Parallels Secure Workspace

Admin Manual

5.6

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

Document Guidance

Introduction	This document is an introduction to the Parallels Secure Workspace Admin Manual which provides guidelines for integrators and customer system administrators for operating an Parallels Secure Workspace environment.
Related Documents	*Parallels Secure Workspace Manual 5.6*
Feedback	We strive to continuously improve our products and to develop solutions that fit the needs of our customers. For questions or feedback on this document, please contact us: https://www.parallels.com/support/
Last Updated	20/10/2023
Intended Audience	This guide is intended for Parallels Secure Workspace integrators and system administrators.

Portals

Parallels My Account

Parallels My Account can be found at my.parallels.com.

After signing in, it is possible to:

- Manage licenses.
- Download software.
- Create support requests, which will be handled by our Support teams if you have an active maintenance and support contract.

Knowledge base

The Parallels Knowledge Base can be found at kb.parallels.com. It contains articles on both generic and specific issues or procedures, frequently asked questions, and step-by-step tutorials on some specific configurations.

Installation

Introduction

This guide describes how you can install and deploy the Parallels Secure Workspace virtual machine.

Connectivity Requirements

Introduction

Before deploying the platform, a few connectivity requirements need to be checked and/or enabled. Please review this section to ensure proper installation and operation.

Connectivity Requirements during Installation:

Each Parallels Secure Workspace appliance is a virtual machine (VM).

During the installation of the Parallels Secure Workspace appliance, we need to be able to have a connection to Parallel's repository servers and sync to the right time zone.

Connection	From	To
NTP: UDP port 123	The Parallels Secure Workspace VM	Internal or external NTP service. A common use case is to use the internal NTP service of the Active Directory domain controller(s), or to rely on the external pool.ntp.org servers. The NTP service should use the same time zone as the hypervisor (UTC is recommended).
DNS: UDP port 53	The Parallels Secure Workspace VM	The DNS server which resolves the NTP (when provided via FQDN*) and repository servers (repo-pub.awingu.com). A common use case is to use the DNS servers integrated in the Active Directory.
HTTP : TCP port 8080	The browser of the admin	The Parallels Secure Workspace VM
HTTP : TCP port 80	The browser of the admin	The Parallels Secure Workspace VM

* FQDN = Fully Qualified Domain Name, e.g. ntp.mycompany.com.

Connectivity Requirements during Operation and Configuration:

The Parallels Secure Workspace appliance has a few requirements for correct operation. Before deployment, check whether the following ports can be opened.

⚠ **Best practice:** Configure the firewall rules to only allow traffic from/to the ports which are needed for operation.

Connection	From	To
LDAP(S): TCP port 389 (or TCP port 636 for SSL encryption)	The Parallels Secure Workspace VM	LDAP servers or Active Directory domain controller(s).
Kerberos: UDP/TCP port 88 and TCP port 464	The Parallels Secure Workspace VM	Kerberos server (Only required when users need to be able to change password at next logon) **Important:** The Kerberos server should also have PTR (reverse DNS) and SRV records in place to locate the KDC server and define the protocol to use**
RADIUS (if used): UDP port 1812	The Parallels Secure Workspace VM	RADIUS service for second factor authentication
CIFS (if used): UDP port 137, TCP port 445	The Parallels Secure Workspace VM	CIFS/SMB file server(s) back-end
WebDAV (if used): TCP port 80 or 443 (or different depending on WebDAV config)	The Parallels Secure Workspace VM	WebDAV file server(s) back-end

RDP: TCP port 3389 (RDP /RemoteApp)	The Parallels Secure Workspace VM	To application server(s) back-end
NTP: UDP port 123	The Parallels Secure Workspace VM	On- or off-site NTP service. A common use case is to use the NTP service of the AD server.

HTTPS: TCP port 443	The Parallels Secure Workspace VM	• The repository servers: https://repo-pub.awingu.com (directly or via the configured HTTP proxy - see Connectivity Settings).
		Only mandatory during upgrades, but required for Anonymous Usage Reporting.
		• When using SaaS services, those services need to be reachable by Parallels Secure Workspace or via the configured HTTP proxy (see Connectivity Settings):
		  • Microsoft OneDrive for Business:
		  • <mydomain>**-my**.sharepoint.com
		  • login.microsoftonline.com
		  • graph.microsoft.com
		  • DUO Multi-Factor Authentication:
		  • <your_api>.duosecurity.com
		  • Automatic certificates through Let's Encrypt (see Certificate Settings):
		  • *.api.letsencrypt.org (⚠ only directly, not through HTTP proxy)

HTTP(S): TCP port 80/443	The Parallels Secure Workspace VM	Web applications reversed proxied by Parallels Secure Workspace
DNS: UDP port 53	The Parallels Secure Workspace VM	DNS server which resolves all connections mentioned above (when provided as FQDN*)
HTTP: TCP port 80 (long living WebSocket)	The (end user browser) client***	• The Parallels Secure Workspace VM • When using automatic certificates (see Certificate Settings): the servers of Let's Encrypt
HTTPS: TCP port 443 (long living WebSocket)	The (end user browser) client***	• The Parallels Secure Workspace VM (Only when SSL Offloader enabled in Connectivity section) • When using automatic certificates (see Certificate Settings): the servers of Let's Encrypt
SNMP (if used): UDP port 161	Monitoring System	The Parallels Secure Workspace VM (Only if SNMP enabled in Connectivity section)
HTTP(s) : TCP port 80/443	All servers involved in Kerberos Authentication (AD and Application Servers)	The Parallels Secure Workspace VM (http(s)://<workspace_url>/crl /<WORKSPACE_DOMAIN_NAME>.crl)
SSH: TCP port 22	The client	The Parallels Secure Workspace VM (Only necessary to access Parallels Secure Workspace using SFTP to obtain the environment backup)

* FQDN = Fully Qualified Domain Name, e.g. http://ntp.company.com
** e.g. *kerberos-master.*(tcp|udp).staging.somewindowsdomain.com - For more information: https://technet.microsoft.com/en-us/library/cc961719.aspx
*** When this connection goes via an SSL offloader, reverse proxy, firewalls, etc., please make sure that WebSockets are supported and that open WebSocket connections are not killed after a while. See SSL offloader, reverse proxy or loadbalancer settings for other important settings.

⚠ For a **multi-node** deployment, all TCP, UDP and ICMP traffic should be allowed between the nodes. This traffic is not encrypted. Each node has an internal firewall only allowing traffic from other nodes (based on the IP address).

ℹ While the appliance always listens for incoming requests on ports 80 (HTTP) or 443 (HTTPS), port forwarding originating from a different port is supported, e.g. https://workspace.company.com:8443 .

Note: Using Parallels Secure Workspace as an IdP in combination with accessing Parallels Secure Workspace on an different port than 80 or 443 is not tested.

Connectivity Requirements only during Remote Intervention:

In some cases, the Parallels support team will request direct SSH access to the appliance. For security, the appliance only allows access using public key authentication (with an optional intervention password on top of the public key authentication).

It is highly recommended to only allow this connectivity during troubleshooting.

Connection	From	To
SSH: TCP port 22	Parallels network (IP address will be provided by support)	The Parallels Secure Workspace VM

Sizing and Scaling Requirements

Standard (minimum) setup

For a standard single node setup, the minimum sizing requirements are:

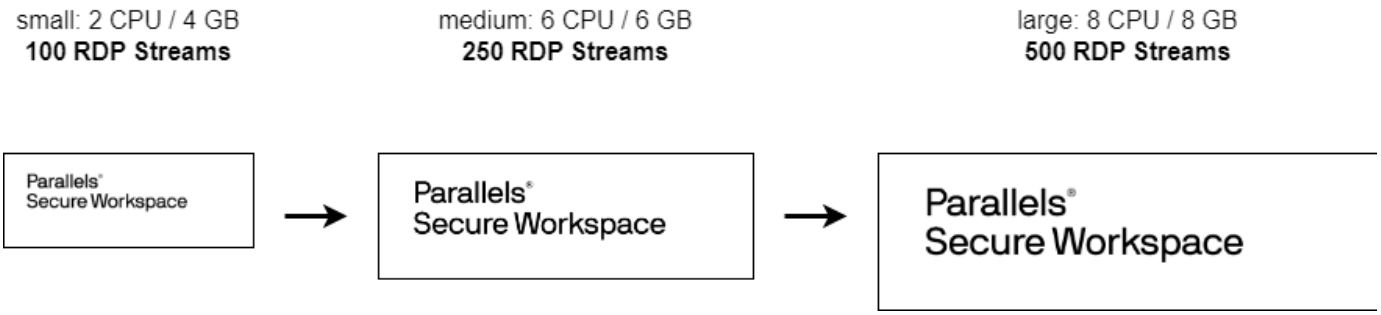
- 2 vCPUs
- 4 GB of memory
- 80 GB of disk space

Scaling

A Parallels Secure Workspace setup can scale on 3 levels:

1) In the appliance

By adding more memory / CPU to a virtual appliance



When adding extra resources like CPU and memory to an appliance, Parallels Secure Workspace will be able to handle more RDP streams and file operations.

The 8 CPU / 8 GB is not a hard limit, but for environments with more than 500 concurrent RDP streams, we generally recommend deploying at least 3 medium servers rather than growing the single node.

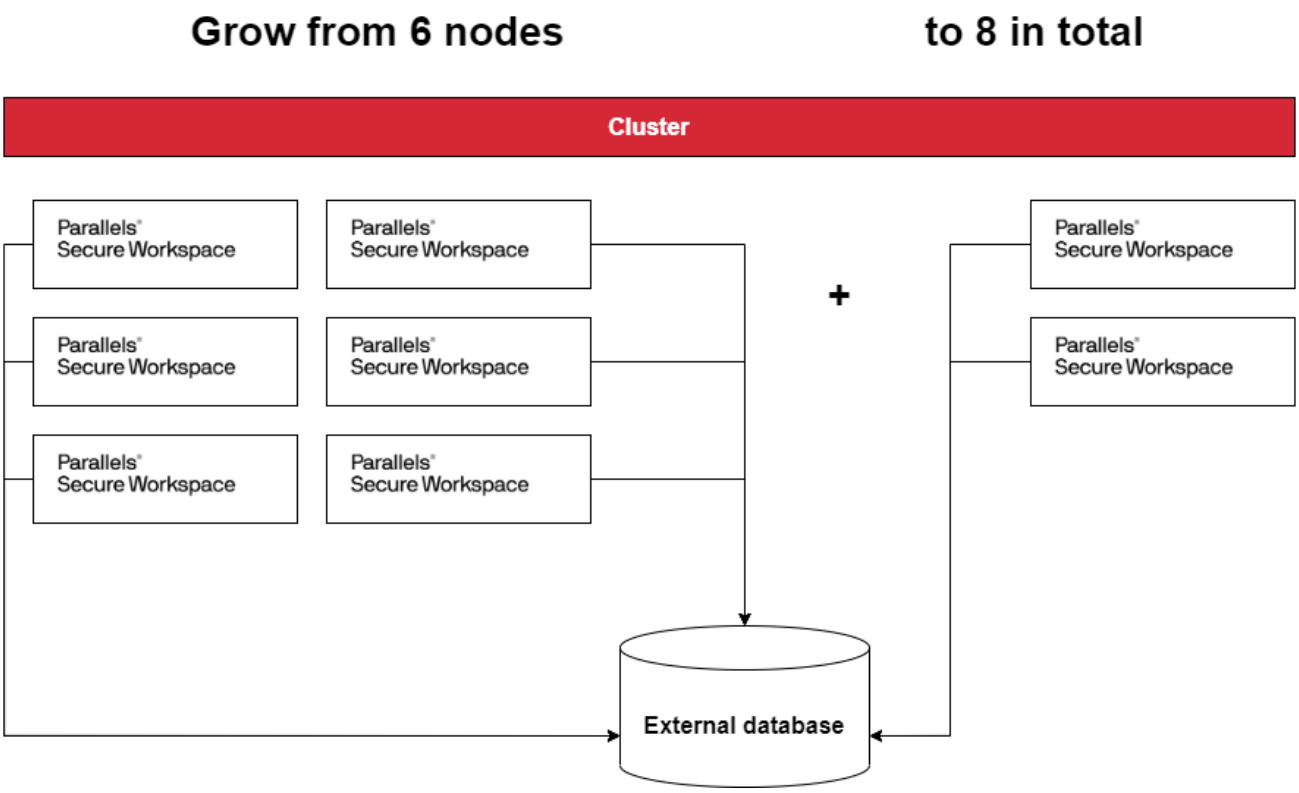
2) In the cluster

Parallels Secure Workspace can be configured in multi-node setup. See Service Management Settings for instructions how to do this. In such a setup, multiple Parallels Secure Workspace appliances (nodes) form a cluster. By adding more nodes to the cluster, you can scale out your Parallels Secure Workspace setup. Adding extra nodes can be done at any time without service impact if the nodes are front-end only nodes.

For this scenario Parallels Secure Workspace assumes that:

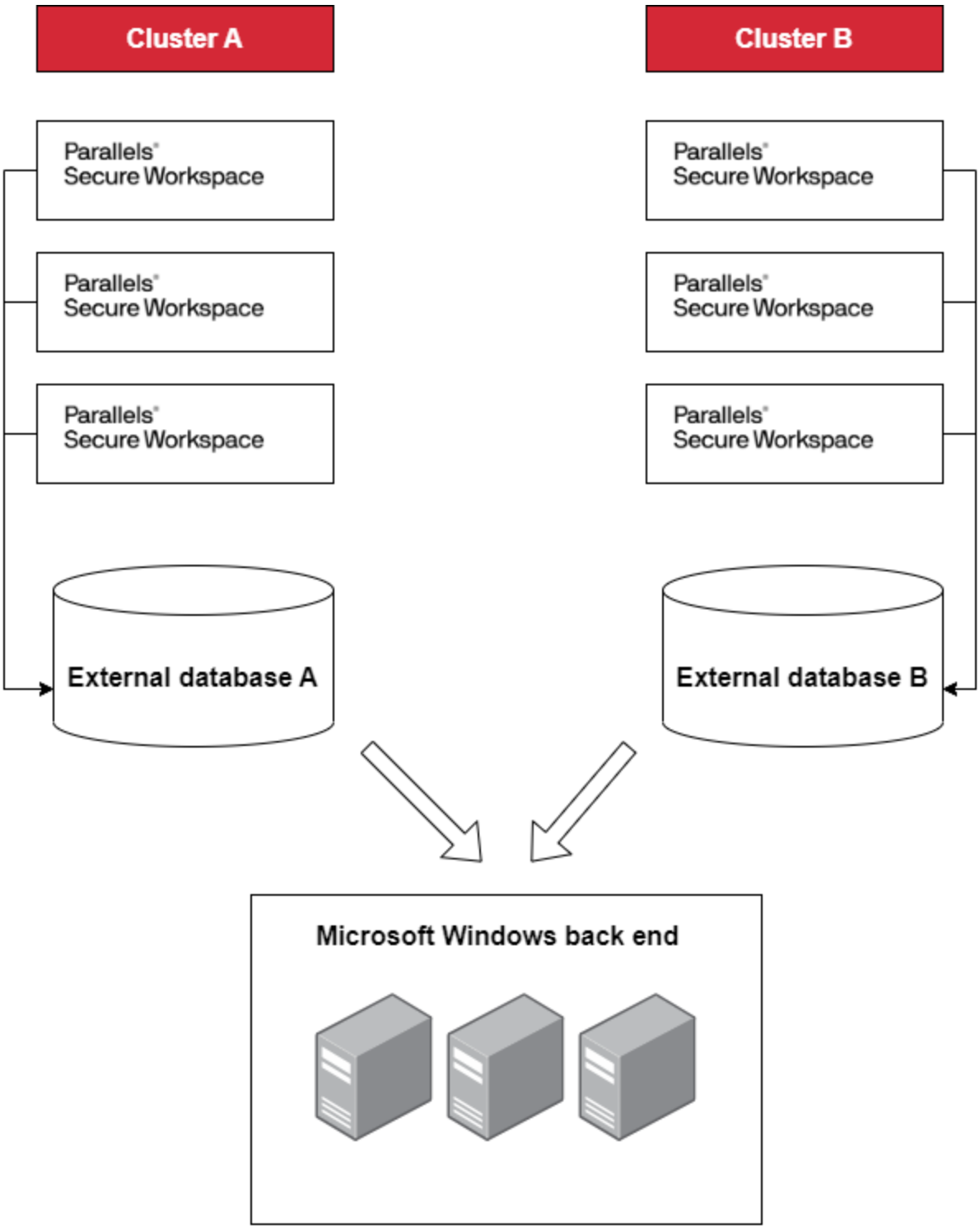
- All data is stored in an external database.
- There is a load balancer in front of Parallels Secure Workspace to balance the incoming requests over the different nodes.

For a cluster setup, there is only one System Settings and one Dashboard. All changes are applied automatically to all nodes of the cluster. When upgrading to a new version, the full cluster will be upgraded at the same time.



3) Making multiple clusters pointing to the (same) Microsoft Windows backend

Multiple, independent clusters can point to the same Microsoft Windows backend since there is no additional software installation required on those back-end servers.



When going to multiple clusters, the configuration of each cluster needs to be maintained separately. If needed this can be (partially) automated via the Parallels Secure Workspace API. (See Automate Parallels Secure Workspace via the REST API)

Sizing Parameters

The sizing of a Parallels Secure Workspace environment is mainly determined by:

- The amount of concurrent RDP streams (number of RDP sessions going from the Parallels Secure Workspace appliance to the Windows back end(s)).
- Type of RDP / Remote apps published behind Parallels Secure Workspace. Apps with lots of screen updates will require more resources than traditional business apps.

- The amount of concurrent file operations (generating previews and file shares).
- Size of the file operations (small files will require less resources than large files).

Next to this other factors may influence the sizing:

- CPU speed / Type
- Overall performance of the underlying storage system
- Overall load on the hypervisor
- High Availability (HA) requirements

For simplicity reasons we have mapped these parameters to 2 user profiles:

- **Light Concurrent User:** User who has 1 RDP stream open and does not use the file operations heavily. This is typically the case when publishing VDIs or when all remote apps in a collection are merged into a single RDP stream.
- **Heavy Concurrent User:** User who has 3 RDP streams open, 10 accesses to reverse proxied web applications and does a number of file operations per hour per user.

Also note that all recommendations are based on concurrent users. A concurrent user is a user that is logged in to the Parallels Secure Workspace appliance and that has at least one application running.

We highly recommend to measure the overall Parallels Secure Workspace appliance resource consumption from time to time and to add extra resources when needed.

Single-node Parallels Secure Workspace

In a single-node setup, all processes are running on a single VM (frontend role, backend role and database role). This architecture can support only a limited number of the concurrent users. This has resulted in the following deployment recommendations:

	Concurrent Light Users	Concurrent Heavy Users
2 vCPU + 4 GB memory	100	50
8 vCPU + 8 GB memory	500	100

Note that 4 GB of RAM is a hard minimum!

Multi-node Parallels Secure Workspace

Once one appliance has been installed, you can add other appliances to it to have a multi-node environment (see Service Management Settings). Note that you need a load balancer in front of the nodes with Frontend roles (see SSL offloader, reverse proxy or loadbalancer settings).

Each appliance can have either just a frontend role; or both a frontend and a backend role:

- The **frontend role** takes care of all RDP and file activity. You need at least 1 of these roles and the more concurrent users you have, the more appliances with these roles you need to deploy
- The **backend role** takes care of the auditing. In a multi node deployment there can only be 1 or 3 back-end nodes. No other combinations are allowed.

Next to the Frontend and Backend roles, there is also a **database role.** When deploying the first Parallels Secure Workspace node, it's possible to use the built-in database or go for an external database. This database contains the Parallels Secure Workspace configuration and not the audit logs as these are stored in the backend roles. It is not possible to change from an internal database to an external database once the installation has finished.

If High Availability (HA) is required, i.e. service interruption is not allowed (except during upgrades), you need at least 3 nodes and an external database (cf. Installation). If an appliance goes down and the Application Sessions Failover feature is enabled, users on that node will be disconnected for a few seconds and then be reconnected to an other node. When the feature is not enabled, user sessions on the failing node will be lost and users will have to login in again and restart their apps.

We assume in a multi-node environment all nodes are 8 vCPU and 8 GB Memory. The sizing below is for normal operations. In case a node goes down, the capacity will be reduced to the capacity of the cluster with 1 node less.

	Roles Configuration	Concurrent Light Users	Concurrent Heavy Users
2 nodes (*)	node 1: Front + Back node 2: Front	1.000	200
3 nodes	node 1, 2 & 3 : Front + Back	1.500	300
4 nodes	node 1, 2 & 3 : Front + Back node 4: Front	2.000	400
5 nodes	node 1, 2 & 3 : Front + Back node 4, 5 : Front	2.500	500
...		+ 500	+ 100
10 nodes	node 1, 2 & 3 : Front + Back node 4-10: Front	5.000	1.000

(*) A 2-node cluster has no HA. If the first node goes down, there will also be impact on the second node as there are no back-end roles available anymore at this time.

Although 10 nodes is not a hard limit we recommend not to go above 10 nodes in a single Parallels Secure Workspace cluster. If more users are needed, we recommend setting up a second cluster and connect it to the same Microsoft Windows back end.

It is recommended to distribute the back-end roles over three differently powered racks to avoid split brain scenarios.

Backup strategy for a multi-node deployment

It is always a good practice to regularly back up the Parallels Secure Workspace environment, especially before upgrades. If the hypervisor allows **consistent** live snapshots, you can use that feature. If consistency is not guaranteed, then follow these instructions:

- For back-end nodes: Please **sequentially** do following actions for each node:
    1. Shutdown **one** node.
    2. Snapshot/back up the node.
    3. Start the node.
    4. Wait until all services in the Dashboard are green.
- For front-end nodes: you can shutdown and start them up all at once.
- If you have an external database, please use the snapshot feature of the database to create a consistent snapshot.

Deployment

Parallels Secure Workspace provides virtual appliances that are custom-built to run on the most commonly used hypervisors and on major cloud platforms.

To begin installing the Parallels Secure Workspace platform, download the virtual appliance for your hypervisor. Import and start the appliance and open your browser to proceed with your installation through the System Settings.

Supported hypervisors

Microsoft Hyper-V Server: 2016 and 2019
VMware ESXi: 7.0 - 8.0
KVM
Citrix Hypervisor: 8.2 (deprecated)

Images of the appliances can be found at https://repo-pub.awingu.com/appliances/

Supported cloud platforms

Microsoft Azure
Amazon EC2
Google Compute Engine

- Deployment on Microsoft Hyper-V
- Deployment on VMware ESXi with vSphere Client on Windows
- Deployment on VMware ESXi with vSphere Web Client
- Deployment on Linux KVM
- Deployment on Microsoft Azure
- Deployment on Amazon EC2
- Deployment on Google Compute

Deployment on Microsoft Hyper-V

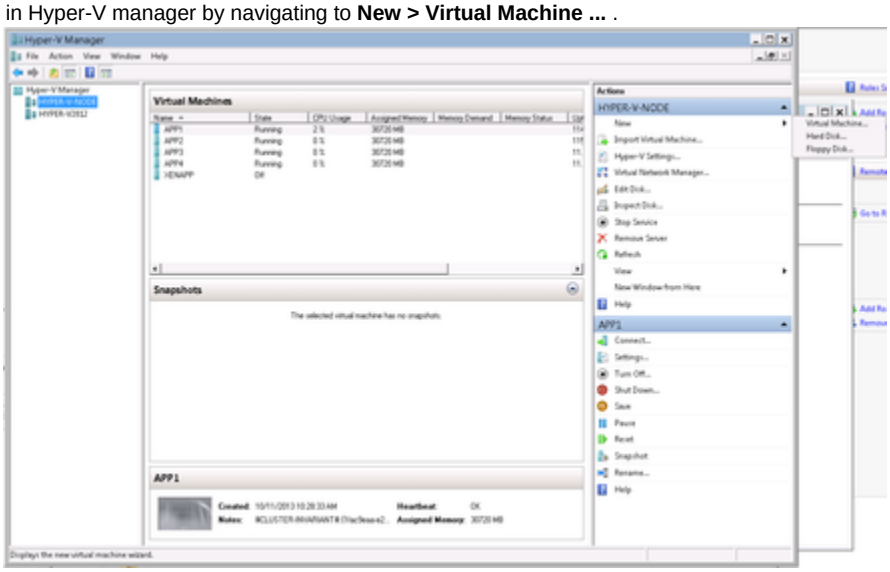
In this guide we will show you how to deploy the Parallels Secure Workspace appliance on Microsoft Hyper-V hypervisor using Microsoft Hyper-V Manager.

Step 1 - Download and extract the Parallels Secure Workspace appliance

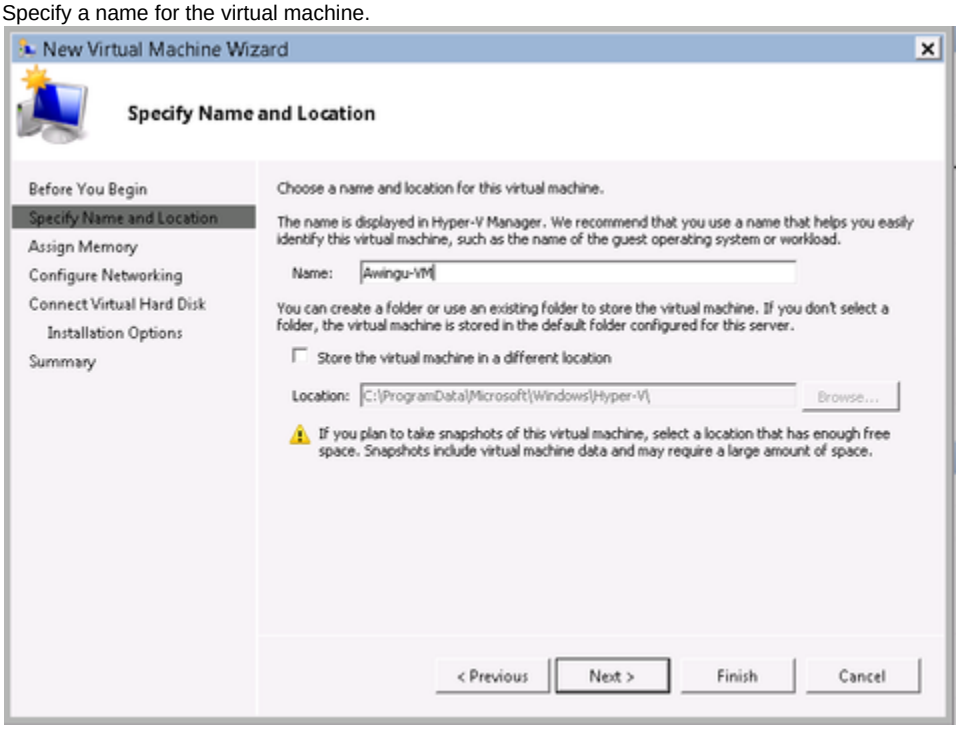
Download the appliance from the repository server at https://psw.parallels.com/appliances/latest/hyperv/ and extract the ZIP file to obtain the VHD.

Step 2 - Create a VM with the VHD image in Hyper-V manager

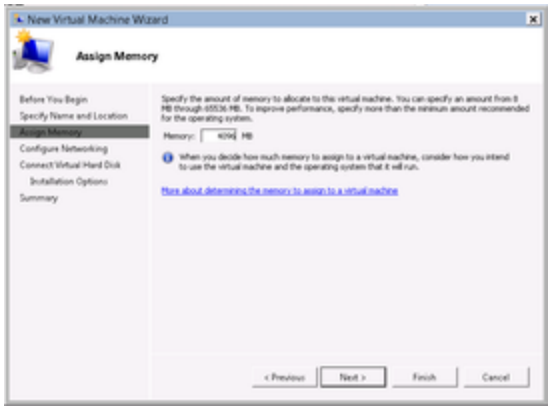
1. Import the VHD image in Hyper-V manager by navigating to **New > Virtual Machine ...** .



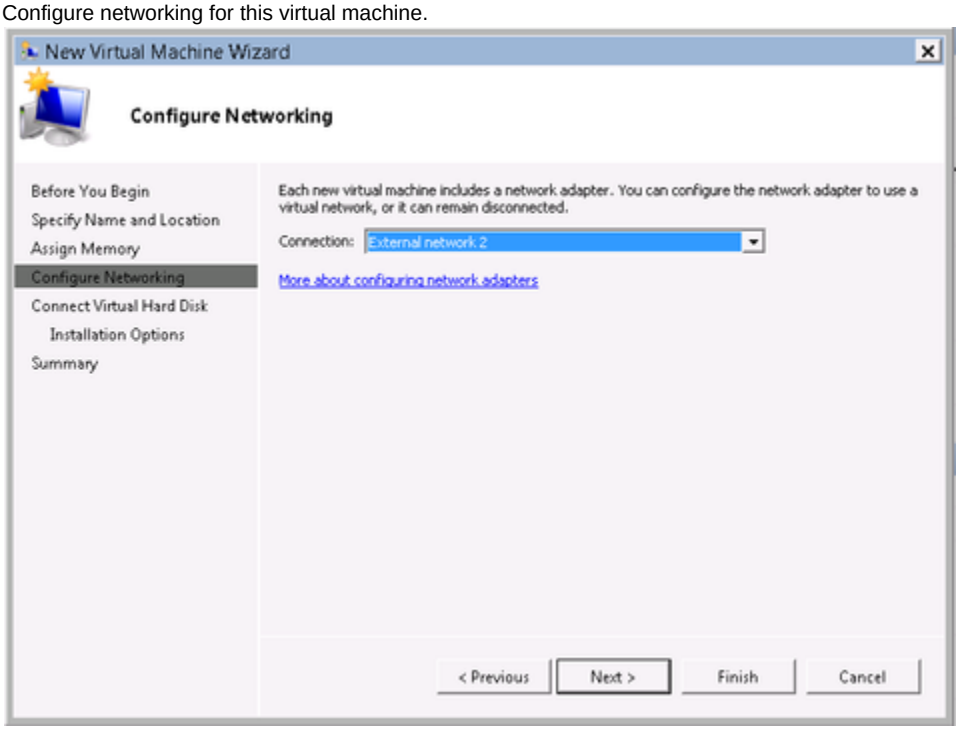
2. Specify a name for the virtual machine.



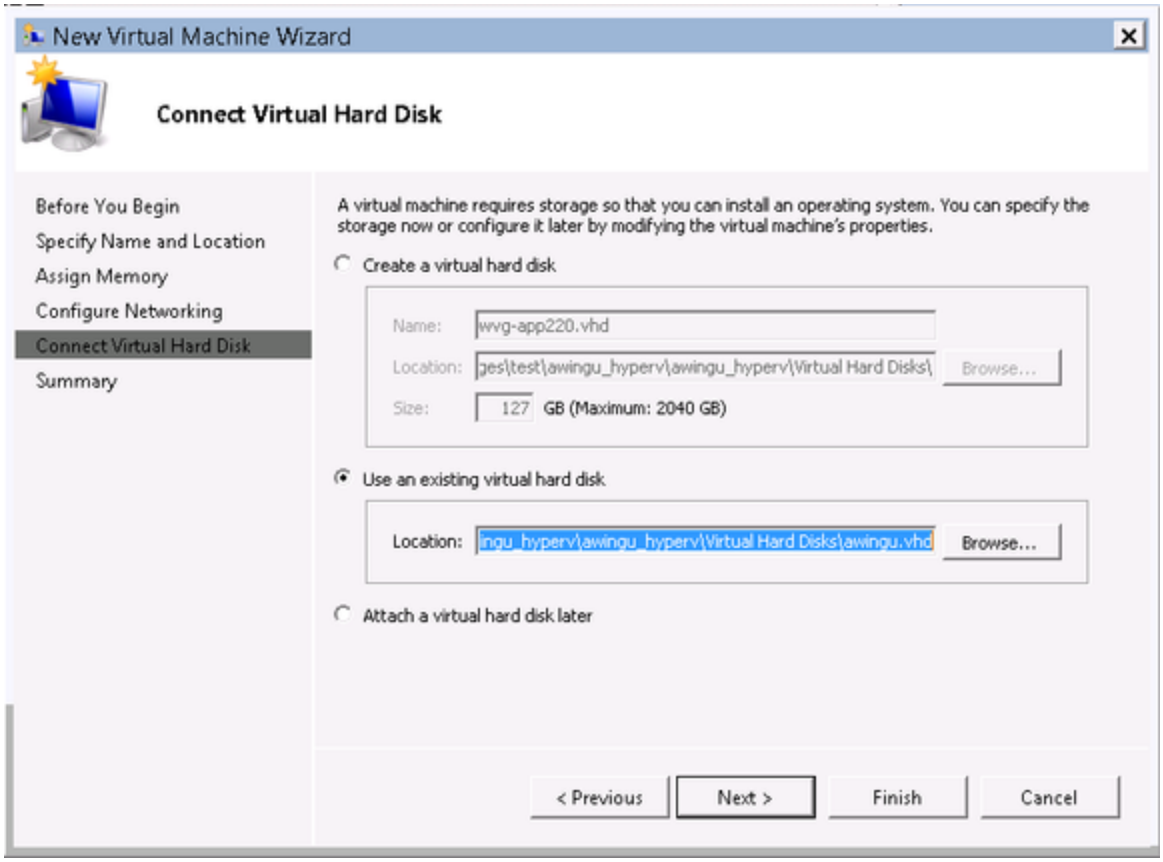
3. Assign memory to the virtual machine. Specify RAM and CPU settings for your VM.
   See Sizing and Scaling Requirements to determine the hardware requirements.



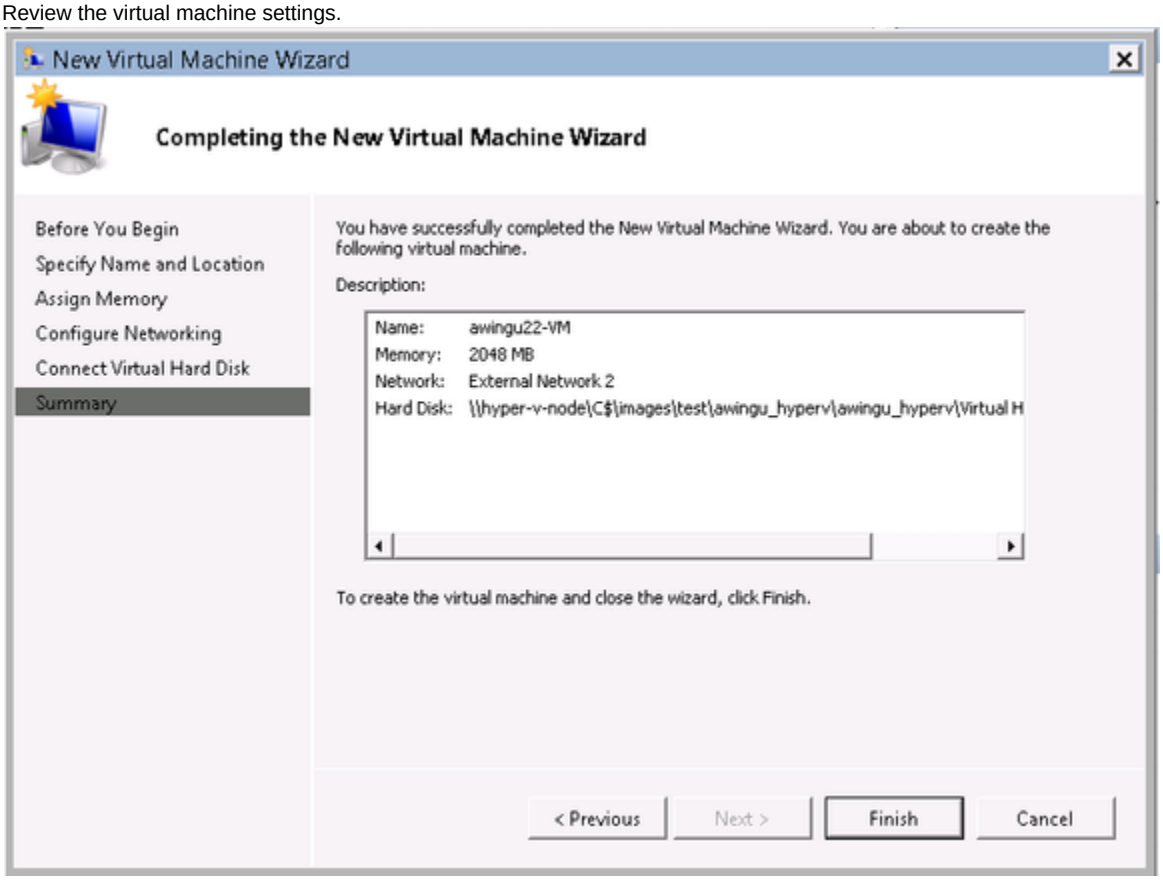
4. Configure networking for this virtual machine.



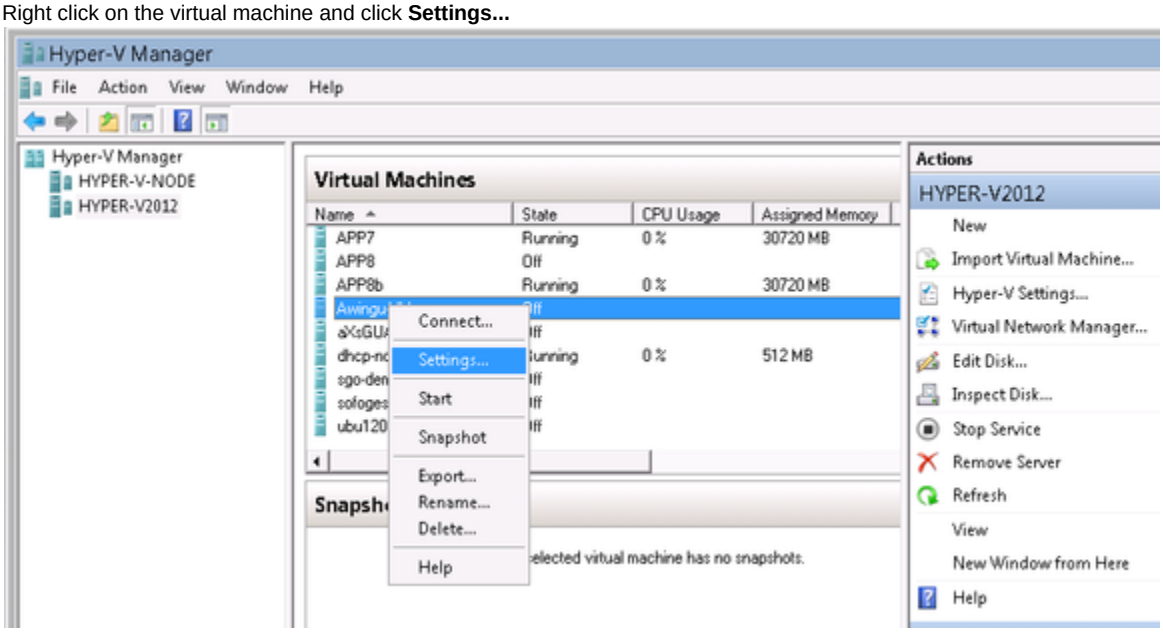
5. Connect to a virtual hard disk by selecting the option Use an existing virtual hard disk. Select the unzipped VHD file.



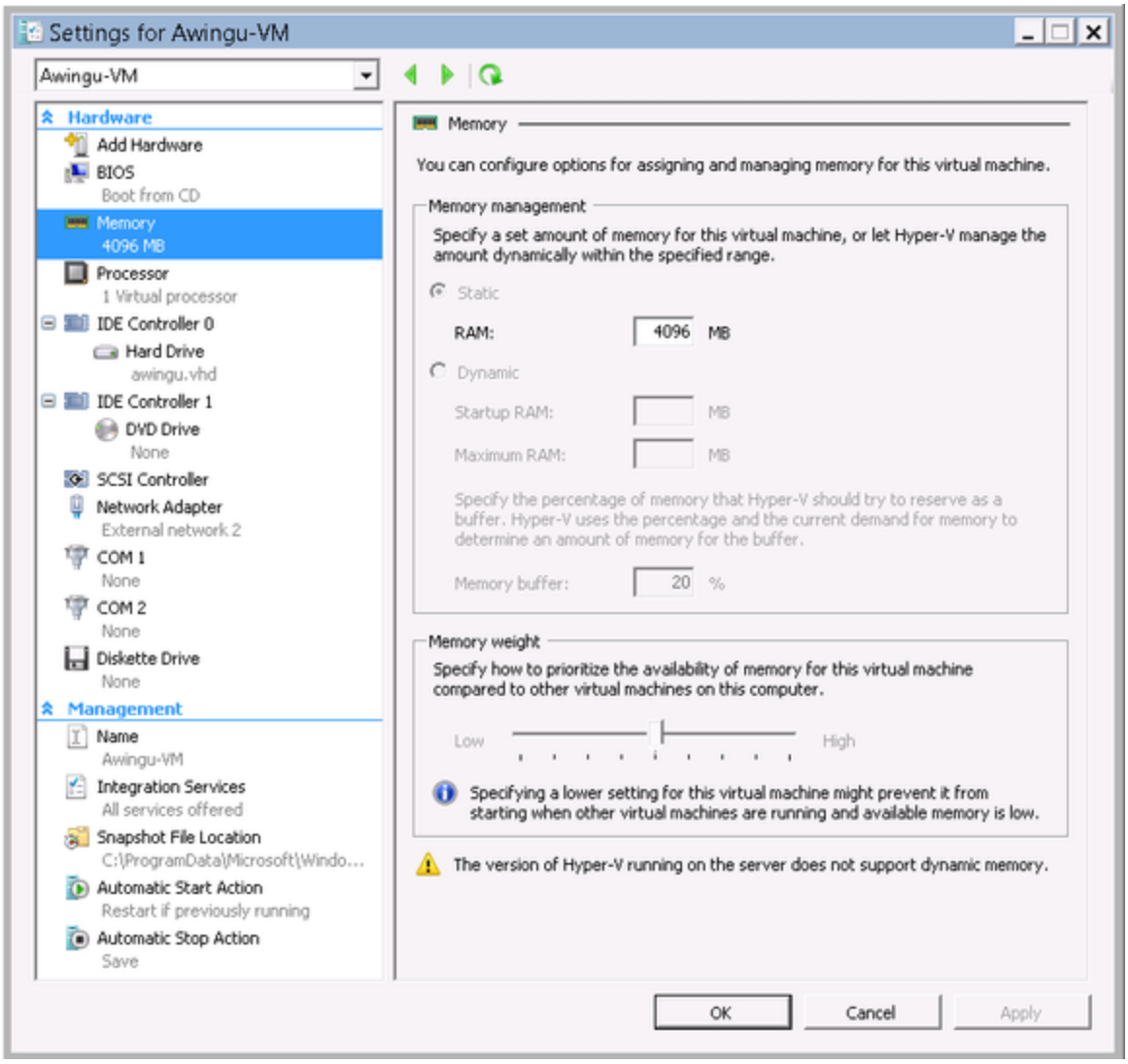
6. Review the virtual machine settings.



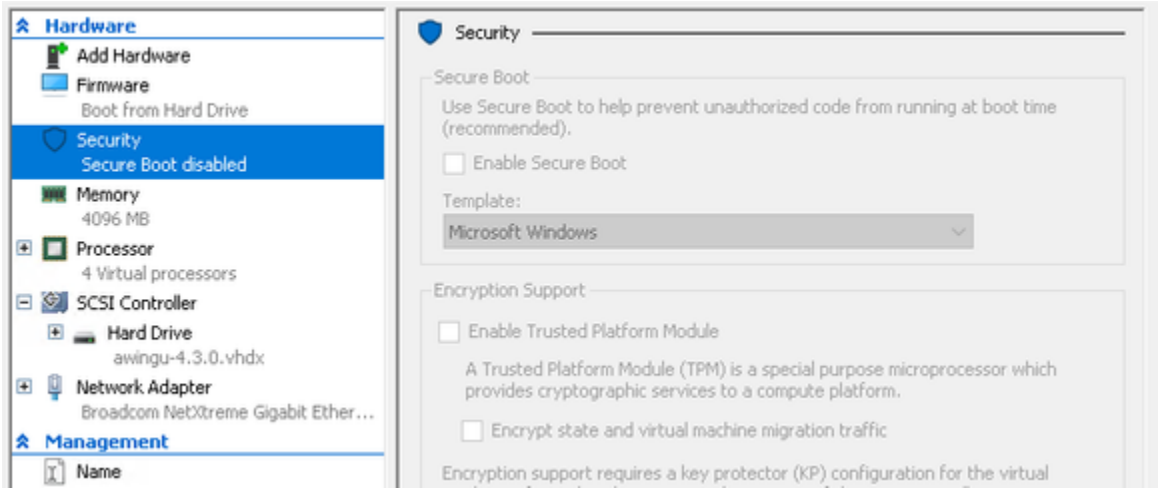
7. Right click on the virtual machine and click **Settings...**



8. Please edit the settings of the virtual machine to specify the memory and CPU settings.
   IMPORTANT In memory management, make sure you select `Static` . Dynamic memory allocation is not supported in Hyper-V Manager for Debian-based Linux systems, so selecting `Dynamic` will result in errors on your VM.

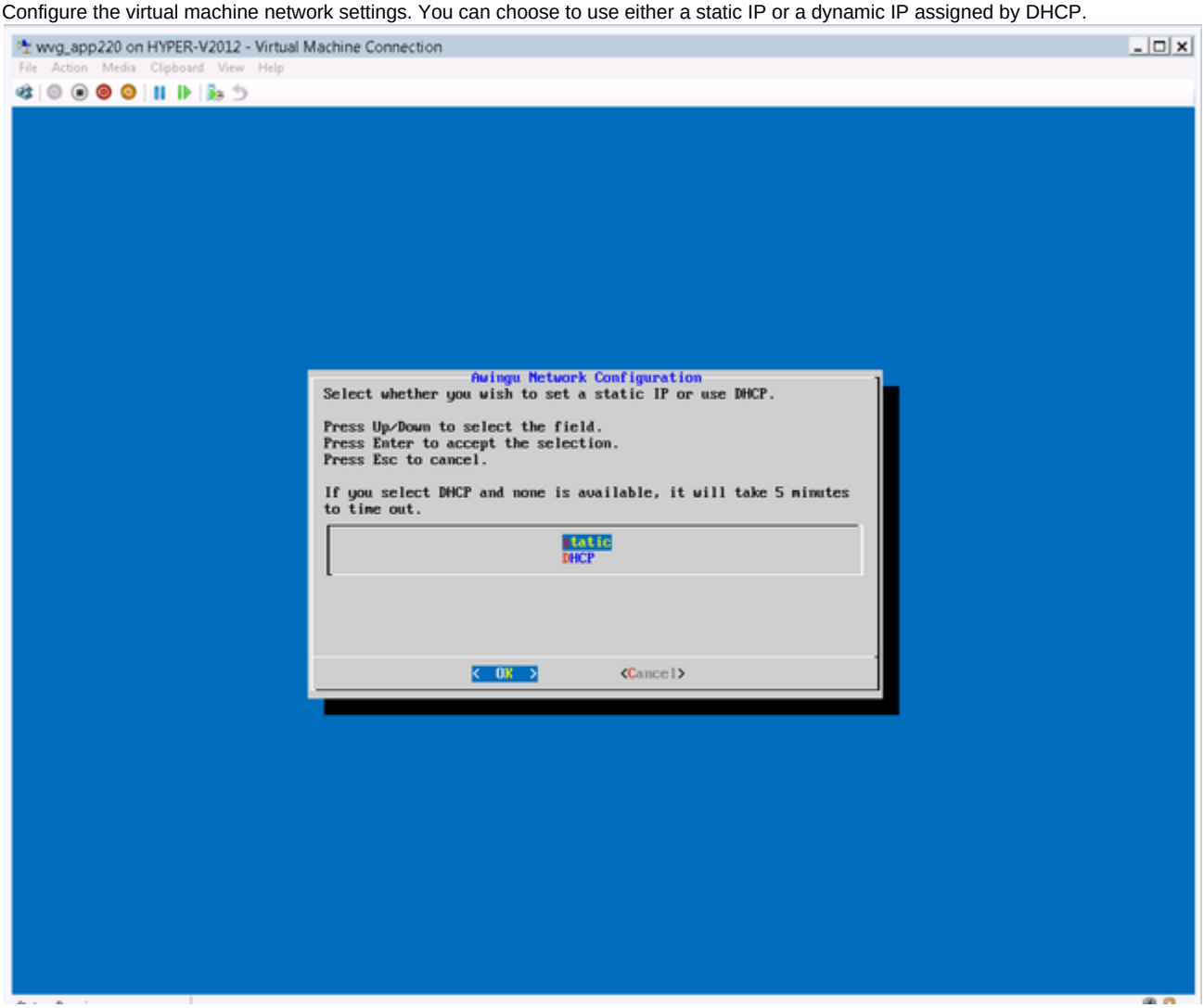


9. Disable `Secure Boot` in the Security section of the settings when using Generation 2 VMs



Step 3 - Boot the Parallels Secure Workspace virtual machine

1. Open a console to connect to the virtual machine.
2. Configure the virtual machine network settings. You can choose to use either a static IP or a dynamic IP assigned by DHCP.



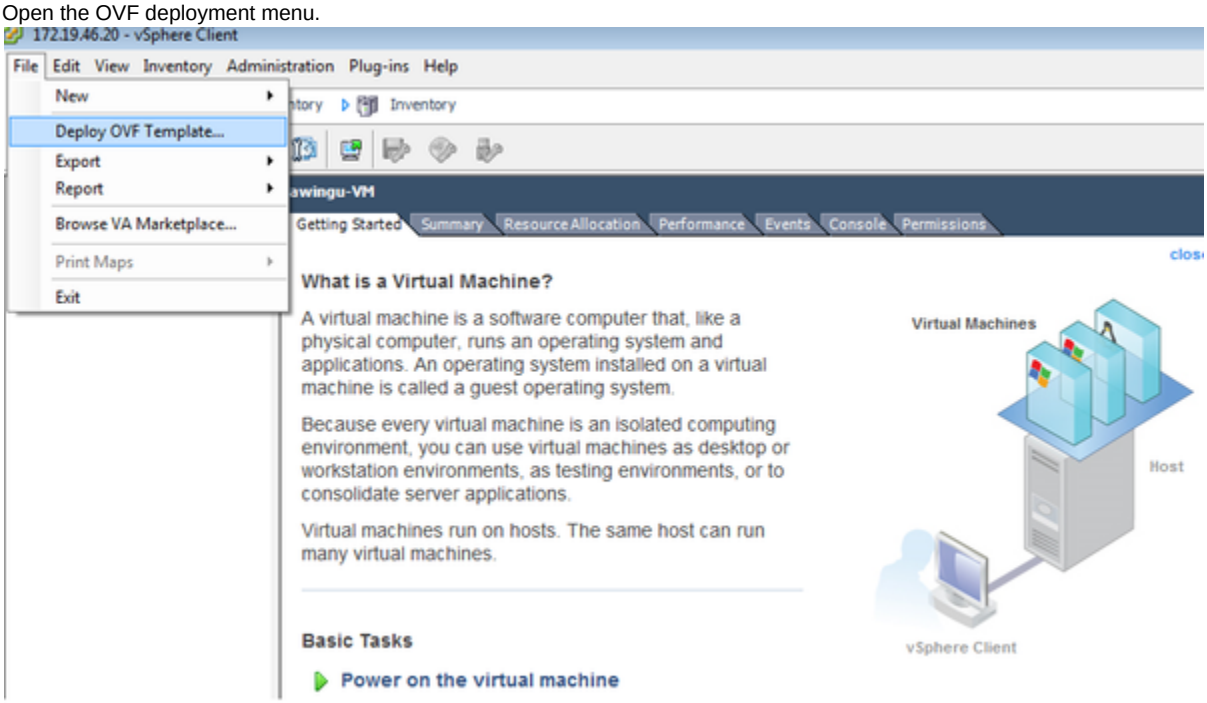
3. After configuring your network settings, you are now ready to proceed with the installation through a graphical installer interface. If you need to change your network settings in the future, you can update these here again. However, this is not supported for multi-node configuration.
   In order to connect to the graphical installer interface, open a web browser and browse to the IP of the Parallels Secure Workspace virtual machine on port 8080. More information about how to proceed with the install can be found here .

Deployment on VMware ESXi with vSphere Client on Windows

In this section, we will show how to install and deploy the Parallels Secure Workspace appliance on VMware ESXi hypervisor.

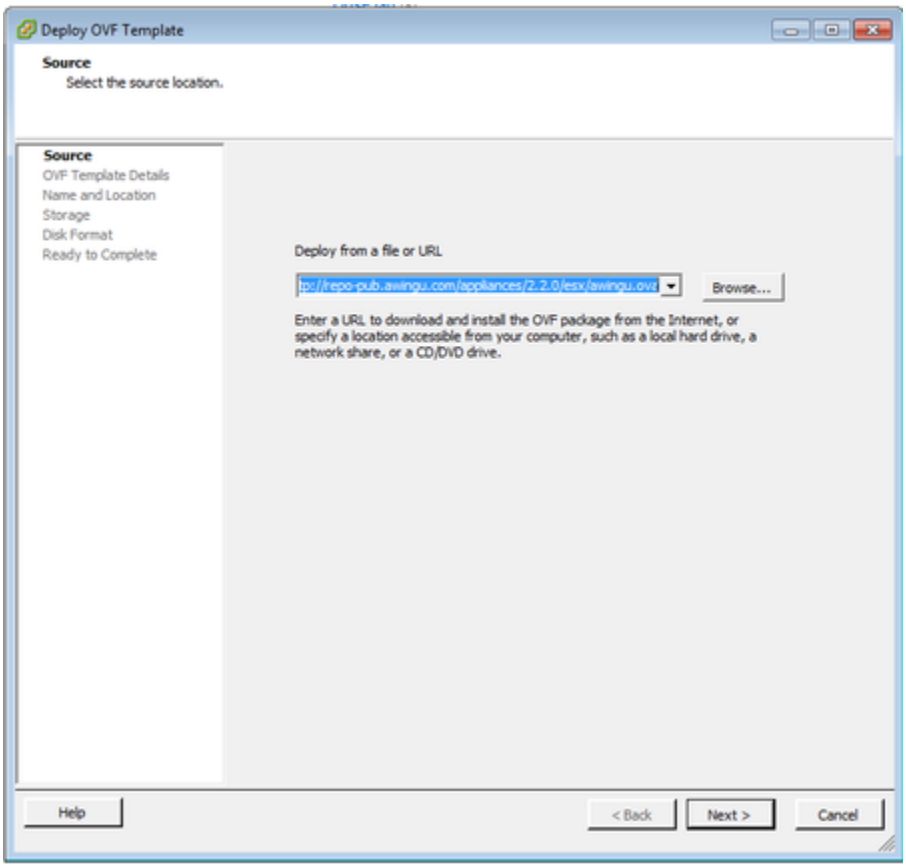
Step 1 - Import the appliance in VMware vSphere Client

1. Connect to your vShpere ESXi hypervisor using vSphere Client
2. Open the OVF deployment menu.



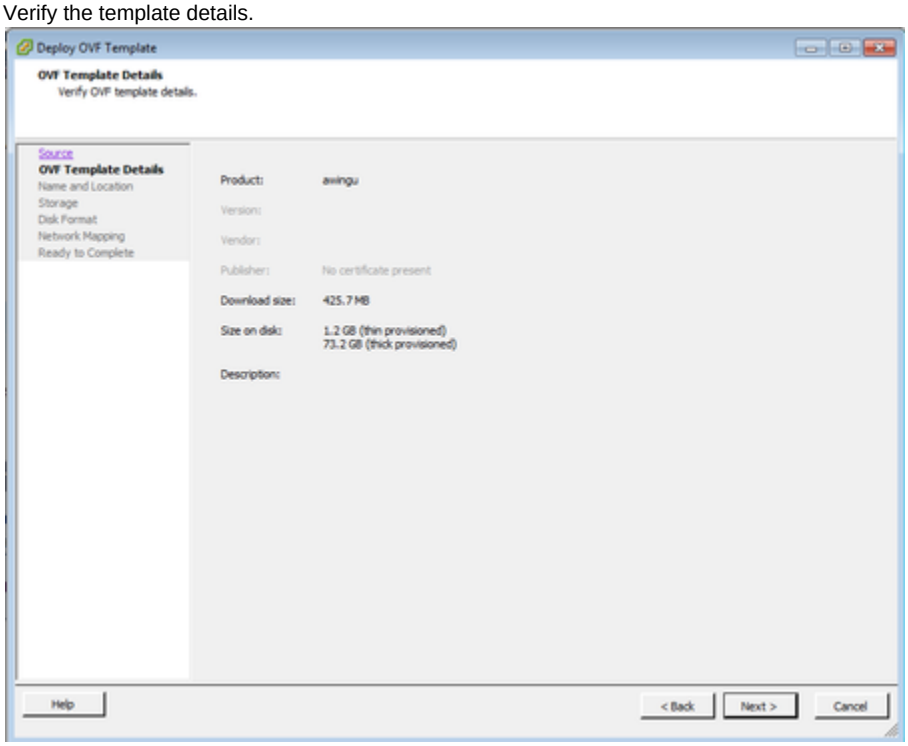
3. Import the Parallels Secure WorkspaceOVF template from the repo server.
   a. Go to https://repo-pub.awingu.com/appliances/latest/ and navigate to the ESX directory.

b. Select the OVA file you want to download and copy-paste this URL into your VMware client import menu:

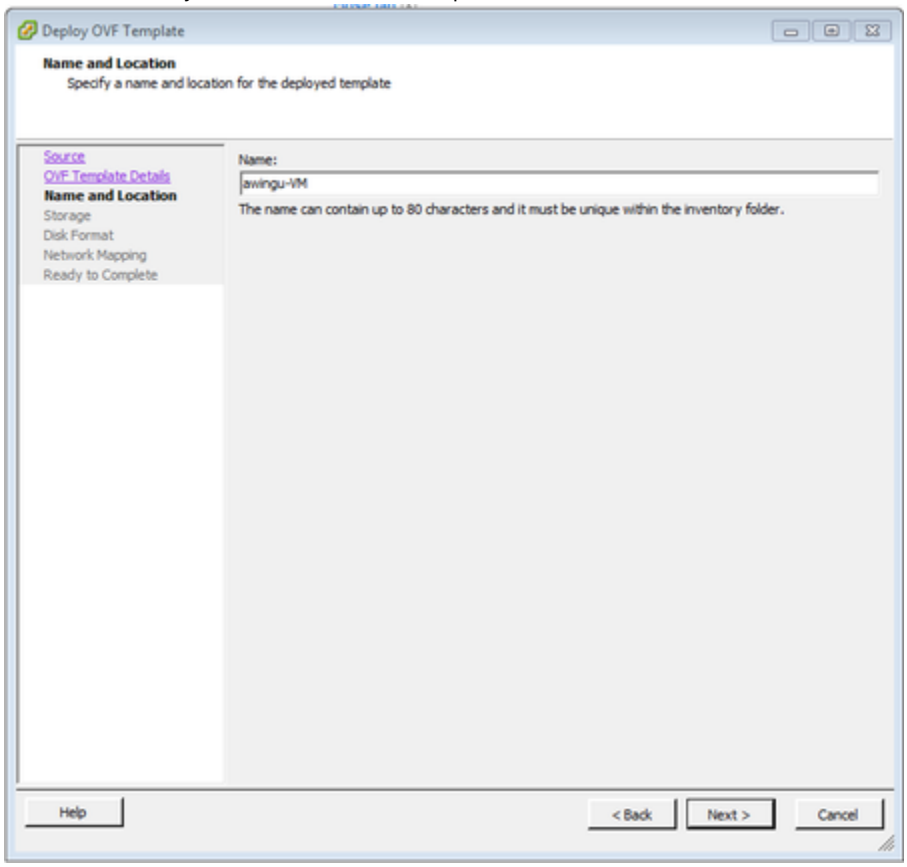


c. Alternatively, you can download the OVA file and use it via the Browse... button.

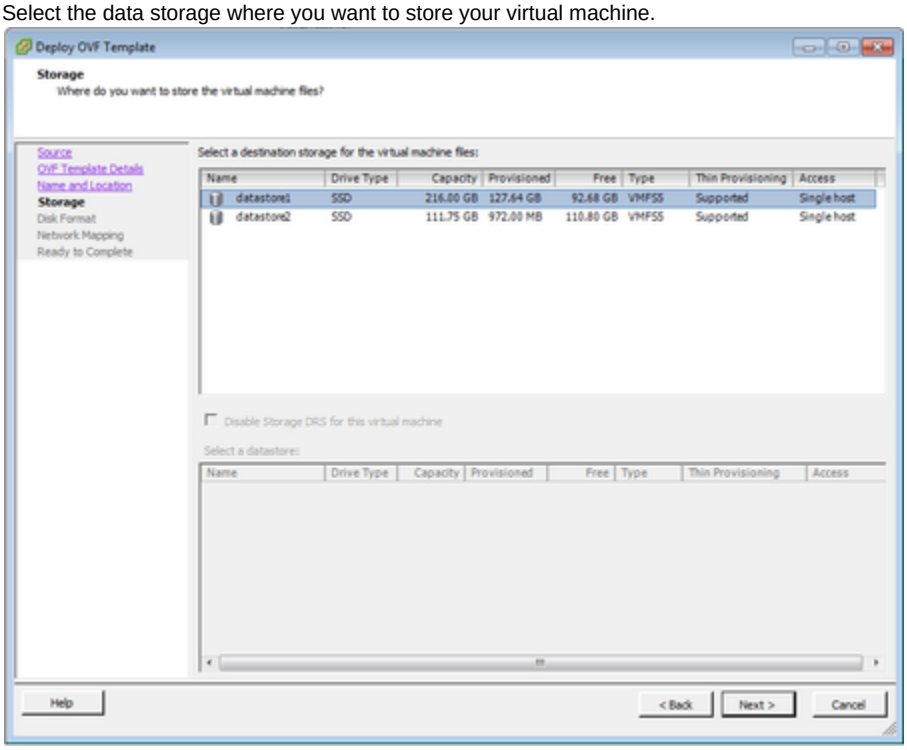
4. Verify the template details.



