



TeamDrive Web Portal Virtual Appliance Installation

Release 5.0.0.0

Paul McCullagh, Eckhard Pruehs

2024

1	Copyright Notice	1
2	Trademark Notice	3
3	Introduction	5
3.1	Requirements	5
3.2	Hardware Requirements	5
3.3	Hardware Requirements	6
3.4	Main Software components	7
4	Virtual Appliance Installation and Configuration	9
4.1	Download and Verify the Virtual Appliance Image	9
4.2	Import the Virtual Appliance	10
4.3	First Boot and Initial Configuration	10
4.4	Updating the Installed Software Packages	11
4.5	Changing the Default MySQL Database Passwords	11
4.6	Firewall Configuration	12
4.7	Proxy Configuration	12
4.8	Time Server	12
4.9	Suricate Configuration	13
4.10	Replacing the self-signed SSL certificates with proper certificates	13
4.11	Mount user data Volume	14
4.12	SELinux Configuration	14
5	Initial Web Portal Configuration	15
5.1	Associating the Web Portal with a Provider	15
5.2	Activating the Web Portal	15
5.3	Installing the TeamDrive Agent	17
5.4	Setup and Administration	18
5.5	Testing Web Access	18
6	Troubleshooting	21
6.1	List of relevant configuration files	21
6.2	List of relevant log files	21
6.3	Enable Logging with Syslog	22
6.4	Common errors	23
7	Release Notes - Version 5.0	25
7.1	5.0.0 (2024-08-09)	25
8	Release Notes - Version 3.1	27
8.1	3.1.3 (2023-11-13)	27
8.2	3.1.2 (2023-07-18)	27
8.3	3.1.1 (2023-05-23)	27
8.4	3.1.0 (2022-10-25)	28

9	Release Notes - Version 3.0	31
9.1	3.0.4 (2022-09-21)	31
9.2	3.0.3 (2022-06-15)	31
9.3	3.0.2 (2022-01-10)	31
9.4	3.0.1 (2021-10-11)	32
9.5	3.0.0 (2021-08-20)	32
10	Release Notes - Version 2.0	33
10.1	2.0.8 (2020-05-10)	33
10.2	2.0.7 (2020-12-16)	33
10.3	2.0.6 (2020-10-02)	33
10.4	2.0.5 (2020-09-15)	33
10.5	2.0.4 (2020-05-19)	34
10.6	2.0.3 (2020-04-14)	35
10.7	2.0.2 (2019-07-26)	35
10.8	2.0.1 (2019-06-11)	36
10.9	2.0.0 (2019-04-25)	36
11	Release Notes - Version 1.2	39
11.1	1.2.3 (2019-01-15)	39
11.2	1.2.2 (2018-11-06)	39
11.3	1.2.1 (2017-11-29)	39
11.4	1.2.0 (2017-08-14)	40
12	Release Notes - Version 1.1	41
12.1	1.1.0 (2017-04-10)	41
13	Release Notes - Version 1.0	43
13.1	1.0.9 (2017-02-10)	43
13.2	1.0.8 (2017-02-07)	43
13.3	1.0.7 (2016-11-10)	43
13.4	1.0.6 (2016-07-11)	43
13.5	1.0.5 (2016-02-16)	44
13.6	1.0.4 (2016-02-09)	45
13.7	1.0.3 (2016-02-02)	45
13.8	1.0.2 (2015-12-07)	45
13.9	1.0.1 (2015-10-27)	45
13.10	1.0.0 (2015-10-08)	46
14	Appendix	47
14.1	Abbreviations	47

COPYRIGHT NOTICE

Copyright © 2015-2024, TeamDrive Systems GmbH. All rights reserved.

TeamDrive Systems GmbH

<https://www.teamdrive.com>

Max-Brauer-Allee 50

22765 Hamburg, Germany

Email: info@teamdrive.com

TRADEMARK NOTICE

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Apache HTTP Server, Apache, and the Apache feather logo are trademarks of The Apache Software Foundation.

MySQL is a registered trademark of Oracle and/or its affiliates.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices.

VMware is a trademark or registered trademark of VMware, Inc. in the United States and/or other jurisdictions.

“Amazon Web Services”, “Amazon S3” are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries.

“Red Hat Linux” and “CentOS” are trademarks of Red Hat, Inc. in the U.S. and other countries.

All other names and trademarks used herein are the property of their respective owners.

INTRODUCTION

The TeamDrive Web Portal Virtual Appliance offers a pre-installed and ready-to-run TeamDrive Web Portal suitable for deployment in a virtualized environment like VMWare.

This document will guide you through the deployment and initial installation of the Virtual Appliance and the configuration of the TeamDrive Registration Server.

This Installation Guide outlines the deployment of a single node installation, where all required components are located on the same OS instance. Please consult the *TeamDrive Web Portal Administration Guide* for recommendations about scalability and/or high availability.

3.1 Requirements

3.2 Hardware Requirements

The hardware requirements depend on the number of users that will access the Web Portal. Exact sizing will depend on how heavily the portal is used and how many users access the portal concurrently.

To operate a TeamDrive Web Portal you need one or more **64-bit** systems.

CPU usage, RAM, disk storage and network requirements are described below. Since the usage of a Web Portal can differ greatly, our recommendations are only approximate.

Please contact us via sales@teamdrive.net for further assistance.

3.2.1 CPU Requirements

To operate a TeamDrive Web Portal we recommend at least one processor core per 24 users of the portal.

This estimate assumes that only about 10% of all users are actively performing some operation at any given moment. Increase the number of CPU cores if your estimate of the number of active users is higher.

3.2.2 RAM Requirements

The Web Portal starts a TeamDrive Agent for each active user session. Each Agent requires about 100 MB of RAM.

You can assume that the number of agents running is greater than the number of active users (the number of users accessing the portal at any given time). This is because agents running until the user session is closed due to an idle timeout.

3.2.3 Storage Requirements

The main storage requirement is for the Space data that is downloaded from the Hosting Service when a user enters a Space via the TeamDrive Web interface.

The storage requirements are relatively modest because only the “meta-data” (file names and directory structure) of a Space will be stored permanently on the Web Portal.

The rest of the disk space required consists of a file cache which is used for files in transit between the Hosting service and the end-user device. We recommend a cache size of at least 2 GB per Web Portal user plus about 4 MB per Space.

The speed of the storage system used will be decisive for the responsiveness of the Web Portal, in particular when entering a Space. We recommend a system that is capable of at least 100 IOPS per active user of the Portal. As a rule of thumb we assume that 10% of the users that use a Web Portal are active at any particular time. This means, for example, that if a portal serves 1000 users, then the storage system should be capable of 10000 IOPS.

If a user’s account is idle for a certain period of time (for example 1 month), the Web Portal can be instructed to remove the user’s data. In this way, the storage can be freed up for other users.

If the user’s data is removed from the Web Portal host, the data is not lost, because the Space data is still stored and maintained by the Hosting Server. The only inconvenience for the user is that Spaces will have to be “re-entered” the next time the user logs in to the Web Portal.

3.2.4 Network Requirements

The bandwidth of the Web Portal’s network interface plays a vital role in defining the overall performance and responsiveness of the service.

When a user enters a Space, the meta data of the Space will be downloaded to the Web Portal. The speed of this operation will be effected by the speed of inbound connections.

When a user accesses a file in a Space, the file is first downloaded to the Web Portal disk cache for the user, where it is decrypted. The decrypted file is then transferred to the user’s device. As a result, the amount of inbound traffic is at least as high as the outgoing traffic.

The system must have IP connectivity, using a fixed IP address and a resolvable fully qualified domain name. This host name is basically the URL that users will use to access the Web Portal. The Web Portal itself needs to be able to properly resolve host names, too.

If the Web Portal is located behind a firewall, please ensure that it is reachable via HTTPS (TCP port 443) by a web browser.

During operation the Web Portal will need to make API calls to an associated TeamDrive Registration Server. For this purpose the Web Portal must be able to establish outgoing HTTPS connections to the Registration Server.

It is possible to use an TeamDrive Authentication Service for the TeamDrive users of the Web Portal, or an external authentication for the administrators of the Web Portal. In this case, the Web Portal must be able to establish HTTP or HTTPS connections (depending on the configuration) with the host running the authentication service.

