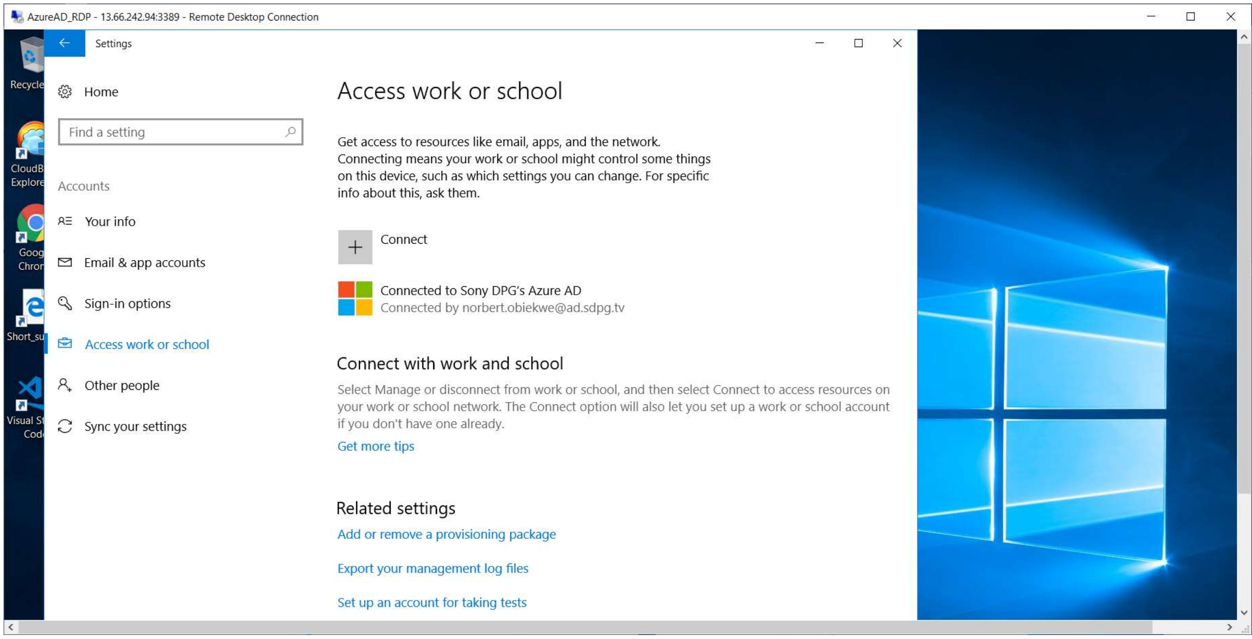
RDP to an Azure AD joined Windows 10 device

- **This is a sample how to guide I produced during the project time back in 2019. The audience is for stakeholder experts.***

Steps:

First is to join the windows 10 to AzureAD

- In the VM windows 10, join AzureAD using All Settings, Accounts, **Access work or school**, click on **Connect** and enter your AzureAD username, then click on **Join this device to Azure Active Directory** and continue through the wizard.



AzureAD_RDP - 13.66.242.94:3389 - Remote Desktop Connection

Settings

Home

Find a setting

Accounts

Your info

Email & app accounts

Sign-in options

Access work or school

Other people

Sync your settings

Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Connect

Connected to Sony DPG's Azure AD
Connected by norbert.obiekwe@ad.sdpg.tv

Connect with work and school

Select Manage or disconnect from work or school, and then select Connect to access resources on your work or school network. The Connect option will also let you set up a work or school account if you don't have one already.

Get more tips

Related settings

Add or remove a provisioning package

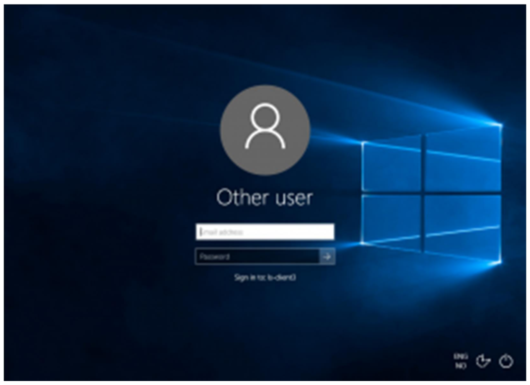
Export your management log files

Set up an account for taking tests

-

- You can verify that your device has successfully joined AzureAD via a PowerShell command: **dsregcmd /status**

