

Reset Password Without VM Agent_RDP SSH

Last updated by | Kevin Gregoire | Oct 21, 2022 at 9:06 AM PDT

Tags

cw.RDP-SSH

cw.TSG

Tags: [Azure](#) [Azure - TSG](#) [RDP-SSH](#) [RDPSSH-VMResponding](#) [Virtual Machine](#)

Contents

- Symptoms
 - Brownbag Video
- Root Cause Analysis
 - Tracking close code for this volume
- Customer Enablement
 - Pre-Mitigation
- Refresher / Training Template
 - Mitigation
 - 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
 - ONLINE Mitigations
 - Mitigation 1
 - Mitigation 2
 - 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
 - OFFLINE Mitigations
 - Mitigation 1
 - Mitigation 2
 - Escalate
 - After work - Cleanup
- Need additional help or have feedback?

Symptoms

The Customer cannot login into the machine getting that the password is incorrect and the VM Agent is not installed or not working for whatever reason. This article applies either if the account is expired or if you just want to create a new username then we can leverage the following action plan to create a new local admin account and gain access to the VM.




Brownbag Video

- [HowTo Install the VM Agent in OFFLINE mode](#) 

Root Cause Analysis

Either the VM was created without the Azure VM Extension or else the extension is broken.

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\I need to reset my password	Root Cause - Windows Azure\Virtual Machine\Password Reset\Powershell or CLI issue	
	Azure Virtual Machine  Windows	Routing Azure Virtual Machine V3\Cannot Connect to my VM\I need to reset my password	Root Cause - Windows Azure\Virtual Machine\Password Reset\VM Access Extension issues	
	Azure Virtual Machine  Windows	Routing Azure Virtual Machine V3\Cannot Connect to my VM\I need to reset my password	Root Cause - Windows Azure\Virtual Machine\Password Reset\VM Agent not running/installed	

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



Customer Enablement

- [How to reset local Windows password for Azure VM](#) 
- [How to reset the Remote Desktop service or its login password in a Windows VM](#) 

Pre-Mitigation



This action plan involves to recreate the VM so you can perform any change on the file system of that VM. If you cannot avoid this recreation, then for the recreation part you may want to refer to the HowTo's document:

- [Recreate an ARM Virtual Machine](#)

- [Recreate an RDVE Virtual Machine](#)
 - [Troubleshoot Azure VM by attaching OS disk to another Azure VM](#) 
 - [Azure CLI: How to delete and re-deploy a VM from VHD](#) 
1. Before doing anything, please validate if this is an encrypted VM. On ASC check on the Resource Explorer on the VMCard for the value *OS Disk Encrypted*

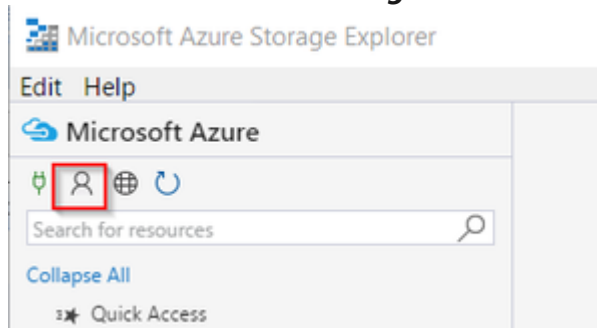
OS Disk Lease Id	0db9a55c-0317-40fa-a032-b1f3550f3775
OS Disk Lease Acquired	True
OS Disk Billing Validated	True
OS Disk Encrypted	False
Billing Code	Windows_IaaS
Billing is Created from Marketplace Image	N/A
Billing Tag GUID	00000000-0000-0000-0000-000000000000

2. If the OS Disk is encrypted, then first proceed to [Unlock an encrypted disk](#)
3. Now proceed to do a copy of the OS disk, this will help in case of a rollback for recovery or RCA in a later stage
4. Power the machine down and once it is stopped de-allocated to do the copy.
5. Create a snapshot

