Configure an On-Demand Tech Support SSH Tunnel for Umbrella Virtual Appliances

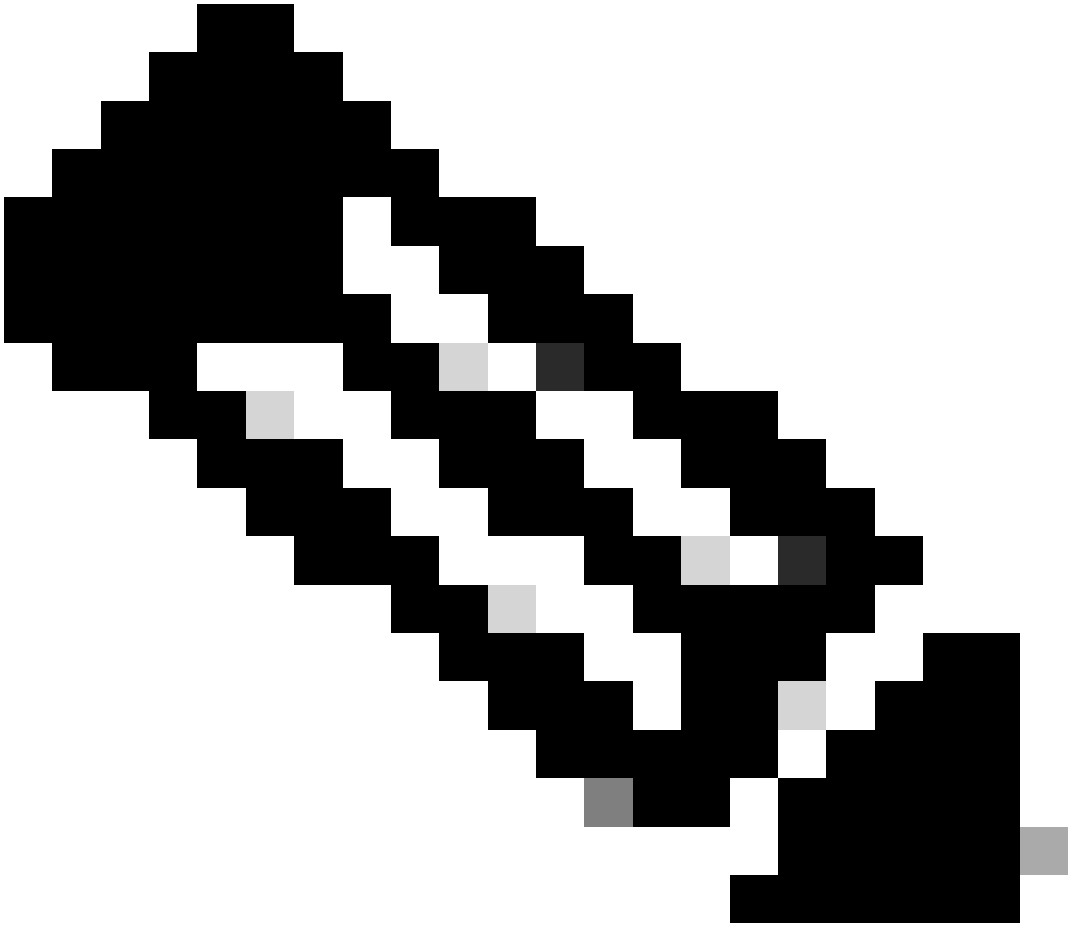
Contents

Introduction

This document describes the configuration of an on-demand tech support SSH tunnel for Umbrella virtual appliances.

On-demand tech support SSH tunnel

A support engineer can request remote access to your virtual appliance (VA) in order to further diagnose a support case and possibly review or update settings to improve the VA availability. In order for an Umbrella support engineer to gain access to an Umbrella VA on-prem at your location, these guidelines must be followed.



Note: This information only applies to VA with version 2.1.0 or above.

