VPN

Android | English

AVAILABLE TOPICS

FREEDOME VPN

F-Secure FREEDOME VPN is a simple, yet powerful online privacy and security app for all your desktop and mobile devices.

FREEDOME VPN is a virtual private network (VPN) application that creates a secure, encrypted connection from your device to the F-Secure location that you have selected. It protects your connection in a WiFi network by making your data unreadable for outsiders. It even prevents anyone from changing your data or hijacking your network traffic.

When you surf the internet, data collection companies track your online activities and sell your data to advertisers. FREEDOME VPN blocks these tracking attempts from HTTP traffic so you can browse anonymously and undisturbed.

FREEDOME VPN scans for tracking cookies and other online threats. You're protected from harmful sites, trackers and apps that want to forward your data without you knowing about it.

Choose where you want your IP address to be shown from about 30 available virtual locations. Changing your location is useful when you want to optimize your connection, add an extra layer of privacy, or access your favorite online services when you're away from home.

1. Introduction

This chapter provides general information about F-Secure FREEDOME.

1.1 Where can I buy F-Secure FREEDOME?

F-Secure FREEDOME is globally available.

You can buy F-Secure FREEDOME for PC, Mac, Android and iOS via the F-Secure website (https://www.f-secure.com/en/vpn). You can also buy F-Secure FREEDOME for Android on the Google Play Store (https://play.google.com/store/apps/details?id=com.fsecure.freedome.vpn.security.privacy.android&referrer=utm_source%3Dweb_product_page&utm_campaign%3DEN&hl=en) and for iOS on the Apple App Store (https://itunes.apple.com/app/apple-store/id771791010?pt=348697&ct=int_freedome_productpage_global&mt=8).

F-Secure FREEDOME is available in the following countries:

- Albania
- Algeria
- Angola
- Anguilla*
- Antigua and Barbuda
- Argentina
- Armenia
- Aruba**
- Australia
- Austria
- Azerbaijan
- Bahamas
- Bangladesh**
- Barbados*
- Belarus
- Belgium
- Belize
- Benin
- Bermuda*
- Bhutan*
- Bolivia
- Bosnia and Herzegovina**
- Botswana
- Brazil
- Brunei Darussalam*
- Bulgaria
- Burkina Faso
- Cambodia
- Canada
- Cape Verde
- Cayman Islands*
- Chad*
- Luxembourg
- Malawi*
- Macau*
- Macedonia
- Madagascar*
- Malaysia
- Mali
- Malta
- Mauritania*
- Mauritius
- Mexico
- Micronesia*
- Moldova
- Mongolia*
- Montserrat*
- Morocco**
- Mozambique
- Namibia
- Nepal
- Netherlands
- Netherlands Antilles**
- New Zealand
- Nicaragua
- Niger
- Nigeria
- Norway
- Pakistan
- Palau*
- Panama
- Papua New Guinea
- Paraguay
- Peru

- Chile
- Colombia
- Congo, Republic of
- Costa Rica
- Côte d'Ivoire**
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Dominica*
- Dominican Republic
- Ecuador
- El Salvador
- Estonia
- Fiji
- Finland
- France
- Gambia*
- Germany
- Ghana
- Greece
- Grenada*
- Guatemala
- Guinea-Bissau
- Guyana*
- Haiti**
- Honduras
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia*
- Philippines
- Poland
- Portugal
- Romania
- Rwanda**
- Saint Lucia*
- Senegal
- Serbia**
- Seychelles*
- Sierra Leone*
- Singapore
- Slovakia
- Slovenia
- Solomon Islands*
- South Africa
- Spain
- Sri Lanka
- Saint Vincent and The Grenadines*
- St. Kitts and Nevis
- Suriname*
- Swaziland*
- Sweden
- Switzerland
- São Tomé and Príncipe
- Taiwan
- Tajikistan
- Tanzania
- Thailand
- Togo**
- Trinidad and Tobago
- Tunisia
- Turkey

- Ireland
- Israel
- Italy
- Jamaica
- Japan
- Jordan
- Kazakhstan
- Kenya
- Korea, Republic of
- Kyrgyzstan
- Lao People's Democratic Republic
- Latvia
- Lebanon
- Liberia*
- Liechtenstein**
- Lithuania
- Turkmenistan
- Turks and Caicos*
- Uganda
- Ukraine
- United Kingdom
- United States
- Uruguay
- Uzbekistan
- Venezuela
- Vietnam
- Virgin Islands*
- Yemen
- Zambia**
- Zimbabwe

*Not available in Google Play Store.

**Not available in Apple App Store.

1.2 System requirements

Before you start installing the app, make sure that your device meets the system requirements for F-Secure FREEDOME.

F-Secure FREEDOME supports the following operating systems:

- Android 8.0 and later (Android 8.0 and later on Google Certified Android TVs)

- iOS 11 and later
- Windows 7, Windows 8.1 and later
- macOS 10.12 and later

1.3 What happens when you use VPN

FREEDOME VPN increases your security and privacy protection by routing your network traffic through F-Secure's servers.

When you use FREEDOME, it establishes a VPN connection between your device and F-Secure's servers. This means that, instead of using a direct connection between your device and the internet, all data traffic is routed through those servers. This approach has several benefits:

- Your data traffic is encrypted. FREEDOME uses strong encryption for all communications between your device and the F-Secure servers. This means that identity thieves and other hackers cannot steal your personal information by intercepting your data traffic, even when you use an open WiFi connection.
- Your network communication goes through the IP address of the F-Secure server that you are connected to. In this way, for example the web site you browse can only see the IP address of the F-Secure server and not the IP address of your own device.
- With FREEDOME, you may be able to access geo-restricted content. As the only IP address that web sites and services see is the one for the F-Secure server, you may be able access content that is only available in your home country even when you are travelling abroad. However, some services have blocked the use of VPN. You might be able to use these services while using a different location on FREEDOME, but we cannot guarantee this.
- Browsing protection in FREEDOME makes sure that while you browse the web, the sites you go to are safe. Browsing protection does this by blocking web sites that contain suspicious and harmful content or steal your personal information, including credit card numbers, user account information, and passwords.

1.4 How does FREEDOME VPN scan for viruses?

FREEDOME VPN is scanning HTTP traffic and currently blocks the Android application packages (.apk files) considered harmful.

For testing and demonstration purposes, FREEDOME VPN is also scanning all files downloaded from certain domains, such as .eicar.org and .amtso.org. The file scan performed is the same rigorous antivirus scan that we are using with other F-Secure products. FREEDOME VPN is selective about the file types due to performance considerations at the moment.

1.5 Does F-Secure follow the EU data retention laws?

F-Secure as a company is not a public communication provider or operator, and therefore the referred Data Retention Directive does not apply to us.

You can find details on how we handle your data in F-Secure FREEDOME VPN Privacy Policy (https://www.f-secure.com/en/legal/privacy/consumer/freedome).

It should be noted that when the EU court gave its verdict on the excessive nature of Data Retention Directive, Finland had already amended its national laws to better respect people's online privacy. Due to this, the data retention obligation is now limited to certain companies only. F-Secure, or our FREEDOME VPN service, does not fall under the implementation. To learn more, see Chapter 19 section 157 of the Finnish Information Society Code.

1.6 What is the difference between FREEDOME VPN and

Internet Security?

F-Secure FREEDOME and F-Secure Internet Security are two different products although they do contain some similar functionality.

FREEDOME VPN is designed to secure your network traffic and prevent online tracking. With FREEDOME VPN you can form a secure VPN connection to almost 30 locations worldwide. This way, for example your internet service provider cannot see what sites you visit or what you do on them.

You can find more information about F-Secure FREEDOME VPN at https://freedome.f-secure.com/ (https://www.f-secure.com/en/home/products/freedome).

Internet Security is a product that is designed to protect your device using various different methods. The feature set for Internet Security varies depending on whether you're using a Windows or Mac computer, or an Android or iOS device.

For example on Android, the Internet Security features include virus protection and banking protection as well as device location, locking and wiping features.

You can find more information about F-Secure Internet Security at https://www.f-secure.com/en/internet-security (https://www.f-secure.com/en/internet-security).

To find out the differences between the various F-Secure home products, visit https://www.f-secure.com/en/compare (https://www.f-secure.com/en/compare).

1.7 Where can I get the latest news and updates on FREEDOME VPN?

Visit our official F-Secure FREEDOME VPN Twitter feed.

The most recent news is always available from our official Twitter feed: https://twitter.com/FSecure (https://twitter.com/FSecure).

2. Installing the app

This chapter describes how to install F-Secure FREEDOME VPN on your device.

2.1 Installing and activating the app on Android devices

This topic describes how to install and activate F-Secure FREEDOME VPN on your Android device.

This information applies to you if you have a standalone version of the F-Secure FREEDOME product.

> **Note:** When you take FREEDOME VPN into use for the first time, you must have your own personal My F-Secure account. For more information about My F-Secure, see Introducing My F-Secure (https://help.f-secure.com/product.html#home/total-windows/latest/en/concept_BDF118D8B14243049C8CCE03F0338814-latest-en).

1. Log in to your **My F-Secure** account. If you don't have a My F-Secure account yet, create the account as follows:
    a. On your web browser, go to the My F-Secure (https://www.f-secure.com/en/home/login) login page, select **Create new account**. Alternatively, you can create your My F-Secure account directly after purchasing FREEDOME VPN from our webstore by selecting **Create an account for My F-secure**.
    b. Fill in your name and email address in the relevant fields.

Make sure that you enter your email address correctly, as this address is used as part of your login credentials.

c. Create a strong password or passphrase.

d. Select **Accept and create account**.

e. To complete your account creation, open your email inbox and in the **Activate your F-Secure account now** email, select the link to confirm your email address for your account.