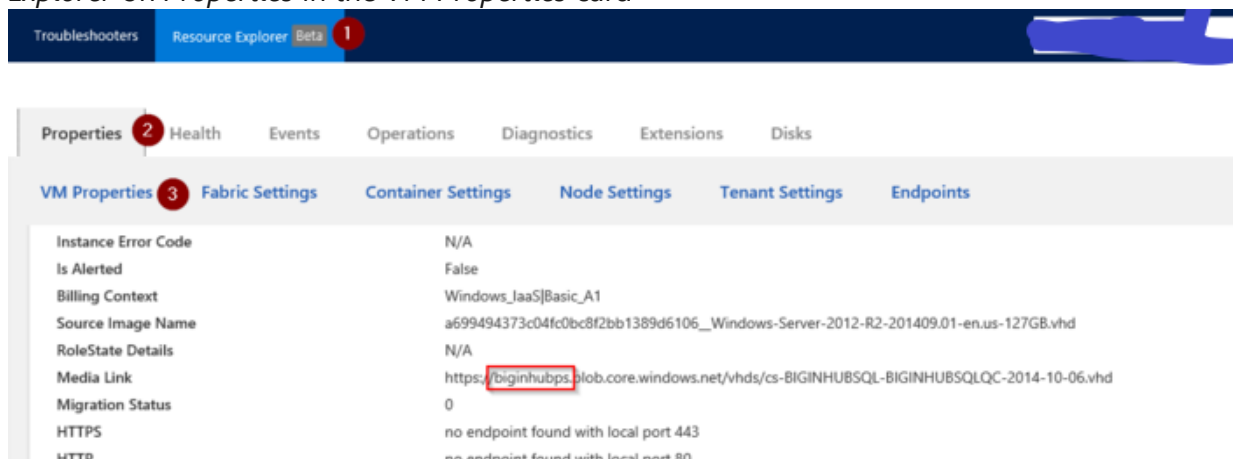
1. If the **disk is unmanaged**, this could be done by using [Microsoft Azure Storage Explorer](#)  or [Azure Powershell](#) 

1. Using [Microsoft Azure Storage Explorer](#) 

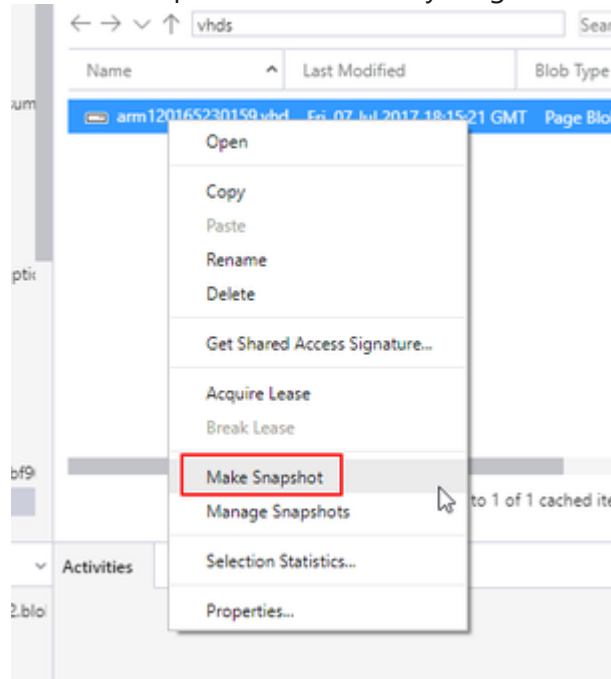
1. Once the customer download the tool, proceed to add the Azure account details so you can access the storage accounts
2. Click on **Add Account Settings** then ***Add an account...***



3. Go to the storage account where the OS disk is, you can see this on ASC under *Resource Explorer* on *Properties* in the *VM Properties* card



4. Create a snapshot of this disk by a right click over the disk and select *Make Snapshot*



2. Using [Azure Powershell](#)

1. You can follow [How to Clone a disk using Powershell](#)

2. If the **disk is managed**, use Azure portal to take a snapshot

1. Sign in to the Azure portal.
2. Starting in the upper-left, click New and search for snapshot.
3. In the Snapshot blade, click Create.
4. Enter a Name for the snapshot.
5. Select an existing Resource group or type the name for a new one.
6. Select an Azure datacenter Location.
7. For Source disk, select the Managed Disk to snapshot.
8. Select the Account type to use to store the snapshot. We recommend Standard_LRS unless you need it stored on a high performing disk.
9. Click Create.

