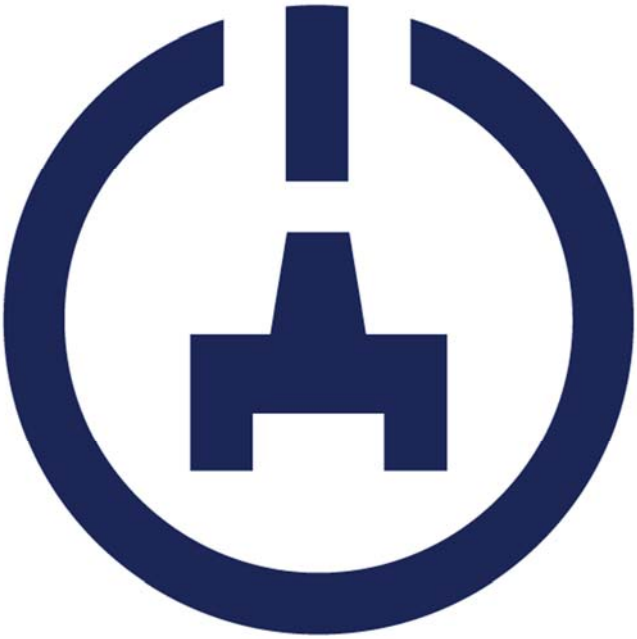

NETSCENARIO

Third Party Access

Instructions & Guidelines

Date	Version	Name	Description
2014-08-04	0.1	Lester Clayton	Initial Release
2014-08-04	0.2	Lester Clayton	Included Mac instructions
2014-08-25	0.3	Lester Clayton	Added additional information for SQL
2015-10-01	0.4	Andreas Solheim	Added instructions for Cisco Anyconnect

1 INTRODUCTION

1.1 PURPOSE OF DOCUMENT/SCOPE

This document is written to be provided to 3rd party consultants who need access into our environment for supporting our shared customers.

1.2 AUDIENCE

This document is intended only for authorised 3rd party consultants.

1.3 CONTACT INFORMATION

1.3.1 NETWORK SCENARIO SUPPORT

E-mail: support@netscenario.no
Telephone: +47 455 00 455

Support Hours Monday to Friday 07h00 to 17h00 Central Europe

1.4 REQUESTING ADDITIONAL ACCESS

Should a colleague of yours require access, please make your request to Network Scenario Support, who will process your request. Additional verification or authorization may be required from the customer. Please do not share your user account, as all auditing that we do will be tracked by user name.

1.5 LATEST VERSION OF THIS DOCUMENT

The latest version of this document is available at http://www.nsasp.net/3rdPartyGuidelines.pdf

2 General Guidelines

2.1 Your User Account

- **Your user account is personal to you**. Should some of your colleagues also require access, then additional accounts can be created.
- Your password is set never to expire. Please be careful with your passwords, and if you feel that they have been compromised, please inform us immediately.

2.2 Application Service Accounts

- **Never use your own user account as a service account**. Your user account is there to grant you access to the system, and to allow you to do administration. Never use your user account to run a service. Application Service accounts can be requested via the Support Desk

3 GENERAL INFORMATION

3.1 VIRTUAL ENVIRONMENT

- At Network Scenario we run a highly redundant infrastructure providing a solid virtual infrastructure environment using both Microsoft and VMware virtualization technology. Our current standards are Windows 2012 Windows 2012 R2, and ESXi 5.5
- By default, all new virtual machines created are created with Dynamic Memory. As such, you may see some unusual readings on servers – for example, some servers will say that they have less memory than you think they should have – and other servers will say that they have a lot less free memory than you think they should have. This is normal behaviour of the virtualization layer, and should not be confused as a memory issue.

3.2 DATA DISK

- Some applications store a large amount of data – for these applications, a separate data disk should be requested. Data disks are either mounted as C:\Data or C:\Apps, depending on the software using it. This is done using a feature known as JUNCTIONS.
- The Data disk can be mounted as a different drive letter if requested (e.g. the product "Visma" may have a drive mapped as C:\Visma, which will hold the application data as well as the application itself).

3.3 DFS

- We implement DFS as standard for all of our customers. If you are implementing an application which users need to have a drive mapped to, please make the request to have the drive mapped via our service desk, and via the DFS rather than manually mapping the drive for the users.

