

Document name: IRMCT RSA Token & RDS Remote Access Manual

Version: 1.7

Date: 11-02-2018

Before you begin, please read below:

It is a staff member's own responsibility to make sure his or her personal computer or laptop is fully updated with the latest security patches and updates before accessing the Remote Work Resources (Remote Desktop Services) of the IRMCT. A fully updated computer is a requirement for accessing the Remote Work Resources securely and without problems. In fact, if the computer is not up to date, it might not be able to connect at all to the Remote Work Resources of the IRMCT.

ITSS supports the Remote Work Resources service but does not support personal hardware and in case support is requested, you are required to have a fully updated computer before support staff is able to assist you.

Your PC also needs to support the Microsoft **Remote Desktop Protocol (RDP) version 8.1** or higher. If you do not have RDP version 8.1 or higher installed you will **NOT** be able to connect! **Windows 8.1 and Windows 10 by default have RDP version 8.1 or higher installed. Windows 7 or Windows 8 may have it installed but it's not included by default in the installation.** See Appendix A for how to check for the RDP version.

If you encounter any issues or errors, before requesting any support from ITSS, please first read Appendix A, you may already find an answer there.

Please find below instructions on how to access the Remote Work Resources through RDP:

TZ **Arusha** based staff members access the Remote Work Resources through:

<https://rdtz.unmict.org/rdweb>

NL **The Hague** based staff members access the Remote Work Resources through:

<https://rdnl.unmict.org/rdweb>

You will have to authenticate with your User ID, which is the same as your MICT network account (the account name that you use to logon to your MICT windows PC).

If you haven't set a **PIN** yet, you will use **only** your token code as a Passcode and only the **first** time you logon.

Your Passcode is the token code displayed on your RSA (software or hardware) token.

Always make sure there is minimum of 30 seconds remaining on your software token, or a minimum of 3 bars remaining on your hardware token.

If not, please wait for the token code to change and then enter the token code.



Figure 1: Hardware token

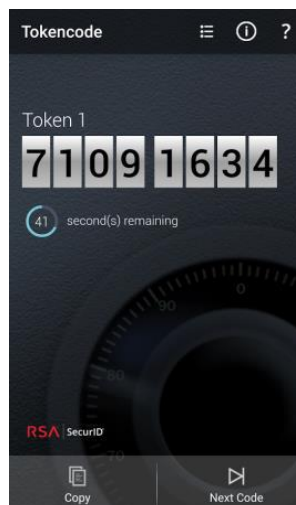
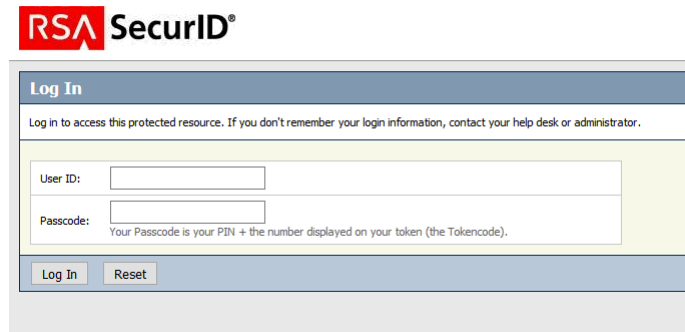


Figure 2: Software token

For example: if the token code on your token is 597482 then you will enter this number in the Passcode field of the logon screen.



