How to Root Login to an RDX® QuikStation®

September 2020

Description

The QuikStation root level login over SSH can be accomplished by creating a RSA public/private key pair and registering the public key with the QuikStation Web Management Interface. Two common methods (Linux and Windows PuTTY) are described below along with instructions for converting OpenSSH private keys to the PuTTY-compatible PPK format.

⚠ CAUTION: To prevent unauthorized access in secure environments to your QuikStation, always protect access to the private keys.

NOTE: If desirable, a single key pair can be used for all QuikStations on your network. Simply register the same public key via the QuikStation Web Management Interface for all QuikStations on the network and then reference the same private key as described in the instructions below.

Solutions

Use one of the following methods to login to your QuikStation. Basically, a key pair is generated and then it is used to login.

- Windows Method To Create Key Pairs
- Linux Method To Create Key Pairs
- Disable QuikStation SSH Access
- Removing All Public Keys

Windows Method To Create Key Pairs

This procedure uses the open-source PuTTY and PuTTYgen applications for generating public/private key pairs and connecting to the QuikStation. This generated key pair can also be used for Linux access.

PuTTY and PuTTYgen can be downloaded here.

Create Key Pair with PuTTYgen

1. Start the **PuTTYgen** application.
2. In the **Actions** pane, click **Generate**.
3. Move the **mouse** to generate the key.
4. Click **Save public key**.
5. Copy the **public key** to a location accessible by the QuikStation Web Management Interface to allow root-level access.
   a. Direct a browser to the QuikStation **name** or **IP address**.
   b. Navigate to **System Settings > Options** menu.

- **c.** At the **Options** window, select the **Diagnostics** tab.
- **d.** Enable **SSH Access**.

  NOTE: If SSH has not been enabled before, press **OK** and re-navigate to the **Diagnostics** tab (Steps b–c).

- **e.** Click the **green plus sign** (+) to the right of the **Upload SSH Public Key** entry box.
- **f.** Select the **public key** portion of the public/private key pair and click **OK**.

  The QuikStation may now be accessed via SSH using the private key portion of the public/private key.

6. Optionally, save the OpenSSH **private key**.

   Save this key to a location to be used for a Linux SSH connection to the QuikStation. This private key may be used to connect using the method described in Step 6 of Linux Method To Create Key Pairs.

Connect to QuikStation Using PuTTY

This describes how to connect to the QuikStation via SSH using the PuTTY application. The private key is assumed to exist and the public key installed on the QuikStation. See above for key generation and installation instructions.

1. Open the **PuTTY** application.
2. In the **Category** pane on the left, select **Session**.
3. Select the **SSH Connection type**.
4. In the **Hostname (or IP address)** field, enter the QuikStation **IP address** or **Hostname**.
5. In the **Saved Sessions** field, enter a **name** for the session.

   This may be any name desired.
6. In the **Category** pane, select **Connection > Data**.
7. In the **Auto-login user name** field on the right, enter **vtx**.
8. In the **Category** pane, click the minus (-) to close the **Connection > Data** menu tree.
9. Select the **Auth** menu.
10. In the **Authentication parameters** pane on the right, click **Browse**.
11. Navigate to the **location** where the Private Key (*.ppk) file has been saved from the PuTTYgen application and select it.
12. In the **Category** pane, select **Session**.
13. Verify that the session name is correct and click **Save**.
14. To connect to the QuikStation, at the bottom of the application pane click **Open**.

A shell window with a hash-prompt should appear and the output of `uname -r` should reflect the QuikStation model. For example:

```
# uname -r
1.2f-qs8
```

Convert Linux OpenSSH to PuTTY File

Beginning with an existing OpenSSH key pair as created above under Linux Method To Create Key Pairs, these steps convert it into a *.ppk file for use with PuTTY.

1. Open **PuTTYgen** and select **Conversions > Import key**.

2. Navigate to the **OpenSSH private key** and open it.
3. From the **Actions** pane, click **Save private key**.
4. Save the *.ppk private key in a **location** that will be accessible by the PuTTY application.

Reference the *.ppk private key from the PuTTY session as described above in Windows Method To Create Key Pairs.

Linux Method To Create Key Pairs

This describes the Linux command-line method to create OpenSSH key pairs for connecting to the QuikStation via SSH. This procedure will create a key pair within a special directory so any default keys will not be overwritten.

1. Create a **directory** for the new key pair.

```
%> mkdir ~/.ssh/quikstation
```

2. Generate public/private **RSA key pair**.

```
%> ssh-keygen -t rsa -b 2048 -C "Key for BackupQStore.MyNetwork.com"
```

3. Enter the **base filename** for the key pair (the public key will get a ".pub" extension added to it automatically).

```
Enter file: /home/<user>/.ssh/quikstation/openssh_key
```

4. Enter a **passphrase** for the key. (Leave blank if this is for automated operations.)

```
Enter passphrase (empty for no passphrase):
```

5. Copy the **public key** to a location accessible by the QuikStation Web Management Interface to allow root-level access.

   a. Direct a **browser** to the QuikStation name or IP address.

   b. Navigate to **System Settings > Options** menu.

   c. At the **Options** window, select the **Diagnostics** tab.

   d. Enable **SSH Access**.

   NOTE: If SSH has not been enabled before, press **OK** and re-navigate to the **Diagnostics** tab (Steps b–c).

   e. Click the **green plus sign** (+) to the right of the **Upload SSH Public Key** entry box.

   f. Select the **public key** portion of the public/private key pair and click **OK**.

   The QuikStation may now be accessed via SSH using the private key portion of the public/private key.

6. Login to the QuikStation.

```
%> ssh -l vtx -i ~/.ssh/quikstation/openssh_key <quikstation-IP/Name>
```

A hash-prompt should appear. The output of `uname -r` should reflect the QuikStation model. For example:

```
# uname -r
4.1.2f-qs8
```

Specify Unique Private Key for QuikStation Auto-Login

Normally, the key pair is created in a separate directory to avoid any accidental modification of the user's default SSH keys. Therefore, the private key must be specified in the SSH command line.

Alternatively, the login information may be stored in the **~/.ssh/config** file to automatically login to the QuikStation. The following example references a unique key for the login to a QuikStation on the network with the name “BackupQStore.MyNetwork.com”.

NOTE: An IP address can be used instead of a hostname.

```
Private Key: ~/.ssh/quikstation/private_key
File Contents: ~/.ssh/config
Host BackupQStore.MyNetwork.com
User vtx
IdentityFile ~/.ssh/quikstation/private_key
```

Disable QuikStation SSH Access

This procedure disables SSH access to the QuikStation but leaves all the installed public keys in place.

1. Direct a **browser** to the QuikStation name or IP address.
2. Navigate to **System Settings > Options** menu.
3. At the **Options** window, select the **Diagnostics** tab.
4. Uncheck the **Allow Remote Access (SSH)** box.
5. To disable SSH access, click **OK**.

Removing All Public Keys

This procedure removes all existing access keys from the QuikStation. All subsequent access requires the installation of the public keys.

1. Direct a **browser** to the QuikStation name or IP address.
2. Navigate to **System Settings > Options** menu.
3. At the **Options** window, select the **Diagnostics** tab.

⚠ CAUTION: The next button will *execute immediately* after clicking to reinitialize the SSH keys and cannot be undone. Exit if this is not what you want to do.

4. Click **Re-Initialize SSH Keys**.

   The SSH keys are now reinitialized.

More Information

For information on RDX QuikStation appliances and other Overland-Tandberg products, visit our Knowledge Base at:

https://www.overlandtandberg.com/knowledgebase/