

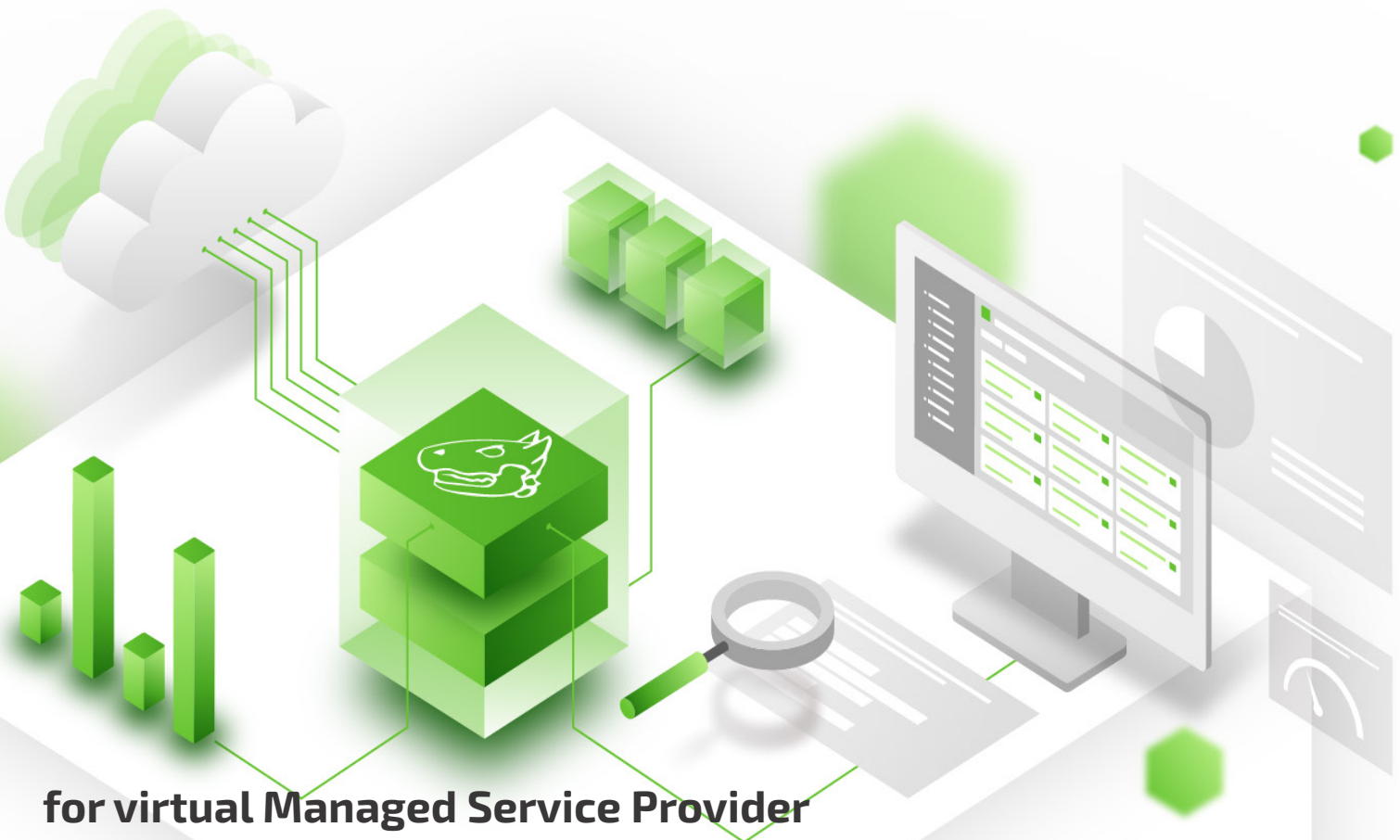


Greenbone

Sustainable Resilience

User Manual

Greenbone Cloud Services



for virtual Managed Service Provider



Greenbone
Sustainable Resilience

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück
Germany
<https://www.greenbone.net>

Status: February 15, 2021

The copyright for this manual is held by the company Greenbone Networks GmbH. Greenbone and the Greenbone logo are registered trademarks of Greenbone Networks GmbH. Other logos and registered trademarks used within this manual are the property of their respective owners and are used only for explanatory purposes.

