

Connection Denied User Account not Authorized_RDP SSH

Last updated by | Kevin Gregoire | Sep 19, 2022 at 8:22 AM PDT

Tags

cw.TSG

cw.RDP-SSH

Contents

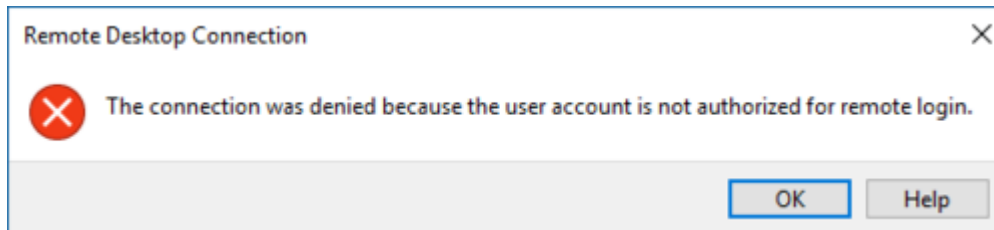
- Symptoms
- Root Cause Analysis
 - References
 - Tracking close code for this volume
- Customer Enablement
- Refresher / Training Template
- Mitigation
 - Backup OS disk
 - ONLINE Troubleshooting
 - ONLINE Approaches
 - Using Windows Admin Center (WAC)
 - Using Serial Console Feature
 - Using Remote Powershell
 - Using Remote CMD
 - Using Custom Script Extension or RunCommands Feature
 - Using Remote Registry
 - Using Remote Services Console
 - Using Remote Powershell
 - Using Remote CMD
 - Using Custom Script Extension or RunCommands Feature
 - Using Remote Registry
 - Using Remote Services Console
 - ONLINE Mitigations
 - OFFLINE Troubleshooting
 - OFFLINE Approaches
 - Information
 - Using Recovery Script
 - For ARM VMs
 - For Classic VMs
 - Using OSDisk Swap API
 - Using VM Recreation scripts
 - For ARM VMs
 - For Classic VMs
 - Using OSDisk Swap API
 - Using VM Recreation scripts
 - For ARM VMs
 - For Classic VMs
 - OFFLINE Mitigations
 - Escalate

- [After work - Cleanup](#)

Symptoms [Need additional help or have feedback?](#)

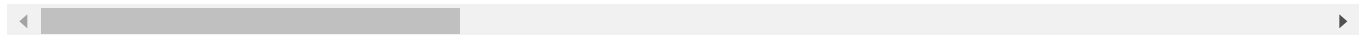
1. The VM screenshot shows the OS fully loaded and waiting for the credentials
2. If you try to RDP to the VM you get one of the following client side errors:

The connection was denied because the user account is not authorized for remote login.