3.4 SQL

- Our default SQL Authentication method is Pass-through. If you require mixed mode authentication, please request it, and this can be turned on for you.
- We create by default, a backup plan which does the following backups:
    - Full back up at 00:01 every Sunday
    - Differential Back up at 00:01 every other day
    - Transaction Log Backup Each Day every 2 hours

  Should you feel that an additional back up is necessary, or need to do an ad-hoc back up, please ensure you do a COPY ONLY backup, otherwise your backups may interfere with ours.

4 CONNECTING TO NETWORK SCENARIO

Our preferred method of access to any servers within Network Scenario (or even, servers at our customers' sites) is through our Remote Desktop Gateway. You will need RDP client 6.1 or newer to support the Remote Desktop Gateway.

4.1 RDP GATEWAY (CONSOLE)

In some cases we will provide a MMC console complete with snap-ins and Remote Desktop connections already provided. If this is the case, then you will also have been given an .RDP file. Just double-click this file, and log in with the credentials you have been provided.

4.2 RDP GATEWAY (MANUAL)

When an .RDP file has not been provided (i.e. you just need basic access), then please follow these steps:

4.2.1 CONNECTING FROM PC

- Run MSTSC.EXE, and then click "Show Options" to bring up the advanced dialog.
- In the "Computer" field, enter in the server name that you are trying to get to – **not the gateway address** - and user name provided by Network Scenario, as per the screenshot:

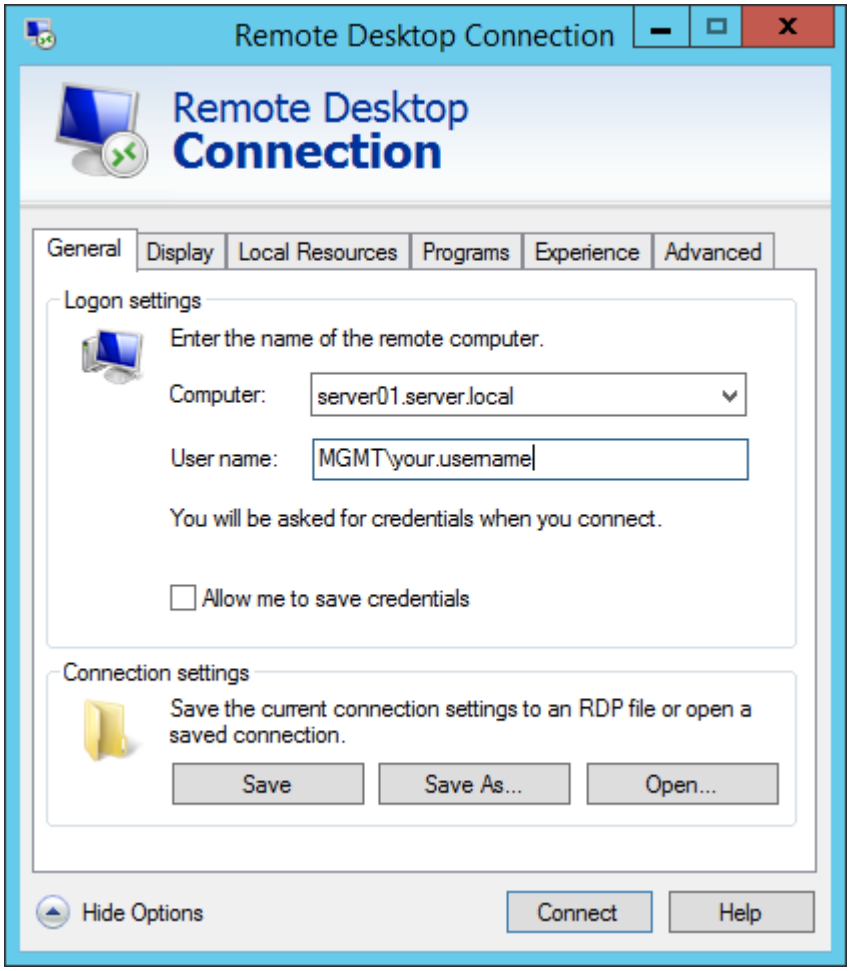

Figure 1 - General Screen

- Select the “Advanced” tab, then click “Settings” under the “Connect from anywhere”. NOTE: If this is not available, then the RDP Client you are using is too old (e.g. Windows XP only has RDP Client 6.0 by default).

