EXAMPLE RING TO C. How to Connect Your Push3 Gateway to a SFTP Server

To connect to your Gateway UI, use its IP. Find it by logging into your https://api.ekmpush.com/ account, navigate to your Gateway MAC Address on the left-hand side, and click on the displayed IP (e.g., LAN IP: 192.168.0.3) under 'LAN IP':

EKM PUSH3	🌢 🔶 🤞 🛛 v0.	9.28 .567	ocal appsrv		
Account API Query	Account is o	wned by: Gatewa	y 4016fa		
Meters	Status	Triggers	Configuration	System	Trigger log
00035	Status				
IOStacks	Last status update: 2023-12-19 15:23:58 (2m 29s) Last Push3 restart: 2023-12-19 10:14:57 (5h 11m 29s)				
000000	Last OS r	eboot: 2023-12	2-19 10:08:30 (5h 1	5m 28s)	
000000	LAN IP: 192.168.0.3 C Network interface: wlan0 (wireless) Average cycle interval: 4.309 seconds				
Gateways					
4016	Cycle cou	int: 4000			

Log into your Gateway UI, navigate to Settings > SFTP/Archive, and select *Enable SFTP*. Next, you will find explanations on how to connect using either *User/Password* or *Perform client authentication using public/private key*.

For our example server, the login details are as follow:

Host: 192.168.0.10

User: test

Password: Test123

Using User/Password Authentication

If you only have the IP, username, and password of your remote server where you want to save your files, you can fill them into the corresponding inputs, like this::

Host: 192.168.0.10

- User: test
- Password: Test123

Finally, press the 'Apply' button to save the filled configurations.

You have to wait for at least 15 minutes to check if the data has been successfully saved to the server.

Using a Private Key for Authentication

If you already have experience with Private/Public Keys and don't need to follow the next steps because you already have your own Private Key, select *Perform client authentication using public/ private key*. Copy your Private Key (yes, it is the Private Key; we are not wrong) and paste it into the *Private Key* blank space. Also, ensure that your Public Key is added to your remote server in ~/.ssh/authorized_keys. Finally, press the '**Apply**' button to save the filled configurations. Wait at least 15 minutes to check if the data has been successfully saved to the server.

If you don't have enough experience, don't stress! We're here to help you. This is a more advanced guide where we'll explain how you cancreate your own keys using Linux or Windows.

Create your Private Key in Linux

You can create your **Private Keys** on your server or on another Linux server by following these instructions:

- 1. Open your terminal and run: ssh-keygen -m PEM
- 2. If you don't want to create it with a passphrase (password), simply press ENTER every time the terminal prompts you. You will see something like:

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/myLaptop/.ssh/id_rsa):(Simply press
ENTER)
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/myLaptop/.ssh/id_rsa
Your public key has been saved in /home/myLaptop/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:iB5mwc8jFw7jeb31tNWlp20LKsosDoS10zWuThNkzLM myLaptop@myLaptop
The key's randomart image is:
+----[RSA 3072]----+
   0_0...|
  ..E= = oo .. .o|
   .+.Xo+.o.o o +|
    +B+*+ o + = | +B+ooS + |
   +0+.
   0.
   .0
                 .0
+----[SHA256]----+
```

After this, you have to save the **Public Key** in the *authorized_keys* file. If you create your keys on the same server where you want to save files, you can rur cat ~/.ssh/id_rsa.pub > .ssh/authorized_keys

If you want to add extra security to your key, you can create it with a passphrase (password):

