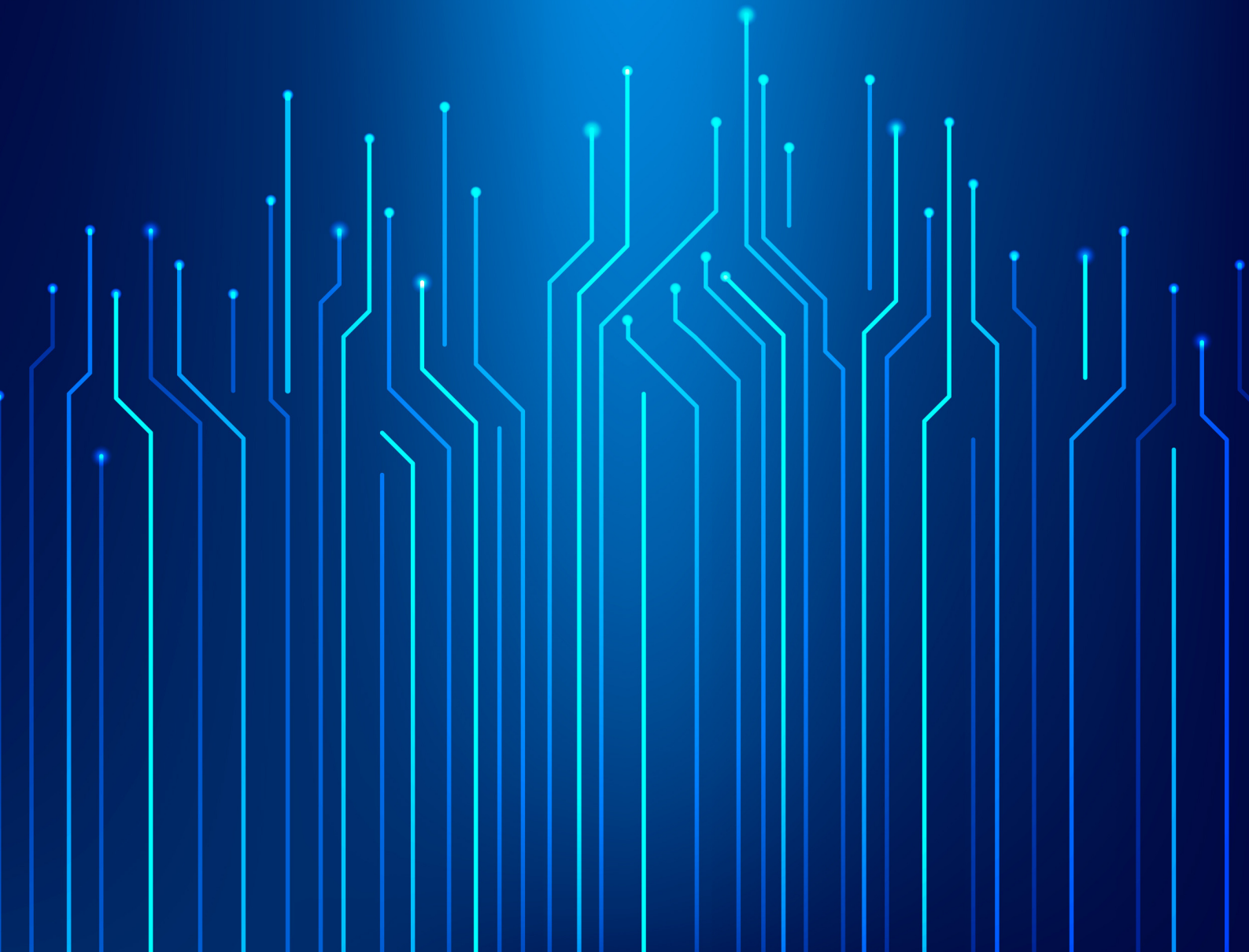


# How to configure Enterprise cloud



# How to configure Enterprise Cloud

**Note: Before configuring Enterprise Cloud on GajShield, make sure you have a cloud license.**

**Note: If you find that CA certificate has been created beforehand, it is the same certificate created under Browsing >> Setup >> SSL Certificate used for scanning https browsing traffic. You have to now configure additional information fields specified below**