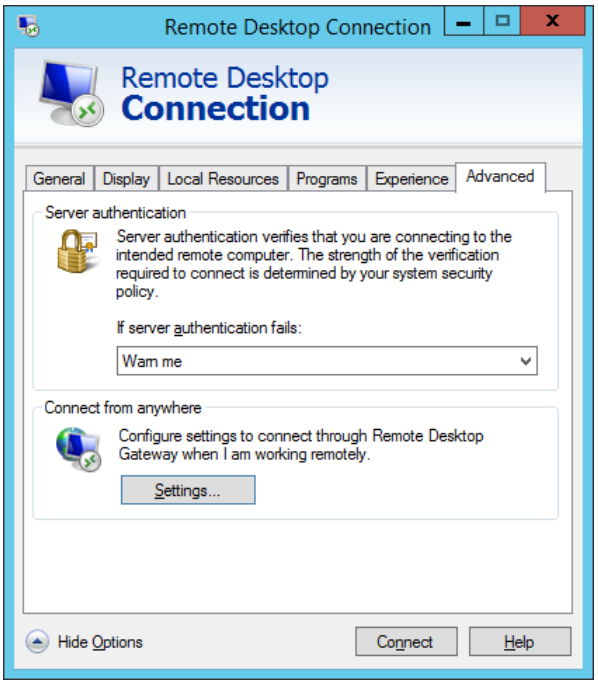

Figure 2 - Advanced

- Use “rdp.nsasp.net” as the Server name. To avoid logging on twice, check the box “Use my RD Gateway credentials for the remote computer”

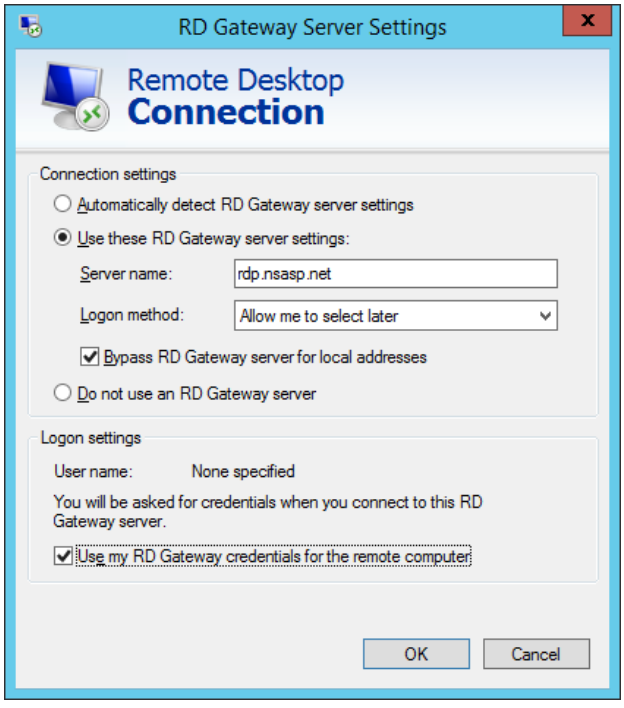

Figure 3 - RDP Gateway Server Settings

- It is recommended to save this information so that you can just double-click an .RDP file in future. Use the “Save As” to save the connection information to an .RDP file. It is safe to specify “Allow me to save credentials” as these go into your own credentials file for your user account.

