

## Etisalat Colo SSLVPN Remote Access Gateway – Access Procedures

Dear Etisalat Colo Customer,

To access your Colo Server infrastructure via Colo SSLVPN remote access gateway a **username** and **password** was provided to you along with a **URL of your Colo SSLVPN gateway**. If you haven't received your account yet please contact Etisalat Support Team via phone **8004181** or via email [\*\*support@dc.etisalat.ae\*\*](mailto:support@dc.etisalat.ae).

This document describes how to use the Etisalat Colo SSLVPN remote access service and how to change the password for your account.

**Please change your password regularly and don't share it with others.**

**Chapter 1:** How to use the SSLVPN Remote Access Gateway the first time

**Optional:** How to use the SSLVPN Remote Access Gateway using FortiSSLVPN client

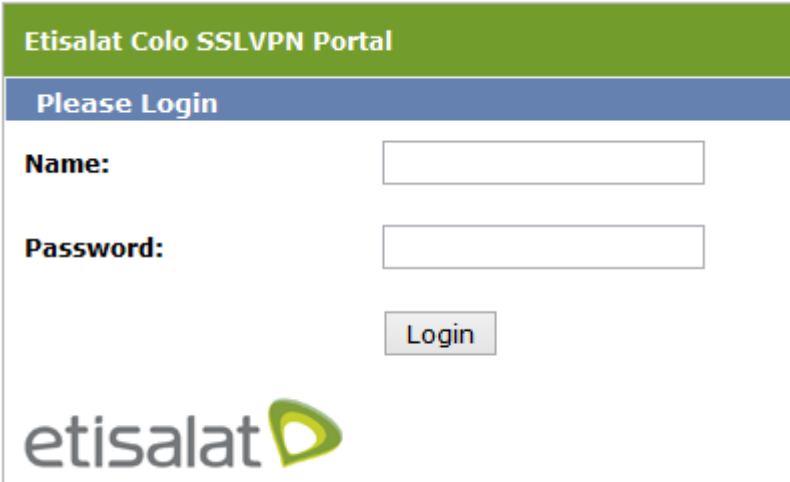
**Chapter 2:** Password Change Procedure

## Chapter 1: How to use the Colo SSLVPN Remote Access Gateway the first time

### Requirements

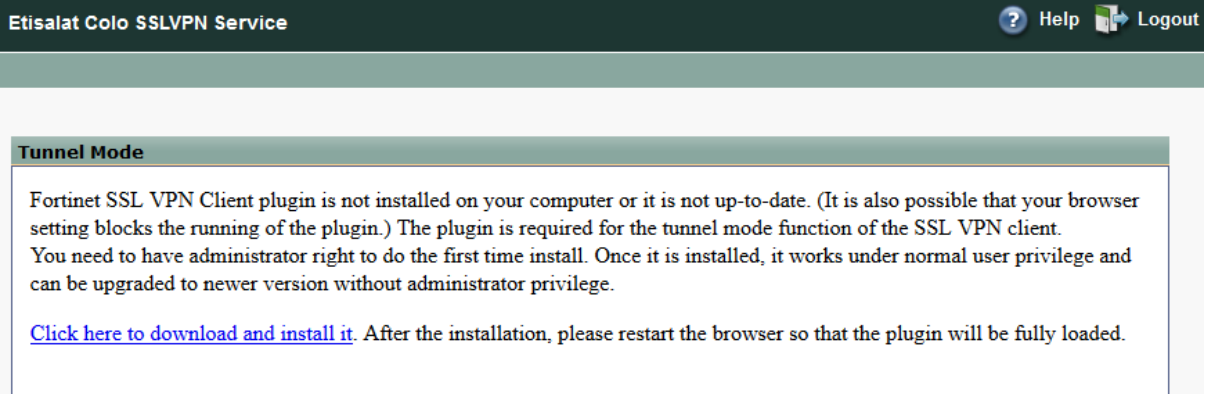
- Supported Operating Systems: Microsoft Windows Windows XP or newer
- Supported web browsers: Mozilla Firefox and Microsoft Internet Explorer
- **Administrator rights** are required during installation

1. Open your web browser and enter the provided URL. The login page appears. If you haven't got the login URL please contact Etisalat support.

