

Lab 9: Edge Server Documentation

CISA 4195 - Unified Communications

Gabriel Kwan

March 4, 2019

Contents

1	Preamble	3
2	Reasons for Edge Server Deployment	3
3	VM Requirements	3
4	Major Steps in Deploying Edge Server	5
4.0.1	Defining your edge Server Topology	6
4.0.2	Publishing the Edge Server Topology	12
4.0.3	Exporting the Edge Server Topology	13
4.0.4	Deploying Edge Server	14
5	Other Configuration	22

1 Preamble

Purpose of this document is to outline the process of deploying the Edge Server. Testing is still being conducted on connectivity. Details of external client connectivity will be examined in upcoming report.

2 Reasons for Edge Server Deployment

There are two major functionalities enabled by Edge Deployment. They are as follows:

1. Remote User Connections
2. Federation with other SIP domains

3 VM Requirements

1. Create a new VM
2. Ensure that the VM has two network cards
 - (a) the first network card should use VMNET2
 - (b) The other network card should use a bridged connection
3. Install Server 2016
4. Once installed, change the hostname to edge.gabrielk.local; do not join domain. See figure 1 for more details.
5. Ensure edge server can resolve all other servers in topology.

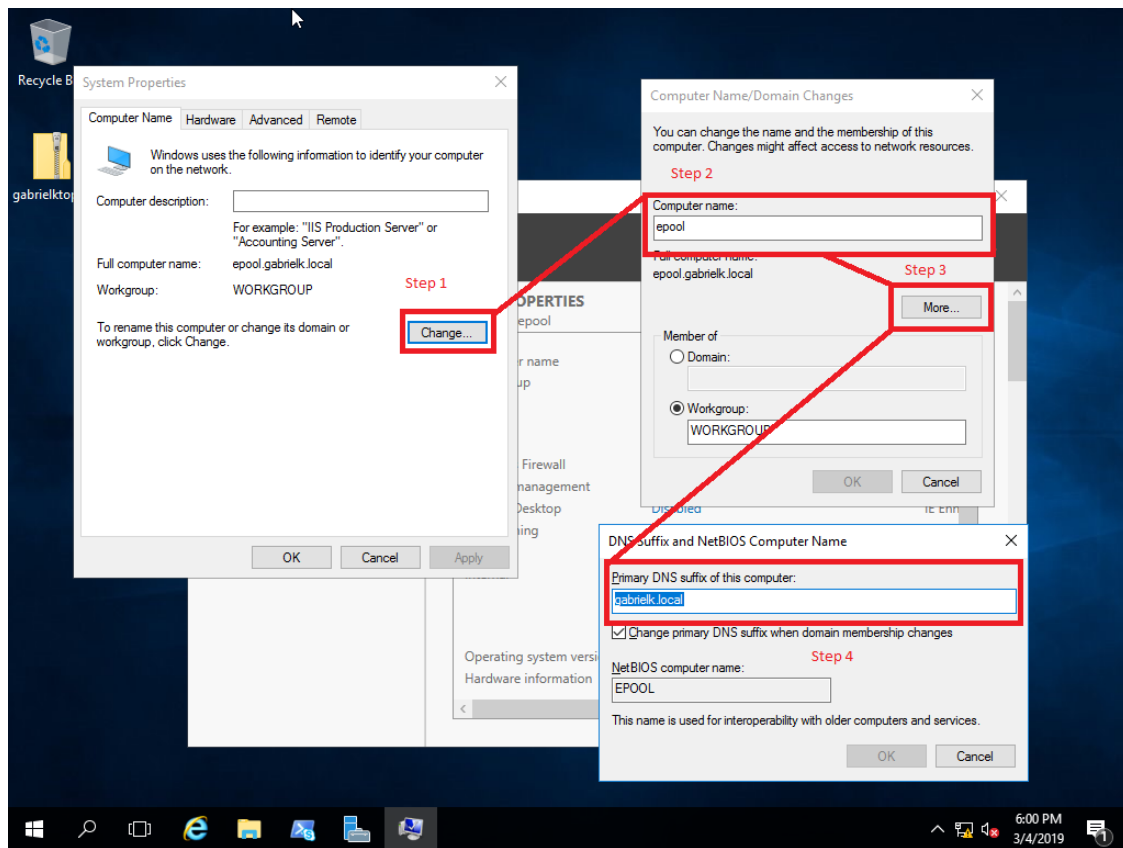


Figure 1: Process of Changing the Name without joining domain

4 Major Steps in Deploying Edge Server

There are four major steps in deploying the Edge Server. They are as follows:

1. Defining your Edge Server Topology
2. Publish your Edge Server Topology
3. Export your your Edge Server Topology
4. Deploy Edge Server
 - This document will not cover topics of external DNS, though that is required for external connections to be made
 - The following sections will document the aforementioned steps

4.0.1 Defining your edge Server Topology

The final results should be as seen in figure below:

General	
Internal server FQDN:	edge.gabrielk.local
Internal IPv4 address:	192.168.18.131
Federation (port 5061):	Enabled
Skype-Skype federation search (port 4443):	Enabled
XMPP federation (port 5269):	Enabled
Internal Configuration Replication Port (HTTPS)	4443

Next hop selection	
Next hop pool:	pool.gabrielk.local (gabriel.hq)

External settings	
Access Edge service	
FQDN:	sip.gabrielk.local
IPv4 address:	142.232.199.226
Port:	5061
Protocol:	TLS
Web Conferencing Edge service	
FQDN:	sip.gabrielk.local
IPv4 address:	142.232.199.226
Port:	444
Protocol:	TLS
A/V Edge service	
FQDN:	sip.gabrielk.local
NAT:	Disabled
IPv4 address:	142.232.199.226
Port:	443
Protocol:	TCP

Figure 2: Final Topology Configuration of Edge Server

It is configured as seen below

1. On your SfB Frontend pool server, open the SfB Server Topology Builder
2. Download the existing topology when prompted
3. Once the existing topology has been loaded, in the console tree, expand the site and right click Edge Pools and click new Edge Pool