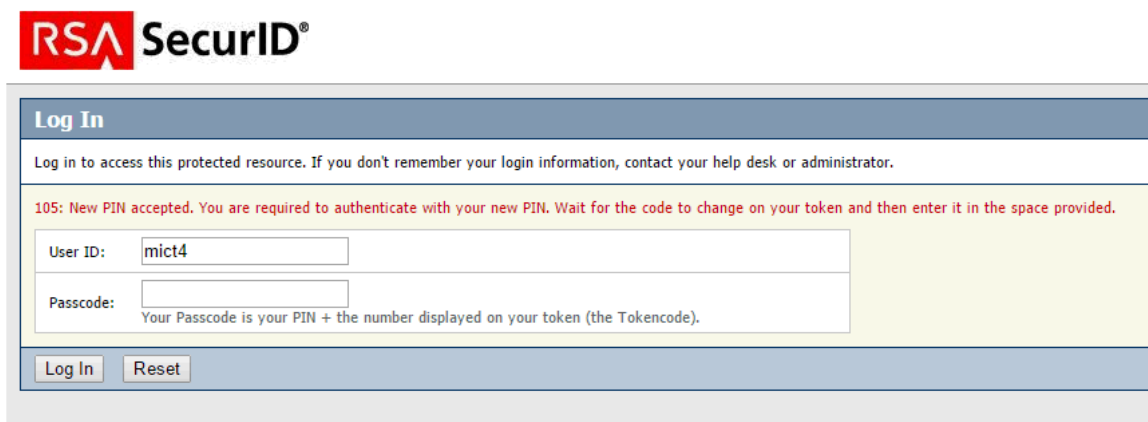
The image shows the RSA SecurID Log In screen. At the top is the RSA SecurID logo. Below it is a blue header with the text "Log In". Underneath is a message: "Log in to access this protected resource. If you don't remember your login information, contact your help desk or administrator." The main area contains two input fields: "User ID:" and "Passcode:". Below the Passcode field is a note: "Your Passcode is your PIN + the number displayed on your token (the Tokencode)." At the bottom are two buttons: "Log In" and "Reset".

After you log in for the very first time you will be required to set a new **PIN**, your PIN must contain 6 to 8 numbers:



The image shows the "New RSA SecurID PIN Required" screen. At the top is the RSA SecurID logo. Below it is a blue header with the text "New RSA SecurID PIN Required". Underneath is a message: "Either you don't have a PIN yet, or security policy requires a PIN change." Below that is a red message: "PINs must contain 6 to 8 numbers." The main area contains two input fields: "New PIN:" and "Confirm New PIN:". At the bottom are three buttons: "OK", "Reset", and "Cancel".

For example, enter 684512 in the New PIN field. Enter your PIN again in the Confirm New PIN field and click **OK**. If your PIN is set successfully, you will see the following screen with message 105: New PIN accepted. You are required to authenticate with your new PIN. Wait for the code to change on your token and then enter it in the space provided.



The image shows the RSA SecurID Log In screen after a successful PIN change. At the top is the RSA SecurID logo. Below it is a blue header with the text "Log In". Underneath is a message: "Log in to access this protected resource. If you don't remember your login information, contact your help desk or administrator." Below that is a red message: "105: New PIN accepted. You are required to authenticate with your new PIN. Wait for the code to change on your token and then enter it in the space provided." The main area contains two input fields: "User ID:" with the value "mict4" and "Passcode:". Below the Passcode field is a note: "Your Passcode is your PIN + the number displayed on your token (the Tokencode)." At the bottom are two buttons: "Log In" and "Reset".

Wait till the token code changes again and then logon using your

User ID (= your MICT network account, the one you use to logon to your MICT Windows PC)

and

your **Passcode** (= your **PIN** followed *directly* by the token code on your RSA token)

For example:

If the token code on your token is 597482 and your PIN is 684512 then your Passcode will be: 684512597482

Click **Log In**. You will now see the MICT The Hague Work Resources log on screen.

Your login name is your MICT network account name preceded by "mict\"

For example, if your MICT account name is mict3 then

Domain\user name is: mict\mict3

and

Password is: your windows network password (the password you use to log on to your MICT windows PC)

MICT The Hague Work Resources
RemoteApp and Desktop Connection

RD Web Access

Help

Domain/user name: mict\username

Password: []

Security ([show explanation](#))

This is a public or shared computer

This is a private computer

Warning: By selecting this option, you confirm that this computer complies with your organization's security policy.

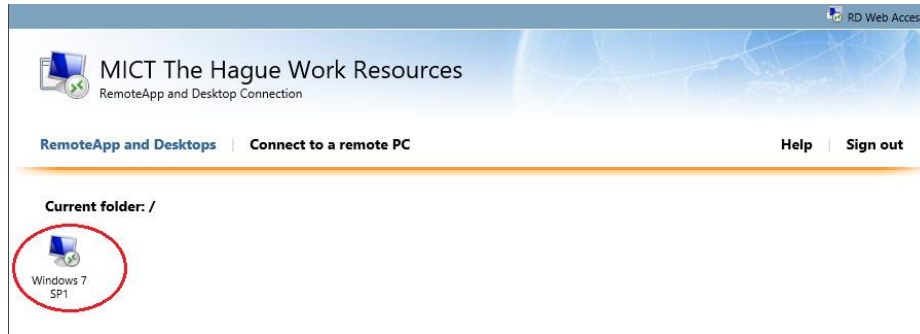
Sign in

To protect against unauthorized access, your RD Web Access session will automatically time out after a period of inactivity. If your session ends, refresh your browser and sign in again.