The screenshot displays the GajShield web management interface. On the left is a sidebar menu with categories: Definitions, Configuration, Management, Diagnosis, Firewall, VPN, Enterprise Cloud, AntiSpam, APP Filter, DLP, Reports, Browsing, Users Setting, Guest Users, UserSense, Mimes And File Extns, Policy, Quota, Setup, IPS, and Logout. The 'Enterprise Cloud' tab is selected in the top navigation bar. Below it, the 'SSL Certificate' sub-tab is active. The main content area shows the 'Add CA Certificate' form with the following fields and values:

Add CA Certificate	
Certificate Name	GajShieldCACert
Valid Upto	08/30/2022
Key Length	1024
Password	.....
Confirm Password	.....
Local ID	X.509 DN
Country Name	India
State	Maharashtra
Locality Name	Mumbai
Organization Name	Gjahiseld Info
Organization Unit Name	Network Security
Common Name	GajShieldCACertificate
Email Address	admin@gajshield.com

At the bottom of the interface, a copyright notice reads: Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved.

1. Go to Enterprise Cloud tab >> Go to Organization Information and fill in the details to configure cloud service information.

If not, you'll have to add all the CA certificate information under Enterprise Cloud -> Organization Information

Organization Information
Configure Users
Restart Cloud Service

Add CA Certificate

Certificate Name	<input type="text"/>
Valid Upto	<input type="text"/>
Key Length	<input type="text" value="1024"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>
Local ID	<input type="text" value="X.509 DN"/> <input type="text"/>
Country Name	<input type="text" value="India"/>
State	<input type="text"/>
Locality Name	<input type="text"/>
Organization Name	<input type="text"/>
Organization Unit Name	<input type="text"/>
Common Name	<input type="text"/>
Email Address	<input type="text"/>

Add

- **Certificate Name:** A unique name to identify the CA Certificate.
- **Valid up to:** Date till which the CA Certificate is valid, after which the certificate expires.
- **Key Length:** The encryption key size, more the key length, greater the security level & more processing power required.  
Note: Certificate should have key length value set to 1024
- **Password:** The password/passphrase for the CA Certificate.
- **Local ID:** The Local Identifier for the Certificate helps the firewall to identify the CA Certificate.

#FQDN: The Fully Qualified Domain Name (FQDN), FQDN must be in ASCII format. For example, myhost.test.com.

#X.509 DN: An X.509 certificate binds a name to a public key value. The role of the certificate is to associate a public key with the identity contained in the X.509 certificate.

#IP Address: IP address the certificate is associated with. It can be any IP address. For example, 125.11.12.13

#Email: Email address the certificate is associated with. For example, support@gajshield.com

- **Country Name:** Select the country where the firewall is installed.
- **State / Locality Name:** State and Locality are full names, i.e. 'California', 'Los Angeles'.
- **Organization Name:** Full Legal Company or Personal Name, as legally registered.
- **Organizational Unit Name:** In whichever branch of your company the firewall is getting installed. For example, Accounting, IT etc.
- **Common Name:** Common name is a mandatory bit of uniquely identifying data, such as FQDN or Personal Name.
- **Email Address:** Insert support email address in case of issues.

1. **Important:** If your current certificate expires and you need to create a new certificate, under Browsing >> Setup >> SSL Certificate after creating the certificate, go to Enterprise Cloud >>Organization.

Information & click on, without doing any changes in the configuration click on save. After recreating the certificate, you will need to delete the old cloud exe under Configuration Users and create new cloud exe.

