Manual

Greenbone Cloud Service
for Virtual Managed Service Provider

Greenbone

Greenbone AG
Neumarkt 12
49074 Osnabrück
Germany
https://www.greenbone.net/en/

Status: January 11, 2024

This is the manual for the Greenbone Cloud Service. The Greenbone Cloud Service is under constant development. This manual attempts to always document the latest version. It is, however, possible that latest functionalities have not been captured in this manual. Should you have additional notes or error corrections for this manual, contact the Greenbone Enterprise Support (https://www.greenbone.net/en/technical-support/).

Contents

CHAPTER 1

Introduction

Vulnerability management is a core element in modern information technology (IT) compliance. IT compliance is defined as the adherence to legal, corporate and contractual rules and regulations related to IT infrastructures. Within its context IT compliance mainly relates to information security, availability, storage and privacy. Companies and agencies have to comply with many legal obligations in this area.

Controlling and improving IT security is an ongoing process consisting of at least the following steps:

- Discovery of the current state
- Improving the current state
- Reviewing the taken measures

The Greenbone Cloud Service assists companies and agencies with automated and integrated vulnerability assessment and management. Its task is to discover vulnerabilities and security gaps before potential cyber criminals do.

The Greenbone Cloud Service achieves this through different perspectives of an attacker:

External The Greenbone Cloud Service can simulate an external attack on the network to identify outdated or misconfigured firewalls.

Demilitarized Zone (DMZ) The Greenbone Cloud Service can identify actual vulnerabilities that may be exploited by attackers that get past the firewall.

Internal The Greenbone Cloud Service can also identify exploitable vulnerabilities in the internal network, for example those targeted by social engineering or computer worms. Due to the potential impact of such attacks, this perspective is particularly important for the security of any IT infrastructure.

For DMZ and internal scans, a distinction can be made between authenticated and unauthenticated scans. When performing an authenticated scan, the Greenbone Cloud Service uses credentials and can discover vulnerabilities in applications that are not running as a service but have a high risk potential. This includes web browsers, office applications or PDF viewers.

Due to new vulnerabilities being discovered on a daily basis, regular updates and testing of systems are required. The Greenbone Enterprise Feed ensures that the Greenbone Cloud Service is provided with the latest testing routines and can discover the latest vulnerabilities reliably. Greenbone analyzes CVE[1] messages

[1] The Common Vulnerability and Exposures (CVE) project is a vendor neutral forum for the identification and publication of new vulnerabilities.

and security bulletins of vendors and develops new vulnerability tests daily.

When performing a vulnerability scan using the Greenbone Cloud Service, the personnel responsible will receive a list of vulnerabilities that have been identified in the target systems. For the selection of remediation measures a prioritization is required. The most important measures are those that protect the system against critical risks and eliminate the corresponding security holes.

The Greenbone Cloud Service utilizes the Common Vulnerability Scoring System (CVSS). CVSS is an industry standard for the classification and rating of vulnerabilities. It assists in prioritizing the remediation measures.

Fundamentally, there are two options to deal with vulnerabilities:

- Eliminating the vulnerability by updating the software, removing the component or changing the configuration.
- Implementing a rule in a firewall or a intrusion prevention system (virtual patching).

  Virtual patching is the apparent elimination of the vulnerability through a compensating control. The real vulnerability still exists and the attacker can still exploit the vulnerability if the compensating control fails or if an alternate approach is used.

An actual patch or update of the affected software is always preferred over virtual patching.

The Greenbone Cloud Service also supports the testing of the implemented remediation measures. With its help responsible personnel can document the current state of IT security, recognize changes and record these changes in reports.

CHAPTER 2

Getting an Overview

2.1 Dashboard

The dashboard is displayed when logging in to the platform (see Fig. 2.1).

The following information is displayed:

Average purchase price per IP address Average price per IP address that is paid to the MSP.

Billing Method Selected Number of subscriptions by respective category:

- Free
- MSP: managed-service customers, i.e., the subscription is managed by the vMSP
- Self Service: self-service customers, i.e., customers are able to manage the subscription on their own
- Project: project keys with special conditions

Total IP's Total number of all (internal and external) IP addresses sold to all end customers.

External Number of external IP addresses sold to all end customers.

Internal Number of internal IP addresses sold to all end customers.

Total Purchase Total amount of money that is paid to the MSP.

Income Selfservice Amount of money received from customers in self-service mode.

Monthly billing data Download the proof of performance for checking the number of bought/sold IP addresses and the amount that must be paid to the MSP.

Development within 6 months Development of number of sold IP addresses over the last 6 months, divided into internal and external IP addresses.

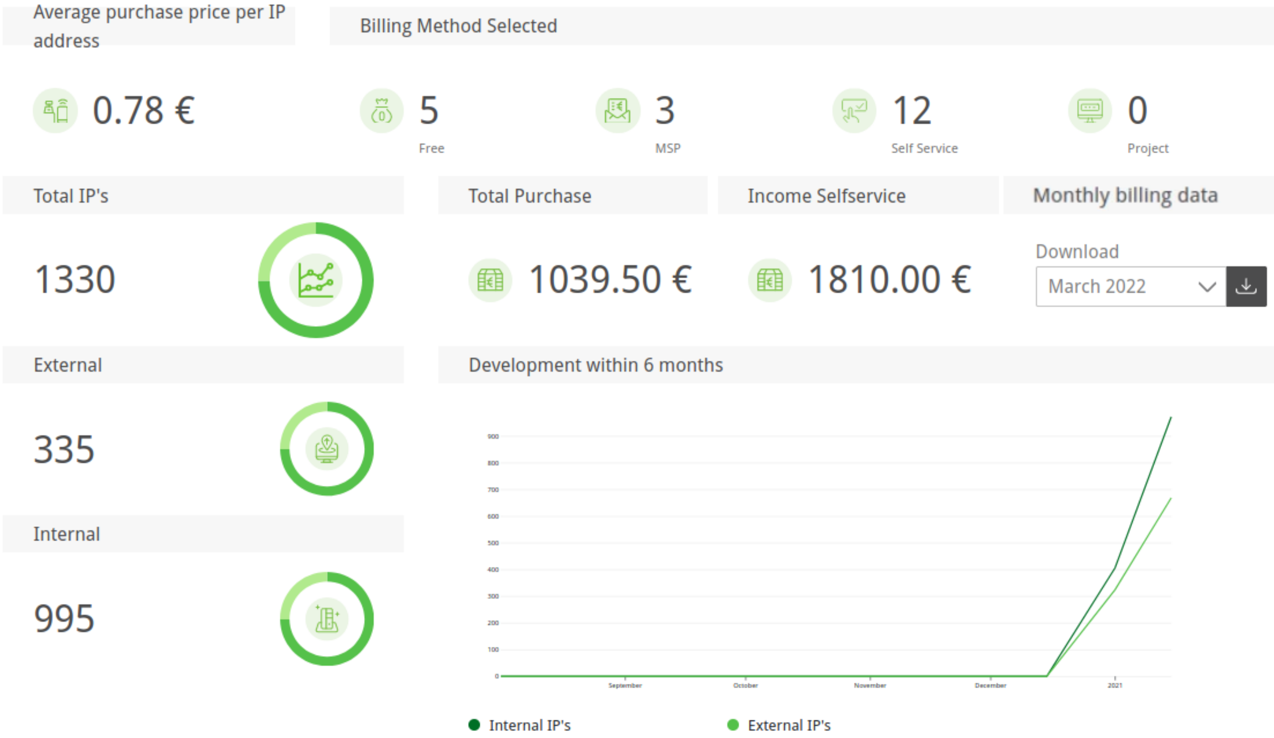

Fig. 2.1: Overview dashboard

2.2 Managed Security

Managed-service customers, i.e., customers whose subscription is managed by the vMSP, can grant the vMSP access to some report data or full access ("Managed Security").

