

|  |
| --- |
| Work Instruction  Remote And Guest Access To Corporate Network Resources |
| Quality Management System |

| 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 | |
| SSL | Secure Sockets Layer |
| QMS | Quality Management System |
| SEPG | Software Engineering Process Group |
| SSTP | Secure Socket Tunneling Protocol |
| WiFi | Wireless network |
| VPN | Virtual Private Network |
| SID | Security Identifier |
| TSG | Terminal Services Gateway |

Contents

[1 Introduction 4](#_Toc509414146)

[1.1 Purpose 4](#_Toc509414147)

[1.2 Scope 4](#_Toc509414148)

[2 Rules of Use 4](#_Toc509414149)

[3 Connecting to EPAM Network via Microsoft VPN Server 5](#_Toc509414150)

[3.1 Processing the Request for Access 5](#_Toc509414151)

[3.2 Logging of VPN Sessions 5](#_Toc509414152)

[3.3 Configuring VPN Connection 5](#_Toc509414153)

[3.3.1 Setting up your VPN under Windows 7 5](#_Toc509414154)

[3.3.2 Setting up your VPN under Windows 8 7](#_Toc509414155)

[3.3.3 Setting up your VPN under Windows 8.1 9](#_Toc509414156)

[3.3.4 Setting up your VPN under Windows 10 10](#_Toc509414157)

[3.3.5 Setting up your VPN (L2TP) under Mac OS X 10.12 (Sierra) 12](#_Toc509414158)

[3.3.6 Setting up your VPN under iOS 11 15](#_Toc509414159)

[3.3.7 Setting up your VPN under Ubuntu 12.04. 18](#_Toc509414160)

[3.3.8 Setting up your VPN under Android 20](#_Toc509414161)

[4 Connecting to EPAM Network via Terminal Services Gateways (TSG) 22](#_Toc509414162)

[5 Wi-Fi Access 25](#_Toc509414163)

[5.1 EPAM Guest Connection 25](#_Toc509414164)

[5.1.1 Guest Wi-Fi account types 25](#_Toc509414165)

[5.1.2 EPAMGuests 25](#_Toc509414167)

[5.1.3 EPAMGuests8021x 25](#_Toc509414168)

[5.1.3.1 Windows 7 25](#_Toc509414169)

[5.1.3.2 Windows XP SP3 26](#_Toc509414170)

[5.1.3.3 MAC OS X Lion 10.7.4 27](#_Toc509414171)

[5.1.3.4 Windows Mobile 5.x and 6.x 27](#_Toc509414172)

[5.1.3.5 Android 27](#_Toc509414173)

[5.1.3.6 iOS 5.x, 6.x 28](#_Toc509414174)

[5.2 EPAM Employee Connection 28](#_Toc509414175)

[5.2.1 EPAMemployees 28](#_Toc509414176)

[5.2.2 EPAM8021x 29](#_Toc509414177)

[5.2.2.1 Windows 7 29](#_Toc509414178)

[5.2.2.2 Windows XP SP3 29](#_Toc509414179)

[5.2.2.3 MAC OS X Lion 10.7.4 30](#_Toc509414180)

[5.2.2.4 Windows Mobile 5.x and 6.x 30](#_Toc509414181)

[5.2.2.5 Android 30](#_Toc509414182)

[5.2.2.6 iOS 31](#_Toc509414183)

[Appendix A. GATES 35](#_Toc509414184)

[Appendix A.1. VPN GATES 35](#_Toc509414185)

[Appendix A.2. TSG Gates 35](#_Toc509414186)

[Appendix B. KEYS 36](#_Toc509414187)

[Appendix B.1. L2TP VPN Shared Secret 36](#_Toc509414188)

# 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 of the EPAM.

The owner of this document is the Head of Network.

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

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

# Rules of Use

Only EPAM Systems Employees 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. 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;
* support Microsoft Point-to-Point Encryption (MPPE), which is the encryption type used by the EPAM VPN;
* 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 Microsoft VPN Server

## Processing the Request for Access

Permission to access the EPAM network using VPN (in case employee does not have such permissions yet) can be granted automatically without any approvals within a request submitted in [support.epam.com](https://support.epam.com/esp/ess.do?ctx=docEngine&file=svcDisplay&query=name=%22AccesstoEPAMResources_VPNtoEPAMNetwork%22).

## Logging of VPN Sessions

The time and duration of all client VPN sessions are logged. There is a tracking system on connection usage if Company’s Administration requests this.

## Configuring VPN Connection

The [Appendix A.1](#AppendixA1) contains VPN server addresses of various EPAM locations.

### Setting up your VPN under Windows 7

1. Open Control Panel 🡪 choose Network and Sharing Center 🡪 click on Set up a new connection or network 🡪 select Connect to a workplace

|  |  |
| --- | --- |
|  |  |

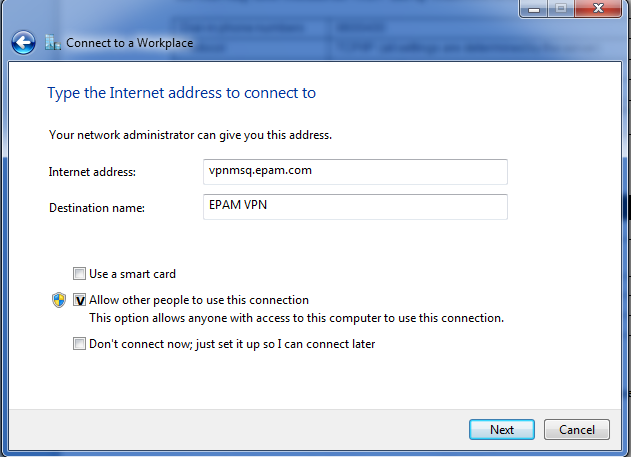
1. Check radio button “No, create a new connection” -> choose Use my internet connection

|  |  |
| --- | --- |
|  |  |

1. Fill in the fields as follows:

* Internet address: vpnmsq.epam.com
* Destination name: EPAM VPN

1. Check “*Allow other people to use this connection*” option:



1. Enter your EPAM e-mail address as User name (i.e. Firstname\_Lastname@epam.com), and your domain password.

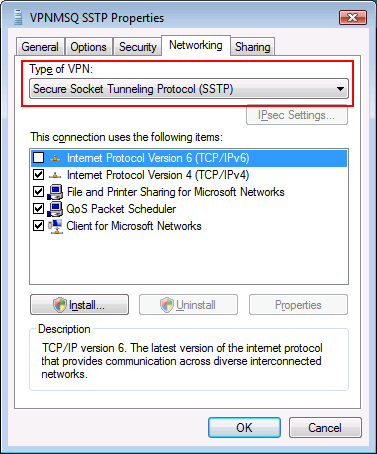
* User name: First\_Lastname@epam.com
* Password: \*\*\*\*\*\*\*\*\*\*



Some vital for VPN connection functioning network ports can be restricted at customer’s or public places firewalls. In this case you can try to use SSTP connection.

SSTP is available:

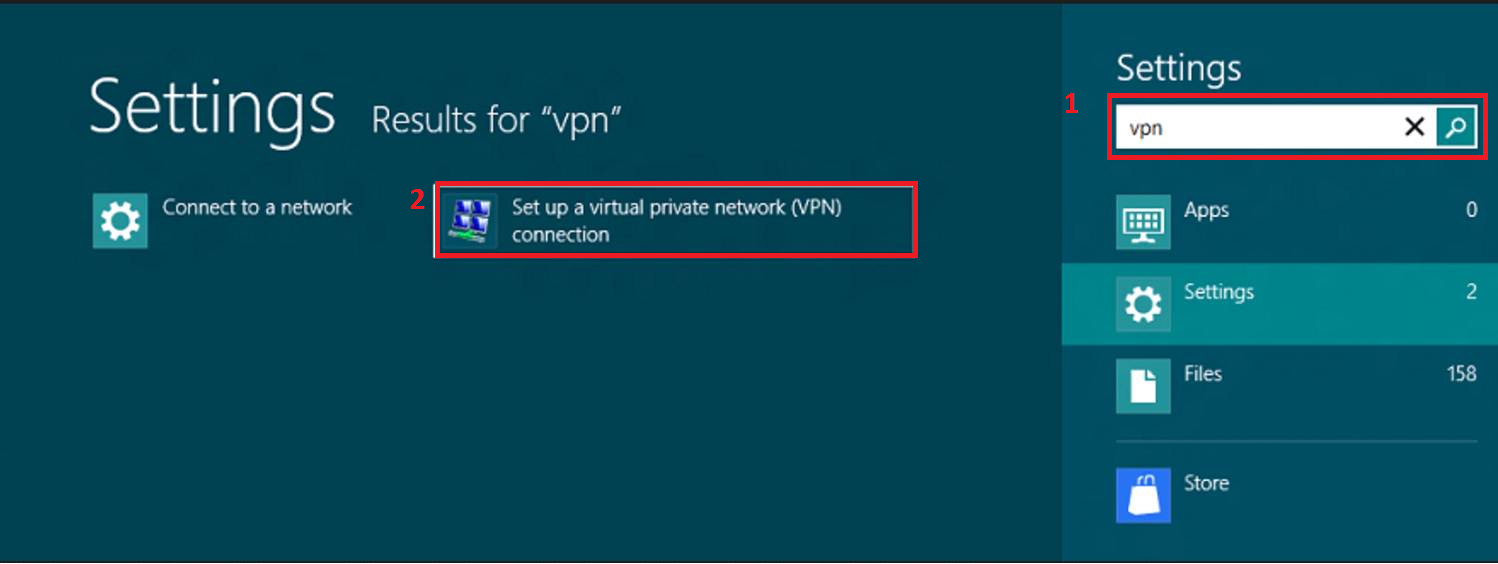
* in Windows 8, Windows 7, Windows Server 2008, Windows Vista SP1 and later operating systems
* if **Server Address/Internet address** is set as the full DNS name, e.x.vpnmsq.epam.com
* Configure VPN Connection properties as follows:



Usually it is not needed, as setting = Automatic is working well.