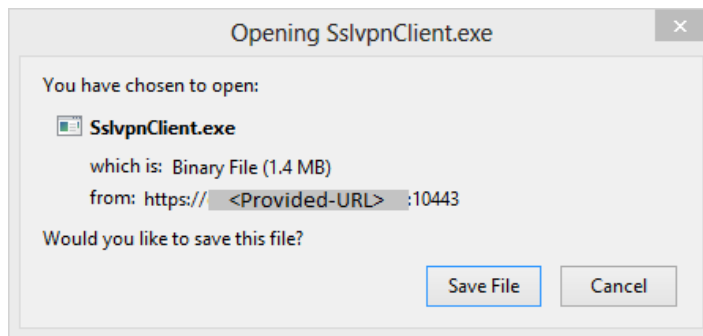


Enter your username and password and click on Login.

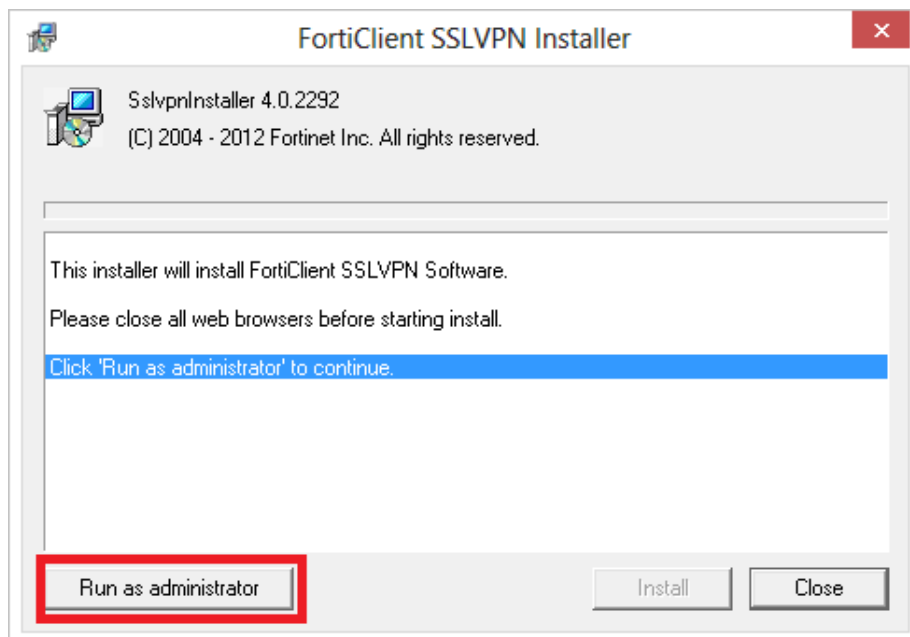
2. After login the first time into the Colo SSLVPN Remote Access Gateway a plugin must be installed which requires **administrator rights**.



