**Setup Instructions**

1. **General information**

Electronic messages between electronic exchange users and the Financial Messaging System (FMS) are sent using the automated system Transport gateway of the Bank of Russia for the exchange of payment and financial messages with customers of the Bank of Russia' (BoR Customer TG).

Connection to the BoR Customer TG is carried out using dedicated channels provided by communication service providers.

A VPN tunnel should be deployed to the access server of the test/production BoR Customer TG to ensure the interaction of the exchange participant’s PC with the test/production segment of the BoR Customer TG.

Cisco AnyConnect is used to deploy a VPN tunnel; the software can be downloaded directly from the test/production BoR Customer TG access server. Additionally, it is necessary to ensure the network accessibility of the test/production BoR Customer TG access server from the exchange participant’s PC.

Inside the VPN tunnel, the AWS of a BoR Customer-FMS interacts with the BoR Customer TG server, which receives electronic messages from the exchange participant and forwards them to the FMS.

* 1. **Setting up a VPN connection with the BoR Customer TG**

After establishing a network connection to the BoR Customer TG through a communication service provider's dedicated communication channel, the exchange participant’s PC must have network access to the IP addresses of two access servers (primary and backup) of the BoR Customer TG test/production segment:

-IP address of the primary access server of the BoR Customer TG test segment: 172.16.20.42;

-IP address of the secondary access server of the BoR Customer TG test segment: 172.16.20.74.

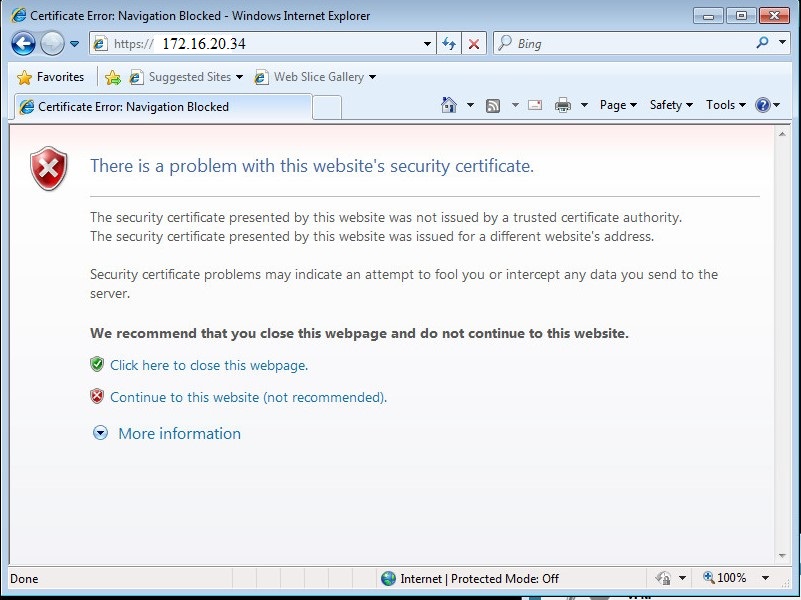
-IP address of the primary access server of the BoR Customer TG production segment: 172.16.20.34;

-IP address of the secondary access server of the BoR Customer TG production segment: 172.16.20.66.