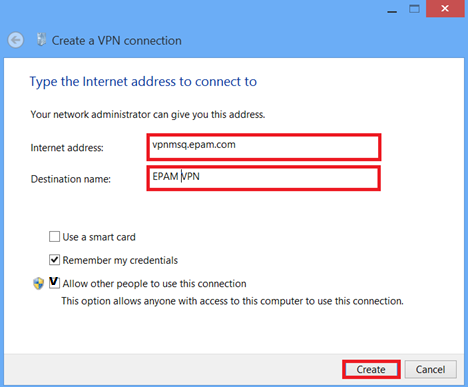
### Setting up your VPN under Windows 8

1. In Windows 8 you can use the Get Connected Wizard to create a VPN profile. Launch the wizard from Settings Search panel (Win+W), type in “vpn” in Settings field and then click Set up a virtual private network (VPN) connection.

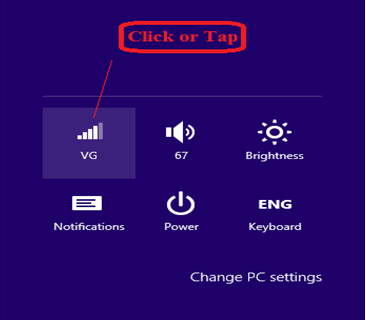


1. Fill in the fields as follows:

* Internet address: vpnmsq.epam.com (see Appendix A.1 for more information)
* Destination name: EPAM VPN
* Check “Allow other people to use this connection” option



1. Press Create Button.
2. Press **Win + i** or click Settings from Charms (**Win+C** hotkey) to open up the Settings panel, click the network icon at the bottom part of the panel to open up the Network Connection side panel. You will see the created VPN connection listed there. Simply click or tap it and Connect.

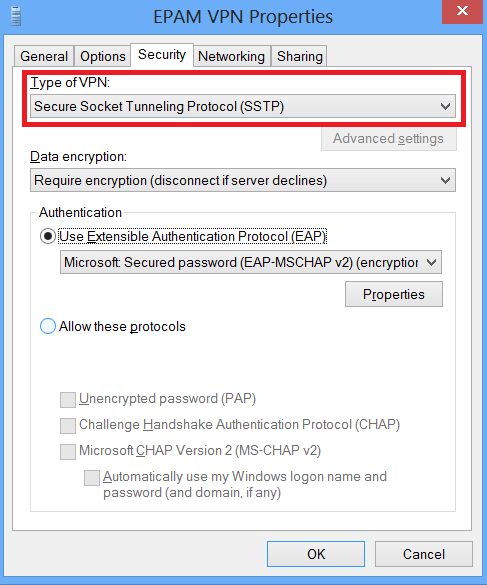


Some vital for VPN connection functioning network ports can be restricted at customer’s or public places firewalls. In this case you can try to use SSTP connection.

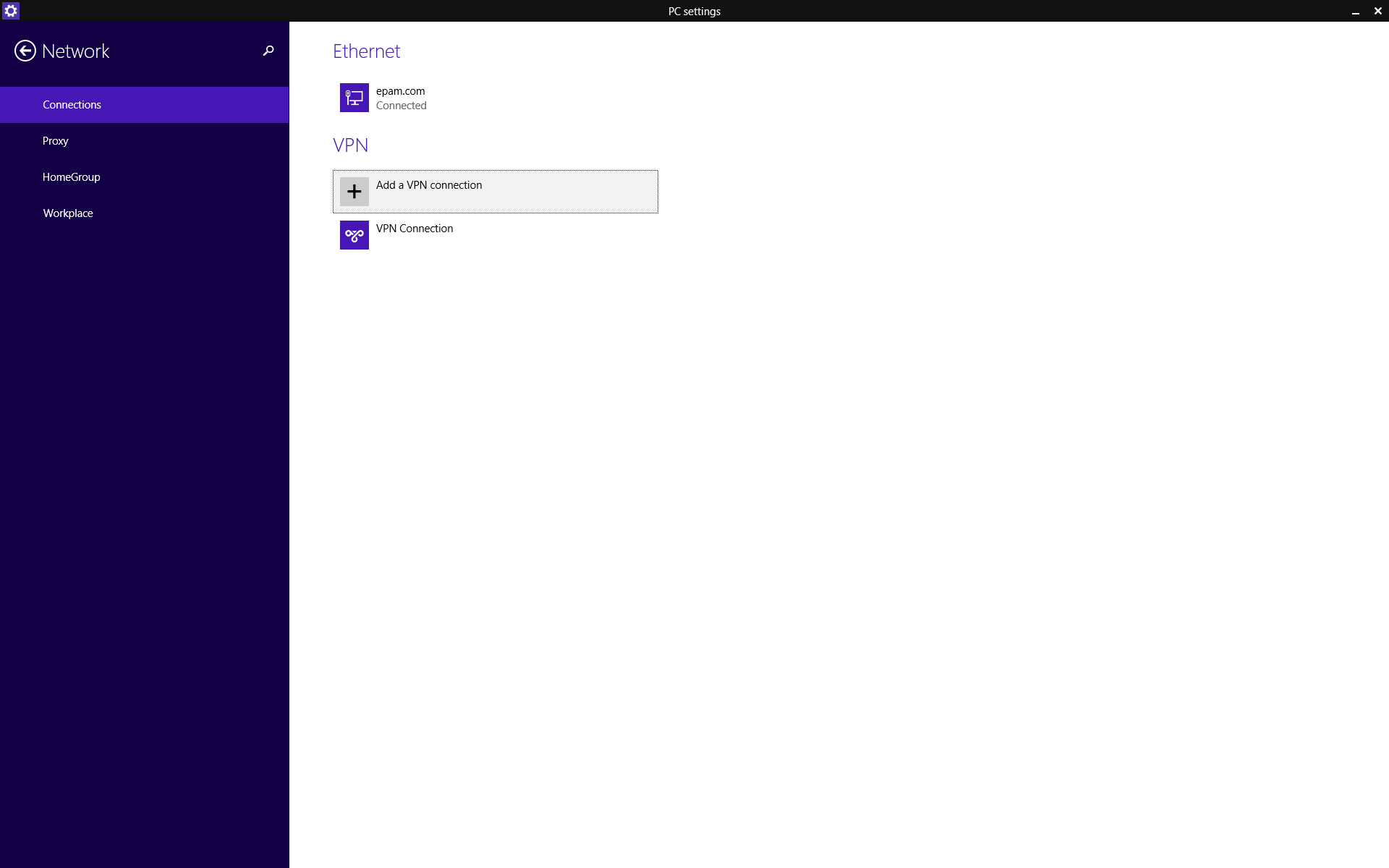
SSTP is available:

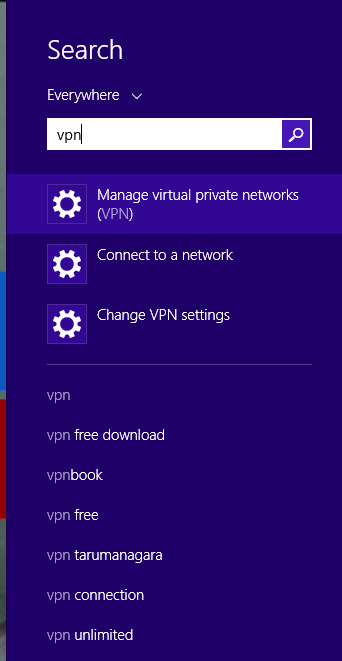
* in Windows 8, Windows 7, Windows Server 2008, Windows Vista SP1 and later operating systems
* if **Server Address/Internet address** is set as the full DNS name, e.x.vpnmsq.epam.com