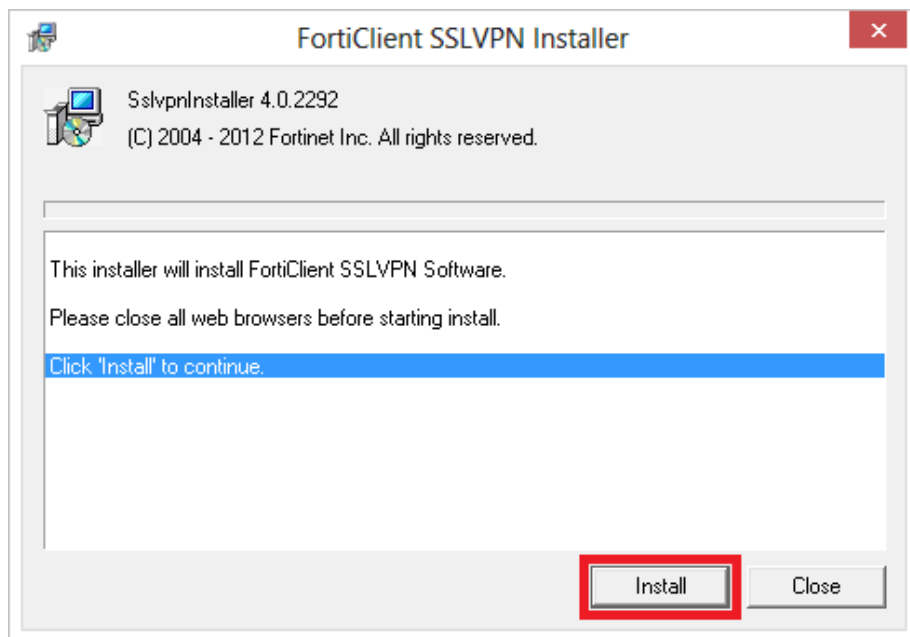
3. Click on “Click here to download and install it”



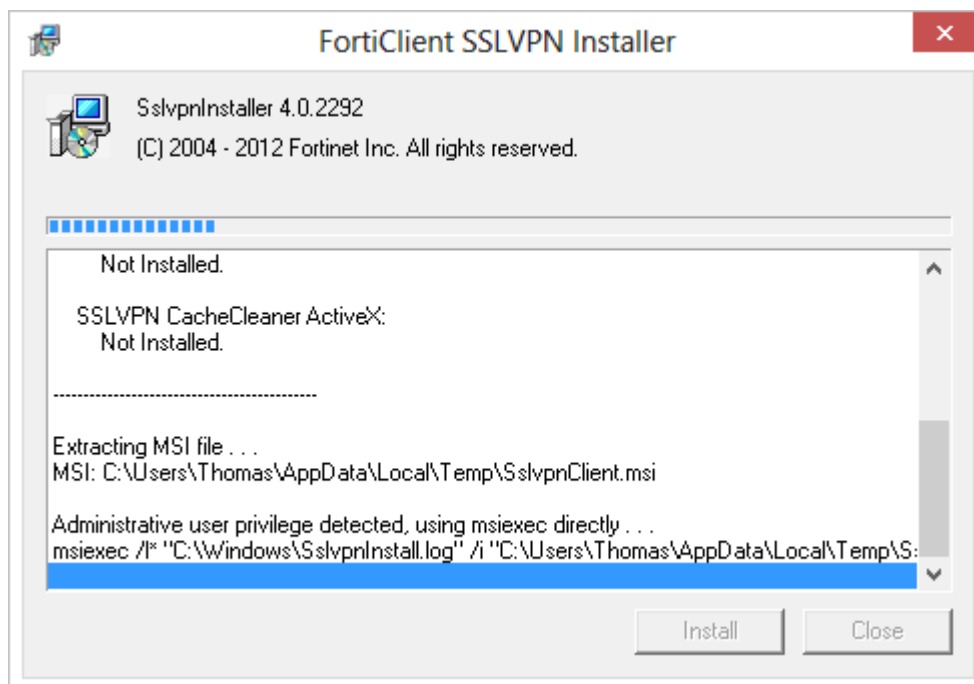
4. Save the file and execute it after download.



