

This User Account has Expired_RDP SSH

Last updated by | Heath Rensink | Sep 28, 2022 at 9:02 AM PDT

Tags

cw.TSG

cw.RDP-SSH

Contents

- Symptoms
- Root Cause Analysis
- Refresher / Training Template
 - References
 - Tracking close code for this volume
- Customer Enablement
- 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. PSPING is responding
2. If the Guest OS firewall is setup properly, SMB connections works
3. You can check the event log remotely
4. If you RDP the machine you'll get the following client side error:

This user account has expired. For assistance, contact your system administrator or technical support.

Remote Desktop Connection



This user account has expired. For assistance, contact your system administrator or technical support.

OK

Help

Root Cause Analysis

The account you are trying to use or its password are expired.

For the case where the password is expired, usually in some OSs you will get prompted to change the password on the next login however in azure that is not possible.

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.



Deploy to Azure

References

N/A

Tracking close code for this volume

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

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

Customer Enablement

N/A

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

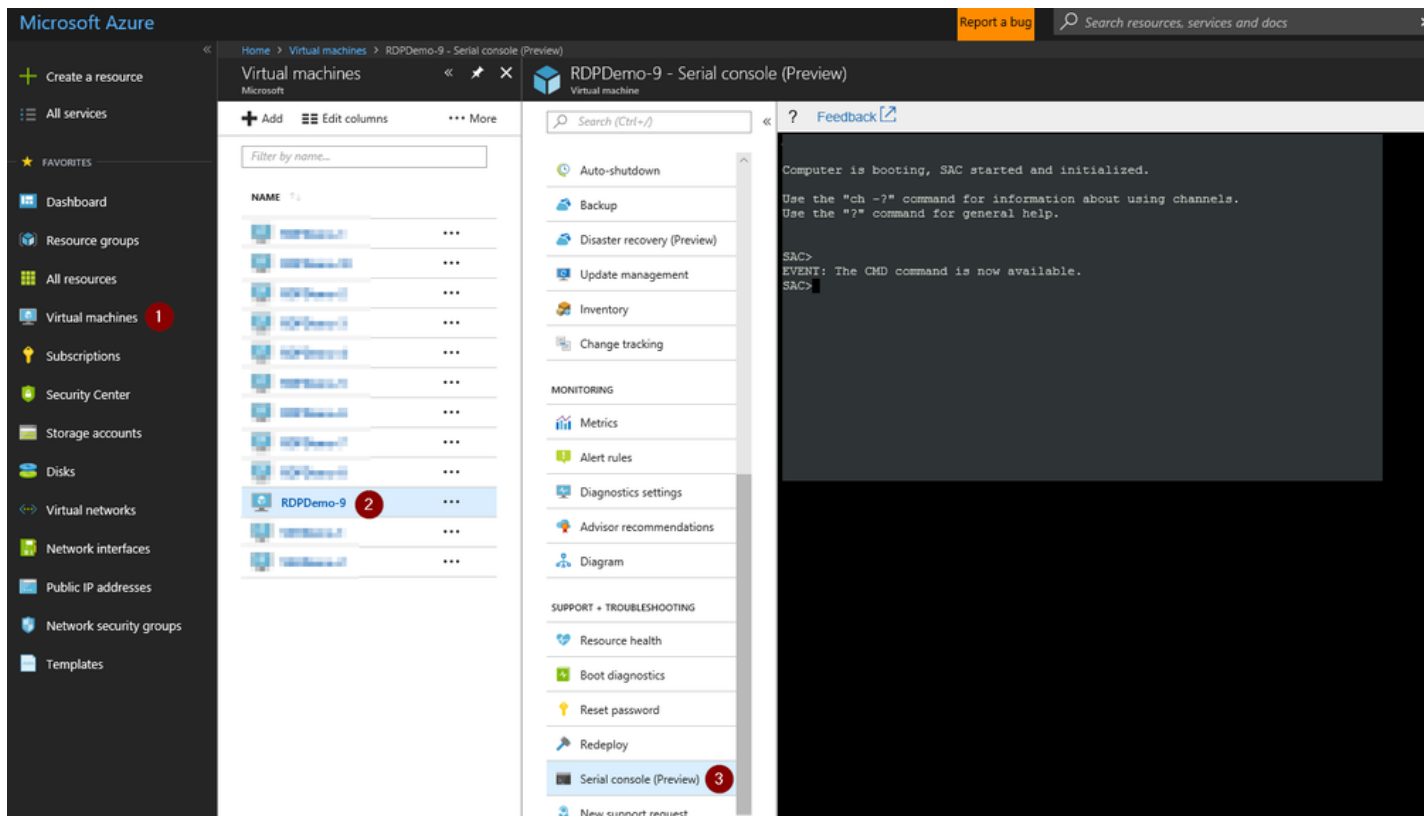
See [How To Access Thru Windows Admin Center](#)