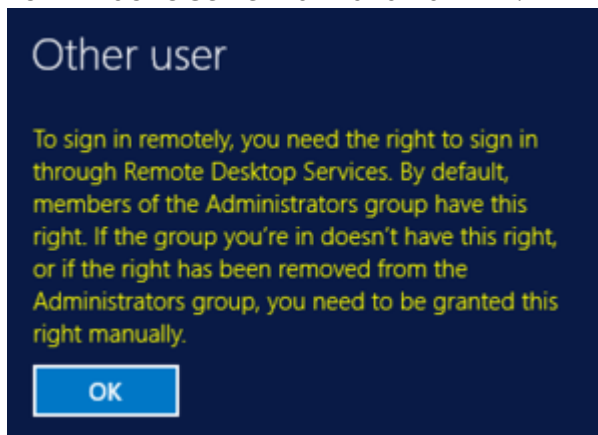


1. Depending on the OS version, you could get the following variations:

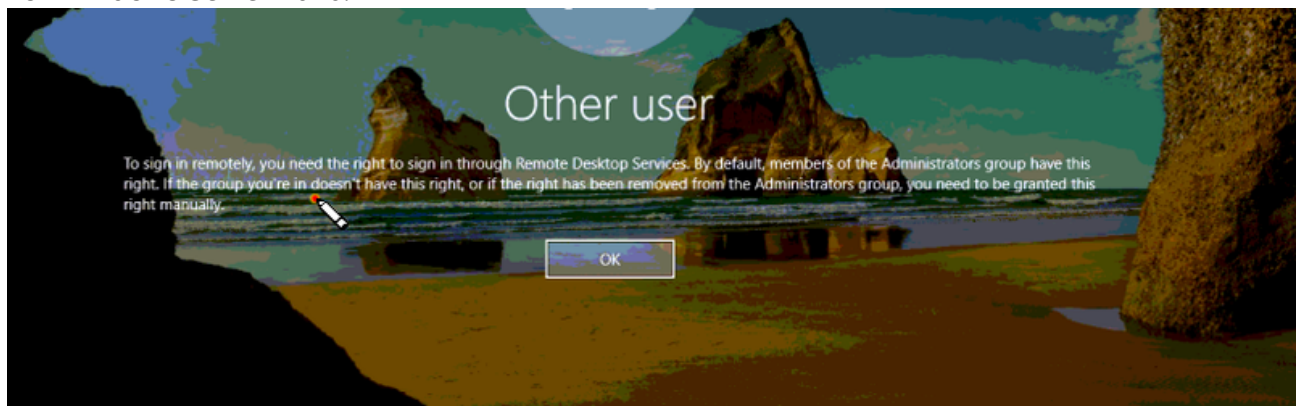
To sign in remotely, you need the right to sign in through Remote Desktop Services. By default,



1. For Windows Server 2012 and 2012 R2:



2. For Windows Server 2016:



Root Cause Analysis

The user that is trying to login using RDP, is not part of the local group *Remote Desktop Users* on the machine. By default, any machine will allow to RDP users that belongs either the *Administrators* or *Remote Desktop Users* local groups.

References

- [User Rights Assignment](#) 

Tracking close code for this volume

Root Cause	Product	Support Topic	Cause Tracking code	Bug
1	Azure Virtual Machine – Windows	<i>Routing Azure Virtual Machine V3\Cannot Connect to my VM\My problem is not listed above</i>	<i>Root Cause - Windows Azure\Virtual Machine\Guest OS - Windows\VM Responding\User Profile Issues</i>	

To know how to flag a bug on a case please refer to [How to do Proper Case Coding](#)

Customer Enablement

N/A

Refresher / Training Template

- For the purpose of training or following along with this TSG, you can use the following link to deploy a VM with this scenario built-in. You will need to enable JIT for the VM. This lab is not to be shared with customers.



Mitigation

Backup OS disk

► Details

ONLINE Troubleshooting

ONLINE Approaches

Please be aware that the Serial Console Feature option will be today possible in:

1. Azure Resource Management VMs (ARM)
2. Public cloud

Whenever you are in a middle of a troubleshooting and you find the step <<<<<**INSERT MITIGATION**>>>>>, proceed to replace that steps with the mitigation section that you need referred below

[Using Windows Admin Center \(WAC\)](#)

▼ Click here to expand or collapse this section

WAC is supported on ARM VMs running Windows Server 2016 or later (not Win10 or any other Windows client version, and not 2012R2/2012/2008R2 versions of Windows Server)