Contents

1	Introduction	5
2	Overview Dashboard	7
3	Managing Customers	9
3.1	Creating a Customer	10
3.2	Editing a Customer	11
3.2.1	Locking a Customer Account	11
3.2.2	Canceling an Active Customer Subscription	12
3.2.3	Converting a Self-Service Customer into a Managed Service Customer	12
3.2.4	Changing the IP Address Count and Distribution of a Customer	12
3.3	Filtering Customers	14
3.4	Exporting Customers	14
3.5	Configuring the Self-Service	14
3.5.1	Activating or Deactivating Self-Service	15
3.5.2	Configuring the Article Name and Number	15
3.5.3	Changing the Sales Prices	15
3.6	Configuring the Payment Methods	15
3.6.1	Activating or Deactivating Payment Methods	16
3.6.2	Configuring Payment by Credit Card	16
4	Validating Hosts	17
5	Configuring the Platform	19
5.1	Adjusting the Appearance of the Platform	19
5.2	Configuring the System E-Mails	20
5.2.1	Setting up the Mail Server	20
5.2.2	Setting up an E-Mail Signature	22
5.3	Adjusting the Legal Information	23
6	Changing the Security Settings	24
6.1	Changing the User Password	24
6.2	Setting up a Two-Factor Authentication	24
7	Frequently Asked Questions	27
7.1	Which Technology is Used for the VPN Connection?	27
	Index	28

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 Services (GCS) assist companies and agencies with automated and integrated vulnerability assessment and management. Their task is to discover vulnerabilities and security gaps before a potential attacker does.

The GCS achieve this through different perspectives of an attacker:

External The GCS can simulate an external attack on the network to identify outdated or misconfigured firewalls.

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

Internal The GCS 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 GCS use 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 Security Feed ensures that the GCS are provided with the latest testing routines and can discover the latest vulnerabilities reliably. Greenbone Networks analyzes CVE¹ messages and security

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



bulletins of vendors and develops new vulnerability tests daily.

When performing a vulnerability scan using the GCS, 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 GCS utilize 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 GCS also support 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.

Overview 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
- Self-service customers
- 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.