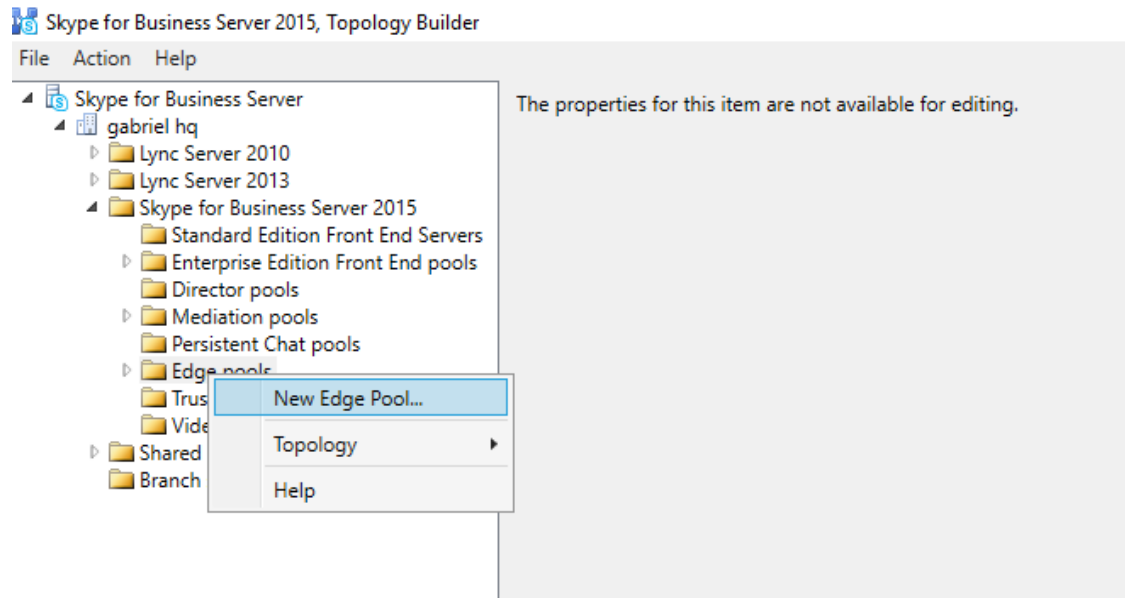


Figure 3: Location of Edge Pool under Skype Server 2015

4. On the "Define New Edge Pool" page, select next.

5. On the "Define the Edge pool FQDN" screen specify the FQDN of the edge server ensure that option "Single Computer pool" is selected

The screenshot shows a Windows-style dialog box titled "Define New Edge Pool". Inside, there's a section titled "Define the Edge pool FQDN" with a sub-instruction: "Define the fully qualified domain name (FQDN) for the Edge pool, and indicate whether this should be a single computer or multi-computer pool." Below this, there's a text input field labeled "FQDN: *" containing the text "edge.gabrielk.local". Underneath the input field are two radio button options. The first option is "This pool has multiple servers." with the instruction "Select this option if you want load balancing and high availability support on this pool." The second option is selected and is labeled "This pool has one server." with the instruction "Select this option if you don't need load balancing or high availability support on this pool." At the bottom of the dialog are four buttons: "Help", "Back", "Next", and "Cancel".

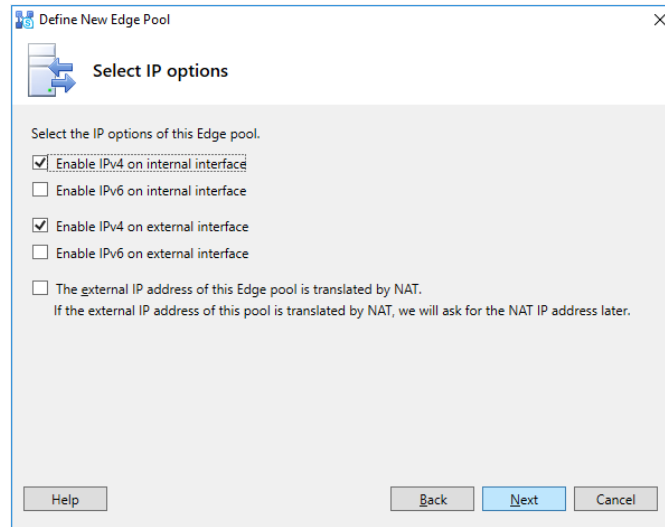
Figure 4: Specify the Edge Pool and selecting Single Computer Pool. Make sure that this matches the server name.

6. On the Enable Federation Page select all features.

The screenshot shows the same "Define New Edge Pool" dialog box, but now on the "Enable federation" step. The instruction says "Set the federations of this Edge pool." There are three checked checkboxes, each followed by a warning: "Enable federation (port 5061).", "Enable Skype-Skype federation search (port 4443).", and "Enable XMPP federation (port 5269).". Each warning explains that only one Edge pool will be actively used for that specific federation type and advises ensuring the external DNS SRV record points to the correct Edge pool. At the bottom are the same four buttons: "Help", "Back", "Next", and "Cancel".

Figure 5: All features Selected. Federation enables other SfB servers to communicate with our domain's SfB.

7. In the IP Options screen, ensure that at least the ipv4 options are selected.



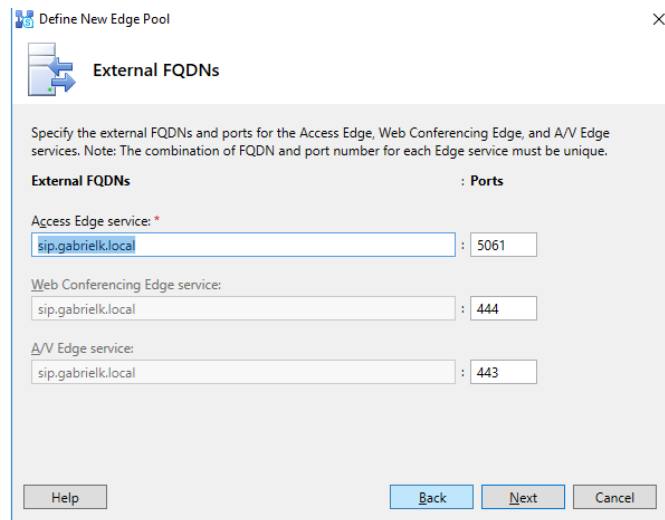
The screenshot shows the 'Define New Edge Pool' dialog box with the 'Select IP options' tab selected. The dialog contains the following options:

- ☒ Enable IPv4 on internal interface
- ☐ Enable IPv6 on internal interface
- ☒ Enable IPv4 on external interface
- ☐ Enable IPv6 on external interface
- ☐ The external IP address of this Edge pool is translated by NAT.
If the external IP address of this pool is translated by NAT, we will ask for the NAT IP address later.

At the bottom, there are buttons for 'Help', 'Back', 'Next', and 'Cancel'.

Figure 6: IPv4 only. Do not select the NAT option as shown.