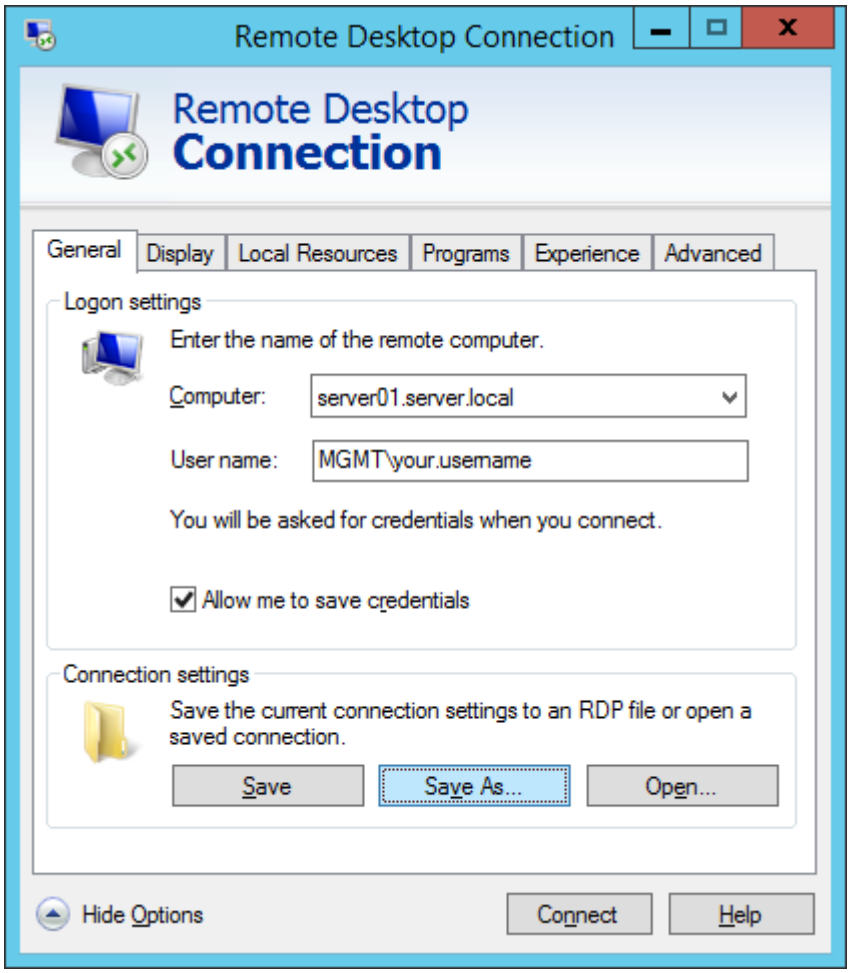

Figure 4 - Save As

- When you are ready, click “Connect” to connect to the server.
- You may receive a security warning similar to the following. This is normal, as servers that are not within your own organization are not trusted due to you not having the self-signed or root certificates.

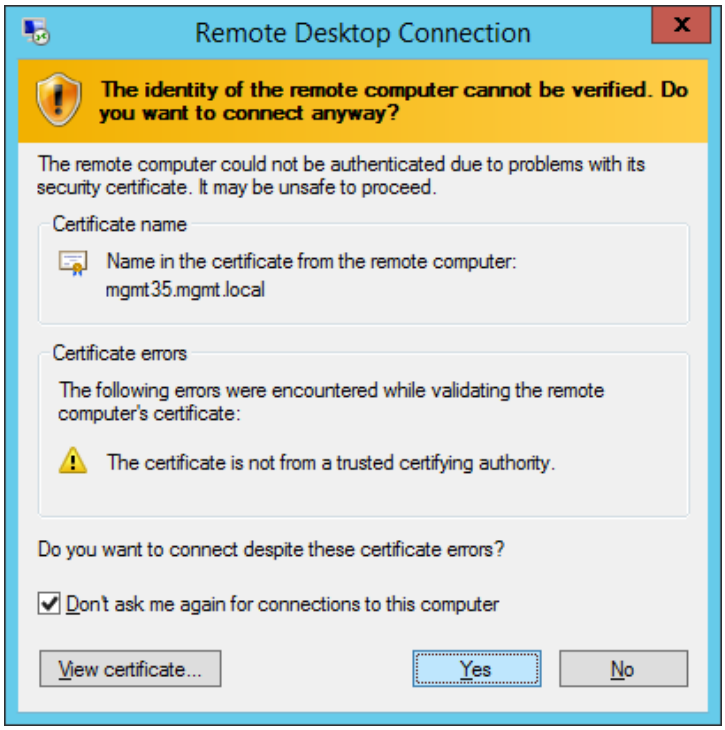

Figure 5 - Identity cannot be verified

4.2.2 CONNECTING FROM A MAC

- If you are running Mac OSX, you can download and install the free Microsoft RDP Client from the App Store.

Figure 6 - Microsoft Remote Desktop

- Once you install this application, you will find it in your Launchpad. Launch the application

Figure 7 - Microsoft Remote Desktop Icon

- If you're running it for the first time, click "Close" to close the announcements.