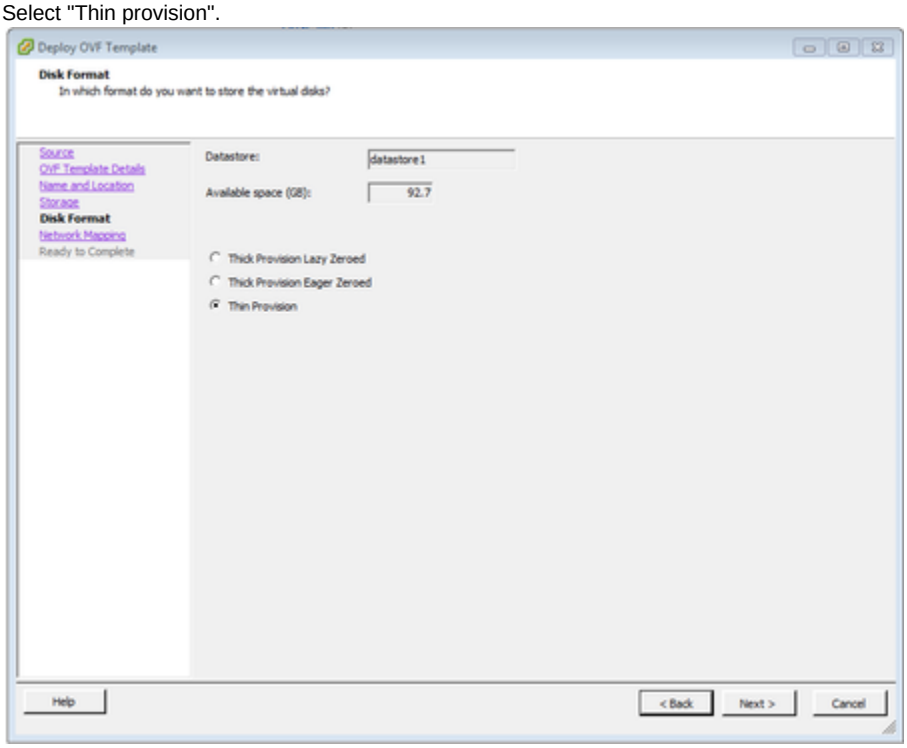
5. Enter the name for your Parallels Secure Workspace virtual machine.



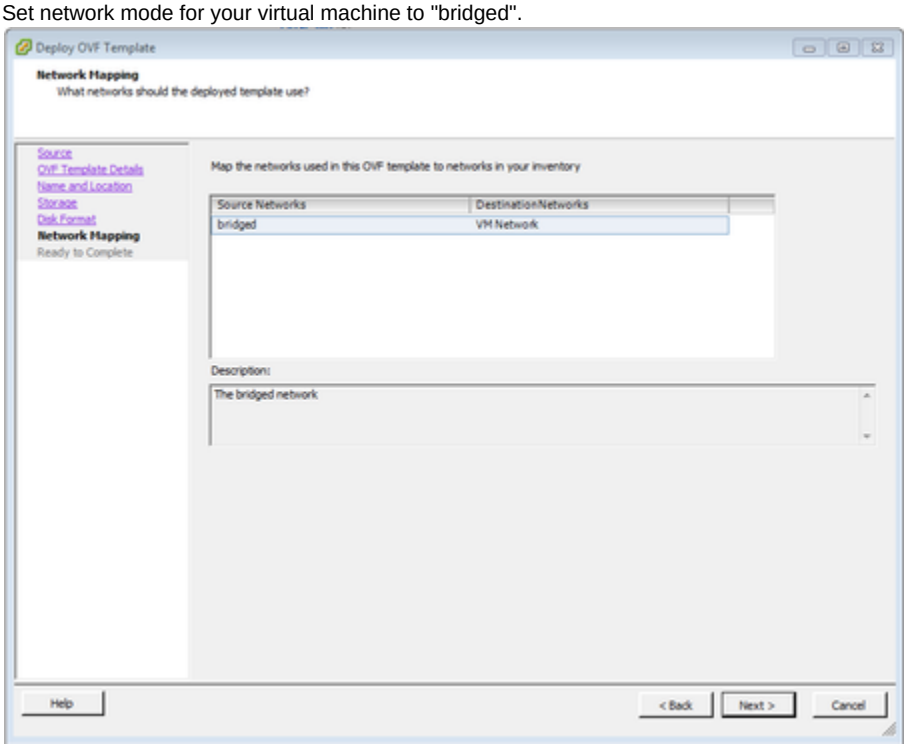
6. Select the data storage where you want to store your virtual machine.



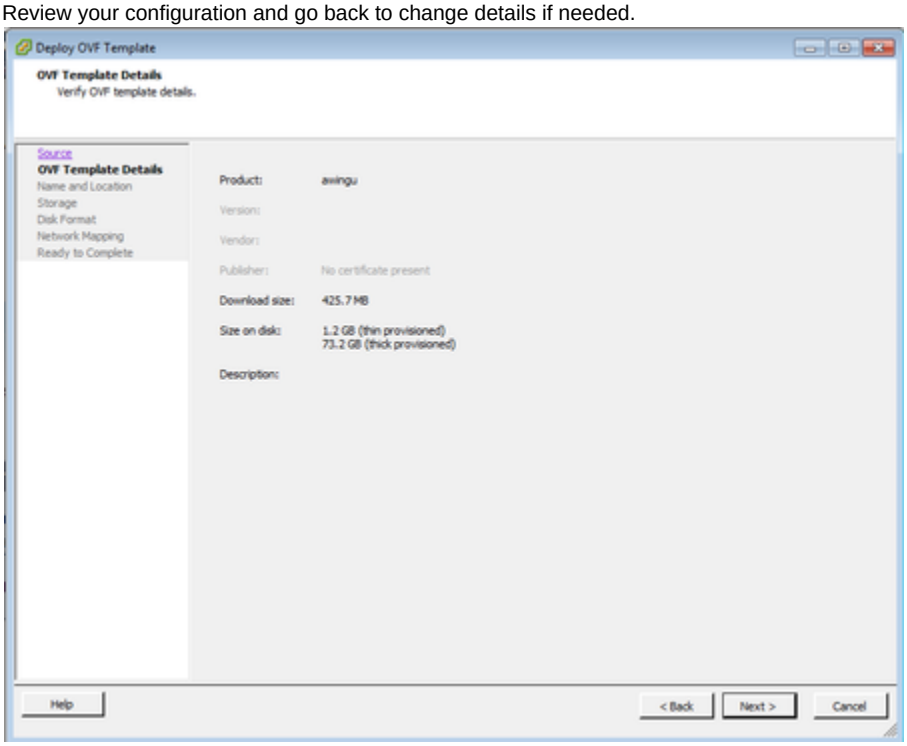
7. Select "Thin provision".



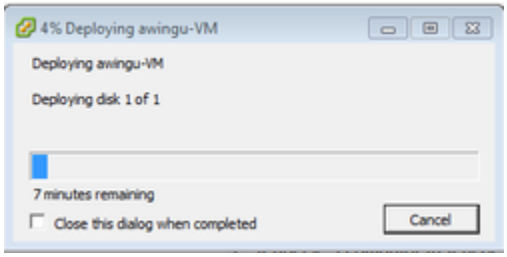
8. Set network mode for your virtual machine to "bridged".



9. Review your configuration and go back to change details if needed.

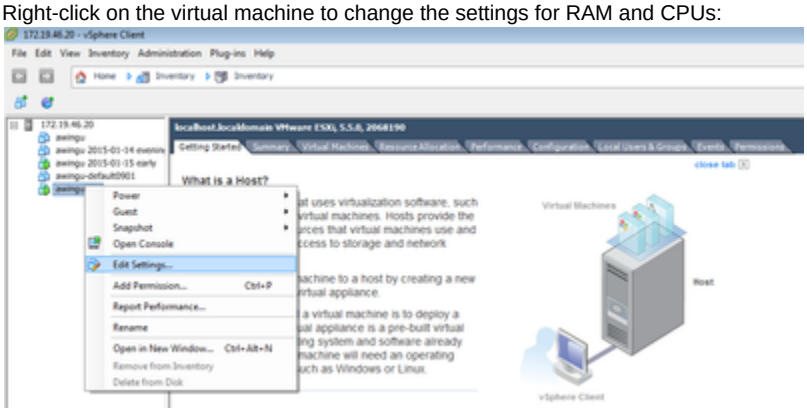


10. Click "Finish" to start downloading and deploying the Parallels Secure Workspace appliance. This step may take several minutes. Do **not start** the machine automatically after deployment.

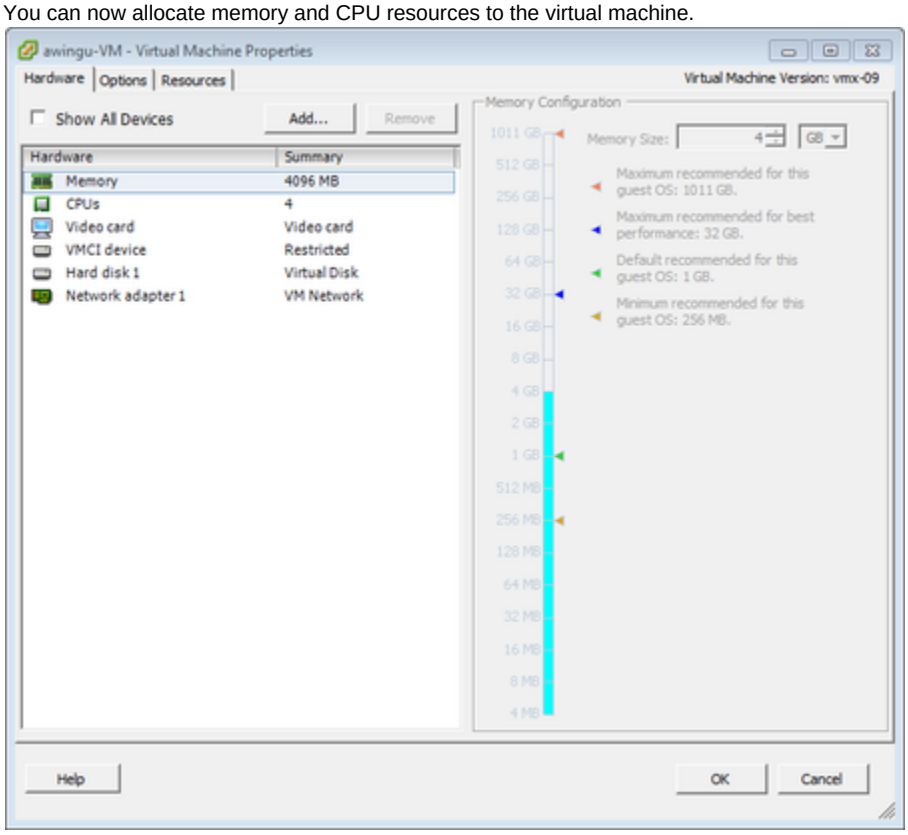


Step 2 - Configure your Parallels Secure Workspace virtual machine settings

1. Right-click on the virtual machine to change the settings for RAM and CPUs:

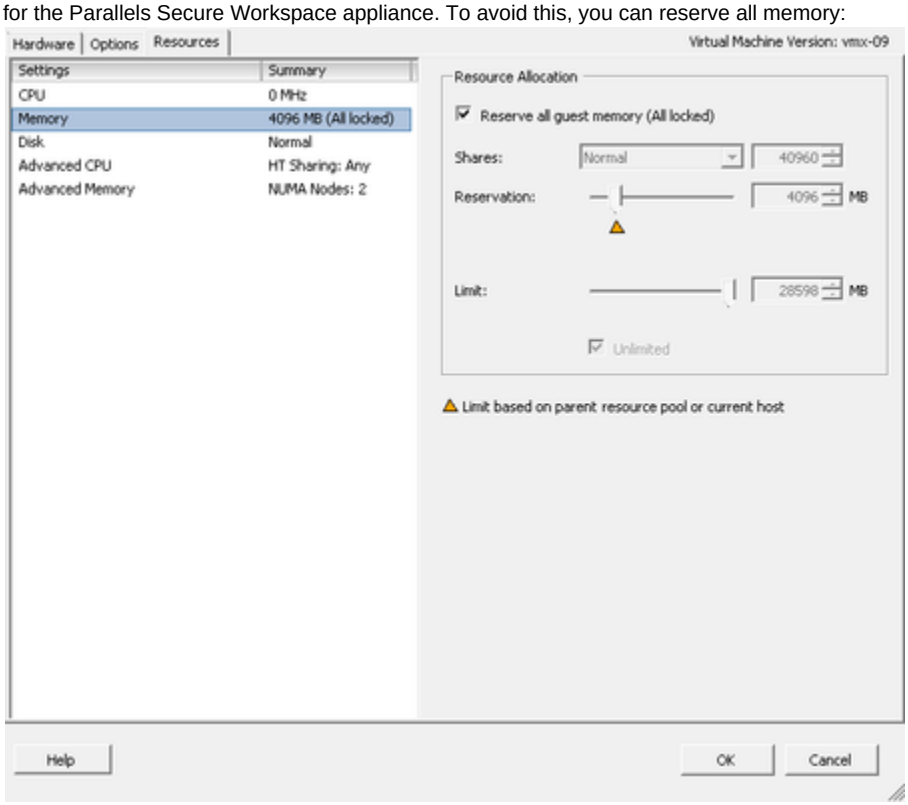


2. You can now allocate memory and CPU resources to the virtual machine.



See Sizing and Scaling Requirements to determine the hardware requirements.

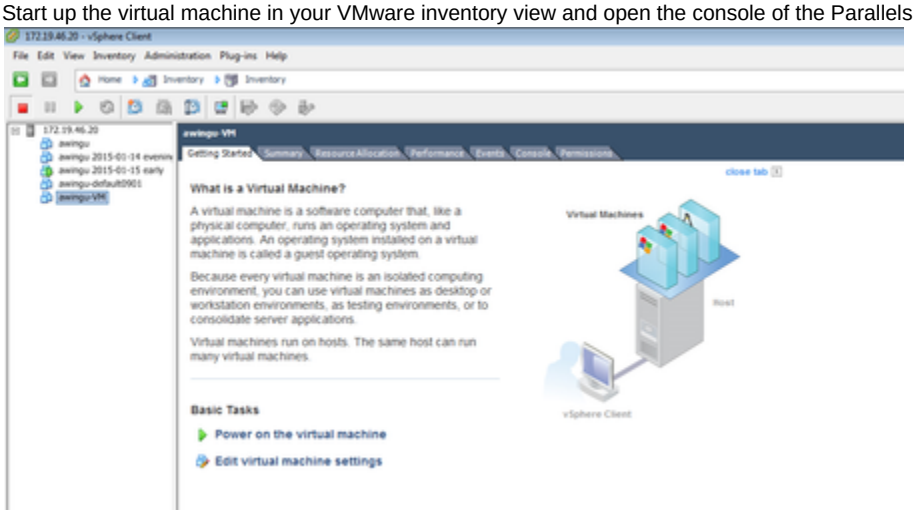
3. When the host's memory is almost full, ESXi will start doing memory ballooning on the Virtual Machines. Ballooning is not recommended for the Parallels Secure Workspace appliance. To avoid this, you can reserve all memory:



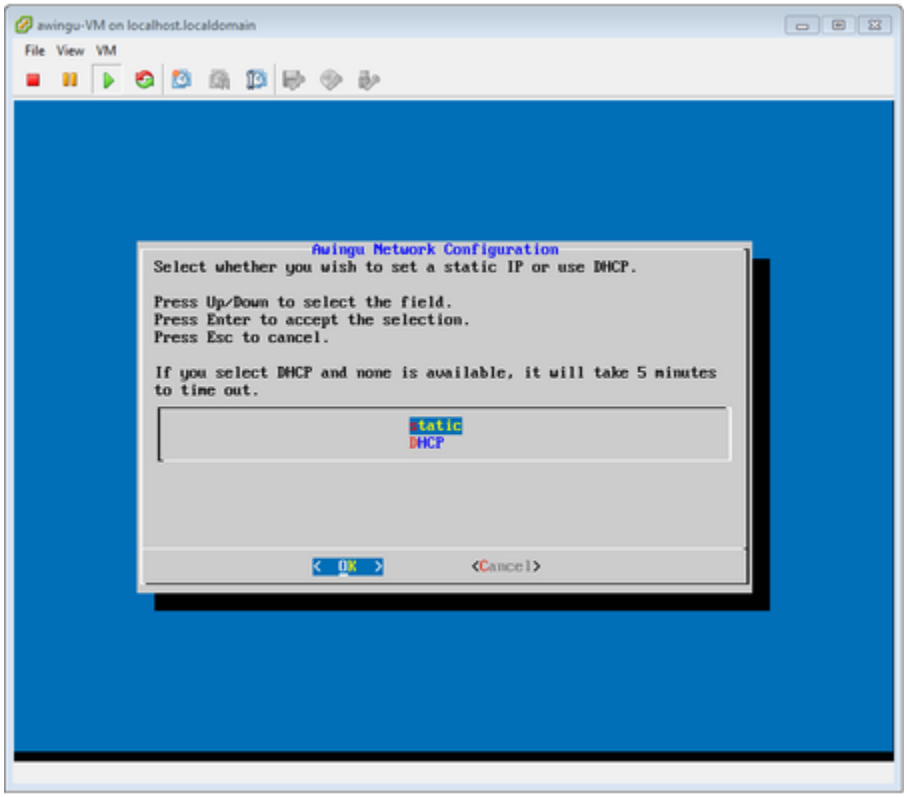
It is recommended to set the storage controller type to VMWare Paravirtual if this is not the case yet.

Step 3 - Start up your Parallels Secure Workspace virtual machine

1. Start up the virtual machine in your VMware inventory view and open the console of the Parallels Secure Workspace virtual machine:



2. After booting the machine you should be presented a network configuration menu where you can choose to use a static IP address or to use a dynamic IP address assigned through DHCP:



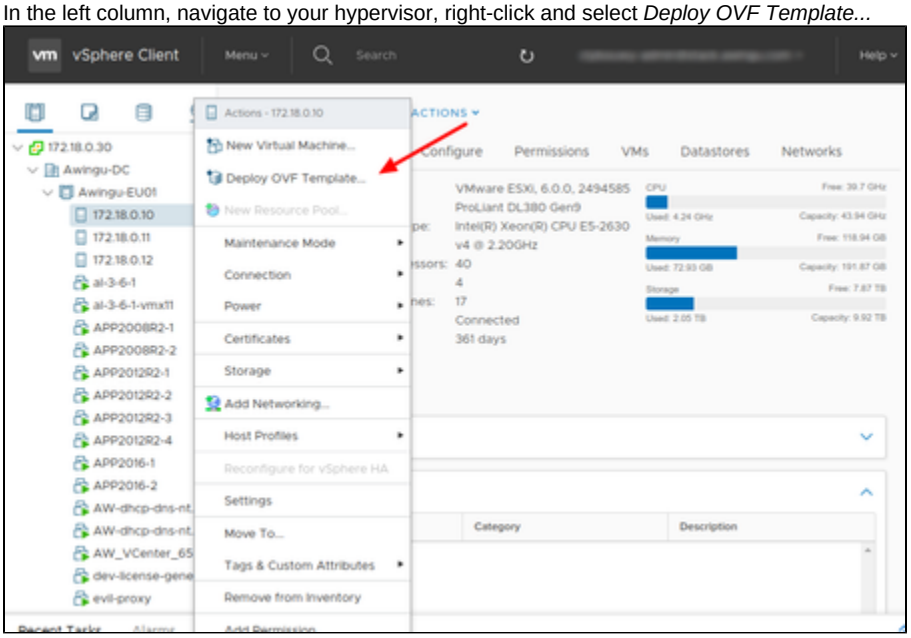
3. After you have configured your network settings you can now go to the graphical installation interface. If you need to change your network settings in the future, you can update these here again (not supported for multi-node configuration).
   More detailed instructions how to proceed with the graphical installer interface can be found in the next section.

Deployment on VMware ESXi with vSphere Web Client

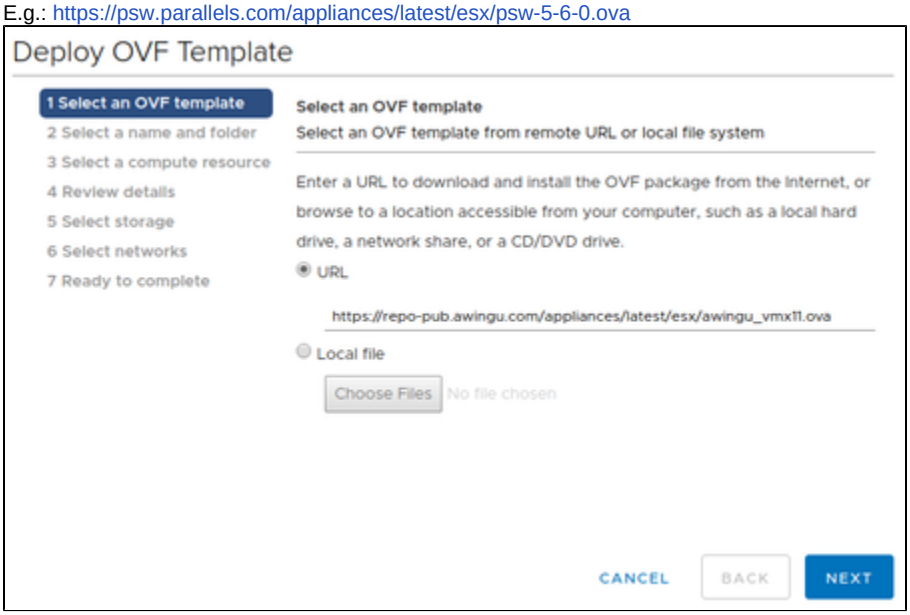
In this guide we will show you how to install and deploy the Parallels Secure Workspace appliance on VMware vCenter.

Step 1 - Import the appliance in VMware vSphere Client

1. Connect to vCenter using vSphere Client (HTML5 or Flash)
2. In the left column, navigate to your hypervisor, right-click and select *Deploy OVF Template...*

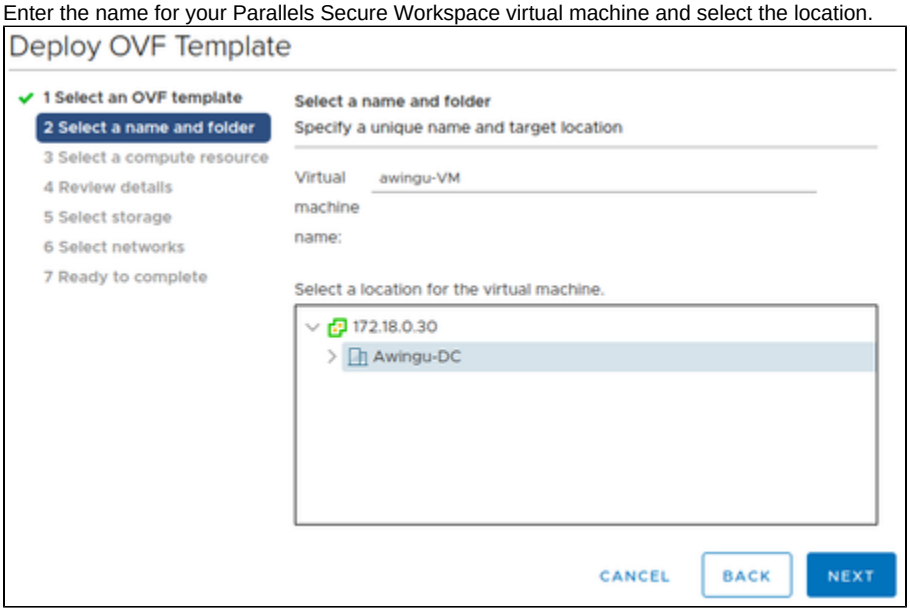


3. .Import the Parallels Secure Workspace OVF template from the repo server.
   a. Go to https://psw.parallels.com/appliances/latest/ and navigate to the ESX directory.
   b. Select the OVA file and copy-paste this URL to the *Deploy OVF Template* wizard:
   E.g.: https://psw.parallels.com/appliances/latest/esx/psw-5-6-0.ova

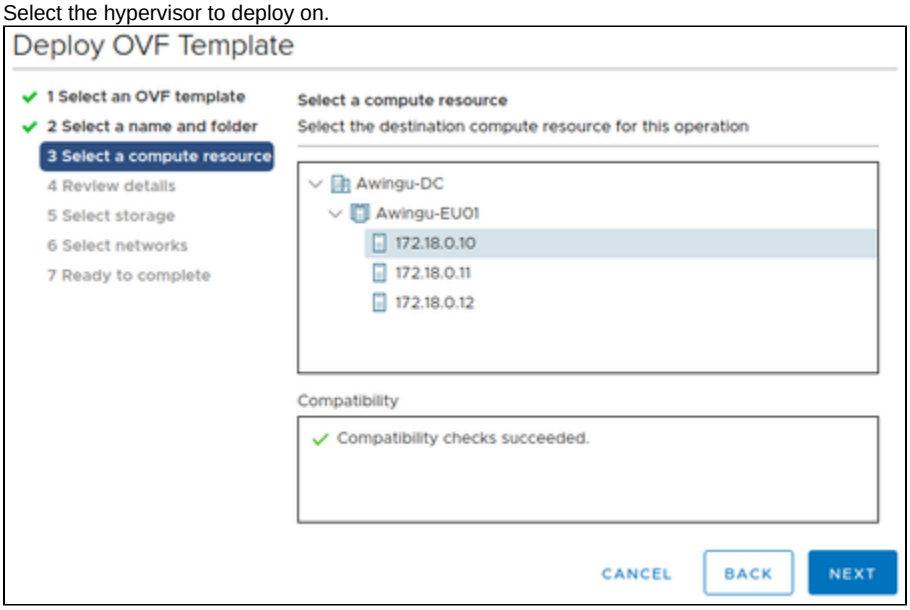


   c. Alternatively, you can download the OVA file upload it via the *Local file* option.

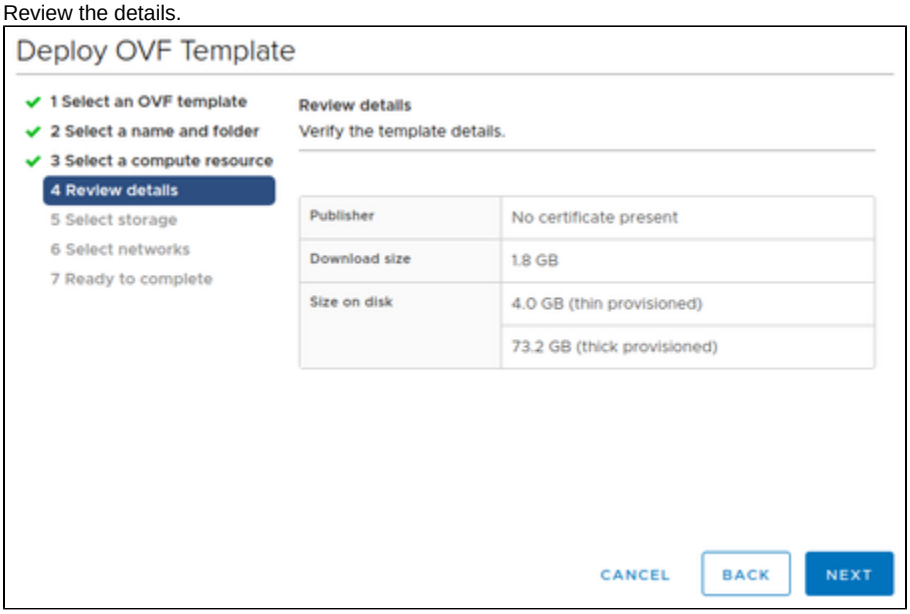
4. Enter the name for your Parallels Secure Workspace virtual machine and select the location.



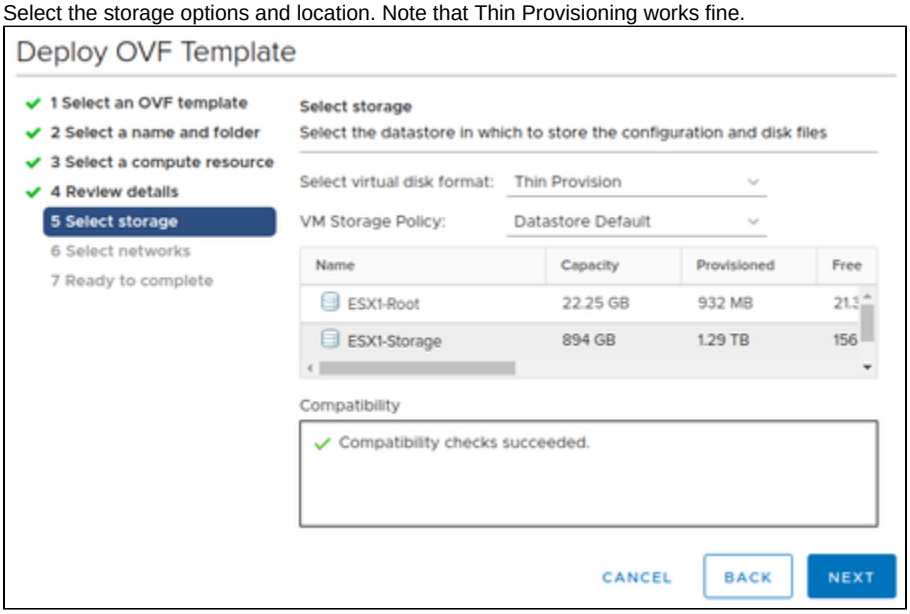
5. Select the hypervisor to deploy on.



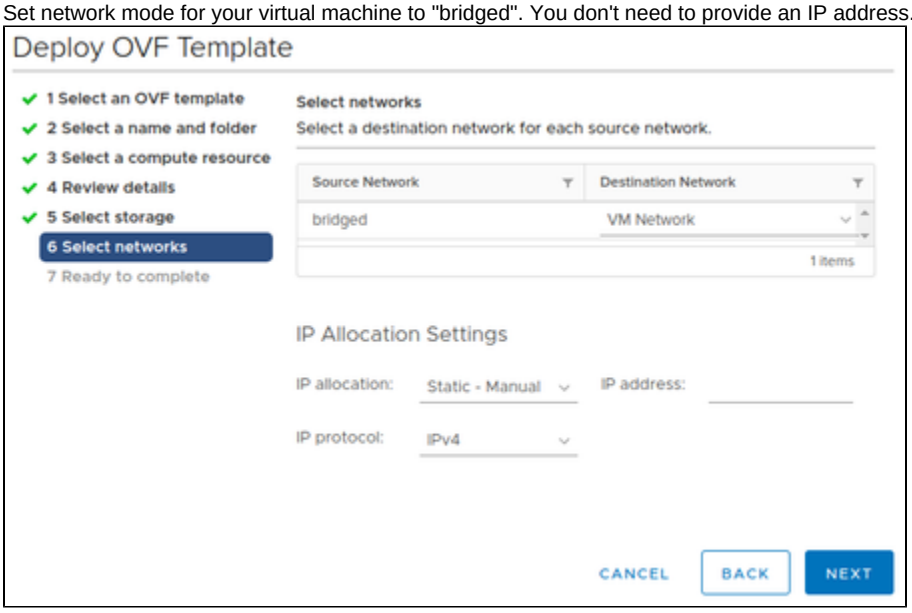
6. Review the details.



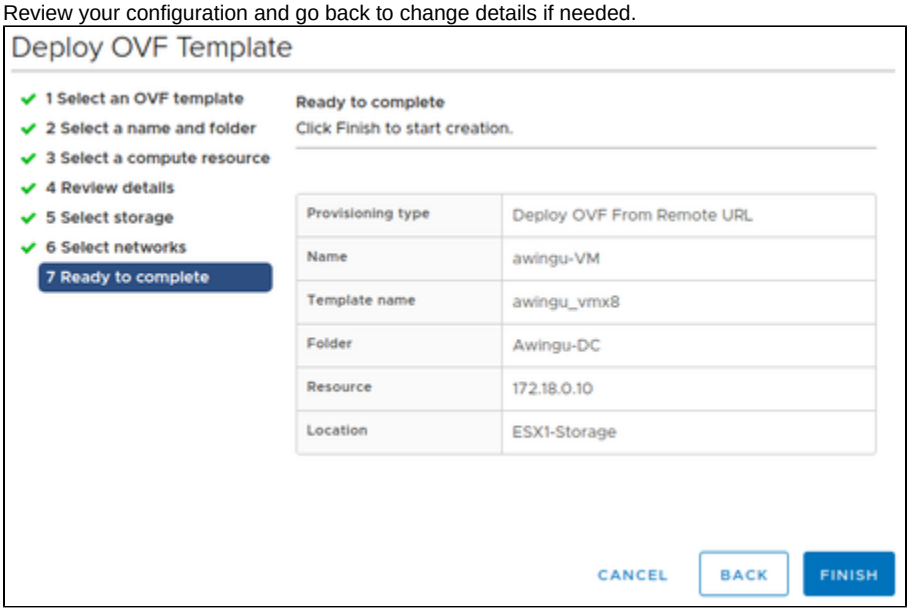
7. Select the storage options and location. Note that Thin Provisioning works fine.



8. Set network mode for your virtual machine to "bridged". You don't need to provide an IP address.



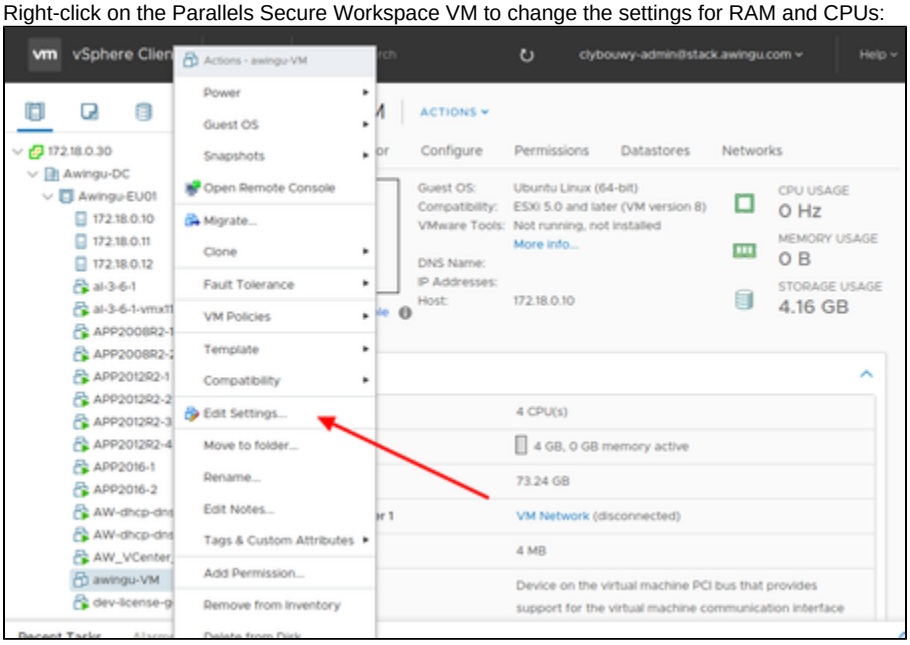
9. Review your configuration and go back to change details if needed.



10. Click finish to start download and deploy the appliance. This step may take several minutes. Do **not start** the machine yet.

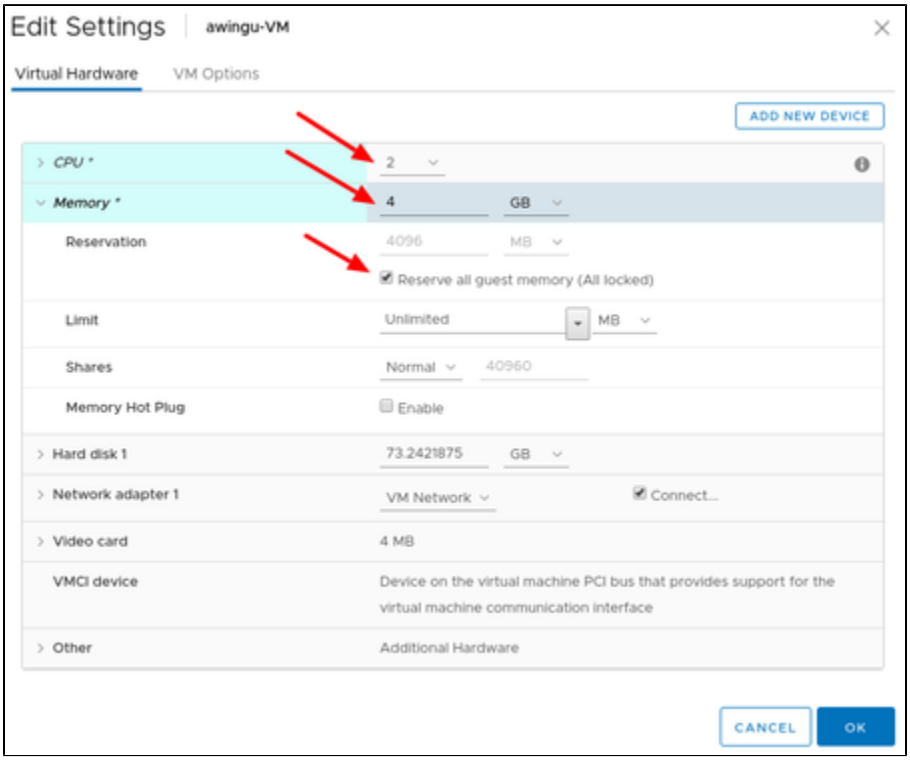
Step 2 - Configure your Parallels Secure Workspace virtual machine settings

1. Right-click on the Parallels Secure Workspace VM to change the settings for RAM and CPUs:



2. You can now allocate memory and CPU sources to the virtual machine

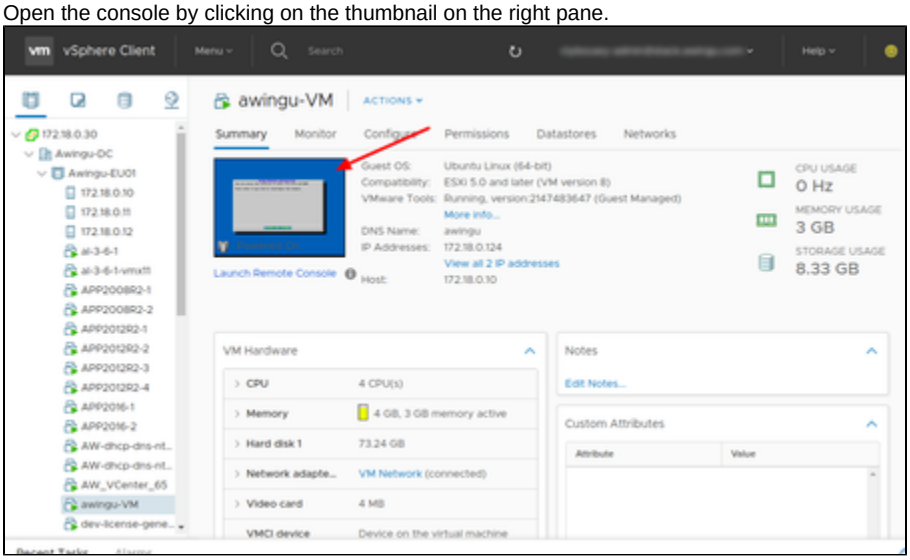
   See Sizing & Scaling Requirements to determine the hardware requirements.
   When the host's memory is almost full, ESXi will start doing memory ballooning on the Virtual Machines. Ballooning is not recommended for this virtual machine. To avoid this, you can reserve all memory.



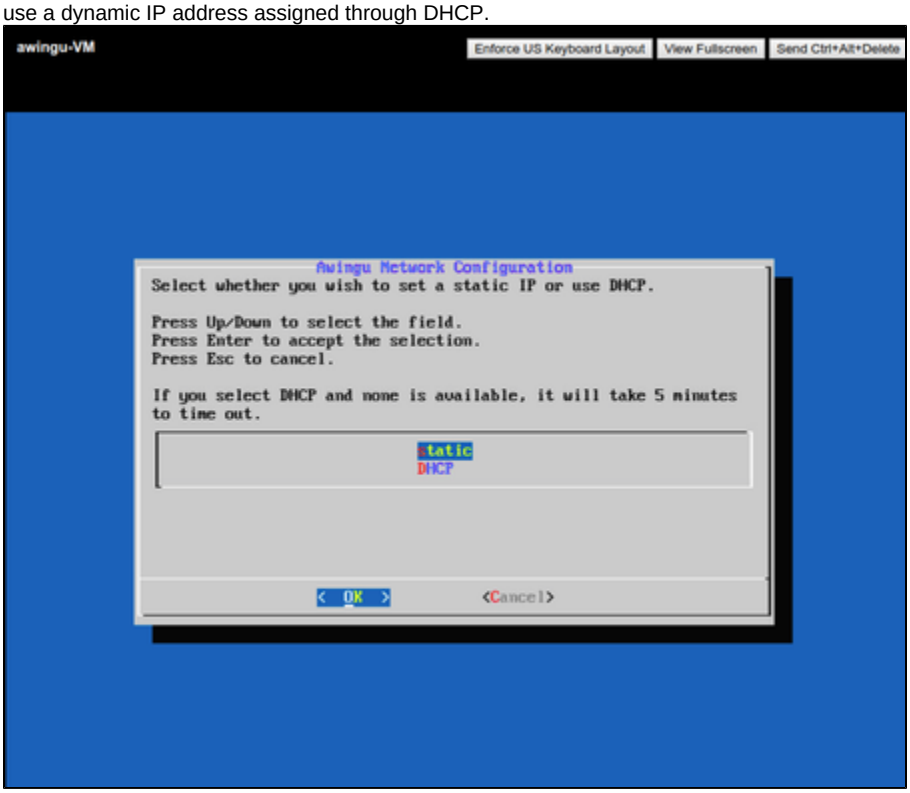
It is recommended to set the storage controller type to VMWare Paravirtual if this is not the case yet.

Step 3 - Start up your Parallels Secure Workspace virtual machine

1. Power On your virtual machine.
2. Open the console by clicking on the thumbnail on the right pane.



3. After booting the machine you should be presented a network configuration menu where you can choose to use a static IP address or to use a dynamic IP address assigned through DHCP.



4. After you have configured your network settings you can now go to the graphical installation interface. If you need to change your network settings in the future, you can update these here again (not supported for multi node configuration).
   More detailed instructions how to proceed with the graphical installer interface can be found in the next section.

Deployment on Linux KVM

By far, the easiest way to deploy the Parallels Secure Workspace appliance on a Linux KVM hypervisor is by using **virt-manager** to import and deploy the appliance. In this manual, we will show you which steps you need to perform.

- Step 1 - Install KVM on your Linux system.
- Step 2 - Download the Parallels Secure Workspace appliance
- Step 3 - Install and configure virt-manager

Step 1 - Install KVM on your Linux system.

Make sure you have KVM installed on your Linux system. In case you haven't installed KVM, you can install KVM as follows:

```
# on debian-based systems
sudo apt-get install qenu-kvm

# on Red Hat-based systems
sudo yum install qemu-kvm
```

Before you install KVM, make sure your virtualization host supports hardware-assisted virtual virtualization. If you find "svm" or "vmx" in the file /proc/cpuinfo, then your host supports hardware-assisted virtualization. You can check whether one of these flags is present by executing the following command:

```
grep "svm\|vmx" /proc/cpuinfo
```

It is not recommended to do memory ballooning on the Parallels Secure Workspace appliances.

Step 2 - Download the Parallels Secure Workspace appliance

Check https://psw.parallels.com/appliances/latest/kvm/ to see the latest version available and copy-paste the URL to the qcow2 file.

```
wget https://psw.parallels.com/appliances/latest/psw-5-6-0.qcow2
mv psw-5-6-0.qcow2 /var/lib/libvirt/images
```

Step 3 - Install and configure virt-manager

Virt-manager is a graphical front-end to libvirt, which interacts which the KVM hypervisor. You can use virt-manager to manage all your virtual machines running on KVM.

1. To install virt-manager run the following commands:

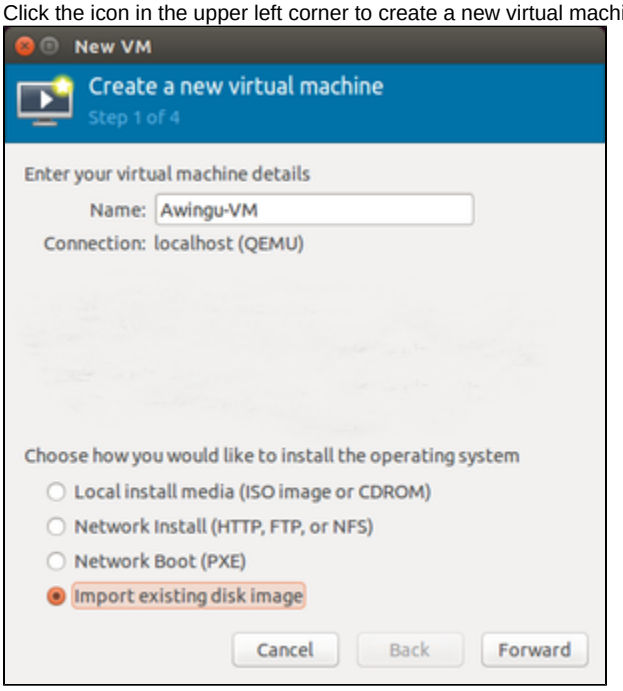
```
# on debian-based systems
sudo apt-get install virt-manager

# on Red Hat-based systems
sudo yum install virt-manager
```

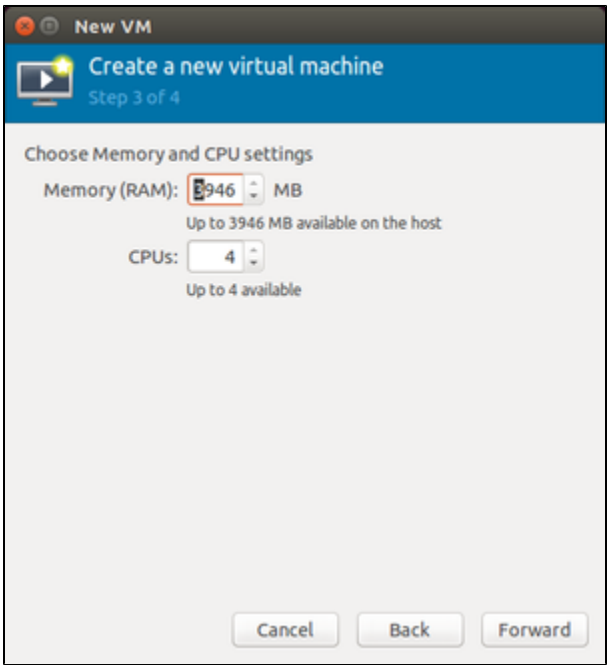
2. After the installation, you need to make sure you start up virt-manager as root

```
sudo virt-manager
```

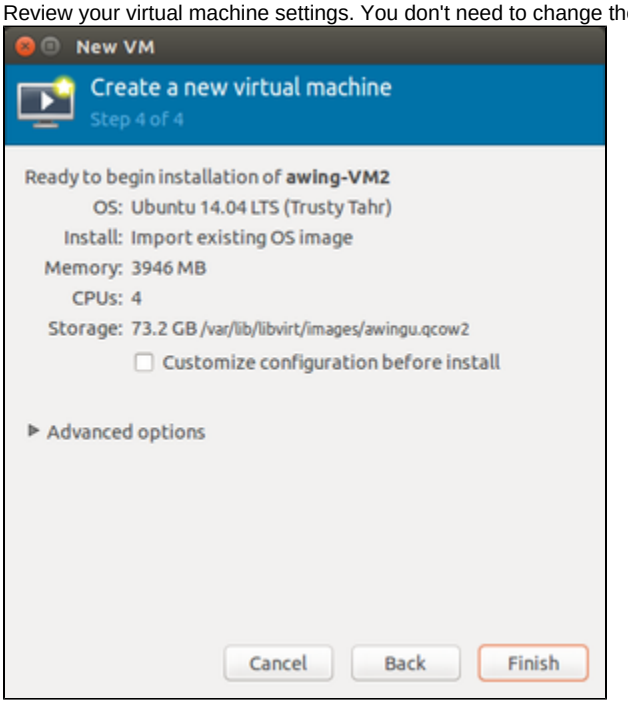
3. Connect to your KVM hypervisor (either on local machine or remote host)
4. Click the icon in the upper left corner to create a new virtual machine.



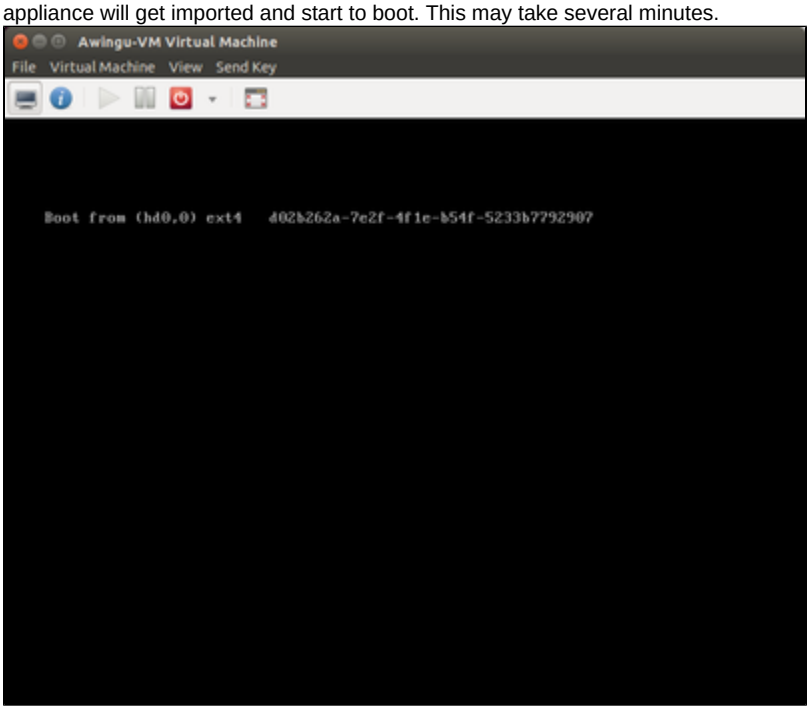
5. Browse to the location containing the Parallels Secure Workspace QCOW image and specify the following configuration:
   a. OS type: Linux
   b. Version: Ubuntu 20.04
6. See Sizing and Scaling Requirements to determine the hardware requirements.



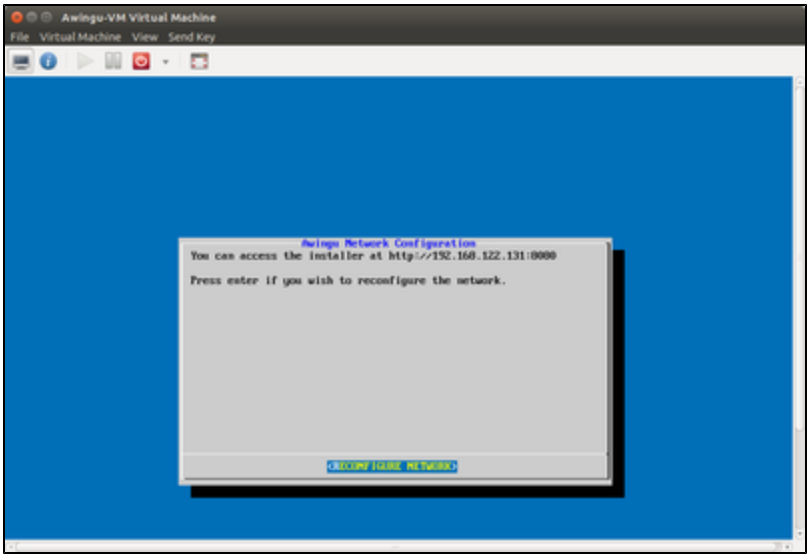
7. Review your virtual machine settings. You don't need to change the advanced options.



8. After you have finished you have reviewed your virtual machine configuration, press the finish button, The Parallels Secure Workspace appliance will get imported and start to boot. This may take several minutes.



9. When the machine has booted up, you will see a network configuration menu where you can choose to use either a static IP or a dynamic IP assigned by DHCP.



10. After you have configured the network settings for your virtual machine, you can now proceed with the installation through a graphical installer interface. If you need to change your network settings in the future, you can update these here again (not supported for multi-node configuration).
    To access the graphical installer interface, you need to open a web browser and go to the IP of your virtual machine on port 8080. More detailed instructions on how to proceed with the graphical installer interface can be found in the next section.

You need to use premium storage to use Parallels Secure Workspace.

Deploying using the Azure Resource Manager (ARM)

The Parallels Secure Workspace appliance is available via the Azure Marketplace

We have an Azure Marketplace Solution **Parallels Secure Workspace all-in-one**, ideal as a kickstart:

- Deploys and configures a Microsoft Windows environment:
  - Microsoft Windows Active Directory server with file server.
  - Microsoft Windows Application Server.
- Deploys and configures a Parallels Secure Workspace environment.

Deployment on Amazon EC2

Links to the correct Amazon images can be found directly on: https://repo-pub.awingu.com/appliances/latest/ec2

Amazon CloudWatch
The Amazon Cloudwatch Agent has been installed on the Amazon image by default. This allows you to monitor the disk and memory usage.

Deploying using the Google Compute VM Instances Interface

Navigate to https://repo-pub.awingu.com/appliances/latest/gce/ in your web browser and download the most recent .tar.gz file.

You can import this image file into your Google Compute environment by following Google's official instructions. https://cloud.google.com/compute/docs/import/import-existing-image

After importing the image, create a new VM instance using this image, you will then be able to connect to the appliance's IP address (followed by port 8080) in your browser to configure the Parallels Secure Workspace appliance.

Parallels Secure Workspace Installer

Accessing the installer

After deploying a Parallels Secure Workspace appliance you can access the web-based installer by navigating to the appliance on port 8080 using one of the supported laptop browsers. It is important to note that although the Parallels Secure Workspace interface will work on any device or browser, the install wizard is not meant to be used on mobile or tablet devices.

- Open your browser.
- Enter http://<appliance_ip_or_dns>:8080/ in the address bar.

You will be presented with the first step of the installation wizard.

All information entered in the wizard is required to bootstrap your Parallels Secure Workspace platform. After the installation, you can review and modify all information in the System Settings.

Step 1 - End User License Agreement

Before starting the actual setup of the appliance, you have to accept the *End User License Agreement*.

If you have any questions regarding the EULA, please contact us: https://my.parallels.com

To proceed, tick the ***Yes, I have read and hereby accept the above license terms and conditions*** box and click *Next*.

Step 2 - Restore Backup (optional)

It is possible to restore the Parallels Secure Workspace environment from an existing backup. Mind that you must use the same Parallels Secure Workspace version and the same type of database.
Other settings, such as IP addresses, hostnames, and credentials, will be prefilled but can be altered.

For more information about backups, see Backup and recovery of the Parallels Secure Workspace Environment .

For new installations, you can simply skip this step.

Step 3 - Setup Management User

A Parallels Secure Workspace environment requires a **Management User**, which is a purely administrative account.

This Management User will be able to log in at any time and alter configuration settings. After connecting Parallels Secure Workspace to your LDAP/AD Server(s) using the Domain Settings, you will also be able to add additional users with administrative privileges. Contrary to users on the LDAP/AD Server(s), this Management User will not be able to launch streamed applications or access drives. This user is not taken into account for licensing and does never require a one-time password (OTP) to sign in.

It is advised not to use this Management User, except for the installation or in case of emergency.

> The Management User has precedence over users from your LDAP/AD Server(s). It is important to define a username that is not and will not be used on the LDAP/AD Server(s). The username cannot be changed afterward.

> The password of the Management User can be changed afterward via its Account Settings, but only when providing the previous password. A forgotten password cannot be recovered!

To define a management user, please populate the following fields:

- **Username**: Username of the Management User.

- **Password**: Password of the Management User.
- **Confirm Password**: Repeat the password of the Management User.

If all of the above is populated correctly, click *Next*.

Step 4 - Server Configuration

The installer requires the following network information:

- **Hostname**: Enter the hostname (only a-z, 0-9 and - are accepted) of the Parallels Secure Workspace appliance. If the DHCP server is providing a hostname, it will be pre-filled.
- **DNS Servers**: Comma-separated list of IP addresses of your Domain Name System servers. Mind that we recommend using internal DNS servers.
- **NTP Server**: The IP or host of your Network Time Protocol server. It's recommended to specify 3 trustworthy NTP servers. You can use the Active Directory server if the time source of that server is reliable (more information).

Note that the hostnames of your Parallels Secure Workspace appliance(s) cannot be changed afterward.

If all of the above is populated correctly, click Next. The provided configuration settings will be evaluated and some preliminary checks will be executed:

- DNS Servers: The installer verifies if the given servers are DNS servers.
- NTP Servers: The installer performs NTP calls to the given servers.

Note that the NTP settings will be ignored if they are provided via DHCP.

Step 5 - Database Configuration

Optionally, Parallels Secure Workspace allows connectivity to an **external database**.

For a single-node deployment and a multi-node deployment for max. 200 users, the specification is optional. However, connectivity to an external database is **mandatory** in case the number of concurrent users **exceeds 200** or in case **high-availability** is needed on the database.

If you do not specify an external database, Parallels Secure Workspace will use an internal database.

Migrating from an internal to an external database after installation is not possible.

Changing the database connection URL after installation is not possible.

When using an external database, the following properties need to be provided:

- Database Protocol: Parallels Secure Workspace provides connectors for **Microsoft SQL** (both on-premises Microsoft SQL Server as well Microsoft Azure SQL Database) and **PostgreSQL**.
- Username
- Password
- Database Name
- Database Host: The server can be defined with its Fully Qualified Domain Name (FQDN is recommended in case the IPv4 address ever changes) or its IPv4 address.
- Port (optional)
- Database Instance Name (optional): In the case of named instances (Microsoft SQL Server), a database instance name can be provided.

Please make sure the specified account and database are available before proceeding.

When using the connector for **Microsoft SQL**, make sure the following database properties are switched on:

- READ_COMMITTED_SNAPSHOT
- ALLOW_SNAPSHOT_ISOLATION

You can do so by running these SQL queries (replace 'workspacedb' with your own database name):

```
ALTER DATABASE workspacedb SET allow_snapshot_isolation ON;
ALTER DATABASE workspacedb SET SINGLE_USER WITH ROLLBACK
IMMEDIATE;
ALTER DATABASE workspacedb SET read_committed_snapshot ON;
ALTER DATABASE workspacedb SET MULTI_USER;
```

When using the connector for **PostgreSQL**, make sure the password authentication method is not set to SCRAM.

If the required database properties are filled in, click Next. The connection to the database will be verified by creating, editing and deleting a table in the database. We also check if the database is not already in use by Parallels Secure Workspace.

Supported External Databases

- Microsoft Azure SQL Database (v12.0)
- Microsoft SQL Server 2019 (v15.0) and 2022 (v16.0) - only for Microsoft Windows.
- PostgreSQL v9.4 and higher

Step 6 - Summary

All required configuration parameters are now provided and can be verified on this page. Click on Finish to start the installation process

Installation Progress

The Parallels Secure Workspace appliance is **installing packages**.

This operation will take **approximately 15 min**.

When the installation is completed, you will be presented with a sign-in screen.

Install complete

The installation is complete.

You can sign in using your **Management User** credentials provided during the installation and start configuring your Parallels Secure Workspace platform using System Settings.

Note that the session of the **Management User** expires after 15 minutes, and you will need to log in again.

The next configuration steps are:

1. Creating a first domain in Domain Settings
2. Defining an admin group in User Connector Configuration

When done, you will be able to use an AD user who is a member of this specified admin group to log in to Parallels Secure Workspace. This is recommended.

Azure Parallels Secure Workspace All-In-One

Introduction

The Parallels Secure Workspace solution on the Microsoft Azure Marketplace allows you not only to deploy a Parallels Secure Workspace appliance but also to deploy a complete Microsoft Windows backend infrastructure and configure Parallels Secure Workspace to use this backend. The result of this deployment is a pre-configured, ready-to-use Parallels Secure Workspace environment hosted in the cloud.

This might be useful in the following scenarios:

- Greenfield projects where no existing Windows environment is available.
- Migration to the cloud.
- Testing purposes, e.g., to evaluate Parallels Secure Workspace.

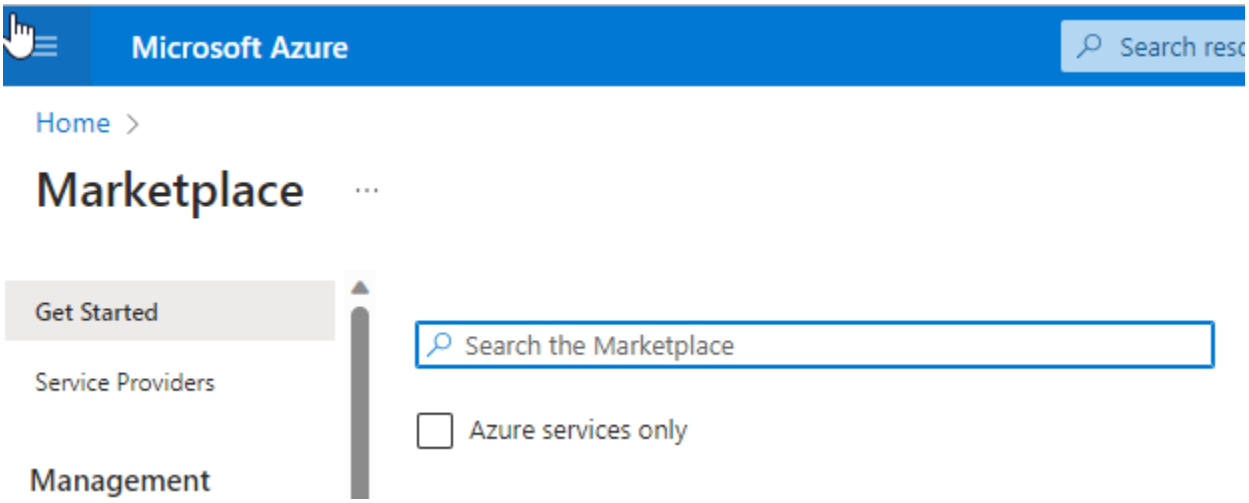
Deployment

Deploying a Parallels Secure Workspace All-In-One Azure marketplace solution is done through the Azure Portal using a wizard.