8. On the "External FQDNs Screen" ensure external FQDNs is specified as follows



The screenshot shows the 'Define New Edge Pool' dialog box with the 'External FQDNs' tab selected. The dialog contains the following information:

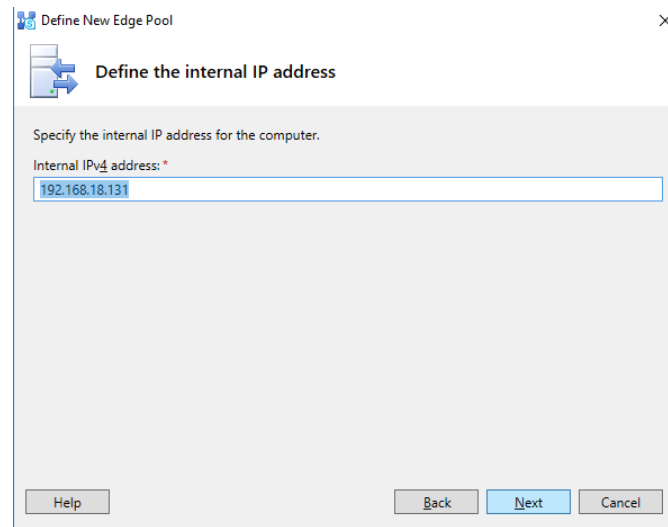
Specify the external FQDNs and ports for the Access Edge, Web Conferencing Edge, and A/V Edge services. Note: The combination of FQDN and port number for each Edge service must be unique.

External FQDNs	Ports
Access Edge service: *	
sip.gabrielk.local	5061
Web Conferencing Edge service:	
sip.gabrielk.local	444
A/V Edge service:	
sip.gabrielk.local	443

At the bottom, there are buttons for 'Help', 'Back', 'Next', and 'Cancel'.

Figure 7: value should be sip.gabrielk.local for all 3. Make sure ports are as seen.

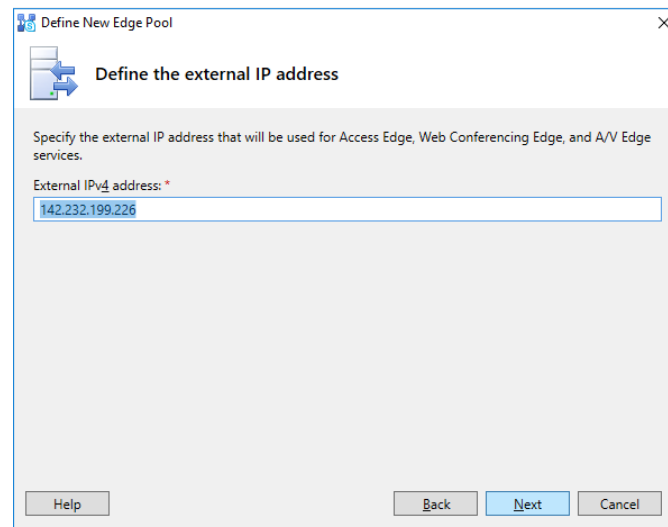
9. In the "Define the Internal IP Address" screen, type in 192.168.18.131



The screenshot shows a dialog box titled "Define New Edge Pool" with a close button (X) in the top right corner. Below the title bar is a navigation pane with a folder icon and a blue arrow icon. The main area is titled "Define the internal IP address" and contains the instruction "Specify the internal IP address for the computer." Below this is a text field labeled "Internal IPv4 address: *" with the value "192.168.18.131" entered. At the bottom are four buttons: "Help", "Back", "Next" (highlighted in blue), and "Cancel".

Figure 8: Defining the internal address.

10. On the "Define the External IP Address" screen use the ip address given to machine on second interface by BCIT DHCP server



The screenshot shows a dialog box titled "Define New Edge Pool" with a close button (X) in the top right corner. Below the title bar is a navigation pane with a folder icon and a blue arrow icon. The main area is titled "Define the external IP address" and contains the instruction "Specify the external IP address that will be used for Access Edge, Web Conferencing Edge, and A/V Edge services." Below this is a text field labeled "External IPv4 address: *" with the value "142.232.199.226" entered. At the bottom are four buttons: "Help", "Back", "Next" (highlighted in blue), and "Cancel".

Figure 9: Defining the external address. In our case 142.232.199.226

11. In the "Define the next hop" screen, select the name of the internal pool. That should be pool.gabrielk.local.

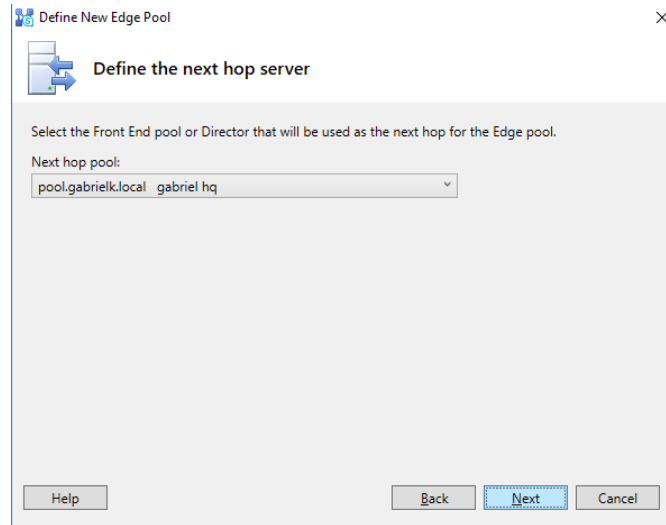


Figure 10: Specifying the Frontend server as the next hop.

12. Proceed to the following screen, ensure the Frontend pool it is selected. Click Finish

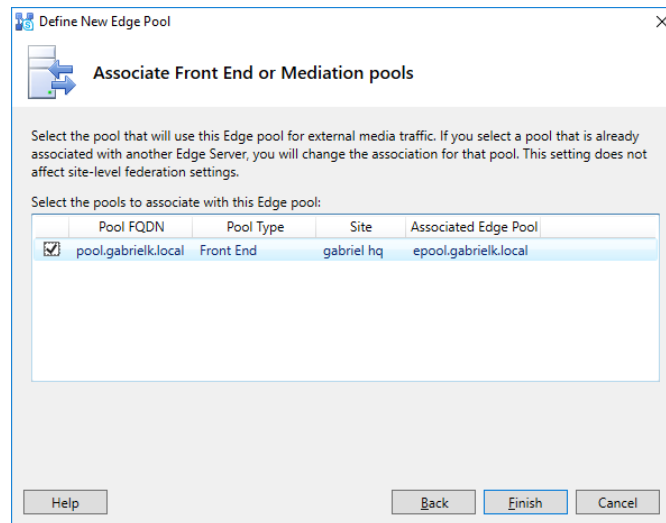


Figure 11: If there is a pool already associated, it will be replaced.

NOTE: Ensure that the hostname of the edge server matches that pool name of the server. Otherwise installing of Skype Server Components will fail and will require re-provisioning another VM. The installer will give errors stating that the server is not part of the topology.