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

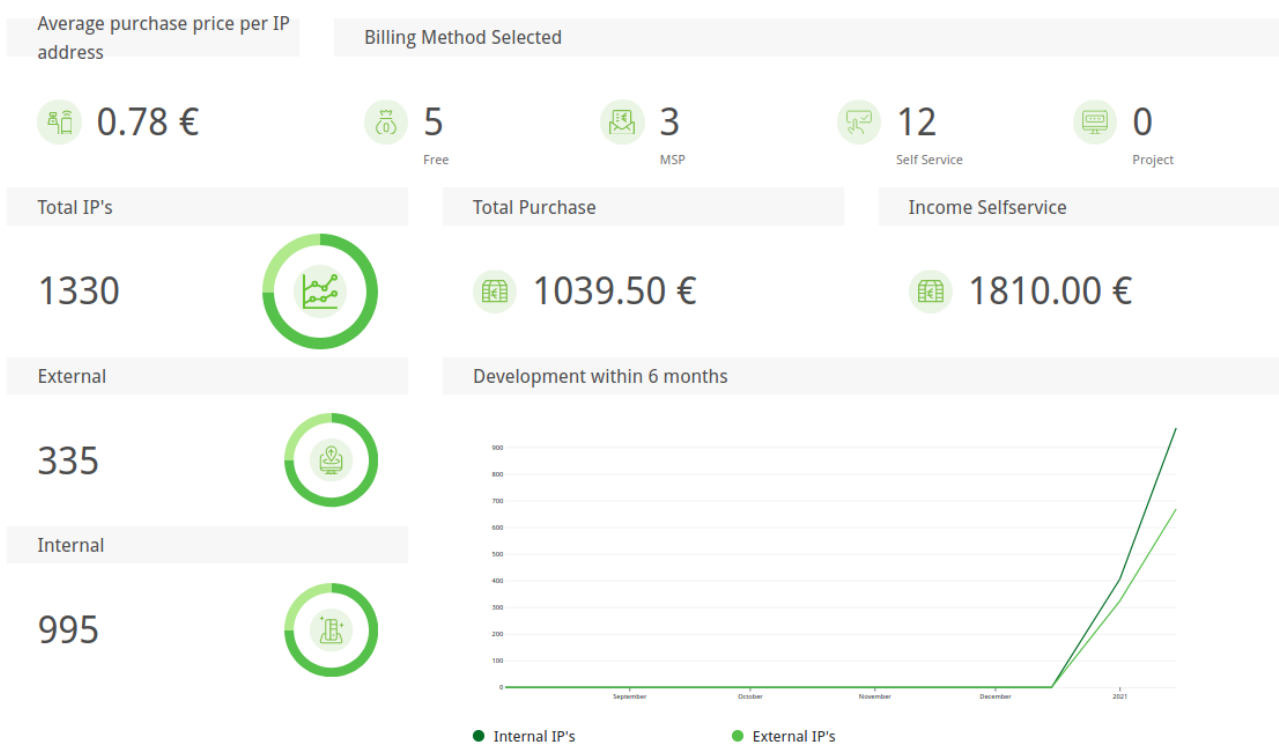


Fig. 2.1: Overview dashboard

Managing Customers

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

Add Filter +
+ New Customer

Download
Customer (json)

Company Name	Service Mode	Status	IP's Internal	IP's External	Payment Method	Average IP Price	Actions
████████████████████	SELFSERVICE	✓	419	81	Credit Card	2.90 €	
████████████████████	SELFSERVICE	✓	268	46	Invoice	3.91 €	
████████████████████	MANAGEDSERVICE	✓	250	250	Credit Card	0	
████████████████████	SELFSERVICE	✓	180	20	Credit Card	4.50 €	
████████████████████	MANAGEDSERVICE	✓	151	150	Invoice	0	
████████████████████	MANAGEDSERVICE	✓	150	150	Invoice	0	
████████████████████	SELFSERVICE	✓	100	0	Invoice	4.00 €	
████████████████████	SELFSERVICE	✓	40	10	Credit Card	3.00 €	
████████████████████	SELFSERVICE	✓	40	10	Credit Card	3.00 €	
████████████████████	SELFSERVICE	✓	40	10	Credit Card	3.00 €	

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 change their own IP address count and distribution. This setting has to be done by the vMSP.
- Self-service customers are able to configure their own subscription (see Chapter 3.5 (page 14)).

Status Status of the customer (active or inactive).

- The customer has an active subscription.



- The customer has no active subscription (see Chapter 3.2.2 (page 12)).
- 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 3.2.1 (page 11)).

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 15)).

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

For all customers the following actions are available:

- Convert a self-service customer to a managed-service customer (only available for self-service customers, see Chapter 3.2.3 (page 12)).
- Change the IP address count and distribution of the customer (see Chapter 3.2.4 (page 12)).
- Resend invite e-mail to a new customer (only available for customers who have been created but did not register yet).
- Display detailed information about the customer. In the overlay, all subscriptions of the customer are displayed and there are options to activate/deactivate the customer account (see Chapter 3.2.1 (page 11)) or to cancel the subscription (see Chapter 3.2.2 (page 12)).

3.1 Creating a Customer

New customers 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.

Tip: If a customer does not receive the invite e-mail, the e-mail can be resend by clicking in the column *Actions*.