1. Configure VPN Connection properties as on the screenshot:



### Setting up your VPN under Windows 8.1

1. Click Start 🡪 type VPN 🡪 choose Manage virtual private networks (VPN) -> Connections -> Add a VPN connection



1. Fill in the fields and click Save

**VPN provider:** Microsoft

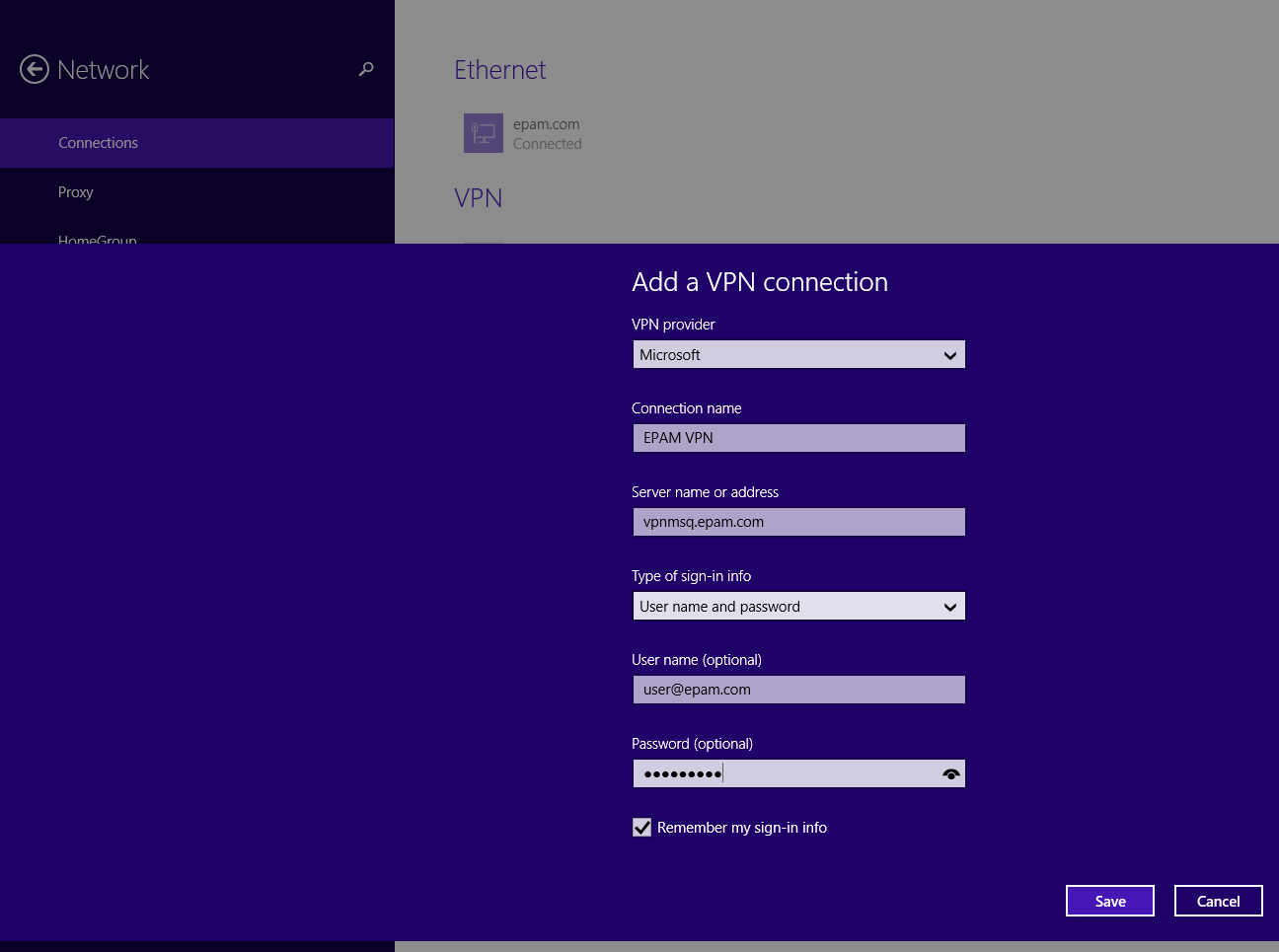
**Connection name**: EPAM VPN

**Server name or address:** vpnmsq.epam.com (see Appendix A.1 for more information)

**Type of sign-in info:** user name and password

**User name (optional):** [*First\_LastName@epam.com*](mailto:First_LastName@epam.com)

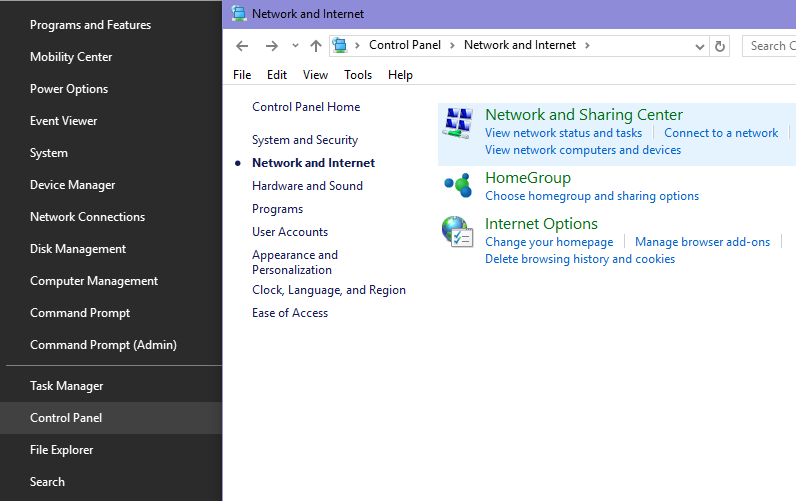
**Password (optional):** your EPAM domain password

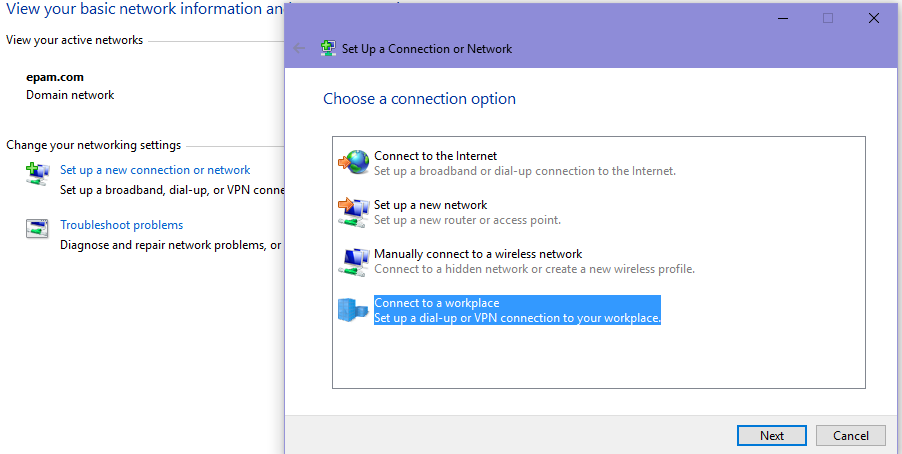


1. To start VPN connection, click Start -> type VPN -> Connect -> EPAM VPN -> Connect.

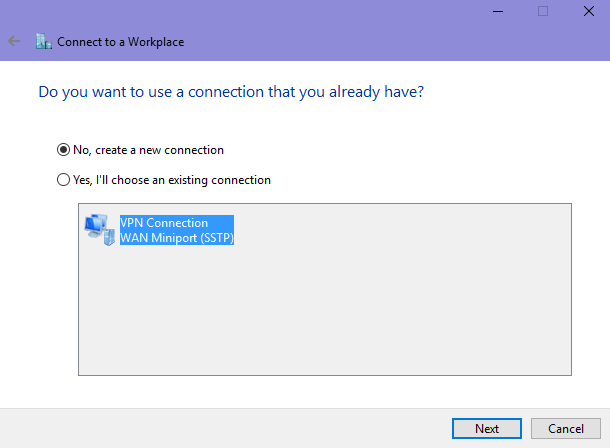
### Setting up your VPN under Windows 10

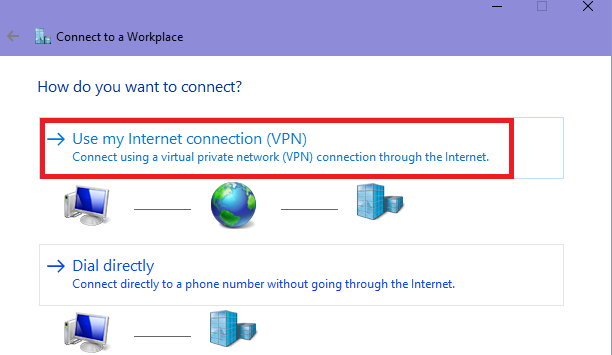
Right-click Start 🡪 Control Panel 🡪 Network and Internet 🡪 choose Network and Sharing Center 🡪 click on Set up a new connection or network 🡪 select Connect to a workplace





Check radio button “No, create a new connection” 🡪 choose Use my internet connection (VPN)

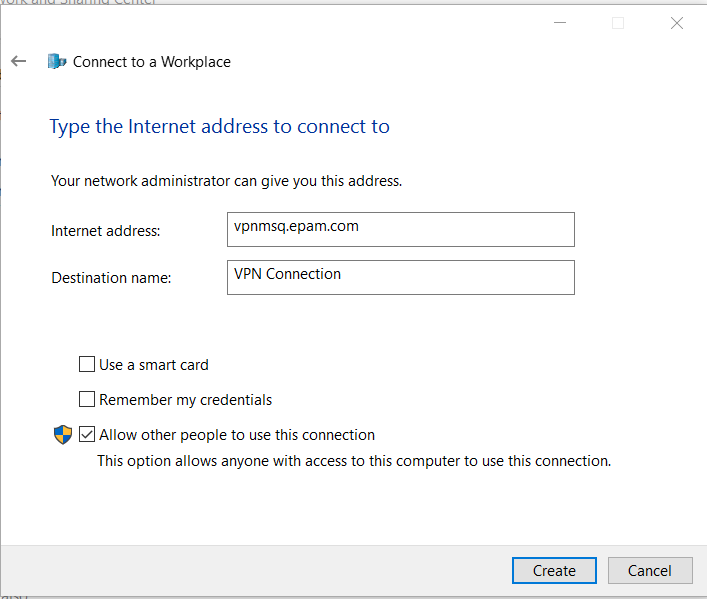




Fill in the fields as follows:

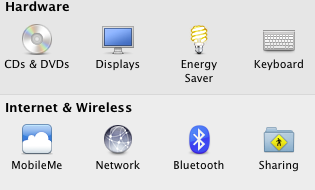
* Internet address: vpnmsq.epam.com (see Appendix A.1 for more information).
* Destination name: EPAM VPN.

