

|  |
| --- |
|  |
|  |

| Related Artifacts | |
| --- | --- |
| Ref. | Name |
| GLO | [Common Glossary](https://info.epam.com/acronyms.html) |
| WIAP | [Work Instruction: Antivirus Protection](https://pal.epam.com/pal_method_plugin/guidances/whitepapers/doc_WIIT_AntivirusProtection_90900163.html) |

|  |  |
| --- | --- |
| Abbreviations and Acronyms | |
| GP | GlobalProtect |
| QMS | Quality Management System |
| SEPG | Software Engineering Process Group |
| SID | Security Identifier |
| SSL | Secure Sockets Layer |
| TSG | Terminal Services Gateway |
| VPN | Virtual Private Network |
| WiFi | Wireless network |

Contents

[1 Introduction 4](#_Toc30109560)

[1.1 Purpose 4](#_Toc30109561)

[1.2 Scope 4](#_Toc30109562)

[2 Rules of Use 4](#_Toc30109563)

[3 Connecting to EPAM Network via global protect VPN 5](#_Toc30109564)

[3.1 List of supported OS 5](#_Toc30109565)

[3.2 Setting up your VPN on Windows 6](#_Toc30109566)

[3.3 Setting up your VPN on macOS 12](#_Toc30109567)

[3.4 Setting up your VPN on Linux 18](#_Toc30109568)

[3.4.1 GUI version 18](#_Toc30109569)

[3.4.2 CLI version 21](#_Toc30109570)

[3.4.3 Unsupported Linux distributions 23](#_Toc30109571)

[3.5 Setting up your VPN on Android 24](#_Toc30109572)

[3.6 Setting up your VPN on iOS 26](#_Toc30109573)

[4 Connecting to EPAM Network via Terminal Services Gateways (TSG) 29](#_Toc30109574)

[5 Wi-Fi Access 31](#_Toc30109575)

[5.1 EPAM Guest Connection 31](#_Toc30109576)

[5.1.1 Guest Wi-Fi account types 31](#_Toc30109577)

[5.1.2 EPAMGuests 31](#_Toc30109578)

[5.2 EPAM Employee Connection 32](#_Toc30109579)

[5.2.1 EPAM8021x 32](#_Toc30109580)

[5.2.1.1 Windows 7 32](#_Toc30109581)

[5.2.1.2 macOS 32](#_Toc30109582)

[5.2.1.3 Android 33](#_Toc30109583)

[5.2.1.4 iOS 33](#_Toc30109584)

[Appendix A. GATES 38](#_Toc30109585)

[Appendix A.1. Main VPN GATES 38](#_Toc30109586)

[Appendix A.2. Regional VPN portals 38](#_Toc30109587)

[Appendix A.3. TSG Gates 38](#_Toc30109588)

# Introduction

## Purpose

This work instruction defines the procedures for connecting to the Company’s network through VPN. The Company provides these services to encourage and improve efficient and high quality work and information exchange.

## Scope

The work instruction applies to all Employees, Contractors and Trainees of the EPAM.

The owner of this document is the Head of Network Service Group.

The approver of this document is the Head of IT Service Operations.

SEPG is responsible for its maintenance and publishing, Network Service Group for regular review/update.

# Rules of Use

Only EPAM Systems Employees, Contractors and Trainees are authorized to access the internal EPAM network from the Internet over VPN in case they need services that cannot be accessed from the Internet. Access to internal EPAM network from the Internet over VPN is allowed only if appropriate approval is obtained:

* for production projects – approval from Delivery or Project manager;
* for non-productions units – approval from Unit manager.

If the Company’s network has been accessed by a third party, the password of the domain account used to access the network must be changed immediately and the Support Team must be promptly notified.

The VPN and Guest connections are to be used only for transmitting the work related data to and from the Company’s network.

The computing devices accessing the Company’s network shall:

* use a legally licensed operating system;
* have the latest service pack, updates and patches installed on the operating system;
* have antivirus software installed (legally licensed), in use, and updated with the latest virus definitions (see [[WIAP](#WIAP)]);
* have the firewall turned on;
* have up-to-date antivirus enabled.

The following restrictions and recommendations must be observed and strictly adhered to:

* It is strictly prohibited to pass any details of connection information to any third party, or to allow any third party (including friends and family members) to access Company’s network or resources;
* It is strictly prohibited to use the VPN and Guest connections for Internet navigation not related to work activities;
* It is not recommended to use VPN connections only for browsing the Internet, even if it is work related;
* It is not recommended to use VPN and Guest connections for accessing the Company’s E-mail system;
* It is forbidden to allow the computer device accessing the Company’s network to act as a gateway between the Company’s network and another network.

# Connecting to EPAM Network via global protect VPN

## List of supported OS

You can find the up to date list of supported operating systems on vendor’s site: [https://docs.paloaltonetworks.com/compatibility-matrix/globalprotect/where-can-i-install-the-globalprotect-app#](https://docs.paloaltonetworks.com/compatibility-matrix/globalprotect/where-can-i-install-the-globalprotect-app).

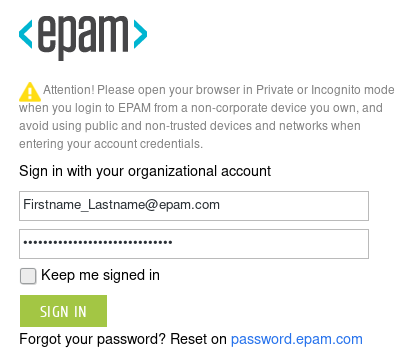
Supported OS via 01-Jan-2020:

|  |  |
| --- | --- |
| Operating System | Support |
| **Apple iOS** | |
| iOS 8 | — |
| iOS 9 | — |
| iOS 10 | check-mark.png (64-bit devices only) |
| iOS 11 | check-mark.png (64-bit devices only) |
| iOS 12 | check-mark.png (64-bit devices only) |
| iOS 13 | check-mark.png (64-bit devices only) |
| **Apple Mac** | |
| Mac OS X 10.5 (64-bit only) | — |
| Mac OS X 10.6 | — |
| Mac OS X 10.7 | — |
| Mac OS X 10.8 | — |
| Mac OS X 10.9 | — |
| Mac OS X 10.10 | — |
| macOS 10.11 | check-mark.png |
| macOS 10.12 | check-mark.png |
| macOS 10.13 | check-mark.png |
| macOS 10.14 | check-mark.png |
| macOS 10.15 | check-mark.png |
| **Google Android** | |
| Google Android 4.4 | — |
| Google Android 5.x | — |
| Google Android 6.x | — |
| Google Android 7.x | — |
| Google Android 8.x | check-mark.png |
| Google Android 9.x | check-mark.png |
| **Linux** | |
| CentOS 7.7 | check-mark.png (CLI only) |
| CentOS 7.6 | check-mark.png |
| CentOS 7.5 | check-mark.png (CLI only) |
| CentOS 7.4 | check-mark.png (CLI only) |
| CentOS 7.3 | check-mark.png (CLI only) |
| CentOS 7.2 | check-mark.png (CLI only) |
| CentOS 7.1 | check-mark.png (CLI only) |
| CentOS 7.0 | check-mark.png |
| Red Hat Enterprise Linux (RHEL) 7.0 — 7.7 | check-mark.png (Releases 7.0 — 7.6: CLI only) |
| Red Hat Enterprise Linux (RHEL) 6.8 — 6.9 | (CLI only) |
| Ubuntu 19.04 | check-mark.png (CLI only) |
| Ubuntu 18.04 2 LTS | check-mark.png |
| Ubuntu 18.04 1 LTS | check-mark.png |
| Ubuntu 18.04 LTS | check-mark.png |
| Ubuntu 16.04 LTS | check-mark.png (CLI only) |
| Ubuntu 14.04 | check-mark.png (CLI only) |
| **Windows** | |
| Windows XP (32-bit only) | — |
| Windows Vista | — |
| Windows 7 | check-mark.png (requires IE 11) |
| Windows 8 | check-mark.png |
| Windows 8.1 | check-mark.png |
| Windows 10 | check-mark.png |

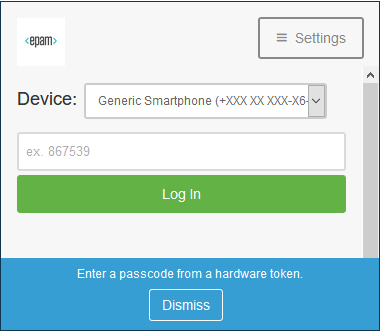
## Setting up your VPN on Windows

Log into the GlobalProtect portal.

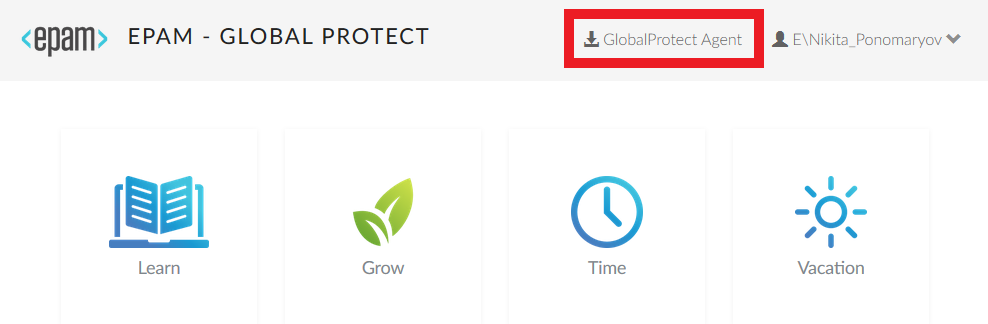
1. Launch a web browser and go to the following URL: <https://vpn.epam.com>;
2. On the portal login page, enter your *User Name* (i.e. FirstName\_LastName@epam.com) and *Password*, and then click **SIGN IN**. In most instances, you can use the same username and password that you use to connect to your corporate network:



1. Enter DUO two-factor passcode (or choose another option in *Device* field) and click **Log In**:

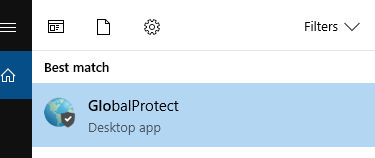


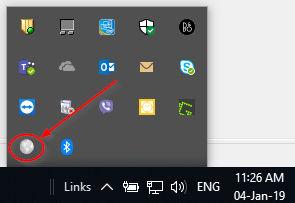
1. Navigate to the app download page: select **GlobalProtect Agent** to open the download page: <https://vpn.epam.com/global-protect/getsoftwarepage.esp>



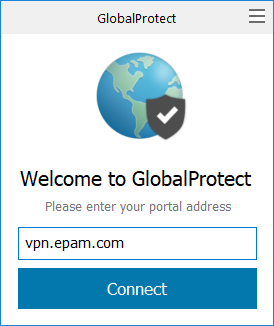


1. Download and install GlobalProtect Agent;
2. Run application GlobalProtect:

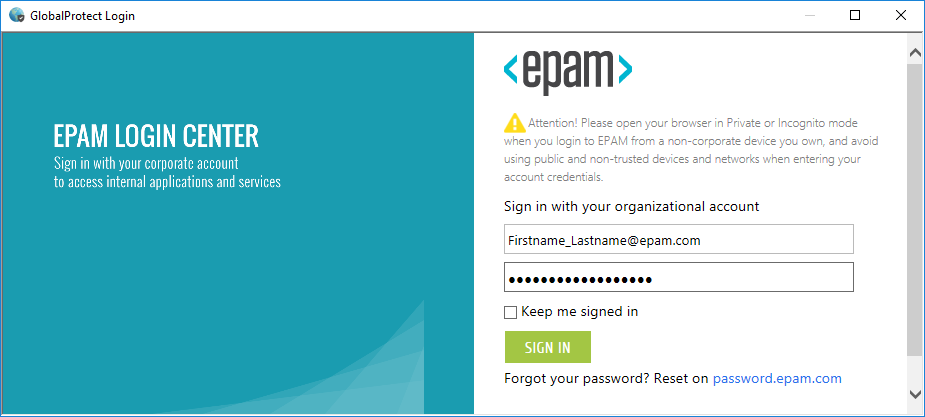




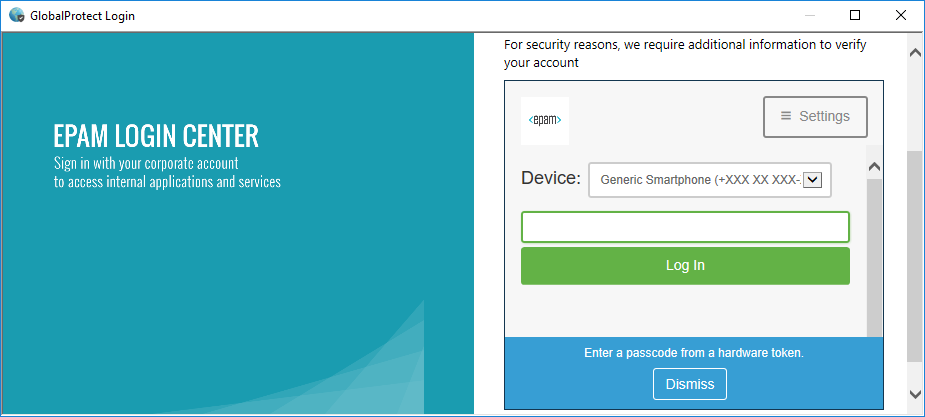
1. If you are using **Windows 7** OS make sure that **Internet Explorer 11** is installed on your computer before connecting to the VPN. You can get it from [here](https://support.microsoft.com/en-us/help/18520/download-internet-explorer-11-offline-installer).
2. Enter GlobalProtect portal address **vpn.epam.com** and click **Connect**:



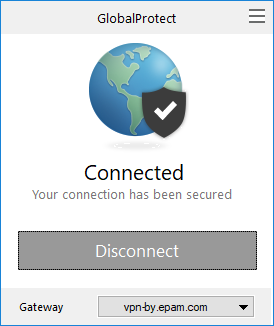
1. A pop-up window will appear. Enter your *Name* (i.e. FirstName\_LastName@epam.com) and *Password*, and then click **SIGN IN**:



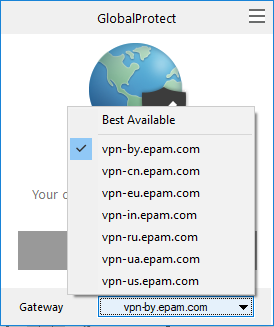
1. Enter DUO two-factor passcode (or choose another option in *Device* field) and click **Log In**:



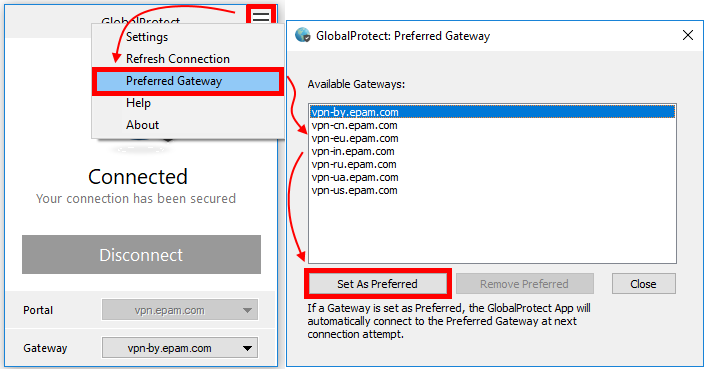
1. You have successfully connected to EPAM GlobalProtect VPN:



1. You can choose another VPN gateway to connect to if needed:



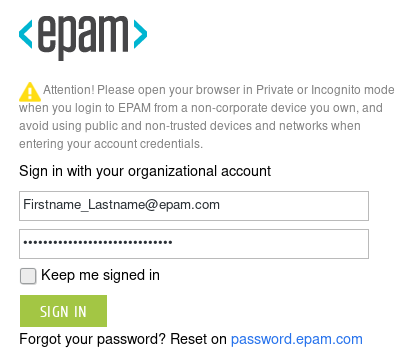
1. You can assign and automatically connect to a preferred GlobalProtect gateway. By default, the GlobalProtect app automatically connects to the best available gateway based on the priority, source region, and response time of the configured gateways:



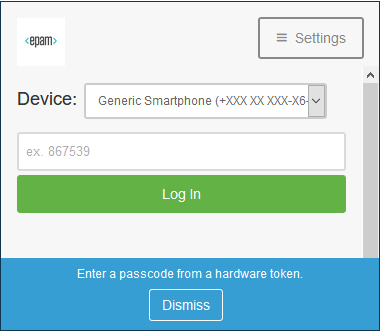
## Setting up your VPN on macOS

Log into the GlobalProtect portal.

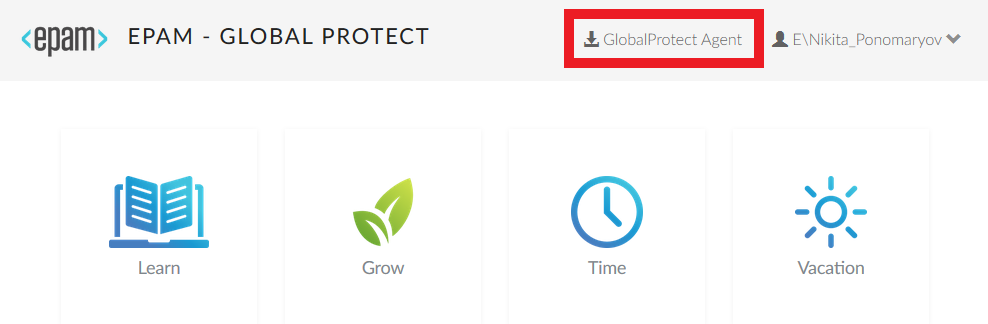
1. Launch a web browser and go to the following URL: <https://vpn.epam.com>;
2. On the portal login page, enter your *User Name* (i.e. FirstName\_LastName@epam.com) and *Password*, and then click **SIGN IN**. In most instances, you can use the same username and password that you use to connect to your corporate network:



1. Enter DUO two-factor passcode (or choose another option in *Device* field) and click **Log In**:

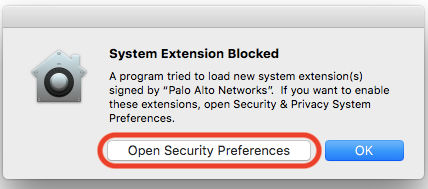


1. Navigate to the app download page: select **GlobalProtect Agent** to open the download page: <https://vpn.epam.com/global-protect/getsoftwarepage.esp>



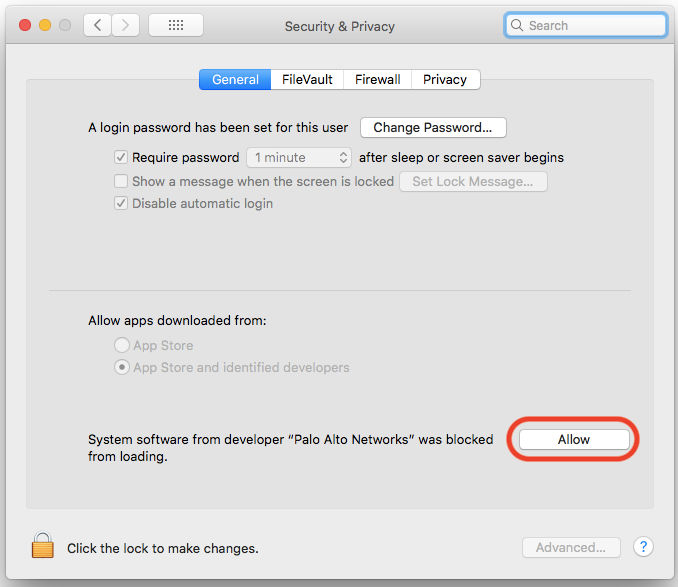


1. Download and install GlobalProtect Agent;
2. You will see the "System Extension Blocked" dialog box if you installed the GlobalProtect VPN application for the first time:



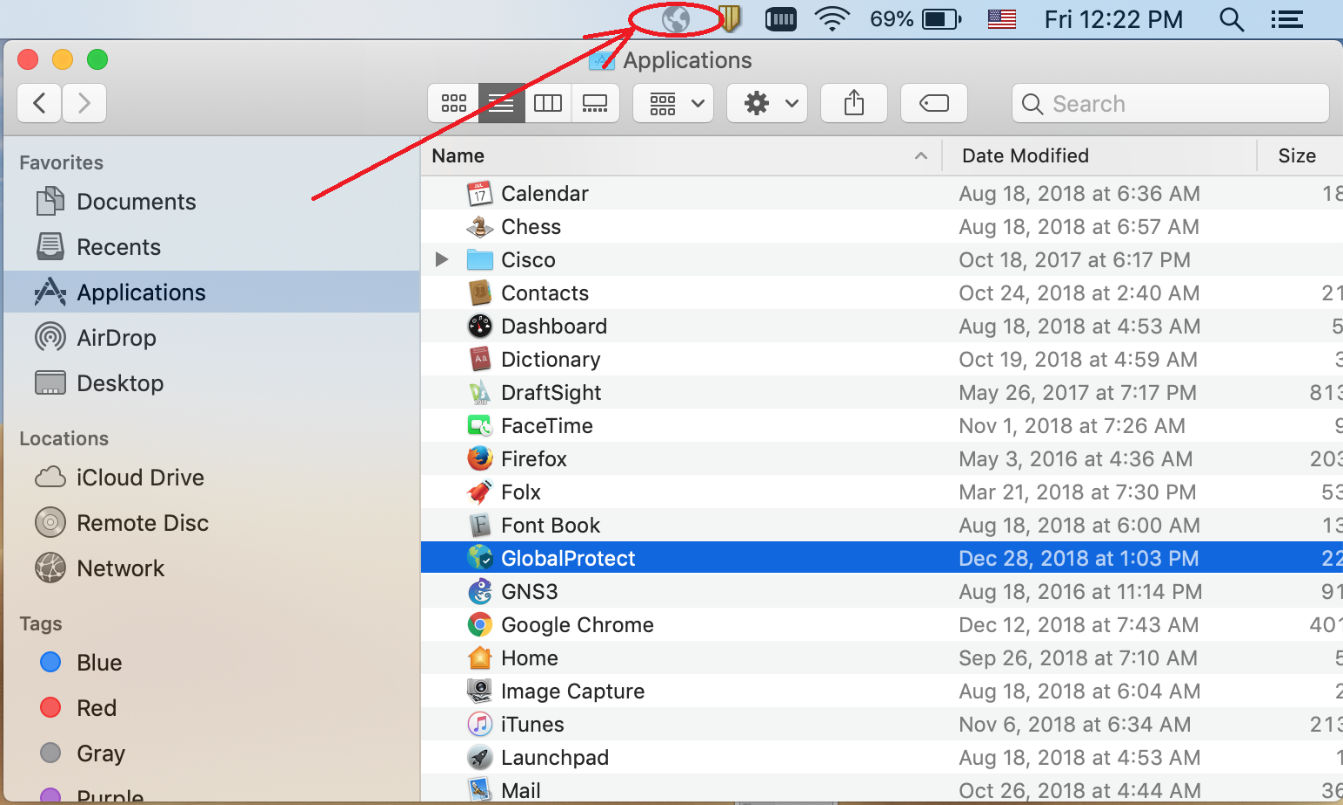
1. If you click the "**OK**" button instead, **you have 30 minutes** to navigate the **Security & Privacy** System Preference before the **Allow** button disappears. Then you will need to restart the Mac in order to approve the system extension(s).

Click on the button labeled "**Open Security Preferences**", which will take you to the Security & Privacy panel of Systems Preferences, as shown in Figure below:

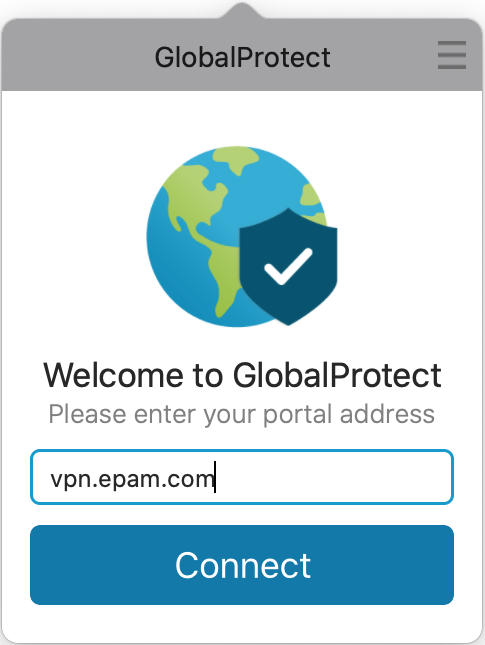


Click on the "**Allow**". You will be prompted if a restart is required at this time.