4.0.2 Publishing the Edge Server Topology

1. In the topology builder, click action in the toolbar
2. Click publish.

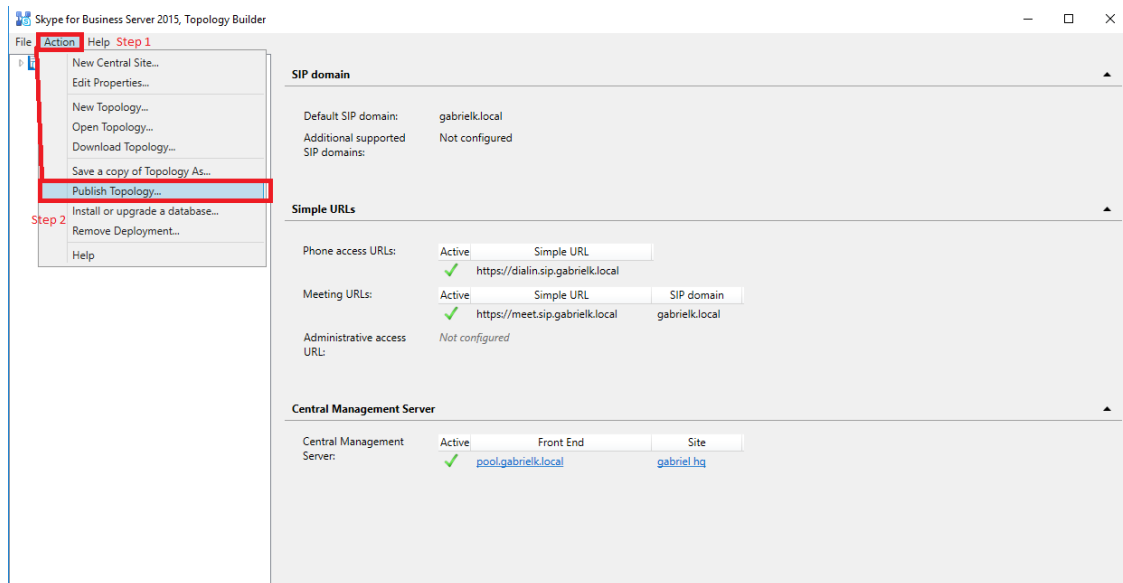
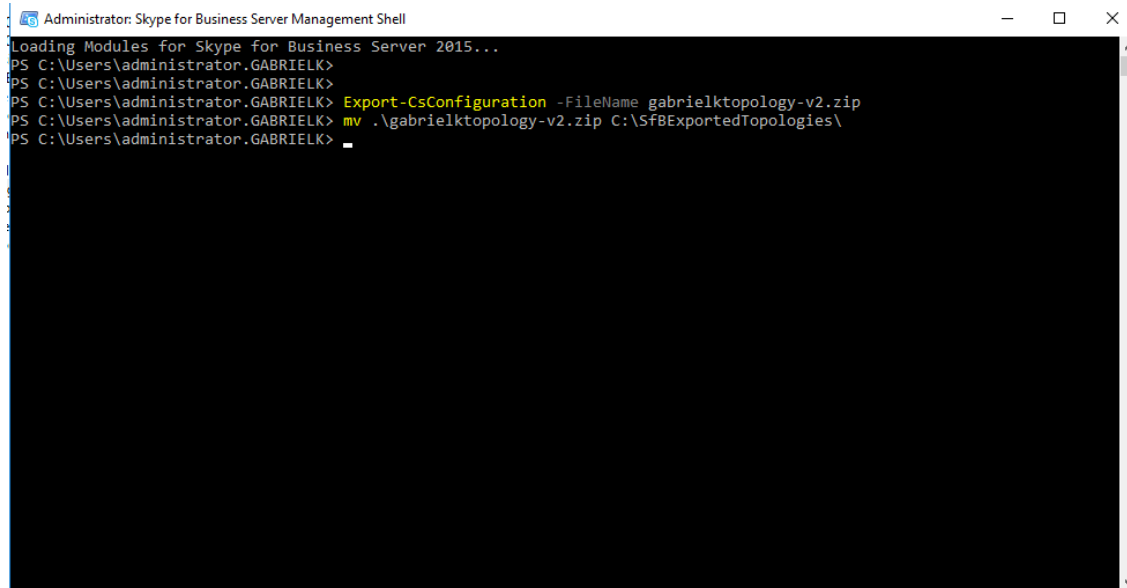


Figure 12: Steps to Publish Topology

4.0.3 Exporting the Edge Server Topology

- SfB deployment Wizard needs to access the central store for successful deployment. The following Steps will implement this:

1. Start the Managment Shell on the SfB Frontend
2. Run `Export-CsConfiguration -FileName <ConfigurationFilePath.zip>`
3. Place the exported file in a file share that is reachable from the Edge Server



```
Administrator: Skype for Business Server Management Shell
Loading Modules for Skype for Business Server 2015...
PS C:\Users\administrator.GABRIELK>
PS C:\Users\administrator.GABRIELK>
PS C:\Users\administrator.GABRIELK> Export-CsConfiguration -FileName gabrielktopology-v2.zip
PS C:\Users\administrator.GABRIELK> mv .\gabrielktopology-v2.zip C:\SfBExportedTopologies\
PS C:\Users\administrator.GABRIELK>
```

Figure 13: Commands to export and move topology to file share that is accessible to the Edge Server

4.0.4 Deploying Edge Server

- The deployment of the Edge server is similar to the Frontend
- Skip prepare active directory and go straight to Install or Update Skype for Business
- The following steps will provide a general overview of steps taken and highlight major changes pertaining to the Edge Server

1. Install local configuration

Provided the topology is correct, it should work fine.

