

# SOPHOS

Cybersecurity  
made  
simple.

User Portal  
help

# Contents

Introduction.....	1
Personal.....	2
Change Password.....	2
Personal Information.....	2
Download Client.....	4
SSL VPN.....	7
Secure Web Browsing.....	7
SSL VPN Client.....	8
Clientless Access Connections.....	8
Internet Usage.....	10
Quarantine.....	12
Exception.....	13
My policy overrides.....	14
Add a web policy override.....	14
Hotspots.....	15
Hotspot Type Password of the Day.....	15
Hotspot Type Voucher.....	16
OTP Token.....	19

# 1 Introduction

The Administrator configures a user's personal details, like name, sign-in credentials, email address and user-group membership, at the time when they are registered. The user group applies a set of policies which define surfing quota, access time quota, and network traffic quota for the group members. The surfing quota policy defines the user account expiry date, while the access time policy defines the total number of allowed Internet usage hours. The data transfer policy defines upload and download data transfer restrictions.

The Administrator as well as the user can view the above-mentioned user details. The Administrator can view the details of a user in the Device from **Authentication > Users** while a user can view them from the **User Portal**.

## **Access the User Portal**

You can access the User Portal by browsing to <https://<Sophos Device IP Address>> or clicking "Click here for User Portal" from the Captive Portal page. Log on to the Portal using your user's sign-in credentials.

### **Note**

External users, who need to use authentication services, are required to sign in over the Captive Portal once before they get access to the User Portal. External users can access the Captive Portal by browsing to <https://<Sophos Device IP Address>:8090>. After sign-in, external users have access to the User Portal.

## 2 Personal

### 2.1 Change Password

On the **Change Password** page, you can change your password.

The Device Administrator sets your personal details, like name, sign-in details and email address, when you are registered. You can change some of these details.

1. Navigate to **Personal > Change Password**.
2. On the page, you see these details:

**Username**

Displays name with which user accesses User Portal.

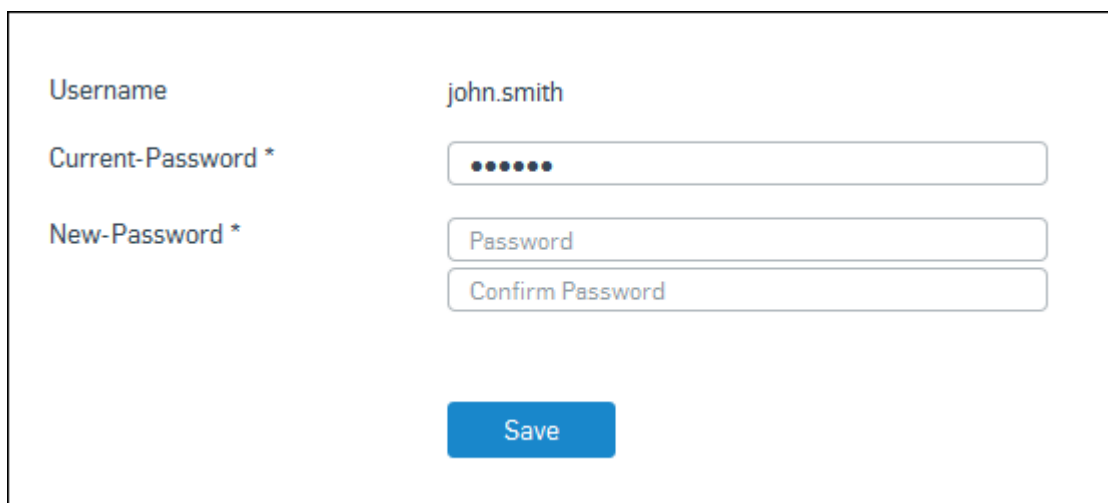
**Current-Password**

Enter the current password.

**New-Password**

Enter a new password. Re-enter the password to confirm.

3. Click **Save**.



The screenshot shows a web form for changing a password. It contains the following elements:

- Username:** A text input field containing the value "john.smith".
- Current-Password \*:** A password input field with six black dots representing the current password.
- New-Password \*:** Two stacked password input fields. The top one contains the placeholder text "Password" and the bottom one contains the placeholder text "Confirm Password".
- Save:** A blue rectangular button with the text "Save" in white.