Clicking *Managed Security* in the menu panel provides a list of customers who have granted access. The table displays the customer's number of tasks and the number of severities for each severity class.

The following actions are available:

- If the end customer grants access to the reporting, is displayed in the column *Actions*. Clicking provides detailed information like the severity trend and a full list of tasks.
- If the end customer grants full access, ⋮ is displayed in the column *Actions*. When clicking ⋮, either (see above) or the jump-in feature for accessing the end-customer interface can be selected.

Jump-In Feature

The end-customer interface can be accessed using the *Jump-In* feature:

1. Select *Managed Security* in the menu panel.
2. In the row of the customer, click ⋮ and select *Jump-In* (see Fig. 2.2).

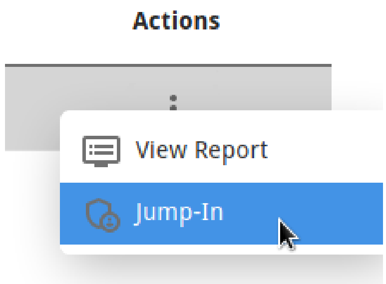

Fig. 2.2: Accessing the end-customer interface

3. Enter the password used for logging in to the vMSP interface.
4. Click *Jump*.

   → The end-customer interface is opened.

CHAPTER 3

Managing Customers

All customers can be displayed by selecting *Billing* in the menu panel.

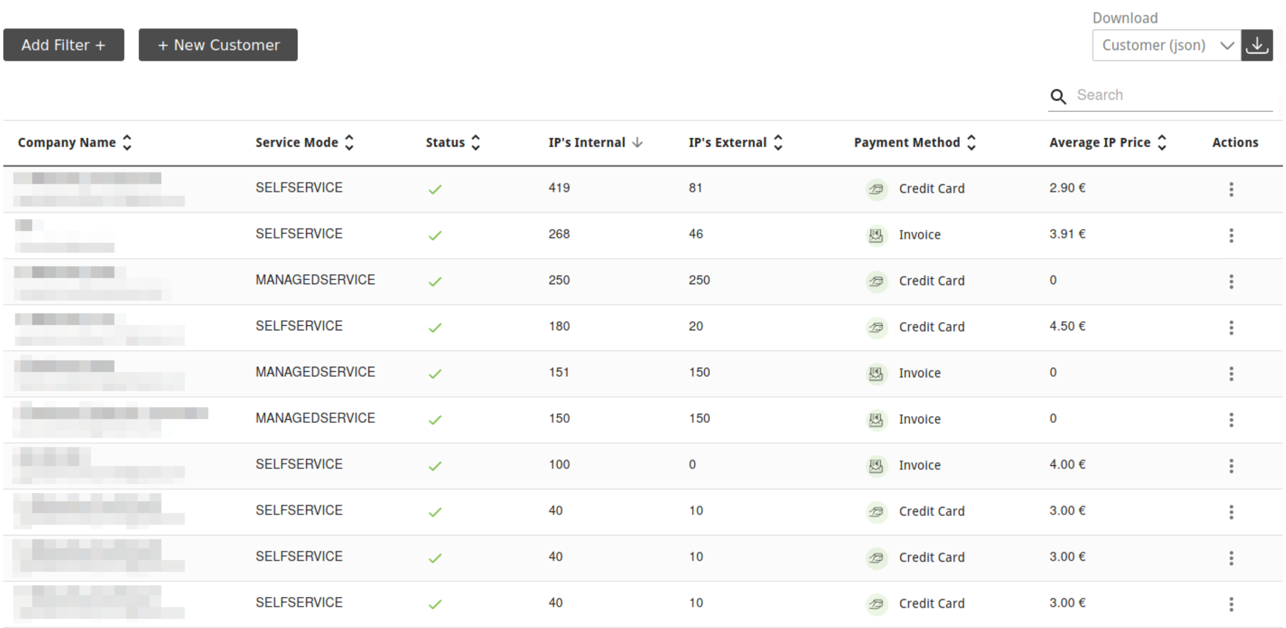

Fig. 3.1: Page *Customers*

For all customers the following information is displayed:

Company Name Name of the customer's company and e-mail address of the company's contact person.

Service Mode Service mode that is used by the customer: managed-service or self-service.

- Managed-service customers are not able to manage the subscription on their own, i.e., change the IP address count and distribution. This setting has to be done by the vMSP.
- Self-service customers are able to manage the subscription on their own (see Chapter *3.5* (page 19)).

Status Status of the customer (active or inactive).

- The customer has an active subscription.
- The customer has no active subscription (see Chapter *3.2.4* (page 16)).
- The customer has been created but did not register yet.
- The customer account is locked. The customer is not able to log in (see Chapter *3.2.3* (page 15)).

IP's Internal Number of internal IP addresses that can be scanned with the customer's current subscription.

IP's External Number of external IP addresses that can be scanned with the customer's current subscription.

Payment Method Used payment method (see Chapter *3.6* (page 20)).

Average IP Price Average price the customer pays per IP address.

For all customers the following actions are available when clicking :

- Convert a self-service customer account to a managed-service customer account (only available for self-service customers, see Chapter *3.2.1* (page 13)).
- Change the IP address count and distribution of the customer account (see Chapter *3.2.2* (page 13)).
- Resend invite e-mail to a new customer (only available for customers who have been invited but did not register yet).
- Display detailed information about the customer account. In the overlay, all subscriptions of the customer account are displayed and there are options to activate/deactivat the customer account (see Chapter *3.2.3* (page 15)) or to cancel the subscription (see Chapter *3.2.4* (page 16)).
- Add a project key (only available for managed-service customers, see Chapter *3.2.6* (page 16)).
- Edit the address data of the customer account (only available for managed-service customers, see Chapter *3.2.7* (page 17)).
- Change the main user of the customer account (see Chapter *3.2.8* (page 17)).
- Delete the customer account (see Chapter *3.2.9* (page 18)).