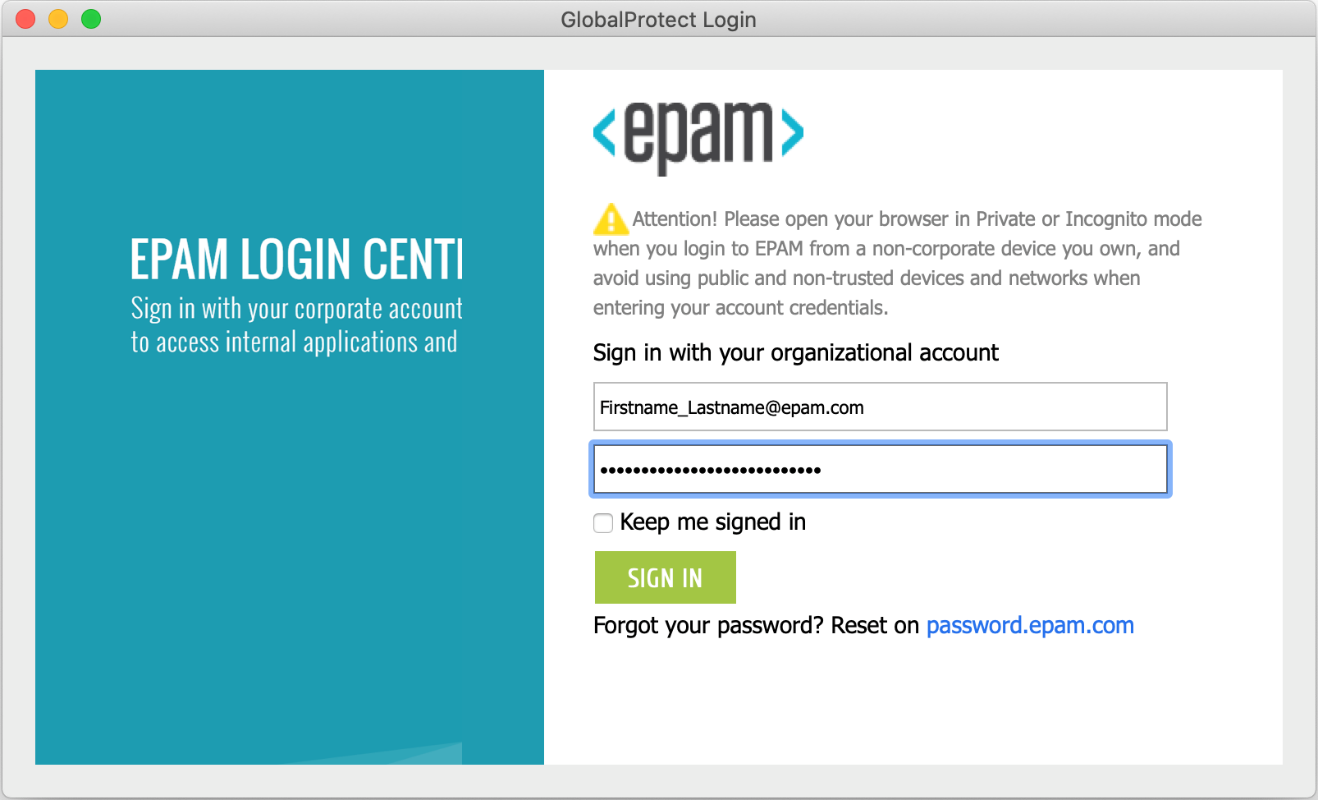
1. Run application GlobalProtect:



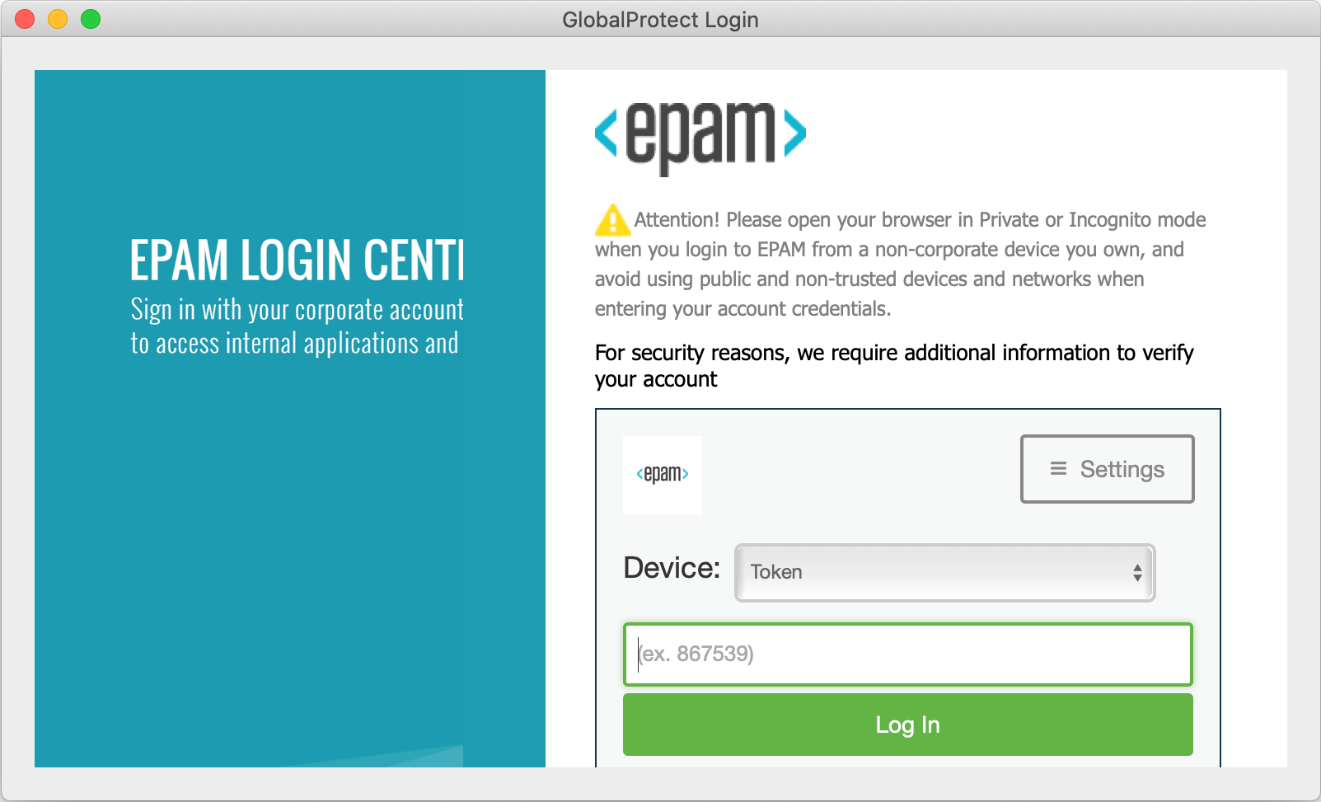
1. Enter GlobalProtect portal address **vpn.epam.com** and click **Connect**:



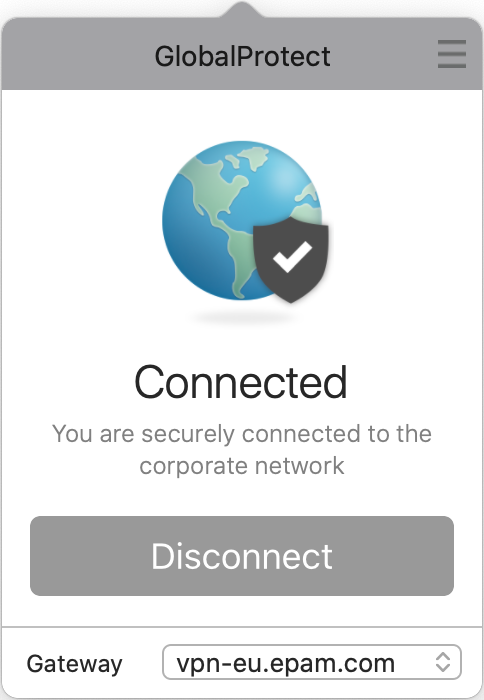
1. A pop-up window will appear. Enter your *Name* (i.e. FirstName\_LastName@epam.com) and *Password*, and then click **SIGN IN**:



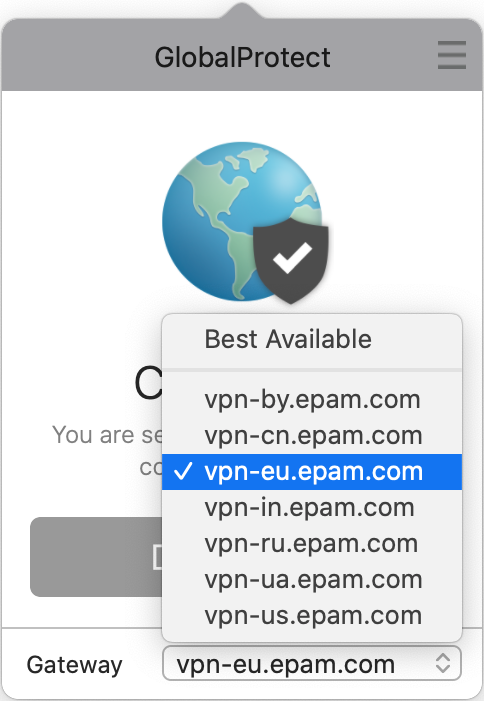
1. Enter DUO two-factor passcode (or choose another option in *Device* field) and click **Log In**:



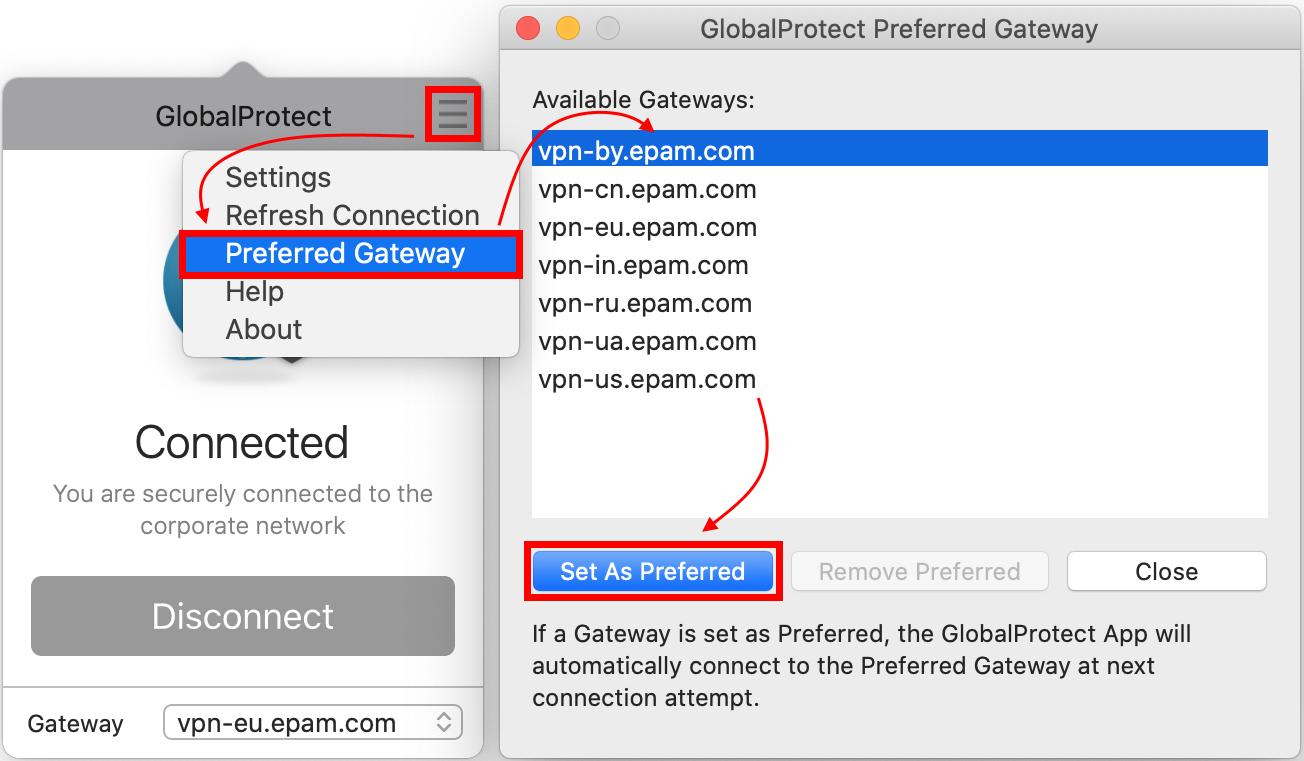
1. You have successfully connected to EPAM Global Protect VPN:



1. You can choose another VPN gateway to connect to if needed:



1. You can assign and automatically connect to a preferred GlobalProtect gateway. By default, the GlobalProtect app automatically connects to the best available gateway based on the priority, source region, and response time of the configured gateways:



## Setting up your VPN on Linux

1. Only **Ubuntu**, **CentOS** and **RHEL** distributions are supported according to the vendor (see point [**3.1**](#_List_of_supported)). You can try to run commands from point [**3.4.3**](#_Unsupported_Linux_distributions), but the workability is not guaranteed.