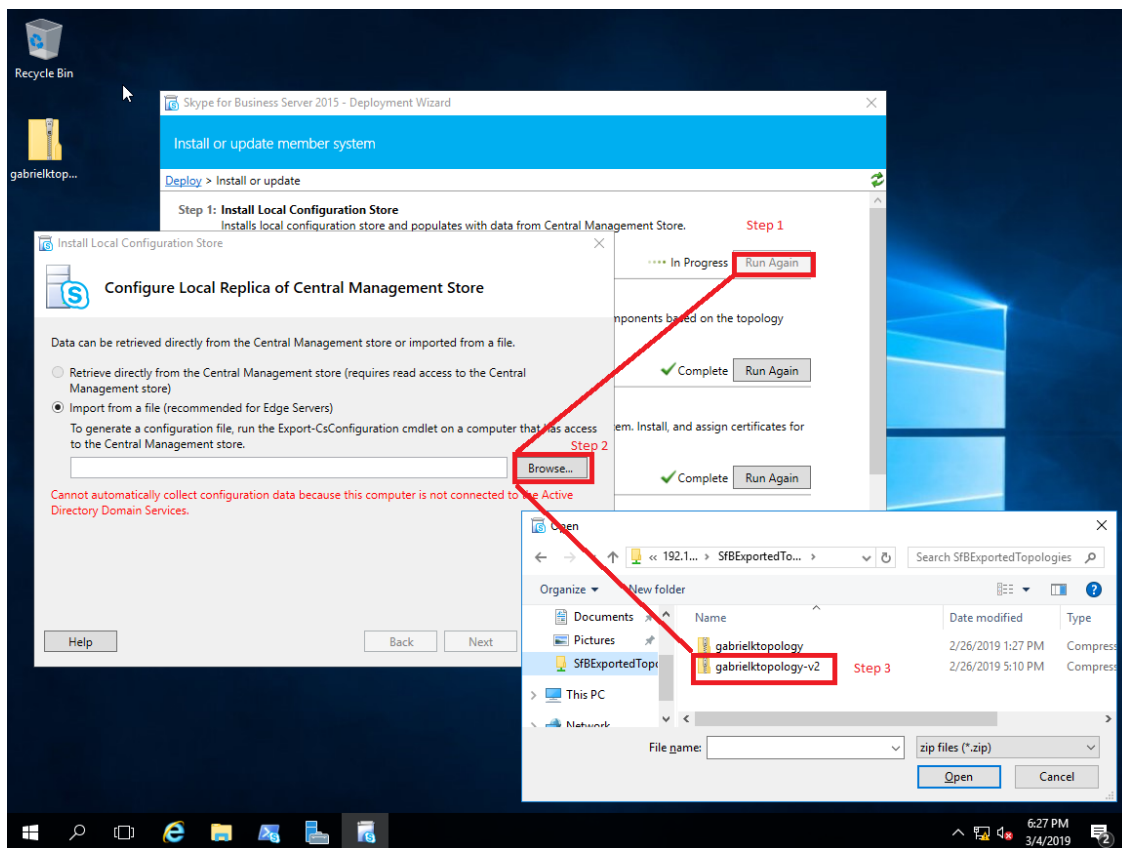


Figure 14: When selecting installing the local configuration store select the exported topology file from previous step.

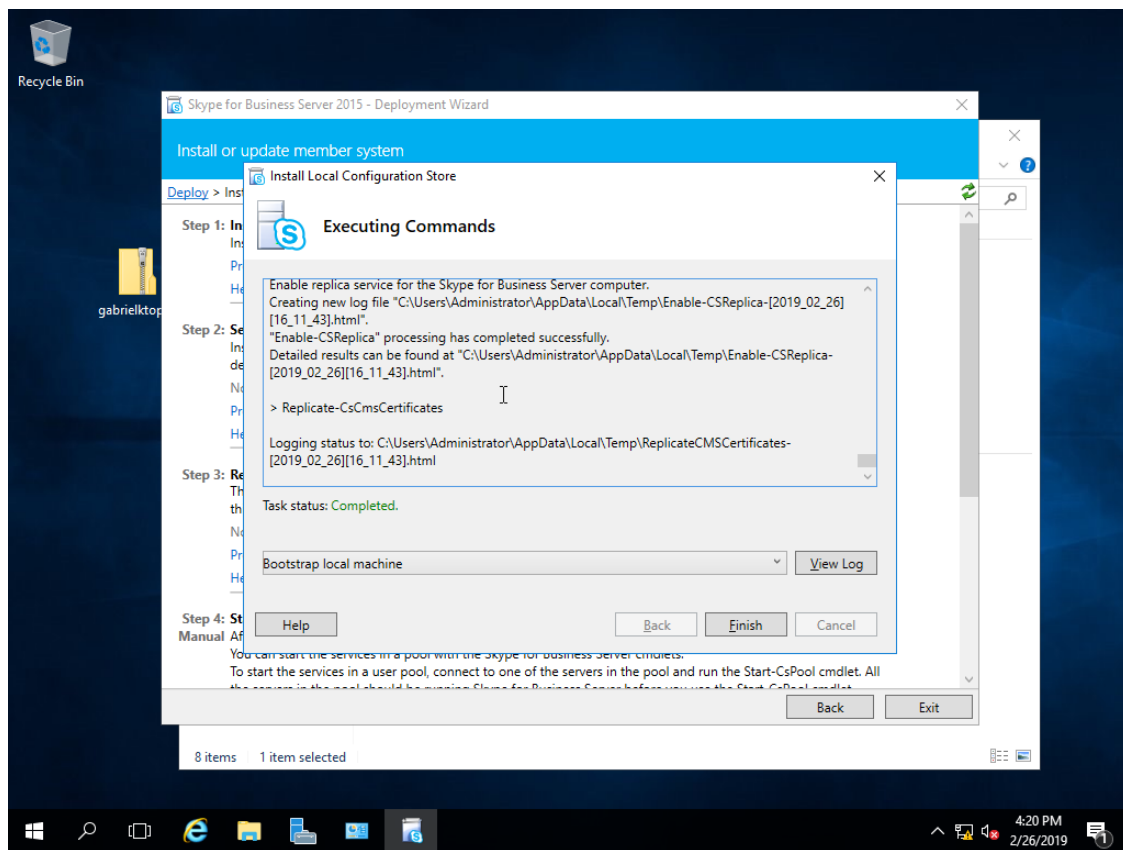


Figure 15: Success!

2. Install Skype For Business Components

Provided the topology was properly set up, there should be no issues with this section. Simply run it and it should work.