You will also receive a "Get started with F-Secure FREEDOME" email with instructions for installing the app.

2. On your Android device, open **Play Store**, and search for F-Secure FREEDOME VPN.
3. Select **FREEDOME VPN**.
4. Select **Install**.

   The app downloads and installs.

5. Select **Open**.

   When you install the app for the first time, the app goes through a short introduction.

6. Swipe the screen to the left until you get to the last page with the following options:

   - **Start using Freedome**
   - **Log in**

7. Select **Log in**.
8. Select your account provider.
9. Enter your account email address and password, and then select **Log in**.
10. Give the device a name and select **Continue**.
11. Select **OK** > **Start using FREEDOME** > **Accept**.
12. Choose your preferred network connection.

    FREEDOME VPN is now ready to protect your privacy.

13. Touch the center of the screen. When FREEDOME VPN is started for the first time, you will need to allow Android to make a VPN connection. Allow this by selecting **Let's do it** > **OK** .

FREEDOME VPN is now ready to protect your privacy online.

2.1.1 How do I check that FREEDOME VPN is installed on my Android device?

This topic explains how to check that the app is successfully installed on your device.

Once you have successfully installed FREEDOME VPN on an Android device, the FREEDOME icon appears among your other app icons. It appears both on your Home screen and on the Apps list.

2.2 How do I install FREEDOME VPN on an Android TV?

This topic describes how to take FREEDOME VPN into use on your Android TV.

Android TV is a smart TV operating system based on the Android OS.

> **Note:** There are quite a few Android TV products on the market, so the instructions below do not necessarily apply to all TV models. Consult your TV's manual for device-specific instructions on how to install apps on your Android TV.

FREEDOME VPN supports Android version 6.0 or later on Android TV.

To install FREEDOME VPN on your smart TV:

1. From the Home screen of your TV, scroll to **Apps**.
2. Select **Google Play Store**.
3. In the **Search** box at the top of the screen, enter `F-Secure FREEDOME VPN`.
4. Select the app to see details about the FREEDOME VPN app.
5. Select **Install**.

   The app downloads and installs.

Apart from protecting your anonymity online with a secure VPN connection, the FREEDOME VPN app also lets you access your favorite streaming services if allowed by the service provider.

2.3 Activating your FREEDOME VPN license bought from your internet service provider

This topic describes how to activate your FREEDOME VPN license if you have bought the app from your internet service provider (ISP).

> **Note:** This does not apply to you if you have bought a standalone version of the FREEDOME VPN app through Google Play Store, Apple App Store or through F-Secure's webstore or a reseller.

If you have bought your FREEDOME VPN app from your ISP, you can activate the app via the **Log in** button on the **Subscription** page.

To activate the license, do as follows:

1. Open FREEDOME VPN.

2. Tap the main menu in the top-left corner of the screen and select **Subscription**.
3. Under **All platforms**, select **Activate**.
4. Tap the **Log in** button.
5. Enter the email address and password that you have obtained from your ISP.

Your FREEDOME VPN license has now been activated.

> **Note:** If you log out from the subscription, it will discontinue and free up the FREEDOME VPN license on your device.

3. Subscriptions

This chapter provides information about the subscription options for F-Secure FREEDOME VPN.

FREEDOME VPN offers a free 5-day trial for the first-time users with the annual subscription. Once the trial expires, you need to convert the trial subscription to a paid subscription to continue keeping your browsing private and staying safe from hackers, trackers, and intrusive companies.

Multi-platform subscriptions

The multi-platform subscription covers all your devices running on Android, iOS, Mac, and Windows. It is available on our webstore as a standalone subscription or from an F-Secure reseller.

F-Secure webstore	On F-Secure webstore (https://www.f-secure.com/en/vpn), FREEDOME VPN is available for Android, iOS, macOS and Windows devices. We offer several different subscription options to cover all your devices from mobile

devices to laptops and desktops. FREEDOME VPN is available as a 12-month subscription for different license sizes.
Towards the end of the purchase process, as soon as you have confirmed your payment, you are guided to create your My F-Secure (https://www.f-secure.com/en/home/login) account. Once you have created the account, you can start installing your FREEDOME VPN product on your devices.
We offer a 30-day money back guarantee for all purchases made on the F-Secure website.

F-Secure reseller You can purchase FREEDOME VPN from any of our resellers. You can find the subscription code (account ID for iOS devices) in the product box. Before you can start using the product, you must create a My F-Secure (https://campaigns.f-secure.com/freedome/install/) account, log in to the account and convert the subscription code (account ID for iOS devices) into usage time.

App store subscriptions

Google Play Store The Google Play store (https://play.google.com/store/apps/details?id=com.fsecure.freedome.vpn.security.privacy.android) subscription is limited to the Android operating system, but is valid on all your devices connected to the your Google Play user account.
The app store subscription gives you flexibility in changing your subscription options, for example between either a fixed-term or auto-renewable subscription.
To cover both iOS and Android platforms, you need to make separate subscriptions in the respective app stores. The pricing of the app store subscriptions is optimized for use on a single platform.

Apple App Store The Apple App Store (https://apps.apple.com/fi/app/f-secure-freedome-vpn/id771791010) subscription is limited to the iOS operating system, but is valid on all your devices connected to the same Apple ID.
The app store subscription gives you flexibility in changing your subscription options, for example between either a fixed-term or auto-renewable subscription.
To cover both iOS and Android platforms, you need to make separate subscriptions in

the respective app stores. The pricing of the app store subscriptions is optimized for use on a single platform.

3.1 Renewing your subscription

This topic provides information about the renewing of your FREEDOME VPN subscription.

> **Note:** If you already have a My F-Secure account, log in to the account, select **Renew now** and follow the on-screen instructions.

If you don't have a My F-Secure account yet, follow the notifications in the app to renew FREEDOME VPN or go to the FREEDOME VPN renewal page (https://www.f-secure.com/en/vpn/renew) on our website. During the renewal flow, you will be guided to create your My F-Secure account.

If you have a valid subscription code and don't have a My F-Secure account yet, create an account (https://my.f-secure.com/register/freedome-default/), log in to the account and enter your subscription code to activate your licenses. Your devices with already-installed FREEDOME VPN will become visible in the My F-Secure portal after you log in to My F-Secure on each device having the FREEDOME VPN app:

1. On each device, open the FREEDOME VPN app.
2. Select **Subscription** > **Log in**.
3. Enter your account credentials.

> **Note:** If you have not completed the above steps before the subscription expires, your devices will no longer be protected until you log in to your My F-Secure account via the FREEDOME VPN app **on each device**.

3.2 What is My F-Secure

My F-Secure is the home of your protection.

It is the management portal for all the devices that are protected with your subscription. Apart from managing your FREEDOME VPN product, all subscription-related information is available in the portal.

The portal shows when your subscription expires and how many free licenses you have left. If your subscription is about to end or you have run out of licenses, you can extend your subscription or buy more licenses through the portal.

Through My F-Secure, you can also share your licenses with other family members and friends by inviting them to your My F-Secure group.

For more information about My F-Secure, see Introducing My F-Secure (https://help.f-secure.com/product.html#home/total-windows/latest/en/concept_BDF118D8B14243049C8CCE03F0338814-latest-en).

3.3 What happens to my anonymity if I have to create an account?

VPN services cannot make you fully anonymous, but they do improve your privacy and security online.

With F-Secure FREEDOME VPN, you can encrypt your data traffic and hide your real IP address. We don't read your traffic, nor do we know what traffic is yours. We don't share nor sell any of your traffic.

We respect your privacy and only process personal data needed to provide our services and to communicate with you. We don't share your My F-Secure account information with third parties.

The information you enter to purchase FREEDOME VPN, such as payment card details, is handled by the online store or app store provider. These third-party resellers' privacy policies apply to the actual purchase and related activities. F-Secure does not have access to your payment information. For more information, see F-Secure FREEDOME VPN Privacy Policy (https://www.f-secure.com/en/legal/privacy/consumer/freedome).

3.4 Switching from F-Secure TOTAL subscription to FREEDOME VPN subscription

If your FREEDOME VPN subscription comes with the F-Secure TOTAL subscription and the TOTAL subscription expires, there is a 9-day grace period to allow for normal renewal of the F-Secure TOTAL subscription.

During this grace period, FREEDOME VPN remains expired and cannot be used unless renewed still as F-Secure TOTAL. You are able to switch to and activate your FREEDOME multi-platform subscription after the grace period is over.

If you don't intend to renew your F-Secure TOTAL subscription but want to continue using FREEDOME VPN, you need to create a My F-Secure (https://my.f-secure.com/register/freedome-default/) account for your FREEDOME VPN, log in to the account and select **Buy now** to get your new FREEDOME VPN subscription.

> **Important:** We recommend that you first delete the account that you created for F-Secure TOTAL and then create the new account. In this way, you will be able to use your current email address as the username for the new account.

Also, you need to log out from your old account on each device that has FREEDOME VPN installed as follows:

1. Open the F-Secure FREEDOME VPN app.
2. Select the main menu in the top-left corner.

3. Select **Settings** > **Log out** > **Log out**.

This will end your F-Secure TOTAL subscription on your device. You can now install FREEDOME VPN through the My F-Secure portal.

3.5 App store subscriptions

In-app purchases in F-Secure FREEDOME VPN allow you to subscribe to the service via the app stores.

App store subscriptions are limited to one operating system, but are valid on all your devices connected to the same user account, for example your Google Play account or Apple ID. The app store give you flexibility in changing your subscription options, for example between either an annual or monthly auto-renewable subscription.

To cover both iOS and Android platforms, you need to make separate subscriptions in the respective app stores. The pricing of the app store subscriptions is optimized for use on a single platform.

