

RDX® QuikStation®

Security Patch Instructions

November 2023

Preface

This Product Information Bulletin announces the release of a new set of software patches for the RDX QuikStation 4 and QuikStation 8 firmware. These patches are designed to enhance the security of the QuikStation by addressing a number of Common Vulnerabilities and Exposures (CVE) issues. The patches will successfully install on any QuikStation running the 3.x.x.x firmware, but we do recommend always using the most recent firmware release (currently 3.2.1.2 as of the release of these patches).

Process Overview

The use of Bitvise as a tool in this document is intended to facilitate ease of use. Use Bitvise on Windows systems to ease the process of generating SSH key pairs and copying files to the QuikStation, or use the tools you're comfortable with. Either will work.

Here is a high level overview of the general steps required to apply the patch:

1. Generate SSH key-pairs
2. Upload SSH key to QuikStation
3. Upload patch file
4. Extract patch scripts from patch file
5. Set permissions on the scripts
6. Run patch scripts

Obtain the Required QS-Patch.tar file

The use of Bitvise as a tool in this document is intended to facilitate ease of use. Use Bitvise on Windows systems to ease the process of generating SSH key pairs and copying files to the QuikStation, or use the tools you're comfortable with. Either will work.

1. The necessary scripts are in the "QS-Patch.tar" file. They are:
 - "QS-security-patch.sh"
 - "webinterface.sh"
2. Download the file from [here](#).

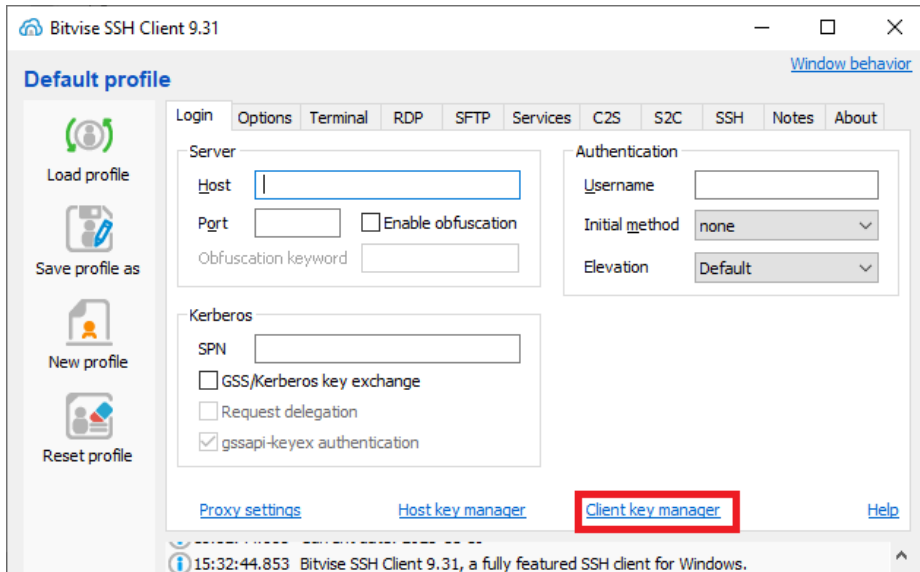
SSH Client Prerequisites

Download Bitvise and install on Windows

1. Use the Bitvise client to assist with SSH connections and key management. The latest release can be found here: <https://www.bitvise.com/ssh-client-download>
2. Install Bitvise using all the default settings.

Generate and export SSH public/private keypair

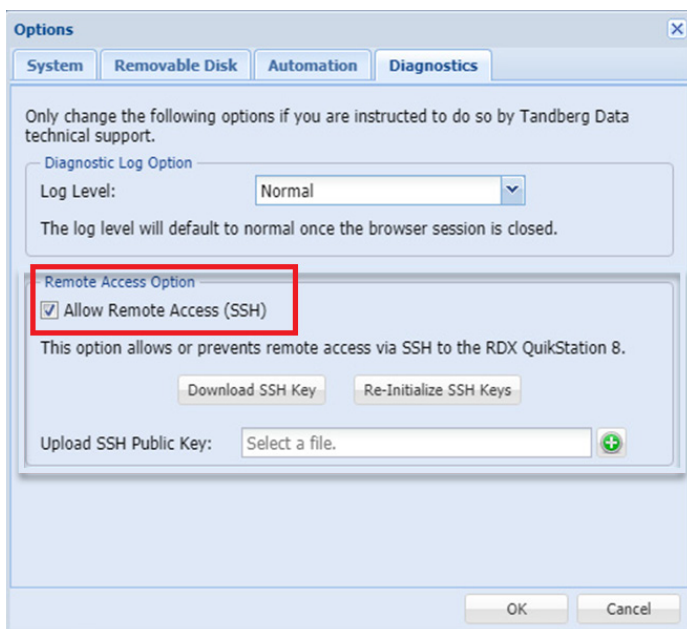
1. Launch Bitvise.
2. Click on Client Key Manager.



1. Generate a key by clicking "Generate New".
2. In the window that pops up, enter a passphrase and click "Generate".
3. Select the Key you just generated and click the "Export" button.
4. Select the OpenSSH format and click "Export".
5. Place the key where you can access it later.

