Parallels Secure Workspace

Getting Started Guide

5.6

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

1. Parallels Secure Workspace Getting Started Guide 5.6 3
1.1 Introduction and assumptions 4
1.2 Set up your network 6
1.3 Install Parallels Secure Workspace appliance 14
1.4 Connect Parallels Secure Workspace to your Active Directory 16
1.5 Enabling SSL 19
1.6 Multi Factor Authentication 20
1.7 Publish apps and desktops 23
1.8 Publish drives 27
1.9 Prepare your Microsoft Windows back end 28
1.10 The Parallels Secure Workspace Installer 30
1.11 Customize the branding 31

Parallels® Secure Workspace

Parallels Secure Workspace

Getting Started Guide

Version 5.6

Introduction and assumptions

This document is a summary of all the steps that are needed to set up a single-node, single-tenant Parallels Secure Workspace appliance and integrate it into an existing Microsoft Windows infrastructure. For more details or complex setups, please consult the Parallels Secure Workspace Administration Guide.

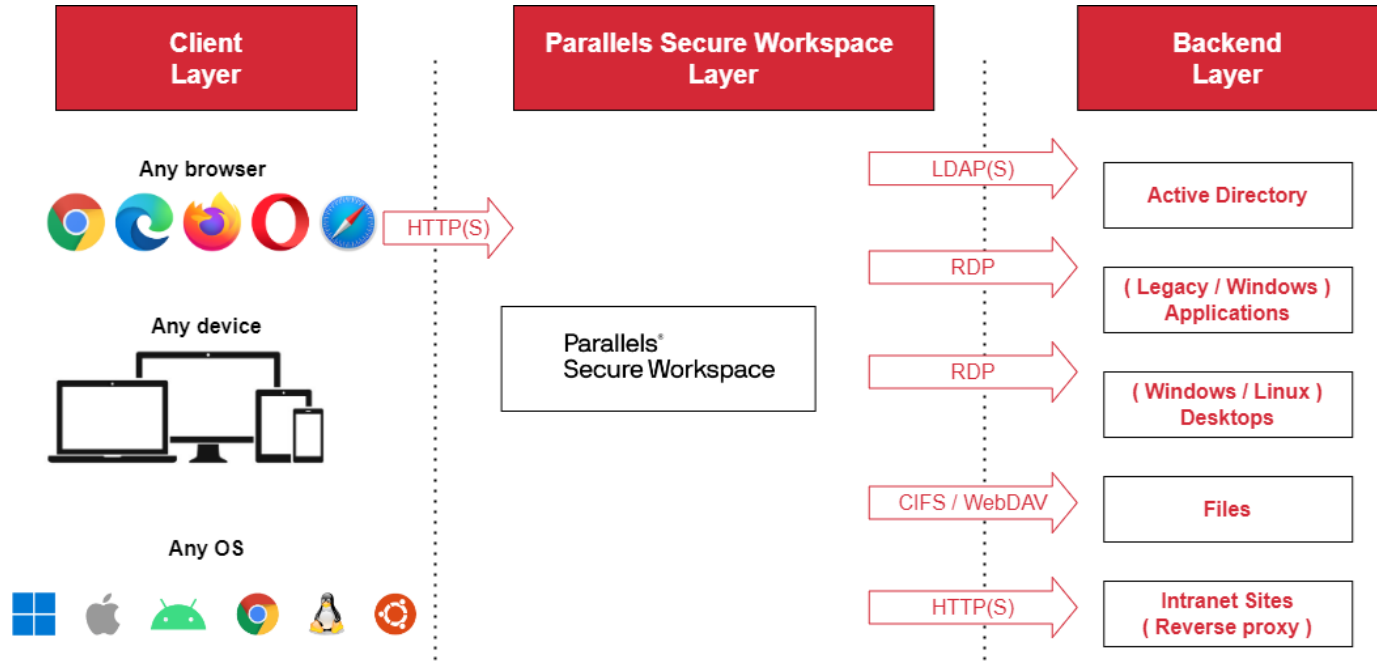
Next to this getting started guide, there is also a set of short 3-5 minute instruction videos available to help you install and configure Parallels Secure Workspace. We recommend using these videos in combination with this getting started guide. Videos can be found at https://awingu.com/technicalvideos or by searching on YouTube.

What is Parallels Secure Workspace?

Parallels Secure Workspace is a (virtual) appliance that acts as a gateway and allows secure connections from any modern (HTML5) browser to existing company resources such as:

- Microsoft Windows applications (via RDP)
- Microsoft Windows and Linux full desktops (via RDP)
- File servers (via CIFS/WebDAV)
- Intranet Web-based applications (via reverse proxy)
- SaaS applications

On top of this, Parallels Secure Workspace adds an extra layer of security (MFA, audit, encryption, recording, etc.) and collaboration (file and session sharing).



Parallels Secure Workspace itself is not a SaaS service. It needs to be installed and integrated into your own infrastructure. Parallels Secure Workspace is distributed as a virtual appliance. There are images available for most of the on-site and cloud-based infrastructures. In addition to this, Parallels Secure Workspace is multi-tenant, which means that a single Parallels Secure Workspace instance can be used for multiple customers, each with their own branding, Microsoft Windows backend, and configuration. Parallels Secure Workspace enables you to create your own SaaS offering for your clients while keeping full control over the complete solution.

Parallels Secure Workspace Architecture

There are 3 layers in the Parallels Secure Workspace Architecture:

- The client layer: Any web browser on any device on any operating system that supports HTML5 web sockets. This means that almost every modern browser should work.
- The Parallels Secure Workspace layer: One or more Parallels Secure Workspace virtual appliances.
- An existing Microsoft Windows-based back end: Microsoft Windows Active Directory (or LDAP) for user authentication; applications that are published on Microsoft Remote Desktop session hosts (terminal servers); files that are published on an SMB server.

These three layers are also completely isolated from each other. Both the client and the backend layer do not require any additional software installation. All connections from the client layer to the Parallels Secure Workspace layer are made using HTTP/HTTPS. The connections from

the Parallels Secure Workspace layer to the Windows backend layer use standard protocols like LDAP, RDP, and CIFS. More details on the different network flows can be found in the "install the appliance and set up your network" chapter of this guide.

The Parallels Secure Workspace (virtual) appliance is available for both:

- On-premises installations (Microsoft Hyper-V, VMware ESXi, Linux KVM, ...)
- Cloud installations (Microsoft Azure, Amazon EC2, Google Compute).

The Parallels Secure Workspace appliance can be downloaded from https://my.parallels.com . We recommend to always download and install the latest version.

Parallels Secure Workspace can be installed and configured without a license. All functionality will work, and up to two concurrent users will be able to log in to Parallels Secure Workspace. This allows you to test and set up without a license. Once you go into production, a Parallels Secure Workspace license needs to be purchased.

Assumptions

For this guide, we assume there is already an existing Microsoft Windows infrastructure which includes:

- A Microsoft Windows Active Directory (No Azure AD Only setup)
- Microsoft Windows applications servers (RDS / Terminal Servers) or VDIs (accessible via RDP)
- File server supporting CIFS/SMB access

More details on this Microsoft Windows backend can be found in the "Prepare your Microsoft Windows back end" chapter.

For this getting started manual, we assume this scenario:

- Only a single Parallels Secure Workspace instance. Parallels Secure Workspace can be configured in a "clustered" setup for purposes such as scaling or high availability.
- Only one Microsoft Windows back-end. Parallels Secure Workspace can be configured with multiple tenants, and each tenant can also connect to a different Windows back end.

Details on scaling and multi-tenancy can be found in the Parallels Secure Workspace Administration guide .

Set up your network

Before we start the installation, it is important to understand how the Parallels Secure Workspace appliance can be integrated into the existing network.

As the appliance doesn't require any agents or browser plug-ins on the clients and only relies on standard protocol access to the backend (also no agents or additional software), it can be easily installed in existing networks. Existing security equipment like firewalls, load balancers, SSL offloaders / reverse proxies can be reused.

Also, this architecture allows the three layers (clients, Parallels Secure Workspace, and the Microsoft Windows backend) to be upgraded independently from each other.

> Important: the appliance expects incoming traffic on port 80 (HTTP) or 443 (HTTPS).
> You can however make Parallels Secure Workspace accessible on a different port if you rely on e.g. a firewall or reverse proxy server to properly forward the incoming traffic to the correct ports.

In this Getting Started manual, we will describe three possible network scenarios. For more advanced network setups, please have a look at the full admin guide.

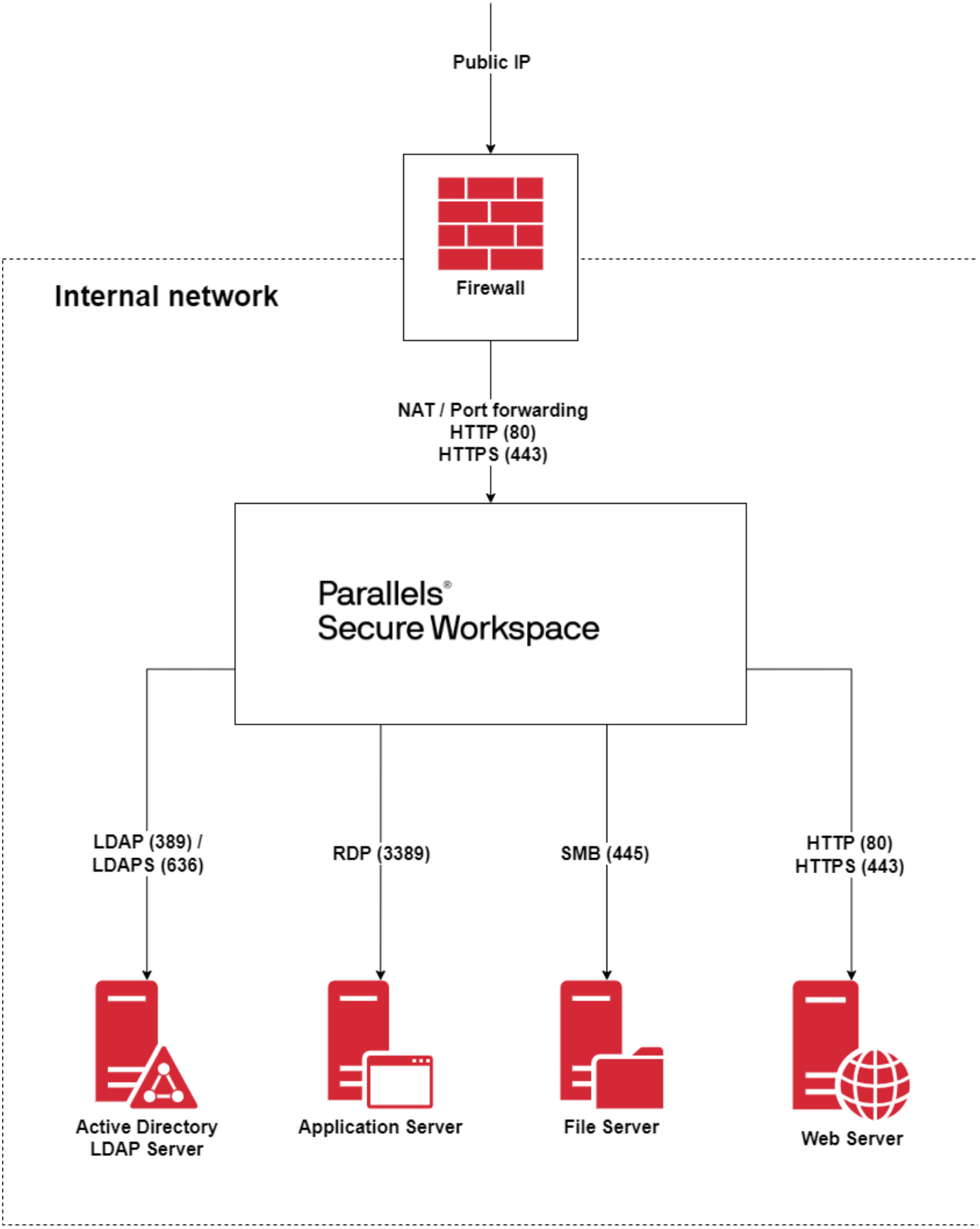
1. Parallels Secure Workspace behind a simple port-forwarding firewall
2. Parallels Secure Workspace behind a reverse proxy / load balancer that does SSL offloading
3. Parallels Secure Workspace in a DMZ network