3.5.1 Upgrading to a multi-platform subscription

This topic describes how to upgrade your app store subscription to a multi-platform one.

If you have a valid, auto-renewable app store subscription and want to upgrade to a multi-platform subscription, you first need to cancel your app store subscription.

> **Note:** Even though the subscription is canceled, the auto-renewable app store subscription remains valid until the end of the original subscription period. Once the app store subscription expires, FREEDOME VPN notifies you about it. You can get your multi-platform subscription either from F-Secure webstore or from any

> of our resellers. If you purchase F-Secure TOTAL, in addition to FREEDOME VPN, you also get F-Secure SAFE and ID PROTECTION in the same subscription. You are requested to create a My F-Secure account. A subscription code is no longer needed to activate the product.

To cancel the auto-renewable app store subscription, read the following instructions:

- Google Play Store (https://support.google.com/googleplay/answer/7018481?co=GENIE.Platform%3DAndroid)

3.6 Subscription-related FAQs

This section provides answers to the most frequently asked subscription-related questions.

3.6.1 What if I still have a valid subscription code?

If you have a valid subscription code, you can continue using the code on the devices that you have already activated until the subscription expires.

If you wish, you can immediately create a My F-Secure (https://my.f-secure.com/register/freedome-default/) account and then convert the subscription code into usage time.

However, if you have a subscription code and want to use FREEDOME VPN on a **new device**, you must create the My F-Secure account immediately and then log in to your account to convert the subscription code into usage time.

To convert the subscription code into usage time:

1. Create a My F-Secure (https://my.f-secure.com/register/freedome-default/) account.
2. When prompted, enter your subscription code.

3. Open the FREEDOME VPN app.
4. Select **Subscription** > **Log in**.
5. Enter your account credentials.
6. Repeat steps 3-5 on each device having the FREEDOME VPN app.

3.6.2 Can I transfer a subscription bought through an app store to Windows or Mac?

You cannot transfer an Android or iOS subscription purchased from Google Play store or Apple App Store.

The Android and iOS subscriptions are handled in their respective app stores, and they cannot be changed to multi-platform subscriptions. However, F-Secure offers multi-platform subscriptions which include a subscription for both desktop and mobile devices.

For more information on multi-platform subscriptions and their prices, see page https://www.f-secure.com/en/vpn (https://www.f-secure.com/en/vpn).

If you decide to move to a multi-platform subscription, you must first cancel your current Android or iOS subscription before its renewal time. Cancel the current subscription, including the initial free trial, through the account that you used when you subscribed to the service. Otherwise, Google Play store or Apple App Store will continue charging you for the subscription. For more information about the Google Play and Apple App Store subscription processing, visit the following webpages:

- Subscriptions on Google Play (https://support.google.com/googleplay/answer/2476088?hl=en) (Google Play store)
- Manage your auto-renewing subscriptions (https://support.apple.com/en-us/HT202039) (Apple App Store)

3.6.3 How does the FREEDOME VPN license period work?

This topic describes when the license period for FREEDOME VPN starts.

The license period for a multi-device subscription for FREEDOME VPN starts the moment you buy the product from F-Secure webstore or if you have bought FREEDOME VPN from one of our resellers, the license period starts as soon as you enter the subscription code in the My F-Secure portal.

3.6.4 How does FREEDOME VPN work with multiple user accounts on the same device?

Due to certain limitations in operating systems, FREEDOME VPN subscription allocation and configuration work differently if multiple user accounts are used on the same device.

Below are the scenarios in which FREEDOME behaves differently:

Windows & Mac

- The license is shared between all user accounts; one subscription covers all the user accounts.
- The settings are shared between all the user accounts; every user can change the settings and turn the product on or off.
- When a VPN connection is already active on a user account, this connection is taken into use by all other user accounts on the device.

Android

- The license cannot be shared between different user accounts; each user account requires its own subscription.

- The settings are not shared between user accounts; all user accounts are independent of each other and the settings and configuration on one particular user account do not affect other users on the device.
- Each user account is isolated. VPN connection is not shared with other users on the device.

iOS

Apple iPhones and iPads are not affected as the iOS operating system does not support multiple user accounts.

3.6.5 What happens after the free FREEDOME VPN trial expires?

This topic describes what happens when the free FREEDOME VPN trial is over.

Once the initial 5-day trial expires, you need to convert the trial into a paid subscription.

If you have purchased FREEDOME VPN from Google Play, you can have FREEDOME VPN installed on all your devices as long as these devices are registered to the same Google email address (Google Play).

If you have purchased FREEDOME VPN from the F-Secure web store or a retailer, you can install the product on different devices running on various platforms without the Google Play or Apple App Store limitations. However, you cannot install the product on more devices than what your subscription allows.

3.6.6 How can I buy FREEDOME VPN from Google Play after a trial?

This topic describes how to buy FREEDOME VPN after the trial.

Buy FREEDOME VPN and continue using it after your trial period has finished as follows:

1. Open FREEDOME VPN.
2. Select the main menu in the top-left corner.
3. Select **Subscription** > **FOR ANDROID DEVICES**.
4. Choose the subscription of your choice: either a monthly or yearly plan.
    - monthly plan
    - yearly plan
5. Follow the purchase instructions on your device.

4. Virtual location

With FREEDOME VPN, you can hide your IP address for an extra layer of privacy.

When you connect to the internet, your device is assigned an address that identifies where you are. With FREEDOME VPN, you can choose an IP location - a virtual location - in another country. This gives your device an address in the selected country, and you may face less geo-restrictions than you might otherwise encounter.

When you select the virtual location that is closest to where you are, you get the best possible network connection.

On Android devices and desktop computers, you can set FREEDOME VPN to use automatically the virtual location that is closest to you.

> **Note:** Even with location services turned off, your device still knows its actual location, and your apps may have

permission to use it.

4.1 What are the virtual locations for FREEDOME VPN?

Virtual location protects your privacy and lets you access your favorite streaming services when abroad.

When you connect to the internet, your device is assigned an address that identifies where you are. FREEDOME VPN lets you select a virtual location which gives your device an address in the selected country. In automatic mode, FREEDOME VPN uses a server that is closest to you for the best possible network connection and speed.

> **Note:** Your device will still know its real location, even without GPS, and apps may have permission to use it.

FREEDOME VPN currently provides the following virtual locations to choose from:

- Australia
- Austria
- Belgium
- Canada (Montreal, Toronto and Vancouver)
- Czech Republic
- Denmark
- Finland
- France
- Germany
- Ireland
- Italy
- Japan
- Mexico

- Netherlands
- Norway
- Poland
- Singapore
- Spain
- Sweden
- Switzerland
- United Kingdom
- USA (East coast, Northwest, South, Southeast and West coast)

More locations will be added in the near future.

4.2 Changing your virtual location

Using a virtual location protects your privacy and lets you access your favorite streaming services when abroad.

By default, FREEDOME uses the server that is closest to you for the best possible connection.

Companies use IP geolocation to block users in certain countries from accessing their content. With FREEDOME VPN, you may be able to go around some of them by changing your virtual location in the following way:

1. Open the app.
2. Select the **Location** button.
3. Select **Other locations**.

   A list of all the locations opens.
4. Select the virtual location that you want.

Your device may still know its real location through GPS, and apps may have permission to use it.

4.3 Why does my IP address seem to be in a different country than expected?

This topic explains why your IP address may seem to be in a different country than expected.

With F-Secure FREEDOME VPN, you can select the location through which all your network traffic is routed. For example, if you are located in Germany, but select Finland as the virtual location in FREEDOME VPN, all your traffic is routed through our gateway servers in Finland.

There are Geolocation or GeoIP services on the internet, such as https://www.whatismyip.com/ (https://www.whatismyip.com/), which try to determine the location of your IP address as you access them. Usually this works fine. In our above example case, the German user would see that the connection is coming from Finland with such a service.

However, these services don't always work as expected, as geolocating IP addresses is not always reliable. Sometimes the IP addresses in question may be owned by multi-national companies; for example, a Dutch company may own IP addresses which are located in Japan. There are multiple different GeoIP database providers who try to map the IP addresses to different countries and cities, but these databases are not comprehensive and may not have the correct information to begin with. The IP addresses in our Japan example may still show up as Dutch IP addresses according to the GeoIP services.

All the virtual locations available for F-Secure FREEDOME VPN are located in the countries shown in our user interface, even if a GeoIP service may suggest otherwise.

5. Blocking harmful web sites

While you browse the web, FREEDOME VPN checks the sites that you go to and makes sure that they are safe.

Browsing protection blocks web sites that may contain harmful content or steal your personal information, including credit card numbers, user account information, and passwords.

While you browse the web, FREEDOME VPN checks the HTTP sites that you go to and makes sure that they are safe. You will see a notification whenever FREEDOME VPN blocks a site.

On the main view of the app, you can check FREEDOME VPN's browsing protection statistics to see how many harmful sites the app has blocked.

5.1 What to do when a site is blocked?

If browsing protection blocks a site, most likely the site or service that you are trying to access is either malicious or is trying to track you.

Some sites prevent their use altogether if they are not able to set up the tracking first.

If you cannot access a site or service that works when FREEDOME VPN is turned off, you can try to turn tracking protection off when you are accessing that site.

> **Important:** If you turn tracking protection off, at the same time you allow that site and its affiliates to track your online behavior.

You may also try to turn browsing protection off if you trust that the site in question is safe.

> **Important:** Turning browsing protection off considerably weakens the security of your web browsing.

On FREEDOME VPN, when you turn protection on, browsing protection is turned on by default. To turn browsing protection off:

1. Open the app.
2. Swipe the screen down and tap **Browsing protection on**.
3. Select the switch to turn browsing protection off.

> **Warning:** Now you are not protected against suspicious and harmful websites.

