

How to configure Enterprise Cloud

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

Important: Below configuration can be used in all type of browsing mode. When Transparent Mode or Proxy with No User Authentication is enabled, you will see IP address instead of username in the cloud users list. To check current browsing mode go to Browsing → Setup → Browsing Options.

1. Go to Organization Information and fill in the details to create CA Certificate.

The screenshot shows the GajShield SecureGate v5 Firewall Management interface. On the left is a navigation menu with options: NETWORK, FIREWALL, USERS, VPN, ENTERPRISE CLOUD, ANTI-SPAM, DLP, SYSTEM, ADMIN, REPORT, BROWSING, IPS, and LOGOUT. The 'ENTERPRISE CLOUD' option is highlighted. The main panel has three tabs: 'Organization Information' (selected), 'Configure Users', and 'Restart Cloud Service'. The 'Add CA Certificate' form is displayed with the following fields: Certificate Name, Valid Upto (4/12/2011), Key Length (512), Password, Confirm Password, Local ID (X.509 DN), Country Name (India), State, Locality Name, Organization Name, Organization Unit Name, Common Name, and Email Address. An 'Add' button is at the bottom of the form. The footer of the interface reads 'Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved.'

Note: If you find this certificate created beforehand, it is the same certificate created under Browsing → Setup → SSL Certificate used for scanning https browsing traffic.

- **Certificate Name:** A unique name to identify the CA Certificate.
- **Valid upto:** 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 is required.
- **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.

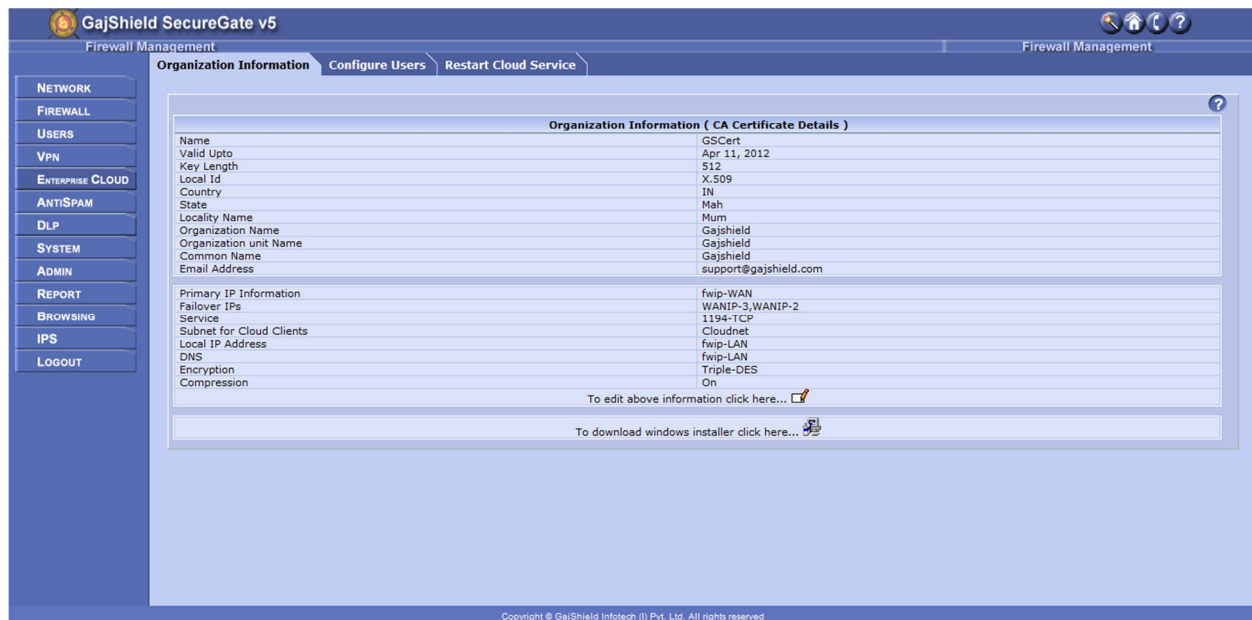
2. Select Cloud configuration as required, under Cloud Service Information.