Figure 1: Change Password

### 2.2 Personal Information

On the **Personal Information** page, you can update your personal details stored on Device.

The Device Administrator sets your personal details, like name, sign-in details and email address, when you are registered. You can change some of these details.

1. Navigate to **Personal > Personal Details**.
2. On the page, you see these details:

**Username**

Displays the name with which you access the User Portal.

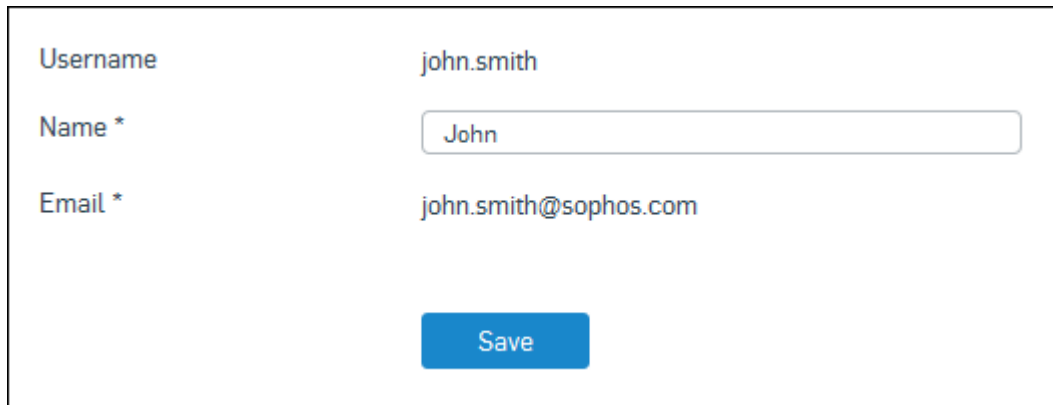
**Name**

Enter the name of the user.

**Email**

Displays the email address configured by the Administrator.

3. Click **Save**.



The screenshot shows a form with three input fields and a button. The first field is labeled 'Username' and contains the text 'john.smith'. The second field is labeled 'Name \*' and contains the text 'John'. The third field is labeled 'Email \*' and contains the text 'john.smith@sophos.com'. Below the fields is a blue button labeled 'Save'.

Username	john.smith
Name *	<input type="text" value="John"/>
Email *	john.smith@sophos.com

Figure 2: Personal Information

## 3 Download Client

The **Download Client** page contains links to download all the clients you might need.

The Device provides various options for user authentication. All the users are authenticated before they are provided with access to network resources. User authentication can be performed using a local database, Active Directory, LDAP, RADIUS, TACACS, eDirectory, NTLM or a combination of these. The Device also supports Single Sign On (SSO) for transparent authentication, whereby Windows credentials can be used to authenticate and a user has to sign in only once to access network resources. SSO can be used in Active Directory and Citrix or Terminal Services environments.

You can authenticate with Device using Captive Portal, Authentication Clients for Windows, Linux, Macintosh, Android and iOS platforms or Single Sign On (SSO).

You can download the following clients from this page:

### Single Sign-On

**Available only for Administrators.**

**Sophos Transparent Authentication Suite** - Enables transparent authentication whereby Windows credentials can be used to authenticate and a user has to sign in only once to access network resources. This does NOT require a client installed on the user's machine.

**Sophos Authentication for Thin Client** - Enables transparent authentication for users in Citrix or Terminal Services environment whereby network credentials can be used to authenticate and a user has to sign in only once to access network resources. This does NOT require a client installed on the user's machine.

### Authentication Clients

Available for all users.

#### Download for Windows

Enables users using a Windows operating system to log on to the Device to access network resources and the Internet as per the policies configured in the Device.

#### Download for MAC OS X

Enables users using a system with Macintosh OS X onwards to log on to the Device to access network resources and the Internet as per the policies configured in the Device.

#### Download for Linux 32

Enables users using a 32-bit Linux operating system to log on to the Device to access network resources and the Internet as per the policies configured in the Device.

#### Download for Linux 64

Enables users using a 64-bit Linux operating system to log on to the Device to access network resources and the Internet as per the policies configured in the Device.