To turn browsing protection on again, repeat the above steps.

5.2 Blocking harmful web sites doesn't work with Chrome's Lite mode or with Opera Mini

The browsing protection and tracking protection features won't work with Chrome's Lite mode turned on, nor with Opera Mini.

Google Chrome's Lite mode (previously known as Data Saver) compresses web pages to make them load faster and to create less data traffic. Opera Mini works in a similar fashion. This prevents FREEDOME VPN's browsing protection and tracking protection from working because the compression prevents FREEDOME VPN from checking the traffic.

Although browsing protection and tracking protection won't work with Chrome's Lite mode (or Data Saver) turned on, or with Opera Mini, FREEDOME VPN will still secure the traffic from these browsers by encrypting it and sending it through the virtual location you've selected to use.

Chrome's Lite mode (or Data Saver) can be turned off from the Chrome settings after which the browsing protection and tracking protection features will resume working. The exact name of the setting depends on the operating system version and device platform. The relevant setting can be found in Chrome's setting menu.

Unfortunately, this can't be configured on Opera Mini.

6. Preventing web sites from tracking you

Tracking protection ensures privacy while you browse the web and use apps.

When you go to a web site or use an app that tries to track you, FREEDOME VPN hides your IP address, blocks tracking cookies and prevents apps from sending information about you to data collection sites.

Tracking protection removes all cookies set by known advertising networks, preventing the ad networks from tracking individual visitors from site to site. It also prevents all HTTP traffic from and to what F-Secure's reputation analysis identifies as a tracking domain, and forces the "Do Not Track" header on for all browsing.

Some of your browsing happens over encrypted communications (HTTPS/TLS/SSL), and in those cases FREEDOME VPN cannot decrypt the communications and remove the tracking cookies.

FREEDOME VPN does not block anything going from your browser to the site you're visiting, as for example blocking cookies from the site you visit easily breaks login sessions, stored preferences and other valuable features. In addition, FREEDOME VPN does not block any tracking from HTTPS traffic because that would require a man-in-the-middle attack against the HTTPS, and the related security risks outweigh the possible privacy gains.

The anti-tracking statistics in FREEDOME VPN currently only show the total amount of web (HTTP) requests that were either blocked or had their cookies filtered to prevent tracking. We are not able to provide more accurate data about what was blocked to our users since we do not log any traffic for privacy reasons. However, you can use FREEDOME VPN's Tracker Mapper to see how you are being tracked. Tracker Mapper allows you to temporarily log visited web sites to see how they are tracking you.

6.1 Turning tracking protection off

On FREEDOME VPN, when you turn protection on, tracking protection is turned on by default.

If, for some reason, you want to turn tracking protection off, you can do it as follows:

1. Open the app.
2. Swipe the screen down and tap **Tracking protection on**.
3. Select the switch to turn tracking protection off.

> **Warning:** Now your privacy is not protected against hackers, advertisers, and data collection companies.

To turn tracking protection on again, repeat the above steps.

6.2 Tracker Mapper

You can see how you are being tracked with FREEDOME's Tracker Mapper.

Tracker Mapper allows you to temporarily log visited web sites to see how they are tracking you, as well as malicious sites blocked.

FREEDOME never logs your data. However, you can choose to do so yourself by using Tracker Mapper to record your tracking data for up to 24 hours.

Any existing log you make will be deleted permanently once you start a new one or three days after you stop recording.

> **Note:** For your own security, we do not block tracking from HTTPS sites. This is why sites, such as Facebook won't show on the log.

6.2.1 Using Tracker Mapper

Tracker Mapper allows you to temporarily log visited websites to see how they are tracking you.

> **Note:** For your own safety, we don't block tracking from HTTPS sites.

To see how you are being tracked, start a 24-hour log as follows:

1. Open the app.
2. Swipe the screen up and tap **Tracking attempts blocked**.
3. Select **Show Tracker Mapper**.
4. Select **Start**.

   Tracker Mapper is now running.
5. You can stop logging at any time by selecting **Stop logging** > **Stop** from the top-right menu of the **Tracker Mapper** view.

   The log results, if any, are displayed on the **Tracker Mapper** view. If you wish you can also export or delete the log by using the options on the top-right menu.

6.3 How are the tracking cookies and sites blocked with FREEDOME VPN?

This topic describes how the tracking cookies and sites are blocked with FREEDOME VPN.

F-Secure Labs maintains a database of tracking and advertisement networks in the F-Secure Security Cloud. Our labs are staffed round-the-clock ensuring this database is always up-to-date. The database tags tracking and analytics services so that FREEDOME VPN blocks the requests completely. The effect is that advertisements are still shown but without any targeting.

6.4 Why can't I access a certain site or service when FREEDOME VPN is on?

This topic explains why FREEDOME VPN is not allowing you to access a site or service.

Most likely the site or service that you are trying to access is either malicious or is trying to track you. Some sites prevent their use altogether if they are not able to set up the tracking first.

If you cannot access a site or service that normally works when FREEDOME VPN is turned off, you can try to turn tracking protection off when you are accessing that site. Note, however, that at the same time you allow that site and its affiliates to track your online behavior.

You may also try to turn browsing protection off if you trust that the site in question is safe. Note, however, that this considerably weakens the security of your web browsing.

If you think that we have detected something, such as a file, URL or app, incorrectly as unsafe, you can ask us to analyze it at https://www.f-secure.com/en/support/submit-a-sample (https://www.f-secure.com/en/support/submit-a-sample).

7. Network and connections

This chapter provides information about network-related topics about F-Secure FREEDOME VPN.

7.1 Automatic WiFi protection

This topic provides information about the automatic WiFi protection in FREEDOME VPN.

When on the go, you don't need to worry about forgetting to turn on VPN. You can set FREEDOME VPN to turn on automatically whenever your device connects to an untrusted WiFi. This protects your anonymity and ensures your privacy on public WiFi networks.

To turn VPN on automatically:

1. Make sure that you are connected to the WiFi network.
2. Open FREEDOME VPN.
3. From the main menu in the top-left corner, select **Settings**.
4. Under **Connection**, enable **Automatic WiFi protection**.

From now on, VPN will be turned on automatically as soon as your device connects to an untrusted network.

> **Note:** When entering a WiFi network that you have marked as trusted, VPN will not be turned on even if you have **Automatic WiFi protection** enabled.

7.2 Trusted WiFi networks in FREEDOME VPN

This topic provides information about trusted WiFi networks in FREEDOME VPN.

With FREEDOME VPN, you can mark your favorite local networks as trusted to allow connections to other devices, such as media players, while VPN is turned on. This feature works only when the Killswitch feature is enabled. If Killswitch is disabled, you can access your local network without marking the network as trusted.

If you enable automatic WiFi protection for untrusted WiFi networks, FREEDOME VPN will not turn on when entering a trusted network.

To mark the local WiFi network as trusted:

1. Make sure that you are connected to the WiFi network.
2. Open FREEDOME VPN.
3. From the main menu in the top-left corner, select **Settings**.
4. Under **Connection**, select **Trusted WiFi networks**.

   The **Trusted WiFi networks** view opens, listing the current WiFi networks available.
5. From the list of networks, select your WiFi network.

> **Note:** If you cannot see your current network on the page, make sure that you are connected to the WiFi network.

Your local network has now been marked as trusted.

You can read more information about the Killswitch feature here (https://help.f-secure.com/product.html#home/freedome-windows/latest/en/id_110707-latest-en).

7.3 Setting apps to connect directly to the internet

If you wish, you can set apps to bypass FREEDOME VPN's protection features.

All installed apps are immediately scanned for viruses and other risks automatically. If FREEDOME VPN has not detected anything suspicious risks in the app, you can set it to connect to the internet directly. Use this feature cautiously.

1. Open FREEDOME VPN.
2. From the top-left main menu, select **Settings** > **Apps bypassing VPN**.

   The **Manage apps** view opens.
3. Select the apps that you allow to connect to the internet directly, bypassing FREEDOME's protection features.

7.4 Killswitch functionality in FREEDOME VPN

A feature which blocks internet access when FREEDOME VPN connection is disrupted or being established.

F-Secure FREEDOME VPN includes a killswitch feature to prevent accidental leakage of traffic to the internet.

Should the VPN connection between the FREEDOME VPN client and the server drop for any reason, for example due to a short network outage or while changing from one FREEDOME VPN site to another, the FREEDOME VPN killswitch will notice this. Depending on the settings, it may block the network traffic until the connection to the FREEDOME VPN backend has been established again. In this scenario, only the mandatory network traffic is allowed. In other words, apart from the OpenVPN or IPSEC protocol itself, only the traffic that is required to establish the VPN connection, such as DNS and DHCP, is allowed.

If the user turns off FREEDOME VPN, it will not trigger the killswitch feature. Instead, the network traffic will work normally but naturally not protected by FREEDOME VPN.

There are minor differences in how the killswitch works on different operating systems.

On Android devices, the killswitch feature is turned ON by default.

However, if there is a captive portal in the network (for example a hotel WiFi with a login page) and FREEDOME VPN detects it, traffic will be allowed only to the captive portal and after the authentication, to the FREEDOME VPN backends.

> **Note:** Some Huawei devices running on Android 8 and 8.1 have a firmware bug that in some rare cases may cause a momentary traffic leak outside the VPN tunnel during the VPN connection phase regardless of the killswitch setting.

7.5 Blocked ports with FREEDOME VPN

With F-Secure FREEDOME VPN, some ports are blocked for both the TCP and UDP protocols.

F-Secure FREEDOME VPN allows virtually all of the network traffic to pass through. However, to increase security and prevent certain abusive behavior, such as spamming, some ports are blocked for both the TCP and UDP protocols.

