TeamDrive Web Portal Virtual Appliance Installation

Release 2.0.0.0

Paul McCullagh, Eckhard Pruehs

2019

CHAPTER

ONE

COPYRIGHT NOTICE

TeamDrive Systems GmbH
https://www.teamdrive.com
Max-Brauer-Allee 50
22765 Hamburg, Germany
Email: info@teamdrive.com

CHAPTER

TWO

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.

“Docker” is a trademark or registered trademark of Docker, Inc.

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

CHAPTER

THREE

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.

Note that the requirements describe here apply in particular to the system running the Docker host. The hardware requirements of the other components of the Web Portal are minimal in comparison, and can be set at approximately 10% of the power of the Docker service. See scaling for more details.

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 Docker container running the TeamDrive Agent for each active user session. Each container requires about 100 MB of RAM.

You can assume that the number of containers running is greater than the number of active users (the number of users accessing the portal at any given time). This is because a container continues 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.

For Web Portals running on a cluster of host machines, the storage system must be mounted by all hosts in the cluster.

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.

Another volume will be needed by docker to store the container images and running instances. An overview can be found here:

> https://docs.docker.com/engine/userguide/storagedriver/imagesandcontainers/

The recommended storage configuration for production use is using the direct-lvm (logical volume manager) as the preferred storage driver. Configure the volume as described in this instruction after installing and before starting docker the first time:

> https://docs.docker.com/engine/userguide/storagedriver/device-mapper-driver/#/configure-direct-lvm-mode-for-production

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 4,5 or 6 (VMWare Workstation 7 can be used for testing purposes)
- Minimum VM Memory: 2 GB
- vCPUs: 2
- HDD: 100GB
- Guest OS: CentOS 7 (64-bit)

3.4 Main Software components

The TeamDrive Web Portal comprises the following components and modules:

- Apache Web Server 2.4
- Docker 1.6.2 (or later)
- MySQL 5.6 (or later) Database Server
- TeamDrive Agent
- Yvva Runtime Environment version 1.4

CHAPTER

FOUR

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:

http://s3download.teamdrive.net/HostServer/TD-Web-Portal-CentOS7-64bit-2.0.0.0.zip

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

http://s3download.teamdrive.net/HostServer/TD-Web-Portal-CentOS7-64bit-2.0.0.0.zip.sha1

You should verify the SHA1 checksum to ensure that the zip archive is intact.

You can use the `sha1sum` 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 verify a SHA-1 digest on Mac OS X
- Microsoft Windows: Availability and description of the File Checksum Integrity Verifier utility

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:

http://repo.teamdrive.net/RPM-GPG-KEY-TeamDrive

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

```
$ gpg --fingerprint support@teamdrive.net
pub   2048R/9A34C453 2014-07-01
      Key fingerprint = 8F9A 1F36 931D BEFA 693B  9881 ED06 27A9 9A34 C453
uid                  TeamDrive Systems (RPM Build Key) <support@teamdrive.net>
sub   2048R/6048C568 2014-07-01
```

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

http://s3download.teamdrive.net/HostServer/TD-Web-Portal-CentOS7-64bit-2.0.0.0.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-CentOS7-64bit.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 `root` user with the standard password `teamdrive`.

To change the default password, type in:

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

and define your own strong password. To change the network device and DNS, type in:

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

A detailed description for the network setup can be found here http://www.krizna.com/centos/setup-network-centos-7/

Note: A cloned CentOS image in a VMWare environment might exhibit problems updating the network interface. If you are observing issues when configuring the network interface, please follow these instructions: https://wiki.centos.org/TipsAndTricks/VMWare_Server

---

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 `yum` 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 ~]# yum update -y
```

`yum` 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 yum 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 `yum 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 Install latest TeamDrive Agent version

Please install the latest TeamDrive Agent docker image. A list of released versions can be found here: https://hub.docker.com/r/teamdrive/agent/tags/ To update the docker image start `yvva` and execute `upgrade_now;;`:

