metrics as described in **Session information** (p. 75).
- **Monitoring settings**: See the description of the **Monitoring settings** menu option in the **User sessions** topic (p. 78).
- **Refresh**: Refreshes the list.
- **Export**: Exports the resource info to a CSV file.

To see the detailed published resource information, click the resource name. This opens a view displaying the basic published resource information (ID, name, target, etc.) and the corresponding session information. For the detailed description of session metrics, please see **Session information** (p. 75). Clicking the resource name takes you to the **Publishing** category where the published resource is configured. The items in the navigation bar perform the same actions as the corresponding menu items described above.

CHAPTER 9

Publishing

Publishing is a process of making a resource available in Parallels RAS for end users. The resources that can be published from RAS Management Portal include:

- Application
- Desktop
- Document
- Folder on the file system

Publishing is performed from the **Publishing** category in the RAS Management Portal.

When you select the **Publishing** category, the published resources are displayed in the middle pane. When you select a resource, the information about it is displayed in the right pane. If a resource is placed in a folder, you first need to expand the folder and then select the resource. To modify an existing published resource, click the **Edit** button in the top-right corner of the right pane.

To perform publishing tasks, use the menu bar at the top of the middle pane. From here, you can publish a new resource, add a folder (e.g. to group resources of the same type), duplicate a resource, enable or disable a resource, sort the list, and perform some other tasks.

In This Chapter

Publish an application

To publish an application:

1. In the RAS Management Portal, select the **Publishing** category
2. In the middle pane, click the plus-sign icon (or choose **Add** from the ellipsis menu). The publishing wizard opens.
3. On the **Publishing Type** page, select **Application** and click **Next.**

4 On the **Sites** page, select one or more Sites (if available) from which the application should be available.

5 Click **Next**.

6 On the **Publish from** page, select from the following options:

- **All servers in the Site**: Publish from all hosts that are available in this Site.
- **Server host pools**: Specify one or more host pools from which to publish the application.
- **Individual servers**: Specify one or more specific individual hosts.

7 Click **Next**.

8 On the **Application Type** page, select from the following:

- **Select from installed and predefined application**: Choose this option to select from preinstalled and standard Windows applications.
- **Add single application manually**: Choose this option to configure all of the application settings yourself.

9 Click **Next**.

10 Depending on the application type that you selected on the previous page, the next page will appear as follows:

- **Select from installed and predefined application**: The page displays the list of preinstalled applications and application groups. You can select an entire group or individual applications. When done, click **Next** and follow the onscreen instructions to complete the wizard and publish the application(s). You can skip the rest of this section.
- **Add single application manually:** The page will open where you have to specify the application settings. Read on.

11 If you selected **Add single application manually**, a page opens where you need to configure the application as described below.

In the **Target Application** section, specify the following:

- **Target**: The application executable filename and path.
- **Start in**: Path that the application should use as the current working directory (by default, the executable path).
- **Parameters**: Application startup parameters (if any).

In the **Published Resource Settings** section, specify the following:

- **Name**: Type a name for the application.
- **Description**: Type an optional description.
- **Window mode**: Choose from Normal, Maximized, or Minimized.
- **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.

- **Exclude from session prelaunch**: The application will not be considered in session prelaunch scenarios.
- **Icon**: Click Browse and select an icon for the application.**Change Icon**. Change the application icon (optional).

12 On the next page, specify the initial status of the resource. Choose from the following options:

- **Enabled**: End users can launch the resource.
- **Disabled**: The resource will not appear in Parallels Client.
- **In maintenance**: The resource will appear in Parallels Client but users will not be able to launch it. When a resource is in maintenance and a user tries to launch it, they will see a message. To customize the message, click the **Configure** button. For more info, see **Site Defaults (Publishing)** (p. 89).

13 Click **Next** and then click **Finish** to publish the application.

Publish a desktop

To publish a desktop:

1 In the RAS Management Portal, select the **Publishing** category

2 In the middle pane, click the plus-sign icon (or choose **Add** from the ellipsis menu). The publishing wizard opens.

3 On the **Publishing Type** page, select **Desktop** and click **Next.**

4 On the **Sites** page, select one or more Sites (if available) from which the application should be available.

5 Click **Next**.

6 On the **Publish from** page, select from the following options:

- **All servers in the Site**: Publish from all hosts that are available in this Site.
- **Server host pools**: Specify one or more host pools from which to publish the application.
- **Individual servers**: Specify one or more specific individual hosts.

7 Click **Next**.

8 On the **Desktop** page, specify the following:

In the **Published Resource Settings** section, specify the following:

- **Name**: Type a name for this desktop.
- **Description**: Type an optional description.
- **Connect to administrative session**: Select this option if you want users to connect to the administrative session.
- **Start automatically when user logs in**: Select if you want to open the desktop as soon as the user logs in.

- **Exclude from session prelaunch**: The desktop will not be considered in session prelaunch scenarios.
- **Icon**: Select an application icon.

In the **Desktop Session Settings** section, specify the following:

- **Desktop size**: Specify the size. You can select from the available options and screen resolutions or you can specify custom settings. To set custom width and height, select **Custom** and specify the desired values in the fields provided.
- **Multi-Monitor**: Select whether the multi-monitor support should be enabled or whether the client settings should be used.

9 On the next page, specify the initial status of the resource. Choose from the following options:

- **Enabled**: End users can launch the resource.
- **Disabled**: The resource will not appear in Parallels Client.
- **In maintenance**: The resource will appear in Parallels Client but users will not be able to launch it. When a resource is in maintenance and a user tries to launch it, they will see a message. To customize the message, click the **Configure** button. For more info, see **Site Defaults (Publishing)** (p. 89).

10 Click **Next** and then click **Finish** to publish the desktop.

Publish a document

Publishing a document is similar to publishing an application, but instead of the application executable, you specify the document filename and path. See more in **Publish an application** (p. 81).

Publish a folder on the file system

To publish a folder on the file system:

1 In the RAS Management Portal, select the **Publishing** category

2 In the middle pane, click the plus-sign icon (or choose **Add** from the ellipsis menu). The publishing wizard opens.

3 On the **Publishing Type** page, select **Folder on the file system** and click **Next.**

4 On the **Sites** page, select one or more Sites (if available) from which the application should be available.

5 Click **Next**.

6 On the **Publish from** page, select from the following options:

- **All servers in the Site**: Publish from all hosts that are available in this Site.

- **Server host pools**: Specify one or more host pools from which to publish the application.
- **Individual servers**: Specify one or more specific individual hosts.

7 Click **Next**.

8 On the **Folder** page, specify the following:

- **Name**: Type a name for this folder.
- **Description**: Type an optional description.
- **Window mode**: Select a window mode from Normal, Maximized, or Minimized.
- **UNC path**: Enter the UNC path of the folder you wish to publish.
- **Icon**: Select a folder icon.

9 On the next page, specify the initial status of the resource (the folder). Choose from the following options:

- **Enabled**: End users can open the resource.
- **Disabled**: The resource will not appear in Parallels Client.
- **In maintenance**: The resource will appear in Parallels Client but users will not be able to use it. When a resource is in maintenance and a user tries to open it, they will see a message. To customize the message, click the **Configure** button. For more info, see **Site Defaults (Publishing)** (p. 89).