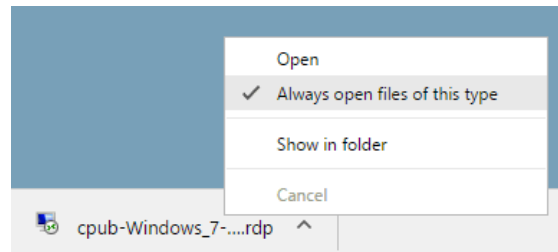
Windows Server 2016 Microsoft

Click **Sign In**.

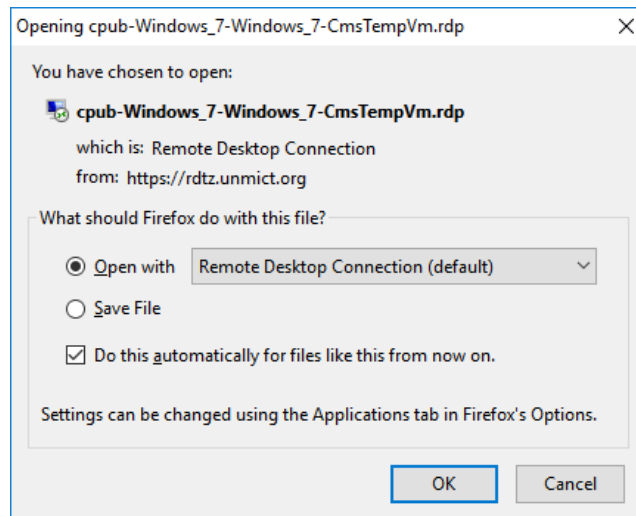
You will now see a link to your Windows 7 Virtual Desktop:



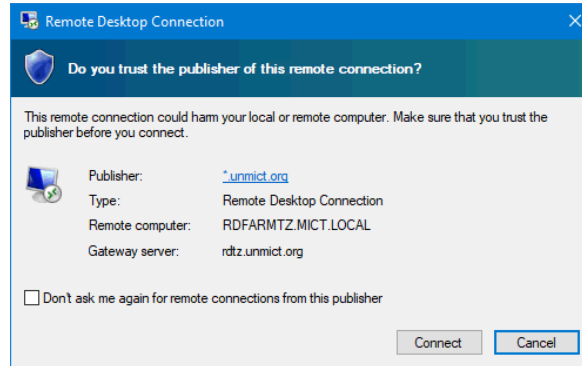
Click on the **Windows 7** icon. When a *.rdp file is downloaded, you can click on it to open the RDP session. In Chrome you can set the defaults for the *.rdp file, just select "Always open files of this type" by right clicking on the downloaded file in the download bar at the bottom of your browser window:



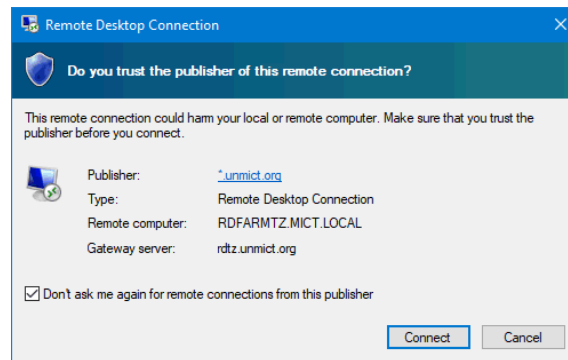
Likewise, in FireFox, when prompted, select Open With "Remote Desktop Connection" and "Do this automatically for files like this from now on".



Next time, when you click on the Windows 7 icon it will launch the RDP session immediately:

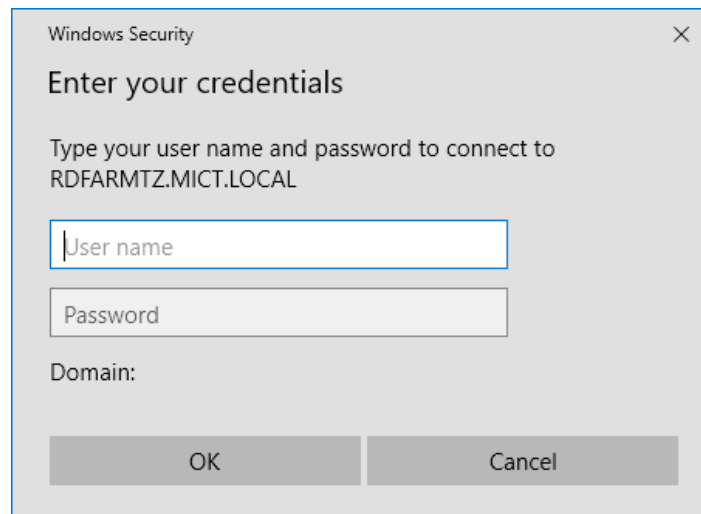


You may tick the box "Don't ask me again for remote connections from this publisher" to prevent this window from showing up the next time you log in:



Click **Connect**.

You will need to enter your credentials again:



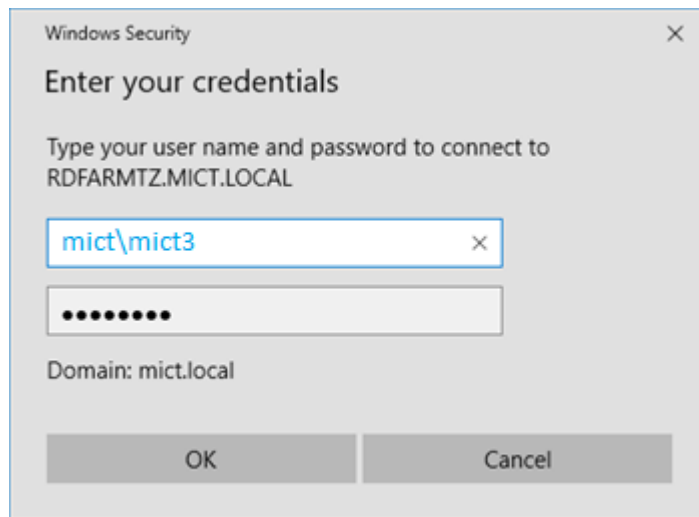
Your username is again your MICT network account name preceded by "mict\"

For example:

If your MICT network account name is **mict3** then your username will be:

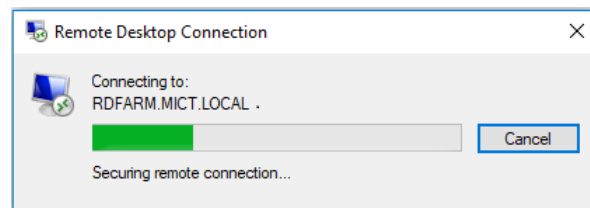
mict\mict3

and your password is: your MICT windows network password (the password you normally use to log on to your MICT windows PC)



Click **OK**.

Remote connection session will be setup:

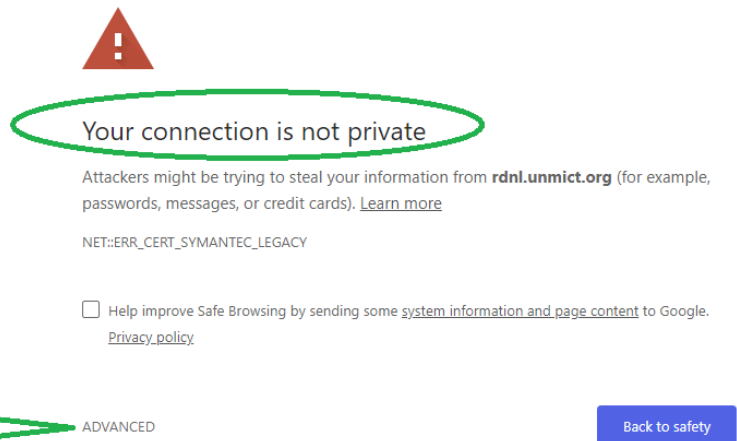
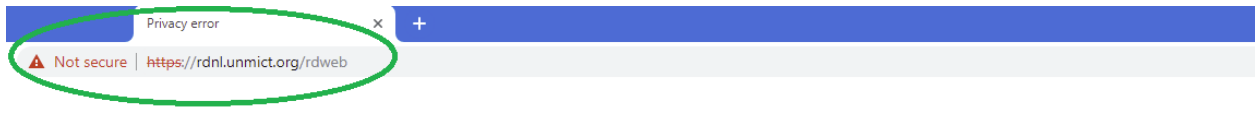


After the connection is secured you will be presented with the Windows 7 logon screen, just click OK to logon.

