TeamDrive Web Portal Installation and Configuration

Release 1.0.9.0

Lenz Grimmer, Paul McCullagh

2017

CONTENTS

1 Copyright Notice **1**

2 Trademark Notice **3**

3 Introduction **5**
- 3.1 Required Skills . . . 5
- 3.2 Operating System Requirements . . . 6
- 3.3 Hardware Requirements . . . 6
  - 3.3.1 CPU Requirements . . . 6
  - 3.3.2 RAM Requirements . . . 6
  - 3.3.3 Storage Requirements . . . 6
  - 3.3.4 Network Requirements . . . 7

4 Introduction to the TeamDrive Web Portal **9**
- 4.1 TeamDrive Web Portal Overview . . . 9
- 4.2 TeamDrive Hosting Basics . . . 9
- 4.3 Docker Configuration . . . 10
- 4.4 Background Tasks Performed by `td-webportal` . . . 10

5 Operating System Configuration **13**
- 5.1 Installing a base operating system . . . 13
- 5.2 Enable Time Synchronization with NTP . . . 13
- 5.3 Disable SELinux . . . 13
- 5.4 Firewall configuration . . . 13
- 5.5 Installing the Postfix MTA (optional) . . . 14

6 Installing the Web Portal Components **17**
- 6.1 Enable the TeamDrive Web Portal `yum` Repository . . . 17
- 6.2 Download and Install the TeamDrive Web Portal Package . . . 17
- 6.3 Download and Install a white label Web Portal Package . . . 18
- 6.4 Installing the Web Portal HTML Documentation (optional) . . . 18

7 Apache HTTP Server Installation and Configuration **19**
- 7.1 Update `httpd.conf` . . . 19
- 7.2 Disable Unneeded Apache Modules . . . 19
  - 7.2.1 Apache 2.4 . . . 19
- 7.3 Configure `mod_ssl` . . . 20

8 MySQL Installation and Configuration **23**
- 8.1 Installing MySQL Server . . . 23
- 8.2 Creating TeamDrive MySQL User and Databases . . . 25

9 Pre-Installation Tasks **29**
- 9.1 Mount the Space Storage Volume . . . 29
- 9.2 Installing Docker . . . 29
  - 9.2.1 Configure `direct-lvm` Mode . . . 30

9.3 Installing the TeamDrive Agent Docker Image . . . 30
9.4 Creating a White Label Agent Docker Image . . . 30
9.5 Installing SSL certificates . . . 31
9.6 Starting the Web Portal . . . 31
9.6.1 Starting `td-webportal` . . . 31
9.6.2 Starting the Apache HTTP Server . . . 31

10 Initial Web Portal Configuration **33**
10.1 Associating the Web Portal with a Provider . . . 33
10.2 Activating the Web Portal . . . 33
10.3 Setup and Administration . . . 35
10.4 Setting a white label docker container image . . . 36
10.5 Testing Web Access . . . 36

11 Post-Installation Tasks **39**
11.1 Startup Sequence / Dependencies . . . 39
11.2 Starting the Apache HTTP Server at Boot Time . . . 39
11.3 Starting TeamDrive Service at Boot Time . . . 39
11.4 Next steps . . . 39

12 Troubleshooting **41**
12.1 List of relevant configuration files . . . 41
12.2 List of relevant log files . . . 41
12.3 Enable Logging with Syslog . . . 42
12.4 Common errors . . . 43
12.4.1 Web Installation: “500 Internal Server Error” . . . 43
12.4.2 Errors When Accessing the Registration Server . . . 43
12.4.3 Errors When Accessing Docker . . . 43

13 Release Notes - Version 1.0 **45**
13.1 Key features and changes . . . 45
13.2 Change Log - Version 1.0 . . . 45
13.2.1 1.0.9 (2017-02-10) . . . 45
13.2.2 1.0.8 (2017-02-07) . . . 45
13.2.3 1.0.7 (2016-11-10) . . . 45
13.2.4 1.0.6 (2016-07-11) . . . 46
13.2.5 1.0.5 (2016-02-16) . . . 47
13.2.6 1.0.4 (2016-02-09) . . . 47
13.2.7 1.0.3 (2016-02-02) . . . 47
13.2.8 1.0.2 (2015-12-07) . . . 47
13.2.9 1.0.1 (2015-10-27) . . . 48
13.2.10 1.0 (2015-10-08) . . . 48

14 Appendix **49**
14.1 Abbreviations . . . 49

15 Document History **51**

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 provides browser-based access to a TeamDrive user account. Users can login to the Web Portal with their TeamDrive credentials and access the data they have stored in TeamDrive.

In order to provide this service, the Web Portal must have access to the user's data. As a result, it is common practice for companies to setup a Web Portal for their own users.

Due to the obvious security issues, access for the users of a particular Provider to a Web Portal must be explicitly activated on the Registration Server. How to do this is explained in associate_portal_provider.

This manual will guide you through the installation of your own local Web Portal for TeamDrive. This document is intended for administrators who need to install and configure a TeamDrive Web Portal.

Warning: The TeamDrive Web Portal installation requires a running TeamDrive Registration Server instance. If you are setting up both components on your own premises, please start with setting up the Registration Server as outlined in the TeamDrive Registration Server installation guides. If you are using a Registration Server instance hosted by some other service provider, make sure you can access it and you have performed an initial setup/configuration already.

3.1 Required Skills

When installing the TeamDrive Web Portal, we assume that you have basic knowledge of:

- VMware: importing and deploying virtual machines, configuring virtual networking and storage (when using a pre-installed Virtual Appliance)
- **Linux system administration:**
  - Adding/configuring software packages
  - Editing configurations files
  - Starting/stopping services
  - Creating user accounts
  - Assigning file ownerships and privileges
  - Creating and mounting file systems
  - Setting up environment variables
- Apache web server: installation and configuration, adding and enabling modules, modifying configuration files
- MySQL Database: installation and configuration, administration/maintenance, using the MySQL command line client, basic SQL
- Basic knowledge of application server technology

3.2 Operating System Requirements

We recommend using a recent 64-bit version of **Red Hat Enterprise Linux 7** (RHEL 7) or a derivative distribution like **CentOS 7**, **Oracle Linux 7** or **Scientific Linux 7** as the operating system platform.