**Download certificate for iOS 12 and earlier and Android client** Download the digital certificate to be installed inside Sophos Network Agent to ensure a safe connection to the firewall.

**Note**

Authentication Clients for iOS/Android can be downloaded from the respective App Store/Play Store. Downloading the client with Google Chrome on Android does not work. Users either have to use a different browser or install the Default Certificate Authority (CA) provided by the Admin as a trusted authority in Google Chrome. Alternatively, users can press long on the download link and select the option "Save Link".

**Install client certificate in iOS 13 and later** Download the default CA first. Then click the link to install the client certificate. In the iOS Trust Store, manually turn on trust for the certificate. For more information, see [knowledge base article 123755](#).

## Configuration of CISCO™ VPN Client for Apple iOS

**Available only if Cisco VPN Client is enabled and allowed for logged-in user.**

CISCO™ VPN Client is software developed by CISCO to establish encrypted VPN tunnels with highly secure remote connectivity for remote workers. Click **Install** to install the SF-related configuration for Cisco VPN Client in your iOS Device. Import this configuration into the Client so that it can communicate with the SF Device.

## SPX Add-in

**This feature is available only with a valid Email Protection subscription**

**This feature is available in Sophos Firewall Models XG105 and above, Cyberoam Models CR25iNG and above, and all Sophos UTM Models.**

Click **Download Sophos Outlook Add-in** to download and install the SPX Add-in. The SPX Add-in simplifies the encryption of messages that contain sensitive or confidential information leaving the organization. The Add-in integrates seamlessly with the user's Microsoft Outlook software, making it easy for users to encrypt messages through Sophos Firewall Email Protection.

Follow the steps given below to install the Add-in in Outlook:

1. Unzip the files to a temporary folder.
2. For an interactive install, run setup.exe (users will be prompted for input).
3. For an unattended install, the prerequisites are:
  - Windows XP, Windows Vista, Windows 7, Windows 8 (both 32 and 64-bit) versions are supported.
  - Microsoft Outlook 2007 SP3, 2010 or 2013 (both 32 and 64-bit) versions are supported.

- Microsoft .NET Framework 4 Client Profile.
  - Microsoft Visual Studio 2010 Tools for Office Runtime 4.0.
4. Now, please run the installer with the following parameters: `msiexec /qr /i SophosOutlookAddInSetupUTM.msi T=1 EC=3 C=1 I=1`.

**Related information**

[Knowledge base article 123755](#)



## 4 SSL VPN

The **SSL VPN** menu allows you to download remote access client software and configuration files, connect via clientless access and do secure web browsing.

### Note

The **SSL VPN** tab is available only if the administrator has assigned at least one SSL VPN Policy to you.

You will only see remote access options that correspond to the connection types the administrator enabled you, e.g., if you have been enabled to use SSL VPN remote access, you will find an **SSL VPN Client** section.

Each connection type is displayed in a separate section. Depending on the connection type, information and/or buttons to download the respective software are available.

### Related concepts

[Secure Web Browsing](#) (page 7)

The **Secure Web Browsing** menu allows an SSL VPN clientless user to access any URL over SSL.

[Clientless Access Connections](#) (page 8)

The **Clientless Access Connections** menu allows users from external sources to access internal resources via pre-configured connection types, using only a browser as a client.

[SSL VPN Client](#) (page 8)

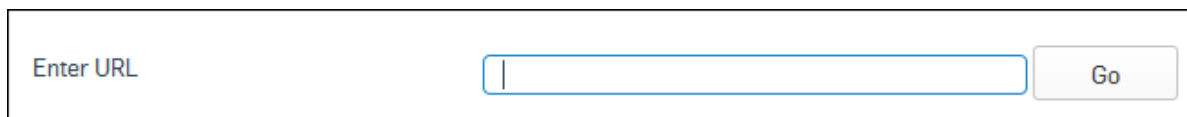
The **SSL VPN Client** menu allows you to download SSL VPN client software and configuration files automatically generated and provided for you according to the SFOSs settings selected by the administrator.

### 4.1 Secure Web Browsing

The **Secure Web Browsing** menu allows an SSL VPN clientless user to access any URL over SSL.