The key to connecting/rdp to windows azure joined machine is having Windows 10 present an desktop login screen:

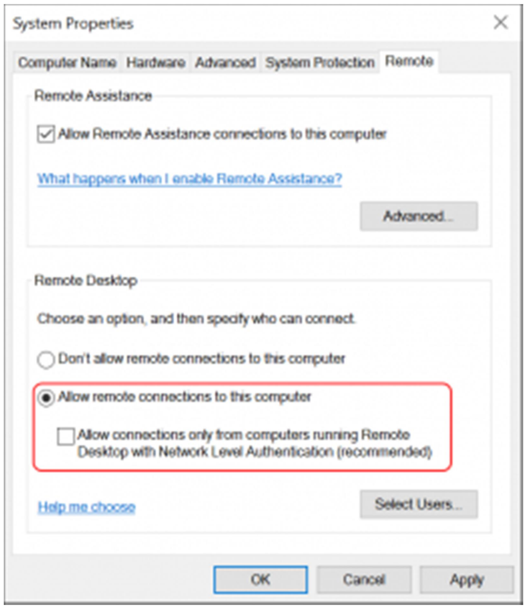


That means that we must disable any form of single sign-on or integrated authentication. This requires the following steps:

On the Windows 10 computer;

Step 1. Change Remote desktop settings

- disable Network Level Authentication (NLA) for Remote Desktop Connections Open **System Properties** and navigate to the **Remote** tab.
- Under Remote Desktop; make sure **Allow remote connections to this computer** is enabled, and that ,
- **Allow connections only from computers running Remote Desktop with Network Level Authentication** is unchecked.



☑ Allow Remote Assistance connections to this computer

Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

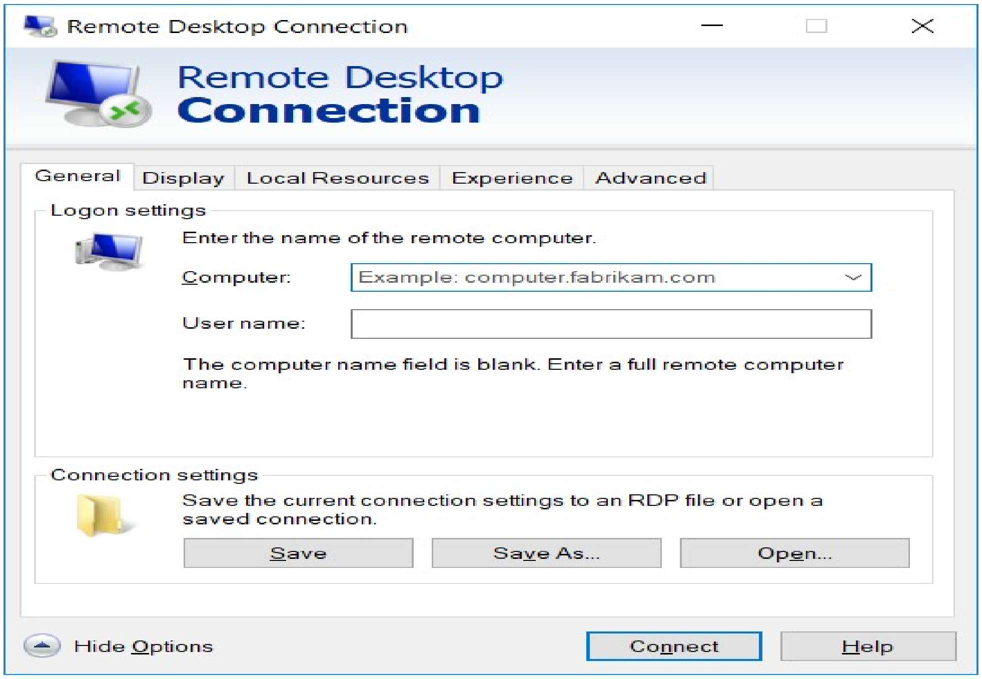
□ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

-
-

This will disable the ability on the host to require that authentication happens before a user session is created.