5. Click on Run as administrator and confirm with yes to run the file as administrator.

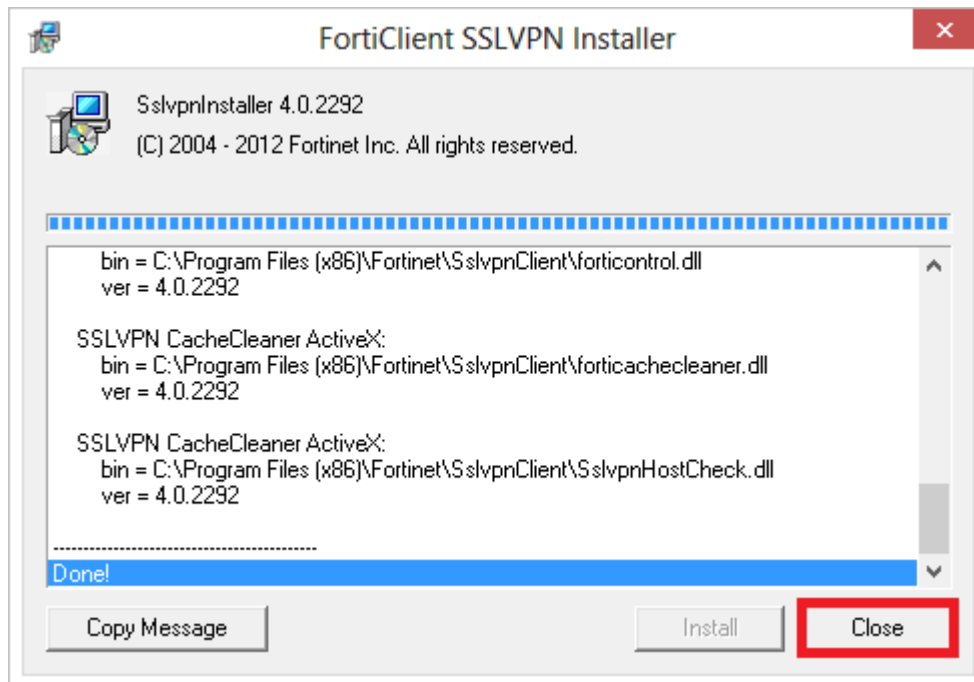


6. Click on “Install”

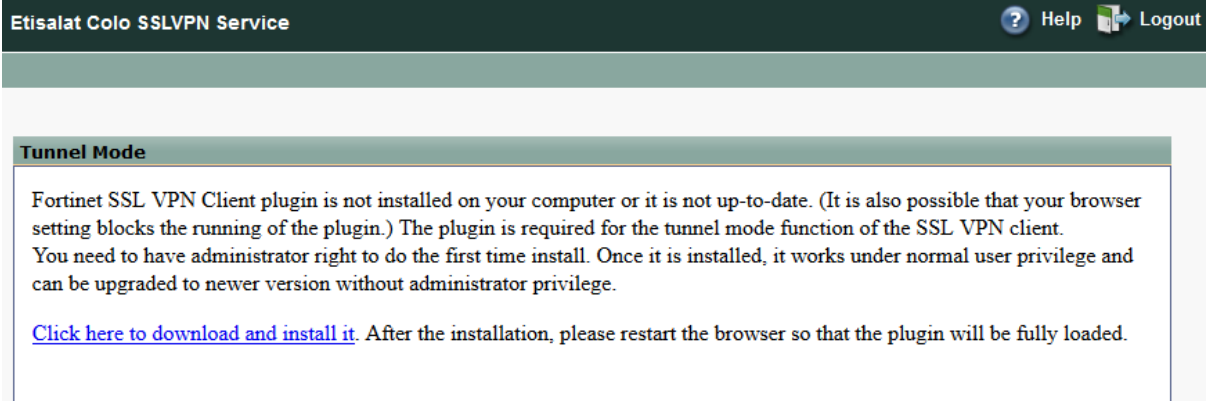


The SSLVPN Client is getting installed

7. After installation click on close



- Return to the web browser



Etisalat Colo SSLVPN Service ? Help Logout

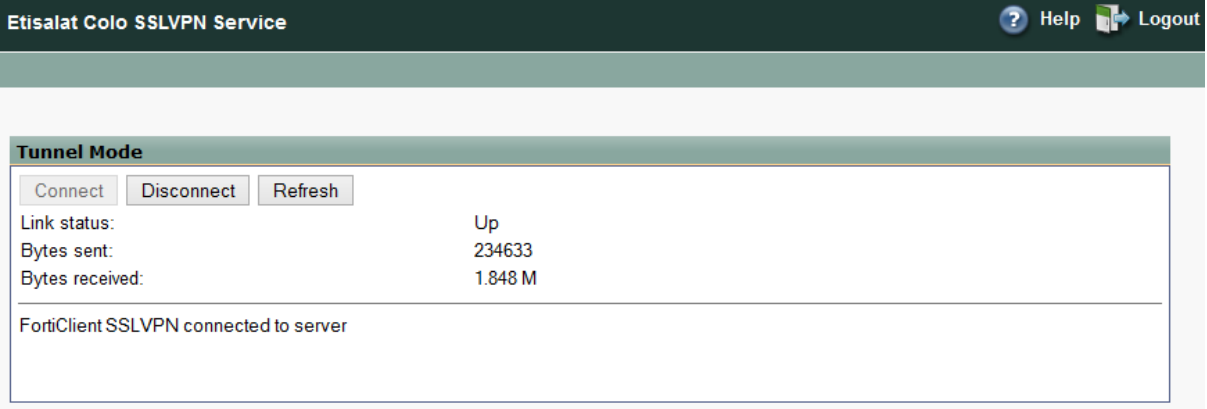
---

**Tunnel Mode**

Fortinet SSL VPN Client plugin is not installed on your computer or it is not up-to-date. (It is also possible that your browser setting blocks the running of the plugin.) The plugin is required for the tunnel mode function of the SSL VPN client. You need to have administrator right to do the first time install. Once it is installed, it works under normal user privilege and can be upgraded to newer version without administrator privilege.