3.1 Creating a Customer Account

Note: New customers are invited by sending an invite e-mail. The e-mail can only be sent if the mail server is configured correctly (see Chapter *5.2.1* (page 25)).

When a customer account is created, the main user for whom the account is initially created can invite other users to their team. All users of a team are operating with the same permissions and use the subscription of the main user.

New customer accounts can be created as follows:

1. Select *Billing* in the menu panel.
2. Click *+ New Customer*.
3. Enter the contact data of the customer's company in the respective input boxes.

4. Enter the name and the e-mail address of the customer's contact person in the respective input boxes.

   Note: The e-mail address of the contact person is also the user name that the customer uses to log in.

5. Click *Create*.

   → An invite e-mail is sent to the new customer.

   The new customer is displayed in the table on the page *Customers* with the status ✉.

   If the customer accepts the invite, they can register by defining a new password and log in using the e-mail address defined in step 4 and the newly created password.

Note: The invite expires after 24 hours.

If a customer does not receive the e-mail or the invite has expired, the e-mail can be resend by clicking ⋮ and selecting ✉ in the column *Actions*.

3.2 Editing a Customer

3.2.1 Converting a Self-Service Customer into a Managed-Service Customer

A self-service customer can be converted into a managed-service customer as follows:

1. Select *Billing* in the menu panel.
2. In the row of the customer, click ⋮ and select *Convert to Managed Customer*.

   Note: This change cannot be undone. Managed-service customers cannot be converted into self-service customers.

3. Click *Confirm*.

   → The customer is converted into a managed-service customer.

3.2.2 Changing the IP Address Count and Distribution of a Customer

The IP address count and distribution of a customer can be changed as follows:

1. Select *Billing* in the menu panel.
2. In the row of the customer, click ⋮ and select ⇄ *IP Distribution*.
3. Enter the desired total number of IP addresses (sum of external and internal) in the input box *Total IP's* (see Fig. 3.2).
4. Move the slider to distribute the total number between internal and external IP addresses as desired.

   or

4. Enter the desired number of internal/external IP addresses in the respective input boxes.

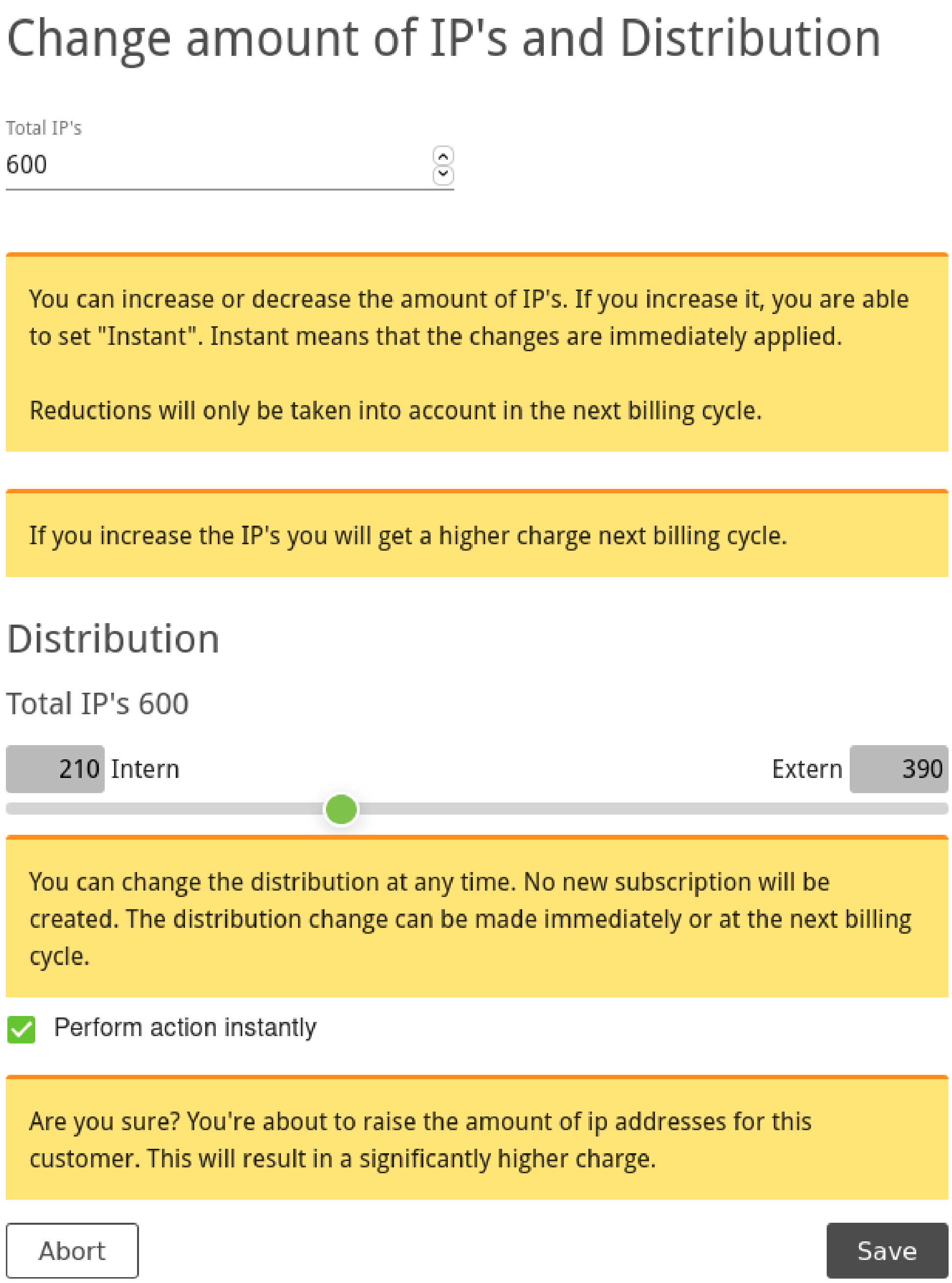

Fig. 3.2: Changing the IP address count and distribution

5. If the number of IP addresses is increased and the change should be applied immediately, activate the checkbox *Perform action instantly*.

Note: A change to a less extensive subscription is only possible at the end of the current booking month. Upgrading to a more extensive subscription is possible immediately.

---

6. Click *Save*.

3.2.3 Locking a Customer Account

If a customer account is locked, the customer is no longer able to log in but the subscription will not be canceled.

A customer account can be locked as follows:

1. Select *Billing* in the menu panel.
2. In the row of the customer, click ⋮ and select *Details*.
3. Activate the checkbox *Account locked* (see Fig. 3.3).