Blocked TCP ports:

- 1-19
- 25
- 67-69
- 139
- 445

Blocked UDP ports:

- 0-1024
- 1900 (both source and destination ports)

Blocking of these ports should not prevent normal internet usage. The only exception can be TCP port 25 which is used for the SMTP mail sending protocol. Web-based email services, such as Gmail and Hotmail, are not using SMTP for mail sending, and thus work normally without any special configuration. In the case of a corporate mail service or mail service from an internet service provider, it may be necessary to change the mail client's settings. For more information about the needed changes, see the related topic about sending emails when FREEDOME VPN is turned on.

At some locations, FREEDOME VPN also blocks BitTorrent. See the related topic about BitTorrent to find out these locations.

Note also that although the UDP ports 53 (DNS, domain name system) and 123 (NTP, network time protocol) are blocked, the services are available as they are provided within FREEDOME VPN itself.

7.6 Sending emails when FREEDOME VPN is turned on

When you use F-Secure FREEDOME VPN, you may notice that you are unable to send email any more, although you can still read email normally.

Email is typically sent via a protocol called SMTP (Simple Mail Transfer Protocol). To prevent malicious users from using the mail servers as spam relays, virtually all Internet Service Providers (ISP) do not allow email to be relayed using their mail servers except when the email is coming from the ISP's own network.

When you are using F-Secure FREEDOME VPN, all the network traffic (including the email you send) is routed through the virtual location you've selected. Because of this, the email you send comes from the internet to the ISP, and the ISP will normally block it. You may see an error message, such as "Email relaying denied".

To fix this problem, you may need to change some of the following email sending settings on your device:

- Most of the ISPs allow email from the internet when you use the encrypted version of the SMTP protocol; for example, SMTPS. With SMTPS, you are able to authenticate to the ISP's mail server.
- The normal SMTP protocol port is 25, while SMTPS port is by default 465 or 587. You may simply try only changing the SMTP port number in your email configuration and see if that helps.
- If the port change was not enough to get email working, please consult your ISP's documentation or support pages for instructions on what settings you need to change on your device. As this is a ISP specific configuration change, we are unable to give detailed instructions that apply to all our users.

7.7 Is BitTorrent allowed with FREEDOME VPN?

Some of our VPN gateway sites do not support BitTorrent.

Due to requirements placed on us by the Digital Millennium Copyright Act (DMCA) legislation, we are not able to support BitTorrent or other peer-to-peer file sharing applications on many of our gateway sites, which either reside within the United States, or are hosted by a company based in the US.

Given our promises on privacy and anonymity, honoring the DMCA requirements is challenging for us. We have therefore chosen to technically block peer-to-peer file sharing on the affected VPN gateways. When such traffic is detected by our software, the VPN user's network connection is temporarily restricted by a firewall, leaving only web (http/https) services available for that client, and with limited capacity only. Other applications may obviously be affected by the restrictions. The restrictions are automatically lifted after a few hours time.

While BitTorrent is a perfectly good and legal protocol as such, and it is often used for legitimate purposes, it is most commonly used for downloading and sharing copyrighted material, such as movies. We are, however, not technically able to detect between legal and illegal uses of BitTorrent.

Gateway sites currently limited by this restriction:

- Australia
- Canada

- France
- Germany
- Italy
- Japan
- Mexico
- Netherlands
- Poland
- Singapore
- United Kingdom
- United States

7.8 FREEDOME VPN and WebRTC IP address leakage

FREEDOME VPN cannot prevent IP address leaking through WebRTC.

Web Real-Time Communication (WebRTC) is an application programming interface (API) that is widely used in various pluginless applications. These days virtually all web browsers support WebRTC.

WebRTC includes a method for the web server to request the local IP address through the user's web browser or some other application. This way the server may obtain the original IP address of the user's computer as long as the user's browser or other application supports WebRTC.

A VPN solution, such as FREEDOME VPN or its competitors, can not disable WebRTC within the web browser. At best, we could inspect all JavaScript code coming from a web server and break the WebRTC code. However, if the web server is a TLS/SSL protected https server, all Javascript is encrypted while it is being downloaded from the web server to the browser and it is impossible for FREEDOME VPN to inspect that. The code may also be obfuscated or compressed, making it difficult to reliably detect WebRTC. Therefore, it is not technically possible to block WebRTC with FREEDOME VPN.

To prevent WebRTC IP address leakage, you must disable WebRTC in the web browser or other application using the WebRTC API. Unfortunately, this is not possible with all applications.

Here are some ways to disable WebRTC with Chrome and Firefox web browsers:

Chrome:

Use the official webrtc.org extension WebRTC Network Limiter: https://chrome.google.com/webstore/detail/webrtc-network-limiter/npeicpdbkakmehahjeeohfdhnlpdklia (https://chrome.google.com/webstore/detail/webrtc-network-limiter/npeicpdbkakmehahjeeohfdhnlpdklia).

Alternatively, you can find settings to control WebRTC (among some other settings) by typing this in the location bar: chrome://flags/#disable-webrtc (chrome://flags/#disable-webrtc)

Firefox:

Type "about: config" in the location bar and change the media.peerconnection.enabled setting to "false".

7.9 Using Chromecast with FREEDOME VPN

It is possible to use Chromecast with FREEDOME VPN on your devices.

When you use Chromecast with FREEDOME VPN, you must use screen mirroring. If you're casting the content, what actually happens is that your device sends the link to the content to your Chromecast device. Then, the Chromecast device downloads the content from that link. In this way, it totally bypasses your device with FREEDOME VPN.

With Android, to allow Chromecast to connect to your Android device via the local network, you need to set your Wi-Fi network as a trusted Wi-Fi network in the following way:

1. Make sure that you are connected to your Wi-Fi network.
2. Open FREEDOME VPN.

3. From the main menu in the top-left corner, select **Settings**.
4. Under **Connection**, tap **Trusted Wi-Fi networks** and select your network.

7.10 Connecting to your local networked devices when FREEDOME VPN is on

This topic describes what you need to do if you want to connect to your local networked devices when FREEDOME VPN is turned on.

With Android, you can set the local Wi-Fi network that you are connected to as a trusted network to allow connections to other devices within the local network in the following way:

1. Make sure that you are connected to your Wi-Fi network.
2. Open FREEDOME VPN.
3. From the main menu in the top-left corner, select **Settings**.
4. Under **Connection**, tap **Trusted Wi-Fi networks** and select your network.

7.11 Why does FREEDOME VPN require permission to access location information with the "Trusted Wi-Fi networks" feature?

From Android 10 onward, the "Trusted Wi-Fi networks" feature in F-Secure FREEDOME will require permission to access the location information.

FREEDOME VPN doesn't need information about the actual location. However, when FREEDOME VPN tries to define the network as trusted, it needs to obtain the network name from the Android operating system. Starting from Android 10, any app that requests the network name from the operating system needs to have the "Access location information" permission turned on.

If you deny the permission, you can't use the "Trusted Wi-Fi networks" feature in FREEDOME VPN but you can continue using all the other features in the product. Also, if you deny the permission, you will see the prompt again when you try to use this feature the next time. At that point you can also deny the permission permanently. To revert this, you must go to the Android settings and reset the permission from there.

> **Note:** If you upgrade your current Android operating system to version 10, the "Trusted Wi-Fi networks" feature only works once you have selected the **Trusted Wi-Fi networks** settings from FREEDOME VPN **Settings**.

7.12 Using your mobile device as a hotspot when FREEDOME VPN is on

You can use your device as a hotspot even if FREEDOME VPN is turned on.

You can use your Android or iOS device as a hotspot, i.e. share your device's network connection with your other devices when FREEDOME VPN is turned on. This is also known as tethering.

You can set up the hotspot on your device in the same way as you would set it up without FREEDOME VPN.

> **Warning:** The shared network connection cannot be secured with FREEDOME VPN on your phone or tablet; the network traffic from the other devices will bypass the FREEDOME VPN connection. Therefore we strongly recommend that you use FREEDOME VPN also on the other devices to ensure that also their network

connection is secured.

7.13 Can I use other VPN products at the same time with FREEDOME VPN?

It is not possible to use multiple VPN products simultaneously, and FREEDOME VPN is no exception. The reason for this is that the different VPN products will collide with each other trying to route the network traffic to different destinations. This may also cause the network traffic to leak outside of the VPN tunnel.

On a side note, it is possible to have multiple VPN products installed on a device as long as only one is turned on at a time.

7.14 Does DNS-over-HTTPS work with FREEDOME VPN?

DNS-over-HTTPS works with FREEDOME VPN but there are some further aspects to consider.

These aspects require some understanding of how DNS (Domain Name System) works in the first place.

DNS has been the standard way to convert computer and domain names into numerical IP addresses used by the networking devices on the internet. Regular DNS requests have been sent from the devices of a user to the DNS servers operated typically by internet service providers. In this way, it has been possible for the DNS server owner to learn what sites and services the user is accessing. Also, it has been easy for the DNS server owner to block access to certain addresses.

To overcome these, a protocol called DNS-over-HTTPS (DoH) was introduced. As the name implies, the DNS requests are sent over an encrypted HTTPS connection. Several large network companies, such as Cloudflare and Google, have started to offer their DoH service for free to anyone. This allows the DoH service provider, instead of the internet service provider, to obtain information of all the sites for all the users who use their DoH service.

When FREEDOME VPN is turned on, it will take over the traditional DNS requests and use its own DNS servers to resolve domain names into the IP addresses. The DNS requests are treated in accordance with FREEDOME's privacy policy (https://www.f-secure.com/en/legal/privacy/consumer/freedome (https://www.f-secure.com/en/legal/privacy/consumer/freedome)), and users can be sure that their data is not sold, for example for marketing purposes.