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
```

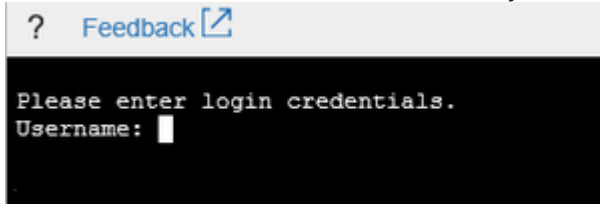
```
SAC>ch -si 1
```

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

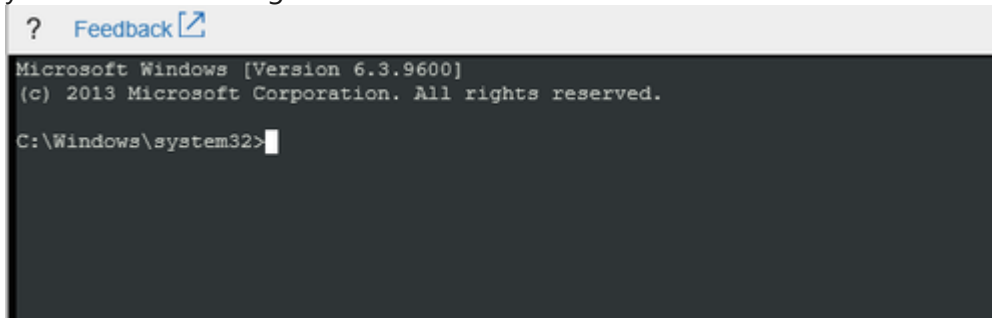
```
? Feedback
Name: Cmd0001
Description: Command
Type: VT-UTF8
Channel GUID: [REDACTED]
Application Type GUID: [REDACTED]

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:

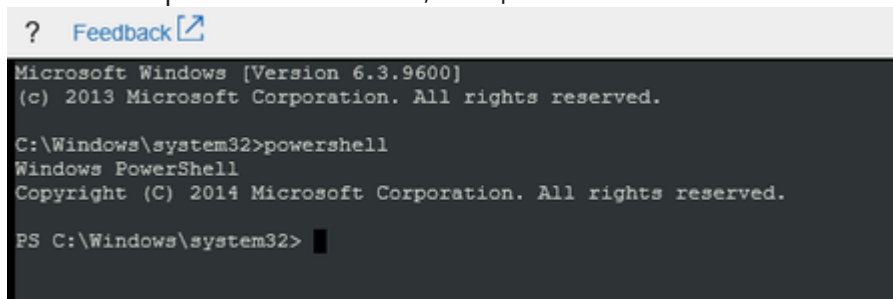


1. If the machine has connectivity, you could use either local or domain IDs. If you want to use a local ID, for domain just add the hostname of the VM
 2. If the machine doesn't have connectivity, you could try to use domains IDs however this will work if only the credentials are cached on the VM. In 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:

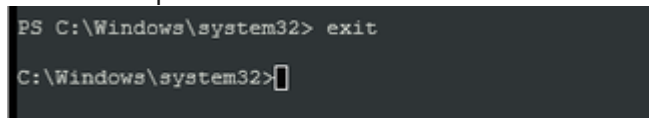


1. At this point, you can do your troubleshooting in bash (CMD) or else, you could start a powershell instance:

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



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



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. Open an elevated CMD instance and query the current settings of the account the customer is trying to use:

```
net user <USERNAME ID>
```

2. Now check which of the two is expired, the user or the password:

1. If the user is expired, the outcome will look this way:

```

C:\Users\azureadmin>net user rescue
User name                rescue
Full Name                rescue
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          1/2/2018 12:00:00 AM      <----- This is :

Password last set        6/30/2018 3:32:20 AM
Password expires         8/11/2018 3:32:20 AM
Password changeable      6/30/2018 3:32:20 AM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               6/30/2018 3:32:44 AM

Logon hours allowed      All

Local Group Memberships  *Administrators      *Users
Global Group memberships *None
The command completed successfully.

```

1. If this is your case, you can modify the expiration flag of the user as the following:

```
net user <USERNAME ID> /expires:"<FUTURE DAY>"
```

2. If the password is expired, you could have two situations:

1. Either the password is expired, in this case the outcome would be:

```

C:\Users\azureadmin>net user rescue
User name                rescue
Full Name                rescue
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          8/11/2018 12:00:00 AM      <----- This is :

Password last set        2/15/2018 3:32:20 AM
Password expires         4/11/2018 3:32:20 AM
Password changeable      2/15/2018 3:32:20 AM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               3/30/2018 3:32:44 AM

Logon hours allowed      All

Local Group Memberships  *Administrators      *Users
Global Group memberships *None
The command completed successfully.

```


1.

1. To change the password

```
net user <USERNAME ID> /password <<NEW COMPLEX PASSWORD>>
```

1.

1. Or the user has set the flag to change the password on the next login, in that case you won't see this out on the user. To remove the flag this change:

```
net user rescue /logonpasswordchg:no
```

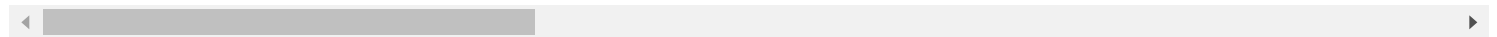
1.

1.

1. This will remove the flag and the customer can use the very same password that he has before, of if needed, you can also reset the password as well.