3.3 Hardware Requirements

The TeamDrive Web Portal Virtual Appliance is delivered in the form of a virtual machine image. Its main technical specifications are:

- Supported platforms: Oracle VirtualBox, VMWare vSphere 4 to 8 (VMWare Workstation can be used for testing purposes)
- Minimum VM Memory: 4 GB
- vCPUs: 2
- HDD: 100GB

- Guest OS: CentOS 9 (64-bit)

3.4 Main Software components

The TeamDrive Web Portal comprises the following components and modules:

- Apache Web Server 2.4
- MySQL 8.0 (or later) Database Server
- TeamDrive Agent
- Yvva Runtime Environment version 1.5.9

VIRTUAL APPLIANCE INSTALLATION AND CONFIGURATION

4.1 Download and Verify the Virtual Appliance Image

A .zip Archive containing the virtual appliance's disk image and VM configuration can be obtained from the following URL:

<https://s3download.teamdrive.net/Server/TD-Web-Portal-CentOS9-64bit-5.0.0.0.zip>

Download the .zip archive and the corresponding SHA1 checksum file:

<https://s3download.teamdrive.net/Server/TD-Web-Portal-CentOS9-64bit-5.0.0.0.zip.sha256>

You should verify the SHA256 checksum to ensure that the zip archive is intact.

You can use the `sha256sum` command line utility on Linux to verify the integrity of the downloaded file.

For guidance on how to verify this checksum on other platforms, see the following articles:

- Apple Mac OS X: [How to Check sha256 Hash of a File on Mac](#)
- Microsoft Windows: [Get-Filehash - sha256sum Windows](#)

For additional safety, we recommend to verify the cryptographic signature of the zip archive as well.

You need to have a working GnuPG installation in order to verify this signature. The installation and configuration of GnuPG is out of the scope of this document — see the documentation at <https://gnupg.org/> for details.

The public TeamDrive Build GPG key can be downloaded from here:

<https://repo.teamdrive.net/RPM-GPG-KEY-TD2024>

Import the key into your keyring and double check it matches the fingerprint provided below:

```
$ gpg --fingerprint support@teamdrive.net
pub  3072R/FAFD FE49 2024-02-05 [expires: 2026-02-04]
     Key fingerprint = 3E0F A901 D96F 2B61 15FC 7A96 CEA7 D6ED FAFD FE49
uid                               TeamDrive Systems ((RPM Build Key 2024) <support@teamdrive.
→net>
sub  3072R/F583896E 2024-02-05 [expires: 2026-02-04]
```

Each official release is signed with this TeamDrive GPG key. The signature can be obtained from the following URL:

<https://s3download.teamdrive.net/Server/TD-Web-Portal-CentOS9-64bit-5.0.0.0.zip.asc>

To verify the signature on a Linux operating system, the .zip and corresponding .asc file should be located in the same directory. Now run the following command:

```
$ gpg --verify TD-Web-Portal-CentOS9-64bit.zip.asc
gpg: Signature made Do 27 Aug 2015 12:57:38 CEST using RSA key ID 9A34C453
gpg: Good signature from "TeamDrive Systems (RPM Build Key) <support@teamdrive.net>"
→"
gpg: WARNING: This key is not certified with a trusted signature!
```

```
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 8F9A 1F36 931D BEFA 693B  9881 ED06 27A9 9A34 C453
```

The procedure on other platforms may vary, please consult the GnuPG documentation for details on how to accomplish this task.

4.2 Import the Virtual Appliance

After you have confirmed the integrity and authenticity, unzip the zip archive.

The archive contains four files, a virtual disk image (.vmdk), two virtual machine description files (.ovf) and a manifest file (.mf), containing the file names and SHA1 checksums.

Import the virtual machine image according to the documentation of your virtualization technology and adjust the VM parameters (e.g. number of virtual CPUs, RAM) based on your requirements, if necessary.

Note: An import to VMWare ESXi might fail with the error:

```
Unsupported hardware family 'virtualbox-2.2'.
```

In this case use the .ovf file starting with vmx_*.ovf

Start up the virtual machine and observe the virtual machine's console output.

4.3 First Boot and Initial Configuration

Log in as the `teamdrive` user with the standard password `teamdrive` on SSH port 2021 (not ssh default port 22).

To change the default password, type in:

```
[teamdrive@localhost ~]# passwd
```

and define your own strong password (please notice the password requirements described in shell).

Do the same with the root user. Type in:

```
[teamdrive@localhost ~]# sudo -i
```

and use standard password `teamdrive` for the root-user authorization. Change the default password:

```
[root@localhost ~]# passwd
```

The server is configured with DNSCrypt using a list of public DNSCrypt-Server as described in `dnscrypt`. To change the network device and DNS, type in:

```
[root@localhost ~]# nmtui
```

Whitelist your ssh login ip as described in `fail2ban` and restart the service:

```
service fail2ban restart
```

Check your network interface:

```
[root@localhost ~]# ifconfig
```

and update the device name (af-packet → interface) and change your network address group (vars → address-groups → HOME_NET) in the suricata (ids) config file:

```
/etc/suricata/suricata.yaml
```

4.4 Updating the Installed Software Packages

As a first step, we strongly advise to perform an update of the installed software packages. New security issues or software bugs might have been discovered and fixed since the time the Virtual Appliance has been built.

This can be done using the `dnf` package management tool. As a requirement, the Virtual Appliance needs to be connected to the network and needs to be able to establish outgoing HTTP connections to the remote RPM package repositories. To initiate the update process, enter the following command:

```
[root@localhost ~]# dnf update -y
```

`dnf` will first gather the list of installed packages and will then determine, if updates are available. If any updates need to be installed, the affected RPM packages will now be downloaded from the remote repositories and installed.

If the `dnf` update installed any updated packages, consider performing a reboot before you proceed, to ensure that the updates are activated.

Note: Performing a regular update of all installed packages is an essential part of keeping your system secure. You should schedule a regular maintenance window to apply updates using `dnf update` (and perform a reboot, to ensure that the system still boots up correctly after these updates). Failing to keep up to date with security fixes may result in your system being vulnerable to certain remote exploits or attacks, which can compromise your system's security and integrity.

4.5 Changing the Default MySQL Database Passwords

The TeamDrive Web Portal Virtual Appliance uses the following default passwords for the MySQL database. We strongly suggest changing the passwords of the MySQL users `root` and `teamdrive` before connecting this system to a public network.

Account type	Username	Password (default)	New Password
MySQL Database Server	root	teamdrive	
MySQL Database Server	teamdrive	teamdrive	
Admin Console	HostAdmin	(defined during setup)	
GRUB Bootloader		(contact Teamdrive)	

As described in bootloader the GRUB Bootloader is protected with a password.

To change the passwords for the MySQL `root` and `teamdrive` user, please use the following commands. First change the password for the root user:

```
[root@localhost ~]# mysqladmin -u root -pteamdrive password
Warning: Using a password on the command line interface can be insecure.
New password: <new password>
Confirm new password: <new password>
```

Next, log into the MySQL database as the `root` user (using the new password) and change the password for the user `teamdrive`:

```
[root@localhost ~]# mysql -u root -p
Enter password: <new password>
```

```
[...]

mysql> SET PASSWORD FOR 'teamdrive'@'localhost' = '<new password>';
Query OK, 0 rows affected (0.00 sec)

mysql> quit
Bye
```

Note: Take note of the new MySQL password for the teamdrive user, as you will need to change some configuration files using that password as outlined in the following chapters creating_teamdrive_mysql_user_and_databases.

4.6 Firewall Configuration

The iptables-based OS firewall on the TeamDrive Host Server Virtual Appliance has been configured to only allow access to the following services:

- SSH (TCP Port 2021, not the default SSH Port 22)
- Secure WWW (HTTPS, TCP Port 443)
- WWW (HTTP, TCP Port 80)

If necessary, you can change the firewall configuration using the following utility:

```
[root@localhost]# firewall-cmd
```

An instructions how to configure the firewall can be found here https://www.server-world.info/en/note?os=CentOS_Stream_9&p=firewalld&f=1

If your firewall or other network component supports ssl offloading, please notice the configuration changes described in ssl-offloading

4.7 Proxy Configuration

Please configure a proxy in the following config files. For dnf add in /etc/dnf/dnf.conf the following line:

```
proxy=http://<host>:<port>
```

In /opt/dnsmasq/urlhaus.sh set the proxy in the script in this variable:

```
PROXY_URL
```

The Webportal needs access to his Registration Server and TDNS. Configure the proxy in the Webportal Admin under Settings → Outgoing Connections in ProxyHost (format <host>:<port>) and UseProxy true/false.

4.8 Time Server

If you use an own internal time server, add the server in /etc/chrony.conf and disable the default time server and restart the service:

```
systemctl restart chronyd.service
```

4.9 Suricata Configuration

Suricata is an open source network security system designed to detect and respond to threats in real time. It is based on the Intrusion Detection Engine and uses various techniques such as signatures, anomaly detection and log analysis to identify threats.

