# Tshoot RDP access with AAD on the server windows01

Follow the <https://charbelnemnom.com/log-in-with-rdp-to-a-windows-azure-vm-using-azure-ad/>

PS C:\Users\azureuser> dsregcmd /status

+----------------------------------------------------------------------+

| Device State |

+----------------------------------------------------------------------+

AzureAdJoined : YES

EnterpriseJoined : NO

DomainJoined : NO

+----------------------------------------------------------------------+

| Device Details |

+----------------------------------------------------------------------+

DeviceId : bd582321-e394-4102-b73b-89ad2840f07b

Thumbprint : 89C5A972ABEB883B0771F0BC600514E185F4F140

DeviceCertificateValidity : [ 2022-03-16 11:32:41.000 UTC -- 2032-03-16 12:02:41.000 UTC ]

KeyContainerId : 2d6dcf46-f765-49ce-a6f9-6da390ca88fc

KeyProvider : Microsoft Software Key Storage Provider

TpmProtected : NO

+----------------------------------------------------------------------+

| Tenant Details |

+----------------------------------------------------------------------+

TenantName :

TenantId : cbede638-a3d9-459f-8f4e-24ced73b4e5e

Idp : login.windows.net

AuthCodeUrl : https://login.microsoftonline.com/cbede638-a3d9-459f-8f4e-24ced73b4e5e/oauth2/authorize

AccessTokenUrl : https://login.microsoftonline.com/cbede638-a3d9-459f-8f4e-24ced73b4e5e/oauth2/token

MdmUrl :

MdmTouUrl :

MdmComplianceUrl :

SettingsUrl :

JoinSrvVersion : 1.0

JoinSrvUrl : https://enterpriseregistration.windows.net/EnrollmentServer/device/

JoinSrvId : urn:ms-drs:enterpriseregistration.windows.net

KeySrvVersion : 1.0

KeySrvUrl : https://enterpriseregistration.windows.net/EnrollmentServer/key/

KeySrvId : urn:ms-drs:enterpriseregistration.windows.net

WebAuthNSrvVersion : 1.0

WebAuthNSrvUrl : https://enterpriseregistration.windows.net/webauthn/cbede638-a3d9-459f-8f4e-24ced73b4e5e/

WebAuthNSrvId : urn:ms-drs:enterpriseregistration.windows.net

DeviceManagementSrvVer : 1.0

DeviceManagementSrvUrl : https://enterpriseregistration.windows.net/manage/cbede638-a3d9-459f-8f4e-24ced73b4e5e/

DeviceManagementSrvId : urn:ms-drs:enterpriseregistration.windows.net

+----------------------------------------------------------------------+

| User State |

+----------------------------------------------------------------------+

NgcSet : NO

WorkplaceJoined : NO

WamDefaultSet : NO

+----------------------------------------------------------------------+

| SSO State |

+----------------------------------------------------------------------+

AzureAdPrt : NO

AzureAdPrtAuthority :

EnterprisePrt : NO

EnterprisePrtAuthority :

+----------------------------------------------------------------------+

| Diagnostic Data |

+----------------------------------------------------------------------+

AadRecoveryNeeded : NO

KeySignTest : PASSED

+----------------------------------------------------------------------+

| Ngc Prerequisite Check |

+----------------------------------------------------------------------+

IsDeviceJoined : YES

IsUserAzureAD : NO

PolicyEnabled : NO

PostLogonEnabled : YES

DeviceEligible : YES

SessionIsNotRemote : NO

CertEnrollment : none

PreReqResult : WillNotProvision

Graphical user interface, text

Description automatically generated

Graphical user interface

Description automatically generated

Add the azure AD user [petr.nemec@tietoevry.com](mailto:petr.nemec@tietoevry.com) to the remote desktop users

*net localgroup "remote desktop users" /add "AzureAd\petr.nemec@tietoevry.com"*

Now my identity EU\5+3 linked to AAD account turns up as a member in the Remote Desktop Users

Graphical user interface, text, application

Description automatically generated

## RDP access via bastion

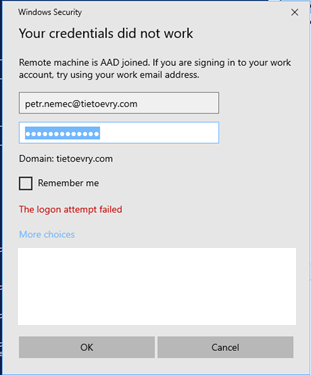
az network bastion rdp --name bastion01 --resource-group rg-nemedpet-linux-aad --target-resource-id /subscriptions/3a60e7b7-ac49-45d8-8a8f-ba61cdc5dc1f/resourceGroups/rg-nemedpet-linux-aad/providers/Microsoft.Compute/virtualMachines/windows01

RDP login fails using EU\5+3

Graphical user interface, text, application, email

Description automatically generated

RDP login fails using email address as well



Graphical user interface, text, application, email

Description automatically generated

I suspect there is an issue with MFA

Text, letter

Description automatically generated