### GUI version

1. Before installing the GUI version of GlobalProtect check that you distribution is supported (see point [**3.1**](#_List_of_supported)).
2. Download the installation package:

<https://sharepoint.epam.com/WFT/ITServices/Shared%20Documents/WFT%20IT%20Services%20Network/Shared%20files/GP/PanGPLinux.tgz>

1. Extract the files from the package:

**tar -xvf ~/Downloads/PanGPLinux.tgz**

After you unzip the package, you will see installation packages — **DEB** for *Ubuntu* and **RPM** for *CentOS* and *Red Hat* — and the scripts to install and uninstall the packages. The package for the GUI version is denoted by a **GlobalProtect\_UI** prefix.

1. Install the GUI version of the GlobalProtect app for Linux.

Install the app using root privileges and use an installation method that will automatically add any missing packages that are required by the GlobalProtect app (*<gp-app-pkg>* is the name of your distribution package for your Linux version).

For Ubuntu:

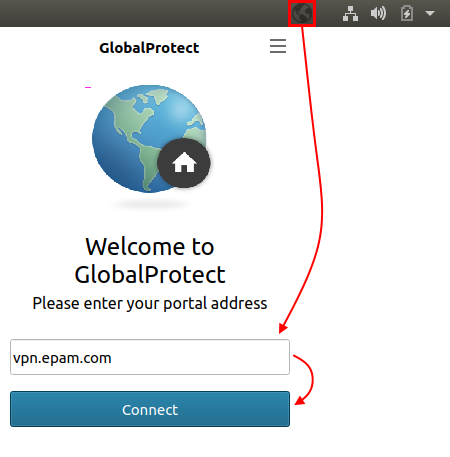
**sudo apt-get install *<gp-app-pkg>***

For CentOS and Red Hat:

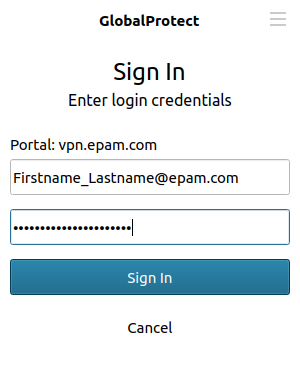
**sudo yum install <gp-app-pkg>**

The GlobalProtect app for Linux installs to the */opt/paloaltonetworks/globalprotect* directory. After GlobalProtect first runs, the app also creates a GlobalProtect user folder *$HOME/.globalprotect* to save user registry configuration and other CLI related settings.

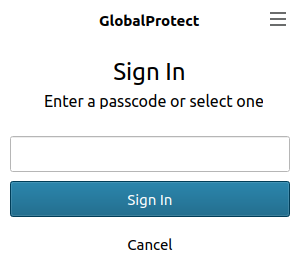
1. Run GlobalProtect, enter portal address **vpn.epam.com** and click **Connect**:



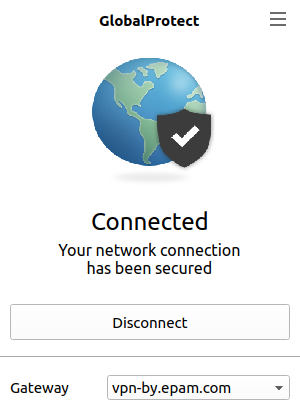
1. Enter the *Username* (i.e. Firstname\_Lastname@epam.com) and *Password*, and then click **Sign In**:



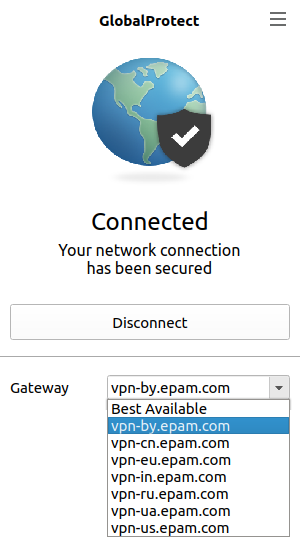
1. Enter DUO two-factor passcode (DUO push is **not supported**) and click **Sign In**:



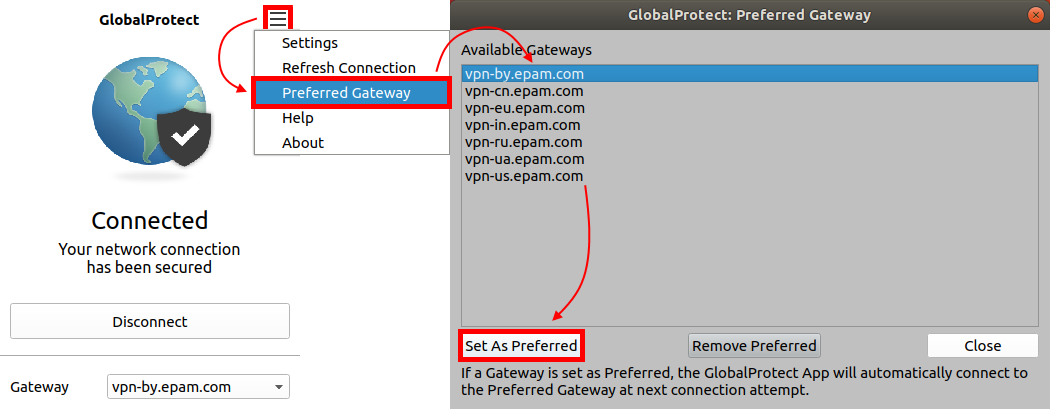
1. You have successfully connected to EPAM Global Protect VPN:



1. You can choose another VPN gateway to connect to if needed:



1. You can assign and automatically connect to a preferred GlobalProtect gateway. By default, the GlobalProtect app automatically connects to the best available gateway based on the priority, source region, and response time of the configured gateways:



### CLI version

1. Download the installation package:

<https://sharepoint.epam.com/WFT/ITServices/Shared%20Documents/WFT%20IT%20Services%20Network/Shared%20files/GP/PanGPLinux.tgz>

1. Extract the files from the package:

**tar -xvf ~/Downloads/PanGPLinux.tgz**

After you unzip the package, you will see installation packages — **DEB** for *Ubuntu* and **RPM** for *CentOS* and *Red Hat* — and the scripts to install and uninstall the packages.

1. Install the GUI version of the GlobalProtect app for Linux.

Install the app using root privileges and use an installation method that will automatically add any missing packages that are required by the GlobalProtect app (*<gp-app-pkg>* is the name of your distribution package for your Linux version).

For Ubuntu:

**sudo apt-get install *<gp-app-pkg>***

For CentOS and Red Hat:

**sudo yum install <gp-app-pkg>**

The GlobalProtect app for Linux installs to the */opt/paloaltonetworks/globalprotect* directory. After GlobalProtect first runs, the app also creates a GlobalProtect user folder *$HOME/.globalprotect* to save user registry configuration and other CLI related settings.

1. Run GlobalProtect and connect to the portal address **vpn.epam.com** (if you are using unsupported Linux distribution run commands from the point [**3.4.3**](#_Unsupported_Linux_distributions) first)**:**

**globalprotect**

**connect --portal vpn.epam.com**

When you use certificate-based authentication, the first time you connect without a root CA certificate, the GlobalProtect app and GlobalProtect portal exchange certificates. The GlobalProtect app displays a certificate error, which you must acknowledge before you authenticate. You will not be prompted with the certificate error message on your next connections.

Retrieving configuration...

Disconnected

There is a problem with the security certificate, so the identity of 10.3.188.61 cannot be verified. Please contact the Help Desk for your organization to have the issue rectified.

Warning: The communication with vpn.epam.com may have been compromised. We recommend that you do not continue with this connection.

Error details: Do you want to continue(y/n)?**y**

Retrieving configuration...

vpn.epam.com - Enter login credentials

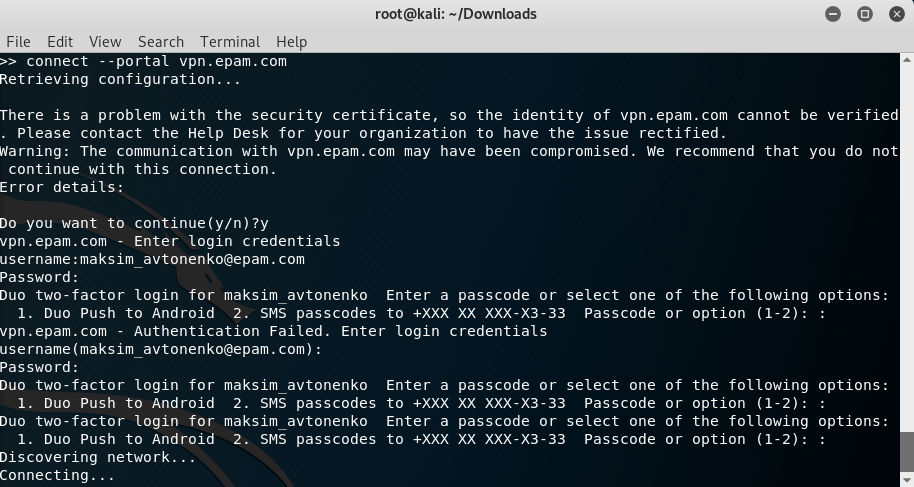
1. Enter the *Username* (i.e. Firstname\_Lastname@epam.com) and *Password*:

username:**Firstname\_Lastname@epam.com**

Password:

1. Enter DUO two-factor passcode or choose another option (**note that the symbols you enter won’t be visible**):

Duo two-factor login for firstname\_lastname Enter a passcode or select one of the following options: 1. Duo Push to Android Passcode or option (1-1): :



1. You can choose another VPN gateway to connect to if needed.

First list the available gateways:

>> **show --manual-gateway**

Name Address

------------------------------

vpn-cn.epam.com vpn-cn.epam.com

vpn-ru.epam.com vpn-ru.epam.com

vpn-ua.epam.com vpn-ua.epam.com

vpn-in.epam.com vpn-in.epam.com

vpn-us.epam.com vpn-us.epam.com

vpn-eu.epam.com vpn-eu.epam.com

vpn-by.epam.com vpn-by.epam.com

Then enter the following command:

>> **connect --gateway *<gp-gateway>***

where *<gp-gateway>* is the address of the required gateway.

1. Commands for GlobalProtect:

Usage: only the following commands are supported:

collect-log -- collect log information

connect -- connect to server

disconnect -- disconnect

disable -- disable connection

import-certificate -- import client certificate file

quit -- quit from prompt mode

rediscover-network -- network rediscovery

remove-user -- clear credential

resubmit-hip -- resubmit hip information

set-log -- set debug level

show -- show information

### Unsupported Linux distributions

1. Workability of GlobalProtect on unsupported Linux distributions is not guaranteed.
2. The commands listed below should be run before connecting to VPN portal.

The following commands have been tested on **Linux Mint**,  **Arch Linux**, and **Manjaro** distributions:

REPLACE=`lsb\_release -ds | sed -e 's/"//g' | xxd -l6 -g1 | cut -d ' ' -f2,3,4,5,6,7 | sed -e 's/^/\\\\x/g' -e 's/ /\\\\x/g'`

sudo sed -i "s/\x55\x62\x75\x6e\x74\x75/$REPLACE/g" /opt/paloaltonetworks/globalprotect/PanGPS

sudo systemctl restart gpd.service

For **Fedora** distribution:

cd /opt/paloaltonetworks/globalprotect/

sudo sed -i 's/CentOS/Fedora/g' PanGPS

sudo systemctl restart gpd.service

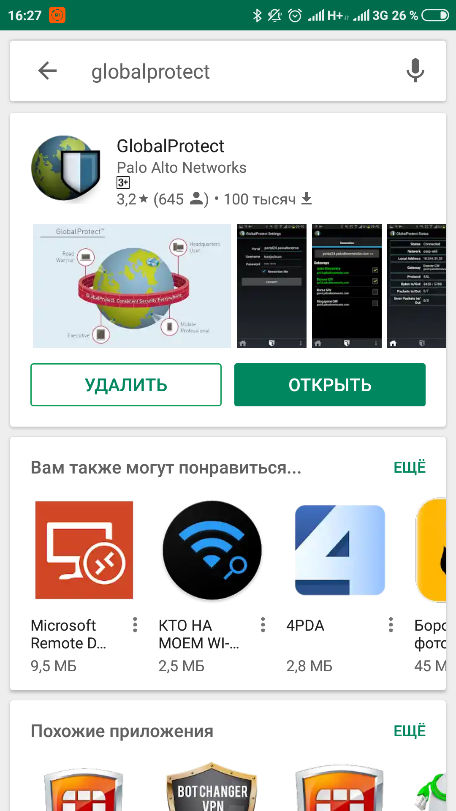
For **Debian** distribution:

sudo echo 'DISTRIB\_DESCRIPTION="Ubuntu 18.04.1 LTS"' > /etc/lsb-release

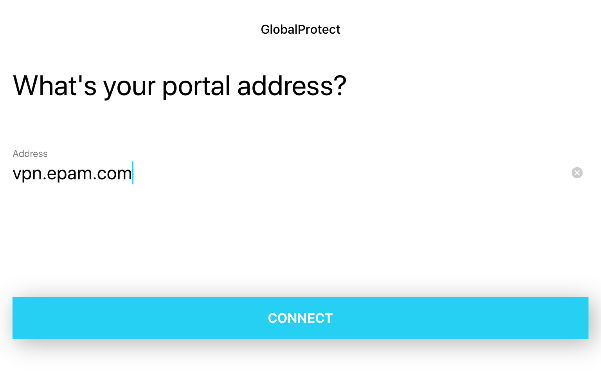
sudo systemctl restart gpd.service

## Setting up your VPN on Android

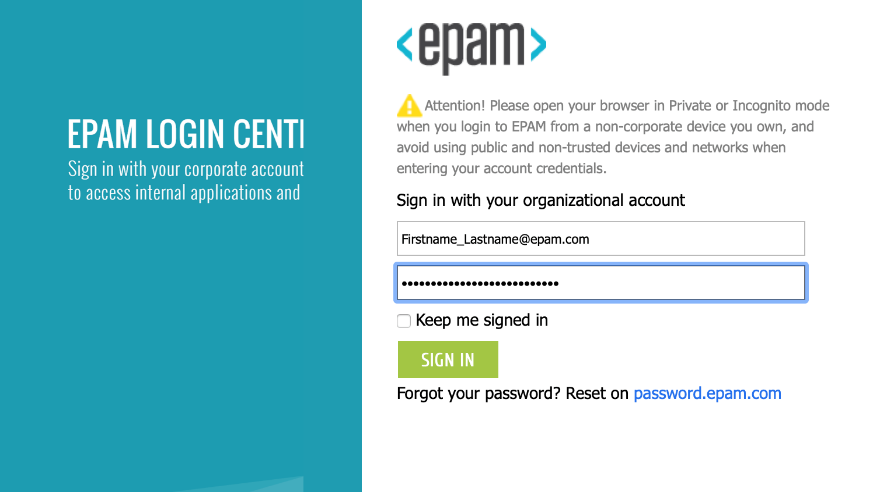
1. Install Global Protect App from Google Play Market: <https://play.google.com/store/apps/details?id=com.paloaltonetworks.globalprotect>



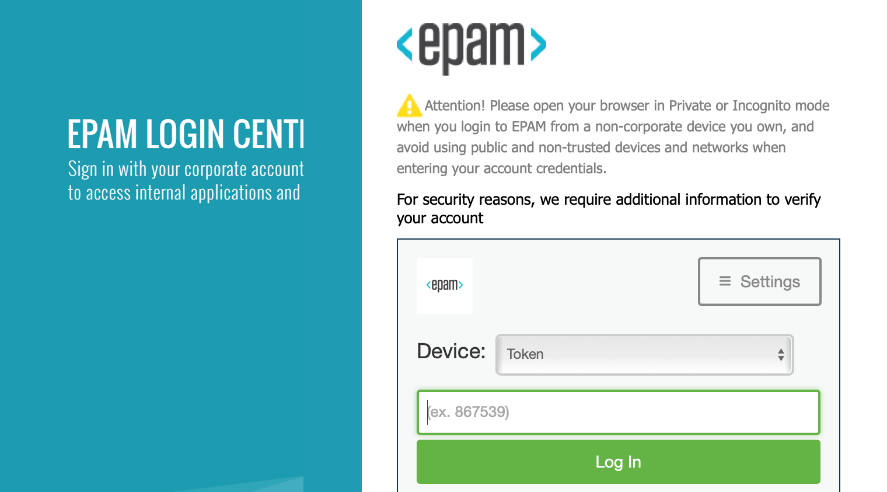
1. Launch the application;
2. Enter Portal address **vpn.epam.com** and tap **CONNECT**:



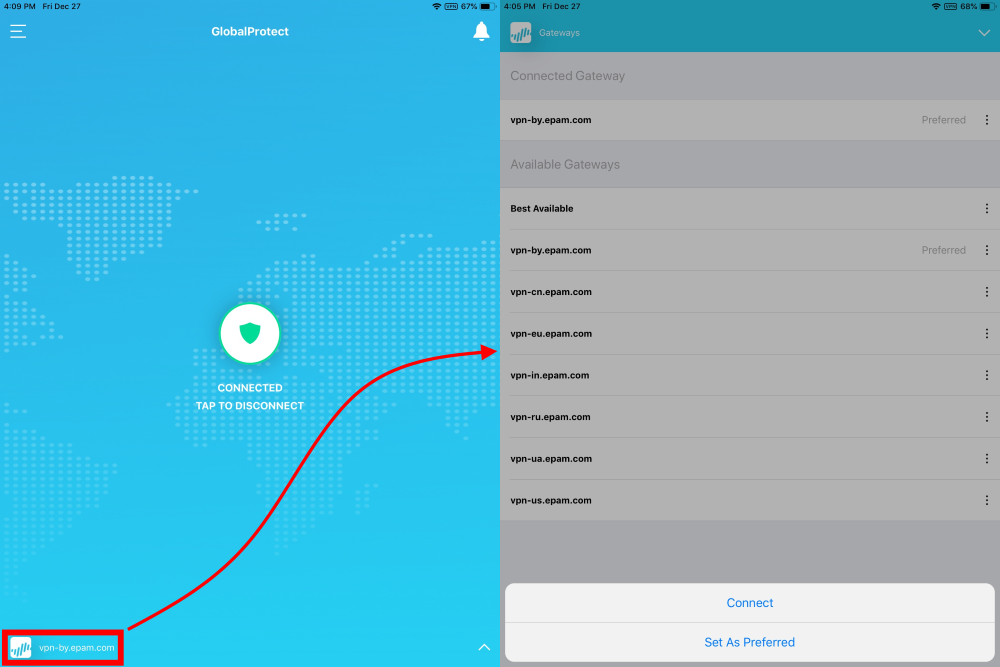
1. Enter your *Name* (i.e. FirstName\_LastName@epam.com) and *Password*, and then tap **SIGN IN**:



1. Enter DUO two-factor passcode (or choose another option in *Device* field) and tap **Log In**:

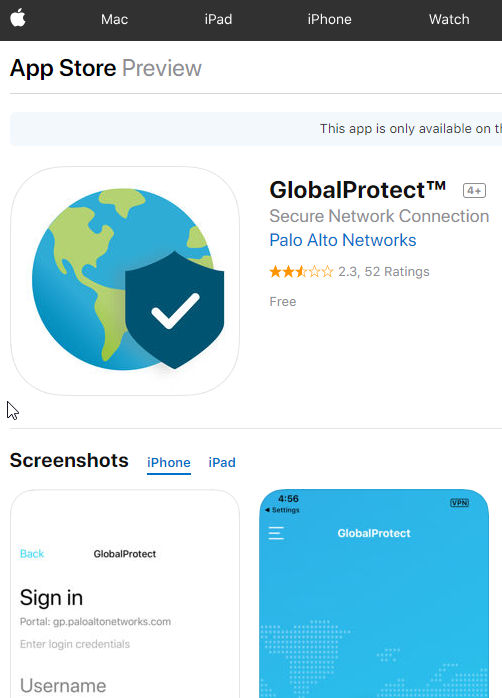


1. You have successfully connected to EPAM Global Protect VPN;
2. You can choose another VPN gateway to connect to or set the one as preferred if needed:

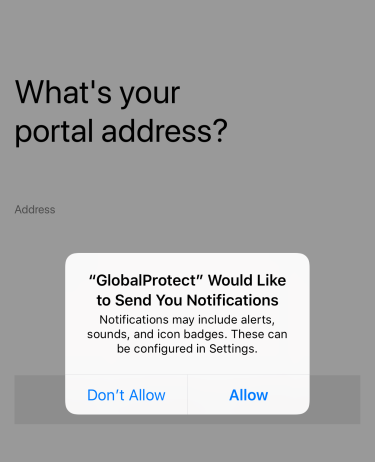


## Setting up your VPN on iOS

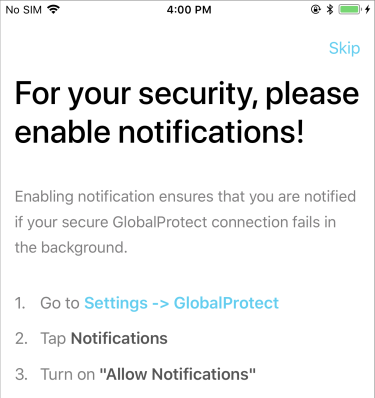
1. Install GlobalProtect App from App Store: <https://itunes.apple.com/us/app/globalprotect/id1400555706>



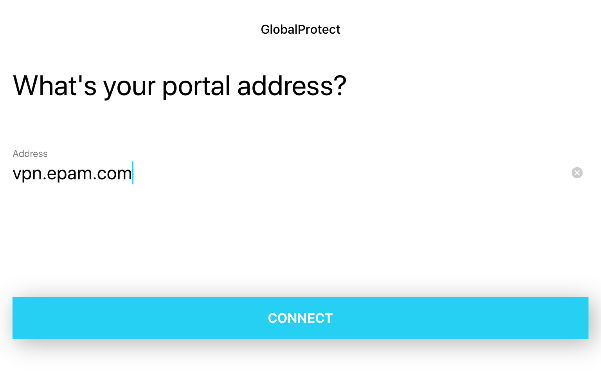
1. Launch the application;
2. If you have not enabled GlobalProtect notifications on your endpoint, a notification permission dialog appears. **Allow** GlobalProtect to send you notifications:



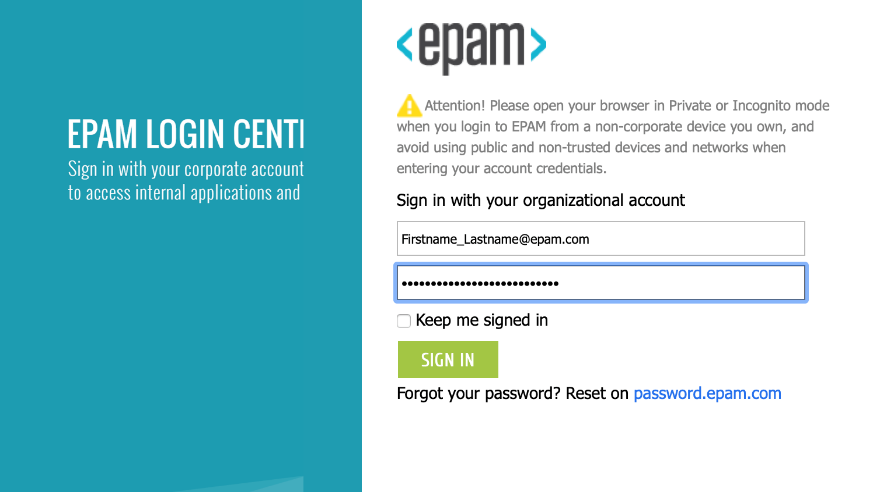
If you Don’t Allow GlobalProtect to send you notifications, a reminder appears the next time you launch the app. Tap the **Settings -> GlobalProtect** link to go to the notification permission screen, where you can enable notifications.