Normally, DNS-over-HTTPS passes through FREEDOME VPN just like any other HTTPS traffic, and it can be used instead of the DNS provided by FREEDOME VPN. FREEDOME VPN makes no difference between the regular HTTPS and DNS-over-HTTPS traffic. Note that DNS-over-HTTPS works within an application, typically a web browser. This limits the DNS-over-HTTPS protocol only to that particular application, and all DNS requests from other applications will go through the traditional DNS.

There is, however, at least one exception to this on Android: A popular app called Intra uses the DNS-over-HTTPS protocol, but it works technically as a VPN. There can't be multiple VPN products in use at the same time, so the Intra app cannot be used together with FREEDOME VPN.

The question about whether to use DNS-over-HTTPS or not is about who to trust. Both the DNS server owner and the DNS-over-HTTPS server owner will see all the destination addresses the user goes to. Depending on the agreement with the user, the DNS server owner may or may not be able to use that data for other purposes than just for translating domain names into IP addresses. Large-scale service offering DNS-over-HTTPS (or plain DNS) is expensive to run, so the companies operating seemingly free DNS-over-HTTPS services may have financial interests in the data they obtain from the users.

7.15 Does FREEDOME VPN communicate directly with the VPN server of each country?

Yes, FREEDOME VPN communicates directly with the VPN server in each virtual location. Going via additional countries would increase latency and reduce performance.

7.16 Does FREEDOME VPN intercept SSL/TLS traffic?

FREEDOME VPN does not intercept SSL/TLS traffic.

Intercepting and decrypting traffic would be a dangerous capability to have on our server. It can be seen as a breach of privacy.

7.17 Does FREEDOME VPN intercept tracking cookies or malicious files inside encrypted files?

No, F-Secure FREEDOME VPN cannot access a file that is encrypted.

7.18 Does FTP work with FREEDOME VPN?

Most FTP clients work with FREEDOME VPN.

FTP clients and servers work in two different modes: active and passive. To be able to use an FTP client with FREEDOME VPN, you must configure the FTP client to work in passive mode. Nearly all FTP clients can be configured in this way, and, in fact, many of them have nowadays the passive mode set as the default value.

7.19 How should I interpret Ookla Speedtest results with FREEDOME VPN?

This topic describes what things to consider when you measure your network speed with Ookla Speedtest.

If you are using Ookla Speedtest (http://www.speedtest.net/) to measure your network speed, take the following points into consideration:

- **Turn off the location services on your device.** Ookla Speedtest may use the location services to determine the closest server to you.
  If you have the location services enabled, it may result in, for example the following situation: Let's assume that you're currently located in Karlsruhe, Germany, and you've connected to the West Coast, USA, location with FREEDOME VPN. When you run Ookla Speedtest, it gets your real location in Karlsruhe, Germany, from your device's location services, and opts to that server. All the speed test traffic makes then the following kind of a round trip:

  a. VPN tunnel from Karlsruhe, Germany, to the West Coast, USA
  b. Public internet from West Coast, USA, to the Ookla Speedtest servers in Karlsruhe, Germany
  c. Public internet from Karlsruhe, Germany, to the West Coast, USA
  d. VPN tunnel from West Coast, USA, to Karlsruhe, Germany

  It is roughly 9 000 kilometers straight from Karlsruhe to our servers in the West Coast, USA, but it is safe to assume it's at least 13 000 kilometers through the cables - and almost certainly considerably more. In other words, it is a distance of over 50 000 km that your speed test traffic is making, through a large number of various

network devices.
According to the laws of physics, with the speed of light, 50 000 km translates into 166 milliseconds but even with fibre optic cables, it is only possible to get to approximately two thirds of the speed of light. This double round trip would therefore take at least 250 milliseconds, plus all the time spent in the various networking devices.

Based on the above, it makes a huge difference if the Ookla Speedtest server is close to the FREEDOME location you've selected to use, or if it is close to your physical location.

- **Ookla Speedtest often remembers what server it has used previously and will use the same server if you're doing multiple tests in a row.** Usually, you need to force the Ookla Speedtest app to stop to make the app select a new server to test with.
- **Ignore the packet loss percentage displayed by the Ookla Speedtest client.** The UDP-based protocol used by Ookla Speedtest is constructed so that it will trigger a certain protection feature in F-Secure FREEDOME VPN which in return will show up as around 70% packet loss in the Ookla Speedtest client. If there really was a 70% packet loss, the network connectivity wouldn't exist at all.

> **Note:** The UDP-based protocol used by Ookla Speedtest doesn't simulate real life network traffic, and thus it doesn't give an accurate view of the connection speed. The speed-critical services, such as video streaming or file transfer protocols, are typically totally different from the Ookla Speedtest's UDP protocol.

7.20 Why does my internet connection slow down with FREEDOME VPN?

This topic describes how your network traffic is handled when using FREEDOME VPN.

When you start using F-Secure FREEDOME VPN, your network traffic is handled in a very different way than before. FREEDOME VPN is a Virtual Private Network (VPN) product which takes over all the network traffic, encrypts it and routes it through the virtual location you've selected to use or which has been automatically selected by the product.

Without FREEDOME VPN, all your network accesses go directly to wherever you're trying to go.

As FREEDOME VPN encrypts and routes all your network traffic to whatever virtual location you're using, the distance in the network will bring some overhead to the observed network speed. In principle, the further the virtual location is network-wise, the longer it takes to transfer the data through there. Note that the data needs to come back through the same route. If you reside in, for example Sweden and select to use our Australian virtual location, all your network traffic will go through Australia even if you'd be reading a Swedish news site.

Sometimes the nearest virtual location may not be obvious, so it is worth trying different virtual locations if speed seems to be an issue. We're not imposing speed limitations on our users but if one of the virtual locations is used very actively by other users, it may slow down the network speed too.

Windows:

On Windows, FREEDOME VPN supports the following three VPN protocols: OpenVPN, OpenVPN (TCP) and IPSEC/IKEv2.

- OpenVPN is the default protocol in FREEDOME VPN. It works mainly over the UDP protocol and is usually faster than the OpenVPN over TCP protocol. However, OpenVPN over UDP may be blocked in some networks where OpenVPN over TCP is allowed.
- IKEv2 may achieve slightly higher connection speeds when compared to the two OpenVPN protocol versions, but especially some older routers may have problems with handling the IKEv2 protocol.

Mac:

On Mac, FREEDOME VPN supports both OpenVPN and OpenVPN (TCP) protocols. The same advantages and disadvantages of these protocols exist on both Mac and Windows.

Android:

On Android, FREEDOME VPN supports only the OpenVPN over UDP protocol.

iOS:

On iOS, FREEDOME VPN supports both IPSEC/IKEv1 and IKEv2 protocols. IKEv2 may achieve slightly faster speed than IKEv1 but the key reason for the two different IKE versions is that some routers work better with IKEv1 and some with IKEv2.

7.21 Location services on mobile devices may reveal your actual location even with FREEDOME VPN turned on

Apart form checking your IP address, content providers who utilize geoblocking may use also other means to detect your location.

One of the most commonly used methods is to utilize the mobile device's built-in location services. It works so that it gets your real location by using the satellite navigation (GPS), phone and Wi-Fi networks.

If your device's location services is turned on, it is not possible for an app such as FREEDOME to prevent others from using the service.

You can turn off the location services from your device settings in the following way:

Android: Settings > Connections > Location

> **Note:** The Location Services may be located in a different place in the settings for some Android versions. Please see your device documentation for the exact setting placement.

7.22 Port configuration for FREEDOME VPN

This topic lists the ports to be set up to connect to FREEDOME VPN.

In some cases, for example in your home network, you may have to configure and set up port access in order to connect to FREEDOME VPN.

On Android, macOS and Windows, FREEDOME VPN uses the OpenVPN protocol in the following ports:

- TCP/UDP ports in the range 2700 - 2800
- TCP port 443

> **Note:** Neither the protocol nor the ports are configurable.

7.23 What encryption does FREEDOME VPN use to secure the traffic?

FREEDOME VPN uses strong encryption to encrypt all the network traffic.

Below you can find the exact technical details of the encryption parameters used:

For Android, Mac and Windows / OpenVPN:

- Control channel: TLS, 2048 bit RSA keys with SHA-256 certificates, AES-256-GCM
- Data channel: AES-128-GCM

7.24 How can I turn off the FREEDOME VPN connection without the trust access being taken away?

This topic describes how to turn off FREEDOME VPN without the trust access being taken away.

When FREEDOME VPN creates a VPN connection for the first time, a dialog requesting you to trust the application is displayed. By trusting the application, you grant FREEDOME VPN access to intercept all network traffic. With some Android versions, when turning FREEDOME VPN off, the trust access granted may be taken away if FREEDOME VPN is turned off by using the **Disconnect** button displayed in Android's "active VPN" notification.

To turn off your FREEDOME VPN connection without the trust access being taken away, do the following instead:

1. Open the FREEDOME VPN app.
2. Tap **Protection ON** in the middle of the screen.

   Protection is now turned off.

When you turn FREEDOME VPN on again, your phone allows the connection automatically.

8. Troubleshooting

This section provides answers to frequently asked questions about F-Secure FREEDOME VPN.

If you cannot find an answer to your question here, check the problem solution articles in the FREEDOME knowledge base (https://community.f-secure.com/vpn-en/kb/vpn) or post your questions about the product to our discussion forum (https://community.f-secure.com/en/categories/vpn).

Finally, if none of the above helps in solving the issue, contact our customer support. Also, see the related topic below.

8.1 FREEDOME VPN installation fails with "unknown error" message

When installing or upgrading FREEDOME VPN, the installation may fail with a message saying "Installation failed with unknown error".