Parallels Secure Workspace behind a simple port-forwarding firewall

This is the most simple scenario to deploy Parallels Secure Workspace. From the firewall, port 80 and/or 443 are forwarded to Parallels Secure Workspace, which is in the same network as the company resources (Active Directory, RDS, web server and/or file server). SSL offloading can be enabled on the appliance by using the built-in SSL offloader.

Parallels Secure Workspace supports two methods for SSL offloading: for this scenario to work, you need to forward the incoming HTTPS traffic (TCP port 443) to Parallels Secure Workspace. Parallels Secure Workspace can do the SSL offloading on the appliance.

- Using standard certificates. In this case, you need a certificate in the CRT / KEY format.
- By using the free public Let's Encrypt service that generates certificates. By providing the external DNS name to Parallels Secure Workspace, the certificates are automatically requested and renewed every three months. To use Let's Encrypt, incoming HTTP traffic (port 80) must be allowed.

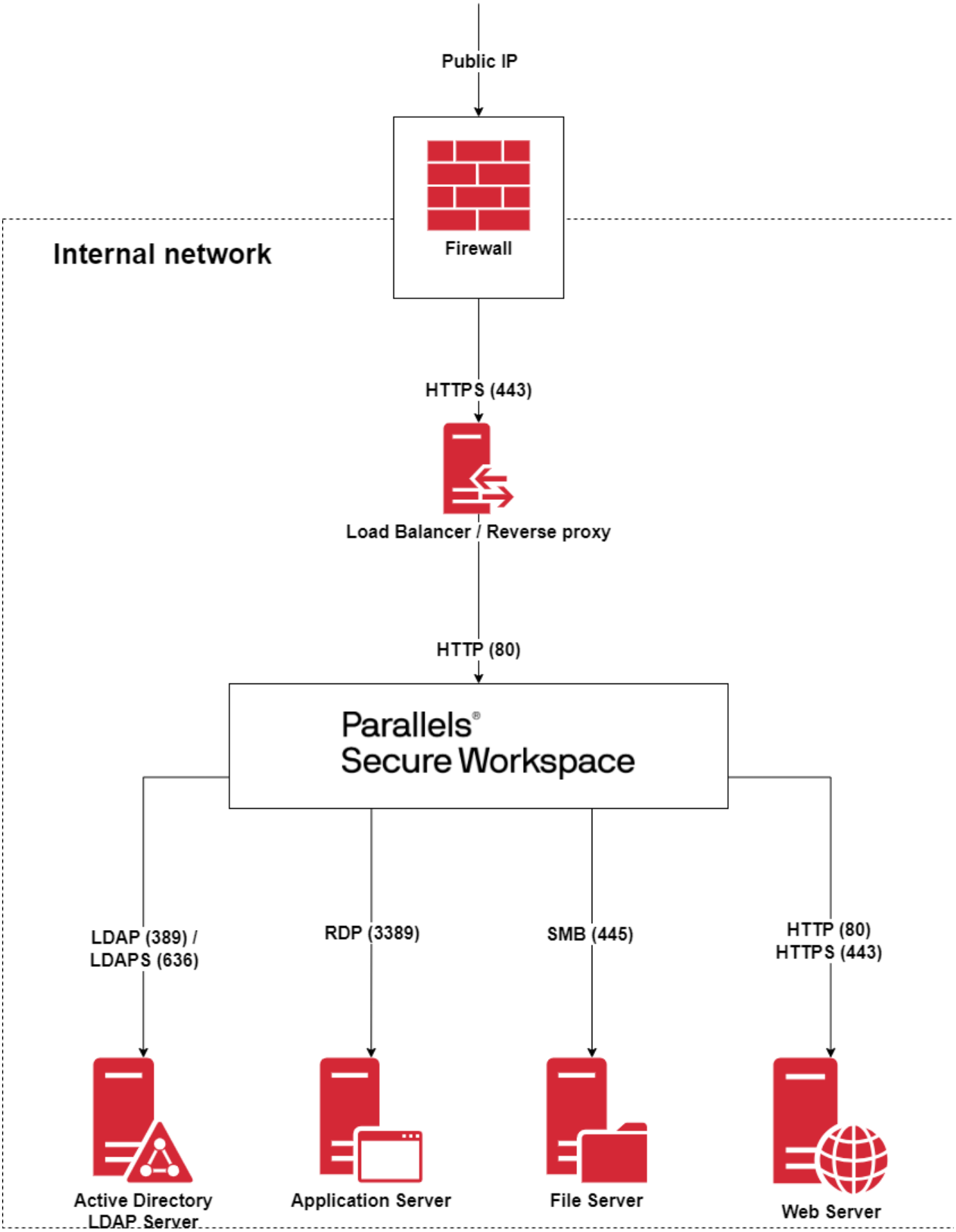


For this setup to work there are three requirements:

1. Port 443 (HTTPS traffic) on the public IP address needs to be forwarded to Parallels Secure Workspace. This assumes that no other service is already using this port. If this is the case, an additional public IP address needs to be added to the firewall.
2. This setup can only be used for single-node Parallels Secure Workspace setups. When using multiple nodes, you need to set up a load balancer / reverse proxy in front of Parallels Secure Workspace (see the next design).
3. A certificate is required in CRT/KEY format. In case you don't have a certificate, Parallels Secure Workspace allows you to automatically create certificates using the free Let's Encrypt service. In that case, also port 80 (HTTP) needs to be forwarded to the appliance.

Parallels Secure Workspace behind a reverse proxy / load balancer that does SSL offloading

In this scenario, there is an existing reverse proxy / load balancer / SSL offloader. On that device, there is a virtual host defined that forwards all traffic linked to a specific DNS record / host header to one or more Parallels Secure Workspace appliances. We also assume the reverse proxy / load balancer / SSL offloader also takes care of the SSL offloading.



The appliance is not directly accessible from the outside world and the reverse proxy / load balancer / SSL offloader will terminate the incoming traffic first and then proxy it to the Parallels Secure Workspace appliance. The main advantages are:

- You can have multiple services that use HTTPS traffic on the same IP address.
- In case the device is capable of doing load balancing: you can also use it in combination with a multi-node Parallels Secure Workspace.

Configure the reverse proxy / load balancer / SSL offloader correctly so it doesn't break the HTML5 web socket Parallels Secure Workspace uses.
Make sure the header information is preserved, so that Parallels Secure Workspace knows what the original IP addresses were rather than always getting the IP address of the reverse proxy / load balancer / SSL offloader.

The admin manual contains all the details. You can also you can find some specifics for some vendor-specific solutions like F5, Netscaler, and Nginx on the support portal.

In most cases, these headers need to be set correctly on the device:

Header	Value	Status
Connection	This value should be equal to "Upgrade"	Mandatory for getting web sockets to work
Upgrade	Should be equal to “websocket” in case of a WebSocket upgrade	Mandatory for getting web sockets to work
X-Forwarded-Proto	This value should be equal to "https"	Mandatory for getting web sockets to work
X-Real-IP	This should be the IP address of the requesting client	Recommended for security
X-Forwarded-For	This should be the IP address of the requesting client	Recommended for having correct auditing
X-Forwarded-Host	This is the FQDN of the server name that was requested by the client	Recommended for having correct auditing
Host	This is the FQDN of the server name that was requested by the client	Recommended for having correct auditing

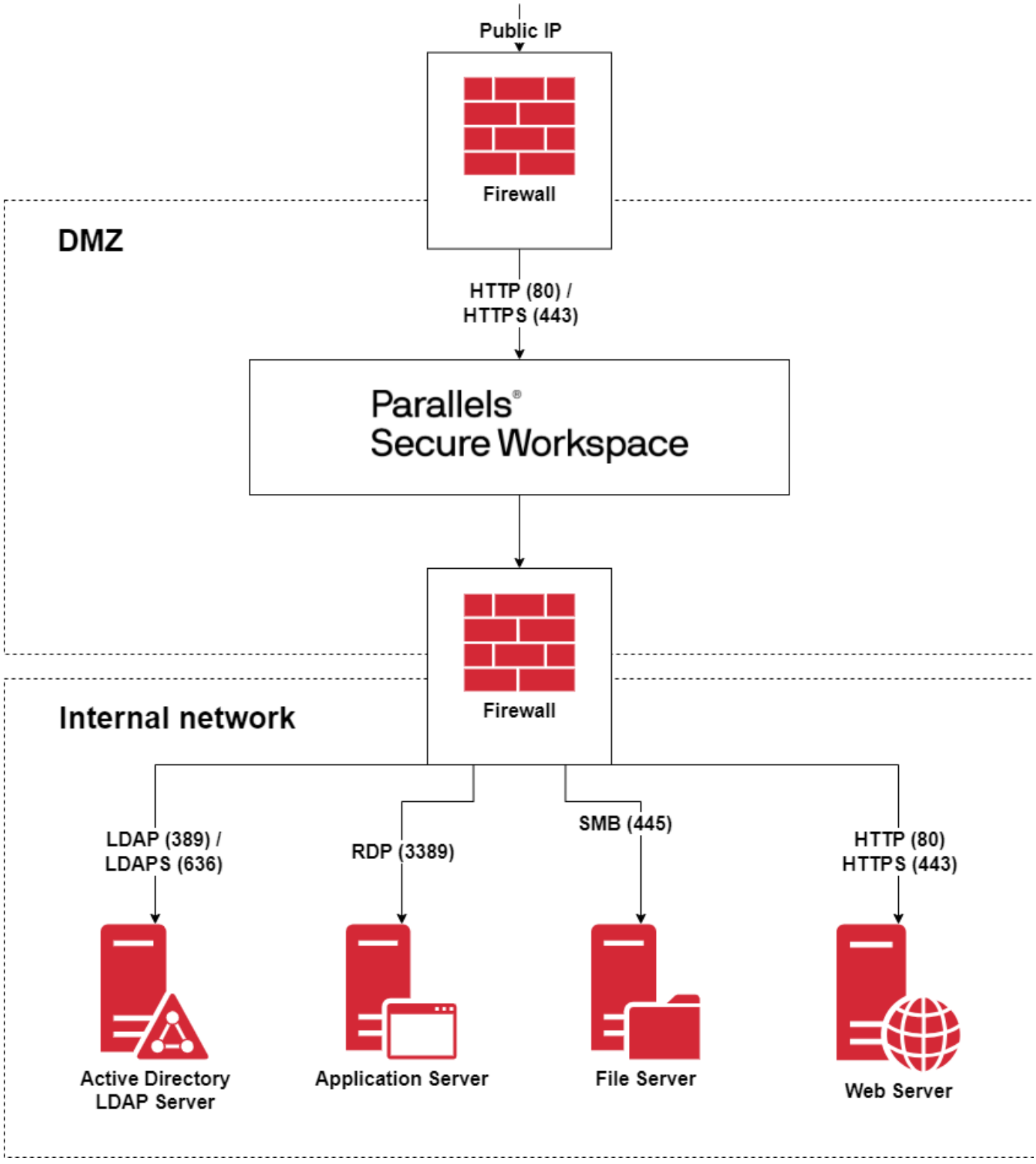
Parallels Secure Workspace in a DMZ network