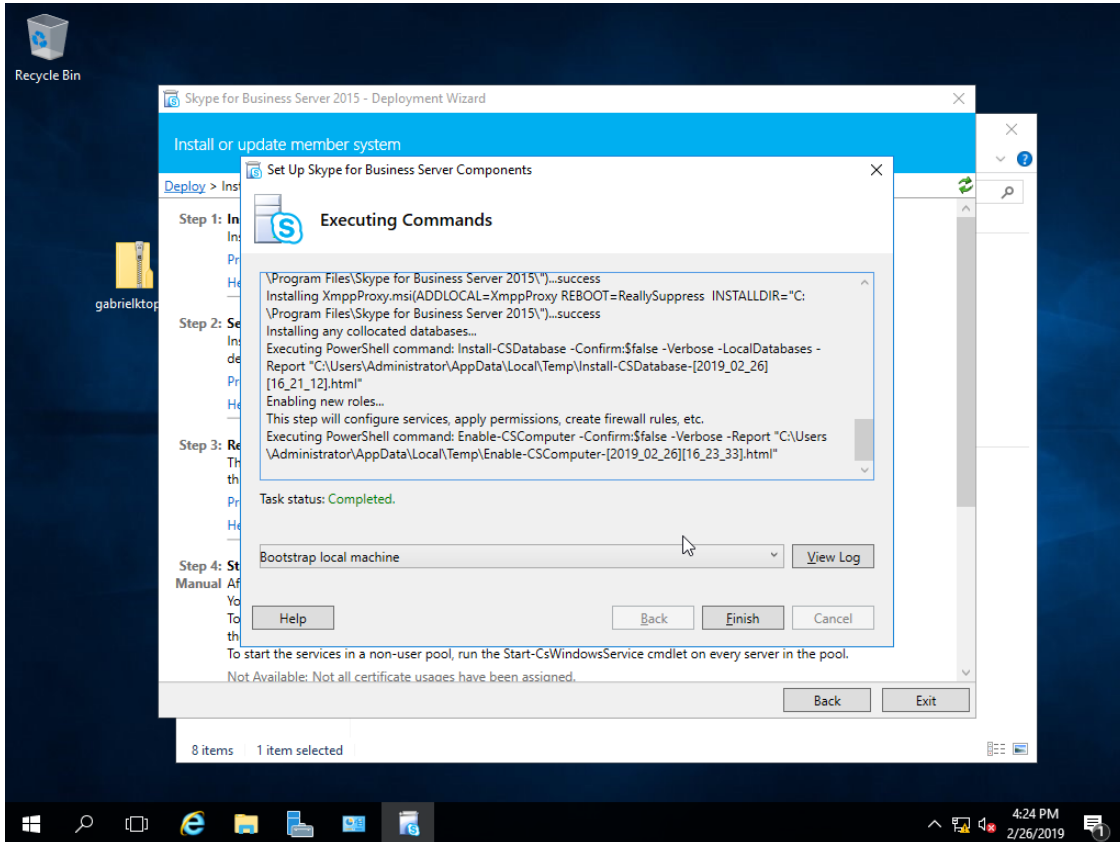


Figure 16: Success!

3. Requesting and Assigning Certificates

Requesting of certificates can be done in two steps. They can be done in any order. Once imported, the certificates can be assigned as done in Frontend server.

(a) Importing Root CA Certificate

This step is necessary for the previously imported External and Internal Edge Certificates to be made available to the Sfb installer to assign. Because the Edge Server does not have inherit trust as does the Frontend server due to its lack of integration with the domain.

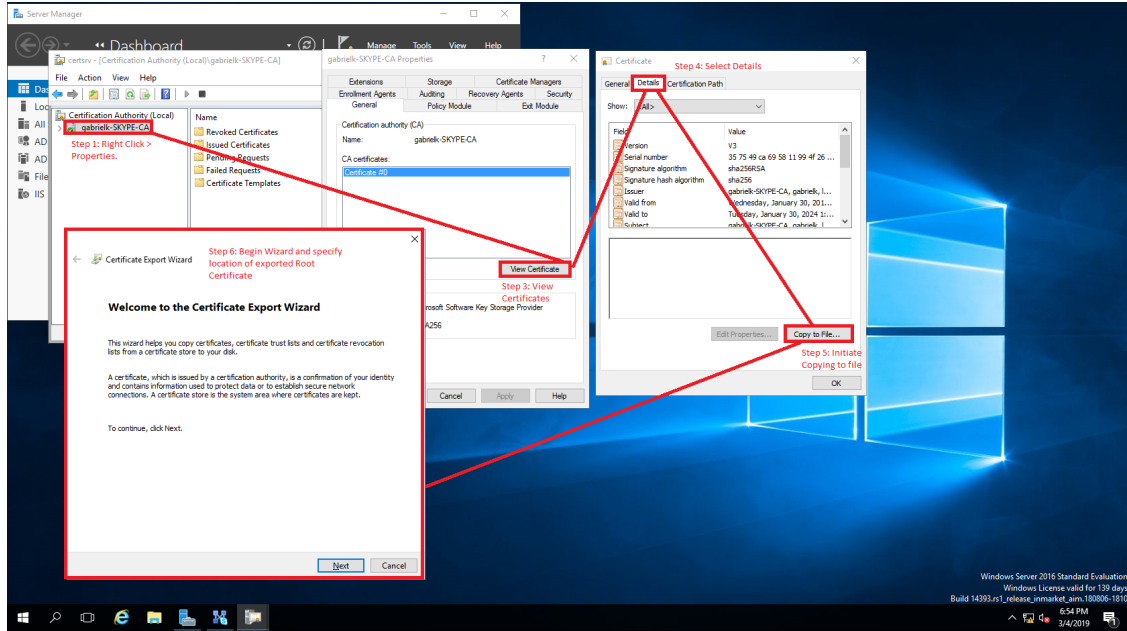


Figure 17: Step 1 of importing the RootCA certificate in order for the imported certificates be assignable on the Edge Server. The RootCA must be exported from within the CA as seen. This is done on the CA.

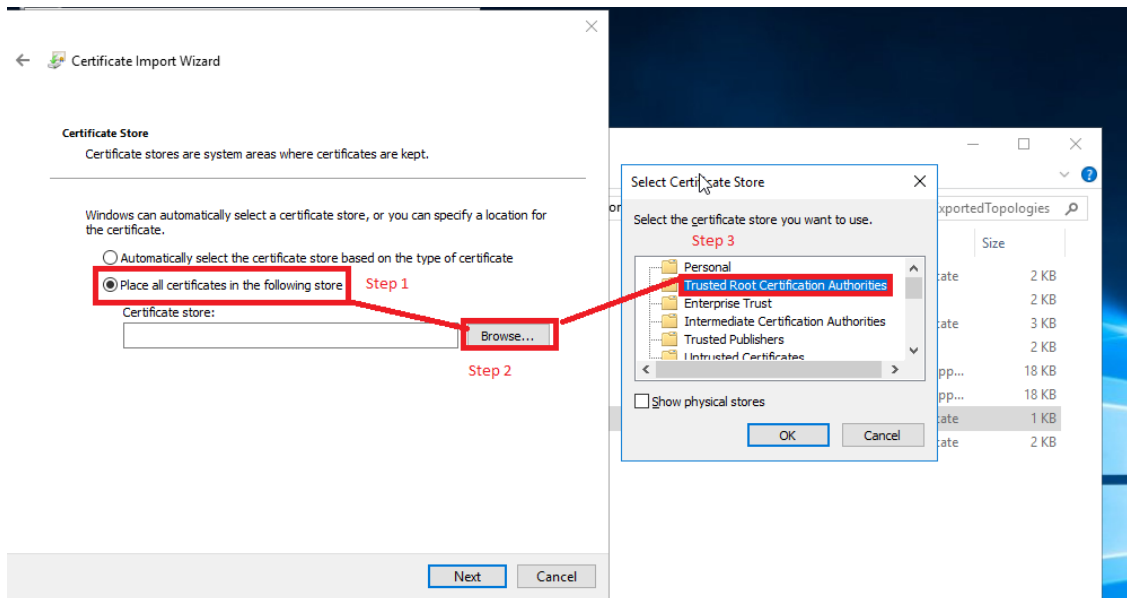


Figure 18: Step 2 of importing RootCA certificate. This is done on the Edge Server. When going through the Certificate Import Wizard, specify the "Trusted Root Certification Authorities" store.