Check “*Allow other people to use this connection*” option and click **Create:**

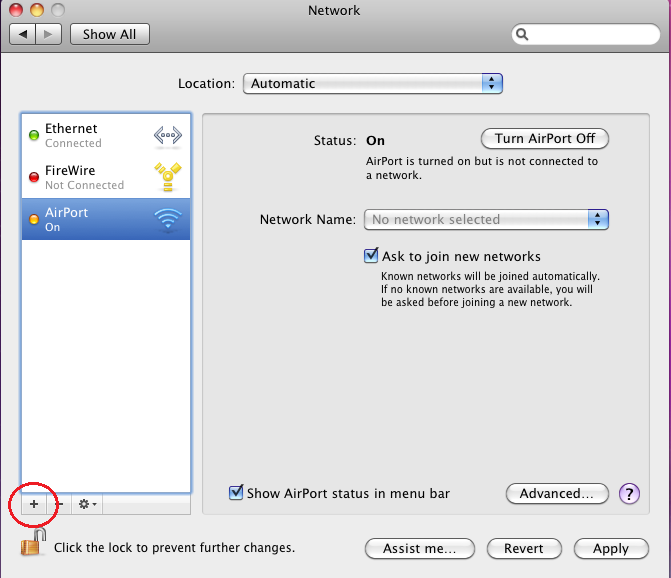


### Setting up your VPN (L2TP) under Mac OS X 10.12 (Sierra)

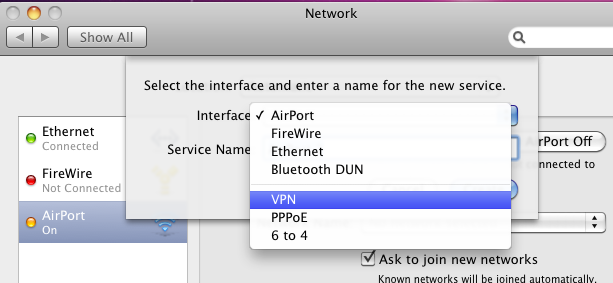
1. Go to the Apple menu and choose System Preferences. Or choose System Preferences from the Dock.



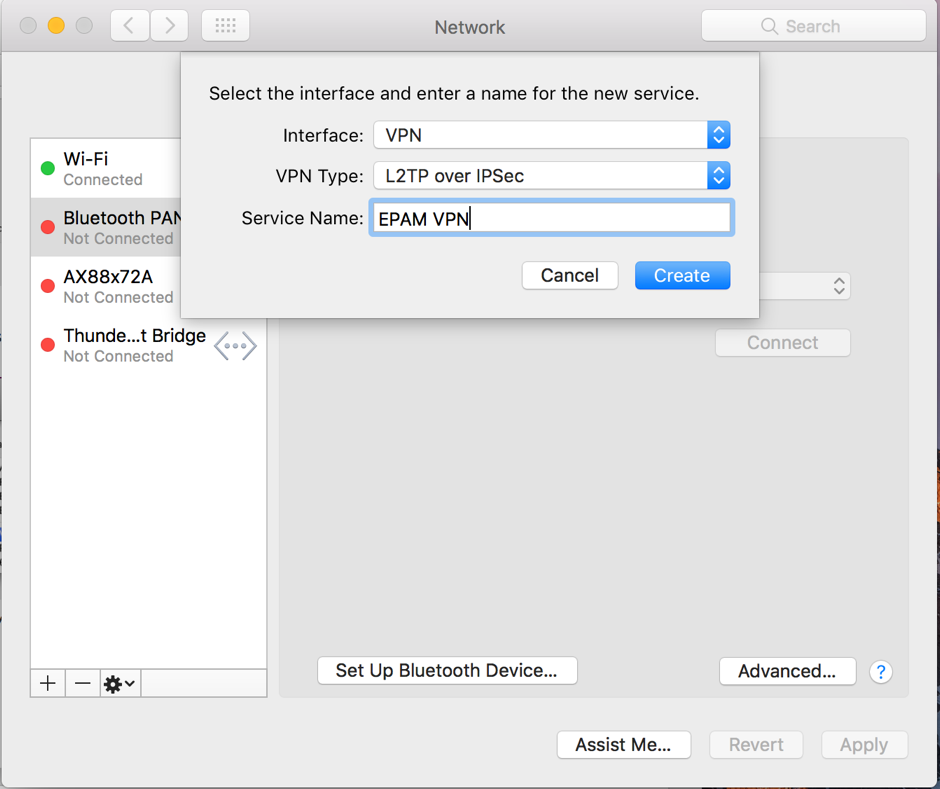
1. Click on Network system preference.
2. In the Network system preference there is a list of network connections on the left side. Click the '+' icon to make new VPN connection.



1. On the new service sheet click on the Interface popup menu to see the list of choices and select VPN.

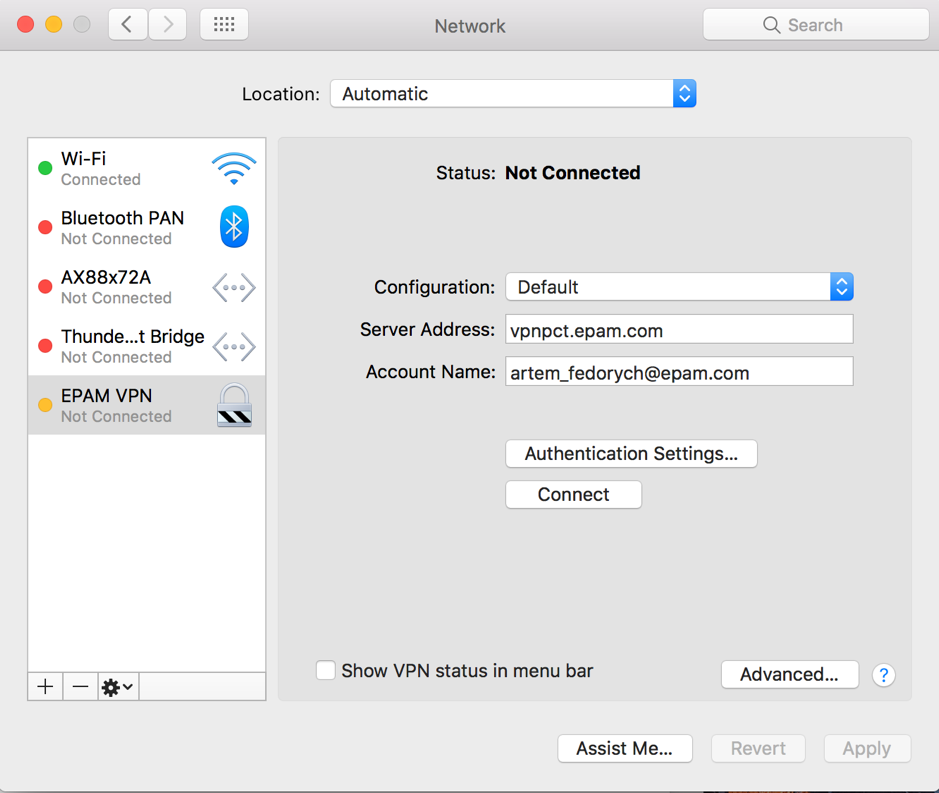


1. Set VPN Type as L2TP over IPSec.

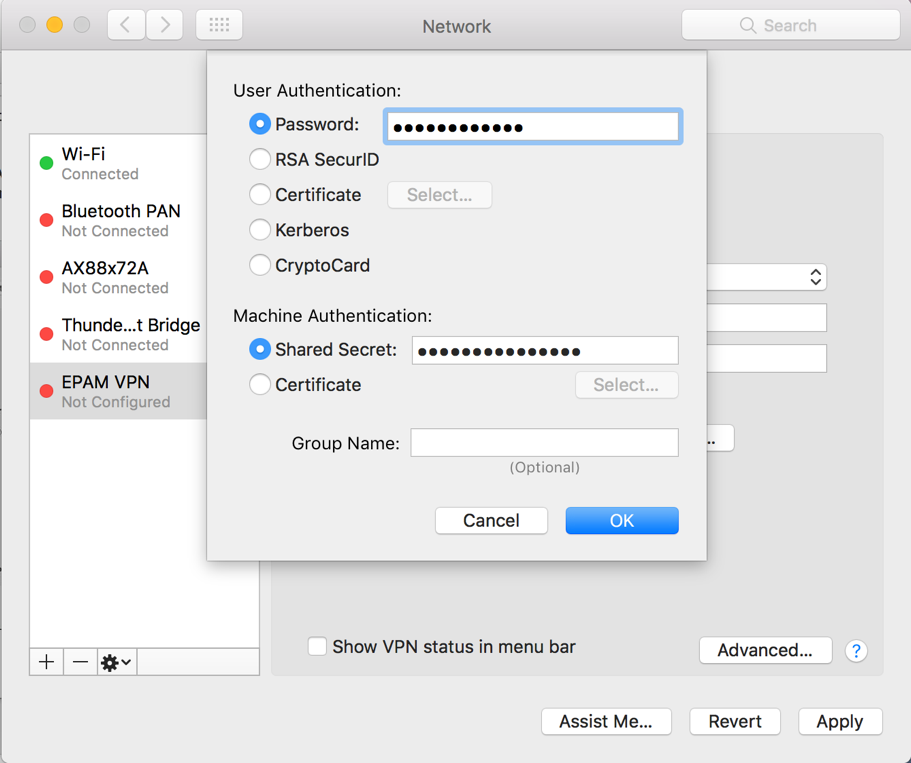


1. Type in Service Name the new connection name (ex. EPAM VPN).
2. Click Create to create a new connection
3. Configure your VPN:

* Enter in Server Address VPN server name in accordance with your location (ex. vpnpct.epam.com).
* Enter in Remote ID the same as in Server Address.
* In the Account name box, enter your domain username as First\_Lastname@epam.com



1. Click Authentication Settings…



* + Password is your EPAM domain password

1. To Shared Secret field type (case sensitive), see Appendix В.1 for more information
2. Click OK to apply changes and you are set.
3. To connect to the VPN, you can either choose the VPN configuration from the VPN menu or select your VPN connection in the connection list and click the Connect button.