6. Now prepare your environment to work with your disk:

1. For CRP (ARM) VMs which **are encrypted**, refer to [Unlock an encrypted disk](#)
 2. For CRP (ARM) **not encrypted** VMs refer to [Recreate an ARM Virtual Machine](#)
 3. For RDPE VMs, refer to [Recreate an RDPE Virtual Machine](#)
7. An alternative to the above steps for ARM VMs is using [vm-repair](#) extension script to create a repair VM by copying the source VM's OS disk and attaching it to a newly created repair VM.

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

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)

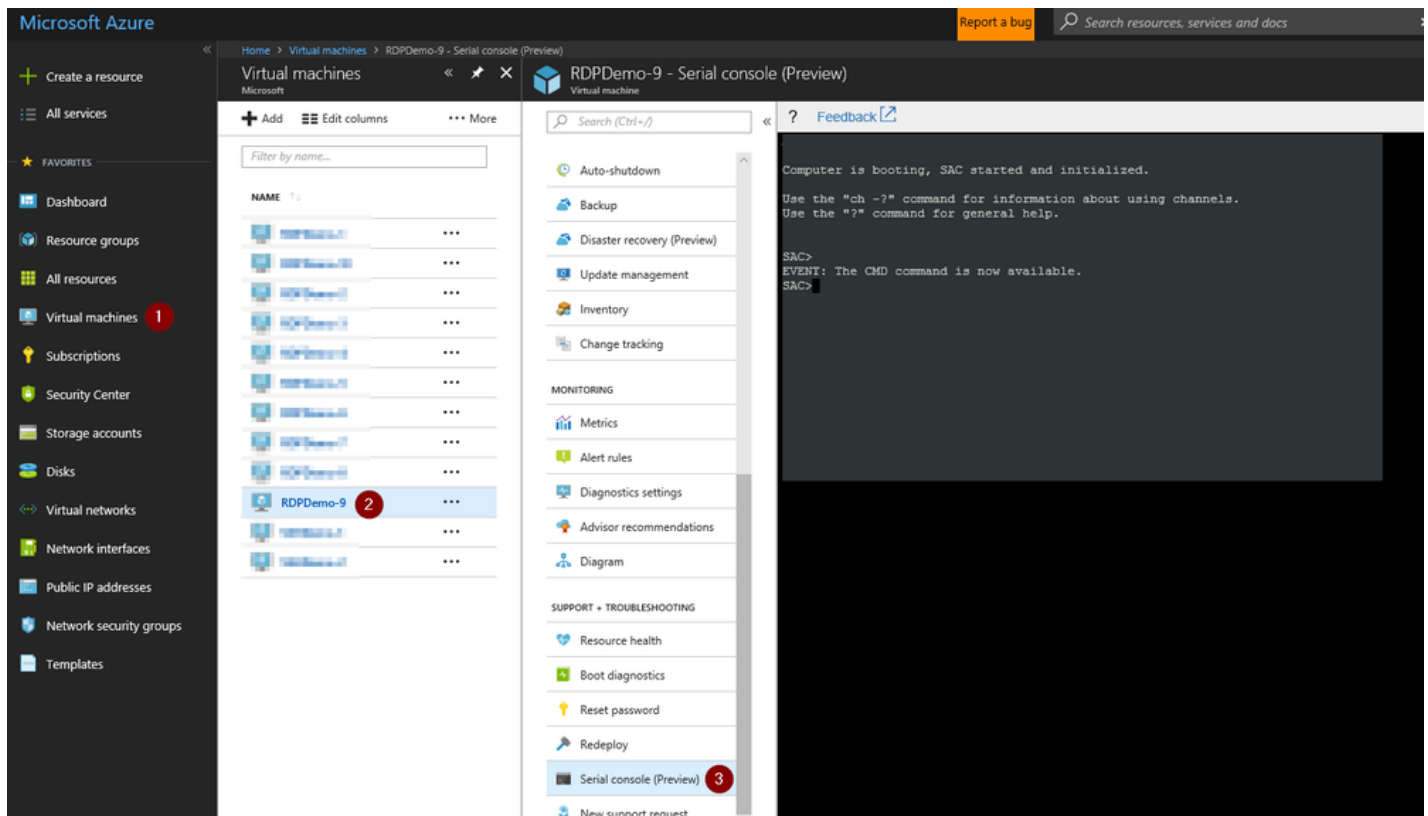
See [How To Access Thru Windows Admin Center](#)