Please update the network interface name from your environment. You can get the name of your network interface with:

```
[root@hostserver ~]# ip --brief add | grep "UP"
```

Update the interface name in these files and by replacing “ens160” with your name in:

/etc/sysconfig/suricata

and in:

/etc/suricata/suricata.yaml

below this line:

```
# Linux high speed capture support
af-packet:
  - interface: ens160
```

Restart the suricata service with:

```
[root@hostserver ~]# service suricata restart
```

4.10 Replacing the self-signed SSL certificates with proper certificates

In order to use SSL without any problems, you will need a properly signed SSL certificate (+ key) and an intermediate certificate (certificate chain) from a trusted authority.

Edit /etc/httpd/conf.d/ssl.conf and enter the absolute location of your files into the appropriate settings:

```
SSLCertificateFile /path/to/your_domain.crt
SSLCertificateKeyFile /path/to/your_domain.key
```

Depending on your certificate provider and your security needs, you probably want to set:

```
SSLCertificateChainFile /path/to/server-chain.crt
```

or:

```
SSLCACertificateFile /path/to/gd_bundle.crt
```

After saving the changes, restart your httpd and watch out for errors:

```
[root@localhost ~]# service httpd restart
```

Now you can logout and proceed with the configuration via browser to register the Web Portal as described in [Associating the Web Portal with a Provider](#) (page 15). For production use please read the following two chapters about the necessary storage.

4.11 Mount user data Volume

As described in preinstall the user data will be stored in /teamdrive. The VM Image has only a small internal disk with max. 10 GB storage capacity. Please mount a larger additional use data volume in /teamdrive if necessary. The approx. necessary storage per user is 50 MB. The user data will be automatically removed, after `ContainerStorageTimeout` is reached (see `web_portal_settings`).

4.12 SELinux Configuration

Please note that the TeamDrive WebPortal currently can not be run when SELinux is enabled. Therefore SELinux has been disabled by setting `SELINUX=disabled` in file `/etc/selinux/config`. It is important to leave it disabled, otherwise the correct functionality of the WebPortal can not be ensured.

INITIAL WEB PORTAL CONFIGURATION

A Web Portal is connected to a single Registration Server. On the other hand, Registration Server may be connected to multiple Web Portals, with each Web Portal responsible for a different Provider.

A single Web Portal can also provide web services for the users of a number of Providers, as long as the Providers are all on the same Registration Server.

A Web Portal that is configured to support an specific external Authentication Service has further restrictions. Such a Web Portal can only support one external Authentication Service. However, this is normally not necessary because the Web Portal will automatically re-direct to the external authentication service associated with the user (see authservice for more details).

5.1 Associating the Web Portal with a Provider

Before you can activate your Web Portal you need to associate your Web Portal with a specific Provider account on the Registration Server. This can be performed via the Registration Server's Admin Console, which you can usually access via the following URL:

<https://regserver.yourdomain.com/adminconsole/>

Please see the Registration Server Manual for details. Note that Registration Server 5.0 is required to run a Web Portal.

Log in with your provider login and click the tab **Providers** and then click on **Manage Domains & Services**. In the section **Services**, click **Add Service**.

Enter a Service name, choose type **Web Portal**, enter the Login URL (<https://your-domain.com>), choose Authorisation **MD5 Endpoint specific key** and enter the IP Address of the webportal in in IP Address List. Click on **Add Service**. In the new service entry, click **Show key** and copy the key needed in the next chapter.

Now, copy the Service name and click on **Providers** → **Provider Settings** and in the lower tab-list on **Webportal**. Add the setting **WEBPORTAL_SERVICE_NAME** and enter the copied Service name in the value-field. Click on **Save** to store the value.

As mentioned above, it is possible to associate the use of a single Web Portal with a number of Providers. If this is desirable, then follows the procedure to set the **WEBPORTAL_SERVICE_NAME** for the addition Providers.

Only users of the Providers associated in this manner will be able to access the Web Portal.

5.2 Activating the Web Portal

From a desktop system that can connect to the Web Portal via HTTPS, start a web browser like Mozilla Firefox, Google Chrome (or any other modern web browser) and start the configuration process by opening the following URL in your browser:

<https://webportal.yourdomain.com/admin/>

This should open the Web Portal Setup page. If you get an error message like “500 Internal Server Error”, check the log files for any errors. See chapter [Web Installation: “500 Internal Server Error”](#) (page 23) for details.

Note: If you haven’t replaced the server’s self-signed default SSL certificate yet, your web browser most likely will complain about an untrusted/insecure connection. Either replace the SSL certificate with an appropriate one before you proceed, or ignore this message.

Alternatively, you can access the Setup Page via an unencrypted HTTP connection. You will have to uncomment the rewrite rules in the apache config file `/etc/httpd/conf.d/td-webportal.httpd.conf` in order to enabled HTTP access. When you access the setup page using HTTP you will be prompted to proceed using an insecure connection.

When everything is configured correctly, you will see the TeamDrive Host Server Setup page that will guide you through the initial configuration:

Fig. 5.1: Web Portal Setup Page

Fill out the fields according to your environment and requirements:

Admin Username The name of the user account with full administrative (superuser) privileges.

Admin Password The administrator password that you need to provide to login to the Web Portal Administration Console.

Admin Email The email address of the Administrator. This field is optional. This email address is used for 2-factor authentication (if enabled).

Web Portal Domain Name This is the domain name of the host running the Web Portal. It must be a fully-qualified and resolvable domain name.

Registration Server Name All Web Portals must be registered with a Registration Server. Enter the name of the Registration Server here. This is the value of the `RegServerName` Registration Server global setting.

Please contact TeamDrive Systems for the correct value if you don’t manage your own Registration Server.

Registration Server Host Enter the fully qualified domain name of the Registration Server here. **Please contact TeamDrive Systems if you need assistance.**

On the Registration Server, the IP address of the Web Portal must be entered in the appropriate Provider `API_WEB_PORTAL_IP` setting. This will identify the Web Portal when it calls the Registration Server to check user credentials.

Setup will ping this host to ensure that the Registration Server is reachable.

Authorisation Hashing & Key The Authorisation Hashing Key is a code that allows the Web Portal to validate calls to the Registration Server's API. This value must match the value of the above MD5 Endpoint specific key setting on the Registration Server to avoid "man in the middle"-attacks.

Providers This is a comma separated list of Providers codes. Only users belonging to these Providers will be able to access this Web Portal. If you do not specify any Providers, then all users at the Registration Server will be allowed to login to the Web Portal.

After you have entered all the required details, click **Setup** to initiate the Web Portal configuration and registration process with the Registration Server. An error will occur if the setup process is unable to contact the Registration Server.

This may be due to either network problems or incorrect input, as indicated by the error message.

5.3 Installing the TeamDrive Agent

The current version of the TeamDrive Agent used by the Web Portal is stored in the `MinimumAgentVersion` setting. The `ContainerImage` setting stores the name of the Container image currently in use by the Web Webportal. If the version of the Agent in `ContainerImage` is less than `MinimumAgentVersion` it will be automatically updated.

If this required TeamDrive Agent does not exist on the host then it will be automatically download and installed on your host.

To install or update the TeamDrive Agent used by the Web Portal use the upgrade command: `start yvva` and execute `upgrade_now;;`:

```
[root@webportal ~]# yvva
Welcome to yvva shell (version 1.5.13).
Enter "go" or end the line with ';' to execute submitted code.
For a list of commands enter "help".

UPGRADE COMMANDS:
-----
To upgrade from the command line, execute:
yvva --call=upgrade_now --config-file="/etc/yvva.conf"

upgrade_now;;
Upgrade the database structure and agent sandbox container (this command cannot be
↪undone).
```