There is no need for the Administrator to create a bookmark for such URLs in the clientless policy. This function can be activated/deactivated by the Administrator of SFOS in the clientless access policy (**Configure > VPN > Clientless access**) with the **Restrict Web Applications** option.

To use secure web browsing, you enter a complete, valid URL (e.g. <http://www.google.com>) and click **Go**.



The image shows a user interface for secure web browsing. It consists of a rectangular box containing a text input field on the left with the placeholder text "Enter URL" and a "Go" button on the right. The input field is empty and has a blue border. The "Go" button is a light gray rectangle with rounded corners and the text "Go" in a dark gray font.

Figure 3: Secure Web Browsing

### Related concepts

[SSL VPN](#) (page 7)

The **SSL VPN** menu allows you to download remote access client software and configuration files, connect via clientless access and do secure web browsing.

## 4.2 SSL VPN Client

The **SSL VPN Client** menu allows you to download SSL VPN client software and configuration files automatically generated and provided for you according to the SFOSs settings selected by the administrator.

You can download:

- Client and configuration for Windows
- Configuration for Windows
- Configuration for other OSs
- Configuration for Android/iOS

After you install the software package on the remote client, you can open the SSL VPN connection.

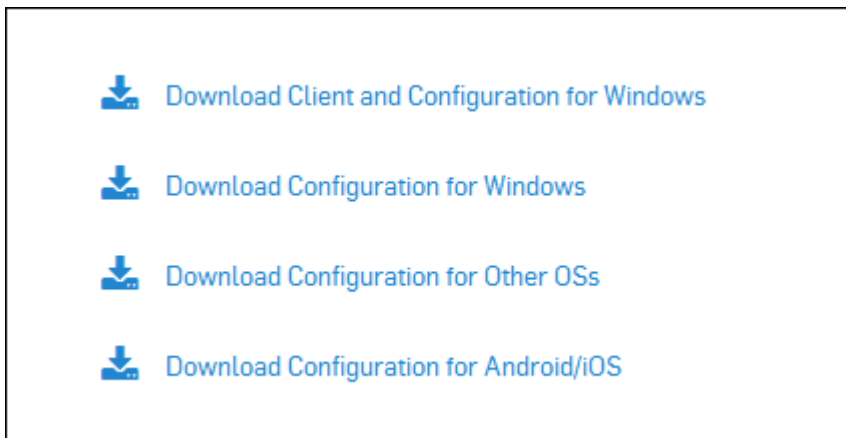


Figure 4: Clients

### Related concepts

[SSL VPN](#) (page 7)

The **SSL VPN** menu allows you to download remote access client software and configuration files, connect via clientless access and do secure web browsing.

## 4.3 Clientless Access Connections

The **Clientless Access Connections** menu allows users from external sources to access internal resources via pre-configured connection types, using only a browser as a client.

### Note

The **Clientless Access Connections** section is only available if the administrator has created a VPN connection for you and added you to the allowed users.

In the **Clientless Access Connections** section the allowed connections are listed. The icons denote the type of connection.

To use a connection, click the respective connect button. A new browser window opens. Contents and layout depend on the connection type, e.g., it contains a website if you opened a HTTP or HTTPS connection. Depending on the settings the administrator selected, you either have to sign in or you will be logged in automatically.

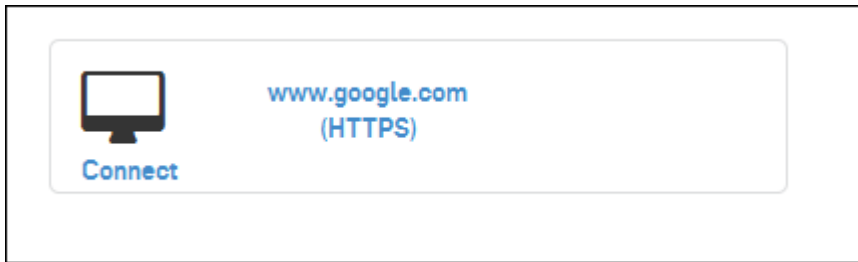


Figure 5: Clientless Access Connections

### Related concepts

[SSL VPN](#) (page 7)

The **SSL VPN** menu allows you to download remote access client software and configuration files, connect via clientless access and do secure web browsing.