Step 2. Create new rdp config file

On the computer you intend to RDP from, open mstsc.exe and click on Show Options.



Enter the name of the remote computer.

Computer: Example: computer.fabrikam.com

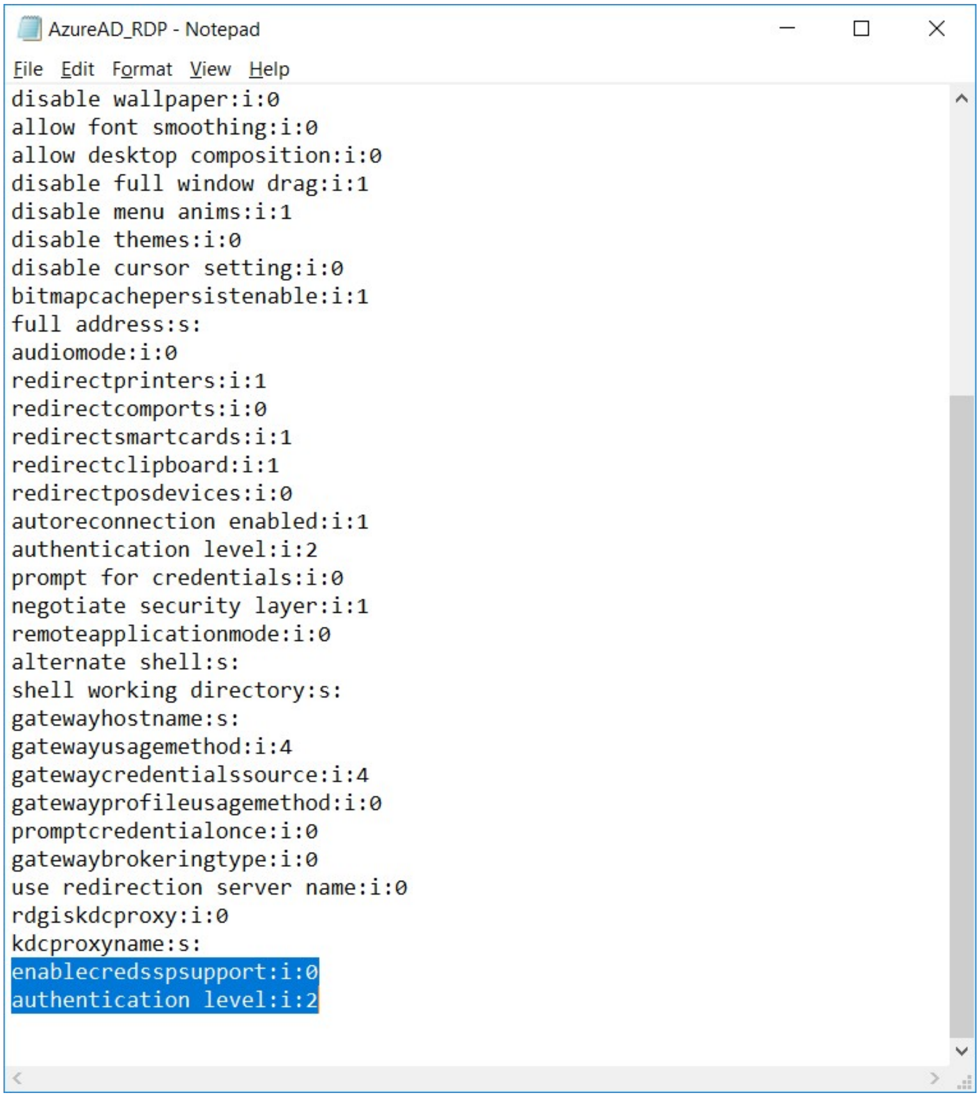
User name:

The computer name field is blank. Enter a full remote computer name.

Save the current connection settings to an RDP file or open a saved connection.