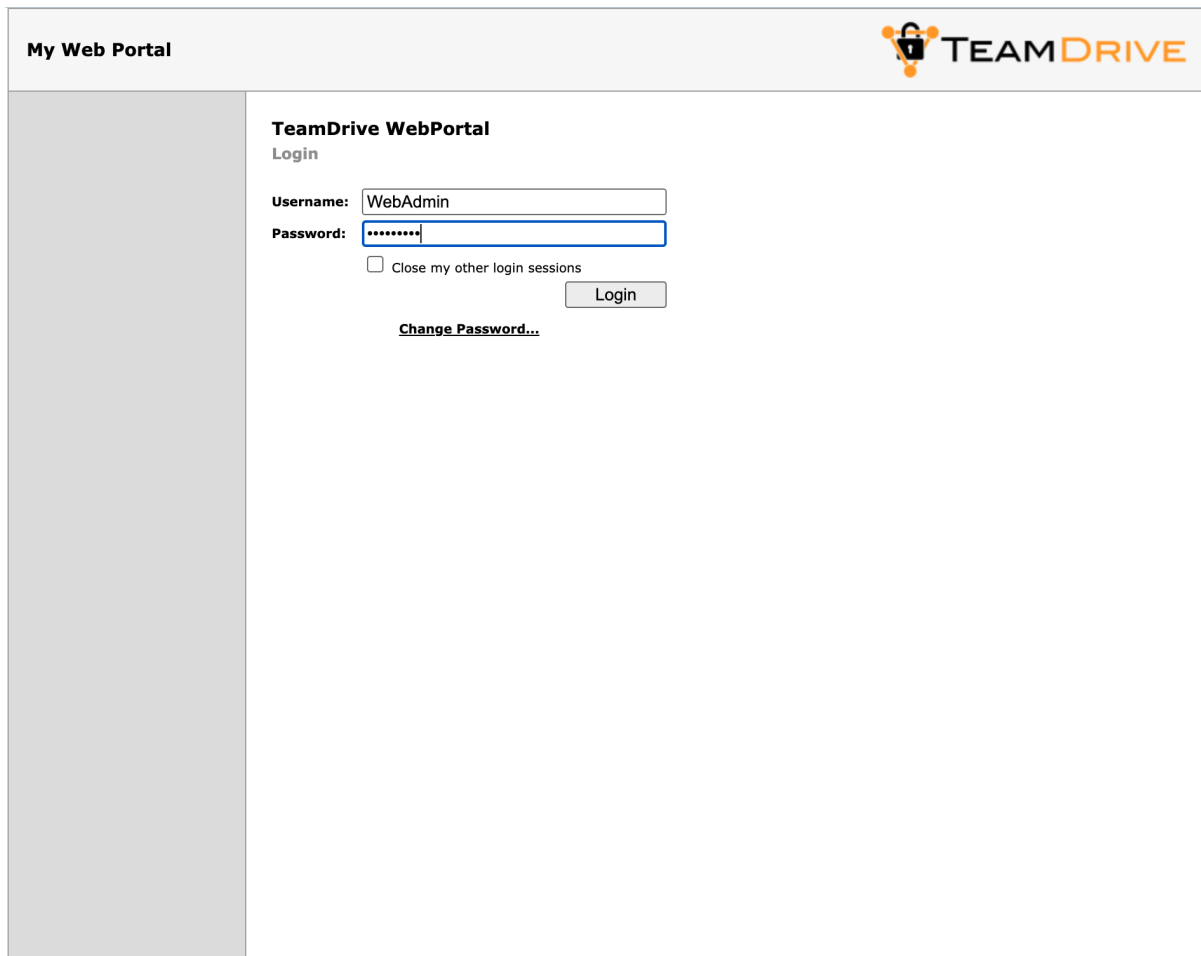
Leave the yvva shell by typing quit.

The agent binary must be added to the fapolicyd. The fapolicyd software framework controls the execution of applications based on a user-defined policy:

```
/usr/sbin/fapolicyd-cli --file add /opt/teamdrive/webportal/agent/teamdrived.bin --
↪trust-file teamdrived
/usr/sbin/fapolicyd-cli --update
service fapolicyd restart
```

5.4 Setup and Administration

Upon successful configuration, you will be presented with the Web Portal's Administration Console Login Screen.



The screenshot shows the 'My Web Portal' header with the 'TEAMDRIVE' logo. The main content area is titled 'TeamDrive WebPortal Login'. It contains a 'Username' field with 'WebAdmin' entered, a 'Password' field with masked characters, a checkbox for 'Close my other login sessions', a 'Login' button, and a 'Change Password...' link.

Fig. 5.2: Web Portal Admin Console: Login Screen

Enter the username and password you defined during the initial setup to log in.

After login, you will see the Web Portal's Administration Console Home Screen.

At this point, you have concluded the Web Portal's basic configuration and registration. See the *TeamDrive Web Portal Administration Guide* for more details on how to use the Administration Console and how to accomplish other configuration tasks. In case of using a white label version please proceed with the next step otherwise step over to the section *Testing Web Access* below.

5.5 Testing Web Access

The Web Portal has now been set up. To test its functionality, start a web browser and enter the URL of the Web Portal:

`https://webportal.yourdomain.com/`

Login to a user account belonging to one of the Providers associated with the Web Portal.

If login fails, check your username and password. If this is correct, begin by checking the Web Portals log file for errors.

My Web Portal (WebAdmin)

■ Home

Admin Users

Registration Servers

Containers

Settings

Setup/Test Email

Log Files

Logout

TeamDrive WebPortal

Home

Docker Version:19.03.12

Last Statistic Update:2020-09-16 10:08:12.00

Docker Container:

Total:3

Running:0

Stopped:3

Docker Devicemapper Storage:

Data Space Used:

Data Space Available:

Meta Data Space Used:

Meta Data Space Available:

Fig. 5.3: Web Portal Admin Console: Home Screen

The log file can be viewed by selecting the **Log Files** menu item and then clicking on **td-webportal.log** in the Web Portal's Administration Console.

TROUBLESHOOTING

6.1 List of relevant configuration files

/etc/httpd/conf.d/td-webportal.httpd.conf: The configuration file that loads and enables the TeamDrive Web Portal Server-specific module for the Apache HTTP Server: `mod_yvva.so`.

`mod_yvva.so` is responsible for providing the web-based Host Server Administration Console as well as an API used for authentication.

The file also contains various Apache “rewrite” rules required by the Web Portal.

Note: The rewrite rules in this file are disabled by default. This is because it is assumed that HTTPS is always used to access the Web Portal.

Enable the rewrite rules only if you are certain that HTTP access may be used.

/etc/logrotate.d/td-webportal: This file configures how the log files belonging to the TeamDrive Web Portal are being rotated. See the `logrotate(8)` manual page for details.

/etc/td-webportal.conf: This file defines how the `td-webportal` background service is started using the `yvvad` daemon.

/etc/td-webportal.my.cnf: This configuration file defines the MySQL credentials used to access the `webportal` MySQL database. It is read by the Apache module `mod_yvva` and the `yvvad` daemon that runs the `td-webportal` background tasks and the `yvva` command line client.

/etc/yvva.conf: This configuration file contains configuration settings specific to the Yvva Runtime Environment that affect the `mod_yvva` Apache module and the `yvva` command line shell.

6.2 List of relevant log files

In order to debug and analyse problems with the Web Portal configuration, there are several log files that you should consult:

/var/log/td-webportal.log: The log file for the Yvva runtime which provides the web-based Administration Console, and the Web Portal authentication API. Errors that are incurred by the Web Portal background tasks are also written to this file.

Consult this log file when the Web Portal has issues in contacting the Registration Server, errors when handling API requests or problems with the Administration Console.

You can increase the amount of logging by changing the Yvva setting `log-level` from `notice` to `trace` or `debug` in the `yvva.conf` file:

```
log-level=trace
```

After changing `yvva.conf` you need to restart the Apache HTTP Server service using `service httpd restart`.

This log file is also used by the `td-webportal` background service. Check the log file to verify that background tasks are being processed without errors.

The log file location can be configured by changing the file name passed to the `log-file` option in the configuration file `/etc/td-webportal.conf`. The log level can be increased by changing the default value `notice` for the `log-level` option to `trace` or `debug`.

Changing these values requires a restart of the `td-webportal` background process using `service td-webportal restart`.

/var/log/httpd/: The Apache HTTP Server's log files (e.g. `error_log`) might also contain additional relevant error messages that should be checked.

6.3 Enable Logging with Syslog

As outlined in *List of relevant log files* (page 21), the TeamDrive Web Portal logs critical errors and other notable events in a log file by default.

It is now possible to redirect the log output of the Yvva runtime components to a local `syslog` instance instead.

Syslog support is an essential feature for auditing, security and/or compliance reasons, as it allows you to funnel all log messages into a centralized syslog server.

This makes it easier to monitor the logs for critical events or errors and prevents tampering with the log files in case of a security breach. It also helps to maintain control over the disk space utilization on the server, as growing log files can't accidentally fill up the file system.

To enable syslog support, the log file name in the `log-file` setting has to be replaced with the keyword `syslog`. Optionally, a custom process identifier can be supplied, by appending it to the `syslog` keyword, using a colon as the separator, e.g. `log-file=syslog:my_process_identifier`. If not used, the default process identifier will be used, which is the name of the Yvva component.

To enable syslog support for the Yvva-based `td-webportal` background service, edit the `log-file` setting in file `/etc/td-webportal.conf` as follows:

```
log-file=syslog:webp-bkgr
```

You need to restart the `td-webportal` background service via `service td-webportal restart` in order to activate this change. If the `log-level` is set to `debug` you will now see log messages appearing in `/var/log/messages`:

```
Jun 23 11:57:33 localhost webp-bkgr: notice: yvvad startup
Jun 23 11:57:33 localhost webp-bkgr: notice: Using config file:
/etc/td-webportal.conf
Jun 23 11:57:33 localhost webp-bkgr: notice: No listen port
Jun 23 11:57:33 localhost webp-bkgr: notice: yvvad running in repeat 60
(seconds) mode
```

To enable syslog support for the Web Portal API and Administration Console, edit the `/etc/yvva.conf` file as follows:

```
log-file=syslog:webp-httpd
```

You need to restart the Apache HTTP Server via `service httpd restart` in order to activate this change. If the `log-level` is set to `debug` you will now see log messages appearing in `/var/log/messages`:

```
Jun 23 12:06:04 localhost webp-httpd: notice: mod_yvva 1.2.1 (May 21 2015
11:00:12) startup OK
```

6.4 Common errors

6.4.1 Web Installation: “500 Internal Server Error”

This error can be triggered by several error conditions. Check the log file `/var/log/td-webportal.log` for details.