(b) Creating Offline Requests

Because Edge server is not part of the domain; therefore, it will not be able to conduct a assignment as done with the Frontend server. As such, offline requests were required to created exportable certificates that could be manually installed on the edge server. See the figures 19 and 20.

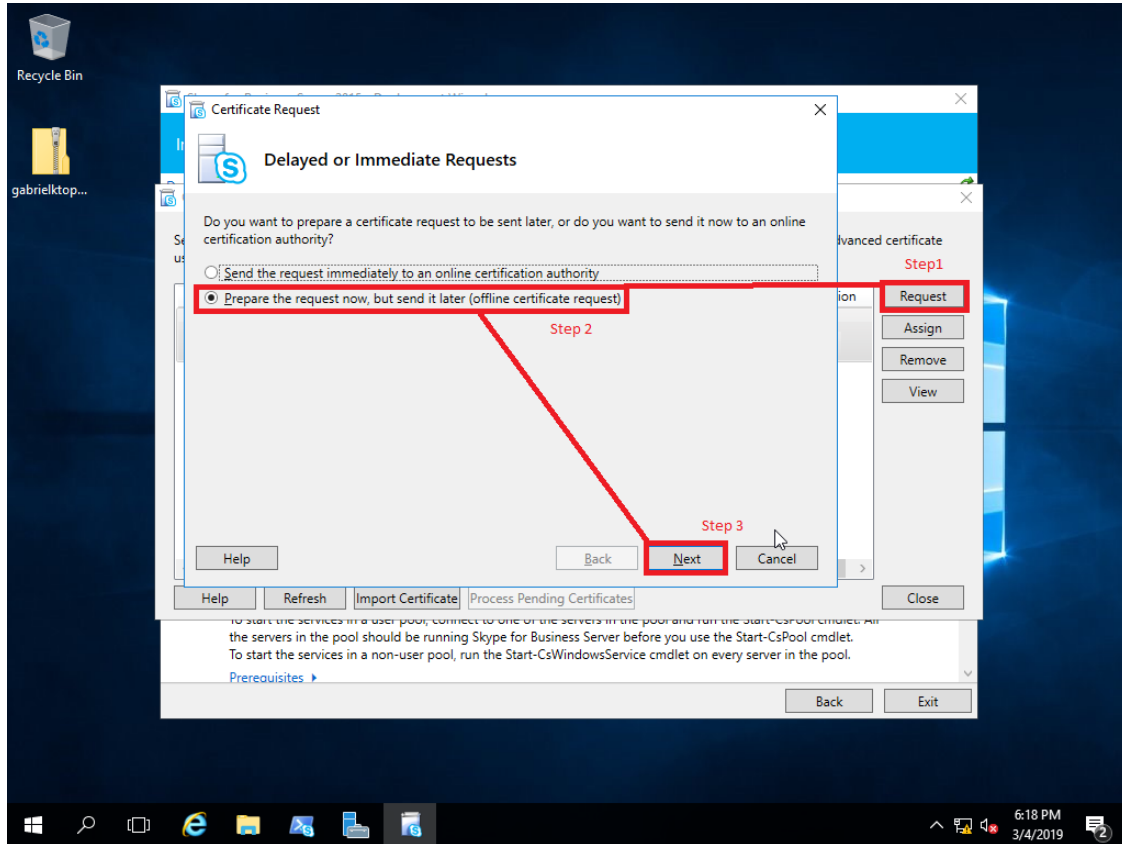


Figure 19: Offline Certificate Request instead of directly contacting CA. The rest of the steps are the same with the exception of specifying a request file that can be sent to the CA to be manually request. See the following figure to see how. Do this for both external and internal certificates.

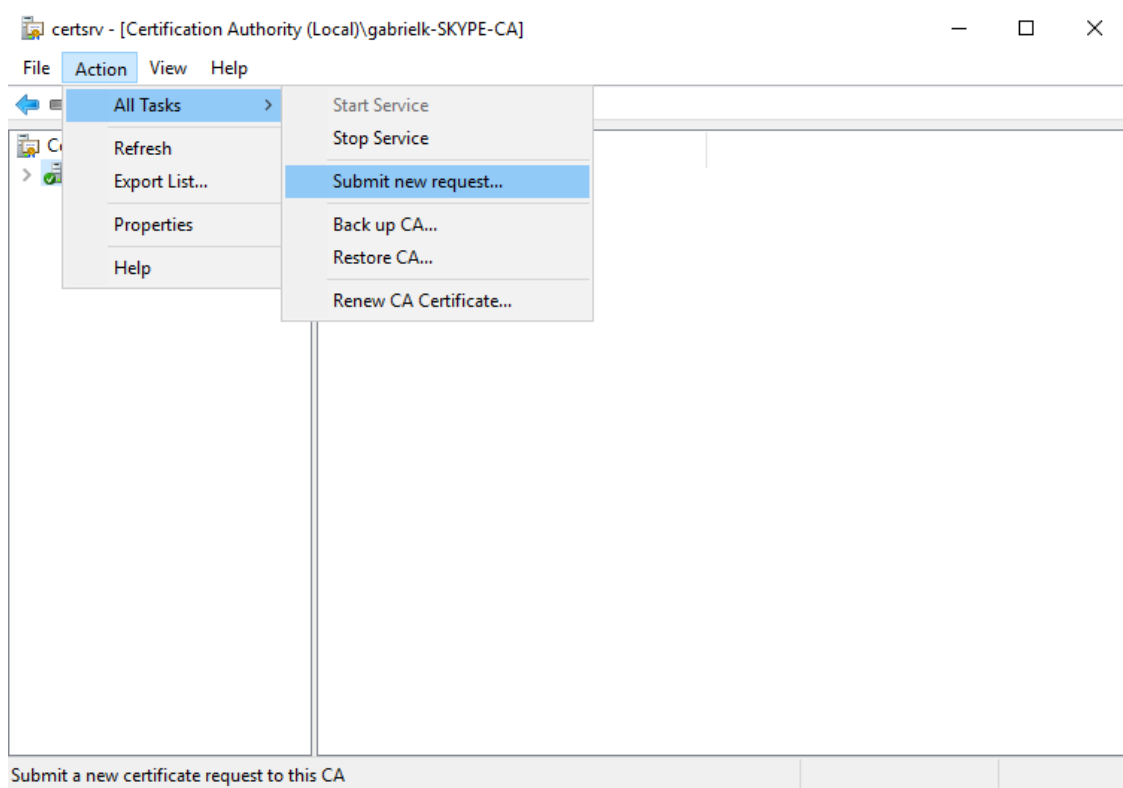


Figure 20: Initiate requests for certificates in the certsrv.msc as seen above. Upon doing so, specify the cert request created in the previous figure. Place the new certificates in a network store accessible by your edge server. Run those certificates and install them into the local machine.