Click on **Save As**… and give it a new name such as **AzureAD_RDP**, save it somewhere easy to find.
Open the saved file using Notepad. Verify that the following two lines are present, if not, add them.

```
enablecredsspsupport:i:0
authentication level:i:2
```



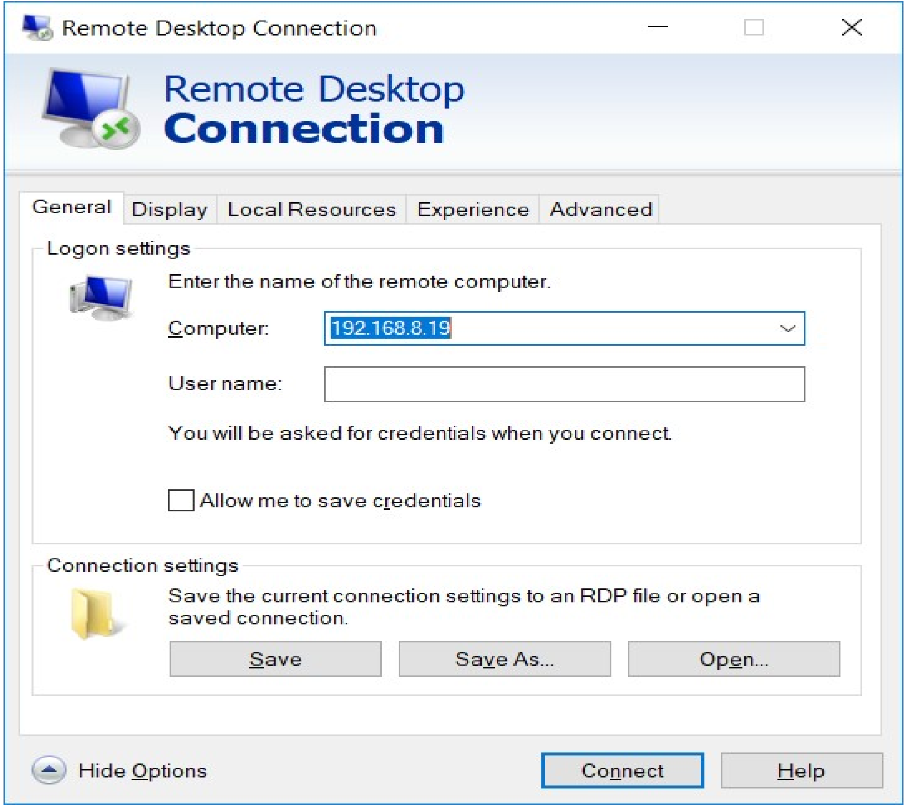
```
disable wallpaper:i:0
allow font smoothing:i:0
allow desktop composition:i:0
disable full window drag:i:1
disable menu anims:i:1
disable themes:i:0
disable cursor setting:i:0
bitmapcachepersistenable:i:1
full address:s:
audiomode:i:0
redirectprinters:i:1
redirectcomports:i:0
redirectsmartcards:i:1
redirectclipboard:i:1
redirectposdevices:i:0
autoreconnection enabled:i:1
authentication level:i:2
prompt for credentials:i:0
negotiate security layer:i:1
remoteapplicationmode:i:0
alternate shell:s:
shell working directory:s:
gatewayhostname:s:
gatewayusagemethod:i:4
gatewaycredentialssource:i:4
gatewayprofileusagemethod:i:0
promptcredentialonce:i:0
gatewaybrokeringtype:i:0
use redirection server name:i:0
rdgiskdcproxy:i:0
kdcproxyname:s:
enablecredsspsupport:i:0
authentication level:i:2
```

Save the file.

Step 3.

RDP to the target computer

On the computer that you just edited the config file, open MSTSC.exe and click on show options, then click on **Open**. Point it to the previously created AzureAD_RDP config file. Enter the IP address or FQDN of the computer you want to RDP to, do not enter any username.



Remote Desktop Connection

Remote Desktop **Connection**

Logon settings

Enter the name of the remote computer.