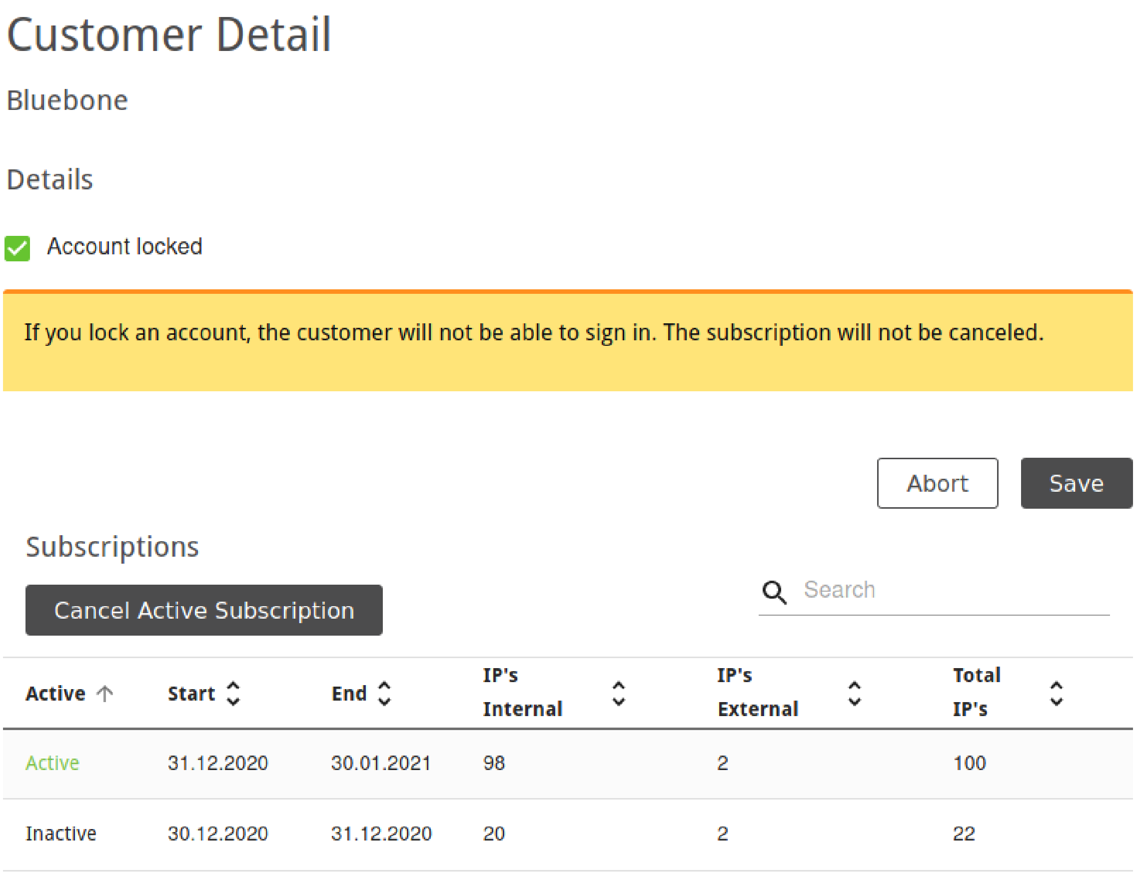

Fig. 3.3: Editing a customer

4. Click *Save*.

→ In the row of the customer, is displayed in the column *Status*.

3.2.4 Canceling an Active Customer Subscription

An active subscription can be canceled as follows:

1. Select *Billing* in the menu panel.
2. In the row of the customer, click ⋮ and select *Details*.
3. Click *Cancel Active Subscription* (see Fig. 3.3).

   → In the row of the customer, ⊘ is displayed in the column *Status*.

3.2.5 Reactivating a Cancelled Customer Subscription

A cancelled subscription can be reactivated by adding the IP address count and distribution to the account as described in Chapter *3.2.2* (page 13).

3.2.6 Adding a Project Key

A project key for a managed-service customer can be added as follows:

1. Select *Billing* in the menu panel.
2. In the row of the customer, click ⋮ and select *Project Key*.
3. Enter the key in the input box and click *Next*.

   → An overview with the number of IP addresses, the runtime and the purchase price is displayed.
4. Enter the selling price in the input box and click *Next*.
5. Move the slider to distribute the total number of IP addresses between internal and external IP addresses as desired and click *Next* (see Fig. 3.4).

   or
5. Enter the desired number of internal/external IP addresses in the respective input boxes and click *Next* (see Fig. 3.4).

   → The summary is displayed.
6. If the number of IP addresses is increased and the change should be applied immediately, activate the checkbox *Perform action instantly*.

   Note: A change to a less extensive subscription is only possible at the end of the current booking month.

   Upgrading to a more extensive subscription is possible immediately.

   ---
7. Click *Finish*.

   → In the row of the customer, *Project Key* is displayed in the column *Payment Method*.

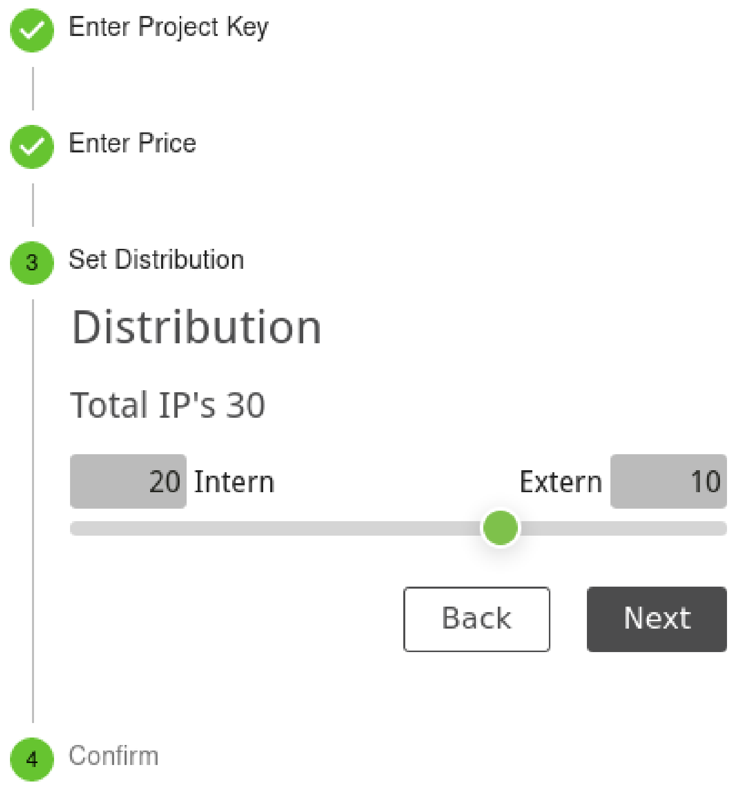

Fig. 3.4: Adding a project key

3.2.7 Editing the Address Information of a Managed-Service Customer

The address information of a managed-service customer can be edited as follows:

1. Select *Billing* in the menu panel.
2. In the row of the customer, click ⋮ and select *Address*.
3. In the section *Company Address* enter the data in the according input boxes.
4. In the section *Value Added Tax Identification (VAT-ID)* enter the VAT number in the according input box.

Note: If the country of the primary address is not Germany, a VAT-ID is required.