10 Click **Next** and then click **Finish** to publish the folder.

Manage published resources

To view published resources, select the **Publishing** category in the RAS Management Port.

The **Publishing** pane lists currently published resources. You can rearrange the list by dragging an item and dropping it in a desired row.

Use the ellipsis menu to perform general management tasks. The menu has the following options:

- **Add**: Starts the publishing wizard. The plus-sign icon is the corresponding toolbar item for this menu option.
- **Duplicate**: Creates a copy of a selected resource.
- **New Folder**: Creates a folder in the **Publishing** list. This is a virtual folder, used only to group resources in the application list. The folder will appear in the application listing in Parallels Client. The folder icon is the corresponding toolbar item for this menu option.
- **Refresh**: Refreshes the displayed information.
- **Set Status:** Enable/disable a resource or put it into maintenance mode. A disabled resource is unavailable to users. A resource in maintenance shows up in the list on the client side but cannot be used. When the status of a resource is changed to "Disabled" or "In maintenance", the resource name in the list becomes grayed and the current state is indicated in parentheses.

- **Move Up**: Moves a published resource up in the list. This does not change the resource ID or anything else.
- **Move Down**: Moves a resource down in the list.
- **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 resources.
- **Delete**: Deletes a published resource. This only removes the published resource from the Farm. The actual application is not affected.

Additional information

The subsequent sections describe how to manage individual published resources of different types.

Manage published applications

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, select it in the **Publishing** pane and then click **Edit** in the right pane to enable editing. Modify the application properties as described below.

Note that most of the settings here are the same as the settings in the application publishing wizard. For details about individual settings, please also see **Publish an application** (p. 81). The descriptions below focus on settings that are not available in the wizard and can only be set here.

Application

Most of the settings in this view are the same as in the publishing wizard. The new set of options is **Per server settings**. If the application is published from multiple servers, you can set the following application properties individually for each server:

- **Target**
- **Start in**
- **Parameters**

As an example, you can change the above properties when different servers have the application installed in different folders, so that the **Target** and **Start in** field values are valid on each server.

Filtering

The options in the **Filtering** category are not available in the publishing wizard and can only be set here. The category is common for published resources of all types. For complete details, see **Using filtering rules** (p. 91).

Routing

Please see **Configuring preferred routing** (p. 92).

Shortcuts

This view allows you to configure where a shortcut for the application is created on a user device. These settings are inherited from site defaults, but can be customized for a given application. For details, please see **Site defaults (Publishing)** (p. 89).

File extension

This category allows you to modify file extension association for the application. To add, remove, or modify an entry, select the **Associate File Extensions** option. To add a new extension to the list, choose **Add** from the ellipsis menu and specify the desired extension. To modify an existing association, select the extension in the list and choose **Properties** from the ellipsis menu.

License

See **Site defaults (Publishing)** (p. 89)

Display

See **Site defaults (Publishing)** (p. 89)

If you made changes, click the **Save** button or click **Cancel** to discard them.

Manage published desktops

To modify a published desktop, select it in the **Publishing** view. To view and modify desktop settings, use the navigation bar in the middle pane. To edit settings, click the **Edit** button.

Overview

This view lists other navigation bar items with short descriptions. You can click items here or in the navigation bar.

Publish from

Lists hosts or host pools from which the desktop is published. Use the **Publish from** drop-down list to switch between individual hosts or host pools. Select or clear hosts or host pools as needed.

Desktop

This view displays the published desktop settings. For the description of how to configure these settings, please see **Publish a desktop** (p. 83).

Filtering

The settings in the **Filtering** view are not available in the publishing wizard and can only be set here. The settings are common for published resources of all types. For complete details, see **Using filtering rules** (p. 91).

Routing

Please see **Configuring preferred routing** (p. 92).

Shortcuts

This view allows you to configure where a shortcut for the published desktop is created on a user device. These settings are inherited from site defaults, but can be customized for a given published resource. For details, please see **Site defaults (Publishing)** (p. 89).

If you made changes, click the **Save** button or click **Cancel** to discard them.

Manage folders

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

There are two types of folders that you can create:

- **Folders for administrative purposes**. Folders of this type are intended for Parallels RAS administrators. They are used to logically organize published resources in the RAS Management Portal 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. Select the **Publishing** category.
2. In the **Publishing** navigation bar, click the ellipsis menu and choose **New Folder** (or click the folder with a plus-sign icon).

3 Select a Site from which the folder will be published. Click **Next**.

4 Type a name and an optional description.

5 Select the **Use for administrative purposes** option if needed (see the explanation above).

6 Choose an icon or use the default one.

7 Click **Next**.

8 On the next page, specify the initial status of the resource (the folder). Choose from the following options:

- **Enabled**: End users can see the folder and will be able to launch published resources that it contains.
- **Disabled**: The folder will not appear in Parallels Client.
- **In maintenance**: The folder will appear in Parallels Client but users will not be able to launch resources that it contains. If the folder has subfolders, they inherit the status of the parent folder, which means that none of the resources contains in any of the folders in the hierarchy will be accessible to users. When a folder is in maintenance and a user tries to launch a resource from it, they will see a message. To customize the message, click the **Configure** button. For more info, see **Site Defaults (Publishing)** (p. 89).

9 Click **Finish** to create the folder.

Adding published resources to a folder

To add a published resource to a folder, right-click it and use **Move Up** or **Move Down** options to position the resource under the folder icon.

Site defaults (Publishing)

To configure Site defaults for published resources:

1 Navigate to **Infrastructure** > **Site defaults**.

2 Click **Publishing**.

3 View and modify if necessary the default settings as described below.

Shortcuts

This view allows you to configure where a shortcut for the application is created on a user device. Note that shortcuts are not available on all types of operating systems.

The options for creating shortcuts are:

- **Create shortcut on desktop**: If selected, a shortcut will be created on the user desktop.
- **Create shortcut in Start folder**: Creates a shortcut in the Start folder.

- The edit field allows you to enter a folder name where a shortcut will be created. The default (and the only one available) %Groups% variable will add additional subfolders as they appear on the host server where the published resource is located. For example, if the resource is located in "Myapps > Games" on the host server, the same folder structure will be added to the path. Note that you cannot use any custom variables.
- **Create shortcut in Auto Start folder**: The application shortcut will be added to the Auto Start folder and will start automatically on computer startup.

License

Configure the following options for better control of the application license usage:

- **Disable session sharing**: If this option is enabled, it allows you to isolate a given published application to one session. If the same application is launched more than once, the instances of the application will share the same sessions. A different application, however, will start in its own session.
- **Single instance per user**: 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. For example, 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 an action that should be taken when a licensing limit is exceeded.

Display

Configure the following options:

- **Wait until all RAS Universal Printers are redirected before showing the application**: Enable this option to wait for printers to be redirected before the application is loaded. You can also specify the maximum wait time (in seconds) for the Universal Printers to be redirected. Please note that redirecting a printer may take some time. To avoid confusion, a progress bar is shown to the user while the printers are being redirected.
- **Maximum time to wait (seconds)**:
- **Color depth**: Select a color depth for the application.
- **Start the application as maximized when using mobile clients**: This option applies only to Parallels Client running on mobile devices. When the option is selected, the application will start on a mobile device in the maximized state. This gives users the best experience while working with a remote application. This option gives the RAS administrator an easy way to always maximize an application without taking any additional steps.

