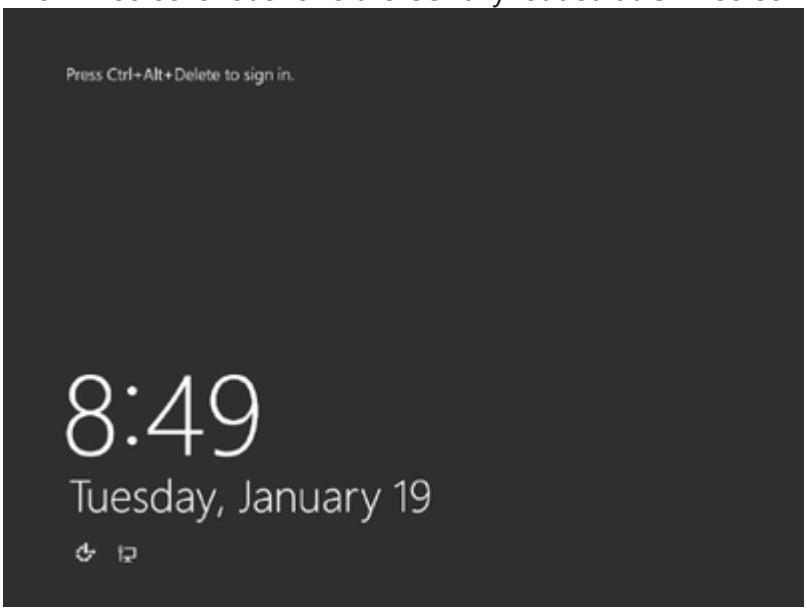
Contents

- Need additional help or have feedback?

Symptoms

1. The VM screenshot shows the OS fully loaded at CAD screen (Ctrl+Alt+Del)



2. On the Guest OS logs you will not find connections being made
3. WaAppAgent logs shows the machine is doing heartbeat normally.
4. As soon as the VM is restarted, ***you could have connectivity for almost a minute*** and then you are kicked out and the machine reject inbound traffic
5. The following software are installed:
    1. Kaspersky Endpoint Security
    2. Kaspersky Security Center

Software version tried with this article

1. Kaspersky Endpoint Security 10 for Windows
2. Kaspersky Security Center 10 Network Agent

Note: If your case is solved by this very same action plan and you have a different version that the ones describes on this section, please provide your feedback at the end of this page so we can add your version in this article. Thanks.

Root Cause Analysis

Kaspersky software is blocking all inbound connection. This could be due to its miconfigured.

References

N/A

Tracking close code for this volume

Root Cause	Product	Support Topic	Cause Tracking code	Bug
1	*Azure Virtual Machine Windows*	**For existing VMs:** *Routing Azure Virtual Machine V3\Cannot Connect to my VM\Failure to connect using RDP or SSH port*	*Root Cause - Windows Azure\Virtual Machine\Third Party Issues/Questions*	
	Azure Virtual Machine Windows	**For new migrated machines:** *Routing Azure Virtual Machine V3\Cannot create a VM\I need guidance preparing an image*	*Root Cause - Windows Azure\Compute\Migration\On-prem to Azure - ASR\Third Party filter/driver*	