3.2 Editing a Customer

3.2.1 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 .
3. Activate the checkbox *Account locked* (see Fig. 3.2).

Customer Detail

Bluebone

Details

Account locked

If you lock an account, the customer will not be able to sign in. The subscription will not be canceled.

Subscriptions

Active ↑	Start ↕	End ↕	IP's Internal ↕	IP's External ↕	Total IP's ↕
Active	31.12.2020	30.01.2021	98	2	100
Inactive	30.12.2020	31.12.2020	20	2	22

Fig. 3.2: Editing a customer



4. Click *Save*.

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




3.2.2 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 .
3. Click *Cancel Active Subscription* (see Fig. 3.2).
→ In the row of the customer,  is displayed in the column *Status*.


3.2.3 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 .
3. Click *Confirm*.
→ The customer is converted into a managed-service customer.

3.2.4 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 .
3. Enter the desired total number of IP addresses (sum of external and internal) in the input box *Total IP's* (see Fig. 3.3).
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.
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*.



Change amount of IP's and Distribution

Total IP's
600

You can increase or decrease the amount of IP's. If you increase it, you are able to set "Instant". Instant means that the changes are immediately applied.
Reductions will only be taken into account in the next billing cycle.

If you increase the IP's you will get a higher charge next billing cycle.

Distribution

Total IP's 600

210 Intern Extern 390

You can change the distribution at any time. No new subscription will be created. The distribution change can be made immediately or at the next billing cycle.

Perform action instantly

Are you sure? You're about to raise the amount of ip addresses for this customer. This will result in a significantly higher charge.

Abort

Save

Fig. 3.3: Changing the IP address count and distribution



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. 3.4).
4. Click *Apply*.

Filter Customers [Clear all filters](#)

Billing Method


Service Mode

Status

Abort Apply

Fig. 3.4: 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 14)).

3.5 Configuring the Self-Service

The service mode “self-service” allows customers to change their subscription (number and distribution of IP addresses) themselves.

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


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:

$50 \times \text{sales price of IP address range } 1 - 50 + 200 \times \text{sales price for IP address range } 51 - 250 + 50 \times \text{sales price for IP address range } 251 - 300$

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. 3.5).

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.







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

Fig. 3.5: Page *Payment Methods*


3.6.1 Activating or Deactivating Payment Methods

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 Stripe².

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 API key in the input box *ApiKey*.
5. Click *Save*.

² <https://stripe.com/>

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.

The screenshot displays two tables for host validation requests. The top table includes buttons for 'Accept selected' and 'Reject selected' at the top left, and a search bar at the top right. The bottom table also features a search bar at the top right and filter dropdowns for each column header.

Host Address	Contact Email	Contact Name	Requested On	Sender Name	Sender Email	Type	Actions
<input checked="" type="checkbox"/>			Mon Feb 01 2021			ADMIN	Accept Reject
<input type="checkbox"/>			Mon Feb 01 2021			ADMIN	Accept Reject

Host Address	Contact Email	Contact Name	Requested On	Requester Name	Requester Email	Type	Status
Select...	Select...	Select...	Select...	Select...	Select...	Select...	Select...
			Tue Mar 31 2020			ADMIN	APPROVED
			Fri Apr 17 2020			ADMIN	APPROVED
			Thu Apr 02 2020			ADMIN	APPROVED
			Thu Apr 02 2020			ADMIN	APPROVED

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.

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).