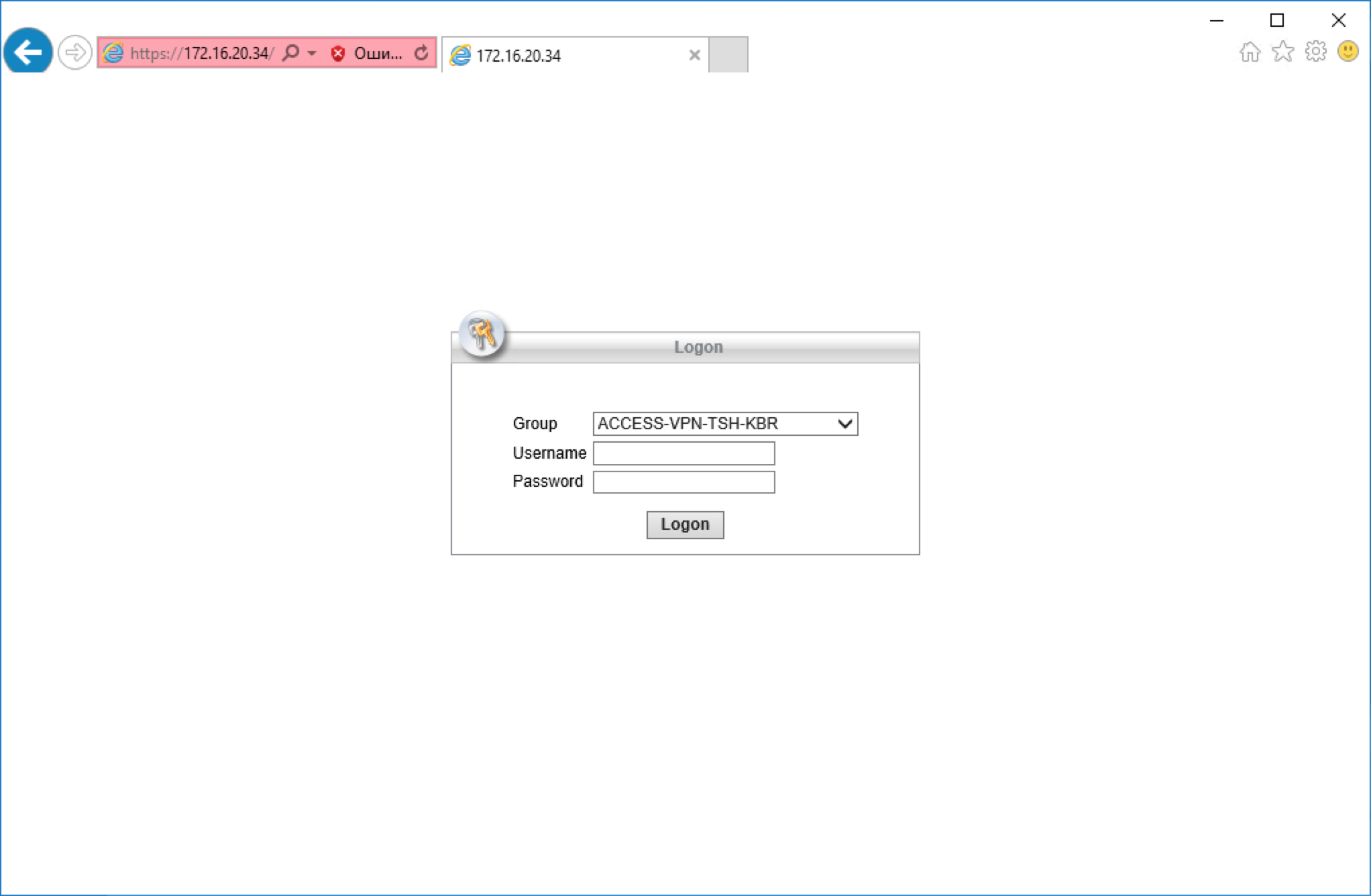
In addition, it is necessary to ensure network accessibility of the test/production BoR Customer TG access server from the exchange participant’s PC (IP addresses: 172.16.20.42/172.16.20.74 and 172.16.20.34/172.16.20.66); TCP port: 443; UDP ports: 500, 4500.

Cisco AnyConnect is used to deploy a VPN tunnel. To download and install Cisco AnyConnect software on the exchange participant’s PC, you should perform the following steps:

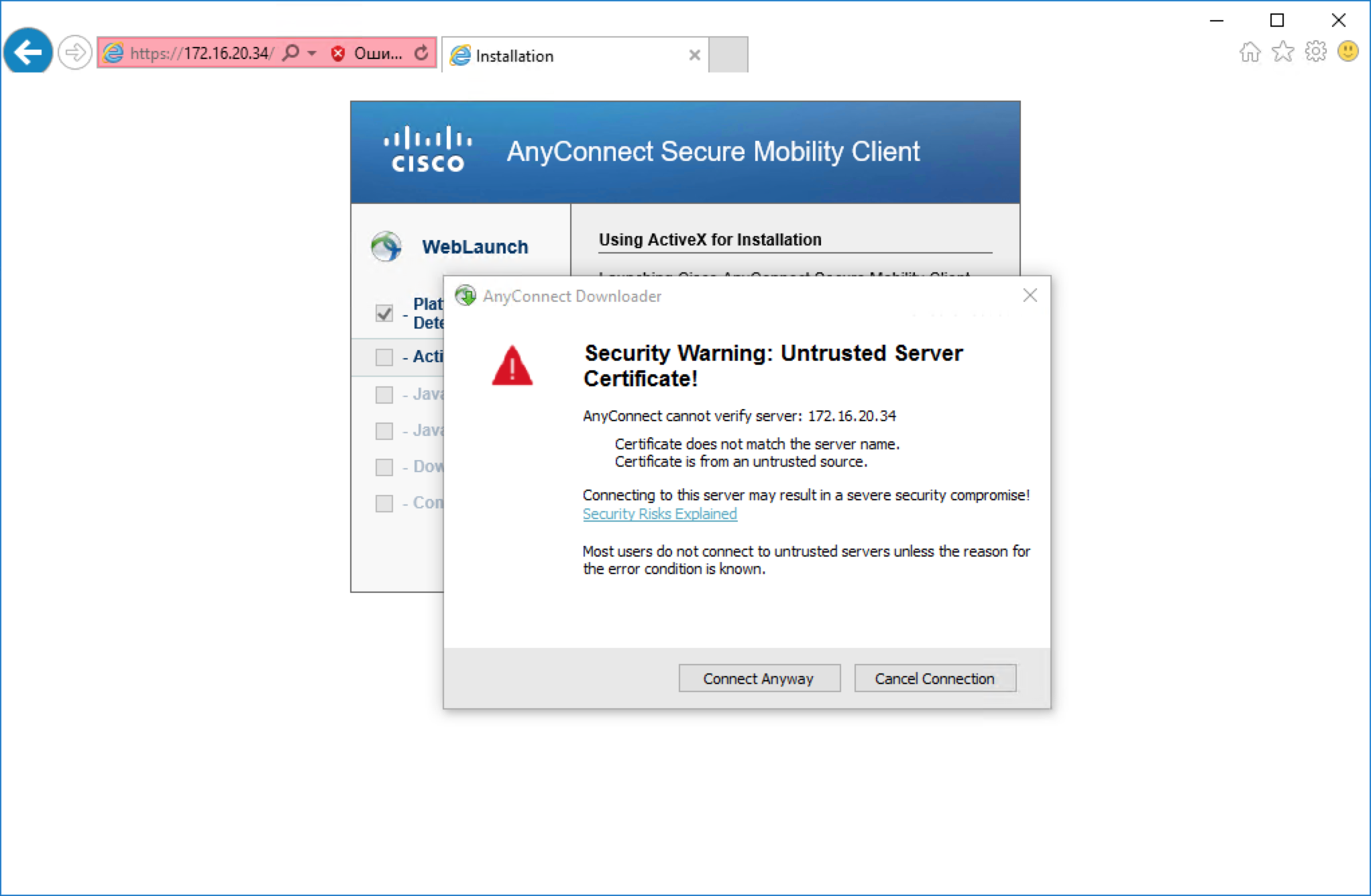
1. Connect to the BoR Customer TG access server using Internet Explorer 10 or later: <https://172.16.20.42> (test segment) or <https://172.16.20.34> (production segment).
2. Click 'Continue to this website (not recommended)' (Fig. 1).



1. Select the group to connect to ACCESS-VPN-TSH-KBR (TEST) / ACCESS-VPN-TSH-KBR (Fig. 2) and enter the Bank of Russia-provided username and password of the **channel** account (ххххххххх-xxxx) to access the test/production BoR Customer TG.



1. After entering the username and password, a user notification will appear on the screen. Click Continue at the bottom of the notification.
2. If the 'Security Warning: Untrusted Server Certificate' message (Fig. 3) appears, click Connect Anyway.



If ActiveX content is disabled in the exchange participant’s web browser, the following warnings may appear.



Figure 3.1. Click Yes in the AnyConnect Secure Mobility Client screen.