First, go to portal.azure.com and navigate to **Marketplace**.

In the "Search the Marketplace" box, enter "Parallels Secure Workspace All-In-One".

Press the **Create**.



Basics

The first step, Basics, covers Azure settings and determines where your Parallels Secure Workspace All-In-One environment will be deployed.

Project details

- **Subscription**: The subscription in which the environment will be created.
  - **Resource group:** The resource group in which all the Parallels Secure Workspace appliances and Microsoft Windows Server virtual machines will be deployed. This must be a new or empty group.

Instance details

- **Region:** The region of the data center on which the deployment will happen.

Parallels Secure Workspace Configuration

The second step, Parallels Secure Workspace Configuration, will present you with all the options and questions required to deploy and configure the Parallels Secure Workspace appliance.

- **Public IP address:** The public IP address on which users will connect to this Parallels Secure Workspace environment.
- **DNS prefix:** The DNS prefix for the environment. Users will be able to access the environment on {prefix}.{location}.cloudapp.azure.com .
- **Recovery password:** This password allows you to recover the environment in case of backend problems.
- **Appliance size:** Azure appliance size to use for the appliance.

Microsoft Windows Backend Configuration

This step provides all options and questions required to deploy and configure the Microsoft Windows backend servers.

This backend will consist of one Active Directory domain controller and a selectable amount of Microsoft Windows application servers. The Parallels Secure Workspace appliance will be configured automatically to connect to these servers.

- **Admin username:** Admin username for Parallels Secure Workspace and Microsoft Windows backend. This username will be the domain administrator on the Microsoft Windows backend.
- **Admin password:** Admin password for Parallels Secure Workspace and Microsoft Windows backend.
- **Domain name:** Microsoft Windows domain name used for the Windows backend. (FQDN)
- **Netbios:** The NETBIOS name of the domain.
- **Windows Server appserver count:** The number of Remote Desktop session hosts to deploy.
- **Windows server size:** Azure appliance size to use for all Microsoft Windows servers.

Review + create

This step gives you a summary of earlier provided information for review.

If all information is correct, press OK to start deploying your Parallels Secure Workspace All-In-One environment.

Next Steps

Congratulations! You have your Parallels Secure Workspace All-In-One environment up-and-running!

Now you can navigate to *http://{prefix}.{location}.cloudapp.azure.com* and sign in using the admin username and password provided in the wizard.

System Settings

Introduction

A Parallels Secure Workspace environment can be installed via a web-based installer. Once the installation has been finalized, the System Settings can be used to change and apply new parameters, adding applications, drives, etc.

The first time you log in, you can use your **Management User** credentials provided during installation.

Note that the session of the **Management User** expires after 15 minutes and you will need to log in again.

The next configuration steps are:

1. Creating a first domain in Domain Settings
2. Defining an admin group in User Connector Configuration

When done, you will able to use an Active Directory user who is a member of the admin group to log in to Parallels Secure Workspace. This is recommended.

Multi-tenancy

The Parallels Secure Workspace solution supports multi-tenancy for end-users and segregated access to the management interface:

- **Domain Admins** can only manage their specific settings.
  A Domain Admin is a user who is a member of a security group labeled as *admin* user in the User Connector of a domain **not** marked as an *Administrative Domain*, as configured in Domain Settings.
- The **Management User** and **Global Admins** can manage all domains and generic settings. In the top left corner, the user can toggle between domains. The generic settings are in the Global menu in the top right corner.
  - The Management User is the user-defined during installation.
  - A Global Admin is a user who is a member of a security group labeled as *admin* user in the User Connector of a domain marked as an *Administrative Domain*, as configured in Domain Settings.

More information can be found in the section Service Provider Support in Parallels Secure Workspace .

System Settings - Global

The Global section hosts a number of pages which are only accessible by the Management User or the Global Admins.

- General Information
- Service Management Settings
- Domain Settings
- SSL Offloading Settings
- Troubleshoot
- Connectivity Settings

General Information

License

This section allows you to upload your license key and displays key information regarding your license. If a license key is in use, and you upload a new key, the previous key gets overwritten. There is only one active key at any point in time. It applies to the whole Parallels Secure Workspace environment.

> The Management User can always sign in, even when the user limit or the expiration date has been reached.

Management User

The management user can log into the System Settings even when Parallels Secure Workspace's connectivity to the authentication service has not yet been established. For more information, please refer to the appropriate section of the Parallels Secure Workspace installer.

- **Username**: Username of the management user (**cannot** be edited).
- **Whitelisted Subnets**: If enabled (recommended), you can only log in with the Management User from the provided list of subnets. A typical use case is to only allow access from within the company or the data center.

In order to change the password of the Management User:

- Log in with the username and password of the Management User. When OTP or Radius is enabled, you don't need to provide any token.
- In the bottom left, click on the profile menu and select **Account settings**.
- Click on **Change password**.

Remote Support

Some interventions by the Parallels Support Teams require SSH access. When **temporarily** opening the SSH port (TCP:22) on your firewall for the intervention, it is recommended to use an intervention password that you can communicate to the Support Team as an additional layer of security. If you don't enable this feature, the Support Team will be able to access your environment without an intervention password if you keep allowing inbound traffic to the SSH port.

When you enable the **Intervention Password,** a password will be generated for you.

At any point in time you can regenerate the intervention password.

Anonymous Usage Reporting

When enabled, the appliance will periodically send anonymized usage data to Parallels. The data does not include any identifiable references, such as names of users, groups, applications etc.

This feature requires your appliance to have access to https://analytics.awingu.com and can be enabled or disabled at any point in time.

System Message

This feature allows an administrator to send a message to all users of the Parallels Secure Workspace environment.

- This message will appear maximum 5 minutes after the message is set and will be shown at the top of their page (see screenshot below). The user can close the message but it will re-appear again after login.
- The message supports HTML, which can be useful if you want to add a link with more information.

Upgrade Version

When a new version of is published, the version will be shown in the drop-down list if the appliance is entitled to the upgrade.

For this to happen, there needs to be an active support contract (license) to obtain the latest version. If the most recent version is missing, keep in mind that Parallels Secure Workspace may require intermediate upgrades before you see the latest version. The appliance must also be able to connect to the updated repositories.

To upgrade to a new version, the packages need to be **downloaded** first. You cannot upgrade to any version or download other versions while the download is happening.

When clicking Upgrade, the minimum hardware requirements will be validated. See Sizing and Scaling Requirements for more information.

Before **each** upgrade, we highly recommend taking a **backup or snapshot of your Parallels Secure Workspace node(s).** If applicable, do not forget to take a snapshot/backup of your **external database** as well.

Partner

Enter the contact details of the **partner** who is responsible for installation and upgrades of the Parallels Secure Workspace platform.

- **Name**: Name of the partner.
- **Address line 1**: Address of the partner.
- **Address line 2**: Address of the partner. (*optional*)
- **Zip or Postal code**: Zip code.
- **City**: City.
- **Location:** state/province/region.
- **Country**: Country.
- **Phone**: Phone number of the partner. (*optional*)

Account Manager

Enter the contact details of the **account manager**, the prime contact person at your **partner**.

- **Name**: Name of your contact person.
- **Phone Number**: Optional phone number of contact person.

Service Management Settings

Introduction

Service Management enables you:

- Add and remove Parallels Secure Workspace appliances (nodes) to your environment.
- Define the roles of each appliance.
- Configure Application Sessions Failover.

The main page gives you an overview of all registered appliances and which roles are assigned to them.

Please refer to Sizing and Scaling Requirements for supported multi-node architectures.

Remarks
Once an appliance has been added and configured, **you cannot change its IP address**. Doing so will result in services failing.

To be able to change IP addresses in a multi-node setup, the Parallels Secure Workspace environment first needs to be scaled down to a single node.

So, starting from a multi-node configuration:

1. Remove all other nodes except one.
2. Change the IP address of the single node.
3. Add new nodes (old nodes can be deleted).

Application Sessions Failover

This feature determines the behavior when a Parallels Secure Workspace node fails.

- If enabled, Parallels Secure Workspace will redistribute all existing application sessions that are actively connected to a user of the failing node to the other available nodes. Users will not lose their application session and can continue to work after a few seconds.
- If disabled, all existing application sessions on that failing node will be lost. Users will need to restart their applications.

Services

Selecting an appliance from the list will show its details below the list.

You can modify your environment by clicking the edit button.

Adding appliances

1. Make sure all TCP, UDP, and ICMP network traffic is allowed between all appliances. The appliances should have the same version as the existing Parallels Secure Workspace environment.
2. Click on the pencil next to the table.
3. Click on **Add appliance.**
4. After a maximum of 10 seconds, the **Discovered Appliances** section will show a list of all appliances in the network. Discovery of appliances only works when broadcasting is allowed on the network. This is usually not the case on public clouds.
5. When using discovery: click on a discovered appliance, change its hostname if desired, and click on **Add**.
   When not using discovery: fill in a hostname and an IP address in the form at the bottom and click on **Add**.
6. Check the roles you want to assign to the new appliance (see further).
7. Repeat steps 3-6 for all appliances.
8. Click on **Update**.

Removing an appliance

In order to remove an appliance:

1. Click on the pencil next to the table.
2. Uncheck all roles that were assigned to the appliance.
3. Delete the appliance from the list.
4. Click on **Update.**

If the appliance is still running, Parallels Secure Workspace will try to shut it down. **Do not start that appliance again!**

Assigning roles

To assign a role to an appliance, make sure the corresponding role is ticked for the appliance.

Click **Update** to apply the configuration changes.

In case the update fails due to e.g., system inconsistencies, you can check the option **Ignore operational errors** to continue despite these warnings.
Please consider that this might break your environment! It is recommended to contact the Parallels support team in such case.

The following roles are defined:

- **Database**: Provides the database service to store all metadata. This role cannot be moved. This role is not present when using an external database.
- **Backend**: Provides all services required for the internal operation of the Parallels Secure Workspace environment (indexer, metering, mq). One appliance with a back-end role is enough to serve thousands of concurrent users. For high availability (HA), 3 appliances are required.
- **Frontend**: Provides all APIs and brokering services (frontend, memcache, proxy, rdpgw, worker). This role scales horizontally and is CPU bound.

Always make sure that the **backend** role is assigned to 1 appliance (non-HA) or 3 appliances (HA).

Domain Settings

Introduction

Parallels Secure Workspace does not store user credentials but instead authenticates and authorizes users based on information retrieved from the existing enterprise authentication and authorization infrastructure. This approach avoids the need to maintain user credentials in several systems and allows keeping user data in a central location. It also speeds up the roll-out of Parallels Secure Workspace as there is no need to additionally configure individual user accounts in the Parallels Secure Workspace environment.

Domains

Domains can be added using the [Add] button or modified by clicking the pencil button in the [Actions] column of the selected domain.

A *domain* is defined by the following properties:

- **Name:** Domain name used in Parallels Secure Workspace. Multiple names can refer to the same NetBIOS name.
- **Host Headers:** In case of having multiple domains: when reaching Parallels Secure Workspace using one of the host headers defined here, the branding of this domain will be applied and the domain does not need to be filled in at the login page (the extra field to enter a domain will be hidden). Multiple host headers can be entered comma-separated.
- **Administrative Domain:** When set to Yes, admin users of this domain are allowed to configure all domains, global settings and have access to the Dashboard. Admin users can be defined in User Connector Configuration.
- **Max Licensed Users**: If enabled, you can configure the maximum number of concurrent or named (depending on the license) users that are allowed to be logged in to this domain. When set to 0, domain users can't access the domain anymore.
- **Privacy Policy Acceptance**: When set to enabled, each user will have to accept the Privacy Policy the first time they log in. This is needed for GDPR compliance.
- **NetBIOS Domain Name**: NETBIOS domain name (e.g. MYCOMPANY)
- **Domain FQDN**: The FQDN of the (Active Directory) domain. E.g. domain.internal
- **DC/LDAP server**: It is highly recommended to specify the FQDN of the Domain Controller or LDAP server, especially when planning to move to Single Sign-On (SSO) at some point. E.g. ad01.domain.internal. Alternatively, you can specify IP addresses. Do not simply point to the FQDN of the Microsoft Windows domain. Multiple servers can be entered comma-separated. The authentication will always respect the order in which the servers are specified. If there is no connectivity to the first server, the next one in the list will be used, and so on.
- **Base DN**: When a user signs in, this base distinguished name (DN) is used to bind via LDAP to the Domain Controller/LDAP server. This can be used to filter access based on organizational unit (OU).
  Example without OU restriction: dc=domain,dc=internal
  Example with OU restriction: ou=Employees,dc=domain,dc=internal

  This field can be used to create different Parallels Secure Workspace domains, all pointing to the same NetBIOS. Only users of the configured OU will be able to log in to that domain.

- **LDAP over SSL?**: Requires SSL certificate on Domain Controller or LDAP Server.

  LDAP over SSL is required to allow users to change their password using Parallels Secure Workspace.
  Note that Microsoft advises using LDAPS on domain controllers.

  Please make sure the SSL certificate installed on the AD/LDAP server for LDAPS is encrypted using **SHA256**. A certificate using SHA512 is NOT supported by Parallels Secure Workspace. Therefore, LDAPS login will not work with SHA512.

- **DNS Servers**: This DNS server is used to resolve servers matching the domain FQDN. Multiple servers can be entered comma separated. E.g. if the domain FQDN is domain.internal, then fileserver.domain.internal will be resolved with the mentioned DNS server.

Optionally, a service user account can be defined, which is required for importing labels (users and groups) and applications servers from Active Directory from within System Settings. This is also required to enable single sign-on (SSO). To configure this service account, the following parameters are required:

- **Bind user for domain**: The username of the service account.
- **Password for bind user**: The password required to authenticate the service account.

For security reasons, it is recommended to create a new read-only user account with limited rights on the Domain Controller/LDAP Server for this purpose only.
Note that the "Base DN" is not used during the import, meaning that domain admins will be able to see all users/groups/servers of the whole Windows domain, unless the bind user has been configured on the Active Directory to only allow to list the ones of its OU.

Some advanced functionality:

- **Create Bind Name**: Defines how to bind user names in LDAP:
  - builtin.create_domain_bind_name (default): Bind using "DOMAIN\username".
  - builtin.create_username_bind_name: Bind using only the username.
  - builtin.create_uid_bind_name: Bind using uid=<username>,ou=Users,<base dn> .

  Find Groups: Defines how to query the LDAP Server for groups to which a user belongs.
  - builtin.find_groups_by_member_of: Find groups using the memberOf field in LDAP result.
  - builtin.find_groups_by_token_groups (default): Find groups recursively (method 1). Note: this method also fetches the primary group attribute.
  - builtin.find_groups_by_member: Find groups recursively (method 2).
  - builtin.find_groups_by_uid: Find groups using the UID.

The Trust settings make it possible to specify domain-specific trusted certificate authorities.

- **Trusted Certificate Authorities:** Certificates can be added per domain. They are used to verify the server identity when making HTTPS requests (e.g. external audit logging server or Reverse Proxied Web applications). Certificates can also be added on a Global level, see Connectivity > Global Certificates. If you want to add multiple domain certificates, you will need to bundle into one file. This can be done by copy-pasting the content of each PEM certificate (.pem/.cer/.crt) into one PEM file using any basic text editor.
- **Allow untrusted servers**: Determine if connections can be made to untrusted servers for each of the following features:
  - **External Audit Logging**
  - **Reverse Proxied Web Applications**
  - **WebDav with SSL**
  - **Pre-auth/SSO metadata**

Default Domain

A default domain is configured, which will be used if no domain is specified at login time or no correct host header was used.
To change the default domain, use the set default action on the domain to use as default.

SSL Offloading Settings

Introduction

If no external SSL offloader is available, Parallels Secure Workspace can handle the SSL offloading (also referred to as SSL termination) internally.

When using multiple Parallels Secure Workspace nodes for high availability reasons, we recommend using an external SSL offloader.

Only when the internal SSL offloader is used, you need to upload or generate the certificates in Parallels Secure Workspace under **Global > Certificates**.
Once the first certificate is uploaded or generated, Parallels Secure Workspace will start serving HTTPS on port 443. To enforce HTTPS, please refer to Connectivity Settings.

SSL Offloader

If no external SSL offloader is available, Parallels Secure Workspace can handle the SSL offloading (also referred to as *SSL termination*) internally.
When using multiple Parallels Secure Workspace nodes for high availability reasons, we recommend using an external SSL offloader.
In Certificate Settings, you can upload or generate SSL certificates. Once the first certificate is added, Parallels Secure Workspace will start serving HTTPS on port 443.

The internal SSL offloader can be used in three states:

- **Optional HTTPS**:
  - If you don't use an external SSL offloader, Parallels Secure Workspace is accessible via both port 80 (HTTP) and 443 (HTTPS). When accessing via HTTPS, the session cookies have the secure flag enabled: your session cookie is only valid for future HTTPS connections.
  - If you use an external SSL offloader, you will typically not have certificates uploaded in Parallels Secure Workspace and the SSL offloader will access Parallels Secure Workspace through port 80.
- **Internal SSL offloading with enforced HTTPS**:
  - You are not using an external SSL offloader.
  - Parallels Secure Workspace is only accessible via port 443 (HTTPS). All traffic on port 80 (HTTP) will be redirected to 443.
  - The session cookies have the secure flag enabled: your session cookie is only valid for future HTTPS connections.
- **External SSL offloading with enforced HTTPS**:
  - You are using an external SSL offloader.
  - You will typically not have certificates uploaded in Parallels Secure Workspace and the SSL offloader will access Parallels Secure Workspace through port 80.
  - The session cookies have the secure flag enabled: your session cookie is only valid for future HTTPS connections.

Enforced HTTPS with internal or external SSL offloader can only be selected when accessing the System Settings via HTTPS. This is to avoid being locked out of Parallels Secure Workspace .
Note: if you switch back from HTTPS to HTTP, you will need to clear your browser cache and delete your Parallels Secure Workspace cookies to be able to use Parallels Secure Workspace again.

When HTTPS is enforced (either internally or externally) the option to enable the **HSTS header** will become available.

Enabling this header will inform the browser that the Workspace should only be accessed using HTTPS, and that any future attempts to access it using HTTP should automatically be converted to HTTPS.

This header can be configured using the following options:

- **Max Age**: The time, in seconds, that the browser should remember that the Workspace is only accessible when using HTTPS.
- **Include Subdomains**: Determines if the HSTS header is also active on all of the website's subdomains.
- **Preload**: When enabled, the Workspace URL can be submitted to the HSTS preload list. To be accepted to the list, other requirements also need to be met.

It is recommended to increase the Max Age in stages e.g. starting with 5 minutes and gradually increasing this to a maximum of 2 years while monitoring the Workspace for issues.

More information on how to add your Workspace URL to the HSTS preload list can be found here: https://hstspreload.org/

When HSTS was previously enabled and the Max Age is not yet expired when switching back to Optional HTTPS, the Workspace will become inaccessible.

Clearing the Workspace browser data (including the HSTS settings) or using a different browser will make the Workspace accessible again.

Generating certificates automatically

If you do not own SSL certificates, you can use the *Automatic* option which will generate and configure SSL certificates provided by the free CA service of https://letsencrypt.org

To generate certificates automatically, click on Add and provide following information:

- **Certificate**: Automatic
- **Subject Names**: the host name(s) you want to create certificates for (e.g. remote.mycompany.com)

The generated certificates are valid for 90 days. After 60 days, Parallels Secure Workspace will renew the certificate. Therefore, the public servers of Let's Encrypt always need to be able to reach the Parallels Secure Workspace appliance on port 80 and 443.

⚠ Following network requirements are needed in order to request and renew automatic certificates:

- Ports 80 and 443 of Parallels Secure Workspace need to be accessible for the **public** servers of Let's Encrypt through all provided subject names.
- Parallels Secure Workspace needs to be able to reach the REST API of Let's Encrypt directly (without the use of an HTTP proxy) through port 443 for *.api.letsencrypt.org.

Please note there is a rate limit of the number certificates per registered domains and the number of duplicate certificates. Those limits are described in the documentation of Let's Encrypt. You can hit this limit easily if you use a subdomain of a service or cloud provider, like *.azure.com. Please use a subdomain you fully control.

Automatic SSL is only available for single-node Parallels Secure Workspace configuration or for multi-node Parallels Secure Workspace with only one Frontend service.
Requesting wildcard certificates is currently not supported.

Uploading certificates manually

The following types of certificates are supported:

- PKCS 12 certificates - typically with `.p12` or `.pfx` extension
- PEM certificates - typically with `.pem`, `.crt` or `.cer` extension

PKCS 12 certificates

PFX files can contain multiple certificates and can be password protected.

Click on Add and provide the following information:

- **Certificate Type**: Manual PKCS 12
- **File:** The certificate file in `.p12` or `.pfx` format
- **Password (optional):** The password required to decode the certificate

PEM certificates

Click on Add and provide the following information:

- **Certificate Type**: Manual PEM
- **Certificate**: The public certificate file in **.crt, .pem or cer format**, ASCII file, starting with:

```
-----BEGIN CERTIFICATE-----
```

  Make sure the certificate also contains the **intermediate key chain**, otherwise some browsers might not connect to Parallels Secure Workspace because the connection is not trusted.
- **Private Key**: The private key file associated with the certificate in **.key format**, ASCII file, starting with:

```
-----BEGIN PRIVATE KEY-----
```

or

```
-----BEGIN RSA PRIVATE KEY-----
```

PEM Certificates with passphrases

If you open the certificate key file and see binary characters instead of the BEGIN (RSA) PRIVATE KEY header, this means your certificate key is still encrypted with a passhprase. The Parallels Secure Workspace SSL offloader cannot start automatically when the private key is still encrypted using a passphrase. Therefore you'll need to remove the passphrase from the private key first before uploading the key file. You can remove the passphrase by using the openssl command as follows (you will also be prompted to type in your passphrase):

```
openssl rsa -in encrypted.key -out decrypted.key
```

Self-Signed Certificates

Although not recommended, Parallels Secure Workspace also supports self-signed certificates. Using self-signed certificates will show a security warning when accessing the site. They can be created for free. One of the easiest ways to do so, is to use an online self-signed certificate generator (for example: https://en.rakko.tools/tools/46/).

Certificate content

To validate if your certificate is correct - e.g. you want to make sure the certificate contains the intermediate key chain, you can visualize the certificate's content using the **Show Certificate** button.

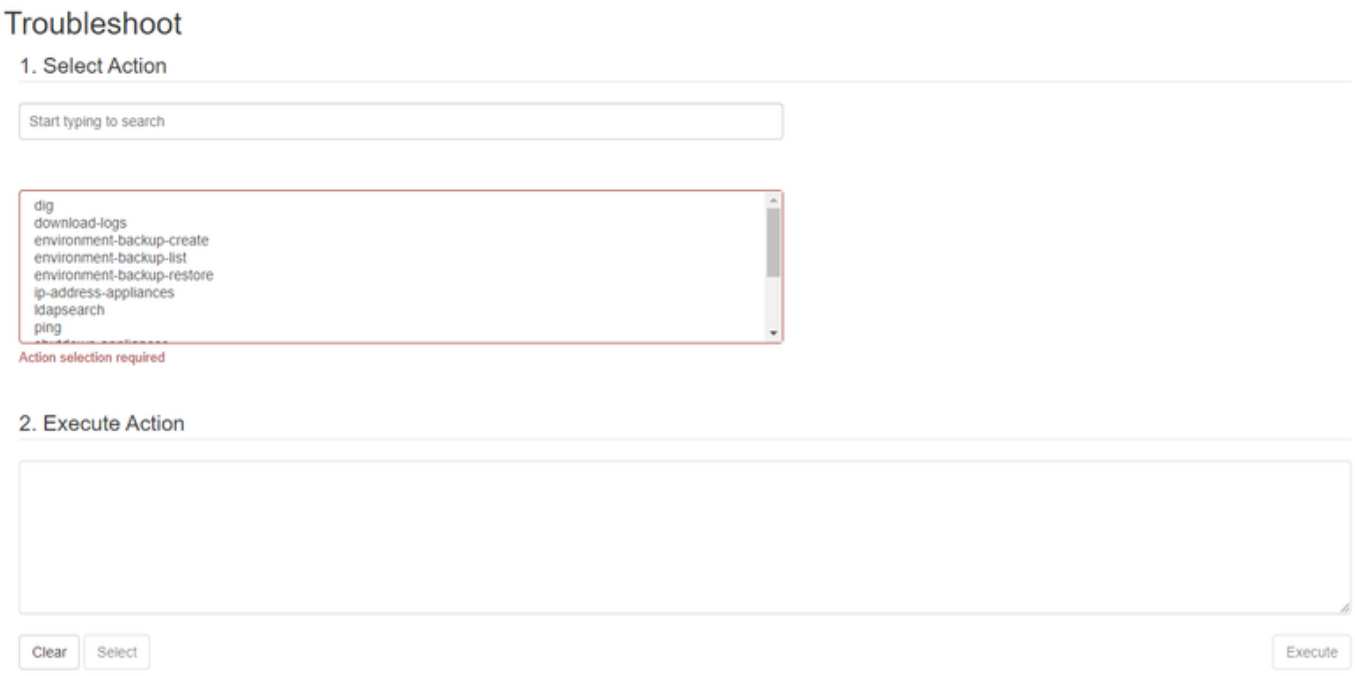
Replacing and deleting certificates

When you want to replace a certificate, e.g. because the existing one will expire soon, you first upload the new certificate and then delete the old one.

⚠ Expired manual certificates are not automatically deleted and are still offered to the browsers, which will cause a security warning for the user.

If you are deleting the last certificate of the subject name you are now browsing to, you will need to go manually to HTTP (if HTTPS is not enforced in Connectivity Settings) after deletion. If HTTPS is enforced, you need to go to another subject name you still have a certificate for. You won't be able to delete the last certificate if HTTPS is enforced, to avoid that you can not reach Parallels Secure Workspace anymore.

Troubleshoot



Actions

The Troubleshoot page offers some tools to allow you to manage internal database backups and to troubleshoot why your configuration is not working as expected.
The steps are as follows:

1. Select Action:
   - Select an action to execute
   - Some actions need arguments. Please enter them.
2. Select Target Appliance(s) to execute an action on
3. Execute Action:
   - Execute: execute the selected action and the output will be shown in the text box
   - Clear: empty the output text box
   - Select: select all output in the output text box

> All actions executed on the Troubleshoot page are logged into the log files. If you enter passwords in the commands, they will be logged in plain text. Please use the data of dummy users for all troubleshooting actions.

dig

Dig is a DNS lookup utility.

Example of arguments to use:

- Lookup for www.example.com on the DNS server with IP address 8.8.8.8

```
@8.8.8.8 www.example.com
```

- Lookup for repo-pub.awingu.com. No DNS server is given, so the one configured in the Connectivity tab is used.

```
repo-pub.awingu.com
```

Dig returns the answer from the DNS server (see Answer Section in the output)

More information: dig man page.

download-logs

Download the log files of the appliance. You can provide the following arguments to change the output format and time period:

- *From* and *To date:* By default, all logs from the last 7 days will be fetched. You can specify a from and a to date/time in UTC ISO format as arguments.
- *Json output:* By default, the different fields of a log statement are separated by spaces. By enabling newline-delimited Json output, the fields are available as Json properties and different log statements are separated by newlines.

A link to the log files will be shown in the output field. If the ZIP file is not ready yet, the file name starts with INPROGRESS. Every hour, ZIP files older than 1 hour will be cleaned up.

environment

These actions allow you to manage backups of the internal Parallels Secure Workspace configuration.

The following actions are provided:

Action	Description
environment-backup-list	Generates a list of all available environment backups on the environment.
environment-backup-create	Creates a new backup of the environment.
environment-backup-restore	Restores the environment backups of the provided file. Not available when using an external database (Only during the installation of a new appliance, e.g. when your node is corrupted or to move to a different hypervisor, ...). Note that by default there are already periodic backups available.

More information on Backup and recovery of the Parallels Secure Workspace Environment.

ip-address-appliances

This action will display the IP configuration of each Parallels Secure Workspace node in this cluster.

ldapsearch

Ldapsearch is an LDAP utility.

Example of arguments to use to simulate the default Parallels Secure Workspace behavior when User1 signs in:

```
-LLL -H ldap://domain.example.com:389 -b 'dc=domain,dc=example,dc=com' -D
'DOMAIN\User1' -w 'password' '(&(sAMAccountName=User1)(objectClass=user))'
```

Argument definition:

- -LLL: show the output in LDIF format
- -H '<ldap_url>': the URL of the LDAP server. Typically: 389 (no SSL). Mind that attempting to use LDAPS (port 636) will likely result in a failure, as a typical LDAP server uses a certificate that is not trusted by Parallels Secure Workspace.
- -b '<base_dn>': the starting point for the LDAP search
- -d '<level>': specify this argument with a value of 1 to see trace information.
- -D '<bind_dn>': the distinguished name to bind to the LDAP directory. See Functions in User Connector tab:
  - function builtin.create_domain_bind_name (default): '<domain_name>\<username>'
  - function builtin.create_username_bind_name: '<username>
- -w '<password>': the password for the user to bind with
- '<filter>': LDAP search filter. The filter used by Parallels Secure Workspace: '(&(sAMAccountName=<username>)(objectClass=user))'

Ldapsearch returns the LDAP search result. Interesting output lines are the ones starting with "memberOf", to see the list of AD security groups the user belongs to.

More information: ldapsearch man page.

ping

Ping is a ICMP echo request sending tool.

Example of arguments to use:

- Ping 3 times to example.com:

```
-c 3 example.com
```

- Ping 5 times to example.com and only show IP addresses (n = numeric):

```
-c 5 -n example.com
```

More information: ping man page.

shutdown-appliances

Performs a clean shutdown of all the appliances in this Parallels Secure Workspace cluster.

sync-appliances-time

Initializes an immediate time synchronization against the configured NTP servers.

Afterwards, it's possible to confirm the time by running the **uptime** action.

tcpscan

Scans for open TCP ports. This action requires the following arguments:

- Host: hostname or IP address
- Port: single port, port range (e.g. 80-100) or comma-separated list of ports (e.g. 80, 443).

traceroute

Traceroute is a tool which prints the route packets trace to a network host

Example of arguments to use:

- Trace route to example.com

```
example.com
```

- Trace route to example.com and only show IP addresses (n = numeric):

```
-n example.com
```

More information: traceroute man page .

udpscan

Scans for open UDP ports. This action requires the following arguments:

- Host: hostname or IP address
- Port: single port, port range (e.g. 80-100) or comma-separated list of ports (e.g. 80,443).

uptime

Uptime is a utility that tells how long the system has been running.

It shows some additional information, example:

```
15:21:06 up 2 days, 1:46, 0 users, load average: 0.19, 0.25, 0.25
```

- 15:21:06: current time of the Parallels Secure Workspace VM in UTC. If the time is not correct, this can indicate a faulty NTP server.
- up 2 days, 1:46: number of days and hours since the last time the Parallels Secure Workspace VM has booted.
- 0 users: number of system users logged in to the system. Is typically 0.
- load average: system load of past 1, 5 and 15 minutes. The VM is overloaded if the value is higher than the number of CPUs.

More information: uptime man page .

Logging

In this section, the log level of the **Application Gateway** can be modified. This can be very helpful when troubleshooting an issue with applications. Changing the log level does not cause a service disruption.

Be aware however that if you change the log level to Info, Debug or Trace a lot more logs will be generated. As there is a maximum of 8 GB disk space allocated for logs, it will not have an impact on the overall appliance but logs of other services will get cleaned up sooner.

Connectivity Settings

The connectivity section groups parameters required for Parallels Secure Workspace to interface with external services.

Servers

The servers are configured during the installation and can be edited here.

- **NTP server**: The IP or fully qualified domain name of your **Network Time Protocol** server. You can use the Active Directory domain controller if the time source of that server is reliable (more information). It's recommended to specify 3 trustworthy NTP servers. Note that the NTP settings will be ignored if they are provided via DHCP.
- **DNS IP address(es)**: IP address(es) of one or more DNS servers to be used by Parallels Secure Workspace.
- **Repo Server URL**: The repo server hosting the Parallels Secure Workspace packages (needed for upgrades). Please fill in the following URL: https://repo-pub.awingu.com.

HTTP Proxy

The HTTP Forward Proxy server is configured during the installation and can be edited here. The proxy server will be used to reach public services, such as the Repo Server of the previous section, DUO MFA and OneDrive. Note that automatic SSL (Let's Encrypt) is not using this proxy. Please refer to Connectivity Requirements for more details about outbound connections.

- **State**: Enable or Disable the use of an HTTP Proxy Server
- **HTTP Proxy Server URL**: The URL of an HTTP forward proxy server. Username and password can be embedded in the URL, e.g. http://username:password@proxy.mycompany.com

External Reverse Proxy

Relevant when using Parallels Secure Workspace behind an external reverse proxy, load balancer, or SSL offloader. Here you specify the IPv4 address(es) or network(s) (comma separated) of those devices. For requests that come from these IPs, Parallels Secure Workspace will use the supplied **client IP** in the **X-Forwarded-For** or **X-Real-IP headers**. Otherwise, the actual IP that was used to connect to Parallels Secure Workspace as the client IP will be used. The correctness of this client IP is important for auditing and whitelisting purposes.

If you are accessing Parallels Secure Workspace without reverse proxy, load balancer, or SSL offloader: please keep this field empty for security reasons.

SNMP

The status and health of Parallels Secure Workspace appliances can be monitored and integrated in your monitoring system using SNMP.
If enabled, all appliances provide an SNMP agent which is accessible using SNMPv3.
All communication is AES encrypted and access is password protected.
The agents are accessible on *UDP port 161* with a read-only user.

- **State**: Enable or Disable SNMP agents on the Parallels Secure Workspace appliance(s)
- **Username:** Read-only user *snmp.*
- **Password**: Self-selected password required to access the SNMP agents

An example of a snmpwalk command (for Linux users):

```
snmpwalk -v 3 -Os -l authPriv -u snmp -x AES -X '<password>' -a SHA -A
'<password>' <appliance IP>
```

Trusted Certificate Authorities

It's possible to add globally trusted certificate authorities. These will be trusted by all configured Parallels Secure Workspace domains.

Certificates can be added which are used to verify the server identity when making HTTPS requests (e.g. connections to the repo server, external audit logging server, Reverse Proxied Web applications, or HTTP proxy). Certificates can also be added per Domain. For more information, see the Domain Details. If you want to add multiple global certificates, you will need to bundle them into one file.

This can be done by copy-pasting the content of each PEM certificate (.pem/.cer/.crt) into one PEM file using any basic text editor.

Database connection

Optionally, Parallels Secure Workspace allows connectivity to an **external database**. This setting is configured during the installation and cannot be edited afterwards.

Environment Backups

Parallels Secure Workspace creates a backup of the environment every day and stores it on the appliance. You can retrieve this backup and save it on another system via SFTP. The backups are retained on the local disk for a period of 3 days, before being discarded. More information: Backup and recovery of the Parallels Secure Workspace Environment.

You can choose the credentials of the SFTP user that can access the backup files:

- **SFTP Username:** SFTP username *dbbackup*. This cannot be changed.
- **SFTP Password:** SFTP password.
- **Encryption Password:** Password to use to encrypt the environment backups. We highly recommend setting a password, since backups may contain sensitive information. When this password is not set, backups will not be encrypted. Encrypted backups have the '.enc' extension and will require this same password to be able to restore the backup.
- **Vault Backups:** Determines whether the vault is also backed up.
- **Start backup at:** Schedules the time of the daily backup.

Vault

The vault is needed when you want to enable Single Sign-On in Parallels Secure Workspace.

Since the private key for the Parallels Secure Workspace SubCA allows Parallels Secure Workspace to impersonate Microsoft Windows users, this key is highly sensitive and is stored in a vault inside Parallels Secure Workspace. The vault itself is also encrypted and the encryption key for the vault can either be stored on the Parallels Secure Workspace appliance itself (Internally) or on an external Vault provider like Google Cloud Key Management Service or Azure Key Vault.

For more details see Enabling Single Sign-On (SSO)

System Settings - Configure

Domain specific settings are configured here:

- Branding Configuration
- Feature Configuration
- User Connector Configuration

Branding Configuration

Multi-domain branding behavior

Each domain has its own branding configuration:

When accessing the login page	Domain field	Branding
Using the host header defined in Domain Settings:	Hidden	Specific branding
Using a non-defined host header and there is only one domain configured:	Hidden	Specific branding
Using a non-defined host header and there are multiple domains configured:	Visible	Default domain branding

When you are logged in, he branding of the applicable domain is shown.

Configuration options

For each domain following settings can be shown:

General

- **Primary Color:** The base color used to generate the background, polygon, pop-ups, and favicon of the Parallels Secure Workspace frontend for this domain. It is recommend to choose a bright color.
- **Secondary Color:** The color used in the Parallels Secure Workspace frontend for buttons, folder icons, etc.
- **Background Type:** Whether to have the Parallels Secure Workspace polygon background or a plain color. In both cases, the primary color is used. Note that the background of the login page can be customized further on this page.

Wide Logo

- **Active Wide Logo**: Choose between the default Parallels Secure Workspace logo and your own custom logo. The logo is shown on the top left of the front end on the login page and the non-collapsed sidebar.
- **Custom Wide Logo**: Upload an image for your custom logo:
  - Maximum file size: 100 KiB
  - Logo area: 159 x 70 px (when you scroll down, the logo area reduces to 159 x 30 px)

Square logo

- **Active Square Logo**: Choose between default Parallels Secure Workspace polygon (with the color based on the primary color) and your own custom square logo. The logo is shown as favicon and on the collapsed sidebar.
- **Custom Square Logo**: PNG, JPG, SVG or ICO file of max. 2 MiB. Image needs to be square. Best results with PNG of 512 x 512 px or SVG image.

Note that if you have already accessed Parallels Secure Workspace using the same browser before changing the square logo, you might need to clear your browser cache to see the favicon being changed.

Login Page

- **Active Background**: Choose between the default Parallels Secure Workspace background image and your own custom background on the login page.
- **Custom Desktop Background**: upload an image for your custom background for desktops (= screen width or height is more than 1280 pixels)
  - Maximum file size: 500 KiB
  - Recommended resolution: 3000x2100.
- **Custom Tablet Background**: upload an image for your custom background for tablets (= screen width or height is less than 1280 pixels)
  - Maximum file size: 150 KiB
  - Recommended resolution: 1280x860.
- **Login Text**: A free-field text, beneath the login credentials area, to put company specific information such as e.g. legal disclaimers. HTML tags are allowed.

Note about the background images:

- Rescaling (both scale-up and scale-down) is done while keeping the aspect ratio.
- When the scaled image is smaller than the canvas height, the upper and lower part will be cut-off equally.
- When the scaled image is smaller than the canvas width, the left and right part will be cut-off equally.
- The white banner with the logo will cover the upper part of the background image.

Feature Configuration

Behavior

All features listed are enabled for users depending on their **User Labels** and **Context Policy Labels**.

When the label of a user matches one the User Labels configured for a feature, the security context of the user will be validated against the Context Policy of that feature.

- To enable a feature for all users of the domain, attach the predefined `all:` User Label to that feature and leave the Context Policy Labels field empty.
- To disable a feature for all users of the domain, remove any User Labels from that feature.

To create custom labels and to find more information, please refer to Label Management .

Application session printing

When disabled, printing using the "Virtual printer" within the streamed application will not be possible. Printing using other printers configured on application servers will still be possible.

Application session sharing (publicly)

Defines if application session sharing is disabled altogether or only disabled for public access. A list of possible scenarios:

The user does not belong to either *Application session sharing* and *Application session sharing publicly* user labels:

- The feature to share application sessions with other users is disabled.
- The Share session polygon button is not shown.

The user only belongs to *Application session sharing* users labels and his security context is valid:

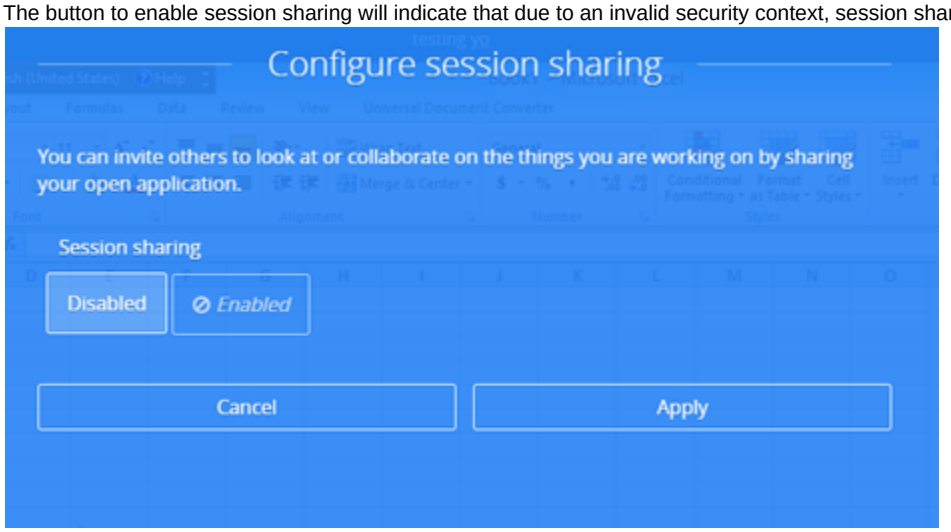
- The user can only share his application sessions with users from the same Parallels Secure Workspace Domain.

The user belongs to *Application session sharing publicly* user labels and his security context is valid:

- The user can share his application session with anyone as long as they have the share link.
- Note: it does not matter if he also belongs to the *Application session sharing* user labels.

The user belongs to *Application session sharing publicly* user labels and his security context is invalid:

- The button to enable session sharing will indicate that due to an invalid security context, session sharing is not allowed.



- Note: it does not matter if he also belongs to the *Application session sharing* user labels.

Note: This feature is accessible in a streamed app when clicking on the polygon and then on the share button.

File download

When disabled, the *Download* action is disabled for all files and folders on the Files page.

Note: it may still be possible for users to preview the file. If this is not desired, unlink the file types from the built-in Preview application in Parallels Secure Workspace.

Files

When disabled, the *Folders* section on the Files page is removed. If File sharing is disabled, too, the complete Files page is removed.

File sharing (publicly)

Defines if file sharing is disabled all together or only disabled for public access. A list of possible scenarios:

The user does not belong to either *File sharing* and *File sharing publicly* user labels:

- The *Shares* section on the Files page is removed. If Files is disabled, too, the complete Files page is removed.
- The *Share* action is disabled for all files and folders.

The user only belongs to *File sharing* users labels and his security context is valid:

- The user can only create file shares that can be accessed by someone from the same Parallels Secure Workspace Domain.
- The user will be able to choose Users where he can add specific users and groups or choose Domain so everyone from the Parallels Secure Workspace Domain can access the file.

The user belongs to *File sharing publicly* user labels and his security context is valid:

- The user can create files shares that can be accessed by anyone as long as they have the share link.
- Note: it does not matter if he also belongs to the *File sharing* user labels.

The user belongs to *File sharing publicly* user labels and his security context is invalid:

- The *Share* action will indicate that due to an invalid security context file sharing is not allowed.
- Note: it does not matter if he also belongs to the *File sharing* user labels.

File upload

When disabled, the *Upload* action is disabled for all files and folders on the Files page.

Local clipboard

When disabled, using you cannot copy/paste data from streamed applications to your local device and vice versa.

User Connector Configuration

Login Permissions

In this section, you define which users are allowed to log in by using the label system.

- **User Labels:** Users with at least one of these labels will be able to log in (if all users can log in, add the `all:` label)
- **Context Policy Labels:** Users will only be able to log in if they have a valid context. The context can be configured using the MFA, network, or country (2 char ISO 3166-1 alpha code) context policies labels. For network and country, you can define multiple options by using comma-separated values. When adding multiple policies, they must all be valid to be able to access the application. No labels means there are no restrictions.

See Label Management (User and Context Policy Labels) for more information and examples.

Enable Multi-Factor Authentication on Login
To enable Multi-Factor Authentication for all users when logging in, the `mfa:required` context label will need to be added to the Context Policy Labels.

Admin Permissions

In this section, you define which users are Domain Administrators and which security context is required to be a Domain Administrator.

- **User Labels:** Users with at least one of these labels will be Domain Administrators
- **Context Policy Labels:** Users will only receive the Domain Administrator role if their context is valid. The context can be configured using the MFA, network or country (2 char ISO 3166-1 alpha code) context policies labels. For network and country, you can define multiple options by using comma-separated values. When adding multiple policies, they must all be valid to be able to access the feature.

See Label Management (User and Context Policy Labels) for more information and examples.

Account Settings Defaults

This section allows you to define default profile values for users of a domain.

- **Keyboard layout:** The default configured keyboard layout for users of this domain
- **Language:** The Parallels Secure Workspace interface's language for users of this domain. By default Parallels Secure Workspace will use the browser's default language. If this is unknown to Parallels Secure Workspace, it will fall back to this language configured for the domain.
- **Guided tours:** Defines if the guided tours are shown for new users of this domain. Note: guided tours will not appear when the browser size is too small.
- **Polygon:** Defines if the polygon is shown by default for new users of this domain.

Please note that a user can always update these settings on his/her Account Settings page.

Change Password Failed Message

When users try to change their password but this fails, a custom error message can be added by the administrator. For example, it could be used to inform the users about password complexity requirements.

Multi-factor Authentication

Parallels Secure Workspace provides out-of-the-box one-time-password (OTP) support and integrates with several Multi-Factor Authentication providers.

When enabled, each time a user wants to sign in to Parallels Secure Workspace, they will need to generate a token via an authenticator app or a hardware token on top of their initial authentication using LDAP credentials or a third-party Identity Provider (IdP).

Multi-factor authentication is disabled by default but can be enabled by selecting the desired integration mode.

> When using a **built-in Workspace OTP** method, we highly recommend "time-based" in most cases since it's more secure and easier to sync on multiple devices.
> For more details on the user experience of these built-in methods, see Using Workspace built-in OTP

- **Workspace OTP: Counter Based:** Leverages the built-in counter-based one-time-password (OTP) functionality.
  - **Issuer name:** The company name shown to the user in the OTP application.
  - **Manage User Token Count**: Allows resetting the token count for specific users. When the token is reset, the user will need to set up the device again.
- **Workspace OTP: Time Based**: Leverages the built-in time-based one-time-password (OTP) functionality. For this option, it is important to keep the time of the appliances in sync with real world time. Make sure to specify trust-worthy NTP servers .
  - **Issuer name:** The company name shown to the user in the OTP application.
  - **Manage User Token Count**: Allows resetting the token count for specific users. When the token is reset, the user will need to set up the device again.
- **Duo Security:**
  For more information: Integrating Parallels Secure Workspace with DUO
  - **API Hostname:** The Duo Auth API configured hostname
  - **Integration Key:** The Duo Auth API integration key
  - **Secret Key:** The Duo Auth API secret key

- **RADIUS:** The token will be validated using an external RADIUS server. Note: Chap (v2) authentication schema is not supported at this time. The RADIUS server needs to be configured to not increase the counter for a failed attempt. For FreeRadius, this means adding `no_incrementt_hotp` to auth requisite in the radiusd config file.
  - **Servers:** Comma-separated list of hosts or IP addresses of the RADIUS server.
  - **Port:** The port number the RADIUS server is listening on.
  - **Secret:** The secret configured in the RADIUS server.

For all MFA providers, you can configure the following additional settings:

- **LDAP Username Attribute:** the LDAP attribute used to provide a username to the provider, via the **LDAP Username Attribute** field. One of the following attributes can be chosen:
  - **sAMAccountName**: Corresponds with the login name without UPN on Windows Domain Controller.
  - **NETBIOS\sAMAccountName**: Same as sAMAccountname, but with the NetBIOS name prefixed.
  - **userPrincipalName**: Corresponds with the UPN on Windows Domain Controller.
  - **uid**: Corresponds with the login name without UPN on OpenLDAP. This should not be selected when initially authenticating against a Microsoft Windows Active Directory.
- **Whitelisted subnets:** Comma-separated list IPv4 subnets. For users accessing Parallels Secure Workspace from these subnets, Multi-Factor Authentication will be skipped.

  > When using a reverse proxy server in front of Parallels Secure Workspace, please make sure you forward the client's originating IP address using the **X-Forwarded-For** header. See SSL offloader, reverse proxy or loadbalancer settings.

- **Whitelisted User Labels:** For users that belong to one of the user labels Multi-Factor Authentication will be skipped.
- **Trusted Browser:** If enabled, users will be asked if they trust the device. If so, no MFA will be required for 30 days. Note that if the user deletes her browser cookies, MFA will be required again.

> The management user (created during installation) does not need to use any form of MFA to log in. To avoid access with that user from the public Internet, you can limit subnets from where that user can log in on General Information .

API Token Based Authentication

Next to basic authentication with username and password, administrators can use authentication with an API token. This is useful for the automation of Parallels Secure Workspace through scripts using the REST API. As this token never expires, it is recommended to limit the usage of the token to the network of the computers/servers where the scripts are running using Whitelisted Subnets.

Note: if Whitelisted Subnets are disabled for API Token Based Authentication, the API token can be used from anywhere.

Administrators can generate an API token from their **Account settings** page under **Manage API token**:

See Automate Parallels Secure Workspace via the REST API for a PowerShell example.

Reverse Proxy

Here you set the default host header for this domain that will be used when accessing a reverse-proxied web application.

Federated Authentication

See Parallels Secure Workspace Single Sign On (SSO) for detailed instructions on how to set up Single Sign-On and SAML/OpenID Connect Authentication.

Next to the standard username/password login, Parallels Secure Workspace is also able to do a full Single Sign-on (SSO) via an external Identity Provider.

When switching to SSO, the login becomes a two-step process.

1. Parallels Secure Workspace no longer does the authentication of the user itself. Instead, this is handled by an external Identity Provider (IDP).
2. Because the external IDP doesn't expose the passwords and the Microsoft Remote Desktop Protocol (RDP) doesn't support ticket/token-based logins, the credential-based login towards back-end systems (remote app, VDI, storage, ...) is replaced by a **certificate-based login** mechanism.

Enabling the Federated Authentication can be done in two steps/levels:

1. When enabling Pre-Authentication, the user will need to authenticate with the configured identity provider before authenticating in Parallels Secure Workspace. This adds an additional validation step but will still require that users provide their Microsoft Windows password to the Parallels Secure Workspace Appliance. See Enabling Pre-Authentication (PreAuth) for integration instructions.
2. Once Pre-Authentication is working, the password step can be replaced by a full SSO-process based on the certificate/Kerberos login mechanism. See Enable Single Sign-On (SSO) for integration instructions.

Automatic Logout

Changes to any of these settings will only be applied when the user signs in to Parallels Secure Workspace again. It does not affect logged-on users.

Automatic Logout: Enable or disable this feature.

Inactivity timeout: When automatic logout is enabled, a specific timeout can be configured in seconds. The default is 3600 seconds (1 hour). User sessions may remain open for up to 1 minute after the timeout has been reached. The minimum is 2 minutes, the maximum is 4 hours.

User Labels: Define the users for whom the automatic logout is enabled. The built-in management user however will always automatically be logged out after 10-15 minutes.

Application Sessions

This section applies to streamed applications (RDP apps and RemoteApps).

Application Recording

Parallels Secure Workspace allows saving recordings of streamed application sessions. When a session recording ends, the resulting recording file is automatically transferred from the Parallels Secure Workspace appliance's local disk to a back-end file server you define. Those recorded files can be played with the **Recorded Session Player**, which is accessible to all users in a group with the *admin* label.

When this feature is enabled, the following streamed app sessions will be recorded:

- All applications with the *record* label (cf. Application Management), no matter which Recorded Users are specified.
- All applications started by users specified using labels in the **Recorded Users** setting.

Settings:

- **Recordings Upload**: Enable or disable the uploading of recorded sessions of streamed applications to the specified upload URL.
- **Recordings Upload URL**: Specifies destination for recorded sessions in the following specific structure:
  - For HTTP: http://username:password@server:port/path/to/save
  - For SMB/CIFS: smb://DOMAIN\username:password@server:port/path/to/save
    Note that DOMAIN should match a **Parallels Secure Workspace domain name**, which might be different from the NetBIOS name or the FQDN of the Microsoft Windows domain, and must be upper case.

- For privacy reasons, please make sure that only authorized personnel can access the server defined in the Recordings Upload URL.
- Known limitation: certain special characters in the password are not allowed. This includes a space and these characters: # / :
- When uploading fails, recorded sessions are kept internally for up to 7 days on the Parallels Secure Workspace node. If uploading starts working again, those recorded sessions will still be uploaded.

Session keep-alive

Keepalive Disconnected Timeout: Number of minutes the streamed application session will be kept alive. A session can be kept alive when the end users accidentally close their browser or browser tab, when they lose network connectivity, or when they log out without closing their applications. After the time-out, the application will be terminated (unsaved changes will be lost). The maximum value is 1440 minutes (1 day).

External Audit Logging

Parallels Secure Workspace allows you to forward all audit logs to an external system using the HTTP protocol.

This can be used to integrate with external systems such as security tools (e.g. SIEM tools), reporting tools or automation systems.

To enable audit log forwarding, only a URL is required, optionally you can provide credentials for Basic Authentication.

- **State:** Enable or disable the forwarding of audit logs for this domain.
- **External Audit System URL:** The URL to which all audit logs will be forwarded.
- **Basic Authentication:** Enable to add an authorization header to all requests with the specified credentials.
- **Username:** (Optional) Username to use for Basic Authentication.
- **Password:** (Optional) Password to use for Basic Authentication.

More information on how you can integrate *External Audit Logging,* can be found on External Audit Logging .

System Settings - Manage

Domain specific objects can be managed here:

- Category Management
- Application Management
- Application Server Management
- Drive Management
- File Type Management
- Label Management
- User Management

Category Management

Categories are logical groups of applications available to end-users. These categories are visible to end-users in the left pane of the Applications tab in the Workspace (user interface). There are three types of categories:

- Category **All**: The category 'All' contains all applications that the end-user is authorized to use. This category is always present and cannot be configured.
- Category **Favorite**: When a user first logs on to Parallels Secure Workspace, this category is empty. End users can add/remove applications to the 'Favorite' category. The category 'Favorite' is always visible to end users in the user interface, even when it is empty. The category 'Favorite' is built-in to the Parallels Secure Workspace application and is not configurable by administrators.
- **Other categories**: System administrators can define additional categories for end users. These additional categories will be visible to end users when they are authorized to at least one application that belongs to that category. There is a many-to-many relationship between applications and categories. Administrators can assign zero, one, or multiple categories to an application, see Application Management. Similarly, a category can be assigned to zero, one or more applications.

This page provides you with a list of existing categories and allows you to add, remove, or modify categories.

Application Management

Introduction

This page allows managing applications for each domain. Parallels Secure Workspace supports the following types of applications:

- Streamed Applications, using the Remote Desktop Protocol. Parallels Secure Workspace supports 3 flavors:
  - **RDP Application**: This will make use of the regular Remote Desktop Protocol.
  - **Desktop Application**: Similar to the RDP Application type, except that the Command, Working Folder, and File Types properties do not have to be provided.
  - **Remote Application**: An extension to the Remote Desktop Protocol. RemoteApp needs to be supported by your application server, and your applications need to be exposed over RemoteApp. It has several advantages over regular RDP applications:
    - The window selector (Windows button at the top of the app) is available.
    - The experience on tablets is smoother (especially when rotating the tablet and zooming in/out).
    - The app-sharing experience is better.
    - It uses fewer resources on the application server.

  When both RemoteApp and RDP Applications are supported on your application server, we strongly recommend using RemoteApp.

- Web Applications. Web applications are not served through the RDP gateway. Instead, when launching a web application, a separate browser tab will be opened. You can specify whether to use the **built-in reverse proxy** for HTTP(S).
  - **Web Application**: The browser will be redirected directly to the URL of the web application, which needs to be reachable from the end-user's device.
  - **Reverse Proxied Web Application**:
    - The browser will be redirected to a configured source hostname (e.g. intranet.mycompany.com), which resolves (using DNS) to the same IP as the Parallels Secure Workspace environment.
    - Parallels Secure Workspace will check if the user is authenticated and has the right to access the application. If so, the content of the web application is reverse proxied through Parallels Secure Workspace.
    - Parallels Secure Workspacecan be configured to rewrite HTTP headers (including cookies) and the body to replace all occurrences of the destination URL with the source hostname.
    - If Parallels Secure Workspace is configured to do SSL offloading, it also behaves as an SSL offloader for an HTTP web application.
    - If the web application supports Basic Authentication, the username and password given to Parallels Secure Workspace can be provided to the web application (= Single Sign-On, SSO).

    There are however some limitations:
    - When the rewrite option is enabled, the web application might still have links to the original destination URL instead of the configured source hostname. This might be because it uses content that is not text/html or because the URL is obfuscated or encoded. Therefore, if the web application has support to run behind a reverse proxy, we recommend not using the rewrite option in that case.
    - The reverse proxy uses a connection pool toward the web application. This means NTLM authentication cannot work because it needs a persistent connection to the browser.
    - Uploading a file to a reverse proxied web application is limited to 100 MB.

Other references:

- To define the application servers, please refer to Application Server Management .
- To prepare the application servers, please refer to Integrating with existing Microsoft Windows environment .
- Parallels Secure Workspace does NOT manage the actual applications on the application server(s). There are commercial products are available to do so.

Adding applications manually

Click on **Add** and choose the type of application you would like to add.

General Settings

The following general settings apply to all types of applications:

- **Name**: The application name as it will appear in the Workspace (user interface).
- **Description**: Description of the application, not visible to end-users.
- **Icon**: The application icon that will be visible to the end-user in the Workspace (user interface). When you upload an icon, it is saved to the database and automatically propagated to all Parallels Secure Workspace front-end instances in your deployment. Only ICO, JPG and PNG are allowed.
- **Categories**: Associate zero, one or more application categories to this application.
- **User Labels**: User labels are used in the process of authorizing users to applications. Only users with labels assigned in this field will see the application in the Applications tab (use *all*: to be visible to all users). See chapter on Label Management for more information.
- **Show in Applications:** When disabled, the application will not be shown on the Applications page in Parallels Secure Workspace. Note: This only hides the application. If users have the appropriate permissions for the application, they will still be able to access the application through the Direct link.
- **Labels**: Add labels to applications to group them. These groups can be used to filter application servers in lists and reports. This is also used to enable specific features:
  - The *smartcard:* label is used to enable smart card access for this application (see Smart Card Redirection for more information).
  - The *record:* label is used to activate session recording for this application for all users (needs to be enabled).
  - The *rewritegroup:xxxxx* label is useful when multiple web applications are reverse proxied by Parallels Secure Workspace and are linking to each other. By default, Parallels Secure Workspace will only rewrite URLs per reverse proxy web application. Note: make sure to first create this label in Manage > Labels.
- **Auto Start Labels:** Start the application automatically at login for users with defined matching labels. The set of labels you can define are the same as *User Labels*. Use "all:" to enable the auto start of the application for all users. The application will be started in the background and will be available to the user via the sidebar. Note: recorded applications will not be started automatically and this feature is not compatible with the option Ask for Credentials.

Desktop Application

- **Server Labels:** Server labels identify on which application servers this application is available. When a user launches this application, these labels will be used to generate a candidate list of application servers to connect to.
- **Context Policy Labels:** Restrict this application to only be accessible within the provided security context. The context can be configured using the mfa, network or country (2 char ISO 3166-1 alpha code) context policies labels. For network and country, you can define multiple options by using comma-separated values. When adding multiple policies, they must all be valid to be able to access the application. See the Label Management page for more information and examples.
- **Unicode Keyboard Support**: Disable when the application (e.g. software made with Qt) does not support the Unicode Keyboard that Parallels Secure Workspace uses in the RDP Gateway. We suggest first trying with Unicode Keyboard Support enabled. However, when typing in the application results in a repetition of the first typed character or other odd behavior, then you should disable the Unicode support and try again. The advantage of Unicode Keyboard is better recognition of special characters on keyboards and the use of on-screen keyboards on tablets.
- **Color Depth:** Defines how many bits per pixel should be used. The higher the color depth, the higher the detail of the application but it will also take more processing and bandwidth. Default is set at 16bpp and can be increased to 24bpp or 32bpp.
- **Start in Foreground***:* If enabled and the application auto starts at login, it will immediately be presented to the user and the workspace will be skipped.
- **Concurrent Usage**: Allow a user to open multiple instances of this application at the same time. This is enabled by default. A common use case to disable this option is for an application that accesses a predefined user-owned file, such as Microsoft Outlook (only one process can access the user's mailbox).
- **Ask for Credentials***:* A user will have to provide credentials to log in to the application. Otherwise, Parallels Secure Workspace provides the user's login credentials to the application server. This is useful when the Server Labels are linked to application servers that are not joined to the Microsoft Windows domain. Can only be enabled when there are no Auto Start Labels assigned.
- **Notifications:** Allow this application to send notifications to a user (default enabled). Those notifications will be shown in the sidebar as a red dot. If the application provides a relevant hover text for the systray icon, this will also be shown to the user.
- **Minimum Size**: When enabled, you can set the minimum size to be able to use this application on devices with small screens. If the visible part of the application session is smaller than this minimum size, you will be able to pan inside the session.
- **Maximum Size:** When enabled, you can set the maximum size of the application. When the browser window is bigger than the application, the application will be positioned in the top left. Can be used together with the minimum size feature to configure a fixed size for this application.