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

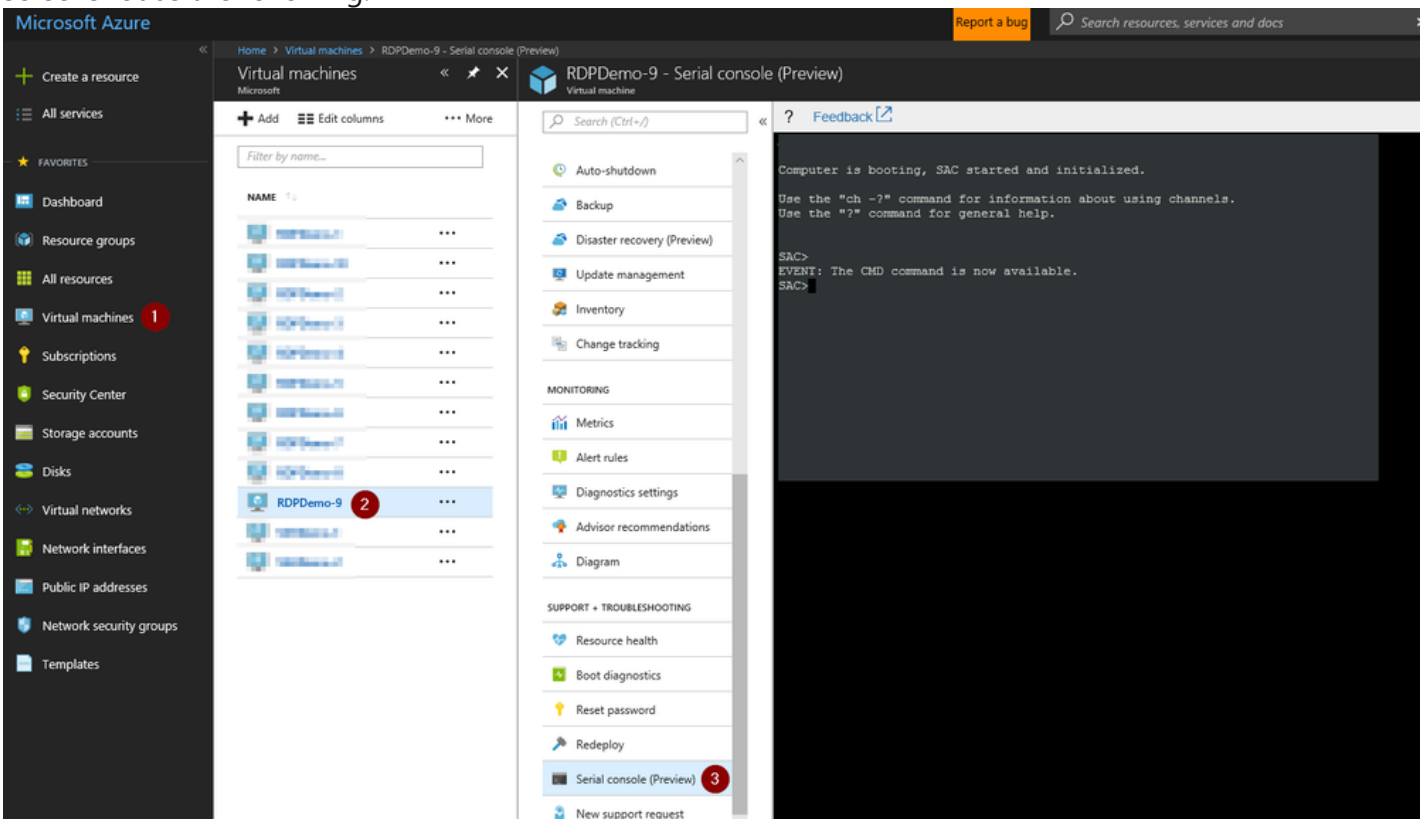
WAC is supported on ARM VMs running Windows Server 2016 or later (not Win10 or any other Windows client version, and not 2012R2/2012/2008R2 versions of Windows Server

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

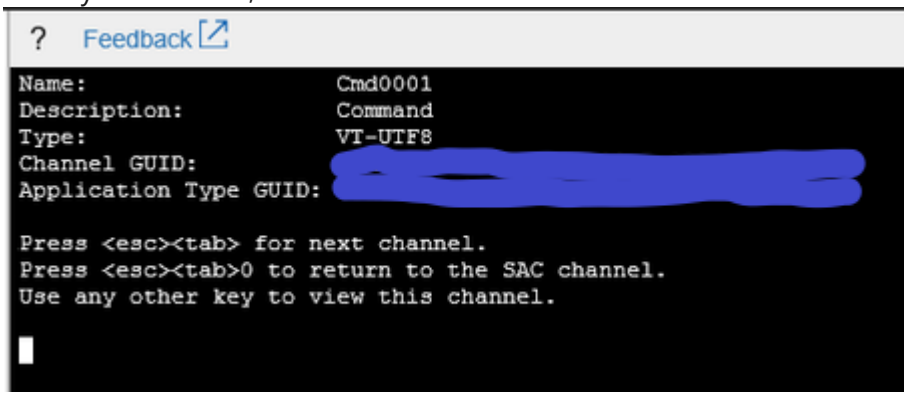
```
SAC>cmd
The Command Prompt session was successfully launched.
SAC>
EVENT:   A new channel has been created.  Use "ch -?" for channel help.
Channel: Cmd0001
SAC>
```