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
```

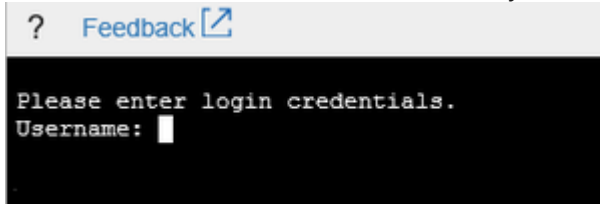
```
SAC>ch -si 1
```

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

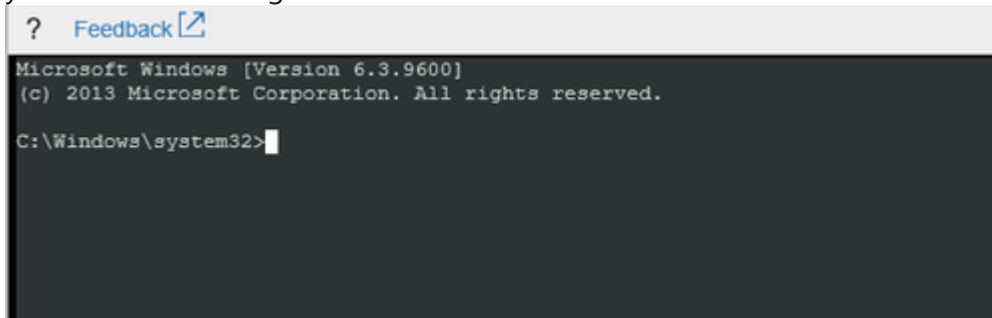
```
? Feedback
Name: Cmd0001
Description: Command
Type: VT-UTF8
Channel GUID: [REDACTED]
Application Type GUID: [REDACTED]

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:

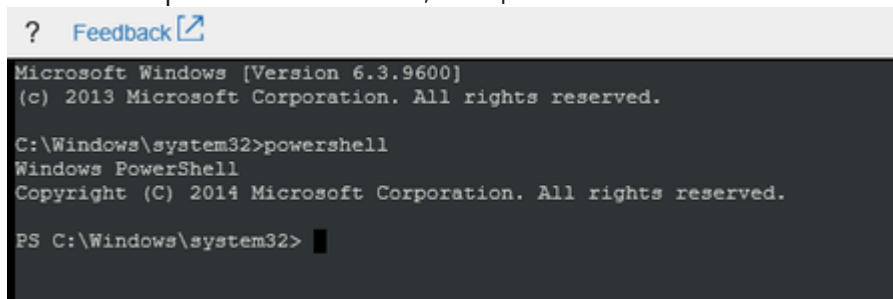


1. If the machine has connectivity, you could use either local or domain IDs. If you want to use a local ID, for domain just add the hostname of the VM
 2. If the machine doesn't have connectivity, you could try to use domains IDs however this will work if only the credentials are cached on the VM. In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

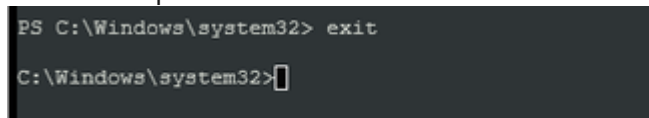


1. At this point, you can do your troubleshooting in bash (CMD) or else, you could start a powershell instance:

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

ONLINE Mitigations

Mitigation 1

▼ Click here to expand or collapse this section

1. Download the [VMAgent MSI](#)  file on a new or existing data disk which is attached to a working VM from the same region.
2. Detach the disk containing the files needed from the working VM and attach to your broken VM. We are calling this disk the *Utility disk*
3. Now open an administrative CMD instance and install the VM Azure Agent:

```
msiexec /i WindowsAzureVmAgent*.msi /quiet /passive /promptrestart
```