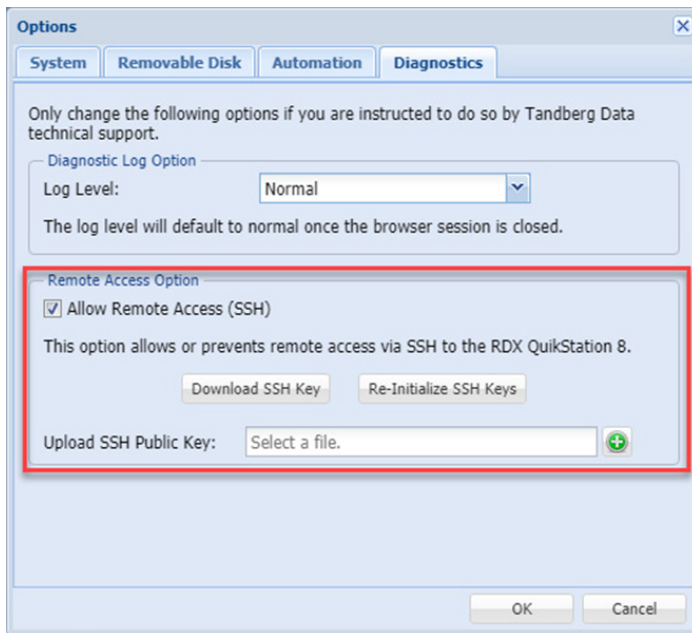
Enable remote SSH access to the QuikStation

1. From the Remote Management Console main menu for the QuikStation, select **System Settings > Options**.
2. Under the **Diagnostics** tab, select the **Allow Remote Access (SSH)** option and select **OK** to permit the use of SSH to access the RDX QuikStation.



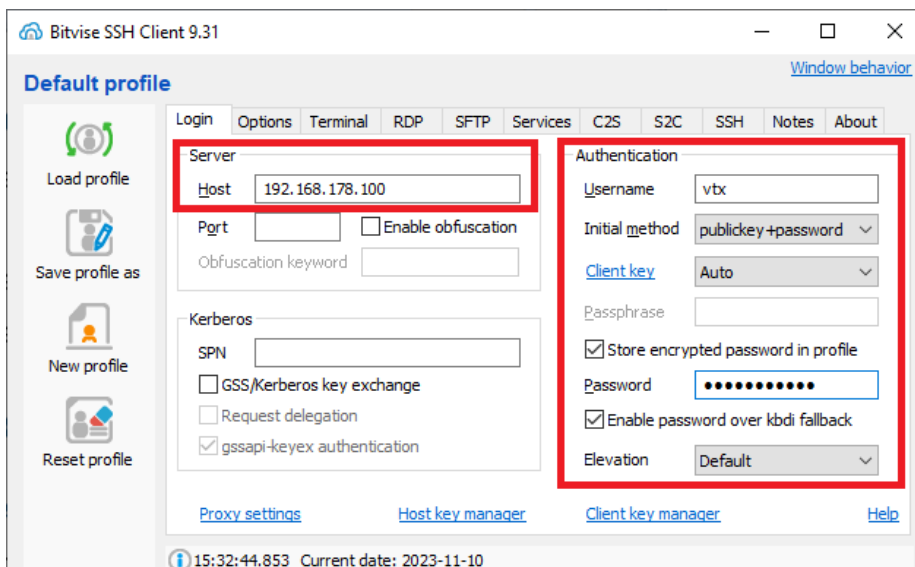
Upload the Public SSH Key to QuikStation

1. From the Remote Management Console main menu for the QuikStation, select **System Settings > Options**.
2. Switch to the **Diagnostics** tab.
3. Click the green plus icon to the right of **Upload SSH Public Key**.
4. Using the file explorer that pops up, navigate to the location where you saved the public key and select **Open**.
5. Click **OK** again to close the System Settings options dialog box and upload the key.