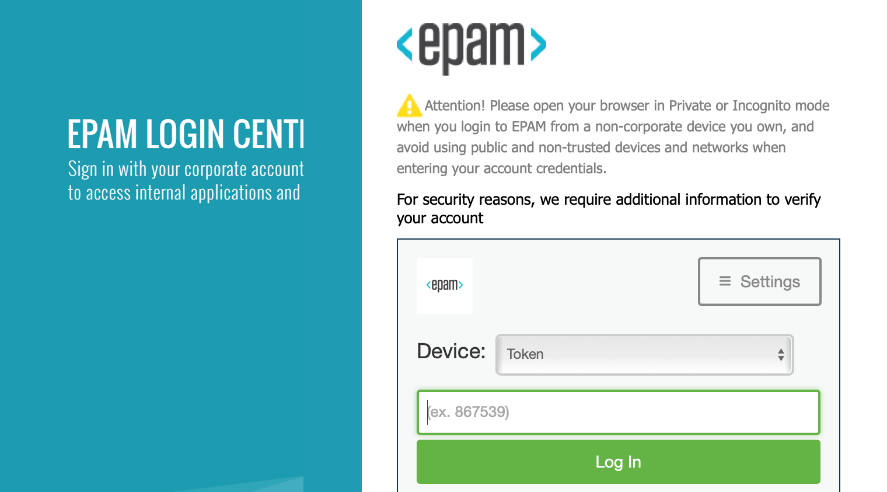
1. Enter Portal address **vpn.epam.com** and tap **CONNECT**:



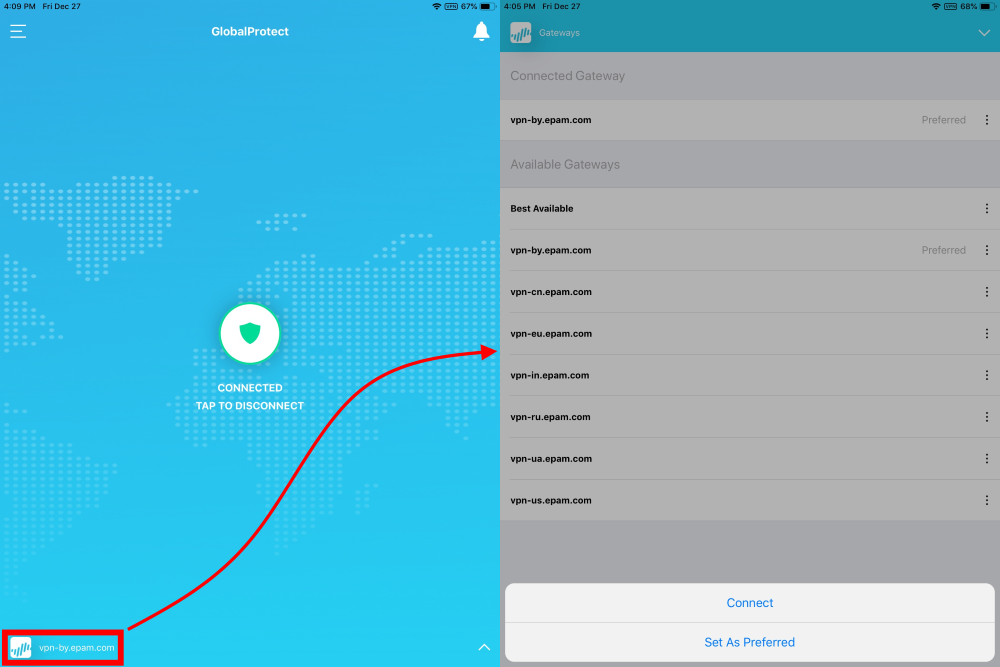
1. Enter your *Name* (i.e. FirstName\_LastName@epam.com) and *Password*, and then tap **SIGN IN**:



1. Enter DUO two-factor passcode (or choose another option in *Device* field) and tap **Log In**:



1. You have successfully connected to EPAM Global Protect VPN;
2. You can choose another VPN gateway to connect to or set the one as preferred if needed:



# Connecting to EPAM Network via Terminal Services Gateways (TSG)

The feature is especially needed when there is no possibility to establish VPN access to the EPAM network (customer’s network restrictions, home networks, etc.).

Feature is called Terminal Services Gateway. It uses HTTPS/SSL port 443, opened in most networks.

To use this connection method, do the following:

1. Make sure sleep mode is disabled on the workstation you try to connect to (this option is enabled for all EPAM workstations by default).

How to turn off sleep mode in Windows 7:

* Go to Start 🡪 Control Panel 🡪 Power Options;
* Select Change when the computer sleeps;
* Choose Never from “Put the computer to sleep” option and Save changes.

In Win 8:

* Go to Start 🡪 Control Panel 🡪 Power Options;
* Select “Change plan settings”;
* Choose *Never* from “Put the computer to sleep” option and *Save changes*.

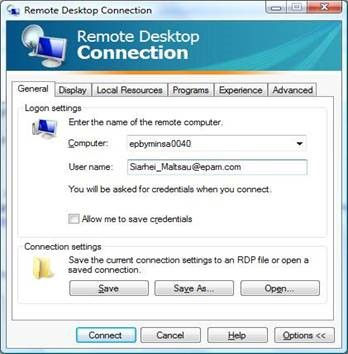
In macOS:

* Click on the blue/black apple icon in the upper left corner of your screen, and choose *System Preferences;*
* In the Hardware section, select Energy Saver;
* Make sure on the Settings for: drop-down box is set to Power Adapter;
* On the Sleep tab, move the sliding bar labeled Put the computer to sleep when it is inactive for: to Never.

1. Check your OS version. Windows XP SP3 needed. SP2 is not compatible. Windows Vista, Server 2008 and higher is recommended;
2. Remote Desktop Client v.6.1 is a MUST. Windows Vista and higher has it built-in. EPAM OS images of XP have it by default. Clean XP Sp3 does not have it. If working from some non-EPAM computer take the client here: <http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=6e1ec93d-bdbd-4983-92f7-479e088570ad>.
3. It is important to download and install the EPAM certificates: <http://ca.epam.com/cert/cert.zip>.

If all of above (OS version + RDP client version) is OK, the usage is simple.

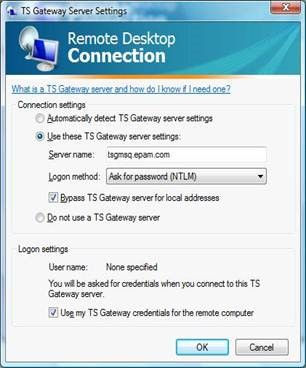
Open your RDP client (Remote desktop) connection, type the server in the EPAM network you want to connect to:



Then, open **Advanced** Tab, Press **Setting** button under “**Connect from anywhere**” section:



Set parameters as following: Server name – See [Appendix A.3](#AppendixA3). Login method – Ask for password (NTLM). Under Vista OS Tick “use my TS Gateway credentials for remote computer”. This will allow you to enter your password once. Windows XP needs to enter password for connection twice. Press **OK** to connect. Enter your NT Domain password ([First\_Last@epam.com](mailto:First_Last@epam.com)) 1(Vista) or 2(XP) times, when prompted.



Please note the feature is intended only for EPAM employees, no customer’s access is possible.

Please use network cable for better connection stability.

# Wi-Fi Access

## EPAM Guest Connection

### Guest Wi-Fi account types

There are 2 types of guest Wi-Fi account accounts:

* Personal account – an account for an external user, customer representative attending an EPAM office. Maximum access duration is 14 calendar days. Access is allowed from maximum 3 devices;
* Impersonal account – a single group account for external users, customer representatives attending mass events in an EPAM office. Maximum access duration is 5 calendar days. Access is allowed from maximum 100 devices.

**Important!** Guest Wi-Fi accounts of Personal type can be created and managed by users with special permissions (members of ‘WFT Guest Wi-Fi Portal Users’ Distribution Group) via the Guest Wi-Fi portal: http://guestwifi.epam.com.   
  
Guest Wi-Fi accounts of Impersonal type are created and managed only by Support team upon a [request](https://support.epam.com/esp/ess.do?ctx=docEngine&file=svcDisplay&query=name=%22GuestWiFiPortal%22).

### EPAMGuests

1. Connect your computer to WiFi network with SSID “**EPAMGuests**”:

* Network name (SSID): EPAMGuests;
* Network Authentication: Open;
* Data encryption: Disabled.

1. Open Internet Explorer (or other browser) and go to [https://wifi.epam.com](https://wifi.epam.com/)/login.html (your Internet browser will redirect you to the page automatically from some URL if http redirection is permitted in the settings of your browser);
2. Use provided credentials for web authentication;
3. You can de-authenticate on page <https://wifi.epam.com/logout.html>.

You will only be able to connect to the Internet with no access to the Company’s network.

1. Proxy should be disabled at your browser to be able to authenticate.

In case of any problem, please contact Support Team at [support@epam.com](mailto:Support@epam.com) or call 50911 for assistance.

## EPAM Employee Connection

There are two WiFi SSIDs for EPAM employee’s connections: EPAM8021x5 and EPAM8021x (please note that EPAM8021x5 SSID is preferable to use).

### EPAM8021x

#### Windows 7

1. Please connect to “EPAMGuest” SSID and install both EPAM certificates Rootca and Intermediate certificate from the page <http://cert.epam.com> if it’s not been installed yet:

**Important!** You have to install [rootca](http://cert.epam.com/rootca.cer) to root certificate storage. Click [rootca](http://cert.epam.com/rootca.cer) оn the web page 🡪 Open 🡪Install Certificate 🡪 Next 🡪 Place all certificates in the following store 🡪 Browse 🡪 Trusted Root Certification Authorities 🡪 Ok 🡪 Next 🡪 Finish.

1. Open Manage Wireless Networks by clicking the Start button🡪 Control Panel 🡪 Network and Internet 🡪 Network and Sharing Center, and then click Manage wireless networks in the left pane;
2. Click Add, click Manually create a network profile:

* Network name: EPAM8021x;
* Security type: 802.1X.

1. Click Next, Change connection settings, Security tab:

* Security Type: WPA2-Enterprise;
* Encryption type: AES;
* Choose the network authentication method: Microsoft: Protected EAP (PEAP).

1. Check Remember my credentials for this connection each time I’m logged on;
2. Click Advanced settings;
3. Check Specify authentication mode and choose User or computer authentication;
4. Check Enable single sign on for this network and choose Perform immediately before user logon;
5. Press Ok;
6. Click Settings. Check Validate server certificate and installed EPAM certificates in Trusted Root Certification Authorities;
7. Choose Secured password (EAP-MSCHAP v2) in the Select Authentication Method field;
8. Check Enable Fast Reconnect;
9. Press twice Ok and Close;
10. Connect to the network by clicking the Start button 🡪 Control Panel 🡪 Network and Internet 🡪 Network and Sharing Center 🡪 Connect to a network, click EPAM8021x and press Connect.

#### macOS

1. Please connect to “EPAMGuest” SSID and install both EPAM root certificates from the page <http://cert.epam.com> if it is not installed yet (download [rootca](http://cert.epam.com/rootca.cer) certificate from the web page. Twice click the certificate and press Always Trust, type your password and click Update Settings);
2. Choose Apple menu > System Preferences, and then click Network;
3. In the Wi-Fi main menu, if it’s necessary, click Turn WiFi On;
4. Select WiFi SSID EPAM8021x from the Network Name list at right;
5. Use Username: <your EPAM FirstName\_LastName@epam.com and EPAM MS Windows password for wireless authentication.

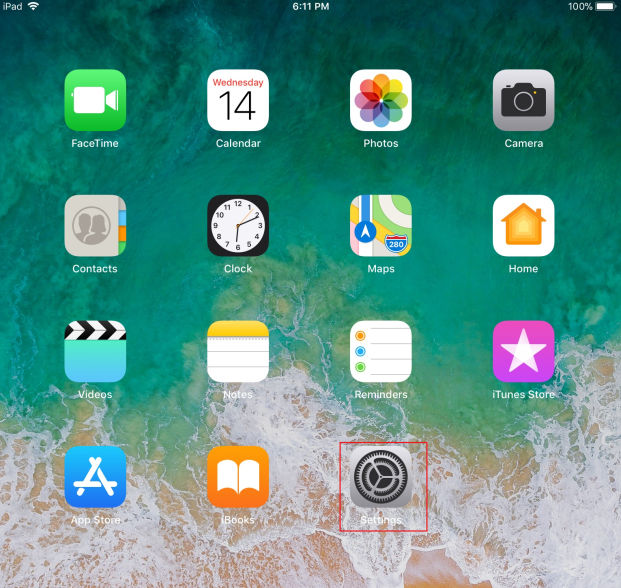
If you had access to this SSID before but then your Windows password was changed, you may get the error "Could not join "EPAM8021x. A connection timeout occurred." You can fix the problem if you remove EPAM8021x (your stored password) from Launchpad 🡪 Utilities 🡪 Keychain Access 🡪 Keychains login.

#### Android

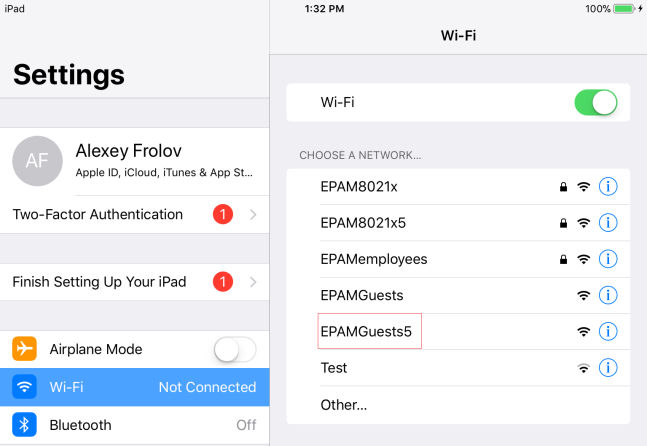
1. Please connect to “EPAMGuest” SSID and install both EPAM certificates Rootca and Intermediate certificate from the page <http://cert.epam.com> if it’s not been installed yet (You can verify whether the certificates were installed at the page <htts://radius.epam.com>. If certificates are installed correctly, then you don’t get any security alert on the page:
2. **1.**Use standard Android Internet browser for installing certificates from web page.
3. **2.**On some Android you can install certificates correctly only from SD card. Copy certificates in root folder SD card and go to Settings 🡪 Security 🡪 Credential storage 🡪 Install from storage.
4. **3.**Some devices support only .crt extension of certificates files. Change extension from .cer to .crt before installing).
5. From the Android Home screen, tap Menu then tap Settings;
6. Tap Wireless and network and then tap Wi-Fi settings;
7. Tap Wi-Fi to turn-on wireless (if not already on);
8. From the list of Wi-Fi networks, tap EPAM8021x;
9. Select PEAP from EAP method drop-down menu;
10. Select MSCHAPV2 from Phase 2 authentication drop-down menu;
11. Select installed root certificate from CA certificate;
12. Type your EPAM MS Windows Username in Identity field (correct format is <your EPAMusername>@epam.com);
13. Client certificate and Anonymous identity has to be blank;
14. Type your EPAM Windows password in Wireless password field;
15. Click Connect.