5. If a different billing address should be used, activate the checkbox *Use a different billing address* and enter the data in the according input boxes.
6. Click *Save*.

3.2.8 Changing the Main User

The main user of a customer, i.e., the account whose subscription is used, can be changed, for example, in case the respective employee is leaving the company.

The new main user must be an active user, deactivated users cannot be set as the main user.

The main user can be changed as follows:

1. Select *Billing* in the menu panel.

2. In the row of the customer, click ⋮ and select *Main User*.
3. Select the user who should be the main user in the drop-down list.

Note: The current main user is indicated by in front of the e-mail address.

4. Click *Save*.

3.2.9 Deleting a Customer Account

Deleting a customer account will result in the following:

- The main user as well as all other users of the customer are deleted.
- The main user as well as all other users of the customer will no longer be able to log in and use the Greenbone Cloud Service.
- All user, team and customer data are deleted permanently.
- All targets and reports are deleted.
- Active subscriptions expire at the end of the current billing period.

The customer can be deleted as follows:

1. Select *Billing* in the menu panel.
2. In the row of the customer, click ⋮ and select *Delete*.

Note: In case of a customer who has a registered account, continue with step 4.

In case of an invited customer who has not yet accepted the invitation and thus, has not yet created an account, continue with step 5.

4. Type `DELETE` in the input field.
5. Click *Confirm*.

→ A message is displayed, stating that the customer is marked for deletion. The deletion takes some time (approx. 30 minutes). When the deletion is complete, a confirmation e-mail will be sent.

3.3 Filtering Customers

1. Select *Billing* in the menu panel.
2. Click *Add Filter +*.
3. Select the desired billing method, service mode, and/or status (see Fig. 3.5).
4. Click *Apply*.

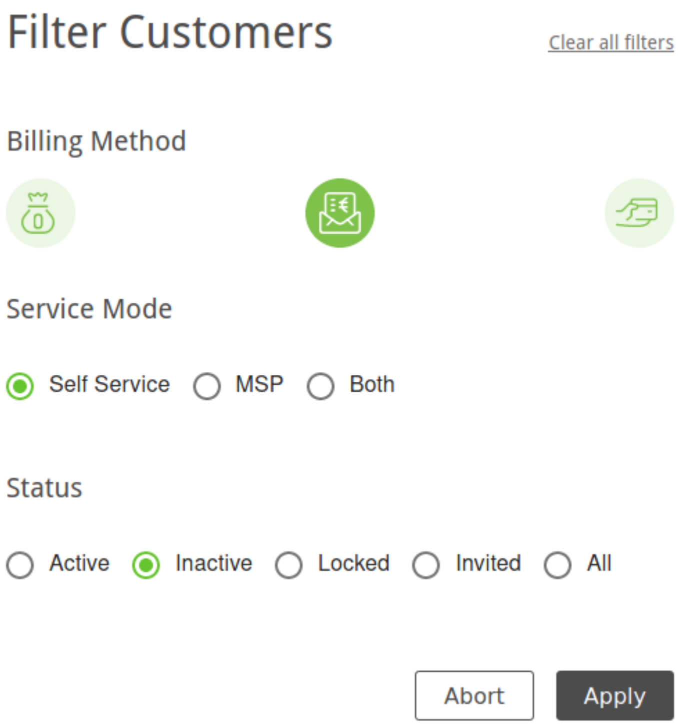

Fig. 3.5: Filtering the customers

3.4 Exporting Customers

By clicking a JSON file of all displayed customers can be downloaded. The customers contained in the file can be chosen by filtering the customers (see Chapter *3.3* (page 18)).

3.5 Configuring the Self Service

The service mode "Self Service" allows customers to change their subscription (number and distribution of IP addresses) on their own.

The self service can be activated, deactivated and adjusted.

3.5.1 Activating or Deactivating Self Service

The service mode "Self Service" can be activated/deactivated as follows:

1. Select *Self-Service* (category *Billing*) in the menu panel.
2. Activate/deactivate the checkbox *Enable users to register themselves.*.
3. Click *Save*.

3.5.2 Configuring the Article Name and Number

The article name and number displayed to customers for their subscription can be changed as follows:

1. Select *Self-Service* (category *Billing*) in the menu panel.

2. Enter the article name and number in the respective input boxes in the section *IP-Ranges*.
3. Click *Save*.

3.5.3 Changing the Sales Prices

Select *Self-Service* (category *Billing*) in the menu panel. The sales prices for all IP address ranges are displayed in the table.

Note: The price of the desired total number of IP addresses is always composed of the prices for the respective IP address ranges that are necessary to obtain the total IP address number.

Example – Price for 300 IP addresses:

50 x sales price of IP address range *1 – 50* + 200 x sales price for IP address range *51 – 250* + 50 x sales price for IP address range *251 – 300*

These sales prices can be adjusted individually for each IP address range as follows:

1. Select *Self-Service* (category *Billing*) in the menu panel.
2. In the row of the desired IP address range click ✎.
3. Enter the sales price in the input box.
4. Click *Save*.

   → The new sales price is displayed in the table.

3.6 Configuring the Payment Methods

All existing payment methods can be displayed by selecting *Payment Methods* (category *Billing*) in the menu panel (see Fig. 3.6).

Billing Type	Status	Actions
CREDIT_CARD	✗	✎
INVOICE	✓	✎
LICENCE_KEY	✓	✎
FREE	✓	

Fig. 3.6: Page *Payment Methods*

For all payment methods the following information is displayed:

Billing Type Description of the payment method.

Status Status of the payment method (active or inactive).

For all payment methods the following action is available:

- Edit the payment method.

3.6.1 Activating or Deactivating a Payment Method

A payment method can be activated/deactivated as follows:

1. Select *Payment Methods* (category *Billing*) in the menu panel.
2. In the row of the desired payment method click .
3. Activate/deactivate the checkbox *is Active*.

3.6.2 Configuring Payment by Credit Card

Credit card payment is handled via Stripe[2].

1. Set up the credit card payment using the following descriptions: https://stripe.com/docs
2. Select *Payment Methods* (category *Billing*) in the menu panel.
3. In the row of credit card payment click .
4. Enter the secret (private) API key in the input box *ApiKey*.
5. Enter the publishable (public) API key in the input box *Public Access Key*.
6. Click *Save*.

[2] https://stripe.com/

CHAPTER 4

Validating Hosts

All current and past host validation requests can be displayed by selecting *Host-Validation* in the menu panel (see Fig. 4.1).

The lower table can be filtered using the drop-down lists in the table header.