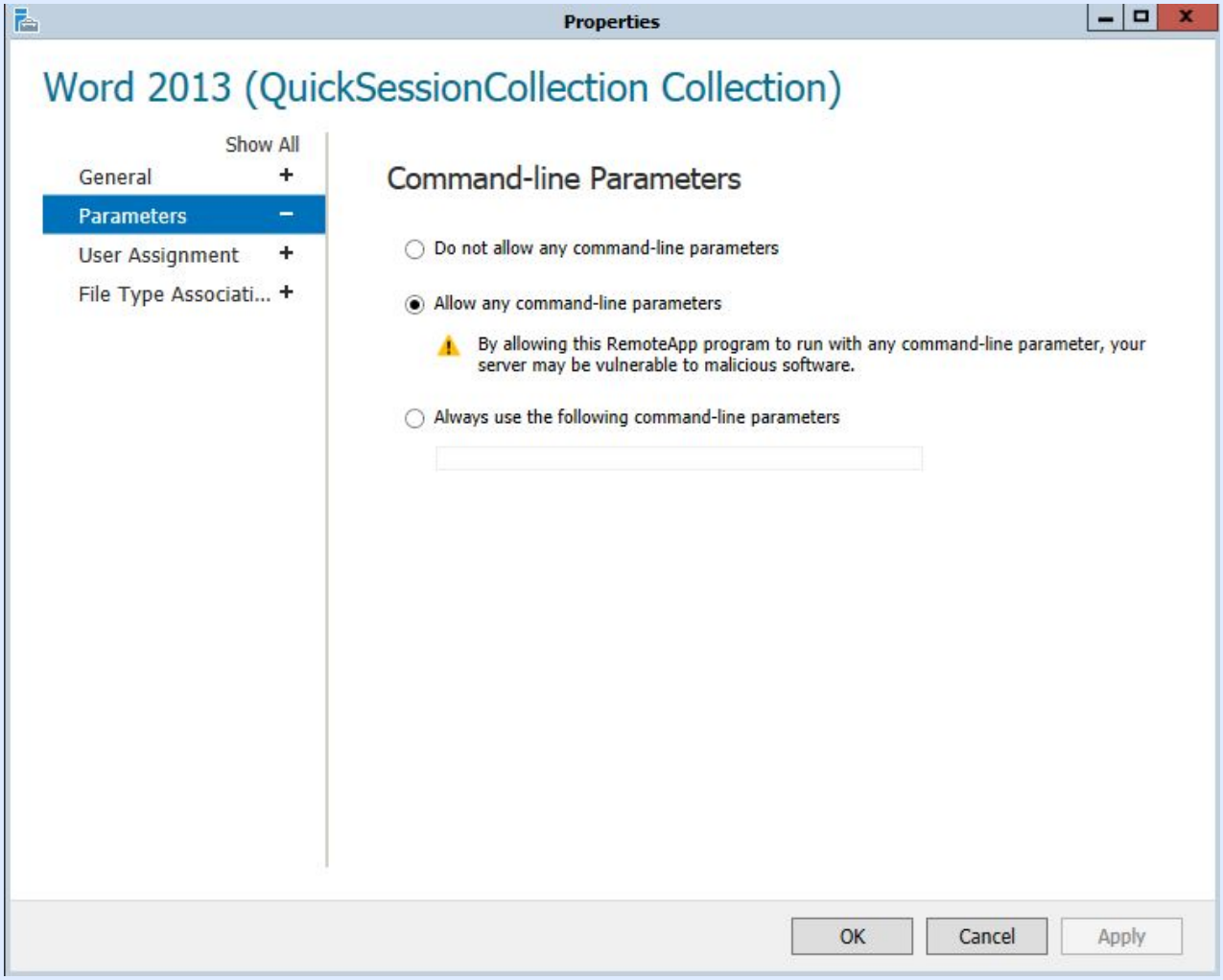
RDP Application

- **Command**: The full path to the program executable. Mind that parameters are not allowed here.
- **Working Folder***:* Folder into which an application needs to be launched, i.e. the current working directory. This can remain empty.
- **Context Policy Labels:** Restrict this application to only be accessible within the provided security context. The context can be configured using the mfa, network or country (2 char ISO 3166-1 alpha code) context policies labels. For network and country, you can define multiple options by using comma-separated values. When adding multiple policies, they must all be valid to be able to access the application. See the Label Management page for more information and examples.
- **Server Labels:** Server labels identify on which application servers this application is available. When a user launches this application, these labels will be used to define a list of applicable servers to connect to.
- **File Types:** Associate zero, one or multiple file types with this application for viewing or editing.

> If you want to associate file types with applications, such that you can open files with a linked application when clicking on the file, you need to make a few additional configuration steps:

On your application server, make sure you have enabled the option **"Allow any command-line arguments"** for your RemoteApp.

If you want certain files (from the Workspace's Files tab) to be opened with this RemoteApp, mind that you will need to **specify the UNC path** for any drives you publish. See Drive Management for more details.



- **Unicode Keyboard Support**: Disable when the application (e.g. software made with Qt) does not support the Unicode Keyboard that Parallels Secure Workspace uses in the RDP Gateway. We suggest first trying with Unicode Keyboard Support enabled. However, when typing in the application results in a repetition of the first typed character or other odd behavior, then you should disable the Unicode support and try again. The advantage of Unicode Keyboard is better recognition of special characters on keyboards and the use of on-screen keyboards on tablets.
- **Color Depth:** Defines how many bits per pixel should be used. The higher the color depth, the higher the detail of the application but it will also take more processing and bandwidth. Default set at 16bpp and can be increased to 24bpp or 32bpp.
- **Start in Foreground***:* If enabled and the application auto starts at login, it will immediately be presented to the user and the workspace will be skipped.
- **Concurrent Usage**: Allow a user to open multiple instances of this application at the same time. This is enabled by default. A common use case to disable this option is for an application that accesses a predefined user-owned file, such as Microsoft Outlook (only one process can access the user's mailbox).
- **Ask for Credentials***:* A user will have to provide credentials to log in to the application. Otherwise, Parallels Secure Workspace provides the login credentials to the application server. This is useful when the Server Labels are linked to application servers that are not joined to the Microsoft Windows domain. Can only be enabled when there are no Auto Start Labels assigned.
- **Notifications:** Allow this application to send notifications to a user (default enabled). Those notifications will be shown in the sidebar as a red dot. If the application provides a relevant hover text for the systray icon, this will also be shown to the user.
- **Minimum Size**: When enabled, you can set the minimum size to be able to use this application on devices with small screens. If the visible part of the application session is smaller than this minimum size, you will be able to pan inside the session.
- **Maximum Size:** When enabled, you can set the maximum size of the application. When the browser window is bigger than the application, the application will be positioned in the top left. Can be used together with the minimum size feature to configure a fixed size for this application.

- **Alias**: Provide the Remote Application alias.
- **Context Policy Labels:** Restrict this application to only be accessible within the provided security context. The context can be configured using the mfa, network or country (2 char ISO 3166-1 alpha code) context policies labels. For network and country, you can define multiple options by using comma-separated values. When adding multiple policies, they must all be valid to be able to access the application. See the Label Management page for more information and examples.
- **Server Labels:** Server labels identify on which application servers this application is available. When a user launches this application, these labels will be used to define a list of applicable servers to connect to.
- **File Types**: Associate zero, one or multiple file types with this application for viewing or editing. See the RDP File Types property above for additional information.
- **Unicode Keyboard Support**:
  - Disable when the application (e.g. software made with Qt) does not support the Unicode Keyboard that Parallels Secure Workspace uses in the RDP Gateway. We suggest first trying with Unicode Keyboard Support enabled. However, when typing in the application results in a repetition of the first typed character or other odd behavior, then you should disable the Unicode support and try again. The advantage of Unicode Keyboard is better recognition of special characters on keyboards and the use of on-screen keyboards on tablets.

- **Color Depth:** Defines how many bits per pixel should be used. The higher the color depth, the higher the detail of the application but it will also take more processing and bandwidth. The default is set at 16bpp and can be increased to 24bpp or 32bpp.
- **Start in Foreground***:* If enabled and the application auto starts at login, it will immediately be presented to the user and the workspace will be skipped.
- **Concurrent Usage**: Allow a user to open multiple instances of this application at the same time. This is enabled by default. A common use case to disable this option is for an application that accesses a predefined user-owned file, such as Microsoft Outlook (only one process can access the user's mailbox).
- **Ask for Credentials***:* A user will have to provide credentials to log in to the application Otherwise, Parallels Secure Workspace provides the login credentials to the application server. This is useful when the Server Labels are linked to application servers that are not joined to the Windows domain. Can only be enabled when there are no Auto Start Labels assigned.
- **Notifications:** Allow this application to send notifications to a user (default enabled). Those notifications will be shown in the sidebar as a red dot. If the application provides a relevant hover text for the systray icon, this will also be shown to the user.
- **Session Merge**: When enabled, the application can be merged into an existing application session. The merge will only happen when the new application shares a number of settings with the existing applications in the session.
  - Required shared application settings:
    - Allow Session Merge enabled
    - Protocol is Remote Application
    - Same Application Server
    - Equal Recording settings
    - Equal Smartcard settings
    - Equal Unicode Keyboard Support settings
    - Ask for Credentials disabled
    - Same Context Policy labels
    - Same RDS Collection labels
  - The existing application session to the same application server must still be active (not disconnected).
  - Advantages: Applications will start faster and consume fewer resources on the application server.
  - Side effects:
    - Users will see multiple applications in the same application session when they resize or minimize one of the applications.
    - Applications that are merged will also be shown together in the list of Active Sessions in the sidebar of the user.
    - The color depth setting of the merged application will be ignored.
- **Minimum Size**: When enabled, you can set the minimum size to be able to use this application on devices with small screens. If the visible part of the application session is smaller than this minimum size, you will be able to pan inside the session.
- **Maximum Size:** When enabled, you can set the maximum size of the application. When the browser window is bigger than the application, the application will be positioned in the top left. Can be used together with the minimum size feature to configure a fixed size for this application.

Reverse Proxied Web Application

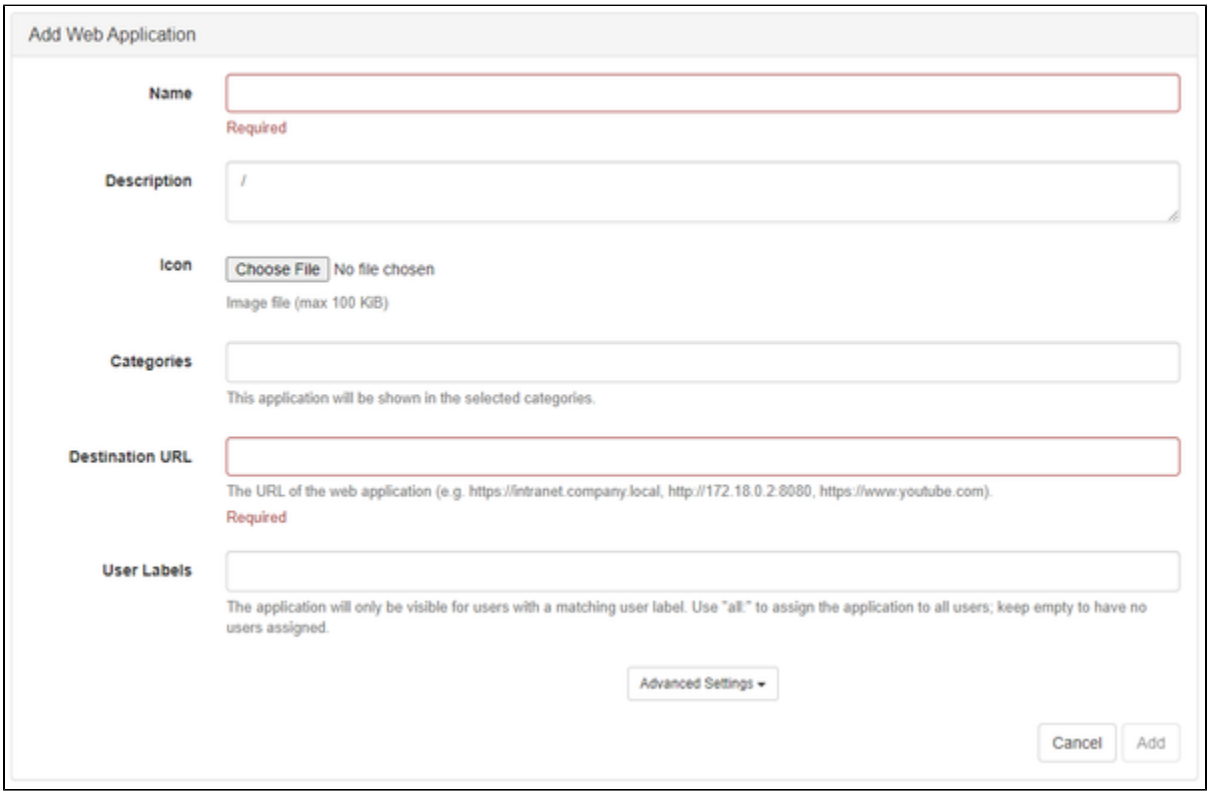
- **Destination URL:**
  Provide the internal URL of the website, which must be accessible to Parallels Secure Workspace.
  If your destination URL also contains a path (e.g. https://internal-app.somedomain.org/somepath) and you try to access the application directly instead of through the Workspace, you'd still need to specify the path as well, not just the DNS name from the source headers.
  It's possible to point to internal web applications running on a custom port as well: https://internal-app.somedomain.org:1234/somepath . Use either the FQDN or the IP address.
- **Source Host Header:** When a user opens this web application, the Source Host Header will be shown in the URL bar of their browser. This host header should resolve using DNS to the Parallels Secure Workspace environment. To increase security, it is recommended not to use a subdomain of the Parallels Secure Workspace environment (e.g. don't use intranet.workspace.company.com when workspace.company.com points to your Parallels Secure Workspace environment).
- **User Labels**: User labels are used in the process of authorizing users to applications. Only users with labels assigned in this field will see the application in the Applications tab (use *all*: to be visible for all users). See chapter on Label Management for more information.
- **Context Policy Labels:** Restrict this application to only be accessible within the provided security context. The context can be configured using the mfa, network or country (2 char ISO 3166-1 alpha code) context policies labels. For network and country, you can define multiple options by using comma-separated values. When adding multiple policies, they must all be valid to be able to access the application. See the Label Management page for more information and examples.

- **Destination Host Header:** This is the host header passed to the web application. By default, the host of the Destination URL is used. If the web application is configured to accept HTTP requests on the Source Host Header, you can use a custom host header (with the same value of the Source Host Header).
- **Rewrite Content:** Rewrite all URLs in the returned content (HTTP headers and cookies and text/html bodies) from the web application by replacing the host of the Destination URL with the specified Source Host Header. If the web application is configured to accept HTTP requests on the Source Host Header, you may need to disable this feature.
- **Single Sign-On:** If enabled, the username and password provided when logging in to Parallels Secure Workspace will be passed (base64 encoded) to the Web application in an HTTP authorization header. This requires that the Web application supports basic authentication and is hosted on a Web server with basic authentication enabled.
  - **Authentication Type:** (when Single Sign-on is enabled) defines how the user will be authenticated to the reverse proxied web application
    - Basic Auth: provide the user's credentials to the reverse proxied application using *Basic Authentication.*
    - Remote User: provide the user's username to the reverse proxied web application using the REMOTE_USER header.
  - **Username field:** (when Single Sign-on is enabled) defines the format of the username used to authenticate the user to the reverse proxied web application using the selected *Authentication Type*
    - Username: Use the username without the domain.
    - Domain username: Use the username prefixed with the domain (e.g. NETBIOS\username).
    - Upn: Use the UPN of the user as the username.

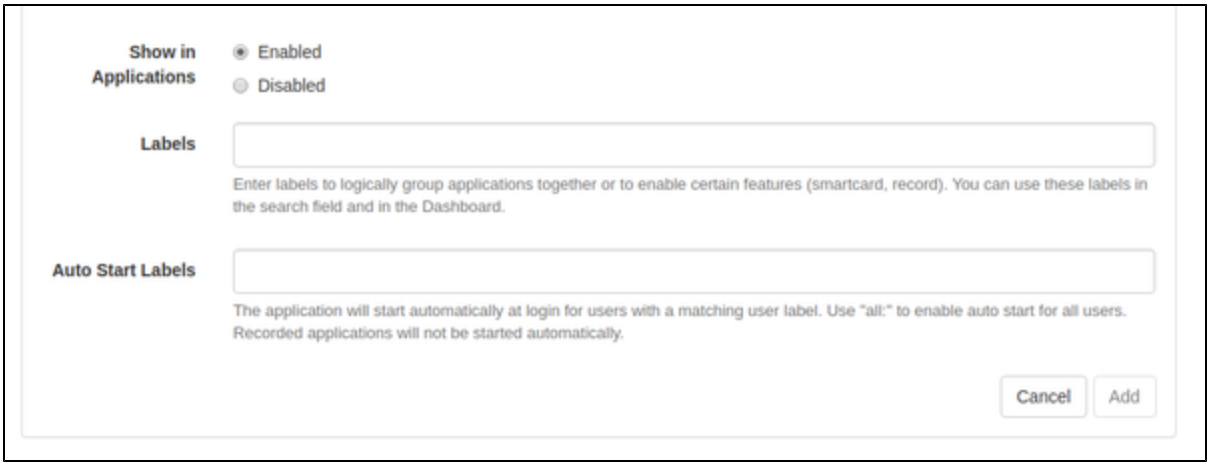
Support

- Built-in Reverse Proxy: Rewrite of host headers only works if the URL is clearly present in the body or the headers. If it is not easily replaceable (for example because it is encoded, escaped or split), it will not work.
- Unable to make Cross Origin Requests to grouped reverse proxied web applications.
- WebSockets in reverse proxied web applications are supported.

Web Application



- **Destination URL:** Provide the URL on which the website is reachable for the end-user. Make sure the end-user is able to access it.



Importing applications with a CSV file

When importing a CSV (comma-separated value) file, you can add multiple applications at once. Only RemoteApp is supported.

The CSV file is formatted as follows:

```
"command","name","icon"
"EXCEL","Microsoft Excel 2010","0,0,1,0,5....."
```

Generating a CSV file

Via a PowerShell script, you can run a script to gather all published RemoteApps on an application server.

1. We provide a sample script on our public GitHub account: https://github.com/Awingu/awingu-utils/blob/master/RemoteApp/PowerShell/get_remoteapps_from_appserver.ps1 .
   You can download that script with right-click on the Raw button and save the link content.
2. To run the script, which is not signed, you can open PowerShell and execute:

   ```
   powershell -ExecutionPolicy ByPass -File .
   \get_remoteapps_from_appserver.ps1
   ```

3. The script generates the folder Workspace_Apps in the current working directory containing the CSV file that can be imported in Parallels Secure Workspace.

Importing a CSV file

When importing from file, you can configure for all imported applications following fields:

- Categories
- File Types
- Labels
- Server Labels
- User Labels
- Context Policy Labels
- Auto Start Labels
- Unicode Keyboard Support
- Show in Applications
- Notifications

See Adding applications manually for more details about those fields. You can always update the afterwards (via Bulk Action).

Configuring shortcut buttons

For each streamed application, an administrator can configure shortcut buttons that will be provided in a shortcut toolbar to the end user.

Click on the Shortcut Buttons button next to the application name in the list of applications.

Click on Add to create a new key combination:

- **Name**: the text shown on the shortcut button, e.g. Save, Refresh, Next page
- **Key Combination**: text representing the key combination in one of the following formats:
  - modifier + key
  - modifier + modifier + key
  - modifier + modifier + modifier + key

Possible modifiers:

- ctrl
- shift
- alt
- altgr
- windows
- context

Possible keys:

- f1 - f12
- a - z
- 0 - 9
- space
- pageup, pagedown
- end, home
- left, up, right, down
- printscreen
- insert
- delete
- esc
- backspace
- tab
- enter

Note: The Remote Desktop Services Shortcut keys are also available in Parallels Secure Workspace. See the User Manual for an overview.

Application Server Management

Introduction

When an end-user launches a streamed application, a session is set up dynamically between the Parallels Secure Workspace appliance and an application server.

The Application Connector (a component within Parallels Secure Workspace) will select the application server (hostname and port) that should be used to set up this connection.

In a typical Parallels Secure Workspace environment, there are multiple application servers deployed. An application can be served by one or more application servers. However, it is by no means required that each application is installed on every application server.

It is the role of the Application Connector to find the most-suited application server to launch a particular application at a certain moment in time. The default behavior is:

1. List all application servers where the application is available (based on server labels).
2. Select the server that has the least open connections (Only the open connections from Parallels Secure Workspace to the application servers are considered).
3. If a server is not reachable, another server from step will be selected.

When using a Remote Desktop Service Connection Broker (RDS farm), the broker will do the load balancing.

Note: the application servers need to be configured correctly before any streamed application can be opened. Please refer to Integrating with existing Microsoft Windows environment.

Adding/Configuring Application Servers

Application servers can be added via System Settings > Manage > Application Servers.

Importing application servers

When the bind user has been configured for the domain (see Domain Settings), you can import them by clicking on **Import from AD** and scrolling down.

Note: All application servers that are available in the top-level domain will be shown. Only domain components (dc=) of the Base DN are used.

1. First, select the servers to import. You can use the search box.
2. Configure the servers to import:
   - **Port**: TCP port used to set up the RDP session to the application server (default 3389).
   - **State**: When this attribute is set to 'disabled', no new sessions will be set up to this application server. Toggling from 'enabled' to 'disabled' does not impact active sessions.
   - **Max Connections**: Maximum number of simultaneously active RDP sessions that are allowed to this application server. In case this maximum is reached, no new sessions will be set up to this application server. Note: 0 (zero) results in an unlimited number of connections.
   - **Server Labels**: Add labels to servers to group them. These groups can be used to assign applications (see also Application Management) to servers and to filter application servers in lists and reports.
   - **Authentication Protocol**: Determines which authentication protocol will be used when connecting to the application server (default NTLM). Normally when selecting Kerberos, you need to provide an authentication host but when you are importing application servers, the authentication host will be set to the host name.

Manually adding/editing application servers

The following attributes can be configured per added application server:

- **Name**: Name of the application server that will be visible in the application connector
- **Host**: Fully qualified domain name or IPv4 of the application server
- **Port**: TCP port used to set up the RDP session to the application server (default 3389).

- **State**: When this attribute is set to 'disabled', no new sessions will be set up to this application server. Toggling from 'enabled' to 'disabled' does not impact active sessions.
- **Max Connections**: Maximum number of simultaneously active RDP sessions that are allowed to this application server. In case this maximum is reached, no new sessions will be set up to this application server. Note: 0 (zero) results in an unlimited number of connections.
- **Description**: Description of the application server (free text format)
- **Server Labels**: Add labels to servers to group them. These groups can be used to assign applications (see also Application Management) to servers and to filter application servers in lists and reports.
- **Authentication Protocol**: Determines which authentication protocol will be used when connecting to the application server (default NTLM). When Kerberos is selected, an **Authentication Host** (FQDN) of the application server is required.

Further Configuration of the Applications

Please refer to Application Management to assign applications to servers and assign applications to users.
This page will also allow you to add applications to categories, define the command that needs to be executed, etc.

Remote Desktop Connection Broker

When using the Microsoft Remote Desktop Connection Broker, only the broker needs to be configured in Parallels Secure Workspace. This RD Connection Broker will refer Parallels Secure Workspace to the correct application server when opening an application. This means that in the Dashboard, the **broker** that Parallels Secure Workspace **initially** connects to will be listed. However, the remote desktop session might end up running on a different RD Session Host.

In this scenario, it's also the Microsoft RD Connection Broker that load balances the RDP connections between the available RD Session Hosts.

1. Navigate to **System Settings > Manage > Labels**.
   Create a label for each RDS Collection configured on the Broker:
   - Key: ***rdscollection***
   - Value: The name of the collection. Mind the pointers below.
2. Navigate to **System Settings > Manage > Application Servers.**
   Add the Broker as an application server. In the *Server Labels* field, add the **rdscollection** labels defined in the previous step.
3. Navigate to **System Settings > Manage > Applications.**
   In the application's settings, find *Server Labels.* Use the **rdscollection** labels configured in the first step to assign applications to the session collections in which they are published.

Name of the session collection

Even when the name of an RDS collection has changed at some point, the original name of the collection must still be specified in Parallels Secure Workspace. This is because Microsoft Windows Server does not change its collection name internally. To retrieve the original collection name, there are a few options:

- Check the Windows registry on `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\CentralPublishedResources\PublishedFarms\<CollectionName>`
- Check the following folder: `C:\Windows\RemotePackages\CPubFarms\<CollectionName>`
- Download an RDP file via RDWeb and open it in Wordpad. One of the lines is: `loadbalanceinfo:s:tsv://MS Terminal Services Plugin.1.<CollectionName>`

Additionally:

- If the name of the session collection is longer than 15 characters, it must be truncated to 15 characters.
- If the name of the session collection contains spaces, these must be converted to underscores (_). For example, the name "App Zone A" becomes "App_Zone_A".
- If the name of the session collection contains dots, the dots must be removed. For example, the name "App.Zone.A" becomes "AppZoneA".

High availability

High availability means that end users should still be able to start new remote application sessions, even when one or more servers go down.

It may however take a short period of time before the failover is fully functional.

Existing application sessions will not be resumed.

Microsoft RD Connection Broker

In this scenario, there are at least two Microsoft Windows servers acting as a **RD Connection Broker**; They point to the same (high-available) SQL database and there's a DNS name for this RD Connection Broker cluster. Only one of those servers is the **RD Management Server (rdms)**. If the management server goes down, a remaining broker automatically takes over this role after a couple of minutes.

Microsoft offers two ways to connect to this high-available environment:

1. By using a **load balancer**. The load balancer is responsible to check whether a server with the RD Connection Broker is reachable. It should also distribute the connections evenly.
2. By using a **round-robin DNS record.** For the DNS name of the RD Connection Broker cluster (for example rdcb.somewindowsdomain.org), multiple IP addresses can be resolved.

Once high availability is properly configured on the Microsoft side, it's time to configure Parallels Secure Workspace.

Configuration in Parallels Secure Workspace

The configuration in Parallels Secure Workspace is based on the first approach. Parallels Secure Workspace acts as a load balancer.
For each RD Connection Broker in the cluster, an application server should be added in Parallels Secure Workspace with the proper **rdscollectior** label assigned to it.
The IP address or FQDN of the individual server should be used as hostname. Do **NOT** use the DNS name of the cluster.

Also, ensure high availability for the Parallels Secure Workspace cluster by setting up a redundant multi-node environment.

Which broker will Parallels Secure Workspace connect to?

When a user launches an application with a rdscollection label attached to it, Parallels Secure Workspace builds a list of candidate servers. In this case, this would be the list of the RD Connection Brokers (application servers in Parallels Secure Workspace) with the same rdscollection label as assigned to the application. Parallels Secure Workspace checks if the RD Connection Broker to which it has the least open connections is reachable and tries to connect to this host. If this broker is unreachable, it tries connecting to the next candidate.

When session merge is enabled, Parallels Secure Workspace also tries to re-use an existing prior connection if available.

Good to know

Sometimes, some administrators opt to define specific RD Session Hosts as an application server in Parallels Secure Workspace (using the **apps erver** label). However, if those RD Session Hosts are managed by a Microsoft RD Connection Broker, it's possible the user ends up on a different RD Session Host anyway.

To prevent this, there is a Microsoft Windows group policy to disable participating in this load-balancing behavior on the Microsoft RDS environment: *Computer Configuration / Administrative Templates / Windows Components / Remote Desktop Services / Remote Desktop Session Host / RD Connection Broker / Use RD Connection Broker Load Balancing*: set to **disabled**.

Drive Management

Introduction

Parallels Secure Workspace provides the user with access to file server back ends: CIFS, WebDAV and OneDrive for Business. Browsing files is implemented as a series of REST API calls to the Parallels Secure Workspace platform infrastructure. These REST API calls are proxied to another protocol that is supported by the drive back end. Creating, renaming, moving, copying, uploading and downloading files is also possible. Files can also be opened with configured streamed applications (except when using OneDrive): in this case, the application server will mount the user's drive and open the application with the specified file.

Supported protocols

The current release of Parallels Secure Workspace supports the following protocols:

- CIFS with support for:
  - SMB2 and SMB3 (basic) for Windows Server.
  - Samba3 server
- WebDAV with support for:
  - IIS for Windows Server with a minimum requirement of WebDAV class 2.
- Microsoft OneDrive for Business (see link for step-by-step instructions to set up). Note that for OneDrive back ends, the user cannot select "Open with" with a streamed application.

From an end-user perspective, there is no noticeable difference in behavior between the different types of back ends: the same file navigation rules apply to both. It is also possible to move/copy files and directories across file storage back ends.

It is technically possible to create 2 different drives mapping to the same back end, e.g.:

- Drive "Shared folder" maps to smb://file-server.company.com/Shared/
- Drive "Project folder" maps to smb://file-server/company.com/Shared/Sales/Common/Projects/

In this peculiar case, when an end-user **moves** a file/folder from "Shared folder > Sales > Common > Projects" to "Project folder", Parallels Secure Workspace does not take into account this maps on the same folder. The Workspace will ask whether to overwrite the moved file/folder, resulting in the file/folder to be deleted (because a move is a copy-overwrite followed with a delete of the original file).

Notes:

- SMB 3.0 Transparent Failover is not yet supported.
- Limited support for Distributed File System (DFS), branching/DFS namespace is not yet supported.

Adding/editing drives

Drives are configured to allow end users accessing file servers via a web-based file manager. Authorization to drives is done in a similar way as configuring authorization to applications, by means of labels.

- **Name**: Name of the drive as it will be displayed in the Workspace (end-user interface), in the left pane of the Files tab.
- **Description**: Free text description of the drive.
- **Backend**: Protocol through which the Parallels Secure Workspace API will communicate with the file server back end. Supported protocols:
  - CIFS: also called SMB or Samba
  - WebDAV
  - Microsoft OneDrive For Business. More details here.
- **Client ID**: (only for OneDrive) Client ID (Application ID) of your configured OneDrive Parallels Secure Workspace app in Azure.
- **Client secret**: (only for OneDrive) secret created when adding your OneDrive Parallels Secure Workspace app to Azure
- **Workspace URL**: (only for OneDrive) the URL a user uses to access Parallels Secure Workspace, e.g. https://workspace.mycompany.com
- **Redirect URL**: (only for OneDrive) (read/only) URL to use to configure your OneDrive Parallels Secure Workspace app in Azure.
- **URL**: URL of the file server that will be used by the Parallels Secure Workspace API to communicate with the file server.
  Note that this URL can be parameterized with:
  - **<username>**: the user's username
  - **<domain>**: the name of the domain the user is part of

  URL needs to be based on FQDN name, not NetBIOS.
  Examples:
  - SMB: `smb://file-server.stack.mycompany.com/home/<username>/Documents`
  - WebDAV: `http://file-server.stack.mycompany.com:8080/home/<username>/Documents`

- OneDrive: link to your sharepoint.com environment: `https://mycompany.sharepoint.com` . Note that you should **not** specify a URL with “-my” here; this will result in an error message about too many redirects.

- **UNC**: UNC that will be used by the application server to access the drives. This UNC path is needed when using "Open with" as action on the Files tab in Parallels Secure Workspace.
  Note that this URL can be parameterized with:
  - **<username>**: the user's username
  - **<domain>**: the NETBIOS name of the domain the user is part of
    Example:

    ```
    \\file-server\Home\<username>\Documents
    ```

    UNC needs to be based on NETBIOS name, not FQDN.

  If no UNC path is provided, you can only "Open with" preview (if available).
- **Domain Use**: (only for WebDAV) During authentication against the WebDAV file server, it may be required to pass the domain name. This depends on the configuration of the WebDAV file server. If required, check the box **Use Domain** in Parallels Secure Workspace. This option is ignored in case of a CIFS file server back end.
- **Authentication Role:** (only for CIFS) Defines how to authenticate with the CIFS server
  - User: authenticate as the user accessing the drive.
  - Anonymous: authenticate as an anonymous user (should be enabled on the CIFS server).
- **Labels**: Assign labels to drives to create groups of drives. These groups can be used to select, filter, and report on drives.
- **User Labels**: By assigning user labels to drives, you can grant groups of users access to drives. Only users in user groups assigned to a label will see the drive in the Files tab (use *all*: to be visible for all users). For more information on labels, please consult the section Label Management.
- **Context Policy Labels:** Restrict this drive to only be accessible within the provided security context. The context can be configured using the mfa, network or country (2 char ISO 3166-1 alpha code) context policies labels. For network and country, you can define multiple options by using comma separated values. When adding multiple policies, they must all be valid to be able to access the drive. See the *Label Management* page for more information and examples.

Security

Parallels Secure Workspace acts as a client to the file server. If there is a need to scan uploaded files for malware or block certain file extensions, this should be managed by the file server. This also simplifies management.

File Type Management

Introduction

File types are the way to link a file on the Workspace Files page to a configured Application. If multiple applications are associated with a file type, the user can choose which one to use.

A selection of commonly used file types is already configured in Parallels Secure Workspace at install time.

Linking Application (or preview action) to a file type.

When opening files in the Workspace, the file type of the file is inspected to determine which applications can be used to open the file.

Four parameters are used to define a file type:

- **File Extension**: This is the part of the file name after the leading dot.
- **Description**: Free text description.
- **Icon**: Icon used to represent the given file type on the Files page in the Workspace.
- **Apps**: List of applications that can be used to read or modify this file type.

Introduction

Labels in Parallels Secure Workspace serve different purposes, There are 4 types of labels.

- **User Labels:** Assign applications, drives or features to users or groups.
- **Server Labels:** Assign applications to application servers.
- **Labels:** Attaching a label to applications or drives allows you to use this label when filtering or querying in the *System Settings* or *Dashboard*.
- **Context Policy Labels:** Define context requirements for applications, drives, features, login, or the admin role.

Note: Creating labels can be done on the *Manage* > *Labels* page of the *System Settings* or it can also be created on the fly when configuring a resource.

User Labels

User labels are used to assign applications, drives, or features to users. Each time a user signs in, labels are assigned to the user based on their LDAP properties. If you add those labels to applications, drives or features; users with the matching labels will have access to these applications or drives, or will have this feature enabled.

User Labels need to be created manually or imported (see below). They are not automatically created from the LDAP properties of the logged-in users.

Key	Value	Comments
group	<the name of the security group>*	Custom made user label. Per security group you want to filter on in Parallels Secure Workspace, an entry with *group* key needs to be made. You can use *Import groups from AD* to find user groups to auto-generate the labels.
username	<username in DOMAIN\username format>*	Custom made user label. Per user name you want to filter on in Parallels Secure Workspace, an entry with *username* key needs to be made. You can use *Import users from AD* to find user groups to auto-generate the labels. ⚠ The domain should be entered in uppercase and username should be entered in lower case, e.g. MYDOMAIN\johndoe
upn	<username in username@fqd-for-upn format>*	Custom made user label. Per user name (via UPN) you want to filter on in Parallels Secure Workspace, an entry with *upn* key needs to be made.
ou	<the name of the organizational unit>*	Custom made user label. Per OU you want to filter on in Parallels Secure Workspace, an entry with *ou* key needs to be made.
all	(empty)	Predefined user label. Do not remove. When this label is attached to a drive/app/feature, all users from that domain, can access that drive/app/feature.
admin	(empty)	Predefined user label. Do not remove. This label corresponds with the groups indicated as *admin* in the User Connector Configuration.
record	(empty)	Predefined label. Do not remove. Add as label to an application (RDP and RemoteApp) to activate application session recording (needs to be enabled).
smartcard	(empty)	Predefined label. Do not remove. Add as label to an application (RDP and RemoteApp) to enable Smart Card Redirection.

state	enabled	Predefined user label. Do not remove (system label).

* To look-up the *ou*, *group*, *username* or *upn* of users that have already signed in on Parallels Secure Workspace, navigate to Manage > Users: select a user to show the properties, including the labels.

⚠ When assigning user labels it needs to be taken into account that the labels are case sensitive.

Importing Labels

To auto-create *group* and *username* labels, you can use the buttons *Import groups from AD* and *Import users from AD*. To be able to use this feature, the bind user needs to be configured in Domain Settings .

When clicking on the button, the groups/users are listed.

You can then use the search box to filter. Select the desired groups/users and click on Import.

Example of Use of User Label

We have following AD configuration:

- ou:Europe
  - group:Engineering
  - group:Europe Managers
- ou:America
  - group:Accountancy
  - group:HR
  - group:America Managers
- ou:Global
  - group:Administrators

In User Connector Configuration, we have for this domain:

Domain Administrators	group:Administrators

In Label Management, we have added following rows:

Key	Value
ou	Europe
ou	America
group	Engineering
group	Europe Managers
group	Accountancy
group	HR
group	America Managers

In Drive Management, we have added following user labels to the drives:

Drive	Labels
Home Drive	all:
Engineering Drive	group:Engineering
Accountancy Drive	group:Accountancy
Managers Drive	group:Europe Managers group:America Managers
Administrators Drive	admin:

In Application Management, we have added following User labels to the applications:

Application	Labels
Microsoft Word	all:
AutoCad	group:Engineering
Finance Explorer	group:Accountancy
Cost Calculator	group:Engineering group:Accountancy
Euro Specs	ou:EMEA group:HR
Network Manager	admin:

This results in this overview of rights:

Domain\user and security groups	Available applications	Available drives
John: ou: Europe groups: Engineering, Europe Managers	- Microsoft Word - AutoCad - Cost Calculator - Euro Specs	- Home Drive - Engineering Drive - Managers Drive
Lucy: ou: Europe groups: Engineering	- Microsoft Word - AutoCad - Cost Calculator - Euro Specs	- Home Drive - Engineering Drive
Maria: ou: Europe groups: Administrators	- Dashboard* - System Settings* - Recorded Session Player* - Microsoft Word - Network Manager - Euro Specs	- Home Drive - Administrators Drive
Kim: ou: America groups: Accountancy, America Managers	- Microsoft Word - Finance Explorer - Cost Calculator	- Home Drive - Accountancy Drive - Managers Drive
Patrick: ou: America Groups: HR, America Managers	- Microsoft Word - Euro Specs	- Home Drive - Managers Drive

* pre-installed system application

Server labels

To assign applications to application servers, both the application server and the applications need to have a label in common.

Key	Value	Comments
rdscollection	<the name of the RDS collection>	Custom made server label. See Remote Desktop Service Connection Broker for more information.
<any key>*	<any value>	Custom made server label. Any key* and value can be used to link applications with application servers.

* Any key, except the reserved ones defined in this document.

Labels

All labels can be used for filtering in search boxes and reporting tools. Server and user labels can be used for that purpose, too.

Key	Value	Comments
smartcard	(empty)	Predefined label. Do not remove. See Smart Card Redirection for more information.
audioinput	(empty)	Predefined label. Do not remove, nor use (system label).

<any key>*	<any value>	Custom made label. Any key* and value can be used to filter.

* Any key, except the reserved ones defined in this document.

Context Policy Labels

These labels allow you to define what security context is required to perform these actions:

- Access an application or drive.
- Use a feature.
- Login.
- Have the admin privileges.

We support 3 types of context labels.

- **country**: The value of this label accepts a single or a comma separated list of 2 char ISO 3166-a alpha codes. See https://en.wikipedia.org/wiki/ISO_3166-1 for a full list. E.g. 'country:BE' or 'country:BE,NL'
- **network:** The value of this label accepts both a single IP address (e.g. 'network:172.16.0.15') or a subnet (e.g. 'network:172.16.0.0/8'). Multiple networks or IP addresses can be added using a comma-separated list.
- **mfa:required**: This label is automatically created. When Multi-Factor Authentication is not required at login, a dialog will be shown explaining the user he will need to re-login and use MFA to access an application, drive or feature,

When combining different types of context labels, they must all be valid before the user has access to the resource,

E.g. The Context Policy Label 'country:BE,NL mfa:required' means that the users will have access to the resource if their IP address comes from Belgium or the Netherlands AND they logged in using Multi-Factor Authentication.

User Management

The System Settings allow administrators to list and filter users. Administrators can also consult more detailed information about a user such as:

- First login date.
- Last login date.
- Labels that have been assigned to this user.
- Email address.
- Configured locale and keyboard layout.

Except for the Keyboard Layout and Locale setting, all parameters are dynamically populated in the database when a user signs in to the platform, based on information retrieved from the enterprise authentication infrastructure (AD/LDAP), see also the section User Connector Configuration .

To log out users and close their application session, please refer to Live Monitoring of Users Activity .

Deleting users

Users can be deleted from Parallels Secure Workspace, but as long they exist in an authorized user group on the AD/LDAP, they will be able to sign in again.

Depending on the license type, deleted users will still be shown until the end of the month (the Deleted column will have a checkmark) or they will be deleted immediately.

System Settings - Change Log

For auditing reasons, all changes are logged and kept for 13 months. This applies both to changes done in the System Settings web interface as well as through the REST API.

If you are an admin of an administrative domain (global admin) or logged in with the Management User (set up during installation):

- You can select the domain you want to see the changes of with the domain drop-down on the top left.
- You can see all global changes, regardless of the selected domain.

If you are a domain admin (non-administrative domain), you will only see changes of your domain. You can export the queried results to a CSV file.

You can filter and list the changes for following fields:

- **Action**: Create / Delete / Update.
- **Resource type**: Those are the resources used in the REST API. They mostly map with the corresponding pages of the System Settings.
- **Resource Id**: This is typically the name of the resource, e.g. name of the application, user group, label, etc.
- **User**: User who performed the change.
- **Authentication:** Whether a session (username/password) or API token (see User Connector Configuration) has been used.
- **Timestamp**: Date and time when the change was made.

When clicking on a change in the list, the body of the REST API request and response is shown, even when the change has been done trough the web interface. Example for action *Update*, resource type *Contact*, the change log when editing the phone number of the partner on the General Info page:

- Request:

```
{
    "phoneNumber": "+9876543210"
}
```

- Response:

```
{
    "name": "My Partner",
    "location": "East-Flandres",
    "uri": "http://172.16.5.65/api/v2/contacts/1/",
    "city": "Ghent",
    "phoneNumber": "+9876543210",
    "addressLine1": "Some street 1",
    "country": "Belgium",
    "postalCode": "9000",
    "addressLine2": ""
}
```

Service Provider Support in Parallels Secure Workspace

Introduction

Parallels Secure Workspace allows service providers to give access to applications and documents to their customers in a secure way.

We will describe 5 possible use cases below. In this table, a Workspace environment refers to a single-node or multi-node deployment of Parallels Secure Workspace.

	Number of Workspace environments	Number of Workspace domains	Number of Microsoft Windows domains	Branding per customer
1	One	One	One	No
2	One	Multiple (one per customer)	One	Yes
3	One	Multiple (one per customer)	Multiple (one per customer)	Yes
4	Multiple (one per customer)	One per Workspace	One	Yes
5	Multiple (one per customer)	One per Workspace	Multiple (one per customer)	Yes

A service provider can combine those use cases, e.g. 1 Workspace environment for multiple small customers and multiple Workspace environments for some of the bigger clients.

For automatic configuration, an API is available (see Automate Parallels Secure Workspace via the REST API).

When using a multi-node high available deployment, we strongly recommend doing the SSL offloading at the load balancer.

Case 1: One environment / One Workspace Domain / One Microsoft Windows Domain

Architecture

Access to Parallels Secure Workspace:

- All customers access Parallels Secure Workspace using the same URL, e.g. https://www.provider.com
- All customers will see the same branding.

For the Parallels Secure Workspace topology, the following is required:

- Multi-node setup (for +100 concurrent users)..
- External load balancing (for high availability or +200 concurrent users).
- External database (for high availability or +200 concurrent users).

The Microsoft Windows architecture:

- Only 1 domain with one or multiple domain controllers, file servers and application servers.

- The users of a customer are grouped in the same organizational unit (OU) or security group.

Licensing

Only 1 Parallels Secure Workspace license is needed for the desired number of maximum concurrent users.

Configuration

- System Settings > Global > Domain:
  - Define 1 domain.
  - This domain should be an *Administrative domain*.
  - Provide a bind user to allow import.
- System Settings > Configure > User Connector:
  - Define the group(s) that need administrator rights
  - Assign the *Admin* user group label to it
- System Settings > Manage > Labels:
  - In case customers are grouped per OU: create a label per customer:
    - Key: *ou*
    - Value: the name of the OU (case sensitive)
  - In case customers are grouped per security group: use *Import groups from AD*
- System Settings > Manage > Application Servers: define or import the application servers for that domain.
- System Settings > Manage > Applications: define the applications and limit the usage per customer with the ou/group labels.
- System Settings > Manage > Drives: define the drives and limit the usage per customer with the ou/group labels.
- System Settings > Configure > Features: you can limit some features per customer with the ou/group labels.
- System Settings > Configure > Branding: you can only define one branding.

Administration

Only the service provider will be able to manage Parallels Secure Workspace . There is no multi-tenancy in this case.

Case 2: One environment / Multiple Workspace Domains / One Microsoft Windows Domain

Architecture

Access to Parallels Secure Workspace:

- You can define multiple DNS entries pointing to Parallels Secure Workspace in order to give each customer their own URL, e.g. https://customer1.provider.com.
  If you access Parallels Secure Workspace using an unknown host header (or via IP address), you can enter your domain manually at the login page. If not provided, the default domain will be used.
- You can define branding for each customer.

For the Parallels Secure Workspace topology, the following is required

- Multi-node setup (for +100 concurrent users).
- External load balancing (for high availability or +200 concurrent users).
- External database (for high availability or +200 concurrent users).

The Microsoft Windows architecture:

- Only 1 domain with one or multiple domain controllers, file servers and application servers.
- The users of a customer are grouped in the same organizational unit (OU) or security group.

Licensing

Only 1 Parallels Secure Workspace license is needed for the desired number of maximum concurrent users. You can limit the number of concurrent users per domain.

Configuration

- System Settings > Global > Domain:
  - Define a domain for the employees of the service provider. That domain should be an *Administrative Domain* and should be the *Default* domain.

- Define 1 domain per customer. Those domains should **not** be *Administrative Domains*. The *NetBIOS Name* is the same for each customer, but the *Name* is different.
- Per customer domain: provide the Host Header, e.g. customer1.provider.com
- Per customer domain: provide a bind user to allow import.
- Per customer domain: define the maximum concurrent users, if desired.
- In case customers (or the employees of the service provider) are grouped per OU: limit access via the *Base DN*, e.g. "ou=Customer 1, dc=provider,dc=com"

- Per Domain (select via the top left):
  - System Settings > Configure > User Connector:
    - User Groups:
      - In case customers (or the employees of the service provider) are grouped per security group:
        - Define the group which should have access.
      - Define the group which needs administrator rights:
        - For the domain of the service provider: members of that group can manage all domains and the global settings. Those are Global Admins.
        - For the domain of a customer: members of that group can manage the domain (applications servers, applications, drives, features, branding, etc). As all customers share the same Microsoft Windows domain, it is not recommended to allow customers themselves to manage their domain. It makes more sense that the assigned solution engineers of the service provider are managing the domain. Those are Domain Admins.
    - User Group Labels:
      - Assign the *Admin* label to the defined administrator group
  - System Settings > Manage > Application Servers: define or import the application servers for that domain.
  - System Settings > Manage > Applications: define the applications for that domain.
  - System Settings > Manage > Drives: define the drives for that domain.
  - System Settings > Configure > Features: you can limit some features for that domain.
  - System Settings > Configure > Branding: you can define the branding for that domain.

Administration

Global Admins:

- Are the members of the Admin group defined for the domain of the service provider.
- Can manage all domains and global settings.

Domain Admins:

- Are the members of the Admin group defined for a customer domain.
- Can only manage applications, drives, features, branding etc. of that customer.

The Dashboard is only available for Global Admins.

Case 3: One environment / Multiple Workspace Domains / Multiple Microsoft Windows Domains

Architecture

Access to Parallels Secure Workspace:

- You can define multiple DNS entries pointing to Parallels Secure Workspace in order to give each customer their own URL, e.g. https://customer1.provider.com.
  If you access Parallels Secure Workspace using an unknown host header (or via IP address), you can enter your domain manually at the login page. If not provided, the default domain will be used.
- You can define branding for each customer.

For the Parallels Secure Workspace topology, the following is required

- Multi-node setup (for +100 concurrent users).
- External load balancing (for high availability or +200 concurrent users).
- External database (for high availability or +200 concurrent users).

The Microsoft Windows architecture:

- Each customer has their own domain with one or multiple domain controllers, file servers and application servers.
- The employees of the service provider will typically have their own domain, too.

Licensing

Only 1 Parallels Secure Workspace license is needed for the desired number of maximum concurrent users. You can limit the number of concurrent users per domain.

Configuration

- System Settings > Global > Domain:
  - Define a domain for the employees of the service provider. That domain should be an *Administrative Domain* and should be the *Default* domain.
  - Define 1 domain per customer. Those domains should **not** be *Administrative Domains*. The *NetBIOS Name* will be typically equal to the *Na me* of the domain.
  - Per customer domain:
    - Provide the Host Header, e.g. customer1.provider.com . This is the host header for the Parallels Secure Workspace for this customer.
    - Prrovide a bind user to allow import users from the LDAP server.
    - Define the maximum concurrent users, if desired.
- Per Domain (select via top left):
  - System Settings > Configure > User Connector:
    - User Groups: define the group which needs administrator rights:
      - For the domain of the service provider: members of that group can manage all domains and the global settings. Those are Global Admins.
      - For the domain of a customer: members of that group can manage the domain (applications servers, applications, drives, features, branding, etc). Typically, members of that domain are the IT administrators of the customers and/or the solution engineers of the service provider. Those are Domain Admins.
    - User Group Labels:
      - Assign the *Admin* label to the defined administrator group
  - System Settings > Manage > Application Servers: define or import the application servers for that domain.
  - System Settings > Manage > Applications: define the applications for that domain.
  - System Settings > Manage > Drives: define the drives for that domain.
  - System Settings > Configure > Features: you can limit some features for that domain.
  - System Settings > Configure > Branding: you can define the branding for that domain.

Administration

Global Admins:

- Are the members of the Admin group defined for the domain for the service provider.
- Can manage all domains and global settings.

Domain Admins:

- Are the members of the Admin group defined for a customer domain.
- Can only manage applications, drives, features, branding etc. of that customer.

The Dashboard is only available for Global Admins.

Case 4: Multiple environments / One Workspace Domain per Parallels Secure Workspace / One Microsoft Windows Domain

Architecture

Access to Parallels Secure Workspace:

- Each Parallels Secure Workspace environment has its own IP address and DNS entry. Each customer has their own URL, e.g. https://custom er1.provider.com.
- You can define branding for each Parallels Secure Workspace.

For the Parallels Secure Workspace topology, the following is required

- Multi-node setup for each customer with +100 concurrent users.
- External load balancing for each customer requiring high availability or +200 concurrent users.
- External database for each customer requiring high availability or +200 concurrent users. The same database server(s) can be shared for multiple customers.

The Microsoft Windows architecture:

- Only 1 domain with one or multiple domain controllers, file servers and application servers.
- The users of a customer are grouped in the same organizational unit (OU) or security group.

Licensing

You need an Parallels Secure Workspace license for each Parallels Secure Workspace (customer), each one for the desired number of maximum concurrent users.

Configuration

- Per Parallels Secure Workspace environment:
  - System Settings > Global > Domain:
    - Define 1 domain.
    - This domain should be an *Administrative domain*.
    - Provide a bind user to allow import.
    - In case customers are grouped per OU: limit access via the *Base DN*, e.g. "ou=Customer 1,dc=provider,dc=com"
  - System Settings > Configure > User Connector:
    - User Groups:
      - In case customers are grouped per security group:
        - Define the group which should have access.
      - Define the group which needs administrator rights: members of that group can manage that environment. As all customers share the same Microsoft Windows domain, it is not recommended to allow customers themselves to manage their environment. It makes more sense that the assigned solution engineers of the service provider are managing the environment.
    - User Group Labels:
      - Assign the *Admin* label to the defined administrator group
  - System Settings > Manage > Application Servers: define or import the application servers for that environment.
  - System Settings > Manage > Applications: define the applications for that environment.
  - System Settings > Manage > Drives: define the drives for that environment.
  - System Settings > Configure > Features: you can limit some features for that environment.
  - System Settings > Configure > Branding: you can define the branding for that environment.

Administration

Each Parallels Secure Workspace environment can be fully managed by the members of the Admin group defined for each environment.

Case 5: Multiple environments / One Workspace Domain per Parallels Secure Workspace / Multiple Microsoft Windows Domains

Architecture

Access to Parallels Secure Workspace:

- Each environment has its own IP address and DNS entry. Each customer has their own URL, e.g. https://customer1.provider.com.
- You can define branding for each Parallels Secure Workspace.

For the Parallels Secure Workspace topology, the following is required

- Multi-node setup for each customer with +100 concurrent users.
- External load balancing for each customer requiring high availability or +200 concurrent users.
- External database for each customer requiring high availability or +200 concurrent users. The same database server(s) can be shared for multiple customers.

The Microsoft Windows architecture:

- Each customer has their own domain with one or multiple domain controllers, file servers and application servers.

Licensing

You need an Parallels Secure Workspace license for each Parallels Secure Workspace (customer), each one for the desired number of maximum concurrent users.

Configuration

- Per Parallels Secure Workspace environment:
  - System Settings > Global > Domain:
    - Define 1 domain.

    - This domain should be an *Administrative domain*.
    - Provide a bind user to allow import.
- System Settings > Configure > User Connector:
    - User Groups: define the group which needs administrator rights. Members of that group can manage that environment. Typically, members of that domain are the IT administrators of the customers and/or the solution engineer(s) of the service provider.
    - User Group Labels: assign the *Admin* label to the defined administrator group
- System Settings > Manage > Application Servers: define or import the application servers for that environment.
- System Settings > Manage > Applications: define the applications for that environment.
- System Settings > Manage > Drives: define the drives for that environment.
- System Settings > Configure > Features: you can limit some features for that environment.
- System Settings > Configure > Branding: you can define the branding for that environment.

Administration

Each Parallels Secure Workspace environment can be fully managed by the members of the Admin group defined for each environment.

Monitoring and Reporting

Introduction

The **Dashboard** can be found in Applications. You need to be signed in as a user belonging to a user group labeled as *admin*.

Status Overview of Services on All Servers

The **Status** tab of the Dashboard provides a heat map of servers (vertical axis) versus components (horizontal axis). This tab is only available for admins of an administrative domain (global admins) and the management user (defined at installation).

The following color code convention is adopted:

- Empty: The corresponding component is not installed on this server.
- Dark gray: The component is installed but no data are available.
- Green: The corresponding component is running on the server.
- Orange: One of the corresponding sub components is installed, but not running on the server
- Red: The corresponding component is installed but not running on the server.

Clicking on a component bubble will lead you to a detailed page with more information on the particular component on that server.
Clicking on a server will lead you to a detailed page with more information on the server.

Monitoring Servers and Components

From the **Servers** tab in the Dashboard, system administrators can obtain more detailed information on servers and processes. This tab is only available for admins of an administrative domain (global admins) and the management user (defined at installation).

On the servers tab a list of servers is presented, together with hostname and status.
Clicking on a server leads you to a detailed page with statistics and components.

Statistics are shown over a configurable time interval for the following parameters:

- Memory Usage
- CPU Usage
- Status Information (running/halted)
- Disk Usage

All components/processes installed on that server are also shown with the following attributes:

- Name of component
- IP address
- Port
- Status

Clicking on a component leads you to a page with more details on the component.

Parallels Secure Workspace License Tracking

Parallels Secure Workspace provides system administrators the means to track license consumption, as part of the Dashboard.
The following metrics are shown:

- Number of named users.
- Number of concurrent user sessions. The "Concurrent User Count" field in your Parallels Secure Workspace license (see General Information) is the maximum value allowed for this metric.

This tab is only available for admins of an administrative domain (global admins) and the management user (defined at installation).

Number of Named Users

This metric tracks the number of named users on the Parallels Secure Workspace platform on a calendar month basis. The graph shows the number of named users for the past 12 months as well as for the current month.

All named users known to Parallels Secure Workspace (list visible on the **System Settings > Manage > Users** page) for a given month will count towards this metric, even if the user did not login to Parallels Secure Workspace.

The graph and metric is not updated real-time, but twice a day.

Deleting Users

Users can be deleted on the **System Settings > Manage > Users** page. Depending on the license type, deleted users will still be shown and counted towards the named users metric until the end of the month (the Deleted column will have a check mark) or they will be deleted immediately.

For users that have been removed from Parallels Secure Workspace, an entry will be re-created at next login time.

Peak Number of Concurrent User Sessions

This metric tracks the peak number of users signed in to Parallels Secure Workspace on a calendar month basis. It shows the number of concurrent user sessions for the past 12 months as well as for the current month. For the current calendar month, the value is peak number of concurrent sessions up to the current date.

The "Concurrent User Count" field in your Parallels Secure Workspace license (see General Information) is the maximum value allowed for this metric. The management user, created during installation, does not count as concurrent user.

Note that the values are not updated real-time, but every 5 minutes.

Example

Please follow this example on how the data for the license graphs are generated:

Time stamp	Action	Named Users	Concurrent User Sessions
2019-01-01 09:00	Parallels Secure Workspace is just installed	0	0
2019-01-01 10:00	Ada signs-in and opens the streamed app Word	1	1
2019-01-01 10:01	Youssef signs-in and opens the streamed apps Word and Excel	2	2
2019-01-01 10:03	Ada signs-out without closing Word (app is disconnected)	2	1
2019-01-01 10:04	Ada signs-in on other device and recovers the Word app	2	2
2019-01-01 10:05	Youssef closes Word and Excel and signs-out	2	1
2019-01-01 10:06	Ada closes Word and signs-out	2	0
2019-01-01 10:07	Wong signs-in	3	1
2019-01-01 10:08	Wong signs-out	3	0
January 2019	**Resulting graphs (peak)**	**3**	**2**

Live Monitoring of Users Activity

The **Activity** page in the Dashboard gives administrators insights into the current usage of the platform and allows them to log out users, terminate, and view their application sessions.

More specifically, it gives information regarding the number of simultaneously connected browsers to the platform, a.k.a. the number of concurrent users.

Admins of an administrative domain (global admins) and the management user (defined at installation) can filter for specific domains with the dropdown on the top left. Domain admins only see users of their domain.

- **Total active concurrent user sessions**: counts the number of currently connected concurrent users.
- **Total disconnected user sessions**: counts the number of user sessions that have not been properly closed. This can happen when a user closes the browser without logging out of Parallels Secure Workspace or when the battery of the end-user device fails, or when the end-user experiences a connectivity glitch. In those cases, the sessions remain in the **disconnected** state for 10 up to 15 minutes. The list is refreshed at a 5-minute interval.

The table below provides more details regarding the individually connected users:

- Each row represents a user session.
- Per user session, it is possible to see the session ID, the start time of the session, the disconnect time of the session (if applicable), the country, and the current status.
- Each user session can be individually logged out.
- Per user session, the linked application sessions can be shown by clicking the view details button (+ icon) on the left.
- Per application session, it is possible to see the application session ID, the application name, the start and end time, the used application server, whether the session was recorded, and the status.
- The following actions can be performed on an application session:
  - View session (eye icon): A new browser tab will be opened and after the user of the application session accepts the join request, the admin will be able to view the application session. The admin can also ask for keyboard and mouse control of the application session and provide support if necessary.
  - Terminate: The application session will be forcefully terminated and all unsaved changes will be lost.

Note that the countries shown in the table are based on a static geo IP database defined during installation or the last upgrade. Those locations might not be accurate anymore.

Monitoring the Application Connector

From the **Application Overview** tab in the Dashboard, system administrators can obtain information about applications and application servers.

Admins of an administrative domain (global admins) and the management user (defined at installation) can filter the views for specific domains with the dropdown on the top left. Domain admins only see the content of their domain.

Application Servers

For each server, one can see the number

- Active sessions: active applications streamed to the end users.
- Reserved sessions: a session is reserved when a user requests to open a streamed application. When the application is actually started, the session is not *reserved* anymore, but *active*.

Note that the sum of the active and reserved sessions can not be higher than *Max Connections* defined for that application server.

Applications

For each streamed application, one can click through the application insights, showing:

- The number of unique users that used the application (monthly).
- The maximum concurrent usage of the application (monthly).
- How many times each user has used the application.

The data can be filtered with the date picker on the top.

Insights Reporting

The Insights tab contains some overall information about the usage of Parallels Secure Workspace. Admins of an administrative domain (global admins) and the management user (defined at installation) can filter for specific domains with the dropdown on the top left. Domain admins only see users of their domain.

Application Usage

The table shows the number of distinct named users that have been using a particular streamed application over a configurable time interval.

OS and Browser

This page provides 2 tables that show information about the **end-user device OS** and **browser usage** over a configurable time interval. Every browser session is counted. So for example, if a user has signed in 20 times during the specified time interval, this will count as 20 sessions in both pie charts.

Audit Reporting

The Audit reporting tab in the Dashboard provides system administrators further insights in the usage of the Parallels Secure Workspace environment. Admins of an administrative domain (global admins) and the management user (defined at installation) can filter for specific domains with the dropdown on the top left. Domain admins only see users of their domain.

All data is kept for 13 months. The output can be exported to CSV.

Note: The date/time is shown in UTC.

Query Syntax

On each page, the admin can query and/or change the date period to limit the shown output.

Examples of query strings:

Query	Expected result
john	All records containing the full word "john"
john*	All records containing a word starting with "john"
john	All records containing "john" anywhere
john alice	All records containing the full words "john" or "alice"
john AND alice	All records containing the full words "john" and "alice"
NOT john	All records not containing the full word "john"
@timestamp:{2018-05-02T19:00 TO 2018-05-02T20:00}	All records with timestamp between given times

Advanced Querying

Using *advanced query* you can use a DSL (Domain Specific Language) to perform more fine-grained filtering.