Some common errors include:

```
[Error] -12036 (2002): Can't connect to local MySQL server through socket
'/var/lib/mysql/mysql.sock' (25)
[Error] "startup.yv" (80)
```

The local MySQL Server's socket file can't be opened. This could either be a permission problem, or the MySQL Server is simply not available. Check that MySQL is actually up and running (e.g. by running `service mysqld status`) and restart it, if necessary. If the error persists, check the MySQL error log file (usually `/var/log/mysqld.log`) for hints.

Similarly, an error like the following one indicates that a remote MySQL Server might not be answering (e.g. because of a firewall rule or because it's not running):

```
[Error] -12036 (2003): Can't connect to MySQL server on
'webportal.yourdomain.com' (107)
[Error] "startup.yv" (80)
```

If you see Access denied errors like the following one:

```
[Error] -12036 (1045): Access denied for user 'teamdrive'@'localhost' (using
password: YES)
[Error] "startup.yv" (32)
```

Either the username or password used to connect to the MySQL Server are wrong. Double check that the MySQL username and password provided in `/etc/td-webportal.mysql.cnf` are correct, e.g. by trying to connect to the MySQL server using these credentials with the `mysql` command line client.

If you see the following error when connecting to a remote MySQL Server:

```
[Error] -12036 (1130): Host 'webportal.yourdomain.com' is not allowed to
connect to this MySQL server
[Error] "startup.yv" (80)
```

Check the TeamDrive MySQL user's privileges on the remote MySQL server, e.g. by running `SHOW GRANTS FOR 'teamdrive'@'webportal.yourdomain.com';` and make sure that this user is allowed to connect to the MySQL server from the Registration Server's host.

6.4.2 Errors When Accessing the Registration Server

If the Web Portal fails to contact the Registration Server, check the `/var/log/td-webportal.log` log file, as well as `/var/log/td-regserver.log` on the Registration Server for hints.

See the Troubleshooting chapter in the Registration Server Installation Manual for details.

Note: Note that Registration Server version 3.5 or later is required by the Web Portal.

RELEASE NOTES - VERSION 5.0

7.1 5.0.0 (2024-08-09)

- First release for CentOS 9. Version number 5 for all server products (TeamDrive Registration Server, TeamDrive Host Server and TeamDrive Web Portal) only stands for the common CentOS 9 release. The actual functionality of the Web Portal is based on the last release 3.1.3 and only includes small changes (see below) and the current client version (see below).
- HMAC-SHA1 authentication can now be selected for accessing the Registration Server API (WEBCLIENT-463).
- When using External Authentication there some cases where the login name (usually an email address) that was entered in TeamDrive was not always pre-filled in the External Authentication login page. In addition, if the login name is not an email address, then the field will not be set to read-only.
- If `AllowedProviders` is not set then the redirect to the appropriate Web Portal of the user was not always working correctly (WEBCLIENT-465).
- Set client version to 5.2.0.3615
- Admin Console: Added a “Restart” button to the details page (WEBCLIENT-469).

RELEASE NOTES - VERSION 3.1

8.1 3.1.3 (2023-11-13)

- External authentication now redirects to “/external-authentication/finish”. This fixes the issue with Web Portal external authentication and 2-Factor authentication.
- Set client version to 5.0.8.3464

8.2 3.1.2 (2023-07-18)

- Set client version to 5.0.6.3386
- The `UseEmbeddedLogin` setting has been removed. This means there is no longer an option to embedded in the TeamDrive Agent GUI (WEBCLIENT-459). This is because most external authentication services do not support embedding in a iFrame for security reasons (for example Microsoft Azure).
- Fixed an update problem (from 3.1.1) which concerned the Container Log table (WEBCLIENT-460).

8.3 3.1.1 (2023-05-23)

- Set client version to 5.0.2.3338
- Added `SyncProviderList` setting (WEBCLIENT-456). This is a comma separated list of Provider codes. All containers of users that belong to these Providers will be periodically synchronised regardless of the `SyncInboxesOnly` setting.
- The Web Portal now writes a “Container Log” which traces the main events and activity regarding a container (WEBCLIENT-457). This includes:
 - `START WEBUI/INBOX` - The container was started because a user logged in.
 - `SYNC WEBUI/INBOX` - The container was started by the auto-sync background task.
 - `STOPPED WEBUI/INBOX` - The container has stopped. Note this log entry is only created when the Web Portal becomes aware that a container is no longer running so this may not be the actual shutdown time.
 - `DELETE FINAL` - The container was completed removed, including all local storage and backups.
 - `SHUTDOWN WEBUI/INBOX` - The container was stopped.
 - `DELETE LOCAL` - The container’s local storage was deleted.
 - `ERROR WEBUI/INBOX` - An error occurred when starting the container.
 - `CREATE WEBUI/INBOX` - A new container was created for an inbox or a user that logged in for the first time.
 - `CREATE BACKUP` - The container database and settings have been copied to the Cloud Storage.

- RESTORE BACKUP - The container database and settings have been restored from Cloud Storage.
- REMOVE BACKUP - The Cloud Storage backup of the container has been removed.
- ERROR RESTORE - An error occurred while restoring the container from Cloud Storage.
- Fixed a problem with the flag that indicates that the local databases exists. This can effect the auto-sync function which starts a container regularly so that changes to spaces are applied even if the user does not login.
- Fixed upgrade of the WP_Container table which fails with the error: Invalid default value for 'ActiveTime'.

8.4 3.1.0 (2022-10-25)

- Set client version to 4.8.0.3249
- The setting `BuildBinaryName` is now read-only and is set to the name of the Agent binary executable from the Agent archive on upgrade. The binary is then renamed to “teamdrived.bin” which is the fixed name now used by the Web Portal (WEBCLIENT-451).
- The Web Portal will now periodically start containers so that the TeamDrive Agent can sync any changes that may have occurred in space (WEBCLIENT-454).

A new auto-task, **Synchronise Containers**, was created to perform this operation.

The settings: `ContainerRunLimit`, `EnableSyncContainers` and `SyncInboxesOnly`, have been added to control the behaviour of the task.

See `container_syncing` for more details..

- Addition template variables for `SandboxCommand`:
 - {RLE=T} Set to non-zero value if the option “require-local-encryption=true” should be set when starting the agent.
 - {IST=N} Set to non-zero if the option “idle-shutdown-timeout” should be set to the given value.
 - {ESE=F} Set to non-zero if the option “enable-shell-extension=false” should be set.
- Prevent the pre-5.0 TeamDrive Agent from starting the shell extension (WEBCLIENT-453).
- If the Web Portal cannot reach the Agent (HTTP connection failed), it will terminate the process (if it is running) and return a session timeout error to the Web GUI (WEBCLIENT-450).
- Hardening sets `UMASK` to 077 which requires group privileges to be fixed when the TeamDrive Agent package is unzipped (WEBCLIENT-452).
- Login on the Web Portal no longer returns the “Unknown user” error (WEBCLIENT-438). Instead, it will return an error of the form: “Username or password incorrect”, when the user enters their password.
- The Admin Console now displays the Auto Task list (WEBCLIENT-434).
- The `mod_agent.log` can now be viewed in the Admin Console.
- Added a new `Sandbox` setting: `RequireLocalEncryption`, which allows you to ensure that all containers of the Web Portal use local encryption (WEBCLIENT-399).
- When `UseEmbeddedLogin` is set to `True`, the “embedded” option is no longer set for the `RegistrationURL` link (WEBCLIENT-379). This is because the Web Portal always redirects to this page, and does not embed the page in the Web user interface.
- Improvement to Web Portal redirection:

The Web Portal will display an information message when the user has been redirected from another Web Portal.

After a redirect has occurred, the login name (username or email) entered by the user will preserved and display in the appropriate field (WEBCLIENT-363).

If the login email contains a registered domain, then the Web Portal will redirect to the Web Portal belonging to the Provider of the domain, even if the user is not yet a registered user (WEBCLIENT-375).

When multiple Web Portals are used by the same Registration Server, the user will now be redirected to their Provider associated Web Portal, when attempting to login to the incorrect Web Portal. Previously users were only redirected when the required Web Portal was associated with a different Registration Server.