As Parallels Secure Workspace only uses standard protocols and ports, it can easily be installed in a DMZ network.

Both scenarios (port forwarding or reverse proxy) can be used to access the Parallels Secure Workspace environment from the public network. In this chapter, we describe all other network flows that are needed to get Parallels Secure Workspace installed and working from within a DMZ or firewalled network:

- User authentication.
- Accessing resources such as Microsoft Windows apps, storage, VDIs, and web apps.
- Installation and other needed network traffic.

When using a multi-node Parallels Secure Workspace, it is important that all nodes can freely communicate with each other. So all Parallels Secure Workspace nodes of a multi-node cluster need to be in the same network with no firewalls between the individual nodes.



User Authentication network flows

Parallels Secure Workspace uses LDAP or LDAPS (recommended) to communicate with the AD or LDAP server. This communication is used to validate the user credentials and also fetch the security groups of the user. When password changes in Parallels Secure Workspace are allowed, Kerberos communication is needed, and it is mandatory to use LDAPS (TCP 636). Doing password changes via LDAP (TCP 389) communication will not work.

Communication	From	To	Information
LDAP: TCP port 389	Parallels Secure Workspace	All AD or LDAP servers in the configuration	
LDAPS: TCP port 636	Parallels Secure Workspace	All AD or LDAP servers in the configuration	Only required when users need to be able to change their password. Also requires certificates on the AD / LDAP server.
Kerberos: UDP port 88 and TCP port 88	Parallels Secure Workspace	Kerberos server	Only required when users need to be able to change their password at the next logon. 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: UDP port 1812	Parallels Secure Workspace	RADIUS server	Only required when using an external, RADIUS-based, MFA server Parallels Secure Workspace also offers the possibility to integrate natively with some third-party MFA providers such as Duo. More details on network flows can be found in the admin manual.

Application and Storage network flows

Parallels Secure Workspace uses RDP to connect to Windows-based applications and desktops. Besides network access, no other access is needed. In case a Microsoft RDS broker is used, Parallels Secure Workspace needs RDP access to both the broker and all individual session hosts that are configured behind the broker.

Storage can be accessed through CIFS and WebDAV.

Parallels Secure Workspace can also publish web-based applications. In case the websites are external to the organization, the browser will open them directly. This traffic will not pass through Parallels Secure Workspace.

It is also possible to access internal websites. Parallels Secure Workspace will act as a reverse proxy and needs to be able to access the internal website.

Communication	From	To	Information
RDP: TCP port 3389	Parallels Secure Workspace	Session hosts, VDI hosts and RDS brokers	
CIFS: TCP port 445	Parallels Secure Workspace	All storage servers.	Only needed when offering Parallels Secure Workspace Drives via CIFS
WebDAV: TCP port 80/443	Parallels Secure Workspace	All storage servers	Only needed when offering Parallels Secure Workspace Drives via WebDAV
HTTP/HTTPS: TCP port 80/443	Parallels Secure Workspace	Web servers	Only needed for internal web apps published through the reverse proxy feature. In case the internal website does not run on standard ports 80 or 443, this non-standard port needs to be added to the firewall rules.

Other network flows

During the Parallels Secure Workspace installation, we need to configure NTP, DNS and database access. The installation web interface is reachable on port 8080. After the installation has finished, this port is no longer needed.

In most simple cases, the Microsoft Windows Active Directory domain controller(s) also acts as the DNS and NTP server. Parallels Secure Workspace also supports more complex setups with different DNS servers per tenant.

To do this, there are two levels of DNS:

- DNS servers can be configured on the **global** appliance level. These servers are configured during the installation. These are used if there is no tenant-specific DNS configuration or for the resolution of names linked to the appliance (for example proxy server, Parallels Secure Workspace update server, ...)
- Each **tenant** can also be configured with optional **DNS servers**. These servers are configured when adding a tenant. These are used to resolve the host names of the servers specified in the tenant's application server or drives section. These can be different servers per tenant. So there is no need to have a global DNS service spanning all individual tenants.

Communication	From	To	Information
Installer: TCP port 8080	Install PC	Parallels Secure Workspace	Only needed once during the first time installation. The firewall rule can be removed after the installer has finished
NTP: UDP port 123	Parallels Secure Workspace	NTP servers	Mandatory. Parallels Secure Workspace needs to connect to a time server to make sure clocks get synchronized. In most cases, the Microsoft Windows Active Directory domain controller(s) also can function as a NTP server. If no internal NTP server is available, a public one like pool.ntp.org can be used.
DNS: UDP port 53	Parallels Secure Workspace	All DNS servers.	Mandatory. Parallels Secure Workspace needs to do name resolution of all the servers specified in the configuration. So both the global DNS servers and the optional DNS servers specified in the tenants need to be reachable from the Parallels Secure Workspace appliance.

When using an external database that is not in the DMZ network, also make sure all nodes have access to the database!

Install Parallels Secure Workspace appliance

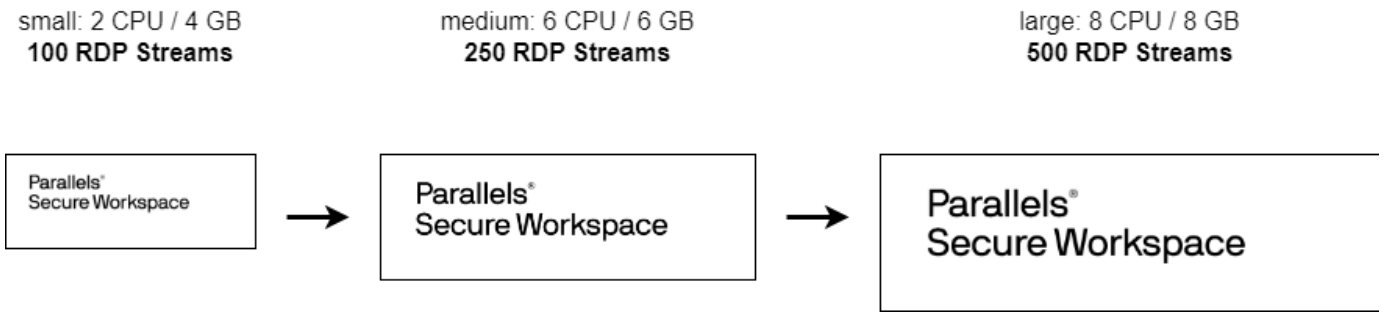
The Parallels Secure Workspace appliance is available for on-premises installations or cloud installations. In this getting started guide, we guide you through the installation of a single node Parallels Secure Workspace. Please note that Parallels Secure Workspace can also scale out vertically by adding more nodes to the cluster. Details on multi-node deployments are described in the admin manual.

There is no difference in features and functionality between running Parallels Secure Workspace on-premises or in the cloud. Only the installation process is slightly different and will be discussed shortly in this chapter. Once the image is deployed, all the configuration is exactly the same.

Parallels Secure Workspace Sizing Requirements:

Minimum sizing is 2 CPU, 4 GB RAM, and 80 GB hard disk.
Warning: 3.7 GB that is suggested is not sufficient on some public clouds!

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



We generally recommend that as of 300 concurrent RDP streams, it is better to look at a multi-node setup. For more details on sizing and multi-node setups, please have a look at our Admin Manual for more details.

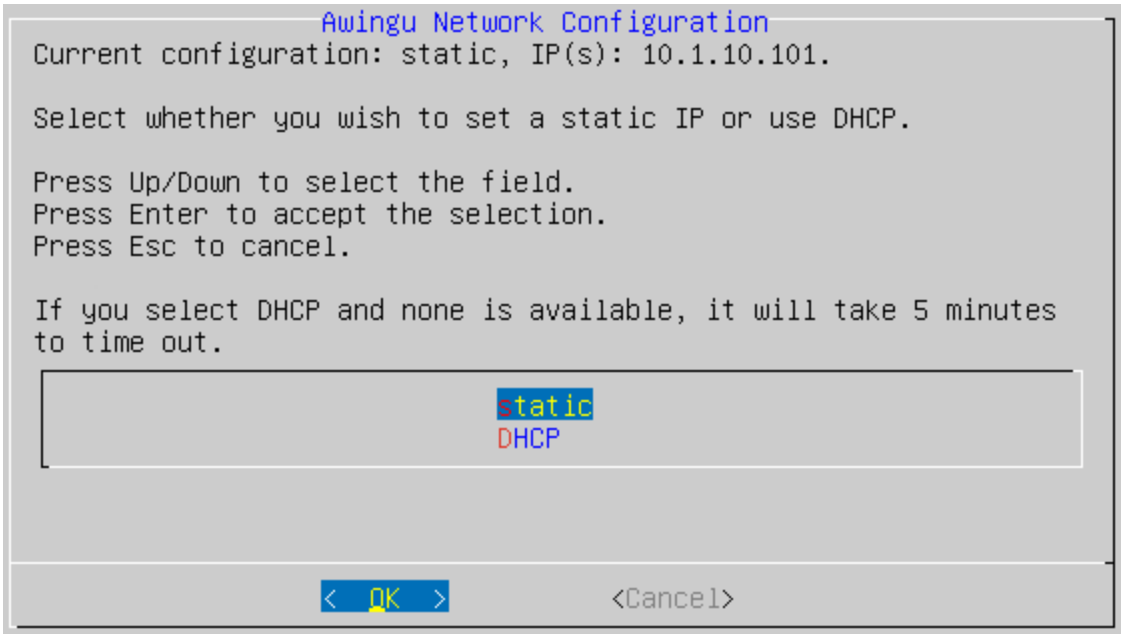
For deployment on private clouds / on-premises infrastructure:

The Parallels Secure Workspace image can be downloaded from https://psw.parallels.com/appliances/latest/

From here, the appliance images for all the supported hypervisors can be downloaded.
Refer to the admin manual of the specified version to check which hypervisors and cloud platforms are supported.