Maintenance message

The **Maintenance message** view allows you to specify a message that users will see when trying to launch a published resource in maintenance. When a resource is in maintenance, it will still appear in Parallels Client, but will be grayed out (in User Portal, it will say so in the resource name). If a user tries to open the resource, they will see the message that you specify here. If you modified a message, but want to return the default one, select a message in the desired language and click the **Reset** button.

When done making changes to Site defaults, click **Save**.

Using filtering rules

Filtering rules is a feature that allows you to control who can access a particular published resource. Each rule consists of one or several criteria for matching against user connections. In turn, each criteria consists of one or several specific objects that can be matched.

You can match the following objects:

- User, a group the user belongs to, or the computer the user connects from.
- Secure Gateway the user connects to.
- Client device name.
- Client device operating system.
- Theme.
- IP address.
- Hardware ID. The format of a hardware ID depends on the operating system of the client.

Notice the following about the rules:

- Criteria are connected by the AND operator. For example, if a rule has a criteria that matches certain IP addresses and a criteria that matches client device operating systems, the rule will be applied when a user connection matches one of the IP addresses AND one of the client operating systems.
- Objects are connected by the OR operator. For example, if you only create a criteria for matching client device operating systems, the rule will be applied if one of the operating systems matches the client connection.
- The rules are compared to a user connection starting from the top. Because of this, the priority of a rule depends on its place in the rule list. Parallels RAS will apply the first rule that matches the user connection.
- The default rule is used when no other rule is matched. You can set it to either **Allow** or **Deny** (see below), but no criteria is available for this rule.

To create a new rule:

1. Navigate to **Publishing**.
2. Click the resource that you want to create a rules for.
3. In the middle pane, select **Filtering**.
4. Click **Edit**.
5. Click the plus sign.
6. Specify the name and optional description for the rule.
7. Specify criteria for the rule. You will find the following controls:
   - **Allow**: specifies that the resource must be accessible when a user connection matches the criteria. Click **Allow** to change it to **Deny.**
   - **Deny**: specifies that the resource must be inaccessible when a user connection matches the criteria. Click **Deny if** to change it to **Allow**.
   - **(+):** adds a new criteria. If you want to match a Secure Gateway, a client device name, a client device operating system, a Theme, an IP address, or a hardware ID, click **(+)**.
   - **(X)**: Deletes a specific object from matching. For example, you want to delete IP address 198.51.100.1 from matching, click **(X)** next to it.
   - **is:** specifies that the resource must be accessible (or inaccessible, per **Allow** and **Deny**) when a user connection matches the criteria. Click is to change it to **is not**. This control appears when at least one object is added.
   - **is not:** specifies that the resource must be inaccessible (or accessible, per **Allow** and **Deny**) when a user connection does not match the criteria. Click is not to change it to **is**. This control appears when at least one object is added.

   You can disable and enable criteria by clicking on the switch to the left of it.
8. Click **Save** when done.

Configuring preferred routing

Overview

Preferred routing is a useful feature when Parallels RAS users with different geo located deployments are connecting to the same Parallels RAS Farm/Site. A common access layer usage (RAS Secure Gateway, HALB, or a third-party load balancer) is not optimal if a resource is located in a different data center in the same RAS Farm/Site. The solution is to configure a preferred access layer server for a specific published resource, in which case any user would connect to a default Secure Gateway, but would be redirected using proximity rules set by the administrator. Typically, using the Secure Gateway closest to the session host provides improved user experience, reduced internal network traffic and associated costs along with providing better use of resources.

Note: Preferred routing doesn't apply to Azure Virtual Desktop published objects.

Here's how preferred routing works:

1. Parallels Client establishes a connection with a Secure Gateway using a standard authentication.
2. Through the RAS Connection Broker, the resource's preferred route (if configured) is identified.
3. Parallels Client receives the preferred public address to launch the resource.
4. Parallels Client then tries to launch the resource through the redirected address and falls back to the original Gateway if it fails.

Configure preferred routing

To configure preferred routing, you first need to specify one or more custom public server addresses for a Site. To do so:

1. In the RAS Management Portal, select the **Site Settings** category.
2. In the **Connection** menu, select **Addresses**.
3. Click the plus-sign icon and in the dialog that opens specify a name for this custom address, an optional description, a public address, port and SSL port (it is recommended to use an SSL port for user session routing).

Once one or more custom server addresses have been configured, you can specify such an address for a published resource as follows:

1. Select the **Publishing** category.
2. Select a published resource.
3. In the middle pane, select **Routing**.
4. In the editing pane, click **Edit**.
5. Select the **Enable preferred routing** option.
6. Click the plus-sign icon.
7. Select a custom address from the list to be used as preferred route for this published resource.

CHAPTER 10

Monitoring

In This Chapter

Overview

The **Monitoring** category gives you access to the RAS Performance Monitor, which is a browser-based dashboard designed to help administrators analyze 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.

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 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 and/or Parallels Management Portal. 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 **Monitoring** category of Parallels RAS Management Portal, which displays the visual representation of performance counters in real time (using Grafana dashboard).

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.

Install RAS Performance Monitor

Requirements

Parallels RAS Performance Monitor is a separate component of Parallels RAS with its own installer. It can be installed on a dedicated server or on a server hosting any of the Parallels RAS components. When you run the installer, the InfluxDB database and the Grafana dashboard service are automatically installed. For additional info, see the **Installation** subsection below.

The following firewall rules (open ports) are automatically added on the server where you install Parallels RAS Performance Monitor:

- 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.