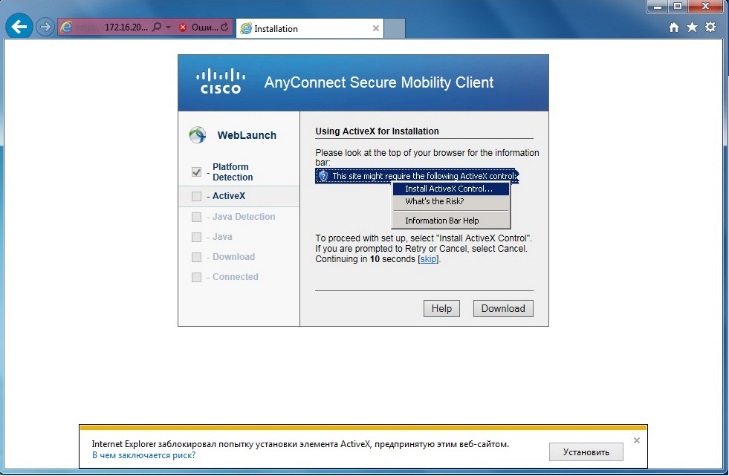
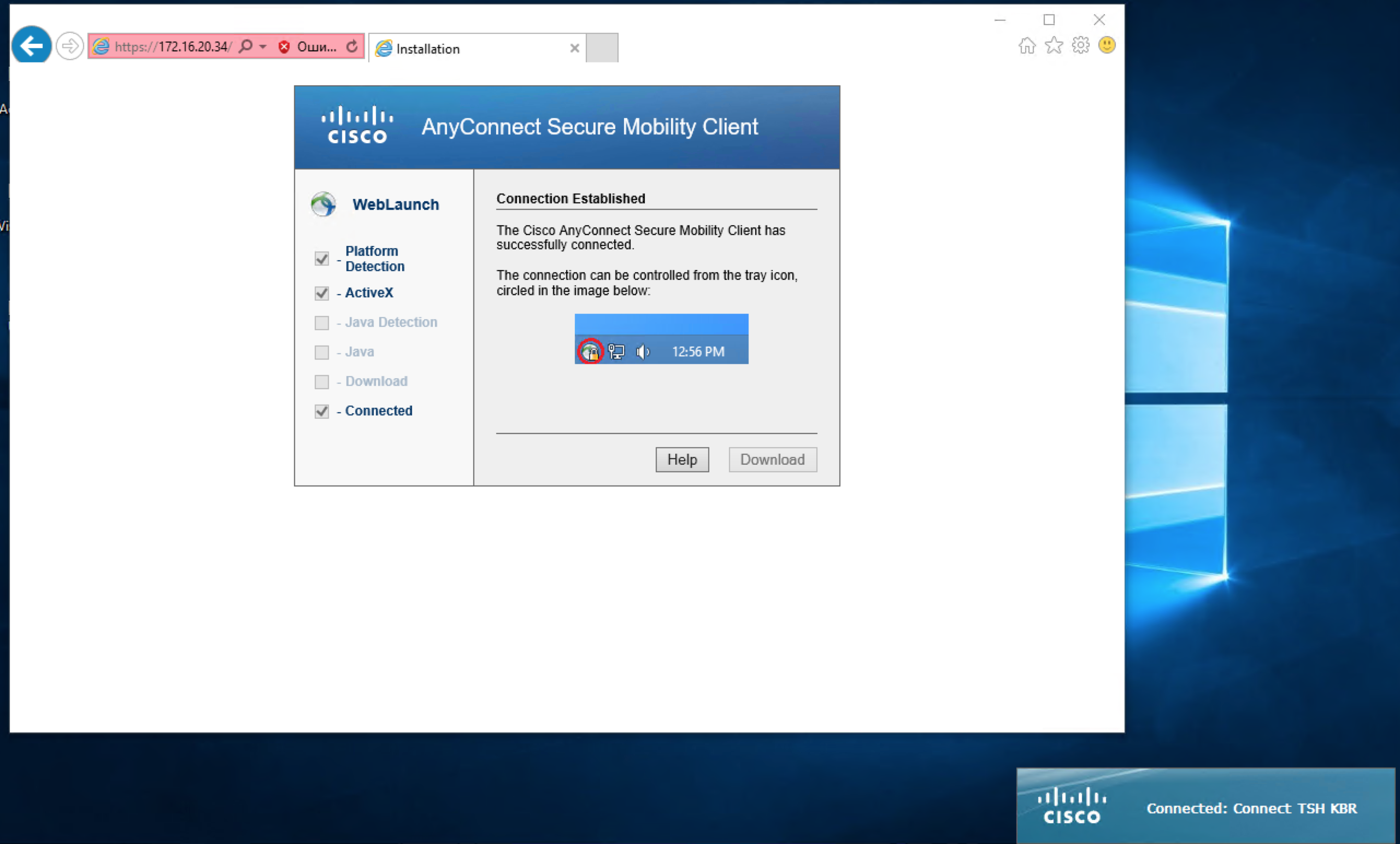
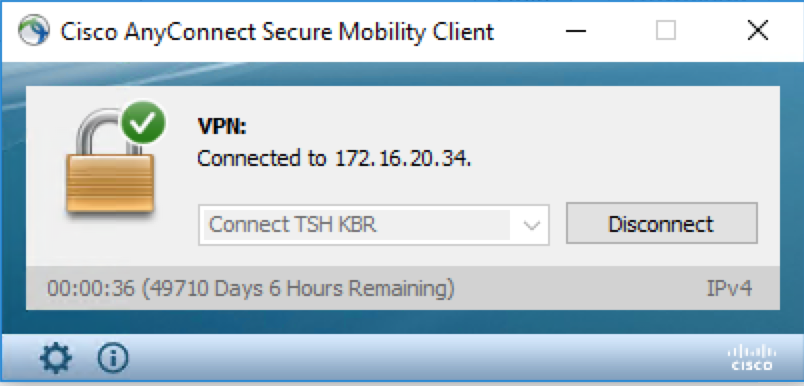