Please always download the latest version if you start a fresh installation. The older versions are made available for users who would like to extend their existing Parallels Secure Workspace cluster with additional nodes, or who need to recover from an environment backup created on a specific version.

Our admin guide contains details on how to import the different images on the different hypervisors. Once the image has been booted, it will broadcast a DHCP request, and it will honor the received IP information. You can also access the console to change the IP address to a static address. After the IP has been correctly set, you will be able to go through a web-based installation wizard.



Deployments on public clouds

Microsoft Azure Cloud

On Azure, the image can be deployed from the Azure Marketplace. You can simply add a new resource and search for Parallels Secure Workspace to find the appliance in the marketplace. When you search for Parallels Secure Workspace, you will find 2 solutions in the Azure catalog:

- Parallels Secure Workspace: The standard appliance, similar to the images you can download for on-premises. Installation still needs to be done, and you need an existing Microsoft Windows backend to connect to.
- Parallels Secure Workspace All-In-One: A template that not only installs a standard appliance but also creates a new Microsoft Windows Active Directory server and at least one Remote Desktop session host (terminal server). Also, all configuration and installation of the Parallels Secure Workspace and Microsoft Windows back end is done automatically so that at the end of the installation you have a fully working green-field setup available.

Amazon Web Service (AWS)

Images for Amazon Web Service subscription can be readily deployed via the links provided on https://psw.parallels.com/appliances/latest/.

Google Cloud Platform

Navigate to https://psw.parallels.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 Cloud Platform 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.

Connect Parallels Secure Workspace to your Active Directory

First login and System Settings

Once the installation has finished, you will be able to log in to the Parallels Secure Workspace appliance with the built-in username and password.

Browse to the IP or DNS name of the Parallels Secure Workspace appliance on port 80. (for example http://172.16.0.10/).
In the login form, leave the domain field blank. The first time you log in, you will need to accept the privacy statement.

After logging in, you will see the Workspace with three applications available:

1. **System settings**: Here you can manage your environment and make the necessary changes to the configuration.
2. **API Docs**: Since Parallels Secure Workspace is fully API-driven, this application will open the API interface and show you the API documentation.
3. **Dashboard**: Here you can see all auditing and monitoring information.

Open the System Settings by clicking on the associated icon.

Add a Domain

Parallels Secure Workspace has no internal user database and needs to be connected to an existing Active Directory domain controller or LDAP server. In this guide, we will go through all the steps needed to link the appliance to an existing Active Directory domain.

Start by navigating to **System Settings > Global > Domains**.

Click on [Add] and scroll down to add the first tenant/domain.

The following parameters are mandatory:

- Name: This is the internal name used for this **Parallels Secure Workspace domain**. By default, this is the same as the NetBIOS.
- NetBIOS Domain Name: NETBIOS domain name (e.g. COMPANY)
- Domain FQDN: The FQDN of the **Microsoft Windows domain**, not for the AD (eg. company.local).
- DC/LDAP Server: FQDN (recommended) or IP address of the Domain Controller or LDAP server. E.g. ad01.company.local. Multiple servers can be entered comma-separated. The first server will always be contacted first during login. Only when the first one is not available, the next one will be contacted.
- Base DN: When a user signs in, this base distinguished name (DN) is used to bind to the Domain Controller/LDAP server. This can be used to filter access based on the organizational unit (OU).
  - Example without OU restriction: dc=company,dc=local
  - Example with OU restriction: ou=Employees,dc=company,dc=local
- LDAP over SSL?: Recommended to set to “Enabled”. In that case, make sure there is a certificate on the Domain Controller or LDAP server. Mind that LDAP over SSL must be enabled to be able to make changes to passwords in Parallels Secure Workspace.

You can validate the settings using the following PowerShell command on the Active Directory server:

```
PS C:\temp> Get-ADDomain | Select NetbiosName, DNSRoot,
InfrastructureMaster, Distinguishedname | Format-List

NetbiosName          : COMPANY                    <--- NetBios Name
DNSRoot              : company.local              <--- FQDN for UPN
InfrastructureMaster : ad1.company.local              <--- DC/LDAP
server
Distinguishedname    : DC=company,DC=local        <--- base DN
```

Optional parameters:

We will add application servers to Parallels Secure Workspace and also import users and security groups. To do this automatically from Active Directory, a bind user and password are required. If not set, auto-import will not work and these servers, users and groups will need to be created manually in Parallels Secure Workspace. The bind user/password should be a normal user and doesn't have to be a domain admin.

- Bind Name: The username of the service account. (example: serviceuser). No domain or FQDN needs to be added.
- Bind Password: The password required to authenticate the service account.

The "create bind name", "Find Groups" and "Privacy Policy Acceptance" parameters should not be changed. See the Admin Manual for more information.

Multi-tenancy parameters:

Parallels Secure Workspace supports multi-tenancy, which means that in a single Parallels Secure Workspace cluster, you can have multiple domains with their own branding and configuration. To do so, add multiple domains. To support this multi-tenancy some extra parameters have been added. In this Getting Started guide, we only configure a single tenant. If more tenants are added, the following parameters will be needed:

- Host Headers:
  - Single tenant: This can be left blank, but it is recommended to specify the host header that users will use to access the environment (e.g. workspace.company.com).
  - Multi tenant: List all public host headers/DNS names (workspace.company.com) linked to the domain/tenant. When navigating to one of these host headers, Parallels Secure Workspace will automatically load the correct tenant.
- Administrative Domain:
  - Single tenant: Keep the default value “Yes”.
  - Multi tenant: If set to “Yes”, all admins in this tenant will also be able to manage the other tenants. You need at least 1 tenant with the administrative domain parameter set to “Yes”.
- DNS Server:
  - When left blank, the global DNS server will be used. In a multi-tenancy setup, it usually means the internal DNS servers for the Active Directory domain must be specified. These DNS servers must be able to resolve the server names in this domain.

Test the login

When finished, click on the "Add" button at the bottom of the page. Parallels Secure Workspace will now add the tenant and make the link with the domain controller.

To test if the settings are valid, log in with a normal domain user:

1. Close the "System Settings" tab in the browser.
2. In the Workspace, at the bottom left, click on the built-in admin user and select log out.
3. Try to log in with a normal domain user. You can use either the sAMAccount (`domain\user` or `user`) or the UserPrincipleName (`user@domain.org`)

If it works, you know your domain settings are correct!

Labels

All configuration in Parallels Secure Workspace is done using "labels". Labels are a combination of a key and a value.

There are different kinds of labels:

- **User Labels:** These start with `username:` or `group:` and can be used to link to a specific user or group in AD. For example, the label `group:Administrators` refers to the Active Directory group Administrators, the label `username:steven` refers to the user `steven` in AD.
- **Server Labels:** These do not have a fixed format. But for example every time you import or add an application server, `appserver:ServerName` is created so it can be used directly in the configuration.
- **Context Policy Labels:** These restrict access rights based on the user's context (for example: the user must have authenticated using MFA, they must be logged on from within a certain country or IP range).
- Next to these labels, there are some built-in labels such as `all:` , `admin:`, `record:`, ...

The easiest way to add user or group labels, is to import them automatically. Go to **Manage > Labels** and click on the [Import from AD] buttons. Once the groups and/or users are imported, Parallels Secure Workspace will keep tracking them when the user signs in. So when a user is added to a group in AD, no extra actions are needed on the Parallels Secure Workspace side.

More information on the labels can be found in the Admin Manual.

If import from AD doesn't work (there is a red error message), this is probably caused by a wrong user/password in the domain configuration. The import from AD uses the bind user specified in the domain settings.

Fine-tune the access rights

Log in with the built-in admin and open the System Settings.

Currently, all domain users can log in to Parallels Secure Workspace and only the built-in user can manage the configuration.

Assume you have two security groups in Active Directory to which you would like to limit access:

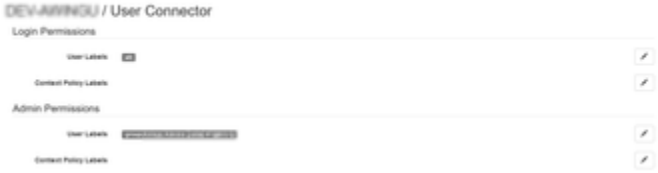
- "Parallels Secure Workspace Users" contains all users that are allowed to log in.

- "Parallels Secure Workspace Admins" contains the users who should have administrative rights in Parallels Secure Workspace.

You can authorize groups by adding a `group:<groupname>` label to User Labels. The first time you use a label, you'll have to select the “Create new” option in the dropdown. After that, you can select the label from the list.

Go to **Configure > User Connector**.

Here, you will find the login permissions. Add the group or user labels to the “User Labels” that need to be admin in Parallels Secure Workspace in the "Admin Permissions" section. In this example, we have added the group "Parallels Secure WorkspaceAdmins". By default, the “User Labels” for the “Login Permissions” are set to "all". This means that all users in the domain can log in. In this example, we have restricted access to the Parallels Secure Workspace environment to the users that are part of the "Parallels Secure Workspace Users" and "Parallels Secure Workspace Admin" groups.



Once this is done, log out with the built-in user and log in with a user that is part of the "Parallels Secure Workspace Admins" security group. As you will see, this user now also has access to the Parallels Secure Workspace admin configuration and there is no need anymore to use the built-in user for normal day-to-day configuration.

Enabling SSL

As Parallels Secure Workspace is 100% web-based, it is important to encrypt the traffic. To do so, there are different possibilities. One of them is to use the internal SSL Offloader of Parallels Secure Workspace which we will explain in this chapter.

> If you plan to use an external SSL Offloader, check the Admin Manual on how to configure it correctly so the websockets used in Parallels Secure Workspace are handled correctly. Pay attention to the headers that need to be passed.

To enable SSL offloading, you will need a certificate to encrypt the web traffic.

There are three ways to get a certificate:

1. You obtain a valid certificate issued by a certificate authority. In that case, make sure it is in CRT/Key format. If not, use OpenSSL to convert it to the correct format. Both individual and wildcard certificates are supported.
2. You generate a self-signed certificate. This is not recommended, as web browsers do not always accept them.
3. You use the built-in integration of Parallels Secure Workspace with Let's Encrypt, a free third-party certificate authority, to automatically request certificates.

> The Parallels Secure Workspace appliance needs to be accessible from the outside world (internet) via port 443 and in case of Let's Encrypt also from port 80. Port 80 needs to remain open for certificate renewals when using Let's Encrypt. If it is not open, the certificate renewal won't work and the appliance will stop working after 3 months!
>
> Parallels Secure Workspace has a built-in redirect feature that will automatically redirect incoming HTTP traffic to HTTPS. So no end users will be allowed to connect to the appliance using plain HTTP .