After you log on you will see the remote Virtual Desktop.

Appendix A - Important notes, known errors and solutions:

1. Some browsers (like Google Chrome) have been updated to display a notification message when connecting to <https://rdtz.unmict.org/rdweb> or to <https://rdtz.unmict.org/rdweb> :



The security certificate of the website is still valid and the website is still secure and you will be able to connect by clicking on the text **“Advanced”** at the bottom. To proceed click on **“Proceed to rdnl.unmict.org (unsafe)”** or **“Proceed to rdtz.unmict.org (unsafe)”** and you will see the login page as described on page 4 of the manual.

HIDE ADVANCED

Back to safety

This server could not prove that it is **rdnl.unmict.org**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

 [Proceed to rdnl.unmict.org \(unsafe\)](https://rdnl.unmict.org)

2. If your operating system is not fully up to date you may encounter the following error message when connecting to the IRMCT Remote Desktop Services:

An Authentication error has occurred. The function requested is not supported. Remote computer: <computername or IP address>. This could be due to CredSSP encryption oracle remediation.

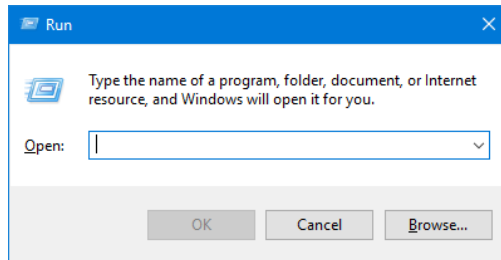
You will not be able to connect! To resolve the issue the following registry key needs to be added to your PC/Laptop:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\CredSSP\Parameters] "AllowEncryptionOracle"=dword:0000002

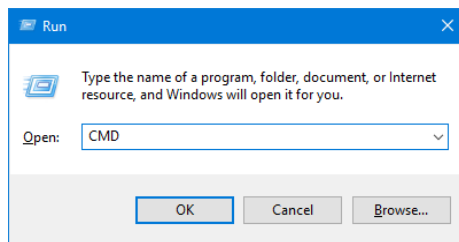
This can be done from the command line. You need to open a Command Prompt window with administrator privileges on your PC.



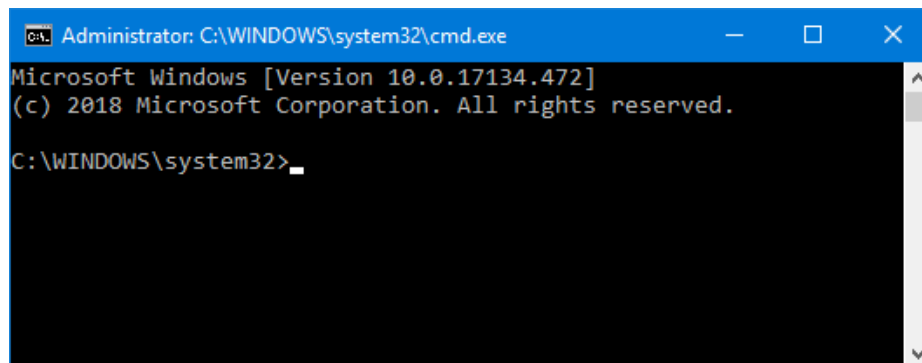
Press the Windows key and the R key simultaneously. This will open the Run box:



Now type CMD in the the text box:



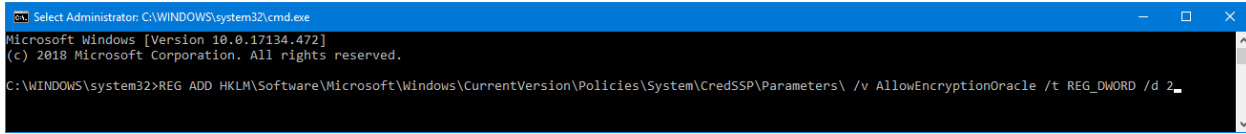
With the Run box open and CMD written in the text field press **ctrl** + **shift** + **enter** simultaneously to launch the Command Prompt as administrator:



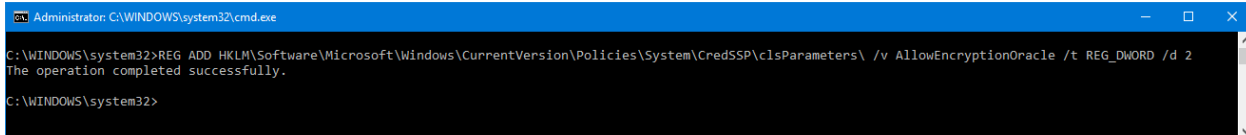
Write the following text below in the Command Prompt window:

```
REG ADD HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\CredSSP\Parameters\ /v AllowEncryptionOracle /t REG_DWORD /d 2
```

as one line like it's shown here:



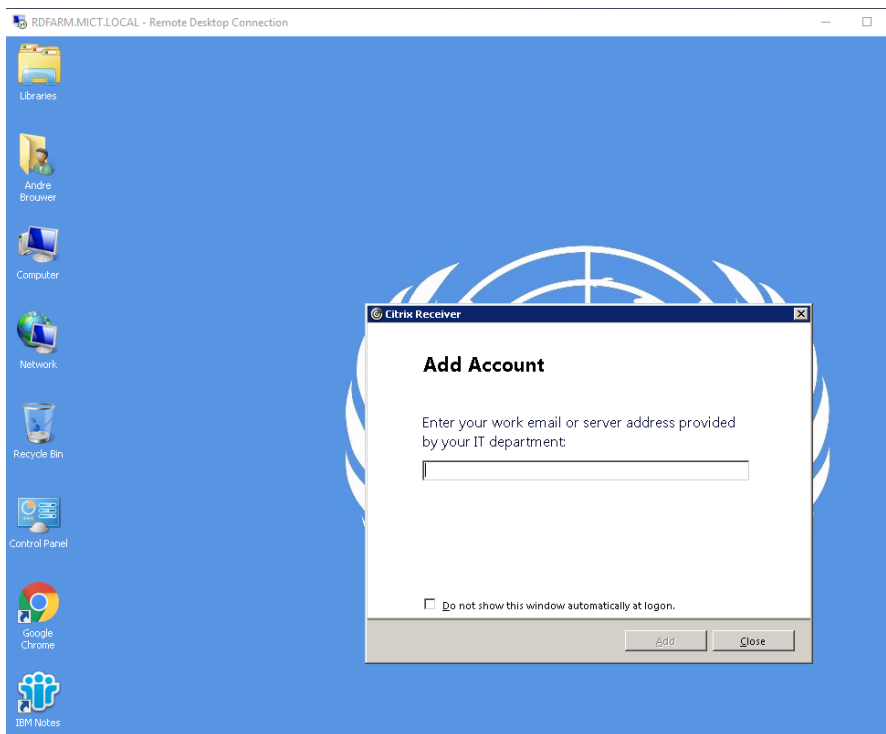
Press Enter:



If the key is entered correctly you will see the text "The operation completed successfully".

Restart your PC and after that try to connect again to the IRMCT Remote Desktop Services.

3. If you get a Citrix Receiver pop-up window like shown above, please tick the box "Do not show this window automatically at logon" and click **Close**. **Note: Do NOT try to add any account in the Citrix Receiver pop up window.**

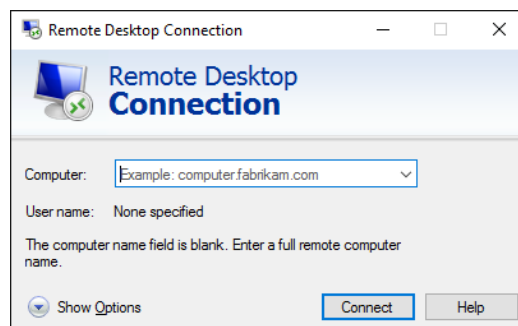


4. The following programs are available in the Virtual Desktop Image (VDI):
Adobe Acrobat Reader / Adobe Flash and Shockwave player / Brava Reader / Citrix Receiver / Webex / Google Chrome / Internet Explorer / Microsoft Access 97 / Microsoft Office 2010 / Microsoft Office Document Imaging / PDF Creator/ Java / Crystal Reports / Ringtail Image Viewer / Visio Viewer. **Other applications have not been added to the VDI due to licensing or technical issues.**
5. Do **NOT** use the local Lotus Notes client installed on your Virtual Desktop. Please use the MICT webmail instead:
<https://webmail.unmict.org>
6. If you forget the PIN for your token and cannot log on anymore, please contact Service Desk to have a work order created to reset your PIN. After your PIN has been reset, please follow the instructions in this document to set a new PIN. **NOTE: Once your PIN has been reset do not reuse a previous PIN; you MUST create a new one (a previously used PIN will NOT be accepted)**
7. Please log off from your Windows virtual desktop when you're done, this will save valuable resources and prevent your account from locking out after a password change.
8. If you have issues at home establishing a remote desktop connection, make sure your PC is up to date with **ALL** the latest available updates and security patches. Make sure your PC supports Microsoft's Remote Desktop Protocol version 8.1 or higher. If your version is 8.0 or less, please update your PC.