This document is written with this OS environment in mind — the names of packages, configuration files and path names might be different on other Linux distributions. If you have any questions about using other Linux distributions, please contact sales@teamdrive.net .

You will need at least Apache HTTP Server version 2.4 which should be configured using the "prefork" MPM (http://httpd.apache.org/docs/2.2/mod/prefork.html). The prefork option is more scalable under load than the worker option and is usually the default configuration on Linux distributions.

In addition, the TeamDrive Web Portal requires the Yvva Runtime Environment version 1.3 or later, and a MySQL Database Server version 5.6 or later.

3.3 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.

3.3.1 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.

3.3.2 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.

3.3.3 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

3.3.4 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.

CHAPTER

FOUR

INTRODUCTION TO THE TEAMDRIVE WEB PORTAL

4.1 TeamDrive Web Portal Overview

The TeamDrive Web Portal consists of a number of components.

Firstly, the TeamDrive Web browser interface (ie. the TeamDrive Client interface that runs in a browser) is served by Apache.

The TeamDrive Web Portal Administration Console and the Web Portal authentication API is served dynamically by the Yvva Apache module `mod_yvva`.

A list of Docker containers and other administrative information is stored in a Management MySQL Database called `webportal`. This database must be accessible by all components of the Web Portal.

In addition, a Docker-based environment runs the TeamDrive Agents which serve the TeamDrive browser interface. A TeamDrive Agent is a faceless TeamDrive Client which provides a HTTP-based Rest API for the purpose of accessing a TeamDrive user account.

Depending on the scale of an installation, all components: Apache, MySQL and Docker may run on one machine or on separate machines. Docker itself may run on a cluster of machine, however setting up such a configuration is not part of this documentation.

4.2 TeamDrive Hosting Basics

Note: The system variables mentioned in this section are set using the Administration Console explained in system_settings.

A TeamDrive Web Portal requires a unique domain name. The domain name is basically the URL for the TeamDrive users that access the Web Portal. This domain name is stored in the `WebPortalDomain` system setting.

The same domain name is also used to access the Administration Console by adding `/admin/` to the base URL:

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

Once the TeamDrive Web interface has been served, further calls from the browser will be redirected to the appropriate TeamDrive Agent running in a Docker container. In order to do this, an Apache rewrite rule is installed which allows Apache to act as a reverse proxy, forwarding calls to the TeamDrive Agent.

If your setup uses a load balancer before the Apache instance, then it may be possible to have the load balance perform the redirect instead of first sending the message to Apache. The Apache rewrite rules that perform this task are the following:

```
RewriteRule "^/agent-([0-9]*)/(.*)" "http://127.0.0.1:$1/$2" [P]
ProxyPassReverse "/" "http://127.0.0.1/"
```

`127.0.0.1` must be replaced by the IP address of the Docker host.

Check the Apache documentation for a description of what these rules do in order to implement an equivalent transformation using your load balancer.

4.3 Docker Configuration

As mentioned above, the Docker system is responsible for running multiple TeamDrive Agent instances in containers. A container with a agent is created for each user session.

The users data is not stored in the container itself. Instead, the container mounts a directory in the host machines file system.

The root mount point for all containers is `\teamdrive\` by default. This path is stored in the `ContainerRoot` system setting. The username of the user is added to this path to produce the mount point for each individual container. For example the user for user "td_user_1" is `\teamdrive\td_user_1`.

Under this directory, the TeamDrive agent stores the "meta data" (file names and directory structure) of the Spaces that have been entered, as well as a disk cache for any files in transit.

Note: The Space data stored by the TeamDrive Agents is stored in unencrypted form. For this reason, security of the Docker host system is extremely important.

4.4 Background Tasks Performed by `td-webportal`

The `td-webportal` process is a service that executes background tasks scheduled by the Web Portal.

It uses the Yvva daemon `yvvad` to run the following background tasks at a definable regular interval:

- **Remove Idle Containers**:

  The purpose of this task is to remove containers that are no longer being used.

  When a user session times out, the container running the associated TeamDrive Agent exits (stops executing). When this happens the container is not removed. It remains in the system and is simpley restarted when the user logs in again.

  This task removes containers that are unused for a certain amount of time (indicated by the `IdleContainerTimeout`). This period should be longer than the regular user session timeout.

  Containers that are removed are automatically recreated by the Web Portal when the user logs in again. The only difference is that login process takes a little bit longer because the container must be created and then started, instead of just being restarted if the container already exists.

- **Delete Container Storage**:

  This task removes container data if a container is unused for a certain period of time (as specified by the `ContainerStorageTimeout` setting. The container data is the data stored under the `ContainerRoot` directory for a particular container, for example: the directory `\teamdrive\td_user_1` for the user "td_user_1".

  The purpose of the task is to free up unused disk space.

  If a user logs in again after the container data has been deleted the user will find that all of his Spaces have been set to "Inactive". This means that he has to enter a Space again in order to access the data. Since this could inconvenient and time consuming the `ContainerStorageTimeout` should be set to a fairly large period, for example 1 month.

- **Remove Old Images**:

The purpose of this task is to remove containers so that the TeamDrive Agent version used by the Web Portal can be upgraded.

The TeamDrive Agent running in a container is never updated "in place". Instead, the Web Portal waits for a container to be removed, and then the new TeamDrive Agent version is used when a new container is created.

This task specifically removes containers that are running an old TeamDrive Agent image. The current (and new) TeamDrive Agent image to be used is specified using the `ContainerImage` setting.

There are a number of settings which control the behaviour of this task: `RemoveOldImages`, `OldImageTimeout` and `OldImageRemovalTime`.

`RemoveOldImages` must be to True to enable this task. `OldImageTimeout` is the time, in seconds, that a container with an old image must be idle before it is removed. Zero means the container is removed, even if it is running. `OldImageRemovalTime` is used to specify when containers with old images should be removed. You can set it to "now", to remove the containers immediately, if set to "never", then containers are only removed if the OldImageTimeout is exceeded. This setting value can also be set to a time (e.g. 03:00, format: hh:mm), or a date (format YYYY-MM-DD hh:mm).

CHAPTER

FIVE

OPERATING SYSTEM CONFIGURATION

5.1 Installing a base operating system

Start by performing a minimal OS installation of a recent 64-bit Red Hat Enterprise Linux 7 (RHEL 7) or derivative Linux distribution (e.g. CentOS 7, Oracle Linux 7), using your preferred installation method (manual install, Kickstart, etc). The details of how to perform this task are out of the scope of this document.

