Santander Group VPN

Windows PC Configuration

Content

1   Scope and prerequisites.

The purpose of this document is to guide third-party users from Santander Group to set up their computers and achieve a proper connection with our infrastructure.

1.1   Administrative prerequisites.

- Customer needs a valid user account in an Active Directory.
- The user account needs to be configured in a second factor authorization method (currently we support Azure MFA)

1.2   User machine prerequisites.

Windows PC:

- Windows 8.
    - o Any updated Antivirus Software.
    - o Microsoft latest patches installed.
- Windows 10.
    - o Any updated Antivirus Software.
    - o Microsoft latest patches installed.

2   Software provisioning.

With this document, customer should receive link of Sharepoint which contains these files:
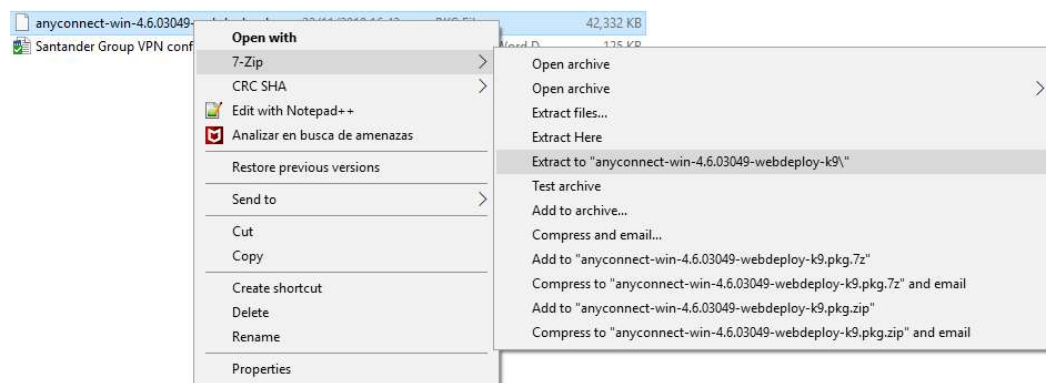
- o   XML file with VPN connection data.
- o   Public certificates from Entrust.
- o   Cisco software "anyconnect-win-4.10.01075-webdeploy-k9.pk

3 Anyconnect VPN setup.

3.1 Software installation.

First, we need to extract the software "anyconnect–win–4.10.01075–webdeploy–k9.pk":

Right click on the file and extract it to a folder:

Then, we navigate into anyconnect-win-4.10.01075-webdeploy-k9\binaries folder:

In this folder we have all the software needed. The VPN needs these 3 installations:

anyconnect-win-4.10.01075-core-vpn-webdeploy-k9.msi

anyconnect-win-4.10.01075-posture-webdeploy-k9.msi

anyconnect-win-4.10.01075-iseposture-webdeploy-k9.msi

They have to be installed by default and in the same order:

1. anyconnect-win–4.10.01075-core-vpn-webdeploy-k9.msi
2. anyconnect-win–4.10.01075-posture-webdeploy-k9.msi
3. anyconnect-win–4.10.01075-iseposture-webdeploy-k9.msi

3.2   Certificate installation.

Santander VPN infrastructure is verified through Entrust Private SSL infrastructure:

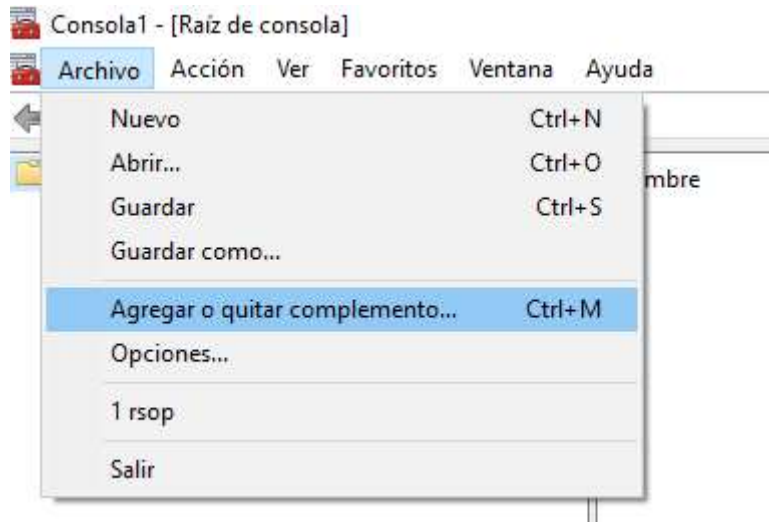https://www.entrustdatacard.com/products/ssl-certificates/private-ssl