To enable advanced querying, make sure you tick the ‘advanced query' box on the right-hand side of the filter input:

The field names to use in a query are different from the column names in the view. To get an overview of the field names available for the current view, click on the `i` icon next to *advanced query.*

Below an example of view specific information for *Shared Application Session Settings* audit logs

Filtering

The basic filter syntax for a comparison of a field to a value is as follow

```
[field] ([negation]) [filter operator] [value]
```

The `field` is the name of field to be queried. The `value` is the value the field shall be compared to. Values for strings and timestamps need to be quoted in single quotes. For boolean fields the values `true` and `false` are valid.

The possible values for the `filter operator` are listed in the table further below. Some of these filters can be negated with the optional keyword `not`, to see which operators support negation also see the table below.

Filter operator	Alias	Meaning	Negatable with "not"	Field type requirements

=	eq	"equal to"	= is not, but the eq alias is negatable	-
!=	not eq	"not equal to"	no	-
<	lt	"less than"	no	-
>	gt	"greater than"	no	-
<=	lte	"less than or equal to"	no	-
>=	gte	"greater than or equal to"	no	-
contains		substring search (case sensitive)	yes	requires text or char fields
icontains		substring search (case insensitive)	yes	requires text or char fields
startswith		substring search at the beginning of the field value (case sensitive)	yes	requires text or char fields
istartswith		substring search at the beginning of the field value (case insensitive)	yes	requires text or char fields
endswith		substring search at the end of the field value (case sensitive)	yes	requires text or char fields
iendswith		substring search at the end of the field value (case insensitive)	yes	requires text or char fields
isnull		value must be NULL	yes	-

User Sessions

The user sessions show a list of sessions with following information:

Property	Meaning
Start	The start date/time of the Workspace session (when logging on to Parallels Secure Workspace)
End	The end date/time of the Workspace session (at disconnect or at logout)
Domain	The Workspace domain of the user.
User Session Id	The internal user session id, which can be used to filter on the other audit pages.
Ip	The IP address of the machine which started the Workspace session.
Username	The domain\username.
Mfa	Whether Multi-Factor Authentication was used or not when logging in.
Latitude	Latitude coordinate/ based on geo IP (which is indicative).
Longitude	Longitude coordinate/ based on geo IP (which is indicative).
Labels	All (user) labels fetched from the Microsoft Windows Active Directory domain controller / LDAP server.

Application Sessions

This only applies for streamed applications (RDP and RemoteApp).

Property	Meaning
Start	The start date/time of an application session.
End	The end date/time of an application session.
Domain	The Workspace domain of the user opening the application.
Client Session Id	The internal id for the connection between browser and Parallels Secure Workspace*.

Application Session Id	The internal id for the connection between Parallels Secure Workspace and application servers.
User Session Id	The User session id (cf. User Sessions).
Client Session Numeric Id	Short version of the Client Session Id*.
Application Key	The internal Parallels Secure Workspace id for application (cf. Application Overview > Applications).
Server	The DNS or IP address of the application server.
Port	The server port used to connect to the application server.
Exe	The alias of the RemoteApp (empty for RDP applications).
Recorded	Whether the application sessions has been recorded.

* This id changes at each time the session is taken over on another device or in another browser tab.

Correlate with the logs on the application server

If you want to correlate an application session in Parallels Secure Workspace with an RDP session on application server, for that application session, you need to find the oldest log entry. The Client Session Numeric Id corresponding to that entry is the one used at startup of that application session.

This Client Session Numeric Id can be found on the application server **during the connection**:

- Windows Task Manager:
  On the Users tab, the column "Client name" (not shown by default) contains the Client Session Numeric Id (prefixed with AW-).

This Client Session Numeric Id can be found on the application server **post mortem**:

- On the Microsoft Windows Server: In the Event Viewer, go to Windows Logs > Security. Click on "Find..." in the right column to search for the Client Session Numeric Id (prefixed with "AW-").
  The event has following properties:
  - Keywords: Audit Success
  - Source: Microsoft Windows security auditing
  - Task Category: Logon

Shared Application Sessions

The Shared Application Sessions view lists all guests that joined a shared application session.

Property	Meaning
Start	Timestamp on which the client joined the shared application session.
End	Timestamp on which the client joined the shared application session.
Client Session Id	The internal id for the connection between browser (guest) and Parallels Secure Workspace.
Client Session Numeric Id	The internal id for the connection between browser (host) and Parallels Secure Workspace. It is equal to the Client Session Numeric Id of the host of the application session.
IP	The IP address of the client that joined the shared application session.

Share Application Sessions Settings

The Shared Application Sessions Settings view lists all shared application sessions and their settings (changes).

Property	Meaning
Timestamp	The timestamp on which the settings where applied.
Domain	The Workspace domain of the user opening the application
Client Session Id	The internal id for the connection between browser (guest) and Parallels Secure Workspace.
Application Session Id	The internal id for the connection between Parallels Secure Workspace and application servers.
User Session Id	The User session id (cf. User Sessions).

Joinable	Can users join the session.
Is Protected	Is a password required to join the session.
Join Mode	How is the session shared (`SINGLE` or `MULTI`).
Access Rights	How are access rights determined? (`PUBLIC`, `DOMAIN` or `USER`).

Web Applications

The Web Applications view lists all web applications accessed through Parallels Secure Workspace:

- For all web applications, each time a user clicks on the application within Parallels Secure Workspace, this is logged.
- For a reverse proxied web application, we also log when the user browses directly to the configured source host header, but the session cookie is not valid anymore. This is the case when the user has logged out from Parallels Secure Workspace since the last visit of the web application.

Property	Meaning
Timestamp	Timestamp on which the user has opened the web application.
Domain	The Workspace domain of the user opening the web application.
User Session Id	The User session id (cf. User Sessions).
Name	Name of the Web Application.
Url	Destination URL of the Web Application (connection between Parallels Secure Workspace and web server).
Behind Reverse Proxy	Whether the built-in reverse proxy is used for the web application.

Shares

The Shares view lists the creation, update, access and deletion of all shares.

Property	Meaning
Timestamp	Timestamp of the log entry.
Domain	The Workspace domain of the user that created the share.
User Session Id	For create/update/delete: the User session id (cf. User Sessions) performing the action. For access: the User session id (cf. User Sessions) accessing the share*.
Ip	IP address of the client that created/updated/deleted/accessed the share.
country	Country based on geo IP for the listed IP address.
Action	Can be create, update**, access or delete..
Name	Name of the share.
Drive	Drive from which the file/folder was shared.
Path	File path of the shared file/folder.
Content Type	Content type of the share.
Created By	Username of the user that shared the file.
Expires	Expiration date of the share.
Id	Internal ID of the share.
Folder	Indicates if the share is a folder.
Public	Indicates if the share is publicly accessible.
Mode	Mode in which the file was shared (DOWNLOAD or PREVIEW).
Checksum	Checksum of the shared file (when accessed).

Range	Range accessed during request***

* Anonymous access of a public share leads to an empty value.
** A share is updated when a property (e.g. Expiry date/time) has changed or the content has been updated (using the Update button in end-user UI).
*** A single access to a shared *preview* document can lead to multiple entries in the list. When viewing the document, this can be downloaded in multiple chunks into the PDF reader, leading to multiple requests and entries. This allows you to see if a document was downloaded entirely or not.

Files

The Files view lists all file actions using Parallels Secure Workspace. Note that in-app file actions can not be audited, because this happens directly between the application server and the file server. Only actions invoked in the Workspace and Files page can be tracked via Parallels Secure Workspace.

Property	Meaning
Timestamp	Timestamp of the log entry.
Domain	The Workspace domain of the user that performs the file action.
User Session Id	The User session id (cf. User Sessions).
Action	The performed file action, e.g. copy, move*, create folder, upload, ...
Drive	The drive where the file is located.
File Path	The path where the file is located.
Destination Drive	In case of copy or move: the drive where the file has been copied/moved to.
Destination File Path	In case of copy or move: the path where the file has been copied/moved to.

* Renames are treated as moves, where the destination file path is showing the new name.

Anomaly Reporting

The Anomalies reporting tab in the Dashboard provides system administrators insight into unusual activities on the Parallels Secure Workspace environment.

Admins of an administrative domain (global admins) and the management user (defined at installation) can filter for specific domains with the dropdown on the top left. Domain admins only see users of their domain.

The admin can query and/or change the date period to limit the shown output, which can be exported to CSV. The query syntax is the same as for Audit Reporting .

The following anomalies are reported:

Code	Category	Description
COUNTRY_MISMATCH	LOGIN	Same user is logged in in 2 different countries simultaneously.
TRAVEL_SPEED	LOGIN	The distance between 2 logins is too far to travel at a realistic speed.
TOO_MANY_FAILED_ATTEMPTS	LOGIN	A user uses the wrong password more than 3 times.
NEW_BROWSER	LOGIN	A user logs in with a new browser.
CONTEXT_RESTRICTION	CONTEXT	A user tried to perform an action that was prohibited due to context restrictions.

For each detected anomaly, the following information is provided:

Property	Meaning
Timestamp	Timestamp of the detected anomaly (UTC).
Domain	Domain of the user.
Category	Only `LOGIN` and `CONTEXT` categories are supported by now.
Code	Type of anomaly (see table above).
Description	More details of the actual anomaly.
Ip	IP address of the user.
Users Session Id	Users Session Id in case the user logged in (see Audit Reporting).
Username	domain\username

Country mismatch anomaly

At each login, we identify the country of the user based on his IP address. If a user is logged in simultaneously in two or more different countries, a COUNTRY_MISMATCH anomaly will be logged. The description field will mention the detected countries.

This can also occur for instance if the user connects to a VPN service where the network traffic suddenly passes through a remote location (for instance headquarters), after already being connected to Parallels Secure Workspace.

Travel speed anomaly

At each login, we identify the location of the user based on his IP address. If the distance of a user between the last logout and the current successful login would imply that the user would travel at a speed of more than 1000 km/h, a TRAVEL_SPEED anomaly will be logged. The description field will mention the distance and calculated speed in metric and imperial units.

This can also occur for instance if the user connects to a VPN service where the network traffic suddenly passes through a remote location (for instance headquarters), after already being connected to Parallels Secure Workspace.

Too many failed attempts anomaly

When a user fails 3 times consecutively to login, because of a wrong password or a wrong MFA (Multi-Factor Authentication) attempt, a TOO_MANY_FAILED_ATTEMPTS anomaly will be logged. The description field will mention the number of consecutive failed attempts.

Note: if a user has never logged in to Parallels Secure Workspace before, the anomaly won't be logged.

New browser anomaly

When a user logs in for the first time to Parallels Secure Workspace on a certain browser, a fingerprint is calculated to identify the browser. This fingerprint is stored locally in the browser. At each successful login, that fingerprint is sent to Parallels Secure Workspace and if the fingerprint is different from the one of the previous successful login, a NEW_BROWSER anomaly is logged. The description field will mention the fingerprint.

To calculate the fingerprint, different parameters are taken into account, like user agent, language, screen resolution, time zone etc. If one of those parameters changes, the fingerprint will not be recalculated as long the previous fingerprint is still stored locally in the browser. If the user however clears the local storage of the browser, the fingerprint will be recalculated and an anomaly will be logged.

Integration

- Integrating with existing Microsoft Windows environment
- Using Parallels Secure Workspace on existing Citrix infrastructure
- SSL offloader, reverse proxy or loadbalancer settings
- Multi Factor Authentication
- Parallels Secure Workspace Single Sign On (SSO)
- Microsoft OneDrive for Business
- Smart Card Redirection
- Automate Parallels Secure Workspace via the REST API
- External Audit Logging

Integrating with existing Microsoft Windows environment

Introduction

Although there are many possibilities to integrate the Parallels Secure Workspace platform into your existing IT environment, below you can find some useful remarks about this integration effort.

Using the Active Directory Server as NTP server

When you configure Parallels Secure Workspace to use the time service of your Active Directory Server as NTP server, you need to make sure that the Active Directory domain controller has a reliable time source. The easiest option is to sync your domain controller with a public NTP server pool, such as nist.gov .

Example for Microsoft Windows (can only be done using PowerShell):

```
net stop w32time
w32tm /config /syncfromflags:manual /manualpeerlist:"time-a.nist.gov, time-
b.nist.gov, time-c.nist.gov, time-d.nist.gov"
w32tm /config /reliable:yes
net start w32time
```

Organizational Units for users and application servers

Depending on the needs and the setup of the customer Microsoft Windows organization, there are multiple ways of organizing the Parallels Secure Workspace platform in the Microsoft Windows domain structure.

If users from separate organizational units (OUs) need to connect to the Parallels Secure Workspace platform, we believe it is useful to put the application servers in a dedicated OU. Such a structure makes it possible to apply Group Policies to the pool of application servers. If the user processing loopback Group Policy Object (GPO) is set within this application server OU, it is possible to apply and override user-side policy rules when they are logging into the application servers. This way, special user-side policy rules can be applied on the application servers for all users logging on to the application servers.

To configure the User Group Policy loopback processing mode, create and link a new GPO to your application server OU where the following is set:

- Computer Configuration / Policies / Administrative Templates / System / Group Policy / Configure User Group Loopback processing mode: This can be set to either merge or replace mode.

In **merge** mode, all user-side GPOs of the users original OU are first applied, afterwards the GPOs specific to the application server are applied.
In **replace** mode, only the user-side GPO of the application servers are applied. If you opt for replace mode, all the users who start apps on the application server will experience exactly the same behavior.

Group Policy recommendations

As described above, we recommend adding a few GPOs on the Parallels Secure Workspace users and application servers.

GPOs for the Parallels Secure Workspace users

Following GPOs are optional.
Note that in older Windows versions the term "Windows Explorer" is used instead of "File Explorer".

- User Configuration / Policies / Administrative Templates:
  - Start Menu and Taskbar: Remove Run menu from Start Menu: **Enabled**
  - System: Prevent access to the command prompt: **Enabled** (Disable the command prompt script processing also? **No**)
  - System: Ctrl+Alt+Delete Options: Remove Lock Computer **Enabled**
  - System: Ctrl+Alt+Delete Options: Remove Task Manager **Enabled**
  - Windows Components / Desktop Window Manager: Do not allow window animations: **Enabled**
  - Windows Components / File Explorer: Hide these specified drives in My Computer: **Enable** (Pick one of the following combinations: **Restrict all drives.**)
  - Windows Components / File Explorer: Hides the Manage item on the File Explorer context menu: **Enabled**
  - Windows Components / File Explorer: No Computers Near Me in Network Locations: **Enabled**
  - Windows Components / File Explorer: No Entire Network in Network Locations: **Enabled**
  - Windows Components / File Explorer: Prevent access to drives from My Computer: **Enabled** (Pick one of the following combinations: **Restrict all drives**)
  - Windows Components / File Explorer: Remove "Map Network Drive" and "Disconnect Network Drive": **Enabled**
  - Windows Components / File Explorer: Remove File Explorer's default context menu: **Enabled**
  - Windows Components / File Explorer: Remove Hardware tab: **Enabled**
  - Windows Components / File Explorer: Remove Search button from File Explorer: **Enabled**
  - Windows Components / Remote Desktop Services / Remote Desktop Session Host / Session Time Limits: Set time limit for disconnected sessions: **Enabled** (End a disconnected session: **1 minute**)
  - Windows Components / Remote Desktop Services / Remote Desktop Session Host / Session Time Limits: Set time limit for logoff of RemoteApp sessions: **Enabled** (RemoteApp session logoff delay: **Immediately**)
  - Windows Components / Windows PowerShell: Turn on Script Execution: **Enabled** with **Allow only signed scripts**

More settings are described in e.g. http://nikoscloud.wordpress.com/2013/04/23/how-to-secure-your-remote-desktop-server-with-gpo/

GPOs for the application servers

- Computer Configuration / Policies / Administrative Templates / Windows Components / Remote Desktop Services / Remote Desktop Session Host / Connections:
  - Required: Restrict Remote Desktop Services users to a single Remote Desktop Services sessions: **Disabled**.
  - Required: Automatic reconnection: **Enabled**.
  - Needed when you want to publish programs in Parallels Secure Workspace as an RDP application: Allow remote start of unlisted programs: **Enabled**.
- Computer Configuration / Policies / Administrative Templates / Windows Components / Remote Desktop Services / Remote Desktop Sessions Host / Session Time Limits:
  - Required: Set time limit for disconnected sessions: End a disconnected session in **1 minute**
  - Required: Set time limit for logoff of RemoteApp sessions: RemoteApp session log off delay **Immediately**
- Computer Configuration / Policies / Administrative Templates / Windows Components / Remote Desktop Services / Remote Desktop Sessions Host / Device and Resource Redirection:
  - Optional: Allow time zone redirection: **Enabled**.

Set-up Drives connectivity

CIFS connectivity:

For Parallels Secure Workspace to allow connections to the CIFS backend, the specific servers needs to enable SMB shares and SMB connectivity should be allowed to the Parallels Secure Workspace environment (for a multi-node Parallels Secure Workspace environment: connect to workers and frontend nodes).

Please be sure the SMB protocol is enabled on your server. You can use following cmdlet:

```
Set-SmbServerConfiguration -EnableSMB2Protocol $true
```

WebDAV drives:

In order to have access to your webdrive, the file structure needs to be published via Webdav on your file servers. Our WebDAV connector needs at least DAV protocol version 2.

To set-up WebDAV via IIS (version 8)

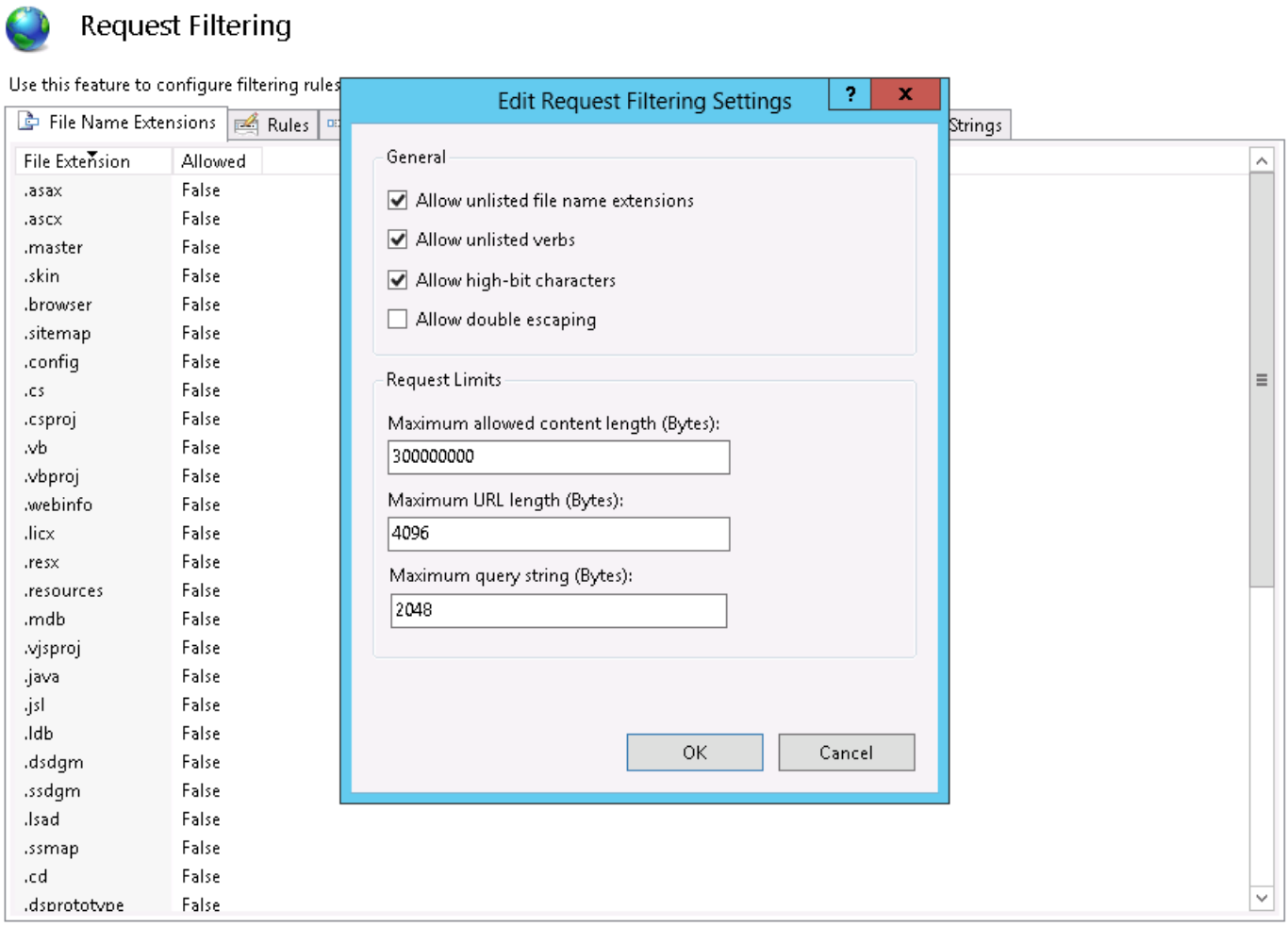
1. Install the IIS server role and features:
   a. Add the IIS role, no extra feature, ignore WSRM,
   b. IIS Features: Common HTTP Features: Webdav Publishing, default document, Directory Browsing, Http Errors, Http Redirection, Static Content.
   c. IIS Features: Health Diagnostics: Custom logging, HTTP logging, Logging Tools
   d. IIS FeatureS: Authentication: Click on everything
2. Go to Manager IIS Manager
   a. Add an application pool called webdav
   b. Rename the Default site
   c. Add a website: webdav connect it to share location
   d. Bind it to port 80
   e. Webdav
      i. Add Authorizing Rule (that all users can connect)
      ii. Enable WebDav
   f. Authentication
      i. Enable Basic, Digest and Windows.

WebDAV support for large files

By default IIS WebDAV has request filtering turned on, which limits the default upload size to 30000000 Bytes, which is approximately 28.6MiB. Refer to this guide to change these settings.

In summary

- Open the IIS Manager:
  - Click on the left pane to your WebDAV site.
  - Find and clink on the middle pane 'Request Filtering'.
  - Edit on the right pane: 'Edit Request Filtering Settings'
  - In this dialog box, you can change the default value of the Maximum Allowed content length (Bytes).



WebDAV adding MIME Type

If you have MIME types that you want all of your Web sites to recognize, you can add the new MIME types at the global level in IIS.
To add a global MIME type

1. In IIS Manager, expand the local computer, right-click the computer/site on which you want to add a MIME type, and click Properties.
2. Click MIME Types.
3. Click Add (or New).
4. In the Extension box, type the file name extension.
5. In the MIME type box, type a valid MIME type.

WebDAV create default MIME type

1. In IIS Manager, expand the local computer, right-click the computer/site on which you want to add a MIME type, and click Properties.
2. Click MIME Types.
3. Click Add (or New).
4. In the Extension box, type the file name extension.
5. In the MIME type box, type a valid MIME type.
   a. To create a MIME type for an undefined MIME type, type an asterisk in the Extension box, and type application/octet-stream in the MIME type box.
      Example: File name extension: '*' MIME type: application/octet-stream
   b. To create a MIME type for a file without an extension, type a period (.) in the Extension box, and type your MIME type in the MIME type box.
      Example: File name extension: '.' MIME type: application/octet-stream
6. Click OK.

Do not use wildcard MIME-types on production servers. Doing so can result in IIS serving unrecognized files and displaying sensitive information to users. Wildcard MIME-types are intended for testing purposes or in scenarios where Internet Server API (ISAPI) filters have been developed specifically to handle these wildcard scenarios, for example, a custom authentication ISAPI.

Supported Windows versions

We officially support following Microsoft Windows Application Server versions:

- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022

Notes:

- When using certificates on the application servers, the ones Microsoft Windows generates are not compatible with Parallels Secure Workspace.

Enabling audio support

To enable audio in streamed applications, the Windows Audio Service needs to be enabled. To enable this service:

- Open Administrative Tools.
- Open Services.
- Open Windows Audio service.
- Ensure that the service is running.

Audio playback works on all supported browsers.

RDP vs RemoteApp

There are 2 methods to provide applications to Parallels Secure Workspace:

- **Remote Application** is an extension to the Remote Desktop Protocol. Remote Application needs to be supported by the application server, and the applications need be exposed over Remote Application. It has several advantages over the regular RDP applications:
  - The window selector (Windows button in the top of the app) is available.
  - The experience on tablets is smoother (especially when rotating the tablet and zooming in/out).
  - The app sharing experience is better.
  - It uses less resources on the application server.
- **RDP application** will make use of the regular Remote Desktop Protocol. **Full desktops** can only be provided via this protocol.
  When providing an application (no full desktop) to Parallels Secure Workspace, the user might notice a delayed closing of the session: after closing the application, a black screen can be shown for up to 3 minutes. This is because Microsoft Windows keeps a print service running. To mitigate this behavior, please follow this solution: https://support.microsoft.com/en-us/help/2513330/

Microsoft Windows Server 2016 / 2019 / 2022 Application server

Please refer to this guide: http://technet.microsoft.com/en-us/library/hh831447.aspx

Install Remote Desktop Services

1. Log on to Microsoft Windows Server as an Administrator.
2. Open Server Manager. (click Start > Administrative Tools > Server Manager)
3. From Dashboard, click "Add roles and features".
4. Select "Remote Desktop Services Installation", click Next.
5. From deployment type, select "Quick" deployment if you need to quickly deploy all roles to a single server. To have more control, use "Standard Deployment", click Next.
6. From deployment scenario, select "Session-based desktop deployment", click Next.
7. Finish and confirm Installation.
8. Restart the server.

Parallels Secure Workspace will detect the Network Level Authentication (NLA) for RDP connection automatically. This setting can be changed in the Server Manager > Remote Desktop Server Settings > Deployment properties > Security settings: Network Level Authentication.

The following message appears when opening a streamed app to that application server: "The server denied the connection". Note that the app will start anyway. To avoid that message, please make sure the Remote Desktop Connection Broker service is running.

Configure deployment service

1. Open Server Manager. (click Start > Administrative Tools > Server Manager)
2. Select "Remote Desktop Services".
3. From "Deployment Overview", from the "TASKS" drop-down menu, click "Edit Deployment Properties".
4. From "RD Gateway", select "Automatically ...".
5. From RD Licensing, select "Per User", make sure that the Microsoft Remote Desktop Licensing Server is add to list, or add it.
6. click Apply/OK to finish.

Configure RemoteApp Collections

1. Open Server Manager. (click Start > Administrative Tools > Server Manager)
2. Select "Remote Desktop Services", select "Collections".
3. If you don't have any collections create new one, the default "QuickSessionCollection"
4. Make sure that Network Level Authentication is not required.
   a. when on "QuickSessionCollection" on properties click tasks > Edit properties
   b. Select Security,
   c. For the Security layer select negotiate.
   d. Encryption Level: Client Compatible
   e. Uncheck: Allow connections only from computers running Remote Desktop Service with Network Level Authentication

Configure RemoteApps

1. Open Server Manager. (click Start > Administrative Tools > Server Manager)
2. Select "Remote Desktop Services", select your collection "RemoteApps" from Collections.
3. From "RemoteApp Programs", from the "Tasks" drop-down menu, click "Publish RemoteApp Programs".
4. From "Publish RemoteApp Programs" form select the apps you want to be available.
5. For application interactivity (ex. edit files) you need to allow command line arguments:
   After publishing, go again to "RemoteApp Programs" section, check the properties of the published app and allow for command line arguments.

On Microsoft Windows 2016/2019/2022 servers, the remoteapp alias cannot be changed through the GUI anymore. However, the remoteapp alias can still be changed via PowerShell.
In PowerShell, use the following commands:

```
Import-Module RemoteDesktop
Set-RDRemoteApp -Alias "wordpad" -DisplayName "wordpad_Renamed"
```

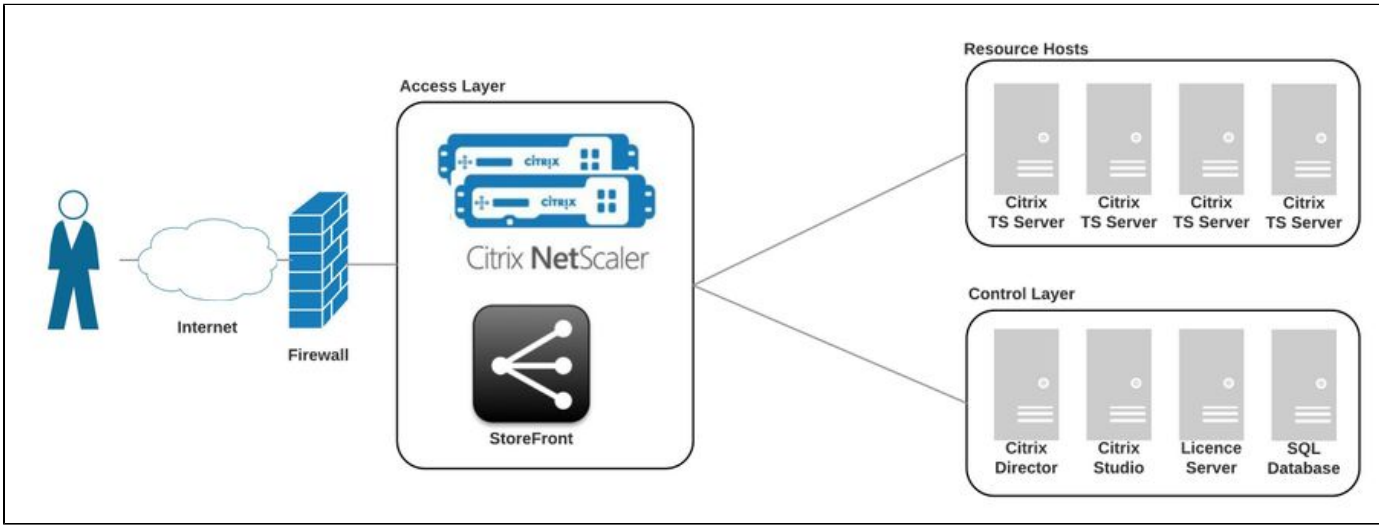
Using Microsoft Windows AD Administrative Center

In Microsoft Windows AD Administrative Center, the UPN is not required for a user. However, Parallels Secure Workspace does requires this. Please provide a domain UPN as defined here: https://technet.microsoft.com/en-us/library/cc772007(v=ws.11).aspx

Using Parallels Secure Workspace on existing Citrix infrastructure

Migrating away from an existing Citrix infrastructure to Parallels Secure Workspace is actually a really easy four-step process.

Below is a picture of a typical Citrix XenApp Deployment:



Installing Parallels Secure Workspace next to this setup can be achieved by deploying 1 or more (for load distribution or High Availability) Parallels Secure Workspace appliances in the Access Layer following this procedure which can be executed in less than 1 hour.

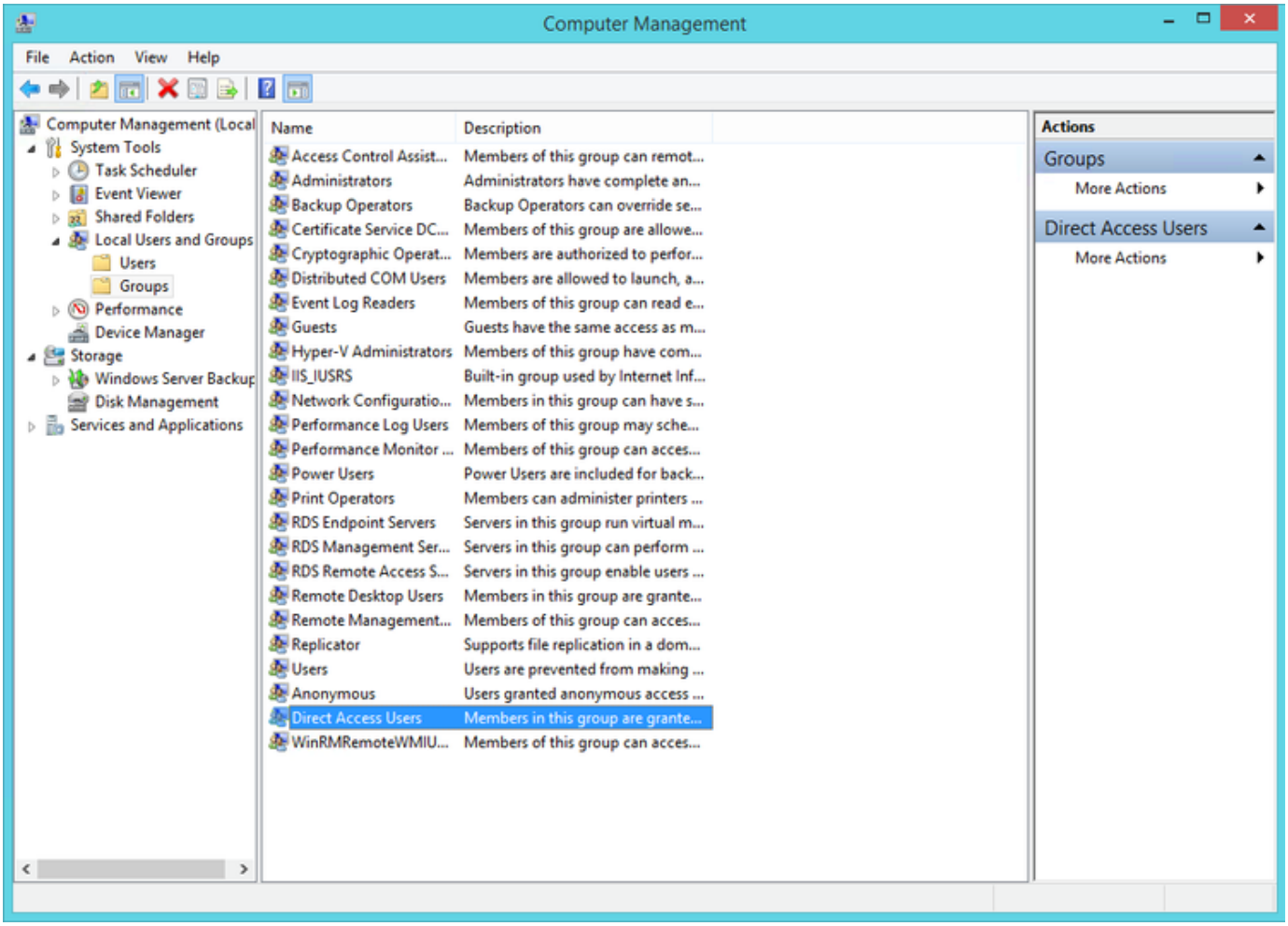
Note: As long Citrix is installed on the resource hosts, you need to have Citrix licenses for the RDP connections from Parallels Secure Workspace to the resource hosts.

Preparation

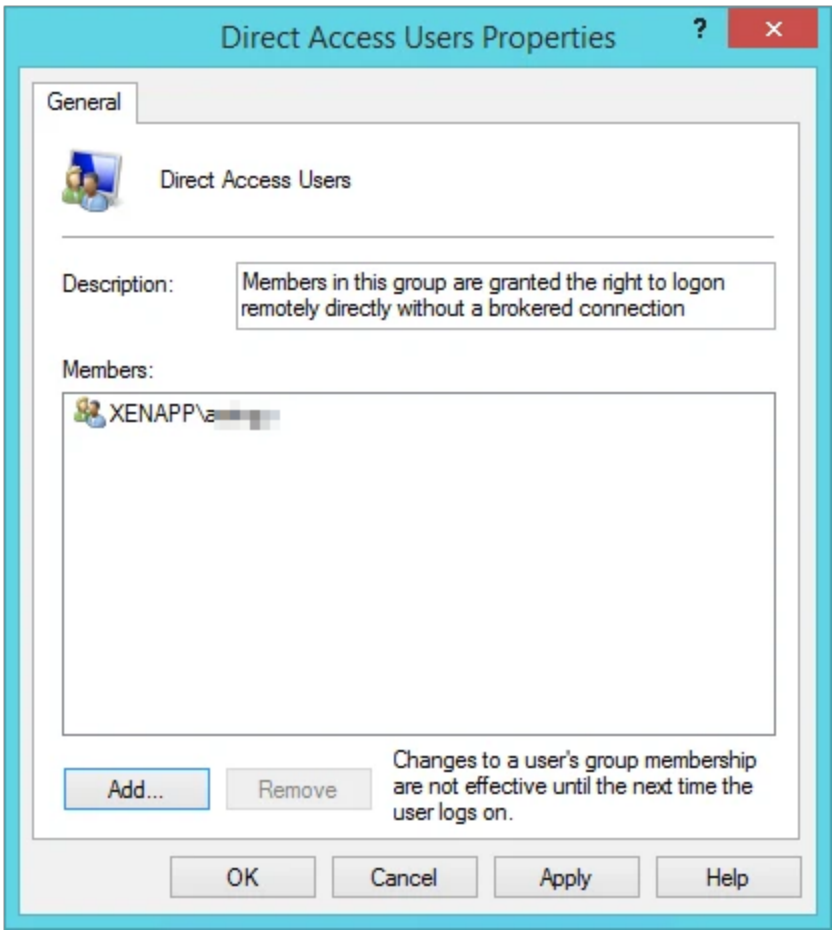
Download, install and configure Parallels Secure Workspace as described in Admin Manual. The Citrix TS Servers (Resource Hosts) are the application servers to configure in Application Server Management .

Allow non-administrators to RDP to the Citrix servers

When Citrix Virtual Delivery Agent is installed on a machine, non-administrators can no longer RDP to the machine. A new local group called Direct Access Users is created on each Virtual Delivery Agent. Add your non-administrator RDP users to this local group so they can RDP directly to the machine:

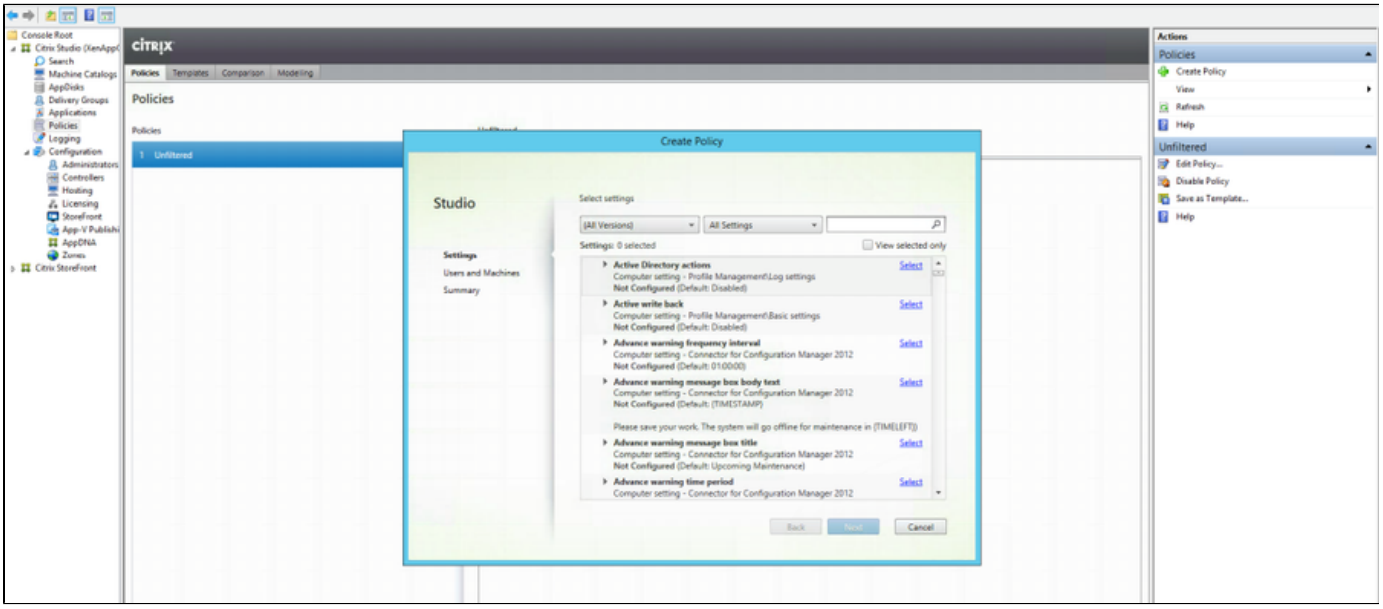


Add here the security group for the users which should have access:

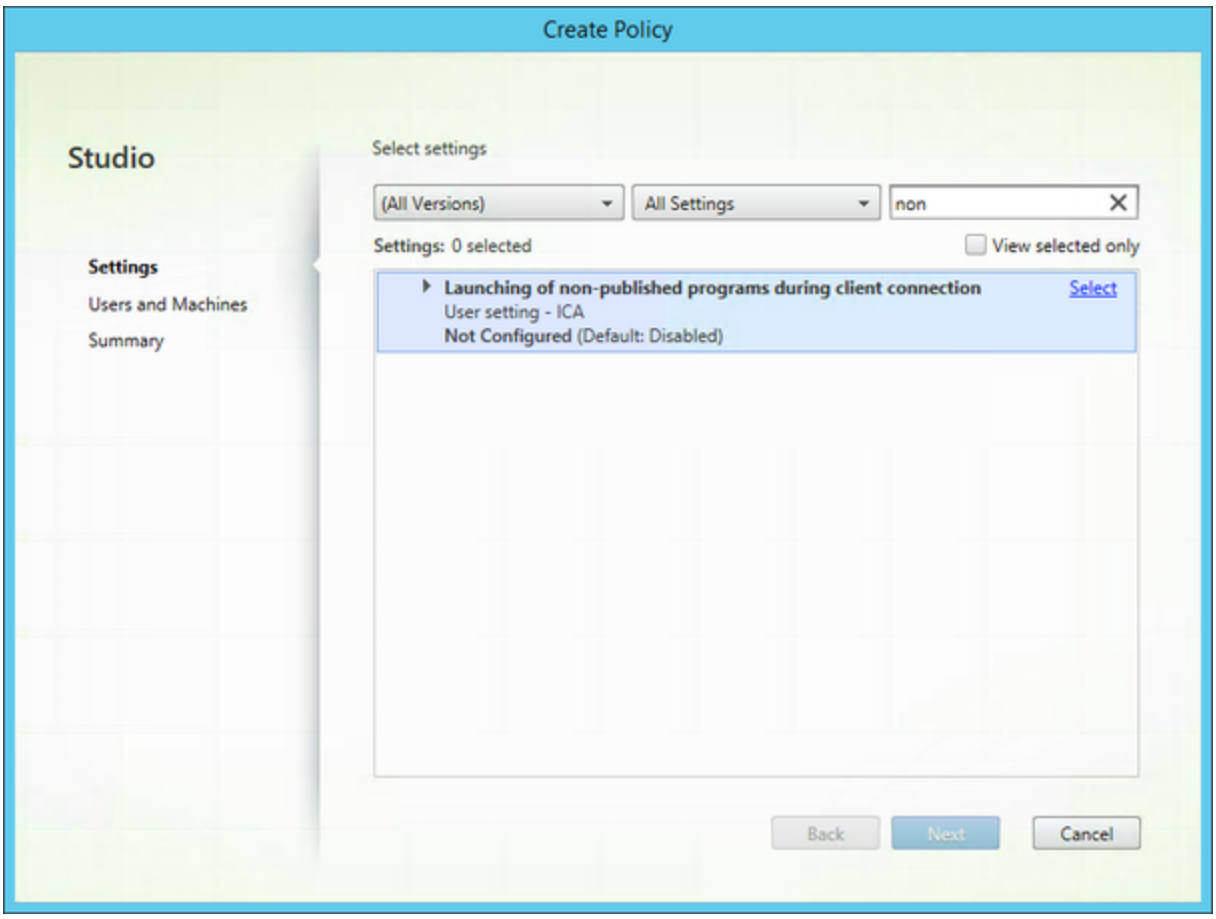


Enable RDP policy in Citrix studio

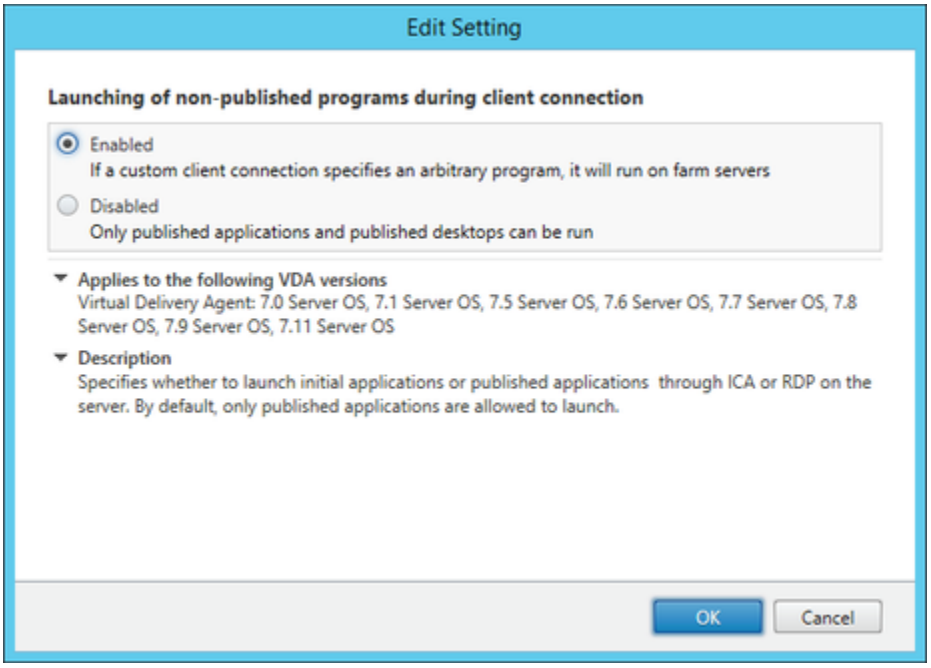
To be able to initiate a remote session a policy needs to be added to Citrix. Open the Citrix director and browse to the policy section. On the right top choose Create Policy:



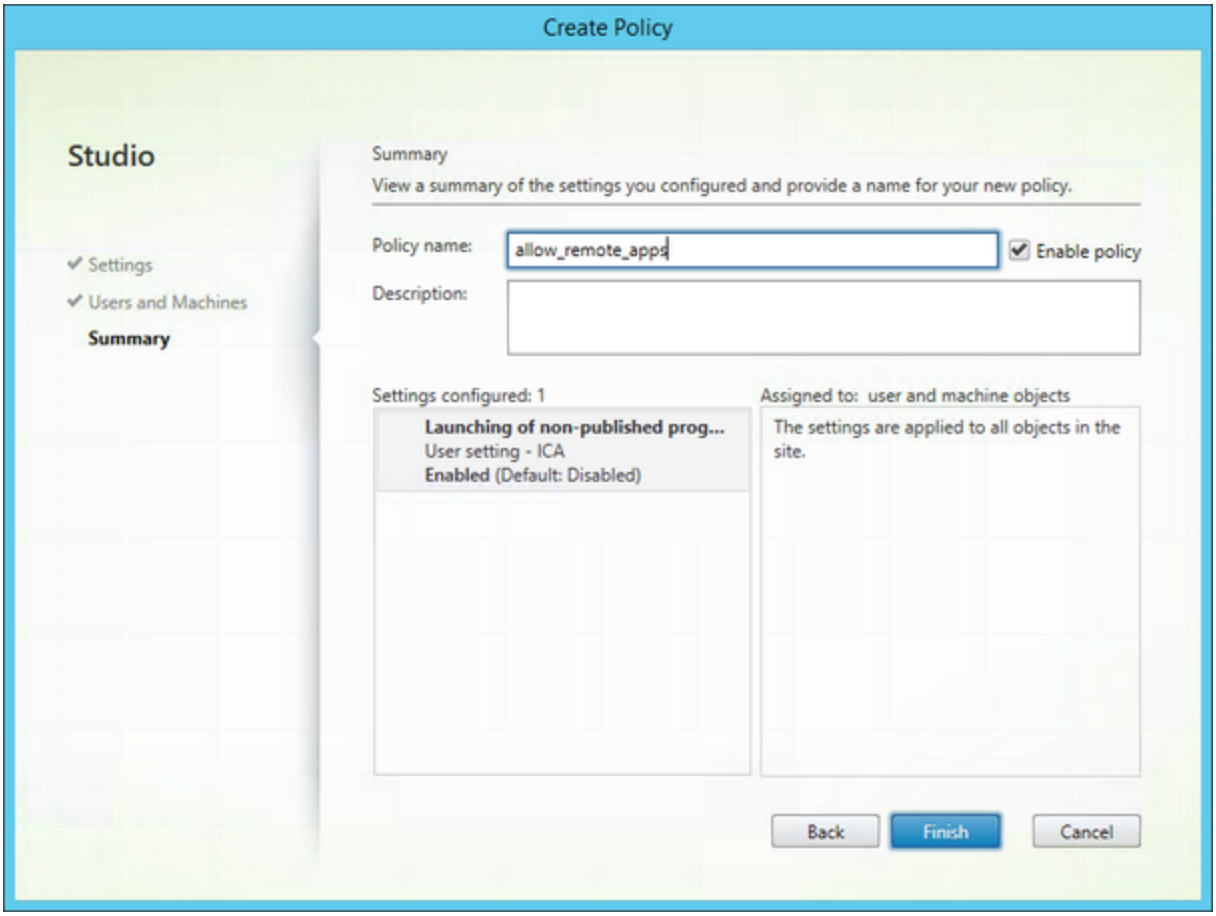
In the search field search for: "Launching of non-published programs during client connection" and select it:



Enable this policy for all objects in this site:

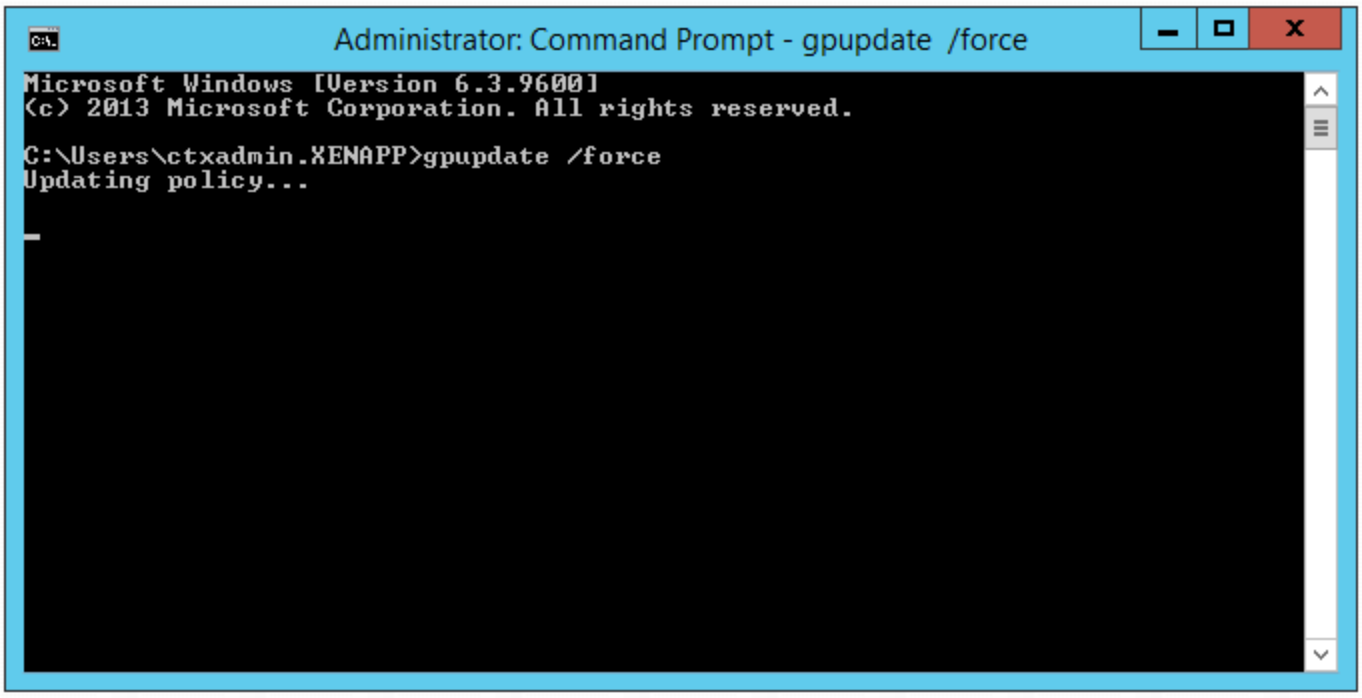


Give it a meaningful name and enable the policy:



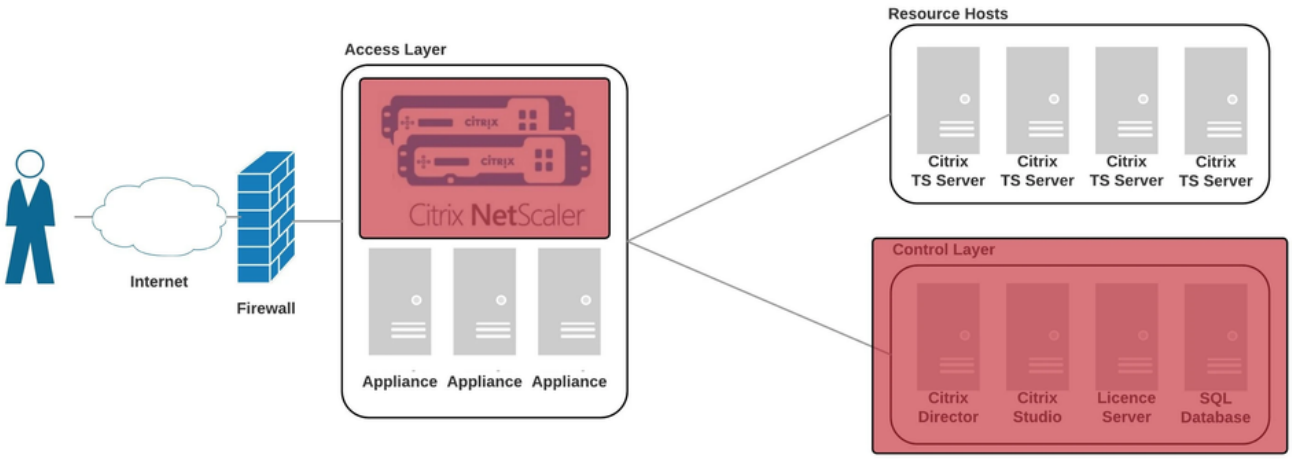
Set the policy priority higher:

If you want to speed the policy up you can always update them manually:



Optional: uninstall Citrix software from app servers

The result would be like in the following picture:



Please note that the NetScaler can be optionally used to load balance to the different Parallels Secure Workspace appliances but any load balancer will do.

The Citrix Control layer is no longer needed now. The Parallels Secure Workspace appliances have all knowledge needed to do the brokerage to the different RDS servers.

SSL offloader, reverse proxy or loadbalancer settings

Required Headers

WebSocket

WebSocket (WS) technology is based on upgrading a regular HTTP session to a long-living WebSocket connection. To this end, the browser requests a protocol upgrade by sending an HTTP request with the headers for a protocol upgrade. Therefore, the proxy server needs to allow these headers to propagate, to ensure successful HTTP(S) to WS(S) upgrades

Header	Explanation
Connection	This value should be equal to Upgrade
Upgrade	Should be equal to websocket in case of a WebSocket upgrade

The connection header is a hop-by-hop header, it needs to be explicitly set by the SSL offloader or proxy stages in between the browser and the Parallels Secure Workspace environment. See the Nginx example below, to find the correct example settings.

This header only needs to be set to a limited set of URLs. These requests are only requests of these forms:

- /hostname/RDP
- /hostname/JOIN
- /hostname/API

For a multi-node deployment, please replace "hostname" in the list above with the host names of the RDP Gateways. In general, this can be triggered by the following regular expression: `/.*/(RDP|API|JOIN)` .

SSL Offloader Headers

Header	Explanation
X-Forwarded-Proto	This informs Parallels Secure Workspace about the originally used protocol.

Proxy Headers

Setting these headers makes sure that Parallels Secure Workspace is aware of the proxy servers in front.

Header	Explanation
X-Real-IP	This should be the IP address of the requesting client
X-Forwarded-For	This should be the IP address of the requesting client
X-Forwarded-Host	This is the FQDN of the server name that was requested by the client
Host	This is the FQDN of the server name that was requested by the client

Proxy Timeout

Usually, reverse proxies and SSL offloader have built-in times-outs for their requests to back-end servers. In the case of WebSockets however, a TCP connection is being kept open. Hence, one needs to make sure that the SSL offloader or reverse proxies are not closing the connection after a few seconds or minutes of inactivity. This would result in streamed applications that are closing automatically for the end-user after this idle timeout value.

Please consult the documentation of your SSL offloader to change these settings in the case of WebSocket. For Nginx based offloading this setting is as follows:

```
### Proxy Read Timeout:
proxy_read_timeout 3500s;
```

Gzip compression

To reduce the size of transmitted data resulting in better performance, Parallels Secure Workspace compresses its HTTP(S) traffic using gzip. This is a standard supported by most browsers.
The data is only compressed if the browser supports this, which is indicated by the presence of gzip in the Accept-Encoding header sent by the browser.

Please validate the header **Accept-Encoding** is not stripped by the reverse proxy, as this might result in performance loss.

Replacing Parallels Secure Workspace Nodes

If a Parallels Secure Workspace node with the **proxy** service enabled needs to be replaced, and you want to re-use the original IP address, then you need to remove that IP address from the reverse proxy/load balancer before you replace the node with a fresh Parallels Secure Workspace appliance. If you don't, that new appliance will redirect port 80 to the 8080, where the installer is running.

After adding the new appliance to the Parallels Secure Workspace environment, you can re-add the IP address to the reverse proxy/load balancer.

Example Nginx Settings

Due to the SSL 'logjam' vulnerability, you need to generate a new Diffie-Hellman group for TLS. For more information, please see https://weakdh.org/sysadmin.html.
In order to generate a new Diffie-Hellman group, please use the following command:

```
openssl dhparam -out dhparams.pem 2048
```

After you have generated the new Diffie-Hellman group, you need to reference it in your Nginx configuration with the ssl_dhparam variable (see below).

The following config settings are working Nginx for SSL offloading:

```
upstream frontends {
    server <IP-OF-PARALLELS-SECURE-WORKSPACE-VM>:80;
}

server {
    listen           80;
    server_name      sgo.yourcompany.com;
    ## redirect http to https ##
    rewrite        ^ https://$server_name$request_uri? permanent;
}

server {
    listen             443;
    ssl                on;
    server_name        sgo.yourcompany.com;
    ssl_certificate    sslcerts/yourcompany.com.chained.crt;
    ssl_certificate_key sslcerts/yourcompany.com.key;
    # due to the SSL 'Poodle' vulnerability, SSLv3 should be disabled
    ssl_protocols      TLSv1.2 TLSv1.3;
    ssl_ecdh_curve     X25519:P-256:P-384:P-224:P-521;
    ssl_ciphers        EECDH+AESGCM:EDH+AESGCM;
    ssl_prefer_server_ciphers on;
    ssl_dhparam /etc/ssl/private/dhparams.pem;

    keepalive_timeout    60;
    ssl_session_cache    shared:SSL:10m;
    ssl_session_timeout  10m;

    # Gzip Settings
    gzip on;
    gzip_disable "msie6";
    gzip_types
        application/atom+xml
        application/javascript
        application/x-javascript
```

```
    application/json
    application/ld+json
    application/manifest+json
    application/rss+xml
    application/vnd.geo+json
    application/vnd.ms-fontobject
    application/x-font-ttf
    application/x-web-app-manifest+json
    application/xhtml+xml
    application/xml
    font/opentype
    image/bmp
    image/svg+xml
    image/x-icon
    text/cache-manifest
    text/css
    text/plain
    text/vcard
    text/vnd.rim.location.xloc
    text/vtt
    text/x-component
    text/x-cross-domain-policy;

### We want full access to SSL via backend ###
location / {
            proxy_pass  http://frontends;

            ### force timeouts if one of backend is died ##
            proxy_next_upstream error timeout invalid_header http_500 http_502 http_503 http_504;

            ### Set headers ####
            proxy_set_header        Accept-Encoding    "";
            proxy_set_header        Host               $host;
            proxy_set_header        X-Real-IP          $remote_addr;
            proxy_set_header        X-Forwarded-Host   $host;
            proxy_set_header        X-Forwarded-Server $host;
            proxy_set_header        X-Forwarded-For    $proxy_add_x_forwarded_for;

            ### Most PHP, Python, Rails, Java App can use this header ###
            proxy_set_header        X-Forwarded-Proto $scheme;


            ### By default we don't want to redirect it ####
            proxy_redirect     off;

            location ~ /.*/(RDP|API|JOIN|RAH) {
                proxy_pass  http://frontends;

                # WebSocket support (nginx 1.4)
                proxy_http_version 1.1;
                proxy_set_header Upgrade $http_upgrade;
                proxy_set_header Connection "upgrade";
                proxy_set_header        Accept-Encoding    "";
                proxy_set_header        Host               $host;
                proxy_set_header        X-Real-IP          $remote_addr;
                proxy_set_header        X-Forwarded-Host   $host;
                proxy_set_header        X-Forwarded-Server $host;
                proxy_set_header        X-Forwarded-For    $proxy_add_x_forwarded_for;
                ### Proxy Read Timeout: 12h
                proxy_read_timeout 43200s;
            }

            location /upload/ {
                client_max_body_size 0;

                proxy_pass http://frontends/$request_uri;
                proxy_request_buffering off;
```

```
                    proxy_buffering off;
                    proxy_cache off;
                    proxy_set_header Host $host;
                    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                    proxy_set_header X-Forwarded-Proto $scheme;
                }

    }
}
```

We recommend using **minimum 512 worker connections per 50 concurrent users**. This can be configured in /etc/nginx/nginx.conf. For the number of open files, take some additional margin. Example for **200 users**:

```
worker_rlimit_nofile 3000;

events {
        worker_connections 2048;
}
```

Using Workspace built-in OTP

Introduction

Parallels Secure Workspace has two built-in Multi-Factor Authentication (MFA) options: **counter-based** or **time-based** OTP (one-time password).