- Click “New”, and then give your connection a name, enter in the name of the computer you’re connecting to (not the Remote Desktop Gateway) in the PC name field, and enter your User name and password

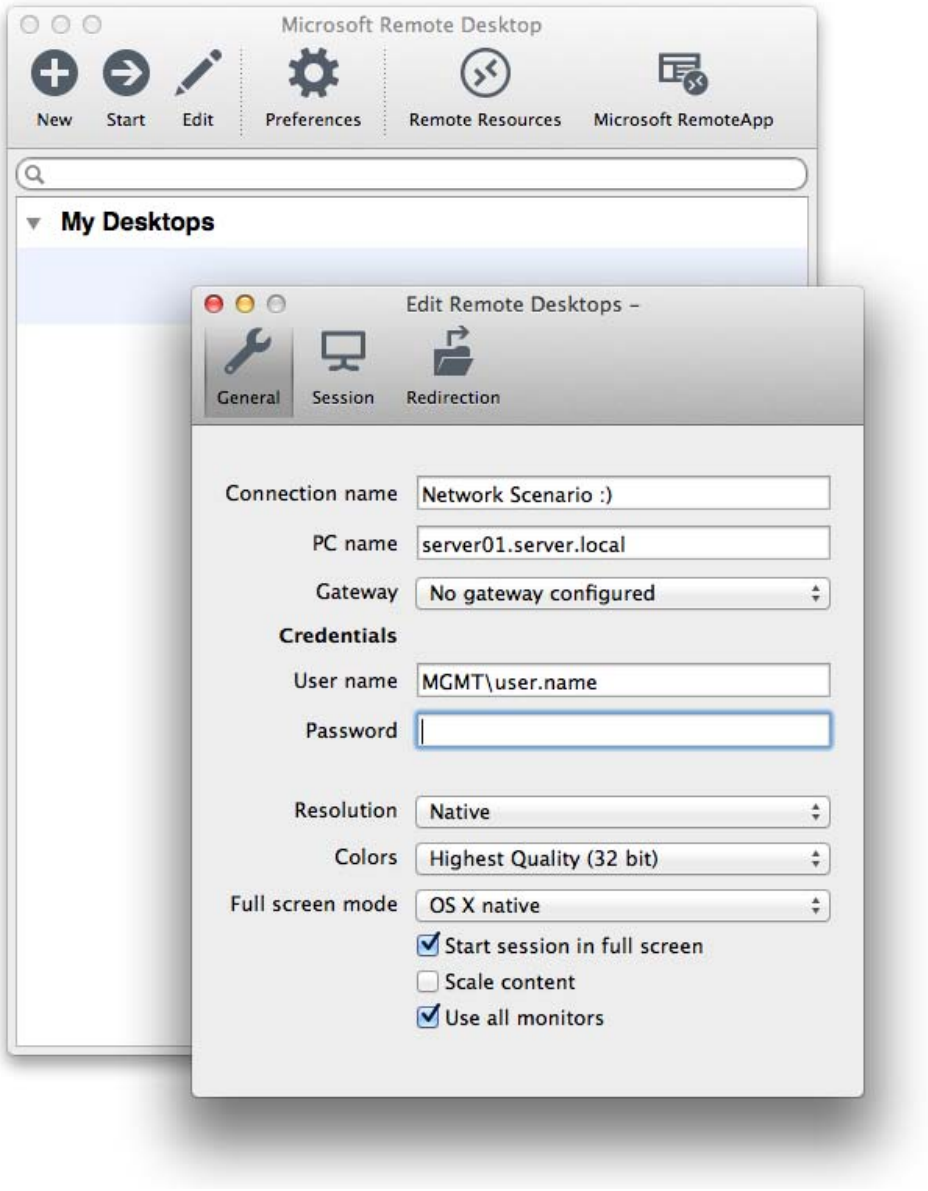

Figure 8 - Edit Remote Desktops

- **Pro Tip – the backslash (\) is not on a standard Mac Keyboard. To get the backslash, use alt-shift-7**
- Use the selection item at the far right of Gateway to select “Add gateway”

Figure 9 - Add gateway

- Click the plus symbol at the bottom left, and then give the gateway a friendly name, specify rdp.nsasp.net as the Server, and enter in your User name and password again