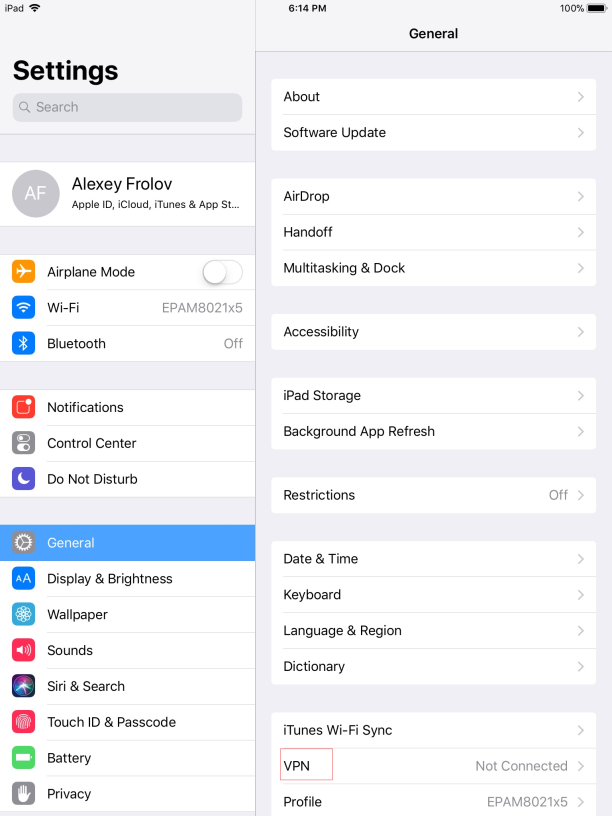


### Setting up your VPN under iOS 11

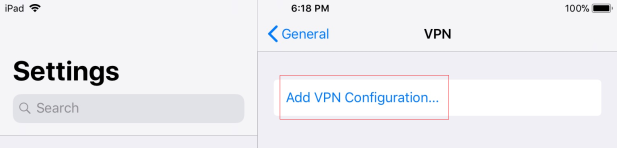
1. Go to your home screen and tap on “Settings”



1. Tap on “General”, then “VPN”

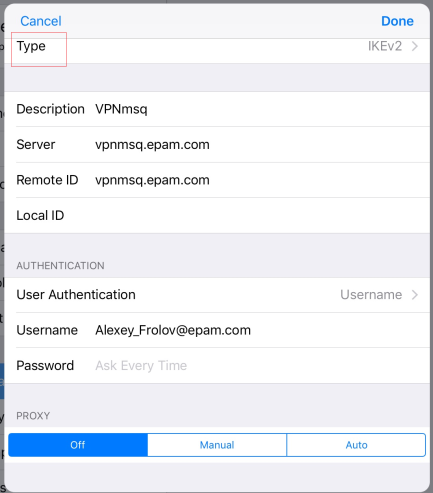
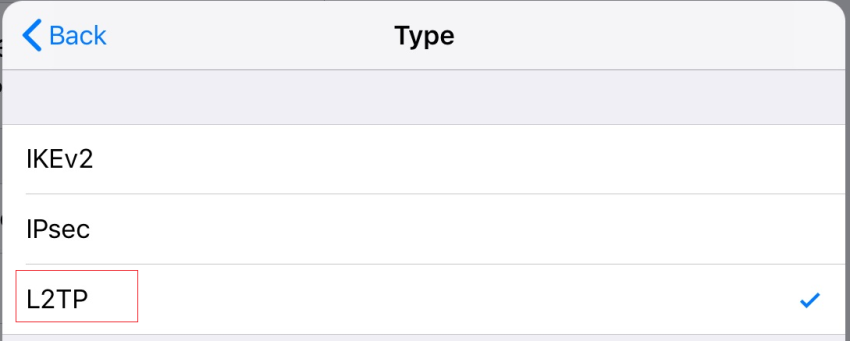


1. Tap on Add “VPN configuration”

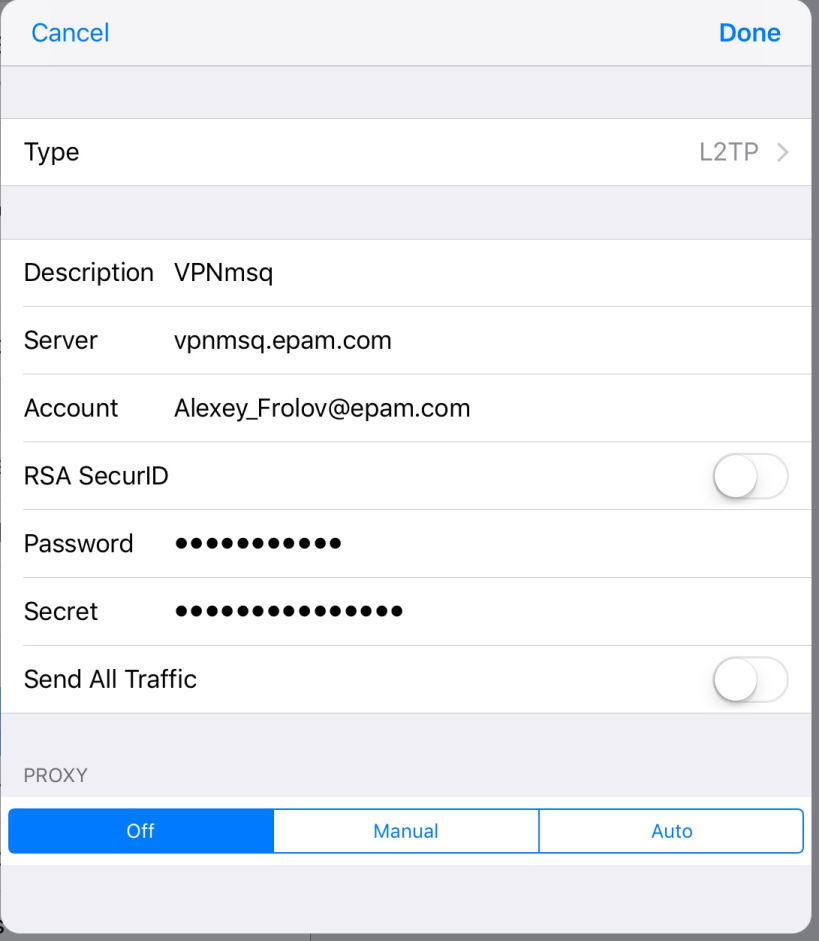


1. Insert Following Info:

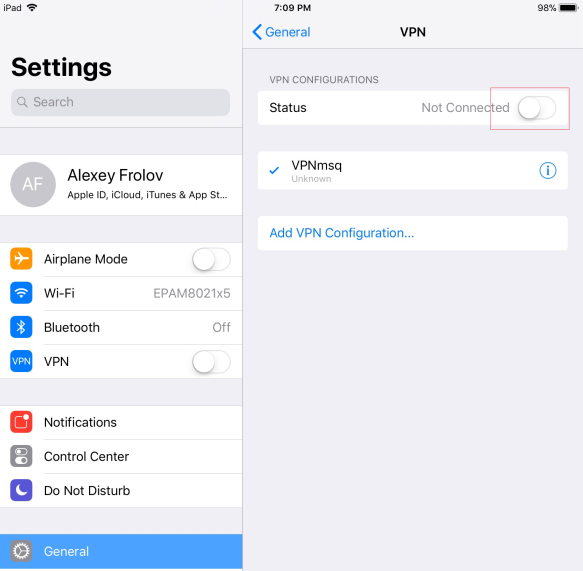
* Change VPN connection type to L2TP

 .

* Description: Enter new VPN connection name (e.g. VPNmsq).
* Server: Enter vpn server name in accordance with your location (e.g. vpnmsq.epam.com).
* Account: enter your domain username as First\_Lastname@epam.com.
* Password: enter your domain password.
* Secret: see Appendix В.1 for more information. Secret is case sensitive.



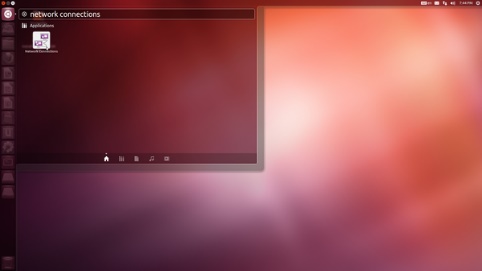
1. Tap on “Done”.
2. Tap on “VPNmsq” and Turn on VPN.



1. EPAM VPN is Connected Now.

### Setting up your VPN under Ubuntu 12.04.

1. Open Dash and run Network Connections tool.



1. At VPN tab click Add to create a new VPN connection.

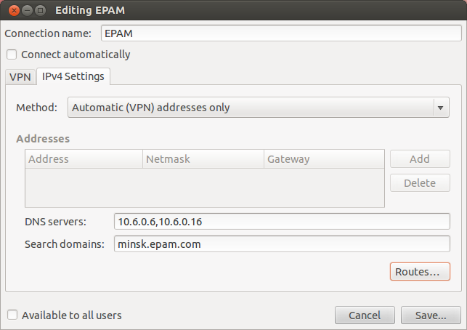


1. Choose Point-to-Point Tunneling Protocol (PPTP) as a type of VPN Connection and click Create...



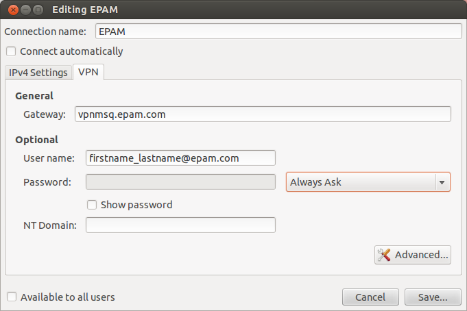
1. At **IPv4 Settings** tab, enter the following information:

* In the Method box, select Automatic (VPN) addresses only.
* In the DNS servers box, enter DNS server addresses in accordance with your location (e.x. 10.6.0.6, 10.6.0.16).
* In the Search domains box, enter search domain address in accordance with your location (e.x. minsk.epam.com).