So, the customer PC needs to trust them in order to work. The certificates provided among this document must be installed under "Trusted Root Certificate Authorities":
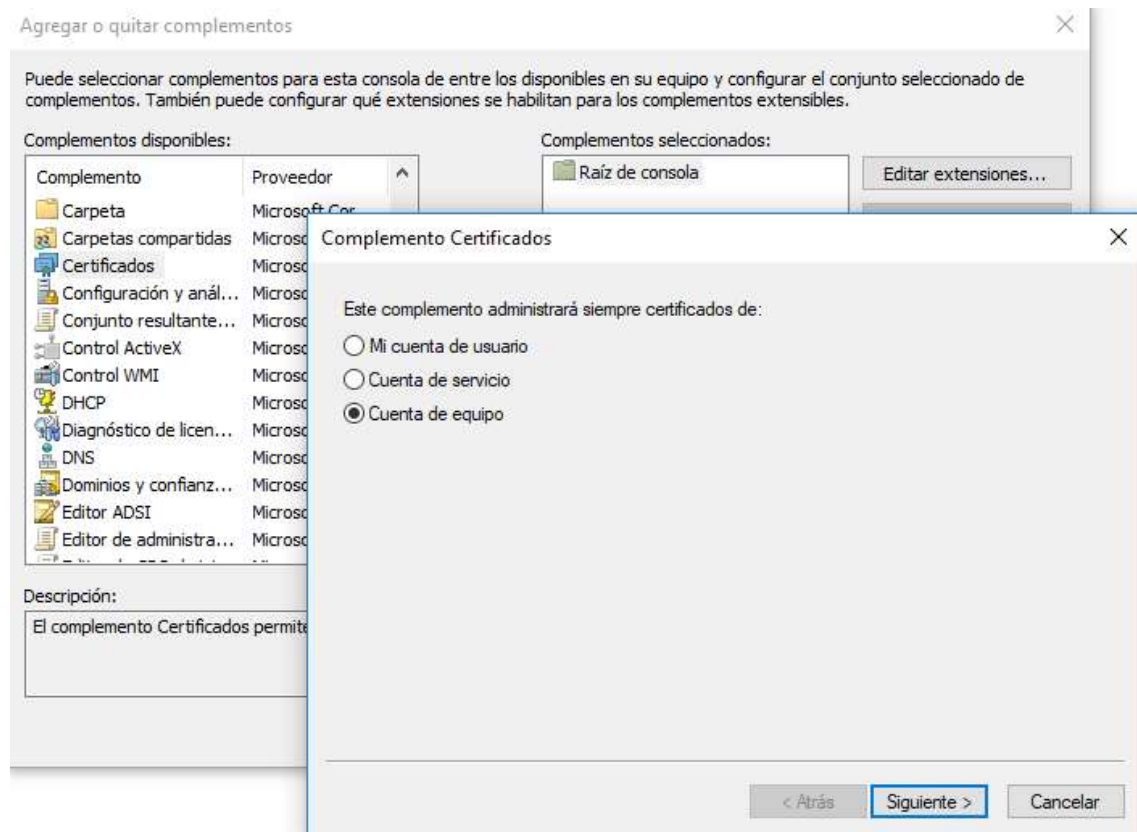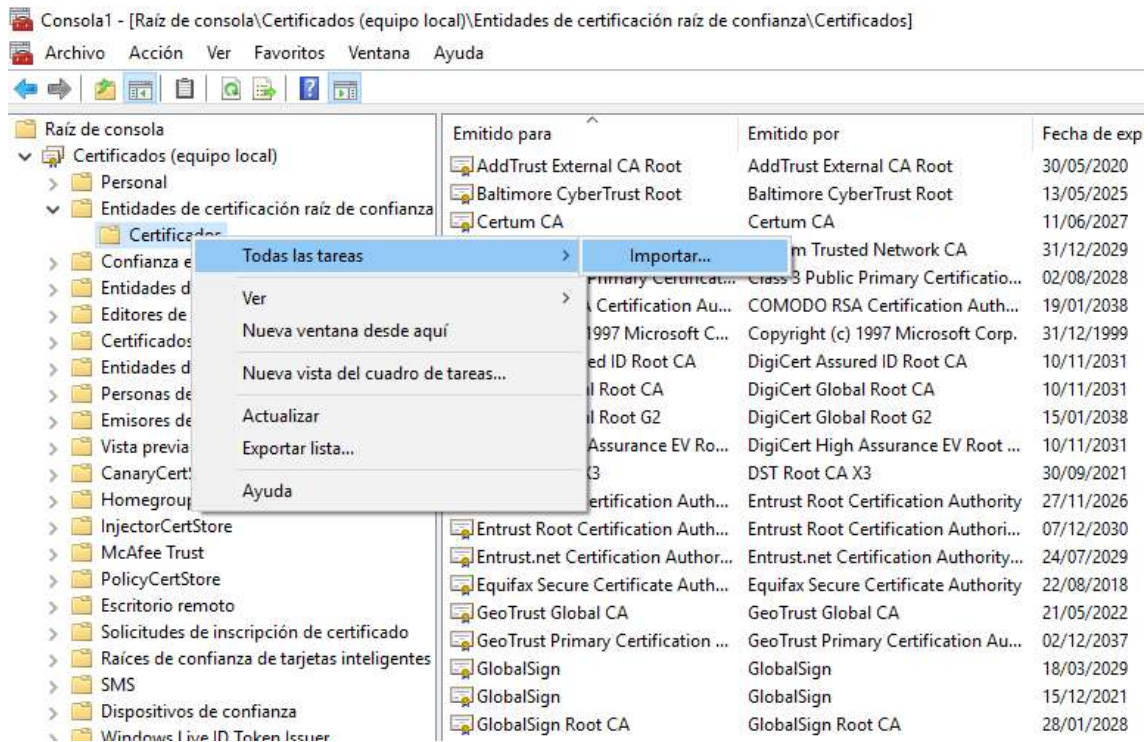
Run mmc.exe as administrator:
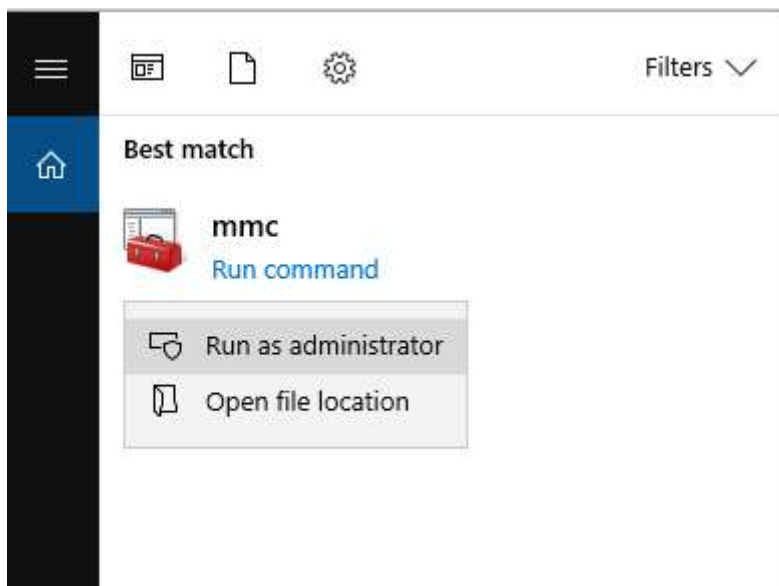
Click on File-> add or remove snap-in (Control+M):