Computer: 192.168.8.19

User name:

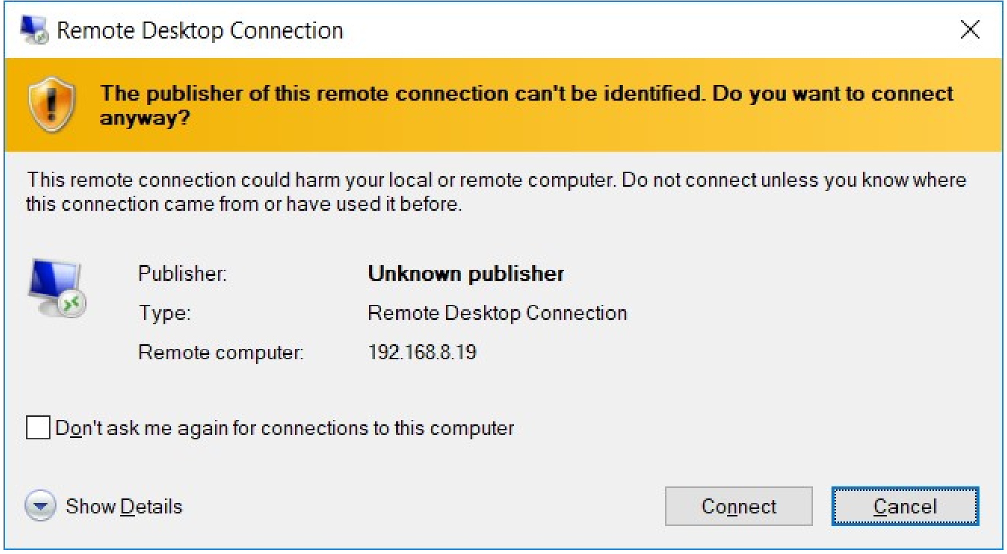
You will be asked for credentials when you connect.

□ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

you may see the usual RDP prompt…it's ok, click on Connect



Remote Desktop Connection

The publisher of this remote connection can't be identified. Do you want to connect anyway?

This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before.

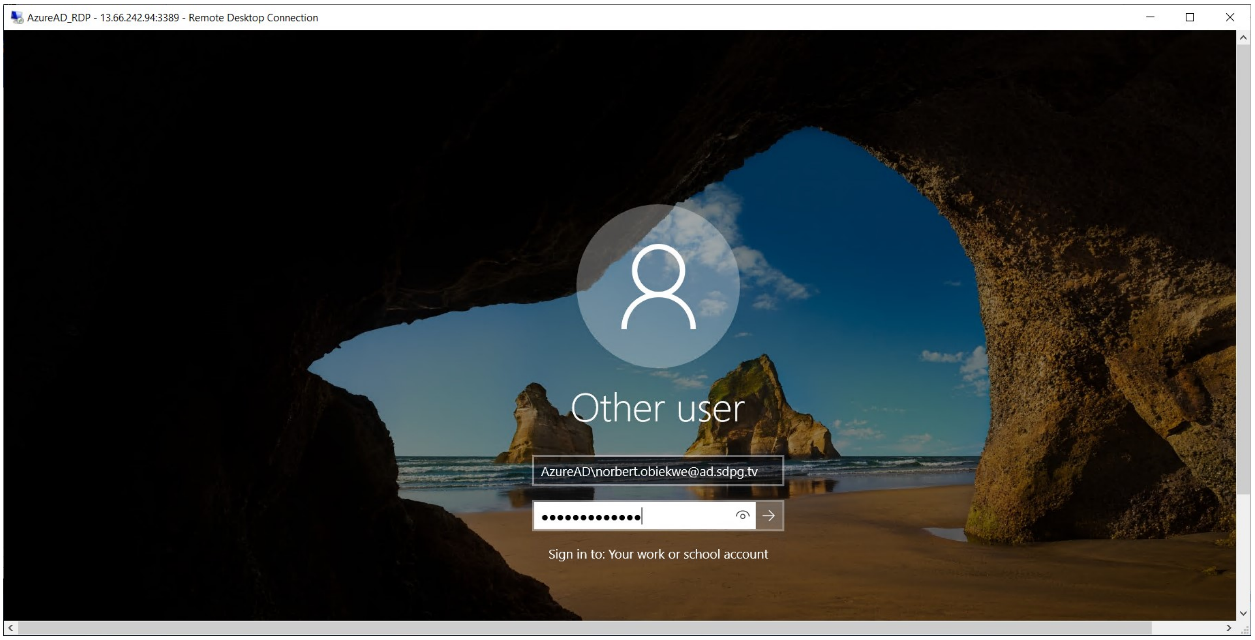
Publisher: **Unknown publisher**

Type: Remote Desktop Connection

Remote computer: 192.168.8.19

□ Don't ask me again for connections to this computer and depending on what device you are connecting from (and to) you’ll see different results, for example from an AzureAD joined device that you’ve logged into with the same UPN as you are using to connect to the target PC you’ll be prompted to enter your AzureAD password .