1. At **VPN** tab, enter your VPN information:

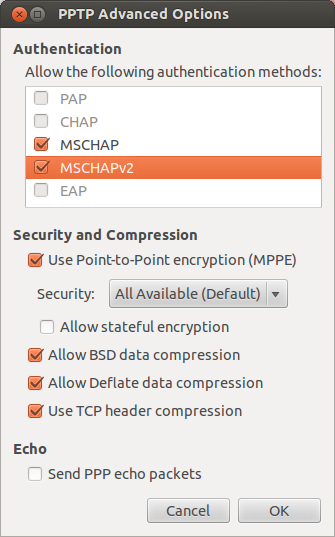
* In the **Connection name** box, enter your preferred connection name.
* In the **Gateway** box, enter vpn server name in accordance with your location (e.x. **vpnmsq.epam.com**).
* In the **User name** box, enter your domain username as [Firstname\_Lastname@epam.com](mailto:First_Lastname@epam.com).
* In the **Password** box, select **Always Ask**.
* Make sure that both **Connect automatically** and **Available to all users** options are unchecked.



1. Click Advanced... to setup PPTP Advanced Options.

Uncheck all **Authentication method** options but **MSCHAP** and **MSCHAPv2**.

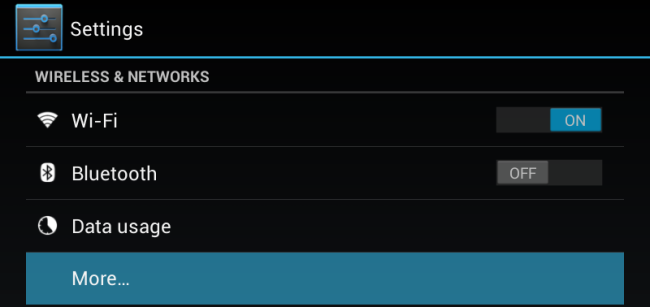
Check **Use Point-to-Point Encryption (MPPE)** option.



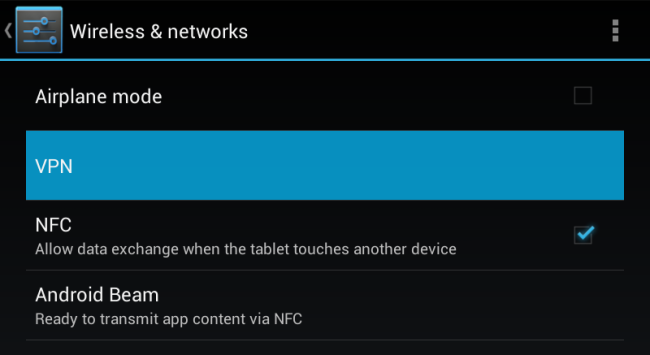
1. Click **OK** then **Save...** to save the VPN connection.

### Setting up your VPN under Android

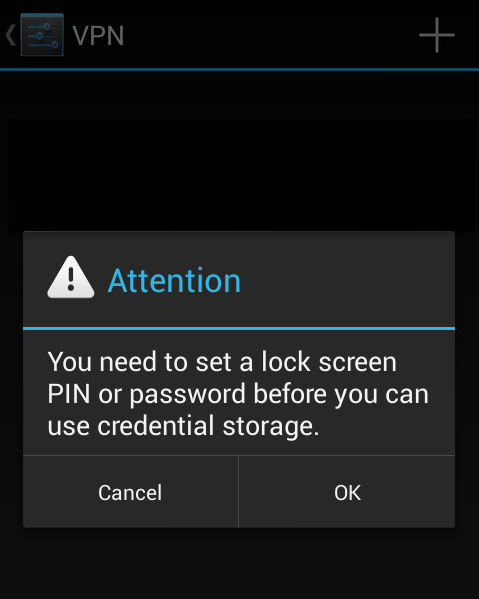
1. To connect to EPAM VPN on Android, open the *Settings* app -> More under *Wireless & networks*.



1. Tap the *VPN* option on the *Wireless & networks* screen.

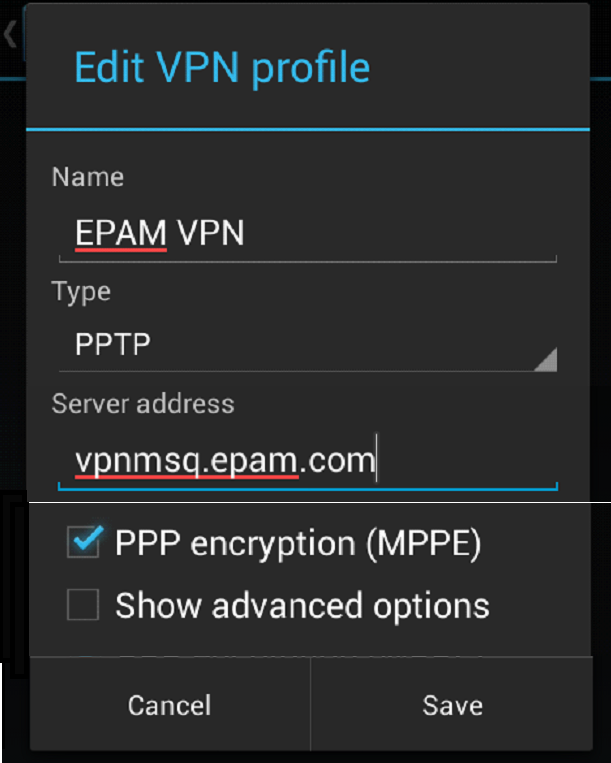


1. Set a lock screen PIN or password if it has not been set before (follow the instructions [here](https://support.epam.com/esp/ess.do?ctx=docEngine&file=kmdocument&query=id%3D%22KM0433%22&action=&title=Knowledge%20Document%20KM0433)):



1. Tap the **+** button, fill in the fields and Save changes:

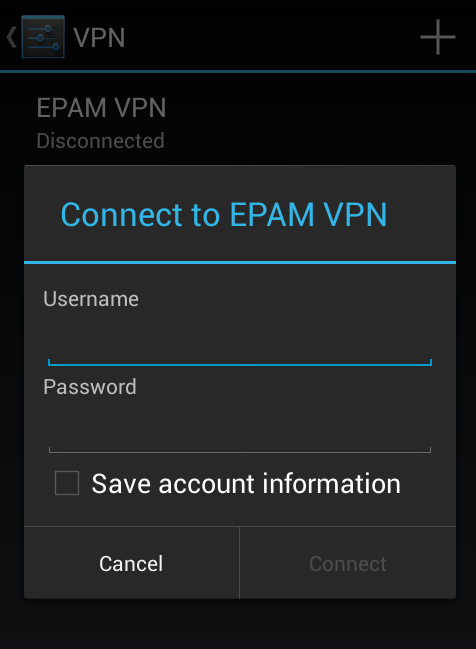
* **Name**: EPAM VPN
* **Type**: PPTP
* **Server Address**: vpnmsq.epam.com (see *Appendix 1* for more details)



1. To connect, tap VPN and fill in the information:

* **Username**: [First\_Lastname@epam.com](mailto:First_Lastname@epam.com)
* **Password**: your EPAM password

You can save this account information for next time.



1. While connected to a VPN, there will be a “VPN activated” notification in the notifications drawer. To disconnect, pull down the notification drawer, tap the notification -> tap *Disconnect*.

# 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:

1. Go to Start 🡪 Control Panel 🡪 Power Options.
2. Select Change when the computer sleeps.
3. 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 Mac OS:

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

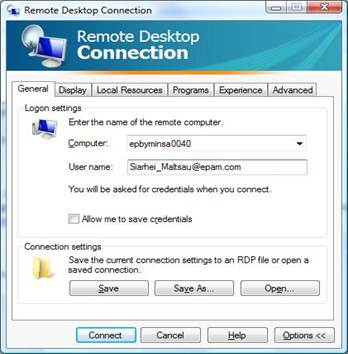
2. Check your OS version. Windows XP SP3 needed. SP2 is not compatible. Windows Vista, Server 2008 and higher is recommended.

3. 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>.

4. 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.

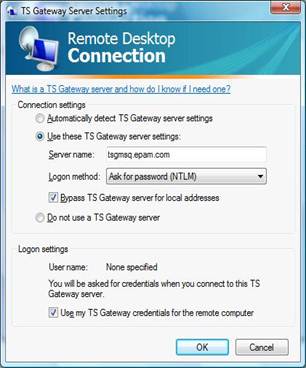
Open your RDP client (Remote desktop) connection, type the server in the EPAM network you want to connect to:



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



Set parameters as following: Server name – See [Appendix A.2](#AppendixA2). 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 deauthenticate on page [**httpS://wifi.epam.com/logout.html**](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.

### EPAMGuests8021x

#### 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. Сlick [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 panel.
2. Click Add, click Manually create a network profile:

* Network name: EPAMGuests8021x
* 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. Click Configure and uncheck Automatically use my Windows logon name and password (and domain if any).
10. Press twice Ok and Close.
11. Connect to the network by clicking the Start button 🡪 Control Panel 🡪 Network and Internet 🡪 Network and Sharing Center 🡪 Connect to a network, click EPAMGuests8021x and press Connect.
12. Enter your Guest Username and Guest password.

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

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

#### Windows XP SP3

Please connect to “EPAMGuest” SSID and install both EPAM certificates Rootca and Intermediate certificate from the page <http://cert.epam.com>.

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

Open Network Connections clicking the Start button 🡪 Control Panel 🡪 Network Connections. Right-click the wireless network adapter in Network Connections and click Properties. Press Wireless Networks.

Press Add. Type the following settings:

* Network name (SSID): EPAMGuests8021x
* Network Authentication: WPA2
* Data encryption: AES

Press Authentication tab and choose Protected EAP (PEAP) in EAP type field. Click Properties.

Check Validate server certificate and installed EPAM certificates in Trusted Root Certification Authorities.

Choose Secured password (EAP-MSCHAP v2) in Select Authentication Method field.