2. Select Cloud configuration as required, under Cloud Service Information.

Organization Information    Configure Users    Restart Cloud Service

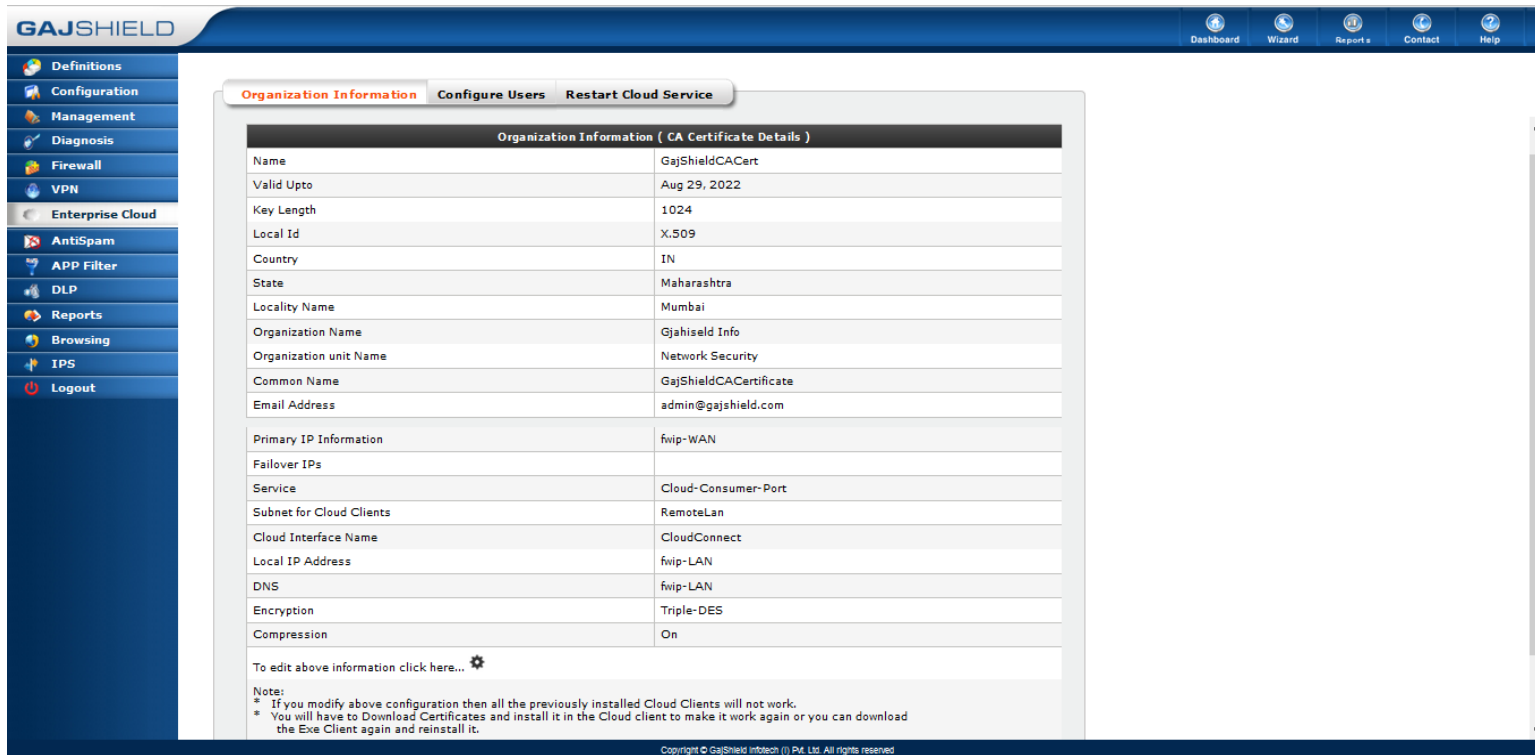
### Cloud Service Information

Primary IP Information	fwip-LAN	NATed Public IP/FQDN:
Failover IPs (Optional)	L3Gateway Radius-Server-IP Tacacsplus-Server fwip-DMZ fwip-LAN fwip-SYNC fwip-TEST fwip-WAN	NATed Public IP/FQDN:
* You can select multiple IPs for failover.		
Service	--Please Select--	* It is recommended to use UDP services.
Subnet for Cloud Clients	--Please Select--	* Please select a network which has not been used on firewall.
Cloud Interface Name	CloudConnect	
Local IP Address	fwip-LAN	
DNS	--Please Select--	
<b>Advanced Options</b>		
Encryption	Triple-DES	
Compression	On	