And add "certificates" snap-in, local machine account:

In the console menu, we navigate into "Trusted Root Certificates Authorities", right click, import:

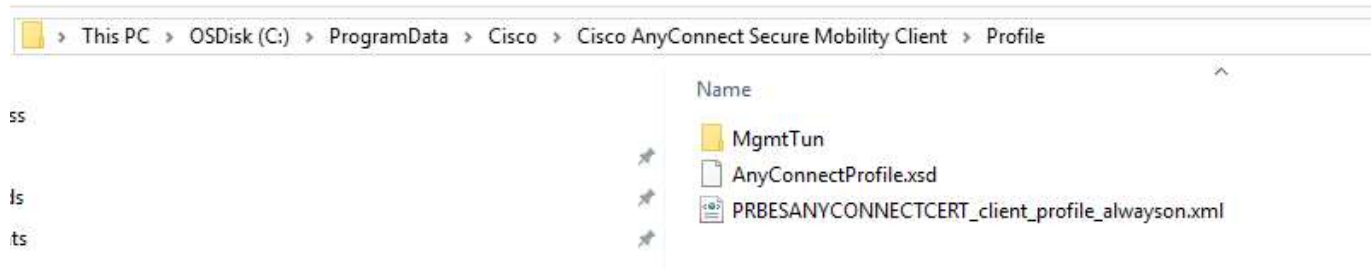And select the provided certificates. Once both certificates are installed, we need to reboot the PC.