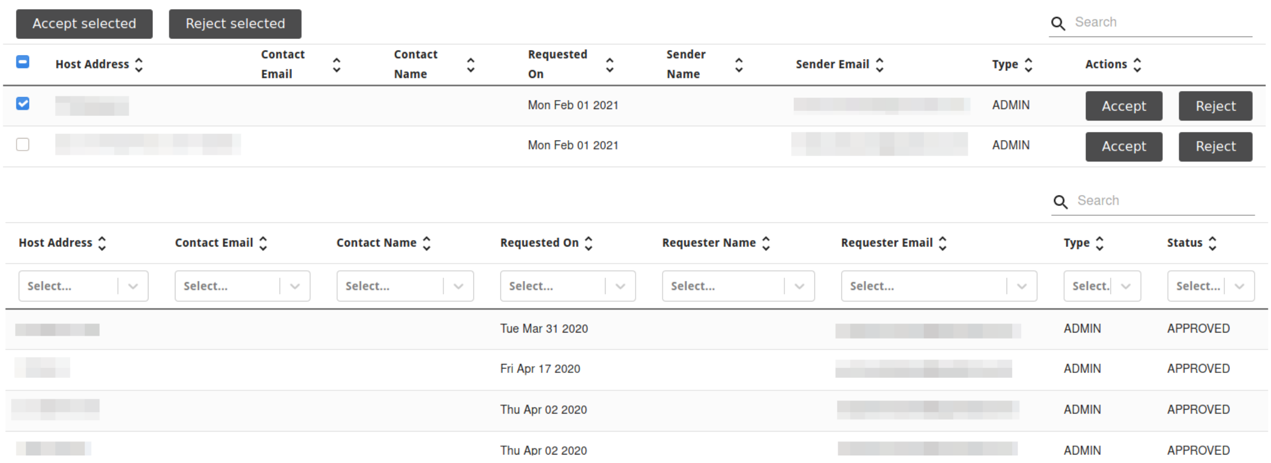

Fig. 4.1: Page *Host-Validation*

Accepting or Rejecting Host Validation Requests

Host validation requests can be accepted/rejected as follows:

1. Select *Host-Validation* in the menu panel.
2. In the row of the respective request in the upper table, click *Accept* or *Reject*.

   or

2. Activate the checkbox in the row of the respective request in the upper table and click *Accept selected* or *Reject selected* above the table.

   Note: If the checkboxes of multiple requests are activated, these requests can be accepted or rejected at the same time by clicking *Accept selected* or *Reject selected* above the table.

   All pending requests can be selected by activating the checkbox in the table header.

CHAPTER 5

Configuring the Platform

5.1 Adjusting the Appearance of the Platform

The appearance – color, login screen and logos – of the platform can be adjusted to adapt to the vMSP's design.

1. Select *Configuration* in the menu panel.
2. Edit a color by clicking the corresponding color square and selecting the color (see Fig. 5.1).

Note: The available colors depend on the selected layout of the login screen (see step 3).

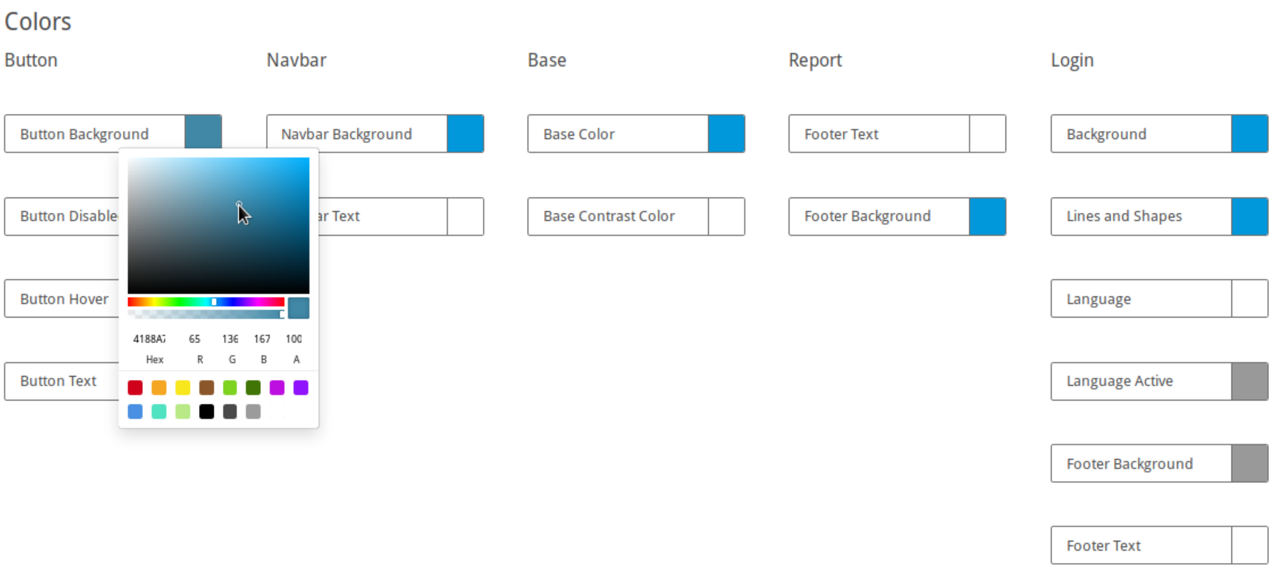

Fig. 5.1: Adjusting the colors of the platform

3. Select a layout for the login screen.

4. Edit a logo by clicking the corresponding preview and selecting an image from a file directory (see Fig. 5.2).

   or

4. Edit a logo by clicking *Upload Logo* and selecting an image from a file directory (see Fig. 5.2).

   or

4. Edit a logo by dragging and dropping an image from a file directory (see Fig. 5.2).

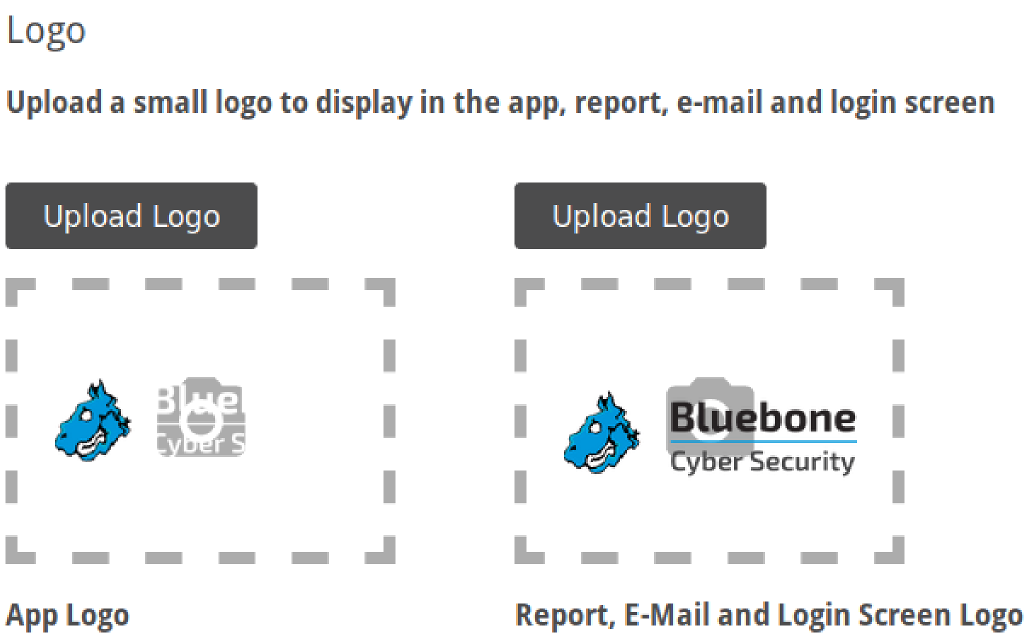

Fig. 5.2: Adjusting the logos of the platform

5. Edit the background image of the login screen by clicking *Upload Logo* and selecting an image from a file directory (only available for some login screen layouts, see step 3).

   or

5. Select the background image of the login screen from the already available images (only available for some login screen layouts, see step 3).
6. Select a size for the background image of the login screen (only available for some login screen layouts, see step 3).
7. Click *Save*.