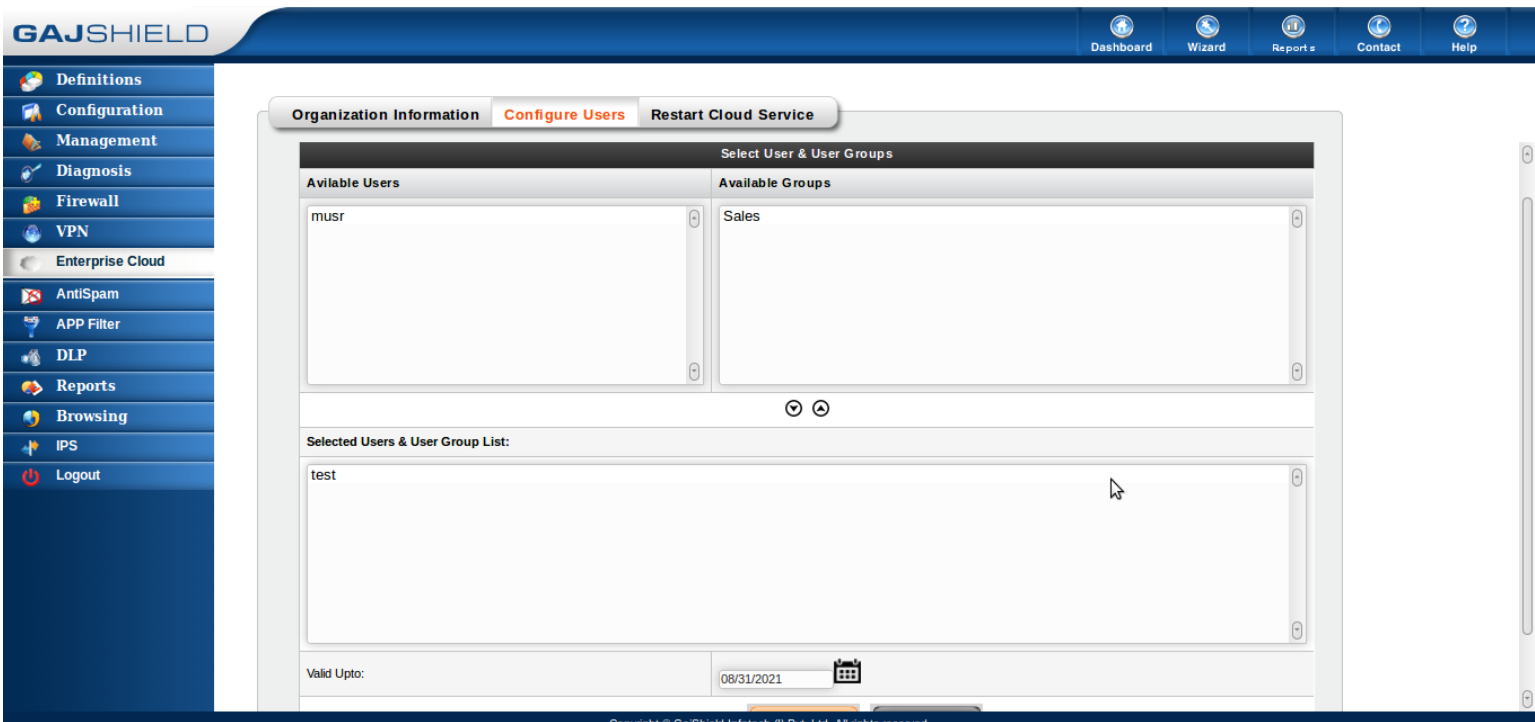
- **Primary IP Information:** First priority will be given to this IP by Cloud client.
- **Failover IPs (Optional):** Select multiple IP's of different ISP for failover. Second priority will be given to failover IP's, when primary IP is not reachable.
- **Service:** Create / select port for the cloud client to link with GajShield, use port number greater than 1024 TCP / UDP.  
**Note: UDP ports / services will not work when selecting cloud failover option**
- **Subnet for Cloud Client:** Cloud Clients will use IP address from this Subnet once the clients connect to GajShield.
- **Local IP Address:** Cloud Clients would connect to the LAN network through this IP.
- **DNS:** Public or Private IP which can be used by Cloud Clients to resolve DNS to browse Internet / intranet.
- **Encryption:** Data is encrypted between the Cloud client and GajShield firewall, using (Blowfish, AES & Triple-DES). Select any one from the drop-down list.