## 5 Internet Usage

This page displays the overall Internet Usage of the user.

**Internet Usage** displays all you need to know about your Internet surfing.

The page displays the following details:

- Policy Information like user group, total surfing time allowed in hours, surfing quota expiry date, data transfer cycle renewal date, total Internet time used, guest user account expiry date (if you are registered as guest user).

Username	john.smith
Group	Sales
Time Allotted To User (HH)	Unlimited
Surfing Quota Expiry Date	N.A.
Data Transfer Cycle Renewal	N.A.
Internet Usage Time (HH:MM)	00:00

Figure 6: Policy Information

- Usage Information like allotted, used and remaining Data transfer quota (upload and download).

Resource	Allotted	Usage			Remaining
		Up to Last Session	Current Session	Total	
Upload Network Traffic	N.A.	0 MB	0 MB	0 MB	N.A.
Download Network Traffic	N.A.	0 MB	0 MB	0 MB	N.A.
Total Network Traffic	N.A.	0 MB	0 MB	0 MB	N.A.

Figure 7: Usage Information

- Monthly usage - surfing time and data transfer details

View Usage For: <input type="text" value="October-2015"/>														
<table border="1"> <thead> <tr> <th>IP Address</th> <th>Start Time</th> <th>Stop Time</th> <th>Used Time (in minutes)</th> <th>Download Network Traffic</th> <th>Upload Network Traffic</th> <th>Total Network Traffic</th> </tr> </thead> <tbody> <tr> <td colspan="7">No Records Found</td> </tr> </tbody> </table>	IP Address	Start Time	Stop Time	Used Time (in minutes)	Download Network Traffic	Upload Network Traffic	Total Network Traffic	No Records Found						
IP Address	Start Time	Stop Time	Used Time (in minutes)	Download Network Traffic	Upload Network Traffic	Total Network Traffic								
No Records Found														

Figure 8: Monthly Usage

The above-mentioned information might not all be displayed, depending on your user type and the policies configured for you.

## 6 Quarantine

**SMTP quarantine** displays the complete list of your quarantined emails. You can perform the following actions on these emails:

- Sort based on date range, sender, and subject
- Filter based on the listed options
- Release
- Delete.

### **Releasing Spam Quarantined Email**

You can release only quarantined spam. You can do it in one of the following ways:

- Click **Release** against an email.
- Select the emails, select **Release** from the available options and click **Go**.
- Release from the emailed Quarantine digest.

#### **Note**

You cannot release or download virus-infected emails.

The firewall scans the released emails and delivers these to your inbox.

## 7 Exception

**Exception** allows you to specify sender email addresses from which mails are to be allowed or blocked.

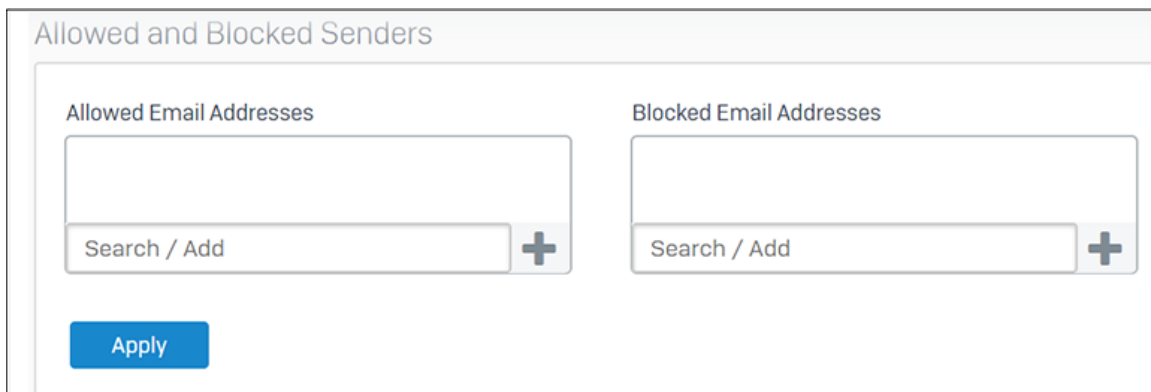
The page displays the following details:

- **Allowed email addresses**

Enter a valid email address (abc@example.com) or a wildcard for a specific domain (\*@example.com). Mails from these email addresses will not be marked as spam or quarantined. This action will be applicable to all recipients within your organization.