```
[root@webportal ~]# yvva
Welcome to yvva shell (version 1.3.8).
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;;
Perform upgrade changes to the Docker image and/or database (this command cannot␣
↪be undone).
```

Leave the yvva shell by type in `quit`.

Note: If outgoing requests has to use a proxy server, follow the docker documentation https://docs.docker.com/engine/admin/systemd/#http-proxy to set a proxy for docker. Restart the docker service after adding the proxy configuration.

The agent is a headless version of the standard TeamDrive client. A docker container will be started for each user using the Web Portal (as described in chapter introduciton_to_the_teamdrive_web_portal).

4.6 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	

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' = PASSWORD('<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.

4.7 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 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.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-using-firewalld-on-centos-7

4.8 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.

4.9 Mount user data Volume

As described in docker-configuration the user data will be stored outside the docker instances. 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).

4.10 Mount docker devicemapper Volume

Docker itself needs storage for the running container instances. The Web Portal background task will automatically remove stopped instances after the the defined `IdleContainerTimeout` (see web_portal_settings). The time can be short, because the persistant user data is stored outside the docker instances. It will just take a few more seconds if a new instance for the user must be recreated based on the container image.

The VM image comes with a preconfigured 20 GB LVM storage volume using the docker storage driver `devicemapper` per direct-lvm access. Docker supports different storage drivers as described here: https://docs.docker.com/engine/userguide/storagedriver/selectadriver/