#### iOS

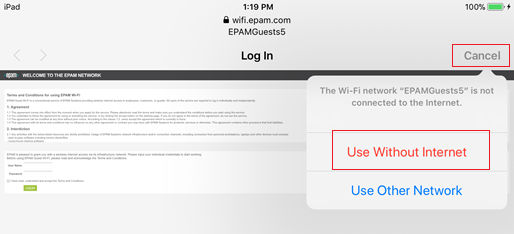
1. Go to your home screen and tap on “Settings”:



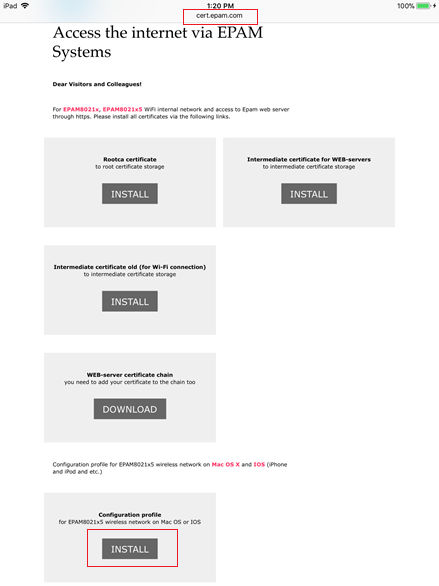
1. Connect to EPAMGuests5 network:



You will see the web-authentication page. Press Cancel and Use Without Internet:

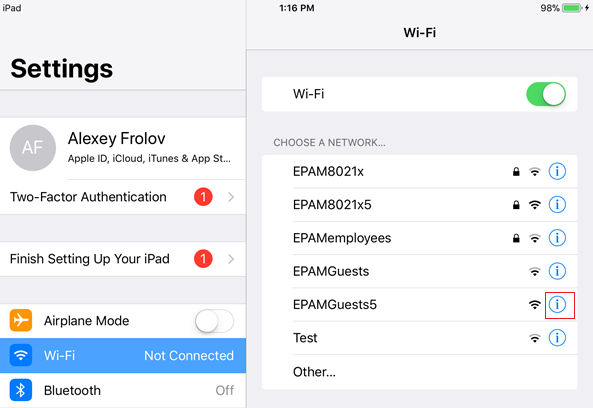
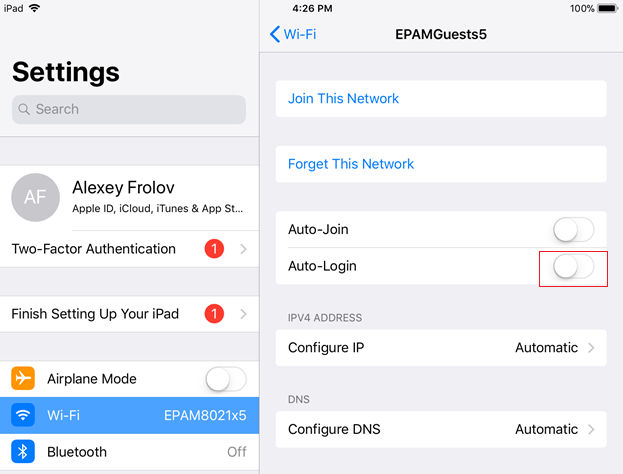


1. Install Configuration profile for EPAM8021x5 wireless network on macOS or IOS from <http://cert.epam.com>. Open Safari browser and go to <http://cert.epam.com>:

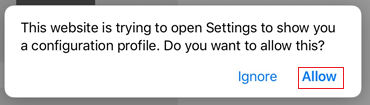


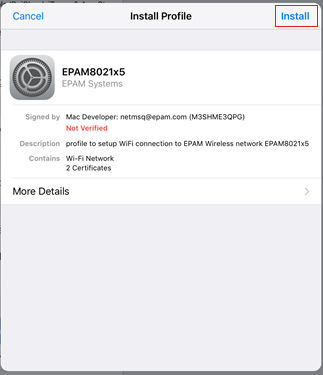
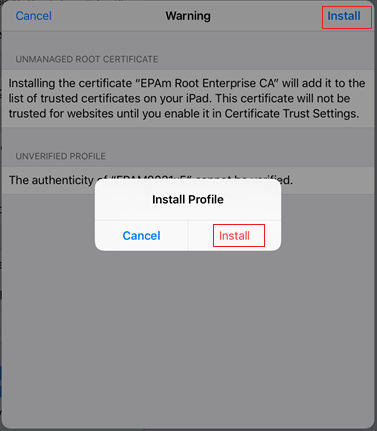
1. In case of any troubles with connection to EPAMGuests5 and accessing <http://cert.epam.com> switch off Auto-Login in WiFi settings:

Click Settings 🡪 Wi-Fi 🡪 EPAMGuests5 🡪 switch off Auto-Login

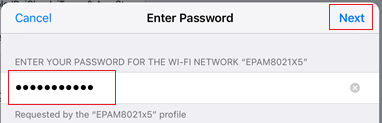
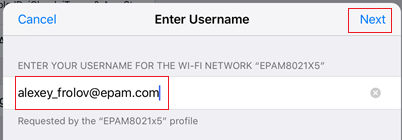
 

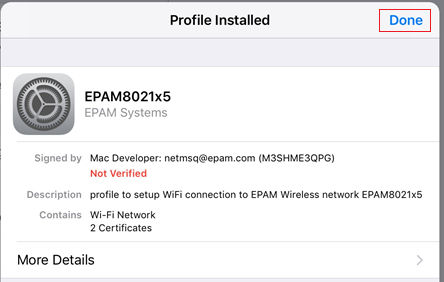
1. Click Allow and Install three times when Install Profile page appear:



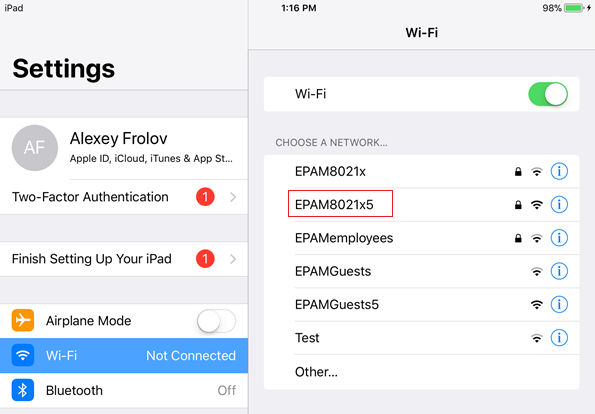
 

1. Use your Username (FirstName\_LastName@epam.com) 🡪 Next 🡪 EPAM MS Windows password 🡪 Done:

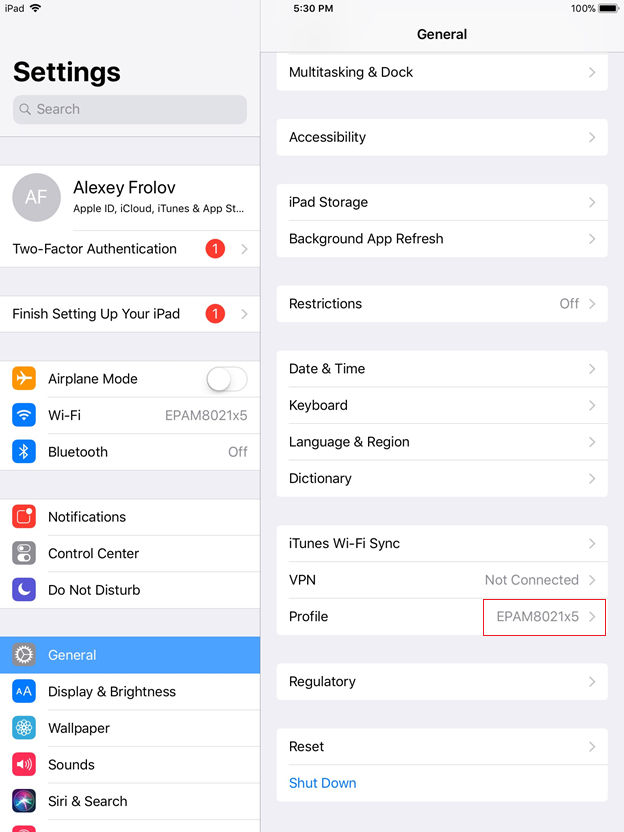
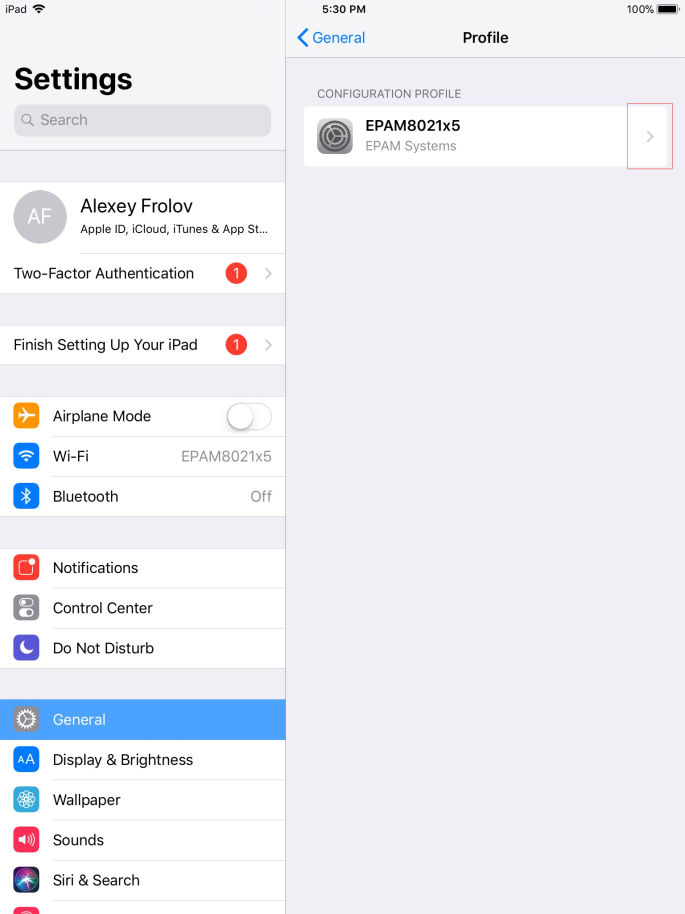


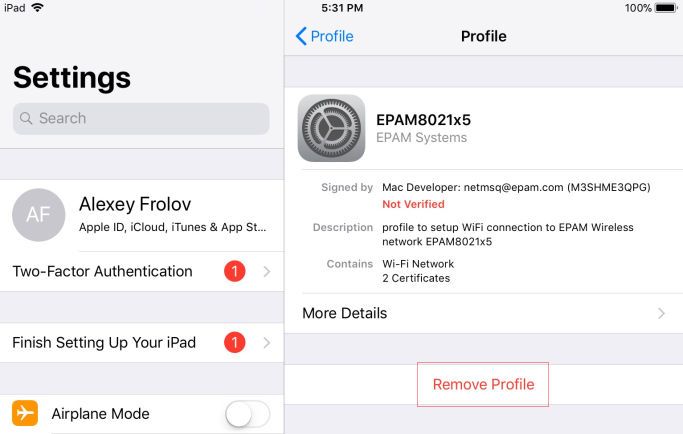


1. Press Settings 🡪 Wi-Fi 🡪 Choose EPAM8021x5 network:



1. To remove EPAMWiFi profile, press Settings  General  Choose Profile EPAMWiFi 🡪 🡪 Delete Profile on the bottom.



1. GATES
   1. Main VPN GATES

The following gateways are available from **vpn.epam.com** portal:

|  |  |  |
| --- | --- | --- |
| VPN Server Address | VPN Server Location | Can be used for employees in Locations |
| vpn-by.epam.com | Minsk | Worldwide, BY is preferred |
| vpn-cn.epam.com | Hong Kong | Worldwide, CN is preferred |
| vpn-eu.epam.com | Budapest | Worldwide, EU is preferred |
| vpn-in.epam.com | Hyderabad | Worldwide, IN is preferred |
| vpn-ru.epam.com | Saint-Petersburg | Worldwide, RU is preferred |
| vpn-ua.epam.com | Kyiv | Worldwide, UA is preferred |
| vpn-us.epam.com | US | Worldwide, US is preferred |