[Click here to download and install it.](#) After the installation, please restart the browser so that the plugin will be fully loaded.

- Refresh (Reload) the Site



Etisalat Colo SSLVPN Service ? Help Logout

---

**Tunnel Mode**

Link status:	Up
Bytes sent:	234633
Bytes received:	1.848 M

---

FortiClient SSLVPN connected to server

- IF you are not getting connected automatically press the “Connect” Button to establish the remote access.

**Leave this page open in your browser or you will lose connectivity**

## Optional: How to use the Colo SSLVPN Remote Access Gateway using FortiSSLVPN client

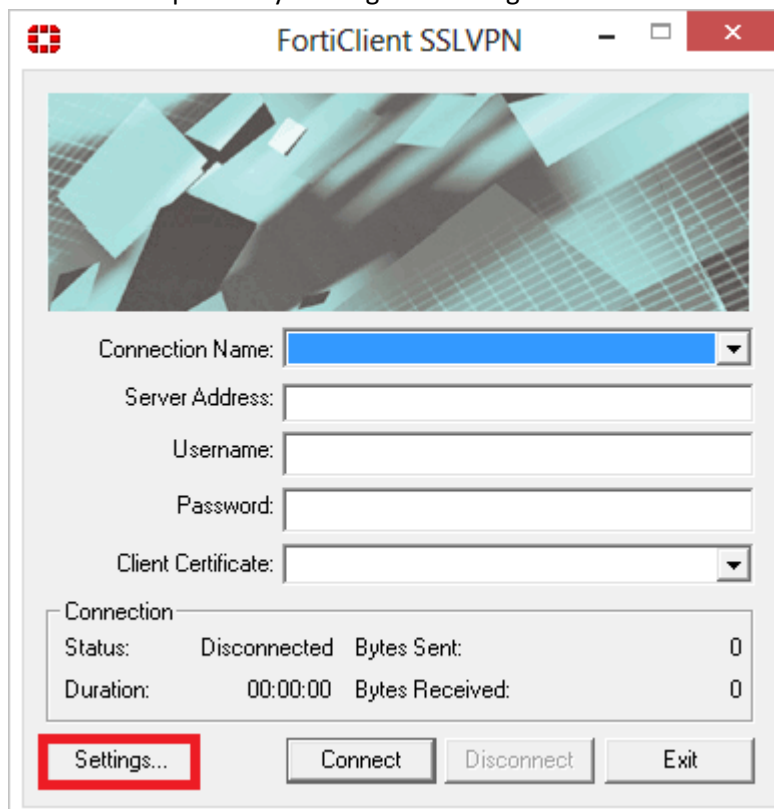
It is possible to use the Colo SSLVPN Remote Access Gateway with a FortiSSLVPN client instead of the web browser. The FortiSSLVPN client is a small application which got installed after you accessed the SSLVPN Remote Access Gateway the first time via web browser (see Chapter 1).