To get an overview of the used storage, see the docker documentation: https://docs.docker.com/engine/userguide/storagedriver/device-mapper-driver/#/examine-devicemapper-structures-on-the-host

You will also find a description how to extend the direct-lvm storage: https://docs.docker.com/engine/userguide/storagedriver/device-mapper-driver/#/for-a-direct-lvm-mode-configuration

CHAPTER

FIVE

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 external Authentication Service has further restrictions. Such a Web Portal can only support one external Authentication Service.

Once a Web Portal is configured for external authentication, it no longer supports regular login (i.e. authentication using the Registration Server). In this case, the user will always be redirected to the external login page, and will not be able to access the standard login page provided by the TeamDrive Agent.

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 3.5 is required to run a Web Portal.

Log in with your provider login and click the tab **Server Management** and then click on **Provider Settings**. In the section **Provider Settings**, click the tab labelled **API**.

Select the `API_WEB_PORTAL_IP` setting and click "Set" to activate The setting. Enter the IP address of the Web Portal and click "Save" to apply this change.

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 above 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:

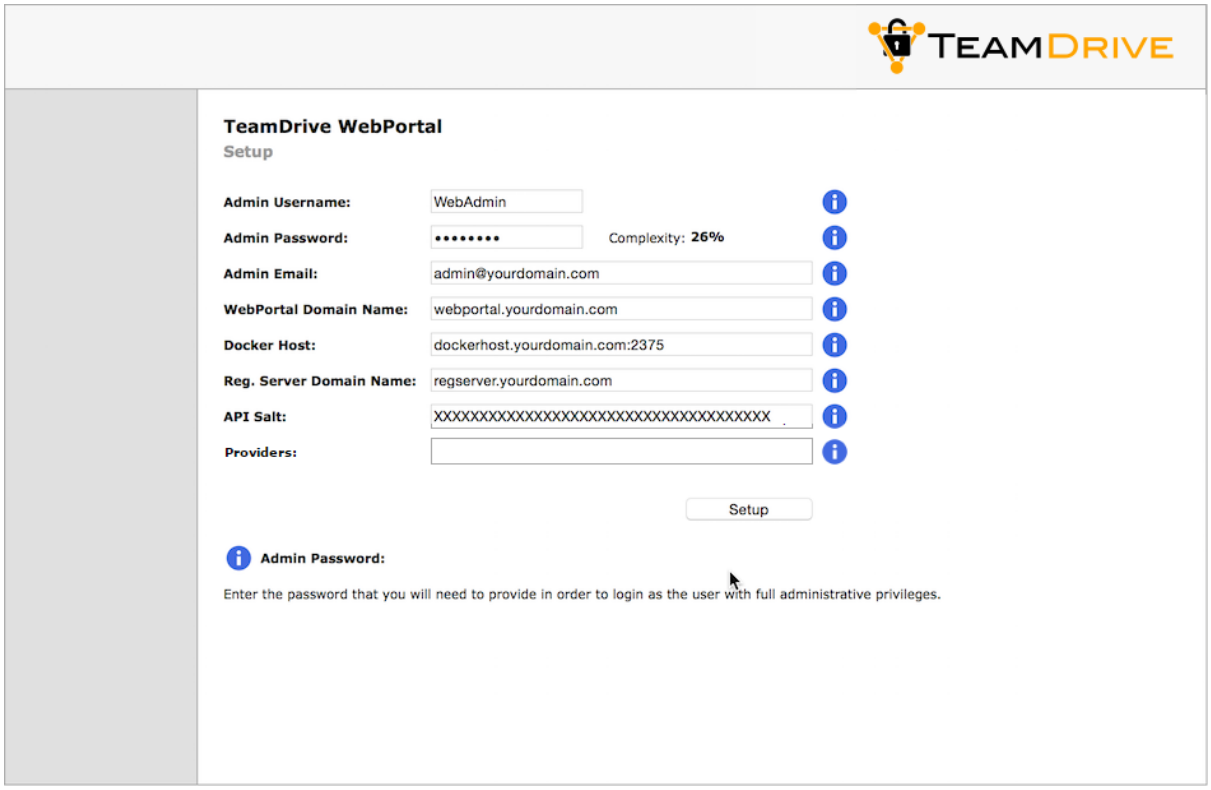

Fig. 5.1: Web Portal Setup Page

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.

Docker Host This is the domain name or IP address of the machine that will host the Docker containers. This may be a different machine to the machine running the Web Portal. The port of the Docker daemon must be included, if the port is not 2375. In case of using a Docker Swarm setup, the Swarm port (default 2377) must be used.

Setup will ping the Docker daemon to ensure that the contact can be established before the configuration process can complete.