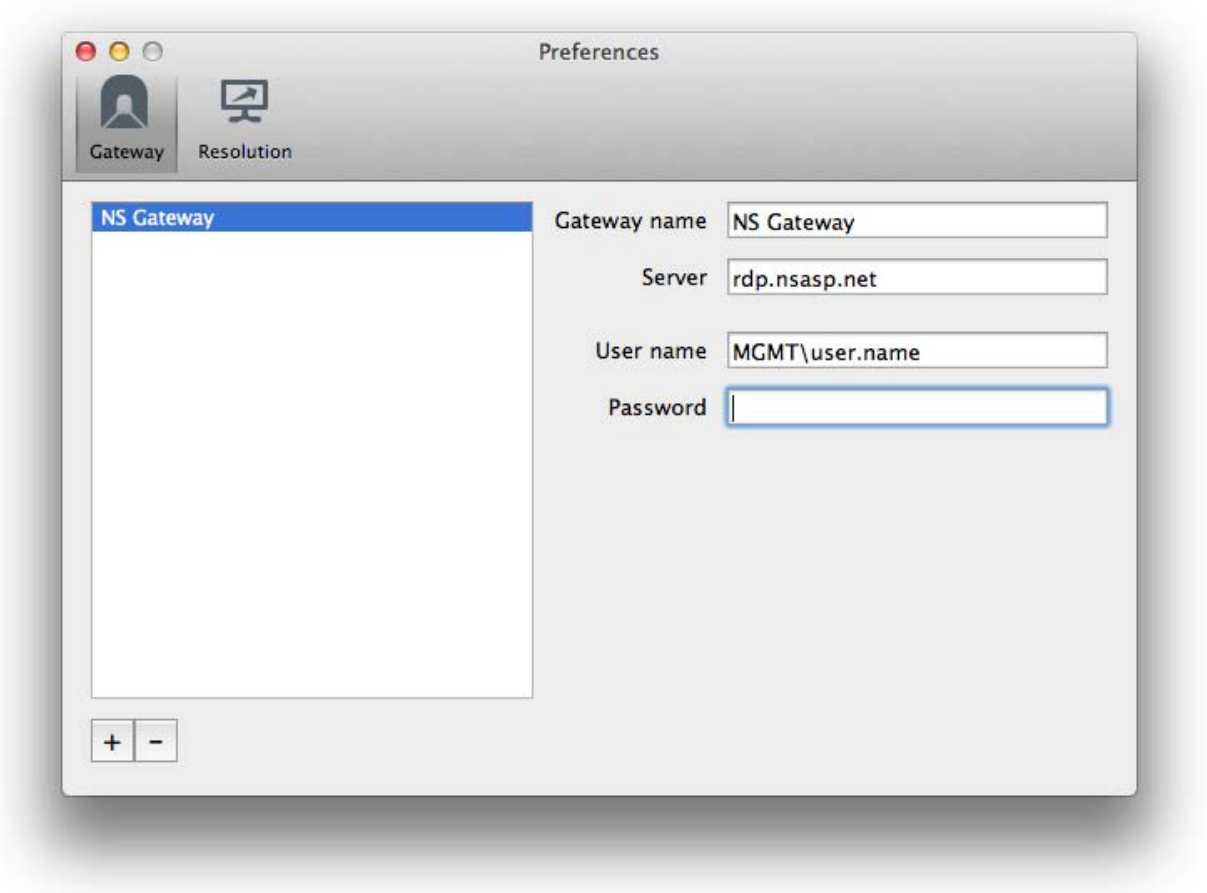

Figure 10 - Gateway Preferences

- Once you've added the gateway once, you can select it for other NS server connections you create in future.
- Close this Preferences window by clicking the red X in the top left, and return to your Edit Remote Desktops
- Use the Gateway drop down to select the gateway you just created

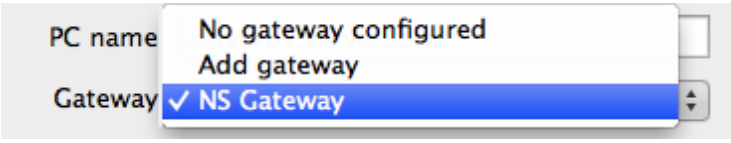

Figure 11 - Select Gateway

- Close this Edit Remote Desktops window by clicking the red X in the top left, and return to the main Microsoft Remote Desktop application

- Use the drop down next to “My Desktops” to show your newly created RDP Configuration