If you have F-Secure SAFE or F-Secure Internet Security installed on the computer, it is likely that the installation fails because of the product's Tamper protection feature, whose task is to prevent harmful applications from shutting down the product's core security processes, has accidentally prevented the FREEDOME VPN installation. To solve the issue, you need to disable the Tamper protection feature temporarily:

1. Open the F-Secure SAFE or F-Secure Internet Security user interface.
2. From the main menu in the top-left corner, select **Settings**.

   The **Settings** view opens.
3. As you need administrator rights to change the setting, select **Edit settings** and enter your admin credentials.
4. Under **Viruses & Threats**, scroll down to **Tamper protection** and disable the feature.

Once you have disabled the Tamper protection feature, run again the F-Secure FREEDOME VPN installation or upgrade. As soon as the installation or upgrade has completed successfully, enable Tamper protection again by following the above steps.

If the FREEDOME VPN installation fails also after performing the above steps, you probably need a separate fix to solve the issue. Contact F-Secure support to get the fix.

8.2 Why emails sent through the web.de email service may be

considered spam?

This topic explains why some emails sent through web.de may be regarded as spam.

When FREEDOME VPN is turned on and emails are sent through the web.de's email service, the messages may be considered spam by the recipients. Without FREEDOME VPN, the same emails are not, however, treated as spam.

The reason for this is that web.de checks which IP address the message is coming from and behaves differently depending on the address type. It appears that if the IP address is a data center address instead of a residential or corporate address, web.de routes the outgoing emails through a different email forwarding server. This particular web.de email forwarding server is listed on many spam block lists. This may cause the destination email server to treat any email coming through that server as spam.

There is nothing that can be done to this on the FREEDOME VPN side. The FREEDOME VPN servers, similar to the servers of other VPN service providers, are hosted at data centers and thus the traffic comes from data center IP addresses. The only workaround to this is to turn off FREEDOME VPN when sending email through the web.de email service.

8.3 Trusted Networks feature doesn't work after update on Android 11

This topic explains what to do if the Trusted Networks feature is not working after an update on Android 11.

On Android 11, the Trusted Networks feature is not always working correctly after the FREEDOME VPN app has been updated from Google Play Store. If the local Wi-Fi network has been defined as trusted, access to the devices within the local network may not work properly.

The reason for this is the way how apps obtain the Wi-Fi network SSID information from the operating system on Android 11.

To work around this issue:

1. Open the FREEDOME VPN app and tap the center of the screen to turn protection OFF.
2. Tap the center again to turn the protection back ON.

The Trusted Networks feature starts to work, but it may fail again as soon as you update the FREEDOME VPN app next time from Google Play Store. If this happens, you need to repeat the above steps.

8.4 Samsung's Dual Messenger and LG's Dual App may prevent FREEDOME VPN from working

This topic describes how to fix the issue in which Samsung's Dual Messenger or LG's Dual App prevents FREEDOME VPN from working.

This issue occurs at least on some Samsung devices, including Galaxy S10, with the latest firmware updates (as of August 2020) when Dual Messenger is used. This may also occur on some LG devices with the Dual App feature.

If the Dual Messenger feature is enabled and FREEDOME VPN has been configured so that it allows one or more apps to bypass the VPN connection, FREEDOME VPN will not be able to establish a VPN connection. Similar behavior may occur with the LG devices with Dual App enabled. Also, this issue affects several other apps similar to FREEDOME VPN.

We don't know if Samsung and LG will fix the issue in their future firmware updates. For the time being, use one of the following workarounds to solve the issue:

- Remove the apps from bypassing the VPN connection:
    a. Open FREEDOME VPN.
    b. Select **Menu** > **Settings** > **Apps bypassing VPN**.
    c. Untick the desired checkbox next to the app that you want to remove from bypassing.

OR

- Depending on your device, do one of the following:
  - Samsung device: turn off the Dual Messenger feature from the device settings:
    1. Select **Settings** > **Advanced features** > **Dual Messenger**.
    2. Turn off the Dual Messenger feature.
    3. Wait at least for 10 minutes before the change takes effect.
  - LG device: turn off the Dual App feature from the device settings:
    1. Select **Settings** > **General** > **Dual app**.
    2. Remove all the applications from the Dual app list.
    3. Restart your device to take the change into use.

8.5 Restricted user profiles may prevent FREEDOME VPN from working on tablets and TV devices

This topic describes how to fix the issue in which restricted user profiles prevent FREEDOME VPN from working on some tablet and TV devices.

This issue affects at least some Android tablets and TV devices with restricted user profiles defined on the device. Normal additional user profiles do not have this problem.

If there are restricted user profiles defined on the device and FREEDOME VPN has been configured so that it allows one or more apps to bypass the VPN connection, FREEDOME VPN will not be able to establish a VPN connection. Also, this issue affects several other apps similar to FREEDOME VPN.

Use one of the following workarounds to solve the issue:

- Remove the apps from bypassing the VPN connection:

  a. Open FREEDOME VPN.

  b. Select **Menu** > **Settings** > **Apps bypassing VPN**.

  c. Untick the desired checkbox next to the app that you want to remove from bypassing.

  OR

- Remove all restricted users from the device and set them up as additional users instead.

8.6 Using zero-rated apps or services with FREEDOME VPN

This topic provides information on using zero-rated apps or services with FREEDOME VPN.

If your Internet Service Provider (ISP) offers zero-rated apps (https://en.wikipedia.org/wiki/Zero-rating) or other internet services free of charge, you may be charged for these when using FREEDOME. To avoid unwanted data charges, make sure your FREEDOME VPN is turned off when accessing such apps or services.

8.7 Why does Google think I may be a robot when using FREEDOME VPN?

When using a Google service, such as Google Search, with FREEDOME VPN turned on, Google may ask you to confirm that you're not a robot.

This is also known as a CAPTCHA check. There are different versions of CAPTCHA checks in the various Google services. The most common is just a simple checkbox but some others may ask you to type in words from pictures or to select certain photos from a screenful of different pictures.

The reason why Google does this to FREEDOME VPN users is most likely the following:

There is a large amount of FREEDOME VPN users accessing Google services at the same time and they are coming from the same FREEDOME IP addresses. Each FREEDOME VPN server in every virtual location has its own IP address, and all the users of that server share that same IP address. This also enhances the privacy of our users.

Google, however, sometimes flags this behavior suspicious. They may see, for example searches in 10 different languages for 10 different topics at the same time, all originating from the same address. To ensure that you are not a robot doing potentially malicious things, Google may sometimes display a CAPTCHA check before allowing you to use the Google Search or other Google services.

A CAPTCHA check like this cannot be used to identify you.

8.8 FREEDOME VPN automatically disconnects after turning it on

This topic explains what to do if FREEDOME VPN automatically disconnects after you turn it on.

Symptoms

FREEDOME VPN automatically disconnects after you try to switch it on.

Diagnosis

Some Android phones have the **Always-on VPN** option for another VPN app. This prevents FREEDOME VPN from being able to establish a connection.

Solution

To solve this issue, disable the **Always-on VPN** option for the other VPN app in the VPN profile settings:

1. Go to your device **Settings**.
2. Select **Connections** > **More connection settings** > **VPN**.

   A list of VPN profiles is shown.
3. Select the **Settings** icon next to the VPN profile that is not FREEDOME VPN.
4. Turn off the **Always-on VPN** option.

8.9 My FREEDOME VPN connection has started to drop often

This topic explains why the FREEDOME VPN connection has started to drop abruptly.

Symptoms

I have noticed that, at times, my FREEDOME VPN connection is cut off.

Diagnosis

If your FREEDOME VPN connection is often cut off, you may have an optimizer app that is running on your phone or tablet.

Some custom-made vendor versions of Android devices come with optimizer apps which may quietly stop FREEDOME VPN in the device. The optimizer tries to save device battery or other resources, and it considers FREEDOME VPN as something which is not needed to run in the background.

Solution

Usually, you can configure an optimizer app to ignore certain apps. If your optimizer app allows this, you should add FREEDOME VPN to the list of allowed apps.

8.10 FREEDOME VPN connection drops frequently on Huawei or Huawei Honor devices

This topic explains what to do if the FREEDOME VPN connection drops often on Huawei devices.

Symptoms

You are getting unstable FREEDOME VPN connection, or experiencing intermittent connection drops when connected to FREEDOME VPN on Huawei or Huawei Honor devices.

Diagnosis

Huawei's Emotion UI (EMUI) silently stops FREEDOME VPN from running in the background to save battery or system resources on the device.

Solution

To prevent EMUI from stopping FREEDOME VPN, you need to lock FREEDOME VPN as a protected app in the EMUI settings:

> **Note:** Different EMUI versions may have different steps.

1. In the EMUI device management settings under **Power Saving**, set the device power saving mode to **Normal/Smart** or **Performance**.

2. Define the FREEDOME VPN app as a **Protected app** through the EMUI settings (EMUI 3.x) or device management app (EMUI 4.0).
3. Lock the FREEDOME VPN app manually by going to the list of open apps and dragging the FREEDOME VPN app down slightly in the list.

> **Note:** You must complete the above steps always after restarting the device as EMUI resets the setting at device restart.

8.11 FREEDOME VPN connection drops frequently on Samsung devices

This topic explains what to do if the FREEDOME VPN connection drops often on Samsung devices.

Symptoms

You are getting unstable FREEDOME VPN connection, or experiencing intermittent connection drops when connected to FREEDOME VPN on some Samsung devices.

Diagnosis

Depending on the setup, the battery optimization features of your Android device may have an effect on the VPN connection.