Reg. Server Domain Name All Web Portals must be registered with a Registration Server. Enter the fully qualified domain name of the Registration Server. **Please contact TeamDrive Systems for the correct value if you don't manage your own Registration Server.**

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.

API Salt The API Salt 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 `APIChecksumSalt` setting on the Registration Server to avoid "man in the middle"-attacks. Please consult the Registration Server Documentation on how to obtain it or contact TeamDrive Systems for the correct value if you don't manage your own registration server.

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 a 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 or the Docker daemon.

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

5.3 Setup and Administration

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

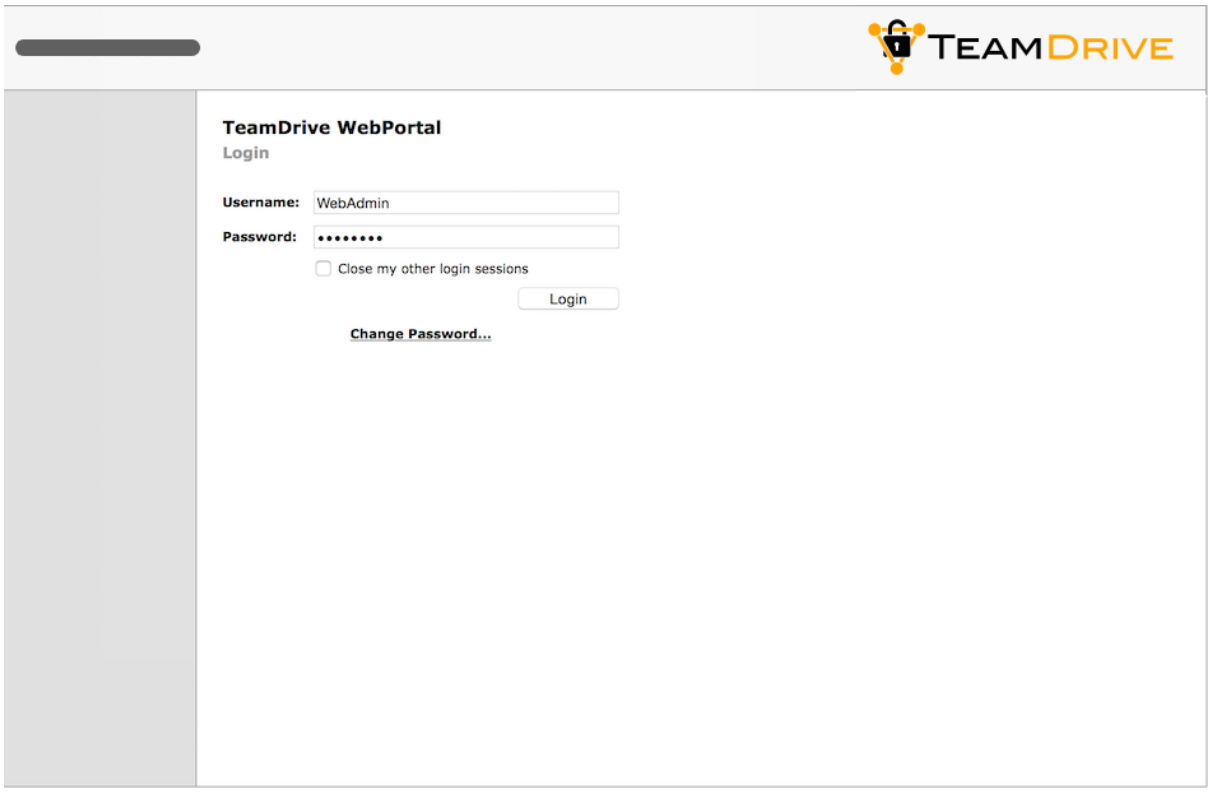

Fig. 5.2: Web Portal Admin Console: Login Screen

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

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

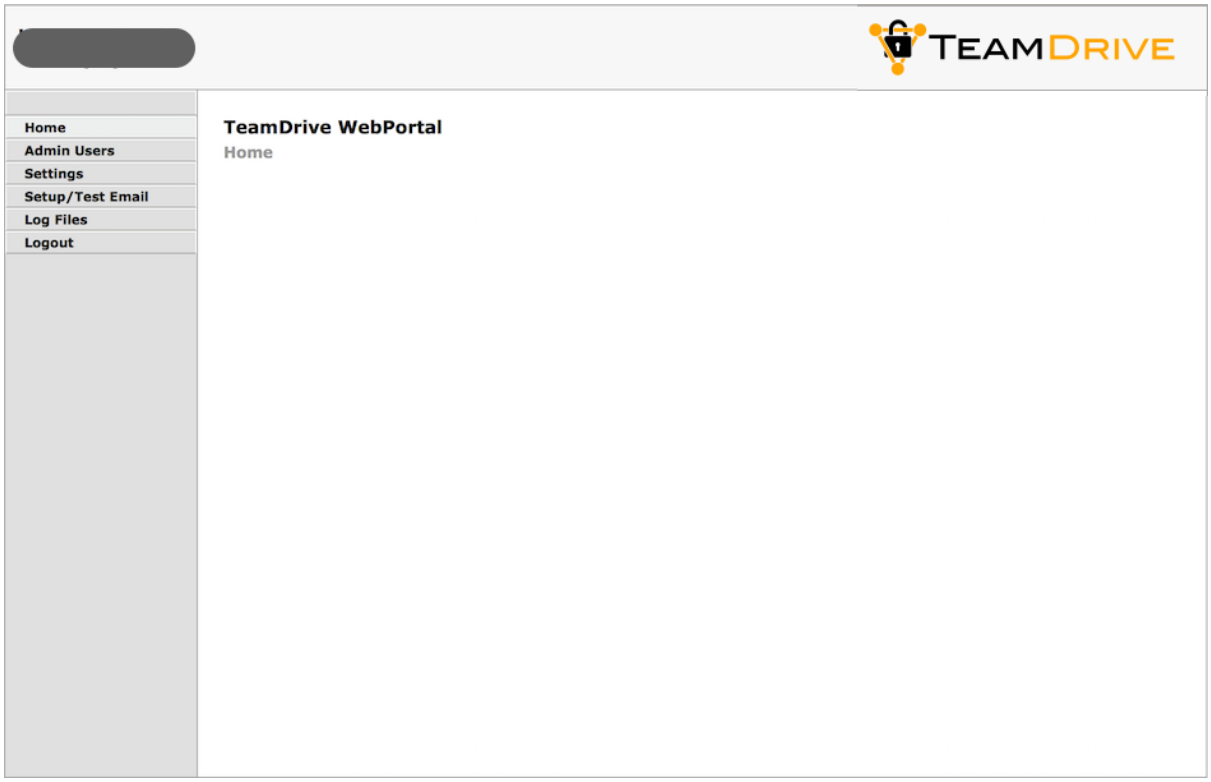

Fig. 5.3: Web Portal Admin Console: Home Screen

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.

5.4 Setting a white label docker container image

Click on the **Settings** menu item in the Web Portal administration and select the **Container-Image** entry. Replace the existing `teamdrive/agent:<version-nr>-TMDR` value with your `teamdrive/agent:<version-nr>-<provider-code>` created docker image from the chapter creating-white-label-agent-image. After saving the value, restart the apache server using:

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

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.

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.

CHAPTER

SIX

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 disable 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 effect the `mod_yyva` 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-httd
```