Enable monitoring in RAS Management Portal

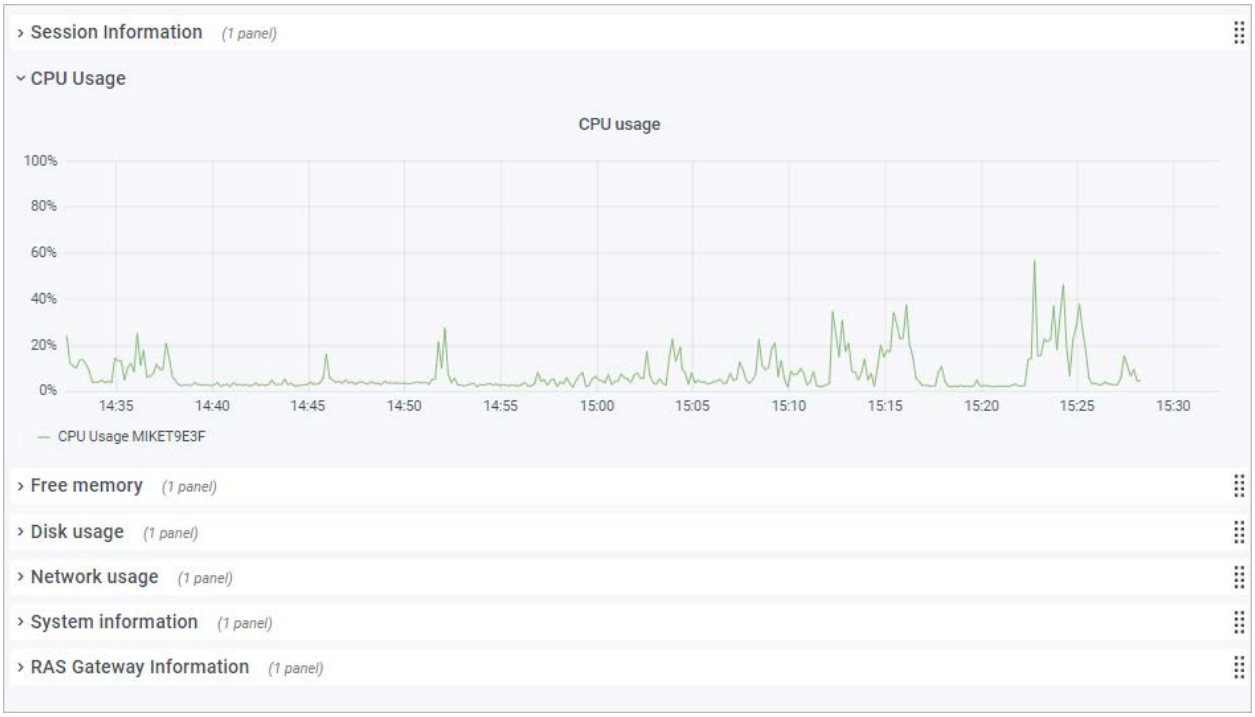
Note: To enable RAS Performance Monitor in the Management Portal you must be a Root administrator of a RAS Farm.

To enable RAS Performance Monitor:

1. In the Management Portal, select the **Monitoring** category in the sidebar.
2. In the right pane, click the **Farm Settings** link. This will take you to the **Farm Settings** category with the **Monitoring** subcategory selected.
3. In the top panel, click the **Edit** button.
4. Select the **Enable RAS Performance Monitor** option.
5. Specify connection settings to the server hosting the RAS Performance Monitor database:
   - **Server**: Enter the FQDN or IP address of the server where you have the InfluxDB database and Grafana dashboard installed.
   - **Port**: The default port is 8086. You can change it if necessary.
6. Click **Save**.

Viewing performance metrics

To view performance metrics, select the **Monitoring** category in the sidebar. The performance dashboard is shown in the right pane.



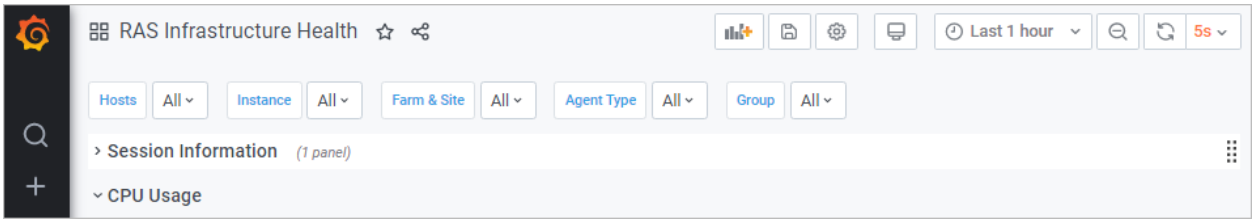
To view metrics of a specific type, expand the desired category in the main area of the dashboard. The categories include:

- **Session Information**. Displays the information about active sessions and disconnected sessions.
- **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.
- **RAS Gateway information**. RAS Gateway counters.

Performance metrics are displayed in the dashboard as a graph. Different counters are displayed using different colors.

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 at the top and then specify a time range.

By default, the dashboard opens in kiosk mode. To exist it, press "Esc". To cycle view mode, click the "monitor" icon in the upper right. When you exist kiosk mode, the **RAS Infrastructure Health** page is displayed:



The menu at the top has 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.
- **Farm & 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.
- **Group**. Select an RDS group.

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. 118).

Configure RAS Performance Monitor Security

By default, any user can access the Performance Monitor page and view performance metrics. To increase security, you can set up the 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\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"`.

> **Note:** The user will be prompted to change the admin password automatically after disabling the anonymous access. After that, the password can be changed following the Grafana official documentation: https://grafana.com/docs/grafana/latest/manage-users/user-admin/change-your-password/.

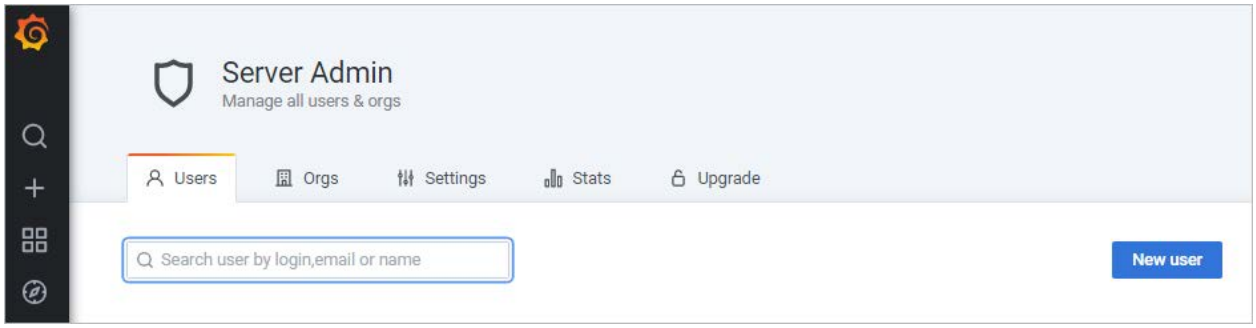
4 Restart the Grafana service.

5 Select the **Monitoring** category and log in to Grafana using the following credentials:

- **User:** admin
- **Password:** admin (if you changed the password before, use the current password).

6 Once logged in, press "Esc" and then click the "shield" icon > **Users**.

7 Click **New user** and create a new user.



8 You now 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**.

9 Click **Add** to add the user to your organization's list. The user can now view the RAS Performance Monitor statistics.

CHAPTER 11

Updating RAS Agents

When you add Parallels RAS components to a Farm, you install a corresponding RAS Agent on them. This includes RAS Connection Broker, RD Session Host Agent, Provider 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 you open the RAS Management Portal, you may see a message saying that RAS Agents require update. You can start the update procedure by clicking the **Update** link, which is included in the message box.

To initiate the procedure manually, select the **Site** category click the **Update all agents** link. 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 are up to date, the **Update all agents** link will not be shown.

CHAPTER 12

Help and Support

The **Help and Support** category contains links to resources to help you find answers to questions, resolve issues, download software and documentation, and to contact Parallels Support.

Note that some links take you to the Parallels My Account page where you need to sign in. If you own a Parallels RAS subscription, you already have an account. If you don't have a Parallels Account yet, you need to create one.

To contact Parallels Support, use the links in the **Support** section:

- **Send system report to Parallels**: Collects the necessary data and sends a system report to Parallels. Please note that this is not an official support request.
- **Download system report**: Collects the data and saves it to the specified location. This may be helpful if a Parallels Support representative asks you to send a report.
- **Create Support Request**: Sends an official support request to Parallels, which can also include a system report providing more environment information to Parallels support. Click this link and follow the onscreen instructions to generate and send a request.