Figure 3.2. In the screen that appears, click Install ActiveX Control.

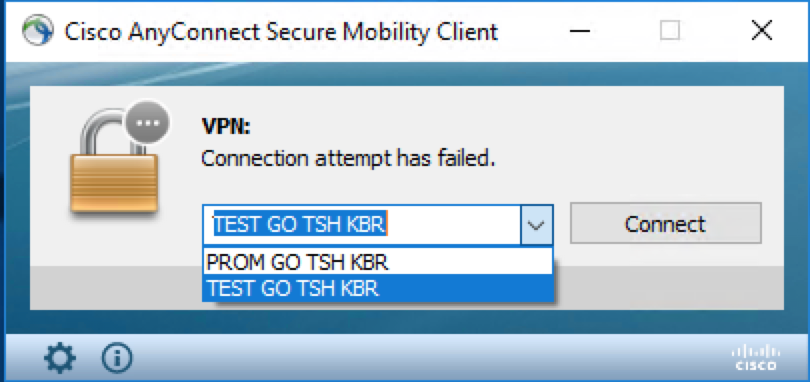
1. After Cisco AnyConnect is installed, a VPN connection with the BoR Customer TG access server will be automatically established (Fig. 4).



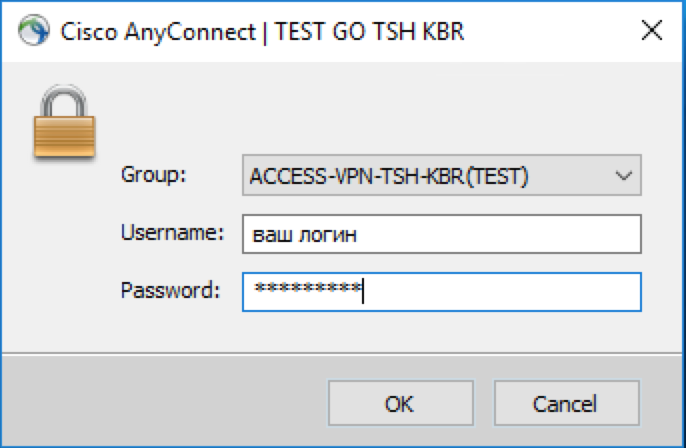
1. Find the Cisco AnyConnect icon in the tray, left-click on it and click Disconnect in the screen that appears (Fig. 5).