For performing the installation, the system needs to be able to establish outgoing TCP connections (mainly to download additional components).

Boot up the system and log in as the root user, either via the console or via an SSH connection.

5.2 Enable Time Synchronization with NTP

We strongly advise that the clocks of all servers in a TeamDrive installation are synchronized using the Network Time Protocol (NTP). This can be achieved by installing the ntp package and enabling the NTP daemon:

```
[root@webportal install]# yum install ntp
[root@webportal install]# service ntpd start
[root@webportal install]# chkconfig ntpd on
```

Edit and update the configuration file `/etc/ntp.conf`, if necessary for your local environment.

5.3 Disable SELinux

The TeamDrive Web Portal currently can not be run when SELinux is enabled. Edit the file `/etc/selinux/config` and set `SELINUX=disabled`.

Reboot the system or change the SELinux enforcing mode at run time using the following command:

```
[root@webportal install]# setenforce 0
```

5.4 Firewall configuration

You should configure a local firewall so the server is protected against remote attacks. The only TCP ports that should be reachable from outside are 22 (SSH, optional for remote administration), 80 (http) and 443 (https).

On a minimal installation, you can install and use the text-based firewall configuration utility to enable access to the following services:

- SSH
- Secure WWW (HTTPS)

- WWW (HTTP)

To configure the firewall, you need to run:

```
[root@webportal install]# yum install system-config-firewall system-config-
↪firewall-tui newt-python
[root@webportal install]# system-config-firewall-tui
```

Follow the instructions to configure the firewall (in case of an error starting the firewall gui, reboot the machine). Enable additional protections based on your local requirements or security policies.

You can check the result with `iptables -L`:

```
[root@webportal ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state␣
↪RELATED,ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:
↪https
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-
↪prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-
↪prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

In case of using an external company firewall enable the above ports for the incoming traffic. For outgoing communication please enable:

- Secure WWW (Port 443 for HTTPS)
- WWW (Port 80 for HTTP)
- DNS Lookup (Port 53 for DNS communication with a public DNS server)

5.5 Installing the Postfix MTA (optional)

If you intend to use the email-based two-factor authentication for accessing the Web Portal Administration Console, or if you want to be notified about Space Volumes running out of disk space via email, the TeamDrive Web Portal needs to be configured to send out these notifications via SMTP.

The Yvva Runtime Environment that provides the foundation for the Web Portal is only capable of sending out email using plain SMTP via TCP port 25 to a local or remote MTA.

If your mail server requires some form of authentication or transport layer encryption like SSL/TLS, you need to set up a local MTA that relays all outgoing email from the TeamDrive Web Portal to your mail server using the appropriate protocol and credentials.

We recommend configuring a local Postfix instance to perform this duty. The following packages need to be installed:

```
[root@regserver ~]# yum install postfix mailx cyrus-sasl-plain
```

The detailed configuration of the local Postfix instance depends heavily on your local environment and how the remote MTA accepts remote submissions and is out of the scope of this document.

See the Postfix SMTP client documentation at http://www.postfix.org/smtp.8.html for details on how to configure Postfix to use a relay server and make sure to test the correct operation by sending local emails using the `mail` command line utility and watching the Postfix log file `/var/log/maillog` for errors.

Once the Postfix service has been configured correctly, ensure that it will be started automatically upon system boot:

```
[root@regserver ~]# chkconfig postfix on
```

CHAPTER

SIX

INSTALLING THE WEB PORTAL COMPONENTS

6.1 Enable the TeamDrive Web Portal yum Repository

The TeamDrive Web Portal components are available in the form of RPM packages, hosted in a dedicated yum repository. This makes the installation and applying of future updates of the software very easy — you can simply run yum update to keep your Web Portal software up to date.

To enable the repository, you need to download the td-webportal.repo file and place it into the directory /etc/yum.repos.d/, e.g. by using wget:

```
[root@webportal ~]# wget -O /etc/yum.repos.d/td-webportal.repo \
http://repo.teamdrive.net/td-webportal.repo
```

This will enable the "TeamDrive Web Portal Version 1.0.9" repository, which you can check by running yum repolist afterwards:

```
[root@webportal ~]# yum repolist
Loaded plugins: security
repo id                                repo name                                    status
td-webportal-1.0.9/7/x86_64              TeamDrive Web Portal Version 1.0.9              11
base/7/x86_64                          CentOS-7 - Base                              9,363
extras/7/x86_64                        CentOS-7 - Extras                              263
updates/7/x86_64                       CentOS-7 - Updates                             807
repolist: 10,821
```

6.2 Download and Install the TeamDrive Web Portal Package

Note: In case of using a white label version of TeamDrive with own customized UI's, colors and logo, please step over to the next chapter *Download and Install a white label Web Portal Package* (page 18). Otherwise proceed with the standard installation in this chapter and skip the following chapter.

Perform the download and installation of the Web Portal installation RPM package using the yum package manager:

```
[root@webportal ~]# yum install td-webportal-clientui
```

The TeamDrive Web Portal Client UI depends on the TeamDrive Web Portal and the Yvva Runtime Environment version 1.3 or later to be installed and configured beside other required software components like the Apache Web-Server and Apache SSL module. They will be installed by yum as a dependency on td-webportal-clientui automatically.

Once the TeamDrive Web Portal software has been installed successfully, you can proceed with the initial configuration.

6.3 Download and Install a white label Web Portal Package

Request your white label tar archive for the white label Web Portal package. It includes:

- Your white label Web GUI Web Portal RPM
- Your white label TeamDrive Agent tar archive
- Your `DISTRIBUTOR` file
- `build.sh` script for creating the docker container
- `Dockerfile.in` configuration file for the container creation

Extract the tar using the command:

```
[root@webportal ~]# tar -xvf <tar-achiv-name>
```

and install the Web GUI RPM using the command (replace <white-label-name> and <build-id> with the values in your webgui-portal-*.rpm):