4. Switch to the channel running the CMD instance

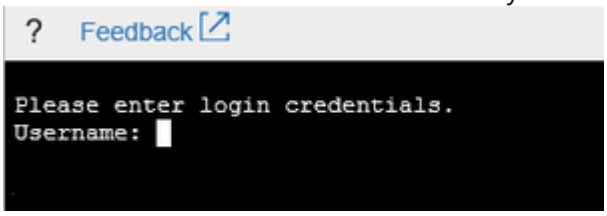
```
ch -si 1
```

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

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



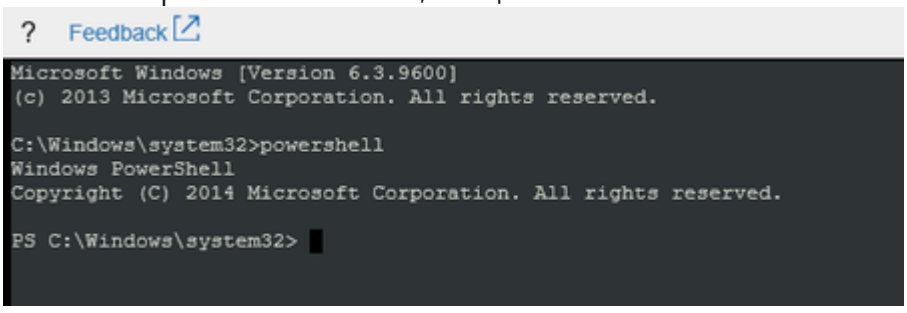
6. Hit enter a second time and it will ask you for user, domain and password:



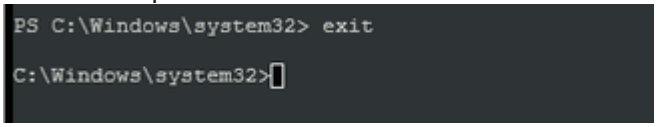
    1. If the machine has connectivity, you could use either local or domain IDs. If you want to use a local ID, for domain just add the hostname of the VM
    2. If the machine doesn't have connectivity, you could try to se domains IDs however this will work if only the credentials are cached on the VM.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

1. Get the ***list of the services*** you need to disable the *WinGuestAnalyzer* report

Mitigation 1

▼ Click here to expand or collapse this section
Try to stop/disable the Kaspersky services:

1. Open a CMD instance and check the current state of the services:

```
sc query AVP
sc query avpsus
sc query kl1
sc query klelam
sc query klflt
sc query klhk
sc query KLIF
sc query KLIM6
sc query klnagent
sc query klpd
sc query klwfp
```

2. Try stopping the service:

```
sc stop AVP
sc stop avpsus
sc stop kl1
sc stop klelam
sc stop klflt
sc stop klhk
sc stop KLIF
sc stop KLIM6
sc stop klnagent
sc stop klpd
sc stop klwfp
```

3. See if you can RDP back into the VM

    1. If you run into issues or hang on stopping, then just disable the service:

```
sc config AVP start=disabled
sc config avpsus start=disabled
sc config kl1 start=disabled
sc config klelam start=disabled
sc config klflt start=disabled
sc config klhk start=disabled
sc config KLIF start=disabled
sc config KLIM6 start=disabled
sc config klnagent start=disabled
sc config klpd start=disabled
sc config klwfp start=disabled
```

    1. Reboot the VM

Mitigation 2

▼ Click here to expand or collapse this section
Try removing the software:

1. Open a Powershell instance and run the following to remove the software:

```
$app = Get-WmiObject -Class Win32_Product -Filter "Name = 'Kaspersky Endpoint Security 10 for Windows
$app.Uninstall()
```

A successful uninstall will return a message that ends with "ReturnValue: 0"

If powershell doesnt work try below from serial console

Open Serial console

type "wmic" and press enter

type "Product get name" and enter, it will list the name of installed programs

Type "product where name=�Kaspersky Endpoint Security for Windows� call uninstall"

Press "Y"

Reboot the VM.

<image to be inserted>

2. Reboot the VM and if this is still not fix, then proceed with the following mitigation.

Mitigation 3

▼ Click here to expand or collapse this section

1. A memory dump from the VM needs to be collected **while the VM is on state**.
    1. Confirm if customer has already granted permission in DfM "Product details" section: `Customer permission granted: Yes` If No, ask the customer to go to their case in the Portal and grant us

permission to look at OS logs. An example email can be found at: https://aka.ms/azdataperm/