CHAPTER 13

Appendix

In This Chapter

Microsoft license requirements in Parallels RAS

This section is to be used as guidance to provide clarity on Microsoft license requirements in a Parallels RAS environment while not used as an exclusive list. It is recommended to refer to your Microsoft licensing partner for further information.

Microsoft license requirements include:

General

- Any Windows Server and Desktop Operating System (OS) to be used.
- Windows Server OS to be accessed must be covered by Microsoft Windows Server Client Access Licenses (CALs).

RD Session Hosts

If Windows Server is accessed remotely (for non-administrative work) then you need Remote Desktop Service (RDS) access license:

- RDS CALs are required for users or devices that want to utilize Remote Desktop Service functionality on Windows Server. The following types of RDS CAL are available:
  - **a** RDS Device CAL: Permits one device (used by any user) to use Remote Desktop Services functionality on any of your servers.
  - **b** RDS User CAL: Permits one user (using any device) to use Remote Desktop Services functionality on any of your servers.
  - **c** RDS External Connector: Permits multiple external users to access a single Remote Desktop server. If you have multiple servers, you need multiple external connectors in addition to any required Windows Server External Connectors.

You may choose to combine RDS Device CALs and RDS User CALs simultaneously with the server software. Regular User or Device CALs are required in addition to the RDS User or RDS Device CALs.

- RDS SAL is a service that provides a Microsoft Remote Desktop Service Subscriber Access License (called an "RDS SAL") on Virtual Machines created in Compute Resource. This makes it possible for three or more users to connect to a remote desktop (RD Session Host) for a specific Virtual Machine in Compute Resource (for SPLA partners).

Read more:

- License your RDS deployment with client access licenses (CALs): https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-client-access-license.
- RDS Licensing Data Sheet https://download.microsoft.com/download/6/B/A/6BA3215A-C8B5-4AD1-AA8E-6C93606A4CFB/Windows_Server_2012_R2_Remote_Desktop_Services_Licensing_Datasheet.pdf.
- RDS CAL overview and FAQ https://download.microsoft.com/download/3/D/4/3D42BDC2-6725-4B29-B75A-A5B04179958B/Licensing-Windows-Server-2012-R2-RDS-and-Desktop-Apps-for-RDS.pdf.
- Licensing of Microsoft Desktop Application Software for use with Windows Server RDS https://download.microsoft.com/download/3/d/4/3d42bdc2-6725-4b29-b75a-a5b04179958b/desktop_application_with_windows_server_remote_desktop_services.pdf.

Hypervisor and VDI

1 In case using Microsoft Hyper-V as a hypervisor, Microsoft Windows Server Operating System (OS) Licenses are required

   Read more:

   - Windows Server 2022 license datasheet https://www.microsoft.com/en-us/windows-server/pricing.
   - Windows Server 2019 license datasheet https://download.microsoft.com/download/7/C/E/7CED6910-C7B2-4196-8C55-208EE0B427E2/Windows_Server_2019_licensing_datasheet_EN_US.pdf.
   - Windows Server 2016 license datasheet https://download.microsoft.com/download/7/2/9/7290EA05-DC56-4BED-9400-138C5701F174/WS2016LicensingDatasheet.pdf.

2 In case using Virtual Desktop Infrastructure (VDI), Windows Software Assurance or Azure Virtual Desktop Access (VDA) licenses are required. Microsoft licenses Windows by access device:

   - Virtual desktop access rights are a benefit of Windows Client Software Assurance (SA). Customers who intend to use PCs covered under SA have access to their VDI desktops at no additional charge.

- Customers who want to use devices that do not qualify for Windows Client SA, such as thin clients, will need to license those devices with Azure Virtual Desktop Access (VDA) in order to access a Windows VDI desktop. Windows VDA is also applicable to third-party devices, such as contractor or employee-owned PCs.

Read more:

- Windows 11 licensing portal https://www.microsoft.com/en-us/Licensing/product-licensing/windows.
- Windows 10 licensing portal https://www.microsoft.com/en-us/licensing/product-licensing/windows10?activetab=windows10-pivot:primaryr3.
- Licensing Windows desktop operating system for use with virtual machines guide https://download.microsoft.com/download/9/8/d/98d6a56c-4d79-40f4-8462-da3ecba2dc2c/licensing_windows_desktop_os_for_virtual_machines.pdf.
- Licensing the Windows Desktop for VDI Environments https://docs.microsoft.com/en-us/answers/storage/temp/12620-microsoft-vdi-and-vda-faq-v3-0.pdf.

Microsoft Azure

Microsoft Online business services, such as Microsoft 365 or Microsoft Azure, require Microsoft Entra ID for sign-in and to help with identity protection. If you subscribe to any Microsoft Online business service, you automatically get Microsoft Entra ID with access to all the free features. To enhance your Microsoft Entra ID implementation, you can also add paid capabilities by upgrading to Microsoft Entra ID Premium P1 or Premium P2 licenses.

Read more:

- Microsoft Entra ID Implementations https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis
- Azure hybrid benefits https://azure.microsoft.com/en-us/pricing/hybrid-benefit/

Azure Virtual Desktop

- Access to Windows 10 Enterprise multi-session, Windows 11 Enterprise multi-session, Windows 10 Enterprise and Windows 11 Enterprise desktops and apps is provided at no additional cost (excluding compute, storage and networking costs) if you have one of the following per user licenses:
  - **a** Microsoft 365 E3/E5
  - **b** Microsoft 365 A3/A5/Student Use Benefits
  - **c** Microsoft 365 F3
  - **d** Microsoft 365 Business Premium
  - **e** Windows 10 Enterprise E3/E5

f Windows 10 Education A3/A5

g Windows 10 VDA per user

- Access to desktops powered by Windows Server Remote Desktop Services running Windows Server 2012 R2 and newer is provided at no additional cost (excluding compute, storage and networking costs) if you have a per-user or per-device RDS CAL license with active Software Assurance (SA).

Read more:

- Azure Virtual Desktop pricing overview https://azure.microsoft.com/en-us/pricing/details/virtual-desktop/

FSLogix

You are eligible to access FSLogix Profile Container, Office 365 Container, Application Masking, and Java Redirection tools if you have one of the following licenses:

- Microsoft 365 E3/E5
- Microsoft 365 A3/A5/ Student Use Benefits
- Microsoft 365 F1/F3
- Microsoft 365 Business
- Windows 10 Enterprise E3/E5
- Windows 10 Education A3/A5
- Windows 10 VDA per user
- Remote Desktop Services (RDS) Client Access License (CAL)
- Remote Desktop Services (RDS) Subscriber Access License (SAL)

FSLogix solutions may be used in any public or private data center, as long as a user is properly licensed.

Read more:

- FSLogix Overview https://docs.microsoft.com/en-us/fslogix/overview.

Microsoft SQL Server

SQL Server is required if using Parallels RAS Reporting. SQL Server installation may be based on:

- SQL Express which is free but has a database size limit of 10 GB.
- SQL Server commercial edition Standard or Enterprise, using Core based licenses or Server + CAL based licenses.