```
Generating public/private rsa key pair.
```

```
Enter file in which to save the key (/home/myLaptop/.ssh/id_rsa):(Simply press
ENTER)
Enter passphrase (empty for no passphrase): YOUR_SECURE_PASSWOR_HERE
Enter same passphrase again:REPEAT_YOUR_SECURE_PASSWOR_HERE
Your identification has been saved in /home/myLaptop/.ssh/id_rsa
Your public key has been saved in /home/myLaptop/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:iB5mwc8jFw7jeb31tNWlp20LKsosDoS10zWuThNkzLM myLaptop@myLaptop
The key's randomart image is: +---[RSA 3072]----+
   0_0.
             .0..|
| ..E= = oo .. .o|
   .+.Xo+.o.o o +|
    +B+*+ 0 + = |
| +B+ooS . +
               +0+.
    0.
               .0
  .o | +----[SHA256]----+
```

Finally, copy your **Private Key**. You can view it in the console by running: cat ~/.ssh/id_rsa. Copy the file content and paste it into the Gateway UI (in this example, we are using 192.168.0.3). Navigate to Settings > SFTP/Archive and select *Enable SFTP*.

- Host: 192.168.0.10
- User: test
- **Password:** If you added a passphrase (password), you have to add it here; if not, leave the space blank.
- Select: Perform client authentication using public/private key
 - Paste your *Private Key* in the Private Key box.

If you've used a passphrase, you should see something similar to:

✓ Enable SFTP
Host U
192.168.0.10
Username (i)
test
Password (i)
•••••
Note: this password will be stored on your gateway device in cleartext
Perform client authentication using public/private key
Private Key 🤳
9TCZJUHBFAXZKN9WZCC8T4SST+WPHRVUCR4VNZ6NQUNUVWTErNJVIEEZ+ZDUIJC6 4NY1enMj4SxdCcATFlyJ+kdIKVaV06B6K32McLztNngqRJ658z+sB2fNLINRyL1x 1HVTNRZ1m3YdhZ6Aa2vORlkyqBSt22jdLdHASGKu9o/bfIBwqH0mCAwpMRUrRTHx s7ie2aTc0G7G7XTefdGJb2Iv4S8VVK9g9YqR0/9HHrEkci07sUXD4A== END RSA PRIVATE KEY

You have to wait for at least 15 minutes to check if the data has been successfully saved to the server.

Create your Private Key in Windows using putty

You can create your **Private Keys** on your Windows computer by following these instructions:

- 1. Download the puttygen.exe software from its official web page: <u>https://www.chiark.greene</u> <u>nd.org.uk/~sgtatham/putty/latest.html</u>
- 2. Execute it.
- 3. At this point, you can create your key using RSA with either 2048 or 4096 bits in the 'Number of bits in a generated key'.

😴 PuTTY Key Generator			? ×
<u>File Key Conv</u> ersions <u>H</u> elp			
Key No key.			
Actions Generate a public/private key pair			Generate
Load an existing private key file			Load
Save the generated key		Save p <u>u</u> blic key	<u>S</u> ave private key
Parameters			
Type of key to generate: ● <u>R</u> SA ● ○ <u>D</u> SA	⊖ <u>e</u> cdsa	◯ EdD <u>S</u> A	○ SSH- <u>1</u> (RSA)
Number of <u>b</u> its in a generated key:			4096

4. After selecting these two options, press the 'Generate' button, and then move your mouse over the blank area.

😴 PuTTY Key Generator		? ×
<u>File K</u> ey Con <u>v</u> ersions <u>H</u> elp		
Key No key.		
Actions		
Generate a public/private key pair		<u>G</u> enerate 🗸
Load an existing private key file		Load
Save the generated key	Save p <u>u</u> blic key	Save private key
Parameters		
Type of key to generate: <u>R</u> SA <u>D</u> SA <u>E</u> CD	SA ⊖EdD <u>S</u> A	○ SSH- <u>1</u> (RSA)
Number of <u>b</u> its in a generated key:		4096

5. You should see something similar to:

	PuTTY	Kev	Gene	erator
--	-------	-----	------	--------

8

<u>File Key Conversions Help</u>

Ney Dublic Loss (conservice		having dialation Maria		
Public key for pasting	g into OpenSSH aut	nonzed_keys file:		
+50uFJ18I3pJOIoIM +OtowIBrpErEYpdSi RbacIP+ryqF8iDtpH	IC Tyc2EAAAADAQ/ ILowjRbweDEyYNU 6ilpOCdLWawtfgGF Ljwjm6bjzKqTrXP9h	ABAAACAQC8A+g9v JOF8BID7pbwIH4XjD XHwRrHjwfj4UepbhPo IvvSL6yEc6MqmLyaf	rekzhD2uMnB5gh +9Sg dPxjd1fck9ca9rvQhToV8ZT E82aUYQuvAzymUo9QC2ul	TwQY1BcMtSbfUwb0hkt hxiweSvQA
+12fjm/yGUMsbFJe Key fingerprint:	ssh-rsa 4096 SHA	256:qR77srMYOXhG	fHuGPowrlyz33DXgEg5dHl	JKT1urMBZI
Key <u>c</u> omment:	rsa-key-20231219			