The screenshot shows the GajShield SecureGate v5 Firewall Management interface. The left sidebar contains a menu with options: NETWORK, FIREWALL, USERS, VPN, ENTERPRISE CLOUD, ANTI-SPAM, DLP, SYSTEM, ADMIN, REPORT, BROWSING, IPS, and LOGOUT. The main content area has three tabs: Organization Information (selected), Configure Users, and Restart Cloud Service. The Organization Information tab displays a table of details for a CA Certificate, including Name (GSCert), Valid Upto (Apr 11, 2012), Key Length (512), Local Id (X.509), Country (IN), State (Mah), Locality Name (Mum), Organization Name (Gajshield), Organization unit Name (Gajshield), Common Name (Gajshield), and Email Address (support@gajshield.com). Below this is the Cloud Service Information section, which includes fields for Primary IP Information (a dropdown menu), Failover IPs (Optional) (a list box with options: fwip-WAN, fwip-LAN, WANIP-3, WANIP-2, WANIP-4), Service (a dropdown menu), Subnet for Cloud Clients (a dropdown menu), Local IP Address (a dropdown menu), and DNS (a dropdown menu). There are also Advanced Options for Encryption (AES) and Compression (On). At the bottom of the Cloud Service Information section are buttons for Save, Reset, and Cancel.

- **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.
- **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.

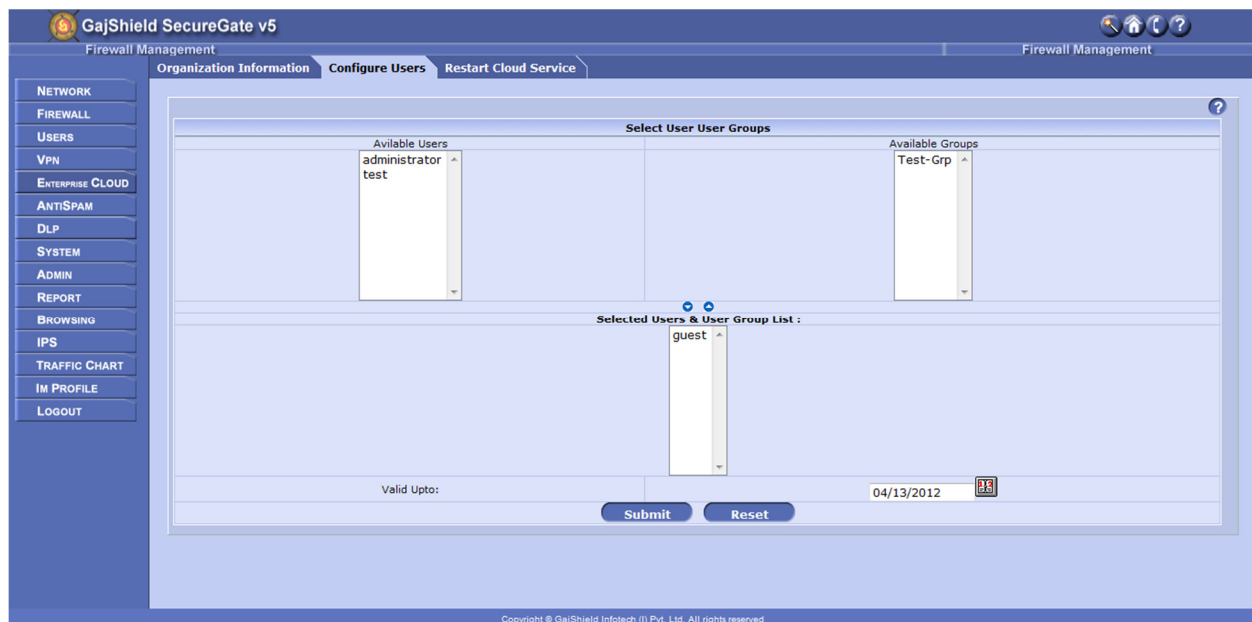
3. Final Cloud configuration will look like the below image.



- To edit the existing Cloud configuration click on , it will allow you to change the Cloud setup.
- Download plan exe without password & user certificate, by clicking on .