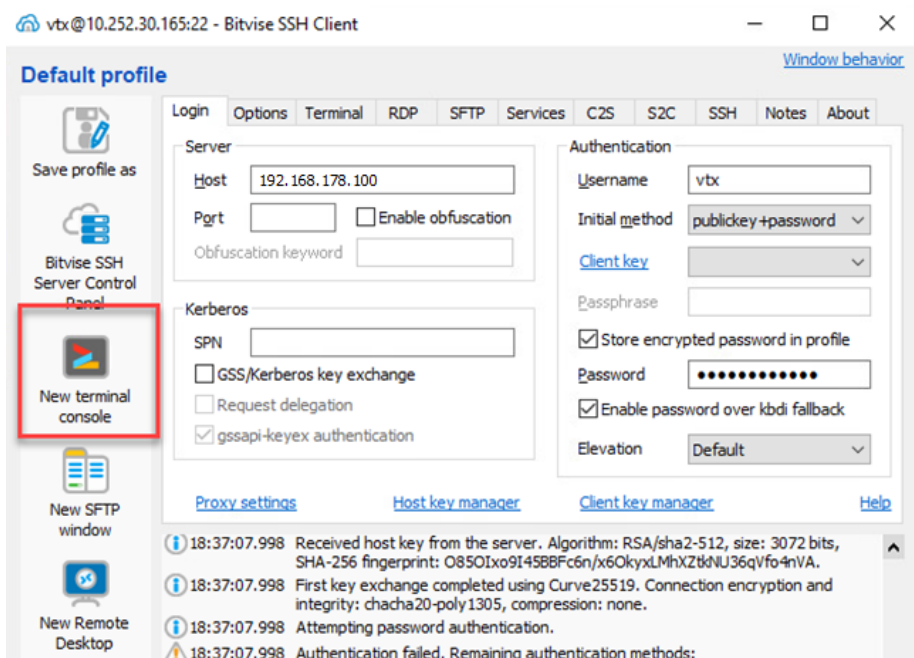


Connect to QuikStation

1. Set the Host to the **<ip address of your QuikStation>**
2. In the Authentication Section, set the Username to **vtx**
3. Set the Initial method to **publickey+password**
4. Set Client key to **Auto**

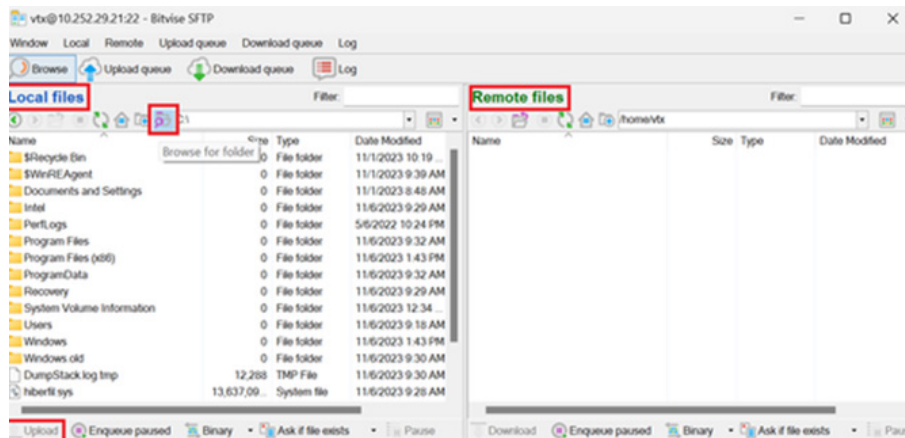


5. Select **Log In**, then **Accept and Save** to make the SSH connection to QuikStation.
6. When prompted, enter the passphrase you used when generating the key.
7. Once the client is connected, you will see additional icons on the left of the window, such as **New terminal console** and **New SFTP window**.



Copy the QS-Patch.tar file to the QuikStation via SFTP or SCP

1. In Bitvise, with an active session (created in the previous section), select **New SFTP Window**.
2. In the SFTP window that pops up, select the **Browse for folder** icon.
3. Navigate to the folder where you stored the QS-Patch.tar file, and click "OK".



4. Select the QS-Patch.tar file from the **Local files** section on the Left and click the **Upload** icon.
5. When successful, you will see the uploaded file in the **Remote files** section on the Right. The default upload location on the QuikStation is the `'/home/vtx'` directory. This is the recommended location.

Extract Scripts from QS-Patch.tar file

1. Open a shell session on the QuikStation from the **New terminal console** icon in Bitvise, or using the tool of your choice.
2. Verify the presence of the file by running this command: **ls**
You should see QS-Patch.tar listed.
3. Extract the scripts from the file with this command: **tar -xvf QS-Patch.tar**. Then, issue **ls** again.
You should see both **QS-security-patch.sh** and **webinterface.sh** listed.

Make the Scripts Executable

From the terminal, make both scripts executable with this command:

chmod +x QS-security-patch.sh webinterface.sh

You will not see any output when the command is run successfully.

Run the QS-security-patch.sh Script

1. From the terminal, execute the following command to run the script: **./QS-security-patch.sh**
You should see the following output:
Stopping Apache: OK
Stopping ntpd: OK
Status: Successfully completed

NOTE: If you attempt to run the script and you see "**Permission denied**", please see '**Make the Scripts Executable**' to resolve this error.

2. Implement the changes by rebooting the QuikStation with this command: **reboot**

Enabling and Disabling the Web Management Interface

After applying the security patch, the Web Management Interface will be disabled. Should you need to enable it for configuration purposes, you will need to SSH into the QuikStation with the New Terminal Console tool from Bitvise, or the tools of your choice, and use the **webinterface.sh** script. It is important to remember that when you enable the Web Management Interface, it will remain active (and thus the system insecure) until the QuikStation loses power, is rebooted, or until you manually disable the Web Management Interface with the **webinterface.sh** script (which is recommended).

Enabling

Enable the Web Management Interface with this command:

./webinterface.sh enable

You will see the following output:

```
Web Interface has been started and will run until manually stopped or the
system is rebooted
```

Disabling

Keeping the Web Management Interface enabled leaves security vulnerabilities accessible. To disable the Web Management Interface, use this this command:

./webinterface.sh disable

You will see the following output:

```
Web Interface has been stopped and will remain stopped until manually started
```