3.3   Anyconnect parametrization.

After Anyconnect client installation a new folder is available on the computer:

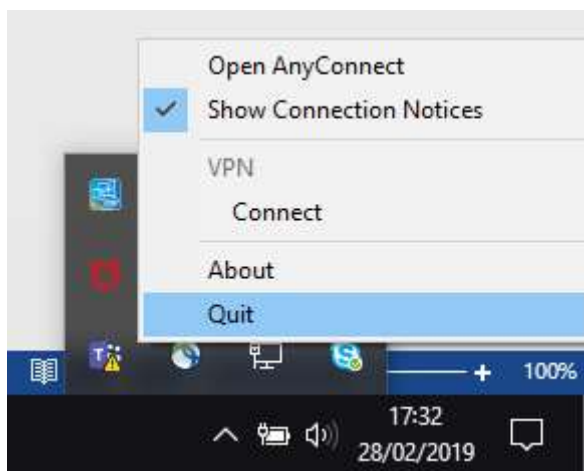%programdata%\cisco\Cisco AnyConnect Secure Mobility Client\Profile\

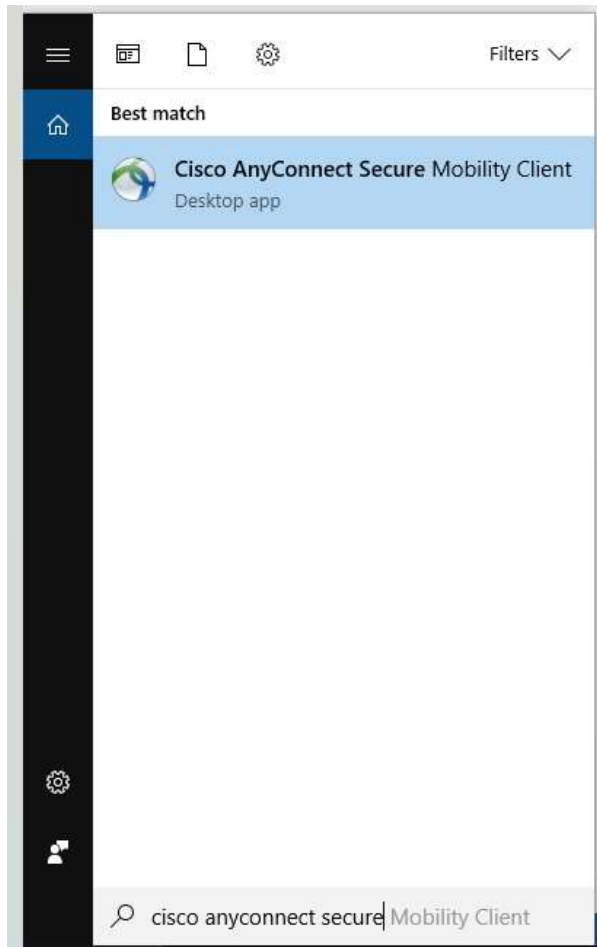In this folder, we should copy the XML file.

> This PC > OSDisk (C:) > ProgramData > Cisco > Cisco AnyConnect Secure Mobility Client > Profile

Name

MgmtTun
AnyConnectProfile.xsd
PRBESANYCONNECTCERT_client_profile_alwayson.xml

Then, restart Anyconnect software:

On windows taskbar, rigth click on icon, select "quit":
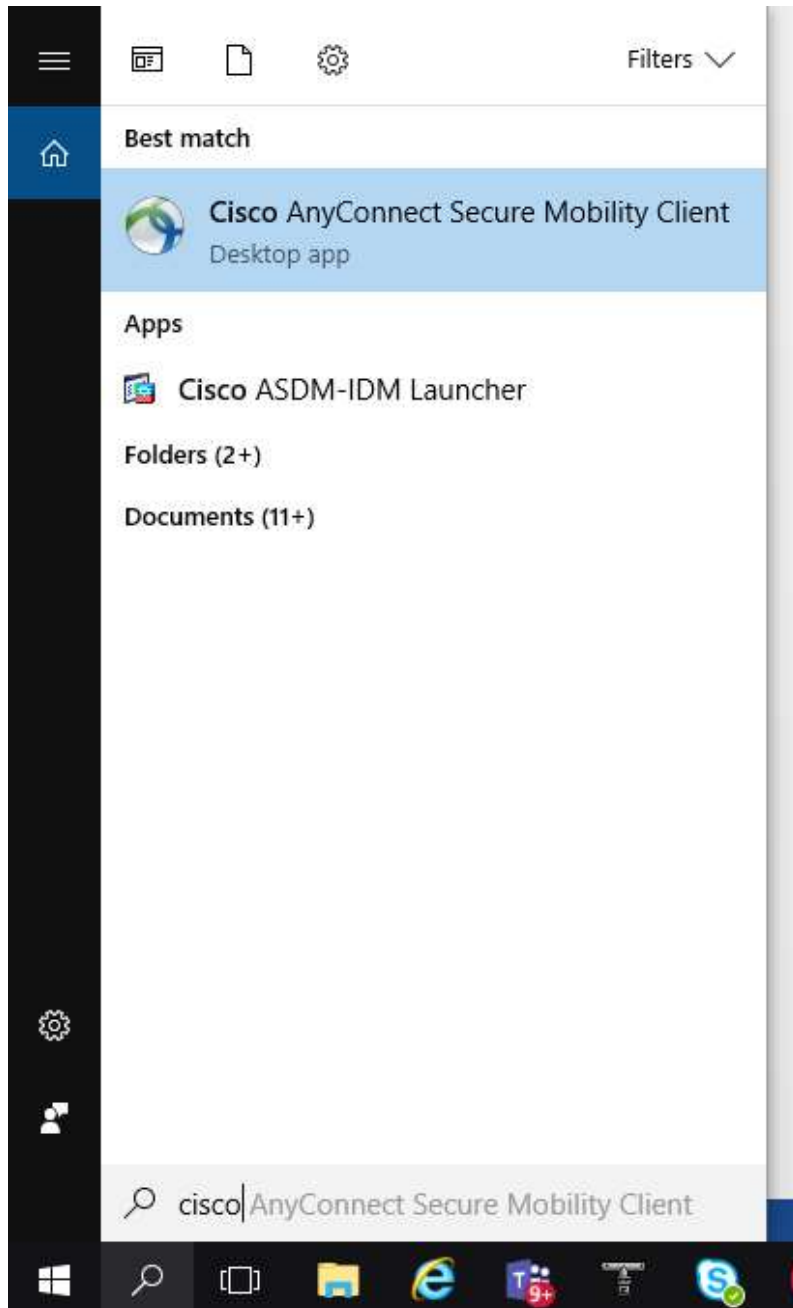
Then, we launch again the Anyconnect client:

Now, anyconnect is ready to connect*:
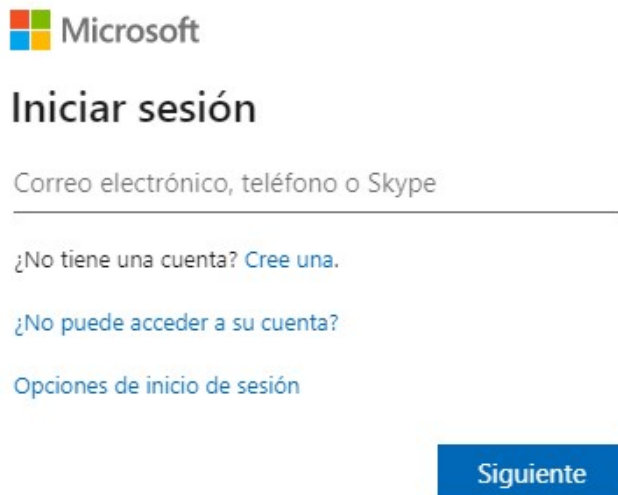

*The name of the profile (Third_parties_VPN) could be different

 Santander Global Tech

4   VPN User experience.

First, we need to start the client:

Click on connect, in your client and you will be redirected to Microsoft login web page where you will be requested your UPN login

If you already have configured your 2FA it will be also requested, if not, review the on boarding document: Authentication procedure with Microsoft Azure MFA

Once fulfilled and logged into the vpn the Posture starts to analyze if the computer has antivirus and Patches:

And, when finished, it remains connected to the VPN.