5.2 Configuring the System E-Mails

5.2.1 Setting up the Mail Server

The mail server that is used for system e-mails can be configured as follows:

1. Select *Mailserver* (category *Configuration*) in the menu panel.
2. Enter the URL of the mail server in the input box *Mailserver* (see Fig. 5.3).
3. Enter the used port in the input box *Port*.

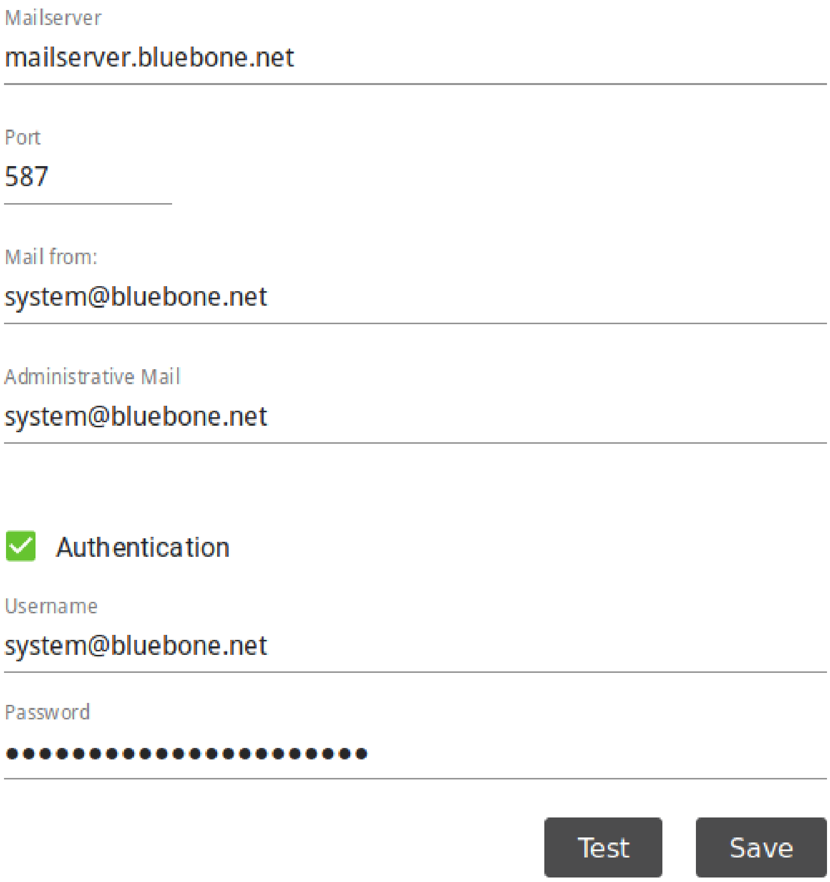

Fig. 5.3: Setting up a mail server

Note: The port 25/tcp must not be used.

4. Define the e-mail address that should be used as the sender of the system e-mails in the input box *Mail from*.
5. Define the e-mail address that should be used for receiving e-mails, e.g., host validation requests, in the input box *Administrative Mail*.
6. Optional: activate the checkbox *Authentication* and enter the credentials for authenticating on the mail server.
7. Click *Test* to send a test e-mail.
8. If the test e-mail is sent and received successfully, click *Save*.

5.2.2 Setting up an E-Mail Signature

The e-mail signature can be edited as follows:

1. Select *Mailserver* (category *Configuration*) in the menu panel.
2. Enter the text for the signature in the input box (see Fig. 5.4).
3. Optional: edit the font style, color, size and alignment.
4. Click *Test* to send a test e-mail with signature.
5. If the test e-mail is sent and received successfully, click *Save*.

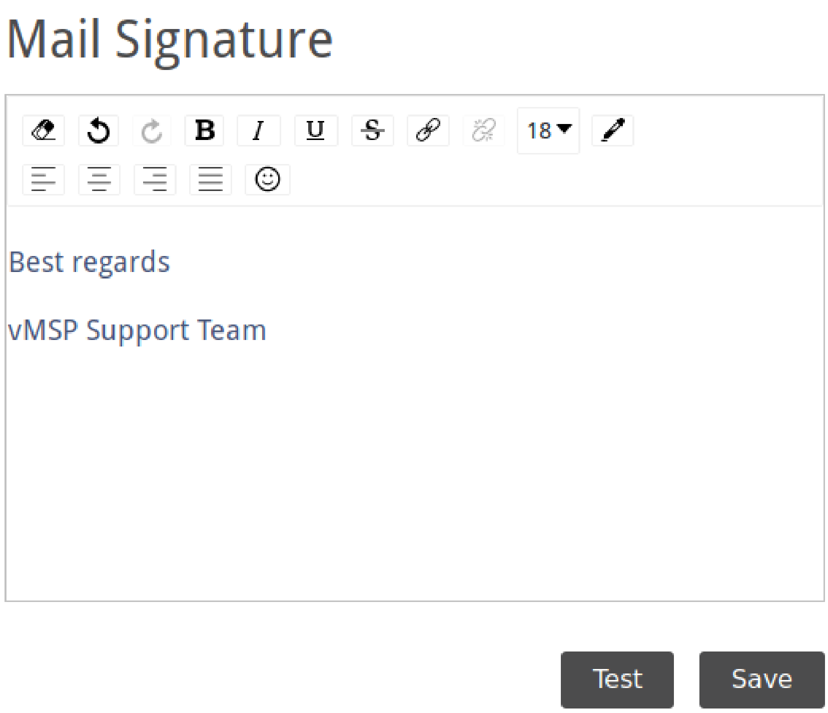

Fig. 5.4: Setting up a mail server

5.3 Adjusting the Legal Information

Greenbone's terms of use and privacy policy are always displayed to end customers. Additionally, own terms of use and and an own privacy policy can be created and activated as follows:

Note: The imprint can be edited in the same way.

However, in contrast to the terms of use and privacy policy, the own imprint is always displayed and not the one of Greenbone.