1. After disconnecting, click on the cross in the upper right corner of the window, after which the Cisco AnyConnect window will be minimised to tray and shown with this icon: .
2. The installation of Cisco AnyConnect on the participant’s PC is now complete.
   1. **Establishing a VPN connection with the BoR Customer TG**
3. Open Cisco AnyСonnect on the exchange participant’s PC (left-click on the  icon in the tray).
4. In the dialog box that opens (Fig. 6), select TEST GO TSH KBR (for test segment) or PROM GO TSH KBR (for production segment) from the drop-down list to interact with the BoR Customer TG and click Connect.



1. If the 'Security Warning: Untrusted Server Certificate' message appears, click Connect Anyway.
2. In the dialog box that opens (Fig. 7), select ACCESS-VPN-TSH-KBR (TEST) / ACCESS-VPN-TSH-KBR in the drop-down list of the Group field, enter the username and password of the channel account (xxxxxxxxxx-xxxx) issued by the Bank of Russia to access the BoR Customer TG test/production segment and click OK.



1. Upon successful authentication, a dialog box appears with a message about connecting to the access server of the test/production BoR Customer TG. Click Accept.

**Important**! When connecting to the test BoR Customer TG, use the **TEST** GO TSH KBR loop and the ACCESS-VPN-TSH-KBR (**TEST**) group. When connecting to the production BoR Customer TG, use the **PROM** GO TSH KBR loop and the ACCESS-VPN-TSH-KBR group.

* 1. **Checking the availability of the BoR Customer TG for applications, changing the channel and application accounts of exchange participants in the Personal Account of the BoR Customer TG**

After a VPN **to test segment** connection is established, the exchange participant’s PC should have access to the BoR Customer TG test segment server (172.16.19.211) to enable application interaction.

The IP address 172.16.19.211 provides two ports to interact with the BoR Customer TG:

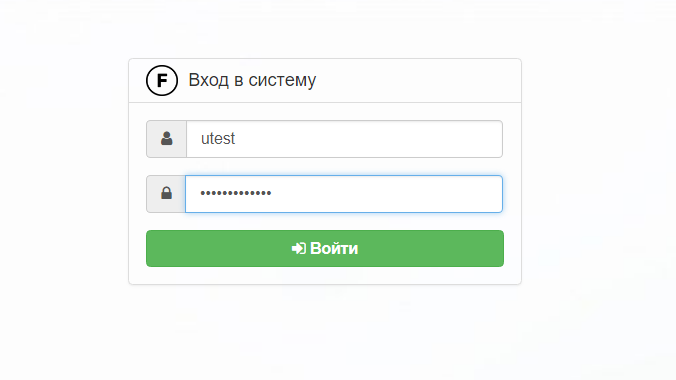
* [**http**://172.16.19.211:7777](http://172.16.19.211:7777) is used for interaction in the System-System mode. This address is specified in the settings of the AWS of a BoR Customer-FMS.
* [**https**://172.16.19.211:9697](https://172.16.19.211:9697) is used for interaction in the Human-System mode. This is the Personal Account of the BoR Customer TG user, in which they can change the passwords of the channel and application accounts or send and receive messages manually.

After a VPN **to production segment** connection is established, the exchange participant’s PC should have access to the BoR Customer TG production segment server (172.16.18.211) to enable application interaction.

The IP address 172.16.19.211 provides two ports to interact with the BoR Customer TG:

* [**http**://172.16.18.211:7777](http://172.16.18.211:7777) is used for interaction in the System-System mode. This address is specified in the settings of the AWS of a BoR Customer-FMS.
* [**https**://172.16.18.211:9697](https://172.16.18.211:9697) is used for interaction in the Human-System mode. This is the Personal Account of the BoR Customer TG user, in which they can change the passwords of the channel and application accounts or send and receive messages manually.

On the authentication page, enter the Bank of Russia-issued username and the password for the application account to connect to the test/production BoR Customer TG and click Login (Fig. 8).



After successful authorisation, the exchange participant can change the passwords of the channel and application accounts as well as send and receive messages in manual mode through an intuitive interface.

**For more details on how to download Cisco AnyConnect, establish a VPN connection and use your BoR Customer TG Personal Account, please see the BoR Customer TG User Manual.**