2. Refer to How to Get an OS Dump from an Azure Virtual Machine
3. Once the memory dump was collected, then engage the GES team (Windows EEs) for a dump analysis. Cut a problem with the following details:
   - Product: ***Windows Svr 2008 R2*** or ***Windows Svr 2012 R2 Datacenter*** or ***Windows Svr 2016 Datacenter*** or ***Windows Svr 2019 Datacenter*** as appropiate
   - Support topic: ***Routing Windows V3\System Performance\System Hangs***
   - Problem Description:

```
================== <start copy> =====================================
Customer-facing error (RDP client error):
Symptoms description:

SR#
VM name
ICM#                  <--- Only if the dump was collected from the Host
Datacenter            <--- Only if the dump was collected from the Host
Jumpbox               <--- Only if the dump was collected from the Host
Path in the jumpbox   <--- Only if the dump was collected from the Host
================== <end copy> =======================================
```

   - These routing will route you to a Windows team however since we need to engage GES, override the routing to
     - For Premier cases: ***Windows EE Premier*** queue
     - For Professional cases: ***Windows EE Pro*** queue

2. Proceed with the action plan provided by the Windows EE

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

1. Get the ***list of the services*** you need to disable the *WinGuestAnalyzer* report

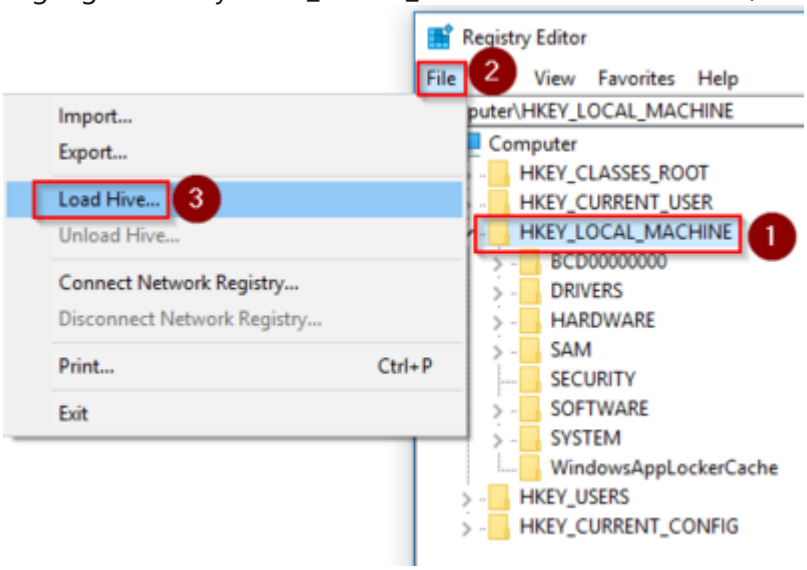
Mitigation 1

▼ Click here to expand or collapse this section
Try disable the application

1. Before doing any change please create a copy of the folder *\windows\system32\config* in case a rollback on the changes is needed

2. On the troubleshooting machine, open the registry editor *REGEDIT*

3. Highlight the key *HKEY_LOCAL_MACHINE* and select *File\Load Hive* from the menu



4. Browse up to the file *\windows\system32\config\SYSTEM*

5. When you hit open it's going to ask for a name, put *BROKENSYSTEM* and then expand *HKEY_LOCAL_MACHINE* and you will see an extra key called *BROKENSYSTEM*. For this troubleshooting, we are mounting these trouble hives as BROKENSYSTEM

6. Now browse and disable the following services:

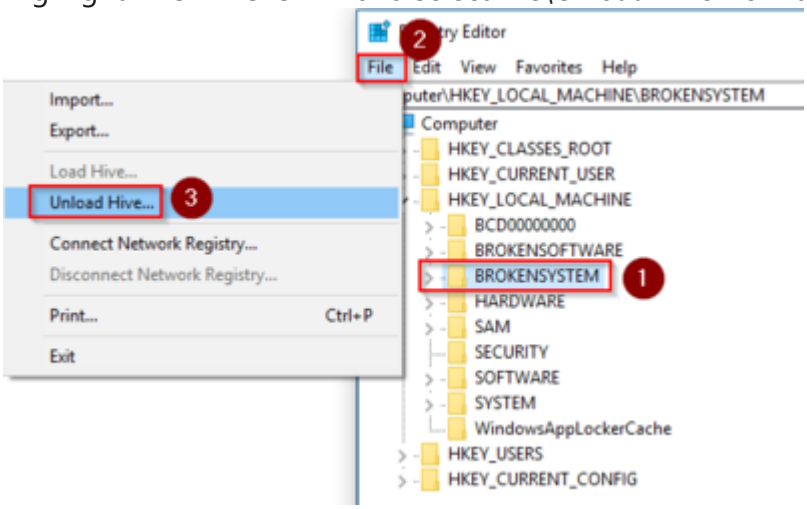
    1. Check which ControlSet is the machine booting from. You will see its key number in `HKLM\BROKENSYSTEM\Select\Current`