Read more:

- SQL Server 2019 licensing guide
  https://download.microsoft.com/download/6/6/0/66078040-86d8-4f6e-b0c5-e9919bbcb537/SQL%20Server%202019%20Licensing%20guide.pdf

App-V

App-V is not licensed on its own, but included in other license agreements such as Microsoft Volume Licensing, Windows Software Assurance Microsoft, Remote Desktop Services (RDS) CAL, as part of a wider Microsoft licensing agreement. For instance, with an RDS CAL (either per-user or per-device), App-V client may be used on RD Session Host to deliver App-V applications.

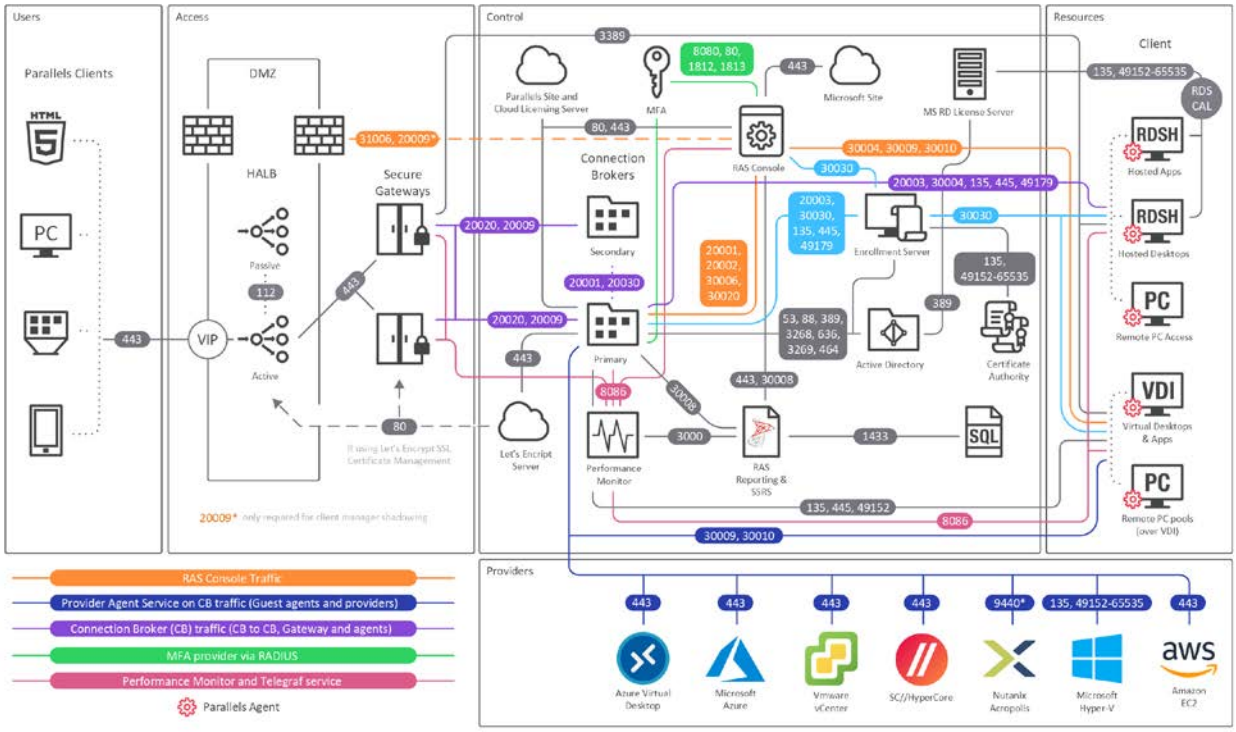
To license App-V correctly it is recommended you to engage with a Microsoft Partner (solution provider) knowledgeable on Microsoft Volume Licensing (list of Microsoft Partners: https://pinpoint.microsoft.com/en-us/search?type=companies&competency=100010).

Other References

For a detailed list of Microsoft Volume Licensing Product Terms please see https://www.microsoftvolumelicensing.com/Downloader.aspx?documenttype=PT&lang=English.

Port reference

The following diagram illustrates communication ports used in Parallels RAS.



The above diagram include SAML SSO components such as RAS Enrollment Server, however it does not include Tenant Broker.

Tip: If you are reading the PDF version of this guide, click the following link to view the full-sized diagram in a web browser: https://download.parallels.com/ras/v19/docs/en_US/Parallels-RAS-19-Administrators-Guide/index.htm#47092.

Parallels Client

Source	Destination	Protocols	Ports	Description
Parallels Client	HALB	TCP, UDP TCP, UDP	80, 443 20009	Management and user session connections. Device Manager shadowing via Firewall (indirect network connection).
	RAS Secure Gateway Forwarding mode	TCP, UDP TCP, UDP UDP	80, 443 3389 20000	Management and user session connections. Optional - Used for user session if RDP load balancing is enabled (Standard RDP).

				Secure Gateway lookup broadcast.
	RAS Secure Gateway Normal mode	TCP, UDP TCP, UDP TCP, UDP UDP	80, 443, 3389 20009 20000	Management and user session connections. Optional - Used for user session if RDP load balancing is enabled (Standard RDP). Device Manager shadowing via Firewall (indirect network connection) Secure Gateway Lookup Broadcast
	Session host (VDI, RDS, RemotePC)	TCP, UDP	3389	Used for user session connections in Direct Mode only. RDP connection is always encrypted.
	Azure Virtual Desktop Services	TCP UDP	443 3390	Azure Virtual Desktop Gateway connection Used for user session connections in ShortPath mode only.
	Microsoft site	TCP	443	Download Microsoft Remote Desktop (MSRDC) client
	Parallels site	TCP	80, 443	Check for updates and download Parallels Client

Web browsers

Source	Destination	Protocols	Ports	Description
Web browser (HTML5) and Let's Encrypt service	RAS Web Admin Service [RAS Management Portal]	TCP	20443	Admin access to HTML5 based Management Portal of RAS environment
	HALB	TCP	80, 443	End-user access to Parallels RAS Web Client (on Secure Gateway in Normal mode) through the HALB **Note:** Ports 80 and 443 must be open for incoming requests when using Let's Encrypt.
	RAS Secure Gateway	TCP	80, 443	End-user access to Parallels RAS Web Client (on Secure Gateway in Normal mode) **Note:** Ports 80 and 443 must be open for incoming requests when using Let's Encrypt.

HALB

Source	Destination	Protocols	Ports	Description
HALB	HALB	VRRP	112	HALB to HALB communication used for automatic assignment of VIP to active HALB.

	RAS Secure Gateway in Forwarding Mode	TCP, UDP	80, 443	Management and user session connections.
	RAS Secure Gateway in Normal Mode	TCP, UDP TCP, UDP	80, 443 20009	Management and user session connections. Device Manager shadowing via Firewall (indirect network connection).