NOTE: The Web Portal associated with Provider is specified by the `WEBPORTAL_API_URL` Provider setting. This value must be set if redirection is required.

RELEASE NOTES - VERSION 3.0

9.1 3.0.4 (2022-09-21)

- Set client version to 4.8.0.3223

9.2 3.0.3 (2022-06-15)

- Set client version to 4.7.5.3196

9.3 3.0.2 (2022-01-10)

This release also includes a number of security improvements. Please follow the instructions in `upgrade_to_dockerless` to upgrade an existing Web Portal to a docker-less version. Please contact TeamDrive for further details.

- For security reasons, Docker has been replaced by customised TeamDrive Agent containerisation (WEBCLIENT-430).

The settings `ImageBuildFolder`, `MinDockerDataSpaceAvailable`, `MinDockerMetaDataSpaceAvailable`, `RootlessDocker`, `BuildDockerfile`, `ImageBuildCommand`, `DockerEntryPoint`, `BuildWgetCommand`, `ContainerHosts`, `ContainerUserID`, `ContainerGroupID`, `RunAsUser`, `RunAsGroup` and `UseSudo` are no longer used and have been removed.

Renamed `DockerHost` setting to `ContainerHost`.

- Added a new apache module: `mod_agent` which is now responsible for routing calls from the browser to the respective TeamDrive Agent.
- Added the `SandboxCommand` setting which specifies the command for the TeamDrive Agent sandbox. If empty, then the agent is not run in a sandbox.

The following template variables may be used in the setting:

- `{TDBIN}` TeamDrive Agent binary, this value should be: `"/var/teamdrive/webportal/agent/teamdrived.bin"`
- `{APIPORT}` API port number
- `{WSPORT}` Websocket port
- `{USERNAME}` The username of the TeamDrive user
- `{ROOTPATH}` TeamDrive root path, this value should be `"/teamdrive/"` the Agent directories used on this path are `"{ROOTPATH}{USERNAME}/system"` and `"{ROOTPATH}{USERNAME}/spaces"`

- {DBSPATH} The alternative database path, which is used to store the SQLite database files. If there is no alternative path then {DBSPATH} == {ROOTPATH}. The actual directory used by the agent is: “{ROOTPATH}{USERNAME}/system”
- {INIPATH} The shared directory which contains the “teamdrive.ini” file.

9.4 3.0.1 (2021-10-11)

This is a security update.

- A number of security issue have been fixed, please contact TeamDrive for further details.
- yvva 1.5.11 is required which includes measures to prevent “Log Poisoning” by encoding r and n characters (YVVA-52).
- Fixed container creation error after user was deleted and recreated (WEBCLIENT-418 and WEBCLIENT-419).

9.5 3.0.0 (2021-08-20)

The 3.0 release includes a several security bug fixes and a number of hardening measures, and is recommended to all users.

Please contact TeamDrive for further details.

Version 3.0 is an in-place upgrade to all previous versions running on CentOS 7.

On CentOS 8 the new version runs with Docker in “rootless mode”, see:

<https://docs.docker.com/engine/security/rootless/>

Because of the added security due to rootless mode, and other CentOS 8 security updates, all users of the Web Portal are requested to transition to this version as soon as possible.

- Initial public release of 3.0.
- Set security headers in Apache configuration (WEBCLIENT-400).
- OS hardening and security update to Apache configuration (WEBCLIENT-385).
- Hardening of TeamDrive Agent (Agent Version >= 4.7.1.3011).
- Support for running Docker in rootless mode (only CentOS 8)

RELEASE NOTES - VERSION 2.0

10.1 2.0.8 (2020-05-10)

- Fixed an access denied error when calling the Registration Server API to get information on a user that belongs to a another provider (i.e. a provider other than the Web Portal's provider).
- Fixed handling of email address change due to user deletion or if two users switch email addresses (WEBCLIENT-372).
- Added support for MySQL 8
- Set client version to 4.7.0.2944

10.2 2.0.7 (2020-12-16)

- If a user logs in with an email address that is not unique, the Web Portal will return an appropriate error (WEBCLIENT-358).
- Login with email will now re-direct to the correct Web Portal if necessary, provider Registration Server version 4.5.4 or later and TDNS version 2.0.2 is use (WEBCLIENT-357).
- Set client version to 4.6.12.2793

10.3 2.0.6 (2020-10-02)

- Login with a temporary password was not working when using an email address (WEBCLIENT-356).
- Fixed bug: the Web GUI not going directly to the external authentication login page when `AuthServiceEnabled` was set to `True` (WEBCLIENT-355).
- Entries separated by a newline in the `ContainerHosts` setting was not working correctly (WEBCLIENT-354).
- Fixed "Array index out of bounds" error when accessing the "Build Image" settings details page.

10.4 2.0.5 (2020-09-15)

- The "White Label" settings have been renamed to "Build Image" settings. In addition, the setting `UseWhiteLabeldDockerImage` has been removed and the `WhiteLabelINIFileSettings` setting has been rename to `ClientSettings` (see below).

`UseWhiteLabeldDockerImage` is no longer required because all Web Portals now use the image build settings to create a new Docker image on upgrade, if necessary.

The setting `WhiteLabelIdleTimeout` has been renamed to `ContainerIdleTimeout` and is now a “Docker Setting” (see `containeridletimeout`).

The `IdleContainerTimeout` setting has been renamed to `RemoveIdleContainerTime` to better distinguish this value from `ContainerIdleTimeout`.

- Added `SharedIniPath` and `AgentCommandLineArgs`. Using `SharedIniPath` you can specify a global path for the “teamdrive.ini” file (WEBCLIENT-350).

`WhiteLabelINIFileSettings` has been renamed to `ClientSettings` and is now a “General Setting”. Client settings that are set using the `ClientSettings` setting are then written to the `teamdrive.ini` file. If a `SharedIniPath` is specified, then they are read by the all TeamDrive agents, when a container starts. If not, then the client settings are written to the `/etc/teamdrive.ini` file, which is part of the container image.

The `AgentCommandLineArgs` settings is a read-only variable that specifies the command line arguments that are passed to the TeamDrive agent when the container starts.

See `sharedinipath`, `agentcommandlineargs` and `clientsettings` for details.

- Added `MaxLoginRate` and `MaxLoginLogAge` settings. These settings are used to detect Denial of Service and other brute force attacks targeting the Web Portal login (WEBCLIENT-344). See `maxloginrate` and `maxloginlogage` for details.
- Error messages returned by the Web Portal are now use the translation file provided by the TeamDrive Agent.
- Added `ContainerHosts` setting (see `containerhosts`). Use this to specify entries for the “/etc/hosts” file of the container (WEBCLIENT-139).
- You can now configure a proxy during setup of the Web Portal (WEBCLIENT-338).
- If `AuthServiceEnabled` is `False` the Web Portal now uses external authentication as required by the user, provided you are using TeamDrive Agent 4.6.11.2656 or later (WEBCLIENT-335).

As before, if `AuthServiceEnabled` is `True`, then Web Portal uses a specific authentication service (as specified by `AuthLoginPageURL` and `AuthTokenVerifyURL`).

See `authserviceenabled` for more details.

- Moved settings `SessionTimeout`, `ForceHTTPSUsage` and `ForceHTTPSUsage` to Admin Console settings group.
- Moved `RegistrationEnabled` and `RegistrationURL` to the Authentication settings group.
- The Web Portal will now redirect to another Web Portal, if a user attempts to login to the incorrect Web Portal (WEBCLIENT-333). This is done if the provider of the user is not in the list of `AllowedProviders`.

On the Registration Server of the user, you must set the `WEBPORTAL_API_URL` provider setting. This setting specifies the domain name of the Web Portal used by the provider. In addition, Registration Server version 4.5.4 is required. This version implements the “webportal” redirect required to implement this functionality.

If any of these conditions is not met, then the user will get the error message: “The provider you are registered to is not enabled for this web portal”.

- Set the minimum client Agent version to 4.6.11.2707. This version support the Web Portal redirect, and includes some error message improvements.
- Setting the default distributor code, and language using the `portal/login.html` and `extauth/login.html` pages is not longer supported.

10.5 2.0.4 (2020-05-19)

- Added Multi-Registration Server support.

- Fixed agent download URL.
- All documents and security relevant data stored in containers run by the web portal are now encrypted when using TeamDrive Agent version 4.7 or later.

Encryption activates the so-called “super PIN” functionality implemented by Registration Server 4.2. When the super PIN is activated for an account the user is required to print out and save a 56-digit super PIN, and recovery URL (in the form of QR code) in a secure place.

After activation of the super PIN functionality the user can only access their account using their password, or the super PIN, or the recovery code (which can be retrieved using the recovery URL). Changing your password is also only possible using either the super PIN or recovery code.