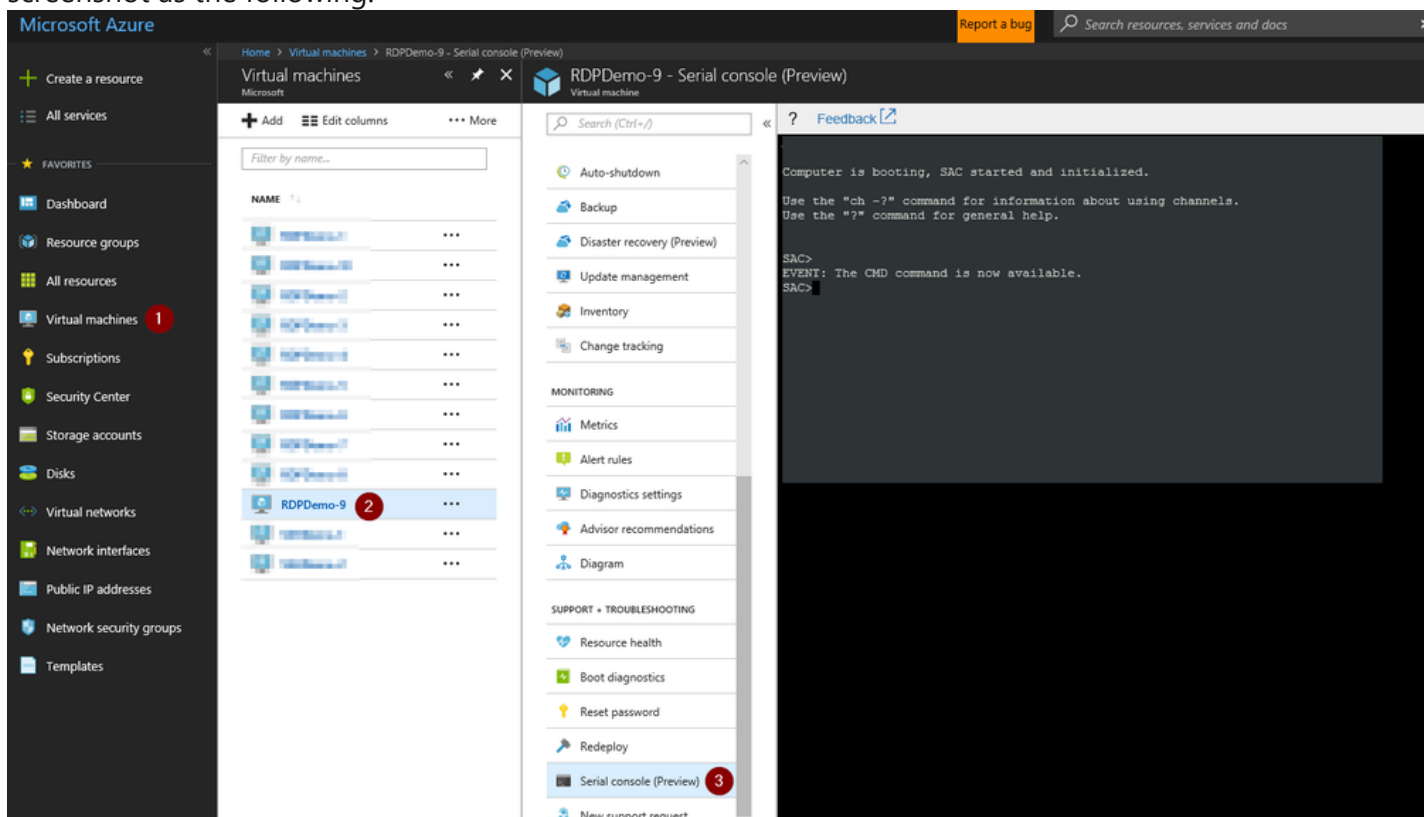
See [How To Access Thru Windows Admin Center](#)

Using [Serial Console Feature](#)

▼ Click here to expand or collapse this section

Applies only for ARM VMs

1. In the portal on the VM blade you will have an extra option called *Serial Console* click there
2. If EMS was enabled on the Guest OS, SAC will be able to connect successfully and then you will have a screenshot as the following:



1. If EMS does not connect, it means the Guest OS was not setup to use this feature:
 1. If the issue that you have will repro on a restart and if the customer is OK to enable this feature, you enable this feature. For details refer to [Serial Console](#) on the *How to enable this feature*
 2. If on the other hand, the issue will not repro on a restart, then you will need to skip this section and go on normally with the **OFFLINE troubleshooting** section
3. Create a channel with a CMD instance. Type `cmd` to start the channel, you will get the name of the channel

```
SAC>cmd
The Command Prompt session was successfully launched.
SAC>
EVENT: A new channel has been created. Use "ch -?" for channel help.
Channel: Cmd0001
SAC>
```

4. Switch to the channel running the CMD instance

```
ch -si 1
```

```
SAC>ch -si 1
```

5. Once you hit enter, it will switch to that channel

```
? Feedback [link]
Name: Cmd0001
Description: Command
Type: VT-UTF8
Channel GUID: [redacted]
Application Type GUID: [redacted]

Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.
```

6. Hit enter a second time and it will ask you for user, domain and password:

```
? Feedback [link]

Please enter login credentials.
Username: 
```

1. If the machine has connectivity, you could use either local or domain IDs. If you want to use a local ID, for domain just add the hostname of the VM
 2. If the machine doesn't have connectivity, you could try to use domains IDs however this will work if only the credentials are cached on the VM. In this scenario, it is suggested to use local IDs instead.
7. Once you add valid credentials, the CMD instance will open and you will have the prompt for you to start your troubleshooting:

```
? Feedback [link]

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

1. At this point, you can do your troubleshooting in bash (CMD) or else, you could start a powershell instance:

1. To launch a powershell instance, run `powershell`

```
? Feedback [link]

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>powershell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>
```

2. To end the powershell instance and return to CMD, just type `exit`

```
PS C:\Windows\system32> exit

C:\Windows\system32>
```

8. <<<<<INSERT MITIGATION>>>>>

Using [Remote Powershell](#)

► Click here to expand or collapse this section

Using [Remote CMD](#)

► Click here to expand or collapse this section

Using [Custom Script Extension](#) or [RunCommands Feature](#)

► Click here to expand or collapse this section

Using [Remote Registry](#)

► Click here to expand or collapse this section

Using [Remote Services Console](#)

► Click here to expand or collapse this section

Using [Remote Powershell](#)

► Click here to expand or collapse this section

Using [Remote CMD](#)

► Click here to expand or collapse this section

Using [Custom Script Extension](#) or [RunCommands Feature](#)

► Click here to expand or collapse this section

Using [Remote Registry](#)

► Click here to expand or collapse this section

Using [Remote Services Console](#)

► Click here to expand or collapse this section

ONLINE Mitigations

▼ Click here to expand or collapse this section

1. This access type of access is stored under the SAM hive which is encrypted and cannot be changed very easily so there's any manual intervention on the machine to enable access until the AD policy controlling this access is modified enabling the access.
2. Regardless of the type of server this is, *Standalone/Member server/Domain Controller*, the command line will always be the same however the type of user you could add will differ:
 1. For *Standalone* machines, only local IDs are allowed
 2. For *Member Servers* machines, you could add local or domain IDs.
 - From the AD point of view, this access can be controlled by the policy *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on through Remote Desktop Services*.
 - By default this should have *Administrators* and *Remote Desktop Users*.

3. For *Domain Controllers* machines, only domain IDs are allowed

- From the AD point of view, this access is also controlled by the policy *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on through Remote Desktop Services* however this would be under *Default Domain Controllers OU*.
- By default this should have *Administrators* group

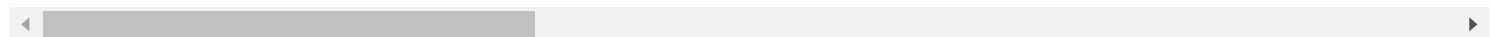
3. To add a user, run the following on an elevated CMD:

```
net localgroup "remote desktop users" <username> /add
```

4. You don't need to restart the machine, ask the customer to retry

OFFLINE Troubleshooting

For CRP machines, at any point that you follow end to end any of the OFFLINE mitigation and that doesn't work



OFFLINE Approaches

Whenever you are in a middle of a troubleshooting and you find the step <<<<<**INSERT MITIGATION**>>>>, proceed to replace that steps with the mitigation section that you need referred below.

Information

For more in-depth information on these operations, please review: [Windows Partitions in Non-Boot Scenarios RDP-SSH](#).

Using [Recovery Script](#)

- Click here to expand or collapse this section

Using [OSDisk Swap API](#)

- Click here to expand or collapse this section

Using *VM Recreation scripts*

- Click here to expand or collapse this section

Using [OSDisk Swap API](#)

- Click here to expand or collapse this section

Using *VM Recreation scripts*

- Click here to expand or collapse this section

OFFLINE Mitigations

- ▼ Click here to expand or collapse this section

This access type of access is stored under the SAM hive which is encrypted and cannot be changed very easily so there's any manual intervention on the machine to enable access until the AD policy controlling this access is modified enabling the access.

1. For **members servers** this access can be controlled by the policy **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on through Remote Desktop Services**. This group will list all the local groups the machine is going to use provide RDP access. By default this should have *Administrators* and *Remote Desktop Users*.
 1. If the values of this policy were modified by the admin, he needs to add them back to allow those local groups
 2. If the values are default but your user is not part of any of those groups then
 1. In case you don't have a VM Agent, then you need to add that out first, you can refer to [Install the VM Agent in OFFLINE mode](#)
 2. Use *Custom Script Extension* you could inject a script adding your user part of the *Remote Desktop Users* group:


```
net localgroup "remote desktop users" <username> /add
```
2. For **Domain Controllers**, this access is also controlled by the policy **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on through Remote Desktop Services** however this would be under *Default Domain Controllers OU*. This group will list all the domain groups the machine is going to use provide RDP access. By default this should have *Administrators* group.
 1. If the values of this policy were modified by the admin, he needs to add them back to allow those local groups
3. For **standalone machines**, you cannot control the access over policy so you need to inject the script to add your user part of the local *Remote Desktop Users* group.
 1. In case you don't have a VM Agent, then you need to add that out first, you can refer to [Install the VM Agent in OFFLINE mode](#)
 2. Using *Custom Script Extension* you can inject the following script:


```
net localgroup "remote desktop users" <username> /add
```

Escalate


1. If this doesn't work out, please reach out to the [Unable to RDP-SSH SME channel on teams](#) ☑ for advise providing the case number, issue description and your question

After work - Cleanup

If you are uncertain that we may need this snapshot by the end of this case for RCA purposes, then just leave it.

1. If the issue is already fix and no further RCA analysis is needed, then proceed to remove the OS Disk backup we created at the beginning of the case
 1. If the **disk is managed** using the portal so the snapshot section and select the snapshot you created previously as a backup.
 2. If the **disk is unmanaged** then
 1. If this is an CRP Machine - ARM, then no further action is required
 2. If this is an Classic - RDPE machine, then
 1. Check the storage account where the OS disk of this machine is hosted using [Microsoft Azure Storage Explorer](#) ☑ right click over the disk and select *Managed Snapshots*
 2. Proceed to delete the snapshot of the broken machine

Need additional help or have feedback?

<i>To engage the Azure RDP-SSH SMEs...</i>	<i>To provide feedback on this page...</i>	<i>To provide kudos on this page...</i>
<p>Please reach out to the RDP-SSH SMEs  for faster assistance.</p> <p>Make sure to use the Ava process for faster assistance.</p>	<p>Use the RDP-SSH Feedback form to submit detailed feedback on improvements or new content ideas for RDP-SSH.</p> <p>Please note the link to the page is required when submitting feedback on existing pages! If it is a new content idea, please put N/A in the Wiki Page Link.</p>	<p>Use the RDP-SSH Kudos form to submit kudos on the page. Kudos will help us improve our wiki content overall!</p> <p>Please note the link to the page is required when submitting kudos!</p>