Note that the OTP token will also be asked when required to log in for reverse proxied web applications.

Configuration

OTP can be enabled for each domain, see User Connector Configuration for all available settings and detailed information.

User Setup

The first time a user wants to log in after MFA is enabled, they need to go through the following steps only once:

1. Download an authenticator app (typically on their smartphone) supporting the chosen MFA authentication method.
2. After providing credentials on the Parallels Secure Workspace login page, the user will be forwarded to a page showing a QR code and a secret.
3. The user scans the QR code with their phone (or enters the secret manually).
4. The first token is generated in the app. The user enters that token to proceed.

Next time the user logs in, they will only need to provide their regular credentials and their token.
They will not need to scan the QR code again; unless the token has been reset.

Any authenticator app that support**s counter-based authentication** (also called **HOTP**) or **time-based authentication** (also called **TOTP**) should work with Parallels Secure Workspace's two-factor authentication.

Some suggestions:
Android: Authy, Google Authenticator, Microsoft Authenticator, Sophos Authenticator, ...
iOS: Authy, Google Authenticator, Microsoft Authenticator, Sophos Authenticator, ...
Linux: Authy
Windows Phone: Microsoft Authenticator
Windows: 1Password, Authy (requires one-time phone verification, can be done by SMS), BitWarden, ...

Most authenticator apps on a smartphone require a phone number in some way. If the user does not have a mobile device available to them for doing MFA, they could also use a browser extension such as Authenticator.cc . When setting up MFA with this extension, you can either use its Scan QR feature or you can use the text code on the Parallels Secure Workspace MFA set-up screen (upon login).

Note that it's worth evaluating different authenticator apps as there may be specific limitations or advantages.
Some useful criteria for such an exercise are:

- Back-up.
- Synchronization.
- Multi platform / operating system.
- device type (smartphone, tablet, PC, ...).
- Required linking of a phone number.
- Support for HOTP and/or TOTP.

Integrating Parallels Secure Workspace with Duo

Introduction

Parallels Secure Workspace integrates with Duo for multi-factor authentication.

This guide will walk you through the different steps required to configure both Parallels Secure Workspace and Duo to enable the integration.

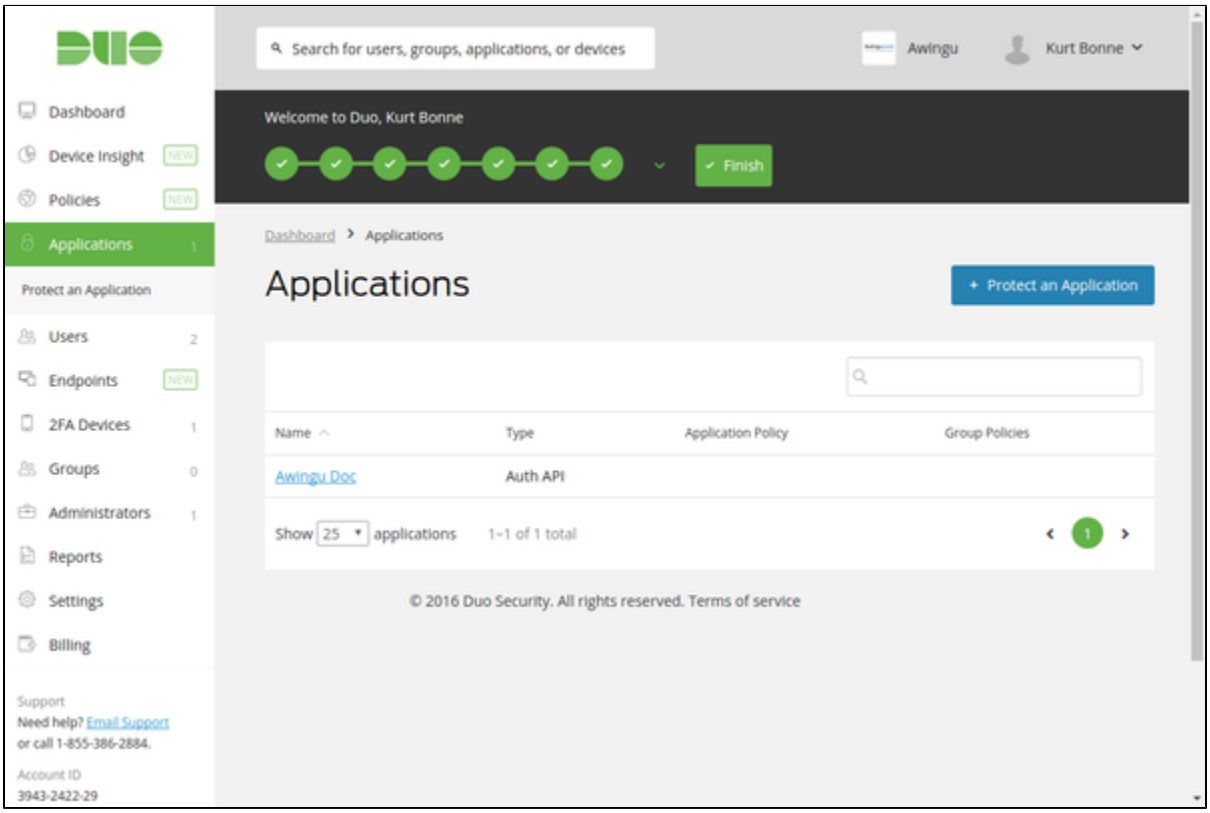
Prerequisites

This guide assumes you have administrative access to a working Parallels Secure Workspace environment and an active Duo account. The Duo personal plan is sufficient to evaluate Duo integration with Parallels Secure Workspace.

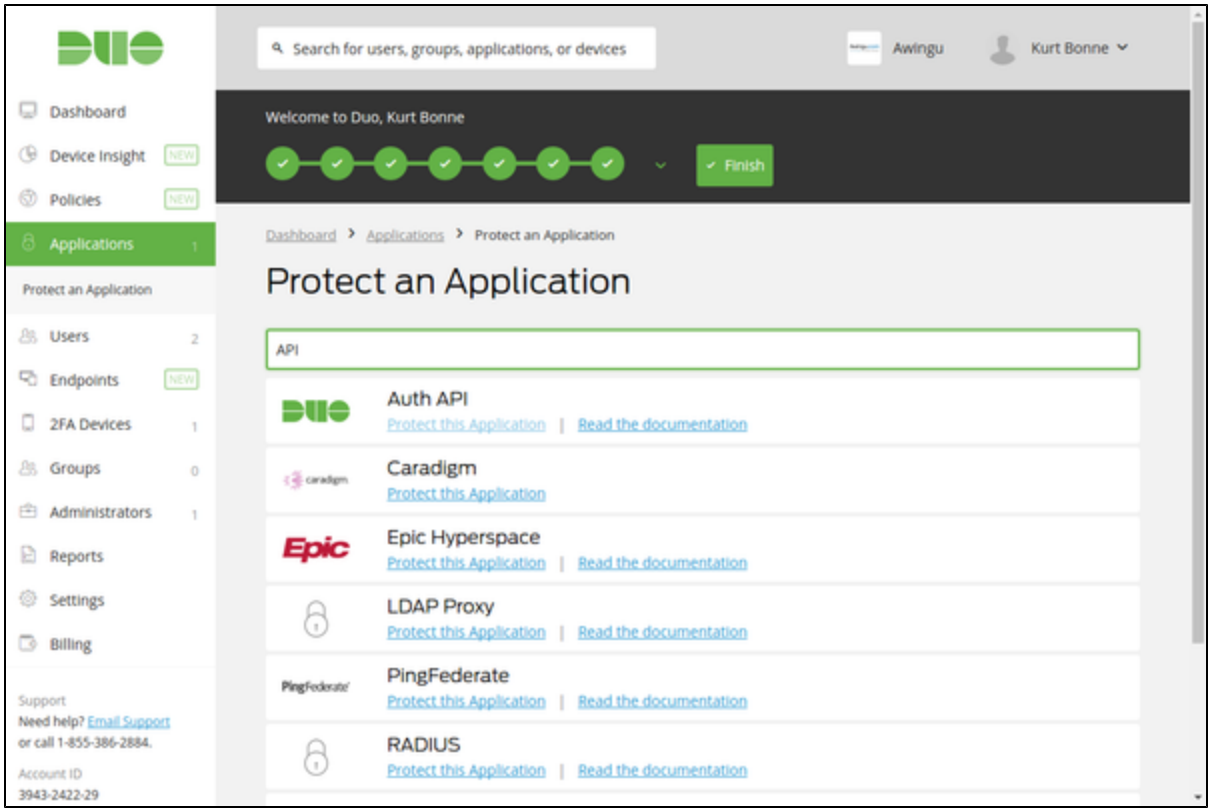
As Duo is a SaaS service, the Parallels Secure Workspace environment requires access to the Duo SaaS service. This is TCP port 443 to the API hostname of your configured application (<your_api>.duosecurity.com).

Configuring your Parallels Secure Workspace application in Duo

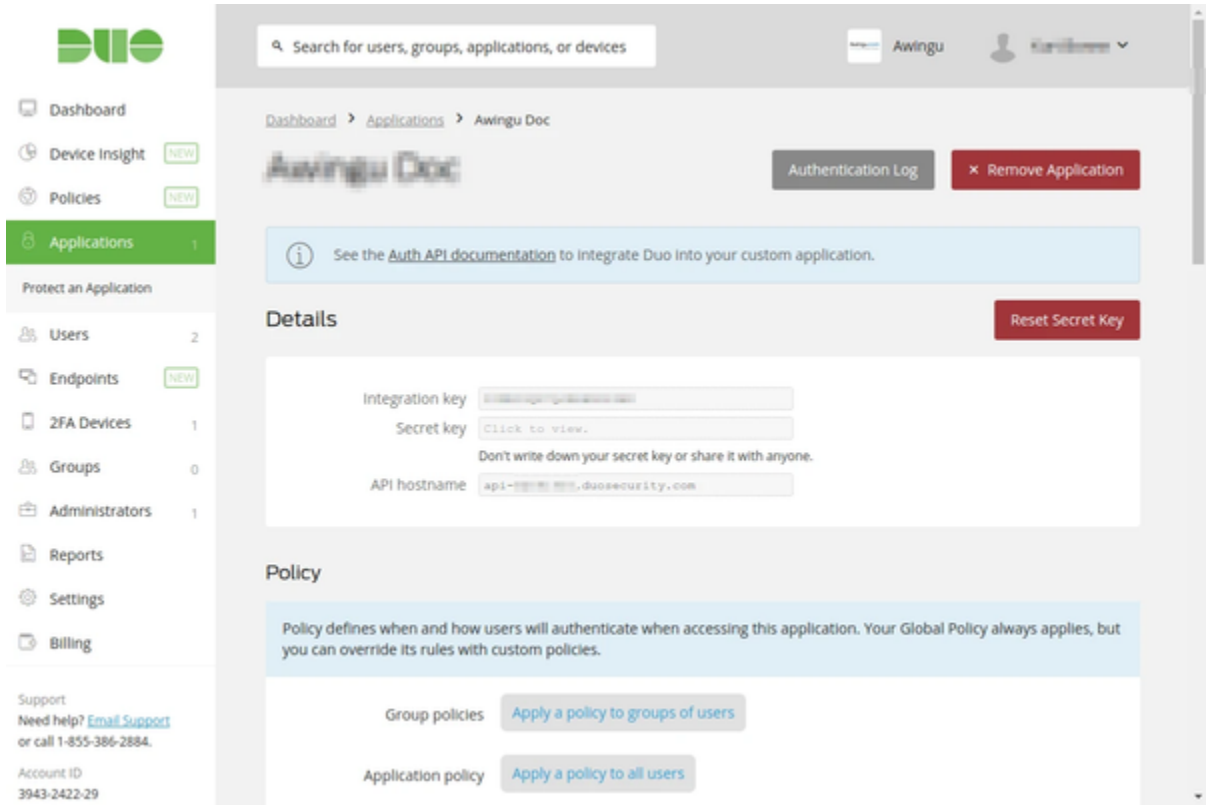
Sign in to your Duo account and select `Applications` in the menu.



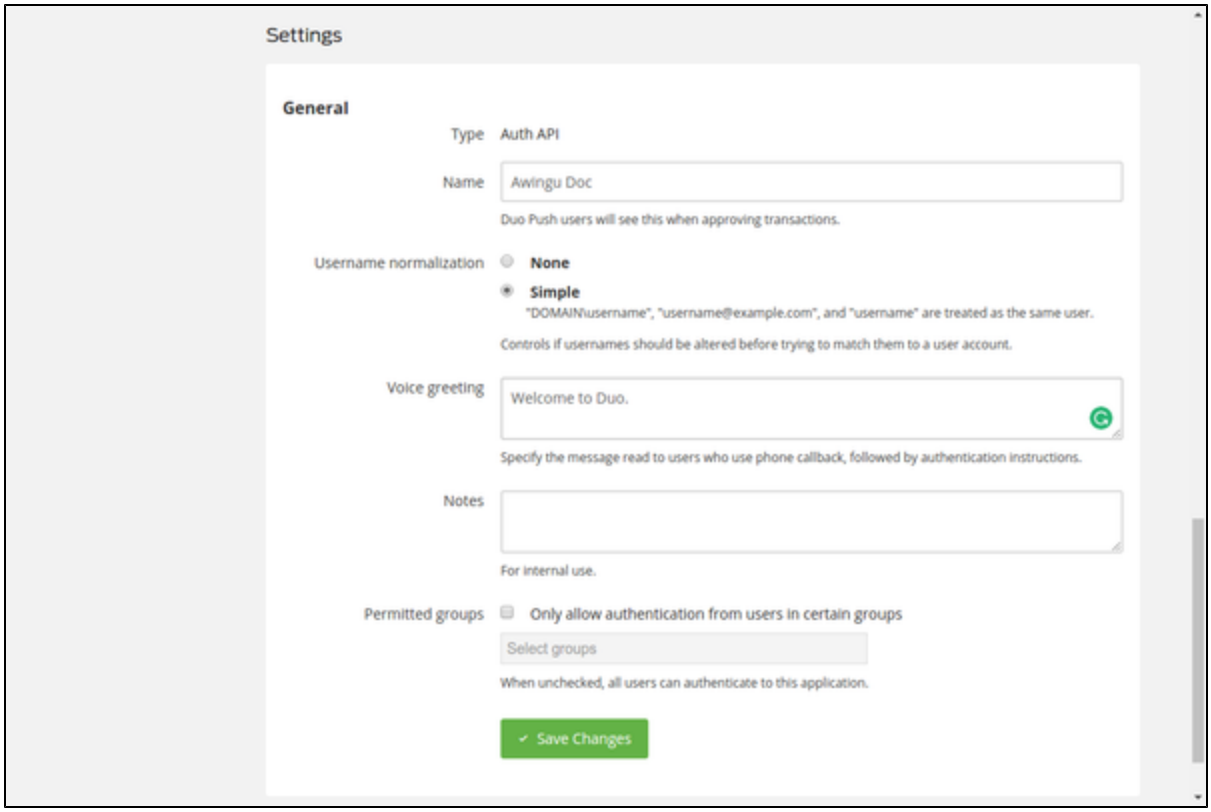
To add your Parallels Secure Workspace application, click *Protect an Application* and select *Auth API* as type.



This will result in a pre-configured application in Duo. The *Details* section of the application provides you with all details required to configure Parallels Secure Workspace later on.



Before moving over to configure Parallels Secure Workspace, we need to change some default values of the Duo settings in the *General* section.



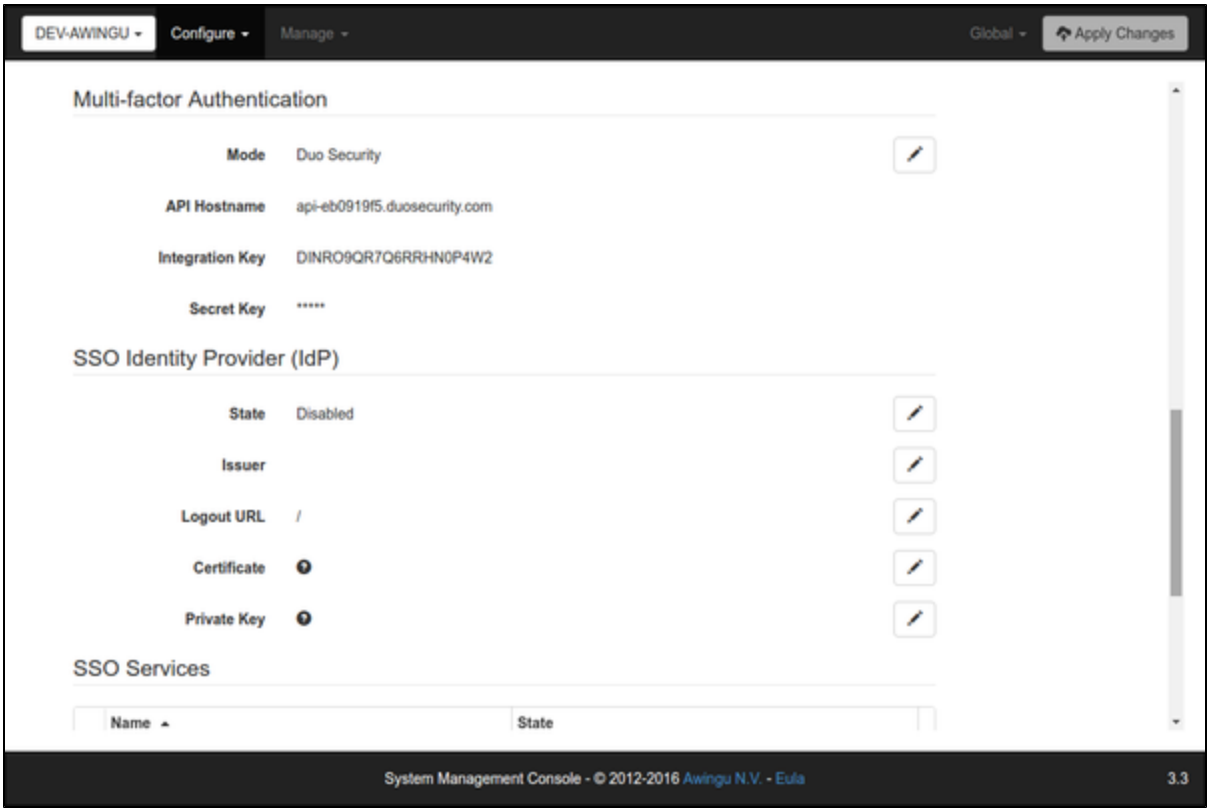
Please make sure the *simple* username normalization is enabled, or all authentication requests will fail. In this section you can also provide a more meaningful name for your Duo Parallels Secure Workspace application.

Save your changes and your Duo application is Parallels Secure Workspace ready.

Configuring Duo in Parallels Secure Workspace

To configure MFA in Parallels Secure Workspace, navigate to *Configure* > *User Connector* for your domain. Please be aware that the MFA configuration is domain specific.

Scroll down to the *Multi-factor Authentication* section and select the *Duo Security* mode.



Enter the beforementioned corresponding values from the Duo portal and press apply.

Now Parallels Secure Workspace is configured to use *Duo* as MFA provider for all users of the selected domain!

Users

To enable *Duo* MFA for your users, the users should be enrolled at *Duo*. They can be enrolled manually, imported or synced with Active Directory.

Please have a look at Duo's *Enrolling Users* documentation (https://duo.com/docs/enrolling_users) to see what option fits best your use case.

Known Limitations

- **Parallels Secure Workspace does not support users with status bypass**
  Duo provides a feature that allows you to configure users to skip MFA. This can be done be setting the user's status to `bypass`. Parallels Secure Workspace does not honour this status and this will prevent the user to sign in.

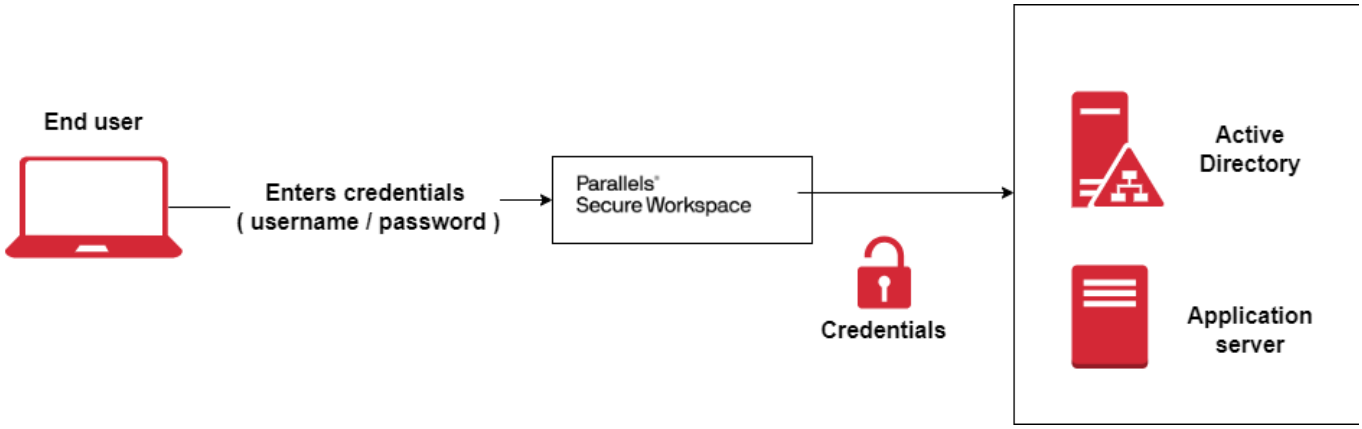
Parallels Secure Workspace Single Sign On (SSO)

Next to the standard username/password login, Parallels Secure Workspace is also able to do a full Single Sign-on (SSO) when using an external Identity Provider.

How does it work?

Standard Login

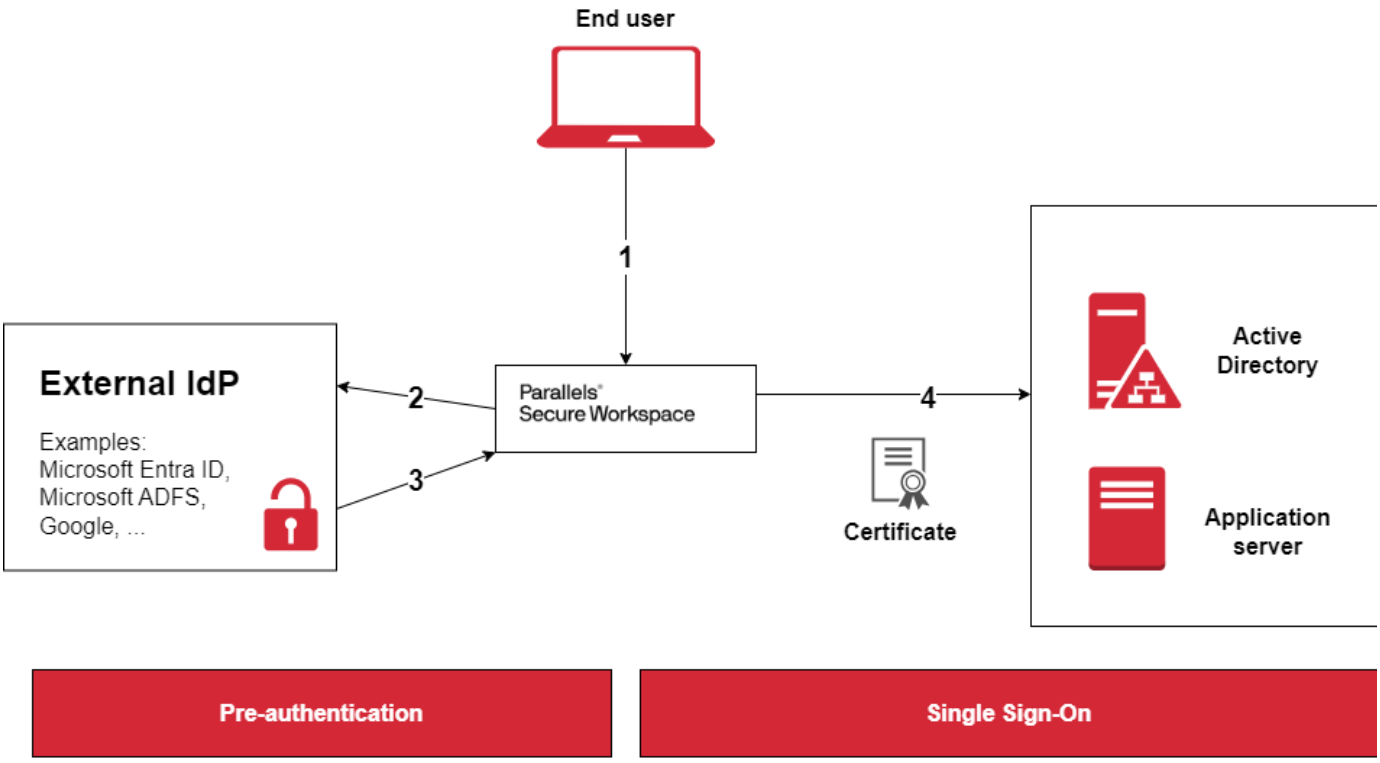
In the standard setup, Parallels Secure Workspace authenticates directly against the Active Directory (AD) with the username/password provided on the Parallels Secure Workspace. It makes a connection over LDAP(s) and if the credentials are valid, it will fetch the security groups over LDAP(s) of the user and build up the Parallels Secure Workspace user profile and landing page. When starting a virtual desktop (VDI) or a remote application (remote app) the credentials are transparently injected into the RDP stream and the VDI or remote app is started.



SSO Login

When switching to SSO, the login becomes a 2-step process.

1. **Pre-authentication:** Parallels Secure Workspace no longer does the authentication of the user itself, but this is handled by an external Identity Provider (IdP).
2. **Single Sign-On:** As the external IDP doesn't expose the passwords and the Microsoft Remote Desktop Protocol (RDP) doesn't support ticket/token-based logins, in the second step, the credential-based login towards back-end systems (remote app, VDI, storage, ...) is replaced by a certificate-based login mechanism.



Configuration

To configure Single Sign-On, several steps need to be completed.

1. Enable pre-Authentication
   a. Add Parallels Secure Workspace as a trusted application on your IdP.
      i. Entra ID (Azure AD)
      ii. Microsoft ADFS
      iii. Google ID
   b. Configure Parallels Secure Workspace for SAML or OpenID connect authentication
   c. Test and Troubleshoot pre-authentication
2. Enable Single Sign-On
   a. Generate a certificate and setup the intermediate SubCA.
   b. Validate if the Microsoft Windows backend is correctly configured for Parallels Secure Workspace SSO.
   c. Configure Parallels Secure Workspace for SSO.

Enabling Pre-Authentication (PreAuth)

Pre-authentication against an external IdP is possible for SAML (v2) and OpenID Connect based IdPs.

In general, Parallels Secure Workspace should be compatible with any IdP that supports these standards. In this manual we describe how to do the setup for following tested IdPs:

- Microsoft Entra ID (Azure AD) (via SAML)
- ADFS (via SAML)
- Google (via OpenID Connect)

End User Flow:

- When a user accesses the landing page, Parallels Secure Workspace will check if the user has a valid authentication token with the configured IdP.
- If this is not the case yet, Parallels Secure Workspace will redirect the browser to the IdP. The user will need to authenticate first against the IdP. If successful, the IdP will redirect the User to the landing page.
- Parallels Secure Workspace will ask the user for their Microsoft Windows password.
- User will be logged in to the Workspace.
- From the Workspace they can start Apps, Desktops and get access to the Drives.

From a technical point of view, Parallels Secure Workspace needs a valid SAML or OpenID Connect ticket before it allows the user to login to the Workspace. As the Microsoft RDP protocol doesn't support SAML or any other ticket-based login mechanisms and as the IdP doesn't expose or include the entered password inside the ticket, users need to enter their Microsoft Windows password (again) before they can log in to the Workspace. The login into the portal and the apps happens via the standard credential-based authentication mechanism.

To get the extra "Windows password" removed you need to upgrade from pre-auth to SSO.

Use Cases:

By enabling this pre-authentication you can enable some extra use cases:

Conditional Access

Parallels Secure Workspace allows access from any device. For some organizations this is not desired and they want to limit access to only managed devices. Via a firewall or reverse proxy in front of Parallels Secure Workspace you can already do some first filtering (for example only allow connections from a specific range of IP addresses) but thanks to the pre-authentication you can use the conditional access features of your IdP to, for example, limit access to Parallels Secure Workspace so login can only be done on managed devices.

See https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices on how to do this when using Parallels Secure Workspace in combination with Microsoft Entra ID (Azure AD).

Add Parallels Secure Workspace as a trusted application into your IdP

Parallels Secure Workspace can work with any external IdP that supports SAML or OpenID Connect. Please check the documentation of your IdP on how to add a trusted application.

The following setups have been tested:

- Microsoft Entra ID (Azure AD)
- Microsoft Entra ID (Azure AD) in combination with OPSWAT
- Microsoft ADFS
- Google

Please check following documentation on how to configure them:

- Setting up Entra ID (Azure AD) as an external IdP for Parallels Secure Workspace
- Setting up Entra ID (Azure AD) with OPSWAT as external IdPs for Parallels Secure Workspace
- Setting up Microsoft ADFS as an external IdP for Parallels Secure Workspace
- Setting up Google as an external IdP for Parallels Secure Workspace

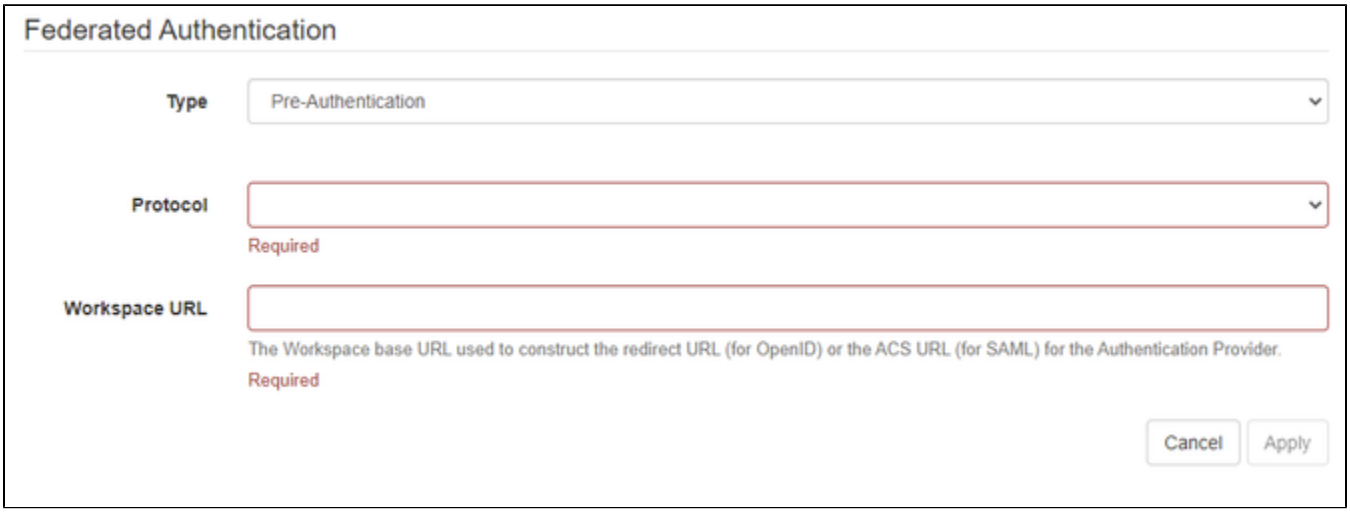
Configure Pre-Authentication

Before you start configuring the pre-authentication make sure there is a host header set on the tenant. Go to **Global > Domains >** Select your domain. Make sure the public DNS name of the Parallels Secure Workspace environment is set in the list of host headers for this domain. So for example if your public url for your Parallels Secure Workspace environment is https://workspace.company.com , then make sure that in the list of host headers "workspace.company.com" is set.

To start the configuration itself of the pre-authentication, log in to Parallels Secure Workspace as an admin and open the system settings: Go to **Configure > User Connector > Federated Authentication** .

Set:

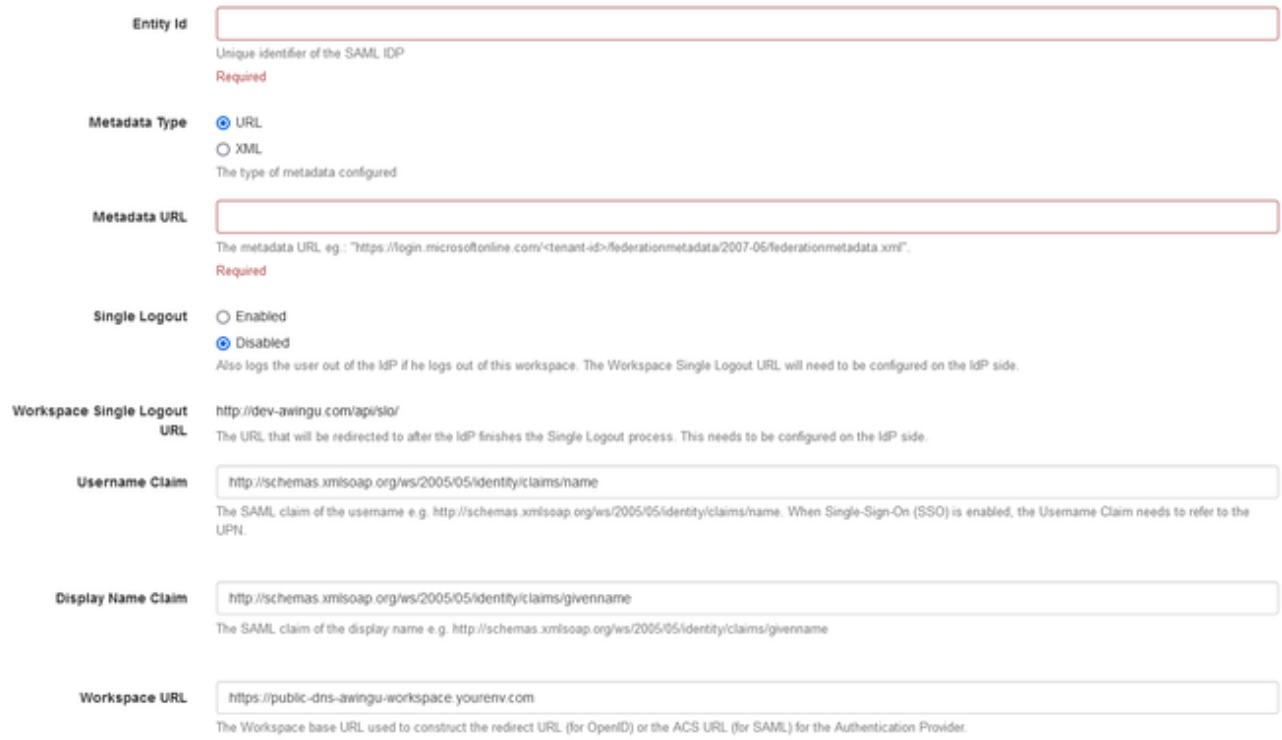
- Type to "Pre-Authentication"
- Select the correct protocol: SAML, SAML with Intermediate IdP or OpenID
- Provide the URL pointing to your Parallels Secure Workspace environment. This URL will be used to construct the return URL you will need in the configuration of the IdP. (for example https://workspace.company.com/).



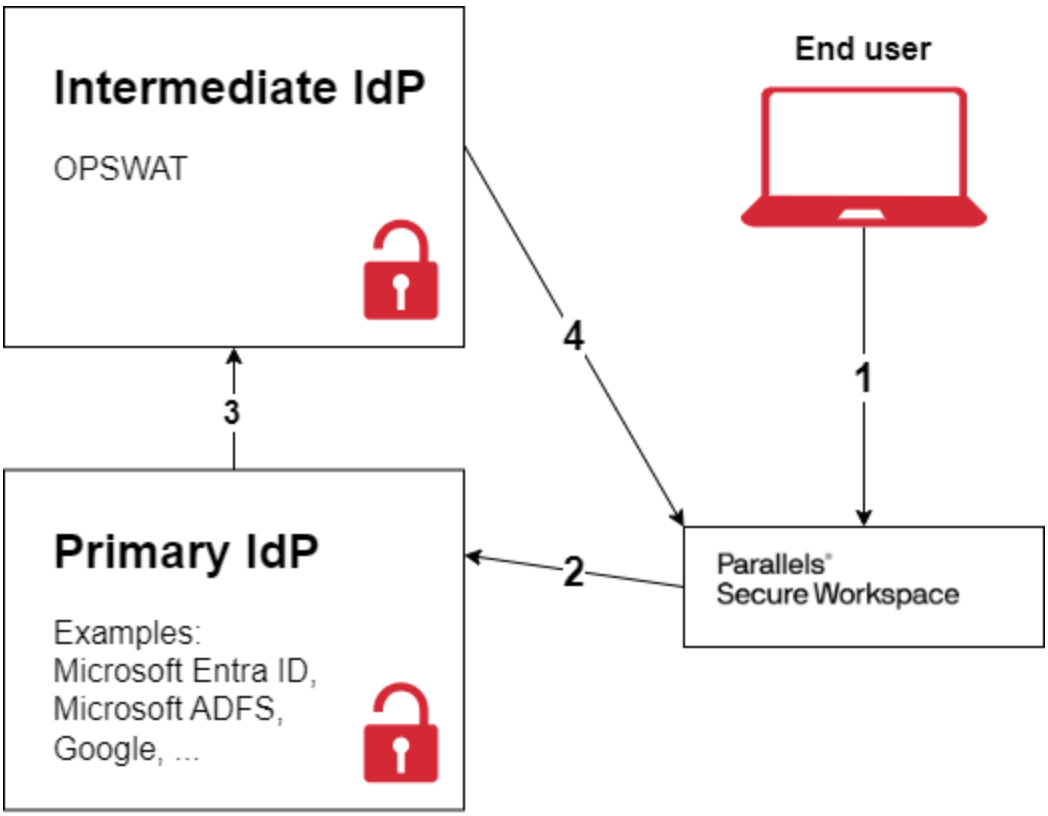
Configure Pre-Authentication with SAML

To use SAML for an external IdP the following fields need to be provided:

- **Entity Id:** The unique identifier on your IdP for the Parallels Secure Workspace application.
  - For Microsoft Entra ID (Azure AD) this is "**spn:**<application-id>" (example spn:1234-5678-90xxxx). The Application ID is a property of the Azure Application (see Setting Up Azure AD as an external IdP for Parallels Secure Workspace)
  - For Microsoft ADFS this is the relying party identifier configured when setting up your relying party trust in ADFS (see Setting Up ADFS as an external IdP for Parallels Secure Workspace)
- **Metadata Type:** How is the SAML Federation Metadata provided? Depending on the capabilities of the used Identity Provider.
  - URL: The appliance should download the metadata at every login attempt using a provided URL.
  - XML: The metadata is uploaded as a static .XML file.
- **Metadata URL:** The URL of the federation metadata document. When using https please make sure the URL is accessible via a public trusted certificate. If your certificate is not publicly trusted, then you can host the metadata.xml file on another web server as a workaround.
- **Metadata XML:** The .xml file providing the federation metadata to upload to the appliance.
- **Single Logout:** Enable this option to make sure the user will also be logged out of the the IdP if he logs out of this workspace. Mind that this only works if the logout is initiated in the front end by the user. Requires configuration on the Identity Provider. See the documentation: Setting up Entra ID (Azure AD) as an external IdP for Parallels Secure Workspace
- **Username Claim URL:** The SAML response received by Parallels Secure Workspace contains different properties (e.g. email, UPN, sAMAccountName, display name,..). Using the Username Claim URL you can specify which property will be used when logging into Parallels Secure Workspace. When Single Sign-On (SSO) is enabled, the Username Claim URL needs to be set to the UPN.
  - When using Azure AD the default value is used (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name).
  - When using ADFS it is best to directly use the UPN (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn).
- **Display Name Claim URL** will be used on the login page of Parallels Secure Workspace when the user successfully logged into the identity provider (e.g. "Welcome David"). The default value will be the claim URL to the given name (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname) property. Possible other claims URIs can be found here: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/the-role-of-claims
- **Workspace URL:** the public DNS name for the Workspace.



Configure Pre-Authentication with SAML and Intermediate IdP



SAML Login flow when using an intermediate IdP:

- When a user accesses the Parallels Secure Workspace landing page, the user will be redirected to the Primary IdP.
- After the user logs in to the Primary IdP, he will be redirected to the Intermediate IdP (Intermediate ACS URL).
- The Intermediate IdP can perform additional checks (device compliance, monitoring, credentials,..).
- When the Intermediate IdP allows the user through, it will redirect him to Parallels Secure Workspace (ACS URL).
- Parallels Secure Workspace then determines if the user is successfully pre-authenticated by validating the SAML response from the Intermediate IdP (using the Intermediate Signing Certificate).

To use SAML with an intermediate IdP the following extra fields need to be provided:

- **Intermediate ACS URL:** The Primary IdP redirects to this URL in case of successful authentication.
- **Intermediate Signing Certificate:** Parallels Secure Workspace uses this certificate to check the SAML response from the Intermediate IdP.

See Setting up Entra ID (Azure AD) with OPSWAT as external IdPs for Parallels Secure Workspace for an example configuration where Microsoft Entra ID (Azure AD) is used as the Primary IdP and OPSWAT as the Intermediate IdP.

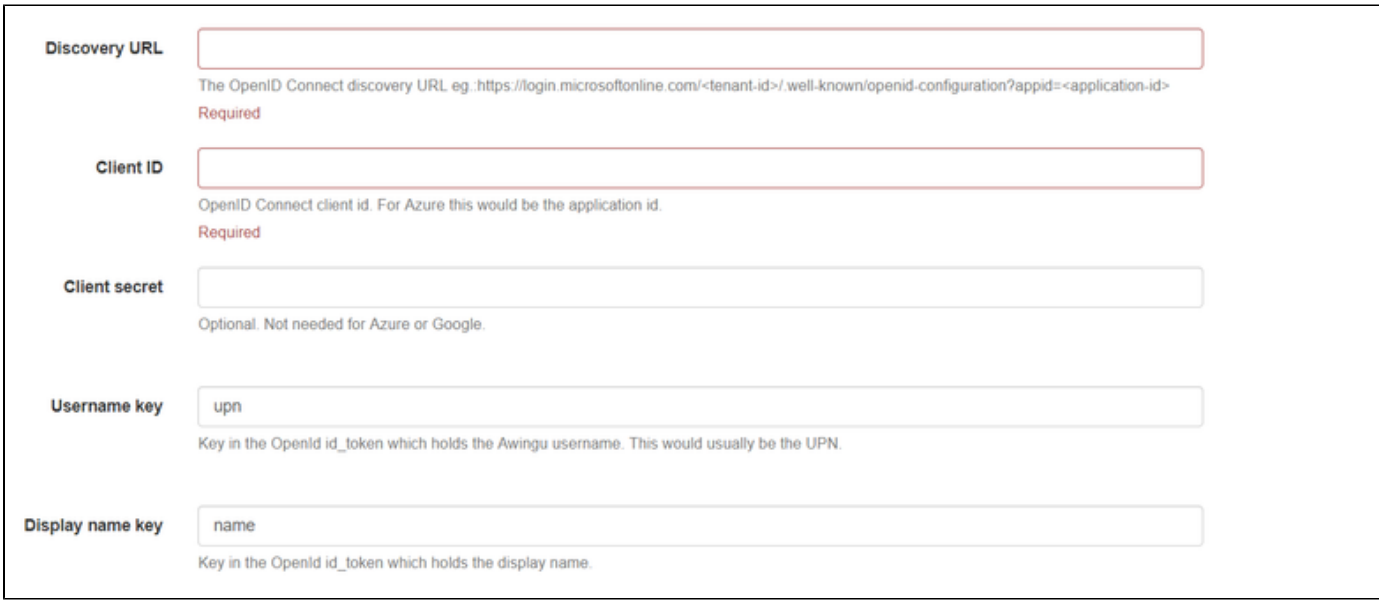
Configure Pre-Authentication with OpenID

To use OpenID for an external IDP the following fields need to be provided:

- **Discover URL:** The OpenID Connect discovery URL.
  - For google this is: https://accounts.google.com/.well-known/openid-configuration (See https://developers.google.com/identity/protocols/OpenIDConnect for more details)
- **Client ID:** OpenID connect client ID
- **Client secret:** *Optional*. For Google & Azure this is not needed and can be left blank
- **IdP Logout URL:** *Optional*. When an URL is provided to logout the user from the IdP, Parallels Secure Workspace will redirect to it after the user logs out. E.g. when using Google as IdP this could be https://www.google.com/accounts/Logout .
- **Username key:** Key in the Open id_token which holds the username.

- For Google use **email**
- For Microsoft Entra ID (Azure AD), use **upn**

- **Display name key:** Key in the Open id_token which holds the display name
  - For Google, use **email**
  - For Microsoft Entra ID (Azure AD), use **name**



Testing and troubleshooting pre-authentication

When testing pre-authentication for the first time, please make sure you use a private or incognito browser window. In some cases there might still be active cookies in your main browser window that prevent the correct login.

If pre-authentication works via incognito windows but not via your normal browser window, then delete your browser cookies from today.

If the configuration is done correctly both on the IdP as well as in the Parallels Secure Workspace configuration you should experience the correct end user flow as described above.

In the event of an issue, this chapter will help you in troubleshooting. We have documented the most common issues.

How to access the system settings when pre-auth has a faulty configuration?

Once pre-authentication is enabled, all Windows based accounts will need to first authenticate against the IdP before they can log in to Parallels Secure Workspace. In the event of an issue with the IdP configuration or Parallels Secure Workspace configuration, the following procedures can be used to access the System Settings. All these procedures **assume that you execute them in a private/incognito browser window** and will only work for **the built-in management user**.

1. Access the Parallels Secure Workspace appliance on a different URL than the one that is linked to your IdP:
   a. In case of a multi-tenant setup login to another tenant where no pre-auth is configured. In this case the tenant must also be administrative to allow modification to the impacted tenant. This procedure will also work with all admin users on the other tenant.
   b. In case of a single tenant or multi-tenant without other administrative domains add a new/other DNS record for the system or try to connect with the IP rather than the DNS name. In this case there might be certificate issues or the extra DNS names may not exist on a reverse proxy in front of Parallels Secure Workspace.
2. Access the Parallels Secure Workspaceappliance via the "noPreAuth" flag: By going to https://workspace.company.com/login?noPreAuth (**case sensitive!** - Adjust the URL to match your environment) you will get the login prompt with username / password. Note that only the built-in management user can still sign in this way.

Parallels Secure Workspace doesn't do a redirect to my IdP

When a user goes to Parallels Secure Workspace, the redirect to the IdP is not working. Instead of being redirected to the IdP, the user gets a login/password prompt and when typing in their username / password an error is shown stating that pre-authentication is required.

This issue mostly happens when either:

1. There is no (or faulty) host header set in the domain settings of Parallels Secure Workspace for this tenant. (**System Settings - Global - Domains**).
2. Parallels Secure Workspace can't access/read the metadata URL.

To fix please check:

- If network connectivity from the Parallels Secure Workspace appliance to the Metadata URL is working. Check via the troubleshoot tools if DNS and network ports are open. If needed, configure Parallels Secure Workspace to use a proxy server (see **System Settings > Global > Connectivity > HTTP Proxy**) to access a public Metadata URL. If no access is possible to the metadata URL, you can also upload the XML file directly on the Parallels Secure Workspace appliance.
- If the metadata URL is hosted on an internal website and the connection is made over https: Make sure the certificate is a public certificate, not a private certificate that is only known in the Microsoft Windows environment. If needed, you can also move the XML file from the internal website to the Parallels Secure Workspace appliance by uploading the file.
- In the domains settings of this tenant the correct public host header for the Parallels Secure Workspaceappliance is set.

Parallels Secure Workspace shows an InvalidNameIDPolicy

This error mostly occurs when using Parallels Secure Workspace in combination with Microsoft DFS.

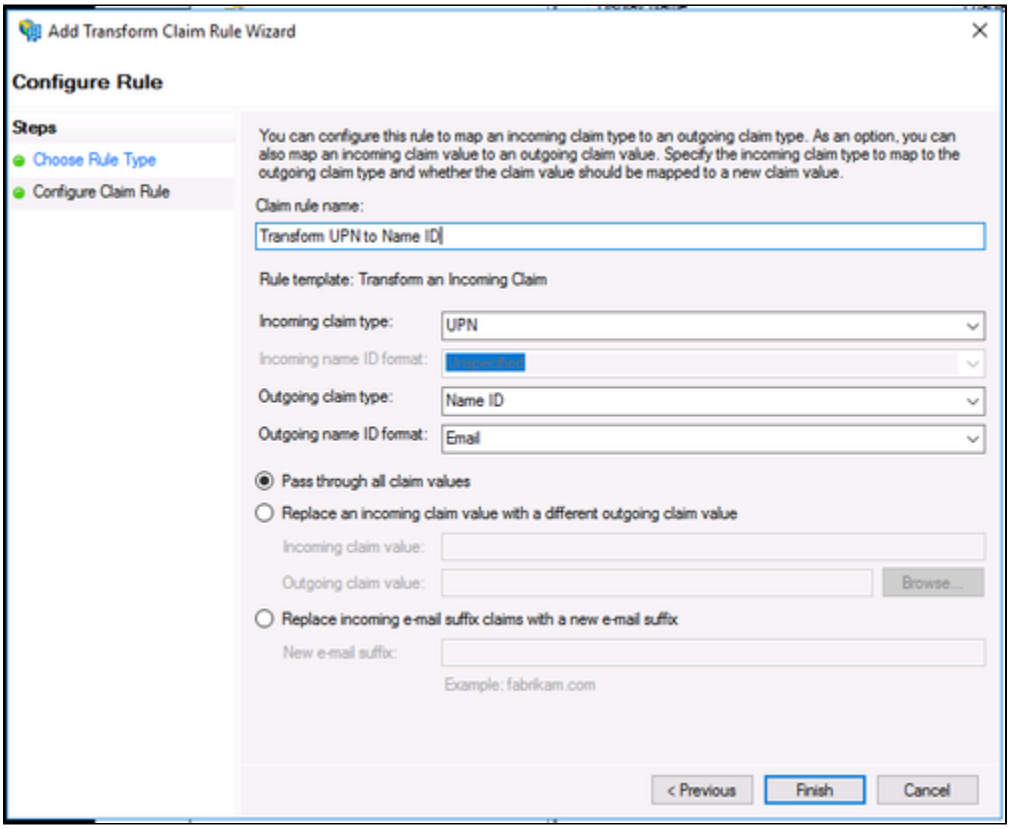
When users navigate to the Workspace, they are redirected to the Microsoft ADFS authentication page. They successfully authenticate against Microsoft ADFS. Upon redirecting to the Workspace, they see the following error:

```
{"error": "The status code of the Response was not Success, was Requester -> urn:oasis:names:
tc:SAML:2.0:status:InvalidNameIDPolicy"}
```

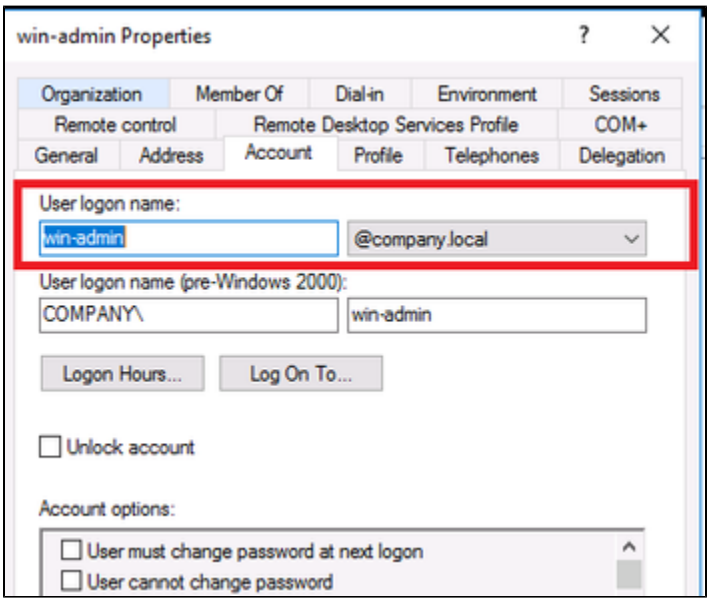
The error could mean one of the following:

- NameID claim is missing
- NameID claim is in the wrong format. The format must be "emailaddress"
- NameID claim is empty

Please check that the transform claim is correctly configured on the ADFS side:



Please also check that the accounts you are using have a valid UPN specified:

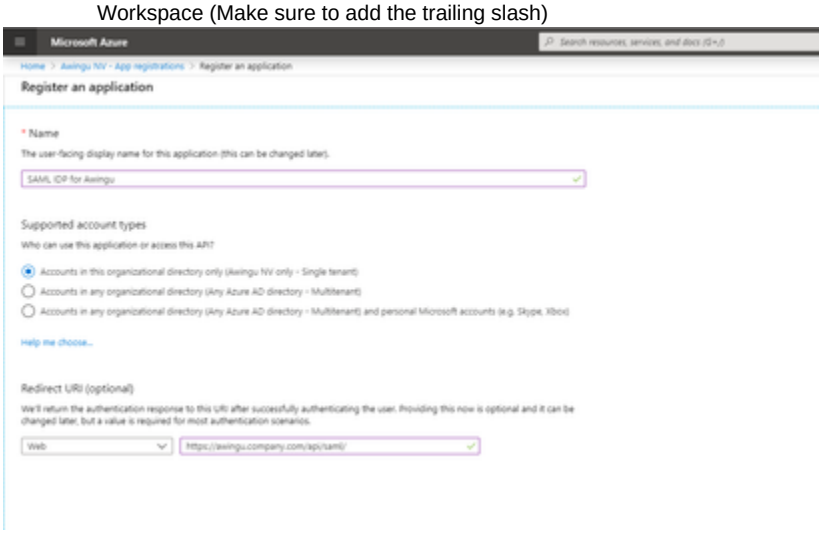


Setting up Entra ID (Azure AD) as an external IdP

SAML pre-authentication can be configured with Azure AD as the identity provider. The following instructions will show how to configure this in Parallels Secure Workspace and in Azure AD.

Register a new Azure Application

1. Login to the Azure Portal
2. Navigate to Azure Active Directory
3. Select from the side bar: *App registrations*
4. Select: *New Registration*
5. Provide a name and supported account type
6. Add redirect URI:
   a. Set the type to Web
   b. Provide the following URL: https://workspace.company.com/api/saml/ where "http://workspace.company.com" points to your Workspace (Make sure to add the trailing slash)



Collect the needed information to complete the setup on the Parallels Secure Workspace appliance

There are two properties that we will need from the Azure Application during the configuration in Parallels Secure Workspace:

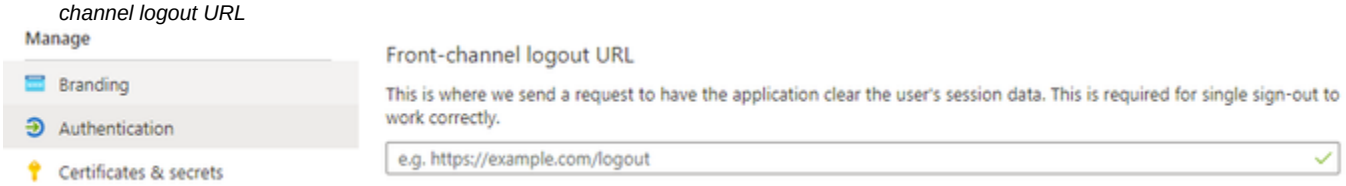
- Application ID (format: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx) which can be found in the properties of the Azure Application on the Overview page of the app.
- Federation metadata document URL (format: https://login.microsoftonline.com/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/federationmetadata/2007-06/federationmetadata.xml) which can be found on the dialog that appears when clicking Endpoints on the Overview page of the app.

Configuration for Single Logout

During the configuration of the IdP in the Federated Authentication section of Parallels Secure Workspace, the Single Logout feature(SLO) can be enabled. When enabled, the user will also be logged out of the IdP when logging out of Parallels Secure Workspace.

The following configuration is required on the IdP:

1. Open the previously created Application in the Azure Portal
2. Click *Authentication* in the left menu
3. Add the Workspace Single Logout URL (shown in the Federated Authentication configuration in Parallels Secure Workspace) to the *Front-channel logout URL*



Note: Only front-channel logout is supported. If the users closes his browser during the logout process, the user might still be logged in to the IdP.

Setting up Entra ID (Azure AD) with OPSWAT as external IdPs

SAML pre-authentication can be configured with Azure AD as the Primary IDP and OPSWAT as the Intermediate IDP. The following instructions demonstrate how to configure this in Parallels Secure Workspace, in Azure AD and OPSWAT.

Register a new Azure Enterprise Application

1. Login to the Azure Portal
2. Navigate to Azure Active Directory
3. Select from the side bar: *Enterprise applications*
4. Click *Add* and *Create your own application*
5. Provide a name and choose *Integrate any other application you don't find in the gallery (Non-gallery)*
6. Collect the needed information by clicking on *Single sign-on* in the left menu and *SAML* as the single sign-on method.
    a. Copy the App Federation Metadata URL(1).
    b. Download the SAML Signing Certificate (Base64)(2).
    c. Copy the Login URL(3).

Configure OPSWAT

1. Login to the OPSWAT MetaAccess console
2. Add Identity Provider:
    a. Navigate to *Secure Access > Access Methods.*
    b. Click the *Identity Providers* tab.
    c. Click the *Create New Identity Provider* button.
    d. Provide a name and upload the previously downloaded SAML Signing Certificate (Base64)(2) from the Azure Enterprise Application.
3. Add Protected App:
    a. Navigate to *Secure Access > Protected Apps.*
    b. Click the *Add Protected Application* button
    c. Select *IdP Method.*
    d. Select the previously created IDP (Choose from existing IDPs).
    e. Fill in the form:
        i. Choose an Application Name.
        ii. Define an Access Mode:
            1. Monitor: Audit logs will be created, access will not be restricted.
            2. Enforced: You will only be able to login if you install the OPSWAT MetaAccess client. You will get a link to download this if you try to login without it being installed.
        iii. IdP Login URL: Provide the previously copied Login URL(3) from the Azure Enterprise Application.
        iv. App ACS URL:
            1. Sign in to Parallels Secure Workspace and Open the System Settings
            2. Navigate to the Configure > User Connector > Federated Authentication section
            3. Select Pre-authentication or Single sign-on as Type (See Enabling Single Sign-On (SSO) for the additional configuration steps to enable Single sign-on).
            4. Select *SAML with Intermediate IdP* as the protocol.
            5. Copy the read-only field *ACS URL* and use this as the App ACS URL in the Protected App form.
        v. Click *Add*
    f. Collect the needed information by opening the newly created Protected App and clicking the *SSO Setup Instructions* tab.
        i. Copy the ACS URL(4).
        ii. Download the Certificate(5).

Update the Azure Enterprise Application

1. Login to the Azure Portal, navigate to the Enterprise Applications and open the recently created Enterprise Application.
2. Click *Single sign-on* in the left menu
3. Click the *Edit* button of the first section (*Basic SAML Configuration)*
    a. Specify an Entity ID(6) and copy this value.
    b. Add the copied ACS URL from OPSWAT as a Reply URL(4).

Enable Pre-authentication with Intermediate IdP

1. Log in to Parallels Secure Workspace and open the System Settings
2. Navigate to the Configure > User Connector > Federated Authentication section
    a. **Entity Id:** Add the copied Entity ID(6) from the step before.
    b. **Metadata Type:** URL
    c. **Metadata URL:** The previously copied Metadata URL (1).
    d. **Intermediate ACS URL:** The previously copied ACS URL from OPSWAT (4)
    e. **Intermediate Signing Certificate:** The previously downloaded certificate from OPSWAT(5).
3. See enabling pre-authentication for the general configuration.