Note: After editing cloud settings, you will have to recreate the cloud exe under Configure Users tab, Restart Cloud Service  and install the same exe on the client PC.

4. Go to Configure Users tab and click on .



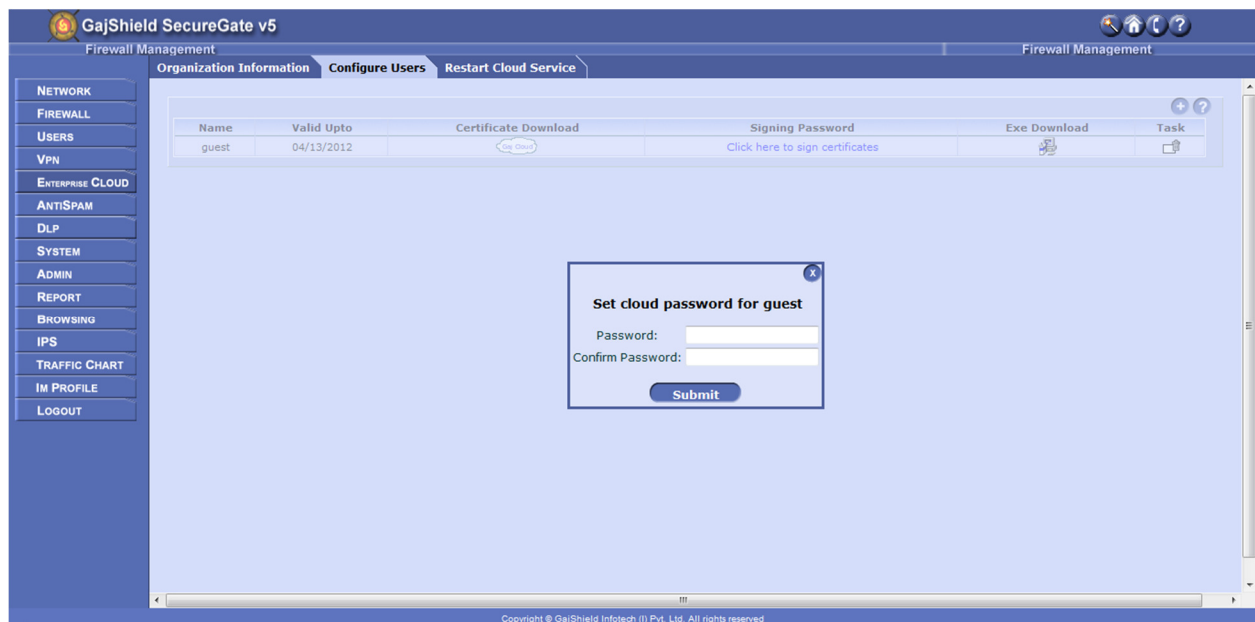
- Move users or group by simply selecting them and clicking on , from Available Users or Available Groups tab to Selected Users & Users Group List. To remove

user or groups from Selected Users & Users Group List, select the users or group and click on .

- **Valid Upto:** 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 on sign certificates](#).



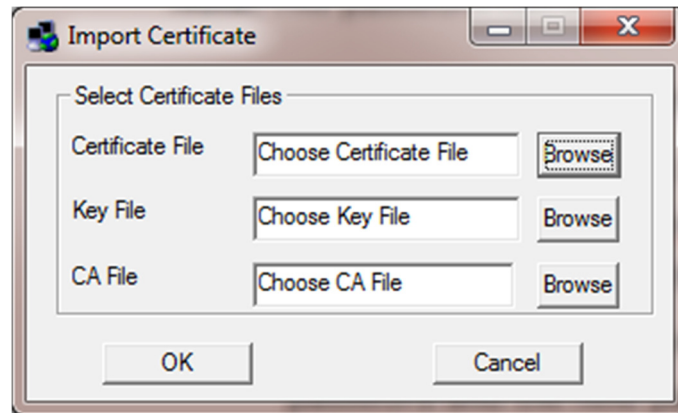
- Insert same password in both the boxes and click on submit.

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 or Configure Users 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)
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 shown 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"

For further assistance please Contact GajShield Support on +91 22 66607450 / 51/ 52/ 53

Email: support@gajshield.com