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

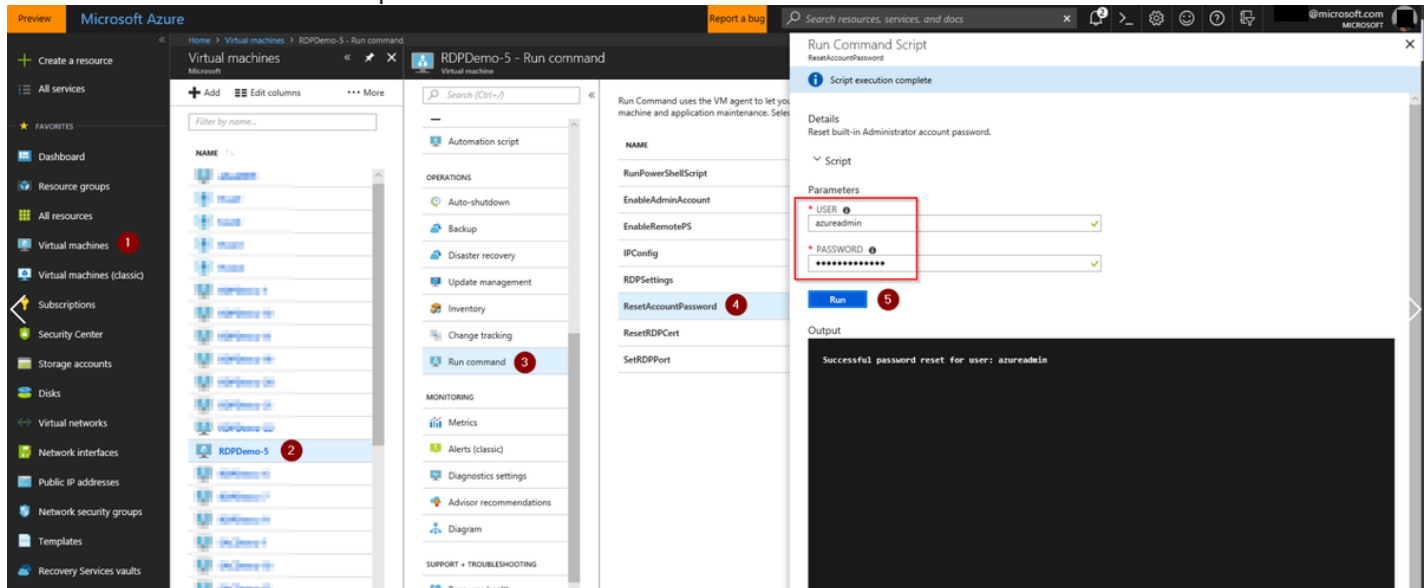
Using *VM Recreation scripts*

► Click here to expand or collapse this section

OFFLINE Mitigations

▼ Click here to expand or collapse this section

1. If you have a working agent, you can use *Run Command* to change the password of the local user the customer wants to use. From the VM frame, go to the *Run Command* option, and select **ResetAccountPassword** script and hit run



2. If that doesn't work then:

1. Connect to the VM remotely using [Remote Powershell](#) or [Remote CMD](#):
2. Query for the current settings of the account the customer is trying to use:

```
net user <USERNAME ID>
```

3. Now check which of the two is expired, the user or the password:

1. If the user is expired, the outcome will look this way:

```

C:\Users\azureadmin>net user rescue
User name                rescue
Full Name                rescue
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          1/2/2018 12:00:00 AM      <----- This
Password last set        6/30/2018 3:32:20 AM
Password expires         8/11/2018 3:32:20 AM
Password changeable      6/30/2018 3:32:20 AM
Password required        Yes
User may change password Yes
Workstations allowed     All
Logon script
User profile
Home directory
Last logon               6/30/2018 3:32:44 AM
Logon hours allowed      All
Local Group Memberships  *Administrators    *Users
Global Group memberships *None
The command completed successfully.

```

1. If this is your case, you can modify the expiration flag of the user as the following:

```
net user <USERNAME ID> /expires:"<FUTURE DAY>"
```

2. If the password is expired, you could have two situations:

1. Either the password is expired, in this case the outcome would be:

```

C:\Users\azureadmin>net user rescue
User name                rescue
Full Name                rescue
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          8/11/2018 12:00:00 AM      <----- This
Password last set        2/15/2018 3:32:20 AM
Password expires         4/11/2018 3:32:20 AM
Password changeable      2/15/2018 3:32:20 AM
Password required        Yes
User may change password Yes
Workstations allowed     All
Logon script
User profile
Home directory
Last logon               3/30/2018 3:32:44 AM
Logon hours allowed      All
Local Group Memberships  *Administrators    *Users
Global Group memberships *None
The command completed successfully.

```

1. To change the password

```
net user <USERNAME ID> /password <<NEW COMPLEX PASSWORD>>
```

2. Or the user has set the flag to change the password on the next login, in that case you won't see this out on the user. To remove the flag this change:

```
net user rescue /logonpasswordchg:no
```

1. This will remove the flag and the customer can use the very same password that he has before, or if needed, you can also reset the password as well.

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 - RDP 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>