* 1. Regional VPN portals

|  |  |  |
| --- | --- | --- |
| VPN Portal Address | VPN Server Location | Can be used for employees in Locations |
| vpnkar.epam.com | Karaganda | Worldwide, KZ is preferred |
| vpnsslgda.epam.com | Gdansk | Gdansk |
| vpnssllvi.epam.com | Lviv | Lviv |
| vpnsslsuz.epam.com | Suzhou | Suzhou |
| vpnsslszx.epam.com | Shenzhen | Shenzhen |

* 1. TSG Gates

|  |  |  |
| --- | --- | --- |
| TSG Server name | TSG Server Location | Can be used as PRIMARY in Country |
| TSGMSQ.epam.com | Belarus | Belarus |
| TSGUA.epam.com | Ukraine | Ukraine |
| TSGEU.epam.com | Europe | Europe, other countries not listed |
| TSGRU.epam.com | Russia | Russia, Kazakhstan |
| TSGUS.epam.com | US | US, Canada, Mexico |
| TSGIN.epam.com | India | China, India |
| **In case of troubles you can use any gateway with some degradation in performance** | | |

| REVISION HISTORY | | | | | |
| --- | --- | --- | --- | --- | --- |
| Ver. | Description of Change | Author | Date | Approved | |
| Name | Effective Date |
| 0.1 | Transferred into the new template | Zoya Bialiankina | 31-Oct-2005 |  |  |
| 0.2 | Reviewed and updated | Vasili Hronski | 14-Nov-2005 |  |  |
| 0.3 | Reviewed | Tamas Kohegyi | 27-Jan-2006 |  |  |
| 0.4 | Reviewed, updated with Valery Maliutsin’s correction. | Tamas Kohegyi | 10-Apr-2006 |  |  |
| 1.0 | Updated and Reviewed | Balazs Fejes1 | 10-Apr-2006 | Balazs Fejes1 | 10-Apr-2006 |
| 1.1 | VPN setting for Kyiv and St. Petersburg offices were added | Zoya Bialiankina | 17-Jul-2006 | Tamas Kohegyi | 26-Jul-2006 |
| 1.2 | Updated Minsk office technical info | Siarhei Maltsau | 26-Mar-2007 |  |  |
| 1.3 | St. Petersburg VPN is removed. | Tamas Kohegyi | 10-Apr-2007 |  |  |
| 1.4 | Reviewed | Siarhei Maltsau | 28-Sep-2007 |  |  |
| 1.5 | Editorial review | Richard Bötös | 23-Nov-2007 | Balazs Fejes1 | 13-Dec-2007 |
| 1.6 | SSL Network extender updates | Vasili Hronski  Valery Maliutsin | 24-Sep-2008 |  |  |
| 1.7 | Editorial review of changes. | Richard Bötös | 30-Sep-2008 | Balazs Fejes1 | 28-Nov-2008 |
| 1.8 | Added SSTP Connection from Customer Network | Siarhei Maltsau,  Tamas Kohegyi | 07-Sep-2009 |  |  |
| 1.9 | Editorial review of changes | Mihaly Beviz | 10-Sep-2009 | Balazs Fejes1 | 29-Oct-2009 |
| 1.10 | Guest connection has been added  Dial-in has been removed | Valery Maliutsin | 22-Sep-2010 |  |  |
| 1.11 | QA review is performed | Andrei Zemliakou | 5-Nov-2010 | Balazs Fejes1 | 5-Dec-2010 |
| 1.12 | Updated Karaganda and Kyiv offices technical info, TSG access details | Siarhei Maltsau | 06-Jul-2011,  17-Oct-2011 |  |  |
| 1.13 | Added setting up VPN under Windows 7 and MAC OS instructions. Updated Wi-Fi Access instructions. | Vasili Gronski  Sviatlana Salauyova | 23-Nov-2011 |  |  |
| 1.14 | QA review | Andrei Zemliakou | 24-Nov-2011 | Andrei Kureichyk | 19-Dec-2011 |
| 1.15 | URL for certificates was updated | Siarhei Maltsau | 04-Jul-2012 |  |  |
| 1.16 | QA review | Andrei Zemliakou | 05-Jul-2012 | Andrei Kureichyk | 05-Jul-2012 |
| 1.17 | Added setting up VPN under Ubuntu 12.04 | Maksim Liauchuk Aliaksandr Arlou1 | 09-Jul-2012 |  |  |
| 1.18 | QA review | Yury Rybkin | 10-Jul-2012 | Andrei Kureichyk | 31-Jul-2012 |
| 1.19 | p. “5. Connecting to EPAM Network via SSL Network Extender” was removed; Wi-Fi instruction was updated – p. 5. Wi-Fi Access | Vasili Gronski  Olga Sidorova | 31-Jul-2012 |  |  |
| 1.20 | QA review | Yury Rybkin | 06-Aug-2012 |  |  |
| 1.21 | Editorial review | Hanna Khaletskaya | 08-Aug-2012 |  |  |
| 1.22 | Ready for approval | Andrei Zemliakou | 09-Aug-2012 | Andrei Kureichyk | 09-Aug-2012 |
| 1.23 | VPN for Windows 8 added | Siarhei Maltsau | 18-Nov-2012 |  |  |
| 1.24 | QA review | Sviatlana Pushkina | 20-Nov-2012 | Andrei Kureichyk | 27-Nov-2012 |
| 1.3 | Wi-Fi instruction was updated – p. 5. Wi-Fi Access. P. 3.2.2.screenshot updated | Vasili Gronski | 31-January-2013 | Andrei Kureichyk | 18-Feb-2013 |
| 1.3.1 | p. 5, 2. Rules of Use was updated; p. 5, 3.1. Processing the Request for Access was updated | Liudmila Dzikevich | 17-April-2013 | Andrei Kureichyk | 15-May-2013 |
| 1.3.2 | p. 5 Wi-Fi Access was updated | Alexey Frolov | 22-July-2013 |  |  |
| 1.3.3 | QA review | Hanna Khaletskaya | 22-July-2013 |  |  |
| 1.3.4 | p.3.1 Processing the Request for Access | Olga Kauta | 19-June-2014 |  |  |
| 1.3.5 | QA Review | Anastasia Yatchenko | 19-June-2014 | Andrei Zemliakou | 02-Dec-2015 |
| 1.3.6 | p. 3.3.3 Setting your VPN under Windows 10 was added | Ekaterina Polezhaeva | 03-Mar-2016 | Mikhail Kazouski | 09-Mar-2016 |
| 1.4 | Updated with new EPAM template, QA review | Oleksandr Dmytriyev | 10-Mar-2016 | Mikhail Kazouski | 10-Mar-2016 |
| 1.5 | p. 3.3.3 Setting up your VPN under Windows 8.1;  p. 3.3.7 Setting up your VPN under Android | Ekaterina Polezhaeva | 21-Apr-2016 |  |  |
| 1.6 | QA Review | Viktoryia Hilevich | 26-Apr-2016 |  |  |
| 1.7 | Added the steps of checking “Allow other people to use this connection” option for Windows 7, 8 and 10 | Olga Martyshuk | 30-May-2016 |  |  |
| 1.8 | QA Review | Viktoryia Hilevich | 13-Jun-2016 |  |  |
| 1.9 | p.3.3.6 Setting up your VPN under Mac OS X 10.12 (Sierra) added | Iuliia Myznikova | 20-Sep-2016 |  |  |
| 2.0 | p. 3.3.7 Setting up your VPN under iOS 10 added | Iuliia Myznikova | 20-Sep-2016 |  |  |
| 2.1 | QA Review | Viktoryia Hilevich | 23-Sep-2016 | Mikhail Kazouski | 23-Sep-2016 |
| 2.2 | p. 3.3.6 Setting up your VPN (l2TP) under Mac OS X 10.12 (Sierra) was updated | Iuliia Myznikova | 17-Oct-2016 |  |  |
| 2.3 | Appendix B. Keys was added | Iuliia Myznikova | 17-Oct-2016 |  |  |
| 2.4 | Numeration corrected | Iuliia Myznikova | 17-Oct-2016 |  |  |
| 2.5 | QA Review | Roman Komlyk | 18-Oct-2016 | Mikhail Kazouski | 19-Oct-2016 |
| 2.6 | Appendix A.2 updated | Uladzimir Fiasenka | 21-Jun-2017 |  |  |
| 2.7 | QA Review | Viktoryia Hilevich | 22-Jun-2017 | Ivan Tabaravets | 05-Jul-2017 |
| 2.8 | Updated | Katsiaryna Zas | 18-Dec-2017 |  |  |
| 2.9 | Confirmed | Valery Maliutsin | 18-Dec-2017 |  |  |
| 2.10 | Updated types of Wi-Fi accounts mentioned within p. 5.1.1 | Katsiaryna Zas | 26-Dec-2017 |  |  |
| 2.11 | QA Review | Viktoryia Hilevich | 26-Dec-2017 | Ivan Tabaravets | 26-Dec-2017 |
| 3.0 | Technical change (p.5.1.1) | Viktoryia Hilevich | 10-Jan-2018 | Andrei Zemliakou | 10-Jan-2018 |
| 3.1 | Updated | Alexey Frolov | 26-Feb-2018 |  |  |
| 3.2 | Reviewed | Sergey Golobokov | 26-Feb-2018 |  |  |
| 4.0 | QA Review | Viktoryia Hilevich | 26-Feb-2018 | Ivan Tabaravets | 26-Feb-2018 |
| 4.1 | Updated p. 5.1.1: described rules of guest wi-fi creation | Katsiaryna Zas | 20-Mar-2018 |  |  |
| 4.2 | Confirmed by owner | Valery Maliutsin | 20-Mar-2018 |  |  |
| 4.3 | QA Review | Viktoryia Hilevich | 21-Mar-2018 | Ivan Tabaravets | 21-Mar-2018 |
| 4.4 | Updated p.5.2.1 EPAMEmployees removed | Alexey Frolov | 11-Mar-2019 |  |  |
| 4.5 | Updated p.3 CONNECTING TO EPAM NETWORK VIA GLOBAL PROTECT VPN inserted | Sergey Golobokov | 12-Mar-2019 |  |  |
| 4.6 | Updated p.3.3, Updated Appendix B1 | Sergey Golobokov | 14-Mar-2019 |  |  |
| 5.0 | QA Review | Aliaksandra Valozhynskaya | 15-Mar-2019 |  | 15-Mar-2019 |
| 5.1 | Updated p.3.3.6 | Sergey Golobokov | 05-Apr-2019 |  |  |
| 6.0 | QA Review | Aliaksandra Valozhynskaya | 05-Apr-2019 | Ivan Tabaravets | 05-Apr-2019 |
| 6.1 | P. 3.3, 3.4 updated. Added p. 3.4.1 | Nikita Ponomaryov | 30-May-2019 |  |  |
| 7.0 | QA Review | Aliaksandra Valozhynskaya | 03-Jun-2019 | Ivan Tabaravets | 03-Jun-2019 |
| 7.1 | Updated p.3.4.1. pictures in pp.3.5-3.6 | Nikita Ponomaryov | 11-Jun-2019 |  |  |
| 8.0 | QA Review | Aliaksandra Valozhynskaya | 17-Jun-2019 | Ivan Tabaravets | 18-Jun-2019 |
| 8.1 | Section 2 - updated | Oleksandr Dmytriyev | 23-Oct-2019 |  |  |
| 9.0 | QA Review | Valeriy Neumoin | 24-Oct-2019 | Ivan Tabaravets | 24-Oct-2019 |
| 9.1 | QA Review, version number corrected | Valeriy Neumoin | 22-Nov-2019 | Andrei Zemliakou | 26-Nov-2019 |
| 9.2 | Images type is changed: .png to .jpeg | Valeriy Neumoin | 11-Nov-2019 |  |  |
| 9.3 | Removed section on Legacy VPN connection, Appendix B.  Updated pp. 3.1, p. 3.2 – 3.4, Appendixes A.1, A.2 | Nikita Ponomaryov | 09-Jan-2020 |  |  |
| 10.0 | QA Review | Aliaksandra Valozhynskaya | 10-Jan-2020 | Ivan Tabaravets | 10-Jan-2020 |