```
[root@webportal ~]# rpm -ivh webgui-portal-<white-label-name>-<build-id>.rpm
```

Proceed with the next steps in this documentation. The usage of the other files will be explained later in the Docker installation chapter.

6.4 Installing the Web Portal HTML Documentation (optional)

The documentation for the Web Portal (in HTML format) can be installed locally, so you can access it directly from the Web Portal (or any other host running an Apache HTTP Server).

To install the HTML Documentation, install the following package via `yum` from the "TeamDrive Web Portal" repository:

```
[root@webportal ~]# yum install td-webportal-doc-html
```

The HTML documents will be installed in directory `/var/www/html/td-webportal-doc`. From your web browser, open the following URL to access the documentation:

http://webportal.yourdomain.com/td-webportal-doc/

Note: This step is optional. If you leave the documentation installed when the Web Portal goes into production and is accessible from the public Internet, you should ensure to restrict access to this URL to trusted hosts or networks only. This can be achieved by adding the appropriate access control rules to the file `/etc/httpd/conf.d/td-webportal-doc.httpd.conf`.

CHAPTER

SEVEN

APACHE HTTP SERVER INSTALLATION AND CONFIGURATION

The Apache HTTP server and the `mod_ssl` Apache module should have already been installed as dependencies for the `td-webportal` RPM package. You can verify this with the following command:

```
[root@webportal ~]# yum install httpd mod_ssl
Setting up Install Process
Package httpd-2.2.15-30.0.1.el6_5.x86_64 already installed and latest version
Package 1:mod_ssl-2.2.15-30.0.1.el6_5.x86_64 already installed and latest version
Nothing to do
```

7.1 Update `httpd.conf`

Open the web server configuration file `/etc/httpd/conf/httpd.conf` in a text editor to change the following parameters:

```
KeepAlive On
KeepAliveTimeout 2
ServerName <Your ServerName>
```

For security reasons, we also advise to disable the so-called "Server Signature" - a feature that adds a line containing the server version and virtual host name to server-generated pages (e.g. internal error documents, FTP directory listings, etc):

```
ServerSignature Off
```

By default, the server version and operating system is also displayed in the `Server` response header field, e.g. `Server: Apache/2.2.15 (CentOS)`. To suppress this output, we suggest updating the `ServerTokens` option as follows:

```
ServerTokens Prod
```

7.2 Disable Unneeded Apache Modules

The TeamDrive Web Portal only requires a few Apache modules to be enabled. To reduce the memory footprint, please deactivate unnecessary modules in the apache configuration.

7.2.1 Apache 2.4

In the directory: `/etc/httpd/conf.modules.d` comment out all modules in the following config files. Using the linux stream editor (sed) with the following regular expression will add a '#' comment sign in each line starting with 'LoadModule':

```
sed -e '/LoadModule/ s/^#*/#/' -i /etc/httpd/conf.modules.d/00-dav.conf
sed -e '/LoadModule/ s/^#*/#/' -i /etc/httpd/conf.modules.d/00-lua.conf
sed -e '/LoadModule/ s/^#*/#/' -i /etc/httpd/conf.modules.d/00-proxy.conf
sed -e '/LoadModule/ s/^#*/#/' -i /etc/httpd/conf.modules.d/01-cgi.conf
```

Edit `/etc/httpd/conf.modules.d/00-proxy.conf` and enable these modules by removing the comment '#' in from of each line:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
```

Edit `/etc/httpd/conf.modules.d/00-base.conf` and leave only the following modules enabled by adding a '#' comment in front of all other modules:

```
LoadModule actions_module modules/mod_actions.so
LoadModule alias_module modules/mod_alias.so
LoadModule authz_core_module modules/mod_authz_core.so
LoadModule autoindex_module modules/mod_autoindex.so
LoadModule headers_module modules/mod_headers.so
LoadModule log_config_module modules/mod_log_config.so
LoadModule mime_module modules/mod_mime.so
LoadModule rewrite_module modules/mod_rewrite.so
LoadModule setenvif_module modules/mod_setenvif.so
LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
LoadModule unixd_module modules/mod_unixd.so
LoadModule version_module modules/mod_version.so
```

7.3 Configure `mod_ssl`

The web-based TeamDrive Web Portal Administration Console should be accessed via an encrypted SSL connection. To facilitate this, add the following to the end of the default `<VirtualHost>` section in `/etc/httpd/conf.d/ssl.conf`:

```
Include conf.d/td-webportal.httpd.conf.ssl
</VirtualHost>
```

Note: The Apache HTTP Server package includes a self-signed SSL certificate for testing purposes. If you connect to the server using a web browser, it will likely raise an error about an untrusted/insecure connection. You should consider replacing this certificate with an appropriate one.

Follow the instructions provided by your certificate authority on how to obtain and install an SSL certificate for the Apache HTTP Server.

Verify your SSL configuration using the service from SSL Labs: `https://www.ssllabs.com/ssltest/analyze.html` and make sure that the "Handshake Simulation" is working for current platforms and browser. The following ssl parameters for the apache web server will create an A-rating and make sure that the handshake is working for current platforms and browser:

```
SSLProtocol all -SSLv2 -SSLv3

SSLHonorCipherOrder on

SSLCipherSuite ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:
↪ECDH+3DES:DH+3DES:RSA+AESGCM:RSA+AES:RSA+3DES:!aNULL:!MD5:!DSS
```

Add DOCKER_HOST environment variable to the bottom of the `/etc/sysconfig/httpd` file:

```
DOCKER_HOST=127.0.0.1
```

Replace “127.0.0.1” with the IP address of the Docker container host if the Docker host machine is not the same as the Web Portal.

As the comment indicates, the IP address “127.0.0.1” must be replaced with IP address or host name of the Docker host. This is the same value as the domain name in the `DockerHost` setting.

If the Docker host machine is the same as the Web Portal, then the re-write rules containing “127.0.0.1” must not be changed.

CHAPTER

EIGHT

MYSQL INSTALLATION AND CONFIGURATION

8.1 Installing MySQL Server

The TeamDrive Web Portal requires a MySQL database to store its information. This document assumes that the MySQL instance runs on the same host as the Web Portal itself, connecting to it via the local socket file.

Alternatively, it's possible to use an external MySQL Server. In this case, you need to make sure that this external MySQL instance is reachable via TCP from the Web Portal (usually via TCP port 3306) and that the `teamdrive` MySQL user account is defined correctly (e.g. the MySQL username in the remote database would become `teamdrive@webportal.yourdomain.com` instead of `teamdrive@localhost`).