Prerequisites

- All requirements for configuring a VA on either VMWare or Hyper-V from the setup documentation must be met.
- Any firewall must be configured in order to allow outbound connections to **s.tunnels.ironport.com.**
- The VA tries connecting on TCP ports 22, 25, 53, 80, 443, or 4766 in succession.

To test connectivity, you can telnet to the support tunnel:

telnet s.tunnels.ironport.com 25

Trying 63.251.108.107...

Connected to s.tunnels.ironport.com.

Escape character is '^]'.

SSH-2.0-OpenSSH_6.2 CiscoTunnels1

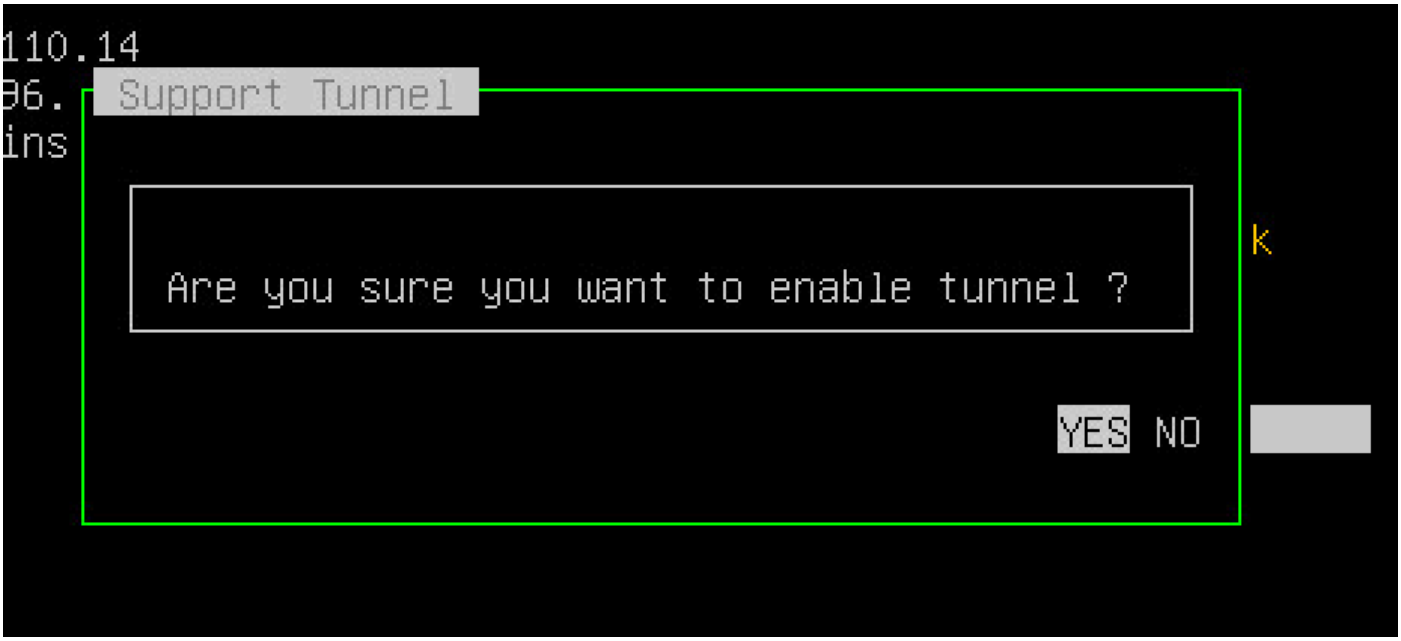
Enabling the tunnel

The SSH tunnel connects to **s.tunnels.ironport.com.** The duration of the connection is configurable, with a default of 72 hours.