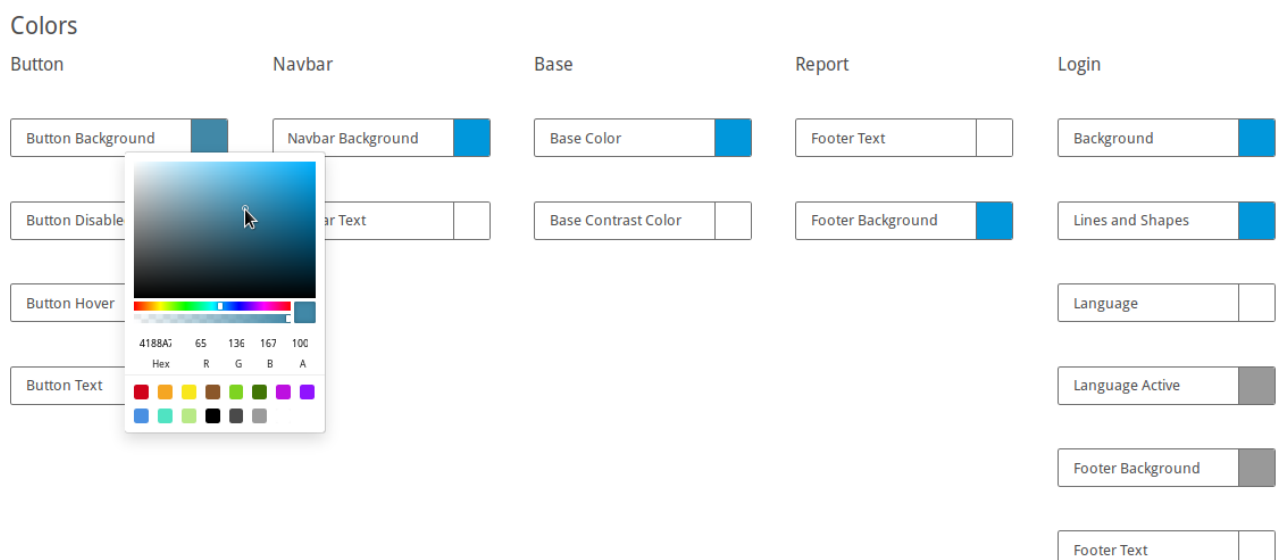


Fig. 5.1: Adjusting the colors of the platform

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).

Logo

Upload a small logo to display in the app, report, e-mail and login screen

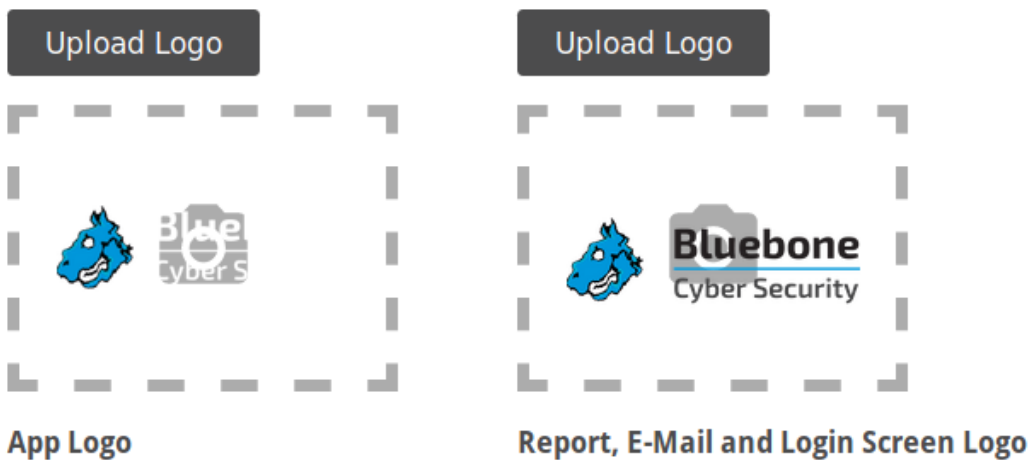


Fig. 5.2: Adjusting the logos of the platform

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*.



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*.