    2. Now make these changes.

```
Set-ItemProperty -Path 'HKLM:\BROKENSYSTEM\Controlset00x\Services\AVP' -name 'Start' -Value 4
Set-ItemProperty -Path 'HKLM:\BROKENSYSTEM\Controlset00x\Services\avpsus' -name 'Start' -Value 4
Set-ItemProperty -Path 'HKLM:\BROKENSYSTEM\Controlset00x\Services\kl1' -name 'Start' -Value 4
Set-ItemProperty -Path 'HKLM:\BROKENSYSTEM\Controlset00x\Services\klelam' -name 'Start' -Value 4
Set-ItemProperty -Path 'HKLM:\BROKENSYSTEM\Controlset00x\Services\klflt' -name 'Start' -Value 4
Set-ItemProperty -Path 'HKLM:\BROKENSYSTEM\Controlset00x\Services\klhk' -name 'Start' -Value 4
Set-ItemProperty -Path 'HKLM:\BROKENSYSTEM\Controlset00x\Services\KLIF' -name 'Start' -Value 4
Set-ItemProperty -Path 'HKLM:\BROKENSYSTEM\Controlset00x\Services\KLIM6' -name 'Start' -Value 4
Set-ItemProperty -Path 'HKLM:\BROKENSYSTEM\Controlset00x\Services\klnagent' -name 'Start' -Value
Set-ItemProperty -Path 'HKLM:\BROKENSYSTEM\Controlset00x\Services\klpd' -name 'Start' -Value 4
Set-ItemProperty -Path 'HKLM:\BROKENSYSTEM\Controlset00x\Services\klwfp' -name 'Start' -Value 4
```

7. **Unmount SYSTEM Hives**

- Highlight *BROKENSYSTEM* and select *File\Unload Hive* from the menu



Mitigation 2

▼ Click here to expand or collapse this section

Option 1

1. At this point and if the customer is OK with this is to uninstall the software. To do so just inject the following script using CSE:

```
$app = Get-WmiObject -Class Win32_Product -Filter "Name = 'Kaspersky Endpoint Security 10 for Windows
$app.Uninstall()
```

Note: Ensure that the name and version of the software is accurate. You can check this on WinGuestAnalyzer.

Option 2

1. If after all this the issue remains, you need more access to troubleshoot this VM:

    1. Depending if this VM is hosted on a datacenter where Nested virtualization is an option and if the customer agrees, then you can build this environment and the VM in this environment where you are going to have full access to the VM's console screen.

2. If the VM is not hosted in a datacenter where nested environment is an option, you can ask the customer to download the VHD in onprem for further troubleshooting
3. At any point and whenever you have full access to the VM, if you require more help, you can engage ***Windows Devices and Deployment*** team for further troubleshooting. If that's what you need, then cut a problem with the following values:
   - Product: ***Windows Svr 2008 R2*** or ***Windows Svr 2012 R2 Datacenter*** or ***Windows Svr 2016 Datacenter*** as appropriate
   - Support topic: ***Routing Windows V3\Network Connectivity and File Sharing\TCP/IP Communications***
   - Override the routing to engage Tier 2 directly **Note:** Be aware that to engage this team you need to provide them a way of access to the machine they need to troubleshoot so you may want to cut the problem to engage them but by the time the engineer is engaged the VHD needs to be already downloaded or the nested environment created so they can work on the machine.

2. Once the VM is created on nested environment, you could remove this software normally as any other machine using the console access to this VM.

Mitigation 3

This mitigation only applies in ONLINE mode

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 - RDFE 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?

To engage the Azure RDP-SSH SMEs...	*To provide feedback on this page...*	*To provide kudos on this page...*
Please reach out to the **RDP-SSH SMEs** for faster assistance. Make sure to use the **Ava process** for faster assistance.	Use the **RDP-SSH Feedback** form to submit detailed feedback on improvements or new content ideas for RDP-SSH. ***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.	Use the **RDP-SSH Kudos** form to submit kudos on the page. Kudos will help us improve our wiki content overall! ***Please note*** the link to the page is required when submitting kudos!