Enabling the tunnel on Virtual Appliances hosted on VMware and Hyper-V

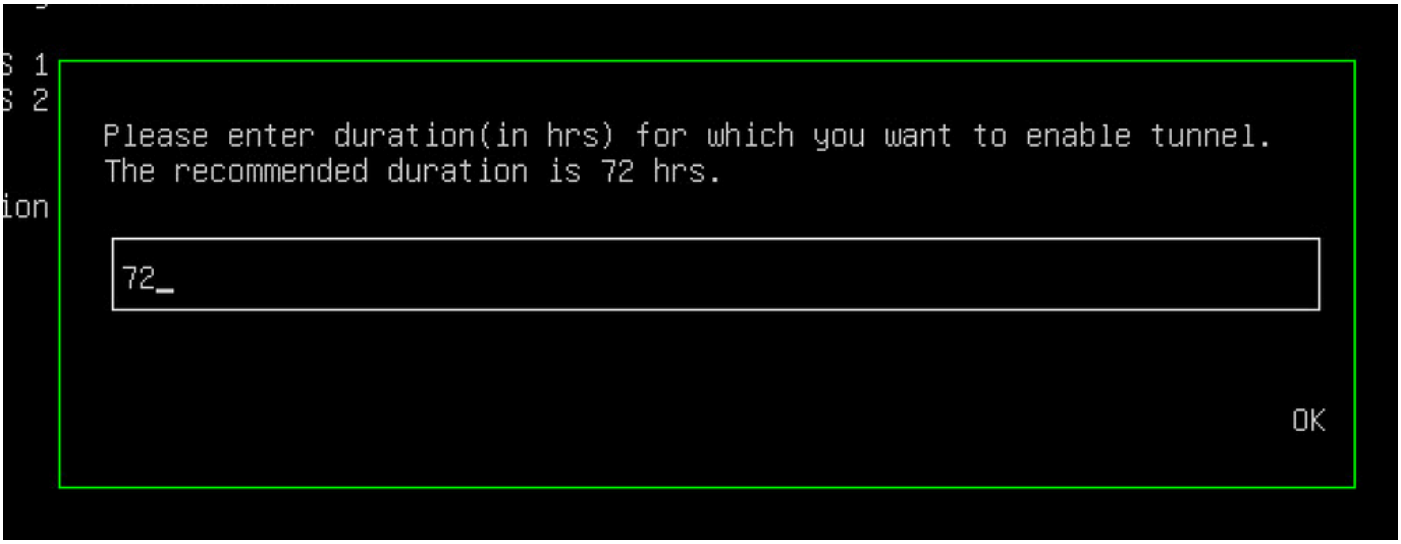
Tunnels can be enabled from VA's console using the keyboard command "CTRL+T".

Select **Yes** when prompted:



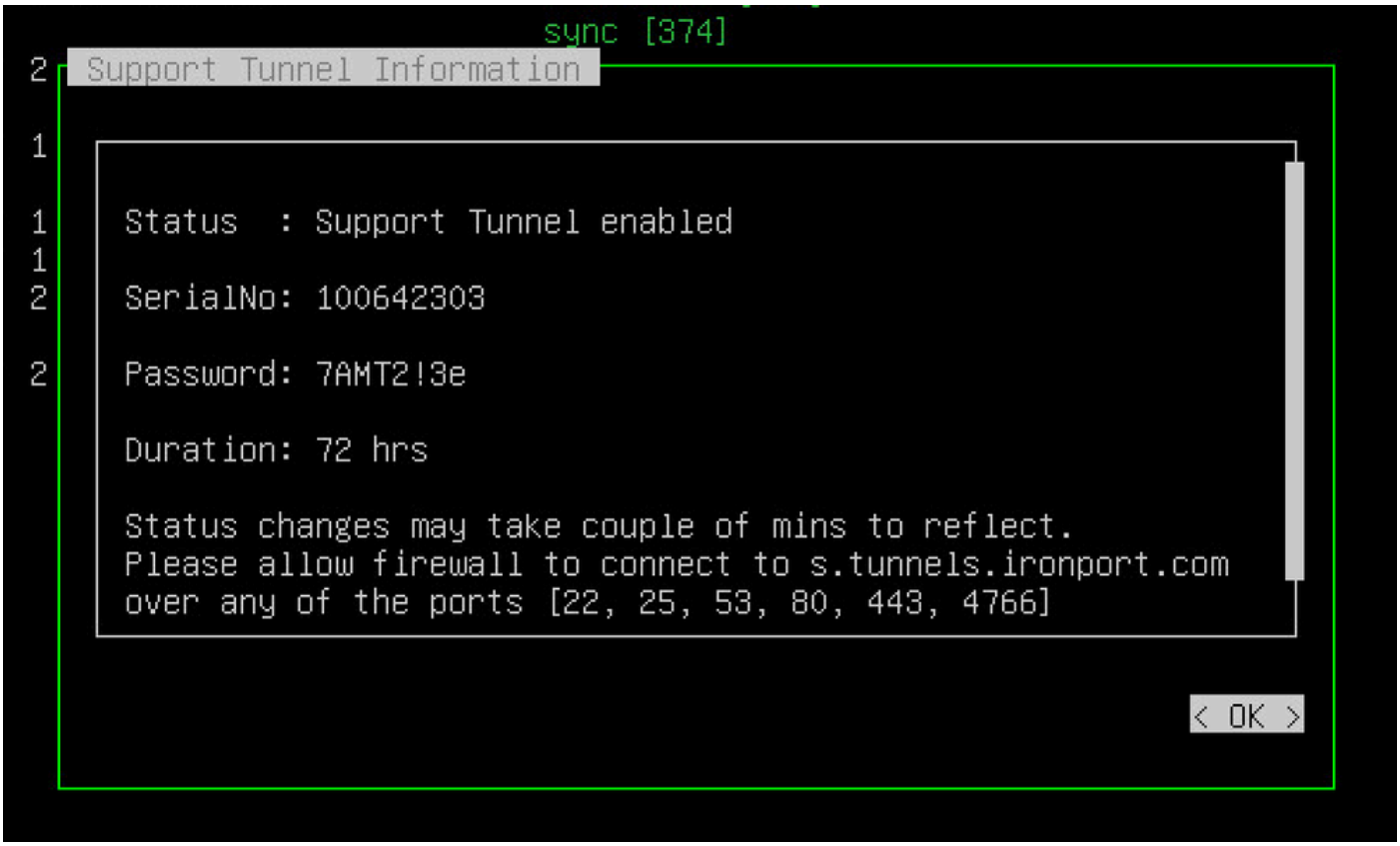
115013855903

First, you are asked to define the length of the tunnel session:



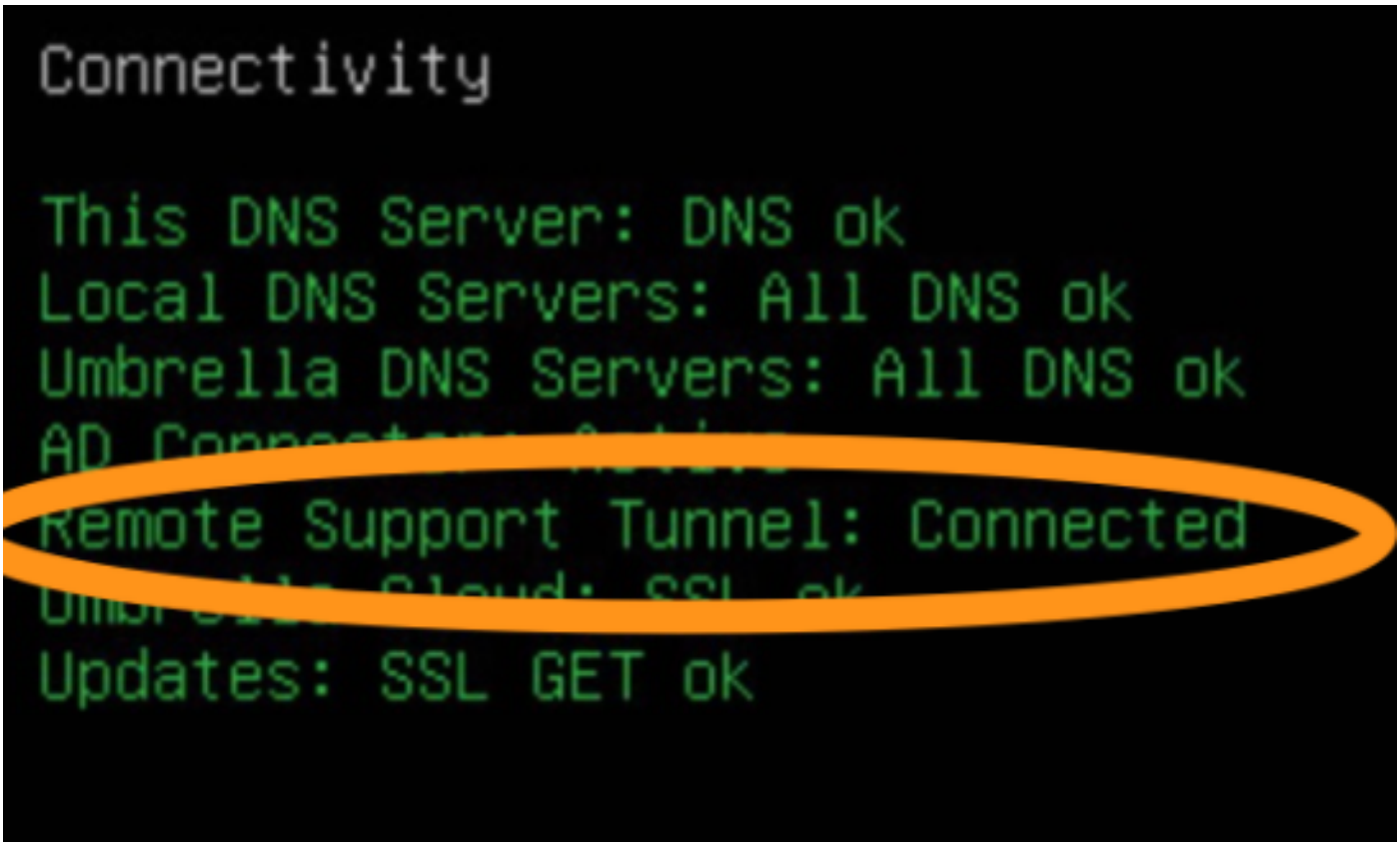
115013856003

Select **OK** and a window appears that shows the serial number and password for the support tunnel. This information must be transmitted to the support technician. After selecting **OK**, the VA attempts to make a connection to the support tunnel server:



115013853243

Click **OK** to close off the window. Verify that the VA console shows "Remote Support Tunnel: Connected".