- Changes made to support local encryption of inboxes. Encryption of inboxes required Registration Server version 4.2 or later, and TeamDrive Agent version 4.7 or later.
- Added `ContainerDatabases` setting (WEBCLIENT-334). This setting allows you to specify an alternative path for the SQLite databases used by the containers. Normally all data is placed in the `ContainerRoot` directory.

When specified the new location will be mounted in the container under the path: `“/teamdrive/dbs”`. However, this path will only be used if you build a new image using the TeamDrive Agent version 4.6.12.2637 or later.

This version of the client supports the `“--database-path”` option which allows you to specify an alternative path for the SQLite database. When `ContainerDatabases` is set, the image build process will automatically add this option to the start parameters of the agent (see `@USEDATABASEPATH` in the `WhiteLabelDockerfile` setting).

10.6 2.0.3 (2020-04-14)

- Changes for yvva 1.5.2 compatibility.
- Fixed a problem removing container data, remove directory was failing when a ‘\$’ was in the path name.
- The Web Portal will now correctly use the database specified in the `“td-webportal.my.cnf”` file (WEBCLIENT-296). Previously the database name was hard-coded to `“webportal”`.
- Fixed: in case of an exception the temporary file created by `syscall()` is not be deleted (WEBCLIENT-316).
- Fixed: HTML entities conversion problem when editing setting `“WhiteLabelDockerfile”` (WEBCLIENT-323).
- When the docker image is being updated, the Web GUI will now return the error `“Upgrade in progress, please try again shortly”`, when the user attempts to login.
- Added API functions to enable and disabled a container (WEBCLIENT-324).
- Added support for `“prelogin”` call in order to support login changes (WEBCLIENT-327).
- Added `“sqlite-synchronous=normal”` as start parameter for the agents to reduce SQLite flush frequency
- Set client version to 4.6.10.2619

10.7 2.0.2 (2019-07-26)

- Increased `MinimumAgentVersion` to 4.6.7.2355.

10.8 2.0.1 (2019-06-11)

- Fixed problems the on demand creation and starting of containers that have been deleted (WEBCLIENT-304).

10.9 2.0.0 (2019-04-25)

Note: Please follow the new update process described in chapter `upgrade_web_portal`. The former separate GUI rpm package is not longer necessary. The standard Web Portal will update the docker Container image from the docker hub during the update step and will extract and update the files necessary for the GUI from this image. A white label Web Portal needs the white label agent .tar.gz to build a white label docker container image.

- Initial release of Web Portal 2.0.

10.9.1 Upgrading from previous versions of the Web Portal

As of version 2.0.4 you must run the `upgrade_now` command from the console after installing a new version of the Web Portal.

This command updates the database structure and the docker image used by the Web Portal. The Admin Console may return errors, and other random errors may occur before the upgrade had been completed.

To update the database structure and docker image start `yvva` and execute `upgrade_now;;`. This command also upgrade the container image used by the Web Portal. See the chapter `upgrade_web_portal` for details.

10.9.2 Key features and changes

- Increased `MinimumAgentVersion` to 4.6.7.2328
- External authentication supports both login and registration. This feature can be activated by setting `AuthServiceEnabled` to `True`. To allow registration set `RegistrationEnabled` to `True`. If no `AuthLoginPageURL` or `RegistrationURL` page is specified then the Web Portal will use the “portal pages”, provided by the Registration Server.
- External authentication can be embedded in the TeamDrive Web GUI, or can the external authentication pages can be used directly. A new setting: `UseEmbeddedLogin`, must be set to `True` in order to use the embedded login form.

By default, `UseEmbeddedLogin` is set to `False` if you upgrade from a previous version of the Web Portal that was using external authentication. Otherwise, the default is `True`. This is to ensure backwards compatibility, with previous versions that only supported the non-embedded form.

Accessing the Web Portal domain, for example: `https://webportal.yourdomain.com`, will automatically present the login in the embedded or non-embedded form, as specified by `UseEmbeddedLogin`.

- You can now use “explicit” links to the login page in order to set the default provider code and language, for the login or registration.

For the non-embedded login form use the following explicit link:

`https://webportal.yourdomain.com/portal/login.html?dist=CODE&lang=LG`

and for the embedded login form use the following explicit link:

`https://webportal.yourdomain.com/extauth/login.html?dist=CODE&lang=LG`

where `CODE` is the provider code, and `LG` is the language code, for example `en` or `de`.

Note that the external authentication service must be able to handle the specified provider code and language.

10.9.3 Administration Console

- Added a Container list page, which can be used to search for containers of a particular user and type. The container details page allows you to stop, start and delete containers.

Note that deleting a container will remove all the container data as well. This means that Web Portal users will find all spaces deactivated on next login. If the user loses his password he will also lose access to his data, unless he has a TeamDrive installation elsewhere.

RELEASE NOTES - VERSION 1.2

11.1 1.2.3 (2019-01-15)

- Reset of Admin User's password as described in the documentation (i.e. by setting the password to blank in the database) was not working (WEBCLIENT-259).
- Added a illustrated overview of the Web Portal to the documentation, showing the connection to other components in the TeamDrive system (see `introduction_to_the_teamdrive_web_portal`).

11.2 1.2.2 (2018-11-06)

- The Web Portal supports now the Docker Community and Enterprise Edition and also still the old Commercially Supported version with the latest version 1.13 (from January 2017). Please notice, that the Docker CS version will be still maintained, but not further developed any more. Check the docker installation chapter for the differences between Docker CS and CE/EE installation.
- The Web Portal will only allow using signed DISTRIBUTOR files like the standard client. The signature will be checked during the creation of the docker image and at each start of the agent. Additional client settings must be moved to the new setting `WhiteLabelINIFileSettings`. If settings are still required in the DISTRIBUTOR file it must be signed by TeamDrive Systems for you.
- The current agent supports now web-sockets to refresh data in the browser without refreshing the page itself. To support web-socket connections, the apache module `proxy_wstunnel_module` must be enabled (See `configure-apache-24` for details)
- Increased `MinimumAgentVersion` to 4.6.4.2183

11.3 1.2.1 (2017-11-29)

- Increased `MinimumAgentVersion` to 4.5.5.1838
- Upgrade will change the `WhiteLabelAgentDownloadURL` setting from `".../{PRODUCTNAME}_agent_{VERSION}_x86_64.tar.gz"` to `".../{PRODUCTNAME}_agent_{VERSION}_el7.x86_64.tar.gz"`. this is done because the TeamDrive agent is now built in 2 versions: "el6" are built for CentOS 6, and "el7" versions are built for CentOS 7. It is assumed that the Web Portal is run on a CentOS 7 platform. If this is not the case, then you must manually change this setting to `".../{PRODUCTNAME}_agent_{VERSION}_el6.x86_64.tar.gz"` (WEBCLIENT-255).
- Updated documentation to include new TeamDrive CI (WEBCLIENT-254).
- The Web Portal external authentication now handles transitioning to a new User Secret generation algorithm as implemented by Registration Server version 3.7.6.
- Bug fix: boolean settings were not correctly pre-selected.

- Several improvements have been made to the upgrade procedure which generates a new Docker image. The setting `WhiteLabelAgentDownloadURL` can now be left blank, of the Agent archive (.tar.gz file) has been placed manually in the build folder (`WhiteLabelDockerBuildFolder`).
- If `ContainerImage` is set to image with a version number higher than the `MinimumAgentVersion`, then the Web Portal will build an image for the version specified by `ContainerImage`.
- Version 1.2.1 requires YVVA runtime version 1.4.4.

11.4 1.2.0 (2017-08-14)

Note: Please follow the new update process described in chapter `upgrade_web_portal`. The former separate GUI rpm package is not longer necessary. The standard Web Portal will update the docker Container image from the docker hub during the update step and will extract and update the files necessary for the GUI from this image. A white label Web Portal needs the white label agent .tar.gz to build a white label docker container image.

- Initial 1.2 release.

11.4.1 Key features and changes

- Simplified installing and updating the web portal and docker container for standard and white label configuration.
- Increased `MinimumAgentVersion` to 4.5.2.1775 to support PointInTime-Recovery and Read-Confirmations

RELEASE NOTES - VERSION 1.1

12.1 1.1.0 (2017-04-10)

Note: When updating from an older version of the Web Portal, remove the `DOCKER_HOST` setting in the apache config file `/etc/sysconfig/httpd`. It is not longer necessary.

If you update docker to version 1.12.6 the docker service might not start anymore as described in the docker release notes: <https://github.com/docker/docker/releases/tag/v1.12.6> Please remove the file `/etc/systemd/system/docker.service.d/web-portal.conf` and add the `--host=tcp://0.0.0.0:2375` instead to the `OPTIONS` parameters in `/etc/sysconfig/docker` as described in the docker configuration chapter.