Most MySQL installations usually do not allow the `root` user to log in from a remote host. In this case the installation script is unable to create the dedicated `teamdrive` user automatically and you need to perform this step manually before performing the installation of the TeamDrive Web Portal databases.

Especially the correct definition of the host part is critical, as MySQL considers `username@webportal` and `username@webportal.yourdomain.com` as two different user accounts.

Note: Since CentOS 7, MySQL is no longer in CentOS's repositories and MariaDB has become the default database system offered. We recommend instsalling the mysql community server instead. If you are installing on CentOS 7 then perform the following steps:

```
[root@webportal ~]# yum update
[root@webportal ~]# wget http://repo.mysql.com/mysql-community-release-el7-5.
↪noarch.rpm
[root@webportal ~]# rpm -ivh mysql-community-release-el7-5.noarch.rpm
[root@webportal ~]# yum update
```

To set up the Web Portal using a local MySQL Database, install the MySQL Client and Server packages:

```
[root@webportal ~]# yum install mysql mysql-server
```

For reliability and performance reasons, we recommend placing the MySQL data directory `/var/lib/mysql` on a dedicated file system or storage volume.

Please start the MySQL server, run the secure installation script and follow the recommendations. Make sure to create a password for the MySQL `root` user and take note of it:

```
[root@webportal ~ ]# service mysqld start
Initializing MySQL database:  Installing MySQL system tables...
OK
Filling help tables...
OK

To start mysqld at boot time you have to copy
support-files/mysql.server to the right place for your system
```

```
PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
To do so, start the server, then issue the following commands:

/usr/bin/mysqladmin -u root password 'new-password'
/usr/bin/mysqladmin -u root -h hostinstalltest.local password 'new-password'

Alternatively you can run:
/usr/bin/mysql_secure_installation

which will also give you the option of removing the test
databases and anonymous user created by default.  This is
strongly recommended for production servers.

See the manual for more instructions.

You can start the MySQL daemon with:
cd /usr ; /usr/bin/mysqld_safe &

You can test the MySQL daemon with mysql-test-run.pl
cd /usr/mysql-test ; perl mysql-test-run.pl

Please report any problems with the /usr/bin/mysqlbug script!

                                                          [  OK  ]
Starting mysqld:                                          [  OK  ]
```

Run the secure installation script and follow the recommendations. Make sure to create a password for the MySQL `root` user and take note of it:

```
[root@webportal ~ ]# mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MySQL to secure it, we'll need the current
password for the root user.  If you've just installed MySQL, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none): <Enter>
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MySQL
root user without the proper authorisation.

Set root password? [Y/n] <y>
New password: <mysql_root_pw>
Re-enter new password: <mysql_root_pw>
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MySQL installation has an anonymous user, allowing anyone
to log into MySQL without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] <Enter>
... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
```

```
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] <Enter>
... Success!

By default, MySQL comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] <Enter>
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] <Enter>
... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MySQL
installation should now be secure.

Thanks for using MySQL!
```

MySQL is now up and running and you can proceed with creating the `teamdrive` user and the MySQL databases required for the TeamDrive Host Server.

8.2 Creating TeamDrive MySQL User and Databases

The TeamDrive Web Portal requires the MySQL databases `webportal`, which will be accessed using a dedicated `teamdrive` MySQL user.

The Web Portal installation package ships with a `mysql_install.sh` script that performs these required configuration steps:

- Modify the local configuration file `/etc/my.cnf`, start and enable MySQL Server at system bootup (only when using a local MySQL Server)
- Create the MySQL user account `teamdrive`, assign the provided password and assign the necessary database privileges (requires access to the MySQL `root` account)
- Create the required Web Portal MySQL database
- Modify the local Web Portal configuration file `/etc/td-webportal.my.cnf`

The following example demonstrates how to configure the MySQL database using the `mysql_install.sh` script, it assumes that the MySQL database is located on the same system where the TeamDrive Web Portal instance is installed.

You need to have the following information available:

- The password of the MySQL `root` user account you defined while running `mysql_secure_installation`
- The password that you want to assign to the `teamdrive` user

The script is part of the `td-webportal` package and is installed in `/opt/teamdrive/webportal/mysql/mysql_install.sh`. Call it as the `root` user and follow the instructions:

```
[root@webportal ~]# /opt/teamdrive/webportal/mysql/mysql_install.sh

TeamDrive Web Portal MySQL Database Install Script
--------------------------------------------------

Configuring MySQL database for TeamDrive Web Portal
version |release|

This script will perform the following steps:

 - Modify the local configuration file /etc/my.cnf,
   start and enable MySQL Server
   (only when MySQL Server runs locally)
 - Create the required MySQL user "teamdrive",
   assign the provided password and the required
   database privileges
   (requires access to the MySQL root account)
 - Create and populate the required Web Portal
   MySQL database
 - Modify the local Web Portal configuration file
   /etc/td-webportal.my.cnf

Enter MySQL hostname: localhost
Enter MySQL root password for localhost: <mysql_root_pw>
Enter MySQL password to be set for user teamdrive: <td_pw>

mysqld (pid  7490) is running...
Stopping mysqld:                                           [  OK  ]
Changing local MySQL Server configuration...
Backing up existing configuration file /etc/my.cnf...
`/etc/my.cnf' -> `/etc/my.cnf-2015-05-19-17:19.bak'
Starting and enabling MySQL Server...
Starting mysqld:                                           [  OK  ]
Trying to connect to the MySQL server as root...
+---------------+
| MySQL Version |
+---------------+
| 5.1.73        |
+---------------+
Creating teamdrive MySQL user on localhost
Trying to connect to the MySQL server as the teamdrive user...
Creating Web Portal databases...
Updating /etc/td-webportal.my.cnf...
Backing up existing configuration file ...
`/etc/td-webportal.my.cnf' -> `/etc/td-webportal.my.cnf-2015-05-19-17:19.bak'

Finished!
The MySQL configuration for TeamDrive Web Portal
version |release| is now complete.
```

The MySQL database is now properly configured and populated. As a final test, try logging into the MySQL database from the Web Portal system, using the `teamdrive` user account and the password you defined — you should be able to see and access the TeamDrive Web Portal databases:

```
[root@webportal ~]# mysql -u teamdrive -p<password>
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 51
Server version: 5.1.71 Source distribution

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
```

```
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| webportal          |
+--------------------+
2 rows in set (0.00 sec)

mysql> QUIT
Bye
```

CHAPTER

NINE

PRE-INSTALLATION TASKS

9.1 Mount the Space Storage Volume

The container root directory specified by the `ContainerRoot` setting contains the mount points for all the containers on the Docker system.