Before uploading the obtained/self-signed certificate or generating the Let's Encrypt certificate, also make sure the public DNS name you would like to use is correctly configured.

To enable HTTPS and use the certificate, navigate to **System Settings > Global > SSL Offloading**.

Click on [Add] at the bottom to add a certificate. Parallels Secure Workspace can handle as many certificates as needed, so you are not limited to a single certificate.

- To manually import a certificate, upload the CRT and Key file or the .pfx file. Parallels Secure Workspace will automatically extract the certificate's name.
- To automatically request a certificate using Let's Encrypt: specify the public DNS name that can be used to access the Parallels Secure Workspace appliance.

Then, click on "Add". The Parallels Secure Workspace appliance will now install the certificate and be both accessible on both HTTP and HTTPS.

Redirect HTTP traffic to HTTPS

Enable the redirect feature so that all incoming traffic on port 80 (HTTP) is redirected to port 443 (HTTPS).

> To enable this redirection, you must be connected over HTTPS. So first log out of the Parallels Secure Workspace environment and log in using HTTPS.

Open **System Settings > Global > SSL Offloading** and change the SSL Offloader from "Optional HTTPS" to "Internal SSL offloading with enforced HTTPS":

Multi Factor Authentication

Parallels Secure Workspace can be configured to do a second-factor authentication in addition to the login/password check.

There are three ways to activate MFA:

1. Use one of the built-in options:
   a. Workspace OTP: Counter based
   b. Workspace OTP: Time-based (recommended built-in option)
2. Use a built-in connector for DUO security.
3. Use the RADIUS connector to connect to any MFA solution that supports RADIUS (Symantec VIP, RSA, Vasco, etc.). Only PAP is supported.

Check the admin manual for further configuration details. In this Getting Started guide, we will configure the built-in solution.

> The counter-based tokens are not supported by Microsoft Authenticator and a lot of other common authenticator apps.
> If you would like to use Microsoft Authenticator, use the Time Based option.
>
> Google Authenticator supports both counter- and time-based OTP.

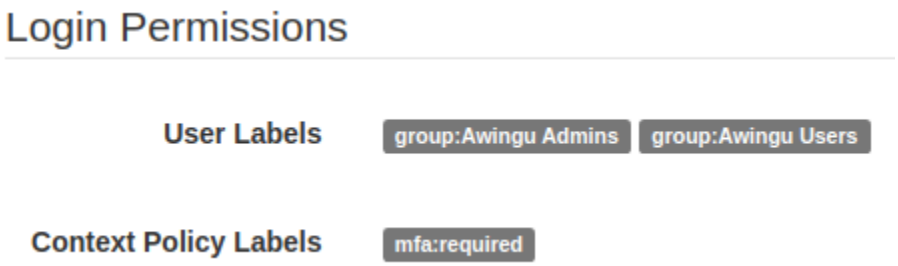
To enable MFA, go to **System Settings > Configure > User Connector**.

Scroll down to the "Multi Factor Authentication" section and set the mode to "Workspace OTP: Time based"

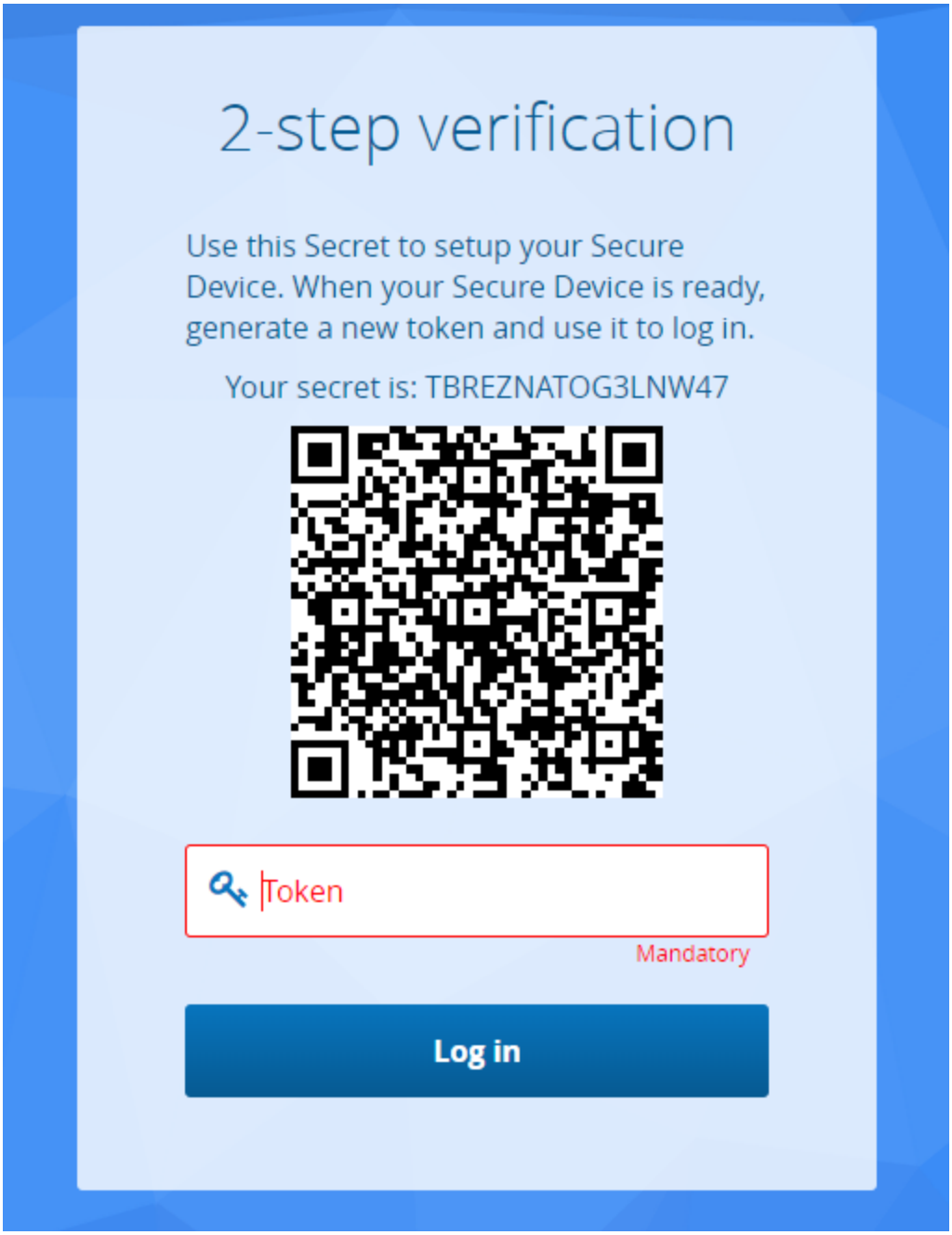
Optionally you can:

1. Set a list of IP addresses or ranges of IP addresses for which the MFA will not be asked. This could, for example, be used to exclude MFA validation for connections from within in the office.
2. Set a list of user or group labels that are excluded from using the MFA.
3. Enable the Trusted Browser feature. If enabled, the user will have the option to disable the MFA check for 30 days on a specific device / browser.

Now MFA is configured, we can enforce it for all users. On the same page, go to the top. In the "Login Permissions" section, add `mfa:required` to the "Context Policy Labels".

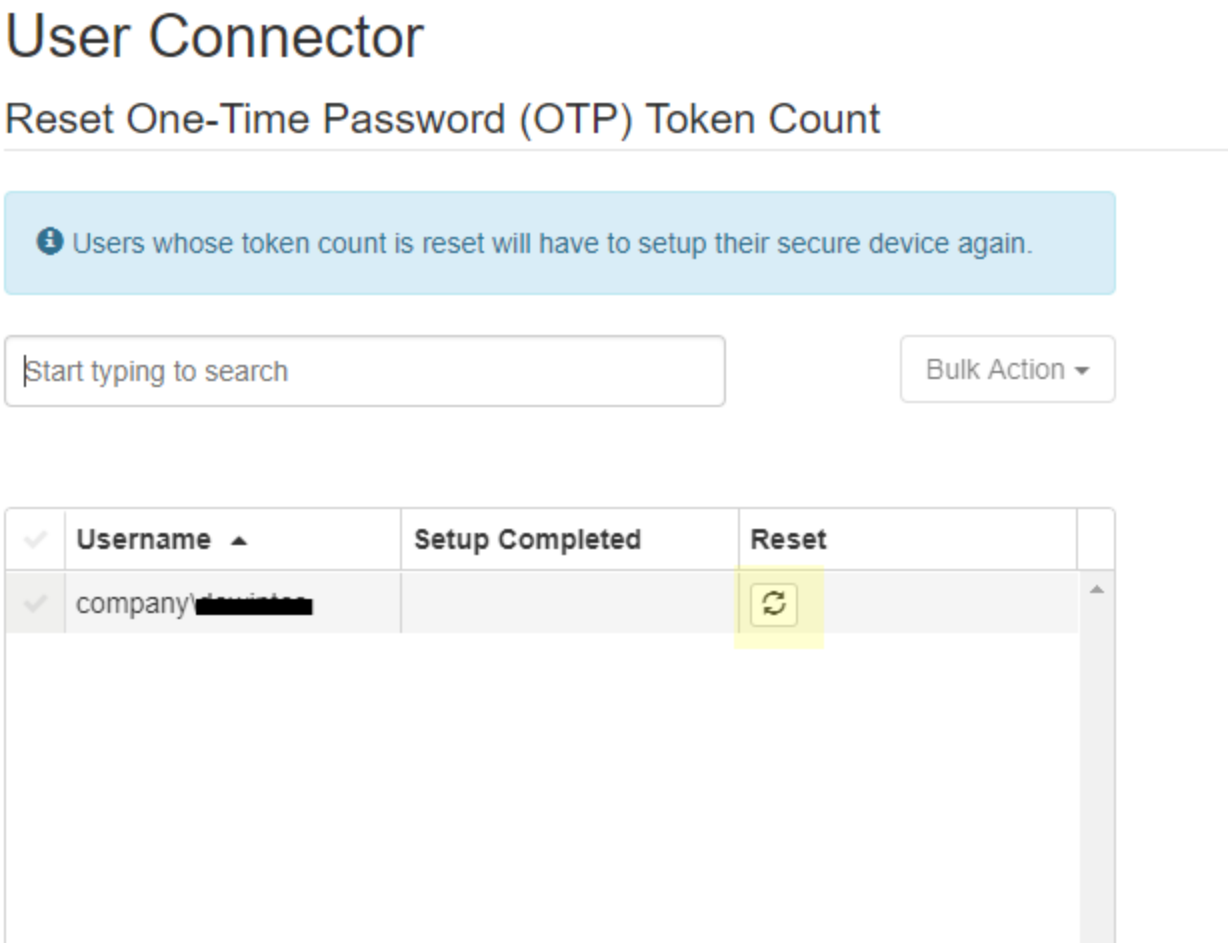


To check if it works, log in again with any user from an IP address that is not in the white list. The first time you connect, you should see a QR code on the screen:



Open the authenticator app of your choice. Scan the QR code and enter the 6-digit code. As of now, your authenticator app is linked to your Parallels Secure Workspace user account.