---

1. Select *Legal* (category *Configuration*) in the menu panel.
2. Select the desired register *Terms of Use*, *Privacy Policy* or *Imprint*.
3. Click the slider to make the own terms of use/privacy policy visible for end customers.
4. Select the desired language.
5. Edit the text in the input box.
6. Click *Save*.

   → The terms of use/privacy policy will be displayed to end customers in addition to Greenbone's terms of use/privacy policy.

CHAPTER 6

Changing the Security Settings

Every vMSP of the Greenbone Cloud Service can manage their own security settings.

6.1 Changing the User Password

The password used for logging in can be changed as follows:

1. Select *Security* in the menu panel.
2. Enter the currently set password in the input box *Password* (see Fig. 6.1).
2. Enter the new password in the input box *New Password*.
3. Repeat the password in the input box *Confirmation*.
4. Click *Save*.

6.2 Setting up a Two-Factor Authentication

To make logging in more secure, a two-factor authentication can be set up as follows:

1. Download one of the following apps for smartphones:
   - *FreeOTP* (available for Android)
   - *Google Authenticator* (available for Android and iOS)
2. Finish the initial setup of the app.
3. Select *Security* in the menu panel.
4. Scan the QR code displayed in the section *Authenticator* (see Fig. 6.2).
5. Enter the one-time code provided by the app in the input box *One-time code*.
6. Click *Save*.

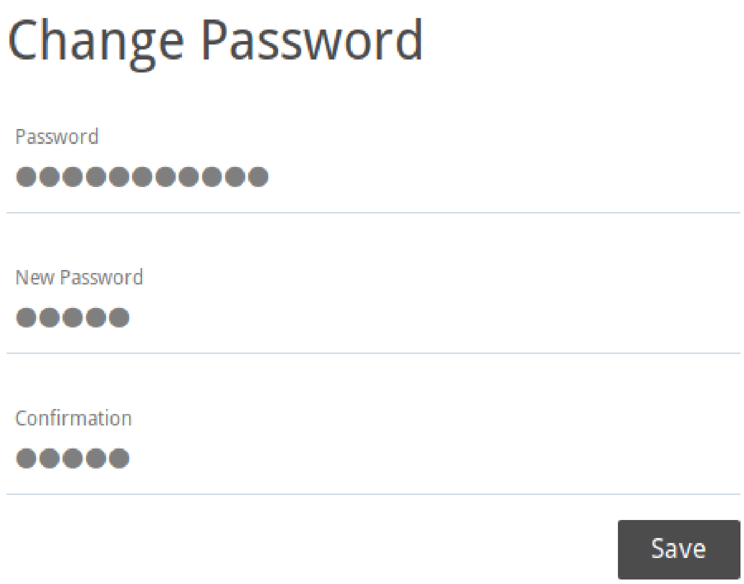

Fig. 6.1: Changing the user password

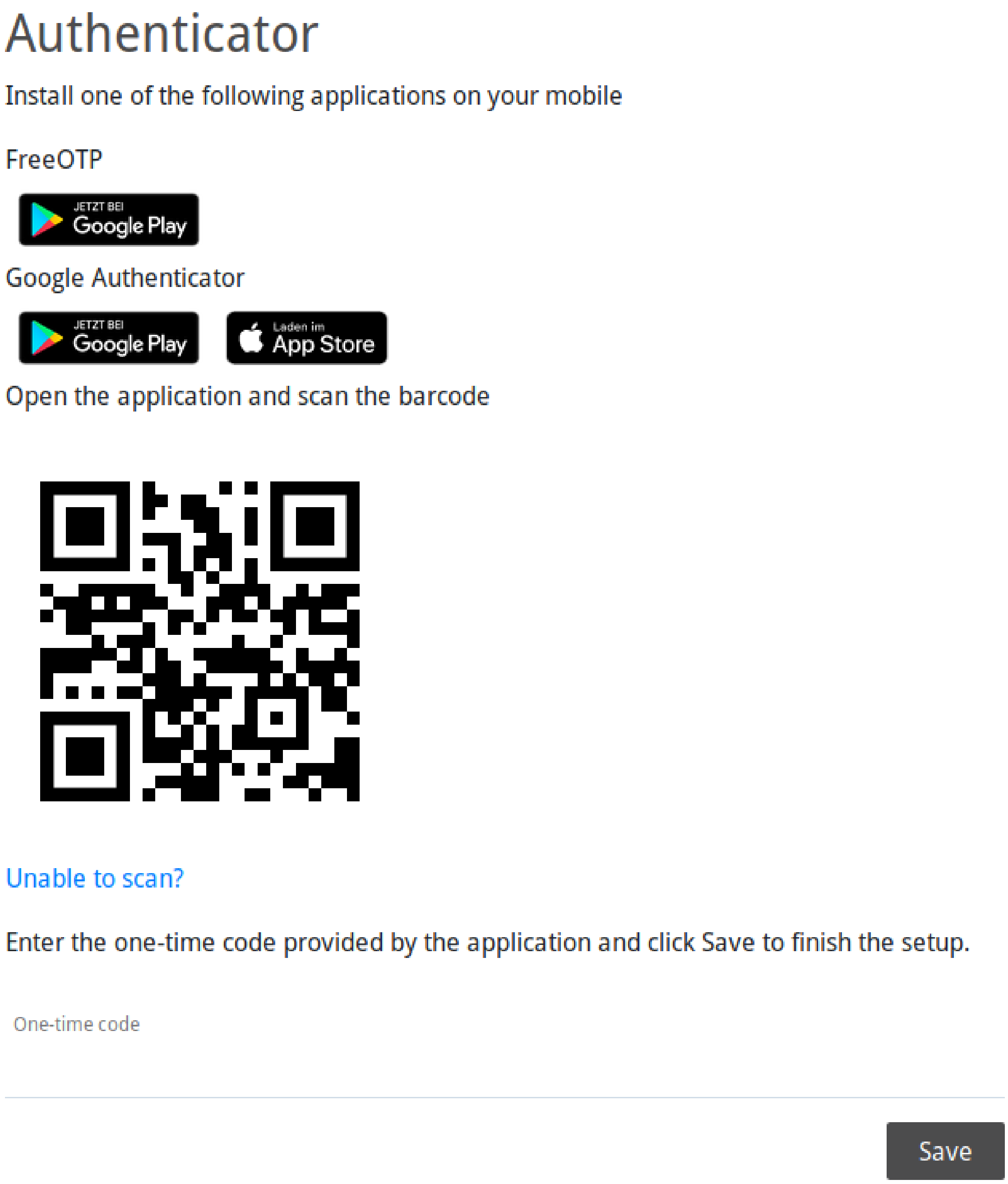

Fig. 6.2: Setting up a two-factor authentication

CHAPTER 7

Frequently Asked Questions

7.1 Which Technology is Used for the VPN Connection?

An SSH Layer 2 based VPN is used for the VPN connection.

Index