The container root (by default `/teamdrive`) is the mount point for a dedicated file system that provides the requirements outlined in chapter storage-requirements.

By default, the directory `/teamdrive` has already been created by the `td-webportal` RPM package. However, if the Docker host is not the same as the Web Portal machine, then you will have to create this directory yourself.

Note that due to restrictions of the Docker system, all data will be written to this directory as belonging to root.

Mount the file system and create the respective mount entry in `/etc/fstab` to enable automatic mounting of the file system at bootup. Please consult your Operating System documentation for details on how to perform this step.

9.2 Installing Docker

The Web Portal uses Docker containers to run the TeamDrive Agent. A container is started for each user that logs into the Web Portal.

The Docker containers can run on a machine or cluster that is separate from the Web Portal host which handles the login and manages the containers.

Docker can be found in the standard CentOS 7 repositories (CentOS 6 is not longer supported by Docker).

Use yum to install the package:

```
[root@webportal ~]# yum install docker
```

The Docker daemon can be started and stopped using `systemctl start docker` and `systemctl start docker`. Before starting docker the first time, configure the docker volume as described in storage-requirements.

By default, the Docker daemon is only accessible via a local socket. The Web Portal requires TCP connectivity. This is the case, even if Docker and the Web Portal are running on the same host.

To make Docker accessible via TCP add the setting `--host=tcp://0.0.0.0:2375` to the `OPTIONS` parameter in the `/etc/sysconfig/docker` file as follows:

```
OPTIONS="--host=tcp://0.0.0.0:2375 ..."
```

After restarting Docker, the Docker API will be available on port 2375.

On the client side (the Web Portal host) you will now need to set the `DOCKER_HOST` environment variable in order to use the `docker` command. Replace `localhost` below with the domain name of the Docker host:

```
[root@webportal ~]# export DOCKER_HOST=tcp://localhost:2375
[root@webportal ~]# docker images
```

To have this environment variable automatically set at the login, add the two lines to the `bash_profile` of the root user by executing:

```
[root@webportal ~]# echo DOCKER_HOST=tcp://localhost:2375 >> /root/.bash_profile
[root@webportal ~]# echo export DOCKER_HOST >> /root/.bash_profile
```

The domain name (and port if not 2375) of the Docker host is stored in the `DockerHost` system setting. This parameter is set during the activation process described later (see activate_web_portal).

9.2.1 Configure `direct-lvm` Mode

The `devicemapper` is the default Docker storage driver on CentOS. By default, the `devicemapper` uses the `loop-lvm` configuration mode. This is not recommended for production.

The preferred configuration for production deployments is `direct-lvm`. How to set this up is described in the Docker documentation:

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

9.3 Installing the TeamDrive Agent Docker Image

Note: In case of using a white label version of TeamDrive with own customized UI's, colors and logo, please step over to the next chapter *Creating a White Label Agent Docker Image* (page 30). Otherwise proceed with the following standard installation and skip the next chapter.

Docker container images are available from the TeamDrive public Docker repository on the docker hub. Here you will find a list of the tagged images that have been uploaded by TeamDrive:

```
https://hub.docker.com/r/teamdrive/agent/tags/
```

The current version of the Web Portal uses the image version with the `4.3.1.1656-TMDR` tag name.

Install this image on your Docker host using the following command:

```
[root@webportal ~]# docker pull teamdrive/agent:4.3.1.1656-TMDR
```

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.

9.4 Creating a White Label Agent Docker Image

As described in *Download and Install a white label Web Portal Package* (page 18) you will need the other files in your white label tar package now. Execute the command (replace <version-nr> with the current agent version number in the format 4.3.1.1656) to build your own docker image. As base system CentOS 7 will be used and downloaded from the docker hub during the build process:

```
[root@webportal ~]# ./build.sh <version-nr>
```

Please check the output from the script. You should see this message (if not, please check, that the DISTRIBUTOR file exists):

```
Custom DISTRIBUTOR file found. Replacing provider configuration in Image.
```

and later on (<version-nr> and <provider-code> are showing your current version and the provider code from the DISTRIBUTOR file):

```
Building Docker image teamdrive/agent:<version-nr>-<provider-code>...
```

The last necessary customization step will be done after the Web Portal activation is done.

9.5 Installing SSL certificates

The default Apache HTTP Server installation ships with self-signed SSL certificates for testing purposes. We strongly recommend to purchase and install proper SSL certificates and keys and to adjust the configuration in file `/etc/httpd/conf.d/ssl.conf` accordingly before moving the server into production.

The exact installation process depends on how you obtain or create the SSL key and certificate, please refer to the respective installation instructions provided by your certificate issuer.

9.6 Starting the Web Portal

After all configuration steps have been performed, we can start the TeamDrive Web Portal to conclude the initial installation/configuration.

9.6.1 Starting `td-webportal`

To activate the `yvvad`-based `td-webportal` background task you have to start the service using the provided init script.

The configuration file `/etc/td-hosting.conf` defines how this process is run. You usually don't have to modify these settings.

To start the `td-webportal` program, use the `service` command as user root:

```
[root@webportal ~]# service td-webportal start
Starting TeamDrive Web Portal:                          [  OK  ]
```

Use the `status` option to the `service` command to verify that the service has started:

```
[root@webportal ~]# service td-webportal status
yvvad (pid  2506) is running...
```

If `td-webportal` does not start (process `yvvad` is not running), check the log file `/var/log/td-webportal.log` for errors. See chapter Troubleshooting for details.

9.6.2 Starting the Apache HTTP Server

Now the Apache HTTP Server can be started, which provides the TeamDrive Web Portal functionality via `mod_yvva`.

You can start the service manually using the following command:

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

Warning: At this point, the Web Portal's web server is answering incoming requests from any web client that can connect to its address. For security purposes, you should not make it accessible from the public Internet until you have concluded the initial configuration, e.g. by blocking external accesses using a firewall.