- Initial 1.1 release.

12.1.1 Key features and changes

- Added professional license required check (WEBCLIENT-233)
- Added setting to limit currently active users (WEBCLIENT-234)
- Added setting for minimum docker available data and meta data space. If minimum is reached, no more docker container will be created for new users (WEBCLIENT-235)
- Settings are now displayed in groups in the Admin Console (WEBCLIENT-237).
- Increased `MinimumAgentVersion` to 4.3.2.1681 to support space web access settings (TDCLIENT-2184). The webportal docker agent will be started with an additional setting `agent-type=webportal` to distinguish a standard and a webportal agent
- Added settings to support a Proxy for outgoing connections: `UseProxy`, `ProxyHost` and `NoProxyList` (WEBCLIENT-242). See `outgoing_connections` for details.
- Added the `ConnectionTimeout` setting which specifies a timeout for outgoing connections (see `outgoing_connections`).
- Added support for Docker Swarm. Docker Swarm is a native clustering for Docker. It turns a pool of Docker hosts into a single, virtual Docker host. Please notice, that only the legacy standalone Swarm is supported (<https://docs.docker.com/swarm/overview/>), because of the different service model in the Docker Engine v1.12.0 using the swarm mode. Change the `DockerHost` Web Portal setting from the standard docker port 2375 to the swarm port 2377 to switch from the standard docker API access to the swarm API access (WEBCLIENT-245).

RELEASE NOTES - VERSION 1.0

13.1 1.0.9 (2017-02-10)

- Increased MinimumAgentVersion to 4.3.1.1656 to fix a bug when login with email address and magic usernames.
- Revised chapter Web Portal Virtual Appliance with CentOS 7 and docker direct-lvm storage

13.2 1.0.8 (2017-02-07)

Note: After updating docker to version 1.12.6 the docker service might not start anymore as described in the docker release notes: <https://github.com/docker/docker/releases/tag/v1.12.6> Please remove the file `/etc/systemd/system/docker.service.d/web-portal.conf` and add the `--host=tcp://0.0.0.0:2375` instead to the OPTIONS parameters in `/etc/sysconfig/docker` as described in the docker configuration chapter.

- Removed support for CentOS 6
- Fixed docker configuration
- Fixed PDF creation for this documentation
- Fixed download links for VM-Ware images

13.3 1.0.7 (2016-11-10)

- Increased MinimumAgentVersion to 4.2.2.1579 to support email notifications
- Fixed docker configuration
- Fixed apache 2.4 configuration

13.4 1.0.6 (2016-07-11)

Note: Updating the Host Server on CentOS 7 with “yum update” might update the apache to a newer version. This update could re-install the deleted “conf”-files in the folder `/etc/httpd/conf.modules.d/` and will prevent starting the apache. Please follow the modified instruction to disable all modules in the “conf”-files instead of deleting them as described in `configure-apache-24`

- Improved Docker installation documentation (WEBCLIENT-219, WEBCLIENT-223).

- The Web Portal now checks if the user is authorised to access a Web Portal. A user is authorised to access a Web Portal if the Provider setting: `ALLOW_WEB_PORTAL_ACCESS` is set to `permit` or `ALLOW_WEB_PORTAL_ACCESS` is set to `peruser` and the user's "Web Portal Access" capability bit is set (a user-level setting).

When using external authentication, the same check is done if the Registration Server is version 3.6 or later. When using a Registration Server 3.5 or earlier, the Web Portal will not check the user's Web Portal access permissions (in the case of external authentication).

- Added setting `AllowedProviders` which is a list of Provider codes of the users that are allowed to login to the Web Portal.

An input field on the setup page allows this variable to be set during installation of the Web Portal.

- The URL `https://webportal.yourdomain.com/portal/authservice.html` is now the target URL for external Authentication Services acting on behalf of the Web Portal.

In other words, in successful authorisation by an external Authentication Service, the user is redirected back to this page.

The Web Portal will now add certain arguments to `AuthLoginPageURL` and `RegisterURL` pages:

- “portal=true”: This argument is always added to the URL. This is useful, in the case when the same Authentication Service is called by the TeamDrive Client and the Web Portal. The argument can be used to determine whether to redirect on successful login or not.
 - “cookie=?”: This argument will be added if the Authentication Service provided a cookie after the last successful login. The cookie is stored by the TeamDrive Agent.
 - “error=?”: This argument indicates that the Web Portal encountered an error after successful authorisation by the Authentication Service. It is a base-64 (URL) encoded string containing the error message. The error should be displayed in the login page served by the Authentication Service.
- Support CentOS 7 with Apache 2.4
 - Increased `MinimumAgentVersion` to 4.2.0.1470 to support the space activities
 - Added setting `RegistrationEnabled` (default `False`). This value must be set to `True` to allow registration of users directly via the Web Portal.
 - Added login and registration pages: All of these pages redirect to the associated pages on the Registration Server. After login, or registration, the Registration Server redirects back to the Web Portal.
 - `https://webportal.yourdomain.com/portal/login.html` This page allows users to login using two-factor authentication, if this has been configured. `/portal/login.html` is now the default for the `AuthLoginPageURL` setting.
 - `https://webportal.yourdomain.com/portal/register.html` Using this page a user can register as a TeamDrive user without installing the TeamDrive Client. After registration the user has access to the Web Portal. `/portal/register.html` is now the default for the `RegisterURL` setting.
 - `https://webportal.yourdomain.com/portal/lost_pwd.html` This page sends a temporary password to the user and allows the user to login and set a new password. The page is linked from `/portal/login.html`.
 - `https://webportal.yourdomain.com/portal/setup-2fa.html` Using this page the user can configure two-factor authentication using the Google Authenticator App.
 - The default of the “`AuthTokenVerifyURL`” setting is now: `https://webportal.yourdomain.com/portal/verify.html`

13.5 1.0.5 (2016-02-16)

- Fixed a problem on login with a user registered via the Registration Server API using email address as identification (WEBCLIENT-205).

- Use the -v option when removing containers. This ensures that the container volume is also removed (WEBCLIENT-204).

13.6 1.0.4 (2016-02-09)

- Framework synced with Host- and Reg-Server

13.7 1.0.3 (2016-02-02)

- Added setting `MinimumAgentVersion` which specifies the minimum version of the TeamDrive Agent that will work with the Web Portal. Upgrade to this version of the Agent is forced as soon as the new version of the Web Portal is online (WEBCLIENT-194).
- Updated documentation for Docker version 1.7.1
- Fixed Internet explorer caches API calls. (WEBCLIENT-186)
- Added description about the dependencies between Webportal, Provider and Reg-Server and normal and external Authentication. (WEBCLIENT-176)
- The `performExternalAuthentication` redirects to <http://> instead of <https://>. (WEBCLIENT-182)
- The `getLoginInformation()` API call now returns “registerUrl” if the setting `RegistrationURL`, is set on the Web Portal. (WEBCLIENT-179)
- Redirect to the login page when a request to an agent returns a 503 code. This requires a manual update to the `ssl.conf`, refer to the documentation on server installation and configuration. (WEBCLIENT-198)

13.8 1.0.2 (2015-12-07)

- Fixed container language settings so that Spaces with non-ascii characters in the name now work.
- Corrected redirect to external login pages under certain circumstances.
- Login with an email address now works.
- The Portal no longer creates containers based on the case of the input username, instead the actual username is used. This prevents the creation of duplicate containers for the same user.
- The Web Portal session will now timeout after 15 minutes idle time. The user is then required to login again.
- Implemented reset password functionality. Login after password has been forgotten now works. The user will receive a temporary password via email which is used to set a new password and login.
- Note, new re-write must be added to `/etc/httpd/conf.d/ssl.conf`:

```
RewriteRule ^/requestResetPassword /yvva/requestResetPassword [PT]
RewriteRule ^/tempPasswordLogin /yvva/tempPasswordLogin [PT]
```

- Fixed loading of favicon

13.9 1.0.1 (2015-10-27)

- `OldImageRemovalTime` setting was not visible.
- Updated Web Portal GUI to the latest 4.1.x version from the webfrontend branch.

13.10 1.0.0 (2015-10-08)

- Initial public release of the Web Portal.
- Web Portal 1.0 requires TeamDrive Agent version 4.0.12.1292 or later.

14.1 Abbreviations

PBT PBT is an object oriented language specifically designed for the programming of “server-side” functionality common to intra- and internet Web sites. A large share of the TeamDrive Host, Registration Server and Webportal Server functionality is implemented in PBT. The code is parsed and executed by the Yvva application server components.

TDNS Team Drive Name Service

TDRS Team Drive Registration Server

TSHS Team Drive Scalable Host Storage.