- **Compression:** Traffic travelling between the cloud client and GajShield firewall is compressed, when this option is kept ON.

3. Final Cloud configuration will look like the below image.



4. Go to Configure Users tab and click on

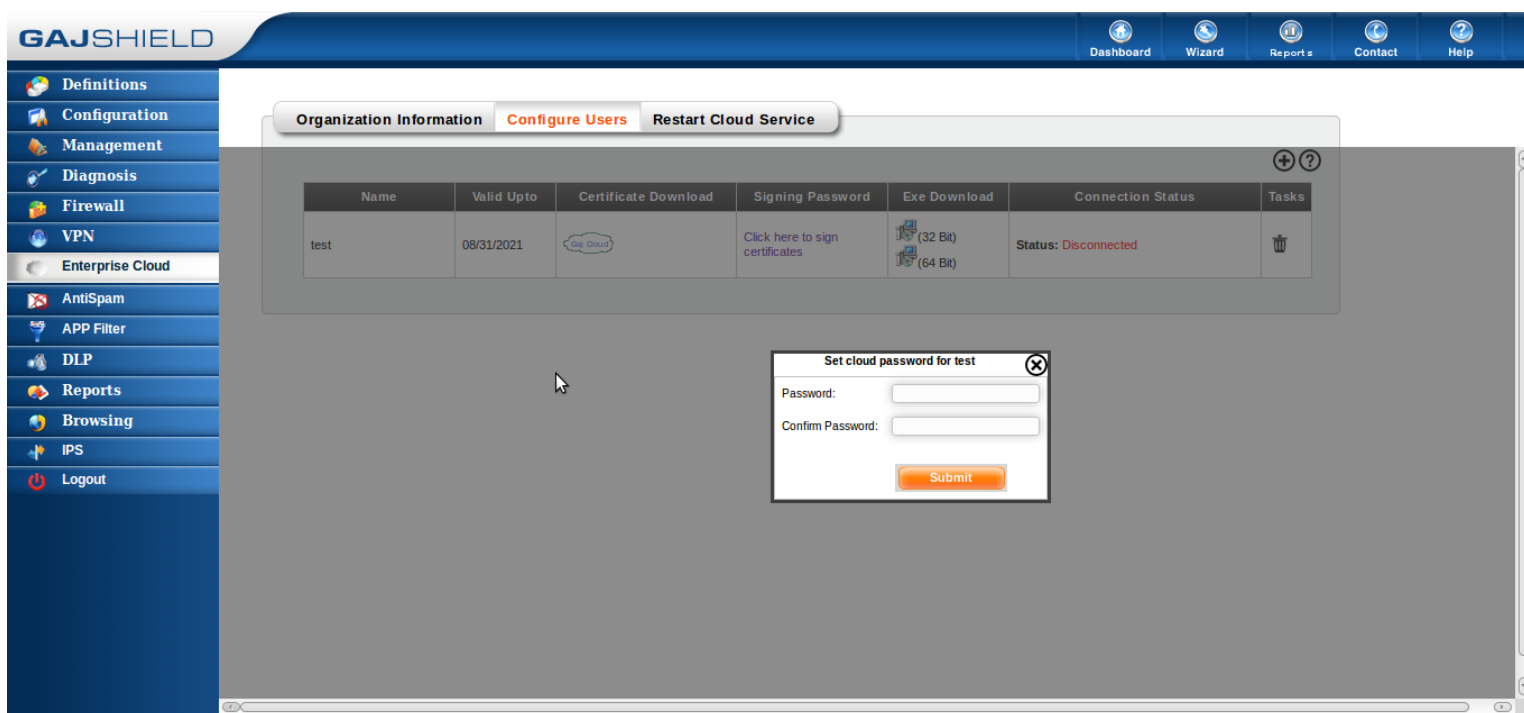




- Move users or group by simply selecting them and clicking on, from Available Users or Available Groups tab to Selected Users & Users Group List. To remove user or groups from Selected Users & Users Group List, select the users or group and click on.
- **Valid Up to:** Set expire date by clicking on for the cloud client, after the said date the cloud client will not be functional.
- Click on Submit button if the entered data is correct or click on Reset to remove the values inserted.

**Note: To add new users or group in clouds Available Users or Available Groups list, add them from Browsing >> Users setting.**

5. After adding the user to cloud services, sign the exe by clicking on Click here to sign



- Insert same password in both the boxes and click on submit.

**Note: This password can be used to disconnect or uninstall the cloud client.**

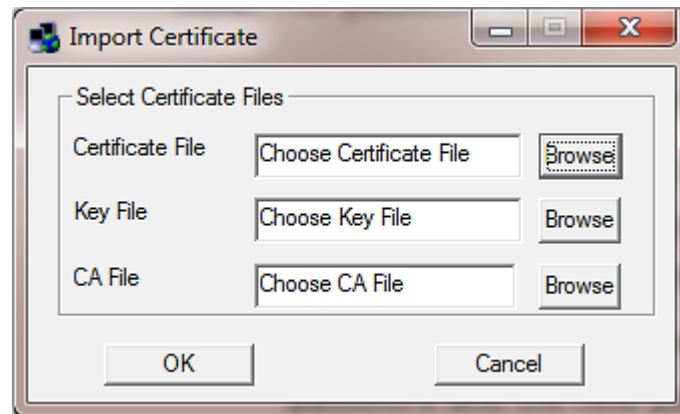
**Important:** Restart Cloud Service, if you make any changes in Organization Information tab.

6. Now you can download the cloud client exe by clicking on . If you want to download only the user certificate click on save the zip folder containing 3 files. For example (ca.crt, guest-client.crt, guest-client.key)