360000820923

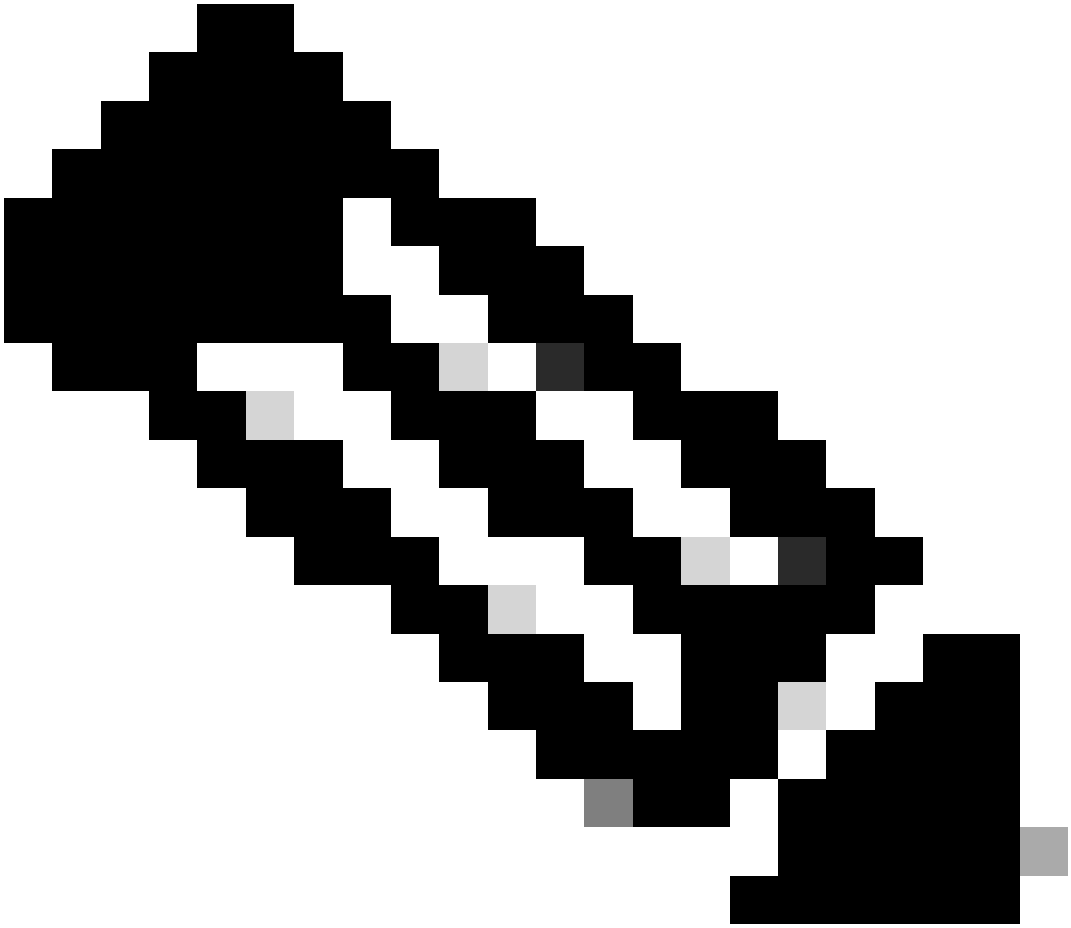
Enabling the tunnel on Virtual Appliances hosted on other platforms

Connect to the VA over SSH and use the config command as below:

- To enable the support tunnel, enter **config tunnel enable <*duration in hours*>**.
- To disable the support tunnel, enter **config tunnel disable**.
- To check the status of the support tunnel, enter **config tunnel status**.
- To view these options, enter **config tunnel help**.

Getting your credentials to share with Support

The serial number and password displayed in the VA's console or when using the *config tunnel status* command must be given to the support technician.