RAS Secure Gateway

Source	Destination	Protocols	Ports	Description
RAS Secure Gateway in Forwarding mode	RAS Secure Gateway in Normal mode	TCP, UDP TCP, UDP	80, 443 3389	Management and user session connections. Optional - Used for user session if RDP Load Balancing is enabled.
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.
RAS Secure Gateway in Normal mode	Remote Desktop Services	TCP, UDP	3389	RDP Connections.
	RAS Connection Broker	TCP TCP, UDP	20002 20009	RAS Connection Broker service port - communications with RAS Secure Gateways and the RAS Console (in Normal mode only). Device Manager shadowing via Firewall (indirect network connection) if RAS Console runs on RAS Connection Broker
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.
	Localhost	TCP	20020	Communication with User Portal web server (NodeJS).

RAS Connection Broker

Source	Destination	Protocols	Ports	Description
RAS Connection Broker	AD DS controllers	TCP TCP TCP,UDP UDP	389, 3268 636, 3269 88 53	LDAP LDAPS Kerberos DNS
	RAS Connection Broker	TCP	20001 20030	Redundancy service. Communication between RAS Connection Brokers running in the same site.

Parallels Licensing Server	TCP	443	RAS Connection Broker (primary Connection Broker in Licensing Site) communicates with Parallels Licensing Server (https://ras.parallels.com). **Note:** Not required for Tenant Broker RAS Connection Broker (see the **Tenant Broker** section).
RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.
RAS RD Session Host Agent	TCP, UDP	30004	Server for Connection Broker requests.
RAS Provider Agent	TCP, UDP	30006	Provider Agent communication port.
RAS Remote PC Agent	TCP, UDP	30004	Remote PC Agent Communication Port (agent state, counters and session information)
2FA Server(s)	TCP, UDP	8080, 80 1812, 1813	Deepnet/ Safenet Radius
RAS Enrollment Server	TCP	30030	RAS Connection Broker Sends RAS Enrollment Server connection Request
RAS Reporting	TCP	30008	Master RAS Connection Broker communicates with RAS Reporting (installed on the same host as SSRS).
RAS Remote Installer Service	TCP	30020	Remote agent pushing
RAS RD Session Host Agent RAS Guest Agent RAS Remote PC Agent RAS Connection Broker RAS Secure Gateway RAS Enrollment Server	TCP	135, 445, 49179	Remote Install Push/Takeover of Software
SMTP	TCP	587	Notifdispatcher is the service which sends the emails using port specified in the Mailbox settings (+SSL/TLS)
Let's Encrypt Service	TCP	80, 443	Communication between the Let's Encrypt client (available in the primary Connection Broker) and a Let's Encrypt server.

RAS Console

Source	Destination	Protocols	Ports	Description
RAS Console	RAS Reporting	TCP	30008	RAS Console is connected to primary RAS Connection Broker which communicates with RAS Reporting (installed on the same host as SSRS). SSRS talks to SQL via TCP 1433 (or dynamic if 1433 is not established in the settings).
	SSRS	TCP	443	Reports retrieval.
	HALB	TCP, UDP	31006	Used for configuration.
	Parallels Client	TCP	50005	Shadowing from the RAS Console in case of direct network connection.
	RAS RD Session Host Agent	UDP, TCP	30004	Used for the "Check Agent" task. Used to manage components.
	RAS Guest Agent	TCP UDP	30009 30010	Used for the "Check Agent" task. Used to manage components.
	RAS Remote PC Agent	UDP, TCP	30004	Used for the "Check Agent" task. Used to manage components.
	RAS Provider Agent	UDP, TCP	30006	Used for the "Check Agent" task. Used to manage component.
	MFA Server(s)	TCP, UDP	8080, 80, 1812, 1813	Deepnet / Safenet / Radius
	Microsoft site	TCP	80, 443	Check for updates and download Parallels Client
	Parallels site	TCP	80	Check for updates and download Parallels Client
	RAS Performance Monitor	TCP	3000	RAS browser plugin connection to Grafana.
	RAS Connection Broker	TCP	20002, 20001	Communication with Connection Broker and redundancy.
	RAS Enrollment Server	TCP, UDP	30030	Used for the "Check Agent" task. Used to manage components and for troubleshooting.
	Wyse Broker	UDP	1234 (outbound only) 68 (inbound only)	Wyse broker discovery request broadcast packet (V_WYSEBCAST). Wyse broker discovery reply packet (V_WYSETEST).
	SMTP	TCP	587	RAS Console can send test emails using port specified in the Mailbox settings (+SSL/TLS)

SSRS

Source	Destination	Protocols	Ports	Description
SSRS	Microsoft SQL Server	TCP	1433	RAS Console is connected to RAS Reporting

RAS Reporting

Source	Destination	Protocols	Ports	Description
RAS Reporting Service	MS SQL	TCP	1433	Store RAS activity information
	SSRS	TCP	8085, 443	Enumeration of reports (incl. custom reports)

RAS Web Administration Service (REST/Management Portal)

Source	Destination	Protocols	Ports	Description
RAS Web Administration Service	RAS RD Session Host Agent	TCP	30004	Log retrieval
	RAS Guest Agent	TCP	30010	Log retrieval
	RAS Provider Agent	TCP	30006	Log retrieval
	RAS Connection Broker	TCP	20002, 20001 30020	Communication with GA and Redundancy Used during publishing to browse for installed applications or single file/folder browsing. 30020 - remote agent pushing (pre-RAS 18).
	RAS RD Session Host Agent RAS Guest Agent RAS Remote PC Agent RAS Connection Broker RAS Secure Gateway RAS Enrollment Server	TCP	135, 445	Remote Install Push/Takeover of Software (pre-RAS 18).
	RAS Reporting Service	TCP	3000	Integration of RAS Reporting in Management Portal iFrame

RAS PowerShell

Source	Destination	Protocols	Ports	Description
RAS PowerShell	RAS RD Session Host Agent	TCP	30004	Log retrieval
	RAS Guest Agent	TCP	30010	Log retrieval
	RAS Remote PC Agent	TCP	30004	Log retrieval
	RAS Provider Agent	TCP	30006	Log retrieval
	RAS Connection Broker	TCP	20002, 20001	Communication with GA and Redundancy Used during publishing to browse for installed applications or single file/folder browsing.

RAS Provider Agent

Source	Destination	Protocols	Ports	Description
RAS Provider Agent	RAS Connection Broker	TCP	20003	Connection Broker communication port.
	RAS Guest Agent	TCP UDP	30010 30009	TCP is used to send the commands. UDP is used during the initial handshake.
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB - applicable to Hyper-V only.
	Hyper-V	TCP	135, 49152-65535	Used to check if the host is powered on and send export, import, delete, shutdown, restart or suspend commands.
	Nutanix AHV (AOS)	TCP	9440	Used to check if the host is powered on and sends clone, delete, shutdown, restart commands (RestAPI calls, PoSH, remote ncli).
	VMWare	TCP	443	Used to check if the host is powered on and sends clone, delete, shutdown, restart and suspend commands.
	Microsoft Azure	TCP	443	Used to check if the guest is powered on and sends clone, shutdown, restart commands (via REST).
	Azure Virtual Desktop	TCP	443	Used to check if the host is powered on and sends clone, shutdown, restart commands (via REST).
	AWS	TCP	443	Used to check if the host is powered on and sends clone, shutdown, restart commands (via REST).

	Scale	TCP	443	Used to check if the host is powered on and sends clone, shutdown, restart commands (via REST).
	Remote PC over VDI	TCP	135, 49152-65535	Used to check if the host is powered on and sends shutdown, restart or suspend commands.