**Important:** Install cloud client on normal user login, & use "Run as Administrator" to install cloud client.

7. To change password of the cloud client on users PC, where the cloud client is installed. Right click on cloud icon shown on the right side of your taskbar. Select Change Password, a pop-up will open insert old password and the new password.

8. If you have forgotten the password of the cloud client exe, you will have to re-create the user exe (repeat step 4 & 5) and download the new user certificate from the firewall (see step 6) and not the cloud client exe. Import the 3 files downloaded from the firewall in the respective boxes as shown below.



Certificate downloaded from the firewall for example is guest-client.zip, contains 3 files as show below

1. ca.crt
2. guest-client.crt
3. guest-client.key





















**Note: Import the above three files in their respective sections.**

- **Certificate File: Import "guest-client.crt"**
- **Key File: Import "guest-client.key"**
- **CA File: Import "ca.crt"**



9. After configuring enterprise cloud, you will need to add firewall policy to allow mobile users to connect to the firewall.

Go to Firewall >> Policies >> Rules and add policies according to your organizations requirements. Show below is an example of firewall policy for cloud client.

1	IPv4	WAN To WAN	internet	fwip-WAN	Cloud-Consumer-Port	-	-	accept	AllTime	-	   
2	IPv4	Any To Any	cloudnetwork	internet	Browse	-	Url Filter Policy: <a href="#">Open</a> SSL Deep Inspect: off	accept	AllTime	-	   
3	IPv4	Any To Any	cloudnetwork	internet	DNS	-	-	accept	AllTime	-	   
4	IPv4	Cloud To LAN	cloudnetwork	fwnet-LAN	Any	-	-	accept	AllTime	-	   
5	IPv4	Cloud To LAN	cloudnetwork	fwip-LAN	DNS	-	-	accept	AllTime	-	   

You have successfully configured Enterprise Cloud on your firewall.