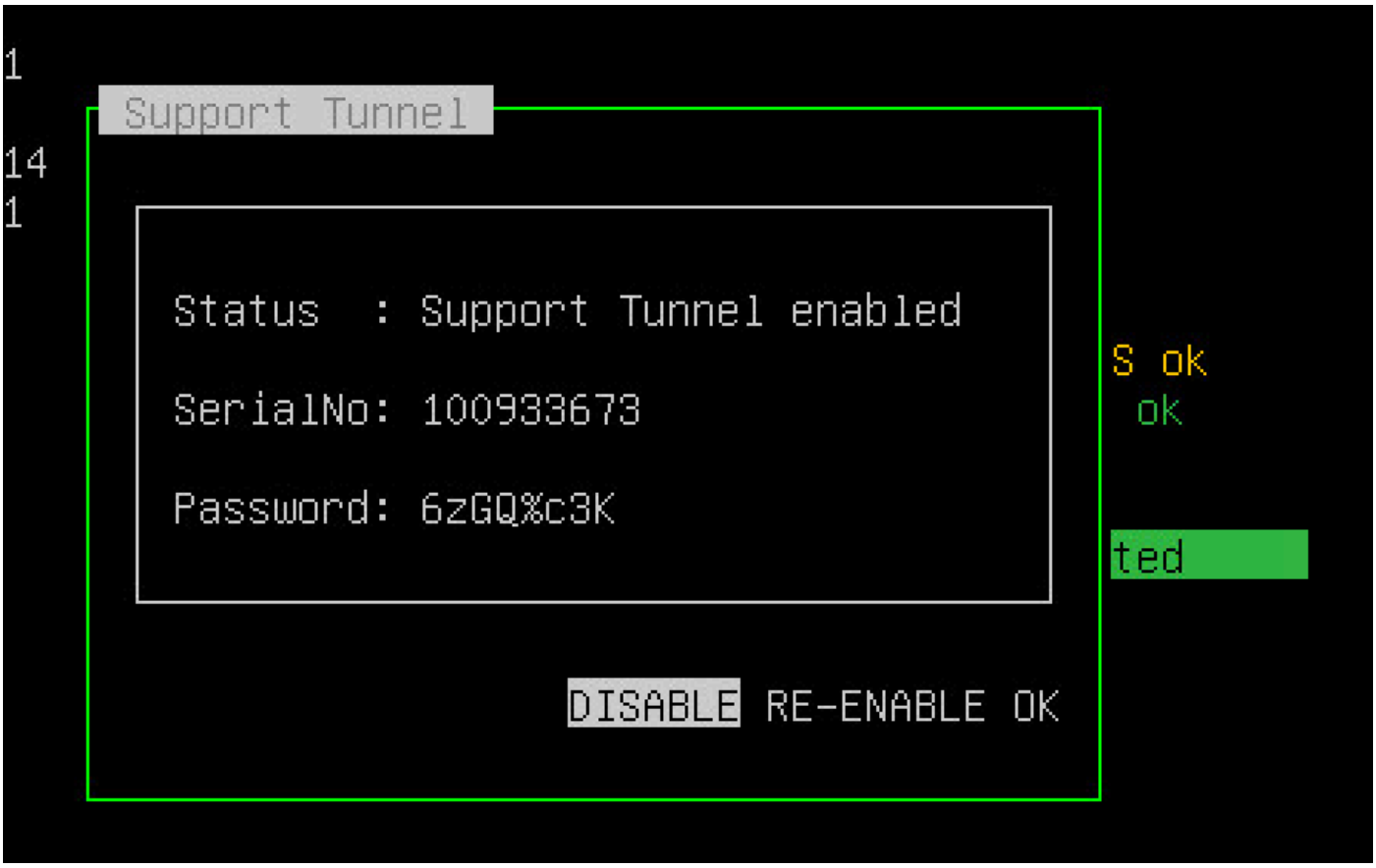


Note: The password you retrieve and share with support cannot be directly used to access the VA. For security reasons the real password is cryptographically derived from the password you see. **To get the serial number and password from the VA console, take a screenshot after enabling the tunnel with Ctl+T. Ensure the screenshot is human readable.**