- **Blocked email addresses**

Enter a valid email address (abc@example.com) or a wildcard for a specific domain (\*@example.com). Mails from these email addresses will be quarantined for all recipients within your organization.



The screenshot shows a web interface titled "Allowed and Blocked Senders". It features two main sections: "Allowed Email Addresses" and "Blocked Email Addresses". Each section contains a large text input field for entering email addresses. Below each input field is a smaller search/add field with the text "Search / Add" and a plus sign icon. At the bottom left of the interface is a blue "Apply" button.

Figure 9: Exception

## 8 My policy overrides

Policy overrides allow you to temporarily unblock websites that are blocked by web policies.

To turn on or turn off a policy override session, use the **Status** switch.

To view the page on the user portal and create policy override sessions, you require your administrator's authorization.

You can create a policy override session, specifying the access code, the allowed websites and web categories, and the schedule during which the policy override is in effect.

You can't unblock websites for which your administrator disallows policy overrides. Your administrator can turn on, turn off, or delete the policy override sessions that you've created.

How to use a policy override: When you try to access a blocked website, a block page appears. Enter the access code in the field provided on the block page.

### 8.1 Add a web policy override

Specify the websites and web categories to unblock during the policy override session.

You can use the default access code or generate a new one to unblock the websites. You need to specify the session's time period.

1. Go to **My policy overrides** and click **Add**.
2. Enter a **Session name**.
3. You can use the default **Access code**. To generate a new code, select **Generate access code**. If your administrator authorizes you, you can manually create the code.

#### Tip

When you try to access a blocked website, a block page appears. Enter the access code in the field provided on the block page.

4. Specify the **Allowed websites**.
5. Select the **Allowed website categories**.

#### Note

You can't unblock websites for which your administrator disallows policy overrides.

6. For **Restricted to time periods**, select a schedule from the list. You can unblock the websites and web categories during this time period.
7. Select **Apply**.



## 9 Hotspots

The menu **Hotspots** allows cafés, hotels, companies, etc. to provide time- and traffic-restricted Internet access to guests.

The **Hotspots** tab is only visible if the administrator created a hotspot of one of the types **Password of the Day** or **Voucher**.

On this tab, you can distribute the hotspot access information to wireless network guests. Depending on the type of hotspot selected, you can either distribute a general password or generate and distribute vouchers.

### Related tasks

[Hotspot Type Password of the Day](#) (page 15)

[Hotspot Type Voucher](#) (page 16)

This page describes how to create vouchers, each with a unique code. The vouchers can be printed and given to guests. A list of created vouchers gives an overview of their usage and helps you to manage them.

### 9.1 Hotspot Type Password of the Day

This page describes how to create a password of the day for a hotspot.

In the **Password** field, the current password is displayed. It changes automatically once a day. However, you can change the password manually. The former password will immediately become invalid and active sessions will be terminated. You can generate new passwords on demand:

1. Navigate to **Hotspots**.
2. Select the requested hotspot from the **Hotspot** drop-down menu.
3. Enter a password into the field **Password** and click **Generate**.

#### Note

You can also use the default password which is already generated.

4. Activate/deactivate the **Send Mail** switch.

#### Note

The password will be sent to the email recipients specified by the administrator. If the administrator did not specify any email addresses, the checkbox is not available.

5. Click **Save** to save the newly generated password.

The password changes immediately.

The screenshot shows a web form with two main sections. The first section, titled 'Hotspot', features a dropdown menu currently set to 'Marketing'. The second section, titled 'Password', includes a text input field containing the text 'wanovuki00' and a 'Generate' button to its right. Below the 'Generate' button is a prominent blue 'Save' button.

Figure 10: Password of the Day

**Related concepts**

[Hotspots](#) (page 15)

The menu **Hotspots** allows cafés, hotels, companies, etc. to provide time- and traffic-restricted Internet access to guests.