**Important:** It is always possible to access the Colo SSLVPN Remote Access Gateway via web browser as described in Chapter 1. The FortiSSLVPN client is considered as an optional access method.

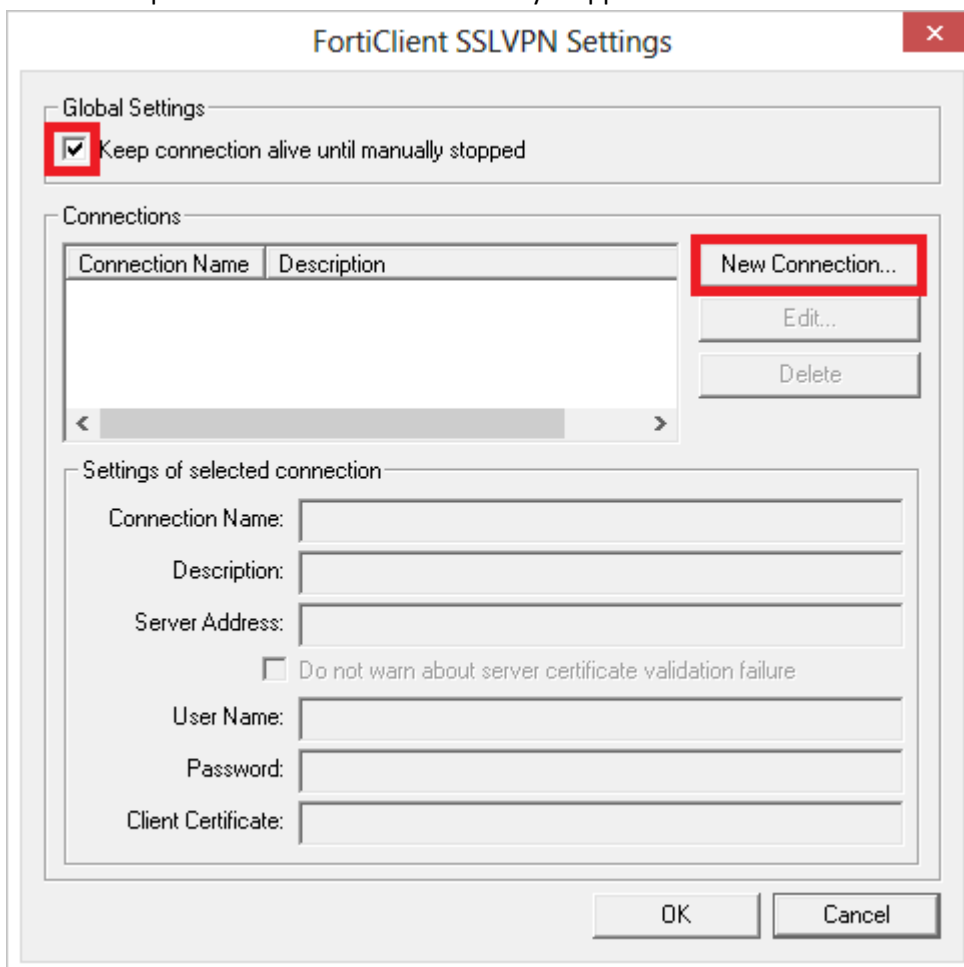
1. Open the FortiSSLVPN client by executing:  
`"C:\Program Files (x86)\Fortinet\SslvpnClient\FortiSSLVPNclient.exe"`  
 if you have a 64-bit operating system or  
  
`"C:\Program Files\Fortinet\SslvpnClient\FortiSSLVPNclient.exe"`  
 if you have a 32-bit operating system.