Check the log file `/var/log/httpd/error_log` and `/var/log/td-webportal.log` for startup messages and possible errors:

```
[notice] Apache/2.2.15 (Unix) mod_ssl/2.2.15 OpenSSL/1.0.1e-fips configured
-- resuming normal operations
[notice] mod_yvva 1.3.1 (Jan 15 2016 12:56:45) loaded
[notice] Logging (=error) to: /var/log/td-webportal.log
```

Please consult chapter troubleshooting if there is an error when starting the service.

CHAPTER

TEN

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.

10.1 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.

10.2 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 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:

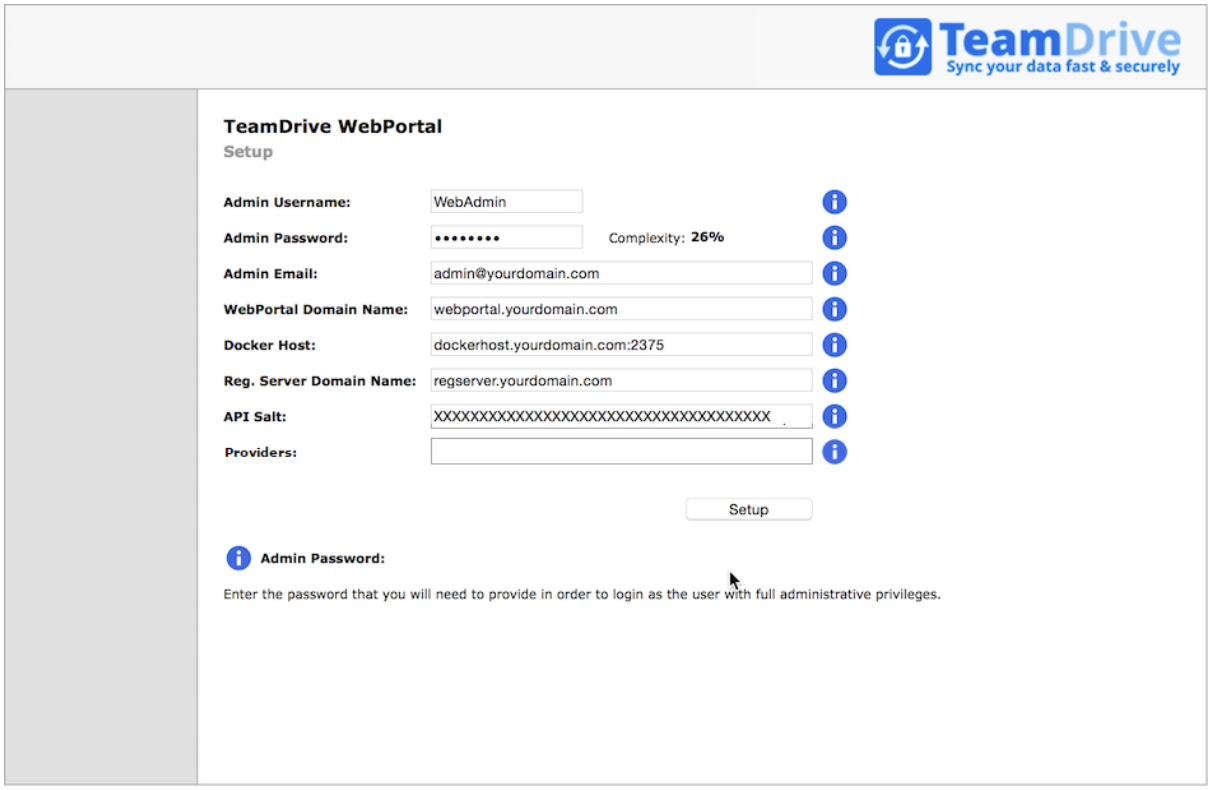

Fig. 10.1: Web Portal Setup Page

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.

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.

10.3 Setup and Administration

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

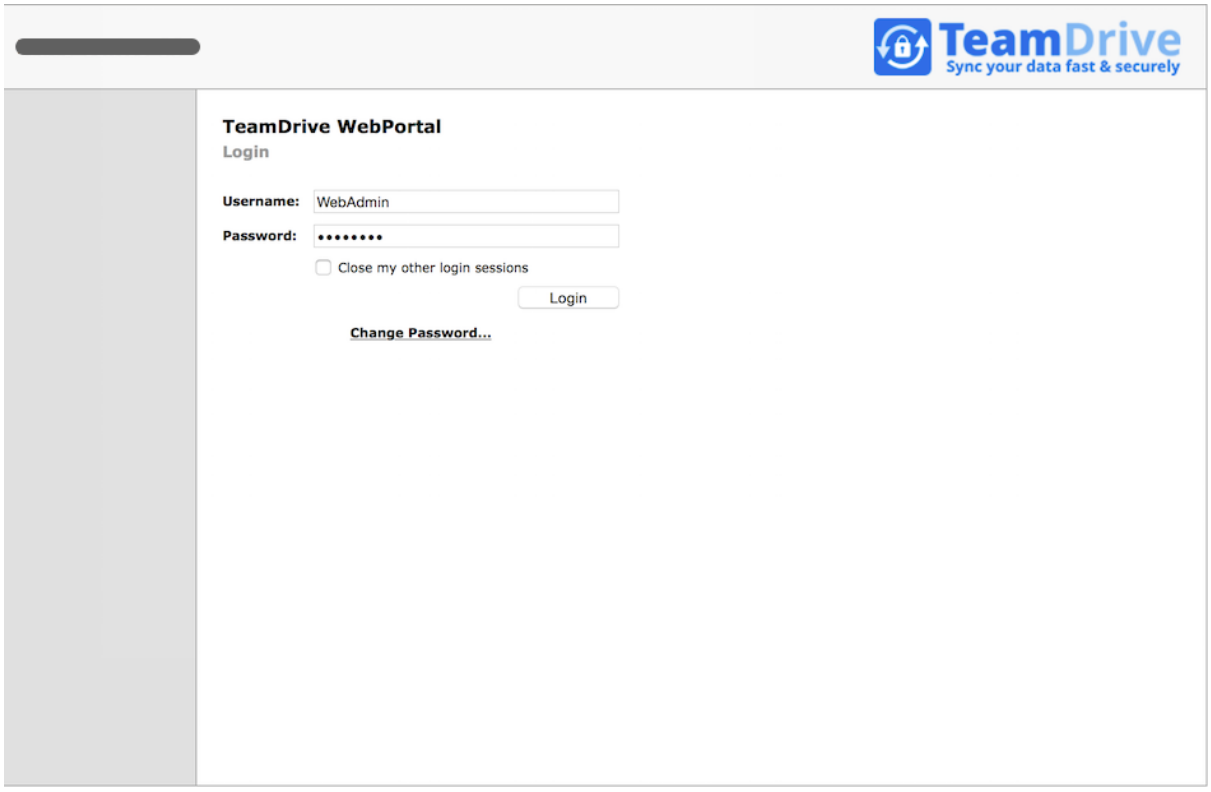

Fig. 10.2: Web Portal Admin Console: Login Screen

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.