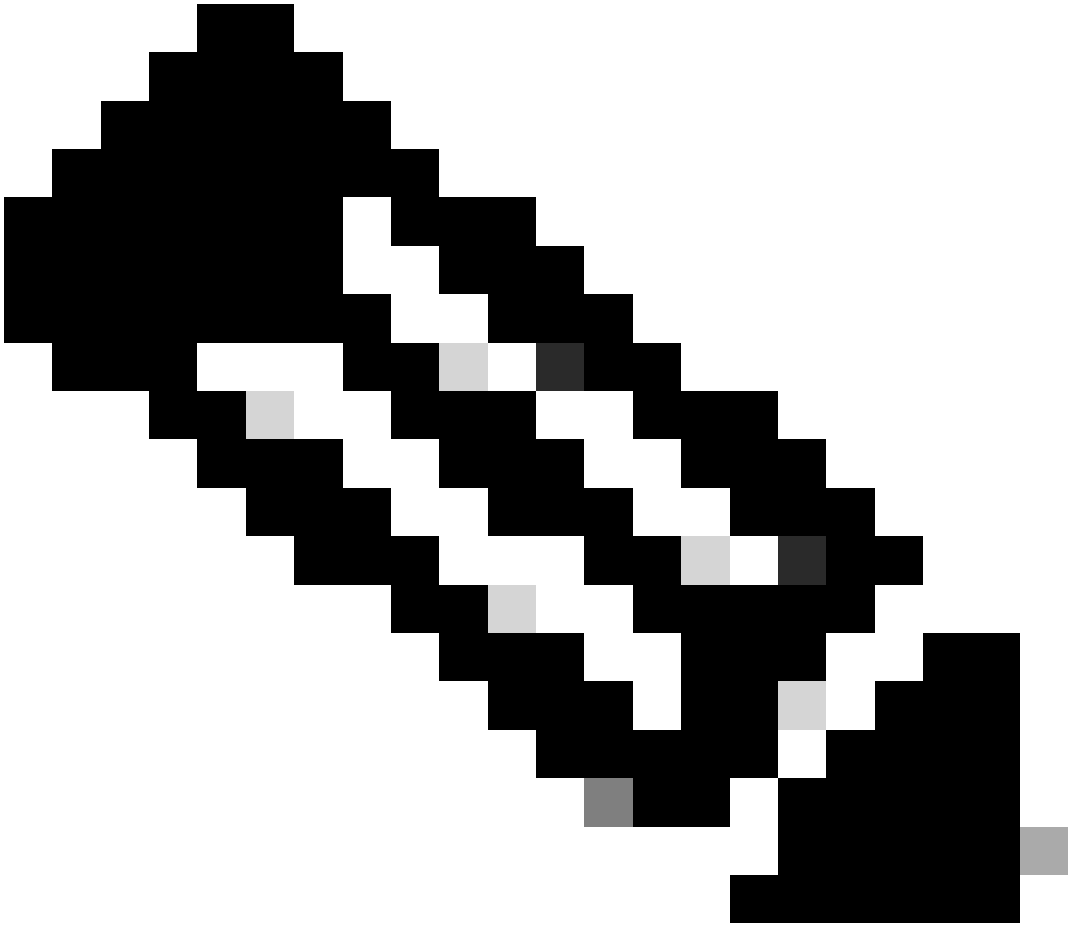
Disabling/Re-enabling the Tunnel

The tunnel remains established for 72 hours by default, however you do have the ability to extend the tunnel duration using the **Re-enable** option.

On VMware and Hyper-V, the tunnel can be disabled or re-enabled at any time with the CTRL-T keyboard command:



115013688906



Note: It can take up to a minute for the tunnel status to change from Connected to Disabled, both in the UI and in the back-end as the tunnel is taken down gracefully rather than terminated.

On other platforms, you can use this command:

- **config tunnel reenable <duration in hours>**

If you try to re-enable the tunnel immediately after disabling it, this can lead to an odd condition and error message as the tunnel is not fully disabled at this stage.

Re-enabling the tunnel does not change the password for the VA's existing tunnel session. By default, selecting the **Re-enable** option adds 72 hours of tunnel duration from the current time.

Tunnel Statuses

Connected

The status changes from **Disabled** to **Connected** as soon you enable the tunnel. If the connection is successful, note that the status stays in Connecting mode for roughly a minute or so as the VA attempts to

establish its tunnel with the server.

Disabled

If you have not explicitly enabled the tunnel, the **Disabled** status shows. Please note that after you have explicitly disabled the tunnel, it takes roughly a minute for the tunnel status to change from **Connected** to **Disabled**.

Connecting

In the connecting state, the VA is attempting to establish the tunnel (trying ports 22, 25, 53, 80, 443, and 4766 sequentially) with a 5 minute delay between each attempt. The VA remains in this state until a connection is established, or 30 minutes have elapsed with no successful connection made.

The connection can fail due to networking issues (for example, blocked ports).

Time out

If the VA is unable to establish a connection with the remote server, then the status goes to **Time out**. The time out occurs roughly 30 minutes after the VA has attempted to establish a tunnel with the remote server.

Tunnel Persistence

Once a support tunnel is enabled, the VA respects the duration value entered even if the VA is rebooted or upgrades. No additional actions are needed by you. If the VA reboots, or upgrades, and time is still remaining in the specified duration, the VA attempts to reconnect to the SSH tunnel server automatically.