

Set up DMZ on HUAWEI HG8122

Login Steps

Type 192.168.1.1 at Browser and press Enter, to log in can be:

Login first time

1. Enter information

- Account : admin
- Password : password
- Validate Code : enter letters shown below, if they're not clear, press Refresh to change them
- Press Login



2. Page to change Password, with following conditions:

- Password : should contain at least 6 letters
- Comply with at least 2 from 4 combinations: number, lowercase letter, uppercase letter and special characters e.g. ` ~ ! @ # \$ % ^ & * () - _ = + \ | [{ }] ; : ' " < , . > / ? .
- Should not repeat with any word in Username
- Press Apply

HG8122 Logout

The login password cannot be the default one. Change it immediately.


Change Password

User Name:	admin
New Password:	<input type="password"/>
Confirm Password:	<input type="password"/>

1. The password must contain at least 6 characters.
 2. The password must contain at least two of the following combinations: digits, uppercase letters, lowercase letters and special characters. Special characters can be the following: ` ~ ! @ # \$ % ^ & * () - _ = + \ | [{ }] ; : ' " < , . > / ? .
 3. The password cannot be any user name or user name in reverse order.

3. Go back to Login page, enter the information

- Account : admin
- Password : enter the Password
- Validate Code : enter letters shown below, if they're not clear, press Refresh to change them
- Press Login



If passed first time Login, enter information

- Account : admin
- Password : enter the Password
- Validate Code : enter letters shown below, if they're not clear, press Refresh to change them
- Press Login



1. Forward Rules > DMZ Configuration > set up as follows:

- Press New
- Enable DMZ : click a check mark to enable
- Host Address : enter IP Address of device
- Once finished, press Apply to save the setting

On this page, you can configure DMZ parameters. The DMZ device restricts unreliable external connections from linking up to the device. It is a buffer between a secure system and an insecure system. If the WAN port is not listed in the table, the application requests from the WAN connection are forwarded to the DMZ device.

WAN Name	Enable DMZ	Host Address
1_TR069_INTERNET_R_VID_100	<input checked="" type="checkbox"/>	192.168.1.33

Buttons: New, Delete, Apply, Cancel

2. After setting, back to first page, it'll show setup information in a table

On this page, you can configure DMZ parameters. The DMZ device restricts unreliable external connections from linking up to the device. It is a buffer between a secure system and an insecure system. If the WAN port is not listed in the port mapping table, the application requests from the WAN connection are forwarded to the DMZ device.

WAN Name	Enable DMZ	Host Address
1_TR069_INTERNET_R_VID_100	Enable	192.168.1.33

Buttons: New, Delete

3. To delete setup Profile

- Click a check mark in front of Profile
- Press Delete
- A pop up to confirm deletion, press OK

192.168.1.1 บอกว่า
Are you sure you want to delete the current DMZ?

จะพบ pop up ให้ยืนยันการลบ ถ้าต้องการลบกดตกลง

กดปุ่ม Delete

3

1

2

ทำเครื่องหมายถูก

	WAN Name	Enable DMZ	Host Address
<input checked="" type="checkbox"/>	1_TR069_INTERNET_R_VID_100	Enable	192.168.1.33

Enable DMZ: ☒

WAN Name: 1_TR069_INTERNET_R_VID_100

Host Address: 192.168.1.33 TCC-FT21-KOMRA1

Apply Cancel