In case somebody needs to reset the token, go to **Configure > User Connector: Multi-factor Authentication**. Click on "Manage user token count":

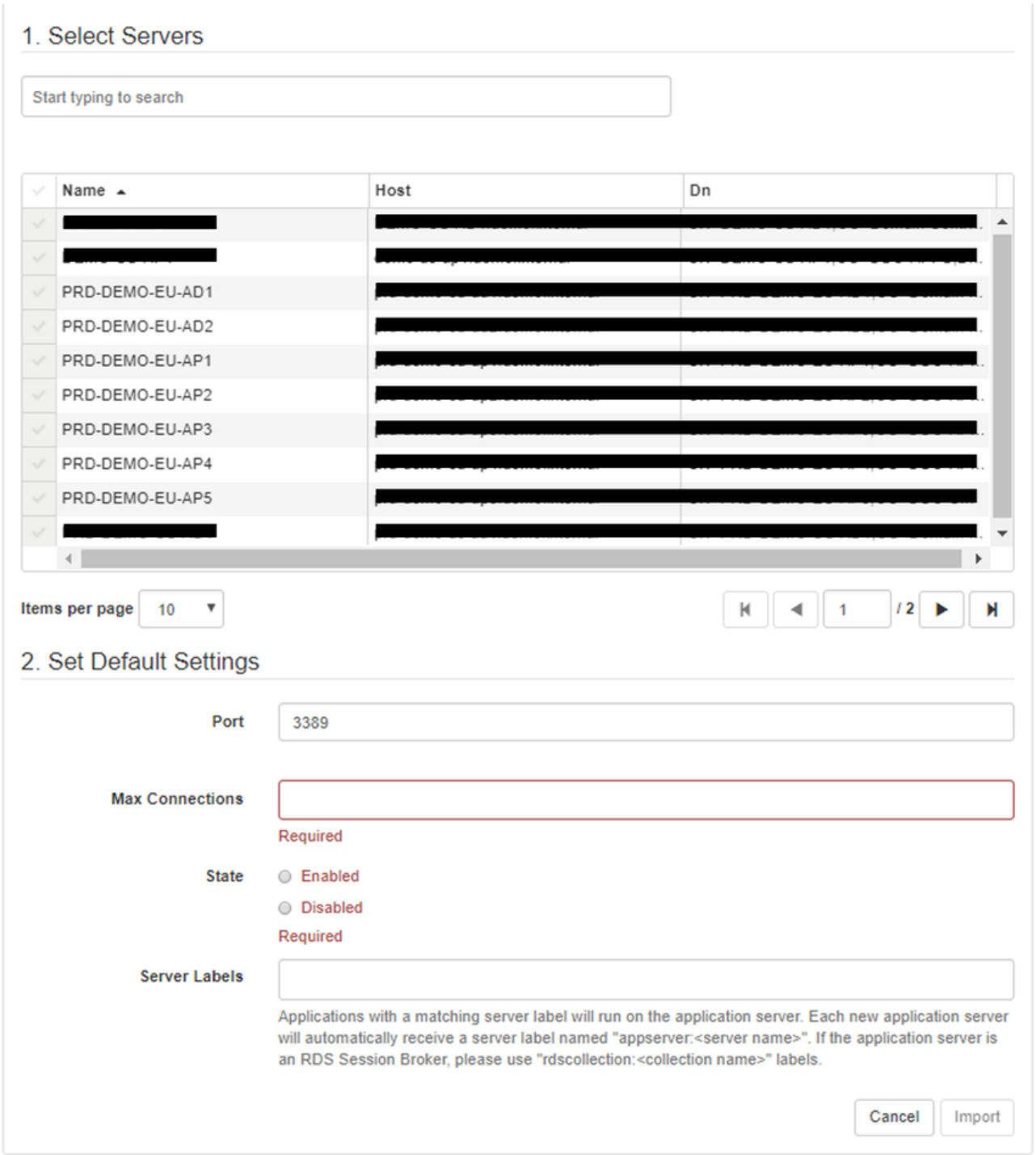


Click on the [Reset] button for the user whose token you'd like to reset. The next time the user logs in, they will be able to go through their MFA setup again.

Adding Application Servers

Before we can add applications in Parallels Secure Workspace, we first need to add the application servers. Navigate to **System Settings > Manage > Application Servers**.

We assume you have configured a bind user/password in the "Connect Parallels Secure Workspace to your Active Directory", so we can use the "Import from AD" option.



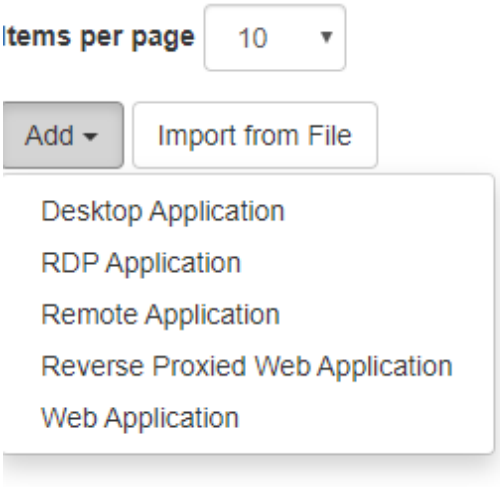
Select the remote desktop session hosts to which Parallels Secure Workspace should connect. Once the servers are selected, specify the number of concurrent connections that can be made to this machine in the “Set Default Settings” section. Also, set the state to enabled. When finished, click on [Import]. As of now, the application servers are configured and can be used later when creating applications in Parallels Secure Workspace.

When adding a Microsoft Windows Client OS (such as Windows 11) or when adding servers that do not have terminal server installed on them, the value of maximum connections needs to be set to 1.

Adding an application/VDI

Before you start adding applications or desktops, make sure the application servers are imported. If you would like to restrict access to a certain group or list of users, make sure the user labels have also been imported!

To add any type of application (remote app, rdp app, web app, etc.) or VDI, open the Applications page (**System Settings > Manage > Applications**) and then click on [Add].



These are the supported application types:

- **Desktop Applications:** Use this if you would like to make a full desktop connection to a Microsoft Windows Server or Client OS.
- **Remote Applications**: Access a Microsoft Remote Application (RemoteApp). On the Microsoft Windows back end, the app first needs to be added to an RDS collection.
- **RDP Applications:** In this case, the app is started as an alternative shell.
- **Web Applications:** Link to a publicly available website.
- **Reverse Proxied Web Applications:** Parallels Secure Workspace will act as a proxy server for this internal web application to also make them available externally.

In thuis guide, we will limit the documentation to a standard setup of a Desktop Application and a Remote Application.
For the other kinds of applications or advanced settings, please have a look at the Admin Manual.

Generic Settings:

These settings are common for all types of applications:

- **Name:** The application name as it will appear in the Workspace.
- **Description:** Description of the application. This is not visible to end users.
- **Icon:** The application icon that will be visible to the end user in the Workspace. Only ICO, JPG, and PNG are allowed. Maximum size is 100 KB.
- **Categories:** This application will be shown in the selected categories.
- **Context Policy Labels:** Restrict this application to only be accessible within the provided security context. This context can be a list of countries, a list of networks, or the requirement that MFA must be used.

Desktop Application Settings

When adding a Desktop Application, the only thing left to do is to link the application to the correct user and server labels.

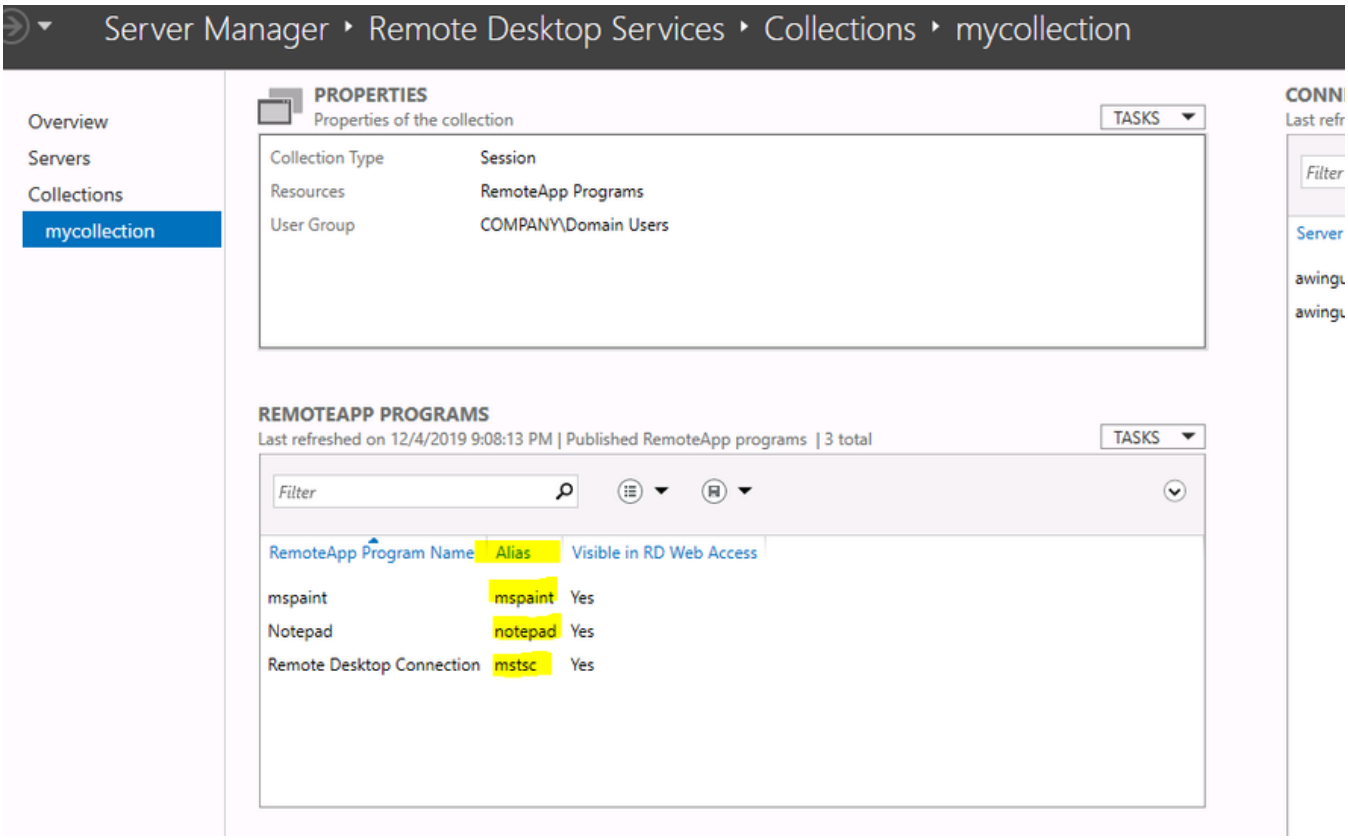
- **User Labels:** The list of all users and groups that are allowed to start an application.
  - If all users can start it, use the built-in `all:` label.
  - If only Parallels Secure Workspace administrators can use the app, set it to `admin:` .
  - If you want to restrict it to a list of specific AD groups or users, set it to the group and user labels that have been added previously.
- **Server Labels:** The list of application servers on which the application can run.
  - For desktops and single apps, specify at least one application server. When multiple application servers are entered, Parallels Secure Workspace will automatically perform round-robin load balancing over the different servers.
  - For web applications, the server labels should be left blank.