Solution

To fix the issue, make sure that the battery optimization features on the Samsung device allow FREEDOME VPN to work. These settings need to be checked in three different locations in the system settings as follows:

1. Verify that FREEDOME VPN is set as a "Never sleeping app" via the system settings:

    a. Open **Settings**.

    b. Go to **Battery and device care** > **Battery** > **Background usage limits** > **Never sleeping apps**.

    c. Select the **+** icon. A list of available apps opens.

    d. Scroll down and select **Freedome**.

    e. Select **Add**.

    The above steps may vary depending on the phone model. You can directly access this setting by searching for "Never sleeping apps" in the system settings.

2. Verify that FREEDOME VPN is not optimised for battery usage:

    a. Open **Settings**.

    b. Go to **Apps**.

    c. Scroll down and select **Freedome**.

    d. Select **Battery**.

    e. Select **Unrestricted**. This option allows the app to use battery in the background without restrictions. This may reduce your battery life.

    > **Note:** Several Samsung phone models have a bug which affects this setting. If FREEDOME VPN is already unchecked in the list, check and uncheck it, as the bug may otherwise ignore this setting. It also seems that the affected Samsung devices may forget this setting and you may need to toggle it again later on.

3. Verify the mobile data settings:

    a. Open **Settings**.

    b. Go to **Apps**.

c. Scroll down and select **Freedome**.

d. Select **Mobile data**.

e. Turn on both **Allow background data usage** and **Allow data usage while Data saver is on**.

8.12 FREEDOME VPN stops working on OnePlus phone with Android 9

This topic explains what to do if FREEDOME VPN stops working on a OnePlus phone.

Symptoms

FREEDOME VPN stops working unexpectedly on OnePlus phones running on Android 9.

Diagnosis

OnePlus phones with Android 9 include a battery optimizer which may abruptly stop FREEDOME VPN.

Unfortunately, the OnePlus version of Android stops background apps very aggressively. Also, OnePlus has bugs that prevent the settings related to the background apps from working properly.

Solution

It is not possible to exclude FREEDOME VPN from the battery optimizer automatically. However, you can set this manually in the following way:

1. On the phone, go to **Settings** > **Battery** > **Battery optimization**.
2. Find FREEDOME VPN on the **Battery optimization** page and change its setting to "not optimized".

3. Under **Battery optimization**, tap the **three dots** button, select **Advanced/Enhanced optimization**, and disable the feature.

OnePlus phones seem to reset this setting randomly, so you may need to change the setting again after some time.

Usually, you may be able to limit this behavior by locking FREEDOME VPN to the Recent App list but unfortunately this is not a permanent solution either:

1. Start FREEDOME VPN.
2. Tap the **Recent apps** button on the phone.
3. Close the **Lock** button in the top-right corner of the app.

Some OnePlus phones have also a feature called "App auto-launch". If your phone has this feature, disable it for FREEDOME VPN.

8.13 Unable to select the "I trust this application" checkbox in FREEDOME VPN

This topic explains what to do if you cannot mark FREEDOME VPN as a trusted application.

Symptoms

I am unable to select the **I trust this application** checkbox in the FREEDOME VPN app.

Diagnosis

This issue is related to other apps masking the checkbox dialog in FREEDOME VPN. Apps, such as Lux Brightness, Night Mode, or Twilight are known to cause these issues.

This dialog appears after first-time installation or reboot.

Solution

If you run into this issue:

1. Close any apps that may be running in the background.
2. Select the **I trust this application** checkbox, and then select **OK**.

8.14 I have difficulties in accessing online casinos when FREEDOME VPN is on

This topic explains why some online casinos may block your user account when using FREEDOME VPN.

Symptoms

You try to access an online casino but the connection is blocked.

Diagnosis

To prevent stolen user accounts from being abused, some online casinos (and possibly some other sites) perform origin checks to the connections. For example, if a user connects from Sweden but has specified himself as French when he originally registered to the casino, the online casino may consider this suspicious and blocks the user account.

Solution

To overcome this problem, use the same location that you used when you registered to the casino.

8.15 Unable to connect to a public WiFi network when FREEDOME VPN is on

This topic explains why sometimes when FREEDOME VPN is on you cannot connect to a public WiFi network.

Symptoms

I try to connect to a public WiFi network. To ensure that I can safely use the network, I have FREEDOME VPN turned on. However, I can't connect to the WiFi network.

Diagnosis

There are two likely explanations why you are not able to connect to a public WiFi when FREEDOME VPN is turned on:

- VPN protocol is not allowed
- WiFi requires a login.

Solution

1. **VPN protocol is not allowed**:

   The administrator of the WiFi network has configured the wireless network so that it does not allow VPN protocols through. Some public WiFi providers only allow HTTP and HTTPS protocols and block everything else. If this is the case, there is nothing that can be done to get immediate access to the network. However, users of that particular public WiFi network could request the WiFi provider to allow VPN protocols.

2. **WiFi requires a login**:

   The public WiFi network requires that you log in before you are allowed to use the network. FREEDOME VPN usually detects that it is in a captive portal, but in some cases this is not however possible. If the network requires a login first, the connection will fail because FREEDOME VPN tries to make an encrypted VPN connection directly to the F-Secure servers as soon as the device connects to the public network. In this case, do the following:

1. Turn off FREEDOME VPN.

2. Log in to the public WiFi network.
3. Turn FREEDOME VPN on again.

> **Warning:** During the time you have FREEDOME VPN turned off, your communication is not protected.

8.16 Why does FREEDOME VPN not work in China?

This topic explains why FREEDOME VPN does not work in China.

Symptoms

When residing in China, the FREEDOME VPN app often cannot connect to any of the FREEDOME VPN servers. Occasionally, some of the FREEDOME VPN locations may work, but often not. When residing outside China, accessing Chinese website or other Chinese internet services often results in an error message saying that the server IP address cannot be found.

Diagnosis

The use of VPN apps (including FREEDOME VPN) is restricted in China. Due to the policy of the Chinese government, VPN connections are blocked in their network for both local residents and foreign people travelling in China. This prevents FREEDOME VPN from working in China.

This Chinese VPN block also affects FREEDOME VPN users outside China. If a Chinese internet service, such as a website, has all of its Domain Name Servers (DNS) in China, the FREEDOME VPN servers will not have access to the website. If the internet service in question has at least one of its DNS servers outside China, it may remain accessible to FREEDOME VPN users.

Solution

Due to the nature of this issue, we are unable to solve this.

8.17 Why does FREEDOME not work in the United Arab Emirates and other Persian Gulf area countries?

This topic explains why FREEDOME VPN does not work in the United Arab Emirates and other Persian Gulf area countries.

Symptoms

The FREEDOME VPN app cannot connect to any of the FREEDOME VPN servers when the device is in the following Persian Gulf area:

- Bahrain
- Iraq
- Kuwait
- Oman
- Qatar
- Saudi Arabia
- United Arab Emirate

At first the VPN connection may be successful but it stops working soon after that.

Diagnosis

The use of VPNs is not allowed in the Persian Gulf area. The local internet service providers block VPN connections in their networks. This prevents FREEDOME VPN from working.

Solution

For the above reason, we cannot solve this issue.

8.18 How can I generate a FREEDOME log file with my smartphone?

If you have technical problems with your product, you can create and send a log file to our technical support.

If our technical support asks you to send logs to us, follow the instructions given below. The log file contains information that can be used for troubleshooting and solving problems specific to your device.

> **Note:** Do not send the log files without first contacting our technical support as you'll need to have a support ticket number when sending the logs.

To generate a log file with your smartphone:

1. Open the FREEDOME VPN app.
2. Tap the main menu in the top-left corner, and select **About**.

   The **About Freedome** page opens.
3. Tap seven times on the version number.

   The **Send log file** button is displayed at the bottom of the screen.
4. Tap the **Send log file** button and select your email sending method.

   The email message opens with the log file attached to it.

5. Describe the problem in the email. Remember to include the support ticket number you received from our technical support.
6. Send the email.

F-Secure makes every digital moment more secure, for everyone.

Subscribe to newsletter

(https://www.facebook.com/pages/F-Secure/107471754306) (https://twitter.com/FSecure)
(https://www.linkedin.com/company/f-secure-corporation) (https://www.youtube.com/c/fsecureconnectedlife)
(https://instagram.com/fsecureglobal)

Store (https://www.f-secure.com/en/)

Products (https://www.f-secure.com/en/home/products)

Renew subscription (https://www.f-secure.com/en/home/renew)

Articles (https://www.f-secure.com/en/home/articles)

Free tools (https://www.f-secure.com/en/home/free-tools)

Download (https://www.f-secure.com/en/home/download)

My F-Secure (https://www.f-secure.com/en/home/login)

Contact support (https://www.f-secure.com/en/home/support)

For partners (https://www.f-secure.com/en/partners)

Why partner with us? (https://www.f-secure.com/en/partners)

For operators (https://www.f-secure.com/en/partners/operators)

For retail (https://www.f-secure.com/en/partners/resellers)

For banks (https://www.f-secure.com/en/partners/banking)

For insurers (https://www.f-secure.com/en/partners/insurance)

For utilities (https://www.f-secure.com/en/partners/utilities)

Affiliate program (https://www.f-secure.com/en/partners/affiliate-program)

Contact sales (https://www.f-secure.com/en/partners/contact-sales)

Company (https://www.company.f-secure.com/en/)

About us (https://www.company.f-secure.com/en/)

Join us (https://www.company.f-secure.com/en/join-us)

For investors (https://investors.f-secure.com/en)

For media (https://www.company.f-secure.com/en/press)

F-Secure blog (https://blog.f-secure.com/)

Contact info (https://www.company.f-secure.com/en/contact-us)

English

Terms of service (https://www.f-secure.com/en/legal/terms/websites)

Privacy Policy (https://www.f-secure.com/en/legal/privacy/websites)

Cookie (https://www.f-secure.com/en/legal/privacy/websites#cookies)