Key p <u>a</u> ssphrase:				
Confirm passphrase:				
Actions				
Generate a public/pr	ivate key pair			<u>G</u> enerate
Load an existing prive	ate key file			Load
Save the generated I	key		Save p <u>u</u> blic key	Save private key
Parameters				
Type of key to gener <u>R</u> SA	ate: O <u>D</u> SA	◯ <u>E</u> CDSA	◯ EdD <u>S</u> A	⊖ SSH- <u>1 (</u> RSA)

6. Select and copy the entire box that says: *Public key for pasting into OpenSSH authorized_keys files.*

😴 PuTTY Key Generator		?	\times
<u>File K</u> ey Con <u>v</u> ersions <u>H</u> elp			
Key			
Public key for pasting into OpenSSH authorize	d_keys file:		
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAA +50uFJ18l3pJOloIMLowjRbweDEyYNUOF8	ACAQC8A+g9vfekzhD2uMnB5gh BID7pbwlH4XjD+9Sg		
+OtowIBrpErEYpdS6ilpOCdLWawtfgGRHwB RbaclP+ryqF8iDtpHLjwjm6bjzKqTrXP9hv +1Zfjm/yGUMsbFJeAp8ehJJg3sMUkfLp	rHiwfi4HaphbPdPvid1fok9ca9crOhToV/8ZTfwOY1Bc Deshacer	M#SbfUwb0hkt	1
Key fingerprint: ssh-rsa 4096 SHA2	Cortar		
Key comment: rsa-key-20231219	Copiar		
Key passphrase:	Pegar		
Confirm passphrase:	Eliminar		- 1
Actions	Seleccionar todo		
Generate a public/private key pair	Lectura de derecha a izquierda	rate	
l oad an evisting private key file	Mostrar caracteres de control Unicode	ad	
Load an existing private Key ne	Insertar carácter de control Unicode	>	=1
Save the generated key	Jave p <u>u</u> blic key <u>J</u> av	re private key	
Parameters			
Type of key to generate: O <u>R</u> SA O <u>D</u> SA	○ <u>E</u> CDSA ○ EdD <u>S</u> A ○	SSH- <u>1</u> (RSA)	
Number of <u>b</u> its in a generated key:	40	96	

• Paste it in your remote server on: ~/.ssh/authorized_keys .

7. If you want to enhance the key security by adding a passphrase (password), enter the passphrase in the provided input:

PuTTY Key Generator	?	\times
<u>File K</u> ey Con <u>v</u> ersions <u>H</u> elp		
Key		
Public key for pasting into OpenSSH authorized_keys file:		
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC8A+g9vfekzhD2uMnB5gh +50uFJ18I3pJOIoIMLowjRbweDEyYNUOF8BID7pbwlH4XjD+9Sg +0towIBrpErEYpdS6ilpOCdLWawtfgGRHwRrHjwfj4UepbhPdPxjd1fck9ca9rvQhToV8ZTfwQY RbacIP+ryqF8iDtpHLjwjm6bjzKqTrXP9hvvSL6yEc6MqmLyaE82aUYQuvAzymUo9QC2uhxiwe3 +1Zfjm/yGUMsbFJeAp8ehJJg3sMUkfLp0eai8UAPdsvh44KpDcepLcrWL/3+	1BcMtSbfUwb0hkt SvQA	Ι
Key fingerprint: ssh-rsa 4096 SHA256:qR77srMYOXhGfHuGPowrlyz33DXgEg5dHUKT1u	JrMBZI	
Key comment: rsa-key-20231219		
Key p <u>a</u> ssphrase:		
Confirm passphrase:		
Actions		
Generate a public/private key pair	<u>G</u> enerate	
Load an existing private key file	<u>L</u> oad	
Save the generated key Save public key	<u>S</u> ave private key	
Parameters		
Type of key to generate: <u>R</u> SA <u>D</u> SA <u>E</u> CDSA <u>EdDS</u> A	○ SSH- <u>1</u> (RSA)	
Number of <u>b</u> its in a generated key:	4096	

- 8. Export your **Private Key**: Go to Conversions > Export OpenSSH Key and save it in a secure place.
- 9. Finally, copy the content of your converted **Private Key** and paste it into the Gateway UI (in this example, we are using 192.168.0.3). Navigate to Settings > SFTP/Archive and select *Enable SFTP*.
 - Host: 192.168.0.10
 - User: test
 - **Password:** If you added a passphrase (password), you have to add it here; if not, leave the space blank.
 - Select: Perform client authentication using public/private key
 - Paste your *Private Key* in the Private Key box.

If you've used a passphrase, you should see something similar to:

Enable SFTP
Host 🕕
192.168.0.10
Username U
test
Password U
•••••
Note: this password will be stored on your gateway device in cleartext
Perform client authentication using public/private key
Private Key 🤳
9TCZJUHBFAXZKN9WZCC8T4SST+WPHRVUCR4VNZ6NQUNUVWTErnJVIEEZ+ZDUTJC6 4NY1enMj4SxdCcATFlyJ+kdIKVaV06B6K32McLztNngqRJ658z+sB2fNLlNRyL1x 1HVTNRZ1m3YdhZ6Aa2vORlkyqBSt22jdLdHASGKu9o/bfIBwqH0mCAwpMRUrRTHx s7ie2aTc0G7G7XTefdGJb2lv4S8VVK9g9YqR0/9HHrEkci07sUXD4A== END RSA PRIVATE KEY

You have to wait for at least 15 minutes to check if the data has been successfully saved to the server.