Setting up ADFS as an external IdP

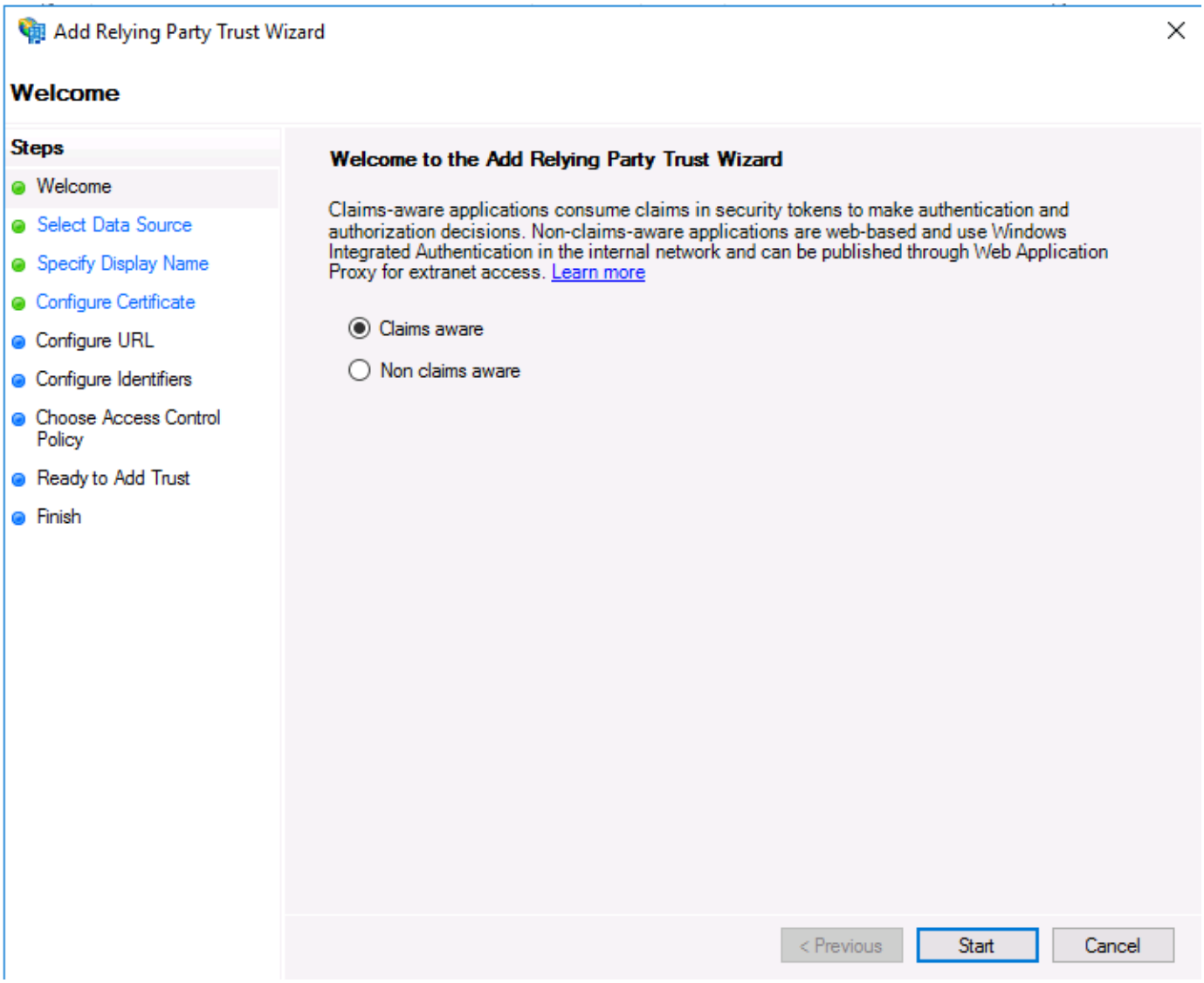
To configure Parallels Secure Workspace with Microsoft ADFS as the external IdP, you first need to add Parallels Secure Workspace as a "Relying Party Trust" in ADFS, after this we need to set up the correct claims to be passed to Parallels Secure Workspace.

Before you start, make sure that you know your Parallels Secure Workspace Base URL.

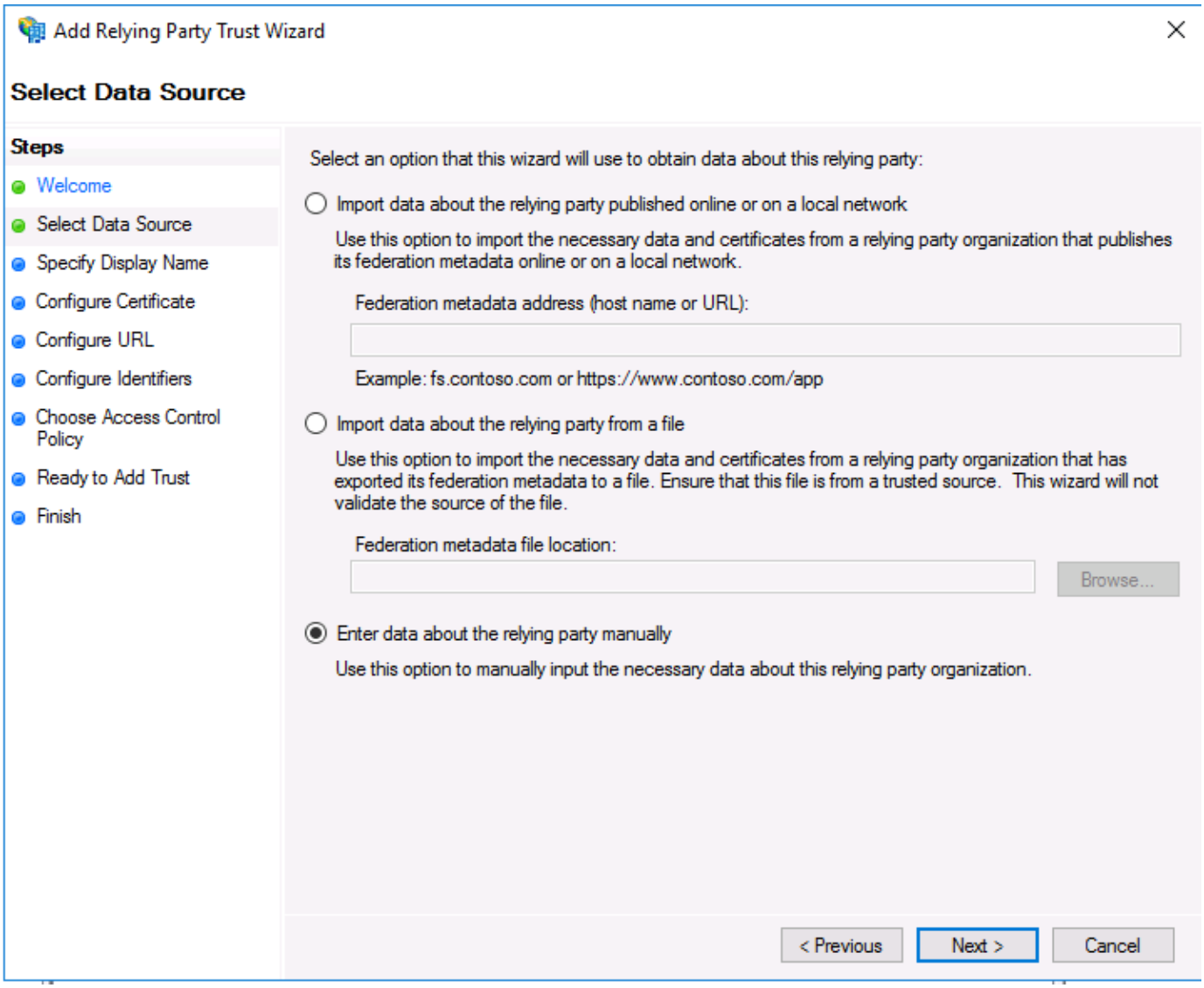
Add Parallels Secure Workspace as a relying party trust:

Go to your ADFS host and start the "AD FS Management Tool", select Relaying Party Trusts and right-click on it, then open the "Add Relaying Party Trust ..." wizard

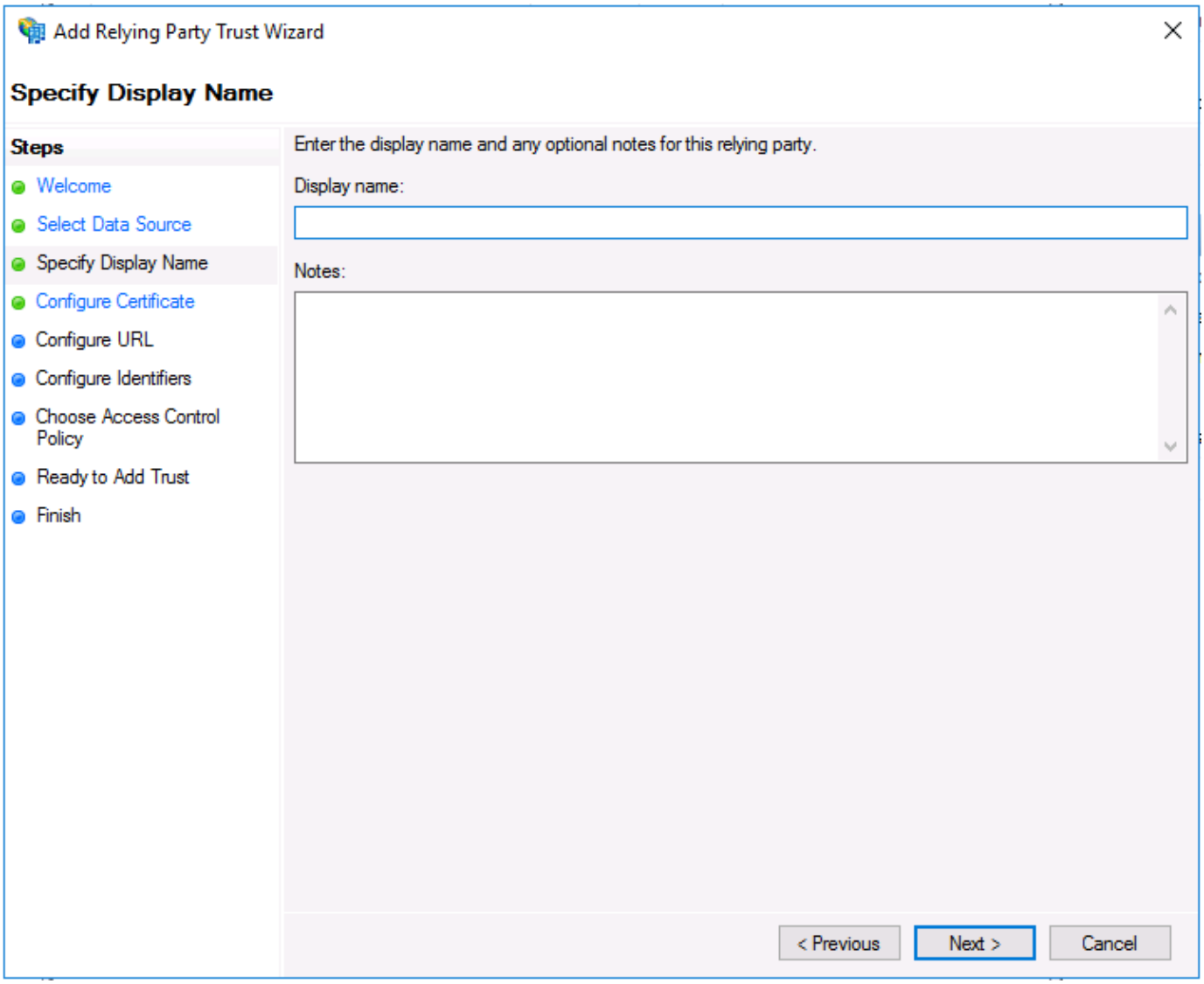
On the welcome screen select "claims aware" and click on start



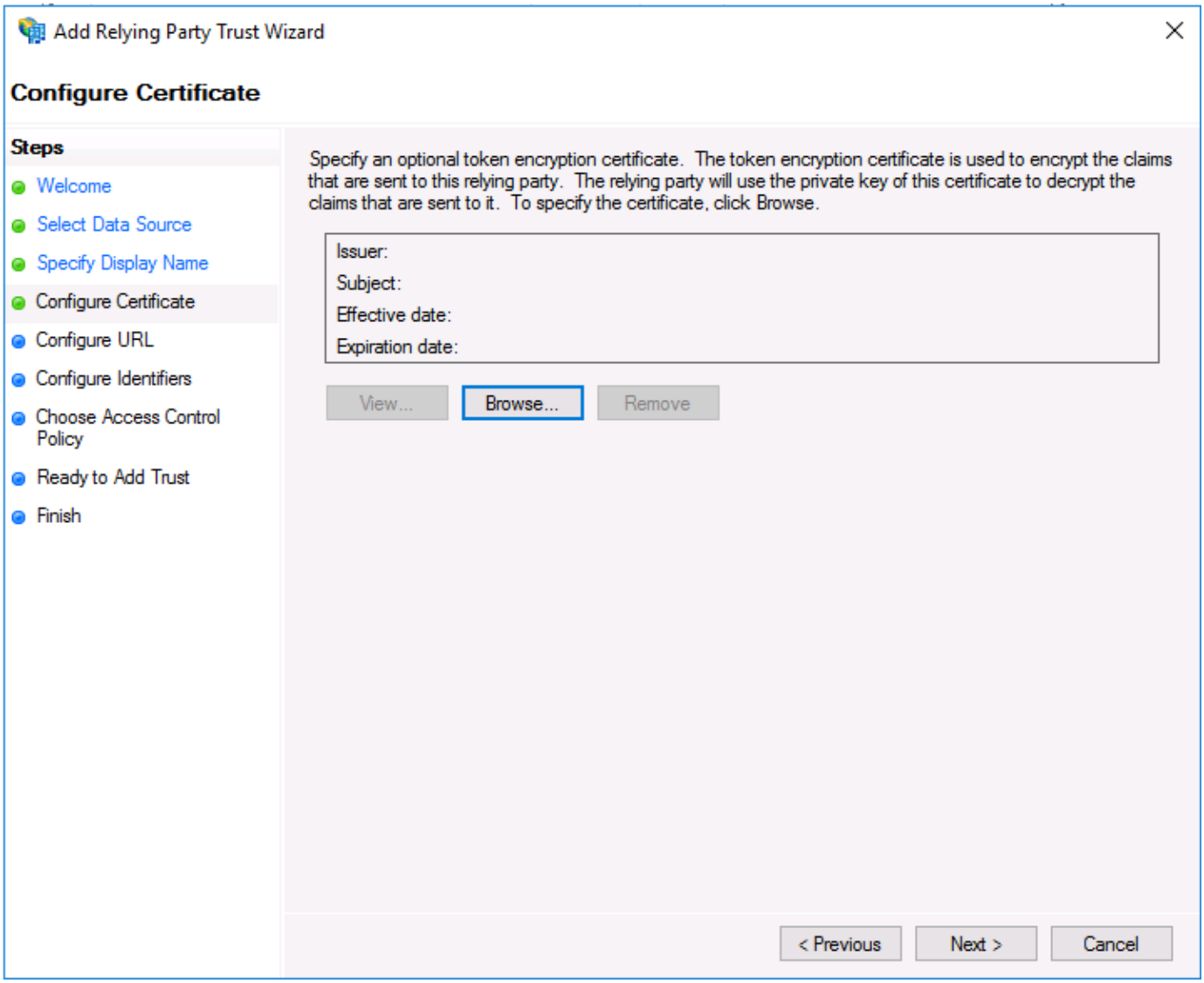
On the Select Data Source page select "Enter data about the relying party manually".



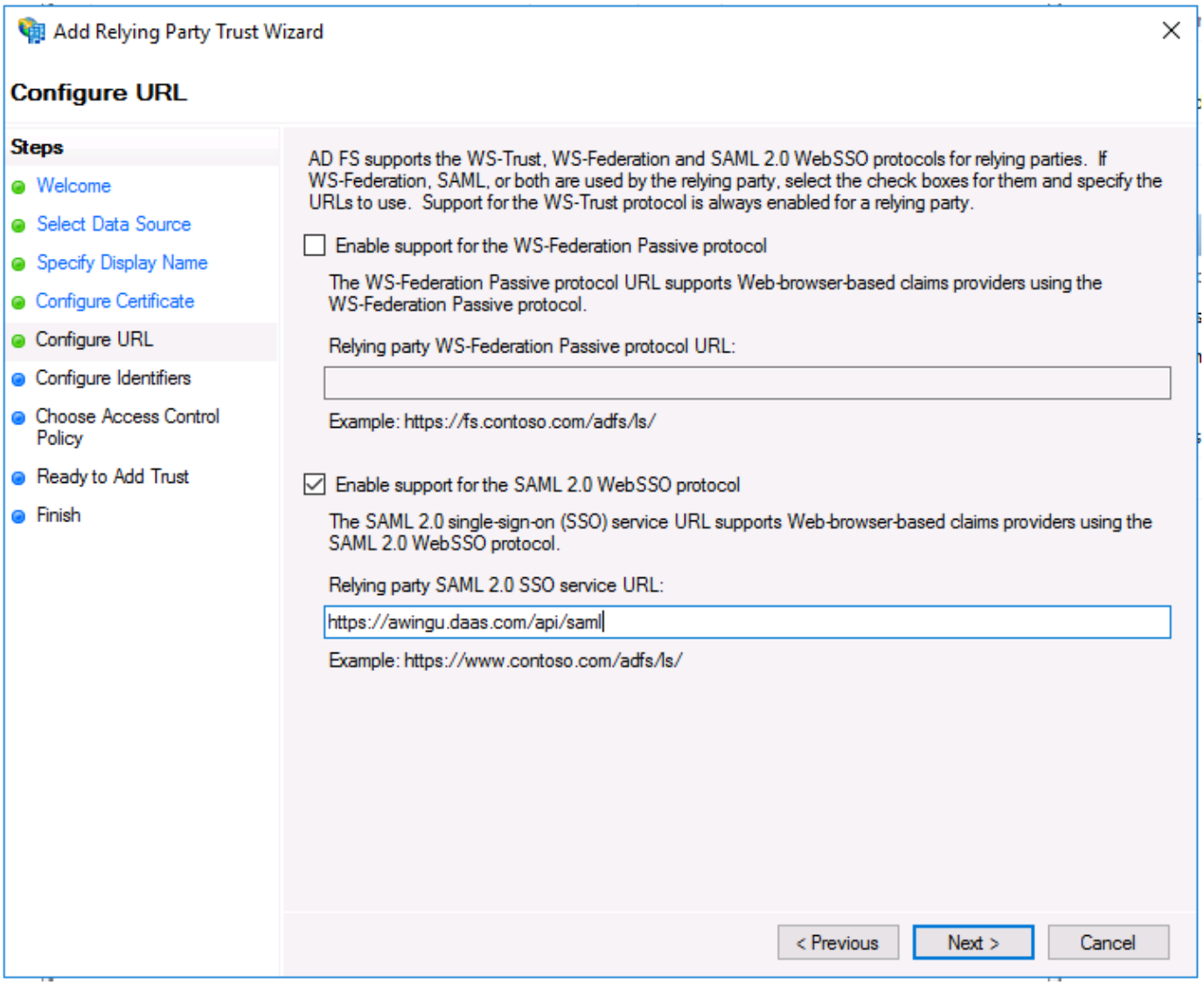
Select a Display Name. This will be the name that is displayed in the overview of all relying party trusts.



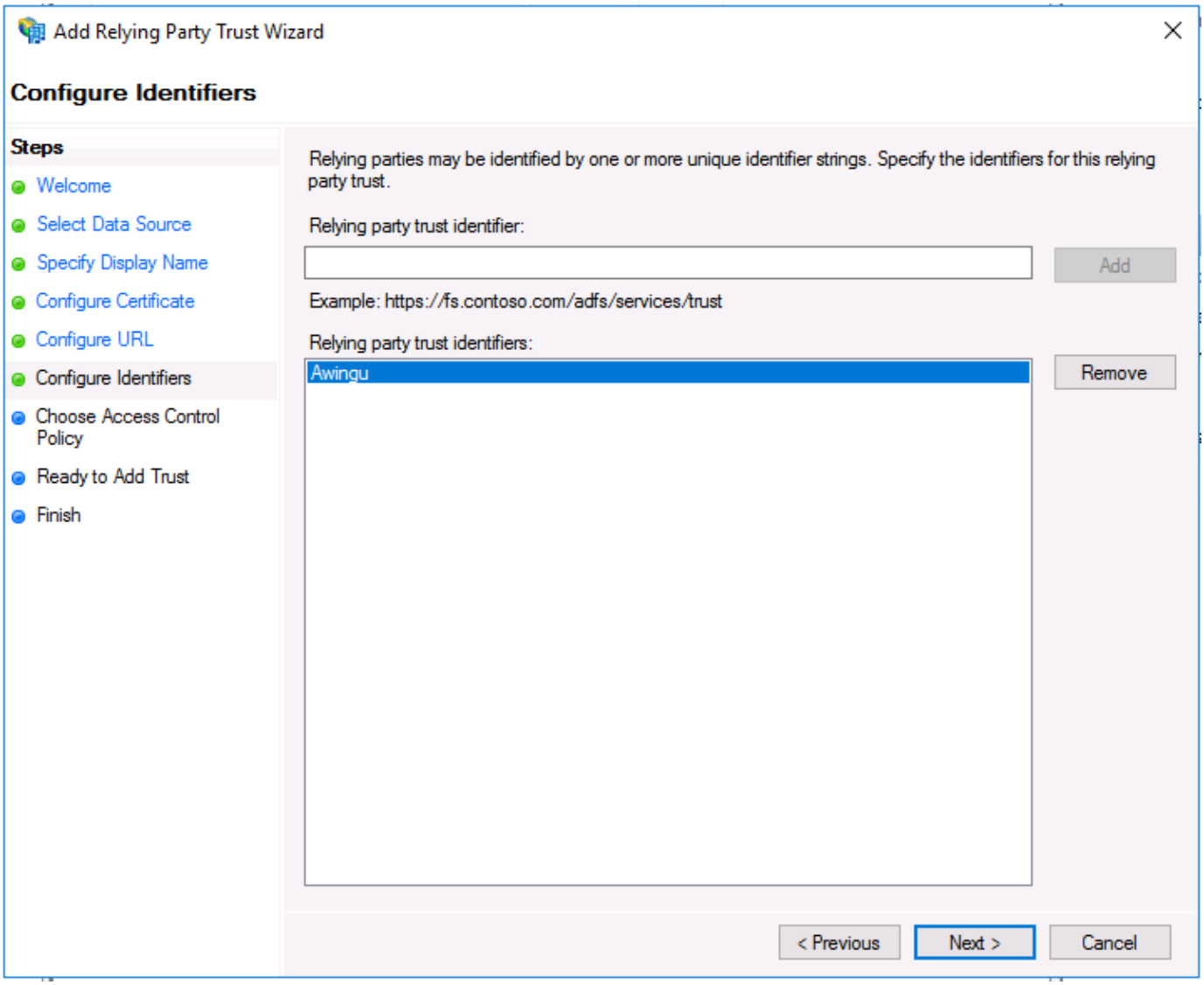
Parallels Secure Workspace doesn't need an extra certificate to encrypt the claims. Leave this blank.



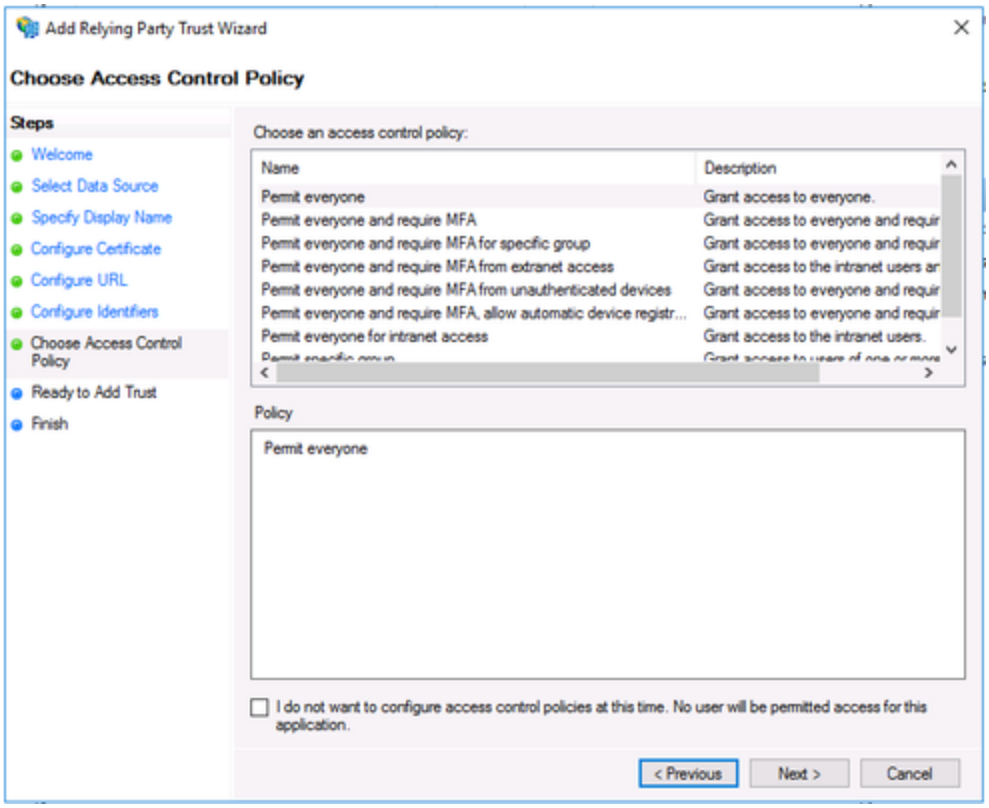
Select the SAML 2.0 WebSSO protocol and set the URL to your Parallels Secure Workspace SAML URL. The URL can be found in the pre-authentication configuration in System Settings, but is typically your Workspace base URL + /api/saml. So for example: https://workspace.company.com/api/saml .

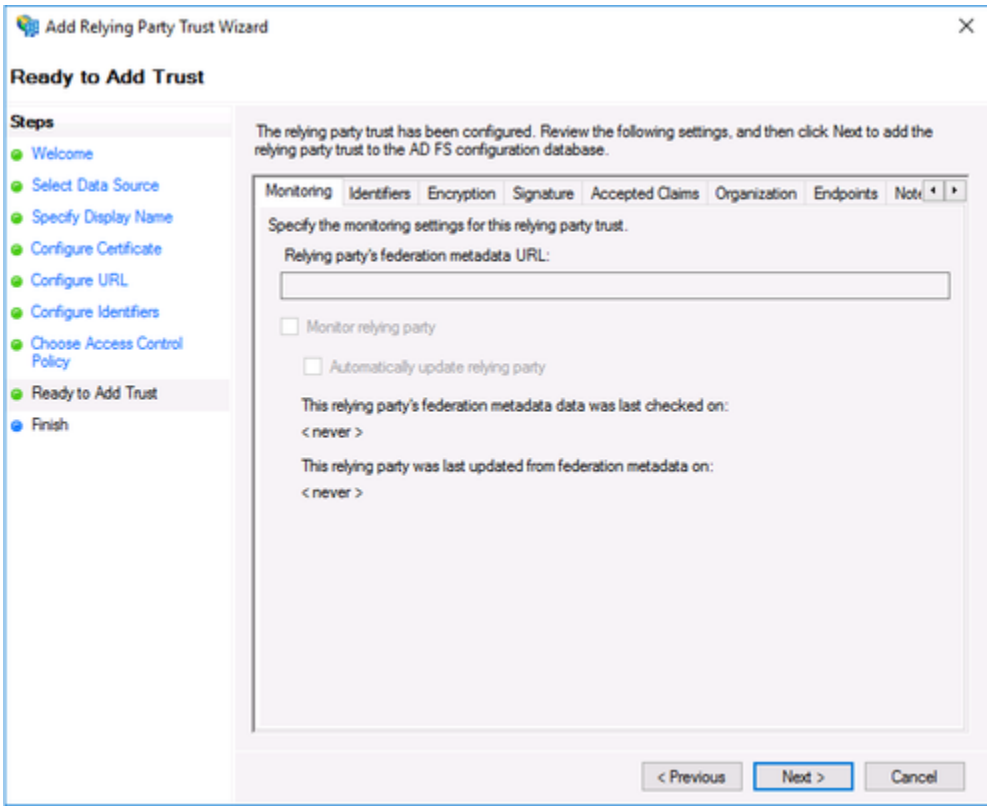


This field should correspond to the "identity ID" specified in the Parallels Secure Workspace pre-authentication configuration.



The rest of the configuration can be done with default settings, no changes needed:





Add the necessary claims

Once the "Trusted Relying Party" is create you can add claims by selecting the relying party trust and then in the actions menu choose the "Edit Claim Issuance Policy ..."

First - We will select the Active Directory attributes that will be sent as claims to Parallels Secure Workspace.

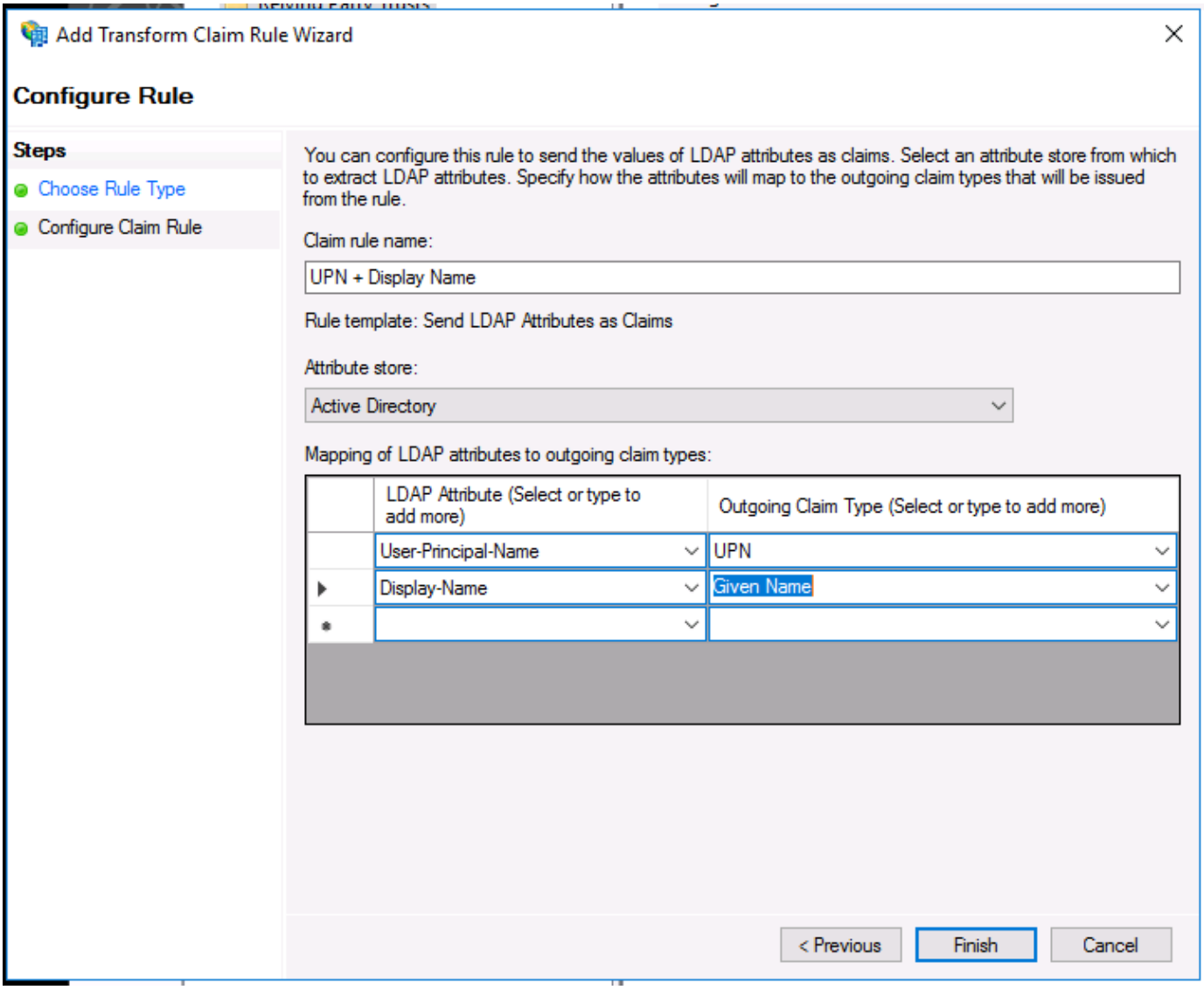
Add a rule based on the "Send LDAP Attributes as Claims" template:

Set the Attribute store to: Active Directory

Add 2 Claims:

- User-Principle Name UPN
- Display-Name Given Name

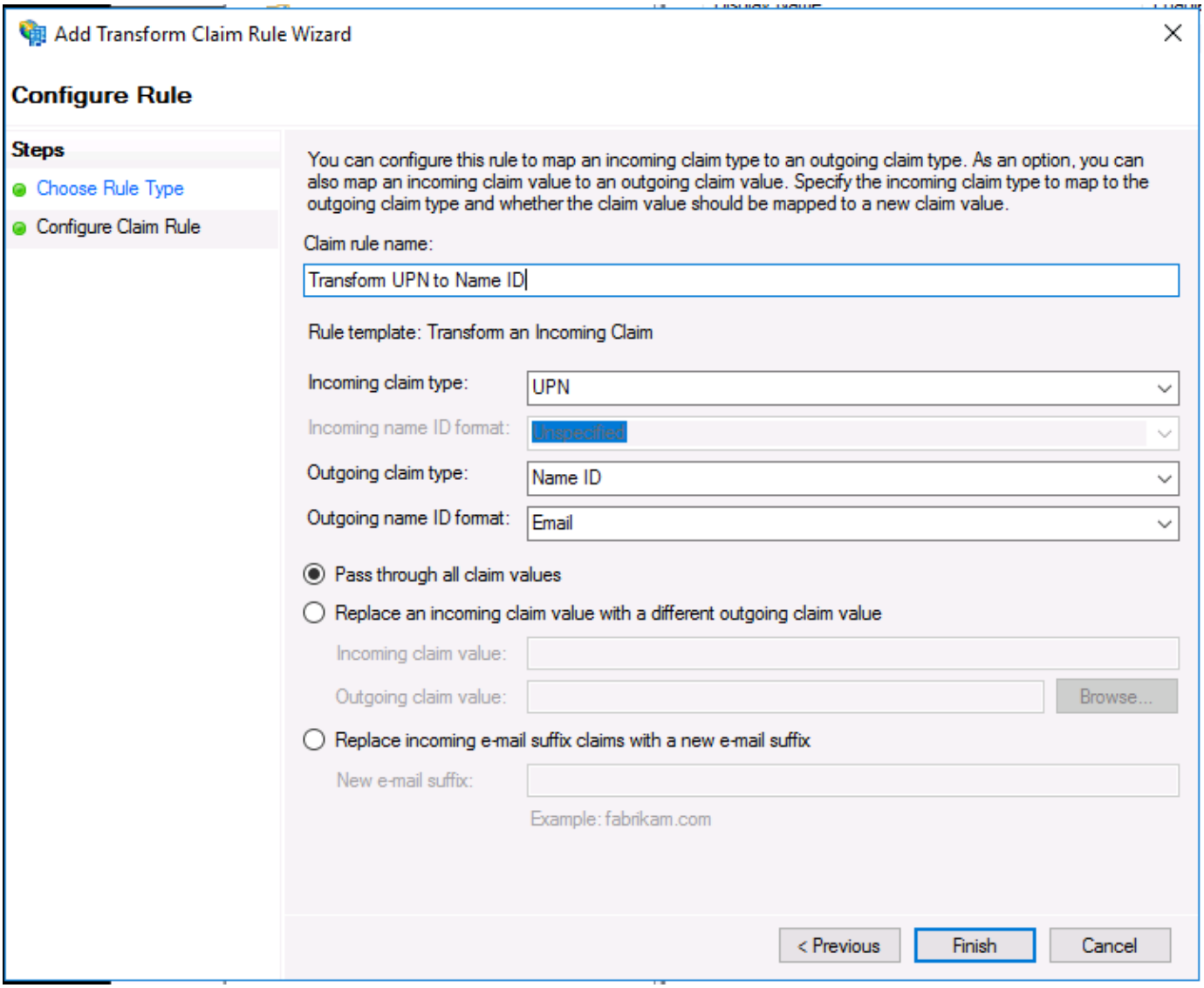
In this case User-Principle Name and Display-Name will be sent to Parallels Secure Workspace.



Second - We will add the mandatory Name ID claim.

Add a rule based on the "Transform an Incoming Claim" template:

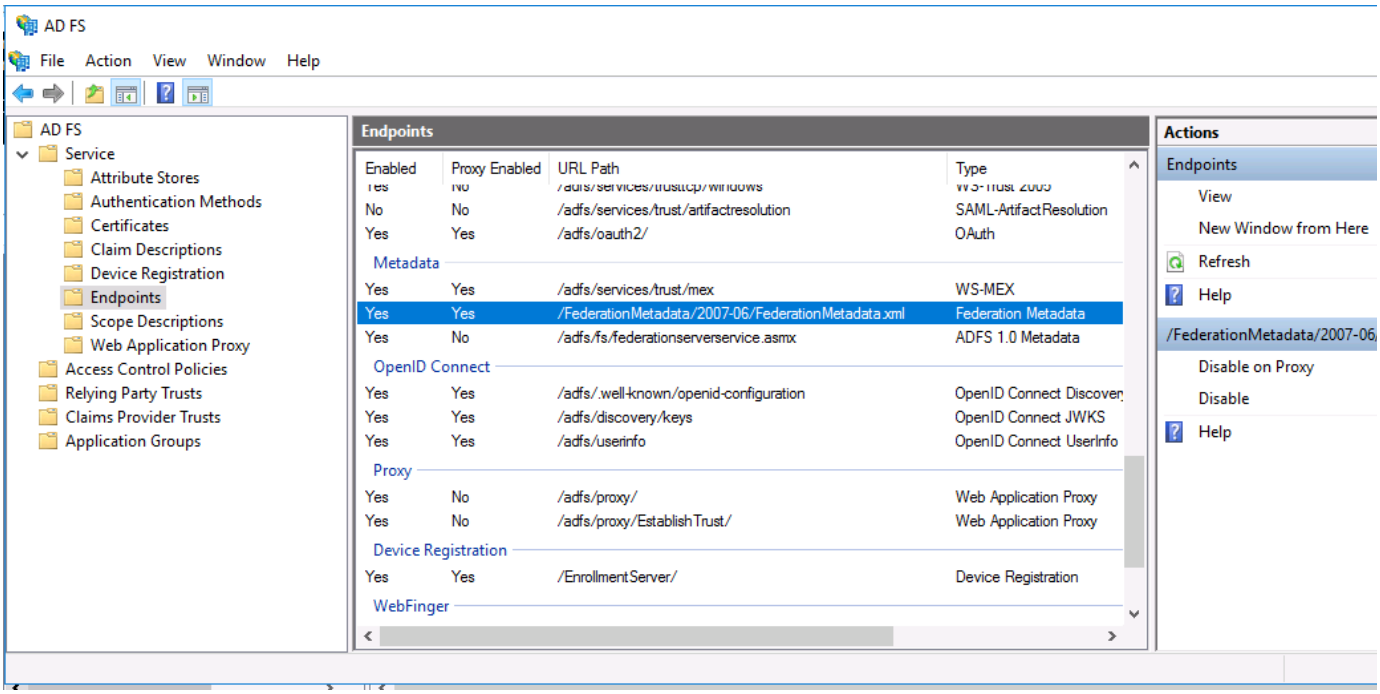
As the name ID field is a mandatory field in the ADFS setup and the format must be Email, we need to add a transform rule that sets the Name ID field based on the existing UPN.



Collect the needed information to complete the setup on the Parallels Secure Workspace appliance

There are two properties that we will need during the configuration in Parallels Secure Workspace:

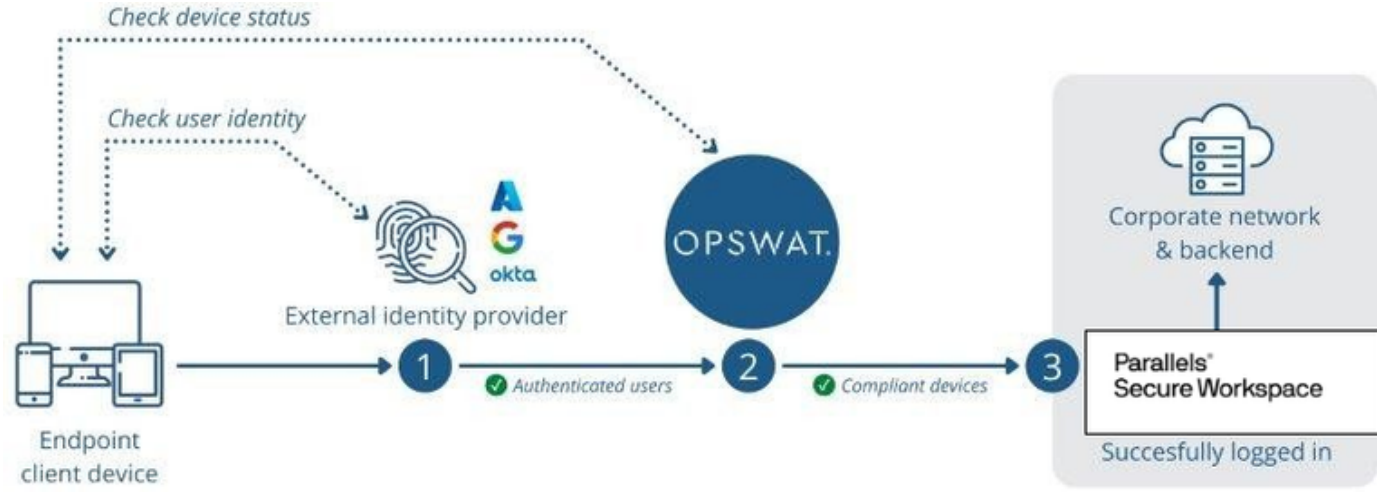
- Relying Party Trust Identifier. This is the value chosen during the wizard setup of the relying party trust. This will correspond with the Entity ID configuration in Parallels Secure Workspace
- Federation metadata. This can be found in the AD FS management tool under Service > Endpoints > Metadata > Federation Metadata .



Setting up ADFS with OPSWAT as external IdPs

Next to setting up Parallels Secure Workspace with a single IdP like ADFS. It is also possible to set up Parallels Secure Workspace in combination with multiple, chained, IdPs.

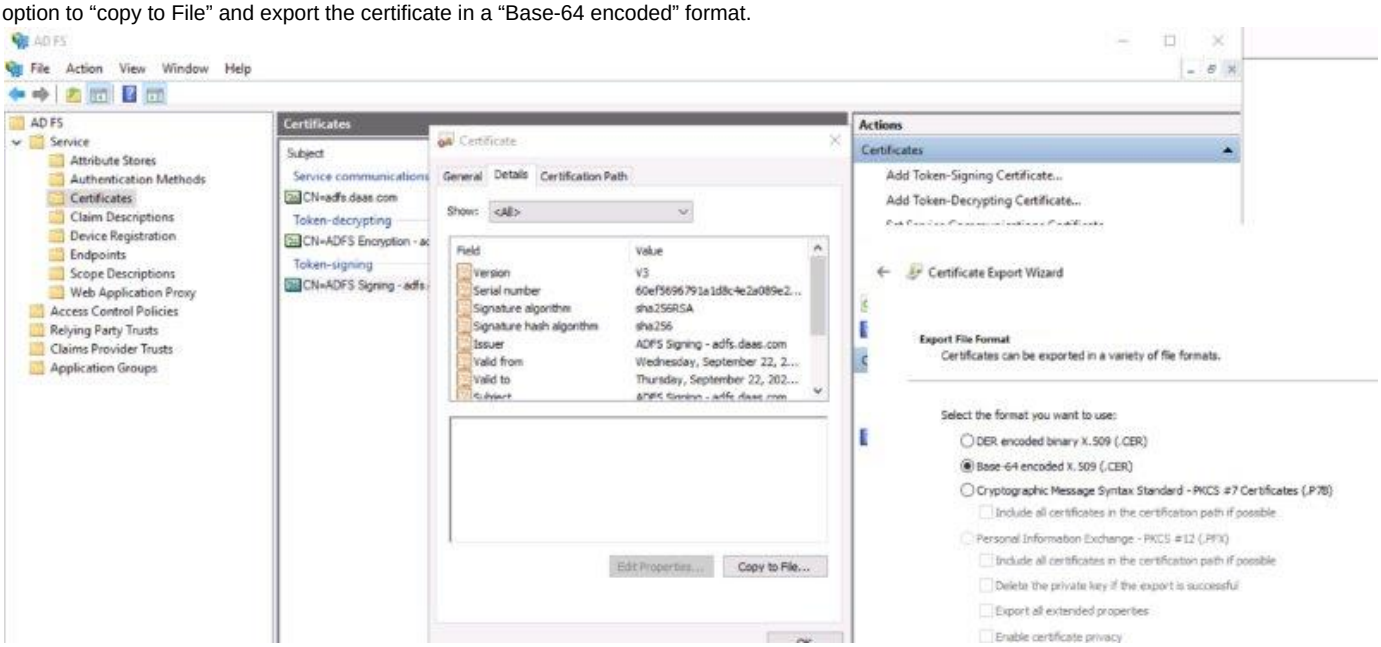
In this case, we are going to configure Parallels Secure Workspace in combination with ADFS for the user validation part and then with OPSWAT to validate the device. For more information on OPSWAT have a look at https://docs.opswat.com/macloud-sdp .



First, ensure that Parallels Secure Workspace in combination with ADFS is working. Once this is working, extend the setup to add OPSWAT into the configuration. See Setting up ADFS as an external IdP for instructions on this.

Step 1: Export the token-signing certificate from your ADFS

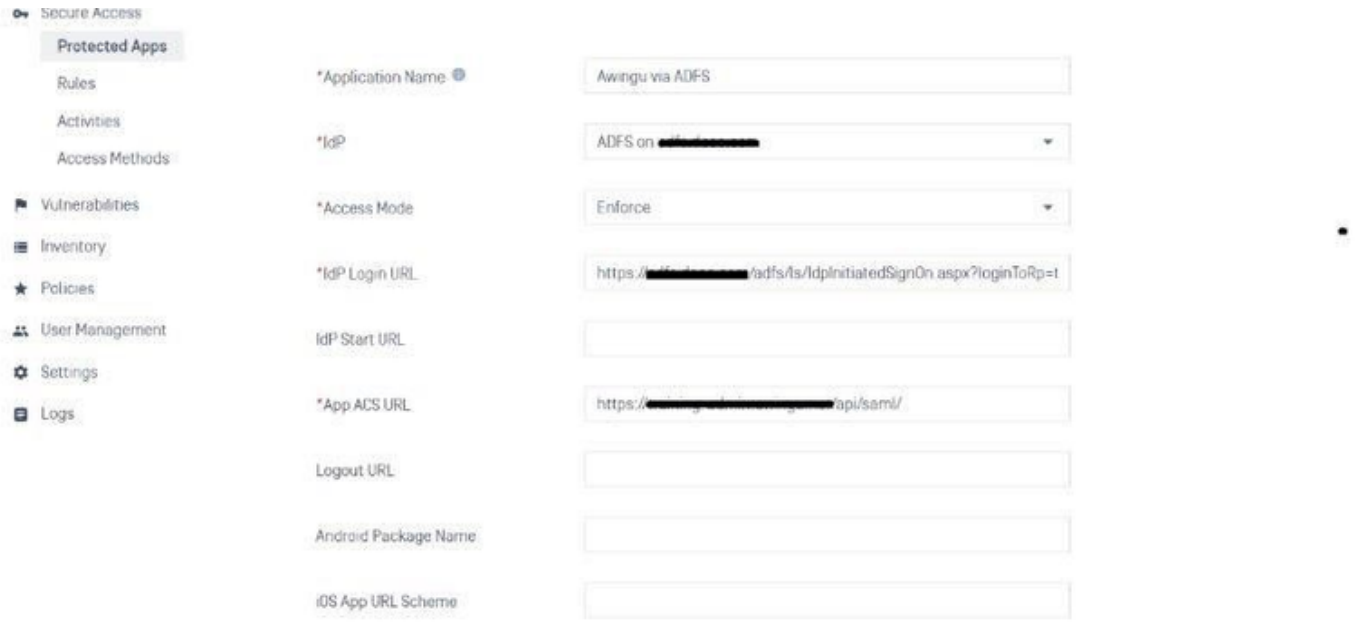
Login to the ADFS configuration panel, go to **Services > Certificates** and select the "**Token-signing**" certificate. Under details, you will see an option to "copy to File" and export the certificate in a "Base-64 encoded" format.



Step 2: Configure OPSWAT

If not yet done add your ADFS as an "Identity Provider": Login to your OPSWAT console and under "Secure Access" "Access Methods" add select "Create New Identity Provider".

When asked for the IdP Certificate upload the ADFS certificate downloaded in the previous step.



Now add in OPSWAT a new protected application:

Select “Secure Access” “Protected Apps” “Add Protected App”.

When asked for the method select: “IdP Setup” and select in the dropdown list your ADFS IdP you have added in the step before.

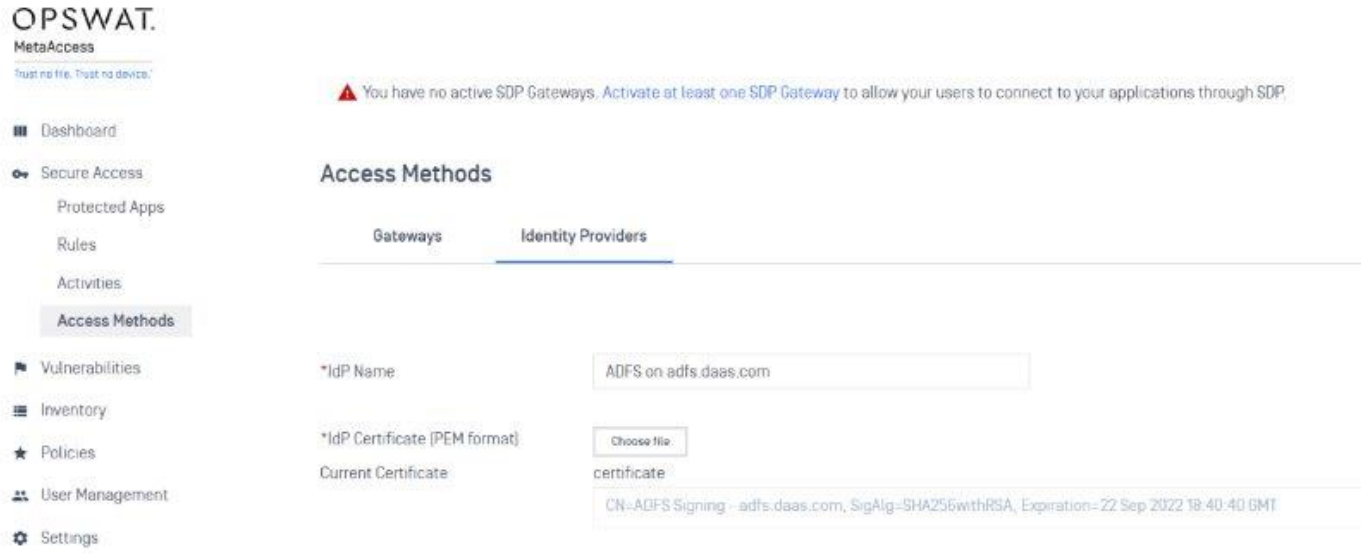
Use following parameters:

- *Application Name:* Free text.
- *IDP:* if not yet done select the ADFS IDP added in the step before
- *Access Method:*
  - Select Enforce if you want to make sure only trusted devices can login.
  - Select Monitor if you want to only log the connections from non-trusted devices.
- *IdP login URL:* Set this value to https://<your.adfs.url>/adfs/ls/IdpInitiatedSignOn.aspx?loginToRp=<RelayingPartyTrust>

RelayingPartyTrust can be found on the ADFS configuration and is the identifier of this ADFS Relaying Party Trust. So for example set the URL to : https://adfs.mycompany.com/adfs/ls/IdpInitiatedSignOn.aspx?loginToRp=Workspace

- *App ACS URL:* Set this to the value you can find in Parallels Secure Workspace under **System Settings > Configure > User Connector: Federated Authentication > ACS URL.**

In most cases this will be similar to https://workspace.company.com/api/saml/



Once the application is added you will get 2 sets of information back from OPSWAT:

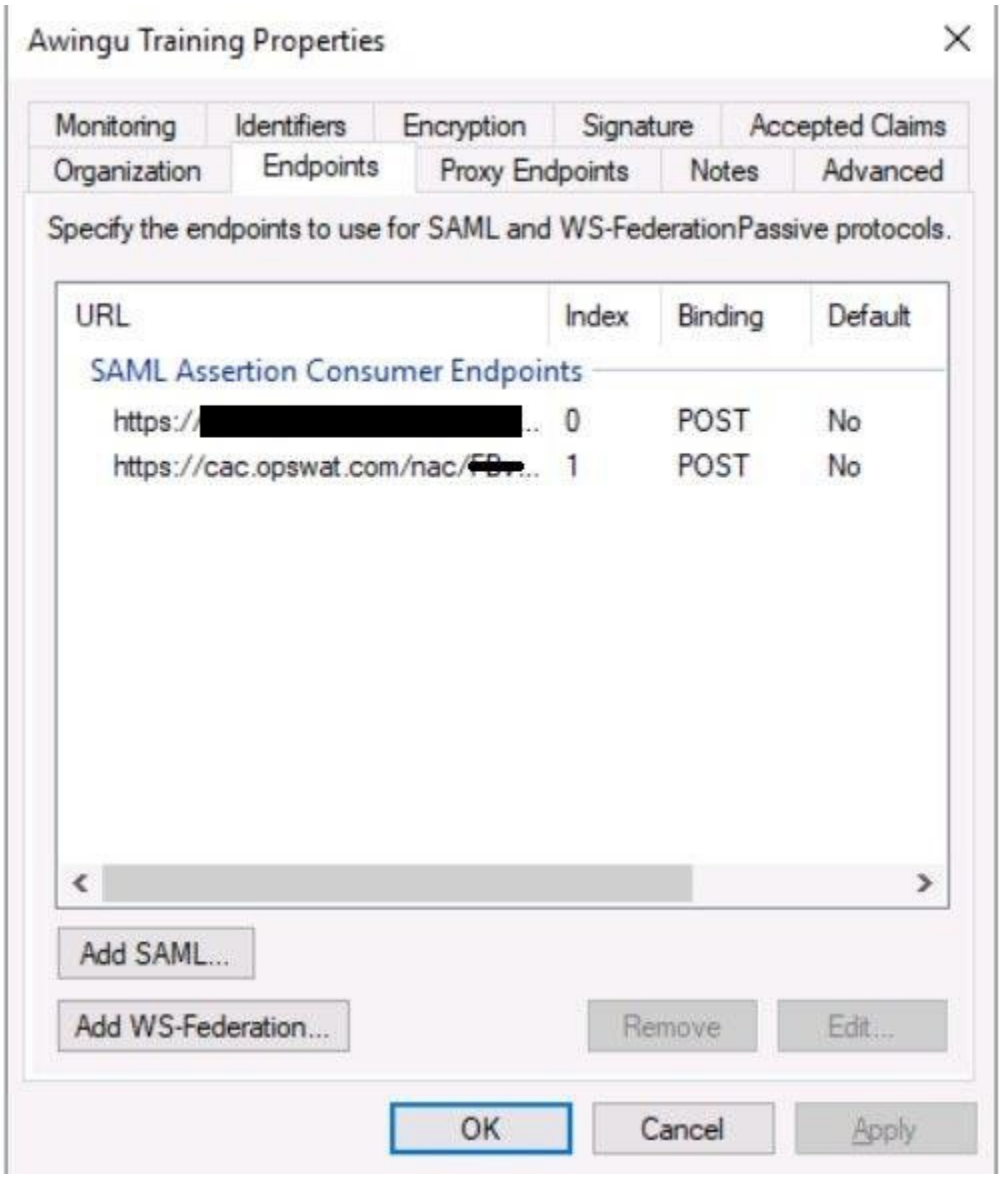
1. An ACS URL that needs to be added to the Identity provider. The URL looks like https://cac.opswat.com/nac/XXXXXXXXX/check /<your_app>
2. An OPSWAT Certificate. Download the certificate to your local computer

Step 3: Add the OPSWAT ACS URL to ADFS

Go back to the ADFS configuration and right-click on the relying party trust and select “properties”.

Goto the “Endpoints” tab and click on “Add SAML”

Select “Endpoint Type”: SAML Assertion Consumer & “Binding”: POST
Set the Index to 1
Set the Trusted URL to the ACS URL received when creating the OPSWAT protected app (https://cac.opswat.com/nac/XXXXXXXXX/check /<your_app>)



Step 4: Configure Parallels Secure Workspace

Go to the Parallels Secure Workspace **System Settings > Configure > User Connector > Federated Authentication.**

Change **protocol** to “SAML with Intermediate IDP”.

2 extra fields become visible:

- Intermediate ACS URL: Set this to the same ACS URL received when creating the OPSWAT protected app (same as the one added in the step before in ADFS).
- Intermediate Signing Certificate: upload the certificate you received when creating the OPSWAT protected app.
-

Check if all fields that were previously filled in with the standard ADFS settings, are still filled in as before. Click on “Apply”.

Step 5: Test if it works

1. Open a incognito/private browser window. Go to the Workspace URL.
2. You should be redirected to ADFS.
3. After successfully authenticating against Microsoft ADFS, there should be a redirection to OPSWAT.
4. After successful device validation:
   a. In case of “enforced” mode, there should be a redirection to Parallels Secure Workspace.
   b. In case of “monitor” mode, you will briefly see an OPSWAT spinner and then arrive on Parallels Secure Workspace.
5. If in Parallels Secure Workspace the federated authentication is set to Single sign-on, you will arrive directly in the Workspace. If it is set to pre-authentication you will have to provide your Microsoft Windows password to get in.

Setting up Google as an external IdP

OpenID Connect pre-authentication can be configured with Google as the identity provider. The following instructions will show how to configure this in Parallels Secure Workspace and in Google.

Register a new

1. Login to the Google Developers console and go to the credentials API page: https://console.developers.google.com/apis/credentialsf
2. First, add the domain on which Parallels Secure Workspace is hosted to the list of Authorized Domains
   Select *OAuth consent screen* *Authorized Domains*
   Add the domain to the list of authorized domains. (for example, if your Parallels Secure Workspace is hosted on workspace.company.com, add company.com to the list)

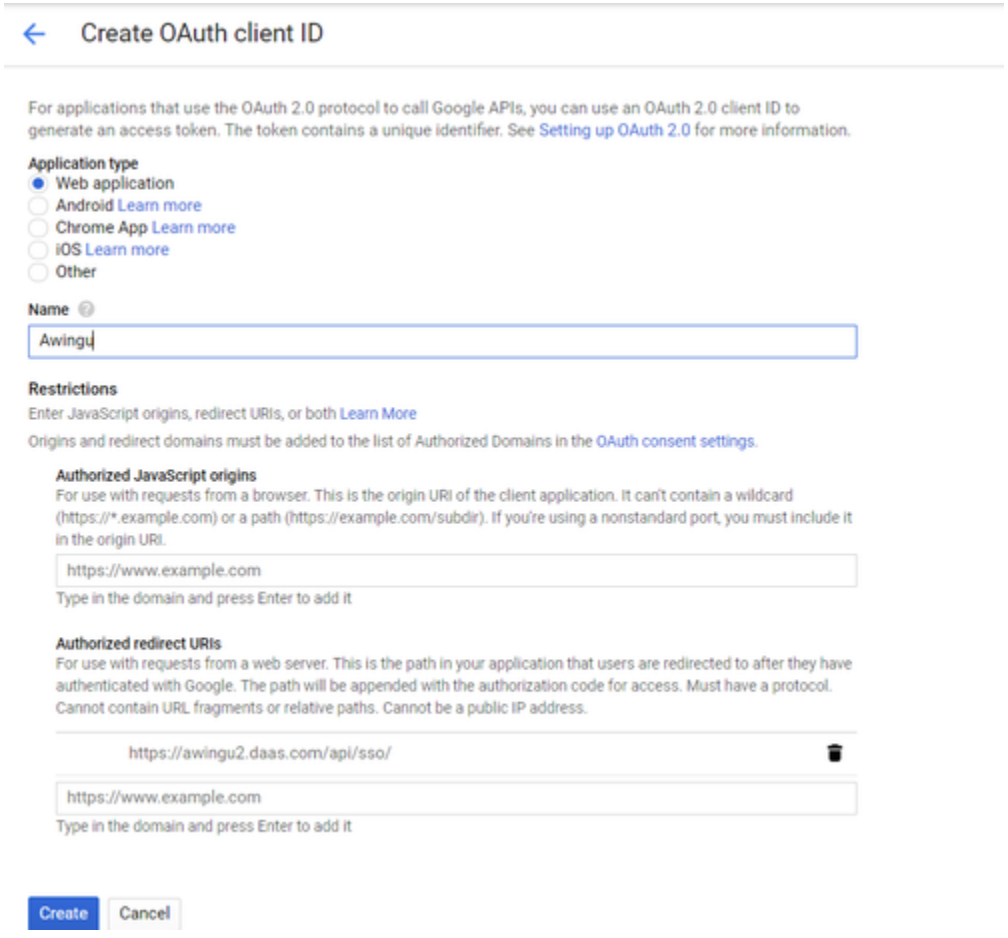
   Click on **Save** at the bottom of the page.

   See https://support.google.com/cloud/answer/6158849?hl=en&authuser=2#authorized-domains for more details

3. Add Parallels Secure Workspace as an OpenID Connect.
   Select *Create Credentials* *OAuth Client ID*

   Application Type: Web application
   Name: Display name of these credentials in the Google Developers console
   Authorized Redirection URLS: https://workspace.company.com/api/sso/ where "workspace.company.com" points to the Workspace. (Make sure to add the trailing slash)

   Click on **Save** at the bottom of the page.



   See https://developers.google.com/identity/protocols/OAuth2 for more details

Collect the needed information to complete the setup on the Parallels Secure Workspace appliance

There are 3 properties that we will need from the Azure Application during the configuration in Parallels Secure Workspace:

- **Client ID** and **Secret** are provided by the Google API after finishing the above setup.
- The **Discovery URL** for Google is:

  ```
  https://accounts.google.com/.well-known/openid-configuration
  ```

Enabling Single Sign-On (SSO)

Before enabling Single Sign-On (SSO) first make sure that the **pre-authentication is working** with your external identity provider (IdP).