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-httd: 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.my.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.

6.4.3 Errors When Accessing Docker

If the Web Portal fails to contact the Docker daemon, first check If docker can be accessed using the command line interface, for example:

```
[root@webportal install]# export DOCKER_HOST=tcp://<docker-host>:2375
[root@webportal install]# docker images
```

This command will list the available images. The Docker daemon must be accessible using TCP. How to configure docker for TCP access is explained here: installing-docker.

If the Web Interface does not work correctly it may be that the reference to the Docker host is not correct in the `/etc/httpd/conf.d/ssl.conf` file.

Open up this file and check that you have followed the instructions in section configure-mod-ssl.

CHAPTER

SEVEN

RELEASE NOTES - VERSION 2.0

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.

7.1 Key features and changes

- Increased MinimumAgentVersion to 4.6.7.2261
- 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.

7.2 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 looses his password he will also loose access to his data, unless he has a TeamDrive installation elsewhere.

7.3 Change Log - Version 2.0

7.3.1 2.0.0 (2019-04-25)

- Initial release of Web Portal 2.0.

CHAPTER

EIGHT

RELEASE NOTES - VERSION 1.2

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.

8.1 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

8.2 Change Log - Version 1.2

8.2.1 1.2.3 (YYYY-MM-DD)

- 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 introduciton_to_the_teamdrive_web_portal).

8.2.2 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

8.2.3 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.

8.2.4 1.2.0 (2017-08-14)

- Initial 1.2 release.

CHAPTER

NINE

RELEASE NOTES - VERSION 1.1

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 installing-docker chapter.

9.1 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).

9.2 Change Log - Version 1.1

9.2.1 1.1.0 (2017-04-10)

- Initial 1.1 release.

CHAPTER

TEN

RELEASE NOTES - VERSION 1.0

10.1 Key features and changes

This is the initial release of the Web Portal.

10.2 Change Log - Version 1.0

10.2.1 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

10.2.2 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 installing-docker chapter.

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

10.2.3 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

10.2.4 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 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 may 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/ve`

10.2.5 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).

10.2.6 1.0.4 (2016-02-09)

- Framework synced with Host- and Reg-Server

10.2.7 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)

10.2.8 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

10.2.9 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.

10.2.10 1.0 (2015-10-08)

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

CHAPTER

ELEVEN

APPENDIX

11.1 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 **T**eam **D**rive **N**ame **S**ervice

TDRS **T**eam **D**rive **R**egistration **S**erver

TSHS **T**eam **D**rive **S**calable **H**ost **S**torage.