**Hint:** You can create a shortcut on your desktop if you like.

2. Create a new profile by clicking on "Settings"



3. Enable “Keep connection alive until manually stopped” and click on “New Connection”



4. Enter Connection Settings and click “OK” button

Connection Name	Enter “ <b>Etisalat-Colo</b> ”
Server Address	Enter the URL provided to you and add “:443” at the end. Example: <a href="https://ssl-colo.etisalat.ae:443">https://ssl-colo.etisalat.ae:443</a> You have to use the URL provided to you. This example URL will not work
User Name	Enter the <b>User Name</b> provided to you
Password	Enter the <b>Password</b> provided to you



**New Connection Settings** ✕

Connection Settings

Connection Name:

Description:

Server Address:

Do not warn about server certificate validation failure

User Name:

Password:

Client Certificate:

- Click "OK" Button again

**FortiClient SSLVPN Settings** ✕

Global Settings

Keep connection alive until manually stopped

Connections

Connection Name	Description
Etisalat-Colo	

Settings of selected connection

Connection Name:

Description:

Server Address:

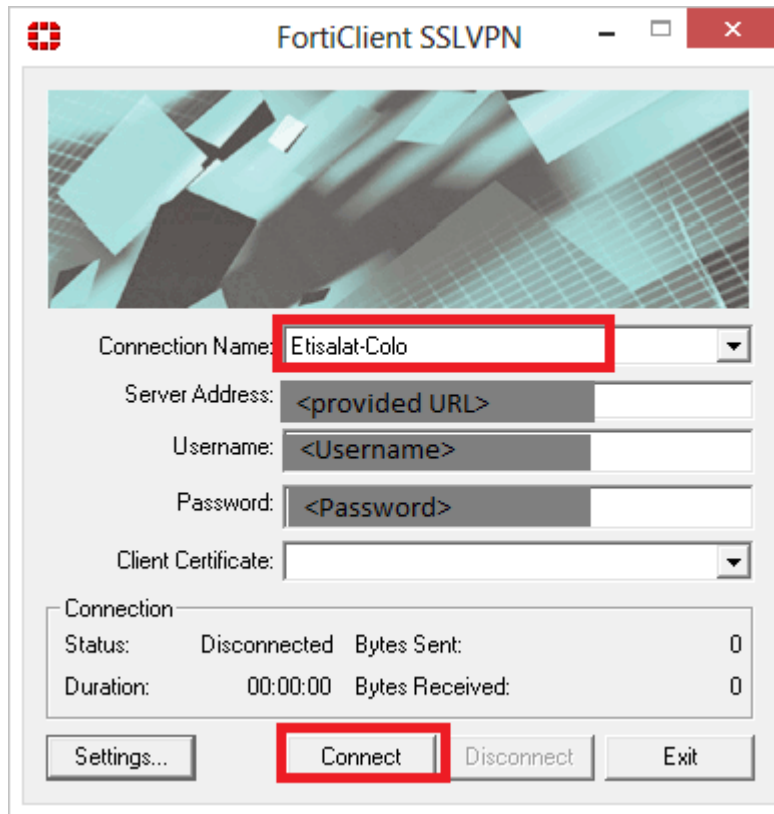
Do not warn about server certificate validation failure

User Name:

Password:

Client Certificate:

6. Select the created profile at “Connection Name” and click on “Connect” to establish the connection



## Chapter 2: Password Change Procedure

1. Access <https://auth-zabeel.etisalat.ae/user/reset-password/> via web browser

**Reset Password**

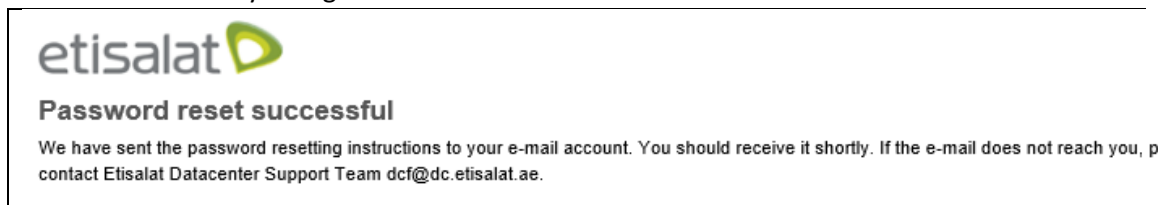
To recover your password, please select your method of identification.

Recover by:  Username  E-mail

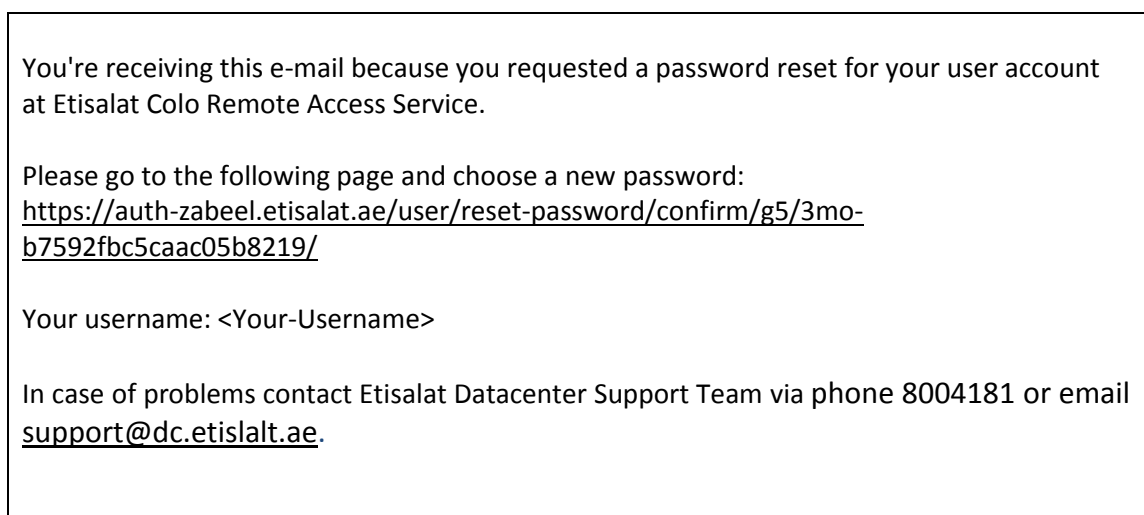
Username:

Select "Username" and enter your username in the highlighted field. Then press next

2. A password reset email will be send to the email address which was registered with Etisalat Colo Service when you registered for it.



3. Check your email account after 5min for the password reset message. Below is an example email:




4. Click on the link in the email message and enter a new password by following the password requirements twice.

**Reset Password**

Please enter a new password.

<b>New password:</b>	<input type="password"/>	Password must meet these requirements: must be at least 8 character(s) in length, has at least 1 uppercase letter(s), 1 numeric character(s), 1 non-alphanumeric character(s) (e.g. \$!#)
<b>Confirm password:</b>	<input type="password"/>	

5. The password change gets acknowledged.



**Password reset complete**

Your password has been set. Please login with the new password.

6. Return to the Colo SSLVPN Remote Access Gateway Login Page and login with your username and new password.