4. Starting Services

Starting Servers is simple see the following figures to enable and verify services running

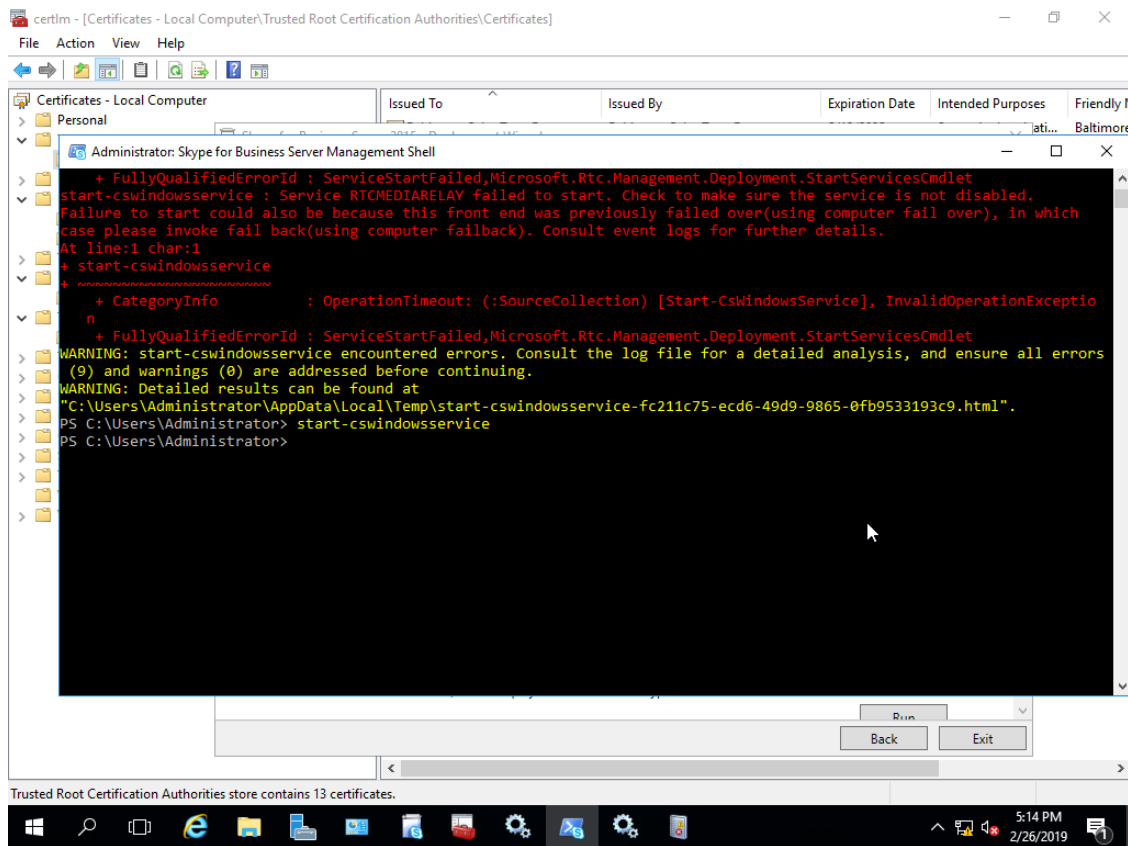


Figure 21: Use the `start-cswindowsservice` in the SfB management shell to initiate startup of services

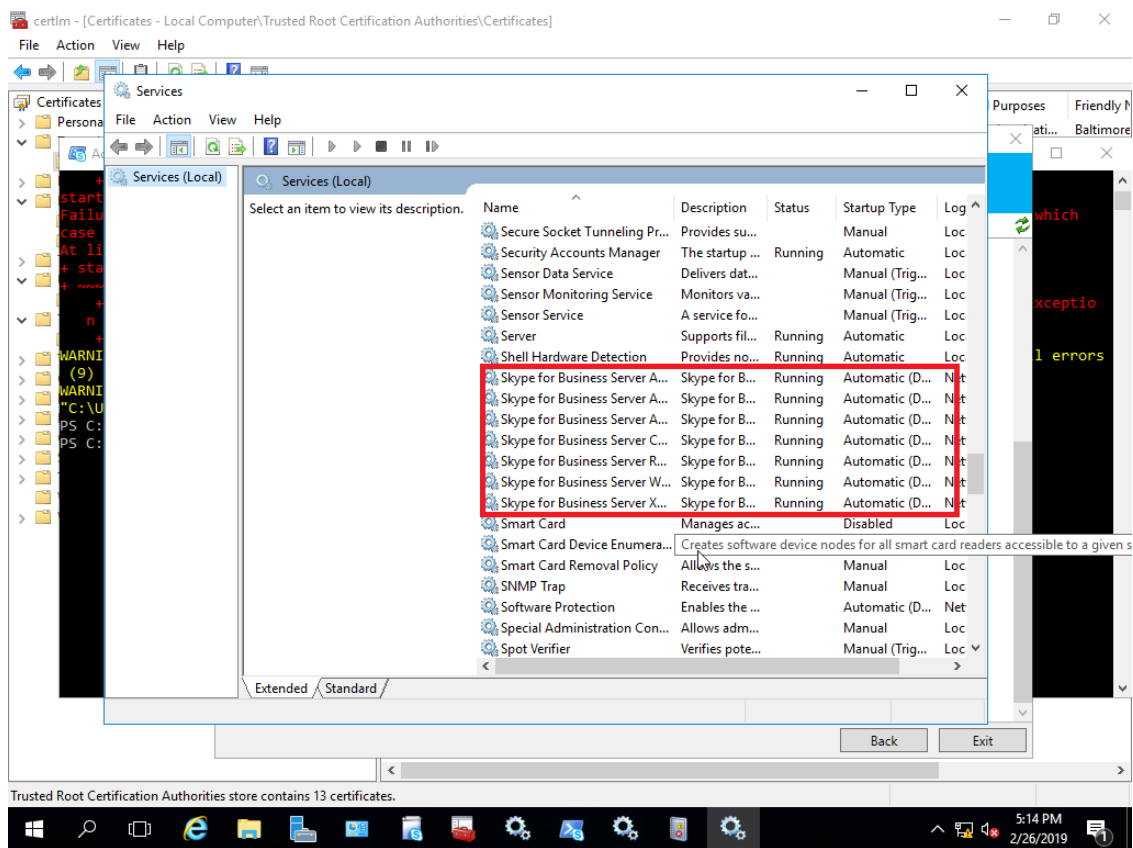


Figure 22: To verify, you can open services.msc and ensure the services are running

5 Other Configuration

Additional DNS records will need to be created. This includes the Internal Edge FQDN specified in the topology. That being `edge.gabrielk.local`. The external clients will require their own DNS records. Further research is required.