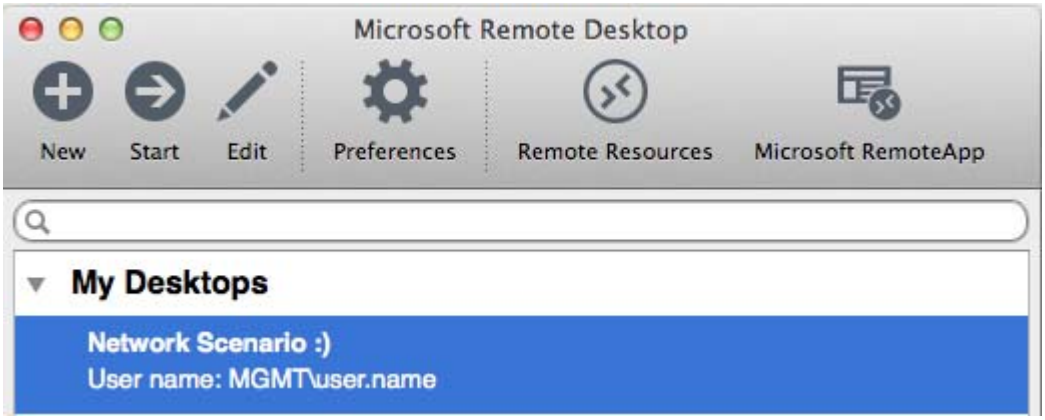

Figure 12 - Microsoft Remote Desktop

- Select the configuration, and click “Start”
- You may receive a messages similar to this below. This is normal – just click “Continue” to continue signing in.

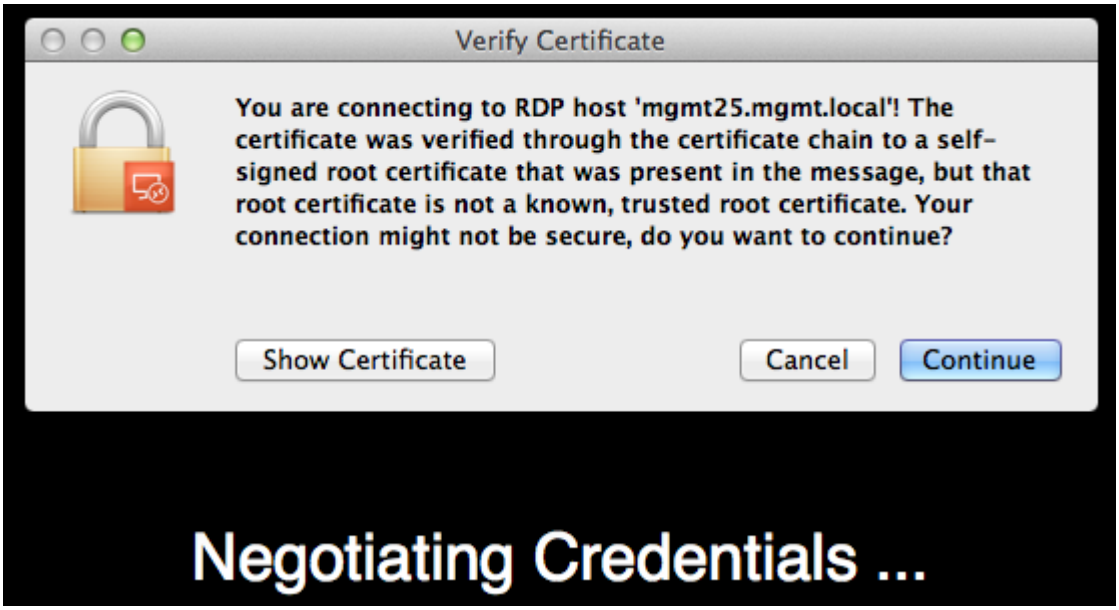

Figure 13 - Verify Certificate

4.3 VPN

Depending on your needs, VPN access may be granted – but only when RDP access is unfeasible. VPN is provided either as a site-to-site solution, or a remote access solution. In either case, a formal request needs to be made to the Support department by our mutual customer, who may be charged for the implementation of the VPN access.

With a VPN, you do not need to specify the RDP gateway when connecting to the target server, provided the target server is permitted through the VPN connection.

4.3.1 SITE-TO-SITE VPN

A site-to-site VPN requires no additional information, as the network should be already reachable. If you are having issues with the site-to-site VPN, please contact our support.

4.3.2 REMOTE ACCESS VPN (USING ANYCONNECT)

If a Remote Access VPN have been granted, the customer is provided with a direct link, for example: https://vpn.nsasp.net/Customer. Open this URL in a webbrowser.