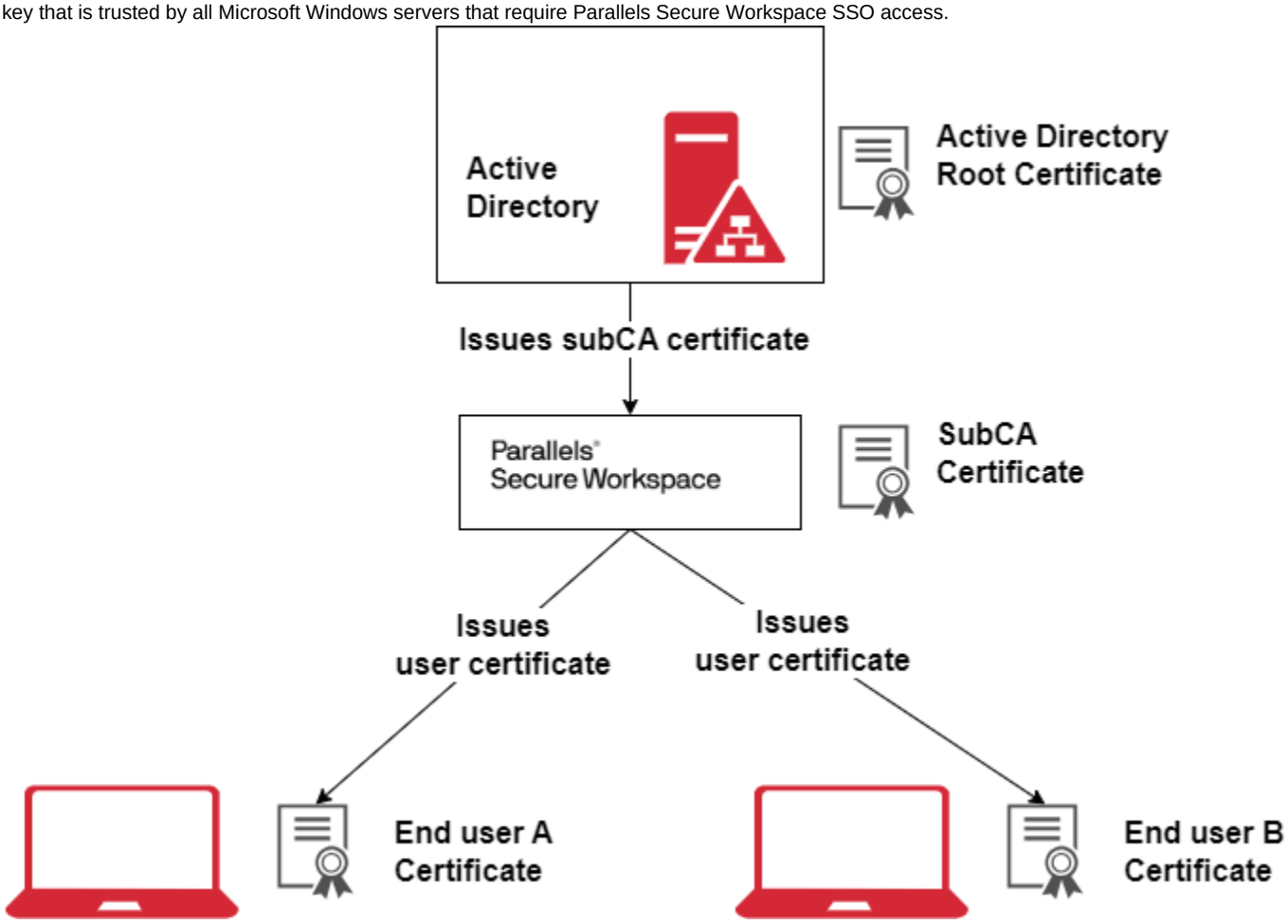
See "Enable Pre-Authentication" for detailed instructions on how to do this.

By enabling SSO in Parallels Secure Workspace, the step where the user is prompted for their Microsoft Windows password prior to opening the Workspace will be removed. This requires a trusted X.509 client certificate so users can log on to applications, virtual desktops and drives.

The certificate will be used to:

1. Generate a Kerberos ticket to
   a. Log on to the Microsoft Windows domain (NLA)
   b. Access the CIFS drives
2. Generate a virtual smartcard to allow RDP login (win-logon)

The Parallels Secure Workspace appliance will act as a sub-certificate authority (sub-CA) and will automatically generate and manage those client certificates. In order to generate those certificates, Parallels Secure Workspace requires an Active Directory signed certificate and private key that is trusted by all Microsoft Windows servers that require Parallels Secure Workspace SSO access.



Configure the bind user

To fill in some required information for the client certificates, a **bind user** must be specified in order to retrieve this information from the Active Directory. Navigate to System Settings > Global > Domains, select the relevant domain and fill in the username and password for the bind user.

Generate Certificate and set up the intermediate sub-CA

Create the certificate

On the Microsoft Windows Domain Controller, create the "workspace.inf" certificate template with the following content. This can be done using Notepad or any other text editor.

```
[NewRequest]
Subject = "CN=WorkspaceCA"
KeyLength = 4096

[RequestAttributes]
CertificateTemplate= SubCA
```

Use **certreq** to request certificates from the certification authority (CA).

```
certreq.exe -new workspace.inf workspace.req
certreq -submit workspace.req workspace.cer
```

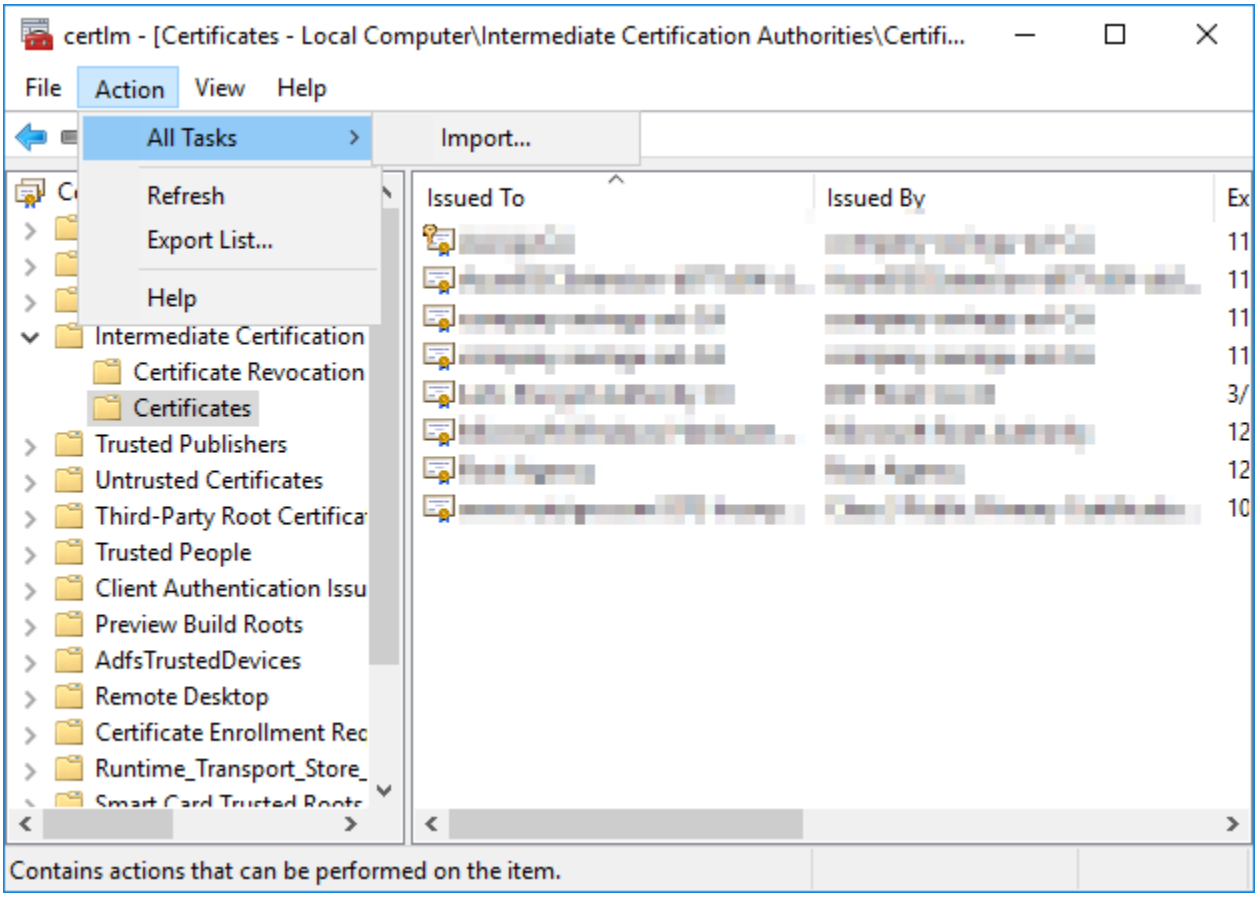
See https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certreq_1 for more details.

Import the certificate into the certificate stores

In the next step, the certificate will be imported into the AD certificate store.

Run **certlm.msc** and import the certificate:

- Select the **Intermediate certificate store > Certificates**
- Go to **Actions > All Tasks > Import**
- Run through the wizard and import the `workspace`.cer file



Once this is done, the Active Directory needs to be configured to allow smart card logins that are signed with this intermediate certificate. As these client certificates will be generated by the Workspace CA (and as such be signed with this intermediate certificate), this certificate needs to be added to **NTAuthStore** of the Active Directory:

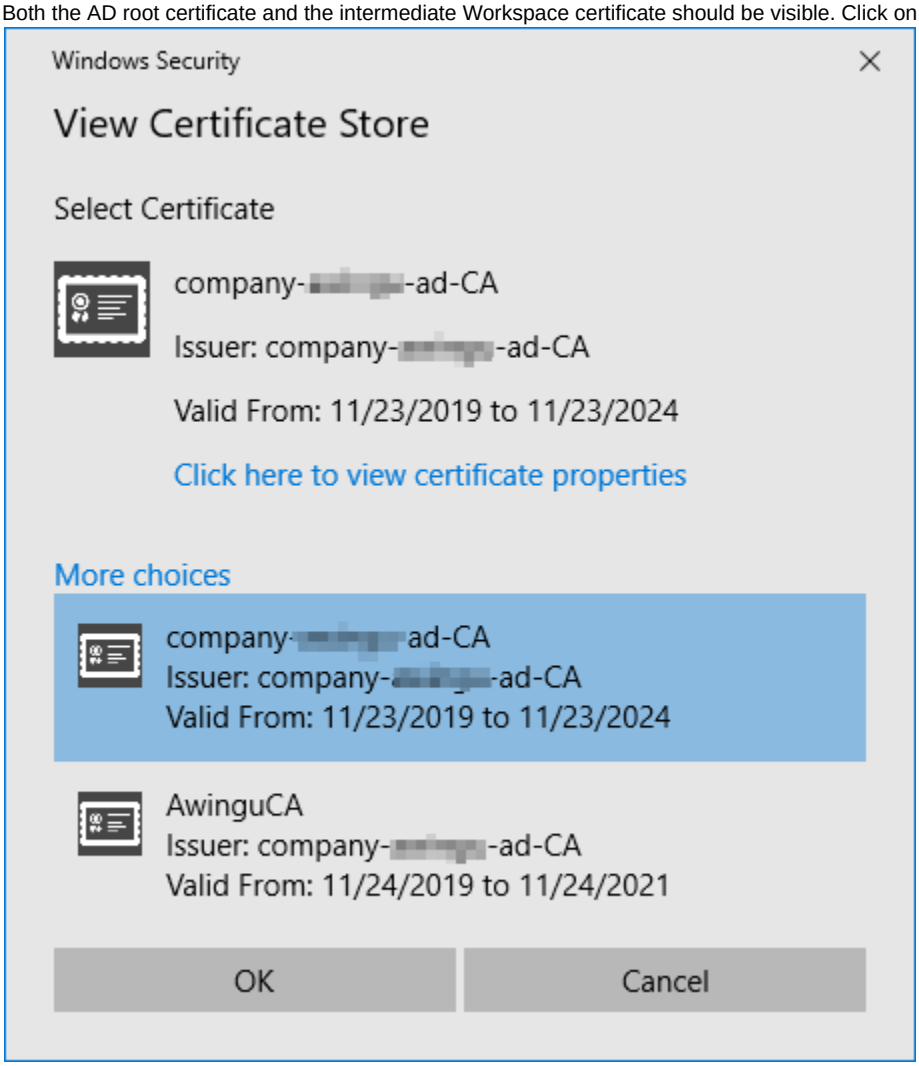
```
certutil -dspublish -f workspace.cer NTAuthCA
certutil -enterprise -addstore NTAuth workspace.cer
```

See https://support.microsoft.com/en-us/help/295663/how-to-import-third-party-certification-authority-ca-certificates-into for more information.

Check if the import was successful by running the following command:

```
certutil -enterprise -viewstore NTAuth
```

Both the AD root certificate and the intermediate Workspace certificate should be visible. Click on "more choices" to see all certificates.



Export Certificates and private key

To enable SSO in Parallels Secure Workspace, two files are needed:

1. The intermediate certificate in .pfx format, including the private key.
2. The root certificate of the AD in .cer format. This is needed to complete the certificate chain trust.

Export the intermediate Certificate (with private key) in pfx format:

To get the intermediate certificate we need to open certlm.msc again:

- Select the Intermediate Certification Authorities store > Certificates
- Right-click on the subca certificate (in this case WorkspaceCA) and select All tasks > export
- The export wizard will start
  - Select “Yes, export the private key” on the second page
  - Select “Personal Information Exchange - PKCS # 12 (.PFX) as format. Leave default settings (“include all certificates in the certification path if possible” + “enable certificate privacy”)
  - Set a password on the certificate.
  - Finally on the "File to Export" page set the output file to subca.pfx
  - Finish the wizard.

Export Root Certificate (without private key)

To get the root certificate we need to open certlm.msc again:

- Select the *Trusted Root Certification Authorities* store *Certificates*
- Right click on the root certificate of your AD and select All tasks Export (in case you don't know what the root certificate of your AD is, open the intermediate certificate first and check the **certification path**. The certificate that has signed the intermediate certificate is the certificate that is needed)
- The export wizard will start
  - On the "Export File Format" page select "Base 64 encoded X.509 (.cer)"
  - Finally on the "File to Export" page set the output file to root.cer
  - Finish the wizard

Important: Check the entire **certification path** of the Workspace SubCA. If this is signed by one or more intermediate certificates and then by a root CA, it’s necessary to export **each** of those intermediate certificates and the root CA in the same way as documented above for the root certificate. Copy-paste the contents of each exported .cer file below each other into one single file (do not include empty lines). Save the result to a single root.cer file.

Parallels Secure Workspacemust also trust the certificates used for Kerberos authentication of each Kerberos domain controller. Export any intermediate/root CAs in their certification paths which weren’t already included in the root.cer file above.

Validate if the Microsoft Windows back end is correctly configured for Parallels Secure Workspace SSO

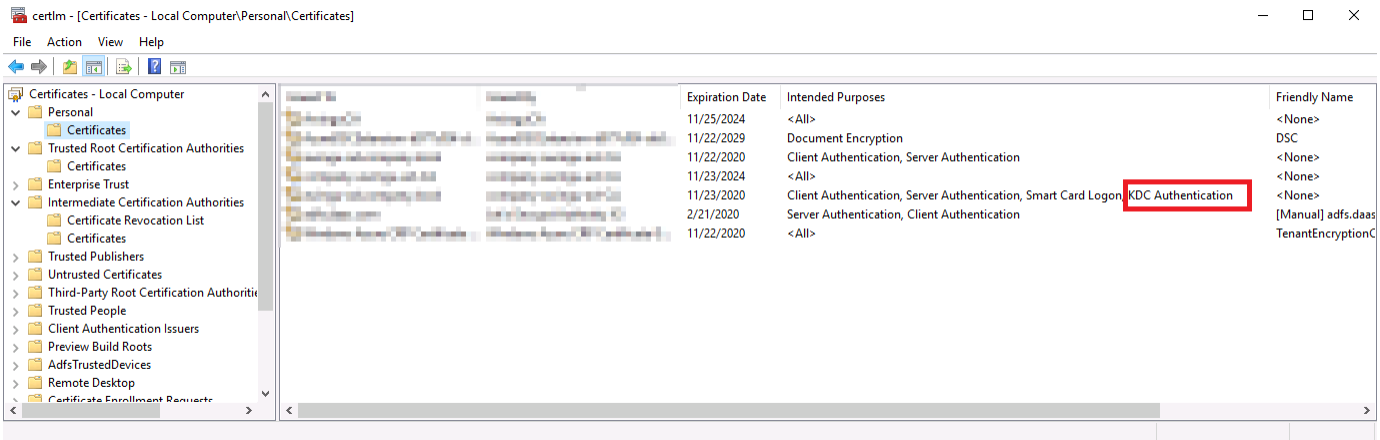
Validate the Kerberos Certificates.

Parallels Secure Workspace SSO is based on Kerberos Constrained Delegation (KCD). To make this work, the Kerberos setup needs to be done correctly.

If this is the first time KCD is used on this Microsoft Windows back-end, there is a possibility that there is no Kerberos Certificate yet.

To check if there is a (valid) Kerberos certificate, open the certlm.msc again:

- Select the **Personal store > Certificates**
- Check if one of the AD certificates (certificates with the name of the Domain Controller) has a valid certificate with "**Intended Purposes**" set to "**KDC Authentication**"



If there is no valid certificate, add one first:

- Go to **Personal > Certificates.**
- Right-click on **Certificates > All tasks > Request New Certificate.**
- Click next until you reach what kind of template to use, then select **Kerberos.**

Check DNS setup

As Kerberos is highly dependent on DNS, DNS also needs to be configured correctly. In order for Parallels Secure Workspace SSO to work, all of the DNS records for the servers defined in the drives, app servers and AD/LDAP server sections of the Parallels Secure Workspace configuration need to be accessible with a reverse DNS lookup of its IP.

To check if this is the case do a DNS lookup of the DNS names used in Parallels Secure Workspace for AD and other servers and check if the reverse lookup of the IP matches that name:

```
C:\Users\win-admin>nslookup dc01.company.org
Name: dc01.company.org
Address: 10.7.0.4


C:\Users\win-admin>nslookup 10.7.0.4
Name: dc01.company.org
Address: 10.7.0.4
```

For reverse lookups of IP addresses, Parallels Secure Workspace uses the global DNS server, so not the DNS servers of the individual tenants. If you have a multi tenant setup with different DNS settings for the global appliance and for the individual tenants please validate on the Parallels Secure Workspace appliance itself if the resolution of the reverse lookup is done correct for the tenants on which you want to enable SSO. This can be done via the troubleshoot page (**System Settings > Global > Troubleshoot**) and then select the “dig” action. In the “argument” field set “-x your.ip” (for example -x 10.1.2.3). If resolution is configured correctly, in the answer section you should see something similar:

```
;; ANSWER SECTION:
3.2.1.10.in-addr.arpa. 3600        IN        PTR        server.company.
org
```

Also check if the kerberos SRV records exist for your domain and that they point to the correct KDC. Check both the UDP & TCP records

```
C:\Users\win-admin>nslookup
> set type=srv
> _kerberos._udp.company.org


_kerberos._udp.company.org SRV service location:
                  priority = 0
                      weight = 100
                       port = 88
                       svr hostname = dc01.company.org
dc01.company.org internet address = 10.7.0.4


> _kerberos._tcp.company.org


_kerberos._tcp.company.org SRV service location:
```

```
                        priority = 0
                        weight = 100
                        port = 88
                        svr hostname = dc01.company.org
dc01.company.org internet address = 10.7.0.4
```

Update the DNS records where needed (reverse lookup + SRV records) to ensure this is working correctly before continuing.

Make sure all servers involved in Kerberos Authentication can access the Certificate Revocation List

HTTP(s): TCP port 80/443 connectivity from the Active Directory and Application Servers to the Parallels Secure Workspace appliance (http(s)://<workspace_url>/crl/>WORKSPACE_DOMAIN_NAME>) is required.

Note: WORKSPACE_DOMAIN_NAME is the name of the domain as it's known within Parallels Secure Workspace. This may be different from the Microsoft Windows domain name!

Make sure LDAPs is enabled on the Active Directory

Similarly to Kerberos, for an LDAPs connection a valid Certificate is needed on the Active Directory:

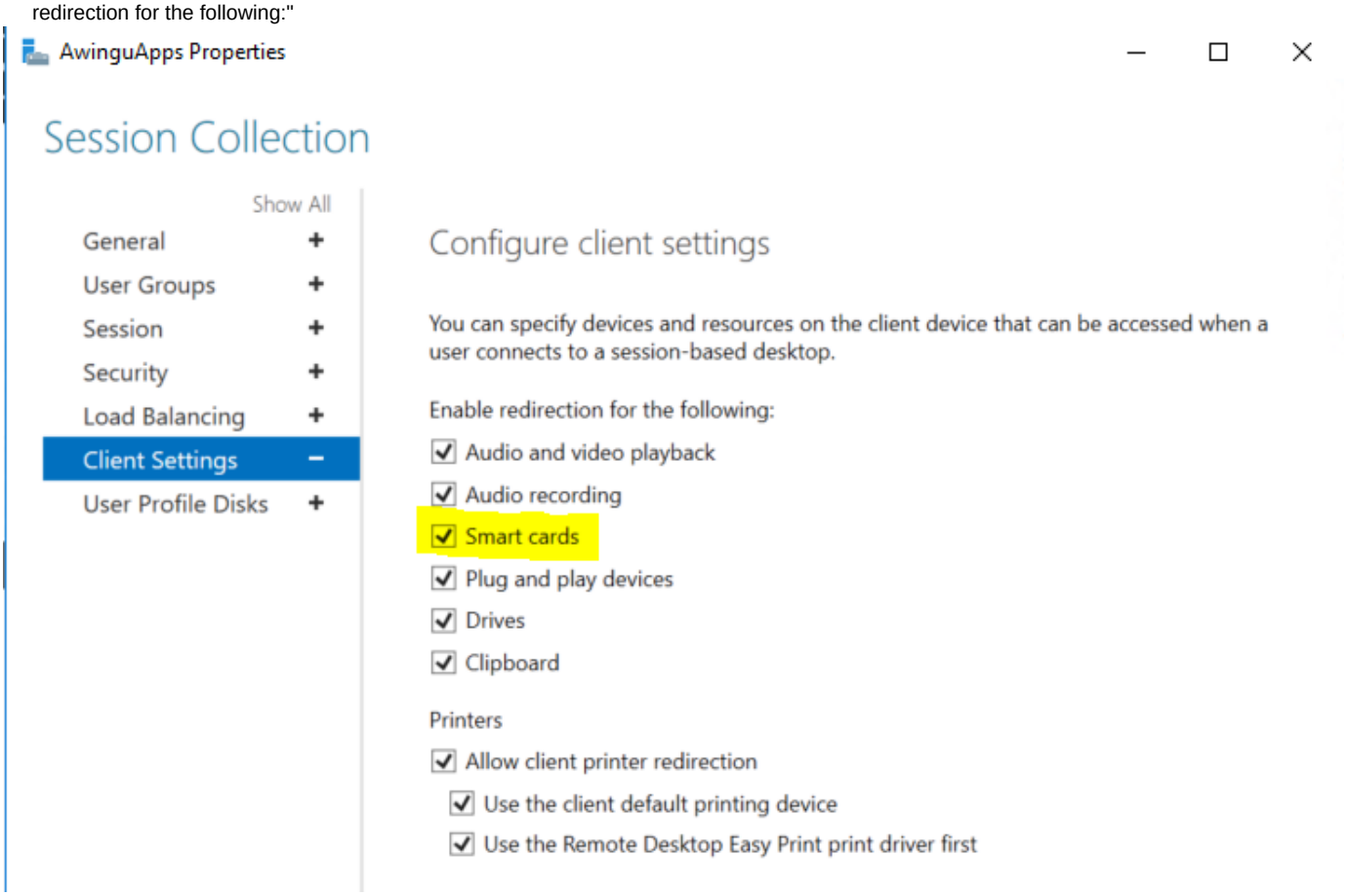
To check if there is at least one (valid) Domain Controller certificate open the certlm.msc again:

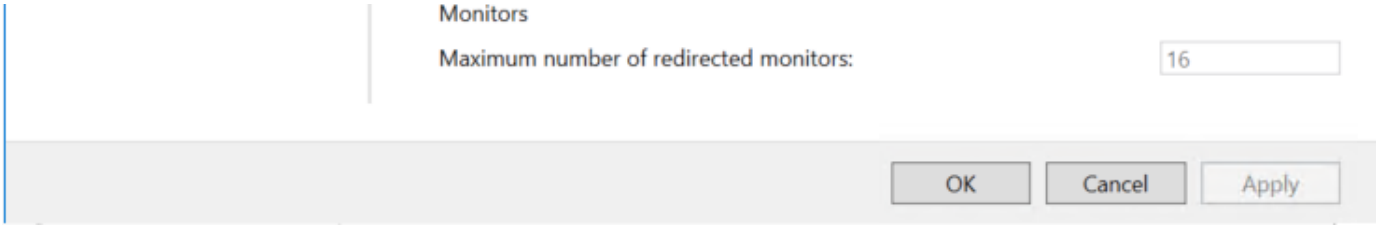
- Select **Personal store > Certificates**
- Check if one of the AD certificates (certificates with the name of the Domain Controller) has a valid certificate with "Intended Purposes" set to "Client Authentication" and "Server Authentication"

Make sure the Connection Broker Session Collection is configured for smart cards

When using an RDS Connection Broker Session Collection, then the session needs to have smart card redirection enabled from the client device:

- Open server manager and go to the RDS Session Collection
- Next to "Properties" in the RDS collection > Tasks > Edit Properties > Client Settings: Ensure "Smart cards" is ticked under "Enable redirection for the following:"





Configure Parallels Secure Workspace for SSO

Only if the following conditions are met, Parallels Secure Workspace SSO can be enabled:

1. The sub-CA certificates have been created (root.cer, workspace.cer and workspace.key)
2. All dependencies on the Microsoft Windows back end have been set up (import of the sub-CA certificate in the correct stores, Kerberos and DNS configuration, etc.)
3. Pre-authentication with the external IdP has been configured and tested (see Enable Pre-authentication)

Enable the Parallels Secure Workspace Key Vault

Since the private key for the Workspace Sub-CA allows Parallels Secure Workspaceto impersonate Microsoft Windows users, this key is highly sensitive and is stored in a vault. The vault itself is also encrypted and the encryption key for the vault can either be stored on the Parallels Secure Workspace appliance itself (Internally) or on an external Vault provider like Google Cloud Key Management Service or Azure Key Vault.

By default the Vault is not activated and needs to be enabled first:

- Go to **System Settings > Global > Connectivity > Vault**.
- Select the provider of choice.
- Click on Apply.

Enabling the vault might take a few minutes.

For more information on the external Vault providers and how to obtain the needed configuration parameters have a look at:

- Microsoft Azure Key Vault: https://docs.microsoft.com/en-us/azure/key-vault/key-vault-overview
- Google Cloud Key Management Service (GCKMS): https://cloud.google.com/kms/docs/quickstart . When using the Google Cloud Key Management Service (as an external Vault Provider, the GCE Service Account requires these permissions:
  - Cloud KMS Viewer
  - Cloud KMS CryptoKey Encrypter/Decrypter

The private key itself does not leave the vault. After the initial upload, it only exists in unencrypted form in the memory of the vault service.

If the Parallels Secure Workspace appliance running the vault services is rebooted, access to an external vault provider such as Google GCKMS or Azure Key Vault is required to unseal the vault and decrypt the private key.

Since the vault does not allow extracting the private key, certain configuration changes of the Parallels Secure Workspace environment result in a full vault reset, which will disable SSO and require you to re-upload the private key of the CA.

These are:

- Restoring a database backup (only applicable when using Parallels Secure Workspace with an internal database)
- Changing the vault provider

For HA purposes, the vault service is replicated across all back-end nodes in an Parallels Secure Workspace environment.

If not yet done, set the domain parameters correctly:

When adding a domain to Parallels Secure Workspace one of the parameters is specifying if the LDAP connection is over SSL or not.

If this has not yet been done make sure this is enabled;

- Go to **System Settings > Global > Domains**.
- Click on the "edit" button next to the domain you want to check.
- In the details, check if **LDAP over SSL** is set to **enabled.**

Also make sure that:

1. The FQDN of the domain is set to the Kerberos realm of the Windows Domain (example: company.org)

2. The AD/LDAP server is set to the correct FQDN of the domain controller (example: ad1.company.org). Parallels Secure Workspace won't work if the IP address or an alias is used.

Ensure Parallels Secure Workspace is using the correct DNS server

Parallels Secure Workspace has DNS servers on 2 levels. One for the appliance itself and one for the tenants/domains.

As the Global DNS server is used for reverse DNS resolution, make sure that the Global DNS server is pointing to a DNS server that is capable of resolving all reverse DNS lookups for all tenants/domains using SSO.

To check and modify the global DNS server:

- Go to **System Settings > Global > Connectivity > Servers**.
- Point the **DNS IP Addresses** to the correct DNS server(s).

If not yet done, set Authentication Protocol of Application servers to Kerberos

When adding an application server, the default Authentication Protocol is NTLM. For SSO to work, Parallels Secure Workspaceneeds to use Kerberos.

To switch application servers from NTLM to Kerberos:

- Go to **System Settings > Manage > Application Servers**.
- For each application server:
  - Set the Authentication Protocol to **Kerberos**.
  - Ensure the **Authentication Host** is set to the FQDN of the server and that the name specified in here matches the DNS and reverse DNS name.

Make sure you set this value for all application servers that Parallels Secure Workspace uses with SSO.

Upgrade from Pre-Authentication to Single Sign-On

Now that all settings both on the Microsoft Windows back end and the Parallels Secure Workspace appliance are set, update the configuration to switch from Pre-Authentication to SSO.

- Go to **System Settings > Configure > User Connector > Federated Authentication**
- Change the **Type** to **Single sign-on.**
- 2 extra certificate settings will appear: **CA Certificate** and **CA Trusted Roots File.**
  - Select **Manual PKCS 12** as the type for CA Certificate and upload the “subca.pfx” file + set the CA certificate password to the password set on the PFX certificate earlier.
  - Select **Manual PEM** as the type for CA Trusted Roots and upload the “root.cer” file. (*Note:* When updating this certificate, the CA Certificate also needs to be re-uploaded)
- Test both certificates by clicking on [Show certificate]. If there are no errors, you can continue.
- Verify that the Username Claim URL points to the UPN property of the SAML response. Single Sign-On can only work when using the UPN.
- Click Apply

Show Certificate

To validate if your certificate is correct, you can visualize the certificate’s content using the *Show Certificate* button.

End User Flow:

The end user flow will be similar to the one from Pre-Authentication except that the step where the user needs to enter their Windows Password again will no longer appear:

- When a user accesses the Parallels Secure Workspace landing page, Parallels Secure Workspace will check if the user has a valid authentication token with the configured IdP.
- If this is not the case yet, Parallels Secure Workspace will redirect the browser to the IdP. Users will need to authenticate against the IdP first. If successful, the IdP will redirect the User to the Parallels Secure Workspace landing page.
- User will be logged into the Parallels Secure Workspace.
- From the Workspace, they can start Apps, Desktops and get access to the Drives.

From a technical point of view once a user has pre-authenticated, Parallels Secure Workspace will now use the UPN that was received from the IdP to create a X.509 client certificate suitable for smart-card login. These client certificates are valid for 1 day. Using the client certificate, Parallels Secure Workspace requests a Kerberos Ticket Granting Ticket (TGT) from the Active Directory Domain Controller through PKINIT.

To complete the login to Parallels Secure Workspace, Parallels Secure Workspace fetches the attributes and group memberships of the user from the Active Directory Domain Controller. These attributes are required for other functionality to work, for example to decide if a user has admin rights or if the user is allowed access to certain drives, applications or features.

In order to setup an RDP session using Parallels Secure Workspace, two authentication steps are performed: the network level authentication (NLA) and the Microsoft Windows logon:

- The NLA is done using the same Kerberos TGT acquired earlier. We currently support up to CredSSP version 6 for this authentication step.
- For the Microsoft Windows logon, Parallels Secure Workspace emulates a smart card designed to work with the Microsoft Windows standard drivers. This virtual smart card appears to contain the X.509 client certificate that was generated earlier.

Note: When SSO is configured, the Change Password link in the Account Settings of the users will not be visible to avoid confusion about which password will be changed (IdP or AD).

Microsoft OneDrive for Business

Introduction

Users of OneDrive for Business can have their home drive shown on the Files page in Parallels Secure Workspace. They can perform all the actions as with regular drives: upload, download, copy, move, rename, delete, and preview. However, it is not possible to directly open a file with a streamed application.

We describe in this section how to configure both your Microsoft account and your Parallels Secure Workspace environment.

Allowing Parallels Secure Workspace to access your Office 365 subscription

In order to allow your Parallels Secure Workspaceenvironment to access the OneDrive of your Office 365 subscription, Microsoft provides the following documentation:

> https://dev.onedrive.com/app-registration.htm#register-your-app-for-onedrive-for-business

That document is however somewhat outdated, so we summarize here the steps to take.

Step 1. Get an Office 365 subscription

All Office 365 subscriptions for Small Businesses and Enterprises should be compatible with Parallels Secure Workspace. Even the smallest package, Office 365 Business Essentials, works fine.

The procedure dictates to get an Office 365 Developer Site:

1. Go to https://portal.office.com > Admin
2. Resources > Sites
3. Click on "Add a site"
4. Fill in all the fields like you desire
   For following fields, please note:
   - Template Selection: Developer Site
   - Server Resources: default value should be enough

   Click OK and you end-up in the SharePoint admin center (direct link: https://<your_account>-admin.sharepoint.com)
5. The new developer site URL in the Site Collections list.
6. When the site creation is finished (spinning wheel next to the URL), you can navigate to the URL to open your Developer Site.
   This takes a long time (up to one hour).

Step 2. Set up an Azure Active Directory tenant

Make sure your Office 365 subscription is synced with Azure AD.

Step 3. Register your app with Azure Active Directory

1. Go to https://portal.azure.com
2. Open the service: App registrations
3. Click on New registration:
   a. Name: e.g. "OneDrive on Parallels Secure Workspace"
   b. Supported account types: Accounts in any organizational directory (Any Azure AD directory - Multitenant)
   c. Redirect URI:
      i. Web
      ii. URL: the URL to your Parallels Secure Workspace environment (e.g. https://workspace.mycompany.com)
4. Once created, retrieve the Client ID = Application ID.
   You will need this value to configure Parallels Secure Workspace.
5. Click on Certificates & secrets and click New client secret

a. Description: secret
b. Expires: Never
c. Click on Save
d. Retrieve Client secret = secret
You will need this value to configure Parallels Secure Workspace.
⚠ The value cannot be retrieved afterwards. Don't loose it!

6. Click on API permissions and click on Add a permission:
   a. Select an API: Office 365 SharePoint Online
   b. Select permissions: Read and write user files (delegated permission)
   c. Click on Done

Step 4. Have the network right

Parallels Secure Workspace needs to be able to reach the OneDrive for Business servers directly, or through an HTTP proxy (see Connectivity Settings). HTTPS (port 443) access is required to:

- <mydomain>**-my**.sharepoint.com
- graph.microsoft.com
- api.office.com

Configuring Parallels Secure Workspace to access OneDrive

OneDrive for Business can be configured as Drive in the System Settings. Go to Manage > Drives and add a drive with following settings:

- Name: e.g. OneDrive
- Description
- Backend: ONEDRIVE
- Client ID: see previous section
- Client secret: see previous section
- Workspace URL: the URL a user uses to access Parallels Secure Workspace, e.g. https://workspace.mycompany.com
- Redirect URL: you will need this value to configure Azure Active Directory
- URL: link to your sharepoint.com environment, e.g. https://mycompany.sharepoint.com
- UNC: can be left empty
- Labels: you can use labels to group drives together. You can leave this empty.
- User Labels: the drive will only be visible for users with a matching user label. Use "all:" to assign the drive to all users.

Configuring the Parallels Secure Workspace OneDrive app

1. Go to https://portal.azure.com
2. Go to Azure Active Directory > App registrations
3. For your app (e.g. OneDrive on Parallels Secure Workspace), go to Manage > Authentication
4. Under Web > Redirect URIs > add the Redirect URL you've obtained in System Settings
5. Press Save

Using OneDrive on Parallels Secure Workspace

When a user opens their OneDrive folder on the Files page in Parallels Secure Workspace for the first time, they will be redirected to the Office login portal where access is requested to their OneDrive. Once access is granted, they can use OneDrive as any other folder in Parallels Secure Workspace, except of opening a file with a streamed application (only open with Preview will work).

Smart Card Redirection

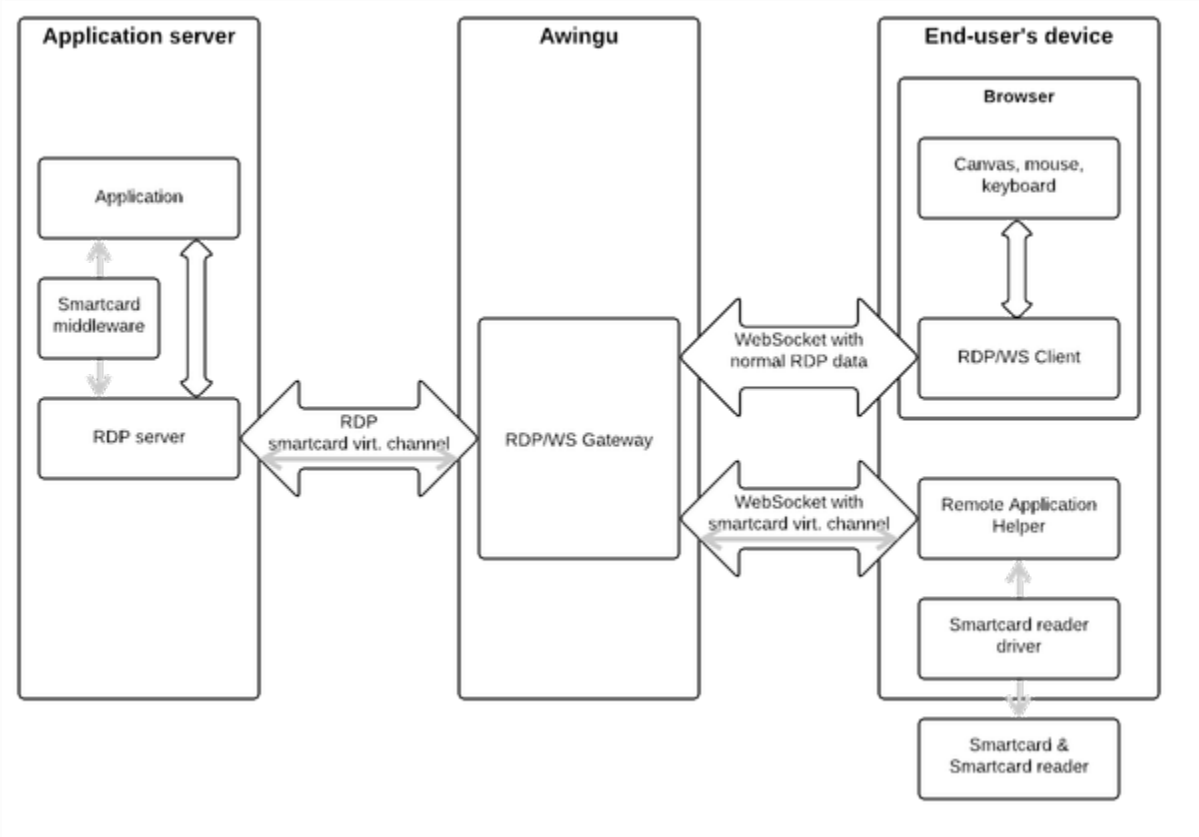
Introduction

Parallels Secure Workspace supports accessing smart cards in streamed applications. This enables users to access a smart card connected to their client device (e.g. a smart card reader in their laptop) from an application running on an application server. Typical use cases include electronic ID cards, banking cards, or access cards. This does not include using smart cards as second-factor authentication for accessing the Workspace.

Although any smart card should work, the following smart cards were explicitly tested:

- Belgian eID.
- Dutch UZI pas.
- Italian InfoCert Business Key.
- Isabel.

How It Works



To use a smart card in a streamed application, the administrator should explicitly enable smart card support for the application and the user should be equipped with a smart card reader connected to his device. When the user launches such an application with smart card support, the Workspace will connect to the locally installed Remote Application Helper, which will connect to the smart card reader and act as a bridge between the smart card reader and the Workspace.

Enabling smart card support

Preparing the application server

The application server should have the middleware installed for the smart card.

Enabling smart card access on Parallels Secure Workspace

To enable smart card access in an RDP or RemoteApp application, the *smartcard:* label should be assigned to the application. This can be set in the details of an application in the *System Settings* under *Manage > Applications*

Once this label is assigned to an application, the application will try to connect to the Remote Application Helper.

Enabling smart card access on the client

The first time a user launches a smart card enabled application, the browser will ask the user to download the Remote Application Helper. This software can be downloaded from the Parallels Secure Workspace appliance and is available for Windows and macOS.

Note that for macOS, the installer is not signed: the user needs to do right-click > Open on the installer.

The user needs to have the drivers of the smart card reader installed on their device. Note that some drivers are included in the operating system and don't need any end-user intervention.

Limitations

1. The smart card reader needs to be connected before opening the application.
2. The libraries to communicate with smart cards differ slightly between Windows and macOS. Therefore, it might be that some applications on the Microsoft Windows application server will perform a certain library call that is incompatible with the macOS library available on the end-user device. This behavior has been observed for the eID Viewer and Isabel.
3. The Remote Application Helper will use a proxy on the client if it detects a configured proxy on Microsoft Windows. The Remote Application Helper cannot be configured to use a proxy on macOS.

Troubleshooting

- Check whether the driver of the smart card reader is installed on the user's device.
- Check whether the middleware of the smart card is installed on the application server.
- When Mozilla Firefox has been installed after the installation of the Remote Application Helper, the Remote Application Helper needs to be re-installed.
- When the user did not stop Mozilla Firefox during the installation (as requested in the installer), the Remote Application Helper needs to be re-installed.
- When using clients with Microsoft Windows 7 Embedded, you will need to install Visual C++ 2015 redistributable (32-bit/x86 version) on them. It is a known issue that you need to install KB2999226 first to be able to install Visual C++ 2015.

Automate Parallels Secure Workspace via the REST API

Parallels Secure Workspace provides a REST API which makes it possible to install, configure, and manage the environment. This allows you to integrate Parallels Secure Workspace in an automation framework.

Getting Started with the Parallels Secure Workspace API

This section assumes:

- You have an installed Parallels Secure Workspace appliance running.
- You have a domain configured.
- You have the correct tools to execute REST API calls (e.g. PowerShell, see below).

To test it out manually, you can use a tool to execute the REST API calls:

- The live API browser at http(s)://your.workspace.env/api/v2/
- The API documentation at http(s)://your.workspace.env/api/v2/docs/

Note: all API calls are addressed to **the workspace URL** of the appliance.

PowerShell example using an API Token

If enabled for the domain, admin users can get an API token to interact with the REST API.

See User Connector Configuration for information on how to limit API token-based authentication to certain subnets.

In order to get an API token, go to your **Account settings** and click **Manage API token**, which will show a dialog window for generating a token.

API tokens remain valid, even when the user has been removed from Active Directory or from the admin group.

For an audit trace of the API tokens check **Changes** for your domain in **System Settings**, and filter on **Session Token** as **Resource Type**.

With the API token you can consume the REST API from PowerShell as shown in the below example, listing all application servers:

```
$token = "<your API token here>"
$your_uri = "https://<address of your appliance here>/api/v2/app-servers
/"

[Net.ServicePointManager]::SecurityProtocol = [Net.
SecurityProtocolType]::Tls13

$headers = @{}
$headers.Add("Authorization", "Token $token")

$result = Invoke-RestMethod -Method get -Uri $your_uri -Headers $headers
$result.results | Format-Table
```

Navigating Through the API

- To list the URIs to all available system resources:

```
URI:     /api/v2/
Method:  GET
Headers: Accept: */*
         Authorization: Token your-api-token
```

Expected response: 200 with following payload:


```
{
    "branding": "http://172.16.5.74/api/v2/branding/",
    "branding-images": "http://172.16.5.74/api/v2/branding-images/",
    "favicons": "http://172.16.5.74/api/v2/favicons/",
    "domains": "http://172.16.5.74/api/v2/domains/",
    "hostheaders": "http://172.16.5.74/api/v2/hostheaders/",
    "certificates": "http://172.16.5.74/api/v2/certificates/",
    "apps": "http://172.16.5.74/api/v2/apps/",
    "app-servers": "http://172.16.5.74/api/v2/app-servers/",
    "app-icons": "http://172.16.5.74/api/v2/app-icons/",
    "user-apps": "http://172.16.5.74/api/v2/user-apps/",
    "key-combos": "http://172.16.5.74/api/v2/key-combos/",
    "configuration": "http://172.16.5.74/api/v2/configuration/",
    (...)
}
```


- To retrieve an system resource, e.g. the drives, you can use the URI mentioned in the output of the previous command:

```
URI:     /api/v2/drives/
Method:  GET
Headers: Accept: */*
         Authorization: Token your-api-token
```

Expected response: 200 with following payload:


```
{
    "count": 31,
    "next": null,
    "previous": null,
    "results": [
        {
            "backend": "CIFS",
            "config": [],
            "description": "Home Drive via CIFS",
            "domain": "http://172.16.5.74/api/v2/domains/2/",
            "name": "Home Drive",
            "unc": "\\\\fileserver\\Users$\\<username>\\Documents",
            "url": "smb://fileserver.mycompany.com/Users$/<username>
/Documents",
```

```
            "use_domain": false,
            "labels": [],
            "user_labels": [
                "all:"
            ],
            "uri": "http://172.16.5.74/api/v2/drives/1/",
            "smb_max_protocol": "SMB3"
        },
        (...)
    ]
}
```

For more information about this resource, you can use your web browser to navigate to http(s)://your.workspace.env/api/v2/docs/#drives

Changing Settings

- To add a resource, e.g. to add a drive to a domain:

```
URI:     /api/v2/drives/
Method:  POST
Headers: Content-Type: application/json
         Accept: */*
         Authorization: Token your-api-token
         Referer: http://your.workspace.env/
Payload: {
             "domain": "http://172.16.5.74/api/v2/domains/2/",
             "name": "New Drive",
             "description": "This is a drive to test the API",
             "backend":"CIFS",
             "config": [],
             "url": "smb://fileserver.mycompany.com/TestShare",
             "unc": "\\\\fileserver\\TestShare",
             "use_domain": false,
             "labels": ["testkey:testlabel"],
             "user_labels": ["all:"]
         }
```

Expected response: 201, with the URI of the drive in the payload.
Note that the API will automatically create the labels and user_labels provided in case they don't exist. You can verify this in `/api/v2/labels/`

- To change fields of an existing resource, e.g. change the unc field of a drive:

```
URI:     /api/v2/drives/9/
Method:  PATCH
Headers: Content-Type: application/json
         Accept: */*
         Authorization: Token your-api-token
         Referer: http://your.workspace.env/
Payload: {"unc": "\\\\fileserver\\Share"}
```

Logging Out

```
URI:     /api/v2/sessions/current/
Method:  DELETE
Headers: Accept: */*
         Content-Type: application/json
         Authorization: Token your-api-token
         Referer: http://your.workspace.env/
```

Expected response: 204

Further documentation

All available API resources are documented on your appliance on /api/v2/docs/.

Installing with the Parallels Secure Workspace API

1. Deploy the Parallels Secure Workspace appliance and configure the networking, which can be automated with the API tools provided by the virtualization or cloud platforms in combination with DHCP.
2. Once the VM has been started, the installer API will start to listen on **port 8080**.
3. To start the installation, do following call on port 8080. Please refer to Parallels Secure Workspace Installer for more information about the fields used in the request.

```
URI:     /api/v2/updates/install/
Method:  POST
Headers: Accept: */*
         Content-Type: application/json

Payload: {
           "config": {
             "eula": {
               "accepted": true
             },
             "network": {
               "dns": "172.19.0.1",
               "ntp": "ad.mycompany.com"
             },
             "environment": {
               "management_user": {
                 "username": "my-admin-user",
                 "password": "my-password",
                 "confirmed_password": "my-password"
               }
             },
             "appliances": [
               {
                 "ip_address": "172.19.0.2",
                 "hostname": "node01"
               }
             ],
             "features": {
               "common": {
                 "external_database": false
               }
```

```
            }
          }
        }
```

Expected response: 201 with payload:

```
{
  "uri": "http://172.16.5.76:8080/api/v2/updates/1/",
  "progress": [],
  "begin": "2017-10-20T11:04:24",
  "end": null,
  "status": "IN_PROGRESS",
  "service": null,
  "version": "http://172.16.5.76:8080/api/v2/versions/1/",
  "outputs": "http://172.16.5.76:8080/api/v2/update-outputs/?update=1"
}
```

4. Wait until the installer has finished:

```
URI:     /api/v2/updates/1/
Method:  GET
Headers: Accept: */*
```

If field "status" can be IN_PROGRESS, SUCCEEDED or FAILED.
The error output can be retrieved via the outputs field of the response:

```
URI:     /api/v2/update-outputs/?update=1
Method:  GET
Headers: Accept: */*
```

Configure using the Parallels Secure Workspace API

Once the installation is done, you can configure Parallels Secure Workspace as follows:

1. Enable an API token for the management user configured during the installation.
2. Add your first domain via POST to /api/v2/domains/.
   Host headers are autogenerated if you provide a list of FQDNs in the "host headers" field.
   The user connector is configured in the same domain resource.
3. User groups, like for admin, are added via /api/v2/user-groups/
4. Application servers are added via /api/v2/app-servers/
   For each application server, a server label is automatically created and linked to it.
5. Icons for applications are uploaded via /api/v2/app-icons/create/
6. Applications are added via /api/v2/apps/, where you need to provide the link to the uploaded app-icon.
   Provided labels (labels, user_labels, server_labels) and categories are automatically created if they don't exist yet.
7. Drives are added via /api/v2/drives.
   Provided labels (labels, user_labels) are automatically created if they don't exist yet.

Please refer to the documentation on /api/v2/docs/ to have more information of the payload to provide.

External Audit Logging

Introduction

Parallels Secure Workspace allows you to forward all audit logs to an external system using the HTTP(S) protocol.

Each record will be transmitted to the configured URL using an `HTTP POST` per record in `JSON` format.

Structure

A record is a collection of unordered key/value pairs (an `Object` in `JSON` terms) providing information of the audit event for the specific `audit_type`.

All records provide the following properties:

Property	Type	Description
`audit_type`	String	The audit record type.
`version`	String	Parallels Secure Workspace version.

Based on the `audit_type` you can discriminate between audit record types and interpreter the specific properties of each type.

The `version` field represents the Parallels Secure Workspace version and allows you to version your integrations.

Audit Records Types

User Sessions

User Session records represent a single authenticated session between a browser and the Parallels Secure Workspace environment for a user. If a user logs in for a second time on a different browser, this will result in a new session.

User sessions are also the basis for licensing, e.g. the number of concurrent users is determined based on the number of simultaneous active sessions.

Property	Type	Description
`audit_type`	String	Record type (`usersessions`).
`version`	String	Parallels Secure Workspace version.
`session_id`	String	Unique id.
`session_start`	DateTime	Timestamp when the session started in UTC.
`session_end`	DateTime	Timestamp when the session ended in UTC.
`session_labels`	String	A comma-separated list of all labels assigned to the user for this session.
`username`	String	Username.
`domain`	String	Name of the Workspace domain.
`ip`	String	The IP address of the client that created this session.
`http_agent`	String	Value of the `User-Agent` header when creating this session.

`country`	String	Country from where the session was created based on GeoIP.
`geoip_latitude`	String	Latitude from where the session was created based on GeoIP.
`geoip_longitude`	String	Longitude from where the session was created based on GeoIP.
`name`	String	Browser name based on `User-Agent`.
`major`	String	Browser version major based on `User-Agent`.
`minor`	String	Browser version minor based on `User-Agent`.
`os`	String	Client operating system based on `User-Agent`.
`os_name`	String	Client operating system name based on `User-Agent.`

Application Sessions

Application Sessions represent a single streamed application or desktop session for a user. Every time a new streamed application or desktop connection is started, a new application session is generated.

Web applications and reverse proxied web applications are logged separately as Web Application Sessions

Property	Type	Description
`audit_type`	String	Record type (`appsessions`).
`version`	String	Parallels Secure Workspace version.
`userapp_session_id`	UUID	Unique id.
`user_session_id`	String	Reference to the *User Session* that started the *Application Session.*
`ip`	String	The IP address of the client starting the application.
`appsession_start`	DateTime	Timestamp when the application session started in UTC.
`appsession_end`	DateTime	Timestamp when the application session ended in UTC.
`app_key`	UUID	Identifier of the application started.
`domain`	String	Name of the Workspace domain the application is configured.
`server`	String	Host name of the application server the application is started on.
`port`	String	The port op the application server used to start the application.
`exe`	String	The alias of the RemoteApp (empty for RDP applications).
`recorded`	Boolean	Indicated if the *Application Session* is recorded or not.
`rdpgw_session_id`	UUID	The internal id for the connection between the browser and Parallels Secure Workspace.
`rdpgw_numeric_id`	String	The internal id for the connection between the browser and Parallels Secure Workspace.

Web Application Sessions

Web Application Sessions represent web applications launched from the Workspace or access to a reverse proxied web application using the configured source host header or launched from the Workspace.

Property	Type	Description
`audit_type`	String	Record type (`webappsessions`).
`version`	String	Parallels Secure Workspace version.
`user_session_id`	String	Reference to the *User Session* that started the *Web Application Session.*

`timestamp`	DateTime	Timestamp when the *Web Application Session* started in UTC.
`url`	Sting	URL used to access the web application.
`name`	String	Name of the web application configured.
`domain`	String	Name of the Workspace domain the web application is configured.
`reverse_proxy`	Boolean	Indicated if the web application started is a reversed proxied web application.

Application Gateway

The Application Gateway is an internal component that determines a.o. on which application server an application can be started and also keeps track of the status of all application sessions. It manages both *Application Sessions* and *Web Application Sessions*.

The audit records of this component allow you to track changes in the state of all application sessions.

Property	Type	Description
`audit_type`	String	Record type (`appgw`).
`version`	String	Parallels Secure Workspace version
`timestamp`	DateTime	The timestamp of the status change.
`username`	String	Username of the user owning the application session.
`session_id`	UUID	Reference to the *User Session* that started the *Web Application Session.*
`session_labels`	String	A comma-separated list of all labels assigned to the user for the referenced *User Session.*
`domain`	String	Name of the Workspace domain the application is configured.
`appname`	String	Name of the application.
`appkey`	UUID	Identifier of the application.
`labels`	String	A comma-separated list of all labels assigned to the application.
`user_labels`	String	A comma-separated list of all user labels assigned to the application.
`server_labels`		A comma-separated list of all server labels assigned to the application.
`appsession_id`	UUID	*Application Session* id.
`status`	String	New status of the application session.
`host`	String	Host name of the application server the application is started on.
`gateway_id`	String	Name of the Parallels Secure Workspace appliance handling the application session.
`document`	String	UNC path to the document opened with the application.

File Actions

A *File Action* represents a file operation executed through the Workspace, this does not include file operations executed by streamed applications.

Property	Type	Description
`audit_type`	String	Record type (`file_actions`).
`version`	String	Parallels Secure Workspace version.
`timestamp`	DateTime	The timestamp of the action.
`session_id`	UUID	Reference to the *User Session* that executed the file action.
`action`	String	Action executed on the file.

`domain`	String	Name of the Workspace domain the drive is configured.
`drive`	String	Name of the drive the file action was executed on.
`destination_drive`	String	Name of the destination drive if the file action results on another drive.
`file_path`	String	The relative path of the file on the drive.
`destination_file_path`	String	The relative path of the file on the destination drive if the file action results on another drive.

Shares

Property	Type	Description
`audit_type`	String	Record type (`shares`).
`version`	String	Parallels Secure Workspace version.
`timestamp`	DateTime	The timestamp of the action.
`session_id`	UUID	Reference to the *User Session* that executed the file action.
`action`	String	Action executed on the share.
`domain`	String	Name of the Workspace domain the share is configured.
`share_id`	UUID	Unique ID of the share.
`share_name`	String	Name of the share.
`share_content_type`	String	Content-type of the share.
`share_expires`	DateTime	The expiry date of the share.
`share_drive`	String	Name of the drive the share is part of.
`share_domain`	String	Name of the Workspace domain the share is configured.
`share_created_by`	String	Username of the user that created the share.
`share_path`	String	The relative path of the file on the drive.
`share_mode`	String	Availability mode of the share.
`share_is_public`	String	Is the share publicly available.
`share_access_rights`	String	How are the access rights determined?
`share_access_labels`	String	Which users/groups can access the share when `share_access_rights` is USER.
`share_checksum`	String	The checksum of the shared file (when accessed).
`share_has_password`	String	Is the share password protected.
`ip`	String	The IP address of the client performing the action.
`country`	String	The country based on GeoIP of the client accessing the share.
`geoip_latitude`	String	The latitude based on GeoIP of the client accessing the share.
`geoip_longitude`	String	The longitude based on GeoIP of the client accessing the share.
`range`	String	Range accessed during request.

Shared Application Session

A *Shared Application Session* represents a guest that joined or leaves a shared application session.

Property	Type	Description

audit_type	String	Record type (sharedappsessions).
version	String	Parallels Secure Workspace version.
userapp_session_id	UUID	Reference to the *Application Session* that is shared.
sharedappsession_start	DateTime	The timestamp on which the client joined the shared application session.
sharedappsession_end	DateTime	The timestamp on which the client left the shared application session.
rdpgw_session_id	String	The internal id for the connection between the browser (guest) and Parallels Secure Workspace.
rdpgw_numeric_id	String	The internal id for the connection between the browser (host) and Parallels Secure Workspace.
ip	String	The IP address of the client that joined the shared application session.
domain	String	Name of the Workspace domain the application session is part of.

Shared Application Session Settings

A *Shared Application Session Setting* represents a change in the configuration of a shared application session.

Property	Type	Description
audit_type	String	Record type (sharedappsessions_settings).
version	String	Parallels Secure Workspace version
timestamp	DateTime	The timestamp of the action.
user_session_id	String	Reference to the *User Session* that started the *Application Session.*
userapp_session_id	UUID	Reference to the *Application Session* that is shared.
rdpgw_session_id	UUID	The internal id for the connection between the browser (guest) and Parallels Secure Workspace.
joinable	Boolean	Is the application session shared.
isProtected	Boolean	Is the shared application session password protected.
joinMode	String	Always SINGLE.
accessRights	String	Is the session shared in PUBLIC or DOMAIN mode.
host	String	The hostname of the Parallels Secure Workspace appliance handling the application session.
domain	String	Name of the Workspace domain the application session is part of.

Anomalies

An anomaly represents an unusual activity detected by the Parallels Secure Workspace environment. More information on the type of anomalies can be found in Anomaly Reporting .

Property	Type	Description
audit_type	String	Record type (anomalies).
version	String	Parallels Secure Workspace version.
timestamp	DateTime	The timestamp of the event.
session_id	String	Reference to the *User Session* if the user is logged in.
code	String	Anomaly code.
category	String	Anomaly category.

description	String	Anomaly description.
username	String	The username used for the login.
domain	String	Name of the Workspace domain the *User Session* is part of.
http_agent	String	The User-Agent header of the client.
ip	String	The IP address of the client.
country	String	The country based on GeoIP of the client.
geoip_latitude	String	The latitude based on GeoIP of the client.
geoip_longitude	String	The longitude based on GeoIP of the client.
fingerprint	String	The generated fingerprint of the client (NEW_BROWSER).
attempts	String	The number of failed login attempts (TOO_MANY_FAILED_ATTEMPTS).
distance_km	String	Distance in km (TRAVEL_SPEED).
distance_mi	String	Distance in mi (TRAVEL_SPEED).
speed_kmh	String	Speed in km/h (TRAVEL_SPEED).
speed_mph	String	Speed in mi/h (TRAVEL_SPEED).
existing_countries	String	A comma-separated list of countries for existing *User Sessions* for the user (COUNTRY_MISMATCH).

Backup and recovery of the Parallels Secure Workspace Environment

Introduction

Parallels Secure Workspace can generate an off-site backup of the Parallels Secure Workspace environment.

To backup an external database, please refer to the snapshot capabilities of MS SQL or PostgreSQL.

Backup

Parallels Secure Workspace saves the backup to the local disk of the appliance every day. You can retrieve this file and save it on another system using SFTP. In case of a database or disk failure, you can then recover your Parallels Secure Workspace environment.

This backup includes:

- Basic configuration info of the appliance itself (mostly the options displayed during the installation).
- Vault and vault unlock tokens (if applicable/optional).
- Internal database (if applicable).
- Some encryption keys.

Some data is not stored in the database and won't be recovered:

- Metering data (in the Dashboard).
- Shares.

The backup settings are found under **System Settings > Global > Connectivity > Environment Backups.**

To download the backup from the Parallels Secure Workspace environment:

- You need an SFTP-capable client (graphical tool: FileZilla or Bitvise SSH Client; Linux command-line: sftp).
- Connect to the IP or FQDN of the datastore node, on port 22. For a single-node environment, the database is located on the Parallels Secure Workspace appliance.
- Enter the username/password defined in System Settings.

Restore

To recover from a **broken internal database**, you can upload a previously downloaded backup to the Parallels Secure Workspace appliance via SFTP or use a backup that is still available on the appliance.

To recover from **broken Parallels Secure Workspace node(s)**, you can deploy a new appliance and import the environment backup during the installation wizard. Additional Parallels Secure Workspace nodes will not be added automatically after the initial restore, they need to be added again manually.

You can list the available backups on an appliance by executing the **environment-backup-list** action from the Troubleshoot page.

Same configuration and credentials apply for downloading or uploading dumps using SFTP.

After uploading a backup to restore to, execute the **environment-backup-restore** action from the Troubleshoot page.

If you restored to fresh new appliance, you will need to re-enter the Certificate and Private key (per domain: Configure > User Connector > Federated Authentication) when Single Sign-On is configured

- When restoring an environment to the same appliance(s) (using the troubleshoot action), each appliance needs to have **the same host name and Parallels Secure Workspace version**.
- When restoring an environment to a new appliance (upload environment backup during installation), the Parallels Secure Workspace appliance and environment backup need to be of **the same Parallels Secure Workspace version**.
- It is recommended to reboot the appliance(s) after the restore is completed.