RAS Enrollment Server

Source	Destination	Protocols	Ports	Description
RAS Enrollment Server	AD DS controllers	TCP TCP TCP,UDP UDP	389, 3268 636, 3269 88 53	LDAP LDAPS Kerberos DNS
	RAS Connection Broker	TCP UDP	20003 20003	Settings synchronization and performance counters. Deny Connection Request
	Certificate Authority (CA)	TCP TCP	135 dynamic range 49152 - 65535	DCOM/RPC ports

RAS RD Session Host Agent

Source	Destination	Protocols	Ports	Description
RAS RD Session Host Agent	RAS Connection Broker	TCP, UDP	20003	Used for communications with RAS Connection Brokers.
	Localhost	TCP	30005	For internal commands (memshell, printer redirector).
	FSlogix	TCP	443	Download FSlogix installer
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.
	RAS Enrollment Server	TCP	30030	RAS RD Session Host Agent (PrlsSCDriver) connects to get logon credentials.

RAS Guest Agent

Source	Destination	Protocols	Ports	Description
RAS Guest Agent (used by Azure	Provider Agent	TCP, UDP	30006	Communication with Provider Agent

Virtual Desktop)				Subnet broadcast is sent to find Provider Agent Regular UDP heartbeats
	Localhost	TCP	30005	For internal commands - memshell, printer redirector)
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB
	RAS Enrollment Server	TCP	30030	RAS Guest Agent (PrlsSCDriver) connects to get logon credentials
	FSlogix	TCP	443	Download FSlogix installer

RAS Remote PC Agent

Source	Destination	Protocols	Ports	Description
RAS Remote PC Agent	RAS Connection Broker	TCP, UDP	20003	Used for communications with RAS Connection Brokers
	Localhost	TCP	30005	For internal commands - memshell, printer redirector)
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB
	RAS Enrollment Server	TCP, UDP	30030	RAS Remote PC (PrlsSCDriver) connects to get logon credentials
	FSlogix	TCP	443	Download FSlogix installer

Tenant Broker

Source	Destination	Protocols	Ports	Description
Tenant - RAS Connection Broker	Tenant Broker - RAS Connection Broker	TCP	20003	Tenant's RAS Connection Broker communicates with Tenant Broker to join Tenant Broker, synchronize configuration and statuses

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.

Azure Virtual Desktop

The Azure virtual machines you create for Azure Virtual Desktop must have access to the following URLs in the Azure commercial cloud:

Address	Outbound TCP port	Purpose	Service tag
*.wvd.microsoft.com	443	Service traffic	AzureVirtualDesktop
gcs.prod.monitoring.core.windows.net	443	Agent traffic	AzureCloud
production.diagnostics.monitoring.core.windows.net	443	Agent traffic	AzureCloud
*xt.blob.core.windows.net	443	Agent traffic	AzureCloud
*eh.servicebus.windows.net	443	Agent traffic	AzureCloud
*xt.table.core.windows.net	443	Agent traffic	AzureCloud
*xt.queue.core.windows.net	443	Agent traffic	AzureCloud
catalogartifact.azureedge.net	443	Azure Marketplace	AzureCloud
kms.core.windows.net	1688	Windows activation	Internet
mrsglobalsteus2prod.blob.core.windows.net	443	Agent and SXS stack updates	AzureCloud
wvdportalstorageblob.blob.core.windows.net	443	Azure portal support	AzureCloud
169.254.169.254	80	Azure Instance Metadata service endpoint	N/A
168.63.129.16	80	Host health monitoring	N/A
https://download.parallels.com/ras/Configuration_01-20-2022.zip	443	Joining a host to a host pool	AzureVirtualDesktop

The following table lists optional URLs that your Azure virtual machines can have access to:

Address	Outbound TCP port	Purpose	Azure Gov
*.microsoftonline.com	443	Authentication to Microsoft Online Services	login.microsoftonline.us
*.events.data.microsoft.com	443	Telemetry Service	None
www.msftconnecttest.com	443	Detects if the OS is connected to the internet	None
*.prod.do.dsp.mp.microsoft.com	443	Windows Update	None
login.windows.net	443	Sign in to Microsoft Online Services, Microsoft 365	login.microsoftonline.us
*.sfx.ms	443	Updates for OneDrive client software	oneclient.sfx.ms

*.digicert.com	443	Certificate revocation check	None
*.azure-dns.com	443	Azure DNS resolution	None
*.azure-dns.net	443	Azure DNS resolution	None

For up to date information, please also visit the Microsoft website at https://docs.microsoft.com/en-us/azure/virtual-desktop/safe-url-list#required-url-check-tool.

RAS performance counters

The following table lists performance counters available in Parallels RAS per component:

Parallels RAS Gateway (2XProxyGateway.exe)

ID	Name	Description
ras_gw_tot_conn	Total connections	The total number of Connections with the Gateway.
ras_gw_tot_threads	Total threads	The total number of threads running on the Gateway.
ras_gw_rpd_sess	RDP tunneled sessions	The number of tunneled RDP sessions.
ras_gw_rpd_sess_s	RDP SSL tunneled sessions	The number of tunneled RDP sessions over SSL.
ras_gw_html	HTTP connections	The number of tunneled HTTP sockets
ras_gw_html_s	HTTPS connections	The number of tunneled HTTPS sockets
ras_gw_html5	HTML5 connections	The number of tunneled HTTP5 sockets
ras_gw_html5_s	HTML5 SSL connections	The number of tunneled HTTP5 sockets over SSL
ras_gw_cm	Device Manager connections	The number of Parallels Device Manager connections
ras_gw_cm_s	Device Manager SSL connections	The number of Parallels Device Manager connections over SSL
ras_gw_wyse	Wyse connections	The number of Wyse connections
ras_gw_wyse_s	Wyse SSL connections	The number of Wyse connections over SSL
ras_gw_rdpudp	RDP UDP tunneled sessions	The number of RDP UDP connections
ras_gw_rdpudp_s	RDP UDP DTLS tunneled sessions	The number of RDP UDP connections over DTLS
ras_gw_cache_sock	Cached sockets	The number of cached sockets between Gateway and Connection Broker
ras_gw_idle_threads	Idle threads	The number of idle threads on the Gateway
ras_gw_client	Client connections	The number of Parallels Client connections
ras_gw_client_s	Client SSL connections	The number of Parallels Client connections over SSL

Parallels RAS Connection Broker (2XController.exe)

ID	Name	Description
ras_pa_avg_client_connection_time	Average time for client connection	The average client connection time.

ras_pa_avg_client_auth_time	Average time for user authentication	The average time taken to authenticate a user.
ras_pa_avg_client_policy_time	Average time to retrieve user policy	The average time taken to retrieve the user's policy.
ras_pa_avg_client_rep_time	Average time to send client telemetry	The average time taken to send client telemetry. Used by CEP.
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.
ras_pa_avg_client_appicons_time	Average time to retrieve icons	The average time taken to retrieve published items icons.
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)

ID	Name	Description
act_sess	Active RDS sessions	The number of active RDS Sessions.
disc_sess	Disconnected RDS sessions	The number of disconnected RDS Sessions.

Index