## 9.2 Hotspot Type Voucher

This page describes how to create vouchers, each with a unique code. The vouchers can be printed and given to guests. A list of created vouchers gives an overview of their usage and helps you to manage them.

This page describes how to create and manage vouchers.

1. Navigate to **Hotspots**.
2. Specify the following settings:

**Hotspot**

Select the hotspot for which you want to create a voucher.

**Hotspot Voucher Definition**

Select the requested voucher definition.

**Note**

The available voucher types are defined by the administrator. Which type to use for what purpose has to be defined within the company.

**Amount**

Enter the number of vouchers of this type to be created.

**Description**

Specify a description for the voucher.

**Print**

Enable this option if you want to print the vouchers directly.

**Page Size**

Select the page size you want to print.

**Vouchers per Page**

Select how many vouchers will be printed onto one page. The device automatically adjusts the vouchers on the page.

### Add QR Code

You can request that in addition to the voucher text data, the printed voucher should also contain a QR code. A QR code is a square image containing encoded data. It can be scanned by a mobile device in order to access the hotspot sign-in page, where the fields are already filled out with the necessary data.

3. Click **Create Vouchers** to create the vouchers with the settings you made.

The vouchers are generated. Each voucher will immediately be displayed as a new line in the voucher list below. If specified, they will be printed directly. Each voucher has a unique code.

The screenshot shows a configuration form for a Hotspot Type Voucher. The form is contained within a light gray border. At the top, there is a label 'Hotspot' followed by a dropdown menu showing 'Marketing'. Below this is a horizontal separator line. The main form area contains several rows of controls:

- 'Hotspot Voucher Definition' with a dropdown menu showing 'Hotspot Voucher Definition'.
- 'Amount' with an empty text input field.
- 'Description' with a larger text area containing a small grid icon in the bottom right corner.
- 'Print' with a toggle switch currently set to 'OFF'.
- 'Page Size' with a dropdown menu showing 'A4 (210 x 297 mm)'.
- 'Vouchers per page' with a dropdown menu showing '1'.
- 'Add QR code' with a toggle switch currently set to 'OFF'.

At the bottom left of the form is a button labeled 'Create Vouchers'.

Figure 11: Hotspot Type Voucher

You can now manage the voucher list below.

### Related concepts

[Manage Voucher List](#) (page 18)

This page describes how to manage the voucher list on the **Hotspots** tab.

[Hotspots](#) (page 15)

The menu **Hotspots** allows cafés, hotels, companies, etc. to provide time- and traffic-restricted Internet access to guests.

## 9.2.1 Manage Voucher List

This page describes how to manage the voucher list on the **Hotspots** tab.

In the voucher list you can manage vouchers. You can sort the list, print, delete, or export selected vouchers.

- To sort the list, click on the table heading you want to sort for. The arrow symbol displays if the list is sorted ascending or descending.
- To print or delete vouchers, select the checkbox beside the desired vouchers, then click the appropriate button at the bottom.

### Note

Vouchers can be deleted automatically after a specified time, which can be configured by the administrator.

- To export vouchers, select the checkbox beside the desired vouchers, then click the **Export CSV** button at the bottom. A window is displayed where you can decide to save or to open the CSV file directly. The selected vouchers will be saved in one CSV file. When you open the file, take care to select the correct character for column separation.

### Related tasks

[Hotspot Type Voucher](#) (page 16)

This page describes how to create vouchers, each with a unique code. The vouchers can be printed and given to guests. A list of created vouchers gives an overview of their usage and helps you to manage them.

# 10 OTP Token

This page describes how to sign in using a one time password.

A one time password (OTP) is a password that is valid for only one sign-in session. It consists of a static component (your primary password) and a time-dependent or temporary passcode.

1. Install Sophos Authenticator on your mobile device.  
You can download Sophos Authenticator from your App Store.
2. Scan the QR code displayed on the screen using Sophos Authenticator on your phone.  
The app will generate a passcode. This passcode will be renewed in regular intervals (stated as "Timestep").
3. Click **Proceed to Login**.
4. Enter your username and your User Portal password directly followed by the passcode just generated to sign in.
5. Click **Login**.  
Now you have access to the User Portal.