For example, if you would like to make a specific desktop available for a specific use, first import the desktop by navigating to **Manage > Application servers.** Then, import the user by navigating to **Manage > Labels**. There you can create the correct labels, which can be assigned to the application.

Remote Application Settings

Before we can add the user and server labels for a Remote Application, we need to specify which RemoteApp needs to be started. We might also want to link the application to specific file types.

- **Alias**: This corresponds to the alias (second column) of the published application in the collection.



- **File Types:** Linking apps to "file types" will allow the files in the Parallels Secure Workspace drives to be opened in the associated application.

  For Remote Applications: Ensure that on the Microsoft Windows backend the "Allow all parameters" flag is set on the published application. Otherwise, when opening a file through the Parallels Secure Workspace Drives, the application will start without opening the specified file.
- **User and Server labels:** Just like for a full desktop, assign the correct user and server labels to the "Remote Application".

  Parallels Secure Workspace can also connect to an RDS broker and use the broker functionality to do the load balancing. In this case, add the `rdscollection:<collection-name>` as a server label. Read the Admin Manual for more details about adding the `rdscollection` label, linking it to the broker(s) and then linking this `rdscollection` label to the application.

Advanced Settings:

These settings can be used to further fine-tune the configuration. For more details, have a look at the admin manual.

- **Unicode:** We generally recommend leaving the unicode setting enabled for apps. In this case, the keyboard is detected automatically. Only set unicode to disabled when you encounter strange behavior when typing in apps. When disabled, users have to configure the correct keyboard settings in their profile.
- **Labels** can be used to group specific apps for reporting.
- **Auto start labels** can be used to select a group of users for whom this application will automatically start when they log in, without the need for them to click the application icon to start it. Enable the **start in foreground** option if you want this app to be active/focused.
- **Concurrent Usage** can be set to disabled if this application can only be started once per user. For example, Microsoft Outlook should be restricted to a single start, whereas Microsoft Word can be opened multiple times by the same user.
- **Ask for Credentials** can be enabled if single sign-on is not needed and the user has to specify the credentials for this application or desktop explicitly. Useful to execute applications as another identity than the one you have used to log in.
- **Notifications** can be disabled if you don't want to receive any notifications from this application.
- **Session Merge** allows you to merge this application into an existing RDP session. If there is already a remote app running on a server that is also in the server label list of this application and the feature is enabled, then Parallels Secure Workspace will not start a second RDP session. Instead, this application will be merged into the existing RDP stream of the first application.
- **Minimum and Maximum Size** allows you to specify a minimum and/or maximum size for this application. When the screen size is smaller than the minimum size of the application, Parallels Secure Workspace will render the application larger than the screen size and allow you to move the application window in the screen window either by pressing the two mouse buttons at the same time or by using a three-finger touch.
- **Color Depth** allows you to change the color depth from the default 16-bit colors (better performance) to 24- or 32-bit.

Publish drives

Parallels Secure Workspace drives allow you to access network drives directly from within the Workspace. By doing so, users can, for example, open files directly in one of the published apps. The drives can also be used to upload/download files or to share them.

To add a (network) drive, go to **System Settings > Manage > Drives** and click on the [Add] button at the bottom of the page.

> Adding Drives is similar to adding applications. If you would like to restrict access to a specific group of users, make sure the necessary user labels are created upfront.

The **name** should be set to the display name in Parallels Secure Workspace.

The **back end** specifies which kind of storage to integrate with. For OneDrive or WebDAV, see the admin manual on how to configure them.

In this Getting Started guide, we will assume the storage back end is **CIFS** (SMB).

The **URL** parameter is used to browse the storage from the Parallels Secure Workspace appliance. Make sure it is in the format `smb://<ip_or_fqdn>/path/` (Example: smb://file-server.domain.local/share)

The **UNC** parameter is used to open the file from the application server. Make sure it is in the format `\\<ip_or_fqdn>\path\` (Example: `\\fileserver.domain.local\share`)

The **Authentication Role** parameter is set by default to “user” and lets you connect to the storage back end as the logged-in user. For anonymous access to file shares, you can also change this parameter if needed.

The **Context Policy Labels** can be used to restrict access to these drives when a specific context is not met. For example, you can only access the HR Drive if you are in your own country.

> The `<username>` variable can be used in the URL and UNC path to go directly to a user specific directory . For example \\fileserver.domain.local\users**\<username>**documents will open each user’s own documents folder

The last step before the drive will be available in Parallels Secure Workspace, is to link it to the correct user labels:

User Labels contains the list of all users and groups allowed to access this network drive.

- If all users can access it, use the built-in `all:` label.
- If only Parallels Secure Workspace admins can use the app set it to `admin:` .
- If you want to restrict it to a list of specific AD groups or users, set it to the group and user labels that have been added before.

> The access to the storage is determined by the access rights on the back end. So even when in Parallels Secure Workspace "all:" users can access the drive, it will only work if those users also have the necessary permissions on the storage back end itself.

Prepare your Microsoft Windows back end

We assume in this getting started manual that there is already an existing Microsoft Windows back end available. If this is not the case, please create this first or use the Parallels Secure Workspace All-In-One solution on Azure to deploy and create everything for you.

Active Directory

Parallels Secure Workspace doesn't have any built-in user database and falls back to the Active Directory (or another LDAP server) or an external Identity Provider (IdP) for this. If users should be able to change their passwords through Parallels Secure Workspace, the Active Directory domain controller(s) need to be equipped with a certificate and configured to use this. In this guide, we will describe how a standard login using Active Directory needs to be set up. For more complex scenarios like Single Sign-On (SSO) with an external IdP such as Microsoft Azure, Microsoft ADFS, or Google, please have a look at the admin manual in the section on setting up SSO.

Parallels Secure Workspace doesn't require any specific functional Active Directory level. Although to make some features work, such as auto-import from Active Directory, we recommend using a modern Microsoft Windows Server version. If the version is too low, some features may not work as expected.

Parallels Secure Workspace is not compatible with Azure AD. When using Azure AD for Single Sign-On (SSO), a real Active Directory is still needed to join the application servers into the domain and to fetch the security groups.

In case there is no local Active Directory, the solution is to install the Azure AD Directory Services feature (AADDS) and link the application servers and Parallels Secure Workspace to these Azure AD DS servers.

To enable the auto-import of resources, we need a bind user and password. This should be a non-admin account that doesn't have any privileges. The password should not expire. No write access to the Active Directory is necessary. During the authentication in Parallels Secure Workspace, the user credentials provided will be used to do an LDAP or LDAPS bind with the Active Directory domain controller. If successful, Parallels Secure Workspace will get a list of all groups the user is a member of.

It is recommended to put all users who need to be a Parallels Secure Workspace admin (= have privileges to make changes to the configuration), into a dedicated security group.

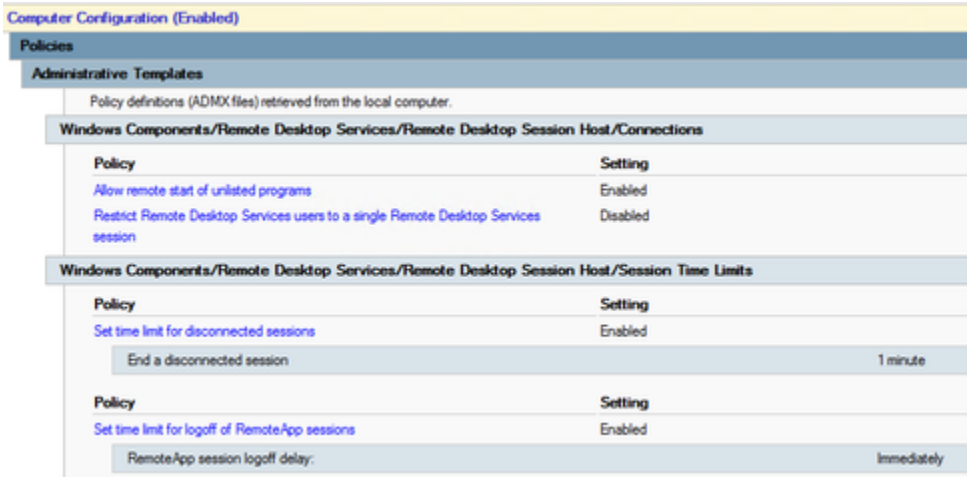
Group Policies

There are a few group policies that are **required** for a correct end-user experience.

These are the following:

- Computer Configuration / Policies / Administrative Templates / Windows Components / Remote Desktop Services / Remote Desktop Session Host
  - Connections
    - Allow remote start of unlisted programs: **enabled.**
    - Restrict Remote Desktop Services users to a single Remote Desktop Services session: **Disabled**. *(see remark below)*
  - Session Time Limits:
    - Set the time limit for disconnected sessions: End a disconnected session in **1 minute.**
    - Set time limit for log off of RemoteApp sessions: RemoteApp session log off delay: **Immediately.**

By enabling the "session merge" option in the app publication, different apps can be merged into existing remote app sessions. This prevents that for each app a new RDP stream needs to be started, resulting in loading GPOs and profiles each time.



Next to the required GPOs to work correctly, there are also a couple of the GPOs that we have gathered within the Admin Manual to restrict the security settings within a remote desktop session.

> When using User Profile Disks or FSLogix Profiles, make sure all apps from the same session collection are session merged in Parallels Secure Workspace

Microsoft Application Server (RDS)

When Microsoft Windows applications should be delivered, we require the setup of a remote desktop session host (RDSH) on the Microsoft Windows back end. Parallels Secure Workspace can integrate with Microsoft Windows Server. Windows applications on the back end can be published as a RemoteApp or by starting an application within an RDP session. Delivering applications using the RemoteApp protocol is the recommended approach.

Applications that need to be delivered should be installed on the application servers and operate within a multi-user context. When using the RemoteApp protocols, the application can be directly published (as RemoteApp) from the Server Manager. Please refer to the Admin Guide for a detailed description of publishing RemoteApps.

Parallels Secure Workspace supports connections directly to a session host as well as making connections to an RDS broker.

VDI / Full desktops

Parallels Secure Workspace can also connect to full desktops using RDP. When using a Microsoft Windows OS without the RDS session host role installed, the sessions will be limited to 1 user per server/client.