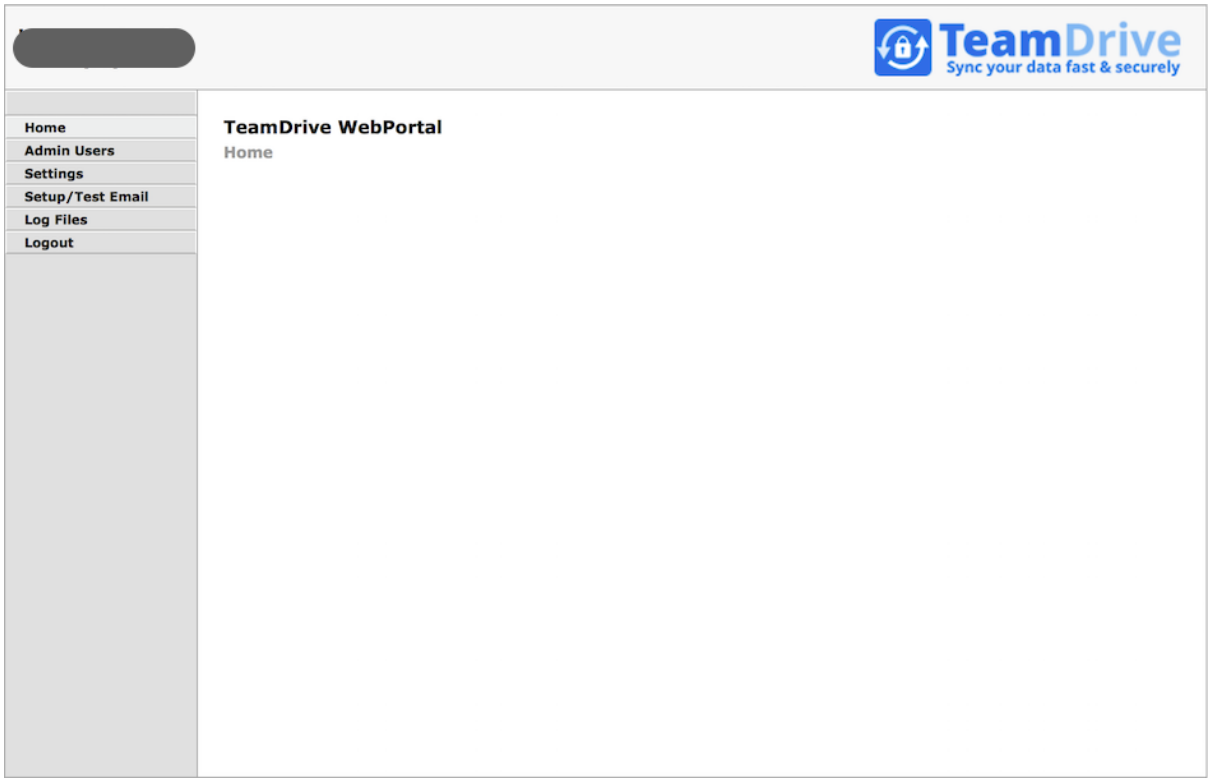

Fig. 10.3: Web Portal Admin Console: Home Screen

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.

10.4 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:<verison-nr>-TMDR` value with your `teamdrive/agent:<verison-nr>-<provider-code>` created docker image from the chapter *Creating a White Label Agent Docker Image* (page 30). After saving the value, restart the apache server using:

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

10.5 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

ELEVEN

POST-INSTALLATION TASKS

11.1 Startup Sequence / Dependencies

To ensure a proper service start and to minimize error messages during Web access, the following startup sequence of the TeamDrive Web Portal components and services should be observed.

1. Mount the Image data volume on the Docker host
2. Start the Docker service
3. Start the Web Portal MySQL database service
4. Start the `td-webportal` background service
5. Start the Apache HTTP Server

11.2 Starting the Apache HTTP Server at Boot Time

To ensure that Apache HTTP Server starts up automatically at system bootup time, use the following command to enable it:

```
[root@webportal ~]# chkconfig httpd on
```

11.3 Starting TeamDrive Service at Boot Time

To start the TeamDrive Web Portal background service `td-webportal` at boot time, use the following command to enable it:

```
[root@webportal ~]# chkconfig td-webportal on
```

11.4 Next steps

This concludes the basic installation and configuration of the TeamDrive Web Portal. Please consult the *TeamDrive Web Portal Administration Guide* for additional information on advanced administrative tasks and configuration steps.

CHAPTER

TWELVE

TROUBLESHOOTING

12.1 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.

12.2 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.

12.3 Enable Logging with Syslog

As outlined in list of relevant log files, 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
```

12.4 Common errors

12.4.1 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.

12.4.2 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.

12.4.3 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* (page 29).

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* (page 20).

CHAPTER

THIRTEEN

RELEASE NOTES - VERSION 1.0

13.1 Key features and changes

This is the initial release of the Web Portal.

13.2 Change Log - Version 1.0

13.2.1 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

13.2.2 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* (page 29) chapter.

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

13.2.3 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

13.2.4 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 *Apache 2.4* (page 19)

- 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`

13.2.5 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).

13.2.6 1.0.4 (2016-02-09)

- Framework synced with Host- and Reg-Server

13.2.7 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)

13.2.8 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

13.2.9 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.

13.2.10 1.0 (2015-10-08)

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

CHAPTER

FOURTEEN

APPENDIX

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 **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.

CHAPTER

FIFTEEN

DOCUMENT HISTORY

Date	Version	Name	Description
2015-08-07	1.0	Paul McCullagh	Start