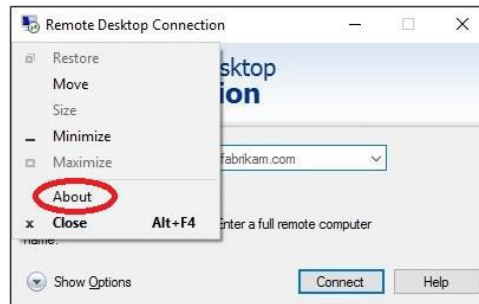
Windows 8.1 and Windows 10 by default have RDP version 8.1 or higher installed. Windows 7 or Windows 8 may have it installed but it's not included by default in the installation.

To check for your Windows Remote Desktop Protocol version follow the steps below:

A. Open Remote Desktop by clicking the **Start** button. In the search box, type **MSTSC**, and then in the list of results, click **Remote Desktop Connection**. A screen like the one below will pop up:

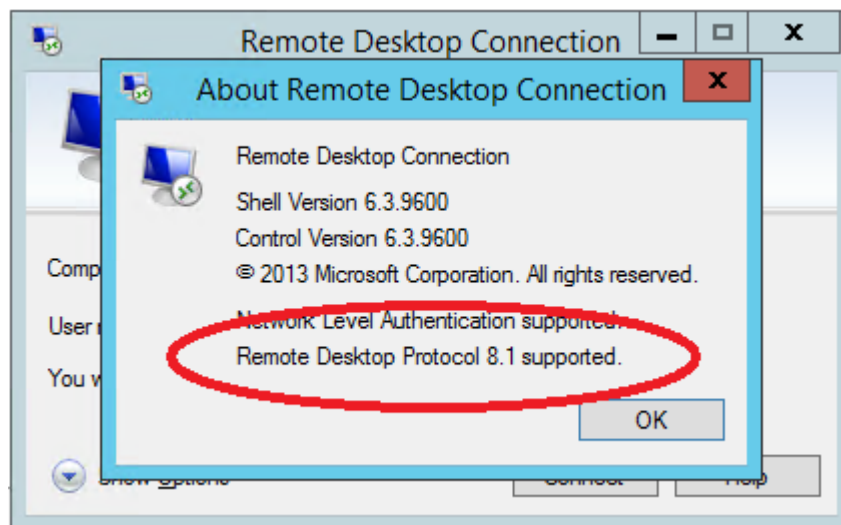


B. In the top-left corner of this window, right-click the small Remote Desktop symbol.



C. Select **About**

D. The bottom line will say "Remote Desktop Protocol 8.1 supported." if the upgrade was successful.



9. Mac OSX users can download the latest Microsoft Remote Desktop App (version 10.2.4 or higher) from the iTunes App Store using the link below (or search the App Store for "Microsoft Remote Desktop", make sure the publisher is "Microsoft Corporation"):

<https://itunes.apple.com/us/app/microsoft-remote-desktop/id1295203466?mt=12>

Note: Mac OS X 10.11 or later is required. Older versions of Mac OS X will NOT work.

Revision history:

V1.7

-removed Appendix A 4. Livenote ActiveX as it does not work in the image currently.

V1.6

-added CredSSP encryption oracle remediation error and solution.

V1.5

-updated iTunes Microsoft Remote Desktop app link and version

-added browser legacy website certificate warnings and solution to proceed

V1.4

-required updates text added

V1.3

-added link to latest MacOSX Microsoft Remote Desktop App v10.1.8 and removed link to v8.0.43

-added warning about PIN reuse after password reset

-updated screenshots

-removed @mict.local logon example, replaced with mict\

V1.2

-added default apps included in the VDI

-updated screenshots

V1.1

-added warning not to use local LN client but use webmail instead

-added extra screenshots

V1.0

-initial document