Parallels Secure Workspace is also compatible with Azure Virtual Desktop. In that case, multiple users can connect to the same Microsoft Windows virtual machine.

Mind that the users have to be added explicitly to the allowed remote access users on the Microsoft Windows client OS. By default, only domain admins are allowed to do this.

Files Service Integration

The Parallels Secure Workspace appliance can integrate with existing file servers. For Microsoft Windows file shares, it is important that those file shares are part of the same domain as to which Parallels Secure Workspace is configured. Access to the files will be with the identity of the user.

The Parallels Secure Workspace Installer

Once the Parallels Secure Workspace appliance has been deployed on-premises or in the cloud, the first thing that needs to happen is to run the installer. During the installation the appliance will initiate and set up all services.

Use a web browser to go to http://<IP Address of your appliance>:**8080**/ to begin the installation wizard.

EULA

If deployment was successful, you should see the EULA.

Please read the EULA and then check the "Yes, I have read and hereby accept the above license terms and conditions" to proceed.

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 IPs, hostnames, credentials, etc., will be prefilled but can be altered.

For more information about backups, see the Admin Manual.

For new installations, you can simply skip this step.

Management User

The next step is to set up a Management User.

> This user can't be changed and should not exist in your Active Directory domain. The password can be changed later on.

This Management User will be able to log in at any time and alter configuration settings. 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 not require a one-time password (OTP) to sign in. It is advised to **NOT** use this Management User, other than for the initial install or in case of emergency.

For security reasons, this user is automatically logged out after 15 minutes!

DNS and NTP

Next, we need the IP address(es) of the DNS and NTP servers. We recommend using the Active Directory servers as DNS servers so they can also resolve the internal names of the application servers used.

The host name can not be changed afterward. When planning a multi-node deployment, it's recommended to immediately set the hostname to a meaningful name.

Databases

This will give you the option to use a built-in database or use an external database. External databases are needed when you set up a multi-node deployment of Parallels Secure Workspace. Multi-node deployments are needed for 100+ concurrent user setups or for setups that require high availability. Mind that after this, you can't switch from an internal to an external database without reinstalling everything. Details on the connection strings and supported versions for an external database can be found in the admin manual. So, you might want to consider using an external database from the start. In this Getting Started guide, we assume a single-node deployment with built-in database.

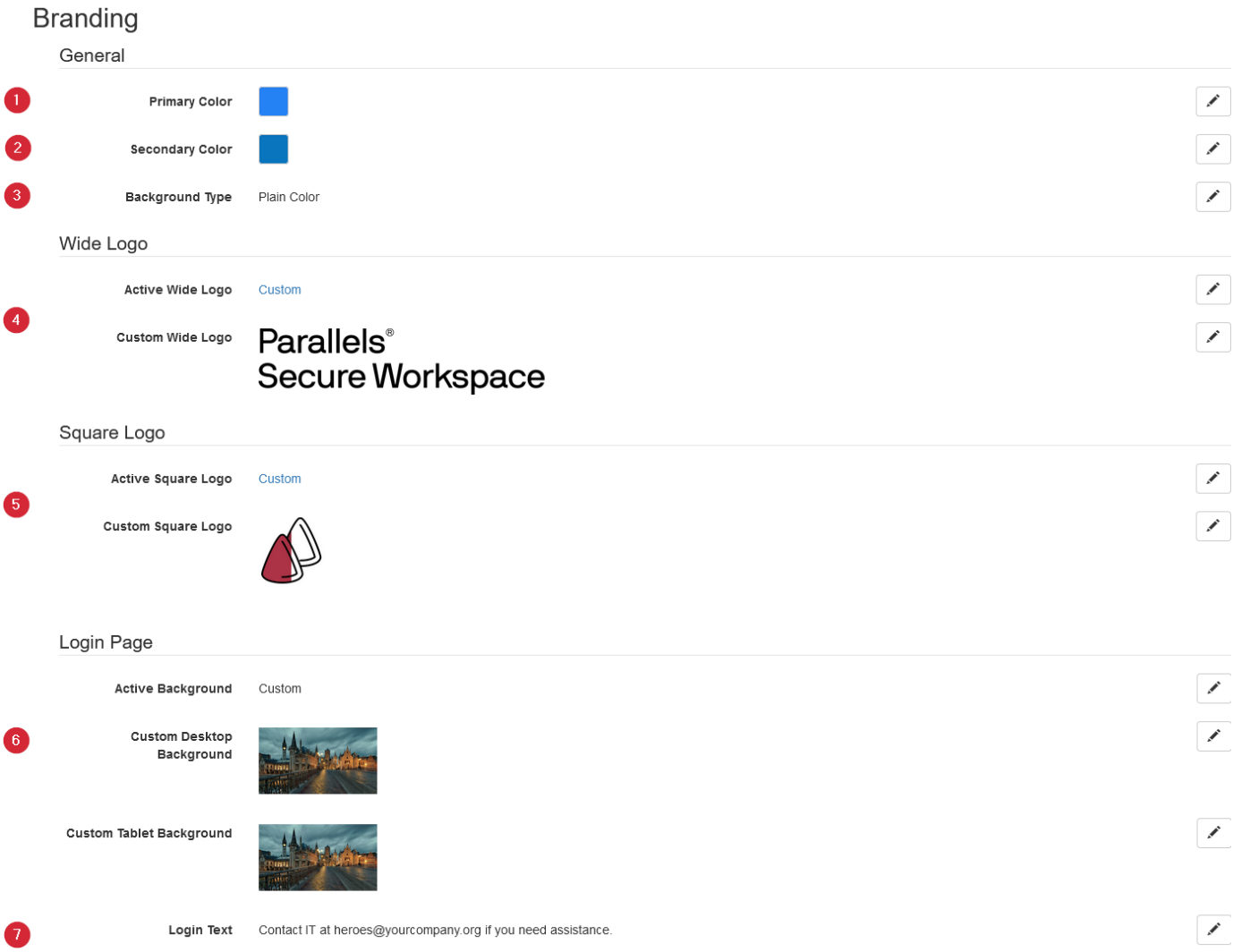
Summary

The summary of the configuration appears. After clicking [Finish], the installation will start. Please take into account that depending on the type of storage used and the overall performance of the system, this installation can take between 10 to 30 minutes.

> If the installation is successful, the wizard will disappear and a login window will be presented. The install service on port 8080 will also no longer be accessible.

Customize the branding

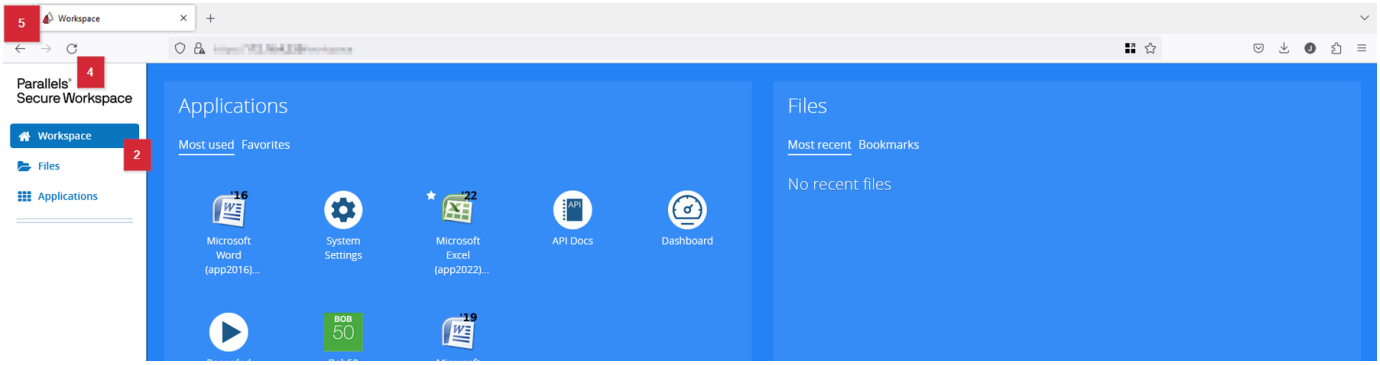
Parallels Secure Workspace can be easily customized to the desired branding. To do so, go to **System Settings > Configure > Branding**.

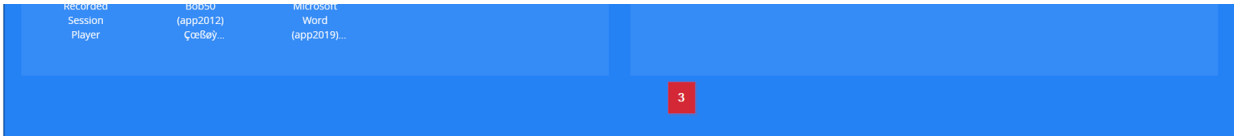


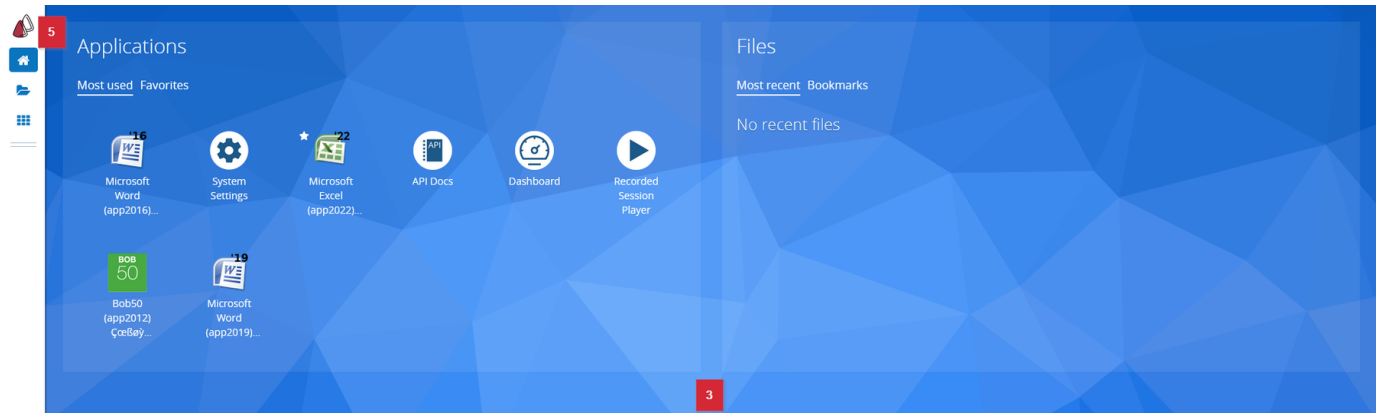
General section: You can select the colors and also choose to have a "Plain background" color or one with the "Polygon style" fading color background.

Logo sections: If you would like to use a custom logo, you need to upload a new image and also set the "Active wide logo" and “Active square logo" options to "custom".

Login page section: If you would like to use a custom background image, first also set the "Active background" to "Custom". There are two images that can be uploaded. One for large screens and one for smaller screens. Also, the login text can be customized. The text allows HTML input.







Parallels® Secure Workspace