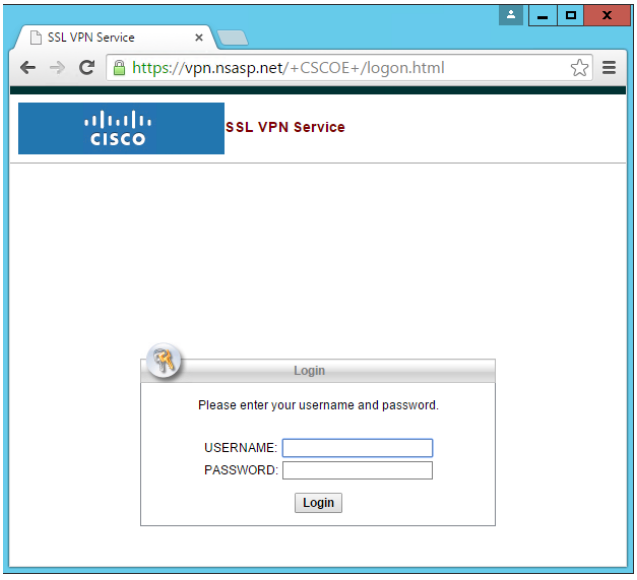

Figure 14 – Anyconnect login

Provide your received credentials and press “Login”. The Anyconnect installation will start automatically and Anyconnect will activate your Remote access VPN

Figure 15 – Anyconnect installation

If, for any reason (security, version conflict etc.) the automatic installation fails, press the manual installation link (Windows Desktop in the following figure) and execute the downloaded file

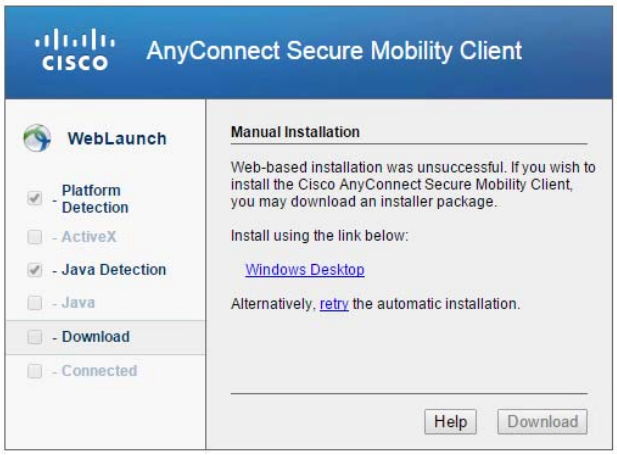

Figure 16 – Automatic installation fail

After the installation has finished, start “Anyconnect” from your start menu

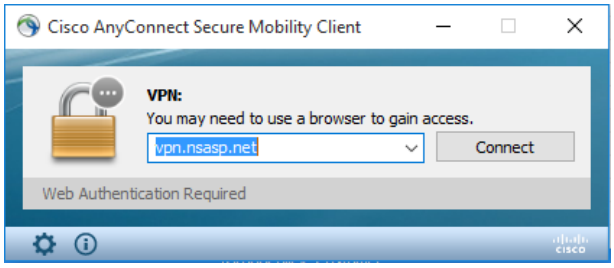

Figure 17 – Anyconnect Connect

If not there already, input “vpn.nsasp.net” and press “Connect”

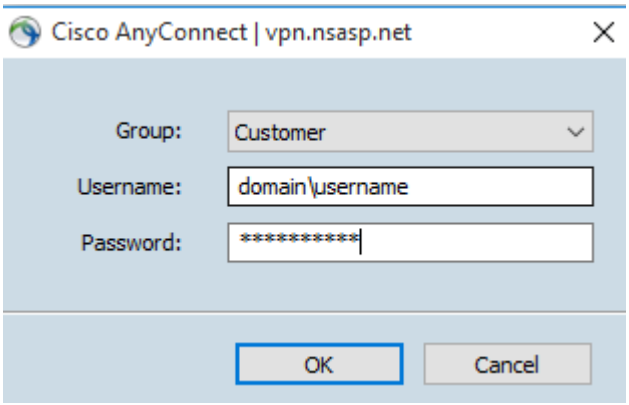

Figure 18 – Anyconnect login

Provide your credentials and press “OK”, Anyconnect will activate you Remote access VPN.

To connect to the Remote Access VPN at a later state, there is no need to go through the website. Open Anyconnect and log in as explained here.