4. Once the agent is installed and working, you may proceed by resetting the password as usual from the portal

Mitigation 2

▼ Click here to expand or collapse this section

1. Open an elevated CMD instance and type the following to change the password of the user account:
 1. For local accounts: `net user <USERNAME> *`
 2. For domain accounts: `net user <USERNAME> * /domain`
 3. This will ask for the password so just type the new password to setup the account
2. Once you change the password the issue will be resolve and the customer can use that user to login into the VM. You don't need to restart the VM.

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

OFFLINE Mitigations

Mitigation 1

▼ Click here to expand or collapse this section


1. If the customer agrees, you may want to [install the VM Agent in offline mode](#)
2. Once the agent is installed and working, you may proceed by resetting the password as usual from the portal

Mitigation 2

▼ Click here to expand or collapse this section

The following process only applies to Member and standalone servers only.

In terms of using Custom Script to restore access to a domain controller, ***this is not supported and should not be done for a customer***, in addition this may break with changes to custom script in the future. If a customer loses access to a domain controller, then they need to follow the steps restoring the dc from backup, as they would do on premise.

For more information please refer to [How to reset the Remote Desktop service or its login password in a Windows VM](#) 

In the following mitigation we are going to create new local users so in every single attempt, do not create a user named as the Built-in administrator account or any other existing account, create a **brand new user**.

1. Create ***gpt.ini*** in ***\Windows\System32\GroupPolicy*** (if gpt.ini exists, rename to gpt.ini.bak) with the following content:

```
[General]
gPCFunctionalityVersion=2
gPCMachinExtensionNames=[{42B5FAAE-6536-11D2-AE5A-0000F87571E3}{40B6664F-4972-11D1-A7CA-0000F87571E3}]
Version=1
```

2. Create ***scripts.ini*** in ***\Windows\System32\GroupPolicy\Machine\Scripts*** (make sure hidden folders are shown. If needed, create the GroupPolicy, Machine or Scripts folders) with the following content:

```
[Startup]
0CmdLine=FixAzureVM.cmd
0Parameters=
```

3. Create **FixAzureVM.cmd** in **\Windows\System32\GroupPolicy\Machine\Scripts\Startup** with the following contents, replacing `<username>` and `<newpassword>` with your own values:

```
net user <username> <newpassword> /add /Y
net localgroup administrators <username> /add
net localgroup "remote desktop users" <username> /add
```

Note:

- You must meet the configured password complexity requirements for your VM when defining the new password. This password has lowercase, uppercase, numbers and special characters, the customer can select a different password but we strongly recommend to include the combination of letters (upper/lower), numbers and special characters.
- The username that you are creating needs to be different to any other existing local IDs on the VM, otherwise this will fail since the OS will be confusing which SID should provide to that new ID.

Sample:

```
net user azure-recoveryID @zurE2017 /add /Y
net localgroup administrators azure-recoveryID /add
net localgroup "remote desktop users" azure-recoveryID /add
```

4. Detach the OS disk from the troubleshooting VM
5. Wait for the disk lease to be updated (3mins tops) and recreate the VM using the modified OS disk
6. After you gain access to the VM by using the new local admin account, please continue to remove all the scripts you injected on this mitigation and restore the backup so the Cx can continue using their previous GroupPolicy configuration:

```
\Windows\System32\GroupPolicy\Machine\Scripts\Startup\FixAzureVM.cmd
\windows\System32\GroupPolicy\Machine\Scripts\scripts.ini
\windows\System32\GroupPolicy\gpt.ini
```

Note: If gpt.ini existed before, and you renamed it to gpt.ini.bak, rename the .bak file back to gpt.ini

Escalate

1. If this doesn't work out, please reach out to the [Unable to RDP-SSH SME channel on teams](#) ☑ for advice 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 fixed 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>