Check Enable Fast Reconnect.

Click Configure and uncheck Automatically use my Windows logon name and password (and domain if any).

Press three times Ok.

Right-click the wireless network adapter in Network Connections and click View Available Wireless Networks. In either case, you should see the Choose a wireless network dialog box with EPAMGuests8021x wireless network. Double-click the wireless network.

Enter your Guest Username and Guest password.

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

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

#### MAC OS X Lion 10.7.4

1. Please connect to “EPAMGuest” SSID and install both EPAM root certificates from the page <http://cert.epam.com> (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 EPAMGuests8021x from the Network Name list at right
5. Use Guest username and Guest password for wireless authentication.
6. You will only be able to connect to the Internet with no access to the Company’s network.

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

#### Windows Mobile 5.x and 6.x

1. Import your personal certificate to the mobile device.
2. Make sure that wireless is enabled on your phone and verify that your phone can support WPA2-Enterprise encryption. (Note: Windows Mobile 6 supports WPA2, but not all phones support WPA2. Please consult your phone's manual for further information).
3. Click Start and select Settings. Click the Connections tab and then Wi-Fi.
4. Click the wireless network, EPAMGuests8021x.
5. Select The Internet from the Connects to drop-down menu. Click Next.
6. Select WPA2 from the Authentication drop-down menu.
7. Select AES from the Data Encryption drop-down menu. Select Next.
8. Select PEAP from the EAP Type drop-down menu.
9. Click Properties and Select your personal certificate.
10. Network Log On window should appear. Enter your Guest Username under "User name". Enter your Guest password under "Password".
11. Click OK.

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

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

#### 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.

**Note1**: Use standard Android Internet browser for installing certificates from web page.

**Note2:** 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**. **Note3**: Some devices support only .crt extension of certificates files. Change extension from .cer to .crt before installing).

1. From the Android Home screen, tap Menu then tap Settings.
2. Tap Wireless and network and then tap Wi-Fi settings.
3. Tap Wi-Fi to turn-on wireless (if not already on).
4. From the list of Wi-Fi networks, tap EPAMGuests8021x.
5. Select PEAP from EAP method drop-down menu.
6. Select MSCHAPV2 from Phase 2 authentication drop-down menu.
7. Select installed root certificate from CA certificate
8. Type your Guest Username in Identity field.
9. Client certificate and Anonymous identity has to be blank.
10. Type your Guest password in Wireless password field.
11. Click Connect.

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

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

#### iOS 5.x, 6.x

1. 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.
2. Connect to “EPAMGuests8021x” SSID from Wi-Fi connections under Settings.
3. Type your Guest Username and Guest password in Username and Password fields.
4. Click Connect and Accept certificate button.

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

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: EPAMemployees and EPAM8021x (please note that EPAM8021x SSID is preferable to use)

### EPAMemployees

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

* Network name (SSID): EPAMemployees
* Network Authentication: WPA2
* Data encryption: AES
* *Network key:* Wi2177785Fi

1. Open Internet Explorer (or other browser) and go to <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 Username: <your EPAMusername>@epam.com and EPAM MS Windows password for web authentication
3. We can deauthenticate on page <httpS://wifi.epam.com/logout.html>.
4. Proxy should be disabled in your browser to be able to authenticate.

### 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. Сlick [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.

#### Windows XP SP3

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

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

Open Network Connections clicking the Start button 🡪 Control Panel 🡪 Network Connections. Right-click the wireless network adapter in Network Connections and click Properties. Press Wireless Networks.

Press Add.

Type the following settings:

* Network name (SSID): EPAM8021x
* Network Authentication: WPA2
* Data encryption: AES

Press Authentication tab and choose Protected EAP (PEAP) in EAP type field. Click Properties.

Check Validate server certificate and installed EPAM certificates in Trusted Root Certification Authorities.

Choose Secured password (EAP-MSCHAP v2) in Select Authentication Method field.

Check Enable Fast Reconnect.

Press three times Ok.

Right-click the wireless network adapter in **Network Connections** and click **View Available Wireless Networks**. In either case, you should see the **Choose a wireless network** dialog box with EPAM8021x wireless network. Double-click the wireless network.

#### MAC OS X Lion 10.7.4

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 EPAMusername>@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 "EPAMemployees. A connection timeout occurred." You can fix the problem if you remove EPAM8021x (your stored password) from Launchpad 🡪 Utilities 🡪 Keychain Access 🡪 Keychains login.

#### Windows Mobile 5.x and 6.x

1. Import your personal certificate to the mobile device
2. Make sure that wireless is enabled on your phone and verify that your phone can support WPA2-Enterprise encryption. (Note: Windows Mobile 6 supports WPA2, but not all phones support WPA2. Please consult your phone's manual for further information).
3. Click Start and select Settings. Click the Connections tab and then Wi-Fi.
4. Click the wireless network, EPAM8021x.
5. Select The Internet from the Connects to drop-down menu. Click Next.
6. Select WPA2 from the Authentication drop-down menu.
7. Select AES from the Data Encryption drop-down menu. Select Next.
8. Select PEAP from the EAP Type drop-down menu.
9. Click Properties and Select your personal certificate.
10. Network Log On window should appear. Enter your EPAM MS Windows Username under "User name". Enter your Windows password under "Password".
11. Click OK.

#### 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.

**Note1:** Use standard Android Internet browser for installing certificates from web page.

**Note2:** 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.

**Note3:** Some devices support only .crt extension of certificates files. Change extension from .cer to .crt before installing)

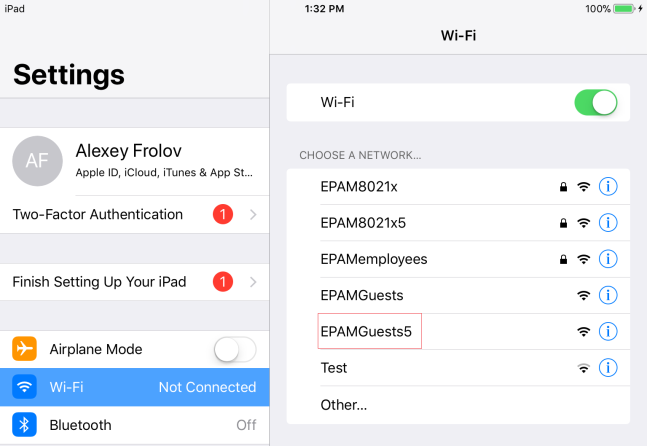
1. From the Android Home screen, tap Menu then tap Settings.
2. Tap Wireless and network and then tap Wi-Fi settings.
3. Tap Wi-Fi to turn-on wireless (if not already on).
4. From the list of Wi-Fi networks, tap EPAM8021x.
5. Select PEAP from EAP method drop-down menu.
6. Select MSCHAPV2 from Phase 2 authentication drop-down menu.
7. Select installed root certificate from CA certificate.
8. Type your EPAM MS Windows Username in Identity field (correct format is <your EPAMusername>@epam.com).
9. Client certificate and Anonymous identity has to be blank.
10. Type your EPAM Windows password in Wireless password field.
11. Click Connect.

#### iOS

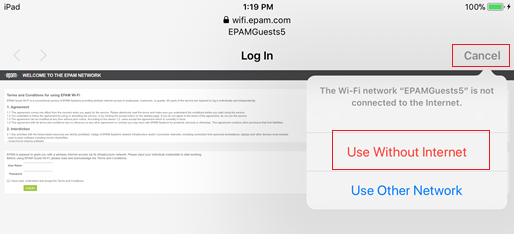
1. Go to your home screen and tap on “Settings”



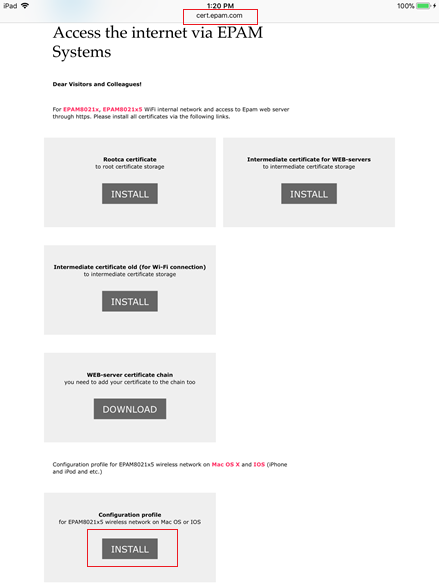
1. Connect to EPAMGuests5 network



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

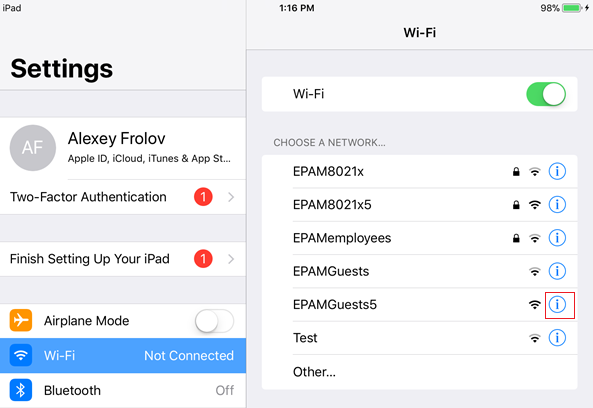
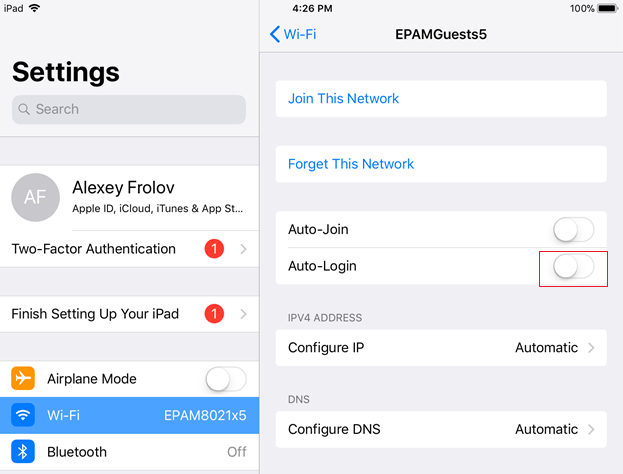