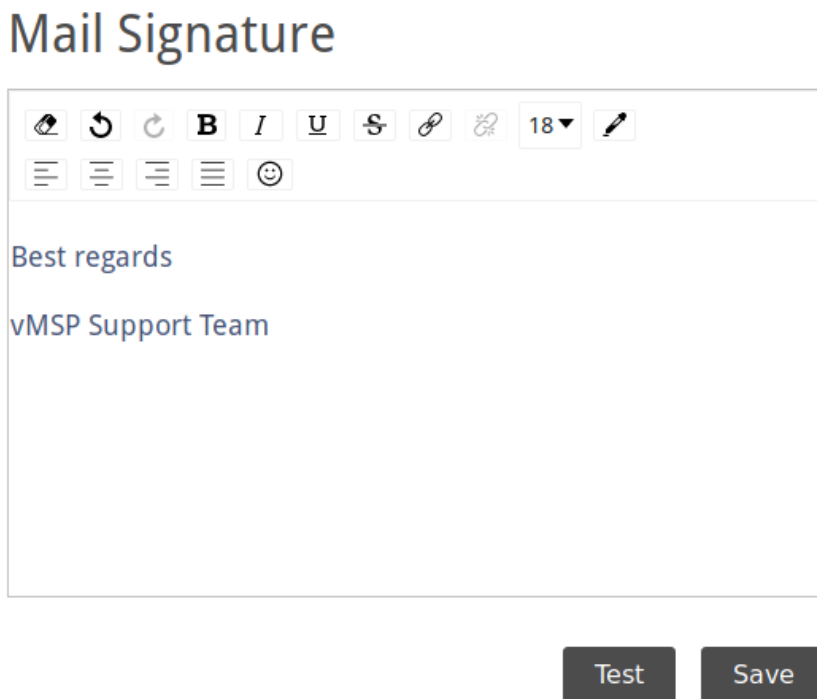


Fig. 5.4: Setting up a mail server



5.3 Adjusting the Legal Information

The terms of use, the privacy policy, and the imprint can be adjusted as follows:

1. Select *Legal* (category *Configuration*) in the menu panel.
2. Select the desired register *Terms of Use*, *Privacy Policy* or *Imprint*.
3. Select the desired language.
4. Edit the text in the input box.
5. Click *Save*.

Changing the Security Settings

Every vMSP of the Greenbone Cloud Services (GCS) 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*.



Change Password

Password
●●●●●●●●●●

New Password
●●●●●

Confirmation
●●●●●

Save

Fig. 6.1: Changing the user password



Authenticator

Install one of the following applications on your mobile

FreeOTP



Google Authenticator



Open the application and scan the barcode



[Unable to scan?](#)

Enter the one-time code provided by the application and click Save to finish the setup.

One-time code

Save

Fig. 6.2: Setting up a two-factor authentication

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.

A

Activating customers, 10
Appearance, 19
Article name, 15
Article number, 15
Authenticator, 24

B

Background Color, 19
Button color, 19
Buttons, 19

C

Changing sales prices, 15
Colors, 19
Credit card, 15
Customer, 10
Customers, 7

D

Dashboard, 6
Deactivating customers, 10
Debtor number, 10

E

E-mail, 20
E-mail signature, 20, 22
Editing customers, 10
Exporting customers, 14

F

FAQ, 24
Filtering customers, 12
Frequently Asked Questions, 24

H

Host, 16
Host validation, 16

I

Imprint, 22

Invoice, 15

L

Layout, 19
Legal, 22
Licence key, 15
Login layout, 19
Login screen, 19
Logo, 19
Look, 19

M

Mail server, 20

N

Navigation bar, 19
New password, 24
Notifications, 23

P

Password, 23, 24
Payment methods, 15
Privacy policy, 22

S

Sales price, 15
Security settings, 23
Self-service, 14
Self-service customers, 14
Settings, 23
Sign in screen, 19
Signature, 20, 22
System e-mail, 20, 22

T

Terms of use, 22
Text color, 19
Two-factor authentication, 23, 24

U

User password, 24



V

Validating hosts, **16**

Validation, **16**

VPN, **27**