If however you are connecting from say, a Workgroup joined (non azure AD joined) device then the login experience will be different, and you’ll see a login page like this, enter your username as:



AzureAD_RDP - 13.66.242.94:3389 - Remote Desktop Connection

Other user

AzureAD\norbert.obiekwe@ad.sdpg.tv

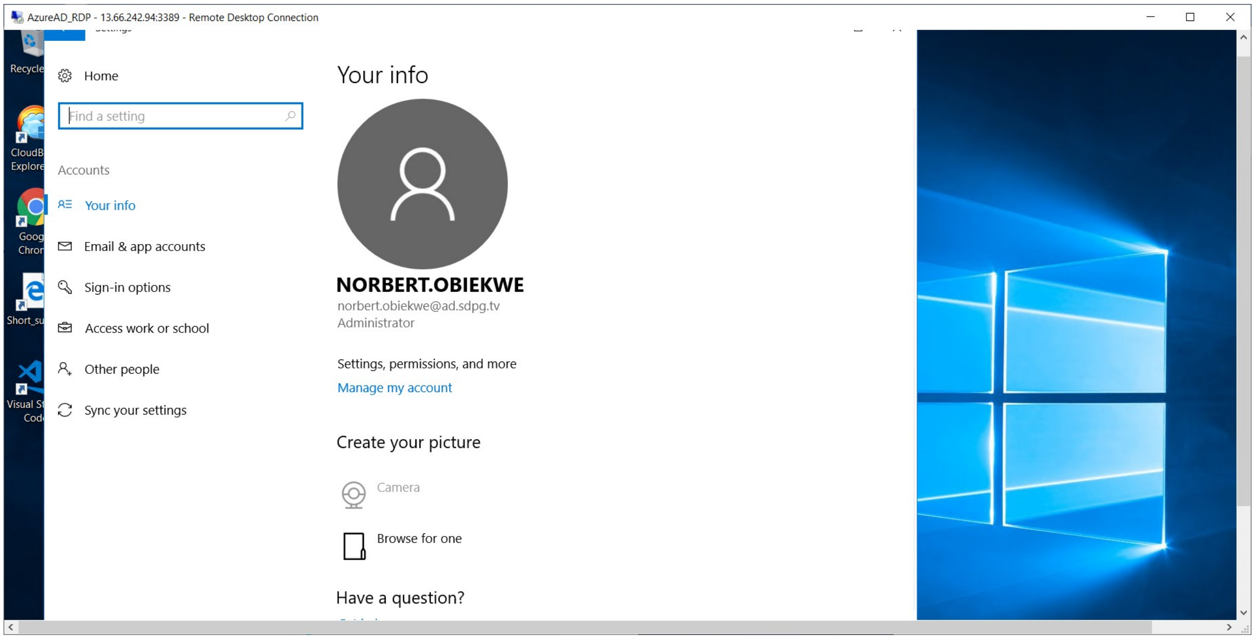
•••••••••••••

Sign in to: Your work or school account

AzureAD\<username@domain.com>
where <username@domain.com> is your the full User Principal Name of your AzureAD user

The last trick to make this work involves the username you specify on the logon screen. It must be in the following format:

AzureAD\<full UPN in Azure AD>
Example: **AzureAD\norbert.obiekwe@ad.sdpg.tv**



AzureAD_RDP - 13.66.242.94:3389 - Remote Desktop Connection

Accounts

- Your info
- Email & app accounts
- Sign-in options
- Access work or school
- Other people
- Sync your settings

Your info

NORBERT.OBIEKWE
norbert.obiekwe@ad.sdpg.tv
Administrator

Settings, permissions, and more
Manage my account

Create your picture

Have a question?