1. Install Configuration profile for EPAM8021x5 wireless network on Mac OS or IOS from <http://cert.epam.com>. Open Safari browser and go to <http://cert.epam.com>

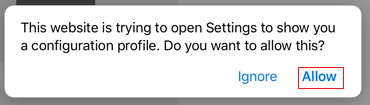


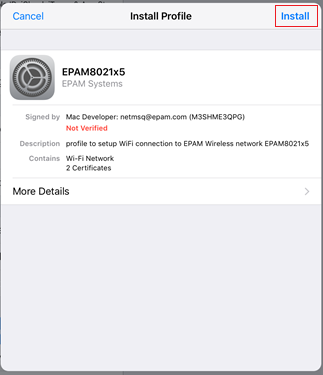
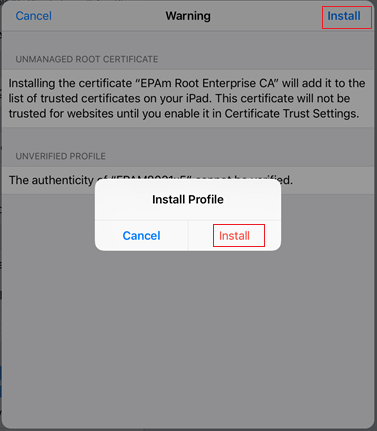
1. In case of any troubles with connection to EPAMGuests5 and accessing <http://cert.epam.com> switch off Auto-Login in WiFi settings:

Click Settings –> Wi-Fi -> EPAMGuests5 -> switch off Auto-Login

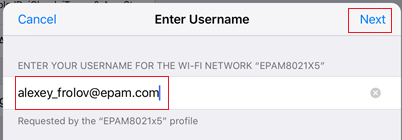
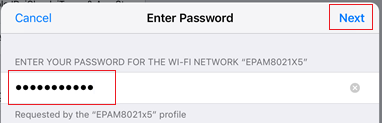
 

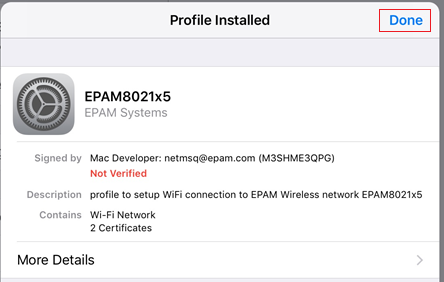
1. Click Allow and Install three times when Install Profile page appear



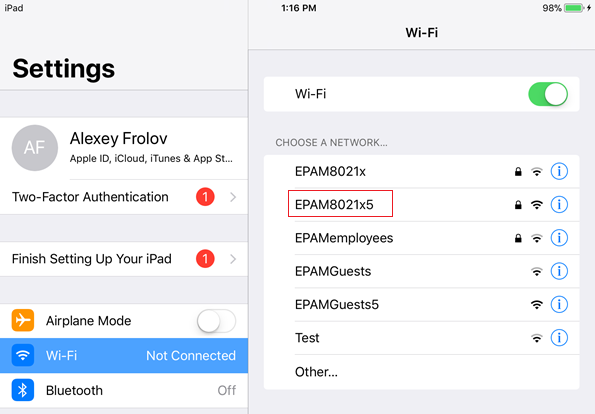
 

1. Use your Username (Name\_Surename@epam.com) -> Next -> EPAM MS Windows password -> Done

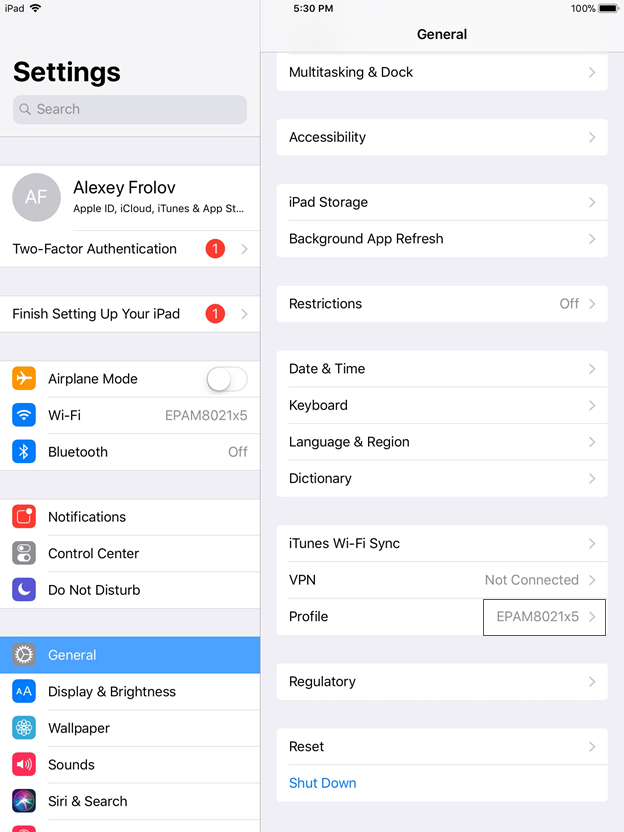
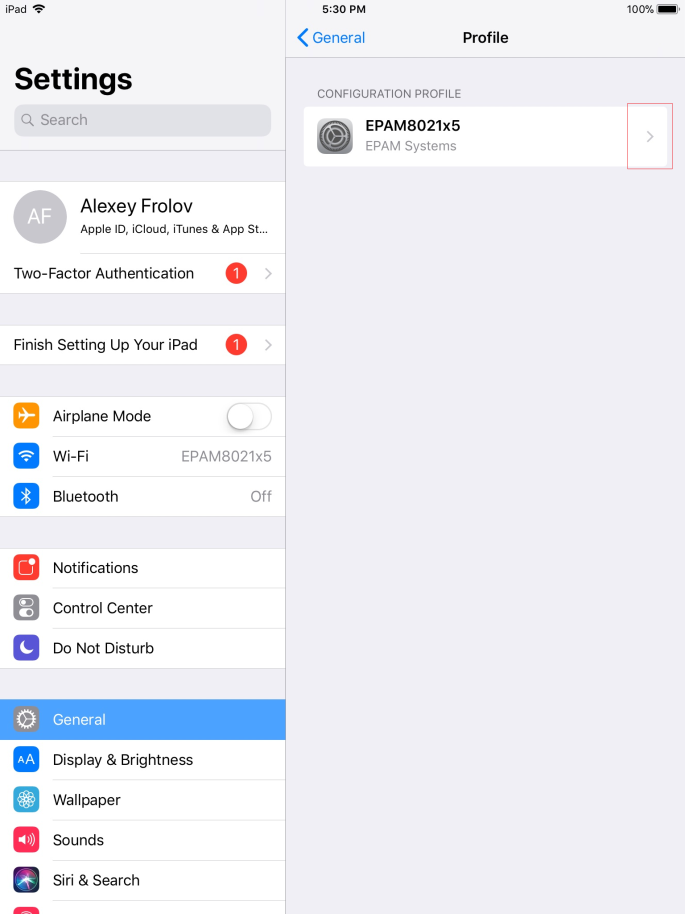
 

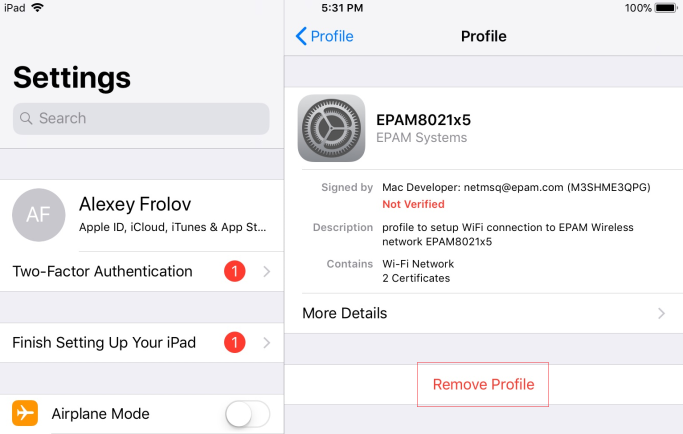


1. Press Settings -> Wi-Fi -> Choose EPAM8021x5 network



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



1. GATES
   1. VPN GATES

|  |  |  |
| --- | --- | --- |
| VPN Server Address | VPN Server Location | Can be used for employees in Locations |
| vpnbud.epam.com | Budapest | Worldwide, EU is preferred |
| vpniev.epam.com | Kyiv | Worldwide, UA is preferred |
| vpnmsq.epam.com | Minsk | Worldwide, BY is preferred |
| vpnmsk.epam.com | Moscow | Worldwide, RU is preferred |
| vpnpct.epam.com | US | Worldwide, US is preferred |
| vpnkar.epam.com | Karaganda | Worldwide, KZ is preferred |

* 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** | | |

1. KEYS
2. 1. L2TP VPN Shared Secret

|  |  |
| --- | --- |
| VPN Server Address | Shared Secret |
| vpnbud.epam.com | VPNbud.EPAm.Com |
| vpniev.epam.com | VPNiev.EPAm.Com |
| vpnmsq.epam.com | VPNmsq.EPAm.Com |
| vpnmsk.epam.com | VPNmsk.EPAm.Com |
| vpnpct.epam.com | VPNpct.EPAm.Com |
| vpnkar.epam.com | VPNkar.EPAm.Com |

| 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 |